

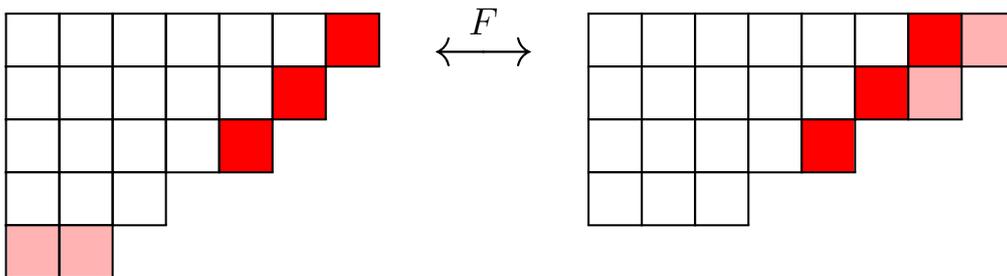
Kombinatorik

Vorlesung im Wintersemester 2018/19

Benjamin Sambale
Friedrich-Schiller-Universität Jena

Version: 10. August 2025

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



Inhaltsverzeichnis

Vorwort	2
1. Endliche Mengen	3
2. Permutationen und Partitionen	10
3. Möbius-Inversion	20
4. Potenzreihen	24
5. Erzeugende Funktionen	34
6. Polynome	50
7. Polynome in mehreren Unbekannten	58
8. Bernoulli-Zahlen	65
9. Catalan-Zahlen	71
10. Gruppen	74
11. Graphen	85
12. Aufgaben	93
A. GAP-Befehle	101
Stichwortverzeichnis	102

Vorwort

Das vorliegende Skript entstand aus einer 3 + 1-Vorlesung im Wintersemester 2018/19 (15 Wochen) an der Friedrich-Schiller-Universität Jena und richtet sich vorrangig an Studierende der Studiengänge:

- Mathematik Lehramt Gymnasium
- B. Sc. Mathematik, Wirtschaftsmathematik, Informatik

Es werden Kenntnisse der Linearen Algebra 1 und Analysis 1 vorausgesetzt. Einige Teile wurden nicht präsentiert (insbesondere das letzte Kapitel). 2020 und 2021 wurden umfangreiche Änderungen und Ergänzungen vorgenommen, unter anderen die Ramanujan-Kongruenzen und die Rogers-Ramanujan-Identitäten.

Literatur:

- P. Tittmann, *Einführung in die Kombinatorik*, 2. Auflage, Springer Spektrum, Heidelberg, 2014, <https://link.springer.com/book/10.1007%2F978-3-642-54589-4>.
- R. P. Stanley, *Enumerative Combinatorics Vol. I, II*, 2nd edition, Cambridge University Press, Cambridge, 2012, <http://www-math.mit.edu/~rstan/ec/ec1.pdf>.

- G. E. Andrews, K. Eriksson, *Integer Partitions*, Cambridge University Press, Cambridge, 2004, <https://doi.org/10.1017/CB09781139167239>

1. Endliche Mengen

Bemerkung 1.1. Kombinatorik ist die Lehre vom Abzählen diskreter Objekte:

- (leicht) Die Anzahl der k -elementigen Teilmengen einer n -elementigen Menge ist $\binom{n}{k}$.
- (mittel) Die Anzahl der fixpunktfreien Permutationen auf $\{1, \dots, n\}$ ist $[n!/e]$.
- (schwer) Die Anzahl der Partitionen von $5n + 4$ ist durch 5 teilbar.
- (sehr schwer) Jede Landkarte lässt sich mit vier Farben färben, sodass benachbarte Länder verschiedene Farben haben.
- (offen) Wie viele magische Quadrate der Größe 6×6 gibt es?

Definition 1.2.

- Leere Menge: \emptyset .
- Natürliche Zahlen: $\mathbb{N} = \{1, 2, \dots\}$ $\mathbb{N}_0 = \{0, 1, \dots\}$.
- Primzahlen: $\mathbb{P} = \{2, 3, 5, 7, \dots\}$.
- Ganze Zahlen: $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$.
- Rationale Zahlen: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$.
- Reelle Zahlen: \mathbb{R} (Analysis).
- Komplexe Zahlen: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$.
- Für eine Menge A sei $|A|$ die Mächtigkeit von A . Man nennt A *endlich*, falls $|A| < \infty$ und anderenfalls *unendlich*. Wir unterscheiden mit der Schreibweise $|A| = \infty$ keine Kardinalitäten (abzählbar, überabzählbar etc.). Zwei Mengen A und B heißen *gleichmächtig*, falls eine Bijektion $A \rightarrow B$ existiert.
- Sind A_i ($i \in I$) Mengen, so auch ihr *kartesisches Produkt* $\times_{i \in I} A_i = \{(a_i : i \in I) : a_i \in A_i\}$. Im Fall $A = A_i$ für alle $i \in I$ schreiben wir auch $A^I := \times_{i \in I} A$. Für $I = \{1, \dots, n\}$ schreiben wir $A_1 \times \dots \times A_n$ und $A^n = A \times \dots \times A$ (n Faktoren).
- Sind A_i ($i \in I$) Mengen, so auch ihre *disjunkte Vereinigung*

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

Für $I = \{1, \dots, n\}$ schreiben wir $A_1 \sqcup \dots \sqcup A_n$.

- Für eine Menge A ist $2^A := \{B \subseteq A\}$ die *Potenzmenge* von A . Für $k \in \mathbb{N}_0$ sei

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

die Menge der k -elementigen Teilmengen von A .

Bemerkung 1.3. Für Mengen A und I kann man A^I mit der Menge aller Abbildungen $I \rightarrow A$ identifizieren, indem man $(a_i)_{i \in I} \in A^I$ durch $f : I \rightarrow A$ mit $f(i) := a_i$ ersetzt.

Satz 1.4. Für endliche Mengen A, B, A_1, \dots, A_n gilt

- (i) $|A_1 \times \dots \times A_n| = |A_1| \dots |A_n|$ und $|A^n| = |A|^n$.
- (ii) $|A_1 \sqcup \dots \sqcup A_n| = |A_1| + \dots + |A_n|$.
- (iii) A und B sind genau dann gleichmächtig, falls $|A| = |B|$.
- (iv) $|2^A| = 2^{|A|}$.

Beweis.

- (i) Für jedes Element $(a_1, \dots, a_n) \in A_1 \times \dots \times A_n$ gibt es $|A_1|$ Möglichkeiten a_1 zu wählen, $|A_2|$ Möglichkeiten für a_2 usw. Umgekehrt liefert jede solche Wahl genau ein Element von $A_1 \times \dots \times A_n$.
- (ii) Jedes Element in $A_1 \sqcup \dots \sqcup A_n$ liegt in genau einer der Mengen $\{(a, i) : a \in A_i\}$. Dabei gilt $|\{(a, i) : a \in A_i\}| = |A_i|$.
- (iii) Sei $A = \{a_1, \dots, a_n\}$ und $f : A \rightarrow B$ eine Bijektion. Dann gilt $B = \{f(a_1), \dots, f(a_n)\}$ mit $f(a_i) \neq f(a_j)$ für $i \neq j$. Dies zeigt $|B| = n = |A|$. Sei umgekehrt $|A| = |B|$ und $A = \{a_1, \dots, a_n\}$ sowie $B = \{b_1, \dots, b_n\}$. Dann ist $f : A \rightarrow B, a_i \mapsto b_i$ eine Bijektion.
- (iv) Sei $A = \{a_1, \dots, a_n\}$. Für $M \subseteq A$ sei $f(M) := (x_1, \dots, x_n) \in \{0, 1\}^n$ mit $x_i = 1 \iff a_i \in M$. Dann ist $f : 2^A \rightarrow \{0, 1\}^n, M \mapsto f(M)$ eine Bijektion. Nach (iii) und (i) folgt

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

Definition 1.5.

- Für $n \in \mathbb{N}_0$ ist $n! := \prod_{k=1}^n k$ die *Fakultät* von n . Beachte: $0! = 1$ (leeres Produkt).
- Für $a \in \mathbb{C}$ und $k \in \mathbb{N}_0$ definiert man den *Binomialkoeffizienten*

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

- Für $n, k_1, \dots, k_s \in \mathbb{N}_0$ mit $n = k_1 + \dots + k_s$ sei

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

der *Multinomialkoeffizient* von n und k_1, \dots, k_s .

Bemerkung 1.6. Es gilt $\binom{a}{0} = 1$ (leeres Produkt) und $\binom{n}{k} = 0$ für $k > n \in \mathbb{N}_0$. Für $k \leq n \in \mathbb{N}_0$ gilt

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

und

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

Beispiel 1.12.

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

Satz 1.13 („Kombination ohne Wiederholung“). Für jede endliche Menge A und $k \in \mathbb{N}_0$ gilt

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

Beweis. Sei A_k die Menge der injektiven Abbildungen $\{1, \dots, k\} \rightarrow A$. Dann ist die Abbildung

$$F : A_k \rightarrow \binom{A}{k}, \\ f \mapsto \{f(1), \dots, f(k)\}$$

surjektiv. Für $\sigma \in S_k$ gilt $F(f \circ \sigma) = \{f(\sigma(1)), \dots, f(\sigma(k))\} = F(f)$. Für $B \in \binom{A}{k}$ ist sogar $F^{-1}(B) = \{f \circ \sigma : \sigma \in S_k\}$, wobei $f \in A_k$ ein festes Urbild von B unter F ist. Insbesondere hat jedes $B \in \binom{A}{k}$ genau $|S_k| = k!$ Urbilder. Es folgt $\left| \binom{A}{k} \right| = \frac{|A_k|}{k!} = \binom{|A|}{k}$ nach Satz 1.9. \square

Beispiel 1.14. Beim Lotto „6 aus 49“ gibt es $\binom{49}{6} = 13.983.816$ Möglichkeiten und die Wahrscheinlichkeit für einen 4er ist

$$\frac{\binom{6}{4} \binom{43}{2}}{\binom{49}{6}} = \frac{645}{665896} \approx 0,1\%.$$

Bemerkung 1.15.

(i) Satz 1.13 liefert eine kombinatorische Interpretation der Identität $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$: Für $a \in A$ gibt es genau $\binom{|A \setminus \{a\}|}{k-1}$ Teilmengen $B \in \binom{A}{k}$, die a enthalten und $\binom{|A \setminus \{a\}|}{k}$ Teilmengen $B \in \binom{A}{k}$, die a nicht enthalten.

(ii) Nach Satz 1.4 und Satz 1.13 ist

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

Dies ist ein Spezialfall des bekannten *Binomialsatz* (setze $a = b = 1$)

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

Satz 1.16 (VANDERMONDE-Identität). Für $n, a_1, \dots, a_n \in \mathbb{N}$ und $k \in \mathbb{N}_0$ gilt

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

Beweis. Seien A_1, \dots, A_n Mengen mit $|A_i| = a_i$ für $i = 1, \dots, n$. Wir bestimmen $|\binom{A_1 \sqcup \dots \sqcup A_n}{k}|$ auf zwei Weisen. Nach Satz 1.13 ist einerseits

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

Jede k -elementige Teilmenge von $A_1 \sqcup \dots \sqcup A_n$ setzt sich andererseits zusammen aus k_i -elementigen Teilmengen von A_i für $i = 1, \dots, n$ und $k_1 + \dots + k_n = k$. Für jede dieser Teilmengen gibt es $|\binom{A_i}{k_i}| = \binom{a_i}{k_i}$ Möglichkeiten. Dies zeigt

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

Beispiel 1.17. Der Spezialfall $n = 2$ und $a_1 = a_2 = k$ in Satz 1.16 liefert

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

Satz 1.18 („Variation mit Wiederholung“ II). Seien $A = \{a_1, \dots, a_n\}$ und B endliche Mengen und $k_1, \dots, k_n \in \mathbb{N}_0$ mit $|B| = k_1 + \dots + k_n$. Dann existieren genau $\binom{|B|}{k_1, \dots, k_n}$ Abbildungen $f : B \rightarrow A$ mit $|f^{-1}(a_i)| = k_i$ für $i = 1, \dots, n$.

Beweis. Sei $|B| = k$ und $f : B \rightarrow A$ mit $|f^{-1}(a_i)| = k_i$ für $i = 1, \dots, n$. Nach Satz 1.13 gibt es $\binom{k}{k_1}$ Möglichkeiten für $f^{-1}(a_1)$. Ist $f^{-1}(a_1)$ festgelegt, so verbleiben noch $\binom{k-k_1}{k_2}$ Möglichkeiten für $f^{-1}(a_2)$ usw. Also gibt es

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

Möglichkeiten für f . □

Beispiel 1.19.

- (i) Ein *Anagramm* ist eine Vertauschung der Buchstaben eines Worts. Nach Satz 1.18 gibt es $\binom{5}{2,1,1,1} = 60$ Anagramme von EULER (wähle $A = \{E, U, L, R\}$, $B = \{1, 2, 3, 4, 5\}$, $k_1 = 2$, $k_2 = k_3 = k_4 = 1$). Zum Beispiel REUEL, LUREE usw.
- (ii) Es gibt $\binom{32}{10,10,10,2} = 2.753.294.408.504.640$ Möglichkeiten 32 Skatkarten an drei Spieler zu verteilen.

Bemerkung 1.20. Nach Bemerkung 1.7 und Satz 1.18 ist

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

Dies ist ein Spezialfall des *Multinomialsatz*

$$(a_1 + \dots + a_n)^k = \sum_{\substack{(k_1, \dots, k_n) \in \mathbb{N}_0^n \\ k_1 + \dots + k_n = k}} \binom{k}{k_1, \dots, k_n} a_1^{k_1} \cdots a_n^{k_n} \quad (a_1, \dots, a_n \in \mathbb{R})$$

(Aufgabe 7). Für $n = 2$ erhält man den Binomialsatz.

Definition 1.21. Für eine beliebige Menge A bezeichnet man die Elemente aus \mathbb{N}_0^A als *Multimengen* über A . Man kann eine Multimenge $m := (n_a)_{a \in A}$ als „Teilmenge“ von A interpretieren, wobei jedes $a \in A$ genau n_a mal vorkommt (im Fall $n_a \leq 1$ für alle $a \in A$ ist m also eine echte Menge). Dementsprechend setzt man $|m| := \sum_{a \in A} n_a$. Wir werden Multimengen oft in der Form $\{a, a, b, c, c, c, \dots\}$ notieren, wobei wie bei Mengen die Reihenfolge keine Rolle spielt.

Satz 1.22 („Kombination mit Wiederholung“). *Eine n -elementige Menge besitzt genau*

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

viele k -elementige Multimengen ($n, k \in \mathbb{N}_0$).

Beweis. O. B. d. A. sei $A = \{1, \dots, n\}$. Man kann dann die k -elementigen Multimengen über A mit den Tupeln $(a_1, \dots, a_k) \in A^k$ mit $a_1 \leq \dots \leq a_k$ identifizieren. Sei A_k die Menge dieser k -Tupel. Offenbar ist dann

$$f : A_k \rightarrow \binom{\{1, \dots, n+k-1\}}{k}, \\ (a_1, \dots, a_k) \mapsto \{a_1, a_2+1, \dots, a_k+k-1\}$$

bijektiv. Aus Satz 1.13 folgt $|A_k| = |f(A_k)| = \binom{n+k-1}{k}$. □

Beispiel 1.23. Beim gleichzeitigen Werfen von drei identischen Würfeln gibt es $\binom{\binom{6}{3}}{3} = \binom{8}{3} = 56$ mögliche Ereignisse, die allerdings nicht alle gleichwahrscheinlich sind.

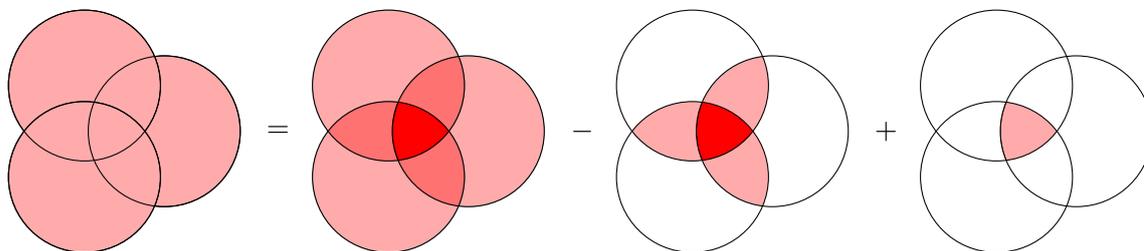
Bemerkung 1.24.

(i) Für $1 \leq k \leq n$ gilt

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

(ii) Für endliche Mengen A und B ist bekanntlich $|A \cup B| = |A| + |B| - |A \cap B|$. Offenbar gilt auch

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



Dies lässt sich wie folgt verallgemeinern.

Satz 1.25 (Inklusions-Exklusions-Prinzip). *Für endliche Mengen A_1, \dots, A_n gilt*

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

Beweis. Wir zählen wie oft ein Element $a \in A_1 \cup \dots \cup A_n$ auf der rechten Seite berücksichtigt wird. Dafür sei o. B. d. A. $a \in A_1 \cap \dots \cap A_l$ und $a \notin A_i$ für $i > l$. Dann wird a genau dann gezählt, wenn $\{i_1, \dots, i_k\} \subseteq \{1, \dots, l\}$ gilt. Im k -ten Summanden wird a also $(-1)^{k+1} \binom{l}{k}$ -mal gezählt. Insgesamt wird a auf der rechten Seite genau

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

Mal gezählt. Dies zeigt die Behauptung. □

Definition 1.26. Wie üblich heißen $a, b \in \mathbb{N}$ *teilerfremd*, falls 1 der einzige gemeinsame positive Teiler von a und b ist, d. h. $\text{ggT}(a, b) = 1$. Man nennt

$$\varphi(n) := |\{1 \leq a \leq n : \text{ggT}(a, n) = 1\}| \quad (n \in \mathbb{N})$$

die *eulersche φ -Funktion*.

Satz 1.27. Sei $n = p_1^{a_1} \dots p_k^{a_k}$ die Primfaktorzerlegung von $n \in \mathbb{N}$. Dann gilt

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

Beweis. Für $i = 1, \dots, k$ sei $A_i := \{1 \leq a \leq n : p_i \mid a\}$. Dann ist $A := \{1 \leq a \leq n : \text{ggT}(a, n) \neq 1\} = A_1 \cup \dots \cup A_k$. Für $1 \leq i_1 < \dots < i_l \leq k$ ist

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

Mit Satz 1.25 folgt

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

Bemerkung 1.28. In der Algebra beweist man Satz 1.27 mit dem chinesischen Restsatz.

Satz 1.29 (ERDŐS-SZEKERES). Jede reelle Folge paarweiser verschiedener Zahlen a_1, \dots, a_{n^2+1} mit $n \in \mathbb{N}$ besitzt eine monotone Teilfolge der Länge $n + 1$.

Beweis. Für $i = 1, \dots, n^2 + 1$ sei α_i (bzw. β_i) die maximale Länge einer monoton steigenden (bzw. fallenden) Teilfolge, die mit a_i endet. Nehmen wir an, dass alle monotonen Teilfolgen Länge $\leq n$ haben. Dann gibt es höchstens n^2 Paare (α_i, β_i) . Nach dem Schubfachprinzip existieren $1 \leq i < j \leq n^2 + 1$ mit $(\alpha_i, \beta_i) = (\beta_j, \beta_j)$. Im Fall $a_i < a_j$ (bzw. $a_i > a_j$) kann man die mit a_i endende monoton steigende (bzw. fallende) Folge mit a_j erweitern. Dann wäre aber $\alpha_i < \alpha_j$ oder $\beta_i < \beta_j$. Widerspruch. □

Beispiel 1.30. Die Folge

$$n, n-1, \dots, 1, 2n, 2n-1, \dots, n+1, \dots, n^2, n^2-1, \dots, n^2-n+1$$

der Länge n^2 besitzt keine monotone Teilfolge der Länge $n + 1$.

2. Permutationen und Partitionen

Definition 2.1.

- Sei A eine Menge und $\sigma \in \text{Sym}(A)$. Man nennt $a \in A$ *Fixpunkt* von σ , falls $\sigma(a) = a$. Besitzt σ keine Fixpunkte, so nennt man σ *fixpunktfrei*.
- Für $x \in \mathbb{R}$ sei $[x] \in \mathbb{Z}$ mit $|x - [x]| < \frac{1}{2}$ oder $[x] = x + \frac{1}{2}$ („Runden“).

Satz 2.2 (MONTMORT). Die Anzahl der fixpunktfreien Permutationen in S_n beträgt $[n!/e]$, wobei e die eulersche Zahl ist.

Beweis. Für $i = 1, \dots, n$ sei $F_i := \{\sigma \in S_n : \sigma(i) = i\}$. Die Anzahl f_n der fixpunktfreien Permutationen von S_n ist dann $f_n = |S_n \setminus (F_1 \cup \dots \cup F_n)| = n! - |F_1 \cup \dots \cup F_n|$. Für $1 \leq i_1 < \dots < i_k \leq n$ ist

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

Satz 1.25 zeigt

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

Nun ist

$$\left| \frac{n!}{e} - f_n \right| = \left| n! \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \right| = \frac{1}{n+1} - \frac{1}{(n+1)(n+2)} \pm \dots < \frac{1}{n+1} \leq \frac{1}{2}$$

und $f_n = [n!/e]$. □

Beispiel 2.3.

- Die fixpunktfreien Permutationen von S_4 sind $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.
- Beim vorweihnachtlichen Wichteln schenken sich n Personen gegenseitig etwas, indem sie vorher Lose ziehen, auf denen steht, an wem das Geschenk zu richten ist. Dies beschreibt eine Permutation auf $\{1, \dots, n\}$, die genau dann fixpunktfrei ist, wenn keine Person ihr eigenes Los zieht. Die Wahrscheinlichkeit, dass eine Person ihr eigenes Los zieht, beträgt daher $1 - \frac{[n!/e]}{n!} \approx 1 - \frac{1}{e} \approx 63\%$.
- Die im zweiten Weltkrieg benutzte Verschlüsselungsmaschine *Enigma* permutiert die 26 Buchstaben des lateinischen Alphabets. Um die Verschlüsselung vermeintlich sicherer zu machen, wurden nur fixpunktfreie Permutationen eingesetzt. Dies war jedoch eine entscheidende Schwachstelle, die es den Alliierten ermöglichte, die Enigma zu entschlüsseln.¹

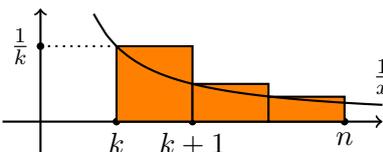
Beispiel 2.4 (Sekretärinnenproblem). Es werden n Bewerber auf eine offene Stelle nacheinander zum Vorstellungsgespräch geladen. Direkt nach jedem Gespräch soll dem Bewerber mitgeteilt werden, ob er genommen oder abgelehnt wurde. Im ersten Fall ist das Verfahren beendet und es werden keine weiteren Bewerber berücksichtigt. Mit welcher Strategie findet man einen möglichst guten Bewerber?

¹[https://de.wikipedia.org/wiki/Enigma_\(Maschine\)#Kryptographische_Schw%C3%A4chen](https://de.wikipedia.org/wiki/Enigma_(Maschine)#Kryptographische_Schw%C3%A4chen)

Man lehne zunächst die ersten $k < n$ Bewerber konsequent ab und wähle unter den verbleibenden $n - k$ den ersten, der besser als die ersten k Bewerber ist (möglicherweise muss man alle Bewerber ablehnen, womit die Strategie gescheitert ist). Die Reihenfolge der Bewerber beschreibt eine Permutation $\sigma \in S_n$, wobei $\sigma(1)$ die Position des besten Bewerbers ist und $\sigma(2)$ die Position des zweitbesten usw. Sei

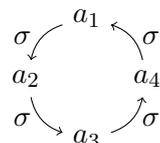
$$m := \min\{i \leq n : \sigma(i) < \sigma(1)\}.$$

Die obige Strategie findet genau dann den besten Bewerber, wenn $\sigma(1) > k$ und $\sigma(m) \leq k$ gilt. Die Wahrscheinlichkeit, dass $\sigma(1)$ an Stelle l steht, beträgt $1/n$. Die Wahrscheinlichkeit für $\sigma(m) \leq k$ ist dann $\frac{k}{l-1}$. Die Erfolgswahrscheinlichkeit der Strategie ist daher

$$\sum_{l=k+1}^n \frac{1}{n} \frac{k}{l-1} = \frac{k}{n} \sum_{l=k}^{n-1} \frac{1}{l} \geq \frac{k}{n} \int_k^n \frac{1}{x} dx = \frac{k}{n} (\log n - \log k).$$


Die Funktion $f(x) = \frac{x}{n} (\log n - \log x)$ hat Ableitung $f'(x) = \frac{1}{n} (\log n - \log x - 1)$ und nimmt daher ihr Maximum bei $x = n/e$ an. Für $k = \lceil n/e \rceil$ ist die Erfolgswahrscheinlichkeit also ca. $f(n/e) = 1/e \approx 37\%$ (für „große“ n). Man kann zeigen, dass dies die beste Strategie ist. Für $n = 20$ ergibt sich $k = 7$ und ca. 38%.

Definition 2.5. Für eine Menge A nennt man $\sigma \in \text{Sym}(A)$ einen (k -)Zyklus (oder Zyklus der Länge k), falls paarweise verschiedene $a_1, \dots, a_k \in A$ existieren, sodass

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


Man schreibt dann $\sigma = (a_1, \dots, a_k)$. Diese Schreibweise ist eindeutig bis auf „Rotation“, d. h.

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

Der einzige 1-Zyklus ist id_A . Um Formulierungen einheitlich zu gestalten, werden wir dennoch die 1-Zyklen $(1), (2), \dots, (n)$ formal unterscheiden. Außerdem fassen wir id_A als Produkt aller 1-Zyklen auf. Zyklen der Länge 2 heißen *Transpositionen*. Zyklen $\sigma = (a_1, \dots, a_k)$ und $\tau = (b_1, \dots, b_l)$ heißen *disjunkt*, falls

$$\{a_1, \dots, a_k\} \cap \{b_1, \dots, b_l\} = \emptyset.$$

Bemerkung 2.6.

- (i) Es gilt $(a_1, \dots, a_k)^{-1} = (a_k, a_{k-1}, \dots, a_1)$.
- (ii) Disjunkte Zyklen $\sigma, \tau \in \text{Sym}(A)$ sind vertauschbar, d. h. $\sigma \circ \tau = \tau \circ \sigma$. Wir werden im Folgenden das Verknüpfungssymbol \circ oft weglassen.

Lemma 2.7. Jede Permutation σ einer endlichen Menge A ist eine Komposition von paarweise disjunkten Zyklen $\sigma = \sigma_1 \dots \sigma_k$ der Länge > 1 und diese sind bis auf die Reihenfolge eindeutig bestimmt.

Beweis. Existenz: Sei $A_\sigma := \{a \in A : \sigma(a) \neq a\}$. Wir argumentieren durch Induktion nach $|A_\sigma|$. Im Fall $A_\sigma = \emptyset$ ist $\sigma = \text{id}_A$ das leere Produkt. Sei also $a \in A_\sigma \neq \emptyset$. Wegen $|A_\sigma| \leq |A| < \infty$ können die Elemente $a, \sigma(a), \sigma^2(a), \dots \in A_\sigma$ nicht alle verschieden sein. Sei also $0 \leq k < l$ mit $\sigma^k(a) = \sigma^l(a)$. Dann ist $\sigma^{l-k}(a) = a$. Sei $s \in \mathbb{N}$ minimal mit $\sigma^s(a) = a$. Dann sind $a, \sigma(a), \dots, \sigma^{s-1}(a)$ paarweise verschieden und $\sigma_1 = (a, \sigma(a), \dots, \sigma^{s-1}(a))$ ist ein s -Zyklus mit $s > 1$. Für $\tau := \sigma_1^{-1}\sigma \in \text{Sym}(A_\sigma)$ und $i = 0, \dots, s-1$ gilt dann

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

Dies zeigt $A_\tau = A_\sigma \setminus A_{\sigma_1}$. Nach Induktion existieren paarweise disjunkte Zyklen $\sigma_2, \dots, \sigma_k \in \text{Sym}(A_\tau)$ mit Länge > 1 und $\tau = \sigma_2 \dots \sigma_k$. Offenbar sind auch $\sigma_1, \dots, \sigma_k$ paarweise disjunkt und $\sigma = \sigma_1 \dots \sigma_k$.

Eindeutigkeit: Seien $\sigma = \sigma_1 \dots \sigma_k = \tau_1 \dots \tau_l$ zwei Darstellungen mit paarweise disjunkten Zyklen $\sigma_1, \dots, \sigma_k$ sowie τ_1, \dots, τ_l . Sei $a \in A$ mit $\sigma_1(a) \neq a$. Dann existiert genau ein τ_i mit $\tau_i(a) = \sigma_1(a)$. Weiter ist $\sigma_1^2(a) = \tau_i^2(a)$ usw. Dies zeigt $\sigma_1 = \tau_i$. Indem man beide Seiten mit σ_1^{-1} multipliziert, erhält man $\sigma_2 \dots \sigma_k = \tau_1 \dots \tau_{i-1} \tau_{i+1} \dots \tau_l$. Die Behauptung folgt nun leicht durch Induktion nach k . \square

Bemerkung 2.8.

- (i) Man kann die Schreibweise in disjunkte Zyklen

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

vollständig eindeutig machen, indem man $a_1 = \min\{a_1, \dots, a_s\} < b_1 = \min\{b_1, \dots, b_t\} < \dots$ fordert. Dies wird im Computeralgebrasystem GAP realisiert.

- (ii) Im Folgenden sagen wir, dass $\sigma \in S_n$ einen Zyklus τ *enthält*, falls τ in der disjunkten Zyklendarstellung vorkommt. Dabei wollen wir die Fixpunkte als 1-Zyklen mitzählen.
- (iii) Bekanntlich (Lineare Algebra?) lässt sich jede Permutation auch als Produkt von Transpositionen schreiben, allerdings sind diese in der Regel nicht disjunkt.

Beispiel 2.9.

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

(ii) $(2, 5, 3, 1)(3, 1, 6) = (1, 6)(2, 5, 3)$ (Abbildungen werden von rechts nach links ausgewertet).

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

Satz 2.10. Für $1 \leq k \leq n$ gilt:

(i) Die Anzahl der k -Zyklen von S_n ist $\frac{n!}{k(n-k)!}$.

(ii) Ist $z_k(\sigma)$ die Anzahl der k -Zyklen von σ , so gilt

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

(iii) Die durchschnittliche Anzahl von Zyklen einer Permutation $\sigma \in S_n$ ist die n -te harmonische Zahl

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

Beweis.

- (i) Jeder k -Zyklus permutiert eine k -elementige Menge $\{a_1, \dots, a_k\} \subseteq \{1, \dots, n\}$. Für die Wahl dieser Menge gibt es $\binom{n}{k}$ Möglichkeiten (Satz 1.13). Jeder k -Zyklus auf dieser Menge lässt sich eindeutig in der Form (a_1, b_2, \dots, b_k) mit $\{b_2, \dots, b_k\} = \{a_2, \dots, a_k\}$ schreiben. Dies liefert $(k-1)!$ Zyklen, denn die Ziffern b_2, \dots, b_k kann man beliebig permutieren. Insgesamt gibt es

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

Zyklen der Länge k .

- (ii) Sei $C_k \subseteq S_n$ die Menge der k -Zyklen. Jeder k -Zyklus ist in $(n-k)!$ vielen Permutationen enthalten, denn man kann die $n-k$ Ziffern außerhalb des Zyklus beliebig permutieren. Es folgt

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

- (iii) Die durchschnittliche Zyklenanzahl ist

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

nach (ii). □

Bemerkung 2.11. Bekanntlich (Analysis) ist

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

die *Euler-Mascheroni-Konstante*. Für große n ist daher $H_n \approx \log(n) + \gamma$. Man weiß bislang nicht, ob γ rational ist.

Beispiel 2.12.

- (i) Die durchschnittliche Zyklenanzahl von $\sigma \in S_8$ ist $H_8 = \frac{761}{280} \approx 2,71$.
- (ii) (Problem der 100 Gefangenen) Die Namen von 100 Gefangenen werden in 100 verschlossenen nummerierten Umschlägen aufbewahrt. Die Gefangenen werden nacheinander gebeten 50 Umschläge ihrer Wahl zu öffnen mit dem Ziel ihren eigenen Namen zu finden. Gelingt es jedem Gefangenen seinen eigenen Namen zu finden, so erhalten alle die Freiheit. Sie dürfen sich vorher eine Strategie überlegen, aber während des Experiments nicht kommunizieren. Was ist eine gute Strategie? Ohne Strategie (d. h. jeder öffnet 50 zufällige Umschläge) beträgt die Erfolgswahrscheinlichkeit nur

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

Die Gefangenen werden durchnummeriert, sodass die Verteilung der Namen in die Umschläge eine Permutation $\sigma \in S_{100}$ beschreibt. Ist der Gefangene mit Nummer a an der Reihe, so öffnet er zunächst Umschlag a und findet darin den Namen vom Gefangenen $\sigma(a)$. Danach öffnet er Umschlag $\sigma(a)$ und findet darin den Namen von $\sigma^2(a)$ usw. Auf diese Weise findet er seinen eigenen Namen genau dann, wenn der Zyklus von σ , der a enthält Länge ≤ 50 hat. Das Verfahren ist also genau dann erfolgreich, wenn σ keinen Zyklus der Länge > 50 enthält. Offenbar kann σ

höchstens einen solchen Zyklus enthalten. Die Anzahl der Permutationen mit Zyklus der Länge $k > 50$ ist daher

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

Die Wahrscheinlichkeit, dass die Strategie scheitert ist folglich

$$\frac{1}{n!} \sum_{k=51}^{100} \sum_{\sigma \in S_n} z_k(\sigma) \stackrel{2.10}{=} \sum_{k=51}^{100} \frac{1}{k} \leq \int_{50}^{100} \frac{1}{x} dx = \log(2 \cdot 50) - \log(50) = \log(2) < 0,7$$

(vgl. Beispiel 2.4). Die Erfolgswahrscheinlichkeit ist daher größer als 30% (unabhängig von der Anzahl der Gefangenen).

Definition 2.13. Die Anzahl der Permutationen von S_n mit genau k Zyklen nennt man *Stirling-Zahl erster Art* und schreibt dafür $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$. Fasst man die Identität auf der leeren Menge als Produkt von 0 Zyklen auf, so erhält man $\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right] = 1$.

Bemerkung 2.14. Für $n \in \mathbb{N}_0$ gilt

$$n! = |S_n| = \sum_{k=0}^n \left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right].$$

Beispiel 2.15.

- (i) Nach Definition ist $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] = 0$, falls $k = 0 < n$ oder $k > n$. Da id die einzige Permutation in S_n mit n Zyklen ist, gilt $\left[\begin{smallmatrix} n \\ n \end{smallmatrix} \right] = 1$. Im Gegensatz zum Binomialkoeffizient ist also im Allgemeinen $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] \neq \left[\begin{smallmatrix} n \\ n-k \end{smallmatrix} \right]$.
- (ii) Eine Permutation mit nur einem Zyklus ist ein n -Zyklus. Aus Satz 2.10 folgt $\left[\begin{smallmatrix} n \\ 1 \end{smallmatrix} \right] = (n-1)!$.
- (iii) Offenbar ist $\left[\begin{smallmatrix} n \\ n-1 \end{smallmatrix} \right]$ die Anzahl der Transpositionen und damit auch die Anzahl der 2-elementigen Teilmengen von $\{1, \dots, n\}$. Dies zeigt $\left[\begin{smallmatrix} n \\ n-1 \end{smallmatrix} \right] = \binom{n}{2}$.
- (iv) Nach Bemerkung 2.14 ist $\left[\begin{smallmatrix} 4 \\ 2 \end{smallmatrix} \right] = 4! - \left[\begin{smallmatrix} 4 \\ 1 \end{smallmatrix} \right] - \left[\begin{smallmatrix} 4 \\ 3 \end{smallmatrix} \right] - \left[\begin{smallmatrix} 4 \\ 4 \end{smallmatrix} \right] = 24 - 6 - 6 - 1 = 11$. Die entsprechenden Permutationen sind $(1, 2, 3)$, $(1, 3, 2)$, $(1, 2, 4)$, $(1, 4, 2)$, $(1, 3, 4)$, $(1, 4, 3)$, $(2, 3, 4)$, $(2, 4, 3)$, $(1, 2)(3, 4)$, $(1, 3)(2, 4)$, $(1, 4)(2, 3)$.

Lemma 2.16. Für $k, n \in \mathbb{N}$ gilt

$$\boxed{\left[\begin{smallmatrix} n \\ k-1 \end{smallmatrix} \right] + n \left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] = \left[\begin{smallmatrix} n+1 \\ k \end{smallmatrix} \right].}$$

Beweis. Sei $\sigma \in S_n$ mit genau $k-1$ Zyklen. Durch Anfügen des 1-Zyklus $(n+1)$ erhält man eine Permutation in S_{n+1} mit genau k Zyklen. Sei nun $\sigma \in S_n$ mit genau k Zyklen. Dann lässt sich die Ziffer $n+1$ an n Stellen in der Zyklendarstellung von σ anfügen (Beispiel: 4 einfügen in $(1, 2)(3)$ ergibt $(4, 1, 2)(3)$, $(1, 4, 2)(3)$, $(1, 2)(4, 3)$). Auf diese Weise erhält man n verschiedene Permutation in S_{n+1} mit genau k Zyklen. Offenbar entsteht jede Permutation von S_{n+1} mit genau k Zyklen auf genau eine der beiden Weisen. Dies zeigt die Behauptung. \square

Satz 2.17. Für $0 \leq k < n$ gilt

$$\boxed{\binom{n}{k} = \sum_{0 < a_1 < \dots < a_{n-k} < n} a_1 \dots a_{n-k}.}$$

Beweis. Induktion nach n : Für $k = 0$ erhält man die leere Summe, denn es gibt nur $n - 1$ natürliche Zahlen zwischen 1 und $n - 1$. In der Tat ist $\binom{n}{0} = 0$. Insbesondere gilt die Behauptung für $n = 1$. Sei nun $k > 0$ und die Behauptung für n bereits bewiesen. Nach Lemma 2.16 ist

$$\begin{aligned} \binom{n+1}{k} &= \binom{n}{k-1} + n \binom{n}{k} = \sum_{0 < a_1 < \dots < a_{n-k+1} < n} a_1 \dots a_{n-k+1} + n \sum_{0 < a_1 < \dots < a_{n-k} < n} a_1 \dots a_{n-k} \\ &= \sum_{0 < a_1 < \dots < a_{n+1-k} < n+1} a_1 \dots a_{n+1-k}. \quad \square \end{aligned}$$

Beispiel 2.18. Für $n \in \mathbb{N}$ gilt

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

(vgl. Beispiel 2.15).

Definition 2.19.

- Eine *Partition* einer (endlichen) Menge A ist eine Menge von paarweise disjunkten, nichtleeren Teilmengen $\{A_1, \dots, A_k\} \subseteq 2^A$ mit $A = A_1 \cup \dots \cup A_k$. Die Menge aller Partitionen von A bezeichnen wir mit $P(A)$. Man nennt $b(n) := |P(\{1, \dots, n\})|$ die *n-te Bellzahl*.
- Eine *Partition* von $n \in \mathbb{N}_0$ ist eine Multimenge $\lambda := \{k_1, \dots, k_s\} \subseteq \mathbb{N}$ mit $n = k_1 + \dots + k_s$. Man nennt k_1, \dots, k_s die *Teile* von λ . Die Menge aller Partitionen von n sei $P(n)$ und $p(n) := |P(n)|$.

Beispiel 2.20. Die Partitionen von $\{1, 2, 3\}$ sind $\{\{1, 2, 3\}\}$, $\{\{1\}, \{2, 3\}\}$, $\{\{2\}, \{1, 3\}\}$, $\{\{3\}, \{1, 2\}\}$ und $\{\{1\}, \{2\}, \{3\}\}$. Die Partitionen von 3 sind $3 = 1 + 2 = 1 + 1 + 1$. Also ist $b(3) = 5$ und $p(3) = 3$.

Bemerkung 2.21.

- Beachte: $b(0) = 1 = p(0)$, denn die leere (Multi)menge ist eine Partition von \emptyset (bzw. 0).
- Ist $\{A_1, \dots, A_k\}$ eine Partition einer endlichen Menge A , so ist $\{|A_1|, \dots, |A_k|\}$ eine Partition von $|A|$. Umgekehrt kann man aus jeder Partition von $n \in \mathbb{N}$ eine Partition von $\{1, \dots, n\}$ konstruieren. Daher gilt $b(n) \geq p(n)$ und $b(n) > p(n)$, falls $n \geq 3$.
- Wir werden Partitionen von Zahlen oft in der Form (k_1, \dots, k_s) mit $k_1 \geq \dots \geq k_s$ oder in der Form $(\underbrace{1, \dots, 1}_{m_1}, \dots, \underbrace{n, \dots, n}_{m_n})$ mit $m_1, \dots, m_n \in \mathbb{N}_0$ schreiben.
- Eine *Relation* auf einer Menge A ist eine Teilmenge $\sim \subseteq A \times A$. Man schreibt $a \sim b := \Leftrightarrow (a, b) \in \sim$. Man nennt \sim *Äquivalenzrelation*, falls für alle $a, b, c \in A$ gilt:
 - $a \sim a$ (reflexiv),
 - $a \sim b \implies b \sim a$ (symmetrisch),
 - $a \sim b \sim c \implies a \sim c$ (transitiv).

Für $a \in A$ nennt man $[a] := \{b \in A : a \sim b\}$ die *Äquivalenzklasse* von a . Sei

$$A/\sim := \{[a] : a \in A\}$$

die Menge der Äquivalenzklassen. Wegen $a \in [a]$ ist $\bigcup_{a \in A} [a] = A$. Sei nun $x \in [a] \cap [b]$ für $a, b \in A$. Mit $a \sim x$ gilt auch $x \sim a$. Für ein beliebiges $c \in A$ folgt

$$c \in [a] \implies x \sim a \sim c \implies b \sim x \sim c \implies b \sim c \implies c \in [b],$$

d. h. $[a] \subseteq [b]$. Aus Symmetriegründen gilt auch $[b] \subseteq [a]$, also $[a] = [b]$. Je zwei Äquivalenzklassen sind also entweder gleich oder disjunkt. Somit ist A/\sim eine Partition von A .

(v) Ist umgekehrt eine Partition $\{A_1, \dots, A_k\}$ von A gegeben, so erhält man durch

$$a \sim b : \iff \exists i : a, b \in A_i$$

eine Äquivalenzrelation auf A . Dabei gilt $A/\sim = \{A_1, \dots, A_k\}$. Auf diese Weise entsprechen sich Partitionen und Äquivalenzrelationen.

Beispiel 2.22. Die Gleichheitsrelation $=$ ist eine Äquivalenzrelation auf jeder Menge A . Die entsprechende Partition ist $\{\{a\} : a \in A\}$.

Satz 2.23. Sei $(1^{a_1}, \dots, n^{a_n})$ eine Partition von n . Dann besitzt jede n -elementige Menge genau

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

Partitionen der Form $\{A_1, \dots, A_l\}$ mit $\{|A_1|, \dots, |A_l|\} = (1^{a_1}, \dots, n^{a_n})$.

Beweis. O. B. d. A. sei $A = \{1, \dots, n\}$. Man kann jede Anordnung b_1, \dots, b_n der Zahlen $1, \dots, n$ in eine Partition des gesuchten Typs verwandeln, indem man entsprechende Klammern $\{$ und $\}$ verteilt. Wir können dabei zunächst die a_1 1-elementigen Teilmengen klammern, danach die a_2 2-elementigen Teilmengen usw.:

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

Von den $n!$ möglichen Anordnungen b_1, \dots, b_n führen allerdings einige zur gleichen Partition. Man kann einerseits die Elemente jeder k -elementigen Teilmenge beliebig permutieren, ohne die Partition zu verändern. Andererseits kann man die a_k k -elementigen Teilmengen untereinander permutieren, ohne die Partition zu verändern. Je $\prod_{k=1}^n (k!)^{a_k} a_k!$ Anordnungen führen daher zur gleichen Partition. Dies zeigt die Behauptung. \square

Beispiel 2.24. Die Anzahl der Partitionen von $\{1, 2, 3, 4\}$ vom Typ $(2, 2) = (1^0, 2^2)$ ist $\frac{4!}{(2!)^2 2!} = \frac{24}{8} = 3$. Diese sind $\{\{1, 2\}, \{3, 4\}\}$, $\{\{1, 3\}, \{2, 4\}\}$ und $\{\{1, 4\}, \{2, 3\}\}$.

Definition 2.25. Ist $\sigma \in S_n$ ein disjunktes Produkt von $a_i \geq 0$ Zyklen der Länge i , so nennt man $(1^{a_1}, \dots, n^{a_n})$ den *Zyklentyp* von σ . Nach Lemma 2.7 ist dies eine wohldefinierte Partition von n . Die Anzahl der Fixpunkte von σ ist a_1 .

Satz 2.26. Die Anzahl der Permutationen von S_n mit Zyklentyp $(1^{a_1}, \dots, n^{a_n})$ ist

$$\frac{n!}{1^{a_1} \dots n^{a_n} a_1! \dots a_n!}$$

Beweis. Fasst man Zyklen als Teilmengen von $\{1, \dots, n\}$ auf, so entspricht jede Permutation einer Partition von $\{1, \dots, n\}$. Nach Satz 2.23 entsprechen die Permutationen mit Zyklentyp $(1^{a_1}, \dots, n^{a_n})$ dabei genau

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

Partitionen. Es bleibt zu zählen wie viele Permutationen die gleiche Partition liefern. Da sich jeder k -Zyklus eindeutig in der Form (b_1, \dots, b_k) mit $b_1 := \min\{b_1, \dots, b_k\}$ schreiben lässt, liefern genau $(k-1)!$ Zyklen die gleiche Menge $\{b_1, \dots, b_k\}$ (man kann die b_2, \dots, b_k beliebig permutieren). Die Anzahl der gesuchten Permutationen ist daher

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

Beispiel 2.27. Die k -Zyklen von S_n haben Zyklentyp $(1^{n-k}, k^1)$. Deren Anzahl ist $\frac{n!}{1^{n-k}(n-k)!k^1 1!} = \frac{n!}{k(n-k)!}$ in Übereinstimmung mit Satz 2.10.

Definition 2.28. Die Anzahl der k -elementigen Partitionen einer n -elementigen Menge nennt man *Stirling-Zahl zweiter Art* und schreibt dafür $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$.

