

# Kombinatorik und Graphentheorie

Skript nach der Vorlesung von Ernst-Ulrich Gekeler im SS 2009  
(im Wesentlichen aufgeschrieben von Ralf Krömer,  
wobei Ergänzungen im letzten Kapitel (nach den Anweisungen des Dozenten)  
und Korrekturen von Bernd Mehnert vorgenommen wurden)

7. Dezember 2011

# Inhaltsverzeichnis

0	Was ist Kombinatorik?	3
1	Einige Existenzsätze	6
2	Ordnung im Chaos	17
3	Was heißt Zählen?	28
4	Elementare Zählprobleme	34
5	Die Siebformel	41
6	Permutationen	47
7	Der zwölfwache Weg	55
8	Partitionen	58
9	Mehr über Permutationen	71
10	Graphen und Untergraphen	82
11	Abzählansagen über Graphen	94
12	Polya-Abzählung	100
13	Etwas algebraische Graphentheorie	108

## 0 Was ist Kombinatorik?

Eine sehr allgemeine Definition der Kombinatorik ist die folgende: Kombinatorik ist die Lehre vom Arrangement von (diskreten, z.B. endlichen) Mengen unter Nebenbedingungen. Der Begriff "Arrangement" bleibt hierbei recht unbestimmt; gemeint sind solche Dinge wie Abbildungen, Zerlegungen einer Menge in Teilmengen, Systeme von Teilmengen mit Überlappungseigenschaften etc.

Die Hauptfragen der Kombinatorik sind:

- (1) Gibt es Arrangements einer bestimmten Form?
- (2) Wie viele Arrangements einer bestimmten Form gibt es?
- (3) Wie findet bzw. konstruiert man solche Arrangements?

Konkrete Beispiele sind etwa:

Zu (1): Seien  $n \geq k \geq r$  natürliche Zahlen. Gibt es in  $\mathbb{N}_n := \{1, 2, \dots, n\}$  ein System von Teilmengen  $\mathcal{S} = \{S_i\}$ , so daß gilt:

- jedes  $S_i$  hat  $k$  Elemente;
- jede Teilmenge  $T$  von  $\mathbb{N}_n$  mit  $r$  Elementen ist in genau einem  $S_i$  enthalten?

(Solche  $\mathcal{S}$  heißen Steiner-Systeme. Ihre Existenz hängt stark von der Natur von  $(n, k, r)$  ab.)

Zu (2): Wieviele Steiner-Systeme vom Typ  $(n, k, r)$  gibt es?

- Ist  $\pi$  eine Permutation von  $\mathbb{N}_n$  und  $\mathcal{S}$  ein Steiner-System vom Typ  $(n, k, r)$ , so auch

$$\pi(\mathcal{S}) := \{\pi(S_i)\}$$

(man überlege sich dies). Also: Wenn es überhaupt Steiner-Systeme eines gegebenen Typs gibt, dann sehr viele.

- Ferner stellt sich die Frage: Sind  $\mathcal{S}, \mathcal{S}'$  Steiner-Systeme vom Typ  $(n, k, r)$ , existiert dann ein  $\pi$  mit  $\mathcal{S}' = \pi(\mathcal{S})$ ?

Zu (3): Finde zu gegebenem  $(n, k, r)$  ein Steiner-System!

(Manchmal sagt uns (1), z.B. durch Abzählargumente oder Kongruenzüberlegungen, daß eine Struktur des gesuchten Typs existieren muß; dies muß aber noch nicht heißen, daß es auf der Hand liegt, wie man eine solche Struktur auch angeben kann.)

Entsprechend unterscheidet man die drei Hauptzweige der Kombinatorik:

- (1) Existenzfragen
- (2) Abzählende Kombinatorik
- (3) Konstruktive Kombinatorik

Es sollte klar sein (und wird sich im Laufe der Vorlesung in Übungsaufgaben niederschlagen), daß alle Aspekte der Kombinatorik stark anwendungsorientiert sind. Wir werden uns hauptsächlich, nach einem kurzen Abstecher zum Zweig (1), mit dem Zweig (2) beschäftigen. Der Zweig (3) bezieht seine Hilfsmittel hauptsächlich aus Zahlentheorie, projektiver und algebraischer Geometrie und wird in der Vorlesung keine Rolle spielen. Trotzdem noch das

*Beispiel:* Seien  $q$  eine Primzahl,  $n = \frac{q^{l+1}-1}{q-1}$  für eine natürliche Zahl  $l \geq 2$  und  $k = q+1$ . Dann können wir  $(n, k, 2)$ -Steiner-Systeme wie folgt konstruieren: Seien

$$\begin{aligned} \mathbb{F}_q &:= \mathbb{Z}/q\mathbb{Z} \quad \text{der Körper mit } q \text{ Elementen,} \\ V &:= \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{l+1 \text{ Faktoren}}, \\ X &:= (V - \{0\})/\mathbb{F}_q^* \quad (= \mathbb{P}^l(\mathbb{F}_q)) \\ &= \text{Menge der Nullpunktsgersten in } V. \end{aligned}$$

$X$  hat  $n = \frac{q^{l+1}-1}{q-1}$  Elemente und ist die Trägermenge unseres Steiner-Systems. Jedes  $h \in X$  entspricht einer Nullpunktsgersten in  $V$ . Wir setzen

$$\mathcal{S} := \left\{ \begin{array}{l} S \subset X \text{ der Form: } S = (U - \{0\})/\mathbb{F}_q^*, \text{ wobei } U \subset V \\ \text{ein zweidimensionaler Untervektorraum ist} \end{array} \right\}.$$

- Man verifiziere, daß  $\mathcal{S}$  ein  $(n, k, 2)$ -Steiner-System ist!
- Wieviele  $S \in \mathcal{S}$  gibt es?
- Es genügt, daß  $q$  eine *Primzahlpotenz* ist.

Das Beispiel macht klar, wieso wir vorläufig von Konstruktionsfragen die Finger lassen.

Graphentheorie wird in der Vorlesung in doppelter Weise auftreten: Einerseits stellen sich beim Arbeiten mit Graphen viele Fragen kombinatorischer Art (z.B.: Wie viele Graphen eines bestimmten Typs gibt es?); andererseits werden wir im letzten Drittel der Vorlesung die Anfangsgründe einer Strukturtheorie von Graphen besprechen, verschiedene Invarianten von Graphen einführen und deren Beziehungen studieren.

Die Kombinatorik hat eine ganz andere Struktur als diejenigen mathematischen Disziplinen, die dem durchschnittlichen Hörer bisher begegnet sein werden, also lineare Algebra, Analysis, Funktionentheorie etc. In jenen Gebieten ist jeweils von der Natur der Sache eine klare Ordnung der Inhalte vorgegeben. Man geht aus von Grundstrukturen (z.B. Vektorraum, lineare Abbildung etc.), untersucht deren Eigenschaften, erhält verhältnismäßig wenige substantielle Hauptsätze, deren Anwendung dann (hoffentlich) die jeweils untersuchten Probleme löst.

Die innere Ordnung der Kombinatorik dagegen ist eher diffus; es gibt keine klare Reihenfolge der Darstellung, sehr viel mehr “elementare” Begriffe und keine “alles erschlagenden” Hauptsätze (wie etwa die Existenz einer Jordanschen Normalform in der linearen Algebra oder Cauchy’sche Integralformel und Residuensatz in der Funktionentheorie). Die Beweise in der Kombinatorik sind im allgemeinen wesentlich kürzer als in Algebra, Analysis etc.; man nimmt weniger “Anlauf” durch vorgelagerte Aussagen. Dies macht die Kombinatorik aber nicht unbedingt “leichter”: Man ist stärker auf *ad-hoc*-Konstruktionen, Einfälle, Tricks und dergleichen angewiesen als in den intern stärker strukturierten Disziplinen, deren Beweise oft einen bürokratisch-gewaltsamen Eindruck machen. Demgegenüber finden sich in den Beweisen der Kombinatorik viele Perlen der Mathematik, die ästhetisch besonders reizvoll sind (so man eine für solche Reize empfängliche Natur besitzt). Man könnte sagen:

Die Kombinatorik ist eher Kunst als Wissenschaft.
---

Aus dem Gesagten ergibt sich, daß es für die Kombinatorik keine “verbindliche” Darstellung gibt; es gibt so viele verschiedene Konzeptionen für Lehrbücher (und so viele verschiedene Notationen!) wie Autoren. Aus diesem Grund ist auch der Dozent dieser Vorlesung mit keinem der vorliegenden Textbücher voll einverstanden — d.h. es gibt kein einzelnes Buch, an das sich die Vorlesung in Struktur und Inhalt einigermaßen eng anlehnte. Zur *begleitenden* Lektüre empfehle ich dessen ungeachtet die folgenden Bücher. Sie werden die meisten in der Vorlesung angesprochenen Themen in irgendeinem dieser Bücher behandelt finden, jedoch zuweilen in anderer Darstellung und Notation.

Biggs, *Algebraic Graph Theory*, Cambridge University Press.

Bollobas, *Graph Theory*, Springer.

Bona, *A Walk Through Combinatorics*, World Scientific.

Charalambides, *Enumerative Combinatorics*, Chapman & Hall.

Erickson, *Introduction to Combinatorics*, John Wiley & Sons.

Godsil-Royle, *Algebraic Graph Theory*, Springer.

Stanley, *Enumerative Combinatorics I*, Cambridge University Press.

Wilf, *generatingfunctionology*, Academic Press.

## 1 Einige Existenzsätze

**Satz 1.1. (Schubfachprinzip):** Ist  $f : A \rightarrow B$  eine Abbildung mit endlichen Mengen  $A, B$ , so gelten:

$$\begin{aligned} (i) \quad & \text{Es existiert } b \in B \quad \text{mit} \quad |f^{-1}(b)| \geq \frac{|A|}{|B|}; \\ (ii) \quad & \text{,,} \quad b' \in B \quad \text{mit} \quad |f^{-1}(b')| \leq \frac{|A|}{|B|}. \end{aligned}$$

*Beweis.* Klar! □

Dieses Prinzip macht einen fast primitiven Eindruck, hat aber, wie wir gleich sehen werden, zahlreiche interessante Anwendungen.

**Beispiel 1.2.** Sei  $X$  eine  $n$ -Menge (d.h.  $|X| = n$ ) mit  $t$  Teilmengen  $U_1, \dots, U_t$ , so daß gilt  $|U_i| = k$  für  $1 \leq i \leq t$ . Können wir ein  $x \in X$  finden, das in möglichst vielen der  $U_i$  liegt?

*Numerisches Beispiel:*  $n = 15, k = 8, t = 4$ ; Lösung: Es läßt sich in jedem Fall ein  $x$  angeben, das in 3 der 4 Teilmengen liegt. (Man überzeuge sich hiervon!)

Zur allgemeinen Lösung dieser Fragestellung legen wir zunächst folgende (in der gesamten Vorlesung verwendete) Bezeichnungsweise fest:  $\mathbb{N}_t$  soll die Menge  $\{1, \dots, t\}$  bezeichnen. Definiere nun

$$A := \{(x, i) \in X \times \mathbb{N}_t \mid x \in U_i\}$$

und eine Abbildung  $f : A \rightarrow X$  durch  $(x, i) \mapsto x$  (Projektion auf die erste Komponente). Es gilt  $|A| = k \cdot t$  und  $|X| = n$ ; damit ergibt eine Anwendung des Schubfachprinzips:

$$\exists x \in X \quad \text{mit} \quad |f^{-1}(x)| \geq \frac{k \cdot t}{n}.$$

Im numerischen Beispiel ergibt diese Formel den behaupteten Wert 3.

**Beispiel 1.3. Erinnerung:** Für  $p_i = (x_i, y_i) \in \mathbb{R}^2, 1 \leq i \leq 3$  heißt  $s = \left(\frac{x_1+x_2+x_3}{3}, \frac{y_1+y_2+y_3}{3}\right)$  der Schwerpunkt von  $\{p_1, p_2, p_3\}$ .

*Behauptung:* Ist  $S \subset \mathbb{Z}^2 \subset \mathbb{R}^2$  eine Menge mit mindestens  $n$  Elementen, so existiert eine Teilmenge  $T \subset S$  mit 3 Elementen, so daß der Schwerpunkt von  $T$  wieder ganzzahlig ist (d.h. in  $\mathbb{Z}^2$  liegt), falls  $n \geq 13$ .

*Beweis.* (i) Ist  $g : A \rightarrow B$  eine Abbildung,  $|A| = 5$ ,  $|B| = 3$ , so ist  $g$  entweder surjektiv, oder es existiert  $b \in B$  mit  $|f^{-1}(b)| \geq 3$ . Dies ergibt sich aus dem Schubfachprinzip.

(ii) Sei in der Situation der Behauptung o.B.d.A.  $|S| = 13$ . Definiere

$$\begin{aligned} f : S &\rightarrow \{0, 1, 2\} \\ p = (x, y) &\mapsto \text{Repräsentant von } x \bmod 3 \text{ in } \{0, 1, 2\} \end{aligned}$$

Wegen  $13/3 > 4$  existieren nach dem Schubfachprinzip 5 Elemente von  $S$  mit demselben Bild unter  $f$ ; o.B.d.A. seien dies  $p_1, \dots, p_5$ .

(iii) Seien  $A = \{p_1, \dots, p_5\}$  und  $B = \{0, 1, 2\}$ , und sei  $g : A \rightarrow B$  diejenige Abbildung, die  $(x, y)$  auf den Repräsentanten von  $y \bmod 3$  in  $\{0, 1, 2\}$  abbildet. Mit (i) folgt, daß es in  $A$  drei Elemente gibt, deren  $y$ -Komponenten entweder alle inkongruent sind (d.h.  $g$  ist surjektiv) oder alle kongruent (da es ein  $b \in B$  gibt mit  $|g^{-1}(b)| \geq 3$ ). In *beiden* Fällen ist die Summe dieser Komponenten durch 3 teilbar!

(ii) und (iii) ergeben zusammen die Behauptung. □

Mit 12 statt 13 geht *dieser* Beweis nicht mehr; dennoch gilt folgende

*Bemerkung:*  $n = 13$  ist nicht minimal mit diesen Eigenschaften; vielmehr ist  $n = 9$  die kleinste derartige Zahl. (Zum Beweis verwendet man die Menge  $\mathbb{P}^2(\mathbb{F}_3)$ ; diese hat 13 Elemente, die in bestimmter Weise angeordnet sind.)

**Beispiel 1.4.** (Eine Anwendung des Schubfachprinzips auf diophantische Approximation.)

*Behauptung:* Sind  $x \in \mathbb{R}$  und  $n \in \mathbb{N}$ , so existieren ein Zähler  $r \in \mathbb{Z}$  und ein Nenner  $s \in \mathbb{N}$ ,  $1 \leq s \leq n$ , mit der Eigenschaft

$$\left| x - \frac{r}{s} \right| < \frac{1}{s \cdot n}.$$

(Die Abschätzung ist schärfer als die auf der Hand liegende Abschätzung mit  $1/n$ .)

*Beweis.* Zerlege  $[0, 1)$  in  $[0, \frac{1}{n}) \cup [\frac{1}{n}, \frac{2}{n}) \cup \dots \cup [\frac{n-1}{n}, 1)$  und betrachte die Funktion

$$\begin{aligned} f : \mathbb{N}_{n+1} &\rightarrow \left\{ \left[ \frac{i}{n}, \frac{i+1}{n} \right) \mid 0 \leq i \leq n-1 \right\} \\ j &\mapsto \text{Dasjenige Teilintervall von } [0, 1), \text{ das } jx - [jx] \text{ enthält.} \end{aligned}$$

(Es wird daran erinnert, daß  $[y]$  den *ganzzahligen Teil* der reellen Zahl  $y$  bezeichnet.) Nach dem Schubfachprinzip gibt es ein  $j < k$  in  $\mathbb{N}_n$  mit  $f(j) = f(k)$ , d.h.

$$\frac{1}{n} > |jx - [jx] - (kx - [kx])| = |(j - k)x - [jx] + [kx]|. \quad (*)$$

Setze  $s := k - j$  und  $r := [jx] - [kx]$ ; der Ausdruck rechts bei  $(*)$  ist also gleich  $|sx - r|$ . Es gilt  $r \in \mathbb{Z}$ ,  $s \in \mathbb{N}_n$  und insgesamt

$$\frac{1}{sn} > \left| x - \frac{r}{s} \right|.$$

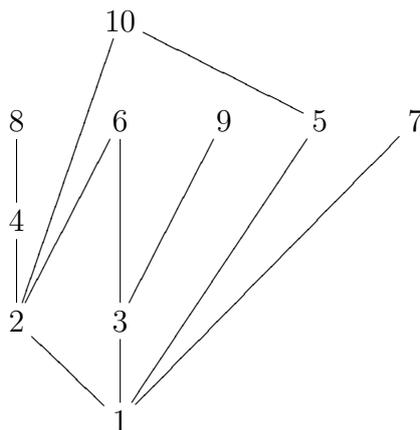
□

*Numerisches Beispiel:* Seien  $x = \pi$  und  $n = 10$ . Mit  $\frac{r}{s} = \frac{22}{7}$  ist in der Tat  $|\pi - \frac{22}{7}| < \frac{1}{70}$ . (Solche Näherungen für  $\pi$  sind seit der Antike bekannt. Literaturhinweis: Berggren, Lennart; Borwein, Jonathan; Borwein, Peter, *Pi: a source book*. Second edition. Springer 2000.)

**Definition 1.5.** *Es sei  $X$  oder genauer  $(X, \leq)$  eine geordnete Menge. (Unter “geordnet” wird in dieser Vorlesung stets “partiell geordnet” verstanden.) Eine Kette in  $X$  ist eine vollständig geordnete Teilmenge; eine Antikette ist eine Teilmenge, in der je zwei Elemente unvergleichbar sind.*

*Die Länge von  $X$  ist  $l(X) := \sup_Y \text{Kette} |Y|$ , die Weite ist  $w(X) := \sup_Y \text{Antikette} |Y|$ .*

*Beispiel:* Sei  $X = (\mathbb{N}_{10}, |)$ ; es ist also auf  $\mathbb{N}_{10}$  folgende Ordnungsrelation gegeben:  $a|b \Leftrightarrow a$  ist Teiler von  $b$ . Es ergibt sich folgendes Hasse-Diagramm:



Eine Kette ist  $\{1, 2, 4, 8\}$ , eine Antikette  $\{5, 6, 7, 8, 9\}$ ; diese sind jeweils maximal (d.h. man kann sie nicht vergrößern, ohne die Ketten- bzw. Antiketteneigenschaft zu verletzen), und es gilt sogar  $l(X) = 4$  sowie  $w(X) = 5$  (man überzeuge sich hiervon).

**Proposition 1.6** (Dilworth's Lemma). *Ist  $X$  eine geordnete Menge, so gelten:*

(i) *Falls  $|X| = mn + 1$  für bestimmte  $m, n \in \mathbb{N}$ , so existiert in  $X$  eine Kette mit  $m + 1$  Elementen oder eine Antikette mit  $n + 1$  Elementen<sup>1</sup>.*

(ii)  $|X| \leq l(X) \cdot w(X)$ .

*Beweis.* Zu (i): Angenommen, es existiert keine Kette mit  $m + 1$  Elementen. Dann ist durch

$$x \mapsto \sup\{l(Y) \mid Y \subset X \text{ Kette; } x \text{ maximal in } Y\}$$

eine Abbildung  $f : X \rightarrow \mathbb{N}_m$  gegeben. (*Bemerkung:* Da das Supremum ausschließlich über Ketten gebildet wird, kann man statt  $l(Y)$  ebensogut  $|Y|$  setzen.) Nach dem Schubfachprinzip existieren  $y_1, \dots, y_{n+1}$  mit demselben Bild unter  $f$ , da  $\frac{|X|}{|\mathbb{N}_m|} = n + \frac{1}{m}$  ist. Diese  $y_1, \dots, y_{n+1}$  bilden eine Antikette mit  $n + 1$  Elementen.

Zu (ii): Wäre  $|X| > l(X) \cdot w(X)$ , so gäbe es nach (i) entweder eine Kette mit einer Länge  $> l(X)$  oder eine Antikette mit einer Länge  $> w(X)$ , was jeweils der Definition der Ausdrücke  $l(X)$  bzw.  $w(X)$  widerspricht.  $\square$

**Beispiel 1.7.** In  $\mathbb{N}_n$  existieren mindestens  $\frac{n}{1+\log_2 n}$  Zahlen, die einander paarweise nicht teilen.

*Beweis.* Sei dazu  $k := \lceil \log_2 n \rceil$ ; es gilt also  $2^k \leq n < 2^{k+1}$ . Dann ist  $\{1, 2, 2^2, \dots, 2^k\}$  eine Kette in  $(\mathbb{N}_n, |)$ , und zwar eine maximale Kette der maximalen Länge  $k + 1 = l(\mathbb{N}_n)$  (denn jede andere maximale Kette kann nur kürzer sein, da die auftretenden Zahlen größer werden). Es gilt also nach 1.6.(ii)

$$w(\mathbb{N}_n) \geq \frac{n}{k + 1} .$$

$\square$

**Satz 1.8** (Dilworth). *Sei  $X$  eine endliche geordnete Menge mit Länge  $l$  und Weite  $w$ . Dann kann  $X$  disjunkt zerlegt werden in*

(i)  $l$  Antiketten;

(ii)  $w$  Ketten.

*Beweis.* Zu (i): Sei

$$\begin{aligned} f : X &\rightarrow \mathbb{N}_l \\ x &\mapsto \sup\{l(Y) \mid Y \subset X \text{ Kette; } x \text{ maximal in } Y\} . \end{aligned}$$

---

<sup>1</sup>und damit wegen  $mn = nm$  natürlich auch eine Kette mit  $n + 1$  Elementen oder eine Antikette mit  $m + 1$  Elementen; ferner ist die Zerlegung  $|X| = m \cdot n + 1$  für gegebenes  $X$  nicht automatisch eindeutig.

Dann ist  $f$  surjektiv, und jedes Urbild  $f^{-1}(i)$  ( $i \in \mathbb{N}_l$ ) ist eine Antikette.

Zu (ii): Der Beweis wird durch Induktion nach  $n = |X|$  geführt. Für  $n = 1$  ist nichts zu zeigen; seien also  $n > 1$  und  $X$  mit  $n = |X|$  gegeben, und die Behauptung gelte für  $n' < n$ . O.B.d.A. enthalte  $X$  keine isolierten Elemente. (Erinnerung: ein Element  $x$  einer geordneten Menge  $X$  heißt isoliert, wenn es minimal und maximal zugleich ist, also wenn einerseits für jedes  $y \in X$  aus  $y \leq x$  folgt, daß  $y$  gleich  $x$  ist, und andererseits für jedes  $z \in X$  aus  $x \leq z$  folgt, daß  $x$  gleich  $z$  ist.) Wir unterscheiden zwei Fälle:

*Fall a):*  $X$  besitzt eine  $w$ -Antikette  $Y$  (d.h.  $|Y| = w$ ), die sowohl nicht-minimale als auch nicht-maximale Elemente enthält. Definiere

$$\begin{aligned} U &:= \{u \in X \mid \exists y \in Y \text{ mit } u \not\leq y\}; \\ V &:= \{v \in X \mid \exists y \in Y \text{ mit } v \not\geq y\}. \end{aligned}$$

Wir stellen einige Eigenschaften dieser Mengen zusammen.

- Es gilt  $U \neq \emptyset$  und  $V \neq \emptyset$  (hier geht die Voraussetzung des Falls  $a$ ) ein);
- $U, V, Y$  sind paarweise disjunkt (dies ist für  $U, Y$  und  $V, Y$  klar; für  $U, V$  ergibt es sich aus der Transitivität);
- $X = U \dot{\cup} Y \dot{\cup} V$ ;
- $w(U \cup Y) = w = |Y|$ ;  
 $w(V \cup Y) = w = |Y|$ .

Außerdem ist sowohl  $|U \cup Y|$  als auch  $|V \cup Y| < n$ ; nach Induktionsvoraussetzung besitzen also  $U \cup Y$  und  $V \cup Y$  disjunkte Zerlegungen in  $w$  Ketten;  $C_1, \dots, C_w$  bzw.  $D_1, \dots, D_w$ . Die minimalen Elemente der  $C_1, \dots, C_w$  sind genau die Elemente von  $Y$ , die maximalen Elemente der  $D_1, \dots, D_w$  ebenso. Nach evtl. Ummummerierung der  $D_i$  (so dass gilt  $\min(C_i) = \max(D_i)$ ) ist  $X = \dot{\cup}_{1 \leq i \leq w} (C_i \cup D_i)$  die gesuchte Zerlegung. *Fall b):* Alle maximalen Antiketten mit  $w$  Elementen enthalten nur minimale oder nur maximale Elemente. Ein derartiges  $Y$  muß aus *allen* minimalen bzw. maximalen Elementen von  $X$  bestehen (denn zwei minimale Elemente sind unvergleichbar, ebenso zwei maximale); o.B.d.A. bestehe  $Y$  aus allen maximalen Elementen von  $X$ . Sei  $x \in X$  ein minimales Element. Da  $x$  nicht isoliert ist, existiert ein  $y \in Y$  mit  $x < y$ . Sei  $X' := X - \{x, y\}$ . Dann ist natürlich  $|X'| = |X| - 2$  und außerdem  $w(X') = w - 1$  (da nach den Voraussetzungen des Falls  $b$ )  $Y \cap X' = Y - \{y\}$  die Weite von  $X'$  realisiert). Daher läßt sich die Induktionsvoraussetzung anwenden: es ist  $X'$  disjunkte Vereinigung von  $w - 1$  Ketten. Demnach ist  $X = X' \cup \{x, y\}$  disjunkte Vereinigung von  $w$  Ketten.  $\square$

**Definition 1.9.** Ein Graph  $G$  ist ein geordnetes Paar  $(V, E)$  von Mengen, bestehend aus einer nichtleeren Menge  $V$  (der Knotenmenge) und einer Teilmenge  $E \subset \mathfrak{P}_2(V)$ . Wir benutzen auch die Schreibweisen  $V(G)$  bzw.  $E(G)$  für die beiden Mengen.

Erinnerung: *Es bezeichnen*

$\mathfrak{P}(V)$  die Potenzmenge einer Menge  $V$  (also die Menge all ihrer Teilmengen) und

$\mathfrak{P}_k(V)$  die Menge aller  $k$ -elementigen Teilmengen von  $V$ .

Ist  $|V| < \infty$ , so gilt  $\mathfrak{P}(V) = \bigcup_{0 \leq k \leq |V|} \mathfrak{P}_k(V)$ .

Die Elemente  $\{x, y\}$  von  $E$  (mit  $x, y \in V$ ) heißen Kanten, und  $x, y \in V$  heißen benachbart (oder verbunden oder Nachbarn), falls  $\{x, y\} \in E$ .

Zwei Graphen  $G = (V, E), G' = (V', E')$  heißen isomorph (in Zeichen  $G \cong G'$ ), falls eine Bijektion  $f : V \rightarrow V'$  existiert mit

$$\forall x, y \in V : \{x, y\} \in E \Leftrightarrow \{f(x), f(y)\} \in E' .$$

Die Kardinalität  $|V|$  heißt die Ordnung von  $G$ .

Spezielle Graphen sind:

$K_n$ : der vollständige Graph auf  $\mathbb{N}_n$  für  $n \in \mathbb{N}$ ,  
d.h.  $V(K_n) = \mathbb{N}_n$  und  $E(K_n) = \mathfrak{P}_2(\mathbb{N}_n)$ .

$C_n$ : der zyklische Graph auf  $\mathbb{N}_n$  für  $n \in \mathbb{N}, n \geq 3$ ,  
d.h.  $V(C_n) = \mathbb{N}_n$  und  $E(C_n) = \{\{i, i+1\} \mid 1 \leq i \leq n-1\} \cup \{\{n, 1\}\}$ .

$P_n$ : der Weg der Länge  $n$  für  $n \in \mathbb{N}$ ,  
d.h.  $V(P_n) = \mathbb{N}_n$  und  $E(P_n) = E(C_n) - \{\{n, 1\}\}$ .

$G = (V, E)$  heißt bipartit, falls eine disjunkte Zerlegung  $V = V_1 \dot{\cup} V_2$  existiert mit der Eigenschaft

$$\{x, y\} \in E \Rightarrow x \in V_1, y \in V_2 \text{ oder } x \in V_2, y \in V_1 .$$

Ein Untergraph  $G'$  von  $G$  ist ein Graph  $(V', E')$  mit  $V' \subset V(G)$  und  $E' \subset E(G)$ . Ist  $G'$  Untergraph von  $G$ , so heißt  $G'$  induziert, falls sogar gilt:

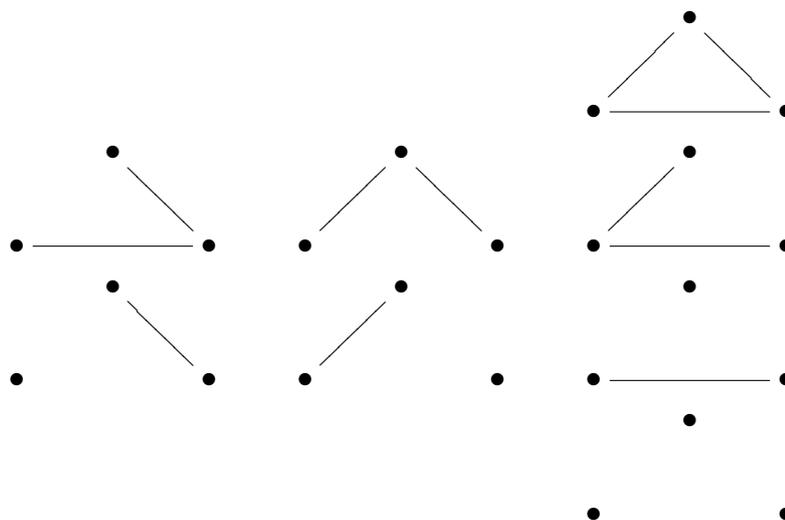
$$\forall x, y \in V(G') : \{x, y\} \in E(G') \Leftrightarrow \{x, y\} \in E(G) .$$

Ein induzierter Untergraph ist also vollständig bestimmt durch den Graphen, als dessen Untergraph er aufgefaßt wird, und durch seine Knotenmenge.

Ist  $p \in \mathbb{N}$  mit  $p \leq |V(G)|$ , so heißt ein Untergraph  $C$  von  $G$  mit  $C \cong K_p$  eine  $p$ -Clique in  $G$ .  $C$  ist automatisch induziert.

*Bemerkung:* Diese lange Definition ist von grundlegender Bedeutung für die gesamte Vorlesung; insbesondere sei angemerkt, daß in vielen Büchern leicht abweichende, nicht notwendig äquivalente Definitionen von Graphen gegeben werden, für die die Resultate bzw. Beweise der Vorlesung nicht unbedingt richtig sind.

Wir repräsentieren Graphen häufig durch eine Figur, bei der für jedes  $x \in V$  ein Punkt gezeichnet wird und Punkte verbunden werden, falls die zugehörigen  $x, y$  benachbart sind. Sei z.B.  $V = \{1, 2, 3\} = \mathbb{N}_3$ ; die Graphen  $G$  mit  $V(G) = V$  sind dann (sortiert nach Isomorphieklassen)



Allgemein gilt: Es gibt  $\binom{k}{2}$  Elemente von  $\mathfrak{P}_2(\mathbb{N}_k)$ , und die Angabe eines Graphen  $G$  mit  $V(G) = \mathbb{N}_k$  ist gleichbedeutend mit der Auszeichnung einer bestimmten Teilmenge von  $\mathfrak{P}_2(\mathbb{N}_k)$ . Daher gibt es  $2^{\binom{k}{2}}$  solche Graphen  $G$ .

Es ist weitaus schwieriger, zu entscheiden, wie viele Isomorphieklassen von Graphen einer gegebenen Ordnung existieren. Wir werden im Laufe der Vorlesung nicht zu exakten Formeln gelangen, wohl aber zu Abschätzungen.

Wir werden uns nun mit dem Finden von Cliques in einem gegebenen Graphen beschäftigen. Dies ist in der Praxis häufig eine wichtige Fragestellung in solchen Situationen, die man als (i.a. sehr große) Graphen auffassen kann (z.B. Telefon- oder Computernetzwerke). Wir notieren zunächst:  $G$  mit  $|V(G)| = n$  hat höchstens  $\binom{n}{2} = \frac{n(n-1)}{2} \approx \frac{n^2}{2}$  Kanten.

**Satz 1.10. (Turán 1941)** Sei  $G$  ein Graph der Ordnung  $n$  mit

$$|E(G)| > \left(\frac{p-2}{p-1}\right) \frac{n^2}{2} .$$

Dann existiert in  $G$  eine  $p$ -Clique.

Sei z.B.  $p = 3$ ; der Satz besagt dann: Für  $|E| > \frac{n^2}{4}$  existieren Dreiecke in  $G$ .

Die Konstanten sind im wesentlichen scharf (d.h. für große  $n$  lassen sich Graphen mit wenig kleinerem  $|E(G)|$  finden, die keine  $p$ -Cliques besitzen).

*Beweis.* O.B.d.A. sei  $V = \mathbb{N}_n$ .

(i) Eine *Wahrscheinlichkeitsverteilung* (kurz: W-Verteilung) auf  $V$  ist ein Vektor

$$\underline{w} := (w_1, \dots, w_n) \in \mathbb{R}_{\geq 0}^n \quad \text{mit} \quad \sum_{1 \leq i \leq n} w_i = 1 .$$

Wir ordnen jedem  $\underline{w}$  die Zahl

$$f(\underline{w}) = \sum_{\{k,l\} \in E(G)} w_k w_l$$

zu. Die Funktion  $f$  auf der Menge aller W-Verteilungen besitzt ein Maximum, da  $f$  stetig ist und die besagte Menge kompakt (denn sie ist als Teilmenge des Einheitskubus beschränkt und als Hyperebene abgeschlossen).

(ii) Annahme:  $G$  besitze keine  $p$ -Clique. Zu zeigen ist also  $|E(G)| \leq \binom{p-2}{p-1} \frac{n^2}{2}$ . Für  $\underline{w}$  wie oben,  $i, j \in \mathbb{N}_n$ ,  $\{i, j\} \notin E$  und  $w_i, w_j \neq 0$  seien

$$s_i := \sum_{k \text{ mit } \{k,i\} \in E} w_k ; \quad s_j := \sum_{k \text{ mit } \{k,j\} \in E} w_k .$$

Sei o.B.d.A.  $s_j \leq s_i$  (andernfalls numeriert man um). Setze

$$\underline{w}' := (w'_1, \dots, w'_n) \quad \text{mit} \quad \begin{cases} w'_k := w_k, & \text{falls } k \neq i, j ; \\ w'_i := w_i + w_j ; \\ w'_j := 0 . \end{cases}$$

(Es liegt auf der Hand, daß sich wieder eine W-Verteilung ergibt. Die Strategie besteht darin, das Gewicht auf immer weniger Knoten zu konzentrieren;  $\underline{w}'$  hat eine echt kleinere Trägermenge — d.h. Menge der Knoten mit positivem Gewicht — als  $\underline{w}$ ).

(iii) Es ist

$$\begin{aligned} f(\underline{w}') &= f(\underline{w}) + w_j \cdot s_i - w_j \cdot s_j = f(\underline{w}) + w_j(s_i - s_j) \\ &\geq f(\underline{w}) . \end{aligned}$$

(iv) Diesen Prozeß des Änderns von  $\underline{w}$  zu  $\underline{w}'$  bei Verkleinern der Trägermenge und eventuellem Vergrößern von  $f$  können wir solange durchführen, wie es möglich ist, nicht benachbarte  $i, j \in \mathbb{N}_n$  zu finden, für die  $w_i, w_j > 0$  gilt (wir schreiben hier wieder  $\underline{w}$  für die

aus einem Schritt des Prozesses hervorgehende  $W$ -Verteilung). Bricht der Prozeß ab, so ist  $\underline{w}$  konzentriert auf einer  $k$ -Clique  $C$  in  $G$  mit einem gewissen  $k$  (weil jetzt alle Knoten der Trägermenge benachbart sind).

(v) Das Maximum von  $f$  wird angenommen für solche  $\underline{w}$ , die auf einer Clique konzentriert sind (allerdings möglicherweise nicht *nur* für solche). Ein solches  $\underline{w}$  sei gewählt.

(vi) *Behauptung:* Es gilt  $w_i = \begin{cases} \frac{1}{k}, & \text{falls } i \in V(C); \\ 0, & \text{falls } i \notin V(C). \end{cases}$

*Beweis der Behauptung:* Zu zeigen ist nur, daß in  $C$  alle  $w_i$  gleich sind. Wäre aber z.B.  $w_i > w_j > 0$  für  $i \neq j, i, j \in V(C)$ , so definiere  $\underline{w}'$  durch  $w'_k := w_k$ , falls  $k \in V(C)$  von  $i$  und  $j$  verschieden ist, und  $w'_i = w'_j := \frac{w_i + w_j}{2} = w_i - h = w_j + h$  mit  $h = \frac{w_i - w_j}{2}$ . Dann ist, wie unter (vii) nachgerechnet wird,  $f(\underline{w}') = f(\underline{w}) + h^2 > f(\underline{w})$  im Widerspruch zur Maximalität von  $f(\underline{w})$ .

(vii) Es ergibt sich

$$\begin{aligned}
f(\underline{w}') &= \sum_{\substack{\{k,l\} \in E(C) \\ \text{(d.h. } k,l \in V(C), \text{ da } C \text{ Clique)}}} w'_k \cdot w'_l \\
&= \sum_{\substack{\{k,l\} \\ \{k,l\} \cap \{i,j\} = \emptyset}} w_k w_l + \underbrace{\sum_{\substack{\{k,l\} \\ \{k,l\} \cap \{i,j\} = \{i\}}} w'_i w_l}_{\sum_{\substack{l \neq i,j \\ l \in V(C)}} (w_i - h) w_l} + \underbrace{\sum_{\substack{\{k,l\} \\ \{k,l\} \cap \{i,j\} = \{j\}}} w'_j w_l}_{\sum_{\substack{l \neq i,j \\ l \in V(C)}} (w_j + h) w_l} + \underbrace{w'_i w'_j}_{(w_i - h)(w_j + h)} \\
&= \sum_{\substack{\{k,l\} \\ k,l \in V(C)}} w_k w_l + (w_i - w_j)h - h^2 \\
&= f(\underline{w}) + h^2.
\end{aligned}$$

(viii) Also wird das Maximum von  $f$  angenommen in  $\underline{w}$  (definiert wie in (vi)), und es ist

$$f(\underline{w}) = \frac{k(k-1)}{2} \frac{1}{k^2} = \frac{k-1}{2k}.$$

(xi) Da nach Voraussetzung  $G$  keine  $p$ -Clique enthält, ist auf jeden Fall

$$\frac{k-1}{2k} = f(\underline{w}) \leq \frac{p-2}{2(p-1)}, \text{ da ja } k \leq p-1;$$

diese Ungleichung gilt mit der  $W$ -Verteilung, für die  $f$  das Maximum annimmt, natürlich auch für jede andere  $W$ -Verteilung, also insbesondere für  $\underline{w}^{(0)} = (\frac{1}{n}, \dots, \frac{1}{n})$ . Also ist

$$\frac{p-2}{2(p-1)} \geq f(\underline{w}^{(0)}) = |E| \cdot \frac{1}{n^2}$$

bzw.

$$|E| \leq \left( \frac{p-2}{p-1} \right) \frac{n^2}{2}.$$

□

*Bemerkungen:*

- Die Funktion  $f$  hat ein Maximum der Form  $\frac{k(k-1)}{2} \frac{1}{k^2} = \frac{k-1}{2k}$ , wobei in  $G$  eine  $k$ -Clique existiert; dabei ist  $k = k_{\max}$  sogar die *maximale* Ordnung einer Clique in  $G$  (die "Cliquenzahl").

- Für den Wert  $\left(\frac{|E|}{n^2}\right)$  von  $f$  auf der Gleichverteilung (alle Knoten haben Gewicht  $\frac{1}{n}$ ) gilt

$$\frac{|E|}{n^2} \leq \frac{k-1}{2k}. \quad (*)$$

- Ist also  $k$  *minimal* mit  $(*)$  (d.h.

$$\frac{k-2}{2(k-1)} < \frac{|E|}{n^2} \leq \frac{k-1}{2k} \Big),$$

so existiert eine  $k$ -Clique in  $G$ , die durch das Verfahren konstruiert wird (mit der Gleichverteilung als Startvektor), und zwar in  $n - k$  Schritten mit einer Gesamtkomplexität von  $\approx |E|$  Operationen. Jedoch hat die so konstruierte Clique nicht unbedingt maximale Ordnung. Es ist ein besonderer Vorzug des dargestellten Beweises, daß er *konstruktiv* ist — während durchaus noch *kürzere* Beweise bekannt sind.

- Satz 1.10 ist ein Beispiel eines Typs von Aussagen, wo eine quantitative Eigenschaft (hier: die Zahl der Kanten) auf eine qualitative Eigenschaft (hier: die Existenz einer  $p$ -Clique) schließen läßt.

Zum Schluß des Kapitels sei noch ein weiterer etwas komplexerer Existenzsatz bewiesen.

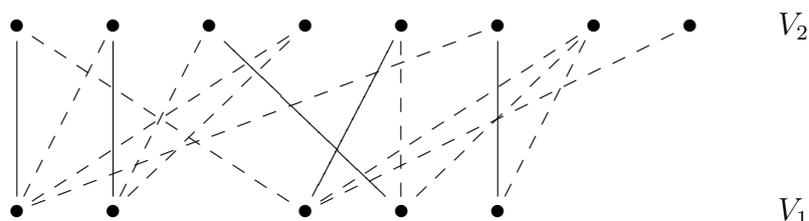
**Problem 1.11.** Gegeben seien eine endliche Menge  $X$  und ein System  $A_1, \dots, A_n$  von Teilmengen von  $X$ . Unter welchen Voraussetzungen können wir  $s_1, \dots, s_n \in X$  finden, für die gilt

(i) die  $s_i$  sind paarweise verschieden;

(ii)  $s_i \in A_i$  für  $1 \leq i \leq n$ ?

Eine derartige Menge  $\{s_1, \dots, s_n\}$  heie kurz ein *Repräsentantensystem* für  $A_1, \dots, A_n$ .

**Variante 1.12.** Es sei  $G = (V, E)$  ein bipartiter Graph mit Knotenmenge  $V = V_1 \dot{\cup} V_2$ . Unter welchen Voraussetzungen können wir für jedes  $x \in V_1$  eine Kante  $\{x, s(x)\}$ , ( $s(x) \in V_2$ ) finden, so daß gilt:  $x \neq y \Rightarrow s(x) \neq s(y)$ ? Die Wahl eines solchen Systems von Kanten heie ein *Matching* von  $V_1$  nach  $V_2$ .



Die Probleme 1.11 und 1.12 sind äquivalent. Betrachtet man nämlich in der Situation von 1.11 den bipartiten Graphen  $G = (V_1 \dot{\cup} V_2, E)$  mit  $V_1 = \mathbb{N}_n, V_2 = X$ , für den  $\{i, x\}$  mit  $i \in \mathbb{N}_n, x \in X$  genau dann eine Kante ist, wenn  $x \in A_i$ , so ist das Problem 1.11 gerade dasjenige, ein Matching von  $V_1$  nach  $V_2$  zu finden. Umgekehrt kann man das Matching-Problem 1.12 als die Suche nach einem Repräsentantensystem, also als ein Problem des Typs 1.11, formulieren (Übung!).

Man könnte das Matching-Problem folgendermaßen veranschaulichen: Seien  $V_1$  eine Menge von Frauen und  $V_2$  eine Menge von Männern, und bedeute das Vorhandensein einer Kante, daß die betreffende Frau mit dem betreffenden Mann bekannt ist. Das Problem ist dann das folgende: Unter welchen Voraussetzungen kann sich jede Frau unter ihren Bekannten einen Mann aussuchen, ohne daß es zu Konflikten kommt?<sup>2</sup> Von dieser Veranschaulichung hat der folgende Satz seinen Namen.

**Satz 1.13. (“Heiratssatz”)** *In der Situation von 1.11 existiert ein Repräsentantensystem genau dann, wenn folgende Bedingung erfüllt ist:*

*Für alle  $m \leq n$  enthält die Vereinigung von  $m$  beliebig aus  $A_1, \dots, A_n$  ausgewählten Mengen mindestens  $m$  Elemente.*

*Beweis.* Die Bedingung ist offensichtlich notwendig.

Sei sie erfüllt; wir zeigen durch Induktion nach  $n$ , daß ein Repräsentantensystem existiert.

$n = 1$  : Es ist nichts zu zeigen.

$n > 1$  :

*1.Fall:* Für alle  $l < n$  und je  $l$  der Mengen  $A_1, \dots, A_n$  hat die Vereinigung *mehr* als  $l$  Elemente.

---

<sup>2</sup>Es ist hier an Konflikte gedacht, die darauf zurückzuführen sind, daß mehrere Frauen sich denselben Mann aussuchen. Über die Voraussetzungen für das Ausbleiben von Konflikten anderer Art, etwa zwischen der Frau und dem von ihr ausgesuchten Mann, kann die Kombinatorik keine Aussage machen.

Sei  $x \in A_n$ ; betrachte  $A'_i := A_i - \{x\}$  in  $X' := X - \{x\}$ . Wegen der im vorliegenden Fall gemachten Voraussetzung ist die Bedingung des Satzes für die  $A'_i$ ,  $1 \leq i \leq n - 1$  erfüllt. Nach Induktionsvoraussetzung existiert ein Repräsentantensystem  $\{x_1, \dots, x_{n-1}\}$  für die  $A'_i$  ( $1 \leq i \leq n - 1$ ); setzt man  $x_n := x$ , erhält man insgesamt ein Repräsentantensystem für die  $A_i$  ( $1 \leq i \leq n$ ).

*2. Fall:* Für ein  $l < n$  und für  $A_1, \dots, A_l$  (nach eventuellem Umnúmerieren der  $A_i$ ) gilt  $|Y| = l$  (wobei  $Y := \bigcup_{1 \leq i \leq l} A_i$ ).

