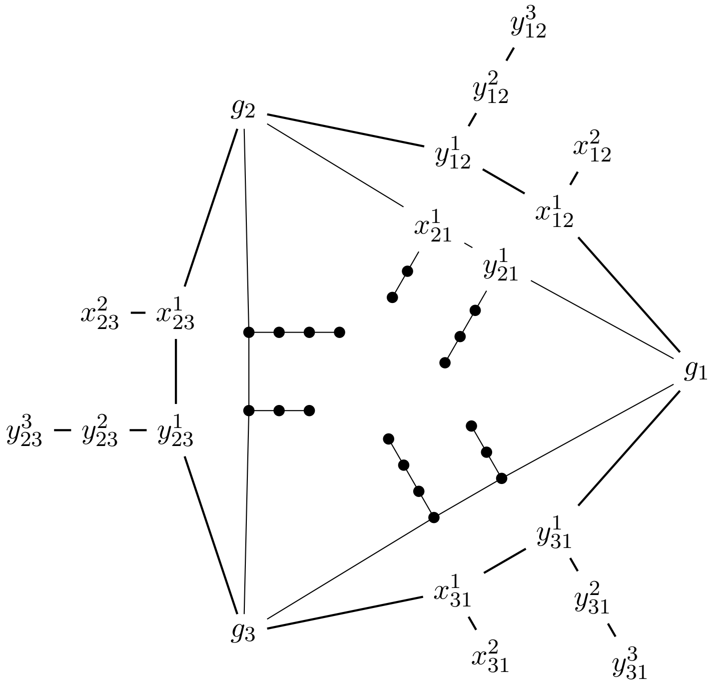
Discrete Mathematics

Lecture notes summer semester 2021

Benjamin Sambale
Leibniz Universität Hannover

Version: April 6, 2026



Contents

Warning: This is an AI-translated version of my German lecture notes, performed by *Gemini 3 Flash Preview*. I have not checked whether Gemini introduced errors. Use with care!

Preface

These notes originated from a 4+2 lecture in the summer semester 2021 (14 weeks) at Leibniz University Hannover. The course was primarily aimed at Bachelor students of mathematics as well as students in interdisciplinary Bachelor programs (teacher training). Knowledge of Algebra 1 was assumed.

Discrete mathematics deals with objects that are in some sense *finite* (e.g., finite sets, graphs, finite-dimensional vector spaces). It differs in this point from analysis, where *continuous* (not "indiscrete") objects are studied (e.g., real numbers, limits, infinite series, integrals). Discrete mathematics is thus a very extensive field, from which we study only the subareas *combinatorics* and *graph theory* in this lecture. Some sections of the notes (especially Chapter 3 and Chapter 8) were not discussed in the lecture.

Literature:

- M. Aigner, *Diskrete Mathematik*, 6th edition, Vieweg Verlag, Wiesbaden, 2006
- R. Diestel, *Graphentheorie*, 5th edition, Springer Verlag, Heidelberg, 2017

I especially thank David Munkacsi for his very careful reading and numerous error reports. For further error reports, I am also grateful to: Luca Blaas, Karl Böhlke, Lars Kühne, Lara Lütkemeyer, Luca Pawletzki, Claude Sonnet (4.6), Inga Stolley, Júlia Víllora Martí, and Alexander Witt.

Combinatorics

Remark. Combinatorics is the study of counting discrete objects:

- (easy) The number of k-element subsets of an n-element set is $\binom{n}{k}$.
- (medium) The number of fixed-point-free permutations on $\{1, \ldots, n\}$ is $[n!/e]$.
- (hard) The number of partitions of $5n + 4$ is divisible by 5.
- (very hard) Every map can be colored with four colors such that adjacent countries have different colors.
- (unsolved) How many magic squares of size 6×6 are there?

1 Finite Sets

Definition 1.1.

- Empty set: $\varnothing$.
- Natural numbers: $\mathbb{N} = \{1, 2, \ldots\}$, $\mathbb{N}_0 = \{0, 1, \ldots\}$.
- Integers: $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$.
- Rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\}$.
- Real numbers: $\mathbb{R}$ (Analysis).
- Complex numbers: $\mathbb{C} = \{a + b\mathrm{i} : a, b \in \mathbb{R}\}$.
- For a set A, let $|A|$ be the cardinality of A. One calls A *finite*, if $|A| < \infty$ and otherwise *infinite*. We do not distinguish between cardinalities (countable, uncountable etc.) with the notation $|A| = \infty$. Two sets A and B are called *equinumerous*, if a bijection $A \to B$ exists.
- If A_i $(i \in I)$ are sets, then so is their *Cartesian product* $\bigtimes_{i\in I} A_i = \big\{(a_i : i \in I) : a_i \in A_i\big\}$. In the case $A = A_i$ for all $i \in I$, we also write $A^I := \bigtimes_{i\in I} A$. For $I = \{1, \ldots, n\}$, we write $A_1 \times \ldots \times A_n$ and $A^n = A \times \ldots \times A$ (n factors).
- If A_i $(i \in I)$ are sets, then so is their *disjoint union*

  $$\bigsqcup_{i\in I} A_i := \bigcup_{i\in I}\{(a, i) : a \in A_i\} \subseteq \big(\bigcup_{i\in I} A_i\big) \times I.$$

  For $I = \{1, \ldots, n\}$, we write $A_1 \sqcup \ldots \sqcup A_n$.
- For a set A, $2^A := \{B \subseteq A\}$ is the *power set* of A. For $k \in \mathbb{N}_0$, let

  $$\binom{A}{k} := \{B \subseteq A : |B| = k\} \subseteq 2^A$$

  be the set of k-element subsets of A.

Remark 1.2. For sets A and I, one can identify A^I with the set of all mappings $I \to A$ by replacing $(a_i)_{i\in I} \in A^I$ with $f\colon I \to A$ where $f(i) := a_i$.

Theorem 1.3. *For finite sets $A, B, A_1, \dots, A_n$, the following hold:*

(i) $|A_1 \times \dots \times A_n| = |A_1| \dots |A_n|$ *and* $|A^n| = |A|^n$.

(ii) $|A_1 \sqcup \dots \sqcup A_n| = |A_1| + \dots + |A_n|$.

(iii) A *and* B *are equinumerous if and only if* $|A| = |B|$.

(iv) $|2^A| = 2^{|A|}$.

Proof.

(i) For each element $(a_1, \dots, a_n) \in A_1 \times \dots \times A_n$, there are $|A_1|$ possibilities to choose a_1, $|A_2|$ possibilities for a_2, and so on. Conversely, each such choice yields exactly one element of $A_1 \times \dots \times A_n$.

(ii) Each element in $A_1 \sqcup \dots \sqcup A_n$ lies in exactly one of the sets $\{(a, i) : a \in A_i\}$. Furthermore, $|\{(a, i) : a \in A_i\}| = |A_i|$ holds.

(iii) Let $A = \{a_1, \dots, a_n\}$ and $f\colon A \to B$ be a bijection. Then $B = \{f(a_1), \dots, f(a_n)\}$ with $f(a_i) \neq f(a_j)$ for $i \neq j$. This shows $|B| = n = |A|$. Conversely, let $|A| = |B|$ and $A = \{a_1, \dots, a_n\}$ as well as $B = \{b_1, \dots, b_n\}$. Then $f\colon A \to B$, $a_i \mapsto b_i$ is a bijection.

(iv) Let $A = \{a_1, \dots, a_n\}$. For $B \subseteq A$, let $f(B) := (x_1, \dots, x_n) \in \{0, 1\}^n$ with $x_i = 1 \iff a_i \in B$. Then $f\colon 2^A \to \{0, 1\}^n$, $B \mapsto f(B)$ is a bijection. From (iii) and (i) it follows that

$$|2^A| = |\{0, 1\}^n| = |\{0, 1\}|^n = 2^n = 2^{|A|}. \qquad \square$$

Definition 1.4.

- For $n \in \mathbb{N}_0$, $n! := \prod_{k=1}^{n} k$ is the *factorial* of n. Note: $0! = 1$ (empty product).
- For $a \in \mathbb{C}$ and $k \in \mathbb{N}_0$, one defines the *binomial coefficient*

$$\boxed{\binom{a}{k} := \frac{a(a-1)\dots(a-k+1)}{1 \cdot 2 \cdot \dots \cdot k}.}$$

- For $n, k_1, \dots, k_s \in \mathbb{N}_0$ with $n = k_1 + \dots + k_s$, let

$$\boxed{\binom{n}{k_1, \dots, k_s} := \frac{n!}{k_1! \dots k_s!}}$$

be the *multinomial coefficient* of n and $k_1, \dots, k_s$.

Remark 1.5. We have $\binom{a}{0} = 1$ (empty product) and $\binom{n}{k} = 0$ for $k > n \in \mathbb{N}_0$. For $k \leq n \in \mathbb{N}_0$ it holds that

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{1 \cdot 2 \cdot \dots \cdot k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k} = \binom{n}{k, n-k}$$

and

$$\boxed{\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}}$$

(see Remark 1.14). One can therefore calculate the binomial coefficients using *Pascal's triangle*:

$$\begin{array}{ccccccccc} &&&&\binom{0}{0}&&&& \\ &&&\binom{1}{0}&&\binom{1}{1}&&& \\ &&\binom{2}{0}&&\binom{2}{1}&&\binom{2}{2}&& \\ &\binom{3}{0}&&\binom{3}{1}&&\binom{3}{2}&&\binom{3}{3}& \\ \binom{4}{0}&&\binom{4}{1}&&\binom{4}{2}&&\binom{4}{3}&&\binom{4}{4} \end{array} \qquad \begin{array}{ccccccccc} &&&&1&&&& \\ &&&1&&1&&& \\ &&1&&2&&1&& \\ &1&&3&&3&&1& \\ 1&&4&&6&&4&&1 \end{array}$$

Remark 1.6 ("Variation with repetition")**.** For finite sets A and B, there exist exactly $|B^A| = |B|^{|A|}$ maps $A \to B$ according to Theorem 1.3.

Example 1.7. A 4-digit combination lock has $10^4 = 10{,}000$ possible states (choose $A = \{1, 2, 3, 4\}$ and $B = \{0, 1, \ldots, 9\}$ in Remark 1.6). If a thief checks one state per second, he needs on average approx. 83 minutes to crack the lock.[1]

Theorem 1.8 ("Variation without repetition")**.** *For finite sets A and B, there exist exactly $\binom{|B|}{|A|}|A|!$ injective maps $A \to B$.*

Proof. In the case $|A| > |B|$, there are no injective maps $A \to B$ and indeed $\binom{|B|}{|A|} = 0$. Now let $k := |A| \le |B| =: n$ and $A = \{a_1, \ldots, a_k\}$. For every injective map $f : A \to B$, there are n possibilities for $f(a_1)$. Once $f(a_1)$ is fixed, there remain $n - 1$ possibilities for $f(a_2) \in B \setminus \{f(a_1)\}$ and so on. The number of injective maps is therefore $n(n-1)\ldots(n-k+1) = \frac{n!}{(n-k)!} = \binom{n}{k}k!$. ☐

Example 1.9 (Birthday Paradox)**.** For persons $P_1, \ldots, P_n$ we consider the mapping

$$f : \{1, \ldots, n\} \to \{1, \ldots, 365\},$$

which maps i to the birthday of P_i (leap years, twins etc. neglected). According to Remark 1.6 there are 365^n such mappings, of which $\binom{365}{n}n!$ are injective. The probability that at least two persons have their birthday on the same day is therefore

$$1 - \binom{365}{n}\frac{n!}{365^n}$$

(Laplace formula). For $n = 23$ one already obtains $> 50\%$.

Remark 1.10.

(i) The case $|A| > |B|$ in Theorem 1.8 yields the *Dirichlet pigeonhole principle*: If one distributes n objects into $k < n$ drawers, then at least one drawer must contain several objects. Example: In Hanover there are two persons with the same number of hairs on their head, because nobody has more hairs than Hanover has inhabitants ($> 500{,}000$).

---

[1] That was the 32,000-Euro question in the TV show "Who Wants to Be a Millionaire" (German edition) on 26.04.21.

(ii) In the case $|A| = |B|$, every injective mapping $A \to B$ is also bijective (provided $|A| < \infty$). Bijections $A \to A$ are called *permutations* on A. As is well known, the permutations on A form the *symmetric group* $\mathrm{Sym}(A)$ with respect to composition of mappings. The neutral element is id_A and the inverse to $f \in \mathrm{Sym}(A)$ is the inverse mapping f^{-1}. We set $S_n := \mathrm{Sym}(\{1, \ldots, n\})$. According to Theorem 1.8 we have

$$|\mathrm{Sym}(A)| = |S_{|A|}| = \binom{|A|}{|A|}|A|! = |A|!.$$

Example 1.11.

$$S_3 := \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Theorem 1.12 ("Combination without repetition"). *For every finite set A and $k \in \mathbb{N}_0$ we have*

$$\boxed{\left|\binom{A}{k}\right| = \binom{|A|}{k}.}$$

Proof. Let $K := \{1, \ldots, k\}$. Every k-element subset $B \subseteq A$ is the image of an injective mapping $f\colon K \to A$. If two such mappings f and g have the same image, then $f^{-1} \circ g\colon K \to K$ is injective, thus in $\mathrm{Sym}(K)$. Every B therefore arises from exactly $|\mathrm{Sym}(K)| = k!$ many injective mappings. The assertion now follows from Theorem 1.8. □

Example 1.13. In the lottery "6 out of 49" there are $\binom{49}{6} = 13,983,816$ possibilities and the probability for a 4-match is

$$\frac{\binom{6}{4}\binom{43}{2}}{\binom{49}{6}} = \frac{645}{665896} \approx 0.1\%.$$

Remark 1.14.

(i) The bijection $\binom{A}{k} \to \binom{A}{|A|-k}$, $B \mapsto A \setminus B$ explains the symmetry $\binom{n}{k} = \binom{n}{n-k}$. Likewise, the identity $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ can be interpreted combinatorially: For $a \in A$, there are exactly $\binom{|A\setminus\{a\}|}{k-1}$ subsets $B \in \binom{A}{k}$ that contain a and $\binom{|A\setminus\{a\}|}{k}$ subsets $B \in \binom{A}{k}$ that do not contain a.

(ii) According to Theorem 1.3 and Theorem 1.12,

$$2^n = |2^{\{1,\ldots,n\}}| = \sum_{k=0}^{n} \binom{n}{k}.$$

This is a special case of the well-known *binomial theorem* (set $a = b = 1$)

$$\boxed{(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}} \qquad (a, b \in \mathbb{C}).$$

Lemma 1.15 (Polynomial method). *Two polynomials $\alpha, \beta \in \mathbb{C}[X]$ are identical if they coincide at infinitely many points $x \in \mathbb{C}$.*

Proof. By assumption, $\alpha - \beta$ has infinitely many roots. According to Algebra 1, $\alpha - \beta$ must be the zero polynomial (otherwise the number of roots would be bounded by the degree). □

Theorem 1.16 (VANDERMONDE identity)**.** *For $n, k \in \mathbb{N}_0$ and $a_1, \ldots, a_n \in \mathbb{C}$, the following holds:*

$$\boxed{\binom{a_1 + \ldots + a_n}{k} = \sum_{\substack{(k_1,\ldots,k_n)\in\mathbb{N}_0^n\\ k_1+\ldots+k_n=k}} \binom{a_1}{k_1}\ldots\binom{a_n}{k_n}.}$$

Proof. We first prove the claim only for $a_1, \ldots, a_n \in \mathbb{N}$. Let $A_1, \ldots, A_n$ be sets with $|A_i| = a_i$ for $i = 1, \ldots, n$. We determine $\left|\binom{A_1\sqcup\ldots\sqcup A_n}{k}\right|$ in two ways. According to Theorem 1.12, on the one hand,

$$\left|\binom{A_1 \sqcup \ldots \sqcup A_n}{k}\right| = \binom{|A_1 \sqcup \ldots \sqcup A_n|}{k} = \binom{a_1 + \ldots + a_n}{k}.$$

On the other hand, every k-element subset of $A_1 \sqcup \ldots \sqcup A_n$ is composed of k_i-element subsets of A_i for $i = 1, \ldots, n$ and $k_1 + \ldots + k_n = k$. For each of these subsets, there are $\left|\binom{A_i}{k_i}\right| = \binom{a_i}{k_i}$ possibilities. This shows

$$\left|\binom{A_1 \sqcup \ldots \sqcup A_n}{k}\right| = \sum_{\substack{(k_1,\ldots,k_n)\in\mathbb{N}_0^n\\ k_1+\ldots+k_n=k}} \binom{a_1}{k_1}\ldots\binom{a_n}{k_n}.$$

We now fix $a_1, \ldots, a_{n-1} \in \mathbb{N}$ and replace a_n with an indeterminate X. Then both sides of the equation are polynomials in X that coincide at infinitely many points $x \in \mathbb{N}$. According to the polynomial method, the polynomials are equal and the equation also holds when a complex number a_n is substituted for X. One can now fix $a_1, \ldots, a_{n-2}, a_n$ and repeat the argument with a_{n-1}, and so on. ☐

Example 1.17. The special case $n = 2$ and $a_1 = a_2 = k$ in Theorem 1.16 yields

$$\binom{2k}{k} = \sum_{i=0}^{k} \binom{k}{i}\binom{k}{k-i} = \sum_{i=0}^{k} \binom{k}{i}^2.$$

Theorem 1.18 ("Variation with repetition" II)**.** *Let $A = \{a_1, \ldots, a_n\}$ and B be finite sets and $k_1, \ldots, k_n \in \mathbb{N}_0$ with $|B| = k_1 + \ldots + k_n$. Then there exist exactly $\binom{|B|}{k_1,\ldots,k_n}$ mappings $f\colon B \to A$ with $|f^{-1}(a_i)| = k_i$ for $i = 1, \ldots, n$.*

Proof. Let $|B| = k$ and $f\colon B \to A$ with $|f^{-1}(a_i)| = k_i$ for $i = 1, \ldots, n$. According to Theorem 1.12 there are $\binom{k}{k_1}$ possibilities for $f^{-1}(a_1)$. Once $f^{-1}(a_1)$ is fixed, there remain $\binom{k-k_1}{k_2}$ possibilities for $f^{-1}(a_2)$ etc. Thus there are

$$\binom{k}{k_1}\binom{k-k_1}{k_2}\ldots\binom{k-k_1-\ldots-k_{n-1}}{k_n} = \frac{k!(k-k_1)!\ldots(k-k_1-\ldots-k_{n-1})!}{k_1!(k-k_1)!k_2!(k-k_1-k_2)!\ldots k_n!} = \binom{k}{k_1,\ldots,k_n}$$

possibilities for f. ☐

Example 1.19.

(i) An *anagram* is a permutation of the letters of a word.[2] According to Theorem 1.18 there are $\binom{9}{3,2,1,1,1,1} = 30{,}240$ anagrams of RAMANUJAN (choose $A = \{a, n, r, m, u, j\}$, $B = \{1, \ldots, 9\}$, $k_1 = 3$, $k_2 = 2$, $k_3 = \ldots = k_6 = 1$). For example JANUARMAN or MANJURANA.

---

[2] Galileo published his discovery of the rings of Saturn (Altissimvm planetam tergeminvm observavi) as the anagram SMAISMRMILMEPOETALEVMIBVNENVGTTAVIRAS, which however no one could decipher.

(ii) There are $\binom{32}{10,10,10,2} = 2,753,294,408,504,640$ possibilities to distribute 32 Skat cards to three players (choose $A = \{1,2,3,4\}$, $B = \{1,\ldots,32\}$, $k_1 = k_2 = k_3 = 10$ and $k_4 = 2$ in Theorem 1.18). If one does not wish to distinguish the players, the number is reduced by the factor $3! = 6$. The number of possible game courses is much larger and most likely not exactly known.

Remark 1.20. According to Remark 1.6 and Theorem 1.18

$$n^k = |\{1,\ldots,n\}^k| = \sum_{\substack{(k_1,\ldots,k_n)\in\mathbb{N}_0^n \\ k_1+\ldots+k_n=k}} \binom{k}{k_1,\ldots,k_n}.$$

This is a special case of the *multinomial theorem*

$$\boxed{(a_1+\ldots+a_n)^k = \sum_{\substack{(k_1,\ldots,k_n)\in\mathbb{N}_0^n \\ k_1+\ldots+k_n=k}} \binom{k}{k_1,\ldots,k_n} a_1^{k_1}\ldots a_n^{k_n}} \qquad (a_1,\ldots,a_n \in \mathbb{C})$$

(Exercise 6). For $n = 2$ one obtains the binomial theorem.

Definition 1.21. For an arbitrary set A, the elements from $\mathbb{N}_0^A$ are called *multisets* over A. One can interpret a multiset $M := (m_a)_{a\in A}$ as a “subset” of A, where each $a \in A$ occurs exactly m_a times (in the case $m_a \le 1$ for all $a \in A$, M is thus a true set). Accordingly, one sets $|M| := \sum_{a\in A} m_a$. We will often denote multisets in the form $\{a,a,b,c,c,c,\ldots\}$, where, as with sets, the order of the elements does not matter.

Theorem 1.22 (“Combination with replacement”). *An n-element set has exactly*

$$\boxed{\left(\!\!\binom{n}{k}\!\!\right) := \binom{n+k-1}{k}}$$

k-element multisets $(n,k \in \mathbb{N}_0)$.

Proof. Wlog. let $A = \{1,\ldots,n\}$. One can then identify the k-element multisets over A with the tuples $(a_1,\ldots,a_k) \in A^k$ with $a_1 \le \ldots \le a_k$. Let A_k be the set of these k-tuples and let $B_k = \binom{\{1,\ldots,n+k-1\}}{k}$. Then the maps

$$\begin{aligned} f\colon A_k &\to B_k, \\ (a_1,\ldots,a_k) &\mapsto \{a_1, a_2+1,\ldots,a_k+k-1\} \\ g\colon B_k &\to A_k, \\ \{b_1,\ldots,b_k\} &\mapsto (b_1, b_2-1,\ldots,b_k-k+1) \end{aligned}$$

are inverse bijections to each other. From Theorem 1.12 it follows that $|A_k| = |f(A_k)| = \binom{n+k-1}{k}$. □

Example 1.23.

(i) The 3-element multisets of $\{1,2\}$ are $\{1,1,1\}$, $\{1,1,2\}$, $\{1,2,2\}$ and $\{2,2,2\}$.

(ii) When simultaneously throwing three identical dice, there are $\left(\!\binom{6}{3}\!\right) = \binom{8}{3} = 56$ possible events, which, however, are not all equally probable.

Remark 1.24.

(i) For $1 \leq k \leq n$ it holds that

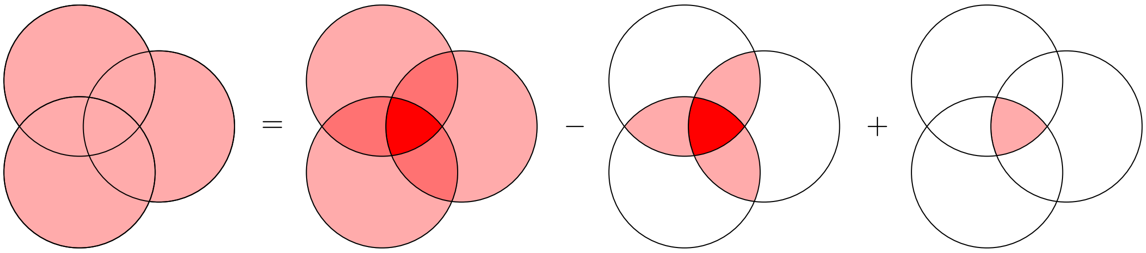
$$\left(\!\!\binom{n+1}{k}\!\!\right) = \binom{n+k}{k} = \binom{n+k-1}{k-1} + \binom{n+k-1}{k} = \left(\!\!\binom{n+1}{k-1}\!\!\right) + \left(\!\!\binom{n}{k}\!\!\right).$$

(ii) Summary:

	with replacement	without replacement
Variation	n^k	$n(n-1)\dots(n-k+1)$
Combination	$\binom{n+k-1}{k}$	$\binom{n}{k}$

Remark 1.25. For finite sets A and B, it is well known that $|A \cup B| = |A| + |B| - |A \cap B|$. Apparently, it also holds that

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$



This can be generalized as follows.

Theorem 1.26 (Inclusion-Exclusion Principle)**.** *For finite sets $A_1, \dots, A_n$ it holds that*

$$\boxed{|A_1 \cup \dots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}|.}$$

Proof. We count how many times an element $a \in A_1 \cup \dots \cup A_n$ is taken into account on the right side. For this, let wlog. $a \in A_1 \cap \dots \cap A_l$ and $a \notin A_i$ for $i > l$. Then a is counted if and only if $\{i_1, \dots, i_k\} \subseteq \{1, \dots, l\}$ holds. In the k-th summand, a is thus counted $(-1)^{k+1}\binom{l}{k}$ times. In total, a is counted on the right side exactly

$$\sum_{k=1}^{l} (-1)^{k+1} \binom{l}{k} = 1 - \sum_{k=0}^{l} (-1)^k \binom{l}{k} = 1 - (1-1)^l = 1$$

time. This shows the assertion. ☐

Definition 1.27. As usual, $a, b \in \mathbb{N}$ are called *coprime*, if 1 is the only common positive divisor of a and b, i. e. $\gcd(a, b) = 1$. One calls

$$\varphi(n) := \big|\{1 \leq a \leq n : \gcd(a, n) = 1\}\big| \qquad (n \in \mathbb{N})$$

the *Euler φ-function*.

Theorem 1.28. *Let $n = p_1^{a_1} \dots p_k^{a_k}$ be the prime factorization of $n \in \mathbb{N}$. Then*

$$\boxed{\varphi(n) = \prod_{i=1}^{k} (p_i^{a_i} - p_i^{a_i - 1}).}$$

Proof. For $i = 1, \dots, k$ let $A_i := \{1 \le a \le n : p_i \mid a\}$. Then $A := \{1 \le a \le n : \gcd(a, n) \neq 1\} = A_1 \cup \ldots \cup A_k$. For $1 \le i_1 < \ldots < i_l \le k$ we have

$$A_{i_1} \cap \ldots \cap A_{i_l} = \Big\{ j p_{i_1} \dots p_{i_l} : j = 1, \dots, \frac{n}{p_{i_1} \dots p_{i_l}} \Big\}.$$

With Theorem 1.26 it follows that

$$\begin{aligned} \varphi(n) &= |\{1, \dots, n\} \setminus A| = n - |A| = n + \sum_{l=1}^{k} (-1)^l \sum_{1 \le i_1 < \ldots < i_l \le k} \frac{n}{p_{i_1} \dots p_{i_l}} \\ &= n\Big(1 - \frac{1}{p_1}\Big) \dots \Big(1 - \frac{1}{p_k}\Big) = (p_1^{a_1} - p_1^{a_1 - 1}) \dots (p_k^{a_k} - p_k^{a_k - 1}). \end{aligned}$$

□

Example 1.29. $\varphi(100) = \varphi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 2 \cdot 20 = 40$.

Remark 1.30. In algebra, Theorem 1.28 is usually proven using the Chinese Remainder Theorem.

2 Permutations and Partitions

Definition 2.1.

- Let A be a set and $\sigma \in \mathrm{Sym}(A)$. One calls $a \in A$ a *fixed point* of σ, if $\sigma(a) = a$. If σ has no fixed points, then σ is called *fixed-point-free*.
- For $x \in \mathbb{R}$ let $[x] \in \mathbb{Z}$ with $|x - [x]| < \frac{1}{2}$ or $[x] = x + \frac{1}{2}$ ("rounding").

Theorem 2.2 (Montmort)**.** *The number of fixed-point-free permutations in S_n is $[n!/e]$, where $e = 2.718\dots$ is Euler's number.*

Proof. For $i = 1, \dots, n$ let $F_i := \{\sigma \in S_n : \sigma(i) = i\}$. The number f_n of fixed-point-free permutations of S_n is then $f_n = |S_n \setminus (F_1 \cup \ldots \cup F_n)| = n! - |F_1 \cup \ldots \cup F_n|$. For $1 \le i_1 < \ldots < i_k \le n$ we have

$$|F_{i_1} \cap \ldots \cap F_{i_k}| = |\mathrm{Sym}(\{1, \dots, n\} \setminus \{i_1, \dots, i_k\})| = (n - k)!.$$

Theorem 1.26 shows

$$f_n = n! + \sum_{k=1}^{n} (-1)^k \sum_{1 \le i_1 < \ldots < i_k \le n} (n-k)! = n! + \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Now

$$\Big| \frac{n!}{e} - f_n \Big| = \Big| n! \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \Big| = \frac{1}{n+1} - \frac{1}{(n+1)(n+2)} \pm \ldots < \frac{1}{n+1} \le \frac{1}{2}$$

and $f_n = [n!/e]$. □

Example 2.3.

(i) The fixed-point-free permutations of S_4 are

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\tag{2.1}$$

$$\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}.\tag{2.2}$$

(ii) In the pre-Christmas Secret Santa, n people give each other gifts by drawing lots beforehand, which state to whom the gift is to be directed. This describes a permutation on $\{1,\ldots,n\}$, which is fixed-point-free if and only if no person draws their own lot. The probability that at least one person draws their own lot is therefore $1-\frac{[n!/e]}{n!}\approx 1-\frac{1}{e}\approx 63\%$.

(iii) The encryption machine *Enigma* used in World War II permutes the 26 letters of the Latin alphabet. To supposedly make the encryption more secure, only fixed-point-free permutations were used. However, this was a decisive weakness that allowed the Allies to decrypt the Enigma.[3]

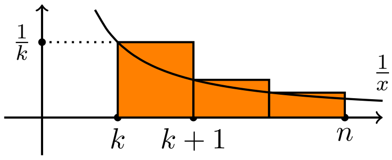
Example 2.4 (Secretary Problem)**.** There are n applicants for a vacant position invited one after another for an interview. Immediately after each interview, the applicant must be informed whether they have been hired or rejected. In the first case, the process is finished and no further applicants are considered. With which strategy does one find the best possible applicant?

One should first consistently reject the first $k<n$ applicants and then choose from the remaining $n-k$ the first one who is better than the first k applicants (possibly one must reject all applicants, in which case the strategy has failed). The order of the applicants describes a permutation $\sigma\in S_n$, where $\sigma(1)$ is the position of the best applicant and $\sigma(2)$ is the position of the second best, etc. Let

$$m:=\min\{i\le n:\sigma(i)<\sigma(1)\}.$$

The above strategy finds the best applicant if and only if $\sigma(1)>k$ and $\sigma(m)\le k$ holds. The probability that $\sigma(1)$ is at position l is $1/n$. The probability for $\sigma(m)\le k$ is then $\frac{k}{l-1}$. The success probability of the strategy is therefore

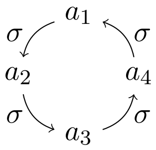
$$\sum_{l=k+1}^{n}\frac{1}{n}\frac{k}{l-1}=\frac{k}{n}\sum_{l=k}^{n-1}\frac{1}{l}\ge\frac{k}{n}\int_k^n\frac{1}{x}\,\mathrm{d}x=\frac{k}{n}(\log n-\log k).$$



The function $f(x)=\frac{x}{n}(\log n-\log x)$ has derivative $f'(x)=\frac{1}{n}(\log n-\log x-1)$ and therefore takes its maximum at $x=n/e$. For $k=[n/e]$, the success probability is thus approx. $f(n/e)=1/e\approx 37\%$ (for "large" n). One can show that this is the best strategy. For $n=20$, this results in $k=7$ and approx. 38%.

Definition 2.5. For a set A, one calls $\sigma\in\mathrm{Sym}(A)$ a (k-)*cycle* (or cycle of *length* k), if pairwise distinct $a_1,\ldots,a_k\in A$ exist, such that

$$\sigma(x)=\begin{cases}a_{i+1} & \text{if } x=a_i \text{ mit } i<k,\\ a_1 & \text{if } x=a_k,\\ x & \text{otherwise.}\end{cases}$$



---

[3] Wikipedia

One then writes $\sigma = (a_1, \ldots, a_k)$. This notation is unique up to "rotation", i. e.

$$\sigma = (a_2, \ldots, a_k, a_1) = \ldots = (a_k, a_1, \ldots, a_{k-1}).$$

The only 1-cycle is id_A. To keep formulations uniform, we will nevertheless formally distinguish the 1-cycles $(1), (2), \ldots, (n)$. Furthermore, we regard id_A as the product of all 1-cycles. Cycles of length 2 are called *transpositions*. Cycles $\sigma = (a_1, \ldots, a_k)$ and $\tau = (b_1, \ldots, b_l)$ are called *disjoint*, if

$$\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \varnothing.$$

Remark 2.6.

(i) It holds that $(a_1, \ldots, a_k)^{-1} = (a_k, a_{k-1}, \ldots, a_1)$.

(ii) Disjoint cycles $\sigma, \tau \in \mathrm{Sym}(A)$ commute, i. e. $\sigma \circ \tau = \tau \circ \sigma$. In the following, we will often omit the composition symbol $\circ$.

Lemma 2.7. *Every permutation σ of a finite set A is a composition of pairwise disjoint cycles $\sigma = \sigma_1 \ldots \sigma_k$ of length > 1 and these are uniquely determined up to their order.*

Proof. Existence: Let $A_\sigma := \{a \in A : \sigma(a) \neq a\}$. We argue by induction on $|A_\sigma|$. In the case $A_\sigma = \varnothing$, $\sigma = \mathrm{id}_A$ is the empty product. Now let $a \in A_\sigma \neq \varnothing$. Because $|A_\sigma| \le |A| < \infty$, the elements $a, \sigma(a), \sigma^2(a), \ldots \in A_\sigma$ cannot all be distinct. Thus, let $0 \le k < l$ with $\sigma^k(a) = \sigma^l(a)$. Then $\sigma^{l-k}(a) = a$. Let $s \in \mathbb{N}$ be minimal with $\sigma^s(a) = a$. Then $a, \sigma(a), \ldots, \sigma^{s-1}(a)$ are pairwise distinct and $\sigma_1 = (a, \sigma(a), \ldots, \sigma^{s-1}(a))$ is an s-cycle with $s > 1$. For $\tau := \sigma_1^{-1}\sigma \in \mathrm{Sym}(A_\sigma)$ and $i = 0, \ldots, s-1$, it then holds that

$$\tau(\sigma^i(a)) = \sigma_1^{-1}\sigma^{i+1}(a) = \sigma^i(a).$$

This shows $A_\tau = A_\sigma \setminus A_{\sigma_1}$. By induction, there exist pairwise disjoint cycles $\sigma_2, \ldots, \sigma_k \in \mathrm{Sym}(A_\tau)$ with length > 1 and $\tau = \sigma_2 \ldots \sigma_k$. Obviously, $\sigma_1, \ldots, \sigma_k$ are also pairwise disjoint and $\sigma = \sigma_1 \ldots \sigma_k$.

Uniqueness: Let $\sigma = \sigma_1 \ldots \sigma_k = \tau_1 \ldots \tau_l$ be two representations with pairwise disjoint cycles $\sigma_1, \ldots, \sigma_k$ as well as $\tau_1, \ldots, \tau_l$. Induction on k: For $k = 0$, $\sigma = \mathrm{id}_A$ and it follows that $l = 0$. Now let $k \ge 1$ and $a \in A$ with $\sigma_1(a) \neq a$. Then there exists exactly one τ_i with $\tau_i(a) = \sigma_1(a)$. Furthermore, $\sigma_1^2(a) = \tau_i^2(a)$ etc. This shows $\sigma_1 = \tau_i$. By multiplying both sides by σ_1^{-1}, one obtains $\sigma_2 \ldots \sigma_k = \tau_1 \ldots \tau_{i-1}\tau_{i+1} \ldots \tau_l$. The claim now follows easily by induction. $\square$

Remark 2.8.

(i) One can make the notation in disjoint cycles

$$\sigma = (a_1, \ldots, a_s)(b_1, \ldots, b_t) \ldots$$

completely unique by requiring $a_1 = \min\{a_1, \ldots, a_s\} < b_1 = \min\{b_1, \ldots, b_t\} < \ldots$. This is implemented in the computer algebra system GAP.

(ii) In the following, we say that $\sigma \in S_n$ *contains* a cycle τ if τ occurs in the disjoint cycle representation. In this context, we want to count the fixed points as 1-cycles.

(iii) As is well known (linear algebra), every permutation can also be written as a product of transpositions, although these are generally not disjoint.

Example 2.9.

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix} = (1,4,2)(3,6)$.

(ii) $(2,5,3,1)(3,1,6) = (1,6)(2,5,3) = (1,6)(2,5)(3,5)$ (maps are evaluated from right to left).

(iii) $S_3 = \{(), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

Theorem 2.10. *For $1 \leq k \leq n$, the following holds:*

(i) The number of k-cycles of S_n is $\frac{n!}{k(n-k)!}$.

(ii) If $z_k(\sigma)$ is the number of k-cycles of σ, then

$$\frac{1}{n!} \sum_{\sigma \in S_n} z_k(\sigma) = \frac{1}{k}.$$

(iii) The average number of cycles of a permutation $\sigma \in S_n$ is the n-th harmonic number

$$H_n := \sum_{s=1}^{n} \frac{1}{s}.$$

Proof.

(i) Each k-cycle permutes a k-element set $\{a_1, \ldots, a_k\} \subseteq \{1, \ldots, n\}$. For the choice of this set, there are $\binom{n}{k}$ possibilities (Theorem 1.12). Each k-cycle on this set can be uniquely written in the form $(a_1, b_2, \ldots, b_k)$ with $\{b_2, \ldots, b_k\} = \{a_2, \ldots, a_k\}$. This yields $(k-1)!$ cycles, because the digits $b_2, \ldots, b_k$ can be permuted arbitrarily. In total, there are

$$\binom{n}{k}(k-1)! = \frac{n!(k-1)!}{k!(n-k)!} = \frac{n!}{k(n-k)!}$$

cycles of length k.

(ii) Let $Z_k \subseteq S_n$ be the set of k-cycles. Each k-cycle is contained in $(n-k)!$ many permutations, because one can permute the $n-k$ digits outside the cycle arbitrarily. It follows that

$$\sum_{\sigma \in S_n} z_k(\sigma) = |\{(\sigma, c) \in S_n \times Z_k : \sigma \text{ contains } c\}| = \sum_{c \in Z_k} (n-k)! = |Z_k|(n-k)! \overset{\text{(i)}}{=} \frac{n!(n-k)!}{k(n-k)!} = \frac{n!}{k}.$$

(iii) The average number of cycles is

$$\frac{1}{n!} \sum_{\sigma \in S_n} \sum_{k=1}^{n} z_k(\sigma) = \frac{1}{n!} \sum_{k=1}^{n} \sum_{\sigma \in S_n} z_k(\sigma) \overset{\text{(ii)}}{=} \sum_{k=1}^{n} \frac{1}{k}.$$ □

Remark 2.11. As is well known (Analysis),

$$\gamma := \lim_{n \to \infty} (H_n - \log n) = 0{,}577\ldots$$

is the *Euler-Mascheroni constant*. For large n, $H_n \approx \log(n) + \gamma$ therefore holds. It is not yet known whether γ is rational.

Example 2.12.

(i) The average number of cycles of $\sigma \in S_8$ is $H_8 = \frac{761}{280} \approx 2{,}71$ (comparison: $\log(8) + \gamma \approx 2{,}67$).

(ii) (100 prisoners problem) The names of 100 prisoners are kept in 100 closed numbered envelopes. The prisoners are asked one after another to open 50 envelopes of their choice with the goal of finding their own name. If every prisoner succeeds in finding their own name, they all receive their freedom. They may decide on a strategy beforehand, but may not communicate during the experiment. What is a good strategy? Without a strategy (i. e. everyone opens 50 random envelopes), the probability of success is only

$$2^{-100} = (2^{10})^{-10} = 1024^{-10} < 1000^{-10} = 10^{-30}.$$

The prisoners are numbered, so that the distribution of names into the envelopes describes a permutation $\sigma \in S_{100}$. When it is the turn of the prisoner with number a, they first open envelope a and find therein the name of prisoner $\sigma(a)$. After that, they open envelope $\sigma(a)$ and find therein the name of $\sigma^2(a)$ etc. In this way, they find their own name if and only if the cycle of σ containing a has length ≤ 50. The procedure is therefore successful if and only if σ contains no cycle of length > 50. Obviously, σ can contain at most one such cycle. The number of permutations with a cycle of length $k > 50$ is therefore

$$\sum_{\sigma \in S_{100}} \sum_{k=51}^{100} z_k(\sigma) = \sum_{k=51}^{100} \sum_{\sigma \in S_{100}} z_k(\sigma).$$

The probability that the strategy fails is consequently

$$\frac{1}{100!} \sum_{k=51}^{100} \sum_{\sigma \in S_{100}} z_k(\sigma) \overset{2.10}{=} \sum_{k=51}^{100} \frac{1}{k} \leq \int_{50}^{100} \frac{1}{x} \, \mathrm{d}x = \log(2 \cdot 50) - \log(50) = \log(2) < 0{,}7$$

(cf. Example 2.4). The probability of success is therefore greater than 30% (independent of the number of prisoners).[4]

Definition 2.13. The number of permutations of S_n with exactly k cycles is called *Stirling number of the first kind* and is written as $\left[{n \atop k}\right]$. If one considers the identity on the empty set as a product of 0 cycles, one obtains $\left[{0 \atop 0}\right] = 1$.

Remark 2.14. For $n \in \mathbb{N}_0$ it holds that

$$n! = |S_n| = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}.$$

This is generalized in Theorem 2.17.

Example 2.15.

(i) By definition, $\left[{n \atop k}\right] = 0$ if $k = 0 < n$ or $k > n$. Since id is the only permutation in S_n with n cycles, $\left[{n \atop n}\right] = 1$ holds. In contrast to the binomial coefficient, in general $\left[{n \atop k}\right] \neq \left[{n \atop n-k}\right]$.

(ii) A permutation with only one cycle is an n-cycle. From Theorem 2.10 it follows that $\left[{n \atop 1}\right] = (n-1)!$.

---

[4] Youtube video by Veritasium: `https://www.youtube.com/watch?v=iSNsgj1OCLA`

(iii) Apparently, $\begin{bmatrix} n \\ n-1 \end{bmatrix}$ is the number of transpositions and thus also the number of 2-element subsets of $\{1, \ldots, n\}$. This shows $\begin{bmatrix} n \\ n-1 \end{bmatrix} = \binom{n}{2}$.