Bemerkung 2.29.

- (i) Da jede Permutation mit k Zyklen eine Partition mit k Teilmengen definiert, ist $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} \leq \left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ für alle $k, n \in \mathbb{N}$.
- (ii) Es gilt $b(n) = |P(\{1, \dots, n\})| = \sum_{k=0}^n \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$.

Beispiel 2.30.

- (i) Wie üblich ist $\left\{ \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right\} = 1$ und $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = 0$ für $k = 0 < n$ oder $k > n$. Außerdem ist $\left\{ \begin{smallmatrix} n \\ 1 \end{smallmatrix} \right\} = 1 = \left\{ \begin{smallmatrix} n \\ n \end{smallmatrix} \right\}$ und $\left\{ \begin{smallmatrix} n \\ n-1 \end{smallmatrix} \right\} = \left[\begin{smallmatrix} n \\ n-1 \end{smallmatrix} \right] = \binom{n}{2}$.
- (ii) Jede 2-elementige Partition von A hat die Form $\{B, A \setminus B\}$ mit $B \in 2^A \setminus \{\emptyset, A\}$. Dies zeigt $\left\{ \begin{smallmatrix} n \\ 2 \end{smallmatrix} \right\} = \frac{1}{2}(|2^{\{1, \dots, n\}}| - 2) \stackrel{1.4}{=} 2^{n-1} - 1$.
- (iii) Nach Bemerkung 2.29 ist $b(4) = \left\{ \begin{smallmatrix} 4 \\ 1 \end{smallmatrix} \right\} + \left\{ \begin{smallmatrix} 4 \\ 2 \end{smallmatrix} \right\} + \left\{ \begin{smallmatrix} 4 \\ 3 \end{smallmatrix} \right\} + \left\{ \begin{smallmatrix} 4 \\ 4 \end{smallmatrix} \right\} = 1 + 2^3 - 1 + \binom{4}{2} + 1 = 15$.

Lemma 2.31. Für $k, n \in \mathbb{N}$ gilt

$$\left\{ \begin{smallmatrix} n \\ k-1 \end{smallmatrix} \right\} + k \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} n+1 \\ k \end{smallmatrix} \right\}.$$

Beweis. Sei $A = \{1, \dots, n\}$ und $\{A_1, \dots, A_{k-1}\}$ eine Partition von A . Dann ist $\{A_1, \dots, A_{k-1}, \{n+1\}\}$ eine k -elementige Partition von $\{1, \dots, n+1\}$. Sei nun $\{A_1, \dots, A_k\}$ eine Partition von A . Dann kann man die Zahl $n+1$ zu jeder der Mengen A_1, \dots, A_k hinzufügen und erhält auf diese Weise eine k -elementige Partition von $\{1, \dots, n+1\}$. Offenbar entsteht jede k -elementige Partition von $\{1, \dots, n+1\}$ auf genau einer der beiden Weisen. Dies zeigt die Behauptung. \square

Satz 2.32. Für $0 \leq k < n$ gilt

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \sum_{1 \leq a_1 \leq \dots \leq a_{n-k} \leq k} a_1 \dots a_{n-k}.$$

Beweis. Induktion nach n : Für $k = 0$ erhält man die leere Summe in Übereinstimmung mit $\left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = 0$. Insbesondere gilt die Behauptung für $n = 1$. Sei nun $k > 0$ und die Behauptung für n bereits bewiesen. Nach Lemma 2.31 ist

$$\begin{aligned} \left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} &= \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\} + k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \sum_{1 \leq a_1 \leq \dots \leq a_{n-k+1} \leq k-1} a_1 \dots a_{n-k+1} + k \sum_{1 \leq a_1 \leq \dots \leq a_{n-k} \leq k} a_1 \dots a_{n-k} \\ &= \sum_{1 \leq a_1 \leq \dots \leq a_{n+1-k} \leq k} a_1 \dots a_{n+1-k}. \quad \square \end{aligned}$$

Beispiel 2.33. Für $n \in \mathbb{N}$ gilt

$$\left\{ \begin{matrix} n \\ 2 \end{matrix} \right\} = \sum_{1 \leq a_1 \leq \dots \leq a_{n-2} \leq 2} a_1 \dots a_{n-2} = \sum_{k=0}^{n-2} 2^k = 2^{n-1} - 1$$

(vgl. Beispiel 2.30).

Bemerkung 2.34. Man vergleiche das folgende Ergebnis mit Satz 1.9.

Satz 2.35. Für endliche Mengen A und B existieren genau $\left\{ \begin{matrix} |A| \\ |B| \end{matrix} \right\} |B|!$ surjektive Abbildungen $A \rightarrow B$.

Beweis. O. B. d. A. sei $B = \{1, \dots, k\}$. Jede surjektive Abbildung $f: A \rightarrow B$ liefert eine k -elementige Partition $\{f^{-1}(1), \dots, f^{-1}(k)\}$ von A . Für $\sigma \in \text{Sym}(B)$ ist auch $\sigma \circ f: A \rightarrow B$ surjektiv und führt zur Partition

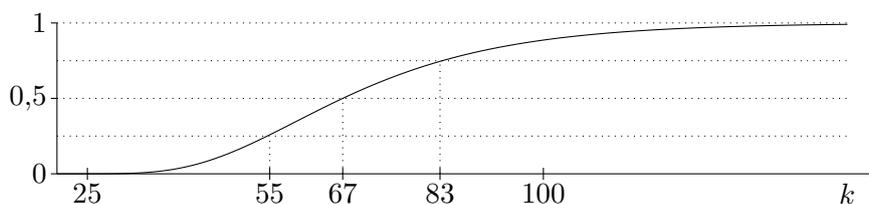
$$\{(\sigma \circ f)^{-1}(1), \dots, (\sigma \circ f)^{-1}(k)\} = \{f^{-1}(\sigma^{-1}(1)), \dots, f^{-1}(\sigma^{-1}(k))\} = \{f^{-1}(1), \dots, f^{-1}(k)\}.$$

Man sieht leicht, dass dies die einzigen Abbildungen sind, die zur gleichen Partition führen. Die Anzahl der surjektiven Abbildungen ist daher $\left\{ \begin{matrix} |A| \\ k \end{matrix} \right\} |\text{Sym}(B)| = \left\{ \begin{matrix} |A| \\ k \end{matrix} \right\} k!$. \square

Beispiel 2.36 (Sammelbilderproblem). Bei jedem Einkauf im Supermarkt bekommen Sie eine von n verschiedenen Sammelkarten (zufällig und gleichverteilt). Wie hoch ist die Wahrscheinlichkeit, dass Sie nach k Einkäufen alle Sammelkarten besitzen? Die k Einkäufe liefern eine Abbildung $\{1, \dots, k\} \rightarrow \{1, \dots, n\}$. Es gibt n^k solche Abbildungen, von denen $\left\{ \begin{matrix} k \\ n \end{matrix} \right\} n!$ surjektiv sind. Die Wahrscheinlichkeit ist daher

$$\frac{n!}{n^k} \left\{ \begin{matrix} k \\ n \end{matrix} \right\}.$$

Für $n = 20$ erhält man:



Satz 2.37. Für $k, n \in \mathbb{N}_0$ gilt

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

Beweis. Sei $A := \{1, \dots, n\}$, $B := \{1, \dots, k\}$ und M die Menge der surjektiven Abbildungen von A nach B . Nach Satz 2.35 genügt es $|M| = \sum_{l=0}^k (-1)^{k-l} \binom{k}{l} l^n$ zu zeigen. Für $i = 1, \dots, k$ sei

$$M_i := \{f : A \rightarrow B : i \notin f(A)\}.$$

Für $1 \leq i_1 < \dots < i_l \leq k$ ist dann $M_{i_1} \cap \dots \cap M_{i_l}$ die Menge aller Abbildungen von A nach $B \setminus \{i_1, \dots, i_l\}$. Insbesondere ist $|M_{i_1} \cap \dots \cap M_{i_l}| = (k-l)^n$ nach Bemerkung 1.7. Satz 1.25 zeigt

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

Die Behauptung folgt aus $\binom{k}{l} = \binom{k}{k-l}$. □

Bemerkung 2.38. Aus Satz 2.37 folgt

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

Asymptotisch gilt die *Stirling-Formel*

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

d. h.

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

(ohne Beweis). Beispiel: $100! \approx 9,333 \cdot 10^{157}$ und $\sqrt{200\pi} (100/e)^{100} \approx 9,325 \cdot 10^{157}$.

Satz 2.39 (DOBIŃSKI-Formel). Für $n \in \mathbb{N}_0$ ist

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

Beweis. Wegen $\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = 0$ für $k > n$ gilt

$$\begin{aligned} b(n) &\stackrel{2.29}{=} \sum_{k=0}^{\infty} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \stackrel{2.37}{=} \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{l=0}^k (-1)^{k-l} \binom{k}{l} l^n = \sum_{k=0}^{\infty} \sum_{l=0}^k (-1)^{k-l} \frac{l^n}{l!(k-l)!} \\ &= \sum_{k=0}^{\infty} \sum_{l=0}^k \frac{(-1)^l}{l!} \frac{(k-l)^n}{(k-l)!} \stackrel{(*)}{=} \left(\sum_{l=0}^{\infty} \frac{(-1)^l}{l!} \right) \left(\sum_{k=0}^{\infty} \frac{k^n}{k!} \right) = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}, \end{aligned}$$

wobei in (*) die Cauchy-Produktformel für absolut konvergente Reihe benutzt wird (Analysis). □

Satz 2.40. Für $n \in \mathbb{N}_0$ ist

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

Beweis. Sei \mathcal{A} eine Partition von $\{1, \dots, n+1\}$ und $n+1 \in A \in \mathcal{A}$ mit $k := |A| - 1 \geq 0$. Dann gibt es $\binom{n}{k}$ Möglichkeiten für A und $\mathcal{A} \setminus \{A\}$ ist eine Partition $\{1, \dots, n\} \setminus A$. Für $\mathcal{A} \setminus \{A\}$ gibt es also $b(n-k)$ Möglichkeiten. Es folgt

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

Bemerkung 2.41. Man kennt keine einfache Formel für $p(n)$. Hardy und Ramanujan haben aber

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

bewiesen. Beispiel: $p(10^4) \approx 3,617 \cdot 10^{106}$ und $\frac{e^{\pi\sqrt{20000/3}}}{40000\sqrt{3}} \approx 3,633 \cdot 10^{106}$.

3. Möbius-Inversion

Definition 3.1. Eine Relation \leq auf einer Menge A heißt *Ordnungsrelation* (oder *partielle Ordnung*), falls für alle $a, b, c \in A$ gilt:

- $a \leq a$ (reflexiv),
- $a \leq b \leq a \implies a = b$ (antisymmetrisch),
- $a \leq b \leq c \implies a \leq c$ (transitiv).

Gegebenenfalls nennt man (A, \leq) eine *geordnete Menge*. Man schreibt auch $a \geq b$, falls $b \leq a$ und $a < b$ (bzw. $a > b$), falls $a \leq b \neq a$ (bzw. $b \leq a \neq b$).

Beispiel 3.2.

- (i) Die übliche „Kleiner-gleich-Relation“ \leq auf \mathbb{R} .
- (ii) Die Teilmengenrelation \subseteq auf 2^A für jede Menge A .
- (iii) Die Teilbarkeitsrelation $|$ auf \mathbb{N} , aber nicht auf \mathbb{Z} , denn $1 | -1 | 1$.
- (iv) Für jede geordnete Menge (A, \leq) ist auch (A, \geq) eine geordnete Menge.
- (v) Für geordnete Mengen $(A_1, \leq_1), \dots, (A_n, \leq_n)$ ist $A_1 \times \dots \times A_n$ durch

$$(a_1, \dots, a_n) < (b_1, \dots, b_n) :\iff \exists k \in \mathbb{N}_0 : a_1 = b_1, \dots, a_k = b_k, a_{k+1} <_{k+1} b_{k+1}$$

lexikografisch geordnet.

Definition 3.3. Für eine geordnete Menge (A, \leq) und $a, b \in A$ sei

$$[a, b] := \{c \in A : a \leq c \leq b\}.$$

Man nennt (A, \leq) *lokal endlich*, falls $|\{b \in A : b \leq a\}| < \infty$ für alle $a \in A$ gilt. Gegebenenfalls definiert man die *Möbius-Funktion* $\mu_A : A \times A \rightarrow \mathbb{Z}$ rekursiv durch

$$\mu_A(a, b) := \begin{cases} 1 & \text{falls } a = b, \\ -\sum_{a \leq x < b} \mu_A(a, x) & \text{falls } a \neq b. \end{cases}$$

Bemerkung 3.4. In der Situation von Definition 3.3 gilt $\sum_{x \in [a,b]} \mu_A(a, x) = 0$, falls $a \neq b$. Wir zeigen $\sum_{x \in [a,b]} \mu_A(x, b) = 0$ durch Induktion nach $k := |[a, b]| \geq 2$. Für $k = 2$ ist

$$\sum_{x \in [a,b]} \mu_A(x, b) = \mu_A(a, b) + \mu_A(b, b) = \mu_A(a, b) + \mu_A(a, a) = \sum_{x \in [a,b]} \mu_A(a, x) = 0.$$

Sei nun die Behauptung für $k - 1$ bereits bewiesen. Dann gilt

$$\begin{aligned} \sum_{x \in [a,b]} \mu_A(x, b) &= \mu_A(b, b) - \sum_{a \leq x < b} \sum_{x \leq y < b} \mu_A(x, y) = \mu_A(a, a) - \sum_{a \leq y < b} \sum_{x \in [a,y]} \mu_A(x, y) \\ &= \mu_A(a, a) - \mu_A(a, a) = 0. \end{aligned}$$

Satz 3.5 (MÖBIUS-INVERSION). Sei (A, \leq) lokal endlich. Für $f, F: A \rightarrow \mathbb{R}$ sind dann äquivalent:

(1) $\boxed{F(a) = \sum_{x \leq a} f(x)}$ für alle $a \in A$.

(2) $\boxed{f(a) = \sum_{x \leq a} \mu_A(x, a) F(x)}$ für alle $a \in A$.

Beweis. Da (A, \leq) lokal endlich ist, sind die Summen wohldefiniert. Sei $F(a) = \sum_{x \leq a} f(x)$ für alle $a \in A$. Dann gilt

$$\sum_{x \leq a} \mu_A(x, a) F(x) = \sum_{x \leq a} \mu_A(x, a) \sum_{y \leq x} f(y) = \sum_{y \leq a} f(y) \sum_{x \in [y,a]} \mu_A(x, a) \stackrel{3.4}{=} f(a).$$

Sei nun umgekehrt $f(a) = \sum_{x \leq a} \mu_A(x, a) F(x)$ für alle $a \in A$. Dann folgt

$$\sum_{x \leq a} f(x) = \sum_{x \leq a} \sum_{y \leq x} \mu_A(y, x) F(y) = \sum_{y \leq a} F(y) \sum_{x \in [y,a]} \mu_A(y, x) \stackrel{3.4}{=} F(a). \quad \square$$

Bemerkung 3.6. Satz 3.5 ist besonders nützlich, wenn μ_A eine einfache Form hat.

Beispiel 3.7.

- (i) Für jede Menge A ist $(A, =)$ lokal endlich. Die Möbius-Funktion ist das Kronecker-Delta $\mu_A(a, b) = \delta_{ab}$ und die Möbius-Inversion reduziert sich auf $f = F$.
- (ii) Offenbar ist (\mathbb{N}, \leq) lokal endlich. Für $a \in \mathbb{N}$ gilt $\mu_{\mathbb{N}}(a, a) = 1$, $\mu_{\mathbb{N}}(a, a+1) = -\mu_{\mathbb{N}}(a, a) = -1$ und $\mu_{\mathbb{N}}(a, a+2) = -1 + 1 = 0$. Induktiv zeigt man leicht $\mu_{\mathbb{N}}(a, b) = 0$ für $b \notin \{a, a+1\}$. Satz 3.5 liefert in diesem Fall

$$F(n) = \sum_{k=1}^n f(k) \iff f(n) = F(n) - F(n-1).$$

Dies ist eine diskrete Version des Hauptsatzes der Differential- und Integralrechnung (F entspricht dem Integral von f und f entspricht der Ableitung von F).

(iii) Für jede endliche Menge A ist $(2^A, \subseteq)$ lokal endlich. Wir zeigen

$$\mu_{2^A}(X, Y) = \begin{cases} (-1)^{|Y \setminus X|} & \text{falls } X \subseteq Y, \\ 0 & \text{falls } X \not\subseteq Y. \end{cases}$$

Die Fälle $X = Y$ und $X \not\subseteq Y$ sind klar. Sei also $X \subsetneq Y$ und $k := |Y \setminus X| \geq 1$. Induktiv nehmen wir an, dass die Aussage für $k - 1$ bereits gilt. Dann ist

$$\begin{aligned} \mu_{2^A}(X, Y) &= - \sum_{X \subseteq Z \subsetneq Y} \mu_{2^A}(X, Z) = - \sum_{X \subseteq Z \subsetneq Y} (-1)^{|Z \setminus X|} \\ &= - \sum_{l=0}^{k-1} \binom{k}{l} (-1)^l = -(1-1)^k + (-1)^k = (-1)^k. \end{aligned}$$

Für $f, F: 2^A \rightarrow \mathbb{R}$ gilt daher

$$F(B) = \sum_{X \subseteq B} f(X) \iff f(B) = \sum_{X \subseteq B} (-1)^{|B \setminus X|} F(X).$$

Ersetzt man \subseteq durch \supseteq , so erhält man analog

$$F(B) = \sum_{X \supseteq B} f(X) \iff f(B) = \sum_{X \supseteq B} (-1)^{|X \setminus B|} F(X). \quad (3.1)$$

(iv) Seien A_1, \dots, A_n endliche Mengen und $N := \{1, \dots, n\}$. Wir definieren $f, F: 2^N \rightarrow \mathbb{R}$ durch

$$\begin{aligned} f(I) &:= \left| \bigcap_{i \in I} A_i \setminus \bigcup_{j \in N \setminus I} A_j \right|, \\ F(I) &:= \left| \bigcap_{i \in I} A_i \right| \end{aligned}$$

für $I \subseteq N$. Für $a \in \bigcap_{i \in I} A_i$ existiert genau ein $J \supseteq I$ mit $a \in \bigcap_{j \in J} A_j \setminus \bigcup_{l \in N \setminus J} A_l$. Dies zeigt $F(I) = \sum_{J \supseteq I} f(J)$ und (3.1) liefert

$$0 = f(\emptyset) = \sum_{I \supseteq \emptyset} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right| = |A_1 \cup \dots \cup A_n| + \sum_{\emptyset \neq I \subseteq N} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|.$$

Dies ist genau das Inklusions-Exklusions-Prinzip.

(v) Auch $(\mathbb{N}, |)$ ist lokal endlich. Sei $n = p_1^{a_1} \dots p_s^{a_s}$ die Primfaktorzerlegung von $n \in \mathbb{N}$. Wir definieren die *klassische Möbius-Funktion* $\mu: \mathbb{N} \rightarrow \mathbb{R}$ durch

$$\mu(n) := \begin{cases} (-1)^s & \text{falls } a_1 = \dots = a_s = 1, \\ 0 & \text{sonst.} \end{cases}$$

Beachte: $\mu(1) = (-1)^0 = 1$. Es gilt dann

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{k=0}^s \sum_{q_1, \dots, q_k \in \{p_1, \dots, p_s\}} \mu(q_1 \dots q_k) = \sum_{k=0}^s \sum_{\substack{M \subseteq \{p_1, \dots, p_s\} \\ |M|=k}} (-1)^k \\ &= \sum_{k=0}^s (-1)^k \binom{s}{k} = (1-1)^s = 0, \end{aligned}$$

falls $n \neq 1$. Wir zeigen $\mu_{\mathbb{N}}(a, b) = \mu(b/a)$, falls $a \mid b$. Dies ist klar für $a = b$. Wir nehmen nun $a \neq b$ an und argumentieren durch Induktion nach b/a . Dann gilt

$$\mu_{\mathbb{N}}(a, b) = - \sum_{\substack{a \mid x \mid b \\ x \neq b}} \mu_{\mathbb{N}}(a, x) = - \sum_{\substack{a \mid x \mid b \\ x \neq b}} \mu(x/a) = \mu(b/a) - \sum_{y \mid \frac{b}{a}} \mu(y) = \mu(b/a).$$

Satz 3.5 hat also folgende Form

$$\boxed{F(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu(n/d) F(d).} \quad (3.2)$$

(vi) Sei $n = p_1^{a_1} \dots p_s^{a_s}$ die Primfaktorzerlegung von $n \in \mathbb{N}$. Dann gilt

$$\sum_{d \mid n} \mu(n/d) d = \sum_{t=0}^s \sum_{1 \leq i_1 < \dots < i_t \leq s} (-1)^t \frac{n}{p_{i_1} \dots p_{i_t}} = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right) = \varphi(n)$$

nach Satz 1.27. Gleichung 3.2 zeigt

$$\boxed{\sum_{d \mid n} \varphi(d) = n.}$$

Bemerkung 3.8. Man kann Satz 3.5 verallgemeinern, indem man \mathbb{R} durch eine beliebige abelsche Gruppe (G, \cdot) ersetzt. Man erhält dann

$$\boxed{F(a) = \prod_{x \leq a} f(x) \iff f(a) = \prod_{x \leq a} F(x)^{\mu(x, a)}}$$

(Beweis ist genau der gleiche).

Definition 3.9. Sei (A, \leq) eine lokal endliche geordnete Menge und $a, b \in A$. Ein Weg der Länge $l \leq 0$ zwischen a und b ist eine Folge der Form $a = x_1 < \dots < x_{k+1} = b$ mit $x_1, \dots, x_{k+1} \in A$.

Satz 3.10 (HALL). Sei (A, \leq) eine lokal endliche geordnete Menge und $a, b \in A$. Sei w_l die Anzahl der Wege der Länge l zwischen a und b . Dann gilt

$$\mu_A(a, b) = w_0 - w_1 + w_2 \mp \dots$$

Beweis. Induktion nach $k := |[a, b]| < \infty$. In der Summe sind nur endlich viele Summanden ungleich 0, denn $c_l = 0$ für $l \geq k$. Im Fall $k = 1$ gibt es nur den Weg der Länge 0 zwischen a und a , d. h. $\mu_A(a, a) = 1 = c_0$. Sei nun $k \geq 2$ und die Behauptung für $k - 1$ bereits bewiesen. Sei $a = x_1 < \dots < x_{l+1} = b$ und $c := x_l$. Dann ist $x_1 < \dots < x_l$ ein Weg der Länge $l - 1$ zwischen a und c . Nach Induktion liefert dieser Weg den Beitrag $(-1)^l$ zu $\mu_A(a, c)$. Wegen $\mu_A(a, b) = - \sum_{a \leq c < b} \mu_A(a, c)$ liefert $x_1 < \dots < x_{l+1}$ den Beitrag $(-1)^{l+1}$ zu $\mu_A(a, b)$. Umgekehrt lässt sich jeder Weg der Länge $l - 1$ zwischen a und c zu einem Weg der Länge l zwischen a und b fortsetzen. Dies zeigt die Behauptung. \square

4. Potenzreihen

Bemerkung 4.1. Für viele Zählprobleme kennt man keine einfachen Formeln (man denke an $p(n)$). Oft ist es günstiger die Folge der gewünschten Anzahlwerte in ihrer Gesamtheit zu betrachten. Durch geschickte algebraische Umformungen kann man dadurch neue Identitäten generieren. In diesem Abschnitt werden hierfür die Grundlagen gelegt.

Definition 4.2. Für einen Körper K sei $K[[X]] := K^{\mathbb{N}_0} = \{(a_0, a_1, \dots) : a_i \in K\}$. Zwei Elemente $\alpha := (a_0, \dots)$ und $\beta := (b_0, \dots)$ von $K[[X]]$ lassen sich wie folgt addieren und multiplizieren:

$$\alpha + \beta := (a_0 + b_0, a_1 + b_1, \dots) \in K[[X]],$$

$$\alpha \cdot \beta := (a_0 b_0, a_1 b_0 + a_0 b_1, \dots, \sum_{i=0}^n a_i b_{n-i}, \dots) \in K[[X]].$$

Wir setzen $0 := (0, 0, \dots) \in K[[X]]$ und $1 := (1, 0, 0, \dots) \in K[[X]]$.

Lemma 4.3. Für $\alpha, \beta, \gamma \in K[[X]]$ gilt

$$\begin{aligned} (\alpha + \beta) + \gamma &= \alpha + (\beta + \gamma) & \alpha + \beta &= \beta + \alpha & \alpha + 0 &= \alpha \\ (\alpha \cdot \beta) \cdot \gamma &= \alpha \cdot (\beta \cdot \gamma) & \alpha \cdot \beta &= \beta \cdot \alpha & \alpha \cdot 1 &= \alpha \\ \alpha \cdot (\beta + \gamma) &= (\alpha \cdot \beta) + (\alpha \cdot \gamma) & \exists \delta \in K[[X]] : \alpha + \delta &= 0, & \alpha\beta = 0 &\implies \alpha = 0 \vee \beta = 0. \end{aligned}$$

Beweis. Die ersten drei Aussagen folgen direkt aus den entsprechenden Axiomen in K . Sei nun $\alpha = (a_0, \dots)$, $\beta = (b_0, \dots)$ und $\gamma = (c_0, \dots)$. Für $\delta := (-a_0, -a_1, \dots)$ gilt dann $\alpha + \delta = 0$. Der n -te Eintrag von $\alpha \cdot (\beta \cdot \gamma)$ ist

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

Dies zeigt $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$. Wegen $\sum_{i=0}^n a_i b_{n-i} = \sum_{i=0}^n b_i a_{n-i}$ ist $\alpha \cdot \beta = \beta \cdot \alpha$. Die Gleichung $\alpha \cdot 1 = \alpha$ ist leicht zu sehen. Der n -te Eintrag von $\alpha \cdot (\beta + \gamma)$ ist

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

und $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$ folgt. Sei schließlich $\alpha\beta = 0$. Nehmen wir indirekt $\alpha \neq 0 \neq \beta$ an. Sei $k := \min\{n \in \mathbb{N}_0 : a_n \neq 0\}$ und $l := \min\{n \in \mathbb{N}_0 : b_n \neq 0\}$. Der $(k+l)$ -te Eintrag von $\alpha\beta$ ist dann $\sum_{i=0}^{k+l} a_i b_{k+l-i} = a_k b_l \neq 0$. Dieser Widerspruch zeigt $\alpha = 0$ oder $\beta = 0$. \square

Bemerkung 4.4.

- (i) Lemma 4.3 besagt, dass man in $K[[X]]$ wie in \mathbb{Z} rechnen kann. Man nennt $K[[X]]$ *Ring der (formalen) Potenzreihen*. Seine Elemente schreibt man auch in der Form $\sum_{n=0}^{\infty} a_n X^n = a_0 + a_1 X + a_2 X^2 + \dots$, wobei $X = (0, 1, 0, 0, \dots)$ eine *Unbekannte* ist. Es gilt dabei

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

Bei der Multiplikation von Potenzreihen multipliziert man summandenweise und fasst anschließend gleiche X -Potenzen zusammen. Man nennt a_0 das *Absolutglied* von α . Wenn der Summationsbereich

klar ist, schreiben wir kürzer $\sum a_n X^n$. Außerdem werden wir das Multiplikationssymbol \cdot weglassen und „Punkt- vor Strichrechnung“ benutzen, d. h. $\alpha\beta + \gamma := (\alpha \cdot \beta) + \gamma$. Das Inverse von α bzgl. $+$ sei $-\alpha$. Wie üblich schreiben wir $\alpha - \beta$ anstatt $\alpha + (-\beta)$.

- (ii) Die Bedeutung des Wortes „formal“ liegt darin, dass wir im Gegensatz zur Analysis keine Konvergenz beachten, da X stets eine Unbekannte und keine reelle Zahl ist (daher auch die Verwendung des Großbuchstabens). Stattdessen führen wir in Definition 4.11 eine viel einfachere Metrik auf $K[[X]]$ ein.
- (iii) Für $\alpha \in K[[X]]$ definieren wir $\alpha K[[X]] := \{\alpha\beta : \beta \in K[[X]]\}$. Zum Beispiel ist $XK[[X]]$ die Menge der Potenzreihen mit Absolutglied 0.
- (iv) Man kann $K[[X]]$ zu einem Körper $K((X))$ erweitern, indem man Potenzreihen durch (formale) *Laurent-Reihen* der Form $\sum_{n=k}^{\infty} a_n X^n$ mit $k \in \mathbb{Z}$ und $a_n \in K$ ersetzt (Aufgabe 25).

Beispiel 4.5. Für jeden Körper K existieren $\sum_{n=0}^{\infty} X^n$, $\sum nX^n$ und $\sum (-1)^n X^n \in K[[X]]$. Außerdem ist

$$\boxed{\exp(X) := \sum_{n=0}^{\infty} \frac{X^n}{n!} = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \dots \in \mathbb{Q}[[X]]} \quad ((\text{formale}) \text{ Exponentialfunktion}).$$

Es gilt

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

Definition 4.6. Man nennt $\alpha \in K[[X]]$ *invertierbar*, falls ein $\beta \in K[[X]]$ mit $\alpha\beta = 1$ existiert.

Bemerkung 4.7.

- (i) Sind α, β, γ mit $\alpha\beta = 1 = \alpha\gamma$, so gilt $\alpha(\beta - \gamma) = 0$ und es folgt $\beta = \gamma$, denn anderenfalls wäre $1 = \alpha\beta = 0\beta = 0$. Also existiert höchstens ein β mit $\alpha\beta = 1$. Man nennt β das *Inverse* von α und schreibt $\alpha^{-1} := \beta$ oder $1/\alpha$. Allgemeiner setzen wir

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

für $k \in \mathbb{Z}$.

- (ii) Für $\alpha, \beta, \gamma \in K[[X]]$ mit $\alpha\beta = \gamma$ schreiben wir $\frac{\gamma}{\beta} := \alpha$, falls $\beta \neq 0$ (wie in (i) ist dies wohldefiniert).

Lemma 4.8. Sei $\alpha = \sum a_n X^n \in K[[X]]$.

- (i) Genau dann ist α invertierbar, wenn $a_0 \neq 0$ gilt.
- (ii) Existiert ein $m \in \mathbb{N}$ mit $\alpha^m = 1$, so ist $\alpha \in K$.

Beweis.

- (i) Sei $\beta = \sum b_n X^n \in K[[X]]$ mit $\alpha\beta = 1$. Dann ist $a_0 b_0 = 1$ und $a_0 \neq 0$. Sei umgekehrt $a_0 \neq 0$. Wir definieren $b_0, b_1, \dots \in K$ induktiv durch $b_0 := 1/a_0$ und

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

für $k \in \mathbb{N}$. Es gilt dann

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

Dies zeigt $\alpha\beta = 1$ für $\beta := \sum b_n X^n$.

- (ii) Wir können $m > 1$ annehmen. Für einen Primteiler p von m gilt $(\alpha^{m/p})^p = 1$. Durch Induktion nach m dürfen wir daher $m = p$ voraussetzen. Sei indirekt $\alpha \notin K$ und $n \in \mathbb{N}$ minimal mit $a_n \neq 0$. Der n -te Koeffizient von $\alpha^p = 1$ ist $pa_0^{p-1}a_n = 0$. Da α invertierbar ist ($\alpha^{-1} = \alpha^{m-1}$), gilt $a_0 \neq 0$ und es folgt $p = 0$ in K (gilt beispielsweise für $|K| = p$). Wir untersuchen nun den Koeffizienten von X^{np} in α^p . Dieser hängt nur von a_0, \dots, a_{np} ab. Nach dem Multinomialssatz gilt

$$(a_0 + \dots + a_{np} X^{np})^p = \sum_{\substack{(k_0, \dots, k_{np}) \in \mathbb{N}_0^{np+1} \\ k_0 + \dots + k_{np} = p}} \binom{p}{k_0, \dots, k_{np}} a_0^{k_0} \dots a_{np}^{k_{np}} X^{k_1 + 2k_2 + \dots + npk_{np}}.$$

Für $k_0, \dots, k_{np} < p$ ist $\binom{p}{k_0, \dots, k_{np}}$ offenbar durch p teilbar und verschwindet daher in K . Es bleiben somit nur die Multimengen $\{k_0, \dots, k_{np}\} = \{0, \dots, 0, p\}$, d. h.

$$(a_0 + \dots + a_{np} X^{np})^p = a_0^p + a_n^p X^{np} + a_{n+1}^p X^{(n+1)p} + \dots + a_{np}^p X^{np^2}.$$

Der np -te Koeffizient von α^p ist also $a_n^p \neq 0$ im Widerspruch zu $\alpha^p = 1$. □

Bemerkung 4.9. Sind $\alpha, \beta \in K[[X]]$ invertierbar, so auch α^{-1} und $\alpha\beta$ nach Lemma 4.8. In diesem Fall ist $(\alpha^{-1})^{-1} = \alpha$ und $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$. Die invertierbaren Potenzreihen bilden bzgl. Multiplikation eine abelsche Gruppe mit neutralem Element 1 (vgl. Definition 10.2). Man nennt sie *Einheitengruppe* von $K[[X]]$ und schreibt dafür $K[[X]]^\times$. Nach Lemma 4.8 gilt $K[[X]]^\times = K[[X]] \setminus XK[[X]]$.

Beispiel 4.10.

- (i) Nach Beispiel 4.5 ist $\frac{1}{1-X} = \sum X^n$ die (formale) *geometrische Reihe*. Allgemeiner gilt

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

für $a \in K \setminus \{0\}$ und

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

für $\alpha \in K[[X]] \setminus \{1\}$ und $n \in \mathbb{N}$.

- (ii) Für verschiedene $a, b \in K \setminus \{0\}$, sind $X+a$ und $X+b$ invertierbar und es gilt die *Partialbruchzerlegung*

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

(rechte Seite auf Hauptnenner bringen).

Definition 4.11. Für $\alpha = \sum a_n X^n \in K[[X]]$ sei

$$|\alpha| := 2^{-\inf\{k \in \mathbb{N}_0 : a_k \neq 0\}} \in \mathbb{R}$$

die *Norm* von α , wobei $|0| = 2^{-\infty} = 0$.

Beispiel 4.12. Genau dann ist $\alpha \in K[[X]]$ invertierbar, wenn $|\alpha| = 1$.

Lemma 4.13. Für $\alpha, \beta \in K[[X]]$ gilt $|\alpha\beta| = |\alpha||\beta|$ und $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$ mit Gleichheit falls $|\alpha| \neq |\beta|$ (ultrametrische Ungleichung).

Beweis. O. B. d. A. sei $\alpha = \sum a_n X^n \neq 0 \neq \beta = \sum b_n X^n$. Sei $|\alpha| = 2^{-k}$, $|\beta| = 2^{-l}$ und o. B. d. A. $k \geq l$. Dann gilt

$$\alpha\beta = a_k b_l X^{k+l} + \sum_{n=k+l+1}^{\infty} c_n X^n$$

für geeignete $c_n \in K$. Wegen $a_k b_l \neq 0$ folgt $|\alpha\beta| = 2^{-k-l} = |\alpha||\beta|$.

Aus $a_n + b_n \neq 0$ folgt $a_n \neq 0$ oder $b_n \neq 0$. Wegen $k \geq l$ ist dann $n \geq l$ und $|\alpha + \beta| \leq 2^{-l} = \max\{|\alpha|, |\beta|\}$. Für $k > l$ ist $a_l + b_l = b_l \neq 0$ und $|\alpha + \beta| = 2^{-l}$. \square

Satz 4.14. Durch $d(\alpha, \beta) := |\alpha - \beta|$ wird $K[[X]]$ zu einem vollständigen metrischen Raum.

Beweis. Offenbar gilt $d(\alpha, \beta) = d(\beta, \alpha) \geq 0$ mit Gleichheit genau dann, wenn $\alpha = \beta$. Daher ist d symmetrisch und positiv definit. Die Dreiecksungleichung folgt aus der ultrametrischen Ungleichung

$$d(\alpha, \gamma) = |\alpha - \gamma| = |\alpha - \beta + \beta - \gamma| \leq \max\{|\alpha - \beta|, |\beta - \gamma|\} \leq |\alpha - \beta| + |\beta - \gamma| = d(\alpha, \beta) + d(\beta, \gamma).$$

Sei $\alpha_1, \alpha_2, \dots \in K[[X]]$ eine Cauchyfolge mit $\alpha_m = \sum a_{m,n} X^n$ für $m \in \mathbb{N}$. Für jedes $k \in \mathbb{N}$ existiert $M = M(k) \geq 1$ mit $|\alpha_m - \alpha_M| < 2^{-k}$ für alle $m \geq M$. Dies zeigt $a_{m,n} = a_{M,n}$ für alle $m \geq M$ und $n \leq k$. Wir definieren

$$a_k := a_{M(k),k}$$

und $\alpha = \sum a_n X^n$. Dann gilt $|\alpha - \alpha_{M(k)}| < 2^{-k} \rightarrow 0$, d. h. $\lim_{m \rightarrow \infty} \alpha_m = \alpha$. Also ist $K[[X]]$ vollständig bzgl. d . \square

Lemma 4.15. Ist $\alpha_1, \alpha_2, \dots \in K[[X]]$ eine Nullfolge, so konvergieren $\sum_{k=1}^{\infty} \alpha_k$ und $\prod_{k=1}^{\infty} (1 + \alpha_k)$.

Beweis. Nach Satz 4.14 genügt es zu zeigen, dass die Partialsummen Cauchyfolgen sind. Für $\epsilon > 0$ sei $N \geq 0$ mit $|\alpha_k| < \epsilon$ für alle $k \geq N$. Für $k > l \geq N$ gilt

$$\begin{aligned} \left| \sum_{i=1}^k \alpha_i - \sum_{i=1}^l \alpha_i \right| &= \left| \sum_{i=l+1}^k \alpha_i \right| \stackrel{4.13}{\leq} \max\{|\alpha_i| : i = l+1, \dots, k\} < \epsilon, \\ \left| \prod_{i=1}^k (1 + \alpha_i) - \prod_{i=1}^l (1 + \alpha_i) \right| &= \prod_{i=1}^l \underbrace{|1 + \alpha_i|}_{\leq 1} \left| \prod_{i=l+1}^k (1 + \alpha_i) - 1 \right| = \left| \sum_{\emptyset \neq I \subseteq \{l+1, \dots, k\}} \prod_{i \in I} \alpha_i \right| \\ &\leq \max\{|\alpha_i| : i = l+1, \dots, k\} < \epsilon. \end{aligned} \quad \square$$

Bemerkung 4.16.

- (i) Sei $\alpha_1, \dots \in K[[X]]$ eine Nullfolge und $\alpha_k = \sum a_{k,n} X^n$. Für jedes n sind dann nur endlich viele der Koeffizienten $a_{1,n}, a_{2,n}, \dots$ von 0 verschieden. Dies zeigt

$$\sum \alpha_k = \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} a_{k,n} \right) X^n,$$

d. h. für die Berechnung des Koeffizienten von X^n braucht man nur endlich viele Terme auszuwerten. Das Gleiche gilt für $\prod_{k=1}^{\infty} (1 + \alpha_k)$. Zum Beispiel ist

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

- (ii) Für $\gamma \in K[[X]]$ und Nullfolgen $\alpha_1, \dots, \beta_1, \dots$ gilt wie üblich $\sum \alpha_k + \sum \beta_k = \sum (\alpha_k + \beta_k)$ und $\gamma \sum \alpha_k = \sum \gamma \alpha_k$.

- (iii) Es gilt

$$\left(\sum a_n X^n \right) \left(\sum b_n X^n \right) = \sum_{k,l \geq 0} a_k b_l X^{k+l},$$

denn die rechte Seite konvergiert egal in welcher Reihenfolge über die Paare (k, l) summiert wird.

Beispiel 4.17. Für $\alpha \in XK[[X]]$ ist $|\alpha^n| = |\alpha|^n \leq 2^{-n} \rightarrow 0$ und $\sum \alpha^n = \frac{1}{1-\alpha}$. Wir haben in der geometrischen Reihe also X durch α ersetzt.

Definition 4.18. Für $\alpha = \sum a_n X^n \in K[[X]]$ und $\beta \in XK[[X]]$ definiert man

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

Bemerkung 4.19. Für beliebige $\alpha, \beta \in K[[X]]$ wäre der 0-te Koeffizient $\sum_{k=0}^{\infty} a_0 b_0^k$ von $\alpha(\beta)$ im Allgemeinen nicht wohldefiniert.

Beispiel 4.20. Für $\alpha = \sum a_n X^n \in K[[X]]$ gilt $\alpha(X^2) = \sum a_n X^{2n}$ und $\alpha(0) = a_0$.

Lemma 4.21. Für $\alpha, \beta, \gamma \in K[[X]]$ und jede Nullfolge $\alpha_1, \dots \in K[[X]]$ gilt (falls wohldefiniert):

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

$$\left(\sum \alpha_k \right) \circ \beta = \sum (\alpha_k \circ \beta), \tag{4.2}$$

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

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

Beweis. Gleichung 4.1 ist trivial. Mit den Bezeichnungen aus Bemerkung 4.16 gilt

$$\left(\sum \alpha_k \right) \circ \beta = \sum_{n=0}^{\infty} \left(\sum_{k=1}^{\infty} a_{k,n} \right) \beta^n = \sum_{k=1}^{\infty} \left(\sum_{n=0}^{\infty} a_{k,n} \beta^n \right) = \sum (\alpha_k \circ \beta).$$

Gleichung 4.3 erhält man durch

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

In (4.4) dürfen wir $\alpha = X^n$ nach (4.2) annehmen. Mit (4.3) folgt

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

Bemerkung 4.22. Im Allgemeinen ist $\alpha \circ \beta \neq \beta \circ \alpha$, $\alpha \circ (\beta \gamma) \neq (\alpha \circ \beta) (\alpha \circ \gamma)$ und $\alpha \circ (\beta + \gamma) \neq \alpha \circ \beta + \alpha \circ \gamma$ (Aufgabe 23). Die letzte Gleichung lässt sich für die Exponentialfunktion korrigieren.

Lemma 4.23 (Funktionalgleichung). *Für jede Nullfolge $\alpha_1, \alpha_2, \dots \in X\mathbb{Q}[[X]]$ gilt*

$$\boxed{\exp\left(\sum \alpha_k\right) = \prod \exp(\alpha_k).} \quad (4.5)$$

Insbesondere ist $\exp(kX) = \exp(X)^k$ für $k \in \mathbb{Z}$.

Beweis. Wegen $\sum \alpha_k \in X\mathbb{Q}[[X]]$ und $\exp(\alpha_k) \in 1 + \alpha_k + \frac{\alpha_k^2}{2} + \dots$ sind beide Seiten von (4.5) wohldefiniert (Lemma 4.15). Für zwei Summanden $\alpha, \beta \in X\mathbb{Q}[[X]]$ gilt

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

Induktiv erhält man (4.5) für endlich viele Summanden. Schließlich ist

$$\left| \prod \exp(\alpha_k) - \exp\left(\sum_{k=1}^n \alpha_k\right) \right| = \prod_{k=1}^n |\exp(\alpha_k)| \left| \prod_{k=n+1}^{\infty} \exp(\alpha_k) - 1 \right| \rightarrow 0.$$

Für $k \in \mathbb{N}_0$ ist $\exp(kX) = \exp(X + \dots + X) = \exp(X)^k$. Wegen $\exp(kX) \exp(-kX) = \exp(kX - kX) = \exp(0) = 1$ gilt $\exp(-kX) = \exp(kX)^{-1} = \exp(X)^{-k}$. Daher gilt die letzte Behauptung für alle $k \in \mathbb{Z}$. \square

Satz 4.24. *Für jedes $\alpha = \sum a_n X^n \in K[[X]]$ mit $a_0 = 0$ und $a_1 \neq 0$ existiert genau ein $\beta \in K[[X]]$ mit $\beta(\alpha) = \alpha(\beta) = X$. Daher ist $K[[X]]^\circ := XK[[X]] \setminus X^2K[[X]]$ eine Gruppe bzgl. \circ mit neutralem Element X .*

Beweis. Sei $\alpha^k = \sum_{n=0}^{\infty} a_{kn} X^n$ für $k \in \mathbb{N}_0$. Wegen $a_0 = 0$ ist $a_{kn} = 0$ für $n < k$ und $a_{nn} = a_1^n \neq 0$. Wir definieren induktiv $b_0 := 0$, $b_1 := \frac{1}{a_1} \neq 0$ und

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

für $n \geq 2$. Für $\beta := \sum b_n X^n \in K[[X]]^\circ$ gilt dann

$$\beta(\alpha) = \sum_{k=0}^{\infty} b_k \alpha^k = \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} b_k a_{kn} X^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n b_k a_{kn} \right) X^n = X.$$

Vertauscht man die Rollen von α und β , so erhält man $\gamma \in K[[X]]^\circ$ mit $\gamma(\beta) = X$. Nach Lemma 4.21 gilt

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

Also ist β das Inverse von α bzgl. \circ . Insbesondere ist β eindeutig bestimmt und $K[[X]]^\circ$ ist eine Gruppe. \square

Bemerkung 4.25. In der Situation von Satz 4.24 nennt man β die *Umkehrfunktion* von α . Beachte: $\beta \neq \alpha^{-1}$ (wir werden keine Bezeichnung für die Umkehrfunktion einführen).

Beispiel 4.26. Sei α die Umkehrfunktion von $X + X^2 + \dots = \frac{X}{1-X}$. Dann gilt

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

und es folgt $\alpha = \frac{X}{1+X} = X - X^2 + X^3 - \dots$

Definition 4.27. Für $\alpha = \sum a_n X^n \in K[[X]]$ nennt man

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

die (formale) *Ableitung* von α . Sei außerdem $\alpha^{(0)} := \alpha$ und $\alpha^{(n)} := (\alpha^{(n-1)})'$ die *n-te Ableitung* für $n \in \mathbb{N}$.

Beispiel 4.28. Es gilt $1' = 0$, $X' = 1$ sowie

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

Bemerkung 4.29. Mit Ableitungen lassen sich die Koeffizienten von $\alpha = \sum a_n X^n \in \mathbb{C}[[X]]$ berechnen: $\alpha^{(0)}(0) = \alpha(0) = a_0$, $\alpha'(0) = a_1$, $\alpha''(0) = 2a_2$, \dots , $\alpha^{(n)}(0) = n!a_n$. Daher gilt

$$\boxed{\alpha = \sum_{n=0}^{\infty} \frac{\alpha^{(n)}(0)}{n!} X^n} \quad (\text{Taylorreihe}).$$

Über beliebigen Körpern K kann man nicht immer durch $n!$ teilen. Als Ersatz kann man die *k-te Hasse-Ableitung*

$$H^k(\alpha) := \sum_{n=k}^{\infty} \binom{n}{k} a_n X^{n-k}$$

für $\alpha = \sum a_n X^n \in K[[X]]$ definieren. Es gilt nun analog $\alpha = \sum_{n=0}^{\infty} H^n(\alpha)(0) X^n$.

