Diskrete Algebraische Strukturen

Markus Junker
Mathematisches Institut
Albert–Ludwigs–Universität Freiburg

Sommersemester 2010

Inhaltsverzeichnis

Teil I: Endliche Kombinatorik

I.1 Mengen, Abbildungen, Partitionen

Voraussetzungen dieser Vorlesung sind Kenntnisse einer einführenden Mathematik–Vorlesung, insbesondere:

- mathematische Grundbegriffe und Formelschreibweise
- „naive Mengenlehre“ (im Gegensatz zur axiomatischen Mengenlehre)
- „naives“ Verständnis der natürlichen Zahlen samt dem Beweisprinzip der vollständigen Induktion (in allen Varianten)

Ich verwende folgende nicht völlig standardisierte Schreib– und Sprechweisen:

$\mathbb{N}$	:	die Menge $\{0, 1, 2, 3, \dots\}$
$A \subseteq M$	:	A ist Teilmenge von M
$A \subset M$	:	A ist echte Teilmenge von M
$M = M_1 \cup M_2$	:	M ist disjunkte Vereinigung von M_1 und M_2
$M = \bigcup_{i \in I} M_i$	:	M ist die disjunkte Vereinigung der Mengen M_i für $i \in I$
$\lvert M \rvert$	:	die Anzahl der Elemente von M, auch *Mächtigkeit* von M genannt (entweder ein Element von $\mathbb{N}$ oder ∞)
$\mathfrak{P}(M)$	:	Potenzmenge von M
$\square$	:	Beweisende
n-Menge	:	eine Menge mit n-Elementen
n-Teilmenge	:	eine n-elementige Teilmenge

Einige Konventionen:

Damit Formeln auch für Extremfälle gelten (was bei Rekursionen wichtig sein kann), braucht man einige Konventionen, die insbesondere die leere Menge bzw. das Rechnen mit 0 betreffen. Man kann diese Extremfälle in der Regel auch übergehen, muss dann aber bei Beweisen und Berechnungen gegebenenfalls mit höheren Anfangswerten starten.

Eine „*leere Vereinigung*“ (also eine Vereinigung über eine leere Indexmenge) ist die leere Menge; ein leeres Mengenprodukt ist die Menge $\{\emptyset\}$, also die Menge, welche als einziges Element die leere Menge enthält. Entsprechend hat die leere Summe den Wert 0 und das leere Produkt (von Zahlen) den Wert 1. Es gibt keine Abbildung einer nicht-leeren Menge in die leere Menge und genau eine Abbildung der leeren Menge in eine andere Menge (die im Falle der Abbildung von $\emptyset$ nach $\emptyset$ bijektiv ist). Insbesondere gilt $0^0 = 0! = 1$.

Mengen

In diesem Unterabschnitt sei nun stets M eine $\mathfrak{m}$-Menge und N eine $\mathfrak{n}$-Menge, und alle betrachteten Mengen seien endlich.

Satz 1.1 (Additive Mächtigkeitsregeln)

(a) *Angenommen* $M \subseteq N$.
Dann gilt $\mathfrak{m} \leqslant \mathfrak{n}$ *und* $|N \setminus M| = \mathfrak{n} - \mathfrak{m}$. *Außerdem ist genau dann* $\mathfrak{m} < \mathfrak{n}$ *wenn* $M \subset N$.

(b) *Es gilt*

$$\begin{aligned} \max\{\mathfrak{m},\mathfrak{n}\} &\leqslant |M \cup N| \leqslant \mathfrak{n}+\mathfrak{m} \\ 0 &\leqslant |M \cap N| \leqslant \min\{\mathfrak{m},\mathfrak{n}\} \end{aligned}$$

mit den Extremfällen

$$\begin{aligned} |M \cup N| = \mathfrak{n}+\mathfrak{m} &\iff M \text{ und } N \text{ sind disjunkt} \iff |M \cap N| = 0 \\ |M \cup N| = \max\{\mathfrak{m},\mathfrak{n}\} &\iff (M \subseteq N \text{ oder } N \subseteq M) \iff |M \cap N| = \min\{\mathfrak{m},\mathfrak{n}\} \end{aligned}$$

und dem allgemeinen Zusammenhang

$$|M| + |N| = |M \cup N| + |M \cap N|$$

(c) *Allgemeiner gilt* $\left|\dot{\bigcup_{i=0}^{k}} M_i\right| = \sum_{i=0}^{k} |M_i|$.

Beweis: (a) und die erste Hälfte von (b) sind offensichtliche Regeln, die der Funktionsweise der natürlichen Zahlen zugrundeliegen. Beweisen könnte man diese nur in einer axiomatischen Theorie der Mengen und Zahlen.

Die Regel für disjunkte Mengen erlaubt es, den letzten Teil von (b) auf die Beobachtungen $M \cup N = M \cup (N \setminus M)$ und $N = (N \setminus M) \cup (M \cap N)$ zurückzuführen.

(c) folgt mit Induktion. □

Den „allgemeinen Zusammenhang“ kann man per Induktion ebenfalls verallgemeinern zu dem folgenden Satz:

Satz 1.2 (Inklusion–Exklusions–Prinzip oder auch Sylvestersche Siebformel)
Seien $M_1, \ldots, M_k$ *endliche Mengen. Dann gilt:*

$$\left|M_1 \cup \cdots \cup M_k\right| = \sum_{\emptyset \neq I \subseteq \{1,\ldots,k\}} (-1)^{|I|+1} \cdot \left|\bigcap_{i \in I} M_i\right|$$

Beweis: Beweis durch Induktion nach k:
Für $k = 1$ ist die Formel trivialerweise richtig und für $k = 2$ stimmt sie nach Satz 1.1 (b). Für $k > 2$ gilt dann:

$$\begin{aligned} \left|M_1 \cup \cdots \cup M_k\right| &= \left|M_1 \cup \cdots \cup M_{k-1}\right| + \left|M_k\right| - \left|(M_1 \cup \cdots \cup M_{k-1}) \cap M_k\right| \\ &= \left|M_1 \cup \cdots \cup M_{k-1}\right| + \left|M_k\right| - \left|(M_1 \cap M_k) \cup \cdots \cup (M_{k-1} \cap M_k)\right| \\ &= \sum_{\emptyset \neq I \subseteq \{1,\ldots,k-1\}} (-1)^{|I|+1} \cdot \left|\bigcap_{i \in I} M_i\right| + \left|M_k\right| - \sum_{\emptyset \neq I \subseteq \{1,\ldots,k-1\}} (-1)^{|I|+1} \cdot \left|\bigcap_{i \in I} (M_i \cap M_k)\right| \\ &= \sum_{\emptyset \neq I \subseteq \{1,\ldots,k\}} (-1)^{|I|+1} \cdot \left|\bigcap_{i \in I} M_i\right| \end{aligned}$$

Die erste Gleichheit benutzt den Fall $k = 2$, die dritte Gleichheit die Induktionsvoraussetzung. Für die letzte Gleichheit muss man prüfen, dass alle nicht-leeren Teilmengen von $\{1, \ldots, k\}$ in der vorletzten Zeile genau einmal und mit dem richtigen Vorzeichen vorkommen. □

Zwei Bemerkungen zur Formel: Zum einen kann man sich anhand der Konventionen überzeugen, dass die Formel auch für $k = 0$ gilt. Zum andern kann man in diesem Zusammenhang $\bigcap_{i\in\emptyset} M_i = M_1 \cup \cdots \cup M_k$ setzen (eine sinnvolle und übliche Konvention, wenn man in der Booleschen Algebra $\mathfrak{P}(M_1 \cup \cdots \cup M_k)$ arbeitet). Dann ergibt sich die einprägsamere Formel:

$$\sum_{I\subseteq\{1,\ldots,k\}} (-1)^{|I|} \cdot \Big|\bigcap_{i\in I} M_i\Big| \;=\; 0$$

Satz 1.3 (Multiplikative Mächtigkeitsregeln)

(a) *Es gilt* $|M \times N| = mn$ *und allgemeiner* $|M_1 \times \cdots \times M_k| = |M_1| \cdot \ldots \cdot |M_k|$.

(b) *Insbesondere gilt* $|M^k| = m^k$, *wobei* $M^k := \underbrace{M \times \cdots \times M}_{k \text{ mal}}$, *also* $M^1 = M$ *und* $M^0 = \{\emptyset\}$.

Beweis: $M \times N = \bigcup_{x\in M} \{x\} \times N$ und jede Menge $\{x\} \times N$ enthält offenbar n Elemente. Der Rest folgt mit Induktion über k. □

Abbildungen

Eine Abbildung (oder auch Funktion) $f : M \to N$ heißt

injektiv, falls $f(x) \neq f(x')$ für alle $x, x' \in M$ mit $x \neq x'$;
surjektiv, falls es zu jedem $y \in N$ ein $x \in M$ mit $f(x) = y$ gibt;
bijektiv, falls f injektiv und surjektiv ist.

Der Kürze halber benutze ich folgende Schreibweisen (kein Standard!):

$$\left.\begin{array}{l}\mathrm{Abb}(M,N)\\ \mathrm{Inj}(M,N)\\ \mathrm{Surj}(M,N)\\ \mathrm{Bij}(M,N)\end{array}\right\} \text{ sei die Menge aller } \left\{\begin{array}{l}\text{Abbildungen}\\ \text{Injektionen}\\ \text{Surjektionen}\\ \text{Bijektionen}\end{array}\right\} f : M \to N$$

Die Menge aller Abbildungen $\mathrm{Abb}(M, N)$ wird oft mit ${}^M N$ (oder auch N^M) bezeichnet.

Eine bijektive Abbildung ordnet jedem Element des Definitionsbereiches genau ein Element des Wertebereiches zu, und erreicht jedes Element der Wertebereiches. Bijektive Abbildungen erhalten also den intuitiven Anzahlbegriff. (Es ist sogar eher umgekehrt, dass man die Zahlen als so konstruiert verstehen kann, dass sie unter bijektiven Abbildungen erhalten bleiben.)

Eine beliebige Abbildung $f : M \to N$ setzt sich zusammen aus drei Teilinformationen:

- einer Äquivalenzrelation auf M (nämlich: zwei Elemente sind äquivalent, wenn sie dasselbe Bild unter f haben);
- einer Teilmenge von N (nämlich dem Bild von f);
- und einer Bijektion zwischen den Äquivalenzklassen und dem Bild von f.

Eine Abbildung $f : M \to N$ ist daher genau dann injektiv, wenn die Einschränkung von f im Wertebereich $M \to \text{Bild}(f)$ eine Bijektion zwischen M und der Teilmenge $\text{Bild}(f)$ von N ist.

Eine Abbildung $f : M \to N$ ist daher genau dann surjektiv, wenn es eine Teilmenge $M' \subseteq M$ gibt, so dass die Einschränkung von f im Definitionsbereich $M' \to N$ eine Bijektion ist (M' hat aus jeder Äquivalenzklasse genau ein Element).

Aus diesen Betrachtungen ergibt sich folgendes Ergebnis:

Satz 1.4 *Sei wie bisher M eine m-Menge, N eine n-Menge und $f : M \to N$ gegeben.*

(a) *Ist f bijektiv, so gilt* $m = n$
surjektiv $m \geqslant n$
injektiv $m \leqslant n$

(b) *Ist $m = n$ und f injektiv oder surjektiv, so ist f bereits bijektiv.*

Für unendliche Mengen gibt es Injektionen und Surjektionen, die keine Bijektionen sind, z.B. ist die Abbildung $n \mapsto 2n$ eine injektive, aber nicht surjektive Abbildung $\mathbb{N} \to \mathbb{N}$.

Aus den Überlegungen bzw. aus Satz 1.4 den ergeben sich zwei nützliche Abzählprinzipien:

Das Prinzip des doppelten Abzählens:

„Wenn man eine Menge auf zwei verschiedene Arten abzählt, kommt das gleiche Ergebnis heraus."

Die Gültigkeit des Prinzips ist natürlich eine Trivialität; seine Nützlichkeit ergibt sich dann, wenn man zwei verschiedene, aber aussagekräftige Arten des Abzählens findet. Angewandt wird es oft in folgender Situation: Ist $R \subseteq X \times Y$, so gilt

$$\sum_{x \in X} \Big|\{y \in Y \mid (x,y) \in R\}\Big| \;=\; \sum_{y \in Y} \Big|\{x \in X \mid (x,y) \in R\}\Big|.$$

In vielen Anwendungen wird durch geschickte Wahl von R eine Beziehung zwischen X und Y hergestellt. Hat man z.B. einen durch Dreiecke begrenzten räumlichen Körper, so folgt aus dem Prinzip die Beziehung $3f = 2k$ für die Anzahl k der Kanten und die Anzahl f der Seitenflächen, indem man für R die Menge der Paare (x, y) von Kanten und Flächen wählt, bei denen x eine Seite von y ist.

Das Schubfachprinzip:

„Wenn man die Elemente einer Menge in Schubfächer verteilt und weniger Schubfächer als Elemente hat, dann gibt es ein Schubfach mit mehr als einem Element."

Dieses Prinzip kann man verallgemeinern. Dazu definiert man für eine reelle Zahl r

— die *obere Gaussklammer* $\lceil r \rceil$ als die kleinste ganze Zahl, die nicht kleiner als r ist und
— die *untere Gaussklammer* $\lfloor r \rfloor$ als die größte ganze Zahl, die nicht größer als r ist.

Zum Beispiel ist also $\lceil \pi \rceil = 4$, $\lfloor \pi \rfloor = 3$, $\lceil -\pi \rceil = -3$, $\lfloor -\pi \rfloor = -4$ und $\lceil 2 \rceil = \lfloor 2 \rfloor = 2$.

Satz 1.5 (verallgemeinertes Schubfachprinzip)
Ist $f : M \to N$ und $k := \left\lceil \frac{m}{n} \right\rceil$, so gibt es eine k-Teilmenge von M, auf der f konstant ist.

BEWEIS: Andernfalls gibt es zu jedem $y \in N$ höchstens $\lceil \frac{m}{n} \rceil - 1$ viele Urbilder; also ist $m \leqslant n \cdot \left(\lceil \frac{m}{n} \rceil - 1 \right) < n \cdot (\frac{m+n}{n} - 1) = m$, dies ist ein Widerspruch! □

Satz 1.6 (Exponentielle Mächtigkeitsregeln)

Es gilt $\left|\mathrm{Abb}(M,N)\right| = n^m$.

Als Spezialfälle erhält man $\left|\mathfrak{P}(M)\right| = 2^m$ *und* $\left|N^k\right| = n^k$.

BEWEIS: Bei einer beliebigen Abbildung $M \to N$ hat man für jedes Element aus M genau n Möglichkeiten, ein Bild zu wählen, also insgesamt n^m Möglichkeiten. (Andere Betrachtungsweise: man kann eine Abbildung mit ihrem Funktionsgraphen identifizieren, der ein Element von $N \times \cdots \times N$ ist, wobei das Produkt über die Elemente von M indiziert ist, also ein m-faches Produkt ist.)

Dann gibt es eine Bijektion zwischen der Potenzmenge von M und der Menge ${}^M\{0,1\}$, indem man jeder Teilmenge ihre *charakteristische Funktion* zuordnet (die den Wert 1 für die Elemente der Teilmenge annimmt und sonst den Wert 0).

Schließlich kann man N^k identifizieren mit der Menge der Abbildungen von einer k-Menge (der Indexmenge) nach N. □

Bemerkung: Nach Konvention gibt es genau eine Abbildung der leeren Menge in eine beliebige Menge, insbesondere auch in die leere Menge selbst, aber keine Abbildung einer nicht-leeren Menge in die leere Menge. Dem entsprechen die Rechenregeln $n^0 = 1$ für alle n und $0^m = 0$ für alle $m > 0$. Damit kann man sich vergewissern, dass auch in den Sonderfällen $M = \emptyset$ bzw. $N = \emptyset$ der Satz stimmt.

Als erstes schwierigeres Abzählungsproblem fragen wir uns nun, wieviele Injektionen, Surjektionen und Bijektionen von M nach N es gibt. Dafür brauchen wir zwei Definitionen, die im Anschluss noch ausführlich behandelt werden:

Definition:

- die Anzahl der k-Teilmengen einer l-Menge wird mit $\binom{l}{k}$ bezeichnet und
- die Anzahl der Äquivalenzrelationen auf einer l-Menge mit k Äquivalenzklassen mit $S_{l,k}$.

Satz 1.7

$$\begin{aligned}
\left|\mathrm{Abb}(M,N)\right| &= n^m \\
\left|\mathrm{Bij}(M,N)\right| &= \begin{cases} n! & \textit{falls} \quad m = n \\ 0 & \textit{sonst} \end{cases} \\
\left|\mathrm{Inj}(M,N)\right| &= n(n-1)\cdots(n-m+1) = m! \cdot \tbinom{n}{m} \\
\left|\mathrm{Surj}(M,N)\right| &= \sum_{i=0}^{n} (-1)^i \tbinom{n}{i} (n-i)^m = n! \cdot S_{m,n}
\end{aligned}$$

BEWEIS: Die Anzahl der allgemeinen Abbildungen haben wir bereits bestimmt. Für die Anzahl der Injektionen wählt man eine Aufzählung von M: für das Bild des ersten Elements hat man n Möglichkeiten, für das Bild des zweiten Elemente dann noch $n-1$ Möglichkeiten, usw. Für $m = n$ liefert dies auch die Formel für die Bijektionen, die es nur zwischen gleichmächtigen

Mengen geben kann. Alternativ ist eine Injektion bestimmt durch ihr Bild – einer von $\binom{n}{m}$ vielen m-Teilmengen von N – und einer von $m!$ vielen Bijektionen zwischen M und dem Bild der Injektion. Die Anzahl der Surjektionen berechnet man mit der Siebformel:

$$\begin{aligned}\big|\mathrm{Surj}(M,N)\big| &= \big|\mathrm{Abb}(M,N)\big| - \Big|\bigcup_{y\in N}\mathrm{Abb}(M,N\setminus\{y\})\Big| \\ &= n^m - \sum_{\emptyset\neq I\subseteq N}(-1)^{|I|+1}\cdot\big|\mathrm{Abb}(M,N\setminus I)\big| \\ &= n^m + \sum_{\emptyset\neq I\subseteq N}(-1)^{|I|}(n-|I|)^m \;=\; \sum_{i=0}^{n}(-1)^i\tbinom{n}{i}(n-i)^m\end{aligned}$$

wobei i in der letzten Umformung die verschiedenen Größen für I durchläuft. Alternativ ist eine Surjektion bestimmt durch eine Äquivalenzrelation auf M und einer Bijektion der n Klassen mit N mit $S_{m,n}$ bzw. $n!$ Möglichkeiten. □

Satz 1.8
$$\begin{aligned} n^m &= \sum_{j=0}^{\min\{m,n\}}\tbinom{n}{j}\cdot j!\cdot S_{m,j} \\ n! &= \sum_{j=0}^{n}(-1)^j\tbinom{n}{j}\cdot(n-j)^n\end{aligned}$$

Bemerkung: In der ersten Formel werden die Summanden für $j > \min\{m,n\}$ alle null; man kann daher die Summe auch weiter laufen lassen.

Beweis: Da jede Abbildung eine Surjektion auf ihr Bild ist, kann man $|\mathrm{Abb}(M,N)|$ auch durch die rechte Seite der ersten Formel berechnen: j durchläuft mögliche Größe der Bildes, das weder größer als n noch größer als m sein kann; $\binom{n}{j}$ steht für die Anzahl der Möglichkeiten, ein Bild der Größe j zu wählen; es folgt die Anzahl der Surjektionen auf eine j-Menge.

Die zweite Formel bestimmt rechts die Anzahl der Surjektionen von N nach N; dies ist aber nach Satz 1.4 (b) gleich der Anzahl der Bijektionen von N. □

In diesem Kapitel über Kombinatorik wird es noch oft darum gehen, eine Menge mathematischer Objekte zu zählen. Aus den bisherigen Regeln begründet sich ein dabei meist angewandtes Verfahren: Es wird zunächst eine Bijektion konstruiert zwischen der zu zählenden Menge und einer Menge von Objekten, die man kombinatorisch bereits bestimmen kann. Solche eine Menge wird manchmal durch eine Fallunterscheidung beschrieben: dann addieren sich die (Anzahlen der) Möglichkeiten; und manchmal durch zwei unabhängig voneinander festlegbaren Eigenschaften: dann multiplizieren sich die (Anzahlen der) Möglichkeiten.

Teilmengen und Binomialkoeffizienten

Zur Wiederholung noch einmal die für diesen Abschnitt entscheidende Definition:

Definition: Sei M m-Menge. Die Anzahl der k-Teilmengen von M wird mit $\binom{m}{k}$ bezeichnet, dem sogenannten *Binomialkoeffizienten* „m über k“.

Es ist klar, dass eine Bijektion zwischen zwei m-Mengen auch eine Bijektion zwischen den jeweiligen Mengen der k-Teilmengen ergibt; mit Satz 1.4 hängt der Binomialkoeffizient also

tatsächlich nur von m ab und nicht von der konkreten Menge M. Solche Überlegungen werde ich in Zukunft nicht mehr explizit erwähnen.

Satz 1.9 (Eigenschaften der Binomialkoeffizienten)

Explizite Formel:

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

Rekursion

$$\binom{m+1}{k+1} = \binom{m}{k} + \binom{m}{k+1}$$

mit Anfangswerten:

$$\binom{m}{0} = 1, \qquad \binom{0}{k} = 0 \quad \textit{für} \quad k > 0$$

Einige konkrete Werte:

$$\binom{m}{0} = \binom{m}{m} = 1 \quad \textit{für alle} \quad m \qquad \binom{m}{1} = \binom{m}{m-1} = m \quad \textit{für alle} \quad m > 0$$

$$\binom{m}{k} = 0 \quad \textit{für alle} \quad k > m$$

Summenformel:

$$\sum_{k=0}^{m} \binom{m}{k} = 2^m$$

Komplementformel:

$$\binom{m}{k} = \binom{m}{m-k} \quad \textit{für} \quad m \geqslant k$$

Eine weitere Formel:

$$k \cdot \binom{m}{k} = m \cdot \binom{m-1}{k-1} = (m-k+1) \cdot \binom{m}{k-1} \quad \textit{für} \quad m \geqslant k > 0$$

Beweis: Die expliziten Formeln ergeben sich aus den beiden Formeln für die Anzahl der Injektionen in Satz 1.7 und einfachen Umformungen. Die konkreten Werte sind klar nach Definition. Die Komplementformel gilt, da jede k-Teilmenge per Komplementbildung genau einer $(n-k)$-Teilmenge entspricht und jede $(n-k)$-Teilmenge dabei vorkommt. Die Summenformel gilt, weil die Summe die Mächtigkeit der Potenzmenge angibt, nach dem Prinzip des doppelten Abzählens hier nach Größen der Teilmengen sortiert abgezählt.

Zum Beweis der Rekursionsformel betrachtet man ein festes Element der $(m+1)$-Menge: eine $(k+1)$-Teilmenge enthält entweder dieses Element und entspricht dann einer k-Teilmenge der restlichen m-Menge; oder sie enthält es nicht und entspricht dann einer $(k+1)$-Teilmenge der restlichen m-Menge.

In der letzten Formel bezeichnet die linke Seite die Anzahl der Möglichkeiten, in einer m-Menge eine k-Teilmenge und in dieser ein Element auszuwählen. Alternativ kann man ein Element aus der m-Menge und eine $(k-1)$-Teilmenge aus dem Rest (Mitte) oder eine $(k-1)$-Teilmenge aus der m-Menge und ein Element aus dem Rest (rechts) wählen. □

Aus der Rekursionsformel ergibt sich die Möglichkeit, die Binomialkoeffizienten im sogenannte *Pascalschen Dreieck* anzuordnen und zu berechnen (siehe Abbildung). Die Einträge für k laufen dabei schräg nach links unten. Die Einträge mit Wert 0 (kleiner gedruckt) werden in der Regel weggelassen, um die Dreiecksgestalt zu erhalten.

m :	k :	0	/	1	/	2	/	3	$\Sigma = 2^m$
0	1	0		0		0			1
1	1	1		0		0			2
2	1	2		1		0			4
3	1	3		3		1			8
4	1	4	+	6		4		1	16
5	1	5		10		10		5	32
6	1	6		15		20		15	64

Abbildung 1.1: Das Pascalsche Dreieck

Satz 1.10 (Binomischer Satz)

$$(x+y)^m = \sum_{k=0}^{m} \binom{m}{k} \cdot x^k \cdot y^{m-k} \qquad \textit{für } x, y \in \mathbb{C}, m \in \mathbb{N}$$

Beweis: Seien zunächst $x, y \in \mathbb{N}$. Dann steht links die Anzahl der Abbildungen einer m-Menge in die disjunkte Vereinigung einer x- und einer y-Menge. Diese berechnet sich aber auch folgendermaßen: Für zwischen 0 und m variierendem k wählt man eine beliebige k-Menge aus der m-Menge, eine Abbildung der k-Menge in die x-Menge und eine Abbildung der verbleibenden $(m-k)$-Menge in die y-Menge.

Für beliebige komplexe Zahlen x, y folgt das Ergebnis aus der Tatsache, dass zwei auf den natürlichen Zahlen übereinstimmende Polynome gleich sind. □

Alternativ kann man den binomischen Satz auch per Induktion nach m beweisen.

Es gibt auch sogenannte *Polynomialkoeffizienten* (auch *Multinomialkoeffizienten* genannt):

$$\binom{m}{k_1, \ldots, k_r} := \binom{m}{k_1}\binom{m-k_1}{k_2}\cdots\binom{m-(k_1+\cdots+k_{r-1})}{k_r} = \frac{m!}{k_1! \cdot \ldots \cdot k_r!},$$

wobei stets $k_1 + \cdots + k_r = m$ gelten soll. Speziell ist also $\binom{m}{k} = \binom{m}{k, m-k}$. Die Polynomialkoeffizienten kann man auch kombinatorisch definieren als die Anzahl der Möglichkeiten, eine m-Menge zu zerlegen in (paarweise disjunkte) k_1-,k_2-,…,k_r-Teilmengen, wobei die Reihenfolge dieser Mengen beachtet wird. Da sich dies aus der sukzessiven Wahl einer k_1-Teilmenge aus der m-Menge, einer k_2-Teilmenge aus der verbleibenden $(m-k_1)$-Menge usw. ergibt, kann man leicht die explizite Formel aus der expliziten Formel für die Binomialkoeffizienten herleiten, und beweist dann analog zum binomischen Satz (oder ebenfalls durch Induktion):

Satz 1.11 (Polynomischer Satz)

$$(x_1 + \cdots + x_r)^m = \sum_{k_1+\cdots+k_r=m} \binom{m}{k_1, \ldots, k_r} \cdot x_1^{k_1} \cdot x_2^{k_2} \cdots x_r^{k_r} \qquad \textit{für } x_i \in \mathbb{C}, m \in \mathbb{N}$$

Mengenpartitionen und Stirling–Zahlen zweiter Art

Definition: Eine k-*Partition* einer Menge M ist eine Darstellung $M = M_1 \cup \ldots \cup M_k$ mit paarweise disjunkten, nicht-leeren Teilmengen M_i, die *Blöcke* der Partition genannt werden. Eine *Partition* von M ist eine k-Partition für ein $k \in \mathbb{N}$.

Ist eine Partition wie oben gegeben, so definiert $x \in M_i \iff y \in M_i$ eine Äquivalenzrelation $x \sim y$, deren Klassen gerade die M_i sind. Umgekehrt bilden die Klassen einer Äquivalenzrelation eine Partition.

Die Anzahl der k-Partitionen von M (bzw. der Äquivalenzrelationen auf M mit k Klassen) wird mit $S_{m,k}$ bezeichnet, und die Anzahl der Partitionen von M (bzw. der Äquivalenzrelationen auf M) mit B_m. Die Zahlen $S_{m,k}$ heißen *Stirling–Zahlen zweiter Art* und die Zahlen B_m *Bell–Zahlen*.

Satz 1.12 (Eigenschaften der Stirling–Zahlen zweiter Art)

Explizite Formel:

$$S_{m,k} = \frac{1}{k!}\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^m = \frac{1}{k!}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}j^m = \sum_{j=0}^{k}(-1)^{k-j}\frac{j^m}{j!(k-j)!}$$

Rekursion $S_{m+1,k+1} = S_{m,k} + (k+1)\cdot S_{m,k+1}$ *mit Anfangswerten:* $S_{0,0} = 1$, $S_{m,0} = 0$ *für* $m > 0$ *und* $S_{m,k} = 0$ *für* $k > m$

Einige konkrete Werte:

$S_{m,m} = 1$ $S_{m,k} = 0$ *für* $k > m \geqslant 0$

$S_{m,1} = 1$ *und* $S_{m,m-1} = \binom{m}{2}$ *für* $m \geqslant 1$

$S_{m,2} = 2^{m-1} - 1$ *für* $m \geqslant 2$

Beweis: Die expliziten Formeln ergeben sich aus den beiden Formeln für die Anzahl der Surjektionen in Satz 1.7 und der expliziten Formel für die Binomialkoeffizienten.

Für die Rekursionsformel nimmt man eine $(k+1)$-Partition einer $(m+1)$-Menge und betrachtet darin ein festes Element. Entweder dieses bildet selbst einen Block der Partition und es bleibt eine k-Partition der restlichen m Elemente; oder es bleibt eine $(k+1)$-Partition der restlichen m Elemente und es gibt $(k+1)$ Möglichkeiten, zu welchem Block das gesonderte Element gehört.

Eine Partition in zwei Blöcke entspricht der Auswahl einer Teilmenge, die weder leer noch das Ganze ist, also der Mächtigkeit der Potenzmenge minus zwei. Dabei wird aber jede Partition doppelt gezählt (statt dem einen Block kann auch sein Komplement gewählt werden). Insgesamt sind dies $S_{m,2} = \frac{1}{2}(|\mathfrak{P}(M)| - 2)$ Möglichkeiten für eine m-Menge M.

Eine Partition einer m-Menge in $m-1$ Blöcke entspricht der Auswahl einer 2-Teilmenge: dem einzigen Block, der aus mehr als einem Element besteht. Alle anderen konkreten Werte sind klar nach Definition. □

$S_{0,0} = 1$ kann man als Konvention auffassen, um die Gültigkeit von Rekursionsformeln zu

erhalten. Man kann dem aber auch Sinn verleihen, indem man die Vereinigung von 0 Mengen als Partition von $\emptyset$ ansieht, also $\emptyset = \bigcup_{i \in \emptyset} M_i$.

Übung: Man überprüfe, dass die Formel für die Anzahl der Surjektionen auch für die Sonderfälle gilt, dass eine der beiden Mengen leer ist.

Aus der Rekursionsformel ergibt sich die Darstellung und Berechnung der Stirling–Zahlen zweiter Art im „Stirling–Dreieck zweiter Art“, analog zum Pascalschen Dreieck (die Einträge mit Wert 0 sind nun weggelassen).

m :	k :	0	/	1	/	2	/	3	$\Sigma = B_m$
0		1							1
1		0		1					1
2		0		1		1			2
3		0		1		1			5
4		0		1		3		1	15
5		0		1		15		10	52
6		0		1		31		90	65	15	1	203

$+\,2\cdot 3$ $+\,3\cdot 6$

Abbildung 1.2: Das Stirling–Dreieck zweiter Art

Satz 1.13 (Eigenschaften der Bell–Zahlen)

Rekursion mit Anfangswert:

$$B_{m+1} = \sum_{k=0}^{m} \binom{m}{k} \cdot B_k \qquad B_0 = 1$$

Zusammenhang mit den Stirling–Zahlen zweiter Art:

$$B_{m+1} = \sum_{k=0}^{m+1} S_{m+1,k} = \sum_{j=0}^{m} (j+1) \cdot S_{m,j}$$

Beweis: Die zweite Formel oben und die erste unten gelten per Definition. Sei nun eine Partition einer $(m+1)$-Menge gegeben; ein Element wird wiederum ausgesondert. Dieses Element lag in einem Block der Größe $m+1-k$: also erhält man diese Partition auch durch eine Auswahl der $m-k$ anderen Elemente dieses Blocks mit $\binom{m}{m-k} = \binom{m}{k}$ Möglichkeiten und einer Partition der restlichen k Elemente mit B_k Möglichkeiten. Dies ergibt die Rekursionsgleichung.

