

**Skriptum**  
**zur Vorlesung**  
**Mathematik: Diskrete Strukturen**

*gehalten im Sommersemester 2018*

*von*

*Sven Kosub*

**19. Juli 2018**

*Version 7.17*

---



---

# Inhaltsverzeichnis

---

<b>1</b>	<b>Kombinatorik</b>	<b>1</b>
1.1	Einfache Urnenmodelle . . . . .	1
1.2	Kombinatorisches Beweisen . . . . .	4
1.2.1	Grundregeln des Abzählens . . . . .	4
1.2.2	Doppeltes Abzählen . . . . .	7
1.2.3	Das Inklusion-Exklusions-Prinzip . . . . .	8
1.2.4	Der Schubfachschluss . . . . .	10
1.3	Abzählprobleme . . . . .	12
1.3.1	Kombinationen und Binomialkoeffizienten . . . . .	12
1.3.2	Permutationen und Stirling-Zahlen erster Art . . . . .	15
1.3.3	Mengenpartitionen und Stirling-Zahlen zweiter Art . . . . .	19
1.3.4	Klammerausdrücke und Catalan-Zahlen . . . . .	20
1.3.5	Zahlpartitionen* . . . . .	24
1.4	Mehrfache Urnenmodelle* . . . . .	26
<b>2</b>	<b>Rekursionen</b>	<b>27</b>
2.1	Analyse von Algorithmen . . . . .	27
2.2	Lineare Rekursionsgleichungen . . . . .	29
2.3	Die Methode der erzeugenden Funktionen . . . . .	32
2.4	Höhere Rekursionsgleichungen . . . . .	38

<b>3</b>	<b>Graphentheorie</b>	<b>43</b>
3.1	Gerichtete und ungerichtete Graphen . . . . .	43
3.2	Wege in Graphen . . . . .	49
3.2.1	Anzahl der Wege in Graphen . . . . .	50
3.2.2	Distanzen in Graphen . . . . .	53
3.2.3	Zusammenhang in Graphen . . . . .	55
3.2.4	Mehrfacher Zusammenhang in Graphen* . . . . .	57
3.3	Klassen von Graphen . . . . .	60
3.3.1	Ungerichtete, kreisfreie Graphen: Bäume und Wälder . . . . .	60
3.3.2	Gerichtete, kreisfreie Graphen . . . . .	65
3.3.3	Bipartite Graphen . . . . .	67
3.3.4	Planare Graphen . . . . .	69
3.4	Kombinatorische Probleme in Graphen . . . . .	71
3.4.1	Touren* . . . . .	71
3.4.2	Färbungen . . . . .	74
3.4.3	Paarungen . . . . .	75
<b>4</b>	<b>Algebraische Strukturen</b>	<b>79</b>
4.1	Universelle Algebren . . . . .	79
4.1.1	Neutrale und inverse Elemente, Assoziativität . . . . .	80
4.1.2	Homomorphismen . . . . .	82
4.2	Algebrentypen . . . . .	85
4.2.1	Algebren mit einer Verknüpfung . . . . .	85
4.2.2	Algebren mit zwei Verknüpfungen . . . . .	87
4.2.3	Algebren mit drei Operatoren . . . . .	88
4.3	Gruppen* . . . . .	89
4.4	Endliche Körper* . . . . .	94
	<b>Literaturverzeichnis</b>	<b>97</b>

Der Schwerpunkt in diesem einführenden Kapitel über Kombinatorik liegt auf dem Abzählen endlicher Mengen.

## 1.1 Einfache Urnenmodelle

Urnenmodelle stellen ein exemplarisches Szenario für kombinatorische Problemstellungen dar. Die einfachste Situation ist die folgende: In *einer* Urne (daher: einfache Urnenmodelle) liegen  $n$  *unterscheidbare* Kugeln, von den  $k$  Kugel gezogen werden dürfen. Die zu beantwortende Frage ist dann: Wie viele Möglichkeiten gibt es, diese  $k$  Kugeln zu ziehen? Zur Präzisierung des Szenarios werden Unterschiede danach gemacht, ob

- die Reihenfolge, in der die Kugeln gezogen werden, eine Rolle spielt,
- gezogene Kugeln wieder zurückgelegt werden oder nicht.

Damit ergeben sich vier verschiedene Szenarios.

**Theorem 1.1** *Die Anzahl der Möglichkeiten, aus einer Urne mit  $n$  Kugeln  $k$  Kugeln auszuwählen, ist durch folgende Tabelle gegeben:*

	<i>mit Zurücklegen</i>	<i>ohne Zurücklegen</i>
<i>mit Reihenfolge</i>	$n^k$	$n^{\underline{k}} =_{\text{def}} \frac{n!}{(n-k)!}$
<i>ohne Reihenfolge</i>	$\binom{n+k-1}{k}$	$\binom{n}{k} =_{\text{def}} \frac{n!}{k!(n-k)!}$

Die im Theorem mitdefinierten Größen  $n^{\underline{k}}$  und  $\binom{n}{k}$  heißen *fallende Faktorielle von  $n$  der Länge  $k$*  sowie *Binomialkoeffizient* („ $n$  über  $k$ “).

**Beispiele:** Wir geben für vier Beispiele die Szenarien und Anzahlen an:

- Die Anzahl der Ziehungen der Lotto-Zahlen „6 aus 49“ entspricht der Anzahl der Ziehungen von 6 Kugeln aus einer Urne mit 49 Kugeln ohne Zurücklegen und ohne Reihenfolge. Somit gibt es  $\binom{49}{6} = 13.983.816$  verschiedene Ziehungen (bzw. Lottoscheine).

- Die Anzahl der vierstelligen PIN-Codes entspricht der Anzahl der Ziehungen von 4 Kugeln aus einer Urne mit 10 Kugeln (Ziffern) mit Zurücklegen und mit Reihenfolge. Somit gibt es  $10^4 = 10.000$  verschiedene PIN-Codes.
- Die Anzahl der Siegerehrungen mit Gold-, Silber- und Bronzemedailles bei einem Wettkampf mit 8 Startern entspricht dem Ziehen von 3 Kugeln aus einer Urne mit 8 Kugeln ohne Zurücklegen und mit Reihenfolge. Somit gibt es  $8^3 = 336$  verschiedene Siegerehrungen.
- Die Anzahl verschiedener Stimmenverteilungen auf 3 zur Wahl stehenden Kandidaten mit 100 Wählern entspricht dem Ziehen von 100 Kugeln aus einer Urne mit 3 Kugeln mit Zurücklegen und ohne Reihenfolge. Somit gibt es  $\binom{102}{100} = 5.151$  verschiedene Wahlausgänge.

**Beweis:** Wir beweisen alle Fälle einzeln, aber aufeinander aufbauend:

- *Ziehen mit Zurücklegen, mit Reihenfolge:* Für die erste gezogene Kugel gibt es  $n$  Möglichkeiten, für die zweite gezogene Kugel gibt es ebenfalls  $n$  Möglichkeiten unabhängig davon, welche Kugel vorher gezogen wurde. Für die  $k$ -te gezogene Kugel gibt es weiterhin  $n$  Möglichkeiten unabhängig davon, welche Kugeln vorher gezogen wurden. Insgesamt gibt es damit

$$\underbrace{n \cdot n \cdot \dots \cdot n}_{k\text{-mal}} = n^k$$

Möglichkeiten.

- *Ziehen ohne Zurücklegen, mit Reihenfolge:* Für die erste gezogene Kugel gibt es  $n$  Möglichkeiten, für die zweite gezogene Kugel gibt es  $n - 1$  Möglichkeiten. Für die  $k$ -te gezogene Kugel ( $k \leq n$ ) gibt es mithin noch  $n - k + 1$  Möglichkeiten. Insgesamt gibt es damit

$$n \cdot (n - 1) \cdot \dots \cdot (n - k + 1) = \frac{n!}{(n - k)!} = n^{\underline{k}}$$

Möglichkeiten.

- *Ziehen ohne Zurücklegen, ohne Reihenfolge:* Mit Berücksichtigung der Reihenfolge gibt es  $\frac{n!}{(n - k)!}$  Auswahlmöglichkeiten. Wenn die Reihenfolge keine Rolle mehr spielt, zählen alle Auswahlfolgen, bei denen die gleichen  $k$  Kugeln gezogen wurden, nur noch als eine Auswahlmöglichkeit. Dies sind gerade  $k!$  viele. Damit gibt es insgesamt

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

Möglichkeiten.

- *Ziehen mit Zurücklegen, ohne Reihenfolge:* Da jede Kugel mehrmals gezogen werden kann, die Reihenfolge jedoch keine Rolle spielt, ist nur wichtig, wie oft eine Kugel gezogen wird. Es sei also  $(a_1, \dots, a_n)$  ein Tupel mit den entsprechenden Anzahlen,

wobei  $a_j$  gerade angibt, wie oft die Kugel  $j$  gezogen wird. Für ein Anzahltuplel  $(a_1, \dots, a_n)$  muss nun gelten:

- (i)  $a_j \in \{0, \dots, k\}$  für alle  $j \in \{1, \dots, n\}$
- (ii)  $a_1 + \dots + a_n = k$

Wir müssen nun zählen, wie viele derartige Tupel es geben kann. Dazu repräsentieren wir die Tupel in einer anderen Weise, die es uns ermöglicht, das Szenario zu wechseln. Wir verwenden  $k$ -mal das Symbol  $*$  und  $(n-1)$ -mal das Symbol  $|$ . Ein Anzahltuplel  $(a_1, \dots, a_n)$  kann nun als Symbolfolge

$$\underbrace{**\dots*}_{a_1} | \underbrace{**\dots*}_{a_2} | \dots | \underbrace{**\dots*}_{a_n}$$

aufgeschrieben werden. Umgekehrt entspricht auch jede Symbolfolge, die  $k$ -mal das Symbol  $*$  und  $(n-1)$ -mal das Symbol  $|$  enthält, einem Anzahltuplel mit obigen Eigenschaften. Statt Anzahltuplel zu zählen, können wir also auch Symbolfolgen zählen. Die Anzahl möglicher Symbolfolgen zu bestimmen, entspricht aber gerade dem Ziehen von  $k$  Positionen für das Symbol  $*$  aus  $n+k-1$  möglichen Positionen ohne Zurücklegen und ohne Reihenfolge. Mithin gibt es insgesamt

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

Möglichkeiten.

Damit ist das Theorem bewiesen. ■

Ein weiteres Beispiel für die Anwendung von Theorem 1.1 ist das Binomialtheorem.

**Theorem 1.2 (Binomialtheorem)** Für alle  $a, b \in \mathbb{R}$  und  $n \in \mathbb{N}$  gilt

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

**Beweis:** Es seien  $a, b \in \mathbb{R}$  und  $n \in \mathbb{N}$  beliebig. Ausmultiplizieren von  $(a+b)^n$  ergibt:

$$\begin{aligned} (a+b)^n &= \overbrace{a \cdot \dots \cdot a \cdot a}^{n \text{ Faktoren}} + \\ &+ a \cdot \dots \cdot a \cdot b + \\ &+ a \cdot \dots \cdot b \cdot a + \\ &+ a \cdot \dots \cdot b \cdot b + \\ &\vdots \\ &+ \underbrace{b \cdot \dots \cdot b \cdot b}_{n \text{ Faktoren}} \end{aligned}$$

Die Summanden können zusammengefasst werden zu Produkten von jeweils  $n$  Faktoren, von denen  $k$  Faktoren gerade  $b$  und  $n - k$  Faktoren gerade  $a$  sind. Die Summanden sind also von der Form  $a^{n-k}b^k$ , da die Reihenfolge bei der Multiplikation keine Rolle spielt. Die Anzahl der Produkte  $a^{n-k}b^k$  entspricht somit gerade dem Ziehen von  $k$  Kugeln (die Positionen für  $b$  im Produkt) aus  $n$  Kugeln (die Gesamtheit aller Positionen für Faktoren), d.h.  $\binom{n}{k}$ . Folglich gilt insgesamt:

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$$

Damit ist das Theorem bewiesen. ■

**Korollar 1.3** Für alle  $n \in \mathbb{N}_+$  gilt

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

**Beweis:** Nach dem Binomialtheorem gilt

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

Damit ist das Korollar bewiesen. ■

**Korollar 1.4** Für alle  $n \in \mathbb{N}$  gilt

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

**Beweis:** Nach dem Binomialtheorem gilt

$$2^n = (1 + 1)^n = \sum_{k=0}^n \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^n \binom{n}{k}.$$

Damit ist das Korollar bewiesen. ■

## 1.2 Kombinatorisches Beweisen

### 1.2.1 Grundregeln des Abzählens

**Lemma 1.5 (Gleichheitsregel)** Es seien  $A$  und  $B$  endliche Mengen. Es gibt genau dann eine Bijektion  $f : A \rightarrow B$ , wenn  $|A| = |B|$  gilt.



**Beweis:** Siehe Satz 3.19 (aus dem Kapitel über Funktionen und Abbildungen im Skriptum *Mathematische Grundlagen der Informatik*). ■

**Lemma 1.6 (Summenregel)** *Es seien  $A_1, \dots, A_n$  endliche, paarweise disjunkte Mengen. Dann gilt:*

$$|A_1 \cup \dots \cup A_n| = \sum_{j=1}^n |A_j|$$

**Beweis:** Wegen der paarweisen Disjunktheit der Mengen kommt jedes Element aus  $A_1 \cup \dots \cup A_n$  in genau einer Menge  $A_j$  vor. ■

**Lemma 1.7 (Produktregel)** *Es seien  $A_1, \dots, A_n$  endliche Mengen. Dann gilt:*

$$|A_1 \times \dots \times A_n| = \prod_{j=1}^n |A_j|$$

**Beweis:** Wir beweisen die Aussage mittels Induktion über die Anzahl  $n$  der Mengen.

- *Induktionsanfang:* Für  $n = 1$  ist die Aussage offensichtlich.
- *Induktionsschritt:* Es sei  $n > 1$ . Weiterhin seien  $A_1, \dots, A_n$  endliche Mengen. Wir setzen

$$\begin{aligned} A^* &=_{\text{def}} A_1 \times \dots \times A_{n-1} \\ B_y &=_{\text{def}} \{ (x_1, \dots, x_{n-1}, y) \mid (x_1, \dots, x_{n-1}) \in A^* \} \quad \text{für } y \in A_n \end{aligned}$$

Für die so definierten Mengen gelten folgende Eigenschaften:

- Die Mengenfamilie  $\{ B_y \mid y \in A_n \}$  ist eine Partition von  $A_1 \times \dots \times A_n$ .
- Für jedes  $y \in A_n$  ist die Funktion

$$f_y : B_y \rightarrow A^* : (x_1, \dots, x_{n-1}, y) \mapsto (x_1, \dots, x_{n-1})$$

eine Bijektion, d.h.  $|B_y| = |A^*|$  für alle  $y \in A_n$  (nach Lemma 1.5).

Damit erhalten wir:

$$\begin{aligned} |A_1 \times \dots \times A_n| &= \left| \bigcup_{y \in A_n} B_y \right| && \text{(nach Eigenschaft (i))} \\ &= \sum_{y \in A_n} |B_y| && \text{(nach Lemma 1.6 und Eigenschaft (i))} \end{aligned}$$

$$\begin{aligned}
&= \sum_{y \in A_n} |A^*| && \text{(nach Lemma 1.5 und Eigenschaft (ii))} \\
&= |A^*| \cdot |A_n| \\
&= \left( \prod_{j=1}^{n-1} |A_j| \right) \cdot |A_n| && \text{(nach Induktionsvoraussetzung)} \\
&= \prod_{j=1}^n |A_j|
\end{aligned}$$

Damit ist das Lemma bewiesen. ■

**Lemma 1.8 (Potenzregel)** *Es seien  $A$  und  $B$  endliche Mengen mit  $|A| = m$  und  $|B| = n$ . Dann existieren genau  $n^m$  Funktionen  $f : A \rightarrow B$ .*

**Beweis:** Nach Lemma 1.5 dürfen wir  $A = \{1, \dots, m\}$  ohne Beeinträchtigung der Allgemeinheit annehmen. Jeder Funktion  $f : A \rightarrow B$  kann nun eineindeutig (injektiv) ein Tupel  $(f(1), \dots, f(m)) \in B^m$  zugeordnet werden. Außerdem entspricht jedes Tupel (die Wertetabelle)  $(y_1, \dots, y_m) \in B^m$  einer Funktion  $f : A \rightarrow B : j \mapsto y_j$ . Damit ist die Zuordnung sowohl injektiv als auch surjektiv, also eine Bijektion. Aus Lemma 1.5 und Produktregel (Lemma 1.7) folgt somit

$$|\{ f \mid f : A \rightarrow B \}| = |B^m| = |B|^m = n^m.$$

Damit ist das Lemma bewiesen. ■

**Beispiel:** Wie viele boolesche Funktionen mit  $n$  Variablen gibt es? Die Antwort lautet  $|\{ f \mid f : \{0, 1\}^n \rightarrow \{0, 1\} \}| = 2^{2^n}$ .

**Korollar 1.9** *Für endliche Mengen  $A$  mit  $|A| = n$  gilt  $|\mathcal{P}(A)| = 2^n$ .*

**Beweis:** Wir konstruieren eine Bijektion zwischen  $\mathcal{P}(A)$  und der Menge der Funktionen  $f : A \rightarrow \{0, 1\}$ . Dazu definieren wir für eine Menge  $B \in \mathcal{P}(A)$  die Funktion:

$$c_B : A \rightarrow \{0, 1\} : x \mapsto \begin{cases} 1 & \text{falls } x \in B \\ 0 & \text{falls } x \notin B \end{cases}$$

Diese Zuordnung ist offensichtlich eine Bijektion zwischen  $\mathcal{P}(A)$  und der Menge der Funktionen  $f : A \rightarrow \{0, 1\}$ . Nach der Potenzregel (Lemma 1.8) und Lemma 1.5 gilt folglich

$$|\mathcal{P}(A)| = |\{ f \mid f : A \rightarrow \{0, 1\} \}| = 2^n.$$

Damit ist das Korollar bewiesen. ■

Die im Beweis von Korollar 1.9 angegebenen Funktionen haben einen Namen: Für eine Menge  $B \subseteq A$  heißt  $c_B$  die *charakteristische Funktion* von  $B$ .

### 1.2.2 Doppeltes Abzählen

Unter *Doppeltem Abzählen* fassen wir Techniken zusammen, bei denen die Elemente derselben Menge auf unterschiedliche Weise gezählt werden, um so Gleichheiten (oder manchmal auch Ungleichheiten) zu gewinnen. Am deutlichsten ist dieses Beweisprinzip beim Bestimmen der Kardinalität von binären Relationen zu sehen.

**Lemma 1.10 (Doppeltes Abzählen)** *Es sei  $R \subseteq A \times B$  eine endliche Relation. Dann gilt*

$$\sum_{a \in A} |\{ b \in B \mid (a, b) \in R \}| = \sum_{b \in B} |\{ a \in A \mid (a, b) \in R \}| = |R|.$$

**Beweis:** Jedes Paar  $(a, b) \in R$  wird in beiden Summen genau einmal gezählt. ■

**Beispiel:** Wir wollen die Anzahl der Einsen in einer Matrix  $A \in \{0, 1\}^{n \times m}$  zählen. Man beachte, dass jede binäre Relation  $R \subseteq \{1, \dots, n\} \times \{1, \dots, m\}$  durch eine Matrix  $A$  beschrieben werden kann mittels  $(i, j) \in R \iff a_{i,j} = 1$ . Konkret sei die folgende Matrix gegeben:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{array}{l} \rightarrow 8 \\ \rightarrow 4 \\ \rightarrow 2 \\ \rightarrow 2 \\ \rightarrow 1 \\ \rightarrow 1 \\ \rightarrow 1 \\ \rightarrow 1 \end{array}$$

$$\begin{array}{cccccccc} \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 2 & 3 & 2 & 4 & 2 & 4 \end{array} \rightarrow 20$$

Im allgemeinen Fall einer Matrix  $A \in \{0, 1\}^{n \times m}$  mit den Einträgen  $a_{i,j}$  stehen in der letzten Spalte in der  $i$ -ten Zeile die *Zeilensumme*  $\sum_{j=1}^m a_{i,j}$  und in der letzten Zeile in der  $j$ -ten Spalte die *Spaltensumme*  $\sum_{i=1}^n a_{i,j}$ . Klarerweise muss die Summe über alle Zeilensummen stets gleich der Summe über alle Spaltensummen sein:

$$\sum_{j=1}^m \sum_{i=1}^n a_{i,j} = \sum_{i=1}^n \sum_{j=1}^m a_{i,j}$$

**Theorem 1.11 (Vandermondese Identität)** *Für  $k, m, n \in \mathbb{N}$  gilt*

$$\binom{n+m}{k} = \sum_{j=0}^k \binom{n}{j} \binom{m}{k-j}.$$

**Beweis:** Es seien  $A$  und  $B$  disjunkte Mengen mit  $|A| = n$  und  $|B| = m$ . Für jedes  $j \in \{0, \dots, k\}$  definieren wir die Mengenfamilie

$$\mathcal{X}_j =_{\text{def}} \{ X \mid X \subseteq A \cup B, |X \cap A| = j \text{ und } |X \cap B| = k - j \}$$

Es gibt  $\binom{n}{j}$  viele  $j$ -elementige Teilmengen von  $A$  und  $\binom{m}{k-j}$  viele  $(k-j)$ -elementige Teilmengen von  $B$ . Damit gilt

$$|\mathcal{X}_j| = \binom{n}{j} \binom{m}{k-j}.$$

Wegen  $\mathcal{X}_i \cap \mathcal{X}_j = \emptyset$  für  $i \neq j$  folgt nun

$$\binom{n+m}{k} = \sum_{j=0}^k |\mathcal{X}_j| = \sum_{j=0}^k \binom{n}{j} \binom{m}{k-j}.$$

Damit ist das Theorem bewiesen. ■

**Beispiel:** Wenn zum Beispiel in einer Vorlesung  $n + m$  Studenten sitzen,  $n$  weibliche und  $m$  männliche, wie viele verschiedene Gruppen mit genau  $k$  Studenten gibt es dann? Dies lässt sich auf zwei Arten bestimmen:

- Ohne Berücksichtigung des Geschlechts erhalten wir  $\binom{n+m}{k}$  Gruppen.
- Mit Berücksichtigung des Geschlechts zählen wir für jedes  $j \in \{0, 1, \dots, k\}$  alle Gruppen mit jeweils genau  $j$  weiblichen und genau  $k - j$  männlichen Studenten, damit also insgesamt  $\sum_{j=0}^k \binom{n}{j} \binom{m}{k-j}$  Gruppen.

Da wir über dieselbe Menge von Studenten argumentieren, sind beide Anzahlen gleich.

### 1.2.3 Das Inklusion-Exklusions-Prinzip

Das Inklusion-Exklusions-Prinzip ist eine Verallgemeinerung der Summenregel (Lemma 1.6) auf beliebige, nicht notwendig paarweise disjunkte Mengen.

**Theorem 1.12 (Inklusions-Exklusions-Prinzip)** *Es seien  $A_1, \dots, A_n$  endliche Mengen. Dann gilt:*

$$\left| \bigcup_{j=1}^n A_j \right| = \sum_{\emptyset \neq K \subseteq \{1, \dots, n\}} (-1)^{1+|K|} \left| \bigcap_{k \in K} A_k \right|$$

**Beispiel:**

- Für  $n = 2$  reduzieren sich die Ausdrücke in Theorem 1.12 zu folgender Identität:

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

- Für  $n = 3$  reduzieren sich die Ausdrücke in Theorem 1.12 zu folgender Identität:

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| \\ &\quad - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &\quad + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

**Beweis:** Wir bestimmen, wie oft jedes Element auf beiden Seiten der Gleichung gezählt wird. Es sei  $x \in \bigcup_{j=1}^n A_j$ .

- *Linke Seite:* Das Element  $x$  wird genau einmal gezählt.
- *Rechte Seite:* Wir müssen zeigen, dass  $x$  auch hier genau einmal gezählt wird. Dazu sei  $\ell =_{\text{def}} |\{j \mid x \in A_j\}|$ . Ohne Beeinträchtigung der Allgemeinheit komme  $x$  genau in den Mengen  $A_1, \dots, A_\ell$  vor. Dann gilt:
  - Für  $\emptyset \neq K \subseteq \{1, \dots, \ell\}$  wird  $x$  genau  $(-1)^{1+|K|}$ -mal gezählt.
  - Für alle anderen Menge  $K$  wird  $x$  gar nicht gezählt.

Somit folgt für den Beitrag von  $x$  zur rechten Seite der Gleichung insgesamt:

$$\begin{aligned} \sum_{\emptyset \neq K \subseteq \{1, \dots, \ell\}} (-1)^{1+|K|} &= \sum_{k=1}^{\ell} \binom{\ell}{k} (-1)^{1+k} = - \sum_{k=1}^{\ell} \binom{\ell}{k} (-1)^k \\ &= 1 - \sum_{k=0}^{\ell} \binom{\ell}{k} (-1)^k \\ &= 1 \qquad \qquad \qquad \text{(nach Korollar 1.4)} \end{aligned}$$

Damit ist das Theorem bewiesen. ■

Wir wollen an einem Beispiel verdeutlichen, wie der doch recht kompliziert wirkende Ausdruck auf der rechten Seite gewinnbringend angewendet werden kann.

**Beispiel:** Wie viele Primzahlen gibt es zwischen 2 und 100? Um diese Frage zu beantworten, bestimmen wir die zusammengesetzten Zahlen zwischen 2 und 100 mit Hilfe des Inklusions-Exklusions-Prinzip. Es sei  $A =_{\text{def}} \{2, \dots, 100\}$ . Eine Zahl  $x \in A$  ist zusammengesetzt, falls  $x = p \cdot n$  für geeignete Zahlen  $p, n \in A$  gilt, wobei  $p$  eine Primzahl mit  $p \leq \sqrt{100} = 10$  ist. Damit kommen als Primzahlen nur  $p_1 = 2$ ,  $p_2 = 3$ ,  $p_3 = 5$  und  $p_4 = 7$  in Frage. Für  $i \in \{1, 2, 3, 4\}$  betrachten wir die Menge der Vielfachen von  $p_i$ , d.h. die Menge

$$A_i =_{\text{def}} \{x \in A \mid (\exists n \in A)[x = p_i \cdot n]\}.$$

Damit gilt:

- $A_1 \cup A_2 \cup A_3 \cup A_4$  ist die Menge der zusammengesetzten Zahlen aus  $A$

- Die Kardinalitäten der möglichen Schnittmengen sind

$$|A_i| = \left\lfloor \frac{100}{p_i} \right\rfloor - 1 \quad (\text{da } p_i \notin A_i)$$

$$\left| \bigcap_{j=1}^k A_{i_j} \right| = \left\lfloor \frac{100}{\prod_{j=1}^k p_{i_j}} \right\rfloor \quad \text{für } k \in \{2, 3, 4\} \text{ und } 1 \leq i_1 < \dots < i_k \leq 4$$

Nach Theorem 1.12 erhalten wir:

$$\begin{aligned} & |A_1 \cup A_2 \cup A_3 \cup A_4| \\ &= \left( \left\lfloor \frac{100}{2} \right\rfloor - 1 + \left\lfloor \frac{100}{3} \right\rfloor - 1 + \left\lfloor \frac{100}{5} \right\rfloor - 1 + \left\lfloor \frac{100}{7} \right\rfloor - 1 \right) \\ &\quad - \left( \left\lfloor \frac{100}{6} \right\rfloor + \left\lfloor \frac{100}{10} \right\rfloor + \left\lfloor \frac{100}{14} \right\rfloor + \left\lfloor \frac{100}{15} \right\rfloor + \left\lfloor \frac{100}{21} \right\rfloor + \left\lfloor \frac{100}{35} \right\rfloor \right) \\ &\quad + \left( \left\lfloor \frac{100}{30} \right\rfloor + \left\lfloor \frac{100}{42} \right\rfloor + \left\lfloor \frac{100}{70} \right\rfloor + \left\lfloor \frac{100}{105} \right\rfloor \right) \\ &\quad - \left\lfloor \frac{100}{210} \right\rfloor \\ &= 49 + 32 + 19 + 13 - 16 - 10 - 7 - 6 - 4 - 2 + 3 + 2 + 1 + 0 - 0 \\ &= 74 \end{aligned}$$

Damit gibt es  $99 - 74 = 25$  Primzahlen zwischen 2 und 100.

