TU Graz

NAWI Graz
Natural Sciences

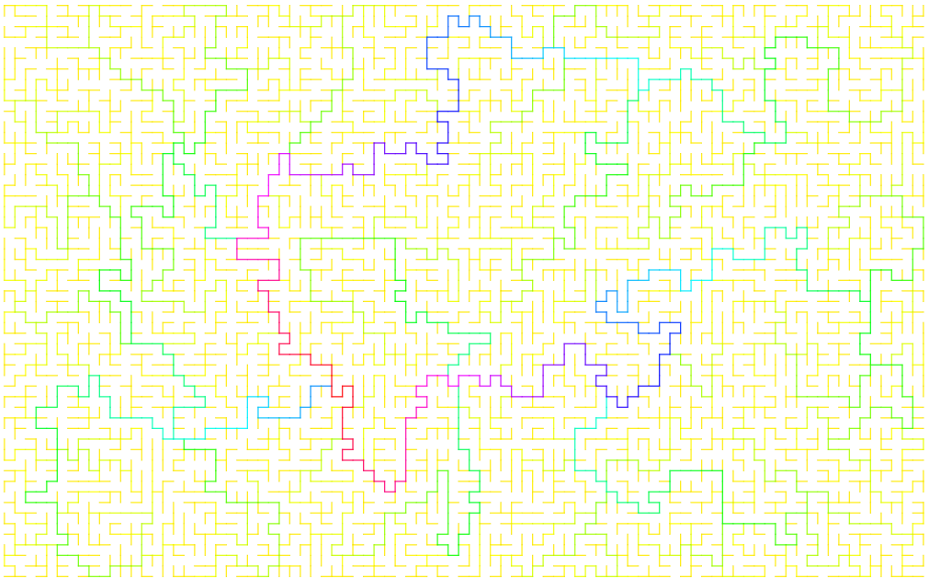
UNIVERSITÄT GRAZ
Institut für Mathematik und
Wissenschaftliches Rechnen

UNI GRAZ

Diskrete Mathematik

Begleitskript zu MAT.106UB, S24

Sarah Frisch, Benjamin Hackl, Clemens Heuberger,
Daniel Georg Holzfeind, Daniel Krenn, Florian Lehner,
Gabriel Lipnik, Jutta Rath



Stand: 07.07.2024

Inhaltsverzeichnis

Acknowledgements

Die Anzahl der abgedruckten Fehler konnte dank der Unterstützung der folgenden Studierenden wesentlich reduziert werden:

Marie Bisping, Laurenz Bonelli, Fabio Buchacher, Paul Kaltenegger, Jonas Kiesenhofer, Mia Klapf, Eric Maier, Laurent Nhim, Kathrin Schrenk, Anika Walther

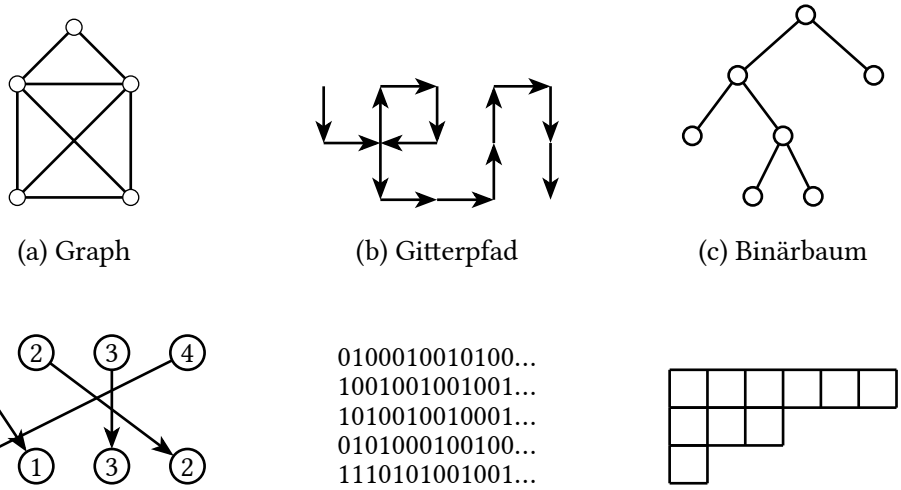
◆ **Vielen Dank fürs genaue Lesen!** ◆

§1 – Einleitendes

In dieser Vorlesung begeben wir uns auf einen Streifzug durch dreierlei mathematischer Teilgebiete: die *Kombinatorik*, die *Graphentheorie* und die *Elementare Zahlentheorie*.

1.1 Motivation: Worum geht es?

Das mathematische Teilgebiet der *Kombinatorik* beschäftigt sich in erster Linie mit *Abzählproblemen*, sowie mit der *Existenz* und auch der *Konstruktion* von mathematischen Objekten, an die gewisse Anforderungen gestellt werden. Um auch Abzählprobleme mit oder auf solchen Objekten studieren zu können, werden wir – vor allem im Rahmen dieser Vorlesung – ständig über den natürlichen Zahlen $\mathbb{N}$ arbeiten; die entsprechenden Objekte werden in diesem Zusammenhang auch *diskrete Strukturen* – oder eben *kombinatorische Strukturen* – genannt. Abbildung 1 zeigt ein paar Visualisierungen von solchen Strukturen.



(a) Graph (b) Gitterpfad (c) Binärbaum

(d) Permutation (e) Wörter (f) Partition

Abbildung 1: Eine Auswahl von einigen verschiedenen kombinatorischen Strukturen.

Im Rahmen der *Graphentheorie* konzentrieren wir uns auf das Untersuchen der Eigenschaften einer besonderen kombinatorischen Struktur – *Graphen*. Graphen sind besonders nützliche Werkzeuge um Beziehungen zwischen Objekten sowie Netzwerke zu modellieren.

Im dritten und letzten Block der Lehrveranstaltung, der *elementaren Zahlentheorie*, werden wir uns intensiv mit den Eigenschaften natürlicher Zahlen beschäftigen; *Teilbarkeit* und *Primzahlen* werden dort die Hauptrolle spielen.

Der inhaltliche Fokus dieser Lehrveranstaltung liegt allerdings nicht darin, so viele kombinatorische Strukturen bzw. klassische Resultate aus der Zahlentheorie wie möglich kennen zu lernen, sondern vielmehr darin, sich „Werkzeuge“ zur Analyse solcher Strukturen und zahlentheoretischen Problemen in der Form von allgemeingültigen Aussagen und Beweisstrategien anzueignen.

Beispiel 1.1: Sudoku ist ein relativ bekanntes Spiel, bei dem die Zahlen von 1 bis 9 derart in ein 9×9-Feld einzutragen sind, sodass sie je Zeile, Spalte, und 3×3-Teilfeld jeweils genau einmal vorkommen.

Die Gesamtanzahl von möglichen Sudokus wurde erst 2005 von Felgenbauer und Jarvis ermittelt und beträgt

$$6.670.903.752.021.072.936.960,$$

womit es also mehr verschiedene 9×9-Sudokus gibt, als die Anzahl von Sekunden, auf die das Alter des Universums geschätzt wird ($\approx 4.3 \times 10^{20}$). Zählt man anstatt aller möglichen Lösungen nur jene, die tatsächlich unterschiedlich sind und nicht etwa durch Spiegelung oder Umordnung der Zahlen 1 bis 9 aus einer anderen Lösung hervorgehen, so bleiben immer noch stolze

$$5.472.730.538$$

Sudokus übrig.

Würde man Sudoku auf einem 16×16-Feld mit 4×4-Teilfeldern untersuchen, so ist die exakte Anzahl der möglichen Konfigurationen im Übrigen noch unbekannt[1]! ⬠

Der möglicherweise durch die Wahl des Beispiels entstandene Eindruck, dass (enumerative) Kombinatorik lediglich im Kontext von lustigen Puzzles und nicht wirklich für praktische Anwendungen relevant ist, ist **jedenfalls falsch**. Auch wenn die konkreten Anwendungen zwar nicht Hauptgegenstand der Vorlesung sind, so finden sich kombinatorische Strukturen in den verschiedensten Disziplinen wieder, beispielsweise bei

- Sortier- und Suchverfahren,
- Datenstrukturen und Dateisystemen,
- Straßennetzen und allgemein Logistik,
- Fehlerkorrektur bei übertragenen Nachrichten,
- Entwurf von Netzwerken,
- und viele weitere.

Ganz allgemein spielt Kombinatorik beim Entwurf komplexer Systeme eine wichtige Rolle. Darüber hinaus sind die verwendeten Techniken (relativ) elementar und lassen sich oft auf Probleme aus anderen mathematischen Teilgebieten anwenden.

Die Zahlentheorie galt lange als besonders reine und anwendungsferne Disziplin (in dem Zusammenhang wurde sie auch von *Gauß* als „Königin der Mathematik“ bezeichnet). Heutzutage liefern zahlentheoretische Probleme sogenannte *Einwegfunktionen*, die in der Kryptographie eine wichtige Rolle spielen. So stecken etwa hinter jedem Besuch einer `https://`-Website zahlentheoretische Mechanismen; auf manche davon werden wir im Rahmen der Vorlesung einen kleinen Ausblick bekommen.

1.2 Notation

Wir führen nun noch einige nützliche Notationen ein, die uns vieles erleichtern werden.

Notation 1.2: In dieser Vorlesung verwenden wir die Schreibweisen

$$\mathbb{N} = \{1, 2, 3, 4, ...\} \quad \text{und} \quad \mathbb{N}_0 = \{0, 1, 2, 3, 4, ...\}$$

für die Menge der natürlichen Zahlen ohne und mit der Zahl 0.

[1] Siehe https://oeis.org/A107739.

Weiters definieren wir für ganze Zahlen $m, n \in \mathbb{Z}$ mit $m \leq n$ das *diskrete Intervall*

$$[m : n] := \{m, m+1, m+2, ..., n-1, n\}$$

wobei wir als Spezialfall für $m = 1$ auch

$$[n] := [1 : n] = \{1, 2, ..., n\}$$

schreiben.

Notation 1.3 (Iverson-Notation): Sei A eine Aussage, dann setzen wir

$$[\![A]\!] := \begin{cases} 1 \text{ wenn } A \text{ wahr ist,} \\ 0 \text{ wenn } A \text{ nicht wahr ist.} \end{cases}$$

Die Iverson-Notation ist gelegentlich im Zusammenhang mit Summen ein sehr nützliches Werkzeug.

Beispiel 1.4:

$$\sum_{j=0}^{10} [\![j \text{ ist gerade}]\!] = 6,$$

da unter den Zahlen von 0 bis 10 genau 6 gerade Zahlen sind (nämlich $0, 2, 4, 6, 8, 10$). ⬠

§2 – Elementare Kombinatorik

2.1 Schubfachschluss

Der *Schubfachschluss* ist ein besonders elementares – und dennoch vergleichsweise mächtiges – nicht-konstruktives Abzählargument. Die Idee ist sehr intuitiv: Teilen wir zehn Bälle auf neun Schachteln auf, so muss es, ganz egal wie die Aufteilung konkret ausschaut, zumindest eine Schachtel geben in der sich mindestens zwei Bälle befinden. Eine Veranschaulichung findet sich in Abbildung 2.

Abbildung 2: Der Schubfachschluss wird – offensichtlich – auch *Taubenschlagprinzip* genannt. Bild von Wikimedia Commons.

Satz 2.1 (Schubfachschluss / Taubenschlagprinzip): Sei $n > m$. Teilt man eine Menge mit n Elementen auf m Teilmengen auf, so enthält zumindest eine der Teilmengen mindestens zwei Elemente.

Beweis: Indirekt. Angenommen, jede der m Teilmengen enthält höchstens ein Element. Dann gibt es insgesamt höchstens m Elemente, was ein Widerspruch zur Annahme $n > m$ ist. ↯ □

Der „klassische“ Schubfachschluss lässt sich auch noch in einer etwas schärferen Fassung formulieren:

Satz 2.2 (Starker Schubfachschluss): Sei $n > m$. Teilt man eine Menge mit n Elementen auf m Teilmengen auf, so enthält zumindest eine der Teilmengen mindestens $\left\lceil \frac{n}{m} \right\rceil$ viele Elemente.

Beweis: Analog zum Beweis von Satz 2.1. □

An den folgenden Beispielen möchten wir den Schubfachschluss veranschaulichen.

Beispiel 2.3 (Haareszahlen): In der Metropolregion Graz gibt es zwei Personen, die exakt gleich viele Haare auf dem Kopf haben.

Um diese Behauptung verifizieren zu können, brauchen wir ein paar Hintergrundinformationen:

- Mit Stand vom 1. Jänner 2023 leben in der Metropolregion Graz rund 660.000 Menschen (660.238),
- abhängig von der Haarfarbe haben Menschen im Durchschnitt zwischen 90.000 und 150.000 Kopfhaare.

Eine großzügige obere Schranke für die Anzahl der Kopfhaare wäre also etwa 200.000. Um es uns nicht zu leicht zu machen, könnten wir sogar den „einfachen" Fall von Glatzenträger:innen ausschließen – deren Anteil wird unter Männern auf etwa 30% geschätzt. Dehnen wir diese Schätzung auf die gesamte Bevölkerung in der Metropolregion aus, so bleiben immer noch rund 460.000 Menschen ohne Glatze übrig.

Stellen wir uns jetzt vor, dass wir die 460.000 Menschen entsprechend ihrer *Haareszahl* in verschiedene Räume aufteilen; für jede der rund 200.000 möglichen *Haareszahlen* gibt es also einen eigenen Raum. Bei 200.000 Räumen und 460.000 Menschen muss es also laut Satz 2.1 mindestens einen Raum geben, in dem sich mindestens zwei Menschen – mit der exakt gleichen Anzahl von Kopfhaaren – befinden.

Aus der schärferen Fassung des Schubfachschlusses können wir sogar schließen, dass es mindestens $\left\lceil \frac{460.000}{200.000} \right\rceil = 3$ Personen mit der gleichen *Haareszahl* in der Metropolregion Graz geben muss. ⬠

Beispiel 2.4: In der Folge $7, 77, 777, 7777, \ldots$ gibt es eine Zahl, die durch 501 teilbar ist.

Wenn wir die Zahlen in der Folge jeweils durch 501 dividieren und uns den entsprechenden Rest notieren, so muss es nach Satz 2.1 unter den ersten 502 Zahlen zwei geben, die den gleichen Rest liefern. Seien das die Zahlen

$$\underbrace{77\ldots7}_{k \text{ viele}} \text{ und } \underbrace{77\ldots7}_{\ell \text{ viele}},$$

mit $\ell \geq k$. Liefern bei Division durch 501 beide den gleichen Rest, so muss die Differenz

$$\underbrace{77\ldots7}_{\ell-k}\underbrace{0\ldots0}_{k} = \underbrace{77\ldots7}_{\ell-k} \cdot 10^k$$

bei Division durch 501 als Rest 0 liefern – also ein Vielfaches von 501 sein. Da 10 nur 2 und 5 als Teiler besitzt, die beide nicht in 501 auftreten, muss also bereits $77\ldots7$ mit $\ell - k$ vielen Ziffern ein Vielfaches von 501 gewesen sein. ⬠

Beispiel 2.5 (Zehn Punkte im Einheitsquadrat): In einem Quadrat mit Seitenlänge 1 werden zehn Punkte beliebig platziert. Dann muss es mindestens zwei Punkte geben, deren Abstand weniger als 0.48 beträgt.

Um das zu sehen können wir unser Quadrat in neun Teilquadrate, jeweils mit Seitenlänge $\frac{1}{3}$ zerteilen. Laut Satz 2.1 muss es bei zehn Punkten und neun Quadraten wieder mindestens ein Teilquadrat geben, das zwei Punkte enthält. Der Abstand zwischen diesen beiden Punkten ist höchstens die Diagonale des Teilquadrates, welche

$$\sqrt{\left(\frac{1}{3}\right)^2 + \left(\frac{1}{3}\right)^2} = \frac{\sqrt{2}}{3} < 0.48$$

beträgt. ⬠

2.2 (Ab-)zählen mit Mengen

Weil sie besonders nützlich und wichtig sind, beschäftigen wir uns kurz mit ein paar Fragen zur Anzahl von Elementen in durch Mengenoperationen erhaltenen Mengen.

Definition 2.6 (Kardinalität, Mächtigkeit): Sei A eine Menge. Die Anzahl der Elemente in A wird *Kardinalität* oder *Mächtigkeit* genannt und als $|A|$ oder manchmal auch $\#A$ geschrieben.

Ist $|A| < \infty$, so sagen wir, dass A eine *endliche Menge* ist.

Wir entziehen uns an dieser Stelle weitestgehend der „Problematik“ verschieden großer Unendlichkeiten und konzentrieren uns in erster Linie auf den Fall endlicher Mengen.

Beispiel 2.7: Wenig überraschend gilt etwa $|[10]| = 10$, oder

$$|\{n \in \mathbb{N} \mid n \text{ ist prim und } 1 \leq n \leq 30\}| = |\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}| = 10.$$

Im Fall einer Menge wie $\mathbb{N}$ würden wir etwa $|\mathbb{N}| = \infty$ schreiben (und *noch* nicht genauer darüber nachdenken, was das eigentlich heißt). ⬠

Satz 2.8 (Kardinalität und Mengenoperationen): Seien A, B endliche Mengen. Dann gilt:

(a) $|A \times B| = |A| \cdot |B|$, wobei $A \times B$ das kartesische Produkt der Mengen A und B beschreibt,

(b) $|A \cup B| = |A| + |B| - |A \cap B|$,

(c) $|\{f \text{ Funktion} \mid f : A \to B\}| = |B|^{|A|}$.

Beispiel 2.9: Sei $A = \{1, 2, ✸\}$, $B = \{x, y\}$. Das kartesische Produkt ist durch

$$A \times B = \{(1, x), (2, x), (✸, x), (1, y), (2, y), (✸, y)\}$$

gegeben, also ist $6 = |A \times B| = |A| \cdot |B| = 3 \cdot 2$. ⬠

Beweis von Satz 2.8:

(a) Die Elemente von $A \times B$ sind Tupel, die aus je einem Element aus A und einem Element aus B bestehen. Damit gibt es für jedes fixierte $a \in A$ genau $|B|$ Möglichkeiten um ein Element aus B zu wählen. Insgesamt gibt es damit

$$\underbrace{|B| + |B| + |B| + \cdots + |B|}_{|A| \text{ viele}} = |A| \cdot |B|$$

verschiedene Möglichkeiten, ein Tupel zu bilden.

(b) Zählt man die Kardinalitäten von A und B zusammen, so werden jene Elemente doppelt gezählt die sowohl in A als auch in B vorkommen. Diese doppelt gezählten (in $A \cap B$) müssen abgezogen werden, und so erhalten wir

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

(c) Eine Funktion $f : A \to B$ ordnet jedem der $a \in A$ genau ein $b \in B$ zu. Für jedes der $|A|$ vielen Elemente in A gibt es jetzt also (unabhängig voneinander) $|B|$ viele Möglichkeiten ein Bild $f(a) \in B$ zuzuweisen. Damit gibt es insgesamt

$$\underbrace{|B| \cdot |B| \cdot |B| \cdots |B|}_{|A| \text{ viele}} = |B|^{|A|}$$

Möglichkeiten um eine Funktion f zu konstruieren. □

Beispiel 2.10: Wir überlegen uns, wie viele verschiedene Dateien am Computer es geben kann, die aus n Bit (eine winzige Speichereinheit die Werte 0 oder 1 annehmen kann) bestehen. Der Einfachheit halber nehmen wir an, dass jede Bit-Kombination auch tatsächlich auftreten kann (was praktisch nicht wirklich möglich oder sinnvoll ist).

In diesem einfachen Modell können wir n-Bit-Dateien als Funktionen $f : [n] \to \{0, 1\}$ sehen: die „Datei“ f kann so sagen, welchen Wert das Bit an Stelle j (nämlich $f(j)$) hat. Mit Satz 2.8 haben wir also $|\{0, 1\}|^{|[n]|} = 2^n$ mögliche n-Bit-Dateien. ⬠

2.3 Der Binomialkoeffizient und seine Freunde

Die sogenannten *Permutationen* sind besonders einfache, aber auch besonders interessante kombinatorische Objekte. Wir definieren den Begriff im Folgenden:

Definition 2.11 (Permutation): Eine *Permutation* von n Elementen ist eine Anordnung dieser Elemente, wobei die Reihenfolge wesentlich ist.

Beispiel 2.12: Wir bestimmen alle Permutationen der Menge $\{1, 2, 3\}$. Diese sind

$$123, \quad 132, \quad 213, \quad 231, \quad 312, \quad 321.$$ ⬠

Anmerkung 2.13: Formal können wir eine Permutation auch als eine bijektive Funktion von einer endlichen Menge (mit n Elementen) in sich selbst sehen.

Uns interessiert, wie viele verschiedene Permutationen von n verschiedenen Elementen existieren. Dazu führen wir zunächst die *Fakultät* einer natürlichen Zahl ein.

Definition 2.14 (Faktorielle, Fakultät): Für $n \in \mathbb{N}_0$ nennen wir die Zahl

$$n! := n \cdot (n-1) \cdots 2 \cdot 1$$

Faktorielle oder *Fakultät* von n. Insbesondere gilt[2] nach dieser Definition auch $0! = 1$.

Proposition 2.15: Es gibt $n!$ verschiedene Permutationen von n Elementen.

[2] Die Fakultät $n!$ beschreibt das Produkt der ersten n natürlichen Zahlen. Für $n = 0$ wird ein sogenanntes *leeres Produkt* gebildet, das per Konvention den Wert 1 hat.

Beweis: Wir „basteln“ eine beliebige Permutation: für das erste Element gibt es n Möglichkeiten, für das zweite $n-1$ viele – und so weiter – bis es für das letzte Element nur mehr eine einzige Möglichkeit gibt.

Damit (und weil jede dieser Entscheidungen unabhängig – zumindest bezogen auf die Anzahl der möglichen „Unterentscheidungen“ – ist) gibt es insgesamt

$$n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 = n!$$

viele Möglichkeiten, eine Permutation zu konstruieren. □

Wir können uns jetzt näher mit Permutationen beschäftigen. Dazu betrachten wir das folgende, motivierende Beispiel.

Beispiel 2.16 (Fun with flags):

- Wie viele verschiedene Permutationen der Farben im Wappen von Graz gibt es? Das Wappen ist mit Grün, Weiß, Schwarz, Rot, Gelb eingefärbt; wir suchen alle möglichen Permutationen dieser fünf Farben. Es gibt $5! = 120$ viele davon.
- Auf wie viele Arten können die drei Farbstreifen in der Flagge von Österreich angeordnet werden? Während die Flagge zwar aus drei Streifen besteht, sind zwei der drei Streifen rot (und nicht voneinander unterscheidbar). Durch Aufzählen finden wir die möglichen Farbkombinationen (rot, weiß, rot), (rot, rot, weiß), (weiß, rot, rot) – es gibt also nur 3, und nicht $3! = 6$ Möglichkeiten... ⬠

Im Beispiel mit der Österreich-Flagge kommt eine Situation vor, die wir oben bei der Permutation von Elementen nur implizit ausgeschlossen haben: bisher haben wir angenommen, dass die zu permutierenden Elemente voneinander unterschieden werden können. Wie sich die Situation genau verhält wenn mehrere gleiche Elemente vorliegen, das untersuchen wir nochmal langsam im folgenden Beispiel.

Beispiel 2.17: Eine Gärtnerin möchte ein Beet mit 5 roten, 3 gelben, und 2 weißen Blumen setzen. Wie viele Möglichkeiten gibt es, die Blumen anzuordnen?

Wir könnten, so wie im Beispiel zuvor, wieder versuchen alle Möglichkeiten systematisch aufzuzählen. Das ist aber nicht besonders effizient, wir entscheiden uns daher für eine andere Strategie: *doppeltes Abzählen*.

Nehmen wir für den Moment an, dass die 10 Blumen (ungeachtet der Tatsache dass manche die gleiche Farbe haben) allesamt unterscheidbar wären. In diesem Fall gibt es nach Proposition 2.15 schlicht $10! = 3628800$ viele Möglichkeiten, die Blumen anzuordnen.

Andererseits: angenommen, es gibt X mögliche Anordnungen (mit ununterscheidbaren Farben). In diesem Fall können wir die Blumen etwa durch Anbringen eines Etiketts wieder unterscheidbar machen. Es gibt 5! viele Möglichkeiten die roten Blumen unterscheidbar zu machen, 3! viele Möglichkeiten für die gelben, und 2! viele Möglichkeiten für die weißen Blumen.

Die beiden verschiedenen Ansätze haben uns jeweils eine Formel für die Anzahl der (unterscheidbaren) Anordnungen geliefert – und so muss

$$10! = X \cdot 5! \cdot 3! \cdot 2!,$$

oder dazu äquivalent,

$$X = \frac{10!}{5! \cdot 3! \cdot 2!} = 2520$$

sein. Es gibt also 2520 verschiedene Möglichkeiten, die 10 (zum Teil ununterscheidbaren Blumen) im Beet anzuordnen. ⬠

Dieses Beispiel motiviert die folgende Definition.

Definition 2.18 (Multinomialkoeffizient): Seien $n, k \in \mathbb{N}_0$ und $a_1, a_2, \ldots, a_k \in \mathbb{N}_0$ so gewählt, dass $a_1 + a_2 + \cdots + a_k = n$ gilt. Dann heißt

$$\binom{n}{a_1; a_2; \cdots; a_k} := \frac{n!}{a_1!\, a_2! \cdots a_k!}$$

ein *Multinomialkoeffizient*; gesprochen „n über $a_1, a_2, \ldots, a_k$“.

Beispiel 2.19: Im letzten Beispiel haben wir bereits einen Multinomialkoeffizienten berechnet, nämlich

$$\binom{10}{5; 3; 2} = 2520.$$

⬠

Proposition 2.20: Wir betrachten eine Ansammlung von n (nicht notwendigerweise unterscheidbaren) Elementen. Unter den n Elementen gibt es k verschiedene Typen, wobei es a_j-viele Elemente vom Typ j geben soll. Dann zählt der Multinomialkoeffizient $\binom{n}{a_1;a_2;\cdots;a_k}$ die Anzahl von Permutationen dieser n (zum Teil ununterscheidbaren) Elemente.

Die formal sauberere Formulierung von Proposition 2.20 würde über das Konstrukt von *Multimengen* erfolgen; das sind Mengen die Elemente auch mehrfach beinhalten können. Die Vielfachheit eines Elementes wird dabei üblicherweise hochgestellt und eingeklammert beschrieben.

Beispiel 2.21: Die Multimenge $B = \{\text{rot}^{(5)}, \text{gelb}^{(3)}, \text{weiß}^{(2)}\}$ hat genau $\binom{10}{5;3;2} = 2520$ viele verschiedene Permutationen.

Für ein kleineres Beispiel können wir die Permutationen auch noch explizit aufschreiben, z.B. gibt es für $\{x^{(2)}, y^{(1)}, z^{(1)}\}$ die $\binom{4}{2;1;1} = 12$ verschiedenen Permutationen:

$$\begin{array}{cccc} xxyz & xxzy & xyxz & xyzx \\ xzxy & xzyx & yxxz & yxzx \\ yzxx & zxxy & zxyx & zyxx \end{array}$$

⬠

Beweis von Proposition 2.20: Durch doppeltes Abzählen – wie im Blumenbeet-Beispiel, nur formalisiert. Übung. □

Definition 2.22 (Binomialkoeffizient): Seien $n, k \in \mathbb{N}_0$. Der spezielle Multinomialkoeffizient

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

wird *Binomialkoeffizient* genannt und als $\binom{n}{k} := \binom{n}{k;n-k}$, gesprochen „$n$ über k“, bezeichnet.

Anmerkung 2.23: Da wir den Binomialkoeffizient jetzt als speziellen Multinomialkoeffizienten definiert haben, wissen wir noch nicht, ob er mit der „handelsüblichen“ kombinatorischen Interpretation (als Anzahl der möglichen k-elementingen Teilmengen einer n-elementigen Menge) übereinstimmt. Das müssen wir uns zuerst überlegen.

Beispiel 2.24: Ein kleines Beispiel zur Verifikation: aus der Menge $M = \{w, x, y, z\}$ können wir die zweielementigen Teilmengen

$$\{w, x\}, \{w, y\}, \{w, z\}, \{x, y\}, \{x, z\}, \{y, z\}$$

bilden. Passend dazu ist $\binom{4}{2} = \frac{4!}{2!\cdot 2!} = \frac{4\cdot 3\cdot 2\cdot 1}{2\cdot 1\cdot 2\cdot 1} = \frac{4\cdot 3}{2\cdot 1} = \frac{12}{2} = 6$, wie erwartet. ⬠

Proposition 2.25: Der Binomialkoeffizient $\binom{n}{k}$ zählt die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge.

Beweis: Wir beweisen die Aussage durch Konstruktion einer bijektiven Abbildung zwischen der Menge aller Permutationen der Multimenge $\left\{\text{ja}^{(k)}, \text{nein}^{(n-k)}\right\}$ und der Menge aller k-elementigen Teilmengen von $[n]$. Denn: wenn es eine Bijektion zwischen den beiden Mengen gibt, so müssen sie gleich viele Elemente beinhalten.

Sei S nun eine k-elementige Teilmenge von $[n]$, $S = \{e_1, e_2, ..., e_k\}$. Wir konstruieren zu S nun eine Permutation der ja/nein-Multimenge, indem wir genau an die in S vorkommenden Indizes jeweils „ja“ schreiben, und die restlichen $n - k$ Plätze mit „nein“ füllen.

Als konkretes Beispiel: für $n = 5$ und $S = \{2, 5\} \subseteq [5]$ ergibt sich die Permutation „nein ja nein nein ja“.

Diese Konstruktion lässt sich auch einfach „von unten nach oben lesen“; aus einer gegebenen ja/nein-Permutation erhalten wir die entsprechende Teilmenge S indem wir die Indizes der „ja“-Elemente notieren. Damit liegt eine Bijektion vor, und die Behauptung ist bewiesen. □

Der Binomialkoeffizient hat eine Reihe von nützlichen Eigenschaften, im Folgenden wollen wir ein paar davon beweisen.

