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 m-Menge und N eine n-Menge, und alle betrachteten Mengen seien endlich.

Satz 1.1 (Additive Mächtigkeitsregeln)

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

(b) *Es gilt*

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

mit den Extremfällen

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

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

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

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 *mit Anfangswerten:*

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

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: *Komplementformel:*

$$\sum_{k=0}^{m} \binom{m}{k} = 2^m \qquad \binom{m}{k} = \binom{m}{m-k} \quad \textit{für} \quad m \geqslant k$$

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:

$S_{m,m} = 1$ $\qquad$ $S_{m,k} = 0$ *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
				$+2\cdot 3$					
4		0		1		7		1	15
						$+3\cdot 6$			
5		0		1		15		25	10	1		52
6		0		1		31		90	65	15	1	203

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):

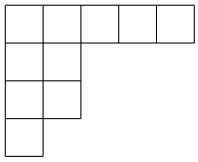


Abbildung 1.3: Ferrers–Diagramm für die Partition $10 = 5 + 2 + 2 + 1$.

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 $\tau \circ \sigma$.

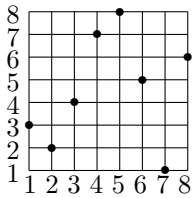
Wenn die Elemente einer Menge M angeordnet sind, z.B. als $x_1, x_2, \ldots, x_m$, dann überführt eine Permutation σ diese Anordnung in die Anordnung $\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_m)$. Umgekehrt legen zwei Anordnungen einer Menge genau eine Permutation fest, welche auf diese Weise die erste 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:

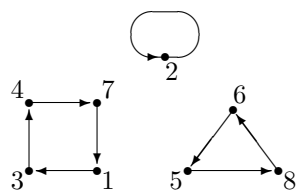
Wertetabelle

i	1	2	3	4	5	6	7	8
$\sigma(i)$	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:

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

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* $k > m \geqslant 0$

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

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

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

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:
$s_{m+1,2} = s_{m,1} + m \cdot s_{m,2} = (m-1)! + m \cdot (m-1)!\left(1 + \frac{1}{2} + \cdots + \frac{1}{m-1}\right) = m!\left(1 + \frac{1}{2} + \cdots + \frac{1}{m}\right)$.
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	$\Sigma = m!$
0	1			1
1	0	1		1
2	0	1	1	2
3	0	2	3	6
4	0	6	11	24
5	0	24	50	120
6	0	120	274	225	85	15	1	720

$+ m \cdot 6$

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:

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

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

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

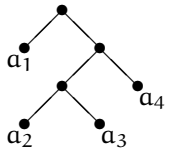
gegeben. Das charakteristische Polynom ist $X^3 - X^2 - 8X + 12 = (X-2)^2(X+3)$. Eine Basis der Lösungsmenge ist also durch $\left\{ 2^n, n \cdot 2^n, (-3)^n \right\}$ gegeben, die Lösungen sind genau die Folgen der Form $k_1 2^n + k_2 n 2^n + k_3 (-3)^n$. Für gegebene Anfangswerte A_0, A_1, A_2 erhält 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 49). 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:

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

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

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

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*“	$f \sim g$	$:\Longleftrightarrow$	$\lim\limits_{n\to\infty} \frac{f(n)}{g(n)} = 1$
„*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 $\lim\limits_{n \to \infty} \frac{|f(n)|}{|g(n)|}$ 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

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

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

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

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:

$$\begin{aligned} f \in O(g) &\iff \mathrm{grad}(f) \leqslant \mathrm{grad}(g) \\ f \in \Omega(g) &\iff \mathrm{grad}(f) \geqslant \mathrm{grad}(g) \\ f \in \Theta(g) &\iff \mathrm{grad}(f) = \mathrm{grad}(g) \end{aligned}$$

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.*

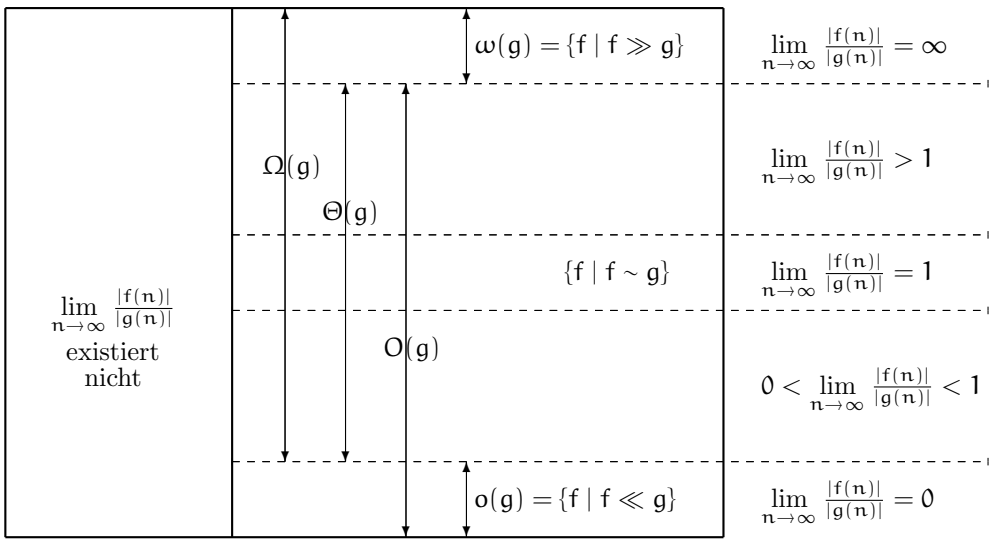
(c) *Verträglichkeit mit* $\ll$*:* $\quad f' \in O(f), g' \in \Omega(g), f \ll g \Longrightarrow f' \ll g'$.

(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 $\omega(g) := \{f \mid g \leqslant f\} = \{f \mid g \in o(f)\}$, so ergibt sich folgendes Bild, für eine feste Funktion g:



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 $n \ln n - n + 1 \leq \ln(n!) \leqslant (n+1)\ln(n+1) - n$ 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 folgt aus solchen Überlegungen (hier ohne Beweis) eine asymptotische Betsimmung der Fakultätsfunktion:

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.

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*:*

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

Beweis: Man überlege sich zunächst, dass A monoton verläuft. 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 $a = 1$ folgt daraus $A(b^k) \in \Theta(k)$, für $a > 1$ folgt $A(b^k) \in \Theta(a^k)$. Wegen der Monotonie erhält man, dass $A(k) = A(b^{\log_b k})$ im Θ-Sinne wie $\log_b k$ bzw. wie $a^{\log_b k} = k^{\log_b a}$ wächst. □