#### 1.2.4 Der Schubfachschluss

Ein weiteres wichtiges Abzählprinzip, um die Existenz von Objekten zu beweisen, ist der Schubfachschluss (engl. *pigeonhole principle*).

**Theorem 1.13 (Schubfachschluss)** *Es seien  $A$  und  $B$  endliche Mengen mit  $|A| > |B| > 0$  und  $f : A \rightarrow B$  eine Funktion. Dann gibt es ein  $y \in B$  mit  $|f^{-1}(y)| > 1$ .*

**Beweis:** (*Widerspruch*) Angenommen es gilt  $|f^{-1}(y)| \leq 1$  für alle  $y \in B$ . Dann wissen wir aus dem letzten Semester, dass  $f$  eine injektive Funktion ist. Daraus folgt  $|A| \leq |B|$ . Dies ist ein Widerspruch zu  $|A| > |B|$ . Mithin war die Annahme falsch, und das Theorem ist bewiesen. ■

Mit anderen Worten: Um  $|A|$  Objekte in  $|B|$  Schubfächer zu stecken, müssen sich in mindestens einem Schubfach 2 Objekte befinden (falls  $|A| > |B|$  ist).

**Beispiele:** An folgenden Fällen wollen wir die Anwendung des Schubfachschlusses demonstrieren:

- Von 13 Personen feiern mindestens zwei Personen im gleichen Monat ihren Geburtstag.
- In jeder Menge  $P$  von mindestens zwei Personen gibt es immer mindestens zwei Personen, die die gleiche Anzahl von Personen in  $P$  kennen. (Hierbei sei angenommen, dass „kennen“ eine symmetrische Relation ist.)

Zur Begründung: Es seien  $P = \{p_1, \dots, p_n\}$  die Personenmenge mit  $n \geq 2$  Personen sowie  $f : P \rightarrow \{0, \dots, n-1\}$  eine Funktion, die der Person  $p_i$  die Anzahl ihrer Bekannten in  $P$  zuordnet. Wegen  $|P| = |\{0, \dots, n-1\}| = n$  kann Theorem 1.13 nicht direkt angewendet werden. Eine genauere Analyse ermöglicht jedoch die folgende Fallunterscheidung:

- Es gibt ein  $p \in P$  mit  $f(p) = 0$ . Wegen der Symmetrie der Bekanntschaftsrelation gibt es auch keine Person, die alle Personen in  $P$  kennt. Also gilt  $f(q) \neq n-1$  für alle  $q \in P$  und folglich  $f(P) \subseteq \{0, \dots, n-2\}$ .
- Für alle  $p \in P$  gilt  $f(p) \neq 0$ . Damit gilt  $f(P) \subseteq \{1, \dots, n-1\}$ .

In beiden Fällen gilt also  $|f(P)| < |P|$ . Nach Theorem 1.13 folgt die Aussage.

**Theorem 1.14 (Verallgemeinerter Schubfachschluss)** *Es seien  $A$  und  $B$  endliche, nichtleere Mengen und  $f : A \rightarrow B$  eine Funktion. Dann existiert ein  $y \in B$  mit  $|f^{-1}(y)| \geq \left\lceil \frac{|A|}{|B|} \right\rceil$ .*

**Beweis:** (*Widerspruch*) Wir nehmen wiederum an, dass  $|f^{-1}(y)| \leq \left\lceil \frac{|A|}{|B|} \right\rceil - 1$  für alle  $y \in B$  gilt. Dann folgt:

$$\begin{aligned}
 |A| &= \sum_{y \in B} |f^{-1}(y)| \\
 &\leq |B| \cdot \left( \left\lceil \frac{|A|}{|B|} \right\rceil - 1 \right) \\
 &\leq |B| \cdot \left( \frac{|A| + |B| - 1}{|B|} - 1 \right) \\
 &= |B| \cdot \frac{|A| - 1}{|B|} \\
 &= |A| - 1
 \end{aligned}$$

Dies ist jedoch ein Widerspruch. Mithin war die Annahme falsch, und das Theorem ist bewiesen. ■

**Beispiel:** Wir wollen wieder an zwei Beispielen den verallgemeinerten Schubfachschluss verdeutlichen.

- Von 100 Personen feiern mindestens 9 Personen im gleichen Monat ihren Geburtstag.
- In jeder Menge von 6 Personen gibt es 3 Personen, die sich alle untereinander kennen, oder 3, die sich alle nicht kennen. (Hierbei nehmen wir wiederum an, dass „kennen“ eine symmetrische Relation ist.)

Zur Begründung: Es sei  $P = \{p_1, \dots, p_6\}$  eine beliebige Personenmenge. Wir betrachten für die Person  $p_1$  die Funktion

$$f : \{p_2, \dots, p_6\} \rightarrow \{\text{„bekannt“}, \text{„nicht bekannt“}\},$$

die jeder Person  $p_2, \dots, p_6$  zuordnet, ob  $p_1$  diese Person kennt. Nach Theorem 1.14 sind  $\lceil \frac{5}{2} \rceil = 3$  Personen mit  $p_1$  „bekannt“ oder 3 Personen mit  $p_1$  „nicht bekannt“. Ohne Beeinträchtigung der Allgemeinheit seien 3 Personen mit  $p_1$  bekannt (sonst vertauschen wir in nachfolgender Argumentation einfach „kennen“ und „nicht kennen“) und zwar  $p_2, p_3$  und  $p_4$ . Nun gibt es zwei Möglichkeiten für die Personen  $p_2, p_3$  und  $p_4$ :

- Es gibt zwei Personen in  $\{p_2, p_3, p_4\}$ , die sich kennen. Diese beiden Personen kennen aber auch  $p_1$ . Somit gibt es also 3 Personen, die sich alle untereinander kennen.
- Die Personen  $p_2, p_3$  und  $p_4$  kennen sich nicht. Also gibt es 3 Personen, die sich untereinander nicht kennen.

## 1.3 Abzählprobleme

### 1.3.1 Kombinationen und Binomialkoeffizienten

Aus dem ersten Abschnitt (Theorem 1.1) wissen wir, dass die Anzahl der Kombinationen von  $k$  Elementen aus  $n$  Elementen (d.h. die Anzahl der Möglichkeiten aus  $n$  Kugeln  $k$  Kugeln ungeordnet ohne Zurücklegen zu ziehen) gerade dem Binomialkoeffizienten  $\binom{n}{k}$  entspricht. Da Binomialkoeffizienten auch über die reine Kombinatorik hinaus wichtig sind, wollen in diesem Abschnitt die wichtigsten Eigenschaften von Binomialkoeffizienten festhalten. Dazu definieren wir den Binomialkoeffizienten noch einmal explizit: Für  $n, k \in \mathbb{N}$  definieren wir

$$\binom{n}{k} \stackrel{\text{def}}{=} \frac{n!}{k!(n-k)!}, \quad \text{mit } \binom{n}{k} = 0 \quad \text{für } k > n .$$



Eine einfache, sofort einsichtige Beobachtung ist:

$$\binom{n}{k} = \binom{n}{n-k}$$

Damit lässt sich der Binomialkoeffizient konsistent auch für negative Werte für  $k$  definieren:

$$\binom{n}{k} =_{\text{def}} 0 \quad \text{für } k \in \mathbb{Z} \setminus \mathbb{N}.$$

**Theorem 1.15 (Pascalsches Dreieck)** Für  $n \in \mathbb{N}_+$  und  $k \in \mathbb{N}$  gilt

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

Wir geben zwei Beweise für das Theorem an.

**Beweis:** (*rechnerisch*) Wir führen eine Fallunterscheidung bezüglich der Werte von  $k$  durch:

- Für  $k = 0$  und  $n > 1$  gilt  $\binom{n}{0} = 1 = \binom{n-1}{-1} + \binom{n-1}{0}$ .
- Für  $0 < k < n$  rechnen wir aus:

$$\begin{aligned} \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-1-k)!} \\ &= \frac{(n-1)!}{(k-1)!(n-k)!} \cdot \frac{k}{k} + \frac{(n-1)!}{k!(n-1-k)!} \cdot \frac{n-k}{n-k} \\ &= \frac{(n-1)! \cdot k}{k!(n-k)!} + \frac{(n-1)!(n-k)}{k!(n-k)!} \\ &= \frac{(n-1)!(k+n-k)}{k!(n-k)!} \\ &= \frac{(n-1)! \cdot n}{k!(n-k)!} \\ &= \binom{n}{k} \end{aligned}$$

- Für  $k = n$  und  $n > 1$  gilt  $\binom{n}{n} = 1 = \binom{n-1}{n-1} + \binom{n-1}{n}$ .
- Für  $k > n > 1$  gilt  $\binom{n}{k} = 0 = \binom{n-1}{k-1} + \binom{n-1}{k}$ .



### 1.3.2 Permutationen und Stirling-Zahlen erster Art

Es sei  $A$  eine endliche Menge mit  $|A| = n$ . Eine *Permutation* von  $A$  ist eine bijektive Funktion  $\pi : A \rightarrow A$ . Ohne Beeinträchtigung der Allgemeinheit setzen wir stets  $A = \{1, \dots, n\}$  voraus. Die Menge  $\{1, \dots, n\}$  notieren wir auch als  $[n]$ . Weiterhin definieren wir die Menge

$$\mathcal{S}_n =_{\text{def}} \{ \pi \mid \pi : [n] \rightarrow [n] \text{ ist eine Permutation} \},$$

die sogenannte *symmetrische Gruppe* von  $n$  Elementen.

**Theorem 1.16** Für alle  $n \in \mathbb{N}_+$  gilt  $|\mathcal{S}_n| = n!$ .

**Beweis:**  $|\mathcal{S}_n|$  entspricht dem Ziehen von  $n$  Kugeln aus einer Urne mit  $n$  Kugeln ohne Zurücklegen mit Berücksichtigung der Reihenfolge. Nach Theorem 1.1 gilt

$$|\mathcal{S}_n| = \frac{n!}{(n-n)!} = n!.$$

Damit ist das Theorem bewiesen. ■

Ohne Beweis geben wir folgendes Resultat über das Verhalten der Fakultätsfunktion an:

**Theorem 1.17 (Stirlingsche Formel)** Für alle  $n \in \mathbb{N}_+$  gilt

$$\sqrt{2\pi n} \left(\frac{n}{e}\right)^n < n! < \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n}},$$

wobei  $e = e^1 = 2,718281828459\dots$  die EULERSche Konstante ist.

Permutationen können auf verschiedene Arten geschrieben werden. Im Folgenden behandeln wir drei Schreibweisen:

**Matrixschreibweise:** Dazu schreiben wir die Permutation  $\pi : [n] \rightarrow [n]$  als  $2 \times n$ -Matrix der Form

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Da  $\pi$  bijektiv ist, kommen alle Werte  $1, \dots, n$  in der zweiten Zeile vor.

**Beispiel:** Folgende Permutation ist in Matrixschreibweise gegeben:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix}$$

**Tupelschreibweise:** Im Prinzip genügt es, von der Matrixschreibweise lediglich die zweite Zeile zu übernehmen, d.h. Permutationen können angegeben werden in der Form

$$\pi = (\pi(1), \pi(2), \pi(3), \dots, \pi(n)).$$

**Beispiel:**  $\pi = (4, 1, 6, 2, 5, 3)$  ist obige Permutation in Tupelschreibweise.

**Zyklenschreibweise:** Die Zyklenschreibweise entsteht, wenn wir für  $x \in [n]$  die iterierte Hintereinanderausführung von  $\pi$  auf  $x$  betrachten. Dadurch entsteht eine Folge:

$$\begin{aligned} \pi^0(x) &=_{\text{def}} x, \\ \pi^1(x) &=_{\text{def}} \pi(x), \\ \pi^2(x) &=_{\text{def}} \pi(\pi(x)), \\ &\vdots \\ \pi^k(x) &=_{\text{def}} \pi(\pi^{k-1}(x)), \\ &\vdots \end{aligned}$$

Für jedes  $x \in [n]$  gibt es dann ein minimales  $0 < k < n$  mit  $\pi^k(x) = x$ .

**Beispiel:** Für die Permutation  $\pi = (4, 1, 6, 2, 5, 3)$  gilt

$$\begin{array}{llll} \pi^0(1) = 1, & \pi^1(1) = 4, & \pi^2(1) = 2, & \pi^3(1) = 1; \\ \pi^0(2) = 2, & \pi^1(2) = 1, & \pi^2(2) = 4, & \pi^3(2) = 2; \\ \pi^0(3) = 3, & \pi^1(3) = 6, & \pi^2(3) = 3; & \\ \pi^0(4) = 4, & \pi^1(4) = 2, & \pi^2(4) = 1, & \pi^3(4) = 4; \\ \pi^0(5) = 5, & \pi^1(5) = 5; & & \\ \pi^0(6) = 6, & \pi^1(6) = 3, & \pi^2(6) = 6. & \end{array}$$

Eine Folge  $x, \pi(x), \pi^2(x), \dots, \pi^{k-1}(x)$  mit minimalem  $k > 0$ , so dass  $\pi^k(x) = x$ , heißt *Zyklus* der Länge  $k$  und wird als  $(x \ \pi(x) \ \pi^2(x) \ \dots \ \pi^{k-1}(x))$  geschrieben.

**Beispiel:**  $\pi = (4, 1, 6, 2, 5, 3)$  enthält die Zyklen  $(1 \ 4 \ 2)$ ,  $(3 \ 6)$  und  $(5)$ .

Jede Permutation kann als *Produkt von Zyklen* geschrieben werden, indem die Zyklen einfach hintereinander gesetzt werden. Die Schreibweise ist jedoch nicht eindeutig. Insbesondere kann jeder Zyklus der Länge  $k$  auf genau  $k$  Arten geschrieben werden.

**Beispiel:** Die Permutation  $\pi = (4, 1, 6, 2, 5, 3)$  können wir als Produkt von Zyklen wie folgt schreiben:

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

$$\begin{aligned}
 &= (4\ 2\ 1)(6\ 3)(5) \\
 &= (5)(2\ 1\ 4)(6\ 3)
 \end{aligned}$$

Insbesondere gilt  $(1\ 4\ 2) = (4\ 2\ 1) = (2\ 1\ 4)$ .

Die Anzahl der Zyklen, aus der eine Permutation bestehen kann, liegt zwischen 1, wie in  $(1\ 2\ 3\ \dots\ n)$ , und  $n$ , wie in  $(1)(2)(3)\dots(n)$ . Im Folgende wollen wir die Anzahl der Permutationen mit genau  $k$  Zyklen genauer bestimmen.

Für  $n, k \in \mathbb{N}$  sei  $\begin{bmatrix} n \\ k \end{bmatrix}$  (manchmal auch  $s_{n,k}$ ) geschrieben) die Anzahl der Permutationen von  $n$  Elementen mit genau  $k$  Zyklen. Dann gilt also

$$\sum_{k=1}^n \begin{bmatrix} n \\ k \end{bmatrix} = n!.$$

Die Zahlen  $\begin{bmatrix} n \\ k \end{bmatrix}$  heißen *Stirling-Zahlen erster Art*. Folgende Sonderfälle sind zu beachten:

- Für  $k > n$  gilt  $\begin{bmatrix} n \\ k \end{bmatrix} = 0$ , da eine Permutation von  $n$  Elementen höchstens  $n$  Zyklen enthalten kann.
- Für  $n > 0$  gilt  $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$ , da jede Permutation mindestens einen Zyklus enthält.
- Wir definieren  $\begin{bmatrix} 0 \\ 0 \end{bmatrix} =_{\text{def}} 1$ .

Mit diesen Sonderfällen können wir wiederum eine Rekursionsvorschrift für die Berechnung der Stirling-Zahlen erster Art angeben.

**Theorem 1.18 (Stirling-Dreieck erster Art)** Für alle  $k, n \in \mathbb{N}$  mit  $n \geq k$  gilt

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}.$$

**Beweis:** (*kombinatorisch*) Es sei  $\pi \in \mathcal{S}_n$  eine Permutation mit  $k$  Zyklen. Dann kann  $\pi$  auf zwei Arten aus einer Permutation aus  $\mathcal{S}_{n-1}$  entstanden sein:

- Einfügen eines Zyklus  $(n)$  in Permutationen aus  $\mathcal{S}_{n-1}$  mit  $k-1$  Zyklen
- Einfügen des Elementes  $n$  in einen der Zyklen einer Permutation aus  $\mathcal{S}_{n-1}$  mit  $k$  Zyklen

Beide Fälle sind disjunkt. Für die Anzahl der Möglichkeiten, Permutationen mit  $k$  Zyklen auf diese zwei Arten zu erzeugen, ergibt sich jeweils:

$$(i) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$$



### 1.3.3 Mengenpartitionen und Stirling-Zahlen zweiter Art

In diesem Abschnitt wollen wir bestimmen, wie viele Möglichkeiten es gibt  $n$ -elementige Grundmengen in  $k$  nichtleere, disjunkte Komponenten zu zerlegen.

Es sei  $A$  eine endliche Menge mit  $|A| = n$ . Eine  $k$ -Partition  $\mathcal{F} = \{A_1, A_2, \dots, A_k\}$  ist eine  $k$ -elementige Familie von nichtleeren Teilmengen von  $A$  mit  $A_1 \cup A_2 \cdots \cup A_k = A$  und  $A_i \cap A_j = \emptyset$ , falls  $i \neq j$ .

Es sei  $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$  (manchmal auch:  $S_{n,k}$ ) die Anzahl der  $k$ -Partitionen einer  $n$ -elementigen Grundmenge. Die Zahlen  $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$  heißen *Stirling-Zahlen zweiter Art*. Folgende Spezialfälle sind zu beachten:

- Für  $k > n$  gilt  $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = 0$ , da die  $n$  Elemente höchstens in  $n$  Komponenten liegen können.
- Für  $k = 0$  gilt  $\left\{ \begin{smallmatrix} n \\ 0 \end{smallmatrix} \right\} = 0$ , da die  $n$  Elemente in wenigstens einer Komponenten liegen müssen.
- Wir definieren  $\left\{ \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right\} =_{\text{def}} 1$ .

Wir können nun eine ähnliche rekursive Darstellung wie in Theorem 1.18 für die Stirlingzahlen erster Art auch für die Stirling-Zahlen zweiter Art beweisen.

**Theorem 1.19 (Stirling-Dreieck zweiter Art)** Für alle  $k, n \in \mathbb{N}$  mit  $n \geq k$  gilt

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

**Beweis:** (*kombinatorisch*) Es sei  $\mathcal{F}$  eine  $k$ -Partition einer  $n$ -elementigen Menge. Dann kann  $\mathcal{F}$  auf zwei Arten aus einer Partition einer  $(n-1)$ -elementigen Menge entstehen:

- Hinzufügen der Menge  $\{n\}$  zu einer  $(k-1)$ -Partition von  $n-1$  Elementen
- Einfügen von  $n$  in einer der Mengen einer  $k$ -Partition von  $n-1$  Elementen

Die Anzahl der Möglichkeiten  $k$ -Partitionen von  $n$  Elementen zu bilden, ist wie folgt:

- $\left\{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\}$
- $k \cdot \left\{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\}$

Mithin gilt also:

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

Damit ist das Theorem bewiesen. ■

Wir geben wieder einen Eindruck für das Wachstum der Zahlen  $\binom{n}{k}$  gemäß Theorem 1.19.

**Beispiel:** Der Dreiecksaufbau des rekursiven Zusammenhangs in Theorem 1.19 lässt sich wie folgt veranschaulichen:

$$\begin{array}{cccccccc}
 & & & & & & & 1 \\
 & & & & & & & 0 & 1 \\
 & & & & & & & 0 & 1 & 1 \\
 & & & & & & & 0 & 1 & 3 & 1 \\
 & & & & & & & 0 & 1 & 7 & 6 & 1 \\
 & & & & & & & 0 & 1 & 15 & 25 & 10 & 1 \\
 & & & & & & & 0 & 1 & 31 & 90 & 65 & 15 & 1 \\
 & & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
 \end{array}$$

Interessieren wir uns nur für die Anzahl aller möglichen Partitionen einer Grundmenge  $A$  mit  $|A| = n$ , so kann man die *Bell-Zahlen* bestimmen:

$$B_n =_{\text{def}} \sum_{k=0}^n \binom{n}{k}$$

Insbesondere gibt  $B_n$  also die Anzahl aller Äquivalenzrelationen auf  $n$  Elementen an.

### 1.3.4 Klammersausdrücke und Catalan-Zahlen

Wir betrachten das Problem, korrekte bzw. legale Klammersausdrücke zu zählen. Ein Klammersausdruck ist *legal*, wenn es zu jeder öffnenden eine schließende Klammer gibt und sich zwischen den Klammern oder hinter den Klammern nur wieder legale Klammersausdrücke befinden. Beispielsweise sind  $(( ))$  und  $()(( ))$  korrekt geklammert;  $(( ))()()$  ist dagegen nicht korrekt geklammert. Legale Klammersausdrücke werden durch eine kontextfreie Grammatik mit den Regeln

$$S \rightarrow \varepsilon, S \rightarrow (S), S \rightarrow SS$$



erzeugt. Mittels Induktion über den Aufbau legaler Klammerausdrücke kann gezeigt werden, dass ein legaler Klammerausdruck  $x = x_1 \dots x_n \in \{(,)\}^*$  folgende Bedingungen erfüllt:

- Es gibt genauso viele öffnende wie schließende Klammern, d.h.:

$$|\{ i \mid 1 \leq i \leq n \text{ und } x_i = ( \}| = |\{ i \mid 1 \leq i \leq n \text{ und } x_i = ) \}|$$

- Zu jedem Zeitpunkt gibt es mindestens so viele öffnende wie schließende Klammern, d.h.:

$$|\{ i \mid 1 \leq i \leq j \text{ und } x_i = ( \}| \geq |\{ i \mid 1 \leq i \leq j \text{ und } x_i = ) \}|$$

für alle  $j \in \{1, \dots, n-1\}$

Klarerweise müssen legale Klammerausdrücke stets eine gerade Länge besitzen.

Die  $n$ -te Catalan-Zahl  $C_n$  ist definiert als die Anzahl legaler Klammerausdrücke mit genau  $n$  öffnenden Klammern;  $C_0 =_{\text{def}} 1$ .

### Beispiele:

1.  $C_1 = 1$ , denn  $()$  ist einziger legaler Klammerausdruck mit einer öffnenden Klammer.
2.  $C_2 = 2$ , denn  $()()$  und  $(( ))$  sind die einzigen legalen Klammerausdrücke mit zwei öffnenden Klammern.
3.  $C_3 = 5$ , denn  $()()()$ ,  $(( ))()$ ,  $()(( ))$ ,  $(( ))()$  und  $(( ( )))$  sind die einzigen legalen Klammerausdrücke mit drei öffnenden Klammern.

Catalan-Zahlen können gemäß folgender Rekursion bestimmt werden.

**Lemma 1.20** Für alle  $n \in \mathbb{N}_+$  gilt

$$C_n = \sum_{k=1}^n C_{k-1} \cdot C_{n-k}.$$

**Beweis:** (*kombinatorisch*) Es sei  $A_{n,k}$  die Menge legaler Klammerausdrücke, bei denen die erste öffnende Klammer an der Position  $2k$  geschlossen wird, d.h., Wörter der Form

$$\left( \boxed{v} \right) \boxed{w}$$

1                      2k                      2n

Das Wort  $v$  enthält  $k - 1$  öffnende Klammern,  $w$  enthält  $n - k$  öffnende Klammern. Somit folgt  $|A_{n,k}| = C_{k-1} \cdot C_{n-k}$ . Wegen  $A_{n,k} \cap A_{n,k'} = \emptyset$  für  $k \neq k'$  gilt

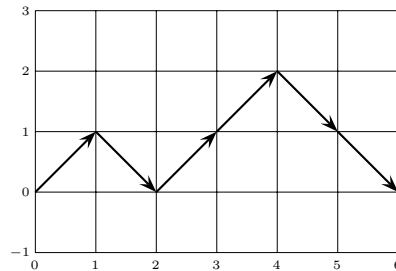
$$C_n = \left| \bigcup_{k=1}^n A_{n,k} \right| = \sum_{k=1}^n |A_{n,k}| = \sum_{k=1}^n C_{k-1} \cdot C_{n-k}.$$

Damit ist das Lemma bewiesen. ■

**Theorem 1.21** Für alle  $n \in \mathbb{N}$  gilt

$$C_n = \frac{1}{n+1} \binom{2n}{n}.$$

**Beweis:** (*kombinatorisch*) An Stelle legaler Klammersausdrücke mit  $n$  öffnenden Klammern werden Wanderungen von  $(0, 0)$  nach  $(2n, 0)$  in einem ganzzahligen Gitter gezählt. Jeder öffnenden Klammer entspricht dabei ein Schritt  $(+1, +1)$  (Aufwärtspfeil), jeder schließenden Klammer entspricht ein Schritt  $(-1, +1)$  (Abwärtspfeil). So entspricht etwa der Klammersausdruck  $()(())$  der Wanderung:



Ein legaler Klammersausdrücke entspricht genau einem Pfad, der komplett oberhalb der  $x$ -Achse verläuft.

Es sei  $D_n$  die Menge aller Pfade von  $(0, 0)$  nach  $(2n, 0)$ . Ein Abwärtspfeil in einem Pfad, die sich unterhalb der  $x$ -Achse befindet, heißt *Fehler*. Es sei  $D_{n,k}$  für  $k \in \{0, 1, \dots, n\}$  die Menge aller Pfade mit genau  $k$  Fehlern. Somit entspricht  $D_{n,0}$  gerade der Menge der legalen Klammersausdrücke mit  $n$  öffnenden Klammern.