Nach Induktionsvoraussetzung existiert ein Repräsentantensystem  $\{x_1, \dots, x_l\}$  von  $A_1, \dots, A_l$ ; insbesondere gilt  $Y = \{x_1, \dots, x_l\}$ . Die Vereinigung von je  $m$  der Mengen  $A_{l+1}, \dots, A_n$  mit  $Y$  enthält mindestens  $l + m$  Elemente (weil ja angenommen wird, daß die Bedingung des Satzes für die  $A_1, \dots, A_n$  insgesamt erfüllt ist, insbesondere also auch für die  $A_{l+1}, \dots, A_n$ ). D.h. diese  $m$  Mengen enthalten mindestens  $m$  Elemente, die nicht in  $Y$  liegen. Mit anderen Worten: Die  $A_{l+1} - Y, \dots, A_n - Y$  erfüllen die Bedingung des Satzes. Nach Induktionsvoraussetzung existiert ein Repräsentantensystem für  $A_{l+1} - Y, \dots, A_n - Y$  — also ein Repräsentantensystem für  $A_{l+1}, \dots, A_n$ , das disjunkt ist zu  $Y$ . Zusammen mit  $Y$  ergibt sich ein Repräsentantensystem für  $A_1, \dots, A_n$ .  $\square$

---

In diesem ersten Kapitel wurden unterschiedliche Typen von Existenzaussagen mit teilweise sehr einfachen, teilweise komplexeren Beweisen erarbeitet. Man kann ein *Prinzip* festhalten: Oft kann man aus quantitativen Aussagen (dem Wert irgendeiner Größe, einer "Invariante" der zugrundeliegenden Struktur) eine qualitative Aussage (eine Existenzaussage) herleiten.

## 2 Ordnung im Chaos

(Der Titel dieses Kapitels wird sich im folgenden selbst erklären.)

**Proposition 2.1. (Satz von Erdős-Szekeres):** Seien  $n, m \in \mathbb{N}_n$  und  $(a_i)_{1 \leq i \leq mn+1}$  eine reelle Folge der Länge  $mn + 1$ . Dann existiert

- entweder eine monoton steigende Teilfolge der Länge  $m + 1$
- oder eine monoton fallende Teilfolge der Länge  $n + 1$ .

*Erster Beweis.* Sei  $(S, \prec)$  folgende geordnete Menge:

$$S := \mathbb{N}_{mn+1};$$

$$i \prec j := i \leq j \text{ und } a_i \leq a_j .$$

Zwei Elemente  $i, j, i < j$  sind genau dann unvergleichbar in  $S$ , wenn  $a_i > a_j$ . D.h.

$$\begin{aligned} \{i_1 < \dots < i_r\} & \text{ Kette in } S \Leftrightarrow a_{i_1} \leq a_{i_2} \leq \dots \leq a_{i_r}; \\ & \text{Antikette in } S \Leftrightarrow a_{i_1} > a_{i_2} > \dots > a_{i_r} . \end{aligned}$$

Die Behauptung folgt dann aus ‘‘Dilworth’s Lemma’’ 1.6. □

*Zweiter Beweis. (direkt):* Angenommen, es gäbe keine monotonen Teilfolgen wie verlangt. Definiere

$$\begin{aligned} f : \mathbb{N}_{mn+1} & \rightarrow \mathbb{N}_m \times \mathbb{N}_n \\ t & \mapsto (x_t, y_t) , \end{aligned}$$

wobei  $x_t$  (bzw.  $y_t$ ) als die Länge der größten monoton steigenden (bzw. fallenden) Teilfolge, die mit  $a_t$  beginnt, gewählt wird. Dann existieren  $j < k$  mit  $f(j) = f(k)$ . Ist  $a_j \leq a_k$ , so ist  $x_j > x_k$ ; andernfalls ist  $y_j > y_k$ . In beiden Fällen ergibt sich also ein Widerspruch. □

*Bemerkung:* Die angegebenen Schranken sind scharf, denn für alle  $m, n$  existieren Folgen  $(a_i)_{1 \leq i \leq mn}$ , die weder monoton steigende Teilfolgen der Länge  $m + 1$  noch monoton fallende Teilfolgen der Länge  $n + 1$  besitzen. (Man überlege sich dies!)

---

Wir betrachten jetzt einen vollständigen Graphen  $K_n$ , dessen Kanten ‘‘zufällig’’ entweder rot oder grün eingefärbt sind. Finden wir immer monochrome Untergraphen  $K_l$  großer Ordnung?

**Satz 2.2** (Ramsey 1930). *Gegeben seien  $a, b \in \mathbb{N}, a, b \geq 2$ .*

(i) *Es gibt eine minimale Zahl  $R(a, b) \in \mathbb{N}$  mit der Eigenschaft: Für jedes  $n \geq R(a, b)$  und für jede Rot-Grün-Färbung seiner Kanten enthält  $K_n$*

- *entweder einen roten Untergraphen  $\cong K_a$*
- *oder einen grünen Untergraphen  $\cong K_b$ .*

(ii) *Es gilt die Ungleichung*

$$R(a, b) \leq R(a - 1, b) + R(a, b - 1) .$$

Die  $R(a, b)$  heißen *Ramsey-Zahlen*, die  $R(a, a)$  *diagonale Ramsey-Zahlen*.

*Beispiel:* Wie wir sehen werden, ist  $R(3, 3) = 6$ . Das heißt: In jeder beliebigen Gruppe von 6 Personen gibt es eine Teilmenge von dreien, in der

- entweder jede(r) die beiden übrigen Personen kennt
- oder jede(r) keine der beiden übrigen Personen kennt.

*Bemerkung:* Zwischen 2.1 und 2.2 besteht folgende Gemeinsamkeit (die dann auch den Titel des Kapitels rechtfertigt): Gegeben sind “große” Strukturen (im ersten Fall eine Folge mit vielen Gliedern, im zweiten ein großer gefärbter  $K_n$ ) mit unvorhersehbarem (“chaotischem”) Verhalten. Sind die Strukturen allerdings groß genug, kann man in ihnen Teilstrukturen vorgegebener Größe finden, deren Verhalten vorhersehbar/deterministisch ist.

*Beweis von 2.2.* (1) Wenn wir überhaupt eine Zahl  $R$  finden, die die in (i) formulierten Eigenschaften hat, so hat auch  $R + 1$  diese Eigenschaft, und es existiert eine minimale unter diesen Zahlen.

(2) Wir zeigen die Existenz solcher  $R$  durch simultane Induktion nach  $a$  und  $b$ . Trivialerweise ist

$$R(a, 2) = a, R(2, b) = b .$$

(3) Induktionsannahme:  $R(a - 1, b)$  und  $R(a, b - 1)$  existieren. Wir zeigen, daß  $R(a, b)$  existiert und daß die Ungleichung aus (ii) erfüllt ist.

Sei für  $a, b \geq 3$  der Graph  $G = K_n$  mit  $n = R(a - 1, b) + R(a, b - 1)$  rot-grün gefärbt, und bezeichne  $v$  einen beliebigen Knoten von  $G$ . Nach dem Schubfachprinzip existieren entweder  $R(a - 1, b)$  rote oder  $R(a, b - 1)$  grüne Kanten, die von  $v$  ausgehen; wir nehmen o.B.d.A. an, daß  $R(a - 1, b)$  rote Kanten  $\epsilon_i$  von  $v$  ausgehen. Sei  $H \cong K_{R(a-1,b)}$  der vollständige Untergraph, der die von  $v$  verschiedenen Endpunkte der  $\epsilon_i$  als Knoten hat. Nach der Definition von  $R(a - 1, b)$  und der Induktionsvoraussetzung enthält  $H$  einen roten  $K_{a-1}$  oder einen grünen  $K_b$ . Im zweiten Fall sind wir fertig; im ersten Fall nehmen wir  $v$  und die  $\epsilon_i$  zum roten  $K_{a-1}$  hinzu und erhalten einen roten  $K_a$ .  $\square$

Es ist also recht einfach, die *Existenz* der Ramsey-Zahlen nachzuweisen; wie wir sehen werden, ist demgegenüber die *Bestimmung* dieser Zahlen äußerst schwierig und bisher nur in Einzelfällen möglich. Einige Ergebnisse hierzu stellen wir im Folgenden zusammen.

**Korollar 2.3.** *Mit den Bezeichnungen des Satzes 2.2 gilt*

- (i)  $R(a, b) = R(b, a) \forall a, b;$
- (ii)  $R(a, b) \leq \binom{a+b-2}{a-1} \forall a, b;$
- (iii)  $R(3, 3) = 6.$

*Beweis.* Zu (i): Vertausche rot mit grün.

Zu (ii): Wir führen den Beweis durch Induktion nach  $a + b$ ; als Induktionsanfang dient uns die schon eingesehene Tatsache  $R(a, 2) = a \forall a$ . Zum Induktionsschritt:

$$R(a, b) \stackrel{2.2(ii)}{\leq} R(a-1, b) + R(a, b-1) \stackrel{i.v.}{\leq} \binom{a+b-3}{a-2} + \binom{a+b-3}{a-1} \\ = \binom{a+b-2}{a-1}.$$

Zu (iii): Zunächst ist wegen 2.2 (ii)  $R(3, 3) \leq 2R(2, 3) = 6$ . Die Gleichheit folgt aus der Existenz einer Färbung von  $K_5$  ohne monochrome Dreiecke; eine solche gebe man zur Übung selbst an!  $\square$

**Korollar 2.4.** (Verallgemeinerung auf mehr als 2 Farben.) Für  $l \geq 2$  und  $a_1, \dots, a_l \in \mathbb{N}, a_i \geq 2$  für  $1 \leq i \leq l$  existiert ein minimales  $R = R(a_1, \dots, a_l)$  mit folgender Eigenschaft: Für jedes  $n \geq R$  und für jede  $l$ -Färbung (d.h. Färbung mit  $l$  Farben) von  $K_n$  existiert ein  $k$  zwischen 1 und  $l$ , so daß ein monochromer Untergraph der Farbe  $k$  isomorph zu  $K_{a_k}$  existiert.

*Beweisskizze.* Wir führen den Beweis durch Induktion nach  $l$ . Der Induktionsanfang für  $l = 2$  ist gerade die Aussage des Satzes 2.2. Sei also  $l > 2$ ; betrachte die  $l$ -Färbung als 2-Färbung mit den Farben  $\{1, 2, \dots, l-1\}$  und  $l$ . Nach 2.2 gibt es also entweder einen Untergraphen der Farbe  $l$  mit den gewünschten Eigenschaften, oder es gibt einen solchen mit der Farbe  $\{1, 2, \dots, l-1\}$ ; auf diesen kann man die Induktionsvoraussetzung anwenden.  $\square$

**Tabelle 2.5.** Wir stellen noch einige weitere bekannte Ramsey-Zahlen zusammen; wir werden in der Folge in den einfachsten Fällen die hier angegebenen exakten Werte nachrechnen. Für größere  $a, b$  sind nur noch Abschätzungen bekannt; beispielsweise ist der Eintrag 40-43 an der Stelle (3,10) der Tabelle so zu verstehen, daß  $40 \leq R(3, 10) \leq 43$ . Werte oder Abschätzungen, die sich aus der Symmetrieeigenschaft von  $R(a, b)$  ergeben, sind weggelassen.

	$b = 3$	4	5	6	7	8	9	10
$a = 3$	6	9	14	18	23	28	36	40-43
4		18	25	35-41				
5			43-49	58-87				
6				102-165				

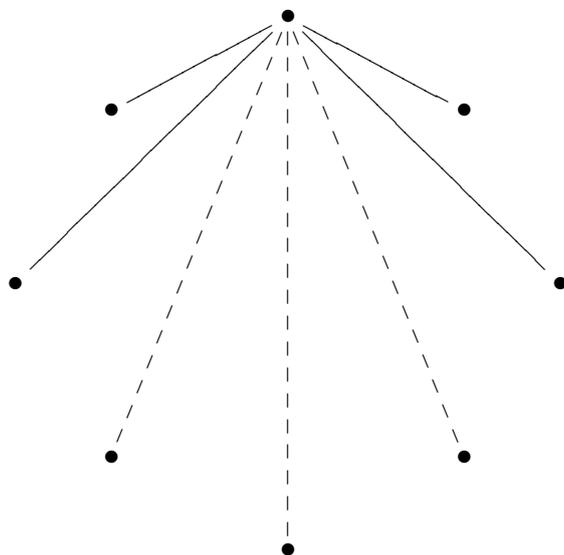
Die vollständige Tabelle der jeweils aktuell bekannten Ergebnisse findet man unter <http://mathworld.wolfram.com/>.

**Proposition 2.6.**  $R(3, 4) = 9$ .

*Beweis.* (i) Die Ungleichung 2.2 (ii) liefert zunächst nur  $R(3, 4) \leq R(2, 4) + R(3, 3) = 4 + 6 = 10$ .

(ii) Es gilt aber sogar  $R(3, 4) \leq 9$ . Wir nehmen dazu an, es würde auf  $K_9$  eine Färbung existieren ohne rotes  $K_3$  und ohne grünes  $K_4$ , und führen diese Annahme zum Widerspruch. Wegen  $R(2, 4) = 4$  und  $R(3, 3) = 6$  müssen in diesem Fall von jedem Knoten von  $K_9$  genau 3 rote und genau 5 grüne Kanten ausgehen. Dies überlegt man sich so: es können von keinem Knoten 4 rote Kanten ausgehen, da man sonst deren Endpunkte zu einem  $K_4$  verbinden könnte; da dieser nach Annahme nicht ganz grün sein darf, gibt es in ihm mindestens eine rote Kante — und diese zusammen mit den beiden roten Kanten zum ursprünglichen Knoten ergäbe ein rotes Dreieck, im Widerspruch zur Annahme. Ähnlich können von keinem Knoten 6 grüne Kanten ausgehen; insgesamt müssen also genau 3 rote und genau 5 grüne Kanten von dem Knoten ausgehen (da im  $K_9$  jedenfalls genau  $8 = 5 + 3$  Kanten von jedem Knoten ausgehen). Damit müßte aber gelten, daß der rote Untergraph von  $K_9$  genau  $\frac{3 \cdot 9}{2}$  Kanten hat (wobei der Nenner durch das Herausrechnen doppelt gezählter Kanten zustande kommt), was offensichtlich unsinnig ist.

(iii) Es existiert eine Färbung auf  $K_8$  ohne rotes  $K_3$  und ohne grünes  $K_4$ . Betrachte dazu folgendes Schema, in dem rote Kanten als gestrichelte Kanten und grüne Kanten als durchgezogene Kanten dargestellt sind:



Stellt man sich die Knoten des  $K_8$  als auf einem Kreis liegend vor, ergibt sich aus dem Schema eine Vorschrift für eine solche Färbung: Verbinde jeden Knoten rot mit dem ihm gegenüberliegenden Knoten und dessen unmittelbaren Nachbarn<sup>3</sup> auf dem Kreis und grün

<sup>3</sup>Das Wort “Nachbar” ist hier nicht im Sinne der Graphendefinition zu verstehen — dann wären *alle*

mit den übrigen Knoten. Mit anderen Worten: Übertrage das Schema in einer sukzessiven Rotation auf jeden Knoten. Man überzeuge sich davon, daß dies in der Tat eine wohldefinierte Färbung ergibt.

Man überlegt sich leicht, daß hierbei kein roter  $K_3$  entstehen kann. Ferner gibt es keinen grünen  $K_4$ , denn geht man im Schema beispielsweise von den am weitesten links gelegenen derjenigen fünf Punkte aus, bei denen grüne Kanten ansetzen, so wird dieser mit zwei anderen dieser Punkte rot verbunden; es bleiben also nur drei Punkte übrig, die miteinander grün verbunden werden.  $\square$

Es sei hier noch angemerkt, daß ein direktes Angehen der Frage der Ramseyzahlen durch computergestützte Auflistung sämtlicher Färbungen der einzelnen  $K_n$  im allgemeinen nicht realisierbar ist: bereits der  $K_9$  hat 36 Kanten, kann also auf  $2^{36}$  verschiedene Arten eingefärbt werden! Der voranstehende Beweis lehrt uns also etwas, was wir nicht "einfacher" wissen könnten. Um so mehr gilt dies für den nächsten Satz, bei dem allerdings bereits in gewissem Maße Hilfsmittel aus der Zahlentheorie benutzt werden.

**Satz 2.7.**  $R(4, 4) = 18$ .

*Beweis.*  $R(4, 4) \leq 2R(3, 4) \stackrel{2.6}{=} 18$ . Es bleibt also zu zeigen: Auf  $K_{17}$  existiert eine Färbung ohne monochromen  $K_4$ . Hierzu macht man sich zunutze, daß 17 eine Primzahl kongruent 1 modulo 4 ist. Man numeriert die Knoten von  $K_{17}$  durch mit den Elementen des endlichen Körpers  $\mathbb{Z}/17\mathbb{Z} = \mathbb{F}_{17}$ . Es ist bekannt, daß  $\mathbb{F}_{17}^*$  eine zyklische Gruppe mit 16 Elementen ist. Betrachte

$$\begin{aligned} \phi : \mathbb{F}_{17}^* &\rightarrow \mathbb{F}_{17}^* \\ x &\mapsto x^2 ; \end{aligned}$$

dies ist ein Homomorphismus mit Kern  $\{\pm 1\}$  (hierbei ist  $-1 \equiv 16 \pmod{17}$ ). Aus  $|\text{Ker}(\phi)| = 2$  ergibt sich  $|\text{Bild}(\phi)| = 8$ , und zwar ist  $\text{Bild}(\phi) = \{1, 4, 9, 16, 8, 2, 15, 13\}$ , also gleich  $\{1, 2, 4, 8, 9, 13, 15, 16\}$ . Definiere für  $a \in \mathbb{Z}$  das *quadratische Symbol*

$$\left(\frac{a}{17}\right) := \begin{cases} 1 : & \exists x \in \mathbb{Z} : a \equiv x^2 \pmod{17}; \quad a \not\equiv 0 \pmod{17} \quad (8 \text{ Fälle}); \\ 0 : & a \equiv 0 \pmod{17} \quad (1 \text{ Fall}); \\ -1 : & \text{sonst} \quad (8 \text{ Fälle}). \end{cases}$$

Das so definierte quadratische Symbol hat offenbar folgende Eigenschaften:

- $\left(\frac{ab}{17}\right) = \left(\frac{a}{17}\right) \left(\frac{b}{17}\right)$ ;
- $\left(\frac{-1}{17}\right) = +1$  (da 16 ein Quadrat ist).

---

Knoten eines vollständigen Graphen Nachbarn —, sondern im anschaulichen Sinn!

Definiere nun auf dem mit den Elementen von  $\mathbb{Z}/17\mathbb{Z}$  durchnummerierten  $K_{17}$  folgende Färbung: Eine Kante  $\{a, b\}$  (mit  $a, b \in \mathbb{F}_{17}, a \neq b$ ) sei

$$\begin{aligned} \text{rot} & :\Leftrightarrow \left(\frac{a-b}{17}\right) = +1, \\ \text{grün} & :\Leftrightarrow \left(\frac{a-b}{17}\right) = -1. \end{aligned}$$

Diese Färbung hat folgende Eigenschaften:

- sie ist wohldefiniert: es hat nämlich  $\{a, b\}$  dieselbe Farbe wie  $\{b, a\}$  (dies ergibt sich aus den Eigenschaften des quadratischen Symbols);
- sie ist translationsinvariant: Für ein  $c \in \mathbb{F}_{17}$  hat  $\{a+c, b+c\}$  dieselbe Farbe wie  $\{a, b\}$  (trivial);
- multipliziert man (die Nummern der Knoten) eine(r) Kante  $\{a, b\}$  mit  $c \in \mathbb{F}_{17}^*$ , so multipliziert sich die Farbe mit  $\left(\frac{c}{17}\right)$  (d.h. sie ändert sich bei  $\left(\frac{c}{17}\right) = -1$  und bleibt gleich bei  $\left(\frac{c}{17}\right) = 1$ ).

Treffen wir nun die *Annahme*, der  $K_{17}$  mit der beschriebenen Färbung enthielte einen monochromen  $K_4$  mit Knoten  $a, b, c, d \in \mathbb{F}_{17}$ . Wegen der Translationsinvarianz können wir o.B.d.A. annehmen, daß hierbei  $a = 0$  gilt. Weiter sei  $b = 1$ ; auch dies beschränkt die Allgemeinheit nicht, diesmal wegen der Multiplikationseigenschaft (zunächst gilt für das *ursprüngliche*  $b$ , daß es von den übrigen drei Knoten verschieden ist, also auch von  $a = 0$ ; man kann also mit  $b$  durchdividieren, wobei der Graph monochrom bleibt — mit eventuell anderer Farbe in Abhängigkeit von  $\left(\frac{b}{17}\right)$ ). Insgesamt ist also  $V(K_4) = \{0, 1, c, d\}$ . Weil nun dieser  $K_4$  als monochrom angenommen ist, müssen sämtliche der folgenden quadratischen Symbole denselben Wert haben:

$$\left(\frac{1-0}{17}\right), \left(\frac{c-0}{17}\right), \left(\frac{d-0}{17}\right), \left(\frac{c-1}{17}\right), \left(\frac{d-1}{17}\right), \left(\frac{d-c}{17}\right);$$

und zwar ist dieser gemeinsame Wert  $= \left(\frac{1}{17}\right) = +1$ . Es müßte also gelten:

$$c, d, c-1, d-1, d-c \in \{1, 2, 4, 8, 9, 13, 15, 16\}.$$

Da also insbesondere mit  $c, d$  auch  $c-1, d-1$  Quadrate sein sollen, muß  $c, d \in \{2, 9, 16\}$  gelten; in diesem Fall ist jedoch eine Wahl, für die überdies  $d-c$  Quadrat ist, nicht möglich. Die Annahme muß also falsch gewesen sein; wir haben eine Färbung auf  $K_{17}$  ohne monochromen  $K_4$  konstruiert.  $\square$

**Satz 2.8.** Für  $k \geq 2$  gelten die Ungleichungen

$$2^{\frac{k}{2}} \leq R(k, k) < 2^{2k-2}.$$

*Beweis.* Wir zeigen zunächst die Gültigkeit der *oberen* Schranke. Es gilt für alle  $k \in \mathbb{N}$ :  
 $\binom{2k}{k} < \sum_{0 \leq i \leq 2k} \binom{2k}{i} = (1+1)^{2k} = 2^{2k}$ ; insbesondere gilt also

$$R(k, k) \stackrel{2.3(ii)}{\leq} \binom{2k-2}{k-1} < 2^{2k-2}.$$

Was nun die *untere* Schranke betrifft, sei o.B.d.A.  $k \geq 4$  (für  $k = 2, 3$  beachte  $R(2, 2) = 2 \geq 2^1$  und  $R(3, 3) = 6 \geq 2^{3/2}$ ). Sei ferner  $n < 2^{k/2}$ ; wir zeigen: Es existieren Färbungen auf  $K_n$ , so daß es keine monochromen Untergraphen der Form  $K_k$  gibt.

Betrachte dazu die Menge aller  $2^{\binom{n}{2}}$  Färbungen des  $K_n$ . Alle Kanten seien mit Wahrscheinlichkeit  $1/2$  rot bzw. grün gefärbt; da die Färbungen zweier verschiedener Kanten unabhängige Ereignisse sind, sind also alle Färbungen des  $K_n$  gleichwahrscheinlich, und die Wahrscheinlichkeit für eine bestimmte Färbung ist  $2^{-\binom{n}{2}}$ .

Ist  $S$  eine  $k$ -Menge von Knoten des  $K_n$ , so ist die Wahrscheinlichkeit, daß der induzierte Graph zu  $S$  rot gefärbt ist, gegeben durch

$$P_{\text{rot}}(S) = 2^{-\binom{k}{2}}$$

(im Exponenten steht hierbei die Kantenzahl des induzierten Graphen). Die Wahrscheinlichkeit, daß für eine zufällige Färbung irgendeine  $k$ -Menge  $S$  vollständig rot ist, ist also

$$P_{\text{rot}}^{(k)} \leq \sum_{\substack{S \subset V(K_n) \\ |S|=k}} P_{\text{rot}}(S) = \binom{n}{k} \cdot 2^{-\binom{k}{2}} = (*).$$

Hierbei kann man die Anzahl der Summanden, also  $\binom{n}{k}$ , folgendermaßen abschätzen:

$$\binom{n}{k} = \frac{\overbrace{n(n-1) \cdots (n-k+1)}^{k \text{ Faktoren}}}{k!} \leq \frac{n^k}{k!} \leq \frac{n^k}{2^{k-1}};$$

die Abschätzung von  $P_{\text{rot}}^{(k)}$  läßt sich also so fortsetzen:

$$(*) \leq \frac{n^k}{2^{k-1}} 2^{-\binom{k}{2}} \stackrel{n < 2^{k/2}}{<} 2^{\frac{k^2}{2} - \binom{k}{2} - k + 1} \stackrel{\binom{k}{2} = \frac{k^2}{2} - \frac{k}{2}}{=} 2^{-\frac{k}{2} + 1} \stackrel{k \geq 4}{\leq} \frac{1}{2}.$$

Man hat also gezeigt, daß  $P_{\text{rot}}^{(k)} < \frac{1}{2}$  gilt. Ähnlich zeigt man  $P_{\text{grün}}^{(k)} < \frac{1}{2}$ ; da also insgesamt  $P_{\text{rot}}^{(k)} + P_{\text{grün}}^{(k)} < 1$  folgt, existiert eine Färbung, die kein monochromes  $K_k$  enthält.  $\square$

*Bemerkungen:*

- (i) In diesen Beweis gehen keine tiefliegenden Ergebnisse der Wahrscheinlichkeitstheorie ein; diese kommt eigentlich nur an der Stelle, wo man  $P_{\text{rot}}^{(k)}$  durch die Summe der  $P_{\text{rot}}$  abschätzt, ein wenig zum Tragen. In der Tat könnte man den Beweis so umformulieren, daß er völlig auf Wahrscheinlichkeitstheorie verzichtet.
- (ii) Sei  $\epsilon > 0$ ; es scheint weder in der Abschätzung nach oben der Exponent  $2k - 2$  durch  $(2 - \epsilon)k - 2$  noch in der Abschätzung nach unten der Exponent  $\frac{k}{2}$  durch  $(\frac{1}{2} + \epsilon)k$  ersetzt werden zu können (es sind zwar keine Gegenbeispiele für diese schärferen Abschätzungen bekannt, aber auch kein Beweis für sie).
- (iii) Dagegen kann man beweisen:

$$R(k, 3) \sim \frac{k^2}{\log k}.$$

(*Erinnerung:* Zwei reelle Funktionen  $f, g$  heißen *asymptotisch äquivalent* — in Zeichen  $f \sim g$  — genau dann, wenn  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$ .)

Betrachte  $c$ -Färbungen von  $\mathbb{N}_n$ , d.h. Abbildungen  $f : \mathbb{N}_n \rightarrow \mathbb{N}_c$ , und *arithmetische Progressionen der Länge  $l$*  (dies sind Mengen der Form  $\{a, a + d, a + 2d, \dots, a + (l - 1)d\}$ ); wir fragen, ob es zu einer vorgegebenen Färbung von  $\mathbb{N}_n$  eine monochrome arithmetische Progression der Länge  $l$  gibt.

*Beispiel:* Färbe  $\mathbb{N}_8$  wie folgt mit 2 Farben (dargestellt durch unterstrichene bzw. nicht unterstrichene Zahlen):

$$1 \quad \underline{2} \quad \underline{3} \quad 4 \quad 5 \quad \underline{6} \quad \underline{7} \quad 8$$

Hier gibt es *keine* monochrome arithmetische Progression der Länge 3. Bei 9 Zahlen jedoch gibt es eine solche arithmetische Progression für *jede* 2-Färbung!

**Satz 2.9. (van der Waerden 1928)** *Seien  $c, l \in \mathbb{N}, c, l \geq 2$ . Es gibt eine minimale Zahl  $W = W(c, l)$  mit der Eigenschaft, daß für alle  $n \geq W$  und alle  $c$ -Färbungen von  $\mathbb{N}_n$  eine monochrome arithmetische Progression der Länge  $l$  in  $\mathbb{N}_n$  existiert.*

**Korollar 2.10.** *Für jede  $c$ -Färbung von  $\mathbb{N}$  und jedes  $l \in \mathbb{N}$  existieren monochrome arithmetische Progressionen der Länge  $l$ .*

*Beweis von 2.9.* Wir schreiben kurz “ $l$ -AP” für “arithmetische Progression der Länge  $l$ ”.

- (0) Ist die Behauptung richtig für  $\mathbb{N}_n$ , so ist sie auch richtig für jeden Abschnitt von  $\mathbb{N}$  der Länge  $n$ , also der Form  $k + 1, k + 2, \dots, k + n$ .

(i) Die Aussage ist richtig für kleine Werte von  $c$  oder  $l$ ; es sind

$$W(1, l) = l \quad \forall l ; \quad W(c, 1) = 1 \quad \forall c ; \quad W(c, 2) = c + 1 \quad \forall c .$$

(ii) Wir führen den Beweis durch Induktion nach  $l$ . (i) liefert uns den Wert von  $W$  für  $l = 1, 2$  und alle  $c$ . Die Behauptung gelte nun für ein festes  $l$  und alle  $c$  (d.h. alle Zahlen  $W(c, l)$  seien bekannt). Wir zeigen: die Behauptung gilt dann auch für  $l + 1$  und alle  $c$ , und es gilt darüber hinaus für jedes  $c$ :

$$W(c, l + 1) \leq f(c) , \quad \text{wobei } f(0) = 1 , \\ f(n) = 2W(c^{f(n-1)}, l)f(n-1) \quad \text{für } 1 \leq n \leq c .$$

Daß die in der Definition von  $f$  auftretenden Zahlen  $W$  existieren, ergibt sich aus der Induktionsvoraussetzung (von der ja angenommen wurde, daß sie für alle  $c$  gelten solle, insbesondere also für die Zahl  $c^{f(n-1)}$ ).

(iii) *Annahme:*  $\mathbb{N}_{f(c)}$  sei  $c$ -gefärbt *ohne* eine monochrome  $(l + 1)$ -AP. Zerlege  $\mathbb{N}_{f(c)}$  in  $\frac{f(c)}{f(c-1)}$  Teilintervalle ("Blöcke") der Länge  $f(c - 1)$ , jeden solchen Block in  $\frac{f(c-1)}{f(c-2)}$  Blöcke der Länge  $f(c - 2)$  und so weiter, so daß zuletzt jeder Block der Länge  $f(1)$  (kurz: jeder  $f(1)$ -Block) in  $\frac{f(1)}{f(0)} = f(1)$  Blöcke der Länge  $f(0) = 1$  (d.h. Zahlen) zerlegt wird.

Aufgrund des Faktors 2 in der Definition von  $f$  kann man auf allen Niveaus dieser Zerlegung zu einem jeden Block seine untere und seine obere Hälfte (in Bezug auf die Ordnung der natürlichen Zahlen) betrachten. Die untere Hälfte jedes  $f(1)$ -Blocks enthält nach Definition von  $W(c, l)$  und nach (0) eine monochrome  $l$ -AP.

(iv) Ein  $f(1)$ -Block hat eine von  $c^{f(1)}$  möglichen Färbungen; wir fassen nun jede der möglichen Färbungen als eine eigene Farbe auf! Wir betrachten die Menge der  $f(1)$ -Blöcke in einem  $f(2)$ -Block als mit einer Färbung aus diesen  $c^{f(1)}$  "Farben" versehen (es müssen nicht alle "Farben" vorkommen, aber dies spielt keine Rolle).

Die Trägermenge dieser Färbung hat offenbar  $\frac{f(2)}{f(1)} = 2W(c^{f(1)}, l)$  Elemente: ein  $f(2)$ -Block enthält  $2 \cdot W(c^{f(1)}, l)$  Blöcke der Länge  $f(1)$ . In dieser Situation kann man die Induktionsvoraussetzung anwenden (von der ja angenommen wurde, daß sie für alle  $c$  gelten solle, insbesondere also für die Zahl  $c^{f(1)}$ ): Die untere Hälfte jedes  $f(2)$ -Blocks enthält eine monochrome  $l$ -AP von  $f(1)$ -Blöcken ("monochrom" hier in Bezug auf die "Farben", mit denen diese Blöcke gefärbt sein sollen; unter einer arithmetischen Progression von Blöcken ist eine arithmetische Progression innerhalb der Nummern der Blöcke zu verstehen).

Entsprechend zeigt man für  $1 \leq n \leq c$ : Die untere Hälfte jedes  $f(n)$ -Blocks enthält eine monochrome  $l$ -AP von  $f(n-1)$ -Blöcken. Wähle ein System von monochromen  $l$ -APen auf allen Stufen.

(v) Betrachte jetzt nur solche Zahlen  $x \in \mathbb{N}_{f(c)}$ , die auf jedem  $n$ -Niveau der Zerlegung zu den gewählten monochromen  $l$ -APen in der unteren Hälfte des entsprechenden  $f(n)$ -Blocks gehören.

Wir versehen diese Zahlen  $x$  mit “Koordinaten” in Bezug auf die Zerlegungsniveaus; dazu schreiben wir  $x = (x_1, x_2, \dots, x_c)$ , wobei  $x_i$  angibt, zu welchem der  $l$  Blöcke in der monochromen  $l$ -AP von  $f(i-1)$ -Blöcken in der unteren Hälfte eines  $f(i)$ -Blocks die Zahl  $x$  gehört. Es gilt also  $1 \leq x_i \leq l$  für  $1 \leq i \leq c$ .

(vi) Sei  $x = (x_1, x_2, \dots, x_c)$  wie in (v). In jedem  $f(1)$ -Block bilden die  $l$  Zahlen

$$(1, x_2, \dots, x_c), (2, x_2, \dots, x_c), \dots, (l, x_2, \dots, x_c)$$

eine monochrome  $l$ -AP, deren Farbe wir als  $A_1$  bezeichnen. Sei  $(*) = (l+1, x_2, \dots, x_c)$  das entsprechend fortgesetzte Glied der arithmetischen Progression (zähle das entsprechende  $d$  hinzu; man verläßt nun möglicherweise die untere Hälfte des jeweiligen  $f(1)$ -Blocks).  $(*)$  hat nach der Annahme aus (iii) eine Farbe  $A_2 \neq A_1$ .

(vii) Betrachte die  $l$  Zahlen  $(l+1, 1, x_3, \dots, x_c), (l+1, 2, x_3, \dots, x_c), \dots, (l+1, l, x_3, \dots, x_c)$ . Sie bilden ebenfalls eine  $l$ -AP, die monochrom ist — und zwar mit Farbe  $A_2$ , da ja  $(*)$  unter ihnen vorkommt! Ähnlich wie in (vi) bildet man  $(l+1, l+1, x_3, \dots, x_c)$ , eine Zahl, die entsprechend eine Farbe  $A_3 \neq A_2$  hat. Man kann noch mehr über  $A_3$  sagen: die  $l$ -AP  $(1, 1, x_3, \dots, x_c), (2, 2, x_3, \dots, x_c), \dots, (l, l, x_3, \dots, x_c)$  ist monochrom nach der Voraussetzung über  $x$ , und zwar mit der Farbe  $A_1$  (da ja  $1 \leq x_2 \leq l$  gilt). Da  $(l+1, l+1, x_3, \dots, x_c)$  Fortsetzung dieser  $l$ -AP ist, gilt also  $A_3 \neq A_1$ .

Induktiv ergibt sich: Die Farbe  $A_{n+1}$  von

$$\underbrace{(l+1, l+1, \dots, l+1, x_{n+1}, \dots, x_c)}_{\substack{n \text{ Stellen} \\ n \leq c}}$$

ist verschieden von den Farben  $A_1, \dots, A_n$ ; insbesondere hat  $(l+1, \dots, l+1)$  eine Farbe  $A_{c+1} \neq A_1, \dots, A_c$ . Somit führt die in (iii) gemachte Annahme auf einen Widerspruch.  $\square$

**Bemerkung 2.11.** Bisher sind folgende Werte von  $W(c, l)$  bekannt:

$c \setminus l$	3	4	5	6
2	9	35	178	1132
3	27			
4	76			

Der Kenntnistand auf diesem Feld hat sich in den letzten Jahrzehnten nicht mehr verändert mit Ausnahme des Wertes für  $W(2, 6)$ , der 2007 gefunden wurde.

### 3 Was heißt Zählen?

Die Leitfrage der abzählenden Kombinatorik lautet:

Auf wieviele Weisen kann man...?

— wobei für die Pünktchen jeweils eine bestimmte Aufgabenstellung einzusetzen ist. Es gibt verschiedene Möglichkeiten, Antworten auf diese Leitfrage anzugeben.

Die *erste mögliche Antwort* ist: *eine Zahl*.

**Frage 3.1.** Auf wieviele verschiedene Weisen können wir vier numerierte Objekte in drei numerierte Fächer legen, so daß in jedem Fach wenigstens ein Objekt liegt?

“Mathematischer” formuliert lautet die Frage: Wieviele surjektive Abbildungen  $\mathbb{N}_5 \rightarrow \mathbb{N}_3$  gibt es? Die Antwort wird auf dem 1.Übungsblatt in Aufgabe 2 gegeben; sie ist: 150.

Man kann sich nun fragen, wie befriedigend diese Antwort ist. Sie hat einige Nachteile: Man sieht ihr nicht unmittelbar an, auf welcher kombinatorischen Struktur des Problems sie beruht, und kann sie dementsprechend auch nicht auf “ähnliche” Probleme übertragen.

Hieraus ergibt sich die *zweite mögliche Antwort* auf die Leitfrage: Für Probleme  $P(n)$ , die von dem Parameter  $n \in \mathbb{N}$  abhängen, ist die Zahl  $f(n)$  aller möglichen Arrangements zu  $P(n)$  gegeben durch eine “*explizite Formel*” für  $f(n)$ ; ähnlich für mehrere Parameter. Hierbei wäre zu definieren, was “explizite Formel” eigentlich heißen soll; wir wollen uns der etwas vagen Formulierung “etwas, womit man die gesuchte Zahl auf einfache Weise ausrechnen kann, wenn man  $n$  kennt” bedienen.

**Frage 3.2.** Welchen Wert hat die Zahl  $f(n, k)$  aller Injektionen  $\mathbb{N}_k \rightarrow \mathbb{N}_n$ ?

*Antwort:* Sei o.B.d.A.  $k \leq n$  (sonst ist  $f(n, k) = 0$ ); dann gilt:

$$\begin{aligned} f(n, k) &= n(n-1) \cdots (n-k+1) \\ &= k! \binom{n}{k} \\ &= \frac{n!}{(n-k)!} . \end{aligned}$$

Diese Antwort ist “befriedigend” (denn sie ist sowohl explizit im Sinne unserer obigen Definition dieses Ausdrucks als auch durchsichtig: man erkennt sogleich, wie die Formel zustandekommt). So befriedigend sind nicht alle expliziten Formeln, wie die nächsten Beispiele zeigen werden.

**Frage 3.3.** Welchen Wert hat die Zahl  $f(n, k)$  aller Surjektionen  $\mathbb{N}_n \rightarrow \mathbb{N}_k$ ?

Es gibt vieles, was den Begriff der Surjektion als “dual” zum Begriff der Injektion erscheinen läßt; von daher ist es erstaunlich, daß es auf die Frage nach  $f(n, k)$  keine ebenso

einfache Antwort gibt wie im Falle der Injektionen. Wie wir später noch sehen werden, gilt nämlich

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

Diese Formel ist zwar explizit, aber relativ undurchsichtig: Man sieht nicht sofort, wie sie zustandekommt; man kann nicht direkt erkennen, was beispielsweise für  $n = 2k$  bei  $k \rightarrow \infty$  passiert etc. Die Antwort ist also weniger befriedigend als die auf die Frage 3.2.

**Frage 3.4.** Welchen Wert hat die Zahl  $f(n)$  der  $n \times n$ -Matrizen (für  $n \geq 3$ ) mit Einträgen 0, 1, so daß in jeder Zeile und in jeder Spalte der Matrix genau 3 Einsen auftreten?

Die Antwort (die wir in dieser Vorlesung *nicht* herleiten werden), lautet

$$f(n) = 6^{-n} (n!)^2 \sum_{\substack{a, b, c \geq 0 \\ a+b+c=n}} \frac{(-1)^b (b+3c)! 2^a 3^b}{a! b! (c!)^2 6^c} .$$

Diese Antwort kann kaum als befriedigend gelten, denn eine Berechnung ist wohl nur noch mit einem Computer realisierbar, und die Formel ist extrem undurchsichtig (beispielsweise ist völlig unklar, wieso die  $a, b, c$  einerseits einer *symmetrischen* Bedingung unterworfen sind —  $a + b + c = n$  —, andererseits aber in den Summanden in sehr *unterschiedlicher* Weise auftreten). Bereits die Frage, wieviele Summanden die Summe überhaupt hat (d.h. wieviele Lösungstriple der Gleichung  $a + b + c = n$  es gibt), ist ein eigenständiges, wenn auch einfaches, kombinatorisches Problem (das hier zur Übung empfohlen sei).

Doch es kann noch “schlimmer” kommen: bei vielen expliziten Formeln verlangt die Auswertung z.B. die Summation über die Lösungen eines diophantischen Gleichungssystems, dessen Lösung (anders als im Falle der obigen sehr einfachen diophantischen Gleichung  $a + b + c = n$ ) die gleiche Komplexität haben kann wie die Auflistung aller Objekte des gesuchten Typs! (Man gewinnt also durch die explizite Formel überhaupt nichts mehr: man kann die gesuchte Anzahl ebenso einfach durch Herstellen und Abzählen der fraglichen Objekte bestimmen.) Diese Phänomene deuten darauf hin, daß explizite Formeln nicht die einzig möglichen Antworten auf die Leitfrage der abzählenden Kombinatorik sind.

Eine *dritte mögliche Antwort* auf diese Leitfrage ist eine *Rekursion*.

**Frage 3.5.** Welchen Wert hat die Zahl  $f(n)$  der Teilmengen von  $\mathbb{N}_n$ , die keine zwei aufeinanderfolgenden Zahlen enthalten?

*Antwort:* Es ist offenbar  $f(1) = 2, f(2) = |\{\{\}, \{1\}, \{2\}\}| = 3$ . Ist  $S \subset \mathbb{N}_n$  wie verlangt, und ist  $n \geq 3$ , so gilt *entweder*  $S \subset \mathbb{N}_{n-1}$  *oder*  $n \in S$  und  $S \cap \mathbb{N}_{n-1} \subset \mathbb{N}_{n-2}$ . Dies hat zur Folge

$$f(n) = f(n-1) + f(n-2), \quad n \geq 3 . \tag{1}$$

$f(n)$  ist also die  $n + 1$ -te Fibonaccizahl  $F_{n+1}$  (mit  $F_0 = F_1 = 1$  und  $F_k = F_{k-1} + F_{k-2}$  für alle  $k \geq 2$ ).

Wir fragen wie üblich: ist diese Antwort auf die Frage befriedigend? Die Antwort ist nicht sehr explizit, dafür aber sehr durchsichtig. Das Problem der fehlenden expliziten Formel läßt sich im vorliegenden Fall lösen: Aus (1) erhält man durch vollständige Induktion

$$f(n) = \frac{\tau^{n+2} - \bar{\tau}^{n+2}}{\sqrt{5}}, \quad \text{wobei } \tau := \frac{1 + \sqrt{5}}{2}, \quad \bar{\tau} := \frac{1 - \sqrt{5}}{2}. \quad (2)$$

Die Rekursion aus (1) ist sehr einfach: sie bestimmt  $f(n)$  aus  $f(n-1), \dots, f(1)$  *linear* und *mit Tiefe 2* (d.h. nur die beiden letzten vorangehenden Werte werden benötigt; dies ist etwa relevant für die Implementierung: geringe Speicherplatzkomplexität). Es gibt natürlich Rekursionen, die solche angenehmen Eigenschaften nicht haben. Aus solchen und anderen Gründen betrachtet man eine *vierte mögliche Antwort* auf die Leitfrage der abzählenden Kombinatorik: *erzeugende Funktionen*.

**Definition 3.6.** *Ist*

$$\begin{aligned} f(n) : \mathbb{N}_0 &\rightarrow \mathbb{C} \\ n &\mapsto f(n), \end{aligned}$$

so heißt die *formale Potenzreihe*

$$F(X) := \sum_{n \geq 0} f(n) X^n$$

die erzeugende Funktion von  $f$ . Weiter heißt

$$E(X) := \sum_{n \geq 0} f(n) \frac{X^n}{n!}$$

die exponentielle erzeugende Funktion oder die erzeugende Exponentialfunktion von  $f$ .

(*Bemerkung:* Dies sind strenggenommen gar keine Funktionen, sondern eben formale Potenzreihen; sie tragen ihren Namen also zu Unrecht. Diese Namensgebung ist allerdings die historisch gewachsene und wird daher — eingedenk der Ungenauigkeit — beibehalten.)

*Erinnerung:* Mit  $\mathbb{C}[X]$  bezeichnet man den Ring der Polynome in der Unbestimmten  $X$  mit Koeffizienten in  $\mathbb{C}$ , also die Menge

$$\left\{ \sum_{0 \leq i \leq n} a_i X^i \mid n \in \mathbb{N}_0, a_i \in \mathbb{C} \right\},$$

die  $\mathbb{C}$ -Vektorraum ist und mit der offensichtlichen Multiplikation sogar Ring. Eine Basis des Vektorraums bilden die Monome  $X^i$  ( $i \in \mathbb{N}_0$ ).

