Sommersemester 2013

Algebraische Kombinatorik

Prof. Dr. Burkhard Külshammer

Ausarbeitung: Philipp Reichhardt

Inhaltsverzeichnis

1 Mengen

Literatur: Aigner, Jacobs & Jungnickel, van Lint & Wilson, Cameron, Stanley.

1.1 Bemerkung Einige Bezeichungen und Fakten:

- $\emptyset$
- $\mathbb{N} = \{1, 2, 3, \dots\}$
- $\mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$ wie üblich
- $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$ Primzahlen
- $|M|$ Mächtigkeit bzw. Kardinalität
- $|M \cup N| = |M| + |N|$, falls M, N disjunkt
- $|M \times N| = |M| \cdot |N|$
- Verallgemeinerung auf endlich viele Mengen möglich. Insbesondere: $|M^n| = |M|^n$.
- $\mathfrak{P}(M) = 2^M = \{A : A \subseteq M\}$ Potenzmenge von M

1.1 Satz *M endl. Menge* $\Rightarrow |2^M| = 2^{|M|}$

Beweis. Œ sei $M = \{1, 2, \dots, n\}$, $n \in \mathbb{N}$. Für $A \in \mathfrak{P}(M)$ definiert man

$$\chi_{_A} = (x_1, \dots\ , x_n) \in \{0,1\}^n \text{ durch } x_i = \begin{cases} 1, & \text{falls } i \in A \\ 0, & \text{falls } i \notin A \end{cases}.$$

Dann ist $f\colon \mathfrak{P}(M) \to \{0,1\}^n$, $A \mapsto \chi_{_A}$ bijektiv. Daher: $|2^M| = |\{0,1\}^n| = |\{0,1\}|^n = 2^n$. □

1.2 Definition Eine *Permutation* einer Menge M ist eine Bijektion $\sigma\colon M \to M$.

Bemerkung Bekanntlich ist $\mathrm{Sym}(M) \coloneqq \{\sigma\colon M \to M, \sigma \text{ bijektiv}\}$ eine Gruppe bzgl. $\circ$.

Beispiel $(M = \{1, 2, 3\})$

$$\mathrm{Sym}(M) = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

1.2 Satz *M Menge,* $|M| = n < \infty \implies |\mathrm{Sym}(M)| = n!$.

Beweis. Permutationen σ von $M = \{a_1, a_2, \dots, a_n\}$ kann man folgendermaßen konstruieren: Für $\sigma(a_1)$ gibt es n Möglichkeiten. Für $\sigma(a_2)$ gibt es $n-1$ Möglichkeiten. Für $\sigma(a_3)$ gibt es $n-2$ Möglichkeiten usw. Insgesamt hat man für σ also $n(n-1)(n-2)\dots 1$ Möglichkeiten. □

1.3 Bemerkung Das gleiche Argument zeigt, dass für endliche Mengen M, N mit $|M| = m$, $|N| = n$ gilt:

$$|\{f\colon M \to N : \text{f injektiv}\}| = n(n-1)(n-2)\dots(n-m+1)\,.$$

Definition Ist M eine endliche Menge und $|M| = n$, so heißt M *n-Menge*. Für $k \in \mathbb{N}_0$ sei $\mathfrak{P}_k(M) = \binom{M}{k}$ die Menge aller k-Teilmengen von M.

1.3 Satz *Für $k, n \in \mathbb{N}$ und jede n-Menge N gilt:*

$$\left|\binom{N}{k}\right| = \binom{n}{k} \coloneqq \frac{n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k+1)}{1\cdot 2\cdot 3\cdot\ldots\cdot k}\,.$$

Beweis. Es existieren genau $n(n-1)(n-2)\dots(n-k+1)$ Injektionen

$$f\colon K \coloneqq \{1,\dots,k\} \to N\,.$$

Für solche f ist $f(K) = \{f(1), f(2), \dots, f(k)\}$ eine k-Teilmenge von N. So erwischt man jede k-Teilmenge von N. Zwei Injektionen $f, g\colon K \to N$ haben genau dann das gleiche Bild, wenn sie sich nur durch eine Permutation von $\{1,\dots,k\}$ unterscheiden. Wegen $|\mathrm{Sym}(K)| = k(k-1)\dots 1 = k!$ folgt die Behauptung. □

1.4 Bemerkung Aus den Sätzen 1.1 und 1.3 folgt sofort die bekannte Formel

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

Oft schreibt man die *Binomialkoeffizienten* $\binom{n}{k}$ als Pascal'sches Dreieck auf.

$$\binom{0}{0}$$

$$\binom{1}{0}\quad\binom{1}{1}$$

$$\binom{2}{0}\quad\binom{2}{1}\quad\binom{2}{2}$$

$$\binom{3}{0}\quad\binom{3}{1}\quad\binom{3}{2}\quad\binom{3}{3}$$

$$\binom{4}{0}\quad\binom{4}{1}\quad\binom{4}{2}\quad\binom{4}{3}\quad\binom{4}{4}$$

Die obige Formel bestimmt eine Zeilensumme. Man zeigt leicht:

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

[Denn für eine k-Teilmenge A von $N \coloneqq \{1,\dots,n\}$ gibt es zwei Alternativen:
(1) $n \in A$ (2) $n \notin A$

Im Fall 1 ist $A = \{n\} \cup \{B\}$ für eine $(k-1)$-Teilmenge B von $\{1, \ldots, n-1\}$. Deren Anzahl ist $\binom{n-1}{k-1}$. Im Fall 2 ist $A \subseteq \{1, 2, \ldots, n-1\}$. Deren Anzahl ist $\binom{n-1}{k}$.]
Wichtig ist die bekannte binomische Formel:

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

Satz *Für $k, n \in \mathbb{N}$ existieren genau $\binom{n+k-1}{k}$ Elemente $(x_1, \ldots, x_k) \in \mathbb{N}^k$ mit*

$$1 \leq x_1 \leq x_2 \leq \ldots \leq x_k \leq n\,.$$

Beweis. Durch $(x_1, \ldots, x_k) \mapsto \{x_1 + 0, x_2 + 1, x_3 + 2, \ldots, x_k + k - 1\}$ erhält man eine Bijektion zwischen der Menge der obigen k-Tupel $(x_1, \ldots, x_k)$ und der Menge aller k-Teilmengen von $\{1, \ldots, n+k-1\}$. Deren Anzahl ist $\binom{n+k-1}{k}$. □

Beispiel $n = 3$, $k = 2$: $(1,1)$, $(1,2)$, $(1,3)$, $(2,2)$, $(2,3)$, $(3,3)$.
Probe: $\binom{n+k-1}{k} = \binom{3+2-1}{2} = \binom{4}{2} = 6$.

1.5 Satz *Sei $M = \{a_1, \ldots, a_n\}$ für $n \in \mathbb{N}$, seien $r_1, \ldots, r_n \in \mathbb{N}$ und $k = r_1 + \ldots + r_n$. Dann existieren genau $\frac{k!}{r_1! r_2! \ldots r_n!}$ Elemente $(b_1, \ldots, b_k) \in M^k$ mit $|\{i : 1 \leq i \leq k, b_i = a_j\}| = r_j$ für $j = 1, \ldots, n$.*

Beispiel $M = \{a, b, c\}$, $r_1 = 1 = r_2$, $r_3 = 2 \Rightarrow k = 1 + 1 + 2 = 4$. Gesucht sind also Wörter der Länge 4 mit $1 \times a$, $1 \times b$, $2 \times c$.

$$\curvearrowright abcc, acbc, accb, bacc, bcac, bcca, cabc, cacb, cbac, cbca, ccab, ccba\,.$$

Beweis. Seien $A_1, \ldots, A_n$ paarweise disjunkt mit $|A_1| = r_1$, $|A_2| = r_2$, … usw. Setze $A := A_1 \cup A_2 \cup \ldots \cup A_n$. Dann: $|A| = |A_1| + |A_2| + \ldots + |A_n| = r_1 + r_2 + \ldots + r_n = k$. Nach Satz 1.2 existieren genau $k!$ Bijektionen $f\colon \{1, \ldots, k\} \to A$. Jedes solche f liefert eine Funktion $\bar{f}\colon \{1, \ldots, k\} \to \{1, \ldots, n\}$, $i \mapsto j$, falls $f(i) \in A_j$. Dann hat $\bar{f}$ die Eigenschaft $|\{i : 1 \leq i \leq k, \bar{f}(i) = j\}| = r_j$ (für $j = 1, \ldots, n$). Ferner entsteht jede Funktion $F\colon \{1, \ldots, k\} \to \{1, \ldots, n\}$ mit $|\{i : 1 \leq i \leq k, F(i) = j\}| = r_j$ so. Für Bijektionen $f, g\colon \{1, \ldots, n\} \to A$ ist genau dann $\bar{f} = \bar{g}$, wenn f und g sich nur durch ein Element in $\mathrm{Sym}(A_1) \times \ldots \times \mathrm{Sym}(A_n)$ unterscheiden. Wegen $|\mathrm{Sym}(A_j)| = r_j!$ $(j = 1, \ldots, n)$ folgt die Behauptung. □

Bemerkung Die Zahlen

$$\frac{k!}{r_1! r_2! \ldots r_n!} =: \binom{k}{r_1, r_2, \ldots, r_n}$$

heißen *Multinomialkoeffizienten*. Sie treten in der *multinomischen Formel* auf:

$$(x_1 + \ldots + x_n)^k = \sum_{\substack{r_1, \ldots, r_n \in \mathbb{N}_0 \\ r_1 + \ldots + r_n = k}} \binom{k}{r_1, r_2, \ldots, r_n} x_1^{r_1} x_2^{r_2} \ldots x_n^{r_n} \quad (x_1, \ldots, x_n \in \mathbb{C},\, k \in \mathbb{N}).$$

Für $n = 2$, d.h. $r_1 + r_2 = k$ ist $\binom{k}{r_1, r_2} = \binom{k}{r_1} = \binom{k}{r_2}$, d.h. man erhält die Binomialkoeffizienten zurück als Spezialfall.

2 Vektorräume

2.1 Vorbemerkung Im Folgenden werden wir versuchen, Mengen, Teilmengen, Abbildungen zu ersetzen durch Vektorräume, Untervektorräume und lineare Abbildungen. Dazu sei $\mathbb{K}$ ein endlicher Körper und $q := |\mathbb{K}|$. In der Algebra lernt man, dass q eine Primzahlpotenz ist (z.B. $q = 81 = 3^4$). Ferner lernt man, dass umgekehrt zu jeder Primzahlpotenz q im Wesentlichen genau ein Körper $\mathbb{K}$ mit $|\mathbb{K}| = q$ existiert. Diesen bezeichnet man mit $\mathbb{F}_q = \mathrm{GF}(q)$.

Beispiel ($q = 2$)

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

2.1 Satz *Sei $\mathbb{K}$ ein Körper mit $q := |\mathbb{K}| < \infty$. Für $m, n \in \mathbb{N}$ mit $m \leq n$ existieren dann genau $(q^n - 1)(q^n - q) \dots (q^n - q^{m-1})$ $m \times n$-Matrizen des Rangs m mit Koeffizienten in $\mathbb{K}$.*

Beweis. (Wir zählen $m \times n$-Matrizen mit m linear unabhängigen Zeilen) Die erste Zeile einer solchen Matrix A ist ein von 0 verschiedener Vektor a_1 in $\mathbb{K}^n$. Dafür gibt es $|\mathbb{K}^n \setminus \{0\}| = q^n - 1$ Möglichkeiten. Die zweite Zeile von A ist ein von a_1 linear unabhängiger Vektor a_2 in $\mathbb{K}^n$. Dafür gibt es $|\mathbb{K}^n \setminus \mathbb{K}a_1| = q^n - q$ Möglichkeiten. Die dritte Zeile ist ein von a_1 und a_2 linear unabhängiger Vektor a_3 in $\mathbb{K}^n$. Da a_1,a_2 einen zweidimensionalen Untervektorraum von $\mathbb{K}^n$ aufspannen, gibt es für a_3 genau $|\mathbb{K}^n \setminus (\mathbb{K}a_1 + \mathbb{K}a_2)| = q^n - q^2$ Möglichkeiten usw. Insgesamt gibt es für A genau $(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{m-1})$ Möglichkeiten. □

2.2 Beispiel Für $n \in \mathbb{N}$ sei $\mathrm{GL}(n, \mathbb{K}) := \{A \in \mathbb{K}^{n \times n} : A \text{ invertierbar}\}$, d.h.

$$\mathrm{GL}(n, \mathbb{K}) = \{A \in \mathbb{K}^{n \times n} : \mathrm{rg}(A) = n\}.$$[1]

Dann:

$$|\mathrm{GL}(n, \mathbb{K})| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}).$$

Bemerkung Sei wieder $\mathbb{K}$ ein endlicher Körper und $q := |\mathbb{K}|$. Dann entsprechen Matrizen vom Rang m in $\mathbb{K}^{n \times m}$ injektiven linearen Abbildungen f eines m-dimensionalen $\mathbb{K}$-Vektorraums V in einen n-dimensionalen $\mathbb{K}$-Vektorraum W. Daher gibt es genau

$$(q^n - 1)(q^n - q) \dots (q^n - q^{m-1})$$

injektive lineare Abbildungen $f \colon V \to W$ und

$$(q^n - 1)(q^n - q) \dots (q^n - q^n - 1)$$

bijektive lineare Abbildungen $g \colon W \to W$.

[1] allgemeine lineare Gruppe des Grades n über $\mathbb{K}$.

Satz *Für $k, n \in \mathbb{N}_0$ mit $k \leq n$ hat ein n-dimensionaler Vektorraum V über dem Körper $\mathbb{K}$ mit $|\mathbb{K}| =: q < \infty$ genau*

$$\frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} =: \binom{n}{k}_q$$

Untervektorräume der Dimension k.

Beweis. Œ sei $V = \mathbb{K}^n$. Nach Satz 2.1 existieren genau

$$(q^n-1)(q^n-q)\dots(q^n-q^{k-1})$$

k-Tupel $(u_1, \dots, u_k)$ linear unabhängiger Vektoren $u_1, \dots, u_k$ in $\mathbb{K}^n$. Jedes solche k-Tupel $(u_1, \dots, u_k)$ liefert einen k-dimensionalen Untervektorraum $\operatorname{Span}(u_1, \dots, u_k)$ von $\mathbb{K}^n$ und jeder k-dimensionale Untervektorraum von $\mathbb{K}^n$ entsteht so. Analog existieren zu jedem k-dimensionalen Untervektorraum $U \subseteq V$ genau

$$(q^k-1)(q^k-q)\dots(q^k-q^{k-1})$$

k-Tupel $(u_1, \dots, u_k)$ linear unabhängiger Vektoren in U. Daher ergeben jeweils

$$(q^k-1)(q^k-q)\dots(q^k-q^{k-1})$$

k-Tupel $(u_1, \dots, u_k)$ den gleichen Untervektorraum von V. Die Anzahl der k-dimensionalen Untervektorräume von V ist also

$$\frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}\,.$$

□

Definition Die Zahlen $\binom{n}{k}_q$ heißen *Gauß-Koeffizienten* (bzgl. q).

2.3 Satz *Für $n \in \mathbb{N}_0$ und $k = 0, \dots, n$ ist* $\binom{n}{k}_q = \binom{n}{n-k}_q$.

Beweis. Man kann das natürlich direkt nachrechnen. Wir argumentieren anders. Für jeden Vektorraum V der Dimension n über einem endlichen Körper $\mathbb{K}$ mit $|\mathbb{K}| =: q$ hat der Dualraum $V^* := \{f \colon V \to \mathbb{K} : f \text{ linear}\}$ auch Dimension n. Für jeden Untervektorraum $U \subseteq V$ mit $\dim U = k$ ist $U^\perp := \{f \in V^* : f(U) = 0\}$ ein Untervektorraum der Dimension $n-k$ von V^*. Ferner ist die Abbildung $U \mapsto U^\perp$ eine Bijektion zwischen

$$\{U \subseteq V : U \text{ Untervektorraum}, \dim U = k\}$$

und

$$\{W \subseteq V^* : W \text{ Untervektorraum}, \dim W = n-k\}\,.$$

Daraus folgt die Behauptung. □

2.4 Satz *Für $x \in \mathbb{C}$ und $n \in \mathbb{N}_0$ gilt:*

$$x^n = \sum_{k=0}^{n} \binom{n}{k}_q (x-1)(x-q)\dots(x-q^{k-1})\,.$$

Bemerkung Diese Formel ist das q-Analogon zu der bekannten Formel

$$x^n = \sum_{k=0}^{n} \binom{n}{k} (x-1)^k\,.$$

Beweis. Sei V ein $\mathbb{K}$-Vektorraum der Dimension $n < \infty$ und W ein $\mathbb{K}$-Vektorraum der Dimension $m < \infty$ ($\mathbb{K}$ Körper mit $|\mathbb{K}| = q < \infty$). Betrachte

$$\mathrm{Hom}(V,W) \coloneqq \{f\colon V \to W : f \text{ linear}\}\,.$$

Da jedes $f \in \mathrm{Hom}(V,W)$ durch die Bilder einer Basis eindeutig bestimmt ist, gilt:

$$|\mathrm{Hom}(V,W)| = |W|^n = q^{m\cdot n} \quad (\text{mit } |W| = q^m).$$

Für jedes $f \in \mathrm{Hom}(V,W)$ ist $\mathrm{Ker}(f) \subseteq V$ ein Untervektorraum. Wir sortieren die $f \in \mathrm{Hom}(V,W)$ nach ihren Kernen. Sei $U \subseteq V$ ein Untervektorraum und $u_1,\dots,u_k$ eine Basis von U. Wir ergänzen $u_1,\dots,u_k$ zu einer Basis $u_1,\dots,u_k,u_{k+1},\dots,u_n$ von V. Für jedes $f \in \mathrm{Hom}(V,W)$ mit $\mathrm{Ker}(f) = U$ ist dann $f(u_1) = \dots = f(u_k) = 0$ und $f(u_{k+1}),\dots,f(u_n)$ sind linear unabhängige Vektoren in W. Daher existieren genau $(q^m-1)(q^m-q)(q^m-q^2)\dots(q^m-q^{n-k-1})$ Möglichkeiten für f. Jetzt variieren wir U und erhalten

$$\begin{aligned}(q^m)^n = |\mathrm{Hom}(V,W)| &= \sum_{\substack{U\subseteq V\\ U \text{ Untervektorraum}}} (q^m-1)(q^m-q)\dots(q^m-q^{n-\dim U-1})\\ &= \sum_{k=0}^{n} \binom{n}{k}_q (q^m-1)(q^m-q)\dots(q^m-q^{n-k-1})\\ &= \sum_{l=0}^{n} \binom{n}{l}_q (q^m-1)(q^m-q)\dots(q^m-q^{l-1})\,.\end{aligned}$$

Die Polynome

$$x^n \text{ und } \sum_{l=0}^{n} \binom{n}{l}_q (x-1)(x-q)\dots(x-q^{l-1})$$

stimmen also auf allen q-Potenzen q^m ($\neq 1$) überein. Daher sind sie gleich. □

2.5 Satz *Für $n \in \mathbb{N}$ und $k = 1,\dots,n$ gilt: $\binom{n}{0}_q = \binom{n}{n}_q = 1$ und*

$$\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q\,.$$

Beweis. Die erste Aussage ist klar. Sei $\mathbb{K}$ ein Körper mit $|\mathbb{K}| = q < \infty$. Sei V ein n-dimensionaler $\mathbb{K}$-Vektorraum und es sei W ein fester $(n-1)$-dimensionaler Untervektorraum von V. Für einen k-dimensionalen Untervektorraum U von V hat man zwei Alternativen:
(1) $U \subseteq W$ (2) $U \not\subseteq W$.

Im Fall 1 hat man nach Definition genau $\binom{n-1}{k}_q$ Möglichkeiten für U. Im Fall 2 ist jeweils $U \cap W$ ein $k-1$-dimensionaler Untervektorraum von W. Für $U \cap W$ gibt es genau $\binom{n-1}{k-1}_q$ Möglichkeiten. Wie viele Möglichkeiten für U gibt es bei festem $U \cap W$? Jeder $(k-1)$-dimensionale Untervektorraum X von V ist in $\frac{q^{n-k+1}-1}{q-1}$ Untervektorräumen Y von V der Dimension k enthalten. [Denn: $Y = \mathbb{K}y + X$ für ein $y \in V \setminus X$. Für y gibt es also $q^n - q^{k-1}$ Möglichkeiten. Dabei gilt für $y, y' \in V \setminus X$: $\mathbb{K}y + X = \mathbb{K}y' + X \Leftrightarrow y' \in \mathbb{K}^\times y + X$.[2] Wegen $|\mathbb{K}^\times y + X| = (q-1)q^{k-1}$ gibt es also für Y genau $\frac{q^n - q^{k-1}}{q^k - q^{k-1}} = \frac{q^{n-k+1}-1}{q-1}$ Möglichkeiten.] Analog ist jeder $(k-1)$-dimensionale Untervektorraum X von W in genau $\frac{q^{n-k}-1}{q-1}$ Untervektorräumen Y von W der Dimension k enthalten. Bei festem $U \cap W$ gibt es also $\frac{q^{n-k+1}-1}{q-1} - \frac{q^{n-k}-1}{q-1} = \frac{q^{n-k+1}-q^{n-k}}{q-1} = q^{n-k}$ Möglichkeiten für U. Im Fall 2 gibt es daher $q^{n-k}\binom{n-1}{k-1}_q$ Möglichkeiten für U. □

2.6 Definition Sei V ein Vektorraum der Dimension $n < \infty$ über einem Körper $\mathbb{K}$ mit $|\mathbb{K}| = q < \infty$. Dann heißt die Anzahl $G_{n,q}$ aller Untervektorräume von V die n-te *Galoiszahl* (bzgl. q).

Bemerkung $G_{n,q} = \sum_{k=0}^{n} \binom{n}{k}_q$ ist dann das q-Analogon zu $2^n = \sum_{k=0}^{n} \binom{n}{k}$.

Beispiel

- $G_{0,q} = 1$, da der Nullraum genau einen Untervektorraum hat.
- $G_{1,q} = 2$, da ein eindimensionaler Vektorraum V genau $\{0\}, V$ als Untervektorräume hat.
- $G_{2,q} = 1 + \frac{q^2-1}{q-1} + 1 = q + 3$.

Satz *Für $n \in \mathbb{N}$ gilt: $G_{n+1,q} = 2G_{n,q} + (q^n - 1)G_{n-1,q}$.*

Beweis.

$$\begin{aligned} G_{n+1,q} &= \sum_{k=0}^{n+1} \binom{n+1}{k}_q \\ &= \binom{n+1}{0}_q + \sum_{k=1}^{n} \binom{n+1}{k}_q + \binom{n+1}{n+1}_q \end{aligned}$$

[2] $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$.

$$
\begin{aligned}
&\overset{2.5}{=} 1 + \sum_{k=1}^{n} \left[\binom{n}{k}_q + q^{n+1-k} \binom{n}{k-1}_q \right] + 1 \\
&= \underbrace{1 + \sum_{k=1}^{n} \binom{n}{k}_q}_{G_{n,q}} + \underbrace{\sum_{k=1}^{n} (q^{n+1-k} - 1) \binom{n}{k-1}_q}_{\sum_{l=0}^{n-1} (q^{n-l}-1)\binom{n}{l}_q} + \underbrace{\sum_{k=1}^{n} \binom{n}{k-1}_q + 1}_{\sum_{l=0}^{n-1} \binom{n}{l}_q + 1 = G_{n,q}} \\
&= 2G_{n,q} + \sum_{l=0}^{n-1} (q^{n-l} - 1) \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{l-1})}{(q^l - 1)(q^l - q) \dots (q^l - q^{l-1})} \\
&= 2G_{n,q} + \sum_{l=0}^{n-1} \underbrace{(q^{n-l} - 1) \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-l+1} - 1)}{(q^l - 1)(q^{l-1} - 1) \dots (q - 1)}}_{(q^n-1)\binom{n-1}{l}_q} \\
&= 2G_{n,q} + (q^n - 1) \underbrace{\sum_{l=0}^{n-1} \binom{n-1}{l}_q}_{G_{n-1,q}} \\
&= 2G_{n,q} + (q^n - 1) G_{n-1,q} \,.
\end{aligned}
$$

□

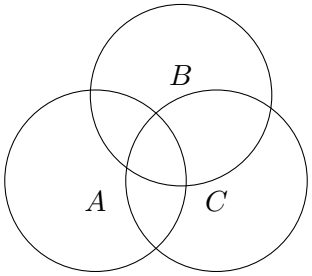
3 Das Prinzip vom Ein- und Ausschließen

3.1 Bemerkung Für endliche Mengen A,B ist folgendes richtig:

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

Analog gilt für endliche Mengen A, B, C:

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



Wie sieht die entsprechende Formel für n Mengen $A_1, \ldots, A_n$ aus?