Man kann aber auch die Anzahl j der Blöcke der auf den restlichen m Elementen induzierten Partition betrachten. Das gesonderte Element kann man jedem Block hinzufügen oder als eigenen Block, was $j+1$ Möglichkeiten für jedes j und damit die letzte Gleichung liefert. □

Zahlpartitionen

Eine *Zahlpartition* der natürlichen Zahl m ist eine Darstellung $m = m_1 + \cdots + m_k$ mit $m_i \geqslant 1$ für alle i, wobei die Reihenfolge der Summanden keine Rolle spiele. Ohne Einschränkung kann

man also $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_k$ annehmen. Eine solche Zahlpartition von m in k Stücke entspricht einer k-Partition einer m-Menge, deren Elemente nicht zu unterscheiden sind. Die m_i sind dann die Mächtigkeiten der Blöcke.

Definition: Die Anzahl der Zahlpartitionen von m in k Stücke wird mit $P_{m,k}$ bezeichnet, und die Anzahl der Zahlpartitionen von m überhaupt mit der m-ten *Partitionszahl* P_m.

Die Darstellung einer Zahlpartition erfolgt oft durch ein *Ferrers–* oder *Young–Diagramm* (in der Literatur oft auch gedreht oder gespiegelt):

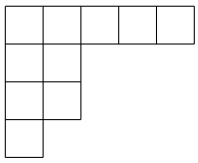


Abbildung 1.3: Ferrers–Diagramm für die Partition $10 = 5 + 2 + 2 + 1$.

Satz 1.14 (Eigenschaften der Zahlpartitionszahlen)

Rekursion *mit Anfangswerten:*

$$P_{m,k} = \sum_{j=0}^{k} P_{m-k,j} \qquad P_{0,0} = 1, \qquad P_{m,0} = 0 \ \textit{für} \ m > 0, \qquad P_{m,k} = 0 \ \textit{für} \ k > m$$

$$P_{m+1,k+1} = P_{m,k} + P_{m-k,k+1}$$

Einige konkrete Werte:

$$P_{m,1} = P_{m,m} = 1 \ \textit{für} \ m \geqslant 1, \qquad P_{m,m-1} = 1 \ \textit{für} \ m \geqslant 2, \qquad P_{m,2} = \left\lfloor \frac{m}{2} \right\rfloor \ \textit{für} \ m \geqslant 2$$

Asymptotisches Verhalten: $P_{m,k} \leqslant P_{m-k}$ *für* $m \geqslant k$

$P_{m,k} = P_{m-k}$ *für* $2k \geqslant m \geqslant k$

insbesondere: $P_{m,m-2} = 2$ *für* $m \geqslant 4$, $P_{m,m-3} = 3$ *für* $m \geqslant 6$

Beweis: Für $P_{m,2}$ überlegt man sich, dass jede Partition die Form $m = n + (m - n)$ mit $\frac{m}{2} \leq n < m$ hat. Die anderen konkreten Werte überlegt man sich leicht.

Die Rekursionsformel ergibt sich aus dem Wegstreichen der ersten Spalte im Young–Diagramm; bei einer $P_{m,k}$-Partition besteht diese aus genau k Kästchen, also bleibt eine Partition von $m-k$ in maximal k Stücke. Falls $m - k \leqslant k$, d.h. falls $2k \geqslant m$, so ist dies eine beliebige Zahlpartition von $m - k$, woraus sich die asymptotische Formel ergibt. Im allgemeinen erlaubt $m - k$ aber weitere Partitionen, nämlich in mehr als k Stücke, daher die Ungleichung.

Für die zweite Rekursionsgleichung macht man folgende Fallunterscheidung: Entweder die letzte Zeile des Young–Diagramms besteht nur aus einem Kästchen, das man wegstreicht (und erhält eine Partition der um eins kleineres Zahl in ein Stück weniger), oder jede Zeile hat mindestens zwei Kästchen. Dann kann man die erste Spalte wegstreichen und erhält eine Partition der entsprechend verminderten Zahl in ebensoviele Stücke. □

$P_{m,m-k}$ wird also konstant gleich P_k ab $m = 2k$. Zum Beispiel $P_{m,m-3} = P_3 = 3$ für $m \geqslant 6$, nämlich $m = 4 + \underbrace{1+\cdots+1}_{m-4 \text{ mal}} = 3+2+\underbrace{1+\cdots+1}_{m-5 \text{ mal}} = 2+2+2+\underbrace{1+\cdots+1}_{m-6 \text{ mal}}$.

Bemerkung: Für die Partitionszahlen P_m gibt es folgende Rekursionsgleichung:

$$P_m = \sum_{k=0}^{m} P_{m,k} = \sum_{k \geqslant 0} (-1)^k \cdot \left(P_{m-\frac{1}{2}k(3k-1)} + P_{m-\frac{1}{2}k(3k+1)} \right)$$

mit der Konvention $P_m = 0$ für negative m. (In Wirklichkeit ist die Summe also endlich). Ein (nicht ganz einfacher) Beweis hierfür findet sich in dem Buch von Cameron [C], 13.2.3. Explizite Formeln für die Partitionszahlen $P_{m,k}$ und P_m sind nicht bekannt.

Aus der Rekursionsgleichung ergibt sich wiederum eine Berechnungsmethode im Zahlpartitionsdreiecks: Die Summe der oberen Zeile eines in der linken Diagonale beginnenden Dreiecks ergibt die Spitze. Wendet man diese Regel zunächst auf das kleinere Dreieck an, welches durch Weglassen der rechten schrägen Spalte entsteht, erhält man aus der ersten Rekursionsgleichung die zweite, welche der Rekursion der Binomialkoeffizienten bzw. Stirling–Zahlen ähnlicher ist.

m :	k : 0	1	2	3	$\Sigma = P_m$
0	1				1
1	0	1			1
2	0	1	1		2
3	0	1	1	1	3
4	0	1	2	1	5
5	0	1	2	2	7
6	0	1	3	3	11
7	0	1	3	4	15
8	0	1	4	5	22

Abbildung 1.4: Das Zahlpartitionsdreieck

Geordnete Zahlpartitionen

Eine Surjektion einer m-Menge auf die Menge $\{1, \ldots, k\}$ kann man als eine „angeordnete Partition“ der m-Menge in k Blöcke auffasen: Der i-te Block besteht aus den Elementen, die auf i abgebildet werden. Analog gibt es auch eine angeordnete Version der Zahlpartitionen:

Eine *geordnete Zahlpartition* der natürlichen Zahl m ist eine Darstellung $m = m_1 + \cdots + m_k$ mit $m_i \geqslant 1$ für alle i, unter Beachtung der Reihenfolge der Summanden. Etwa sind $1+2$ und $2+1$ verschiedene geordnete Zahlpartitionen von 3.

Satz 1.15 *Die Anzahl der geordneten Zahlpartition von* m *in* k *Stücke ist*

$$\begin{cases} \binom{m-1}{k-1} & \text{für } m \geqslant 1, k \geqslant 1 \\ 0 & \text{für } m = 1, k = 0 \text{ oder für } k > m \\ 1 & \text{für } m = k = 0 \end{cases}$$

Beweis: Man betrachte die Teilsummen $a_1 := m_1$, $a_2 := m_1 + m_2$, ..., $a_{k-1} := m_1 + \cdots + m_{k-1}$. Die Zahlen a_i bilden dann eine $(k-1)$-Teilmenge von $\{1, \ldots, m-1\}$. Umgekehrt erhält man aus $0 < a_1 < \cdots < a_{k-1} < m$ eine Zahlpartition durch Differenzenbildung: $m_1 := a_1$, $m_2 := a_2 - a_1$,...,$m_{k-1} := a_{k-1} - a_{k-2}$ und $m_k := m - a_{k-1}$. Dies sind zueinander inverse Umformungen, also gibt es ebensoviele geordnete Zahlpartition von m in k Stücke wie $(k-1)$-Teilmengen einer $(m-1)$-Menge. □

Kleine Zusammenfassung

Insgesamt haben wir vier Arten von Partitionen von einer m-Menge in k Blöcke untersucht:

Blöcke / Elemente	ungeordnet	Anzahl	angeordnet	Anzahl
ununterscheidbar	Zahlpartition	$P_{m,k}$	geordnete Zahlpartition	$\binom{m-1}{k-1}$
unterschieden	Mengenpartition	$S_{m,k}$	Surjektion	$k! \cdot S_{m,k}$

Ähnlich kann man vier verschiedene Arten von Auswahlen (oder Teilmengen) von k Elementen aus einer m-Menge betrachten.

Auswahl / Wiederholungen	ungeordnet	Anzahl	angeordnet	Anzahl
nicht erlaubt	Teilmenge	$\binom{m}{k}$	Injektion	$k! \cdot \binom{m}{k}$
erlaubt	„Multiteilmenge“	$\binom{m+k-1}{k}$	beliebige Abbildung	m^k

„Multimenge“ ist ein verallgemeinerter Begriff von Menge, bei dem ein Objekt mehrfaches Element sein kann. Zu den Elementen einer Multimenge gehört also die Zusatzinformation, wievielfaches Element es ist. Analog dazu sei hier der Begriff der Multiteilmenge verstanden. Eine (k-)Multiteilmenge einer Menge M soll also eine Multimenge sein, deren Elemente alle Elemente von M sind (und deren Vielfachheiten sich zu k summieren). Eine nicht-leere m-Menge hat also k-Multiteilmengen auch für $k > m$.

Das einzige bislang noch nicht bewiesene Ergebnis darin ist:

Satz 1.16 *Die Anzahl der* k*-elementigen Multiteilmengen einer* m*-Menge ist* $\binom{m+k-1}{k}$.

BEWEIS: Diese Anzahl kann man auf geordnete Zahlpartitionen zurückführen. Dazu komme die Zahl i in der Multiteilmenge a_i mal vor. Um Zahlen $\geqslant 1$ zu erhalten, betrachten wir $b_i := a_i+1$. Die b_i bilden dann eine geordnete Zahlpartition von $\sum_{i=1}^{m} b_i = \sum_{i=1}^{m}(a_i+1) = k+m$ in m Stücke. Deren Anzahl ist nach Satz 1.15 $\binom{m+k-1}{m-1} = \binom{m+k-1}{k}$. □

Permutationen und Stirling–Zahlen erster Art

Eine *Permutation* einer Menge M ist eine Bijektion von M auf M. Die Komposition von zwei Bijektionen ist wieder eine Bijektion. Unter der Komposition bilden die Permutationen von M eine Gruppe, d.h.

- die Komposition ist assoziativ;
- es gibt die *identische Permutation* id_M, die $\sigma \circ \mathrm{id}_M = \mathrm{id}_M \circ \sigma = \sigma$ für alle Permutationen σ von M erfüllt;
- zu jeder Permutation σ gibt es eine Permutation σ^{-1} (die Umkehrabbildung), welche $\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = \mathrm{id}_M$ erfüllt.

Diese Gruppe heißt die *symmetrische Gruppe* auf M und wird meist mit $\mathrm{Sym}(M)$ oder S_M bezeichnet. Für $M = \{1,\ldots,m\}$ schreibt man auch $\mathrm{Sym}(m)$ oder S_m. Für $m \geqslant 3$ ist S_m nicht kommutativ, d.h. im allgemeinen ist $\sigma \circ \tau$ verschieden von $\tau \circ \sigma$.

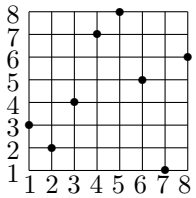
Wenn die Elemente einer Menge M angeordnet sind, z.B. als $x_1, x_2, \ldots, x_m$, dann überführt eine Permutation σ diese Anordnung in die Anordnung $\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_m)$. Umgekehrt legen zwei Anordnungen einer Menge genau eine Permutation fest, welche auf diese Weise die erste Anordnung in die zweite überführt. Es gibt also ebensoviele Anordnungen einer Menge wie es Permuationen dieser Menge gibt. Die Bijektion zwischen den Permutationen und den Anordnungen hängt aber von der Wahl einer Anfangsanordnung ab. Bei einer Menge wie $\{1,\ldots,m\}$, die eine natürliche Anordnung trägt, gibt es dann auch eine natürliche Bijektion zwischen einer Permutation σ und der Anordnung $\sigma(1), \sigma(2), \ldots, \sigma(m)$ der Zahlen von 1 bis m.

Es gibt viele Arten, wie man Permutationen (hier der Menge $\{1,\ldots,8\}$) darstellen kann:

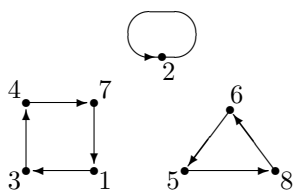
Wertetabelle

i	1	2	3	4	5	6	7	8
σ(i)	3	2	4	7	8	5	1	6

Funktionsgraph



Graph



Wort (Anordnung)	3 2 4 7 8 5 1 6
Zyklenzerlegung	(4713)(586)(2)

Im Beispiel zerfällt der Graph in drei Teile, die sogenannten Zusammenhangskomponenten. Diese bestimmen die Zyklen der Permutation. Wenn σ eine Permutation der Menge M ist, dann ist ein *Zyklus* von σ (der *Länge* k) eine Folge $x_1, \ldots, x_k$ von Elementen aus M mit $\sigma(x_i) = x_{i+1}$ für $i = 1, \ldots, k-1$ und $\sigma(x_k) = x_1$. Ein Element, das einen Zyklus der Länge 1 bildet, heißt *Fixpunkt* der Permutation. Jede Permutation lässt sich als „Produkt“ ihrer Zyklen schreiben wie im obigen Beispiel; die Schreibweise ist eindeutig bis auf Reihenfolge der Zyklen und zyklische Vertauschung der Elemente in jedem Zyklus.

(Wenn man Permutationen von $\{1 \ldots, m\}$ betrachtet, erhält man eine kanonische Schreibweise, wenn man mit der 1 beginnt und den jeweils nächsten Zyklus mit dem minimalen noch verbleibenden Element. Im Beispiel wäre dies (1347)(2)(586). Wenn man aus dem Kontext weiß, um die Permutationen welcher Menge es sich handelt, lässt man in der Zyklenzerlegung die Fixpunkte meist weg.)

Bemerkung: Als *Zyklus der Länge* k oder kurz k*-Zyklus* bezeichnet man auch eine Permutation, die in der Zyklenzerlegung einen Zyklus der Länge k und sonst nur Fixpunkte hat. Ein 2-Zyklus heißt auch *Transposition*. In diesem Sinne kann man die Zyklenzerlegung einer Permutation tatsächlich als Produkt (im Sinne von Komposition) von Zyklen verstehen. Man überlegt sich dazu auch leicht, dass disjunkte Zyklen (d.h. jedes Element der permutierten Menge ist Fixpunkt aller Zyklen bis auf höchstens einen) untereinander kommutieren.

Vorsicht: Man kann eine Permutation σ auf viele Arten als Produkt von (nicht disjunkten) Zyklen schreiben. Zum Beispiel gilt $(123) \circ (123) = (132)$. Die Zerlegung ist nur dann eindeutig (bis auf Reihenfolge der Zyklen), wenn es sich um die Zyklen von σ handelt, so wie sie oben definiert wurden.

Satz 1.17

(a) *Die Anzahl der* m*-Zyklen unter den Permutationen von* m *Elementen ist* $(m-1)!$.

(b) *Die Anzahl der fixpunktfreien Permutationen von* m *Elementen ist* $m! \cdot \sum_{j=0}^{m} \frac{(-1)^j}{j!}$.

Beweis: (a) Es gibt $m!$ Möglichkeiten, einen m-Zyklus $(x_1\, x_2 \ldots x_m)$ aufzuschreiben; da man einen m-Zyklus mit jedem beliebigen der m Elemente beginnen kann, wird dabei jeder m-fach gezählt.

(b) Für Elemente $x_1, \ldots, x_m$ gibt es genau $(m-i)!$ Permutationen, welche (mindestens) $x_1, \ldots, x_i$ als Fixpunkte zu haben. Mit der Siebformel kann man ganz ähnlich wie bei der Anzahl der Surjektionen in Satz 1.7 die Anzahl der Permutationen mit Fixpunkten berechnen. □

Definition: Die Anzahl der Permutationen von m Elementen mit k Zyklen wird mit $s_{m,k}$ bezeichnet. Diese Zahlen heißen *Stirling–Zahlen erster Art*.

Die Zyklenzerlegung der Permutation einer Menge liefert eine Partition dieser Menge; mit zusätzlich einer „zyklischen Ordnung“ auf jedem Block. Zu jeder Partition findet man umgekehrt

eine Permutation; es gilt also stets $s_{m,k} \geqslant S_{m,k}$, aber im allgemeinen werden die Stirling–Zahlen erster Art viel größer werden als die zweiter Art.

Der *Typ* einer Permutation ist bestimmt durch die Anzahl b_i der i-Zyklen. Wenn man die Permutationen eines gegebenen Typs zählen will, so kann man zunächst die m Elemente beliebig (also mit $m!$ Möglichkeiten) auf das Zyklenmuster verteilen, das z.B. folgendermaßen aussieht:

$$\underbrace{(\,\ldots\,)(\,\ldots\,)}_{b_3=2}\underbrace{(\,\ldots\,)(\,\ldots\,)(\,\ldots\,)(\,\ldots\,)}_{b_2=4}\underbrace{(\,\ldots\,)(\,\ldots\,)}_{b_1=2}$$

Dabei spielt die Reihenfolge der i-Zyklen untereinander keine Rolle, man hat also jede Permutation bereits $(b_1! \cdot b_2! \cdot \ldots \cdot b_m!)$-fach gezählt. Außerdem kann man jeden i-Zyklus mit einem beliebigen seiner i Elemente beginnen, d.h. jeder i-Zyklus wurde i-fach gezählt, was zusammen einen Faktor $1^{b_1} \cdot 2^{b_2} \cdot \ldots \cdot m^{b_m}$ ergibt. Für den festen, durch $b_1, \ldots, b_m$ bestimmten Typ gibt es also

$$\frac{m!}{b_1! \cdots b_m! \cdot 1^{b_1} \cdots m^{b_m}}$$

Permutationen dieses Typs. Summiert man über sämtliche möglichen Typen, ergibt sich folgende explizite Formel für die Stirling–Zahlen erster Art:

$$s_{m,k} \;=\; \sum \left\{ \frac{m!}{b_1! \cdots b_m! \cdot 1^{b_1} \cdots m^{b_m}} \;\middle|\; \sum_{i=1}^{m} b_i = k, \sum_{i=1}^{m} i b_i = m \right\}$$

Diese Formel ist allerdings für praktische Belange wenig nützlich.

Satz 1.18 (Eigenschaften der Stirling–Zahlen erster Art)

Rekursion *mit Anfangswerten:*

$s_{m+1,k+1} = s_{m,k} + m \cdot s_{m,k+1}$ $\quad s_{0,0} = 1, \quad s_{m,0} = 0$ *für* $m > 0$

und $\quad s_{m,k} = 0$ *für* $k > m$

Einige konkrete Werte:

$s_{m,m} = 1 \qquad s_{m,k} = 0$ *für* $k > m \geqslant 0$

$s_{m,1} = (m-1)! \quad$ *und* $\quad s_{m,m-1} = \binom{m}{2}$ *für* $m \geqslant 1$

$s_{m,2} = (m-1)!\big(1 + \frac{1}{2} + \cdots + \frac{1}{m-1}\big)$ *für* $m \geqslant 2$

Summenformel: $\quad \sum_{k=0}^{m} s_{m,k} = m!$

BEWEIS: Für die Rekursionsformel nimmt man wie üblich ein Element heraus. Dieses war entweder ein Fixpunkt und es bleibt eine Permutation von m Elementen mit k Zyklen. Oder es bleiben $k+1$ Zyklen übrig: dann gibt es m Möglichkeiten, wie man das ausgesonderte Element wieder einfügen kann, nämlich hinter jeder Zahl in deren Zyklus.

$s_{m,1}$ wurde in Satz 1.17 (a) berechnet. Für $s_{m,m-1}$ überlegt man sich, dass genau die Transpositionen $m-1$ Zyklen haben, von denen es ebensovielen wie 2-Teilmengen gibt. Schließlich berechnet man $s_{m,2}$ per Induktion, mit dem Induktionsschritt:
$s_{m+1,2} = s_{m,1} + m \cdot s_{m,2} = (m-1)! + m \cdot (m-1)!\big(1 + \frac{1}{2} + \cdots + \frac{1}{m-1}\big) = m!\big(1 + \frac{1}{2} + \cdots + \frac{1}{m}\big)$.
Alles andere gilt offensichtlich per Definition. □

Als letztes Zahlendreieck erhalten wir das Stirling–Dreieck erster Art. Man beachte die Ähnlichkeiten und Unterschiede zum Stirling–Dreieck zweiter Art!

$m:$	$k:$ 0	1	2	3	4	5	6	$\Sigma = m!$
0	1							1
1	0	1						1
2	0	1	1					2
3	0	2	3	1				6
4	0	6	11	$+ m \cdot 6$	1			24
5	0	24	50	35	10	1		120
6	0	120	274	225	85	15	1	720

Abbildung 1.5: Das Stirling–Dreieck erster Art

Bemerkung: Man kann die *fallenden Fakultäten* definieren als

$$x_{(0)} := 1 \quad \text{und} \quad x_{(n)} := x_{(n-1)} \cdot (x - n + 1) = x(x-1)\cdots(x-n+1)$$

Setzt man für x eine natürliche Zahl m ein, so gilt $m_{(n)} = \frac{m!}{(n-m)!} = \binom{m}{n} \cdot n!$.

Die Polynome über $\mathbb{C}$ vom Grad $\leqslant n$ bilden einen Vektorraums $\mathbb{C}_n[x]$. Sowohl die Potenzen $\{1, x, x^2, \ldots, x^n\}$ als auch die fallenden Fakultäten $\{1, x, x_{(2)}, \cdots, x_{(n)}\}$ bilden Basen dieses Vektorraums. Die zweite Basis ist interessant für den sogenannten Differenzen–Kalkül, der eine Art diskretes Analogon der Differentialrechnung darstellt. Der Zusammenhang der Stirling–Zahlen besteht nun darin, dass sie jeweils die Einträge der Basiswechselmatrizen bilden (bis auf Vorzeichen), denn es gilt:

Satz 1.19

$$x^n = \sum_{k=0}^{n} S_{n,k} \cdot x_{(k)} \quad \textit{und} \quad x_{(n)} = \sum_{k=0}^{n} (-1)^{n-k} s_{n,k} \cdot x^k$$

In der Literatur werden daher auch oft die $(-1)^{n-k}s_{n,k}$ Stirling–Zahlen erster Art genannt und mit $s_{n,k}$ bezeichnet.

Beweis: Nach Satz 1.8 gilt die erste Formel für alle natürlichen Zahlen x, damit sind aber schon die beiden Polynome gleich. Die zweite Formel beweist man z.B. durch Induktion nach n mit Hilfe der Rekursionsformel. □

Es sind also die beiden Matrizen $\left(S_{n,k}\right)_{k,n\geqslant 0}$ und $\left((-1)^{n-k} \cdot s_{n,k}\right)_{k,n\geqslant 0}$ zueinander invers, d.h. das Produkt der beiden Matrizen ergibt die Identitätsmatrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 1 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 1 & 1 & 0 & 0 & 0 & \ldots \\ 0 & 1 & 3 & 1 & 0 & 0 & \ldots \\ 0 & 1 & 7 & 6 & 1 & 0 & \ldots \\ 0 & 1 & 15 & 25 & 10 & 1 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 1 & 0 & 0 & 0 & 0 & \ldots \\ 0 & -1 & 1 & 0 & 0 & 0 & \ldots \\ 0 & 2 & -3 & 1 & 0 & 0 & \ldots \\ 0 & -6 & 11 & -6 & 1 & 0 & \ldots \\ 0 & 24 & -50 & 35 & -10 & 1 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \mathrm{id}$$

Da es beides untere Dreiecksmatrizen sind, kann man hier das Produkt unendlicher Matrizen sinnvoll definierten. Alternativ kann man links oben quadratische Teilmatrizen ausschneiden und deren Produkte betrachten, die dann jeweils die Identität ergeben.

Binomialkoeffizienten, Partitionszahlen und die Stirling–Zahlen beider Arten sind kombinatorische Grundzahlen, auf die man viele kombinatorische Probleme zurückführen kann. Ein solches Problem wird als gelöst gelten, wenn man eine einfache explizite Formel gefunden hat, in welcher diese Zahlen vorkommen.

I.2 Erzeugende Funktionen

Formale Potenzreihen

Sei K ein Körper, etwa $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Definition 2.1 *Eine (formale)* Potenzreihe *über* K *ist ein Ausdruck der Form* $\sum_{n\in\mathbb{N}} a_n X^n$ *mit* $a_n \in K$. *Die Menge der Potenzreihen über* K *bezeichnet man mit* $K[[X]]$.
Zwei Potenzreihen $\sum_{n\in\mathbb{N}} a_n X^n$ *und* $\sum_{n\in\mathbb{N}} b_n X^n$ *sind per Definition genau dann gleich, wenn* $a_n = b_n$ *für alle* $n \in \mathbb{N}$ *gilt.*

In den Potenzreihen wird X als Variable bezeichnet; die a_n heißen die Koeffizienten der Potenreihe. „Formal“ werden sie deshalb manchmal genannt, da das Konvergenzverhalten in der Regel keine Rolle spielt: Es ist im allgemeinen nicht möglich, für X eine Zahl einzusetzen und einen Wert der Reihe auszurechnen. Potenzreihen sind zunächst nur eine Möglichkeit, eine Folge von Zahlen $(a_n)_{n\in\mathbb{N}}$ als ein einzelnes Objekt aufzufassen. Der Vorteil gegenüber den Folgen ist, dass die Darstellung Rechenoperationen suggerieren, die sich dadurch ergeben, dass man die üblichen Rechenoperationen auf K so fortsetzt, dass Kommutativ–, Assoziativ– und Distributivgesetze gelten. Damit erhält man folgende Addition, Subtraktion, Multiplikation und formale Ableitung:

$$\begin{aligned}
\sum_{n\in\mathbb{N}} a_n X^n \pm \sum_{n\in\mathbb{N}} b_n X^n &:= \sum_{n\in\mathbb{N}} (a_n \pm b_n) X^n \\
-\sum_{n\in\mathbb{N}} a_n X^n &:= \sum_{n\in\mathbb{N}} (-a_n) X^n \\
\sum_{n\in\mathbb{N}} a_n X^n \cdot \sum_{n\in\mathbb{N}} b_n X^n &:= \sum_{n\in\mathbb{N}} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) X^n \\
\Big(\sum_{n\in\mathbb{N}} a_n X^n \Big)' = \frac{d}{dX}\Big(\sum_{n\in\mathbb{N}} a_n X^n \Big) &:= \sum_{n\in\mathbb{N}} (n+1) a_{n+1} X^n
\end{aligned}$$

Jedes Polynom $a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ über K, insbesondere jede Zahl aus K selbst, kann man als eine Potenzreihe auffassen, nämlich $a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n + 0X^{n+1} + 0X^{n+2} + \cdots$. Man sieht leicht, dass 0 ein neutrales Element der Addition ist und $(K[[X]], +)$ eine Gruppe ist, und dass 1 ein neutrales Element der Multiplikation ist. Im allgemeinen hat aber eine

Potenzreihe kein multiplikatives Inverses. Das Inverse zu $\sum_{n\in\mathbb{N}} a_n X^n$ existiert genau dann, wenn $a_0 \neq 0$; dann gilt:

$$\Big(\sum_{n\in\mathbb{N}} a_n X^n\Big)^{-1} = \frac{1}{\sum_{n\in\mathbb{N}} a_n X^n} = \sum_{n\in\mathbb{N}} b_n X^n \quad \text{mit } b_0 = \frac{1}{a_0} \text{ und } b_n = -\frac{1}{a_0}\sum_{k=1}^{n} a_k b_{n-k}$$

Die Rechenregeln für $K[[X]]$ sind so gestaltet, dass die üblichen Rechenregeln gelten, etwa Kommutativität und Assoziativität von $+$ und $\cdot$ und Distributivität von Addition und Multiplikation, was erklärt, warum die Multiplikation nicht koeffizientenweise erklärt wird. $K[[X]]$ ist ein sogenannter *kommutativer Ring mit Eins*, wie es auch $\mathbb{Z}$ ist. (Und ähnlich wie man $\mathbb{Z}$ zu dem Körper $\mathbb{Q}$ machen kann, kann man auch $K[[X]]$ zu einem Körper $K((X))$ machen.)

Die Ableitung ist eine formale Derivation, d.h. es gelten die folgenden Rechenregeln:

$$\Big(\sum_{n\in\mathbb{N}} a_n X^n \pm \sum_{n\in\mathbb{N}} b_n X^n\Big)' = \Big(\sum_{n\in\mathbb{N}} a_n X^n\Big)' \pm \Big(\sum_{n\in\mathbb{N}} b_n X^n\Big)'$$

$$\Big(\sum_{n\in\mathbb{N}} a_n X^n \cdot \sum_{n\in\mathbb{N}} b_n X^n\Big)' = \Big(\sum_{n\in\mathbb{N}} a_n X^n\Big)' \cdot \Big(\sum_{n\in\mathbb{N}} b_n X^n\Big) + \Big(\sum_{n\in\mathbb{N}} a_n X^n\Big) \cdot \Big(\sum_{n\in\mathbb{N}} b_n X^n\Big)'$$

Insgesamt ist $K[[X]]$ damit eine sogenannte *differentielle* K*-Algebra*. Man kann übrigens auch die Einsetzung einer Potenzreihe in eine andere definieren, was für konvergenten Reihen der Verknüpfung der dadurch gegebenen Funktionen miteinander entspricht.

Beispiele

Einige Identitäten, die man aus den Analysis kennt (dort für konvergente Reihen innerhab des Konvergenzbereiches) gelten allgemeiner als für formale Potenzreihen; man kann es jeweils mit den Rechenregeln überprüfen (Übung!).

$$\text{geometrische Reihe:} \quad \sum_{n\in\mathbb{N}} (cX)^{kn} = \frac{1}{1-(cX)^k} \quad \text{für } k \in \mathbb{N}, k \neq 0, c \in \mathbb{C}$$

$$\text{und somit} \quad \frac{1}{1-X} \cdot \sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\in\mathbb{N}} \Big(\sum_{k=0}^{n} a_k\Big) X^n$$

$$\text{hypergeometrische Reihe:} \quad \sum_{n\in\mathbb{N}} \binom{m+n-1}{n} X^n = \frac{1}{(1-X)^m} \quad \text{für } m \in \mathbb{Z}$$

$$\text{binomische Reihe:} \quad \sum_{n\in\mathbb{N}} \binom{c}{n} X^n = (1+X)^c \quad \text{für } c \in \mathbb{Q}$$

$$\text{wobei } \binom{c}{n} := \frac{c(c-1)\cdots(c-n+1)}{n!}$$

Die Exponentiation mit einer rationalen Zahl $\frac{1}{q}$ im letzten Beispiel bedeutet eine „q-te Wurzel“, d.h. eine Reihe, die q-fach mit sich selbst multipliziert die Ausgangsreihe ergibt. Solch eine Wurzel ist, sofern sie existiert, im allgemeinen nicht eindeutig bestimmt!