Proposition 2.26: Seien $n, k \in \mathbb{N}_0$. Der Binomialkoeffizient hat die folgenden Eigenschaften:

1. Symmetrie: $\binom{n}{k} = \binom{n}{n-k}$,
2. Spezielle Werte: $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = n$, $\binom{n}{2} = \frac{n(n-1)}{2}$,

3. Rekursion: für $n, k \geq 1$ gilt $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, insbesondere gilt $\binom{n}{k} = 0$ für $k > n$ (und ebenso, falls $k \in \mathbb{Z}$, für $k < 0$),
4. „Herausheben“: für $n, k \geq 1$ gilt $\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1}$.

Beweis:

1. Symmetrie: Aus der Definition des Binomialkoeffizienten folgt
$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n!}{(n-k)!\,(n-(n-k))!} = \binom{n}{n-k}.$$
2. Spezielle Werte: durch Symmetrie und direkte Rechnung erhalten wir
$$\binom{n}{n} = \binom{n}{0} = \frac{n!}{0!\,n!} = 1,$$
$$\binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n \cdot (n-1)!}{1!\,(n-1)!} = \frac{n}{1!} = n,$$
$$\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n \cdot (n-1) \cdot (n-2)!}{2!\,(n-2)!} = \frac{n \cdot (n-1)}{2}.$$
3. Rekursion: Zunächst kurz zu den speziellen Werten: für $k \in \mathbb{Z}$ ist im Fall $k < 0$ bzw. $k > n$ der Binomialkoeffizient $\binom{n}{k} = 0$. Technisch ist das mehr eine Konvention/Definitionsfrage als eine Eigenschaft die direkt aus $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ folgt: in diesen Fällen entsteht im Nenner die Fakultät einer negativen ganzen Zahl, für diese haben wir aber keine Definition. Aus analytischen Gründen (konkret: einer Beziehung der Fakultät zur sogenannten Γ-Funktion) bietet es sich an, $k! = \infty$, beziehungsweise jedenfalls $\frac{1}{k!} = 0$ für negative ganze Zahlen k festzulegen. Als Konsequenz dieser Konvention folgt $\binom{n}{k} = 0$ in diesen Fällen. Auch die kombinatorische Interpretation passt in diesen Fällen: es gibt keine Möglichkeit, weniger als 0 Elemente bzw. mehr als n Elemente aus einer n-elementigen Menge auszuwählen.

   Nun zur Rekursionsgleichung. Diese wollen wir auf zwei verschiedene Arten beweisen:

   - Durch direkte Rechnung:
$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!\,((n-1)-(k-1))!} + \frac{(n-1)!}{k!\,((n-1)-k)!} \\
&= \frac{(n-1)!}{(k-1)!\,(n-k-1)!} \cdot \left(\frac{1}{n-k} + \frac{1}{k}\right) \\
&= \frac{(n-1)!}{(k-1)!\,(n-k-1)!} \cdot \left(\frac{k}{k \cdot (n-k)} + \frac{n-k}{k \cdot (n-k)}\right) \\
&= \frac{(n-1)!}{(k-1)!\,(n-k-1)!} \cdot \frac{n}{k \cdot (n-k)} \\
&= \frac{n!}{k!\,(n-k)!} = \binom{n}{k}.
\end{aligned}$$

- Durch ein kombinatorisches Argument. Wir suchen Interpretationen für die beiden Seiten der Rekursionsgleichung

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

Der Binomialkoeffizient auf der rechten Seite zählt die Anzahl der k-elementigen Teilmengen von $[n]$. Um zu sehen, dass die linke Seite das ebenso tut, betrachten wir die folgenden beiden disjunkten Fälle für die Konstruktion einer Teilmenge $S \subseteq [n]$:

  - $n \in S$: aus den $n-1$ verbleibenden Elementen in $[n-1]$ sind jetzt noch $k-1$ viele auszuwählen, um eine k-elementige Teilmenge zu erhalten. Dafür gibt es $\binom{n-1}{k-1}$ viele Möglichkeiten.
  - $n \notin S$: hier sind alle k Elemente aus den übrigen $n-1$ vielen auszuwählen, dafür gibt es $\binom{n-1}{k}$ viele Möglichkeiten.

Die beiden disjunkten (also überschneidungsfreien) Fälle decken so die Konstruktion aller möglicher k-elementiger Teilmengen ab – und liefern zugleich eine Interpretation für die linke Seite der Gleichung.

Beide Seiten der Rekursionsgleichung zählen also die Anzahl der k-elementigen Teilmengen von $[n]$ auf verschiedene Arten; daraus ergibt sich die Gleichheit.

4. Das „Herausheben“ folgt ebenfalls aus direkter Rechnung:

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

□

Anmerkung 2.27 (Pascal'sches Dreieck): Die Rekursionsgleichung $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ lässt sich auch schön in einem dreieckigen Diagramm darstellen, in der sich jede Zelle in dem Dreieck aus der Summe der beiden schräg darüber liegenden Zellen ergibt; „leere“ Zellen werden dabei als 0 interpretiert. Eine Visualisierung der ersten paar Zeilen des *Pascal'schen Dreiecks* ist in Abbildung 3 zu sehen. Mittels SageMath lassen sich die ersten paar Zeilen etwa mittels

```
sage: for n in srange(10):
....:     print(" ".join(str(binomial(n, k)) for k in srange(n + 1)))
```

ausgeben.

$$\begin{array}{ccccccccccc}
 & & & & & \binom{0}{0} & & & & & \\
 & & & & \binom{1}{0} & & \binom{1}{1} & & & & \\
 & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & \\
 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \\
 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5}
\end{array}
\qquad
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Abbildung 3: Symbolische und numerische Darstellung der Binomialkoeffizienten im Pascal'schen Dreieck.

Die Zeilen im Pascal'schen Dreieck sind dafür bekannt, dass sie im Zusammenhang mit den Potenzen von Summen auftauchen. Mit dem Wissen um die kombinatorische Interpretation können wir feststellen, dass das natürlich kein Zufall ist.

Satz 2.28 (Binomischer Lehrsatz): Seien $a, b \in \mathbb{C}$ und $n \in \mathbb{N}_0$. Dann gilt:

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\ &= \binom{n}{0} a^0 b^n + \binom{n}{1} a^1 b^{n-1} + \cdots + \binom{n}{n} a^n b^0.\end{aligned} \tag{1}$$

Anmerkung 2.29: Die „Einschränkung" $a, b \in \mathbb{C}$ ist völlig willkürlich. Alles was benötigt wird damit der binomische Lehrsatz gilt ist eine kommutative Multiplikation, $a \cdot b = b \cdot a$.

Beweis: Satz 2.28 kann auf sehr direkte (und mechanische) Art und Weise durch vollständige Induktion nach n bewiesen werden. Wir überlassen diesen Zugang den geneigten Lesern zur Übung – und präsentieren stattdessen einen kombinatorischen Beweis.

Wir stellen zunächst fest, dass das Produkt auf der linken Seite von (1) eine Kurzschreibweise für

$$(a+b)^n = \underbrace{(a+b) \cdot (a+b) \cdot (a+b) \cdots (a+b)}_{n\text{-mal}}$$

ist.

Praktisch wählen wir, wenn wir so einen Ausdruck ausmultiplizieren, aus jeder der n Klammern den Term a oder b, bilden das Produkt der Auswahl (wobei wir einen Ausdruck der Form $a^k b^{n-k}$ erhalten) – und müssen die entsprechenden Ergebnisse für alle Auswahlmöglichkeiten aufsummieren („jedes mit jedem").

Eine Auswahl ist nun aber nichts anderes als ein Wort der Länge n über dem Alphabet $\{a, b\}$; jeder „Buchstabe" steht für die Auswahl in einer Klammer. Die Worte, die genau k-mal den Buchstaben „a" beinhalten (und damit genau $(n-k)$-mal den Buchstaben „b") tragen einen Faktor von $a^k b^{n-k}$ bei.

Da jedes dieser Wörter genau eine Permutation der Multimenge $\left\{a^{(k)}, b^{(n-k)}\right\}$ ist, gibt es nach Proposition 2.20 $\binom{n}{k}$ viele von ihnen. Im ausmultiplizierten Produkt muss also der Summand $\binom{n}{k} a^k b^{n-k}$ vorkommen. Andere Ausdrücke als diese für $0 \leq k \leq n$ kann es nicht geben – womit

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

gleich dem Produkt $(a+b)^n$ sein muss. □

Korollar 2.30: Für $n \in \mathbb{N}_0$ gelten die Identitäten

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n, \quad \text{und} \quad \sum_{k=0}^{n}\binom{n}{k}(-1)^k = 0.$$

Beweis: Wende Satz 2.28 mit $a = b = 1$, bzw. $a = 1, b = -1$ an. □

Mit SageMath können wir beide Identitäten natürlich auch verifizieren:

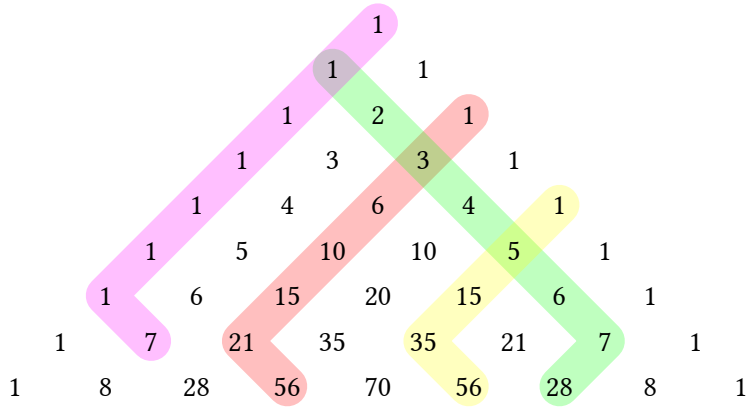
```
sage: N = 42
sage: sum(binomial(N, k) for k in srange(N + 1)) == 2^(N)
True
sage: sum(binomial(N, k) * (-1)^k for k in srange(N + 1)) == 0
True
```

Summen, die Binomialkoeffizienten beinhalten tauchen in kombinatorischen Zusammenhängen immer wieder auf. Oft lassen sich sogar geschlossene Formeln für solche Summen finden. Die folgenden beiden Resultate zeigen das in zwei einfacheren Fällen.

Proposition 2.31 (Hockey Stick Theorem): Für $k, m \in \mathbb{N}_0$ gilt

$$\sum_{n=0}^{m}\binom{n}{k} = \binom{m+1}{k+1}. \tag{2}$$

Anmerkung 2.32: Das Resultat ist unter anderem als *Hockey Stick Theorem* bekannt, weil es auf spezielle Art und Weise im Pascal'schen Dreieck visualisiert werden kann: eine am Rand beginnende Summe entlang einer Diagonalen hat den jeweils schräg darunter liegenden Binomialkoeffizienten als Ergebnis:



Beweis: Wir beweisen (2) indem wir die beiden Seiten der Gleichung kombinatorisch interpretieren.

Die rechte Seite von (2) ist der Binomialkoeffizient $\binom{m+1}{k+1}$ und zählt damit die Anzahl der $(k+1)$-elementigen Teilmengen von $[m+1]$.

Auf der linken Seite greifen wir uns für ein festes n einen Summanden, $\binom{n}{k}$ heraus. Wir wählen hier aber nicht die „klassische" Interpretation für den Binomialkoeffizienten. Wir können

beobachten, dass die Anzahl der $(k+1)$-elementigen Teilmengen von $[m+1]$ in denen $n+1$ das größte Element ist ebenso von $\binom{n}{k}$ gezählt wird: wenn wir wissen, dass $n+1$ das maximale Element ist, so erhalten wir alle möglichen Teilmengen durch Hinzufügen von $n+1$ zu allen möglichen k-elementigen Teilmengen von $[n]$. Dafür gibt es $\binom{n}{k}$-viele Möglichkeiten.

Summieren wir also über alle möglichen maximalen Werte in den $k+1$-elementigen Teilmengen, so erhalten wir praktisch die Summe auf der linken Seite von (2) – und gleichzeitig zählt die Summe, so wie die rechte Seite, alle möglichen $(k+1)$-elementigen Teilmengen von $[m+1]$. Das beweist die Gleichheit in (2). □

Proposition 2.33: Für $n \in \mathbb{N}_0$ gilt

$$\sum_{k=1}^{n} k \cdot \binom{n}{k} = n \cdot 2^{n-1}.$$

Um eine weitere sehr oft nützliche Technik im Zusammenhang mit solchen kombinatorischen Identitäten kennenzulernen, wollen wir diese Proposition auf zwei verschiedene Arten beweisen.

Beweis von Proposition 2.33, kombinatorische Variante: Mittels doppeltem Abzählen. Wir zählen die Anzahl der Möglichkeiten, ein Komitee in einer n-köpfigen Gruppe zu bilden.

Eine Strategie zur Bildung des Komitees wäre, zuerst eine:n Vorsitzende:n zu wählen (wofür es n Möglichkeiten gibt), und dann für jede der verbleibenden $n-1$ Personen (unabhängig voneinander) zu entscheiden, ob sie im Komitee sein soll oder nicht. Dafür gibt es jeweils 2 Möglichkeiten, insgesamt also 2^{n-1}-viele Möglichkeiten. Kombiniert mit den n Möglichkeiten für die Vorsitzenden-Wahl erhalten wir $n2^{n-1}$, was genau die rechte Seite von unserer Behauptung ist.

Andererseits können wir uns aber auch a priori darauf festlegen, dass das Komitee aus k Personen bestehen soll. In dem Fall gibt es $\binom{n}{k}$ Möglichkeiten zur Auswahl der k Personen – und um aus den gewählten jetzt noch eine:n Vorsitzende:n zu bestimmen gibt es nochmal k Möglichkeiten. Bei vorgegebener Gruppengröße k ergeben sich so $k \cdot \binom{n}{k}$ verschiedene Komitees.

Summieren jetzt noch über die möglichen Gruppengrößen, so erhalten wir alle möglichen Komiteezusammensetzungen – und den Ausdruck auf der linken Seite unserer Behauptung. Da wir uns gerade überlegt haben, dass die beiden Seiten der Identität genau Kommiteezusammensetzungen zählen, müssen sie gleich sein. □

Beweis von Proposition 2.33, analytische Variante: Wir können diese Identität auch „analytisch“, also mit Mitteln der Analysis beweisen. Dazu betrachten wir die Funktion $f(x) = (x+1)^n$, die wir nach Satz 2.28 auch als

$$f(x) = \sum_{k=0}^{n} \binom{n}{k} x^k$$

schreiben können. Da die Ausdrücke auf beiden Seiten dieser Gleichung unabhängig von der Wahl von x gelten (also als Funktionen *ident* sind), müssen auch deren Ableitungen nach x identisch sein. Es ergibt sich

$$n(1+x)^{n-1} = f'(x) = \sum_{k=1}^{n} \binom{n}{k} k x^{k-1},$$

wobei der Summand für $k = 0$ auf der rechten Seite gleich 0 ist und wir somit auch erst ab $k = 1$ zu summieren beginnen können. Setzen wir nun $x = 1$ in die Ableitung ein, so erhalten wir aus den beiden Seiten der Gleichung genau unsere Behauptung. □

Die nächsten paar Resultate beschäftigen sich mit klassischen Abzählproblemen in deren Kontext Binomialkoeffizienten auftreten.

Proposition 2.34: Sei $n \in \mathbb{N}_0$ und $k \in \mathbb{N}$. Die Anzahl der Möglichkeiten, n gleiche Objekte auf k (unterscheidbare) Boxen zu verteilen beträgt $\binom{n+k-1}{k-1}$.

Beweis: Wir verwenden eine Strategie, die üblicherweise als *„stars and bars"* bezeichnet wird. Dabei visualisieren wir unsere Situation indem wir die Objekte („Stars") hintereinander in eine Zeile schreiben, und die Einteilung in die Boxen durch Trennlinien („Bars") vornehmen.

Als Beispiel, eine Einteilung von 7 Objekten auf 3 Boxen könnte durch

$$\underbrace{\star\star}_{\text{Box 1}} \mid \underbrace{\star\star\star\star}_{\text{Box 2}} \mid \underbrace{\star}_{\text{Box 3}}$$

dargestellt werden.

Mit anderen Worten: eine Zuordnung von n Objekten auf k Boxen kann also als Wort über dem Alphabet $\{\star, |\}$ gesehen werden, wobei $\star$ in dem Wort n-fach, und $|$ $(k-1)$-fach vorkommen muss. Die Anzahl dieser Worte ist die Anzahl der Permutationen der Multimenge $\{\star^{(n)}, |^{(k-1)}\}$ gegeben – wovon es nach Proposition 2.20 $\binom{n+k-1}{k-1}$-viele gibt. □

Beispiel 2.35: Der österreichische Nationalrat hat $n = 183$ Abgeordnete, aufgeteilt auf 5 Parteien (plus „wilde" / fraktionslose Abgeordnete). Damit gibt es

$$\binom{183+6-1}{6-1} = \binom{188}{5} = 1854900872$$

mögliche Mandatszuteilungen. *(Praktisch stimmt das aber nicht.)* ⬠

Proposition 2.36: Sei $n \in \mathbb{N}_0$ und $k \in \mathbb{N}$. Die Anzahl von Möglichkeiten, n ununterscheidbare Objekte auf k *nicht leere* Boxen aufzuteilen beträgt $\binom{n-1}{k-1}$.

Beweis: Wieder via „stars and bars". Diesmal schreiben wir die n Objekte zuerst wieder als $\star$ in eine Zeile. Um sicher zu stellen, dass zwei Trennwände direkt hintereinander nicht erlaubt sind,

wählen wir aus den ersten $n-1$ Sternen $k-1$ viele aus, hinter denen wir „|“ einfügen. Der n-te Stern darf nicht ausgewählt werden, weil sonst die letzte Box leer wäre.

Um aus $n-1$ Elementen genau $(k-1)$-viele auszuwählen gibt es jetzt nach Proposition 2.25 $\binom{n-1}{k-1}$-viele Möglichkeiten. □

Beispiel 2.37: Für $n = 183$ Abgeordnete und $k = 6$ Gruppierungen im österreichischen Nationalrat gibt es (nachdem keine leer sein darf, sonst wäre sie ja nicht im Nationalrat) damit

$$\binom{183-1}{6-1} = 1574397006$$

mögliche Mandatszuteilungen. *(Das ist besser und im Zusammenhang mit „Gruppierungen“ die richtige Antwort – in der Realität wäre das Beispiel im Kontext von „Fraktionen“ bzw. „Klubs“ interessanter, wird dann wegen zusätzlicher Einschränkungen (z.B.: mindestens 5 Mandate) aber schnell komplizierter.)* ⬠

Wir sind jetzt schon mehrfach auf kombinatorische Argumente gestoßen, in denen „Wörter“ über einem gegebenen Alphabet eine Rolle spielen. Gerade im Zusammenhang von bijektiven Beweisen sind sie ein nützliches Werkzeug. Es ist also Zeit, Worte etwas systematischer zu betrachten.

Definition 2.38 (Wörter und Sprachen): Sei $n \in \mathbb{N}$ und Ω eine endliche Menge. Dann heißt die Menge

$$\mathcal{L}(\Omega) := \{w \mid \exists k \in \mathbb{N}_0 \, \exists w_1, w_2, ..., w_k \in \Omega : w = w_1 w_2 ... w_k\}$$

die *Menge der Worte* (bzw. die *Sprache*) über Ω. Die Sprache $\mathcal{L}(\Omega)$ wird auch oft als Ω^* geschrieben. In diesem Kontext nennt man Ω auch das *Alphabet* der Sprache, und die Elemente von Ω werden als *Buchstaben* oder *Symbole* bezeichnet.

Ein Wort ist also insbesondere die Konkatenation („Hintereinanderreihung“) von endlich vielen Elementen aus Ω. Ist $w = w_1 w_2 ... w_k$, so schreiben wir $|w| = k$ für die Länge des Wortes w.

Proposition 2.39: Seien $n \in \mathbb{N}$ und $k \in \mathbb{N}_0$. Dann gibt es n^k verschiedene Worte der Länge k über einem Alphabet mit n Symbolen.

Beweis: Sei Ω ein Alphabet mit $|\Omega| = n$. Die Menge der Worte der Länge k über Ω steht auf sehr direkte[3] Art und Weise in Bijektion mit der Menge der k-Tupel über Ω, Ω^k: Durch Konkatenation der einzelnen Komponenten eines Tupels $(w_1, w_2, ..., w_k)$ erhalten wir das entsprechende Wort $w_1 w_2 ... w_k$ – und umgekehrt können wir ebenso natürlich aus dem Wort das entsprechende Tupel gewinnen. Dank Satz 2.8 wissen wir, dass $\left|\Omega^k\right| = |\Omega|^k = n^k$, was gemeinsam mit der Bijektion die Behauptung beweist. □

Beispiel 2.40: Vierstellige Zahlen sind Worte über dem Alphabet $\Omega = \{0, 1, 2, ..., 9\}$ der Länge 4, die nicht mit 0 beginnen. Jedes „verbotene“ Wort beginnt mit 0, gefolgt von einem beliebigen Wort der

[3] Es ist sogar nicht unüblich, die Menge der Worte über Ω der Länge k direkt mit dem kartesischen Produkt Ω^k zu identifizieren.

Länge 3 – diese können wir von der Gesamtzahl einfach abziehen. Es gibt also $|\Omega|^4 - |\Omega|^3 = 10^4 - 10^3 = 10^3 \cdot (10-1) = 9000$ vierstellige Zahlen.

Alternativer Zugang: Es gibt 10 Möglichkeiten für jede Ziffer, abgesehen von der ersten, dort gibt es nur 9 Möglichkeiten. ⬠

Proposition 2.41: Seien $n, k \in \mathbb{N}$ und $n \geq k$. Dann ist die Anzahl der Wörter der Länge k über einem Alphabet der Größe n in denen kein Symbol doppelt vorkommt gleich

$$n \cdot (n-1) \cdot (n-2) \cdots (n-k+1) = \frac{n!}{(n-k)!}.$$

Beweis: Für das erste Symbol gibt es n Möglichkeiten. Das zweite Symbol darf nicht gleich dem ersten sein, es gibt dafür also nur mehr $n-1$ Möglichkeiten. So gibt es für das dritte Symbol nur mehr $n-2$ Möglichkeiten, und so weiter. Das k-te Symbol muss schließlich aus verbleibenden $n-k+1$ möglichen gewählt werden. □

Ein „fallendes Produkt“ wie in der vorhergehenden Proposition kommt auch direkt im Zusammenhang mit dem Binomialkoeffizienten vor. Es ist nützlich, dafür eigene Notation einzuführen.

Definition 2.42 (fallende/steigende Faktorielle): Für $x \in \mathbb{C}$, $k \in \mathbb{N}_0$ schreiben wir

$$x^{\underline{k}} := x \cdot (x-1) \cdot (x-2) \cdots (x-k+1),$$

$$x^{\overline{k}} := x \cdot (x+1) \cdot (x+2) \cdots (x+k-1)$$

für die fallende bzw. steigende Faktorielle. Die steigende Faktorielle ist auch unter dem Namen *Pochhammer-Symbol*[4] bekannt.

Anmerkung 2.43 (verallgemeinerter Binomialkoeffizient, binomische Reihe): Wenn wir die Definition des Binomialkoeffizienten etwas umschreiben,

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

$$= \frac{n \cdot (n-1) \cdots (n-k+1)}{k!} = \frac{n^{\underline{k}}}{k!}$$

so sind wir nun nicht mehr darauf angewiesen, dass $n \in \mathbb{N}_0$ gelten muss: wir können beliebige $n \in \mathbb{C}$ (oder sogar n aus anderen Strukturen) einsetzen. Für $\alpha \in \mathbb{C}$ und $k \in \mathbb{N}_0$ nennen wir

$$\binom{\alpha}{k} := \frac{\alpha^{\underline{k}}}{k!}$$

den *verallgemeinerten Binomialkoeffizienten* α über k. Die Definition mit der fallenden Faktoriellen macht auch klar, dass wenn wir als oberes Argument die Variable x eines Polynomrings $\mathbb{Q}[x]$ einsetzen, $\binom{x}{k} = \frac{x^{\underline{k}}}{k!}$ ein Polynom in x vom Grad k ist.

[4] Nach *Leo August Pochhammer* (1841 – 1920), deutscher Mathematiker.

Eine leicht adaptierte, „analytische“ Fassung des binomischen Lehrsatzes, Satz 2.28, lautet:

Sei $\alpha \in \mathbb{C}$ und $x \in \mathbb{C}$ mit $|x| < 1$. Dann gilt

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

man spricht von der *binomischen Reihe*. Hier ohne Beweis – das überlassen wir der *Analysis*. Aber: wir werden später noch in einem kombinatorischen Kontext auf die binomische Reihe treffen…

Fassen wir die verschiedenen Abzählformeln für verschiedene kombinatorische Objekte aus diesem Kapitel kurz zusammen:

Permutationen	Menge mit n Elementen	$n!$
	Multimenge mit a_j vielen Elementen vom Typ j für $1 \leq j \leq k$ und $a_1 + a_2 + \cdots + a_k = n$	$\binom{n}{a_1; a_2; \ldots; a_k}$
Mengen	Auswahl von k der insgesamt n Elemente	$\binom{n}{k}$
Aufteilung: n Objekte in k Boxen	leere Boxen erlaubt	$\binom{n+k-1}{k-1}$
	leere Boxen nicht erlaubt	$\binom{n-1}{k-1}$
Wörter über Alphabet mit n Symbolen	Wiederholung der Symbole erlaubt	n^k
	jedes Symbol höchstens ein Mal	$n^{\underline{k}}$

2.4 Gitterpfade und Catalan-Zahlen

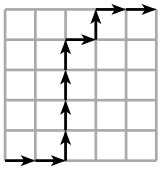
In diesem Abschnitt wollen wir eine klassische Struktur kennenlernen, sogenannte *Gitterpfade*. Diese Strukturen (und ihr stochastisches Pendant, sogenannte *random walks*) sind wichtige Werkzeuge um Prozesse in verschiedenen Disziplinen (z.B. Biologie, Physik, Chemie – aber natürlich auch in innermathematischen Zusammenhängen) zu modellieren.

Definition 2.44 (d-dimensionaler Gitterpfad): Sei $d \in \mathbb{N}$ und $S \subseteq \mathbb{Z}^d$. Für eine Zahl $n \in \mathbb{N}_0$ heißt jede Folge $(s_k)_{0 \leq k \leq n}$ für $s_j \in \mathbb{Z}^d$ mit $s_{j+1} - s_j \in S$ für alle $j \in [n-1]$ ein d-dimensionaler S-Gitterpfad der Länge n. Die Menge S heißt in dem Zusammenhang eine *Schrittmenge*, und die Elemente von S heißen *erlaubte Schritte*.

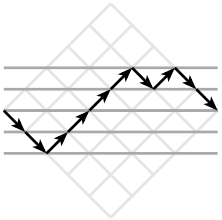
In anderen Worten, *Gitterpfade* sind Folgen von Punkten sodass wir von einem zum nächsten Punkt nur über vorbestimmte Schritte in S gelangen können. Im Rahmen dieser Vorlesung wollen wir uns vor allem auf den Fall $d = 2$ (bzw. eigentlich sogar $d = 1$) beschränken. Im folgenden Beispiel wollen wir die recht abstrakte Definition anhand zweier Beispiele veranschaulichen.

Beispiel 2.45:

Betrachten wir die zweidimensionale Schrittmenge $S_1 = \{(1,0),(0,1)\}$. Dann beschreibt die Folge (0, 0), (1, 0), (2, 0), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4), (3, 5), (4, 5), (5, 5) einen möglichen Gitterpfad von $(0,0) \to (5,5)$. Dieser Pfad ist in der Abbildung rechts durch Pfeile in einem Gitter dargestellt.



Durch Rotation um 45 Grad (und Änderung der Skalierung) erhalten wir einen neuen Pfad bezüglich der Schrittmenge $S_2 = \{(1,1),(1,-1)\}$. Dadurch, dass die x-Koordinate bei den erlaubten Schritten immer gleich 1 ist, ist die gesamte Information über den Pfad in den y-Koordinaten, den „Höhen“ des Pfades, enthalten.



Der betrachtete Pfad ist damit eigentlich *nur* ein eindimensionaler Pfad. ⬠

Proposition 2.46: Sei $S = \{(1,0),(0,1)\}$ und sei $(a,b) \in \mathbb{N}_0^2$ beliebig. Dann gibt es

$$\binom{a+b}{a}$$

verschiedene S-Gitterpfade vom Ursprung $(0,0)$ zum Punkt (a,b).

Beweis: Um vom Ursprung zum Punkt (a,b) zu gelangen brauchen wir einen Gitterpfad in dem a-mal der Schritt nach rechts, $(1,0)$, und b-mal der Schritt nach oben, $(0,1)$, vorkommt. Jede beliebige Permutation dieser $a+b$ Schritte beschreibt genau einen der möglichen Pfade – derer es damit $\binom{a+b}{a;b} = \binom{a+b}{a}$ viele gibt. □

Wir können diese Verbindung zwischen Gitterpfaden und Binomialkoeffizienten nun nutzen, um eine wichtige Identität für Binomialkoeffizienten auf elegant zu beweisen. Dazu halten wir zunächst noch fest, dass der Binomialkoeffizient $\binom{n}{k}$ nach Proposition 2.46 die Anzahl der Gitterpfade vom Ursprung nach $(n-k,k)$ beschreibt.

Satz 2.47 (Vandermonde[5]-Identität): Für beliebige $a,b,n \in \mathbb{N}_0$ gilt die Identität

$$\sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k} = \binom{a+b}{n}. \tag{3}$$

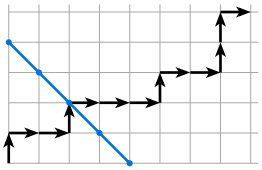
Beweis: Wir beweisen die Formel durch doppeltes Abzählen mit $\{(1,0),(0,1)\}$-Gitterpfaden. Die rechte Seite von (3) zählt die Anzahl der von $(0,0)$ nach $(a+b-n,n)$ reichenden Gitterpfade.

Betrachten wir nun einen der Summanden auf der linken Seite der Behauptung. Darin zählt der Binomialkoeffizient $\binom{a}{k}$ die Anzahl der Pfade von $(0,0) \to (a-k,k)$, und der Binomialkoeffizient $\binom{b}{n-k}$ die Anzahl der Pfade von $(0,0) \to (b-n+k,n-k)$. Der erste der beiden Pfade hat

[5] Alexandre-Théophile Vandermonde (1735 – 1796), französischer Mathematiker.