(iv) According to Remark 2.14, $\begin{bmatrix} 4 \\ 2 \end{bmatrix} = 4! - \begin{bmatrix} 4 \\ 1 \end{bmatrix} - \begin{bmatrix} 4 \\ 3 \end{bmatrix} - \begin{bmatrix} 4 \\ 4 \end{bmatrix} = 24 - 6 - 6 - 1 = 11$. The corresponding permutations are $(1,2,3)$, $(1,3,2)$, $(1,2,4)$, $(1,4,2)$, $(1,3,4)$, $(1,4,3)$, $(2,3,4)$, $(2,4,3)$, $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$.

Lemma 2.16. *For $k, n \in \mathbb{N}$ we have*

$$\boxed{\begin{bmatrix} n \\ k-1 \end{bmatrix} + n \begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n+1 \\ k \end{bmatrix}.}$$

Proof. Let $\sigma \in S_n$ with exactly $k-1$ cycles. By appending the 1-cycle $(n+1)$, one obtains a permutation in S_{n+1} with exactly k cycles. Now let $\sigma \in S_n$ with exactly k cycles. Then the digit $n+1$ can be inserted at n positions in the cycle representation of σ (example: inserting 4 into $(1,2)(3)$ yields $(4,1,2)(3)$, $(1,4,2)(3)$, $(1,2)(4,3)$). In this way, one obtains n different permutations in S_{n+1} with exactly k cycles. Apparently, every permutation of S_{n+1} with exactly k cycles arises in exactly one of the two ways. This shows the claim. $\square$

Theorem 2.17. *For $n \in \mathbb{N}_0$ we have $X(X+1)\ldots(X+n-1) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} X^k \in \mathbb{C}[X]$.*

Proof. Induction on n: For $n = 0$, the left side is the empty product and the right side is $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$. Now let $n \geq 1$ and the claim be already proven for $n-1$. We can extend the summation to $-\infty \ldots \infty$ to simplify index shifts:

$$\begin{aligned} X(X+1)\ldots(X+n-1) &= (X+n-1) \sum_{k=-\infty}^{\infty} \begin{bmatrix} n-1 \\ k \end{bmatrix} X^k \\ &= \sum \begin{bmatrix} n-1 \\ k \end{bmatrix} X^{k+1} + \sum (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} X^k \\ &= \sum \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} X^k + \sum (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} X^k \overset{2.16}{=} \sum \begin{bmatrix} n \\ k \end{bmatrix} X^k. \end{aligned}$$ $\square$

Example 2.18. The coefficient of X^{n-1} in $X(X+1)\ldots(X+n-1)$ is

$$\begin{bmatrix} n \\ n-1 \end{bmatrix} = \sum_{k=1}^{n-1} k = \binom{n}{2}$$

in agreement with Example 2.15.

Definition 2.19.

- A *partition* of a (finite) set A is a set of pairwise disjoint, non-empty subsets $\{A_1, \ldots, A_k\} \subseteq 2^A$ with $A = A_1 \cup \ldots \cup A_k$. The set of all partitions of A is denoted by $P(A)$. One calls $b(n) := |P(\{1, \ldots, n\})|$ the *n-th Bell number*.
- A *partition* of $n \in \mathbb{N}_0$ is a multiset $\lambda := \{k_1, \ldots, k_s\} \subseteq \mathbb{N}$ with $n = k_1 + \ldots + k_s$. One calls $k_1, \ldots, k_s$ the *parts* of λ. Let the set of all partitions of n be $P(n)$ and $p(n) := |P(n)|$.

Example 2.20. The partitions of $\{1,2,3\}$ are

$$\{1,2,3\} = \{1\} \cup \{2,3\} = \{2\} \cup \{1,3\} = \{3\} \cup \{1,2\} = \{1\} \cup \{2\} \cup \{3\}.$$

The partitions of 3 are $3 = 1+2 = 1+1+1$. Thus $b(3) = 5$ and $p(3) = 3$.

Remark 2.21.

(i) Note: $b(0) = 1 = p(0)$, because the empty (multi)set is a partition of $\varnothing$ (resp. 0).

(ii) If $\{A_1, \ldots, A_k\}$ is a partition of a finite set A, then $\{|A_1|, \ldots, |A_k|\}$ is a partition of $|A|$. Conversely, from every partition of $n \in \mathbb{N}$ one can construct a partition of $\{1, \ldots, n\}$. Therefore $b(n) \geq p(n)$ and $b(n) > p(n)$ if $n \geq 3$.

(iii) We will often write partitions of numbers in the form $(k_1, \ldots, k_s)$ with $k_1 \geq \ldots \geq k_s$ or in the form $(1^{m_1}, \ldots, n^{m_n}) := (\underbrace{1, \ldots, 1}_{m_1}, \ldots, \underbrace{n, \ldots, n}_{m_n})$ with $m_1, \ldots, m_n \in \mathbb{N}_0$.

(iv) The equivalence classes of an equivalence relation on A form a partition of A. The equality relation $(=)$ yields, for example, the partition $\{\{a\} : a \in A\}$.

Theorem 2.22. *Let $(1^{a_1}, \ldots, n^{a_n})$ be a partition of n. Then every n-element set has exactly*

$$\boxed{\frac{n!}{(1!)^{a_1} \ldots (n!)^{a_n} a_1! \ldots a_n!}}$$

partitions of the form $\{A_1, \ldots, A_k\}$ with $\{|A_1|, \ldots, |A_k|\} = (1^{a_1}, \ldots, n^{a_n})$.

Proof. Wlog. let $A = \{1, \ldots, n\}$. One can transform every arrangement $b_1, \ldots, b_n$ of the numbers $1, \ldots, n$ into a partition of the desired type by distributing corresponding braces { and }. We can first brace the a_1 one-element subsets, then the a_2 two-element subsets, etc.:

$$\{b_1\}, \{b_2\}, \ldots, \{b_i, b_{i+1}\}, \ldots.$$

Of the $n!$ possible arrangements $b_1, \ldots, b_n$, however, several lead to the same partition. On the one hand, one can arbitrarily permute the elements of each l-element subset without changing the partition. On the other hand, one can permute the a_l l-element subsets among themselves without changing the partition. Therefore, each $\prod_{l=1}^{n} (l!)^{a_l} a_l!$ arrangements lead to the same partition. This shows the claim. $\square$

Example 2.23. The number of partitions of $\{1,2,3,4\}$ of type $(2,2) = (1^0, 2^2)$ is $\frac{4!}{(2!)^2 2!} = \frac{24}{8} = 3$. These are $\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$ and $\{\{1,4\},\{2,3\}\}$.

Definition 2.24. If $\sigma \in S_n$ is a disjoint product of $a_i \geq 0$ cycles of length i, then $(1^{a_1}, \ldots, n^{a_n})$ is called the *cycle type* of σ. According to Lemma 2.7, this is a well-defined partition of n. The number of fixed points of σ is a_1.

Theorem 2.25. *The number of permutations of S_n with cycle type $(1^{a_1}, \ldots, n^{a_n})$ is*

$$\boxed{\frac{n!}{1^{a_1} \ldots n^{a_n} a_1! \ldots a_n!}.}$$

Proof. If one regards cycles as subsets of $\{1,\ldots,n\}$, then every permutation corresponds to a partition of $\{1,\ldots,n\}$. According to Theorem 2.22, the permutations with cycle type $(1^{a_1},\ldots,n^{a_n})$ correspond exactly to

$$\frac{n!}{\prod_{k=1}^{n}(k!)^{a_k}a_k!}$$

partitions. It remains to count how many permutations yield the same partition. Since every k-cycle can be uniquely written in the form $(b_1,\ldots,b_k)$ with $b_1 := \min\{b_1,\ldots,b_k\}$, exactly $(k-1)!$ cycles yield the same set $\{b_1,\ldots,b_k\}$ (one can arbitrarily permute $b_2,\ldots,b_k$). The number of the desired permutations is therefore

$$\frac{n!}{\prod_{k=1}^{n}(k!)^{a_k}a_k!}\prod_{k=1}^{n}\bigl((k-1)!\bigr)^{a_k} = \frac{n!}{\prod_{k=1}^{n}k^{a_k}a_k!}. \qquad \square$$

Example 2.26. The k-cycles of S_n have cycle type $(1^{n-k},k^1)$. Their number is

$$\frac{n!}{1^{n-k}k^1(n-k)!1!} = \frac{n!}{k(n-k)!}$$

in accordance with Theorem 2.10.

Definition 2.27. The number of k-element partitions of an n-element set is called the *Stirling number of the second kind* and is written as $\left\{{n \atop k}\right\}$.

Remark 2.28.

(i) Since every permutation with k cycles defines a partition with k subsets, $\left\{{n \atop k}\right\} \le \left[{n \atop k}\right]$ for all $k,n\in\mathbb{N}$.

(ii) It holds that

$$b(n) = \bigl|P\bigl(\{1,\ldots,n\}\bigr)\bigr| = \sum_{k=0}^{n}\left\{{n \atop k}\right\}.$$

Example 2.29.

(i) As usual, $\left\{{0 \atop 0}\right\} = 1$ and $\left\{{n \atop k}\right\} = 0$ for $k = 0 < n$ or $k > n$. Furthermore, $\left\{{n \atop 1}\right\} = 1 = \left\{{n \atop n}\right\}$ and $\left\{{n \atop n-1}\right\} = \left[{n \atop n-1}\right] = \binom{n}{2}$.

(ii) Every 2-element partition of A has the form $\{B, A\setminus B\}$ with $B \in 2^A \setminus \{\varnothing, A\}$. This shows $\left\{{n \atop 2}\right\} = \frac{1}{2}\bigl(|2^{\{1,\ldots,n\}}| - 2\bigr) \overset{1.3}{=} 2^{n-1} - 1$.

(iii) According to Remark 2.28, $b(4) = \left\{{4 \atop 1}\right\} + \left\{{4 \atop 2}\right\} + \left\{{4 \atop 3}\right\} + \left\{{4 \atop 4}\right\} = 1 + 2^3 - 1 + \binom{4}{2} + 1 = 15$.

Lemma 2.30. *For $k,n\in\mathbb{N}$ it holds that*

$$\boxed{\left\{{n \atop k-1}\right\} + k\left\{{n \atop k}\right\} = \left\{{n+1 \atop k}\right\}.}$$

Proof. Let $A = \{1,\ldots,n\}$ and $\{A_1,\ldots,A_{k-1}\}$ be a partition of A. Then $\{A_1,\ldots,A_{k-1},\{n+1\}\}$ is a k-element partition of $\{1,\ldots,n+1\}$. Now let $\{A_1,\ldots,A_k\}$ be a partition of A. Then one can add the number $n+1$ to each of the sets $A_1,\ldots,A_k$ and in this way obtains a k-element partition of $\{1,\ldots,n+1\}$. Obviously, every k-element partition of $\{1,\ldots,n+1\}$ arises in exactly one of the two ways. This shows the claim. $\square$

Theorem 2.31. *For $n \in \mathbb{N}_0$ it holds that $X^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} X(X-1)\dots(X-k+1)$.*

Proof. Induction on n: For $n=0$, $X^0 = 1 = \left\{ {0 \atop 0} \right\}$ holds. Now let $n \geq 1$ and the claim be already proven for $n-1$. Then

$$\begin{aligned}
X^n = XX^{n-1} &= (X-k+k)\sum_{k=-\infty}^{\infty} \left\{ {n-1 \atop k} \right\} X(X-1)\dots(X-k+1) \\
&= \sum \left\{ {n-1 \atop k} \right\} X(X-1)\dots(X-k) + \sum k \left\{ {n-1 \atop k} \right\} X(X-1)\dots(X-k+1) \\
&= \sum \left\{ {n-1 \atop k-1} \right\} X(X-1)\dots(X-k+1) + \sum k \left\{ {n-1 \atop k} \right\} X(X-1)\dots(X-k+1) \\
&\overset{2.30}{=} \sum \left\{ {n \atop k} \right\} X(X-1)\dots(X-k+1).
\end{aligned}$$

□

Example 2.32. If one sets $X=2$ in Theorem 2.31, then it follows that $2^n = \left\{ {n \atop 0} \right\} + \left\{ {n \atop 1} \right\}2 + \left\{ {n \atop 2} \right\}2 = 2(1 + \left\{ {n \atop 2} \right\})$ and $\left\{ {n \atop 2} \right\} = 2^{n-1} - 1$ for $n \geq 1$ in agreement with Example 2.29.

Corollary 2.33. *For $0 \leq m < n$ it holds that*

$$\boxed{\sum_{k=0}^{n} (-1)^k \left\{ {n \atop k} \right\} \left[{k \atop m} \right] = 0.}$$

Proof. Replacing X by $-X$ in Theorem 2.17 yields $(-1)^n X(X-1)\dots(X-n+1) = \sum_{k=0}^{n} (-1)^k \left[{n \atop k} \right] X^k$. With Theorem 2.31 it follows that

$$\begin{aligned}
X^n &= \sum_{k=0}^{n} \left\{ {n \atop k} \right\} X(X-1)\dots(X-k+1) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \sum_{m=0}^{k} (-1)^{k+m} \left[{k \atop m} \right] X^m \\
&= \sum_{m=0}^{n} (-1)^m \sum_{k=m}^{n} (-1)^k \left\{ {n \atop k} \right\} \left[{k \atop m} \right] X^m.
\end{aligned}$$

The claim follows by comparing coefficients. □

Remark 2.34. One should compare the following result with Theorem 1.8.

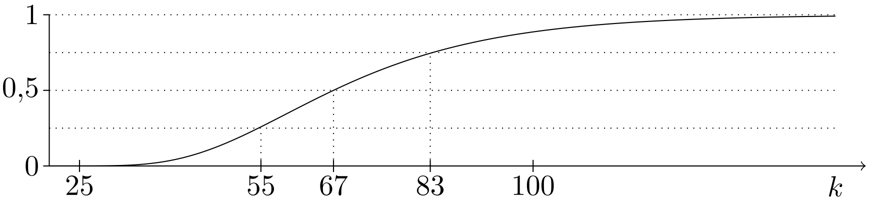
Theorem 2.35. *For finite sets A and B, there exist exactly $\left\{ {|A| \atop |B|} \right\}|B|!$ surjective mappings $A \to B$.*

Proof. Wlog. let $B = \{1, \dots, k\}$. Every surjective mapping $f\colon A \to B$ yields a k-element partition $\{f^{-1}(1), \dots, f^{-1}(k)\}$ of A. Let $g\colon A \to B$ with $\{f^{-1}(1), \dots, f^{-1}(k)\} = \{g^{-1}(1), \dots, g^{-1}(k)\}$. Then there exists a permutation $\sigma \in S_k$ with $f^{-1}(i) = g^{-1}(\sigma(i))$ for $i = 1, \dots, k$. Here, g is uniquely determined by f and σ. Conversely, if $\sigma \in S_k$ is given, then $g := \sigma \circ f$ yields the same partition as f. There are therefore exactly $|S_k| = k!$ mappings that yield the same k-element partition of A. The number of surjective mappings is therefore $\left\{ {|A| \atop k} \right\}k!$. □

Example 2.36 (Coupon collector's problem)**.** With every purchase at the supermarket, you receive one of n different trading cards (randomly and uniformly distributed). What is the probability that you own all trading cards after k purchases? The k purchases provide a mapping $\{1,\ldots,k\}\to\{1,\ldots,n\}$. There are n^k such mappings, of which $\left\{ {k \atop n} \right\} n!$ are surjective. The probability is therefore

$$\frac{n!}{n^k}\left\{ {k \atop n} \right\}.$$

For $n = 20$ one obtains:



Theorem 2.37. *For $n \in \mathbb{N}_0$,*

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

Proof. Let $\mathcal{A}$ be a partition of $\{1,\ldots,n+1\}$ and $n+1\in A\in\mathcal{A}$ with $k := |A|-1\ge 0$. Then there are $\binom{n}{k}$ possibilities for A and $\mathcal{A}\setminus\{A\}$ is a partition of $\{1,\ldots,n\}\setminus A$. For $\mathcal{A}\setminus\{A\}$ there are thus $b(n-k)$ possibilities. It follows that

$$b(n+1)=\sum_{k=0}^{n}\binom{n}{k}b(n-k)=\sum_{k=0}^{n}\binom{n}{k}b(k). \qquad \square$$

Example 2.38.

$$b(5)=b(0)+4b(1)+6b(2)+4b(3)+b(4)\overset{2.29}{=}1+4+12+20+15=52.$$

Lemma 2.39. *For $k, n \in \mathbb{N}_0$, it holds that*

$$\left\{ {n \atop k} \right\}=\frac{1}{k!}\sum_{l=0}^{k}(-1)^{k-l}\binom{k}{l}l^n.$$

Proof. Let $A := \{1,\ldots,n\}$, $B := \{1,\ldots,k\}$ and M be the set of surjective mappings from A to B. According to Theorem 2.35, it suffices to show $|M| = \sum_{l=0}^{k}(-1)^{k-l}\binom{k}{l}l^n$. For $i = 1,\ldots,k$ let

$$M_i := \bigl\{f\colon A\to B : i\notin f(A)\bigr\}.$$

For $1\le i_1<\ldots<i_l\le k$, $M_{i_1}\cap\ldots\cap M_{i_l}$ is then the set of all mappings from A to $B\setminus\{i_1,\ldots,i_l\}$. In particular, $|M_{i_1}\cap\ldots\cap M_{i_l}| = (k-l)^n$ according to Remark 1.6. The inclusion-exclusion principle shows

$$|M| = |B^A\setminus(M_1\cup\ldots\cup M_k)| = k^n+\sum_{l=1}^{k}(-1)^l\binom{k}{l}(k-l)^n=\sum_{l=0}^{k}(-1)^l\binom{k}{l}(k-l)^n.$$

The claim follows from $\binom{k}{l}=\binom{k}{k-l}$. $\square$

Remark 2.40. From Lemma 2.39 it follows that

$$n! = n!\left\{ {n \atop n} \right\} = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^n.$$

Asymptotically, the *Stirling formula* holds

$$n! \sim \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n,$$

i. e.

$$\lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n}(n/e)^n} = 1$$

(without proof). Example: $100! \approx 9.333 \cdot 10^{157}$ and $\sqrt{200\pi}(100/e)^{100} \approx 9.325 \cdot 10^{157}$.

Theorem 2.41 (Dobiński formula). *For $n \in \mathbb{N}_0$,*

$$\boxed{b(n) = \frac{1}{e}\sum_{k=0}^{\infty} \frac{k^n}{k!}.}$$

Proof. Because $\left\{ {n \atop k} \right\} = 0$ for $k > n$, it holds that

$$\begin{aligned} b(n) &\overset{2.28}{=} \sum_{k=0}^{\infty} \left\{ {n \atop k} \right\} \overset{2.39}{=} \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{l=0}^{k} (-1)^{k-l} \binom{k}{l} l^n = \sum_{k=0}^{\infty}\sum_{l=0}^{k} (-1)^{k-l} \frac{l^n}{l!(k-l)!} \\ &= \sum_{k=0}^{\infty}\sum_{l=0}^{k} \frac{(-1)^l}{l!} \frac{(k-l)^n}{(k-l)!} \overset{(*)}{=} \Big(\sum_{l=0}^{\infty} \frac{(-1)^l}{l!}\Big)\Big(\sum_{k=0}^{\infty} \frac{k^n}{k!}\Big) = \frac{1}{e}\sum_{k=0}^{\infty} \frac{k^n}{k!}, \end{aligned}$$

where in $(*)$ the Cauchy product formula for absolutely convergent series is used (Analysis). □

Remark 2.42. No simple formula for $p(n)$ is known. However, Hardy and Ramanujan proved

$$p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$$

(cf. Corollary 5.17). Example: $p(10^4) \approx 3{,}617 \cdot 10^{106}$ and $\frac{e^{\pi\sqrt{20000/3}}}{40000\sqrt{3}} \approx 3{,}633 \cdot 10^{106}$.

3 Recursions and Differences

Example 3.1. From algebra you know the *Euclidean* algorithm for calculating the greatest common divisor of $a, b \in \mathbb{N}$:

$$x_0 := \max\{a, b\}, \qquad x_1 := \min\{a, b\}, \qquad x_{n+1} := x_{n-1} \pmod{x_n} \qquad (n \geq 1).$$

After finitely many iterations, $x_n = 0$ and $x_{n-1} = \gcd(a, b)$. For $k \geq 1$, $x_{k+1} \leq x_{k-1} - x_n \leq x_{k-1}$ holds. The algorithm therefore takes particularly long if $x_{n-1} = 1$ and $x_{k+1} = x_{k-1} - x_k$ holds for all $k \geq 1$. In reverse order, these are the terms of the *Fibonacci sequence*:

$$F_0 := 0, \quad F_1 := 1, \quad F_{n+1} := F_{n-1} + F_n$$

for $n \in \mathbb{N}$. Conclusion: For $a, b \leq F_n$, the Euclidean algorithm for calculating $\gcd(a, b)$ takes at most n iterations (Lamé's Theorem). It is therefore of interest to calculate F_n. The first values are

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

We see that F_n grows rapidly. We want to determine an explicit formula for F_n (i. e. without having to calculate F_k for $k < n$ beforehand).

Definition 3.2 (Linear recurrence equation of k-th order)**.** Let $k \in \mathbb{N}$, $c_0, \ldots, c_k, a_1, \ldots, a_k \in \mathbb{C}$ with $a_k \neq 0$ be given. We seek an explicit formula for the numbers $x_0, x_1, \ldots \in \mathbb{C}$ that satisfy the following system of equations:

$$x_n = \begin{cases} c_n & \text{if } n < k, \\ a_1 x_{n-1} + a_2 x_{n-2} + \ldots + a_k x_{n-k} + c_k & \text{if } n \geq k. \end{cases}$$

In the case $c_k = 0$, the recurrence equation is called *homogeneous* and otherwise *inhomogeneous.*

Theorem 3.3. *The recurrence equation of first order $x_0 = c_0$, $x_n = a x_{n-1} + c_1$ has the following solution*

$$x_n = \begin{cases} c_0 a^n & \text{if } c_1 = 0, \\ c_0 a^n + \frac{a^n - 1}{a - 1} c_1 & \text{if } a \neq 1, \\ c_0 + n c_1 & \text{if } a = 1. \end{cases}$$

for $n \in \mathbb{N}_0$.

Proof. In the case $c_1 = 0$, $x_n = a x_{n-1} = a^2 x_{n-2} = \ldots = a^n x_0 = c_0 a^n$. In the case $a = 1$,

$$x_n = x_{n-1} + c_1 = x_{n-2} + c_1 + c_1 = \ldots = x_0 + n c_1 = c_0 + n c_1.$$

In the case $a \neq 1$, we argue by induction on n. The claim holds for $n = 0$. Now let the claim already be proven for $n - 1$. Then

$$x_n = a x_{n-1} + c_1 = c_0 a^n + a \frac{a^{n-1} - 1}{a - 1} c_1 + c_1 = c_0 a^n + \frac{a^n - a + a - 1}{a - 1} c_1 = c_0 a^n + \frac{a^n - 1}{a - 1} c_1. \qquad \square$$

Remark 3.4.

(i) We show that an inhomogeneous recurrence equation as in Definition 3.2 can always be converted into a homogeneous one. Analogous to Theorem 3.3, we distinguish two cases:

Case 1: $\alpha := 1 - a_1 - \ldots - a_k \neq 0$.
Here $y_n := x_n - \frac{c_k}{\alpha}$ satisfy the homogeneous system

$$y_n = \begin{cases} c_n - \frac{c_k}{\alpha} & \text{if } n < k \\ a_1 y_{n-1} + \ldots + a_k y_{n-k} & \text{if } n \geq k. \end{cases}$$

Case 2: $\alpha = 0$.
Here we pass to the following homogeneous recurrence equation of order $k+1$:

$$\begin{aligned}
x_i &= c_i \qquad (i = 0, \ldots, k-1),\\
x_k &= a_1 c_{k-1} + a_2 c_{k-2} + \ldots + a_k c_0 + c_k,\\
x_n &= a_1 x_{n-1} + a_2 x_{n-2} + \ldots + a_k x_{n-k} + c_k \qquad (n > k)\\
&= a_1 x_{n-1} + a_2 x_{n-2} + \ldots + a_k x_{n-k} + (x_{n-1} - a_1 x_{n-2} - \ldots - a_k x_{n-k-1})\\
&= (a_1 + 1) x_{n-1} + (a_2 - a_1) x_{n-2} + \ldots + (a_k - a_{k-1}) x_{n-k} - a_k x_{n-k-1}
\end{aligned}$$

($\alpha = 0$ is not needed). We therefore focus on homogeneous recurrence equations in the following.

(ii) (Superposition) If

$$\begin{aligned}
x_n &= a_1 x_{n-1} + a_2 x_{n-2} + \ldots + a_k x_{n-k},\\
y_n &= a_1 y_{n-1} + a_2 y_{n-2} + \ldots + a_k y_{n-k}
\end{aligned}$$

holds for all $n \geq k$, then every linear combination $z_n = \lambda x_n + \mu y_n$ with $\lambda, \mu \in \mathbb{C}$ also satisfies the recurrence condition.

Lemma 3.5. *Let $\alpha \in \mathbb{C}[X]$ be a polynomial with an m-fold root $x \in \mathbb{C}$. Then m is the smallest natural number with $\alpha^{(m)}(x) \neq 0$, where $\alpha^{(m)}$ denotes the m-th derivative.*

Proof. By assumption, $\alpha = (X - x)^m \beta$ with $\beta \in \mathbb{C}[X]$ and $\beta(x) \neq 0$. The Leibniz rule for derivatives shows

$$\alpha^{(k)} = \sum_{i=0}^{k} \binom{k}{i} \big((X - x)^m\big)^{(i)} \beta^{(k-i)}.$$

From $\big((X-x)^m\big)^{(i)} = m(m-1)\ldots(m-i+1)(X-x)^{m-i}$ it follows that $\alpha^{(k)}(x) = 0$ for $k = 1, \ldots, m-1$ and $\alpha^{(m)}(x) = m!\beta(x) \neq 0$. □

Theorem 3.6. *Let a linear homogeneous recurrence equation of k-th order be given as in Definition 3.2. Then there exist pairwise distinct numbers $\zeta_1, \ldots, \zeta_s \in \mathbb{C}$ and multiplicities $m_1, \ldots, m_s \in \mathbb{N}$ with*

$$\chi := X^k - a_1 X^{k-1} - \ldots - a_k = (X - \zeta_1)^{m_1} \ldots (X - \zeta_s)^{m_s}.$$

The system of equations

$$\begin{pmatrix}
\zeta_1^0 & 0 \cdot \zeta_1^0 & \cdots & 0^{m_1-1}\zeta_1^0 & \cdots & \zeta_s^0 & 0 \cdot \zeta_s^0 & \cdots & 0^{m_s-1}\zeta_s^0\\
\zeta_1^1 & 1 \cdot \zeta_1^1 & \cdots & 1^{m_1-1}\zeta_1^1 & \cdots & \zeta_s^1 & 1 \cdot \zeta_s^1 & \cdots & 1^{m_s-1}\zeta_s^1\\
\vdots & & & & & \vdots & & & \\
\zeta_1^{k-1} & (k-1)\zeta_1^{k-1} & \cdots & (k-1)^{m_1-1}\zeta_1^{k-1} & \cdots & \zeta_s^{k-1} & (k-1)\zeta_s^{k-1} & \cdots & (k-1)^{m_s-1}\zeta_s^{k-1}
\end{pmatrix} y = \begin{pmatrix} c_0 \\ \vdots \\ c_{k-1} \end{pmatrix}$$

possesses exactly one solution $(y_{1,1}, \ldots, y_{1,m_1}, y_{2,1}, y_{2,2}, \ldots, y_{s,m_s}) \in \mathbb{C}^k$. The solution of the recurrence equation is

$$x_n = \sum_{i=1}^{s} \zeta_i^n \sum_{j=1}^{m_i} y_{i,j} n^{j-1}. \tag{3.1}$$

Proof. The existence of the ζ_i follows from the Fundamental Theorem of Algebra. The assumption $a_k \neq 0$ implies $\zeta_i \neq 0$ for $i = 1, \dots, s$. The sequences $x_n = \zeta_i^n$ satisfy the recurrence equation without initial conditions, because

$$\zeta_i^n - a_1\zeta_i^{n-1} - \ldots - a_{n-k}\zeta_i^{n-k} = \zeta_i^{n-k}\chi(\zeta_i) = 0$$

for $n \geq k$. In the case $m_i > 1$, ζ_i is a root of the j-th derivative $\chi^{(j)}$ for $j = 1, \dots, m_i - 1$ according to Lemma 3.5. Since the derivative is linear, $x_n = (\zeta_i^n)^{(j)} = n(n-1)\dots(n-j)\zeta_i^{n-j}$ also satisfy the recurrence equation. Now $x_n = n^j\zeta_i^n$ can be written as a linear combination of the $(\zeta_i^n)^{(j)}$ (where ζ_i is used as a scalar). As a linear combination of these sequences, (3.1) is a solution of the recurrence equation by superposition. By setting $n = 0, \dots, k-1$, one sees that the initial conditions $x_n = c_n$ are now also satisfied (note: $0^0 = 1$).

To show the unique existence of the $y_{i,j}$, we must prove that the coefficient matrix $A \in \mathbb{C}^{k\times k}$ of the system of equations is invertible. Because $\zeta_i \neq 0$, $(\zeta_i^n)^{(j)}$ can be written as a linear combination of the columns of A. By elementary column operations, A can therefore be transformed into an equivalent matrix $\widetilde{A}$ with columns $(\zeta_i^n)^{(j)}$ for $i = 1, \dots, s$ and $j = 0, \dots, m_i - 1$. Now let $z = (z_0, \dots, z_{k-1}) \in \mathbb{C}^k$ with $z\widetilde{A} = 0$. Then $\zeta_1, \dots, \zeta_s$ are roots of the polynomial $\gamma := z_0 + z_1X + \ldots + z_{k-1}X^{k-1}$. In the case $m_i > 1$, ζ_i is a root of the derivatives $\gamma^{(l)}$ for $l = 1, \dots, m_i - 1$. According to Lemma 3.5, ζ_i is an m_i-fold root of γ. Counting multiplicities, γ thus possesses at least k roots. On the other hand, $\deg\gamma \leq k-1$. This shows $\gamma = 0$ and $z = 0$. Thus $\widetilde{A}$ and A are invertible. ☐

Example 3.7.

(i) The Fibonacci numbers are solutions of a homogeneous recursion equation of second order with $\chi = X^2 - X - 1$. Using the p-q-formula, one determines the roots

$$\varphi := \frac{1+\sqrt{5}}{2} \qquad (\textit{golden ratio}), \qquad \psi := \frac{1-\sqrt{5}}{2}.$$

The system of equations for y is $\left(\begin{smallmatrix}1 & 1\\ \varphi & \psi\end{smallmatrix}\right)y = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$. The unique solution is $y = \frac{1}{\sqrt{5}}(1, -1)$. The Binet formula follows:

$$\boxed{F_n = \frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \frac{1}{\sqrt{5}}\Big(\frac{1-\sqrt{5}}{2}\Big)^n.}$$

Since the second summand is smaller than $\frac{1}{2}$, one obtains the simpler formula by rounding

$$F_n = \left[\frac{1}{\sqrt{5}}\Big(\frac{1+\sqrt{5}}{2}\Big)^n\right].$$

For example: $F_{100} = 354.224.848.179.261.915.075$. For the Euclidean algorithm, the estimate $\log F_n \approx \log(\varphi)n$ means that the runtime grows only logarithmically in the input. It is therefore a particularly fast algorithm.

Remark 3.8.

(i) It is known from algebra that equations of degree ≥ 5 can generally no longer be solved exactly. The roots ζ_i can then be calculated approximately, for example, using Newton's method. However, the solution of the recurrence equation is extremely sensitive to rounding errors.

(ii) Recurrence equations can also be solved using linear algebra: The equation $x_n = a_1x_{n-1}+a_2x_{n-2}+\ldots+a_kx_{n-k}$ can be expressed by matrix multiplication

$$\underbrace{\begin{pmatrix} a_1 & a_2 & \cdots & a_k \\ 1 & 0 & \cdots & 0 \\ & \ddots & \ddots & \vdots \\ 0 & & 1 & 0 \end{pmatrix}}_{=:A} \begin{pmatrix} x_{n-1} \\ x_{n-2} \\ \vdots \\ x_{n-k} \end{pmatrix} = \begin{pmatrix} x_n \\ x_{n-1} \\ \vdots \\ x_{n-k+1} \end{pmatrix}.$$

This shows

$$\begin{pmatrix} x_n \\ \vdots \\ x_{n-k+1} \end{pmatrix} = A^{n-k+1} \begin{pmatrix} x_{k-1} \\ \vdots \\ x_0 \end{pmatrix} = A^{n-k+1} \begin{pmatrix} c_{k-1} \\ \vdots \\ c_0 \end{pmatrix}.$$

Using induction on k and Laplace expansion, one shows that $\chi_A = X^k - a_1X^{k-1} - \ldots - a_k$ is the characteristic polynomial of A. As in Theorem 3.6, $X^k - a_1X^{k-1} - \ldots - a_k = (X - \zeta_1)^{m_1} \ldots (X - \zeta_s)^{m_s}$ holds, where $\zeta_1, \ldots, \zeta_s$ are the distinct eigenvalues of A. According to linear algebra, there exists an $S \in \mathrm{GL}(k, \mathbb{C})$ such that $SAS^{-1} = J$ is the Jordan normal form. Because of $A^n = S^{-1}J^nS$, one must calculate the powers of J. For a single Jordan block for the eigenvalue λ, the following holds

$$\begin{pmatrix} \lambda & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda \end{pmatrix}^n = \begin{pmatrix} \lambda^n & & & & \\ n\lambda^{n-1} & \ddots & & & \\ \binom{n}{2}\lambda^{n-2} & \ddots & \ddots & & \\ \vdots & \ddots & \ddots & \ddots & \\ \binom{n}{k-1}\lambda^{n-k+1} & \cdots & \binom{n}{2}\lambda^{n-2} & n\lambda^{n-1} & \lambda^n \end{pmatrix}$$

(note the similarity of the entries to the derivatives $(\lambda^i)^{(j)}$). This allows the recurrence equation to be solved. One can show that χ_A is also the minimal polynomial of A. Therefore, A is diagonalizable if and only if the eigenvalues are pairwise distinct, i.e., $s = k$. In this case, J is a diagonal matrix and the formula simplifies.

(iii) When solving differential equations in analysis, recurrence equations occur in which the c_i may also depend on n.

Example 3.9. The well-known formulas

$$\sum_{n=1}^{a} n = \binom{a+1}{2}, \qquad \sum_{n=1}^{a}(2n-1) = a^2, \qquad \sum_{n=1}^{a} 2^n = 2^{a+1} - 1$$

can be easily proven by induction. However, one must first guess them. Difference calculus is a tool for deriving such summation formulas.

Remark 3.10. In analysis, one calculates areas under integrable functions $f\colon \mathbb{R} \to \mathbb{R}$ with the help of the integral $\int_a^b f(x)\mathrm{d}x$ with respect to the Lebesgue measure. In discrete mathematics, we consider functions $f\colon \mathbb{Z} \to \mathbb{R}$ and equip $\mathbb{Z}$ with the *counting measure* $m(A) = |A|$ for $A \subseteq \mathbb{Z}$. The integral then corresponds to the sum $\sum_{n=a}^{b-1} f(n)$ (cf. Example 2.4). Analogous to the fundamental theorem of calculus, such sums can be determined using (discrete) antiderivatives. These in turn are obtained as the inverse of the (discrete) derivative.

Definition 3.11. For $f\colon \mathbb{Z} \to \mathbb{R}$, we define the (*discrete*) *derivative*

$$\Delta(f)\colon \mathbb{Z} \to \mathbb{R}, \qquad\qquad n \mapsto f(n+1) - f(n)$$

(this is obtained from the analytical definition $f'(x) = \lim_{h\to 0} \frac{f(x+h)-f(x)}{h}$ for $h = 1$). A (*discrete*) *antiderivative* of f is a function $F\colon \mathbb{Z} \to \mathbb{R}$ with $\Delta(F) = f$.

Remark 3.12. In contrast to analysis, every function $f\colon \mathbb{Z} \to \mathbb{R}$ has (exactly) one discrete derivative. Through the recursive rule

$$F(n) := \begin{cases} 0 & \text{if } n = 0, \\ F(n-1) + f(n-1) & \text{if } n > 0, \\ F(n+1) - f(n) & \text{if } n < 0 \end{cases}$$

one always obtains a discrete antiderivative of f (however, there is often no closed-form formula for $F(n)$). If F and G are discrete antiderivatives of f, then

$$\begin{aligned} F(n+1) - G(n+1) &= \Delta(F)(n) - \Delta(G)(n) + F(n) - G(n) \\ &= f(n) - f(n) + F(n) - G(n) = F(n) - G(n) \end{aligned}$$

holds for all $n \in \mathbb{Z}$, i. e. F and G differ (as in analysis) only by a constant. Such an (indefinite) antiderivative is expressed with the modified integral symbol $\lceil\!\rfloor f$.

Example 3.13. For the constant function $f = C$, $\Delta(f) = 0$ holds. For $f = \mathrm{id}_{\mathbb{Z}}$, $\Delta(f) = 1$ holds. Because of $\frac{1}{2}\big((n+1)n - n(n-1)\big) = n = f(n)$, we have $\lceil\!\rfloor f = \lceil\!\rfloor n = \frac{1}{2}n(n-1)$ (in analysis it would be $\frac{1}{2}x^2$).

Theorem 3.14 (Fundamental Theorem of Difference Calculus)**.** *Let $f\colon \mathbb{Z} \to \mathbb{R}$ with discrete antiderivative F. For $a, b \in \mathbb{Z}$ with $a \le b$, it then holds that*

$$\boxed{\sum_{n=a}^{b} f(n) = F(b+1) - F(a).}$$

Proof.

$$\sum_{n=a}^{b} f(n) = \sum_{n=a}^{b} \Delta(F)(n) = \sum_{n=a}^{b} (F(n+1) - F(n)) = F(b+1) - F(a). \qquad \square$$

Remark 3.15. As in analysis, we write $\lceil\!\rfloor_a^b f := F(b) - F(a)$. According to Remark 3.12, this does not depend on the choice of the discrete antiderivative.

Example 3.16.

$$\sum_{n=0}^{a} n = \lceil\!\rfloor_{0}^{a+1} n \overset{3.13}{=} \frac{1}{2}(a+1)a = \binom{a+1}{2}.$$

Definition 3.17. The functions $\mathbb{Z} \to \mathbb{R}$ form a ring as well as an $\mathbb{R}$-vector space with the following operations:

$$(f+g)(n) := f(n) + g(n), \quad (fg)(n) := f(n)g(n), \quad (\lambda f)(n) := \lambda f(n) \quad (f, g\colon \mathbb{Z} \to \mathbb{R}, n \in \mathbb{Z}, \lambda \in \mathbb{R})$$

(the composition $f \circ g$, however, is not well-defined). Additionally, we define $\mathrm{E}(f)\colon \mathbb{Z} \to \mathbb{R}$, $n \mapsto f(n+1)$.

Lemma 3.18. *For $f, g\colon \mathbb{Z} \to \mathbb{R}$ and $\lambda \in \mathbb{R}$, we have $\Delta(\lambda f) = \lambda\Delta(f)$, $\Delta(f+g) = \Delta(f) + \Delta(g)$ and*

$$\boxed{\Delta(fg) = \Delta(f)\mathrm{E}(g) + f\Delta(g)} \qquad (\textit{product rule}).$$

Proof. For $n \in \mathbb{Z}$, we have

$$\begin{aligned} \Delta(\lambda f)(n) &= \lambda f(n+1) - \lambda f(n) = \lambda\Delta(f)(n), \\ \Delta(f+g)(n) &= (f+g)(n+1) - (f+g)(n) = f(n+1) - f(n) + g(n+1) - g(n) \\ &= \Delta(f)(n) + \Delta(g)(n), \\ \Delta(fg)(n) &= f(n+1)g(n+1) - f(n)g(n) = (f(n+1) - f(n))g(n+1) + f(n)(g(n+1) - g(n)) \\ &= \Delta(f)(n)\mathrm{E}(g)(n) - f(n)\Delta(g)(n). \end{aligned}$$ ☐

Remark 3.19. It is easy to see that our previous definitions and results also hold for functions $f\colon \mathbb{N} \to \mathbb{R}$.

Lemma 3.20.

(i) For $k \in \mathbb{N}_0$, let $p_k\colon \mathbb{Z} \to \mathbb{R}$, $n \mapsto n(n-1)\ldots(n-k+1)$. Then $\lceil\!\rfloor p_k = \frac{1}{k+1}p_{k+1}$ holds.

(ii) For $k \in \mathbb{N}_0$, let $q_k\colon \mathbb{N} \to \mathbb{R}$, $n \mapsto \frac{1}{n(n+1)\ldots(n+k-1)}$. Then $\Delta(q_k) = -kq_{k+1}$ holds.

(iii) For $c \in \mathbb{R} \setminus \{0, 1\}$, we have $\lceil\!\rfloor c^n = \frac{c^n}{c-1}$.

Proof. For $n \in \mathbb{Z}$, we have

$$\begin{aligned} \Delta(p_{k+1})(n) &= (n+1)p_k(n) - p_k(n)(n-k) = (k+1)n(n-1)\ldots(n-k+1) = (k+1)p_k(n), \\ \Delta(q_k)(n) &= nq_{k+1}(n) - q_{k+1}(n)(n+k) = -kq_{k+1}(n), \\ \Delta(c^n) &= c^{n+1} - c^n = (c-1)c^n. \end{aligned}$$ ☐

Example 3.21.

(a) Because $\lceil\!\rfloor 2^n = 2^n$, 2^n is the discrete analogue of the exponential function. Because $n^2 = n(n-1) + n = p_2(n) + p_1(n)$, we have

$$\lceil\!\rfloor n^2 = \frac{1}{3}p_3(n) + \frac{1}{2}p_2(n) = \frac{2n^3 - 3n^2 + n}{6}.$$

(b) Lemma 3.20 provides no formula for $\lceil\!\rfloor q_1$. For $a \in \mathbb{N}$,

$$\mathop{\lceil\!\rfloor}_{1}^{a+1} \frac{1}{n} \overset{3.14}{=} \sum_{n=1}^{a} \frac{1}{n} = H_a$$

is the a-th harmonic number (compare with analysis $\int \frac{1}{x} = \log(x)$, see Remark 2.11).