Wenn eine formale Potenzreihe auf einem Intervall konvergiert, definiert sie darauf eine Funktion. Solch eine Funktion heißt *analytische Funktion*, die Potenzreihe erhält man dann als Taylor–Reihe der Funktion. Die Rechenregeln für die Potenzreihen stimmen dann mit den Rechenregeln

für Funktionen überein, d.h. die Reihe von Summe bzw. Produkt zweier analytischer Funktionen ist die Summe bzw. das Produkt der Reihen. Für konvergente Reihen ist es daher möglich, zwischen den beiden Aspekten (Reihe bzw. Funktion) hin– und herzuspringen.

Für Funktionen kann man auch die Exponentiation mit komplexen Zahlen definieren; dann gilt die Reihenentwicklung der Funktion $(1+X)^c$ auch für $c \in \mathbb{C}$. Für formale Reihen dagegen kann man nicht ohne weiteres eine sinnvolle Exponentiation mit komplexen Zahlen definieren, nur (bis auf Mehrdeutigkeit von Wurzeln) mit rationalen Zahlen.

Zwei andere wichtige konvergente Reihen sind (innerhalb ihres Konvergenzbereiches):

$$\sum_{n\in\mathbb{N}} \frac{X^n}{n!} = e^X \qquad\qquad \sum_{n\geqslant 1} \frac{(-1)^n X^n}{n} = \ln(1+X)$$

Zwei einfache Rekursionsgleichungen

Definition 2.2 *Für eine Folge von Zahlen* $a_0, a_1, a_2, \ldots$ *sei die* erzeugende Funktion *die Potenzreihe*

$$\sum_{n\in\mathbb{N}} a_n X^n$$

(Der Name ist gebräuchlich, aber unglücklich, denn die erzeugende Funktion definiert nur dann eine Funktion für Einsetzungen von X, wenn die Reihe konvergiert. *Erzeugende Reihe* wäre ein besserer Name.)

Typischerweise sind die a_n durch ein kombinatorisches Problem gegeben, also etwa die Anzahl von Permutationen von n Elementen oder die n-te Bellzahl. Durch Rechnen mit den erzeugenden Funktionen lassen sich nun viele kombinatorisch gegebene Zahlen bestimmen, insbesondere Rekursionsgleichungen auflösen.

Beispiel der Ordnung 1:

Sei t_n die Anzahl der Teilmengen einer n-Menge. Dann gilt die Rekursion $t_{n+1} = 2t_n$ (warum?); zusätzlich hat man den Anfangswert $t_0 = 1$. Also gilt

$$\sum_{n\in\mathbb{N}} t_n X^n = t_0 + \sum_{n\in\mathbb{N}} t_{n+1} X^{n+1} = 1 + \sum_{n\in\mathbb{N}} 2t_n X^{n+1} = 1 + 2X \cdot \sum_{n\in\mathbb{N}} t_n X^n$$

Es folgt $\displaystyle\sum_{n\in\mathbb{N}} t_n X^n = \frac{1}{1-2X} = \sum_{n\in\mathbb{N}} 2^n X^n$ und damit $t_n = 2^n$ für alle n.

Beispiel der Ordnung 2:

Die *Fibonacci–Zahlen* sind definiert durch die Anfangswerte $F_0 = 0, F_1 = 1$ und die Rekursion $F_{n+2} = F_n + F_{n+1}$. Also gilt hier:

$$\begin{aligned} F(X) := \sum_{n\in\mathbb{N}} F_n X^n &= 0 + 1\cdot X + \sum_{n\in\mathbb{N}} F_{n+2} X^{n+2} \\ &= X + \sum_{n\in\mathbb{N}} (F_n + F_{n+1}) X^{n+2} \\ &= X + X^2 \cdot \sum_{n\in\mathbb{N}} F_n X^n + X \cdot \sum_{n\in\mathbb{N}} F_{n+1} X^{n+1} \\ &= X + X^2 \cdot F(X) + X \cdot F(X) - X \cdot F_0 \end{aligned}$$

Es folgt also $F(X) = \dfrac{-X}{X^2+X-1}$. Jetzt muss man nur noch den Bruch als Reihe ausrechnen. Dazu bestimmt man die Nullstellen des Polynoms $X^2+X-1 = (X+\frac{1+\sqrt{5}}{2})(X+\frac{1-\sqrt{5}}{2})$. Durch Partialbruchzerlegung erhält man dann

$$\frac{-X}{X^2+X-1} = -X\cdot\Big(\frac{A}{X+\frac{1-\sqrt{5}}{2}} + \frac{B}{X+\frac{1+\sqrt{5}}{2}}\Big)$$

mit noch zu bestimmenden A und B. Ausrechnen der rechten Seite und Koeffizientenvergleich ergibt $A+B=0$ und $A\frac{1+\sqrt{5}}{2} + B\frac{1-\sqrt{5}}{2} = 1$, also $A = \frac{1}{\sqrt{5}}$ und $B = -\frac{1}{\sqrt{5}}$. Um die Summanden der Partialbruchzerlegung in eine Reihe zu entwickeln, braucht man folgende Variante der geometrischen Reihe:

$$\frac{a}{X+c} = \frac{a}{c}\cdot\frac{1}{1-\frac{1}{-c}X} = \frac{a}{c}\cdot\sum_{n\in\mathbb{N}}\Big(\frac{X}{-c}\Big)^n = \sum_{n\in\mathbb{N}}\frac{(-1)^n a}{c^{n+1}}\cdot X^n$$

Also gilt:

$$F(X) = \sum_{n\in\mathbb{N}}\left(\frac{(-1)^n A}{(\frac{1-\sqrt{5}}{2})^{n+1}} + \frac{(-1)^n B}{(\frac{1+\sqrt{5}}{2})^{n+1}}\right)\cdot X^{n+1},$$

woraus man nach Einsetzen von A und B (und nachdem man die Brüche auf den Hauptnenner gebracht hat), schließlich herausbekommt:

$$F(X) = \sum_{n\in\mathbb{N}}\frac{1}{\sqrt{5}}\left(\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\right)\cdot X^n$$

Wir haben also folgenden Satz gezeigt:

Satz 2.1 (Fibonacci–Zahlen) *Für die Fibonacci–Zahlen gilt*

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

Sie sind bestimmt durch die Anfangswerte $F_0 = 0$, $F_1 = 1$ *und die Rekursion* $F_{n+2} = F_n + F_{n+1}$ *bzw. durch die erzeugende Funktion* $F(X) = -\dfrac{X}{X^2+X-1}$.

Zur konkreten Berechnung der Fibonacci–Zahlen ist allerdings die Rekursion geeigneter als die explizite Formel, der man nicht einmal ansieht, dass sie natürliche Zahlen liefert.

Lösungsverfahren für lineare Rekursionsgleichungen endlicher Ordnung

Allgemeiner funktioniert dieses Verfahren für Rekursionsgleichungen der Form:

$$A_{n+k+1} = c_0 A_n + c_1 A_{n+1} + \cdots + c_k A_{n+k} \qquad (*)$$

Solch eine Rekursiongleichung heißt *lineare Rekursionsgleichung der Ordnung* $k+1$. Eine Lösung der Rekursionsgleichung besteht in einer Zahlenfolge, welche die Gleichung für alle n erfüllt. Die Menge aller (komplexwertiger) Zahlenfolgen bildet einen ($\mathbb{C}$)-Vektorraum. Man rechnet problemlos nach, dass die Lösungen von $(*)$ einen Unterraum bilden (d.h. die Summe zweier Lösungen und das Produkt einer Lösung mit einer konstanten Zahl sind wieder Lösungen. Insbesondere ist die konstane Nullfolge immer eine Lösung). Für beliebige $k+1$ Anfangswerte

$A_0, \ldots, A_k$ erhält man offensichtlich eine eindeutige Lösung. Der Lösungsraum ist also $(k+1)$-dimensional.

Um eine explizite Formel für die A_n zu erhalten, setzt man $A(X) := \sum_{n\in\mathbb{N}} A_n X^n$ als die erzeugende Funktion der A_n und formt um

$$\begin{aligned}
A(X) &= A_0 + A_1X + \cdots + A_kX^k + \sum_{n\in\mathbb{N}} A_{n+k+1}X^{n+k+1} \\
&= A_0 + A_1X + \cdots + A_kX^k + \sum_{n\in\mathbb{N}} \big(c_0A_n + c_1A_{n+1} + \cdots + c_kA_{n+k}\big)X^{n+k+1} \\
&= A_0 + A_1X + \cdots + A_kX^k + c_0X^{k+1}\cdot A(X) \\
&\qquad\qquad + c_1X^k \cdot A(X) - c_1A_0X^k \\
&\qquad\qquad + c_2X^{k-1}\cdot A(X) - c_2A_0X^{k-1} - c_2A_1X^k \\
&\qquad\qquad \vdots \\
&\qquad\qquad + c_kX \cdot A(X) - c_kA_0X - c_kA_1X^2 - \cdots - c_kA_{k-1}X^k,
\end{aligned}$$

so erhält man durch Auflösen:

Satz 2.2

$$A(X) = \frac{\textit{Polynom } P \textit{ in } X \textit{ vom Grad } \leqslant k}{1 - c_kX - c_{k-1}X^2 - \cdots - c_1X^k - c_0X^{k+1}}$$

wobei das Zählerpolynom $P(X)$ *folgendermaßen aussieht:*

$$\begin{aligned}
P(X) &= \big(A_k - c_1A_0 - c_2A_1 - \cdots - c_kA_{k-1}\big)\cdot X^k \\
&\quad + \big(A_{k-1} - c_2A_0 - c_3A_1 - \cdots - c_kA_{k-2}\big)\cdot X^{k-1} \\
&\quad + \cdots + \big(A_1 - c_kA_0\big)\cdot X + A_0
\end{aligned}$$

Wie im Fall der Fibonacci–Zahlen ergibt sich nun folgendes Lösungsverfahren:

(1) *Man bestimmt das Nennerpolynom* $Q(X)$ *und zerlegt es in Linearfaktoren.*

(2) *Man bestimmt die Partialbruchzerlegung von* $\frac{1}{Q(X)}$.

(3) *Jeden Summanden entwickelt man mit der Formel für die (hyper-)geometrische Reihe in eine Potenzreihe.*

(4) *Man summiert diese Potenzreihen und multipliziert das Ergebnis mit* $P(X)$.
Anschließend kann man die Formeldarstellung des Ergebnisses nach Möglichkeit noch vereinfachen.

Schwierig und im allgemeinen nicht möglich ist dabei nur der erste Schritt. Sofern dies geht, kann man sich in einem vereinfachten Verfahren einige Rechenarbeit sparen. Um dieses Verfahren plausibel zu machen, einige Vorüberlegungen:

Jede Nullstlle β von $Q(X)$ ergibt einen Summanden der Form $K\cdot\sum_n \beta^{-n}X^n$ in der gesuchten erzeugenden Funktion (K ist hier eine Konstante). Man kann sich übrigens schnell durch Einsetzen in $(*)$ davon überzeugen, dass $A_n = \alpha^n$ genau dann eine Lösung der Rekursiongleichung ist, wenn $\frac{1}{\alpha}$ eine Nullstelle von $Q(X)$ ist.

Wenn $Q(X)$ nur einfache Nullstellen β hat, kann man die Lösungsformel als Linearkombination der β^{-n} ansetzen. Ist β mehrfache Nullstelle , etwa mit Vielfachheit d, so ergeben sich aus dem

Lösungsverfahren wegen $\frac{1}{(1-X)^m} = \sum_{n\in\mathbb{N}} \binom{m+n-1}{n} X^n$ auch Summanden der Form:

$$K' \cdot \sum_n (\text{Polynom in } n \text{ vom Grad} \leqslant d-1) \cdot \beta^{-n} X^n.$$

Die Lösungsformel der A_n wird daher eine Linearkombination von Ausdrücken der Form $n^j \cdot \beta^{-n}$ mit $0 \leqslant j < d$ sein. Dies stimmt dann wieder genau mit der Dimension ds Lösungsraumes überein.

Nun kann man noch das Bestimmen von Q vereinfachen: Angenommen $Q(X) = -c_0 \cdot \prod_{i=0}^{k} (X - \beta_i)$. Durch Einsetzen von $X = Y^{-1}$ und Durchmultiplizieren mit Y^{k+1} erhält man

$$-c_0 - c_1 Y - \cdots - c_k Y^k + Y^{k+1} = -c_0 \prod_{i=0}^{k} (1 - Y\beta_i) = \pm c_0 \beta_0 \cdots \beta_k \prod_{i=0}^{k} (Y - \frac{1}{\beta_i})$$

(denn da Q den konstanten Term 1 hat, sind alle $b_i \neq 0$). Die Nullstellen von $Q(X)$ sind also genaue die Kehrwerte der Nullstellen des *reflektierten* Polynoms

$$x^{k+1} = c_0 + c_1 x + \cdots + c_k x^k \qquad (**)$$

Dieses Polynom heißt auch *charakteristisches Polynom* der Rekursiongleichung $(*)$. Man sieht auch, dass man es ganz leicht aus der Rekursionsgleichung $(*)$ ablesen kann, indem man A_{n+i} durch X^i ersetzt.

Zusammengefasst hat man also folgendes

Vereinfachtes Verfahren zur Lösung linearer Rekursionsgleichungen:

Betrachten man A_n als Funktion $\mathbb{N} \to \mathbb{C}, n \mapsto A_n$, so bilden die Lösungen der Rekursionsgleichung $(*)$ einen $k+1$-dimensionalen Unterraum von $\mathrm{Abb}(\mathbb{N}, \mathbb{C})$*. Eine Basis dieses Lösungsraumes ist durch*

$$\left\{ \alpha_i^n,\ n \cdot \alpha_i^n,\ \ldots,\ n^{d_i - 1} \alpha_i^n \;\middle|\; i = 1, \ldots, m \right\}$$

gegeben, wobei die $\alpha_1, \ldots, \alpha_m$ die verschiedenen Nullstellen des charakteristischen Polynoms $(**)$ mit jeweiliger Vielfachheit d_i sind. Jede andere Lösung ist dann eine Linearkombination

$$\sum_{i=1}^{m} \left(k_{i1} \alpha_i^n + k_{i2} n \alpha_i^n + \cdots + k_{id_i} n^{d_i - 1} \alpha_i^n \right)$$

Durch Vergleich der Werte für $n = 0, \ldots, k$ mit $k+1$ Anfangswerten $A_0, \ldots, A_k$ ermittelt man die eindeutg bestimmten Konstanten $k_{ij} \in \mathbb{C}$.

Ein Beispiel: Sei die Rekursionsgleichung

$$A_{n+3} = -12A_n + 8A_{n+1} + A_{n+2}$$

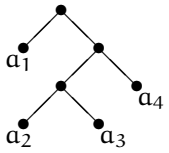
gegeben. Das charakteristische Polynom ist $X^3 - X^2 - 8X + 12 = (X-2)^2(X+3)$. Eine Basis der Lösungsmenge ist also durch $\left\{ 2^n, n \cdot 2^n, (-3)^n \right\}$ gegeben, die Lösungen sind genau die Folgen der Form $k_1 2^n + k_2 n 2^n + k_3 (-3)^n$. Für gegebene Anfangswerte A_0, A_1, A_2 erhält man dann für $n = 0, 1, 2$ die eindeutig nach k_1, k_2, k_3 auflösbaren Gleichungen

$$\begin{aligned} k_1 + k_3 &= A_0 \\ 2k_1 + 2k_2 - 3k_3 &= A_1 \\ 4k_1 + 8k_2 + 9k_3 &= A_2 \end{aligned}$$

Eine nicht lineare Rekursionsgleichung

Die *Catalan–Zahl* C_n gibt die Anzahl der Möglichkeiten an, einen Ausdruck $a_1+\cdots+a_n$ sinnvoll zu klammern. Pro Pluszeichen gibt es also ein Klammerpaar (wobei das äußerste Klammerpaar weggelassen werden kann), die eine eindeutige Weise festlegen, in der die Summe ausgerechnet werden kann. Es ist dann $C_1 = 1$, und per Konvention sei $C_0 = 0$.

Man sieht sofort, dass C_n auch die Anzahl der *binären Bäume* (genauer: geordnete vollständige binäre Wurzelbäume) mit n Blättern ist (für die genaue Definition siehe Seite 50). Rechts der $a_1 + ((a_2 + a_3) + a_4)$ entsprechende Baum.



Aus der Baumdarstellung sieht man durch Weglassen der *Wurzel* (d.h. des obersten Knotens in der Darstellung oben), dass die Catalan–Zahlen die Rekursionsgleichung $C_n = \sum_{j=1}^{n-1} C_j \cdot C_{n-j}$ für $n \geqslant 2$ erfüllen; j zählt die Anzahl der auf der einen Seite verbleibenden Blätter. Wegen der Konvention $C_0 = 0$ folgt also $C_n = \sum_{j=0}^{n} C_j \cdot C_{n-j}$ für alle $n \neq 1$. Setzt man $C(X) := \sum_{n\in\mathbb{N}} C_n X^n$, so sieht man:

$$C(X)^2 = \sum_{n\in\mathbb{N}} \sum_{j=0}^{n} C_j C_{n-j} X^n = C(X) - X,$$

der „Korrekturterm“ $-X$ kommt daher, dass $C_1 = 1$, aber $C_0C_1 + C_1C_0 = 0$.

Um $C(X)$ zu berechnen, muss man also eine quadratische Gleichung lösen. Man kann leicht nachrechnen, dass die Lösungsformel für quadratische Gleichungen immer dann tatsächlich Lösungen liefert, wenn man die nötigen Wurzeln ziehen kann und wenn die üblichen Rechenregeln für Addition, Subtraktion und Multiplikation gelten. Das zweite gilt in jedem Ring, also insbesondere in $\mathbb{C}[[X]]$ (und wenn der Ring ein sogenannter Integritätsbereich ist, d.h. sich zu einem Körper erweitern lässt, was für $\mathbb{C}[[X]]$ der Fall ist, dann gibt es sogar keine anderen Lösungen). Die binomische Reihe erlaubt es, Wurzeln aus Reihen mit konstantem Term 1 zu ziehen. Wir erhalten also

$$C(X) \;=\; \frac{1}{2}\bigl(1 \pm \sqrt{1-4X}\bigr) \;=\; \frac{1}{2} \pm \frac{1}{2} \cdot \sum_{k\geqslant 0} \binom{\frac{1}{2}}{k} \cdot (-4X)^k$$

Jede der beiden Möglichkeiten erfüllt die Rekursionsgleichung; die mit dem Minuszeichen liefert zusätzlich den richtigen Anfangswert $C(0) = C_0 = 0$, ist also die tatsächliche Lösung. Daraus bestimmt man nach einigem Rechnen eine hübsche explizite Formel:

Satz 2.3 (Catalan–Zahlen) *Für die Catalan–Zahlen gilt*

$$C_n = \frac{1}{n}\binom{2n-2}{n-1}.$$

Sie sind bestimmt durch die Rekursion

$$C_n = \sum_{j=1}^{n-1} C_j \cdot C_{n-j}$$

mit Anfangswerten $C_0 = 0$ und $C_1 = 1$. Ihre erzeugende Funktion ist die Lösung der Gleichung $C(X) = X + C(X)^2$ mit Anfangswert $C_0 = 0$.

(Wer den Überlegungen, die zu diesem Ergebnis führen, nicht traut, kann versuchen, für die explizite Formel nachzurechnen, dass die Rekursionsgleichung erfüllt ist. Eine Alternative besteht darin, durch Weglassen eines beliebigen Blattes eine andere Rekursionsgleichung zwischen C_{n+1} und C_n aufzustellen.)

Exponentielle erzeugende Funktionen

In vielen Fällen ist es nützlich, eine Variante der erzeugenden Funktionen zu betrachten:

Definition 2.3 *Für eine Folge von Zahlen* $a_0, a_1, a_2, \ldots$ *sei*

$$\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n$$

die exponentielle erzeugende Funktion.

Insbesondere wenn Permutationen im Spiel sind, etwa wenn die Elemente eines kombinatorischen Objektes durchnumeriert sind und jede Umsortierung ein neues Objekt ergibt, ist diese Normierung mit $n!$ sinnvoll. Außerdem erhält man so eher konvergente Reihen!

Als Rechenregeln ergeben sich für die exponentiellen erzeugenden Funktionen:

(1) $$\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n + \sum_{n\in\mathbb{N}} \frac{b_n}{n!} X^n = \sum_{n\in\mathbb{N}} \frac{(a_n + b_n)}{n!} X^n$$

(2) $$\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n \cdot \sum_{n\in\mathbb{N}} \frac{b_n}{n!} X^n = \sum_{n\in\mathbb{N}} \frac{1}{n!} \Big(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \Big) X^n$$

(3) $$\frac{d}{dX}\Big(\sum_{n\in\mathbb{N}} \frac{a_n}{n!} X^n \Big) = \sum_{n\in\mathbb{N}} \frac{a_{n+1}}{n!} X^n$$

Die formale Ableitung entspricht also gerade einem Shift in der Folge der Koeffizienten. Die Exponentialfunktion ist die der konstanten Folge $1, 1, \ldots$ zugehörige exponentielle erzeugende Funktion.

Rechnet man mit den exponentiellen erzeugenden Funktionen statt mit den gewöhnlichen, so werden die linearen Rekursionsgleichungen zu linearen Differentialgleichungen. Im Fall der Fibonacci–Zahlen erhält man mit $\tilde{F}(X) = \sum_{n\in\mathbb{N}} \frac{F_n}{n!} X^n$

$$\tilde{F}(X) = \sum_{n\in\mathbb{N}} \frac{F_{n+2} - F_{n+1}}{n!} X^n = \frac{d^2}{dX^2}\tilde{F}(X) - \frac{d}{dX}\tilde{F}(X),$$

also die Differentialgleichung: $\tilde{F}(X)'' - \tilde{F}(X)' - \tilde{F}(X) = 0$. (Daraus erklärt sich die Analogie zwischen den Lösungsverfahren für lineare Rekursionsgleichungen und dem für lineare Differentialgleichungen. Der Rechenaufwand verringert sich freilich durch diese Betrachtungsweise nicht.)

Anwendung auf die Bell–Zahlen

Für die exponentielle erzeugende Funktion der Bell–Zahlen, $\tilde{B}(X)$, erhalten wir folgende Differentialgleichung:

$$\frac{d}{dX}\tilde{B}(X) = \sum_{n\in\mathbb{N}} \frac{B_{n+1}}{n!} X^n = \sum_{n\in\mathbb{N}} \frac{1}{n!} \Big(\sum_{k=0}^{n} \binom{n}{k} B_k \Big) X^n = \sum_{n\in\mathbb{N}} \frac{X^n}{n!} \cdot \sum_{n\in\mathbb{N}} \frac{B_n}{n!} X^n = \exp(X) \cdot \tilde{B}(X)$$

Diese Differentialgleichung wollen wir nun lösen:

Satz 2.4 (Exponentielle erzeugende Funktion der Bell–Zahlen; explizite Formel)

$$\tilde{B}(X) = e^{e^X - 1} \qquad\qquad B_n = \frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}$$

Beweis: Dieser Beweis geht davon aus, dass die exponentielle erzeugende Funktion der Bell–Zahlen konvergiert (dies müsste man durch Abschätzungen und Konvergenzbetrachtungen erst noch beweisen), rechnet also mit Funktionen. Während das Ergebnis für die exponentielle erzeugende Funktion dann auch ohne Konvergenzbetrachtung gilt (wobei man noch definieren muss, was die Einsetzung einer Reihe in eine andere Reihe bedeutet), ist die explizite Formel für die Bell–Zahlen ohne Konvergenz sinnlos.

Da $B_0 = 1$, brauchen wir nur Lösungen der Differentialgleichung mit konstantem Koeffizienten $\neq 0$ zu betrachten, können also beliebig dividieren. Wie man leicht nachrechnet, ist e^{e^X} eine Lösung. Sind $\tilde{B}_1(X), \tilde{B}_2(X)$ zwei Lösungen, so folgt nach Division und Umformung die Gleichheit $\tilde{B}_1'(X)/\tilde{B}_1(X) = \tilde{B}_2'(X)/\tilde{B}_2(X)$ der logarithmischen Ableitungen $\tilde{B}_i'(X)/\tilde{B}_i(X) = \ln(\tilde{B}_i(X))'$. Daraus erhält man leicht, dass sich $\tilde{B}_1$ und $\tilde{B}_2$ nur um einen konstanten Faktor voneinander unterscheiden können. Also gilt $\tilde{B}(X) = c \cdot e^{e^X}$ und mit dem Anfangswert $B_0 = 1$ findet man $c = \frac{1}{e}$. Nun folgt:

$$\tilde{B}(X) = e^{e^X - 1} = \frac{1}{e}\cdot e^{e^X} = \frac{1}{e}\sum_{k\in\mathbb{N}}\frac{e^{Xk}}{k!} = \frac{1}{e}\sum_{k\in\mathbb{N}}\Big(\frac{1}{k!}\cdot\sum_{n\in\mathbb{N}}\frac{X^n k^n}{n!}\Big) = \sum_{n\in\mathbb{N}}\Big(\frac{1}{e}\cdot\sum_{k\in\mathbb{N}}\frac{k^n}{k!}\Big)\frac{X^n}{n!}$$

Damit liefert Koeffizientenvergleich die explizite Formel für die Bell–Zahlen. □

Obwohl die explizite Formel eine unendliche Summe beinhaltet, könnte man sie zur Berechnung der Bell–Zahlen heranziehen, wenn man durch Konvergenzbetrachtungen zunächst Schranken N bestimmt mit $B_n = \big\lceil \frac{1}{e}\sum_{k=0}^{N}\frac{k^n}{k!}\big\rceil$. Wegen des hohen Rechenaufwandes für die Potenzen k^n liefern die Rekursionsformeln schnellere Verfahren.

Noch ein Beispiel ...

Satz 2.5 (Erzeugende Funktion der Partitionszahlen)
Für die (normale) erzeugende Funktion der Partitionszahlen $P(X) := \sum_{n\in\mathbb{N}} P_n X^n$ *gilt*

$$P(X) = \prod_{n\geqslant 1}\frac{1}{1-X^n} = (1 + X + X^2 + \cdots)(1 + X^2 + X^4 + \cdots)(1 + X^3 + X^9 + \cdots)\cdots$$

(Dabei ist ein unendliches Produkt formaler Reihen gar nicht definiert und im allgemeinen auch nicht sinnvoll definierbar. Man kann es als eine Gleichheit konvergenter Reihen innerhalb des Konvergenzbereiches, z.B. für $|X| < 1$, betrachten. In dem besonderen Fall hier ist auch eine formale Definition möglich, da es insgesamt nur endlich viele Terme $\neq 1$ festen Grades gibt: Man kann das Produkt formal ausmultiplizieren; dabei gibt es Produkte mit unendlich vielen Monomen X^i mit $i > 0$ – diese werden weggelassen (man kann sich X als unendlich klein

vorstellen, um dies zu motivieren) – und Produkte aus endlich vielen Monomen X^i mit $i > 0$ und unendlich oft 1 – dies ergibt ein X^n, wobei für festen n nur endlich viele X^n vorkommen, die man alle aufsummieren kann.)

BEWEIS: Durch Ausmultiplizieren erhält man einen Term X^n genau aus $X^{a_1}(X^2)^{a_2}\cdots(X^k)^{a_k}$, wobei $a_1 + 2a_2 + \cdots + ka_k = n$. Dies entspricht der Partition

$$n = \underbrace{1+\cdots+1}_{a_1 \text{ mal}} + \underbrace{2+\cdots+2}_{a_2 \text{ mal}} + \cdots + \underbrace{k+\cdots+k}_{a_k \text{ mal}} \qquad \square$$

Von dieser Darstellung der erzeugenden Funktion kommt man mit einiger (nicht offensichtlicher) Arbeit zur Rekursionsgleichung auf Seite 16.

I.3 Größenwachstum von Funktionen

Größenvergleich von Funktionen, Definitionen

Falls eine explizite Darstellung einer Zählfunktion nicht möglich ist, kann man eventuell eine Einschätzung des Größenwachstum erhalten. Zum Beispiel legt ein Vergleich der ersten Werte nahe, dass B_n stärker wächst als 2^n und schwächer als $n!$.

Obwohl wir in der Regel nur an Zählfunktionen $\mathbb{N} \to \mathbb{N}$ interessiert sind, ist es günstig, die Definitionen allgemein für Funktionen $\mathbb{N} \to \mathbb{C}$ einzuführen. Um dabei Größen vergleichen zu können, muss man mit Beträgen arbeiten. Stattdessen könnte man auch nur positive Funktionen $f : \mathbb{N} \to \mathbb{R}_0^+$ betrachten.

Eine Grundannahme für dieses Abschnitt sei, dass alle betrachteten Funktionen $f : \mathbb{N} \to \mathbb{C}$, die im Nenner eines Bruches auftreten, nur endlich viele Nullstellen haben mögen. Die endlich vielen undefinierten Stellen sind dann bei den folgenden Grenzwertbetrachtungen unerheblich.

Definition 3.1

„g *wächst stärker als* f“:	$f \ll g$	$:\Longleftrightarrow$	$\lim\limits_{n\to\infty} \frac{\lvert f(n)\rvert}{\lvert g(n)\rvert} = 0$
„f *und* g *sind asymptotisch gleich*“	$f \sim g$	$:\Longleftrightarrow$	$\lim\limits_{n\to\infty} \frac{\lvert f(n)\rvert}{\lvert g(n)\rvert} = 1$
„*klein o von* g“	$o(g)$	$:=$	$\{f \mid f \ll g\}$

(f und g sollen auch dann asymptotisch gleich sein, wenn $f = g$ gilt — zum Beispiel für die konstanten Nullfunktion folgt dies nicht aus der Definition oben.)

Man schreibt in der Regel leider $f = o(g)$ statt $f \in o(g)$. Meist taucht die Notation in Ausdrücken wie $f = h + o(g)$ auf, was für $f - h \in o(g)$ steht und intuitiv bedeutet, dass f und h für große Werte übereinstimmen bis auf einen Fehler, der weniger stark wächst als g.

Per Definition gilt also: $f \ll g \iff f \in o(g)$, und zur Erinnerung: Die Grenzwertbedingung dafür bedeutet $\forall \varepsilon > 0 \quad \exists n_\varepsilon \quad \forall n \geqslant n_\varepsilon \quad |f(n)| \leqslant \varepsilon \cdot |g(n)|$.

Beispiele:

$f \in o(1) \iff \lim\limits_{n\to\infty} f(n) = 0$

$f \in o(n) \iff \lim\limits_{n\to\infty} \frac{f(n)}{n} = 0$, also etwa konstante Funktionen f.

Satz 3.1

(a) $\sim$ *ist eine Äquivalenzrelation und* $\ll$ *ist eine strikte partielle Ordnungsrelation (d.h. transitiv und irreflexiv).*

(b) *Verträglichkeit von* $\ll$ *mit* $\sim$*: falls* $f \ll g$ *und* $f \sim f'$, $g \sim g'$, *so gilt auch* $f' \ll g'$.