Länge a, der zweite hat Länge b. Wir kombinieren die beiden Pfade jetzt zu einem Pfad der Länge $a+b$, indem wir den zweiten Pfad ans Ende des ersten Pfades anhängen. So entsteht ein Pfad von $(0,0) \to (a-k,k) \to (a-k+b-n+k, k+n-k) = (a+b-n, n)$. Ein Summand auf der linken Seite von (3) zählt also alle jene Gitterpfade, die von $(0,0)$ über $(a-k,k)$ nach $(a+b-n,n)$ laufen.

Die Zwischenpunkte liegen für verschiedene Werte von k auf einer Geraden, die von jedem Pfad vom Ursprung zum Zielpunkt in einem der möglichen Zwischenpunkte passiert werden muss.



Die linke und rechte Seite von (3) zählen daher beide die gleichen Pfade – was die Behauptung beweist. □

Korollar 2.48: Für $n \in \mathbb{N}_0$ gilt die Beziehung

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

Beweis: Wir setzen $a = b = n$ in Satz 2.47 und verwenden die Symmetrie des Binomialkoeffizienten. □

Anmerkung 2.49: Der Binomialkoeffizient $\binom{2n}{n}$ wird auch oft *zentraler Binomialkoeffizient* genannt. Bei einer Schrittmenge mit Schritten nach Norden und Osten zählt er die Anzahl der Pfade durch ein quadratisches Gitter – vom Ursprung bis nach (n,n). Im Modell mit Schritten $(1,1)$ und $(1,-1)$ zählt er die Anzahl der Pfade von $(0,0)$ nach $(2n,0)$.

Wieder können wir die Identität für konkrete Werte von n leicht mit SageMath verifizieren:

```
sage: sum(binomial(10, k)^2 for k in srange(11)) == binomial(20, 10)
True
```

Tatsächlich kann die Summe aus dem Korollar sogar symbolisch berechnet werden – führt in diesem Fall aber zu einem Ausdruck, für den wir mit unserem aktuellen Wissensstand nicht entscheiden können, ob er richtig ist…

```
sage: var('n k')
sage: assume(n, 'integer'); assume(k, 'integer')
sage: sum(binomial(n, k)^2, k, 0, n)
2^(2*n)*factorial(n - 1/2)/(sqrt(pi)*factorial(n))
```

Die Bestimmung der Anzahl der verschiedenen Gitterpfade einer vorgegebenen Länge n ist ein klassisches Problem in der abzählenden Kombinatorik. Typischerweise wird es umso schwerer die exakte Anzahl zu bestimmen, je mehr Einschränkungen an die entsprechende Familie von Pfaden gestellt werden.

Beispiel 2.50 (Kreweras-Pfade): Wir betrachten die Schrittmenge $S = \{(-1,0),(0,-1),(1,1)\}$. Wenn wir unsere Aufmerksamkeit jetzt nur auf genau jene Gitterpfade richten, die ...

- ihren Start im Ursprung $(0,0)$ haben,
- den 1. Quadranten nicht verlassen,
- und am Ende wieder zum Ursprung zurückkehren,

... so erhalten wir die sogenannten *Kreweras*[6]*-Pfade*. Kreweras konnte 1965 durch einen „guess and prove"-Ansatz zeigen, dass die Anzahl solcher Pfade der Länge n durch

$$\frac{4^n}{(n+1)(2n+1)}\binom{3n}{n}$$

gegeben ist; die ersten paar Werte dieser Folge sind

```
sage: [binomial(3*n, n) * 4^n / ((n + 1) * (2*n + 1)) for n in srange(10)]
[1, 2, 16, 192, 2816, 46592, 835584, 15876096, 315031552, 6466437120]
```

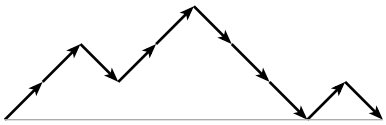
Während es wünschenswert wäre, eine „einfache" kombinatorische Erklärung dieser Abzählformel zu finden, ist das immer noch ein offenes (und intensiv untersuchtes) Problem. ⬠

Damit wollen wir uns jetzt einer anderen Familie von Gitterpfaden zuwenden (die im Gegensatz zu den Kreweras-Pfaden eine einfachere und kombinatorisch leicht beweisbare Abzählformel besitzen). Wir motivieren die Familie durch das folgende Problem.

Beispiel 2.51: Eine Studentin hat in ihrem Zimmer eine Schachtel mit Wechselgeld. Am Anfang ist die Schachtel leer, dann legt sie jeden Tag entweder eine Münze hinein, oder nimmt eine Münze heraus. Am Ende des 10. Tages ist die Schachtel leer. Auf wie viele Arten kann das passiert sein?

Wir modellieren die Situation als Gitterpfad mit Schritten $S = \{(1,1),(1,-1)\}$, wobei ein Schritt $(1,1)$ für das Hinzugeben einer Münze, und $(1,-1)$ für das Herausnehmen steht. Wenn wir den Pfad im Ursprung $(0,0)$ starten lassen, so können wir von der x-Koordinate des Pfades die Anzahl der bisher vergangenen Tage ablesen, und an der y-Koordinate die aktuelle Anzahl der Münzen in der Schachtel. Die relevanten Pfade können also notwendigerweise nicht unter die Achse fallen.

Die Frage nach der Anzahl der möglichen *Münzanzahl-Verläufe* ist also äquivalent zur Frage nach der Anzahl der möglichen Pfade, die...



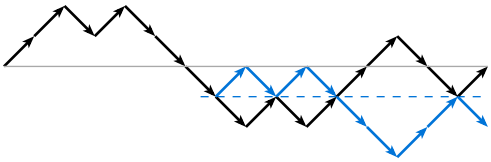
- in $(0,0)$ starten und in $(10,0)$ enden,
- und die nie unter die x-Achse fallen.

Der Wert von 10 ist für die folgenden Überlegungen unerheblich, wir schreiben daher einfach $10 = 2n$. Nach Anmerkung 2.49 wissen wir, dass *alle* möglichen Pfade von $(0,0) \to (2n,0)$ durch den zentralen Binomialkoeffizienten $\binom{2n}{n}$ gezählt werden. Wenn wir es schaffen, nun alle „verbotenen" Pfade zu zählen, die also an irgendeiner Stelle die x-Achse unterschreiten, so könnten wir die Anzahl der gesuchten Pfade, C_n, als Differenz zu $\binom{2n}{n}$ ermitteln: $C_n = \binom{2n}{n} -$ verbotene Pfade.

Die „verbotenen" Pfade lassen sich durch das sogenannte *Spiegelungsprinzip* zählen.

[6] Nach Germain Kreweras (1918 – 1998), französischer Mathematiker.

Dazu gehen wir so vor: für einen gegebenen verbotenen Pfad P konstruieren wir uns einen neuen „gespiegelten“ Pfad indem wir P bis zum ersten Punkt kopieren an dem er die x-Achse unterschreitet. Dann hängen wir den Rest von P an der Gerade $y = -1$ gespiegelt an.



Der so erhaltene Pfad führt nicht mehr vom Ursprung nach $(2n, 0)$: der Teil bis inklusive dem ersten Schritt unter die Achse ist gleich, aber während der ursprüngliche Pfad dann von Höhe -1 bis zum Ende zurück auf die Achse (also Höhe 0) steigt, muss der gespiegelte Teil bis zum Ende genau in die andere Richtung gehen, also bei einem y-Wert von -2, und damit im Punkt $(2n, -2)$, enden.

Diese Spiegelung lässt sich aber auch (auf die genau gleiche Art und Weise) wieder umkehren: für einen beliebigen Pfad der von $(0, 0) \to (2n, -2)$ reicht muss es einen Punkt geben an dem er das erste Mal unter die x-Achse fällt. Spiegeln wir dann den Rest des Pfades entsteht wieder ein „verbotener“ Pfad von $(0, 0) \to (2n, 0)$. Die (teilweise) Spiegelung beschreibt damit eine Bijektion zwischen den „verbotenen Pfaden“ und beliebigen Pfaden von $(0, 0) \to (2n, -2)$.

Letztere können wir leicht zählen: die Pfade von $(0, 0) \to (2n, -2)$ enthalten $2n$ Schritte, davon müssen $n - 1$ Schritte nach oben, und $n + 1$ Schritte nach unten gehen. Die Anzahl ist daher gleich der Anzahl der Möglichkeiten, $n + 1$ von $2n$ Stellen auszuwählen an denen die Schritte nach unten platziert werden – also $\binom{2n}{n+1}$ viele.

Für C_n, die Anzahl unserer gesuchten „erlaubten“ Pfade ergibt sich damit also

$$\begin{aligned} C_n &= \binom{2n}{n} - \binom{2n}{n+1} = \frac{(2n)!}{n!\,n!} - \frac{(2n)!}{(n+1)!\,(n-1)!} \\ &= \frac{(2n)!}{n!\,(n-1)!}\left(\frac{1}{n} - \frac{1}{n+1}\right) = \frac{(2n)!}{n!\,(n-1)!}\left(\frac{(n+1)-n}{n(n+1)}\right) \\ &= \frac{(2n)!}{n!\,n!}\frac{1}{n+1} = \frac{1}{n+1}\binom{2n}{n}. \end{aligned}$$

Einsetzen liefert schließlich die gesuchte Antwort: die Münzen konnten auf $C_5 = \frac{1}{6}\binom{10}{5} = 42$ verschiedene Arten hinzugefügt und entfernt werden. ⬠

Wir haben im vorhergehenden Beispiel eine klassische Familie von Gitterpfaden – die sogenannten *Dyck*[7]*-Pfade* – kennengelernt und deren Anzahl für eine gegebene (Halb-)Länge n bestimmt. Das Ergebnis verdient es jedenfalls, nochmals separat festgehalten zu werden.

Satz 2.52: Sei $n \in \mathbb{N}_0$. Dann gibt es

$$C_n := \frac{1}{n+1}\binom{2n}{n} \tag{4}$$

[7]Nach Walther Franz Anton Ritter von Dyck, 1856 – 1934, deutscher Mathematiker und ehemaliger Rektor der TU München.

viele Dyck-Pfade (Gitterpfade bezüglich $S = \{(1, -1), (1, 1)\}$ die im Ursprung starten, nie unter die x-Achse fallen, und wieder auf der Achse enden) mit $2n$ Schritten.

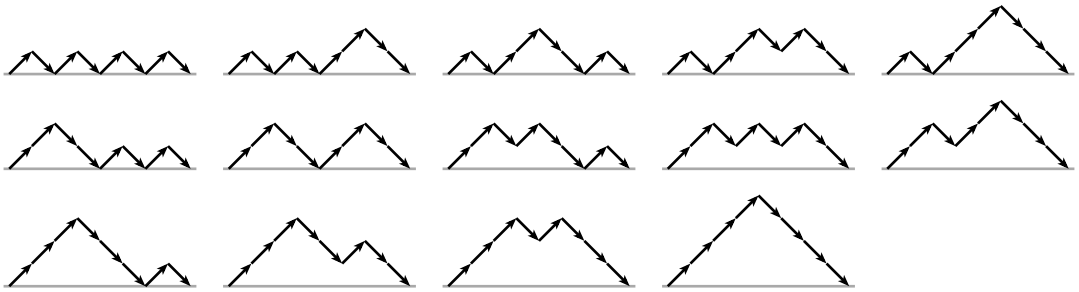


Abbildung 4: Alle $C_4 = 14$ Dyck-Pfade mit 8 Schritten.

Beweis: In Beispiel 2.51 durch das Spiegelungsprinzip erledigt. □

Definition 2.53 (Catalan-Zahlen): Die Zahlen

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

werden *Catalan-Zahlen* genannt.

Anmerkung 2.54: Die Folge der Catalan-Zahlen ist die vermutlich wichtigste Zahlenfolge in der abzählenden Kombinatorik (vielleicht mit Ausnahme der Folge der natürlichen Zahlen selbst). Es gibt über 100 verschiedene kombinatorische Objekte und Parameter die auf mehr oder weniger direkte Art und Weise mit den Catalan-Zahlen zusammenhängen. Die ersten paar Glieder der Folge (beginnend bei $C_0 = C_1 = 1$) sind

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, 742900, 2674440, \ldots$$

Zu den kombinatorischen Objekten die durch Catalan-Zahlen gezählt werden gehören beispielsweise

- Dyck-Pfade der Länge $2n$,
- die Anzahl der Möglichkeiten, ein konvexes $(n+2)$-Eck in Dreiecke zu zerlegen (zu *triangulieren*),
- die Anzahl der Möglichkeiten ein Produkt mit $(n+1)$-vielen Faktoren legal zu klammern,
- die Anzahl der verschiedenen Binärbäume mit n inneren Knoten,
- die Anzahl der planaren Bäume mit insgesamt $n+1$ Knoten,
- die Anzahl der Möglichkeiten, wie sich $2n$ Personen die um einen runden Tisch herum sitzen über den Tisch hinweg die Hände überkreuzungsfrei reichen können,
- und noch viele, viele mehr.

Die Folge wird in der *Online Encyclopedia of Integer Sequences* unter dem Eintrag A000108 gelistet. Das Buch *Catalan Numbers* von Richard Stanley enthält eine lange, explizite Liste mit verschiedenen Anwendungen dieser Zahlen.

In SageMath sind natürlich einerseits die numerischen Werte der Catalan-Zahlen selbst über die `catalan_number`-Funktion zugänglich:

```
sage: [catalan_number(n) for n in srange(10)]
[1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862]
```

Andererseits sind aber auch diverse von Catalan-Zahlen gezählte Objekte implementiert. Direkt mit den Dyck-Pfaden verwandt sind sogenannte Dyck-Wörter, die etwa balancierten Klammerausdrücken entsprechen:

```
sage: [str(word) for word in DyckWords(3)]
['()()()', '()(())', '(())()', '(()())', '((()))']
```

Diesen Dyck-Objekt-Generator können wir nutzen um Objekte mit speziellen Eigenschaften zu finden, wie etwa den Pfad der Länge 20 mit den meisten „Gipfeln“,

```
sage: max_peaks_word = max(DyckWords(10), key=lambda word: len(word.peaks()))
sage: str(max_peaks_word)
'()()()()()()()()()()'
```

oder die Anzahl der „symmetrischen“ Dyck-Pfade zu finden:

```
sage: num_symmetric_paths = []
sage: for n in srange(10):
....:     symmetric_paths = [word for word in DyckWords(n) if word == word.reverse()]
....:     num_symmetric_paths.append(len(symmetric_paths))
....:
sage: num_symmetric_paths
[1, 1, 2, 3, 6, 10, 20, 35, 70, 126]
```

2.5 Inklusions-Exklusions-Prinzip

Wir haben das Inklusions-Exklusions-Prinzip bereits in seiner einfachsten Form in Satz 2.8 in Aktion gesehen, bei der Beobachtung dass sich die Anzahl der Elemente in der Vereinigung zweier Mengen A und B nicht notwendigerweise einfach nur aus der Summe $|A| + |B|$ ergibt. Falls die beiden Mengen nicht disjunkt sind, also manche Elemente gemeinsam haben, dann würden wir genau diese bei der Summe doppelt zählen – was wir durch das Abziehen der Anzahl der gemeinsamen Elemente korrigieren müssen: $|A \cup B| = |A| + |B| - |A \cap B|$.

Im folgenden Beispiel wollen wir das Prinzip an einem etwas größeren konkreten Beispiel untersuchen.

Beispiel 2.55: Mathematik-Studierende sind sehr sportlich.

- 14 Personen spielen Tennis,
- 10 Personen spielen Fußball,
- 15 Personen spielen Volleyball,
- je 4 Personen spielen Tennis und Fußball, sowie Tennis und Volleyball,
- 5 Personen spielen Fußball und Volleyball,
- und zwei Personen betreiben alle drei Sportarten.

Neben den oben erwähnten Studierenden gibt es auch noch ein paar, die keine der drei Sportarten betreiben – konkret halb so viele wie die oben gezählten. Wie viele Studierende gibt es insgesamt?

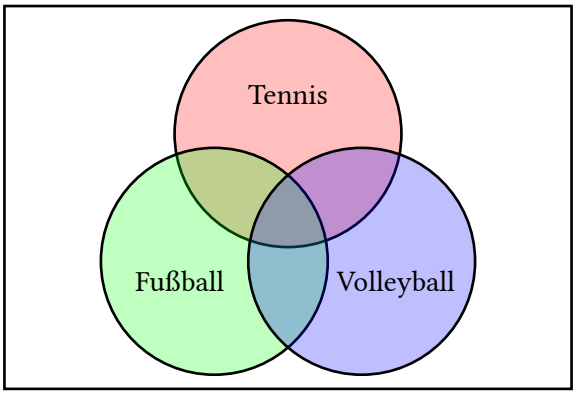


Abbildung 5: Veranschaulichung der Situation im Beispiel durch ein Venn-Diagramm.

Wenn wir einfach die 14 Tennisspieler:innen, die 10 Fußballspieler:innen und die 15 Volleyballspieler:innen zusammenzählen, dann erhalten wir $14 + 10 + 15 = 39$ – zählen dabei aber jene Studierende, die mehr als eine Sportart betreiben mehrfach. Konkret werden dabei die 4 Tennis- und Fußballspieler:innen, die 4 Tennis- und Volleballspieler:innen, und die 5 Fußball- und Volleyballspieler:innen jeweils doppelt gezählt. Ziehen wir die Anzahl ab erhalten wir $39 - (4 + 4 + 5) = 26$. Die 2 Studierenden, die alle drei Sportarten betreiben wurden zuerst dreifach gezählt, im zweiten Schritt jetzt aber auch wieder dreifach abgezogen: sie werden im letzten Zwischenergebnis, 26, also gar nicht gezählt. Die Anzahl aller Studierenden, die mindestens eine der drei Sportarten betreiben, beträgt also $26 + 2 = 28$.

Zuzüglich gibt es jetzt noch einmal halb so viele, $\frac{28}{2} = 14$, Studierende, die keine der drei Sportarten betreiben, womit wir insgesamt also $28 + 14 = 42$ Studierende zählen. ⬠

Systematisch, auf die gleiche Art und Weise wie in diesem Beispiel, können wir uns die Situation auch allgemein für n Mengen überlegen. Die zentrale Beobachtung ist dabei, dass wir die Anzahl der verschiedenen Elemente; die Kardinalität der Vereinigung der Mengen, aus der Summe der Einzelkardinalitäten nach schrittweiser Korrektur durch abwechselndes Abziehen und Wiederhinzufügen der mehrfach vorkommenden Elemente erhalten.

Satz 2.56 (Inklusions-Exklusions-Prinzip): Sei $n \in \mathbb{N}$ und seien $A_1, A_2, \ldots, A_n$ endliche Mengen. Dann ist

$$\left|\bigcup_{j=1}^{n} A_j\right| = \sum_{\emptyset \neq J \subseteq [n]} (-1)^{|J|+1} \left|\bigcap_{j \in J} A_j\right|. \tag{5}$$

Beweis: Sei x ein beliebiges Element (es ist nicht erforderlich, dass x in einer oder mehrerer der Mengen A_j enthalten ist). Wir definieren uns die Indexmenge $K := \{k \in [n] \mid x \in A_k\}$, also die Menge der Indizes jener Mengen, die x enthalten.

Wir zählen jetzt, wie oft das beliebige Element x auf der linken bzw. rechten Seite von (5) gezählt wird.

Zunächst, falls $K = \emptyset$ ist (x also in keiner der Mengen A_j vorkommt), so wird x weder auf der linken noch auf der rechten Seite von (5) gezählt.

Andernfalls ist $K \neq \emptyset$, kommt also in der Vereinigung $\bigcup_{j=1}^{n} A_j$ genau einmal vor, und wird damit auf der linken Seite genau einmal gezählt. Untersuchen wir die rechte Seite:

$$\begin{aligned}\sum_{\emptyset \neq J \subseteq [n]} (-1)^{|J|+1} \left[\!\!\left[x \in \bigcap_{j \in J} A_j \right]\!\!\right] &= \sum_{\emptyset \neq J \subseteq [n]} (-1)^{|J|+1} \left[\!\!\left[\bigwedge_{j \in J} x \in A_j \right]\!\!\right] \\ &= \sum_{\emptyset \neq J \subseteq [n]} (-1)^{|J|+1} [\![J \subseteq K]\!] \\ &= \sum_{\emptyset \neq J \subseteq K} (-1)^{|J|+1}.\end{aligned}$$

Diese Summe können wir weiter vereinfachen, indem wir die Summe über die Teilmengen nach der Kardinalität der Menge J gruppieren und uns daran erinnern, dass es genau $\binom{|K|}{\ell}$ Teilmengen von K mit ℓ Elementen gibt:

$$\begin{aligned}\sum_{\emptyset \neq J \subseteq K} (-1)^{|J|+1} &= \sum_{\ell=1}^{|K|} \sum_{\substack{J \subseteq K \\ |J|=\ell}} (-1)^{\ell+1} = \sum_{\ell=1}^{|K|} (-1)^{\ell+1} \cdot \sum_{\substack{J \subseteq K \\ |J|=\ell}} 1 \\ &= \sum_{\ell=1}^{|K|} (-1)^{\ell+1} \binom{|K|}{\ell} = 1 - \sum_{\ell=0}^{|K|} (-1)^{\ell} \binom{|K|}{\ell} \\ &= 1 - (1-1)^{|K|} = 1.\end{aligned}$$

Ein beliebiges Element x wird damit also entweder auf beiden Seiten genau einmal, oder gar nicht gezählt. □

Beispiel 2.57 (Fixpunktfreie Permutationen / Derangements): Eine Abendveranstaltung wird von n huttragenden Mathematiker:innen besucht, bei der sie ihre Hüte jeweils zu Beginn bei der Garderobe abgeben. Am Ende der Veranstaltung bricht Chaos bei der Hutrückgabe aus: die Zuordnungen sind durcheinander geraten, und jede:r Besucher:in erhält einen zufälligen Hut zurück. Tatsächlich stellen die Mathematiker:innen fest, dass *niemand* den eigenen Hut zurückerhalten hat. Bei wie vielen der möglichen Zuordnungen passiert das?

Mathematisch können wir diese Frage in die Ermittlung der Anzahl der *fixpunktfreien Permutationen* übersetzen: wir suchen die Anzahl der bijektiven Funktionen $\sigma : [n] \to [n]$ mit $\sigma(i) \neq i$ für alle $1 \leq i \leq n$. Die Zuordnung $i \mapsto \sigma(i)$ modelliert dabei, dass Person i den Hut von Person $\sigma(i)$ erhält.

Wir definieren $A_i := \{\sigma \text{ Permutation auf } [n] \mid \sigma(i) = i\}$, die Menge der Permutationen die i als Fixpunkt besitzen. Die Vereinigung $A_1 \cup A_2 \cup \ldots \cup A_n$ beschreibt dann die Menge der Permutationen mit mindestens einem Fixpunkt. Nach Satz 2.56 können wir die Kardinalität der dieser Vereinigung bestimmen, wenn wir die Kardinalität der Schnittmengen der A_i kennen. Dazu beobachten wir: für eine gegebene Teilmenge $J \subseteq [n]$ bedeutet $\sigma \in \bigcap_{j \in J} A_j$, dass $\sigma(j) = j$ für alle $j \in J$ fixiert ist. Es bleiben damit nur noch $n - |J|$ frei zu wählende Elemente, wofür es $(n - |J|)!$ viele Möglichkeiten

gibt. Daher ist $\left|\bigcap_{j\in J} A_j\right| = (n-|J|)!$, und wir können das Prinzip von Inklusion und Exklusion anwenden.

Die Anzahl der Permutationen die mindestens einen Fixpunkt besitzen ist also

$$\begin{aligned}|A_1 \cup \ldots \cup A_n| &= \sum_{\emptyset\neq J\subseteq[n]} (-1)^{|J|+1}(n-|J|)! = \sum_{\ell=1}^{n}\sum_{\substack{J\subseteq[n]\\|J|=\ell}} (-1)^{\ell+1}(n-\ell)! \\ &= \sum_{\ell=1}^{n}(-1)^{\ell+1}(n-\ell)!\binom{n}{\ell} = \sum_{\ell=1}^{n}(-1)^{\ell+1}\frac{n!}{\ell!} \\ &= n!\sum_{\ell=1}^{n}\frac{(-1)^{\ell+1}}{\ell!}.\end{aligned}$$

Als direkte Konsequenz erhalten wir damit auch die Anzahl der fixpunktfreien Permutationen (*Derangements*) als Differenz zur Gesamtanzahl aller Permutationen von $[n]$, nämlich

$$n! - n!\sum_{\ell=1}^{n}\frac{(-1)^{\ell+1}}{\ell!} = n!\left(1+\sum_{\ell=1}^{n}\frac{(-1)^{\ell}}{\ell!}\right) = n!\sum_{\ell=0}^{n}\frac{(-1)^{\ell}}{\ell!}.$$

Das ist die gesuchte Anzahl der Möglichkeiten, dass niemand den eigenen Hut erhält. Unter der Annahme, dass alle $n!$ Permutationen der Hüte gleich wahrscheinlich sind (in diesem Fall spricht man oft von einer *kombinatorischen Wahrscheinlichkeit*; „günstige durch mögliche Fälle“) beträgt die Wahrscheinlichkeit, dass von n Personen niemand den eigenen Hut zurückerhält damit gleich

$$\frac{n!\sum_{\ell=0}^{n}\frac{(-1)^{\ell}}{\ell!}}{n!} = \sum_{\ell=0}^{n}\frac{(-1)^{\ell}}{\ell!} \xrightarrow{n\to\infty} \frac{1}{e} \approx 0.3679\ldots,$$

wobei sich die gegebene Reihe numerisch sehr schnell stabilisiert und selbst für kleine n bereits nah an $\frac{1}{e}$ liegt. ⬠

§3 – Graphentheorie

In diesem Kapitel beschäftigen wir uns mit *Graphen*. Ein Graph ist eine abstrakte Struktur, die eine Menge von Objekten und Verbindungen zwischen manchen dieser Objekten darstellt. Dargestellt wird ein Graph durch Punkte, welche die Objekte repräsentieren, und durch Linien, die diese Punkte verbinden und die Verbindungen zwischen den Objekten repräsentieren. Später werden wir die Objekte *Knoten* und die Linien *Kanten* nennen.

Graphen sind in vielerlei Bereichen von großer Bedeutung und viele Sachverhalte können mithilfe von Graphen modelliert werden. Beispielsweise lässt sich das U-Bahn-Netz einer Stadt mittels Graphen darstellen. Des Weiteren lässt sich die Route eines Postboten mit Graphen modellieren: Jeder Knoten im Graphen repräsentiert ein Haus und zwei Knoten sind durch eine Kante verbunden, wenn es eine Straße zwischen den entsprechenden Häusern gibt. Ordnet man den Kanten noch die Länge der Straße zu, so kann man die Route des Postboten optimieren und die kürzeste Route suchen.

Auch Stammbäume sind Graphen, in denen die Familienmitglieder die Knoten sind und Verwandschaftsverhältnisse durch Kanten repräsentiert werden. Außerdem stellen Graphen in der Informatik eine wichtige Struktur zum Speichern von Daten dar.

Das soll nun Motivation genug sein, um uns etwas näher mit dieser Struktur zu beschäftigen, spezielle Graphen anzusehen und deren Eigenschaften zu untersuchen.

3.1 Definitionen und Begriffe

Definition 3.1 (Graph, Knoten, Kante): Ein *Graph* G ist ein Paar (V, E), wobei V eine beliebige Menge und E eine Menge mit $E \subseteq \{\{i, j\} \mid i, j \in V, i \neq j\}$ ist.

- V heißt die Menge der *Knoten / Ecken / nodes / vertices*,
- E heißt die Menge der *Kanten / edges*.

Die Kardinalität der Knotenmenge, $|V|$ wird *Ordnung* (bzw. manchmal auch *Größe*) des Graphen G genannt. Falls $|V| < \infty$, dann heißt G ein *endlicher Graph*.

Im Rahmen dieser Lehrveranstaltung betrachten wir in erster Linie *endliche Graphen*: falls nicht explizit die Rede von unendlichen Graphen ist, so setzen wir $|V| < \infty$ voraus.

Notation 3.2: Für einen Graphen G schreiben wir $V(G)$ und $E(G)$ für die Knoten- bzw. Kantenmenge von G. Für eine Kante $\{i, j\} \in E(G)$ schreiben wir abkürzend auch einfach $ij \in E(G)$.

Beispiel 3.3 (Ein Graph und seine Darstellung): Gegeben seien $V = [5]$ und $E = \{\{1, 2\}, \{2, 3\}, \{3, 1\}, \{3, 4\}\}$. Dann ist $G = (V, E)$ ein Graph der Ordnung 5 und kann graphisch folgend dargestellt werden: wir zeichnen alle Knoten als „Punkte“ und verbinden je zwei Knoten i und j mit einer Linie falls $\{i, j\} \in E$. Der Graph G ist so wie hier beschrieben in Abbildung 6 dargestellt.⬠

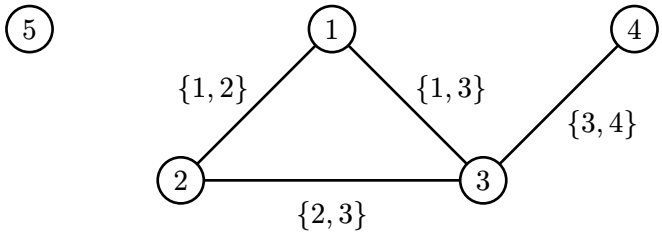


Abbildung 6: Ein Graph G auf 5 Knoten.

Definition 3.4 (Adjazenz, Inzidenz): Sei $G = (V, E)$ ein Graph.

1. Zwei Knoten $i, j \in V$ heißen *adjazent*, falls $\{i, j\} \in E$; wenn sie also durch eine Kante verbunden sind.
2. Zwei Kanten $e, f \in E$ heißen *adjazent*, falls $e \cap f \neq \emptyset$; das heißt, wenn sie einen gemeinsamen Knoten haben.
3. Ein Knoten $i \in V$ und eine Kante $e \in E$ heißen *inzident*, falls $i \in e$.
4. Falls $e \in E$ mit $e = \{i, j\}$, so heißen die Knoten i und j die *Endpunkte* von e.