Wir werden zeigen, dass  $|D_{n,k}| = |D_{n,\ell}|$  für alle  $k, \ell \in \{0, 1, \dots, n\}$  (\*) gilt. Daraus folgt

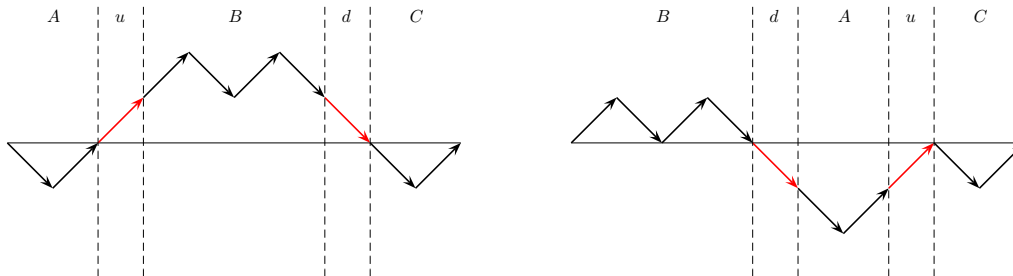
$$|D_n| = \left| \bigcup_{k=0}^n D_{n,k} \right| = \sum_{k=0}^n |D_{n,k}| = \sum_{k=0}^n |D_{n,0}| = (n+1) \cdot |D_{n,0}|$$

und mithin

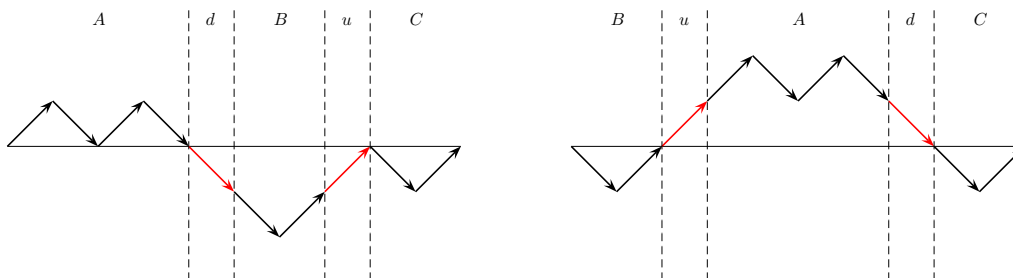
$$C_n = |D_{n,0}| = \frac{1}{n+1} \cdot |D_n| = \frac{1}{n+1} \binom{2n}{n}.$$

Für (\*) geben wir Bijektionen zwischen  $D_{n,k}$  und  $D_{n,k+1}$  für alle  $k \in \{0, \dots, n-1\}$  an:

- Es sei  $P$  ein Pfad in  $D_{n,k}$ . Dann kann  $P$  in  $AuBdC$  zerlegt werden mit folgenden Bedeutungen:  $u$  ist der erste Aufwärtspfeil oberhalb der  $x$ -Achse;  $d$  ist der erste Abwärtspfeil nach  $u$ , der die  $x$ -Achse berührt;  $A, B, C$  sind die möglicherweise leeren Reststücke. Es gilt:  $A$  liegt unterhalb der  $x$ -Achse und hat  $k_1$  Fehler,  $B$  liegt oberhalb der  $x$ -Achse und hat somit 0 Fehler,  $C$  hat folglich  $k - k_1$  Fehler. Wir ordnen  $P$  eineindeutig den Pfad  $P' = BdAuC$  zu, d.h., wir vertauschen  $Au$  und  $Bd$ . Folglich gilt in  $P'$ :  $B$  hat 0 Fehler,  $dAu$  hat  $k_1 + 1$  Fehler,  $C$  hat  $k - k_1$  Fehler. Somit hat  $P'$  genau  $k + 1$  Fehler, d.h.,  $P'$  liegt in  $D_{n,k+1}$ . Beispielhaft ist hier die Zuordnung eines Pfades in  $D_{5,2}$  auf einen Pfad in  $D_{5,3}$  angegeben:



- Für die Umkehrabbildung sein nun  $P$  ein Pfad in  $D_{n,k+1}$ . Dann kann  $P$  in  $AdBuC$  zerlegt werden mit folgenden Bedeutungen:  $d$  ist erster Abwärtspfeil unterhalb der  $x$ -Achse,  $u$  ist erster Aufwärtspfeil nach  $d$ , der die  $x$ -Achse berührt,  $A, B, C$  sind die möglicherweise leeren Reststücke. Es gilt:  $A$  liegt oberhalb der  $x$ -Achse und hat 0 Fehler,  $dBu$  liegt unterhalb der  $x$ -Achse und hat  $1 + k_1$ ,  $k_1 \geq 0$ , Fehler,  $C$  hat  $k + 1 - (k_1 + 1) = k - k_1$  Fehler. Wir bilden  $P$  auf  $P' = BuAdC$  ab, d.h., wir vertauschen  $Ad$  und  $Bu$ . Folglich gilt:  $B$  hat  $k_1$  Fehler,  $uAd$  mit 0 Fehlern,  $C$  hat  $k - k_1$  Fehler. Somit hat  $P$  genau  $k$  Fehler, d.h.,  $P$  liegt in  $D_{n,k}$ . Exemplarisch:



Damit ist das Theorem bewiesen. ■

### 1.3.5 Zahlpartitionen\*

In diesem Abschnitt gehen wir der Frage nach, wie viele Möglichkeiten es gibt, einen Zahl als Summe anderer Zahlen darzustellen.

Eine *Zahlpartition* von  $n \in \mathbb{N}$  mit  $k$  Summanden besteht aus ganzen Zahlen  $n_1, \dots, n_k > 0$  mit  $n = n_1 + \dots + n_k$ . Spielt die Reihenfolge der Summanden keine Rolle, dann heißt die Zahlpartition *ungeordnet*, sonst *geordnet*.

**Beispiel:**  $7 = 1 + 1 + 2 + 3$  ergibt eine Zahlpartition von 7 mit 4 Summanden. Ungeordnet repräsentieren 1, 1, 2, 3 und 3, 2, 1, 1 die gleiche, geordnet unterschiedliche Zahlpartitionen.

Die Frage ist also: Wie viele Zahlpartitionen von  $n$  mit  $k$  Summanden gibt es?

**Ungeordnete Zahlpartitionen:** Es sei  $P_{n,k}$  die Anzahl der Möglichkeiten die Zahl  $n$  ungeordnet in  $k$  Summanden zu zerlegen. Klarerweise gilt  $P_{n,n} = 1$  sowie  $P_{n,1} = 1$  für  $n \geq 1$ . Außerdem sind folgende Spezialfälle zu beachten:

- Für  $k > n$  gilt  $P_{n,k} = 0$ .
- Für  $n \geq 1$  gilt  $P_{n,0} = 0$ .
- Wir definieren  $P_{0,0} =_{\text{def}} 1$ .

Folgendes Theorem gibt eine rekursive Vorschrift zur Berechnung von  $P_{n,k}$  an.

**Theorem 1.22** Für  $n, k \in \mathbb{N}_+$  mit  $n \geq k$  gilt

$$P_{n+k,k} = \sum_{j=1}^k P_{n,j}.$$

**Beweis:** (*kombinatorisch*) Wir unterscheiden die Summanden bei der Zerlegung von  $n+k$  in  $k$  Summanden nach Einsen und größeren Summanden. Für eine Partition mit genau  $i$  Einsen gilt

$$n+k = \underbrace{1+1+\dots+1}_i + \underbrace{n_{i+1}+n_{i+2}+\dots+n_k}_{k-i}$$

mit  $n_{i+1}, \dots, n_k \geq 2$ . Wir definieren  $n'_j =_{\text{def}} n_j - 1$  für  $j \in \{1, \dots, k\}$ . Dann gilt

$$\begin{aligned} n'_{i+1} + n'_{i+2} + \dots + n'_k &= n_{i+1} + n_{i+2} + \dots + n_k - (k-i) \\ &= n + (k-i) - (k-i) \\ &= n \end{aligned}$$

Mithin ist  $n'_{i+1}, \dots, n'_k$  eine Zahlpartition von  $n$  mit  $k - i$  Summanden. Umgekehrt kann jede Zahlpartition von  $n$  mit  $k - i$  Summanden in eine Zahlpartition von  $n + k$  mit  $k$  Summanden, von denen genau  $i$  den Wert 1 haben, umgewandelt werden. Insgesamt gilt also

$$P_{n+k,k} = \sum_{i=0}^{k-1} P_{n,k-i} = \sum_{j=1}^k P_{n,j}.$$

Damit ist das Theorem bewiesen. ■

**Beispiel:** Es gilt  $P_{5,3} = 2$ . Einerseits sind die Zahlpartitionen  $1 + 1 + 3 = 5$  sowie  $1 + 2 + 2 = 5$ . Andererseits ergibt sich mit der Formel aus obigem Theorem

$$P_{5,3} = \sum_{j=1}^3 P_{2,j} = P_{2,1} + P_{2,2} + P_{2,3} = 1 + 1 + 0 = 2.$$

**Geordnete Zahlpartitionen:** Die Anzahl der Möglichkeiten, die Zahl  $n$  geordnet in  $k$  Summanden zu verteilen, kann auf bereits bekannte Größen zurückgeführt werden.

**Theorem 1.23** Für alle  $n, k \in \mathbb{N}_+$  mit  $n \geq k$  gibt es

$$\binom{n-1}{k-1}$$

geordnete Zahlpartitionen von  $n$  mit  $k$  Summanden.

**Beweis:** Jede Zahl  $n \geq 2$  kann mit  $n$  Einsen dargestellt werden:

$$n = \underbrace{1 + \dots + 1}_{x_1} + \underbrace{1 + \dots + 1}_{x_2} + \dots + \underbrace{1 + \dots + 1}_{x_k}$$

Somit kann jede geordnete Zahlpartition von  $n$  mit  $k$  Summanden umkehrbar eindeutig durch die Positionen der Pluszeichen zwischen Einserblöcken repräsentiert werden. Folglich werden aus  $n - 1$  möglichen Positionen genau  $k - 1$  ausgewählt. Insgesamt ergeben sich

$$\binom{n-1}{k-1}$$

Möglichkeiten. Damit ist das Theorem bewiesen. ■

**Beispiel:** Wie viele Lösungen besitzt die lineare Gleichung

$$x_1 + x_2 + \dots + x_k = n$$

in den natürlichen Zahlen? Die Null ist hier also als Summand zugelassen.  
Wegen

$$x_1 + x_2 + \cdots + x_k = n \iff (x_1 + 1) + (x_2 + 1) + \cdots + (x_k + 1) = n + k$$

gibt es genau  $\binom{n+k-1}{k-1}$  Lösungen.

## 1.4 Mehrfache Urnenmodelle\*

Im Folgenden betrachten wir ein verallgemeinertes kombinatorisches Szenario, in dem viele der bisher angestellten Überlegungen zur Anwendung kommen: Wie viele Möglichkeiten gibt es,  $n$  Bälle auf  $m$  Urnen zu verteilen?

Hierbei sind wieder verschiedene Szenarien möglich, je nachdem

- ob die Bälle unterscheidbar oder nicht unterscheidbar sind,
- ob die Urnen unterscheidbar oder nicht unterscheidbar sind und
- ob die Urnen jeweils mindestens, genau oder höchstens einen Ball enthalten müssen.

Theorem 1.24 fasst für alle möglichen Szenarien die Anzahlen zusammen.

**Theorem 1.24** Die Anzahl der Möglichkeiten,  $n$  Bälle auf  $m$  Urnen zu verteilen, ist durch folgende Tabelle angegeben:

$ B  = n,  U  = m$	Zuordnung beliebig	Zuordnung injektiv	Zuordnung surjektiv	Zuordnung bijektiv
$B$ untersch., $U$ untersch.	$m^n$	$\begin{cases} m^n & m \geq n \\ 0 & m < n \end{cases}$	$m! \cdot S_{n,m}$	$\begin{cases} n! & m = n \\ 0 & m \neq n \end{cases}$
$B$ nicht untersch., $U$ untersch.	$\binom{m+n-1}{n}$	$\binom{m}{n}$	$\binom{n-1}{m-1}$	$\begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$
$B$ untersch., $U$ nicht untersch.	$\sum_{k=1}^m S_{n,k}$	$\begin{cases} 1 & m \geq n \\ 0 & m < n \end{cases}$	$S_{n,m}$	$\begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$
$B$ nicht untersch., $U$ nicht untersch.	$\sum_{k=1}^m P_{n,k}$	$\begin{cases} 1 & m \geq n \\ 0 & m < n \end{cases}$	$P_{n,m}$	$\begin{cases} 1 & m = n \\ 0 & m \neq n \end{cases}$

**Beweis:** Der Beweis des Theorems bleibt als Übungsaufgabe überlassen. ■

## 2.1 Analyse von Algorithmen

Rekursionsgleichungen treten häufig bei Laufzeitanalysen von Algorithmen auf. Exemplarisch werden wir dies am wohlbekannten euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier natürlicher Zahlen diskutieren. Zur Erinnerung geben wir den Algorithmus noch einmal an (für Korrektheit und Herleitung siehe Skriptum „Brückenkurs Mathematik“):

Algorithmus: EUKLID  
Eingabe: positive natürliche Zahlen  $n, m$  mit  $m \leq n$   
Ausgabe:  $\text{ggT}(m, n)$

1. IF  $m$  teilt  $n$
2.     RETURN  $m$
3. ELSE
4.     RETURN EUKLID( $\text{mod}(n, m), m$ )

Die Laufzeit des Algorithmus wird sicher maßgeblich von der Anzahl der rekursiven Aufrufe bestimmt. Es ist also die Frage zu beantworten, wie viele rekursive Aufrufe von EUKLID( $m, n$ ) benötigt werden. Wir nehmen im Folgenden stets an, dass  $m \leq n$  gilt.

**Beispiel:** Eine triviale obere Schranke für die Anzahl der Aufrufe ist sicher  $n$ . Dabei sind wir aber viel zu pessimistisch. Beispielsweise gilt

$$\text{EUKLID}(36, 120) = \text{EUKLID}(12, 36) = 12,$$

womit also nur eine rekursiver Aufrufe erfolgt. Für EUKLID(89, 144) werden genau 9 rekursive Aufrufe benötigt. Und dies ist die maximale Anzahl rekursive Aufrufe von EUKLID( $m, 144$ ) für alle  $1 \leq m \leq 144$ .

Die maximale Anzahl der rekursiven Aufrufe ist eng mit den FIBONACCI-Zahlen verbunden. Die  $n$ -te FIBONACCI-Zahl  $F_n$  ist wiederum rekursiv wie folgt definiert:

$$\begin{aligned} F_n &=_{\text{def}} F_{n-1} + F_{n-2} && \text{für } n \geq 2 \\ F_1 &=_{\text{def}} 1 \\ F_0 &=_{\text{def}} 0 \end{aligned}$$

Die Folge der FIBONACCI-Zahlen beginnt mit  $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \dots$ . Die in obigem Beispiel verwendeten Zahlen 89 und 144 sind also gerade  $F_{11}$  und  $F_{12}$ . Benachbarte FIBONACCI-Zahlen sind nun gerade schlechteste Eingaben für den euklidischen Algorithmus.

**Lemma 2.1** *Es seien  $k, m, n \in \mathbb{N}_+$  beliebige natürliche Zahlen. Dann gilt:*

1.  $\text{EUKLID}(F_{k+2}, F_{k+3})$  benötigt genau  $k$  rekursive Aufrufe.
2. Wenn  $\text{EUKLID}(m, n)$  mindestens  $k$  rekursive Aufrufe benötigt, dann gilt  $n \geq F_{k+3}$  und  $m \geq F_{k+2}$ .

**Beweis:** (*Induktion*) Wir zeigen beide Aussagen im Block mittels vollständiger Induktion über  $k$ .

- *Induktionsanfang:* Es sei  $k = 1$ . Es gilt  $F_3 = 2$  und  $F_4 = 3$ .
  1. Wegen  $\text{EUKLID}(2, 3) = \text{EUKLID}(1, 2) = 1$  erfolgt genau ein rekursiver Aufruf.
  2. Wir betrachten alle Fälle mit  $n < 3$  oder  $m < 2$ . Wegen  $\text{EUKLID}(2, 2) = 2$  und  $\text{EUKLID}(1, n) = 1$  erfolgt in allen diesen Fällen kein rekursiver Aufruf. Damit ist die Kontraposition der Aussage für  $k = 1$  gezeigt und die Aussage ist wahr.
- *Induktionsschritt:* Es sei  $k > 1$ . Damit gilt

$$1 \leq F_{k+1} < F_{k+2} < F_{k+3} = F_{k+2} + F_{k+1} < 2 \cdot F_{k+2}$$

und folglich  $F_{k+2} \nmid F_{k+3}$  mit  $\text{mod}(F_{k+3}, F_{k+2}) = F_{k+1}$ .

1. Es gilt  $\text{EUKLID}(F_{k+2}, F_{k+3}) = \text{EUKLID}(F_{k+1}, F_{k+2})$ . Nach Induktionsvoraussetzung benötigt  $\text{EUKLID}(F_{(k-1)+2}, F_{(k-1)+3})$  genau  $k-1$  rekursive Aufrufe. Mithin benötigt  $\text{EUKLID}(F_{k+2}, F_{k+3})$  genau  $k$  rekursive Aufrufe.
2. Für  $m$  und  $n$  benötige  $\text{EUKLID}(m, n)$  mindestens  $k \geq 2$  rekursive Aufrufe. Dann gilt  $\text{EUKLID}(m, n) = \text{EUKLID}(\text{mod}(n, m), m)$  und  $\text{EUKLID}(\text{mod}(n, m), m)$  benötigt mindestens  $k-1 \geq 1$  rekursive Aufrufe. Nach Induktionsvoraussetzung gilt  $m \geq F_{(k-1)+3}$  sowie  $\text{mod}(n, m) \geq F_{(k-1)+2}$ . Mithin gilt:

$$n \geq m + \text{mod}(n, m) \geq F_{k+2} + F_{k+1} = F_{k+3}$$

Damit ist das Lemma bewiesen. ■

**Korollar 2.2** *Es seien  $m, n \in \mathbb{N}_+$  beliebige natürliche Zahlen mit  $m \leq n$ . Dann ist die Anzahl der rekursiven Aufrufe von  $\text{EUKLID}(m, n)$  nach oben beschränkt (mit Gleichheit) durch*

$$k^* =_{\text{def}} \max \{ k \mid F_{k+3} \leq n \}.$$



Mit dem Wissen um die Formel

$$F_n = \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^n \quad (2.1)$$

folgt  $k^* = O(\log n)$  und damit eine asymptotisch präzise Aussage über das Laufzeitverhalten von EUKLID. Der Algorithmus terminiert also für alle Eingaben mit höchstens logarithmisch vielen rekursiven Aufrufen im Wert der größeren Zahl und ist damit schnell.

Im Folgenden wollen Gleichheiten wie die Formel (2.1) beweisen und auch herleiten.

## 2.2 Lineare Rekursionsgleichungen

**Definition 2.3** Eine Rekursionsgleichung der Form

$$x_n = a_1 x_{n-1} + \dots + a_k x_{n-k} + b_k \quad \text{für alle } n \geq k$$

mit den Anfangsbedingungen

$$x_i = b_i \quad \text{für alle } i \in \{0, \dots, k-1\}$$

heißt lineare Rekursionsgleichung  $k$ -ter Ordnung. Für  $b_k = 0$  heißt die Rekursionsgleichung homogen sonst inhomogen.

**Beispiel:** Die einfachsten, nicht trivialen Rekursionsgleichungen sind homogene, lineare Rekursionsgleichungen erster Ordnung:

$$\begin{aligned} x_n &= a \cdot x_{n-1} & \text{für } n \geq 1 \\ x_0 &= b_0 \end{aligned}$$

Die Lösung der Gleichung ist sofort einzusehen:  $x_n = b_0 \cdot a^n$ .

**Theorem 2.4** Es sei eine inhomogene, lineare Rekursionsgleichung erster Ordnung

$$\begin{aligned} x_n &= a \cdot x_{n-1} + b_1 & \text{für } n \geq 1 \\ x_0 &= b_0 \end{aligned}$$

mit beliebigen Konstanten  $a, b_0, b_1$  gegeben. Dann hat die Lösung der Gleichung die Form:

$$x_n = \begin{cases} b_0 \cdot a^n + b_1 \cdot \frac{a^n - 1}{a - 1}, & \text{falls } a \neq 1 \\ b_0 + n \cdot b_1 & \text{falls } a = 1 \end{cases}$$

**Beweis:** (*Induktion*) Wir zeigen das Theorem mittels vollständiger Induktion über  $n$ .

- *Induktionsanfang:* Es sei  $n = 0$ . Dann gilt für  $a \neq 1$

$$x_0 = b_0 \cdot a^0 + b_1 \cdot \frac{a^0 - 1}{a - 1} = b_0$$

und für  $a = 1$

$$x_0 = b_0 + 0 \cdot b_1 = b_0.$$

- *Induktionsschritt:* Es sei  $n > 0$ . Für  $a \neq 1$  gilt

$$\begin{aligned} x_n &= a \cdot x_{n-1} + b_1 && \text{(nach Definition)} \\ &= a \cdot \left( b_0 \cdot a^{n-1} + b_1 \cdot \frac{a^{n-1} - 1}{a - 1} \right) + b_1 && \text{(nach Induktionsvoraussetzung)} \\ &= b_0 \cdot a^n + b_1 \left( \frac{a^n - a}{a - 1} + 1 \right) \\ &= b_0 \cdot a^n + b_1 \cdot \frac{a^n - 1}{a - 1} \end{aligned}$$

Für  $a = 1$  ergibt sich aus der rekursiven Definition und der Induktionsvoraussetzung

$$x_n = x_{n-1} + b_1 = b_0 + (n - 1) \cdot b_1 + b_1 = b_0 + n \cdot b_1.$$

Damit ist das Theorem bewiesen. ■

**Theorem 2.5** *Es sei eine homogene, lineare Rekursionsgleichung zweiter Ordnung*

$$\begin{aligned} x_n &= a_1 \cdot x_{n-1} + a_2 \cdot x_{n-2} && \text{für } n \geq 2 \\ x_1 &= b_1 \\ x_0 &= b_0 \end{aligned}$$

mit  $a_1 \neq 0$  oder  $a_2 \neq 0$  gegeben. Es seien  $\alpha, \beta \in \mathbb{R}$  Lösungen von  $t^2 - a_1 t - a_2 = 0$  und  $A, B \in \mathbb{R}$  wie folgt definiert:

$$\begin{aligned} A &=_{\text{def}} \begin{cases} \frac{b_1 - b_0 \beta}{\alpha - \beta}, & \text{falls } \alpha \neq \beta \\ \frac{b_1 - b_0 \alpha}{\alpha}, & \text{falls } \alpha = \beta \end{cases} \\ B &=_{\text{def}} \begin{cases} \frac{b_1 - b_0 \alpha}{\alpha - \beta}, & \text{falls } \alpha \neq \beta \\ b_0, & \text{falls } \alpha = \beta \end{cases} \end{aligned}$$

Dann hat die Lösung der Gleichung die Form:

$$x_n = \begin{cases} A\alpha^n - B\beta^n, & \text{falls } \alpha \neq \beta \\ (An + B)\alpha^n, & \text{falls } \alpha = \beta \end{cases}$$

**Beweis:** (*Induktion*) Wir zeigen das Theorem nur für den Fall  $\alpha \neq \beta$  und verwenden dazu wiederum vollständige Induktion über  $n$ .

- *Induktionsanfang:* Es sei  $n \in \{0, 1\}$ . Für  $n = 0$  gilt

$$x_0 = A\alpha^0 - B\beta^0 = A - B = \frac{b_1 - b_0\beta - b_1 + b_0\alpha}{\alpha - \beta} = b_0 \cdot \frac{\alpha - \beta}{\alpha - \beta} = b_0$$

und für  $n = 1$  gilt

$$x_1 = A\alpha^1 - B\beta^1 = A\alpha - B\beta = \frac{b_1\alpha - b_0\alpha\beta - b_1\beta + b_0\alpha\beta}{\alpha - \beta} = b_1 \cdot \frac{\alpha - \beta}{\alpha - \beta} = b_1.$$

- *Induktionsschritt:* Es sei  $n > 1$ . Dann gilt:

$$\begin{aligned} x_n &= a_1 \cdot x_{n-1} + a_2 \cdot x_{n-2} && \text{(nach Definition)} \\ &= a_1 \cdot (A\alpha^{n-1} - B\beta^{n-1}) + a_2 \cdot (A\alpha^{n-2} - B\beta^{n-2}) && \text{(nach Induktionsvoraussetzung)} \\ &= a_1A\alpha^{n-1} + a_2A\alpha^{n-2} - a_1B\beta^{n-1} - a_2B\beta^{n-2} \\ &= A\alpha^{n-2} \cdot (a_1\alpha + a_2) - B\beta^{n-2} \cdot (a_1\beta + a_2) \\ &= A\alpha^{n-2} \cdot \alpha^2 - B\beta^{n-2} \cdot \beta^2 \\ & && \text{(wegen } \alpha^2 - a_1\alpha - a_2 = 0 \text{ und } \beta^2 - a_1\beta - a_2 = 0) \\ &= A\alpha^n - B\beta^n \end{aligned}$$

Damit ist das Theorem bewiesen. ■

Die Folge der FIBONACCI-Zahlen ist durch eine homogene, lineare Rekursionsgleichung zweiter Ordnung gegeben. Somit kann das Theorem 2.5 angewendet werden.

**Korollar 2.6** Für alle  $n \in \mathbb{N}$  gilt

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

**Beweis:** Nach Definition der FIBONACCI-Zahlen ist  $a_1 = a_2 = 1$ . Die Nullstellen von  $t^2 - t - 1$  sind

$$\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}, \quad \beta = \frac{1}{2} - \frac{1}{2}\sqrt{5}.$$

Für  $A$  und  $B$  rechnen wir aus:

$$A = \frac{1 - 0 \cdot \beta}{\sqrt{5}} = \frac{1}{\sqrt{5}}, \quad B = \frac{1 - 0 \cdot \alpha}{\sqrt{5}} = \frac{1}{\sqrt{5}}$$

Aus Theorem 2.5 folgt die Formel und das Korollar ist bewiesen. ■

## 2.3 Die Methode der erzeugenden Funktionen

Wir gehen nunmehr dazu über, Lösungen linearer Rekursionsgleichungen nicht mehr nur zu beweisen sondern zu *konstruieren*. Dazu verwenden wir formale Potenzreihen und erzeugende Funktionen. Für diese Begrifflichkeiten sind einige Sachverhalte aus der Analysis (siehe Skriptum „Mathematische Grundlagen der Informatik“) zu wiederholen.

Rekursionen definieren unendliche Folgen  $a_0, a_1, a_2, \dots$  von Zahlen. Wir repräsentieren eine solche Folge durch eine *formale Potenzreihe* in der Variablen  $x$ :

$$A(x) =_{\text{def}} \sum_{k=0}^{\infty} a_k \cdot x^k$$

Die rechte Seite der Definition ist die formale Potenzreihe – „formal“ deshalb, weil Konvergenzfragen von Potenzreihen unbeachtet bleiben. Insbesondere können ganz allgemein die Koeffizienten der Potenzreihe (die Folgenglieder) aus beliebigen Objekten wie z.B. Graphen oder Wörtern bestehen, für die der Konvergenzbegriff gar nicht definiert ist.

Eine formale Potenzreihe kann als Funktion  $A(x)$  in  $x$  aufgefasst werden.  $A(x)$  heißt dann *erzeugende Funktion* der Folge  $a_0, a_1, a_2, \dots$

Aus der Analysis entnehmen wir folgenden Sachverhalt (Identitätssatz für Potenzreihen):

*Sind für zwei Folgen  $a_0, a_1, \dots$  und  $b_0, b_1, \dots$  ihre erzeugenden Funktionen  $A(x)$  und  $B(x)$  gleich, so gilt  $a_n = b_n$  für alle  $n \in \mathbb{N}$ .*

Erzeugende Funktionen repräsentieren also formale Potenzreihen und die zugehörigen Folgen eindeutig.