Satz (Prinzip vom Ein- und Ausschließen) *Für endliche Mengen $A_1, \ldots, A_n$ gilt stets:*

$$|A_1 \cup \ldots \cup A_n| = \sum_{\emptyset \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|-1} \Big| \bigcap_{i \in I} A_i \Big|\,.$$

Beweis (Induktion nach n). Im Fall $n = 1$ steht links $|A_1|$. Rechts steht genau ein Summand, nämlich $|A_1|$. Sei also jetzt $n > 1$ und schon gezeigt, dass für $(n-1)$ Mengen $B_1, \ldots, B_{n-1}$ gilt:

$$|B_1 \cup \ldots \cup B_{n-1}| = \sum_{\emptyset \neq J \subseteq \{1,\ldots,n-1\}} (-1)^{|J|-1} \Big| \bigcap_{j \in J} B_j \Big|\,.$$

Dann gilt für $A_1, \ldots, A_n$ nach obiger Bemerkung:

$$\begin{aligned}
|A_1 \cup \ldots \cup A_n| &= |(A_1 \cup \ldots \cup A_{n-1}) \cup A_n| \\
&= |A_1 \cup \ldots \cup A_{n-1}| + |A_n| - |\underbrace{(A_1 \cup \ldots \cup A_{n-1}) \cap A_n}_{(A_1 \cap A_n) \cup \ldots \cup (A_{n-1} \cap A_n)}| \\
&= \sum_{\emptyset \neq J \subseteq \{1,\ldots,n-1\}} (-1)^{|J|-1} \Big| \bigcap_{j \in J} A_j \Big| + |A_n| - \sum_{\emptyset \neq J \subseteq \{1,\ldots,n-1\}} (-1)^{|J|-1} \Big| \bigcap_{j \in J} A_j \cap A_n \Big| \\
&= \sum_{\emptyset \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|-1} \Big| \bigcap_{i \in I} A_i \Big|\,.
\end{aligned}$$

□

3.2 Definition Sei M eine Menge, $n = |M| < \infty$ und $\sigma \in \mathrm{Sym}(M)$. Ein Element $a \in M$ mit $\sigma(a) = a$ heißt *Fixpunkt* von σ. Hat σ keine Fixpunkte, so heißt σ *fixpunktfrei*. Man setzt $D_n \coloneqq |\{\sigma \in \mathrm{Sym}(M) : \sigma \text{ fixpunktfrei}\}|$[3].

[3] D steht für das englische Wort *derangements*.

Beispiel

- $n = 3 \Rightarrow D_n = D_3 = 2$: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
- $n = 4 \Rightarrow D_n = D_4 = 9$ (nachrechnen!)

Satz $n \in \mathbb{N} \Longrightarrow D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

Beweis. Œ sei $M = \{1, \ldots, n\}$. Für $i = 1, \ldots, n$ sei $A_i := \{\sigma \in \mathrm{Sym}(M) : \sigma(i) = i\}$. Für $J \subseteq M$ ist

$$\bigcap_{j \in J} A_j = \{\sigma \in \mathrm{Sym}(M) : \sigma(j) = j \text{ für alle } j \in J\}\,, \text{ also } \Big|\bigcap_{j \in J} A_j\Big| = (n - |J|)!\,.$$

Das Prinzip vom Ein- und Ausschließen liefert also:

$$\begin{aligned} D_n &= |\{\sigma \in \mathrm{Sym}(M) : \sigma \text{ fixpunktfrei}\}| = |\mathrm{Sym}(M) \setminus \{A_1 \cup \ldots \cup A_n\}| \\ &= n! - \sum_{\emptyset \neq J \subseteq \{1,\ldots,n\}} (-1)^{|J|-1} \Big|\bigcap_{j \in J} A_j\Big| \\ &= n! + \sum_{\emptyset \neq J \subseteq \{1,\ldots,n\}} (-1)^{|J|} (n - |J|)! \\ &= n! + \sum_{k=1}^{n} \binom{n}{k} (-1)^k (n-k)! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}\,. \end{aligned}$$

□

Bemerkung $\frac{D_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ ist die Wahrscheinlichkeit, dass eine zufällig gewählte Permutation $\sigma \in \mathrm{Sym}(M)$ fixpunktfrei ist. Für $n \to \infty$ erhält man $\frac{D_n}{n!} \to \frac{1}{e} \sim 0,367$. Für große n ist also mehr als jede 3. Permutation fixpunktfrei. Steckt also Sekretärin Schusseline n Briefe in n Umschläge, so liegt die Wahrscheinlichkeit bei $\frac{1}{e}$, dass kein Brief im richtigen Umschlag ist.

3.3 Satz *Für $1 \neq n \in \mathbb{N}$ gilt:*

(i) $D_n = nD_{n-1} + (-1)^n$,

(ii) $D_{n+1} = n(D_n + D_{n-1})$.

Beweis.

(i)

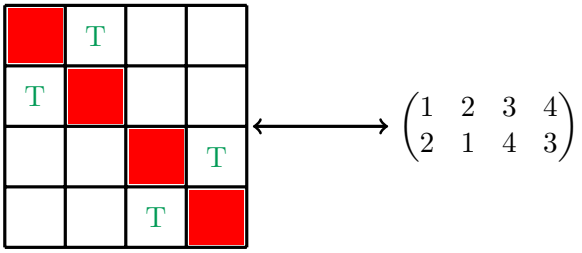
$$nD_{n-1} + (-1)^n = n \sum_{k=0}^{n-1} (-1)^k \frac{(n-1)!}{k!} + (-1)^n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = D_n\,.$$

(ii)

$$\begin{aligned} D_{n+1} &= (n+1)D_n + (-1)^{n+1} = nD_n + D_n + (-1)^{n+1} \\ &= nD_n + nD_{n-1} + (-1)^n + (-1)^{n+1} = n(D_n + D_{n-1})\,. \end{aligned}$$

□

Bemerkung D_n ist auch die Anzahl der Möglichkeiten, n Türme auf einem $n \times n$ Schachbrett so aufzustellen, dass keine zwei Türme in einer Zeile oder Spalte stehen und kein Turm auf der Diagonale steht.



3.4 Satz *Seien X, Y endliche Mengen und $n := |X|$, $k := |Y|$. Dann gilt für die Anzahl $s_{n,k}$ der surjektiven Abbildungen $f\colon X \to Y$:*

$$s_{n,k} = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n\,.$$

Insbesondere:

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^n = n!$$

und

$$\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n = 0 \quad \textit{für } k > n.$$

Beweis. Œ sei $Y = \{1, \ldots, k\}$. Für $i = 1, \ldots, k$ sei $A_i := \{f\colon X \to Y : i \notin f(X)\}$. Für $\emptyset \neq J \subseteq \{1, \ldots, k\}$ ist dann

$$\Big| \bigcap_{j \in J} A_j \Big| = |\mathrm{Abb}(X, Y \setminus J)| = (k - |J|)^n\,.$$

Das Prinzip vom Ein- und Ausschließen ergibt also:

$$\begin{aligned} s_{n,k} &= |\mathrm{Abb}(X,Y) \setminus \bigcup_{i=1}^{n} A_i| = k^n - \sum_{\emptyset \neq J \subseteq \{1,\ldots,k\}} (-1)^{|J|-1} \Big| \bigcap_{j \in J} A_j \Big| \\ &= k^n + \sum_{\emptyset \neq J \subseteq \{1,\ldots,k\}} (-1)^{|J|} \, (k - |J|)^n \\ &= k^n + \sum_{i=1}^{k} \binom{k}{i} (-1)^i (k-i)^n \\ &= \sum_{i=0}^{k} \binom{k}{i} (-1)^i (k-i)^n \, . \end{aligned}$$

□

3.5 Definition Für $x \in \mathbb{R}$ sei $\lfloor x \rfloor \in \mathbb{Z}$ definiert durch $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

3.5 Satz *Seien $a_1, \ldots, a_r \in \mathbb{N}$ paarweise teilerfremd, d.h. $\mathrm{ggT}(a_i, a_j) = 1$ für alle $i \neq j$. Für $n \in \mathbb{N}$ existieren dann genau*

$$n - \sum_{i=1}^{r} \left\lfloor \frac{n}{a_i} \right\rfloor + \sum_{1 \leq i < j \leq r} \left\lfloor \frac{n}{a_i a_j} \right\rfloor - + \ldots + (-1)^r \left\lfloor \frac{n}{a_1 a_2 \ldots a_r} \right\rfloor$$

Zahlen in $\{1, \ldots, n\}$, die durch keine der Zahlen $a_1, \ldots, a_r$ teilbar sind.

Beweis. Sei $M = \{1, \ldots, n\}$. Für $i = 1, \ldots, r$ sei $A_i := \{k \in M : a_i \text{ teilt } k\}$. Für $\emptyset \neq J \subseteq \{1, \ldots, r\}$ ist dann

$$\bigcap_{j \in J} A_j = \{k \in M : a_j \text{ teilt } k \text{ für alle } j \in J\} = \{k \in M : \prod_{j \in J} a_j \text{ teilt } k\} \, ,$$

also

$$\Big| \bigcap_{j \in J} A_j \Big| = \left\lfloor \frac{n}{\prod\limits_{j \in J} a_j} \right\rfloor .$$

Daher:

$$\begin{aligned} |A_1 \cup \ldots \cup A_r| &= \sum_{\emptyset \neq I \in \{1,\ldots,r\}} (-1)^{|I|-1} \Big| \bigcap_{i \in I} A_i \Big| \\ &= \sum_{i=1}^{r} \left\lfloor \frac{n}{a_i} \right\rfloor - \sum_{1 \leq i < j \leq r} \left\lfloor \frac{n}{a_i a_j} \right\rfloor + - \ldots + (-1)^{r-1} \left\lfloor \frac{n}{a_1 a_2 \ldots a_r} \right\rfloor . \end{aligned}$$

Die Behauptung folgt unmittelbar. □

3.6 Definition

(i) Für $a, b \in \mathbb{Z}$ schreibt man $a \mid b$, falls a ein Teiler von b ist.

(ii) Die *Euler'sche Phifunktion* $\varphi\colon \mathbb{N} \to \mathbb{R}$ ist definiert durch

$$\varphi(n) \coloneqq |\{k \in \mathbb{N} : 1 \leq k \leq n \ , \ \mathrm{ggT}(k,n) = 1\}| \, .$$

Beispiel $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, ...

Satz *Ist $n \in \mathbb{N}$ und sind $p_1, \ldots, p_r$ die verschiedenen Primteiler von n, so gilt:*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_r}\right) .$$

Beweis.

$$\begin{aligned} \varphi(n) &\overset{3.5}{=} n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} - + \ldots + (-1)^r \frac{n}{p_1 \ldots p_r} \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right) . \end{aligned}$$

□

Bemerkung Hat also n die Primfaktorzerlegung $n = p_1^{a_1} \ldots p_r^{a_r}$, so ist

$$\boxed{\varphi(n) = \left(p_1^{a_1} - p_1^{a_1 - 1}\right) \ldots \left(p_r^{a_r} - p_r^{a_r - 1}\right) .}$$

Zum Beispiel ist

$$\begin{aligned} \varphi(10000) = \varphi(10^4) = \varphi(2^4 \cdot 5^4) &= (2^4 - 2^3)(5^4 - 5^3) \\ &= (16 - 8)(625 - 125) = 8 \cdot 500 = 4000 \, . \end{aligned}$$

3.7 Definition Die *Möbius-Funktion* $\mu\colon \mathbb{N} \to \mathbb{R}$ wird definiert durch:

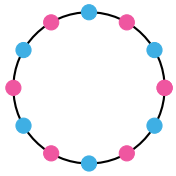
- $\mu(1) \coloneqq 1$,
- $\mu(n) \coloneqq 0$, falls $p^2 \mid n$ für ein $p \in \mathbb{P}$,
- $\mu(n) \coloneqq (-1)^r$, falls $n = p_1 \ldots p_r$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$.

3.7 Bemerkung Aus der obigen Formel folgt:

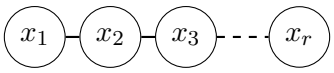
$$\boxed{\varphi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}} \qquad \text{(für } n \in \mathbb{N}\text{)}$$

Dabei durchläuft d alle positiven Teiler von n.

3.8 Bemerkung (Ehepaarproblem - Lucas 1891) $n \geq 2$ Ehepaare sollen in bunter Reihe so an einem runden Tisch sitzen, dass kein Mann neben seiner eigenen Frau sitzt. Dabei werden Sitzordnungen als verschieden angesehen, die durch Verschieben entstehen. Wie groß ist die Anzahl $\alpha(n)$ der möglichen Sitzordnungen? Wir werden $\alpha(n)$ in mehreren Schritten berechnen.



Satz *Für $1 \neq r \in \mathbb{N}$ und $t = 1, \ldots, r$ sei $f(r,t)$ die Anzahl der Möglichkeiten aus r in einer Reihe angeordneten Objekten t Stück so auszuwählen, dass keine zwei benachbarten Objekte ausgewählt werden. Dann ist $f(r,t) = \binom{r-t+1}{t}$.*



Beweis. (Induktion nach r) Die Behauptung stimmt für $t = 1$ und $t = r > 1$. Sei also $1 < t < r$, d.h. $r \geq 3$. Die Behauptung stimmt auch für $r = 3$ ($\curvearrowright t = 2$). Die Behauptung sei schon für alle $r' < r$ gezeigt. Es gibt zwei Alternativen:

(i) Das erste Objekt wird ausgewählt. Dann darf man das zweite Objekt nicht auswählen. Es gibt also noch $f(r-2, t-1)$ Wahlmöglichkeiten für die übrigen Objekte.

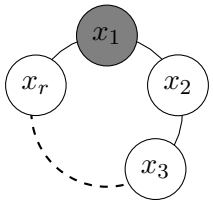
(ii) Das erste Objekt wird nicht ausgewählt. Dann gibt es noch $f(r-1, t)$ Wahlmöglichkeiten.

Daher gilt insgesamt nach Induktion:

$$\begin{aligned} f(r,t) &= f(r-2, t-1) + f(r-1, t) \\ &= \binom{r-2-(t-1)+1}{t-1} + \binom{r-1-t+1}{t} \\ &= \binom{r-t}{t-1} + \binom{r-t}{t} \\ &= \binom{r-t+1}{t}. \end{aligned}$$

□

3.9 Satz *Für $1 \neq r \in \mathbb{N}$ und $t = 0, \ldots, r-1$ sei $g(r,t)$ die Anzahl der Möglichkeiten aus r in einem Kreis angeordneten Objekten t Stück so auszuwählen, dass keine benachbarten Objekte ausgewählt werden. Dann ist $g(r,t) = \frac{r}{r-t}\binom{r-t}{t}$.*



Beweis. Wir legen auf dem Kreis einen Anfangspunkt fest und zählen von da aus. Die Behauptung ist richtig für $t \in \{0, 1\}$. Daher ist die Behauptung richtig für $r = 2$. Sei also $r \geq 3$. Die Behauptung ist dann auch richtig für $t = r - 1$. Dann ist die Behauptung auch für $r = 3$ richtig. Sei also $r \geq 4$. Wegen $g(4, 2) = 2 = \frac{4}{4-2}\binom{4-2}{2}$ kann man sogar $r \geq 5$ annehmen (und $2 \leq t \leq r - 2$). Dann gibt es zwei Alternativen:

(i) Das erste Objekt wird gewählt. Dann darf weder das zweite noch das r-te Objekt gewählt werden. Es gibt also noch $f(r-3, t-1) = \binom{r-3-(t-1)+1}{t-1} = \binom{r-t-1}{t-1}$ Wahlmöglichkeiten.

(ii) Das erste Objekt wird nicht ausgewählt. Dann gibt es noch $f(r-1, t) = \binom{r-1-t+1}{t} = \binom{r-t}{t}$ Wahlmöglichkeiten.

Insgesamt folgt:

$$\begin{aligned} g(r,t) &= \binom{r-t-1}{t-1} + \binom{r-t}{t} \\ &= \frac{(r-t-1)(r-t-2)\dots(r-2t+1)}{(t-1)!} \cdot \frac{r-t}{t} \cdot \frac{t}{r-t} + \binom{r-t}{t} \\ &= \binom{r-t}{t}\frac{t}{r-t} + \binom{r-t}{t} \\ &= \binom{r-t}{t}\frac{r}{r-t}\,. \end{aligned}$$

□

3.10 Satz *Für die Anzahl $\alpha(n)$ der Sitzordnungen beim Ehepaarproblem gilt:*

$$\alpha(n) = 2(n!)\sum_{t=0}^{n}(-1)^t\,(n-t)!\;\frac{2n}{2n-t}\binom{2n-t}{t}\,.$$

Beweis. Es gibt $2\,(n!)$ mögliche Sitzordnungen für die Damen. Daher: $\alpha(n) = 2(n!)\beta(n)$ wobei $\beta(n)$ die Anzahl der Sitzordnungen der Herren bei fester Platzverteilung für die Damen ist. Im Folgenden seien $D_1, \dots, D_n$ die Damen, kreisförmig um den Tisch verteilt. Die entsprechenden Herren seien also $H_1, \dots\ H_n$. Für $i = 1, \dots, n$ habe der Platz links von D_i die Nummer i. Jede Sitzordnung der Herren liefert eine Permutation σ von

$$M = \{1, \dots, n\} : \text{Herr } i \text{ sitzt auf Platz } \sigma(i)\,.$$

Umgekehrt liefert jede Permutation σ von M eine (evtl. verbotene) Sitzordnung der Herren. Eine Permutation σ von M heißt *erlaubt*, falls gilt:

- $\sigma(i) \neq i$ für $i = 1, \ldots, n$
- $\sigma(i) \neq i+1$ für $i = 1, \ldots, n-1$ und $\sigma(n) \neq 1$.

Wir müssen also jetzt die erlaubten Permutationen σ von M zählen. Für $i = 1, \ldots, n$ sei A_{1i} die Menge der Permutationen σ von M mit $\sigma(i) = i$. Für $j = 1, \ldots, n-1$ sei A_{2j} die Menge der Permutationen σ von M mit $\sigma(j) = j+1$. Fener sei A_{2n} die Menge der Permutationen σ von M mit $\sigma(n) = 1$. Wir setzen $I := \{(1,1), (1,2), \ldots, (1,n), (2,1), (2,2), \ldots, (2,n)\}$. Das Prinzip vom Ein- und Ausschließen liefert:

$$\begin{aligned}
\beta(n) &= n! - \Big|\bigcup_{i=1}^{n} A_{1i} \cup \bigcup_{i=1}^{n} A_{2i}\Big| \\
&= n! - \sum_{\emptyset \neq J \subseteq I} (-1)^{|J|-1} \Big|\bigcap_{j \in J} A_j\Big| \\
&= n! + \sum_{\emptyset \neq J \subseteq I} (-1)^{|J|} \Big|\bigcap_{j \in J} A_j\Big|
\end{aligned}$$

Für jede nichtleere Teilmenge $J \subseteq I$ ist also $\Big|\bigcap_{j \in J} A_j\Big|$ zu bestimmen. Dabei können verschiedene Fälle auftreten:

Fall 1: Es existieren $i \in \{1, \ldots, n\}$ mit $(1,i), (2,i) \in J$. Für $\sigma \in \bigcap_{j \in J} A_j$ ist $\sigma(i) = i$ und $\sigma(i) = i+1$. Das geht nicht. Also ist in diesem Falle $\bigcap_{j \in J} A_j = \emptyset$.

Fall 2: Es existieren $i \in \{1, \ldots, n-1\}$ mit $(2,i), (1,i+1) \in J$. Für $\sigma \in \bigcap_{j \in J} A_j$ ist dann $\sigma(i) = i+1$ und $\sigma(i+1) = i+1$. Das geht nicht. Also ist $\bigcap_{j \in J} A_j = \emptyset$.

Fall 3: $(2,n), (1,1) \in J$. Für $\sigma \in \bigcap_{j \in J} A_j$ ist $\sigma(n) = 1$ und $\sigma(1) = 1$. Dieser Fall kann nicht eintreten, also $\bigcap_{j \in J} A_j = \emptyset$.

In den übrigen Fällen haben wir $|J| \leq n$ und $\Big|\bigcap_{j \in J} A_j\Big| = (n - |J|)!$. Daher:

$$\beta(n) = n! + \sum_{t=1}^{n} (-1)^t (n-t)!\, h(n,t)\,.$$

Dabei ist $h(n,t)$ die Anzahl der Möglichkeiten t der Indizes in I so auszuwählen, dass keiner der Fälle 1-3 auftritt. Wir ordnen die Indizes in I in der Reihenfolge

$$(1,1), (2,1), \ldots, (1,n), (2,n)$$

auf einem Kreis an und erhalten mit den Bezeichnungen aus Satz 3.9:

$$h(n,t) = g(2n,t) = \frac{2n}{2n-t}\binom{2n-t}{t}\,.$$

Einsetzen ergibt die Aussage des Satzes. □

4 Partitionen

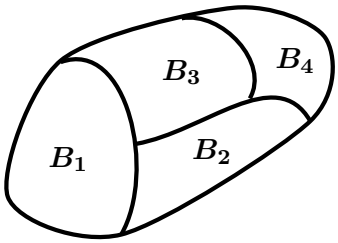
4.1 Definition Eine *Partition* einer (endlichen) Menge M ist eine Menge

$$\mathcal{P} = \{B_1, \ldots, B_n\}$$

nichtleerer, paarweise disjunkter Teilmengen $B_1, \ldots, B_n$ von M mit

$$M = B_1 \cup \ldots \cup B_n \,.$$

Man nennt $B_1, \ldots, B_n$ *Blöcke* von $\mathcal{P}$ und schreibt: $N(\mathcal{P}) = n$.



4.1 Beispiel $M = \{1, 2, 3, 4\}$ hat die folgenden Partitionen:

$N(\mathcal{P}) = 1$	$\big\{\{1,2,3,4\}\big\}$
$N(\mathcal{P}) = 2$	$\big\{\{1,2,3\},\{4\}\big\}, \big\{\{1,2,4\},\{3\}\big\}, \big\{\{1,3,4\},\{2\}\big\}, \big\{\{2,3,4\},\{1\}\big\}$
	$\big\{\{1,2\},\{3,4\}\big\}, \big\{\{1,3\},\{2,4\}\big\}, \big\{\{1,4\},\{2,3\}\big\}$
$N(\mathcal{P}) = 3$	$\big\{\{1,2\},\{3\},\{4\}\big\}, \big\{\{1,3\},\{2\},\{4\}\big\}, \big\{\{1,4\},\{2\},\{3\}\big\}$
	$\big\{\{2,3\},\{1\},\{4\}\big\}, \big\{\{2,4\},\{1\},\{3\}\big\}, \big\{\{3,4\},\{1\},\{2\}\big\}$
$N(\mathcal{P}) = 4$	$\big\{\{1\},\{2\},\{3\},\{4\}\big\}$.

Bemerkung Für $k, n \in \mathbb{N}$ sei $S(n,k)$ die Anzahl der Partitionen von $\{1, \ldots, n\}$ in k Blöcke. Außerdem sei $S(0,0) \coloneqq 1$ und $S(0,k) \coloneqq 0 =: S(n,0)$. Die Zahlen $S(n,k)$ heißen *Stirling-Zahlen* zweiter Art. Wir haben gesehen: $S(4,2) = 7$.

4.1 Satz *Für $k, n \in \mathbb{N}$ gilt:*

$$S(n,k) = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n \,.$$

Beweis. Jede surjektive Abbildung $f\colon \{1, \ldots, n\} \to \{1, \ldots, k\}$ liefert eine Partition

$$\mathcal{P} = \{B_1, \ldots, B_n\}$$

von $\{1, \ldots, n\}$ durch

$$B_i \coloneqq f^{-1}(\{i\})$$

für $i = 1, \ldots, k$ und jede Partition von $\{1, \ldots, n\}$ in k Blöcke entsteht so. Ferner liefern jeweils $k!$ surjektive Abbildungen $f\colon \{1, \ldots, n\} \to \{1, \ldots, k\}$ die gleiche Partition. Nach Satz 3.4 gilt also: $S(n,k) = \dfrac{1}{k!} s_{n,k} = \dfrac{1}{k!} \displaystyle\sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$. □

4.2 Satz *Für $x \in \mathbb{R}$ und $n \in \mathbb{N}$ gilt:* $x^n = \displaystyle\sum_{k=0}^{n} S(n,k)\, x(x-1)\ldots(x-k+1)$.

Beweis. Für $m, n \in \mathbb{N}$ existieren genau m^n Abbildungen $f\colon \{1, \ldots, n\} \to \{1, \ldots, m\}$. Für jede k-Teilmenge $Y \subseteq \{1, \ldots, m\}$ existieren genau $s_{n,k} = k!S(n,k)$ surjektive Abbildungen $f\colon \{1, \ldots, n\} \to Y$. Daher:

$$\begin{aligned} m^n &= \sum_{Y \subseteq \{1,\ldots,m\}} s_{n,|Y|} \\ &= \sum_{k=0}^{m} k!\, S(n,k) \binom{m}{k} \\ &= \sum_{k=0}^{m} S(n,k)\, m(m-1)(m-2)\ldots(m-k+1)\,. \end{aligned}$$

Im Fall $m > n$ ist $S(n,k) = 0$ für $k > n$, d.h.

$$m^n = \sum_{k=0}^{n} S(n,k)\, m(m-1)\ldots(m-k+1).$$

Die Polynome x^n und $\sum_{k=0}^{n} S(n,k)\, x(x-1)\ldots(x-k+1)$ nehmen also für $m > n$ die gleichen Werte an. Daher sind sie gleich. □

4.3 Satz *Für $k, n \in \mathbb{N}$ gilt:* $S(n,k) = kS(n-1,k) + S(n-1,k-1)$.

Beweis. Für $n = 1$ ist

$$S(n,k) = \begin{cases} 1, & \text{für } k = 1 \\ 0, & \text{für } k > 1 \end{cases}$$

und

$$kS(n-1,k) + S(n-1,k-1) = 0 + S(0,k-1) = \begin{cases} 1, & \text{für } k = 1 \\ 0, & \text{für } k > 1 \end{cases}.$$

Sei also $n > 1$. Für $k = 1$ ist

$$kS(n-1,k) + S(n-1,k-1) = S(n-1,1) + S(n-1,0) = 1 + 0 = 1 = S(n,1) = S(n,k)\,.$$

Sei also auch $k > 1$. Aus einer Partition von $\{1, \ldots, n-1\}$ kann man eine Partition von $\{1, \ldots, n\}$ machen, indem man entweder n als neuen Block nimmt oder indem man n zu einem der Blöcke hinzufügt. □

Bemerkung Für $n \in \mathbb{N}$ heißt

$$B(n) \coloneqq \sum_{k=0}^{n} S(n,k)$$

n-te *Bellzahl*. Ferner sei $B(0) \coloneqq 1$. $B(n)$ ist also die Anzahl *aller* Partitionen von $\{1,\dots,n\}$.