Theorem 3.22 (Summation by parts). *For $f, g\colon \mathbb{Z} \to \mathbb{R}$, we have* $\boxed{\int f\Delta(g) = fg - \int \Delta(f)\mathrm{E}(g).}$

Proof.

$$\Delta\Big(fg - \int \Delta(f)\mathrm{E}(g)\Big) \overset{3.18}{=} \Delta(fg) - \Delta(f)\mathrm{E}(g) = f\Delta(g). \qquad \square$$

Remark 3.23. For real sequences (a_n) and (b_n), Theorem 3.22 can also be written in the form

$$\sum_{n=1}^{k} a_n b_n = a_k \sum_{n=1}^{k} b_n + \sum_{n=1}^{k-1} (a_n - a_{n+1}) \sum_{l=1}^{n} b_l.$$

This is called *Abelian summation.*

Example 3.24. For $a \in \mathbb{N}$ and $c \in \mathbb{R} \setminus \{0, 1\}$, it holds that

$$\begin{aligned}\sum_{n=0}^{a-1} nc^n &\overset{3.20}{=} \frac{1}{c-1} \int\limits_0^a n\Delta(c^n) = \frac{1}{c-1}\Big(ac^a - \int\limits_0^a \Delta(n)\mathrm{E}(c^n)\Big) = \frac{1}{c-1}\Big(ac^a - c\int\limits_0^a c^n\Big) \\ &= \frac{1}{c-1}\Big(ac^a - \frac{c}{c-1}(c^a - 1)\Big) = \frac{c^a(ac - a - c) + c}{(c-1)^2}.\end{aligned}$$

Theorem 3.25 (Faulhaber's formula). *For $a, k \in \mathbb{N}$, it holds that*

$$\sum_{n=1}^{a-1} n^k = \sum_{n=1}^{k} \frac{1}{n+1} \left\{ k \atop n \right\} a(a-1)\dots(a-n).$$

This is a polynomial in a of degree $k+1$.

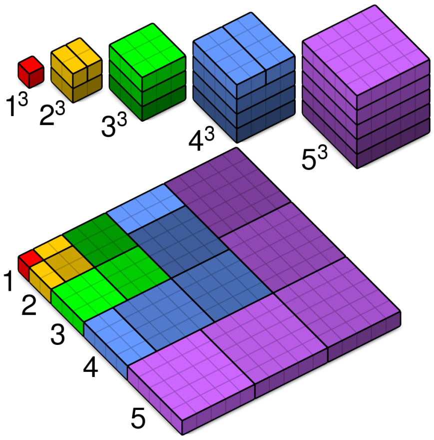
Proof. According to Theorem 2.31,

$$\sum_{n=0}^{a-1} n^k = \int\limits_0^a n^k = \sum_{l=0}^{k} \left\{ k \atop l \right\} \int\limits_0^a p_l = \sum_{l=0}^{k} \frac{1}{l+1} \left\{ k \atop l \right\} p_{l+1}(a) = \sum_{l=0}^{k} \frac{1}{l+1} \left\{ k \atop l \right\} a(a-1)\dots(a-l). \qquad \square$$

Example 3.26. For $k = 3$, one obtains the *Nicomachus identity*

$$\begin{aligned}\sum_{n=1}^{a-1} n^3 &= \sum_{n=1}^{3} \frac{1}{n+1} \left\{ 3 \atop n \right\} a(a-1)\dots(a-n) = \frac{1}{2}a(a-1) + a(a-1)(a-2) + \frac{1}{4}a(a-1)(a-2)(a-3) \\ &= \frac{a(a-1)}{2}\Big(1 + 2(a-2) + \frac{1}{2}(a-2)(a-3)\Big) = \Big(\frac{a(a-1)}{2}\Big)^2 = \binom{a}{2}^2 = \Big(\sum_{n=1}^{a-1} n\Big)^2.\end{aligned}$$

It can also be justified geometrically:[5]:



Remark 3.27. The (leading) coefficient of a^{k+1} in Faulhaber's formula is $\frac{1}{k+1}\left\{ {k \atop k} \right\} = \frac{1}{k+1}$. The coefficient of a^k is

$$\frac{1}{k}\left\{ {k \atop k-1} \right\} - \frac{1}{k+1}\sum_{i=1}^{k} i = \frac{k+1}{2} - \frac{k}{2} = \frac{1}{2}.$$

The coefficient of a is the k-th *Bernoulli number*

$$B_k := \sum_{n=1}^{k} \frac{(-1)^n}{n+1} n! \left\{ {k \atop n} \right\}.$$

The Bernoulli numbers also appear for negative (even) k:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}, \qquad \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{(2\pi)^{2k}(-1)^{k+1}B_{2k}}{2(2k)!}$$

(without proof). On the other hand, no formula is known for the *Apéry constant* $\sum_{n=1}^{\infty} \frac{1}{n^3} = 1{,}202\ldots$. These are values of the *Riemann ζ-function* $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ defined for real $s > 1$. Through

$$\zeta(z) = \frac{1}{1 - 2^{1-z}} \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{(k+1)^z} \qquad (z \in \mathbb{C} \setminus \{1\})$$

ζ can be continued to $\mathbb{C} \setminus \{1\}$. One can show that $\zeta(-2a) = 0$ holds for all $a \in \mathbb{N}$ (this is related to $B_{2a+1} = 0$, Exercise 21). The *Riemann hypothesis* states that all other zeros of ζ have real part $\frac{1}{2}$. This is one of the greatest mathematical questions of the present (one can again earn a million dollars). Surprisingly, the Riemann hypothesis is equivalent to the following discrete statement: For all $n \in \mathbb{N}$ it holds that

$$\sum_{d \mid n} d \le H_n + e^{H_n} \log(H_n) \qquad (\textit{Lagarias criterion})^6.$$

---

[5] Source: math.stackexchange, see also hyrodium.tumblr.com

[6] see [J. C. Lagarias, *An Elementary Problem Equivalent to the Riemann Hypothesis*, Amer. Math. Monthly 109 (2002), 534–543]

4 Formal Power Series

Remark 4.1. From analysis you know power series as functions of the form $f\colon \mathbb{C} \to \mathbb{C}$, $x \mapsto \sum_{n=0}^{\infty} a_n x^n$. In discrete mathematics, one is not interested in the value of such functions, but only in the occurring coefficients a_n. In this section, we lay the foundations for the applications in the next section.

Definition 4.2. Let $\mathbb{C}[[X]] := \mathbb{C}^{\mathbb{N}_0} = \{(a_0, a_1, \ldots) : a_i \in \mathbb{C}\}$. Two elements $\alpha := (a_0, \ldots)$ and $\beta := (b_0, \ldots)$ of $\mathbb{C}[[X]]$ can be added and multiplied as follows:

$$\begin{aligned} \alpha + \beta &:= (a_0 + b_0, a_1 + b_1, \ldots) \in \mathbb{C}[[X]], \\ \alpha \cdot \beta &:= (a_0 b_0, a_1 b_0 + a_0 b_1, \ldots, \sum_{i=0}^{n} a_i b_{n-i}, \ldots) \in \mathbb{C}[[X]]. \end{aligned}$$

We set $0 := (0, 0, \ldots) \in \mathbb{C}[[X]]$ and $1 := (1, 0, 0, \ldots) \in \mathbb{C}[[X]]$.

Lemma 4.3. *The set* $\mathbb{C}[[X]]$ *is an integral domain, i.e., for* $\alpha, \beta, \gamma \in \mathbb{C}[[X]]$ *it holds that*

$$\begin{array}{ccc} (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) & \alpha + \beta = \beta + \alpha & \alpha + 0 = \alpha \\ (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma) & \alpha \cdot \beta = \beta \cdot \alpha & \alpha \cdot 1 = \alpha \\ \alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma) & \exists \delta \in \mathbb{C}[[X]] : \alpha + \delta = 0, & \alpha\beta = 0 \Longrightarrow \alpha = 0 \vee \beta = 0. \end{array}$$

Proof. The proof works as for polynomials (Algebra 1). The first three statements follow directly from the corresponding axioms in $\mathbb{C}$. Now let $\alpha = (a_0, \ldots)$, $\beta = (b_0, \ldots)$ and $\gamma = (c_0, \ldots)$. For $\delta := (-a_0, -a_1, \ldots)$ it then holds that $a + \delta = 0$. The n-th entry of $\alpha \cdot (\beta \cdot \gamma)$ is

$$\sum_{i=0}^{n} a_i \sum_{j=0}^{n-i} b_j c_{n-i-j} = \sum_{i+j+k=n} a_i b_j c_k = \sum_{i=0}^{n} \Big(\sum_{j=0}^{i} a_j b_{i-j} \Big) c_{n-i}.$$

This shows $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$. Because of $\sum_{i=0}^{n} a_i b_{n-i} = \sum_{i=0}^{n} b_i a_{n-i}$, we have $\alpha \cdot \beta = \beta \cdot \alpha$. The equation $\alpha \cdot 1 = \alpha$ is easy to see. The n-th entry of $\alpha \cdot (\beta + \gamma)$ is

$$\sum_{i=0}^{n} a_i (b_{n-i} + c_{n-i}) = \sum_{i=0}^{n} a_i b_{n-i} + \sum_{i=0}^{n} a_i c_{n-i}$$

and $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$ follows. Finally, let $\alpha\beta = 0$. Assume indirectly $\alpha \neq 0 \neq \beta$. Let $k := \min\{n \in \mathbb{N}_0 : a_n \neq 0\}$ and $l := \min\{n \in \mathbb{N}_0 : b_n \neq 0\}$. The $(k + l)$-th entry of $\alpha\beta$ is then $\sum_{i=0}^{k+l} a_i b_{k+l-i} = a_k b_l \neq 0$. This contradiction shows $\alpha = 0$ or $\beta = 0$. □

Remark 4.4.

(i) One calls $\mathbb{C}[[X]]$ the *ring of (formal) power series*. Its elements are written in the form $\sum_{n=0}^{\infty} a_n X^n = a_0 + a_1 X + a_2 X^2 + \ldots$, where $X = (0, 1, 0, 0, \ldots)$ is an *indeterminate*. It holds that

$$\sum_{n=0}^{\infty} a_n X^n = \sum_{n=0}^{\infty} b_n X^n \Longleftrightarrow a_n = b_n \ \forall n \in \mathbb{N}_0.$$

In the multiplication of power series, one multiplies term by term and subsequently groups identical powers of X. One calls a_0 the *constant term* of α. If the range of summation is clear, we write more briefly $\sum a_n X^n$. Furthermore, we will omit the multiplication symbol $\cdot$ and use “order of operations”, i. e. $\alpha\beta + \gamma := (\alpha \cdot \beta) + \gamma$. Let the inverse of α with respect to $+$ be $-\alpha$. As usual, we write $\alpha - \beta$ instead of $\alpha + (-\beta)$.

(ii) The meaning of the word “formal” lies in the fact that, in contrast to analysis, we do not consider convergence, since X is always an indeterminate and not a number (hence also the use of the capital letter).

(iii) For $\alpha \in \mathbb{C}[[X]]$ we define $\alpha\mathbb{C}[[X]] := \{\alpha\beta : \beta \in \mathbb{C}[[X]]\}$ (a principal ideal in $\mathbb{C}[[X]]$). For example, $X\mathbb{C}[[X]]$ is the set of power series with constant term 0.

(iv) One can extend $\mathbb{C}[[X]]$ to a field $\mathbb{C}((X))$ by replacing power series with (formal) *Laurent series* of the form $\sum_{n=k}^{\infty} a_n X^n$ with $k \in \mathbb{Z}$ and $a_n \in \mathbb{C}$ (Exercise 19).

Example 4.5.

(i) Every (formal) polynomial is a power series.

(ii) It holds that

$$\begin{aligned}(1 + 2X + 3X^2 + 4X^3 + \ldots)(1 - X + X^2 - X^3 \pm \ldots) &= 1 + (2 - 1)X + (3 - 2 + 1)X^2 \\ &+(4 - 3 + 2 - 1)X^3 + \ldots = 1 + X + 2X^2 + 2X^3 + \ldots, \\ (1 - X)\sum_{n=0}^{\infty} X^n = \sum_{n=0}^{\infty} X^n - \sum_{n=1}^{\infty} X^n = 1.\end{aligned}$$

(iii) The (formal) *exponential function* is

$$\boxed{\exp(X) := \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \ldots \in \mathbb{C}[[X]].}$$

Definition 4.6. One calls $\alpha \in \mathbb{C}[[X]]$ *invertible* if there exists a $\beta \in \mathbb{C}[[X]]$ with $\alpha\beta = 1$.

Remark 4.7.

(i) If α, β, γ satisfy $\alpha\beta = 1 = \alpha\gamma$, then $\alpha(\beta - \gamma) = 0$ and it follows that $\beta = \gamma$, because otherwise $1 = \alpha\beta = 0\beta = 0$. Thus there exists at most one β with $\alpha\beta = 1$. One calls β the *inverse* of α and writes $\alpha^{-1} := \beta$ or $1/\alpha$. More generally, we set

$$\alpha^k := \begin{cases} \underbrace{\alpha \ldots \alpha}_{k \text{ times}} & \text{if } k > 0, \\ 1 & \text{if } k = 0, \\ (\alpha^{-1})^{-k} & \text{if } k < 0. \end{cases}$$

for $k \in \mathbb{Z}$.

(ii) For $\alpha, \beta, \gamma \in \mathbb{C}[[X]]$ with $\alpha\beta = \gamma$ we write $\frac{\gamma}{\beta} := \alpha$, if $\beta \neq 0$ (as in (i) this is well-defined).

Lemma 4.8. *Let* $\alpha = \sum a_n X^n \in \mathbb{C}[[X]]$.

(i) α *is invertible if and only if* $a_0 \neq 0$ *holds.*

(ii) If there exists an $m \in \mathbb{N}$ *with* $\alpha^m = 1$*, then* $\alpha \in \mathbb{C}$.

Proof.

(i) Let $\beta = \sum b_n X^n \in \mathbb{C}[[X]]$ with $\alpha\beta = 1$. Then $a_0 b_0 = 1$ and $a_0 \neq 0$. Conversely, let $a_0 \neq 0$. We define $b_0, b_1, \ldots \in \mathbb{C}$ inductively by $b_0 := 1/a_0$ and

$$b_k := -\frac{1}{a_0}\sum_{i=1}^{k} a_i b_{k-i} \in \mathbb{C}$$

for $k \in \mathbb{N}$. It then holds that

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} 1 & \text{if } k = 0, \\ 0 & \text{if } k > 0. \end{cases}$$

This shows $\alpha\beta = 1$ for $\beta := \sum b_n X^n$.

(ii) Suppose by way of contradiction $\alpha \notin \mathbb{C}$. Let $n \in \mathbb{N}$ be minimal with $a_n \neq 0$. Then $m a_0^{m-1} a_n$ is the n-th coefficient of α^m, thus $m a_0^{m-1} a_n = 0$. By (i) we have $a_0 \neq 0$ and the contradiction $a_n = 0$ follows. □

Remark 4.9. If $\alpha, \beta \in \mathbb{C}[[X]]$ are invertible, then so are α^{-1} and $\alpha\beta$ by Lemma 4.8. In this case $(\alpha^{-1})^{-1} = \alpha$ and $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$. The invertible power series form an abelian group with respect to multiplication with identity element 1. One calls it the *unit group* of $\mathbb{C}[[X]]$ and writes $\mathbb{C}[[X]]^\times$ for it. By Lemma 4.8 we have $\mathbb{C}[[X]]^\times = \mathbb{C}[[X]] \setminus X\mathbb{C}[[X]]$.

Example 4.10.

(i) According to Example 4.5, $\frac{1}{1-X} = \sum X^n$ is the (formal) *geometric series*. More generally,

$$\frac{1}{a - X} = \sum a^{-n-1} X^n$$

holds for $a \in \mathbb{C} \setminus \{0\}$ and

$$\sum_{k=0}^{n-1} \alpha^k = \frac{\alpha^n - 1}{\alpha - 1}$$

for $\alpha \in \mathbb{C}[[X]] \setminus \{1\}$ and $n \in \mathbb{N}$.

(ii) For distinct $a, b \in \mathbb{C} \setminus \{0\}$, $X + a$ and $X + b$ are invertible and the *partial fraction decomposition*

$$\frac{1}{(X+a)(X+b)} = \frac{1}{b-a}\Big(\frac{1}{X+a} - \frac{1}{X+b}\Big)$$

holds (bring the right side to a common denominator).

Remark 4.11. For $k \in \mathbb{N}_0$, let $\alpha_k \in X^{e_k}\mathbb{C}[[X]]$ with $\lim_{k\to\infty} e_k = \infty$. Then the infinite sum $\sum_{k=0}^{\infty} \alpha_k$ can be formed, because the coefficient of X^n depends only on finitely many α_k.[7] More precisely: Let $\alpha_k = \sum a_{k,n} X^n$. Then

$$\sum \alpha_k = \sum_{n=0}^{\infty}\Big(\sum_{\substack{k\in\mathbb{N}_0\\ e_k \le n}} a_{k,n}\Big) X^n.$$

Likewise, $\prod_{k=1}^{\infty}(1 + \alpha_k)$ is well-defined. In the following, all infinite sums and products will be of this type.

---

[7] Formally, one can define a norm on $\mathbb{C}[[X]]$ by $|\alpha| := 2^{-\inf\{n\in\mathbb{N}_0 : a_n \neq 0\}}$ and define the infinite sum as the limit of the partial sums as in analysis. The details can be found in my combinatorics notes.

Example 4.12.

(i) For $\alpha \in X\mathbb{C}[[X]]$, we have $\alpha^k \in X^k\mathbb{C}[[X]]$ and $\sum \alpha^n = \frac{1}{1-\alpha}$. Thus, in the geometric series, we have replaced X by α.

(ii) We will investigate the coefficients of

$$(1+X)(1+X^2)(1+X^3)(1+X^4)\ldots = 1+X+X^2+2X^3+2X^4+\ldots$$

in the next chapter.

Definition 4.13. For $\alpha = \sum a_nX^n \in \mathbb{C}[[X]]$ and $\beta \in X\mathbb{C}[[X]]$, one defines the *composition*

$$\alpha \circ \beta := \alpha(\beta) := \sum_{n=0}^{\infty} a_n\beta^n.$$

Remark 4.14. For arbitrary $\alpha, \beta \in \mathbb{C}[[X]]$, the constant term $\sum_{k=0}^{\infty} a_0 b_0^k$ of $\alpha(\beta)$ would in general not be well-defined. For example, one cannot substitute 1 for X in the geometric series.

Example 4.15. For $\alpha = \sum a_nX^n \in \mathbb{C}[[X]]$, we have $\alpha(X^2) = \sum a_nX^{2n}$ and $\alpha(0) = a_0$.

Lemma 4.16. *For $\alpha, \beta, \gamma, \alpha_1, \ldots \in \mathbb{C}[[X]]$ the following holds (if well-defined):*

$$X \circ \alpha = \alpha = \alpha \circ X, \tag{4.1}$$

$$\Bigl(\sum \alpha_k\Bigr) \circ \beta = \sum(\alpha_k \circ \beta), \tag{4.2}$$

$$(\alpha\beta) \circ \gamma = (\alpha \circ \gamma)(\beta \circ \gamma), \tag{4.3}$$

$$\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma. \tag{4.4}$$

Proof. Equation (4.1) is trivial. With the notation from Remark 4.11 we have

$$\Bigl(\sum \alpha_k\Bigr) \circ \beta = \sum_{n=0}^{\infty}\Bigl(\sum_k a_{k,n}\Bigr)\beta^n = \sum_k\Bigl(\sum_{n=0}^{\infty} a_{k,n}\beta^n\Bigr) = \sum(\alpha_k \circ \beta).$$

Equation (4.3) is obtained by

$$(\alpha\beta) \circ \gamma = \sum_{n=0}^{\infty}\sum_{k=0}^{n} a_kb_{n-k}\gamma^n = \sum_{n=0}^{\infty}\sum_{k=0}^{n}(a_k\gamma^k)(b_{n-k}\gamma^{n-k}) = (\alpha \circ \gamma)(\beta \circ \gamma).$$

In (4.4) we may assume $\alpha = X^n$ according to (4.2). With (4.3) it follows that

$$\alpha \circ (\beta \circ \gamma) = (\beta \circ \gamma)^n = \beta^n \circ \gamma = (\alpha \circ \beta) \circ \gamma. \qquad \square$$

Remark 4.17. In general $\alpha \circ \beta \neq \beta \circ \alpha$, $\alpha \circ (\beta\gamma) \neq (\alpha \circ \beta)(\alpha \circ \gamma)$ and $\alpha \circ (\beta + \gamma) \neq \alpha \circ \beta + \alpha \circ \gamma$ (Exercise 26). The last equation can be corrected for the exponential function.

Lemma 4.18 (Functional equation)**.** *For $\alpha_1, \alpha_2, \ldots \in X\mathbb{C}[[X]]$ the following holds (if well-defined)*

$$\boxed{\exp\Bigl(\sum \alpha_k\Bigr) = \prod \exp(\alpha_k).} \tag{4.5}$$

In particular, $\exp(kX) = \exp(X)^k$ *for* $k \in \mathbb{Z}$.

Proof. Because of $\sum \alpha_k \in X\mathbb{C}[[X]]$ and $\exp(\alpha_k) \in 1 + \alpha_k + \frac{\alpha_k^2}{2} + \ldots$, both sides of (4.5) are well-defined (Remark 4.11). For two summands $\alpha, \beta \in X\mathbb{C}[[X]]$, it holds that

$$\begin{aligned}\exp(\alpha+\beta) &= \sum \frac{(\alpha+\beta)^n}{n!} = \sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}\frac{\alpha^k\beta^{n-k}}{n!}\\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{n}\frac{\alpha^k\beta^{n-k}}{k!(n-k)!} = \sum \frac{\alpha^n}{n!}\cdot\sum\frac{\beta^n}{n!} = \exp(\alpha)\exp(\beta).\end{aligned}$$

Inductively, one obtains (4.5) for finitely many summands. Finally, (4.5) also holds for infinitely many summands, because each coefficient depends only on finitely many summands. For example:

$$\begin{aligned}\exp(X+X^2+X^3+\ldots) &= 1 + (X+X^2+\ldots) + \frac{(X+X^2+\ldots)^2}{2} + \ldots = 1 + X + \frac{3}{2}X^2 + \ldots\\ &= \Bigl(1+X+\frac{X^2}{2}+\ldots\Bigr)\Bigl(1+X^2+\frac{(X^2)^2}{2}+\ldots\Bigr)\ldots = \exp(X)\exp(X^2)\ldots.\end{aligned}$$

For $k \in \mathbb{N}_0$, $\exp(kX) = \exp(X+\ldots+X) = \exp(X)^k$. Because of $\exp(kX)\exp(-kX) = \exp(kX-kX) = \exp(0) = 1$, it follows that $\exp(-kX) = \exp(kX)^{-1} = \exp(X)^{-k}$. Therefore, the last assertion holds for all $k \in \mathbb{Z}$. ☐

Theorem 4.19. *For every $\alpha = \sum a_n X^n \in \mathbb{C}[[X]]$ with $a_0 = 0$ and $a_1 \neq 0$, there exists exactly one $\beta \in \mathbb{C}[[X]]$ with $\beta(\alpha) = \alpha(\beta) = X$. Therefore, $\mathbb{C}[[X]]^\circ := X\mathbb{C}[[X]] \setminus X^2\mathbb{C}[[X]]$ is a group with respect to $\circ$ with identity element X.*

Proof. Let $\alpha^k = \sum_{n=0}^{\infty} a_{k,n}X^n$ for $k \in \mathbb{N}_0$. Because of $a_0 = 0$, we have $a_{k,n} = 0$ for $n < k$ and $a_{n,n} = a_1^n \neq 0$. We define inductively $b_0 := 0$, $b_1 := \frac{1}{a_1} \neq 0$ and

$$b_n := -\frac{1}{a_{n,n}}\sum_{k=0}^{n-1} a_{k,n}b_k$$

for $n \geq 2$. For $\beta := \sum b_n X^n \in \mathbb{C}[[X]]^\circ$, it then holds that

$$\beta(\alpha) = \sum_{k=0}^{\infty} b_k\alpha^k = \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} b_k a_{k,n}X^n = \sum_{n=0}^{\infty}\Bigl(\sum_{k=0}^{n} b_k a_{k,n}\Bigr)X^n = X.$$

Interchanging the roles of α and β, one obtains $\gamma \in \mathbb{C}[[X]]^\circ$ with $\gamma(\beta) = X$. According to Lemma 4.16, it holds that

$$\alpha(\beta) = X \circ (\alpha \circ \beta) = (\gamma \circ \beta) \circ (\alpha \circ \beta) = \gamma \circ (\beta \circ \alpha) \circ \beta = \gamma \circ X \circ \beta = \gamma(\beta) = X.$$

Thus β is the inverse of α with respect to $\circ$. In particular, β is uniquely determined and $\mathbb{C}[[X]]^\circ$ is a group. ☐

Remark 4.20. In the situation of Theorem 4.19, β is called the *inverse function* of α. Note: $\beta \neq \alpha^{-1}$ (we will not introduce a notation for the inverse function).

Example 4.21.

(i) Let α be the inverse function of $X + X^2 + \ldots = \frac{X}{1-X}$. Then

$$X = \frac{\alpha}{1-\alpha}$$

and it follows that $\alpha = \frac{X}{1+X} = X - X^2 + X^3 - \ldots$.

(ii) Let $\alpha = \sum a_n X^n$ be the inverse function of $X - X^2$. Then

$$(a_1 X + a_2 X^2 + \ldots) - (a_1^2 X^2 + 2a_1 a_2 X^3 + (a_2^2 + 2a_1 a_3) X^4 + \ldots) = \alpha - \alpha^2 = X.$$

A comparison of coefficients yields $\alpha = X + X^2 + 2X^3 + 5X^4 + \ldots$ and in general $a_n = \sum_{k=1}^{n-1} a_k a_{n-k}$. These are the *Catalan numbers*.

Definition 4.22. For $\alpha = \sum a_n X^n \in \mathbb{C}[[X]]$,

$$\alpha' := \sum_{n=1}^{\infty} n a_n X^{n-1} \in \mathbb{C}[[X]]$$

is called the (formal) *derivative* of α. Furthermore, let $\alpha^{(0)} := \alpha$ and $\alpha^{(k)} := (\alpha^{(k-1)})'$ be the *k-th derivative* for $k \in \mathbb{N}$.

Example 4.23. We have $1' = 0$, $X' = 1$ as well as

$$\exp(X)' = \sum_{n=1}^{\infty} n \frac{X^{n-1}}{n!} = \sum_{n=0}^{\infty} \frac{X^n}{n!} = \exp(X).$$

Remark 4.24. The coefficients of $\alpha = \sum a_n X^n \in \mathbb{C}[[X]]$ can be calculated using derivatives: $\alpha^{(0)}(0) = \alpha(0) = a_0$, $\alpha'(0) = a_1$, $\alpha''(0) = 2a_2, \ldots, \alpha^{(n)}(0) = n! a_n$. Therefore

$$\boxed{\alpha = \sum_{n=0}^{\infty} \frac{\alpha^{(n)}(0)}{n!} X^n} \qquad (Taylor series).$$

Lemma 4.25. *For $\alpha, \beta, \alpha_1, \alpha_2, \ldots \in \mathbb{C}[[X]]$ the following holds (if well-defined):*

$$\begin{aligned}
\Big(\sum \alpha_k\Big)' &= \sum \alpha_k' && (\textit{sum rule}),\\
(\alpha\beta)' &= \alpha'\beta + \alpha\beta' && (\textit{product rule}),\\
\Big(\frac{\alpha}{\beta}\Big)' &= \frac{\alpha'\beta - \alpha\beta'}{\beta^2} && (\textit{quotient rule}),\\
(\alpha \circ \beta)' &= \alpha'(\beta)\beta' && (\textit{chain rule}).
\end{aligned}$$

Proof. With the notation from Remark 4.11, it holds that

$$\Big(\sum \alpha_k\Big)' = \Big(\sum_{n=0}^{\infty}\sum_{k=1}^{\infty} a_{k,n} X^n\Big)' = \sum_{n=0}^{\infty}\sum_{k=1}^{\infty} n a_{k,n} X^{n-1} = \sum_{k=1}^{\infty}\Big(\sum_{n=0}^{\infty} n a_{k,n} X^{n-1}\Big) = \sum \alpha_k'.$$

In the product rule, one may now assume $\alpha = X^k$ and $\beta = X^l$. Then

$$(\alpha\beta)' = (X^{k+l})' = (k+l)X^{k+l-1} = kX^{k-1}X^l + lX^{l-1}X^k = \alpha'\beta + \beta'\alpha.$$

It follows that

$$\alpha' = \Big(\frac{\alpha}{\beta}\beta\Big)' = \Big(\frac{\alpha}{\beta}\Big)'\beta + \frac{\alpha\beta'}{\beta}.$$

By rearranging, one obtains the quotient rule. By induction, we now show $(\alpha^n)' = n\alpha^{n-1}\alpha'$ for $n \in \mathbb{N}_0$. This is clear for $n = 0$. For $n \geq 1$, it holds that

$$(\alpha^n)' = (\alpha\alpha^{n-1})' = \alpha'\alpha^{n-1} + \alpha(\alpha^{n-1})' = \alpha'\alpha^{n-1} + (n-1)\alpha\alpha^{n-2}\alpha' = n\alpha^{n-1}\alpha'.$$

From the sum rule, it follows that

$$(\alpha \circ \beta)' = \Big(\sum a_n\beta^n\Big)' = \sum a_n(\beta^n)' = \sum_{n=1}^{\infty} na_n\beta^{n-1}\beta' = \alpha'(\beta)\beta'. \qquad \square$$

Remark 4.26. The product rule also implies the *constant factor rule* $(\lambda\alpha)' = \lambda\alpha'$ for $\lambda \in \mathbb{C}$ and $\alpha \in \mathbb{C}[[X]]$.

Example 4.27. We define the (formal) *logarithm* by the *Mercator series*

$$\boxed{\log(1+X) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} X^n = X - \frac{X^2}{2} + \frac{X^3}{3} \mp \ldots \in \mathbb{C}[[X]].}$$

According to Theorem 4.19, $\alpha := \exp(X) - 1$ possesses an inverse function and $\log(\exp(X)) = \log(1+\alpha) \in \mathbb{C}[[X]]^\circ$. Due to

$$\log(1+X)' = 1 - X + X^2 \mp \ldots = \sum (-X)^n = \frac{1}{1+X}$$

it follows from the chain rule that

$$\log(\exp(X))' = \frac{\alpha'}{1+\alpha} = \frac{\exp(X)}{1+\alpha} = \frac{1+\alpha}{1+\alpha} = 1.$$

This shows $\log(\exp(X)) = X$. Thus $\log(1+X)$ is the inverse function of $\alpha = \exp(X) - 1$ as in analysis. Furthermore, $\log(1-X) = -\sum_{n=1}^{\infty} \frac{X^n}{n}$ holds.

Lemma 4.28 (Functional equation)**.** *For* $\alpha_1, \alpha_2, \ldots \in X\mathbb{C}[[X]]$ *it holds* (*if well-defined*)

$$\boxed{\log\Big(\prod(1+\alpha_k)\Big) = \sum \log(1+\alpha_k).}$$

Proof.

$$\begin{aligned}\log\Big(\prod(1+\alpha_k)\Big) &= \log\Big(\prod \exp(\log(1+\alpha_k))\Big) \overset{4.18}{=} \log\Big(\exp\Big(\sum \log(1+\alpha_k)\Big)\Big) \\ &= \sum \log(1+\alpha_k). \qquad \square\end{aligned}$$

Example 4.29. According to Lemma 4.28, it holds that

$$\begin{aligned}\log\Bigl(\frac{1}{1-X}\Bigr) &= \log\Bigl(\frac{1}{1-X}\Bigr) + \log(1-X) - \log(1-X) = \log\Bigl(\frac{1}{1-X}(1-X)\Bigr) - \log(1-X)\\ &= \log(1) - \log(1-X) = -\log(1-X) = \sum_{n=1}^{\infty} \frac{X^n}{n}.\end{aligned}$$

Definition 4.30. For $c \in \mathbb{C}$ and $\alpha \in X\mathbb{C}[[X]]$ we define

$$(1+\alpha)^c := \exp(c\log(1+\alpha)).$$

In the case $c = 1/k$ with $k \in \mathbb{N}$ we write $\sqrt[k]{1+\alpha} := (1+\alpha)^{1/k}$ and specifically $\sqrt{1+\alpha} := \sqrt[2]{1+\alpha}$.

Remark 4.31.

(i) For $c = k \in \mathbb{Z}$, $(1+\alpha)^k$ coincides with the usual power according to Lemma 4.18. For $c, d \in \mathbb{C}$, the power law

$$(1+\alpha)^c(1+\alpha)^d = \exp(c\log(1+\alpha) + d\log(1+\alpha)) = (1+\alpha)^{c+d}$$

holds as usual. For $k \in \mathbb{N}$, it follows that $\sqrt[k]{1+\alpha}^{\,k} = 1+\alpha$, i. e. $\sqrt[k]{1+\alpha}$ is a k-th *root* of $1+\alpha$ with constant term 1. Let also $\beta \in \mathbb{C}[[X]]$ with $\beta^k = 1+\alpha$. Then $\sqrt[k]{1+\alpha}\beta^{-1}$ has order $\le k$ in $\mathbb{C}[[X]]^\times$. From Lemma 4.8 it follows that $\sqrt[k]{1+\alpha}\beta^{-1}$ is constant, i. e. $\beta = \beta(0)\sqrt[k]{1+\alpha}$. Therefore, $\sqrt[k]{1+\alpha}$ is the unique k-th root of $1+\alpha$ with constant term 1.

(ii) The following theorem generalizes both the binomial theorem ($c \in \mathbb{N}$) and the geometric series ($c = -1$).

Theorem 4.32 (NEWTON's Binomial Theorem). *For $\alpha \in X\mathbb{C}[[X]]$ and $c \in \mathbb{C}$ we have*

$$\boxed{(1+\alpha)^c = \sum_{k=0}^{\infty} \binom{c}{k} \alpha^k.}$$

Proof. It suffices to prove the claim for $\alpha = X$. According to the chain rule, we have

$$((1+X)^c)' = (\exp(c\log(1+X)))' = c\frac{(1+X)^c}{1+X} = c(1+X)^{c-1}$$

and by induction it follows that $((1+X)^c)^{(k)} = c(c-1)\ldots(c-k+1)(1+X)^{c-k}$. The claim now follows from the Taylor series. $\square$

Example 4.33.

(i) We have

$$\sqrt{1+X} = \sum_{k=0}^{\infty} \binom{1/2}{k} X^k = 1 + \frac{1}{2}X - \frac{1}{8}X^2 + \frac{1}{16}X^3 - \frac{5}{2^7}X^4 \pm \ldots.$$

(ii) Let $\zeta \in \mathbb{C}$ with $\zeta^n = 1$ and $\alpha := (1+X)^\zeta - 1 \in X\mathbb{C}[[X]]$. Then $\alpha \circ \alpha = (1+(1+X)^\zeta - 1)^\zeta - 1 = (1+X)^{\zeta^2} - 1$ and by induction $\alpha \circ \ldots \circ \alpha = (1+X)^{\zeta^n} - 1 = X$, i. e. the order of α in the group $\mathbb{C}[[X]]^\circ$ divides n. In contrast to Lemma 4.8, $\mathbb{C}[[X]]^\circ$ thus possesses “interesting” elements of finite order.

Definition 4.34. For $n \in \mathbb{N}_0$ let $X^n! := (1-X)(1-X^2)\dots(1-X^n)$. For $0 \le k \le n$ one calls

$$\left\langle {n \atop k} \right\rangle := \frac{X^n!}{X^k!X^{n-k}!} = \frac{1-X^n}{1-X^k} \cdots \frac{1-X^{n-k+1}}{1-X} \in \mathbb{C}[[X]]$$

Gaussian binomial coefficients. For $k<0$ or $k>n$ let $\left\langle {n \atop k} \right\rangle := 0$.

Remark 4.35. As always, $\left\langle {n \atop 0} \right\rangle = \left\langle {n \atop n} \right\rangle = 1$ and $\left\langle {n \atop k} \right\rangle = \left\langle {n \atop n-k} \right\rangle$ for all $n \in \mathbb{N}_0$ and $k \in \mathbb{Z}$. Furthermore, $\left\langle {n \atop 1} \right\rangle = \frac{1-X^n}{1-X} = 1 + X + \ldots + X^{n-1}$ and

$$\left\langle {4 \atop 2} \right\rangle = \frac{(1-X^4)(1-X^3)}{(1-X^2)(1-X)} = (1+X^2)\frac{1-X^3}{1-X} = (1+X^2)(1+X+X^2) = 1 + X + 2X^2 + X^3 + X^4.$$

The next lemma shows inductively that $\left\langle {n \atop k} \right\rangle$ is always a polynomial.

Lemma 4.36. *For $n \in \mathbb{N}_0$ and $k \in \mathbb{Z}$, we have*

$$\left\langle {n+1 \atop k} \right\rangle = X^k \left\langle {n \atop k} \right\rangle + \left\langle {n \atop k-1} \right\rangle = \left\langle {n \atop k} \right\rangle + X^{n+1-k} \left\langle {n \atop k-1} \right\rangle.$$

Proof. For $k > n+1$ or $k < 0$, all terms are 0. For $k = n+1$ or $k = 0$, both sides are 1. For $1 \le k \le n$, we have

$$\begin{aligned} X^k \left\langle {n \atop k} \right\rangle + \left\langle {n \atop k-1} \right\rangle &= \Big(X^k \frac{1-X^{n-k+1}}{1-X^k} + 1\Big) \frac{X^n!}{X^{k-1}!X^{n-k+1}!} = \frac{1-X^{n+1}}{1-X^k} \frac{X^n!}{X^{k-1}!X^{n+1-k}!} \\ &= \left\langle {n+1 \atop k} \right\rangle = \left\langle {n+1 \atop n+1-k} \right\rangle = X^{n+1-k} \left\langle {n \atop n+1-k} \right\rangle + \left\langle {n \atop n-k} \right\rangle \\ &= \left\langle {n \atop k} \right\rangle + X^{n+1-k} \left\langle {n \atop k-1} \right\rangle. \end{aligned}$$

□

Remark 4.37. One may compare the recursion formulas[8]

$$\begin{aligned} \binom{n+1}{k} &\overset{1.5}{=} \binom{n}{k-1} + \binom{n}{k}, \\ \left(\!\!\binom{n+1}{k}\!\!\right) &\overset{1.24}{=} \left(\!\!\binom{n+1}{k-1}\!\!\right) + \left(\!\!\binom{n}{k}\!\!\right), \\ \begin{bmatrix} n+1 \\ k \end{bmatrix} &\overset{2.16}{=} \begin{bmatrix} n \\ k-1 \end{bmatrix} + n \begin{bmatrix} n \\ k \end{bmatrix}, \\ \begin{Bmatrix} n+1 \\ k \end{Bmatrix} &\overset{2.30}{=} \begin{Bmatrix} n \\ k-1 \end{Bmatrix} + k \begin{Bmatrix} n \\ k \end{Bmatrix}, \\ \left\langle {n+1 \atop k} \right\rangle &\overset{4.36}{=} \left\langle {n \atop k-1} \right\rangle + X^k \left\langle {n \atop k} \right\rangle. \end{aligned}$$

Thus, one can compute $\left(\!\binom{n}{k}\!\right)$, $\left[{n \atop k}\right]$, $\left\{{n \atop k}\right\}$ and $\left\langle {n \atop k} \right\rangle$ with a modified Pascal's triangle.

Theorem 4.38 (GAUSSian Binomial Theorem). *For $n \in \mathbb{N}_0$ and $\alpha \in \mathbb{C}[[X]]$, we have*

$$\boxed{\prod_{k=0}^{n-1} (1 + \alpha X^k) = \sum_{k=0}^{n} \left\langle {n \atop k} \right\rangle \alpha^k X^{\binom{k}{2}}.}$$

---

[8] All formulas can be unified: [J. Konvalina, *A unified interpretation of the binomial coefficients, the Stirling numbers, and the Gaussian coefficients*, Amer. Math. Monthly 107, (2000), 901–910]

Proof. Induction on n: For $n = 0$, both sides are 1. For $n \geq 1$, we have

$$\begin{aligned}
\prod_{k=0}^{n}(1+\alpha X^k) &= (1+\alpha X^n)\sum_{k=-\infty}^{\infty}\left\langle{n \atop k}\right\rangle \alpha^k X^{\binom{k}{2}} \\
&= \sum \left\langle{n \atop k}\right\rangle \alpha^k X^{\binom{k}{2}} + \sum \left\langle{n \atop k}\right\rangle \alpha^{k+1} X^{n-k} X^{\overbrace{\binom{k}{2}+k}^{\binom{k+1}{2}}} \\
&= \sum \left\langle{n \atop k}\right\rangle \alpha^k X^{\binom{k}{2}} + \sum X^{n+1-k}\left\langle{n \atop k-1}\right\rangle \alpha^k X^{\binom{k}{2}} \\
&\overset{4.36}{=} \sum \left\langle{n+1 \atop k}\right\rangle \alpha^k X^{\binom{k}{2}}.
\end{aligned}$$

□

Remark 4.39. There is also a Vandermonde identity for $\left\langle{n \atop k}\right\rangle$.

5 Generating Functions

Definition 5.1. The *generating function* of a sequence of numbers $a_0, a_1, \ldots \in \mathbb{C}$ is the power series

$$\sum_{n=0}^{\infty} a_n X^n \in \mathbb{C}[[X]].$$

This seemingly trivial reformulation has astonishing consequences.

Example 5.2.

(i) The generating function of the constant sequence $1, 1, \ldots$ is $(1-X)^{-1}$.

(ii) If $\alpha \in \mathbb{C}[[X]]$ is the generating function of $a_0, a_1, \ldots$, then $\alpha(-X)$ is the generating function of $a_0, -a_1, a_2, \ldots$.

(iii) If α is the generating function of $a_0, a_1, \ldots$, then α' is the generating function of $a_1, 2a_2, 3a_3, \ldots$. For example, $\left(\frac{1}{1-X}\right)' = \frac{1}{(1-X)^2}$ (quotient rule) is the generating function of $1, 2, 3, \ldots$.

(iv) The generating function of the binomial coefficients is $(1+X)^n = \sum_{k=0}^{\infty}\binom{n}{k}X^k$.