(c) *Verträglichkeit von* $\ll$ *mit der algebraischen Struktur:*

- $f_1 \ll g, f_2 \ll g \Longrightarrow \alpha f_1 + \beta f_2 \ll g$ *für alle* $\alpha, \beta \in \mathbb{C}$*; also ist* $o(g)$ *ein Untervektorraum von* $\mathrm{Abb}(\mathbb{N}, \mathbb{C})$.
- $f \ll g \Longrightarrow fh \ll gh$ *(für* h *mit endlich vielen Nullstellen) und* $f \sim g \Longrightarrow fh \sim gh$.
- *Insbesondere gilt* $f \ll g \iff \frac{1}{g} \ll \frac{1}{f}$ *und* $f \sim g \iff \frac{1}{g} \sim \frac{1}{f}$

Beweis: Einfaches Nachrechnen. Zum Beispiel (b):

$$\lim \frac{f'(n)}{g'(n)} = \lim \left(\frac{f'(n)}{f(n)} \frac{f(n)}{g(n)} \frac{g(n)}{g'(n)} \right) = \lim \frac{f'(n)}{f(n)} \lim \frac{f(n)}{g(n)} \lim \frac{g(n)}{g'(n)} = 0$$

Für den letzten Punkt von e) multipliziert man mit $h = (fg)^{-1}$. □

Wegen (b) induziert $\ll$ eine partielle Ordnung auf den $\sim$-Klassen. Auch dies ist keine totale Ordnung, da man einfach Beispiele findet, wo der Grenzwert $\lim_{n\to\infty} \frac{|f(n)|}{|g(n)|}$ nicht existiert.

Beispiele:

- Für Polynome f, g gilt:

$$f \ll g \iff \mathrm{grad}(f) < \mathrm{grad}(g)$$
$$f \sim g \iff \mathrm{grad}(f) = \mathrm{grad}(g) \text{ und im Absolutbetrag gleicher Leitkoeffizienten}$$

- Für $0 < a < b$ und $1 < c < d$ weiß man:

$$\text{konstante Fkt} \ll \log\log(n) \ll \log(n) \ll n^a \ll n^b \ll c^n \ll d^n \ll n! \ll n^n$$

- Logarithmen verschiedener Basen $a > 1, b > 1$ wachsen „gleich schnell“, ohne für $a \neq b$ asymptotisch gleich zu sein, da (vergleiche Seite 35)

$$\lim_{n\to\infty} \frac{\log_a(n)}{\log_b(n)} = \log_a(b)$$

Aus $f \ll g$ folgt im allgemeinen nicht $h \circ f \ll h \circ g$, nicht einmal fur monoton wachsende Funktionen h, denn $c^n \ll d^n$, aber $\log_c(c^n) = n \not\ll \log_c(d) \cdot n = \log_c(d^n)$.

Logarithmen verhalten sich also wie Polynome gleichen Grades; dafür fehlt noch ein „Zwischenbegriff“:

Definition 3.2

$$O(g) := \{ f \mid \exists C > 0\, \exists n_0\, \forall n \geq n_0 : |f(n)| \leqslant C \cdot |g(n)| \}$$
$$\Omega(g) := \{ f \mid \exists C' > 0\, \exists n_0\, \forall n \geqslant n_0 : C' \cdot |g(n)| \leqslant |f(n)| \} \qquad = \{ f \mid g \in O(f) \}$$
$$\Theta(g) := \{ f \mid \exists C, C' > 0\, \exists n_0\, \forall n \geqslant n_0 : C' \cdot |g(n)| \leqslant |f(n)| \leqslant C \cdot |g(n)| \} = O(g) \cap \Omega(g)$$

Die für o üblichen Schreibweisen werden auch für O, Ω und Θ verwendet, etwa $f = \Omega(g)$ statt $f \in \Omega(g)$.

Beispiel: Für Polynome f, g gilt:

$$f \in O(g) \iff grad(f) \leqslant grad(g)$$
$$f \in \Omega(g) \iff grad(f) \geqslant grad(g)$$
$$f \in \Theta(g) \iff grad(f) = grad(g)$$

Satz 3.2

(a) $f \in O(g)$ *definiert eine Quasi– oder Präordnung (reflexiv und transitiv), die* $\ll$ *echt vergröbert, d.h.* $f \ll g \Longrightarrow f \in O(g)$*, aber die Umkehrung gilt im allgemeinen nicht.*

(b) $f \in \Theta(g)$ *ist die von dieser Präordnung induzierte Äquivalenzrelation. Sie ist echt gröber als* $\sim$ *ist, d.h.* $f \sim g \Longrightarrow f \in \Theta(g)$*, aber die Umkehrung gilt im allgemeinen nicht.*

(c) *Verträglichkeit mit* $\ll$*:* $\quad f' \in O(f), g' \in \Omega(g), f \ll g \Longrightarrow f' \ll g'$.

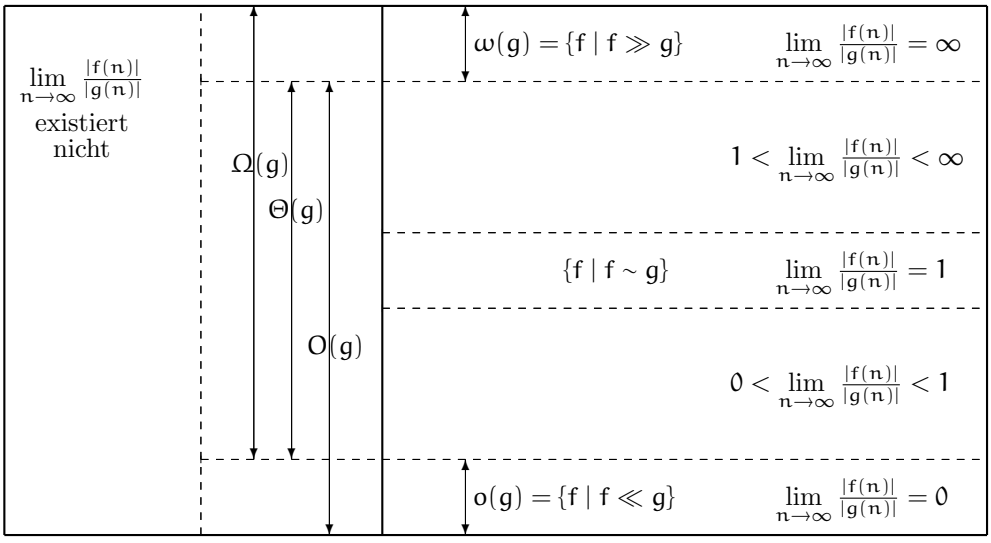
(d) *Verträglichkeit mit der algebraischen Struktur:*

- $f_1, f_2 \in O(g) \Longrightarrow \alpha f_1 + \beta f_2 \in O(g)$ *für alle* $\alpha, \beta \in \mathbb{C}$*; also ist* $O(g)$ *ein Untervektorraum von* $\mathrm{Abb}(\mathbb{N}, \mathbb{C})$.
- $f \in \Theta(g) \Longrightarrow fh \in \Theta(gh)$.

Beweis: Nachrechnen auf Grundlage von Satz 3.1. Beispiele dafür, dass die Umkehrungen nicht gelten, liefern die Polynome. □

$\Omega(g)$ und $\Theta(g)$ sind keine Untervektorräume; $o(g)$ ist ein Teilraum von $O(g)$.

Wegen (c) induziert $\ll$ auch eine partielle Ordnung auf den Θ-Klassen. Falls der Grenzwert $\lim\limits_{n\to\infty} \frac{|f(n)|}{|g(n)|}$ existiert, so gilt entweder $f \ll g$ oder $f \in \Theta(g)$ oder $f \gg g$. Setzt man noch $\omega(g) := \{f \mid g \ll f\} = \{f \mid g \in o(f)\}$, so ergibt sich folgendes Bild, für eine feste Funktion g:



Bemerkung: Für eine Funktion $f \in O(g)$ muss der Grenzwert $\lim\limits_{n\to\infty} \frac{|f(n)|}{|g(n)|}$ nicht unbedingt existieren!

Wie schnell wächst die Fakultätsfunktion?

Im folgenden soll „log“ für einen Logarithmus fester Basis > 1 stehen.

Satz 3.3 $\log(n!) \sim n \cdot \log n$

Beweis: Da sich der Logarithmus zu einer Basis durch einen konstanten Faktor in den Logarithmus zu einer anderen Basis umrechnet, kann man mit dem natürlichen Logarithmus „ln“ arbeiten. Wegen $\ln(n!) = \sum_{k=1}^{n} \ln(k)$ kann man $\ln(n!)$ als Ober– bzw. Untersumme für das Integral $\int \ln(x)dx$ mit Stammfunktion $x \ln x - x$ ansetzen, bekommt also die Abschätzungen

$$\ln(n-1)! = \sum_{k=1}^{n-1} \ln(k) \leqslant \int_1^n \ln(x)dx = n \ln n - n + 1 \leqslant \sum_{k=1}^{n} \ln(k) = \ln(n!)$$

und daraus

$$1 - \frac{\ln n}{\ln(n!)} = \frac{\ln(n!/n)}{\ln(n!)} = \frac{\ln((n-1)!)}{\ln(n!)} \leqslant \frac{n \ln n}{\ln(n!)} - \frac{n-1}{\ln(n!)} \leqslant \frac{\ln(n!)}{\ln(n!)} = 1$$

Außerdem bekommt man aus der gleichen Abschätzung

$$\frac{\ln(n!)}{n-1} \geqslant \frac{n \ln n - (n-1)}{n-1} = \frac{n}{n-1} \ln(n) - 1 \longrightarrow +\infty$$

Also hat man $\frac{n-1}{\ln n!} \to 0$ und erst recht $\frac{\ln n}{\ln n!} \to 0$, und daraus folgt mit der Abschätzung oben $\frac{n \ln n}{\ln(n!)} \to 1$. □

Auch an diesem Beispiel sieht man, dass aus $f \sim g$ nicht notwendig $h \circ f \sim h \circ g$ folgt, da $e^{\ln(n!)} = n! \not\sim n^n = e^{n \ln n}$.

Wenn man die Abschätzung $n \ln n - n + 1 \leqslant \ln(n!) \leqslant (n+1)\ln(n+1) - n$ aus dem Beweis von Satz 3.3 exponenziert, erhält man

$$\frac{n^n}{e^{n-1}} \leqslant n! \leqslant \frac{(n+1)^{n+1}}{e^n} = \frac{n^n}{e^{n-1}}(n+1)\frac{1}{e}\left(\frac{n+1}{n}\right)^n \leqslant \frac{n^n}{e^{n-1}}(n+1).$$

Dies zeigt, dass das Wachstum von $n!$ grob zwischen $(\frac{n}{e})^n$ und $(\frac{n}{e})^{n+1}$ liegt. Mit einiger Mehrarbeit kann man diese Überlegungen zu einer asymptotische Bestimmung der Fakultätsfunktion verfeinern:

Satz 3.4 (Stirlingsche Formel)

$$\begin{aligned} n! &\sim \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n = \frac{\sqrt{2\pi}}{e^n} \cdot n^{n+\frac{1}{2}} \\ n! &= \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{12}n + O\left(\frac{1}{n^2}\right)\right) \end{aligned}$$

Für den Fehler gibt es noch deutlich genauerer Abschätzungen.

(Die Stirling–Formel beweise ich hier nicht. Man kann z.B. die Γ-Funktion $\Gamma(x) = \int_0^\infty t^{x-1}e^t dt$ zu Hilfe nehmen, die eine glatte Interpolation der Fakultätsfunktion zu einer reellen Funktion darstellt. Es gilt nämlich $n! = \Gamma(n+1) = \int_0^\infty t^n e^t dt$.)

Wie schnell wachsen die Bellzahlen?

Für die Bellzahlen gibt es ebenfalls asymptotische Formeln, in denen aber andere, in dieser Vorlesung nicht behandelte Funktionen vorkommen. Für das Verhältnis $\ln(B_n)$ zu n (also in etwa: Anzahl der Ziffern von B_n im Verhältnis zu n) gibt es aber ein Formeln, die schön zeigt, wie man sich auch im sublogarithmischen Bereich durch im $\ll$-Sinne immer kleinere Funktionen dem Fehler annähert. Es gilt (ohne Beweis):

$$\frac{\ln B_n}{n} = \ln n - \ln(\ln n) - 1 + \frac{\ln(\ln n)}{\ln n} + \frac{1}{\ln n} + \frac{1}{2}\Big(\frac{\ln(\ln n)}{\ln n}\Big)^2 + O\Big(\frac{\ln(\ln n)}{(\ln n)^2}\Big)$$

Größenwachstum von Rekursionen

In manchen Fällen ist es schwierig, explizite Lösungen für Rekursionsgleichungen zu finden; Wachstumsabschätzungen dagegen erhält man leicht:

Satz 3.5 *Seien $a \geqslant 1, b > 1, c$ gegeben und $A(n)$ bestimmt durch eine der beiden Rekursionsformeln*

$$A(n) = a \cdot A\left(\left\lceil \frac{n}{b} \right\rceil\right) + c \qquad A(n) = a \cdot A\left(\left\lfloor \frac{n}{b} \right\rfloor\right) + c$$

und den Anfangswert $A(1)$ bzw. $A(0)$. Dann gelten folgende Wachstumsabschätzungen für A:

$$A \in \Theta(\log n) \quad \textit{falls } a = 1$$
$$A \in \Theta\big(n^{\log_b a}\big) \textit{ falls } a > 1$$

Beweis: Man überlege sich zunächst, dass A (schwach) monoton verläuft. Dies folgt per Induktion, weil alle in der Rekursionformel vorkommenden Ausdrücke (einschließlich Gaussklammer) schwach monotone Funktionen definieren und die Verkettung monotoner Funktionen wieder monoton ist. Für $n = b^k$ ergibt sich aus der Rekursionsformel $A(b^k) = a^k \cdot A(1) + c \cdot \sum_{j=0}^{k-1} a^j$.

Für $a = 1$ ist also $A(b^k) = A(1) + kc$, somit gilt $A(b^k) \in \Theta(k)$ und wegen der Monotonie $A(n) \in \Theta(\log n)$.

Für $a = 1$ ist $A(b^k) = a^k \cdot A(1) + c\frac{a^k-1}{a-1}$. Wegen $x^{k-1} \ll x^k$ folgt daraus $A(b^k) \in \Theta(a^k)$ und wiederum aus der Monotonie erhält man, dass $A(n) = A(b^{\log_b n})$ im Θ-Sinne wie $a^{\log_b n} = n^{\log_b a}$ wächst. □

Erinnerung an Logarithmenrechnung:

$$\log_a(b) = \log_a(n^{\log_n(b)}) = \log_a(n) \cdot \log_n(b) = \frac{\log_a(n)}{\log_b(n)}.$$

Daraus ergibt sich

$$n^{\log_b(a)} = n^{\log_b(n)\log_n(a)} = \big(n^{\log_n(a)}\big)^{\log_b(n)} = a^{\log_b(n)}.$$

Teil II: Graphen

Graphen sind grundlegende mathematische Strukturen, die in vielen Anwendungen, insbesondere auch in der Informatik, auftreten. Anschaulich ist ein Graph eine Menge von Punkten mit Verbindungen, wie sie etwa im Modell eines Wegenetzes vorkommen. In gewissem Sinne sind Graphen die einfachsten mathematischen Strukturen, in denen bereits Phänomene größtmöglicher Komplexität auftauchen. Graphen sind in der Informatik nicht nur für die Modellierung wichtig, sondern auch, weil viele in der Informatik auftretende Strukturen (z.B. Programme, Webseiten) Graphen zugrundeliegen.

II.4 Definition und Begriffe

Mehrere Definitionen von Graphen sind möglich und in der Literatur vertreten; einige Varianten sind auf Seite 40 dargestellt. In der Regel aber werden Graphen so definiert, dass weder Schleifen (auch Schlingen genannt), d.h. Verbindungen eines Punktes mit sich selbst, noch Mehrfachkanten, d.h. mehrere Verbindungen zwischen denselben Punkten, erlaubt sind. Für diesen Begriff von Graphen gibt es mehrere gleichwertige Möglichkeiten, ihn mathematisch zu modellieren:

- Man hat eine Menge E von *Ecken* (auch Knoten, engl. vertices), eine Menge K von *Kanten* (engl.: edges) und eine *Inzidenzrelation* zwischen E und K, die jeder Kante genau zwei Ecken zuordnet und so, dass es für jedes Paar von Ecken höchstens eine Kante gibt. Anschaulich sind eine Ecke und eine Kante inzident, wenn die Kante von der Ecke ausgeht.
- Oder man hat die Menge E von Ecken und identifiziert jede Kante mit der zweielementigen Teilmenge von E der zu ihr inzidenten Ecken; man betrachtet K also als Teilmenge der zweielementigen Teilmengen $\mathfrak{P}_2(\mathsf{E})$ von E. Eine Kante k ist dann von der Form $\mathsf{k} = \{\mathsf{e}_1, \mathsf{e}_2\}$.
- Oder man betrachtet K als eine zweistellige, irreflexive, symmetrische Relation auf E. Man schreibt dann $\mathsf{e}_1 \mathsf{K} \mathsf{e}_2$ oder $(\mathsf{e}_1, \mathsf{e}_2) \in \mathsf{K}$ dafür, dass e_1 und e_2 in der Kantenrelation zueinander stehen, also dass es eine Kante zwischen e_1 und e_2 gibt.

Ich werde meist mit der dritten Art arbeiten; bisweilen aber auch K als die Menge der Kanten auffassen.

Zwei verschiedene Ecken $\mathsf{e}_1, \mathsf{e}_2$ heißen *benachbart* oder *adjazent*, wenn sie durch eine Kante verbunden sind. Die Menge der *Nachbarn* von e sei $\mathsf{N}(\mathsf{e})$ und $\mathsf{d}(\mathsf{e}) := |\mathsf{N}(\mathsf{e})|$ heißt der *Grad* (oder die Valenz) von e.

Für die Größe eines Graphen gibt es zwei Parameter: die Anzahl der Ecken, auch *Ordnung* des Graphen genannt, und die Anzahl der Kanten, auch *Größe* des Graphen genannt. Wir werden nur endliche Graphen betrachten, d.h. Graphen endlicher Ordnung. Diese haben dann auch automatisch nur endliche viele Kanten.

Möchte man die Komplexität von Algorithmen auf Graphen berechnen, muss man festlegen, welches Maß für die Größe eines Graphen zugrundegelegt wird. Wegen

$$|K| \leqslant \binom{|E|}{2} = \frac{1}{2} \cdot n(n-1) \sim \frac{1}{2} n^2$$

unterscheidet sich in der Regel die Komplexität, wenn man sie in Abhängigkeit von der Anzahl der Ecken oder in Abhängigkeit von der Anzahl der Kanten berechnet. Oft legt man daher $|E| + |K|$ als Maß zugrunde.

Satz 4.1

$$\sum_{e \in E} d(e) = 2 \cdot |K|$$

Beweis: Jede Kante wird links doppelt gezählt – mit ihren zwei Endpunkten. □

Folgerung: Jeder Graph hat eine gerade Anzahl von Ecken ungeraden Grades.

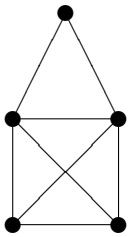
Dieses kleine Ergebnis wird etwas versteckt bei Satz 2.2 und deutlich in der Chriostofides–Heuristik auf Seite 59 eine Rolle spielen.

Beispiele

- Der *vollständige Graph* K_n: dieser hat n Ecken und alle $\binom{n}{2}$ möglichen Kanten zwischen diesen Ecken.
- Der *Kreis* oder *Zyklus* C_n ($n \geqslant 3$) hat n Ecken $e_1, \ldots, e_n$ und Kanten (e_i, e_{i+1}) für $i = 1, \ldots, n-1$ sowie die Kante (e_1, e_n), insgesamt also auch n Kanten. Der Graph $K_3 = C_3$ heißt auch das *Dreieck*.
- Bei *bipartiten* Graphen gibt es eine Partition $E = E' \cup E''$ der Eckenmenge, so dass Kanten nur zwischen Ecken aus E' und E'' bestehen.
  Beim vollständigen bipartiten Graphen $K_{n,m}$ ist dabei $|E'| = n$, $|E''| = m$ und alle möglichen Kanten zwischen Ecken aus E' und E'' sind vorhanden. Es gilt also $|E| = n+m$ und $|K| = nm$.
- Entsprechend liegt bei r-*partiten* Graphen eine Partition $E = E_1 \cup \ldots \cup E_r$ vor und Kanten bestehen nur zwischen Ecken aus verschiedenen Blöcken. Der vollständige r-partite Graph $K_{n_1,\ldots,n_r}$ besitzt Blöcke der Größe $n_1, \ldots, n_r$ und alle möglichen Kanten dazwischen, also $|E| = n_1 + \cdots + n_r$ und $|K| = \sum_{i<j} n_i n_j$.
- Ein k-*regulärer* Graph ist ein Graph, bei dem sämtliche Ecken Grad k haben. Beispielsweise ist C_n 2-regulär und K_n ist $(n-1)$-regulär. In k-regulären Graphen gilt $k \cdot |E| = 2 \cdot |K|$.
- Ein *planarer* Graph ist ein in die reelle Ebene einbettbarer Graph, d.h. ein Graph, den man zeichnen kann, ohne dass sich die Kanten überschneiden. Die beiden Graphen K_5 und $K_{3,3}$ sind nicht planar und in gewissem Sinne die kleinsten nicht planaren Graphen. Jeder nicht-planare Graph enthält in einem technischen Sinne (als sogenannter Minor, vgl. [D]) einen dieser beiden Graphen.

Darstellungen von Graphen

graphisch: als Adjazenzmatrix: als Inzidenzmatrix:



$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Bei der graphischen Darstellung sind nur die dicken Punkte Ecken; die Überschneidung der beiden sich kreuzenden Kanten in der Mitte ist nur der graphischen Darstellung geschuldet und existiert nicht im Graphen. Wie die Kanten gezeichnet sind, spielt keine Rolle; man hätte die Überschneidung in der Mitte zum Beispiel auch vermeiden können, wenn man die Kante im Bogen außen herum geführt hätte.

Bei der Darstellung als Adjazenzmatrix sind die Ecken durchnummeriert; in der i-ten Spalte und j-ten Zeile der Matrix steht eine 1, wenn es eine Kante zwischen der i-ten und der j-ten Ecke gibt, sonst eine 0. Diese Matrix hat dann stets Nullen auf der von links oben nach rechts untern verlaufenden Diagonale und ist symmetrisch bzgl. dieser Diagonalen.

Bei der Darstellung als Inzidenzmatrix sind die Ecken und Kanten durchnummeriert; in der i-ten Spalte und j-ten Zeile der Matrix steht eine 1, wenn die j-te Ecke eine Endecke der i-ten Kante ist, und eine 0 sonst.

Zwei Graphen $G = (E, K)$ und $G' = (E', K')$ heißen *isomorph*, wenn es einen Isomorphismus zwischen G und G' gibt, d.i. eine Bijektion $\varphi : G \to G'$ mit

$$(e_1, e_2) \in K \iff (\varphi(e_1), \varphi(e_2)) \in K'.$$

Ein Isomorphismus von G auf sich selbst heißt Automorphismus.

Es ist im allgemeinen nicht einfach zu entscheiden, ob zwei Darstellungen (auch der gleichen Art) isomorphe Graphen ergeben. Dieses Problem ist zwar nicht NP-vollständig, man kennt aber nur in Spezialfällen polynomiale Algorithmen (etwa für planare Graphen oder für Graphen beschränkter Valenz).

Ein Graph $G' = (E', K')$ heißt *Untergraph* von $G = (E, K)$, falls $E' \subseteq E$ und $K' \subseteq K$ gilt. Man sagt dann auch, dass G den Graphen G' enthält. G' heißt *induzierter Untergraph*, falls zusätzlich $K' = K \cap (E' \times E')$ gilt, d.h. falls G' alle Kanten enthält, die in G zwischen Ecken aus E' bestehen. Zu jeder Teilmenge E' gibt es genau einen induzierten Untergraphen mit Eckenmenge E'; dieser wird mit $G[E']$ bezeichnet. G' heißt *aufspannender Untergraph* von G, falls G' ein Untergraph von G mit $E = E'$ ist. Insbesondere ist G der einzige aufspannende induzierte Untergraph von sich selbst. Dieser Begriff wird dann interessant, wenn man aufspannende Untergraphen mit besonderen Eigenschaften sucht.

Varianten von Graphen

In *Multigraphen* lässt man Schlingen zu und Mehrfachkanten, also mehrere Kanten zwischen zwei Ecken. Multigraphen tauchen immer wieder auf natürliche Weise in der Graphentheorie auf. Manche der folgenden Überlegungen gelten auch für Multigraphen. Multigraphen modelliert man z.B. wie Graphen in der ersten Art: als Ecken– und Kantenmenge mit Inzidenzrelation, wobei nun nur noch gefordert wird, dass jede Kante genau mit zwei Ecken inzident ist. In der Adjazenzmatrix hat man dann natürliche Zahlen als Einträge.

Bei *gerichteten Graphen* haben die Kanten eine Orientierung, also festgelegte Anfangs– und Endpunkte. Man lässt dann auf jeden Fall Kanten in beide Richtungen zwischen zwei Ecken zu und meist auch Schlingen. Einen gerichteten Graphen kann man daher als Eckenmenge E mit einer zweistelligen Relation K ohne weitere Bedingungen ansehen. Die Adjazenzmatrix ist dann nicht mehr symmetrisch.

In *nummerierten Graphen* sind die Ecken wohlunterschieden; man kann sie sich als fest von 1 bis n durchnummeriert denken. Nummerierte Graphen haben als solche also keine nicht-trivialen Automorphismen.

In Anwendungen betrachtet man oft *gewichtete Graphen* G trägt dann noch eine Kosten– oder Gewichtsfunktion, entweder auf den Ecken als $w : E \to \mathbb{R}_0^+$, oder auf den Kanten als $w : K \to \mathbb{R}_0^+$. Letzteres kann etwa eine Straßenkarte mit Abständen zwischen Städten wiedergeben. Geht die Gewichtsfunktion in eine endliche Menge von „Farben“, spricht man auch von *gefärbten Graphen*.

Anzahl der Graphen

Wieviele Graphen mit n Ecken gibt es? Nummeriert man die Ecken, hat man für jedes Eckenpaar die beiden Möglichkeiten, eine Kante zu ziehen oder nicht. Also existieren $2^{\binom{n}{2}}$ viele nummerierte Graphen auf n Ecken. Man kann die n Ecken auf $n!$ viele Arten nummerieren; verschiedenen Nummerierungen führen aber eventuell zu isomorphen nummerierten Graphen, und zwar genau dann, wenn die eine durch einen Automorphismus des Graphen in die andere übergeht. Man kann aber zeigen, dass für große n fast kein Graph nicht-triviale Automorphismen besitzt. Asymptotisch hat man also oben jeden Graph $n!$ Mal gezählt; es gilt daher

$$\text{Anzahl der Graphen auf } n \text{ Ecken} \quad \sim \quad \frac{1}{n!} \cdot 2^{\binom{n}{2}} \quad \sim \quad \frac{1}{\sqrt{2\pi n}} \cdot \left(2^{\frac{n}{2}} \frac{e}{n}\right)^n$$

was grob gesehen wie $(e\frac{\sqrt{2}^n}{n})^n$ wächst, also stärker als jedes exponentielle Wachstum.

Wege, Abstand, Zusammenhang

Definition 4.1 *Ein* Weg *der* Länge n *ist eine Folge* $e_0 k_1 e_1 \dots k_n e_n$ *von Ecken* e_i *und Kanten* $k_i = (e_{i-1}, e_i)$. *Dabei heißt* e_0 *der Anfangs– und* e_n *der Endpunkt des Weges. Ist* $e_0 = e_n$, *so heißt der Weg geschlossen, sonst offen.*

*Ein (Kanten–)*Zug *ist ein Weg, bei dem* $k_i \neq k_j$ *für* $i \neq j$ *gilt.*

Ein Pfad *ist ein Weg, bei dem* $e_i \neq e_j$ *für* $i \neq j$ *gilt.*

Ein Kreis *soll im Grunde ein geschlossenen Pfad sein (nur dass Pfade per Definition offen sind). Es gibt zwei Fälle: Ein* triviale Kreis *ist ein Weg der Länge* 0. *Ein* nicht-trivialer Kreis *ist ein geschlossener Weg der Länge mindestens* 3, *bei dem also* $e_0 = e_n$ *gilt, sonst aber* $e_i \neq e_j$ *für* $i \neq j$.

Achtung: Diese Terminologie ist nicht standardisiert!

Jeder Pfad und jeder Kreis ist automatisch auch ein Zug. In G gibt es genau dann einen Kreis der Länge n, wenn C_n Untergraph von G ist, daher ist die Doppelbesetzung des Wortes „Kreis“ unproblematisch.

Man sagt, dass ein Weg mit Anfangspunkt e und Endpunkt e' die Ecken e und e' verbindet. Jeder e und e' verbindende Weg lässt sich zu einem e und e' verbindenden Pfad verkürzen; jeder geschlossene Weg $e_0k_1e_1 \dots e_{n-1}k_ne_0$ mit $e_1 \neq e_{n-1}$ läßt sich zu einem nicht-trivialen Kreis verkürzen.

Wir definieren auf E eine Äquivalenzrelation K^* durch eK^*e', falls e und e' durch einen Weg verbunden sind. Die Äquivalenzklassen von K^* heißen die *Zusammenhangskomponenten* des Graphen. Ein Graph heißt *zusammenhängend*, falls er aus nur einer Zusammenhangskomponente besteht, d.h. wenn je zwei Ecken durch einen Weg verbunden sind.

Der *Abstand* $d(e, e')$ zweier Ecken ist definiert als die minimale Länge eines e und e' verbindenden Weges, falls ein solcher existiert, und als ∞ sonst. Es gilt dann also

$$\begin{aligned}
d(e,e') = 0 &\iff e = e' \\
d(e,e') = 1 &\iff e \text{ und } e' \text{ sind benachbart} \\
d(e,e') = 2 &\iff e \text{ und } e' \text{ haben gemeinsamen Nachbarn, aber } e \neq e', e \notin N(e') \\
d(e,e') = \infty &\iff e \text{ und } e' \text{ liegen in verschiedenen Zusammenhangskomponenten}
\end{aligned}$$

Algorithmus zum Finden der Zusammenhangskomponenten:

Sei $E = \{e_0, \dots, e_n\}$. Starte in der Ecke e_0 und definiere $E_{-1} = \emptyset$ und $E_0 := \{e_0\}$. Setze im i-ten Schritt $E_{i+1} := E_i \cup \bigcup \{N(e) \mid e \in E_i \setminus E_{i-1}\}$. Halte an, falls $E_{i+1} = E_i$; dann ist E_i die Zusammenhangskomponente von e_0. Falls $E_i = E$, so ist G zusammenhängend; andernfalls nicht. Starte dann neu mit Ecken, die nicht in den bereits gefundenen Zusammenhangskomponenten liegen. Dieser Algorithmus berechnet in $O(|E|^2)$ vielen Schritten die Zusammenhangskomponenten und/oder testet, ob G zusammenhängend ist.

Satz 4.2 *Ein nicht trivialer Graph ist genau dann bipartit, wenn alle Kreise darin gerade Länge haben.*

Beweis: “$\Rightarrow$” : Ein Kreis in einem bipartiten Graphen muss abwechselnd zwischen Ecken aus den beiden Blöcken der Bipartition verlaufen, hat also gerade Länge.