**Bestimmung der erzeugenden Funktion zu einer Folge.** Um erzeugende Funktionen zu bestimmen, benutzen wir Regeln zum Rechnen mit formalen Potenzreihen:

- *Addition:* Für zwei Folgen  $a_0, a_1, \dots$  und  $b_0, b_1, \dots$  gilt

$$\left( \sum_{k=0}^{\infty} a_k \cdot x^k \right) + \left( \sum_{k=0}^{\infty} b_k \cdot x^k \right) = \sum_{k=0}^{\infty} (a_k + b_k) \cdot x^k$$

- *Multiplikation:* Für zwei Folgen  $a_0, a_1, \dots$  und  $b_0, b_1, \dots$  gilt

$$\left( \sum_{k=0}^{\infty} a_k \cdot x^k \right) \cdot \left( \sum_{k=0}^{\infty} b_k \cdot x^k \right) = \sum_{n=0}^{\infty} \left( \sum_{k=0}^n a_k \cdot b_{n-k} \right) \cdot x^n$$

- *Indexverschiebung aufwärts:* Für die Potenzreihe zu der Folge, die aus der Transformation  $a_0, a_1, a_2, \dots \mapsto \underbrace{0, 0, \dots, 0}_m, a_0, a_1, a_2, \dots$  resultiert, gilt

$$\sum_{k=0}^{\infty} a_k \cdot x^{m+k} = x^m \cdot \sum_{k=0}^{\infty} a_k \cdot x^k$$

- *Indexverschiebung abwärts:* Für die Potenzreihe zu der Folge, die aus der Transformation  $a_0, a_1, a_2, \dots \mapsto a_m, a_{m+1}, a_{m+2}, \dots$  resultiert, gilt

$$\sum_{k=0}^{\infty} a_{k+m} \cdot x^k = x^{-m} \cdot \sum_{k=0}^{\infty} a_{k+m} \cdot x^{k+m} = x^{-m} \cdot \left( \sum_{k=0}^{\infty} a_k \cdot x^k - \sum_{k=0}^{m-1} a_k \cdot x^k \right)$$

- *Differenzieren:* Für die erste Ableitung der Potenzreihe zu  $a_0, a_1, \dots$  gilt

$$\left( \sum_{k=0}^{\infty} a_k \cdot x^k \right)' = \sum_{k=0}^{\infty} (a_k \cdot x^k)' = \sum_{k=0}^{\infty} k \cdot a_k \cdot x^{k-1} = \sum_{k=0}^{\infty} (k+1) a_{k+1} \cdot x^k$$

Die Ableitung einer Potenzreihe entspricht somit der Transformation auf Folgen:  
 $a_0, a_1, a_2, \dots, a_k, \dots \mapsto a_1, 2a_2, \dots, ka_k, \dots$

Die im Zusammenhang mit linearen Rekursionsgleichungen fundamentale Potenzreihe ist die *geometrische Reihe*

$$A(x) =_{\text{def}} \sum_{k=0}^{\infty} x^k,$$

d.h. die formale Potenzreihe von  $1, 1, 1, \dots$ . Die erzeugende Funktion  $A(x)$  können wir wie folgt explizit bestimmen:

$$A(x) = \sum_{k=0}^{\infty} x^k = 1 + \sum_{k=1}^{\infty} x^k = 1 + x \cdot \sum_{k=1}^{\infty} x^{k-1} = 1 + x \cdot \sum_{k=0}^{\infty} x^k = 1 + x \cdot A(x)$$

Die erzeugende Funktion der Folge  $1, 1, 1, \dots$  ist somit:

$$A(x) = \frac{1}{1-x}$$

**Beispiele:** Wir wollen die erzeugende Funktion  $A(x) = (1-x)^{-1}$  von  $1, 1, 1, \dots$  benutzen, um beispielhaft weitere Potenzreihen und erzeugende Funktionen zu bestimmen.

1. Die erzeugende Funktion  $B(x)$  von  $1, 2, 3, 4, \dots$  ist die erste Ableitung von  $A(x)$ :

$$B(x) = A'(x) = \left( \frac{1}{1-x} \right)' = \frac{1}{(1-x)^2}$$

2. Die erzeugende Funktion von  $0, 1, 2, 3, 4, \dots$  ergibt sich durch Indexverschiebung um eine Position aufwärts aus  $B(x)$ :

$$x \cdot B(x) = \frac{x}{(1-x)^2}$$

3. Die erzeugende Funktion von  $1, \alpha, \alpha^2, \alpha^3, \dots$  ergibt sich durch Substitution aus  $A(x)$ :

$$\sum_{k=0}^{\infty} \alpha^k \cdot x^k = \sum_{k=0}^{\infty} (\alpha x)^k = A(\alpha x) = \frac{1}{1-\alpha x}$$

Die nachfolgende Übersicht fasst einige Beispiele wichtiger Potenzreihen und erzeugender Funktionen zusammen, die benutzt werden können, um erzeugende Funktionen zu einer gegebenen Folge zu bestimmen:

Folglied $a_k$	Folgenanfang	formale Potenzreihe	erzeugende Funktion
1	$1, 1, 1, 1, \dots$	$\sum_{k=0}^{\infty} x^k$	$\frac{1}{1-x}$
$k$	$0, 1, 2, 3, \dots$	$\sum_{k=0}^{\infty} k \cdot x^k$	$\frac{x}{(1-x)^2}$
$\alpha^k$	$1, \alpha, \alpha^2, \alpha^3, \dots$	$\sum_{k=0}^{\infty} \alpha^k \cdot x^k$	$\frac{1}{1-\alpha x}$
$k^2$	$0, 1, 4, 9, \dots$	$\sum_{k=0}^{\infty} k^2 \cdot x^k$	$\frac{x(1+x)}{(1-x)^3}$
$\frac{1}{k}$	$0, 1, \frac{1}{2}, \frac{1}{3}, \dots$	$\sum_{k=1}^{\infty} \frac{1}{k} \cdot x^k$	$\ln(1-x)$
$\frac{1}{k!}$	$1, 1, \frac{1}{2}, \frac{1}{6}, \dots$	$\sum_{k=0}^{\infty} \frac{1}{k!} \cdot x^k$	$e^x$

**Bestimmung der Folge zu einer erzeugenden Funktion.** Haben wir nun eine erzeugende Funktion  $A(x)$  gegeben, wie bestimmen wir die zugehörige Folge? Dazu betrachten wir die  $n$ -te Ableitung von  $A(x)$  (soweit dies möglich ist, was in unseren Fälle aber stets der Fall ist):

$$A^{(n)}(x) = \left( \sum_{k=0}^{\infty} a_k \cdot x^k \right)^{(n)} = \sum_{k=n}^{\infty} k^{\underline{n}} \cdot a_k \cdot x^{k-n}$$

Setzen wir  $x = 0$ , so ist  $x^m = 0$  für  $m > 0$  und wir erhalten:

$$A^{(n)}(0) = n! \cdot a_n$$

Mithin gilt also für das  $k$ -te Folgenglied der zu  $A(x)$  gehörenden Folge

$$a_k = \frac{A^{(k)}(0)}{k!}$$

und die zu  $A(x)$  gehörende Potenzreihe ist die TAYLOR-Reihe von  $A(x)$  (um den Entwicklungspunkt  $x_0 = 0$ ):

$$A(x) = \sum_{k=0}^{\infty} \frac{A^{(k)}(0)}{k!} \cdot x^k$$

**Beispiel:** Es gilt  $(e^x)' = e^x$  und somit

$$e^x = \sum_{k=0}^{\infty} \frac{1}{k!} \cdot x^k.$$

**Die Methode der erzeugenden Funktionen.** Lineare Rekursionsgleichungen können nun mit Hilfe der auf formalen Potenzreihen basierenden *Methode der erzeugenden Funktionen* gelöst werden. Diese Methode vollzieht sich in einer Reihe von Rechenschritten (siehe Kasten).

**Schema der Methode der erzeugenden Funktion zur Auflösung linearer Rekursionsgleichungen  $k$ -ter Ordnung:**

1. Aufstellen der erzeugenden Funktion als Potenzreihe
2. Anwendung der Rekursionsgleichung
3. Umformen der rechten Seite nach der erzeugenden Funktion
4. Auflösen nach der erzeugenden Funktion
5. Ersetzen der neuen rechten Seite durch eine Potenzreihe (TAYLOR-Reihe)
6. Koeffizientenvergleich (nach dem Identitätssatz für Potenzreihen)

Wir wollen die Methode der erzeugenden Funktion exemplarisch an den Fibonacci-Zahlen nachvollziehen.

*1. Aufstellen der erzeugenden Funktion als Potenzreihe*

Für die Folge  $(F_n)_{n \in \mathbb{N}}$  definieren wir die erzeugende Funktion  $F(x)$  als Potenzreihe:

$$F(x) =_{\text{def}} \sum_{n=0}^{\infty} F_n \cdot x^n$$

### 2. Anwendung der Rekursionsgleichung

Wir setzen zunächst die Anfangsbedingungen und anschließend die rekursive Definition der Folge  $(F_n)_{n \in \mathbb{N}}$  in die Potenzreihe ein:

$$\begin{aligned} F(x) &= F_0 + F_1x + \sum_{n=2}^{\infty} F_n \cdot x^n \\ &= x + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) \cdot x^n \end{aligned}$$

### 3. Umformen der rechten Seite nach der erzeugenden Funktion

Wir drücken die rechte Seite durch Umformung der Potenzreihe und Indexverschiebung mit Hilfe von  $F(x)$  aus:

$$\begin{aligned} F(x) &= x + \sum_{n=2}^{\infty} F_{n-1} \cdot x^n + \sum_{n=2}^{\infty} F_{n-2} \cdot x^n \\ &= x + \sum_{n=1}^{\infty} F_n \cdot x^{n+1} + \sum_{n=0}^{\infty} F_n \cdot x^{n+2} \\ &= x + x \sum_{n=1}^{\infty} F_n \cdot x^n + x^2 \sum_{n=0}^{\infty} F_n \cdot x^n \\ &= x + x(F(x) - F_0) + x^2F(x) \\ &= x + xF(x) + x^2F(x) \end{aligned}$$

### 4. Auflösen nach der erzeugenden Funktion

Durch Umstellung nach  $F(x)$  erhalten wir:

$$F(x) = \frac{x}{1 - x - x^2}$$

### 5. Ersetzen der neuen rechten Seite durch eine Potenzreihe (TAYLOR-Reihe)

Anstatt  $F(x)$  in eine TAYLOR-Reihe zu entwickeln, verwenden wir die Partialbruchzerlegung, um  $F(x)$  in uns schon bekannte Potenzreihen zu überführen. Wir verwenden für die Partialbruchzerlegung den Ansatz

$$\frac{x}{1 - x - x^2} = \frac{A}{1 - \alpha x} + \frac{B}{1 - \beta x}$$



und versuchen  $A, B, \alpha$  und  $\beta$  geeignet zu bestimmen. Mit Hilfe des Ansatzes erhalten wir dann für  $F(x)$  unter Verwendung der geometrischen Reihe:

$$F(x) = A \sum_{n=0}^{\infty} (\alpha x)^n + B \sum_{n=0}^{\infty} (\beta x)^n$$

Gemäß dem Ansatz müssen die Parameter die beiden folgenden Gleichungen erfüllen:

$$(1 - \alpha x)(1 - \beta x) = 1 - x - x^2 \quad (2.2)$$

$$A(1 - \beta x) + B(1 - \alpha x) = x \quad (2.3)$$

Aus Gleichung (2.2) folgt  $1 - (\alpha + \beta)x + \alpha\beta x^2 = 1 - x - x^2$  und mithin durch Koeffizientenvergleich  $\alpha + \beta = 1$  und  $\alpha\beta = -1$ . Daraus folgt  $\alpha(1 - \alpha) = -1$  und somit  $\alpha^2 - \alpha - 1 = 0$ . Durch Bestimmung der Nullstellen erhalten wir

$$\alpha = \frac{1 + \sqrt{5}}{2}, \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

Aus Gleichung (2.3) folgt zunächst:

$$\begin{aligned} x &= A(1 - \beta x) + B(1 - \alpha x) \\ &= A - A\beta x + B - \alpha Bx \\ &= A + B - (A\beta + B\alpha)x \end{aligned}$$

Durch Koeffizientenvergleich ergeben sich die Bedingungen  $A + B = 0$  und  $A\beta + B\alpha = -1$ . Folglich muss  $A(\beta - \alpha) = -1$  gelten. Durch Einsetzen der konkreten Werte für  $\alpha$  und  $\beta$  erhalten wir:

$$A \left( \frac{1 - \sqrt{5}}{2} - \frac{1 + \sqrt{5}}{2} \right) = -A\sqrt{5} = -1$$

Damit finden wir für die Parameter  $A$  und  $B$  die Werte

$$A = \frac{1}{\sqrt{5}}, \quad B = -\frac{1}{\sqrt{5}}.$$

Die erzeugende Funktion  $F(x)$  ist somit durch folgende Potenzreihe ausdrückbar:

$$\begin{aligned} F(x) &= \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \left( \frac{1 + \sqrt{5}}{2} \cdot x \right)^n - \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \left( \frac{1 - \sqrt{5}}{2} \cdot x \right)^n \\ &= \sum_{n=0}^{\infty} \left[ \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^n \right] \cdot x^n \end{aligned}$$

### 6. Koeffizientenvergleich

Da wir die für  $F(x)$  angesetzte Potenzreihe nur algebraisch äquivalent umgeformt haben, können wir einen Koeffizientenvergleich durchführen und erhalten als Ergebnis für die  $n$ -te Fibonacci-Zahl:

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

## 2.4 Höhere Rekursionsgleichungen

Die Methode der erzeugenden Funktion kann auch auf nichtlineare Rekursionsgleichungen angewendet werden. Dies führt unter Umständen zu sehr komplizierten Berechnungen, die häufig zu keinen geschlossen darstellbaren Ergebnissen führen. Wir wollen an einem Beispiel aus der Kombinatorik höhere Rekursionsgleichungen diskutieren.

**Catalanzahlen.** Wir betrachten das Problem, die Anzahl korrekt geklammerter Zeichenkette zu zählen. Eine Zeichenkette ist korrekt geklammerter, wenn es für jede öffnende Klammer eine schließende existiert. Beispielsweise sind  $()$  und  $()()$  korrekt geklammerter;  $((()))$  ist dagegen nicht korrekt geklammerter. Formal: Ein Wort  $x = x_1 \dots x_n \in \{(\,)\}^*$  heißt *legaler Klammerausdruck*, falls gilt:

- (i)  $|\{ i \mid 1 \leq i \leq n \text{ und } x_i = ( \}| = |\{ i \mid 1 \leq i \leq n \text{ und } x_i = ) \}|$
- (ii)  $|\{ i \mid 1 \leq i \leq j \text{ und } x_i = ( \}| \geq |\{ i \mid 1 \leq i \leq j \text{ und } x_i = ) \}|$  für alle  $j \in \{1, \dots, n-1\}$

Klarerweise müssen legale Klammerausdrücke stets eine gerade Länge besitzen. Die  $n$ -te *Catalanzahl*  $C_n$  ist definiert als die Anzahl legaler Klammerausdrücke mit genau  $n$  öffnenden Klammern;  $C_0 =_{\text{def}} 1$ .

### Beispiele:

1.  $C_1 = 1$ , denn  $()$  ist einziger legaler Klammerausdruck mit einer öffnenden Klammer.
2.  $C_2 = 2$ , denn  $()()$  und  $(())$  sind die einzigen legalen Klammerausdrücke mit zwei öffnenden Klammer.
3.  $C_3 = 5$ , denn  $()()()$ ,  $(())()$ ,  $()(())$ ,  $(())()$  und  $((()))$  sind die einzigen legalen Klammerausdrücke mit drei öffnenden Klammer.

Catalanzahlen können gemäß folgender Rekursion bestimmt werden.

**Lemma 2.7** Für alle  $n \in \mathbb{N}_+$  gilt

$$C_n = \sum_{k=1}^n C_{k-1} \cdot C_{n-k}.$$

**Beweis:** (*kombinatorisch*) Es sei  $A_{n,k}$  die Menge legaler Klammerausdrücke, bei denen die erste öffnende Klammer an der Position  $2k$  geschlossen wird, d.h., Wörter der Form

$$\left( \underbrace{\quad v \quad}_{1 \quad 2k} \right) \underbrace{\quad w \quad}_{2n}$$

Das Wort  $v$  enthält  $k - 1$  öffnende Klammern,  $w$  enthält  $n - k$  öffnende Klammern. Somit folgt  $|A_{n,k}| = C_{k-1} \cdot C_{n-k}$ . Wegen  $A_{n,k} \cap A_{n,k'} = \emptyset$  für  $k \neq k'$  gilt

$$C_n = \left| \bigcup_{k=1}^n A_{n,k} \right| = \sum_{k=1}^n |A_{n,k}| = \sum_{k=1}^n C_{k-1} \cdot C_{n-k}.$$

Damit ist das Lemma bewiesen. ■

**Theorem 2.8** Für alle  $n \in \mathbb{N}$  gilt

$$C_n = \frac{1}{n+1} \binom{2n}{n}$$

**Beweis:** Wir verwenden die Methode der erzeugenden Funktion.

1. *Aufstellen der erzeugenden Funktion als Potenzreihe:* Wir definieren  $C(x)$  als

$$C(x) =_{\text{def}} \sum_{n=0}^{\infty} C_n \cdot x^n$$

2. *Anwendung der Rekursionsgleichung:* Mit Hilfe von Lemma 2.7 erhalten wir

$$C(x) = 1 + \sum_{n=1}^{\infty} C_n \cdot x^n = 1 + \sum_{n=1}^{\infty} \left( \sum_{k=1}^n C_{k-1} \cdot C_{n-k} \right) x^n$$

3. *Umformen der rechten Seite nach der erzeugenden Funktion:* Wir rechnen weiter aus

$$\begin{aligned} C(x) &= 1 + \sum_{n=1}^{\infty} \left( \sum_{k=1}^n C_{k-1} \cdot C_{n-k} \right) x^n \\ &= 1 + \sum_{n=1}^{\infty} \left( \sum_{k=0}^{n-1} C_k \cdot C_{n-1-k} \right) x^n \\ &= 1 + x \cdot \sum_{n=1}^{\infty} \left( \sum_{k=0}^{n-1} C_k \cdot C_{n-1-k} \right) x^{n-1} \\ &= 1 + x \cdot \sum_{n=0}^{\infty} \left( \sum_{k=0}^n C_k \cdot C_{n-k} \right) x^n \\ &= 1 + x \cdot \left( \sum_{n=0}^{\infty} C_n \cdot x^n \right)^2 \\ &= 1 + x \cdot C(x)^2 \end{aligned}$$

4. *Auflösen nach der erzeugenden Funktion:* Es gilt also  $0 = x \cdot C(x)^2 - C(x) + 1$  bzw.

$$\left(C(x) - \frac{1}{2x}\right)^2 - \frac{1}{4x^2} + \frac{1}{x} = 0.$$

Somit folgt  $\left|C(x) - \frac{1}{2x}\right| = \frac{\sqrt{1-4x}}{2x}$ , d.h.

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

Wegen  $C(0) = C_0 = 1$  entfällt die Lösung für  $+$  und die erzeugende Funktion ist:

$$C(x) = \frac{1 - \sqrt{1-4x}}{2x}$$

5. *Ersetzen der neuen rechten Seite durch eine Potenzreihe (TAYLOR-Reihe):* Um  $C(x)$  in eine Potenzreihe zu entwickeln, betrachten wir zunächst die Funktion  $f(z) =_{\text{def}} \sqrt{1-z}$ . Für  $n \geq 1$  gilt:

$$f^{(n)}(z) = -\frac{1}{2} \cdot \prod_{k=1}^{n-1} \frac{2k-1}{2} \cdot (1-z)^{-k+\frac{1}{2}} \quad (2.4)$$

Gleichung (2.4) beweisen wir mittels vollständiger Induktion über  $n$ :

- *Induktionsanfang:* Für  $n = 1$  gilt  $f'(z) = \left((1-z)^{\frac{1}{2}}\right)' = -\frac{1}{2} \cdot (1-z)^{-\frac{1}{2}}$ .
- *Induktionsschritt:* Für  $n > 1$  gilt mit Hilfe der Induktionsvoraussetzung

$$\begin{aligned} f^{(n)}(z) &= \left(f^{(n-1)}(z)\right)' \\ &= -\frac{1}{2} \cdot \prod_{k=1}^{n-2} \frac{2k-1}{2} \cdot \left((1-z)^{-(n-1)+\frac{1}{2}}\right)' \\ &= -\frac{1}{2} \cdot \prod_{k=1}^{n-2} \frac{2k-1}{2} \cdot \underbrace{\left(-\left(n-1\right) + \frac{1}{2}\right)}_{-\frac{2n-1}{2}} \cdot (1-z)^{-(n-1)+\frac{1}{2}-1} \cdot (-1) \\ &= -\frac{1}{2} \cdot \prod_{k=1}^{n-1} \frac{2k-1}{2} \cdot (1-z)^{-n+\frac{1}{2}} \end{aligned}$$

Damit ist die Gleichung (2.4) gezeigt und wir erhalten für  $f(z)$  die folgende TAYLOR-Reihe:

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} \cdot z^n$$

$$\begin{aligned}
&= 1 + \sum_{n=1}^{\infty} \frac{f^{(n)}(0)}{n!} \cdot z^n \\
&= 1 + \sum_{n=1}^{\infty} \left(-\frac{1}{2}\right) \cdot \frac{1}{n!} \cdot \prod_{k=1}^{n-1} \frac{2k-1}{2} \cdot z^n \\
&= 1 - \frac{1}{2} \cdot \sum_{n=0}^{\infty} \frac{1}{(n+1)!} \cdot \prod_{k=1}^n \frac{2k-1}{2} \cdot z^{n+1} \\
&= 1 - \frac{z}{2} \cdot \sum_{n=0}^{\infty} \frac{1}{(n+1)!} \cdot \prod_{k=1}^n \frac{2k-1}{2} \cdot z^n
\end{aligned}$$

Daraus folgt nun für  $1 - \sqrt{1-4x} = 1 - f(4x)$ :

$$\begin{aligned}
1 - \sqrt{1-4x} &= 1 - \left(1 - \frac{4x}{2} \cdot \sum_{n=0}^{\infty} \frac{1}{(n+1)!} \cdot \prod_{k=1}^n \frac{2k-1}{2} \cdot 4^n \cdot x^n\right) \\
&= 2x \cdot \sum_{n=0}^{\infty} \frac{2^n}{(n+1)!} \cdot \prod_{k=1}^n (2k-1) \cdot x^n
\end{aligned}$$

Mithin erhalten wir für die erzeugende Funktion  $C(x)$ :

$$C(x) = \sum_{n=0}^{\infty} \frac{2^n}{(n+1)!} \cdot \prod_{k=1}^n (2k-1) \cdot x^n$$

6. *Koeffizientenvergleich:* Aus der Potenzreihendarstellung von  $C(x)$  gewinnen für  $n \in \mathbb{N}$ :

$$\begin{aligned}
C_n &= \frac{2^n}{(n+1)!} \cdot \prod_{k=1}^n (2k-1) \\
&= \frac{2^n}{(n+1)!} \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1) \cdot \frac{2 \cdot 4 \cdot 6 \cdot \dots \cdot (2n)}{2 \cdot 4 \cdot 6 \cdot \dots \cdot (2n)} \\
&= \frac{2^n}{(n+1)!} \cdot \frac{(2n)!}{2^n \cdot n!} \\
&= \frac{1}{n+1} \binom{2n}{n}
\end{aligned}$$

Damit ist das Theorem bewiesen. ■



Graphen sind kombinatorische Strukturen zur Beschreibung binärer Relationen. Binäre Relationen sind entweder symmetrisch oder nicht symmetrisch. Dementsprechend gibt es unterschiedliche Typen von Graphen.

## 3.1 Gerichtete und ungerichtete Graphen

Wir beginnen zunächst mit dem Studium ungerichteter Graphen, da sich viele Sachverhalte für diese einfacher beschreiben lassen. Eine Erweiterung auf den Fall gerichteter Graphen ist meist leicht möglich und nur fallweise erklärungsbedürftig.

**Definition 3.1** Ein Graph  $G$  ist ein Paar  $(V, E)$ , wobei  $V$  eine endliche, nichtleere Menge von Knoten (oder Ecken) ist und  $E$  eine Teilmenge aller zweielementigen Teilmengen von  $V$  ist:

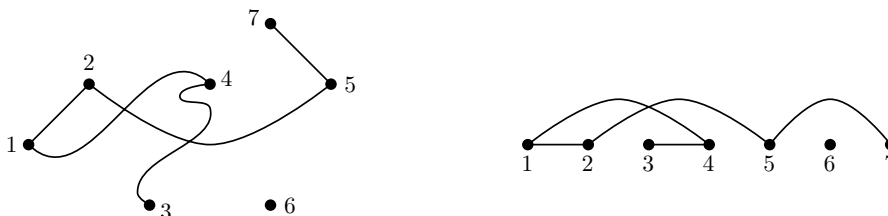
$$E \subseteq \mathcal{P}_2(V) =_{\text{def}} \{ \{x, y\} \mid x, y \in V \wedge x \neq y \}$$

Die Elemente von  $E$  heißen Kanten.

Ein Graph  $G = (V, E)$  kann wie folgt visualisiert werden:

- Die Knotenmenge  $V = \{v_1, \dots, v_n\}$  wird durch eine Menge von Punkten in der Ebene dargestellt.
- Für eine Kante  $e = \{v_i, v_k\} \in E$  verbinden wir  $v_i$  und  $v_k$  mit einer Linie.

**Beispiel:** Der Graph  $G = (V, E)$  mit Knotenmenge  $V = \{1, 2, 3, 4, 5, 6, 7\}$  und Kantenmenge  $E = \{ \{1, 2\}, \{1, 4\}, \{2, 5\}, \{3, 4\}, \{5, 7\} \}$  kann auf die beiden folgenden Arten dargestellt werden:



Wir unterscheiden zwischen *markierten* und *unmarkierten* Graphen. Bei einem markierten Graphen spielen die Namen der Knoten eine Rolle, wobei wir den jeweiligen Namen direkt neben den Knoten schreiben. Bei unmarkierten Graphen lassen wir die Knotennamen weg.

**Definition 3.2** *Es seien  $G = (V, E)$  und  $G' = (V', E')$  Graphen.  $G$  heißt isomorph zu  $G'$ , symbolisch:  $G \simeq G'$ , wenn es eine bijektive Funktion  $\varphi : V \rightarrow V'$  gibt mit*

$$\{u, v\} \in E \iff \{\varphi(u), \varphi(v)\} \in E'$$

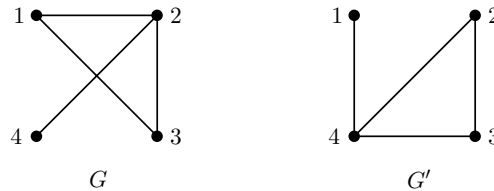
für alle  $u, v \in V$ . Die Funktion  $\varphi$  heißt (Graph-)Isomorphismus.

Anschaulich sind zwei Graphen genau dann isomorph, wenn sie mit dem gleichen Bild (ohne Knotennamen) gezeichnet werden können. Mit unmarkierten Graphen sind also gleichzeitig alle isomorphen Graphen mitgemeint.

**Beispiel:** Wir betrachten die beiden Graphen  $G = ([4], E)$  und  $G' = ([4], E')$  mit derselben Knotenmenge  $[4] = \{1, 2, 3, 4\}$  und den Kantenmengen

$$E =_{\text{def}} \{ \{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\} \}, \quad E' =_{\text{def}} \{ \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\} \}.$$

Bei gleicher Positionierung der Knoten ergeben sich die folgenden Abbildungen:



Wie nun leicht einzusehen ist, definiert die bijektive Funktion  $\varphi : [4] \rightarrow [4]$  mit

$$\varphi : 1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 3, 4 \mapsto 1$$

einen Isomorphismus von  $G$  nach  $G'$ . Für die 6 möglichen Kanten von  $G$  gilt:

$$\begin{array}{ll} \{1, 2\} \in E & \{\varphi(1), \varphi(2)\} = \{2, 4\} \in E' \\ \{1, 3\} \in E & \{\varphi(1), \varphi(3)\} = \{2, 3\} \in E' \\ \{1, 4\} \notin E & \{\varphi(1), \varphi(4)\} = \{1, 2\} \notin E' \\ \{2, 3\} \in E & \{\varphi(2), \varphi(3)\} = \{3, 4\} \in E' \\ \{2, 4\} \in E & \{\varphi(2), \varphi(4)\} = \{1, 4\} \in E' \\ \{3, 4\} \notin E & \{\varphi(3), \varphi(4)\} = \{1, 3\} \notin E' \end{array}$$

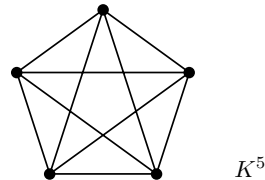
Mithin gilt  $\{u, v\} \in E \iff \{\varphi(u), \varphi(v)\} \in E'$ , also  $G \simeq G'$  (via  $\varphi$ ).