(v) Every k-element multiset $A \subseteq \{1, \ldots, n\}$ corresponds exactly to one decomposition $k = k_1 + \ldots + k_n$, where $k_i \in \mathbb{N}_0$ denotes the multiplicity of i in A. This shows

$$\frac{1}{(1-X)^n} = \Bigl(\sum_{k=0}^{\infty} X^k\Bigr)^n = \sum_{k=0}^{\infty}\Bigl(\sum_{\substack{(k_1,\ldots,k_n)\in\mathbb{N}_0^n \\ k_1+\ldots+k_n=k}} 1\Bigr)X^k = \sum_{k=0}^{\infty}\left(\!\binom{n}{k}\!\right)X^k$$

for $n \in \mathbb{N}$ (cf. Theorem 4.32 and Exercise 12).

(vi) The generating function of the Stirling numbers $\left[{n \atop k}\right]$ is given by Theorem 2.17:

$$X(X+1)\ldots(X+n-1) = \sum_{k=0}^{\infty}\left[{n \atop k}\right]X^k.$$

(vii) For the generating function $\alpha := \sum F_n X^n$ of the Fibonacci sequence (Example 3.1), it holds that

$$\alpha = X + \sum_{n=2}^{\infty} F_n X^n = X + \sum_{n=2}^{\infty} (F_{n-2} + F_{n-1}) X^n = X + X^2\alpha + X\alpha.$$

Thus

$$\alpha = \frac{X}{1 - X - X^2}.$$

One can use this to provide an alternative proof of the Binet formula (Exercise 20).

(viii) In Example 4.21 we introduced the generating function α of the Catalan numbers C_n via the equation $\alpha - \alpha^2 = X$. Using the quadratic formula for quadratic equations, one obtains

$$\alpha = \frac{1}{2}\Big(1 - \sqrt{1-4X}\Big) \in \mathbb{C}[[X]]^\circ \tag{5.1}$$

(the second solution does not lie in $\mathbb{C}[[X]]^\circ$). Check:

$$\alpha - \alpha^2 = \frac{1}{2}\Big(1 - \sqrt{1-4X}\Big) - \frac{1}{4}\Big(1 - 2\sqrt{1-4X} + 1 - 4X\Big) = X.$$

Theorem 5.3 (Catalan)**.** *For $n \in \mathbb{N}_0$ it holds that*

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

Proof. According to Newton's binomial theorem,

$$\sum C_n X^n \overset{(5.1)}{=} \frac{1}{2}\Big(1 - \sqrt{1-4X}\Big) = \frac{1}{2}\Big(1 - \sum \binom{1/2}{n} (-4)^n X^n\Big).$$

A comparison of coefficients shows

$$\begin{aligned} C_{n+1} &= (-1)^n \frac{1}{2}\binom{1/2}{n+1} 4^{n+1} = (-1)^n \frac{2^{n+1}}{2} \cdot \frac{2(1/2)\cdot 2(1/2-1)\cdot \ldots \cdot 2(1/2-n)}{(n+1)!} \\ &= \frac{2^n}{n+1} \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2n-1)}{n!} = \frac{1}{n+1} \frac{2\cdot 4\cdot \ldots \cdot 2n}{n!} \cdot \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2n-1)}{n!} \\ &= \frac{1}{n+1} \frac{(2n)!}{(n!)^2} = \frac{1}{n+1}\binom{2n}{n}. \end{aligned}$$

□

Theorem 5.4. *The following holds:*

(*i*) $$\boxed{\sum_{n=0}^{\infty} p(n) X^n = \prod_{k=1}^{\infty} \frac{1}{1 - X^k}}$$ (Euler),

(*ii*) $$\boxed{\sum_{n=0}^{\infty} \frac{b(n)}{n!} X^n = \exp(\exp(X) - 1).}$$

Proof.

(i) Since $(1-X^k)^{-1} = \sum_{n=0}^{\infty}(X^k)^n \in 1+X^k\mathbb{C}[[X]]$, the infinite product is well-defined (Remark 4.11). The partition $(1^{a_1},\ldots,n^{a_n})$ of $n \in \mathbb{N}_0$ satisfies $a_1 + 2a_2 + \ldots + na_n = n$. Therefore, $p(n)$ is the number of all tuples $(a_1,\ldots,a_n) \in \mathbb{N}_0^n$ with $a_1 + 2a_2 + \ldots + na_n = n$. This is exactly the n-th coefficient of

$$(1+X+X^2+X^3+\ldots)(1+X^2+X^{2\cdot 2}+X^{2\cdot 3}+\ldots)(1+X^3+X^{3\cdot 2}+X^{3\cdot 3}+\ldots)\ldots = \prod_{k=1}^{\infty}\frac{1}{1-X^k}.$$

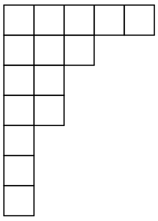
(ii) Let $\alpha := \exp(\exp(X)-1) = \sum \frac{a_n}{n!}X^n$. Then $a_0 = \exp(\exp(0)-1) = \exp(0) = 1 = b(0)$. The chain rule yields

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{a_{n+1}}{n!}X^n &= \alpha' = \exp(X)\exp(\exp(X)-1)\\ &= \Big(\sum_{k=0}^{\infty}\frac{1}{k!}X^k\Big)\Big(\sum_{k=0}^{\infty}\frac{a_k}{k!}X^k\Big) = \sum_{n=0}^{\infty}\sum_{k=0}^{n}\frac{a_k}{k!(n-k)!}X^n.\end{aligned}$$

Therefore $a_{n+1} = \sum_{k=0}^{n}\binom{n}{k}a_k$ for $n \geq 0$ and the claim follows from Theorem 2.37. □

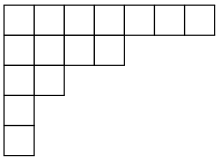
Remark 5.5. One can visualize partitions $\lambda = (\lambda_1,\ldots,\lambda_k)$ (with $\lambda_1 \geq \ldots \geq \lambda_k$) of $n \in \mathbb{N}$ by *Young diagrams* (also called *Ferrers diagrams*). For example:

$(5,3,2^2,1^3) =$



By reflection across the diagonal, one obtains the Young diagram of the *conjugate* partition $\lambda' = (\lambda'_1,\ldots,\lambda'_l)$ of n. For example:

$(5,3,2^2,1^3)' =$



$= (7,4,2,1^2)$

In general, $\lambda'_i = |\{j : \lambda_j \geq i\}|$ for $i = 1,\ldots,l$. Furthermore, $\lambda'' = \lambda$. One calls λ *symmetric*, if $\lambda' = \lambda$.

Theorem 5.6. *Let $n, k \in \mathbb{N}_0$.*

(i) (Euler) *The number of partitions of n into distinct parts is equal to the number of partitions into odd parts.*

(ii) The number of partitions of n into k parts is equal to the number of partitions with largest part k.

(iii) (Sylvester) *The number of symmetric partitions of n is equal to the number of partitions into distinct, odd parts.*

Proof.

(i) If $u(n)$ is the number of partitions into distinct parts, then

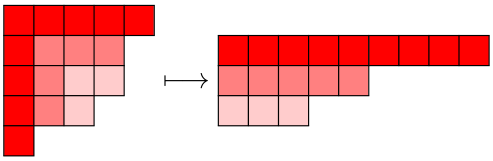
$$\begin{aligned}\sum u(n)X^n &= (1+X)(1+X^2)(1+X^3)\ldots = \frac{(1-X^2)(1-X^4)}{(1-X)(1-X^2)}\cdots \\ &= \frac{1}{(1-X)(1-X^3)(1-X^5)\ldots} \\ &= (1+X+X^2+\ldots)(1+X^3+X^6+\ldots)\ldots.\end{aligned}$$

On the right side stands the generating function of the number of partitions into odd parts.

(ii) The map $\lambda \mapsto \lambda'$ provides a bijection between the specified sets.

(iii) The following map provides the desired bijection:

$$\begin{aligned}\{\text{symmetric partitions of } n\} &\longrightarrow \{\text{partitions into distinct, odd parts}\},\\ (\lambda_1,\ldots,\lambda_k) &\longmapsto (2\lambda_1-1, 2\lambda_2-3, 2\lambda_3-5,\ldots)\end{aligned}$$



□

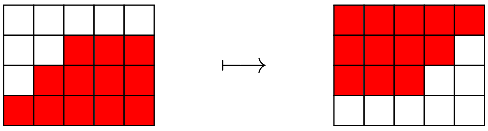
Example 5.7. For $n = 8$ one obtains

Partitions into distinct parts:	(8), $(7,1)$, $(6,2)$, $(5,3)$, $(5,2,1)$, $(4,3,1)$
Partitions into odd parts:	$(7,1)$, $(5,3)$, $(5,1^3)$, $(3^2,1^2)$, $(3,1^5)$, (1^8)
Partitions into distinct, odd parts:	$(7,1)$, $(5,3)$
Symmetric partitions:	$(3^2,2)$, $(4,2,1^2)$
Partitions into 4 parts:	$(5,1^3)$, $(4,2,1^2)$, $(3^2,1^2)$, $(3,2^2,1)$, (2^4)
Partitions with largest part 4:	(4^2), $(4,3,1)$, $(4,2^2)$, $(4,2,1^2)$, $(4,1^4)$

Remark 5.8. Let $p_k(n)$ be the number of partitions of n into parts $\le k$ (according to Theorem 5.6, this is also the number of partitions into at most k parts). The proof of Theorem 5.4 shows

$$\sum_{n=0}^{\infty} p_k(n)X^n = (1+X+X^2+\ldots)(1+X^2+X^4+\ldots)\ldots(1+X^k+X^{2k}+\ldots) = \frac{1}{X^k!}.$$

We now study the number $p_{k,l}(n) = p_{l,k}(n)$ of partitions of n with at most k parts and each part $\le l$. These are exactly the partitions whose Young diagram fits into a rectangle of size $k \times l$. The remaining part of the rectangle rotated by 180° yields a partition of $kl - n$ of the same format:



This shows $p_{k,l}(n) = p_{k,l}(kl-n)$.

Theorem 5.9. *For $k, l \ge 0$ we have*

$$\sum_{n=0}^{\infty} p_{k,l}(n)X^n = \left\langle {k+l \atop k} \right\rangle.$$

Proof. Induction on $k+l$. For $k=0$ or $l=0$, both sides are equal to 1. So let $k,l \geq 1$. Let $\lambda = (\lambda_1, \lambda_2, \ldots) \in P(n)$ with at most k parts and each part $\leq l$. If $\lambda_1 = l$, then $(\lambda_2, \lambda_3, \ldots) \in P(n-l)$ with at most $k-1$ parts. Otherwise, every part of λ is at most $l-1$. This shows $p_{k,l}(n) = p_{k,l-1}(n) + p_{k-1,l}(n-l)$. For $P(k,l) := \sum p_{k,l}(n)X^n$ it therefore holds that

$$P(k,l) = P(k,l-1) + X^l P(k-1,l).$$

The claim now follows by induction and Lemma 4.36. $\square$

Remark 5.10. Because of $p_{k,l}(kl) = 1$ and $p_{k,l}(n) = 0$ for $n > kl$, $\langle{n \atop k}\rangle$ is a polynomial of degree $k(n-k)$ with positive coefficients. From $p_{k,l}(n) = p_{k,l}(kl-n)$ it also follows that the coefficients are "symmetric". If one sets $X = 1$ in Theorem 5.9, one obtains on the left side the number of partitions that fit into the $k \times l$-rectangle. The right side becomes the ordinary binomial coefficient for $X = 1$, because

$$\left\langle {n \atop k} \right\rangle = \frac{\frac{1-X^n}{1-X} \cdots \frac{1-X^{n-k+1}}{1-X}}{\frac{1-X^k}{1-X} \cdots \frac{1-X}{1-X}} = \frac{(1+X+\ldots+X^{n-1})\ldots(1+\ldots+X^{n-k})}{(1+\ldots+X^{k-1})\ldots 1}.$$

The Gaussian binomial theorem thus becomes the ordinary binomial theorem for $X = 1$.

Example 5.11.

$$\left\langle {5 \atop 2} \right\rangle = p_{2,3}(0) + \ldots + p_{2,3}(6)X^6 = 1 + X + 2X^2 + 2X^3 + 2X^4 + X^5 + X^6.$$

Theorem 5.12 (Erdős-Turán). *Let $n, d \in \mathbb{N}$. The number of permutations of S_n whose cycle lengths are not divisible by d is*

$$n! \prod_{k=1}^{\lfloor n/d \rfloor} \frac{kd-1}{kd}.$$

Proof (Pólya). The number of permutations of type $(1^{l_1}, \ldots, n^{l_n})$ is

$$\frac{n!}{1^{l_1} \ldots n^{l_n} l_1! \ldots l_n!}$$

according to Theorem 2.25. The sought number, divided by $n!$, is therefore the coefficient of X^n in

$$\begin{aligned}\prod_{\substack{k=1\\ d\nmid k}}^{\infty} \sum_{l=0}^{\infty} \frac{1}{l!}\Big(\frac{X^k}{k}\Big)^l &= \prod_{d\nmid k} \exp(X^k/k) \overset{4.18}{=} \exp\Big(\sum_{d\nmid k} \frac{X^k}{k}\Big) = \exp\Big(\sum_{k=1}^{\infty} \frac{X^k}{k} - \sum_{k=1}^{\infty} \frac{X^{dk}}{dk}\Big) \\ &= \exp(-\log(1-X) + \frac{1}{d}\log(1-X^d)) \overset{4.28}{=} \frac{1}{1-X}\sqrt[d]{1-X^d} \\ &= \frac{1-X^d}{1-X}(1-X^d)^{\frac{1-d}{d}} \overset{4.32}{=} \Big(\sum_{r=0}^{d-1} X^r\Big)\Big(\sum_{q=0}^{\infty} \binom{(1-d)/d}{q} (-X^d)^q\Big).\end{aligned}$$

In this, X^n occurs if and only if $n = qd + r$ with $0 \leq r < d$ and $q = \lfloor n/d \rfloor$ (division with remainder). The coefficient is then

$$(-1)^q \binom{(1-d)/d}{q} = (-1)^q \prod_{k=1}^{q} \frac{\frac{1}{d} - k}{k} = \prod_{k=1}^{q} \frac{kd-1}{kd}. \qquad \square$$

Example 5.13. A permutation has odd order if and only if it consists only of cycles of odd length. The number of permutations in S_n with odd order is therefore

$$n!\prod_{k=1}^{\lfloor n/2\rfloor}\frac{2k-1}{2k}=\begin{cases}1^2\cdot 3^2\cdot\ldots\cdot(n-1)^2 & \text{if } n \text{ is even,}\\ 1^2\cdot 3^2\cdot\ldots\cdot(n-2)^2\cdot n & \text{if } n \text{ is odd}\end{cases}$$

(cf. Exercise 22). Specifically for $n=5$, one counts $4!=24$ 5-cycles (Theorem 2.10), $\frac{5!}{3\cdot 2!}=20$ permutations of cycle type $(3,1^2)$ and the identity. Thus a total of $24+20+1=45=3^2\cdot 5$.

Theorem 5.14 (EULER's Pentagonal Number Theorem)**.**

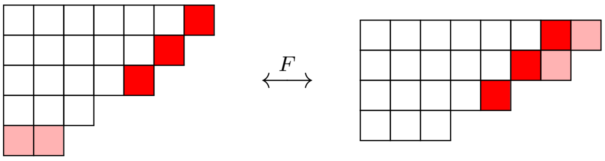
$$\prod_{k=1}^{\infty}(1-X^k)=1+\sum_{k=1}^{\infty}(-1)^k\Big(X^{\frac{3k^2-k}{2}}+X^{\frac{3k^2+k}{2}}\Big)=\sum_{k=-\infty}^{\infty}(-1)^kX^{\frac{3k^2+k}{2}}$$
$$=1-X-X^2+X^5+X^7-X^{12}-X^{15}+\ldots.$$

Proof (FRANKLIN). Let $n\in\mathbb{N}$ and Λ_n be the set of partitions of n into distinct parts. For $\lambda\in\Lambda_n$ let $|\lambda|$ be the number of parts of λ. The n-th coefficient of $(1-X)(1-X^2)\ldots$ is then $\sum_{\lambda\in\Lambda_n}(-1)^{|\lambda|}$ (cf. proof of Theorem 5.6). Suppose first $n\ne(3k^2\pm k)/2$ for all $k\in\mathbb{N}$. We construct a permutation F on Λ_n with $|F(\lambda)|=|\lambda|\pm 1$ for all $\lambda\in\Lambda_n$. Then it follows

$$\sum_{\lambda\in\Lambda_n}(-1)^{|\lambda|}=\sum_{\lambda\in\Lambda_n}(-1)^{|F(\lambda)|}=-\sum_{\lambda\in\Lambda_n}(-1)^{|\lambda|}=0$$

as desired. Let $\lambda=(\lambda_1,\ldots,\lambda_l)\in\Lambda_n$ with $\lambda_1>\ldots>\lambda_l$ and $s:=\max\{1\le i\le l:\lambda_i=\lambda_1-i+1\}$. We define

$$F(\lambda):=\begin{cases}(\lambda_1-1,\ldots,\lambda_s-1,\lambda_{s+1},\ldots,\lambda_l,s) & \text{if } s<\lambda_l,\\ (\lambda_1+1,\ldots,\lambda_{\lambda_l}+1,\lambda_{\lambda_l+1},\ldots,\lambda_{l-1}) & \text{if } s\ge\lambda_l.\end{cases}$$



This fails only in two cases: In the first case $\lambda=(2k-1,2k-2,\ldots,k)$ and

$$n=\sum_{i=k}^{2k-1}i=\binom{2k}{2}-\binom{k}{2}=\frac{3k^2-k}{2}.$$

In the second case $\lambda=(2k,2k-1,\ldots,k+1)$ and

$$n=\sum_{i=k+1}^{2k}i=\binom{2k+1}{2}-\binom{k+1}{2}=\frac{3k^2+k}{2}.$$

Both were excluded. Thus F is well-defined and $|F(\lambda)|=|\lambda|\pm 1$ for all $\lambda\in\Lambda_n$. Since $F^2=\mathrm{id}$, F is a permutation.

If now $n=(3k^2\pm k)/2$, then F can still be defined on $\Lambda_n\setminus\{\mu\}$, where μ is one of the two partitions mentioned above. One then obtains

$$\sum_{\lambda\in\Lambda_n}(-1)^{|\lambda|}=(-1)^{|\mu|}+\sum_{\lambda\in\Lambda_n\setminus\{\mu\}}(-1)^{|F(\lambda)|}=(-1)^k-\sum_{\lambda\in\Lambda_n\setminus\{\mu\}}(-1)^{|\lambda|}=(-1)^k$$

as desired. □

Remark 5.15. From Theorems 5.4 and 5.14 it follows that

$$\sum_{n=0}^{\infty} p(n)X^n \cdot \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{3k^2+k}{2}} = 1$$

and

$$\sum_{k=-n}^{n} (-1)^k p\Big(n - \frac{3k^2+k}{2}\Big) = 0$$

for $n \in \mathbb{N}$, where $p(k) := 0$ for $k < 0$. One obtains a recurrence formula:

$$\begin{aligned} &p(0) = 1, \\ &p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + \dots \qquad (n \in \mathbb{N}). \end{aligned}$$

Example 5.16. It holds that

$$\begin{aligned} p(1) &= p(0) = 1, \\ p(2) &= p(1) + p(0) = 2, \\ p(3) &= p(2) + p(1) = 3, \\ p(4) &= p(3) + p(2) = 3 + 2 = 5, \\ p(5) &= p(4) + p(3) - p(0) = 5 + 3 - 1 = 7, \\ p(6) &= p(5) + p(4) - p(1) = 7 + 5 - 1 = 11 \end{aligned}$$

(cf. `https://oeis.org/A000041`).

Corollary 5.17. *For all $n \in \mathbb{N}_0$, it holds that $p(n) \le F_{n+1}$, where F_n is the n-th Fibonacci number.*

Proof. Since one can produce a partition of $n + 1$ from every partition of n by appending a 1, it holds that $p(n) \le p(n+1)$ for all $n \in \mathbb{N}_0$. From Remark 5.15, it therefore follows that $p(n) \le p(n-1)+p(n-2)$. Because of $p(0) = 1 = F_1$ and $p(1) = 1 = F_2$, one obtains $p(n) \le F_{n+1}$ by induction. ☐

Remark 5.18. Ramanujan proved

$$\begin{aligned} 5 &\mid p(5n+4), \\ 7 &\mid p(7n+5), \\ 11 &\mid p(11n+6) \end{aligned}$$

for all $n \in \mathbb{N}_0$.[9]

6 Counting up to symmetry

Remark 6.1. Many counting problems simplify if one takes symmetries into account. Symmetries are modeled by groups. We repeat a few facts from algebra.

Definition 6.2. An *action* of a group G on a set Ω is a map $G \times \Omega \to \Omega$, $(g, \omega) \mapsto {}^g\omega$ with the following properties:

- $\forall \omega \in \Omega : {}^1\omega = \omega$,

---

[9] A proof of the first two statements can be found in my combinatorics notes.

- $\forall g,h \in G \,\forall \omega \in \Omega : {}^{g}({}^{h}\omega) = {}^{gh}\omega$.

For $\omega \in \Omega$, one calls ${}^{G}\omega := \{{}^{g}\omega : g \in G\} \subseteq \Omega$ the *orbit* of ω and $G_\omega := \{g \in G : {}^{g}\omega = \omega\} \le G$ the *stabilizer* of ω in G. If only one orbit exists, the action is called *transitive*. One calls $|{}^{G}\omega|$ the *length* of the orbit.

Example 6.3.

(i) For every set A, $G := \mathrm{Sym}(A)$ operates on A by ${}^{\sigma}a := \sigma(a)$, because $\mathrm{id}(a) = a$ and ${}^{\sigma}({}^{\tau}a) = \sigma(\tau(a)) = (\sigma\tau)(a) = {}^{\sigma\tau}a$ for $a \in A$ and $\sigma, \tau \in G$. This operation is transitive, because for distinct $a, b \in A$ the transposition (a, b) lies in G and ${}^{(a,b)}a = b$. This shows ${}^{G}a = A$ for all $a \in A$. The length of a cycle $\sigma \in \mathrm{Sym}(A)$ is simultaneously the length of an orbit of $\langle\sigma\rangle$.

(ii) For every K-vector space V, $G := \mathrm{GL}(V)$ operates on V by ${}^{f}v := f(v)$ for $f \in \mathrm{GL}(V)$ and $v \in V$. This follows from (i) because $G \le \mathrm{Sym}(V)$. The orbit of the zero vector is ${}^{G}0 = \{0\}$. In particular, the operation is only transitive if $V = \{0\}$.

(iii) Let $\Omega := \{1, \ldots, n\}$ be the set of vertices of a regular n-gon $\Delta \subseteq \mathbb{R}^2$ with $n \ge 3$. With a suitable arrangement, the n-cycle $\sigma = (1, \ldots, n) \in S_n$ describes a rotation of Δ by the angle $2\pi/n$. In this way, the cyclic group $\langle\sigma\rangle$ operates transitively on Ω. The permutation $\tau = (1, n)(2, n-1) \ldots \in S_n$ describes a reflection of Δ (if n is odd, the axis of reflection passes through the fixed point $(n+1)/2$; if n is even, τ has no fixed points). The symmetries σ and τ together generate the *dihedral group* $D_{2n} := \langle\sigma, \tau\rangle \le S_n$. As is well known, D_{2n} consists of all products of the form $\sigma^{i_1}\tau^{i_2}\sigma^{i_3}\ldots$. Because of $\sigma^n = \tau^2 = 1$ and $\tau\sigma = \sigma^{-1}\tau$, every element can be uniquely written in the form $\sigma^i\tau^j$ with $0 \le i \le n-1$ and $0 \le j \le 1$. This shows $|D_{2n}| = 2n$.

Remark 6.4.

(i) For $g \in G$, the map $\omega \mapsto {}^{g}\omega$ is a bijection on Ω with inverse map $\omega \mapsto {}^{g^{-1}}\omega$, because ${}^{g}({}^{g^{-1}}\omega) = {}^{gg^{-1}}\omega = {}^{1}\omega = \omega = \ldots = {}^{g^{-1}}({}^{g}\omega)$. Therefore, each g determines a permutation in $\mathrm{Sym}(\Omega)$.

(ii) We show that

$$\alpha \sim \beta \;:\Longleftrightarrow\; \exists g \in G : {}^{g}\alpha = \beta$$

defines an equivalence relation on Ω. Due to ${}^{1}\alpha = \alpha$, $\sim$ is reflexive. From ${}^{g}\alpha = \beta$ it follows that ${}^{g^{-1}}\beta = {}^{g^{-1}}({}^{g}\alpha) = {}^{g^{-1}g}\alpha = {}^{1}\alpha = \alpha$. Thus $\sim$ is symmetric. Finally, let ${}^{g}\alpha = \beta$ and ${}^{h}\beta = \gamma$ for $g, h \in G$ and $\alpha, \beta, \gamma \in \Omega$. Then ${}^{hg}\alpha = {}^{h}({}^{g}\alpha) = {}^{h}\beta = \gamma$. Therefore $\sim$ is transitive and an equivalence relation. The equivalence classes are exactly the orbits. In particular, the orbits form a partition of Ω.

(iii) Let $H \le G$. Then H acts on G by ${}^{h}x := xh^{-1}$ for $h \in H$ and $x \in G$, because ${}^{1}x = x1^{-1} = x$ and

$${}^{g}({}^{h}x) = {}^{g}(xh^{-1}) = (xh^{-1})g^{-1} = x(h^{-1}g^{-1}) = x(gh)^{-1} = {}^{gh}x$$

for $g, h \in H$. The orbits are the *left cosets* $xH := \{xh : h \in H\}$ for $x \in G$. Let $G/H := \{xH : x \in G\}$ and $|G : H| := |G/H|$ be the *index* of H in G. For $x \in G$, the map $H \to xH$, $h \to xh$ is bijective with inverse map $g \mapsto x^{-1}g$. Thus all left cosets of H have the cardinality $|H|$. The theorem of *Lagrange* follows: $\boxed{|G| = |G : H||H|.}$ In particular, $|H|$ and $|G : H|$ are divisors of $|G|$ if $|G| < \infty$.

Theorem 6.5 (Orbit-Stabilizer Theorem). *For every action of G on a set Ω, it holds that*

$$\boxed{|{}^{G}\omega| = |G : G_\omega|}$$

for all $\omega \in \Omega$.

Proof. It suffices to show that the map $F\colon G/G_\omega \to {}^G\omega$, $xG_\omega \mapsto {}^x\omega$ is a bijection. Due to

$$xG_\omega = yG_\omega \iff y^{-1}x \in G_\omega \iff {}^{y^{-1}x}\omega = \omega \iff {}^y\omega = {}^y({}^{y^{-1}x}\omega) = {}^x\omega$$

for $x, y \in G$, F is well-defined and injective. The surjectivity follows from the definition of the orbit. $\square$

Remark 6.6.

(i) Theorem 6.5 and Lagrange show that the orbit lengths are always divisors of the group order if $|G| < \infty$.

(ii) If Δ is a system of representatives for the orbits of G on Ω, then one obtains the *orbit equation*

$$\boxed{|\Omega| = \sum_{\delta\in\Delta} |{}^G\delta| = \sum_{\delta\in\Delta} |G : G_\delta|.}$$

(iii) Let $|G| = 77$ and $|\Omega| = 23$. According to the orbit equation, there exist $a, b, c \in \mathbb{N}_0$ with $23 = a + 7b + 11c$. It follows that $a > 0$, i.e., G always has a fixed point on Ω.

Theorem 6.7 (BURNSIDES Lemma). *Let G be a finite group acting on a set Ω. For $g \in G$, let $f(g) := |\{\omega \in \Omega : g \in G_\omega\}|$ be the number of fixed points of g on Ω. Then*

$$\boxed{\frac{1}{|G|}\sum_{g\in G} f(g)}$$

is the number of orbits of G on Ω.

Proof. If $\alpha, \beta \in \Omega$ lie in the same orbit, then $|G : G_\alpha| = |{}^G\alpha| = |{}^G\beta| = |G : G_\beta|$. By Lagrange it follows that $|G_\alpha| = |G_\beta|$ (note: $|G| < \infty$). Let $\Delta \subseteq \Omega$ be a transversal for the orbits of G on Ω. Then

$$\begin{aligned}\sum_{g\in G} f(g) &= |\{(g,\omega) \in G \times \Omega : {}^g\omega = \omega\}| = \sum_{\omega\in\Omega} |G_\omega| = \sum_{\delta\in\Delta} |{}^G\delta||G_\delta| \\ &= \sum_{\delta\in\Delta} |G : G_\delta||G_\delta| = \sum_{\delta\in\Delta} |G| = |\Delta||G|.\end{aligned}$$

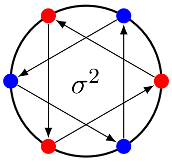
This proves the claim. $\square$

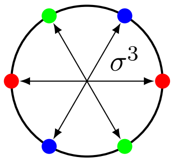
Example 6.8.

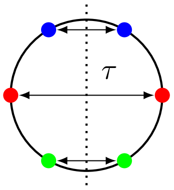
(i) Let G be a finite group acting transitively on Ω with $|\Omega| > 1$. According to Burnside's Lemma, 1 is the average number of fixed points of elements from G. On the other hand, $f(1) = |\Omega| > 1$. There must therefore always be fixed-point-free elements in G. This generalizes Theorem 2.2.

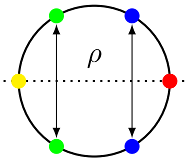
(ii) We want to count necklaces with six beads, where beads in three colors are available. Naively, there are initially 3^6 such necklaces, some of which are however identical. We arrange the necklace such that the beads form a regular hexagon. Rotation by $\pi/3$ will not change the necklaces. Likewise, we can rotate the necklace in space and thereby realize a reflection of the 6 vertices. Two necklaces are thus identical if and only if they lie in the same orbit under $G := D_{12}$. We apply Burnside's Lemma to the set Ω of the 3^6 necklaces.

Certainly $f(1) = 3^6$. A rotation $\sigma \in G$ by $\pi/3$ leaves only the three monochromatic necklaces fixed, i. e. $f(\sigma) = 3$. The rotation σ^2 by $2\pi/3$ leaves the monochromatic necklaces and the necklaces with alternating colors fixed. There are $f(\sigma^2) = 3^2$ of these. Analogously, one shows $f(\sigma^3) = 3^3$. Furthermore, $f(\sigma^4) = f(\sigma^{-2}) = 3^2$, $f(\sigma^5) = f(\sigma^{-1}) = 3$ as well as $\sigma^6 = 1$. Now let τ be one of the three reflections through two midpoints of sides. Then $f(\tau) = 3^3$. Finally, let ρ be one of the three reflections through two vertices. Then $f(\rho) = 3^4$.









According to Burnside's Lemma there are

$$\begin{aligned}\frac{1}{12}\left(3^6 + 2\cdot 3 + 2\cdot 3^2 + 3^3 + 3\cdot 3^3 + 3\cdot 3^4\right) &= \frac{1}{4}\left(3^4(3+1) + 3^2(1+3) + 2 + 6\right)\\ &= 81 + 9 + 2 = 92\end{aligned}$$

distinct necklaces.

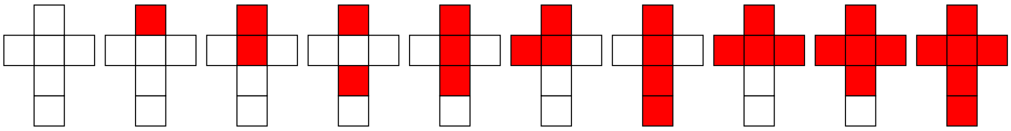
(iii) In how many ways can one color the six faces of a cube $W \subseteq \mathbb{R}^3$ if n colors are available? Naively: n^6. Rotations in space do not change W essentially. Reflections, however, do. We therefore seek the number of orbits under the rotation group of W.

Rotation axis	Angle	Number of rotations	Number of fixed points
opposite face midpoints	0°	1	n^6
opposite face midpoints	±90°	6	n^3
opposite face midpoints	180°	3	n^4
opposite edge midpoints	180°	6	n^3
space diagonal	±120°	8	n^2
		24	

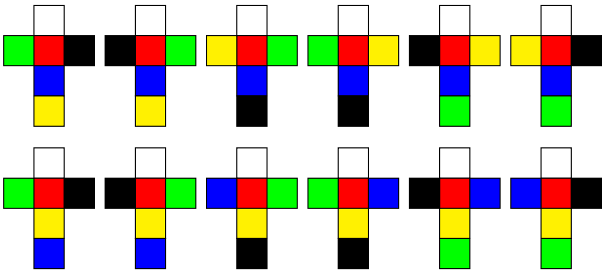
According to Burnside's Lemma, the number of colored cubes is given by

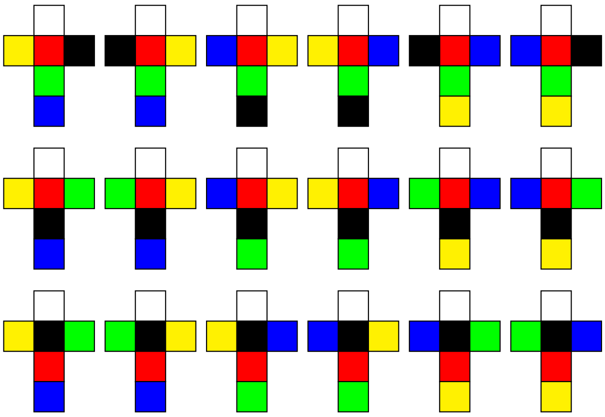
$$\frac{1}{24}\left(n^6 + 6n^3 + 3n^4 + 6n^3 + 8n^2\right) = \frac{n^2}{24}\left(n^4 + 3n^2 + 12n + 8\right).$$

For $n = 2$ one obtains the following ten cubes:



If one wants only cubes with pairwise distinct face colors, then one initially has $n(n-1)\dots(n-5)$ possibilities (variations without repetition). Since now every non-trivial rotation is fixed-point-free, Burnside's Lemma simplifies to $\frac{1}{24}n(n-1)\dots(n-5)$. For $n = 6$ one obtains the 30 MacMahon cubes:





(iv) There are

$$3^{14} \cdot 5^3 \cdot 7^2 \cdot 11 = 43.252.003.274.489.856.000$$

states of the $3 \times 3 \times 3$ Rubik's Cube, many of which can however be transformed into each other by spatial rotation and reflection. With Burnside's Lemma, the number reduces to

$$901.083.404.981.813.616$$

essentially distinct states.[10] With this, it was possible to show in 2010 that every state can be solved in at most 20 "moves" ("god's number", see `https://cube20.org/`).

(v) With Burnside's Lemma, one can also show that there are

$$5.472.730.538$$

essentially distinct (filled) 9×9 Sudokus.[11]

Remark 6.9. In the following, we refine Burnside's Lemma to count, for example, necklaces with a certain *value* (the bead colors should no longer necessarily be equivalent). For this, we consider an operation of G on Ω ("beads") and another finite set Δ ("colors"). Then G operates on $\Delta^\Omega = \{f\colon \Omega \to \Delta\}$ ("necklaces") by $({}^g f)(\omega) := f({}^{g^{-1}}\omega)$ for $g \in G$, $\omega \in \Omega$ and $f \in \Delta^\Omega$, because $({}^1 f)(\omega) = f(\omega)$ and

$$\left({}^g({}^h f)\right)(\omega) = ({}^h f)({}^{g^{-1}}\omega) = f\left({}^{h^{-1}}({}^{g^{-1}}\omega)\right) = f\left({}^{h^{-1}g^{-1}}\omega\right) = f\left({}^{(gh)^{-1}}\omega\right) = \left({}^{gh}f\right)(\omega)$$

for $g, h \in G$. For a function $w\colon \Delta \to \mathbb{N}_0$ ("value"), we define $w(f) := \sum_{\alpha\in\Omega} w(f(\alpha))$, $w_i := |w^{-1}(i)|$ for $i \in \mathbb{N}_0$ and

$$W(X) := \sum_{i=0}^{\infty} w_i X^i \in \mathbb{C}[X].$$

Let

$$(\Delta^\Omega)_k := \left\{f \in \Delta^\Omega : w(f) = k\right\}$$

("necklaces of value k"). Because of

$$w({}^g f) = \sum_{\alpha\in\Omega} w\big(({}^g f)(\alpha)\big) = \sum_{\alpha\in\Omega} w\big(f({}^{g^{-1}}\alpha)\big) = \sum_{\alpha\in\Omega} w(f(\alpha)) = w(f)$$

for $g \in G$, G also operates on $(\Delta^\Omega)_k$. Finally, let $(1^{z_1(g)}, 2^{z_2(g)}, \ldots)$ be the cycle type of g as an element of $\mathrm{Sym}(\Omega)$ (cf. Theorem 2.25).

---

[10] see [Sambale, Endliche Permutationsgruppen, Springer, 2017]

[11] see [Russell-Jarvis, Mathematics of Sudoku II, Mathematical Spectrum 39 (2006), 54–58]

Theorem 6.10 (Pólya). *With the notation from Remark 6.9, the number of orbits of G on $(\Delta^\Omega)_k$ is the coefficient of X^k in*

$$\frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^\infty W(X^i)^{z_i(g)}. \tag{6.1}$$

Proof. Let $f_k(g)$ be the number of fixed points of $g\in G$ on $(\Delta^\Omega)_k$. By Burnside's Lemma, we must show that

$$\sum_{k=0}^\infty\Big(\frac{1}{|G|}\sum_{g\in G}f_k(g)\Big)X^k=\frac{1}{|G|}\sum_{g\in G}\sum_{k=0}^\infty f_k(g)X^k$$

coincides with (6.1). It thus suffices to prove

$$\sum_{k=0}^\infty f_k(g)X^k=\prod_{i=1}^\infty W(X^i)^{z_i(g)}$$

for $g\in G$. Let $\Delta_1,\ldots,\Delta_s\subseteq\Omega$ be the orbits of g with lengths $l_1,\ldots,l_s$. Then $l_1,\ldots,l_s$ are also the cycle lengths of g and it follows that

$$\prod_{i=1}^\infty W(X^i)^{z_i(g)}=\prod_{i=1}^s(w_0+w_1X^{l_i}+w_2X^{2l_i}+\ldots)=\sum_{k=0}^\infty\sum_{\substack{(k_1,\ldots,k_s)\in\mathbb{N}_0^s\\k_1l_1+\ldots+k_sl_s=k}}w_{k_1}\ldots w_{k_s}X^k.$$

So we must verify

$$f_k(g)=\sum_{\substack{(k_1,\ldots,k_s)\in\mathbb{N}_0^s\\k_1l_1+\ldots+k_sl_s=k}}w_{k_1}\ldots w_{k_s}.$$

Every fixed point $f\in(\Delta^\Omega)_k$ of g is constant on Δ_i for each i. For the choice of $f(\delta)$ with $w(f(\delta))=k_i$, there are w_{k_i} possibilities. In this case,

$$k=w(f)=\sum_{i=1}^s\sum_{\delta\in\Delta_i}w(f(\delta))=k_1l_1+\ldots+k_sl_s.$$

This shows the claim. □

Example 6.11.

(i) We consider once again the necklaces with six beads of three colors (red, blue, and green). Let the red beads be worth 3 €, the blue ones 2 €, and the green ones 1 €. How many necklaces worth 12 € can be produced? Let $\Omega:=\{1,\ldots,6\}$, $\Delta:=\{r,b,g\}$ and $w(r):=3$, $w(b):=2$ and $w(g):=1$. Then $W(X)=X+X^2+X^3$ and we are looking for the number of orbits of $G:=D_{12}$ on $(\Delta^\Omega)_{12}$. The trivial element of G has cycle type (1^6). The rotation σ by $\pi/3$ has cycle type (6^1). Analogously, one obtains $z_3(\sigma^2)=2=z_3(\sigma^4)$ and $z_2(\sigma^3)=3$. For the reflections $\tau\in G$ through midpoints of sides, $z_2(\tau)=3$ and the remaining three reflections through vertices have cycle type $(1^2,2^2)$. Equation (6.1) now has the form

$$\begin{aligned}\frac{1}{12}\Big(&W(X)^6+2W(X^6)+2W(X^3)^2+W(X^2)^3+3W(X^2)^3+3W(X)^2W(X^2)^2\Big)\\&=\ldots=X^{18}+X^{17}+4X^{16}+6X^{15}+12X^{14}+13X^{13}\\&+18X^{12}+13X^{11}+12X^{10}+6X^9+4X^8+X^7+X^6\end{aligned}$$

Thus, there are 18 necklaces worth 12 €.

(ii) Pólya used Theorem 6.10 to determine the number of isomers of alcohols and paraffins.

Graph Theory

Remark. Graph theory could be described as the discretization of geometry. In contrast to geometry, we are not interested in angles, areas, or curvature behavior, but only in the relation in which objects stand to one another (adjacent, connected, etc.).

7 Eulerian Tours and Hamiltonian Cycles

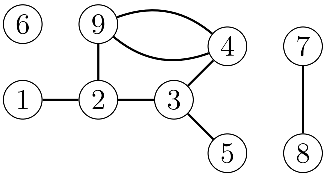
Definition 7.1.

- A *(multi)graph* $\Omega = (\Omega_E, \Omega_K)$ consists of a finite non-empty set Ω_E of *vertices* and a (multi)set $\Omega_K \subseteq \binom{\Omega_E}{2}$ of *edges*.[12] If Ω_K is a set, then Ω is called *simple*.
- Vertices $\alpha, \beta \in \Omega_E$ are called *adjacent*, if $\{\alpha, \beta\} \in \Omega_K$. More generally, vertices $\alpha, \beta \in \Omega_E$ are called *connected*, if a *path* $\alpha = \alpha_1, \ldots, \alpha_m = \beta \in \Omega_E$ with $\{\alpha_i, \alpha_{i+1}\} \in \Omega_K$ for $i = 1, \ldots, m-1$ exists ($m-1$ is the *length* of the path). This describes a partition on Ω_E, whose parts are called (*connected*) *components* of Ω.
- If there is only one component, then Ω is called *connected* and otherwise *disconnected.*

Remark 7.2. As usual, we will illustrate multigraphs using diagrams. On a computer, graphs can be described as a DOT file and visualized using Graphviz.

Example 7.3.

(i) The following multigraph Ω has vertex set $\Omega_E = \{1, \ldots, 9\}$.



Between 4 and 9 lies a double edge (we also call these multiple edges). Thus Ω is not simple. The vertices 1 and 5 are connected, but not adjacent. The components of Ω are $\{1, 2, 3, 4, 5, 9\}$, $\{6\}$ and $\{7, 8\}$.