Man erweitert diesen Ring folgendermaßen zum Ring der Potenzreihen in  $X$ : man betrachtet die Menge

$$\mathbb{C}[[X]] := \left\{ \sum_{i \in \mathbb{N}_0} a_i X^i \mid a_i \in \mathbb{C} \right\};$$

auch dies ist mit der offensichtlichen Addition ein komplexer Vektorraum (man kann allerdings nicht mehr ohne weiteres eine Basis hinschreiben, da der Raum überabzählbare Dimension hat). Sind ferner  $f, g \in \mathbb{C}[[X]]$  mit  $f = \sum_{i \in \mathbb{N}_0} a_i X^i$ ,  $g = \sum_{j \in \mathbb{N}_0} b_j X^j$ , so ist

$$f \cdot g := \sum_{k \in \mathbb{N}_0} c_k X^k \text{ mit } c_k := \sum_{\substack{i, j \geq 0 \\ i+j=k}} a_i b_j$$

ein wohldefiniertes Element von  $\mathbb{C}[[X]]$ . (Hier sind keine Konvergenzbetrachtungen erforderlich, da die Summe in der Definition der  $c_k$  endlich ist.) Mit diesem Produkt versehen, ist  $\mathbb{C}[[X]]$  ein kommutativer Ring, der  $\mathbb{C}[X]$  als Unterring enthält; man hat also eine Einbettung  $\mathbb{C}[X] \hookrightarrow \mathbb{C}[[X]]$ .

Für  $f = \sum_{i \in \mathbb{N}_0} a_i X^i \in \mathbb{C}[[X]]$  heißt die Zahl

$$\rho(f) := \sup_{r \in \mathbb{R}_{\geq 0}} \left\{ r \mid \sum_{i \geq 0} |a_i| r^i \text{ konvergiert} \right\} \in \mathbb{R}_{\geq 0} \cup \{\infty\}$$

der *Konvergenzradius* von  $f$ . Ist  $z \in \mathbb{C}$  mit  $|z| < \rho(f)$ , so konvergiert  $f(z) := \sum_{i \geq 0} a_i z^i$ , und  $z \mapsto f(z)$  ist eine komplex differenzierbare Funktion von  $\{z \in \mathbb{C} \mid |z| < \rho(f)\} \rightarrow \mathbb{C}$ . Es gilt die *Formel von Abel-Hadamard*:

$$\rho(f) = \left( \overline{\lim}_{n \in \mathbb{N}_0} (|a_n|)^{\frac{1}{n}} \right)^{-1}.$$

Außerdem gilt das *Identitätsprinzip* für Potenzreihen: Existiert für  $f \in \mathbb{C}[[X]]$  eine unendliche Teilmenge  $S \subset \{z \in \mathbb{C} \mid |z| < \rho(f)\}$ , die einen Häufungspunkt besitzt, und ist  $f(s) = 0$  für alle  $s \in S$ , so ist  $f \equiv 0$ . Dies eröffnet die Möglichkeit des Koeffizientenvergleichs.

Durch Manipulation von  $F(X)$  bzw.  $E(X)$  zu einem  $f : \mathbb{N}_0 \rightarrow \mathbb{C}$  (also durch Konvergenzbetrachtungen, Einsetzen von Werten, Untersuchung von Differential- und Funktionalgleichungen für  $F(X)$  oder  $E(X)$ ) erhalten wir Aussagen über  $f$ .

**Beispiel 3.7.** Sei  $e(X) := \sum_{n \geq 0} \frac{X^n}{n!}$ . Bekanntlich ist  $\rho(e) = \infty$ . Sei  $e : \mathbb{C} \rightarrow \mathbb{C}$  die zugehörige Funktion; es gilt  $e(x+y) = e(x)e(y)$ , insbesondere  $e(x)e(-x) = 1$ . Das Identitätsprinzip sagt uns  $e(X)e(-X) = 1$  (hier bezeichnet 1 die Eins des Ringes  $\mathbb{C}[[X]]$ ).

Durch Koeffizientenvergleich erhalten wir aus

$$1 = \left( \sum_{i \geq 0} \frac{X^i}{i!} \right) \left( \sum_{j \geq 0} (-1)^j \frac{X^j}{j!} \right),$$

daß für alle  $k > 0$  gilt

$$\sum_{\substack{i, j \geq 0 \\ i+j=k}} \frac{1}{i!} \frac{(-1)^j}{j!} = 0, \quad \text{also} \quad \sum_{0 \leq j \leq k} (-1)^j \binom{k}{j} = 0.$$

Mit anderen Worten:  $1 + \binom{k}{2} + \binom{k}{4} + \dots = \binom{k}{1} + \binom{k}{3} + \dots$ ; d.h. es gibt ebensoviele Teilmengen gerader Ordnung wie Teilmengen ungerader Ordnung in  $\mathbb{N}_k$  (also jeweils  $2^{k-1}$  Stück).

**Beispiel 3.8.** Betrachte die Funktion  $f$  aus 3.5. mit “richtigen” Indizes (d.h.  $f(n) = F_n$ ); setze  $f(n) = 0$  für  $n < 0$ . Es ist

$$\begin{aligned} \sum_{n \geq 0} f(n) X^n &= F(X), \quad \text{also} \\ \sum_{n \geq 0} f(n-1) X^n &= XF(X) \quad \text{und} \\ \sum_{n \geq 0} f(n-2) X^n &= X^2 F(X). \end{aligned}$$

Die Rekursion (1) für  $n \geq 2$  ergibt

$$\begin{aligned} F(X) &= 1 + XF(X) + X^2 F(X), \\ \text{also } F(X)(1 - X - X^2) &= 1 \quad \text{bzw. } F(X) = \frac{1}{1 - X - X^2} \\ &= \frac{1}{(1 - \tau X)(1 - \bar{\tau} X)}. \end{aligned}$$

Man kann die explizite Formel (2) für  $f$  jetzt durch Berechnung der Taylorentwicklung von  $F(X)$  erhalten (denn dabei ermittelt man ja den  $n$ -ten Koeffizienten der Potenzreihe).

*Kombinatorische Identitäten.* Betrachte die  $f(n)$  aus 3.5 mit der Rekursion (1). Die  $f(n)$  sind Kardinalitäten von Mengen, und (1) kommt von einer Bijektion von Mengen. In einer solchen Situation spricht man allgemein von einer *kombinatorischen Identität*. Der Beweis von (1) ist ein kombinatorischer, wohingegen der Beweis der Identität aus 3.7 nicht kombinatorisch ist.

**Beispiel 3.9.** Mit der Konvention  $\binom{m}{k} = 0$  für  $m < k$  gilt für  $a, b, n \in \mathbb{N}$ :

$$\sum_{0 \leq i \leq n} \binom{a}{i} \binom{b}{n-i} = \binom{a+b}{n}.$$

*Erster Beweis.* Beweis durch Induktion nach  $a + b$ . Ein solcher Beweis ist möglich, aber “dumm”.  $\square$

*Zweiter Beweis.* Beweis über erzeugende Funktionen:

$$\underbrace{\left(\sum_{i \geq 0} \binom{a}{i} X^i\right)}_{(1+X)^a} \underbrace{\left(\sum_{i \geq 0} \binom{b}{i} X^i\right)}_{(1+X)^b} = (1+X)^{a+b};$$

Koeffizientenvergleich.  $\square$

*Dritter Beweis.* (kombinatorisch.)  $\binom{a+b}{n}$  ist die Anzahl der  $n$ -Teilmengen von  $\mathbb{N}_{a+b}$ . Teile  $\mathbb{N}_{a+b}$  auf in die  $a$  Zahlen  $1, \dots, a$  einerseits und die  $b$  Zahlen  $a+1, \dots, a+b$  andererseits; fertig!  $\square$

Oft sind wir an Angaben über die Größenordnung von  $f(n)$  interessiert; solche Angaben können eventuell durch Formeln, Rekursionen oder erzeugende Funktionen gewonnen werden — dies *muß* aber nicht der Fall sein!

Betrachten wir als ein Beispiel  $f(n, k)$  aus 3.2, also  $f(n, k) = \frac{n!}{(n-k)!}$ . Allgemein gilt die *Stirling-Formel*

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}, \text{ d.h. } \lim_{n \rightarrow \infty} \frac{\left(\frac{n}{e}\right)^n \sqrt{2\pi n}}{n!} = 1.$$

Diese Formel liefert eine für praktische Zwecke brauchbare Approximation für  $n!$ ; z.B. ist der relative Fehler bei  $n = 5$  kleiner als 2 %.

Damit gilt

$$f(n, k) \approx \frac{n^n}{(n-k)^{n-k} e^k} \sqrt{\frac{n}{n-k}} \cdot;$$

Ähnlich gute Approximationen für 3.3 und 3.4 sind nicht bekannt. Man kann aber noch im Beispiel der Fibonacci-Zahlen (3.5 bzw. 3.8) etwas aussagen. Es ist dort

$$F(X) = \sum_{n \geq 0} f(n) X^n = \frac{1}{1-X-X^2} = \frac{1}{(1-\tau X)(1-\bar{\tau} X)};$$

ferner weiß man, daß  $F(X)$  konvergiert für alle  $z \in \mathbb{C}$  mit  $|z| < \min\{|\tau|, |\bar{\tau}|\}$ . Dieses Minimum ist  $-\bar{\tau} = \frac{\sqrt{5}-1}{2}$ ; es gilt also  $\rho(F) = \frac{\sqrt{5}-1}{2}$ . Daraus folgt mit der Formel von Abel-Hadamard

$$\overline{\lim} |f(n)|^{\frac{1}{n}} = \frac{1}{\rho(F)} = \frac{\sqrt{5}+1}{2} = \tau.$$

Heuristisch heißt dies: “ $f(n)$  wächst nicht schneller als  $\tau^n$ ”. Diese Aussage ist schärfer als diejenige, die man aus der expliziten Formel bekommen würde (diese Formel lautete ja  $f(n) = \frac{1}{\sqrt{5}}(\tau^{n+1} - \bar{\tau}^{n+1})$ ).

Im Zusammenhang mit Angaben über die Größenordnung von  $f(n)$  werden wir folgende Sprechweisen benutzen:

**Definition 3.10.** Seien  $f, g : \mathbb{N} \rightarrow \mathbb{C}$  gegeben. Schreibe

$$f \sim g \quad :\Leftrightarrow \quad \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1 ; \quad (\text{i})$$

$$f = \mathcal{O}(g) \quad :\Leftrightarrow \quad \exists C > 0 \text{ mit } |f(n)| \leq C \cdot |g(n)| \quad \forall n \in \mathbb{N} ; \quad (\text{ii})$$

$$f = \mathbf{o}(g) \quad :\Leftrightarrow \quad \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0 . \quad (\text{iii})$$

Diese Definitionen gelten sinngemäß auch für solche  $f, g$ , die nur auf unbeschränkten Teilmengen von  $\mathbb{N}$  definiert sind.

*Beispiele:*

$$\text{Zu (i):} \quad n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n} ;$$

$$\text{Zu (ii):} \quad f(n) = \mathcal{O}(\tau^n) \text{ für } f(n) \text{ aus 3.5/3.8 ;}$$

$$\text{Zu (iii):} \quad 2^n = \mathbf{o}(n!) .$$

## 4 Elementare Zählprobleme

**Definition 4.1.** Für eine Menge  $X$  sei  $\text{Sym}(X)$  die symmetrische Gruppe von  $X$ , also die Gruppe aller Bijektionen  $\pi : X \rightarrow X$ . Die Elemente von  $\text{Sym}(X)$  heißen Permutationen von  $X$ . Wir schreiben  $S_n$  für  $\text{Sym}(\mathbb{N}_n)$ .

Es gilt:

- $|X| = |Y| \Rightarrow \text{Sym}(X) \cong \text{Sym}(Y)$  (dies erlaubt es häufig, bei  $|X| = n$  ohne Einschränkung  $X = \mathbb{N}_n$  anzunehmen);
- $|S_n| = n(n-1)(n-2) \cdots 2 \cdot 1 =: n!$  für  $n \in \mathbb{N}$ ; weiter definieren wir  $0! := 1$  ;
- $|S_n| = n!$  ist die Zahl aller Anordnungen von  $\mathbb{N}_n$ .

**Satz 4.2.** (hier ohne Beweis)

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

Eine noch bessere Näherung liefert der Ausdruck  $\left(\frac{n}{e}\right)^n \sqrt{2\pi n} \cdot e^{\frac{1}{12n}}$ .

**Beobachtung 4.3.** Die Zahl der Abbildungen einer  $k$ -Menge in eine  $n$ -Menge ist  $n^k$ ; diese Zahl ist gleich der Anzahl der Wörter der Länge  $k$  aus einem Alphabet mit  $n$  Buchstaben.

*Anwendung:*  $|\mathfrak{P}(\mathbb{N}_n)| = 2^n$ , da eine Bijektion zwischen  $\mathfrak{P}(\mathbb{N}_n)$  und der Menge der Abbildungen  $\mathbb{N}_n \rightarrow \{0, 1\}$  ("charakteristische Funktionen" der Teilmengen) existiert.

**4.4.** Die Zahl der injektiven Abbildungen einer  $k$ -Menge in eine  $n$ -Menge (also die Zahl der  $k$ -Wörter aus einem  $n$ -Alphabet, wobei jedes Wort jeden Buchstaben nur höchstens einmal enthält) ist gleich

$$\underbrace{n(n-1)(n-2)\cdots(n-k+1)}_{k \text{ Faktoren}} =: (n)_k$$

(für  $k > n$  setzen wir  $(n)_k = 0$ ).

**4.5.** Die Zahl der  $k$ -Teilmengen einer  $n$ -Menge (also die Zahl der Möglichkeiten, aus  $n$  nummerierten Objekten  $k$  Objekte auszuwählen) ist gleich der Anzahl der injektiven Abbildungen einer  $k$ -elementigen Indexmenge in diese  $n$ -Menge unter Absehen von der Reihenfolge der Werte einer solchen Abbildung, also gleich

$$\frac{(n)_k}{k!} = \frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k} =: \binom{n}{k}$$

(auch hier setzen wir  $\binom{n}{k} := 0$  für  $k > n$ ).

*Anwendung:*

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

**4.6.** Was passiert, wenn beim “Urnenexperiment” in (4.5) jedes Objekt nach Ziehen zurückgelegt wird?

*Definition:* eine *Multimenge*  $(X, m)$  ist eine Menge  $X$ , versehen mit einer Abbildung  $m : X \rightarrow \mathbb{N}_0$ ; für  $x \in X$  heißt  $m(x)$  die *Multiplizität* oder *Vielfachheit* von  $x$  in  $(X, m)$ . Ist  $X$  endlich, so heißt  $\sum_{x \in X} m(x)$  die *Kardinalität* von  $(X, m)$ .

Unsere Frage lautet also: Auf wieviele Weisen können wir Multimengen der Kardinalität  $k$  aus einer  $n$ -Menge  $X$  bilden?

**Satz 4.7.** Die Zahl der  $k$ -Multimengen aus einer  $n$ -Menge ist  $\binom{n+k-1}{k}$ .

*Beweis.* Wir konstruieren eine Bijektion von der Menge der  $k$ -Multimengen in  $\mathbb{N}_n$  mit der Menge der  $k$ -Mengen in  $\mathbb{N}_{n+k-1}$ . Sei dazu  $(X, m)$  eine  $k$ -Multimenge in  $\mathbb{N}_n$ ;  $X$  hat eine Darstellung

$$X = \{a_1, \dots, a_r\} \text{ mit } a_1 < \dots < a_r \text{ für ein } r \leq k, n .$$

Führe nun zu jedem  $a_i$  so viele “Kopien” ein, wie die Multiplizität von  $a_i$  angibt:

$$\begin{aligned} b_1 = b_2 = \dots = b_{m(a_1)} &:= a_1 ; \\ b_{m(a_1)+1} = \dots = b_{m(a_1)+m(a_2)} &:= a_2 ; \\ &\dots \\ b_{k-m(a_r)+1} = \dots = b_k &:= a_r ; \end{aligned}$$

für diese  $k$  Zahlen  $b_1, \dots, b_k$  gilt offenbar  $b_1 \leq b_2 \leq \dots \leq b_k$ . Man kann  $(X, m)$  durch  $(b_j)_{1 \leq j \leq k}$  repräsentieren.

Setze jetzt  $Y := \{b_1, b_2 + 1, b_3 + 2, \dots, b_j + j - 1, \dots, b_k + k - 1\}$ . Man überlegt sich:

- die Elemente von  $Y$  (die Zahlen der Form  $b_j + j - 1$ ) sind paarweise verschieden;
- sie liegen alle in  $\mathbb{N}_{n+k-1}$ ;
- jede Teilmenge von  $\mathbb{N}_{n+k-1}$  tritt als ein solches  $Y$  auf (die Abbildung  $(X, m) \mapsto Y$  ist also surjektiv);
- Die Abbildung  $(X, m) \mapsto Y$  ist injektiv.

Daraus ergibt sich die Behauptung. □

**Satz 4.8.** (*Binomialsatz*) Sind  $X, Y$  Unbestimmte, so gilt

$$(X + Y)^n = \sum_{0 \leq k \leq n} \binom{n}{k} X^k Y^{n-k} .$$

*Erster Beweis.* Induktion nach  $n$ . □

*Zweiter Beweis.* (kombinatorisch) Multipliziere das Produkt

$$\underbrace{(X + Y)(X + Y) \cdots (X + Y)}_{n \text{ Faktoren}} \tag{*}$$

aus; da es jeweils 2 Summanden gibt, erhält man  $2^n$  Terme. Diese Terme entsprechen den Teilmengen von  $\mathbb{N}_n$ , und zwar entspricht die Teilmenge  $S \subset \mathbb{N}_n$  dem Term  $\prod_{1 \leq i \leq n} Z_i^{(S)}$ , wobei

$$Z_i^{(S)} := \begin{cases} X, & \text{falls } i \in S ; \\ Y & \text{sonst.} \end{cases}$$

Dies ist eine Bijektion (eine Injektion gleichmächtiger Mengen). Deshalb ist der Koeffizient von  $X^k Y^{n-k}$  in (\*) gleich der Zahl der  $k$ -Teilmengen von  $\mathbb{N}_n$ , d.h.  $\binom{n}{k}$ . □

*Bemerkung:* Das Interesse des zweiten Beweises liegt darin, daß sich das dort zur Anwendung gebrachte Prinzip besser zur Verallgemeinerung eignet als das Vorgehen des ersten Beweises.

**Proposition 4.9.** *Es gelten z.B.*

$$\begin{aligned} \sum_{0 \leq k \leq n} \binom{n}{k} &= 2^n & \text{(i)} & & \sum_{k \leq j \leq n} \binom{j}{k} &= \binom{n+1}{k+1} & \text{(v)} \\ \binom{n}{k} &= \binom{n}{n-k} & \text{(ii)} & & \sum_{0 \leq k \leq n} k \binom{n}{k} &= n \cdot 2^{n-1} & \text{(vi)} \\ \sum_{0 \leq k \leq n} (-1)^k \binom{n}{k} &= 0 \text{ für } n \geq 1 & \text{(iii)} & & \sum_{\substack{i+j=k \\ i,j \geq 0}} \binom{a}{i} \binom{b}{j} &= \binom{a+b}{k} & \text{(vii)} \\ \binom{n}{k} + \binom{n}{k+1} &= \binom{n+1}{k+1} & \text{(iv)} & & & & \end{aligned}$$

*Beweis.* (i): Dies kann man mit 4.8 oder alternativ über die kombinatorische Bedeutung der Binomialkoeffizienten (Stichwort Teilmengen; vgl. 4.5) zeigen.

(ii): Man erhält eine Bijektion auf  $\mathfrak{P}(\mathbb{N}_n)$ , wenn man jeder Teilmenge ihr Komplement in  $\mathbb{N}_n$  zuordnet.

(iii): Über 4.8.

(iv): Über die Definition der Binomialkoeffizienten oder alternativ über Teilmengen (in Analogie zum Beweis von 3.5).

(v): Jede  $k+1$ -Teilmenge von  $\mathbb{N}_{n+1}$  enthält als Maximum eine Zahl  $j+1$  zwischen  $k+1$  und  $n+1$ . Läßt man diese Zahl weg, so erhält man eine  $k$ -Teilmenge der ersten  $j$  Zahlen für ein  $k \leq j \leq n$ .

(vi): Man kann die Möglichkeiten, in  $\mathbb{N}_n$  eine Teilmenge und ein Element daraus auszuwählen, auf zwei verschiedene Arten zählen. Wählt man zuerst eine Zahl  $x$  aus, so hat man hierfür  $n$  Möglichkeiten; das Komplement  $\mathbb{N}_n - \{x\}$  hat  $2^{n-1}$  Teilmengen. Wählt man zuerst eine Teilmenge mit  $k$  Elementen aus, so hat man noch  $k$  Möglichkeiten, ein Element aus dieser Teilmenge auszuwählen.

(vii): Dies wurde schon bei 3.9 gezeigt. □

Diese Sammlung von Beweisen verdeutlicht, daß man in der Kombinatorik oft mehrere verschiedene Beweise für eine Aussage erbringen kann; es wird daher als Übung empfohlen, für die oben zusammengestellten Aussagen möglichst viele verschiedene Beweise zu erbringen.



*Definition:* Eine Zerlegung einer Menge  $X$  ist eine Darstellung

$$X = \dot{\bigcup}_{1 \leq i \leq r} S_i .$$

Mit  $k_i = |S_i|$  heißt  $(k_1, \dots, k_r)$  der *Typ* der Zerlegung.

**Proposition 4.11.**  $\binom{n}{k_1, k_2, \dots, k_r}$  ist die Zahl der Zerlegungen einer  $n$ -Menge in numerierte Teilmengen  $S_1, \dots, S_r$  mit  $|S_i| = k_i$ . Insbesondere ist  $\binom{n}{k_1, k_2, \dots, k_r} \in \mathbb{N}$  als Kardinalität einer Menge.

*Bemerkung:* Die Numerierung der  $S_i$  hat zur Folge, daß beispielsweise die beiden Zerlegungen  $S_1 = \{1, 2\}, S_2 = \{3, 4\}$  und  $S_1 = \{3, 4\}, S_2 = \{1, 2\}$  von  $\mathbb{N}_4$  als verschiedene Zerlegungen gezählt werden.

*Erster Beweis.* Induktion nach  $r$ ; Für  $r = 2$  (also für Binomialkoeffizienten) haben wir die Aussage in 4.5 bewiesen. Der Rest wird als Übung empfohlen (Hinweis: Fasse zwei der  $r$  Teilmengen zu einer zusammen).  $\square$

*Zweiter Beweis.* (Kombinatorisch) O.B.d.A sei die  $n$ -Menge die Menge  $\mathbb{N}_n$ . Ordnen wir alle Elemente von  $\mathbb{N}_n$  den Mengen  $S_1, S_2, \dots, S_r$  zu, so haben wir für  $S_1$  genau

$$\underbrace{n(n-1) \cdots (n-k_1+1)}_{k_1 \text{ Faktoren}}$$

Möglichkeiten, die in  $k_1!$  Reihenfolgen auftreten. Für  $S_2$  haben wir noch

$$\underbrace{(n-k_1)(n-k_1-1) \cdots (n-(k_1+k_2)+1)}_{k_2 \text{ Faktoren}}$$

Möglichkeiten, die in  $k_2!$  Reihenfolgen auftreten etc. Für  $S_r$  haben wir schließlich nur noch

$$\underbrace{\left( n - \left( \sum_{1 \leq i \leq r-1} k_i \right) \right) \left( n - \left( \sum_{1 \leq i \leq r-1} k_i \right) - 1 \right) \cdots 2 \cdot 1}_{k_r \text{ Faktoren}}$$

Möglichkeiten, die in  $k_r!$  Reihenfolgen auftreten. Zusammen haben wir also  $\frac{n!}{k_1!k_2! \cdots k_r!}$  Möglichkeiten.  $\square$

Einige der Eigenschaften von Binomialkoeffizienten aus Proposition 4.9 lassen sich analog für Multinomialkoeffizienten nachweisen. Wir stellen hier zwei solche Eigenschaften zusammen (weitere seien zur Übung empfohlen):

**Proposition 4.12.**

$$\sum_{\substack{k_1, \dots, k_r \in \mathbb{N}_0 \\ k_1 + \dots + k_r = n}} \binom{n}{k_1, \dots, k_r} = r^n ; \quad (\text{i})$$

$$\binom{n}{k_1, \dots, k_r} = \binom{n}{k_{\sigma(1)}, \dots, k_{\sigma(r)}} \quad \forall \sigma \in S_r . \quad (\text{ii})$$

□

(i) bringt zum Ausdruck, daß eine Zerlegung von  $\mathbb{N}_n$  in  $r$  disjunkte numerierte Teilmengen letztlich eine Abbildung  $\mathbb{N}_n \rightarrow \mathbb{N}_r$  ist.

**Satz 4.13.** (*Multinomialssatz*) Für Unbestimmte  $X_1, \dots, X_r$  gilt

$$(X_1 + \dots + X_r)^n = \sum_{\substack{k_1, \dots, k_r \in \mathbb{N}_0 \\ k_1 + \dots + k_r = n}} \binom{n}{k_1, \dots, k_r} X_1^{k_1} X_2^{k_2} \dots X_r^{k_r} .$$

*Erster Beweis.* Induktion nach  $n$ ; von diesem Weg wird abgeraten! □

*Zweiter Beweis.* (Kombinatorisch; hier kommt nun zum Tragen, daß der zweite Beweis von 4.8 sich leicht verallgemeinern läßt.) Multipliziere das Produkt

$$\underbrace{(X_1 + \dots + X_r)(X_1 + \dots + X_r) \dots (X_1 + \dots + X_r)}_{n \text{ Faktoren}} \quad (*)$$

aus; da es jeweils  $r$  Summanden gibt, erhält man  $r^n$  Terme. Diese Terme entsprechen bijektiv den Zerlegungen von  $\mathbb{N}_n$  in  $r$  disjunkte numerierte Teilmengen, und zwar entspricht der Zerlegung  $\mathbb{N}_n = S_1 \dot{\cup} \dots \dot{\cup} S_r$  der Term  $\prod_{1 \leq i \leq n} Z_i^{(S_1, \dots, S_r)}$  mit

$$Z_i^{(S_1, \dots, S_r)} := X_j, \text{ falls } i \in S_j .$$

Deshalb ist der Koeffizient von  $X_1^{k_1} X_2^{k_2} \dots X_r^{k_r}$  gleich der Zahl der Zerlegungen von  $\mathbb{N}_n$  vom Typ  $(k_1, \dots, k_r)$ , d.h.  $\binom{n}{k_1, \dots, k_r}$ . □

Bisher war  $n$  stets ein ganzzahliger Exponent; wir gehen nun zu reellen und komplexen Exponenten über. Die Potenz  $a^x$  ist wohldefiniert mit den üblichen Eigenschaften der Potenzrechnung, falls:

- $a \in \mathbb{R}_{>0}$  ;
- $x \in \mathbb{R}$  bzw.  $x \in \mathbb{C}$  .

Sei  $a = 1 + t$  mit  $t \in \mathbb{R}, |t| < 1$ ; betrachte die Funktion  $t \mapsto (1 + t)^x$  für festes  $x$  (definiert z.B. vermittle der Logarithmusfunktion und der Exponentialreihe). Was ergibt sich für die Reihenentwicklung der Funktion?

**Definition 4.14.** Für  $x \in \mathbb{R}, k \in \mathbb{N}_0$  sei

$$(x)_k := \underbrace{x(x-1)\cdots(x-k+1)}_{k \text{ Faktoren}}; \quad \binom{x}{k} := \frac{(x)_k}{k!} = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

(diese Definition verallgemeinert die Ausdrücke aus 4.4 bzw. 4.5).

**Satz 4.15.** (allgemeiner Binomialsatz; Newton.) Die Reihe  $\sum_{k \geq 0} \binom{x}{k} t^k$  konvergiert für  $x \in \mathbb{R}$  (sogar für  $x \in \mathbb{C}$ ) und  $|t| < 1$  gegen  $(1 + t)^x$ . (Hier ohne Beweis; dieser Satz wird in der Analysis bewiesen.)

**Korollar 4.16.** Für Unbestimmte  $X, Y$  gilt (z.B.)

$$\binom{X+Y}{k} = \sum_{\substack{i,j \geq 0 \\ i+j=k}} \binom{X}{i} \binom{Y}{j}.$$

(vgl. 4.9 (vii).)

*Erster Beweis.* Betrachte die Potenzreihe in drei Unbestimmten  $(1 + T)^{X+Y}$ ; diese ist gleich  $(1 + T)^X (1 + T)^Y$ . Als Koeffizient von  $T^k$  links findet man  $\binom{X+Y}{k}$ ; als Koeffizient von  $T^i$  im ersten Faktor rechts bzw.  $T^j$  im zweiten Faktor rechts findet man  $\binom{X}{i}$  bzw.  $\binom{Y}{j}$ .  $\square$

*Zweiter Beweis.* Polynome stimmen dann überein, wenn sie an genügend vielen Stellen übereinstimmen; verwende 4.9 (vii).  $\square$

## 5 Die Siebformel

**Problem 5.1.**  $n$  Personen sitzen auf  $n$  Stühlen, erheben sich und suchen sich zufällig einen neuen Sitzplatz. Wie groß ist die Wahrscheinlichkeit, daß alle auf anderen Plätzen als zuvor sitzen?

Mathematisch formuliert: Wie groß ist die Wahrscheinlichkeit  $P_n$  für eine zufällig gewählte Permutation  $\sigma \in S_n$ , fixpunktfrei zu sein (d.h. dafür, daß gilt  $\sigma(i) \neq i$  für alle  $i \in \mathbb{N}_n$ )?

Man überlegt sich leicht, daß  $P_1 = 0, P_2 = \frac{1}{2}, P_3 = \frac{1}{3}$  und  $P_4 = \frac{9}{24}$  ist. Wie sieht das Verhalten von  $P_n$  bei  $n \rightarrow \infty$  aus? Man unterscheidet sinnvollerweise die folgenden vier Möglichkeiten:  $\lim_{n \rightarrow \infty} P_n = 0, \lim_{n \rightarrow \infty} P_n = 1, \lim_{n \rightarrow \infty} P_n = C$  für  $C \in (0, 1)$  oder die



*Beweis.* Nach 5.2 gilt Gleichheit, falls  $t = n$  ist. Es genügt also zu zeigen, daß gilt:

$$\sum_{t < j \leq n} (-1)^{j+1} N_j \quad \begin{cases} \leq 0 & \text{für } t \text{ ungerade;} \\ \geq 0 & \text{für } t \text{ gerade.} \end{cases} \quad (*)$$

Dazu betrachten wir, ähnlich wie im Beweis von 5.2, den Beitrag von  $x \in X$  zu (\*). Für  $m = 0$  ist alles in Ordnung. Ist  $m > 0$ , so ist der Beitrag von  $x$  zur linken Seite von (\*)

$$\begin{aligned} \sum_{t < j \leq n} (-1)^{j+1} \binom{m}{j} &= \sum_{t < j \leq m} (-1)^{j+1} \binom{m}{j} = \sum_{0 \leq j \leq m} (-1)^{j+1} \binom{m}{j} - \sum_{0 \leq j \leq t} (-1)^{j+1} \binom{m}{j} \\ &= \sum_{0 \leq j \leq t} (-1)^j \binom{m}{j}. \end{aligned}$$

Nun gilt

$$\sum_{0 \leq j \leq t} (-1)^{t-j} \binom{m}{j} = \binom{m-1}{t},$$

wie man sich leicht über Potenzreihen klarmacht. Man vergleicht hierzu die Koeffizienten der beiden Potenzreihen  $(1+X)^{m-1}$  und  $(1+X)^m(1-X+X^2-X^3\dots)$  (der rechte Faktor der zweitgenannten Reihe ist ja nichts anderes als  $\frac{1}{1-X}$ ).

Also gilt auch

$$\sum_{0 \leq j \leq t} (-1)^j \binom{m}{j} = (-1)^t \binom{m-1}{t},$$

und damit ist man fertig. □

**Korollar 5.4.** Die Wahrscheinlichkeit  $P_n$  aus 5.1 ist

$$P_n := \sum_{0 \leq j \leq n} \frac{(-1)^j}{j!}.$$

Die Zahl der fixpunktfreien Elemente von  $S_n$  ist also  $D_n = n!P_n = \sum_{0 \leq j \leq n} \frac{(-1)^j n!}{j!}$ .

*Beweis.* Sei  $A_i$  erklärt wie zuvor; es gilt  $|A_i| = (n-1)!$  (die Anzahl der Permutationen der übrigen, nicht festgehaltenen Elemente). Sind die  $k_1, \dots, k_j$  alle verschieden, so ist  $|A_{k_1} \cap A_{k_2} \cap \dots \cap A_{k_j}| = (n-j)!$ . Also

$$\begin{aligned} \left| \bigcup_{1 \leq i \leq n} A_i \right| &\stackrel{\text{Siebformel}}{=} \sum_{1 \leq j \leq n} (-1)^{j+1} \sum_{\substack{T \subset \mathbb{N}_n \\ |T|=j}} (n-j)! \\ &= \sum_{1 \leq j \leq n} (-1)^{j+1} \binom{n}{j} (n-j)! \end{aligned}$$

Damit

$$D_n = n! - \sum_{1 \leq j \leq n} (-1)^{j+1} \frac{n!}{j!} = n! + \sum_{1 \leq j \leq n} (-1)^j \frac{n!}{j!} = \sum_{0 \leq j \leq n} (-1)^j \frac{n!}{j!}.$$

□

Damit hat man nun auch die Frage des Grenzwertens von  $P_n$  entschieden: Es ist

$$\lim_{n \rightarrow \infty} P_n = \sum_{j=0}^{\infty} \frac{(-1)^j}{j!} = e^{-1}.$$

**Satz 5.5.** Der Erwartungswert  $E_n$  für die Zahl der Fixpunkte einer zufällig ausgewählten Permutation  $\sigma \in S_n$  ist 1.

*Beweis.*

$$\begin{aligned} E_n &:= \frac{1}{n!} \sum_{\sigma \in S_n} |\{i \in \mathbb{N}_n \mid \sigma(i) = i\}| \\ &= \frac{1}{n!} \sum_{1 \leq k \leq n} k \cdot |\{\sigma \in S_n \mid \sigma \text{ hat genau } k \text{ Fixpunkte}\}| \\ &= \frac{1}{n!} \sum_{1 \leq k \leq n} k \binom{n}{k} D_{n-k} \end{aligned}$$

(wobei  $\binom{n}{k}$  die Anzahl der  $k$ -elementigen Fixpunktmengeten ist)

$$\begin{aligned} &= \frac{1}{n!} \sum_{1 \leq k \leq n} \left[ k \binom{n}{k} \sum_{0 \leq j \leq n-k} \frac{(-1)^j (n-k)!}{j!} \right] \\ &= \sum_{\substack{1 \leq k \leq n \\ 0 \leq j \leq n-k}} (-1)^j \frac{1}{(k-1)! j!} = \sum_{\substack{0 \leq k \leq n-1 \\ 0 \leq j \leq n-k-1}} (-1)^j \frac{1}{k! j!} =: (*) \end{aligned}$$

Setze  $k + j := t$ , also  $k = t - j$ . Damit ist

$$(*) = \sum_{0 \leq t \leq n-1} \frac{1}{t!} \sum_{0 \leq j \leq t} (-1)^j \binom{t}{j} = 1.$$

□

Solcherlei Ergebnisse sind von großer Bedeutung, da das Rechnen in  $S_n$  Ausgangspunkt für viele kombinatorische Überlegungen ist.

**Satz 5.6.** Die Zahl der Surjektionen von  $\mathbb{N}_t \rightarrow \mathbb{N}_n$  ist

$$\sum_{0 \leq j \leq n} (-1)^j \binom{n}{j} (n-j)^t .$$

*Beweis.* Setze dazu

$$\begin{aligned} X &:= \{f : \mathbb{N}_t \rightarrow \mathbb{N}_n\} ; \text{ es gilt also } |X| = n^t ; \\ A_i &:= \{f : \mathbb{N}_t \rightarrow \mathbb{N}_n \mid f \text{ "vermeidet" } i \in \mathbb{N}_n\} \forall i \in \mathbb{N}_n . \end{aligned}$$

Gesucht ist also  $|X - \bigcup A_i|$ ; es gilt  $|A_i| = (n-1)^t$  für alle  $i$  und  $|A_{i_1} \cap \dots \cap A_{i_j}| = (n-j)^t$ , falls die  $i_1, \dots, i_j$  paarweise verschieden sind. Mit der Siebformel ermittelt man

$$\left| \bigcup_{1 \leq i \leq n} A_i \right| = \sum_{1 \leq j \leq n} (-1)^{j+1} \sum_{\substack{S \subset \mathbb{N}_n \\ |S|=j}} (n-j)^t = \sum_{1 \leq j \leq n} (-1)^{j+1} \binom{n}{j} (n-j)^t .$$

Daher

$$|X - \bigcup A_i| = n^t - \sum_{1 \leq j \leq n} (-1)^{j+1} \binom{n}{j} (n-j)^t = \sum_{0 \leq j \leq n} (-1)^j \binom{n}{j} (n-j)^t .$$

□

*Bemerkung:* Die Formel gilt für beliebige  $t, n \in \mathbb{N}$ . Für  $t < n$  ist also

$$\sum_{0 \leq j \leq n} (-1)^j \binom{n}{j} j^t = 0 .$$

**Satz 5.7.** Sei  $X$  eine endliche Menge, und seien  $f, g$  Funktionen von  $\mathfrak{P}(X)$  nach  $\mathbb{C}$ . Dann sind äquivalent:

$$\forall S \in \mathfrak{P}(X) \text{ gilt } g(S) = \sum_{T \subset S} f(T) ; \tag{i}$$

$$\forall S \in \mathfrak{P}(X) \text{ gilt } f(S) = \sum_{T \subset S} (-1)^{|S-T|} g(T) . \tag{ii}$$

Das Verhältnis zwischen  $f$  und  $g$  ist vergleichbar dem zwischen einer Funktion und ihrer Fouriertransformierten. Aus dem ausgesprochenen Satz kann die ursprüngliche Siebformel als Korollar erhalten werden (Übung). Eine Theorie, die solche Siebformeln verallgemeinert, ist die Theorie der Möbius-Funktionen.

*Beweis.* Wir zeigen (i)  $\Rightarrow$  (ii); die andere Richtung geht "genauso" und wird zur Übung empfohlen.

Angenommen,  $f$  und  $g$  genügen der Bedingung (i). Dann ist für festes  $S$

$$\sum_{T \subset S} (-1)^{|S-T|} g(T) = \sum_{T \subset S} (-1)^{|S-T|} \sum_{R \subset T} f(R) = \sum_{R \subset S} \left( \sum_{\substack{T \\ R \subset T \subset S}} (-1)^{|S-T|} f(R) \right).$$

Über den Koeffizienten von  $f(R)$  behaupten wir

$$\sum_{\substack{T \\ R \subset T \subset S}} (-1)^{|S-T|} = \begin{cases} 0, & \text{falls } R \subsetneq S; \\ 1, & \text{falls } R = S; \end{cases}$$

ist diese Behauptung gezeigt, so sind wir fertig. In der Tat ist

$$\begin{aligned} \sum_{\substack{T \\ R \subset T \subset S}} (-1)^{|S-T|} &= \sum_{0 \leq i \leq |S-R|} (-1)^{|S-R|-i} \cdot |\{T \mid |T-R| = i\}| \\ &= (-1)^{|S-R|} \sum_{0 \leq i \leq |S-R|} (-1)^i \binom{|S-R|}{i} = \begin{cases} 1, & \text{falls } |S-R| = 0; \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

□

**Beispiel 5.8.** Für  $\sigma \in S_n$  sei  $D(\sigma) := \{i \in \mathbb{N}_{n-1} \mid \sigma(i) > \sigma(i+1)\}$ . Wir fragen: für wieviele  $\sigma \in S_8$  gilt  $D(\sigma) \subset \{1, 4, 6\}$ , für wieviele gilt  $D(\sigma) = \{1, 4, 6\}$ ? Wegen  $|S_8| = 8! = 40320$  empfiehlt es sich nicht, das Problem direkt anzugehen. Wir lösen es in folgenden Schritten:

(i) Seien für  $S \subset \mathbb{N}_7$

$$\begin{aligned} g(S) &:= |\{\sigma \in S_8 \mid D(\sigma) \subset S\}|; \\ f(S) &:= |\{\sigma \in S_8 \mid D(\sigma) = S\}|. \end{aligned}$$

Die so definierten Funktionen stehen offensichtlich in der Beziehung (i) von Satz 5.7, also auch in der Beziehung (ii) dieses Satzes.

(ii) Bestimme  $g(\{1, 4, 6\})$ . Für  $\sigma \in S_8$  gilt:

$$D(\sigma) \subset \{1, 4, 6\} \Leftrightarrow \sigma(2) < \sigma(3) < \sigma(4), \sigma(5) < \sigma(6), \sigma(7) < \sigma(8).$$

Wie viele derartige  $\sigma$  gibt es? Man hat folgende Wahlmöglichkeiten:

Wähle $\sigma(1)$ beliebig	$\binom{8}{1}$ Möglichkeiten
Wähle $\sigma(2) < \sigma(3) < \sigma(4)$ beliebig in $\mathbb{N}_8 - \{\sigma(1)\}$	$\binom{7}{3}$ Möglichkeiten
Wähle $\sigma(5) < \sigma(6)$ beliebig in $\mathbb{N}_8 - \{\sigma(1), \sigma(2), \sigma(3), \sigma(4)\}$	$\binom{4}{2}$ Möglichkeiten
Wähle $\sigma(7) < \sigma(8)$ beliebig in $\mathbb{N}_8 - \{\sigma(1), \sigma(2), \sigma(3), \sigma(4), \sigma(5), \sigma(6)\}$	$\binom{2}{2}$ Möglichkeiten

Insgesamt hat man also  $8 \cdot 35 \cdot 6 = 1860$  Möglichkeiten, d.h.  $g(\{1, 4, 6\}) = 1860$ .

(iii) Nach 5.7 ist  $f(\{1, 4, 6\}) = \sum_{T \subset \{1, 4, 6\}} (-1)^{3-|T|} g(T)$ . Man hat folgende Tabelle:

$T$	Bedingung an $\sigma$ mit $D(\sigma) \subset T$	Zahl der Möglichkeiten	$g(T)$
$\emptyset$	$\sigma(1) < \dots < \sigma(8)$	1	1
$\{1\}$	$\sigma(2) < \sigma(3) < \dots < \sigma(8)$	$\binom{8}{1} \binom{7}{7}$	8
$\{4\}$	$\sigma(1) < \dots < \sigma(4), \sigma(5) < \dots < \sigma(8)$	$\binom{8}{4} \binom{4}{4}$	70
$\{6\}$	$\sigma(1) < \dots < \sigma(6), \sigma(7) < \sigma(8)$	$\binom{8}{6} \binom{2}{2}$	28
$\{1, 4\}$	$\sigma(2) < \dots < \sigma(4), \sigma(5) < \dots < \sigma(8)$	$\binom{8}{1} \binom{7}{3} \binom{4}{4}$	280
$\{1, 6\}$	Übung	$\binom{8}{1} \binom{7}{5}$	168
$\{4, 6\}$	Übung	$\binom{8}{4} \binom{4}{2}$	420
$\{1, 4, 6\}$	s.o.	s.o.	1680

Also ist  $f(\{1, 4, 6\}) = 1680 - 420 - 168 - 280 + 28 + 70 + 8 - 1 = 917$ ; es gibt demnach genau 917 Elemente  $\sigma$  von  $S_8$  mit  $\sigma(1) > \sigma(2) < \sigma(3) < \sigma(4) > \sigma(5) < \sigma(6) > \sigma(7) < \sigma(8)$ .

## 6 Permutationen

**Definition 6.1.** Es sei  $G$  eine Gruppe,  $X$  eine nichtleere Menge. Eine Operation von  $G$  auf  $X$  ist eine Abbildung  $G \times X \rightarrow X$ ,  $(g, x) \mapsto gx$  mit den Eigenschaften

- (i)  $1_G \cdot x = x \forall x \in X$  ;
- (ii)  $(gh)x = g(hx) \forall g, h \in G, x \in X$  .

**Lemma 6.2.** Sei eine Operation von  $G$  auf  $X$  gegeben. Es gelten:

- (i) Für alle  $g \in G$  ist  $\pi(g) : X \rightarrow X, x \mapsto gx$  eine Bijektion von  $X$  auf sich; die Inverse von  $\pi(g)$  ist  $\pi(g^{-1})$ .
- (ii) Die Abbildung  $\pi : G \rightarrow \text{Sym}(X), g \mapsto \pi(g)$  (definiert wie in (i)) ist ein Gruppenhomomorphismus.
- (iii) Ist ein Homomorphismus  $\pi : G \rightarrow \text{Sym}(X)$  gegeben, so definiert für  $g \in G, x \in X$  die Abbildung  $gx := (\pi(g))x$  eine Operation von  $G$  auf  $X$ . Auf diese Weise erhalten wir eine kanonische Bijektion zwischen der Menge der Operationen von  $G$  auf  $X$  und  $\text{Hom}(G, \text{Sym}(X))$ .

*Beweis.* Übung. □

**Beispiele 6.3.** (i)  $S_n$  operiert tautologisch auf  $\mathbb{N}_n$  durch die Vorschrift  $\sigma i := \sigma(i)$  für  $\sigma \in S_n, i \in \mathbb{N}_n$ .

(ii) Sei  $X := \mathbb{R}^n$  mit Standardbasis  $B := \{e_1, \dots, e_n\}$  gegeben.  $S_n$  operiert auf  $B$  durch Umnummerieren:  $\sigma e_i := e_{\sigma(i)}$  für alle  $i \in \mathbb{N}_n$ .

Entsprechend operiert  $S_n$  auf  $\mathbb{R}^n$  durch lineare Fortsetzung:

$$\sigma \left( \sum_{1 \leq i \leq n} a_i e_i \right) = \sum_{1 \leq i \leq n} a_i e_{\sigma(i)} = \sum_{1 \leq i \leq n} a_{\sigma^{-1}(i)} e_i .$$

(iii) Ist  $G$  eine beliebige Gruppe, so operiert  $G$  auf  $X := G$  durch Multiplikation: Für  $g \in G, x \in X$  ist  $gx := g \cdot x$ .

(iv) Ist  $G$  eine beliebige Gruppe, so operiert  $G$  auf  $X := G$  durch Konjugation; schreibt man für die Operation das Zeichen  $*$ , so ist also  $g * x := gxg^{-1}$  für  $g, x \in X$ .