Wenn in  $G'$  jedoch eine Kante entfernt wird, dann sind die beiden Graphen klarerweise nicht mehr isomorph.

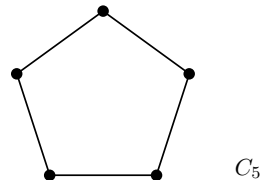


Wir erwähnen einige wichtige Typen unmarkierter Graphen.

1.  $K^n$  bezeichnet einen *vollständigen* Graphen mit  $n$  Knoten, d.h., alle Knoten sind miteinander verbunden. Der  $K^5$  kann beispielsweise wie folgt dargestellt werden:



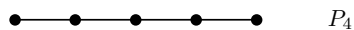
2.  $C_n$  bezeichnet einen *Kreis* mit  $n$  Knoten, die jeweils zyklisch verbunden sind. Der  $C_5$  kann beispielsweise wie folgt dargestellt werden:



Knoten- und die Kantenmenge des  $C_n$  können wie folgt definiert werden:

$$V =_{\text{def}} \{0, 1, \dots, n-1\}, \quad E =_{\text{def}} \{ \{i, j\} \mid \text{mod}(i+1, n) = j \}$$

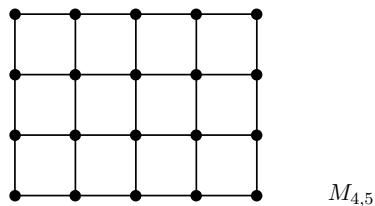
3.  $P_n$  bezeichnet einen *Pfad* mit  $n+1$  Knoten und  $n$  Kanten, die aufeinander folgende Knoten verbinden. Der  $P_4$  kann beispielsweise wie folgt dargestellt werden:



Knoten- und die Kantenmenge des  $P_n$  können wie folgt definiert werden:

$$V =_{\text{def}} \{0, 1, \dots, n\}, \quad E =_{\text{def}} \{ \{i, j\} \mid |i - j| = 1 \}$$

4.  $M_{n,m}$  bezeichnet einen *Gittergraph* mit  $n$  Zeilen und  $m$  Spalten, bei dem die Knoten jeweils zeilen- und spaltenweise verbunden sind. Der  $M_{4,5}$  kann beispielsweise wie folgt dargestellt werden:



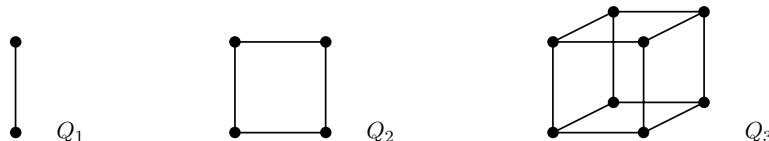
Knoten- und die Kantenmenge des  $M_{n,m}$  können wie folgt definiert werden:

$$V =_{\text{def}} \{1, \dots, n\} \times \{1, \dots, m\}, \quad E =_{\text{def}} \{ \{(i, j), (i', j')\} \mid |i - i'| + |j - j'| = 1 \}$$

5.  $Q_d$  bezeichnet den  $d$ -dimensionalen Hyperwürfel mit der Knotenmenge  $\{0, 1\}^d$  und Kanten zwischen Knoten, die sich in genau einer Komponente unterscheiden, d.h.,

$$V =_{\text{def}} \{0, 1\}^d, \quad E =_{\text{def}} \{ \{(i_1, \dots, i_d), (j_1, \dots, j_d)\} \mid \sum_{r=1}^d |i_r - j_r| = 1 \}$$

$Q_1$ ,  $Q_2$  und  $Q_3$  können beispielsweise wie folgt dargestellt werden:



*Bemerkung:* In verschiedenen Anwendungen werden manchmal noch zusätzliche Kanten betrachtet:

- *Schleifen:* Kanten, die Knoten  $v$  mit sich selbst verbinden
- *Mehrfachkanten:* Knoten  $u$  und  $v$  können durch mehr als eine Kante verbunden sein.

Wir betrachten ausschließlich schlichte, einfache Graphen, d.h. Graphen ohne Schleifen und Mehrfachkanten.

Ein wichtiges Unterscheidungskriterium für Knoten in einem Graphen ist ihre Nachbarschaft. Es seien  $G = (V, E)$  ein Graph,  $u, v \in V$  Knoten und  $e, f \in E$  Kanten.

- Die Knoten  $u$  und  $v$  heißen *adjazent* (oder *benachbart*), falls  $\{u, v\} \in E$  gilt.
- Der Knoten  $u$  und die Kante  $e$  heißen *inzident*, falls  $u \in e$  gilt.
- Die Kanten  $e$  und  $f$  heißen *inzident*, falls  $e \cap f \neq \emptyset$  gilt.

**Definition 3.3** Es seien  $G = (V, E)$  ein Graph und  $v \in V$  ein Knoten.

1. Die Nachbarschaft  $N_G(v)$  von  $v$  in  $G$  ist definiert als

$$N_G(v) =_{\text{def}} \{ u \in V \mid \{v, u\} \in E \}.$$

2. Der Grad  $d_G(v)$  von  $v$  in  $G$  ist definiert als

$$d_G(v) =_{\text{def}} |N_G(v)|.$$

Der Grad eines Knoten  $v$  entspricht ebenso der Anzahl der mit  $v$  inzidenten Kanten. Wenn der Graph  $G$  im Kontext klar ist, so lassen wir den Index  $G$  sowohl bei der Nachbarschaft als auch beim Grad weg.

### Beispiele:

1. Für alle Knoten  $v$  im  $K^n$  gilt  $d(v) = n - 1$ .

2. Für alle Knoten  $v$  im  $C_n$  gilt  $d(v) = 2$ .
3. Für alle Knoten  $v$  im  $Q_d$  gilt  $d(v) = d$ .

Ein Graph  $G = (V, E)$  heißt  $k$ -regulär, falls  $d(v) = k$  für alle  $v \in V$  gilt;  $G$  heißt *regulär*, falls  $G$   $k$ -regulär für irgendein  $k \in \mathbb{N}$  ist.  $K^n$ ,  $C_n$  und  $Q_d$  sind jeweils reguläre Graphen.

**Proposition 3.4** Für jeden Graphen  $G = (V, E)$  gilt

$$\sum_{v \in V} d_G(v) = 2 \cdot |E|.$$

**Beweis:** (*Doppeltes Abzählen*) Es sei  $e = \{u, v\} \in E$  eine Kante. Wie oft trägt  $e$  zu beiden Seiten der Gleichung bei?

- *Linke Seite:* Für beide Endknoten  $u$  und  $v$  trägt  $e$  jeweils 1 zum Grad bei, d.h.,  $e$  wird zweimal gezählt.
- *Rechte Seite:*  $e$  wird zweimal gezählt.

Somit wird  $e$  auf beiden Seite gleich oft gezählt und die Proposition ist bewiesen. ■

**Korollar 3.5** Für jeden Graphen  $G = (V, E)$  ist die Anzahl der Knoten mit ungeradem Grad gerade.

**Beweis:** Es sei  $V_i =_{\text{def}} \{v \in V \mid \text{mod}(d(v), 2) = i\}$ , d.h.,  $V_0$  enthält die Knoten mit geradem Grad,  $V_1$  die mit ungeradem Grad. Es gilt  $V = V_0 \cup V_1$  und  $V_0 \cap V_1 = \emptyset$ . Somit gilt mit Proposition 3.4:

$$2 \cdot |E| = \sum_{v \in V} d(v) = \sum_{v \in V_0} d(v) + \sum_{v \in V_1} d(v)$$

Damit die rechte Summe gerade wird, muss also  $|V_1|$  gerade sein und das Korollar ist bewiesen. ■

Der Knotengrad ist eine lokale Eigenschaft für einen Knoten. Die zugehörigen globalen Graphenparameter sind in folgender Definition zusammengefasst.

**Definition 3.6** Es sei  $G = (V, E)$  ein ungerichteter Graph,  $|V| = n$ .

1.  $\Delta(G) =_{\text{def}} \max \{d_G(v) \mid v \in V\}$  heißt Maximalgrad von  $G$ .
2.  $\delta(G) =_{\text{def}} \min \{d_G(v) \mid v \in V\}$  heißt Minimalgrad von  $G$ .
3.  $\bar{d}(G) =_{\text{def}} \frac{1}{n} \cdot \sum_{v \in V} d_G(v)$  heißt Durchschnittgrad von  $G$ .

Nach Proposition 3.4 gilt  $\bar{d}(G) = 2|E|/|V|$ .

**Proposition 3.7** Für jeden Graphen  $G = (V, E)$  mit  $|V| = n$  gilt

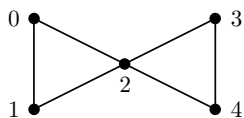
$$0 \leq \delta(G) \leq \bar{d}(G) \leq \Delta(G) \leq n - 1.$$

**Definition 3.8** Es sei  $G = (V_G, E_G)$  ein Graph.

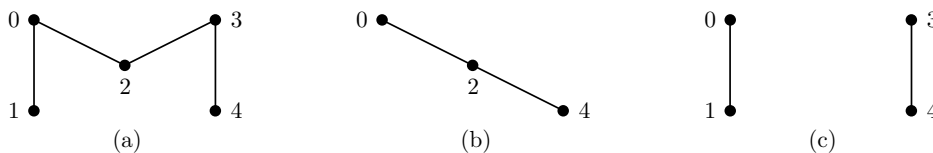
1. Ein Graph  $H = (V_H, E_H)$  heißt Teilgraph von  $G$ , symbolisch:  $H \subseteq G$ , falls  $V_H \subseteq V_G$  und  $E_H \subseteq E_G$  gilt.
2. Ein Graph  $H = (V_H, E_H)$  heißt induzierter Teilgraph von  $G$ , symbolisch:  $H = G[V_H]$ , falls  $V_H \subseteq V_G$  und  $E_H = E_G \cap \mathcal{P}_2(V_H)$ .

Ein induzierter Teilgraph  $G[V_H]$  von  $G$  ist ein kantenmaximaler Teilgraph von  $G$  mit dieser Knotenmenge, d.h., alle Kanten aus  $G$ , für die beide Endknoten in  $V_H$  liegen, gehören zu  $G[V_H]$ .

**Beispiel:** Für den Graphen  $G = (V, E)$  mit Knotenmenge  $V = \{0, 1, 2, 3, 4\}$



zeigt (a) einen Teilgraphen von  $G$ , (b) einen induzierten Teilgraphen von  $G$  und (c) den durch die Knotenmenge  $\{0, 1, 3, 4\}$  induzierten Teilgraph  $G[\{0, 1, 3, 4\}]$ :



Abschließend für diesen Abschnitt nehmen wir noch einige begriffliche Anpassungen für gerichtete Graphen vor.

**Definition 3.9** Ein gerichteter Graph  $G$  ist ein Paar  $G = (V, E)$  mit endlicher, nichtleerer Knotenmenge  $V$  und Kantenmenge

$$E \subseteq V \times V = \{ (u, v) \mid u, v \in V \}.$$

Für eine Kante  $e = (u, v) \in E$  heißt  $u$  der Startknoten und  $v$  der Endknoten.

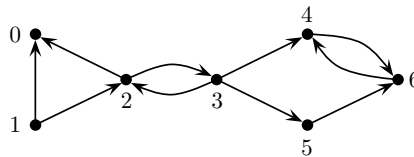
In der graphischen Repräsentierung einer gerichteten Kante  $(u, v)$  wird die Orientierung von  $u$  nach  $v$  durch  $u \rightarrow v$  wiedergegeben.

Knotengrade fallen in einem gerichteten Graph  $G = (V, E)$  auseinander nach eingehenden oder ausgehenden Kanten:

- $d_G^+(v) =_{\text{def}} |\{ u \in V \mid (v, u) \in E \}|$  ist der *Ausgangsgrad* von  $v$  in  $G$
- $d_G^-(v) =_{\text{def}} |\{ u \in V \mid (u, v) \in E \}|$  ist der *Eingangsgrad* von  $v$  in  $G$
- $d_G(v) =_{\text{def}} d_G^+(v) + d_G^-(v)$  ist der *Grad* von  $v$  in  $G$

Ein Knoten  $v$  mit  $d_G^+(v) = 0$  heißt *Senke*. Ein Knoten  $v$  mit  $d_G^-(v) = 0$  heißt *Quelle*.

**Beispiel:** In folgendem gerichteten Graphen



sind der Knoten 0 eine Senke und der Knoten 1 eine Quelle. Somit sind der minimale Ausgangsgrad  $\delta^+(G) = 0$  und der minimale Eingangsgrad  $\delta^-(G) = 0$ . Der maximale Ausgangsgrad  $\Delta^+(G)$  beträgt 2. Ebenso gilt für den maximalen Eingangsgrad  $\Delta^-(G) = 2$ . Der maximale Grad  $\Delta(G)$  ist 4 und der minimale Grad  $\delta(G) = 2$ .

## 3.2 Wege in Graphen

**Definition 3.10** Es sei  $G = (V, E)$  ein Graph.

1. Ein Weg (oder Kantenzug) der Länge  $k$  in  $G$  ist eine Folge

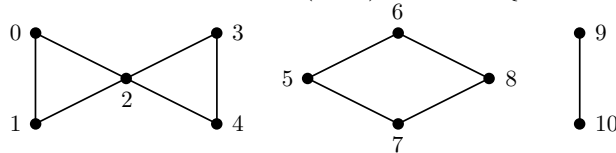
$$W =_{\text{def}} (v_0, e_1, v_1, e_2, v_2, \dots, v_{k-1}, e_k, v_k)$$

mit  $v_0, \dots, v_k \in V$ ,  $e_1, \dots, e_k \in E$  sowie  $e_i = \{v_{i-1}, v_i\}$  für alle  $i \in \{1, \dots, k\}$ . Der Knoten  $v_0$  heißt Anfangsknoten von  $W$ ; der Knoten  $v_k$  heißt Endknoten von  $W$ ; die anderen Knoten heißen innere Knoten. Eine Weg mit  $u$  als Anfangsknoten und  $v$  als Endknoten heißt  $(u, v)$ -Weg.

2. Ein Pfad in  $G$  ist ein knotendisjunkter Weg in  $G$ , d.h., alle Knoten auf dem Weg sind paarweise verschieden.
3. Ein Kreis in  $G$  ist ein Weg mit gleichem Anfangs- und Endknoten.
4. Ein einfacher Kreis in  $G$  ist ein Kreis der Länge  $k \geq 3$ , bei dem alle inneren Knoten paarweise verschieden und verschieden zum Anfangs- und Endknoten sind.

Wenn uns die Kanten nicht interessieren, dann lassen wir der Beschreibung eines Weges  $(v_0, e_1, v_1, e_2, v_2, \dots, v_{k-1}, e_k, v_k)$  die Kanten  $e_1, \dots, e_k$  weg und sprechen stattdessen vom Weg  $(v_0, v_1, \dots, v_k)$ . Dabei gilt jedoch nach wie vor  $\{v_{i-1}, v_i\} \in E$  für alle  $i \in \{1, \dots, k\}$ .

**Beispiel:** In folgendem Graphen  $G = (V, E)$  mit  $V = \{0, 1, \dots, 10\}$



sind  $(0, 1, 2)$ ,  $(0, 2, 3, 4, 2, 1)$ ,  $(5, 6, 5, 7)$  Wege der Längen 2, 5 und 3; nur  $(0, 1, 2)$  ist ein Pfad. Die Folge  $(2, 3, 4, 5, 6)$  ist kein Weg. Die Folge  $(0)$  ist ein Weg der Länge 0. Weiterhin sind  $(0, 1, 2, 0)$  und  $(6, 8, 7, 5, 6)$  einfache Kreise der Längen 3 und 4; der  $(0, 0)$ -Weg  $(0, 2, 3, 4, 2, 1, 0)$  ist ein Kreis, aber kein einfacher Kreis.

**Proposition 3.11** *Es seien  $G = (V, E)$  ein Graph und  $u, v \in V$  Knoten.*

1. *Gibt es einen  $(u, v)$ -Weg in  $G$ , so gibt es einen  $(u, v)$ -Pfad in  $G$ .*
2. *Liegt die Kante  $\{u, v\}$  auf einem kante, vndisjunkten Kreis in  $G$ , so liegt  $\{u, v\}$  auf einem einfachen Kreis in  $G$ .*

**Beweis:** Übungsaufgabe. ■

### 3.2.1 Anzahl der Wege in Graphen

Es sei  $G = (V, E)$  ein ungerichteter Graph,  $u, v \in V$  seien Knoten.

- $W_k(G)_{u,v}$  bezeichne die Anzahl der  $(u, v)$ -Wege der Länge  $k$  in  $G$ ,
- $W_k(G)_u$  bezeichne die Anzahl der Wege der Länge  $k$  in  $G$ , mit  $u$  als Anfangsknoten,
- $W_k(G)$  bezeichne die Anzahl der Wege der Länge  $k$  in  $G$ .

Es gelten folgende Zusammenhänge:

$$W_k(G)_u = \sum_{v \in V} W_k(G)_{u,v}, \quad W_k(G) = \sum_{u \in V} W_k(G)_u = \sum_{u \in V} \sum_{v \in V} W_k(G)_{u,v}$$

**Beispiele:** Folgende Beispiele verdeutlichen die Definitionen:

1. Für einen beliebigen ungerichteten Graph  $G = (V, E)$  gilt

$$W_0(G) = |V| = \sum_{v \in V} d_G(v)^0,$$

$$W_1(G) = 2|E| = \sum_{v \in V} d_G(v)^1,$$

$$W_2(G) = \sum_{v \in V} W_1(G)_v \cdot W_1(G)_v = \sum_{v \in V} d_G(v)^2.$$

Für  $k = 3$  gilt die entsprechende Formel  $W_3(G) = \sum_{v \in V} d_G(v)^3$  im Allgemeinen nicht mehr.

2. In einem  $r$ -regulären Graphen  $G = (V, E)$  mit  $|V| = n$  gilt

$$W_k(G)_u = r^k, \quad W_k(G) = n \cdot r^k.$$

Eine einfache Formel für  $W_k(G)_{u,v}$  ist hingegen nicht immer möglich.

**Proposition 3.12** Für jeden Graphen  $G = (V, E)$  mit  $|V| = n$  gilt

$$\delta(G)^k \leq W_k(G)_u \leq \Delta(G)^k, \quad n \cdot \delta(G)^k \leq W_k(G) \leq n \cdot \Delta(G)^k$$

für  $u \in V$ ,  $k \in \mathbb{N}$ . Für reguläre Graphen gilt Gleichheit.

Es sei  $G = (V, E)$  ein Graph mit  $V = [n]$  (ohne Beeinträchtigung der Allgemeinheit). Wir definieren die *Adjazenzmatrix*  $A(G) \in \{0, 1\}^{n \times n}$  mit den Einträgen  $a_{ij} = (A(G))_{ij}$  für  $i, j \in \{1, \dots, n\}$  wie folgt:

$$a_{ij} =_{\text{def}} \begin{cases} 1 & \text{falls } \{i, j\} \in E \\ 0 & \text{sonst} \end{cases}$$

Für ungerichtete Graphen  $G$  ist die Adjazenzmatrix symmetrisch, d.h.  $A_{ij} = A_{ji}$ , und auf der Diagonale stehen nur Nullen, d.h.  $A_{ii} = 0$ .

Wir verwenden Matrizenmultiplikation: Für Matrizen  $A, B \in \mathbb{R}^{n \times n}$  definieren wir wie üblich

$$(A \cdot B)_{ij} =_{\text{def}} \sum_{k=1}^n a_{ik} b_{kj}$$

für  $i, j \in \{1, \dots, n\}$ . Für Matrizen  $A, B, C \in \mathbb{R}^{n \times n}$  gilt:

- $(A \cdot B) \cdot C = A \cdot (B \cdot C)$  (d.h., Matrizenmultiplikation ist assoziativ)
- $A \cdot I = I \cdot A = A$  für die Einheitsmatrix  $I$  (d.h.,  $I_{ii} =_{\text{def}} 1$  und  $I_{ij} =_{\text{def}} 0$  für  $i \neq j$ )
- $A \cdot B \neq B \cdot A$  (im Allgemeinen)

Für  $k \in \mathbb{N}$  definieren wir die  $k$ -te Potenz von  $A$  induktiv wie folgt:

$$A^0 =_{\text{def}} I, \quad A^k =_{\text{def}} A \cdot A^{k-1} \text{ für } k > 0$$

**Lemma 3.13** *Es sei  $G = (V, E)$  ein Graph,  $V = [n]$ . Es  $A = A(G) \in \{0, 1\}^{n \times n}$  die Adjazenzmatrix von  $G$ . Für alle  $k \in \mathbb{N}$  und für alle  $i, j \in V$  gilt*

$$W_k(G)_{ij} = (A^k)_{ij}.$$

**Beweis:** (*Induktion*) Wir führen den Beweis mittels vollständiger Induktion über  $k$ :

- *Induktionsanfang  $k = 0$ :* Für  $i \neq j$  gilt  $W_0(G)_{ij} = 0 = I_{ij} = (A^0)_{ij}$ . Weiterhin gilt  $W_0(G)_{ii} = 1 = I_{ii} = (A^0)_{ii}$ .
- *Induktionsschritt  $k > 0$ :* Es sei  $B =_{\text{def}} A^{k-1}$ . Dann gilt  $A^k = A \cdot B$ . Außerdem gilt nach Induktionsvoraussetzung  $b_{ij} = W_{k-1}(G)_{ij}$  für alle  $i, j \in \{1, \dots, n\}$ . Somit erhalten wir:

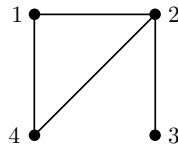
$$W_k(G)_{ij} = \sum_{\ell \in N_G(i)} W_{k-1}(G)_{\ell j} = \sum_{\ell \in N_G(i)} b_{\ell j} = \sum_{\ell=1}^n a_{i\ell} b_{\ell j} = (A \cdot B)_{ij} = (A^k)_{ij}$$

Damit ist das Lemma bewiesen. ■

**Korollar 3.14** *Es sei  $A = A(G)$  die Adjazenzmatrix von  $G = (V, E)$ ,  $V = [n]$ . Dann gilt:*

1.  $(A^2)_{ii} = d_G(i)$  für alle  $i \in \{1, \dots, n\}$
2.  $(A^3)_{ii} = 2 \cdot \text{triad}_G(i)$  für alle  $i \in \{1, \dots, n\}$ , wobei  $\text{triad}_G(i)$  die Anzahl der Dreiecke  $K^3$  ist, die  $i$  enthalten.

**Beispiel:** Für den Graphen  $G = ([4], E)$  und die Adjazenzmatrix  $A(G)$



erhalten wir als Adjazenzmatrix

$$A(G) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

Für  $k = 2$  ergibt sich:

$$A^2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 3 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}$$



Damit erhalten wir die Knotengrade 2, 3, 1, 2 für die Knoten 1, 2, 3, 4.

Für  $k = 3$  ergibt sich nun:

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

Das einzige Dreieck im Graphen bilden die Knoten 1, 2, 4. Dies entspricht gemäß obiger Formel genau den Einträgen 2, 2, 0, 2 auf der Diagonale.

### 3.2.2 Distanzen in Graphen

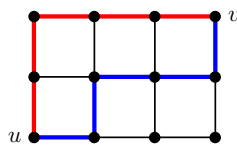
**Definition 3.15** Es sei  $G = (V, E)$  ein Graph. Für Knoten  $u, v \in V$  ist der Abstand (oder die Distanz)  $\text{dist}_G(u, v)$  definiert als die kürzeste Länge eines  $(u, v)$ -Weges, d.h.

$$\text{dist}_G(u, v) =_{\text{def}} \min \{ k \in \mathbb{N} \mid \text{es gibt einen } (u, v)\text{-Weg der Länge } k \},$$

wobei  $\text{dist}_G(u, v) =_{\text{def}} \infty$ , falls kein  $(u, v)$ -Weg in  $G$  existiert.

Offenbar ist ein kürzester  $(u, v)$ -Weg stets ein Pfad. Im Allgemeinen muss ein kürzester  $(u, v)$ -Weg nicht eindeutig sein.

**Beispiel:** Für die Knoten  $u$  und  $v$  im  $M_{3,4}$  gilt  $\text{dist}_G(u, v) = 5$ .



Angegeben sind mindestens zwei der kürzesten Wege.

**Proposition 3.16** Es sei  $G = (V, E)$  ein ungerichteter Graph. Für die  $u, v, w \in V$  gilt:

1.  $\text{dist}_G(v, v) \geq 0$  und  $\text{dist}_G(u, v) = 0 \Leftrightarrow u = v$  (positive Definitheit)
2.  $\text{dist}_G(u, v) = \text{dist}_G(v, u)$  (Symmetrie)
3.  $\text{dist}_G(u, v) \leq \text{dist}_G(u, w) + \text{dist}_G(w, v)$  (Dreiecksungleichung)
4.  $\text{dist}_G(u, v) = \text{dist}_G(u, w) + \text{dist}_G(w, v)$ , falls  $w$  auf einem kürzesten  $(u, v)$ -Weg liegt

Mit anderen Worten:  $\text{dist}_G$  ist eine Metrik auf der Knotenmenge  $V$  von  $G = (V, E)$ .

**Beweis:** Wir bewiesen die Aussagen einzeln für beliebige Knoten  $u, v, w \in V$  eines ungerichteten Graphen  $G = (V, E)$ :

1. Klar.
2. Klar ( $G$  ist ungerichtet).
3. Es seien  $W_u = (u, \dots, w)$  und  $W_v = (w, \dots, v)$  kürzeste  $(u, w)$ - bzw.  $(w, v)$ -Wege. Dann gibt es auch den  $(u, v)$ -Weg  $W = (u, \dots, w, \dots, v)$  in  $G$ . Die Länge von  $W$  ist gerade  $\text{dist}_G(u, w) + \text{dist}_G(w, v)$ . Folglich gilt

$$\text{dist}_G(u, w) + \text{dist}_G(w, v) \geq \text{dist}_G(u, v).$$

4. Der Knoten  $w$  liege auf einem kürzesten  $(u, v)$ -Weg  $W$  der Länge  $k = \text{dist}_G(u, v)$  in  $G$ ,  $W = (v_0, \dots, v_\ell, \dots, v_k)$  mit  $v_0 = u$ ,  $v_\ell = w$  und  $v_k = v$ . Dann gilt sowohl  $\text{dist}_G(u, w) \leq \ell$  als auch  $\text{dist}_G(w, v) \leq k - \ell$ . Mithin erhalten wir

$$\text{dist}_G(u, w) + \text{dist}_G(w, v) \leq \ell + k - \ell = k = \text{dist}_G(u, v) \leq \text{dist}_G(u, w) + \text{dist}_G(w, v);$$

letzteres mit der Dreiecksungleichung. Somit gilt

$$\text{dist}_G(u, w) + \text{dist}_G(w, v) = \text{dist}_G(u, v).$$

Damit ist die Proposition bewiesen. ■

**Definition 3.17** *Es sei  $G = (V, E)$  ein Graph.*

1. Der Durchmesser  $\text{diam}(G)$  von  $G$  ist der längste kürzeste Weg zwischen zwei Knoten  $u, v \in V$ , d.h.

$$\text{diam}(G) =_{\text{def}} \max \{ \text{dist}_G(u, v) \mid u, v \in V \}$$

2. Ein Knoten  $u \in V$  heißt (Abstands-)zentral in  $G$ , falls für alle Knoten  $v \in V$  gilt:

$$\max \{ \text{dist}_G(u, w) \mid w \in V \} \leq \max \{ \text{dist}_G(v, w) \mid w \in V \}$$

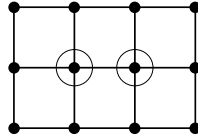
Der Radius  $\text{rad}(G)$  ist der maximale Abstand eines zentralen Knotens zu einem anderen Knoten, also gerade die linke Seite der Ungleichung.