Beispiel Nach Beispiel 4.1 ist $B(4) = 15$.

4.4 Satz $n \in \mathbb{N} \Longrightarrow B(n) = \dfrac{1}{e}\sum_{k=0}^{\infty}\dfrac{k^n}{k!}$.

Beweis.

$$\begin{aligned}
\frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!} &= \sum_{j=0}^{\infty}\frac{(-1)^j}{j!}\sum_{k=0}^{\infty}\frac{k^n}{k!} \\
&= \sum_{l=0}^{\infty}\sum_{i=0}^{l}\frac{(-1)^i}{i!}\frac{(l-i)^n}{(l-i)!} \\
&= \sum_{l=0}^{\infty}\frac{1}{l!}\sum_{i=0}^{l}\binom{l}{i}(-1)^i(l-i)^n \\
&\overset{4.1}{=} \sum_{l=0}^{\infty} S(n,l) = \sum_{l=0}^{n} S(n,l) = B(n)\,.
\end{aligned}$$

□

4.5 Satz $n \in \mathbb{N}_0 \Longrightarrow B(n+1) = \sum_{r=0}^{n}\binom{n}{r}B(r)$.

Beweis. Œ sei $n \neq 0$. Sei $\mathcal{P}$ eine Partition von $\{1,\dots,n+1\}$. Sei A der Block von $\mathcal{P}$ mit $n+1 \in A$ und es sei $k \coloneqq |A| - 1$. Für A gibt es $\binom{n}{k}$ Möglichkeiten. Dann ist $\mathcal{P} \setminus \{A\}$ eine Partition von $\{1,\dots,n\} \setminus A$. Dafür gibt es $B(n-k)$ Möglichkeiten. Somit:

$$B(n+1) = \sum_{k=0}^{n}\binom{n}{k}B(n-k) = \sum_{r=0}^{n}\binom{n}{r}B(r)\,.$$

□

4.6 Definition Seien $k, n \in \mathbb{N}$. Eine *Partition* von n in k *Teile* ist ein k-Tupel

$$\lambda = (\lambda_1,\dots,\lambda_k)$$

von Zahlen $\lambda_1,\dots,\lambda_k \in \mathbb{N}$ mit $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$ und $\lambda_1 + \dots + \lambda_k = n$. Die Anzahl dieser Partitionen sei $p(n,k)$ (*Partitionszahlen*). Zusätzlich sei $p(0,0) \coloneqq 1$ und $p(0,k) \coloneqq 0 =: p(n,0)$ sowie $p(n) \coloneqq \sum_{k=1}^{\infty} p(n,k)$ und $p(0) \coloneqq 1$.

Beispiel $n = 7, k = 3:\ 7 = 5+1+1 = 4+2+1 = 3+3+1$, d.h. $p(7,3) = 4$.

Satz *Seien $k, n \in \mathbb{N}$ mit $k \leq n$. Dann gilt: $p(n,k) = p(n-1,k-1) + p(n-k,k)$.*

Beweis. Für $n = 1$, also auch $k = 1$ gilt:

$$p(n-1,k-1) + p(n-k,k) = p(0,0) + p(0,1) = 1 = p(1,1) = p(n,k)\,.$$

Für $n \neq 1 = k$ gilt:

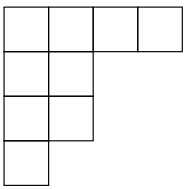
$$p(n-1,k-1) + p(n-k,k) = p(n-1,0) + p(n-1,1) = 1 = p(n,1)\,.$$

Sei also $n \neq 1 \neq k$. Für eine Partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ von n hat man zwei Alternativen:
(1) $\lambda_k = 1$, (2) $\lambda_k > 1$.

Im Fall 1 ist $(\lambda_1, \ldots, \lambda_{k-1})$ eine Partition von $n-1$ in $k-1$ Teile. Dafür existieren $p(n-1,k-1)$ Möglichkeiten. Im Fall 2 ist $(\lambda_1 - 1, \ldots, \lambda_k - 1)$ eine Partition von $n-k$ in k Teile. Dafür gibt es genau $p(n-k,k)$ Möglichkeiten. □

4.7 Definition Sei $n \in \mathbb{N}$ und $\lambda = (\lambda_1, \ldots, \lambda_k)$ eine Partition von n. Man schreibt $\lambda \vdash n$ und nennt $Y(\lambda) := \{(1,1), \ldots, (1,\lambda_1), (2,1), \ldots, (2,\lambda_2), \ldots, (k,1), \ldots, (k,\lambda_k)\} \subseteq \mathbb{N}^2$ das *Young-Diagramm* (bzw. *Ferrers-Diagramm*) von λ. Man veranschaulicht diese Young-Diagramme folgendermaßen:

$\lambda = (4,2,2,1) \vdash 9$ $\qquad Y(\lambda):$



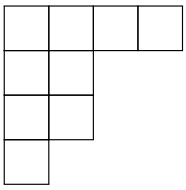
Literatur:

- W. Fulton, Young tableaux, Cambridge University Press 1996
- G.E. Andrews, The theory of partitions, Addison-Wesley 1976

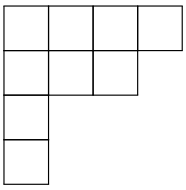
Bemerkung Für $\lambda \vdash n$ sei $\lambda' \vdash n$ dadurch definiert, dass $Y(\lambda')$ zu $Y(\lambda)$ "transponiert" ist. Dann heißt λ' zu λ *konjugiert*. Die Abbildung $\lambda \mapsto \lambda'$ ist eine Bijektion auf der Menge aller Partitionen (von n).

Beispiel

$\lambda = (4,2,2,1)$ $\qquad Y(\lambda):$



$\qquad Y(\lambda'):$



$\curvearrowright \lambda' = (4,3,1,1)$

Bemerkung Für $k, n \in \mathbb{N}$ ist also $p(n,k)$ auch die Anzahl der Partitionen $\mu = (\mu_1, \ldots, \mu_l)$ mit $\mu_1 = k$.

4.8 Bemerkung Wir wollen jetzt eine weitere Formel für die Gauß-Koeffizienten $\binom{n}{k}_q$ herleiten. Œ sei $V = \mathbb{K}^n$. Jeder k-dimensionale Untervektorraum $U \subseteq V$ hat eine Basis $b_1, \ldots, b_k$ und $b_1, \ldots, b_k$ bilden die Zeilen einer Matrix $B \in \mathbb{K}^{k\times n}$ vom Rang k. Umgekehrt liefert jede Matrix $A \in \mathbb{K}^{k\times n}$ vom Rang k einen k-dimensionalen Untervektorraum von $V = \mathbb{K}^n$, nämlich den Untervektorraum $\mathrm{ZR}(A)$ (*Zeilenraum*), der von den Zeilen von A aufgespannt wird. Natürlich können verschiedene Matrizen A, B den gleichen Untervektorraum von V liefern. Geht etwa B durch elementare Zeilenumformungen aus A hervor, so ist $\mathrm{ZR}(A) = \mathrm{ZR}(B)$. Man nennt Matrizen A,B *zeilenäquivalent*, wenn sie durch mehrfache elementare Zeilenumformungen auseinander hervorgehen. Zeilenäquivalente Matrizen liefern also jeweils den gleichen Untervektorraum von $\mathbb{K}^n$. Aus der Linearen Algebra ist bekannt, dass jede Matrix $A \in \mathbb{K}^{k\times n}$ vom Rang k zu genau einer Matrix $R \in \mathbb{K}^{k\times n}$ in rZSF[4] zeilenäquivalent ist. Das bedeutet:

(1) In jeder Zeile von R ist der erste von 0 verschiedene Koeffizient gleich 1.

(2) Die führende 1 in Zeile i steht jeweils links von der führenden 1 in Zeile $i+1$. $(i = 1, \ldots, k-1)$

(3) Eine Spalte, die eine führende 1 enthält, enthält sonst lauter Nullen.

Zur Verdeutlichung listen wir die Matrizen vom Rang 3 in $\mathbb{K}^{3\times 5}$ auf, die rZSF haben:

$$\begin{pmatrix} 1&0&0&*&*\\ 0&1&0&*&*\\ 0&0&1&*&* \end{pmatrix}, \begin{pmatrix} 1&0&*&0&*\\ 0&1&*&0&*\\ 0&0&0&1&* \end{pmatrix}, \begin{pmatrix} 1&0&*&*&0\\ 0&1&*&*&0\\ 0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&*&0&0&*\\ 0&0&1&0&*\\ 0&0&0&1&* \end{pmatrix},$$
$$\begin{pmatrix} 1&*&0&*&0\\ 0&0&1&*&0\\ 0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&*&*&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&0&*\\ 0&0&1&0&*\\ 0&0&0&1&* \end{pmatrix}, \begin{pmatrix} 0&1&0&*&0\\ 0&0&1&*&0\\ 0&0&0&0&1 \end{pmatrix},$$
$$\begin{pmatrix} 0&1&*&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}$$

Wir erhalten also eine Surjektion

$$\{R \in \mathbb{K}^{k\times n} : R \text{ in rZSF}, \ \mathrm{rg}(R) = k\} \to \{U : U \text{ Untervektorraum von } \mathbb{K}^{k\times n}, \dim U = k\},$$
$$A \mapsto \mathrm{ZR}(A)$$

Wir wollen zeigen, dass diese Surjektion auch bijektiv ist. Dazu seien R, S Matrizen vom Rang k in $\mathbb{K}^{k\times n}$, die beide rZSF haben und für die $\mathrm{ZR}(R) = \mathrm{ZR}(S)$ gilt. Dann ist jede Zeile von R eine Linearkombination der Zeilen von S. Also existiert $P \in \mathbb{K}^{k\times k}$ mit $R = PS$. Analog existiert ein $Q \in \mathbb{K}^{k\times k}$ mit $S = QR$. Daher $R = PQR$. Wegen $\mathrm{rg}(R) = k$ folgt $PQ = 1_k$, d.h. $P, Q \in \mathrm{GL}(k, \mathbb{K})$. Also kann man P durch mehrfache elementare

[4] reduzierte Zeilenstufenform.

Zeilenumformungen in 1_k überführen. Daher kann man $R = PS$ durch mehrfache elementare Zeilenumformungen in S überführen. Daher sind R und S zeilenäquivalent. Wegen der Eindeutigkeit folgt $R = S$. Die obige Surjektion ist also auch injektiv, also bijektiv. Folglich ist $\binom{n}{k}_q$ auch die Anzahl der Matrizen vom Rang k in $\mathbb{K}^{k\times n}$, die rZSF haben. Jede Matrix $R \in \mathbb{K}^{k\times n}$ vom Rang k in rZSF liefert eine Partition einer Zahl $l \leq k(n-k)$.[5] Im obigen Beispiel erhält man die folgenden Partitionen:

$$(2,2,2),(2,2,1),(2,2),(2,1,1),(2,1),(2),(1,1,1),(1,1),(1),()\,.$$

Man erhält so alle Partitionen, deren Young-Diagramm in ein Rechteck der Größe $k \times (n-k)$ passt. Jeweils q^l Matrizen liefern die gleiche Partition (für $*$ kann man jeweils ein beliebiges Element aus $\mathbb{K}$ einsetzen). Damit folgt:

Satz *Für alle (sinnvollen) n, k, q gilt:*

$$\binom{n}{k}_q = \sum_{l=0}^{k(n-k)} a_l\, q^l\,.$$

Dabei ist a_l die Anzahl der Partitionen von l, deren Young-Diagramm in ein Rechteck der Größe $k \times (n-k)$ passt. Insbesondere ist also $\binom{n}{k}_q$ für feste n, k ein Polynom in q mit Koeffizienten in $\mathbb{N}_0$. Das Polynom hat Grad $k(n-k)$.

Beispiel Für $k = 3$, $n = 5$ erhält man das Polynom:

$$q^6+q^5+q^4+q^4+q^3+q^2+q^3+q^2+q+1 = q^6+q^5+2q^4+2q^3+2q^2+q+1\,.$$

Probe:

$$\binom{5}{3}_q = \frac{(q^5-1)(q^4-1)(q^3-1)}{(q^3-1)(q^2-1)(q-1)} = (q^4+q^3+q^2+q+1)(q^2+1)\,.$$

[5] Sterne $\Leftrightarrow$ Young-Diagramm. Man ignoriert Spalten mit führenden Einsen und führende Nullspalten.

5 Geordnete Mengen

5.1 Definition Eine (*partielle*) *Ordnung* ist eine Relation $\leq$ auf einer Menge X mit folgenden Eigenschaften:

(i) (Reflexivität) $x \in X \Longrightarrow x \leq x$,

(ii) (Antisymmetrie) $x, y \in X$ mit $x \leq y$ und $y \leq x \Longrightarrow x = y$,

(iii) (Transitivität) $x, y, z \in X$ mit $x \leq y$ und $y \leq z \Longrightarrow x \leq z$.

Ggf. heißt das Paar $(X, \leq)$ (partiell) *geordnete Menge*.[6] Ist die Ordnung $\leq$ aus dem Zusammenhang klar, so sagt man: X ist eine geordnete Menge. Statt $x \leq y$ schreibt man auch $y \geq x$. Ist $x \leq y$ und $x \neq y$ schreibt man auch $x < y$ bzw. $y > x$.

Beispiel

(a) $\mathbb{R}$ mit der üblichen Ordnung $\leq$.

(b) Die Potenzmenge $\mathfrak{P}(M)$ einer Menge M mit der Inklusion $\subseteq$.

(c) $\mathbb{N}$ mit Teilbarkeit $|$.

(d) Für jede geordnete Menge $(X, \leq)$ hat man die *entgegengesetzt* geordnete Menge $(X, \geq) = (X, \leq)^o = X^o$.[7]

(e) Für geordnete Mengen X, Y sieht man die *disjunkte Vereinigung* folgendermaßen als geordnete Menge an:

$$x \leq y \text{ in } X \dot{\cup} Y \Longleftrightarrow (x, y \in X \text{ und } x \leq y \text{ in } X) \text{ oder } (x, y \in Y \text{ und } x \leq y \text{ in } Y)\,.$$

(f) Für geordnete Mengen X, Y sieht man das *direkte Produkt* $X \times Y$ folgendermaßen als geordnete Mengen an:

$$(x, y) \leq (x', y') \Longleftrightarrow x \leq x' \text{ und } y \leq y'\,.$$

(g) Jede Teilmenge Y einer geordneten Menge X wird selbst zu einer geordneten Menge, indem man die Ordnung entsprechend einschränkt. Beispielsweise bilden die Untervektorräume eines Vektorraums auch eine geordnete Menge bzgl. "$\subseteq$".

Bemerkung Die folgenden Teilmengen einer geordneten Menge X heißen *Intervalle*:

- $[x, y] \coloneqq \{z \in X : x \leq z \leq y\}$,
- $[x, y[\coloneqq \{z \in X : x \leq z < y\}$,
- $]x, y] \coloneqq \{z \in X : x < z \leq y\}$,
- $]x, y[\coloneqq \{z \in X : x < z < y\}$,

[6] engl.: *poset = partially ordered set.*
[7] engl.: *o = opposite poset.*

- $X_{\geq x} \coloneqq \{z \in X : z \geq x\}$,
- $X_{>x} \coloneqq \{z \in X : z > x\}$,
- $X_{\leq x} \coloneqq \{z \in X : z \leq x\}$,
- $X_{<x} \coloneqq \{z \in X : z < x\}$

für $x, y \in X$ beliebig. Eine geordnete Menge X heißt *lokal endlich*, falls $[x, y]$ endlich ist für alle $x, y \in X$.

5.2 Definition Elemente x, y in einer geordneten Menge X heißen *vergleichbar*, falls $x \leq y$ oder $y \leq x$ gilt. Sind je zwei Elemente in X vergleichbar, dann heißt X *total geordnet*. Eine total geordnete Teilmenge Y einer (partiell) geordneten Menge X heißt *Kette*[8] in X. Ggf. heißt

$$l(Y) \coloneqq |Y| - 1 \text{ } \textit{Länge} \text{ von } Y\,.$$

Im Fall $Y = \{y_1, \ldots, y_n\}$ mit $y_1 < \ldots < y_n$ spricht man von einer *Kette von* y_1 *nach* y_n. Man schreibt:

$$Y : y_1 < \ldots < y_n\,.$$

Eine Teilmenge Y einer geordneten Menge X heißt *Antikette*[9], falls je zwei verschiedene Elemente in Y unvergleichbar sind.

Bemerkung Seien x, y Elemente in einer geordneten Menge X. Wir schreiben $x \sim y$, falls Elemente $x_0 = x, x_1, \ldots, x_n = y$ existieren derart, dass x_{i-1} und x_i $(i = 1, \ldots, n)$ vergleichbar sind. Dann ist $\sim$ eine Äquivalenzrelation auf X, deren Äquivalenzklassen *Zusammenhangskomponenten* heißen.

5.3 Definition Sei X eine geordnete Menge und $m \in X$.

(i) m heißt *maximal* in X, falls kein $x \in X$ existiert mit $m < x$. Analog heißt m *minimal*, falls kein $x \in X$ existiert mit $x < m$.

(ii) Man nennt m *das Maximum* von X und schreibt $m = \max X$, falls $x \leq m$ für alle $x \in X$ gilt. Analog heißt m *das Minimum* von X, falls $m \leq x$ für alle $x \in X$ gilt. Man schreibt: $m = \min X$.

(iii) Ist $Y \subseteq X$ und existiert

$$s \coloneqq \min\{x \in X : y \leq x \text{ für alle } y \in Y\}\,,$$

so nennt man s *Supremum* von Y und schreibt $s = \sup Y$. Existiert

$$i \coloneqq \max\{x \in X : x \leq y \text{ für alle } y \in Y\}\,,$$

so nennt man i *Infimum* von Y und schreibt $i = \inf Y$.

(iv) Für $a, b, \in X$ setzt man $a \vee b \coloneqq \sup\{a, b\}$ und $a \wedge b \coloneqq \inf\{a, b\}$.

[8] engl.: *chain.*
[9] engl.: *antichain.*

(v) X heißt *Verband*[10], falls $a \vee b$ und $a \wedge b$ in X für alle $a, b \in X$ existieren.

5.4 Definition Eine Abbildung $f\colon X \to Y$ zwischen geordneten Mengen X und Y heißt *monoton*[11] (bzw. *antiton*), falls $f(x) \leq f(x')$ (bzw. $f(x) \geq f(x')$) für alle $x, x' \in X$ mit $x \leq x'$ gilt.

Bemerkung Offenbar ist die Identitätsabbildung $\mathrm{id}_X\colon X \to X, x \mapsto x$ monoton. Für montone Abbildungen $f\colon X \to Y$, $g\colon Y \to Z$ zwischen geordneten Mengen X, Y, Z ist auch die Komposition $g \circ f$ monoton. Antitone Abbildungen $f\colon X \to Y$ kann man auch als monotone Abbildungen $f\colon X \to Y^o$ bzw. $f\colon X^o \to Y$ auffassen. Für bijektive monotone Abbildungen $f\colon X \to Y$ ist die Umkehrabbildung $f^{-1}\colon Y \to X$ i.A. *nicht* monoton.

Beispiel

$$\mathrm{id}_{\mathbb{N}}\colon (\mathbb{N}, |) \to (\mathbb{N}, \leq), n \mapsto n$$

ist monoton, aber die Umkehrabbildung

$$\mathrm{id}_{\mathbb{N}}\colon (\mathbb{N}, \leq) \to (\mathbb{N}, |)$$

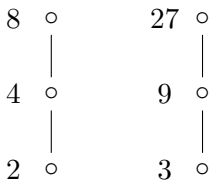
ist *nicht* monoton.

5.5 Definition Eine Abbildung $f\colon X \to Y$ zwischen geordneten Mengen X, Y heißt *Isomorphismus* (geordneter Mengen), falls f bijektiv ist und f, f^{-1} monoton sind.

Bemerkung Ggf. ist auch $f^{-1} : Y \to X$ ein Isomorphismus. Man nennt X, Y isomorph und schreibt $X \cong Y$. Wie üblich ist $\cong$ eine Äquivalenzrelation.

Beispiel In $(\mathbb{N}, |)$ gilt:

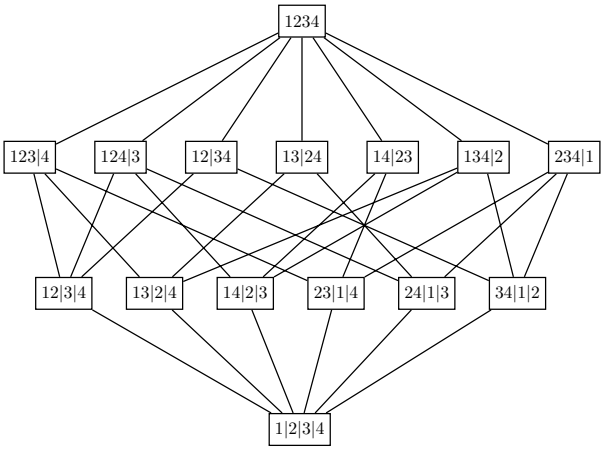
$$[2, 8] = \{2, 4, 8\} \cong \{3, 9, 27\} = [3, 27]$$



5.6 Bemerkung Sei M eine Menge und $\mathcal{P}(M)$ die Menge aller Partitionen von M. Für $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}(M)$ schreibt man $\mathfrak{p} \leq \mathfrak{q}$, falls jeder Block von $\mathfrak{p}$ in einem Block von $\mathfrak{q}$ enthalten ist. Dann ist $(\mathcal{P}(M), \leq)$ eine geordnete Menge.

Beispiel Wir bestimmmen $\leq$ auf $\mathcal{P}(M)$ für $M = \{1, 2, 3, 4\}$.

[10] engl.: *lattice*.
[11] d.h. "ordnungserhaltend".



5.7 Bemerkung Sei $n \in \mathbb{N}$ und $P(n)$ die Menge aller Partitionen von n. Für

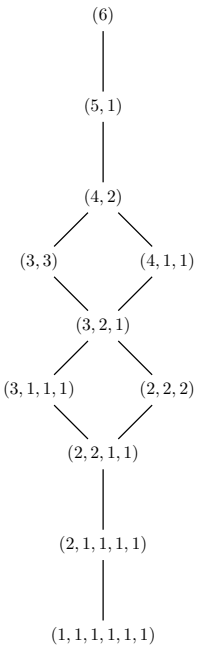
$$\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n, \mu = (\mu_1, \ldots, \mu_l) \vdash n$$

schreibt man:

$$\begin{aligned} \lambda \trianglelefteq \mu :\Longleftrightarrow & \lambda_1 \leq \mu_1 \,, \\ & \lambda_1 + \lambda_2 \leq \mu_1 + \mu_2 \,, \\ & \lambda_1 + \lambda_2 + \lambda_3 \leq \mu_1 + \mu_2 + \mu_3 \,, \\ & \vdots \end{aligned}$$

So wird $P(n)$ zu einer geordneten Menge. Man nennt $\trianglelefteq$ die *Dominanzordnung* auf $P(n)$.

Beispiel $n = 6$



6 Inzidenzalgebra und Möbius-Inversion

6.1 Bemerkung Sei X eine lokal endliche geordnete Menge. Dann ist die Menge $\mathrm{Abb}(X \times X, \mathbb{R})$ aller Abbildungen $f\colon X \times X \to \mathbb{R}$ ein $\mathbb{R}$-Vektorraum mit

$$\left.\begin{aligned}(f+g)(x,y) &= f(x,y) + g(x,y)\\ (rf)(x,y) &= rf(x,y)\end{aligned}\right\} \qquad \begin{aligned}(f,g \in \mathrm{Abb}(X\times X,\mathbb{R}))\\ (x,y \in X, r \in \mathbb{R})\end{aligned}$$

Offenbar ist $I(X) \coloneqq \{f \in \mathrm{Abb}(X \times X, \mathbb{R}) : f(x,y) \neq 0 \Longrightarrow x \leq y\} \subseteq \mathrm{Abb}(X \times X, \mathbb{R})$ ein Untervektorraum. Wir definieren eine Multiplikation auf $I(X)$ durch

$$(fg)(x,y) \coloneqq \sum_{z \in [x,y]} f(x,z)g(z,y) \quad (f,g \in I(X),\, x,y \in X)\,.$$

Die Summe ist endlich, da X lokal endlich ist. Man rechnet leicht nach, dass für $f,g,h \in I(X)$, $r \in \mathbb{R}$ gilt:

- $(fg)h = f(gh)$ (Assoziativitätsgesetz),
- $f(g+h) = fg + fh$ (Distributivgesetz),
- $(f+g)h = fh + gh$ (Distributivgesetz),
- $r(fg) = (rf)g = f(rg)$.