**Definition/Lemma 6.4.**  $G$  operiere auf  $X$ . Es gelten:

(i) Für  $x, y \in X$  sei

$$x \sim_G y :\Leftrightarrow \exists g \in G \text{ mit } y = gx .$$

Dann ist “ $\sim$ ” eine Äquivalenzrelation auf  $X$ . Die Äquivalenzklassen bezüglich “ $\sim$ ” heißen Bahnen oder Orbits von  $G$  in  $X$ . Die Bahn von  $x$  wird mit  $Gx$  oder  $[x]$  bezeichnet, die Menge aller Äquivalenzklassen mit  $G \setminus X$ .

(ii) Ein  $x \in X$  heißt Fixpunkt von  $g \in G$ , falls  $gx = x$  gilt.

(iii) Für  $x \in X$  heißt  $G_x := \{g \in G \mid gx = x\}$  die Fixgruppe von  $x$ .

(iv) Die Abbildung  $G/G_x \rightarrow Gx, gG_x \mapsto gx$  ist für alle  $x \in X$  wohldefiniert und bijektiv. □

*Folgerung:* Ist  $|G| < \infty$ , so ist  $|Gx|$  ein Teiler von  $|G|$  für alle  $x \in X$ .

*Bemerkung:* Wir haben bisher nur Operationen von  $G$  auf  $X$  von links betrachtet. Analog definiert man Operationen von rechts als Abbildungen von  $X \times G$  nach  $X$  mit Eigenschaften entsprechend denen aus 6.1. Die Lemmata 6.2 und 6.4 gelten dann sinngemäß auch für solche Operationen; die Bahnen werden mit  $xG$  und die Menge der Bahnen mit  $X/G$  bezeichnet.

**Satz 6.5** (Burnside-Lemma). *Die endliche Gruppe  $G$  operiere auf der endlichen Menge  $X$ . Dann gilt:*

$$|G \setminus X| = \frac{1}{|G|} \sum_{g \in G} \phi_g ,$$

wobei  $\phi_g$  die Anzahl der Fixpunkte von  $g$  bezeichnet. Insbesondere ist also der Mittelwert über die Fixpunktzahlen eine ganze Zahl.

*Beweis.* Sei  $S := \{(g, x) \in G \times X \mid gx = x\}$ . Dann gilt einerseits  $|S| = \sum_{g \in G} \phi_g$ ; andererseits ist

$$|S| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|} = |G| \sum_{G \setminus X} 1 = |G| |G \setminus X|$$

(wobei sich die vorletzte Gleichheit daraus ergibt, daß jedes der  $|Gx|$  Elemente einer Bahn  $Gx$  einen Summanden  $\frac{1}{|Gx|}$  beiträgt). □

**Korollar 6.6.** (vgl. 5.5) *Der Erwartungswert für die Zahl der Fixpunkte einer zufällig gewählten Permutation aus  $S_n$  ist 1.*

*Beweis.* Es gibt nur eine Bahn der tautologischen Operation von  $S_n$  auf  $\mathbb{N}_n$ . □

**Korollar 6.7.** *Sei  $G$  eine endliche Gruppe. Dann gilt*

$$|\{\text{Konjugationsklassen in } G\}| = \frac{1}{|G|} \sum_{g \in G} |\text{Zent}_G(g)| ,$$

wobei  $\text{Zent}_G(g) := \{h \in G \mid hg = gh\}$ . □

**Definition 6.8.** *Ein Element  $\pi$  von  $S_n$  wird geschrieben*

(a) *als Wort:  $\pi = \pi(1), \pi(2), \dots, \pi(n)$ . In dieser Darstellung werden die Kommata meist weggelassen.*

Beispiel: 1423 bezeichnet die Permutation  $\begin{pmatrix} 1 \mapsto 1 \\ 2 \mapsto 4 \\ 3 \mapsto 2 \\ 4 \mapsto 3 \end{pmatrix}$

b) *als Zykelprodukt: Hierbei sind folgende Nebenbedingungen vorgegeben:*

- $l_i$  ist der kleinste positive Exponent  $l$  von  $\pi$  mit  $\pi^l x_i = x_i$ ;
- die durch die Klammern beschriebenen Teilmengen von  $\mathbb{N}_n$  sind disjunkt;
- $\sum_{1 \leq i \leq k} l_i = n$ .

Die Teilausdrücke der Form  $(x_i, \pi(x_i), \pi^2(x_i), \dots, \pi^{l_i-1}(x_i))$  heißen Zykel von  $\pi$ ; sie werden meist ohne Kommata geschrieben.

Die Darstellung  $(*)$  ist für  $\pi \in S_n$  nicht eindeutig, denn 1) die Zykeln können beliebig vertauscht werden und 2) jedes Element eines Zyklus kann an dessen erste Stelle geschrieben werden, ohne  $\pi$  zu verändern.

Z.B. ist  $\pi_0 := (134)(25)(67) = (76)(413)(25)$  in  $S_7$ .

Die Standarddarstellung von  $\pi \in S_n$  ist die Darstellung als Zykelprodukt, wobei Eindeutigkeit hergestellt wird durch die zusätzlichen Nebenbedingungen:

- in jedem Zykel steht das größte Element vorn;
- die Zykeln werden ansteigend nach der Größe ihres größten Elements geordnet.

Die Standarddarstellung von  $\pi_0$  ist also  $(413)(52)(76)$ .

Die verschiedenen Zykeln einer Zykeldarstellung von  $\pi$  entsprechen den Bahnen auf  $\mathbb{N}_n$  von  $\langle \pi \rangle$ , der von  $\pi$  in  $S_n$  erzeugten Untergruppe.

**Lemma 6.9.** Die Abbildung  $(\hat{\phantom{x}}) : S_n \rightarrow S_n$ ,  $\pi \mapsto \hat{\pi}$  sei folgendermaßen definiert:  $\hat{\pi}$  habe als Wortdarstellung das Wort, das man aus der Standarddarstellung von  $\pi$  durch Weglassen der Klammern erhält. Dann ist diese Abbildung bijektiv.

Beispiel: Zu  $\pi_0 \in S_7$  wie oben ist  $\hat{\pi}_0 = 4135276 = (1452)(3)(67) = (3)(5214)(76)$  in Standarddarstellung.

*Beweis.* Sei ein Wort  $a_1 a_2 \cdots a_n$  gegeben; es ist also  $\{a_1, a_2, \dots, a_n\} = \mathbb{N}_n$ . Füge vor  $a_j$  eine linke Klammer ein, wenn gilt  $a_j > a_i$  für alle  $i < j$ ; ergänze durch passende rechte Klammern. Dann hat man die Standarddarstellung des Urbildes von  $a_1 \cdots a_n$  unter der Abbildung  $(\hat{\phantom{x}})$ .  $\square$

Hat  $\pi$  die Wortdarstellung  $a_1 \cdots a_n$ , so heißt  $a_j$  ein *Links-Rechts-Maximum*, falls gilt  $a_j > a_i$  für alle  $i < j$ . Nach dem Lemma hat die Teilmenge von  $S_n$  aller Permutationen mit einer vorgegebenen Zahl von Links-Rechts-Maxima genauso viele Elemente wie die Teilmenge von  $S_n$  aller Permutationen, die (dieselbe) vorgegebene Zahl von Zykeln haben.

**Definition 6.10.** Für  $\pi \in S_n$  sei  $c_i = c_i(\pi)$  die Zahl der Zyklen der Länge  $i$  in einer Zykeldarstellung von  $\pi$ . Dann heißen

$\text{typ}(\pi) := (c_1, \dots, c_n)$  der Zykeltyp von  $\pi$  und

$c(\pi) := \sum_{1 \leq i \leq n} c_i(\pi)$  die Zykelzahl von  $\pi$ .

Der Zykeltyp liefert eine Zerlegung

$$\underbrace{1 + \dots + 1}_{c_1} + \underbrace{2 + \dots + 2}_{c_2} + \dots + \underbrace{k + \dots + k}_{c_k} = n ;$$

solche Zerlegungen von  $n$  als Summen heißen Partitionen von  $n$ .

Setze  $p(n) := |\{\text{Partitionen von } n\}|$ . Es ist

$p(3) = 3$ , denn die Partitionen von 3 sind  $3, 1 + 2, 1 + 1 + 1$ ;

$p(4) = 5$ , denn die Partitionen von 4 sind  $4, 1 + 3, 2 + 2, 1 + 1 + 2, 1 + 1 + 1 + 1$ .

**Proposition 6.11.** (i) Zwei Permutationen  $\pi, \pi' \in S_n$  haben genau dann den gleichen Zykeltyp, wenn sie konjugiert sind. Es gilt also

$$|\{\text{Konjugationsklassen von } S_n\}| = p(n) .$$

(ii) Die Zahl der  $\pi \in S_n$  mit Zykeltyp  $\underline{c} = (c_1, \dots, c_n)$  ist

$$\frac{n!}{1^{c_1} \cdot c_1! \cdot 2^{c_2} \cdot c_2! \cdot \dots \cdot n^{c_n} \cdot c_n!} .$$

*Beweis.* (i) “ $\Leftarrow$ ”. Sei  $\pi' = \sigma\pi\sigma^{-1}$  mit  $\sigma \in S_n$ . Aus einem Zykel  $(a_1 a_2 \dots a_l)$  in einer Zykeldarstellung von  $\pi$  wird durch die Konjugation der Zykel  $(\sigma(a_1)\sigma(a_2)\dots\sigma(a_l))$ ;  $\pi$  und  $\pi'$  haben also gleichen Zykeltyp.

“ $\Rightarrow$ ”. Sei  $\pi = (a_1 \dots a_l)(b_1 \dots b_m)(\dots)$  eine Darstellung für  $\pi$ . Dann gibt es eine Darstellung  $\pi' = (a'_1 \dots a'_l)(b'_1 \dots b'_m)(\dots)$ . Definiere  $\sigma \in S_n$  durch  $\sigma(a_i) := a'_i$  für  $1 \leq i \leq l$ ,  $\sigma(b_j) := b'_j$  für  $1 \leq j \leq m$  etc. Dann ist nach dem Vorhergehenden  $\pi' = \sigma\pi\sigma^{-1}$ .

(ii) Betrachte die Abbildung

$$\begin{array}{ccc} S_n & \rightarrow & S_{n, \underline{c}} := \{\pi \in S_n \mid \text{typ}(\pi) = \underline{c}\} \\ \underbrace{a_1 \dots a_n}_{\text{Wort}} & \mapsto & \underbrace{(a_1) \dots (a_{c_1})}_{c_1 \text{ Zykel der Länge } 1} \underbrace{(a_{c_1+1} a_{c_1+2}) \dots (a_{c_1+c_2-1} a_{c_1+c_2})}_{c_2 \text{ Zykel der Länge } 2} \dots ; \end{array}$$

wegen  $\sum_{1 \leq i \leq n} c_i \cdot i = n$  ergibt sich insgesamt ein Zykelprodukt der Länge  $n$ , bestehend aus jeweils  $c_i$  Zykeln der Länge  $i$ . Die Abbildung ist wohldefiniert und surjektiv (dies überlegt man sich durch Weglassen der Klammern). Die Zahl der Urbilder eines festen Elements

$\pi \in S_{n,c}$  ist gleich der Zahl der verschiedenen Zykeldarstellungen von  $\pi$  mit Zykeln, die der Länge nach angeordnet sind, also gleich  $1^{c_1} \cdot c_1! \cdot 2^{c_2} \cdot c_2! \cdot \dots \cdot n^{c_n} \cdot c_n!$  (diese Zahl kommt so zustande, daß man zum einen nur noch Zykel gleicher Länge miteinander vertauschen kann — daher die Faktoren  $c_i!$  — und zum andern jeweils  $i$  Möglichkeiten für das erste Element eines der  $c_i$  Zykeln der Länge  $i$  hat — daher die Faktoren  $i^{c_i}$ ).

□

**Definition 6.12.** Für ganze Zahlen  $n, k$  seien Zahlen  $c(n, k)$  und  $s(n, k)$  wie folgt definiert:

$$c(n, k) := \begin{cases} \text{Zahl der } \pi \in S_n \text{ mit } c(\pi) = k, \text{ falls } n, k \in \mathbb{N}, n \geq k ; \\ 0, \text{ falls } n < k ; \\ 0, \text{ falls } n \geq k, \text{ wobei } n \leq 0 \text{ oder } k \leq 0 \text{ und } (n, k) \neq (0, 0) ; \\ 1 \text{ für } (n, k) = (0, 0) ; \end{cases}$$

$$s(n, k) := (-1)^{n-k} c(n, k) .$$

Diese Zahlen heißen Stirling-Zahlen erster Art. Die  $c(n, k)$  heißen unsigniert, die  $s(n, k)$  signiert.

**Proposition 6.13.** Für  $n, k \geq 1$  gelten die Rekursionsformeln

$$\begin{aligned} c(n, k) &= (n-1)c(n-1, k) + c(n-1, k-1) ; \\ s(n, k) &= -(n-1)s(n-1, k) + s(n-1, k-1) . \end{aligned}$$

*Beweis.* Sei  $\pi' \in S_{n-1}$  mit genau  $k$  Zykeln durch seine Standarddarstellung gegeben. Wir können  $n$  hinter jede der  $n-1$  Zahlen dieser Darstellung einfügen, wodurch wir genau  $n-1$  Elemente  $\pi$  von  $S_n$  erhalten, in denen  $n$  in Zykeln der Länge  $\geq 2$  erscheint; man erhält so alle derartigen  $\pi$  von  $S_n$ . In den verbleibenden Permutationen  $\pi'' \in S_n$  mit  $k$  Zykeln ist  $\pi''(n) = n$ , d.h.  $\pi''$  ist Fortsetzung einer Permutation von  $\mathbb{N}_{n-1}$  mit  $k-1$  Zykeln. □

**6.14. Wertetabelle für  $c(n, k)$ :**

$c(n, k)$	$k = 1$	2	3	4
$n = 1$	1	0	0	0
2	1	1	0	0
3	2	3	1	0
4	6	11	6	1
5	24	50	35	10
6	120	274	225	85

*Bemerkung:* Es gelten

$$\sum_k c(n, k) = n! ; \quad c(n, 1) = (n-1)!$$

**Proposition 6.15.** Für  $n \geq 1$  gelten

$$\begin{aligned} \sum_{1 \leq k \leq n} c(n, k) X^k &= X(X+1) \cdots (X+n-1) = (X+n-1)_n ; \\ \sum_{1 \leq k \leq n} s(n, k) X^k &= X(X-1) \cdots (X-n+1) = (X)_n . \end{aligned} \tag{i}$$

*Beweis.* (ii) folgt direkt durch Ersetzen von  $X$  durch  $-X$  in (i); (i) ergibt sich durch Induktion nach  $n$  unter Verwendung der Rekursionsformel 6.13.  $\square$

Für die  $s(n, k)$  sind bekannt:

- verschiedene explizite Formeln;
- erzeugende Funktionen für festes  $n$  oder festes  $k$ ;
- verschiedene Identitäten.

Solche Ergebnisse finden sich in “besseren” Formelsammlungen.

**6.16.** Seien  $n, k \geq 1$ . Es gilt:

$$c(n, k) := |\{\pi \in S_n \mid c(\pi) = k\}| \tag{1}$$

$$\stackrel{6.9}{=} |\{\pi \in S_n \mid \pi \text{ hat genau } k \text{ Links-Rechts-Maxima}\}| \tag{2}$$

$$\stackrel{6.15}{=} k\text{-Koeffizient von } (X+n-1)_n = |k\text{-Koeffizient von } (X)_n| \tag{3}$$

$$= |\{\text{Folgen } (a_i)_{1 \leq i \leq n} \mid a_i \in \mathbb{Z}, 0 \leq a_i \leq n-i, \text{ genau } k \text{ der } a_i \text{ verschwinden}\}| \tag{4}$$

$$= |\{\text{Folgen } (a_i)_{1 \leq i \leq n} \mid a_i \in \mathbb{Z}, 0 \leq a_i \leq i-1, \text{ genau } k \text{ der } a_i \text{ verschwinden}\}| \tag{5}$$

*Beweis.* Noch zu zeigen sind (4) und (5); (5) folgt durch Induktion nach  $n$  mittels 6.13. Im Blick auf einen kombinatorischen Beweis von (4) konstruieren wir eine Bijektion von  $S_n$  auf die Menge  $A$  der Folgen  $(a_i)_{1 \leq i \leq n}$  mit  $a_i \in \mathbb{Z}$  und  $0 \leq a_i \leq n-i$  für alle  $i \in \mathbb{N}_n$ . Hierbei heißt für  $\pi \in S_n$  das Bild  $I(\pi)$  unter dieser Bijektion die *Inversionstafel* von  $\pi$ .

Sei zunächst eine Folge  $(a_i)_{1 \leq i \leq n}$  aus  $A$  gegeben. Sei  $w_1$  das Wort mit dem einzigen Buchstaben  $n$ , und für  $1 \leq i \leq n-1$  sei  $w_{i+1}$  das Wort, das aus  $w_i$  entsteht durch Einfügen von  $n-i$  derart, daß links von  $n-i$  genau  $a_{n-i}$  Buchstaben stehen. Es ergibt sich ein Wort  $w_n := b_1 \cdots b_n$  der Länge  $n$ ; dieses Wort enthält alle Elemente von  $\mathbb{N}_n$  genau einmal als Buchstaben. Durch den Übergang zu derjenigen Permutation  $\pi = \pi((a_i))$  von  $\mathbb{N}_n$ , deren Wortdarstellung  $w_n$  ist, ist also insgesamt eine wohldefinierte Abbildung  $A \rightarrow S_n$  erklärt.

Beispiel:  $n = 7, (a_i) = 4, 0, 2, 3, 0, 1, 0$ . Es ist

$$\begin{aligned} w_1 &= 7 ; \\ w_2 &= 76 ; \\ w_3 &= 576 ; \\ w_4 &= 5764 ; \\ w_5 &= 57364 ; \\ w_6 &= 257364 ; \\ w_7 &= 2573164 . \end{aligned}$$

Nach Konstruktion gilt:

$$\begin{aligned} a_i &:= \text{Zahl der } j > i, \text{ die in } w_n \text{ links von } i \text{ stehen} \\ &= |\{j > i \mid \pi^{-1}(j) < \pi^{-1}(i)\}| \\ &= \text{Zahl der "Inversionen" (vgl. Def. 6.18) von } \pi^{-1}, \text{ die } i \text{ enthalten.} \end{aligned}$$

D.h.  $(a_i)$  ist vollständig bestimmt durch  $\pi$ . Wir haben insgesamt bewiesen:

**Proposition 6.17.** *Die Abbildungen  $A \rightleftharpoons S_n, (a_i) \mapsto \pi((a_i)), \pi \mapsto I(\pi)$  sind inverse Bijektionen, die die Zahl der Nullen in  $(a_i)$  in die Zahl der Links-Rechts-Maxima von  $\pi$  überführen.  $\square$*

Damit ist also die Identität (4) bewiesen, da man (2)  $\Rightarrow$  (4) bewiesen hat.

Die Rede von der "Inversionstafel" erklärt sich durch folgende

**Definition 6.18.** *Eine Inversion von  $\pi \in S_n$  ist ein Element  $(i, j)$  von  $\mathbb{N}_n \times \mathbb{N}_n$  mit  $i < j$  und  $\pi(i) > \pi(j)$ . Wir schreiben  $i(\pi)$  für die Zahl aller Inversionen von  $\pi$ .*

Beispielsweise ist  $i(\text{id}) = 0$ , und für die Permutation  $\pi$  mit der Wortdarstellung  $n, n - 1, \dots, 2, 1$  ist  $i(\pi) = \frac{n(n-1)}{2}$ ; dies ist offenbar der maximal mögliche Wert von  $i$ .

Nach 6.17 bestimmt die Inversionstafel von  $\pi$  dieses  $\pi$  eindeutig; es reicht sogar schon, die Zahl der  $j > i$ , für die  $\pi^{-1}(j) < \pi^{-1}(i)$  ist, zu kennen, um  $\pi$  eindeutig festzulegen.

---

Zum Abschluß des Kapitels sei noch an einige Sachverhalte zur Struktur der Gruppe  $S_n$  erinnert, die üblicherweise in der Anfängervorlesung erarbeitet werden:

- Eine *Transposition* in  $S_n$  ist eine Permutation, die genau zwei Elemente  $i, j \in \mathbb{N}_n$  miteinander vertauscht und alle sonstigen Elemente festläßt, also eine Permutation mit einzigem nichttrivialem Zykel  $(ij)$ .

- Die Gruppe  $S_n$  wird erzeugt von den Transpositionen; es gilt sogar

$$S_n = \langle \tau \in S_n \mid \tau = (i, i+1), 1 \leq i \leq n-1 \rangle .$$

- Ist  $\sigma \in S_n$  geschrieben als Produkt von Transpositionen:

$$\sigma = \prod_{1 \leq i \leq l} \tau_i , \tag{*}$$

so gilt (unabhängig von der Darstellung (\*))  $(-1)^l = (-1)^{i(\sigma)}$ ; diese Zahl heißt die *Signatur* von  $\sigma$ , geschrieben  $\text{sgn}(\sigma)$ .

- Für  $n \geq 2$  ist die Abbildung

$$\begin{aligned} S_n &\rightarrow \{1, -1\} \\ \sigma &\mapsto \text{sgn}(\sigma) \end{aligned}$$

ein surjektiver Gruppenhomomorphismus mit Kern  $A_n \subset S_n$ ; hierbei heißt  $A_n$  die *alternierende Gruppe auf  $n$  Elementen*.

- $A_n$  ist einfach, falls  $n \geq 5$  ist.

## 7 Der zwölfwache Weg

**Problem 7.1.** Verteile  $n$  Kugeln auf  $r$  Boxen. Auf wieviele verschiedene Weisen ist dies möglich bei Einhaltung gewisser Nebenbedingungen? Hierbei können die Bedeutung des Wortes “verschieden” sowie die Nebenbedingungen variieren.

Mathematisch formuliert besteht das Problem darin, anzugeben, wie viele verschiedene Abbildungen von  $\mathbb{N}_n$  nach  $\mathbb{N}_r$  es unter Beachtung der Nebenbedingungen gibt.

Schreibe kurz  $\mathbb{N}_n =: X, \mathbb{N}_r =: Y$ . Auf  $Y^X = \text{Abb}(X, Y)$ , der Menge der Abbildungen  $X \rightarrow Y$ , operieren die Gruppen  $\text{Sym}(Y) = S_r := G$  und  $\text{Sym}(X) = S_n := H$  durch Ummumerieren; genauer:

- $G$  operiert von links auf  $\text{Abb}(X, Y)$  durch  $(\sigma, f) \mapsto \sigma \circ f$ . Zwei Abbildungen  $f, g$  sind unter (der Operation von)  $G$  äquivalent (kurz:  $f \sim_G g$ ) genau dann, wenn es ein  $\sigma \in G$  gibt mit  $g = \sigma \circ f$ . Wir schreiben  $G \setminus \text{Abb}(X, Y)$  für die Menge der Äquivalenzklassen;  $|G \setminus \text{Abb}(X, Y)|$  ist die Zahl der Möglichkeiten, die Kugeln in ununterscheidbare Boxen abzulegen.

*Beispiel:* Seien  $X = \mathbb{N}_6, Y = \mathbb{N}_3$ , und seien

$$f = \begin{pmatrix} \{1, 3, 6\} & \{2, 4\} & \{5\} \\ 1 & 2 & 3 \end{pmatrix} ; \quad g = \begin{pmatrix} \{2, 4\} & \{5\} & \{1, 3, 6\} \\ 1 & 2 & 3 \end{pmatrix} .$$

Dann gilt  $f \sim_G g$  wegen  $(123)f = g$ .

- $H$  operiert von rechts auf  $\text{Abb}(X, Y)$  durch  $(f, \pi) \mapsto f \circ \pi$ . (*Bemerkung:*  $H$  operiert *nicht* von links, da nicht alle Elemente von  $S_n$  miteinander vertauschen). Zwei Abbildungen  $f, g$  sind unter  $H$  äquivalent (kurz:  $f \sim_H g$ ) genau dann, wenn es ein  $\pi \in H$  gibt mit  $g = f \circ \pi$ . Wir schreiben  $\text{Abb}(X, Y)/H$  für die Menge der Äquivalenzklassen;  $|\text{Abb}(X, Y)/H|$  ist die Zahl der Möglichkeiten,  $n$  ununterscheidbare Kugeln in  $r$  unterscheidbare Boxen abzulegen.

*Beispiel:* Seien wieder  $X = \mathbb{N}_6, Y = \mathbb{N}_3$ , sei  $f$  wie oben, und sei

$$g' = \begin{pmatrix} \{1, 4, 5\} & \{3, 6\} & \{2\} \\ 1 & 2 & 3 \end{pmatrix} .$$

Dann gilt  $f \sim_H g'$  wegen  $g' = f(23465)$ .

**Definition 7.2.** Seien  $G, H$  Gruppen, die auf einer Menge  $S$  operieren ( $G$  von links,  $H$  von rechts), wobei gilt

$$(\sigma f)\tau = \sigma(f\tau) \quad \forall \sigma \in G, \tau \in H, f \in S .$$

Dann definiert

$$f \sim G := \Leftrightarrow \exists \sigma \in G, \tau \in H \text{ mit } g = \sigma f \tau$$

eine Äquivalenzrelation auf  $S$ . Die Menge der Äquivalenzklassen ("Doppelnebenklassen") wird mit  $G \setminus S/H$  bezeichnet.

*Beispiele:*

- (i)  $S = \text{Abb}(X, Y), G = \text{Sym}(Y), H = \text{Sym}(X)$  ;
- (ii)  $S$  Gruppe,  $G, H$  Untergruppen.

*Bemerkung:* Es gilt  $G \setminus S/H = G \setminus (S/H) = (G \setminus S)/H$ .  $G$  operiert nämlich von links auf  $S/H$  durch  $\sigma(fH) := (\sigma f)H$  für  $f \in S, \sigma \in G$ .

Mit den Bezeichnungen von 7.1 und 7.2 ist also  $|G \setminus \text{Abb}(X, Y)/H|$  die Zahl der Möglichkeiten,  $n$  ununterscheidbare Kugeln in  $r$  ununterscheidbare Boxen abzulegen.

**Beispiel 7.3.** Seien  $n = 4$  und  $r = 2$ ; es sind also  $G = S_2$  und  $H = S_4$ .

- $|\text{Abb}(X, Y)| = 16$  ;
- $|S_2 \setminus \text{Abb}(X, Y)| = 8$  ;
- $|\text{Abb}(X, Y)/S_4| = 5$  (die in Frage kommenden Verteilungen sind  $(4, 0), (3, 1), (2, 2), (1, 3), (0, 4)$ ; als Übung empfiehlt sich, die einzelnen Bahnen zu beschreiben);
- $|S_2 \setminus \text{Abb}(X, Y)/S_4| = 3$  .

Für  $X, Y$  wie in 7.1 seien folgende Bezeichnungen erklärt:

$$\begin{aligned} \text{In}(X, Y) &:= \{f : X \rightarrow Y \mid f \text{ injektiv}\} ; \\ \text{Sur}(X, Y) &:= \{f : X \rightarrow Y \mid f \text{ surjektiv}\} ; \\ \text{Bi}(X, Y) &:= \{f : X \rightarrow Y \mid f \text{ bijektiv}\} . \end{aligned}$$

Für  $\sigma \in G, \tau \in H$  und  $f \in \begin{Bmatrix} \text{In}(X, Y) \\ \text{Sur}(X, Y) \\ \text{Bi}(X, Y) \end{Bmatrix}$  sind auch  $\sigma f$  und  $f\tau$  sowie  $\sigma f\tau$  in der entsprechenden Menge. Deshalb operieren  $G$  und  $H$  auch auf allen diesen Teilmengen von  $\text{Abb}(X, Y)$ .

**7.4. Der ‘‘zwölfache Weg.’’** Seien nun wieder  $|X| = n, |Y| = r$ . Wir haben gesehen, daß es sinnvoll ist, vier wesentlich verschiedene Bedeutungen des Wortes ‘‘verschieden’’ im Problem 7.1 zu unterscheiden (sowohl die Kugeln als auch die Boxen können unterscheidbar oder ununterscheidbar sein); ferner wollen wir drei verschiedene Nebenbedingungen betrachten, nämlich  $f \in \text{Abb}(X, Y)$  (keine Nebenbedingungen),  $f \in \text{In}(X, Y)$  und  $f \in \text{Sur}(X, Y)$ . Der Fall  $f \in \text{Bi}(X, Y)$  interessiert uns weniger, weil hier die Anzahl der Möglichkeiten schnell anzugeben ist: ist  $n \neq r$ , so gibt es kein solches  $f$ ; für  $n = r$  hat man, je nach getroffener Unterscheidbarkeitsannahme, eine Möglichkeit oder  $n!$  Möglichkeiten.

Somit ergibt sich die folgende Tafel mit zwölf Einträgen mit den Zahlen der jeweiligen Möglichkeiten; bei den einzelnen Einträgen ist entweder angegeben, an welcher Stelle der bisherigen Vorlesung wir sie begründet haben, oder die Begründung wird unten nachgeliefert.

Elemente von $X$	Elemente von $Y$	$f$ beliebig	$f$ injektiv	$f$ surjektiv
unterscheidbar	unterscheidbar	$r^n$ ① (4.3)	$(r)_n$ ② (4.4)	$\sum_{0 \leq j \leq r} (-1)^j \binom{r}{j} (r-j)^n$ ③ (5.6)
ununterscheidbar	unterscheidbar	$\binom{r+n-1}{n}$ ④ (4.7)	$\binom{r}{n}$ ⑤	$\binom{n-1}{n-r} = \binom{n-1}{r-1}$ ⑥ (4.7)
unterscheidbar	ununterscheidbar	$\sum_{0 \leq i \leq r} S(n, i)$ ⑦	$1, n \leq r$ $0, n > r$ ⑧	$S(n, r)$ ⑨
ununterscheidbar	ununterscheidbar	$p_r(n)$ ⑩	$1, n \leq r$ $0, n > r$ ⑪	$q_r(n)$ ⑫

Hierbei wird die Bedeutung der Ausdrücke  $S(n, r)$ ,  $p_r(n)$  und  $q_r(n)$  gleich noch erklärt werden.

**Definition 7.5.** Für  $r \leq n$  sei

$$S(n, r) := \frac{1}{r!} \sum_{0 \leq j \leq r} (-1)^j \binom{r}{j} (r-j)^n ;$$

dies ist eine natürliche Zahl. Für  $r > n$  sei außerdem  $S(n, r) := 0$  gesetzt. Die Zahlen  $S(n, r)$  heißen Stirling-Zahlen zweiter Art.

$S(n, r)$  ist die Zahl der Zerlegungen von  $\mathbb{N}_n$  in  $r$  nichtleere disjunkte nicht numerierte Teilmengen. Der Eintrag ③ in der Tafel 7.4 könnte auch als  $r!S(n, r)$  geschrieben werden.

**Definition 7.6.** Für  $r, n \in \mathbb{N}$  seien  $p_r(n)$  die Zahl der Partitionen von  $n$  mit höchstens  $r$  Termen und  $q_r(n)$  die Zahl der Partitionen von  $n$  mit genau  $r$  Termen.

Es sind noch einige Beweise zu den Einträgen der Tafel nachzuliefern; dies soll nun geschehen.

④ : Es kommt für die Beschreibung einer Verteilung nur an auf die Zahl  $m(i)$  der Kugeln, die in die Box mit der Nummer  $i$  fallen. Dann bilden die  $m(i)$  eine Multimenge auf  $Y$  der Kardinalität  $\sum_{1 \leq i \leq r} m(i) = n$ .

⑤ : Die gesuchte Zahl ist die Zahl der  $n$ -Teilmengen von  $\mathbb{N}_r$ .

⑥ : Sei  $f$  surjektiv gegeben; jede Box enthält also mindestens eine Kugel. Läßt man aus jeder Box eine Kugel weg, so entsteht eine Multimenge der Kardinalität  $n - r$  auf  $Y$ , die  $f$  bis auf Äquivalenz eindeutig bestimmt.

⑦ : Ein  $f$  wie gesucht ist dasselbe wie eine Zerlegung von  $X$  in  $r'$  nichtleere nichtnumerierte Teilmengen,  $r' \leq r$ . Nach ⑨ gibt es davon genau  $\sum_{1 \leq r' \leq r} S(n, r')$  viele.

Die übrigen Fälle sind klar.

## 8 Partitionen

**8.1.** Sei  $S$  eine endliche Menge mit  $|S| = n$ . Wir haben in 4.11 Zerlegungen von  $S$  in  $r$  disjunkte numerierte Teilmengen  $S_i \neq \emptyset, 1 \leq i \leq r$  betrachtet. Wir hatten gesehen, daß die Zahl solcher Zerlegungen eines Typs  $(k_1, \dots, k_r) \in \mathbb{N}^r$  gleich  $\binom{n}{k_1, \dots, k_r}$  ist.

Man kann die Numerierung der  $S_i$  "vergessen", d.h. solche Zerlegungen identifizieren, die sich nur in der Reihenfolge der beteiligten Teilmengen unterscheiden. Man ist dann in der Situation von Fall 9 des zwölffachen Wegs: es gibt  $S(n, r)$  solche Zerlegungen.

**Definition 8.2.** Eine Zerlegung einer endlichen Menge  $S$  in nichtnumerierte Teilmengen  $S_i \neq \emptyset (1 \leq i \leq k)$  heiße fortan eine Partition von  $S$ .

Ist  $S = \bigcup S_i$  eine derartige Partition, so heißt  $(k_1, \dots, k_r)$  mit  $k_i = |S_i|$  der Typ der Partition, und die  $S_i$  heißen die Blöcke der Partition. Weiter heißt für  $|S| = n$  die

Zahl  $B(n)$  aller Partitionen von  $S$  die  $n$ -te Bell-Zahl.  $B(n)$  ist zugleich die Zahl aller Äquivalenzrelationen auf  $S$ ; wir setzen  $B(0) := 1$ .

Da  $S(n, r)$  die Zahl aller  $r$ -Partitionen von  $\mathbb{N}_n$  ist, gilt

$$B(n) = \sum_{1 \leq r \leq n} S(n, r) \quad \text{für } n \in \mathbb{N} .$$

**Proposition 8.3.**

$$S(n, 1) = S(n, n) = 1 \quad \text{für } n \geq 1 ; \quad S(n, n-1) = \binom{n}{2} \quad \text{für } n \geq 2 . \quad (\text{i})$$

$$S(n, r) = S(n-1, r-1) + rS(n-1, r) \quad \text{für } 1 \leq r \leq n . \quad (\text{ii})$$

*Beweis.* Betrachte das Verhalten des Elements  $n \in \mathbb{N}$  in einer  $r$ -Partition von  $\mathbb{N}_n$ .

- Die Zahl der  $r$ -Partitionen, in denen  $n$  zu einem 1-Block  $\{n\}$  gehört, ist  $S(n-1, r-1)$ , denn  $\{n\}$  kann auf genau  $S(n-1, r-1)$  Weisen zu einer  $r$ -Partition fortgesetzt werden.
- Gehört  $n$  zu einem Block der Größe  $\geq 2$ , so liefert Weglassen von  $n$  eine  $r$ -Partition von  $\mathbb{N}_{n-1}$ . Die so entstehende Abbildung von der Menge der  $r$ -Partitionen von  $\mathbb{N}_n$ , bei denen  $n$  zu einem Block der Größe  $\geq 2$  gehört, in die Menge der  $r$ -Partitionen von  $\mathbb{N}_{n-1}$  hat Urbilder der Kardinalität  $r$ , denn  $r$  Blöcke kommen für  $n$  in Frage.

□

**8.4. Wertetabelle für  $S(n, r)$ :**

$S(n, r)$	$r = 1$	2	3	4	5	6	7	$B(n)$
$n = 1$	1	0	0	0	0	0	0	1
2	1	1	0	0	0	0	0	2
3	1	3	1	0	0	0	0	5
4	1	7	6	1	0	0	0	15
5	1	15	25	10	1	0	0	52
6	1	31	90	65	15	1	0	203
7	1	63	301	350	140	21	1	877

Insbesondere gilt  $S(n, 2) = 2^{n-1} - 1$ .

**Proposition 8.5.** Für  $n \geq 1$  gilt

$$B(n+1) = \sum_{0 \leq i \leq n} \binom{n}{i} B(i) .$$

*Erster Beweis.* Durch Induktion nach  $n$  unter Verwendung von  $B(n) = \sum_{1 \leq r \leq n} S(n, r)$  und 8.3 (ii).  $\square$

*Zweiter Beweis.* (kombinatorisch) Betrachte das Verhalten von  $n + 1$  in Partitionen von  $\mathbb{N}_{n+1}$ . Liegt  $n + 1$  in einem Block der Größe  $n - i + 1$  für ein  $i$  zwischen 0 und  $n$ , so gibt es  $\binom{n}{n-i} = \binom{n}{i}$  Möglichkeiten, die  $n - i$  übrigen Elemente des Blocks zu wählen. Weiter gibt es wegen  $n + 1 - (n - i + 1) = i$  genau  $B(i)$  Möglichkeiten, die verbleibenden Elemente zu partitionieren.  $\square$

**Proposition 8.6.** Für  $n \geq 1$  gilt

$$X^n = \sum_{0 \leq r \leq n} S(n, r)(X)_r .$$

*Beweis.* Wir zeigen, daß beide Seiten ausgewertet auf  $m \in \mathbb{N}$  übereinstimmen.

Die linke Seite gibt  $m^n$ ; es ist nun zweckmäßig, sich daran zu erinnern, daß  $m^n = |\text{Abb}(\mathbb{N}_n, \mathbb{N}_m)|$  ist. Jede Abbildung  $f : \mathbb{N}_n \rightarrow \mathbb{N}_m$  ist surjektiv auf ihr Bild  $B \subset \mathbb{N}_m$ ; hierbei hat  $B$  eine Kardinalität  $r$  zwischen 1 und  $m$ .  $f$  ist bestimmt durch

- die Wahl von  $B$  (dafür gibt es  $\binom{m}{r}$  Möglichkeiten) und
- die Wahl einer surjektiven Abbildung von  $\mathbb{N}_n$  nach  $B$  (dafür gibt es  $r! \cdot S(n, r)$  Möglichkeiten).

Also gibt es insgesamt  $\binom{m}{r} \cdot r! \cdot S(n, r) = \binom{m}{r} S(n, r)$  Abbildungen  $f$  mit  $|B| = r$ .  $\square$

In 6.15 hatten wir ein zu 8.6 recht ähnliches Ergebnis, nämlich

$$\sum_{1 \leq k \leq n} s(n, k) X^k = (X)_n .$$

Die beiden Mengen  $\{X, X^2, \dots, X^n\}$  und  $\{(X)_1, (X)_2, \dots, (X)_n\}$  sind Basen des  $\mathbb{Q}$ -Vektorraums der Polynome des Grades  $\leq n$  ohne Absolutglied; die beiden Gleichungen 8.6 und 6.15 beschreiben den Basiswechsel. Folglich sind die beiden  $n \times n$ -Matrizen

$$\underline{s} := (s(i, j))_{1 \leq i, j \leq n} \quad \text{und} \quad \underline{S} := (S(i, j))_{1 \leq i, j \leq n}$$

zueinander invers.

**Korollar 8.7.** Für alle  $k, i$  zwischen 1 und  $n$  gilt

$$\begin{aligned} \sum_{1 \leq j \leq i} S(i, j) s(j, k) &= \delta(i, k) ; \\ \sum_{1 \leq j \leq i} s(i, j) S(j, k) &= \delta(i, k) . \end{aligned}$$

$\square$

Dies geht alles auch *ohne* Gradbeschränkung (also für den entsprechenden unendlich-dimensionalen  $\mathbb{Q}$ -Vektorraum); bei der Multiplikation der zugehörigen Matrizen ist keine Konvergenzbetrachtung erforderlich, weil es sich um untere Dreiecksmatrizen handelt (vgl. z.B. die Tabellen). Korollar 8.7 gilt sogar für  $k, i \in \mathbb{N}$ .

**Korollar 8.8.** *Sind  $f, g$  Funktionen von  $\mathbb{N} \rightarrow \mathbb{C}$ , so sind äquivalent:*

$$\forall n : \quad g(n) = \sum_{1 \leq k \leq n} S(n, k) f(k) ; \quad (\text{i})$$

$$\forall n : \quad f(n) = \sum_{1 \leq k \leq n} s(n, k) g(k) . \quad (\text{ii})$$

*Beweis.* Fasse  $f, g$  als Spaltenvektoren auf. Die Aussage (i) ist dann  $g = \underline{S}f$ , die Aussage (ii) ist  $f = \underline{s}g$ ; die auftretenden Summen sind endlich.  $\square$

**Definition 8.9.** *Für  $n \in \mathbb{N}$  seien folgende Bezeichnungen eingeführt:*

- $\omega(n) \quad := \quad \text{Zahl der Ordnungsrelationen auf } \mathbb{N}_n ;$
- $\tau(n) \quad := \quad \text{Zahl der } t\text{-Relationen (d.h. der transitiven und reflexiven Relationen) auf } \mathbb{N}_n ;$
- $\omega^*(n) \quad := \quad \text{Zahl der Ordnungsrelationen auf } \mathbb{N}_n \text{ bis auf Isomorphie ;}$
- $\tau^*(n) \quad := \quad \text{Zahl der } t\text{-Relationen auf } \mathbb{N}_n \text{ bis auf Isomorphie .}$

**Proposition 8.10.** *Es gilt*

$$\tau(n) = \sum_{1 \leq k \leq n} S(n, k) \omega(k) \quad (\text{also auch } \omega(n) = \sum_{1 \leq k \leq n} s(n, k) \tau(k) ).$$

*Beweis.* (i) Sei  $R$  eine  $t$ -Relation auf  $\mathbb{N}_n$ . Definiere eine Relation  $R'$  durch

$$aR'b \Leftrightarrow aRb \wedge bRa .$$

Man überzeuge sich davon, daß  $R'$  eine Äquivalenzrelation ist.

(ii) Die Klassen von  $R'$  sind die  $[a] := \{b \in \mathbb{N}_n \mid aRb \wedge bRa\}$ . Für  $a_1, a_2, b_1, b_2$  mit  $a_1R'a_2$  und  $b_1R'b_2$  gilt

$$a_1Rb_1 \Leftrightarrow a_2Rb_2 .$$

(iii) Man erhält also  $t$ -Relationen  $R$  aus Äquivalenzrelationen  $R'$  durch Einfügen von Pfeilen zwischen den Äquivalenzklassen von  $R'$ . Die  $t$ -Relation  $R$  induziert eine Ordnungsrelation auf der Menge der Äquivalenzklassen von  $R'$ ; umgekehrt gibt jede Ordnungsrelation auf der Menge der Äquivalenzklassen von  $R'$  eine  $t$ -Relation.

(iv) Deshalb ist

$$\tau(n) = \sum_{1 \leq k \leq n} s_k ;$$

hierbei bezeichnet  $s_k$  die Zahl der  $t$ -Relationen, zu denen eine Äquivalenzrelation  $R'$  mit  $k$  Klassen gehört, und jedes  $s_k$  ist das Produkt der Zahl  $S(n, k)$  der Äquivalenzrelationen mit  $k$  Klassen und der Zahl  $\omega(k)$  der Ordnungsrelationen auf der  $k$ -elementigen Menge der Klassen.  $\square$

### 8.11. Wertetabelle:

$n$	1	2	3	4	5	6
$\omega(n)$	1	3	19	219	4231	130023
$\omega^*(n)$	1	2	5	16	318	2045
$\tau(n)$	1	4	29	355	6942	209527
$\tau^*(n)$	1	3	9	32		

*Bemerkung:*  $\tau(n)$  ist die Zahl aller Topologien auf  $\mathbb{N}_n$  (Übungsaufgabe).

**Satz 8.12.** *Es gelten:*

$$B(n) = e^{-1} \sum_{i \geq 0} \frac{i^n}{i!} \quad (n \geq 1) \quad (\text{i})$$

$$\sum_{n \geq 0} \frac{B(n) X^n}{n!} = e^{e^X - 1} \quad (\text{ii})$$

Bei (ii) ist an eine Identität formaler Potenzreihen gedacht; dazu ist zunächst zu klären, inwiefern der rechte Ausdruck überhaupt eine formale Potenzreihe ist. Man kann eine Potenzreihe in eine andere formal einsetzen, wenn sie kein Absolutglied hat. Es gilt also

$$e^{e^X - 1} = 1 + \frac{\left(\frac{X}{1!} + \frac{X^2}{2!} + \dots\right)^1}{1!} + \frac{\left(\frac{X}{1!} + \frac{X^2}{2!} + \dots\right)^2}{2!} + \dots$$

*Beweis.* Zu (i): Es ist

$$B(n) = \sum_{1 \leq k \leq n} S(n, k) = \sum_{0 \leq k \leq n} S(n, k) = \sum_{0 \leq k \leq \infty} S(n, k),$$

da  $S(n, 0) = 0$  für  $n \geq 1$  und  $S(n, k) = 0$  für  $k > n$ . Damit

$$B(n) = \sum_{0 \leq k \leq \infty} \frac{1}{k!} \sum_{0 \leq i \leq k} (-1)^i \binom{k}{i} (k-i)^n = \sum_{i \geq 0} \frac{i^n}{i!} \sum_{k \geq i} \frac{(-1)^{k-i}}{(k-i)!}$$

(wobei sich die letzte Gleichheit aus dem Umordnungssatz ergibt aufgrund der absoluten Konvergenz der betreffenden Doppelsomme)

$$= \sum_{i \geq 0} \frac{i^n}{i!} \sum_{j \geq 0} \frac{(-1)^j}{j!} = e^{-1} \sum_{i \geq 0} \frac{i^n}{i!}.$$

Zu (ii): Für  $x \in \mathbb{C}$  ist

$$\begin{aligned} \sum_{n \geq 0} \frac{B(n)x^n}{n!} &= \sum_{n \geq 0} \frac{1}{n!} e^{-1} \sum_{i \geq 0} \frac{i^n}{i!} \cdot x^n = e^{-1} \sum_{i \geq 0} \frac{1}{i!} \sum_{n \geq 0} \frac{(ix)^n}{n!} \\ &\quad \text{(auch diese Umordnung ist zulässig)} \\ &= e^{-1} \sum_{i \geq 0} \frac{e^{ix}}{i!} = e^{e^x - 1}. \end{aligned}$$

□

*Bemerkungen:*

- Beide Teilaussagen benötigen zum Beweis analytische Operationen, obgleich (ii) eine *formale* Identität ist ;
- beide Aussagen haben nur theoretischen Wert, sind also für praktische Rechnungen ungeeignet. Denn die Summendarstellung in (i) konvergiert so schlecht, daß ein Berechnen von  $B(n)$  mit der Rekursionsformel schneller möglich ist, und bei (ii) bringt die Taylor-Strategie nichts neues gegenüber der Rekursionsformel.