(ii) The *trivial* graph $\mathcal{T}_n := \big(\{1, \ldots, n\}, \varnothing\big)$ without edges and the *complete* graph

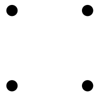
$$\mathcal{V}_n := (\{1, \ldots, n\}, \binom{\{1, \ldots, n\}}{2})$$

---

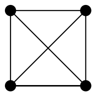
[12] In contrast to many books, we do not allow *loops*, i.e., edges of the form $\{\omega, \omega\}$.

with $n \geq 1$ vertices each.[13]

$\mathcal{T}_4$:



$\mathcal{V}_4$:

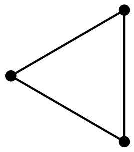


(iii) A *path graph* $\mathcal{G}_n := \big(\{1,\dots,n\}, \{\{i,i+1\} : i = 1,\dots,n-1\}\big)$ with $n \geq 2$ vertices.

$\mathcal{G}_5$:

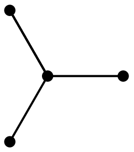
(iv) A *cycle* $\mathcal{K}_n := \big(\{1,\dots,n\}, \{\{i,i+1\} : i = 1,\dots,n-1\} \cup \{1,n\}\big)$ with $n \geq 3$ vertices (we also say *n-gon* to emphasize the number of vertices).

$\mathcal{K}_3 = \mathcal{V}_3$:



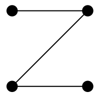
(v) A *star* $\mathcal{S}_n := (\{1,\dots,n\}, \{\{i,n\} : i = 1,\dots,n-1\})$ with $n \geq 4$ vertices.

$\mathcal{S}_4$:

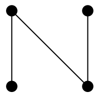


(vi) For every (simple) graph Ω there exists the *complementary* graph $\Omega^C = (\Omega_E, \binom{\Omega_E}{2} \setminus \Omega_K)$. Obviously $\mathcal{T}_n = \mathcal{V}_n^C$.

Ω :



Ω^C :

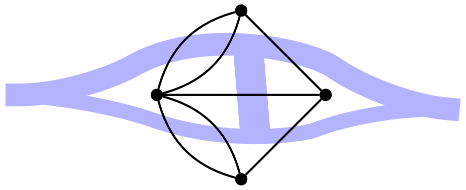


(vii) For multigraphs Ω and Δ, the (*disjoint*) *union* $\Omega \sqcup \Delta := (\Omega_E \sqcup \Delta_E, \Omega_K \sqcup \Delta_K)$ is also a graph with $|\Omega \sqcup \Delta| = |\Omega| + |\Delta|$. Obviously, every multigraph is the union of its components.

(viii) For induction purposes, we will often remove vertices or edges of a multigraph Ω. When removing vertices, the incident edges are also removed. Specifically, we define

$$\Omega \setminus \Delta := \begin{cases} (\Omega_E, \Omega_K \setminus \Delta) & \text{if } \Delta \subseteq \Omega_K, \\ (\Omega_E \setminus \Delta, \Omega_K \cap \binom{\Omega_E \setminus \Delta}{2}) & \text{if } \Delta \subseteq \Omega_E. \end{cases}$$

Remark 7.4 (Seven Bridges of Königsberg)**.** The following question, answered by Euler, marks the birth of graph theory: At that time, Königsberg was divided by seven bridges over the Pregel river; roughly like this:



Is it possible to organize a city tour in which each of the bridges is crossed exactly once?

---

[13] In the literature, the complete graph is usually denoted by K_n.

Definition 7.5. Let Ω be a multigraph.

- The *degree* $\deg(\alpha)$ of a vertex $\alpha \in \Omega_E$ is the number of edges (counted with multiplicities) that contain α. If all vertices have the same degree k, then Ω is called *k-regular.*
- A path $w = (\alpha_1, \ldots, \alpha_n) \in \Omega_E^n$ is called *closed*, if $\alpha_1 = \alpha_n$ (start = destination). A closed path w is called an *Eulerian tour*, if w uses every edge of Ω_K exactly once, i. e. the multisets $\{\{\alpha_1, \alpha_2\}, \ldots \{\alpha_{n-1}, \alpha_n\}\}$ and Ω_K are equal (vertices may appear in w any number of times).
- Ω is called *Eulerian*, if Ω possesses an Eulerian tour.

Lemma 7.6 (Handshaking Lemma)**.** *For every multigraph Ω, it holds that $\sum_{\alpha \in \Omega_E} \deg(\alpha) = 2|\Omega_K|$. In particular, the number of vertices with odd degree is even.*

Proof. Every edge $\{\alpha, \beta\}$ provides one contribution to $\deg(\alpha)$ and one contribution to $\deg(\beta)$. This shows the formula. The second statement follows from

$$|\{\alpha \in \Omega_E : \deg(\alpha) \text{ odd}\}| \equiv \sum_{\alpha \in \Omega_E} \deg(\alpha) \equiv 2|\Omega_K| \equiv 0 \pmod 2. \qquad \square$$

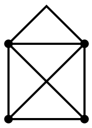
Remark 7.7. A disconnected multigraph Ω is Eulerian if and only if it has an Eulerian component Δ with $\Omega = \Delta \sqcup \mathcal{T}_n$ for some $n \geq 1$ (since every Eulerian tour takes place within one component). We can therefore concentrate on connected multigraphs.

Theorem 7.8 (EULER-HIERHOLZER)**.** *A connected multigraph is Eulerian if and only if all vertices have even degree.*

Proof. Let $w = (\alpha_1, \ldots, \alpha_n)$ be an Eulerian tour in Ω. Suppose α_1 is visited k times on w. Since w is closed, one "consumes" $2k$ distinct edges for this (one each for "arrival" and "departure"). Since all edges at α_1 must be used in this way, $\deg(\alpha_1) = 2k$ is an even number. Now obviously $(\alpha_2, \ldots, \alpha_n, \alpha_2)$ is also an Eulerian tour and $\deg(\alpha_2)$ must be even, etc.

Now let $\deg(\alpha)$ be even for all $\alpha \in \Omega_E$. Let $w = (\alpha_1, \ldots, \alpha_n)$ be a longest possible path in Ω in which each edge is used at most once. Since w cannot be extended, all edges at α_n have been used. If α_n is visited in between, i. e. $\alpha_n = \alpha_i$ for $1 < i < n$, then two edges of α_n are consumed. Since $\deg(\alpha_n)$ is even, $\alpha_1 = \alpha_n$ must hold, i. e. w is closed. Suppose that w is not an Eulerian tour. Then at least one edge, say $\{\alpha, \beta\}$, was not used in w. Since Ω is connected, we can choose this edge such that α belongs to w, wlog. $\alpha = \alpha_n$. However, this contradicts the observation that all edges at α_n have already been consumed. Thus w is an Eulerian tour and Ω is Eulerian. $\square$

Example 7.9. The Königsberg bridge problem is unsolvable because all vertices here have odd degree. Even if one waives the requirement of the Eulerian tour being closed, there can be no solution, because for that at most two vertices could have odd degree (namely the start and end vertices; if one connects these vertices with an additional edge, one obtains an Eulerian tour). For this reason, on the other hand, the *House of Santa Claus* can be drawn without lifting the pen and without drawing edges twice:



The two lower vertices with odd degree serve as start and end vertices.

Definition 7.10. Let Ω be a multigraph.

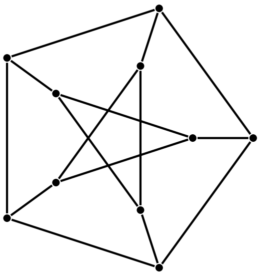
- A closed path of length ≥ 3 is called a *cycle*, if it visits every vertex at most once (obviously, every edge is then also visited at most once). The corresponding vertices thus form a $\mathcal{K}_n$.
- A cycle is called *Hamiltonian*, if it visits every vertex of Ω (exactly) once. One calls Ω *Hamiltonian*, if Ω possesses a Hamiltonian cycle.

Remark 7.11. Since every edge is used at most once in cycles, the existence of cycles does not depend on possible multiple edges. When considering the question of whether a graph is Hamiltonian, one can therefore restrict oneself to simple connected graphs.

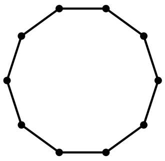
Example 7.12.

(i) Of course, the cycle graph $\mathcal{K}_n$ is Hamiltonian and likewise the complete graph $\mathcal{V}_n$ for $n \geq 3$, because it "contains" $\mathcal{K}_n$. On the other hand, $\mathcal{G}_n$ and $\mathcal{S}_n$ cannot be Hamiltonian, because they do not possess any cycles at all.

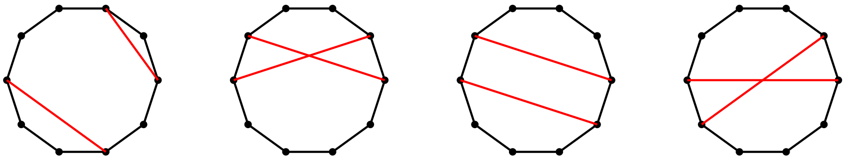
(ii) We consider the connected, 3-regular *Petersen graph* Ω:



Suppose Ω possesses a Hamiltonian cycle. By reshaping, this has the form



In the "interior" of the cycle, five further edges run, because Ω possesses a total of 15 edges ($2|\Omega_K| = \sum \deg(\alpha) = 3 \cdot 10$). Since every vertex has degree 3, the interior edges are pairwise disjoint. Through this condition, a triangle or quadrilateral always arises:



However, one easily checks that Ω possesses neither triangles nor quadrilaterals. Thus Ω is not Hamiltonian.

(iii) (Knight's tour problem) A knight stands as the only piece on a chessboard. Can the knight visit each of the 64 squares exactly once through successive moves and subsequently land back on its starting square? Thus, a Hamiltonian cycle in a graph with 64 vertices is sought.

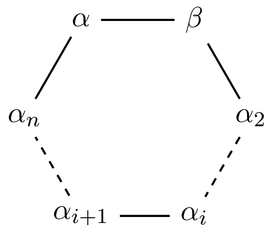
(iv) (Traveling salesman problem) A businessman wants to visit 10 cities. Due to traffic obstacles (mountains, lakes, borders, …), there is not a direct connection between all cities. Is there a route where the businessman visits every city exactly once and finally finds his way back to the home location? It becomes even more difficult if one wants to minimize the travel time (or fuel consumption). One then has to assign weights to the edges of the graph.

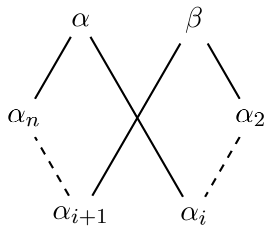
Theorem 7.13 (Ore). *Let Ω be a graph with at least three vertices. For any two distinct vertices $\alpha, \beta \in \Omega_E$, let $\{\alpha, \beta\} \in \Omega_K$ or $\deg(\alpha) + \deg(\beta) \geq |\Omega_E|$ hold. Then Ω is Hamiltonian.*

Proof. Let Ω be a counterexample with as many edges as possible, i.e., after adding any edge, let Ω no longer be a counterexample. Since the complete graph is Hamiltonian, there exist distinct $\alpha, \beta \in \Omega_E$ with $\{\alpha, \beta\} \notin \Omega_K$, thus $\deg(\alpha) + \deg(\beta) \geq |\Omega_E|$. The graph $\Omega' := (\Omega_E, \Omega_K \cup \{\{\alpha, \beta\}\})$ also satisfies the assumption and must be Hamiltonian according to our assumption. Furthermore, there is a Hamiltonian cycle $(\alpha_1, \ldots, \alpha_n, \alpha_1)$ that uses the edge $\{\alpha, \beta\}$, wlog. $\alpha_1 = \alpha$ and $\alpha_2 = \beta$. Let S_α be the set of neighbors of α in Ω and let

$$S_\beta := \{\alpha_i : i < n, \{\alpha_{i+1}, \beta\} \in \Omega_K\}.$$

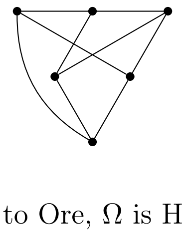
Then $\alpha \notin S_\alpha \cup S_\beta$ and therefore $|S_\alpha \cup S_\beta| < |\Omega_E| = n$. Because of $\{\alpha, \beta\} \notin \Omega_K$, every neighbor of β has the form α_{i+1} with $i < n$. This shows $|S_\alpha| + |S_\beta| = \deg(\alpha) + \deg(\beta) \geq n$. Thus there exists $\alpha_i \in S_\alpha \cap S_\beta$. But then $(\alpha, \alpha_i, \alpha_{i-1}, \ldots, \underbrace{\alpha_2}_{=\beta}, \alpha_{i+1}, \ldots, \alpha_n, \alpha)$ would be a Hamiltonian cycle in Ω.





□

Example 7.14. The graph Ω



has six vertices and is 3-regular. According to Ore, Ω is Hamiltonian.

Remark 7.15.

(i) The cycle graph $\mathcal{K}_5$ shows that the converse of Ore's Theorem is false. In contrast to Eulerian tours, it is difficult to decide when a graph is Hamiltonian. This question is even NP-complete, i. e. it is just as difficult as a series of well-known problems. The discovery of an algorithm with polynomial runtime would solve the Millennium Prize Problem "P = NP", for which a prize money of one million dollars is offered.

(ii) For the knight's tour problem, one finds explicit solutions on Wikipedia, but no abstract mathematical justification why a solution must exist (Ore's condition is not satisfied).

Definition 7.16. Let Ω be a multigraph with $\Omega_E = \{\alpha_1, \ldots, \alpha_n\}$. Let a_{ij} be the number of edges $\{\alpha_i, \alpha_j\} \in \Omega_K$. One calls $A(\Omega) := (a_{ij}) \in \mathbb{C}^{n\times n}$ the *adjacency matrix* of Ω.

Theorem 7.17. *Let Ω be a multigraph with $\Omega_E = \{\alpha_1, \ldots, \alpha_n\}$. The number of paths of length l from α_i to α_j is equal to the entry of $A(\Omega)^l$ at position (i, j).*

Proof. The paths of length $l = 1$ correspond exactly to the edges $\{a_i, a_j\} \in \Omega_K$. Therefore, the statement holds for $l = 1$. Now let $l \geq 2$ and $A(\Omega)^{l-1} = (b_{st})$. By induction on l, we can assume that b_{it} is the number of paths of length $l - 1$ from α_i to α_t. Each such path can be extended to α_j in a_{tj} different ways. Therefore, $\sum_{t=1}^n b_{it}a_{tj}$ is the number of paths of length l from α_i to α_j. This is also the entry of $A(\Omega)^{l-1}A(\Omega) = A(\Omega)^l$ at position (i, j). $\square$

Example 7.18. Let $v := (1, \ldots, 1) \in \mathbb{R}^n$. Then $vv^{\mathrm{t}} = n$ and $J := v^{\mathrm{t}}v \in \mathbb{R}^{n\times n}$ is the matrix containing only ones. For $k \geq 1$, $J^k = (v^{\mathrm{t}}v)^k = v^{\mathrm{t}}vv^{\mathrm{t}} \ldots v = n^{k-1}J$. For the complete graph, $A := A(\mathcal{V}_n) = J - 1_n$ holds. Since J commutes with 1_n, the binomial formula can be applied:

$$\begin{aligned} A^l &= \sum_{k=0}^{l} \binom{l}{k} (-1)^{l-k} J^k = (-1)^l 1_n + J \sum_{k=1}^{l} (-1)^{l-k} \binom{l}{k} n^{k-1} \\ &= (-1)^l 1_n + \frac{1}{n}((n-1)^l - (-1)^l)J. \end{aligned}$$

The number of paths of length l between two vertices α, β in $\mathcal{V}_n$ is therefore $\frac{1}{n}((n-1)^l - (-1)^l)$ if $\alpha \neq \beta$ and $\frac{n-1}{n}((n-1)^{l-1} + (-1)^l)$ if $\alpha = \beta$.

Remark 7.19. By construction, the adjacency matrix $A(\Omega)$ is real and symmetric. Therefore, all eigenvalues are real and $A(\Omega)$ is diagonalizable (principal axis transformation).

Theorem 7.20. *Let $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ be the eigenvalues (with multiplicities) of the adjacency matrix of a multigraph Ω. Then $\lambda_1^l + \ldots + \lambda_n^l$ is the number of all closed walks of length l in Ω.*

Proof. Let $A := A(\Omega)$. The number of (closed) walks of length l from α_i to α_i is the diagonal entry (i, i) of A^l according to Theorem 7.17. Therefore, the trace $\mathrm{tr}(A^l)$ is the number of all closed walks of length l. Let $S \in \mathrm{GL}(n, \mathbb{R})$ with $SAS^{-1} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) =: D$. Then

$$\mathrm{tr}(A^l) = \mathrm{tr}(S^{-1}D^lS) = \mathrm{tr}(D^lSS^{-1}) = \mathrm{tr}(D^l) = \lambda_1^l + \ldots + \lambda_n^l. \qquad \square$$

8 Neighbors and Connectivity

Remark 8.1. Suppose at a party any two people have exactly one common friend. We show that there must be a “host”, i.e., a person who is friends with everyone.

Theorem 8.2 (Friendship Theorem)**.** *Let Ω be a graph in which any two distinct vertices have exactly one common neighbor. Then there exists a vertex that is adjacent to all other vertices.*

Proof. Assume the opposite, i. e.. every vertex is not adjacent to at least one other vertex. From the assumption, it follows that Ω is connected. We first show that Ω is regular. Let $\alpha, \beta \in \Omega_E$ be distinct and non-adjacent. Let $\gamma_1, \ldots, \gamma_d$ be the neighbors of α. Wlog. let γ_2 be the common neighbor of α and β and let γ_1 be the common neighbor of α and γ_2. For $i = 2, \ldots, d$ let δ_i be the common neighbor of β and γ_i. In the case $\delta_i = \gamma_1$, α and β would have the two neighbors γ_1 and γ_2. In the case $\delta_i = \delta_j$ with $i \neq j$, γ_i and γ_j would be two common neighbors of δ_i and α. Thus β has at least the neighbors $\gamma_2, \delta_2, \ldots, \delta_d$. This shows $\deg(\beta) \geq d$. For reasons of symmetry, $d \geq \deg(\beta)$ also holds. Every vertex that is not adjacent to α therefore has degree d. Since γ_i for $i \neq 2$ are not adjacent to β, $\deg(\gamma_i) = d$ also holds for $i \neq 2$. Finally, by assumption, there exists a vertex ϵ that is not adjacent to γ_2. From $\deg(\epsilon) = d$ it follows that $\deg(\gamma_2) = d$. Therefore Ω is d-regular.

In particular, $\sum_{i=1}^{d} \deg(\gamma_i) = d^2$. In this sum, every $\beta \neq \alpha$ is counted exactly once, while α itself is counted exactly d times. It follows that $n = d^2 - d + 1$. Let A be the adjacency matrix of Ω. By assumption, every row of A has exactly d ones. Therefore $v = (1, \ldots, 1)$ is an eigenvector of A with eigenvalue d. From Theorem 7.17 we obtain

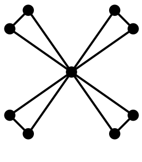
$$A^2 = \begin{pmatrix} d & 1 & \cdots & 1 \\ 1 & d & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & d \end{pmatrix} = (d-1)1_n + J,$$

where $J = (1)_{i,j}$ as in Example 7.18. The eigenvalues of J are n (with eigenvector v) and 0 with multiplicity $n - 1$ (since J has rank 1). Therefore $n + d - 1 = d^2$ and $d - 1$ are the eigenvalues of A^2 (with the same eigenvectors). Thus A has, besides d, eigenvalues of the form $\pm\sqrt{d-1}$. Let us say the multiplicity of $\sqrt{d-1}$ (resp. $-\sqrt{d-1}$) is r (resp. s). Then $r + s = n - 1$ holds. As is well known (linear algebra), $0 = \operatorname{tr}(A) = d + r\sqrt{d-1} - s\sqrt{d-1}$, so $r \neq s$ and $\sqrt{d-1} = \frac{d}{s-r}$. Since the square of a fractional rational number cannot be an integer (consider prime factorization), $s - r$ must be a divisor of d, say $m := \sqrt{d-1} \in \mathbb{N}$. Then

$$1 \equiv m^2 + 1 = d = (s-r)m \equiv 0 \pmod{m}$$

holds. This shows $m \leq 1$, $d \leq 2$ and $n = d^2 - d + 1 \leq 3$. Only the possibilities $\Omega \in \{\mathcal{V}_1, \mathcal{V}_3\}$ remain. Both, however, satisfy the assertion. ☐

Example 8.3. The graphs in the friendship theorem have the shape of windmills:



Theorem 8.4 (Erdős-Gallai). *For integers $d_1 \geq d_2 \geq \ldots \geq d_n \geq 0$, the following statements are equivalent:*

(1) There exists a graph with n vertices $e_1, \ldots, e_n$, such that $\deg(e_i) = d_i$ holds for $i = 1, \ldots, n$.

(2) $\sum_{i=1}^{n} d_i$ is even and for $k = 1, \ldots, n$ it holds that

$$\sum_{i=1}^{k} d_i \leq k(k-1) + \sum_{i=k+1}^{n} \min\{d_i, k\}.$$

Proof (TRIPATHI-VENUGOPALAN-WEST).

(1)⇒(2): Let Ω be a graph with the given vertex degrees. From the handshaking lemma it follows that $\sum d_i = 2|\Omega_K| \equiv 0 \pmod 2$. Let $1 \le k \le n$ and s be the number of edges between $e_1, \dots, e_k$. Then $s \le k(k-1)/2$ and $-2s + \sum_{i=1}^k d_i$ is the number of edges from $e_1, \dots, e_k$ to $e_{k+1}, \dots, e_n$. Since the graph is simple, at each vertex e_i with $i > k$ at most $\min\{d_i, k\}$ such edges can arrive. This shows $-2s + \sum_{i=1}^k d_i \le \sum_{i=k+1}^n \min\{d_i, k\}$. It follows

$$\sum_{i=1}^{k} d_i \le 2s + \sum_{i=k+1}^{n} \min\{d_i, k\} \le k(k-1) + \sum_{i=k+1}^{n} \min\{d_i, k\}.$$

(2)⇒(1): We start with $\Omega = \mathcal{T}_n$ and successively add edges until (1) is satisfied. In the case $d_1 = 0$ we are already finished. Now let $d_1 > 0$. Inductively we assume that Ω has the following properties:

(a) $\deg(e_i) = d_i$ for $i = 1, \dots, r-1$, $\deg(e_r) < d_r$ and $\deg(e_i) \le d_i$ for $i = r+1, \dots, n$.

(b) There are no edges between $e_{r+1}, \dots, e_n$.

We will step by step increase $\deg(e_r)$ and r.

Step 1: For i with $\deg(e_i) < d_i$, $\{e_r, e_i\} \in \Omega_K$.
If $\{e_r, e_i\}$ is not an edge, then add it. This increases $\deg(e_r)$ and $\deg(e_i)$ by 1 each. In the case $\deg(e_r) = d_r$ we can increase r, so that (a) and (b) continue to hold.

Step 2: e_r is adjacent to $e_1, \dots, e_{r-1}$.
Assume that e_r is not adjacent to e_i with $i < r$. Because of $\deg(e_i) = d_i \ge d_r > \deg(e_r)$ there exists a neighbor f of e_i that is not adjacent to e_r. In the case $d_r - \deg(e_r) \ge 2$ we can replace the edge $\{e_i, f\}$ by the edges $\{e_i, e_r\}$ and $\{e_r, f\}$. Thereby $\deg(e_r)$ is increased by 2, while $\deg(e_i)$ and $\deg(f)$ remain the same. Now let $d_r - \deg(e_r) = 1$. By assumption and Lemma 7.6 we have

$$1 + \sum_{i=r+1}^{n} (d_i - \deg(e_i)) = \sum_{i=1}^{n} d_i - \sum_{i=1}^{n} \deg(e_i) \equiv 0 \pmod 2.$$

Therefore there exists $k > r$ with $\deg(e_k) < d_k$. By Step 1, e_k is adjacent to e_r. We replace the edges $\{e_r, e_k\}$, $\{e_i, f\}$ by $\{e_i, e_r\}$, $\{e_r, f\}$. In doing so, $\deg(e_r)$ is increased by 1, $\deg(e_k)$ is decreased by 1 and $\deg(e_i)$ as well as $\deg(f)$ remain the same.

Step 3: For all $k > r$, $\deg(e_k) = \min\{r, d_k\}$.
Assume $\deg(e_k) \ne \min\{r, d_k\}$ for some $k > r$. By property (b), e_k can only be adjacent to $e_1, \dots, e_r$. This shows $\deg(e_k) \le r$. Because of $\deg(e_k) \le d_k$ we thus have $\deg(e_k) < \min\{r, d_k\}$. By Step 1, e_k and e_r are adjacent. Because of $\deg(e_k) < r$ there exists an $i < r$ such that e_k is not adjacent to e_i. Because of $\deg(e_i) = d_i \ge d_r > \deg(e_r)$ there exists, as in the previous step, a neighbor f of e_i that is not adjacent to e_r. Since e_r is a neighbor of e_i (Step 2), we can choose $f \ne e_r$. We now replace $\{e_i, f\}$ by $\{e_r, f\}$ and $\{e_i, e_k\}$. This increases $\deg(e_r)$ and $\deg(e_k)$ by 1, while $\deg(e_i)$ and $\deg(f)$ remain the same. Because of $i < r$, property (b) is also preserved.

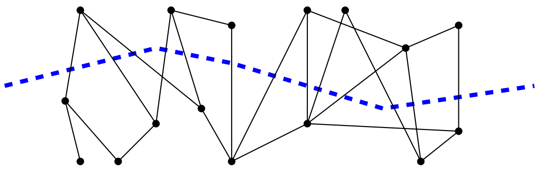
Step 4: For $1 \le i < j < r$, e_i and e_j are adjacent.
Assume e_i and e_j are not adjacent. Because of $\deg(e_i), \deg(e_j) > \deg(d_r)$ there exist neighbors f of e_i and g of e_j such that e_r is adjacent to neither f nor g (the case $f = g$ is allowed). We replace $\{e_i, f\}$, $\{e_j, g\}$ by $\{e_i, e_j\}$, $\{e_r, f\}$. This increases $\deg(e_r)$ and decreases $\deg(g)$ by 1 each, while $\deg(e_i)$, $\deg(e_j)$ and $\deg(f)$ remain the same (except in the case $f = g$).

Step 5: $\deg(e_r) = d_r$.
By Step 2 and 4, $e_1, \ldots, e_r$ are pairwise adjacent. From property (b) and Step 3 it follows

$$\sum_{i=1}^{r} d_i \leq r(r-1) + \sum_{i=r+1}^{n} \min(r, d_i) = \sum_{i=1}^{r} \deg(e_i) \leq \sum_{i=1}^{r} d_i$$

and $\deg(e_r) = d_r$. We can now increase r and repeat the process. □

Example 8.5. At the German-Austrian border, toll stations are to be installed on all connecting roads. Since different paths can overlap, it is not immediately clear how many toll stations are needed.



Definition 8.6. A multigraph Ω with more than k vertices is called *k-connected*, if Ω is (still) connected after removing $k-1$ arbitrary vertices. The *connectivity* $k(\Omega)$ of Ω is the largest number $k \geq 0$ such that Ω is k-connected.

Remark 8.7.

(i) As usual, multiple edges do not affect the connectivity. We will therefore restrict ourselves to simple graphs.

(ii) Every graph is 0-connected. The 1-connected graphs are exactly the connected graphs except for $\mathcal{T}_1$.

(iii) The only k-connected graph with $k+1$ vertices is $\mathcal{V}_{k+1}$.

Example 8.8. One easily shows

Ω	$\mathcal{T}_n$	$\mathcal{V}_n$	$\mathcal{V}_{k,l}$	$\mathcal{G}_n$	$\mathcal{K}_n$	$\mathcal{S}_n$
$k(\Omega)$	0	$n-1$	$\min\{k,l\}$	1	2	1

Definition 8.9. Let Ω be a graph and $\Delta, \Gamma \subseteq \Omega_E$.

- A path $(\alpha_1, \ldots, \alpha_k)$ in Ω is called a Δ-Γ-*path*, if $\alpha_1 \in \Delta$ and $\alpha_k \in \Gamma$ ($k = 1$ is allowed). Two paths $(\alpha_1, \ldots, \alpha_k)$ and $(\beta_1, \ldots, \beta_l)$ are called *internally disjoint* (or *cross-free*), if they have no vertices in common except for the start and end, i.e., $\{\alpha_2, \ldots, \alpha_{k-1}\} \cap \{\beta_2, \ldots, \beta_{l-1}\} = \varnothing$.
- A Δ-Γ-*separator* is a subset $\Lambda \subseteq \Omega_E$ such that there are no Δ-Γ-paths in $\Omega \setminus \Lambda$. In the case $\Delta = \{\delta\}$ and $\Gamma = \{\gamma\}$, we speak of δ-γ-separators.

Remark 8.10.

(i) Disjoint paths are obviously crossing-free.

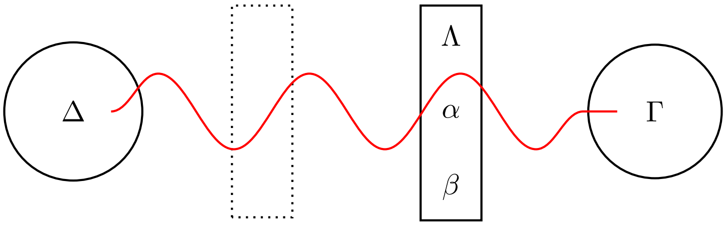
(ii) Both Δ and Γ are Δ-Γ-separators. Conversely, every Δ-Γ-separator must contain $\Delta \cap \Gamma$.

(iii) For $\delta \neq \gamma$ and every δ-γ-separator $\Lambda \subseteq \Omega_E \setminus \{\delta, \gamma\}$, it holds that $k(\Omega) \leq |\Lambda|$, because $\Omega \setminus \Lambda$ is disconnected. Conversely, there exists $\Lambda \subseteq \Omega_E$ with $|\Lambda| = k(\Omega)$ such that $\Omega \setminus \Lambda$ is disconnected. For non-adjacent vertices $\delta, \gamma \in \Omega_E \setminus \Lambda$, Λ is a δ-γ-separator.

Theorem 8.11 (Menger). *Let Ω be a graph and $\Delta, \Gamma \subseteq \Omega_E$. The minimum cardinality of a Δ-Γ-separator is the maximum number of pairwise disjoint Δ-Γ-paths in Ω.*

Proof. Let Λ be a minimal Δ-Γ-separator and $k := |\Lambda|$. Since every Δ-Γ-path uses a vertex from Λ, there can be at most k pairwise disjoint Δ-Γ-paths in Ω. For the reverse inequality, we argue by induction on $|\Omega_K|$. In the case $\Omega_K = \varnothing$, $\Lambda = \Delta \cap \Gamma$ and the Δ-Γ-paths in Ω have the form $\{\delta\}$ with $\delta \in \Delta \cap \Gamma$. So let $a := \{\alpha, \beta\} \in \Omega_K$. By removing a and merging α and β, one obtains a graph Ω' in which $\alpha = \beta$ holds. Suppose that Ω (and thus also Ω') does not possess k pairwise disjoint Δ-Γ-paths. By induction, there exists a Δ-Γ-separator $\Lambda' \subseteq \Omega'_E$ with $|\Lambda'| < k$. Here $\alpha = \beta \in \Lambda'$ holds, because otherwise Λ' would also be a Δ-Γ-separator in Ω. Thus $\Lambda' \cup \{\alpha, \beta\}$ is a k-element Δ-Γ-separator in Ω. We can therefore set $\Lambda = \Lambda' \cup \{\alpha, \beta\}$ (in particular, Λ now contains adjacent vertices).

We now examine $\Omega' := \Omega \setminus \{a\}$. Since every Δ-Γ-path in Ω passes through Λ, every Δ-Λ-separator in Ω' is also a Δ-Γ-separator in Ω (note: $\alpha, \beta \in \Lambda$).



Every such separator thus consists of at least k vertices. By induction, there are k pairwise disjoint Δ-Λ-paths in Ω'. For reasons of symmetry, Ω' also possesses k pairwise disjoint Λ-Γ-paths. Since Λ is a Δ-Γ-separator in Ω, these paths can be joined to form k pairwise disjoint Δ-Γ-paths in Ω. Contradiction. ☐

Corollary 8.12. [14] *A graph is k-connected if and only if there are at least k internally vertex-disjoint paths between any two distinct vertices.*

Proof. Let Ω be a graph. If there are at least k internally disjoint paths between any two distinct vertices in Ω, then $|\Omega_E| > k$ and $\Omega \setminus \Lambda$ is connected for all $\Lambda \subseteq \Omega_E$ with $|\Lambda| < k$. Thus Ω is k-connected.

Conversely, let Ω be k-connected and $\alpha, \beta \in \Omega_E$ be distinct. Suppose there are fewer than k internally disjoint paths between α and β. First, assume $a := \{\alpha, \beta\} \notin \Omega_K$. Let $\Omega' := \Omega \setminus \{\alpha, \beta\}$, Δ be the set of neighbors of α and Γ be the set of neighbors of β. Disjoint Δ-Γ-paths in Ω' correspond to internally disjoint α-β-paths in Ω. According to Menger, there exists a Δ-Γ-separator $\Lambda \subseteq \Omega'_E$ with fewer than k elements. But then α and β would not be connected in $\Omega \setminus \Lambda$. This contradiction shows $a \in \Omega_K$. In $\Omega' := \Omega \setminus \{a\}$ there are at most $k-2$ internally disjoint α-β-paths. As before, Menger's theorem provides an α-β-separator $\Lambda \subseteq \Omega_E \setminus \{\alpha, \beta\}$ in Ω' with at most $k-2$ elements. Because $|\Omega_E| > k$, there exists a vertex $\gamma \notin \Lambda \cup \{\alpha, \beta\}$. Now Λ is an α-γ-separator or a β-γ-separator in Ω', wlog. we assume the first case. Then $\Lambda \cup \{\beta\}$ is an α-γ-separator in Ω. Because $|\Lambda \cup \{\beta\}| = k - 1$, this contradicts $k(\Omega) \geq k$. ☐

---

[14] Called the *global* Menger's theorem in the literature.

9 Isomorphic Graphs

Remark 9.1. In this section we consider exclusively simple graphs Ω. The number of all graphs with $\Omega_E = \{1,\ldots,n\}$ is $|2^{\binom{\Omega_E}{2}}| = 2^{\binom{n}{2}}$. However, many of these graphs look the same. For example, there are six graphs with four vertices and one edge.

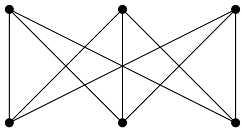
Definition 9.2. Graphs Ω and Δ are called *isomorphic*, if a bijection $\sigma\colon \Omega_E \to \Delta_E$ with

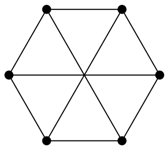
$$\{x,y\} \in \Omega_K \iff \{\sigma(x),\sigma(y)\} \in \Delta_K$$

exists. We then write $\Omega \cong \Delta$.

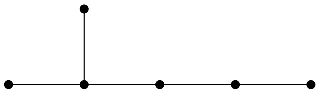
Remark 9.3. As with groups or vector spaces, the isomorphism of graphs is an equivalence relation. Isomorphic graphs differ only by the labeling of the vertices and therefore have the same properties (number of components, multiset of vertex degrees, etc.). Whether two given graphs are isomorphic is one of the few questions for which it is not yet known how difficult they are.

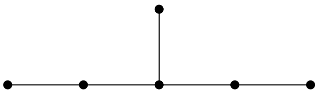
Example 9.4. The graphs





are isomorphic, while





are not isomorphic (although the multiset of vertex degrees coincides).

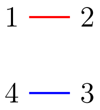
Definition 9.5. Let $g(n)$ be the number of isomorphism classes of graphs with n vertices.

Remark 9.6. To determine $g(n)$, it suffices to consider the set Γ_n of all graphs Ω with $\Omega_E = \{1,\ldots,n\} =: N$. Thus $g(n) \le |\Gamma_n| = 2^{\binom{n}{2}}$. We count the isomorphism classes in Γ_n. For this, we consider that S_n acts on $\binom{N}{2}$ by

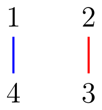
$$^{\sigma}\{a,b\} := \{\sigma(a),\sigma(b)\}$$

for $\sigma \in S_n$ and $\{a,b\} \in \binom{N}{2}$. This induces an action of S_n on $2^{\binom{N}{2}}$. Therefore S_n also acts on Γ_n by $^{\sigma}\Omega := (N, {}^{\sigma}\Omega_K)$.

Example: $\Omega :$



$\xrightarrow{\sigma = (1,2,3)}$ $^{\sigma}\Omega :$



Two graphs in Γ_n are isomorphic if and only if they lie in the same orbit of S_n. To calculate the number of these orbits, we use Burnside's Lemma. For this, we must count how many fixed points $\sigma \in S_n$ has on Γ_n. Let $\widetilde{\sigma}$ be the permutation on $\binom{N}{2}$ induced by σ. For $\sigma = (1,2,3)$ as above, for example,

$$\widetilde{\sigma} = \big(\{1,2\},\{2,3\},\{1,3\}\big)\big(\{1,4\},\{2,4\},\{3,4\}\big).$$

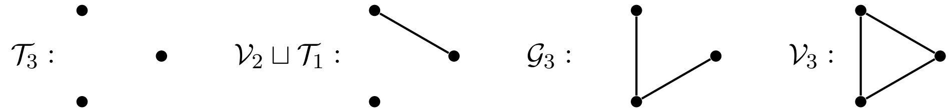
A graph $\Omega \in \Gamma_n$ remains fixed under σ if and only if Ω_K is the union of orbits of $\widetilde{\sigma}$. The number $f(\sigma)$ of these fixed points is thus $2^{z(\widetilde{\sigma})}$, where $z(\widetilde{\sigma})$ is the number of cycles of $\widetilde{\sigma}$. Burnside's Lemma shows

$$g(n) = \frac{1}{n!}\sum_{\sigma \in S_n} 2^{z(\widetilde{\sigma})}. \tag{9.1}$$

It is easy to see that $f(\sigma)$ only depends on the cycle type of σ (cf. Exercise 36). Furthermore, we know from Theorem 2.25 how many elements of each cycle type exist. Thus, in (9.1) one "only" needs to sum over the partitions of n. Nevertheless, no explicit formula for $g(n)$ is known. It holds that $g(50) \approx 1.9 \cdot 10^{304}$ (see `https://oeis.org/A000088`).

Example 9.7.

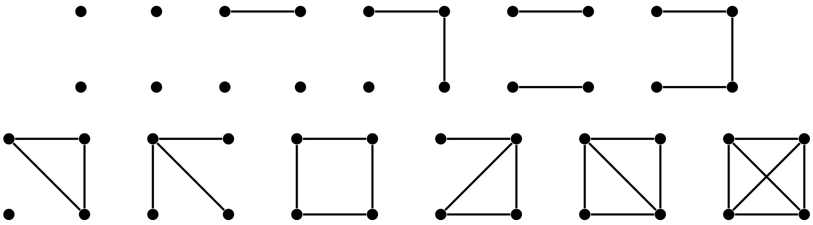
(i) Certainly $g(1) = 1$, $g(2) = 2$ and $g(3) = 4$:



(ii) We consider the case $n = 4$ in Remark 9.6. Obviously $\sigma = 1$ has exactly $z(\widetilde{\sigma}) = \binom{4}{2} = 6$ cycles (of length 1) on $\binom{N}{2}$, i.e. $f(\sigma) = 2^6$. Furthermore $\sigma = (1,2)$ has the cycles $(\{1,2\})$, $(\{3,4\})$, $(\{1,3\},\{2,3\})$ and $(\{1,4\},\{2,4\})$ on $\binom{N}{2}$ and it follows $f(\sigma) = 2^4$. Analogously one shows $f((1,2,3)) = 2^2$, $f((1,2)(3,4)) = 2^4$ and $f((1,2,3,4)) = 2^2$. According to Theorem 2.25 there are six permutations of cycle type (2), eight of type (3), three of type (2^2) and six of type (4). With (9.1) one obtains

$$\begin{aligned} g(4) &= \frac{1}{4!}\big(f(1) + 6f((1,2)) + 8f((1,2,3)) + 3f((1,2)(3,4)) + 6f((1,2,3,4))\big) \\ &= \frac{1}{24}\big(2^6 + 6\cdot 2^4 + 8\cdot 2^2 + 3\cdot 2^4 + 6\cdot 2^2\big) = \frac{1}{24}\big(2^5(2+3+1) + 3\cdot 2^3(2+1)\big) = 11. \end{aligned}$$

Representatives of these graphs are:



(iii) With Pólya's theorem we can count the graphs with a given number of vertices and edges more precisely. For this, let $\Lambda := \binom{N}{2}$ and $\Delta := \{0,1\}$. Every graph $\Omega \in \Gamma_n$ corresponds to a mapping $f \in \Delta^\Lambda$ with $f(a) = 1$ if a is an edge of Ω and 0 otherwise. As in (i), S_n acts on Δ^Λ. With the notation from Theorem 6.10, let $w\colon \Delta \to \mathbb{N}_0$, $w(0) = 0$, $w(1) = 1$. Then $W(X) = 1 + X$. The number of orbits of S_n on $(\Delta^\Lambda)_k$ is exactly the number of graphs with n vertices and k edges up to isomorphism. With the calculations from (i) one obtains the polynomial

$$\begin{aligned}\frac{1}{4!}\sum_{\sigma\in S_4}\prod_{i=1}^{4}(1+X^i)^{z_i(\widetilde{\sigma})} &= \frac{1}{24}\Big((1+X)^6+6(1+X)^2(1+X^2)^2 \\ &\quad +8(1+X^3)^2+3(1+X)^2(1+X^2)^2+6(1+X^2)(1+X^4)^1\Big) \\ &= \ldots = X^6+X^5+2X^4+3X^3+2X^2+X+1.\end{aligned}$$

There are thus exactly three graphs with four vertices and three edges up to isomorphism ($\mathcal{G}_3 \sqcup \mathcal{T}_1$, $\mathcal{S}_4$, $\mathcal{S}_4^C$, see figure above). The symmetry in the coefficients is explained by the bijection $\Omega \mapsto \Omega^C$.

Definition 9.8. The *automorphism group* $\operatorname{Aut}(\Omega)$ of a graph Ω consists of the isomorphisms from Ω to itself, i. e.