Wie zu erwarten, gilt stets  $\text{rad}(G) \leq \text{diam}(G) \leq 2 \cdot \text{rad}(G)$ .

**Beispiel:**

1. Es gilt  $\text{diam}(C_{2n}) = n$ ,  $\text{diam}(C_{2n+1}) = n$ .

2. Es gilt  $\text{rad}(M_{3,4}) = 3$  mit den zentralen Knoten:



**Proposition 3.18** Enthält  $G = (V, E)$  einen einfachen Kreis, so gilt

$$g(G) \leq 2 \cdot \text{diam}(G) + 1,$$

wobei  $g(G)$  die Tailleweite von  $G$  ist, d.h.,  $g(G)$  ist die minimale Länge eines einfachen Kreises in  $G$ .

**Beweis:** Übungsaufgabe. ■

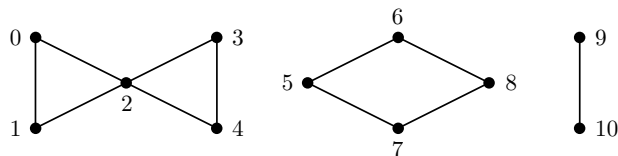
### 3.2.3 Zusammenhang in Graphen

**Definition 3.19** Es seien  $G = (V, E)$  ein Graph und  $C \subseteq G$  ein induzierter Teilgraph.

1.  $G$  heißt zusammenhängend, falls für jedes Paar von Knoten  $u, v \in V$  ein  $(u, v)$ -Pfad in  $G$  existiert.
2.  $C$  heißt Zusammenhangskomponente von  $G$ , falls  $C$  zusammenhängend und ein knotenmaximaler induzierter Teilgraph mit dieser Eigenschaft ist.

Jeder Knoten  $v$  eines Graphen  $G = (V, E)$  liegt in einer Zusammenhangskomponente, denn der induzierte Teilgraph  $G[\{v\}]$  ist beispielsweise zusammenhängend. Außerdem sind zwei Zusammenhangskomponenten entweder identisch oder knotendisjunkt. Somit lässt sich die Knotenmenge als disjunkte Vereinigung von Komponenten  $V_1, \dots, V_\ell$  schreiben. Es ist üblich, sowohl  $V_j$  als auch den induzierten Teilgraph  $G[V_j]$  als Zusammenhangskomponente zu bezeichnen.

**Beispiel:** Der schon bekannte Graph  $G = (V, E)$



besteht aus den Teilgraphen  $G[\{0, 1, 2, 3, 4\}]$ ,  $G[\{5, 6, 7, 8\}]$  und  $G[\{9, 10\}]$  und den zugehörigen Komponenten.

**Theorem 3.20** Jeder Graph  $G = (V, E)$  enthält mindestens  $|V| - |E|$  Zusammenhangskomponenten.

**Beweis:** (*Vollständige Induktion*) Wir beweisen den Satz mittels Induktion über  $m = |E|$ .

- *Induktionsanfang:* Es sei  $m = 0$ . Somit bildet jeder Knoten eine eigene Zusammenhangskomponente. Mithin enthält  $G$  genau  $|V| = |V| - 0 = |V| - |E|$  Komponenten.
- *Induktionsschritt:* Es sei  $m > 0$ . Somit gibt es eine Kante  $e \in E$ . Wir wählen eine feste Kante  $e \in E$  und betrachten den Graph  $G' = (V, E')$  mit  $E' =_{\text{def}} E \setminus \{e\}$ . Es gilt  $|E'| = m - 1$  und wir können die Induktionsvoraussetzung anwenden. Damit enthält  $G'$  mindestens

$$|V| - |E'| = |V| - (m - 1) = |V| - m + 1$$

Komponenten. Beim Einfügen von  $e$  in  $G'$  können zwei Fälle auftreten:

1. Beide Endknoten von  $e$  liegen in einer Zusammenhangskomponente von  $G'$ . Dann sind die Anzahlen der Komponenten in  $G$  und  $G'$  gleich.
2. Die Endknoten von  $e$  liegen in verschiedenen Zusammenhangskomponenten von  $G'$ . Damit ist die Anzahl der Komponenten von  $G$  um genau 1 kleiner als die Anzahl der Komponenten von  $G'$ .

Insgesamt enthält  $G$  somit mindestens

$$\begin{aligned} & (\text{Anzahl der Komponenten von } G') - 1 \\ &= (|V| - m + 1) - 1 = |V| - m = |V| - |E| \end{aligned}$$

Komponenten.

Damit ist das Theorem bewiesen. ■

**Korollar 3.21** Für jeden zusammenhängenden Graph  $G = (V, E)$  gilt  $|E| \geq |V| - 1$ .

**Beweis:** Ein zusammenhängender Graph besteht aus genau einer Zusammenhangskomponente. Nach Theorem 3.20 gilt somit  $1 \geq |V| - |E|$ . Durch Umstellung der Ungleichung nach  $|E|$  ergibt sich das Korollar. ■

**Definition 3.22** Es sei  $G = (V, E)$  ein gerichteter Graph,  $C \subseteq V$ .

1.  $G$  heißt (schwach) zusammenhängend, falls der zu Grunde liegende ungerichtete Graph  $G = (V, \{ \{u, v\} \mid (u, v) \in E \})$  zusammenhängend ist.
2.  $G$  heißt stark zusammenhängend, falls für alle Knoten  $u, v \in V$  jeweils ein  $(u, v)$ -Weg und ein  $(v, u)$ -Weg in  $G$  existiert.
3.  $C$  heißt starke (Zusammenhangs)Komponente von  $G$ , falls  $G[C]$  stark zusammenhängend und knotenmaximal mit dieser Eigenschaft ist.

### 3.2.4 Mehrfacher Zusammenhang in Graphen\*

Wir führen Parameter ein, um den Zusammenhang in einem Graphen zu quantifizieren.

**Definition 3.23** Es sei  $G = (V, E)$  ein Graph,  $k, \ell \in \mathbb{N}$ .

1.  $G$  heißt  $k$ -zusammenhängend (oder  $k$ -fach zusammenhängend), falls  $|V| > k$  und für jede Knotenmenge  $X \subseteq V$  mit  $|X| < k$  der Graph  $G[V \setminus X]$  zusammenhängend ist. Der (Knoten)Zusammenhang  $\kappa(G)$  von  $G$  ist definiert als

$$\kappa(G) =_{\text{def}} \max \{ k \mid G \text{ ist } k\text{-zusammenhängend} \}.$$

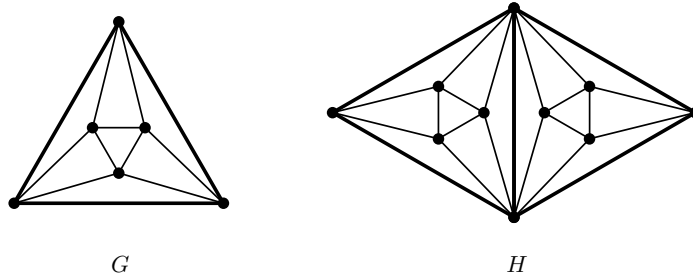
2.  $G$  heißt  $\ell$ -kanten zusammenhängend (oder  $\ell$ -fach kanten zusammenhängend), falls  $|V| > 1$  und für jede Kantenmenge  $X \subseteq E$  mit  $|X| < \ell$  der Graph  $(V, E \setminus X)$  zusammenhängend ist. Der Kantenzusammenhang  $\lambda(G)$  von  $G$  ist definiert als

$$\lambda(G) =_{\text{def}} \max \{ \ell \mid G \text{ ist } \ell\text{-kanten zusammenhängend} \}.$$

Natürlich ist jeder  $k$ -zusammenhängende Graph  $(k - 1)$ -zusammenhängend für  $k > 0$  und jeder  $\ell$ -kanten zusammenhängende Graph auch  $(\ell - 1)$ -kanten zusammenhängend für  $\ell > 1$ .

**Beispiele:** Wir verdeutlichen die Begriffsbildungen:

1. Jeder nichtleere Graph ist 0-zusammenhängend.
2. Jeder zusammenhängende Graph (mit mindestens einer Kante) ist 1-zusammenhängend.
3.  $\kappa(K^n) = \lambda(K^n) = n - 1$ .
4. Ist  $G$  nicht zusammenhängend, so gilt  $\kappa(G) = \lambda(G) = 0$ .
5. Für die folgenden Graphen  $G$  und  $H$



gilt  $\kappa(G) = \lambda(G) = 4$  und  $\kappa(H) = 2, \lambda(H) = 4$ .

**Proposition 3.24** Für Graphen  $G = (V, E)$  mit  $|V| \geq 2$  gilt  $\kappa(G) \leq \lambda(G) \leq \delta(G)$ .

**Beweis:** Für  $\lambda(G) \leq \delta(G)$  betrachten wir einen Knoten  $v \in V$  mit  $d_G(v) = \delta(G) = \ell$ . Sind  $e_1, \dots, e_\ell$  die mit  $v$  inzidenten Kanten, so ist der Graph  $(V, E \setminus \{e_1, \dots, e_\ell\})$  nicht zusammenhängend. Somit gilt  $\lambda(G) \leq \ell = \delta(G)$ .

Für  $\kappa(G) \leq \lambda(G)$  sei  $X \subseteq E$  mit  $|X| = \lambda(G)$ , sodass  $(V, E \setminus X)$  nicht zusammenhängend ist. Wir führen eine Fallunterscheidung:

1. Es gibt einen Knoten  $v \in V$ , der mit keiner Kante  $e \in X$  inzident ist, d.h.,  $v \cap e = \emptyset$  für alle  $e \in X$ . Es sei  $C$  die Komponente von  $(V, E \setminus X)$ , die  $v$  enthält. Es seien  $v_1, \dots, v_r \in C$  Knoten, die mit Kanten in  $X$  inzident sind. Insbesondere gilt  $r \in |X|$ , da es keine Kante  $e = \{x, y\} \in X$  mit  $x, y \in C$  gibt. Dann ist  $G[V \setminus \{v_1, \dots, v_r\}]$  nicht zusammenhängend. Somit gilt  $\kappa(G) \leq r \leq \lambda(G)$ .
2. Jeder Knoten  $v \in V$  ist mit einer Kante  $e \in X$  inzident. Es sei  $v \in V$  beliebig,  $C$  sei die  $v$  enthaltende Komponente von  $(V, E \setminus X)$ . Für alle  $w \in N_G(v)$  mit  $\{v, w\} \notin X$  gilt  $w \in C$ . Damit gilt  $d_G(v) \leq |X|$ , da jedes  $w$  mit einer Kante aus  $X$  inzident ist. Somit ist  $G[V \setminus N_G(v)]$  nicht zusammenhängend. Mithin  $\kappa(G) \leq d_G(v) \leq |X| = \lambda(G)$ .

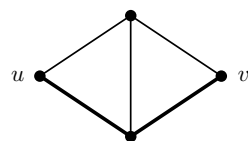
Damit ist die Proposition bewiesen. ■

Für Knoten  $u, v \in V$  von  $G = (V, E)$  heißt eine Menge  $X \subseteq V \setminus \{u, v\}$  ein  $(u, v)$ -Trenner in  $G$ , falls  $u$  und  $v$  in  $G[V \setminus X]$  zu verschiedenen Zusammenhangskomponenten gehören. Insbesondere gibt es dann also keinen  $(u, v)$ -Weg in  $G[V \setminus X]$ . Es sei  $k_G(u, v)$  die minimale Kardinalität eines  $(u, v)$ -Trenners in  $G$ . Zwei  $(u, v)$ -Pfade heißen *(knoten)disjunkt*, falls sie keine gemeinsamen inneren Knoten enthalten. Es sei  $\mu_G(u, v)$  die maximale Anzahl paarweise disjunkter  $(u, v)$ -Pfade in  $G$ . Es gilt:  $\mu_G(u, v) \leq k_G(u, v)$  für  $\{u, v\} \notin E$ .

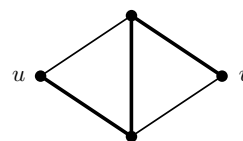
**Theorem 3.25 (Menger – lokale Version)** *Es sei  $G = (V, E)$  ein Graph. Für unterschiedliche Knoten  $u, v \in V$  mit  $\{u, v\} \notin E$  gilt  $k_G(u, v) = \mu_G(u, v)$ .*

**Beweis:** Wir beweisen die Aussage mittels Induktion über die Anzahl  $m = |E|$  der Kanten von  $G$ .

- *Induktionsanfang  $m = 0$ :* Es sei  $G$  ein leerer Graph. Dann liegen  $u$  und  $v$  in verschiedenen Komponenten. Damit ist  $\emptyset$  ein  $(u, v)$ -Trenner und es gibt keinen  $(u, v)$ -Pfad in  $G$ . Mithin gilt  $k_G(u, v) = \mu_G(u, v) = 0$ .
- *Induktionsschritt  $m > 0$ :* Es sei  $G = (V, E)$  ein Graph mit  $|E| = m$  Kanten. Wir führen eine Fallunterscheidung an Hand der Länge induzierter  $(u, v)$ -Pfade. Ein Pfad  $P = (v_0, v_1, \dots, v_r)$  der Länge  $r$  in  $G$  heißt *induziert* in  $G$ , falls  $G[\{v_0, v_1, \dots, v_r\}]$  ein Pfad ist. Induzierte Pfade erlauben keine Abkürzungen im Graphen.



induzierter Pfad



kein induzierter Pfad

Wir unterscheiden zwei Fälle:

1. Alle induzierten  $(u, v)$ -Pfade haben die Länge  $\leq 2$  (siehe die Abbildung oben). Wegen  $\{u, v\} \notin E$  haben alle induzierten  $(u, v)$ -Pfade genau die Länge 2. Wir definieren

$$X =_{\text{def}} \{ w \in V \mid w \text{ ist innerer Knoten auf einem induzierten } (u, v)\text{-Pfad} \}.$$

Dann gilt:

- (i)  $X$  ist  $(u, v)$ -Trenner in  $G$ : Dazu sei  $W$  ein  $(u, v)$ -Pfad in  $G$ . Dann gibt es einen inneren Knoten  $w$  auf  $W$ , der auf einem induzierten  $(u, v)$ -Pfad liegt, d.h.  $w \in X$ . Somit gibt es den  $(u, v)$ -Pfad  $W$  in  $G[V \setminus X]$  nicht.
- (ii) Die Pfade  $(u, w, v)$  für  $w \in X$  sind paarweise disjunkt.

Damit gilt  $|X| \leq \mu_G(u, v) \leq k_G(u, v) \leq |X|$ , mithin  $\mu_G(u, v) = k_G(u, v)$ .

2. Es gibt einen induzierten  $(u, v)$ -Pfad der Länge  $\geq 3$ . Es sei  $W = (u, v_1, \dots, v_r, v)$  ein solcher Pfad,  $r \geq 2$ . Es gilt  $\{u, v_2\} \notin E$  und  $\{v_1, v\} \notin E$ . Wir kontrahieren die Kante  $e = \{u, v_1\}$ . Dabei entsteht der Graph  $G' = (V', E')$  wie folgt:

$$\begin{aligned} V' &=_{\text{def}} V \setminus \{u, v_1\} \cup \{x\}, \quad \text{wobei } x \notin V \\ E' &=_{\text{def}} E \setminus \{ f \in E \mid u \in f \text{ oder } v_1 \in f \} \\ &\quad \cup \{ \{x, w\} \mid \{u, w\} \in E \text{ oder } \{v_1, w\} \in E \} \end{aligned}$$

Es gilt:  $|E'| < m$ ,  $\{x, v\} \notin E'$  und außerdem  $\mu_G(u, v) = \mu_{G'}(x, v)$ . Nach Induktionsvoraussetzung gibt es einen  $(x, v)$ -Trenner  $X \subseteq V' \setminus \{x, v\} = V \setminus \{u, v_1, v\}$  mit  $|X| = \mu_{G'}(x, v)$ . Somit ist  $X \subseteq V \setminus \{u, v\}$  auch ein  $(u, v)$ -Trenner in  $G$ . Damit gilt  $\mu_G(u, v) = \mu_{G'}(x, v) = |X| \geq k_G(u, v) \geq \mu_G(u, v)$  und mithin  $\mu_G(u, v) = k_G(u, v)$ .

Damit ist das Theorem bewiesen. ■

Die globale Version von Theorem 3.25 formulieren wir sowohl für den Knoten- als auch den Kantenzusammenhang.

**Theorem 3.26 (Menger – globale Version)** *Es sei  $G = (V, E)$  ein Graph,  $k, \ell \in \mathbb{N}$ .*

1.  $G$  ist genau dann  $k$ -zusammenhängend, wenn für alle unterschiedlichen Knoten  $u, v \in V$  mindestens  $k$  paarweise disjunkte  $(u, v)$ -Pfade in  $G$  existieren.
2.  $G$  ist genau dann  $\ell$ -kantenzusammenhängend, wenn für alle unterschiedlichen Knoten  $u, v \in V$  mindestens  $\ell$  paarweise kantendisjunkte  $(u, v)$ -Pfade in  $G$  existieren.

**Beweis:** (*nur 1. Aussage*) Wir zeigen die beiden Richtungen getrennt.

- ( $\Leftarrow$ ): Gibt es für alle Knoten  $u, v$  zumindest  $k$  paarweise disjunkte  $(u, v)$ -Pfade, so können mit einem beliebigen  $X \subseteq V$ ,  $|X| < k$ , in  $G[V \setminus X]$  nicht alle zerstört werden.  $G$  ist somit  $k$ -zusammenhängend.
- ( $\Rightarrow$ ): Es sei  $G = (V, E)$  ein  $k$ -zusammenhängender Graph,  $|V| > k$ . Angenommen es gibt Knoten  $u, v \in V$  mit  $\mu_G(u, v) < k$ .
  1.  $\{u, v\} \notin E$ : Nach Theorem 3.25 gibt es einen  $(u, v)$ -Trenner  $X$  mit  $|X| < k$ . Dann liegen  $u$  und  $v$  in verschiedenen Komponenten von  $G[V \setminus X]$ . Mithin ist  $G$  nicht  $k$ -zusammenhängend. Dies ist ein Widerspruch.
  2.  $\{u, v\} \in E$ : Wir betrachten den Graphen  $G' = (V, E \setminus \{ \{u, v\} \})$ . Dann gilt  $\mu_{G'}(u, v) = \mu_G(u, v) - 1 \leq k - 2$ . Nach Theorem 3.25 gibt es einen  $(u, v)$ -Trenner  $X \subseteq V \setminus \{u, v\}$  mit  $|X| \leq k - 2$ . Wegen  $|V| > k$  gibt es in  $V$  einen Knoten  $x \notin X \cup \{u, v\}$ . Dann ist  $X$  auch ein  $(u, x)$ - oder  $(v, x)$ -Trenner in  $G'$ . Wir nehmen an,  $X$  wäre ein  $(u, x)$ -Trenner in  $G'$ . Dann ist  $X \cup \{v\} \subseteq V \setminus \{u, x\}$  ein  $(u, x)$ -Trenner in  $G$ . Wegen  $|X \cup \{v\}| \leq k - 1 < k$  ist  $G$  dann nicht  $k$ -zusammenhängend. Dies ist ein Widerspruch.

Somit ist die Annahme falsch und es gibt für alle  $u, v \in V$  mit  $u \neq v$  mindestens  $k$  paarweise disjunkte  $(u, v)$ -Pfade in  $G$ .

Damit ist das Theorem bewiesen. ■

## 3.3 Klassen von Graphen

### 3.3.1 Ungerichtete, kreisfreie Graphen: Bäume und Wälder

Einen Graph nennen wir *kreisfrei*, wenn er keinen einfachen Kreis enthält.

**Definition 3.27** 1. Ein Baum ist ein zusammenhängender, kreisfreier Graph.

2. Ein Wald ist ein Graph, dessen Zusammenhangskomponenten Bäume sind.

3. Ein Blatt eines Baumes ist ein Knoten  $v$  mit  $d(v) = 1$ .

**Lemma 3.28** Jeder Baum  $T = (V, E)$  mit  $|V| \geq 2$  Knoten enthält mindestens zwei Blätter.

**Beweis:** Es sei  $e$  eine beliebige Kante. Wir laufen von den Endknoten durch den Baum, bis es keine Kante mehr gibt, über die der aktuelle Knoten wieder verlassen werden kann



(ohne Zurückgehen). Da  $T$  ein Baum ist, wird kein Knoten doppelt besucht. Somit müssen Läufe enden und die gefundenen Knoten sind Blätter. Da  $e$  zwei Endknoten besitzt, gibt es mindestens zwei Blätter und das Lemma ist bewiesen. ■

**Lemma 3.29** *Es sei  $T = (V, E)$  ein Baum mit  $|V| \geq 2$  und  $v \in V$  ein Blatt. Dann ist der Graph  $T' =_{\text{def}} T[V \setminus \{v\}]$  ein Baum.*

**Beweis:** Durch Wegnahme von Knoten und Kanten können keine neuen Kreise entstehen; somit ist  $T'$  kreisfrei, da  $T$  kreisfrei ist. Es sei  $x, y \in V \setminus \{v\}$ . Da  $T$  zusammenhängend ist, gibt es einen  $(x, y)$ -Pfad  $P$  in  $T$ . Für jeden Knoten  $u \notin \{x, y\}$  auf dem Pfad  $P$  gilt mithin  $d(u) \geq 2$ . Somit liegt  $v$  nicht auf  $P$ . Der Pfad  $P$  existiert also auch in  $T'$ . Damit ist  $T'$  zusammenhängend und das Lemma ist bewiesen. ■

**Theorem 3.30** *Für jeden Baum  $T = (V, E)$  gilt  $|E| = |V| - 1$ .*

**Beweis:** (*Induktion*) Wir führen einen Beweis mittels vollständiger Induktion über die Anzahl  $n$  der Knoten von  $V$ , d.h., wir beweisen die Aussage: Für alle  $n \in \mathbb{N}_+$  und alle Bäume  $T = (V, E)$  mit  $|V| = n$  gilt  $|E| = |V| - 1$ .

- *Induktionsanfang:* Es sei  $n = 1$ . Dann gilt für jeden Baum  $T$  mit einem Knoten  $|E| = 0$  und folglich  $|E| = |V| - 1$ .
- *Induktionsschritt:* Es sei  $n > 1$ . Es sei  $T = (V, E)$  ein Baum mit  $|V| = n \geq 2$  Knoten. Dann gibt es nach Lemma 3.28 ein Blatt  $v \in V$  mit der zugehörigen Kante  $e = \{u, v\} \in E$ . Wir definieren  $T' =_{\text{def}} T[V \setminus \{v\}]$ . Nach Lemma 3.29 ist  $T'$  ein Baum. Außerdem besteht  $T'$  aus  $n - 1$  Knoten und besitzt somit nach Induktionsvoraussetzung  $n - 2$  Kanten. Wir erhalten:

$$\begin{aligned} |V| &= |V \setminus \{v\} \cup \{v\}| = |V \setminus \{v\}| + |\{v\}| = (n - 1) + 1 = n \\ |E| &= |E \setminus \{e\} \cup \{e\}| = |E \setminus \{e\}| + |\{e\}| = (n - 2) + 1 = n - 1 \end{aligned}$$

Mithin gilt  $|E| = |V| - 1$ .

Damit ist das Theorem bewiesen. ■

**Lemma 3.31** *Es seien  $T = (V, E)$  ein Baum,  $v \in V$  ein Knoten und  $T_1, \dots, T_k$  die Komponenten von  $T[V \setminus \{v\}]$ . Dann gilt  $k = d(v)$  und  $T_1, \dots, T_k$  sind Bäume.*

**Beweis:** Da  $T$  zusammenhängend und kreisfrei, sind  $T_1, \dots, T_k$  zusammenhängend und kreisfrei, d.h.,  $T_1, \dots, T_k$  sind Bäume. Es sei  $T_i = (V_i, E_i)$  die  $i$ -te Komponente von  $T[V \setminus \{v\}]$ . Dann gilt:

- Jeder Knoten aus  $V \setminus \{v\}$  gehört zu einem  $T_i$ , d.h., es gilt

$$|V| = 1 + \sum_{i=1}^k |V_i|$$

- Jede Kante  $e \in E$  mit  $v \notin e$  gehört zu einem  $T_i$ , d.h., es gilt

$$|E| = d(v) + \sum_{i=1}^k |E_i|$$

Mit Hilfe von Theorem 3.30 erhalten wir somit:

$$\begin{aligned} |V| - 1 &= d(v) + \sum_{i=1}^k (|V_i| - 1) \\ &= d(v) + \sum_{i=1}^k |V_i| - k \\ &= d(v) + |V| - 1 - k \end{aligned}$$

Umstellung nach  $d(v)$  ergibt  $d(v) = k$  und das Lemma ist bewiesen. ■

**Lemma 3.32** *Es seien  $G = (V, E)$  ein zusammenhängender Graph und  $C$  ein einfacher Kreis in  $G$ . Dann gilt für alle auf  $C$  liegenden Kanten  $e$ , dass der Graph  $(V, E \setminus \{e\})$  zusammenhängend ist.*

**Beweis:** (*Widerspruch*) Angenommen es gibt eine Kante  $e = \{u, v\} \in C$ , sodass der Graph  $G - e =_{\text{def}} (V, E \setminus \{e\})$  nicht zusammenhängend ist. Dann liegen die Endknoten  $u$  und  $v$  in verschiedenen Komponenten von  $G - e$ . Da aber  $e$  auf einem einfachen Kreis  $C$  liegt gibt es einen  $(u, v)$ -Pfad, der  $e$  nicht enthält (wir laufen in  $C$  einfach „außen“ herum). Somit existiert der  $(u, v)$ -Pfad auch in  $G - e$ . Folglich liegen  $u$  und  $v$  in der gleichen Komponente. Dies ist ein Widerspruch und somit muss  $G - e$  zusammenhängend sein, egal welche Kante aus dem Kreis aus  $G$  entfernt wird. Damit ist das Lemma bewiesen. ■

Ein Graph  $T = (V_T, E_T)$  heißt *Spannbaum* (oder *aufspannender Baum*) eines Graphen  $G = (V_G, E_G)$ , falls  $T$  ein Baum mit  $V_T = V_G$  und  $E_T \subseteq E_G$  ist.