Im weiteren Verlauf des Kapitels wollen wir uns nun noch mit Partitionen von *Zahlen* beschäftigen. In 6.10 bzw. 7.6 wurden die Zahlen  $p(n)$ ,  $p_r(n)$  und  $q_r(n)$  definiert als Anzahlen bestimmter Arten von *Partitionen von  $n$* . Eine Partition von  $n$  in  $r$  Terme war eine Darstellung der Form

$$n = a_1 + a_2 + \dots + a_r \quad (*)$$

mit  $a_i \in \mathbb{N}$ , also ein  $r$ -String  $(a_1, a_2, \dots, a_r) \in \mathbb{N}^r$  mit  $\sum a_i = n$ , wobei wir zusätzlich noch verlangt haben, daß  $a_i \leq a_{i+1}$  für alle  $i = 1, 2, \dots, r-1$ . Der *Typ* der Partition (\*) ist  $(c_1, c_2, \dots, c_r)$ , wobei  $c_i$  die Zahl der Terme  $i$  in (\*) ist.

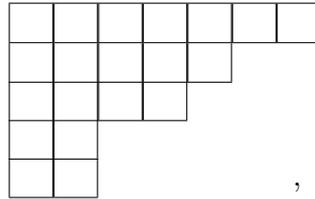
Es besteht folgender Zusammenhang zwischen Partitionen von Mengen und Partitionen von Zahlen: Sei  $X$  Menge mit  $|X| = n$ , und sei  $X = \dot{\bigcup}_{1 \leq k \leq r} X_k$  eine Partition von  $X$ . Dann ist bei geeigneter Numerierung der  $X_i$  der String  $(|X_1|, |X_2|, \dots, |X_r|)$  (also der *Typ* der betreffenden Partition von  $X$  im Sinne von Definition 8.2) eine Partition von  $n$ .

*Konvention:* Wir ändern den Begriff der Partition einer Zahl so ab, daß in (\*) gelten soll  $a_i \geq a_{i+1}$  für alle  $i = 1, 2, \dots, r-1$ . Dies ändert nichts an den bisherigen Überlegungen.

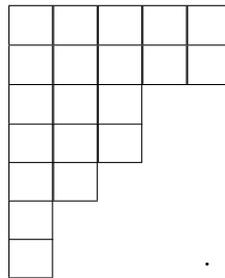
**Definition 8.13.** Das (Ferrers-)Diagramm einer Partition (\*) ist eine Figur mit  $a_1$  Kästchen in der 1. Zeile,  $a_2$  Kästchen in der 2. Zeile,  $\dots$   $a_r$  Kästchen in der  $r$ -ten Zeile.

Die konjugierte Partition  $\pi^*$  zu einer Partition  $\pi$  von  $n$  ist diejenige Partition von  $n$ , deren Diagramm durch Spiegelung des Diagramms von  $\pi$  an der Hauptachse hervorgeht.

Zum Beispiel entspricht der Partition (7,5,4,2,2) von 20 das Diagramm



und die konjugierte Partition von  $(7,5,4,2,2)$  ist  $(5,5,3,3,2,1,1)$  mit dem Diagramm



Durch Betrachtung des Diagramms einer Partition erhalten wir

**Korollar 8.14.** (i)  $p_k(n)$  ist gleich der Zahl der Partitionen von  $n$  mit größtem Term  $\leq k$  ;

(ii)  $q_k(n)$  ist gleich der Zahl der Partitionen von  $n$  mit größtem Term  $= k$  ;

(iii)  $p_k(n) = q_k(n + k)$  .

*Beweis.* Zu (iii): Schreibe eine Partition von  $n$  in höchstens  $k$  Termen in ein Diagramm mit  $k$  Zeilen (manche davon eventuell leer); füge in alle Zeilen des Diagramms (auch die leeren) ein Kästchen hinzu. Es ergibt sich das Diagramm einer Partition von  $n + k$  in genau  $k$  Termen. Streiche umgekehrt aus dem Diagramm einer Partition von  $n + k$  in genau  $k$  Termen in jeder Zeile ein Kästchen; es ergibt sich das Diagramm einer Partition von  $n$  in höchstens  $k$  Termen.

Alternativ kann man so argumentieren: (iii) folgt aus (ii) (lasse den höchsten Term  $k$  in der Partition von  $n + k$  weg).  $\square$

**Korollar 8.15.** Sei  $q(n)$  die Zahl der Partitionen von  $n$  mit Termen  $\geq 2$ . Für  $n \geq 2$  gilt

$$q(n) = p(n) - p(n - 1) .$$

$\square$

**Proposition 8.16.** Die Zahl der Partitionen von  $n$  in verschiedene ungerade Terme ist gleich der Zahl der selbstkonjugierten Partitionen von  $n$ .

*Beweis.* Wir konstruieren eine Bijektion

$$\begin{aligned} \{\pi \mid \pi = \pi^*\} &\rightarrow \{\rho = (\rho_1, \rho_2, \dots) \mid \rho_i \text{ alle verschieden und ungerade}\} \\ \pi &\mapsto \rho_\pi . \end{aligned}$$

Sei  $\pi = (\pi_1, \pi_2, \dots)$  gegeben mit  $\pi = \pi^*$ . Streiche die erste Zeile und die erste Spalte des Diagramms von  $\pi$  (man streicht also  $2\pi_1 - 1$  Kästchen) und setze  $\rho_1 := 2\pi_1 - 1$ ; entsprechend  $\rho_i := 2\pi_i - (2i - 1)$ . Aufgrund der Selbstkonjugiertheit von  $\pi$  kann man dieses Verfahren fortsetzen, bis alle Kästchen verbraucht sind. Dann ist  $\rho_\pi := (\rho_1, \rho_2, \dots)$  eine Partition von  $n$  mit ungeraden und verschiedenen Termen;  $\pi \mapsto \rho_\pi$  ist also eine wohldefinierte Abbildung.

Die Konstruktion ist umkehrbar: Ist  $\rho = (\rho_1, \rho_2, \dots)$  mit den obigen Nebenbedingungen gegeben, so ist es möglich, jedes  $\rho_i$  in der Form  $2\pi_i - (2i - 1)$  zu schreiben;  $\pi_\rho := (\pi_1, \pi_2, \dots)$  ist dann selbstkonjugiert, und die Abbildungen  $\pi \mapsto \rho_\pi$  und  $\rho \mapsto \pi_\rho$  sind invers.  $\square$

**8.17. Wertetabelle** für  $q_k(n)$  und  $p(n)$ .

$q_k(n)$	$k = 1$	2	3	4	5	6	7	8	9	10	$p(n)$
$n = 1$	1										1
2	1	1									2
3	1	1	1								3
4	1	2	1	1							5
5	1	2	2	1	1						7
6	1	3	3	2	1	1					11
7	1	3	4	3	2	1	1				15
8	1	4	5	5	3	2	1	1			22
9	1	4	7	6	5	3	2	1	1		30
10	1	5	8	9	7	5	3	2	1	1	42

Man überlegt sich leicht  $q_1(n) = q_{n-1}(n) = 1$  und  $q_2(n) = \lfloor \frac{n}{2} \rfloor$ .

**Satz 8.18.** Mit  $p(0) = p_r(0) := 1$  gelten

$$\sum_{n \geq 0} p(n) X^n = \prod_{k \in \mathbb{N}} (1 - X^k)^{-1} = \prod_{k \in \mathbb{N}} (1 + X^k + X^{2k} + \dots) ; \quad (\text{i})$$

$$\sum_{n \geq 0} p_r(n) X^n = \prod_{1 \leq k \leq r} (1 - X^k)^{-1} ; \quad (\text{ii})$$

$$\sum_{n \geq r} q_r(n) X^n = X^r \prod_{1 \leq k \leq r} (1 - X^k)^{-1} . \quad (\text{iii})$$

*Beweis.* Zu (i): Für  $n \geq 1$  gilt: Der  $n$ -Koeffizient der rechten Seite ist gleich dem  $n$ -Koeffizienten von  $\prod_{1 \leq k \leq n} (1 - X^k)^{-1}$ ; und zwar ist dieser Koeffizient die Zahl der Lösungen

$(m_1, m_2, \dots, m_n) \in \mathbb{N}_0^n$  von  $m_1 + 2 \cdot m_2 + \dots + n \cdot m_n = n$  (vom  $k$ -ten Faktor des Produkts wählt man den Term  $X^{m_k \cdot k}$  als Beitrag zu  $X^n$ ), also gleich der Zahl der Partitionen von  $n$  (eine Partition ist durch ihren Typ eindeutig charakterisiert).

*Bemerkung:* Multipliziert man die rechte Seite aus und faßt zusammen, so konvergiert die entsprechende Reihe bei Einsetzen von  $x \in \mathbb{C}, |x| < 1$  absolut; die Konvergenz ist gleichmäßig für  $|x| \leq \rho$ , falls  $0 < \rho < 1$ .

Zu (ii): Für  $n \geq 1$  gilt: Der  $n$ -Koeffizient der rechten Seite ist gleich der Zahl der Lösungen  $(m_1, m_2, \dots, m_r) \in \mathbb{N}_0^r$  von  $m_1 + 2 \cdot m_2 + \dots + r \cdot m_r = n$ , also gleich der Zahl der Partitionen von  $n$  mit Termen  $\leq r$ ; diese Zahl ist nach 8.14 (i) gleich  $p_r(n)$ .

Zu (iii):

$$\begin{aligned} \sum_{n \geq r} q_r(n) X^n &= \sum_{n \geq 1} q_r(n) X^n \stackrel{8.15}{=} \sum_{n \geq 1} p_r(n) X^n - \sum_{n \geq 1} p_{r-1}(n) X^n \\ &\quad (\text{man beachte } p_r(n) = 0 \text{ für } n \leq 0) \\ &= \sum_{n \geq 0} p_r(n) X^n - \sum_{n \geq 0} p_{r-1}(n) X^n \\ &\stackrel{(ii)}{=} \prod_{1 \leq k \leq r} (1 - X^k)^{-1} - \prod_{1 \leq k \leq r-1} (1 - X^k)^{-1} = X^r \prod_{1 \leq k \leq r} (1 - X^k)^{-1}, \end{aligned}$$

wobei man die letzte Gleichheit zur Übung nachrechnen sollte. □

**Korollar 8.19.** Für  $S \subset \mathbb{N}$  bezeichne  $p(n, S)$  die Zahl der Partitionen von  $n$  mit Gliedern in  $S$  und  $p_{\text{versch}}(n, S)$  die Zahl der Partitionen von  $n$  mit lauter verschiedenen Gliedern, alle aus  $S$ ; setze  $p(0, S) := 1$  für alle  $S$ . Es gelten:

$$\begin{aligned} \sum_{n \geq 0} p(n, S) X^n &= \prod_{k \in S} (1 - X^k)^{-1}; \\ \sum_{n \geq 0} p_{\text{versch}}(n, S) X^n &= \prod_{k \in S} (1 + X^k) \end{aligned} \tag{i}$$

*Beweis.* Zu (ii): Die Terme von  $1 + X^k$  sind gerade diejenigen Terme aus der Menge der Terme  $\{1, X^k, X^{2k}, \dots\}$  von  $(1 - X^k)^{-1}$ , die zu Lösungen  $(m_1, m_2, \dots, m_n) \in \mathbb{N}_0^n$  von  $m_1 + 2 \cdot m_2 + \dots + n \cdot m_n = n$  gehören mit  $m_i \in \{0, 1\}$  für  $1 \leq i \leq n$ . □

**Korollar 8.20.** Für  $U := \mathbb{N} - 2\mathbb{N}$  und  $n \in \mathbb{N}$  gilt:

$$p(n, U) = p_{\text{versch}}(n)$$

*Beweis.*

$$\begin{aligned}
\sum_{n \geq 0} p(n, U) X^n &\stackrel{8.19(i)}{=} \frac{1}{(1-X)} \cdot \frac{1}{(1-X^3)} \cdot \frac{1}{(1-X^5)} \cdots \\
&= \frac{(1-X^2)}{(1-X)(1-X^2)} \cdot \frac{(1-X^4)}{(1-X^3)(1-X^4)} \cdots \\
&\stackrel{\text{Umordnung}}{=} \frac{(1-X^2)(1-X^4) \cdots}{(1-X)(1-X^2)(1-X^3)(1-X^4) \cdots} \\
&= (1+X)(1+X^2)(1+X^3) \cdots \\
&= \prod_{k \geq 1} (1+X^k) \stackrel{8.19(ii)}{=} \sum_{n \geq 0} p_{\text{versch}}(n) X^n
\end{aligned}$$

□

**Definition 8.21.** Für  $n \in \mathbb{Z}$  sei

$$\nu(n) := \frac{n(3n-1)}{2} \in \mathbb{N}_0$$

die  $n$ -te Fünfeckzahl.

Man hat also

$n$	-4	-3	-2	-1	0	1	2	3	4
$\nu(n)$	26	15	7	2	0	1	5	12	22

Weiter sei

$$\begin{aligned}
P_n(X) &:= \prod_{1 \leq i \leq n} (1 - X^i) ; \\
S_n(X) &:= \sum_{-n \leq i \leq n} (-1)^i X^{\nu(i)} = 1 + \sum_{1 \leq i \leq n} (-1)^i (X^{\nu(i)} + X^{\nu(-i)}) ; \\
F_n(X) &:= \sum_{0 \leq i \leq n} (-1)^i \frac{P_n(X)}{P_i(X)} \cdot X^{in+g(i)} \quad \text{mit } g(i) := \frac{i(i+1)}{2} .
\end{aligned}$$

Da  $\nu(n) \in \mathbb{N}_0$  für alle  $n \in \mathbb{Z}$ , ist  $S_n(X)$  ein Polynom; dasselbe gilt auch für  $F_n(X)$ , denn man hat folgendes

**Lemma 8.22.** Für alle  $n \in \mathbb{N}$  ist  $F_n = S_n$ .

*Beweis.* Induktion nach  $n$ .

$n = 1$  :

$$\begin{aligned}
S_1 &= 1 - (X + X^2) ; \\
F_1 &= P_1 - X^{1+1} = 1 - X - X^2 .
\end{aligned}$$

$n > 1$ : Wir berechnen  $F_n - F_{n-1}$  und  $S_n - S_{n-1}$ . Wegen  $P_n = (1 - X^n)P_{n-1}$  ist

$$\begin{aligned}
F_n - F_{n-1} &= \sum_{0 \leq i \leq n} (-1)^i \frac{P_n}{P_i} \cdot X^{in+g(i)} - \sum_{0 \leq i \leq n-1} (-1)^i \frac{P_{n-1}}{P_i} \cdot X^{i(n-1)+g(i)} \\
&= (-1)^n X^{n^2+g(n)} + (1 - X^n) \sum_{0 \leq i \leq n-1} (-1)^i \frac{P_{n-1}}{P_i} \cdot X^{in+g(i)} \\
&\quad - \sum_{0 \leq i \leq n-1} (-1)^i \frac{P_{n-1}}{P_i} \cdot X^{i(n-1)+g(i)} \\
&= (-1)^n X^{n^2+g(n)} + \sum_{0 \leq i \leq n-1} (-1)^i \frac{P_{n-1}}{P_i} [X^{in+g(i)} - X^{(i+1)n+g(i)} - X^{i(n-1)+g(i)}] \\
&= (-1)^n X^{n^2+g(n)} + \sum_{1 \leq i \leq n-1} (-1)^i \frac{P_{n-1}}{P_i} [X^{i(n-1)+g(i)}(X^i - 1)] \\
&\quad - \sum_{1 \leq i \leq n} (-1)^{i-1} \frac{P_{n-1}}{P_{i-1}} X^{in+g(i-1)} =: (*).
\end{aligned}$$

Nun sind  $i(n-1) + g(i) = in + g(i-1)$  und

$$\frac{X^i - 1}{P_i} = \frac{-1}{P_{i-1}};$$

die meisten Terme der beiden Summen stimmen also überein und heben sich weg. Die übrigbleibenden Terme lassen sich wegen

$$\begin{aligned}
n^2 + g(n) &= n^2 + \frac{n(n+1)}{2} = \frac{n(3n+1)}{2} = \nu(-n), \\
n^2 + g(n-1) &= n^2 + \frac{n(n-1)}{2} = \frac{n(3n-1)}{2} = \nu(n)
\end{aligned}$$

so umrechnen:

$$\begin{aligned}
(*) &= (-1)^n X^{n^2+g(n)} + (-1)^n X^{n^2+g(n-1)} \\
&= (-1)^n [X^{\nu(-n)} + X^{\nu(n)}] \\
&= S_n - S_{n-1}.
\end{aligned}$$

□

**Satz 8.23** (Jacobi 1831). *Es gilt die Potenzreihenidentität*

$$\begin{aligned}
P(X) &:= \prod_{n \geq 1} (1 - X^n) = 1 + \sum_{n \geq 1} (-1)^n (X^{\nu(n)} + X^{\nu(-n)}) \\
&= \sum_{n \in \mathbb{Z}} (-1)^n X^{\nu(n)}.
\end{aligned}$$

*Beweis.* Sei  $x \in \mathbb{C}, |x| < 1$ . Wir zeigen, daß bei Einsetzen von  $x$  beide Seiten der behaupteten Identität absolut konvergieren und daß die Identität dann auch gültig ist.

(i) Es gilt  $\lim_{n \rightarrow \infty} P_n(x) = P(x)$  punktweise; für  $|x| \leq \rho < 1$  liegt sogar gleichmäßige Konvergenz vor.

(ii) Für festes  $x \in \mathbb{R}, 0 \leq x < 1$  ist  $|S_n(x) - P_n(x)| \leq nx^{n+1}$ , denn

$$S_n(x) \stackrel{8.22}{=} F_n(x) = \underbrace{P_n(x)}_{i=0} + \sum_{1 \leq i \leq n} (-1)^i \underbrace{\frac{P_n(x)}{P_i(x)}}_{\leq 1} \cdot \underbrace{x^{in+g(i)}}_{\leq x^{n+1}}.$$

(iii) Wegen  $nx^{n+1} \rightarrow 0$  gleichmäßig für  $x \in \mathbb{R}, 0 \leq x \leq \rho, \rho < 1$  gilt dort

$$\prod_{n \geq 1} (1 - x^n) = \lim_{n \rightarrow \infty} P_n(x) = \lim_{n \rightarrow \infty} S_n(x) = \sum_{n \in \mathbb{Z}} (-1)^n x^{\nu(n)}.$$

□

**Korollar 8.24.** Seien  $p^g(n)$  bzw.  $p^u(n)$  die Zahlen der Partitionen von  $n$  mit einer geraden bzw. einer ungeraden Zahl von lauter verschiedenen Termen. Es gilt:

$$p^g(n) = \begin{cases} p^u(n), & \text{falls } n \text{ keine Fünfeckzahl ist;} \\ p^u(n) + (-1)^k, & \text{falls } n = \frac{k(3k-1)}{2} \text{ für ein } k \in \mathbb{Z}. \end{cases}$$

*Beweis.* Einerseits gilt nach Satz 8.23

$$P(X) = \sum a_n X^n \quad \text{mit } a_n = \begin{cases} 0, & \text{falls } n \neq \frac{k(3k-1)}{2} \text{ für alle } k \in \mathbb{Z}; \\ (-1)^k & \text{sonst;} \end{cases}$$

andererseits ist

$$\begin{aligned} P(X) &= (1 - X)(1 - X^2)(1 - X^3) \cdots \\ &\stackrel{\text{Umordnung}}{=} 1 - (X + X^2 + X^3 + \cdots) + (X^{1+2} + X^{1+3} + \cdots) - \cdots + \cdots \text{ etc.} \\ &= \sum_{r \geq 0} (-1)^r \sum_{\substack{S \subset \mathbb{N} \\ |S|=r}} \prod_{i \in S} X^i \stackrel{\text{Umordnung}}{=} \sum_{n \geq 0} b_n X^n, \end{aligned}$$

wobei der Koeffizient  $b_n$  die Differenz der Zahl der Darstellungen  $n = k_1 + k_2 + \cdots + k_r$  mit einer geraden Anzahl  $r$  von verschiedenen Gliedern und der Zahl der Darstellungen  $n = k_1 + k_2 + \cdots + k_r$  mit einer ungeraden Anzahl  $r$  von verschiedenen Gliedern ist; es gilt also

$$P(X) = \sum_{n \geq 0} (p^g(n) - p^u(n)) X^n,$$

und die Behauptung ergibt sich aus einem Koeffizientenvergleich der beiden Summendarstellungen für  $P(X)$ . □

**Beispiel 8.25.**

- $n = 7$ . Es ist  $p(7) = 15$ , wobei genau die 5 Partitionen  $(7), (6, 1), (5, 2), (4, 3), (4, 2, 1)$  verschiedene Terme haben. Also ist  $p^g(7) = 3$  und  $p^u(7) = 2$ , in Übereinstimmung mit  $7 = \nu(-2)$  und 8.24.
- $n = 8$ . Es ist  $p(8) = 22$  und  $p^g(8) = p^u(8) = 3$ , was mit 8.24 übereinstimmt, da 8 keine Fünfeckzahl ist.

**Korollar 8.26.** Für  $p(n)$  gilt die Rekursionsformel

$$\begin{aligned} p(n) &= \sum_{k \geq 1} (-1)^{k+1} [p(n - \nu(k)) + p(n - \nu(-k))], \quad n \geq 1 \\ &= p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) \\ &\quad - p(n-22) - p(n-30) + \dots \end{aligned}$$

(Hierbei werden  $p(0) := 1$  und  $p(m) := 0$  für  $m < 0$  gesetzt; die Summe ist also endlich.)

*Beweis.* Nach 8.18 und 8.23 gilt

$$1 = \left( \sum_{l \geq 0} p(l) X^l \right) \left( 1 + \sum_{k \geq 1} (-1)^k [X^{\nu(k)} + X^{\nu(-k)}] \right);$$

die Behauptung ergibt sich aus einem Koeffizientenvergleich. □

**Bemerkung 8.27.** Es seien hier noch einige Ergebnisse zu  $p(n)$  genannt, die im Rahmen der Vorlesung nicht bewiesen werden können:

- Hardy und Ramanujan haben 1918 gezeigt, daß gilt

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

solche Ergebnisse hängen mit sogenannten Rogers-Ramanujan-Identitäten zusammen, von denen die oben benutzte Jacobi-Identität ein Spezialfall ist;

- man kann Kongruenzaussagen machen:

$$p(5k + 4) \equiv 0 \pmod{5}; \quad p(7k + 5) \equiv 0 \pmod{7}; \quad p(11k + 6) \equiv 0 \pmod{11};$$

solcherlei Aussagen sind allerdings nicht für die Primzahlen 2 und 3 möglich.

## 9 Mehr über Permutationen

*Erinnerung:* Ein  $\sigma \in S_n$  ist gegeben durch

- (a) eine Zykeldarstellung (im allgemeinen nicht eindeutig bestimmt);
- (a') die Standarddarstellung (eindeutig bestimmt);
- (b) die Wortdarstellung;
- (c) die Inversionstafel.

Zu  $\sigma \in S_n$  sind definiert

- $\text{typ}(\sigma)$ , der Zykeltyp oder die Konjugationsklasse von  $\sigma$ ; ein Teil der Information über den Typ ist in  $c(\sigma)$  enthalten;
- die Menge der Links-Rechts-Maxima;
- $I(\sigma)$ ;
- $D(\sigma)$ ;
- $\text{sgn}(\sigma)$ .

**Lemma 9.1.** Für  $\sigma \in S_n$  gilt:

$$\begin{aligned} \text{sgn}(\sigma) = +1 &\Leftrightarrow \text{Die Zahl der Zyklen gerader Ordnung von } \sigma \text{ ist gerade;} \\ \text{sgn}(\sigma) = -1 &\Leftrightarrow \text{Die Zahl der Zyklen gerader Ordnung von } \sigma \text{ ist ungerade.} \end{aligned}$$

*Beweis.* Es reicht zu zeigen

$$(a_1, \dots, a_r) = \underbrace{(a_1 a_2)(a_2 a_3) \cdots (a_{r-1} a_r)}_{r-1 \text{ Transpositionen}},$$

und das ist klar. □

**Proposition 9.2.** Für  $\sigma \in S_n$  bezeichne  $c_i(\sigma)$  die Zahl der Zyklen der Länge  $i$  von  $\sigma$ . Es gilt:

$$\exists \tau \in S_n \text{ mit } \tau^2 = \sigma \Leftrightarrow \text{Alle Zahlen } c_2(\sigma), c_4(\sigma), \dots \text{ sind gerade.}$$

*Beweis.* “ $\Rightarrow$ ”: Sei  $(a_1, \dots, a_t)$  ein Zykel von  $\tau$ . Unter  $\tau^2$  wird dieser Zykel zu

$$\begin{aligned} (a_1 a_3 a_5 \dots a_{t-1})(a_2 a_4 a_6 \dots a_t) &\text{ für } t \text{ gerade;} \\ (a_1 a_3 \dots a_t a_2 a_4 \dots a_{t-1}) &\text{ für } t \text{ ungerade.} \end{aligned}$$

D.h. Zykel ungerader Länge gehen in Zykel ungerader Länge über, und ein Zykel gerader Länge zerfällt in zwei Zykel der halben Länge. Zykel gerader Länge von  $\tau^2$  können also nur von einer Aufspaltung von Zykeln gerader Länge von  $\tau$  herkommen; sie treten demnach immer in Paaren auf, und ihre Zahl ist gerade.

“ $\Leftarrow$ ”: Sei  $\sigma = (a_1 a_2 \dots a_{r_1})(a_{r_1+1} \dots) \dots (\dots)$  mit  $c_2 \equiv c_4 \equiv \dots \equiv 0 \pmod{2}$  für  $c_i := c_i(\sigma)$ . Wir konstruieren ein  $\tau$  mit  $\tau^2 = \sigma$ . O.B.d.A. kann man annehmen: es gilt entweder

- (a)  $\sigma$  ist ein Produkt  $(a_1, \dots, a_r)(b_1, \dots, b_r)$  zweier Zykel gerader Länge  $r$  oder
- (b)  $\sigma = (a_1, \dots, a_r)$  mit ungeradem  $r = 2m + 1$ .

Im Fall (a) leistet  $\tau = (a_1, b_1, a_2, b_2, \dots, a_r, b_r)$  das gewünschte; diese “Quadratwurzel” ist allerdings nicht eindeutig.

Im Fall (b) ist  $\tau = (a_1, a_{m+2}, a_2, a_{m+3}, \dots, a_m, a_{2m+1}, a_{m+1})$  eine eindeutige Quadratwurzel.  $\square$

In diesem Zusammenhang ergeben sich einige Fragen kombinatorischer Art:

- (1) Wie viele “Quadratwurzeln”  $\tau$  von  $\sigma$  gibt es, falls die Bedingung (a) aus dem Beweis von 9.2 erfüllt ist?
- (2) Wieviele  $\sigma \in S_n$  gibt es, die eine Quadratwurzel  $\tau$  besitzen?
- (3) Wieviele Elemente  $\tau$  der Ordnung 2 (also Quadratwurzeln der Identität) gibt es?
- (4) Ersetze  $k = 2$  in (1), (2), (3) durch  $k \in \mathbb{N}$ .

Eine Antwort auf (3) wird in der folgenden Proposition gegeben:

**Proposition 9.3.** Sei  $r(n) := |\{\sigma \in S_n \mid \sigma^2 = 1\}|$ . Dann gelten  $r(1) = 1, r(2) = 2$  und

$$r(n+1) = r(n) + nr(n-1), \quad n \geq 2.$$

*Beweis.* Zunächst gilt:

$$\sigma^2 = 1 \Leftrightarrow \sigma \text{ enthält nur Zykel der Länge 1 und 2.} \quad (*)$$

Ferner läßt sich  $\{\sigma' \in S_{n+1} \mid \sigma'^2 = 1\}$  disjunkt zerlegen in

$$\{\sigma \in S_{n+1} \mid \sigma^2 = 1, \sigma(n+1) = n+1\} \dot{\cup} \{\sigma \in S_{n+1} \mid \sigma^2 = 1, \sigma(n+1) = i \in \mathbb{N}\}.$$

Mit (\*) zeigt man die Wohldefiniertheit der Abbildungen

$$\begin{aligned} \{\sigma \in S_{n+1} \mid \sigma^2 = 1, \sigma(n+1) = n+1\} &\xrightarrow{\cong} \{\sigma' \in S_n \mid \sigma'^2 = 1\} \\ \sigma &\mapsto \sigma|_{\mathbb{N}_n} \end{aligned}$$

und

$$\{\sigma \in S_{n+1} \mid \sigma^2 = 1, \sigma(n+1) = i \in \mathbb{N}_0\} \xrightarrow{\cong} \{(i, \sigma'') \mid i \in \mathbb{N}_n, \sigma'' \in \text{Sym}(\mathbb{N}_n - i), \sigma''^2 = 1\}$$

$$\sigma \mapsto (\sigma(n+1), \sigma|_{\mathbb{N}_n - \{\sigma(n+1)\}}),$$

und es gilt

$$|\{\sigma' \in S_n \mid \sigma'^2 = 1\}| = r(n);$$

$$|\{(i, \sigma'') \mid i \in \mathbb{N}_n, \sigma'' \in \text{Sym}(\mathbb{N}_n - i), \sigma''^2 = 1\}| = n \cdot r(n-1).$$

□

**Proposition 9.4.** *Seien  $i, j \in \mathbb{N}_n, i \neq j$  (d.h. insbesondere  $n \geq 2$ ). Die Wahrscheinlichkeit, daß  $j$  für eine zufällig gewählte Permutation  $\sigma \in S_n$  im gleichen Zykel wie  $i$  liegt, ist  $\frac{1}{2}$ .*

*Beweis.* O.B.d.A. sei  $\{i, j\} = \{n, n-1\}$ . Die Wortdarstellung von  $\sigma \in S_n$  sei

$$\sigma = a_1 a_2 \cdots a_n; \quad (*)$$

ferner sei  $\sigma = \hat{\tau}$ , wobei  $(\hat{\cdot}) : S_n \rightarrow S_n$  die Abbildung aus 6.9 ist, d.h.

$$\tau = (a_1 a_2 \dots)(\dots) \dots (\dots a_{n-1} a_n) \quad \text{in Standarddarstellung}$$

(( $\hat{\cdot}$ ) "läßt die Klammern weg"). Der letzte Zykel in der Standarddarstellung von  $\tau$  beginnt mit  $n$ , und die Elemente dieses Zyklus  $(n, \dots, a_n)$  sind genau die in (\*) rechts von  $n$  stehenden  $a_k$ . Also gilt:

$$n-1 \text{ und } n \text{ liegen im selben } \tau\text{-Zykel} \Leftrightarrow n-1 \text{ steht in } (*) \text{ rechts von } n,$$

und wir haben eine Bijektion

$$\{\sigma \mid n-1 \text{ steht links von } n \text{ in } (*)\} \leftrightarrow \{\sigma \mid n-1 \text{ steht rechts von } n \text{ in } (*)\}$$

$$a_n \cdots a_1 \leftrightarrow a_1 \cdots a_n.$$

Also ist die Kardinalität jeweils  $\frac{n!}{2}$ . □

**Proposition 9.5.** *Die Wahrscheinlichkeit, daß ein festes  $i \in \mathbb{N}_n$  in einem  $k$ -Zykel der zufällig gewählten Permutation  $\sigma \in S_n$  liegt, ist  $\frac{1}{n}$  (unabhängig von  $k$ ).*

*Beweis.* O.B.d.A. sei  $i = n$ . Wie im Beweis von 9.4 sei

$$\sigma = a_1 a_2 \cdots a_n = \hat{\tau}, \quad \tau = (a_1, a_2, \dots)(\dots) \dots (n, \dots, a_n).$$

Sei  $n = a_j$ . Der Zykel, der  $n$  enthält, hat dann Länge  $n-j+1 =: k$ ; es gilt also  $j := n-k+1$ . Aber die Zahl der  $\sigma$ , bei denen  $n$  an der Stelle  $n-k+1$  steht, ist offensichtlich  $(n-1)!$ . □

**Frage 9.6.** Was ist der Erwartungswert für die Zahl  $c(\sigma)$  einer zufällig gewählten Permutation  $\sigma \in S_n$ ?

A priori ist dieser Erwartungswert  $= \frac{1}{n!} \sum_{1 \leq k \leq n} c(n, k)k$ , denn  $c(n, k)$  war ja die Zahl der  $\sigma \in S_n$  mit  $c(\sigma) = k$ . Über diese Summe können wir uns mit einem Resultat zur erzeugenden Funktion für die  $c(n, k)$  bei festem  $n$  Information beschaffen:

$$\begin{aligned}
 X(X+1) \cdots (X+n-1) & \stackrel{6.15}{=} \sum_{1 \leq k \leq n} c(n, k) X^k & \left| \frac{d}{dX} \right. \\
 \prod_{i=0}^{n-1} (X+i) \sum_{i=0}^{n-1} \frac{1}{X+i} & = \sum_{1 \leq k \leq n} k \cdot c(n, k) X^{k-1} & \left| 1 \text{ einsetzen} \right. \\
 n! \underbrace{\left[ 1 + \frac{1}{2} + \cdots + \frac{1}{n} \right]}_{=: H_n = \text{Erwartungswert}} & = \sum_{1 \leq k \leq n} c(n, k) k
 \end{aligned}$$

□

Es wird daran erinnert, daß es eine Konstante  $\gamma$  (die sogenannte *Euler-Konstante*) gibt mit

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

und zwar ist  $\gamma = 0,577215 \dots$ . Beispielsweise ist für  $n = 100$  der Erwartungswert für  $c(\sigma)$  die Zahl  $H_{100} \approx \log 100 + \gamma \approx 4,605 + \gamma \approx 5,182$ .

**Definition 9.7.**

$$\begin{aligned}
 G_n & := \{ \sigma \in S_n \mid \sigma \text{ hat nur Zyklen gerader Länge} \} ; \\
 U_n & := \{ \sigma \in S_n \mid \sigma \text{ hat nur Zyklen ungerader Länge} \} .
 \end{aligned}$$

$G_n$  und  $U_n$  sind zunächst Teilmengen von  $S_n$ ;  $U_n$  kann ausnahmsweise sogar Untergruppe sein.

*Beispiele:*

- Für  $n = 3$  ist  $G_n = \emptyset$  und  $U_n = \{(123), (132), 1\}$ . Generell ist für ungerades  $n$  die Menge  $G_n$  leer, wie man sich sofort klarmacht.
- Für  $n = 4$  enthält  $S_n - (U_n \cup G_n)$  nur Elemente der Form  $(ab)(c)(d)$  und hat demnach Kardinalität  $\binom{4}{2} = 6$ .

**Proposition 9.8.** Für alle geraden Zahlen  $n = 2m$  gilt  $|G_{2m}| = |U_{2m}|$ .

*Beweis.* Wir konstruieren eine Bijektion  $\phi : U_{2m} \xrightarrow{\cong} G_{2m}$ . Sei also  $\pi \in U_{2m}$ ; die Standarddarstellung von  $\pi$  sei  $\pi = C_1 C_2 \dots C_k$  mit Zykeln  $C_i$ . Sei  $\phi(\pi)$  die Permutation  $C'_1 C'_2 \dots$  mit Zykeln

$$\begin{aligned} C'_{2i-1} &:= C_{2i-1} \text{ ohne sein letztes Element } a_i ; \\ C'_{2i} &:= C_{2i} \text{ mit } a_i \text{ angehängt .} \end{aligned}$$

(Enthält  $C_{2i-1}$  nur ein Element, so ist  $C'_{2i-1}$  leer und wird weggelassen, ohne daß sich an der Numerierung der  $C'_k$  etwas ändert.)

*Beispiel:* Zu  $\pi = (4)(513)(726)(8) \in U_8$  ist  $\phi(\pi) = (5134)(72)(86) \in G_8$ .

Es gilt:

- $\phi(\pi) \in G_{2m}$ , d.h.  $\phi : U_{2m} \rightarrow G_{2m}$  ist wohldefiniert;
- die Darstellung von  $\phi(\pi)$  durch die  $C'_i$  ist in Standardform.

Es bleibt also noch zu zeigen: zu  $\sigma \in G_{2m}$  gibt es genau ein  $\pi \in U_{2m}$  mit  $\phi(\pi) = \sigma$ . Sei  $\sigma = D_1 D_2 \dots D_h$  die Standarddarstellung eines  $\sigma$  mit geraden Zykeln  $D_i$ ; schreibe  $D_i = (a_i \dots b_i)$ . Verändere die  $D_i$ , beginnend von rechts, wie folgt ( $(\hat{\phantom{a}})$  bedeutet: "steht nicht da"):

$$\begin{aligned} b_h > a_{h-1} &: \text{ ersetze } D_h = (a_h \dots b_h) \text{ durch } (b_h)(a_h \dots \hat{b}_h) ; \\ &\text{ weiter mit } D_{h-2}, D_{h-1} ; \\ b_h < a_{h-1} &: \text{ ersetze } D_{h-1} D_h = (a_{h-1} \dots b_{h-1})(a_h \dots b_h) \text{ durch } (a_{h-1} \dots b_{h-1} b_h)(a_h \dots \hat{b}_h) ; \\ &\text{ weiter mit } D_{h-3}, D_{h-2} . \end{aligned}$$

In jedem Schritt verbleibt eine gerade Anzahl veränderter Zykeln ungerader Länge. Bleibt bei Abbruch des Verfahrens ein Zykel  $(a \dots b)$  übrig (notwendigerweise von gerader Länge), so ersetze ihn durch  $(b)(a \dots \hat{b})$ . Ist

$$\pi = D'_1 \dots D'_k \tag{*}$$

mit den so erhaltenen Zykeln  $D'_i$ , so gelten:

- $\pi \in U_{2m}$  ;
- (\*) ist in Standardform;
- $\phi(\pi) = \sigma$  ;
- $\pi$  ist durch  $\phi(\pi)$  vollständig bestimmt.

□

*Bemerkungen:*

- (i) die Zykelzahl von  $\phi(\pi)$  ist  $\leq$  der Zykelzahl von  $\pi$  ;
- (ii) ist  $X$  eine beliebige endliche Menge mit  $2m$  Elementen, so erhalten wir für jede Numerierung  $\nu : \mathbb{N}_{2m} \xrightarrow{\cong} X$  eine Bijektion  $\phi_\nu : U(X) \xrightarrow{\cong} G(X)$  mit

$$\begin{aligned} U(X) &:= \{ \sigma \in \text{Sym}(X) \mid \sigma \text{ hat nur Zykel ungerader Länge} \} \quad \text{und} \\ G(X) &:= \{ \sigma \in \text{Sym}(X) \mid \sigma \text{ hat nur Zykel gerader Länge} \} . \end{aligned}$$

Aber  $\phi_\nu$  hängt von  $\nu$  ab.

**Satz 9.9.** (i)  $|G_{2m}| = |U_{2m}| = 1^2 \cdot 3^2 \cdot 5^2 \cdot \dots \cdot (2m-1)^2 = \left( \frac{(2m)!}{2^m m!} \right)^2$  ;

(ii)  $|U_{2m+1}| = (2m+1)|U_{2m}|$  .

*Beweis.* Zu (i): Für  $\sigma \in G_{2m}$  setze

$$b_1 := 1 ;$$

$$b_2 := \text{irgendein Element aus } \mathbb{N}_{2m} - \{ \text{Elemente des Zyklus, der } b_1 \text{ enthält} \} ;$$

...

$$b_{k+1} := \text{irgendein Element aus } \mathbb{N}_{2m} - \{ \text{Elemente der Zykel, die } b_1, \dots, b_k \text{ enthalten} \} .$$

Wir beschreiben  $\sigma$  durch

$$\begin{array}{ccccccc} (\sigma(b_1), \sigma^2(b_1), \dots, b_1) & (\sigma(b_2), \sigma^2(b_2), \dots) & \dots & (\dots) & ; \\ \text{abgekürzt geschrieben} & & & & \\ a_1 & a_2 & \dots & & a_n \end{array}$$

Wie viele solche  $\sigma$  gibt es?

- für  $a_1 = \sigma(b_1)$  haben wir  $2m-1$  Möglichkeiten: alles außer  $b_1$  ;
- für  $a_2 = \sigma^2(b_1)$  haben wir  $2m-1$  Möglichkeiten: alles außer  $\sigma(b_1)$  .

Hier sind nun allerdings zwei Fälle zu unterscheiden:

Fall  $\sigma^2(b_1) = b_1$ :  $\sigma = (\sigma(1), 1)(a_3, \dots) \dots (\dots)$ .

- für  $a_3$  gibt es  $2m-3$  Möglichkeiten: alles außer  $\sigma(1), 1, b_2$  ;
- für  $a_4$  gibt es  $2m-3$  Möglichkeiten: alles außer  $\sigma(1), 1, a_3 = \sigma(b_2)$  .

Fall  $\sigma^2(b_1) \neq b_1$ :  $\sigma = (\sigma(1), \sigma^2(1), \sigma^3(1), \dots) \dots (\dots)$ .

- für  $a_3 = \sigma^3(1)$  gibt es  $2m-3$  Möglichkeiten: alles außer  $a_1, a_2, b_1$  ;

- für  $a_4 = \sigma^4(1)$  gibt es  $2m - 3$  Möglichkeiten: alles außer  $a_1, a_2, a_3$ .

Entsprechend fährt man fort und findet jeweils

- für  $a_{2i-1}$  gibt es  $2m - 2i + 1$  Möglichkeiten: alles außer  $a_1, \dots, a_{2i-2}$  und dem zugehörigen  $b_k$ ;
- für  $a_{2i}$  gibt es  $2m - 2i + 1$  Möglichkeiten: alles außer  $a_1, \dots, a_{2i-1}$ .

Läuft  $i$  zwischen 1 und  $m$ , so erhält man als Gesamtzahl der Möglichkeiten für ein  $\sigma \in G_{2m}$

$$\prod_{1 \leq i \leq m} (2m - 2i + 1)^2 = \prod_{\substack{1 \leq j \leq 2m \\ j \text{ ungerade}}} j^2.$$

Zu (ii): Zunächst erklären wir den Begriff der *Lücke* oder *Lückenposition*. Ist  $\pi = (a_1 \dots a_r)(a_{r+1} \dots) \dots (\dots a_n)$  in Standarddarstellung, so ist eine solche Lücke von  $\pi \in S_n$  die Position links von  $a_i$  im gleichen Zykel oder eine Position rechts von  $\pi$ . Es gibt also genau  $n + 1$  solche Lückenpositionen.

*Beispiel:* Sei  $n = 5$  und  $\pi = (321)(54) \in S_5$ . Die Lückenpositionen sind

$$\begin{array}{ccccccc} & & 3 & 2 & 1 & & 5 & 4 \\ & \uparrow & & \uparrow & \uparrow & & \uparrow & \uparrow & \uparrow \end{array}$$

Wir können nun mit Hilfe dieses Begriffs eine Bijektion  $\psi : U_{2m} \times \mathbb{N}_{2m+1} \xrightarrow{\cong} U_{2m+1}$  konstruieren. Sei  $\phi(\pi) \in G_{2m}$  wie in 9.8; füge  $2m + 1$  in die  $k$ -te Lücke ein; wir erhalten  $\tilde{\pi} \in S_{2m+1}$  mit genau einem ungeraden Zykel  $C$ . Die Menge der in  $C$  enthaltenen Elemente von  $\mathbb{N}_{2m+1}$  bezeichnen wir mit  $\underline{C}$ ; es ist dann  $\mathbb{N}_{2m+1} - \underline{C}$  eine Menge mit einer geraden Anzahl von Elementen mit einer bestimmten Numerierung.

Wir wenden jetzt  $\phi^{-1}$  an auf die Permutation  $\tilde{\pi}|_{\mathbb{N}_{2m+1} - \underline{C}}$  und erhalten ein  $\tilde{\tilde{\pi}} \in U(\mathbb{N}_{2m+1} - \underline{C})$ . Wir setzen

$$\psi(\pi, k) = \begin{cases} \tilde{\tilde{\pi}} & \text{auf } \mathbb{N}_{2m+1} - \underline{C}; \\ C & \text{auf } \underline{C}. \end{cases}$$

Die so definierte Abbildung  $\psi$  geht nach  $U_{2m+1}$ , ist also wohldefiniert. Um die Umkehrabbildung zu finden, entwickeln wir einen Algorithmus zur Bestimmung von  $(\pi, k)$  mit  $\psi(\pi, k) = \sigma \in U_{2m+1}$ :

- streiche denjenigen Zykel  $C$  von  $\sigma$ , der  $2m + 1$  enthält;
- wende  $\phi$  an auf die verbleibende Permutation von  $\mathbb{N}_{2m+1} - \underline{C}$  (einer Menge mit gerader Kardinalität); die entstehende Permutation hat lauter gerade Zykellängen;

- füge  $C$  wieder hinzu;
- $k$  ist die Position von  $2m + 1$  in der Standarddarstellung der entstehenden Permutation; es gilt  $k \in \mathbb{N}_{2m+1}$ ;
- streiche  $2m + 1$ , das erste Element des letzten Zyklus; es verbleibt ein Element von  $S_{2m}$ , das sogar zu  $G_{2m}$  gehört;
- wende  $\phi^{-1}$  auf dieses Element von  $G_{2m}$  an; man erhält ein Element  $\pi \in U_{2m}$ .

Man überlegt sich, daß man so tatsächlich eine Umkehrabbildung von  $\psi$  erhält.  $\square$

**Beispiel 9.10.** Für  $n = 5$  ist  $|U_5| = 45$ , wie man aus  $|U_5| = 5 \cdot |U_4|$  ableitet, in Übereinstimmung mit der Gestalt der Elemente von  $U_5$ : ein solches Element ist entweder die Identität oder hat eine der Formen  $(abcde)$  oder  $(abc)(d)(e)$ ; davon gibt es  $1+4!+\binom{5}{3} \cdot 2 = 45$  Stück.