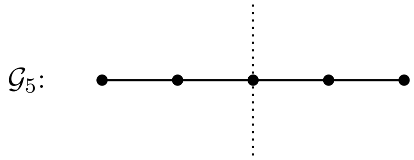
$$\operatorname{Aut}(\Omega) := \big\{\sigma \in \operatorname{Sym}(\Omega_E) : \{x,y\} \in \Omega_K \Longleftrightarrow \{\sigma(x),\sigma(y)\} \in \Omega_K\big\} \le \operatorname{Sym}(\Omega_E).$$

In the case $|\operatorname{Aut}(\Omega)| \neq 1$, Ω is called *symmetric* and otherwise *asymmetric*.

Example 9.9.

(i) For every graph Ω, $\operatorname{Aut}(\Omega) = \operatorname{Aut}(\Omega^C)$ holds. In particular, $\operatorname{Aut}(\mathcal{T}_n) = \operatorname{Aut}(\mathcal{V}_n) \cong S_n$.

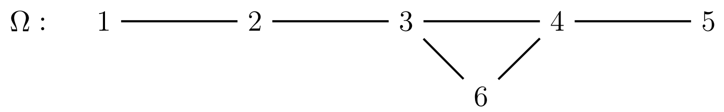
(ii) For $n \geq 2$, $\operatorname{Aut}(\mathcal{G}_n)$ is a cyclic group of order 2, where the non-trivial automorphism describes a reflection across the center of the path graph.



(iii) For $n \geq 3$, $\operatorname{Aut}(\mathcal{K}_n) \cong D_{2n}$ holds, because every automorphism must preserve the distances of the vertices and thus corresponds to a symmetry of the regular n-gon (cf. Example 6.3).

(iv) For $n \geq 4$, $\mathcal{S}_n^C \cong \mathcal{T}_1 \sqcup \mathcal{V}_{n-1}$ and $\operatorname{Aut}(\mathcal{S}_n) \cong S_{n-1}$ hold.

(v) We examine the automorphism group of the graph



Every $\alpha \in \operatorname{Aut}(\Omega)$ must permute the two vertices 3 and 4 of degree 3, i. e. $\{\alpha(3),\alpha(4)\} = \{3,4\}$. The only common neighbor of 3 and 4 must therefore remain fixed, so $\alpha(6) = 6$. Besides 6, only vertex 2 has degree 2. This shows $\alpha(2) = 2$. It now follows easily that $\alpha = \mathrm{id}$ and $\operatorname{Aut}(\Omega) = \{\mathrm{id}\}$, i. e. Ω is asymmetric. This is the smallest asymmetric graph with at least two vertices. Surprisingly, however, almost all graphs are asymmetric.

Theorem 9.10 (Erdős-Rényi)**.** *It holds that*

$$g(n) \sim \frac{1}{n!}2^{\binom{n}{2}}.$$

In particular, almost all graphs are asymmetric.

Proof. Let $m := \binom{n}{2}$. With (9.1) from Remark 9.6 we must show

$$\lim_{n\to\infty} \frac{1}{2^m} \sum_{\sigma\in S_n} 2^{z(\widetilde{\sigma})} = 1.$$

In the following, let n therefore always be “large enough”.

Let $2 \le k < n$ and $\Sigma_k \subseteq S_n$ be the set of permutations with at most k fixed points. For $\sigma \in \Sigma_k$, $\widetilde{\sigma}$ then has at most $\binom{k}{2} + \frac{n-k}{2}$ fixed points (where equality only holds if σ is a disjoint product of $\frac{n-k}{2}$ transpositions). All other orbits of $\widetilde{\sigma}$ have length at least 2. Thus

$$\begin{aligned} z(\widetilde{\sigma}) &\le m - \frac{1}{2}\Big(m - \binom{k}{2} - \frac{n-k}{2}\Big) = m - \frac{n(n-1) - k(k-1) - n + k}{4} \\ &= m - \frac{n(n-2) - k(k-2)}{4} \le m - \frac{n(n-k)}{4} \qquad \text{(replace } k(k-2) \text{ by } n(k-2)\text{)}. \end{aligned}$$

For $1 \neq \sigma \in S_n \setminus \Sigma_k$ we have $\sigma \in \Sigma_{n-2}$ and

$$\begin{aligned} z(\widetilde{\sigma}) &\le m - \frac{1}{2}\Big(m - \binom{n-2}{2} - 1\Big) \\ &= m - \frac{n(n-1) - (n-2)(n-3) - 2}{4} = m - n + 2. \end{aligned}$$

Because of $|\Sigma_k| \le n! \le n^n$ and $|S_n \setminus \Sigma_k| \le \binom{n}{k}(n-k)! = \frac{n!}{k!} \le n^{n-k}$ it follows that

$$\begin{aligned} \sum_{\sigma\in S_n} 2^{z(\widetilde{\sigma})} &= 2^{z(1)} + \sum_{\sigma\in\Sigma_k} 2^{z(\widetilde{\sigma})} + \sum_{1\neq\sigma\in S_n\setminus\Sigma_k} 2^{z(\widetilde{\sigma})} \\ &\le 2^m + n^n 2^{m-n(n-k)/4} + n^{n-k} 2^{m-n+2}. \end{aligned}$$

We divide both sides by 2^m. It then suffices to show that $n^n 2^{-n(n-k)/4}$ and $n^{n-k}2^{2-n}$ tend to 0 if one chooses k appropriately. We take the logarithm to the base 2 and then set $k = n - 5[\log n]$ (which is allowed for large n). Then

$$\begin{aligned} n\log(n) - \frac{n(n-k)}{4} &\longrightarrow -\frac{n\log(n)}{4} \longrightarrow -\infty \\ (n-k)\log(n) + 2 - n &\longrightarrow 5\log(n)^2 - n \longrightarrow -\infty \end{aligned}$$

for $n \to \infty$.

For the second assertion, let $t(n)$ be the number of asymmetric graphs with n vertices up to isomorphism. The orbits of these graphs under the above operation then have length $n!$. All other orbits have length at most $n!/2$. This shows

$$2^m \le n!t(n) + \frac{n!}{2}(g(n) - t(n)) = \frac{n!}{2}\big(g(n) + t(n)\big).$$

We divide by $g(n)n!$ and obtain

$$1 = \lim_{n\to\infty} \frac{2^m}{g(n)n!} \le \frac{1}{2}\Big(1 + \lim_{n\to\infty}\frac{t(n)}{g(n)}\Big) \le 1.$$

Thus $\frac{t(n)}{g(n)}$ tends to 1, i. e. almost all graphs are asymmetric. $\square$

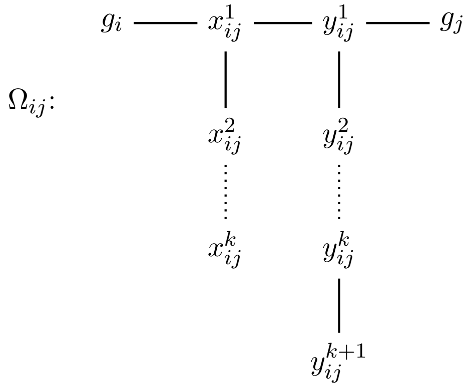
Example 9.11. The probability that a randomly chosen graph with 20 vertices is asymmetric is already

$$\frac{t(20)}{g(20)} \geq \frac{2^{191}}{g(20)20!} - 1 > 0{,}998$$

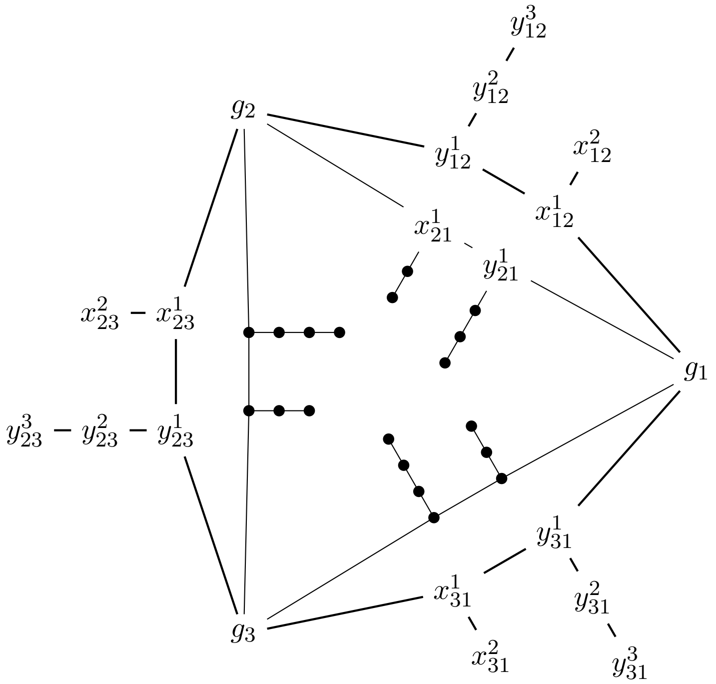
(see `https://oeis.org/A000088`).

Theorem 9.12 (Frucht)**.** *Every finite group is the automorphism group of a graph.*

Proof. For a given group $G = \{1 = g_1, \ldots, g_n\}$, we first consider the trivial graph with vertex set G. Between each pair of distinct vertices (g_i, g_j), we insert the following graph, where $g_k = g_i^{-1}g_j$:



Let Ω be the resulting graph. For $n = 3$, one obtains for example



For $g \in G$ let $\sigma \in S_n$ with $gg_i = g_{\sigma(i)}$ for $i = 1, \ldots, n$. Because of $g_{\sigma(i)}^{-1}g_{\sigma(j)} = g_i^{-1}g^{-1}gg_j = g_i^{-1}g_j$, the map $\alpha_g \in \mathrm{Sym}(\Omega_E)$ with

$$\alpha_g(g_i) := g_{\sigma(i)}, \qquad \alpha_g(x_{ij}^l) := x_{\sigma(i)\sigma(j)}^l, \qquad \alpha_g(y_{ij}^l) := y_{\sigma(i)\sigma(j)}^l$$

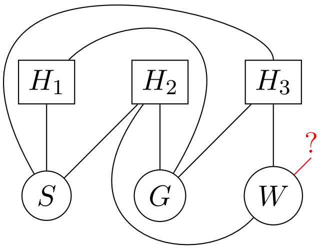
is an automorphism on Ω. Because of $\alpha_{gh}(g_i) = ghg_i = \alpha_g(\alpha_h(g_i))$ for $g, h, g_i \in G$, $\Gamma\colon G \to \operatorname{Aut}(\Omega)$, $g \mapsto \alpha_g$ is an injective group homomorphism.

Now let $\alpha \in \operatorname{Aut}(\Omega)$ be arbitrary and wlog. $n \geq 3$. Then the vertices g_i have degree $2(n-1) > 3$, while the vertices x_{ij}^l and y_{ij}^l have degree at most 3. Therefore, there exists a $\sigma \in S_n$ with $\alpha(g_i) = g_{\sigma(i)}$ for $i = 1, \ldots, n$. For $i \neq j$, α maps the line g_i—x_{ij}^1—y_{ij}^1—g_j to $g_{\sigma(i)}$—$x_{\sigma(i)\sigma(j)}^1$—$y_{\sigma(i)\sigma(j)}^1$—$g_{\sigma(j)}$ or to $g_{\sigma(i)}$—$y_{\sigma(j)\sigma(i)}^1$—$x_{\sigma(j)\sigma(i)}^1$—$g_{\sigma(j)}$. Obviously, α must then map the entire graph Ω_{ij} to $\Omega_{\sigma(i)\sigma(j)}$ or to $\Omega_{\sigma(j)\sigma(i)}$. However, the second case is excluded, because $\alpha(x_{ij}^k) = y_{\sigma(j)\sigma(i)}^k$ and $\alpha(y_{ij}^{k+1}) = x_{\sigma(j)\sigma(i)}^{k+1}$ with $g_k = g_i^{-1}g_j$ cannot both have degree 1. Thus $\alpha(\Omega_{ij}) = \Omega_{\sigma(i)\sigma(j)}$ and $g_{\sigma(i)}^{-1}g_{\sigma(j)} = g_i^{-1}g_j$ for all $i \neq j$. This shows $\alpha(g_i) = g_{\sigma(i)} = g_{\sigma(1)}g_i$ for $i = 1, \ldots, n$. It follows that $\alpha = \alpha_{g_{\sigma(1)}}$ and Γ is surjective. Thus $\operatorname{Aut}(\Omega) \cong G$ holds. ☐

Remark 9.13. The graph constructed in the proof is obviously not minimal. Babai has shown that every group $G \notin \{C_3, C_4, C_5\}$ is the automorphism group of a graph with at most $2|G|$ vertices. For $G \in \{C_3, C_4, C_5\}$, there are minimal graphs with order 9, 10 and 15 respectively (cf. Exercise 52).

10 Planar and bipartite graphs

Example 10.1. Three houses H_1, H_2, H_3 are to be supplied with electricity, gas, and water. Can this be achieved without the lines crossing?[15]

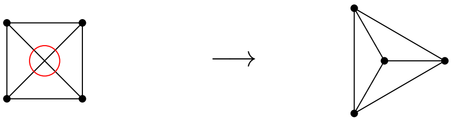


Definition 10.2. Let Ω be a multigraph. Ω is called

- *planar*, if Ω can be drawn in the plane without two edges intersecting. Such a drawing is called a *planar embedding*.
- *bipartite*, if a disjoint union $\Omega_E = \Delta \cup \Gamma$ exists with $\Omega_K \cap \left(\binom{\Delta}{2} \cup \binom{\Gamma}{2}\right) = \varnothing$, i. e. every edge connects Δ with Γ.

Example 10.3.

(i) The complete graph $\mathcal{V}_4$ is (at second glance) planar:



(ii) In the definition of bipartite, we allow $\Delta = \varnothing$ (or $\Gamma = \varnothing$). If necessary, Ω is trivial.

---

[15] Try also the game Planarity.

(iii) For $n, m \in \mathbb{N}$, let $\Omega = \mathcal{V}_{n,m}$ be the *complete bipartite* graph with $\Omega_E = \{\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m\}$ and $\Omega_K = \{\{\alpha_i, \beta_j\} : 1 \le i \le n, 1 \le j \le m\}$. The question in Example 10.1 is equivalent to: Is $\mathcal{V}_{3,3}$ planar?

Remark 10.4.

(i) A multigraph Ω is planar if and only if the corresponding simple graph is planar, because multiple edges can always be drawn in parallel. Furthermore, Ω is planar if and only if every component of Ω is planar. We will therefore restrict ourselves mostly to connected simple graphs.

(ii) The theorem of WAGNER-FÁRY states that a planar embedding of a simple graph can always be drawn such that all edges are straight lines. Open, however, is the conjecture of HARBORTH that the edge lengths can additionally be chosen to be integers.

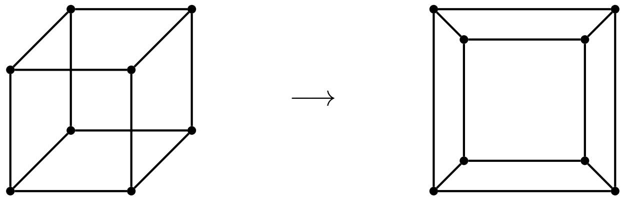
Theorem 10.5. *A graph is bipartite if and only if it contains only cycles of even length. In particular, every graph without cycles is bipartite.*

Proof. Let Ω be bipartite with decomposition $\Omega_E = \Delta \cup \Gamma$. Every path visits vertices in Δ and Γ alternately. Every closed path must therefore have even length. Conversely, let Ω be a graph with exclusively cycles of even length. Wlog. let Ω be connected. Let $\omega \in \Omega_E$ be fixed. For $\alpha \in \Omega_E$, let $d(\omega, \alpha) \in \mathbb{N}_0$ be the *distance* between ω and α, i.e., the length of a shortest path between α and ω. We define

$$\Delta := \{\alpha \in \Omega_E : d(\omega, \alpha) \text{ is even}\},$$
$$\Gamma := \{\alpha \in \Omega_E : d(\omega, \alpha) \text{ is odd}\}.$$

Certainly $\Omega_E = \Delta \cup \Gamma$ is a partition. Suppose there exist $\alpha, \beta \in \Delta$ with $\{\alpha, \beta\} \in \Omega_K$. Let $(\omega = \alpha_1, \ldots, \alpha_{2k} = \alpha)$ and $(\omega = \beta_1, \ldots, \beta_{2l} = \beta)$ be shortest paths and let i be maximal with $\alpha_i = \beta_i$ (if necessary $i = 1$). Then $(\alpha_i, \ldots, \alpha_{2k}, \beta_{2l}, \ldots, \beta_i)$ is a cycle with odd length $2(k + l - i) + 1$. Analogously, the case $\alpha, \beta \in \Gamma$ leads to a contradiction. □

Example 10.6. The vertices and edges of a Platonic solid in $\mathbb{R}^3$ (more generally of any polyhedron) form a (regular) planar graph by infinitely extending one face (cf. Exercise 42):



More generally, every planar embedding of a (planar) graph divides the plane into *faces*, one of which is infinitely large (the "exterior").[16] The following theorem shows that the number of faces does not depend on the planar embedding.

Theorem 10.7 (EULER's polyhedron formula). *For every planar embedding of a connected multigraph Ω with e vertices, f faces and k edges,* $\boxed{e + f - k = 2.}$ *holds.*[17]

---

[16] This intuitive fact is actually the deep-seated *Jordan curve theorem*.

[17] Mnemonic: If one writes the formula as an alternating sum $e - k + f$, then the "dimensions" are ascending (vertices are 0-dimensional, edges 1-dimensional and faces 2-dimensional). As a generalization, one considers the *Euler characteristic* in topology.

Proof. Induction on k. In the case $k = 0$, we have $e = f = 1$ and the formula holds. So let $k \geq 1$. Suppose there exists a vertex $\omega \in \Omega$ with degree 1. The connected, planar graph $\Omega \setminus \{\omega\}$ has $e - 1$ vertices, f faces and $k - 1$ edges. By induction, the formula is correct. Since Ω is connected, we can now assume that all vertices have degree ≥ 2. One then finds a cycle by following a path long enough. By removing an edge of a cycle, a connected, planar graph with e vertices, $f - 1$ faces and $k - 1$ edges is created. Again, the formula holds. $\square$

Lemma 10.8. *Let Ω be a connected, planar graph with e vertices, f faces and k edges. Then:*

(i) If $e \geq 3$, then $k \leq 3e - 6$ with equality if and only if all faces are triangles.

(ii) There exists a vertex of degree ≤ 5.

Proof.

(i) Wlog. let $k \geq 3$. Every face is bounded by at least three edges and every edge separates at most two faces. This shows
$$k \geq \frac{3}{2}f \overset{10.7}{=} \frac{3}{2}(k + 2 - e).$$
Rearranging yields $k \leq 3e - 6$ with equality if and only if every face is bounded by three edges.

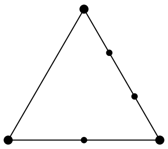
(ii) If all vertices have degree ≥ 6, then $e > 6$ and one obtains the contradiction
$$6e \leq \sum_{\alpha \in \Omega_E} \deg(\alpha) \overset{7.6}{=} 2k \overset{\text{(i)}}{\leq} 6e - 12.$$
$\square$

Example 10.9. According to Lemma 10.8, $\mathcal{V}_5$ is not planar ($e = 5$, $k = 10$). Suppose now that $\Omega = \mathcal{V}_{3,3}$ is planar. Then there is a planar embedding with $f = 2 + k - e = 2 + 3^2 - 6 = 5$ faces. Since Ω has no triangles (Theorem 10.5), every face is bounded by at least four edges. Thus, one would need $\frac{5 \cdot 4}{2} > 9$ edges. Therefore, $\mathcal{V}_{3,3}$ is also not planar.

Definition 10.10. Let Ω be a graph.

- A *subgraph* of Ω is a graph Δ with $\Delta_E \subseteq \Omega_E$ and $\Delta_K \subseteq \Omega_K$.
- By adding a new vertex ω on an edge $\{\alpha, \beta\} \in \Omega_K$, a new graph $(\Omega_E \cup \{\omega\}, (\Omega_K \setminus \{\{\alpha, \beta\}\}) \cup \{\{\alpha, \omega\}, \{\beta, \omega\}\})$ is created. A *subdivision* of Ω is a graph that is created by finitely many such replacements.

Example 10.11. A subdivision of $\mathcal{V}_3$:

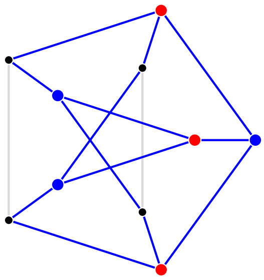


Theorem 10.12 (Kuratowski). *A graph is planar if and only if it contains no subdivisions of $\mathcal{V}_5$ or $\mathcal{V}_{3,3}$ as subgraphs.*

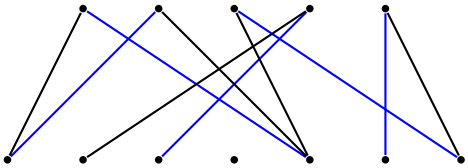
Sketch of proof. If $\mathcal{V}_5$ or $\mathcal{V}_{3,3}$ is a subdivision of a subgraph of Ω, then every planar embedding of Ω also yields a planar embedding of these two graphs. According to Example 10.9, this is impossible.

Conversely, let Ω be non-planar. Since vertices of degree 1 have no influence on planarity, they can be removed. Likewise, one can remove vertices of degree 2 by directly connecting the two involved edges. Subsequently, $\deg\alpha \geq 3$ holds for all $\alpha \in \Delta_E$. It follows that $3|\Delta_E| \leq 2|\Delta_K|$ from the handshaking lemma. According to Lemma 10.8, we can furthermore remove edges until $|\Delta_K| \leq 3|\Delta_E| - 5 \leq 2|\Delta_K| - 5$ holds. One now performs an extensive case distinction based on the k-connectivity of Ω. $\square$

Example 10.13. The Petersen graph is not planar because it contains a subdivision of $\mathcal{V}_{3,3}$ as a subgraph:



Example 10.14. At a ball, women and men want to dance at the same time (only mixed pairs). Is it possible for every woman to dance with a man she is friends with? This can only work if every group of n women is friends with at least n men in total. We show that this condition is even sufficient. To do this, we arrange the men and women as a bipartite graph, such that the edges correspond exactly to the friendships between man and woman. In the following example, the women are the upper points. The blue edges form a possible selection of dance pairs.



Definition 10.15. Let Ω be a graph.

- For $\Delta \subseteq \Omega_E$, let $N(\Delta) := \{\alpha \in \Omega_E : \exists \beta \in \Delta : \{\alpha, \beta\} \in \Omega_K\}$ be the set of neighbors of Δ.
- A *matching* P of Ω is a set of pairwise disjoint edges in Ω, i. e. every vertex occurs in at most one edge of P. One calls P *perfect*, if every vertex occurs in (exactly) one edge. If applicable, $|\Omega_E| = 2|P|$.
- A *vertex cover* of Ω is a subset $U \subseteq \Omega_E$, such that every edge contains a vertex from U.

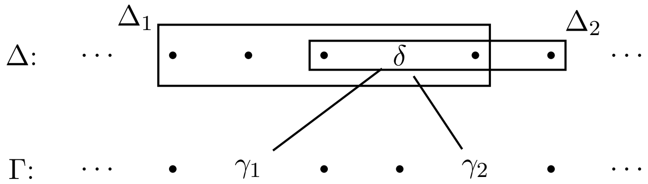
Theorem 10.16 (König). *Let Ω be a bipartite graph. The maximum cardinality of a matching of Ω is the minimum cardinality of a vertex cover of Ω.*

Proof. Let $\Omega = \Delta \cup \Gamma$ be a bipartite partition. A matching of Ω consists of pairwise disjoint Δ-Γ-paths. A vertex cover of Ω is a Δ-Γ-separator. The statement therefore follows from Menger's theorem. $\square$

Theorem 10.17 (HALL's Marriage Theorem). *Let Ω be a bipartite graph with partition $\Omega_E = \Delta \cup \Gamma$. A matching with $|\Delta|$ edges exists if and only if $|N(\Delta_1)| \geq |\Delta_1|$ holds for all $\Delta_1 \subseteq \Delta$.*

Proof. Let $\Delta = \{\delta_1, \ldots, \delta_n\}$. If a matching P with n edges exists, then it has the form $P = \{\{\delta_i, \gamma_i\} : i = 1, \ldots, n\}$, where $\gamma_1, \ldots, \gamma_n \in \Gamma$ are pairwise distinct. For $\Delta_1 = \{\delta_{i_1}, \ldots, \delta_{i_k}\}$, it then holds that $\gamma_{i_1}, \ldots, \gamma_{i_k} \in N(\Delta_1)$ and $|N(\Delta_1)| \geq k = |\Delta_1|$.

Now let $|N(\Delta_1)| \geq |\Delta_1|$ for all $\Delta_1 \subseteq \Delta$. The choice $\Delta_1 = \{\delta_i\}$ shows $\deg(\delta_i) \geq 1$ for $i = 1, \ldots, n$. By induction on $|\Omega_K|$, we can assume that the condition $|N(\Delta_1)| \geq |\Delta_1|$ is violated by removing any arbitrary edge. If we can show $\deg(\delta_i) = 1$ for $i = 1, \ldots, n$, then Ω_K is a matching with n edges. Suppose indirectly there exists $\delta \in \Delta$ with neighbors $\gamma_1, \gamma_2 \in \Gamma$. The graphs $\Omega_i := \Omega \setminus \{\{\delta, \gamma_i\}\}$ for $i = 1, 2$ violate the condition $|N_i(\Delta_1)| \geq |\Delta_1|$, where N_i is the neighbor function N on Ω_i. Choose $\Delta_i \subseteq \Delta$ with $|N_i(\Delta_i)| < |\Delta_i|$ for $i = 1, 2$. It holds that $N_i(\Delta_i) = N(\Delta_i) \setminus \{\gamma_i\}$ and $\delta \in \Delta_1 \cap \Delta_2$.



This shows $N(\Delta_1 \cap \Delta_2 \setminus \{\delta\}) \subseteq N_1(\Delta_1) \cap N_2(\Delta_2)$ and $N_1(\Delta_1) \cup N_2(\Delta_2) = N(\Delta_1 \cup \Delta_2)$. Using the inclusion-exclusion principle, one obtains the contradiction

$$\begin{aligned}|N(\Delta_1 \cap \Delta_2 \setminus \{\delta\})| &\leq |N_1(\Delta_1) \cap N_2(\Delta_2)| = |N_1(\Delta_1)| + |N_2(\Delta_2)| - |N_1(\Delta_1) \cup N_2(\Delta_2)| \\ &= |N_1(\Delta_1)| + |N_2(\Delta_2)| - |N(\Delta_1 \cup \Delta_2)| \leq |\Delta_1| - 1 + |\Delta_2| - 1 - |\Delta_1 \cup \Delta_2| \\ &= |\Delta_1 \cap \Delta_2 \setminus \{\delta\}| - 1.\end{aligned}$$

☐

Remark 10.18. In the situation of Theorem 10.17, one can interpret a matching as an injective mapping $f\colon \Delta \to \Gamma$. In the case $|\Delta| = |\Gamma|$, f is bijective and the matching is perfect.

Corollary 10.19. *Let $M = A_1 \cup \ldots \cup A_n = B_1 \cup \ldots \cup B_n$ be two partitions of a finite set M into parts of equal size. Then $A_i \cap B_i \neq \varnothing$ for $i = 1, \ldots, n$ given a suitable ordering.*

Proof. We consider the bipartite graph Ω with $\Omega_E = \{A_1, \ldots, A_n\} \cup \{B_1, \ldots, B_n\}$. Here, let $\{A_i, B_j\} \in \Omega_K$ if and only if $A_i \cap B_j \neq \varnothing$. For $I \subseteq \{1, \ldots, n\}$, it holds that

$$\Big|\bigcup_{i \in I} A_i\Big| = |I||A_1| = |I|\frac{|M|}{n} = |I||B_1|.$$

Therefore, at least $|I|$ of the B_j are adjacent to vertices A_i with $i \in I$. According to Hall's Marriage Theorem, Ω possesses a perfect matching. The claim follows from this. ☐

Example 10.20.

(i) A well-shuffled deck of Skat cards is dealt into eight stacks of four cards each. Then it is always possible to draw one card from each stack such that the eight drawn cards represent exactly the values $7, 8, \ldots$, King, Ace (in arbitrary suits). This follows from Corollary 10.19 by additionally laying out the cards in a sorted manner, one stack for each value in the four suits.

(ii) Among six people, are there always three who all know each other or all do not know each other? Let the acquaintance relation be symmetric and modeled by the edges of a graph Ω with six vertices. Let $\alpha_1 \in \Omega_E$ be arbitrary. By the pigeonhole principle, there exist $\alpha_2, \alpha_3, \alpha_4 \in \Omega_E$ such that α_1 is either adjacent to all or none of the three vertices. By replacing Ω with its complement, one can assume that the first case occurs. If there is no edge between $\alpha_2, \alpha_3, \alpha_4$, then one has three people who do not know each other. Otherwise, an edge exists, wlog. $\{\alpha_2, \alpha_3\}$. Then $\alpha_1, \alpha_2, \alpha_3$ are three people who know each other. We generalize:

Definition 10.21. Let Ω be a graph and $\Delta \subseteq \Omega_E$. Then $(\Delta, \Omega_K \cap \binom{\Delta}{2})$ is called the *induced* subgraph of Δ. This is exactly the graph that arises by removing $\Omega_E \setminus \Delta$.

Theorem 10.22 (Ramsey)**.** *Let $k \in \mathbb{N}$ and Ω be a graph with at least 4^{k-1} vertices. Then there exist k vertices in Ω that induce a complete or trivial subgraph.*

Proof. We choose $\delta_1 \in \Delta_1 \subseteq \Omega_E$ with $|\Delta_1| = 4^{k-1} = 2^{2k-2}$ arbitrarily. Let $\Gamma \subseteq \Delta_1$ be the set of neighbors of δ_1 in Δ_1. In the case $|\Gamma| \ge 2^{2k-3}$, we choose $\delta_2 \in \Delta_2 \subseteq \Gamma \subseteq \Delta_1 \setminus \{\delta_1\}$ with $|\Delta_2| = 2^{2k-3}$. Otherwise, we choose $\delta_2 \in \Delta_2 \subseteq \Delta_1 \setminus (\Gamma \cup \{\delta_1\})$ with $|\Delta_2| = 2^{2k-3}$. Analogously, we construct $\delta_3 \in \Delta_3 \subseteq \Delta_2 \setminus \{\delta_2\}$ etc. In the end, one obtains $\Delta_1, \ldots, \Delta_{2k-1} \subseteq \Omega_E$ and $\delta_i \in \Delta_i$ with the following properties:

(i) $|\Delta_i| \ge 2^{2k-1-i}$ for $i = 1, \ldots, 2k-1$,

(ii) $\Delta_{i+1} \subseteq \Delta_i \setminus \{\delta_i\}$ for $i = 1, \ldots, 2k-2$,

(iii) δ_i is either adjacent to every or to no vertex in Δ_{i+1} for $i = 1, \ldots, 2k-2$.

By the pigeonhole principle, there exist $1 \le i_1 < \ldots < i_{k-1} \le 2k-2$ such that for $\delta_{i_1}, \ldots, \delta_{i_{k-1}}$ the same case in (iii) occurs. Because of $\Delta_{i_1} \supseteq \Delta_{i_2} \supseteq \ldots \supseteq \Delta_{i_{k-1}} \supseteq \Delta_{2k-1}$, the vertices $\delta_{i_1}, \ldots, \delta_{i_{k-1}}, \delta_{2k-1}$ induce a complete or trivial subgraph. □

Remark 10.23. Obviously, the condition $|\Omega_E| \ge 4^{k-1}$ in Theorem 10.22 is not optimal (consider $k = 2$). Better estimates are obtained by the following refinement: The *Ramsey number* $R(k,l)$ is the smallest natural number such that every graph with at least $R(k,l)$ vertices contains $\mathcal{V}_k$ or $\mathcal{T}_l$ as an induced subgraph. According to Theorem 10.22, $R(k,l) \le 4^{\max\{k,l\}-1}$. Obviously, $R(k,l) = R(l,k)$ (consider the complementary graph) and $R(1,l) = 1$. Every graph with l vertices is either complete or possesses $\mathcal{T}_2$ as an induced subgraph. This shows $R(2,l) = l$.

Lemma 10.24. *For $k, l \ge 2$, it holds that*

$$R(k,l) \le R(k-1,l) + R(k,l-1) \le \binom{k+l-2}{k-1}.$$

If $R(k-1,l)$ and $R(k,l-1)$ are both even, then $R(k,l) < R(k-1,l) + R(k,l-1)$.

Proof. Let Ω be a graph with $n := R(k-1,l) + R(k,l-1)$ vertices. Let $\omega \in \Omega_E$ be arbitrary. Let $\Delta \subseteq \Omega_E$ be the set of neighbors of ω and $\Gamma := \Omega_E \setminus (\Delta \cup \{\omega\})$. Then

$$|\Delta| + |\Gamma| = |\Delta \dot{\cup} \Gamma| = |\Omega_E \setminus \{\omega\}| = n - 1 = R(k-1,l) + R(k,l-1) - 1.$$

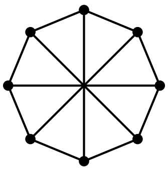
It follows that $|\Delta| \ge R(k-1,l)$ or $|\Gamma| \ge R(k,l-1)$. Wlog. let $|\Delta| \ge R(k-1,l)$. If Δ has an induced $\mathcal{V}_{k-1}$, then Ω has a $\mathcal{V}_k$, since ω is adjacent to all vertices in Δ. Otherwise, Δ (and thus also Ω) has an induced $\mathcal{T}_l$. This shows $R(k,l) \le n$. Because $R(1,l) = R(k,1) = 1 = \binom{l-1}{0} = \binom{k-1}{0}$, it follows inductively that

$$R(k,l) \le R(k-1,l) + R(k,l-1) \le \binom{k+l-3}{k-2} + \binom{k+l-3}{k-1} \overset{1.5}{=} \binom{k+l-2}{k-1}.$$

Now assume that $R(k-1,l)$ and $R(k,l-1)$ are even. Let $|\Omega_E| = n-1$. The above argument only fails if $|\Delta| = R(k-1,l)-1$ and $|\Gamma| = R(k,l-1)-1$ holds for all $\omega \in \Omega_E$. In this case, Ω is $R(k-1,l)$-regular and it follows that $|\Omega_K| = \frac{1}{2}(n-1)\big(|R(k-1,l)|-1\big)$. By assumption, however, this is not an integer. Therefore, $R(k,l) \le n-1$. $\square$

Remark 10.25. From Lemma 10.24 and Catalan's theorem, it follows that $R(k,k) \le \binom{2(k-1)}{k-1} = kC_k$. One can show that this estimate is slightly better than Theorem 10.22.

Example 10.26. From Lemma 10.24 or Example 10.20, it follows that $R(3,3) \le 6$. The $\mathcal{K}_5$ shows $R(3,3) > 5$ and thus $R(3,3) = 6$. Since $R(3,3)$ and $R(2,4) = 4$ are even, $R(3,4) \le 9$ follows from Lemma 10.24. Conversely, the following graph (called "wheel") shows $R(3,4) \ge 9$:



Other known values are (without proof):

$R(3,5) = 14$, $R(3,6) = 18$, $R(3,7) = 23$, $R(3,8) = 28$,
$R(3,9) = 36$, $R(4,4) = 18$, $R(4,5) = 25$.

Theorem 10.27 (Erdős)**.** *For $k \ge 3$, $R(k,k) > 2^{k/2}$ holds.*

Proof. For $k = 3$, $R(3,3) = 6 > 2\sqrt{2}$ holds. So let $k \ge 4$ and $n := 2^{k/2}$. Let v be the number of all graphs with n (fixed) vertices that have $\mathcal{V}_k$ as an (induced) subgraph. For the choice of the k vertices that induce $\mathcal{V}_k$, there are $\binom{n}{k}$ possibilities. One then has $2^{\binom{n}{2}-\binom{k}{2}}$ possibilities to choose the remaining edges. Thus $v \le \binom{n}{k}2^{\binom{n}{2}-\binom{k}{2}}$ (many graphs are counted multiple times this way). The map $\Omega \to \Omega^C$ shows that v is also the number of graphs with an induced $\mathcal{T}_k$. The number of all graphs with n (fixed) vertices is $2^{\binom{n}{2}}$. Because of $k \ge 4$, $k! > 2^k$ holds (induction on k). This shows

$$\begin{aligned} 2v &\le 2\binom{n}{k}2^{\binom{n}{2}-\binom{k}{2}} = 2\frac{n(n-1)\ldots(n-k+1)}{k!}2^{\binom{n}{2}-\binom{k}{2}} < 2\frac{n^k}{2^k}2^{\binom{n}{2}-\frac{k(k-1)}{2}} \\ &= 2^{1+\frac{k^2}{2}-k}2^{\binom{n}{2}-\frac{k(k-1)}{2}} = 2^{1-\frac{k}{2}}2^{\binom{n}{2}} < 2^{\binom{n}{2}}. \end{aligned}$$

Thus there must exist graphs with n vertices that contain neither $\mathcal{V}_k$ nor $\mathcal{T}_k$ as an induced subgraph. $\square$

Remark 10.28. Ramsey's theorem can be generalized as follows: For $r,s,t \in \mathbb{N}$ there exists an $n \in \mathbb{N}$ with the following property: For every n-element set M and every partition $\binom{M}{r} = \mathcal{M}_1 \dot\cup \ldots \dot\cup \mathcal{M}_s$ there exists a t-element subset $A \subseteq M$ with $\binom{A}{r} \subseteq \mathcal{M}_i$ for some $i \in \{1,\ldots,s\}$.[18]

---

[18] See notes on logic and set theory

Theorem 10.29 (Turán)**.** *Let Ω be a graph with n vertices without an induced complete subgraph $\mathcal{V}_k$. Then*

$$|\Omega_K| \le \frac{k-2}{k-1} \cdot \frac{n^2}{2}.$$

Proof.[19] Induction on k: Since every graph contains $\mathcal{V}_1$, it follows that $k \ge 2$. In the case $k = 2$, Ω is trivial and $|\Omega_K| = 0$. Now let $k \ge 3$. We can assume that $|\Omega_K|$ is as large as possible, i. e.. by adding an edge, an induced $\mathcal{V}_k$ would be created. Under this assumption, Ω possesses an induced subgraph $\Delta \cong \mathcal{V}_{k-1}$. The graph $\Omega' := \Omega \setminus \Delta_E$ satisfies the induction hypothesis, i. e..

$$|\Omega'_K| \le \frac{k-2}{k-1}\frac{(n-k+1)^2}{2}.$$

Every vertex $\alpha \in \Omega'$ has at most $k-2$ neighbors in Δ_E, because otherwise $\mathcal{V}_k$ is induced by $\Delta_E \cup \{\alpha\}$. This shows

$$\begin{aligned}|\Omega_K| &\le |\Delta_K| + |\Omega'_K| + (n-k+1)(k-2)\\ &= \frac{1}{2}\Big((k-1)(k-2) + \frac{k-2}{k-1}(n-k+1)^2 + 2(n-k+1)(k-2)\Big)\\ &= \frac{1}{2}\frac{k-2}{k-1}\Big((k-1)^2 + n^2 + (k-1)^2 - 2n(k-1) + 2(n-k+1)(k-1)\Big)\\ &= \frac{k-2}{k-1}\cdot\frac{n^2}{2}\end{aligned}$$

□

Example 10.30. In contrast to Ramsey's Theorem, the estimate in Theorem 10.29 is optimal: Let Ω be a graph and $\Omega_E = \Delta_1 \cup \ldots \cup \Delta_{k-1}$ a partition with $|\Delta_1| = \ldots = |\Delta_{k-1}| = s$. Furthermore, let

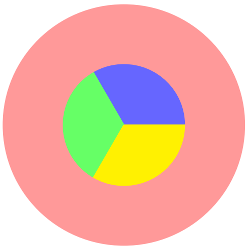
$$\Omega_K = \big\{(\delta_i, \delta_j) : \delta_i \in \Delta_i, \delta_j \in \Delta_j, i \ne j\big\}$$

(thus Ω is an obvious generalization of $\mathcal{V}_{k,k}$). Obviously, Ω satisfies the requirement of Theorem 10.29 with $n = s(k-1)$ and $|\Omega_K| = \binom{k-1}{2}s^2 = \frac{k-2}{k-1}\cdot\frac{n^2}{2}$. One calls Ω a *Turán graph*.

11 Coloring of Graphs

Example 11.1.

(i) How many colors are needed to color a political map such that any two adjacent countries are colored differently? Three colors are not enough:



Are four colors enough?[20] Idea: Interpret the capitals of the countries as vertices of a graph and connect two such vertices if the countries are adjacent.

---

[19] alternative proofs can be found in [Aigner-Ziegler, Proofs from THE BOOK, Springer, 2018]

[20] Try this game for that: kongregate.com

(ii) Can all lectures at LUH be scheduled such that no student has a scheduling conflict? Idea: Each lecture is a vertex of a graph. Connect two lectures if they have at least one common listener. Assign a time slot (color) to each lecture such that "adjacent" lectures are colored differently.

Definition 11.2. Let C be a set (of colors). A *coloring* of a multigraph Ω is a map $f\colon \Omega_E \to C$ such that adjacent vertices have different values, i. e. for $\{\alpha, \beta\} \in \Omega_K$ we have $f(\alpha) \ne f(\beta)$. The *chromatic number* $\chi(\Omega)$ is the smallest natural number c such that a coloring with $c = |C|$ colors exists.

Remark 11.3. Since multiple edges do not change the chromatic number, we can restrict ourselves to simple graphs as usual. If $\Omega_1, \ldots, \Omega_n$ are the components of Ω, then clearly $\chi(\Omega) = \max\{\chi(\Omega_i) : i = 1, \ldots, n\}$. Therefore, it suffices to investigate connected graphs.