Beispiel 3.5 (Fortsetzung von Beispiel 3.3): Wir betrachten wieder den Graphen $G = (V, E)$ mit

$$V = [5], \quad E = \{\{1, 2\}, \{2, 3\}, \{3, 1\}, \{3, 4\}\}.$$

Die Knoten 1 und 2, 2 und 3, 3 und 1, sowie 3 und 4 sind jeweils adjazent. Weiters sind etwa die Kanten $\{1, 2\}$ und $\{1, 3\}$ adjazent, da sie gemeinsam den Knoten 1 enthalten. Die Kante $\{1, 2\}$ ist inzident zu den Knoten 1 und 2. ⬠

Definition 3.6 (Unabhängige Menge / Clique): Sei $G = (V, E)$ ein Graph und sei $W \subseteq V$ eine Teilmenge der Knoten.

a) Falls je zwei Knoten in W nicht adjazent sind, so heißt W eine *unabhängige Menge* (oder *stabile Menge*, *Anticlique*, *Co-Clique*).

b) Falls, andererseits, je zwei Knoten in W adjazent sind, so heißt W eine *Clique*.

Beispiel 3.7 (Fortsetzung von Beispiel 3.3): Im Graphen $G = (V, E)$ aus Beispiel 3.3 ist $\{1, 4, 5\} \subseteq V$ eine unabhängige Menge, da es keine Kanten zwischen den Knoten 1, 4, und 5 gibt.

Wir wollen nun auch alle Cliquen im Graphen G suchen. Wir betrachten die Teilmengen der Größe nach:

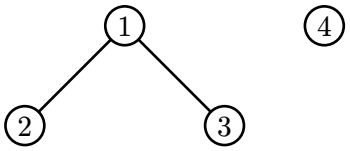
- Größe 1: jeder einzelne Knoten ist eine Clique.
- Größe 2: jede Kante $e \in E$ ist eine Clique.
- Größe 3: die Knoten $W = \{1, 2, 3\}$ formen ein *Dreieck* – eine Clique der Größe 3, da sie alle untereinander verbunden sind.

⬠

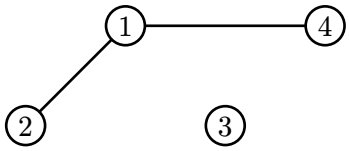
Definition 3.8 (Teilgraph): Sei $G = (V, E)$ ein Graph, $W \subseteq V$ und $F \subseteq E$ mit $f \subseteq W$ für alle $f \in F$.

1. Der Graph $H = (W, F)$ heißt ein *Teilgraph* oder *Subgraph* von G, in Zeichen $H \subseteq G$.
2. Der Teilgraph $H = (W, F)$ heißt *aufspannend*, falls $W = V$.
3. Sei $e \in E$. Für den aufspannenden Teilgraphen von G, der bis auf die Kante e auch die gleichen Kanten enthält, schreiben wir $G - e := (V, E \setminus \{e\})$.
4. Jener Teilgraph, der entsteht wenn alle nicht in W enthaltenen Knoten (sowie alle dazu inzidenten Kanten) aus G entfernt werden, heißt der *von W induzierte Teilgraph* von G; wir schreiben
$$G[W] := (W, \{\{i, j\} \in E \mid i, j \in W\}).$$

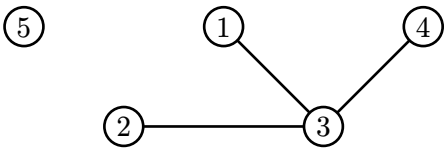
Beispiel 3.9 (Fortsetzung von Beispiel 3.3): Wir betrachten wieder den Graphen $G = (V, E)$ mit
$$V = [5], \quad E = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{3, 4\}\}.$$
Wir betrachten die folgenden vier Graphen:



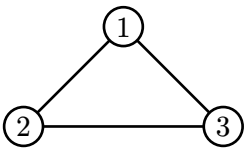
$H_1 = (\{1, 2, 3, 4\}, \{\{1, 2\}, \{1, 3\}\})$



$H_2 = (\{1, 2, 3, 4\}, \{\{1, 3\}, \{1, 4\}\})$



$H_3 = G - \{1, 2\}$



$H_4 = G[\{1, 2, 3\}]$

Von den vier Graphen ist H_1 ein Teilgraph von G, H_2 hingegen ist *kein* Teilgraph da $\{1, 4\} \notin E(G)$ ist. Der Graph H_3 entsteht durch Löschung der Kante $\{1, 2\}$ aus G (und ist insbesondere ein aufspannender Teilgraph) – und der Graph H_4 ist der durch $\{1, 2, 3\}$ induzierte Teilgraph von G. ⬠

Definition 3.10 (Isomorphe Graphen): Seien G und H zwei Graphen. Gibt es eine bijektive Abbildung $\varphi : V(G) \to V(H)$ mit der Eigenschaft
$$\{i, j\} \in E(G) \iff \{\varphi(i), \varphi(j)\} \in E(H),$$
so heißen G und H *zueinander isomorph* und wir schreiben $G \cong H$.

Beispiel 3.11: Wir betrachten die beiden Graphen H_1 und H_2 mit
$$H_1 = ([5], \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{5, 1\}\})$$
und
$$H_2 = (\{a, ..., e\}, \{\{a, c\}, \{a, d\}, \{b, d\}, \{b, e\}, \{c, e\}\}).$$

Die Abbildung $\varphi : V(H_1) \to V(H_2)$ mit $1 \mapsto c, 2 \mapsto e, 3 \mapsto b, 4 \mapsto d, 5 \mapsto a$ ist als „1 zu 1“-Abbildung zwischen den Knotenmengen jedenfalls bijektiv – und es lässt sich leicht überprüfen, dass $\{i, j\} \in E(H_1)$ genau dann der Fall ist, wenn $\{\varphi(i), \varphi(j)\} \in E(H_2)$ vorliegt.

Die beiden Graphen sind also bijektiv zueinander, $H_1 \cong H_2$. Ebenso leicht lässt sich feststellen, dass H_1 nicht zum Graphen G aus Beispiel 3.3 isomorph ist: in H_1 besitzt jeder Knoten mindestens eine inzidente Kante, in G hingegen ist Knoten 5 isoliert. ⬠

Definition 3.12 (gerichteter Graph): Seien V, A zwei Mengen und $\text{head}, \text{tail} : A \to V$ zwei Abbildungen. Dann heißt das Tupel $D = (V, A)$ zusammen mit den Abbildungen head und tail ein *gerichteter Graph*. Die Menge V wird die Knotenmenge von D genannt und die Elemente in A heißen die *Bögen* (engl.: *arcs*) von D. Die Menge A wird dementsprechend die *Bogenmenge* genannt. Ein Bogen $a \in A$ mit $\text{head}(a) = \text{tail}(a)$ heißt *Schleife*.

Beispiel 3.13: Gerichtete Graphen können ähnlich wie normale („ungerichtete“) Graphen durch Knoten und Verbindungen dargestellt werden. Statt Linien kommen hier jedoch Pfeile zum Einsatz, wobei für ein $a \in A$ der Pfeil von $\text{tail}(a)$ nach $\text{head}(a)$ zeigt. Für die Menge $V = [5]$ mit $A = \{a_1, ..., a_6\}$ und den durch

	a_1	a_2	a_3	a_4	a_5	a_6
head	1	2	3	1	1	1
tail	2	1	3	4	5	5

gegebenen Abbildungen lässt sich der Graph $D = (V, A)$ wie in Abbildung 7 darstellen. ⬠

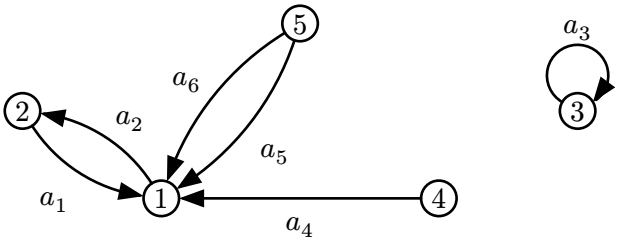


Abbildung 7: Der gerichtete Graph aus Beispiel 3.13.

Praktisch könnten wir gerichtete Graphen auch definieren, indem wir als Kantenmenge einfach eine Teilmenge der geordneten Knotenpaare, $A \subseteq V \times V$ erlauben. Die Definition über die Abbildungen head und tail ist jedoch eher mit der folgenden Verallgemeinerung von ungerichteten Graphen kompatibel.

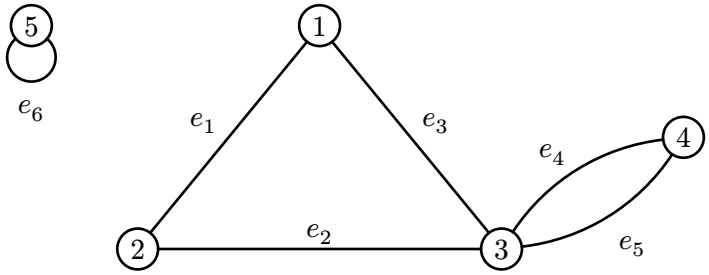
Definition 3.14 (Multigraph): Seien V, E Mengen. Dann ist das Paar $G = (V, E)$ gemeinsam mit einer Abbildung $\varphi : E \to V \cup \{\{i, j\} : i, j \in V, i \neq j\}$ ein *Multigraph*.

Im Gegensatz zur formalen Definition von Graphen aus Definition 3.1 erlaubt es die Definition eines Multigraphen, dass zwei Knoten durch mehrere verschiedene Kanten verbunden sind. Außerdem sind auch Schleifen erlaubt; das sind jene Kanten $e \in E$ die durch die Abbildung φ auf einen einzelnen Knoten statt auf eine zweielementige Teilmenge abgebildet werden.

Beispiel 3.15: Der Multigraph, der durch $V = [5]$, $E = \{e_1, ..., e_6\}$ und der Abbildung φ mit

	e_1	e_2	e_3	e_4	e_5	e_6
φ	$\{1,2\}$	$\{2,3\}$	$\{1,3\}$	$\{3,4\}$	$\{3,4\}$	5

gegeben ist, lässt sich als



darstellen. ⬠

Beispiel 3.16 (Graphen in SageMath): Graphen sind selbstverständlich auch als mathematische Objekte in SageMath verfügbar. Unser Beispiel-Graph aus Beispiel 3.3 lässt sich etwa als

```
sage: G = Graph([
....:     [1, 2, 3, 4, 5],
....:     [(1, 2), (1, 3), (2, 3), (3, 4)]
....: ])
sage: G
Graph on 5 vertices
```

einlesen (wobei Sage hier auch ein Bild des Graphen zeichnet), wenn man eine geeignete Oberfläche wie ein Jupyter Notebook, und nicht unbedingt die Konsole verwendet. Viele Operationen und Algorithmen sind für die Graphen in SageMath schon ausimplementiert und stehen zur Verwendung bereit. Wir können etwa testen, ob G isomorph zu einem Kreis-Graphen auf 5 Knoten ist:

```
sage: G.is_isomorphic(graphs.CycleGraph(5))
False
```

Gerichtete Graphen sind (via `DiGraph`) ebenso unterstützt. Der gerichtete Graph aus Beispiel 3.13 wird etwa durch

```
sage: DiGraph([[1, 2, 3, 4, 5],
....:     [(2, 1), (1, 2), (3, 3), (4, 1), (5, 1), (5, 1)]],
....:     loops=True)
Looped digraph on 5 vertices
```

erzeugt. ⬠

3.2 Grad und Vollständigkeit

In diesem Abschnitt widmen wir uns einem der einfachsten Parameter eines Graphen: der Anzahl der Kanten, die jeweils an einem gegebenen Knoten anliegen.

Definition 3.17 (Knotengrad, Grad): Sei $G = (V, E)$ ein Graph und $v \in V$. Dann nennen wir...

1. $N(v)$ die *Menge der Nachbarn* von v, definiert durch $N(v) := \{u \in V : \{u, v\} \in E\}$.
2. $d(v)$ die Anzahl der zu v inzidenten Kanten, den *Grad* des Knotens v. Formal: $d(v) := |N(v)|$.
3. $\delta(G)$ den *minimalen Knotengrad* des Graphen G, also $\delta(G) := \min_{v \in V} d(v)$.
4. $\Delta(G)$ den *maximalen Knotengrad* des Graphen G, also $\Delta(G) := \max_{v \in V} d(v)$.

Ein Knoten $v \in V$ mit $d(v) = 1$ wird *Blatt* genannt, und im Fall von $d(v) = 0$ heißt der Knoten *isoliert*.

Beispiel 3.18 (Fortsetzung von Beispiel 3.3): Für unser Standardbeispiel finden wir etwa $N(5) = \emptyset$, also ist $d(5) = 0$; $N(3) = \{1, 2, 4\}$, also $d(3) = 3$; oder etwa $N(4) = \{3\}$, also $d(4) = 1$. Der Knoten 4 ist ein Blatt, Knoten 5 ist isoliert. Es ist $\delta(G) = 0$ (wegen Knoten 5), sowie $\Delta(G) = 3$ (wegen Knoten 3).⬠

Satz 3.19 (Handschlaglemma): Sei $G = (V, E)$ ein endlicher Graph. Dann gilt:

$$\sum_{v \in V} d(v) = 2|E|.$$

Beweis:

$$2|E| = \sum_{e \in E} 2 = \sum_{v \in V} \underbrace{\sum_{u \in N(v)} 1}_{d(v)} = \sum_{v \in V} d(v).$$

□

Korollar 3.20: Sei $G = (V, E)$ ein endlicher Graph. Dann ist die Anzahl der Knoten mit ungeradem Grad gerade.

Beweis: Dank Satz 3.19 wissen wir, dass die Summe aller Knotengrade gleich $2|E|$ und damit eine gerade Zahl ist. Ziehen wir hiervon die Summe der geraden Knotengrade ab, so bleibt einerseits nur mehr die Summe der ungeraden Knotengrade übrig – und da wir bislang nur gerade Zahlen abgezogen haben, muss diese Summe immer noch gerade sein.

Eine Summe ungerader Zahlen ist nur dann gerade, wenn die Anzahl der Summanden gerade ist. □

Beispiel 3.21: Wir können die beiden letzten Resultate an großen zufällig erzeugten Graphen verifizieren. Eine Strategie für die zufällige Erzeugung ist das sogenannte Erdős–Rényi[8]-Modell: für eine

gewünschte Graphordnung n und eine fixierte Wahrscheinlichkeit $p \in [0,1]$ beschreibt die Zufallsvariable $G(n,p)$ einen Graphen auf n Knoten, bei der für jede Kante unabhängig mit Wahrscheinlichkeit p entschieden wird, ob sie im Graphen vorkommt oder nicht.

```
sage: G = graphs.random.RandomGNP(n=1000, p=0.5)
sage: G.num_verts(), G.num_edges()  # random!
(1000, 248414)
sage: sum(G.degree(v) for v in G.vertices()) == 2*G.num_edges()
True
sage: len([v for v in G.vertices() if G.degree(v) % 2 == 1])  # result must be even
484
```

⬠

Definition 3.22 (Gradfolge): Sei $G = (V,E)$ ein endlicher Graph wobei $n \in \mathbb{N}$ und $V = \{v_1, ..., v_n\}$ mit $d(v_1) \geq d(v_2) \geq ... \geq d(v_n)$. Dann heißt das Tupel der Knotengrade $(d(v_1), ..., d(v_n))$ die *geordnete Gradfolge* von G.

Verzichtet man darauf, die Knoten entsprechend ihrem Grad absteigend zu ordnen, so heißt das Tupel einfach nur *Gradfolge*.

Beispiel 3.23 (Fortsetzung von Beispiel 3.3): Die geordnete Gradfolge von G aus unserem Standardbeispiel ist $(3,2,2,1,0)$. ⬠

Für einen gegebenen Graphen ist es relativ einfach, die zugehörige geordnete Gradfolge zu bestimmen. Das entsprechende *inverse Problem*, also die Frage, ob eine gegebene Gradfolge von einem Graphen realisiert werden kann ist weniger offensichtlich – wird aber vollständig im folgenden Satz beantwortet.

Satz 3.24 (Satz von Havel und Hakimi[9]): Sei $n \in \mathbb{N}$ und $(a_1, a_2, ..., a_n)$ ein Tupel von nicht-negativen ganzen Zahlen mit $a_1 \geq a_2 \geq ... \geq a_n$. Dann gibt es genau dann einen Graphen G, der diese Zahlenfolge als geordnete Gradfolge realisiert, wenn die folgenden beiden Bedingungen erfüllt sind:

1. $a_1 \leq n-1$,
2. es gibt einen Graphen H mit Gradfolge $\left(a_2 - 1, a_3 - 1, ..., a_{a_1+1} - 1, a_{a_1+2}, ..., a_n\right)$.

Beweis:

($\Leftarrow$) Zuerst „von rechts nach links“, nehmen wir also an dass die beiden Bedingungen aus dem Satz gelten. Fügen wir jetzt einen neuen Knoten zu H hinzu und verbinden diesen mit den ersten a_1 Knoten (sortiert nach dem Knotengrad), so entsteht ein Graph mit (sortierter) Gradfolge $(a_1, a_2, ..., a_n)$. ✓

[8] Nach *Paul Erdős* (1913 – 1996) und *Alfréd Rényi* (1921 – 1970), beide ungarische Mathematiker.

[9] Der Satz wurde unabhängig durch *Václav Jaromír Havel* (tschechischer Mathematiker, * 1972) in 1955 und durch *Seifollah Louis Hakimi* (iranisch-amerikanischer Mathematiker, 1932 – 2005) in 1962 bewiesen und publiziert.

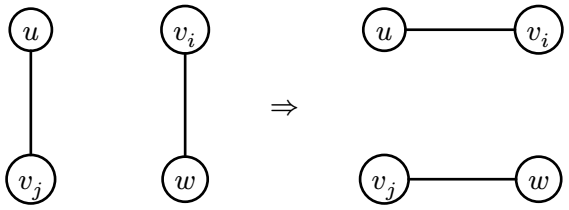
($\Rightarrow$) Angenommen, G sei ein Graph mit sortierter Gradfolge $(a_1, ..., a_n)$.

Die Bedingung $a_1 \leq n-1$ muss dann klarerweise erfüllt sein, da der zu a_1 gehörende Knoten höchstens zu $n-1$ anderen Knoten adjazent sein kann. Um das folgende Argument etwas lesbarer zu machen, bezeichnen wir $V(G) = \{v_1, ..., v_n\}$ mit $d(v_j) = a_j$ für alle $1 \leq j \leq n$, und weiters setzen wir $u := v_1$ und $k := d(v_1)$.

- Fall 1: Falls u bereits adjazent zu $v_2, v_3, ..., v_{k+1}$ ist, so löschen wir den Knoten u und seine inzidenten Kanten aus G. Der so konstruierte Teilgraph H hat die gewünschte Gradfolge

$$(a_2 - 1, a_3 - 1, ..., a_{k+1} - 1, a_{k+2}, ..., a_n).$$

- Fall 2: Es gibt einen Knoten v_i, $2 \leq i \leq k+1$, sodass u nicht adjazent zu v_i ist. Da u aber k adjazente Knoten hat, muss es ein $j > k+1$ geben, sodass u zu v_j adjazent ist. Wegen der Sortierung der Grade gilt damit $d(v_i) \geq d(v_j) \geq 1$, v_i muss also auch zu einem weiteren Knoten $w \neq v_j$ adjazent sein. Ersetzen wir in G jetzt die beiden Kanten uv_j und v_iw durch die Kanten uv_i und v_jw,



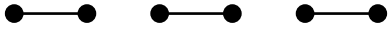
so erhalten wir einen neuen Graphen G' mit der gleichen Gradfolge wie G, in G' ist nach Konstruktion nun aber v_i adjazent zu u. Wiederhole diesen Kantentausch für jeden der Knoten v_i ($2 \leq i \leq k+1$) die noch nicht zu u adjazent sind – dann liegt Fall 1 vor und der gesuchte Teilgraph entsteht durch Entfernen des Knotens u. □

Satz 3.24 führt zu einem (rekursiven) Konstruktionsalgorithmus um zu einer gegebenen Gradfolge einen entsprechenden Graphen zu finden (sofern die Gradfolge realisiert werden kann).

Beispiel 3.25: Wir untersuchen, ob es einen Graphen mit sortierter Gradfolge $(5, 5, 4, 4, 3, 2, 2, 2, 1)$ gibt. Dazu wenden wir den Satz wiederholt an, bis wir entweder eine Verletzung der ersten Bedingung, oder alternativ eine Gradfolge finden für die es offensichtlich einen zugehörigen Graphen gibt:

$$\Big(5, \underbrace{5, 4, 4, 3, 2}, 2, 2, 1\Big) \to \Big(4, \underbrace{3, 3, 2, 2}, 2, 1, 1\Big) \to \Big(2, \underbrace{2, 2}, 1, 1, 1, 1\Big) \to (1, 1, 1, 1, 1, 1).$$

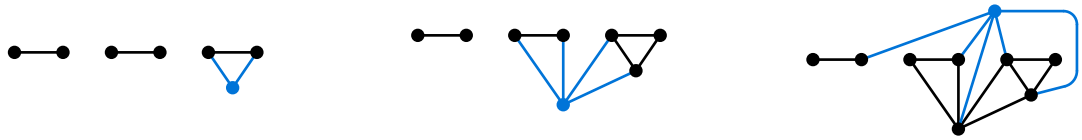
Wir könnten die Reduktion an dieser Stelle natürlich auch weiter fortsetzen, die nächste Folge würde etwa $(1, 1, 1, 1, 0)$ lauten – praktisch ist das aber nicht notwendig, da wir direkt einen Graphen mit sechs Knoten mit jeweils Grad 1 angeben können:



Wenn wir jetzt die Reduktion der Knotengradfolgen rückwärts lesen, so sehen wir, dass wir

- zuerst einen Knoten einführen müssen, der mit zwei Knoten vom Grad jeweils 1 verbunden ist,
- dann einen Knoten hinzufügen müssen der mit zwei Knoten vom Grad 2, und zwei Knoten vom Grad 1 verbunden ist,

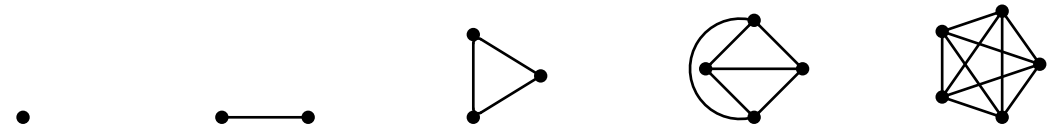
- und schließlich noch einen dritten Knoten hinzufügen müssen der mit einem Knoten vom Grad 4, zwei Knoten vom Grad 3, einem Knoten vom Grad 2, und einem Knoten vom Grad 1 verbunden ist.



Der so erhaltene Graph hat nun die gesuchte sortierte Gradfolge von $(5, 5, 4, 4, 3, 2, 2, 2, 1)$. ⬠

Definition 3.26 (Reguläre und vollständige Graphen): Sei $G = (V, E)$ ein Graph. Wenn es ein $k \geq 0$ gibt, sodass $d(v) = k$ für alle $v \in V$ ist, so nennt man G einen k-regulären Graphen (i.e., ein Graph in dem alle Knoten Grad k haben.)

Ein $(n-1)$-regulärer Graph der Ordnung n heißt *vollständiger Graph* und wird mit K_n bezeichnet.



K_1 K_2 K_3 K_4 K_5

Abbildung 8: Vollständige Graphen der Ordnung 1 bis 5.

3.3 Wanderungen in Wäldern

In diesem Abschnitt beschäftigen wir uns mit mit dem „Abgehen“ von Graphen, der „Erreichbarkeit“ von Knoten, sowie mit speziellen Graphen die in dem Zusammenhang besondere Eigenschaften haben.

Definition 3.27 (Wanderung, Weg, Kreis): Sei $G = (V, E)$ ein (möglicherweise gerichteter) Graph.

- Eine *Wanderung (walk)* in G ist eine alternierende Folge inzidenter Knoten und Kanten der Gestalt

$$x_0, x_0x_1, x_1, x_1x_2, ..., x_{n-1}x_n, x_n$$

  mit $x_j \in V$ und $x_jx_{j+1} \in E$. Der Knoten x_0 heißt *Startknoten*, x_n heißt *Endknoten*, und n (die Anzahl der Kanten) heißt die *Länge der Wanderung*.
- Eine Wanderung heißt *Weg (path)*, wenn die Knoten $x_0, x_1, ..., x_n$ paarweise verschieden sind.
- Eine Wanderung heißt *geschlossene Wanderung (circuit)*, falls $x_0 = x_n$.
- Eine geschlossene Wanderung heißt *Kreis*, falls die Knoten $x_0, ..., x_{n-1}$ paarweise verschieden sind.

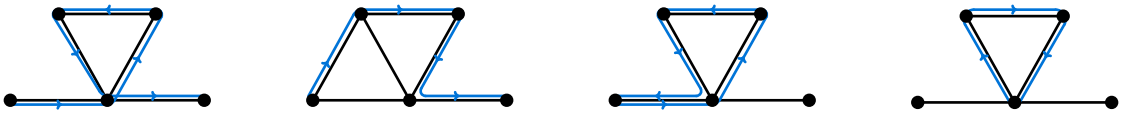


Abbildung 9: Von links nach rechts: eine Wanderung, ein Weg, eine geschlossene Wanderung, und ein Kreis.

Anmerkung 3.28: Gelegentlich ist es nützlich, Wege und Kreise wieder als Teilgraphen zu sehen. In diesem Fall identifizieren wir die Wanderung

$$x_0, x_0x_1, x_1, x_1x_2, ..., x_{n-1}x_n, x_n$$

mit dem Graphen

$$W = (\{x_0, x_1, ..., x_n\}, \{x_0x_1, x_1x_2, ..., x_{n-1}x_n\}).$$

Definition 3.29 (Abstand): Sei $G = (V, E)$ ein (eventuell gerichteter) Graph. Für $x, y \in V$ definieren wir

$$d(x, y) := \begin{cases} \text{Länge einer kürzesten Wanderung von } x \text{ nach } y, \\ \infty, \text{ falls es keine Wanderung von } x \text{ nach } y \text{ gibt.} \end{cases}$$

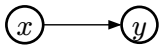
als den Abstand von x zu y in G. Auch Wanderungen der Länge 0 sind zugelassen: $d(x, x) = 0$.

Proposition 3.30: Sei G ein (ungerichteter) Graph. Dann wird durch die Abstandsfunktion d eine Metrik[10] auf $V(G)$ definiert.

Beweis: Damit eine Funktion $d : V(G) \times V(G) \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ eine Metrik ist, müssen für alle $x, y, z \in V(G)$ die Bedingungen

- *(Symmetrie)* $d(x, y) = d(y, x)$,
- *(positive Definitheit)* $d(x, y) \geq 0$ und $d(x, y) = 0 \Leftrightarrow x = y$,
- *(Dreiecksungleichung)* $d(x, y) + d(y, z) \geq d(x, z)$

erfüllt sind. Alle drei lassen sich leicht als Übungsaufgabe überprüfen. □

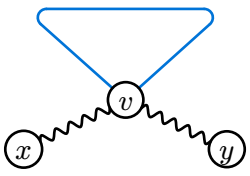
Beachte: in einem gerichteten Graphen muss Proposition 3.30 nicht notwendigerweise gelten, da im Allgemienen die Symmetrie $d(x, y) = d(y, x)$ nicht erfüllt sein muss: Im einfachen gerichteten Graphen 

ist etwa $d(x, y) = 1$, aber $d(y, x) = \infty$.

Proposition 3.31: Sei G ein (eventuell gerichteter) Graph, und seien $x, y \in V(G)$ mit $x \neq y$. Dann ist jede Wanderung der Länge $d(x, y)$ von x nach y ein Weg.

Beweis:

Indirekt: angenommen, es gäbe eine Wanderung der Länge $d(x, y)$ von x nach y, die kein Weg ist – also einen Knoten v mindestens doppelt besucht. Dann könnten wir den Teil der Wanderung zwischen dem ersten und letzten Besuch von v aber einfach entfernen.



So würde eine kürzere Wanderung von x nach y entstehen – ein Widerspruch zur Definition von $d(x, y)$. ↯ □

[10] Streng genommen muss die übliche Definition einer Metrik dafür leicht erweitert werden, damit ein Abstand von ∞ erlaubt ist – das ist aber auf sehr natürliche Art und Weise möglich.

Definition 3.32 (Zusammenhang): Ein Graph $G = (V, E)$ heißt *zusammenhängend*, wenn $d(x, y) < \infty$ für alle $x, y \in V$ ist.

Die Relation $\sim_G$, die durch $x \sim_G y :\Leftrightarrow d(x, y) < \infty$ definiert ist, ist eine Äquivalenzrelation auf $V(G)$ deren Äquivalenzklassen die *Zusammenhangskomponenten* von G genannt werden. Die Anzahl der verschiedenen Zusammenhangskomponenten wird die *Zusammenhangszahl* von G genannt.

Gibt es keine Knoten mit $d(x, y) = \infty$, so gibt es notwendigerweise auch nur eine Zusammenhangskomponente – der Graph ist also zusammenhängend. Es gilt die Äquivalenz

$$\begin{aligned} G \text{ ist zusammenhängend} &\Leftrightarrow G \text{ hat nur eine Zusammenhangskomponente} \\ &\Leftrightarrow G \text{ hat Zusammenhangszahl } 1. \end{aligned}$$

Der von einer Zusammenhangskomponente induzierte Teilgraph ist – nach Konstruktion – immer zusammenhängend.

Definition 3.33 (starker/schwacher Zusammenhang): Ein gerichteter Graph $D = (V, A)$ heißt *stark zusammenhängend*, wenn für alle Knoten $x, y \in V$ der Abstand $d(x, y) < \infty$ ist, es also einen gerichteten Weg von x nach y gibt.

Die Äquivalenzklassen der Relation $\sim_D$ mit $x \sim_D y :\Leftrightarrow d(x, y) < \infty \wedge d(y, x) < \infty$ heißen die *starken Zusammenhangskomponenten* von D, und deren Anzahl die *starke Zusammenhangszahl*.