Definiert man $\delta_X\colon X \times X \to \mathbb{R}$ durch $\delta_X(x,x) \coloneqq 1$ für $x \in X$ und $\delta_X(x,y) \coloneqq 0$ für $x \neq y$, so gilt für alle $f \in I(X)$: $\delta_X f = f = f\delta_X$. δ_X heißt *Kronecker-Funktion* und $I(X)$ heißt *Inzidenzalgebra*. Weitere wichtige Funktionen in $I(X)$ sind die *Zeta-Funktion* ζ_X und die *Kettenfunktion* η_X. Diese sind definiert durch:

$$\zeta_X(x,y) \coloneqq \begin{cases}1, & x \leq y\\ 0, & \text{sonst}\end{cases} \qquad \eta_X(x,y) \coloneqq \begin{cases}1, & x < y\\ 0, & \text{sonst}\end{cases}$$

Offenbar ist $\zeta_X = \delta_X + \eta_X$ und für $x,y \in X$ gilt:

$$\zeta_X^2(x,y) = \sum_{z \in [x,y]} \zeta_X(x,z)\zeta_X(z,y) = \sum_{z \in [x,y]} 1 = |[x,y]|\,.$$

6.1 Satz *Sei X eine lokal endliche Menge. Für $x,y \in X$ und $m \in \mathbb{N}$ ist dann $\eta_X^m(x,y)$ die Anzahl der Ketten der Länge n von x nach y in X.*

Beweis. Nach Definition ist

$$\eta_X^2(x,y) = \sum_{z \in [x,y]} \eta_X(x,z)\,\eta_X(z,y) = \sum_{x<z<y} 1\,.$$

Induktiv folgt:

$$\eta_X^n(x,y) = \sum_{x=x_1<\ldots<x_n=y} 1\,.$$

□

6.2 Satz *Sei X eine lokal endliche geordnete Menge und $f \in I(X)$. Dann sind äquivalent:*

(i) $\exists g \in I(X) : fg = \delta_X$,

(ii) $f(x,x) \neq 0$ *für alle* $x \in X$,

(iii) $\exists h \in I(X) : hf = \delta_X$.

Ggf. gilt: $g = h$.

Beweis.

(1) $\Rightarrow$ (2) Sei $g \in I(X)$ mit $fg = \delta_X$. Für $x \in X$ ist dann

$$1 = \delta_X(x,x) = \sum_{z \in [x,x]} f(x,z)g(z,x) = f(x,x)g(x,x), \text{ d.h. } f(x,x) \neq 0\,.$$

(2) $\Rightarrow$ (1) Sei $f(x,x) \neq 0$ für alle $x \in X$. Wir suchen ein $g \in I(X)$ mit $fg = \delta_X$, d.h.

- $g(x,y) = 0$, falls $x \not\leq y$,
- $1 = f(x,x)g(x,x)$ für alle $x \in X$,
- $0 = \sum\limits_{x \leq z \leq y} f(x,z)g(z,y)$, falls $x < y$.

Die zweite Bedingung bedeutet: $g(x,x) = \dfrac{1}{f(x,x)}$ und die dritte Bedingung bedeutet:

$$f(x,x)g(x,y) = -\sum_{x < z \leq y} f(x,z)g(z,y), \text{ d.h. } g(x,y) = \frac{-1}{f(x,x)} \sum_{x < z \leq y} f(x,z)g(z,y)\,.$$

So kann man $g(x,y)$ mit Induktion nach $|[x,y]|$ definieren.

(2) $\Leftrightarrow$ (3) analog.

Ferner: $h = h\delta_X = h(fg) = (hf)g = \delta_X g = g$. □

Bemerkung Bezeichnung: $g = h = f^{-1}$ heißt die zu f *inverse* Funktion.

6.2 Beispiel Wegen $\zeta_X(x,x) = 1$ für alle $x \in X$ hat ζ_X eine inverse Funktion $\zeta_X^{-1} =: \mu_X$, die *Möbius-Funktion* von X. Nach dem obigen Beweis ist $\mu_X(x,x) = 1$ für alle $x \in X$ und

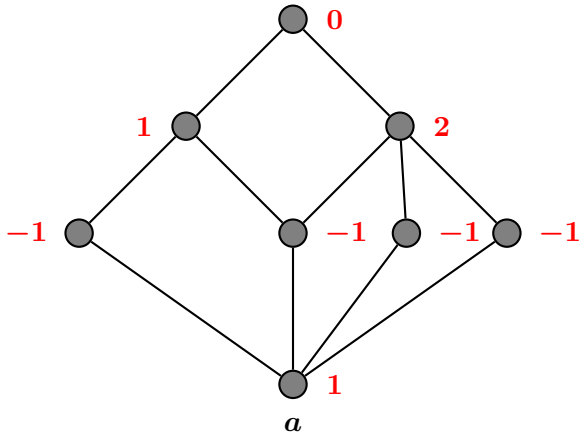
$$\mu_x(x,y) = -\sum_{x < z \leq y} \mu_X(z,y), \text{ d.h. } \boxed{\sum_{z \in [x,y]} \mu_X(z,y) = 0} \quad (\text{falls } x < y).$$

Analog erhält man aus (2) $\Leftrightarrow$ (3):

$$\mu_X(x,y) = -\sum_{x \leq z < y} \mu_X(x,z), \text{ d.h. } \boxed{\sum_{z \in [x,y]} \mu_X(x,z) = 0} \quad (\text{für } x < y).$$

Offenbar ist $\mu_X(x,y) = \mu_{[x,y]}(x,y)$ für alle $x, y \in X$, d.h. $\mu_X(x,y)$ hängt nur von dem Intervall $[x,y]$ ab.

6.3 Beispiel Wir betrachten $\mu_X(a,\cdot)$.



6.3 Satz (Möbius-Inversion) *Sei X eine lokal endliche geordnete Menge. Für $x \in X$ sei $X_{\leq x}$ endlich. Dann sind für $f, F\colon X \to \mathbb{R}$ äquivalent:*

(1) $F(y) = \sum_{x \leq y} f(x)$ *für alle* $y \in X$

(2) $f(y) = \sum_{x \leq y} \mu_X(x,y) F(x)$ *für alle* $y \in X$.

Beweis.

(1) $\Rightarrow$ (2) Sei (1) erfüllt. Für $z \in X$ gilt dann nach Beispiel 6.2:

$$\begin{aligned}\sum_{x \leq z} \mu_X(x,z) F(x) &= \sum_{w \leq x \leq z} \mu_X(x,z) f(w) \\ &= \sum_{w \leq z} f(w) \underbrace{\sum_{x \in [w,z]} \mu_X(x,z)}_{=0 \text{ für } w \neq z} \\ &= f(z)\mu_X(z,z) \\ &= f(z)\,.\end{aligned}$$

(2) $\Rightarrow$ (1) Sei (2) erfüllt. Für $z \in X$ gilt dann nach Beispiel 6.2:

$$\begin{aligned}\sum_{x \le z} f(x) &= \sum_{w \le x \le z} \mu_X(w,x) F(w) \\ &= \sum_{w \le z} F(w) \underbrace{\sum_{x \in [w,z]} \mu_X(w,x)}_{=0 \text{ für } w \neq z} \\ &= F(z)\mu_X(z,z) \\ &= F(z)\,.\end{aligned}$$

□

Bemerkung Satz 6.3 hat formale Ähnlichkeit mit dem Hauptsatz der Differential- und Integralrechnung. $F \leftrightarrow$ Integral von f, $f \leftrightarrow$ Ableitung von F.

6.4 Bemerkung Sei $f\colon X \to Y$ ein Isomorphismus zwischen zwei lokal endlichen geordneten Mengen X, Y. Für $a, b \in X$ gilt dann: $\mu_X(a,b) = \mu_Y(f(a), f(b))$.

Satz *Seien X, Y lokal endliche geordnete Mengen. Dann ist $X \times Y$ als geordnete Menge lokal endlich und für $x, x' \in X$, $y, y' \in Y$ gilt:*

$$\mu_{X\times Y}\big((x,y),(x',y')\big) = \mu_X(x,x')\,\mu_Y(y,y')\,.$$

Beweis. Die erste Aussage ist klar: $[(x,y),(x',y')] = [x,x'] \times [y,y']$. Die Formel beweisen wir mit Induktion nach der Länge des Intervalls $n = |[(x,y),(x',y')]| = |[x,x']| \cdot |[y,y']|$. Im Fall $n = 0$ ist $[x,x'] = \emptyset$ oder $[y,y'] = \emptyset$, d.h. $x \not\le x'$ oder $y \not\le y'$. Dann ist auch $(x,y) \not\le (x',y')$ und somit sind beide Seiten der Formel 0. Im Fall $n = 1$ ist dann $x = x'$, $y = y'$ und auf beiden Seiten der Formel steht 1. Sei jetzt $n > 1$, d.h. $(x,y) < (x',y')$. Dann: $x < x'$ oder $y < y'$. Nach Beispiel 6.2 und Induktion gilt:

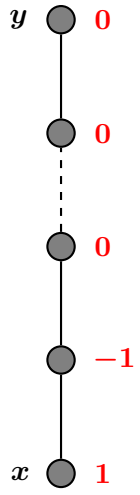
$$\begin{aligned}\mu_{X\times Y}\big((x,y),(x',y')\big) &= -\sum_{(a,b)\in[(x,y),(x',y')[} \underbrace{\mu_{X\times Y}\left((x,y),(a,b)\right)}_{\overset{\text{Ind.}}{=}\mu_X(x,a)\mu_Y(y,b)} \\ &= \mu_X(x,x')\,\mu_Y(y,y') - \sum_{(a,b)\in\underbrace{[(x,y),(x',y')]}_{[x,x']\times[y,y']}} \mu_X(x,a)\mu_Y(y,b) \\ &= \mu_X(x,x')\,\mu_Y(y,y') - \underbrace{\left(\sum_{a\in[x,x']}\mu_X(x,a)\right)\left(\sum_{b\in[y,y']}\mu_Y(y,b)\right)}_{\text{einer der beiden Faktoren ist Null}} \\ &= \mu_X(x,x')\,\mu_Y(y,y')\,.\end{aligned}$$

□

6.4 Beispiel (a) Sei $X = \mathbb{N}$ mit der gewöhnlichen Ordnung $\leq$. Nach Beispiel 6.2 gilt dann:

$$\mu_{\mathbb{N}}(x,y) = \begin{cases} 1, & \text{falls } y = x \\ -1, & \text{falls } y = x+1 \\ 0, & \text{falls } y > x+1 \end{cases}$$

Analog gilt für die Werte $\mu_X(x,\cdot)$ der Möbius-Funktion in einem total geordneten Intervall einer lokal endlichen geordneten Menge X:



$\boldsymbol{\mu_X(x,\cdot)}$

(b) Sei $X = \mathbb{N}$ mit der Teilbarkeit $\mid$ als Ordnung und seien $x, y \in \mathbb{N}$. Im Fall $x \nmid y$ ist $\mu_X(x,y) = 0$. Sei also $x \mid y$ und $\frac{y}{x} = p_1^{r_1} \dots p_k^{r_k}$ mit $r_1, \dots, r_k \in \mathbb{N}$ und paarweise verschiedenen Primzahlen $p_1, \dots, p_k$. Dann:

$$[x,y] \cong \left[1, \frac{y}{x}\right] \cong \bigtimes_{i=1}^{k} \{0, \dots, r_i\}\,.$$

Daher:

$$\mu_X(x,y) = \mu_X(1, \frac{y}{x}) = \prod_{i=1}^{k} \mu_{\{0,1,\dots,r_i\}}(0, r_i) \overset{\text{(a)}}{=} \begin{cases} (-1)^k, & \text{falls } r_i = 1 \text{ für } i = 1, \dots, k \\ 0, & \text{sonst} \end{cases}$$

Dies ist das klassische Beispiel einer Möbius-Funktion.

(c) Sei $X = \mathfrak{P}(M)$ für eine endliche Menge M mit der Inklusion $\subseteq$ als Ordnung. Dann gilt für $A \subseteq B \subseteq M$:

$$[A,B] \cong [\emptyset, B \setminus A] \cong \prod_{b \in B \setminus A} \{0,1\}\,.$$

Daher:

$$\mu_X(A,B) = \prod_{b \in B \setminus A} \mu_{\{0,1\}}(0,1) = (-1)^{|B \setminus A|}$$

6.5 Satz *Sei X eine lokal endliche geordnete Menge. Für $x, y \in X$ ist dann $\mu_X(x,y)$ die Differenz aus der Anzahl der Ketten gerader Länge von x nach y in X und der Anzahl der Ketten ungerader Länge von x nach y in X.*

Beweis. Wir definieren $\nu_X \in I(X)$ durch

$$\nu_X(x,y) = \sum_{k=0}^{\infty} (-1)^k \eta^k(x,y)\,.$$

Die Summe ist nach Satz 6.1 endlich, da $[x,y]$ endlich ist. Nach Satz 6.1 ist zu zeigen: $\mu_X = \nu_X$, d.h. $\zeta_X \nu_X = \delta_X$. Dazu seien $x, y \in X$ und sei $N \in \mathbb{N}$ mit $N > |[x,y]|$ Dann:

$$\begin{aligned}
(\zeta_X\, \nu_X)\,(x,y) &= \sum_{z \in [x,y]} \zeta_X(x,z)\nu_X(z,y) \\
&= \sum_{z \in [x,y]} \zeta_X(x,z) \sum_{k=0}^{N} (-1)^k \eta^k(z,y) \\
&= \left((\delta_X + \eta_X) \sum_{k=0}^{N} (-1)^k \eta^k \right)(x,y) \\
&= \left(\delta_X + (-1)^N \eta^{N+1}\right)(x,y) \\
&= \delta_X(x,y)\,.
\end{aligned}$$

□

Literatur: E. Spiegel, C.J. O'Donnell, Incidence algebras, Marcel Dekker, New York 1997

6.6 Bemerkung Sei L ein endlicher Verband. Für $x, y \in L$ existieren dann

$$x \wedge y = \inf\{x,y\} \text{ und } x \vee y = \sup\{x,y\}\,.$$

Induktiv folgt die Existenz von $\inf(M)$ und $\sup(M)$ für $\emptyset \neq M \subseteq L$. Insbesondere existieren $0_L \coloneqq \inf(L)$ und $1_L \coloneqq \sup(L)$.

Satz (Weisner) *Sei L ein endlicher Verband und sei $0_L < a \in L$, dann gilt:*

$$\sum_{\substack{x \in L \\ x \vee a = 1_L}} \mu_L(0_L, x) = 0\,.$$

Beweis. Betrachte

$$\begin{aligned} S &\coloneqq \sum_{\substack{x,y\in L\\ y\geq x,\, y\geq a}} \mu_L(0_L,x)\,\mu_L(y,1_L) \\ &= \sum_{\substack{x,y\in L\\ y\geq x\vee a}} \mu_L(0_L,x)\,\mu_L(y,1_L) \\ &= \sum_{x\in L} \mu_L(0_L,x) \underbrace{\sum_{y\in[x\vee a,1_L]} \mu_L(y,1_L)}_{=0,\text{ falls } x\vee a\neq 1_L} \\ &= \sum_{\substack{x\in L\\ x\vee a=1_L}} \mu_L(0_L,x)\,. \end{aligned}$$

Andererseits:

$$S = \sum_{\substack{y\in L\\ y\geq a}} \mu_L(y,1_L) \underbrace{\sum_{x\in[0_L,y]} \mu_L(0_L,x)}_{=0 \text{ für } y\neq 0_L} = \sum_{\substack{y\in L\\ y\geq a\\ y=0_L}} \mu_L(y,1_L) = 0\,.$$

□

6.7 Satz *Sei $\mathbb{K}$ ein endlicher Körper mit $q \coloneqq |\mathbb{K}| < \infty$, sei V ein $\mathbb{K}$-Vektorraum der Dimension $n < \infty$ und es sei $\mathfrak{U} \coloneqq \mathfrak{U}(V)$ die Menge aller Untervektorräume von V, geordnet durch "$\subseteq$". Dann gilt: $\mu_{\mathfrak{U}}(0,V) = (-1)^n q^{\binom{n}{2}}$.*

Beweis. (Induktion nach n) $\mathfrak{U}$ ist ein Verband mit $U \vee U' = U + U'$ und $U \wedge U' = U \cap U'$. Im Fall $n = 0$ (d.h. $V = \{0\}$) ist $\mu_{\mathfrak{U}}(0,V) = \mu_{\mathfrak{U}}(0,0) = 1 = (-1)^0 q^{\binom{0}{2}}$. Sei also $n > 0$, $W \subseteq V$ ein eindimensionaler Untervektorraum und $W' \subseteq V$ ein Untervektorraum mit $V = W \oplus W'$. Nach Weisner gilt:

$$\mu_{\mathfrak{U}}(0,V) = -\sum_{\substack{V\neq U\in\mathfrak{U}(V)\\ U+W=V}} \mu_{\mathfrak{U}}(0,U)\,.$$

Für $V \neq U \in \mathfrak{U}$ gilt dabei:

$$U + W = V \Leftrightarrow \dim U = n-1 \text{ und } W \not\subseteq U$$

Daher gilt nach Induktion:

$$\begin{aligned}
\mu_{\mathfrak{U}}(0,V) &= -\sum_{\substack{V\neq U\in\mathfrak{U}\\ U+W=V}} (-1)^{n-1} q^{\binom{n-1}{2}} \\
&= (-1)^n q^{\binom{n-1}{2}} |\{U\in\mathfrak{U} : V\neq U, U+W=V\}| \\
&= (-1)^n q^{\binom{n-1}{2}} |\{U\in\mathfrak{U} : \dim U = n-1, W\not\subseteq U\}| \\
&= (-1)^n q^{\binom{n-1}{2}} \left(\binom{n}{n-1}_q - |\{U\in\mathfrak{U} : \dim U = n-1, W\subseteq U\}| \right) \\
&= (-1)^n q^{\binom{n-1}{2}} \left(\binom{n}{n-1}_q - \binom{n-1}{n-2}_q \right),
\end{aligned}$$

denn wir haben eine Bijektion

$$\{U'\in\mathfrak{U}(W') : \dim U' = n-2\} \to \{U\in\mathfrak{U}(V) : \dim U = n-1,\, W\subseteq U\}, U'\mapsto U'+W\,.$$

Also:

$$\begin{aligned}
\mu_{\mathfrak{U}}(0,V) &= (-1)^n q^{\binom{n-1}{2}} \Bigg(\underbrace{\binom{n}{n-1}_q}_{\binom{n}{1}_q} - \underbrace{\binom{n-1}{n-2}_q}_{\binom{n-1}{1}_q} \Bigg) \\
&= (-1)^n q^{\binom{n-1}{2}} \left(\frac{q^n-1}{q-1} - \frac{q^{n-1}-1}{q-1} \right) \\
&= (-1)^n q^{\binom{n-1}{2}} q^{n-1} \\
&= (-1)^n q^{\binom{n}{2}}\,.
\end{aligned}$$

□

6.7 Bemerkung Für $U\in\mathfrak{U}(V)$ und $r := \dim U$ folgt leicht:

$$\boxed{\mu_{\mathfrak{U}}(U,V) = (-1)^{n-r} q^{\binom{n-r}{2}}}\,.$$

Denn ist $U'\subseteq V$ ein Untervektorraum mit $U\oplus U' = V$, so ist $\dim U' = n-r$ und $[U,V]\cong[0,U']$.

6.8 Satz *Sei $\mathbb{K}$ ein Körper mit $q := |\mathbb{K}| < \infty$. Für $m,n\in\mathbb{N}$ ist die Anzahl der surjektiven linearen Abbildungen $\mathbb{K}^n\to\mathbb{K}^m$ gleich:*

$$\sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k}_q q^{nk+\binom{m-k}{2}}\,.$$

Beweis. Für jeden Untervektorraum $U\subseteq\mathbb{K}^m$ sei $f(U)$ die Anzahl der linearen Abbildungen $\alpha\colon \mathbb{K}^n\to\mathbb{K}^m$ mit Bild U. Analog sei $F(U)$ die Anzahl aller linearen Abbildungen $\mathbb{K}^n\to U$. Dann:

$$F(U) = \sum_{W\in\mathfrak{U}(U)} f(W)\,.$$

Möbius-Inversion auf $\mathfrak{U}(\mathbb{K}^m)$ liefert für jeden Untervektorraum $U \subseteq \mathbb{K}^m$ der Dimension r:

$$\begin{aligned} f(U) &= \sum_{W \in \mathfrak{U}(U)} \mu(W,U) F(W) \\ &= \sum_{W \in \mathfrak{U}(U)} \mu(W,U) q^{n \dim W} \\ &\overset{6.7}{=} \sum_{W \in \mathfrak{U}(U)} (-1)^{\dim U - \dim W} q^{\binom{dim U - dim W}{2}} q^{n \dim W} \\ &= \sum_{k=0}^{r} (-1)^{r-k} \binom{r}{k}_q q^{\binom{r-k}{2}} q^{nk} \,. \end{aligned}$$

Setze $U = \mathbb{K}^m$. Es folgt die Behauptung. □

Bemerkung Man kann die Anzahl der surjektiven Abbildungen $\mathbb{K}^n \to \mathbb{K}^m$ auch anders berechnen. Bekanntlich stehen die surjektiven linearen Abbildungen $\mathbb{K}^n \to \mathbb{K}^m$ in Bijektion mit den Matrizen vom Rang m in $\mathbb{K}^{m \times n}$. Deren Anzahl ist nach Satz 2.1 gleich $(q^n - 1)(q^n - q) \dots (q^n - q^{n-m+1})$. Wir erhalten die Identität:

$$\sum_{k=0}^{n} (-1)^{m-k} \binom{m}{k}_q q^{mk + \binom{m-k}{2}} = (q^n - 1)(q^n - q) \dots (q^n - q^{n-m+1}) \,.$$

6.9 Bemerkung Für jede endliche Menge M ist die Menge $\mathcal{P}(M)$ aller Partitionen von M ein Verband.

Beispiel

$$\begin{aligned} &M = \{1, \dots, 10\}, \\ &\mathfrak{p} = \{\{1,2,3\}, \{4,5\}, \{6\}, \{7\}, \{8,9,10\}\} \,, \\ &\mathfrak{q} = \{\{1\}, \{6\}, \{2,5\}, \{3,4\}, \{7,10\}, \{8,9\}\} \,, \\ &\mathfrak{p} \wedge \mathfrak{q} = \{\{1\}, \{3\}, \{6\}, \{7\}, \{8,9\}, \{10\}, \{2\}, \{5\}, \{4\}\} \\ &\mathfrak{p} \vee \mathfrak{q} = \{\{1,2,3,5,4\}, \{6\}, \{7,8,9,10\}\} \\ &1_{\mathcal{P}(M)} = \{\{1,2,3,4,5,6,7,8,9,10\}\} \\ &0_{\mathcal{P}(M)} = \{\{1\}, \dots, \{10\}\} \end{aligned}$$

Satz *Sei $M = \{1, \dots, n\}$ und seien $\mathfrak{a}, \mathfrak{b} \in \mathcal{P}(M)$ mit $\mathfrak{a} \leq \mathfrak{b}$. Für jeden Block $B \in \mathfrak{b}$ sei n_B die Anzahl der Blöcke $A \in \mathfrak{a}$ mit $A \subseteq B$. Dann gilt:*

$$\mu_{\mathcal{P}(M)}(\mathfrak{a}, \mathfrak{b}) = (-1)^{|\mathfrak{a}| - |\mathfrak{b}|} \prod_{B \in \mathfrak{b}} (n_B - 1)! \,.$$

Beweis. Sei $\mathfrak{b} = \{B_1, \dots, B_r\}$. Jeder Block B_i ist Vereinigung von $n_{B_i} =: n_i$ Blöcken von $\mathfrak{a}$. Das Intervall $[\mathfrak{a}, \mathfrak{b}]$ ist als geordnete Menge isomorph zu $\mathcal{P}(N_1) \times \mathcal{P}(N_2) \times \dots \times \mathcal{P}(N_r)$

mit $N_i = \{1, \dots, n_i\}$. Daher $\mu_{\mathcal{P}(M)}(\mathfrak{a}, \mathfrak{b}) = \mu_{\mathcal{P}(N_1)}(0,1) \times \mu_{\mathcal{P}(N_2)}(0,1) \times \dots \times \mu_{\mathcal{P}(N_r)}(0,1)$. Also genügt es zu zeigen: $\mu_{\mathcal{P}(M)}(0,1) = (-1)^{n-1}(n-1)!$, denn dann ist

$$\begin{aligned}\mu_{\mathcal{P}(M)}(\mathfrak{a}, \mathfrak{b}) &= (-1)^{n_1-1}(n_1-1)! \dots (-1)^{n_r-1}(n_r-1)! \\ &= (-1)^{n_1+\dots+n_r-r} \prod_{i=1}^{r} (n_i-1)! \\ &= (-1)^{|\mathfrak{a}|-|\mathfrak{b}|} \prod_{B \in \mathfrak{b}} (n_B-1)! \,.\end{aligned}$$

Zum Beweis von $\mu_{\mathcal{P}(M)}(0,1) = (-1)^{n-1}(n-1)!$ wählen wir

$$\mathfrak{p} \coloneqq \{\{1,2\}, \{3\}, \dots, \{n\}\} \in \mathcal{P}(M) \,.$$

Wir suchen dann die Partition $\mathfrak{q}$ von M mit $\mathfrak{p} \vee \mathfrak{q} = \{M\}$. Von $\{M\}$ abgesehen sind das genau die Partitionen $\mathfrak{q} = \{\{1, \dots\}, \{2, \dots\}\}$. Nach Weisner gilt:

$$\mu_{\mathcal{P}(M)}(0,1) = -\sum_{\mathfrak{q}=\{\{1,\dots\},\{2,\dots\}\}} \mu_{\mathcal{P}(M)}(0, \mathfrak{q}) \,.$$

Es gibt genau 2^{n-2} solcher $\mathfrak{q}$'s. Bei $\binom{n-2}{i}$ von diesen hat der Block, der 1 enthält, gerade $i+1$ Elemente. Argumentiert man mit Induktion nach n, so kann man voraussetzen: $\mu_{\mathcal{P}(M)}(0, \mathfrak{q}) = (-1)^i \, i! (-1)^{n-i-2}(n-i-2)!$. Also:

$$\begin{aligned}\mu_{\mathcal{P}(M)}(0,1) &= -\sum_{i=0}^{n-2} \binom{n-2}{i} (-1)^i \, i! \, (-1)^{n-i-2}(n-i-2)! \\ &= (-1)^{n-1} \sum_{i=0}^{n-2} \binom{n-2}{i} i! \, (n-i-2)! \\ &= (-1)^{n-1} \underbrace{\sum_{i=0}^{n-2} (n-2)!}_{(n-1)!} \,. \qquad \square\end{aligned}$$

7 Anwendungen der Möbius-Inversion

7.1 Satz *Für Abbildungen $f, F\colon \mathbb{N} \to \mathbb{R}$ sind äquivalent:*

(1) $F(n) = \sum_{d|n} f(d)$ *für* $n \in \mathbb{N}$

(2) $f(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$ *für* $n \in \mathbb{N}$.