Example 11.4. One easily shows

Ω	$\mathcal{T}_n$	$\mathcal{V}_n$	$\mathcal{V}_{k,l}$	$\mathcal{G}_n$	$\mathcal{K}_{2n}$	$\mathcal{K}_{2n+1}$	$\mathcal{S}_n$
$\chi(\Omega)$	1	n	2	2	2	3	2

Lemma 11.5. *For every graph Ω, we have $\chi(\Omega) \le \frac{1}{2} + \sqrt{2|\Omega_K| + \frac{1}{4}}$.*

Proof. Let $f\colon \Omega_E \to C$ be a coloring with $|C| = \chi(\Omega)$. For distinct colors $c, d \in C$, there must be at least one edge between the preimages $f^{-1}(c)$ and $f^{-1}(d)$, because otherwise one could set $c = d$ and get by with $\chi(\Omega) - 1$ colors. Therefore, $|\Omega_K| \ge |\binom{C}{2}| = \chi(\Omega)(\chi(\Omega) - 1)/2$. The assertion follows from the p-q-formula for quadratic equations. ☐

Lemma 11.6. *A graph Ω is bipartite if and only if $\chi(\Omega) \le 2$.*

Proof. Let Ω be bipartite with partition $\Omega_E = \Delta \cup \Gamma$. Then it suffices to choose one color for Δ and one for Γ. Thus $\chi(\Omega) \le 2$. Conversely, let $\chi(\Omega) \le 2$. In the case $\chi(\Omega) = 1$, Ω is trivial and bipartite. So let $\chi(\Omega) = 2$ and $f\colon \Omega_E \to C$ be a coloring with $C = \{c, d\}$. Let $\Delta := \{\omega \in \Omega_E : f(\omega) = c\}$ and $\Gamma := \{\omega \in \Omega_E : f(\omega) = d\}$. Then Ω is bipartite with partition $\Omega_E = \Delta \cup \Gamma$. ☐

Definition 11.7. For a graph Ω, let $\deg(\Omega) := \max\{\deg(\omega) : \omega \in \Omega\}$ be the *maximum degree* of Ω.

Theorem 11.8. *For every graph Ω, we have $\chi(\Omega) \le \deg(\Omega) + 1$.*

Proof. Let $\Omega_E := \{\alpha_1, \ldots, \alpha_n\}$ and $C := \{1, \ldots, \deg(\Omega) + 1\}$. Because of $\deg(\alpha_i) \le \deg(\Omega) < |C|$, one can define

$$f(\alpha_i) := \min\ C \setminus \{f(\alpha_j) : 1 \le j < i, \{\alpha_i, \alpha_j\} \in \Omega_K\}$$

for $i = 1, \ldots, n$. Clearly $f\colon \Omega_E \to C$ is a coloring. ☐

Remark 11.9. Example 11.4 shows that the estimate in Theorem 11.8 cannot be improved in general. However, the exceptions can be precisely classified. For this, we use the following argument. Let Ω be a graph with $\deg(\Omega) \le d$, in which some vertices are already colored with at most d colors. Let $(\alpha_1, \ldots, \alpha_n)$ be a path of uncolored vertices. Since α_1 has at most $d - 1$ colored neighbors (α_2 is uncolored), α_1 can be colored. Analogously, one can color $\alpha_2, \ldots, \alpha_{n-1}$ one after another. Only α_n might possibly not be colorable.

Theorem 11.10 (Brooks)**.** *For every graph Ω, one of the following statements holds:*

(1) $\chi(\Omega) \leq \deg(\Omega)$.

(2) $\mathcal{V}_{\chi(\Omega)}$ *is a component of* Ω.

(3) $\chi(\Omega) = 3$ *and* $\mathcal{K}_{2n+1}$ *is a component of* Ω *for some* $n \in \mathbb{N}$.

Proof (Zając). According to Theorem 11.8, we can assume $d := \deg(\Omega) = \chi(\Omega) - 1$.

Step 1: $d \geq 3$.
In the case $d \leq 1$, $\mathcal{V}_{d+1}$ is a component of Ω. In the case $d = 2$, every component of Ω is a line or a circle. If no circle of odd length occurs, then $\chi(\Omega) = 2$ would hold. Thus (3) holds.

Now let Ω be a counterexample with as few vertices as possible.

Step 2: For every subgraph Δ of Ω with $|\Delta_E| < |\Omega_E|$, $\chi(\Delta) \leq d$ holds.
According to Theorem 11.8, $\chi(\Delta) \leq \deg(\Delta) + 1 \leq d + 1$. Let us assume $\chi(\Delta) = d + 1$. Since Δ is not a counterexample and $\chi(\Delta) > 3$, $\mathcal{V}_{d+1}$ is a component of Δ. Thus $\mathcal{V}_{d+1}$ is a subgraph of Ω. Because of $\deg(\Omega) = d$, $\mathcal{V}_{d+1}$ would then even be a component of Ω.

Step 3: Ω is d-regular.
Let $\alpha \in \Omega_E$ with $\deg(\alpha) < d$. According to Step 2, $\Omega \setminus \{\alpha\}$ can be colored with d colors. Because of $\deg(\alpha) < d$, α can also be colored without using a new color. This contradicts $\chi(\Omega) = d + 1$.

Since $\mathcal{V}_{d+1}$ is not a subgraph of Ω, there exists a path $(\alpha_1, \alpha_2, \alpha_3)$ such that α_1 and α_3 are not adjacent. We extend this path as far as possible $(\alpha_1, \ldots, \alpha_s)$ without using vertices multiple times. Then all neighbors of α_s are in $\{\alpha_1, \ldots, \alpha_{s-1}\}$.

Case 1: $\Omega_E = \{\alpha_1, \ldots, \alpha_s\}$.
Because of $d \geq 3$, there exists $i \notin \{1, 3\}$ such that α_i is a neighbor of α_2. By assumption, we can color α_1 and α_3 with the same color. Subsequently, we color $(\alpha_4, \alpha_5, \ldots, \alpha_{i-1}, \alpha_i)$ and $(\alpha_s, \alpha_{s-1}, \ldots, \alpha_i, \alpha_2)$ as described in Remark 11.9. Finally, we can also color α_2, because α_2 has two neighbors of the same color (α_1 and α_3). Thus all vertices are colored with at most d colors. Contradiction.

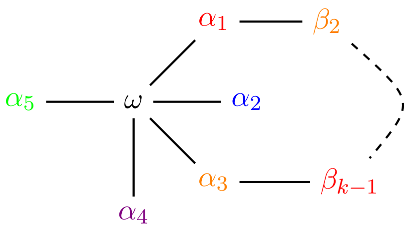
Case 2: $\Omega_E \neq \{\alpha_1, \ldots, \alpha_s\}$.
Let i be minimal such that α_i is a neighbor of α_s (all neighbors of α_s lie in $\{\alpha_1, \ldots, \alpha_{s-1}\}$). According to Step 2, $\Omega' := \Omega \setminus \{\alpha_i, \ldots, \alpha_s\}$ can be colored with d colors. Furthermore, Ω is connected. Let j be maximal such that α_j has a neighbor β in Ω'. Then $j < s$. Since α_{j+1} has no neighbor in Ω', we can color α_{j+1} with the same color as β. Now we apply Remark 11.9 to the path $(\alpha_{j+2}, \ldots, \alpha_s, \alpha_i, \alpha_{i+1}, \ldots, \alpha_j)$. Subsequently, we can also color α_j, because α_j has two neighbors of the same color (α_{j+1} and β). Thus all vertices are colored with at most d colors. Contradiction. □

Theorem 11.11 (Heawood)**.** *For every planar graph Ω, $\chi(\Omega) \leq 5$ holds.*

Proof. Wlog. let Ω be connected. Induction on $e := |\Omega_E|$. For $e \leq 5$, $\chi(\Omega) \leq \chi(\mathcal{V}_5) = 5$ holds. So let $e \geq 6$. We consider a planar embedding of Ω. According to Lemma 10.8, there exists $\omega \in \Omega_E$ with $\deg(\omega) \leq 5$. For the planar graph $\Omega' = \Omega \setminus \{\omega\}$, $\chi(\Omega') \leq 5$ holds by induction. Let $f \colon \Omega'_E \to C = \{1, \ldots, 5\}$ be a corresponding coloring. Let $\alpha_1, \ldots, \alpha_n \in \Omega'_E$ be the neighbors of ω numbered clockwise. In the case $|\{f(\alpha_i) : i = 1, \ldots, n\}| \leq 4$, we can choose $f(\omega) \in C \setminus \{f(\alpha_i) : i = 1, \ldots, n\}$. So let $n = 5$ and wlog. $f(\alpha_i) = i$ for $i = 1, \ldots, 5$. Let Ω_{13} be the subgraph of Ω induced by the vertices $\beta \in \Omega'_E$ with $f(\beta) \in \{1, 3\}$. We define Ω_{24} analogously.

Case 1: α_1 and α_3 lie in different components Δ and Γ of Ω_{13}.
Here we swap the colors 1 and 3 in Δ and set $f(\omega) = 1$. Then $\chi(\Omega) \leq 5$ holds.

Case 2: α_1 and α_3 are connected in Ω_{13}.
Let $(\alpha_1 = \beta_1, \dots, \beta_k = \alpha_3)$ be a shortest path in Ω_{13}. Then $(\beta_1, \dots, \beta_k, \omega, \alpha_1)$ is a cycle, in whose interior either α_2 or α_4, α_5 lies. In particular, α_2 and α_4 are not connected in Ω_{24}. We can then argue analogously to Case 1.



□

Theorem 11.12 (Four Color Theorem)**.** *For every planar graph Ω, $\chi(\Omega) \leq 4$ holds.*

Proof. The proof by Appel and Haken from the year 1976 was the first computer proof in mathematics. Almost two thousand cases had to be checked. In 1996, the number of cases was reduced to 633. As before, no proof is known that can manage without the computer. □

Remark 11.13.

(i) The four color theorem implies the fact already known to us that $\mathcal{V}_5$ is not planar (Example 10.9).

(ii) Determining the chromatic number of a (not necessarily planar) graph is NP-complete (so one can again earn a million dollars…). Even the question of whether a planar graph has chromatic number 3 is NP-complete.

Definition 11.14. Let Ω be a graph and C a set of colors. An *edge coloring* of Ω is a map $f\colon \Omega_K \to C$ with $f(A) \neq f(B)$ if $A \cap B \neq \varnothing$. An edge with color c is also called a *c-edge*. The minimum number of colors required for an edge coloring is called the *chromatic index* $\chi'(\Omega)$.

Remark 11.15.

(i) Obviously $\chi'(\Omega) \geq \deg(\Omega)$ for every graph Ω.

(ii) In the case $\deg(\Omega) \leq 2$, every component of Ω is a line or a cycle. One then easily sees: $\chi'(\Omega) \leq \chi(\Omega) \leq 3$.

(iii) Ramsey's theorem can be interpreted with colors: Let $k \in \mathbb{N}$ and $n \geq 4^{k-1}$. We color the edges of $\mathcal{V}_n$ arbitrarily with red and blue (without satisfying the condition of an edge coloring). Then one can always choose k vertices that are connected only by red or only by blue edges (apply Theorem 10.22 to the "red" subgraph).

(iv) One can consider the edges of Ω as vertices of a new graph $\widehat{\Omega}$. Here, two vertices in $\widehat{\Omega}$ are adjacent if the corresponding edges in Ω share a common vertex. $\widehat{\Omega}$ is called the *line graph* of Ω. It holds that $\chi'(\Omega) = \chi(\widehat{\Omega})$. Because of $\deg(\widehat{\Omega}) \leq 2\deg(\Omega) - 2$, one obtains $\chi'(\Omega) \leq 2\deg(\Omega) - 1$ from Theorem 11.8. To sharpen this estimate, we use the following argument:

Let e, f be colors of an edge coloring. Let $(\alpha_1, \ldots, \alpha_n)$ be a path whose edges $\{\alpha_i, \alpha_{i+1}\}$ are colored alternately with e and f. Suppose the path can be extended neither at the front nor at the back without losing the alternating coloring. Then one may swap the colors e and f on the path $(\alpha_1, \ldots, \alpha_n)$ without violating the coloring property.

Theorem 11.16 (König)**.** *For every bipartite graph* Ω*,* $\chi'(\Omega) = \deg(\Omega)$ *holds.*

Proof. We must show $\chi'(\Omega) \leq \deg(\Omega) =: d$. Induction on $|\Omega_K|$. If Ω is trivial, no color is needed. Let therefore $A := \{\alpha, \beta\} \in \Omega_K$ and $\Omega' := \Omega \setminus A$. By induction, Ω' possesses an edge coloring with $d \geq \deg(\Omega')$ colors. In Ω', $\deg(\alpha), \deg(\beta) < d$ holds. Therefore, at least one color e is "missing" at α (i. e. there is no e-edge in Ω' containing α). Analogously, let the color f be missing at β. In the case $e = f$, we can color A with e and are finished. So let $e \neq f$. Furthermore, we can assume that α possesses an f-edge. Starting from α, we construct a maximal path $(\alpha = \alpha_1, \ldots, \alpha_n)$ with alternating f- and e-edges (since e is missing at α, the path cannot be extended at the beginning either). In the case $\alpha_n = \beta$, n is odd because Ω is bipartite. Then $\{\alpha_{n-1}, \alpha_n\}$ would be an f-edge, which cannot be the case since f is missing at β. Thus $\alpha_n \neq \beta$. As described in Remark 11.15, one may swap e and f on the path. Subsequently, f is missing at α and at β. We can therefore color $\{\alpha, \beta\}$ with f. ☐

Theorem 11.17 (Vizing)**.** *For every graph* Ω*,* $\chi'(\Omega) \in \{\deg(\Omega), \deg(\Omega) + 1\}$ *holds.*

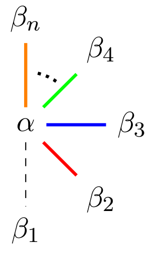
Proof. We show $\chi'(\Omega) \leq \deg(\Omega) + 1$ by induction on $|\Omega_K|$. Wlog. let $\Omega_K \neq \varnothing$ and $d := \deg(\Omega) \geq 1$. Let $A = \{\alpha, \beta\} \in \Omega_K$ and $\Omega' := \Omega \setminus A$. By induction, there exists an edge coloring $\varphi\colon \Omega'_K \to C$ with $|C| = d + 1$ colors. As in the proof of Theorem 11.16, at least one color is missing at each vertex. Suppose the color e is missing at α and f is missing at β. A maximal path with alternating e- and f-edges starting from α must then end at β, because otherwise one could swap e and f on this path as in Remark 11.15 and subsequently color A with f.

We choose a sequence of distinct neighbors $\beta = \beta_1, \ldots, \beta_n$ of α as long as possible, such that $\varphi(\{\alpha, \beta_{i+1}\})$ is missing at β_i for $i = 1, \ldots, n-1$. On the graphs $\Omega_i := \Omega \setminus \{\{\alpha, \beta_i\}\}$ we define a coloring

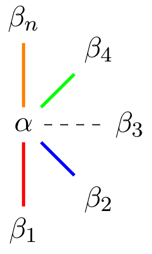
$$\varphi_i(B) := \begin{cases} \varphi(\{\alpha, \beta_{j+1}\}) & \text{if } 1 \leq j \leq i-1 \text{ and } B = \{\alpha, \beta_j\}, \\ \varphi(B) & \text{otherwise} \end{cases}$$

for $i = 1, \ldots, n$. In each of these colorings, the same colors are missing at α as in Ω'.

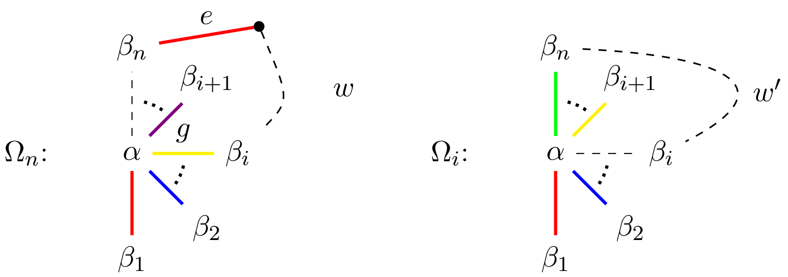
$\Omega' = \Omega_1$:



Ω_3:



Let g be a color missing at β_n. The maximal path w with alternating e- and g-edges in Ω_n starting from β_n must end at α (by the first part of the proof). The last edge on this path, say $\{\alpha, \gamma\}$, carries color g. Since the sequence $\beta_1, \ldots, \beta_n$ cannot be extended, it must hold that $\gamma = \beta_i$ with $1 \le i < n$. Now $g = \varphi_n(\{\alpha, \beta_i\}) = \varphi(\{\alpha, \beta_{i+1}\})$ holds.

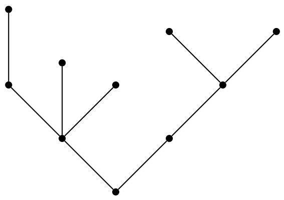


By the choice of β_{i+1}, this means that g is missing at β_i in φ. Thus g is also missing at β_i in φ_i. We can therefore consider the alternating path w' with g- and e-edges in Ω_i starting from β_i. The first segment of the path must coincide with w (in the reverse direction). However, with respect to $\varphi_1 = \varphi$ and φ_i, color g is missing at β_n. Therefore w' must end in β_n. According to the first part of the proof, however, w' should have ended in α. Contradiction. ☐

12 Trees

Definition 12.1. A connected graph Ω is called a *tree*, if Ω contains no cycle, i. e. any two vertices of Ω are connected by exactly one path. Vertices of degree ≤ 1 are then (fittingly) called *leaves*.

Example 12.2. Lines and stars are always trees. In contrast, $\mathcal{T}_n$, $\mathcal{V}_n$ and $\mathcal{K}_n$ are not trees for $n \ge 3$. Typical trees are family trees:



Remark 12.3. According to Theorem 10.5, every tree Ω is a bipartite graph. In particular, $\chi(\Omega) \le 2$ and $\chi'(\Omega) = \deg(\Omega)$ according to Theorem 11.16.

Theorem 12.4. *A connected graph Ω with n vertices is a tree if and only if $|\Omega_K| = n - 1$ holds. In particular, every connected graph with n vertices has at least $n - 1$ edges.*

Proof. Induction on n: For $n = 1$, the claim is clear. So let Ω be a tree with $n \ge 2$ vertices. Let $\omega = \omega_1, \ldots, \omega_k$ be a path of maximal length without duplicate vertices. Then ω is a leaf, because otherwise one could extend the path by one vertex. By induction, $\Omega \setminus \{\omega\}$ is a tree with $n - 1$ vertices and $n - 2$ edges. Thus $|\Omega_K| = n - 1$.

Conversely, let Ω be a connected graph with n vertices and k edges. Suppose that Ω contains a cycle Δ. Then one can remove an edge from Δ such that Ω is still connected. This can be repeated until a tree is obtained. According to the first part, $k \geq n-1$ holds, where equality occurs if and only if Ω is already a tree. $\square$

Remark 12.5.

(i) From the proof of Theorem 12.4, it follows that every tree has at least one leaf. By induction on the number of vertices, it follows easily that every tree is planar (in a planar embedding, a leaf can be added to any vertex). This is of course also obtained from Kuratowski, since $\mathcal{V}_5$ and $\mathcal{V}_{3,3}$ contain cycles.

(ii) As is well known, there are exactly $2^{\binom{n}{2}} = 2^{n(n-1)/2}$ graphs with n given vertices (without considering isomorphism). We count how many such graphs are trees.

Theorem 12.6 (Cayley formula)**.** *There are exactly n^{n-2} trees with vertex set $\{1,\ldots,n\}$.*

Proof[21] (Prüfer). wlog. let $n \geq 3$. For an n-element subset $M \subseteq \mathbb{N}$, let $B(M)$ be the set of all trees Ω with $\Omega_E = M$. We construct mutually inverse bijections

$$f\colon B(M) \to M^{n-2},$$
$$g\colon M^{n-2} \to B(M)$$

by induction on n. For $n=3$, $\Omega \in B(M)$ is a path and we define $f(\Omega)$ as the center of Ω (the only vertex of degree 2). Conversely, if $\alpha \in M = M^{n-2}$ is given, we define $g(\alpha)$ as the path with center α. Then certainly $f \circ g = \mathrm{id}_{M^{n-2}}$ and $g \circ f = \mathrm{id}_{B(M)}$.

Now let $n \geq 4$ and $\Omega \in B(M)$ be given. Let $\alpha \in \Omega_E = M$ be the leaf with the smallest value in M and let β be the unique neighbor of α. We define inductively $f(\Omega) := \big(\beta, f(\Omega \setminus \{\alpha\})\big)$. By induction it follows that $M \setminus f(\Omega)$ is the set of leaves of Ω. Conversely, let $(\alpha_1,\ldots,\alpha_{n-2}) \in M^{n-2}$ be given. We set $\alpha := \min M \setminus \{\alpha_1,\ldots,\alpha_{n-2}\}$. Inductively, $\Delta := g(\alpha_2,\ldots,\alpha_{n-2}) \in B\big(M \setminus \{\alpha\}\big)$ already exists and we can define

$$g(\alpha_1,\ldots,\alpha_{n-2}) := \big(M, \Delta_K \cup \{\alpha_1,\alpha\}\big) \in B(M).$$

To calculate $g \circ f$, we choose $\Omega \in B(M)$, the smallest leaf $\alpha \in \Omega_E$, the neighbor β of α and $\Delta := \Omega \setminus \{\alpha\} \in B(M \setminus \{\alpha\})$. Since $M \setminus f(\Omega)$ is the set of leaves of Ω, we have $\min M \setminus f(\Omega) = \alpha$. Inductively, $g(f(\Delta)) = \Delta$ holds and it follows that

$$g\big(f(\Omega)\big) = g\big(\beta, f(\Delta)\big) = \big(M, \Delta_K \cup \{\beta,\alpha\}\big) = \Omega.$$

Conversely, let $(\alpha_1,\ldots,\alpha_{n-2}) \in M^{n-2}$, $\alpha := \min M \setminus \{\alpha_1,\ldots,\alpha_{n-2}\}$ and $\Delta := g(\alpha_2,\ldots,\alpha_{n-2}) \in B(M \setminus \{\alpha\})$. Inductively, $f(\Delta) = (\alpha_2,\ldots,\alpha_{n-2})$. Thus $M \setminus \{\alpha,\alpha_2,\ldots,\alpha_{n-2}\}$ are the leaves of Δ and $M \setminus \{\alpha_1,\ldots,\alpha_{n-2}\}$ are the leaves of $g(\alpha_1,\ldots,\alpha_{n-2})$. Therefore α is the smallest leaf of $g(\alpha_1,\ldots,\alpha_{n-2})$ and it follows that

$$f\big(g(\alpha_1,\ldots,\alpha_{n-2})\big) = f\big(M, \Delta_K \cup \{\alpha_1,\alpha\}\big) = \big(\alpha_1, f(\Delta)\big) = (\alpha_1,\ldots,\alpha_{n-2}).$$

Thus f and g are mutually inverse bijections. In particular, f is bijective and $|B(M)| = |M^{n-2}| = n^{n-2}$. $\square$

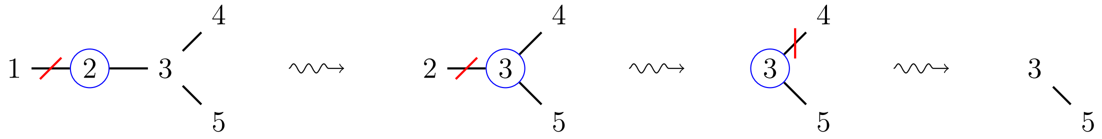
Remark 12.7. Using the notation from the above proof, $f(\Omega)$ is called the *Prüfer code* of a tree Ω.

---

[21] alternative proofs can be found in [Aigner-Ziegler, Proofs from THE BOOK, Springer, 2014]

Example 12.8.

(i) The Prüfer code of



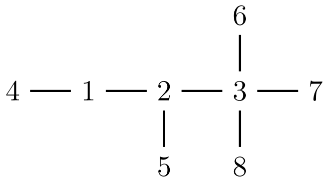
is $(2, 3, 3)$. As claimed in the proof, the leaves do not appear in the Prüfer code.

(ii) Conversely, let the Prüfer code $(\alpha_1, \ldots, \alpha_{n-2})$ be given and $M = \{1, \ldots, n\}$. The construction of the corresponding tree is done according to the following algorithm: For $k = 1, \ldots, n-2$, connect the vertices α_k and

$$\beta_k := \min M \setminus \big(\{\beta_1, \ldots, \beta_{k-1}\} \cup \{\alpha_k, \ldots, \alpha_{n-2}\}\big)$$

with an edge. Then connect the remaining two vertices in $M \setminus \{\beta_1, \ldots, \beta_{n-2}\}$. For the Prüfer code $(1, 2, 2, 3, 3, 3)$ one obtains:

α_k	1	2	2	3	3	3
β_k	4	1	5	?		



Remark 12.9.

(i) Let Ω be a tree with $\Omega_E = \{1, \ldots, n\}$ and let d_i be the degree of the vertex $i \in \{1, \ldots, n\}$. In the construction of the Prüfer code, $d_i - 1$ neighbors of i are removed and each time i is written into $f(\Omega)$. Subsequently, i is a leaf and no longer appears in $f(\Omega)$. Thus, $d_i - 1$ is the multiplicity of i in the Prüfer code. According to Theorem 12.4, Ω has exactly $n - 1$ edges and it follows that $\sum_{i=1}^n d_i = 2(n-1)$ from the handshaking lemma. The number of trees with given vertex degrees $d_1, \ldots, d_n$ is therefore

$$\binom{n-2}{d_1 - 1, \ldots, d_n - 1}$$

according to Theorem 1.18.

(ii) The multiset $\{d_1 - 1, \ldots, d_n - 1\}$ describes a partition of $n - 2$ (if one omits zeros) and conversely, for every partition of $n - 2$ there is a corresponding tree. Isomorphic trees obviously yield the same multiset $\{d_1, \ldots, d_n\}$. The number of isomorphism classes of trees of order n is thus at least $p(n-2)$.

(iii) Let $e_1, \ldots, e_s$ be the multiplicities in the multiset $\{d_1, \ldots, d_n\}$ (so $e_1 + \ldots + e_s = n$). Then one can arrange the numbers $d_1, \ldots, d_n$ in

$$\binom{n}{e_1, \ldots, e_s}$$

ways. The number of trees whose vertex degrees yield the multiset $\{d_1, \ldots, d_n\}$ is thus

$$\binom{n-2}{d_1 - 1, \ldots, d_n - 1}\binom{n}{e_1, \ldots, e_s}.$$

For $n = 7$ and $\{d_1, \dots, d_7\} = \{1, 1, 1, 2, 2, 2, 3\}$ one obtains

$$\binom{5}{1,1,1,2}\binom{7}{3,3,1} = \frac{5!7!}{2!3!3!} = 5! \cdot 2 \cdot 5 \cdot 7 = 120 \cdot 70 = 8.400.$$

Theorem 12.10. *The number of trees with n vertices, of which k are leaves, is $\left\{ {n-2 \atop n-k} \right\} \frac{n!}{k!}$.*

Proof. For the choice of the leaves $\alpha_1, \dots, \alpha_k \in \{1, \dots, n\}$ of Ω there are $\binom{n}{k}$ possibilities. Let $\alpha_{k+1}, \dots, \alpha_n$ be the remaining vertices. The Prüfer code of Ω then corresponds to a surjective mapping $\{1, \dots, n-2\} \to \{\alpha_{k+1}, \dots, \alpha_n\}$. The sought number of trees is therefore

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

according to Theorem 2.35. □

Example 12.11. According to Theorem 12.6 there are $5^3 = 125$ trees with vertex set $\{1, \dots, 5\}$. We determine the isomorphism classes by going through the partitions of 3:

- The partition (1^3) yields the $\binom{5}{2,3} = 10$ possible degree sequences $(1, 1, 2, 2, 2), \dots, (2, 2, 2, 1, 1)$. There are therefore

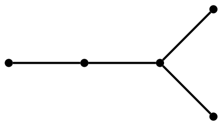
  $$10\binom{3}{1,1,1} = 60$$

  such trees, which are all isomorphic to the path $\mathcal{G}_5$ (these are the trees with exactly two leaves).

- The partition $(2, 1)$ yields $\binom{5}{1,1,3} = 20$ possible degree sequences $(1, 1, 1, 2, 3), \dots, (3, 2, 1, 1, 1)$. This results in

  $$20\binom{3}{1,2} = 60$$

  trees, which are all isomorphic to

  (these are the trees with exactly three leaves).

- The partition (3) yields $\binom{5}{4,1} = 5$ degree sequences $(1, 1, 1, 1, 4), \dots, (4, 1, 1, 1, 1)$ and 5 trees, which are all isomorphic to $\mathcal{S}_5$ (these are the trees with exactly four leaves).

There are therefore only three trees with five vertices up to isomorphism (cf. `https://oeis.org/A000055`).

Remark 12.12. In contrast to Theorem 9.10, Erdős and Rényi also proved that almost all trees are symmetric. For this, they showed that most trees possess *cherries*. These are two leaves with a common neighbor. Swapping these leaves yields a non-trivial automorphism.

Example 12.13. In a newly developed residential area, street lamps are to be supplied with electricity. How many possibilities are there to connect the lamps with as few power cables as possible.

Definition 12.14. Let Ω be a multigraph with adjacency matrix $A = (a_{ij}) \in \mathbb{Q}^{n\times n}$ and vertex degrees $d_1, \ldots, d_n$.

- The matrix
$$L(\Omega) := (\delta_{ij}d_i - a_{ij})_{i,j} = \begin{pmatrix} d_i & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -a_{n-1,n} \\ -a_{n,1} & \cdots & -a_{n,n-1} & d_n \end{pmatrix}$$
is called the *Laplacian matrix* of Ω.
- A (simple) subgraph Δ of Ω is called a *spanning tree* of Ω if Δ is a tree and $\Omega_E = \Delta_E$.

Example 12.15. Obviously, only connected multigraphs can possess spanning trees. By removing suitable edges (as in the proof of Theorem 12.4), one sees that every connected multigraph Ω possesses a spanning tree. The number of spanning trees is at most $\binom{|\Omega_K|}{|\Omega_E|-1}$ according to Theorem 12.4. In particular, every tree is its own spanning tree. The spanning trees of the complete graph $\mathcal{V}_n$ are exactly the n^{n-2} trees with n vertices.

Theorem 12.16 (Kirchhoff's Matrix Tree Theorem)**.** *Let Ω be a multigraph with Laplacian matrix L. Let L' be the matrix formed by deleting the last row and last column from L. Then* $\det(L')$ *is the number of spanning trees in Ω.*

Proof. Induction on $|\Omega_K|$: In the case $\Omega = \mathcal{T}_n$, L and L' are zero matrices and there is only one spanning tree if $n = 1$. We then interpret the determinant of the 0×0-matrix L' as 1. So let $\Omega_K \neq \varnothing$. We number the vertices of Ω such that the last two vertices are connected by an edge a. The spanning trees of Ω that do not contain a are exactly the spanning trees of $\Omega' := \Omega \setminus \{a\}$. Their number is $\det(L(\Omega')')$ by induction. Let Δ be the graph formed from Ω by removing a and merging the last two vertices[22] (this may create multiple edges). Every spanning tree of Ω that contains a can now be uniquely interpreted as a spanning tree of Δ. By induction, Ω thus possesses exactly $\det(L(\Omega')') + \det(L(\Delta)')$ spanning trees.

Let $L = (x_{ij}) \in \mathbb{Q}^{n\times n}$. Since the determinant is linear in the last column, it holds that

$$\begin{aligned}\det L' &= \det\begin{pmatrix} x_{1,1} & \cdots & x_{1,n-1} \\ \vdots & \ddots & \vdots \\ x_{n-1,1} & \cdots & x_{n-1,n-1} - 1 \end{pmatrix} + \det\begin{pmatrix} x_{1,1} & \cdots & x_{1,n-2} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ x_{n-2,1} & \cdots & x_{n-2,n-2} & 0 \\ x_{n-1,1} & \cdots & x_{n-1,n-2} & 1 \end{pmatrix} \\ &= \det(L(\Omega')') + \det\begin{pmatrix} x_{1,1} & \cdots & x_{1,n-2} \\ \vdots & & \vdots \\ x_{n-2,1} & \cdots & x_{n-2,n-2} \end{pmatrix} \\ &= \det(L(\Omega')') + \det(L(\Delta)')\end{aligned}$$

using Laplace's expansion theorem. □

Remark 12.17.

(i) Obviously, in the Matrix Tree Theorem, one can just as well delete the i-th row and column of L instead of the last row and column.

---

[22] one speaks of *edge contraction*

(ii) Since $L = L(\Omega)$ is real and symmetric, all eigenvalues are real. By construction, every row sum (and column sum) of L is equal to 0. Therefore, $(1, \dots, 1)$ is an eigenvector for the eigenvalue 0.

Theorem 12.18. *Let Ω be a multigraph and let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of $L(\Omega)$ (with multiplicities), such that $\lambda_n = 0$. Then Ω has exactly $\frac{1}{n}\lambda_1 \dots \lambda_{n-1}$ spanning trees.*

Proof. The characteristic polynomial of $L = L(\Omega)$ has the form

$$\chi := \det(X1_n - L) = X(X - \lambda_1)\dots(X - \lambda_{n-1}) = (-1)^{n-1}\lambda_1 \dots \lambda_{n-1}X + \dots.$$

We add the rows $1, \dots, n-1$ of $X1_n - L$ to the n-th row. This does not change the determinant. Since the column sums of L vanish, the last row of the new matrix has the form $(X, \dots, X)$. We now extract the factor X from the last row and obtain a matrix $M(X)$ whose last row is $(1, \dots, 1)$ (the other rows coincide with $X1_n - L$). It now holds that $\chi = X \det(M(X))$. The constant term of $\det(M(X))$ is obtained by setting $X = 0$. The coefficient $(-1)^{n-1}\lambda_1 \dots \lambda_{n-1}$ of X in χ is therefore $\det(M(0))$. We now add the columns $1, \dots, n-1$ of $M(0)$ to the last column of $M(0)$. This does not change $\det(M(0))$ and the last column has the form $(0, \dots, 0, n)^{\mathrm{t}}$. Laplace's expansion theorem shows

$$(-1)^{n-1}\lambda_1 \dots \lambda_{n-1} = \det(M(0)) = n\det(-L') = n(-1)^{n-1}\det(L').$$

The assertion follows from the Matrix Tree Theorem. □

Example 12.19.

(i) If Ω is not connected, then the Laplacian matrix has block diagonal form $L = \left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ for a suitable numbering of the vertices. Now $(1, \dots, 1, 0, \dots, 0)$ and $(0, \dots, 0, 1, \dots, 1)$ are two linearly independent eigenvectors for the eigenvalue 0. The algebraic multiplicity of 0 is therefore at least 2. According to Theorem 12.18, Ω has no spanning trees in accordance with Example 12.15.

(ii) For $\Omega = \mathcal{V}_n$, $L = L(\Omega) = n1_n - J$, where as usual $J = (1)_{i,j}$. The eigenvalues of L are 0 with multiplicity 1 and n with multiplicity $n - 1$ (see proof of Theorem 8.2). From Theorem 12.18 thus follows Cayley's formula.

(iii) We now want to connect the street lamps from Example 12.13 such that the total length of the required cables is as small as possible.

Definition 12.20. Let Ω be a (simple) graph. A function $w\colon \Omega_K \to \mathbb{R}$ with $w(a) \geq 0$ for all $a \in K$ is called a *weight function* on Ω. The number $w(\Omega) := \sum_{a \in \Omega_K} w(a)$ is the *total weight* of Ω.

Theorem 12.21 (KRUSKAL's Algorithm). *Let Ω be a connected graph with n vertices and weight function w. The following (greedy[23]) algorithm constructs a spanning tree Δ of Ω with minimal total weight $w(\Delta)$:*

```
(1) Set $\Delta_K := \varnothing$.
(2) For $i = 1, \dots, n-1$ do:
        • Determine $A := \{a \in \Omega_K \setminus \Delta_K : (\Omega_E, \Delta_K \cup \{a\})$ has no cycle$\}$.
        • Choose $a_i \in A$ with $w(a_i) = \min\{w(a) : a \in A\}$.
        • Set $\Delta_K := \Delta_K \cup \{a_i\}$.
```

---

[23] German: gierig

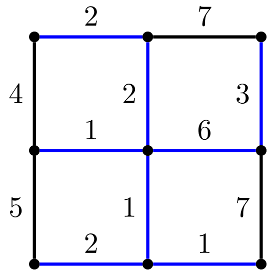
Proof. Suppose in the i-th iteration of the loop $A = \varnothing$ holds. Then Δ must already be connected, because otherwise one could connect two components with a new edge without creating a cycle. Theorem 12.4 yields the contradiction $i - 1 = |\Delta_K| \geq n - 1$. Thus, $A \neq \varnothing$ always holds and a_i can be chosen appropriately. At the end of the algorithm, $|\Delta_K| = n - 1$. Every component Γ of Δ has at most $|\Gamma_E| - 1$ edges, as otherwise a cycle would be present. Since n is the sum over $|\Gamma_E|$, there can only be one component, i. e.. Δ is indeed a spanning tree.

It remains to show that $w(\Delta)$ is minimal. Among all spanning trees with minimal total weight, we choose Δ' such that $|\Delta_K \cap \Delta'_K|$ is as large as possible. Let us assume $\Delta \neq \Delta'$. Let i be minimal with $a_i \notin \Delta'_K$. Now $\Gamma := (\Omega_E, \Delta'_K \cup \{a_i\})$ must possess a cycle. One edge of this cycle, let us call it b_i, does not belong to Δ_K. By removing b_i, one obtains the spanning tree $\Gamma' := \Gamma \setminus \{b_i\}$ with

$$w(\Delta') \leq w(\Gamma') = w(\Delta') + w(a_i) - w(b_i).$$

This shows $w(b_i) \leq w(a_i)$. Since $a_1, \ldots, a_{i-1}, b_i$ are edges of the spanning tree Δ', they cannot contain a cycle. Since the algorithm chose a_i instead of b_i in the i-th iteration of the loop, $w(b_i) \geq w(a_i)$ holds. Overall, we have $w(b_i) = w(a_i)$. Thus, Γ' is also a spanning tree with minimal total weight $w(\Gamma') = w(\Delta')$. On the other hand, $|\Delta_K \cap \Gamma'_K| = |\Delta_K \cap \Delta'_K| + 1$ holds, in contradiction to the choice of Δ'. □

Example 12.22. The following spanning tree (marked in blue) has total weight 18:



Exercises

The following exercises do not necessarily coincide with the homework assignments.

Exercise 1. (In-class exercise) Let $n \in \mathbb{N}$. Find "combinatorial" proofs (i. e. if possible without induction) for the following identities:

(a) $1 + 2 + \ldots + n - 1 = \binom{n}{2}$.

(b) $1 + 3 + 5 + \ldots + 2n - 1 = n^2$.

(c) $1^2 + 2^2 + \ldots + (n-1)^2 = \frac{1}{4}\binom{2n}{3}$.
Hint: Determine the cardinality of $\{(a, b, c) \in \mathbb{N}^3 : a, b < c \leq n\}$ in two ways.

(d) $1\binom{n}{1} + 2\binom{n}{2} + \ldots + n\binom{n}{n} = n2^{n-1}$.

(e) $2^0\binom{n}{0} + 2^1\binom{n}{1} + \ldots + 2^n\binom{n}{n} = 3^n$.

Exercise 2 (3 points)**.** Show

$$\binom{n}{0} < \binom{n}{1} < \ldots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \binom{n}{\lceil n/2 \rceil + 1} > \ldots > \binom{n}{n}$$

for $n \in \mathbb{N}$, where $\lfloor n/2 \rfloor$ denotes rounding down and $\lceil n/2 \rceil$ denotes rounding up.

Exercise 3 (3 points)**.** Let M be a non-empty finite set. Show that M has as many subsets with even cardinality as with odd cardinality. Determine the number of these subsets.

Exercise 4 (3 + 3 points)**.** Let $a_1, \ldots, a_5 \in \mathbb{Z}^2$ be distinct points in the Euclidean plane with integer coordinates. Show that there exist $i \neq j$ such that the midpoint between a_i and a_j also has integer coordinates. How many points would be needed for the analogous statement in Euclidean space $\mathbb{R}^3$?
Hint: Pigeonhole principle.

Exercise 5 (3 + 3 + 3 + 3 points)**.** When juggling, balls are thrown and caught alternately with the left and right hand. The ball thrown at time $k \in \mathbb{N}$ is to be thrown next at time $k + a_k$. The number a_k is thus a measure of the throw height. If a_k is odd, the ball is thrown from the left to the right hand or vice versa. The special case $a_k = 0$ means that no ball is thrown at time k. The art of juggling consists of avoiding that two balls have to be caught at the same time (with the same hand). We therefore call the sequence $a = (a_1, a_2, \ldots) \in \mathbb{N}_0^{\mathbb{N}}$ a *juggling pattern*, if

$$k + a_k \neq l + a_l$$

holds for all $k \neq l$. Let the *height* of a be $h(a) := \max\{a_k : k \in \mathbb{N}\}$ (realistically, the throw height is bounded). Furthermore, a is called *periodic* if there exists a $p \in \mathbb{N}$ with $a_k = a_{k+p}$ for all $k \in \mathbb{N}$. If applicable, one writes $a = (a_1, \dots, a_p)$ and calls the smallest such p the *period* of a. The classical 3-ball juggling pattern ("cascade") is (3). A popular variant is $(4, 4, 1)$. Somewhat more difficult to juggle is $(5, 1)$ ("shower").

Show that:

(a) $(a_1, \dots, a_p) \in \mathbb{N}_0^p$ is a periodic juggling pattern if and only if $1 + a_1, \dots, p + a_p$ is a system of representatives for $\mathbb{Z}/p\mathbb{Z}$. In particular, the *shifts*

$$(a_2, \dots, a_p, a_1), \dots, (a_p, a_1, a_2, \dots, a_{p-1})$$

are then also juggling patterns with the same period.

(b) The number of balls required for a juggling pattern $(a_1, \dots, a_p)$ is $\frac{1}{p}(a_1 + \dots + a_p)$. In particular, this is an integer.

(c) Determine all periodic 3-ball juggling patterns with period 3 and height ≤ 5 up to shifts.

(LA) Prove with a video that you can juggle the pattern $(5, 0, 1)$ for at least 30 seconds.

Remark: Ron Graham (1935–2020) was one of the most famous discrete mathematicians and at the same time a 6-ball juggler.

Exercise 6 (In-class exercise)**.** Prove without induction the multinomial theorem

$$(a_1 + \dots + a_n)^k = \sum_{\substack{(k_1,\dots,k_n) \in \mathbb{N}_0^n \\ k_1 + \dots + k_n = k}} \binom{k}{k_1, \dots, k_n} a_1^{k_1} \dots a_n^{k_n}$$

for $a_1, \dots, a_n \in \mathbb{C}$ and $k \in \mathbb{N}$.

Exercise 7 ($2 + 3 + 3$ points)**.** Answer the following questions with justification:

(a) How many subsets of $\{1, \dots, 12\}$ contain at least one even number?

(b) How many ways are there to arrange the letters of POSSESSES such that the five S are not all next to each other?

(c) In how many ways can one put together a bouquet with 12 flowers if roses, tulips, and dahlias are available in any quantity?