**Korollar 9.11.** *Die Wahrscheinlichkeiten für die folgenden Ereignisse sind gleich:*

- (i) *eine zufällige Permutation  $\sigma \in S_n$  hat eine gerade Anzahl von Zykeln, die alle ungerade Länge haben;*
- (i') *Eine zufällige Permutation  $\sigma \in S_n$  hat lauter gerade Zykellängen;*
- (ii) *Eine Münze werde  $n$  mal geworfen und liefert genau  $\frac{n}{2}$  mal "Zahl".*

Bevor wir dieses Korollar beweisen, ist ein Exkurs in die elementare Wahrscheinlichkeitstheorie angebracht:

**Exkurs 9.12.** Ein Versuch liefere zwei mögliche Ergebnisse, "Treffer" (1) und "kein Treffer" (0), mit Wahrscheinlichkeiten  $p$  bzw.  $1 - p$ ,  $0 \leq p \leq 1$ . Führt man den Versuch  $n$  mal aus, so ist die Wahrscheinlichkeit für den Ergebnisvektor  $(e_1, \dots, e_n)$  ( $e_i \in \{0, 1\}$ ) das Produkt  $p^k \cdot (1 - p)^{n-k}$ , wobei  $k$  die Zahl der Einsen unter den  $e_i$  ist.

Die Wahrscheinlichkeit, nach  $n$  Versuchen genau  $k$  Treffer zu haben, ist

$$|\{\text{Vektoren } (e_i)_{1 \leq i \leq n} \text{ mit genau } k \text{ Einsen}\}| \cdot p^k (1-p)^{n-k} = \binom{n}{k} \cdot p^k (1-p)^{n-k} := \text{Bin}(n, k, p);$$

diese Wahrscheinlichkeitsverteilung heißt *Binomialverteilung*, das Verfahren *Bernoulli-Prozeß*.

Beispiele:

- Urnenexperimente “mit Zurücklegen”:  $p = \frac{\text{Zahl der markierten Kugeln}}{\text{Zahl aller Kugeln}}$  ;
- Würfeln:  $p = \frac{1}{6}$  .

(Ende des Exkurses)

*Beweis von 9.11.* Alle Wahrscheinlichkeiten sind 0 für ungerades  $n$ ; für  $n = 2m$  ergibt sich

$$\begin{aligned} p(ii) &= \binom{n}{\frac{n}{2}} \left(\frac{1}{2}\right)^n, \\ p(i) = p(i') &= \frac{1^2 \cdot 3^2 \cdot 5^2 \cdot \dots \cdot (2m-1)^2}{(2m)!} \\ &= \frac{\left(\frac{(2m)!}{m!2^m}\right)^2}{(2m)!} = \frac{(2m)!}{m!m!} \cdot \frac{1}{2^{2m}} = \binom{n}{\frac{n}{2}} \left(\frac{1}{2}\right)^n. \end{aligned}$$

□

Unter Verwendung der Stirling-Formel  $n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$  erhält man die Abschätzung

$$\binom{2m}{m} 2^{-2m} \approx \frac{1}{\sqrt{\pi m}}$$

(die Rechnungen seien zur Übung empfohlen). Diese Abschätzung ist recht brauchbar:

$m$	exakter Wert	Näherungswert
2	$\frac{9}{2^4} = 0,375$	0,399...
3	$\frac{5}{16} = 0,3125$	0,325...

Wir “wissen”:

- wieviele  $\sigma \in S_n$  mit  $c(\sigma) = k$  gibt es? Antwort:  $c(n, k)$  Stück;
- wieviele  $\sigma \in S_n$  haben nur gerade bzw. nur ungerade Zykel? Antwort: vgl. 9.9;
- wieviele  $\sigma \in S_n$  haben mindestens bzw. genau eine vorgegebene Anzahl  $r$  von Fixpunkten? Die Antwort ist implizit in 5.4 enthalten: Mit

$$D_n := n! \cdot \sum_{0 \leq j \leq n} (-1)^j \frac{1}{j!}$$

gilt

$$|\{\sigma \in S_n \mid \sigma \text{ hat genau } r \text{ Fixpunkte}\}| = \binom{n}{r} \cdot D_{n-r} ;$$

- der Erwartungswert für die Zahl der Fixpunkte von  $\sigma \in S_n$  ist 1; dies haben wir in 5.5 und 6.6 auf zwei verschiedene Weisen bewiesen.

Es ergeben sich zwei “natürliche” Fragen:

- wieviele  $\sigma \in S_n$  haben genau eine vorgegebene Anzahl  $r$  von  $k$ -Zykeln?
- welches ist der Erwartungswert für die Zahl der  $k$ -Zykel?

Für den Rest des Kapitels, den wir der Beantwortung dieser Fragen widmen, fixieren wir  $n \in \mathbb{N}$  und  $k \in \mathbb{N}_0$ .

**Definition 9.13.** Ein  $k$ -Zykel aus oder von  $\mathbb{N}_n$  ist eine  $k$ -Teilmenge von  $\mathbb{N}_n$ , versehen mit einer Anordnung bis auf zyklische Vertauschung; es gibt  $\binom{n}{k} \cdot (k-1)! = \frac{n!}{(n-k)!k}$  solche  $k$ -Zykel von  $\mathbb{N}_n$ .

Sei  $\Gamma$  die Menge der  $k$ -Zykel aus  $\mathbb{N}_n$ ; für eine Teilmenge  $\Delta \subset \Gamma$  sei

$$A(\Delta) := \{\sigma \in S_n \mid \sigma \text{ enthält die Elemente von } \Delta\}$$

(Wir setzen  $A(\Delta) := \emptyset$ , falls  $\Delta$  nicht disjunkt ist, d.h. falls die Elemente von  $\Delta$  nicht paarweise disjunkt sind). Ferner seien

$$\begin{aligned} \alpha_r &:= \sum_{\substack{\Delta \subset \Gamma \text{ disjunkt} \\ |\Delta|=r}} |A(\Delta)| ; \\ B_r &:= \{\sigma \in S_n \mid \sigma \text{ enthält genau } r \text{ verschiedene } k\text{-Zykel}\} ; \\ \beta_r &:= |B_r| . \end{aligned}$$

Wir bestimmen zunächst die  $\alpha_r$ .

Für die Wahl des ersten  $k$ -Zykels in  $\Delta \subset \Gamma$ ,  $|\Delta| = r$ ,  $\Delta$  disjunkt gibt es  $\binom{n}{k} \cdot (k-1)! = \frac{n!}{(n-k)!k}$  Möglichkeiten. Für die Wahl des zweiten  $k$ -Zykels in  $\Delta$  gibt es entsprechend  $\frac{(n-k)!}{(n-2k)!k}$  Möglichkeiten; so verfährt man weiter und erhält  $\frac{(n-(r-1)k)!}{(n-rk)!k}$  Möglichkeiten für die Wahl des  $r$ -ten  $k$ -Zykels, solange  $rk \leq n$ .

Es gibt also insgesamt

$$\frac{n!}{(n-k)!k} \cdot \frac{(n-k)!}{(n-2k)!k} \cdots \frac{(n-(r-1)k)!}{(n-rk)!k} = \frac{n!}{(n-rk)!k^r}$$

Möglichkeiten, eine *geordnete* Menge von  $r$  disjunkten  $k$ -Zykeln zu wählen. Für die Wahl von  $\Delta$ , für die die Reihenfolge der  $k$ -Zykel keine Rolle spielt, gibt es demnach  $\frac{n!}{(n-rk)!k^r r!}$  Möglichkeiten. Weiter ist  $|A(\Delta)| = (n-rk)!$ . Wir erhalten also

9.14.

$$\begin{aligned}\alpha_r &= |A(\Delta)| \times \text{Zahl der disjunkten } \Delta \text{ mit } |\Delta| = r \\ &= \frac{n!(n-rk)!}{(n-rk)!k^r r!} = \frac{n!}{k^r k!}.\end{aligned}$$

**Proposition 9.15.** *Der Zusammenhang zwischen  $\alpha_r$  und  $\beta_r$  ist*

$$\alpha_r = \sum_{t \geq 0} \binom{t}{r} \beta_t.$$

*Beweis.* Sei  $\sigma \in B_t$ , d.h.  $\exists \Lambda \in \Gamma, |\Lambda| = t, \Lambda$  disjunkt, so daß  $\sigma$  genau die  $k$ -Zykel aus  $\Lambda$  enthält. Sei  $0 \leq r \leq t$ . Dann enthält  $\Lambda$  genau  $\binom{t}{r}$   $r$ -Teilmengen  $\Delta$ , d.h.  $\sigma$  tritt in genau  $\binom{t}{r}$  der Mengen  $A(\Delta)$  auf und trägt  $\binom{t}{r}$  zu  $\alpha_r$  bei.  $\square$

**Korollar 9.16.** *Seien  $f(X) := \sum_{r \geq 0} \alpha_r X^r$  und  $g(X) := \sum_{t \geq 0} \beta_t X^t$ . Dann ist  $f(X) = g(X+1)$  und  $g(X) = f(X-1)$ .*

*Beweis.* 9.15 und Koeffizientenvergleich (unter Verwendung des Binomialsatzes).  $\square$

**Korollar 9.17.** *Für  $1 \leq k \leq n$  ist der Erwartungswert  $E$  für die Zahl der  $k$ -Zykeln einer zufällig gewählten Permutation  $\sigma \in S_n$  gleich  $\frac{1}{k}$ .*

*Beweis.*

$$E = \frac{1}{n!} \sum_{t \geq 0} t \cdot \beta_t \stackrel{9.15}{=} \frac{1}{n!} \alpha_1 \stackrel{9.14}{=} \frac{n!}{n! \cdot k \cdot 1} = \frac{1}{k}.$$

$\square$

**Korollar 9.18.**

$$\beta_t := |\{\sigma \in S_n \mid \sigma \text{ enthält genau } t \text{ verschiedene } k\text{-Zykel}\}| = n! \sum_{0 \leq r \leq \frac{n}{k}} \binom{r}{t} (-1)^{r-t} \frac{1}{r! k^r}.$$

*Beweis.* 9.16 und Koeffizientenvergleich.  $\square$

**Korollar 9.19.** *Die Zahl  $\frac{\beta_t}{n!}$ , also die Wahrscheinlichkeit, daß eine zufällige  $n$ -Permutation genau  $t$  verschiedene  $k$ -Zykeln enthält, konvergiert bei festem  $t$  und  $k$  für  $n \rightarrow \infty$  gegen  $\frac{1}{k^t t!} e^{-\frac{1}{k}}$ .*

*Beweis.*

$$\begin{aligned}\frac{\beta_t}{n!} &\stackrel{9.18}{=} \sum_{t \leq r \leq \frac{n}{k}} (-1)^{r-t} \frac{1}{(r-t)! t! k^r} = \frac{1}{t! k^t} \sum_{t \leq r \leq \frac{n}{k}} (-1)^{r-t} \frac{1}{(r-t)! k^{r-t}} \\ &\stackrel{r-t=s}{=} \frac{1}{t! k^t} \sum_{0 \leq s \leq \frac{n}{k}-t} (-1)^s \frac{1}{(s)! k^s} \xrightarrow{n \rightarrow \infty} \frac{1}{t! k^t} e^{-\frac{1}{k}}.\end{aligned}$$

$\square$

**Exkurs 9.20.** Die *Poisson-Verteilung*  $\text{Poi}(\lambda, t)$  mit Parameter  $\lambda \geq 0$  ist die Wahrscheinlichkeitsverteilung auf  $\mathbb{N}_0$  mit

$$\text{Poi}(\lambda, t) = \frac{\lambda^t}{t!} \cdot e^{-\lambda}.$$

Der Erwartungswert von  $\text{Poi}(\lambda, \cdot)$  ist  $\lambda$ .

Es gilt also:  $\frac{\lambda^t}{t!}$  konvergiert für  $n \rightarrow \infty$  gegen  $\text{Poi}(\frac{\lambda}{n}, t)$ .

$\text{Poi}(\cdot, \cdot)$  beschreibt die Häufigkeiten von Summen von Einzelereignissen, die alle mit der gleichen kleinen Wahrscheinlichkeit eintreten; Beispiele:

- Unter fabrikneuen Glühbirnen sind erfahrungsgemäß 0,1% defekt. Die Wahrscheinlichkeit, in einer Stichprobe von 50 Glühbirnen genau  $r$  defekte zu haben, ist  $\approx \text{Poi}(\lambda, r)$  mit  $\lambda = 50 \cdot p = 0,05$ .
- Radioaktiver Zerfall (Zahl der Ausschläge des Geigerzählers pro Zeiteinheit).
- Zahl der Anrufe pro Zeiteinheit in einer Telefonzentrale.

## 10 Graphen und Untergraphen

Die grundlegenden Begriffe der Graphentheorie sind bereits in Definition 1.9 zusammengestellt. Einige weitere Begriffe dieser Theorie bringt die folgende

**Definition 10.1.** Sei  $G = (V, E)$  ein Graph.

- Für  $v \in V$  heißt  $d(v) := |\{e \in E \mid e \text{ trifft } v\}|$  der Grad von  $v$ ;
- $v$  heißt isoliert genau dann, wenn  $d(v) = 0$ , und Endpunkt genau dann, wenn  $d(v) \leq 1$ ;
- eine orientierte Kante ist eine Kante versehen mit einer Orientierung, d.h. einer Anordnung der beiden Knoten  $v, w$  von  $e$ . Wir schreiben  $(v, w)$  bzw.  $(w, v)$  für die beiden Orientierungen auf  $e = \{v, w\}$  und symbolisieren  $(v, w)$  durch einen Pfeil von  $v$  nach  $w$ . Ist  $e$  eine orientierte Kante, so sei  $\bar{e}$  dieselbe Kante mit inverser Orientierung. Eine Orientierung auf  $G$  ist die Wahl einer Orientierung für alle  $e \in E$ .
- Ein Weg der Länge  $r \in \mathbb{N}$  auf  $G$  ist eine Folge  $\gamma = (e_1, \dots, e_r)$  von orientierten Kanten  $e_i = (v_{i-1}, v_i)$ . Dabei heißen  $v_0$  bzw.  $v_r$  der Anfangs- bzw. Endpunkt von  $\gamma$  (geschrieben  $A(\gamma)$  bzw.  $E(\gamma)$ ). Ein Weg der Länge 0 ist ein Knoten  $v$ , er hat Anfangs- und Endpunkt  $v$ . Für einen Weg  $\gamma$  sei  $l(\gamma) \in \mathbb{N}_0$  die Länge von  $\gamma$ .

- Ein Weg  $\gamma$  heißt reduziert genau dann, wenn für alle  $i = 1, \dots, r - 1$  gilt  $e_i \neq \overline{e_{i+1}}$  ("keine Rückwege") und geschlossen genau dann, wenn Anfangs- und Endpunkt übereinstimmen.

Zu jedem Weg erhalten wir durch Streichen der Paare  $e_i, e_{i+1}$  mit  $e_i = \overline{e_{i+1}}$  einen wohlbestimmten reduzierten Weg (eventuell der Länge 0). Zwei Wege  $\gamma, \delta$  der Längen  $r, s$  können zu einem Weg  $\gamma * \delta$  (oder einfach  $\gamma\delta$ ) der Länge  $r + s$  komponiert werden, falls  $E(\gamma) = A(\delta)$  ist.

- $G$  heißt zusammenhängend, wenn zu je zwei  $v, w \in V$  ein Weg  $\gamma$  existiert mit  $v = A(\gamma), w = E(\gamma)$ .

- Durch

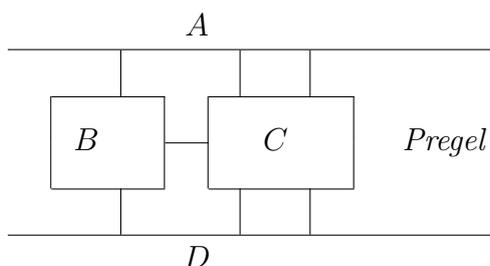
$$v \sim w :\Leftrightarrow \exists \gamma \text{ mit } A(\gamma) = v, E(\gamma) = w$$

wird eine Äquivalenzrelation auf  $V$  definiert. Für die Äquivalenzklassen  $V_i (i \in I)$  gilt  $E = \dot{\bigcup} E_i$  mit  $E_i = E \cap \mathfrak{P}_2(V_i)$  in  $\mathfrak{P}_2(V)$ , und die Graphen  $G_i := (V_i, E_i)$  sind zusammenhängend. Sie heißen die Zusammenhangskomponenten von  $G$ .

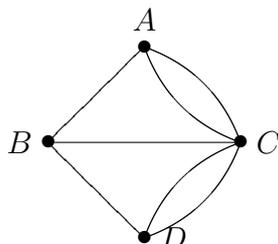
- Ist  $G$  zusammenhängend, so ist  $d(v, w) := \min\{l(\gamma) \mid \gamma \text{ ist ein Weg mit } A(\gamma) = v, E(\gamma) = w\}$  eine Metrik auf  $V$ . Wir setzen  $d(G) := \sup\{d(v, w) \mid v, w \in V\}$  und bezeichnen diese Zahl als den Durchmesser von  $G$ .
- Ein Zykel von  $G$  der Länge  $r \geq 3$  ist ein Untergraph isomorph zu  $C_r$ , also ein reduzierter geschlossener Weg der Länge  $r$ , in dem alle Knoten  $v_1, \dots, v_r$  verschieden sind, modulo zyklischer Vertauschung der  $v_i$  sowie der Orientierung.
- Ein Euler-Weg in  $G$  ist ein geschlossener Weg in  $G$ , der alle Kanten genau einmal durchläuft.
- Ein Hamilton-Zykel in  $G$  ist ein Zykel in  $G$ , der alle Knoten enthält.

Wir treffen folgende *Verabredung*: Alle betrachteten Graphen  $G$  seien endlich, falls nicht ausdrücklich anderes gesagt wird.

**Beispiel 10.2.** In der Stadt Königsberg sind die beiden Ufer  $A, D$  des Flusses Pregel und zwei in diesem Fluß gelegene Inseln  $B, C$  so durch sieben Brücken verbunden wie in der folgenden schematischen Darstellung:



Gibt es einen geschlossenen Weg, der jede Brücke genau einmal benutzt? Um das Problem mathematisch zu formulieren, bietet sich auf den ersten Blick eine graphentheoretische Sichtweise an; allerdings ist das folgende Gebilde kein Graph nach unserer Definition:



man kann es aber zu einem Graphen machen, indem man auf den zwei Kanten zwischen  $A$  und  $C$  sowie auf den zwei Kanten zwischen  $D$  und  $C$  jeweils einen zusätzlichen Knoten einführt; man erhält einen Graphen  $G$  mit 8 Knoten und 11 Kanten. Die Frage ist nun: Gibt es einen Eulerweg in  $G$ ? Nein, denn es gilt folgender

**Satz 10.3.** *Ein zusammenhängender Graph  $G$  besitzt genau dann einen Eulerweg, wenn gilt: für alle  $v \in V$  ist  $d(v)$  gerade.*

*Beweis.* “ $\Rightarrow$ ” ist klar; “ $\Leftarrow$ ”:

(i) Ist  $E \neq \emptyset$ , so existiert ein geschlossener Weg der Länge  $> 0$  in  $G$ , in dem alle Kanten verschieden sind. Starte hierzu mit  $e_1 = (v_0, v_1)$ . Es existiert  $e_2 = (v_1, v_2)$  mit  $v_2 \neq v_0$ ; man kann entsprechend solange eine Kante  $e_{i+1} = (v_i, v_{i+1})$  finden, die als nichtorientierte Kante verschieden von den bisher verwendeten nichtorientierten Kanten ist, wie  $v_i \neq v_0, \dots, v_{i-1}$  ist. Irgendwann ist  $v_{i+1} = v_{j-1}$  für ein  $j < i$ . Dann ist  $\gamma = e_j e_{j+1} \cdots e_{i+1}$  ein geschlossener Weg mit  $A(\gamma) = v_{j-1} = E(\gamma)$ .

(ii) Induktion nach der Zahl der Kanten  $|E|$ . Für  $|E| = 0$  ist nichts zu zeigen. Im Fall  $|E| \neq 0$  seien  $\gamma$  ein geschlossener Weg maximaler Länge, in dem alle auftretenden Kanten verschieden sind, und  $C$  der entsprechende Untergraph.

*Behauptung:*  $C = G$ .

Angenommen, es wäre  $C \neq G$ . Dann ist für  $G' := G - E(C)$  die Menge  $E(G') \neq \emptyset$ ; sei also  $e'$  ein Element von  $E(G')$ .

(iii) Weil  $G$  zusammenhängend ist, existiert in  $C$  ein Knoten  $v$  mit einer Kante  $e = \{v, w\}$ , die in  $C$  nicht vorkommt. Denn es gibt zwei Möglichkeiten für  $e'$ :

- 1) einer der Knoten von  $e'$  gehört zu  $C$ ; dann kann man diesen Knoten als  $v$  nehmen und  $e := e'$  setzen;
- 2) keiner der Knoten von  $e'$  gehört zu  $C$ ; es gibt dann aus Zusammenhangsgründen einen Weg von einem der Knoten von  $e'$  nach irgendeinem Knoten  $\tilde{v}$  von  $C$ . Man setzt dann  $v := \tilde{v}$  und nimmt als  $e$  die erste Kante dieses Wegs, die nicht mehr zu  $C$  gehört.

(iv) O.B.d.A sei  $A(\gamma) = E(\gamma) = v$ .

(v) Sei  $H$  die Zusammenhangskomponente von  $G'$ , die  $e$  enthält.  $H$  ist zusammenhängend, und alle  $v' \in H$  haben geraden Grad.

(vi) Nach Induktionsvoraussetzung existiert in  $H$  ein Euler-Weg  $\delta$ ; o.B.d.A. sei  $A(\delta) = E(\delta) = v$ .

(vii)  $\gamma$  und  $\delta$  haben gleiche Basispunkte und sind kantendisjunkt. Also ist  $\gamma * \delta$  ein Weg der Länge  $> l(\gamma)$ , in dem alle Kanten verschieden sind, im Widerspruch zur Maximalität von  $\gamma$ .  $\square$

**Beobachtung 10.4.** Die Zahl der  $v \in V$ , für die gilt, daß  $d(v)$  ungerade ist, ist gerade.

*Beweis.* Wegen  $\sum_{v \in V} d(v) = 2|E|$  ist

$$\sum_{\substack{v \in V \\ d(v) \equiv 1 \pmod{2}}} d(v) = 2|E| - \sum_{\substack{v \in V \\ d(v) \equiv 0 \pmod{2}}} d(v);$$

insbesondere ist die links stehende Summe gerade, da der rechts stehende Ausdruck gerade ist.  $\square$

**Satz 10.5.** Gilt in einem Graphen  $G$  mit  $|V| \geq 3$ , daß  $d(v) \geq \frac{|V|}{2}$  für alle  $v \in V$ , so enthält  $G$  einen Hamilton-Zykel.

*Beweis.* (i) Die Aussage ist richtig für  $G = K_n$  mit  $n \geq 3$  (triviale Induktion nach  $n$ ).

(ii) Angenommen, die Aussage sei falsch; füge zu  $G$  weitere Kanten  $e$  hinzu, solange dies geht, ohne daß ein Hamilton-Zykel entsteht. Es entsteht ein Graph  $G'$ , für den folgendes gilt:

- $V' = V$ , also  $|V'| \geq 3$ ;
- $G'$  ist zusammenhängend;
- $d(v) \geq \frac{|V'|}{2} \forall v \in V'$ ;
- $G'$  hat keinen Hamilton-Zykel;
- jede weitere Kante erzeugt einen Hamilton-Zykel.

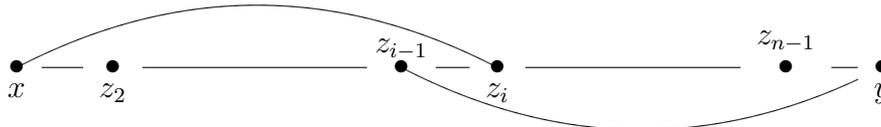
O.B.d.A sei von jetzt an  $G := G'$ .

(iii) Da  $G \neq K_n$ , gibt es  $x, y \in V$ , die nicht benachbart sind. Sei  $\tilde{G}$  der Graph mit  $V(\tilde{G}) := V(G)$  und  $E(\tilde{G}) := E(G) \cup \{\{x, y\}\}$ . Dieser Graph  $\tilde{G}$  enthält einen Hamilton-Zyklus, also enthält  $G$  selbst einen Weg  $x = z_1, z_2, \dots, z_n = y$ , der alle Knoten von  $G$  genau einmal trifft.

(iv) Es ist  $d(x) + d(y) \geq n$ . Verteile wie folgt  $d(x) + d(y) - 1$  Kugeln auf  $\{i \mid 2 \leq i \leq n - 1\}$ :

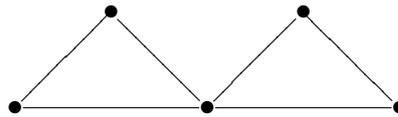
- nach  $i$  kommt eine Kugel, falls  $\{x, z_i\} \in E$  (dies sind  $d(x)$  viele);
- nach  $i$  kommt eine Kugel, falls  $\{z_{i-1}, y\} \in E$  (dies sind  $d(y) - 1$  viele).

Nach dem Schubfachprinzip gibt es ein  $i$  zwischen 2 und  $n - 1$  mit  $\{x, z_i\} \in E$  und  $\{z_{i-1}, y\} \in E$ .



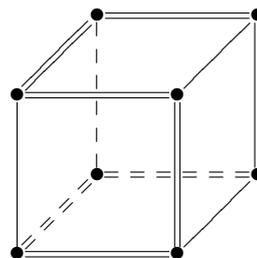
(v) Dann bildet  $x, z_2, \dots, z_{i-1}, y, z_{n-1}, \dots, z_i, x$  einen Hamilton-Zykel in  $G$ , im Widerspruch zur Annahme.  $\square$

**Bemerkungen, Beispiele 10.6.** (i) Es gibt zusammenhängende Graphen ohne Hamilton-Zykeln, z.B. wenn ein  $v \in V$  mit  $d(v) = 1$  existiert, oder



etc.

(ii) 10.5 ist hinreichend, aber bei weitem nicht notwendig. Dies sieht man am Beispiel des Würfels (der Hamilton-Weg verläuft entlang der doppelt gezeichneten Kanten):



es ist hier  $|V| = 8$  und  $d(v) = 3$  für alle  $v \in V$ .

(iii) Es ist also ziemlich undurchsichtig, welche Graphen Hamilton-Zykeln besitzen. Es ist kein in  $n = |V|$  polynomialer Algorithmus bekannt, der für einen gegebenen Graphen entscheidet, ob ein Hamilton-Zykel existiert, und diesen gegebenenfalls konstruiert.

**Definition/Satz 10.7.** Sei  $G = (V, E)$  ein endlicher zusammenhängender Graph. Es sind äquivalent:

- (i)  $G$  ist minimal zusammenhängend, d.h. läßt man eine Kante  $e$  weg, so ist  $G - \{e\}$  nicht mehr zusammenhängend;
- (ii)  $G$  besitzt keine Zykel;
- (iii)  $|E| = |V| - 1$ .

Solche Graphen heißen Bäume.

*Beweis.* (i) $\Rightarrow$ (ii): Man könnte in einem Zykel  $C$  eine beliebige Kante weglassen, ohne den Zusammenhang von  $C$  zu zerstören.

(ii) $\Rightarrow$ (iii): Weil  $G$  zusammenhängend ist, ist  $|E| \geq |V| - 1$ ; wir zeigen die Gleichheit durch Induktion nach  $|E|$ . Für  $|E| = 0$  ist nichts zu zeigen; wir behaupten: für  $|E| > 0$  existiert  $v \in V$  mit  $d(v) = 1$ .

Zum Beweis dieser Behauptung starten wir mit  $v_0$  und laufen entlang eines Wegs  $v_0, v_1, \dots, v_r$  mit lauter verschiedenen Knoten  $v_i$ , solange dies möglich ist. Bei Abbruch ist  $d(v_r) = 1$ , denn sonst gäbe es einen Nachbarn  $w$  von  $v_r$ , der schon besucht wurde, also  $w = v_i$  für ein  $i$ . Damit hätte man einen geschlossenen reduzierten Weg  $v_i \dots v_r v_i$  im Widerspruch zur Voraussetzung (ii). Insgesamt können wir also  $v := v_r$  setzen.

Setze ferner  $G' := (V', E')$  mit  $V' := V - \{v\}$  und  $E' := E - \{e\}$ , wobei  $e$  die einzige Kante ist, zu der  $v$  gehört. Dann ist  $G'$  zusammenhängend und zyklfrei, so daß nach Induktionsannahme  $|E'| = |V'| - 1$  ist; also ist auch  $|E| = |V| - 1$ .

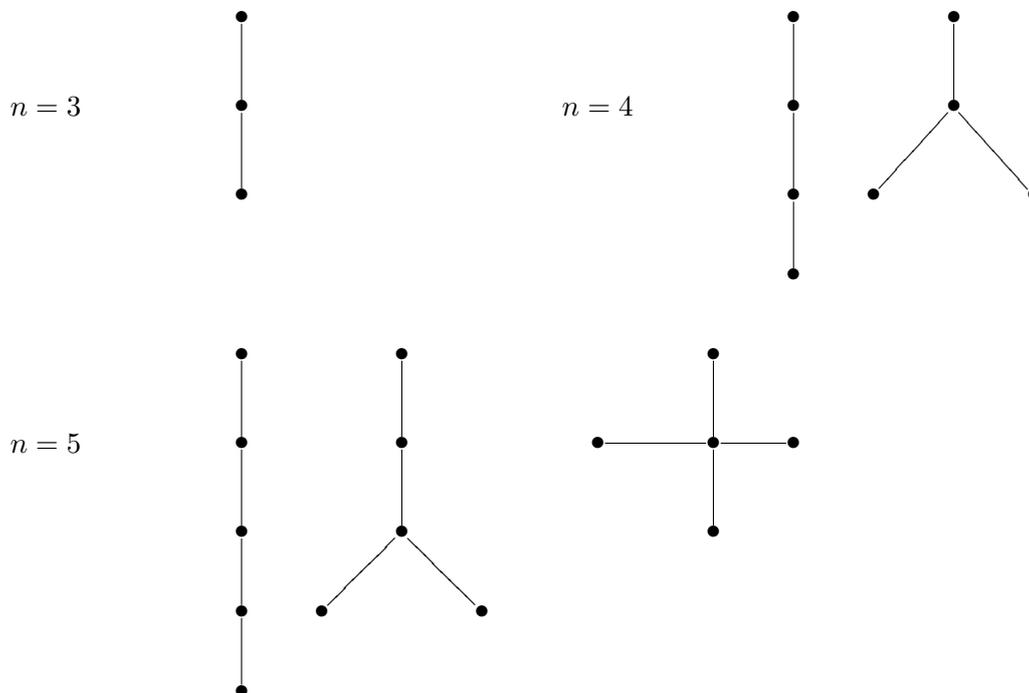
(iii) $\Rightarrow$ (i): Ließe man eine Kante weg, hätte man im verbleibenden Graph die Ungleichung  $|E| < |V| - 1$ ; dieser wäre also nicht mehr zusammenhängend.  $\square$

**Korollar 10.8.** Sei  $T$  ein Baum.

- (i) Zu  $v, w \in V(T)$  existiert ein eindeutiger reduzierter Weg  $\gamma$  mit  $A(\gamma) = v$  und  $E(\gamma) = w$ ;
- (ii)  $\exists v \in V(T)$  mit  $d(v) = 1$ .

$\square$

**Beispiel 10.9.** Es gibt folgende Isomorphieklassen von Bäumen mit  $n$  Knoten:



Die Frage, wieviele solche Isomorphieklassen es bei beliebigem  $n$  gibt, ist nicht ohne weiteres zu beantworten; die Beantwortung wird leichter, wenn die Knoten mit Nummern versehen sind.

**Korollar 10.10.** Sei  $G = (V, E)$  und  $|V| = n$ .

(i) Ist  $G$  zykliefrei, so gilt  $|E| \leq n - 1$  und

$$|E| = n - 1 \Leftrightarrow G \text{ ist Baum} \Leftrightarrow G \text{ ist zusammenhängend};$$

(ii) Ist  $G$  zusammenhängend, so gilt  $|E| \geq n - 1$  und

$$|E| = n - 1 \Leftrightarrow G \text{ ist Baum} \Leftrightarrow G \text{ ist zykliefrei}.$$

*Beweis.* Zu (i): Sind  $G_i = (V_i, E_i)$  für  $1 \leq i \leq r$  die Zusammenhangskomponenten von  $G$ , so gilt

$$G = \dot{\bigcup}_{1 \leq i \leq r} G_i ;$$

außerdem sind die  $G_i$  zusammenhängend und zykliefrei, also Bäume. Es ist

$$|E| = \sum |E_i| = \sum_{1 \leq i \leq r} (|V_i| - 1) = \left( \sum_{1 \leq i \leq r} |V_i| \right) - r = n - r .$$

Zu (ii): Ist  $G$  Baum, so ist  $|E| = n - 1$ . Andernfalls kann eine Kante weggelassen werden, ohne daß die Zusammenhangseigenschaft verloren geht, und zwar solange, bis ein Baum  $T$  mit derselben Knotenmenge  $V$  entsteht. Bezeichnet  $s$  die Zahl der weggelassenen Kanten, so ist

$$|E| = |E(T)| + s = n - 1 + s .$$

□

**Satz 10.11** (Cayley um 1860). *Die Zahl der Bäume  $T = (V, E)$  mit  $V = \mathbb{N}_n$  ist  $t_n = n^{n-2}$  für  $n \geq 2$ .*

*Beweis.* Zunächst überlegt man sich: Man kann anstelle der Baumstrukturen insgesamt auch die *zwei-markierten Bäume* zählen, d.h. die Bäume  $T$  mit zwei ausgezeichneten Knoten  $v, w$  (die gleich sein können, deren Reihenfolge aber festliegt). Es gibt  $n^2$  Zwei-Markierungen auf jedem  $T$ ; es genügt also zu zeigen, daß es  $n^n$  zwei-markierte Bäume gibt.

Wir konstruieren eine Bijektion von  $\text{Abb}(\mathbb{N}_n, \mathbb{N}_n)$  auf die Menge der zwei-markierten Bäume zu  $\mathbb{N}_n$ . Sei dazu  $f \in \text{Abb}(\mathbb{N}_n, \mathbb{N}_n)$ ; wir setzen

$$\begin{aligned} C &:= \{x \in \mathbb{N}_n \mid \exists i \in \mathbb{N} \text{ mit } f^i(x) = x\} \\ &=: \{c_1 < c_2 < \dots < c_k\} \end{aligned}$$

( $C$  ist nichtleer, denn  $x, f(x), f^2(x), \dots$  muß sich irgendwann wiederholen.)

Weiter ist  $f|_C$  bijektiv auf  $C$ .) und

$$d_i := f(c_i) .$$

Für  $1 \leq i \leq k - 1$  zeichnen wir je eine Kante von  $d_i$  nach  $d_{i+1}$  (zusammen also  $k - 1$  Stück); wir setzen  $v := d_1$  und  $w := d_k$ . Für alle weiteren  $j \in \mathbb{N}_n - C$  verbinden wir  $j$  mit  $f(j)$  durch eine Kante (dies ergibt  $n - k$  Kanten). Wir erhalten einen Graphen  $T$  mit  $n$  Knoten und  $n - 1$  Kanten. Da in  $j, f(j), f^2(j), \dots$  irgendwann Wiederholungen auftreten, sind der Knoten  $j$  und einer der Knoten  $d_i$  verbunden. Der entstehende Graph  $T$  ist also zusammenhängend; da er  $n - 1$  Kanten hat, ist er ein Baum, der durch  $v$  und  $w$  zwei-markiert ist.

Sei umgekehrt  $(T, v, w)$  ein zwei-markierter Baum auf  $\mathbb{N}_n$ . Sei  $\gamma$  der wohlbestimmte reduzierte Weg von  $v$  nach  $w$ ,  $\gamma = (v = d_1, d_2, \dots, d_k = w)$ . Die  $d_i$  seien der Größe nach geordnet als  $c_1 < c_2 < \dots < c_k$ . Für  $j \in \mathbb{N}_n, j \neq d_i$  sei  $f(j)$  der Nachbar von  $j$  auf dem wohlbestimmten Weg von  $j$  nach  $\gamma$ ; ferner sei  $f(c_i) := d_i$ . Dann ist  $f$  eine wohldefinierte Abbildung von  $\mathbb{N}_n$  nach  $\mathbb{N}_n$ , und  $f \leftrightarrow (T, v, w)$  ist bijektiv. □

*Bemerkungen:*

- (i) Hat der ausgezeichnete Weg  $\gamma = (v = d_1, d_2, \dots, d_k = w)$  in  $(T, v, w)$  die Länge  $k - 1$ , so ist  $k = |\text{Bild}(f^\infty)| = |\text{Bild}(f^{n-1})|$ . Insbesondere gilt:  $T$  ist genau dann isomorph zu  $P_n$ , der Strecke von  $v$  nach  $w$ , wenn  $f$  bijektiv ist, und dafür gibt es genau  $n!$  Möglichkeiten.
- (ii) Die Zahl der Isomorphieklassen von Bäumen mit  $n$  Knoten ist  $\geq \frac{n^{n-2}}{n!} \gg \frac{e^n}{n^2 \sqrt{2\pi n}}$ . Z.B. ist diese Zahl 823065 für  $n = 20$ , während  $20^{18}/20!$  den Wert 107750 liefert.

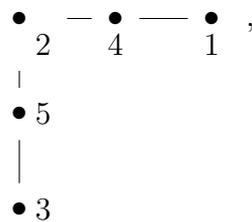
**Beispiel 10.12.** Die Konstruktionen des Beweises sollen an einem Beispiel veranschaulicht werden. Sei  $n = 5$  und  $f : \mathbb{N}_5 \rightarrow \mathbb{N}_5$  gegeben durch

$$\frac{k \in \mathbb{N}_5 \mid 1 \quad 2 \quad 3 \quad 4 \quad 5}{f(k) \mid 2 \quad 4 \quad 5 \quad 1 \quad 2} ;$$

$f^2$  ist also

$$\frac{k \in \mathbb{N}_5 \mid 1 \quad 2 \quad 3 \quad 4 \quad 5}{f^2(k) \mid 4 \quad 1 \quad 2 \quad 2 \quad 4}$$

Insgesamt ist hier  $C = \{1, 2, 4\}$ . Der im Beweis konstruierte Baum hat die Darstellung



wobei  $v$  der Knoten mit der Nummer 2 und  $w$  der Knoten mit der Nummer 1 ist.

**Definition 10.13.** Sei  $G = (V, E)$  ein zusammenhängender endlicher Graph. Ein Untergraph  $T$  heißt maximaler Unterbaum (oder spannender oder erzeugender Unterbaum), wenn gilt:

- (i)  $T$  ist Baum;
- (ii)  $V(T) = V$ .

Nach 10.11 hat  $K_n$  genau  $n^{n-2}$  maximale Unterbäume. Jeder zusammenhängende endliche Graph besitzt einen maximalen Unterbaum. Dieser entsteht nach 10.10 durch Weglassen von  $|E| - |V| + 1$  Kanten; allerdings müssen die weggelassenen Kanten gewissen Bedingungen unterworfen werden. Z.B. hat der  $K_4$  genau  $4^2 = 16$  maximale Unterbäume; es gibt aber  $\binom{6}{3} = 20$  Möglichkeiten, 3 Kanten wegzulassen (die Zusammenstellung der maximalen Unterbäume wird zur Übung empfohlen).

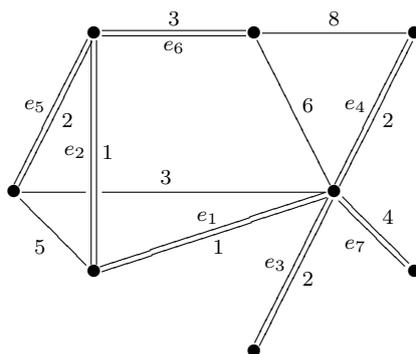
Maximale Unterbäume kommen in technischen Problemstellungen vor:

- elektrische Netzwerke: ein Potential auf den Knoten kann durch Potentialdifferenz auf den Kanten eines maximalen Unterbaums festgelegt werden.
- Telefonnetze, Datennetze, Transportnetze.

Die grundlegenden Probleme im Zusammenhang mit diesem Begriff bestehen darin, einen Algorithmus zu finden

- zur Bestimmung eines maximalen Unterbaums zu einem gegebenen Graphen  $G$ , eventuell mit Nebenbedingungen;
- zur Bestimmung der Zahl aller maximalen Unterbäume.

**Beispiel 10.14.** Sei  $G$  der folgende Graph, wobei die Kanten mit den eingezeichneten Gewichten versehen sind.



Ein maximaler Unterbaum ist mit den doppelt gezeichneten Kanten gegeben. Suche den maximalen Unterbaum  $T$  mit minimalem Gewicht (d.h.  $\sum_{e \in E(T)} w(e)$  ist minimal unter allen  $T$ )!

Sei im folgenden  $G = (V, E)$  ein zusammenhängender Graph mit  $|V| = n$  und  $w : E \rightarrow \mathbb{R}_{\geq 0}$  eine Gewichtsfunktion.

**Algorithmus 10.15.** (“Greedy-Algorithmus” zur Bestimmung des maximalen Unterbaums minimalen Gewichts)

- (0)  $E' = \emptyset$ .
- (1) Wähle  $e_1$  mit  $w(e_1)$  minimal (diese Wahl ist nicht notwendig eindeutig; wähle ein solches  $e_1$ ); füge  $e_1$  zu  $E'$  hinzu.
- (2) Wähle  $e_2$  mit minimalem Gewicht in  $E - E'$ ; füge  $e_2$  zu  $E'$  hinzu.

(3) Für  $i \geq 3$  wähle  $e_i$  mit:

- (i)  $e_i \notin E'$  ;
- (ii)  $(V, E' \cup \{e_i\})$  hat keinen Zykel;
- (iii)  $w(e_i)$  minimal mit (i), (ii);

füge  $e_i$  zu  $E'$  hinzu.

(4) Falls dies nicht geht: breche ab.

(5) Vergrößere  $i$  um 1 und gehe nach (3).

**Satz 10.16.** *Dieser Algorithmus liefert einen maximalen Unterbaum minimalen Gewichts des zusammenhängenden Graphen  $G$ . Insbesondere bricht das Verfahren genau bei  $i = n = |V|$  ab, d.h. bei Abbruch ist  $E' = \{e_1, \dots, e_{n-1}\}$ .*

**Lemma 10.17.** *Seien  $H_1, H_2$  zykelfreie Untergraphen von  $G$  mit derselben Knotenmenge  $V$  wie  $G$  und  $|E(H_1)| < |E(H_2)|$ . Dann existiert  $e \in E(H_2) - E(H_1)$ , so daß auch  $(V, E(H_1) \cup \{e\})$  zykelfrei ist.*

*Beweis.* Angenommen, die Aussage sei falsch. Dann gilt für alle  $e \in E(H_2)$ , daß  $e$  bereits zu  $E(H_1)$  gehört oder in  $H_1$  einen Zykel erzeugt. In beiden Fällen verbindet  $e$  Knoten, die schon in  $H_1$  durch einen Weg verbunden sind, also zur selben Zusammenhangskomponente gehören.

Dies hat zur Folge, daß jede Zusammenhangskomponente von  $H_2$  in einer Zusammenhangskomponente von  $H_1$  enthalten ist. Deshalb besitzt  $H_2$  mindestens so viele Zusammenhangskomponenten wie  $H_1$  im Widerspruch zu 10.10 (i), wonach  $H_2$ , da es mehr Kanten hat, weniger Zusammenhangskomponenten besitzen muß.  $\square$

*Beweis von 10.16.* (i) Der Algorithmus bricht ab bei  $E' = \{e_1, \dots, e_{i-1}\}$ , wenn kein  $e_i$  existiert mit  $e_i \notin E'$  und  $(V, E' \cup \{e_i\})$  zykelfrei. Wird in 10.17  $H_1 := (V, E')$  gesetzt und für  $H_2$  ein maximaler Unterbaum  $T$  genommen, so folgt  $i \geq n$ , und wegen 10.10 dann sogar  $i = n$ . Dies zeigt, daß der Algorithmus jedenfalls einen maximalen Unterbaum  $T$  liefert; es bleibt zu zeigen, daß dieser minimales Gewicht hat.

(ii) Angenommen,  $H$  wäre ein maximaler Unterbaum mit  $w(H) < w(T)$ .

Seien  $h_1, \dots, h_{n-1}$  die Kanten von  $H$ , so geordnet, daß gilt

$$w(h_1) \leq w(h_2) \leq \dots \leq w(h_{n-1}) ,$$

und seien  $e_1, \dots, e_{n-1}$  die Kanten von  $T$  in der Reihenfolge ihrer Auswahl, so daß also gilt

$$w(e_1) \leq w(e_2) \leq \dots \leq w(e_{n-1}) .$$

Sei  $i$  der kleinste Index mit

$$\sum_{1 \leq j \leq i} w(h_j) < \sum_{1 \leq j \leq i} w(e_j) ;$$

dann ist  $i \geq 2$  und  $w(h_i) < w(e_i)$ .

(iii) Seien

$$\begin{aligned} T_{i-1} &:= (V, \{e_1, \dots, e_{i-1}\}) ; \\ H_i &:= (V, \{h_1, \dots, h_i\}) . \end{aligned}$$

Nach (10.17) existiert ein  $j$  zwischen 1 und  $i$ , so daß für  $h_j$  gilt

- $h_j \notin E(T_{i-1})$  ;
- $h_j$  produziert zusammen mit  $T_{i-1}$  keinen Zykel (d.h.  $(V, \{e_1, \dots, e_{i-1}, h_j\})$  ist zykel-frei).