**Theorem 3.33** *Jeder zusammenhängende Graph  $G = (V, E)$  enthält einen Spannbaum.*

**Beweis:** Für  $|V| = 1$  gilt die Aussage trivialerweise. Es sei also  $G = (V, E)$  ein Graph mit  $|V| \geq 2$  und  $|E| = m$ . Wir definieren eine Folge  $E_0, E_1, \dots, E_m$  von Kantenmengen in  $G$  wie folgt:

$$E_0 =_{\text{def}} E$$

$$E_i =_{\text{def}} \begin{cases} E_{i-1} \setminus \{e_i\}, & \text{wobei } e_i \in E_{i-1} \text{ eine beliebige auf einem Kreis in } (V, E_{i-1}) \\ & \text{liegende Kante ist} \\ E_{i-1}, & \text{falls kein Kreis in } (V, E_{i-1}) \text{ existiert} \end{cases}$$

Klarerweise gilt  $E_0 \supseteq E_1 \supseteq E_2 \supseteq \dots \supseteq E_m$ . Nach Lemma 3.32 ist  $(V, E_m)$  zusammenhängend und kreisfrei, da höchstens  $m$  Kanten aus  $G$  entfernt werden können. Somit ist  $(V, E_m)$  ein Spannbaum und das Theorem ist bewiesen. ■

**Theorem 3.34 (Cayley)** *Für  $n \geq 2$  gibt es genau  $n^{n-2}$  markierte Bäume mit  $n$  Knoten.*

**Beweis:** Wir konstruieren eine Bijektion zwischen der Menge aller markierten Bäume mit  $n$  Knoten und der Menge  $\{1, \dots, n\}^{n-2}$ . Dabei fassen wir die Elemente von  $\{1, \dots, n\}^{n-2}$  als Wörter der Länge  $n-2$  über dem Alphabet  $\{1, \dots, n\}$  auf. Wir betrachten folgende Abbildung  $\varphi$  für einen Baum  $T = (V, E)$  mit  $V \subseteq [n]$ :

$$\begin{aligned} \varphi(T) &=_{\text{def}} \varepsilon, & \text{falls } |V| = 2 \\ \varphi(T) &=_{\text{def}} v \cdot \varphi(T[V \setminus \{u\}]), & \text{wobei } u \text{ das kleinste Blatt in } T \text{ ist und} \\ & & v \text{ der zu } u \text{ adjazente Knoten ist} \end{aligned}$$

Nach Lemma 3.29 sind die induzierten Teilgraphen stets Bäume. Außerdem gilt: Jeder Knoten  $v$  von  $T$  kommt  $(d(v) - 1)$ -mal im Wort  $\varphi(T)$  vor. Somit erhalten wir für die Länge:

$$\begin{aligned} |\varphi(T)| &= \sum_{v \in V} (d(v) - 1) \\ &= \sum_{v \in V} d(v) - |V| \\ &= 2 \cdot |E| - |V| \\ &= 2 \cdot (|V| - 1) - |V| \\ &= |V| - 2 \end{aligned}$$

Die Injektivität der Abbildung ist leicht zu sehen.

Zum Nachweis der Bijektivität der Abbildung  $\varphi$  geben wir an, wie wir zu einem gegebenen Wort  $t = t_1 \dots t_{n-2}$  einen Baum  $T$  finden mit  $\varphi(T) = t$ :

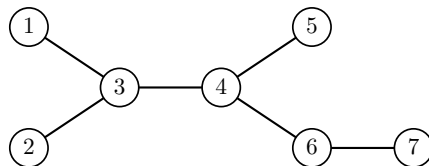
- [1]  $S := \emptyset$
- [2]  $E := \emptyset$

- [3] for  $i := 1$  to  $n - 2$  do  
 [4]      $s_i := \min [n] \setminus (S \cup \{t_i, \dots, t_{n-2}\})$   
 [5]      $E := E \cup \{\{s_i, t_i\}\}$   
 [6]      $S := S \cup \{s_i\}$   
 [7]  $E := E \cup \{[n] \setminus S\}$

Damit ist  $\varphi$  surjektiv und somit bijektiv. Es gibt also genauso viele Bäume, wie es Wörter in  $\{1, \dots, n\}^{n-2}$  gibt. Dies sind nach der Produktregel der Kombinatorik  $n^{n-2}$  viele. Damit ist das Theorem bewiesen. ■

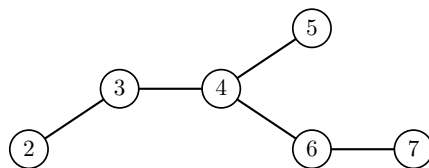
Theorem 3.33 kann auf verschiedene Arten bewiesen werden. Die in unserem Beweis angegebene Kodierung eines markierten Baumes als Wort heißt *Prüfer-Code* nach dem Erfinder der Kodierung.

**Beispiel:** Wir bestimmen den Prüfer-Code für den folgenden Baum  $T = T_0$ :  
 Im Baum  $T_0$  ist das Blatt mit der kleinsten Nummer der Knoten 1.



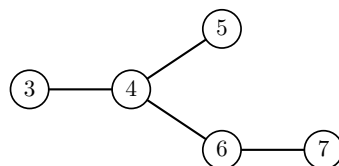
$$\varphi(T_0) = 3\varphi(T_1)$$

Im Baum  $T_1$  ist das Blatt mit der kleinsten Nummer der Knoten 2.



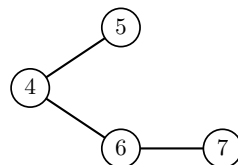
$$\varphi(T_0) = 33\varphi(T_2)$$

Im Baum  $T_2$  ist das Blatt mit der kleinsten Nummer der Knoten 3.



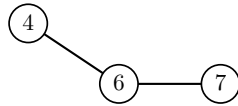
$$\varphi(T_0) = 334\varphi(T_3)$$

Im Baum  $T_3$  ist das Blatt mit der kleinsten Nummer der Knoten 5.



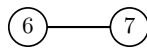
$$\varphi(T_0) = 3344\varphi(T_4)$$

Im Baum  $T_4$  ist das Blatt mit der kleinsten Nummer der Knoten 4.



$$\varphi(T_0) = 33446\varphi(T_5)$$

Der Baum  $T_5$  enthält nur noch zwei Knoten.



$$\varphi(T_0) = 33446$$

Somit ergibt sich der Prüfer-Code  $\varphi(T) = 33446$ .

Wenn nun umgekehrt das Wort 33446 gegeben ist, so bestimmen wieder den zugehörigen Baum  $T$  wie folgt:

$i$	$s_i$	$S$	$t_i \dots t_{n-2}$	$E$
0	–	$\emptyset$	33446	$\emptyset$
1	1	$\{1\}$	3446	$\{\{1, 3\}\}$
2	2	$\{1, 2\}$	446	$\{\{1, 3\}, \{2, 3\}\}$
3	3	$\{1, 2, 3\}$	46	$\{\{1, 3\}, \{2, 3\}, \{3, 4\}\}$
4	5	$\{1, 2, 3, 5\}$	6	$\{\{1, 3\}, \{2, 3\}, \{3, 4\}, \{4, 5\}\}$
5	4	$\{1, 2, 3, 4, 5\}$	$\varepsilon$	$\{\{1, 3\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{4, 6\}\}$
–	–	–	–	$\{\{1, 3\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{4, 6\}, \{6, 7\}\}$

### 3.3.2 Gerichtete, kreisfreie Graphen

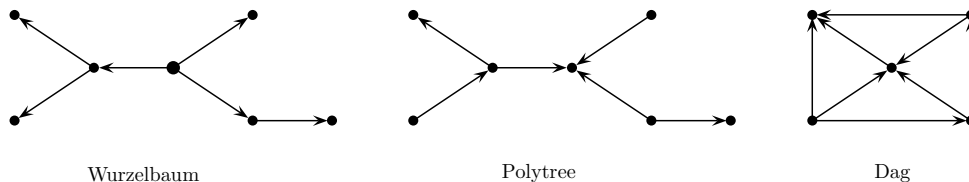
Im Falle eines gerichteten Graphen macht es einen Unterschied, ob für eine Kante  $(u, v)$  auch die umgekehrte Kante  $(v, u)$  im Graphen vorkommt oder nicht. Daher benötigen wir eine eigenen Begriff für einen Kreises, um die Kreisfreiheit zu definieren.

**Definition 3.35** *Es sei  $G = (V, E)$  ein gerichteter Graph.*

1. Ein Weg  $(v_0, e_0, v_1, \dots, v_{n-1}, e_n, v_n)$  mit  $v_0 = v_n$  und  $n > 0$  heißt (gerichteter) Kreis in  $G$ .
2. Enthält  $G$  keinen gerichteten Kreis, so heißt  $G$  gerichteter, kreisfreier (oder azyklischer) Graph (englisch: directed acyclic graph oder kurz dag).

Es ist auch im Deutschen üblich, einen gerichteten, kreisfreien Graph nach dem englischen Ausdruck *Dag* zu nennen.

**Beispiel:** Folgende gerichtete Graphen sind Beispiele für kreisfreie Graphen:



**Theorem 3.36** Für einen gerichteten Graphen  $G = (V, E)$  sind die folgende Aussagen äquivalent:

1.  $G$  ist kreisfrei.
2. Jeder (induzierte) Teilgraph von  $G$  enthält eine Senke.
3. Jeder (induzierte) Teilgraph von  $G$  enthält eine Quelle.

**Beweis:** Wir beweisen nur, dass die Aussage 1 zu Aussage 2 äquivalent ist. Durch die Vertauschung von ausgehenden und eingehenden Kanten (und aller zugehörigen Begriffe) ergibt sich dann auch die Äquivalenz von 1 und 3. Wir zeigen beide Richtungen einzeln:

- 1.  $\Rightarrow$  2.: Wir zeigen die Kontraposition. Es gibt  $U \subseteq V$ , sodass  $G[U]$  keine Senke enthält, d.h.  $d_{G[U]}^+(v) > 0$  für alle Knoten  $v \in U$ . Somit gibt es für jeden Knoten eine ausgehende Kante in  $G[U]$ . Wir wählen einen beliebigen Knoten  $v_0 \in U$ . Wegen  $d_{G[U]}^+(v_0) > 0$  gibt es eine Kante  $e_1 = (v_0, v_1)$  in  $G[U]$ . Wiederum wegen  $d_{G[U]}^+(v_1) > 0$  gibt es eine Kante  $e_2 = (v_1, v_2)$  in  $G[U]$  usw. usf. Auf diese Weise erhalten wir eine unendlich lange Knotenfolge  $(v_0, v_1, v_2, \dots)$ . Da es nur endlich viele Knoten gibt, muss ein Knoten doppelt vorkommen. Somit gibt es einen Kreis in  $G$ .
- 2.  $\Rightarrow$  1.: Wir zeigen die Kontraposition.  $G$  enthalte einen Kreis  $W = (v_0, v_1, \dots, v_k)$ , d.h.  $v_k = v_0$  und  $k \geq 2$ . Dann besitzen alle Knoten  $v_i$  in  $G' =_{\text{def}} G[\{v_0, v_1, \dots, v_{k-1}\}]$  einen Ausgangsgrad  $d_{G'}^+(v_i) > 0$ . Mithin enthält  $G'$  keine Senke.

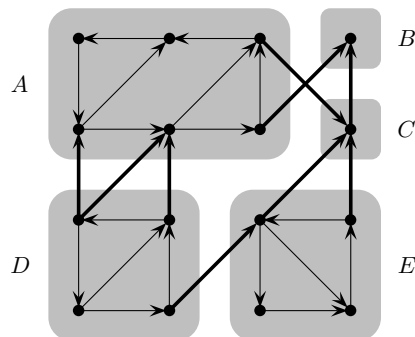
Damit ist das Theorem bewiesen. ■

Betrachten wir die Erreichbarkeitsrelation  $\rightarrow^*$  auf gerichteten Graphen, d.h. die für den Graphen  $G = (V, E)$  und die Knoten  $u, v \in V$  wie folgt definierte Relation

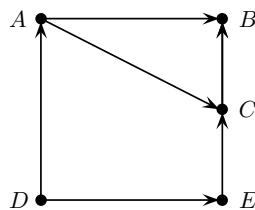
$$u \rightarrow^* v \iff_{\text{def}} \text{es gibt einen } (u, v)\text{-Weg in } G,$$

so bedeutet das Vorhandensein eines Kreises, dass alle Knoten auf dem Kreis in derselben starken Zusammenhangskomponente liegen. Gilt dagegen  $u \rightarrow^* v$  und  $v \not\rightarrow^* u$ , so liegen  $u$  und  $v$  in jedem Fall in verschiedenen Komponenten und auf keinem Kreis. Wir können somit jeden gerichteten Graphen eindeutig in seine starken Zusammenhangskomponenten sowie einen gerichteten, kreisfreien Graphen zerlegen.

**Beispiel:** Wir betrachten exemplarisch für die Zerlegung den Graphen  $G$ :



Die grau unterlegten Teilgraphen sind jeweils starke Zusammenhangskomponenten. Es ist ersichtlich, dass alle Kanten, die zwischen zwei unterschiedlichen Komponenten verlaufen, in dieselbe Richtung zeigen. Führen wir die Superknoten  $A, B, C, D, E$  ein, um die Komponenten zu repräsentieren, so können wir den Graphen in naheliegender Weise auf den folgenden Graphen reduzieren:



Der reduzierte Graph ist der gesuchte gerichtete, kreisfreie Graph.

### 3.3.3 Bipartite Graphen

Im Folgende betrachten wir für die Bipartitheit nur ungerichtete Graphen.

**Definition 3.37** Ein ungerichteter Graph  $G = (V, E)$  heißt bipartit, falls es disjunkte, nichtleere Knotenmengen  $A$  und  $B$  mit  $A \cup B = V$  gibt, sodass die induzierten Teilgraphen  $G[A]$  und  $G[B]$  keine Kante enthalten.

In bipartiten Graphen verlaufen Kanten also nur zwischen den Knotenmengen  $A$  und  $B$ , aber nicht innerhalb der Mengen. Wenn wir uns auf die Bipartitheit beziehen, schreiben

wir auch  $G = (A \uplus B, E)$ . (Hierbei bedeutet  $A \uplus B$ , dass wir die Vereinigung von zwei disjunkten Mengen  $A$  und  $B$  bilden.)

**Theorem 3.38** *Ein Graph  $G = (V, E)$  ist genau dann bipartit, wenn er keinen einfachen Kreis ungerader Länge als Teilgraph enthält.*

**Beweis:** Wir zeigen beide Richtungen einzeln. Ohne Beeinträchtigung der Allgemeinheit kann der Graph als zusammenhängend angenommen werden. Anderenfalls argumentieren wir für jede Komponente.

( $\Rightarrow$ ) Wir beweisen die Kontraposition. Ein einfacher Kreis  $C_{2n+1}$  ungerader Länge ist nicht bipartit. Somit ist ein Graph, der einen solchen Kreis enthält, nicht bipartit.

( $\Leftarrow$ ) Es sei  $G = (V, E)$  ein Graph, der nur einfache Kreise gerader Länge enthält. Wir wählen einen beliebigen Knoten  $v$  und betrachten die zugehörigen Knotenmengen:

$$\begin{aligned} A &=_{\text{def}} \{ u \mid \text{kürzester } (u, v)\text{-Weg hat gerade Länge} \} \\ B &=_{\text{def}} \{ u \mid \text{kürzester } (u, v)\text{-Weg hat ungerade Länge} \} \end{aligned}$$

Dann gilt sicherlich  $A \cap B = \emptyset$  sowie  $A \cup B = V$ . Wir müssen noch zeigen, dass die induzierten Teilgraphen  $G[A]$  und  $G[B]$  keine Kanten enthalten. Es seien  $x, y \in V$  zwei verschiedene Knoten, die entweder beide in  $A$  oder beide in  $B$  liegen. Es seien  $P_x = (u_0, u_1, \dots, u_k)$  mit  $x = u_0$  und  $u_k = v$  ein kürzester  $(x, v)$ -Pfad und  $P_y = (u'_0, u'_1, \dots, u'_{k'})$  mit  $y = u'_0$  und  $u'_{k'} = v$  ein kürzester  $(y, v)$ -Weg. Dann ist  $k+k'$  gerade. Es sei  $u_j$  der erste Knoten auf  $P_x$ , der auch auf  $P_y$  vorkommt, d.h.,  $u_j = u'_{j'}$  für ein geeignetes  $j'$ . Betrachten wir die Pfade  $P'_x = (u_0, \dots, u_j, u'_{j'+1}, \dots, u'_{k'})$  und  $P'_y = (u'_0, \dots, u'_{j'}, u_{j+1}, \dots, u_k)$ , dann sind  $P'_x$  wieder ein kürzester  $(x, v)$ -Pfad und  $P'_y$  ein kürzester  $(y, v)$ -Pfad. Mithin gilt  $j+k'-j' = k$ . Also gilt  $j+j' = k+k'+2(j'-k')$ , und  $j+j'$  ist gerade. Wenn nun  $\{x, y\} \in E$  gelten würde, so würde  $G$  den einfachen Kreis  $(x, \dots, u_j, u'_{j'-1}, \dots, y, x)$  der Länge  $j+j'+1$  enthalten. Da einfache Kreise ungerader Länge ausgeschlossen sind, gilt  $\{x, y\} \notin E$ . Somit verlaufen keine Kanten zwischen Knoten in  $A$  und keine Kanten zwischen den Knoten in  $B$ . Damit ist  $G$  bipartit.

Damit ist das Theorem bewiesen. ■

**Korollar 3.39** *Jeder Baum ist bipartit.*

**Beweis:** Bäume enthalten keine Kreise, also auch keine Kreise ungerader Länge. ■

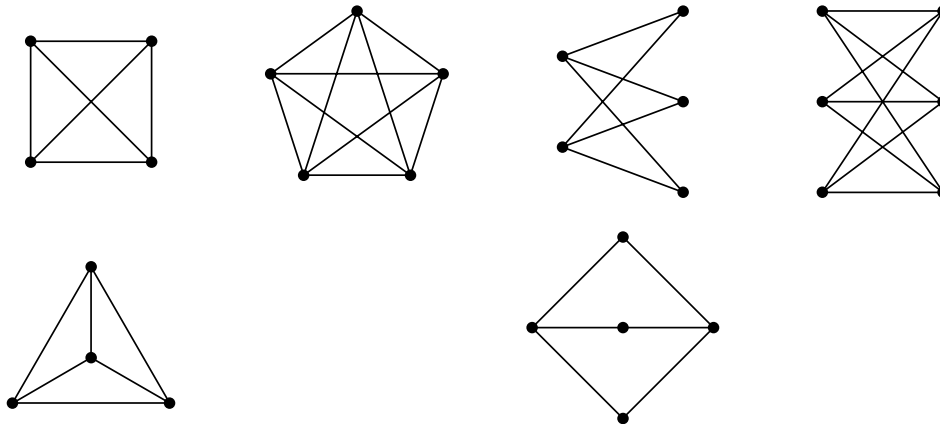


### 3.3.4 Planare Graphen

**Definition 3.40** *Es sei  $G = (V, E)$  ein Graph.*

1.  $G$  heißt *planar* (oder *plättbar*), falls  $G$  so gezeichnet werden kann, dass sich keine Kanten kreuzen.
2.  $G$  heißt *eben*, falls  $G$  planar und in einer kreuzungsfreien Darstellung (Einbettung in der Ebene) gegeben ist.

**Beispiele:** Im Folgenden sind der oberen Reihe die vier Graphen  $K^4$ ,  $K^5$ ,  $K_{2,3}$  und  $K_{3,3}$  angegeben. Die Reihe darunter enthalten Darstellungen der ebenen Graphen im Falle, dass die darüber liegenden Graphen planar sind.



$K^4$  und  $K_{2,3}$  sind planar,  $K^5$  und  $K_{3,3}$  sind nicht planar.

Es sei  $G = (V, E)$  ein ebener Graph. Ein *Gebiet* (Facette) ist ein Teil der Ebene, der entsteht, wenn die Ebene entlang der Kanten zerschnitten wird.

**Beispiele:** Wir zählen leicht nach, dass der  $K^4$  vier Gebiete und der  $K_{2,3}$  drei Gebiete besitzt. Dabei heißen die endlichen Gebiete im Inneren von Kreisen *innere Gebiete* und das unendliche Gebiet *äußeres Gebiet*.

**Theorem 3.41 (Eulersche Polyederformel)** *Es sei  $G = (V, E)$  ein zusammenhängender, ebener Graph. Es sei  $F$  die Menge der Gebiete von  $G$ . Dann gilt:*

$$|F| = |E| - |V| + 2$$

**Beweis:** (*Induktion*) Wir führen ein Beweis mittels vollständiger Induktion über den Exzess von Graphen. Der *Exzess* von  $G = (V, E)$  ist definiert als

$$\text{ex}(G) =_{\text{def}} |E| - |V| + k,$$

wobei  $k$  die Anzahl der Zusammenhangskomponenten von  $G$  ist. Für zusammenhängende Graphen  $G = (V, E)$  gilt somit  $\text{ex}(G) = |E| - |V| + 1 \geq 0$ .

- *Induktionsanfang:* Es sei  $G = (V, E)$  ein zusammenhängender, ebener Graph mit  $\text{ex}(G) = 0$ , d.h.  $|E| = |V| - 1$ . Somit ist  $G$  ein Baum. Da  $G$  keine Kreise enthält, gibt es genau *ein* Gebiet und es gilt  $1 = |E| - |V| + 2$ .
- *Induktionsschritt:* Es sei  $G = (V, E)$  ein zusammenhängender, ebener Graph mit  $\text{ex}(G) > 0$ . Somit ist  $G$  kein Baum. Es gibt also einen einfachen Kreis  $C$  in  $G$ . Es sei  $e$  eine beliebige Kante auf  $C$ . Die Kante  $e$  trennt das Gebiet  $f_1$  innerhalb des Kreises  $C$  von dem Gebiet  $f_2$  außerhalb von  $C$ . Es sei  $G' =_{\text{def}} (V, E \setminus \{e\})$  der ebene Graph, der aus  $G$  entsteht, wenn  $e$  entfernt wird. Dadurch verschmelzen die Gebiet  $f_1$  und  $f_2$  zu einem Gebiet in  $G'$ . Außerdem ist  $G'$  nach ... wieder zusammenhängend, also gilt  $\text{ex}(G') = \text{ex}(G) - 1$ . Nach Induktionsvoraussetzung gilt somit:

$$|F| = \underbrace{|F| - 1}_{\text{Gebiete von } G'} + 1 = \underbrace{|E| - 1}_{\text{Kanten von } G'} - |V| + 2 + 1 = |E| - |V| + 2$$

Damit ist das Theorem bewiesen. ■

**Theorem 3.42** Für jeden planaren Graphen  $G = (V, E)$  mit  $|V| \geq 3$  gilt

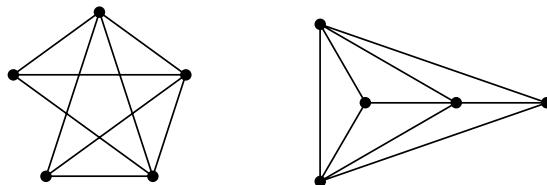
$$|E| \leq 3|V| - 6.$$

**Beweis:** Es genügt die Aussage für kantenmaximale planare Graphen zu zeigen. Es sei  $G = (V, E)$  ein kantenmaximaler planarer Graph. Das Einfügen einer weiteren Kante in  $G$  würde also die Planarität zerstören. Somit ist  $G$  zusammenhängend.  $G$  sei als ebener Graph gegeben. Jede Kante begrenzt höchstens zwei Gebiete von  $G$ . Somit gilt  $|F| \leq 2|E|$ . Weiterhin wird jedes Gebiet von mindestens drei Kanten begrenzt. Somit folgt  $|F| \leq \frac{2}{3} \cdot |E|$ . Mit Theorem 3.41 erhalten wir:

$$\frac{2}{3} \cdot |E| \geq |F| = |E| - |V| + 2$$

Umstellung der Ungleichung nach  $|E|$  ergibt das Theorem. ■

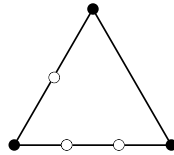
**Beispiele:**  $K^5$  ist nicht planar, denn es gilt  $10 \not\leq 3 \cdot 5 - 6 = 9$ . Der  $K^5$  hat also eine Kante zuviel. Entfernen wir eine beliebige Kante aus dem  $K^5$ , so erhalten wir den fast vollständigen Graphen  $K^{5*}$ . Dieser erfüllt die Kantenbilanz und ist auch planar:



Der  $K_{3,3}$  erfüllt auch die Kantenbilanz, ist jedoch nicht planar (siehe Übungsaufgabe).

Eine *Unterteilung* eines Graphen  $G = (V, E)$  entsteht dadurch, dass Kanten  $e \in E$  durch neue Pfade  $p_e$  ersetzt werden.

**Beispiel:** Eine Unterteilung des  $K^3$  könnte zum Beispiel wie folgt aussehen:



$K^5$  und  $K_{3,3}$  sind gewissermaßen die kleinsten, nicht planaren Graphen. Ohne Beweis geben wir den Satz von Kuratowski an, der planare Graphen durch den Ausschluss von  $K^5$  und  $K_{3,3}$  charakterisiert.

**Theorem 3.43 (Kuratowski)** *Ein Graph  $G$  ist genau dann planar, wenn  $G$  keine Unterteilung des  $K^5$  oder  $K_{3,3}$  als Teilgraph enthält.*

## 3.4 Kombinatorische Probleme in Graphen

### 3.4.1 Touren\*

Im Folgenden interessieren wir uns für die Existenz spezieller Kreise in Graphen, die alle Elemente eines Graphen genau einmal enthalten. Die Elemente können dabei Knoten (Hamiltonkreise) oder Kanten (Eulertouren) sein.

**Definition 3.44** *Es sei  $G = (V, E)$  ein Graph.*

1. Ein Hamiltonkreis in  $G$  ist ein Kreis, der jeden Knoten von  $V$  genau einmal enthält.
2.  $G$  heißt hamiltonsch, falls  $G$  einen Hamiltonkreis enthält.

**Beispiele:** Der  $Q_3$  auf der linken Seite ist hamiltonsch. Der rechte Graph ohne Hamiltonkreis ist der Petersen-Graph:



Der aus den roten Kanten bestehende Weg ist ein Hamiltonkreis.

Zu entscheiden, ob ein gegebener Graph hamiltonsch ist, ist ein NP-vollständiges Problem, d.h., algorithmisch nicht effizient beherrschbar. Wir interessieren uns daher für hinreichende Kriterien für die Existenz von Hamiltonkreisen. Intuitiv sollte zu erwarten sein, dass die Wahrscheinlichkeit einen Hamiltonkreise zu finden, umso höher ist, je mehr Kanten ein Graph enthält.

**Theorem 3.45** *Es sei  $G = (V, E)$  ein Graph. Gilt für alle nicht-adjazenten Knoten  $x, y \in V$  (d.h.,  $x \neq y$  und  $\{x, y\} \notin E$ ) die Ungleichung*

$$d(x) + d(y) \geq |V|,$$

*so enthält  $G$  einen Hamiltonkreis.*

**Beweis:** (*Widerspruch*) Wir nehmen an, dass es einen Graphen  $G = (V, E)$  mit obiger Eigenschaft für alle nicht-adjazenten Knotenpaare gibt, der aber nicht hamiltonsch ist. Wir wählen  $G = (V, E)$  so aus allen diesen Graphen über der Knotenmenge  $V$ , dass  $|E|$  maximal ist. Dann ist  $G$  nicht der vollständige Graph  $K^n$  mit  $n = |V|$ , da dieser einen Hamiltonkreis enthält. Somit gibt es Knoten  $x, y \in V$  mit  $x \neq y$  und  $\{x, y\} \notin E$ .

Wir betrachten nun den Graphen  $G' =_{\text{def}} (V, E \cup \{\{x, y\}\})$ , der aus  $G$  durch Einfügung der Kante  $\{x, y\}$  entsteht. Dann enthält  $G'$  einen Hamiltonkreis  $C$ , da  $G$  ein kantenmaximaler Graph ohne Hamiltonkreis ist, und  $C$  enthält die Kante  $\{x, y\}$ , da  $G$  eben keinen Hamiltonkreis enthält. Es sei  $C = (v_1, v_2, \dots, v_n, v_1)$  mit  $v_1 = x$  und  $v_n = y$ . Wir definieren die beiden Mengen:

$$\begin{aligned} S &=_{\text{def}} \{ v_i \mid 1 \leq i < n \wedge \{x, v_{i+1}\} \in E \} \\ T &=_{\text{def}} \{ v_i \mid 1 \leq i < n \wedge \{x, v_i\} \in E \} \end{aligned}$$

Dann gilt  $y = v_n \notin S \cup T$  (wegen  $\{x, y\} \notin E$ ) sowie  $|S \cup T| < |V|$ . Damit ergibt sich mit Hilfe der Voraussetzung:

$$|S \cap T| = |S| + |T| - |S \cup T|$$

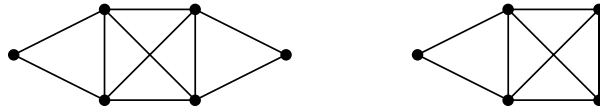
$$\begin{aligned}
&= d(x) + d(y) - |S \cup T| \\
&\geq |V| - |S \cup T| \\
&> |V| - |V| \\
&= 0
\end{aligned}$$

Mithin gibt es ein  $v_i \in S \cap T$ . Werden in  $C$  die Kanten  $\{x, y\}$  und  $\{v_i, v_{i+1}\}$  durch  $\{x, v_{i+1}\}$  und  $\{y, v_i\}$  ersetzt, so entsteht ein Hamiltonkreis ohne  $\{x, y\}$ , also in  $G$ . Dies ist ein Widerspruch zur Annahme, dass  $G$  nicht hamiltonsch ist, und das Theorem ist bewiesen. ■

**Definition 3.46** Es sei  $G = (V, E)$  ein Graph.

1. Eine Eulertour in  $G$  ist ein Kreis, der jede Kante von  $G$  genau einmal durchläuft.
2.  $G$  heißt eulersch, falls  $G$  eine Eulertour enthält.