“$\Leftarrow$” : Es reicht zu zeigen, dass jede Zusammenhangskomponente des Graphen bipartit ist; man kann also o.B.d.A. annehmen, dass der betrachtete Graph $G = (E, K)$ zusammenhängend ist. Sei $e_0 \in E$ beliebig und definiere $E' := \{e \in E \mid d(e_0, e) \text{ gerade}\}$ und $E'' := E \setminus E' = \{e \in E \mid d(e_0, e) \text{ ungerade}\}$. Dies ist eine Bipartition von G: Angenommen, es gäbe eine Kante k

zwischen $e, e' \in E'$ (analog für E''). Betrachte Pfade minimaler Länge von e_0 nach e bzw. e'. Wegen der Minimalität gibt es einen Punkt e'', der auf beiden Pfaden der letzte gemeinsame Punkt ist, und die die beiden Teilpfade von e_0 bis e'' die gleiche Länge. Die Restpfade von e'' nach e bzw. e' ergeben zusammen mit k in geeigneter Reihenfolge einen Kreis ungerader Länge: Widerspruch. □

II.5 Besondere Wege

Euler–Züge

Meist schon als Kind beschäftigt man sich mit Graphentheorie, nämlich mit dem Problem, das „Haus des Nikolaus“ ohne Absetzen zu zeichnen. Tatsächlich gilt ein Problem dieser Art, nämlich das „Königsberger Brückenproblem“, auch als der mathematische Anfang der Graphentheorie. Für das damalige Königsberg hat Euler gezeigt, dass es keinen möglichen Spaziergang gibt, bei dem alle Brücken genau einmal überquert werden. Die mathematische Modellierung des Stadtplans führt zwar zu einem Multigraphen; durch zusätzliche Ecken, etwa auf den Brücken, erhält man aber ein gleichwertiges Problem für normale Graphen.

Definition 5.1 *Ein* Eulerscher Zug *in einem Graphen ist ein alle Kanten durchlaufender Zug. Ein Graph heißt Eulersch, falls es in ihm einen Euler–Zug gibt.*

Satz 5.1 *Ein Graph ohne isolierte Punkte hat genau dann einen geschlossenen (bzw. offenen) Eulerschen Zug, wenn er zusammenhängend ist und keine (bzw. genau zwei) Ecken ungeraden Grades besitzt.*

Beweis: Die Bedingungen sind offenbar notwendig, denn ein Euler–Zug läuft ebensooft in eine Ecke hinein wie hinaus (jedesmal zwei Kanten) bis auf eventuell Anfangs– und End–Ecke.

Umgekehrt führt man den offenen Euler–Zug auf den geschlossenen zurück, indem man eine zusätzliche Verbindung zwischen den beiden Ecken ungeraden Grades einführt (eine Kante, wenn noch keine Kante zwischen den beiden Ecken besteht; sonst ein Weg der Länge zwei über eine neue Ecke). Dadurch haben alle Ecken geraden Grad. Nun betrachtet man einen Zug maximaler Länge $e_0 k_1 \dots k_n e_n$. Es gilt dann $e_0 = e_n$, da sonst nur eine ungerade Anzahl zu e_n inzidenter Kanten in dem Zug vorkäme, dieser also noch verlängert werden könnte. Angenommen es gibt eine in dem Zug nicht vorkommende Kante. Dann gibt es, da G zusammenhängend ist, auch eine Kante k, die in dem Zug nicht vorkommt und mit einer der vorkommenden Ecken e_i inzident ist. Wenn man nun den geschlossenen Zug oben bei e_i beginnen und enden lässt, kann man am Ende die Kante k anhängen und erhält einen längeren Zug: Widerspruch. □

Dieser Beweis ist im Prinzip konstruktiv, d.h. dem Beweis folgend kann man, ausgehend von einem Zug der Länge 0, also von einer Ecke, durch Hinzunehmen von Kanten einen maximalen Zug konstruieren. Dabei ist aber nicht garantiert, dass die jeweils konstruierten Teile Anfangsstücke des letztendlichen Euler–Zugs sind. Es folgt nun ein besserer Algorithmus, der diese Zusatzeigenschaft hat.

Eine *Brücke* in einem Graphen ist eine Kante, die auf keinem Kreis liegt. Man überlegt sich leicht, dass eine Kante genau dann eine Brücke ist, wenn sich die Anzahl der Zusammenhangskomponenten des Graphen erhöht, falls man die Kante herausnimmt.

Algorithmus zur Konstruktion von Euler–Zügen:

Man startet in einer Ecke e_0 ungeraden Grades, falls es eine gibt, sonst in einer beliebigen Ecke. Sei der Anfang $e_0 k_1 e_1 \dots k_i e_i$ des Euler–Zuges bereits konstruiert, und $K_i := K \setminus \{k_1, \dots, k_i\}$. Falls $K_i = \emptyset$, so ist man fertig. Falls $K_i \neq \emptyset$, aber keine zu e_i inzidente Kante enthält, so Abbruch: Der Graph ist nicht Eulersch. Falls K_i eine zu e_i inzidente Kante enthält, die keine Brücke in $G_i := (E, K_i)$ ist, so wählt man eine dieser als k_{i+1}. Andernfalls wählt man eine beliebige zu e_i inzidente Kante aus K_i als k_{i+1}.

Zum Beweis der Korrektheit überlegt man sich, dass wenn man nach und nach die konstruierten Kanten aus dem Graphen entfernt, entweder keine neuen Zusammenhangskomponenten entstehen oder eine, die nur aus einer Ecke besteht. Induktiv sieht man dass der Restgraph die Bedingungen von Satz 5.1 weiterhin erfüllt, also Eulersch bleibt.

Wie groß ist die Komplexität des Algorithmus? Er wird höchstens $|K|$ Mal durchlaufen. In jedem Schritt müssen $|K_i|$ viele Kanten daraufhin getestet werden, ob sie zu e_i inzident sind und ob ein Graph mit $|E|$ Ecken zusammenhängend ist. Letzteres ist in $O(|E|^2)$ möglich. Insgesamt ist der Algorithmus also in $O(|K|^2 \cdot |E|^2) \subseteq O(|E|^6)$, insbesondere polynomial.

Hamiltonsche Kreise

Definition 5.2 *Ein* Hamiltonscher Kreis *in einem Graphen ist ein alle Ecken durchlaufender Kreis.* G *heißt Hamiltonsch, falls es in* G *einen Hamiltonschen Kreis gibt.*

G ist also genau dann Hamiltonsch, wenn G einen aufspannenden Kreis enthält. Das Hamilton–Problem ist das Analogon des Euler–Problems für Ecken statt für Kanten. Erstaunlicherweise ist es viel schwerer zu lösen. Historisch tauchte es bei Hamilton für den Dodekaeder auf.

Beispiele: K_n ist klarerweise Hamiltonsch, $K_{n,m}$ für $n \neq m$ dagegen nicht (da ein Hamilton–Kreis abwechselnd Ecken aus den beiden Blöcken der Bipartition durchläuft). Die Platonischen Körper (d.h. die Graphen, die aus den Ecken und Kanten von Tetraeder, Würfel, Oktaeder, Dodekaeder bzw. Ikosaeder bestehen) sind Hamiltonsch.

Es gibt einen naheliegenden Algorithmus zu entscheiden, ob ein Graph Hamiltonsch ist oder nicht: Man erzeugt sämtliche Kreise des Graphen und überprüft, ob einer davon alle Ecken durchläuft. Aber: Im K_n etwa gibt es $(n-1)!$ viele Kreise mit gegebenem Anfangspunkt; in einem beliebigen Graphen muss man daher auch erwarten, dass es zu viele sind, um in vernünftiger Zeit obigen Algorithmus durchführen zu können. Man kennt bis heute keinen schnellen Algorithmus, einen Hamiltonschen Kreis zu finden, und kein praktikables notwendiges und hinreichendes Kriterium für seine Existenz. Man hat allerdings gute Gründe, einen solchen Algorithmus nicht zu erwarten: Das Hamilton–Problem ist nämlich ein sogenanntes NP-vollständiges Problem. Es gibt aber eine Reihe von hinreichenden Kriterien, von denen das einfachste folgt:

Satz 5.2 *Sei* $G = (E, K)$ *so, dass* $n := |E| \geqslant 3$ *und* $d(e) \geqslant \frac{n}{2}$ *für alle* $e \in E$. *Dann ist* G *Hamiltonsch.*

Beweis: Zunächst ist G zusammenhängend, denn sonst hätte eine Ecke in einer minimalen Zusammenhangskomponente mehr Nachbarn als möglich. Sei $P = e_0 k_1 e_1 \ldots k_m e_m$ ein Pfad maximaler Länge in G. Es muss P bereits alle Nachbarn von e_0 und e_m enthalten; andernfalls könnte man ihn verlängern. Seien nun $I_1 := \{i \mid e_i \in N(e_m)\}$ und $I_2 := \{i \mid e_{i+1} \in N(e_0)\}$. Beides sind Teilmengen von $\{0, \ldots, m-1\}$ der Mächtigkeit mindestens $\frac{n}{2}$, also schneiden sie sich. Es gibt daher ein i mit Kanten $k = \{e_0, e_{i+1}\}$ und $k' = \{e_i, e_m\}$. Aus P, k, k' erhält man einen Kreis der Länge $m+1$, nämlich $e_{i+1} k e_0 k_1 e_1 \ldots k_i e_i k' e_m k_m e_{m-1} \ldots k_{i+2} e_{i+1}$. Dieser Kreis muss dann Hamiltonsch sein, denn andernfalls könnte man ihn analog zum Beweis von Satz 5.1 um eine weitere Kante verlängern und bekäme einen Pfad der Länge $m+1$, im Widerspruch zur Maximalität von m. □

Diesen Beweis kann man leicht in einen polynomialen Algorithmus zur Konstruktion eines Hamiltonschen Kreises umformen.

Die Klasse der Probleme, die man in polynomialer Zeit lösen kann, wird P genannt. NP steht für die Klasse der Probleme, für die man in polynomialer Zeit feststellen kann, ob eine vorgeschlagene Lösung stimmt oder nicht. Das Problem der Euler–Züge („Ist ein gegebener Graph Eulersch oder nicht?“) liegt zum Beispiel in P. Man sieht auch sofort, dass das Hamilton–Problem („Ist ein gegebener Graph Hamiltonsch oder nicht?“) in NP liegt, denn man kann schnell überprüfen, ob eine gegebene Ecken–Kanten–Abfolge ein Hamitonscher Kreis ist oder nicht. Es ist nicht sehr schwierig, P$\subseteq$ NP zu zeigen. Ob P = NP gilt, ist eine der großen offenen Fragen der Mathematik und theoretischen Informatik (für deren Beantwortung 1 Million Dollar ausgesetzt sind). Überwiegend wird davon ausgegangen, dass P $\neq$ NP gilt.

NP-vollständige Probleme sind die „maximal schwierigen“ Probleme in der Klasse NP: Jedes andere NP-Problem lässt sich in polynomialer Zeit auf sie zurückführen, oder anders ausgedrückt: Findet man einen polynomialen Algorithmus für ein NP-vollständiges Problem, so gilt P = NP. Daher gelten NP-vollständige Probleme als schwer. Trotzdem kann es schnelle Algorithmen geben, welche näherungsweise Lösungen liefern: Im Falle von *Entscheidungsproblemen* (d.h. die Lösung besteht in einer Antwort „ ja“ oder „nein“) etwa probabilistische Algorithmen, die mit hoher Wahrscheinlichkeit das richtige Ergebnis liefern. Im Falle von *Optimierungsproblemen*, wie das folgende Problem des Handlungsreisenden, etwa Näherungsalgorithmen, welche bis auf einen festen Fehler an das optimale Ergebnis heankommen.

Problem des Handlungsreisenden

Gegeben ist hier ein zusammenhängender Graph $G = (E, K)$ mit einer Gewichtsfunktion auf den Kanten $w : K \to \mathbb{R}_0^+$. Für einen Weg $W = e_0 k_1 e_1 \ldots k_n e_n$ definiert man das Gewicht des Weges als $w(W) := \sum_{i=1}^{n} w(k_i)$. Das *Problem des Handlungsreisenden* („Travelling Salesman Problem“, TSP) besteht nun darin, einen alle Ecken durchlaufenden (geschlossenen) Weg minimalen Gewichts zu finden. Als Variante des Problems kann man auch nach einem Hamiltonschen Kreis minimales Gewichts fragen.

Bemerkungen:

- Das Hamilton–Problem kann man als Spezialfall des Problems des Handlungsreisenden auffassen, indem man alle Kanten mit konstantem Gewicht 1 versieht. In diesem Sinne ist also das Problem des Handlungsreisenden mindestens so schwer wie das Hamilton–Problem.
- Ohne Einschränkung kann man G als vollständig annehmen, indem man neue Kanten mit einem Gewicht größer als die Summe der bisherigen Gewichte hinzunimmt.
- Falls w die Dreiecksungleichung erfüllt (z.B. falls w Abstände angibt), so ist ein geschlossener Weg minimalen Gewichts dann automatisch Hamiltonsch.
- Ein naheliegender Algorithmus konstruiert einen Weg, indem man in einer Ecke startet und jeweils einen Weg minimalen Gewichts zu einer noch nicht besuchten Ecke anhängt (ein sogenannter „greedy"–Algorithmus). Man kann aber leicht Beispiele konstruieren, in welchen dieser Algorithmus nicht die beste Lösung liefert.

Das Problem des Handlungsreisenden ist ein NP-vollständiges Problem unter den Optimierungsproblemen. Zwei gute Näherungsalgorithmen (meist *Heuristiken* genannt) für das Problem des Handlungsreisenden folgen auf Seite 58.

Kürzeste Wege

Zum Abschluss dieses Abschnittes eine verwandte Fragestellung, für die es einen polynomialen Algorithmus gibt. Gegeben ist wieder ein zusammenhängender kantengewichteter Graph $G = (E, K)$ mit Gewichtsfunktion $w : K \to \mathbb{R}_0^+$. Gesucht ist für zwei gegebene Ecken e und e' ein beide verbindender Weg minimalen Gewichts. Klar ist, dass solch ein Weg in zusammenhängenden Graphen existiert, er braucht allerdings nicht eindeutig zu sein, und dass er ein Pfad ist.

Man kann sich wieder Beispiele überlegen, in denen der „greedy"–Algorithmus nicht funktioniert, in denen es also nicht ausreicht, sich von e schrittweise nach e' vorzutasten, indem man in jedem Schritt eine zu e' hinführende, noch nicht benutzte Kante minimalen Gewichts wählt. Eine geringe Variante dieser lokal günstigsten Wahl genügt allerdings, indem man sukzessive alle von e ausgehenden Pfade nach Gewicht geordnet konstruiert.

Algorithmus zur Konstruktion von Wegen minimalen Gewichts:

Man definiert induktiv Ecken e_i, das minimale Gewicht $W(e_0, e_i)$ eines Weges von e_0 nach e_i und für $i \geqslant 1$ Kanten k_i.

- e_0 ist die Startecke und $W(e_0, e_0) := 0$.
- Im $(i+1)$-ten Schritt berechnet man für alle Paare (e_j, e), wobei $e \notin \{e_0, \ldots, e_i\}$ ein Nachbar von $e_j \in \{e_0, \ldots, e_i\}$ ist, die Größe $W(e_0, e_j) + w((e_j, e))$ und wählt die Kante $k_i := (e, e_j)$ und Ecke $e_{i+1} := e$ so, dass diese Größe minimal wird, und setzt $W(e_0, e_{i+1}) = W(e_0, e_j) + w(k_i)$.
- Der Algorithmus bricht ab, wenn die Zielecke erreicht ist.

Die konstruierten Kanten k_i bilden einen Baum (siehe Seite 50); er enthält einen eindeutigen Pfad von e_0 nach der Zielecke; dies ist der gesuchte Weg minimalen Gewichts.

Man kann den Algorithmus auch laufen lassen, bis keine neuen Ecken mehr zur Verfügung stehen. Die konstruierten Kanten k_i bilden dann einen aufspannenden Baum der Zusammen-

hangskomponente von e_0, in denen der eindeutige Pfad von e_0 zu jeder anderen Ecke minimales Gewicht hat. Im allgemeinen wird dieser Baum aber kein aufspannender Baum minimalen Gewichts sein. Dies kann man aber auch durch „greedy"-Algorithmen erreichen:

Algorithmus zur Konstruktion von Bäumen minimalen Gewichts:

Variante 1: Man konstruiert induktiv einen Baum.

- Man startet mit einer Kante minimalen Gewichts.
- Nun nimmt man, so lange es geht, induktiv zum bereits konstruierten Baum eine Kante minimalen Gewichts hinzu, die zu einer Ecke des bereits konstruierten Baumes inzident ist und mit den bereits gewählten Kanten keinen Kreis bildet.

Variante 2: Man konstruiert induktiv einen Wald.

- Man startet mit einer Kante minimalen Gewichts.
- Nun nimmt man, so lange es geht, induktiv zum bereits konstruierten Wald eine Kante minimalen Gewichts hinzu, die mit den bereits gewählten Kanten keinen Kreis bildet.

Variante 3: Man lichtet nach und nach den Graph zu einem kreisfreien Graphen aus.

- Man startet mit dem gegebenen Graphen.
- Nun nimmt man, so lange es geht, induktiv aus dem Restgraphen Kanten maximalen Gewichts heraus, die keine Brücken im Restgraphen sind.

II.6 Färbungen

Eckenfärbungen

Gegeben sei ein Graph $G = (E, K)$. Eine *Eckenfärbung* (mit k Farben) ist eine Abbildung $c : E \to \{1, \ldots, k\}$, die benachbarte Ecken unterschiedlich färbt, d.h. $(e, e') \in K$ impliziert $c(e) \neq c(e')$. Ein Graph, für den eine Eckenfärbung mit k Farben existiert, heißt auch k-*färbbar* Offenbar ist ein Graph genau dann k-färbbar, wenn er k-partit ist: Die Blöcke der k-Partition werden durch die gleichgefärbten Ecken gebildet.

Beispiel: Man möchte die Länder einer Landkarte so färben, dass benachbarte Länder unterschiedliche Farben haben. Die Landkarte kann man in einen Graphen übersetzen, indem man die Hauptstädte als Ecken nimmt und Kanten zwischen den Haupstädten zieht, deren Länder eine gemeinsame Grenze haben. (Das stimmt allerdings nur unter der Annahme, dass jedes Land aus einer zusammenhängenden Landmasse besteht.) Das berühmte 4*–Farben–Problem* aus der Mitte des vorletzten Jahrhunderts fragte, ob dies stets mit vier Farben möglich ist. Ein erster Beweis von Appel und Haken (1977) führte das Problem auf etwa 1500 durch Computereinsatz überprüfte Einzelfälle zurück. Die mathematische Gültigkeit wurde deshalb und wegen der mangelnden Nachvollziehbarkeit bezweifelt. Seit kurzem gibt es aber kürzere, überschaubarere und unbezweifelte Beweise.

Für die Anzahl der Farben ist es kein Unterschied, ob man Graphen auf der Ebene oder auf der Kugeloberfläche färbt: Eine Landkarte auf einer Kugel kann man im Inneren eines Landes auf-

schneiden und auf eine Ebene ziehen (wie bei Weltkarten). Umgekehrt kann man sich eine ebene Landkarte auf eine Kugel aufgeklebt vorstellen, ohne dass neue Nachbarschaften entstehen.

Sei ein planarer Graph $G = (E, K)$ gegeben mit einer festen Einbettung in die Ebene, d.h. anschaulich auf eine gewisse überschneidungsfreie Art gezeichnet. G grenzt dann eine Menge F von Flächen ab; dies sind die topologischen Zusammenhangskomponenten von $\mathbb{R}^2 \setminus G$, wenn man G als eine Menge von Linien in der Ebene $\mathbb{R}^2$ auffasst. Es zählt also auch die Außenfläche. Wenn G ein nicht-trivialer Kreis ist, gibt es z.B. zwei Flächen (das Innere und das Äußere des Kreises); ein Baum dagegen hat nur eine Fläche. Das „Haus vom Nikolaus“ kann man überschneidungsfrei zeichnen, es hat dann fünf Flächen.

Satz 6.1 (Euler–Formel) *Für zusammenhängende planare Graphen gilt* $|F| - |K| + |E| = 2$.

Beweis–Skizze: Induktion nach $|E|$: Der Satz gilt offenbar für den einpunktigen Graphen mit $|E| = 1$, $|K| = 0$ und $|F| = 1$. Eine neue Ecke e wird in eine Fläche f eingesetzt und über m viele Kanten verbunden. Dabei wird die Fläche f in m viele Flächen zerlegt, es kommen also $m - 1$ neue Flächen hinzu. □

Folgerung: Die Anzahl der Flächen ist unabhängig von der Einbettung des Graphen.
(Die Art der Flächen ist allerdings abhängig von der Einbettung).

Ein zusammenhängender planarer Graph heißt *trianguliert*, wenn alle Flächen (einschließlich der Außenfläche) Dreiecke sind, also durch drei Kanten begrenzt sind.

Folgerung: In einem triangulierten Graphen gilt $|K| = 3 \cdot |E| - 6$.

Beweis: Jede Fläche hat drei Kanten, die jeweils für zwei Flächen zählen, also $3 \cdot |F| = 2 \cdot |K|$. □

Mit Hilfe der Euler–Formel kann man auch elegant beweisen, dass die beiden Graphen K_5 und $K_{3,3}$ nicht planar sind. Da jede Fläche mindestens ein Dreieck ist, aber jede Kante für zwei Flächen zählt, erhält man im Falle des K_5 den Widerspruch:

$$10 = |K| \geqslant \frac{3}{2}|F| = \frac{3}{2}(2 + |K| - |E|) = \frac{3}{2} \cdot 7 = 10{,}5$$

Satz 6.2 *In jedem planaren Graphen gibt es eine Ecke vom Grad höchstens fünf.*

Beweis: Durch Hinzufügen von Kanten kann man annehmen, dass der Graph trianguliert ist. Hätte jede Ecke mindestens 6 Nachbarn, würde $|K| \geqslant \frac{1}{2}6 \cdot |E| = 3 \cdot |E|$ gelten, im Widerspruch zur vorherigen Folgerung. □

Aus diesem Satz erhält man sofort, dass jeder planare Graph 6-färbbar ist, sowie einen Algorithmus, der eine 6-Färbung konstruiert: Man ordnet die n Ecken des Graphen in einer Folge $e_1, e_2, e_3, \ldots, e_n$ so, dass e_1 höchstens Grad 5 hat und induktiv e_i höchsten Grad 5 im Restgraphen $G[E \setminus \{e_1, \ldots, e_{i-1}\}]$ hat. Dann kann man die Ecken in der Reihenfolge $e_n, e_{n-1}, \ldots, e_1$ färben, denn da jede Ecke höchstens fünf Nachbarn hat, bleibt jeweils mindestens eine zugelassene Farbe übrig.

Mit etwas Mehrarbeit kann man das Ergebnis verbessern:

Satz 6.3 *Jeder planare Graph ist* 5*-färbbar.*

Die Umkehrung gilt nicht, z.B. ist $K_{3,3}$ nicht planar, als bipartiter Graph aber 2-färbbar.

Beweis: Ohne Einschränkung kann man annehmen, dass der Graph zusammenhängend ist, denn sonst färbt man die Zusammenhangskomponenten einzeln. Der Beweis geht nun per Induktion nach $|E|$. Graphen mit $|E| \leqslant 5$ sind klarerweise 5-färbbar. Im Induktionsschritt wählt man wieder e_0 mit $d(e_0) \leqslant 5$. Falls $d(e_0) < 5$, geht es wie oben. Sei also $N(e_0) = \{e_1, \ldots, e_5\}$. Da G planar ist, kann G keinen Untergraphen K_5 enthalten, somit gibt es unter den Nachbarn von e_0 zwei nicht benachbarte Ecken e_i, e_j. Man betrachtet nun den Graphen G', der aus $G[E \setminus \{e_0\}]$ durch Zusammenziehen der Ecken e_i und e_j zu einer einzigen Ecke entsteht (Kanten zwischen einer Ecke e und dieser neuen zusammengezogenen Ecke gibt es dann, wenn es eine Kante zwischen e und e_i oder eine Kanten zwischen e und e_j gibt). Der neue Graph ist planar, weil man anschaulich die beiden Ecken entlang der Verbindung von e_i nach e_j über e_0 zusammenziehen kann. Per Induktion gibt es eine 5-Färbung von G', aus der man eine 5-Färbung von $G[E \setminus \{e_0\}]$ erhält, in der e_i und e_j dieselbe Farbe tragen. Also sind nur vier Farben für die Nachbarn von e_0 verwendet und man kann e_0 mit der fünften Farbe färben. □

Ähnliche Ergebnisse gibt es für Graphen, die sich auf andere Flächen als Ebene bzw. Kugel einbetten lassen. So kann man zum Beispiel jeden Graphen, der sich überschneidungsfrei auf einen Torus zeichnen kann, mit sieben Farben färben, und jeden Graphen auf einem Möbiusband mit sechs Farben. Eine andere Variante sind sogenannte Erde–Mond–Karten, bei denen man sich vorstellt, dass Staaten auf der Erde Kolonien auf dem Mond haben, und sowohl Mutterland als auch Kolonie in der gleichen Farbe, aber unterschiedlich zu ihren jeweiligen Nachbarn gefärbt werden. Hier kennt man derzeit nur die untere Schranke 9 und die obere 12. Solche Färbeprobleme haben übrigens Anwendungen in Verfahren zur Chipverifikation.

Die *chromatische Zahl* $\chi(G)$ eines Graphen G ist die kleinste Zahl k, so dass G k-färbbar ist. Zum Beispiel ist $\chi(K_5) = 5$ und $\chi(K_{3,3}) = 2$ und die chromatische Zahl eines planaren Graphen höchstens 4. Es gibt eine offene Vermutung (*Hadwigers Vermutung*), dass in einem Graphen G mit $\chi(G) = n$ in einem gewissen technischen Sinn (als sogenannter Minor, vgl. [D]) ein K_n enthalten ist.

Kantenfärbungen

Unter einer *Kantenfärbung* (mit k Farben) versteht man in der Regel eine Abbildung $c : K \to \{1, \ldots, k\}$, die aneinanderstoßende Kanten unterschiedlich färbt. Man kann nun ähnliche Fragen wie für Eckenfärbungen stellen. Als Anwendungsbeispiel kann man sich einen Turnierplan vorstellen: Ecken repräsentieren Mannschaften, die Farben der Kanten entsprechen Spieltagen.

Der Satz von Ramsey

Nun soll ein gegensätzliches Problem behandelt werden: Statt Graphen so zu färben, dass keine gleichfarbigen Kanten aufeinanderstoßen, sollen in einem gefärbten Graphen möglichst große einfarbige Stücke gefunden werden. Dazu betrachten wir $G = (E, K)$ und eine Abbildung $c : K \to \{1, \ldots, k\}$ *ohne* Zusatzbedingung. Dies ist also keine Kantenfärbung im obigen Sinn, soll

der Einfachheit halber aber auch Färbung genannt werden. Ein induzierter Untergraph $G' = (E', K')$ heißt *einfarbig*, falls $c \restriction_{K'}$ konstant ist.

Auf K_5 gibt es eine 2-Färbung ohne einfarbiges Dreieck: Man färbt ein Fünfeck in einer Farbe, das verbleibende mit der anderen. Auf K_6 dagegen hat man notwendig ein einfarbiges Dreieck: Eine fest gewählte Ecke ist mit fünf Ecken verbunden, also mit dreien davon in einer Farbe c. Entweder zwei dieser drei Ecken sind auch mit der Farbe c verbunden oder die drei Ecken sind untereinander mit der anderen Farbe c' verbunden. In beiden Fällen erhält man ein einfarbiges Dreieck.

Dies ist ein allgemeines Phänomen:

Satz 6.4 (Ramsey) *Gegeben $r, k \in \mathbb{N}$, so gibt es ein $n \in \mathbb{N}$, so dass K_m mit $m \geqslant n$ für jede k-Färbung einen einfarbigen Untergraphen K_r enthält.*

Beweis: Zunächst sei $k = 2$. Es reicht, $m = n$ zu betrachten, da die Eigenschaft mit Vergrößern der Eckenmenge erhalten bleibt. Man wählt $n = 2^{2r-3}$ und konstruiert induktiv Teilmengen $E_i \subseteq E$, eine Ecke $e_i \in E_i$ und Farben $c_i \in \{1, 2\}$ für $i = 0, \ldots, 2r-3$ mit den Eigenschaften:

- $|E_i| \geqslant 2^{2r-3-i}$
- $E_{i+1} \subseteq E_i \setminus \{e_i\}$
- alle Kanten von e_i nach E_{i+1} haben die gleiche Farbe c_i.

Setze $E_0 = E$. Sei E_i bereits konstruiert; $e_i \in E_i$ wählt man beliebig. Da $|E_i \setminus \{e_i\}| \geqslant 2^{2r-3-i} - 1$, gibt es eine Farbe c_i, so dass die Menge E_{i+1} derjenigen Ecken in E_i, die mit e_i in der Farbe c_i verbunden sind, mindestens die Mächtigkeit $\lceil \frac{2^{2r-3-i}-1}{2} \rceil = 2^{2r-3-(i+1)}$ hat. In der Folge $(c_0, c_1, \ldots, c_{2r-4})$ der Länge $2r-3$ taucht nun eine Farbe c mindestens $\lceil \frac{2r-3}{2} \rceil = (r-1)$ Mal auf. Sei nun $R = \{e_i \mid c_i = c\} \cup \{e_{2r-3}\}$. Es gilt dann $|R| \geqslant r$ und jede zwischen Ecken aus R verlaufende Kante hat nach Konstruktion die Farbe c.

Für $k > 2$ ändert man entweder den Beweis entsprechend ab, oder schließt induktiv, indem man zunächst die k Farben in zwei Gruppen zusammenfasst. □

Der Satz von Ramsey hat viele Verallgemeinerungen und ist in vielen Teilgebeiten der Mathematik nützlich. Sein Inhalt wird manchmal durch die Aussage „totale Unordnung ist unmöglich“ paraphrasiert.

Der Beweis oben liefert auch eine obere Schranke für n. Man kennt aber bessere obere Schranken und auch untere Schranken. Nennt man den genauen Wert $R(r, k)$, so wurde am Anfang $R(3, 2) = 6$ gezeigt. Außerdem gilt $R(4, 2) = 18$ und $R(3, 3) = 17$; andere exakte Werte kennt man zur Zeit nicht. So weiß man z.B. nur, dass $43 \leqslant R(5, 2) \leqslant 49$. Obwohl es sich um recht kleine Zahlen handelt, kann man $R(5, 2)$ nicht einfach ausrechnen, weil die Fülle der Möglichkeiten die Rechnerleistung heutiger Computer übersteigt.

II.7 Bäume

Definition 7.1 *Ein* Baum *ist ein zusammenhängender kreisfreier Graph. Ein* Wald *ist ein kreisfreier Graph.*

Also ist ein Baum ein zusammenhängender Wald und die Zusammenhangskomponenten eines Waldes sind Bäume. Ecken vom Grad 1 heißen *Blätter*. Jeder nicht-triviale Baum hat mindestens zwei Blätter. Ist e ein Blatt des Baumes $G = (E, K)$, so ist auch $G[E \setminus \{e\}]$ ein Baum. Dies erlaubt es oft, Eigenschaften von Bäumen per Induktion zu zeigen. Allgemeiner ist jeder Untergraph eines Waldes wieder ein Wald. Wälder sind offenbar bipartit bzw. 2-färbbar nach Satz 4.2.

Satz 7.1 $G = (E, K)$ *ist ein Baum*

$\iff$ *je zwei Ecken sind durch einen eindeutigen Pfad verbunden*

$\iff$ G *ist maximal zusammenhängend, d.h. zusammenhängend und jede Kante ist eine Brücke*

$\iff$ G *ist minimal azyklisch, d.h. kreisfrei, aber durch jede neue Kante zwischen vorhandenen Ecken entsteht ein Kreis*

$\iff$ G *ist zusammenhängend und* $|E| = |K| + 1$.

