Inklusion & Exklusion

Referenz: Matousek-Nesetřil 2006 Invitation to Discrete Mathematics Section 3.7
Hardy Wright 1975 An Introduction to the Theory of Numbers Chapter 16
Halbeisen-Skript: Kapitel 12

Proposition: Für je zwei Mengen X und Y gilt $|X \cup Y| + |X \cap Y| = |X| + |Y|$.

Proposition: Für beliebige Teilmengen $X_1, \ldots, X_n$ einer endlichen Menge X gilt

$$\Big| X \smallsetminus \bigcup_{1 \leqslant i \leqslant n} X_i \Big| \;=\; |X| - \sum_{1 \leqslant i \leqslant n} |X_i| + \sum_{1 \leqslant i < j \leqslant n} |X_i \cap X_j| - \ldots + (-1)^n \cdot \big| X_1 \cap \ldots \cap X_n \big|.$$

Genauer gilt

$$\Big| X \smallsetminus \bigcup_{1 \leqslant i \leqslant n} X_i \Big| \;=\; \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{|I|} \cdot |X_I|$$

mit

$$X_I \;:=\; \big\{ x \in X \;\big|\; \forall i \in i \colon x \in X_i \big\} \;=\; \begin{cases} X & \text{falls } I = \varnothing, \\ \bigcap_{i \in I} X_i & \text{falls } I \neq \varnothing. \end{cases}$$

Anwendung: Ein Übungsleiter gibt n korrigierte Übungsserien zurück, aber verwechselt sie zufällig. Was ist die Wahrscheinlichkeit, dass alle Teilnehmenden eine falsche Serie erhalten?

$$p_n \;:=\; \frac{\left|\left\{\sigma \in S_n \;\middle|\; \forall i\colon \sigma i \neq i\right\}\right|}{|S_n|} \;=\; \ldots$$

Allgemeiner: Die Anzahl der Permutationen in S_n mit genau k Fixpunkten ist ...

Möbius-Inversion

In diesem Abschnitt betrachten wir Funktionen $f, g, h, \ldots : \mathbb{Z}^{\geqslant 1} \to \mathbb{C}$.

Definition: Die *Faltung von f und g* ist die Funktion $f * g$ mit

$$(f * g)(n) \;:=\; \sum_{d|n} f\left(\tfrac{n}{d}\right) \cdot g(d).$$

Beispiel: Die Funktion δ mit $\delta(1) = 1$ und $\delta(n) = 0$ für alle $n > 1$.

Grundeigenschaften: Für alle f, g, h gilt

$f * g$	$=$	$g * f$
$(f * g) * h$	$=$	$f * (g * h)$
$\delta * f$	$=$	f

Beispiel: Betrachte die Funktion τ_k mit $\tau_k(n) = n^k$ für $k \in \mathbb{N}$. Dann gilt

$$(\tau_0 * \tau_k)(n) \;=\; \sum_{d|n} d^k.$$

Für $k = 0$ ist dies die Anzahl aller Teiler von n, für $k = 1$ die Summe aller Teiler, usw.

Definition: Die *Möbiussche Umkehrfunktion* μ ist definiert durch

$$\mu(n) \;:=\; \begin{cases} (-1)^k & \text{falls } n \text{ Produkt von } k \text{ paarweise verschiedenen Primzahlen ist,} \\ 0 & \text{sonst.} \end{cases}$$

Satz: Für beliebige f und g gilt:

(a) $\tau_0 * \mu = \delta$.

(b) $\tau_0 * f = g \iff f = \mu * g$.

Anwendung: Für die *Eulersche φ-Funktion* $\varphi(n) := \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$ gilt $\varphi \ = \ \mu * \tau_1$. Für $n = \prod_{i=1}^r p_i^{\nu_i}$ mit paarweise verschiedenen Primzahlen p_i und Exponenten $\nu_i \geqslant 1$ gilt also

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

Anwendung: Mit welcher Wahrscheinlichkeit sind zwei zufällige positive ganze Zahlen teilerfremd? Das heisst: Bestimme das asymptotische Verhalten für $N \to \infty$ der Grösse

$$\frac{1}{N^2} \cdot \left| \left\{ (m,n) \in \mathbb{Z}^2 \;\middle|\; \begin{array}{c} 1 \leqslant m,n \leqslant N \\ \operatorname{ggT}(m,n) = 1 \end{array} \right\} \right|.$$

Anwendung: Sei k ein endlicher Körper der Ordnung q. Für jedes $d \geqslant 1$ ist die Anzahl der irreduziblen normierten Polynome vom Grad d in $k[X]$ gleich

$$\frac{1}{d} \cdot \sum_{e|d} \mu(\tfrac{d}{e}) \cdot q^e \ > \ 0.$$

Folge: Für jede Primpotenz p^n existiert ein endlicher Körper der Ordnung p^n.

Anwendung: Für $n \geqslant 1$ betrachte die Polynome

$$F_n(X) \;:=\; \prod_{k \in \mathbb{Z}/n\mathbb{Z}} \big(X - e^{\frac{2\pi i k}{n}}\big),$$

$$\Phi_n(X) \;:=\; \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \big(X - e^{\frac{2\pi i k}{n}}\big).$$

Das Polynom Φ_n heisst das *n-te zyklotomische Polynom.*

Proposition: Für alle $n \geqslant 1$ gilt:

(a) $F_n(X) = X^n - 1$.

(b) $F_n(X) = \prod_{d|n} \Phi_d(X)$.

(c) $\Phi_n(X) = \prod_{d|n} F_d(X)^{\mu(\frac{n}{d})}$.

(d) $\Phi_n(X) \in \mathbb{Z}[X]$.

(e) $\Phi_n(X)$ ist irreduzibel über $\mathbb{Q}$. (ohne Beweis)