Exercise 8 ($3 + 3$ points)**.** Show that

$$\sum_{k=0}^{m} \left(\!\binom{n}{k}\!\right) = \left(\!\binom{n+1}{m}\!\right),$$

$$\sum_{k=1}^{n} \binom{n}{k} \left(\!\binom{k}{m-k}\!\right) = \left(\!\binom{n}{m}\!\right)$$

for all $n, m \in \mathbb{N}$.
Hint: Count multisets (no calculation is necessary).

Exercise 9 (4 points)**.** How many natural numbers $\leq 10^5$ are neither square numbers nor cubic numbers nor divisible by 5?
Hint: Inclusion-Exclusion Principle.

Exercise 10 (LA, $1+2+2$ points)**.**

(a) Calculate $\varphi(750)$.

(b) Determine the preimage $\varphi^{-1}(14)$.
Remark: An open conjecture by CARMICHAEL states that $|\varphi^{-1}(n)| \neq 1$ for all $n \in \mathbb{N}$.

(c) Determine the prime factorization of 626.257.
Hint: $\varphi(626.257) = 624.640$.

Exercise 11 (In-class exercise)**.** Let $A_n = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = 1\}$ be the alternating group of degree $n \geq 2$. As in Theorem 2.10, let $z_k(\sigma)$ be the number of k-cycles of $\sigma \in S_n$.

(a) Calculate $\sum_{\sigma \in A_n} z_k(\sigma)$ for $1 \leq k \leq n$.
Hint: Consider the special cases $k \in \{n-1, n\}$.

(b) Show that $\sigma \in A_n$ has on average $H_n + \frac{(-1)^n}{(n-1)n}$ cycles.

Exercise 12 ($2+4+3$ points)**.** A *composition* of $n \in \mathbb{N}$ with t parts is a tuple $(a_1, \ldots, a_t) \in \mathbb{N}^t$ with $a_1 + \ldots + a_t = n$. In contrast to partitions, the order of the a_i shall be taken into account. Let $k_t(n)$ be the number of compositions of n with t parts.

(a) Determine all compositions of 7 with three parts.

(b) Show that $k_t(n) = \binom{n-1}{t-1}$ for all $1 \leq t \leq n$.
Hint: $1\,2 \mid 3\,4\,5 \mid 6 \mid 7\,8\,9$ or $(a_1, \ldots, a_t) \mapsto \{a_1, a_1 + a_2, \ldots, a_1 + \ldots + a_{t-1}\}$.

(c) Calculate the number $k(n)$ of all compositions of n with an arbitrary number of parts. (This is surprisingly much easier than calculating $p(n)$.)

Exercise 13 ($4+4+2$ points)**.** Let p be a prime number. Show:

(a) For natural numbers $0 \leq k < n$, it holds that

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{0 < a_1 < \ldots < a_{n-k} < n} a_1 \ldots a_{n-k}.$$

Hint: Theorem 2.17.

(b) In $\mathbb{F}_p[X]$, it holds that $X^p - X = X(X+1) \ldots (X+p-1)$.
Hint: Polynomial method.

(c) For $1 < k < p$, $\begin{bmatrix} p \\ k \end{bmatrix}$ is divisible by p.

Exercise 14 (LA, $2+2+2$ points)**.**

(a) Write $(1,2,3,4)(7,6,5,4,3)$ as a product of disjoint cycles and as a product of transpositions.

(b) Calculate $\begin{bmatrix} 7 \\ 4 \end{bmatrix}$.

(c) Determine all partitions of 7.

Exercise 15 (In-class exercise)**.** Let $a, b, c_0, c_1 \in \mathbb{C}$ be given and we seek a sequence of numbers $x = (x_0, x_1, \ldots) \in \mathbb{C}^{\mathbb{N}_0}$ that satisfies the following *second-order recurrence equation*:

$$x_0 = c_0, \qquad x_1 = c_1, \qquad x_n = ax_{n-1} + bx_{n-2} \qquad (n \geq 2).$$

Let $\lambda, \mu \in \mathbb{C}$ be the roots of $X^2 - aX - b$. Show:

(a) In the case $\lambda = \mu$, $x_n = c_0(1-n)\lambda^n + c_1 n\lambda^{n-1}$ for all $n \in \mathbb{N}_0$.

(b) In the case $\lambda \neq \mu$, $x_n = \frac{c_1 - \mu c_0}{\lambda - \mu}\lambda^n + \frac{\lambda c_0 - c_1}{\lambda - \mu}\mu^n$ for all $n \in \mathbb{N}_0$.

Exercise 16 $(4+4+4+4$ points$)$**.**

(a) Calculate $\left\{ {7 \atop 4} \right\}$ and $b(6)$.

(b) Show

$$\left[{n+1 \atop 2} \right] = n!H_n$$

for $n \in \mathbb{N}$, where H_n is the n-th harmonic number.

(c) Show

$$\left[{n \atop n-2} \right] = 2\binom{n}{3} + 3\binom{n}{4}$$

for all $n \geq 2$.
Note: Theorem 2.25.

(d) Find and prove an analogous formula for $\left\{ {n \atop n-2} \right\}$.

Exercise 17 (4 points)**.** A Corona model: Every newly infected person infects approx. 0,8 people in the first week, in the second week they infect approx. 0,1 people (quarantine shows effect) and in the third week they are recovered or dead. Let c_n be the number of all Corona-infected people in Hannover in week n. The values from last and this week are $c_0 = 3372$ and $c_1 = 3316$. Calculate c_{21} (period of the retake exam).
Note: Divide c_n into "old" and "newly" infected.

Exercise 18 (LA, 4 points)**.** Let $w(n)$ be the probability that in a city with n inhabitants, at least one inhabitant has a birthday on every day of the year (without leap year). Determine the smallest n with $w(n) > \frac{1}{2}$.
Note: You may use WolframAlpha or a computer algebra system.

Exercise 19 (In-class exercise)**.** Let K be a field. A sum of the form $\sum_{n=-\infty}^{\infty} a_n X^n$ with $a_n \in K$ for $n \in \mathbb{Z}$ is called a (formal) *Laurent series*, if $|\{n \leq 0 : a_n \neq 0\}| < \infty$. Show that the set $K((X))$ of all Laurent series with the operations

$$\sum a_n X^n + \sum b_n X^n = \sum (a_n + b_n) X^n,$$
$$\sum a_n X^n \cdot \sum b_n X^n = \sum_{n=-\infty}^{\infty} \Big(\sum_{k=-\infty}^{\infty} a_k b_{n-k} \Big) X^n$$

becomes a field.
Note: Do not forget to check the well-definedness of addition and multiplication.

Exercise 20 (4 + 4 points)**.** According to Lemma 4.8, $\alpha := 1 - X - X^2 \in \mathbb{C}[[X]]$ is invertible.

(a) Calculate the first seven coefficients of $\frac{1}{\alpha}$ (i.e., up to X^6). Do you recognize a pattern?

(b) Determine the partial fraction decomposition of $\frac{1}{\alpha}$ as in Example 4.10(ii) and expand the resulting geometric series according to 4.10(i).

Exercise 21 (4 + 4 points)**.** The *Bernoulli numbers* $B_n \in \mathbb{Q}$ are defined via their generating function:

$$\frac{X}{\exp(X) - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} X^n.$$

(a) Determine B_0 and prove

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

for $n \geq 2$. Compare with Theorem 2.37 (no points are given for this).

(b) Prove $B_{2n+1} = 0$ for $n \in \mathbb{N}$.
Hint: Compare $\alpha := \sum_{k \neq 1} \frac{B_k}{k!} X^k$ with $\alpha(-X)$.

Exercise 22 (4 points)**.** Show that S_{2n} has exactly $(2n-1)!! := 1 \cdot 3 \cdot \ldots \cdot (2n-1)$ fixed-point-free permutations of order 2. How many such permutations does S_{2n+1} have?

Exercise 23 (LA, 2 + 2 + 2 points)**.** Let

$$\begin{aligned}\sin(X) &:= \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} X^{2n+1} \in \mathbb{C}[[X]],\\ \cos(X) &:= \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} X^{2n} \in \mathbb{C}[[X]].\end{aligned}$$

Show:

(a) (EULER's formula) $\exp(\mathrm{i}X) = \cos(X) + \mathrm{i}\sin(X)$, where $\mathrm{i} = \sqrt{-1} \in \mathbb{C}$.

(b) $\sin(2X) = 2\sin(X)\cos(X)$ and $\cos(2X) = \cos(X)^2 - \sin(X)^2$.

(c) ("trigonometric Pythagoras") $\sin(X)^2 + \cos(X)^2 = 1$.

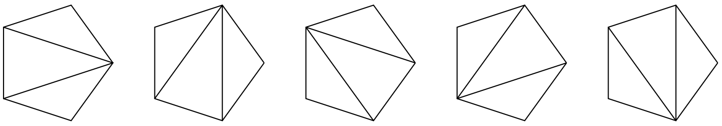
Hint: Your solution should be independent of analysis.

Exercise 24 (In-class exercise)**.** In Example 4.21(ii), the Catalan numbers were defined by $C_1 := 1$ and $C_n := \sum_{k=1}^{n-1} C_k C_{n-k}$ for $n \geq 2$. Show for $n \geq 2$:

(a) C_n is the number of ways to parenthesize n elements of a group. For example $C_4 = 5$:

$$x_1(x_2(x_3x_4)), \qquad x_1((x_2x_3)x_4), \qquad (x_1x_2)(x_3x_4), \qquad ((x_1x_2)x_3)x_4, \qquad (x_1(x_2x_3))x_4.$$

(b) C_n is the number of ways to draw $n-2$ diagonals in a convex $(n+1)$-gon that do not intersect:



Remark: R. P. Stanley's book "Catalan numbers" contains 214 interpretations of C_n.

Exercise 25 (4 points)**.** Calculate the first ten coefficients (up to X^9) of the inverse function of $X - X^3 \in \mathbb{C}[[X]]^\circ$ (many of the coefficients are 0). Enter the non-zero coefficients at `https://oeis.org/`.
Note: Example 4.21(ii).

Exercise 26 $(4+4$ points$)$**.**

(a) Construct power series $\alpha, \beta, \gamma \in \mathbb{C}[[X]]$, such that

$$\alpha \circ \beta \neq \beta \circ \alpha, \qquad \alpha \circ (\beta + \gamma) \neq \alpha \circ \beta + \alpha \circ \gamma, \qquad \alpha \circ (\beta\gamma) \neq (\alpha \circ \beta)(\alpha \circ \gamma).$$

(b) We proved in Theorem 4.19 that every element in $\mathbb{C}[[X]]^\circ$ has an inverse function. However, there are other power series with inverse functions. Construct $\alpha, \beta \in \mathbb{C}[[X]] \setminus \mathbb{C}[[X]]^\circ$ with $\alpha(\beta) = \beta(\alpha) = X$.

Exercise 27 (4 points)**.** For $k \in \mathbb{N}_0$ let

$$\binom{X}{k} := \frac{X(X-1)\ldots(X-k+1)}{k!} \in \mathbb{Q}[X]$$

(already used in the proof of the Vandermonde identity). Let $\alpha \in \mathbb{C}[X]$ be a polynomial with $\alpha(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. Show that α can be uniquely written in the form

$$\alpha = \sum_{k=0}^{\infty} a_k \binom{X}{k}$$

with $a_k \in \mathbb{Z}$. Conclude $\alpha \in \mathbb{Q}[X]$.
Note: Polynomial method.

Exercise 28 (LA, $2+2+2$ points)**.** As a supplement to Exercise 23, let

$$\tan(X) := \frac{\sin(X)}{\cos(X)},$$
$$\arctan(X) := \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} X^{2n+1}.$$

Show:

(a) $\sin(X)' = \cos(X)$ and $\cos(X)' = -\sin(X)$.

(b) $\arctan \circ \tan = X$.
Hint: First check $\tan \in \mathbb{C}[[X]]^\circ$. Then differentiate.

(c) $\arctan(X) = \frac{\mathrm{i}}{2}\log\left(\frac{\mathrm{i}+X}{\mathrm{i}-X}\right)$ with $\mathrm{i} = \sqrt{-1} \in \mathbb{C}$.
Hint: Check that $\log\left(\frac{\mathrm{i}+X}{\mathrm{i}-X}\right)$ is well-defined.

Remark: There are countless other trigonometric identities, but not all can be proven via formal power series. For example, cos has no formal inverse function (nevertheless, one can specify the analytical Taylor series for arccos).

Exercise 29 (Puzzle task for the excursion week, 4^* points)**.** Show that for every natural number $n \in \mathbb{N}$ there exists a number $a \in \mathbb{N}$ that is divisible by n and consists only of the digits 0 and 1.

Exercise 30 (In-class exercise)**.** Prove for all $\alpha \in \mathbb{C}[[X]]$:

$$\prod_{k=0}^{\infty}(1+\alpha X^k) = \sum_{k=0}^{\infty}\frac{\alpha^k X^{\binom{k}{2}}}{X^k!}, \qquad \prod_{k=1}^{\infty}\frac{1}{1-\alpha X^k} = \sum_{k=0}^{\infty}\frac{\alpha^k X^k}{X^k!}.$$

Remark: These equations continue the Gaussian binomial theorem, just as Newton's binomial theorem continues the ordinary binomial theorem.

Exercise 31 ($4+4+3$ points)**.**

(a) Write the generating function of the square numbers $0, 1, 4, 9, 16, \ldots$ as a quotient of polynomials.
Hint: Follow the example in Example 5.2.

(b) Let a_n be the number of ways to compose n Eurocents using any number of 1-, 2- and 5-cent coins. Write the generating function of a_n as a product of geometric series.

(c) Interpret the coefficients of the power series $\prod_{n=0}^{\infty}(1+X^{2^n})$ combinatorially. Can the series be expressed more simply?

Exercise 32 ($3+3+3^*$ Punkte)**.** Let $n, d \in \mathbb{N}$. Prove:

(a) (GLAISHER) The number of partitions of n whose parts are not divisible by d is equal to the number of partitions of n in which no part occurs d times (or more).
Hint: The case $d = 2$ corresponds to Theorem 5.6(i).

(b) (MACMAHON) The number of partitions of n where each part occurs at least twice is equal to the number of partitions of n into parts that do not have the form $\pm 1 + 6k$.

(c) (SUBBARAO) The number of partitions of n where each part occurs exactly twice, three times, or five times is equal to the number of partitions of n into parts of the form $\pm 2 + 12k$, $\pm 3 + 12k$, or $6 + 12k$.

Exercise 33 (LA, $4+2$ Punkte)**.**

(a) Let $k, n \in \mathbb{N}$ and F_n be the n-th Fibonacci number, where $F_0 = 0$. Show $F_{n+k} = F_n F_{k-1} + F_{n+1} F_k$ and derive from this the CATALAN *identity* $F_n^2 - F_{n+k}F_{n-k} = (-1)^{n+k}F_k^2$.

(b) Determine all symmetric partitions of $n = 15$ and draw their Young diagrams.

Exercise 34 (Präsenzaufgabe)**.** In Doppelkopf, 48 playing cards are distributed equally among four players. However, each playing card is present exactly twice (so there are 24 pairwise distinct cards). Let A be the number of possible distributions, where the four players are distinguished. We consider polynomials in four unknowns X_1, X_2, X_3, X_4. Show:

(a) A is the coefficient of $X_1^{12}X_2^{12}X_3^{12}X_4^{12}$ in

$$\Big(\sum_{1\le i\le j\le 4} X_iX_j\Big)^{24}.$$

(b)

$$A = \frac{24!}{2^{24}} \sum_{a_1,a_2,a_3,a_4=0}^{6} \frac{1}{(24-a_1-\ldots-a_4)!a_1!\ldots a_4!}\binom{48-2a_1-\ldots-2a_4}{12-2a_1,\ldots,12-2a_4}.$$

Hint: $\sum_{1\le i\le j\le 4} X_iX_j = \frac{1}{2}(X_1+X_2+X_3+X_4)^2 + \frac{1}{2}(X_1^2+X_2^2+X_3^2+X_4^2)$

Remark: Using a computer, one calculates $A = 2.248.575.441.654.260.591.964$.

Exercise 35 (4 Punkte)**.** Let K be a field with $q < \infty$ elements and let V be an n-dimensional vector space over K. Let $\left\langle {n \atop k} \right\rangle_q$ be the value of the polynomial $\left\langle {n \atop k} \right\rangle$ at $X = q$. Show that $\left\langle {n \atop k} \right\rangle_q$ is the number of k-dimensional subspaces of V.
Hint: How many k-tuples of linearly independent vectors are there and how many of them generate the same subspace?

Exercise 36 ($2+4$ points)**.** Let G be a finite group acting on a set $\Omega \neq \varnothing$. Show:

(a) By

$$x \sim y \;:\Longleftrightarrow\; \exists g \in G : \langle gxg^{-1}\rangle = \langle y\rangle \qquad (x, y \in G)$$

an equivalence relation on G is defined. Let $x_1, \ldots, x_k \in G$ be a system of representatives for the equivalence classes with respect to $\sim$. For $i = 1, \ldots, k$ let $[x_i]$ be the equivalence class of x_i.

(b) For $x \in G$ let $f(x)$ be the number of fixed points of x on Ω. Then

$$\frac{1}{|G|}\sum_{i=1}^{k} |[x_i]| f(x_i)$$

is the number of orbits of G on Ω.
Remark: This accelerates Burnside's Lemma (provided one knows G well enough).

Exercise 37 ($3+3+3^*$ points)**.** We want to color a tetrahedron and have n colors available for this. How many possibilities are there

(a) to color the four vertices?

(b) to color the six edges?

(c) to color vertices, edges and faces simultaneously?

Note: With the notation from Exercise 36, $|G| = 12$ and $k = 3$.

Exercise 38 (LA, 4 points)**.** A *triad* consists of three different tones within an octave $(c, cis, \ldots, b, h)$. Since most of us do not have absolute pitch, we consider two triads as identical if they differ only by transposition. Accordingly, there is only one major triad $(\{c, e, g\})$ and one minor triad $(\{a, c, e\})$. How many triads are there in total?

Exercise 39 (In-class exercise)**.** One can generalize Pólya's Theorem by allowing negative values, i.e., functions $w\colon \Delta \to \mathbb{Z}$. Then $W(X)$ becomes a *Laurent polynomial* (a finite Laurent series, cf. Exercise 19). The proof of Pólya's Theorem remains valid. Count in this way the necklaces with five beads in the colors red, blue, green, black, in which exactly as many red as blue beads occur.
Remark: Pólya's Theorem can also be formulated with polynomials in several variables.

Exercise 40 $(3 + 2$ points$)$**.** Let Ω be a simple graph with $|\Omega_E| > 1$. Show that Ω has two vertices of the same degree. Does the statement also hold for multigraphs?

Exercise 41 $(3 + 4$ points$)$**.** Let Ω be a simple graph. Prove or disprove the following statements:

(a) If Ω is connected, then Ω^C is disconnected.

(b) If Ω is disconnected, then Ω^C is connected.

Exercise 42 $(2 + 2 + 3$ points$)$**.** The n-dimensional *hypercube graph* $\mathcal{W}_n$ has vertex set $\{0, 1\}^n$. Two vertices are connected by an edge if and only if they differ in exactly one coordinate.

(a) Draw $\mathcal{W}_3$.

(b) Calculate the number of edges of $\mathcal{W}_n$.

(c) Let e be an arbitrary vertex of $\mathcal{W}_n$. Check whether $\mathcal{W}_n \setminus \{e\}$ is connected.

Exercise 43 (LA, $2 + 3$ points)**.** Let the trivial graph $\Omega := \mathcal{T}_n$ be given. Euler and Hamilton play the following game: Euler connects two arbitrary vertices of Ω with an edge, where loops at a vertex are also allowed. Subsequently, he draws a new vertex on the new edge. Now Hamilton proceeds in the same way, then Euler again, and so on. The edges must not intersect and the degree of each vertex shall be at most 3. Whoever is the first to be unable to draw an edge loses.

(a) Show that the game ends after at most $3n - 1$ moves.

(b) Show that Hamilton can force a win in the case $n = 2$.

Exercise 44 (In-class exercise)**.** Let $G = \langle X \rangle$ be a finite group with generating set X. The elements of G are the vertices of the *Cayley graph* $\Omega(G, X)$ of G. Two vertices $g, h \in G$ form an edge if and only if $gh^{-1} \in X$ or $hg^{-1} \in X$ holds.

(a) Show that $\Omega(G, X)$ is connected and regular.

(b) Let $\sigma \in D_8$ be the rotation by 90° and $\tau \in D_8$ a reflection. Draw $\Omega(D_8, \{\sigma, \tau\})$.

(c) Prove that $\Omega(D_{2n}, \{\sigma, \tau\})$ is Hamiltonian, where σ is now a rotation by $2\pi/n$.

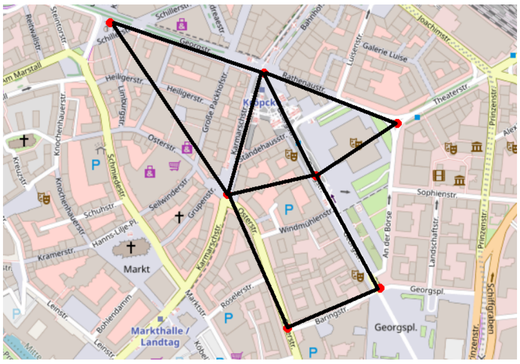
Remark: The *Lovász conjecture*[24] states that $\Omega(G, X)$ is always Hamiltonian for $|G| > 2$. Even for $G = D_{2n}$ and $|X| = 3$, this is still open.

Exercise 45 $(3 + 3$ points$)$**.**

(a) Hanover is divided by the Leine and Ihme rivers similarly to Königsberg:

Check whether there exists a closed path in which exactly five of the six bridges are crossed once each (the sixth bridge shall not be crossed, other edges may be used as often as desired).

(b) Determine the number of Hamiltonian cycles in the following graph:



Two Hamiltonian cycles shall be considered identical if they differ only by the starting point or the direction of travel.

Exercise 46 $(1 + 2 + 3$ points$)$**.** Let $\mathcal{W}_n$ be the cube graph from Exercise 42.

(a) Investigate when $\mathcal{W}_n$ is Eulerian?

(b) Provide a Hamiltonian cycle in $\mathcal{W}_3$.

(c) Prove that $\mathcal{W}_n$ is Hamiltonian for all $n \geq 2$.
Hint: Induction on n.

---

[24] Lovász received the Abel Prize in 2021, one of the highest mathematical awards.

Exercise 47 ($2 + 3 + 3^*$ points)**.** Let $\mathcal{S}_n$ be the star graph and $A = A(\mathcal{S}_n)$ its adjacency matrix.

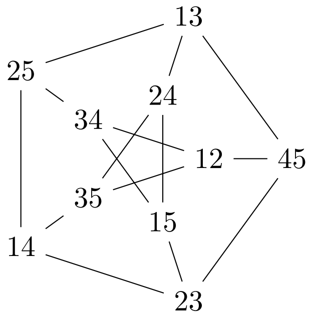
(a) Show that A has the eigenvalue 0 with algebraic multiplicity $n - 2$.

(b) Determine the number of all closed walks of length l in $\mathcal{S}_n$ for $l \in \mathbb{N}$.

(c) Calculate the two missing eigenvalues of A using (b).
Hint: You may also calculate the eigenvalues directly if that is easier.

Exercise 48 (LA, 3 points)**.** For a children's birthday party, we are making garlands with 8 pennants in 4 possible colors. For aesthetic reasons, the first pennant should be red and the last one blue. Furthermore, no two pennants of the same color should be adjacent. How many such garlands can be made?
Hint: Count walks in a graph.

Exercise 49 (In-class exercise)**.** We label the ten vertices of the Petersen graph Ω with the 2-element subsets of $\{1, \dots, 5\}$ (for better clarity, we omit commas and set braces):



Show:

(a) Two vertices A and B of Ω form an edge if and only if $A \cap B = \varnothing$.

(b) The natural action of S_5 on $\binom{\{1,\dots,5\}}{2}$ induces an injective group homomorphism $\alpha\colon S_5 \to \operatorname{Aut}(\Omega)$.

(c) $\operatorname{Aut}(\Omega) \cong S_5$.
Hint: Show $|\operatorname{Aut}(\Omega)| \leq 5!$ using the orbit-stabilizer theorem.

Exercise 50 ($3 + 3 + 3^*$)**.** Let $\mathcal{W}_n$ be the cube graph and $A := \operatorname{Aut}(\mathcal{W}_n)$. We interpret the vertices of $\mathcal{W}_n$ as vectors in $\mathbb{F}_2^n$. Show:

(a) For $\pi \in S_n$, $\alpha_\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, $(a_1, \dots, a_n) \mapsto (a_{\pi(1)}, \dots, a_{\pi(n)})$ is an automorphism of $\mathcal{W}_n$.

(b) For $x \in \mathbb{F}_2^n$, $\beta_x\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, $v \mapsto x + v$ is an automorphism of $\mathcal{W}_n$.

(c) For $\gamma \in A$, there exist uniquely determined $\pi \in S_n$ and $x \in \mathbb{F}_2^n$ such that $\gamma = \alpha_\pi \circ \beta_x$. In particular, $|A| = (2n)!! = 2^n n!$.

Remark: If one replaces $\mathbb{F}_2^n$ with $\{1, -1\}^n$, then A is the symmetry group of the hypercube in $\mathbb{R}^n$ (*Weyl group* of type (B_n)). For the ordinary cube ($n = 3$), one obtains $A \cong S_4 \times C_2$.

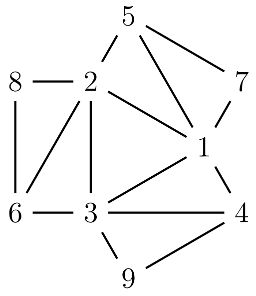
Exercise 51 ($3 + 4 + 3^*$ points)**.**

(a) Determine the number of 3-regular graphs with six vertices up to isomorphism.
Hint: Complement.

(b) Let $0 \leq k < n$. Prove that there exists a k-regular simple graph with n vertices if and only if $2 \mid kn$.

(c) Let $f_k(n)$ be the number of connected k-regular graphs with n vertices up to isomorphism. Some values are listed on Wikipedia. Strikingly, $f_7(16) + 1 = f_8(16)$. Prove this equation (without calculating $f_7(16)$).

Exercise 52 (4 points)**.** Determine the automorphism group of the graph:



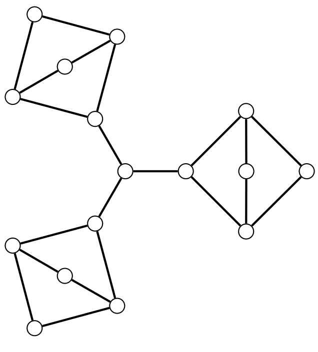
Exercise 53 (LA, $2 + 2$ points)**.** Draw all graphs with exactly five vertices and five edges up to isomorphism. For each of these graphs, provide a non-trivial automorphism.

Exercise 54 (In-class exercise)**.** Let $1 \leq k \leq n$ and $N := \{1, \ldots, n\}$. A matrix $A \in N^{n \times k}$ is called a *Latin rectangle*, if in each row and in each column of A no number occurs more than once. In the case $n = k$, A is called a *Latin square*. Show that every Latin rectangle can be completed to a Latin square by adding $n - k$ columns.
Hint: Consider the bipartite graph Ω with $\Omega_E = \{0, 1\} \times N$ and

$$\{(0, i), (1, j)\} \in \Omega_K \ :\Longleftrightarrow \ i \text{ does \textit{not} occur in the } j\text{-th row of } A.$$

Show that Ω is $(n - k)$-regular and apply Hall's Marriage Theorem.

Exercise 55 ($2 + 2$ points)**.** Investigate whether the following graph is bipartite and whether a perfect matching exists:



Exercise 56 ($2+2+3+3^*$ points)**.**

(a) Show that the hypercube graph $\mathcal{W}_n$ is bipartite.

Now assume that $\mathcal{W}_n$ is planar.

(b) Calculate the number of faces of a planar embedding of $\mathcal{W}_n$.

(c) By how many edges is such a face bounded?

(d) Show that $n \leq 3$.

Exercise 57 (2+3 points)**.** Let $d_1 \geq d_2 \geq \ldots \geq d_n \geq 0$ be integers. Show that the following statements are equivalent:

(a) There exists a multigraph Ω with $\Omega_E = \{e_1, \ldots, e_n\}$ and $\deg(e_i) = d_i$ for $i = 1, \ldots, n$.

(b) $\sum_{i=1}^n d_i$ is even and $d_1 \leq \sum_{i=2}^n d_i$.

Hint: For (b)⇒(a) one can argue by induction.

Exercise 58 (LA, 4 points)**.** The convex hull P of finitely many points in $\mathbb{R}^3$ that do not lie in a plane is called a (convex) *polyhedron* (for example cuboid, pyramid, prism etc.). Geometrically, P is bounded by vertices, edges and faces. P is called *regular* if all faces are congruent regular polygons and each vertex bounds the same number of faces. As shown in the lecture, the vertices of every polyhedron form a planar graph by "breaking open" one face. Show using Euler's polyhedron formula that there are exactly five regular polyhedra (up to rotation, translation and scaling).
Remark: Weakening the regularity condition leads to less known but equally fascinating objects like the Catalan solids.

The following problems were not given as part of the lecture.

Exercise 59 (Discrete intermediate value theorem)**.** Let $f\colon \mathbb{Z} \to \mathbb{Z}$ and $a < b$ with $f(a) \leq 0 \leq f(b)$. For $a < k \leq b$ let $f(k) - f(k-1) \leq 1$. Then there exists a c with $a \leq c \leq b$ and $f(c) = 0$.

Exercise 60. Let A be a subset of $\{1, \ldots, 140\}$ with 71 elements. Are there always $a, b \in A$ with $|a-b| = 10$? What is the answer in the case $|A| = 70$?
Hint: Pigeonhole principle with 10 pigeonholes.

Exercise 61. Let $n \in \mathbb{N}$ and $A \subseteq \{1, \ldots, 2n\}$ with $|A| = n+1$. Show:

(a) A contains two coprime numbers.

(b) There exist $a, b \in A$ with $a \neq b$ and $a \mid b$.

Exercise 62. Ten children are standing in a row during physical education. Show that there are three boys or three girls standing at equal distances from each other (e. g. at positions $3, 5, 7$ or $1, 5, 9$). Is this still true if one is missing?
Remark: The theorem of VAN DER WAERDEN states more generally: If the natural numbers are divided

into two classes, then for every k there exist numbers a, d such that $a, a+d, a+2d, \dots, a+kd$ lie in one class.[25]

Exercise 63. In *Fischer random chess* (or Chess960), pieces are placed randomly according to the following rules:

- The eight white pawns occupy the second rank as usual.
- The remaining eight white pieces (2 rooks, 2 knights, 2 bishops, queen, and king) occupy the first rank.
- The two white bishops must occupy squares of opposite colors (one black and one white square).
- The white king must be placed between the two white rooks.
- The black pieces in ranks 7 and 8 are placed mirror-symmetrically (across the horizontal) to the corresponding white pieces.

How many possible starting positions are there?

Exercise 64. Let $0 < k \leq l < n$ be natural numbers. Show that $\binom{n}{k}$ and $\binom{n}{l}$ have a common divisor > 1.
Hint: $\binom{n}{l}\binom{l}{k} = \binom{n}{k}\binom{n-k}{l-k}$.

Exercise 65. Every permutation $\sigma \in S_n$ can be uniquely written as a product of disjoint cycles

$$\sigma = (a_1, \dots, a_k)(b_1, \dots, b_l) \dots$$

if one requires $a_1 = \max\{a_1, \dots, a_k\} < b_1 = \max\{b_1, \dots, b_l\} < \dots$ (cf. Remark 2.8). Here, we also include the 1-cycles. Show that the map

$$\begin{aligned} \Psi \colon S_n &\to S_n, \\ \sigma &\mapsto \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & k+2 & \cdots & k+l & \cdots \\ a_1 & a_2 & \cdots & a_k & b_1 & b_2 & \cdots & b_l & \cdots \end{pmatrix} \end{aligned}$$

is bijective. Ψ is called the FOATA *transformation.*

Exercise 66 (Coin problem)**.** Suppose you possess an unlimited number of coins with values of a and b euros, where $a, b \in \mathbb{N}$ are coprime. Show that:

(a) You cannot pay the amount of $ab - a - b$ euros exactly (without change).

(b) You can pay every integer euro amount greater than $ab - a - b$.

Exercise 67. Investigate which of the Catalan numbers C_n are odd.
Hint: Consider $\alpha^2 - \alpha = X$ modulo 2.

---

[25] See Number Theory Notes

Exercise 68. Let $\Delta := \{(x, y, z) \in \mathbb{R}^3 : |x|, |y|, |z| \leq 1\} \subseteq \mathbb{R}^n$ be the unit cube and

$$G := \big\{f \in \mathrm{GL}(\mathbb{R}^3) : f(\Delta) = \Delta\big\} \leq \mathrm{GL}(\mathbb{R}^3)$$

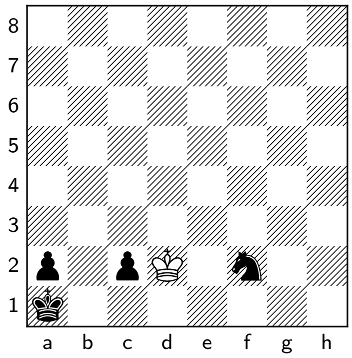
be the symmetry group of Δ.

(a) Show that G acts transitively on the set of the six faces of Δ.

(b) Calculate $|G|$ by iterated application of the orbit-stabilizer theorem.

Exercise 69. How many ways are there to connect two 4×2 Lego bricks of the same color, where the resulting angle is divisible by $90°$.

Exercise 70 (Elkies)**.** In the following chess game, it is White's turn to move:



Show:

(a) If the white king captures the pawn on c2, then Black can force a win.
Hint: Black wins as soon as the pawn on a2 is promoted to a queen.

(b) White can force a draw.
Hint: As long as the white king stays on the squares c1 and c2, Black can only move the knight. Examine the graph of the knight's tour problem (Example 7.12).

Exercise 71. Determine all trees with exactly two or three leaves up to isomorphism.

Exercise 72. Draw all non-isomorphic trees with 10 vertices, none of which have degree 2.
Remark: This problem is solved incompletely in the Oscar-winning feature film "Good Will Hunting". See Youtube.

Exercise 73. Let $\Omega = (\Omega_E, \Omega_K)$ be a simple graph. We define a relation $\leq$ on $M := \Omega_E \cup \Omega_K$ by:

$$x < y \;:\Longleftrightarrow\; x \in \Omega_E, y \in \Omega_K, x \in y.$$

(a) Show that $(M, \leq)$ is a partially ordered set.

(b) The automorphism group $\mathrm{Aut}(M)$ consists of all permutations $\gamma \in \mathrm{Sym}(M)$ with $\gamma(x) \leq \gamma(y) \iff x \leq y$ for all $x, y \in M$. Show that $\mathrm{Aut}(M) \cong \mathrm{Aut}(\Omega)$.

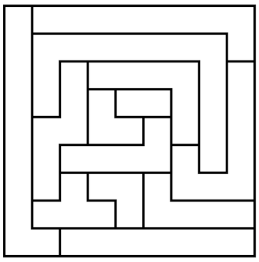
Exercise 74. Let $(M, \leq)$ be a partially ordered set. A subset $U \subseteq M$ is called *open* if for all $u \in U$ and $v \in M$ the following holds: $v \leq u \Longrightarrow v \in U$.

(a) Show that the open sets form a topology T on M. T is called the *Alexandroff topology*.

(b) The automorphism group $\mathrm{Aut}(T)$ consists of all permutations $\gamma \in \mathrm{Sym}(M)$ such that $U \subseteq M$ is open if and only if $\gamma(U)$ is open.[26] Show that $\mathrm{Aut}(T) \cong \mathrm{Aut}(M)$.

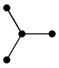
Remark: According to Frucht and Exercise 73, for every finite group G there exists a graph, a partially ordered set, and a topological space with automorphism group G.

Exercise 75. Color the following faces with at most four different colors such that adjacent faces are colored differently.



Exercise 76. Let Ω be a graph with at least one edge. The *line graph* $\widehat{\Omega}$ of Ω is defined by $\widehat{\Omega} := (\Omega_K, \Delta)$, where $\{x, y\} \in \Delta :\Leftrightarrow x \cap y \neq \varnothing$ for distinct $x, y \in \Omega_K$.

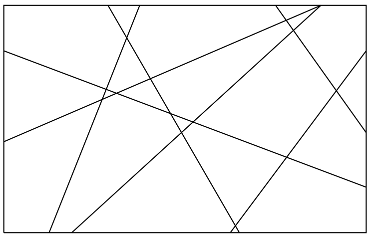
(a) Determine the line graphs $\widehat{\mathcal{G}_n}$, $\widehat{\mathcal{K}_n}$ and $\widehat{\mathcal{S}_n}$ up to isomorphism.

(b) Show that the graph  is *not* a line graph.

(c) Let Ω be a graph with $\widehat{\Omega} \cong \Omega$. Show that every connected component of G is a cycle.
Hint: Examine the degrees of the vertices.

Exercise 77. Show that $\chi(\Omega)\chi(\Omega^C) \geq n$ for every graph Ω with n vertices.
Hint: $\chi(\Omega)\chi(\Omega^C)$ is the cardinality of an obvious set...

Exercise 78. Let a rectangular area be divided into smaller areas by straight lines. How many colors are needed to color each of the small areas such that adjacent areas are colored differently?



Hint: Theorem 10.5.

---

[26] These are the homeomorphisms from analysis.

Exercise 79. Assume the four-color theorem is false. Then there exists a counterexample Ω such that $|\Omega_E| + |\Omega_K|$ is minimal among all counterexamples. Show:

(a) Ω is simple and connected.

(b) Every vertex of Ω has degree ≥ 4.

(c) Ω has no *bridges*. A bridge is an edge $k \in \Omega_K$ such that $\Omega \setminus \{k\}$ is disconnected.

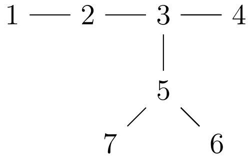
(d) For $a, b, c \in \Omega_K$, $\Omega \setminus \{a, b, c\}$ is always connected.

Exercise 80. Explain why the family tree of all humans born in the last 1000 years cannot be a *tree*.

Exercise 81. Show that every tree has a vertex or edge that is fixed by all automorphisms.
Hint: Induction on the number of vertices.

Exercise 82.

(a) Determine the Prüfer code of the tree

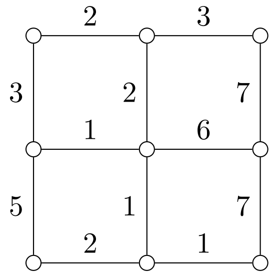


(b) Describe the trees with Prüfer code $(1, 2, \ldots, n-2)$ and $(1, \ldots, 1)$.

Exercise 83. The atomic structure of *alkanes* can be realized by trees whose leaves are hydrogen atoms (H) and all other vertices have degree 4 and are carbon atoms (C). Let a_n be the number of these compounds with n C-atoms up to graph isomorphism. It holds that $a_1 = a_2 = a_3 = 1$ (methane, ethane, propane). For $n \geq 4$, $a_n > 1$ (this phenomenon is called *isomerism*). Calculate a_6 and draw the corresponding compounds.
Remark: Most of the theoretically possible alkanes are not viable.

Exercise 84. We remove an arbitrary edge from the complete graph $\mathcal{V}_n$ and obtain the new graph Ω. Determine the number of spanning trees of Ω.

Exercise 85. Determine a spanning tree with minimal weight in the following graph:



What is the total weight?

Exercise 86. Let G be a connected, weighted graph with pairwise distinct weights. Show that G possesses exactly one spanning tree with minimal weight.

Appendix

n	0	1	2	3	4	5	6	7	8	9	10
$p(n)$	1	1	2	3	5	7	11	15	22	30	42
$b(n)$	1	1	2	5	15	52	203	877	4140	21147	115975
$g(n)$	1	1	2	4	11	34	156	1044	12346	274668	12005168
$\varphi(n)$	0	1	1	2	2	4	2	6	4	6	4
$[n!/e]$	1	0	1	2	9	44	265	1854	14833	133496	1334961
B_n	1	$-1/2$	$1/6$	0	$-1/30$	0	$1/42$	0	$-1/30$	0	$5/66$
C_n	1	1	2	5	14	42	132	429	1430	4862	16796
F_n	0	1	1	2	3	5	8	13	21	34	55

$\binom{n}{k}$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

$\left(\binom{n}{k}\right)$	0	1	2	3	4	5	6	7	8	9	10
0	1	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10	11
3	1	3	6	10	15	21	28	36	45	55	66
4	1	4	10	20	35	56	84	120	165	220	286
5	1	5	15	35	70	126	210	330	495	715	1001
6	1	6	21	56	126	252	462	792	1287	2002	3003
7	1	7	28	84	210	462	924	1716	3003	5005	8008
8	1	8	36	120	330	792	1716	3432	6435	11440	19448
9	1	9	45	165	495	1287	3003	6435	12870	24310	43758
10	1	10	55	220	715	2002	5005	11440	24310	48620	92378

$\left[{n \atop k}\right]$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	0	1									
2	0	1	1								
3	0	2	3	1							
4	0	6	11	6	1						
5	0	24	50	35	10	1					
6	0	120	274	225	85	15	1				
7	0	720	1764	1624	735	175	21	1			
8	0	5040	13068	13132	6769	1960	322	28	1		
9	0	40320	109584	118124	67284	22449	4536	546	36	1	
10	0	362880	1026576	1172700	723680	269325	63273	9450	870	45	1

$\left\{{n \atop k}\right\}$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	0	1									
2	0	1	1								
3	0	1	3	1							
4	0	1	7	6	1						
5	0	1	15	25	10	1					
6	0	1	31	90	65	15	1				
7	0	1	63	301	350	140	21	1			
8	0	1	127	966	1701	1050	266	28	1		
9	0	1	255	3025	7770	6951	2646	462	36	1	
10	0	1	511	9330	34105	42525	22827	5880	750	45	1

$\left\langle{n \atop k}\right\rangle$	0	1	2	3	4	5
0	1					
1	1	1				
2	1	$X+1$	1			
3	1	X^2+X+1	X^2+X+1	1		
4	1	X^3+X^2+X+1	$X^4+X^3+2X^2+X+1$	X^3+X^2+X+1	1	
5	1	$X^4+X^3+X^2+X+1$	$X^6+X^5+2X^4+2X^3+2X^2+X+1$	$X^6+X^5+2X^4+2X^3+2X^2+X+1$	$X^4+X^3+X^2+X+1$	1

Index