Betrachtet man zu D den zugrundeliegenden ungerichteten Graphen G, so heißt D *schwach zusammenhängend*, wenn G zusammenhängend ist.

Beispiel 3.34: In der Abbildungen unten sind zwei Graphen dargestellt, links ein ungerichteter und rechts ein gerichteter Graph.

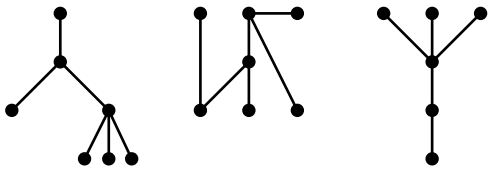
Der ungerichtete Graph besitzt (relativ offensichtlich) zwei Zusammenhangskomponenten, die entsprechenden Knoten sind jeweils in der gleichen Farbe gefärbt.

Es braucht etwas genaueres Hinschauen um zu erkennen, dass der gerichtete Graph auf der rechten Seite vier starke Zusammenhangskomponenten besitzt, auch hier sind die entsprechenden Knoten jeweils gleich gefärbt. Gleichzeitig ist der gerichtete Graph schwach zuasmmenhängend. ⬠

Definition 3.35: Sei $G = (V, E)$ ein Graph. Falls G keine Kreise enthält (also *azyklisch* ist), so wird G ein *Wald* genannt. Ein zusammenhängender Wald ist ein *Baum*.

Beispiel 3.36:

Im Beispiel rechts ist ein Graph mit drei Zusammenhangskomponenten dargestellt, der keine Kreise besitzt. Mit anderen Worten: ein aus drei Bäumen bestehender Wald.



⬠

Satz 3.37 (Charakterisierung von Bäumen): Sei $G = (V, E)$ ein Graph. Dann sind die folgenden Aussagen äquivalent:

(a) G ist ein Baum.

(b) Zwischen je zwei Knoten $x, y \in V(G)$ gibt es *genau einen Weg*.

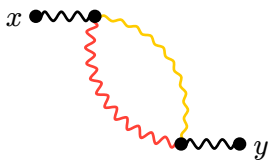
(c) G ist *minimal zusammenhängend*: wird eine beliebige Kante aus G entfernt, so ist G nicht mehr zusammenhängend.

(d) G ist *maximal kreisfrei*: wird eine beliebige Kante zu G hinzugefügt, so entsteht dabei ein Kreis.

Beweis:

(a) ⇒ (b) Sei G ein Baum. Angenommen, es gäbe zwei verschiedene Wege von x nach y.

Die beiden Wege starten jeweils in x und enden in y. Dazwischen muss es einen Knoten geben, nach dem sich die Wege trennen, sowie darauffolgend einen Knoten in dem sie wieder zusammenlaufen. Fügen wir diese Teile zusammen, so entsteht ein Kreis – ein Widerspruch zur Annahme, dass G ein Baum ist. ↯



(b) ⇒ (c) Angenommen, zwischen je zwei Knoten $x, y \in E(G)$ gibt es genau einen Weg. Wähle eine beliebige Kante $xy \in E(G)$. Nach der Annahme ist die Kante der eindeutige Weg von x nach y in G – wird sie entfernt, gibt es also keinen Weg zwischen den beiden Knoten mehr; $G - xy$ ist also nicht zusammenhängend. Da die Kante xy beliebig gewählt war, ist G minimal zusammenhängend.

(c) ⇒ (a) Angenommen, G ist minimal zusammenhängend. Wir wollen zeigen, dass G ein Baum ist, müssen also nachweisen dass G zusammenhängend und kreisfrei ist. Erstere Eigenschaft ist klarerweise erfüllt. Nehmen wir nun an, dass es in G einen Kreis gibt. Dann könnten wir aber jede beliebige Kante aus dem Kreis entfernen ohne den Zusammenhang von G zu zerstören – ein Widerspruch zur Annahme. ↯

(a, b, c) ⇔ (d) Übung, Privatvergnügen. □

Satz 3.38: Angenommen, $G = (V, E)$ ist ein Baum. Dann gilt: $|E| = |V| - 1$.

Wir können die Aussage etwa an den Bäumen im Wald aus Beispiel 3.36 überprüfen. Die Bäume dort haben (von links nach rechts betrachtet) 7 Knoten und 6 Kanten, nochmals 7 Knoten und 6 Kanten, sowie 5 Knoten und 4 Kanten.

Beweis: Wir beweisen die Aussage durch Induktion über die Anzahl der Knoten $n = |V|$.

- Für $n = 1$ gibt es lediglich einen „trivialen“ Baum: einen einzelnen Knoten ohne Kanten; also $|E| = 0$, die Aussage des Satzes stimmt.
- (Starke) Induktionsannahme: Angenommen, $n^* \in \mathbb{N}$ sei beliebig aber fest, und jeder Baum der Ordnung n für $n < n^*$ habe $n - 1$ viele Kanten.
- Sei G nun ein beliebiger Baum der Ordnung n^*. Wähle eine beliebige Kante $e \in E(G)$ und betrachte den Graphen $G - e$. Die beiden Endpunkte von e müssen in $G - e$ in verschiedenen Zusammenhangskomponenten liegen, nenne diese G_1 und G_2. Es kann keine weiteren Zusammenhangskomponenten geben. Da G ein Baum (und damit kreisfrei) ist, müssen auch G_1 und G_2 kreisfrei, und damit Bäume sein. Insbesondere muss $|V(G_1)| < n^*$ und $|V(G_2)| < n^*$ sein, womit jeweils unsere Induktionsannahme greift. Damit:

$$\begin{aligned} |E(G)| &= 1 + |E(G_1)| + |E(G_2)| = 1 + |V(G_1)| - 1 + |V(G_2)| - 1 \\ &= \underbrace{|V(G_1)| + |V(G_2)|}_{|V(G)|} - 1 = |V(G)| - 1, \end{aligned}$$

  womit der Induktionsschritt abgeschlossen ist. □

Bäume haben also immer genau eine Kante weniger als Knoten. Dass diese Eigenschaft aber nicht als Charakterisierung von Bäumen verwendet werden kann, überlegen wir uns im folgenden Beispiel.

Beispiel 3.39:

Wir beobachten: die Folgerung aus Satz 3.38 ist für den Graphen rechts erfüllt, er besteht aus fünf Knoten und vier Kanten. Trotzdem ist der Graph aber offensichtlich kein Baum.

⬠

Proposition 3.40: Sei $G = (V, E)$ ein Baum der Ordnung $|V| \geq 2$. Dann gilt: G hat mindestens 2 Blätter.

Beweis: Angenommen, G ist ein Baum mit keinem oder nur einem Blatt; sei $V = \{v_1, ..., v_n\}$ mit $d(v_1) \geq 1$ das potentielle Blatt und $d(v_j) \geq 2$ für $j \geq 2$. Dann haben wir einerseits

$$\sum_{j=1}^{n} d(v_j) = \underbrace{d(v_1)}_{\geq 1} + \sum_{j=2}^{n} \underbrace{d(v_j)}_{\geq 2} \geq 1 + (n-1) \cdot 2 = 2n - 1,$$

und andererseits, dank dem Handschlaglemma (Satz 3.19) und Satz 3.38,

$$\sum_{j=1}^{n} d(v_j) = 2|E(G)| = 2(n-1) = 2n - 2.$$

Die so entstehende Ungleichungskette erzeugt damit $2n - 2 \geq 2n - 1$, ein Widerspruch. ↯ □

Definition 3.41: Sei $G = (V, E)$ ein Graph. Ein aufspannender Teilgraph T von G, der zugleich ein Baum ist, heißt *Spannbaum*.

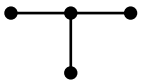
Eine klassische Frage im Zusammenhang mit Spannbäumen ist die Bestimmung der Anzahl der Spannbäume eines Graphen. Der folgende Satz beantwortet die Frage für K_n, den vollständigen Graphen auf n Knoten – wir wollen hier aber auch anmerken, dass die Frage auch für allgemeine Graphen mit Mitteln der Linearen Algebra („*Matrix-Baum-Satz*“) beantwortet werden kann.

Satz 3.42 (Satz von Cayley): Für $n \in \mathbb{N}$ hat der vollständige Graph K_n genau $T_n := n^{n-2}$ viele verschiedene Spannbäume.

Da alle in einem gelabelten Graphen möglichen Kanten in K_n enthalten sind, ist die Menge der Spannbäume von K_n zugleich die Menge *aller* gelabelten Bäume der Ordnung n – wovon es damit also n^{n-2} viele gibt.

Beispiel 3.43: Wir untersuchen die Anzahl der Spannbäume für K_n für $1 \leq n \leq 4$.

- Für $n = 1$ gibt es nur den trivialen Graphen ohne Kanten, der zugleich sein eigener Spannbaum ist: $n^{n-2} = 1^{1-2} = 1^{-1} = 1$. ✓
- Für $n = 2$ gibt es nur einen zusammenhängenden Graphen ( ), bei dem es keine Rolle spielt wie die Knoten mit 1 und 2 beschriftet werden. Das passt zu $n^{n-2} = 2^0 = 1$. ✓
- Der K_3, ein Dreieck, besitzt nur einen Typ von Spannbaum, nämlich . Ein Labeling dieses Baums ist eindeutig durch die Wahl des mittleren Knotens gegeben (alternativ: durch Enternen einer der Kanten des Dreiecks); dafür gibt es 3 Möglichkeiten – und zugleich ist $n^{n-2} = 3^1 = 3$. ✓
- Der K_4 hat zwei nicht-isomorphe Spannbäume, einen Pfad der Länge 4, und einen „Stern“:

Es gibt 12 verschiedene Beschriftungen des Pfades: von den $4! = 24$ Permutation von $[4]$ gehört je eine Permutation und ihre Umkehrung (die von hinten nach vorne gelesene Permutation) zum gleichen Baum (da der Baum sich beim „Umdrehen“ auch nicht verändert).

Ein Labeling des Sterns ist vollständig durch die Wahl des mittleren Knotens gegeben, hier gibt es also 4 verschiedene Versionen. Insgesamt gibt es also $12 + 4 = 16$ Spannbäume – und zugleich ist $n^{n-2} = 4^2 = 16$. ✓ ⬠

Beweis von Satz 3.42 (durch doppeltes Abzählen, nach Jim Pitman): Sei T_n die Anzahl der verschiedenen gelabelten Bäume der Ordnung n. Um eine explizite Formel für T_n zu finden, zählen wir die Anzahl der Konstruktionsmöglichkeiten einen *Wurzelbaum* mit n Knoten zu bauen.

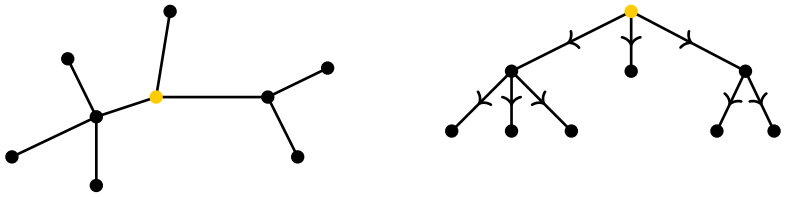


Abbildung 10: Baum zu Wurzelbaum, und die zugehörige Orientierung der Kanten.

Ein Wurzelbaum entsteht, wenn wir in einem Baum der Ordnung n einen der Knoten als *Wurzel* deklarieren. Diese Wahl induziert zugleich eine Orientierung der Kanten; wir betrachten jede Kante als „von der Wurzel weg führend"; ein Beispiel ist in Abbildung 10 dargestellt.

Zählen wir nun die Anzahl der Konstruktionsmöglichkeiten (also die Anzahl der verschiedenen Wege, ausgehend von einem „leeren" Graphen der Ordnung n fortlaufend Kanten hinzuzufügen bis ein Wurzelbaum entsteht; ein gegebener Baum kann insbesondere auf mehrere Arten konstruiert werden).

Variante 1. Wählen wir zunächst einen der T_n möglichen Bäume und wählen eine Wurzel aus (dafür gibt es n Möglichkeiten), der so entstehende Wurzelbaum ist unsere „Blaupause". Fügen wir in einen leeren Graphen der Ordnung n der Reihe nach die $n-1$ Kanten aus dem Vorlagen-Baum ein (dafür gibt es $(n-1)!$ viele Möglichkeiten), so führt das jeweils zu einer möglichen Wurzelbaumkonstruktion. Insgesamt gibt es damit also $T_n \cdot n \cdot (n-1)! = T_n \cdot n!$ viele.

Variante 2. Beginnen wir diesmal mit einem Wald auf n Knoten und keinen Kanten. Wieder fügen wir der Reihe nach (gerichtete) Kanten ein, diesmal aber nicht auf Basis einer bestehenden Vorlage. Stattdessen wählen wir in jedem Schritt:

- einen beliebigen Knoten (jeweils n Möglichkeiten)
- und einen der Bäume des Waldes, die den zuvor gewählten Knoten noch nicht enthalten.

Für die Auswahl des Baumes gibt es in der ersten Runde noch $n-1$ Möglichkeiten; mit jeder neuen Kante wachsen aber zwei Bäume zusammen und die Anzahl verringert sich um 1 (in Runde 2 gibt es also $n-2$ Möglichkeiten, in Runde 3 $n-3$, und so weiter).

Füge dann eine neue gerichtete Kante vom gewählten Knoten zur Wurzel (dem Knoten ohne Vorgänger) des gewählten Baumes ein. Dann wiederhole den Prozess, bis alle $n-1$ Kanten eingefügt sind. Für die erste Runde gibt es $n \cdot (n-1)$ Auswahlmöglichkeiten, für die zweite Runde $n \cdot (n-2)$ viele, und so weiter – bis zur $(n-1)$-sten Runde; die letzte Kante kann auf $n \cdot 1$ viele Arten gezogen werden. Insgesamt ergibt das

$$n \cdot (n-1) \cdot n \cdot (n-2) \cdots n \cdot 1 = n^{n-1} \cdot (n-1)!$$

viele Konstruktionsmöglichkeiten.

Ein Vergleich der beiden Abzählstrategien hat zur Folge, dass

$$T_n \cdot n! = n^{n-1} \cdot (n-1)! \quad \Longleftrightarrow \quad T_n = \frac{n^{n-1} \cdot (n-1)!}{n!} = n^{n-2},$$

was den Satz von Cayley damit beweist. □

3.4 Eulerkreise und das „Haus vom Ni-ko-laus“

In diesem Abschnitt wenden wir uns jenem Problem zu, das gewissermaßen als das Geburtsproblem der modernen Graphentheorie gilt. Wir machen dazu eine Reise in die Provinz (und Stadt) Калининград („Kaliningrad“) in der russischen Enklave zwischen Polen und Litauen. In der Vergangenheit (insbesondere im 18. Jahrhundert) war diese Teil von Ostpreußen – und unter einem anderen Namen, *Königsberg*, bekannt.

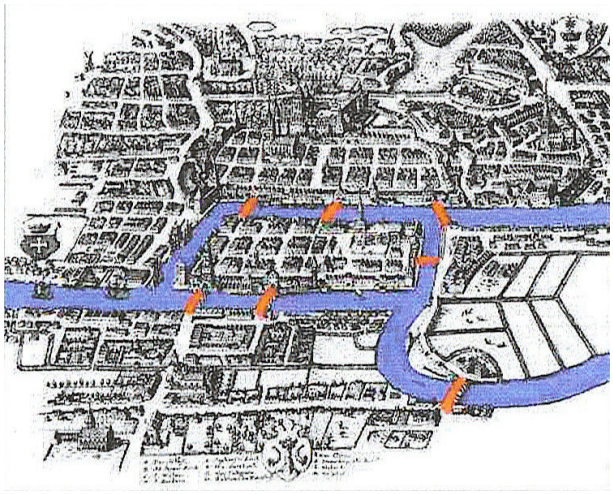


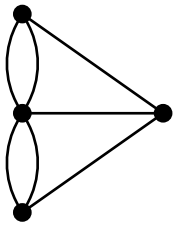
Abbildung 11: Königsberg im 18. Jahrhundert. Sicht auf die Insel Kneiphof, umflossen vom Pregel.

Beispiel 3.44 (Königsberger Brückenproblem): Vom deutschen Politiker und Astronom *Karl Leonhard Gottlieb Ehler* wurde der berühmte Schweizer Mathematiker *Leonhard Euler* (1707 – 1783) um 1736 in einem Brief auf das sogenannte *Königsberger Brückenproblem* aufmerksam gemacht. Konkret lautet die Fragestellung:

> Gibt es einen Weg durch Königsberg, entlang dessen jede der sieben Brücken genau einmal überquert wird? Und falls ja, ist das auch entlang eines Rundwegs (also mit gleichem Start- und Endpunkt) möglich?

Königsberg und die relevanten sieben Brücken sind in Abbildung 11 dargestellt.

Wir können das Problem mittels eines (Multi-)Graphen modellieren: jeder der vier durch den Fluss getrennten Stadtteile wird durch einen Knoten repräsentiert, die Brücken jeweils durch eine Kante.



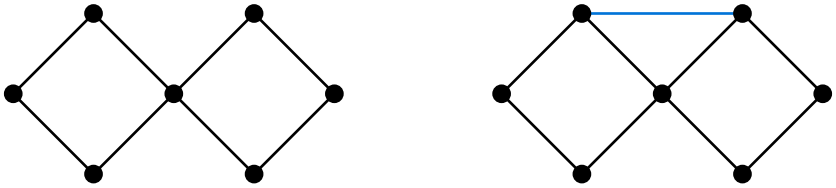
Euler hat bewiesen, dass es im alten Königsberg *keinen solchen Spaziergang* geben kann, bei dem jede Brücke genau einmal verwendet wird. Sein Argument: an jedem der vier Stadtteile grenzen eine ungerade Anzahl von Brücken an (im Zusammenhang mit dem Graphen: alle Knotengrade sind gerade).

Wenn es eine Rundwanderung geben würde, so müssten wir entlang dieser jeden Stadtteil gleich oft betreten wie verlassen. Das funktioniert aber nicht, wenn die Anzahl der Brücken an einem Stadtteil ungerade ist. ⬠

Definition 3.45 (Eulerweg und -kreis): Sei G ein (Multi-)Graph.

1. Eine Wanderung, die jede Kante in G genau einmal verwendet, heißt *Eulerweg*.
2. Ein geschlossener Eulerweg ist ein *Eulerkreis*.
3. Graphen, in denen es einen Eulerkreis gibt, heißen *euler'sche Graphen*.

Beispiel 3.46: Der *Königsberger Brückengraph* aus Beispiel 3.44 ist *kein* euler'scher Graph.



Im linken dieser beiden Graphen finden wir einen Eulerkreis (indem wir einfach den Umfang des Graphen ablaufen), dieser ist also ein euler'scher Graph.

Im rechten Graphen mit der zusätzlichen blauen Kante ist es hingegen nach dem selben Argument wie in Beispiel 3.44 und den ungeraden Knotengraden der oberen beiden Knoten nicht möglich, einen Eulerkreis zu finden – der Graph ist nicht euler'sch. Es ist allerdings schon möglich, einen Eulerweg zu finden, der in den Endpunkten der blauen Kante beginnt und endet. ⬠

Das Argument aus Beispiel 3.44 liefert ein einfaches Kriterium, mit dem wir entscheiden können, ob ein Graph euler'sch ist oder nicht; wir müssen lediglich die Parität der Knotengrade untersuchen. Tatsächlich hat Euler aber noch mehr gezeigt: wir können euler'sche Graphen vollständig mittels der Knotengradparität charakterisieren.

Satz 3.47 (Charakterisierung von euler'schen Graphen): Sei G ein zusammenhängender (Multi-)Graph. Dann ist G genau dann ein euler'scher Graph, wenn alle Knoten in G geraden Grad haben.

Beweis:

„⇒" Um diese Richtung haben wir uns im wesentlichen bereits in Beispiel 3.44 gekümmert: angenommen, G wäre euler'sch. Entlang des damit existierenden Eulerkreises betreten wir jeden Knoten ebenso oft wie wir ihn verlassen; es kann damit also keine ungeraden Knotengrade geben. ✓

„⇐" Sei G nun ein zusammenhängender (Multi-)Graph, für den alle Knotengrade gerade sind. Betrachte eine längstmögliche Wanderung W, bei der jede Kante von G höchstens einmal verwendet wird. (Das dürfen wir machen: da es höchstens endlich viele Kanten gibt, gibt es nur endlich viele Möglichkeiten für solche Wanderungen – mindestens eine da-

von muss längstmöglich sein; jede endliche Menge hat ein Maximum.) Sei konkret $W = (x_0, x_0x_1, x_1, x_1x_2, ..., x_{n-1}x_n, x_n)$. Da W längstmöglich ist, muss jede Kante die zu x_0 oder x_n inzident ist bereits Teil von W sein (andernfalls könnten wir W einfach verlängern). Da die Knotengrade, und insbesondere jene von x_0 und x_n gerade sind, müssen wir die beiden Knoten entlang von W auch jeweils ebenso oft betreten wie verlassen haben.

Da wir in x_0 starten (und den Knoten daher ein einzelnes Mal zusätzlich verlassen) und in x_n enden (und den Knoten so ein einzelnes Mal zusätzlich betreten) ist die Situation mit den geraden Knotengraden und keinen freien inzidenten Kanten nur möglich, wenn $x_0 = x_n$ ist: W muss also eine geschlossene Wanderung sein.

Nehmen wir nun an, es gäbe eine Kante $e \in E(G)$, die noch nicht in W enthalten ist. Da G zusammenhängend ist, muss es nun aber eine Wanderung von einem beliebigen Knoten auf W zur Kante e geben. Diese Wanderung mag ein Stück entlang von W verlaufen, irgendwann muss sie aber eine erste Kante f durchlaufen, die adjazent zu Kanten in W, aber nicht selbst Teil von W ist. Die Kante f kann nun aber genutzt werden, um aus W eine noch längere Wanderung zu konstruieren (drehe den Start- und Endpunkt von W auf einen der Endpunkte von f, dann verlängere das Ende von W um f) – ein Widerspruch zur Annahme, dass W längstmöglich war. Es kann daher keine Kante in G geben, die noch nicht Teil von W ist: wir haben einen Eulerkreis gefunden. ✓ □

Korollar 3.48: Sei G ein zusammenhängender (Multi-)Graph. Dann gibt es genau dann einen Eulerweg in G, wenn es in G höchstens zwei Knoten mit ungeradem Grad gibt.

Beweis: Wenn es keine Knoten mit ungeradem Grad gibt, dann ist G euler'sch. Der damit existierende Eulerkreis ist zugleich ein Eulerweg.

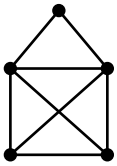
Aufgrund der Folgerung aus dem Handschlaglemma (Korollar 3.20) muss die Anzahl der Knoten mit ungeradem Grad eine gerade Zahl sein, es bleibt also nur mehr der Fall von genau zwei Knoten mit ungeradem Grad.

In diesem Fall können wir die beiden Knoten durch eine Hilfskante verbinden, im so entstehenden Graphen sind alle Knotengrade gerade. Nach Satz 3.47 gibt es darin einen Eulerkreis, der die Hilfskante enthält. Entfernen wir die Kante wieder, zerfällt der Kreis in eine Wanderung, die jede Kante des ursprünglichen Graphen genau einmal verwendet – ein Eulerweg. Die Endpunkte des Eulerweges sind genau die beiden Knoten mit ungeradem Grad. □

In Form von Korollar 3.48 haben wir ein einfaches Kriterium um zu entscheiden, welche Graphen wir zeichnen können, ohne den Stift abzusetzen.

Beispiel 3.49 (Das-ist-das-Haus-vom-Ni-ko-laus):

Das Bild eines Hauses, das zum Vers „Das-ist-das-Haus-vom-Ni-ko-laus“ ohne mit dem Stift abzusetzen gezeichnet werden soll, stellt *keinen* euler'schen Graphen dar: die beiden Knoten unten haben ungeraden Grad, nach Satz 3.47 gibt es daher keinen Eulerkreis. Da es aber nur genau zwei Knoten mit ungeradem Grad gibt, gibt es einen Eulerweg, der in den beiden unteren Knoten beginnt bzw. endet. Das „Haus vom Nikolaus“ *kann* in der Tat nur gezeichnet werden, wenn in einem der beiden unten Knoten begonnen wird. ⬠



Es gibt verschiedene effiziente Algorithmen zur Konstruktion von

in euler'schen Graphen, zum Beispiel der Algorithmus von *Hierholzer*. Dessen Idee besteht im wesentlichen darin, (kleinere) Kreise der Reihe nach abzugehen und zusammenzuhängen.

Beispiel 3.50 (Anwendung: Das Postbotenproblem): Praktisch taucht das Problem der Konstruktion von Eulerkreisen in der Logistik, etwa beim Planen von Briefträgerrouten auf. Das Straßennetz des zu beliefernden Gebietes wird dabei als Graph modelliert; Kreuzungen entsprechen Knoten und Straßen den Kanten.

Wäre der so modellierte Stadtplan ein euler'scher Graph, so wäre ein Eulerkreis die optimale Tour. In der Praxis ist das aber selten der Fall, in diesem Fall entsteht ein Optimierungsproblem: wir betrachten alle Knoten mit ungeraden Grad (davon gibt es eine gerade Anzahl) und führen gewichtete Hilfskanten paarweise zwischen diesen ein. Das Gewicht entspricht dabei der Länge der kürzesten Verbindung zwischen den beiden Knoten.

Im so entstehenden Hilfsgraphen (ein $K_{2\ell}$) suchen wir ein sogenanntes *Matching* – eine Menge von Kanten, die jeden Knoten genau einmal berühren – mit minimalem Gewicht. Sobald die Kanten aus dem Matching zum ursprünglichen Graphen hinzugefügt werden, ist dieser euler'sch, und ein Eulerkreis darin beschreibt die optimale Zustellungstour. ⬠

3.5 Graph-Rundreisen: Hamiltonkreise

Nach der überraschend einfachen Lösung zum Problem, zu entscheiden wann ein Graph einen Kreis besitzt, der jede Kante genau einmal enthält, untersuchen wir hier eine verwandte Frage: Gibt es ein Kriterium, mit dem wir entscheiden können ob ein Graph eine *Knoten-Rundreise* besitzt?

Definition 3.51 (Hamiltonkreis): Sei G ein Graph. Ein Kreis in G, der alle Knoten genau einmal besucht, heißt *Hamiltonkreis*[11]. Gibt es einen Hamiltonkreis in G, so heißt G ein hamilton'scher Graph.

Anmerkung 3.52: Die Frage „Ist ein Graph euler'sch?“ ist leicht und vollständig durch die Parität der Knotengrade (Satz 3.47) zu beantworten. Unglücklicherweise gibt es für Hamiltonkreise kein so einfaches Kriterium – damit aber nicht genug; man kann zeigen, dass die Frage „Ist ein Graph hamilton'sch?“ *sehr* viel schwerer („NP-vollständig“) ist. Das bedeutet, dass es vermutlich[12] keinen effizienten Algorithmus gibt, der für jeden Graphen entscheiden kann, ob er einen Hamiltonkreis besitzt.

[11] Nach Sir William Hamilton (1805 – 1865), irischer Mathematiker. Schöpfer des „Icosian Game“, einem Brettspiel für zwei Spieler das auf dem Problem basiert, einen Hamiltonkreis auf dem Gitternetz eines Dodekaeders zu finden.

[12] Abhängig von der Antwort des (ungelösten) P = NP-Problems.

Als „Trostpreis“ liefert der folgende Satz eine hinreichende Bedingung (unter einer allerdings relativ starken Voraussetzung).

Satz 3.53 (Satz von Dirac): Sei G ein Graph der Ordnung n. Gilt $\delta(G) \geq \frac{n}{2}$, so ist G ein hamilton'scher Graph.

Beweis: Der Beweis erfolgt in drei Schritten. Sei G also ein Graph mit n Knoten sodass jeder Knoten mindestens $\frac{n}{2}$ Nachbarn hat.

Schritt 1. G ist zusammenhängend. Sei dazu $C \subseteq V(G)$ die kleinste Zusammenhangskomponente von G. Da C nicht leer ist, gibt es einen Knoten $v \in C$. Laut Voraussetzung hat v mindestens $\frac{n}{2}$ viele Nachbarn, also muss $|C| \geq 1 + \frac{n}{2}$ sein. Wenn die kleinste Zusammenhangskomponente bereits mehr als die Hälfte der Knoten von G enthält, so muss $C = V(G)$ – und G damit zusammenhängend sein.

Schritt 2. Ein längster Weg in G kann zu einem Kreis umgebaut werden.

Sei $W = (x_0, x_0x_1, x_1, x_1x_2, \ldots, x_k)$ ein längster Weg (also ohne Mehrfachbesuch von Knoten) in G. Nun muss einerseits $N(x_k) \subseteq \{x_0, \ldots, x_{k-1}\}$ sein (sonst könnte der Weg verlängert werden), und andererseits wissen wir, dass nach Voraussetzung $|N(x_k)| \geq \frac{n}{2}$ gilt.

Betrachten wir jetzt die Menge

$$M = \big\{x \in V(G) \mid x = x_j \text{ für ein } 0 \leq j < k \text{ und } x_0x_{j+1} \in E(G)\big\},$$

in der genau jene Knoten enthalten sind, deren Nachfolger entlang W zugleich Nachbarn von x_0 sind. Nach Konstruktion ist $M \subseteq \{x_0, \ldots, x_{k-1}\}$, und zugleich gilt $|M| \geq \frac{n}{2}$ (alle Nachbarn von x_0 müssen aus dem selben Grund wie für x_k auf W liegen; der Weg könnte sonst verlängert werden).

Wir wissen: $M, N(x_k) \subseteq V(G) \setminus \{x_k\}$, in dieser Menge sind $n - 1$ viele Knoten enthalten. Da $|M| + |N(x_k)| \geq n$, muss $M \cap N(x_k) \neq \emptyset$ sein. Wähle $x_j \in M \cap N(x_k)$. Die Situation ist nun in Abbildung 12 dargestellt.

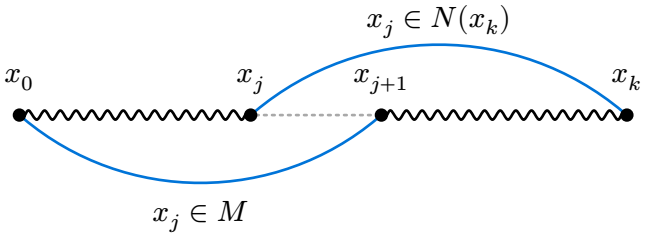


Abbildung 12: Satz von Dirac: Längster Weg zu Kreis.