Dabei durchläuft d alle (positiven) Teiler von n.

Beweis. $\mathbb{N}$ ist durch $|$ geordnet. Nach Satz 6.3 sind äquivalent:

(i) $F(y) = \sum_{x|y} f(x)$ für $y \in \mathbb{N}$

(ii) $f(y) = \sum_{x|y} \mu_{\mathbb{N}}(x, y) F(x)$ für $y \in \mathbb{N}$.

Nach Beispiel 6.4 gilt dabei: $\mu_{\mathbb{N}}(x, y) = \mu(\frac{y}{x})$ mit der klassischen Möbius-Funktion aus Definition 3.7. □

7.2 Bemerkung Sei $\mathbb{K}$ ein Körper mit $q := |\mathbb{K}| < \infty$. Wir betrachten für ein $n \in \mathbb{N}$ die q^n Polynome der Form

$$X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \qquad (a_0, \ldots, a_{n-1} \in \mathbb{K}\,.)$$

Ein solches Polynom heißt *irreduzibel*, wenn es sich nicht in der Form $f = gh$ mit Polynomen g, h kleineren Grades schreiben lässt. Für $q = 2$ und $n = 2$ hat man z.B. die Polynome

$$X^2 = XX,\ X^2 + 1 = (X+1)^2,\ X^2 + X = (X+1)X,\ X^2 + X + 1\,,$$

d.h. $X^2 + X + 1$ ist das einzige irreduzible Polynom vom Grad 2 über $\mathbb{F}_2$. Wie groß ist die Anzahl $a_q(n)$ der irreduziblen Polynome vom Grad n mit Koeffizienten in $\mathbb{K}$? In der Algebra lernt man:

$$\boxed{X^{q^n} - X = \prod_{\substack{f \text{ irreduzibel} \\ \deg f | n}} f\,.}$$

Gradvergleich liefert:

$$\boxed{q^n = \sum_{d|n} d \cdot a_q(d)\,.}$$

Wir wenden Möbius-Inversion (7.1) an auf:

$$f\colon \mathbb{N} \to \mathbb{R}, n \mapsto n\, a_q(n), \quad F\colon \mathbb{N} \to \mathbb{R}, n \mapsto q^n\,.$$

Wir erhalten:

$$n \cdot a_q(n) = \sum_{d|n} \mu(d) q^{n/d} \,,$$

d.h.

$$\boxed{a_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \,.}$$

Speziell:

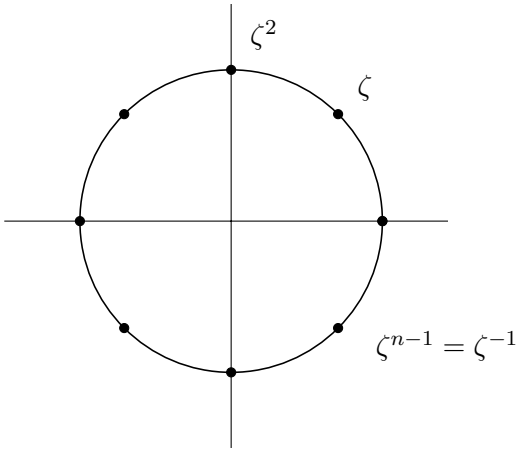
$$\begin{aligned}
a_q(1) &= \frac{1}{1} \sum_{d|1} \mu(d) q^{1/d} = q \,, \\
a_q(2) &= \frac{1}{2} \sum_{d|2} \mu(d) q^{2/d} = \frac{1}{2}(q^2 - q) \,, \\
a_q(3) &= \frac{1}{3} \sum_{d|3} \mu(d) q^{3/d} = \frac{1}{3}(q^3 - q) \,, \\
a_q(4) &= \frac{1}{4} \sum_{d|4} \mu(d) q^{4/d} = \frac{1}{4}(q^4 - q^2) \,, \\
a_q(5) &= \frac{1}{5} \sum_{d|5} \mu(d) q^{5/d} = \frac{1}{5}(q^5 - q) \,, \\
a_q(6) &= \frac{1}{6} \sum_{d|6} \mu(d) q^{6/d} = \frac{1}{6}(q^6 - q^3 - q^2 + q) \,, \\
a_q(7) &= \frac{1}{7} \sum_{d|7} \mu(d) q^{7/d} = \frac{1}{7}(q^7 - q) \,, \\
a_q(8) &= \frac{1}{8} \sum_{d|8} \mu(d) q^{8/d} = \frac{1}{8}(q^8 - q^4) \,.
\end{aligned}$$

Allgemeiner gilt: $n \cdot a_q(n) = q^{n_1} \pm q^{n_2} \pm q^{n_3} \pm \ldots \pm q^{n_r}$ $(n_1 > n_2 > \ldots > n_r)$. Daher ist $n \cdot a_q(n)$ durch q^{n_r} teilbar, aber nicht durch q^{n_r+1}. Insbesondere folgt: $a_q(n) \neq 0$; dies zeigt:

Satz *Sei $\mathbb{K}$ ein endlicher Körper. Für $n \in \mathbb{N}$ existiert dann mindestens ein irreduzibles Polynom vom Grad n mit Koeffizienten in $\mathbb{K}$.*

7.3 Bemerkung Für $n \in \mathbb{N}$ hat das ganzzahlige Polynom $X^n - 1$ die komplexen Nullstellen

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1} \text{ mit } \zeta \coloneqq e^{2\pi i/n} \,.$$



Daher:

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \zeta^k)\,.$$

$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ heißen die n-ten *Einheitswurzeln* (in $\mathbb{C}$). Für $d \mid n$ ist jede d-te Einheitswurzel η auch eine n-te Einheitswurzel:

$$\eta^n = (\eta^d)^{n/d} = 1^{n/d} = 1\,.$$

Eine n-te Einheitswurzel heißt eine primitive n-te Einheitswurzel, wenn sie für keinen echten Teiler d von n eine d-te Einheitzwurzel ist.[12] Sei η eine beliebige n-te Einheitswurzel, d.h. $\eta^n = 1$. Sei außerdem $m \coloneqq \min\{k \in \mathbb{N} : \eta^k = 1\}$ und $d \coloneqq \mathrm{ggT}(m, n)$. Bekanntlich existieren $a, b \in \mathbb{Z}$ mit $am + bn = d$. Daher:

$$\eta^d = \eta^{am+bn} = (\eta^m)^a\,(\eta^n)^b = 1^a 1^b = 1$$

Wegen $d \leq m$ folgt $d = m$, d.h. $m \mid n$. Daher ist jede n-te Einheitswurzel eine primitive m-te Einheitswurzel für (genau) einen Teiler m von n. Für die Anzahl $\psi(n)$ der primitiven n-ten Einheitswurzeln gilt also:

$$\sum_{d|n} \psi(d) = n\,.$$

Möbius-Inversion (7.1) liefert:

$$\psi(n) = \sum_{d|n} \mu(d)\frac{n}{d} \overset{3.7}{=} \varphi(n)\,.$$

Für $n \in \mathbb{N}$ existieren also genau $\varphi(n)$ primitive n-te Einheitswurzeln in $\mathbb{C}$. Man nennt dann

$$\Phi_n \coloneqq \prod_{\substack{k=1 \\ \zeta^k \text{primitive} \\ n\text{-te Einheitswurzel}}}^{n} \left(X - \zeta^k\right)$$

[12] Z.B. ist i eine primitive 4-te Einheitswurzel, da $i^4 = 1$ und $i^2 = -1 \neq 1$.

das n-te *Kreisteilungspolynom*. Z.B. ist

$$\Phi_1 = X - 1, \Phi_2 = X + 1, \Phi_4 = (X - i)(X + i) = X^2 + 1\,.$$

Allgemein ist

$$\boxed{\deg \Phi_n = \varphi(n)}$$

und aus den obigen Überlegungen folgt:

$$\boxed{X^n - 1 = \prod_{d|n} \Phi_d\,.}$$

Wir beweisen jetzt eine multiplikative Variante der Möbius-Inversion.

7.3 Satz $n \in \mathbb{N} \Rightarrow \Phi_n = \prod_{d|n} \left(X^d - 1\right)^{\mu(n/d)}$

Beweis. Wir definieren $\delta, \varepsilon \colon \mathbb{N} \to \mathbb{R}$ durch $\delta(1) = 1$, $\delta(n) = 0$ für $n > 1$ und $\varepsilon(n) = 1$ für $n \in \mathbb{N}$. Dann gilt für $n \in \mathbb{N}$:

$$\sum_{d|n} \delta(d) = \delta(1) = 1 = \varepsilon(n)\,.$$

Möbius-Inversion ergibt

$$\sum_{d|n} \mu(d) \underbrace{\varepsilon(\frac{n}{d})}_{=1} = \delta(n)\,.$$

Daher:

$$\prod_{d|n} \left(X^d - 1\right)^{\mu(n/d)} = \prod_{d|n} \prod_{e|d} \Phi_e^{\mu(n/d)} = \prod_{e|n} \Phi_e^{\sum\limits_{e|d|n} \mu(\frac{n}{d})} = \prod_{e|n} \Phi_e^{\sum\limits_{k|n/e} \mu(k)} = \prod_{e|n} \Phi_e^{\delta(\frac{n}{e})} = \Phi_n\,.$$

□

Beispiel Für $p \in \mathbb{P}$ und $k \in \mathbb{N}$ gilt also:

$$\Phi_{p^k} = \frac{X^{p^k} - 1}{X^{p^{k-1}} - 1} = X^{p^{k-1}(p-1)} + X^{p^{k-1}(p-2)} + \ldots + X^{p^{k-1}} + 1\,.$$

Insbesondere: $\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$.

$$\Phi_1 = X - 1 \qquad \Phi_4 = X^2 + 1$$
$$\Phi_2 = X + 1 \qquad \Phi_5 = X^4 + X^3 + X^2 + X + 1$$
$$\Phi_3 = X^2 + X + 1 \qquad \Phi_6 = \frac{(X^6 - 1)(X - 1)}{(X^2 - 1)(X^3 - 1)} = \frac{X^3 + 1}{X + 1} = X^2 - X + 1$$

7.4 Bemerkung Für $n \in \mathbb{N}$ hat das n-te Kreisteilungspolynom Φ_n Koeffizienten in $\mathbb{Z}$; denn nach Satz 7.3 ist

$$\Phi_n = \frac{X^k + a_{k-1}X^{k-1} + \ldots + a_1X + a_0}{X^l + b_{l-1}X^{l-1} + \ldots + b_1X + b_0} \qquad (a_0, \ldots, a_k, b_0, \ldots, b_l \in \mathbb{Z})$$

und die Polynomdivision geht auf.

7.5 Definition Für $A = (a_{ij}) \in \mathbb{R}^{m\times n}$ heißt

$$\operatorname{per}(A) = \sum_{\substack{\pi\colon \{1,\ldots,m\}\to\{1,\ldots,n\} \\ \pi \text{ injektiv}}} a_{1\pi(1)}a_{2\pi(2)}\ldots a_{m\pi(m)}$$

Permanente von A.

Literatur: H. Minc, Permanents, Addison-Wesley 1978

Beispiel

$$A = \begin{pmatrix} 3 & 0 & 1 & -2 \\ 4 & -1 & 3 & 0 \end{pmatrix}$$

$$\begin{aligned}\operatorname{per}(A) &= 3\cdot(-1) + 3\cdot 3 + 3\cdot 0 + 0\cdot 4 + 0\cdot 3 + 0\cdot 0 \\ &\quad + 1\cdot 4 + 1\cdot(-1) + 1\cdot 0 + (-2)\cdot 4 + (-2)\cdot(-1) + (-2)\cdot 3 = -3\end{aligned}$$

Bemerkung Die Anzahl der Summanden in $\operatorname{per}(A)$ ist $n(n-1)\ldots(n-m+1)$. Im Fall $n = m$ ist das $n!$ und es treten die gleichen Summanden auf wie bei der Determinante, aber ohne "Vorzeichen". Wir werden mit der Möbius-Inversion eine andere Formel für $\operatorname{per}(A)$ herleiten.

Bemerkung Setze $R \coloneqq \{1, \ldots, m\}$ (*rows*) und $C \coloneqq \{1, \ldots, n\}$ (*columns*). Für $I \subseteq C$ sei $A|I$ die $m \times |I|$-Matrix, die aus den i-ten Spalten ($i \in I$) von A besteht. Ferner sei

$$P(A) \coloneqq \prod_{i=1}^{m}\Big(\sum_{j=1}^{n} a_{ij}\Big)$$

das Produkt der Zeilensummen von A. Für $\begin{pmatrix} 3 & 0 & 1 & -2 \\ 4 & -1 & 3 & 0 \end{pmatrix} = A$ ist

$$P(A) = (3+0+1-2)(4-1+3+0) = 12 \text{ und } A|\{1,4\} = \begin{pmatrix} 3 & -2 \\ 4 & 0 \end{pmatrix}$$

Für $\pi\colon R \to C$ sei

$$w(\pi) \coloneqq \prod_{i=1}^{m} a_{i\pi(i)}\,.$$

und für $B \subseteq S \coloneqq \operatorname{Abb}(R, C)$ sei

$$w(B) \coloneqq \sum_{\pi\in B} w(\pi)\,.$$

Dann: $w(\{\pi \in S : \pi \text{ injektiv}\}) = \operatorname{per}(A)$. Für $i \in C$ sei $A_i = \{\pi \in S : i \notin \operatorname{Bld}(\pi)\}$ und für $I \subseteq C$ sei

$$E_I \coloneqq \bigcap_{i \in I} A_i \cap \bigcap_{i \in C \setminus I} (S \setminus A_i) = \{\pi \in S : \operatorname{Bld}(\pi) = C \setminus I\}\,.$$

Dann:

$$\bigcap_{i \in I} A_i = \{\pi \in S : \operatorname{Bld}(\pi) \subseteq C \setminus I\} = \dot{\bigcup}_{I \subseteq J \subseteq C} E_J\,.$$

Setze

$$f(I) \coloneqq w(E_I) \text{ und } F(I) \coloneqq \sum_{I \subseteq J \subseteq C} f(J) = \sum_{I \subseteq J \subseteq C} w(E_J) = w\Big(\bigcap_{i \in I} A_i\Big)\,.$$

Möbius-Inversion liefert

$$f(I) = \sum_{I \subseteq J \subseteq C} \mu(I,J) F(J) = \sum_{I \subseteq J \subseteq C} (-1)^{|J|-|I|}\, w\Big(\bigcap_{j \in J} A_j\Big)\,.$$

Für $p \in \{0, \dots, n\}$ ist also

$$\begin{aligned}\sum_{\substack{I \subseteq C \\ |I|=p}} f(I) &= \sum_{\substack{I \subseteq J \subseteq C \\ |I|=p}} (-1)^{|J|-p}\, w\Big(\bigcap_{j \in J} A_j\Big) = \sum_{\substack{J \subseteq C \\ |J| \geq p}} \sum_{\substack{I \subseteq J \\ |I|=p}} (-1)^{|J|-p}\, w\Big(\bigcap_{j \in J} A_j\Big) \\ &= \sum_{k=p}^{n} (-1)^{k-p} \binom{k}{p} \sum_{\substack{J \subseteq C \\ |J|=k}} w\Big(\bigcap_{j \in J} A_j\Big)\,.\end{aligned}$$

Im Fall $|I| = n - m$ ist E_I die Menge aller (injektiven) Abbildungen $\pi\colon R \to C$ mit Bild $C \setminus I$. Daher:

$$\sum_{\substack{I \subseteq C \\ |I|=n-m}} f(I) = \sum_{\substack{I \subseteq C \\ |I|=n-m}} w(E_I) = w\big(\{\pi \in S : \pi \text{ injektiv}\}\big) = \operatorname{per}(A)\,.$$

Andererseits ist jeweils

$$w\Big(\bigcap_{j \in J} A_j\Big) = \sum_{\substack{\pi \in S \\ \operatorname{Bld}(\pi) \subseteq C \setminus J}} w(\pi) = \sum_{\substack{\pi \in S \\ \operatorname{Bld}(\pi) \subseteq C \setminus J}} a_{1\pi(1)} a_{2\pi(2)} \dots a_{m\pi(m)} = \prod_{i=1}^{m} \Big(\sum_{k \in C \setminus J} a_{ik} \Big) = P(A|C \setminus J)\,.$$

Daher:

$$\operatorname{per}(A) = \sum_{k=n-m}^{n} (-1)^{k-n+m} \binom{k}{n-m} \sum_{\substack{J \subseteq C \\ |J|=k}} P(A|C \setminus J)\,.$$

Substituiere $k = n - l$ und $I = C \setminus J$:

$$\operatorname{per}(A) = \sum_{l=0}^{m} (-1)^{m-l} \binom{n-l}{n-m} \sum_{\substack{I \subseteq C \\ |I|=l}} P(A|I)\,.$$

Der Summand für $l = 0$ verschwindet. Damit ist gezeigt:

Satz (Ryser) *Für $A \in \mathbb{R}^{m\times n}$ ist*

$$\boxed{\operatorname{per}(A) = \sum_{k=1}^{m} (-1)^{m-k} \binom{n-k}{n-m} \sum_{\substack{I\subseteq C \\ |I|=k}} P(A|I)\,.}$$

Für $m = n$ ist

$$\boxed{\operatorname{per}(A) = \sum_{k=1}^{n} (-1)^{n-k} \sum_{\substack{I\subseteq C \\ |I|=k}} P(A|I)\,.}$$

7.6 Beispiel Für $A = \begin{pmatrix} 3 & 0 & 1 & -2 \\ 4 & -1 & 3 & 0 \end{pmatrix}$ ist

$$\begin{aligned}\operatorname{per}(A) = &- \binom{3}{2}\big(3\cdot 4 + 0\cdot(-1) + 1\cdot 3 + (-2)\cdot 0\big) \\ &+ \binom{2}{2}\big(3\cdot 3 + 4\cdot 7 + 1\cdot 4 + 1\cdot 2 + (-2)\cdot(-1) + (-1)\cdot 3\big) = -3\,.\end{aligned}$$

Bemerkung

(i) Für

$$J := \begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{pmatrix} \in \mathbb{R}^{n\times n}$$

ist $\operatorname{per}(J) = n!$ nach Definition. Nach Ryser gilt:

$$\operatorname{per}(J) = \sum_{k=1}^{n} (-1)^{n-k} \binom{n}{k} k^n \text{ (vgl. Satz 3.4).}$$

(ii) Für

$$A = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & 0 \end{pmatrix} = J - 1_n$$

ist

$$\operatorname{per}(A) = D_n = \sum_{k=1}^{n} (-1)^{n-k} \binom{n}{k} (k-1)^k k^{n-k}\,.$$

8 Gruppenoperationen

8.1 Bemerkung

(i) Wir wissen, dass von den $n!$ Permutationen von $\{1,\dots,n\}$ genau

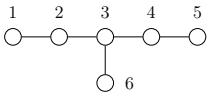
$$D_n = \sum_{k=0}^{n} \frac{(-1)^k n!}{k!} \sim \frac{n!}{e} \sim \frac{n!}{3} \quad \text{fixpunktfrei sind.}$$

Wie viele Fixpunkte hat eine Permutation von {1, …, n} im Durchschnitt?

n	Permutationen	Fixpunkte	Durchschnitt
$n=2$	$\begin{pmatrix}1&2\\1&2\end{pmatrix}, \begin{pmatrix}1&2\\2&1\end{pmatrix}$	2	1
$n=3$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$		
	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	6	1

Wir werden sehen, dass auch für größere n die durchschnittliche Fixpunktzahl 1 ist.

(ii) Wie viele Graphen mit 4 Ecken gibt es? Ein *Graph* ist ein Paar $(V,E)=\Gamma$, das aus einer endlichen Menge V von Ecken[13] und einer Menge E von Kanten[14] besteht. Dabei ist jede Kante eine 2-Teilmenge von V.



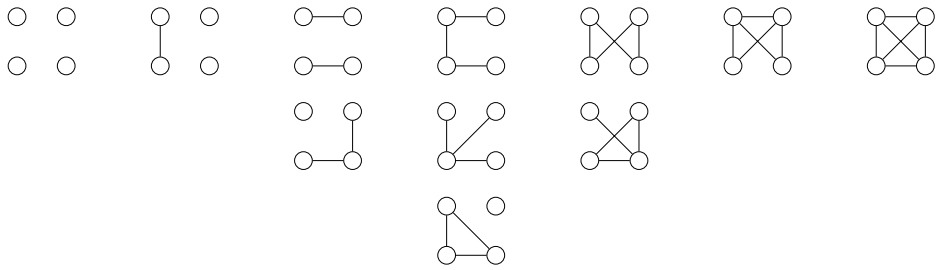
E_6 $\qquad V=\{1,\dots,6\} \quad E=\big\{\{1,2\},\{2,3\},\{3,4\},\{3,6\},\{4,5\}\big\}$

Im Fall $|V|=4$ gibt es $\binom{4}{2}=6$ potentielle Kanten. Für E existieren also $2^6=64$ Möglichkeiten. Allerdings sind z.B. die Graphen

nicht "wesentlich" verschieden, d.h. sie unterscheiden sich nur durch die Nummerierung der Ecken. Wie viele wesentlich verschiedene Graphen mit 4 Ecken gibt

[13] engl.: *vertices*.
[14] engl.: *edges*.

es?



Ergebnis: 11

(iii) Die Ecken eines Quadrats sollen mit 3 Farben (rot, blau, weiß) gefärbt werden. Wie viele Möglichkeiten gibt es? An jeder der 4 Ecken kann man sich für eine der 3 Farben entscheiden. Das ergibt $3^4 = 81$ Möglichkeiten. Allerdings sind die Färbungen

$$\begin{matrix} b\ b \\ r\ w \end{matrix} \qquad \begin{matrix} r\ b \\ w\ b \end{matrix} \qquad \begin{matrix} w\ r \\ b\ b \end{matrix} \qquad \begin{matrix} b\ w \\ b\ r \end{matrix}$$

nicht wesentlich verschieden; sie gehen durch Drehungen des Quadrats ineinander über. Wie viele wesentlich verschiedene Färbungen gibt es?

$$\begin{matrix} b\ b \\ b\ b \end{matrix} \qquad \begin{matrix} r\ r \\ r\ r \end{matrix} \qquad \begin{matrix} w\ w \\ w\ w \end{matrix}$$

$$\begin{matrix} b\ r \\ r\ r \end{matrix} \qquad \begin{matrix} b\ w \\ w\ w \end{matrix} \qquad \begin{matrix} r\ b \\ b\ b \end{matrix} \qquad \begin{matrix} r\ w \\ w\ w \end{matrix} \qquad \begin{matrix} w\ b \\ b\ b \end{matrix} \qquad \begin{matrix} w\ r \\ r\ r \end{matrix}$$

$$\begin{matrix} b\ b \\ r\ r \end{matrix} \qquad \begin{matrix} b\ b \\ w\ w \end{matrix} \qquad \begin{matrix} r\ r \\ w\ w \end{matrix} \qquad \begin{matrix} b\ r \\ r\ b \end{matrix} \qquad \begin{matrix} b\ w \\ w\ b \end{matrix} \qquad \begin{matrix} r\ w \\ w\ r \end{matrix}$$

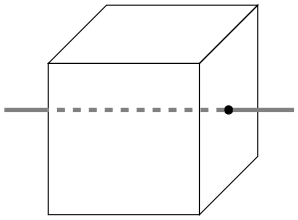
$$\begin{matrix} b\ r \\ w\ b \end{matrix} \qquad \begin{matrix} r\ b \\ w\ r \end{matrix} \qquad \begin{matrix} w\ r \\ b\ w \end{matrix}$$

$$\begin{matrix} b\ b \\ r\ w \end{matrix} \qquad \begin{matrix} b\ b \\ w\ r \end{matrix} \qquad \begin{matrix} r\ r \\ b\ w \end{matrix} \qquad \begin{matrix} r\ r \\ w\ b \end{matrix} \qquad \begin{matrix} w\ w \\ r\ b \end{matrix} \qquad \begin{matrix} w\ w \\ b\ r \end{matrix}$$

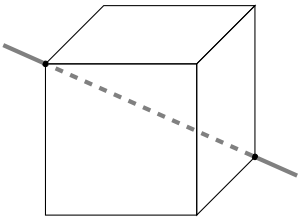
Das ergibt insgesamt 24 "wesentlich verschiedene" Färbungen. Wie ändert sich das Ergebnis, wenn man zusätzlich zu den Drehungen des Quadrats noch Spiegelungen zulässt? Dann fallen in der letzten Zeile jeweils 2 Färbungen zusammen. Es existieren also insgesamt nur noch 21 "wesentlich verschiedene" Färbungen.