Es gilt jedoch  $w(h_j) \leq w(h_i) < w(e_i)$ , im Widerspruch dazu, daß der Algorithmus im  $i$ -ten Schritt  $e_i$  gewählt hat.  $\square$

## 11 Abzähl Aussagen über Graphen

Wir kennen bereits die Zahl der Bäume  $T$  mit  $V(T) = \mathbb{N}_n$  (es sind  $n^{n-2}$  Stück) und die Zahl der Graphen  $G$  mit  $V(G) = \mathbb{N}_n$  (es sind  $2^{\binom{n}{2}}$  Stück). Es stellt sich nun die Frage, wieviele dieser Graphen zusammenhängend sind. Zunächst stellt man fest, daß die Zahl aller Graphen auf  $\mathbb{N}_n$  (die wir kennen) gleich folgender Zahl ist:

$$\sum_{\substack{(V_1, \dots, V_r) \\ \cup V_i = \mathbb{N}_n}} \prod_{1 \leq i \leq r} (\text{Zahl der zusammenhängenden Graphen auf } V_i) .$$

Um diese Feststellung ausnutzen zu können, entwickeln wir zunächst einige abstrakte Begriffe (links), die wir parallel sogleich an der Beispielsituation der zusammenhängenden Graphen illustrieren (rechts).

**11.1. Definition.** Sei  $P$  eine nichtleere Menge, die Bildermenge.

- |  |  |
|--|--|
| <p>(i) Eine Karte <math>C = (S, p)</math> ist ein Paar, bestehend aus einer endlichen Teilmenge <math>S \subset \mathbb{N}</math> (der Nummernmenge) und einem Bild <math>p \in P</math>. Das Gewicht <math>w(C)</math> einer Karte ist die Kardinalität von <math>S</math>. Der Standardrepräsentant der Karte <math>C = (S, p)</math> ist die Karte <math>(\mathbb{N}_{w(C)}, p)</math>.</p> | <p>Ein <i>numerierter Graph</i> ist ein endlicher Graph mit <math>V(G) \subset \mathbb{N}</math>. Wir ordnen jedem numerierten Graphen <math>G</math> den <i>standardnumerierten</i> Graphen <math>\tilde{G}</math> mit <math>V(\tilde{G}) = \mathbb{N}_{ V(G) }</math> zu, wobei wir <math>V(G)</math> mit <math>\mathbb{N}_{ V(G) }</math> in der wohlbestimmten ordnungserhaltenden Weise identifizieren. Als Bildermenge <math>P</math> nehmen wir hier die Menge aller standardnumerierten zusammenhängenden Graphen; eine Karte ist ein Paar <math>(S, p)</math> mit <math>S = V(G)</math> für einen numerierten zusammenhängenden Graphen <math>G</math> und <math>p = \tilde{G}</math>. Die Angabe einer Karte ist also äquivalent zur Angabe eines zusammenhängenden numerierten Graphen.</p> |
| <p>(ii) Eine Hand <math>H</math> ist eine endliche Menge von Karten <math>(S_i, p_i)</math>, deren Nummernmengen <math>S_i</math> eine Zerlegung von <math>\mathbb{N}_n</math> für ein <math>n \in \mathbb{N}</math> bilden. In diesem Fall ist <math>w(H) := n</math> das Gewicht von <math>H</math>.</p>   | <p>Eine Hand vom Gewicht <math>n</math> ist ein Graph <math>G = (V, E)</math> mit <math>V = \mathbb{N}_n</math>; die Karten dieser Hand sind die Zusammenhangskomponenten von <math>G</math>.</p>  |
| <p>(iii) Ein Deck <math>D</math> des Gewichts <math>w(D) = n</math> ist eine endliche Menge von Standardkarten (d.h. standardnumerierten Karten) <math>C_i = (\mathbb{N}_n, p_i)</math> mit lauter verschiedenen <math>p_i</math>.</p>   | <p>Die Menge aller zusammenhängenden Graphen <math>G</math> mit <math>V(G) = \mathbb{N}_n</math> ist ein Deck vom Gewicht <math>n</math>.</p>  |

- (iv) Eine Exponentialfamilie  $\mathcal{F}$  zur Bildermenge  $P$  ist eine Folge  $D_1, D_2, \dots$  von Decks mit  $w(D_i) = i$ .
- (v) Für eine Exponentialfamilie

$$\mathcal{F} = (D_1, D_2, \dots)$$

seien

$$d_n := |D_n| \text{ für } n \geq 1 ; d_0 := 0 ;$$

$$D(X) := \sum_{n \geq 0} d_n \frac{X^n}{n!} \in \mathbb{Q}[[X]] ;$$

$h(n, k) :=$  Zahl der Hände des Gewichts  $n$  mit  $k$  Karten, wobei alle auftretenden Karten  $C = (S, p)$  einen Standardrepräsentanten in  $D_{w(C)}$  besitzen ;

$$h(n) := \sum_k h(n, k) ;$$

$$H(X, Y) := \sum_{n, k \geq 0} h(n, k) \frac{X^n}{n!} Y^k .$$

Im Beispiel sind  $d_n$  die Zahl der zusammenhängenden Graphen mit Knotenmenge  $V = \mathbb{N}_n$ , weiter  $h(n, k)$  die Zahl der standardnumerierten Graphen mit  $V = \mathbb{N}_n$  mit genau  $k$  Zusammenhangskomponenten, schließlich  $h(n)$  die Zahl aller standardnumerierten Graphen mit  $V = \mathbb{N}_n$ , also  $2^{\binom{n}{2}}$ .

**Definition/Lemma 11.2.** Seien zwei Exponentialfamilien  $\mathcal{F}' = (D'_1, D'_2, \dots)$  und  $\mathcal{F}'' = (D''_1, D''_2, \dots)$  mit Bildermengen  $P', P''$  gegeben. Seien  $P' = \cup P'_i, P'' = \cup P''_i$ , wobei  $P'_i$  bzw.  $P''_i$  die Bilder sind, zu denen es in  $\mathcal{F}', \mathcal{F}''$  Standardkarten des Gewichts  $i$  gibt. Für alle  $i$  sei  $P'_i \cap P''_i = \emptyset$ . Betrachte die Exponentialfamilie  $\mathcal{F} = (D_1, D_2, \dots)$  zu  $P = P' \cup P''$  mit  $D_i := D'_i \dot{\cup} D''_i$ . Dieses  $\mathcal{F}$  heißt die direkte Summe  $\mathcal{F}' \oplus \mathcal{F}''$  von  $\mathcal{F}'$  und  $\mathcal{F}''$ . Für die erzeugenden Funktionen  $H, H', H''$  gilt

$$H(X, Y) = H'(X, Y) \cdot H''(X, Y) .$$

*Beweis.* Betrachte eine Hand  $H$  des Gewichts  $n$  in  $\mathcal{F}$ . Einige der Karten von  $H$  kommen von  $\mathcal{F}'$ , die anderen von  $\mathcal{F}''$ . Die von  $\mathcal{F}'$  herkommenden Karten bilden eine "Unterhand"  $H'$  von  $H$  mit Gewicht  $n' \leq n$  mit  $k' \leq k$  Karten und in ordnungstreuer Weise unnumeriert durch eine Teilmenge  $S' \subset \mathbb{N}_n$ ; ebenso für  $\mathcal{F}''$ . Die Angabe von  $H$  ist äquivalent zur Angabe

- von  $H'$  vom Gewicht  $n'$  mit  $k'$  Karten zu  $\mathcal{F}'$  ;
- der Teilmenge  $S'$  von  $\mathbb{N}_n$ , mit der  $H'$  unnumeriert wird;

- von  $H''$  vom Gewicht  $n'' := n - n'$  mit  $k'' := k - k'$  Karten zu  $\mathcal{F}''$  ;
- der Teilmenge  $S'' := \mathbb{N}_n - S'$  von  $\mathbb{N}_n$ , mit der  $H''$  umnumerierte wird

— wobei die letzte Angabe offensichtlich redundant ist. Versehen wir die Funktion  $h(n, k)$  mit Strichen je nachdem, von welcher Exponentialfamilie die jeweils gezählten Hände herkommen, so gilt also

$$h(n, k) = \sum_{\substack{(n', k'), (n'', k'') \\ n' + n'' = n, k' + k'' = k}} h'(n', k') h''(n'', k'') ,$$

und dies ist der Koeffizient von  $\frac{X^n}{n!} Y^k$  in  $H'(X, Y) \cdot H''(X, Y)$  . □

**Satz 11.3.** *Es sei  $\mathcal{F}$  eine Exponentialfamilie mit erzeugenden Funktionen  $D(X)$  bzw.  $H(X, Y)$ . Dann gilt die Exponentialformel*

$$H(X, Y) = e^{Y D(X)} .$$

(Hierbei ist die rechts stehende formale Potenzreihe wohldefiniert, denn die einzusetzende Reihe hat kein Absolutglied, da jeder einzelne Term durch  $Y$  und durch  $X$  teilbar ist.)

*Beweis.* Wir beweisen den Satz für Spezialfälle, die zusehends allgemeiner werden, bis sich schließlich der allgemeine Fall ergibt.

(i) *Spezialfall:*  $\mathcal{F}$  besitze nur ein Deck  $D_r$  (d.h.  $D_i = \emptyset$  für  $i \neq r$ ) mit  $d_r = 1$ . Dann ist

$$D(X) = \sum_i d_i \frac{X^i}{i!} = \frac{X^r}{r!} . \tag{*}$$

Eine Hand  $H$  besteht aus einer gewissen Anzahl  $k$  von umnumerierte “Kopien” der Karte  $C$  in  $D_r$ ; genauer gilt  $H = \{C_1, \dots, C_k\}$  mit  $C_i := (S_i, p)$ ,  $|S_i| = r$  für alle  $i$  und  $\bigcup S_i = \mathbb{N}_n$ . Das Gewicht von  $H$  ist  $k \cdot r$ . Es ist also  $h(n, k) = 0$ , wenn  $n \neq kr$ ; bleibt zu untersuchen, welchen Wert  $h(kr, k)$  hat. Wir haben folgende Abzählungen:

$$\begin{array}{llll} \text{Zahl der Numerierungen } S_1 & \text{für } C_1 & = & \binom{kr}{r} ; \\ \dots & S_2 \dots C_2 & = & \binom{kr-r}{r} ; \\ \dots & \dots & & \dots \\ \dots & S_k \dots C_k & = & \binom{r}{r} . \end{array}$$

Da die Reihenfolge der Karten keine Rolle spielt, gilt also

$$h(kr, k) = \frac{\binom{kr}{r} \binom{kr-r}{r} \dots \binom{r}{r}}{k!} = \frac{\frac{(kr)!}{r!(kr-r)!} \frac{(kr-r)!}{r!(kr-2r)!} \dots \frac{r!}{r! \cdot 1!}}{k!} = \frac{(kr)!}{(r!)^k k!}$$

und damit für unser spezielles  $\mathcal{F}$

$$\begin{aligned} H(X, Y) &= \sum_{n,k} h(n, k) \frac{X^n}{n!} Y^k = \sum_k \frac{(kr)!}{(r!)^k k!} \frac{X^{kr}}{(kr)!} Y^k \\ &= \exp\left(\frac{X^r Y}{r!}\right) \stackrel{(*)}{=} \exp(YD(X)) . \end{aligned}$$

(ii) *Spezialfall:*  $d_r \in \mathbb{N}$ ; alle  $d_i$  sind  $= 0$  für  $i \neq r$ . Wir machen Induktion nach  $d_r$ ; der Fall  $d_r = 1$  wurde unter (i) behandelt. Sei also  $d_r > 1$ . Schreibe  $\mathcal{F} = \mathcal{F}' \oplus \mathcal{F}''$  mit  $d'_r := d_r - 1$  und  $d''_r := 1$ . Dann gilt die Behauptung nach Induktionsvoraussetzung für  $\mathcal{F}'$  und  $\mathcal{F}''$ ; es ist (wenn wir wieder durch Striche kennzeichnen, zu welcher Exponentialfamilie welche erzeugende Funktion gehört)

$$\begin{aligned} H(X, Y) &\stackrel{11.2}{=} H'(X, Y) \cdot H''(X, Y) = e^{YD'(X)} \cdot e^{YD''(X)} \\ &= e^{Y(D'(X)+D''(X))} = e^{Y((d_r-1)\frac{X^r}{r!} + \frac{X^r}{r!})} = e^{Y(d_r \frac{X^r}{r!})} = e^{YD(X)} . \end{aligned}$$

(iii) *Spezialfall:* Nur endlich viele Decks sind nichtleer, d.h. es existiert ein  $r \in \mathbb{N}$ , so daß  $D_i = \emptyset$  für  $i > r$ . In diesem Fall schreiben wir  $\mathcal{F} = \mathcal{F}' \oplus \mathcal{F}'' \oplus \dots \oplus \mathcal{F}^{(r)}$ , wobei  $\mathcal{F}^{(i)}$  die Exponentialfamilie ist, an deren  $i$ -ter Stelle  $D_i$  steht und sonst die leere Menge. Der Beweis erfolgt dann über Induktion nach  $r$  unter Verwendung von 11.2 und (ii).

(iv) *allgemeiner Fall:* Sei  $h^*(n, k)$  der Koeffizient von  $\frac{X^n}{n!} Y^k$  in  $e^{YD(X)}$ . Zu zeigen ist  $h^*(n, k) = h(n, k)$  für alle  $(n, k) \in \mathbb{N}^2$ . Klar ist

$$h(n, k) = 0 = h^*(n, k) \quad \text{für } k > n . \quad (**)$$

Sei  $\bar{\mathcal{F}}$  die Exponentialfamilie  $(D_1, D_2, \dots, D_r, \emptyset, \emptyset, \dots)$ . Dann gilt (mit einer offensichtlichen Kennzeichnung der Herkunft der  $h$ -Funktionen) für  $n \leq r$ :

$$h(n, k) = \bar{h}(n, k) ; \quad h^*(n, k) = \bar{h}^*(n, k) .$$

Für  $\bar{\mathcal{F}}$  gilt die Behauptung nach (iii). Daher ist  $\bar{h}(n, k) = \bar{h}^*(n, k)$  und damit auch  $h(n, k) = h^*(n, k)$  für  $k \leq n \leq r$ , sogar für alle  $(n, k)$  mit  $n \leq r$  wegen (\*\*). Da diese Überlegung für jedes beliebige  $r$  durchgeführt werden kann, gilt insgesamt die Behauptung für alle  $n \in \mathbb{N}$ . □

**Korollar 11.4.**

$$H(X) := \sum_{n \geq 0} h(n) \frac{X^n}{n!} = H(X, 1) = e^{D(X)} .$$

**Bemerkung 11.5.** Im Beispiel der Graphen sind  $h(n) = 2^{\binom{n}{2}}$  und  $d_n$  die Zahl der zusammenhängenden Graphen  $(V, E)$  mit  $V = \mathbb{N}_n$ . Nach dem Satz gilt also die Potenzreihenidentität

$$\sum_{n \geq 0} 2^{\binom{n}{2}} \frac{X^n}{n!} = \exp \left( \sum_{n \geq 0} d_n \frac{X^n}{n!} \right).$$

Die naheliegendste Strategie wäre nun, zu den von den Potenzreihen dargestellten Funktionen überzugehen und mithilfe der Logarithmusfunktion nach  $d_n$  aufzulösen. Leider funktioniert diese Strategie nicht, da die links stehende Potenzreihe Konvergenzradius 0 hat, wie man sich zur Übung klarmachen möge. Glücklicherweise gibt es hierfür Abhilfen:

**Erinnerung 11.6.** Seien  $f(X) = \sum_{i \geq 0} a_i X^i$  mit  $a_0 = 1$  und  $g(X) = \sum_{i \geq 1} b_i X^i$  Potenzreihen mit Koeffizienten in  $\mathbb{C}$ . Definiere  $\log(f) = \log(1 + (f - 1))$  durch Einsetzen von  $f - 1$  in  $\log(1 + X) = X - \frac{X^2}{2} + \frac{X^3}{3} - \dots$ . Dann gelten, unabhängig von Konvergenzüberlegungen:

$$e^{(\log(1+X))} = 1 + X, \quad \log(e^X) = X; \quad (\text{i})$$

$$e^{(\log(f))} = f(X); \quad (\text{ii})$$

$$\log(e^{g(X)}) = g(X); \quad (\text{iii})$$

$$\frac{d}{dX}(\log f) = \frac{f'(X)}{f(X)}. \quad (\text{iv})$$

Sei speziell  $f(X)$  die linke Seite von 11.4, also  $H(X)$ , und sei  $g(X)$  der Exponent der rechten Seite von 11.4, also  $D(X)$ . Es gelten dann (jede der Aussagen ist unmittelbare Folge ihrer Vorgängerin):

$$\begin{aligned} f(X) &= e^{g(X)}; & \log f(X) &= g(X); & \frac{d}{dX}(\log f(X)) &= \frac{d}{dX}g(X); \\ \frac{f'(X)}{f(X)} &= \frac{d}{dX}g(X); & X \frac{f'(X)}{f(X)} &= X \frac{d}{dX}g(X); & X f'(X) &= X g'(X) f(X). \end{aligned}$$

Koeffizientenvergleich liefert

$$n \cdot h(n) = \sum_{\substack{i, j \geq 0 \\ i+j=n}} \binom{n}{i} i \cdot d_i \cdot h(j) = \sum_{0 \leq i \leq n} \binom{n}{i} i \cdot d_i \cdot h(n-i);$$

hieraus erhält man direkt

$$h(n) = \sum_{0 \leq i \leq n} \binom{n-1}{i-1} d_i \cdot h(n-i)$$

und schließlich mit  $h(0) = 1$

$$d_n = h(n) - \sum_{1 \leq i \leq n-1} \binom{n-1}{i-1} d_i \cdot h(n-i). \quad (*)$$

Dies ist eine in beide Richtungen lesbare Rekursion für  $n \geq 2$ . Wir haben bewiesen:

**Satz 11.7.** Für eine beliebige Exponentialfamilie  $\mathcal{F}$  und  $n \geq 2$  gilt (\*).

**Korollar 11.8.** Für die Zahl  $d_n$  der zusammenhängenden Graphen mit Knotenmenge  $\mathbb{N}_n$  gilt die Rekursion

$$d_n = 2^{\binom{n}{2}} - \sum_{1 \leq i \leq n-1} \binom{n-1}{i-1} 2^{\binom{n-i}{2}} d_i .$$

Die Tafel der  $d_n$  in der graphentheoretischen Situation beginnt folgendermaßen:

$n$	1	2	3	4	5	6
$d_n$	1	1	4	38	728	26704

*Bemerkung:* Beschränkt man sich auf den graphentheoretischen Begriffsapparat, ist die Zerlegung von  $\mathcal{F}$  in eine direkte Summe keine sinnvolle Operation. Der allgemeinere begriffliche Rahmen war also der Schlüssel zur Lösung des Problems. Darüberhinaus gibt es weitere Beispiele von Exponentialfamilien, in deren Behandlung der Satz 11.3 nützlich ist:

**Beispiele 11.9.** 1) Sei  $\mathcal{F}$  die folgende Exponentialfamilie:

- eine Karte ist ein beliebiger Zykel in  $S_n$  für  $n \in \mathbb{N}$  (hat der Zykel  $r$  Glieder, so ist die zugehörige Standardkarte das Element von  $S_r$  mit der passenden Reihenfolge);
- eine Hand vom Gewicht  $n$  ist ein Element von  $S_n$ ;
- ein Deck vom Gewicht  $n$  ist die Menge aller Standardkarten vom Gewicht  $n$ , d.h. die Menge der Zykel der Länge  $n$  in  $S_n$ .

Mit diesen Festsetzungen sind offenbar  $h(n, k) = c(n, k)$ ,  $h(n) = \sum_k h(n, k) = n!$  und  $d_n = (n-1)!$ . Aus 11.7 erhalten wir zunächst nur

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

— also nichts Spektakuläres. Doch sieht man sich anstelle von  $H(X, 1)$  allgemeiner  $H(X, Y)$  an, so ergibt sich mit

$$D(X) \stackrel{d_0=0}{=} \sum_{n \geq 1} (n-1)! \frac{X^n}{n!} = \sum_{n \geq 1} \frac{X^n}{n} = \log \left( \frac{1}{1-X} \right)$$

aus 11.3

$$\sum_{n,k} c(n, k) \frac{X^n}{n!} Y^k = \exp \left( Y \log \left( \frac{1}{1-X} \right) \right) = \frac{1}{(1-X)^Y} ,$$

also eine erzeugende Funktion für die  $c(n, k)$ , die wir bisher noch nicht kannten.

2) Eine weitere Exponentialfamilie ergibt sich mit folgenden Setzungen:

- eine Karte ist eine nichtleere Teilmenge von  $\mathbb{N}_n$ ;
- eine Hand ist eine Zerlegung von  $\mathbb{N}_n$ ; die Zahl der Hände ist also die  $n$ -te Bell-Zahl.

Man erhält hier, ganz ähnlich wie in 1), eine erzeugende Funktion in zwei Variablen für die  $S(n, k)$ ; dies sei zur Übung empfohlen.

3) In Abwandlung von Beispiel 1) kann man anstelle aller Zykel von  $S_n$  auch nur die geraden oder nur die ungeraden Zykel betrachten.

## 12 Polya-Abzählung

Wir wissen nun, wieviele Graphen, Bäume oder zusammenhängende Graphen mit Knotenmenge  $\mathbb{N}_n$  es gibt; was wir bisher noch nicht wissen, ist, wieviele *Isomorphieklassen* solcher Graphen etc. es gibt.

**Definition 12.1.** Die endliche Gruppe  $G$  operiere auf der endlichen Menge  $\mathcal{X}$  mit  $|\mathcal{X}| = n$ . Für  $g \in G$  sei  $\underline{c}(g) = (c_1(g), \dots, c_n(g))$  der Zykeltyp von  $g$  auf  $\mathcal{X}$ . Betrachte  $n$  verschiedene Unbestimmte  $X_1, \dots, X_n$  und ordne  $g \in G$  das Monom  $X_1^{c_1(g)} X_2^{c_2(g)} \dots X_n^{c_n(g)}$  zu. Der Ausdruck

$$Z_{G, \mathcal{X}}(X_1, \dots, X_n) := \frac{1}{|G|} \sum_{g \in G} X_1^{c_1(g)} \dots X_n^{c_n(g)}$$

heißt der Zykelzeiger von  $G$  auf  $\mathcal{X}$ .

*Bemerkung:* Ordnen wir  $X_i$  das Gewicht  $i$  zu, so ist  $Z_{G, \mathcal{X}}$  ein isobares Polynom vom Gewicht  $n$ , denn es gilt  $\sum i \cdot c_i(g) = n$ .

Seien  $|\mathcal{X}| = n$  und  $|\mathcal{Y}| = r$ . Operiert  $G$  auf  $\mathcal{X}$ , so operiert  $G$  auch von links auf  $\text{Abb}(\mathcal{X}, \mathcal{Y}) =: \mathcal{Y}^{\mathcal{X}}$  durch  $(gf)(x) = f(g^{-1}x)$  für  $f \in \mathcal{Y}^{\mathcal{X}}, x \in \mathcal{X}$  und  $g \in G$ .

**Satz 12.2.** Die Zahl der Bahnen von  $G$  auf  $\mathcal{Y}^{\mathcal{X}}$  ist

$$Z_{G, \mathcal{X}}(r, \dots, r) := \frac{1}{|G|} \sum_{g \in G} r^{c_1(g) + \dots + c_n(g)} .$$

*Beweis.* Nach dem Lemma von Burnside ist die Zahl der Bahnen auf  $\mathcal{Y}^{\mathcal{X}}$  gegeben durch

$$\frac{1}{|G|} \sum_{g \in G} |\{\text{Fixpunkte von } g \text{ auf } \mathcal{Y}^{\mathcal{X}}\}| .$$

Für ein  $g \in G$  gilt folgende Kette von Äquivalenzen:

$f : \mathcal{X} \rightarrow \mathcal{Y}$  ist  $g$ -invariant  
 $\Leftrightarrow f$  ist konstant auf allen Zykeln von  $g$   
 $\Leftrightarrow f$  ist Funktion auf der Menge der Zykel von  $g$  .

Hat  $g$  den Zykeltyp  $(c_1, \dots, c_n)$ , so gibt es genau  $c_1 + \dots + c_n$  Zykel; da es ferner  $r$  mögliche Werte gibt, die  $f$  auf einem Zykel annehmen kann, gibt es genau  $r^{c_1 + \dots + c_n}$  solche  $g$ -invarianten Funktionen  $f \in \mathcal{Y}^{\mathcal{X}}$ .  $\square$

**Anwendung 12.3.** Ein Graph mit Knotenmenge  $V = \mathbb{N}_k$  ist gegeben durch die Kantenmenge  $E \subset \mathfrak{P}_2(\mathbb{N}_k)$ , d.h. durch eine charakteristische Funktion  $\chi_E : \mathfrak{P}_2(\mathbb{N}_k) \rightarrow \{0, 1\}$ . Es gilt

$$(\mathbb{N}_k, E) \cong (\mathbb{N}_k, E') \Leftrightarrow \exists \sigma \in S_k \text{ mit } \sigma(E) = E' \Leftrightarrow \exists \sigma \in S_k \text{ mit } \sigma(\chi_E) = \chi_{E'} .$$

Daher gibt es eine Bijektion zwischen der Menge der Isomorphieklassen von Graphen mit  $k$  Knoten und der Menge  $S_k \setminus \text{Abb}(\mathfrak{P}_2(\mathbb{N}_k), \{0, 1\})$ . Zu bestimmen ist also

$$Z_{S_k, \mathfrak{P}_2(\mathbb{N}_k)}(X_1, \dots, X_n) \quad \text{mit } n = |\mathfrak{P}_2(\mathbb{N}_k)| = \binom{k}{2} .$$

**Satz 12.4** (Polya 1937). *Seien  $\mathcal{X}, \mathcal{Y}$  und  $G$  wie in der Situation von 12.2; wir schreiben  $\mathcal{Y} = \{y_1, \dots, y_r\}$  und  $\mathcal{Y}^{\mathcal{X}} = \mathcal{F}$ . Für  $\underline{a} = (a_1, \dots, a_r) \in \mathbb{N}_0^r$  mit  $w(\underline{a}) := \sum_{1 \leq j \leq r} a_j = n$  sei*

$$\mathcal{F}(\underline{a}) := \{f \in \mathcal{F} \mid |f^{-1}(y_j)| = a_j\} ,$$

so daß also gilt  $\mathcal{F} = \dot{\bigcup}_{w(\underline{a})=n} \mathcal{F}(\underline{a})$ ; ferner ist  $\mathcal{F}(\underline{a})$  stabil unter der Operation von  $G$ , d.h.  $\mathcal{F}(\underline{a})$  ist disjunkte Vereinigung von Bahnen von  $G$  auf  $\mathcal{F}$ .

Für jedes  $y_j \in \mathcal{Y}$  sei  $Y_j$  eine Unbestimmte. Dann gilt:

$$Z_{G, \mathcal{X}} \left( \sum_{1 \leq j \leq r} Y_j, \sum_{1 \leq j \leq r} Y_j^2, \dots, \sum_{1 \leq j \leq r} Y_j^n \right) = \sum_{\substack{\underline{a} \in \mathbb{N}_0^r \\ w(\underline{a})=n}} |G \setminus \mathcal{F}(\underline{a})| Y_1^{a_1} Y_2^{a_2} \dots Y_r^{a_r} . \quad (*)$$

*Beweis.* (i) Beide Seiten sind homogene Polynome in den  $Y_j$  vom Grad  $n$  (für die rechte Seite ist dies klar; für die linke folgt dies daraus, daß der Zykelzeiger allgemein ein isobares Polynom vom Gewicht  $n$  ist, und aus der speziellen Gestalt der eingesetzten Ausdrücke). Zu zeigen ist also die Gleichheit der Koeffizienten.

(ii) Nach 6.5 ist

$$|G \setminus \mathcal{F}(\underline{a})| = \frac{1}{|G|} \sum_{g \in G} \phi_g ,$$

wobei  $\phi_g$  hier die Anzahl der Fixpunkte von  $g$  bei festgehaltenem  $\underline{a}$  bezeichnet. Sei  $f \in \mathcal{F}(\underline{a})$  und  $g \in G$  mit Zykeltyp  $(c_1, \dots, c_n)$  auf  $\mathcal{X}$ . Dann ist  $f$  invariant unter  $g$  genau dann, wenn jeder Zykel von  $g$  auf  $\mathcal{X}$  ganz in einem  $f^{-1}(y_j)$  liegt. Daher ist  $\phi_g$  die Zahl der Zusammenfassungen der Zykel von  $g$  zu einer Zerlegung von  $\mathcal{X}$  vom Typ  $(a_1, \dots, a_r)$ .

Sind  $C_{i,k}$  die Zykel der Länge  $i$ , indiziert nach  $k$  (d.h.  $1 \leq k \leq c_i$ ), so ist

$$\mathcal{X} = \bigcup_{\substack{1 \leq i \leq n \\ 1 \leq k \leq c_i}} C_{i,k} ;$$

damit ist  $\phi_g$  die Zahl der Zusammenfassungen zu einer Zerlegung

$$\mathcal{X} = \bigcup_{1 \leq j \leq r} D_j \quad \text{mit } |D_j| = a_j .$$

(iii) Das Polynom links in (\*) ist gleich  $\frac{1}{|G|} \sum_{g \in G} X_1^{c_1(g)} \dots X_n^{c_n(g)}$ , wobei der Ausdruck  $\sum_j Y_j^i$  in  $X_i$  eingesetzt wird, also gleich

$$\frac{1}{|G|} \sum_{g \in G} \prod_{1 \leq i \leq n} \left( \sum_j Y_j^i \right)^{c_i(g)} .$$

Für festes  $g$  entsteht jeder Term von  $\prod_{1 \leq i \leq n} \left( \sum_j Y_j^i \right)^{c_i(g)}$  durch die Wahl eines Index  $j$  (d.h. eines der Terme  $Y_j^i$ ) für jeden Faktor; die Faktoren sind durch  $(i, k)$  indiziert mit  $1 \leq i \leq n$  und  $1 \leq k \leq c_i(g)$ . Der Beitrag zu  $Y_1^{a_1} \dots Y_r^{a_r}$  ist die Zahl derjenigen Wahlen unter den  $r^{c_1(g)} \cdot r^{c_2(g)} \cdot \dots \cdot r^{c_n(g)}$  möglichen Wahlen, für die sich die Exponenten von  $Y_j$  zu  $a_j$  aufsummieren.

(iv) Die Beiträge von  $g \in G$  zur linken und rechten Seite von (\*) sind gleich. Denn hat man in (iii) an der  $(i, k)$ -ten Stelle den Faktor  $Y_j^i$  gewählt, so gehört der Zykel  $C_{i,k}$  zu  $D_j$ . Umgekehrt gehört zu jeder Zerlegung wie in (ii) ein Satz von Wahlen wie in (iii): An der  $(i, k)$ -ten Stelle soll  $Y_j^i$  gewählt werden, falls  $C_{i,k}$  zu  $D_j$  gehört.  $\square$

**Beispiele 12.5.** Seien  $\mathcal{X} = \mathbb{N}_n$  und  $G \subset S_n$  eine Untergruppe. Wir berechnen  $Z_{G, \mathbb{N}_n}$  in den folgenden Fällen:

- (i)  $G = C_n$ , die zyklische Gruppe mit  $n$  Elementen; d.h.  $G = \langle \sigma \rangle$  mit  $\sigma = (12 \dots n)$ ;
- (ii)  $G = D_{2n}$ , die Diedergruppe mit  $2n$  Elementen; d.h.  $G = \langle \sigma, \tau \rangle$  mit  $\sigma$  wie in (i) und  $\tau = (1, n)(2, n-1) \dots$  (es gilt also  $D_{2n} = C_n \dot{\cup} \tau C_n$ , und es wird daran erinnert, daß  $\tau \sigma \tau^{-1} = \tau \sigma \tau = \sigma^{-1}$  gilt);
- (iii)  $G = S_n$ ;
- (iv)  $G = A_n$ .

Zu (i): Es ist  $\text{ord}(\sigma^j) = \frac{n}{\text{ggT}(n,j)} =: k$ . Dann hat  $\sigma^j$  genau  $\frac{n}{k}$  Zykeln, alle der Länge  $k$ , und es gibt genau  $\phi(k)$  solcher  $j$  zwischen 0 und  $n-1$  (wobei  $\phi$  die Eulersche  $\phi$ -Funktion bezeichnet). Deshalb gilt

$$Z_{C_n, \mathbb{N}_n} = \frac{1}{n} \sum_{g \in C_n} X_{k(g)}^{\frac{n}{k(g)}} = \frac{1}{n} \sum_{k|n} \phi(k) X_k^{\frac{n}{k}}.$$

Zu (ii): Für ungerades  $n$  hat jedes Element von  $D_{2n} - C_n$  Zykeltyp  $(1, \frac{n-1}{2}, 0, \dots)$ , d.h. einen Fixpunkt und  $\frac{n-1}{2}$  2-Zykel (man überzeuge sich hiervon). Daher gilt

$$Z_{D_{2n}, \mathbb{N}_n} = \frac{1}{2} Z_{C_n, \mathbb{N}_n} + \frac{1}{2} X_1 X_2^{\frac{n-1}{2}}.$$

Für gerades  $n$  gibt es in  $D_{2n} - C_n$  genau  $\frac{n}{2}$  Elemente mit je  $\frac{n}{2}$  2-Zykeln und genau  $\frac{n}{2}$  Elemente mit Zykeltyp  $(2, \frac{n-2}{2}, 0, \dots)$  (man überzeuge sich hiervon). Daher gilt in diesem Fall

$$Z_{D_{2n}, \mathbb{N}_n} = \frac{1}{2} Z_{C_n, \mathbb{N}_n} + \frac{1}{4} \left( X_2^{\frac{n}{2}} + X_1^2 X_2^{\frac{n-2}{2}} \right).$$

Zu (iii): Sei  $\underline{c} = (c_1, \dots, c_n)$  ein Zykeltyp zu  $n$ , d.h.  $\sum_{1 \leq i \leq n} i \cdot c_i = n$ . Es gilt

$$Z_{S_n, \mathbb{N}_n} = \frac{1}{n!} \sum_{\underline{c}} h(\underline{c}) X_1^{c_1} \cdots X_n^{c_n};$$

hierbei bezeichnet  $h(\underline{c})$  die Zahl der  $\sigma \in S_n$  mit  $c(\sigma) = \underline{c}$ , und nach 6.11 gilt

$$h(\underline{c}) = \frac{n!}{1^{c_1} \cdot c_1! \cdot 2^{c_2} \cdot c_2! \cdots n^{c_n} \cdot c_n!}.$$

Zu (iv): Man überlege sich dies zur Übung selbst (man beweise und verwende, daß eine Permutation  $\sigma$  genau dann gerade ist, wenn  $\sum c_{2j}$  eine gerade Zahl ist).

Unser Ziel ist die Berechnung von

$$Z_{S_k, \mathfrak{P}_2(\mathbb{N}_k)}(X_1, \dots, X_n) = \frac{1}{k!} \sum_{\sigma \in S_k} X_1^{d_1(\sigma)} \cdots X_n^{d_n(\sigma)}, \quad (*)$$

wobei  $n = \binom{k}{2}$  ist und  $d_i(\sigma)$  die Zahl der  $i$ -Zykeln von  $S_k$  auf  $\mathfrak{P}_2(\mathbb{N}_k)$  bezeichnet. Wir berechnen den Beitrag zu (\*) für festes  $\sigma \in S_k$  mit Zykeltyp  $\underline{c} = (c_1, \dots, c_k)$  auf  $\mathbb{N}_k$  und  $\{x, y\} \in \mathfrak{P}_2(\mathbb{N}_k)$  (also  $x, y \in \mathbb{N}_k$  und  $x \neq y$ ); dazu unterscheiden wir folgende Fälle:

(i)  $x, y$  liegen in Zykeln  $A, B$  der Längen  $a, b$  mit  $a \neq b$ ; o.B.d.A.  $a < b$ . Es gibt  $c_a$  (bzw.  $c_b$ ) viele mögliche Wahlen von  $A$  (bzw.  $B$ ). Die Menge  $\{\{x, y\} \mid x \in A, y \in B\}$  hat Ordnung  $ab$  und zerfällt unter der Operation von  $\langle \sigma \rangle$  in  $\frac{ab}{\text{kgV}(a,b)} = \text{ggT}(a, b)$  viele Bahnen der Ordnung  $\text{kgV}(a, b)$ . Denn  $\sigma^j \{x, y\} = \{x, y\}$  ist im vorliegenden Fall äquivalent zu

$\sigma^j(x) = x, \sigma^j(y) = y$ , und beides tritt gleichzeitig frühestens ein für  $j \equiv 0 \pmod{\text{kgV}(a, b)}$ . Der Beitrag solcher Zyklen zum Produkt im zu  $\sigma$  gehörenden Summanden von (\*) ist also

$$\prod_{1 \leq a < b \leq k} X_{\text{kgV}(a, b)}^{\text{ggT}(a, b) \cdot c_a \cdot c_b}.$$

(Diese Schreibweise verdient einen Kommentar: zwar kann  $\text{kgV}(a, b) > n$  sein; dies bereitet jedoch keine Probleme, denn man überlegt sich leicht, daß für solche Veränderliche mit zu großem Index der Exponent verschwindet.)

(ii)  $x, y$  liegen in verschiedenen Zykeln  $A, A'$  der gleichen Länge  $a$ . Die Menge  $\{\{x, y\} \mid x \in A, y \in A'\}$  der Ordnung  $a^2$  zerfällt unter der Operation von  $\langle \sigma \rangle$  in  $a$  Bahnen der Ordnung  $a$ ; der Beitrag zu (\*) ist

$$\prod_{1 \leq a \leq k} X_a^{a \cdot \binom{c_a}{2}}.$$

(iii)  $x, y$  liegen im gleichen Zykel  $A$  der Länge  $a$ . Hier kann nun  $\sigma^j\{x, y\} = \{x, y\}$  auch so eintreten, daß  $\sigma^j(x) = y$  und  $\sigma^j(y) = x$  sind. Wir unterscheiden zwei Fälle:

(iii a) Ist  $a$  *ungerade*, gilt immer noch, daß das Eintreten der Gleichheit  $\sigma^j\{x, y\} = \{x, y\}$  äquivalent ist zu  $\sigma^j(x) = x$  und  $\sigma^j(y) = y$ . Die Menge  $\{\{x, y\} \mid x, y \in A\}$  der Ordnung  $\binom{a}{2}$  zerfällt unter der Operation von  $\langle \sigma \rangle$  in  $\frac{a-1}{2}$  Bahnen der Ordnung  $a$ ; der Beitrag zu (\*) ist

$$\prod_{\substack{1 \leq a \leq k \\ a \equiv 1 \pmod{2}}} X_a^{\binom{a-1}{2} \cdot c_a}.$$

(iii b) Ist  $a$  *gerade* und gilt  $y = \sigma^j(x)$  mit  $1 \leq j \leq a, j \neq \frac{a}{2}$ , so hat immer noch  $\{x, y\}$  die Ordnung  $a$ ; die Menge  $\{x, \sigma^{\frac{a}{2}}(x)\}$  allerdings hat Ordnung  $\frac{a}{2}$  unter  $\sigma$ . Damit ist der Beitrag zu (\*)

$$\prod_{\substack{1 \leq a \leq k \\ a \equiv 0 \pmod{2}}} X_a^{\binom{a-2}{2} \cdot c_a} X_{\frac{a}{2}}^{c_a}.$$

Schreiben wir kurz  $Z_{S_k, \mathfrak{P}_2(\mathbb{N}_k)}(X_1, \dots, X_n) =: Z_k$ , so haben wir insgesamt erhalten:

**Satz 12.6.**

$$Z_k = \frac{1}{k!} \sum_{\underline{c}} h(\underline{c}) \prod_{1 \leq a < b \leq k} X_{\text{kgV}(a, b)}^{\text{ggT}(a, b) \cdot c_a \cdot c_b} \prod_{1 \leq a \leq k} X_a^{a \cdot \binom{c_a}{2}} \prod_{\substack{1 \leq a \leq k \\ a \equiv 1 \pmod{2}}} X_a^{\binom{a-1}{2} \cdot c_a} \prod_{\substack{1 \leq a \leq k \\ a \equiv 0 \pmod{2}}} X_a^{\binom{a-2}{2} \cdot c_a} X_{\frac{a}{2}}^{c_a}.$$

Dieser zunächst abschreckende Ausdruck ist noch einigermaßen gut auszuwerten, da ja die  $\underline{c}$  im Allgemeinen stark mit Nullen besetzt sind. Wir halten einige Beispiele fest:

**Beispiele 12.7.**

$$\begin{aligned} Z_2 &= \frac{1}{2}(2X_1) = X_1 ; \\ Z_3 &= \frac{1}{6}(X_1^3 + 3X_1X_2 + 2X_3) ; \\ Z_4 &= \frac{1}{24}(X_1^6 + 9X_1^2X_2^2 + 8X_3^2 + 6X_2X_4) . \end{aligned}$$

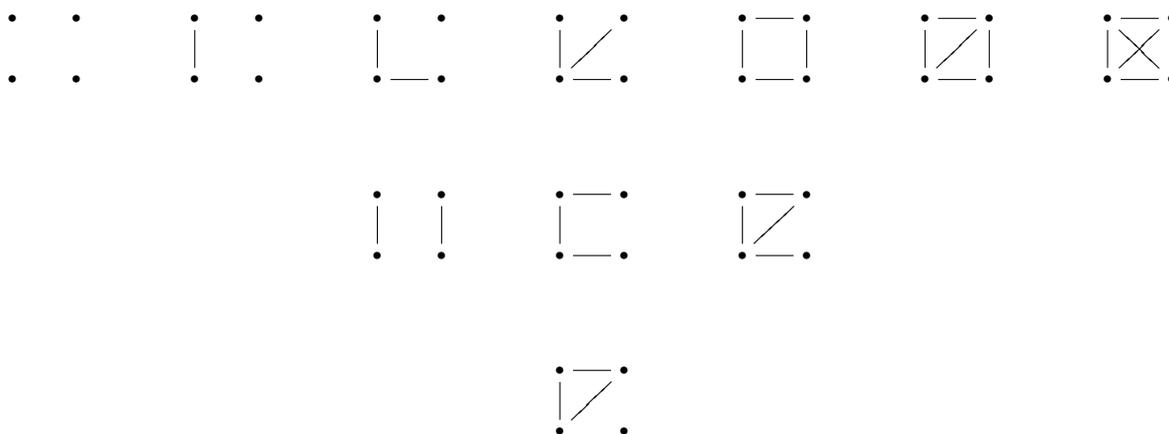
Doch Vorsicht: *im Allgemeinen* gibt es auch  $X_i$  mit  $i > k$ .

**Korollar 12.8.** Die Zahl der Isomorphieklassen von Graphen mit  $k$  Knoten und  $a$  Kanten ist der Koeffizient von  $Y_1^a Y_2^{\binom{k}{2}-a}$  in  $Z_k(Y_1 + Y_2, Y_1^2 + Y_2^2, \dots, Y_1^n + Y_2^n)$ , wobei  $n = \binom{k}{2}$ .

**Beispiel 12.9.** Für  $k = 4$  ist

$$Z_4(Y_1 + Y_2, \dots, Y_1^6 + Y_2^6) = Y_1^6 + Y_1^5 Y_2 + 2Y_1^4 Y_2^2 + 3Y_1^3 Y_2^3 + 2Y_1^2 Y_2^4 + Y_1 Y_2^5 + Y_2^6 ;$$

die 11 Isomorphieklassen haben folgende Gestalt:



**12.10. Tabelle** für die Anzahl  $i_k$  der Isomorphieklassen von Graphen mit  $k$  Knoten:

$k$	1	2	3	4	5	6	7	8	9	10
$i_k$	1	2	4	11	34	156	1044	12346	274668	12005168

Hierzu muß man *nicht* den Satz von Polya verwenden; es genügt, in  $Z_k$  jeweils für alle Veränderlichen den Wert 2 einzusetzen.

Polya entwickelte sein Abzählverfahren im Blick auf Probleme aus der Chemie: dort stellt sich häufig die Frage, wieviele verschiedene Arten von Molekülen einer bestimmten vorgegebenen Struktur es geben kann. Man kann diese Frage sehr vereinfacht auffassen als die Frage nach den verschiedenen Möglichkeiten, einen Graphen mit  $r$  Farben einzufärben. Dies soll am Beispiel des Würfels erläutert werden.

**12.11. Beschreibung der Würfelgruppe.** Welche räumlichen Transformationen führen den Würfel in sich über? Wir setzen

$$G := \{g \in \text{SO}(3) \mid g(W) = W\} \quad \text{und} \\ \tilde{G} := \{g \in \text{O}(3) \mid g(W) = W\},$$

wobei  $W$  den Würfel im euklidischen Raum  $\mathbb{R}^3$  mit Eckpunkten  $\{(\pm 1, \pm 1, \pm 1)\}$  bezeichnet. Wir halten einige Ergebnisse über die Struktur von  $G$  fest:

- Es gilt  $[\tilde{G} : G] = 2$ ; ferner gibt es eine Einbettung von  $G$  in  $\text{Sym}(\text{Knoten})$ .
- $G$  operiert transitiv auf den Mengen der Knoten, Kanten und Flächen von  $W$ .
- $|G| = 24$ ; genauer hat  $G$  folgende Elemente:

$3 \times 2 = 6$	Elemente der Ordnung	4	(Rotationen um die 3 Achsen durch gegenüberliegende Flächenmittelpunkte um $90^\circ$ bzw. $270^\circ$ )
$4 \times 2 = 8$	Elemente der Ordnung	3	(Rotationen um die 4 Raumdiagonalen um $120^\circ$ bzw. $240^\circ$ )
$3 \times 1 = 3$	Elemente der Ordnung	2	(Rotationen um die 3 Achsen durch gegenüberliegende Flächenmittelpunkte um $180^\circ$ )
$6 \times 1 = 6$	Elemente der Ordnung	2	(Rotationen um die 6 Achsen durch gegenüberliegende Kantenmittelpunkte um $180^\circ$ )
1	Element der Ordnung	1	(Identität)
- $G$  operiert treu (d.h. nichttriviale Elemente operieren in nichttriviale Weise) auf der Menge der Raumdiagonalen von  $W$ : der Homomorphismus  $G \rightarrow \text{Sym}(\text{Raumdiagonalen})$  ist injektiv. Wegen  $\text{Sym}(\text{Raumdiagonalen}) \cong S_4$  und  $|G| = |S_4| = 24$  gilt also sogar
- $G \cong S_4$ ; genauer haben die Elemente von  $G$  auf der Menge der Raumdiagonalen die folgende Zykelstruktur:

die Elemente der Ordnung	4	haben Zykelstruktur	$(abcd)$ ;
die Elemente der Ordnung	3	haben Zykelstruktur	$(abc)$ ;
die $3 \times 1$ Elemente der Ordnung	2	haben Zykelstruktur	$(ab)(cd)$

 (es handelt sich also um die nichttrivialen Elemente der Kleinschen Vierergruppe);

die $6 \times 1$ Elemente der Ordnung	2	haben Zykelstruktur	$(ab)$ ;
das Element der Ordnung	1	hat nur Fixpunkte .	