Es ergibt sich ein Kreis $x_0 \rightsquigarrow x_j \to x_k \rightsquigarrow x_{j+1} \to x_0$; wir haben gezeigt, dass wir aus einem längsten Weg W einen Kreis auf den selben Knoten konstruieren können.

Schritt 3. Ein solcher Kreis ist ein Hamiltonkreis.

Sei W jetzt der im zweiten Schritt konstruierte Kreis. Angenommen, es gibt einen Knoten $y \in V(G)$, der nicht auf W liegt. Wir wissen: W enthält sowohl x_k, als auch alle Knoten in $N(x_k)$ – also mindestens $1 + \frac{n}{2}$ Knoten. Nach Voraussetzung ist $|N(y)| \geq \frac{n}{2}$.

Weiters sind die Mengen $\{x_k\} \cup N(x_k)$ mit zumindest $1 + \frac{n}{2}$ vielen Elementen, und $N(y)$ mit mindestens $\frac{n}{2}$ vielen Elementen jeweils Teilmengen von $V(G) \setminus \{y\}$, einer Menge mit $n - 1$ vielen Elementen. Daher gibt es zwei Knoten $x_m, x_\ell \in (\{x_k\} \cup N(x_k)) \cap N(y)$, die Situation ist in Abbildung 13 dargestellt.

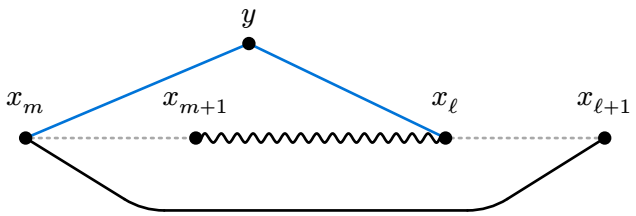


Abbildung 13: Satz von Dirac: Längster Weg zu Kreis.

So würde sich so also ein längerer Weg $(x_{\ell+1} \rightsquigarrow x_m \to y \to x_\ell \rightsquigarrow x_{m+1})$ konstruieren lassen, im Widerspruch zur Maximalität des Weges aus Schritt 2. Der Kreis W muss daher bereits alle Knoten in G enthalten, und ist damit ein Hamiltonkreis. □

3.6 k-partite Graphen

Definition 3.54: Sei G ein Graph.

1. Gibt es eine Partition von $V(G)$ in k Teile, das heißt
$$V(G) = V_1 \uplus V_2 \uplus \ldots \uplus V_k,$$
sodass jedes der V_j eine unabhängige Menge ist (die Endpunkte jeder Kante $e \in E(G)$ also in verschiedenen Teilen liegen), so heißt G ein *k-partiter* Graph.
2. Ist $k = 2$, so heißt G *bipartit*.

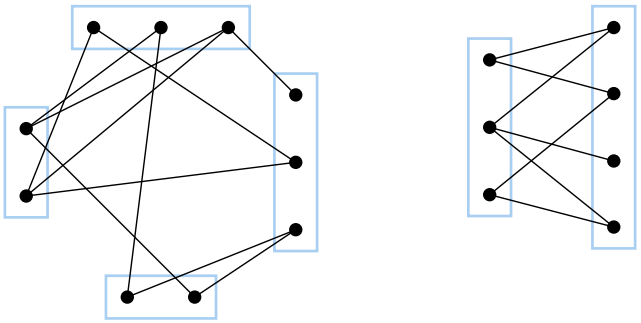


Abbildung 14: Ein 4-partiter Graph (links) und ein bipartiter Graph (rechts).

Definition 3.55: Seien $k, \ell \in \mathbb{N}$, und seien $V_1 := \{a_1, \ldots, a_k\}$ und $V_2 := \{b_1, \ldots, b_\ell\}$ eine k- bzw. ℓ -elementige Menge. Der Graph $G = (V_1 \uplus V_2, E)$ mit Kantenmenge $E = \{\{a, b\} : a \in V_1, b \in V_2\}$ heißt *vollständiger bipartiter Graph* auf k und ℓ Knoten und wird mit $K_{k,\ell}$ bezeichnet.

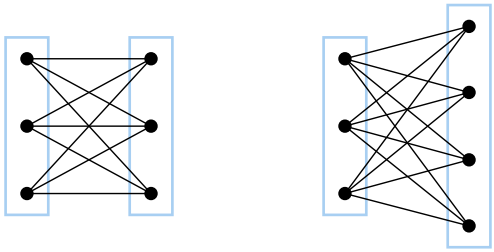


Abbildung 15: Die vollständigen bipartiten Graphen $K_{3,3}$ und $K_{3,4}$.

Satz 3.56: Sei G ein Graph. Dann gilt: G ist genau dann bipartit, wenn G keine Kreise ungerader Länge enthält.

Beweis:

„⇒“ Sei G zunächst bipartit mit Partitionsmengen $V(G) = V_1 \uplus V_2$, und angenommen $C = (x_1, x_1x_2, x_2, ..., x_kx_1, x_1)$ ist ein Kreis in G. Ohne Einschränkung der Allgemeinheit sei $x_1 \in V_1$ (ansonsten tausche die Rollen von V_1 und V_2).

Da Kanten immer zwischen V_1 und V_2 verlaufen, muss $x_2 \in V_2$, $x_3 \in V_1$, $x_4 \in V_2$ und so weiter sein. Knoten mit ungeraden Indizes liegen also in V_1, und jene mit geraden Indizes liegen in V_2. Wegen $x_1x_k \in E(G)$ muss $x_k \in V_2$ liegen, womit k gerade sein muss. Unser Kreis C hat also eine gerade Länge. ✓

„⇐“ Nehmen wir nun an, G enthalte keine Kreise ungerader Länge. Ohne Einschränkung der Allgemeinheit sei G zusammenhängend (ansonsten betrachte alle Zusammenhangskomponenten separat; ein Graph ist bipartit genau dann, wenn alle seine Zusammenhangskomponenten bipartit sind).

Der Graph besitzt dann einen Spannbaum T, der eine Metrik d_T auf dem Graphen G induziert; $d_T(v, w)$ gibt den Abstand der Knoten v und w entlang der Kanten von T an.

Fixiere nun einen beliebigen Knoten $x \in V(G)$ und definiere die beiden Mengen

$V_1 := \{v \in V(G) \mid d_T(x, v) \text{ ist gerade}\}$ und $V_2 := \{v \in V(G) \mid d_T(x, v) \text{ ist ungerade}\}$.

Nach Konstruktion ist dann $V_1 \uplus V_2 = V(G)$, und falls $|V(G)| > 1$, so ist auch $V_1, V_2 \neq \emptyset$. Um zu zeigen, dass G bipartit ist, müssen wir noch zeigen, dass keine Kanten innerhalb von V_1 bzw. V_2 verlaufen; für jede Kante müssen die Endpunkte in verschiedenen Partitionen liegen. Für eine beliebige Kante $yz \in E(G)$ unterscheiden wir jetzt zwei Fälle:

1. $yz \in E(T)$, die Kante kommt im Spannbaum vor. Da es zwischen zwei Knoten in T jeweils einen eindeutigen Weg gibt (Satz 3.37), muss der Weg von y nach x oder von z nach x über die Kante yz verlaufen. Daher ist $|d_T(x, z) - d_T(x, y)| = 1$ und y und z liegen damit in verschiedenen Partitionen. ✓
2. $yz \notin E(T)$. Dann haben die beiden Knoten y und z in T einen ersten gemeinsamen Vorfahren (betrachte die eindeutigen Wege von y nach x und von z nach x und finde den ersten Knoten der in beiden Wegen vorkommt – der Rest der Wege stimmt überein),

nenne diesen u. Innerhalb von G wissen wir so, dass der Weg entlang der Knoten $u \to y \to z \to u$ einen Kreis beschreibt, dieser muss nach Annahme gerade Länge haben. Die Länge des Kreises können wir durch $d_T(u,y) + d_T(u,z) + 1$ ausdrücken, diese Größe ist also gerade. Hinzuzählen einer geraden Zahl wie $2d_T(x,u)$ ändert an der Parität nichts, also ist auch

$$2d_T(x,u) + d_T(u,y) + d_T(u,z) + 1 = d_T(x,y) + d_T(x,z) + 1$$

gerade, wonach $d_T(x,y) + d_T(x,z)$ also ungerade sein muss. Die beiden Abstände können damit nicht die gleiche Parität haben, y und z müssen damit in verschiedenen Partitionen liegen. ✓

□

3.7 Planare Graphen

Die „intuitive Definition“ des Begriffes der Planarität von Graphen lässt sich leicht beschreiben: Ein Graph G heißt *planar*, wenn er so in einer Ebene gezeichnet werden kann, dass sich die Kanten nicht überkreuzen.

Eine technisch saubere Definition erfordert etwas mehr Aufwand. Wir beginnen damit, den Begriff einer „Zeichnung“ eines Graphen zu formalisieren. Eine solche soll durch eine Menge von Punkten in der Ebene und zwischen den Punkten verlaufenden einfachen Kurven gegeben sein.

Definition 3.57 (Ebener Graph): Sei $V \subseteq \mathbb{R}^2$ eine endliche Menge von Punkten und E eine (endliche) Menge von *einfachen Kurven*[13] in $\mathbb{R}^2$, deren Endpunkte in V liegen. Gilt zusätzlich

1. für alle $e_1, e_2 \in E$ ist $e_1^* \cap e_2^* \subseteq V$ („Kanten treffen sich nur in Knoten“),
2. für alle $e_1, e_2 \in E$ ist $|e_1^* \cap e_2^*| \leq 1$ („Kanten haben höchstens einen gemeinsamen Punkt“),
3. für alle $e \in E$ ist $|e^* \cap V| = 2$ („Nur die Endpunkte der Kanten liegen in V“),

so heißt das Tupel $G = (V, E)$ ein *ebener Graph*.

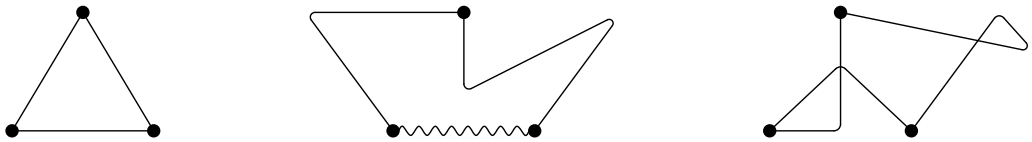


Abbildung 16: Drei Graph-Zeichnungen.

Anmerkung 3.58: Zu einem gegebenen ebenen Graphen $G' = (V, E')$ lässt sich leicht ein zugehöriger „üblicher“ Graph $G = (V, E)$ finden: mittels $e' \mapsto \{e'(0), e'(1)\}$ bilden wir dabei eine Kurve e' auf die durch ihre beiden Endpunkte dargestellte Kante ab. Wir können den ebenen Graphen G' so als zum Graphen G *isomorph* betrachten.

Beispiel 3.59: Die ersten beiden Graphen (von links gesehen) in Abbildung 16 stellen zwei verschiedene ebene Graphen dar, die zu einem Dreieck isomorph sind. Die dritte Zeichnung hingegen ist *kein* ebener

[13] Eine *einfache Kurve* (bzw. *Jordan-Kurve*) im $\mathbb{R}^2$ ist eine injektive, stetige Funktion $\gamma : [0,1] \to \mathbb{R}^2$. Die beiden Punkte $\gamma(0), \gamma(1) \in \mathbb{R}^2$ heißen *Endpunkte* von γ. Mit $\gamma^* := \mathrm{Im}(\gamma) = \{\gamma(t) \mid t \in [0,1]\}$ wird das Bild der Kurve (also die Menge der Punkte in der Ebene, welche die Kurve bilden) bezeichnet.

Graph: die Kante vom oberen zum rechten Knoten ist keine einfache Kurve (sie kreuzt sich selbst, ist also nicht injektiv). Zudem treffen sich die Kante zwischen den unteren beiden Knoten und der Kante zwischen dem oberen und dem linken Knoten in einem Punkt außerhalb der Knotenmenge. ⬠

Während es zu jedem ebenen Graphen also klarerweise einen „normalen“ Graphen gibt, muss das umgekehrt nicht so sein. Wir geben den Graphen, für die wir einen isomorphen ebenen Graphen finden können, einen eigenen Namen.

Definition 3.60 (Planarer Graph): Ein Graph G heißt *planar*, wenn er isomorph zu einem ebenen Graphen ist. In anderen Worten: G ist planar, wenn der Graph eine (überkreuzungsfreie) planare Einbettung besitzt.

Beispiel 3.61: Wie durch die Zeichnungen in Abbildung 8 demonstriert wird, sind die vollständigen Graphen K_n für $1 \leq n \leq 4$ planar. Die in der Abbildung enthaltene Zeichnung von K_5 ist kein ebener Graph (die Kanten sind nicht überkreuzungsfrei) – über die Planarität von K_5 lässt sich an dieser Stelle noch keine Aussage machen. ⬠

Definition 3.62: Sei G ein ebener Graph. Eine *Fläche* von G ist eine topologische Zusammenhangskomponente von $\mathbb{R}^2 \setminus \bigcup_{e \in E(G)} e^*$. Die Menge aller Flächen von G wird mit $F(G)$ bezeichnet.

Beispiel 3.63: Die beiden ebenen Graphen in Abbildung 16 besitzen jeweils zwei Flächen. Für eine Veranschaulichung des Begriffs der „topologischen Zusammenhangskomponenten“ des Komplementes der Bilder der Kanten ist es am einfachsten, ans Kekse backen zu denken. Die Kanten des Graphen bilden dabei die Form, die wir zum Ausstechen verwenden – und die einzelnen Teigstücke entsprechen den Flächen des Graphen. ⬠

Ohne die Aussage streng zu beweisen, verwenden wir die Tatsache, dass zu einem gegebenen planaren Graphen G jeder zugehörige ebene Graph zwar jeweils unterschiedliche Flächenmengen besitzt – die Anzahl der Flächen jedoch gleich bleibt. Aus diesem Grund ist die Notation $|F(G)|$ trotzdem wohldefiniert, obwohl wir die für $F(G)$ eigentlich nötige Zeichnung nicht angeben.

Der folgende Satz stellt jetzt eine Beziehung zwischen der Anzahl der Knoten, Kanten und Flächen von planaren Graphen her.

Satz 3.64 (Euler'sche Polyederformel): Sei G ein zusammenhängender planarer Graph. Dann gilt die Beziehung

$$|V(G)| - |E(G)| + |F(G)| = 2 \tag{6}$$

zwischen den Knoten, Kanten, und Flächen von G.

Beweis: Wir beweisen die Aussage mittels Induktion nach der Anzahl der Kanten $|E(G)| = m$ bei festgehaltener Anzahl der Knoten $|V(G)| = n$.

Induktionsanfang. Minimal zusammenhängende Graphen auf n Knoten sind

genau Bäume (Satz 3.37) – und hat damit nach Satz 3.38 $m = n - 1$ viele Kanten. Da Bäume keine Kreise haben, gibt es nur eine einzige (die „äußere“) Fläche. Damit ist $|V(G)| - |E(G)| + |F(G)| = n - (n-1) + 1 = 2$. ✓

Annahme. Sei $m \in \mathbb{N}$ beliebig aber fest. Die Polyederformel (6)

gelte für alle zusammenhängende planare Graphen mit n Knoten und weniger als m Kanten.

Schluss. Sei G nun zusammenhängend und planar mit n Knoten und m Kanten.

G ist kein Baum (andernfalls wären wir dank des Arguments im Induktionsanfang bereits fertig), also gibt es in G mindestens einen Kreis. Wähle eine beliebige Kante e in diesem Kreis und betrachte den Graphen $G - e$. Nach der Induktionsannahme gilt

$$|V(G-e)| - |E(G-e)| + |F(G-e)| = 2,$$

und zugleich ist $|V(G-e)| = |V(G)|$ und $|E(G-e)| = |E(G)| - 1$. Da e aus einem Kreis in G ausgewählt wurde, verschmelzen in $G - e$ die zwei (verschiedenen) Flächen auf den beiden Seiten von e, also $|F(G-e)| = |F(G)| - 1$. Aus der Gleichung oben folgt so

$$\begin{aligned} 2 &= |V(G-e)| - |E(G-e)| + |F(G-e)| \\ &= |V(G)| - (|E(G)| - 1) + (|F(G)| - 1) \\ &= |V(G)| - |E(G)| + |F(G)|, \end{aligned}$$

was die Polyederformel für G beweist. □

Wir können die Euler'sche Polyederformel dazu verwenden, um notwendige Bedingungen für die Planarität von Graphen zu finden.

Korollar 3.65: Sei $G = (V, E)$ planar und zusammenhängend mit mindestens 3 Knoten. Dann gilt

$$|E| \leq 3(|V| - 2).$$

Beweis: Sei F die Menge der Flächen von G. Für eine Fläche $f \in F$ schreiben wir ∂f für den Rand der Fläche, das heißt die Menge jener Kanten, welche die Fläche f umschließen. Dann gilt:

$$3|F| = \sum_{f \in F} 3 \leq \sum_{f \in F} |\partial f| = \sum_{f \in F} \sum_{e \in \partial f} 1$$

wobei wir in der Ungleichung verwenden, dass jede Fläche von zumindest drei Kanten umschlossen wird. In der Doppelsumme zählen wir für jede Fläche die Anzahl der Kanten – das ist äquivalent dazu, für jede Kante die Anzahl der angrenzenden Flächen zu zählen, also:

$$\sum_{f \in F} \sum_{e \in \partial f} 1 = \sum_{e \in E} \sum_{\substack{f \in F \\ e \in \partial f}} 1 \leq \sum_{e \in E} 2 = 2|E|,$$

wobei wir in der Ungleichung verwenden, dass jede Kante Teil des Randes von höchstens zwei Flächen ist. Insgesamt ergibt sich $3|F| \leq 2|E|$, bzw. $|F| \leq \frac{2}{3}|E|$.

Setzen wir diese Ungleichung in die Polyederformel (6) ein, so erhalten wir

$$2 = |V| - |E| + |F| \leq |V| - |E| + \frac{2}{3}|E| = |V| - \frac{1}{3}|E|,$$

woraus wir nach Umformung die Ungleichung aus der Behauptung erhalten. □

Die Ungleichung aus Korollar 3.65 ist eine notwendige Bedingung dafür, dass ein Graph planar ist. Sie ist aber *nicht* hinreichend: nur weil die Ungleichung erfüllt ist, bedeutet das nicht, dass der Graph auch planar sein muss. Dennoch hilft sie uns jetzt, die Frage nach der Planarität des vollständigen Graphen auf 5 (oder mehr) Knoten zu beantworten.

Korollar 3.66: Der vollständige Graph auf n Knoten, K_n, ist für $n \geq 5$ nicht planar.

Beweis: Für $n = 5$ ist $|E(K_5)| = \binom{5}{2} = 10$ und $|V(K_5)| = 5$. Setzen wir diese Werte in die Ungleichung aus Korollar 3.65 ein, so erhalten wir $10 \leq 3(5-2) = 9$, was offensichtlich falsch ist. Der K_5 kann somit nicht planar sein.

Für jedes $n > 5$ enthält der K_n den K_5 als (induzierten) Teilgraphen. Wenn wir für einen Teilgraphen schon keine überkreuzungsfreie Einbettung zeichnen können, so wird das für den gesamten Graphen ebensowenig funktionieren. □

Nachdem wir die Situation für vollständige Graphen geklärt haben, wenden wir unsere Aufmerksamkeit jetzt den vollständigen bipartiten Graphen zu. Für welche $a, b \in \mathbb{N}$ ist $K_{a,b}$ also planar?

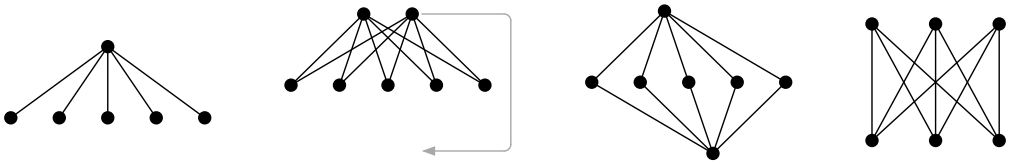


Abbildung 17: Planarität in vollständigen bipartiten Graphen.

- Fixieren wir einen der beiden Parameter auf 1 und betrachten den $K_{1,b}$, so stellen wir leicht fest, dass dieser Graph ein Baum und damit planar ist.
- Für $a = 2$ können wir den vollständigen bipartiten Graphen $K_{2,b}$ wie in Abbildung 17 gezeichnet in die Ebene einbetten. Der Graph ist also ebenso planar.
- Für $a = 3$ ist es schon nicht mehr so leicht, planare Einbettungen für die Graphen $K_{3,b}$ zu finden. Die Vermutung, dass $K_{3,3}$ bereits nicht mehr planar ist, können wir mit dem Mechanismus aus Korollar 3.65 noch nicht beweisen: in diesem Fall ist $\left|V\left(K_{3,3}\right)\right| = 6$ und $\left|E\left(K_{3,3}\right)\right| = 9$. Unsere für die Planarität nötige Ungleichung ist $9 \leq 3 \cdot (6-2) = 12$, eine wahre Aussage.

Um die Situation für $K_{3,3}$ zu entscheiden, brauchen wir eine stärkere Aussage.

Korollar 3.67: Für bipartite, zusammenhängende und planare Graphen $G = (V, E)$ gilt

$$|E| \leq 2(|V| - 2).$$

Beweis: Der Beweis verläuft völlig analog zu jenem von Korollar 3.65, mit der Ausnahme dass wir bei Verwendung der Ungleichung $3 \leq |\partial f|$ für eine Fläche $f \in F$ in diesem Fall wegen Satz 3.56 die stärkere Ungleichung $4 \leq |\partial f|$ verwenden dürfen (da bipartite Graphen keine Kreise ungerader Länge enthalten, muss der kürzeste Kreis damit mindestens Länge 4 haben).

Die Ungleichungskette im Beweis von Korollar 3.65 liefert uns in diesem Fall also $4|F| \leq 2|E|$, bzw. $|F| \leq \frac{1}{2}|E|$, was dann nach Einsetzen in die Polyederformel (6) die Behauptung liefert. □

Korollar 3.68: Für $a, b \geq 3$ ist der vollständige bipartite Graph $K_{a,b}$ nicht planar.

Beweis: Betrachten wir nochmal den $K_{3,3}$ und wenden die Ungleichung speziell für bipartite Graphen aus Korollar 3.67 an. Wir haben $\left|V\left(K_{3,3}\right)\right| = 6$, $\left|E\left(K_{3,3}\right)\right| = 9$, die Ungleichung liest sich damit als

$$9 \leq 2 \cdot (6 - 2) = 8,$$

eine falsche Aussage. Der Graph $K_{3,3}$ kann damit nicht planar sein.

Für $a, b \geq 3$ enthält jeder $K_{a,b}$ den $K_{3,3}$ als Teilgraph, womit auch für $K_{a,b}$ keine überkreuzungsfreie ebene Einbettung existieren kann. □

Mit den beiden vollständigen Graphen K_5 und $K_{3,3}$ haben wir zwei „elementare“ Beispiele für nicht-planare Graphen gefunden. Tatsächlich stellen die beiden Graphen auf gewisse Art und Weise alle möglichen Situationen dar, die zu nicht-planaren Graphen führen können. Um diese Aussage zu präzisieren, brauchen wir den folgenden Begriff.

Definition 3.69: Seien G und K Graphen. Dann heißt K ein *topologischer Minor* von G, wenn es einen Teilgraphen $H \subseteq G$ gibt, sodass H aus K durch Unterteilung von Kanten (durch das Einfügen weiterer Knoten) und Knoten (durch Aufsplitten in zwei durch eine Kante verbundene Knoten) von K hervorgeht.

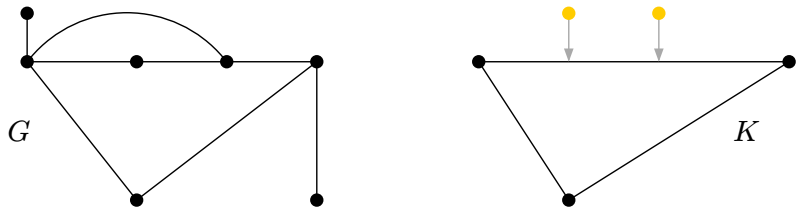


Abbildung 18: Der Graph K rechts (ohne die gelb eingefärbte Knoten) ist ein topologischer Minor des Graphen G links:

Satz 3.70 (Satz von Kuratowski und Wagner): Sei G ein Graph. Dann ist G genau dann planar, wenn G weder K_5 noch $K_{3,3}$ als topologische Minoren enthält.

Beweis: Wir beweisen nur die einfachere der beiden Richtungen dieser Äquivalenz. Nehmen wir an, G sei planar. Würde ein K_5 oder ein $K_{3,3}$ als topologischer Minor in G enthalten sein, so könnten wir also einen Teilgraphen H von G identifizieren, der aus K_5 bzw. $K_{3,3}$ durch Unterteilung von Kanten hervorgeht. Diese Operation ändert aber grundsätzlich nichts an der Planarität des Graphen. Da wir in diesem Abschnitt gezeigt haben, dass sowohl K_5 als auch $K_{3,3}$ nicht planar sind, ist der Teilgraph H demnach auch nicht planar – womit aber auch G nicht planar sein kann; ein Widerspruch. ↯

Für die zweite Richtung des Beweises ist nachzuweisen, dass jeder Graph in dem K_5 und $K_{3,3}$ nicht als topologische Minoren auftauchen, planar ist. Diese Aussage ist relativ langwierig und technisch zu beweisen, wir verweisen daher dafür auf die entsprechende Literatur (etwa Kapitel 6 im Buch Graph decompositions. A study in infinite graph theory. von Reinhard Diestel). □

3.8 Graphfärbungen

Ein klassisches graphentheoretisches Problem im Zusammenhang mit Landkarten hat seinen Ursprung im England des 19. Jahrhunderts (um 1850) genommen:

Francis Guthrie wollte eine Karte der Wahlbezirke in Großbritannien so einfärben, dass benachbarte Bezirke verschiedene Farben haben – gleichzeitig aber insgesamt so wenige Farben wie möglich verwendet werden.

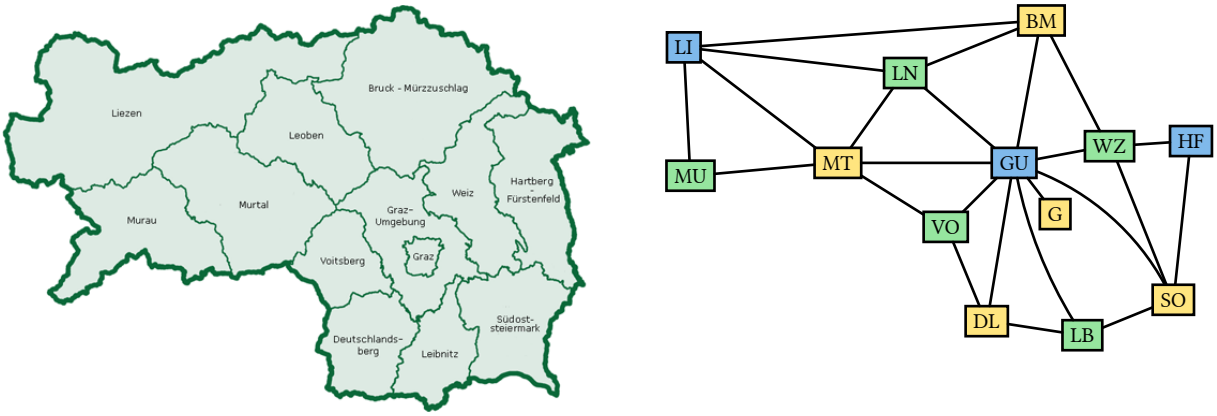


Abbildung 19: Eine Karte der steirischen Bezirke und der zugehörige Landkartengraph.

Zu einer gegebenen Karte betrachten wir den entsprechenden *Landkartengraph*. In diesem steht jeder Knoten für ein Gebiet auf der Karte (bzw. einen Bezirk); Kanten werden genau zwischen den benachbarten Gebieten gezogen. In Abbildung 19 findet sich ein Landkartengraph für die steirischen Bezirke.

Definition 3.71: Sei G ein Graph und $k \in \mathbb{N}$.

1. Eine *zulässige k-Färbung* ist eine Abbildung $c : V(G) \to [k]$, sodass für jede Kante $vw \in E(G)$ die Eigenschaft $c(v) \neq c(w)$ gilt.
2. Der Graph G heißt *k-färbbar*, wenn es eine zulässige k-Färbung gibt.
3. Die *chromatische Zahl* $\chi(G)$ ist die kleinste natürliche Zahl $k \in \mathbb{N}$, sodass der Graph k-färbbar ist.

Beispiel 3.72: Wir machen ein paar Beobachtungen zur Färbbarkeit spezieller Graphen.

- Für eine Färbung des vollständigen Graphen auf n Knoten werden n Farben benötigt: $\chi(K_n) = n$.
- Der Stern-Graph $K_{1,n-1}$ kann in 2 Farben gefärbt werden (eine Farbe für das Zentrum, und eine Farbe für alle anderen Knoten).
- Ganz allgemein ist ein k-partiter Graph k-färbbar: jede Partitionsklasse kann jeweils vollständig mit der gleichen Farbe gefärbt werden.
- Der Kreis-Graph auf n Knoten, C_n, lässt sich für gerade n mit 2 Farben färben (die sich entlang des Kreises einfach abwechseln), für ungerade n (zB den $C_3 = K_3$, ein Dreieck) sind aber 3 Farben nötig.
- Hat ein Graph G eine Clique mit k Knoten, so muss $\chi(G) \geq k$ sein (für die Clique allein werden schon k verschiedene Farben benötigt).
- Der Graph der steirischen Bezirke S erfüllt $\chi(S) = 3$: die Bezirke *Graz-Umgebung*, *Leibnitz*, *Südoststeiermark* bilden eine Clique auf 3 Knoten, $\chi(S)$ ist also mindestens 3 – und die Existenz einer solchen Färbung ist in Abbildung 19 nachgewiesen.