Lemma 4.30. Für $\alpha, \beta \in K[[X]]$ und jede Nullfolge $\alpha_1, \alpha_2, \dots \in K[[X]]$ gilt

$$\begin{aligned} \left(\sum \alpha_k\right)' &= \sum \alpha'_k && \text{(Summenregel),} \\ (\alpha\beta)' &= \alpha'\beta + \alpha\beta' && \text{(Produktregel),} \\ \left(\prod(1 + \alpha_k)\right)' &= \prod(1 + \alpha_k) \sum \frac{\alpha'_k}{1 + \alpha_k}, \\ \left(\frac{\alpha}{\beta}\right)' &= \frac{\alpha'\beta - \alpha\beta'}{\beta^2} && \text{(Quotientenregel),} \\ (\alpha \circ \beta)' &= \alpha'(\beta)\beta' && \text{(Kettenregel).} \end{aligned}$$

Beweis.

(i) Mit den Bezeichnungen aus Bemerkung 4.16 gilt

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

(ii) Nach (i) darf man $\alpha = X^k$ und $\beta = X^l$ annehmen. Dann ist

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

(iii) O.B.d.A. sei $\alpha_k \neq -1$ für alle $k \in \mathbb{N}$ (anderenfalls sind beide Seiten 0). Aus (ii) erhält man induktiv

$$\left(\prod_{k=1}^n (1 + \alpha_k)\right)' = \prod_{k=1}^n (1 + \alpha_k) \sum_{k=1}^n \frac{\alpha'_k}{1 + \alpha_k}$$

für alle $n \in \mathbb{N}$. Die Behauptung folgt mit $n \rightarrow \infty$.

(iv) Aus (ii) folgt

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

(v) Nach (iii) gilt $(\alpha^n)' = n\alpha^{n-1}\alpha'$ für $n \in \mathbb{N}_0$. Aus der Summenregel folgt

$$(\alpha \circ \beta)' = \left(\sum a_n \beta^n\right)' = \sum a_n (\beta^n)' = \sum_{n=1}^{\infty} n a_n \beta^{n-1} \beta' = \alpha'(\beta)\beta'. \quad \square$$

Bemerkung 4.31. Die Produktregel impliziert auch die *Faktorregel* $(\lambda\alpha)' = \lambda\alpha'$ für $\lambda \in K$ und $\alpha \in K[[X]]$.

Beispiel 4.32. Wir definieren den (formalen) *Logarithmus* durch die *Mercator-Reihe*

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

Nach Satz 4.24 besitzt $\alpha := \exp(X) - 1$ eine Umkehrfunktion und $\log(\exp(X)) = \log(1 + \alpha) \in \mathbb{Q}[[X]]^\circ$. Wegen

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

folgt

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

aus der Kettenregel. Dies zeigt $\log(\exp(X)) = X$. Also ist $\log(1+X)$ die Umkehrfunktion von $\alpha = \exp(X) - 1$ wie in der Analysis. Außerdem gilt $\log(1-X) = -\sum_{n=1}^{\infty} \frac{X^n}{n}$.

Lemma 4.33 (Funktionalgleichung). *Für jede Nullfolge $\alpha_1, \alpha_2, \dots \in X\mathbb{Q}[[X]]$ gilt*

$$\log\left(\prod (1 + \alpha_k)\right) = \sum \log(1 + \alpha_k).$$

Beweis.

$$\begin{aligned} \log\left(\prod (1 + \alpha_k)\right) &= \log\left(\prod \exp(\log(1 + \alpha_k))\right) \stackrel{4.23}{=} \log(\exp(\sum \log(1 + \alpha_k))) \\ &= \sum \log(1 + \alpha_k). \end{aligned}$$

□

Beispiel 4.34. Nach Lemma 4.33 gilt

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

Definition 4.35. Für $c \in \mathbb{C}$ und $\alpha \in X\mathbb{C}[[X]]$ definieren wir

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

Im Fall $c = 1/k$ mit $k \in \mathbb{N}$ schreiben wir $\sqrt[k]{1 + \alpha} := (1 + \alpha)^{1/k}$ und speziell $\sqrt{1 + \alpha} := \sqrt[2]{1 + \alpha}$.

Bemerkung 4.36.

(i) Nach der Funktionalgleichung gilt

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

für $c, d \in \mathbb{C}$ wie gewohnt. Für $k \in \mathbb{N}$ ist demnach $\sqrt[k]{1 + \alpha^k} = 1 + \alpha$, d. h. $\sqrt[k]{1 + \alpha}$ ist eine k -te Wurzel von $1 + \alpha$ mit Absolutglied 1. Sei auch $\beta \in \mathbb{C}[[X]]$ mit $\beta^k = 1 + \alpha$. Dann hat $\sqrt[k]{1 + \alpha} \beta^{-1}$ Ordnung $\leq k$ in $\mathbb{C}[[X]]^\times$. Aus Lemma 4.8 folgt, dass $\sqrt[k]{1 + \alpha} \beta^{-1}$ konstant ist, d. h. $\beta = \beta(0) \sqrt[k]{1 + \alpha}$. Daher ist $\sqrt[k]{1 + \alpha}$ die einzige k -te Wurzel von $1 + \alpha$ mit Absolutglied 1.

(ii) Der folgende Satz verallgemeinert sowohl den Binomialsatz ($c \in \mathbb{N}$) als auch die geometrische Reihe ($c = -1$).

Satz 4.37 (NEWTONScher Binomialsatz). *Für $\alpha \in X\mathbb{C}[[X]]$ und $c \in \mathbb{C}$ gilt*

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

Beweis. Es genügt die Behauptung für $\alpha = X$ zu beweisen. Nach der Kettenregel gilt

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

und induktiv folgt $((1+X)^c)^{(k)} = c(c-1)\dots(c-k+1)(1+X)^{c-k}$. Die Behauptung folgt nun aus der Taylorreihe. \square

Beispiel 4.38. Sei $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$ (vgl. Definition 6.29) und $\alpha := (1+X)^\zeta - 1 \in X\mathbb{C}[[X]]$. Dann gilt $\alpha \circ \alpha = (1+(1+X)^\zeta - 1)^\zeta - 1 = (1+X)^{\zeta^2} - 1$ und induktiv $\alpha \circ \dots \circ \alpha = (1+X)^{\zeta^n} - 1 = X$, d. h. die Ordnung von α in der Gruppe $\mathbb{C}[[X]]^\circ$ teilt n . Im Gegensatz zu Lemma 4.8 besitzt $\mathbb{C}[[X]]^\circ$ also „interessante“ Elemente endlicher Ordnung.

Definition 4.39. Für $n \in \mathbb{N}_0$ sei $X^{n!} := (1-X)(1-X^2)\dots(1-X^n)$. Für $0 \leq k \leq n$ nennt man

$$\left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle := \frac{X^{n!}}{X^k! X^{n-k}!} = \frac{1-X^n}{1-X^k} \cdots \frac{1-X^{n-k+1}}{1-X} \in K[[X]]$$

Gaußschen Binomialkoeffizienten. Für $k < 0$ oder $k > n$ sei $\left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle := 0$.

Bemerkung 4.40. Wie immer ist $\left\langle \begin{matrix} n \\ 0 \end{matrix} \right\rangle = \left\langle \begin{matrix} n \\ n \end{matrix} \right\rangle = 1$ und $\left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle = \left\langle \begin{matrix} n \\ n-k \end{matrix} \right\rangle$ für alle $n \in \mathbb{N}_0$ und $k \in \mathbb{Z}$. Außerdem gilt $\left\langle \begin{matrix} n \\ 1 \end{matrix} \right\rangle = \frac{1-X^n}{1-X} = 1 + X + \dots + X^{n-1}$ und

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

Lemma 4.41. Für $n \in \mathbb{N}_0$ und $k \in \mathbb{Z}$ gilt

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

Beweis. Für $k > n+1$ oder $k < 0$ sind alle Terme 0. Für $k = n+1$ oder $k = 0$ sind beide Seiten 1. Für $1 \leq k \leq n$ gilt

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

Bemerkung 4.42. Man vergleiche die Rekursionsformeln²

$$\begin{aligned} \binom{n+1}{k} &\stackrel{1.6}{=} \binom{n}{k-1} + \binom{n}{k}, \\ \left(\binom{n+1}{k}\right) &\stackrel{1.24}{=} \left(\binom{n+1}{k-1}\right) + \left(\binom{n}{k}\right), \\ \left[\begin{matrix} n+1 \\ k \end{matrix} \right] &\stackrel{2.16}{=} \left[\begin{matrix} n \\ k-1 \end{matrix} \right] + n \left[\begin{matrix} n \\ k \end{matrix} \right], \\ \left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} &\stackrel{2.31}{=} \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\} + k \left\{ \begin{matrix} n \\ k \end{matrix} \right\}, \\ \left\langle \begin{matrix} n+1 \\ k \end{matrix} \right\rangle &\stackrel{4.41}{=} \left\langle \begin{matrix} n \\ k-1 \end{matrix} \right\rangle + X^k \left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle. \end{aligned}$$

Man kann also $\left(\binom{n}{k}\right)$, $\left[\begin{matrix} n \\ k \end{matrix} \right]$, $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ und $\left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle$ mit einem modifizierten pascalschen Dreieck berechnen.

Satz 4.43 (GAUSSScher Binomialsatz). Für $n \in \mathbb{N}$ und $\alpha \in K[[X]]$ gilt

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

Beweis. Induktion nach n : Für $n = 1$ sind beide Seiten $1 + \alpha$. Für den Induktionsschritt lassen wir alle Summen von $-\infty$ bis ∞ laufen (das macht Indexverschiebungen einfacher):

$$\begin{aligned} \prod_{k=0}^n (1 + \alpha X^k) &= (1 + \alpha X^n) \sum_{k=-\infty}^{\infty} \left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle \alpha^k X^{\binom{k}{2}} \\ &= \sum \left\langle \begin{matrix} n \\ n-k \end{matrix} \right\rangle \alpha^k X^{\binom{k}{2}} + \sum \left\langle \begin{matrix} n \\ n-k \end{matrix} \right\rangle \alpha^{k+1} X^{n-k} X^{\binom{k+1}{2}} \\ &= \sum \left\langle \begin{matrix} n \\ n-k \end{matrix} \right\rangle \alpha^k X^{\binom{k}{2}} + \sum X^{n-k+1} \left\langle \begin{matrix} n \\ n-k+1 \end{matrix} \right\rangle \alpha^k X^{\binom{k}{2}} \\ &\stackrel{4.41}{=} \sum \left\langle \begin{matrix} n+1 \\ n-k+1 \end{matrix} \right\rangle \alpha^k X^{\binom{k}{2}} = \sum \left\langle \begin{matrix} n+1 \\ k \end{matrix} \right\rangle \alpha^k X^{\binom{k}{2}}. \quad \square \end{aligned}$$

Bemerkung 4.44. Es gibt auch eine Vandermonde-Identität für $\left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle$.

5. Erzeugende Funktionen

Definition 5.1. In diesem Kapitel sei stets $\mathbb{Q} \subseteq K$. Für eine Zahlenfolge $a_0, a_1, \dots \in \mathbb{C}$ nennt man $\sum_{n=0}^{\infty} a_n X^n \in \mathbb{C}[[X]]$ die *erzeugende Funktion* von a_0, a_1, \dots

Beispiel 5.2.

- (i) Die erzeugende Funktion der konstanten Folge $1, 1, \dots$ ist $(1 - X)^{-1}$.

²Alle Formeln lassen sich vereinheitlichen: [J. Konvalina, *A unified interpretation of the binomial coefficients, the Stirling numbers, and the Gaussian coefficients*, Amer. Math. Monthly 107, (2000), 901–910]

- (ii) Ist $\alpha \in \mathbb{C}[[X]]$ die erzeugende Funktion von a_0, a_1, \dots , so ist $\alpha(-X)$ die erzeugende Funktion von $a_0, -a_1, a_2, \dots$.
- (iii) Ist α die erzeugende Funktion von a_0, a_1, \dots , so ist α' die erzeugende Funktion von $0, a_1, 2a_2, 3a_3, \dots$. Zum Beispiel ist $\left(\frac{1}{1-X}\right)' = \frac{1}{(1-X)^2}$ (Quotientenregel) die erzeugende Funktion von $0, 1, 2, 3, \dots$.
- (iv) Jede k -elementige Multimenge $A \subseteq \{1, \dots, n\}$ entspricht genau einer Zerlegung $k = k_1 + \dots + k_n$, wobei $k_i \in \mathbb{N}_0$ die Vielfachheit von i in A angibt. Dies zeigt

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

für $n \in \mathbb{N}$ (vgl. Satz 4.37).

- (v) Wir betrachten die rekursiv definierte *Fibonacci-Folge* $f_0 := 0, f_1 := 1$ und $f_{n+1} := f_{n-1} + f_n$ für $n \in \mathbb{N}$ (also $0, 1, 1, 2, 3, 5, 8, \dots$). Für $\alpha := \sum f_n X^n \in \mathbb{R}[[X]]$ gilt dann

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

Also ist

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

Satz 5.3 (BINET-Formel). Für $n \in \mathbb{N}_0$ gilt

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

Beweis. Sei α wie in Beispiel 5.2. Ist $\varphi := \frac{1+\sqrt{5}}{2} \in \mathbb{R}$ der *goldene Schnitt* und $\psi := \frac{1-\sqrt{5}}{2} \in \mathbb{R}$, so gilt $(X + \varphi)(X + \psi) = X^2 + X - 1$. Partialbruchzerlegung (Beispiel 4.10) ergibt

$$\alpha = \frac{-X}{(X + \varphi)(X + \psi)} = \frac{X}{\varphi - \psi} \left(\frac{1}{X + \varphi} - \frac{1}{X + \psi} \right) = \frac{X}{\sqrt{5}} \left(\frac{1}{X + \varphi} - \frac{1}{X + \psi} \right).$$

Nun ist $\varphi^{-1} = \frac{2}{1+\sqrt{5}} = -\psi$ und

$$\frac{X}{X + \varphi} \stackrel{4.10}{=} - \sum_{n=1}^{\infty} (-\varphi)^{-n-1} X^{n+1} = - \sum_{n=1}^{\infty} \psi^n X^n.$$

Es folgt

$$\alpha = \frac{1}{\sqrt{5}} \left(\sum_{n=1}^{\infty} \varphi^n X^n - \sum_{n=1}^{\infty} \psi^n X^n \right) = \sum_{n=0}^{\infty} \frac{1}{\sqrt{5}} (\varphi^n - \psi^n) X^n.$$

Koeffizientenvergleich liefert die Behauptung. □

Bemerkung 5.4.

- (i) Da der zweite Summand in Satz 5.3 kleiner als $\frac{1}{2}$ ist, erhält man durch Runden die einfachere Formel

$$f_n = \left\lfloor \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n \right\rfloor.$$

- (ii) Man kann f_n auch kombinatorisch interpretieren: Sei g_n die Anzahl der $\{1, 2\}$ -Folgen, deren Summe n ergibt. Sicher ist $g_0 = 0$ und $g_1 = 1$. Ist $(a_1, \dots, a_k) \in \{1, 2\}^k$ mit $\sum a_i = n + 1$, so ist (a_1, \dots, a_{k-1}) eine Folge mit Summe n oder $n - 1$, je nachdem, ob $a_k = 1$ oder $a_k = 2$ gilt. Dies zeigt $g_{n+1} = g_n + g_{n-1}$ und es folgt $g_n = f_n$ für alle $n \in \mathbb{N}_0$.

Satz 5.5. *Es gilt*

$$(i) \quad \sum_{n=0}^{\infty} p(n)X^n = \prod_{k=1}^{\infty} \frac{1}{1 - X^k} \quad (\text{EULER}),$$

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

Beweis.

- (i) Wegen $(1 - X^k)^{-1} = \sum_{n=0}^{\infty} (X^k)^n \in 1 + X^k K[[X]]$ ist das unendliche Produkt wohldefiniert (Lemma 4.15). Die Partition $(1^{a_1}, \dots, n^{a_n})$ von $n \in \mathbb{N}_0$ erfüllt $a_1 + 2a_2 + \dots + na_n = n$. Daher ist $p(n)$ die Anzahl aller Lösungen $(a_1, \dots, a_n) \in \mathbb{N}_0^n$ mit $a_1 + 2a_2 + \dots + na_n = n$. Dies ist genau der n -te Koeffizient von

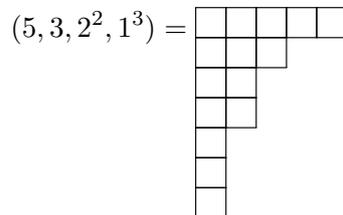
$$(1 + X + X^2 + X^3 + \dots)(1 + X^2 + X^{2 \cdot 2} + X^{2 \cdot 3} + \dots)(1 + X^3 + X^{3 \cdot 2} + X^{3 \cdot 3} + \dots) \dots = \prod_{k=1}^{\infty} \frac{1}{1 - X^k}.$$

- (ii) Sei $\alpha := \exp(\exp(X) - 1) = \sum \frac{a_n}{n!} X^n$. Dann ist $a_0 = \exp(\exp(0) - 1) = \exp(0) = 1 = b(0)$. Die Kettenregel liefert

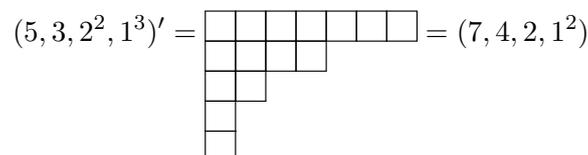
$$\begin{aligned} \sum_{n=0}^{\infty} \frac{a_{n+1}}{n!} X^n &= \alpha' = \exp(X) \exp(\exp(X) - 1) \\ &= \left(\sum_{k=0}^{\infty} \frac{1}{k!} X^k \right) \left(\sum_{k=0}^{\infty} \frac{a_k}{k!} X^k \right) = \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{a_k}{k!(n-k)!} X^n. \end{aligned}$$

Daher ist $a_{n+1} = \sum_{k=0}^n \binom{n}{k} a_k$ für $n \geq 0$ und die Behauptung folgt aus Satz 2.40. \square

Bemerkung 5.6. Man kann Partitionen $\lambda = (\lambda_1, \dots, \lambda_k)$ (mit $\lambda_1 \geq \dots \geq \lambda_k$) von $n \in \mathbb{N}$ durch *Young-Diagramme* (auch *Ferrers-Diagramme* genannt) visualisieren. Zum Beispiel:



Durch Spiegelung an der Diagonalen erhält man das Young-Diagramm der *konjugierten* Partition $\lambda' = (\lambda'_1, \dots, \lambda'_l)$ von n . Zum Beispiel:



Im Allgemeinen gilt $\lambda'_i = |\{j : \lambda_j \geq i\}|$ für $i = 1, \dots, l$. Außerdem ist $\lambda'' = \lambda$. Man nennt λ *symmetrisch*, falls $\lambda' = \lambda$.

Satz 5.7. Seien $n, k \in \mathbb{N}_0$.

- (i) (EULER) Die Anzahl der Partitionen von n in ungleiche Teile ist gleich der Anzahl der Partitionen in ungerade Teile.
- (ii) Die Anzahl der Partitionen von n in k Teile ist gleich der Anzahl der Partitionen mit größtem Teil k .
- (iii) (SYLVESTER) Die Anzahl der symmetrischen Partitionen von n ist gleich der Anzahl der Partitionen in ungleiche, ungerade Teile.

Beweis.

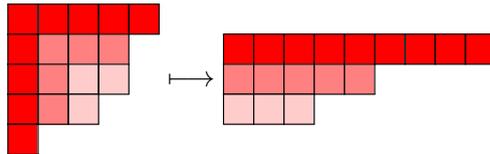
(i) Ist $u(n)$ die Anzahl der Partitionen in ungleiche Teile, so gilt

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

Auf der rechten Seite steht die erzeugende Funktion von der Anzahl der Partitionen in ungerade Teile.

- (ii) Die Abbildung $\lambda \mapsto \lambda'$ liefert eine Bijektion zwischen den angegebenen Mengen.
- (iii) Die folgende Abbildung liefert die gewünschte Bijektion:

$$\begin{aligned} \{\text{symmetrische Partitionen von } n\} &\longrightarrow \{\text{Partitionen in ungleiche, ungerade Teile}\}, \\ (\lambda_1, \dots, \lambda_k) &\longmapsto (2\lambda_1 - 1, 2\lambda_2 - 3, 2\lambda_3 - 5, \dots) \end{aligned}$$



□

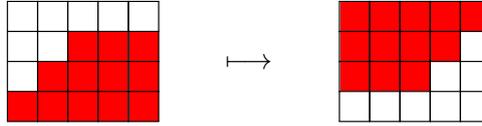
Beispiel 5.8. Für $n = 8$ erhält man

Partitionen in ungleiche Teile:	(8), (7, 1), (6, 2), (5, 3), (5, 2, 1), (4, 3, 1)
Partitionen in ungerade Teile:	(7, 1), (5, 3), (5, 1 ³), (3 ² , 1 ²), (3, 1 ⁵), (1 ⁸)
Partitionen in ungleiche, ungerade Teile:	(7, 1), (5, 3)
Symmetrische Partitionen:	(3 ² , 2), (4, 2, 1 ²)
Partitionen in 4 Teile:	(5, 1 ³), (4, 2, 1 ²), (3 ² , 1 ²), (3, 2 ² , 1), (2 ⁴)
Partitionen mit größtem Teil 4:	(4 ²), (4, 3, 1), (4, 2 ²), (4, 2, 1 ²), (4, 1 ⁴)

Bemerkung 5.9. Sei $p_k(n)$ die Anzahl der Partitionen von n in Teile $\leq k$ (nach Satz 5.7 ist dies auch die Anzahl der Partition in höchstens k Teile). Der Beweis von Satz 5.5 zeigt

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

Wir studieren nun die Anzahl $p_{k,l}(n) = p_{l,k}(n)$ der Partitionen von n mit höchstens k Teilen und jeden Teil $\leq l$. Dies sind genau die Partitionen, deren Young-Diagramm in ein Rechteck der Größe $k \times l$ passt. Der verbleibende Teil des Rechtecks um 180° gedreht ergibt eine Partition von $kl - n$ vom gleichen Format:



Dies zeigt $p_{k,l}(n) = p_{k,l}(kl - n)$.

Satz 5.10. Für $k, l \geq 0$ gilt

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

Beweis. Induktion nach $k + l$. Für $k = 0$ oder $l = 0$ sind beide Seite gleich 1. Sei also $k, l \geq 1$. Sei $\lambda = (\lambda_1, \lambda_2, \dots) \in P(n)$ mit höchstens k Teilen und jeden Teil $\leq l$. Ist $\lambda_1 = l$, so ist $(\lambda_2, \lambda_3, \dots) \in P(n - l)$ mit höchstens $k - 1$ Teilen. Anderenfalls ist jeder Teil von λ höchstens $l - 1$. Dies zeigt $p_{k,l}(n) = p_{k,l-1}(n) + p_{k-1,l}(n - l)$. Für $P(k, l) := \sum p_{k,l}(n) X^n$ gilt daher

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

Die Behauptung folgt nun durch Induktion und Lemma 4.41. □

Bemerkung 5.11. Für $k, N \geq 0$ gilt

$$\sum_{n=0}^{\infty} (p_k(n) - p_{k,N-k}(n)) X^n = \sum_{n=N-k+1}^{\infty} (p_k(n) - p_{k,N-k}(n)) X^n \longrightarrow 0 \quad (N \rightarrow \infty)$$

und

$$\lim_{N \rightarrow \infty} \left\langle \begin{matrix} N \\ k \end{matrix} \right\rangle = \sum_{n=0}^{\infty} p_k(n) X^n = \frac{1}{X^{k!}}.$$

Für $k, l \in \mathbb{Z}$ gilt analog

$$\lim_{N \rightarrow \infty} \left\langle \begin{matrix} 2N+k \\ N+l \end{matrix} \right\rangle = \lim_{N \rightarrow \infty} \sum_{n=0}^{\infty} p_{N+l, N+k-l}(n) X^n = \sum_{n=0}^{\infty} p(n) X^n = \prod_{m=1}^{\infty} \frac{1}{1 - X^m}.$$

Beide Grenzwerte lassen sich auch aus der Definition von $\left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle$ herleiten.

Satz 5.12 (ERDŐS-TURÁN). Seien $n, d \in \mathbb{N}$. Die Anzahl der Permutationen von S_n , deren Zyklenlängen nicht durch d teilbar sind, ist

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

Beweis (PÓLYA). Die Anzahl der Permutationen vom Typ $(1^{l_1}, \dots, n^{l_n})$ ist

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

nach Satz 2.26. Die gesuchte Anzahl, geteilt durch $n!$, ist daher der Koeffizient von X^n in

$$\begin{aligned} \prod_{k=1}^{\infty} \sum_{l=0}^{\infty} \frac{1}{l!} \left(\frac{X^k}{k}\right)^l &= \prod_{d \nmid k} \exp(X^k/k) \stackrel{4.23}{=} \exp\left(\sum_{d \nmid k} \frac{X^k}{k}\right) = \exp\left(\sum_{k=1}^{\infty} \frac{X^k}{k} - \sum_{k=1}^{\infty} \frac{X^{dk}}{dk}\right) \\ &= \exp(-\log(1-X) + \frac{1}{d} \log(1-X^d)) \stackrel{4.33}{=} \sqrt[d]{1-X^d} \frac{1}{1-X} \\ &= \frac{1-X^d}{1-X} (1-X^d)^{\frac{1-d}{d}} \stackrel{4.37}{=} \left(\sum_{r=0}^{d-1} X^r\right) \left(\sum_{q=0}^{\infty} \binom{(1-d)/d}{q} (-X^d)^q\right). \end{aligned}$$

Darin tritt X^n genau dann auf, wenn $n = qd + r$ mit $0 \leq r < d$ und $q = \lfloor n/d \rfloor$ (Division mit Rest). Der Koeffizient ist dann

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

Beispiel 5.13. Eine Permutation hat genau dann ungerade Ordnung, wenn sie nur aus Zyklen ungerader Länge besteht. Die Anzahl der Permutation in S_n mit ungerader Ordnung ist daher

$$n! \prod_{k=1}^{\lfloor n/2 \rfloor} \frac{2k-1}{2k} = \begin{cases} 1^2 \cdot 3^2 \cdot \dots \cdot (n-1)^2 & \text{falls } n \text{ gerade,} \\ 1^2 \cdot 3^2 \cdot \dots \cdot (n-2)^2 \cdot n & \text{falls } n \text{ ungerade.} \end{cases}$$

Satz 5.14 (EULERS Pentagonalzählensatz).

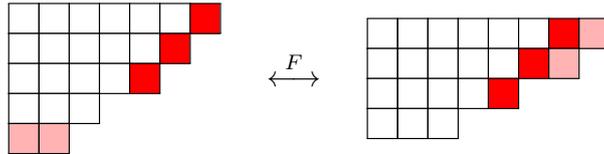
$$\begin{aligned} \prod_{k=1}^{\infty} (1 - X^k) &= 1 + \sum_{k=1}^{\infty} (-1)^k \left(X^{\frac{3k^2-k}{2}} + X^{\frac{3k^2+k}{2}} \right) = \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{3k^2+k}{2}} \\ &= 1 - X - X^2 + X^5 + X^7 - X^{12} - X^{15} + \dots \end{aligned}$$

Beweis (FRANKLIN). Sei $n \in \mathbb{N}$ und Λ_n die Menge der Partitionen von n in ungleiche Teile. Für $\lambda \in \Lambda_n$ sei $|\lambda|$ die Anzahl der Teile von λ . Der n -te Koeffizient von $(1-X)(1-X^2)\dots$ ist dann $\sum_{\lambda \in \Lambda_n} (-1)^{|\lambda|}$ (vgl. Beweis von Satz 5.7). Sei zunächst $n \neq (3k^2 \pm k)/2$ für alle $k \in \mathbb{N}$. Wir konstruieren eine Permutation F auf Λ_n mit $|F(\lambda)| = |\lambda| \pm 1$ für alle $\lambda \in \Lambda_n$. Dann folgt

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

wie gewünscht. Sei $\lambda = (\lambda_1, \dots, \lambda_l) \in \Lambda_n$ mit $\lambda_1 > \dots > \lambda_l$ und $s := \max\{1 \leq i \leq l : \lambda_i = \lambda_1 - i + 1\}$. Wir definieren

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



Dies funktioniert nur in zwei Fällen nicht: Im ersten Fall ist $\lambda = (2k-1, 2k-2, \dots, k)$ und

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

Im zweiten Fall ist $\lambda = (2k, 2k - 1, \dots, k + 1)$ und

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

Beides war ausgeschlossen. Also ist F wohldefiniert und $|F(\lambda)| = |\lambda| \pm 1$ für alle $\lambda \in \Lambda_n$. Wegen $F^2 = \text{id}$ ist F eine Permutation.

Ist nun $n = (3k^2 \pm k)/2$, so kann man F immer noch auf $\Lambda_n \setminus \{\mu\}$ definieren, wobei μ eine der beiden oben genannten Partitionen ist. Man erhält dann

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

wie gewünscht. □

Bemerkung 5.15. Aus den Sätzen 5.5 und 5.14 folgt

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

und

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

für $n \in \mathbb{N}$, wobei $p(k) := 0$ für $k < 0$. Man erhält eine Rekursionsformel:

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

Beispiel 5.16. Es gilt

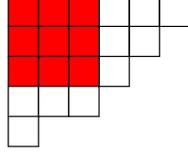
$$\begin{aligned} p(1) &= p(0) = 1, \\ p(2) &= p(1) + p(0) = 2, \\ p(3) &= p(2) + p(1) = 3, \\ p(4) &= p(3) + p(2) = 3 + 2 = 5, \\ p(5) &= p(4) + p(3) - p(0) = 5 + 3 - 1 = 7, \\ p(6) &= p(5) + p(4) - p(1) = 7 + 5 - 1 = 11 \end{aligned}$$

(vgl. <https://oeis.org/A000041>).

Satz 5.17 (DURFEES Quadrat-Satz). *Es gilt*

$$\sum_{n=0}^{\infty} p(n)X^n = \sum_{k=0}^{\infty} \frac{X^{k^2}}{(X^{k!})^2}.$$

Beweis. Sei $\lambda \in P(n)$ und $k \in \mathbb{N}$ maximal mit $\lambda_k \geq k$. Das bedeutet, dass das Young-Diagramm von λ ein Quadrat Q mit Seitenlänge k enthält, aber keines mit Seitenlänge $k + 1$. (Man nennt Q das *Durfee-Quadrat* von λ). Unterhalb von Q befindet sich eine Partition mit größtem Teil $\leq k$. Rechts neben Q befindet sich eine Partition mit höchstens k Teilen.



Die Anzahl beider Partitionen wird durch p_k gezählt. Daher gilt

$$\sum_{n=0}^{\infty} p(n)X^n = \sum_{k=0}^{\infty} X^{k^2} \left(\sum_{n=0}^{\infty} p_k(n)X^n \right)^2 \stackrel{5.9}{=} \sum_{k=0}^{\infty} \frac{X^{k^2}}{(X^{k!})^2}. \quad \square$$

Lemma 5.18 (HIRSCHHORN). Für $n \in \mathbb{N}_0$ gilt

$$\prod_{k=1}^n (1 - X^k)^2 = \sum_{k=0}^n (-1)^k (2k+1) X^{\frac{k^2+k}{2}} \left\langle \begin{matrix} 2n+1 \\ n-k \end{matrix} \right\rangle. \quad (5.1)$$

Beweis. Induktion nach n : Für $n = 0$ sind beide Seiten 1. Sei nun $n \geq 1$. Sei Q_n die rechte Seite von (5.1). Wiederholte Anwendung von Lemma 4.41 ergibt

$$\begin{aligned} Q_n &= X^n \sum_{k=0}^n (-1)^k (2k+1) X^{\frac{k^2-k}{2}} \left\langle \begin{matrix} 2n \\ n-k \end{matrix} \right\rangle + \sum_{k=0}^{n-1} (-1)^k (2k+1) X^{\frac{k^2+k}{2}} \left\langle \begin{matrix} 2n \\ n-k-1 \end{matrix} \right\rangle \\ &= X^n \sum_{k=0}^n (-1)^k (2k+1) X^{\frac{k^2-k}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k \end{matrix} \right\rangle + X^{2n} \sum_{k=0}^{n-1} (-1)^k (2k+1) X^{\frac{k^2+k}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k-1 \end{matrix} \right\rangle \\ &\quad + \sum_{k=0}^{n-1} (-1)^k (2k+1) X^{\frac{k^2+k}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k-1 \end{matrix} \right\rangle + X^n \sum_{k=0}^{n-2} (-1)^k (2k+1) X^{\frac{k^2+3k+2}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k-2 \end{matrix} \right\rangle \\ &= (1 + X^{2n})Q_{n-1} + X^n \left(\left\langle \begin{matrix} 2n-1 \\ n \end{matrix} \right\rangle - 3 \left\langle \begin{matrix} 2n-1 \\ n-1 \end{matrix} \right\rangle + \sum_{k=2}^n (-1)^k (2k+1) X^{\frac{k^2-k}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k \end{matrix} \right\rangle \right) \\ &\quad + \sum_{k=0}^{n-2} (-1)^k (2k+1) X^{\frac{k^2+3k+2}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k-2 \end{matrix} \right\rangle \\ &= (1 + X^{2n})Q_{n-1} + X^n \left(-2 \left\langle \begin{matrix} 2n-1 \\ n-1 \end{matrix} \right\rangle + \sum_{k=1}^{n-1} (-1)^{k+1} (2k+3) X^{\frac{k^2+k}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k-1 \end{matrix} \right\rangle \right) \\ &\quad + \sum_{k=1}^{n-1} (-1)^{k-1} (2k-1) X^{\frac{k^2+k}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k-1 \end{matrix} \right\rangle \\ &= (1 + X^{2n})Q_{n-1} - 2X^n \left(\left\langle \begin{matrix} 2n-1 \\ n-1 \end{matrix} \right\rangle + \sum_{k=1}^{n-1} (-1)^k (2k+1) X^{\frac{k^2+k}{2}} \left\langle \begin{matrix} 2n-1 \\ n-k-1 \end{matrix} \right\rangle \right) \\ &= (1 + X^{2n})Q_{n-1} - 2X^n Q_{n-1} = (1 - X^n)^2 Q_{n-1} = \prod_{k=1}^n (1 - X^k)^2. \quad \square \end{aligned}$$

Satz 5.19 (JACOBI). Es gilt

$$\prod_{k=1}^{\infty} (1 - X^k)^3 = \sum_{k=0}^{\infty} (-1)^k (2k+1) X^{\frac{k^2+k}{2}}.$$

Beweis. Der Koeffizient von X^n in $\prod_{k=1}^{\infty} (1 - X^k)^3$ hängt offensichtlich nur von den ersten n Faktoren ab. Nach Lemma 5.18 gilt

$$\begin{aligned} \prod_{k=1}^n (1 - X^k)^3 &= \prod_{k=1}^n (1 - X^k) \sum_{k=0}^n (-1)^k (2k+1) X^{\frac{k^2+k}{2}} \binom{2n+1}{n-k} \\ &= \sum_{k=0}^n (-1)^k (2k+1) X^{\frac{k^2+k}{2}} (1 - X^{n-k+1}) \dots (1 - X^n) (1 - X^{n+k+2}) \dots (1 - X^{2n+1}). \end{aligned}$$

Wegen $\frac{1}{2}(k^2 + k) + n - k + 1 = n + \frac{1}{2}(k^2 - k) + 1 > n$ für $k \geq 0$ existiert ein $\alpha \in K[[X]]$ mit

$$\prod_{k=1}^n (1 - X^k)^3 = \sum_{k=0}^n (-1)^k (2k+1) X^{\frac{k^2+k}{2}} + \alpha$$

und $|\alpha| < 2^n$. Insbesondere kommt X^n nicht in α vor. \square

Bemerkung 5.20.

- (i) Für $\alpha = \sum a_n X^n, \beta = \sum b_n X^n \in \mathbb{Z}[[X]]$ und $d \in \mathbb{N}$ schreiben wir $\alpha \equiv \beta \pmod{d}$, falls $a_k \equiv b_k \pmod{d}$ für alle $k \in \mathbb{N}_0$ gilt.
- (ii) Ist $\alpha \equiv \beta \pmod{d}$ und $\gamma \equiv \delta \pmod{d}$, so auch $\alpha + \gamma \equiv \beta + \delta \pmod{d}$ und $\alpha\gamma \equiv \beta\delta \pmod{d}$, denn $\sum_{k=0}^n a_k c_{n-k} \equiv \sum_{k=0}^n b_k d_{n-k} \pmod{d}$ für $n \in \mathbb{N}_0$.
- (iii) Ist $a_0 = b_0 = 1$, so folgt $\alpha^{-1}, \beta^{-1} \in \mathbb{Z}[[X]]$ aus dem Beweis von Lemma 4.8. Außerdem ist $\alpha \equiv \beta \pmod{d}$ äquivalent zu $\alpha^{-1} \equiv \beta^{-1} \pmod{d}$.
- (iv) Für jede Primzahl p gilt

$$(\alpha + \beta)^p = \sum_{k=0}^p \binom{p}{k} \alpha^k \beta^{p-k} \equiv \alpha^p + \beta^p \pmod{p},$$

da $\binom{p}{k}$ für $0 < k < p$ stets durch p teilbar ist.

Satz 5.21 (RAMANUJAN). Für $n \in \mathbb{N}_0$ ist $5 \mid p(5n+4)$ und $7 \mid p(7n+5)$.

Beweis. Sei $\alpha := \prod(1 - X^k)$. Nach Bemerkung 5.20 ist $\alpha^5 = \prod(1 - X^k)^5 \equiv \prod(1 - X^{5k}) \equiv \alpha(X^5) \pmod{5}$ und $\alpha^{-5} \equiv \alpha(X^5)^{-1} \pmod{5}$. Für $k \in \mathbb{Z}$ gilt

$$\frac{1}{2}(k^2 + k) \equiv \begin{cases} 0 & \text{falls } k \equiv 0, -1 \pmod{5}, \\ 1 & \text{falls } k \equiv 1, -2 \pmod{5}, \\ 3 & \text{falls } k \equiv 2 \pmod{5}. \end{cases}$$

Wir können Jacobis Identität also in der Form

$$\begin{aligned} \alpha^3 &= \sum_{k \equiv 0, -1 \pmod{5}} (-1)^k (2k+1) X^{\frac{k^2+k}{2}} + \sum_{k \equiv 1, -2 \pmod{5}} (-1)^k (2k+1) X^{\frac{k^2+k}{2}} + \sum_{k \equiv 2 \pmod{5}} (-1)^k (2k+1) X^{\frac{k^2+k}{2}} \\ &\equiv \alpha_0 + \alpha_1 \pmod{5} \end{aligned}$$

schreiben, wobei α_i aus den Termen $a_k X^k$ mit $k \equiv i \pmod{5}$ gebildet wird. Aus Satz 5.5 folgt nun

$$\sum_{n=0}^{\infty} p(n) X^n = \alpha^{-1} = \frac{(\alpha^3)^3}{(\alpha^5)^2} \equiv \frac{(\alpha_0 + \alpha_1)^3}{\alpha(X^5)^2} \pmod{5}. \quad (5.2)$$

In $(\alpha_0 + \alpha_1)^3$ kommen nur die X^k mit $k \equiv 0, 1, 2, 3 \pmod{5}$ vor, während in $\alpha(X^5)^{-2}$ nur X^{5k} vorkommen. Daher kommen die Potenzen der Form X^{5k+4} auf der rechten Seite von (5.2) überhaupt nicht vor. Es muss also $p(5k+4) \equiv 0 \pmod{5}$ gelten.

Für die zweite Aussage beobachten wir $\frac{1}{2}(k^2 + k) \equiv 0, 1, 3, 6 \pmod{7}$, wobei der letzte Fall nur für $k \equiv 3 \pmod{7}$ auftritt und dann ist $2k+1 \equiv 0 \pmod{7}$. Wie oben können wir daher $\alpha^3 \equiv \alpha_0 + \alpha_1 + \alpha_3 \pmod{7}$ schreiben. Dann ist

$$\sum_{n=0}^{\infty} p(n)X^n = \alpha^{-1} = \frac{(\alpha^3)^2}{\alpha^7} \equiv \frac{(\alpha_0 + \alpha_1 + \alpha_3)^2}{\alpha(X^7)} \pmod{7}.$$

Wieder tritt X^{7k+5} auf der rechten Seite nicht auf. □

Bemerkung 5.22. Ramanujan hat auch $11 \mid p(11n+6)$ für alle $n \in \mathbb{N}_0$ bewiesen, aber das ist aufwendiger zu zeigen. Die Relation $5 \mid p(5n+4)$ lässt sich präzisieren zu

$$\sum_{n=0}^{\infty} p(5n+4)X^n = 5 \prod_{k=1}^{\infty} \frac{(1-X^{5k})^5}{(1-X^k)^6},$$

Ramanujans „schönster“ Formel.³ Ono hat bewiesen, dass es für jede Primzahl $p \geq 5$ eine entsprechende Relation gibt. Diese sind jedoch wesentlich unübersichtlicher, wie

$$13 \mid p(11^3 \cdot 13n + 237).$$

Satz 5.23 (JACOBI'S Tripelprodukt). *Für jedes $\alpha \in K[[X]] \setminus X^2K[[X]]$ gilt*

$$\prod_{k=1}^{\infty} (1-X^{2k})(1+\alpha X^{2k-1})(1+\alpha^{-1}X^{2k-1}) = \sum_{k=-\infty}^{\infty} \alpha^k X^{k^2}.$$

Beweis (WRIGHT). Wegen $\alpha \notin X^2K[[X]]$ ist $\alpha^{-1}X$ nach Lemma 4.8 tatsächlich wohldefiniert. Daher ist auch $\alpha^{-1}X^{2k-1}$ für alle $k \in \mathbb{N}$ wohldefiniert. Ebenso ist $\alpha^k X^{k^2} = (\alpha^{-1}X)^{-k} X^{k^2+k}$ für $k < 0$ wohldefiniert. Wie üblich sind auch die unendlichen Produkte und Summen wohldefiniert. Mit $\beta := \alpha X$ und $\gamma := \alpha^{-1}X$ müssen wir

$$\prod_{k=1}^{\infty} (1 + \beta^k \gamma^{k-1})(1 + \beta^{k-1} \gamma^k) = \sum_{k=-\infty}^{\infty} \beta^{\frac{k^2+k}{2}} \gamma^{\frac{k^2-k}{2}} \prod_{n=1}^{\infty} \frac{1}{1 - (\beta\gamma)^n} \quad (5.3)$$

zeigen. Nach Satz 5.5 ist

$$\prod_{l=1}^{\infty} \frac{1}{1 - (\beta\gamma)^l} = \sum_{n=0}^{\infty} p(n)(\beta\gamma)^n.$$

Andererseits ist

$$\prod_{k=1}^{\infty} (1 + \beta^k \gamma^{k-1})(1 + \beta^{k-1} \gamma^k) = \sum_{n,m=0}^{\infty} t(n,m) \beta^n \gamma^m,$$

wobei $t(n, m)$ die Anzahl der Partitionen des Paares $(n, m) \in \mathbb{N}_0^2$ in paarweise verschiedene Teile der Form $(a, a-1)$ und $(b-1, b)$ mit $a, b \in \mathbb{N}$ ist (Beispiel: $(3, 4) = (1, 0) + (0, 1) + (2, 3) = (2, 1) + (0, 1) + (1, 2)$, also $t(3, 4) = 3$). Der Term $\beta^n \gamma^m$ taucht auf der rechten Seite von (5.3) nur für den $(n-m)$ -ten

³siehe [M. Hirschhorn, *The power of q*, Kapitel 5]

Summanden auf. Der entsprechende Koeffizient ist dann $p(n - (n - m)(n - m + 1)/2)$, wobei wir $p(k) = 0$ für $k < 0$ annehmen. Es genügt also

$$t(n, m) = p(n - (n - m)(n - m + 1)/2) \tag{5.4}$$

für alle $n, m \in \mathbb{N}_0$ zu zeigen. Wegen $t(n, m) = t(m, n)$ und

$$n - \frac{(n - m)(n - m + 1)}{2} = \frac{1}{2}(n + m - (n - m)^2) = m - \frac{(m - n)(m - n + 1)}{2}$$

können wir $n \geq m$ annehmen. Sei $k := n - m$. Jede Partition von (n, m) entspricht dann einer Darstellung der Form

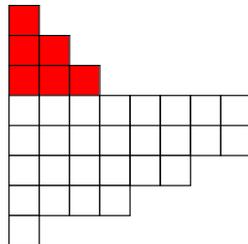
$$n = \sum_{i=1}^{k+s} a_i + \sum_{i=1}^s (b_i - 1) \quad (s \geq 0, 1 \leq a_1 < \dots < a_{k+s}, 1 \leq b_1 < \dots < b_s). \tag{5.5}$$

Sei $N := n - k(k + 1)/2$. Für $N < 0$ ist

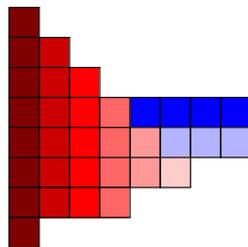
$$\sum_{i=1}^k a_i \geq \sum_{i=1}^k i = \frac{k(k + 1)}{2} > n$$

und (5.5) besitzt keine Lösung. Wegen $p(N) = 0$ ist (5.4) in diesem Fall bewiesen. Im Fall $N = 0$ besitzt (5.5) nur die Lösung $s = 0$ und $a_i = i$ für $i = 1, \dots, k$. Wegen $p(0) = 1$ können wir nun $N > 0$ annehmen.