(iv) Die Seiten eines Würfels sollen wieder mit 3 Farben (blau, rot, weiß) eingefärbt werden. Es gibt 6 Seiten, bei jeder hat man 3 Farben zur Auswahl. Das ergbit $3^6 = 729$ Möglichkeiten. Allerdings sind Färbungen, die durch Drehung des Würfels ineinander übergehen, nicht "wesentlich verschieden". Wie viele "wesentlich verschiedene" Färbungen gibt es? Wir werden sehen: 57 (Probieren Sie!). Zunächst verschaffen wir

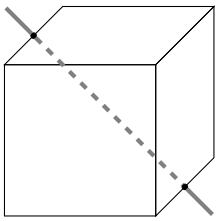
uns einen Überblick über die vorhandenen Drehungen. Nach jeder Drehung liegt eine der 6 Seiten des Würfels oben. Damit ist auch die Unterseite festgelegt. Eine der 4 Seiten liegt vorne. Durch Ober- und Vorderseite ist die Lage des Würfels festgelegt. Daher existieren $6 \cdot 4 = 24$ Drehungen. Diese unterscheiden wir folgendermaßen:



Es existieren Drehungen um eine Achse, die durch die Mittelpunkte gegenüberliegender Seiten geht. Es gibt 3 solche Achsen und man kann jeweils um 90°, 180°, 270° drehen. Dies ergibt 9 Drehungen.



Es gibt Drehungen um eine Achse, die jeweils durch gegenüberliegende Ecken geht. Es gibt 4 solcher Achsen. Man kann jeweils um 120° oder 240° drehen (An jeder Ecke treffen sicht jeweils 3 Kanten). Das ergibt 8 Drehungen.



Es gibt Drehungen um eine Achse, die durch die Mittelpunkte gegenüberliegender Kanten geht. Es existieren 12 Kanten, also 6 solcher Achsen. Man kann jeweils um 180° drehen. Das ergibt 6 Drehungen. Zusätzlich hat man die "triviale" Drehung, die den ganzen Würfel festlässt.

Definition Seien G eine endliche Gruppe und Ω eine (endliche) Menge. Eine *Operation*[15] von G auf Ω ist eine Abbildung $G \times \Omega \to \Omega,\ (g, \alpha) \mapsto g * \alpha$ mit folgenden Eigenschaften:

(i) $1 * \alpha = \alpha$ für alle $\alpha \in \Omega$,

(ii) $g * (h * \alpha) = (gh) * \alpha$ für alle $g, h \in G$, $\alpha \in \Omega$.

[15] engl.: *action*.

Man sagt auch: "G operiert auf Ω" oder "Ω ist eine G-Menge".

Beispiel

(i) Die Menge $G = \mathrm{Sym}(\Omega)$ aller bijektiven Abbildungen auf Ω ist eine Gruppe bzgl. der Komposition von Abbildungen, die *symmetrische Gruppe* auf Ω. Sie operiert auf Ω durch

$$g * \alpha \coloneqq g(\alpha) \quad (g \in \mathrm{Sym}(\Omega),\, \alpha \in \Omega)\,.$$

(ii) Sei $\mathbb{K}$ ein (endlicher) Körper und $n \in \mathbb{N}$. Die Gruppe $\mathrm{GL}(n, \mathbb{K})$ aller invertierbaren $n \times n$-Matrizen mit Koeffizienten in $\mathbb{K}$ operiert auf der Menge $\mathbb{K}^{n\times 1}$ durch Matrixmultiplikation:

$$g * \alpha \coloneqq g\alpha \quad (g \in \mathrm{GL}(n, \mathbb{K}),\, \alpha \in \mathbb{K}^{n\times 1})\,.$$

(iii) Sei $G = \{1, g\}$ eine Gruppe der Ordnung 2. Für $n \in \mathbb{N}$ operiert G auf der Menge Ω aller Teiler von n durch:

$$1 * d = d \text{ und } g * d \coloneqq \frac{n}{d} \quad (d \in \Omega)\,.$$

8.1 Satz *Für jede Operation $G \times \Omega \to \Omega, (g, \alpha) \mapsto g * \alpha$ gilt:*

(i) $g \in G \Longrightarrow f_g \colon \Omega \to \Omega, \alpha \mapsto g * \alpha$ *bijektiv,*

(ii) $g, h \in G \Longrightarrow f_g \circ f_h = f_{gh}$,

(iii) $F \colon G \to \mathrm{Sym}(\Omega), g \mapsto f_g$ *ist ein Gruppenhomomorphismus.*

Beweis.

(i) Sei $g \in G$. Zum Beweis der Injektivität von f_g seien $\alpha, \beta \in \Omega$ mit $f_g(\alpha) = f_g(\beta)$, d.h. $g * \alpha = g * \beta$. Dann:

$$\alpha = 1 * \alpha = (g^{-1}g) * \alpha = g^{-1} * (g * \alpha) = g^{-1} * (g * \beta) = (g^{-1}g) * \beta = 1 * \beta = \beta\,.$$

Zum Beweis der Surjektivität von f_g sei $\gamma \in \Omega$ beliebig. Dann:

$$g^{-1} * \gamma \in \Omega \text{ und } f_g(g^{-1} * \gamma) = g * (g^{-1} * \gamma) = (gg^{-1}) * \gamma = 1 * \gamma = \gamma\,.$$

(ii) Für $g, h \in G$, $\alpha \in \Omega$ gilt:

$$(f_g \circ f_h)(\alpha) = f_g(f_h(\alpha)) = g * (h * \alpha) = (gh) * \alpha = f_{gh}(\alpha)\,.$$

(iii) Für $g, h \in G$ ist $F(g) \circ F(h) = f_g \circ f_h = f_{gh} = F(gh)$.

□

8.2 Bemerkung In der Situation von Satz 8.1 heißt

$$\mathrm{Ker}(F) = \{g \in G : F(g) = 1\} = \{g \in G : f_g = \mathrm{id}_\Omega\} = \{g \in G : g * \alpha = \alpha \text{ für alle } \alpha \in \Omega\}$$

Kern der Operation. Man zeigt leicht: $\mathrm{Ker}(F)$ ist eine Untergruppe von G (sogar ein Normalteiler). Ist F injektiv, d.h. $\mathrm{Ker}(F) = \{1\}$, so heißt die Opertion *treu*. Eine Operation $G \times \Omega \to \Omega, (g, \alpha) \mapsto g * \alpha$, ist also genau dann treu, wenn zu jedem $1 \neq g \in G$ ein $\alpha \in \Omega$ existiert mit $g * \alpha \neq \alpha$. Wir beweisen jetzt die Umkehrung von Satz 8.1.

Satz *Seien G eine endliche Gruppe, Ω eine endliche Menge und $F\colon G \to \mathrm{Sym}(\Omega), g \mapsto f_g$ ein Homomorphismus von Gruppen. Dann ist $G \times \Omega \to \Omega, (g, \alpha) \mapsto f_g(\alpha)$ eine Operation.*

Beweis. Für $g, h \in G$ und $\alpha \in \Omega$ ist

$$g*(h*\alpha) = f_g(f_h(\alpha)) = (f_g \circ f_h)(\alpha) = (F(g) \circ F(h))(\alpha) = (F(gh))(\alpha) = f_{gh}(\alpha) = (gh)*\alpha$$

und

$$1 * \alpha = f_1(\alpha) = (F(1))(\alpha) = (\mathrm{id}_\Omega)(\alpha) = \alpha\,.$$

□

8.3 Satz *Jede Operation $G \times \Omega \to \Omega, (g, \alpha) \mapsto g * \alpha$, definiert eine Relation $\sim_G$ auf Ω durch*

$$\alpha \sim_G \beta \iff \exists g \in G : g * \alpha = \beta\,.$$

Dann ist $\sim_G$ eine Äquivalenzrelation.

Beweis.

Reflexivität: Für $\alpha \in \Omega$ gilt $1 * \alpha = \alpha$, d.h. $\alpha \sim_G \alpha$.

Symmetrie: Seien $\alpha, \beta \in \Omega$ mit $\alpha \sim_G \beta$. Dann existiert ein $g \in G$ mit $g * \alpha = \beta$. Daher ist $g^{-1} \in G$ und $g^{-1} * \beta = g^{-1} * (g * \alpha) = (g^{-1}g) * \alpha = 1 * \alpha = \alpha$, d.h. $\beta \sim_G \alpha$.

Transitivität: Seien $\alpha, \beta, \gamma \in \Omega$ mit $\alpha \sim_G \beta$ und $\beta \sim_G \gamma$. Dann existieren $g, h \in G$ mit $g * \alpha = \beta$ und $h * \beta = \gamma$. Daher: $hg \in G$ und $(hg) * \alpha = h * (g * \alpha) = h * \beta = \gamma$.

□

Bemerkung Für $\alpha \in \Omega$ heißt die Äquivalenzklasse

$$[\alpha] \coloneqq \mathrm{Orb}_G(\alpha) \coloneqq \{g * \alpha : g \in G\}$$

Bahn (bzw. *Orbit*) von α bzgl. $*$. $|\mathrm{Orb}_G(\alpha)|$ heißt Länge der Bahn von α. Die Menge aller Bahnen ist $G\backslash\Omega \coloneqq \{\mathrm{Orb}_G(\alpha) : \alpha \in \Omega\}$. Sei R ein Repräsentantensystem für die Bahnen, d.h. R enthält aus jeder Bahn genau ein Element. Dann:

$$\Omega = \dot{\bigcup_{\alpha \in R}} \mathrm{Orb}_G(\alpha)\,.$$

Daraus folgt die triviale, aber sehr nützliche *Bahnengleichung*

$$|\Omega| = \sum_{\alpha \in R} |\mathrm{Orb}_G(\alpha)| \,.$$

Ist $|G\backslash\Omega| = 1$, d.h. es existiert nur eine Bahn, so heißt die Operation $*$ *transitiv*. Das bedeutet, dass es für je zwei $\alpha, \beta \in \Omega$ ein $g \in G$ mit $g * \alpha = \beta$ gibt.

Beispiel

(i) Sei $G = \{1, g, g^2, g^3\}$ die Gruppe der Drehungen des Quadrats. Dann operiert G in offensichtlicher Weise auf der Menge Ω der 81 Färbungen der Ecken mit 3 Farben (blau, rot, weiß). Die wesentlich verschiedenen Färbungen entsprechen genau den Bahnen von G auf Ω. In Bemerkung 8.1 haben wir berechnet: $|G\backslash\Omega| = 24$.

(ii) Sei $G = \mathrm{Sym}(4)$, d.h. $|G| = 4! = 24$. Dann operiert G in offensichtlicher Weise auf der Menge Ω der 64 Graphen mit Eckenmenge $V = \{1, 2, 3, 4\}$. Die wesentlich verschiedenen Graphen entsprechen dabei genau den Bahnen von G auf Ω. Wir haben berechnet: $|G\backslash\Omega| = 11$.

(iii) Sei $\mathbb{K}$ ein (endlicher) Körper und $n \in \mathbb{N}$. Dann operiert $G := \mathrm{GL}(n, \mathbb{K})$ auf $\Omega = \mathbb{K}^{n\times 1}$ durch Multiplikation. Offenbar ist $\{(0, \ldots, 0)^\top\}$ eine Bahn für sich. Ist $0 \neq (\alpha_1, \ldots, \alpha_n)^\top \in \mathbb{K}^{n\times 1}$, so existiert eine Basis $b_1, \ldots, b_n$ von $\mathbb{K}^{n\times 1}$ mit $b_1 = (\alpha_1, \ldots, \alpha_n)$. Dann ist die Matrix $B = (b_1|b_2|\ldots|b_n) \in \mathrm{GL}(n, \mathbb{K})$ mit

$$B \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} .$$

Also: $\mathrm{Orb}_G((1, 0, \ldots, 0)^\top) = \mathbb{K}^{n\times 1} \setminus \{0\}$, d.h. die Operation hat genau zwei Bahnen.

(iv) Jede Untergruppe H einer endlichen Gruppe G operiert auf $\Omega := G$ durch Linksmultiplikation mit

$$h * g := hg \quad (h \in H,\, g \in G).$$

Für $g \in G$ heißt $\mathrm{Orb}_H(g) = \{hg : h \in H\} = Hg$ Rechtsnebenklasse von g nach H. Die Menge aller Rechtsnebenklassen von H in G ist $H\backslash G = \{Hg : g \in G\}$.

(v) Analog operiert jede Untergruppe H einer endlichen Gruppe $G =: \Omega$ durch Rechtsmultiplikation:

$$h * g := gh^{-1} \quad (g \in G,\, h \in H).$$

Beachte:

$$k * (h * g) = (gh^{-1})k^{-1} = g(h^{-1}k^{-1}) = g(kh)^{-1} = kh * g \quad (g \in G,\, h, k \in H).$$

Für $g \in G$ heißt $\mathrm{Orb}_H(g) = \{gh^{-1} : h \in H\} = gH$ Linksnebenklasse von g nach H. Die Menge aller Linksnebenklassen nach H in G ist $G/H = \{gH : g \in G\}$.

Literatur: A. Kerber, Applied finite group actions, Springer 1999

8.4 Satz *Sei $G \times \Omega \to \Omega, (g, \alpha) \mapsto g * \alpha$ eine Operation. Für $\alpha \in \Omega$ ist dann*

$$G_\alpha := \mathrm{Stb}_G(\alpha) := \{g \in G : g * \alpha = \alpha\}$$

eine Untergruppe von G. Ferner ist

$$f \colon G/G_\alpha \to \mathrm{Orb}_G(\alpha),\ gG_\alpha \mapsto g * \alpha\,,$$

bijektiv. Insbesondere: $|\mathrm{Orb}_G(\alpha)| = |G/G_\alpha|$.

Beweis. Wegen $1 * \alpha = \alpha$ ist $1 \in G_\alpha$. Für $g, h \in G_\alpha$ ist

$$g * \alpha = \alpha = h * \alpha\,, \text{also } gh * \alpha = g * (h * \alpha) = g * \alpha = \alpha\,, \text{d.h. } gh \in G_\alpha\,.$$

Ferner:

$$g^{-1} * \alpha = g^{-1} * (g * \alpha) = (g^{-1}g) * \alpha = 1 * \alpha = \alpha\,,$$

d.h. $g^{-1} \in G_\alpha$. Daher: $G_\alpha \leq G$. Jetzt zeigen wir, dass f wohldefiniert ist. Dazu seien $g, g' \in G$ mit $gG_\alpha = g'G_\alpha$. Dann existiert ein $h \in G_\alpha$ mit $g' = gh$. Daher:

$$g' * \alpha = gh * \alpha = g * (h * \alpha) = g * \alpha\,.$$

Zum Beweis der Injektivität seien $g, g' \in G$ mit $g * \alpha = g' * \alpha$. Dann:

$$(g^{-1}g') * \alpha = g^{-1} * (g' * \alpha) = g^{-1} * (g * \alpha) = (g^{-1}g) * \alpha = 1 * \alpha = \alpha\,,$$

d.h. $g^{-1}g \in G_\alpha$. Daher:

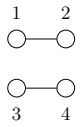
$$g' = gg^{-1}g' \in gG_\alpha\,, \text{d.h. } g'G_\alpha = gG_\alpha\,.$$

Wegen $\mathrm{Orb}_G(\alpha) = \{g * \alpha : g \in G\}$ ist f surjektiv. □

Definition G_α heißt Stabilisator von α in G.

Beispiel

(i) Welche Permutationen $g \in G := \mathrm{Sym}(4)$ lassen den Graphen Γ



fest?

$$\mathrm{Stb}_G(\Gamma) = \left\{ \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \right.$$
$$\left. \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} \right\}$$

(ii) Welche Drehungen lassen die folgende Färbung eines Quadrats fest?

$$\begin{matrix} \boldsymbol{r} & \boldsymbol{w} \\ \boldsymbol{w} & \boldsymbol{r} \end{matrix} \quad \curvearrowright \quad G_\alpha = \{1, g^2\} \subseteq \{1, g, g^2, g^3\} = G$$

Bemerkung Ist R ein Repräsentantensystem[16] für die Bahnen von G auf Ω, so kann man die Bahnengleichung auch folgendermaßen schreiben:

$$\boxed{|\Omega| = \sum_{\alpha \in R} |\mathrm{Orb}_G(\alpha)| = \sum_{\alpha \in R} |G/G_\alpha| \,.}$$

8.5 Satz (Lagrange) *Für jede Untergruppe H einer endlichen Gruppe G ist*

$$|G| = |G/H| \cdot |H|$$

Beweis. Wir wenden auf die Operation $H \times G \to G, (h, g) \mapsto gh^{-1}$, die Bahnengleichung an und erhalten:

$$|G| = \sum_{g \in R} |H/H_g| \,;$$

dabei ist R ein Repräsentantensystem für die Linksnebenklassen nach H in G. Für $g \in G$ ist

$$H_g = \{h \in H : gh^{-1} = g\} = \{h \in H : h^{-1} = 1\} = \{1\} \,,$$

also

$$H/H_g = H/\{1\} = \{h\{1\} : h \in H\} = \{\{h\} : h \in H\}$$

und damit $|H/H_g| = |H|$. Daher: $|G| = |R| \cdot |H| = |G/H| \cdot |H|$. □

Definition $|G/H| = |G : H|$ heißt *Index* von H in G.

Bemerkung

(i) $|H|$ und $|G : H|$ sind also Teiler von $|G|$.

(ii) Die Abbildung $i\colon G/H \to H\backslash G, gH \mapsto Hg^{-1}$, ist wohldefiniert; denn sind $a, b \in G$ mit $aH = bH$, so existiert ein $h \in H$ mit $b = ah$. Daher: $b^{-1} = h^{-1}a^{-1} \in Ha^{-1}$, d.h. $Hb^{-1} = Ha^{-1}$. Offensichtlich ist i surjektiv. Fener ist i injektiv; denn sind $a, b \in G$ mit $Ha^{-1} = Hb^{-1}$, so existiert ein $h \in H$ mit $b^{-1} = ha^{-1}$. Daher: $b = (ha^{-1})^{-1} = (a^{-1})^{-1}h^{-1} = ah^{-1} \in aH$, d.h. $bH = aH$. Also: $|G/H| = |H\backslash G|$.

(iii) Für jede Operation $G \times \Omega \to \Omega$ und jedes $\alpha \in \Omega$ ist $|\mathrm{Orb}_G(\alpha)| = |G/G_\alpha| = |G : G_\alpha|$ ein Teiler von $|G|$.[17]

8.6 Definition Für jede Operation $G \times \Omega \to \Omega$, $(g, \alpha) \mapsto g * \alpha$ und jedes $g \in G$ sei

$$\mathrm{Fix}_\Omega(g) \coloneqq \{\alpha \in \Omega : g * \alpha = \alpha\}$$

die Menge der *Fixpunkte* von g unter α.

[16] engl.: *transversal*.
[17] Dies kann man oft als Probe verwenden.

Satz (Lemma von Burnside) *Für jede Operation $G \times \Omega \to \Omega$, $(g, \alpha) \mapsto g * \alpha$, gilt:*

$$|G\backslash\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_\Omega(g)| \,.$$

Bemerkung Das bedeutet, dass die Anzahl der Bahnen gleich der durchschnittlichen Fixpunktzahl der Elemente in G ist. Der Satz ist nützlich, da es häufig einfacher ist, Fixpunkte zu zählen als Bahnen.

Beweis. Wir betrachten $M \coloneqq \{(g, \alpha) \in G \times \Omega : g * \alpha = \alpha\}$ und bestimmen $|M|$ auf zwei Arten. Einerseits ist

$$|M| = \sum_{g \in G} |\mathrm{Fix}_\Omega(g)| \,.$$

Andererseits:

$$|M| = \sum_{\alpha \in \Omega} |G_\alpha| = \sum_{\alpha \in \Omega} \frac{|G|}{|\mathrm{Orb}_G(\alpha)|} = |G| \sum_{\alpha \in \Omega} \frac{1}{|\mathrm{Orb}_G(\alpha)|} = |G| \cdot |G\backslash\Omega| \,.$$

□

Beispiel

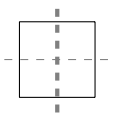
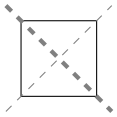
(i) Offenbar operiert $\mathrm{Sym}(\Omega)$ transitiv auf Ω. Daher ist 1 die durchschnittliche Fixpunktzahl in $\mathrm{Sym}(\Omega)$.

(ii) Betrachte die Färbungen der Ecken eines Quadrats:

Drehung		Fixpunkte	Anzahl
90°	$\begin{matrix} \boldsymbol{x} & \boldsymbol{x} \\ \boldsymbol{x} & \boldsymbol{x} \end{matrix}$	$x \in \{b, w, r\}$	3
180°	$\begin{matrix} \boldsymbol{x} & \boldsymbol{y} \\ \boldsymbol{y} & \boldsymbol{x} \end{matrix}$	$x, y \in \{b, r, w\}$	9
0°		alles	$3^4 = 81$

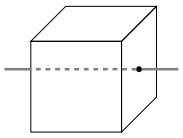
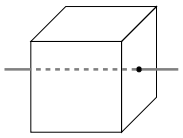
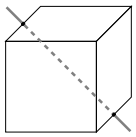
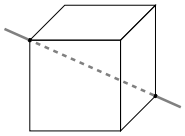
$\curvearrowright$ Bahnenzahl: $\frac{1}{4}(3 + 3 + 9 + 81) = \frac{96}{4} = 24$.

Variante: auch Spiegelungen:

Spiegelung		Fixpunkte	Anzahl
	$\begin{matrix} \boldsymbol{x} & \boldsymbol{x} \\ \boldsymbol{y} & \boldsymbol{y} \end{matrix}$	$x, y \in \{b, r, w\}$	9
	$\begin{matrix} \boldsymbol{y} & \boldsymbol{x} \\ \boldsymbol{x} & \boldsymbol{z} \end{matrix}$	$x, y, z \in \{b, r, w\}$	$3^3 = 27$

$\curvearrowright$ Bahnenzahl: $\frac{1}{8}(3+3+9+81+9+9+27+27) = \frac{168}{8} = 21$.

(iii) Betrachte jetzt die Färbungen der 6 Seiten eines Würfels mit 3 Farben:

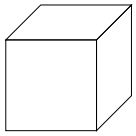
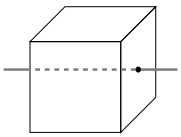
Drehung		Fixpunkte	Vielfachheit
Identität		$3^6 = 729$	1
	$\pm 90°$	$3^3 = 27$	$2 \cdot 3 = 6$
	$180°$	$3^4 = 81$	3
	$180°$	$3^3 = 27$	6
	$\pm 120°$	$3^2 = 9$	$2 \cdot 4 = 8$

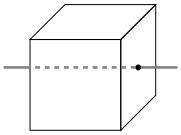
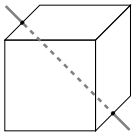
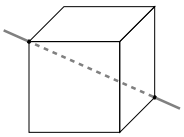
$\curvearrowright$ Bahnenzahl: $\frac{1}{24}(729 + 6 \cdot 27 + 3 \cdot 81 + 6 \cdot 27 + 8 \cdot 9 = \frac{1368}{24} = 57$.

Variante: q Farben

$$\curvearrowright |G\backslash\Omega| = \frac{1}{24}(q^6 + 6q^3 + 3q^4 + 6q^3 + 8q^2) = \frac{1}{24}(q^6 + 3q^4 + 12q^3 + 8q^2)\,.$$

Eine ausgezeichnete Symmetrie ist die Abbildung $-\mathrm{id}_V$, die jede Seite mit der gegenüberliegenden Seite vertauscht.

Spiegelung		Fixpunkte	Vielfachheit
	$-\mathrm{id}_V$	$o \quad u$ $v \quad h$ $l \quad r$	$3^3 = 27$ 1
	$\pm 90° \cdot (-\mathrm{id}_V)$	$o \quad h \quad u \quad v$ $l \quad r$	$3^2 = 9$ 6

Spiegelung		Fixpunkte		Vielfachheit
	$180° \cdot (-\mathrm{id}_V)$	o u v h l r	$3^5 = 243$	3
	$180° \cdot (-\mathrm{id}_V)$	o r v h l u	$3^4 = 81$	6
	$\pm 120° \cdot (-\mathrm{id}_V)$	o, r, v, u, l, h	3	8

Nach Burnside ist die Bahnenzahl:

$$\frac{1}{48}(729 + 6 \cdot 27 + 3 \cdot 81 + 6 \cdot 27 + 8 \cdot 9 + 1 \cdot 27 + \underbrace{6 \cdot 9 + 3 \cdot 243 + 6 \cdot 81 + 8 \cdot 3}_{\text{durch Betrachten der Spiegelungen hinzugekommen}}) = 56\,.$$

8.7 Satz (Satz von Cauchy) *Seien G eine endliche Gruppe und $p \in \mathbb{P}$ mit $p \mid |G|$. Dann teilt p auch die Anzahl der Elemente $g \in G$ mit $g^p = 1$. Insbesondere existiert ein $1 \neq g \in G$ mit $g^p = 1$ (d.h. ein Element der* Ordnung *p).*

Beweis. Für $\Omega := \{(g_0, \ldots, g_{p-1}) \in G^p : g_0 \ldots g_{p-1} = 1\}$ gilt offenbar: $|\Omega| = |G|^{p-1}$. Die Gruppe $Z := \mathbb{Z}/p\mathbb{Z}$ der Ordnung p operiert auf Ω durch:

$$(k + p\mathbb{Z}) * (g_0 \ldots g_{p-1}) := (g_k, \ldots, g_{p-1}, g_0, \ldots, g_{k-1})\,.$$

Wegen

$$g_k \ldots g_{p-1} g_0 \ldots g_{k-1} = g_k \ldots g_{p-1} \underbrace{g_0 \ldots g_{p-1}}_{=1} (g_k \ldots g_{p-1})^{-1} = 1$$

ist tatsächlich $(g_k, \ldots, g_{p-1}, g_0, \ldots, g_{k-1}) \in \Omega$. Das Element $0 + p\mathbb{Z} \in Z$ lässt alle $|G|^{p-1}$ Elemente in Ω fest. Jedes andere Element $k + p\mathbb{Z}$ in Z lässt nur die Elemente der Form $(g, g, \ldots, g)$ mit $g^p = 1$ fest. Deren Anzahl sei n. Nach Burnside ist also die Anzahl der Bahnen von Z auf Ω gleich

$$\frac{1}{p}\left(|G|^{p-1} + (p-1)n\right)\,,\ \text{d.h.}\ \frac{1}{p}\left(|G|^{p-1} + (p-1)n\right) \in \mathbb{Z}\,.$$

Also ist n durch p teilbar. $\square$

Beispiel Jede Gruppe G mit $|G| = 1000$ enthält also Elemente der Ordnung 2 und Elemente der Ordnung 5.