Beweis: Zunächst überlegt man sich folgendes: Wenn es zwei verschiedene Pfade zwischen zwei Ecken eines Graphen gibt (oder allgemeiner zwei Wege, die nicht alle Kanten gemeinsam haben), dann gibt es auch einen Kreis: Man wählt die erste Ecke e auf den beiden Wegen, an die sich auf einem der Wege eine Kante anschließt, die nicht zum anderen Weg gehört. Dann wählt man e' als die auf einem der beiden Wege nächste Ecke nach e, die wieder beiden Wegen gemeinsam ist. Die Kanten der jeweils kürzesten Teilstücke von e nach e' auf den beiden Wegen bilden dann einen Kreis.

„(1)⇔(2)“: Ein Graph ist genau dann zusammenhängend, wenn es zwischen je zwei Ecken einen verbindenden Pfad gibt. Mit der Anfangsüberlegung sind die verbindenden Pfade genau dann alle eindeutig, wenn es keine Kreise gibt.

„(1)⇔(3)“ ist klar, weil Nicht–Brücken gerade Kanten auf Kreisen sind.

„(2)⇔(4)“ ist ebenfalls klar mit der Anfangsüberlegung.

„(2)⇒(5)“: Wählt man eine feste Ecke e_0, so gibt es eine Bijektion zwischen den Kanten und den verbleibenden Ecken, nämlich jeweils die erste Kante des eindeutigen Pfades einer Ecke nach e_0.

„(5)⇒(1)“: Jeder zusammenhängende Graph enthält einen aufspannenden Baum (Satz 7.2), für den wegen (1)⇒(2)⇒(5) die Gleichheit $|E| = |K| + 1$ gilt. Der Graph hat also nicht mehr Kanten als sein aufspannender Baum, ist diesem also gleich. □

Satz 7.2 *Jeder Graph enthält einen aufspannenden Wald mit ebensovielen Zusammenhangskomponenten wie der Graph selbst. Insbesondere enthält jeder zusammenhängende Graph einen aufspannenden Baum.*

Beweis: Man entfernt nach und nach Kanten, die keine Brücken sind. Dadurch erhöht sich die Anzahl der Zusammenhangskomponenten nicht, und am Ende bleibt ein Wald übrig, denn in einem Kreis gibt es Kanten, die keine Brücken sind. □

Dieser Beweis liefert zugleich einen Algorithmus, der allerdings nicht besonders effektiv ist. Der Algorithmus zur Konstruktion von Wegen minimalen Gewichts liefert für die konstante Gewichtsfunktion ebenfalls einen aufspannenden Baum. Zwei weitere häufig vorkommende Möglichkeiten sind die Breiten– und die Tiefensuche. Der Breitensuchalgorithmus konstruiert flache, breitverzweigte Bäume, der Tiefensuchalgorithmus dagegen tiefe und schmale.

Breitensuche: Man startet in einer beliebigen Ecke e_0. Im i-ten Schritt wählt man $e_i \in E \setminus \{e_0, \ldots, e_{i-1}\}$, so dass es eine Kante k_i zwischen e_i und $e_j \in \{e_0, \ldots, e_{i-1}\}$ für minimales j gibt. Die Kanten $k_1, \ldots, k_{|E|-1}$ bilden dann den Baum.

Tiefensuche: Man startet in einer beliebigen Ecke e_0. Im i-ten Schritt wählt man $e_i \in E \setminus \{e_0, \ldots, e_{i-1}\}$, so dass es eine Kante k_i zwischen e_i und $e_j \in \{e_0, \ldots, e_{i-1}\}$ für maximales j gibt. Wieder bilden die Kanten $k_1, \ldots, k_{|E|-1}$ den Baum.

Wieviele Bäume mit n Ecken gibt es? Wie bei allgemeinen Graphen kann man nur nummerierte Bäume explizit zählen. (Anders betrachtet geht es also um die Anzahl der aufspannenden Bäume eines K_n, bei dem man die Ecken unterscheiden kann.)

Dazu zunächst eine Definition: Ein *Wurzelbaum* ist ein Baum mit einer ausgezeichneten Ecke, der sogenannten *Wurzel*. Jeder Wurzelbaum trägt eine natürliche Orientierung der Kanten, etwa von der Wurzel weg. Daher ist es sinnvoll, von Vorgängern und Nachfolgern einer Ecke zu sprechen. Blätter sind dann die Ecken ohne Nachfolger; die Wurzel ist die einzige Ecke ohne Vorgänger. (Achtung: Außer bei dem trivialen Wurzelbaum, der nur aus der Wurzel besteht, ist die Wurzel in einem Wurzelbaum kein Blatt. In dem zugrundeliegenden normalen Baum könnte der die Wurzel bildende Knoten aber durchaus ein Blatt sein, genau dann nämlich, wenn er nur einen Nachbarn hat, wenn also die Wurzel im Wurzelbaum nur einen Nachfolger hat.)

Satz 7.3 (Cayley) *Es gibt n^{n-2} numerierte Bäume auf n Ecken.*

Beweis: Statt Bäume zählt man *Wirbeltiere*, das sind Bäume mit zwei ausgezeichneten Ecken, dem *Kopf* K und dem *Schwanz* S. Es gibt n^2 Möglichkeiten, K und S zu wählen, denn $K = S$ ist gestattet. Der Satz von Cayley behauptet also, dass es n^n Wirbeltiere mit n Ecken gibt. Dies ist aber genau die Anzahl der Funktionen der Menge $\{1, \ldots, n\}$ in sich selbst. Zum Beweis wird also jedem Wirbeltier eineindeutig eine Funktion und umgekehrt zugeordnet.

Ein Wirbeltier ist bestimmt durch

- eine nicht-leere Teilmenge $R = \{e_1, \ldots, e_r\} \subseteq E$, dem sogenannten *Rückgrat*, das aus den Ecken des eindeutigen K und S verbindenden Pfades besteht;
- einer Ordnung auf R (die Ecken von K als minimalem Element bis S als maximales Element geordnet);
- einer Aufteilung der Restecken $E \setminus R$ in r eventuell leere Teile $E_1, \ldots, E_r$;
- einem Wurzelbaum auf $E_i \cup \{e_i\}$ mit Wurzel e_i.

Einer Funktion $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$ ordnen wir zunächst den gerichteten Graphen mit Ecken $\{1, \ldots, n\}$ und Kanten $(i, f(i))$ zu. Sei R die Menge der Ecken, die auf gerichteten Kreisen liegen. Auf R induziert f eine Permutation. Lässt man die Kanten der gerichteten Kreise fort, so

bilden die Zusammenhangskomponenten des Restgraphen Wurzelbäume mit Wurzel in R und natürlicher Orientierung zur Wurzel hin.

Da es gleich viele Permutationen wie totale Ordnungen gibt, sind also Wirbeltiere und Funktionen durch gleichwertige Daten gegeben. Die Zuordnung von Permutation und totaler Ordnung ist allerdings nicht kanonisch, sondern bedarf einer Auswahl (dem Bild der Identitätspermutation etwa.) □

Häufig tauchen in Anwendungen sogenante *Suchbäume* auf. Dies sind Wurzelbäume (mit gedachter Orientierung von der Wurzel weg), bei der die Nachfolger einer Ecke geordnet sind. Solche Bäume tauchen als Modell für Entscheidungs– oder Suchvorgänge auf: Jede Ecke steht für eine Entscheidung oder Anfrage, die auslaufenden Kanten für die Möglichkeiten oder Antworten. Suchbäume zählt man eher nach der Anzahl der Blätter. Ein (n, q)-*Baum* ist ein Suchbaum mit n Blättern, bei dem jede Ecke höchstens q direkte Nachfolger hat. Ein *vollständiger* (n, q)-*Baum* ist einer, bei dem jede Ecke, die kein Blatt ist, genau q Nachfolger hat. Zur Erinnerung: Die Anzahl der vollständigen $(n, 2)$-Bäume ist C_n, die n-te Catalan–Zahl.

II.8 Optimierungsprobleme

Paarungen

Definition 8.1 *Eine* Paarung *(Matching) in einem Graphen* G *ist eine Menge von paarweise nicht-adjazenten Kanten (d.h. je zwei Kanten der Paarung haben keine Ecke gemeinsam). Die* Paarungszahl $m(G)$ *ist das Maximum der Mächtigkeiten von Paarungen in* G*. Eine Paarung* P *heißt* maximal*, falls* $|P| = m(G)$*, und* perfekt*, falls alle Ecken zu* P *inzident sind, falls also* $2|P| = |E|$*.*

Paarungen treten zum Beispiel bei Sportturnieren auf: Die Ecken des Graphen sind die Mannschaften, die Kanten stehen für noch ausstehende Spiele zwischen Mannschaften, und die Begegnungen des nächsten Spieltages bilden die Paarung.

Es gilt offenbar stets $m(G) \leqslant \lfloor \frac{|E|}{2} \rfloor$; diese Schranke wird etwa bei K_n und C_n auch angenommen. Für gerade n haben K_n und C_n also perfekte Paarungen. Dagegen ist $m(K_{1,n}) = 1$.

Der gängige Begriff der „maximalen Paarung“ widerspricht etwas dem üblichen Gebrauch des Wortes „maximal“ in der Mathematik: Es kann vorkommen, dass eine Paarung nicht mehr durch Hinzufügen einer Kante zu einer größeren Paarung erweitert werden kann, ohne darum eine maximale Paarung im Sinne der Definition zu sein. Zum Beispiel bildet in einem Pfad der Länge 3 die mittlere Kante eine nicht mehr vergrößerbare, aber nicht maximale Paarung.

Ein P-*alternierender Pfad* ist ein Pfad $e_0 k_1 e_1 \dots e_{2n+1}$ ungerader Länge, bei dem die Kanten mit geradem Index in P und die mit ungeradem Index nicht in P liegen und die End-Ecken e_0, e_n zu keiner Kante in P inzident sind, d.h. man kann den Pfad nicht alternierend verlängern.

Satz 8.1 P *ist genau dann maximale Paarung, wenn es keine* P*-alternierenden Pfade gibt.*

Beweis: Gibt es einen P-alternierenden Pfad wie oben, so ist $P' := P \setminus \{k_2, k_4, \dots, k_{2n}\} \cup$

$\{k_1, k_3, \dots k_{2n+1}\}$ eine um ein Element größere Paarung.

Sei umgekehrt P eine nicht-maximale Paarung. Dann gibt es eine größere Paarung, und damit (nach eventuellem Weglassen von Kanten) auch eine Paarung P' mit $|P'| = |P| + 1$. Sei nun $N := (P \setminus P') \cup (P' \setminus P)$. Dann ist $|N|$ ungerade und enthält eine Kante mehr aus P' als aus P. Da von keiner Ecke mehr als eine Kante in P bzw. in P' ausgehen kann, können von keiner Ecke mehr als zwei Kanten in N ausgehen. Die Zusammenhangskomponenten des von N aufgespannten Untergraphen sind daher entweder zwischen P und P' abwechselnde Kreise (mit gerader Kantenzahl) oder zwischen P und P' abwechselnde Pfade. Da die Gesamtkantenzahl ungerade ist mit mehr Kanten aus P' als aus P, muss es einen solchen Pfad mit Anfangs- und Endkante aus P' geben. Dies ist dann ein P-alternierender Pfad (denn wären eine End-Ecke e mit einer Kante aus P inzident, so mit einer Kante aus $P \setminus N$, also aus $P \cap P'$, d.h. von e würden zwei Kanten aus P' ausgehen, was nicht erlaubt ist). □

Dieser Satz ist konstruktiv, d.h. er liefert einen (sogar polynomialen) Algorithmus zur Konstruktion maximaler Paarungen, indem man nach und nach P-alternierende Pfade bestimmt und jedesmal die Paarung entsprechend vergrößert.

Paarungen werden meist in bipartiten Graphen betrachtet – oft handelt es sich um Zuordnungsprobleme, wie im Beispiel des Heiratsproblems: Ist es möglich, n Frauen mit n Männern, von denen manche untereinander befreundet sind, so zu verheiraten, dass nur befreundete Paare heiraten? Die Personen werden durch die Ecken, die Freundschaftsrelation durch die Kanten eines bipartiten Graphen wiedergegeben; die Auswahl von Ehepartnern ist eine Paarung.

Für $A \subseteq E$ sei $N(A) := \bigcup_{a \in A} N(a)$ die Menge der Nachbarn von A. Die *Heiratsbedingung für* E' ist die Eigenschaft $|A| \leqslant |N(A)|$ für alle $A \subseteq E'$.

Satz 8.2 (Heiratssatz von Hall) *Sei* $G = (E, K)$ *ein Graph mit Bipartition* $E = E' \cup E''$. *Dann gilt* $m(G) = |E'|$ *genau dann, wenn* G *die Heiratsbedingung für* E' *erfüllt.*

Beweis: "⇒" ist klar, da eine maximale Paarung für jedes $a \in A$ einen verschiedenen Nachbarn aus E'' auswählt.

„⇒": Sei P eine maximale Paarung. Falls $|P| < |E'|$, so gibt es ein $e_0 \in E'$, das zu keiner Kante aus P inzident ist. Induktiv werden nun paarweise verschiedene $f_i \in E''$ gefunden und anschließend $e_i \in E' \setminus \{e_0, \dots, e_{i-1}\}$, mit folgenden Bedingungen:

- $\{f_1, \dots, f_k\} \subseteq N\big(\{e_0, \dots, e_{k-1}\}\big)$ – das geht wegen der Heiratsbedingung für E'
- $(e_i, f_i) \in P$.

Das Verfahren bricht ab, wenn ein f_i gefunden wird, das zu keiner Kante aus P inzident ist. Von diesem kann man dann rückwärts einen P-alternierenden Pfad bis zu e_0 verfolgen mit Widerspruch zur Maximalität. □

Satz 8.3 *Sei* G *wie oben. Dann gilt* $m(G) = |E'| - \max_{A \subseteq E'} \big\{|A| - |N(A)|\big\}$.

Beweis: Offenbar sind für jede Paarung P und jedes $A \subseteq E'$ mindestens $|A| - |N(A)|$ viele Ecken nicht inzident zu P, woraus „⩽" folgt.

Sei nun $A \subseteq E'$ so, dass das Maximum in der Behauptung des Satzes angenommen wird. Dann erfüllt $G\big[(E' \setminus A) \cup (E'' \setminus N(A))\big]$ die Heiratsbedingung für $E' \setminus A$, denn gäbe es ein $A' \subseteq E' \setminus A$, das ihr widerspräche, so wäre $|A \cup A'| - |N(A \cup A')| > |A| - |N(A)|$. Andererseits erfüllt auch $G[A \cup N(A)]$ die Heiratsbedingung für $N(A)$, denn gäbe es ein $A'' \subseteq N(A)$, das ihr widerspräche, so wäre $|A \setminus N(A'')| - |N(A \setminus N(A''))| = |A \setminus N(A'')| - |N(A) \setminus A''| > |A| - |N(A)|$. Man wählt nun für beide induzierte Subgraphen eine maximale Paarung, die nach dem Heiratssatz die Mächtigkeiten $|E' \setminus A|$ bzw. $|N(A)|$ haben. Zusammen ergeben diese eine Paarung von G der Mächtigkeit $|E'| - |A| + |N(A)|$. □

Eine *Eckenüberdeckung* in einem Graphen ist eine Menge von Ecken, zu der jede Kante inzident ist.

Satz 8.4 (König) *Die minimale Mächtigkeit einer Eckenüberdeckung eines bipartiten Graphen ist gleich* $m(G)$.

Beweis: Offenbar gilt „$\geqslant$“, da für jede Kante in einer Paarung eine (verschiedene) Ecke in der Überdeckung sein muss. Umgekehrt ist $(E' \setminus A) \cup N(A)$ im Beweis von Satz 8.3 eine Eckenüberdeckung der Mächtigkeit $m(G)$. □

Der Satz von König ist ein Beispiel für ein in der Graphentheorie häufig auftretendes „Dualitätsphänomen“: Die minimale Lösung eines Problems entspricht der maximalen Lösung eines dualen Problems. Der Satz von König stimmt nicht für allgemeine Graphen: Zum Beispiel ist $m(C_5) = 2$, eine minimale Eckenüberdeckung besteht aber aus drei Ecken.

Gewichtete Paarungen

Nun betrachten wir bipartiten Graphen $G = (E' \cup E'', K)$ mit einer Gewichtsfunktion $w : K \to \mathbb{N}$ auf den Kanten. Die Gewichte sollen natürliche Zahlen sein; rationale Gewichte kann man durch Multiplikation mit dem Hauptnenner auf diesen Fall zurückführen; reelle Gewichte durch rationale beliebig genau annähren. Gesucht ist eine maximale Paarung minimalen Gewichts. Wie üblich ist dabei das Gewicht einer Paarung definiert als die Summe der Gewichte ihrer Kanten.

Für das entsprechende Problem, eine maximale Paarung maximalen Gewichts zu finden, ersetzt man die Gewichtsfunktion durch $w_{\max} - w$, wobei $w_{\max}$ das maximale Gewicht ist.

Zunächst kann man durch Hinzufügen neuer Ecken und neuer Kanten mit großem Gewicht (größer als die Summe der bisherigen Gewichte) annehmen, dass G der vollständige bipartite Graph $K_{n,n}$ ist. Die beiden Eckenmengen der Bipartition seien $E' = \{e_1, \ldots, e_n\}$ und $E'' = \{f_1, \ldots, f_n\}$. Den bipartiten gewichteten Graphen kann man nun durch eine (n, n)-Matrix W mit Einträgen $w_{ij} = w((e_i, f_j))$ darstellen. Eine maximale Paarung entspricht nun einer sogenannten *Diagonalen*, d.h. einer Auswahl von n Einträgen der Matrix, von denen keine zwei in einer Spalte oder einer Zeile liegen. Ziel ist es nun, eine Diagonale mit minimaler Summe ihrer Einträge zu finden. Offenbar ändert man an der Lösungsmenge nichts, wenn man von einer Spalte bzw. einer Zeile einen festen Betrag abzieht.

Algorithmus zum Finden einer minimalen Diagonalen:

1. Schritt: Man zieht von jeder Zeile den minimalen Eintrag in dieser Zeile ab (dadurch entsteht in jeder Zeile eine 0). Dann zieht man von jeder Spalte den minimalen Eintrag in dieser Spalte ab (und erhält auch in jeder Spalte eine 0).

2. Schritt: Gibt es in W eine Diagonale aus lauter Nullen? Falls ja, so entspricht sie einer maximalen Paarung minimalen Gewichts.

Falls nein, so sucht man eine Überdeckung sämtlicher in W vorkommenden Nullen durch eine minimale Anzahl von Spalten und Zeilen. Eine solche Überdeckung entspricht einer Eckenüberdeckung in dem Graphen $G' = (E, K')$ mit $K' = \{(e_i, f_j) \mid w_{ij} = 0\}$. Nach dem Satz von König besteht diese aus weniger als n Spalten und Zeilen (denn sonst wäre man im Fall „ja“ oben). Sei nun m das Minimum der Werte, die weder in einer Spalte noch in einer Zeile dieser Überdeckung liegen. Man zieht m von allen nicht–überdeckten Zeilen ab und addiere es zu allen überdeckten Spalten. Dabei bleiben alle Einträge $\geqslant 0$. Nun wird W durch die entstandene Matrix ersetzt und Schritt 2 wiederholt. Da es insgesamt weniger als n überdeckte Zeilen und Spalten gibt, wird m insgesamt häufiger abgezogen als hinzuaddiert, das Gesamtgewicht der Matrix wird also verringert. Da die Gewichte in $\mathbb{N}$ liegen, muss der Algorithmus nach endlich vielen Schritten abbrechen.

Flüsse in Netzwerken

Ein *gerichteter Graph* ist ein Paar (E, K) bestehend aus einer (endlichen) Eckenmenge E und einer Menge gerichteter Kanten K, d.h. einer binären Relation auf E. Für $k = (e, e') \in K$ sei $e = k^-$ die *Anfangs–* oder *Startecke*, $e' = k^+$ die *End–* oder *Zielecke* der Kante. Für eine Ecke e definiert man den *Ein-Grad* $d^+(e) := |\{k \mid e = k^+\}|$ als die Anzahl der hineinlaufenden Kanten und den *Aus-Grad* $d^-(e) := |\{k \mid e = k^-\}|$ als die Anzahl der hinauslaufenden Kanten.

Jedem gerichteten Graphen liegt ein ungerichteter Graph zugrunde: Dieser hat dieselben Ecken und Kanten, wobei man die Orientierungen vergisst, Schleifen weglässt und eventuelle Mehrfachkanten identifiziert. Formal ergibt sich $G' = (E, K')$ mit $(e, e') \in K' \iff [e \neq e'$ und $(e, e') \in K$ oder $(e', e) \in K]$.

Ein *gerichteter Weg*, der Länge n, von e_0 nach e_n, ist eine Folge $e_0 k_1 e_1 \dots k_n e_n$ von Ecken e_i und Kanten $k_{i+1} = (e_i, e_{i+1})$. Entsprechend sind gerichtete Züge, Pfade und Kreise definiert. Die Eigenschaft, dass es zwischen zwei Ecken e, e' einen gerichteten Weg von e nach e' und einen gerichteten Weg von e' nach e gibt, definiert eine Äquivalenzrelation, deren Klassen *starke Zusammenhangskomponenten* heißen. Die starken Zusammenhangskomponenten sind Vereinigungen gerichteter Kreise. Ein gerichteter Graph heißt *stark zusammenhängend*, falls er nur aus einer starken Zusammenhangkomponente besteht, und (schwach) zusammenhängend, falls der zugrundeliegende ungerichtete Graph zusammenhängend ist.

Definition 8.2 *Ein* Netzwerk *ist ein (o.E. zusammenhängender) gerichteter Graph* $G = (E, K)$ *mit zwei ausgezeichneten Ecken* $e_{ein} \neq e_{aus}$*, so dass ein gerichteter Weg von* e_{ein} *nach* e_{aus} *existiert, und mit einer* Kapazitätsfunktion $c : K \to \mathbb{R}_0^+ \cup \{\infty\}$.

Man nennt e_{ein} den *Eingang*, e_{aus} den *Ausgang* des Netzwerkes und alle anderen Ecken *innere*

Ecken. Allgemeiner könnte man Netzwerke mit mehreren Ein– und Ausgängen betrachten. Diese kann man aber auf die oben definierten Netzwerke zurückführen, indem man einen neuen Ein– bzw. Ausgang mit Kanten mit unendlicher Kapazität zu bzw. von den alten Ein– bzw. Ausgängen hinzunimmt. Manchmal fügt man eine Rückflusskante von e_{aus} nach e_{ein} mit unendlicher Kapazität zu.

Ein *Fluss* in einem gerichteten Graphen $G = (E, K)$ ist eine Funktion $f : K \to \mathbb{R}_0^+$. Der Wert W_e des Flusses f in einer Ecke e ist die Differenz von „Einfluss“ und „Ausfluss“, d.h. $W_e(f) := \sum_{k^+=e} c(k) - \sum_{k^-=e} c(k)$. Der *Wert des Flusses* $W(f)$ ist sein Wert im Augang e_{aus}.

Definition 8.3 *Ein Fluss f in einem Netzwerk $G = (E, K, c)$ heißt* verträglich, *falls einerseits $f(k) \leqslant c(k)$ für alle Kanten k gilt und andererseits der Wert des Flusses an allen inneren Ecken gleich Null ist („Kirchhoffs Gesetz“).*

Da offenbar stets $\sum_{e\in E} W_e(f) = 0$ gilt, folgt für einen verträglichen Fluss $W(f) = -W_{e_{\text{ein}}}(f)$.

Gesucht ist nun für ein gegebenes Netzwerk ein verträglicher Fluss maximalen Wertes.

Satz 8.5 *Ein verträglicher Fluss maximalen Wertes existiert stets.*

Beweis: Sei $\{f_i \mid i \in I\}$ die Menge der verträglichen Flüsse. Falls die Wertfunktion W darauf kein Maximum annimmt, so gibt es eine Teilfamilie $\{f_{i_j} \mid j \in \mathbb{N}\}$ mit $\sup\{W(f_{i_j}) \mid j \in \mathbb{N}\} = \sup\{W(f_i) \mid i \in I\}$ und so, dass $(f_{i_j}(k))_{j\in\mathbb{N}}$ für jede Kante k eine monotone Folge bildet. Man rechnet leicht nach, dass dann durch $f(k) := \lim_{j\in\mathbb{N}} f_{i_j}(k)$ ein verträglicher Fluss definiert wird mit Wert $W(f) = \sup\{W(f_i) \mid i \in I\}$: Widerspruch. □

Ein *Schnitt* (X, Y) ist eine Partition $E = X \cup Y$ der Eckenmenge mit $e_{\text{ein}} \in X$ und $e_{\text{aus}} \in Y$. Sei $K(X, Y) = \{k \in K \mid k^- \in X, k^+ \in Y\}$ die Menge der von X nach Y laufenden Kanten. Die *Kapazität* des Schnittes ist $c(X, Y) := \sum_{k\in K(X,Y)} c(k)$.

Satz 8.6 *Für jeden verträglichen Fluss f und jeden Schnitt (X, Y) gilt $W(f) \leqslant c(X, Y)$.*

Beweis: Da $e_{\text{aus}} \in Y$ und $W_e(f) = 0$ für die anderen $e \in Y$ gilt, folgt:

$$W(f) = W_{e_{\text{aus}}}(f) = \sum_{e\in Y} w_e(f) = \sum_{e\in Y, e=k^+} f(k) - \sum_{e\in Y, e=k^-} f(k) \leqslant \sum_{k\in K(X,Y)} f(k) - 0 \leqslant \sum_{k\in K(X,Y)} c(k) = c(X, Y)$$

□

Ein *zunehmender Zug* für einen verträglichen Fluss f ist ein ungerichteter Zug $e_0 k_1 e_1 \dots k_n e_n$, wobei $f(k_i) < c(k_i)$ für alle *Vorwärtskanten* $k_i = (e_{i-1}, e_i)$ und $f(k_i) > 0$ für alle *Rückwärtskanten* $k_i = (e_i, e_{i-1})$ in dem Zug gilt. Die *Restkapazität* des zunehmenden Zuges Z ist

$$r_f(Z) := \min\Big(\big\{c(k_i) - f(k_i) \;\big|\; k_i \text{Vorwärtskante}\big\} \cup \big\{f(k_i) \;\big|\; k_i \text{Rückwärtskante}\big\}\Big)$$

Der zu Z gehörige *elementare Fluss* f_Z ist definiert durch $f_Z(k) = 1$ für alle Vorwärtskanten, $f_Z(k) = -1$ für alle Rückwärtskanten und $f_Z(k) = 0$ für alle in Z nicht vorkommenden Kanten.

Dies ist kein Fluss im Sinne der obigen Definition, da er negative Werte annimmt; falls aber Z von e_{ein} nach e_{aus} läuft, so erfüllt f_Z die Verträglichkeitsbedingungen. Insbesondere ist dann $f + r_f(Z) \cdot f_Z$ ein verträglicher Fluss.

Außerdem definiert man

$$X_f := \{e \mid \text{ es gibt einen zunehmenden Zug von } e_{ein} \text{ nach } e\} \quad \text{und} \quad Y_f = E \setminus X_f.$$

Insbesondere gilt also $e_{ein} \in X_f$.

Satz 8.7 (Ford, Fulkerson) *Es sind äquivalent:*

- f *ist Fluss maximalen Wertes.*
- *Es gibt keine zunehmenden Züge von* e_{ein} *nach* e_{aus}.
- (X_f, Y_f) *ist ein Schnitt.*

Es gilt dann: (X_f, Y_f) *ist ein Schnitt minimaler Kapazität mit* $c(X_f, Y_f) = W(f)$.

Beweis: (a)⇒(b) Wäre Z solch ein Zug, so wäre $f + r_f(Z) \cdot f_Z$ ein Fluss vom Wert $W(f) + r_f(Z)$.

(b)⇒(c) Alle Bedingungen eines Schnittes sind stets erfüllt bis auf $e_{aus} \in Y_f$, was gerade die Aussage von (b) ist.

(c)⇒(a) Für alle Kanten $k \in K(X_f, Y_f)$ gilt $f(k) = c(k)$, denn sonst könnte man den zu k^- hinführenden zunehmenden Zug noch um k verlängern; ebenso $f(k) = 0$ für alle $k \in K(Y_f, X_f)$. Es folgt dann, dass in der Rechnung im Beweis von Satz 8.6 überall Gleichheit steht, also dass $W(f) = c(X_f, Y_f)$ gilt. Insbesondere ist f maximal. □

Man sieht, dass $K(X_f, Y_f)$ beim maximalen Fluss f aus lauter *saturierten* Kanten besteht, d.h. Kanten, in denen der Wert des Flusses gleich der Kapazität ist. Umgekehrt ist ein Fluss, der einen Schnitt aus saturierten Kanten zulässt, schon maximal.

Folgerung aus dem Beweis:
In einem Netzwerk mit ganzzahligen Kapazitäten gibt es einen maximalen ganzzahligen Fluss.

Algorithmus zum Finden eines maximalen Flusses:

- Man startet mit dem Null–Fluss
- Induktiv such man nach zunehmenden Zügen (z.B. mit einem für gerichtete Graphen angepassten Tiefensuchalgorithmus — in diesen Graphen nimmt man alle Vorwärtskanten, auf denen den Fluss die Kapazität nicht erreicht, und alle Rückwärtskanten mit positivem Fluss). Dann addiert man den mit der Restkapazität multiplizierten elementaren Fluss hinzu.

Bei ganzzahligen (und damit auch bei rationalen) Kapazitäten ist klar, dass der Algorithmus terminiert, da sich der Wert des Flusses in jedem Schritt um mindestens 1 erhöht. Bei reellen Werten ist die Argumentation etwas schwieriger, ähnlich wie in 8.5.

Meist ist es geschickt, im Algorithmus zunächst nach gerichteten zunehmenden Zügen zu suchen. Gibt es keine solchen mehr, so hat man einen *vollständigen Fluss* erreicht, d.h. ein Fluss, in dem jeder gerichtete Zug von e_{ein} nach e_{aus} eine saturierte Kante enthält.

Aus dem Satz von Ford–Fulkerson erhält man ziemlich einfach den wichtigen Satz von Menger. Dazu einige Definitionen: Zwei Ecken e, e' werden durch Ecken $e_1, \ldots, e_m$ (bzw. Kanten

$k_1, \ldots, k_m$) *getrennt*, falls e und e' in $G[E \setminus \{e_1, \ldots, e_m\}]$ (bzw. in $(E, K \setminus \{k_1, \ldots, k_m\})$ in verschiedenen Zusammenhangskomponenten liegen. Pfade (bzw. Züge) zwischen e und e' heißen *unabhängig*, falls sie paarweise außer e und e' keine Ecke (bzw. paarweise keine Kante) gemeinsam haben.

Satz 8.8 (Menger, lokale Version)

(a) *Seien e, e' zwei Ecken. Dann ist die minimale Anzahl von e und e' trennenden Kanten die maximale Anzahl unabhängiger Züge zwischen e und e'.*

(b) *Seien e, e' zwei nicht-benachbarte Ecken. Dann ist die minimale Anzahl von e und e' trennenden Ecken die maximale Anzahl unabhängiger Pfade zwischen e und e'.*

Beweis–Skizze: (a) „$\geqslant$“ ist klar. Für „$\leqslant$“ macht man aus dem Graphen ein Netzwerk mit Eingang e, Ausgang e', jede Kante wird durch gerichtete Kanten in beide Richtungen ersetzt und die Kapazitätsfunktion ist konstant $= 1$. Der Wert eines maximalen Flusses ist dann die Anzahl unabhängiger Züge; die trennenden Kanten die des zugehörigen Schnittes.