Wir konstruieren eine Bijektion zwischen $P(N)$ und den Darstellungen (5.5). Sei $\lambda \in P(N)$. Über dem Young-Diagramm von λ platzieren wir ein rechtwinkliges Dreieck mit Seitenlänge k . Beispiel $(n, m) = (33, 30)$, $k = 3$, $N = 27$ und $\lambda = (8^2, 6, 4, 1)$:



Insgesamt erhält man $N + k(k + 1)/2 = n$ Boxen. Man verlängert nun die Diagonale des Dreiecks und teilt die Boxen darunter und darüber in Spalten bzw. Zeilen auf:



Ist $s \geq 0$ die Anzahl der entstandenen Zeilen, so ist $k + s$ die Anzahl der entstandenen Spalten. Sei a_i die Anzahl der Boxen in der i -ten Spalte und sei $b_i - 1 \geq 0$ die Anzahl der Boxen in der i -ten Zeile. Es gilt dann $1 \leq a_1 < \dots < a_{k+s}$, $1 \leq b_1 < \dots < b_s$ und $\sum_{i=1}^{k+s} a_i + \sum_{i=1}^s (b_i - 1) = n$. Wir haben somit eine Darstellung (5.5) gefunden (im Beispiel gilt $s = 3$, $(a_1, \dots, a_6) = (8, 6, 5, 4, 2, 1)$ und $(b_1, b_2, b_3) = (5, 4, 1)$). Umgekehrt kann man mit einer solchen Darstellung starten, das entsprechende Diagramm zeichnen und das obere Dreieck entfernen. Auf diese Weise erhält man stets ein Young-Diagramm einer Partition von N . Diese beiden Prozesse sind offenbar zueinander invers, sodass man eine Bijektion zwischen $P(N)$ und den Darstellungen (5.5) erhält. Damit ist (5.4) bewiesen. \square

Beispiel 5.24.

(i) Für $\alpha \in \{\pm 1, X\}$ wird Satz 5.23 zu

$$\prod_{k=1}^{\infty} (1 - X^{2k})(1 + X^{2k-1})^2 = \sum_{k=-\infty}^{\infty} X^{k^2}, \quad (5.6)$$

$$\prod_{k=1}^{\infty} \frac{(1 - X^k)^2}{1 - X^{2k}} = \prod_{k=1}^{\infty} (1 - X^{2k})(1 - X^{2k-1})^2 = \sum_{k=-\infty}^{\infty} (-1)^k X^{k^2}, \quad (5.7)$$

$$\prod_{k=1}^{\infty} (1 - X^{2k})(1 + X^{2k})^2 = \frac{1}{2} \sum_{k=-\infty}^{\infty} X^{k^2+k} = \sum_{k=0}^{\infty} X^{k^2+k}, \quad (5.8)$$

wobei die Bijektion $k \mapsto -k - 1$ auf \mathbb{Z} in der dritten Formel benutzt wurde. Darin kommt X nur noch mit geradem Exponenten vor. Durch Koeffizientenvergleich darf man die Exponenten halbieren und erhält

$$\prod_{k=1}^{\infty} (1 - X^{2k})(1 + X^k) = \prod_{k=1}^{\infty} (1 - X^k)(1 + X^k)^2 = \sum_{k=0}^{\infty} X^{\frac{k^2+k}{2}}$$

ähnlich zu Satz 5.19.

(ii) Nach Definition 4.18 dürfen wir X durch X^3 in Satz 5.23 ersetzen. Setzt man anschließend $\alpha = -X$, so ergibt sich

$$\prod_{k=1}^{\infty} (1 - X^{6k})(1 - X^{6k-2})(1 - X^{6k-4}) = \sum_{k=-\infty}^{\infty} (-1)^k X^{3k^2+k}.$$

Wieder darf man die Exponenten halbieren und erhält

$$\prod_{k=1}^{\infty} (1 - X^k) = \prod_{k=1}^{\infty} (1 - X^{3k})(1 - X^{3k-1})(1 - X^{3k-2}) = \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{3k^2+k}{2}},$$

d. h. Satz 5.14.

(iii) Ersetzt man X durch X^5 und wählt $\alpha \in \{-X, -X^3\}$, so erhält man auf ähnliche Weise

$$\prod_{k=1}^{\infty} (1 - X^{5k})(1 - X^{5k-2})(1 - X^{5k-3}) = \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+k}{2}}, \quad (5.9)$$

$$\prod_{k=1}^{\infty} (1 - X^{5k})(1 - X^{5k-1})(1 - X^{5k-4}) = \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+3k}{2}}. \quad (5.10)$$

Satz 5.25 (LAGRANGE-JACOBI). *Jede natürliche Zahl ist die Summe von vier Quadratzahlen. Genauer gilt*

$$q(n) := |\{(a, b, c, d) \in \mathbb{Z}^4 : a^2 + b^2 + c^2 + d^2 = n\}| = 8 \sum_{4 \nmid d | n} d$$

für $n \in \mathbb{N}$.

Beweis. Offensichtlich genügt es die zweite Aussage (von Jacobi) zu beweisen. Da die Summanden $(-1)^k(2k+1)X^{\frac{k^2+k}{2}}$ in Satz 5.19 unter der Transformation $k \mapsto -k-1$ invariant sind, gilt

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

Quadrieren ergibt

$$\alpha := \prod_{k=1}^{\infty} (1-X^k)^6 = \frac{1}{4} \sum_{k,l=-\infty}^{\infty} (-1)^{k+l} (2k+1)(2l+1) X^{\frac{k^2+k+l^2+l}{2}}.$$

Die Paare (k, l) mit $k \equiv l \pmod{2}$ transformieren wir mittels $(k, l) \mapsto (s, t) := \frac{1}{2}(k+l, k-l)$, während wir die Paare mit $k \not\equiv l \pmod{2}$ mittels $(s, t) := \frac{1}{2}(k-l-1, k+l+1)$ transformieren. Es gilt $k = s+t$ und $l = s-t$ bzw. $l = t-s-1$. Daher ist

$$\begin{aligned} \alpha &= \frac{1}{4} \sum_{s,t=-\infty}^{\infty} (2s+2t+1)(2s-2t+1) X^{\frac{(s+t)^2+s+t+(s-t)^2+s-t}{2}} \\ &\quad - \frac{1}{4} \sum_{s,t=-\infty}^{\infty} (2s+2t+1)(2t-2s-1) X^{\frac{(s+t)^2+s+t+(t-s-1)^2+t-s-1}{2}} \\ &= \frac{1}{4} \sum_{s,t} ((2s+1)^2 - (2t)^2) X^{s^2+s+t^2} - \frac{1}{4} \sum_{s,t} ((2t)^2 - (2s+1)^2) X^{s^2+s+t^2} \\ &= \frac{1}{2} \sum_{s,t} ((2s+1)^2 - (2t)^2) X^{s^2+s+t^2} \\ &= \frac{1}{2} \sum_{t=-\infty}^{\infty} X^{t^2} \sum_{s=-\infty}^{\infty} (2s+1)^2 X^{s^2+s} - \frac{1}{2} \sum_{s=-\infty}^{\infty} X^{s^2+s} \sum_{t=-\infty}^{\infty} (2t)^2 X^{t^2}. \end{aligned}$$

Für $\beta := \sum X^{t^2}$ und $\gamma := \frac{1}{2} \sum X^{s^2+s}$ gilt $\gamma + 4X\gamma' = \frac{1}{2} \sum (2s+1)^2 X^{s^2+s}$ und es folgt

$$\alpha = \beta(\gamma + 4X\gamma') - 4X\beta'\gamma.$$

Wir wenden die Produktregel auf (5.6) und (5.8) an:

$$\begin{aligned} \beta' &= \left(\prod_{k=1}^{\infty} (1-X^{2k})(1+X^{2k-1})^2 \right)' = \beta \sum_{k=1}^{\infty} \left(2 \frac{(2k-1)X^{2k-2}}{1+X^{2k-1}} - \frac{2kX^{2k-1}}{1-X^{2k}} \right) \\ \gamma' &= \left(\prod_{k=1}^{\infty} (1-X^{2k})(1+X^{2k})^2 \right)' = \gamma \sum_{k=1}^{\infty} \left(2 \frac{2kX^{2k-1}}{1+X^{2k}} - \frac{2kX^{2k-1}}{1-X^{2k}} \right) \end{aligned}$$

Einsetzen ergibt:

$$\alpha = \beta\gamma \left(1 + 8 \sum_{k=1}^{\infty} \left(\frac{2kX^{2k}}{1+X^{2k}} - \frac{(2k-1)X^{2k-1}}{1+X^{2k-1}} \right) \right).$$

Dabei ist $\beta\gamma = \prod (1-X^{2k})^2(1+X^{2k-1})^2(1+X^{2k})^2 = \prod (1-X^{2k})^2(1+X^k)^2 = \prod (1-X^{2k})^4(1-X^k)^{-2}$. Nachdem wir dies mit α verrechnen, verbleibt

$$\left(\sum_{k=-\infty}^{\infty} (-1)^k X^{k^2} \right)^4 \stackrel{(5.7)}{=} \prod_{k=1}^{\infty} \frac{(1-X^k)^8}{(1+X^{2k})^4} = \frac{\alpha}{\beta\gamma} = 1 + 8 \sum_{k=1}^{\infty} \left(\frac{2kX^{2k}}{1+X^{2k}} - \frac{(2k-1)X^{2k-1}}{1+X^{2k-1}} \right).$$

Schließlich ersetzen wir X durch $-X$:

$$\begin{aligned}
 \sum q(n)X^n &= \left(\sum_{k=-\infty}^{\infty} X^{k^2} \right)^4 = 1 + 8 \sum_{k=1}^{\infty} \left(\frac{2kX^{2k}}{1+X^{2k}} + \frac{(2k-1)X^{2k-1}}{1-X^{2k-1}} \right) \\
 &= 1 + 8 \sum_{k=1}^{\infty} \left(\frac{(2k-1)X^{2k-1}}{1-X^{2k-1}} + \frac{2kX^{2k}}{1-X^{2k}} - \frac{2kX^{2k}}{1-X^{2k}} + \frac{2kX^{2k}}{1+X^{2k}} \right) \\
 &= 1 + 8 \sum_{k=1}^{\infty} \left(\frac{kX^k}{1-X^k} - \frac{4kX^{4k}}{1-X^{4k}} \right) = 1 + 8 \sum_{4 \nmid k} \frac{kX^k}{1-X^k} \\
 &= 1 + 8 \sum_{4 \nmid k} k \sum_{l=1}^{\infty} X^{kl} = 1 + 8 \sum_{n=1}^{\infty} \sum_{4 \nmid d|n} dX^n. \quad \square
 \end{aligned}$$

Beispiel 5.26.

- (i) Für $n = 30$ gilt $\sum_{4 \nmid d|30} d = 1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 = 72$. Daher gibt es $8 \cdot 72 = 576$ Möglichkeiten 30 als Summe von vier Quadratzahlen zu schreiben. Diese entstehen durch Permutation und Vorzeichenwahl aus

$$30 = 1^2 + 2^2 + 3^2 + 4^2 = 0^2 + 1^2 + 2^2 + 5^2.$$

- (ii) Offenbar ist 7 keine Summe von drei Quadratzahlen. Wegen $a^2 + b^2 + c^2 \not\equiv 7 \pmod{8}$ ist allgemeiner jede Zahl $n \equiv 7 \pmod{8}$ keine Summe von drei Quadraten.

Bemerkung 5.27.

- (i) Sind $n, m \in \mathbb{N}$ Summen von vier Quadratzahlen, so auch nm , denn es gilt die eulersche Identität:

$$\begin{aligned}
 (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) &= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 \\
 &+ (a_1b_2 - a_2b_1 + a_3b_4 + a_4b_3)^2 + (a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4)^2 + (a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2)^2
 \end{aligned}$$

Dies reduziert die erste Aussage (von Lagrange) in Satz 5.25 auf den Fall $n \in \mathbb{P}$.

- (ii) Das *Waring-Problem* für $k \in \mathbb{N}$ fragt nach der kleinsten Zahl $w(k) \in \mathbb{N}$, sodass jede natürliche Zahl die Summe von $w(k)$ k -ten Potenzen ist. Hilbert bewies $w(k) < \infty$. Es gilt $w(1) = 1$, $w(2) = 4$ (Satz 5.25), $w(3) = 9$, $w(4) = 19$ und man vermutet allgemein

$$w(k) = \left\lfloor \left(\frac{3}{2} \right)^k \right\rfloor + 2^k - 2.$$

Interessanterweise sind nur die Zahlen $23 = 2 \cdot 2^3 + 7 \cdot 1^3$ und $239 = 2 \cdot 4^3 + 4 \cdot 3^3 + 3 \cdot 1^3$ nicht die Summe von acht Kubikzahlen. Es gibt zudem nur 15 Zahlen, die nicht die Summe von sieben Kubikzahlen sind. Man vermutet allgemeiner, dass jede hinreichend große Zahl die Summe von vier Kubikzahlen ist.

- (iii) Da jede ungerade Zahl die Form $\pm 1 + 4k$ hat, lässt sich Satz 5.7(i) wie folgt formulieren: Die Anzahl der Partitionen in ungleiche Teile ist gleich der Anzahl der Partitionen in Teile der Form $\pm 1 + 4k$. Wir ersetzen nun $\pm 1 + 4k$ durch $\pm 1 + 5k$.

Satz 5.28 (ROGERS-RAMANUJAN-Identitäten). *Es gilt*

$$\prod_{k=1}^{\infty} \frac{1}{(1 - X^{5k-1})(1 - X^{5k-4})} = \sum_{k=0}^{\infty} \frac{X^{k^2}}{X^{k!}}, \quad (5.11)$$

$$\prod_{k=1}^{\infty} \frac{1}{(1 - X^{5k-2})(1 - X^{5k-3})} = \sum_{k=0}^{\infty} \frac{X^{k^2+k}}{X^{k!}}. \quad (5.12)$$

Beweis (CHAPMAN). Für $n \in \mathbb{N}_0$ sei

$$\begin{aligned} \alpha_n &:= \sum_{k=0}^{\infty} X^{k^2} \left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle & \beta_n &:= \sum_{k=0}^{\infty} X^{k^2+k} \left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle \\ \tilde{\alpha}_n &:= \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+k}{2}} \left\langle \begin{matrix} 2n \\ n+2k \end{matrix} \right\rangle & \tilde{\beta}_n &:= \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2-3k}{2}} \left\langle \begin{matrix} 2n+1 \\ n+2k \end{matrix} \right\rangle \end{aligned}$$

(alle Summen sind endlich). Es gilt $\alpha_0 = \beta_0 = \tilde{\alpha}_0 = \tilde{\beta}_0 = 1$. Für $n \geq 1$ ist

$$\begin{aligned} \alpha_n &\stackrel{(4.41)}{=} \sum_{k=0}^{\infty} X^{k^2} \left(\left\langle \begin{matrix} n-1 \\ k \end{matrix} \right\rangle + X^{n-k} \left\langle \begin{matrix} n-1 \\ k-1 \end{matrix} \right\rangle \right) = \alpha_{n-1} + X^n \sum_{k=1}^{\infty} X^{k(k-1)} \left\langle \begin{matrix} n-1 \\ k-1 \end{matrix} \right\rangle \\ &= \alpha_{n-1} + X^n \sum_{k=0}^{\infty} X^{k(k+1)} \left\langle \begin{matrix} n-1 \\ k \end{matrix} \right\rangle = \alpha_{n-1} + X^n \beta_{n-1}, \\ \beta_n - X^n \alpha_n &= \sum_{k=0}^{\infty} X^{k^2+k} \left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle (1 - X^{n-k}) = \sum_{k=0}^{\infty} X^{k^2+k} \frac{X^{n!}}{X^{k!} X^{n-k!}} (1 - X^{n-k}) \\ &= (1 - X^n) \sum_{k=0}^{\infty} X^{k^2+k} \left\langle \begin{matrix} n-1 \\ k \end{matrix} \right\rangle = (1 - X^n) \beta_{n-1}. \end{aligned}$$

Durch diese Rekursionsgleichungen sind α_n und β_n eindeutig bestimmt. Wir zeigen nun, dass eine „Indexverschiebung“ $\tilde{\alpha}_n$ nicht ändert:

$$\begin{aligned} &\sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+k}{2}} \left\langle \begin{matrix} 2n+1 \\ n+2k+1 \end{matrix} \right\rangle \stackrel{(4.41)}{=} \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+k}{2}} \left(\left\langle \begin{matrix} 2n \\ n+2k \end{matrix} \right\rangle + X^{n+2k+1} \left\langle \begin{matrix} 2n \\ n+2k+1 \end{matrix} \right\rangle \right) \\ &= \tilde{\alpha}_n + X^{n+1} \left(\sum_{k=0}^{\infty} (-1)^k X^{\frac{5k^2+5k}{2}} \left\langle \begin{matrix} 2n \\ n+2k+1 \end{matrix} \right\rangle + \sum_{k=-\infty}^{-1} (-1)^k X^{\frac{5k(k+1)}{2}} \left\langle \begin{matrix} 2n \\ n+2k+1 \end{matrix} \right\rangle \right) \\ &= \tilde{\alpha}_n + X^{n+1} \left(\sum_{k=0}^{\infty} (-1)^k X^{\frac{5k^2+5k}{2}} \left\langle \begin{matrix} 2n \\ n+2k+1 \end{matrix} \right\rangle + \sum_{k=0}^{\infty} (-1)^{-k-1} X^{\frac{5(-k-1)(-k)}{2}} \left\langle \begin{matrix} 2n \\ n-2k-1 \end{matrix} \right\rangle \right) \\ &= \tilde{\alpha}_n + X^{n+1} \left(\sum_{k=0}^{\infty} (-1)^k X^{\frac{5k^2+5k}{2}} \left\langle \begin{matrix} 2n \\ n+2k+1 \end{matrix} \right\rangle - \sum_{k=0}^{\infty} (-1)^k X^{\frac{5k^2+5k}{2}} \left\langle \begin{matrix} 2n \\ n+2k+1 \end{matrix} \right\rangle \right) = \tilde{\alpha}_n. \end{aligned}$$

Daher gilt

$$\begin{aligned} \tilde{\alpha}_n - \tilde{\alpha}_{n-1} &= \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+k}{2}} \left\langle \begin{matrix} 2n \\ n+2k \end{matrix} \right\rangle - \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+k}{2}} \left\langle \begin{matrix} 2n-1 \\ n+2k \end{matrix} \right\rangle \\ &\stackrel{(4.41)}{=} \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+k}{2}} X^{n-2k} \left\langle \begin{matrix} 2n-1 \\ n+2k-1 \end{matrix} \right\rangle = X^n \tilde{\beta}_{n-1}, \end{aligned}$$

$$\begin{aligned}
\widetilde{\beta}_n - X^n \widetilde{\alpha}_n &= \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2-3k}{2}} \left(\left\langle \begin{matrix} 2n+1 \\ n+2k \end{matrix} \right\rangle - X^{n+2k} \left\langle \begin{matrix} 2n \\ n+2k \end{matrix} \right\rangle \right) = \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2-3k}{2}} \left\langle \begin{matrix} 2n \\ n+2k-1 \end{matrix} \right\rangle \\
&= \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2-3k}{2}} \left(\left\langle \begin{matrix} 2n-1 \\ n+2k-1 \end{matrix} \right\rangle + X^{n-2k+1} \left\langle \begin{matrix} 2n-1 \\ n+2k-2 \end{matrix} \right\rangle \right) \\
&= \widetilde{\beta}_{n-1} + X^n \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2-7k+2}{2}} \left\langle \begin{matrix} 2n-1 \\ n+2k-2 \end{matrix} \right\rangle \\
&= \widetilde{\beta}_{n-1} + X^n \sum_{k=-\infty}^{\infty} (-1)^{1-k} X^{\frac{5(1-k)^2-7(1-k)+2}{2}} \left\langle \begin{matrix} 2n-1 \\ n-2k \end{matrix} \right\rangle \\
&= \widetilde{\beta}_{n-1} - X^n \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{k^2-3k}{2}} \left\langle \begin{matrix} 2n-1 \\ n+2k-1 \end{matrix} \right\rangle = (1 - X^n) \widetilde{\beta}_{n-1}.
\end{aligned}$$

Somit erfüllen $\widetilde{\alpha}_n$ und $\widetilde{\beta}_n$ die gleichen Rekursionsgleichungen. Induktiv erhält man $\alpha_n = \widetilde{\alpha}_n$ und $\beta_n = \widetilde{\beta}_n$ für alle $n \in \mathbb{N}_0$. Nun gilt

$$\left| \sum_{k=0}^n X^{k^2} \left(\frac{1}{X^{k!}} - \left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle \right) \right| \stackrel{5.11}{\leq} \max_{k=0, \dots, n} 2^{-k^2-n+k-1} \leq 2^{-n} \rightarrow 0 \quad (n \rightarrow \infty).$$

Dies zeigt

$$\begin{aligned}
\sum_{k=0}^{\infty} \frac{X^{k^2}}{X^{k!}} &= \sum_{k=0}^{\infty} X^{k^2} \lim_{n \rightarrow \infty} \left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle = \lim_{n \rightarrow \infty} \alpha_n = \lim_{n \rightarrow \infty} \widetilde{\alpha}_n = \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2+k}{2}} \lim_{n \rightarrow \infty} \left\langle \begin{matrix} 2n \\ n+2k \end{matrix} \right\rangle \\
&\stackrel{(5.9)+5.11}{=} \frac{\prod_{k=1}^{\infty} (1 - X^{5k})(1 - X^{5k-2})(1 - X^{5k-3})}{\prod_{k=1}^{\infty} (1 - X^k)} = \prod_{k=1}^{\infty} \frac{1}{(1 - X^{5k-1})(1 - X^{5k-4})}, \\
\sum_{k=0}^{\infty} \frac{X^{k^2+k}}{X^{k!}} &= \sum_{k=0}^{\infty} X^{k^2+k} \lim_{n \rightarrow \infty} \left\langle \begin{matrix} n \\ k \end{matrix} \right\rangle = \lim_{n \rightarrow \infty} \beta_n = \lim_{n \rightarrow \infty} \widetilde{\beta}_n = \sum_{k=-\infty}^{\infty} (-1)^k X^{\frac{5k^2-3k}{2}} \lim_{n \rightarrow \infty} \left\langle \begin{matrix} 2n+1 \\ n+2k \end{matrix} \right\rangle \\
&\stackrel{(5.10)+5.11}{=} \frac{\prod_{k=1}^{\infty} (1 - X^{5k})(1 - X^{5k-1})(1 - X^{5k-4})}{\prod_{k=1}^{\infty} (1 - X^k)} = \prod_{k=1}^{\infty} \frac{1}{(1 - X^{5k-2})(1 - X^{5k-3})}. \quad \square
\end{aligned}$$

Bemerkung 5.29. Der Koeffizient von X^n auf der linken Seite von (5.11) ist die Anzahl der Partitionen von n in Teile der Form $\pm 1 + 5k$. Die rechte Seite von (5.11) ist

$$\sum_{k=0}^{\infty} \sum_{n=0}^{\infty} p_k(n) X^{n+k^2} = \sum_{n=0}^{\infty} \sum_{k=0}^n p_k(n - k^2) X^n.$$

Ist $(\lambda_1, \dots, \lambda_k) \in P(n - k^2)$ mit höchstens k Teilen, so ist $(\lambda_1 + 2k - 1, \lambda_2 + 2k - 3, \dots, \lambda_k + 1)$ eine Partition von $n - k^2 + 1 + 3 + \dots + 2k - 1 = n$ mit genau k Teilen, die sich alle um mindestens 2 unterscheiden. Fazit: Die Anzahl der Partition von n in Teile, die sich um mindestens 2 unterscheiden, ist gleich der Anzahl der Partitionen in Teile der Form $\pm 1 + 5k$. Benutzt man $k^2 + k = 2 + 4 + \dots + 2k$, so erhält man folgende Interpretation von (5.12): Die Anzahl der Partition von n in Teile, die sich um mindestens 2 unterscheiden und größer als 1 sind, ist gleich der Anzahl der Partitionen mit Teilen der Form $\pm 2 + 5k$.

6. Polynome

Definition 6.1. Eine (formale) Potenzreihe $\alpha = \sum a_n X^n \in K[[X]]$ mit nur endlich vielen von 0 verschiedenen Summanden nennt man *Polynom* vom Grad $\deg(\alpha) := \sup\{n \in \mathbb{N}_0 : a_n \neq 0\}$ (wobei $\deg(0) = \sup \emptyset = -\infty$). Die Menge der Polynome bezeichnet man mit $K[X]$. Man nennt α *normiert*, falls $\alpha \neq 0$ und $a_{\deg(\alpha)} = 1$. Im Allgemeinen ist $a_{\deg(\alpha)}$ der *führende Koeffizient* von α .

Bemerkung 6.2.

- (i) Im Gegensatz zu Potenzreihen schreibt man Polynome oft in umgekehrter Reihenfolge beginnend mit der höchsten X -Potenz. Zum Beispiel $X^2 + 1 \in \mathbb{R}[X]$.
- (ii) Jedes Polynom $\alpha \in K[X] \setminus \{0\}$ lässt sich *normieren*, indem man mit $a_{\deg(\alpha)}^{-1}$ multipliziert.
- (iii) Jede Potenzreihe lässt sich als Cauchyfolge von Polynomen interpretieren, d. h. $K[[X]]$ ist die *Vervollständigung* von $K[X]$ bzgl. der Metrik in Lemma 4.13.

Lemma 6.3. Für $\alpha, \beta \in K[X]$ gilt $\deg(\alpha + \beta) \leq \max\{\deg(\alpha), \deg(\beta)\}$ und $\deg(\alpha\beta) = \deg(\alpha) + \deg(\beta)$. Insbesondere sind $\alpha + \beta$ und $\alpha\beta$ Polynome.

Beweis. O. B. d. A. sei $\alpha = \sum_{n=0}^{\infty} a_n X^n \neq 0$ und $\beta = \sum_{n=0}^{\infty} b_n X^n \neq 0$ mit $d := \deg(\alpha)$ und $e := \deg(\beta)$. Wegen $a_k + b_k = 0$ für $k > \max\{d, e\}$ ist $\deg(\alpha + \beta) \leq \max\{d, e\}$. Analog ist $\sum_{k=0}^{d+e} a_k b_{d+e-k} = a_d b_e \neq 0$ und $\sum_{k=0}^n a_k b_{n-k} = 0$ für $n > d + e$. Dies zeigt $\deg(\alpha\beta) = \deg(\alpha) + \deg(\beta)$. \square

Bemerkung 6.4.

- (i) Man kann in $K[X]$ also wie in \mathbb{Z} rechnen (beachte: $0, 1 \in K[X]$). Ist $\alpha \in K[X]$ invertierbar in $K[[X]]$, so gilt aber nicht unbedingt $\alpha^{-1} \in K[X]$! Zum Beispiel ist $(1 - X)^{-1} \notin K[X]$.
- (ii) Man kann K durch die *konstanten* Polynome KX^0 in $K[X]$ einbetten, d. h. $K \subseteq K[X] \subseteq K[[X]]$. Genau dann gilt $\alpha \in K$, wenn $\deg(\alpha) \leq 0$.
- (iii) Für Polynome $\alpha = \sum a_n X^n \in K[X]$ und $\beta \in K[X]$ ist $\alpha(\beta) = \sum a_n \beta^n$ stets wohldefiniert (auch wenn das Absolutglied von β nicht verschwindet, vgl. Definition 4.18).

Beispiel 6.5.

- (i) Für $\alpha = a_n X^n + \dots + a_1 X + a_0 \in K[X]$ und $b \in K \subseteq K[[X]]$ ist $\alpha(b) = a_n b^n + \dots + a_1 b + a_0 \in K$. Wie üblich nennt man b *Nullstelle* von α , falls $\alpha(b) = 0$ gilt.
- (ii) Nach Satz 5.10 ist $\langle \binom{n}{k} \rangle$ ein normiertes Polynom vom Grad $k(n - k)$. Für $X = 1$ haben $\langle \binom{n}{k} \rangle$ und $\binom{n}{k}$ die gleiche Rekursionsformel nach (4.41). Wegen $\langle \binom{0}{0} \rangle = 1 = \binom{0}{0}$ stimmen $\langle \binom{n}{k} \rangle$ und $\binom{n}{k}$ sogar überein für $X = 1$. Wir berechnen weitere Werte.

Bemerkung 6.6. Im Folgenden sei K ein endlicher Körper. In der Algebra zeigt man, dass $q := |K|$ stets eine Primzahlpotenz ist. Umgekehrt existiert zu jeder Primzahlpotenz $q > 1$ im Wesentlichen genau ein Körper mit q Elementen. Diesen bezeichnet man mit \mathbb{F}_q .

Beispiel 6.7.

- (i) Für jede Primzahl p ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, d. h. man identifiziert die Elemente von \mathbb{F}_p mit den Zahlen $0, \dots, p-1$ und rechnet modulo p (siehe Definition 6.20). Zum Beispiel gilt $1 + 1 = 0$ in \mathbb{F}_2 und $3 \cdot 5 = 1$ in \mathbb{F}_7 .
- (ii) Die Verknüpfungstabellen für $\mathbb{F}_4 = \{0, 1, a, b\}$ sind wie folgt gegeben:

$+$	0	1	a	b	\cdot	0	1	a	b
0	0	1	a	b	0	0	0	0	0
1	1	0	b	a	1	0	1	a	b
a	a	b	0	1	a	0	a	b	1
b	b	a	1	0	b	0	b	1	a

Satz 6.8. *Es gibt genau $(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$ invertierbare $n \times n$ -Matrizen über jedem Körper mit q Elementen.*

Beweis. Sei K ein Körper mit q Elementen und $A \in K^{n \times n}$. Bekanntlich ist A genau dann invertierbar, wenn die Zeilen von A linear unabhängig sind. Die erste Zeile a_1 von A kann beliebig aus $K^n \setminus \{0\}$ gewählt werden. Hierfür gibt es $q^n - 1$ Möglichkeiten. Die zweite Zeile a_2 darf nicht im Span von a_1 liegen, d. h. $a_2 \in K^n \setminus Ka_1$. Hierfür gibt es $q^n - q$ Möglichkeiten. Für die dritte Zeile gilt $a_3 \in K^n \setminus (Ka_1 + Ka_2)$ usw. □

Satz 6.9. *Der Wert von $\langle \binom{n}{k} \rangle$ an der Stelle $X = q$ ist die Anzahl der k -dimensionalen Untervektorräume eines n -dimensionalen Vektorraums über einen Körper mit q Elementen.*

Beweis. Der Beweis ist ähnlich zu Satz 6.8. Es gibt genau $(q^n - 1)(q^n - q) \dots (q^n - q^{k-1})$ linear unabhängige k -Tupel in K^n . Wir zählen nun wie viele von diesen Tupeln den gleichen Untervektorraum $U \subseteq K^n$ aufspannen. Dies ist offenbar die Anzahl der linear unabhängigen k -Tupel in U , d. h. $(q^k - 1)(q^k - q) \dots (q^k - q^{k-1})$. Die Anzahl der k -dimensionalen Untervektorräume ist daher

$$\frac{(q^n - 1)(q^n - q) \dots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \dots (q^k - q^{k-1})} = \frac{(1 - q^n) \dots (1 - q^{n-k+1})}{(1 - q^k) \dots (1 - q)}. \quad \square$$

Definition 6.10. Ein normiertes Polynom $\alpha \in K[X] \setminus K$ heißt *irreduzibel*, falls es sich nicht in der Form $\alpha = \beta\gamma$ mit $\beta, \gamma \in K[X] \setminus K$ schreiben lässt. Anderenfalls heißt α *reduzibel*.

Beispiel 6.11.

- (i) Normierte Polynome vom Grad 1 sind stets irreduzibel, denn $1 = \deg(\alpha) = \deg(\beta\gamma) = \deg(\beta) + \deg(\gamma)$ impliziert $\deg(\beta) = 0$ oder $\deg(\gamma) = 0$.
- (ii) $X^2 - 2$ ist irreduzibel in $\mathbb{Q}[X]$, denn der Ansatz $X^2 - 2 = (X + a)(X + b)$ führt zu $a + b = 0$ und $ab = -2$, d. h. $a^2 = 2$ und $a = \pm\sqrt{2} \notin \mathbb{Q}$. Wegen $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ ist $X^2 - 2$ allerdings reduzibel in $\mathbb{R}[X]$.
- (iii) $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$, aber nicht in $\mathbb{C}[X]$, denn $X^2 + 1 = (X - i)(X + i) \in \mathbb{C}[X]$.

Satz 6.12 (Division mit Rest). *Für $\alpha \in K[X]$ und $\beta \in K[X] \setminus \{0\}$ existieren $\gamma, \delta \in K[X]$ mit $\alpha = \beta\gamma + \delta$ und $\deg \delta < \deg \beta$.*

Beweis. Wähle $\delta = \sum a_i X^i \in \{\alpha - \mu\beta : \mu \in K[X]\}$ mit möglichst kleinem Grad d . Sei $\beta = \sum b_i X^i$. Gilt $d \geq \deg \beta =: e$, so ist $\deg(\delta - a_d b_e^{-1} X^{d-e} \beta) < d$ im Widerspruch zur Wahl von δ . Also ist $d < e$ und die Behauptung folgt. \square

Lemma 6.13. *Sind $\alpha, \beta \in K[X]$ verschiedene irreduzible Polynome, so existieren $\tilde{\alpha}, \tilde{\beta} \in K[X]$ mit $\alpha\tilde{\alpha} + \beta\tilde{\beta} = 1$.*

Beweis. Seien $\tilde{\alpha}, \tilde{\beta} \in K[X]$, sodass $\rho := \alpha\tilde{\alpha} + \beta\tilde{\beta} \neq 0$ minimalen Grad hat und normiert ist. Division mit Rest liefert $\gamma, \delta \in K[X]$ mit $\alpha = \gamma\rho + \delta$ und $\deg \delta < \deg \rho$. Also ist

$$\delta = \alpha - \gamma\rho = \alpha(1 - \gamma\tilde{\alpha}) - \beta(\gamma\tilde{\beta})$$

und die Wahl von ρ zeigt $\delta = 0$, d. h. $\alpha = \gamma\rho$. Analog ergibt sich $\beta = \tau\rho$ für ein $\tau \in K[X]$. Mit α, β und ρ sind auch γ und τ normiert. Im Fall $\rho \neq 1$ wäre $\alpha = \rho = \beta$, da α und β irreduzibel sind. Dies widerspricht $\alpha \neq \beta$. Also ist $\alpha\tilde{\alpha} + \beta\tilde{\beta} = \rho = 1$. \square

Satz 6.14 (Primfaktorzerlegung in $K[X]$). *Für jedes Polynom $\alpha \in K[X] \setminus \{0\}$ existieren bis auf die Reihenfolge eindeutig bestimmte irreduzible Polynome $\sigma_1, \dots, \sigma_n \in K[X]$ und eine eindeutig bestimmte Konstante $c \in K \setminus \{0\}$ mit $\alpha = c\sigma_1 \dots \sigma_n$.*

Beweis. Existenz: Wegen $\alpha \neq 0$ existiert $c \in K \setminus \{0\}$, sodass $c^{-1}\alpha$ normiert ist. Wir können also annehmen, dass α normiert ist. Induktion nach $d := \deg \alpha$: Im Fall $d = 0$ ist $\alpha = 1$ und wir wählen $n = 0$ (leeres Produkt). Ist α irreduzibel (zum Beispiel $d = 1$), so sind wir ebenfalls fertig. Anderenfalls ist $\alpha = \beta\gamma$ mit $\beta, \gamma \in K[X] \setminus K$. Wegen $d = \deg(\beta\gamma) = \deg(\beta) + \deg(\gamma)$ ist $\deg \beta, \deg \gamma < d$. Nach Induktion sind β und γ Produkte von irreduziblen Polynomen und Konstanten und daher auch α .

Eindeutigkeit: Offenbar ist c als führender Koeffizient von α eindeutig bestimmt. Wir können also wieder annehmen, dass α normiert ist. Sei $\alpha = \sigma_1 \dots \sigma_n = \tau_1 \dots \tau_m$ mit irreduziblen $\sigma_1, \dots, \sigma_n, \tau_1, \dots, \tau_m \in K[X]$. Induktion nach m . Im Fall $m = 1$ ist $n = 1$ und $\sigma_1 = \alpha = \tau_1$. Sei nun $m \geq 2$. Im Fall $\sigma_1 = \tau_1$ ist $\sigma_2 \dots \sigma_n = \tau_2 \dots \tau_m$ und Induktion liefert die Behauptung. Sei nun $\sigma_1 \neq \tau_1$. Dann existieren $\tilde{\sigma}, \tilde{\tau} \in K[X]$ mit $\sigma_1\tilde{\sigma} + \tau_1\tilde{\tau} = 1$ nach Lemma 6.13. Es folgt

$$\sigma_1(\tilde{\sigma}\tau_2 \dots \tau_m + \sigma_2 \dots \sigma_n \tilde{\tau}) = \sigma_1\tilde{\sigma}\tau_2 \dots \tau_m + \tau_1 \dots \tau_m \tilde{\tau} = (\sigma_1\tilde{\sigma} + \tau_1\tilde{\tau})(\tau_2 \dots \tau_m) = \tau_2 \dots \tau_m.$$

Induktiv erhält man $\sigma_1 = \tau_i$ für ein $i \in \{1, \dots, m\}$. Dann ist $\sigma_2 \dots \sigma_n = \tau_1 \dots \tau_{i-1} \tau_{i+1} \dots \tau_m$ und Induktion liefert die Behauptung. \square

Bemerkung 6.15. Über einem endlichen Körper mit q Elementen gibt es offenbar genau q^d normierte Polynome vom Grad d . Wir wollen zählen wie viele davon irreduzibel sind.

Definition 6.16. Sei $I_d(K)$ die Anzahl der irreduziblen Polynome vom Grad $d \geq 1$ über einem Körper K .

Satz 6.17 (GAUSS). *Für jeden Körper K mit $q < \infty$ Elementen gilt*

$$I_d(K) = \frac{1}{d} \sum_{e|d} \mu(e) q^{d/e}$$

mit der klassischen Möbius-Funktion μ . Insbesondere hängt $I_d(K)$ nur von $|K|$ ab.

Beweis. Die q^d normierten Polynome vom Grad d lassen sich nach Satz 6.14 eindeutig als Produkt von irreduziblen Polynomen $\sigma_1 \dots \sigma_n$ schreiben. Dabei gilt $d = \deg(\sigma_1) + \dots + \deg(\sigma_n)$. Also ist q^d der d -te Koeffizient von

$$(1 + X + X^2 + \dots)^{I_1(K)} (1 + X^2 + X^4 + \dots)^{I_2(K)} (1 + X^3 + X^6 + \dots)^{I_3(K)} \dots = \prod_{e=1}^{\infty} \left(\frac{1}{1 - X^e} \right)^{I_e(K)}.$$

Andererseits ist $\frac{1}{1 - qX} = 1 + qX + q^2 X^2 + \dots$ und es folgt

$$\frac{1}{1 - qX} = \prod_{e=1}^{\infty} \left(\frac{1}{1 - X^e} \right)^{I_e(K)}.$$

Wir wenden auf beiden Seiten \log an (unter Beachtung von Lemma 4.33 und Beispiel 4.34):

$$\sum_{n=1}^{\infty} \frac{q^n X^n}{n} = \sum_{e=1}^{\infty} I_e(K) \sum_{f=1}^{\infty} \frac{X^{ef}}{f} = \sum_{n=1}^{\infty} \left(\sum_{e|n} \frac{I_e(K)}{n/e} \right) X^n.$$

Ein Koeffizientenvergleich liefert

$$q^n = \sum_{e|n} I_e(K) e.$$

Möbius-Inversion (Beispiel 3.7(v)) impliziert nun die Behauptung. □

Beispiel 6.18. Nach Satz 6.17 können wir $I_d(q) := I_d(K)$ mit $|K| = q$ definieren. Es gilt dann $I_1(q) = \mu(1)q^1 = q$ (jedes normierte Polynom vom Grad 1 ist irreduzibel). Weiter ist

$$I_2(q) = \frac{1}{2}(q^2 - q), \quad I_3(q) = \frac{1}{3}(q^3 - q), \quad I_4(q) = \frac{1}{4}(q^4 - q^2).$$

Wegen $I_2(2) = 1$ ist $X^2 + X + 1$ das einzige irreduzible Polynom vom Grad 2 in $\mathbb{F}_2[X]$.

Satz 6.19. Für jeden endlichen Körper K und jedes $d \in \mathbb{N}$ existiert ein irreduzibles Polynom in $K[X]$ vom Grad d .

Beweis. Nach Satz 6.17 ist $dI_d(K) = q^d \pm q^{e_1} \pm \dots \pm q^{e_k}$ mit $d > e_1 > \dots > e_k > 0$. Dies zeigt $q^{e_k} \mid dI_d(K)$, aber $q^{e_k+1} \nmid dI_d(K)$. Insbesondere ist $I_d(K) > 0$. □

Definition 6.20. Für $a, b \in \mathbb{Z}$ und $d \in \mathbb{N}$ schreiben wir $a \equiv b \pmod{d}$, falls $d \mid a - b$. Man sagt dann a ist kongruent zu b modulo d .

Beispiel 6.21. Es gilt $7 \equiv -11 \pmod{2}$ und $100 \equiv 0 \pmod{10}$.

Bemerkung 6.22 (Division mit Rest). Für $a \in \mathbb{Z}$ und $d \in \mathbb{N}$ gilt $a \pm d \equiv a \pmod{d}$. Daher existiert ein $b \in \{0, \dots, d-1\}$ mit $a \equiv b \pmod{d}$.

Lemma 6.23. Die Kongruenz modulo $d \in \mathbb{N}$ ist eine Äquivalenzrelation auf \mathbb{Z} mit

$$\left. \begin{array}{l} a \equiv a' \pmod{d} \\ b \equiv b' \pmod{d} \end{array} \right\} \implies a \pm b \equiv a' \pm b' \pmod{d}.$$

Beweis. Reflexiv: $d \mid 0 = a - a$.

Symmetrisch: $d \mid a - b \implies d \mid -(a - b) = b - a$.

Transitiv: $(d \mid a - b) \wedge (d \mid b - c) \implies d \mid (a - b) + (b - c) = a - c$.

Für die letzte Aussage sei $d \mid a - a'$ und $d \mid b - b'$. Dann ist $d \mid (a - a') + (b - b') = (a + b) - (a' + b')$ und $d \mid (a - a')b + (b - b')a' = ab - a'b'$. \square

Beispiel 6.24. Lemma 10.8 vereinfacht viele Rechnungen. Wir wollen prüfen, ob $5^{100} + 2^7$ durch 3 teilbar ist:

$$5^{100} + 2^7 \equiv 2^{100} + (-1)^7 \equiv 4^{50} - 1 \equiv 1^{50} - 1 \equiv 0 \pmod{3}.$$

Lemma 6.25 (FERMATs „kleiner“ Satz). Für $a \in \mathbb{Z}$ und $p \in \mathbb{P}$ gilt $a^p \equiv a \pmod{p}$.

Beweis. Für $p = 2$ gilt $p \mid a(a - 1) = a^2 - a$, denn a oder $a - 1$ ist gerade. Sei also $p > 2$. Wegen

$$a^p \equiv a \pmod{p} \iff (-a)^p \equiv -a^p \equiv -a \pmod{p}$$

können wir $a \geq 0$ annehmen. Sicher gilt die Behauptung für $a \in \{0, 1\}$. Sei also $a \geq 2$. Wir argumentieren nun durch Induktion nach der Anzahl der Primteiler von a . Sei zunächst $a \in \mathbb{P}$ und $K := \mathbb{F}_a$. Aus Satz 6.17 folgt

$$\frac{1}{p}(a^p - a) = \frac{1}{p}(\mu(1)a^p + \mu(p)a^1) = I_p(K) \in \mathbb{N}.$$

Sei nun $a = bc$ mit $1 < b < a$. Nach Induktion gilt $b^p \equiv b \pmod{p}$ und $c^p \equiv c \pmod{p}$. Mit Lemma 6.23 folgt $a^p = (bc)^p = b^p c^p \equiv bc \equiv a \pmod{p}$. \square

Bemerkung 6.26. Ist a nicht durch p teilbar, so folgt $a^{p-1} \equiv 1 \pmod{p}$ aus $p \mid (a^p - a) = a(a^{p-1} - 1)$.

Lemma 6.27. Jedes $\alpha \in K[X] \setminus \{0\}$ besitzt höchstens $\deg(\alpha)$ Nullstellen.

Beweis. Induktion nach $d := \deg \alpha$. Im Fall $d = 0$ ist α konstant und hat daher keine Nullstelle. Sei nun $d > 0$ und $a \in K$ eine Nullstelle von α . Division mit Rest liefert $\alpha = (X - a)\beta + r$ mit $\beta, r \in K[X]$ und $\deg(r) < \deg(X - a) = 1$, d. h. $r \in K$. Dann ist $r = \alpha(a) = 0$, also $\alpha = (X - a)\beta$ mit $\deg(\beta) = d - 1$. Für jede weitere Nullstelle $b \neq a$ von α gilt $0 = \alpha(b) = (b - a)\beta(b) = \beta(b)$. Also ist b auch Nullstelle von β . Nach Induktion besitzt β höchstens $d - 1$ Nullstellen. Insgesamt hat α also höchstens d Nullstellen. \square

Beispiel 6.28. Für $k \in \mathbb{N}_0$ definieren wir

$$\binom{X}{k} := \prod_{i=1}^k \frac{X - i + 1}{i} \in \mathbb{C}[X].$$

Sei $\alpha := \binom{2X}{k} \in \mathbb{C}[X]$ und $\beta := \sum_{i=0}^k \binom{X}{i} \binom{X}{k-i} \in \mathbb{C}[X]$. Nach der Vandermonde-Identität 1.16 gilt dann $(\alpha - \beta)(n) = 0$ für alle $n \in \mathbb{N}$. Lemma 6.27 zeigt $\alpha = \beta$. Daher gilt

$$\binom{2x}{k} = \alpha(x) = \beta(x) = \sum_{i=0}^k \binom{x}{i} \binom{x}{k-i}$$

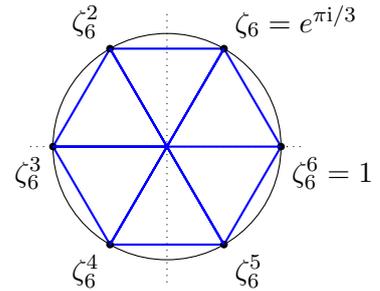
sogar für alle $x \in \mathbb{C}$ und $k \in \mathbb{N}_0$. Zum Beispiel ist

$$\sum_{i=0}^k \binom{1/2}{i} \binom{1/2}{k-i} = \binom{1}{k} = \begin{cases} 1 & \text{falls } k \in \{0, 1\}, \\ 0 & \text{falls } k \geq 2. \end{cases}$$

Definition 6.29. Sei $n \in \mathbb{N}$ und $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$. Die Zahlen $\zeta_n^k := e^{2\pi i k/n} \in \mathbb{C}$ mit $k = 1, \dots, n$ heißen n -te Einheitswurzeln (Stichwort: Polarkoordinaten). Für $\text{ggT}(k, n) = 1$ nennt man ζ_n^k primitiv. Man nennt

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \text{ggT}(k, n) = 1}} (X - \zeta_n^k) \in \mathbb{C}[X]$$

n -tes Kreisteilungspolynom.