⬠

Die Bestimmung der chromatischen Zahl und viele damit direkt verwandte Probleme sind im allgemeinen sehr, sehr schwere Probleme für die es keine effizienten, exakten Lösungsalgorithmen gibt. Selbst das Problem zu entscheiden, ob für einen gegebenen Graphen $\chi(G) \leq 3$ ist, ist NP-vollständig.

Während das Graphfärbungsproblem zwar auch für allgemeine Graphen (etwa im Zusammenhang mit dem Planen von Stundenplänen: Knoten stehen für verschiedene LVen; Farben entsprechen verschiedenen Zeit- und Raumslots. Knoten sind dann verbunden, wenn sie nicht gleichzeitig stattfinden können, etwa weil gleiche:r Vortragende:r) interessant ist, so können wir über den konkreten Fall von Landkartenfärbungen noch ein bisschen mehr sagen: Landkartengraphen sind (solange man sich auf zusammenhängende Gebiete beschränkt) nämlich immer planar.

Der folgende berühmte Satz macht eine wesentliche Aussage über die Färbbarkeit von planaren Graphen.

Satz 3.73 (Vier-Farben-Satz): Jeder planare Graph ist 4-färbbar.

Anmerkung 3.74: Während die Aussage bereits um 1850 vermutet wurde, hat es bis 1976 gebraucht bis ein Beweis erbracht wurde. Kenneth Appel und Wolfgang Haken konnten zeigen, dass die 4-Färbbarkeit zu einer Aussage äquivalent ist, die durch Fallunterscheidung mit einer großen Anzahl von verschiedenen Fällen (1936 viele) bewiesen werden kann – was sie dann mit Unterstützung eines Computers durchführen konnten. Der Vier-Farben-Satz war einer der ersten Sätze, die mittels eines *computergestützten Beweises / computer aided proof* bewiesen wurden – was in manchen Kreisen immer noch ein äußerst kontroverses Thema ist.

Bis heute gibt es keinen Beweis, der voll nur von Menschen mit realistischem Zeitaufwand überprüft werden kann. Auf der „anderen Seite“, der computergestützten Verifikation von Beweisen, wird allerdings sehr aktiv gearbeitet: interaktive Beweisassistenten wie *Isabelle*, *Coq*, *LEAN* erlauben es, aus einem Axiomensystem abgeleitete Resultate semi-automatisch auf Konsistenz und Korrektheit zu über-

prüfen. Die Liste der im Rahmen solcher Systeme verifizierten Beweise wächst laufend[14] das ist ein sehr aktives Forschungsgebiet.

Eine etwas schwächere (und dafür auch innerhalb von etwa einer Seite zu beweisende) Aussage ist der sogenannte Fünf-Farben-Satz.

Satz 3.75 (Fünf-Farben-Satz): Jeder planare Graph ist 5-färbbar.

Beweis (Skizze): Aus Zeitgründen skizzieren wir das Argument nur: Der Beweis basiert darauf, dass für jeden planaren Graphen G der Minimalgrad $\delta(G) \leq 5$ ist. Entfernen wir so einen Knoten mit Grad höchstens 5 aus G entsteht ein kleinerer Graph; ein Induktionsargument erlaubt den Schluss, dass der kleinere Graph 5-färbbar ist – womit wir uns nur mehr um das Wiedereinfügen des entfernten Knoten kümmern müssen. □

[14] https://leanprover-community.github.io/mathlib-overview.html

§4 – Elementare Zahlentheorie

Die *Zahlentheorie* ist jenes mathematische Teilgebiet, in dem Eigenschaften von Zahlen und Zahlbereichen untersucht werden. Die *elementare Zahlentheorie* beschäftigt sich konkret mit der Teilbarkeit ganzer Zahlen.

4.1 Teiler und Teilbarkeit

Definition 4.1: Seien $a, b \in \mathbb{Z}$. Gibt es eine ganze Zahl $k \in \mathbb{Z}$ mit $a \cdot k = b$, so sagen wir, dass a die Zahl b teilt und schreiben $a \mid b$. Insbesondere heißt in diesem Fall a ein *Teiler* von b, bzw. b ein *Vielfaches* von a. In Zeichen:

$$a \mid b \iff \exists k \in \mathbb{Z} : a \cdot k = b.$$

Ist a kein Teiler von b, so schreiben wir $a \nmid b$.

Beispiel 4.2: Die folgenden Eigenschaften lassen sich leicht überprüfen:

$$2 \mid 6, \quad 2 \nmid 2041, \quad 4 \mid -20, \quad 42 \mid 0, \quad 0 \nmid 42, \quad -7 \mid 42.$$

⬠

Proposition 4.3: Seien $a, b, c \in \mathbb{Z}$. Dann gelten die folgenden Aussagen:

1. $ab \mid c \Rightarrow a \mid c$.
2. $c \mid a \Rightarrow c \mid ab$.
3. Ist $c \neq 0$, so ist $a \mid b \iff ac \mid bc$.
4. Gilt $a \mid b$ und $a \mid c$, so ist $a \mid (b \pm c)$.
5. Die Zahl 0 ist Vielfaches jeder Zahl: $\forall a \in \mathbb{Z} : a \mid 0$.
6. Die Zahl 0 ist genau dann Teiler von a, wenn $a = 0$ ist.

Beweis: Die Aussagen lassen sich jeweils durch einfaches Umformen der Definition der Teilbarkeit nachweisen. Wir führen die Beweise exemplarisch für ausgewählte Aussagen durch.

1. Sei $ab \mid c$, es gibt also ein $k \in \mathbb{Z}$ mit $abk = c$. Dann ist auch $a(bk) = c$, also $a \mid c$. ✓
3. Sei $c \neq 0$, dann gelten die folgenden Äquivalenzen: $a \mid b$ genau dann, wenn es ein $k \in \mathbb{Z}$ mit $ak = b$ gibt. Wegen $c \neq 0$ gilt diese Gleichung genau dann, wenn $akc = bc$ ist – was wiederum äquivalent zu $ac \mid bc$ ist. ✓
4. Seien $a \mid b$ und $a \mid c$, es gibt also $k, \ell \in \mathbb{Z}$ mit $ak = b$ und $a\ell = c$. Demnach ist $b \pm c = ak \pm a\ell = a(k \pm \ell)$, woraus $a \mid b \pm c$ folgt, wie behauptet. ✓

□

Definition 4.4: Sei $k \in \mathbb{N}$ und seien $a_1, a_2, ..., a_k \in \mathbb{Z}$. Eine ganze Zahl $d \in \mathbb{Z}$ heißt *gemeinsamer Teiler* von $a_1, a_2, ..., a_k$, wenn $d \mid a_j$ für jedes $j \in [k]$.

Ein gemeinsamer Teiler d von $a_1, ..., a_k$ heißt *größter gemeinsamer Teiler* (kurz: ggT oder gcd; *greatest common divisor*), wenn d betragsmäßig größer (oder gleich) als alle anderen gemeinsamen Teilern ist. Wir schreiben $d = \gcd(a_1, ..., a_k)$.

Gilt $\gcd(a_1, ..., a_k) = 1$, so heißen die Zahlen $a_1, ..., a_k$ *teilerfremd* oder *relativ prim*.

Beispiel 4.5: Wir wollen den größten gemeinsamen Teiler von 42 und 18 bestimmen. Die (positiven) Teiler von 42 sind $1, 2, 3, 6, 7, 14, 21, 42$, und die (positiven) Teiler von 18 sind $1, 2, 3, 6, 9, 18$. Die Zahlen $1, 2, 3, 6$ sind damit die (positiven) gemeinsamen Teiler, und es folgt $\gcd(42, 18) = 6$.

Betrachten wir die beiden Zahlen 9 und 14. Die (positiven) Teiler von 9 sind 1, 3, 9, und jene von 14 sind 1, 2, 7, 14. Die Zahl 1 ist der einzige positive gemeinsame Teiler, also ist auch $\gcd(14, 9) = 1$: die Zahl 9 ist relativ prim zu 14. ⬠

Praktisch ist es nicht effizient, den größten gemeinsamen Teiler durch Bestimmung aller gemeinsamen Teiler zu finden. Wir suchen daher nach einem besseren Weg; das folgende Ergebnis liefert den zentralen Baustein dafür.

Proposition 4.6: Seien $a, b, c \in \mathbb{Z}$. Dann gilt:

1. Für $a \neq 0$ ist $\gcd(a, 0) = |a|$.
2. Der größte gemeinsame Teiler ändert sich nicht, wenn wir ein Vielfaches von b zu a addieren bzw. subtrahieren: $\gcd(a, b) = \gcd(b, a - c \cdot b)$.

Beweis: Zuerst zur ersten Eigenschaft: jede ganze Zahl ist Teiler von 0, der größte gemeinsame Teiler von 0 und a ist damit der größte Teiler von a, dieser ist $|a|$.

Für die zweite Eigenschaft verfolgen wir die *„name and conquer“*-Strategie: wir setzen $d = \gcd(a, b)$ und $e = \gcd(b, a - bc)$. Da d gemeinsamer Teiler von a und b ist, haben wir $d \mid a$ und $d \mid b$, woraus wegen Proposition 4.3 auch $d \mid bc$ folgt. Eine weitere Anwendung der Proposition liefert dann $d \mid a - bc$; die Zahl d ist also auch ein gemeinsamer Teiler von b und $a - bc$. Nach Definition des größten gemeinsamen Teilers gilt damit $d \leq e$.

Umgekehrt wissen wir, dass e gemeinsamer Teiler von b und $a - bc$ ist, mit Proposition 4.3 folgt $e \mid bc$ und daraus $e \mid (a - bc) + bc = a$, die Zahl e ist daher gemeinsamer Teiler von a und b – weswegen $e \leq d$ gelten muss.

Gemeinsam folgt aus den beiden Ungleichungen so $\gcd(a, b) = d = e = \gcd(b, a - bc)$. □

Mittels fortlaufender Subtraktion (*„Wechselwegnahme“*) können wir den größten gemeinsamen Teiler effizient berechnen!

Beispiel 4.7: Wir berechnen den größten gemeinsamen Teiler von $a = 2024$ und $b = 71$. Wir ziehen die kleinere Zahl in jedem Schritt so oft wie möglich (d.h., im ersten Schritt $c = \left\lfloor \frac{a}{b} \right\rfloor = 28$ mal) ab, bis die Zahlen ihre Rollen tauschen.

$$\begin{aligned}\gcd(2024, 71) &= \gcd(71, 2024 - 28 \cdot 71) = \gcd(71, 36) = \gcd(36, 71 - 1 \cdot 36)\\ &= \gcd(36, 35) = \gcd(35, 36 - 1 \cdot 35) = \gcd(35, 1)\\ &= \gcd(1, 35 - 35 \cdot 1) = \gcd(1, 0) = 1.\end{aligned}$$

Wir können die Subtraktionen, die am Ende zum größten gemeinsamen Teiler geführt haben jetzt aber auch „rückwärts lesen“ (die Zahlen, die als Argumente von gcd auftauchen sind der Übersichtlichkeit halber eingefärbt):

$$\begin{aligned}1 &= 36 - 1 \cdot 35 = 36 - 1 \cdot (71 - 1 \cdot 36) = -1 \cdot 71 + 2 \cdot 36\\ &= -1 \cdot 71 + 2 \cdot (2024 - 28 \cdot 71) = 2 \cdot 2024 - 57 \cdot 71.\end{aligned}$$

Für unseren größten gemeinsamen Teiler $d = \gcd(a, b)$ haben wir so Zahlen $x, y \in \mathbb{Z}$ gefunden, die $ax + by = d$ erfüllen – eine Strategie, die immer funktioniert (die wir aber auch effizienter ausführen können). ⬠

Satz 4.8 (Erweiterter Euklid'scher Algorithmus): Gegeben seien $a, b \in \mathbb{Z}$, nicht beide zugleich 0. Dann berechnet die folgende Prozedur die Zahlen $d, x, y \in \mathbb{Z}$, (ausgegeben als Tripel (d, x, y)) für welche $d = \gcd(a, b)$ sowie $d = ax + by$ gilt:

```
def euklid(a: int, b: int) -> (int, int, int):
    d = [a, b]
    x = [1, 0]
    y = [0, 1]
    k = 1
    while d[k] != 0:
        q = floor(d[k-1] / d[k])
        d.append(d[k-1] - q * d[k])  # compute d[k+1]
        x.append(x[k-1] - q * x[k])  # compute x[k+1]
        y.append(y[k-1] - q * y[k])  # compute y[k+1]
        k = k + 1

    return (d[k-1], x[k-1], y[k-1])
```

Insbesondere: die `euklid`-Funktion terminiert (d.h., endet nach endlich vielen Schritten) und ist korrekt.

Beweis: Wir bezeichnen die Zahlen der in der Funktion vorkommenden Listen `d`, `x`, `y` mit $d_j := d[j]$, $x_j := x[j]$ und $y_j := y[j]$.

Zunächst zeigen wir, dass der Algorithmus terminiert. Dazu beobachten wir, dass d_{k+1} der Rest bei Division von d_{k-1} durch d_k ist, es muss daher $0 \leq d_{k+1} < d_k$ gelten. Die Folge $d_1, d_2, d_3, \ldots$ von ganzen Zahlen ist also streng monoton fallend und nicht-negativ – womit nach endlich vielen Schritten der Wert 0 erreicht wird.

Wir zeigen nun die Korrektheit des Algorithmus. Sei dazu $q_k = \left\lfloor \frac{d_{k-1}}{d_k} \right\rfloor$ der Quotient, der bei der Berechnung von d_{k+1} benötigt wird: $d_{k+1} = d_{k-1} - q_k \cdot d_k$. Sei nun k so gewählt, dass $d_{k+1} = 0$ ist, der Algorithmus also den Wert d_k als größten gemeinsamen Teiler gefunden hat. Mit der Proposition zur Wechselwegnahme gilt dann

$$\begin{aligned} d_k &= \gcd(0, d_k) = \gcd(d_{k+1}, d_k) = \gcd(d_{k-1} - q_k \cdot d_k, d_k) = \gcd(d_{k-1}, d_k) \\ &= \gcd(d_k, d_{k-1}) = \ldots = \gcd(d_{k-1}, d_{k-2}) = \ldots = \gcd(d_1, d_0) = \gcd(b, a) \\ &= \gcd(a, b), \end{aligned}$$

die Funktion `euklid` berechnet also tatsächlich den größten gemeinsamen Teiler von a und b.

Es bleibt nun noch zu zeigen, dass die Zahlen $x = x_k$ und $y = y_k$ die Gleichung $ax + by = \gcd(a, b)$ erfüllen. Wir zeigen dazu mittels vollständiger Induktion, dass in jedem Schritt $d_j = ax_j + by_j$ gilt.

Induktionsanfang. Für $j = 0$ bzw. $j = 1$ folgt die Behauptung aus den initialen Werten der Variablen:

$$\begin{aligned} ax_0 + by_0 &= a \cdot 1 + b \cdot 0 = a = d_0, \\ ax_1 + by_1 &= a \cdot 0 + b \cdot 1 = b = d_1. \end{aligned}$$

Induktionsschritt. Angenommen, die Beziehung $ax_\ell + by_\ell = d_\ell$ gelte für alle $0 \leq \ell \leq j$, für beliebiges aber festes j. Wir müssen zeigen, dass dann auch $ax_{j+1} + by_{j+1} = d_{j+1}$ gilt. Setzen wir dazu die Rekursion für d_{j+1} ein, so erhalten wir

$$\begin{aligned} d_{j+1} = d_{j-1} - q_j \cdot d_j &= \underbrace{ax_{j-1} + by_{j-1}}_{d_{j-1} \text{ lt. Annahme}} - q_j \underbrace{(ax_j + by_j)}_{d_j \text{ lt. Annahme}} \\ &= \underbrace{a(x_{j-1} - q_j x_j)}_{x_{j+1}} + \underbrace{b(y_{j-1} - q_j y_j)}_{y_{j+1}} = ax_{j+1} + by_{j+1}, \end{aligned}$$

was den Induktionsschritt vervollständigt.

Es werden also auch die Zahlen x und y mit der gewünschten Eigenschaft gefunden. □

Anmerkung 4.9: Der erweiterte Euklid'sche Algorithmus zeigt, dass sich der größte gemeinsame Teiler *immer* als „Ganzzahl-Linearkombination" der Ausgangszahlen schreiben lässt. Diese Aussage ist auch als *Lemma von Bézout* oder als *Bézout'sche Identität* bekannt.

Beispiel 4.10: Wir berechnen den größten gemeinsamen Teiler von $a = 2024$ und $b = 138$, veranschaulichen diesmal aber die Zwischenwerte des erweiterten Euklid'schen Algorithmus in der folgenden Tabelle:

k	d_k	q_k	x_k	y_k
0	2024	/	1	0
1	138	14	0	1
2	92	1	1	−14
3	46	2	−1	15
4	0	/	/	/

Da $d_4 = 0$ ist, haben wir mit $d_3 = 46$ den größten gemeinsamen Teiler von 2024 und 138 gefunden. Die Zahlen $x = -1$ und $y = 15$ erfüllen die Gleichung $2024 \cdot (-1) + 138 \cdot 15 = 46$. ⬠

Proposition 4.11 (Fundamentallemma der Arithmetik): Seien $a, b, c \in \mathbb{Z}$ mit $a \mid bc$. Wenn $\gcd(a, c) = 1$ ist, dann folgt $a \mid b$.

Beweis: Da $\gcd(a, c) = 1$ folgt aus der Bézout'schen Identität die Existenz von ganzen Zahlen x, y mit $ax + cy = 1$. Da $a \mid bc$ ist a auch ein Teiler von $bcy = b \cdot (1 - ax) = b - abx$. Gleichzeitig ist a aber auch Teiler von abx

Aus $a \mid b - abx$ und $a \mid abx$ folgt, dass a auch Teiler der Summe $(b - abx) + abx = b$ ist, womit die Aussage bewiesen ist. □

4.2 Primzahlen

Definition 4.12: Sei $p \in \mathbb{N}$, $p \geq 2$. Dann heißt p eine *Primzahl*, wenn 1 und p die einzigen Teiler von p sind.

Beispiel 4.13: Die ersten paar Primzahlen sind durch

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

gegeben. **Merke:** die Zahl 1 ist *keine Primzahl*! ⬠

Satz 4.14 (Hauptsatz der Arithmetik): Sei $a \in \mathbb{N}$. Dann gibt es ein $r \in \mathbb{N}_0$ sowie (nicht notwendigerweise verschiedene) Primzahlen $p_1, p_2, p_3, \ldots, p_r$, sodass

$$a = \prod_{j=1}^{r} p_j = p_1 \cdot p_2 \cdot \ldots \cdot p_r.$$

Diese Faktorisierung heißt die *Primfaktorzerlegung* von a und ist bis auf die Reihenfolge der Faktoren eindeutig.

Beweis: Wir beweisen die beiden Teile der Aussage (Existenz und Eindeutigkeit) in zwei Schritten. Zuerst zur Existenz – diese beweisen wir mittels Induktion nach a.

Induktionsanfang. Sei $a = 1$. In diesem Fall ist die gesuchte Faktorisierung durch $r = 0$ und damit durch das „leere Produkt" $\prod_{j=1}^{0} p_j = 1$ gegeben. Die Zahl 1 hat eine aus 0 Primzahlen bestehende Primfaktorzerlegung.

Induktionsschritt. Angenommen, jede Zahl kleiner als a habe eine Primfaktorzerlegung. Zu zeigen ist dann, dass auch a eine solche besitzt.

- Falls a eine Primzahl ist, so ist durch $r = 1$ mit $p_1 = a$ eine Faktorisierung gefunden.
- Andernfalls ist a keine Primzahl, womit es $b, c \in \mathbb{N}$ mit $b, c < a$ geben muss, sodass $a = b \cdot c$. Aufgrund der Induktionsannahme besitzen sowohl b als auch c eine Primfaktorzer-

legung. Multiplizieren wir diese zusammen, so erhalten wir eine Primfaktorzerlegung für a. ✓

Es verbleibt zu zeigen, dass die Zerlegung bis auf die Reihenfolge der Faktoren eindeutig ist. Nehmen wir dazu an, dass eine Zahl a zwei verschiedene Primfaktorzerlegungen

$$p_1 \cdot p_2 \cdot \ldots \cdot p_r = a = q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

besitzen würde, und nehmen wir o.B.d.A. an, dass a die kleinste natürliche Zahl mit dieser Eigenschaft wäre.

Da $q_1 \cdot (q_2 \cdot \ldots \cdot q_s) = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ ist, gilt $q_1 \mid p_1 \cdot \ldots \cdot p_r$. Wäre irgendeine der Zahlen p_j gleich der Zahl q_1, so könnten wir auf beiden Seiten kürzen und erhalten

$$q_2 \cdot \ldots \cdot q_s = p_1 \cdot \ldots \cdot p_{j-1} \cdot p_{j+1} \cdot \ldots \cdot p_r,$$

das sind demnach verschiedene Primfaktorzerlegungen für die ganze Zahl $\frac{a}{q_1} < a$, was wegen unserer Minimalitätsannahme aber nicht möglich ist. Die Zahl q_1 kann damit nicht als einer der Faktoren $p_1, \ldots, p_r$ auftauchen.

Nun können wir das Fundamentallemma anwenden: wegen $\gcd(q_1, p_r) = 1$ folgt $q_1 \mid p_1 \cdot p_2 \cdot \ldots \cdot p_{r-1}$. Dieses Argument können wir jetzt aber beliebig wiederholen um schließlich $q_1 \mid p_1 \cdot p_2$ und daraus $q_1 \mid p_1$ zu folgern – was ein Widerspruch ist ($q_1 \neq p_1$, q_1 ist aber auch mindestens 2 und kann p_1 damit nicht teilen). □

Anmerkung 4.15: In Satz 4.14 ist einer der gewichtigsten Gründe versteckt, warum die Zahl 1 explizit von der Definition der Primzahlen ausgeschlossen wird: wäre 1 prim, so wäre die Primfaktorzerlegung $42 = 7 \cdot 3 \cdot 2 = 7 \cdot 3 \cdot 2 \cdot 1 = 7 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 7 \cdot 3 \cdot 2 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1$ nicht mehr eindeutig. Prinzipiell würde sich das zwar auch ad-hoc reparieren lassen (*die Primfaktorzerlegung ist bis auf die Reihenfolge der Faktoren und die Anzahl der Vorkommen des Faktors 1 eindeutig* …), das ist aber weder besonders elegant, noch bringt es in diesem Zusammenhang irgendwelche Vorteile.

Beispiel 4.16: Es lässt sich leicht nachrechnen, dass die folgenden Primfaktorzerlegungen gelten:

$$2022 = 2 \cdot 3 \cdot 337, \quad 2023 = 7 \cdot 17 \cdot 17, \quad 2024 = 2 \cdot 2 \cdot 2 \cdot 11 \cdot 23, \quad 2027 = 2027.$$

⬠

Anmerkung 4.17: Fasst man alle gleichen Primfaktoren zusammen, so kann man die Primfaktorzerlegung als $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ für verschiedene Primzahlen $p_1, p_2, \ldots, p_r$ und positive ganze Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_r$ schreiben. Für eine Primzahl p soll $v_{p(a)}$ (die sogenannte p-adische Valuation von a) den Exponenten von p in der Primfaktorzerlegung von a angeben.

Beispiel 4.18: Es ist etwa $v_2(14) = v_2(2^1 \cdot 7) = 1$, $v_{17}(2023) = 2$, $v_2(2048) = v_2(2^{11}) = 11$, und insbesondere, im Fall dass eine Primzahl in einer Faktorisierung nicht auftaucht, $v_{13}(42) = v_{13}(2 \cdot 3 \cdot 7 \cdot 13^0) = 0$. ⬠

Satz 4.19 (Satz von Euklid): Es gibt unendlich viele Primzahlen.

Beweis: Mit Widerspruch. Angenommen, es gäbe nur endlich viele Primzahlen, nenne diese $p_1, p_2, ..., p_N$. Betrachten wir die Zahl

$$g := p_1 \cdot p_2 \cdot ... \cdot p_N + 1.$$

Jede Zahl hat eine Primfaktorzerlegung, so auch die Zahl g, also muss eine der Primzahlen in $p_1, ..., p_N$ die Zahl g teilen. Sei p_j nun also ein Primfaktor von g. Dann gilt: $p_j \mid p_1 p_2 ... p_N + 1$ und (da p_j als Faktor in dem Produkt vorkommt) $p_j \mid p_1 p_2 ... p_N$. Dann muss p_j aber auch die Differenz dieser beiden Vielfachen teilen; also ein Teiler von

$$g - p_1 ... p_N = p_1 ... p_N + 1 - p_1 ... p_N = 1$$

sein. Die Zahl 1 hat aber nur sich selbst als Teiler, und es gilt $p_j > 1$ – wir haben also einen Widerspruch gefunden. Es kann nicht nur endlich viele Primzahlen geben. □

Während nicht sonderlich problematisch war zu zeigen, dass es unendlich viele Primzahlen gibt, gibt es auch eine Reihe von ebenso leicht zu formulierenden Fragen, die bis heute nicht beantwortet sind. Die folgenden beiden Aussagen sind Beispiele für offene Probleme.

Vermutung 4.20: Ein Tupel $(p, p+2)$ wird *Primzahlzwilling* genannt, wenn sowohl p als auch $p+2$ Primzahlen sind. Es wird vermutet, dass es unendlich viele solcher Primzahlzwillinge gibt.

Vermutung 4.21 (Goldbach'sche Vermutung): Jede gerade Zahl $n \geq 4$ lässt sich als Summe von zwei Primzahlen darstellen.

Einer der am intensivsten erforschten Themenbereiche in der elementaren Zahlentheorie betrifft die Verteilung der Primzahlen. Ein klassisches Resultat in dem Zusammenhang ist der sogenannte *Primzahlsatz*, der eine Aussage über die Anzahl der Primzahlen bis zu einer gegebenen Schranke macht.

Satz 4.22 (Primzahlsatz): Sei $\pi(x)$ die Anzahl der Primzahlen, die kleiner oder gleich x sind, also $\pi(x) := |\{p \in \mathbb{N} : p \leq x, p \text{ ist Primzahl}\}|$. Dann ist $\pi(x)$ asymptotisch gleich zur Funktion $\frac{x}{\log(x)}$, das heißt

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

Der Beweis des Satzes ist *out of scope* für diese Vorlesung. Es gibt verschiedene Beweisstrategien; eine der in diesem Zusammenhang üblicheren involviert die Untersuchung der analytischen Eigenschaften der Riemann'schen Zeta-Funktion, $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$, in der komplexen Zahlebene. Die Aussage des Primzahlsatzes wird in Abbildung Abbildung 20 veranschaulicht.

4.3 Kongruenzen und modulare Arithmetik

Definition 4.23: Sei $m \in \mathbb{Z}$. Zwei ganze Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* m, wenn $m \mid (a - b)$. Wir schreiben: $a \equiv b \pmod{m}$. Die Zahl m wird in dem Zusammenhang manchmal der *Modul* der Kongruenz genannt.

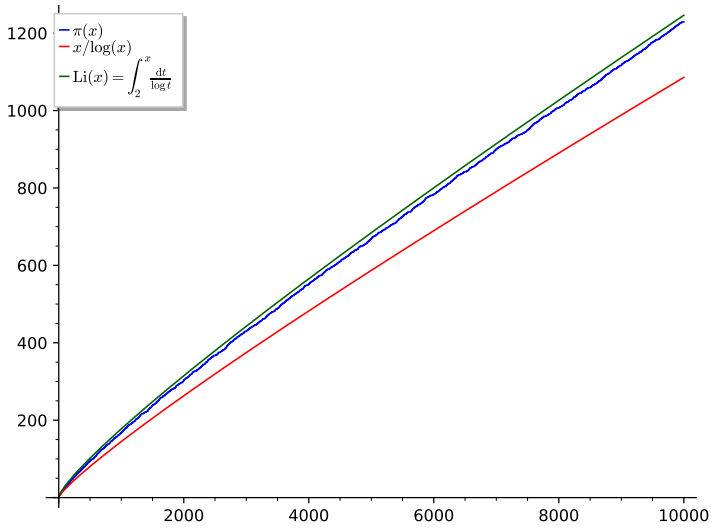


Abbildung 20: Vergleich der Primzahlfunktion $\pi(x)$ (in blau) mit dem nach dem Primzahlsatz asymptotischen Hauptterm $\frac{x}{\log(x)}$ (in rot). Das logarithmische Integral $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$ ist eine asymptotisch ebenfalls äquivalente, praktisch aber sogar noch präzisere Abschätzung für $\pi(x)$.

Beispiel 4.24: Es gilt etwa $1 \equiv 6 \pmod 5$, da $5 \mid 6 - 1$ (bzw. auch $1 - 6 = -5$ – ob in der Definition die Teilbarkeit von $a - b$ oder $b - a$ geprüft wird, ist unerheblich).

Ebenso gilt $1 \equiv -99 \pmod 5$, da $5 \mid 1 - (-99)$. Es ist jedoch $10 \not\equiv 42 \pmod 5$, da $5 \nmid (42 - 10) = 32$.

Zwei spezielle Werte für den Modul m sind die Zahlen 0 und 1:

- Für $m = 1$ ist $a \equiv b \pmod 1$ nach Definition genau dann, wenn $1 \mid a - b \in \mathbb{Z}$. Da 1 *jede* ganze Zahl teilt stimmt $a \equiv b \pmod 1$ also für alle ganzen Zahlen a, b.
- Für $m = 0$ ist die Definition von $a \equiv b \pmod 0$ äquivalent zu $0 \mid a - b$, was laut Proposition 4.3 nur genau dann gilt, wenn $a - b = 0$, also $a = b$ ist.

⬠

Proposition 4.25: Seien $a, b, m \in \mathbb{Z}$. Dann gilt $a \equiv b \pmod m$ genau dann, wenn a und b den gleichen Rest bei Division durch m haben.