(b) Hier verfährt man zunächst wie in (a), die Kapazität der Kanten ist aber konstant $= \infty$. Dann ersetzt man jede Ecke e durch zwei Ecken e^- und e^+ mit einer Kante (e^-, e^+) mit Kapazität 1; Kanten nach e verlaufen nach e^-, Kanten von e laufen aus e^+ heraus. □

Eine schlechte und zwei gute Heuristiken für das Problem des Handlungsreisenden

Sei $K_n = (E, K)$ mit $w : K \to \mathbb{R}_0^+$ gegeben. Im folgenden seien drei polynomiale Näherungs–Algorithmen für das Problem des Handlungsreisenden vorgestellt.

Die Heuristik des nächsten Nachbarn

- Man startet in einer beliebigen Ecke.
- Vom jeweiligen Standpunkt e aus besucht man als nächstes diejenige der noch nicht besuchten Ecken e', welche das Kantengewicht von (e, e') minimiert.
- Wenn alle Ecken besucht sind, kehrt man zur Ausgangsecke zurück.

Für diese Heuristik gibt es keine Gütegarantie.

Die Heuristik des minimalen aufspannenden Baumes

- Man konstruiert einen aufspannenden Baum B minimalen Gewichts.
- Man verdoppelt alle Kanten und sucht einen Euler–Zug in dem entstehenden Eulerschen Multigraphen.
- Durch Überspringen bereits besuchter Ecken kann man diesen Euler–Zug zu einem Hamiltonschen Kreis zusammenziehen (sofern dadurch das Gewicht nicht größer wird, also beispielsweise falls die Dreiecksungleichung erfüllt ist).

Das Gewicht der Ergebniskreises ist nach Konstruktion höchstens das Doppelte des Gewichts der aufspannenden Baums. Da die optimale Lösung auch einen aufspannenden Baum enthält,

liefert diese Heuristik eine Lösung, die nicht mehr als das doppelte Gewicht der optimalen Lösung hat.

Die Christofides–Heuristik

- Man konstruiert einen aufspannenden Baum B minimalen Gewichts.
- Man sucht eine maximale Paarung minimalen Gewichts P auf der Menge U der (geradzahlig vielen) Ecken ungeraden Grades im Ausgangsgraphen K_n. (Dafür gibt es einen hier nicht vorgestellten polynomialen Algorithmus.)
- Man nimmt die Kanten aus P zu B hinzu und sucht einen Euler–Zug in dem entstandenen Eulerschen Multigraphen.
- Durch Überspringen bereits besuchter Ecken kann man gegebenenfalls diesen Euler–Zug zu einem Hamiltonschen Kreis zusammenziehen.

Falls die Gewichtsfunktion die Dreiecksungleichung erfüllt, ergibt sich bei der Christofides–Heuristik höchstens das Anderthalbfache des optimalen Ergebnisses.

Teil III: Algebraische Strukturen

III.9 Gruppen

Definition 9.1 *Eine* Gruppe $(G, \circ)$ *besteht aus einer nicht-leeren Menge* G *und einer zweistelligen Operation* $\circ : G \times G \to G$ *mit folgenden Eigenschaften:*

- $\circ$ *ist assoziativ, d.h.* $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$ *für alle* $g_1, g_2, g_3 \in G$*;*
- *es gibt ein* neutrales Element $e \in G$*, d.h. es gilt* $g \circ e = e \circ g = g$ *für alle* $g \in G$*;*
- *für jedes* $g \in G$ *gibt es ein* inverses Element*, d.h. ein* $h \in G$ *mit* $g \circ h = h \circ g = e$*.*

Gilt zusätzlich $g \circ h = h \circ g$ *für alle* $g, h \in G$*, so heißt die Gruppe* kommutativ *oder* abelsch*.*

Die Ordnung *der Gruppe ist die Anzahl ihrer Elemente.*

Das Inverse ist eindeutig bestimmt: Angenommen h und h' sind Inverse von g, so gilt: $h = h \circ e = h \circ (g \circ h') = (h \circ g) \circ h' = e \circ h' = h'$. (Man braucht hierfür nur, dass h ein Links– und h' ein Rechtsinverses von g ist.) Man schreibt dann $h = g^{-1}$ für das inverse Element von g. Allgemeiner ist jede Gleichung $g \circ x = h$ bzw. $y \circ g = h$ eindeutig lösbar, nämlich durch $x = g^{-1} \circ h$ und $y = h \circ g^{-1}$.

Ebenso sieht man, dass e eindeutig bestimmt ist. Manchmal spezifiziert man das neutrale Element und schreibt die Gruppe als $(G, e, \circ)$. Gerne schreibt man Gruppen multiplikativ, d.h. man lässt das Zeichen $\circ$ weg und schreibt 1 statt e. Im folgenden werden beide Möglichkeiten gemischt auftreten. Kommutative Gruppen notiert man oft additiv, d.h. mit $+$ statt $\circ$, 0 statt e und $-g$ statt g^{-1}.

Beispiele:

- $(\mathbb{Z}, 0, +)$ und die endlichen Gruppen $(\mathbb{Z}_m, 0, +)$, wobei $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, wobei $a + b$ in $\mathbb{Z}_m$ der Rest von $a + b$ in $\mathbb{Z}$ bei der Division mit Rest durch m ist.
- $(K, 0, +)$ und $(K \setminus \{0\}, 1, \cdot)$ für Körper K, z.B. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- $(K^{>0}, 1, \cdot)$ für angeordnete Körper K, z.B. $K = \mathbb{Q}, \mathbb{R}$.
- Dagegen ist $(\mathbb{Z} \setminus \{0\}, 1, \cdot)$ keine Gruppe.
- $(\mathrm{Sym}(M), \mathrm{id}, \circ)$ für eine Menge M.
- $(\mathrm{Aut}(G), \mathrm{id}, \circ)$ für einen Graphen G, oder allgemeiner Automorphismen einer Struktur.
- Symmetriegruppen und Drehgruppen, z.B. die Symmetriegruppe D_n des regelmaßigen n-Ecks; die Drehgruppe eines Würfels oder eines anderen Polyeders.
- Matrizengruppen, z.B. $\mathrm{GL}(n, \mathbb{Q})$.

Seien $(G, e_g, \circ_G)$ und $(H, e_h, \circ_H)$ zwei Gruppen. Eine Abbildung $\varphi : G \to H$ heißt (Gruppen–) *Homomorphismus*, falls

- für alle $g_1, g_2 \in G$ gilt $\varphi(g_1 \circ_G g_2) = \varphi(g_1) \circ_H \varphi(g_2)$;
- $\varphi(e_G) = e_H$;
- und für alle $g \in G$ gilt $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

Man kann zeigen, dass die erste Bedingung bereits die beiden anderen Bedingungen impliziert. Ein bijektiver Gruppenhomomorphismus, dessen Umkehrabbildung auch ein Gruppenhomomorphismus ist, heißt *(Gruppen–)Isomorphismus*. Man kann zeigen, dass ein bijektiver Gruppenhomomorphismus immer schon ein Gruppenisomorphismus ist.

Für einen Homomorphismus $\varphi : G \to H$ definiert man das *Bild* als $\{\varphi(g) \mid g \in G\}$ und den *Kern* als $\{g \in G \mid \varphi(g) = e_H\}$.

Monoide

Eine Struktur, die eine assoziative binäre Verknüpfung mit neutralem Element trägt, heißt *Monoid* (gesprochen: Mono-id). Ein Monoid ist also ähnlich definiert wie eine Gruppe, es muss lediglich keine inversen Elemente geben.

Ein Monoidhomomorphismus zwischen zwei Monoiden $(M_i, \circ, e)$ ist analog zum Gruppenhomomorphismus definiert. Allerdings reicht hier die Bedingung $\varphi(m \circ m') = \varphi(m) \circ \varphi(m')$ nicht aus, um $\varphi(e) = e$ zu implizieren.

Wenn M eine Menge ist, dann gibt es das *von* M *erzeugte freie Monoid* M^*, das aus allen endlichen Folgen von Elementen aus M besteht. Die Verknüpfung ist die *Konkatenation*, d.i. das Hintereinandersetzen zweier Folgen, das neutrale Element ist die leere Folge. Man spricht dann auch von M als einem *Alphabet*, von den Elementen von M als *Buchstaben* und von den Elementen von M^* als *Wörtern* über M.

Ähnlich kann man auch die *von* M *erzeugte freie Gruppe* F_M konstruieren: Zunächst sei $m \mapsto \overline{m}$ eine Bijektion von M auf eine zu M disjunkte gleichmächtige Menge $\overline{M}$, und man bildet $W := (M \cup \overline{M})^*$. Auf dem Monoid W identifiziert man nun zwei Wörter, wenn das eine aus dem anderen durch *Reduzieren* entsteht, was bedeutet, dass man Buchstaben m und $\overline{m}$, die direkt aneinanderstoßen, entfernen darf. Die dadurch erzeugte Äquivalenzrelation ist eine Kongruenzrelation für das Monoid W, der Quotient F_M ist eine Gruppe. Anders formuliert besteht F_M aus den *reduzierten Wörtern*, das sind die Wörter in W, in denen nicht ein Buchstabe m direkt vor oder hinter $\overline{m}$ steht. Die Verknüpfung besteht im Hintereinanderschreiben und anschließenden Reduzieren der Wörter (wobei man sich leicht plausibel machen kann, dass das Endergebnis des Reduzierens nicht von der Reihenfolge abhängt).

Untergruppen

Sei im folgenden $(G, e, \circ)$ eine feste Gruppe.

Definition 9.2 *Eine Teilmenge* $U \subseteq G$ *heißt* Untergruppe *von* G*, in Zeichen* $U \leqslant G$*, falls* $(U, e, \circ\restriction_{U \times U})$ *eine Gruppe ist, d.h. falls* $e \in U$ *und mit* $u, u' \in U$ *auch* $u^{-1} \in U$ *und* $u \circ u' \in U$*.*

Ist U eine Untergruppe von G, so ist die Inklusionsabbildung $U \to G$ ein Gruppenhomomorphismus.

Beispiele:

- $\{e\}$ und G selbst sind die *trivialen* Untergruppen von G.
- Ist $U \leqslant V \leqslant G$, so $U \leqslant G$.
- Das *Zentrum* $Z(G) := \{g \in G \mid g \circ h = h \circ g \text{ für alle } h \in G\}$ einer Gruppe G.
- Ist φ ein Gruppenhomomorphismus, so sind Bild(φ) und Kern(φ) Untergruppen.
- Die Untergruppen von $(\mathbb{Z}, +)$ sind $m\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$.

Sei $A \subseteq G$. Dann ist der Schnitt über alle A enthaltenden Untergruppen von G wieder eine Untergruppe, die *von* A *erzeugte Untergruppe* $\langle A \rangle$. Falls $\langle A \rangle = G$, so sagt man, dass A die Gruppe G erzeugt. Gruppen, die von einem einzigen Element erzeugt werden, heißen *zyklische* Gruppen. Zum Beispiel wird $(\mathbb{Z}, +)$ von 1 erzeugt, und die freie Gruppe F_M ist von M erzeugt (jedes Element $m \in M$ ist insbesondere ein reduziertes Wort und damit ein Element von F_M).

Zyklische Gruppen

Für $g \in G$ und $n \in \mathbb{Z}$ definiert man g^n durch

$$g^0 := e, \quad g^{n+1} := g \circ g^n \text{ für positives } n \text{ und } g^n := (g^{-1})^{-n} \text{ für negatives } n.$$

Man rechnet dann leicht nach, dass

$$(g^n)^m = g^{nm} \quad \text{und} \quad g^n \circ g^m = g^{n+m}.$$

Es folgt, dass $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ und dass die Abbildung $n \mapsto g^n$ einen surjektiven Gruppenhomomorphismus $g^\frown$ von $(\mathbb{Z}, +)$ auf $\langle g \rangle$ definiert. Ausserdem sind zyklische Gruppen stets kommutativ, da $g^n \circ g^m = g^{n+m} = g^{m+n} = g^m \circ g^n$. Insbesondere gilt $g^m = g^n \iff g^{n-m} = e$.

Die *Ordnung* ord(g) von g ist die Ordnung der von g erzeugten Gruppe $|\langle g \rangle| \in \mathbb{N} \cup \{\infty\}$. Es gibt nun zwei Fälle: Entweder die Ordnung von g ist unendlich. Dann ist $g^\frown$ ein Isomorphimus zwischen $\langle g \rangle$ und $(\mathbb{Z}, +)$. Oder die Ordnung von g ist endlich. Dann gibt es eine kleinste natürliche Zahl $m \neq 0$, so dass $g^m = e$. Es folgt dann $\langle g \rangle = \{g^0, g^1, \ldots, g^{m-1}\}$ und Kern($g^\frown$) $= m\mathbb{Z}$. Der Homomorphismus $g^\frown$ induziert dann einen Isomorphismus zwischen $\langle g \rangle$ und $(\mathbb{Z}_m, +)$, und es gilt $g^d = e \iff m \mid d$. Die Ordnung von g ist also die kleinste positive Zahl m mit $g^m = e$. Insbesondere hat das neutrale Element die Ordnung 1 und ist das einzige Element mit dieser Eigenschaft.

Wir haben also gezeigt:

Satz 9.1 *Eine zyklische Gruppe ist entweder isomorph zu* $(\mathbb{Z}, +)$*, falls sie unendliche Ordnung hat, oder zu* $(\mathbb{Z}_m, +)$*, falls sie Ordnung* m *hat.*

Satz 9.2 *Für* $k \neq 0$ *ist die Ordnung von* g^k *unendlich, falls* ord(g) *unendlich ist, sonst* $\text{ord}(g^k) = \frac{\text{ord}(g)}{\text{ggT}(\text{ord}(g),k)}$.

BEWEIS: Das erste ist klar, denn wäre $e = (g^k)^l = g^{kl}$, so wäre die Ordnung von g ein Teiler von kl also endlich. Ist $\mathrm{ord}(g) = m$ endlich, so gilt $e = (g^k)^d = g^{kd}$ genau dann, wenn $m \mid kd$. Das kleinste $d > 0$ mit dieser Eigenschaft ist aber gerade $\frac{m}{\mathrm{ggT}(m,k)}$. □

Satz 9.3 *Für $m_1, m_2 \in \mathbb{Z} \setminus \{0\}$ gibt es $a_1, a_2 \in \mathbb{Z}$ mit $\mathrm{ggT}(m_1, m_2) = a_1 m_1 + a_2 m_2$.*

BEWEIS: Dies folgt aus dem *Euklidischen Algorithmus* zur Bestimmung des ggT, der wie folgt funktioniert: Ohne Einschränkung kann man $m_1, m_2 > 0$ annehmen. Falls $m_1 = m_2$, so ist $\mathrm{ggT}(m_1, m_2) = m_1 = 1m_1 + 0m_2$. Andernfalls sei z.B. $m_1 > m_2$. Dann ist $\mathrm{ggT}(m_1, m_2) = \mathrm{ggT}(m_1 - m_2, m_2)$. Durch sukzessives Verkleinern der beiden Zahlen kommt man schließlich im ersten Fall an. Per Induktion über $m_1 + m_2$ kann man nun annehmen, dass es Zahlen $a_1', a_2' \in \mathbb{Z}$ gibt mit $\mathrm{ggT}(m_1 - m_2, m_2) = a_1'(m_1 - m_2) + a_2' m_2$. Dann gilt $\mathrm{ggT}(m_1, m_2) = \mathrm{ggT}(m_1 - m_2, m_2) = a_1' m_1 + (a_2' - a_1')m_2$. □

Der Euklidische Algorithmus erlaubt nicht nur das schnelle Bestimmen des größten gemeinsamen Teilers zweier ganzer Zahlen, sondern auch die Berechnung der Zahlen a_1, a_2 aus dem Satz.

Satz 9.4 *Untergruppen zyklischer Gruppen sind wieder zyklisch. Homomorphe Bilder zyklischer Gruppen sind wieder zyklisch.*

BEWEIS: Ist $\varphi : G \to H$ Homomorphismus und g ein Erzeuger von G, so wird $\mathrm{Bild}(\varphi) = \{\varphi(g^n) \mid n \in \mathbb{Z}\} = \{\varphi(g)^n \mid n \in \mathbb{Z}\}$ von $\varphi(g)$ erzeugt.

Sei U eine Untergruppe von $\langle g \rangle$. Entweder $U = \{e\}$ ist trivial (und damit von e erzeugt, also zyklisch), oder es gibt ein Element $g^n \in U$ mit $n \neq 0$. Dann liegt auch $g^{-n} \in U$, und eine der beiden Zahlen $n, -n$ ist positiv. Sei n_0 der minimale positive Exponent einer Potenz von g in U. Dann gilt offensichtlich $\langle g^{n_0} \rangle \subseteq U$. Falls $g^k \in U$, so sei $\mathrm{ggT}(k, n_0) = ak + bn_0$. Dann ist auch $g^{\mathrm{ggT}(k,n_0)} = (g^k)^a \circ (g^{n_0})^b \in U$; wegen der Minimalität von n_0 ist also $\mathrm{ggT}(k, n_0) = n_0$, d.h. n_0 ist ein Teiler von k und damit $g^k \in \langle g^{n_0} \rangle$. □

Satz 9.5 (Folgerung/Zusammenfassung)

$\mathbb{Z}$ hat zwei Erzeuger: 1 und -1. Alle Elemente außer 0 haben unendliche Ordnung. Die Untergruppen von $\mathbb{Z}$ sind die $m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$ für $m \in \mathbb{N}$.

Die Erzeuger von $\mathbb{Z}_m$ sind die zu m teilerfremden Zahlen. Die Ordnung von k ist $\frac{m}{\mathrm{ggT}(k,m)}$. Die Untergruppen von $\mathbb{Z}_m$ sind (bis auf Isomorphie) die $\mathbb{Z}_d$ für Teiler d von m. Für jeden Teiler d gibt es genau eine zu $\mathbb{Z}_d$ isomorphe Untergruppe, nämlich die von $\frac{m}{d}$ erzeugte Untergruppe $\{0, \frac{m}{d}, 2\frac{m}{d}, \ldots, (d-1)\frac{m}{d}\}$.

Nebenklassenzerlegung

Sei $U \leqslant G$. Auf G definiert man zwei Äquivalenzrelationen. Zum einen $g \sim_L h :\iff g^{-1}h \in U$. Dies ist genau dann eine Äquivalenzrelation, wenn U eine Untergruppe ist. Die Äquivalenzklassen $gU := \{gu \mid u \in U\}$ heißen *Linksnebenklassen* von U in G. Die Menge der Linksnebenklassen wird mit G/U bezeichnet. Es gilt $gU = hU \iff h^{-1}g \in U$.

Entsprechend ist $g \sim_R h :\iff hg^{-1} \in U$ eine Äquivalenzrelation mit Klassen $Ug := \{ug \mid u \in U\}$, den *Rechtsnebenklassen* von U in G, deren Menge manchmal mit $U\backslash G$ bezeichnet wird.

$U = eU = Ue$ ist selbst sowohl eine Rechts– als auch eine Linksnebenklasse, nämlich jeweils die Äquivalenzklasse von e.

Satz 9.6

(a) $x \mapsto hg^{-1}x$ *ist eine Bijektion zwischen* gU *und* hU.

(b) $x \mapsto xg^{-1}h$ *ist eine Bijektion zwischen* Ug *und* Uh.

(c) $gU \mapsto Ug^{-1}$ *ist eine Bijektion zwischen* G/U *und* $U\backslash G$.

Insbesondere gibt es also ebensoviele Rechts– wie Linksnebenklassen. Deren Anzahl ist der *Index* $|G : U|$ von U in G. Falls G endlich ist, so wird G also von $|G : U|$ vielen Nebenklassen von U überdeckt, die alle zu U gleichmächtig sind. Es gilt also der

Satz 9.7 (Lagrange) *Wenn* G *endlich ist und* $U \leqslant G$*, so* $|U|\big||G|$ *und* $|G| = |U| \cdot |G : U|$*. Insbesondere teilt die Ordnung eines Elements stets die Gruppenordnung.*

Als beispielhafte Anwendung des Satzes von Lagrange ergibt sich der sogenannte „kleine Satz von Fermat“, Satz 10.6. In der symmetrischen Gruppe S_n ist die Ordnung eines Elementes das kleinste gemeinsame Vielfache der Zykellängen in der Zykelzerlegung. Für $n = 5$ gibt es Elemente der Ordnung $k = 1, \ldots, 5$ (die k-Zykel und für $k = 2$ die Doppeltranspositionen) sowie $k = 6$ (eine Transposition und ein 3-Zykel). Das kleinste gemeinsame Vielfache der Ordnungen aller Elemente ist der *Exponent* der Gruppe, das ist die kleinste Zahl k mit $g^k = e$ für alle Gruppenelemente g. Der Exponent der S_5 ist also 60, die Ordnung 120.

Satz 9.8 *Falls* $|G| = p$ *eine Primzahl ist, so ist* G *zyklisch, also* $\cong \mathbb{Z}_p$*. Diese Gruppen sind die einzigen Gruppen ohne andere Untergruppen als die triviale und sich selbst.*

Beweis: Falls $g \in G$, so ist die Ordnung von g ein Teiler von p, also für $g \neq e$ gleich p. Also ist g ein Erzeuger der Gruppe. Falls G eine Gruppe ist ohne Untergruppen anders als $\{e\}$ und G, so muss für jedes $g \in G, g \neq e$ schon $\langle g \rangle = G$ gelten. Nach Satz 9.5 haben aber alle anderen zyklischen Gruppen nicht-triviale echte Untergruppen □

Gruppen von Primzahlordnung sind also bis auf Isomorphie durch ihre Ordnung festgelegt. Zum Beispiel ist $S_2 \cong \mathbb{Z}_2$. Für andere Ordnungen gilt dies nicht. Zum Beispiel gibt es zwei Gruppen der Ordnung vier: $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Faktorgruppen

Man möchte nun gerne G/U so zu einer Gruppe machen, dass die natürliche Surjektion $G \to G/U$, $g \mapsto gU$ ein Gruppenhomomorphismus wird. Damit dies geht, muss $gU \cdot hU = ghU$ gelten (genauer: $\sim_L$ muss eine Kongruenzrelation sein). Insbesondere: Für $g \in G$ und $u, u' \in U$ ist dann $ugu' \in eU \cdot gU = gU$, also $ug \in gU \cdot u^{-1} = gU$ und somit $Ug \subseteq gU$. Ebenso die umgekehrte Inklusion, also $Ug = gU$.

Definition 9.3 *Eine Untergruppe* $U \leqslant G$ *heißt* Normalteiler *oder* normale Untergruppe*, in Zeichen* $U \trianglelefteq G$*, falls* $gU = Ug$ *für alle* $g \in G$ *ist.*

Bemerkung: Äquivalent bedeutet dies, dass die beiden Relationen $\sim_L$ und $\sim_R$ übereinstimmen, oder dass jede Linksnebenklasse auch eine Rechtsnebenklasse ist. Denn da stets $g \in gU \cap Ug$, kann, wenn gU auch eine Rechtsnebenklasse ist, dies nur Ug sein.

Beispiele:

- Die trivialen Untergruppen und das Zentrum sind Normalteiler.
- Jede Untergruppe in einer kommutativen Gruppe ist Normalteiler.
- Eine Untergruppe vom Index 2 ist eine Normalteiler (denn einerseits ist $eU = U = Ue$, also ist für $g \notin U$ die andere Nebenklasse $gU = G \setminus U = Ug$).
  Beispiele sind die alternierende Gruppe A_n in der symmetrischen Gruppe S_n oder die zu $\mathbb{Z}_n$ isomorphe Drehgruppe des regelmäßigen n-Ecks in ihrer Symmetriegruppe D_n.

Satz 9.9

(a) *Sei* $U \trianglelefteq G$*, dann definiert* $gU \cdot hU = ghU$ *eine Gruppenstruktur auf* G/U *mit neutralem Element* eU *und inversen Elementen* $(gU)^{-1} = g^{-1}U$ *und so, dass* $g \mapsto gU$ *ein surjektiver Gruppenhomomorphismus ist (die* Faktorgruppe *oder* Quotientengruppe *„*G *nach* U*“).*

(b) Homomorphiesatz: *Sei* $\varphi : G \to H$ *Gruppenhomomorphismus. Dann ist der Kern von* φ *ein Normalteiler und es gilt* $G/\mathrm{Kern}(\varphi) \cong \mathrm{Bild}(\varphi)$.

Beispiele:

- $\_ \bmod m : \mathbb{Z} \to \mathbb{Z}_m, x \mapsto$ „der Rest von x bei der Division durch m“ ist ein surjektiver Homomorphismus mit Kern $m\mathbb{Z}$, es gilt also $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Für ein Element $a + m\mathbb{Z}$ von $\mathbb{Z}/m\mathbb{Z}$ schreibt man gerne einfach $\overline{a}$, wenn die Zahl m aus dem Zusammenhang ersichtlich ist.
  Außerdem an schreibt man $a \equiv b \pmod m$ — gesprochen „a und b sind kongruent modulo m“ — für die von diesem Homomorphismus induzierte Kongruenzrelation auf $\mathbb{Z}$, also für $m \mid a - b$.
- Das Signum $\mathrm{sgn} : \mathrm{Sym}(n) \to \mathbb{Z}_2$, $\sigma \mapsto$ „Parität der Anzahl von Transpositionen, die σ ergeben“ ist ein surjektiver Homomorphismus. Der Kern ist die sogenannte *alternierende Gruppe* A_n; also $\mathrm{Sym}(n)/A_n = \mathbb{Z}_2$.
- Es gibt einen surjektiven Homomorphismus $D_n \to S_2$, der eine Symmetrie des regelmäßigen n-Ecks auf die dadurch bewirkte Vertauschung von Vorder– und Rückseite abbildet. kern ist die Drehgruppe.
- Die Determinante det ist eine surjektiver Gruppenhomomorphismus von der Matrizengruppe $\mathrm{GL}(n, K)$ auf die multiplikative Gruppe des Körpers K. Der Kern besteht aus der *speziellen linearen Gruppe* $\mathrm{SL}(n, K)$ der Matrizen mit Determinante 1.
- Für bespielsweise $\mathbb{R}$-Vektorräume gilt $\mathbb{R}^{n+1}/\mathbb{R} = \mathbb{R}^n$; der Homomorphismus entspricht der Projektion entlang einer Achse.

Satz 9.10 (Cayley) *Jede (endliche) Gruppe ist isomorph zu einer Untergruppe einer (endlichen) symmetrischen Gruppe.*

BEWEIS: Man definiert eine Abbildung $\lambda : G \to \mathfrak{Sym}(G)$ durch $g \mapsto (x \mapsto g \circ x)$. Wegen der Assoziativität der Gruppenoperation ist es ein Homomorphismus. Der Kern besteht nur aus e, weil für jedes Element $g \neq e$ schon $e \circ g \neq e$ gilt. Also ist es ein injektiver Homomorphismus. □

Eine Gruppe heißt *einfach*, falls sie keine nicht-trivialen echten Normalteiler hat. Jede endliche Gruppe ist aus endlich vielen einfachen Gruppen zusammengebaut, d.h. es gibt $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$ mit G_{i+1}/G_i einfach. Man kennt alle einfachen endlichen Gruppen: Es gibt mehrere unendliche Familien, wie die (einzigen kommutativen einfachen Gruppen) $\mathbb{Z}_p$ für Primzahlen p oder die alternierenden Gruppen A_n für $n \geqslant 5$ (und einige weitere Familien), sowie 26 sogenannte sporadische Gruppen. Allerdings kann es immer noch mehrere Möglichkeiten geben, wie diese einfachen Gruppen zusammengesetzt werden. Für $\mathbb{Z}_4$ wie für $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist $n = 2$ und beide einfachen Quotienten sind $\mathbb{Z}_2$.

Die Einfachheit der A_5 hängt übrigens damit zusammen, dass es für Gleichungen 5-ten Grades keine allgemeine Lösungsformel durch Wurzelausdrücke gibt. Für Gleichungen bis vierten Grades gibt es solche Lösungsformeln; die dabei auftretenden Wurzeln hängen mit der Reihe der G_i wie oben zusammen. Zum Beispiel gibt es eine Reihe $\{e\} \trianglelefteq Z_2 \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$ mit jeweils kommutativen einfachen Faktoren. V ist die sogenannte *Kleinsche Vierergruppe* $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Man sieht sie am Würfel: Die Drehgruppe des Würfels ist isomorph zur S_4; jede Drehung permutiert die drei Mittelsenkrechten der Seitenflächen, sie ist ein Homomorphismus $S_4 \to S_3$, dessen Kern gerade V ist.

III.10 Ringe und Körper

Ringe

Definition 10.1 *Ein* Ring *besteht aus einer nicht-leeren Menge R mit zwei zweistelligen Operationen $+, \cdot : R^2 \to R$ mit folgenden Eigenschaften:*

- *R ist mit $+$ eine kommutative Gruppe, insbesondere existiert ein neutrales Element 0 und zu jedem $r \in R$ ein additives Inverses $-r$;*
- *die Multiplikation $\cdot$ ist assoziativ;*
- *es gelten die Distributivgesetze $(r_1 + r_2) \cdot r = (r_1 \cdot r) + (r_2 \cdot r)$ und $r \cdot (r_1 + r_2) = (r \cdot r_1) + (r \cdot r_2)$ für alle $r, r_1, r_2 \in R$.*

Der Ring heißt kommutativ*, falls zusätzlich die Multiplikation kommutativ ist, und* unitär *oder* Ring mit Eins*, falls es zusätzlich ein neutrales Element 1 der Multiplikation gibt. (Es muss nicht unbedingt $0 \neq 1$ gelten.)*

Man sieht leicht, dass in einem Ring $0 \cdot r = r \cdot 0 = 0$ für alle $r \in R$ gilt.

Oft steht „Ring“ auch für „kommutativer Ring mit Eins“.

Beispiele:

- Der triviale Ring $\{0\}$. Dies ist der einzige Ring mit $0 = 1$, denn daraus folgt $r = r \cdot 1 = r \cdot 0 = 0$.
- $\mathbb{Z}$ und alle Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

- Die endlichen Gruppen $\mathbb{Z}_m$ werden durch Multiplikation modulo m zu Ringen.
- Die (n, n)-Matrizen über einem Körper bilden (für $n \geqslant 2$) einen nicht-kommutativen Ring mit Eins. Für einen endlichen Körper sind diese Matrizenringe Beispiele für endliche nicht-kommutative Ringe.
- Die Polynome $R[X]$ mit Koeffizienten in einem kommutativen Ring R bilden einen kommutativen Ring mit Eins.

Ein Unterring eines Ringes R ist eine Teilmenge von R, die mit den eingeschränkten Operationen selbst wieder ein Ring ist. (Man muss sich darauf verständigen, ob ein Unterring eines Rings mit Eins die Eins auch enthalten muss oder nicht; im ersten Fall sollte man der Deutlichkeit halber von einem unitären Unterring sprechen).

Ein *Ringhomomorphismen* ist eine Abbildung $\varphi : R \to S$ zwischen Ringen, die ein additiver Gruppenhomomorphismus ist und mit der Multiplikation verträglich ist (und gegebenenfalls die Eins auf die Eins abbildet; dann handelt es sich um einen *unitären Ringhomomorphismus*). Es muss also $\varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')$ und gegebenenfalls $\varphi(1) = 1$ erfüllt sein. Das Bild von φ ist dann ein (unitärer) Unterring. Der Kern von φ erfüllt alle Eigenschaften eines Unterrings, außer dass er i.a. die Eins nicht enthält. Wie im Fall von Gruppen besitzen Kerne von Homomorphismen weitere Eigenschaften, und es gilt ein Homomorphiesatz:

Definition 10.2 *Ein* Ideal *in einem Ring* R *ist eine Untergruppe* I *der additiven Gruppe* $(R, 0, +)$ *mit der Eigenschaft* $r \cdot i \subseteq I$ *und* $i \cdot r \subseteq I$ *für alle* $r \in R$ *und* $i \in I$.