Bemerkung 6.30. Mit der eulerschen φ -Funktion gilt $\deg(\Phi_n) = \varphi(n)$.

Beispiel 6.31. Es gilt

- $\zeta_1 = 1$ und $\Phi_1 = X - 1$,
- $\zeta_2 = -1$ und $\Phi_2 = X + 1$,
- $\zeta_3 = \frac{1}{2}(-1 + \sqrt{3}i)$, $\zeta_3^2 = \bar{\zeta}_3$ und

$$\Phi_3 = (X - \zeta_3)(X - \bar{\zeta}_3) = X^2 - (\zeta_3 + \bar{\zeta}_3)X + 1 = X^2 + X + 1,$$

- $\zeta_4 = i$, $\zeta_4^2 = -1 = \zeta_2$, $\zeta_4^3 = -i$ und

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

Satz 6.32. Die n -ten Einheitswurzeln sind die Nullstellen von $X^n - 1$, d. h.

$$X^n - 1 = \prod_{k=1}^n (X - \zeta_n^k)$$

ist die Primfaktorzerlegung von $X^n - 1$ in $\mathbb{C}[X]$.

Beweis. Wegen $(\zeta_n^k)^n = e^{2k\pi i} = (e^{2\pi i})^k = 1$ sind $\zeta_n, \zeta_n^2, \dots, \zeta_n^n$ paarweise verschiedene Nullstellen von $X^n - 1$. Daher hat auch

$$\alpha := X^n - 1 - \prod_{k=1}^n (X - \zeta_n^k)$$

n Nullstellen, aber $\deg \alpha < n$. Lemma 6.27 zeigt $\alpha = 0$. □

Beispiel 6.33. Ein Koeffizientenvergleich (oder eine geometrische Reihe) zeigt $1 + \zeta_3 + \zeta_3^2 = 0$. Für $n \in \mathbb{N}_0$ gilt

$$1 + \zeta_3^n + \zeta_3^{2n} = \begin{cases} 1 + \zeta_3 + \zeta_3^2 = 0 & \text{falls } 3 \nmid n, \\ 1 + 1 + 1 = 3 & \text{falls } 3 \mid n. \end{cases}$$

Für $\alpha = \sum a_n X^n \in \mathbb{C}[[X]]$ erhält man

$$\frac{1}{3}(\alpha + \alpha(\zeta_3 X) + \alpha(\zeta_3^2 X)) = \frac{1}{3} \sum a_n (1 + \zeta_3^n + \zeta_3^{2n}) X^n = \sum a_{3n} X^{3n}.$$

Satz 6.34. Für $n \in \mathbb{N}$ gilt

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

Insbesondere hat Φ_n ganzzahlige Koeffizienten.

Beweis. Für $d \mid n$ ist $\zeta_n^d = e^{2\pi di/n} = \zeta_{n/d}$ eine primitive $\frac{n}{d}$ -te Einheitswurzel. Dies zeigt

$$X^n - 1 \stackrel{6.32}{=} \prod_{k=1}^n (X - \zeta_n^k) = \prod_{d \mid n} \prod_{\substack{1 \leq k \leq n/d, \\ \text{ggT}(k, n/d)=1}} (X - \zeta_n^{dk}) = \prod_{d \mid n} \Phi_{n/d} = \prod_{d \mid n} \Phi_d.$$

Für die zweite Behauptung argumentieren wir durch Induktion nach n . Für $n = 1$ hat $\Phi_1 = X - 1$ ganzzahlige Koeffizienten. Sei nun $n > 1$ und die Behauptung für $d < n$ bewiesen. Dann ist $\alpha := \prod_{d \mid n, d < n} \Phi_d$ normiert mit ganzzahligen Koeffizienten. Da die Polynomdivision $\Phi_n = (X^n - 1)/\alpha$ in $\mathbb{C}[X]$ aufgeht, geht sie auch in $\mathbb{Q}[X]$ auf, d. h. $\Phi_n \in \mathbb{Q}[X]$. Da α normiert ist, treten dabei keine Nenner auf und die Behauptung folgt. \square

Bemerkung 6.35. Gauß hat gezeigt, dass die Kreisteilungspolynome irreduzibel in $\mathbb{Q}[X]$ sind, d. h. $X^n - 1 = \prod_{d \mid n} \Phi_d$ ist die Primfaktorzerlegung von $X^n - 1$ in $\mathbb{Q}[X]$ (ohne Beweis).

Beispiel 6.36. Man kann Satz 6.34 benutzen um Φ_n rekursiv zu berechnen:

$$\begin{aligned} \Phi_1 &= X - 1, \\ \Phi_2 &= \frac{X^2 - 1}{\Phi_1} = X + 1, \\ \Phi_3 &= \frac{X^3 - 1}{\Phi_1} = X^2 + X + 1, \\ \Phi_4 &= \frac{X^4 - 1}{\Phi_1 \Phi_2} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1. \end{aligned}$$

Für $p \in \mathbb{P}$ erhält man allgemein $\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X + 1$ und induktiv

$$\Phi_{p^n} = \frac{X^{p^n} - 1}{\Phi_1 \Phi_p \dots \Phi_{p^{n-1}}} = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \dots + X^{p^{n-1}} + 1 = \Phi_p(X^{p^{n-1}}).$$

Satz 6.37. Für $n \in \mathbb{N}$ gilt

$$\Phi_n = \prod_{d \mid n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$$

mit der klassischen Möbius-Funktion μ .

Beweis. Die Polynome $X^{n/d} - 1$ liegen nach Lemma 4.8 in der abelschen Gruppe $\mathbb{Q}[[X]]^\times$. Die Behauptung folgt daher aus Satz 6.34 und der multiplikativen Version der Möbius-Inversion (Bemerkung 3.8). \square

Beispiel 6.38. Es gilt

$$\Phi_6 = \frac{(X^6 - 1)(X - 1)}{(X^2 - 1)(X^3 - 1)} = \frac{X^3 + 1}{X + 1} = X^2 - X + 1.$$

Satz 6.39.

- (i) Sei $n = p_1^{a_1} \dots p_s^{a_s}$ die Primfaktorzerlegung von $n \in \mathbb{N}$ und $q := p_1 \dots p_s$. Dann gilt $\Phi_n = \Phi_q(X^{\frac{n}{q}})$.
- (ii) Für $n \in \mathbb{N}$ und $p \in \mathbb{P}$ mit $p \nmid n$ gilt $\Phi_{pn} = \frac{\Phi_n(X^p)}{\Phi_n}$.

(iii) Für ungerade $n \geq 3$ gilt $\Phi_{2n} = \Phi_n(-X)$.

Beweis.

(i) Nach Satz 6.37 gilt

$$\Phi_n = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|q} ((X^{\frac{n}{q}})^{\frac{q}{d}} - 1)^{\mu(d)} = \Phi_q(X^{\frac{n}{q}}).$$

(ii) Es gilt

$$\Phi_{pn} = \prod_{d|n} (X^{\frac{pn}{d}} - 1)^{\mu(d)} (X^{\frac{pn}{pd}} - 1)^{\mu(pd)} = \prod_{d|n} \frac{((X^p)^{\frac{n}{d}} - 1)^{\mu(d)}}{(X^{\frac{n}{d}} - 1)^{\mu(d)}} = \frac{\Phi_n(X^p)}{\Phi_n}.$$

(iii) Wegen $n \geq 3$ ist $\varphi(n)$ gerade nach Satz 1.27. Also ist $\Phi_n(-X)$ normiert. Wie in (ii) ist

$$\begin{aligned} \Phi_{2n} &= \prod_{d|n} \left(\frac{(X^{\frac{n}{d}})^2 - 1}{X^{\frac{n}{d}} - 1} \right)^{\mu(d)} = \prod_{d|n} (X^{\frac{n}{d}} + 1)^{\mu(d)} = \pm \prod_{d|n} (-X^{\frac{n}{d}} - 1)^{\mu(d)} \\ &= \pm \prod_{d|n} ((-X)^{\frac{n}{d}} - 1)^{\mu(d)} = \pm \Phi_n(-X) = \Phi_n(-X). \end{aligned} \quad \square$$

Beispiel 6.40. Satz 6.39 erlaubt eine effiziente Berechnung von Φ_n . Zum Beispiel:

$$\begin{aligned} \Phi_{24} &\stackrel{(i)}{=} \Phi_6(X^4) \stackrel{(iii)}{=} \Phi_3(-X^4) \stackrel{6.36}{=} (-X^4)^2 - X^4 + 1 = X^8 - X^4 + 1, \\ \Phi_{300} &= \Phi_{2^2 \cdot 3 \cdot 5^2} \stackrel{(i)}{=} \Phi_{30}(X^{10}) \stackrel{(iii)}{=} \Phi_{15}(-X^{10}) \stackrel{(ii)}{=} \frac{\Phi_3(X^5)}{\Phi_3}(-X^{10}) \\ &= \frac{X^{100} - X^{50} + 1}{X^{20} - X^{10} + 1} = X^{80} + X^{70} - X^{50} - X^{40} - X^{30} + X^{10} + 1. \end{aligned}$$

Bemerkung 6.41. Im Folgenden untersuchen wir die Koeffizienten der Kreisteilungspolynome.

Satz 6.42. Sei $n \geq 2$ und $\Phi_n = \sum_{k=0}^{\varphi(n)} a_k X^k$. Dann gilt $a_k = a_{\varphi(n)-k}$ für $k = 0, \dots, \varphi(n)$, d. h. die Koeffizienten von Φ_n sind „symmetrisch“.

Beweis. Wegen $\Phi_2 = X + 1$ dürfen wir $n \geq 3$ annehmen. Nach Satz 1.27 ist dann $\varphi(n)$ gerade. Mit ζ_n^k ist auch $\zeta_n^{-k} = \zeta_n^{n-k} \neq \zeta_n^k$ eine primitive n -te Einheitswurzel. Dies zeigt

$$a_0 = \Phi_n(0) = \prod_{\substack{1 \leq k \leq n \\ \text{ggT}(k,n)=1}} \zeta_n^k = \prod_{\substack{1 \leq k \leq n/2 \\ \text{ggT}(k,n)=1}} \zeta_n^k \zeta_n^{-k} = 1 = a_{\varphi(n)}.$$

Insbesondere ist $\alpha := \sum_{k=0}^{\varphi(n)} a_k X^{\varphi(n)-k}$ normiert. Für eine primitive n -te Einheitswurzel ζ_n^l gilt

$$\alpha(\zeta_n^l) = \sum_{k=0}^{\varphi(n)} a_k \zeta_n^{l(\varphi(n)-k)} = \zeta_n^{l\varphi(n)} \sum_{k=0}^{\varphi(n)} a_k (\zeta_n^{-l})^k = \zeta_n^{l\varphi(n)} \Phi_n(\zeta_n^{-l}) = 0.$$

Daher hat α die gleichen Nullstellen wie Φ_n und es folgt

$$\alpha = \prod_{\substack{1 \leq k \leq n \\ \text{ggT}(k,n)=1}} (X - \zeta_n^k) = \Phi_n.$$

Also ist $a_k = a_{\varphi(n)-k}$. □

Satz 6.43. Es gilt $\Phi_n = X^{\varphi(n)} - \mu(n)X^{\varphi(n)-1} + \dots - \mu(n)X + 1$ für $n \geq 2$.

Beweis. Für $\alpha = \sum a_n X^n \in \mathbb{Q}[X] \setminus \mathbb{Q}$ sei $f(\alpha) = a_{\deg(\alpha)-1}$. Für $\alpha, \beta \in \mathbb{Q}[X]$ ist dann $f(\alpha\beta) = f(\alpha) + f(\beta)$. Mit dem Kronecker-Delta δ_{ij} folgt

$$\sum_{d|n} f(\Phi_d) = f\left(\prod_{d|n} \Phi_d\right) = f(X^n - 1) = -\delta_{1n} = -\sum_{d|n} \mu(d)$$

für alle $n \in \mathbb{N}$ (siehe Beispiel 3.7). Möbius-Inversion zeigt $f(\Phi_n) = -\mu(n)$. Die anderen Koeffizienten ergeben sich aus Satz 6.42. \square

Bemerkung 6.44. Berechnet man $\Phi_1, \Phi_2, \dots, \Phi_{104}$, so stellt man fest, dass alle Koeffizienten 0 oder ± 1 sind. Suzuki hat aber gezeigt, dass alle ganzen Zahlen als Koeffizienten von Kreisteilungspolynomen auftreten.

7. Polynome in mehreren Unbekannten

Definition 7.1. In diesem Abschnitt sei $n \in \mathbb{N}$ fest. Ein *Polynom* in den Unbekannten X_1, \dots, X_n über einem Körper K ist eine formale Summe der Form $\alpha = \sum a_{k_1, \dots, k_n} X_1^{k_1} \dots X_n^{k_n}$, wobei nur endlich viele der Koeffizienten $a_{k_1, \dots, k_n} \in K$ ungleich 0 sind. Die Menge dieser Polynome wird mit $K[X_1, \dots, X_n]$ bezeichnet. Man nennt $\deg(\alpha) := \sup\{i_1 + \dots + i_n : a_{i_1, \dots, i_n} \neq 0\}$ den *Grad* von α , wobei $\deg 0 = \sup \emptyset = -\infty$.

Bemerkung 7.2.

- (i) Man sieht leicht, dass die Rechenregeln aus Lemma 4.3 auch in $K[X_1, \dots, X_n]$ gelten. Tatsächlich kann man jedes Polynom $\alpha \in K[X_1, \dots, X_n]$ auch als Polynom in X_i mit Koeffizienten in $K[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$ auffassen. Die Regeln $\deg(\alpha + \beta) \leq \max\{\deg \alpha, \deg \beta\}$ und $\deg(\alpha\beta) = \deg \alpha + \deg \beta$ aus Lemma 6.3 gelten auch in $K[X_1, \dots, X_n]$.
- (ii) Obwohl es in $K[X_1, \dots, X_n]$ für $n > 1$ keine Division mit Rest gibt (versuchen Sie X_1 durch X_2 zu teilen), hat Gauß gezeigt, dass $K[X_1, \dots, X_n]$ trotzdem über eine eindeutige Primfaktorzerlegung verfügt (ohne Beweis).
- (iii) Lemma 6.27 gilt in $K[X_1, \dots, X_n]$ für $n > 1$ nicht: Zum Beispiel besitzt $\alpha = X - Y \in \mathbb{R}[X, Y]$ unendlich viele Nullstellen der Form $(x, x) \in \mathbb{R}^2$, obwohl $\deg \alpha = 1$. Wir beweisen einen Ersatz dieser Aussage.

Satz 7.3 (Interpolation). Sei $L \subseteq K^n$ und $d \in \mathbb{N}$ mit $|L| < \binom{n+d}{d}$. Dann existiert ein $\alpha \in K[X_1, \dots, X_n] \setminus \{0\}$ mit $\deg \alpha \leq d$ und $\alpha(x_1, \dots, x_n) = 0$ für alle $(x_1, \dots, x_n) \in L$.

Beweis. Sei V_d der K -Vektorraum aller Polynome $\alpha \in K[X_1, \dots, X_n]$ mit $\deg \alpha \leq d$. Offenbar bilden die Monome $X_1^{a_1} \dots X_n^{a_n}$ mit $a_1 + \dots + a_n \leq d$ eine Basis von V_d . Setzt man $a_0 := d - a_1 + \dots + a_n$, so ist (a_0, \dots, a_n) eine d -elementige Multimenge von $\{0, \dots, n\}$ (a_i ist die Vielfachheit von i). Aus Satz 1.22 folgt $\dim V_d = \binom{n+d}{d}$. Die lineare Abbildung

$$V_d \rightarrow K^{|L|}, \quad \alpha \mapsto (\alpha(x))_{x \in L},$$

hat nicht-trivialen Kern wegen $\dim K^{|L|} = |L| < \dim V_d$. Also existiert $\alpha \in V_d \setminus \{0\}$ mit $\alpha(x_1, \dots, x_n) = 0$ für alle $(x_1, \dots, x_n) \in L$. \square

Lemma 7.4 (SCHWARTZ-ZIPPEL). *Ein Polynom $\alpha \in K[X_1, \dots, X_n] \setminus \{0\}$ besitzt höchstens $|K|^{n-1}$ deg α Nullstellen in K^n .*

Beweis. Induktion nach n . Der Fall $n = 1$ ist genau Lemma 6.27. Sei also $n \geq 2$ und o. B. d. A. $|K| < \infty$. Für $x \in K$ sei $\alpha_x(X_1, \dots, X_{n-1}) := \alpha(X_1, \dots, X_{n-1}, x) \in K[X_1, \dots, X_{n-1}]$. Nehmen wir $\alpha_x = 0$ an. Dann hat $\beta(X_1, \dots, X_n) := \alpha(X_1, \dots, X_{n-1}, X_n + x) \in K[X_1, \dots, X_n]$ die Form $\beta = X_n \gamma$ mit $\gamma \in K[X_1, \dots, X_n]$. Dies zeigt $\alpha = \beta(X_1, \dots, X_{n-1}, X_n - x) = (X_n - x) \tilde{\gamma}$ (man kann also wie gewohnt Linearfaktoren abspalten). Sei $L := \{x \in K : \alpha_x = 0\}$. Durch Iteration erhält man

$$\alpha = \prod_{x \in L} (X_n - x) \gamma$$

mit $\deg \gamma \leq \deg(\alpha) - |L|$ und $\gamma_x \neq 0$ für $x \in K \setminus L$. Sei

$$Z(\alpha) := \{(x_1, \dots, x_n) \in K^n : \alpha(x_1, \dots, x_n) = 0\}$$

die Nullstellenmenge von α . Dann gilt

$$Z(\alpha) \subseteq (K^{n-1} \times L) \cup \bigcup_{x \in K \setminus L} (Z(\gamma_x) \times \{x\}).$$

Nach Induktion ist $|Z(\gamma_x)| \leq |K|^{n-2} \deg \gamma_x \leq |K|^{n-2} (\deg(\alpha) - |L|)$. Insgesamt folgt

$$|Z(\alpha)| \leq |K|^{n-1} |L| + |K| |K|^{n-2} (\deg(\alpha) - |L|) = |K|^{n-1} \deg \alpha. \quad \square$$

Lemma 7.5. *Sei K ein unendlicher Körper und $\alpha, \beta \in K[X_1, \dots, X_n]$ mit $\alpha(x_1, \dots, x_n) = \beta(x_1, \dots, x_n)$ für alle $x_1, \dots, x_n \in K$. Dann ist $\alpha = \beta$.*

Beweis. Für $n = 1$ hat $\alpha - \beta$ unendlich viele Nullstellen und es folgt $\alpha = \beta$. Sei nun $n \geq 2$ und $\alpha - \beta = \sum_{k=0}^d \gamma_k X_n^k$ mit $\gamma_0, \dots, \gamma_d \in K[X_1, \dots, X_{n-1}]$. Für alle $x_1, \dots, x_{n-1} \in K$ hat $\sum_{k=0}^d \gamma_k(x_1, \dots, x_{n-1}) X_n^k \in K[X_n]$ unendlich viele Nullstellen und es folgt wieder $\gamma_k(x_1, \dots, x_{n-1}) = 0$. Durch Induktion nach n ist $\gamma_0 = \dots = \gamma_d = 0$ und damit $\alpha = \beta$. \square

Lemma 7.6. *Sei $\alpha \in K[X_1, \dots, X_n]$. Sei d_i der Grad von α als Polynom in X_i . Seien $L_1, \dots, L_n \subseteq K$ mit $|L_i| > d_i$ für $i = 1, \dots, n$. Ist $\alpha(x_1, \dots, x_n) = 0$ für alle $(x_1, \dots, x_n) \in L_1 \times \dots \times L_n$, so ist $\alpha = 0$.*

Beweis. Für $n = 1$ ist $\deg \alpha = d_1 < |L_1|$ und die Behauptung folgt aus Lemma 6.27. Sei nun $n \geq 2$ und die Behauptung für $n - 1$ bereits bewiesen. Wir schreiben $\alpha = \sum_{i=0}^{d_n} \alpha_i X_n^i$ mit $\alpha_0, \dots, \alpha_{d_n} \in K[X_1, \dots, X_{n-1}]$. Offenbar ist der Grad von α_i als Polynom in X_j höchstens d_j . Seien $(x_1, \dots, x_{n-1}) \in L_1 \times \dots \times L_{n-1}$ fest gewählt. Das Polynom $\beta := \alpha(x_1, \dots, x_{n-1}, X_n) \in K[X_n]$ hat mindestens die Nullstellen $x_n \in L_n$. Wegen $\deg \beta \leq d_n < |L_n|$ ist $\beta = 0$ nach Lemma 6.27. Dies zeigt $\alpha_i(x_1, \dots, x_{n-1}) = 0$ für $i = 0, \dots, d_n$. Nach Induktion folgt $\alpha_0 = \dots = \alpha_{d_n} = 0$ und $\alpha = 0$. \square

Lemma 7.7. *Seien $L_1, \dots, L_n \subseteq K$ nichtleere, endliche Teilmengen und $\alpha \in K[X_1, \dots, X_n]$ mit $\alpha(x_1, \dots, x_n) = 0$ für alle $(x_1, \dots, x_n) \in L_1 \times \dots \times L_n$. Dann existieren $\beta_1, \dots, \beta_n \in K[X_1, \dots, X_n]$ mit $\deg \beta_i \leq \deg(\alpha) - |L_i|$ für $i = 1, \dots, n$ und $\alpha = \sum_{i=1}^n \beta_i \prod_{x_i \in L_i} (X_i - x_i)$.*

Beweis. Für $1 \leq i \leq n$ sei $d_i := |L_i| - 1$ und

$$\gamma_i = \prod_{x_i \in L_i} (X_i - x_i) = X_i^{d_i+1} - \sum_{j=0}^{d_i} c_{ij} X_i^j \in K[X_i].$$

Für $x_i \in L_i$ gilt $x_i^{d_i+1} = \sum_{j=0}^{d_i} c_{ij} x_i^j$. Indem wir jeden Term der Form X_i^e mit $e > d_i$ in α wiederholt durch $X_i^{e-d_i-1} \sum_{j=0}^{d_i} c_{ij} X_i^j$ ersetzen, erhalten wir ein Polynom $\tilde{\alpha} \in K[X_1, \dots, X_n]$ mit folgenden Eigenschaften:

- Der Grad von $\tilde{\alpha}$ in X_i ist höchstens d_i .
- Für $(x_1, \dots, x_n) \in L_1 \times \dots \times L_n$ gilt $\tilde{\alpha}(x_1, \dots, x_n) = \alpha(x_1, \dots, x_n) = 0$.
- $\alpha - \tilde{\alpha} = \sum_{i=1}^n \beta_i \gamma_i$ mit $\beta_1, \dots, \beta_n \in K[X_1, \dots, X_n]$ und $\deg \beta_i \leq \deg(\alpha) - |L_i|$ für $i = 1, \dots, n$.

Aus Lemma 7.6 folgt $\tilde{\alpha} = 0$ und damit die Behauptung. \square

Satz 7.8 (Kombinatorischer Nullstellensatz). *Sei $\alpha \in K[X_1, \dots, X_n]$ mit $\deg \alpha = d_1 + \dots + d_n$, sodass der Koeffizient von $X_1^{d_1} \dots X_n^{d_n}$ in α nicht verschwindet. Seien $L_1, \dots, L_n \subseteq K$ mit $|L_i| > d_i$ für $i = 1, \dots, n$. Dann existiert $(x_1, \dots, x_n) \in L_1 \times \dots \times L_n$ mit $\alpha(x_1, \dots, x_n) \neq 0$.*

Beweis. O. B. d. A. sei $|L_i| = d_i + 1$ für $i = 1, \dots, n$. Nehmen wir indirekt $\alpha(x_1, \dots, x_n) = 0$ für alle $(x_1, \dots, x_n) \in L_1 \times \dots \times L_n$ an. Nach Lemma 7.7 existieren $\beta_1, \dots, \beta_n \in K[X_1, \dots, X_n]$ mit $\deg \beta_i \leq \deg(\alpha) - |L_i| = \sum_{j \neq i} d_j - 1$ und

$$\alpha = \sum_{i=1}^n \beta_i \prod_{x_i \in L_i} (X_i - x_i).$$

Nach Voraussetzung existiert $i \in \{1, \dots, n\}$, sodass der Koeffizient von $X_1^{d_1} \dots X_n^{d_n}$ in $\beta_i \prod_{x_i \in L_i} (X_i - x_i)$ nicht verschwindet. Dann wäre aber $\deg \beta_i \geq \sum_{j \neq i} d_j$. Aus diesem Widerspruch folgt die Behauptung. \square

Bemerkung 7.9.

- Hilberts (ursprünglicher) Nullstellensatz lautet: Sei K ein algebraisch abgeschlossener Körper und $\alpha_1, \dots, \alpha_k, \beta \in K[X_1, \dots, X_n]$, sodass β auf allen gemeinsamen Nullstellen von $\alpha_1, \dots, \alpha_k$ verschwindet. Dann existieren $\beta_1, \dots, \beta_k \in K[X_1, \dots, X_n]$ und $s \in \mathbb{N}$ mit $\beta^s = \alpha_1 \beta_1 + \dots + \alpha_k \beta_k$.
- In der Algebra zeigt man, dass für jede Primzahl p eine *Primitivwurzel* $x \in \mathbb{F}_p$ existiert, d. h. $x^k \neq 1$ für $k = 1, \dots, p-2$ (vgl. Bemerkung 6.26). Ggf. gilt

$$x^k \sum_{y \in \mathbb{F}_p} y^k = \sum_{y \in \mathbb{F}_p} (xy)^k = \sum_{y \in \mathbb{F}_p} y^k.$$

Daraus folgt $\sum_{y \in \mathbb{F}_p} y^k = 0$ für $k = 0, \dots, p-2$ (beachte $0^0 = 1$). Dies wird im nächsten Beweis benutzt.

Satz 7.10 (CHEVALLEY-WARNING). *Seien $\alpha_1, \dots, \alpha_k \in \mathbb{F}_p[X_1, \dots, X_n]$ mit $\sum_{i=1}^k \deg \alpha_i < n$. Dann ist die Anzahl der gemeinsamen Nullstellen von $\alpha_1, \dots, \alpha_k$ in \mathbb{F}_p^n durch p teilbar. Es kann also nie genau eine gemeinsame Nullstelle geben.*

Beweis. Nach Bemerkung 6.26 ist

$$\beta(x) := \prod_{i=1}^k (1 - \alpha_i(x)^{p-1}) = \begin{cases} 1 & \text{falls } x \text{ eine gemeinsame Nullstelle von } \alpha_1, \dots, \alpha_k \text{ ist,} \\ 0 & \text{sonst} \end{cases}$$

für alle $x \in \mathbb{F}_p^n$. Für die Anzahl N der gemeinsamen Nullstellen gilt daher $N \equiv \sum_{x \in \mathbb{F}_p^n} \beta(x) \pmod{p}$. Multipliziert man β aus, so erhält man eine Linearkombination von Monomen der Form $\prod_{i=1}^n x_i^{a_i}$ mit

$$\sum_{i=1}^n a_i \leq (p-1) \sum_{j=1}^k \deg \alpha_j < (p-1)n$$

nach Voraussetzung. In jedem solchen Monom muss es daher ein i mit $a_i < p-1$ geben. O. B. d. A. sei $i = 1$. Nach Bemerkung 7.9 gilt

$$\sum_{x \in \mathbb{F}_p^n} \prod_{i=1}^n x_i^{a_i} = \sum_{x_1 \in \mathbb{F}_p} x_1^{a_1} \sum_{x_2, \dots, x_n \in \mathbb{F}_p} \prod_{i=2}^n x_i^{a_i} = 0.$$

Dies zeigt $N \equiv \sum_{x \in \mathbb{F}_p^n} \beta(x) \equiv 0 \pmod{p}$. Die zweite Behauptung ist klar wegen $p \geq 2$. \square

Satz 7.11 (ERDŐS-GINZBURG-ZIV). *Jede Multimenge aus $2n-1$ ganzen Zahlen besitzt n Elemente, deren Summe durch n teilbar ist.*

Beweis. Sei $k := 2n-1$ und $a_1, \dots, a_k \in \mathbb{Z}$. Nehmen wir zuerst an, dass $n = p$ eine Primzahl ist. Da wir nur an der Teilbarkeit durch p interessiert sind, können wir $a_1, \dots, a_k \in \mathbb{F}_p$ annehmen. Die Polynome

$$\alpha := \sum_{i=1}^k X_i^{p-1}, \quad \beta := \sum_{i=1}^k a_i X_i^{p-1}$$

in $\mathbb{F}_p[X_1, \dots, X_k]$ haben Grad $p-1$ und gemeinsame Nullstelle $(0, \dots, 0)$. Wegen $2(p-1) < k$ muss es nach Chevalley-Warning eine weitere gemeinsame Nullstelle $x := (x_1, \dots, x_k)$ geben. Sei $I := \{1 \leq i \leq k : a_i \neq 0\} \neq \emptyset$. Nach Fermat gilt

$$|I| \equiv \sum_{i=1}^k x_i^{p-1} = \alpha(x) = 0, \quad \sum_{i \in I} a_i = \beta(x) = 0.$$

Aus $|I| \leq k$ folgt $|I| = p$ und $\sum_{i \in I} a_i$ ist durch p teilbar.

Nehmen wir nun $n = pm$ mit $p \in \mathbb{P}$ und $m > 1$ an. Nach dem ersten Teil des Beweises existiert $I_1 \subseteq \{1, \dots, k\}$ mit $|I_1| = p$ und $\sum_{i \in I_1} a_i \equiv 0 \pmod{p}$. Außerdem existiert $I_2 \subseteq \{1, \dots, k\} \setminus I_1$ mit $\sum_{i \in I_2} a_i \equiv 0 \pmod{p}$. Wegen $k - 2(m-1)p = 2p - 1$ finden wir auf die gleiche Weise disjunkte Teilmengen $I_1, \dots, I_{2m-1} \subseteq \{1, \dots, k\}$ mit $|I_j| = p$ und $b_j := \frac{1}{p} \sum_{i \in I_j} a_i \in \mathbb{Z}$ für $j = 1, \dots, 2m-1$. Durch Induktion nach n existiert $J \subseteq \{1, \dots, 2m-1\}$ mit $|J| = m$ und $\sum_{j \in J} b_j \equiv 0 \pmod{m}$. Für $I := \bigcup_{j \in J} I_j$ gilt $|I| = mp = n$ und $\sum_{j \in J} a_j \equiv 0 \pmod{n}$. \square

Beispiel 7.12. Satz 7.11 ist optimal, denn aus der $(2n-2)$ -elementigen Multimenge

$$\underbrace{\{0, \dots, 0\}}_{n-1}, \underbrace{\{1, \dots, 1\}}_{n-1}$$

lassen sich keine n Elemente auswählen, deren Summe durch n teilbar ist.

Definition 7.13. Ein Polynom $\alpha \in K[X_1, \dots, X_n]$ heißt *symmetrisch*, falls

$$\alpha(X_{\pi(1)}, \dots, X_{\pi(n)}) = \alpha(X_1, \dots, X_n)$$

für alle $\pi \in S_n$ gilt. Die *elementar-symmetrischen* Polynome der Ordnung n sind $\sigma_0 := 1$ und

$$\sigma_k := \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k} \quad (k \geq 1).$$

Die *vollständig-symmetrischen* Polynome der Ordnung n sind $\tau_0 := 1$ und

$$\tau_k := \sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} X_{i_1} \dots X_{i_k} \quad (k \geq 1).$$

Die *Potenz-Polynome* sind $\rho_k := X_1^k + \dots + X_n^k$ für $k \geq 0$.

Bemerkung 7.14.

- (i) Die symmetrischen Polynome bilden einen multiplikativ abgeschlossenen Unterraum von $K[X_1, \dots, X_n]$ mit Basis

$$\beta_{(a_1, \dots, a_n)} := \frac{1}{m_1! \dots m_n!} \sum_{\pi \in S_n} X_{\pi(1)}^{a_1} \dots X_{\pi(n)}^{a_n} \quad (a_1 \geq \dots \geq a_n \geq 0),$$

wobei m_i die Vielfachheit von a_i in der Folge (a_1, \dots, a_n) ist (alle Koeffizienten sind 1, sodass die Charakteristik des Körpers keine Rolle spielt). Man erhält

$$\begin{aligned} \sigma_k &= \alpha_{(1^k, 0^{n-k})}, \\ \tau_k &= \sum_{a_1 + \dots + a_n = k} \alpha_{(a_1, \dots, a_n)}, \\ \rho_k &= \alpha_{(k, 0^{n-1})}. \end{aligned}$$

- (ii) Beachte: $\sigma_k = 0$ für $k > n$ und $\rho_0 = n$. Es gilt $\deg \sigma_k = \deg \tau_k = \deg \rho_k = k$ für $k = 1, \dots, n$.

Satz 7.15 (VIETA). *Im Ring der formalen Potenzreihen $K[X_1, \dots, X_n][[Y]]$ mit Koeffizienten in $K[X_1, \dots, X_n]$ gilt*

$$\begin{aligned} \prod_{k=1}^n (1 + X_k Y) &= \sum_{k=0}^n \sigma_k Y^k, \\ \prod_{k=1}^n \frac{1}{1 - X_k Y} &= \sum_{k=0}^{\infty} \tau_k Y^k. \end{aligned}$$

Beweis. Die erste Gleichung ergibt sich durch Ausmultiplizieren. Die zweite Gleichung folgt aus

$$\prod_{k=1}^n \frac{1}{1 - X_k Y} = \prod_{k=1}^n \sum_{l=0}^{\infty} (X_k Y)^l = \sum_{k=0}^{\infty} \left(\sum_{l_1 + \dots + l_n = k} X_1^{l_1} \dots X_n^{l_n} \right) Y^k = \sum_{k=0}^{\infty} \tau_k Y^k. \quad \square$$

Satz 7.16 (GIRARD-NEWTON-Identität). *Für $k \in \mathbb{N}$ gilt*

$$\begin{aligned} \sum_{i=0}^k (-1)^i \sigma_i \tau_{k-i} &= 0, \\ \sum_{i=0}^{\min\{k, n\}} (-1)^i \sigma_i \rho_{k-i} &= \begin{cases} 0 & \text{falls } k \geq n, \\ (-1)^k (n-k) \sigma_k & \text{falls } k < n \end{cases} \end{aligned}$$

Beweis.

(i) Nach Vieta ist

$$1 = \left(\sum_{i=0}^{\infty} (-1)^i \sigma_i Y^i \right) \left(\sum_{j=0}^{\infty} \tau_j Y^j \right) = \sum_{k=0}^{\infty} \left(\sum_{i=0}^k (-1)^i \sigma_i \tau_{k-i} \right) Y^k.$$

Ein Koeffizientenvergleich liefert die erste Behauptung.

(ii) Für $k \in \mathbb{N}_0$ und $0 \leq l \leq n-1$ sei

$$\alpha(k, l) := \sum_{i=1}^n X_i^k \sigma_l(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n).$$

Dann gilt

$$\sigma_i \rho_{k-i} = \begin{cases} \rho_k = \alpha(k, 0) & \text{falls } i = 0, \\ \alpha(k-i, i) + \alpha(k-i+1, i-1) & \text{falls } 1 \leq i \leq k < n, \\ \alpha(k-n+1, n-1) & \text{falls } i = n \leq k. \end{cases}$$

Als Teleskopsumme erhält man die zweite Behauptung (beachte $\alpha(0, l) = (n-l)\sigma_l$). \square

Satz 7.17 (Hauptsatz über symmetrische Polynome). *Für jedes symmetrische $\alpha \in K[X_1, \dots, X_n]$ existiert genau ein $\gamma \in K[X_1, \dots, X_n]$ mit $\alpha = \gamma(\sigma_1, \dots, \sigma_n)$.*

Beweis. Existenz: Sei o. B. d. A.

$$\alpha = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n} \neq 0.$$

Wir ordnen die Tupel (i_1, \dots, i_n) lexikografisch und argumentieren durch Induktion nach

$$f(\alpha) := \max\{(i_1, \dots, i_n) : a_{i_1, \dots, i_n} \neq 0\}.$$

Im Fall $f(\alpha) = (0, \dots, 0)$ ist $\gamma := \alpha = a_{0, \dots, 0} \in K$. Sei nun $f(\alpha) = (d_1, \dots, d_n) > (0, \dots, 0)$. Wegen $\alpha = \alpha(X_{\pi(1)}, \dots, X_{\pi(n)})$ für alle $\pi \in S_n$ ist $d_1 \geq \dots \geq d_n$. Sei

$$\beta := a_{d_1, \dots, d_n} \sigma_1^{d_1-d_2} \sigma_2^{d_2-d_3} \dots \sigma_{n-1}^{d_{n-1}-d_n} \sigma_n^{d_n}.$$

Es gilt $f(\sigma_k^{d_k-d_{k+1}}) = (d_k - d_{k+1}, \dots, d_k - d_{k+1}, 0, \dots, 0)$ und

$$f(\beta) = f(\sigma_1^{d_1-d_2}) + \dots + f(\sigma_n^{d_n}) = (d_1, \dots, d_n).$$

Das symmetrische Polynom $\alpha - \beta$ erfüllt daher $f(\alpha - \beta) < (d_1, \dots, d_n)$ und die Existenz von γ folgt mit Induktion.

Eindeutigkeit: Seien $\gamma, \delta \in K[X_1, \dots, X_n]$ mit $\gamma(\sigma_1, \dots, \sigma_n) = \delta(\sigma_1, \dots, \sigma_n)$. Für $\rho := \gamma - \delta$ ist dann $\rho(\sigma_1, \dots, \sigma_n) = 0$ und wir müssen $\rho = 0$ zeigen. Sei indirekt $\rho \neq 0$. Sei $d_1 \geq \dots \geq d_n$ das lexikografisch größte n -Tupel, sodass der Koeffizient von $X_1^{d_1-d_2} X_2^{d_2-d_3} \dots X_n^{d_n}$ in ρ nicht verschwindet. Wie oben gilt $f(\sigma_1^{d_1-d_2} \dots \sigma_n^{d_n}) = (d_1, \dots, d_n)$. Für jeden weiteren Summanden $X_1^{e_1-e_2} \dots X_n^{e_n}$ von ρ ist $f(\sigma_1^{e_1-e_2} \dots \sigma_n^{e_n}) < (d_1, \dots, d_n)$. Dies ergibt $f(\rho(\sigma_1, \dots, \sigma_n)) = (d_1, \dots, d_n)$ im Widerspruch zu $\rho(\sigma_1, \dots, \sigma_n) = 0$. \square

Beispiel 7.18. Wir betrachten $\alpha = XY^3 + X^3Y - X - Y \in K[X, Y]$. Mit den Bezeichnungen aus dem Beweis ist $f(\alpha) = (3, 1)$ und

$$\beta := \sigma_1^2 \sigma_2 = (X + Y)^2 XY = X^3Y + 2X^2Y^2 + XY^3.$$

Es folgt $\alpha - \beta = -2X^2Y^2 - X - Y$. Im nächsten Schritt ist $f(\alpha - \beta) = (2, 2)$ und

$$\beta_2 := -2\sigma_2^2 = -2X^2Y^2.$$

Es bleibt $\alpha - \beta - \beta_2 = -X - Y = -\sigma_1$. Schließlich ist

$$\alpha = \beta + \beta_2 - \sigma_1 = \sigma_1^2 \sigma_2 - 2\sigma_2^2 - \sigma_1 = \gamma(\sigma_1, \sigma_2)$$

mit $\gamma = X^2Y - 2Y^2 - X$.

Satz 7.19 (WARING-Formel). Für $K = \mathbb{C}$ und $k \in \mathbb{N}$ gilt

$$\begin{aligned} \rho_k &= -k \sum_{(1^{a_1}, \dots, k^{a_k}) \in P(k)} \frac{(a_1 + \dots + a_k - 1)!}{a_1! \dots a_k!} (-\tau_1)^{a_1} \dots (-\tau_k)^{a_k} \\ &= (-1)^k \sum_{(1^{a_1}, \dots, k^{a_k}) \in P(k)} \frac{(a_1 + \dots + a_k - 1)!}{a_1! \dots a_k!} (-\sigma_1)^{a_1} \dots (-\sigma_k)^{a_k}. \end{aligned}$$

Beweis. Wir führen eine neue Variable Y ein und manipulieren die erzeugende Funktion:

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{\rho_k}{k} Y^k &= \sum_{i=1}^n \sum_{k=1}^{\infty} \frac{(X_i Y)^k}{k} = \sum_{i=1}^n \log((1 - X_i Y)^{-1}) = \log\left(\prod_{i=1}^n \frac{1}{1 - X_i Y}\right) \\ &\stackrel{7.15}{=} \log\left(1 + \sum_{i=1}^n \tau_i Y^i\right) = \sum_{l=1}^{\infty} \frac{(-1)^{l-1}}{l} \left(\sum_{i=1}^n \tau_i Y^i\right)^l \\ &\stackrel{1.20}{=} - \sum_{l=1}^{\infty} \frac{1}{l} \sum_{a_1 + \dots + a_n = l} \binom{l}{a_1, \dots, a_n} (-\tau_1)^{a_1} \dots (-\tau_n)^{a_n} Y^{a_1 + 2a_2 + \dots + na_n} \\ &= - \sum_{k=1}^{\infty} \sum_{(1^{a_1}, \dots, k^{a_k}) \in P(k)} \frac{1}{a_1 + \dots + a_k} \binom{a_1 + \dots + a_k}{a_1, \dots, a_k} (-\tau_1)^{a_1} \dots (-\tau_n)^{a_n} Y^k \\ \sum_{k=1}^{\infty} (-1)^k \frac{\rho_k}{k} Y^k &= - \sum_{i=1}^n \sum_{k=1}^{\infty} (-1)^{k-1} \frac{(X_i Y)^k}{k} = - \sum_{i=1}^n \log(1 + X_i Y) = - \log\left(\prod_{i=1}^n (1 + X_i Y)\right) \\ &\stackrel{7.15}{=} - \log\left(1 + \sum_{i=1}^n \sigma_i Y^i\right) = \sum_{l=1}^{\infty} \frac{(-1)^l}{l} \left(\sum_{i=1}^n \sigma_i Y^i\right)^l \\ &\stackrel{1.20}{=} \sum_{l=1}^{\infty} \frac{1}{l} \sum_{a_1 + \dots + a_n = l} \binom{l}{a_1, \dots, a_n} (-\sigma_1)^{a_1} \dots (-\sigma_n)^{a_n} Y^{a_1 + 2a_2 + \dots + na_n} \\ &= \sum_{k=1}^{\infty} \sum_{(1^{a_1}, \dots, k^{a_k}) \in P(k)} \frac{1}{a_1 + \dots + a_k} \binom{a_1 + \dots + a_k}{a_1, \dots, a_k} (-\sigma_1)^{a_1} \dots (-\sigma_n)^{a_n} Y^k. \quad \square \end{aligned}$$

Bemerkung 7.20. Die im nächsten Satz bewiesene Formel hat äußerliche Ähnlichkeit mit der Leibniz-Formel für Determinanten:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)} \quad (A = (a_{ij}) \in K^{n \times n}).$$

Satz 7.21. Für $A \in K^{n \times n}$ und $\sigma \in S_n$ sei $\text{tr}_\sigma(A) := \text{tr}(A^{c_1}) \dots \text{tr}(A^{c_k}) \in K$, wobei c_1, \dots, c_k die Zyklenlängen von σ sind (einschließlich Einerzyklen). Dann gilt

$$\det(A)n! = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \text{tr}_\sigma(A).$$

Beweis. Wir fassen die Einträge von A als unabhängige Variablen im Polynomring $K[X_{ij} : 1 \leq i, j \leq n]$ auf. Nach der Leibniz-Formel ist die Behauptung dann eine Gleichung von Polynomen in $\mathbb{Z}[X_{ij}]$. Nach Lemma 7.5 sind diese Polynome bereits dann gleich, wenn sie an allen Stellen $x_{ij} \in \mathbb{C}$ übereinstimmen. Es genügt daher die Behauptung für $K = \mathbb{C}$ zu beweisen. Seien $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ die Eigenwerte von A mit Vielfachheiten. Nach der Jordanschen Normalform gilt $\text{tr}(A^c) = \lambda_1^c + \dots + \lambda_n^c$ für $c \geq 0$. Für Permutationen $\sigma, \tau \in S_n$ vom gleichen Zyklentyp ist sicher $\text{tr}_\sigma(A) = \text{tr}_\tau(A)$. Wir summieren daher über die Partitionen $(1^{a_1}, \dots, n^{a_n}) \in P(n)$ unter Benutzung von Satz 2.26. Für eine entsprechende Permutation σ gilt $\text{sgn}(\sigma) = \prod_{i=1}^n (-1)^{(i-1)a_i} = (-1)^{n+a_1+\dots+a_n}$. Die rechte Seite ist also

$$\begin{aligned} & n!(-1)^n \sum_{(1^{a_1}, \dots, n^{a_n}) \in P(n)} \frac{(-1)^{a_1+\dots+a_n}}{1^{a_1} a_1! \dots n^{a_n} a_n!} (\lambda_1 + \dots + \lambda_n)^{a_1} \dots (\lambda_1^n + \dots + \lambda_n^n)^{a_n} \\ &= n!(-1)^n \sum_{(1^{a_1}, \dots, n^{a_n}) \in P(n)} \prod_{l=1}^n \frac{(-\rho_l(\lambda_1, \dots, \lambda_n))^{a_l}}{l^{a_l} a_l!} \stackrel{7.5}{=} n! \sigma_n(\lambda_1, \dots, \lambda_n) \\ &= n! \lambda_1 \dots \lambda_n = \det(A)n!. \end{aligned} \quad \square$$

8. Bernoulli-Zahlen

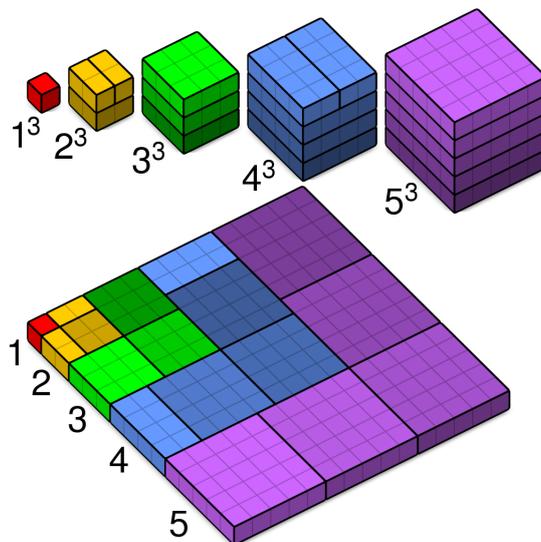
Bemerkung 8.1. Man zeigt leicht (Aufgabe 1):

$$\begin{aligned} 1 + 2 + \dots + n - 1 &= \binom{n}{2}, \\ 1^2 + 2^2 + \dots + (n-1)^2 &= \frac{1}{4} \binom{2n}{3}, \\ 1^3 + 2^3 + \dots + (n-1)^3 &= \binom{n}{2}^2 = (1 + 2 + \dots + (n-1))^2 \quad (\text{Nicomachus-Identität}). \end{aligned}$$

Die erste Formel hat Gauß als Kind durch

$$2(1 + \dots + n - 1) = (1 + n - 1) + (2 + n - 2) + \dots + (n - 1 + 1) = n(n - 1)$$

gefunden. Die dritte sieht man wie folgt⁴:



Wir suchen eine allgemeine Formel für $\sum_{k=1}^n k^m$ mit $m \in \mathbb{N}$. Dafür benutzen wir, dass

$$\frac{\exp(X) - 1}{X} = \sum_{n=1}^{\infty} \frac{X^{n-1}}{n!} = \sum_{n=0}^{\infty} \frac{X^n}{(n+1)!} \in \mathbb{Q}[[X]]$$

invertierbar ist (Lemma 4.8).