8.8 Bemerkung Jede endliche Gruppe G operiert auf sich selbst durch *Konjugation*: $g * x := gxg^{-1}$ $(g, x \in G)$. Denn für $g, h, x \in G$ ist

$$g * (h * x) = g(hxh^{-1)}g^{-1} = ghx \underbrace{h^{-1}g^{-1}}_{(gh)^{-1}} = (gh) * x\,.$$

und $1 * x = 1x1^{-1} = x$. Für $x \in G$ heißt die Bahn

$$\mathrm{cl}_G(x) := \{gxg^{-1} : g \in G\}$$

Konjugationsklasse von x in G. Man nennt

$$Z(G) := \{x \in G : gxg^{-1} = x \text{ für alle } g \in G\} = \{x \in G : gx = xg \text{ für alle } g \in G\}$$

Zentrum von G. Man zeigt leicht, dass $Z(G)$ eine Untergruppe von G ist. Nach Definition ist $Z(G)$ die Menge der Fixpunkte der Operation, d.h. die Vereinigung der 1-elementigen Konjugationsklassen von G. Für $x \in G$ heißt $G_x = C_G(x)$ *Zentralisator* von x in G. Also:

$$C_G(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} \leq G \text{ und } |G : C_G(x)| = |\mathrm{cl}_G(x)|\,.$$

Man setzt $\mathrm{Cl}(G) := \{\mathrm{cl}_G(x) : x \in G\}$ und nennt $|\mathrm{Cl}(G)|$ *Klassenzahl* von G. Ist R ein Repräsentantensystem für die Konjugationsklassen von G, so besagt die Bahnengleichung:

$$|G| = \sum_{x \in R} |G : C_G(x)| = |Z(G)| + \sum_{x \in R \setminus Z(G)} |G : C_G(x)| \qquad \text{(Klassengleichung)}$$

Also

$$1 = \sum_{x \in R} \frac{1}{|C_G(x)|} \qquad (\star)$$

mit $C_G(x) \leq G = C_G(1)$ für $x \in R$.

Beispiel

(i) Im Fall $|\mathrm{Cl}(G)| = 1$ ist $|R| = 1$, d.h. $R = \{1\}$. Also $(\star)$:

$$1 = \frac{1}{|C_G(1)|} = \frac{1}{|G|} \text{ d.h. } |G| = 1\,.$$

Daher: $G = \{1\}$.

(ii) Im Fall $|\mathrm{Cl}(G)| = 2$ ist $|R| = 2$, d.h. $R = \{1, a\}$. Also $(\star)$:

$$1 = \frac{1}{|C_G(1)|} + \frac{1}{|C_G(a)|} = \frac{1}{|G|} + \frac{1}{|C_G(a)|} \leq \frac{2}{|C_G(a)|}\,,\ \text{d.h. } |C_G(a)| \leq 2\,.$$

Daher $|C_G(a)| = 2$, d.h. $1 = \frac{1}{|G|} + \frac{1}{2}$, d.h. $|G| = 2$.

(iii) Im Fall $|\mathrm{Cl}(G)| = 3$ ist $|R| = 3, R = \{1, a, b\}$.Œ sei $|C_G(b)| \leq |C_G(a)| \leq |C_G(1)|$. Also ($\star$):

$$1 = \frac{1}{|C_G(1)|} + \frac{1}{|C_G(a)|} + \frac{1}{|C_G(b)|} \leq \frac{3}{|C_G(b)|}\,,\ \text{d.h. } |C_G(b)| \leq 3\,.$$

Also: $|C_G(b)| \in \{2, 3\}$. Daher:

$$1 \leq \frac{1}{|C_G(1)|} + \frac{1}{|C_G(a)|} + \frac{1}{2}\,,$$

d.h.

$$\frac{1}{2} \leq \frac{1}{|G|} + \frac{1}{|C_G(a)|} \leq \frac{2}{|C_G(a)|}\,,\ \text{d.h. } |C_G(a)| \leq 4\,,\ \text{d.h. } |C_G(a)| \in \{3, 4\}\,.$$

Daher:

$$\frac{1}{2} \leq \frac{1}{|G|} + \frac{1}{3}\,,\ \text{d.h. } \frac{1}{6} \leq \frac{1}{|G|}\,,\ \text{d.h. } |G| \leq 6\,.$$

(iv) So kann man fortfahren.[18]

8.9 Bemerkung Jede endliche Gruppe G operiert auf der Menge $\mathcal{L}(G) =: \Omega$ aller Untergruppen von G durch Konjugation:

$$g * H := gHg^{-1} \quad (g \in G, H \in \mathcal{L}(G))\,.$$

Man zeigt leicht, dass mit H auch gHg^{-1} eine Untergruppe von G ist. Für $H \in \mathcal{L}(G)$ hat die Bahn von H unter G die Form

$$\mathrm{cl}_G(H) := \{gHg^{-1} : g \in G\} \quad (\textit{Konjugationsklasse} \text{ von } H \text{ in } G)\,.$$

Der Stabilisator von H in G hat die Form

$$N_G(H) := \{g \in G : gHg^{-1} = H\} \quad (\textit{Normalisator} \text{ von } H \text{ in } G)\,.$$

Dann ist $N_G(H) \leq G$ eine Untergruppe und $|G : N_G(H)| = |\mathrm{cl}_G(H)|$. Offenbar ist $H \subseteq N_G(H)$. Nach Definition ist H ein Normalteiler von $N_G(H)$.

8.9 Satz *Sei $p \in \mathbb{P}$ und G eine endliche p-Gruppe[19]. Aus $G \neq \{1\}$ folgt $Z(G) \neq \{1\}$.*

Beweis. Sei R ein Repräsentantensystem für die Konjugationsklassen von G. Dann besagt die Klassengleichung:

$$|G| = |Z(G)| + \sum_{x \in R \setminus Z(G)} |G : C_G(x)|\,.$$

Dabei: $p \mid |G|$ und $p \mid |G : C_G(x)|$ für alle $x \in R \setminus Z(G)$. Also: $p \mid |Z(G)|$, d.h. $Z(G) \neq \{1\}$. □

[18] D.h. wenn die Anzahl der Konjugationsklassen vorgegeben ist, so ist $|G|$ beschränkt.
[19] D.h. $|G|$ ist eine p-Potenz.

8.9 Beispiel Sei G eine Gruppe und $|G| = p^2$ für ein $p \in \mathbb{P}$. Aus Satz 8.9 folgt: $|Z(G)| \neq 1$, d.h. $|Z(G)| \geq p$ nach Lagrange. Angenommen $|Z(G)| = p$. Sei $g \in G \setminus Z(G)$. Dann: $H \coloneqq \{g^i z : i \in \mathbb{Z}, z \in Z(G)\} \leq G$.[20] Ferner $|H| > p$, also $|H| = p^2$ nach Lagrange, d.h. $H = G$. Dann:

$$g^i z g^j y = g^{i+j} zy = g^j g^i yz = g^j y g^i z \quad (y, z \in Z(G),\, i, j \in \mathbb{Z})\,.$$

Also: G abelsch, d.h. $Z(G) = G$ und $|Z(G)| = p^2$. Dies ist ein Widerspruch. Also ist $|Z(G)| = p^2$ nach Lagrange, d.h. $G = Z(G)$ abelsch. Fazit: Gruppen der Ordnung p^2 ($p \in \mathbb{P}$) sind abelsch.

8.10 Satz *Jede Primzahl p der Form $p = 4k + 1$ ($k \in \mathbb{N}$) lässt sich als Summe von zwei Quadratzahlen schreiben.*

Beispiel

$$5 = 2^2 + 1^2,\ 13 = 3^2 + 2^2,\ 17 = 4^2 + 1^2,\ 29 = 5^2 + 2^2,\ 37 = 6^2 + 1^2,\ 41 = 5^2 + 4^2\,.$$

Beweis. Betrachte $\Omega \coloneqq \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$. Dann ist

$$\sigma\colon \Omega \to \Omega,\ (x, y, z) \mapsto (x, z, y) \text{ bijektiv mit } \sigma^2 = \mathrm{id}_\Omega\,.$$

Daher ist $G \coloneqq \{\mathrm{id}_\Omega, \sigma\}$ eine Gruppe der Ordnung 2, die auf Ω operiert. Die Bahnen haben also Länge 1 oder 2. Jede Bahn der Länge 1 hat die Form $\{(x, y, y)\}$ mit $p = x^2 + 4y^2 = x^2 + (2y)^2$. Daher genügt es zu zeigen: $|\Omega|$ ungerade. Dazu betrachte man

$$\tau\colon \Omega \to \Omega,\ (x, y, z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z), & \text{falls } x < y - z, \\ (2y - x,\ y,\ x - y + z), & \text{falls } y - z < x < 2y, \\ (x - 2y,\ x - y + z,\ y), & \text{falls } x > 2y\,. \end{cases}$$

(Beachte: Die Fälle $x = y - z$ und $x = 2y$ treten nicht auf!) Man rechnet leicht nach, dass tatsächlich $\tau(\Omega) \subseteq \Omega$ gilt. Ferner rechnet man nach: $\tau^2 = \mathrm{id}_\Omega$. Daher operiert die Gruppe $H \coloneqq \{\mathrm{id}_\Omega, \tau\}$ auf Ω. Jede Bahn hat Länge 1 oder 2. Hat die Bahn von (x, y, z) Länge 1, dann ist $(x, y, z) = \tau(x, y, z) = (2y - x, y, x - y + z)$, d.h. $x = 1$, $p = x + 4z = 1 + 4z$, also $z = k$. Also: $(x, y, z) = (1, 1, k)$. Daher ist tatsächlich $\{(1, 1, k)\}$ die einzige Bahn der Länge 1. Also: $|\Omega|$ ungerade.[21] □

Bemerkung Primzahlen der Form $p = 4k + 3$ lassen sich nie als Summe von zwei Quadratzahlen schreiben; denn ist $a \in \mathbb{Z}$, so gilt im Fall $a = 2m$: $a^2 = 4m^2$. Im Fall $a = 2m + 1$ ist $a^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1$, d.h.

$$x^2 + y^2 = 4k + \begin{cases} 0 \\ 1 \\ 2 \end{cases} \qquad (x, y \in \mathbb{Z}).$$

[20] $g^i z g^j y = g^i g^j zy = g^{i+j} zy$ für $y, z \in Z(G)$, $i, j \in \mathbb{Z}$.
[21] Jede andere Bahn hat Länge 2.

9 Ergänzungen zu den Gruppenoperationen

9.1 Bemerkung Sei $G \times \Omega \to \Omega$, $(g, \alpha) \mapsto g * \alpha$, eine Operation. Die Operation heißt transitiv, falls nur eine Bahn existiert, d.h. falls zu je zwei Elementen $\alpha, \beta \in \Omega$ ein $g \in G$ existiert mit $g * \alpha = \beta$. Ggf. gilt:

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_\Omega(g)| = 1 \,.$$

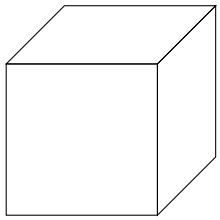
Sei $1 \leq k \leq n := |\Omega|$ und $\Omega_k := \{(\alpha_1, \ldots, \alpha_k) : \alpha_1, \ldots, \alpha_k \in \Omega \text{ paarweise verschieden}\}$. Dann ist $|\Omega_k| = n(n-1)\ldots(n-k+1)$. Ferner operiert G auf Ω_k durch

$$g * (\alpha_1, \ldots, \alpha_k) := (g * \alpha_1, \ldots, g * \alpha_k) \text{ für } g \in G,\ (\alpha_1, \ldots, \alpha_k) \in \Omega_k \,.$$

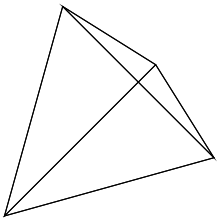
Die Operation von G auf Ω heißt *k-transitiv*, wenn die Operation von G auf Ω_k transitiv ist. Das bedeutet, dass zu je zwei Elementen $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega_k$ ein $g \in G$ mit $g * \alpha_1 = \beta_1$, $g * \alpha_2 = \beta_2$, $\ldots$, $g * \alpha_k = \beta_k$ existiert.[22]

Beispiel

(i) Die Gruppe der Würfeldrehungen operiert transitiv auf den Würfelseiten, aber nicht 2-transitiv.[23]



(ii) Die Gruppe der Drehungen eines Tetraeders ist 2-transitiv auf den Seiten.



(iii) $\mathrm{Sym}(\Omega)$ operiert für $k = 1, \ldots, |\Omega|$ k-transitiv auf Ω; denn für

$$(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega_k$$

existiert stets eine Permutation der Form

$$\begin{pmatrix} \alpha_1 & \ldots & \alpha_k & \alpha_{k+1} & \ldots & \alpha_n \\ \beta_1 & \ldots & \beta_k & \beta_{k+1} & \ldots & \beta_n \end{pmatrix}.$$

[22] Daher: "transitiv" = "1-transitiv".

[23] Man kann jede Seite in jede andere überführen, aber ein Paar gegenüberliegender Seiten nicht in ein Paar benachbarter Seiten.

9.1 Satz *Sei $G \times \Omega \to \Omega$, $(g, \alpha) \mapsto g * \alpha$ eine transitive Operation, $2 \leq k \leq n = |\Omega|$ und $\gamma \in \Omega$. Dann:*

$$G \text{ operiert } k\text{-transitiv auf } \Omega \iff G_\gamma \text{ operiert } (k-1)\text{-transitiv auf } \Omega \setminus \{\gamma\} =: \Omega'.$$

Beweis.

"$\Rightarrow$" Die Operation von G auf Ω sei k-transitiv. Sind

$$(\alpha_1, \ldots, \alpha_{k-1}), (\beta_1, \ldots, \beta_{k-1}) \in \Omega'_{k-1},$$

dann sind $(\alpha_1, \ldots, \alpha_{k-1}, \gamma)$ bzw. $(\beta_1, \ldots, \beta_{k-1}, \gamma) \in \Omega_k$. Daher existiert ein $g \in G$ mit $g * \alpha_1 = \beta_1, \ldots, g * \alpha_{k-1} = \beta_{k-1}$, $g * \gamma = \gamma$, insbesondere: $g \in G_\gamma$. Daher operiert G_γ $(k-1)$-transitiv auf Ω'.

"$\Leftarrow$" Die Operation von G_γ auf Ω' sei $(k-1)$-transitiv. Seien

$$(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k) \in \Omega_k\,.$$

Da G transitiv auf Ω operiert, existiert ein $g \in G$ mit $g * \alpha_k = \gamma$. Analog existiert ein $h \in G$ mit $h * \beta_k = \gamma$. Dann: $(g * \alpha_1, \ldots, g * \alpha_{k-1}), (h * \beta_1, \ldots, h * \beta_{k-1}) \in \Omega'_{k-1}$. Daher existiert ein $a \in G_\gamma$ mit $a * (g * \alpha_i) = h * \beta_i$ $(i = 1, \ldots, k-1)$. Dann:

$$\begin{aligned}(h^{-1}ag) * \alpha_i &= h^{-1} * a * g * \alpha_i = h^{-1} * h * \beta_i = \beta_i\,,\\ (h^{-1}ag) * \alpha_k &= h^{-1} * a * \gamma = h^{-1} * \gamma = \beta_k\,.\end{aligned}$$

Also operiert G k-transitiv auf Ω.

□

9.2 Satz *Sei $G \times \Omega \to \Omega$, $(g, \alpha) \mapsto g * \alpha$ eine Operation und $n = |\Omega|$. Es sei ferner $B(n)$ die n-te Bellzahl, d.h. die Anzahl der Partitionen von Ω. Für $k = 1, \ldots, n$ gilt dann:*

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_\Omega(g)|^k \geq B(k)\,.$$

Gleichheit gilt genau dann, wenn die Operation k-transitiv ist.

Beweis. (Induktion nach k) Für $k = 1$ ist

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_\Omega(g)| = |G \backslash \Omega| \quad \text{(Burnside) und } B(1) = 1\,,$$

d.h. die Aussagen gelten. Sei also $2 \leq k \leq n$ und

$$\Delta \coloneqq \{(g, \alpha_1, \ldots, \alpha_k) \in G \times \Omega^k : g * \alpha_1 = \alpha_1, \ldots, g * \alpha_k = \alpha_k\}\,.$$

Dann ist einerseits:

$$|\Delta| = \sum_{g \in G} |\mathrm{Fix}_\Omega(g)|^k\,.$$

Andererseits:

$$\begin{aligned}|\Delta| &= \sum_{\alpha_k\in\Omega} |\{(g,\alpha_1,\ldots,\alpha_{k-1}) \in G_{\alpha_k} \times \Omega^{k-1} : g*\alpha_1 = \alpha_1,\ldots,g*\alpha_{k-1}=\alpha_{k-1}\}| \\ &= \sum_{\gamma\in\Omega}\sum_{g\in G_\gamma} |\mathrm{Fix}_\Omega(g)|^{k-1}\,.\end{aligned}$$

Für $\gamma \in \Omega$ sei $\Omega_\gamma := \Omega \setminus \{\gamma\}$. Dann:

$$\begin{aligned}|\Delta| &= \sum_{\gamma\in\Omega}\sum_{g\in G_\gamma} \big(|\mathrm{Fix}_{\Omega_\gamma}(g)+1|\big)^{k-1} = \sum_{\gamma\in\Omega}\sum_{g\in G_\gamma}\sum_{j=0}^{k-1}\binom{k-1}{j}|\mathrm{Fix}_{\Omega_\gamma}(g)|^j \\ &= \sum_{\gamma\in\Omega}\sum_{j=0}^{k-1}\binom{k-1}{j}\sum_{g\in G_\gamma}|\mathrm{Fix}_{\Omega_\gamma}(g)|^j \geq \sum_{\gamma\in\Omega}\sum_{j=0}^{k-1}\binom{k-1}{j}|G_\gamma|B(j) \\ &= \sum_{\gamma\in\Omega}|G_\gamma|\sum_{j=0}^{k-1}\binom{k-1}{j}B(j) \overset{4.5}{=} \sum_{\gamma\in\Omega}|G_\gamma|B(k) \\ &= B(k)\sum_{\gamma\in\Omega}\frac{|G|}{|\mathrm{Orb}_G(\gamma)|} = B(k)|G|\sum_{\gamma\in\Omega}\frac{1}{|\mathrm{Orb}_G(\gamma)|} \\ &= B(k)|G||G\backslash\Omega|\end{aligned}$$

Operiert G k-transitiv auf Ω, so operiert G transitiv auf Ω, also $|G\backslash\Omega| = 1$. Ferner operiert G_γ $(k-1)$-transitiv auf Ω_γ, d.h. in der obigen Ungleichungskette tritt dann stets die Gleichheit auf. Es bleibt noch zu zeigen:

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_\Omega(g)|^k = B(k) \Longrightarrow G \text{ operiert } k\text{-transitiv auf } \Omega.$$

Aus

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_\Omega(g)|^k = B(k)$$

folgt $|G\backslash\Omega| = 1$, d.h. G operiert transitiv auf Ω. Ferner:

$$\frac{1}{|G_\gamma|}\sum_{g\in G_\gamma}|\mathrm{Fix}_{\Omega_\gamma}(g)|^j = B(j) \text{ für } j = 1,\ldots,k-1\,.$$

Nach Induktion operiert G_γ $(k-1)$-transitiv auf Ω_γ. Nach Satz 9.1 operiert G k-transitiv auf Ω. □

Bemerkung Wieviele Elemente in $\mathrm{Sym}(\Omega)$ haben genau j Fixpunkte ($|\Omega| = n$)? Es gibt genau $\binom{n}{j}$ Möglichkeiten für die Fixpunkte. Die restlichen $n-j$ Elemente werden fixpunktfrei permutiert. Dafür gibt es D_{n-j} Möglichkeiten. Es gibt also genau $\binom{n}{j}D_{n-j}$ Elemente in $\mathrm{Sym}(\Omega)$ mit j Fixpunkten. Daher:

$$\sum_{g\in\mathrm{Sym}(\Omega)}|\mathrm{Fix}_\Omega(g)|^k = \sum_{j=0}^{n}\binom{n}{j}D_{n-j}j^k = \sum_{j=1}^{n}\binom{n}{j}D_{n-j}j^k \ (k=1,\ldots,n)\,.$$

Aus Satz 9.2 folgt:

$$B(k) = \frac{1}{n!}\sum_{j=1}^{n}\binom{n}{j}D_{n-j}j^k = \sum_{j=1}^{n}\frac{1}{j!(n-j)!}D_{n-j}j^k\,.$$

9.3 Definition Graphen $\Gamma = (V, E)$, $\Gamma' = (V', E')$ heißen *isomorph*, falls eine Bijektion $f\colon V \to V'$ existiert, sodass für alle $a, b \in V$ gilt:

$$\{a, b\} \in E \Longleftrightarrow \{f(a), f(b)\} \in E'\,.$$

Bemerkung Meist nimmt man Œ an: $V = \{1, \ldots, n\} = V'$. Graphen entsprechen dann Färbungen von $\binom{V}{2}$; dabei ist eine *Färbung* von $\binom{V}{2}$ eine Abbildung $\binom{V}{2} \to \{0, 1\}$. $G = \mathrm{Sym}(n)$ operiert auf $\binom{V}{2}$ durch $g * \{a, b\} = \{g(a), g(b)\}$ für $g \in G$ und $\{a, b\} \in \binom{V}{2}$. Ferner operiert G auf $A \coloneqq \mathrm{Abb}\big(\binom{V}{2}, \{0, 1\}\big)$ durch $(g * f)(\{a, b\}) \coloneqq f(\{g^{-1}(a), g^{-1}(b)\})$. Beachte:

$$\begin{aligned}\big(g * (h * f)\big)\big(\{a, b\}\big) &= \big(h * f\big)\big(\{g^{-1}(a), g^{-1}(b)\}\big) = f\big(\{(h^{-1}g^{-1})(a), (h^{-1}g^{-1})(b)\}\big)\\ &= f\big(\{(gh)^{-1}(a), (gh)^{-1}(b)\}\big) = \big((gh) * f\big)(\{a, b\}\big)\,.\end{aligned}$$

Dabei:

$$\begin{aligned}f \in \mathrm{Fix}_A(g) &\Leftrightarrow g * f = f \Leftrightarrow (g * f)(\{a, b\}) = f(\{a, b\}) \text{ für alle } \{a, b\} \in \tbinom{V}{2}\\ &\Leftrightarrow f \text{ konstant auf den Bahnen von } \langle g\rangle \text{ auf } \tbinom{V}{2}\,.\end{aligned}$$

Daher: $|\mathrm{Fix}_A(g)| = 2^{\beta(g)}$, dabei ist $\beta(g)$ die Anzahl der Bahnen von $\langle g\rangle$ auf $\binom{V}{2}$. Also ist nach Burnside die Anzahl der Isomorphieklassen von $\Gamma = (V, E)$ mit $V = \{1, \ldots, n\}$ gleich

$$\frac{1}{n!}\sum_{g \in \mathrm{Sym}(V)} 2^{\beta(g)}\,.$$

9.4 Bemerkung In Anwendungen verwendet man für die Elemente in $\mathrm{Sym}(V)$ die *Zyklenschreibweise*. Z.B. steht $(\alpha_1, \ldots, \alpha_k)$ für die Permutation, die α_1 auf α_2, α_2 auf α_3,…,α_k auf α_1 abbildet. Man zeigt leicht, dass man jedes $g \in \mathrm{Sym}(V)$ als Produkt disjunkter Zyklen schreiben kann, z.B.

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

Disjunkte Zyklen sind so stets vertauschbar. Die Längen der bei einem $g \in \mathrm{Sym}(V)$ auftretenden Zyklen sind durch g eindeutig bestimmt: es sind gerade die Längen der Bahnen von $\langle g\rangle$ auf V. Sind $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k$ die auftretenden Zyklenlängen, dann ist $\lambda_1 + \lambda_2 + \ldots + \lambda_k = n$, d.h. $\lambda = (\lambda_1, \ldots, \lambda_n)$ ist eine Partition von n ($\lambda \vdash n$). Man nennt λ den *(Zyklen-)Typ* von g.

Beispiel (Graphen mit 5 Ecken) Wir sortieren die Elemente von $g \in \mathrm{Sym}(5)$ nach ihrem Typ ($5! = 120$).