Da ein Ideal eine Untergruppe der additiven Gruppe des Ringes ist, notiert man Nebenklassen additiv, also $r + I$ statt rI. Die Notation rI wird in Analogie dazu für die Menge $\{ri \mid i \in I\}$ benutzt. Man kann die Eigenschaft in der Definition der Ideale also auch als $rI \subseteq I$ und $Ir \subseteq I$ schreiben.

Satz 10.1

(a) *Ist* R *ein (kommuativer/unitärer) Ring und* I *ein Ideal von* R*, so wird* R/I *durch* $(r+I)\cdot(r'+I) := rr' + I$ *zu einem (kommutativen/unitären) Ring (dem* Faktor– *oder* Quotientenring *und die natürliche Abbildung* $R \to R/I$*,* $r \mapsto rI$ *zu einem Ringhomomorphismus.*

(b) *Kerne von Ringhomomorphismes* $\varphi : R \to S$ *sind Ideale und es gilt* $R/\mathrm{Kern}(\varphi) \cong \mathrm{Bild}(\varphi)$.

Beispiele:

- $\{0\}$ und R selbst sind Ideale von R; letzteres ist das einzige Ideal, das 1 enthält.
- $m\mathbb{Z}$ ist ein Ideal in $\mathbb{Z}$, also ist $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$ auch als Ring.
- Für ein Element r eines kommutativen Ringes R ist $(x - r) \cdot R[X] := \{f \in R[X] \mid f(r) = 0\}$ ein Ideal in $R[X]$ mit $R[X]/(x - r) \cdot R[X] \cong R$.
- Allgemeiner ist für $r \in R$, R kommutativ, die Menge rR ein Ideal in R, das von r erzeugte *Hauptideal*. Ein Ring, in dem jedes Ideal Hauptideal ist, heißt *Hauptidealring*. Beispiele für Hauptidealringe sind $\mathbb{Z}$, $\mathbb{K}[X]$ für Körper K. Dagegen sind $\mathbb{Z}[X]$ und $K[X, Y]$ keine Hauptidealringe.

- $\mathbb{R}[X]/(X^2+1)\cdot\mathbb{R}[X]$ ist sogar ein Körper, nämlich der Körper $\mathbb{C}$ der komplexen Zahlen.

Einheiten und Körper

Sind $a, b \in R$, so heißt a ein *Teiler* von b, in Zeichen $a \mid b$, falls es ein $c \in R$ gibt mit $ac = b$. Dies ist äquivalent zu $b \in aR$ bzw. $bR \subseteq aR$. Ein Element $r \in R$ heißt eine *Einheit*, falls r ein Inverses r^{-1} besitzt, d.h. $r \cdot r^{-1} = r^{-1} \cdot r = 1$. Einheiten sind also genau die Teiler der 1. Die Menge der Einheiten von R wird mit R^* bezeichnet; $(R^*, 1, \cdot)$ ist dann eine Gruppe (die *Einheitengruppe*, die größte in R enthaltene Gruppe bzgl. der Multiplikation.

Definition 10.3 *Ein* Körper *ist ein kommutativer Ring R, für den $R = R^* \cup \{0\}$ gilt. Insbesondere gilt in einem Körper stets $0 \neq 1$.*

Jedes Element $\neq 0$ in einem Körper K hat also ein Inverses, d.h. $(K \setminus \{0\}, 1, \cdot)$ ist eine Gruppe, die sogenannte *multiplikative Gruppe* $K^\times$ des Körpers, im Gegensatz zur *additiven Gruppe* $K^+ = (K, 0, +)$.

Beispiele:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper.
- $\mathbb{Z}_2$ ist ein Körper mit zwei Elementen, der kleinstmögliche Körper.
- Ist K ein Körper, so bilden die *rationalen Funkionen* über K (also die Quotienten von Polynomen aus $K[X]$) einen Körper $K(X)$. Ebenso kann man aus dem Ring $K[[X]]$ der formalen Potenzreihen durch Quotientenbildung einen Körper $K((X))$ machen. Beides geht analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$.

Ein Körper K hat keine Ideale I außer $\{0\}$ und K, denn mit $1 \neq r \in I$ ist auch $(kr^{-1}) \cdot r = k \in I$ für jedes $k \in K$. Also ist ein Ringhomomorphismus zwischen zwei Körpern immer injektiv; ein Homomorphisatz für Körper daher wenig aussagekräftig.

Die endlichen Ringe $\mathbb{Z}/m\mathbb{Z}$

Satz 10.2 *$\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis: Wegem dem Distributivgesetz ist die Multiplikation mit $a \in \mathbb{Z}_n$, also die Abbildung $\mathbb{Z}_n \to \mathbb{Z}_n, x \mapsto ax$ ein Homomorphismus. Wenn es ein Inverses zu a gibt, ist die Abbildung bijektiv, weil dann die Multiplikation mit a^{-1} eine Umkehrabbildung ist. Umgekehrt folgt aus der Surjektivität der Abbildung, dass es ein x mit $ax = 1$ gibt.

Falls n keine Primzahl ist und a ein nicht-trivialer Teiler von n, so ist $a \cdot 0 = 0$ und $a \cdot \frac{n}{a} = 0$ (daher heißt a auch ein *Nullteiler*), also ist die Multiplikation mit a nicht injektiv und a hat keine Inverses.

Ist n Primzahl und $a \neq 0$, so liegt $a = a \cdot 1$ im Bild der Multiplikation mit a. Da $\mathbb{Z}_n$ eine einfache Gruppe ist, muss das Bild schon die ganze Gruppe sein und die Multiplikation surjektiv, also auch bijektiv als Abbildung zwischen gleichmächtigen endlichen Mengen. □

Satz 10.3 *Ein endlicher Körper* K *hat die Mächtigkeit* p^n *für eine Primzahl* p *und ein* $n \geqslant 1$. *Es ist* $K^+ \cong \mathbb{Z}_p^n = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ mal}}$. *Dabei ist* p *die* Charakteristik *des Körpers, d.h. die kleinste Zahl, für die* $\underbrace{1 + \cdots + 1}_{p \text{ mal}} = 0$ *gilt.*

Beweis: Betrachte die Menge $\{0, 1, 1+1, 1+1+1, \ldots\}$. Wegen der Endlichkeit von K sind zwei dieser Ausdrücke gleich; deren Differenz ergibt einen Ausdruck $m \cdot 1 := 1 + \cdots + 1 = 0$. Gilt $m = kl$, so folgt aus der Distributivität $0 = (k \cdot 1)(l \cdot 1)$, also ist das kleinste solche m eine Primzahl p. Da die Multiplikation wegen des Distributivgesetzes auf $\{0, 1, 1+1, \ldots, (p-1) \cdot 1\}$ festgelegt ist, haben wir $\mathbb{Z}_p$ als Unterkörper von K. Nun ist K offensichtlich ein Vektorraum über $\mathbb{Z}_p$ der Dimension n, also gilt $K^+ \cong \mathbb{Z}_p^n$ und somit $|K| = p^n$. □

Die multiplikative Gruppe eines Körpers ist übrigens stets zyklisch, d.h. es gilt $K^\times \cong \mathbb{Z}_{p^n-1}$.

Satz 10.4 (ohne Beweis) *Für jede Primzahl* p *und jedes* $n \geqslant 1$ *gibt es einen bis auf Isomorphie eindeutig bestimmten Körper der Mächtigkeit* p^n, *der mit* $\mathbb{F}_{p^n}$ *bezeichnet wird.*

(Hinweis zum Beweis: Über den reellen Zahlen gibt es irreduzible Polynome ohne Nullstellen, etwa $X^2 + 1$. Nun kann man $\mathbb{R}$ erweitern zu dem Körper der komplexen Zahlen $\mathbb{C} \cong \mathbb{R}[i] \cong \mathbb{R}[X]/(X^2+1) \cdot \mathbb{R}[X]$. Dies Verfahren konstruiert allgemein für ein irreduzibles Polynomen $P \in K[X]$ einen kleinsten, eindeutig bestimmten Erweiterungkörper $K[X]/P \cdot K[X]$ des Körpers K, in dem P eine Nullstelle hat. $\mathbb{F}_{p^n}$ entsteht auf diese Weise aus $\mathbb{Z}_p$ durch ein irreduzibles Polynom vom Grad n.)

Für eine Primzahl p ist also der endliche Körper $\mathbb{F}_p$ mit p Elementen gerade der Ring $\mathbb{Z}/m\mathbb{Z}$.

$\mathbb{Z}$ ist ein nullteilerfreier Ring, der kein Körper ist, kann aber zu einem Körper $\mathbb{Q}$ erweitert werden. Auf die gleiche Weise kann jeder nullteilerfreie, kommutative, nicht-triviale Ring R in einen Körper eingebettet werden. Der kleinste solche Körper heißt der *Quotientenkörper* von R. Dieser besteht aus Äquivalenzklassen von formalen Brüchen $\frac{r}{s}$ mit $r, s \in R, s \neq 0$ bezüglich der Äquivalenzrelation $\frac{r}{s} \sim \frac{r'}{s'} :\iff rs' = r's$. Es gelten nun die selben Rechenregeln, wie man sie vom Bruchrechnen in $\mathbb{Q}$ her kennt. Jedes Element $r \neq 0$ hat nun ein Inverses: (die Äquivalenzklase von) $\frac{1}{r}$.

Wir wollen nun versuchen, die multiplikative Struktur der Ringe $\mathbb{Z}_m$, d.h. die Einheitengruppe, besser zu verstehen. Zur Erinnerung: Rechnen in $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$ ist das Gleiche wie Rechnen in $\mathbb{Z}$ und anschließend den Rest modulo m nehmen.

Die *Eulersche* φ*-Funktion* gibt für jede positive natürliche Zahl m die Anzahl der zu ihr teilerfremden positiven natürlichen Zahlen $\leqslant m$ an. Dies ist also auch die Anzahl der Erzeuger der Gruppe $(\mathbb{Z}_m, +)$. Da jedes Element a in $\mathbb{Z}_m$ Erzeugendes der einzigen Untergruppe der Ordnung $\operatorname{ord}(a)$ ist, gilt $m = \sum_{d|m} \varphi(d)$.

Satz 10.5 $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \operatorname{ggT}(a, m) = 1\}$. *Insbesondere ist* $\varphi(m)$ *die Ordnung von* $\mathbb{Z}_m^*$.

BEWEIS: Sei $\mathrm{ggT}(a, m) = 1$. Dann gibt es $s, t \in \mathbb{Z}$ mit $as + mt = 1$. Also ist das Bild von s in $\mathbb{Z}/m\mathbb{Z}$ ein Inverses des Bildes von a.

Die Umkehrung geht wie im Beweis von Satz 10.2: Für nicht zu m teilerfremdes a ist die Multiplikation mit dem Bild von a in $\mathbb{Z}/,\mathbb{Z}$ keine Injektion. □

Es ist kein Zufall, dass die zu m teilerfremden Zahlen sowohl die Erzeuger in $\mathbb{Z}_m$ als auch die invertierbaren Elemente sind. Denn wegen des Distributivgesetzes ist die Multiplikation mit einem Element ein additiver Gruppenhomomoprhismus; die Multiplikation mit einem invertierbaren Element a sogar ein Isomorphismus, der den Erzeuger 1 auf einen Erzeuger abbilden muss, hier also $a \cdot 1 = a$. Umgekehrt ist jeder Gruppenhomorphismus der additiven Gruppe in sich selbst durch das Bild a von 1 bestimmt, und wegen $k = 1 + \cdots + 1 \mapsto a + \cdots + a = a \cdot k$ gerade die Multiplikation mit a. Ist es ein Automorphismus, also umkehrbar, so muss a invertierbar sein.

Satz 10.6 (Satz von Euler bzw. kleiner Satz von Fermat)

(a) $a^{\varphi(m)} \equiv 1 \pmod{m}$ *für alle* a *mit* $\mathrm{ggT}(a, m) = 1$.

(b) $a^{p-1} \equiv 1 \pmod{p}$ *für Primzahlen* p *und alle* a *mit* $p \nmid a$.

BEWEIS: Dies ist der Satz von Lagrange für die Gruppen $\mathbb{Z}_m^*$ mit $m = p$ im Fall (b), wo offensichtlich $\varphi(p) = p - 1$ gilt. □

Erste Anwendung: Primzahltest I

Wie testet man, ob eine gegebene Zahl n eine Primzahl ist? Aus der Definition ergibt sich die Möglichkeit, für alle $1 < d \leqslant \lfloor\sqrt{n}\rfloor$ zu überprüfen, ob $d \mid n$. Dies dauert aber bei großen n zu lange für einen praktikablen Test.

Ein schneller Test ergibt sich aus dem kleinen Satz von Fermat: Für ausgewählte Zahlen $a \leqslant n$ überprüft man, ob $a^{n-1} \equiv 1 \pmod{n}$. Dieser Test ist negativ effektiv, d.h. bei negativer Antwort weiß man, dass n keine Primzahl ist. Bei positiver Antwort kann man nicht schließen, dass n eine Primzahl ist, sondern es nur mit einer gewissen Wahrscheinlichkeit vermuten. Selbst beim Testen mit allen Zahlen $a \leqslant n$ (was wiederum zu viele für eine vernünftige Laufzeit wären) ist der Test nicht effektiv, da es die sogenannten Carmichael–Zahlen gibt, die keine Primzahlen sind, aber den kleinen Satz von Fermat für alle a erfüllen. Es gibt unendlich viele Carmichael–Zahlen; die kleinste davon ist 561.

Zweite Anwendung: RSA–Kryptographie

Man möchte ein Verfahren zur Verfügung stellen, das es jedem erlaubt, Nachrichten so verschlüsselt an einen Empfänger zu schicken, dass nur dieser sie entschlüsseln kann. Dazu wählt der Empfänger zwei große (unbekannte) Primzahlen $p \neq q$, bildet $n = pq$ und sucht sich ein „zufälliges“ zu $\varphi(n) = (p-1)(q-1) = n - p - q + 1$ teilerfremdes e (also z.B. nicht $e = \varphi(n) - 1$). Die Zahlen n und e gibt E als öffentlicher Schlüssel bekannt; p, q und damit auch $\varphi(n)$ bleiben geheim. Nachrichten sind Wörter über dem Alphabet $\mathbb{Z}_n$ (zum Beispiel kann man Zeichen zunächst durch ihren ASCII–Code wiedergeben und mehrere dieser Codes hintereinandergeschrieben als eine Zahl in $\mathbb{Z}_n$ auffassen).

Eine Nachricht $A = (a_1, \ldots, a_k) \in (\mathbb{Z}_n)^k$ wird als $A^e := (a_1^e, \ldots, a_k^e)$ verschlüsselt verschickt, wobei a^e in $\mathbb{Z}_n$ berechnet wird. Der Empfänger sucht nun in $\mathbb{Z}^*_{\varphi(n)}$ ein Inverses d zu e. Dies existiert wegen der Teilerfremdheit von e mit $\varphi(n)$ und kann mit dem Euklidischen Algorithmus schnell berechnet werden, wenn man $\varphi(n)$ kennt. Zur Entschlüsselung berechnet der Empfänger $(A^e)^d$, was gerade wieder A ergibt:

Für zu n teilerfremdes a gilt $(a^e)^d = a^{ed} \equiv a \pmod{n}$ wegen Satz 10.6, da $ed \equiv 1 \pmod{\varphi(n)}$. Aufgrund der besonderen Gestalt von n (kein Primfaktor taucht doppelt auf), gilt dies auch für andere Elemente von $\mathbb{Z}_n$: Für 0 gilt es trivialerweise, und alle anderen nicht-invertierbaren Elemente a in $\mathbb{Z}_n$ sind von der Form kp mit zu q teilerfremdem k (oder p und q vertauscht). Dann gilt einerseits $p \mid a^{ed} - a$, da p beide Summanden teilt. Andererseits gilt, da $\varphi(q) = q-1$ ein Teiler von $\varphi(n) = (p-1)(q-1)$ ist, auch $ed \equiv 1 \pmod{\varphi(q)}$ und also wieder mit Satz 10.6 $a^{ed} \equiv a \pmod{q}$, d.h. $q \mid a^{ed} - a$. Da p und q teilerfremd sind, folgt insgesamt $n \mid a^{ed} - a$.

Eine andere Person als der Empfänger müsste zur Entschlüsselung erst $\varphi(n)$ berechnen, dazu also n in Primfaktoren zerlegen, wofür es nach derzeitigem Wissensstand keinen schnellen Algorithmus gibt. Es gibt aber viele Feinheiten bei der technischen Umsetzung zu beachten: Falls z.B. e zu klein oder zu groß ist, so gibt es Möglichkeiten, das Verfahren zu attackieren. Man darf auch nicht einzelne Zeichen oder zu kleine Blöcke von Zeichen kodieren, da sonst die Verschlüsselung durch eine Häufigkeitsanalyse entziffert werden kann. Auch könnten bei besonderen Zahlen durch die Zufälligkeiten der Zahlkodierung etwa im Binärsystem Muster entstehen, welche die Entschlüsselung erlauben. Schließlich enthält jede mit dem Verfahren veschlüsselte Nachricht Informationen über $\varphi(n)$, so dass man nach einiger Zeit e und n wechseln muss.

Der chinesische Restsatz

Für zwei Gruppen bzw. Ringe R, S definiert man das *direkte Produkt* $R \times S = \{(r, s) \mid r \in R, s \in S\}$ mit komponentenweisen Verknüpfungen, also beispielsweise $(r, s) + (r', s') := (r + r', s + s')$. Dies ist dann wieder ein Gruppe bzw. ein Ring.

Satz 10.7 (Chinesischer Restsatz)
Seien $m_1, \ldots, m_k$ paarweise teilerfremde Zahlen. Dann ist

$$\begin{aligned} \mathbb{Z}/(m_1 \cdot \ldots \cdot m_k)\mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \\ a + (m_1 \cdot \ldots \cdot m_k)\mathbb{Z} &\mapsto (a + m_1\mathbb{Z}, \ldots, a + m_k\mathbb{Z}) \end{aligned}$$

ein Ringisomorphismus.

Beweis: Es gibt stets den Ringhomomorphismus $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, der einen Rest modulo mn weiter modulo m reduziert. Mehrere Homomorphismen kann man immer in einen Homomorphismus in das direkte Produkt zusammenfassen (da alles komponentenweise erklärt ist). Die Ringe aus beiden Seiten haben gleich viele Elemente, es reicht also zu zeigen, dass der Homomorphismus injektiv ist. Eine Zahl, die durch jede der paarweise teilerfremden Zahlen m_i teilbar ist, ist aber durch ihr Produkt teilbar. □

Als Folgerung erhält man zum einen, dass $\mathbb{Z}_m \times \mathbb{Z}_n$ wieder zyklisch ist, wenn m und n teilerfremd sind (und die Umkehrung gilt auch).

Außerdem erhält man aus der Surjektivität des Homomorphismus folgende Eigenschaften: Gegeben $r_1, \ldots, r_k \in \mathbb{Z}$, so gibt es eine Zahl $b \in \mathbb{Z}$ mit $b \equiv r_i \pmod{m_i}$ für alle $i = 1 \ldots, k$.

Eine solche Zahl kann man auch leicht berechnen: Für $k = 2$ sucht man $a_1, a_2 \in \mathbb{Z}$ mit $a_1 m_1 + a_2 m_2 = 1$ und setzt $b_2 := r_2 a_1 m_1 + r_1 a_2 m_2$. Es gilt dann $b \equiv r_i \pmod{m_i}$ für $i = 1, 2$. Induktiv berechnet man dann auf die gleiche Weise b_{j+1} mit $b_{j+1} \equiv b_j \pmod{m_1 \cdot \ldots \cdot m_j}$ und $b_{j+1} \equiv r_{j+1} \pmod{m_{j+1}}$. Dann ist b_k eine der gewünschten Zahlen; alle anderen unterscheiden sich durch Vielfache von $m_1 \cdot \ldots \cdot m_j$.

Nun soll noch die genauere Struktur der Einheitengruppen $\mathbb{Z}_m$ angegeben werden. Teil (a) des folgenden Satzes folgt direkt aus dem Chinesischen Restsatz. Zum Beweis von (b) und (c) braucht man aber tiefergehende Gruppentheorie, als sie hier entwickelt werden konnte.

Satz 10.8 (ohne Beweis)

(a) *Ist* $m = \prod_{i=1}^{l} p_i^{k_i}$ *die Primfaktorzerlegung von* m*, so gilt* $\mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \cdots \times \mathbb{Z}_{p_l^{k_l}}^*$.

(b) *Ist* $p > 2$ *Primzahl so ist* $\mathbb{Z}_{p^k}^*$ *zyklisch der Ordnung* $\varphi(p^k) = (p-1) \cdot p^{k-1}$.

(c) $\mathbb{Z}_2^* = \{0\}$ *und für* $k \geqslant 2$ *gilt* $\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$. *Diese Gruppe hat die Ordnung* 2^{k-1} *und ist für* $k \geqslant 3$ *nicht zyklisch.*

Insbesondere ist $\varphi(m) = \prod_{i=1}^{l} \varphi(p_i^{k_i}) = \prod_{i=1}^{l} \left((p_i - 1) \cdot p_i^{k_i - 1}\right)$.

Quadrate

Die Abbildung $\_^2 : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $x \mapsto x^2$ ist ein Gruppenhomomorphismus. Für eine Primzahl $p > 2$ gilt $\mathrm{Kern}(\_^2) = \{1, -1\} = \{1, p-1\}$; der Kern ist also nicht trivial. Damit folgt $\left|\mathrm{Bild}(\_^2)\right| = \frac{p-1}{2}$, d.h. genau die Hälfte der Zahlen in $\mathbb{Z}_p^*$ sind Quadrate.

Man definiert für $a \in \mathbb{Z}$ das *Legendre–Symbol* (wobei ich „$(a \bmod p)$“ für den Rest von a modulo p schreibe):

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } (a \bmod p) \text{ Quadrat in } \mathbb{Z}_p^* \\ 0 & \text{falls } p \text{ ein Teiler von } a \text{ ist} \\ -1 & \text{falls } (a \bmod p) \text{ in } \mathbb{Z}_p^* \text{ liegt, aber kein Quadrat ist} \end{cases}$$

Satz 10.9 (Euler) $p > 2$ *Primzahl. Dann* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Bemerkung: Wegen $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \pmod{p}$ folgt $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, da $\mathbb{Z}_p$ ein Körper ist und damit die Gleichung $X^2 = 1$ höchstens zwei Lösungen hat.

Beweis: Sei g ein Erzeuger von $\mathbb{Z}_p^*$. Dann gilt $g^{\frac{p-1}{2}} = -1$, da $\mathrm{ord}(g) = p - 1$. Nun gibt es ein j mit $a = g^j$. Offensichtlich ist a Quadrat, falls j gerade ist. Da genau die Hälfte aller Zahlen in $\mathbb{Z}_p^* = \{g^0, g^1, \ldots, g^{p-2}\}$ Quadrate sind, bleiben für die Nicht–Quadrate genau die g^j mit ungeradem j übrig. Andererseits ist $a^{\frac{p-1}{2}} = (g^j)^{\frac{p-1}{2}} = (g^{\frac{p-1}{2}})^j = (-1)^j$, also genau dann gleich 1 wenn j gerade ist. □

Das Legendre–Symbol induziert einen Gruppenhomomorphismus $\left(\frac{-}{p}\right) : \mathbb{Z}_p^* \to \{\pm 1\}$, dessen Kern gerade die Quadrate sind. (Dass das Produkt zweier Nicht–Quadrate wieder ein Quadrat ist, liegt daran, dass die Untergruppe der Quadrate Index 2 hat. Die Nebenklasse eines Nicht–Quadrats (d.h. alle Produkte aus diesem Nicht-Quadrat und Quadraten) besteht also aus allen Nicht–Quadraten; das Produkt von zwei Nicht–Quadraten muss daher in der anderen Nebenklasse, d.h. in den Quadraten liegen.)

Außerdem liefert das Legendre–Symbol einen Monoidhomomorphismus $\left(\frac{-}{p}\right) : (\mathbb{Z}, \cdot) \to (\mathbb{Z}_3, \cdot)$. Das Legendre–Symbol ist also multiplikativ in seinem „Zähler“ und außerdem hängt $\left(\frac{a}{p}\right)$ nur von der Restklasse $a \bmod p$ ab. Ferner gelten folgende Eigenschaften:

Satz 10.10 (ohne Beweis) *Seien p, q zwei verschiedene ungerade Primzahlen.*

(a) Quadratisches Reziprozitätsgesetz von Gauss: $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

(b) Ergänzungsgesetze: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ *und* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Für eine ungerade Zahl n mit Primfaktorzerlegung $n = \prod_{i=1}^{l} p_i^{k_i}$ weitet man nun die Definition des Legendre–Symbols aus durch

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{l} \left(\frac{a}{p_i}\right)^{k_i}$$

d.h. man macht es auch in seinem „Nenner“ multiplikativ. Man kann nun nachrechnen, dass die Eigenschaften von Satz 10.10 auch für beliebige ungerade Zahlen $p \neq q$ gelten. Daraus ergibt sich die Möglichkeit, das erweiterte Legendre–Symbol $\left(\frac{a}{b}\right)$ schnell zu berechnen, auch ohne die Primfaktorzerlegung zu kennen. Zunächst reduziert man $a \bmod b$, zieht dann die höchste Zweier–Potenz heraus, die man mit dem Ergänzungsgesetz berechnet, wendet das quadratische Reziprozitätsgesetz an und beginnt von vorne.

Dritte Anwendung: Primzahltest II

Die Frage ist wieder, ob ein gegebenes $n \in \mathbb{N}$ eine Primzahl ist oder nicht. Man testet nun, ob für ungerade a mit $\mathrm{ggT}(a, n) = 1$ der Satz von Euler gilt, d.h. ob $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n$. Bei einer Antwort „nein“ weiß man, dass es sich nicht um eine Primzahl handelt. Ist die Antwort für alle Zahlen $a < n$ „ja“, so handelt es sich um eine Primzahl.

Nach einem Ergebnis von Solovay und Strassen gibt es für zusammengesetztes n weniger als $\frac{1}{2}\varphi(n)$ Zahlen $\leqslant n$, für die der Test eine positive Antwort liefert. Beim Testen von k „unabhängigen“ a erhält man also mit Wahrscheinlichkeit mindestens $1 - \frac{1}{2^k}$ die richtige Antwort.

Die meisten der klassischen Primzahltest beruhen auf Varianten und Kombination von Test I und II.

Vierte Anwendung: Codierungstheorie

Problemstellung: bei der Übertragung von Nachrichten treten in der Regel Fehler auf. Kann man Nachrichten so codieren, dass man fehlerhafte Nachrichten erkennen kann, möglichst viele Fehler korrigieren kann und die Codierung effektiv bleibt?

Eine ineffektive Codierung wäre z.B. das k-malige Wiederholen von Nachrichten: tritt im schlimmsten Fall stets an der selben Stelle ein Übertragungsfehler auf, so kann man immer noch die Fehlerhaftigkeit einer empfangenen Nachricht bei bis zu $k-1$ Fehlern erkennen und bis zu $\lfloor \frac{k-1}{2} \rfloor$ Fehler korrigieren.

Praktisch ist es, die Buchstaben der Nachricht als Elemente in einem endlichen Körper zu wählen. Der alte ISBN–Code bestand z.B. aus einer neunstelligen Zahl $(a_1, \ldots, a_9)$, in der Sprache, Verlag und Buchnummer codiert sind. Zusätzlich fügt man eine Prüfstelle a_{10} so an, dass die Gleichung $\sum_{i=1}^{10} j \cdot a_j = 0$ in $\mathbb{Z}_{11}$ erfüllt ist (für das Element $10 \in \mathbb{Z}_{11}$ schrieb man X). Dieser Code erkennt, wenn eine Ziffer falsch geschrieben wird oder wenn zwei Ziffern vertauscht werden (d.h. dann stimmt die Gleichung nicht mehr).

Der neue ISBN–Code besteht aus einer zwölfstelligen Zahl $(b_1, \ldots, b_{12})$. Zusätzlich fügt man eine Prüfstelle b_{13} so an, dass die Gleichung $b_1 + 3b_2 + b_3 + 3b_4 + \cdots = 0$ in $\mathbb{Z}_{10}$ gilt. Dieser Code erkennt immer noch, wenn eine Ziffer falsch geschrieben wird, aber nur noch, wenn zwei benachbarte Ziffern, die nicht kongruent modulo 5 sind, vertauscht werden.

Viele andere Codierungs–Verfahren beruhen auch auf dem Rechnen in endlichen Körpern $\mathbb{F}_q$.

Sei $K = \mathbb{F}_q$ ein endlicher Körper (das Alphabet der Nachrichten). Ein *Code* (die gültigen Nachrichten) ist eine Teilmenge $C \subseteq K^n$ für ein festes $n \in \mathbb{N}$. Auf K^n definiert man die *Hamming–Metrik* durch $d\big((v_1, \ldots, v_n), (w_1, \ldots, w_n)\big) :=$ die Anzahl der j mit $v_j \neq w_j$. Das Gewicht des Codes ist $d(C) := \min_{\bar{v}, \bar{w} \in C} d(\bar{v}, \bar{w})$.
Günstig sind besonders die *linearen Codes*, bei denen C ein Untervektorraum von K^n ist. Mit $k := \dim C$ und $d^* := d(C)$ nennt man einen solchen Code auch einen $[n, k, d^*]$-Code. Es gilt dann stets $d^* \leqslant n - k + 1$. Ein $[n, k, d^*]$-Code erkennt bis zu $d^* - 1$ Fehler und korrigiert bis zu $r := \lfloor \frac{d^*-1}{2} \rfloor$ Fehler. Ein Code heißt *perfekt*, falls jedes $\bar{v} \in K^n$ höchstens Abstand r zu C hat.

Literaturverzeichnis

[A] Martin Aigner *Diskrete Mathematik*, 2e, Vieweg, Braunschweig 1996.

[Lange Zeit die einzige vernünftige deutschsprachige Einführung in die diskrete Mathematik. Mit viel Material, das allerdings oft unübersichtlich und in einem „Minimum Deutsch“ dargestellt ist.]

[C] Peter J. Cameron *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge 1994.

[Ein sehr schönes Buch, das viele Aspekte der Kombinatorik bietet, mit vielen Algorithmen und einigen überraschenden Beweisen. Auch die Graphentheorie ist mit vielen Aspekten vertreten.]

[D] Reinhard Diestel *Graphentheorie*, Springer, Heidelberg 1996, 2.Auflage 2000.
in Englisch: *Graph Theory*, Springer GTM 173, New York 1997, 3. Auflage 2005.

Beide Versionen sind auch online erhältlich:
`http://www.math.uni-hamburg.de/home/diestel/books/`

[H] Daniel Hug, Lars Diening, Bernd Siebert, Vorlesungsskript „Diskrete Algebraische Strukturen“, Universität Freiburg, SS 2008.

`http://www.mathematik.uni-freiburg.de/IAM/Teaching/scripts/das_SS08/DAS.pdf`

[L] Serge Lang *Algebra*, 3e, Addison–Wesley, Reading 1993.

[Umfangreiche Einführung in die Algebra.]

[S] A. Steger „Diskrete Strukturen“, Band 1, Springer.

[Nach meiner bisherigen Erfahrung ein sehr empfehlenswertes Buch!]

Index