Definition 8.2. Die Zahlen $B_0, B_1, \dots \in \mathbb{Q}$ mit

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

heißen *Bernoulli-Zahlen*.

Beispiel 8.3. Wegen

$$\left(B_0 + B_1 X + \frac{B_2}{2} X^2 + \dots \right) \left(1 + \frac{1}{2} X + \frac{1}{6} X^2 + \dots \right) = 1$$

gilt $B_0 = 1$, $B_1 = -1/2$ und $B_2 = 1/6$. Mit dem folgenden Lemma lässt sich B_n rekursiv aus B_k mit $k < n$ berechnen.

Lemma 8.4. Für $n \geq 2$ gilt

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0.$$

Beweis. Ein Koeffizientenvergleich wie in Beispiel 8.3 ergibt

$$0 = \sum_{k=0}^{n-1} \frac{B_k}{k!} \frac{1}{(n-k)!} = \frac{1}{n!} \sum_{k=0}^{n-1} \binom{n}{k} B_k. \quad \square$$

⁴Quelle: <https://math.stackexchange.com/questions/61482/proving-the-identity-sum-k-1n-k3-big-sum-k-1n-k-big2-without-i>

Lemma 8.5. Für $n \in \mathbb{N}$ gilt $B_{2n+1} = 0$.

Beweis. Sei

$$\alpha = 1 + \sum_{k=2}^{\infty} \frac{B_k}{k!} X^k = \frac{X}{\exp(X) - 1} + \frac{1}{2}X = \frac{X \exp(X) + 1}{2 \exp(X) - 1} \stackrel{4.23}{=} \frac{X \exp(\frac{1}{2}X) + \exp(-\frac{1}{2}X)}{2 \exp(\frac{1}{2}X) - \exp(-\frac{1}{2}X)}.$$

Wegen $\alpha(X) = \alpha(-X)$ folgt die Behauptung durch Koeffizientenvergleich. \square

Beispiel 8.6. Wegen

$$\binom{5}{0} B_0 + \binom{5}{1} B_1 + \binom{5}{2} B_2 + \binom{5}{4} B_4 = 0$$

folgt

$$B_4 = -\frac{1}{5} \left(1 - \frac{5}{2} + \frac{10}{6} \right) = -\frac{1}{30}.$$

Obwohl die ersten Bernoulli-Zahlen relativ klein sind, gilt $|B_{2k}| \sim \frac{2(2k)!}{(2\pi)^{2k}} \rightarrow \infty$ (ohne Beweis).

Lemma 8.7. Für $n \in \mathbb{N}$ gilt $(-1)^n B_{2n} < 0$.

Beweis. Nach (dem Beweis von) Lemma 8.5 ist

$$\alpha := \frac{X}{\exp(X) - 1} + \frac{1}{2}X = \sum_{k=0}^{\infty} \frac{B_{2k}}{(2k)!} X^{2k}.$$

Ableitung mit der Quotientenregel ergibt

$$\alpha' = \frac{\exp(X) - 1 - X \exp(X)}{(\exp(X) - 1)^2} + \frac{1}{2} = \sum_{k=1}^{\infty} \frac{B_{2k}}{(2k-1)!} X^{2k-1}.$$

Andererseits ist

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

Einsetzen liefert

$$\sum_{n=0}^{\infty} \left(\sum_{k=0}^n \frac{B_{2k} B_{2(n-k)}}{(2k)!(2(n-k))!} \right) X^{2n} = 1 + \frac{1}{4}X^2 + \sum_{n=1}^{\infty} B_{2n} \left(\frac{1}{(2n)!} - \frac{1}{(2n-1)!} \right) X^{2n}.$$

Nach Koeffizientenvergleich ist

$$\sum_{k=0}^n \binom{2n}{2k} B_{2k} B_{2(n-k)} = (2n)! B_{2n} \frac{(2n-1)! - (2n)!}{(2n-1)!(2n)!} = (1-2n)B_{2n}$$

für $n \geq 2$. Wir subtrahieren $2B_{2n}$ auf beiden Seiten und erhalten

$$(2n+1)B_{2n} = - \sum_{k=1}^{n-1} \binom{2n}{2k} B_{2k} B_{2(n-k)} \quad (8.1)$$

für $n \geq 2$. Wir beweisen nun die Behauptung durch Induktion nach n . Für $n = 1$ ist $B_2 = \frac{1}{6} > 0$. Ist die Behauptung bereits für alle $k < n$ bewiesen, so folgt

$$(-1)^n (2n+1)B_{2n} = - \sum_{k=1}^{n-1} \binom{2n}{2k} \underbrace{(-1)^k B_{2k} (-1)^{n-k} B_{2(n-k)}}_{>0} < 0$$

nach (8.1). \square

Satz 8.8 (FAULHABERSche Formel). Für $n, m \in \mathbb{N}_0$ gilt

$$\sum_{k=0}^{n-1} k^m = \frac{1}{m+1} \sum_{k=0}^m \binom{m+1}{k} B_k n^{m-k+1}.$$

Beweis. Nach Lemma 4.23 gilt

$$\begin{aligned} \sum_{m=0}^{\infty} \frac{1}{m!} \sum_{k=0}^{n-1} k^m X^m &= \sum_{k=0}^{n-1} \sum_{m=0}^{\infty} \frac{k^m X^m}{m!} = \sum_{k=0}^{n-1} \exp(kX) = \sum_{k=0}^{n-1} \exp(X)^k \\ &= \frac{\exp(X)^n - 1}{\exp(X) - 1} = \frac{X}{\exp(X) - 1} \frac{\exp(nX) - 1}{X} \\ &= \sum_{k=0}^{\infty} \frac{B_k}{k!} X^k \cdot \sum_{k=0}^{\infty} \frac{n^{k+1} X^k}{(k+1)!} = \sum_{m=0}^{\infty} \left(\sum_{k=0}^m \frac{B_k}{k!} \frac{n^{m-k+1}}{(m-k+1)!} \right) X^m. \end{aligned}$$

Koeffizientenvergleich ergibt

$$\sum_{k=0}^{n-1} k^m = m! \sum_{k=0}^m \frac{B_k}{k!} \frac{n^{m-k+1}}{(m-k+1)!} = \frac{1}{m+1} \sum_{k=0}^m \binom{m+1}{k} B_k n^{m-k+1} \quad \square$$

Beispiel 8.9. Für $m = 4$ ist

$$\begin{aligned} 1^4 + 2^4 + \dots + (n-1)^4 &= \frac{1}{5} \left(\binom{5}{0} B_0 n^5 + \binom{5}{1} B_1 n^4 + \binom{5}{2} B_2 n^3 + \binom{5}{4} B_4 n \right) \\ &= \frac{1}{5} n^5 - \frac{1}{2} n^4 + \frac{1}{3} n^3 - \frac{1}{30} n = \frac{6n^5 - 15n^4 + 10n^3 - n}{30}. \end{aligned}$$

Bemerkung 8.10.

- (i) Die Faulhabersche Formel drückt die Summe $\sum_{k=0}^{n-1} k^m$ als Polynom in n vom Grad $m+1$ aus. Pascal hat die Existenz dieses Polynoms induktiv gezeigt, ohne die Koeffizienten explizit auszurechnen.⁵
- (ii) Bernoulli-Zahlen treten auch in der Analysis auf:

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

(ohne Beweis). Man kennt hingegen keine Formel für die *Apéry-Konstante* $\sum_{k=1}^{\infty} \frac{1}{k^3} = 1,202\dots$

Satz 8.11. Für $n \in \mathbb{N}_0$ gilt

$$B_n = \sum_{k=0}^n \frac{(-1)^k}{k+1} k! \left\{ \begin{matrix} n \\ k \end{matrix} \right\}.$$

Beweis. Für $k \in \mathbb{N}_0$ gilt nach der Funktionalgleichung

$$(\exp(X) - 1)^k = \sum_{l=0}^k (-1)^{k-l} \binom{k}{l} \exp(lX) = \sum_{n=0}^{\infty} \sum_{l=0}^k (-1)^{k-l} \binom{k}{l} \frac{l^n}{n!} X^n \stackrel{2.37}{=} \sum_{n=0}^{\infty} \frac{k!}{n!} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} X^n.$$

⁵siehe [Beardon, *Sums of Powers of Integers*, Amer. Math. Monthly 103 (1996), 201–213]

Es folgt

$$\begin{aligned}
\sum \frac{B_n}{n!} X^n &= \frac{X}{\exp(X) - 1} = \frac{\log(1 + (\exp(X) - 1))}{\exp(X) - 1} = \frac{1}{\exp(X) - 1} \sum_{k=1}^{\infty} (-1)^{k-1} \frac{(\exp(X) - 1)^k}{k} \\
&= \sum_{k=0}^{\infty} (-1)^k \frac{(\exp(X) - 1)^k}{k+1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k+1} \sum_{n=0}^{\infty} \frac{k!}{n!} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} X^n \\
&= \sum_{n=0}^{\infty} \frac{1}{n!} \left(\sum_{k=0}^{\infty} \frac{(-1)^k}{k+1} k! \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \right) X^n.
\end{aligned}$$

Die Behauptung folgt durch Koeffizientenvergleich. \square

Satz 8.12 (CLAUSEN, VON STAUDT). Für $n \in \mathbb{N}$ existiert ein $z_n \in \mathbb{Z}$ mit

$$B_{2n} = z_n + \sum_{\substack{p \in \mathbb{P} \\ (p-1) \mid 2n}} \frac{1}{p}.$$

Insbesondere ist der (vollständig gekürzte) Nenner von B_{2n} das Produkt aller Primzahlen p mit $p-1 \mid 2n$.

Beweis. Wir analysieren die Summanden $\frac{(-1)^k}{k+1} k! \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\}$ mit $0 \leq k \leq 2n$ in Satz 8.11. Wegen $(-1)^k \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\} \in \mathbb{Z}$ interessieren wir uns nur für $\frac{k!}{k+1}$. Nehmen wir zunächst an, dass $k+1$ keine Primzahl ist. Dann existieren $a, b \in \mathbb{Z}$ mit $k+1 = ab$ und $a, b \leq k$. Im Fall $a \neq b$ ist $k+1 = ab \mid k!$ und $\frac{(-1)^k}{k+1} k! \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\} \in \mathbb{Z}$ folgt. Sei nun $a = b$. Im Fall $2a \leq k$ gilt wieder $k+1 = ab \mid a(2a) \mid k!$ und $\frac{(-1)^k}{k+1} k! \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\} \in \mathbb{Z}$. Im Fall $2a > k$ ist $k+1 = a^2 \geq 2a \geq k+1$. Es folgt $a = 2$ und $k = 3$. Dann gilt

$$(-1)^k k! \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\} \stackrel{2.37}{\equiv} \sum_{l=0}^3 (-1)^l \binom{3}{l} l^{2n} = -3 + 3 \cdot 2^{2n} - 3^{2n} \stackrel{6.23}{\equiv} 1 + 3 \cdot 4^n - 9^n \equiv 1 - 1 \equiv 0 \pmod{4}.$$

Also ist $\frac{(-1)^3}{4} 3! \left\{ \begin{matrix} 2n \\ 3 \end{matrix} \right\} \in \mathbb{Z}$. Die Summanden in Satz 8.11 mit $k+1 \notin \mathbb{P}$ sind somit alle ganzzahlig.

Sei nun $p := k+1 \in \mathbb{P}$. Im Fall $(p-1) \mid 2n$ gilt

$$l^{2n} = (l^{p-1})^{\frac{2n}{p-1}} \stackrel{6.26}{\equiv} 1^{\frac{2n}{p-1}} \equiv 1 \pmod{p}$$

für $l = 1, \dots, p-1 = k$. Dies liefert

$$(-1)^k k! \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\} \stackrel{2.37}{\equiv} \sum_{l=1}^k (-1)^l \binom{k}{l} l^{2n} \equiv -1 + \sum_{l=0}^k (-1)^l \binom{k}{l} \equiv -1 + (1-1)^k \equiv -1 \pmod{p}.$$

Daher ist

$$\frac{1}{p} + \frac{(-1)^k}{k+1} k! \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\} \in \mathbb{Z}.$$

Sei schließlich $(p-1) \nmid 2n$. Dann existieren $m \in \{1, \dots, p-2\}$ und $q \in \mathbb{Z}$ mit $2n = m + q(p-1)$ (Division mit Rest). Für $l = 1, \dots, p-1$ gilt $l^{2n} = l^m (l^{p-1})^q \equiv l^m 1^q \equiv l^m \pmod{p}$ nach Fermat. Dies zeigt

$$(-1)^k k! \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\} = \sum_{l=1}^k (-1)^l \binom{k}{l} l^{2n} \equiv \sum_{l=1}^k (-1)^l \binom{k}{l} l^m \equiv (-1)^k k! \left\{ \begin{matrix} m \\ k \end{matrix} \right\} \equiv 0 \pmod{p}$$

wegen $m < p - 1 = k$. Wir erhalten erneut $\frac{(-1)^k}{k+1} k! \binom{2n}{k} \in \mathbb{Z}$. Damit ist die erste Behauptung bewiesen.

Für die zweite Behauptung sei α der Nenner von B_{2n} und $\{p \in \mathbb{P} : p - 1 \mid 2n\} = \{p_1, \dots, p_s\}$. Wegen $B_{2n} p_1 \dots p_s \in \mathbb{Z}$ ist α ein Teiler von $p_1 \dots p_s$. Außerdem gilt

$$\sum_{i=1}^s \frac{1}{p_i} = \frac{p_2 \dots p_s + p_1 p_3 \dots p_s + \dots + p_1 \dots p_{s-1}}{p_1 \dots p_s}$$

mit

$$p_2 \dots p_s + p_1 p_3 \dots p_s + \dots + p_1 \dots p_{s-1} \equiv p_1 \dots p_{i-1} p_{i+1} \dots p_s \not\equiv 0 \pmod{p_i}$$

für $i = 1, \dots, s$. Wegen $\alpha \sum \frac{1}{p_i} \in \mathbb{Z}$ folgt $p_1 \dots p_s \mid \alpha$. Insgesamt ist daher $\alpha = p_1 \dots p_s$. \square

Beispiel 8.13. Aus Satz 8.12 folgt, dass der Nenner von B_{2n} stets durch 6 teilbar ist. Der Nenner von B_{12} ist zum Beispiel $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730$.

Satz 8.14 (LUCAS). Sei p eine Primzahl und $n = \sum_{i \geq 0} n_i p^i$ sowie $k = \sum_{i \geq 0} k_i p^i$ mit $0 \leq n_i, k_i \leq p - 1$ für $i \geq 0$ (p -adische Entwicklung). Dann gilt

$$\boxed{\binom{n}{k} \equiv \prod_{i \geq 0} \binom{n_i}{k_i} \pmod{p}.}$$

Insbesondere ist $\binom{n}{k}$ genau dann durch p teilbar, wenn ein $i \geq 0$ mit $n_i < k_i$ existiert.

Beweis. Für $0 \leq m < p$ gilt $\binom{p}{m} = \frac{p(p-1)\dots(p-m+1)}{m!} \equiv 0 \pmod{p}$. In $\mathbb{F}_p[X]$ gilt daher

$$(1 + X)^p = \sum_{m=0}^p \binom{p}{m} X^m = 1 + X^p.$$

Induktiv erhält man $(1 + X)^{p^i} = 1 + X^{p^i}$ für alle $i \geq 0$. Es folgt

$$\sum_{m=0}^n \binom{n}{m} X^m = (1 + X)^n = \prod_{i \geq 0} ((1 + X)^{p^i})^{n_i} = \prod_{i \geq 0} (1 + X^{p^i})^{n_i} = \prod_{i \geq 0} \sum_{m_i=0}^{n_i} \binom{n_i}{m_i} X^{m_i p^i}.$$

Multipliziert man das Produkt auf der rechten Seite aus, so entstehen Summanden der Form

$$X^{\sum_{i \geq 0} m_i p^i} \prod_{i \geq 0} \binom{n_i}{m_i}.$$

Da die p -adische Entwicklung von $m = \sum_{i \geq 0} m_i p^i$ eindeutig bestimmt ist, tritt X^m in der Summe nur einmal auf. Ein Koeffizientenvergleich an der Stelle $m = k$ liefert die erste Behauptung.

Wegen $n_i < p$ ist $\binom{n_i}{k_i} \not\equiv 0 \pmod{p}$, falls $k_i \leq n_i$. Im Fall $k_i > n_i$ ist $\binom{n_i}{k_i} = 0$. Daraus folgt die zweite Behauptung. \square

Beispiel 8.15. Wegen $2^n - 1 = 1 + 2 + \dots + 2^{n-1}$ ist $\binom{2^n - 1}{k}$ ungerade für $k = 0, \dots, 2^n - 1$.

9. Catalan-Zahlen

Bemerkung 9.1.

- (i) Ein *Magma* ist eine Menge M zusammen mit einer Abbildung (*Verknüpfung*) $\cdot: M \times M \rightarrow M$, $(x, y) \mapsto x \cdot y$. Für $x_1, \dots, x_n \in M$ ist dann das Produkt $x_1 \cdot \dots \cdot x_n$ in der Regel nicht wohldefiniert, denn unterschiedliche Klammerungen können verschiedene Ergebnisse liefern (M ist nicht unbedingt assoziativ). Wir untersuchen wie viele mögliche Klammerungen es gibt.
- (ii) Selbst wenn M assoziativ ist, kann man durch geeignete Klammerung Rechenzeit sparen. Sind zum Beispiel A, B und C (reelle) Matrizen vom Format 10×20 , 20×5 und 5×100 , so benötigt man für $(AB)C$ nur

$$10 \cdot 20 \cdot 5 + 10 \cdot 5 \cdot 100 = 6000$$

Multiplikationen (reeller Zahlen), während man für $A(BC)$ bereits

$$20 \cdot 5 \cdot 100 + 10 \cdot 20 \cdot 100 = 30.000$$

Multiplikationen benötigt.

Beispiel 9.2. Die ganzen Zahlen \mathbb{Z} bilden bzgl. Subtraktion ein Magma. Es gilt

$$(1 - 2) - 3 = -4 \neq 2 = 1 - (2 - 3).$$

Definition 9.3. Für $n \in \mathbb{N}_0$ sei C_n die Anzahl der möglichen Klammerungen von $x_1 \cdot \dots \cdot x_{n+1}$, wobei x_1, \dots, x_{n+1} Elemente eines Magmas sind. Man nennt C_n die *n-te Catalan-Zahl*.

Beispiel 9.4. Sicher ist $C_0 = C_1 = 1$ und $C_2 = 2$. Weiter gilt $C_3 = 5$ wegen

$$x_1(x_2(x_3x_4)), \quad x_1((x_2x_3)x_4), \quad (x_1x_2)(x_3x_4), \quad ((x_1x_2)x_3)x_4, \quad (x_1(x_2x_3))x_4.$$

Lemma 9.5 (SEGNER). Für $n \in \mathbb{N}_0$ gilt

$$C_{n+1} = \sum_{k=0}^n C_k C_{n-k}.$$

Beweis. Jede Klammerung von $x_1 \dots x_{n+2}$ hat die Form $(x_1 \dots x_{k+1})(x_{k+2} \dots x_{n+2})$ für ein $k \in \{0, \dots, n\}$. Innerhalb der ersten Klammer $(x_1 \dots x_{k+1})$ gibt es C_k viele Klammerungen und innerhalb der zweiten Klammer gibt es C_{n-k} mögliche Klammerungen. Dies zeigt die Behauptung. \square

Beispiel 9.6.

- (i) Ist $n \geq 2$ gerade, so auch $C_n = 2 \sum_{k=0}^{n/2-1} C_k C_{n-1-k}$. Insbesondere ist

$$C_4 = 2(C_0 C_3 + C_1 C_2) = 2(5 + 2) = 14.$$

- (ii) Sei $\alpha = \sum a_n X^n \in \mathbb{Q}[[X]]$ die Umkehrfunktion von $X - X^2$ (Aufgabe 21). Dann gilt

$$X = \alpha - \alpha^2 = \sum_{n=0}^{\infty} a_n X^n - \sum_{n=0}^{\infty} \sum_{k=0}^n a_k a_{n-k} X^n = \sum_{n=0}^{\infty} \left(a_n - \sum_{k=0}^n a_k a_{n-k} \right) X^n$$

und es folgt $a_0 = 0$ (nach Satz 4.24), $a_1 = 1$ sowie $a_n = \sum_{k=1}^{n-1} a_k a_{n-k}$ für $n \geq 2$. Also ist $a_n = C_{n-1}$ für $n \in \mathbb{N}$.

Satz 9.7 (EULER). Die erzeugende Funktion von C_n ist

$$\frac{1 - \sqrt{1 - 4X}}{2X}.$$

Beweis. Sei $\alpha = \sum C_n X^n$. Dann gilt

$$\begin{aligned} (1 - 2X\alpha)^2 &= (1 - 2C_0X - 2C_1X^2 - 2C_2X^3 - \dots)^2 \\ &= 1 - 4X + \sum_{n=2}^{\infty} \left(-4C_{n-1} + 4 \sum_{k=0}^{n-2} C_k C_{n-2-k} \right) X^n \stackrel{9.5}{=} 1 - 4X. \end{aligned}$$

Dies zeigt $1 - 2X\alpha = \sqrt{1 - 4X}$ und die Behauptung folgt. □

Satz 9.8 (CATALAN). Für $n \in \mathbb{N}_0$ gilt

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

Beweis. Nach dem Newtonschen Binomialsatz ist

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

Ein Koeffizientenvergleich nach Satz 9.7 zeigt

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

Beispiel 9.9. Es gilt

$$C_5 = \frac{1}{6} \binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{120} = 2 \cdot 3 \cdot 7 = 42.$$

Definition 9.10. Sei $n \in \mathbb{N}$ und $\{a, b, c\} = \{1, 2, 3\}$. Eine Permutation $\sigma \in S_n$ besitzt das Muster abc , falls $1 \leq i_1 < i_2 < i_3 \leq n$ mit $\sigma(i_a) < \sigma(i_b) < \sigma(i_c)$ existieren. Anderenfalls sagt man: σ vermeidet das Muster abc .

Beispiel 9.11. Die Permutationen in S_4 , die das Muster 123 besitzen sind:

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

Es gibt also $|S_4| - 10 = 14$ Permutationen, die 123 vermeiden.

Satz 9.12 (MACMAHON). Die Anzahl der Permutationen in S_n , die ein Muster abc vermeiden ist C_n .

Beweis (SIMION-SCHMIDT). Sei $S_n(abc)$ die Menge der Permutationen in S_n , die abc vermeiden. Mit der Konvention $S_0 = \{\text{id}_\emptyset\}$ gilt $|S_0(abc)| = |S_1(abc)| = 1 = C_0 = C_1$ und $|S_2(abc)| = 2 = C_2$. Sei also $n \geq 3$ und die Behauptung für kleinere n bereits bewiesen.

Wir zeigen zunächst $|S_n(132)| = C_n$. Sei $\sigma \in S_n(132)$ und $y := \sigma^{-1}(n)$. Für $1 \leq x < y < z \leq n$ gilt dann $\sigma(x) > \sigma(z)$, denn anderenfalls wäre $\sigma(x) < \sigma(z) < \sigma(y) = n$ und σ besäße das Muster 132. Also ist $\{\sigma(x) : 1 \leq x < y\} = \{n-1, n-2, \dots, n-y+1\}$ und $\{\sigma(z) : y < z \leq n\} = \{1, 2, \dots, n-y\}$. Die Permutationen

$$\begin{pmatrix} 1 & 2 & \cdots & y-1 \\ \sigma(1) - n + y & \sigma(2) - n + y & \cdots & \sigma(y-1) - n + y \end{pmatrix} \in S_{y-1},$$

$$\begin{pmatrix} 1 & 2 & \cdots & n-y \\ \sigma(y+1) & \sigma(y+2) & \cdots & \sigma(n) \end{pmatrix} \in S_{n-y}$$

vermeiden ebenfalls 132. Bei festem $y = \sigma^{-1}(n)$ gibt also $|S_{y-1}(132)||S_{n-y}(132)| = C_{y-1}C_{n-y}$ mögliche σ (Induktion). Insgesamt erhält man

$$|S_n(132)| = \sum_{y=1}^n C_{y-1}C_{n-y} = \sum_{y=0}^{n-1} C_y C_{n-y-1} = C_n$$

nach Segner.

Die Bijektionen

$$\Gamma: S_n(abc) \rightarrow S_n(cba), \quad \Delta: S_n(abc) \rightarrow S_n(4-a, 4-b, 4-c),$$

$$\begin{pmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & \cdots & n \\ a_n & \cdots & a_1 \end{pmatrix}, \quad \begin{pmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & \cdots & n \\ n+1-a_1 & \cdots & n+1-a_n \end{pmatrix}$$

zeigen $|S_n(132)| \stackrel{\Gamma}{=} |S_n(231)| \stackrel{\Delta}{=} |S_n(213)| \stackrel{\Gamma}{=} |S_n(312)|$ und $|S_n(123)| \stackrel{\Gamma}{=} |S_n(321)|$. Es genügt also eine Bijektion $f: S_n(132) \rightarrow S_n(123)$ zu konstruieren. Für $\sigma \in S_n(132)$ sei

$$M(\sigma) := \{(k, \sigma(k)) : \sigma(k) < \sigma(i) \text{ für } i = 1, \dots, k-1\}$$

die Menge der *Linksminima*. Wir konstruieren $f(\sigma)$ aus σ , indem wir $M(\sigma)$ festhalten und die übrigen Bilder von σ absteigend sortieren. Zum Beispiel:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \boxed{6} & 7 & \boxed{3} & 4 & \boxed{1} & 2 & 5 & 8 \end{pmatrix} \xrightarrow{f} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \boxed{6} & 8 & \boxed{3} & 7 & \boxed{1} & 5 & 4 & 2 \end{pmatrix}.$$

Dann ist $f(\sigma)$ die einzige Permutation in $S_n(123)$ mit $M(f(\sigma)) = M(\sigma)$. Für $\sigma \in S_n(123)$ konstruieren wir umgekehrt $\tau \in S_n(132)$ wie folgt: Für $i = 1, \dots, n$ sei $\tau(i) := \sigma(i)$ falls $(i, \sigma(i)) \in M(\sigma)$ und anderenfalls sei $\tau(i)$ die kleinste noch nicht benutzte Zahl, die größer als das nächste Linksminimum links von i ist. Dies liefert eine Abbildung $g: S_n(123) \rightarrow S_n(132)$, $\sigma \mapsto \tau$. Zum Beispiel:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \boxed{6} & 8 & \boxed{3} & 7 & \boxed{1} & 5 & 4 & 2 \end{pmatrix} \xrightarrow{g} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \boxed{6} & 7 & \boxed{3} & 4 & \boxed{1} & 2 & 5 & 8 \end{pmatrix}.$$

Wieder ist $g(\sigma)$ die einzige Permutation in $S_n(132)$ mit $M(g(\sigma)) = M(\sigma)$. Es folgt $f \circ g = \text{id}_{S_n(123)}$ und $g \circ f = \text{id}_{S_n(132)}$. Insbesondere ist f eine Bijektion und $|S_n(132)| = |S_n(123)|$. \square

Bemerkung 9.13. Man kennt keine einfachen Formeln für die Anzahl der Permutationen, die 1234 vermeiden (siehe <https://oeis.org/A005802>).

10. Gruppen

Bemerkung 10.1. Viele Zählprobleme vereinfachen sich, wenn man Symmetrien berücksichtigt. Symmetrien werden durch Gruppen modelliert.

Definition 10.2. Eine *Gruppe* ist eine Menge G mit einer Verknüpfung $\cdot : G \times G \rightarrow G$, $(x, y) \mapsto x \cdot y$, sodass gilt:

- $\forall x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (assoziativ),
- $\exists e \in G : x \cdot e = e \cdot x = x$ (neutrales Element),
- $\forall x \in G : \exists y \in G : x \cdot y = y \cdot x = e$ (inverse Elemente).

Man nennt $|G|$ die *Ordnung* von G . Im Fall $|G| < \infty$ nennt man G *endlich*. Gilt zusätzlich

- $\forall x, y \in G : x \cdot y = y \cdot x$,

so nennt man G *abelsch*.

Bemerkung 10.3. Wie üblich zeigt man, dass das neutrale Element $e \in G$ eindeutig bestimmt ist. Wir schreiben dann $e = 1_G = 1$ oder auch $e = 0$, falls die Verknüpfung $+$ ist. Außerdem besitzt $x \in G$ genau ein inverses Element, welches wir mit x^{-1} oder $-x$ bezeichnen. Es gilt dann $(x^{-1})^{-1} = x$ und $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ (Achtung!). Oft werden wir das Symbol \cdot weglassen und stattdessen xy schreiben.

Beispiel 10.4.

- Die *triviale* Gruppe $G = \{1_G\}$.
- Die ganzen Zahlen \mathbb{Z} bilden bzgl. $+$ eine abelsche Gruppe. Hingegen ist $(\mathbb{N}, +)$ *keine* Gruppe, da zum Beispiel das neutrale Element fehlt.
- Wir hatten bereits erwähnt, dass $\text{Sym}(A)$ für eine Menge A eine Gruppe bzgl. Komposition von Abbildungen ist. Für $|A| \geq 3$ ist $\text{Sym}(A)$ nichtabelsch (betrachte $(1, 2)(1, 3) = (1, 3, 2) \neq (1, 2, 3) = (1, 3)(1, 2)$ in S_3).
- Sei K ein Körper und V ein endlich-dimensionaler K -Vektorraum. Die invertierbaren linearen Abbildungen $V \rightarrow V$ bilden die *allgemeine lineare Gruppe* $\text{GL}(V)$ bzgl. Komposition von Abbildungen.
- Wir betrachten den euklidischen Raum \mathbb{R}^n mit dem Standardskalarprodukt $(x, y) := \sum_{i=1}^n x_i y_i$ für $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{R}^n$. In der linearen Algebra untersucht man die *orthogonale Gruppe*

$$O(\mathbb{R}^n) := \{f \in \text{GL}(\mathbb{R}^n) : \forall x, y \in \mathbb{R}^n : (f(x), f(y)) = (x, y)\}.$$

Die Gleichung $\|f(x)\| \sqrt{(f(x), f(x))} = \sqrt{(x, x)} = \|x\|$ bedeutet, dass $f \in O(\mathbb{R}^n)$ Längen erhält. Bekanntlich ist eine Abbildung genau dann orthogonal, wenn ihre Matrix A die Gleichung $AA^t = 1_n$ erfüllt, wobei A^t die Transponierte von A bezeichnet. Insbesondere ist $\det(A) = \pm 1$.

(vi) Sei $\Delta \subseteq \mathbb{R}^2$ ein regelmäßiges n -Eck ($n \geq 3$) mit Mittelpunkt $(0, 0)$ und sei

$$G := \{f \in O(\mathbb{R}^2) : f(\Delta) = \Delta\}.$$

Sicher ist $\text{id}_{\mathbb{R}^2} \in G$ und für $f, g \in G$ gilt $(f \circ g)(\Delta) = f(g(\Delta)) = f(\Delta) = \Delta$, also $f \circ g \in G$. Außerdem ist $f^{-1}(\Delta) = \Delta$. Dies zeigt, dass G eine Gruppe ist. Man nennt G die *Symmetriegruppe* von Δ . Da orthogonale Abbildungen Längen erhalten, muss $f \in G$ Eckpunkte von Δ auf Eckpunkte abbilden. Da zwei benachbarte Eckpunkte x und y eine Basis von \mathbb{R}^2 bilden ($n \geq 3$), ist f als lineare Abbildung durch $f(x)$ und $f(y)$ bereits eindeutig bestimmt. Wegen $\|f(x) - f(y)\| = \|f(x - y)\| = \|x - y\|$ sind auch $f(x)$ und $f(y)$ benachbarte Ecken. Es gibt somit n Möglichkeiten für $f(x)$ und anschließend noch zwei Möglichkeiten für $f(y)$. Dies impliziert $|G| \leq 2n$. Wir zeigen $|G| = 2n$. Offenbar liegen die Rotationen um $\frac{2\pi k}{n}$ für $k = 1, \dots, n$ alle in G . Ist n gerade, so besitzt G $\frac{n}{2}$ Spiegelungen durch zwei gegenüberliegende Eckpunkte und genauso viele Spiegelungen durch zwei gegenüberliegende Seitenmittelpunkte. Ist n ungerade, so besitzt G genau n Spiegelungen durch einen Eckpunkt und einen Seitenmittelpunkt. Insgesamt haben wir $2n$ Elemente gefunden. Man nennt $D_{2n} := G$ daher auch *Diedergruppe* der Ordnung $2n$. Wenn wir die Eckpunkte mit $1, \dots, n$ beschriften, so beschreibt jedes $f \in D_{2n}$ eine Permutation in S_n . Die Rotationen sind die Potenzen des n -Zyklus $(1, \dots, n)$. Für $n = 3$ erhält man S_3 .

Definition 10.5. Eine nicht-leere Teilmenge H einer Gruppe G heißt *Untergruppe*, falls $xy^{-1} \in H$ für alle $x, y \in H$. Wir schreiben dann $H \leq G$ oder $H < G$ falls $H \neq G$.

Bemerkung 10.6. Sei $H \leq G$. Dann existiert ein $x \in H$. Also ist auch $1_G = xx^{-1} \in H$ und $x^{-1} = 1_G x^{-1} \in H$. Für $x, y \in H$ ist außerdem $xy = x(y^{-1})^{-1} \in H$. Dies zeigt, dass H mit der eingeschränkten Verknüpfung selbst eine Gruppe ist.

Beispiel 10.7.

- (i) Jede Gruppe G besitzt die Untergruppen $\{1_G\}$ und G .
- (ii) Für jede Familie von Untergruppen $H_i \leq G$ ($i \in I$) ist auch $\bigcap_{i \in I} H_i \leq G$ (nachrechnen).
- (iii) Für $x \in G$ und $k \in \mathbb{Z}$ definieren wir

$$x^k := \begin{cases} 1_G & \text{falls } k = 0, \\ x \dots x \text{ (} k \text{ Faktoren)} & \text{falls } k > 0, \\ (x^{-1})^{-k} & \text{falls } k < 0. \end{cases}$$

Sicher ist dann $x^m x^n = x^{m+n}$ und $(x^m)^n = x^{mn}$ für $n, m \in \mathbb{Z}$. Außerdem ist $\langle x \rangle := \{x^k : k \in \mathbb{Z}\}$ eine Untergruppe von G wegen $x^k (x^l)^{-1} = x^{k-l} \in \langle x \rangle$. Man nennt $\langle x \rangle$ die von x erzeugte Untergruppe. Sie ist stets abelsch. Außerdem nennt man $|\langle x \rangle|$ die *Ordnung* von x .

- (iv) Für $x_1, \dots, x_n \in G$ definiert man allgemeiner

$$\langle x_1, \dots, x_n \rangle := \bigcap_{\substack{H \leq G \\ x_1, \dots, x_n \in H}} H \leq G.$$

Offenbar enthält $\langle x_1, \dots, x_n \rangle$ alle Elementen der Form $x_{i_1}^{\pm 1} \dots x_{i_k}^{\pm 1}$. Umgekehrt bilden diese Elemente selbst eine Untergruppe, die dann mit $\langle x_1, \dots, x_n \rangle$ übereinstimmen muss. Im Fall $G = \langle x_1, \dots, x_n \rangle$ nennt man x_1, \dots, x_n ein *Erzeugendensystem* von G .

- (v) Es gilt $D_{2n} \leq O(\mathbb{R}^2) \leq GL(\mathbb{R}^2) \leq \text{Sym}(\mathbb{R}^2)$. Außerdem bilden die n Rotationen in D_{2n} eine Untergruppe, die man *zyklische Gruppe* nennt und mit C_n bezeichnet. Offenbar wird C_n von der Rotation um $2\pi/n$ erzeugt. Im Allgemeinen liegen Rotationen in der *speziellen orthogonalen Gruppe*

$$SO(\mathbb{R}^n) := \{f \in O(\mathbb{R}^n) : \det(f) = 1\} = SL(\mathbb{R}^n) \cap O(\mathbb{R}^n).$$

Lemma 10.8. Für jede Gruppe G und $x \in G$ gilt

$$|\langle x \rangle| = \inf\{n \in \mathbb{N} : x^n = 1_G\}$$

mit der Konvention $\inf \emptyset = \infty$.

Beweis. Sei zunächst $n \in \mathbb{N}$ minimal mit $x^n = 1$. Für $k \in \mathbb{Z}$ existieren $q \in \mathbb{Z}$ und $r \in \mathbb{N}_0$ mit $k = qn + r$ und $0 \leq r < n$ (Division mit Rest). Dann ist $x^k = x^{qn+r} = (x^n)^q x^r = 1^q x^r = x^r$ und es folgt $\langle x \rangle = \{1, x, x^2, \dots, x^{n-1}\}$. Nehmen wir an es existieren $0 \leq k < l < n$ mit $x^k = x^l$. Dann $x^{l-k} = 1$ mit $1 \leq l-k < n$ im Widerspruch zur Wahl von n . Dies zeigt $|\langle x \rangle| = n$.

Sei nun $x^n \neq 1$ für alle $n \in \mathbb{N}$. Für $1 \leq k < l$ ist dann $x^k \neq x^l$, denn anderenfalls wäre $x^{l-k} = 1$. Dies zeigt, dass die Elemente x, x^2, \dots paarweise verschieden sind. Insbesondere ist $|\langle x \rangle| = \infty$. \square

Definition 10.9. Eine *Operation* einer Gruppe G auf einer Menge Ω ist eine Abbildung $G \times \Omega \rightarrow \Omega$, $(g, \omega) \mapsto {}^g\omega$ mit folgenden Eigenschaften:

- $\forall \omega \in \Omega : {}^1\omega = \omega$,
- $\forall g, h \in G \forall \omega \in \Omega : {}^g({}^h\omega) = {}^{gh}\omega$.

Für $\omega \in \Omega$ nennt man $G_\omega := \{g \in G\}$ die *Bahn* von ω und $G_\omega := \{g \in G : {}^g\omega = \omega\}$ den *Stabilisator* von ω in G . Existiert nur eine Bahn, so heißt die Operation *transitiv*. Man nennt $|G_\omega|$ die *Länge* der Bahn.

Beispiel 10.10.

- (i) Für jede Menge A operiert $G := \text{Sym}(A)$ auf A durch ${}^\sigma a := \sigma(a)$, denn $\text{id}(a) = a$ und ${}^{\sigma(\tau)} a = \sigma(\tau(a)) = (\sigma\tau)(a) = {}^{\sigma\tau} a$ für $a \in A$ und $\sigma, \tau \in G$. Diese Operation ist transitiv, denn für verschiedene $a, b \in A$ liegt die Transposition (a, b) in G und ${}^{(a,b)} a = b$. Dies zeigt ${}^G a = A$ für alle $a \in A$. Die Länge eines Zyklus $\sigma \in \text{Sym}(A)$ ist gleichzeitig die Länge einer Bahn von $\langle \sigma \rangle$.
- (ii) Für jeden K -Vektorraum V operiert $G := GL(V)$ auf V durch ${}^f v := f(v)$ für $f \in GL(V)$ und $v \in V$. Dies folgt aus (i) wegen $G \leq \text{Sym}(V)$. Die Bahn des Nullvektors ist ${}^G 0 = \{0\}$. Insbesondere ist die Operation nur transitiv, falls $V = \{0\}$.
- (iii) Die Gruppen $D_{2n} \leq O(\mathbb{R}^n) \leq GL(\mathbb{R}^n)$ operieren auf \mathbb{R}^n . Die Operation von D_{2n} kann man auf das regelmäßige n -Eck Δ einschränken. Weiter operiert D_{2n} transitiv auf der Menge der Eckpunkte von Δ .

Bemerkung 10.11.

- (i) In der Situation von Definition 10.9 gilt $1 \in G_\omega \neq \emptyset$ und für $x, y \in G_\omega$ ist

$$xy^{-1}\omega = x(y^{-1}\omega) = x(y^{-1}(y\omega)) = x(y^{-1}y\omega) = x(1\omega) = x\omega = \omega.$$

Dies zeigt $xy^{-1} \in G_\omega$ und G_ω ist eine Untergruppe von G .

(ii) Für $g \in G$ ist die Abbildung $\omega \mapsto {}^g\omega$ eine Bijektion auf Ω mit Umkehrabbildung $\omega \mapsto {}^{g^{-1}}\omega$, denn $g({}^{g^{-1}}\omega) = {}^{gg^{-1}}\omega = {}^1\omega = \omega = \dots = {}^{g^{-1}}(g\omega)$. Daher bestimmt jedes g eine Permutation in $\text{Sym}(\Omega)$.

(iii) Wir zeigen, dass

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

eine Äquivalenzrelation auf Ω definiert. Wegen ${}^1\alpha = \alpha$ ist \sim reflexiv. Aus ${}^g\alpha = \beta$ folgt ${}^{g^{-1}}\beta = {}^{g^{-1}}({}^g\alpha) = {}^{g^{-1}g}\alpha = {}^1\alpha = \alpha$. Also ist \sim symmetrisch. Sei schließlich ${}^g\alpha = \beta$ und ${}^h\beta = \gamma$ für $g, h \in G$ und $\alpha, \beta, \gamma \in \Omega$. Dann ist ${}^{hg}\alpha = {}^h({}^g\alpha) = {}^h\beta = \gamma$. Daher ist \sim transitiv und eine Äquivalenzrelation. Die Äquivalenzklassen sind genau die Bahnen. Insbesondere bilden die Bahnen eine Partition von Ω .

(iv) Sei $H \leq G$. Dann operiert H auf G durch ${}^hx := xh^{-1}$ für $h \in H$ und $x \in G$, denn ${}^1x = x1^{-1} = x$ und ${}^g({}^hx) = {}^g(xh^{-1}) = (xh^{-1})g^{-1} = x(h^{-1}g^{-1}) = x(gh)^{-1} = {}^{gh}x$ für $g, h \in H$. Die Bahnen haben die Form $xH := \{xh : h \in H\}$ für $x \in G$. Man nennt sie *Linksnebenklassen*. Sei $G/H := \{xH : x \in G\}$ und $|G : H| := |G/H|$. Man nennt $|G : H|$ den *Index* von H in G .

Satz 10.12 (LAGRANGE). Für $H \leq G$ gilt $|G| = |G : H| |H|$. Insbesondere sind $|H|$ und $|G : H|$ Teiler von $|G|$, falls $|G| < \infty$.

Beweis. Für $x \in G$ ist die Abbildung $H \rightarrow xH, h \mapsto xh$ bijektiv mit Umkehrabbildung $g \mapsto x^{-1}g$. Also haben alle Linksnebenklassen von H die Mächtigkeit $|H|$. Die Behauptung folgt, da G die disjunkte Vereinigung der Linksnebenklassen ist. \square

Lemma 10.13. Für $H \leq G$ und $x, y \in G$ gilt $xH = yH \iff y^{-1}x \in H$.

Beweis.

$$\begin{aligned} xH = yH &\iff xH \cap yH \neq \emptyset \iff \exists h, k \in H : xh = yk \\ &\iff \exists h, k \in H : y^{-1}x = kh^{-1} \iff y^{-1}x \in H. \end{aligned} \quad \square$$

Satz 10.14 (Bahn-Stabilisator-Satz). Für jede Operation von G auf einer Menge Ω gilt

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

für alle $\omega \in \Omega$.

Beweis. Es genügt zu zeigen, dass die Abbildung $F : G/G_\omega \rightarrow {}^G\omega, xG_\omega \mapsto x\omega$ eine Bijektion ist. Wegen

$$xG_\omega = yG_\omega \stackrel{10.13}{\iff} y^{-1}x \in G_\omega \iff y^{-1}x\omega = \omega \iff x\omega = y\omega$$

für $x, y \in G$ ist F wohldefiniert und injektiv. Die Surjektivität folgt aus der Definition der Bahn. \square

Bemerkung 10.15.

(i) Satz 10.14 und Lagrange zeigen, dass die Bahnenlängen stets Teiler der Gruppenordnung sind, falls $|G| < \infty$.

(ii) Ist Δ ein Repräsentantensystem für die Bahnen von G auf Ω , so erhält man die *Bahngleichung*

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

- (iii) Sei $|G| = 77$ und $|\Omega| = 23$. Nach der Bahnengleichung existieren $a, b, c \in \mathbb{N}_0$ mit $23 = a + 7b + 11c$. Es folgt $a > 0$, d. h. G hat stets einen Fixpunkt auf Ω .
- (iv) Man kann den Satz von Lucas mit Gruppenoperationen beweisen: Wir zerlegen $N := \{1, \dots, n\}$ in eine Partition der Form

$$N = \bigcup_{i \geq 0} \bigcup_{j=1}^{n_i} A_{ij}$$

mit $|A_{ij}| = p^i$ für $j = 1, \dots, n_i$. Für $A_{ij} = \{\alpha_1, \dots, \alpha_{p^i}\}$ sei $G_{ij} := \langle (\alpha_1, \dots, \alpha_{p^i}) \rangle$. Dann ist

$$G := \prod_{i \geq 0} \prod_{j=1}^{n_i} G_{ij} \leq S_n$$

eine p -Gruppe, die auf N operiert. Sicher operiert G auch auf $\binom{N}{k}$. Die Bahnenlängen sind nach Satz 10.14 stets p -Potenzen. Daher ist die Anzahl der Fixpunkte von G auf $\binom{N}{k}$ kongruent zu $\binom{n}{k}$ modulo p . Eine Teilmenge $K = \{\beta_1, \dots, \beta_k\} \subseteq N$ ist genau dann ein Fixpunkt unter G , wenn K die Vereinigung von gewissen A_{ij} ist. Für jedes $i \geq 0$ muss man genau k_i der Mengen A_{i1}, \dots, A_{in_i} auswählen. Die Anzahl der Fixpunkte ist daher $\prod_{i \geq 0} \binom{n_i}{k_i}$.