Beweis:

⇒: Sei zunächst $a \equiv b \pmod m$, also $m \mid a - b$. Weiters sei r_a bzw. r_b der Rest bei Division von a durch m, bzw. von b durch m. Es gibt also $q_a, q_b \in \mathbb{Z}$ mit $a = q_a m + r_a$ und $b = q_b m + r_b$, wobei die Reste die typische Eigenschaft $0 \leq r_a, r_b < m$ erfüllen. Dann ist

$$a - b = q_a m + r_a - q_b m - r_b = (q_a - q_b)m + (r_a - r_b).$$

Da m ein Teiler von $a - b$, als auch von $(q_a - q_b)m$ ist, muss m auch Teiler der Differenz dieser Vielfachen, also (nach Umformung der Gleichung) $r_a - r_b$ sein. Wegen $0 \leq r_a, r_b < m$ kann diese Differenz nun aber nur Werte in $-m + 1 \leq r_a - r_b \leq m - 1$ annehmen; in

diesem Bereich ist nur die Zahl 0 Vielfaches von m. Wegen $m \mid r_a - r_b$ muss also $r_a - r_b = 0$, und damit $r_a = r_b$ sein. ✓

$\Leftarrow$: Angenommen, a und b haben den gleichen Rest bei Division durch m; es gibt also $q_a, q_b \in \mathbb{Z}$ mit $a = q_a m + r$ und $b = q_b m + r$. Es folgt

$$a - b = (q_a - q_b)m + (r - r) = (q_a - q_b)m,$$

der Modul m teilt also $a - b$ – oder, in anderen Worten, $a \equiv b \pmod m$. ✓

□

Wir wollen nun eine Reihe nützlicher Rechenregeln für Kongruenzen kennenlernen.

Satz 4.26: Seien $a, b, c, d, m \in \mathbb{Z}$. Dann gelten die folgenden Aussagen.

1. Die Relation $\cdot \equiv \cdot \pmod m$ ist eine Äquivalenzrelation (d.h., sie ist reflexiv, symmetrisch, transitiv). Die Äquivalenzklassen sind die Mengen $a + m\mathbb{Z} := \{a + km \mid k \in \mathbb{Z}\}$.
2. Wenn $a \equiv b \pmod m$ und $c \equiv d \pmod m$, so ist $a \pm c \equiv b \pm d \pmod m$ und $a \cdot c \equiv b \cdot d \pmod m$.
3. Für $c \geq 0$ folgt aus $a \equiv b \pmod m$ auch $a^c \equiv b^c \pmod m$.
4. Wenn $c \neq 0$, so ist $a \equiv b \pmod m$ genau dann, wenn $ac \equiv bc \pmod{cm}$.
5. Ist $\gcd(c, m) = 1$, so ist $a \equiv b \pmod m$ genau dann, wenn $ac \equiv bc \pmod m$.

Beweis:

1. Wir untersuchen die Eigenschaften der Relation:
   - Reflexivität: $a \equiv a \pmod m$ ist wegen $m \mid a - a = 0$ erfüllt.
   - Symmetrie: Wenn $a \equiv b \pmod m$, so ist $m \mid a - b = (-1) \cdot (b - a)$, m teilt also auch $b - a$, womit $b \equiv a \pmod m$ gilt.
   - Transitivität: Sei $a \equiv b \pmod m$ und $b \equiv c \pmod m$. Damit ist der Modul m ein Teiler von $a - b$ und von $b - c$, also auch von der Summe $(a - b) + (b - c) = a - c$, womit aber $a \equiv c \pmod m$ gilt.

   Die Relation ist damit eine Äquivalenzrelation. Die Form der Äquivalenzklassen folgt aus Proposition 4.25.
2. Seien $a \equiv b \pmod m$ und $c \equiv d \pmod m$. Dann ist $m \mid a - b$ und $m \mid c - d$, also auch $m \mid (a - b) \pm (c - d) = (a \pm c) - (b \pm d)$; daher ist $a \pm c \equiv b \pm d \pmod m$.

   Für die Multiplikativität beobachten wir, dass es wegen $m \mid a - b$ und $m \mid c - d$ ganze Zahlen $q_a, q_c \in \mathbb{Z}$ mit $a - b = q_a \cdot m$ und $c - d = q_c \cdot m$, bzw. $a = b + q_a \cdot m$ und $c = d + q_c \cdot m$. Multiplizieren wir die beiden Gleichungen miteinander, so erhalten wir

   $$ac = (b + q_a \cdot m)(d + q_c \cdot m) = bd + m \cdot (q_a d + q_c b + q_a q_c m).$$

   Bringen wir bd auf die linke Seite dieser Gleichung, so stellen wir fest, dass m ein Teiler von $ac - bd$ ist – womit $ac \equiv bd \pmod m$ gezeigt ist.

3. Wenden wir die Multiplikativität der Kongruenz $a \equiv b \pmod{m}$ aus Punkt (2) einfach c-mal auf sich selbst an, so erhalten wir $a^c \equiv b^c \pmod{m}$.

4. Unter der Voraussetzung $c \neq 0$ gilt die folgende Äquivalenzkette:

$$\begin{aligned} a \equiv b \pmod{m} &\iff m \mid a-b \iff \exists q \in \mathbb{Z} : a - b = qm \\ &\iff \exists q \in \mathbb{Z} : ac - bc = qmc \iff mc \mid ac - bc \\ &\iff ac \equiv bc \pmod{mc}. \end{aligned}$$

5. Wegen $c \equiv c \pmod{m}$ folgt auch ohne die zusätzliche Einschränkung bzgl. des gcd aus der Multiplikativität in (2) die Relation $ac \equiv bc \pmod{m}$.

   Sei nun $ac \equiv bc \pmod{m}$ und $\gcd(c, m) = 1$. Als Folge der Identität von Bézout gibt es ganze Zahlen $q, c' \in \mathbb{Z}$ mit $qm + cc' = 1$, woraus $cc' \equiv 1 \pmod{m}$ folgt. Multiplizieren wir beide Seiten der Ausgangskongruenz mit c', so erhalten wir

$$a \underbrace{cc'}_{\equiv 1} \equiv b \underbrace{cc'}_{\equiv 1} \pmod{m},$$

   womit $a \equiv b \pmod{m}$ gelten muss.

□

Beispiel 4.27 (Teilbarkeitsregeln): Mit den Rechenregeln für Kongruenzen lassen sich einige der üblichen Teilbarkeitsregeln recht mühelos beweisen. Für eine Zahl mit Ziffern (von links nach rechts) $a_\ell, a_{\ell-1}, ..., a_2, a_1, a_0 \in \{0, ..., 9\}$ schreiben wir $(a_\ell a_{\ell-1} ... a_1 a_0)_{10} = a_\ell \cdot 10^\ell + a_{\ell-1} \cdot 10^{\ell-1} + ... + a_1 \cdot 10^1 + a_0$.

Teilbarkeit durch 2. Eine Zahl ist genau dann durch 2 teilbar, wenn $2 \mid (a_\ell ... a_0)_{10}$, also wenn $(a_\ell ... a_0)_{10} \equiv 0 \pmod{2}$. Da $10 \equiv 0 \pmod{2}$, und damit auch $10^j \equiv 0^j = 0 \pmod{2}$ für alle $j \geq 1$ können wir die Kongruenz wie folgt umformen:

$$a_\ell \cdot \underbrace{10^\ell}_{\equiv 0} + a_{\ell-1} \cdot \underbrace{10^{\ell-1}}_{\equiv 0} + ... + a_1 \cdot \underbrace{10}_{\equiv 0} + a_0 \equiv 0 \pmod{2} \iff a_0 \equiv 2 \pmod{2}.$$

Die letzte Kongruenz ist dabei wieder zu $2 \mid a_0$ äquivalent. In anderen Worten, eine Zahl ist genau dann durch 2 teilbar, wenn ihre Einerziffer durch 2 teilbar ist.

Teilbarkeit durch 9. Analog zu oben, diesmal gilt jedoch $10 \equiv 1 \pmod{9}$, und damit $10^j \equiv 1^j = 1 \pmod{9}$ für alle $j \geq 1$. Es ergibt sich

$$9 \mid (a_\ell ... a_0)_{10} \iff a_\ell + a_{\ell-1} + ... + a_1 + a_0 \equiv 0 \pmod{9},$$

eine Zahl ist also genau dann durch 9 teilbar, wenn ihre Ziffernsumme durch 9 teilbar ist.

Da auch für 3 die Relation $10^j \equiv 1 \pmod{3}$ erfüllt ist, gilt die gleiche Beobachtung auch für die Teilbarkeit durch 3.

Teilbarkeit durch 11. Bei der Teilbarkeit von 11 können wir uns zunutze machen, dass $10 \equiv -1 \pmod{11}$, und damit $10^j \equiv (-1)^j \pmod{11}$ gilt. Die zu überprüfende Regel ist in diesem Fall also

$$11 \mid (a_\ell ... a_0)_{10} \iff a_\ell \cdot (-1)^\ell + a_{\ell-1} \cdot (-1)^{\ell-1} + ... + a_2 - a_1 + a_0 \equiv 0 \,(\mathrm{mod}\, 11).$$

Teilbarkeit durch 11 liegt dann vor, wenn die alternierende Ziffernsumme durch 11 teilbar ist.

⬠

Wenden wir uns jetzt der Frage zu, wann Kongruenzgleichungen der Form $ax \equiv b \,(\mathrm{mod}\, m)$ für gegebene ganze Zahlen $a, b, m \in \mathbb{Z}$ eine Lösung $x \in \mathbb{Z}$ besitzen. Betrachten wir dafür zunächst den Spezialfall $b = 1$.

Proposition 4.28: Seien $a, m \in \mathbb{Z}$ mit $\gcd(a, m) = 1$. Dann gibt es ein $x \in \mathbb{Z}$ mit

$$ax \equiv 1 \,(\mathrm{mod}\, m),$$

den sogenannten *inversen Rest zu a modulo m*.

Beweis: Nach der Identität von Bézout gibt es wegen $\gcd(a, m) = 1$ ganze Zahlen $x, y \in \mathbb{Z}$ mit $ax + my = 1$. Nehmen wir diese Gleichung modulo m, so erhalten wir $ax + my \equiv 1 \,(\mathrm{mod}\, m)$, was wegen $m \equiv 0 \,(\mathrm{mod}\, m)$ äquivalent zu $ax \equiv 1 \,(\mathrm{mod}\, m)$ ist. □

Beispiel 4.29: Wir lösen die Gleichung $4x \equiv 1 \,(\mathrm{mod}\, 29)$, berechnen also den inversen Rest von 4 modulo 29. Eine Anwendung des erweiterten Euklid'schen Algorithmus liefert die Identität $(-7) \cdot 4 + 1 \cdot 29 = 1$, der gesuchte inverse Rest ist also $-7 \equiv 22 \,(\mathrm{mod}\, 29)$: wie gewünscht ist $22 \cdot 4 = 88 \equiv 1 \,(\mathrm{mod}\, 29)$. ✓ ⬠

Satz 4.30 (Lösung von linearen Kongruenzen): Seien $a, b, m \in \mathbb{Z}$ mit $m \neq 0$ und $d = \gcd(a, m)$. Dann ist die Kongruenz

$$ax \equiv b \,(\mathrm{mod}\, m)$$

genau dann lösbar, wenn $d \mid b$. In diesem Fall gibt es genau d verschiedene Lösungen modulo m.

Beweis: Wir müssen beide Richtungen der Äquivalenzaussage beweisen.

„⇒" Sei die gegebene Kongruenz lösbar, wir haben also ein $x \in \mathbb{Z}$ mit $m \mid (ax - b)$. Es gibt daher ein $y \in \mathbb{Z}$ für welches $my = ax - b$, bzw. äquivalent dazu $b = ax - my$ gilt. Da $d = \gcd(a, m)$ ist, teilt d sowohl ax als auch my, und damit auch die Differenz $ax - my = b$ – es ist $d \mid b$.

„⇐" Wähle $a', b', m' \in \mathbb{Z}$ so, dass $a = da'$, $b = db'$ und $m = dm'$. Der größte gemeinsame Teiler der „durchgekürzten" Zahlen a' und m' ist jetzt $\gcd(a', m') = 1$. Nach den Rechenregeln für Kongruenzen ist $ax \equiv b \,(\mathrm{mod}\, m)$ jetzt äquivalent zu

$$a'x \equiv b' \,(\mathrm{mod}\, m').$$

Wegen $\gcd(a', m') = 1$ gibt es einen inversen Rest a'' von a' modulo m'. Eine Lösung der reduzierten (und so auch der ursprünglichen) Kongruenz ist dann $x = b'a''$. Ein Wert y ist genau dann eine weitere Lösung, wenn $a'y \equiv b' \pmod{m'}$, bzw.

$$a'x \equiv a'y \pmod{m'}.$$

Multiplizieren wir diese Kongruenz mit a'', so erhalten wir

$$x \equiv y \pmod{m'}.$$

Wegen $m = dm'$ sind die Reste

$$x, x + m', x + 2m', x + 3m', ..., x + (d-2)m', x + (d-1)m'$$

alle verschieden modulo m und zugleich aber kongruent zu x modulo m' – das sind genau d verschiedene Lösungen der Kongruenz.

□

Während wir die Lage für eine einzelne lineare Kongruenzgleichung mittlerweile gut beschreiben können, ist noch unklar, wie die Situation bei Kongruenzgleichungssystemen ausschaut. Zur Motivation geben wir hier ein Rätsel von Brahmagupta[15] wieder:

„An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?"

Gesucht wird also nach der kleinsten positiven Lösung x, welche jede der Kongruenzgleichungen

$$x \equiv 1 \pmod{2} \quad x \equiv 1 \pmod{3} \quad x \equiv 1 \pmod{4}$$
$$x \equiv 1 \pmod{5} \quad x \equiv 1 \pmod{6} \quad x \equiv 0 \pmod{7}$$

erfüllt. Der folgende Satz liefert uns einen Ansatz für derartige Systeme.

Satz 4.31 (Chinesischer Restsatz[16]): Seien $m_1, ..., m_r \in \mathbb{Z}$ paarweise teilerfremd (also $\gcd(m_i, m_j) = 1$ für $1 \leq i < j \leq r$), und seien $b_1, ..., b_r \in \mathbb{Z}$. Dann gibt es genau ein $x \in \mathbb{Z}$ (modulo $m_1 \cdots m_r$) welches

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \quad ..., \quad x \equiv b_r \pmod{m_r}$$

erfüllt.

[15] Indischer Mathematiker, geboren im Jahr 598.

[16] Die originale Formulierung des Satzes stammt aus dem Buch 孫子算經 / 孙子算经 *(„Sun Zis Handbuch der Arithmetik")* des chinesischen Mathematikers Sun Zi (vmtl. 3. Jh.)

Beweis: Wir zeigen zunächst die Existenz einer Lösung mittels vollständiger Induktion nach der Anzahl von Gleichungen r, und kümmern uns im zweiten Schritt um die Eindeutigkeit der Lösung.

Existenz. *Induktionsanfang.* Für $r = 1$ ist nichts zu tun, betrachten wir also $r = 2$. Wir haben

$$x \equiv b_1 \,(\mathrm{mod}\, m_1) \quad \Longleftrightarrow \quad \exists y \in \mathbb{Z} : x = b_1 + y m_1.$$

Für ein x, das auch die zweite Kongruenzgleichung erfüllt, muss also $x = b_1 + y m_1 \equiv b_2 \,(\mathrm{mod}\, m_2) \quad \Longleftrightarrow \quad y m_1 \equiv (b_2 - b_1) \,(\mathrm{mod}\, m_2)$ gelten. Wegen $\gcd(m_1, m_2) = 1$ und $1 \mid (b_2 - b_1)$ ist es möglich, dank Satz 4.30 ein passendes y zu finden – die Kongruenzen sind also lösbar.

Induktionsschluss. Wir nehmen an, dass das System

$$x \equiv b_1 \,(\mathrm{mod}\, m_1), \quad \ldots, \quad x \equiv b_{r-1} \,(\mathrm{mod}\, m_{r-1})$$

eine Lösung $c \in \mathbb{Z}$ besitzt. Offenbar erfüllt dann auch jedes x mit $x \equiv c \,(\mathrm{mod}\, m_1 \cdots m_{r-1})$ die Eigenschaft $x \equiv c \equiv b_j \,(\mathrm{mod}\, m_j)$ für $1 \leq j < r$. Wenn wir nun noch eine weitere Gleichung, $x \equiv b_r \,(\mathrm{mod}\, m_r)$, erfüllt haben wollen, so ist effektiv das System

$$x \equiv c \,(\mathrm{mod}\, m_1 \cdots m_{r-1})$$
$$x \equiv b_r \,(\mathrm{mod}\, m_r)$$

zu lösen. Da $\gcd(m_1 \cdots m_{r-1}, m_r) = 1$ können wir dazu so wie im Induktionsanfang vorgehen, eine passende Lösung x existiert also.

Eindeutigkeit. Seien nun $y, y' \in \mathbb{Z}$ zwei Lösungen des Systems

$$x \equiv b_1 \,(\mathrm{mod}\, m_1), \quad \ldots, \quad x \equiv b_r \,(\mathrm{mod}\, m_r).$$

Damit ist aber

$$y \equiv y' \,(\mathrm{mod}\, m_j) \quad \Longleftrightarrow \quad m_j \mid (y - y')$$

für alle $1 \leq j \leq r$; insbesondere ist $y - y'$ also ein gemeinsames Vielfaches von allen $m_1, m_2, \ldots, m_r$. Da die gegebenen Moduln paarweise teilerfremd sind, ist das kleinste gemeinsame Vielfache durch deren Produkt gegeben; es muss also

$$m_1 \cdots m_r \mid (y - y')$$

und damit $y \equiv y' \,(\mathrm{mod}\, m_1 \cdots m_r)$ sein.

□

Während in Satz 4.31 keine explizite Formel für die Lösung x des Kongruenzsystems angegeben ist, wird im Existenzbeweis demonstriert, wie die Lösung (schrittweise) konstruiert werden kann. Wir untersuchen in den folgenden Beispielen, wie dieses Verfahren konkret aussieht.

Beispiel 4.32: Wir betrachten das Kongruenzsystem

$$x \equiv 1 \,(\mathrm{mod}\, 5), \quad x \equiv 5 \,(\mathrm{mod}\, 9), \quad x \equiv 7 \,(\mathrm{mod}\, 13),$$

und beobachten, dass alle Voraussetzungen des Chinesischen Restsatzes (Teilerfremdheit der Moduln) erfüllt sind. Um das System zu lösen gehen wir wie im Beweis von Satz 4.31 vor und konzentrieren und zunächst auf die ersten beiden Gleichungen. Für ein geeignetes $y \in \mathbb{Z}$ können wir jedes x, das die erste Gleichung erfüllt als $x = 1 + 5y$ schreiben. Eingesetzt in die zweite Kongruenz (und umgeformt) liefert uns das

$$5y \equiv 5 - 1 = 4 \pmod 9.$$

Um diese lineare Kongruenz zu lösen, brauchen wir den inversen Rest von 5 modulo 9. Mit dem erweiterten Euklid'schen Algorithmus (oder direkt durch Ausprobieren) finden wir $5 \cdot 2 \equiv 1 \pmod 9$, der gesuchte inverse Rest ist also 2. Multiplizieren wir die Kongruenz in y erhalten wir

$$y \equiv 8 \pmod 9,$$

das gesuchte y lässt sich damit als $y = 8 + 9z$ für geeignetes $z \in \mathbb{Z}$ schreiben. Setzen wir diese Darstellung in die Gleichung für x ein, so erhalten wir $x = 1 + 5 \cdot (8 + 9z) = 41 + 45z$ als Lösung der ersten beiden Gleichungen.

Wir wiederholen diesen Ansatz nun auch für die dritte Gleichung; Einsetzen von x liefert die lineare Kongruenz

$$41 + 45z \equiv 7 \pmod{13} \quad \iff \quad 6z \equiv 5 \pmod{13},$$

der inverse Rest von 6 modulo 13 ist (wegen $6 \cdot 11 = 66 = 5 \cdot 13 + 1$) genau 11. Daher erhalten wir $z \equiv 3 \pmod{13}$, bzw. $z = 3 + 13t$ für geeignetes $t \in \mathbb{Z}$. Rückeinsetzen liefert nun die gesuchte Lösung für unser gesamtes Kongruenzsystem, nämlich

$$x = 41 + 45 \cdot (3 + 13t) = 176 + 585t,$$

bzw. erfüllt also jedes $x \equiv 176 \pmod{585}$ das System.

In SageMath lässt sich der Chinesische Restsatz mit dem Befehl `crt` *(„Chinese Remainder Theorem")* anwenden; dazu sind die Reste b_j bzw. die Moduln m_j einfach in zwei Listen zu übergeben:

```
sage: crt([1, 5, 7], [5, 9, 13])
176
```

⬠

Der Chinesische Restsatz, Satz 4.31, setzt voraus, dass die Moduln im Kongruenzsystem paarweise teilerfremd sind – was im allgemeinen eine eher starke Einschränkung ist. Im folgenden Beispiel wollen wir untersuchen, wie wir vorgehen können, wenn diese Voraussetzung nicht erfüllt ist, bzw. was in diesem Fall noch passieren kann.

Beispiel 4.33: Betrachten wir zunächst das System

$$x \equiv 2 \pmod 6, \quad x \equiv 4 \pmod{10}, \quad x \equiv 1 \pmod{15}.$$

Die Moduln sind nicht teilerfremd: $\gcd(6, 10) = 2$, $\gcd(6, 15) = 3$, $\gcd(10, 15) = 5$.

Wir können uns aber die Rechenregeln für Kongruenzen zunutze machen und den Chinesischen Restsatz für einzelne Gleichungen „umdrehen": so ist etwa $x \equiv 2 \pmod 6$ genau dann, wenn sowohl $x \equiv 2 \equiv 0 \pmod 2$ als auch $x \equiv 2 \pmod 3$ erfüllt sind.

Analog können wir die anderen Gleichungen im System aufspalten: es ist

$$x \equiv 4 \pmod{10} \quad \iff \quad x \equiv 4 \equiv 0 \pmod{2} \wedge x \equiv 4 \pmod{5}$$

und

$$x \equiv 1 \pmod{15} \quad \iff \quad x \equiv 1 \pmod{3} \wedge x \equiv 1 \pmod{5}.$$

Im entstandenen System gibt es nun aber Kongruenzen, die einander widersprechen: es gibt kein $x \in \mathbb{Z}$, welches zugleich $x \equiv 4 \pmod{5}$ (aus der zweiten Gleichung) und $x \equiv 1 \pmod{5}$ (aus der dritten Gleichung) erfüllt; das System hat keine Lösung.

Mit dieser Beobachtung können wir nun auch das motivierende Beispiel von Brahmagupta mit den zerbrochenen Eiern lösen: das initiale System

$$x \equiv 1 \pmod{2} \quad x \equiv 1 \pmod{3} \quad x \equiv 1 \pmod{4}$$
$$x \equiv 1 \pmod{5} \quad x \equiv 1 \pmod{6} \quad x \equiv 0 \pmod{7}$$

lässt sich durch Aufspalten der Kongruenzen auf das System

$$x \equiv 1 \pmod{3}, \quad x \equiv 1 \pmod{4}, \quad x \equiv 1 \pmod{5}, \quad x \equiv 0 \pmod{7}$$

reduzieren, für welches wir den Chinesischen Restsatz direkt anwenden können. Die Lösung ist durch $x \equiv 301 \pmod{420}$ gegeben, der Reiter muss der alten Frau also mindestens 301 Eier ersetzen. ⬠

4.4 Potenzreste und die Euler'sche φ-Funktion

Ein modernes Anwendungsgebiet der Zahlentheorie ist die Kryptologie. Mehrere wichtige Verfahren zur sicheren Kommunikation basieren dabei auf dem Verhalten von Potenzresten, also Funktionen der Bauart $k \mapsto a^k \pmod{m}$ für gegebene $a, m \in \mathbb{Z}$. In diesem Abschnitt wollen wir die mathematischen Grundlagen für das RSA-Verfahren, ein weit verbreitetes *asymmetrisches Kryptosystem* kennenlernen.

Bei *symmetrischen* Kryptosystemen wird zwischen zwei Kommunikationspartnern der gleiche Schlüssel für die Ver- und Entschlüsselung verwendet. Diese Verfahren (wie zB das AES-Verfahren) sind üblicherweise sehr effizient und erlauben einen hohen Datendurchsatz – haben aber das Problem, dass zunächst ein passender Schlüssel ausgetauscht werden muss. Hierfür werden oft asymmetrische Kryptosysteme wie das RSA-Verfahren eingesetzt: die Kommunikationspartner besitzen hier üblicherweise einen *öffentlichen Schlüssel* (den andere verwenden können, um Nachrichten für die Besitzer:in des Schlüssels zu verschlüsseln), und einen *privaten Schlüssel*, der zur Entschlüsselung verwendet werden kann.

Eine zahlentheoretische Funktion, die in dem Zusammenhang eine wichtige Rolle spielt, ist die Euler'sche φ-Funktion.

Definition 4.34: Für $n \in \mathbb{Z}_{>0}$ ist die Euler'sche φ-Funktion durch

$$\varphi(n) := |\{k \in [n] : \gcd(k, n) = 1\}|,$$

also durch die Anzahl der positiven ganzen Zahlen von 1 bis n die zu n teilerfremd sind, gegeben.

Es ist beispielsweise $\varphi(12) = |\{1, 5, 7, 11\}| = 4$, $\varphi(1) = 1$, und da für jede Primzahl p alle Zahlen von 1 bis $p-1$ teilerfremd zu p sind gilt insbesondere $\varphi(p) = p - 1$.

Satz 4.35: Die Euler'sche φ-Funktion ist multiplikativ, d.h., für positive $m, n \in \mathbb{Z}_{>0}$ mit $\gcd(m, n) = 1$ gilt $\varphi(mn) = \varphi(m)\varphi(n)$. Konkret gilt für eine positive ganze Zahl $n \in \mathbb{Z}$ mit Primfaktorzerlegung $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, dass

$$\varphi(n) = \prod_{j=1}^{r} (p_j - 1) p_j^{\alpha_j - 1} = n \cdot \prod_{j=1}^{r} \left(1 - \frac{1}{p_j}\right).$$

Beweis: Hier ohne Beweis. □

Satz 4.36 (Satz von Euler–Fermat): Sei $a \in \mathbb{Z}$ und $n \in \mathbb{Z}_{>0}$ mit $\gcd(a, n) = 1$. Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Beweis: Seien $x_1, x_2, \ldots, x_{\varphi(n)}$ genau die $\varphi(n)$ verschiedenen zu n teilerfremden Zahlen von 1 bis n, und sei $a \in \mathbb{Z}$ beliebig mit $\gcd(a, n) = 1$. Betrachte die Zahlen $y_j \in [0, n-1]$

$$y_j \equiv a x_j \pmod{n}$$

für $1 \leq j \leq \varphi(n)$. Dann gilt einerseits $\gcd(y_j, n) = 1$ (da sowohl x_j als auch a zu n teilerfremd sind), zugleich müssen die y_j aber auch alle verschieden sein: wäre für $i \neq j$ etwa $y_i = y_j$, so müsste $a x_i \equiv a x_j \pmod{n}$ sein, wobei wir wegen $\gcd(a, n) = 1$ den gemeinsamen Faktor a aus dieser Kongruenz kürzen dürften und so bei $x_i \equiv x_j \pmod{n}$ landen – was wegen $i \neq j$ aber nicht möglich ist.

Daher muss $\{x_1, \ldots, x_{\varphi(n)}\} = \{y_1, \ldots, y_{\varphi(n)}\}$ (nur in anderer Reihenfolge) sein. Das bedeutet, es muss

$$x_1 x_2 \cdots x_{\varphi(n)} \equiv y_1 y_2 \cdots y_{\varphi(n)} \pmod{n},$$

und nach Definition der y_j in Folge

$$x_1 x_2 \cdots x_{\varphi(n)} \equiv a x_1 \cdot a x_2 \cdots a x_{\varphi(n)} \equiv a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \pmod{n}$$

sein. Da die x_j alle zu n teilerfremd sind, können wir diese Kongruenz jetzt einfach mit den ganzen inversen Resten zu $x_1, \ldots, x_{\varphi(n)}$ multiplizieren und erhalten so

$$1 \equiv a^{\varphi(n)} \pmod{n},$$

wie behauptet. □

Beispiel 4.37: Satz 4.36 kann praktisch etwa dazu verwendet werden, Ziffern von großen Ganzzahlpotenzen zu berechnen. Wollen wir etwa die Einerziffer von $7^{8^{9^{10}}}$ im Dezimalsystem berechnen, so suchen wir effektiv nach der Lösung von

$$7^{8^{9^{10}}} \equiv x \,(\mathrm{mod}\, 10).$$

Wegen $\gcd(7, 10) = 1$ wissen wir, dass $7^{\varphi(10)} \equiv 1 \,(\mathrm{mod}\, 10)$ ist, wobei $\varphi(10) = 4$. Wir können den Exponenten daher um ein geeignetes Vielfaches von 4 reduzieren:

$$7^{8^{9^{10}}} = 7^{4r+t} = \underbrace{\left(7^4\right)^r}_{\equiv 1} \cdot 7^t \equiv 7^t \,(\mathrm{mod}\, 10),$$

für geeignete $r, t \in \mathbb{Z}$. Dabei erfüllt t genau die Kongruenz

$$8^{9^{10}} \equiv t \,(\mathrm{mod}\, 4),$$

wobei die linke Seite offenbar ein Vielfaches von 4 ist, t also kongruent zu 0 modulo 4 ist. Die gesuchte Einerziffer erfüllt daher $x \equiv 7^0 = 1 \,(\mathrm{mod}\, 10)$. ⬠

Korollar 4.38 (Kleiner Satz von Fermat): Sei $p \in \mathbb{Z}_{>0}$ eine Primzahl und $a \in \mathbb{Z}$. Dann gilt

$$a^p \equiv a \,(\mathrm{mod}\, p).$$

Beweis: Der kleine Satz von Fermat folgt direkt aus dem Satz von Euler–Fermat: falls $\gcd(a, p) = 1$, so ist wegen $\varphi(p) = p - 1$ und Satz 4.36

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p),$$

woraus nach Multiplikation mit a die Behauptung folgt. Sind a und p nicht teilerfremd, so muss p ein Teiler von a, also $a \equiv 0 \,(\mathrm{mod}\, p)$ sein; in diesem Fall gilt $a^p \equiv a \equiv 0 \,(\mathrm{mod}\, p)$. □