Typ	Anzahl der g's	Bahnen von $\langle g \rangle$ auf $\binom{V}{2}$	Σ
$\lambda = (5)$ $\curvearrowright g = (\alpha, \beta, \gamma, \delta, \varepsilon)$	$\frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{4} = 24$	$\{\alpha,\beta\}, \{\beta,\gamma\}, \{\gamma,\delta\}, \{\delta,\varepsilon\}, \{\alpha,\varepsilon\}$ $\{\alpha,\gamma\}, \{\beta,\delta\}, \{\gamma,\varepsilon\}, \{\alpha,\delta\}, \{\beta,\varepsilon\}$	2
$\lambda = (4,1)$ $\curvearrowright g = (\alpha, \beta, \gamma, \delta)(\varepsilon)$	$\frac{4 \cdot 3 \cdot 2 \cdot 1}{4} \cdot 5 = 30$	$\{\alpha,\beta\}, \{\beta,\gamma\}, \{\gamma,\delta\}, \{\alpha,\delta\}$ $\{\alpha,\gamma\}, \{\beta,\delta\}$ $\{\alpha,\varepsilon\}, \{\beta,\varepsilon\}, \{\gamma,\varepsilon\}, \{\delta,\varepsilon\}$	3
$\lambda = (3,2)$ $\curvearrowright g = (\alpha, \beta, \gamma)(\delta, \varepsilon)$	$\frac{5 \cdot 4 \cdot 3}{3} \cdot 1 = 20$	$\{\alpha,\beta\}, \{\beta,\gamma\}, \{\alpha,\gamma\}$ $\{\alpha,\delta\}, \{\beta,\varepsilon\}, \{\gamma,\delta\}, \{\alpha,\varepsilon\}, \{\beta,\delta\}, \{\gamma,\varepsilon\}$ $\{\delta,\varepsilon\}$	3
$\lambda = (3,1,1)$ $\curvearrowright g = (\alpha, \beta, \gamma)(\delta)(\varepsilon)$	$\frac{5 \cdot 4 \cdot 3}{3} = 20$	$\{\alpha,\beta\}, \{\beta,\gamma\}, \{\alpha,\gamma\}$ $\{\alpha,\delta\}, \{\beta,\delta\}, \{\gamma,\delta\}$ $\{\alpha,\varepsilon\}, \{\beta,\varepsilon\}, \{\gamma,\varepsilon\}$ $\{\delta,\varepsilon\}$	4
$\lambda = (2,2,1)$ $\curvearrowright g = (\alpha, \beta)(\gamma, \delta)(\varepsilon)$	$\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2} \,/\, 2 = 15$	$\{\alpha,\beta\}$ $\{\alpha,\delta\}, \{\beta,\gamma\}$ $\{\gamma,\delta\}$ $\{\alpha,\gamma\}, \{\beta,\delta\}$ $\{\alpha,\varepsilon\}, \{\beta,\varepsilon\}$ $\{\gamma,\varepsilon\}, \{\delta,\varepsilon\}$	6
$\lambda = (2,1,1,1)$ $\curvearrowright g = (\alpha, \beta)(\gamma)(\delta)(\varepsilon)$	$\binom{5}{2} = 10$	$\{\alpha,\beta\}$ $\{\alpha,\delta\}, \{\beta,\delta\}$ $\{\gamma,\delta\}$ $\{\gamma,\varepsilon\}$ $\{\alpha,\gamma\}, \{\beta,\gamma\}$ $\{\alpha,\varepsilon\}, \{\beta,\varepsilon\}$ $\{\delta,\varepsilon\}$	7
$\lambda = (1,1,1,1,1)$	1		10

Nach Burnside ist die Anzahl der Isomorphieklassen gleich

$$\frac{1}{120}(24 \cdot 2^2 + 30 \cdot 2^3 + 20 \cdot 2^3 + 20 \cdot 2^4 + 15 \cdot 2^6 + 10 \cdot 2^7 + 1 \cdot 2^{10}) = 34\,.$$

9.5 Bemerkung Sei $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n$. Wie viele Elemente $g \in \mathrm{Sym}(n)$ haben den Typ λ? Für $i = 1, \ldots, n$ sei $m_i := |\{j : \lambda_j = i\}|$, d.h. λ enthält m_1 1'en, m_2 2'en, m_3 3'en usw., z.B. sind für $\lambda = (3,3,2,2,2,1,1) \vdash 14$ $m_1 = 2$, $m_2 = 3$, $m_3 = 2$; $m_i = 0$ sonst. Ein $g \in \mathrm{Sym}(n)$ vom Typ λ hat also die Form

$$\underbrace{()\ldots()}_{m_1}\ \underbrace{(\ ,\ )\ldots(\ ,\ )}_{m_2}\ \underbrace{(\ ,\ ,\ )\ldots(\ ,\ ,\ )}_{m_3}\ldots\,.$$

Für die Verteilung der Zahlen $1, \ldots, n$ auf die Klammern gibt es $n!$ Möglichkeiten. Allerdings kann man jeden r-Zyklus $(\alpha_1, \ldots, \alpha_r)$ auf r verschiedene Arten schreiben. Ferner kann man Zyklen gleicher Länge miteinander vertauschen. Es existieren also genau

$$\frac{n!}{1^{m_1}\, m_1!\; 2^{m_2}\, m_2!\; 3^{m_3}\, m_3! \ldots} \text{ Elemente } g \in \mathrm{Sym}(n) \text{ vom Typ } \lambda.$$

Beispiel Für $\lambda = (3, 2, 2) \vdash 7$ sind $m_1 = 0$, $m_2 = 2$ und $m_3 = 1$. Die Anzahl der $g \in \mathrm{Sym}(7)$ vom Typ λ beträgt

$$\frac{7!}{1^0\, 0!\; 2^2\, 2!\; 3^1\, 1!} = 210\,.$$

10 Formale Potenzreihen und erzeugende Funktionen

10.1 Definition Eine *formale Potenzreihe* ist eine unendliche Folge $\alpha = (a_0, a_1, a_2, \dots)$ mit a_0,a_1,a_2,$\dots \in \mathbb{R}$.

Bemerkung Für formale Potenzreihen $\alpha = (a_0, a_1, a_2, \dots)$,$\beta = (b_0, b_1, b_2, \dots)$ sind auch

$$\alpha + \beta \coloneqq (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)\,,$$
$$\alpha \cdot \beta \coloneqq (c_0, c_1, c_2, \dots) \text{ mit } c_k \coloneqq \sum_{i=0}^{k} a_i b_{k-i} \ (k \in \mathbb{N}_0)$$

formale Potenzreihen.[24] Man zeigt leicht, dass die Menge der formalen Potenzreihen so ein kommutativer Ring wird, der *formale Potenzreihenring* $\mathbb{R}[\![X]\!]$. Einselement ist $(1, 0, 0, \dots)$. Statt $\alpha = (a_0, a_1, a_2)$ schreibt man meist:

$$\sum_{i=0}^{\infty} a_i X^i\,.$$

Für

$$\beta = \sum_{j=0}^{\infty} b_j X^j \in \mathbb{R}[\![X]\!]$$

gilt dann:

$$\alpha = \beta \Longleftrightarrow a_i = b_i \text{ für } i \in \mathbb{N}_0,$$
$$\alpha + \beta = \sum_{i=0}^{\infty} (a_i + b_i) X^i\,,$$
$$\alpha \cdot \beta = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k\,.$$

Den Polynomring $\mathbb{R}[X]$ fasst man als Teilmenge[25] von $\mathbb{R}[\![X]\!]$ auf. Insbesondere ist $\mathbb{R}$ selbst ein Teilring von $\mathbb{R}[\![X]\!]$.[26]

Beispiel

$$\exp(X) \coloneqq \sum_{n=0}^{\infty} \frac{X^n}{n!},\ \sum_{n=0}^{\infty} X^n,\ \sum_{n=0}^{\infty} n! X^n \in \mathbb{R}[\![X]\!]\,.$$

10.2 Definition Ein $\alpha \in \mathbb{R}[\![X]\!]$ heißt *invertierbar*, falls ein $\beta \in \mathbb{R}[\![X]\!]$ mit $\alpha\beta = 1$ existiert.

---

[24] $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$,$\dots$

[25] genauer: Teilring.

[26] $a \in \mathbb{R} \longleftrightarrow aX^0 + 0X^1 + 0X^2 + \dots \in \mathbb{R}[\![X]\!]$.

Satz *Ein Element*

$$\alpha = \sum_{i=0}^{\infty} a_i X^i \in \mathbb{R}[\![X]\!]$$

ist genau dann invertierbar, wenn $a_0 \neq 0$ *gilt.*

Beweis.

"$\Rightarrow$" Sei

$$\beta = \sum_{j=0}^{\infty} b_j X^j \in \mathbb{R}[\![X]\!] \text{ mit } 1 = \alpha\beta = \sum_{k=0}^{\infty} \Big(\sum_{i=0}^{k} a_i b_{k-i} \Big) X^k \,.$$

Koeffizientenvergleich bei X^0 liefert $1 = a_0 b_0$, d.h. $a_0 \neq 0$.

"$\Leftarrow$" Sei $a_0 \neq 0$. Gesucht ist ein

$$\beta = \sum_{j=0}^{\infty} b_j X^j \in \mathbb{R}[\![X]\!] \text{ mit } \alpha\beta = 1 \,,$$

d.h.

$$\begin{aligned} &a_0 b_0 = 1 \\ &a_0 b_1 + a_1 b_0 = 0 \\ &a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \\ &\vdots \\ &a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0 = 0 \\ &\vdots \end{aligned}$$

Daraus kann man sukzessive $b_0, b_1, b_2, \ldots$ berechnen ($b_0 = \frac{1}{a_0}$, $b_1 = \frac{-a_1 b_0}{a_0}$,...).

□

Bemerkung Wie üblich ist $\mathbb{R}[\![X]\!]^\times = \{\alpha \in \mathbb{R}[\![X]\!] : \alpha \text{ invertierbar}\}$ eine Gruppe bzgl. der Multiplikation. Das Inverse von $\alpha \in \mathbb{R}[\![X]\!]^\times$ wird mit α^{-1} oder $\frac{1}{\alpha}$ bezeichnet.

Beispiel

$$\sum_{n=0}^{\infty} X^n \in \mathbb{R}[\![X]\!] \text{ mit } \left(\sum_{n=0}^{\infty} X^n \right)^{-1} = 1 - X; \text{ denn}$$

$$(1 - X) \sum_{n=0}^{\infty} X^n = \sum_{n=0}^{\infty} X^n - \sum_{n=0}^{\infty} X^{n+1} = 1$$

10.3 Definition Für

$$\alpha = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{R}[\![X]\!]$$

definiert man die *formale Ableitung* durch

$$\alpha' = \sum_{n=1}^{\infty} n a_n X^{n-1} \in \mathbb{R}[\![X]\!] \,.$$

Bemerkung Man zeigt leicht, dass dann wie üblich gilt:

$$\boxed{(\alpha+\beta)' = \alpha' + \beta'} \text{ und } \boxed{(\alpha\beta)' = \alpha'\beta + \alpha\beta'} \text{ für } \alpha, \beta \in \mathbb{R}[\![X]\!].$$

Ist $\alpha \in \mathbb{R}[\![X]\!]^\times$, so ist $1 = \alpha\alpha^{-1}$, also $0 = 1' = (\alpha\alpha^{-1})' = \alpha'\alpha^{-1} + \alpha(\alpha^{-1})'$, d.h.

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

Beispiel

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

10.4 Definition Für jede reelle Folge $(a_n)_{n\in\mathbb{N}_0}$ heißt

$$a(X) \coloneqq \sum_{n=0}^{\infty} a_n X^n \text{ } \textit{erzeugende Funktion} \text{ von } (a_n)_{n\in\mathbb{N}_0}.$$

Beispiel $a_n = n$ für $n \in \mathbb{N}_0$. Dann:

$$\begin{aligned} a(X) &= \sum_{n=0}^{\infty} nX^n = \sum_{n=1}^{\infty} nX^n = X\sum_{n=1}^{\infty} nX^{n-1} = X\left(\sum_{n=0}^{\infty} X^n\right)' \\ &= X\left(\frac{1}{1-X}\right)' = X\frac{-(1-X)'}{(1-X)^2} = \frac{X}{(1-X)^2}\,. \end{aligned}$$

Bemerkung Für $1 \neq n \in \mathbb{N}$ definiert man die n-te *Fibonacci-Zahl* f_n als Anzahl aller 0-1-Folgen der Länge $n-2$, die keine benachbarten Einsen enthalten:

$$f_2 = 1 \text{ (leere Folge)},\ f_3 = 2,\ f_4 = 3,\ f_5 = 5, \ldots\,.$$

Zusätzlich sei $f_0 \coloneqq 0$, $f_1 \coloneqq 1$.

Satz *Für die Fibonacci-Zahlen gilt:*

(i) $f_n = f_{n-1} + f_{n-2}$ *($n \geq 2$),*

(ii) Die erzeugende Funktion ist

$$f(X) = \frac{X}{1 - X - X^2}\,,$$

(iii) $f_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$ *($n \in \mathbb{N}_0$).*

Beweis.

(i) Sei $a_1 \ldots a_{n-2}$ eine "zulässige" Folge der Länge $n-2$.

- Ist $a_{n-2} = 0$, ist $a_1 \dots a_{n-3}$ eine "zulässige" Folge der Länge $n-3$. Dafür gibt es f_{n-1} Möglichkeiten.
- Ist $a_{n-2} = 1$, dann ist $a_{n-3} = 0$ und $a_1 \dots a_{n-4}$ eine "zulässige" Folge der Länge $n-4$. Dafür gibt es f_{n-2} Möglichkeiten.

Also: $f_n = f_{n-1} + f_{n-2}$.

(ii) Setze

$$f(X) \coloneqq \sum_{n=0}^{\infty} f_n X^n \,.$$

Dann:

$$f(X) = X + \sum_{n=2}^{\infty} f_n X^n \overset{\text{(i)}}{=} X + \underbrace{\sum_{n=2}^{\infty} f_{n-1} X^n}_{=Xf(X)} + \underbrace{\sum_{n=2}^{\infty} f_{n-2} X^n}_{=X^2 f(X)} = X + Xf(X) + X^2 f(X) \,.$$

Daher: $f(X) = \dfrac{X}{1 - X - X^2}$.

(iii) Die Nullstellen von $X^2 + X - 1$ sind $\tau_1 = \frac{1}{2}(-1 + \sqrt{5})$, $\tau_2 = \frac{1}{2}(-1 - \sqrt{5})$. Daher ergibt die Partialbruchzerlegung:

$$\begin{aligned} f(X) &= \frac{-X}{(X - \tau_1)(X - \tau_2)} = \frac{1}{\sqrt{5}} \frac{1}{1 - \frac{1+\sqrt{5}}{2} X} - \frac{1}{\sqrt{5}} \frac{1}{1 - \frac{1-\sqrt{5}}{2} X} \\ &= \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \left(\frac{1 + \sqrt{5}}{2} \right)^n X^n - \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \left(\frac{1 - \sqrt{5}}{2} \right)^n X^n \,. \end{aligned}$$

Koeffizientenvergleich liefert die Behauptung.

□

10.5 Beispiel Für $1 \neq n \in \mathbb{N}$ sei D_n die Anzahl der fixpunktfreien Permutationen von $1, \dots, n$. Ferner sei $D_0 \coloneqq 1$, $D_1 \coloneqq 0$. Setze

$$d_n \coloneqq \frac{D_n}{n!} \text{ für } n \in \mathbb{N}_0.$$

Für die erzeugende Funktion

$$d(X) \coloneqq \sum_{n=0}^{\infty} d_n X^n$$

gilt dann nach Satz 3.3:

$$\begin{aligned}(1-X)d'(X) &= (1-X)\Big(\sum_{n=0}^{\infty}\frac{D_n}{n!}X^n\Big)' = (1-X)\Big(\sum_{n=1}^{\infty}\frac{D_n}{(n-1)!}X^{n-1}\Big)\\ &= \sum_{n=1}^{\infty}\frac{D_n}{(n-1)!}X^{n-1} - \sum_{n=1}^{\infty}\frac{D_n}{(n-1)!}X^n\\ &= \sum_{n=0}^{\infty}\frac{D_{n+1}}{n!}X^n - \sum_{n=1}^{\infty}\frac{D_n}{(n-1)!}X^n\\ &= \sum_{n=1}^{\infty}\Big(\frac{D_{n+1}}{n!} - \frac{D_n}{(n-1)!}\Big)X^n\\ &= \sum_{n=1}^{\infty}\Big(\frac{nD_n + nD_{n-1}}{n!} - \frac{D_n}{(n-1)!}\Big)X^n\\ &= \sum_{n=1}^{\infty}\frac{D_{n-1}}{(n-1)!}X^n = Xd(X)\,.\end{aligned}$$

Also:

$$d'(X) = \frac{X}{1-X}d(X)\,.\ \text{Daraus folgt leicht: } d(X) = \frac{\exp(-X)}{1-X}\,.$$

Literatur: generatingfunctionology

Bemerkung Man kann versuchen, ein Element

$$\alpha(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{R}[\![X]\!]$$

in ein weiteres Element

$$\beta(X) = \sum_{n=0}^{\infty} b_n X^n \in \mathbb{R}[\![X]\!]$$

einzusetzen:

$$\begin{aligned}\beta(\alpha(X)) \coloneqq \sum_{n=0}^{\infty} b_n\alpha(X)^n = {} & b_0\cdot 1\\ & + b_1(a_0 + a_1X + a_2X^2 + \dots)\\ & + b_2(a_0 + a_1X + a_2X^2 + \dots)(a_0 + a_1X + a_2X^2 + \dots)\\ & + \dots\end{aligned}$$

Dies geht gut, wenn $\beta(X)$ ein Polynom ist oder $a_0 = 0$. Es führt zu Problemen im Fall $a_0 \neq 0$.[27]

[27] Dann ist der Koeffizient von X^0 gleich $b_0 + b_1a_0 + b_2a_0^2 + \dots$, was evtl. nicht definiert ist.

10.6 Beispiel Sei F ein Körper mit $|F| = q \leq \infty$. Wie früher sei $N_d = a_d(q)$ die Anzahl der irreduziblen Polynome vom Grad d in $F[Y]$. Wir nummerieren jetzt die irreduziblen Polynome in $F[Y]$ durch:

$$f_1, f_2, f_3, \dots .$$

Die entsprechenden Grade seien $d_1, d_2, d_3, \dots$. Die Anzahl aller normierten Polynome vom Grad n in $F[Y]$ ist q^n. Die entsprechende erzeugende Funktion ist

$$\sum_{n=0}^{\infty} q^n X^n = \frac{1}{1-qX} .$$

Andererseits hat jedes normierte Polynom vom Grad n in $F[Y]$ eine eindeutige Primfaktorzerlegung:

$$f = f_1^{k_1} f_2^{k_2} f_3^{k_3} \cdots ,$$

mit

$$n = k_1 d_1 + k_2 d_2 + k_3 d_3 + \dots . \qquad (\star)$$

Daher ist q^n die Anzahl der Lösungen $(k_1, k_2, k_3, \dots)$ von $(\star)$ mit $k_i \in \mathbb{N}_0$ für alle i. Dies ist genau der Koeffizient von X^n in der formalen Potenzreihe

$$(1+X^{d_1}+X^{2d_1}+X^{3d_1}+\dots)(1+X^{d_2}+X^{2d_2}+X^{3d_2}+\dots)(1+X^{d_3}+X^{2d_3}+X^{3d_3}+\dots)\dots .$$

Daher:

$$\frac{1}{1-qX} = \prod_{i=1}^{\infty} \frac{1}{1-X^{d_i}} = \prod_{d=1}^{\infty} \left(\frac{1}{1-X^d}\right)^{N_d} . \qquad (\star\star)$$

Bekanntlich gilt:

$$\log \frac{1}{1-z} = z + \frac{1}{2}z^2 + \frac{1}{3}z^3 + \dots .$$

Anwendung von log auf $(\star\star)$ liefert:

$$\sum_{n=1}^{\infty} \frac{q^n X^n}{n} = \sum_{d=1}^{\infty} N_d \sum_{j=1}^{\infty} \frac{X^{d \cdot j}}{j} .$$

Koeffizientenvergleich bei X^n liefert:

$$\frac{q^n}{n} = \sum_{d|n} \frac{N_d}{n/d} , \text{ d.h. } \boxed{q^n = \sum_{d|n} N_d \cdot d} \text{ (vgl. Bemerkung 7.2).}$$

10.7 Beispiel Für $n \in \mathbb{N}$ sei p_n die Anzahl der Partitionen von n:

$$p_0 = 1, p_1 = 1, p_2 = 2, p_3 = 3, p_4 = 5, p_5 = 7, \dots .$$

Die erzeugende Funktion sei

$$p(X) \coloneqq \sum_{n=0}^{\infty} p_n X^n .$$

Offenbar ist p_n auch die Anzahl der Lösungen $(y_1, \ldots, y_n) \in \mathbb{N}_0$ mit

$$n = 1y_1 + 2y_2 + 3y_3 + \ldots + ny_n\,.^{28}$$

Dies ist genau der Koeffizient von X^n in

$$(1 + X + X^2 + \ldots)(1 + X^2 + X^4 + X^6 + \ldots)(1 + X^3 + X^6 + \ldots)\ldots\,.$$

Daher:

$$p(X) = \prod_{k=1}^{\infty} \frac{1}{1 - X^k}\,.$$

Satz *Für $n \in \mathbb{N}_0$ seien $p_v(n)$ die Anzahl der Partitionen $\lambda = (\lambda_1, \ldots, \lambda_t) \vdash n$ in lauter verschiedene Teile λ_i und $p_u(n)$ die Anzahl der Partitionen $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n$ in ungerade Teile. Dann: $p_v(n) = p_u(n)$.*

Beweis. Wir zeigen, dass die entsprechenden erzeugenden Funktionen $p_v(X)$ und $p_u(X)$ gleich sind. Offenbar ist

$$\begin{aligned} p_v(X) &= (1 + X)(1 + X^2)(1 + X^3)\ldots = \prod_{k=1}^{\infty}(1 + X^k)\,, \\ p_u(X) &= (1 + X + X^2 + \ldots)(1 + X^3 + X^6 + \ldots)(1 + X^5 + X^7 + \ldots)\ldots \\ &= \prod_{j=1}^{\infty} \frac{1}{1 - X^{2j-1}}\,. \end{aligned}$$

Erweitern mit $\prod_{j=1}^{\infty}(1 - X^{2j})$ ergibt:

$$p_u(X) = \prod_{j=1}^{\infty} \frac{1 - X^{2j}}{1 - X^j} = \prod_{j=1}^{\infty}(1 + X^j) = p_v(X)\,.$$

□

10.8 Bemerkung Wir kennen die Formeln

$$\begin{aligned} 1 + 2 + 3 + \ldots + (n-1) &= \frac{n(n-1)}{2}\,, \\ 1^2 + 2^2 + 3^2 + \ldots + (n-1)^2 &= \frac{n(n-1)(2n-1)}{6}\,, \\ 1^3 + 2^3 + 3^3 + \ldots + (n-1)^3 &= \left(\frac{n(n-1)}{2}\right)^2. \end{aligned}$$

Wie geht das weiter? Setze dazu:

$$P_m(n) \coloneqq 1^m + 2^m + 3^m + \ldots + (n-1)^m = \sum_{k=0}^{n-1} k^m \;\; (m, n \in \mathbb{N})$$

[28] $(y_1, \ldots, y_n) \longleftrightarrow$ Partition mit y_1 Einsen, y_2 Zweien, y_3 Dreien,…

und

$$Q_n(X) \coloneqq \sum_{m=0}^{\infty} \frac{P_m(n)}{m!} X^m = \sum_{m=0}^{\infty} \sum_{k=0}^{n-1} \frac{k^m}{m!} X^m = \sum_{k=0}^{n-1} \sum_{m=0}^{\infty} \frac{(kX)^m}{m!} = \sum_{k=0}^{n-1} \exp(kX)$$
$$= \sum_{k=0}^{n-1} \exp(X)^k = \frac{\exp(X)^n - 1}{\exp(X) - 1}\,.$$

Wegen

$$\exp(X) - 1 = \sum_{m=1}^{\infty} \frac{X^m}{m!}$$

ist

$$\frac{\exp(X) - 1}{X} = \sum_{m=1}^{\infty} \frac{X^{m-1}}{m!} = \sum_{m=0}^{\infty} \frac{X^m}{(m+1)!} \text{ invertierbar in } \mathbb{R}[\![X]\!].$$

Schreibe

$$\frac{X}{\exp(X) - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} X^n =: B(X) \ (B_n \in \mathbb{R} \text{ für } n \in \mathbb{N}_0).$$

Die Zahlen $B_0, B_1, B_2, \ldots$ heißen *Bernoulli-Zahlen*. Dann:

$$X = B(X)(\exp(X) - 1)$$
$$= \left(\sum_{m=0}^{\infty} \frac{B_m}{m!} X^m\right)\left(\sum_{m=1}^{\infty} \frac{X^m}{m!}\right)$$
$$= \sum_{m=0}^{\infty} \left(\sum_{k=0}^{m-1} \frac{B_k}{k!} \frac{1}{(m-k)!}\right) X^m\,.$$

Koeffizientenvergleich bei X und X^2 liefert $B_0 = 1$ und $B_1 = \frac{-1}{2}$. Koeffizientenvergleich bei X^m ergibt:

$$\boxed{0 = \sum_{k=0}^{m-1} \binom{m}{k} B^k\,.}$$

Daraus erhält man sukzessive: $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = \frac{-1}{30}$, $B_5 = 0$, $B_6 = \frac{1}{42}$,.... Wegen

$$XQ_n(X) = X\frac{\exp(nX) - 1}{\exp(X) - 1} = B(X)(\exp(nX) - 1) = \left(\sum_{k=0}^{\infty} \frac{B_k}{k!} X^k\right)\left(\sum_{m=1}^{\infty} \frac{(nX)^m}{m!}\right)$$
$$= \sum_{m=0}^{\infty} \left(\sum_{k=0}^{m-1} \frac{B_k}{k!} \frac{n^{m-k}}{(m-k)!}\right) X^m$$

liefert Koeffizientenvergleich bei X^{m+1}:

$$\frac{P_m(n)}{m!} = \sum_{k=0}^{m} \frac{B_k}{k!} \frac{n^{m+1-k}}{(m+1-k)!}\,,$$

d.h.

$$\boxed{P_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}.}$$

Daraus kann man weitere Formeln berechnen.

Beispiel

$$1^4 + 2^4 + 3^4 + \ldots + (n-1)^4 = \frac{n^5}{5} - \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}.$$

Stichwortverzeichnis