Satz 10.16 (BURNSIDES Lemma). *Sei G eine endliche Gruppe, die auf einer Menge Ω operiert. Für $g \in G$ sei $f(g) := |\{\omega \in \Omega : g \in G_\omega\}|$ die Anzahl der Fixpunkte von g auf Ω . Dann ist*

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

die Anzahl der Bahnen von G auf Ω .

Beweis. Liegen $\alpha, \beta \in \Omega$ in der gleichen Bahn, so gilt $|G : G_\alpha| = |G_\alpha| = |G_\beta| = |G : G_\beta|$. Nach Lagrange folgt $|G_\alpha| = |G_\beta|$ (beachte: $|G| < \infty$). Sei $\Delta \subseteq \Omega$ ein Repräsentantensystem für die Bahnen von G auf Ω . Dann gilt

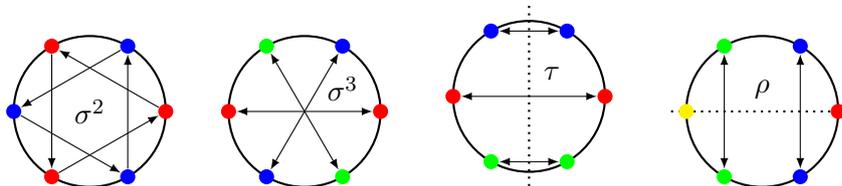
$$\begin{aligned} \sum_{g \in G} f(g) &= |\{(g, \omega) \in G \times \Omega : g\omega = \omega\}| = \sum_{\omega \in \Omega} |G_\omega| = \sum_{\delta \in \Delta} |G_\delta| |G_\delta| \\ &= \sum_{\delta \in \Delta} |G : G_\delta| |G_\delta| = \sum_{\delta \in \Delta} |G| = |\Delta| |G|. \end{aligned}$$

Dies zeigt die Behauptung. □

Beispiel 10.17.

- (i) Sei G eine endliche Gruppe, die transitiv auf Ω mit $|\Omega| > 1$ operiert. Nach Burnsid's Lemma ist 1 die durchschnittliche Anzahl an Fixpunkten von Elementen aus G . Andererseits gilt $f(1) = |\Omega| > 1$. Es muss daher stets fixpunktfreie Elemente in G geben. Dies verallgemeinert Satz 2.2.
- (ii) Wir wollen Halsketten mit sechs Perlen zählen, wobei Perlen in drei Farben zur Verfügung stehen. Naiverweise gibt es zunächst 3^6 solche Halsketten, von denen jedoch einige identisch sind. Wir ordnen die Halskette so an, dass die Perlen ein regelmäßiges 6-Eck bilden. Rotation um $\pi/3$ wird die Halsketten nicht verändern. Ebenso können wir die Halskette im Raum drehen und dadurch eine Spiegelung der 6 Eckpunkte realisieren. Zwei Halsketten sind also genau dann identisch, wenn sie in der gleichen Bahn unter $G := D_{12}$ liegen. Wir wenden Burnsid's Lemma auf die Menge Ω der 3^6 Halsketten an.

Sicher ist $f(1) = 3^6$. Eine Drehung $\sigma \in G$ um $\pi/3$ lässt nur die drei einfarbigen Halsketten fest, d. h. $f(\sigma) = 3$. Die Drehung σ^2 um $2\pi/3$ lässt die einfarbigen Halsketten und die Halsketten mit alternierenden Farben fest. Davon gibt es $f(\sigma^2) = 3^2$ Stück. Analog zeigt man $f(\sigma^3) = 3^3$. Außerdem ist $f(\sigma^4) = f(\sigma^{-2}) = 3^2$, $f(\sigma^5) = f(\sigma^{-1}) = 3$ sowie $\sigma^6 = 1$. Sei nun τ eine der drei Spiegelungen durch zwei Seitenmittelpunkte. Dann ist $f(\tau) = 3^3$. Sei schließlich ρ eine der drei Spiegelungen durch zwei Eckpunkte. Dann ist $f(\rho) = 3^4$.



Nach Burnsid's Lemma gibt es

$$\frac{1}{12}(3^6 + 2 \cdot 3 + 2 \cdot 3^2 + 3^3 + 3 \cdot 3^3 + 3 \cdot 3^4) = \frac{1}{4}(3^4(3 + 1) + 3^2(1 + 3) + 2 + 6) = 81 + 9 + 2 = 92$$

verschiedene Halsketten.

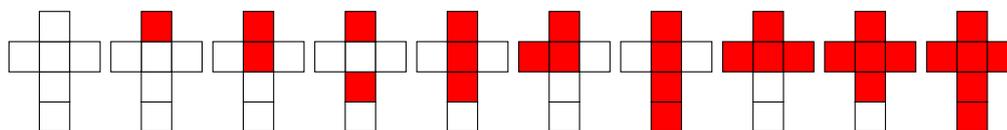
- (iii) Auf wie viele Weisen kann man die sechs Flächen eines Würfels $W \subseteq \mathbb{R}^3$ färben, wenn n Farben zur Verfügung stehen? Naiv: n^6 . Drehungen im Raum verändern W nicht wesentlich. Spiegelungen aber schon. Wir suchen daher die Anzahl der Bahnen unter der Drehgruppe von W (als Untergruppe von $SO(\mathbb{R}^3)$).

Drehachse	Winkel	Anzahl Drehungen	Anzahl Fixpunkte
gegenüberliegende Seitenmittelpunkte	0°	1	n^6
gegenüberliegende Seitenmittelpunkte	$\pm 90^\circ$	6	n^3
gegenüberliegende Seitenmittelpunkte	180°	3	n^4
gegenüberliegende Kantenmittelpunkte	180°	6	n^3
Raumdiagonale	$\pm 120^\circ$	8	n^2
24			

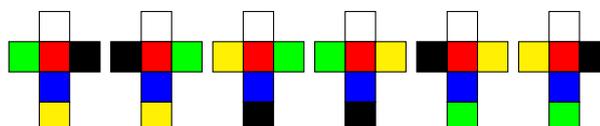
Nach Burnsid's Lemma ist die Anzahl der gefärbten Würfel gegeben durch

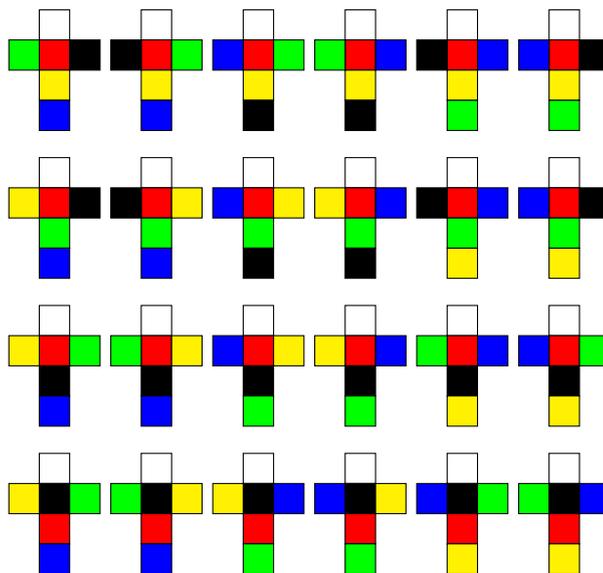
$$\frac{1}{24}(n^6 + 6n^3 + 3n^4 + 6n^3 + 8n^2) = \frac{n^2}{24}(n^4 + 3n^2 + 12n + 8).$$

Für $n = 2$ erhält man folgende zehn Würfel:



Möchte man nur Würfel mit paarweise verschiedenen Seitenfarben, so hat man zunächst $n(n-1) \dots (n-5)$ Möglichkeiten (Variationen ohne Wiederholung). Da nun jede nicht-triviale Drehung fixpunktfrei ist, vereinfacht sich Burnsid's Lemma zu $\frac{1}{24}n(n-1) \dots (n-5)$. Für $n = 6$ erhält man die 30 MACMAHON-Würfel:





(iv) Es gibt

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

Zustände des $3 \times 3 \times 3$ -Zauberwürfels, von denen sich aber viele durch räumliche Drehung und Spiegelung ineinander überführen lassen. Mit Burnsidess Lemma reduziert sich die Anzahl auf

$$901.083.404.981.813.616$$

wesentlich verschiedene Zustände.⁶ Damit konnte man 2010 zeigen, dass sich jeder Zustand durch höchstens 20 „Züge“ lösen lässt (*god's number*, siehe <https://cube20.org/>).

(v) Mit Burnsidess Lemma kann man auch zeigen, dass es

$$5.472.730.538$$

wesentlich verschiedene (ausgefüllte) 9×9 -Sudokus gibt.⁷

Bemerkung 10.18. Im Folgenden verfeinern wir Burnsidess Lemma, um zum Beispiel Halsketten mit bestimmtem *Wert* zu zählen (die Perlenfarben sollen dabei nicht mehr unbedingt gleichwertig sein). Dafür betrachten wir eine Operation von G auf Ω und eine weitere endliche Menge Δ . Dann operiert G auf $\Delta^\Omega = \{f: \Omega \rightarrow \Delta\}$ durch $(g f)(\omega) := f(g^{-1}\omega)$ für $g \in G$, $\omega \in \Omega$ und $f \in \Delta^\Omega$, denn $({}^1 f)(\omega) = f(\omega)$ und

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

für $g, h \in G$. Für eine *Gewichtsfunktion* $w: \Delta \rightarrow \mathbb{N}_0$ definieren wir $w_i := |w^{-1}(i)|$ für $i \in \mathbb{N}_0$ und

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

Schließlich sei

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

⁶siehe [Sambale, Endliche Permutationsgruppen, Springer, 2017]

⁷siehe [Russell-Jarvis, Mathematics of Sudoku II, Mathematical Spectrum 39 (2006), 54–58]

Wegen

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

für $g \in G$ operiert G auch auf $(\Delta^\Omega)_k$. Schließlich sei $(1^{z_1(g)}, 2^{z_2(g)}, \dots)$ der Zyklentyp von g als Element von $\text{Sym}(\Omega)$.

Satz 10.19 (PÓLYA). *Mit den Bezeichnungen aus Bemerkung 10.18 ist die Anzahl der Bahnen von G auf $(\Delta^\Omega)_k$ der Koeffizient von X^k in*

$$\frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{\infty} W(X^i)^{z_i(g)}. \quad (10.1)$$

Beweis. Sei $f_k(g)$ die Anzahl der Fixpunkte von $g \in G$ auf $(\Delta^\Omega)_k$. Nach Burnsid's Lemma müssen wir zeigen, dass

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

mit (10.1) übereinstimmt. Es genügt also

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

für $g \in G$ zu beweisen. Hat g Zyklentyp (l_1, \dots, l_s) (d. h. Zyklen der Länge l_1, l_2, \dots, l_s), so gilt

$$\prod_{i=1}^{\infty} W(X^i)^{z_i(g)} = \prod_{i=1}^s (w_0 + w_1 X^{l_i} + w_2 X^{2l_i} + \dots).$$

Jeder Fixpunkt $f \in (\Delta^\Omega)_k$ von g ist konstant auf den Zyklen von g . Für den l_i -Zyklus σ von g gibt es $|\Delta|$ Möglichkeiten für die Belegung von f auf den Ziffern von σ . Genau w_j von diesen Möglichkeiten tragen jl_i zu k bei. Die Behauptung folgt. \square

Beispiel 10.20.

- (i) Wir betrachten noch einmal die Halsketten mit sechs Perlen aus drei Farben (rot, blau und grün). Die roten Perlen seien 3€ wert, die blauen 2€ und die grünen 1€ . Wie viele Halsketten im Wert von 12€ kann man herstellen? Sei $\Omega := \{1, \dots, 6\}$, $\Delta := \{r, b, g\}$ und $w(r) := 3$, $w(b) := 2$ und $w(g) := 1$. Dann ist $W(X) = X + X^2 + X^3$ und wir suchen die Anzahl der Bahnen von $G := D_{12}$ auf $(\Delta^\Omega)_{12}$. Das triviale Element von G hat Zyklentyp (1^6) . Die Rotation σ um $\pi/3$ hat Zyklentyp (6^1) . Analog erhält man $z_3(\sigma^2) = 2 = z_3(\sigma^4)$ und $z_2(\sigma^3) = 3$. Für die Spiegelungen $\tau \in G$ durch Seitenmittelpunkte ist $z_2(\tau) = 3$ und die verbleibenden drei Spiegelungen durch Eckpunkte haben Zyklentyp $(1^2, 2^2)$. Gleichung 10.1 hat nun die Form

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

Es gibt also 18 Halsketten im Wert von 12€ .

- (ii) Pólya hat mit Satz 10.19 die Anzahl von Isomeren von Alkoholen und Paraffinen bestimmt.

Definition 10.21. Zwei Gruppen G und H heißen *isomorph*, falls eine Bijektion $f: G \rightarrow H$ mit $f(xy) = f(x)f(y)$ für alle $x, y \in G$ existiert. Wir schreiben dann $G \cong H$.

Bemerkung 10.22. Offenbar ist die Isomorphie von Gruppen eine Äquivalenzrelation. Die Äquivalenzklassen heißen *Isomorphieklassen*. Isomorphe Gruppen G und H unterscheiden sich nur durch die Benennung ihrer Elemente. Insbesondere haben G und H die gleichen Eigenschaften (z. B. $|G| = |H|$, G abelsch $\iff H$ abelsch usw.).

Definition 10.23. Sei $g(n)$ die Anzahl der Isomorphieklassen von Gruppen der Ordnung n .

Bemerkung 10.24. Da jede Gruppe der Ordnung n durch ihre Multiplikationstabelle eindeutig bestimmt ist, gilt $g(n) \leq n^{n^2} < \infty$. Die Existenz zyklischer Gruppen zeigt $g(n) \geq 1$ für alle $n \in \mathbb{N}$.

Beispiel 10.25.

(i) Sei G eine Gruppe mit Primzahlordnung $p = |G|$ und sei $x \in G \setminus \{1\}$. Dann ist $|\langle x \rangle| > 1$ und Lagrange zeigt $G = \langle x \rangle$. Nach Lemma 10.8 gilt $G = \{1, x, \dots, x^{p-1}\}$. Wegen $x^i x^j = x^{i+j \pmod p}$ ist die Multiplikationstabelle von G bereits eindeutig bestimmt. Man erhält einen Isomorphismus $G \cong C_p$, indem man x^k auf die Drehung um $2\pi k/p$ abbildet. Daher ist C_p bis auf Isomorphie die einzige Gruppe der Ordnung p , d. h. $g(p) = 1$.

(ii) Sei G eine Gruppe mit vier Elementen. Existiert ein $x \in G$ mit $G = \langle x \rangle$, so gilt wieder $G \cong C_4$. Nach Lagrange können wir also $x^2 = 1$ für alle $x \in G$ annehmen. Dann ist $x = x^{-1}$ für alle $x \in G$. Es folgt

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

für $x, y \in G$, d. h. G ist abelsch. Offenbar hat G die Form $G = \{1, x, y, xy\}$ für gewisse $x, y \in G$. Die Multiplikationstabelle ist dadurch eindeutig festgelegt und G ist isomorph zur *Kleinschen Vierergruppe*

$$V_4 := \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \leq S_4.$$

Insbesondere ist $g(4) = 2$. Man findet V_4 auch als Untergruppe von D_8 wieder:

$$\begin{array}{c} 1 \text{ --- } 4 \\ \vdots \\ \dots \vdots \dots \vdots \dots \\ 2 \text{ --- } 3 \\ \vdots \end{array}$$

Satz 10.26. *Es gilt*

$$g(n) \leq \binom{[n!/e]}{\lambda(n)} \leq n^{n\lambda(n)} \leq n^{n \log_2(n)},$$

wobei $\lambda(n)$ die Anzahl der Primfaktoren von $n \in \mathbb{N}$ mit Vielfachheiten ist.

Beweis. Nach Beispiel 10.25 dürfen wir $n \geq 4$ annehmen. Sei G eine Gruppe der Ordnung n und sei $x_1, \dots, x_d \in G$ ein minimales Erzeugendensystem von G , d. h. G lässt sich nicht mit $d - 1$ Elementen erzeugen. Insbesondere ist $x_i \neq 1$ für $i = 1, \dots, d$. Durch ${}^g x := gx$ für $g, x \in G$ operiert G auf sich selbst. Insbesondere bestimmt jedes $g \in G$ ein Element $f_g \in \text{Sym}(G)$ mit $f_g(x) = gx$ (Bemerkung 10.11(ii)). Da sich jedes Element in G als Produkt der x_i schreiben lässt, ist der Isomorphietyp von G bereits

durch f_{x_1}, \dots, f_{x_d} eindeutig bestimmt. Für $g \in G$ ist $f_{x_i}(g) = x_i g \neq g$, d. h. f_{x_i} ist fixpunktfrei. Wegen $f_{x_i}(1) = x_i$ sind f_{x_1}, \dots, f_{x_d} paarweise verschieden. Nach Satz 2.2 gibt es also höchstens

$$\binom{[n!/e]}{d}$$

Möglichkeiten für G . Sei nun $H_i := \langle x_1, \dots, x_i \rangle$ für $i = 1, \dots, d$. Es gilt dann $1 < H_1 < \dots < H_d = G$, denn anderenfalls könnte man G mit weniger als d Elementen erzeugen. Nach Lagrange ist

$$n = |G| = |H_d : H_{d-1}| |H_{d-1} : H_{d-2}| \dots |H_1|$$

und es folgt $d \leq \lambda(n)$. Da jeder Primteiler von n mindestens 2 ist, gilt außerdem $\lambda(n) \leq \log_2(n) \leq \frac{[n!/e]}{2}$ wegen $n \geq 4$. Dies zeigt

$$g(n) \leq \binom{[n!/e]}{d} \stackrel{\text{Aufgabe 3}}{\leq} \binom{[n!/e]}{\lambda(n)} \leq (n!)^{\lambda(n)} \leq (n^n)^{\lambda(n)} = n^{n\lambda(n)} \leq n^{n \log_2(n)}. \quad \square$$

Beispiel 10.27. Es gilt

$$g(6) \leq \binom{[720/e]}{\lambda(6)} = \binom{265}{2} = 34.980.$$

Tatsächlich gibt es nur zwei Gruppen der Ordnung 6 bis auf Isomorphie, nämlich C_6 und S_3 (ohne Beweis). Andererseits $g(2^{10}) = 49.487.365.422$ und $g(2^{11})$ ist unbekannt. Über 99% aller Gruppen der Ordnung ≤ 2000 haben Ordnung $2^{10} = 1024$ (siehe <https://oeis.org/A000001>). Die Anzahl der abelschen Gruppen der Ordnung 2^{10} ist nur $p(10) = 42$. Dies folgt aus dem Hauptsatz über endliche abelsche Gruppen (siehe Algebra 1).

Bemerkung 10.28.

- (i) Jede Gruppe G operiert auf sich selbst durch *Konjugation*, d. h. ${}^g x := gxg^{-1}$ für $g, x \in G$, denn ${}^1 x = 1x1^{-1} = x$ und ${}^{g(h)} x = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = {}^{gh} x$ für $g, h, x \in G$. Man nennt den Stabilisator von $x \in G$ dann *Zentralisator* und schreibt dafür $C_G(x) := \{g \in G : gx = xg\}$. Die Bahnen heißen *Konjugationsklassen* von G und deren Anzahl $k(G)$ heißt *Klassenzahl* von G . Sicher ist $k(G) \leq |G|$. Die Bahngleichung wird zur *Klassengleichung*

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

wobei R ein Repräsentantensystem für die Konjugationsklassen von G ist.

- (ii) Sei Ω eine Menge, auf der G operiert. Für $\omega \in \Omega$ und $g, x \in G$ gilt

$$x\omega = \omega \iff {}^{xg} \omega = g\omega.$$

Daher ist die Abbildung $\omega \mapsto {}^g \omega$ eine Bijektion zwischen der Menge der Fixpunkte von x und der Menge der Fixpunkte von xg . Insbesondere haben konjugierte Elemente die gleiche Anzahl an Fixpunkten auf Ω . Man braucht in Burnside's Lemma daher nur über ein Repräsentantensystem R der Konjugationsklassen von G zu summieren, d. h.

$$\frac{1}{|G|} \sum_{x \in R} |G : C_G(x)| f(x) = \sum_{x \in R} \frac{f(x)}{|C_G(x)|}$$

ist die Anzahl der Bahnen von G auf Ω .

Lemma 10.29. Genau dann ist eine endliche Gruppe G abelsch, falls $k(G) = |G|$ gilt.

Beweis. Ist G abelsch und $g, x \in G$, so gilt ${}^g x = gxg^{-1} = gg^{-1}x = x$, d. h. jede Konjugationsklasse hat nur ein Element. Dies zeigt $k(G) = |G|$. Ist umgekehrt $k(G) = |G|$, so gilt $\{x\} = {}^G x = \{gxg^{-1} : g \in G\}$ für alle $x \in G$. Dies zeigt, dass G abelsch ist. \square

Satz 10.30 (LANDAU). Bis auf Isomorphie gibt es nur endlich viele endliche Gruppen mit vorgegebener Klassenzahl.

Beweis. Sei G eine endliche Gruppe mit Klassenzahl k und sei $x_1, \dots, x_k \in G$ ein Repräsentantensystem für die Konjugationsklassen von G mit $x_k = 1_G$. Sei $n_i := |C_G(x_i)|$ für $i = 1, \dots, k$. O. B. d. A. sei $n_1 \leq \dots \leq n_k = |G|$. Die Klassengleichung zeigt

$$1 = \frac{1}{n_1} + \dots + \frac{1}{n_k} \leq \frac{k}{n_1}$$

und $n_1 \leq k$. Insbesondere gibt es nur endlich viele Möglichkeiten für n_1 . Nun ist

$$\frac{n_1 - 1}{n_1} = \frac{1}{n_2} + \dots + \frac{1}{n_k} \leq \frac{k - 1}{n_2}$$

und $n_2 \leq \frac{n_1(k-1)}{n_1-1}$. Also gibt es auch nur endlich viele Möglichkeiten für n_2 . Fährt man auf diese Weise fort, so sieht man, dass es nur endlich viele Möglichkeiten für $n_k = |G|$ gibt. Die Behauptung folgt nun aus Bemerkung 10.24. \square

Bemerkung 10.31. Erdős und Turán haben gezeigt, dass $|G| < 2^{2^{k(G)}}$ gilt.

Beispiel 10.32. Eine Gruppe mit Klassenzahl 1 ist trivial, denn $\{1_G\}$ ist stets eine Konjugationsklasse. Sei nun $k(G) = 2$. Wie in Satz 10.30 ist $n_1 \leq 2$ und es gibt nur die Lösung $n_1 = 2 = n_2 = |G|$. Es gilt dann $G \cong C_2$. Schließlich nehmen wir $k(G) = 3$ an. Im Fall $n_1 = 3$ ist $n_1 \leq n_2 \leq 3$ wie in Satz 10.30. Dies führt zu $n_1 = n_2 = n_3 = 3 = |G|$ und $G \cong C_3$ nach Beispiel 10.25. Es verbleibt der Fall $n_1 = 2$. Hier ist $n_2 \leq 4$ und man hat die Lösungen $(n_1, n_2, n_3) \in \{(2, 3, 6), (2, 4, 4)\}$. Die Möglichkeit $n_2 = 4 = |G|$ ist ausgeschlossen, denn dann wäre G abelsch (Beispiel 10.25) und hätte vier Konjugationsklassen nach Lemma 10.29. Die erste Möglichkeit führt zu $G \cong S_3$. Es gibt daher genau zwei Gruppen mit Klassenzahl 3 (bis auf Isomorphie). Man kennt alle Gruppen mit Klassenzahl ≤ 14 (siehe <https://oeis.org/A073043>).

Satz 10.33. Für $n \in \mathbb{N}$ ist $k(S_n) = p(n)$ (Anzahl der Partitionen von n). Insbesondere ist $p(n) \leq n!$.

Beweis. Es genügt zu zeigen, dass die Permutationen mit einem vorgegebenen Zyklentyp eine Konjugationsklasse von S_n bilden. Sei $\sigma = (a_1, a_2, \dots)(b_1, b_2, \dots) \dots \in S_n$ ein Produkt paarweise disjunkter Zyklen und $\tau \in S_n$ beliebig. Dann ist

$$\tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \dots)(\tau(b_1), \tau(b_2), \dots) \dots$$

Da τ injektiv ist, sind auch die Zyklen $(\tau(a_1), \tau(a_2), \dots), (\tau(b_1), \tau(b_2), \dots), \dots$ paarweise disjunkt. Insbesondere haben σ und $\tau\sigma\tau^{-1}$ den gleichen Zyklentyp.

Sei umgekehrt $\sigma' = (a'_1, a'_2, \dots)(b'_1, b'_2, \dots) \dots \in S_n$ eine Permutation mit dem gleichen Zyklentyp wie σ . Für

$$\tau := \begin{pmatrix} a_1 & a_2 & \dots & b_1 & b_2 & \dots \\ a'_1 & a'_2 & \dots & b'_1 & b'_2 & \dots \end{pmatrix}$$

gilt dann $\tau\sigma\tau^{-1} = \sigma'$. Dies zeigt die Behauptung. \square

Beispiel 10.34. Die Konjugationsklassen von S_5 werden durch 1 , $(1, 2)$, $(1, 2, 3)$, $(1, 2, 3, 4)$, $(1, 2, 3, 4, 5)$, $(1, 2)(3, 4)$ und $(1, 2)(2, 3, 4)$ repräsentiert ($p(5) = 7$).

Bemerkung 10.35. Eine Gruppe G operiert auch durch Konjugation auf der Menge aller Untergruppen mittels $gHg^{-1} := \{ghg^{-1} : h \in H\}$ für $g \in G$ und $H \leq G$. Wir schreiben $H \sim K$, falls $H, K \leq G$ konjugiert sind. Der Stabilisator von H ist der *Normalisator* $N_G(H) := \{g \in G : gHg^{-1} = H\}$. Nach dem Bahn-Stabilisator-Satz ist $|G : N_G(H)|$ die Länge der Konjugationsklasse von H .

Satz 10.36. Sei G eine endliche Gruppe, die auf einer Menge Ω operiert. Für $H \leq G$ sei $f(H) := |\{\omega \in \Omega : H \leq G_\omega\}|$ die Anzahl der Fixpunkte von H auf Ω . Sei μ die Möbius-Funktion auf der Menge aller Untergruppen von G (geordnet durch \subseteq). Dann ist

$$\frac{1}{|G|} \sum_{H \leq G} \mu(1, H) f(H)$$

die Anzahl der Bahnen von G auf Ω mit Länge $|G|$.

Beweis. Für $g \in G$ und $\omega \in \Omega$ gilt

$$x \in gG_\omega g^{-1} \iff g^{-1}xg \in G_\omega \iff g^{-1}xg\omega = \omega \iff xg\omega = g\omega \iff x \in G_{g\omega},$$

d. h. $gG_\omega g^{-1} = G_{g\omega}$. Jede Bahn von G auf Ω bestimmt daher eine Konjugationsklasse von Stabilisatoren. Für $H \leq G$ sei $\rho(H)$ die Anzahl der Bahnen, deren Stabilisatoren zu H konjugiert sind. Die Länge dieser Bahnen ist $|G : H|$. Nun gilt

$$\begin{aligned} f(H) &= \sum_{\substack{\omega \in \Omega \\ H \leq G_\omega}} 1 = \sum_{K \geq H} \sum_{\substack{\omega \in \Omega \\ G_\omega = K}} 1 = \sum_{K \geq H} \frac{1}{|G : N_G(K)|} \sum_{\substack{\omega \in \Omega \\ G_\omega \sim K}} 1 \\ &= \sum_{K \geq H} \frac{|G : K|}{|G : N_G(K)|} \rho(H) = \sum_{K \geq H} |N_G(K) : K| \rho(K). \end{aligned}$$

Möbius-Inversion liefert

$$|N_G(H) : H| \rho(H) = \sum_{K \geq H} \mu(H, K) f(K).$$

Die Behauptung folgt aus dem Spezialfall $H = 1$. □

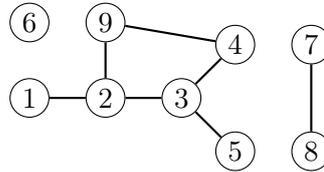
11. Graphen

Definition 11.1. Ein *Graph* $\Omega = (\Omega_E, \Omega_K)$ der *Ordnung* $n \in \mathbb{N}$ besteht aus einer n -elementigen Menge Ω_E von *Ecken* und einer Menge $\Omega_K \subseteq \binom{\Omega_E}{2}$ von *Kanten*. Wir setzen $|\Omega| := |\Omega_E| = n$. Ecken $\alpha, \beta \in \Omega_E$ heißen *benachbart*, wenn $\{\alpha, \beta\} \in \Omega_K$. Der *Grad* einer Ecke ist die Anzahl ihrer benachbarten Ecken. Allgemeiner nennt man Ecken $\alpha, \beta \in \Omega_E$ *verbunden*, falls ein *Weg* $\alpha = \alpha_1, \dots, \alpha_m = \beta \in \Omega_E$ mit $\{\alpha_i, \alpha_{i+1}\} \in \Omega_K$ für $i = 1, \dots, m-1$ existiert. Dies beschreibt eine Partition auf Ω_E , deren Teile man (*Zusammenhangs*)*komponenten* von Ω nennt. Gibt es nur eine Komponente, so heißt Ω *zusammenhängend* und anderenfalls *unzusammenhängend*.

Bemerkung 11.2. Wie üblich werden wir Graphen durch Diagramme veranschaulichen und dabei die Ecken mit natürlichen Zahlen nummerieren.

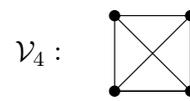
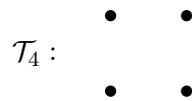
Beispiel 11.3.

(i) Die Komponenten von

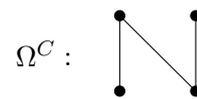
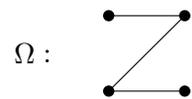


sind $\{1, 2, 3, 4, 5, 9\}$, $\{6\}$ und $\{7, 8\}$.

(ii) Der *triviale* Graph $\mathcal{T}_n := (\{1, \dots, n\}, \emptyset)$ ohne Kanten und der *vollständige* Graph $\mathcal{V}_n := (\{1, \dots, n\}, \binom{\{1, \dots, n\}}{2})$ der Ordnung $n \in \mathbb{N}$.



(iii) Für jeden Graphen Ω existiert der *komplementäre* Graph $\Omega^C = (\Omega_E, \binom{\Omega_E}{2} \setminus \Omega_K)$. Eine Ecke in Ω vom Grad k entspricht einer Ecke in Ω^C vom Grad $|\Omega| - k - 1$. Offenbar ist $\mathcal{T}_n = \mathcal{V}_n^C$.



(iv) Für Graphen Ω und Δ ist auch die (*disjunkte*) *Vereinigung* $\Omega \sqcup \Delta := (\Omega_E \sqcup \Delta_E, \Omega_K \sqcup \Delta_K)$ ein Graph mit $|\Omega \sqcup \Delta| = |\Omega| + |\Delta|$. Offenbar ist jeder Graph die Vereinigung seiner Komponenten.

Bemerkung 11.4. Ein Graph Ω mit $\Omega_E = \{1, \dots, n\}$ ist offenbar durch Ω_K eindeutig bestimmt. Die Anzahl aller Graphen der Ordnung n ist daher $|\mathcal{G}_n| = 2^{\binom{n}{2}} = 2^{\binom{n}{2}}$. Allerdings sehen viele dieser Graphen gleich aus. Zum Beispiel gibt es sechs Graphen der Ordnung 4 mit nur einer Kante.

Definition 11.5. Graphen Ω und Δ heißen *isomorph*, falls eine Bijektion $\sigma: \Omega_E \rightarrow \Delta_E$ mit

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

existiert. Wir schreiben dann $\Omega \cong \Delta$.

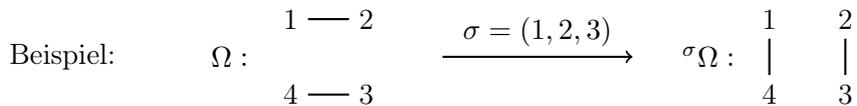
Bemerkung 11.6. Wie bei Gruppen ist die Isomorphie von Graphen eine Äquivalenzrelation. Isomorphe Graphen unterscheiden sich nur durch die Bezeichnung der Eckpunkte und haben daher die gleichen Eigenschaften (gleiche Ordnung, gleiche Kantenanzahl, etc.).

Definition 11.7. Sei $\mathfrak{g}(n)$ die Anzahl der Isomorphieklassen von Graphen der Ordnung n .

Bemerkung 11.8. Um $\mathfrak{g}(n)$ zu bestimmen, genügt es die Menge \mathcal{G}_n aller Graphen Ω mit $\Omega_E = \{1, \dots, n\} =: N$ betrachten. Also $\mathfrak{g}(n) \leq |\mathcal{G}_n| = 2^{\binom{n}{2}}$. Wir zählen die Isomorphieklassen in \mathcal{G}_n . Dafür überlegen wir uns, dass S_n auf $\binom{N}{2}$ operiert durch

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

für $\sigma \in S_n$ und $\{a, b\} \in \binom{[n]}{2}$. Dies induziert eine Operation von S_n auf $2^{\binom{[n]}{2}}$. Daher operiert S_n auch auf \mathcal{G}_n durch ${}^\sigma\Omega := (N, {}^\sigma\Omega_K)$.



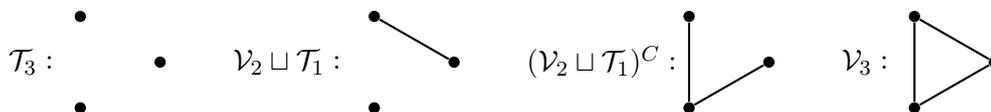
Zwei Graphen in \mathcal{G}_n sind genau dann isomorph, wenn sie in der gleichen Bahn von S_n liegen. Zur Berechnung der Anzahl dieser Bahnen benutzen wir Burnside's Lemma. Dafür müssen wir zählen, wie viele Fixpunkte $\sigma \in S_n$ auf \mathcal{G}_n hat. Sei $\tilde{\sigma}$ die von σ induzierte Permutation auf $\binom{[n]}{2}$. Ein Graph $\Omega \in \mathcal{G}_n$ bleibt genau dann unter σ fest, wenn Ω_K die Vereinigung von Bahnen von $\tilde{\sigma}$ ist. Die Anzahl $f(\sigma)$ dieser Graphen ist also $2^{z(\tilde{\sigma})}$, wobei $z(\tilde{\sigma})$ die Anzahl der Zyklen von $\tilde{\sigma}$ ist. Burnside's Lemma zeigt

$$\mathfrak{g}(n) = \frac{1}{n!} \sum_{\sigma \in S_n} 2^{z(\tilde{\sigma})}. \tag{11.1}$$

Es ist leicht zu sehen, dass $f(\sigma)$ nur vom Zyklentyp von σ abhängt (vgl. Bemerkung 10.28(ii)). Außerdem wissen wir nach Satz 2.26 wie viele Elemente von jedem Zyklentyp existieren. Man braucht in (11.1) also „nur“ über die Partitionen von n zu summieren. Man kennt keine explizite Formel für $\mathfrak{g}(n)$ (vgl. <https://oeis.org/A000088>).

Beispiel 11.9.

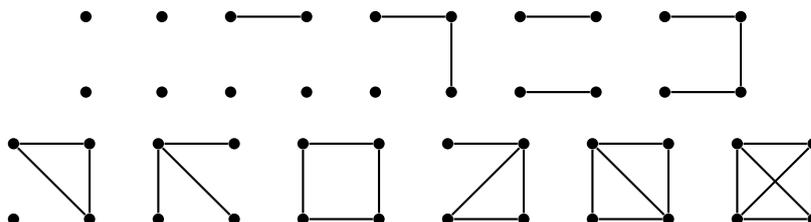
(i) Sicher ist $\mathfrak{g}(1) = 1$, $\mathfrak{g}(2) = 2$ und $\mathfrak{g}(3) = 4$:



(ii) Wir betrachten den Fall $n = 4$ in Bemerkung 11.8. Offenbar hat $\sigma = 1$ genau $z(\tilde{\sigma}) = \binom{4}{1} = 6$ Zyklen (der Länge 1) auf $\binom{[4]}{2}$, d. h. $f(\sigma) = 2^6$. Weiter hat $\sigma = (1, 2)$ die Zyklen $(\{1, 2\})$, $(\{3, 4\})$, $(\{1, 3\}, \{2, 3\})$ und $(\{1, 4\}, \{2, 4\})$ auf $\binom{[4]}{2}$ und es folgt $f(\sigma) = 2^4$. Analog zeigt man $f((1, 2, 3)) = 2^2$, $f((1, 2)(3, 4)) = 2^4$ und $f((1, 2, 3, 4)) = 2^2$. Nach Satz 2.26 gibt es sechs Permutationen vom Zyklentyp (2), acht vom Typ (3), drei vom Typ (2²) und sechs vom Typ (4). Mit (11.1) erhält man

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

Repräsentanten dieser Graphen sind:



- (iii) Mit Pólyas Satz können wir genauer die Graphen mit vorgegebener Anzahl an Ecken und Kanten zählen. Sei dafür $\Gamma := \binom{1, \dots, n}{2}$ und $\Delta := \{0, 1\}$. Jeder Graph Ω der Ordnung n entspricht einer Abbildung $f \in \Delta^\Gamma$ mit $f(a) = 1$, falls a eine Kante von Ω ist und 0 sonst. Wie in (i) operiert S_n auf Δ^Γ . Mit den Bezeichnungen aus Satz 10.19 sei $w: \Delta \rightarrow \mathbb{N}_0$, $w(0) = 0$, $w(1) = 1$. Dann ist $W(X) = 1 + X$. Die Anzahl der Bahnen von S_n auf $(\Delta^\Gamma)_k$ ist genau die Anzahl der Graphen mit n Ecken und k Kanten bis auf Isomorphie. Mit den Rechnungen aus (i) erhält man das Polynom

$$\begin{aligned} \frac{1}{4!} \sum_{\sigma \in S_4} \prod_{i=1}^4 (1 + X^i)^{c_i(\bar{\sigma})} &= \frac{1}{24} \left((1 + X)^6 + 6(1 + X)^2(1 + X^2)^2 \right. \\ &\quad \left. + 8(1 + X^3)^2 + 3(1 + X)^2(1 + X^2)^2 + 6(1 + X^2)(1 + X^4)^1 \right) \\ &= \dots = X^6 + X^5 + 2X^4 + 3X^3 + 2X^2 + X + 1. \end{aligned}$$

Es gibt also genau drei Graphen der Ordnung 4 mit drei Kanten bis auf Isomorphie (vgl. obige Abbildung). Die Symmetrie in den Koeffizienten erklärt sich durch die Bijektion $\Omega \mapsto \Omega^C$.

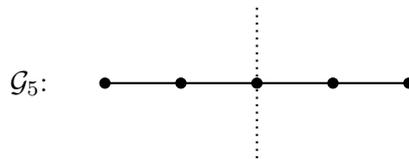
Definition 11.10. Die *Automorphismengruppe* $\text{Aut}(\Omega)$ eines Graphen Ω besteht aus den Isomorphismen von Ω auf sich selbst, d. h.

$$\text{Aut}(\Omega) := \{ \sigma \in \text{Sym}(\Omega_E) : \{x, y\} \in \Omega_K \iff \{\sigma(x), \sigma(y)\} \in \Omega_K \} \leq \text{Sym}(\Omega_E).$$

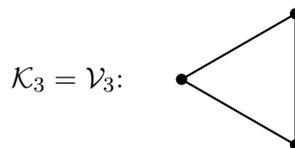
Im Fall $|\text{Aut}(\Omega)| \neq 1$ nennt man Ω *symmetrisch* und anderenfalls *asymmetrisch*.

Beispiel 11.11.

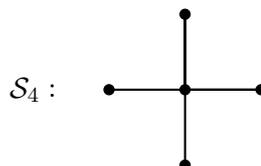
- (i) Für jeden Graphen Ω gilt $\text{Aut}(\Omega) = \text{Aut}(\Omega^C)$. Insbesondere ist $\text{Aut}(\mathcal{T}_n) = \text{Aut}(\mathcal{V}_n) \cong S_n$.
- (ii) Sei $\mathcal{G}_n := (\{1, \dots, n\}, \{\{i, i+1\} : i = 1, \dots, n-1\})$ eine *Gerade* der Ordnung $n \geq 2$. Dann ist $\text{Aut}(\mathcal{G}_n) \cong C_2$, wobei der nicht-triviale Automorphismus eine Spiegelung an der Mitte der Geraden beschreibt.



- (iii) Sei $\mathcal{K}_n := (\{1, \dots, n\}, \{\{i, i+1\} : i = 1, \dots, n-1\} \cup \{1, n\})$ ein *Kreis* der Ordnung $n \geq 3$. Dann ist $\text{Aut}(\mathcal{K}_n) \cong D_{2n}$, denn jeder Automorphismus muss die Abstände der Ecken erhalten und entspricht somit einer Symmetrie des regelmäßigen n -Ecks.



- (iv) Sei $\mathcal{S}_n := (\{1, \dots, n\}, \{\{i, n\} : i = 1, \dots, n-1\})$ ein *Stern* der Ordnung $n \geq 2$. Dann ist $\mathcal{S}_n^C \cong \mathcal{T}_1 \sqcup \mathcal{V}_{n-1}$ und $\text{Aut}(\mathcal{S}_n) \cong S_{n-1}$.



für $n \rightarrow \infty$.

Für die zweite Behauptung sei $t(n)$ die Anzahl der asymmetrischen Graphen der Ordnung n bis auf Isomorphie. Die Bahnen dieser Graphen unter obiger Operation haben dann Länge $n!$. Alle anderen Bahnen haben höchstens Länge $n!/2$. Dies zeigt

$$2^m \leq \frac{n!}{2} (\mathfrak{g}(n) + t(n)).$$

Teilt man durch $\mathfrak{g}(n)n!$ und lässt n gegen ∞ streben, so folgt $\frac{t(n)}{\mathfrak{g}(n)} \rightarrow 1$. □

Bemerkung 11.13. Frucht hat gezeigt, dass jede endliche Gruppe G die Automorphismengruppe eines Graphen Ω ist. Außer in den Fällen $G \in \{C_3, C_4, C_5\}$ kann man dabei $|\Omega| \leq 2|G|$ wählen. Der kleinste Graph mit Automorphismengruppe C_5 hat Ordnung 15 (ohne Beweis).

Definition 11.14. Ein zusammenhängender Graph Ω heißt *Baum*, falls Ω keinen Kreis enthält, d. h. je zwei Ecken von Ω sind durch genau einen Weg verbunden. Ecken vom Grad 1 heißen dann (treffenderweise) *Blätter*.

Beispiel 11.15. Geraden und Sterne sind stets Bäume. Dagegen sind \mathcal{T}_n , \mathcal{V}_n und \mathcal{K}_n für $n \geq 3$ keine Bäume.

Satz 11.16. *Ein zusammenhängender Graph Ω der Ordnung n ist genau dann ein Baum, wenn $|\Omega_K| = n - 1$ gilt. Insbesondere hat jeder zusammenhängende Graph der Ordnung n mindestens $n - 1$ Kanten.*

Beweis. Induktion nach n : Für $n = 1$ ist die Behauptung klar. Sei also Ω ein Baum mit Ordnung $n \geq 2$. Sei $\omega = \omega_1, \dots, \omega_k$ ein Weg maximaler Länge in Ω . Dann ist ω ein Blatt, denn anderenfalls könnte man den Weg um eine Ecke verlängern. Entfernt man ω und die Kante, die ω enthält, so erhält man einen Baum der Ordnung $n - 1$. Nach Induktion hat dieser Baum genau $n - 2$ Kanten. Also ist $|\Omega_K| = n - 1$.

Sei umgekehrt Ω ein zusammenhängender Graph der Ordnung n mit k Kanten. Nehmen wir an, dass Ω einen Kreis Δ enthält (d. h. $\Delta_E \subseteq \Omega_E$ und $\Delta_K \subseteq \Omega_K$). Dann kann man eine Kante von Δ entfernen, sodass Ω immer noch zusammenhängend ist. Dies kann man so oft wiederholen, bis man einen Baum erhält. Nach dem ersten Teil gilt also $k \geq n - 1$, wobei Gleichheit genau dann eintritt, wenn Ω bereits ein Baum ist. □

Bemerkung 11.17. Wir zählen zunächst Bäume ohne Berücksichtigung von Isomorphie.

Satz 11.18 (CAYLEY-Formel). *Es gibt genau n^{n-2} Bäume mit Eckenmenge $\{1, \dots, n\}$.*

*Beweis*⁸(PRÜFER). O. B. d. A. sei $n \geq 3$. Für eine n -elementige Teilmenge $M \subseteq \mathbb{N}$ sei $B(M)$ die Menge aller Bäume Ω mit $\Omega_E = M$. Wir konstruieren zueinander inverse Bijektionen

$$\begin{aligned} f: B(M) &\rightarrow M^{n-2}, \\ g: M^{n-2} &\rightarrow B(M) \end{aligned}$$

⁸alternative Beweise stehen in [Aigner-Ziegler, Das BUCH der Beweise, Springer, 2014]

durch Induktion nach n . Für $n = 3$ ist $\Omega \in B(M)$ eine Gerade und wir definieren $f(\Omega)$ als Mittelpunkt von Ω (die einzige Ecke vom Grad 2). Ist umgekehrt $\alpha \in M = M^{n-2}$ gegeben, so definieren wir $g(\alpha)$ als Gerade mit Mittelpunkt α . Sicher ist dann $f \circ g = \text{id}_{M^{n-2}}$ und $g \circ f = \text{id}_{B(M)}$.