Insgesamt erhalten wir die 5 Konjugationsklassen der  $S_4$ .

Aus obigen Überlegungen erhält man die folgende Tabelle, die der Leser wenigstens zum Teil verifizieren sollte.

**12.12. Zykelstruktur von  $G$  auf Knoten, Kanten, Flächen.**

Zahl	Typ	Knoten	Kanten	Flächen
6	$(abcd)$	$(4, 4)$	$(4, 4, 4)$	$(1, 4, 1)$
8	$(abc)$	$(1, 3, 3, 1)$	$(3, 3, 3, 3)$	$(3, 3)$
3	$(ab)(cd)$	$(2, 2, 2, 2)$	$(2, 2, 2, 2, 2, 2)$	$(1, 2, 2, 1)$
6	$(ab)$	$(2, 2, 2, 2)$	$(1, 2, 2, 2, 2, 2, 1)$	$(2, 2, 2)$
1	id	$\underbrace{(1, \dots, 1)}_8$	$\underbrace{(1, \dots, 1)}_{12}$	$\underbrace{(1, \dots, 1)}_6$

**12.13. Zykelzeiger.** Bezeichnet wieder  $c_i = c_i(g)$  die Zahl der Zykel der Länge  $i$  unter der Operation von  $g \in G$  auf den Knoten, so gilt

$$\begin{aligned} Z_{G, \text{Knoten}} &= \frac{1}{24} \sum_{g \in G} X_1^{c_1} X_2^{c_2} X_3^{c_3} X_4^{c_4} \\ &= \frac{1}{24} (6X_4^2 + 8X_1^2 X_3^2 + 9X_2^4 + X_1^8) . \end{aligned}$$

Bezeichnet  $\underline{a}$  wie üblich ein Element  $(a_1, \dots, a_r)$  von  $\mathbb{N}_0^r$ , so liefert Einsetzen von  $\sum_{1 \leq j \leq r} Y_j^i$  für  $X_i$

$$\sum_{\underline{a}} k_{\underline{a}} Y_1^{a_1} \dots Y_r^{a_r} ,$$

wobei der Koeffizient  $k_{\underline{a}}$  die Zahl der Bahnen von  $G$  auf Knotenfärbungen mit  $a_1$  Knoten der Farbe  $1, \dots, a_r$  Knoten der Farbe  $r$  ist. Für  $r = 2$  ergibt sich zunächst

$$\frac{1}{24} [6(Y_1^4 + Y_2^4)^2 + \underbrace{8(Y_1 + Y_2)^2(Y_1^3 + Y_2^3)^2}_{(*)} + 9(Y_1^2 + Y_2^2)^4 + \underbrace{(Y_1 + Y_2)^8}_{(**)}] .$$

Ein vollständiges Auswerten dieses Ausdrucks wäre zwar möglich, aber mühsam. Relativ schnell kann man etwas über den Koeffizienten des  $Y_1^3 Y_2^5$ -Terms sagen: zu diesem können nur  $(*)$  und  $(**)$  beitragen; daher genügt es, diesen Koeffizienten zu berechnen für

$$\frac{1}{24} [8(Y_1^2 + 2Y_1 Y_2 + Y_2^2)(Y_1^6 + 2Y_1^3 Y_2^3 + Y_2^6) + \binom{8}{5} Y_1^3 Y_2^5] .$$

Doch auch hier können in dem noch auszuwertenden Produkt wieder nur bestimmte Faktoren beitragen; man hat insgesamt, daß der gesuchte Koeffizient

$$\frac{1}{24} \left( 16 + \binom{8}{5} \right) = 3$$

ist. Dies erlaubt uns nun, etwas über die Zahl der Isomorphieklassen bestimmter Färbungen zu sagen:

**12.14.** Die folgende Tabelle gibt Auskunft über die Zahl  $z_l$  der Isomorphieklassen von Rot-Grün-Färbungen mit  $l$  roten Knoten:

$l$	0	1	2	3	4	5	6	7	8
$z_l$	1	1	3	3	7	3	3	1	1

Hierbei sind die Einträge für  $0 \leq l \leq 2$  einfach zu ermitteln; den Wert für  $l = 3$  hatten wir in 12.13 ausgerechnet, und die Werte für  $5 \leq l \leq 8$  ergeben sich aus Symmetrieüberlegungen. Ferner ergibt sich durch Einsetzen von 2 in den Zykelzeiger eine Gesamtzahl von 23 Isomorphieklassen; für  $l = 4$  muß sich also 7 ergeben.

*Bemerkung:*

- (i) Man beschreibe zur Übung die 7 Konfigurationen für  $l = 4$ .
- (ii) Die  $G$ -Isomorphieklassen zu festem  $l$  fallen unter  $\tilde{G}$  entweder paarweise zusammen, oder sie sind auch schon  $\tilde{G}$ -Isomorphieklassen. Die erstgenannten sind "händig" (d.h. die Glieder eines Paares verhalten sich zueinander wie rechte und linke Hand), die zweitgenannten nicht. "Händigkeit" wird in der chemischen Beispielsituation sichtbar bei Hindurchschicken von polarisiertem Licht. Zwei Moleküle, die sich lediglich durch die Händigkeit unterscheiden, können gleichwohl sehr verschiedene Wirkungen auf den Stoffwechsel eines Organismus haben; so beruhte beispielsweise die katastrophale Nebenwirkung des Medikaments Contergan auf einer Verwechslung bei der Händigkeit eines Inhaltsstoffes.

## 13 Etwas algebraische Graphentheorie

Die algebraische Graphentheorie besteht darin, einem Graphen  $G = (V, E)$  Invarianten algebraischer Art zuzuordnen, z.B. Matrizen, Polynome, verschiedene abelsche oder nicht abelsche Gruppen. . . Diese Theorie ist sehr reichhaltig und kann hier nur angeschnitten werden; Ziel des Kapitels ist es, den Leser zu einem eigenständigen Studium eines Werks über algebraische Graphentheorie anzuleiten.

**Definition 13.1.** Seien  $|V| = n$  und  $|E| = m$  (es gilt also  $m \leq \binom{n}{2}$ ). Die Nachbarschaftsmatrix  $A$  von  $G$  ist die  $n \times n$ -Matrix  $A$ , deren Zeilen und Spalten durch  $V$  indiziert werden, mit

$$A = (a_{v,w})_{v,w \in V} \quad a_{v,w} := \begin{cases} 1 & \text{falls } v \neq w \text{ und } \{v, w\} \in E ; \\ 0 & \text{sonst.} \end{cases}$$

Das Spektrum  $\text{Spec}(G)$  von  $G$  ist die Multimenge der Eigenwerte von  $A$  mit Vielfachheiten. Das charakteristische Polynom  $P_G(X)$  von  $G$  ist das charakteristische Polynom von  $A$ , also das Polynom

$$\det(XI_n - A) = \prod_{1 \leq i \leq n} (X - \lambda_i),$$

wobei  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$  die der Größe nach geordneten Eigenwerte von  $A$  sind.

*Bemerkung:* Die Wahl des Buchstabens  $A$  rührt in diesem Fall von der englischen Bezeichnung *adjacency matrix* her.

Wir notieren einige triviale Beobachtungen über diese Matrix:

- (i)  $G$  ist vollständig bestimmt durch  $A$ ; es gibt einige Einschränkungen an  $A$ : die Einträge sind 0 oder 1, die Diagonalelemente sind 0, die Matrix ist symmetrisch.
- (ii) Demnach ist  $A$  diagonalisierbar über  $\mathbb{R}$  und hat reelle Eigenwerte.
- (iii) Zerfällt  $G$  in die  $k$  Zusammenhangskomponenten  $G_i = (V_i, E_i)$  mit Nachbarschaftsmatrizen  $A_i$ , so hat  $A$  eine Blockstruktur

$$\begin{array}{|c|c|c|c|c|} \hline & A_1 & & & 0 \\ \hline & & A_2 & & \\ \hline & & & \ddots & \\ \hline 0 & & & & A_k \\ \hline \end{array}$$

**Beispiele 13.2.** Wir geben die Nachbarschaftsmatrix für einige Graphen an:

$G$	$P_n$	$C_n$	$K_n$
$A$	$\begin{pmatrix} 0 & 1 & & & 0 \\ 1 & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ 0 & & & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 1 \\ 1 & 0 & 1 & & & 0 \\ 0 & 1 & & \ddots & & 0 \\ \vdots & & \ddots & \ddots & \ddots & 1 \\ 0 & & & & & 1 \\ 1 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & 0 & & \\ \vdots & & \ddots & \vdots \\ 1 & \dots & 1 & 0 \end{pmatrix}$

**Lemma 13.3.** Für  $l \in \mathbb{N}_0$  gelten:

- (i)  $(A^l)_{v,w}$  ist die Zahl der Wege in  $G$  der Länge  $l$  von  $v$  nach  $w$  ;
- (ii)  $\text{Tr}(A^l)$  ist die Zahl der geschlossenen Wege der Länge  $l$  in  $G$  .



**Satz 13.5.** Alle Eigenwerte  $\lambda_i$  von  $G$  sind betragslich  $\leq \sqrt{2m \frac{n-1}{n}}$ .

*Beweis.* (i) Sind  $a_1, \dots, a_k$  reelle Zahlen, so gilt die Abschätzung

$$\left( \sum_{1 \leq i \leq k} a_i \right)^2 \leq k \cdot \sum_{1 \leq i \leq k} a_i^2.$$

Schreibe nämlich  $a_i$  als  $m + b_i$  mit  $m := \frac{1}{k} \sum a_i$  (also als Summe aus Mittelwert und Abweichung). Dann ist die linke Seite der behaupteten Ungleichung  $k^2 m^2$  (die Abweichungen addieren sich zu 0 auf), und die rechte Seite ist

$$k \cdot \sum_{1 \leq i \leq k} (m^2 + 2b_i m + b_i^2) = k^2 m^2 + k \cdot \underbrace{\sum_{1 \leq i \leq k} b_i^2}_{\geq 0}.$$

(ii) Wegen  $\sum_{1 \leq i \leq n} \lambda_i = 0$  gilt für jeden Eigenwert  $\lambda_r$ :

$$\lambda_r = - \sum_{i \neq r} \lambda_i, \quad \text{also auch} \quad (\lambda_r)^2 = \left( \sum_{i \neq r} \lambda_i \right)^2 \stackrel{(i)}{\leq} (n-1) \cdot \sum_{i \neq r} \lambda_i^2.$$

Daraus ergibt sich

$$n \lambda_r^2 \leq (n-1) \cdot \sum_{1 \leq i \leq n} \lambda_i^2 \quad \text{bzw.} \quad \lambda_r^2 \leq \frac{n-1}{n} \cdot \sum_{1 \leq i \leq n} \lambda_i^2 = \frac{n-1}{n} \cdot \text{Tr}(A^2) = \frac{n-1}{n} 2m.$$

□

**Korollar 13.6.** Die Zahl der geschlossenen Wege der Länge  $l$  ist  $\leq n \left( 2m \frac{n-1}{n} \right)^{\frac{l}{2}}$ . □

*Bemerkungen:*

- (i) Die Abschätzung ist nicht gut, da ja nicht alle Eigenwerte der oberen Abschätzung aus Satz 13.5 nahekommen. Bessere Abschätzungen erhält man bei genauerer Kenntnis der Eigenwerte.
- (ii) Man kann sich bei Kenntnis von  $P_G(X)$  eine Rekursionsformel für  $\text{Tr}(A^l)$  verschaffen. Denn zunächst ist allgemein für  $A \in \text{Mat}(n, \mathbb{C})$  folgende Identität richtig:

$$\sum_{l \geq 1} \text{Tr}(A^l) X^l = X \frac{d}{dX} \log[\det(1 - XA)]^{-1}. \quad (*)$$

Um dies einzusehen, erinnere man sich, daß allgemein für eine formale Potenzreihe  $f(X)$  die Identität  $\frac{d}{dX} \log f(X) = \frac{f'(X)}{f(X)}$  gilt. Die Identität (\*) (wo also speziell

$f(X) = \det(1 - XA)$  gesetzt wird) beweist man dann durch Induktion über die Dimension  $n$ : Für  $n = 1$  sind die beteiligten Matrizen einfach Zahlen, und es steht letztlich eine geometrische Reihe da. Für den Induktionsschritt macht man sich zunutze, daß der Grundkörper algebraisch abgeschlossen ist: man kann dann die Matrizen trigonalisieren und so durch Entwicklung nach der letzten Zeile den Fall  $n$  auf den Fall  $n - 1$  zurückführen.

Setzt man noch  $f(X) =: \sum b_i X^i$  und bezeichnet die linke Seite von (\*) als  $g(X)$  mit Koeffizienten  $a_l := \text{Tr}(A^l)$ , so hat man

$$g(X) = -X \frac{f'(X)}{f(X)} \quad \text{bzw.} \quad g(X)f(X) = -Xf'(X),$$

also gemäß der Definition der Multiplikation von Potenzreihen

$$\sum_{i+j=k} a_i b_j = -k \cdot b_k;$$

die gesuchte Rekursionsformel schreibt sich also in der Form

$$a_k = -k \cdot b_k - \sum_{i < k} a_i b_{k-i}.$$

Hierbei genügt tatsächlich die Kenntnis von  $P_G(X)$ , denn es gilt

$$f(X) = (-1)^n P_G(X^{-1}) X^n.$$

**Proposition 13.7.** *Ein zusammenhängender Graph mit Durchmesser  $d$  hat mindestens  $d + 1$  verschiedene Eigenwerte.*

*Beweis.* Seien  $v, w \in V$  mit Abstand  $d$ , realisiert z.B. durch den Weg

$$v =: x_0, x_1, \dots, x_{d-1}, x_d := w.$$

Für jedes  $i$  mit  $1 \leq i \leq d$  gibt es einen Weg der Länge  $i$ , aber keinen kürzeren Weg, der  $v$  mit  $x_i$  verbindet. Also ist  $(A^i)_{v, x_i} > 0$ , aber  $(A^j)_{v, x_i} = 0$  für  $j < i$ . Daher sind die  $d + 1$  Matrizen  $A^0, A^1, \dots, A^d$  linear unabhängig.

Ist andererseits  $s$  die Zahl der verschiedenen Eigenwerte von  $A$ , so hat, weil  $A$  diagonalisierbar ist, das Minimalpolynom  $M_A(X)$  den Grad  $s$ ; es muß also gelten  $s \geq d + 1$ .  $\square$

**Beispiel 13.8.** Sei  $G = K_n$ , also  $m = \binom{n}{2}$ . Dann ist

$$A = J - I_n \quad \text{mit} \quad J = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$$

Es ist  $P_J(X) = X^{n-1}(X - n)$ , also

$$P_A(X) = P_J(X + 1) = (X + 1)^{n-1}(X + 1 - n)$$

und  $\text{Spec}(G) = \text{Spec}(A) = \{-1, \dots, -1, n - 1\}$ , wobei der Eigenwert  $-1$  mit Vielfachheit  $n - 1$  vorkommt. Damit ist für  $K_n$  die Schranke von 13.7 scharf, ebenso die Schranke von 13.5. Die Zahl der geschlossenen Wege der Länge  $l$  in  $K_n$  ist  $(n - 1)(-1)^l + (n - 1)^l$ .

**Definition 13.9.** Sei  $G = (V, E)$  ein mit einer Orientierung versehener Graph mit  $|V| = n$  und  $|E| = m$ . Zu  $e \in E$  bezeichne  $o(e)$  den Anfangspunkt,  $t(e)$  den Endpunkt von  $e$  bezüglich der gewählten Orientierung, und  $\bar{e}$  bezeichne die gegenläufig orientierte Kante. Die Inzidenzmatrix von  $G$  (bezüglich der gewählten Orientierung) ist die folgende  $n \times m$ -Matrix:

$$D = (d_{v,e})_{\substack{v \in V \\ e \in E}} \quad \text{mit} \quad d_{v,e} = \begin{cases} -1, & \text{falls } v = o(e) ; \\ 1, & \text{falls } v = t(e) ; \\ 0 & \text{sonst.} \end{cases}$$

Weiter sei  $Z$  die  $n \times n$ -Diagonalmatrix

$$Z = (z_{v,w})_{v,w \in V} \quad \text{mit} \quad z_{v,w} = \begin{cases} 0, & \text{falls } v \neq w ; \\ d(v), & \text{falls } v = w . \end{cases}$$

**Lemma 13.10.**  $Q := DD^t = Z - A$ .

*Beweis.*

$$(DD^t)_{v,w} = \sum_{e \in E} d_{v,e} \underbrace{d_{e,w}^t}_{d_{w,e}} = \begin{cases} -1, & \text{falls } v, w \text{ benachbart und verschieden ;} \\ 0, & \text{falls } v, w \text{ verschieden und nicht benachbart ;} \\ d(v) & \text{falls } v = w . \end{cases}$$

□

**Proposition 13.11.** Der Rang von  $D$  ist  $n$  abzüglich der Zahl der Zusammenhangskomponenten von  $G$ .

*Beweis.* (i) Lässt sich  $G = \dot{\bigcup} G_i$  in die Zusammenhangskomponenten  $G_i = (V_i, E_i)$  mit Inzidenzmatrizen  $D_i$  zerlegen, so hat  $D$  Blockstruktur

$$\begin{array}{|ccc|} \hline D_1 & & 0 \\ \hline & D_2 & \\ \hline & & \ddots \\ \hline 0 & & D_k \\ \hline \end{array} ;$$

der Rang von  $D$  ergibt sich also als die Summe der Ränge der Blöcke. Daher kann man o.B.d.A. annehmen,  $G$  sei zusammenhängend.

(ii) Da alle Spaltensummen von  $D$  gleich 0 sind, ist  $\text{rg}(D) \leq n-1$ . Daher gibt es, wenn  $\underline{d}_v$  den  $v$ -ten Zeilenvektor von  $D$  bezeichnet, eine Linearkombination der Zeilenvektoren der Form

$$\sum_{v \in V} a_v \underline{d}_v = 0, \quad (*)$$

wobei nicht alle  $a_v$  gleich 0 sind. Wähle ein von 0 verschiedenes  $a_v$ ; es muß dann  $\underline{d}_v$  einen Eintrag  $d_{v,e} \neq 0$  haben — es gibt also eine Kante  $e$ , so daß  $v$  und  $e$  inzident sind (d.h. so daß  $v \in e$ ). Für jedes derartige  $e$  existiert genau ein  $w \neq v$  mit  $d_{w,e} \neq 0$ , und es ist  $d_{v,e} + d_{w,e} = 0$ . Damit (\*) gelten kann, muß also  $a_v = a_w$  sein. Da  $G$  zusammenhängend ist, müssen demnach sämtliche Koeffizienten von (\*) gleich sein, d.h. (\*) ist Vielfaches von  $\sum_{v \in V} \underline{d}_v$ , und damit muß auch schon diese Summe gleich 0 gewesen sein. Dies heißt aber  $\text{rg}(D) = n - 1$ .  $\square$

**Proposition 13.12.** *Sei  $D$  die Inzidenzmatrix eines zusammenhängenden Graphen. Dann gelten:*

- (i) *Jede quadratische Teilmatrix  $S$  von  $D$  hat Determinante  $\det S \in \{0, -1, 1\}$ .*
- (ii) *Seien  $F \subset E$  mit  $|F| = n - 1$  und  $G_F = (V, F)$  mit Inzidenzmatrix  $D_F$ , und sei  $D'_F$  eine beliebige quadratische  $(n-1) \times (n-1)$ -Teilmatrix von  $D_F$ . Dann ist  $\det D'_F \neq 0$  genau dann, wenn  $G_F$  maximaler Unterbaum ist.*

*Beweis.* Zu (i): Stehen in jeder Spalte von  $S$  eine 1 und eine -1, so sind alle Spaltensummen 0 und damit  $\det S = 0$ . Ist also  $\det S \neq 0$ , so gibt es mindestens eine Spalte, in der genau ein Eintrag von 0 verschieden ist, und dieser ist  $\pm 1$ . Man kann die Matrix nach dieser Spalte entwickeln und entsprechend fortfahren; insgesamt ergibt sich, daß in jeder Spalte von  $S$  genau ein von 0 verschiedener Eintrag der Form  $\pm 1$  steht;  $S$  ist also bis auf ein Vorzeichen eine Permutationsmatrix.

Zu (ii): Es ist  $\text{rg}(D'_F) = \text{rg}(D_F)$ ; ist dieser Rang  $n - 1$ , so ist dies gemäß 13.11 äquivalent dazu, daß  $G_F$  zusammenhängend ist, was aufgrund der Kardinalität von  $F$  nur so möglich ist, daß  $G_F$  maximaler Unterbaum ist.  $\square$

Im folgenden sei die *Begleitmatrix*  $\tilde{A}$  einer Matrix  $A$  die Matrix  $(\tilde{a}_{ij})$  mit Einträgen  $\tilde{a}_{ij} := (-1)^{i+j} \det(A_{ji})$ , wobei  $A_{ji}$  die  $(ji)$ -te Streichungsmatrix von  $A$  bezeichnet. Es gilt  $A\tilde{A} = \tilde{A}A = (\det A) \cdot I_n$ .

**Definition/Satz 13.13.** *Die Komplexität  $\kappa(G)$  eines Graphen  $G = (V, E)$  ist die Zahl seiner maximalen Unterbäume.*

*Wähle eine Orientierung auf  $G$ ; für die Matrix  $Q = DD^t$  mit Begleitmatrix  $\tilde{Q}$  gilt*

$$\tilde{Q} = \kappa(G) \cdot J \quad \text{mit} \quad J = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} \in \text{Mat}(n, \mathbb{Q}).$$

*Beweis.* (i) Wir zeigen zunächst, daß  $\tilde{Q}$  ein Vielfaches von  $J$  ist. Ist nämlich  $G$  nicht zusammenhängend, so gilt  $\text{Rang}(Q) = \text{Rang}(D) < n - 1$ , also  $\tilde{Q} = 0$ ; ist  $G$  zusammenhängend, so gilt  $\text{Rang}(Q) = \text{Rang}(D) = n - 1$ . Wegen  $Q \cdot \tilde{Q} = (\det Q) \cdot I_n = 0$  gehört jede Spalte von  $\tilde{Q}$  zum Kern von  $Q$ . Aber dieser Kern ist der 1-dimensionale Vektorraum, der

von  $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$  erzeugt wird; deshalb sind alle Spalten von  $\tilde{Q}$  Vielfache dieses Vektors. Da  $Q$

symmetrisch ist, ist dies auch  $\tilde{Q}$ ; also sind die Multiplikatoren alle gleich, und  $\tilde{Q}$  ist wie behauptet ein Vielfaches von  $J$ .

(ii) Es genügt also, einen Eintrag von  $\tilde{Q}$  zu bestimmen, z.B.  $\tilde{q}_{v,v}$ . Sei  $D_v$  die Matrix, die aus  $D$  durch Streichen der  $v$ -ten Zeile entsteht, und  $Q_{v,v}$  die Matrix, die aus  $Q$  durch Streichen der  $v$ -ten Zeile und Spalte entsteht. Dann ist  $D_v D_v^t = Q_{v,v} \in \text{Mat}(n - 1, \mathbb{Q})$  und  $\det(D_v D_v^t) = \tilde{q}_{v,v}$ .

(iii) Wir erinnern an die *Formel von Cauchy-Binet* über die Determinante des Produkts zweier Rechtecksmatrizen: Hat  $A$  (bzw.  $B$ ) genau  $n - 1$  Zeilen (bzw. Spalten) und  $m$  Spalten (bzw. Zeilen), so ist

$$\det AB = \sum \det(A'B') ,$$

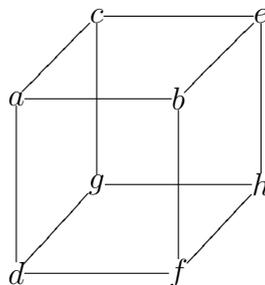
wobei rechts über alle Wahlen von quadratischen  $(n - 1) \times (n - 1)$ - Teilmatrizen  $A'$  von  $A$  und  $B'$  von  $B$ , so daß  $A'$  und  $B'$  "dieselben Indizes" haben, summiert wird; dies ergibt eine Zahl von  $\binom{m}{n-1}$  Summanden.

Deshalb gilt

$$\det(D_v D_v^t) = \sum_{\substack{F \subset E \\ |F|=n-1}} \det(D'_F) \det(D_F^t) ; \quad (*)$$

hierbei entsteht  $D'_F$  aus  $D$  durch Streichen der  $v$ -ten Zeile und aller Spalten zu  $e \notin F$ . Die Determinante von  $D'_F$  ist genau dann von Null verschieden, wenn  $G_F$  mit den Bezeichnungen wie in 13.12 maximaler Unterbaum ist; in diesem Fall ist  $\det(D'_F) = \pm 1$ . Deshalb trägt jeder maximale Unterbaum genau 1 zu (\*) bei, andere  $F \subset E$  nichts.  $\square$

**Beispiel 13.14.** Der Würfelgraph  $W$ .



In diesem Fall ist



- Es ist  $\dim C_0 = n$  und  $\dim C_1 = m$ ; Basen sind gegeben durch

$$\begin{aligned} & \{f_v \mid v \in V\} \quad \text{mit} \quad f_v(w) = \delta_{v,w} \quad \text{für } C_0 \text{ und} \\ & \{g_e \mid e \in E^+\} \quad \text{mit} \quad g_e(e') = \begin{cases} 1, & \text{falls } e' = e; \\ -1, & \text{falls } e' = \bar{e}; \\ 0 & \text{sonst} \end{cases} \quad \text{für } C_1. \end{aligned}$$

- $C_0$  und  $C_1$  sind versehen mit den Standardskalarprodukten  $(\cdot, \cdot)$ , bezüglich derer die  $\{f_v\}$  bzw.  $\{g_e\}$  Orthonormalbasen sind. Es gelten

$$\begin{aligned} (f_1, f_2) &= \sum_{v \in V} f_1(v) f_2(v); \\ (g_1, g_2) &= \frac{1}{2} \sum_{e \in E^\pm} g_1(e) g_2(e) = \sum_{e \in E^+} g_1(e) g_2(e). \end{aligned}$$

Wir definieren  $\delta : C_0 \rightarrow C_1$  durch  $\delta f(e) = f(t(e)) - f(o(e))$  und adjungiert hierzu  $\partial : C_1 \rightarrow C_0$  durch

$$\partial g(v) = \sum_{\substack{e \in E^\pm \\ t(e)=v}} g(e).$$

Bezüglich unserer Basen ist  $\partial$  durch die Inzidenzmatrix  $D$  und  $\delta$  durch  $D^t$  gegeben. Wir setzen weiter

$$\Delta_0 := \partial\delta : C_0 \rightarrow C_0, \quad \Delta_1 := \delta\partial : C_1 \rightarrow C_1;$$

dies sind die Laplace-Operatoren.  $\Delta_0$  ist gegeben durch  $Q = DD^t = Z - A$ . Es gelten

$$\begin{aligned} (\Delta_0 f)(v) &:= d(v)f(v) - \sum_{\substack{w \in V \\ \text{benachbart zu } v}} f(w); \\ (\Delta_1 g)(e) &:= 2g(e) - \sum_{\substack{e' \in E^\pm \\ o(e')=t(e)}} g(e') - \sum_{\substack{e'' \in E^\pm \\ t(e'')=o(e)}} g(e''). \end{aligned}$$

Wir haben die *orthogonalen* Zerlegungen

**Proposition 13.16.**

$$\begin{aligned} C_0 &= \text{Ker}(\Delta_0) \oplus \text{Bild } \partial, \quad \text{wobei } \text{Ker}(\Delta_0) = \text{Ker } \delta, & \text{(i)} \\ C_1 &= \text{Ker}(\Delta_1) \oplus \text{Bild } \delta \quad \text{wobei } \text{Ker}(\Delta_1) = \text{Ker } \partial. & \text{(ii)} \end{aligned}$$

Die Elemente von  $\text{Ker}(\Delta_0)$  bzw.  $\text{Ker}(\Delta_1)$  heißen harmonisch.

*Beweis.* Zu (i): Für  $x \in \text{Ker}(\Delta_0)$  ist  $0 = (\Delta_0 x, x) = (\partial \delta x, x) = (\delta x, \delta x)$ ; es ergibt sich  $\delta x = 0$ , also  $\text{Ker}(\Delta_0) \subset \text{Ker} \delta$ , also Gleichheit  $\text{Ker}(\Delta_0) = \text{Ker} \delta$ . Die Behauptung folgt, weil grundsätzlich gilt:

$$\text{Ker} \delta = \text{Bild}(\partial)^\perp ,$$

da  $\delta$  und  $\partial$  adjungiert sind. Ausführlich:

$$\begin{aligned} x \in \text{Ker} \delta &\Leftrightarrow \delta(x) = 0 \\ &\Leftrightarrow (\delta x, y) = (x, \partial y) = 0 \quad \forall y \in C_1 \\ &\Leftrightarrow x \perp \partial y \quad \forall y \in C_1 . \end{aligned}$$

Zu (ii): ebenso. □

**Bemerkung 13.17.** (i)  $f \in C_0$  ist genau dann harmonisch, wenn  $\Delta_0 f = 0$ , und dies ist äquivalent zu folgender *Mittelwerteigenschaft*:

$$\forall v \in V : \quad d(v)f(v) = \sum_{\substack{w \in V \\ \text{benachbart zu } v}} f(w)$$

$f$  ist also genau dann harmonisch, wenn es konstant auf Zusammenhangskomponenten ist.

(ii)  $g \in C_1$  ist genau dann harmonisch, wenn  $\Delta_1 g = 0$ , und dies ist äquivalent zu  $\partial g = 0$  bzw. zum Bestehen folgender Aussage:

$$\forall v \in V : \quad \sum_{\substack{e \in E^\pm \\ t(e)=v}} g(e) = 0$$

bzw. der entsprechenden Aussage, wo über die  $e$  mit  $o(e) = v$  summiert wird. Wir können also die Elemente von  $\text{Ker} \Delta_1$  als Flüsse interpretieren; die Harmonizitätsbedingung besagt: Flüsse haben keine Quellen und Senken.

**Proposition 13.18.** Sei  $c$  die Anzahl der Zusammenhangskomponenten von  $G$ . Dann gelten

$$\dim \text{Bild} \partial = n - c = \dim \text{Bild} \delta ; \tag{i}$$

$$\dim \text{Ker} \Delta_0 = c ; \tag{ii}$$

$$\dim \text{Ker} \Delta_1 = m - n + c . \tag{iii}$$

*Beweis.* Zum Beweis von (i) stellt man fest, daß  $\text{Rang}(D) = \text{Rang}(D^t) = n - c$ . (ii) und (iii) beweist man durch Abzählen; speziell gilt  $\dim \text{Ker} \Delta_1 = \dim C_1 - \dim \text{Bild} \delta = m - n + c$ . □

Vor der nächsten Definition erinnern wir an den Begriff des Gitters.  $\Gamma \subset W$  heißt *Gitter* in  $W \cong \mathbb{R}^k$  genau dann, wenn  $\Gamma$  eine Untergruppe mit zwei der drei folgenden Eigenschaften ist:

- $$\begin{aligned} \Gamma &\cong \mathbb{Z}^k ; & \text{(i)} \\ W/\Gamma &\text{ ist kompakt ;} & \text{(ii)} \\ \Gamma &\text{ ist in } W \text{ diskret enthalten .} & \text{(iii)} \end{aligned}$$

Äquivalent dazu ist:  $\Gamma$  ist  $\mathbb{Z}$ -Spann einer  $\mathbb{R}$ -Basis von  $W$ .

**Definition 13.19.** *Wir setzen:*

$$\begin{aligned} H(G, \mathbb{R}) &:= \text{Ker } \Delta_1 \quad (\text{die } \mathbb{R}\text{-wertigen Flüsse) ;} \\ H(G, \mathbb{Z}) &:= \text{Ker } \Delta_1 \cap C_0(G, \mathbb{Z}) \quad (\text{die } \mathbb{Z}\text{-wertigen Flüsse}) \end{aligned}$$

( $H(G, \mathbb{Z})$  bildet ein Gitter in  $H(G, \mathbb{R})$ ). Ferner setzen wir

$$\begin{aligned} L(G, \mathbb{R}) &:= \text{Bild } \delta ; \\ L(G, \mathbb{Z}) &:= \text{Bild } \delta \cap C_0(G, \mathbb{Z}) . \end{aligned}$$

Sei jetzt  $G$  zusammenhängend (d.h.  $c = 1$ ) und  $T \subset G$  ein maximaler Unterbaum ( $T$  hat  $n - 1$  Kanten). Sei  $e \in E^\pm(G) - E^\pm(T)$ . Dann existiert ein wohlbestimmter reduzierter Weg  $\gamma = \gamma_{T,e}$  durch  $T$  und  $e$  mit  $A(\gamma) = o(e) = E(\gamma)$ . Sei  $\phi_e \in C_1(G, \mathbb{Z})$  definiert durch

$$\phi_e(e') = \begin{cases} 1, & \text{falls } e' \text{ zu } \gamma \text{ gehört mit gleicher Orientierung wie } e ; \\ -1, & \text{falls } e' \text{ zu } \gamma \text{ gehört mit gegenüber } e \text{ inverser Orientierung ;} \\ 0 & \text{sonst.} \end{cases}$$

Jedes  $e \in E^\pm(T)$  definiert eine disjunkte Zerlegung  $V = V_{o,e} \dot{\cup} V_{t,e}$ , nämlich:

$$\begin{aligned} V_{o,e} &= \{w \in V \mid \text{der reduzierte Weg in } T \text{ von } w \text{ nach } e \text{ trifft } o(e)\}, \\ V_{t,e} &= \{w \in V \mid \text{der reduzierte Weg in } T \text{ von } w \text{ nach } e \text{ trifft } t(e)\}. \end{aligned}$$

Für ein  $e \in E^\pm(T)$  sei  $\psi_e$  das Element aus  $C_1(G, \mathbb{Z})$  mit

$$\psi_e(e') = \begin{cases} 1, & e' \text{ läuft von } V_{o,e} \text{ nach } V_{t,e}; \\ -1, & e' \text{ läuft von } V_{t,e} \text{ nach } V_{o,e}; \\ 0, & \text{sonst.} \end{cases}$$

Dann gelten:

**Satz 13.20.** (i)  $\phi_e \in H(G, \mathbb{Z})$ ,  $\psi_e \in L(G, \mathbb{Z})$  .

(ii)  $\{\phi_e \mid e \in E^+(G) - E^+(T)\}$  ist  $\mathbb{Z}$ -Basis von  $H(G, \mathbb{Z})$ , also auch  $\mathbb{R}$ -Basis von  $H(G, \mathbb{R})$  — d.h.  $H(G, \mathbb{Z})$  bzw.  $H(G, \mathbb{R})$  sind  $\mathbb{Z}$ - bzw.  $\mathbb{R}$ -Spann der Zykel in  $G$ . Daher wird  $H$  auch als Zykelraum bezeichnet.

(iii)  $\{\psi_e \mid e \in E^+(T)\}$  ist  $\mathbb{Z}$ -Basis von  $L(G, \mathbb{Z})$ ; man spricht vom Schnittraum.

*Beweis.* (i)  $\phi_e \in H(G, \mathbb{Z})$  ist offensichtlich. Für  $e \in E^\pm(T)$  gilt:  $\psi_e \in L(G, \mathbb{Z}) \Leftrightarrow \psi_e \perp g$  für alle  $g \in H(G, \mathbb{R})$ . Sei also  $g \in H(G, \mathbb{R})$ . Es ist

$$\begin{aligned} (\psi_e, g) &= \sum_{e' \in E^\pm(T)} \psi_e(e')g(e') \\ &= \sum_{\substack{e' \in E^+(T), \\ e' \text{ von } V_{o,e} \text{ nach } V_{t,e}}} g(e') - \sum_{\substack{e' \in E^+(T), \\ e' \text{ von } V_{t,e} \text{ nach } V_{o,e}}} g(e') \\ &= \text{Gesamtfluß unter } g \text{ von } V_{o,e} \text{ nach } V_{t,e} \\ &= 0, \text{ da } g \text{ keine Quellen und Senken besitzt.} \end{aligned}$$

(ii) Es ist klar, daß die  $m - n + 1$  betrachteten Abbildungen  $\phi_e$  linear unabhängig sind. Deshalb ist  $\{\phi_e \mid e \in E^+(G) - E^+(T)\}$  jedenfalls eine Basis über  $\mathbb{Q}$ . Sei  $\phi \in H(G, \mathbb{Z})$ . Dann gilt für  $\chi := \phi - \sum_{e \in E^+(G) - E^+(T)} \phi(e)\phi_e$ : Es ist  $\chi \in H(G, \mathbb{Z})$  und  $\chi(e) = 0$  für  $e \in E^+(G) - E^+(T)$ . Also ist  $\chi$  ein Fluß mit Träger in  $T$ , d.h.  $\chi = 0$  und damit gilt  $\phi = \sum_{e \in E^+(G) - E^+(T)} \phi(e)\phi_e$ .

(iii) Entsprechend gilt für  $\psi \in L(G, \mathbb{Z})$ :  $\chi := \psi - \sum_{e \in E^+(T)} \psi(e)\psi_e$  verschwindet auf  $E^+(T)$  und damit überall (da  $\chi = \delta f, \chi(e) = f(t(e)) - f(o(e))$  für ein  $f \in C_0(G, \mathbb{R})$ ).  $\square$

Die Gitter  $H := H(G, \mathbb{Z})$  bzw.  $L := L(G, \mathbb{Z})$  haben die Eigenschaft, daß  $(H, H) \subset \mathbb{Z}$  bzw.  $(L, L) \subset \mathbb{Z}$  gilt. Also liegt  $H$  in  $H^* := \{x \in H(G, \mathbb{R}) \mid (x, H) \in \mathbb{Z}\}$  und  $L$  im entsprechend definierten  $L^*$ . Hierbei sind  $H^*$  und  $L^*$  ebenfalls Gitter; nach Wahl einer Basis von  $H$ , auf der  $(\ , \ )$  durch eine Matrix  $B$  gegeben ist, ist  $B^{-1}$  die Matrix des Basiswechsels von  $H$  nach  $H^*$ . Sei  $C_0^0 := \{f \in C_0 \mid \sum_{v \in V} f(v) = 0\}$ .

**Satz 13.21.** (i) Die drei abelschen Gruppen  $H^*/H$ ,  $L^*/L$  und  $C_0^0(\mathbb{Z})/\Delta_0(C_0(\mathbb{Z}))$  sind alle kanonisch isomorph;

(ii) ihre gemeinsame Kardinalität ist  $\kappa(G)$ .

*Zum Beweis:* Da  $\Delta_0$  bzgl. der Basis  $\{f_v \mid v \in V\}$  durch die Matrix  $Q = DD^t$  gegeben ist, folgt

$$\kappa(G) = [C_0^0 : \Delta_0(C_0(G, \mathbb{Z}))]$$

aus 13.13 und elementarer Matrizenrechnung. Es bleibt also, die kanonische Isomorphie der drei Gruppen  $H^*/H, L^*/L$  und  $C_0^0/\Delta_0(C_0(G, \mathbb{Z}))$  zu zeigen, wofür wir ein paar Vorbereitungen brauchen.

**Lemma 13.22.** *Es sei  $W$  eine endlich erzeugte freie abelsche Gruppe mit einem unimodularen  $\mathbb{Z}$ -wertigen Skalarprodukt  $\langle \cdot, \cdot \rangle$ , d.h.*

$$\langle \cdot, \cdot \rangle : W \times W \rightarrow \mathbb{Z}$$

*ist bilinear, symmetrisch, positiv definit mit Determinante 1 bzgl. einer  $\mathbb{Z}$ -Basis von  $W$ . Seien  $U, V$  direkte Summanden von  $W$  mit  $U^\perp = V, V^\perp = U$ . Mit  $U^* = \text{Hom}(U, \mathbb{Z}), V^* = \text{Hom}(V, \mathbb{Z})$  und den durch  $\langle \cdot, \cdot \rangle$  induzierten Einbettungen  $U \hookrightarrow U^*$  und  $V \hookrightarrow V^*$  gilt*

$$V^*/V \xleftarrow{\cong} W/(U+V) \xrightarrow{\cong} U^*/U.$$

*Beweis.* Die Abbildung  $W \rightarrow U^*, x \mapsto \langle \cdot, x \rangle$  ist surjektiv, da  $\langle \cdot, \cdot \rangle$  unimodular und  $U$  direkter Summand ist. Der Kern davon ist  $U^\perp = V$ , der Kern von  $W \rightarrow U^* \rightarrow U^*/U$  ist  $U+V$ . Entsprechendes gilt bei Vertauschung der Rollen von  $U$  und  $V$ .  $\square$

**Bemerkung 13.23.** Entgegen der Intuition gilt trotz  $U+V = U \oplus V$  i.a. nicht, daß  $U+V = W$  ist. Die Größe der (endlichen) Gruppe  $W/(U+V)$  ist ein Maß dafür, wie “schräg”  $U$  und  $V$  in  $W$  liegen, wie das nachfolgende Beispiel zeigt:  $W = \mathbb{Z}^2$  mit dem Standardskalarprodukt,  $U = \mathbb{Z} \cdot (1, 1), V = \mathbb{Z} \cdot (1, -1)$ . Hier ist  $U+V = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv b \pmod{2}\}$ .

*Beweis von 13.21.* Setze  $H, L, C_0, C_1, C_0^0$  für die auftretenden freien abelschen Gruppen und  $H(\mathbb{R}), \dots, C_0^0(\mathbb{R})$  für die zugehörigen  $\mathbb{R}$ -Vektorräume.

(i) Es ist  $C_0^0 = \partial(C_1)$ . Die Inklusion  $\partial(C_1) \subset C_0^0$  ist trivial. Offenbar ist  $C_0^0$  erzeugt von Vektoren  $f = (0, \dots, 0, -1, 0, \dots, 0, +1, 0, \dots, 0)$ , wobei die Einträge  $-1, +1$  an zwei Knoten  $v, w \in V$  auftreten und alle anderen Einträge verschwinden. Ist  $v = x_0, x_1, \dots, x_k = w$  ein Weg von  $v$  nach  $w$ ,  $e_i = (x_{i-1}, x_i)$ , so ist  $f = \sum_{1 \leq i \leq k} \partial(g_{e_i})$ , also auch  $C_0^0 \subset \partial(C_1)$ .

(ii) In  $C_1$  ist  $L = H^\perp = \delta(C_0)$ . Dabei ist die erste Gleichung klar. Nach (13.16) ist  $\delta(C_0^0) \subset H^\perp = L$ . Nach 13.20 wird  $L$  von den  $\psi_e$  mit  $e \in E^+(T)$  erzeugt. Also reicht es zu zeigen:  $\psi_e$  liegt in  $\delta(C_0^0)$ . Mit den Bezeichnungen von 13.20 sei  $f = \sum_{v \in V_{t,e}} f_v$ . Für ein  $e' \in E^\pm(G)$  ist

$$\begin{aligned} (\delta f)(e') &= \sum_{v \in V_{t,e}} \delta f_v(e') \\ &= \sum_{v \in V_{t,e}} \left\{ \begin{array}{l} 1, v = t(e') \\ -1, v = o(e') \\ 0, \text{sonst} \end{array} \right\} \\ &= \left\{ \begin{array}{l} 1, t(e') \in V_{t,e}, o(e') \notin V_{t,e} \\ -1, o(e') \in V_{t,e}, t(e') \notin V_{t,e} \\ 0, \text{sonst} \end{array} \right\} \\ &= \psi_e(e'). \end{aligned}$$

Also ist  $\psi_e = \delta f$ .

(iii) Wir haben die folgenden kanonischen Isomorphismen:

$$\begin{aligned}
 C_0^0 / \Delta_0(C_0) & \stackrel{(i)}{=} \partial(C_1) / \Delta_0(C_0) = \partial(C_1) / \partial\delta(C_0) \\
 \stackrel{(ii)}{=} \partial(C_1) / \partial(H^\perp) & \stackrel{\cong}{\leftarrow} C_1 / H / (H^\perp + H) / H \stackrel{\cong}{\rightarrow} C_1 / (H^\perp + H) \\
 & = C_1 / (L + H),
 \end{aligned}$$

bewirkt durch den Epimorphismus  $\partial : C_1 \rightarrow C_0^0$  mit Kern  $H$ . Setzen wir  $W := C_1, U := H, V := H^\perp = L$ , so ist

$$\begin{aligned}
 H^* = \{x \in H(\mathbb{R}) \mid (x, H) \subset \mathbb{Z}\} & \stackrel{\cong}{\rightarrow} \text{Hom}(H, \mathbb{Z}) \\
 x & \mapsto (x, \cdot)
 \end{aligned}$$

und entsprechend  $L^* \stackrel{\cong}{\rightarrow} \text{Hom}(L, \mathbb{Z})$ , und 13.22 liefert

$$L^* / L \stackrel{\cong}{\leftarrow} C_1 / (H + L) \stackrel{\cong}{\rightarrow} H^* / H.$$

□

Aus Eigenschaften der Gitter  $H, H^*, L, L^*, \dots$  kann man jetzt Eigenschaften von  $G$  ablesen. Die Untersuchung solcher Gitter und die Wechselwirkung ihrer “arithmetischen” Eigenschaften mit den “geometrischen” Eigenschaften von  $G$  ist Gegenstand der aktuellen Forschung.