Sei nun $n \geq 4$ und $\Omega \in B(M)$ gegeben. Sei $\alpha \in \Omega_E = M$ das Blatt mit dem kleinsten Wert in M und sei β der einzige Nachbar von α . Wir entfernen α und die Kante $\{\alpha, \beta\}$ von Ω und erhalten dadurch einen Baum $\Delta \in B(M \setminus \{\alpha\})$. Danach definieren wir $f(\Omega) := (\beta, f(\Delta))$. Sei umgekehrt $(\alpha_1, \dots, \alpha_{n-2}) \in M^{n-2}$ gegeben. Wir setzen $\alpha := \min M \setminus \{\alpha_1, \dots, \alpha_{n-2}\}$. Induktiv existiert bereits $g(\alpha_2, \dots, \alpha_{n-2}) \in B(M \setminus \{\alpha\})$ und wir können

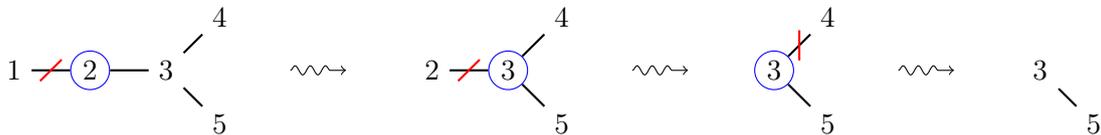
$$g(\alpha_1, \dots, \alpha_{n-2}) := (M, g(\alpha_2, \dots, \alpha_{n-2})_K \cup \{\alpha_1, \alpha\}) \in B(M)$$

definieren.

Um $g \circ f$ zu berechnen, wählen wir $\Omega \in B(M)$, das kleinste Blatt $\alpha \in \Omega_E$ und $\Delta \in B(M \setminus \{\alpha\})$ wie oben. Nach Konstruktion ist $M \setminus f(\Omega)$ die Menge der Blätter von Ω . Insbesondere ist $\min M \setminus f(\Omega) = \alpha$. Induktiv gilt $g(f(\Delta)) = \Delta$ und es folgt $g(f(\Omega)) = \Omega$. Sei umgekehrt $(\alpha_1, \dots, \alpha_{n-2}) \in M^{n-2}$ und $\alpha := \min M \setminus \{\alpha_1, \dots, \alpha_{n-2}\}$. Induktiv ist $f(g(\alpha_2, \dots, \alpha_{n-2})) = (\alpha_2, \dots, \alpha_{n-2})$. Also sind $M \setminus \{\alpha, \alpha_2, \dots, \alpha_{n-2}\}$ die Blätter von $g(\alpha_2, \dots, \alpha_{n-2})$ und $M \setminus \{\alpha_1, \dots, \alpha_{n-2}\}$ sind die Blätter von $g(\alpha_1, \dots, \alpha_{n-2})$. Daher ist α das kleinste Blatt von $g(\alpha_1, \dots, \alpha_{n-2})$ und es folgt $f(g(\alpha_1, \dots, \alpha_{n-2})) = (\alpha_1, \dots, \alpha_{n-2})$. Somit sind f und g zueinander inverse Bijektionen. Insbesondere ist f bijektiv und $|B(M)| = |M^{n-2}| = n^{n-2}$. \square

Bemerkung 11.19. Mit der Bezeichnung aus obigen Beweis nennt man $f(\Omega)$ den *Prüfer-Code* eines Baums Ω .

Beispiel 11.20. Der Prüfer-Code von



ist $(2, 3, 3)$.

Bemerkung 11.21.

- (i) Sei Ω ein Baum mit $\Omega_E = \{1, \dots, n\}$ und sei d_i der Grad der Ecke $i \in \{1, \dots, n\}$. Nach Satz 11.16 hat Ω genau $n - 1$ Kanten und es folgt $\sum_{i=1}^n d_i = 2(n - 1)$. Die Bijektion im Beweis von Satz 11.18 bildet Ω auf eine Folge (a_1, \dots, a_{n-2}) mit $|\{1 \leq i \leq n - 2 : a_i = k\}| = d_k - 1$ für $k = 1, \dots, n$ ab. Umgekehrt entsteht jede solche Folge durch einen Baum mit Eckengraden d_1, \dots, d_n . Die Anzahl dieser Bäume ist somit

$$\binom{n-2}{d_1-1, \dots, d_n-1}$$

nach Satz 1.18.

- (ii) Die Multimenge $\{d_1 - 1, \dots, d_n - 1\}$ beschreibt eine Partition von $n - 2$ (wenn man Nullen weglässt) und umgekehrt gibt es zu jeder Partition von $n - 2$ einen entsprechenden Baum. Isomorphe Bäume liefern offenbar die gleiche Multimenge $\{d_1, \dots, d_n\}$. Die Anzahl der Isomorphieklassen von Bäumen der Ordnung n ist also mindestens $p(n - 2)$.

(iii) Seien e_1, \dots, e_s die Vielfachheiten in der Multimenge $\{d_1, \dots, d_n\}$ (also $e_1 + \dots + e_s = n$). Dann kann man die Zahlen d_1, \dots, d_n auf

$$\binom{n}{e_1, \dots, e_s}$$

Weisen anordnen. Die Anzahl der Bäume, deren Eckengrade die Multimenge $\{d_1, \dots, d_n\}$ liefern ist somit

$$\binom{n-2}{d_1-1, \dots, d_n-1} \binom{n}{e_1, \dots, e_s}.$$

Für $n = 7$ und $\{d_1, \dots, d_7\} = \{1, 1, 1, 2, 2, 2, 3\}$ erhält man

$$\binom{5}{1, 1, 1, 2} \binom{7}{3, 3, 1} = \frac{5!7!}{2!3!3!} = 5! \cdot 2 \cdot 5 \cdot 7 = 120 \cdot 70 = 8.400.$$

Satz 11.22. Die Anzahl der Bäume der Ordnung n mit genau k Blättern ist $\left\{ \begin{smallmatrix} n-2 \\ n-k \end{smallmatrix} \right\} \frac{n!}{k!}$.

Beweis. Für die Wahl der Blätter $e_1, \dots, e_k \in \{1, \dots, n\}$ von Ω gibt es $\binom{n}{k}$ Möglichkeiten. Seien e_{k+1}, \dots, e_n die verbleibenden Ecken. Der Prüfer-Code von Ω entspricht dann einer surjektiven Abbildung $\{1, \dots, n-2\} \rightarrow \{e_{k+1}, \dots, e_n\}$. Die gesuchte Anzahl von Bäumen ist daher

$$\binom{n}{k} \left\{ \begin{smallmatrix} n-2 \\ n-k \end{smallmatrix} \right\} (n-k)! = \left\{ \begin{smallmatrix} n-2 \\ n-k \end{smallmatrix} \right\} \frac{n!}{k!}$$

nach Satz 2.35. □

Beispiel 11.23. Nach Satz 11.18 gibt es $5^3 = 125$ Bäume mit Eckenmenge $\{1, \dots, 5\}$. Wir bestimmen die Isomorphieklassen, indem wir die Partitionen von 3 durchgehen:

- Die Partition (1^3) liefert die $\binom{5}{2,3} = 10$ mögliche Gradfolgen $(1, 1, 2, 2, 2), \dots, (2, 2, 2, 1, 1)$. Es gibt daher

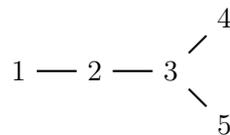
$$10 \binom{3}{1, 1, 1} = 60$$

solche Bäume, die alle zur Gerade \mathcal{G}_5 isomorph sind.

- Die Partition $(2, 1)$ liefert $\binom{5}{1,1,3} = 20$ mögliche Gradfolgen $(1, 1, 1, 2, 3), \dots, (3, 2, 1, 1, 1)$. Dies ergibt

$$20 \binom{3}{1, 2} = 60$$

Bäume, die alle zu



isomorph sind (die Ecke vom Grad 3 bildet mit drei weiteren Ecken einen Stern).

- Die Partition (3) liefert $\binom{5}{4,1} = 5$ Gradfolgen $(1, 1, 1, 1, 4), \dots, (4, 1, 1, 1, 1)$ und 5 Bäume, die alle zu \mathcal{S}_5 isomorph sind.

Es gibt daher nur drei Bäume der Ordnung 5 bis auf Isomorphie (vgl. <https://oeis.org/A000055>).

Bemerkung 11.24. Im Unterschied zu Satz 11.12 haben Erdős und Rényi auch bewiesen, dass fast alle Bäume symmetrisch sind. Dafür zeigten sie, dass die meisten Bäume *Kirschen* besitzen. Dies sind zwei Blätter mit gemeinsamen Nachbarn. Vertauschung dieser Blätter liefert einen nicht-trivialen Automorphismus.

12. Aufgaben

Aufgabe 1 (2 + 2 + 2 + 2 + 2 Punkte). Sei $n \in \mathbb{N}$. Finden Sie „kombinatorische“ Beweise (d. h. möglichst ohne Induktion) für die folgenden Identitäten:

(a) $1 + 2 + \dots + n - 1 = \binom{n}{2}$.

(b) $1 + 3 + 5 + \dots + 2n - 1 = n^2$.

(c) $1^2 + 2^2 + \dots + (n - 1)^2 = \frac{1}{4} \binom{2n}{3}$.

Hinweis: Bestimmen Sie die Mächtigkeit von $\{(a, b, c) \in \mathbb{N}^3 : a, b < c \leq n\}$ auf zwei Weisen.

(d) $1 \binom{n}{1} + 2 \binom{n}{2} + \dots + n \binom{n}{n} = n2^{n-1}$.

(e) $2^0 \binom{n}{0} + 2^1 \binom{n}{1} + \dots + 2^n \binom{n}{n} = 3^n$.

Aufgabe 2 (2 + 2 + 2 Punkte). Beantworten Sie folgenden Fragen mit Begründung:

(a) Wie viele Teilmengen von $\{1, \dots, 10\}$ enthalten mindestens eine ungerade Zahl?

(b) Wie viele Möglichkeiten gibt es die Buchstaben von MISSISSIPPI anzuordnen, sodass die vier S nicht alle nebeneinander stehen?

(c) Wie viele Möglichkeiten gibt es 7 Personen an einem runden Tisch zu platzieren, wobei zwei Möglichkeiten als gleich angesehen werden, falls jede Person die gleichen zwei Sitznachbarn hat?

Aufgabe 3 (3 Punkte). Zeigen Sie

$$\binom{n}{0} < \binom{n}{1} < \dots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \binom{n}{\lfloor n/2 \rfloor + 1} > \dots > \binom{n}{n}$$

für $n \in \mathbb{N}$, wobei $\lfloor n/2 \rfloor$ abrunden und $\lceil n/2 \rceil$ aufrunden bezeichnet.

Aufgabe 4 (2 Punkte). Sei M eine nichtleere Menge. Zeigen Sie, dass M genauso viele Teilmengen mit gerader wie mit ungerader Mächtigkeit besitzt. Bestimmen Sie die Anzahl dieser Teilmengen.

Aufgabe 5 (2 Punkte). Wie viele sechsstellige Dezimalzahlen gibt es, deren Ziffern streng monoton steigend sind?

Aufgabe 6 (2 Punkte). Zeigen Sie

$$\sum_{k=n}^m \binom{k}{n} = \binom{m+1}{n+1}$$

für $n, m \in \mathbb{N}_0$.

Hinweis: Zählen Sie die $(n + 1)$ -elementigen Teilmengen von $\{0, \dots, m\}$ mit vorgegebenem Maximum.

Bemerkung: Da die beteiligten Binomialkoeffizienten im Pascalschen Dreieck die Form eines Hockeyschlägers annehmen, spricht man von der *Hockeyschläger-Identität*.

Aufgabe 7 (3 Punkte). Beweisen Sie ohne Induktion den Multinomialssatz

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

für $a_1, \dots, a_n \in \mathbb{C}$ und $k \in \mathbb{N}$.

Aufgabe 8 (2 + 2 + 2 + 2 Punkte).

- (a) Berechnen Sie $\varphi(1500)$.
- (b) Bestimmen Sie $\{n \in \mathbb{N} : \varphi(n) = 8\}$.
- (c) Schreiben Sie $(1, 2, 3, 4)(7, 6, 5, 4, 3)$ als Produkt von disjunkten Zyklen.
- (d) Schreiben Sie $(1, 4, 6, 3)(2, 7, 9)$ als Produkt von Transpositionen. Wie viele Transpositionen benötigt man dafür?

Aufgabe 9 (3 Punkte). Jede Permutation $\sigma \in S_n$ lässt sich eindeutig als Produkt von disjunkten Zyklen

$$\sigma = (a_1, \dots, a_k)(b_1, \dots, b_l) \dots$$

schreiben, wenn man $a_1 = \max\{a_1, \dots, a_k\} < b_1 = \max\{b_1, \dots, b_l\} < \dots$ fordert (vgl. Bemerkung 2.8). Dabei zählen wir auch die 1-Zyklen mit. Zeigen Sie, dass die Abbildung

$$\Psi: S_n \rightarrow S_n, \\ \sigma \mapsto \begin{pmatrix} 1 & 2 & \dots & k & k+1 & k+2 & \dots & k+l & \dots \\ a_1 & a_2 & \dots & a_k & b_1 & b_2 & \dots & b_l & \dots \end{pmatrix}$$

bijektiv ist. Man nennt Ψ FOATA-Transformation.

Aufgabe 10 (2 + 2 + 2 Punkte). Wie viele Möglichkeiten gibt es n verschiedene Figuren auf einen $n \times n$ -Schachfeld zu platzieren, sodass

- (a) in jeder waagerechten Reihe eine Figur steht?
- (b) in jeder waagerechten und senkrechten Reihe eine Figur steht?
- (c) keine Einschränkungen vorliegen?

Aufgabe 11 (4 + 2 + 2 + 2 Punkte).

- (a) Berechnen Sie $\begin{bmatrix} 7 \\ 4 \end{bmatrix}$, $\{7\}$, $p(7)$ und $b(6)$.
- (b) Zeigen Sie

$$\begin{bmatrix} n+1 \\ 2 \end{bmatrix} = n!H_n$$

für $n \in \mathbb{N}$, wobei H_n die n -te harmonische Zahl ist.

- (c) Zeigen Sie

$$\begin{bmatrix} n \\ n-2 \end{bmatrix} = 2 \binom{n}{3} + 3 \binom{n}{4}$$

für alle $n \geq 2$.

Hinweis: Überlegen Sie sich welche Zyklientypen relevant sind und wenden Sie Satz 2.26 an.

(d) Finden und beweisen Sie eine analoge Formel für $\left\{ \begin{matrix} n \\ n-2 \end{matrix} \right\}$.

Aufgabe 12 (2 + 1 Punkte). Zeigen Sie

$$x(x+1)\dots(x+n-1) = \sum_{k=1}^n \begin{bmatrix} n \\ k \end{bmatrix} x^k$$

für alle $n \in \mathbb{N}$ und $x \in \mathbb{R}$. Folgern Sie:

$$\sum_{k=1}^n (-1)^k \begin{bmatrix} n \\ k \end{bmatrix} = 0.$$

Aufgabe 13 (1 + 1 Punkte). Wie viele Summanden haben die beiden Formeln

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix} &= \sum_{0 < a_1 < \dots < a_{n-k} < n} a_1 \dots a_{n-k}, \\ \left\{ \begin{matrix} n \\ k \end{matrix} \right\} &= \sum_{1 \leq a_1 \leq \dots \leq a_{n-k} \leq k} a_1 \dots a_{n-k} \end{aligned}$$

aus den Sätzen 2.17 und 2.32.

Aufgabe 14 (2 Punkte). Zeigen Sie, dass S_{2n} genau $1 \cdot 3 \cdot \dots \cdot (2n-1)$ fixpunktfreie Permutationen der Ordnung 2 besitzt.

Aufgabe 15 (2 Punkte). Zeigen Sie, dass es unter sechs Personen stets drei gibt, die sich alle kennen oder alle nicht kennen.

Aufgabe 16 (2 Punkte). Zeigen Sie, dass es zwei Primzahlen gibt, deren Differenz durch 2019 teilbar ist.

Hinweis: Mit dem Schubfachprinzip braucht man die Primzahlen nicht explizit anzugeben.

Zusatz: Gibt es zwei Primzahlen, deren Summe durch 2019 teilbar ist?

Aufgabe 17 (2 Punkte). Zu jedem $n \in \mathbb{N}$ existiert ein $m \in \mathbb{N}$, sodass mn nur aus den Ziffern 0 und 1 besteht.

Aufgabe 18 (2+2 Punkte). Für Partitionen $\lambda = (\lambda_1, \dots, \lambda_s)$ und $\mu = (\mu_1, \dots, \mu_t)$ von $n \in \mathbb{N}$ schreiben wir $\lambda \leq \mu$, falls λ eine Verfeinerung von μ ist, d. h. bei geeigneter Nummerierung gilt $\mu_1 = \lambda_1 + \dots + \lambda_{i_1}$, $\mu_2 = \lambda_{i_1+1} + \dots + \lambda_{i_2}$ usw. Zeigen Sie, dass $(P(n), \leq)$ eine lokal endliche geordnete Menge ist. Berechnen Sie die entsprechende Möbius-Funktion $\mu_{P(4)}((1, 1, 1, 1), (4))$.

Aufgabe 19. Sei V ein endlich-dimensionaler Vektorraum über einem Körper mit $q < \infty$ Elementen. Die Menge \mathcal{U} der Unterräume von V ist durch \subseteq geordnet. Zeigen Sie

$$\mu_{\mathcal{U}}(U, W) = (-1)^{\dim(W/U)} q^{\binom{\dim(W/U)}{2}}$$

für $U \leq W \leq V$.

Aufgabe 20. Seien $a_0, a_1, \dots, b_0, b_1, \dots \in \mathbb{C}$. Zeigen Sie:

(a) (Binomial-Inversion)

$$\forall n \in \mathbb{N}_0 : a_n = \sum_{k=0}^n (-1)^k \binom{n}{k} b_k \iff \forall n \in \mathbb{N}_0 : b_n = \sum_{k=0}^n (-1)^k \binom{n}{k} a_k$$

(b) (Stirling-Inversion)

$$\forall n \in \mathbb{N}_0 : a_n = \sum_{k=0}^n (-1)^k \begin{bmatrix} n \\ k \end{bmatrix} b_k \iff \forall n \in \mathbb{N}_0 : b_n = \sum_{k=0}^n (-1)^k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} a_k$$

Aufgabe 21 (2 + 2 Punkte).

(a) Berechnen Sie die Koeffizienten von $(1 + X + X^2)^{-1} \in \mathbb{Q}[[X]]$.

(b) Berechnen Sie die ersten sechs Koeffizienten der Umkehrfunktion von $X - X^2 \in \mathbb{Q}[[X]]$.

Hinweis: Setzen Sie die Umkehrfunktion in der Form $\sum a_n X^n$ an und stellen Sie Gleichungen für a_1, a_2, \dots auf.

Aufgabe 22 (2 Punkte). Für jede Primzahl p bilden die Potenzreihen der Form $X + a_2 X^2 + \dots \in \mathbb{F}_p[[X]]$ eine Untergruppe von $\mathbb{F}_p[[X]]^\circ$, die man *Nottingham-Gruppe* N_p nennt. Konstruieren Sie ein Element der Ordnung p in N_p .

Aufgabe 23 (3 Punkte). Konstruieren Sie für jeden Körper K geeignete Potenzreihen $\alpha, \beta, \gamma \in K[[X]]$, sodass $\alpha \circ \beta \neq \beta \circ \alpha$, $\alpha \circ (\beta + \gamma) \neq \alpha \circ \beta + \alpha \circ \gamma$ und $\alpha \circ (\beta\gamma) \neq (\alpha \circ \beta)(\alpha \circ \gamma)$

Aufgabe 24. Wir betrachten folgende Potenzreihen in $\mathbb{C}[[X]]$:

$$\begin{aligned} \sin(X) &:= \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} X^{2n+1}, & \cos(X) &:= \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} X^{2n}, \\ \tan(X) &:= \frac{\sin(X)}{\cos(X)}, & \arctan(X) &:= \sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1} X^{2k+1}, \\ \arcsin(X) &:= \sum_{n=0}^{\infty} \frac{(2n)!}{(2^n n!)^2} \frac{X^{2n+1}}{2n+1}. \end{aligned}$$

Zeigen Sie:

(a) (EULERSche Formel) $\exp(iX) = \cos(X) + i \sin(X)$, wobei $i = \sqrt{-1} \in \mathbb{C}$.

(b) $\sin(2X) = 2 \sin(X) \cos(X)$ und $\cos(2X) = \cos(X)^2 - \sin(X)^2$.

(c) („trigonometrischer Pythagoras“) $\cos(X)^2 + \sin(X)^2 = 1$.

(d) $\sin(X)' = \cos(X)$ und $\cos(X)' = -\sin(X)$.

(e) $\arctan \circ \tan = X$.

Hinweis: Prüfen Sie zuerst $\tan \in \mathbb{C}[[X]]^\circ$. Danach ableiten.

(f) $\arctan(X) = \frac{i}{2} \log\left(\frac{i+X}{i-X}\right)$ mit $i = \sqrt{-1} \in \mathbb{C}$.

Hinweis: Prüfen Sie, dass $\log\left(\frac{i+X}{i-X}\right)$ wohldefiniert ist.

(g) $\arcsin(X)' = \frac{1}{\sqrt{1-X^2}}$.

Hinweis: Newtonscher Binomialsatz.

(h) $\arcsin \circ \sin = X$.

Bemerkung: Es gibt unzählige weitere trigonometrische Identitäten, aber nicht alle lassen sich über formale Potenzreihen beweisen. Zum Beispiel besitzt \cos keine formale Umkehrfunktion (trotzdem kann man die analytische Taylorreihe für \arccos angeben).

Aufgabe 25 (3 Punkte). Sei K ein Körper. Verifizieren Sie, dass

$$K((X)) := \left\{ \sum_{n=k}^{\infty} a_n X^n : k \in \mathbb{Z}, a_n \in K \right\}$$

mit den Verknüpfungen

$$\begin{aligned} \sum a_n X^n + \sum b_n X^n &= \sum (a_n + b_n) X^n, \\ \sum a_n X^n \cdot \sum b_n X^n &= \sum_{n=-\infty}^{\infty} \left(\sum_{k=-\infty}^{\infty} a_k b_{n-k} \right) X^n \end{aligned}$$

ein Körper ist.

Hinweis: Vergessen Sie nicht die Wohldefiniertheit der Addition und Multiplikation zu prüfen.

Aufgabe 26 (2 Punkte). Finden und beweisen Sie eine explizite Formel für die rekursiv definierte Folge $a_0 := 1$, $a_1 := 2$, $a_{n+1} := 3a_n - a_{n-1}$ für $n \in \mathbb{N}$.

Aufgabe 27 (2 Punkte). Bestimmen Sie alle invertierbaren 2×2 -Matrizen über dem Körper \mathbb{F}_2 .

Aufgabe 28 (2 + 3 + 2 Punkte). Sei $n \in \mathbb{N}$. Beweisen Sie:

- Sei $p_1(n)$ die Anzahl der Partitionen von n mit geraden Teilen. Sei $p_2(n)$ die Anzahl der Partitionen von n , deren Teile gerade Vielfachheit haben. Zeigen Sie $p_1(n) = p_2(n)$ für alle $n \in \mathbb{N}$.
- Sei $p_+(n)$ (bzw. $p_-(n)$) die Anzahl der Partitionen von n mit einer geraden (bzw. ungeraden) Anzahl an Teilen. Zeigen Sie, dass $(-1)^n (p_+(n) - p_-(n))$ die Anzahl der symmetrischen Partitionen von n ist.
- Sei $q_+(n)$ (bzw. $q_-(n)$) die Anzahl der Partitionen von n mit einer geraden (bzw. ungeraden) Anzahl an geraden Teilen. Zeigen Sie, dass $q_+(n) - q_-(n)$ die Anzahl der symmetrischen Partitionen von n ist.

Aufgabe 29 (3 + 3 + 3 Punkte). Seien $n, d \in \mathbb{N}$. Beweisen Sie:

- (GLAISHER) Die Anzahl der Partitionen von n , deren Teile nicht durch d teilbar sind, ist gleich der Anzahl der Partitionen von n , in denen kein Teil d -mal (oder öfter) auftritt.
Hinweis: Der Fall $d = 2$ entspricht Satz 5.7(i).
- (SUBBARAO) Die Anzahl der Partitionen von n , bei denen jeder Teil genau zweimal, dreimal oder fünfmal auftritt, ist gleich der Anzahl der Partitionen von n in Teile der Form $\pm 2 + 12k$, $\pm 3 + 12k$ oder $6 + 12k$.

- (c) (MACMAHON) Die Anzahl der Partitionen von n , bei denen jeder Teil mindestens zweimal auftritt, ist gleich der Anzahl der Partitionen von n in Teile, die nicht die Form $\pm 1 + 6k$ haben.

Aufgabe 30 (2 + 2 Punkte).

- (a) Bestimmen Sie alle irreduziblen Polynome in $\mathbb{F}_3[X]$ vom Grad ≤ 3 .
 (b) Berechnen Sie das Kreisteilungspolynom Φ_{396} .

Aufgabe 31 (3 Punkte). Sei $n \in \mathbb{N}$. Wie viele paarweise verschiedene Zahlen $a, b, c \in \{1, \dots, 2n\}$ gibt es, sodass a das arithmetische Mittel von b und c ist?

Weihnachtsrätsel (+3 Zusatzpunkte). Aus einem Beutel mit r roten und b blauen Perlen werden zufällig zwei entnommen. Haben beide Perlen die selbe Farbe, so entferne man sie und gebe stattdessen eine neue rote Perle in den Beutel. Haben beide Perlen verschiedene Farben, so entferne man die rote und gebe die blaue zurück in den Beutel. Wenn man diesen Prozess oft genug wiederholt, verbleibt am Ende genau eine Perle im Beutel. Wie lässt sich die Farbe dieser verbleibenden Perle aus r und b ermitteln?

Hinweis: Es hat nichts mit Wahrscheinlichkeiten zu tun.

Aufgabe 32 (2 + 2 + 2 Punkte). Sei Z die Menge aller rationalen Polynome mit ganzzahligen Werten, d. h.

$$Z := \{\alpha \in \mathbb{Q}[X] : \alpha(z) \in \mathbb{Z} \forall z \in \mathbb{Z}\}.$$

Zeigen Sie:

- (a) Für $\alpha, \beta \in Z$ gilt $\alpha + \beta, \alpha\beta \in Z$.
 (b) Die in Beispiel 6.28 definierten Polynome $\binom{X}{k}$ liegen in Z für $k \in \mathbb{N}_0$.
 (c) Jedes $\alpha \in Z$ lässt sich eindeutig in der Form $\alpha = \sum_{k=0}^{\infty} a_k \binom{X}{k}$ mit $a_k \in \mathbb{Z}$ schreiben.

Aufgabe 33 (3 + 3 Punkte). Für $\alpha = \sum a_{k_1, \dots, k_n} X_1^{k_1} \dots X_n^{k_n} \in K[X_1, \dots, X_n]$ definieren wir die (l_1, \dots, l_n) -te Hasse-Ableitung durch

$$H^{(l_1, \dots, l_n)}(\alpha) = \sum a_{k_1, \dots, k_n} \binom{k_1}{l_1} \dots \binom{k_n}{l_n} X_1^{k_1-l_1} \dots X_n^{k_n-l_n} \in K[X_1, \dots, X_n].$$

Die *Vielfachheit* von $x = (x_1, \dots, x_n) \in K^n$ als Nullstelle von α sei die kleinste Zahl $m_\alpha(x) \in \mathbb{N}_0 \cup \{\infty\}$ mit $H^{(l_1, \dots, l_n)}(\alpha) = 0$ für alle (l_1, \dots, l_n) mit $l_1 + \dots + l_n < m_\alpha(x)$ (im Fall $m_\alpha(x) = 0$ ist x keine Nullstelle von α). Zeigen Sie:

- (a) Für $\alpha \neq 0$ gilt $\sum_{x \in K^n} m_\alpha(x) \leq \deg(\alpha) |K|^{n-1}$.
 (b) Sei $c: K^n \rightarrow \mathbb{N}_0$ und $d \in \mathbb{N}_0$ mit $\sum_{x \in K^n} \binom{c(x)+n-1}{n} < \binom{d+n}{n}$. Dann existiert ein $\alpha \in K[X_1, \dots, X_n] \setminus \{0\}$ mit $\deg(\alpha) \leq d$ und $m_\alpha(x) \geq c(x)$ für alle $x \in K^n$.

Aufgabe 34 (2 + 2 Punkte). Beweisen Sie die „inversen“ Waring-Formeln

$$\tau_k = \sum_{(1^{a_1}, \dots, k^{a_k}) \in P(k)} \prod_{i=1}^k \frac{\rho_i^{a_i}}{i^{a_i} a_i!},$$

$$\sigma_k = (-1)^k \sum_{(1^{a_1}, \dots, k^{a_k}) \in P(k)} \prod_{i=1}^k \frac{(-\rho_i)^{a_i}}{i^{a_i} a_i!}.$$

für $K = \mathbb{C}$ und $k \in \mathbb{N}$.

Hinweis: Beweis von Satz 5.12.

Aufgabe 35 (2 + 2 Punkte).

(a) Berechnen Sie die Bernoulli-Zahlen B_5, \dots, B_{10} .

(b) Für welche $n < 100$ hat die n -te Bernoulli-Zahl die Form $B_n = \frac{z}{6}$ mit $z \in \mathbb{Z}$?

Aufgabe 36 (2 Punkte). Offenbar ist die Menge $M := \mathbb{Q} \setminus \{0\}$ ein Magma bzgl. Division. Wie viele Ergebnisse erhält man, wenn man $1 : 2 : 3 : 4$ auf alle möglichen Weisen klammert?

Aufgabe 37 (2 + 2 Punkte).

(a) Welche Muster besitzt (bzw. vermeidet) die Permutation $(2, 4, 5, 6, 1, 3) \in S_6$?

(b) Sei $n \geq 4$. Welche Permutationen in S_n besitzen nur ein Muster?

Aufgabe 38 (2 + 2 Punkte). Seien $n, k \in \mathbb{N}$. Zeigen Sie

$$\left| \left\{ (n_1, \dots, n_k) \in \mathbb{N}^k : \sum_{i=1}^k n_i = n \right\} \right| = \binom{n-1}{k-1},$$

$$\left| \left\{ (n_1, \dots, n_k) \in \mathbb{N}_0^k : \sum_{i=1}^k n_i = n \right\} \right| = \binom{n+1}{k-1} = \binom{\binom{k}{n}}{\binom{k}{n}}.$$

Hinweis: Betrachten Sie die Abbildung $(n_1, \dots, n_k) \mapsto (n_1, n_1 + n_2, \dots, n_1 + \dots + n_{k-1})$.

Aufgabe 39 (2 + 2 Punkte). Sei $n \in \mathbb{N}$ und $A \subseteq \{1, \dots, 2n\}$ mit $|A| = n + 1$. Zeigen Sie:

(a) A enthält zwei teilerfremde Zahlen.

(b) Es existieren $a, b \in A$ mit $a \neq b$ und $a \mid b$.

Aufgabe 40 (2 Punkte). Zeigen Sie $\sum_{n=1}^{\infty} \frac{C_n}{4^n} = 1$.

Aufgabe 41 (2 Punkte). Seien $H \leq G$ endliche Gruppen. Beweisen oder widerlegen Sie $k(H) \leq k(G)$.

Aufgabe 42 (2 Punkte). Bestimmen Sie die Automorphismengruppe des Graphen $\mathcal{V}_2 \sqcup \mathcal{V}_2$.

Aufgabe 43 (2+2+2 Punkte). Bestimmen Sie die Bäume mit Prüfer-Code $(1, 2, 2, 3, 3, 3)$, $(1, 2, \dots, n)$ und $(1, 1, \dots, 1)$.

Aufgabe 44 (2 Punkte). Konstruieren Sie alle Bäume der Ordnung 5 bis auf Isomorphie.

Aufgabe 45 (2+2+2 Punkte). Sei K ein Körper. Für $\alpha = \sum a_n X^n \in K[[X]]$ sei

$$m(\alpha) := \inf\{n \in \mathbb{N}_0 : a_n \neq 0\},$$

wobei $m(0) = \inf \emptyset = \infty$. Zeigen Sie:

- (a) Für $\alpha, \beta \in K[[X]]$ gilt $m(\alpha\beta) = m(\alpha) + m(\beta)$ und $m(\alpha + \beta) \geq m(\alpha) + m(\beta)$.
- (b) Für $\alpha, \beta \in K[[X]]$ mit $\beta \neq 0$ existieren eindeutig bestimmte $\delta, \gamma \in K[[X]]$ mit $\alpha = \beta\gamma + \delta$ und ($\gamma = 0$ oder $m(\delta) > m(\beta)$).
- (c) Für $\alpha, \beta \in K[[X]]$ existiert genau dann ein $\gamma \in K[[X]]$ mit $\alpha = \beta\gamma$, falls $m(\alpha) \geq m(\beta)$ gilt (dies verallgemeinert Lemma 4.8).

Aufgabe 46 (3+3+3 Punkte). Beweisen Sie für alle $\alpha \in \mathbb{C}[[X]]$:

(a)

$$\prod_{k=0}^{\infty} (1 + \alpha X^k) = \sum_{k=0}^{\infty} \frac{\alpha^k X^{\binom{k}{2}}}{X^{k!}}.$$

(b) Für $n \in \mathbb{N}$ gilt

$$\prod_{k=1}^n \frac{1}{1 - \alpha X^k} = \sum_{k=0}^{\infty} \alpha^k \left\langle \begin{matrix} n+k-1 \\ k \end{matrix} \right\rangle X^k.$$

Hinweis: Interpretieren Sie den Koeffizienten von $\alpha^k X^l$.

(c)

$$\prod_{k=1}^{\infty} \frac{1}{1 - \alpha X^k} = \sum_{k=0}^{\infty} \frac{\alpha^k X^k}{X^{k!}}.$$

Aufgabe 47 (3 Punkte). Sei $\alpha = \sum a_n X^n \in \mathbb{C}[[X]]$, $k \in \mathbb{N}$ und $\zeta_k = e^{2\pi i/k}$. Zeigen Sie

$$\frac{1}{k} \sum_{l=1}^k \alpha(\zeta_k^l X) = \sum_{n=0}^{\infty} a_{kn} X^{kn}.$$

A. GAP-Befehle

Die meisten kombinatorischen Objekte lassen sich im kostenfreien Computeralgebrasystem GAP⁹ berechnen:

Objekt	Code
$n!$	<code>Factorial(n);</code>
2^A	<code>Combinations(A);</code>
Variationen mit Wiederholung	<code>Tuples([1,2,3],2);</code>
Variationen ohne Wiederholung	<code>Arrangements([1,2,3],2);</code>
Kombinationen mit Wiederholung	<code>UnorderedTuples([1,2,3],2);</code>
Kombinationen ohne Wiederholung	<code>Combinations([1,2,3],2);</code>
S_n	<code>SymmetricGroup(n);</code>
$\binom{n}{k}$	<code>Binomial(n,k);</code>
$\langle \binom{n}{k} \rangle$	<code>GaussianCoefficient(n,k,X(Integers,"q"));</code>
$\left(\binom{n}{k} \right)$	<code>NrUnorderedTuples(n,k);</code>
$\left[\begin{matrix} n \\ k \end{matrix} \right]$	<code>Stirling1(n,k);</code>
$\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$	<code>Stirling2(n,k);</code>
$P(n)$	<code>Partitions(n);</code>
Partitionen in ungerade Teile	<code>RestrictedPartitions(n,[1,3..2*n+1]);</code>
Partitionen in ungleiche Teile	<code>RestrictedPartitionsWithoutRepetitions(n,[1..n]);</code>
Partitionen in k Teile	<code>Filtered(Partitions(n),p->Size(p)=k);</code>
Symmetrische Partitionen	<code>Filtered(Partitions(n),p->AssociatedPartition(p)=p);</code>
$p(n)$	<code>NrPartitions(n);</code>
$P(A)$	<code>PartitionsSet(A);</code>
$b(n)$	<code>Bell(n);</code>
$\varphi(n)$	<code>Phi(n);</code>
Φ_n	<code>CyclotomicPolynomial(Rationals,n);</code>
Faktorisierung in $K[X]$	<code>x:=X(Rationals,"X");; Factors(x^4+3*x^3-7*x+1);</code>
B_n	<code>Bernoulli(n);</code>
f_n	<code>Fibonacci(n);</code>

⁹<https://www.gap-system.org/>

Stichwortverzeichnis

Symbole

\emptyset , 3
 2^A , 3
 $\langle \binom{n}{k} \rangle$, 33
 $|A|$, 3
 A^I , 3
 $\binom{A}{k}$, 3
 $\binom{a}{k}$, 4
 $a \leq b$, 20
 α^{-1} , 25
 $|\alpha|$, 27
 α' , 30
 $\alpha(\beta)$, 28
 $\alpha \circ \beta$, 28
 $\alpha^{(n)}$, 30
 A^n , 3
 $\text{Aut}(\Omega)$, 88
 B_n , 66
 $b(n)$, 15
 \mathbb{C} , 3
 $C_G(x)$, 83
 C_n , 71, 76
 D_{2n} , 75
 $\deg(\alpha)$, 50, 58
 $\exp(X)$, 25
 \mathbb{F}_q , 50
 $\text{GL}(V)$, 74
 \mathcal{G}_n , 88
 $g(n)$, 82
 $\mathfrak{g}(n)$, 86
 $H^k(\alpha)$, 30
 $H^{(l_1, \dots, l_n)}(\alpha)$, 98
 H_n , 12
 $I_d(K)$, 52
 $k(G)$, 83
 $k(S_n)$, 84
 $K[X]$, 50
 $K[[X]]$, 24
 $K[[X]]^\times$, 26
 $K((X))$, 97
 $K[[X]]^\circ$, 29
 \mathcal{K}_n , 88
 λ' , 36
 $\log(1 + X)$, 31
 $m(\alpha)$, 100
 $\mu_A(a, b)$, 20
 $n!$, 4
 $N_G(H)$, 85
 \mathbb{N} , 3
 \mathbb{N}_0 , 3
 $\binom{n}{k_1, \dots, k_s}$, 4
 $\Omega \sqcup \Delta$, 86
 $O(\mathbb{R}^n)$, 74

Ω^C , 86
 \mathbb{P} , 3
 $p_\pm(n)$, 97
 $P(A)$, 15
 $\varphi(n)$, 9
 $p_{k,l}(n)$, 38
 $p_k(n)$, 37
 $p(n)$, 15, 20, 40
 \mathbb{Q} , 3
 $q_\pm(n)$, 97
 \mathbb{R} , 3
 ρ_k , 62
 $\text{SO}(\mathbb{R}^n)$, 76
 σ_k , 62
 S_n , 5
 \mathcal{S}_n , 88
 $\begin{bmatrix} n \\ k \end{bmatrix}$, 14
 $\left\{ \binom{n}{k} \right\}$, 17
 $\text{Sym}(A)$, 5
 τ_k , 62
 \mathcal{T}_n , 86
 V_4 , 82
 \mathcal{V}_n , 86
 $\times_{i \in I} A_i$, 3
 $\langle x_1, \dots, x_n \rangle$, 75
 $\binom{X}{k}$, 54, 98
 \mathbb{Z} , 3
 ζ_n , 55

A

Ableitung, 30
 n-te, 30
Absolutglied, 24
Apéry-Konstante, 68
Anagramm, 7
Anzahl
 k-Zyklen, 12
 Partitionen, 15
 Partitionen in ungleiche Teile, 37
 Partitionen mit festem Typ, 16
 Partitionen mit größtem Teil *k*, 37
 Permutationen mit Zyklentyp, 16
 symmetrischer Partitionen, 37
Äquivalenzklasse, 16
Äquivalenzrelation, 15
asymmetrisch, 88
Automorphismengruppe, 88

B

Bahn, 76
Bahn-Stabilisator-Satz, 77
Bahngleichung, 77
Baum, 90

Bellzahl, 15
Bernoulli-Zahl, 66
Binet-Formel, 35
Binomial-Inversion, 96
Binomialkoeffizient, 4
Binomialsatz, 6
Binomische Inversion, 96
Blatt, 90
Burnsides Lemma, 78

C

Catalan, 72
Catalan-Zahl, 71
Cayley-Formel, 90
Chevalley-Warning, 60
Clausen, 69

D

Diedergruppe, 75
disjunkte Vereinigung, 3
Division mit Rest, 51, 53
Dobiński-Formel, 19
Durfees Quadrat-Satz, 40

E

Ecke, 85
 benachbart, 85
 Grad, 85
 verbunden, 85
Einheitengruppe, 26
Einheitswurzel, 55
 primitive, 55
Enigma, 10
Erdős-Ginzburg-Ziv, 61
Erdős-Rényi, 89
Erdős-Szekeres, 9
Erdős-Turán, 38, 84
erzeugende Funktion, 34
 für $b(n)$, 36
 für $p(n)$, 36
Erzeugendensystem, 75
Euler, 36, 72
Euler-Mascheroni-Konstante, 13
Eulers Pentagonalzahlensatz, 39
eulersche φ -Funktion, 9
Eulersche Formel, 96
Exponentialfunktion, 25

F

Faktorregel, 31
Fakultät, 4
Faulhabersche Formel, 68
Fermats kleiner Satz, 54
Fibonacci-Folge, 35
Fixpunkt, 10
fixpunktfrei, 10
Foata-Transformation, 94

Franklin, 39
Funktionalgleichung
 für $\exp(X)$, 29
 für $\log(1 + X)$, 32
führender Koeffizient, 50

G

Gauß, 52
Gaußscher Binomialkoeffizient, 33
Gaußscher Binomialsatz, 34
Geburtstagsparadoxon, 5
geometrische Reihe, 26
Gerade, 88
Girard-Newton-Identität, 62
Glaisher, 97
Grad, 58
 Ecke, 85
 Polynom, 50
Graph, 85
 asymmetrischer, 88
 komplementärer, 86
 symmetrischer, 88
 trivialer, 86
 Vereinigung, 86
 vollständiger, 86
 zusammenhängend, 85
Gruppe, 74
 abelsche, 74
 allgemeine lineare, 74
 endliche, 74
 orthogonale, 74
 spezielle orthogonale, 76
 symmetrische, 5
 triviale, 74
 zyklische, 76

H

Hall, 23
Halskette, 78, 81
Hardy-Ramanujan, 20
Hasse-Ableitung, 30, 98
Hauptsatz über symmetrische Polynome, 63
Hilberts Nullstellensatz, 60
Hirschhorn, 41
Hockeyschläger-Identität, 93

I

Inklusions-Exklusions-Prinzip, 8
Interpolation, 58
irreduzibel, 51
Isomorphie
 von Graphen, 86
 von Gruppen, 82
Isomorphieklasse, 82

J

Jacobi, 41

Jacobis Tripelprodukt, 43

K

Kante, 85

kartesisches Produkt, 3

Kettenregel, 31

Klassengleichung, 83

Klassenzahl, 83

Kleinschen Vierergruppe, 82

Kombination

mit Wiederholung, 8

ohne Wiederholung, 6

Kombinatorischer Nullstellensatz, 60

Komponente, 85

Kongruenz, 53

Konjugation, 83

Konjugationsklasse, 83

Kreis, 88

Kreisteilungspolynom, 55

L

Lagrange, 77

Lagrange-Jacobi, 45

Landau, 84

Laurent-Reihe, 25

Linksminimum, 73

Linksnebenklasse, 77

Logarithmus, 31

lokal endlich, 20

Lotto, 6

Lucas, 70

Länge

einer Bahn, 76

eines Zyklus, 11

M

MacMahon, 72, 98

MacMahon-Würfel, 79

Magma, 71

Menge

endlich/unendlich, 3

geordnete, 20

gleichmächtig, 3

Mercator-Reihe, 31

modulo, 53

Montmort, 10

Multimenge, 8

Multinomialkoeffizient, 4

Multinomialsatz, 7, 94

Muster, 72

Möbius-Funktion, 20

klassische, 22

Möbius-Inversion, 21

multiplikative, 23

N

Newtonscher Binomialsatz, 32

Nicomachus-Identität, 65

Norm, 27

Normalisator, 85

Nottingham-Gruppe, 96

Nullstelle, 50

O

$\Omega \cong \Delta$, 86

Ono, 43

Operation, 76

transitive, 76

Ordnung

Element, 75

Graph, 85

Gruppe, 74

Ordnungsrelation, 20

lokal endlich, 20

P

Partition

Teile, 15

Partialbruchzerlegung, 26

Partition

einer Menge, 15

einer Zahl, 15

konjugierte, 36

symmetrisch, 37

Pascalsches Dreieck, 5

Permutation, 5

fixpunktfrei, 10

Pólya, 81

Polynom, 50

in mehreren Unbekannten, 58

konstant, 50

normiert, 50

reduzibel/irreduzibel, 51

Potenzmenge, 3

Potenzreihe, 24

Inverse, 25

invertierbar, 25

Norm, 27

Wurzel, 32

Primfaktorzerlegung in $K[X]$, 52

Primitivwurzel, 60

Problem der 100 Gefangenen, 13

Produktregel, 31

Prüfer-Code, 91

Prüfer, 90

Q

Quotientenregel, 31

R

Ramanujan, 42

reduzibel, 51

Relation, 15

antisymmetrisch, 20

reflexiv, 15
symmetrisch, 15
transitiv, 15
Rogers-Ramanujan-Identitäten, 48

S

Sammelbilderproblem, 18
Schubfachprinzip, 5
Schwartz-Zippel, 59
Segner, 71
Sekretärinnenproblem, 10
Simion-Schmidt, 73
Skatkarten, 7
Stabilisator, 76
Stern, 88
Stirling-Formel, 19
Stirling-Inversion, 96
Stirling-Zahl
 erster Art, 14
 zweiter Art, 17
Subbarao, 97
Sudoku, 80
Summenregel, 31
Symmetriegruppe, 75

T

Taylorreihe, 30
teilerfremd, 9
Transposition, 11
trigonometrischer Pythagoras, 96

U

Umkehrfunktion, 30
Unbekannte, 24
Untergruppe, 75
 erzeugte, 75

V

Vandermonde-Identität, 6, 54
Variation
 mit Wiederholung, 5, 7
 ohne Wiederholung, 5
Verknüpfung, 71
Vieta, 62
von Staudt, 69

W

Waring-Formel, 64
 inverse, 99
Waring-Problem, 47
Weg, 85
Wright, 43
Würfel, 8, 79

Y

Young-Diagramm, 36

Z

Zahl
 ganze, 3
 harmonische, 12
 komplexe, 3
 natürliche, 3
 Prim-, 3
 rationale, 3
 reelle, 3
Zahlenschloss, 5
Zauberwürfel, 80
Zentralisator, 83
Zusammenhangskomponente, 85
zusammenhängend, 85
Zyklentyp, 16
Zyklus, 11
 disjunkt, 11