**Beispiele:** Der linke Graph ist eulersch und der rechte Graph dagegen nicht:



**Theorem 3.47 (Euler)** Ein zusammenhängender Graph  $G = (V, E)$  ist genau dann eulersch, wenn alle Knoten geraden Grad haben.

**Beweis:** Wir beweisen beide Richtungen einzeln.

( $\Rightarrow$ ) Offensichtlich: Jeder Knoten muss besucht und wieder verlassen werden.

( $\Leftarrow$ ) Wir benutzen folgendes Verfahren, um eine Eulertour zu finden: Wir starten bei einem beliebigen Knoten  $v_1$  und durchlaufen Kanten in beliebiger Reihenfolge (ohne eine Kante zweimal zu benutzen). Da die Knotengrade alle gerade sind, muss der Weg  $W_1$  wieder in  $v_1$  enden. Liegen nicht alle Knoten auf  $W_1$ , so gibt es einen Knoten  $v_2$  auf  $W_1$ , der zu einer nicht benutzten Kante inzident ist. Wir starten das Verfahren auf  $v_2$ , um einen Weg  $W_2$  zu bekommen, der wieder in  $v_2$  endet. Wir können nun die beiden Wege  $W_1$  und  $W_2$  zu dem längeren Weg

$$\underbrace{(v_1, \dots, v_2)}_{W_1}, \underbrace{(\dots, v_2)}_{W_2}, \underbrace{(\dots, v_1)}_{W_1}$$

verschmelzen, der jede Kante nur einmal benutzt. Wenden wir das Verfahren nun iterativ solange an, bis alle Knoten besucht sind, so erhalten wir die gesuchte Eulertour.

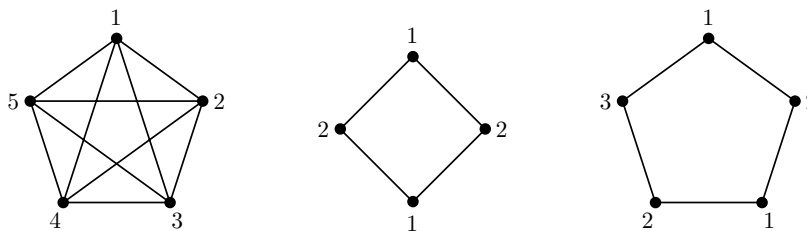
Damit ist das Theorem bewiesen. ■

### 3.4.2 Färbungen

**Definition 3.48** Es sei  $G = (V, E)$  ein Graph.

1. Eine Knotenfärbung von  $G$  mit  $k$  Farben ist eine Abbildung  $c : V \rightarrow \{1, \dots, k\}$  mit  $c(u) \neq c(v)$  für alle Kanten  $\{u, v\} \in E$ .
2. Die chromatische Zahl  $\chi(G)$  von  $G$  ist die minimale Anzahl  $k$  von Farben, sodass eine Knotenfärbung von  $G$  mit  $k$  Farben existiert.

**Beispiele:** In den folgenden Abbildung sind Graphfärbungen mit der minimalen Anzahl von Farben gezeigt:



Dazu korrespondieren die allgemeinen Fälle:

1.  $K^n$  benötigt  $n$  Farben.
2.  $C_{2n}$  benötigt 2 Farben.
3.  $C_{2n+1}$  benötigt 3 Farben.

Die Graphen mit chromatischer Zahl 2 sind genau die bipartiten Graphen.

Ohne Beweis geben wir das folgende berühmte Theorem an, das erstmals 1976 von Appel und Haken unter Einsatz eines Computerprogramms zur Überprüfung von mehr als 1.500 Einzelfällen bewiesen wurde. Insbesondere folgt aus dem Theorem, dass auf politisch-geographischen Landkarten vier Farben genügen, um alle Länder so zu färben, dass Grenzen nur zwischen Ländern unterschiedlicher Farben verlaufen.

**Theorem 3.49 (Vierfarbensatz)** Für jeden planaren Graphen ist  $\chi(G) \leq 4$ .

**Definition 3.50** Es sei  $G = (V, E)$  ein Graph.

1. Eine Kantenfärbung von  $G$  mit  $k$  Farben ist eine Abbildung  $c : E \rightarrow \{1, \dots, k\}$  mit  $c(e) \neq c(f)$  für alle Kanten  $e, f \in E$  mit  $e \cap f \neq \emptyset$ .
2. Der chromatische Index  $\chi'(G)$  von  $G$  ist die minimale Anzahl  $k$  von Farben, sodass eine Kantenfärbung von  $G$  mit  $k$  Farben existiert.

Wiederum ohne Beweis geben wir folgendes Theorem an, das zeigt, dass der chromatische Index eines Graphen nur einen von zwei Werten annehmen kann.

**Theorem 3.51 (Vizing)** Für jeden Graphen  $G = (V, E)$  gilt  $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$ , wobei  $\Delta(G)$  der maximale Grad eines Knoten von  $G$  ist.

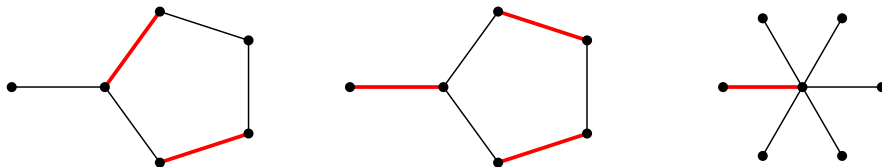
### 3.4.3 Paarungen

**Definition 3.52** Es sei  $G = (V, E)$  ein Graph.

1. Eine Kantenmenge  $M \subseteq E$  heißt Matching in  $G$ , falls  $e \cap f = \emptyset$  für alle Kanten  $e, f \in M$  mit  $e \neq f$  gilt.
2. Ein Matching  $M \subseteq E$  heißt perfektes Matching, falls  $|M| = \frac{1}{2}|V|$  gilt.

Mit anderen Worten: Ist  $M$  ein Matching in einem Graphen  $G$ , so ist jeder Knoten  $v$  von  $G$  zu höchstens einer Kante  $e \in M$  inzident. Gilt  $v \in e$  für eine Kante  $e \in M$ , so wird der Knoten  $v$  von  $M$  überdeckt. Ein perfektes Matching überdeckt somit jeden Knoten des Graphen  $G$ .

**Beispiele:** In folgenden Graphen bilden die roten Kanten jeweils Matchings:



Das Matching in der Mitte ist perfekt, während links nur ein weiteres Matching gezeigt ist. Der Sterngraph rechts besitzt kein perfektes Matching.

Für bipartite Graphen können wir die existierenden Matchings genau charakterisieren. Dafür erweitern für einen Graphen  $G = (V, E)$  die Schreibweise  $N_G(v)$  für die Nachbarschaft eines Knotens  $v$  auf die Nachbarschaft  $N_G(X)$  einer Knotenmenge  $X \subseteq V$ :

$$N_G(X) =_{\text{def}} \bigcup_{v \in X} N_G(v)$$

Wenn der Graph  $G$  aus dem Kontext heraus klar ist, lassen wir wieder den Index  $G$  weg.

**Theorem 3.53 (Hall; Heiratssatz)** Für einen bipartiten Graphen  $G = (A \uplus B, E)$  gibt es genau dann ein Matching  $M$  der Kardinalität  $|M| = |A|$ , wenn  $|N(X)| \geq |X|$  für alle  $X \subseteq A$  gilt.

**Beweis:** Wir beweisen beide Richtungen einzeln.

( $\Rightarrow$ ) Es sei  $M$  ein Matching der Kardinalität  $|M| = |A|$ . Jede Teilmenge  $X \subseteq A$  hat somit genau  $|X|$  Nachbarn in  $B$ . Folglich gilt  $|N(X)| \geq |X|$ .

( $\Leftarrow$ ) Wir führen den Beweis mittels Induktion über die Kardinalität der Menge  $|A|$ .

- *Induktionsanfang:* Für  $m = 1$  ist die Aussage offensichtlich.
- *Induktionsschritt:* Es sei  $m > 1$ . Es sei  $G = (A \uplus B, E)$  ein beliebiger bipartiter Graph mit  $|A| = m$ . Wir unterscheiden zwei Fälle:

- \* *1. Fall:* Für alle  $S \subseteq A$  mit  $0 < |S| < m$  gilt  $|N(S)| \geq |S| + 1$ . Wir konstruieren ein Matching  $M$  wie folgt: Es sei  $e = \{u, v\} \in E$  eine beliebige Kante mit  $u \in A$  und  $v \in B$ . Für den Graphen  $G' =_{\text{def}} G[A \uplus B \setminus \{u, v\}]$  gilt  $N_{G'}(X) = N_G(X) \setminus \{v\}$  und mithin  $|N_{G'}(X)| \geq |X|$  für alle  $X \subseteq A \setminus \{u\}$ . Nach Induktionsvoraussetzung enthält der Graph  $G'$  ein Matching  $M'$  der Kardinalität  $|M'| = |A \setminus \{u\}| = m - 1$ . Somit ist  $M =_{\text{def}} M' \cup \{e\}$  ein Matching in  $G$  der Kardinalität  $|M| = |A| = m$ .
- \* *2. Fall:* Es gibt ein  $S \subseteq A$  mit  $0 < |S| < m$  und  $|N(S)| = |S|$ . Wir halten ein  $S$  fest und konstruieren ein Matching  $M$  wie folgt: Es seien

$$\begin{aligned} G' &=_{\text{def}} G[S \cup N_G(S)] \\ G'' &=_{\text{def}} G[(A \setminus S) \cup (N_G(A) \setminus N_G(S))] \end{aligned}$$

Für alle  $X \subseteq S$  gilt  $N_{G'}(X) = N_G(X)$  und somit  $|N_{G'}(X)| \geq |X|$ . Nach Induktionsvoraussetzung (beachte:  $|S| \leq m - 1$ ) gibt es ein Matching  $M'$  der Kardinalität  $|M'| = |S|$  in  $G'$ . Für alle  $X \subseteq A \setminus S$  gilt  $N_{G''}(X) \cap N_G(S) = \emptyset$ . Wir erhalten:

$$\begin{aligned} |N_{G''}(X)| &= |N_{G''}(X) \cup N_G(S)| - |N_G(S)| \\ &= |N_G(X) \cup N_G(S)| - |N_G(S)| \\ &= |N_G(X \cup S)| - |N_G(S)| \\ &\geq |X \cup S| - |N_G(S)| \\ &= |X| + |S| - |N_G(S)| \\ &= |X| \end{aligned}$$

Nach Induktionsvoraussetzung (beachte:  $|S| \geq 1$  bzw.  $|A \setminus S| \leq m - 1$ ) gibt es ein Matching  $M''$  der Kardinalität  $|M''| = |A \setminus S|$  in  $G''$ . Da die Menge der durch  $M'$  und die Menge der durch  $M''$  überdeckten Knoten disjunkt sind, ist  $M =_{\text{def}} M' \cup M''$  ein Matching in  $G$  der Kardinalität  $|M| = |S| + |A \setminus S| = |A| = m$ .

Damit ist das Theorem bewiesen. ■

**Korollar 3.54** *Jeder  $k$ -reguläre, bipartite Graph  $G$  enthält ein perfektes Matching und hat den chromatischen Index  $\chi'(G) = k$ .*



**Beweis:** Wir beweisen beide Aussagen einzeln.

1. Es sei  $G = (A \uplus B, E)$  ein  $k$ -regulärer, bipartiter Graph. Dann gibt es  $k \cdot |A| = |E|$  Kanten, die von  $A$  nach  $B$  verlaufen. Andererseits verlaufen auch  $|E| = k \cdot |B|$  Kanten von  $B$  nach  $A$ . Mithin gilt  $|A| = |B|$ . Jedes Matching  $M$  der Kardinalität  $|M| = |A|$  ist somit ein perfektes Matching. Es sei  $X \subseteq A$ . Dann gibt es  $k \cdot |X|$  Kanten, die in die Nachbarschaft  $N(X)$  führen. Jeder Knoten  $v \in N(X)$  ist adjazent zu höchstens  $k$  Knoten in  $X$ . Somit gilt  $k \cdot |X| \leq k \cdot |N(X)|$  bzw.  $|X| \leq |N(X)|$ . Nach Theorem 3.53 gibt es somit ein perfektes Matching in  $G$ .
2. Der Nachweis erfolgt über Induktion über  $k$  und ist eine Übungsaufgabe.

Damit ist das Korollar bewiesen. ■



## 4.1 Universelle Algebren

**Definition 4.1** Eine (universelle) Algebra  $\langle S, f_1, \dots, f_t \rangle$  besteht aus einer nichtleeren Menge  $S$  und Operatoren  $f_1, \dots, f_t$  der Stelligkeiten  $m_1, \dots, m_t \in \mathbb{N}$ , d.h. der Operator  $f_i$  ist eine Abbildung  $f_i : S^{m_i} \rightarrow S$ . Das Tupel  $(m_1, \dots, m_t)$  heißt Signatur der Algebra.

**Beispiele:** Im Folgenden werden Beispiele zum Begriff der Algebra diskutiert.

1. Die *boolesche Algebra*  $\langle \{w, f\}, \vee, \wedge, \neg \rangle$  besteht aus der Menge der Wahrheitswerte  $w$  und  $f$  mit den wie folgt beschriebenen Operatoren:

$\vee$	$f$	$w$	$\wedge$	$f$	$w$	$\neg f =_{\text{def}} w$
$f$	$f$	$w$	$f$	$f$	$f$	$\neg w =_{\text{def}} f$
$w$	$w$	$w$	$w$	$f$	$w$	

Die Signatur der Algebra ist somit  $(2, 2, 1)$ .

2.  $\langle \mathbb{N}, + \rangle$ ,  $\langle \mathbb{Z}, + \rangle$  und  $\langle \mathbb{N}, +, \cdot \rangle$  sind Algebren.
3. Für die Menge  $S =_{\text{def}} \{ n \in \mathbb{N} \mid n \text{ ist eine Quadratzahl} \} \subseteq \mathbb{N}$  ist  $\langle S, \cdot \rangle$  eine Algebra.  $\langle S, + \rangle$  ist dagegen keine Algebra.
4. Es seien  $\Sigma$  ein endliches Alphabet und  $\Sigma^*$  die Menge aller endlichen Wörter über  $\Sigma$ . Der zweistellige Operator  $\circ : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$  ist die Konkatenation zweier Wörter  $x$  und  $y$ , d.h.  $x \circ y = xy$ , wobei  $y$  an  $x$  angehängt wird. Dann ist  $\langle \Sigma^*, \circ \rangle$  eine Algebra.
5. Es seien  $U$  eine beliebige, nichtleere Menge,  $F(U) =_{\text{def}} \{ f \mid f : U \rightarrow U \}$  und  $\circ$  die Hintereinanderausführung von Funktionen, d.h.  $f \circ g : U \rightarrow U$  ist definiert durch  $(f \circ g)(x) =_{\text{def}} f(g(x))$  für alle  $x \in U$ . Dann ist  $\langle F(U), \circ \rangle$  eine Algebra.

Für die Stelligkeiten von Operatoren haben sich gewisse Namen eingebürgert:

- Nullstellige Operatoren sind Konstanten, z.B.  $0$ ,  $42$  und  $\perp$ .
- Einstellige Operatoren heißen *unär*, z.B.  $x \mapsto 2^x$ ,  $x \mapsto \neg x$  und  $A \mapsto \mathcal{P}(A)$ .
- Zweistellige Operatoren heißen *binär* (oder *Verknüpfungen*), z.B.  $(x, y) \mapsto \max\{x, y\}$  und  $(x, y) \mapsto \text{ggT}(x, y)$ . Verknüpfungen werden häufig durch die Infix-Notation statt der Funktionsschreibweise angegeben, z.B.  $x + y$  statt  $+(x, y)$ .
- Dreistellige Operatoren heißen *ternär*, z.B.  $(x, y, z) \mapsto \text{if } x \text{ then } y \text{ else } z$  und  $(x, y, z) \mapsto 2 \cdot (xy + xz + yz)$ .

### 4.1.1 Neutrale und inverse Elemente, Assoziativität

**Definition 4.2** Es sei  $\langle S, \circ \rangle$  eine Algebra mit binärer Verknüpfung  $\circ$ . Ein Element  $e \in S$  heißt

1. linksneutral  $\iff_{\text{def}} (\forall a \in S)[e \circ a = a]$
2. rechtsneutral  $\iff_{\text{def}} (\forall a \in S)[a \circ e = a]$
3. neutral  $\iff_{\text{def}} e$  ist linksneutral und rechtsneutral

**Beispiele:**

1.  $\langle \mathbb{N}, \cdot \rangle$  besitzt 1 als neutrales Element, denn es gilt sowohl  $1 \cdot n = n$  als auch  $n \cdot 1 = n$ .
2.  $\langle \mathbb{N}_+, + \rangle$  besitzt kein neutrales Element.
3. Wir betrachten die Algebra  $\langle \{a, b\}, \circ \rangle$  mit der wie folgt definierten Verknüpfung  $\circ$ :

$\circ$	$a$	$b$
$a$	$a$	$b$
$b$	$a$	$b$

Dann gilt sowohl  $a \circ a = a$  und  $a \circ b = b$  als auch  $b \circ a = a$  und  $b \circ b = b$ . Somit sind  $a$  und  $b$  linksneutrale Elemente. Andererseits sind weder  $a$  noch  $b$  rechtsneutral, denn es gilt  $a \circ b = b$  und  $b \circ a = a$ .

**Proposition 4.3** Es sei  $\langle S, \circ \rangle$  eine Algebra mit der binären Verknüpfung  $\circ$ . Sind  $c \in S$  linksneutral und  $d \in S$  rechtsneutral, so gilt  $c = d$ .

**Beweis:** Da  $c$  linksneutral ist, gilt insbesondere  $c \circ d = d$ . Da  $d$  rechtsneutral ist, gilt insbesondere  $c = c \circ d$ . Somit gilt  $c = c \circ d = d$ . Damit ist die Proposition bewiesen. ■

Eine einfache Folgerung aus dieser Proposition ist das folgende Korollar.

**Korollar 4.4** Jede Algebra  $\langle S, \circ \rangle$  mit binäre Verknüpfung  $\circ$  besitzt höchstens ein neutrales Element.

**Beweis:** Sind  $c$  und  $d$  zwei neutrale Elemente von  $\langle S, \circ \rangle$ , so ist insbesondere  $c$  linksneutral und  $d$  rechtsneutral. Mithin gilt  $c = d$ . Damit ist das Korollar bewiesen. ■

**Beispiele:** Wir geben die neutralen Elemente weiterer Algebren an.

1. In  $\langle \Sigma^*, \circ \rangle$  ist das leere Wort  $\varepsilon$  das neutrale Element.

2. In  $\langle F(U), \circ \rangle$  ist die Identitätsfunktion  $\text{id}_U : U \rightarrow U : x \mapsto x$  neutrales Element.

**Definition 4.5** *Es sei  $\langle S, \circ \rangle$  eine Algebra mit binärer Verknüpfung  $\circ$  und neutralem Element  $e \in S$ . Weiterhin seien  $a, x \in S$  beliebig. Dann heißt  $x$*

1. linksinvers zu  $a \iff_{\text{def}} x \circ a = e$
2. rechtsinvers zu  $a \iff_{\text{def}} a \circ x = e$
3. Inverses von  $a \iff_{\text{def}} x$  ist linksinvers und rechtsinvers zu  $a$

### Beispiele:

1. In  $\langle \mathbb{Z}, + \rangle$  ist  $-x$  das Inverse von  $x \in \mathbb{Z}$ .
2. In  $\langle \mathbb{Q}, \cdot \rangle$  ist  $1/x$  das Inverse von  $x \neq 0$ .
3. In  $\langle \mathbb{Z} \setminus \{0\}, \cdot \rangle$  besitzen nur  $-1$  und  $1$  ein Inverses.
4. Wir betrachten die Algebra  $\langle \{e, a, b\}, \circ \rangle$  mit den paarweise verschiedenen Elementen  $e, a, b$  und der wie folgt gegebenen Verknüpfung  $\circ$ :

$\circ$	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$e$	$e$
$b$	$b$	$e$	$e$

Aus der Tabelle kann man ablesen, dass  $e$  das neutrale Element ist. Weiterhin ist zu sehen, dass  $a \circ a = a \circ b = b \circ a = b \circ b = e$  gilt. Mithin sind  $a$  und  $b$  invers zu  $a$  aber auch invers zu  $b$ .

Das letzte Beispiel macht deutlich, dass im Allgemeinen in einer Algebra die Elemente mehrere Inverse besitzen können. In Algebren mit assoziativer Verknüpfung ist dies nicht möglich. Es sei  $\langle S, \circ \rangle$  eine Algebra mit binärer Verknüpfung  $\circ$ . Dann heißt  $\circ$  *assoziativ*, falls für alle  $x, y, z \in S$  gilt:

$$(x \circ y) \circ z = x \circ (y \circ z)$$

**Proposition 4.6** *Es sei  $\langle S, \circ \rangle$  eine Algebra mit assoziativer Verknüpfung  $\circ$  und neutralem Element  $e$ . Weiterhin seien  $a, x, y \in S$  beliebig. Sind  $x$  linksinvers zu  $a$  und  $y$  rechtsinvers zu  $a$ , so gilt  $x = y$ .*

**Beweis:** Da  $e$  ein neutrales Element ist, gilt insbesondere  $x = x \circ e$  und  $y = e \circ y$ . Somit ergibt sich mit Hilfe der Assoziativität:

$$x = x \circ e = x \circ (a \circ y) = (x \circ a) \circ y = e \circ y = y$$

Damit ist die Proposition bewiesen. ■

**Korollar 4.7** Jedes Element  $a \in S$  einer Algebra  $\langle S, \circ \rangle$  mit assoziativer Verknüpfung  $\circ$  und neutralem Element  $e$  besitzt höchstens ein Inverses.

**Beispiele:** Wir geben die inversen Elemente für weitere Algebren an, soweit sie existieren.

1. In  $\langle \Sigma^*, \circ \rangle$  besitzt nur  $\varepsilon$  ein Inverses.
2. In  $\langle F(U), \circ \rangle$  besitzen genau die bijektiven Funktionen  $f$  ein Inverses.

### 4.1.2 Homomorphismen

Im Folgenden führen wir Morphismen ein. Morphismen sind Abbildungen zwischen Algebren, die in einem gewissen Sinne verträglich mit den Operatoren sind.

**Beispiele:** Auf der Menge  $\mathbb{Z}_k =_{\text{def}} \{0, 1, \dots, k-1\}$  definieren wir die Multiplikation  $\cdot_k$  modulo  $k$ :

$$x \cdot_k y =_{\text{def}} \text{mod}(x \cdot y, k)$$

Dann ist  $\langle \mathbb{Z}_k, \cdot_k \rangle$  für alle  $k \in \mathbb{N}_+$  eine Algebra. Wenn wir nun die beiden Algebren  $\langle \mathbb{Z}_2, \cdot_2 \rangle$  und  $\langle \{w, f\}, \wedge \rangle$  und insbesondere die Verknüpfungen

$\cdot_2$	0	1
0	0	0
1	0	1

$\wedge$	f	w
f	f	f
w	f	w

vergleichen, so sind die beiden Algebren sehr ähnlich. Der Unterschied liegt lediglich in der Benennung der Elemente und Operatoren. Später werden wir solche Algebren *isomorph* nennen.

**Definition 4.8** Es seien  $A = \langle S, f_1, \dots, f_t \rangle$  und  $\tilde{A} = \langle \tilde{S}, \tilde{f}_1, \dots, \tilde{f}_t \rangle$  zwei Algebren mit gleicher Signatur  $(m_1, \dots, m_t)$ . Eine Abbildung  $h : S \rightarrow \tilde{S}$  heißt Homomorphismus von  $A$  nach  $\tilde{A}$ , falls für alle  $i \in \{1, \dots, t\}$  und alle  $a_1, \dots, a_{m_i} \in S$  gilt:

$$\tilde{f}_i(h(a_1), \dots, h(a_{m_i})) = h(f_i(a_1, \dots, a_{m_i})),$$

d.h.,  $f_i$  und  $\tilde{f}_i$  sind mit  $h$  vertauschbar.

**Beispiele:** Wir demonstrieren das Konzept von Homomorphismen für einige Algebren.

1. Für die Algebren  $A =_{\text{def}} \langle \mathbb{N}, + \rangle$  und  $\tilde{A} =_{\text{def}} \langle \mathbb{Z}, + \rangle$  ist die Abbildung  $h : \mathbb{N} \rightarrow \mathbb{Z} : n \mapsto n$  ein Homomorphismus von  $A$  nach  $\tilde{A}$ , denn für alle  $n, m \in \mathbb{N}$  gilt

$$h(n) + h(m) = n + m = h(n + m).$$

2. Für  $A =_{\text{def}} \langle \mathbb{N}, + \rangle$  und  $\tilde{A} =_{\text{def}} \langle \mathbb{Z}_k, +_k \rangle$  mit  $+_k : (x, y) \mapsto \text{mod}(x + y, k)$  ist die Abbildung  $h : \mathbb{N} \rightarrow \mathbb{Z}_k : n \mapsto \text{mod}(n, k)$  ein Homomorphismus von  $A$  nach  $\tilde{A}$ , denn wegen der Rechenregeln der Modularen Arithmetik gilt für alle  $n, m \in \mathbb{N}$ :

$$\begin{aligned} h(n) +_k h(m) &= \text{mod}(h(n) + h(m), k) \\ &= \text{mod}(\text{mod}(n, k) + \text{mod}(m, k), k) \\ &= \text{mod}(n + m, k) \\ &= h(n + m) \end{aligned}$$

3. Für die Algebren  $A =_{\text{def}} \langle \Sigma^*, \circ \rangle$  mit der Konkatenation  $\circ$  als Verknüpfung und  $\tilde{A} =_{\text{def}} \langle \mathbb{N}, + \rangle$  ist die Abbildung  $h : \Sigma^* \rightarrow \mathbb{N} : x \mapsto |x|$  (wobei  $|x|$  die Länge von  $x$  bezeichnet) ein Homomorphismus, denn es gilt für alle Wörter  $x, y \in \Sigma^*$

$$h(x) + h(y) = |x| + |y| = |x \circ y| = h(x \circ y).$$

**Definition 4.9** *Es sei  $\langle S, f_1, \dots, f_t \rangle$  eine Algebra mit Signatur  $(m_1, \dots, m_t)$ . Eine nicht-leere Teilmenge  $S' \subseteq S$  erzeugt eine Unteralgebra, falls  $S'$  abgeschlossen ist unter  $f_1, \dots, f_t$ , d.h., für alle  $i \in \{1, \dots, t\}$  und alle  $a_1, \dots, a_{m_i} \in S'$  gilt  $f_i(a_1, \dots, a_{m_i}) \in S'$ .*

**Beispiele:**

1.  $\langle \mathbb{N}, + \rangle$  ist eine Unteralgebra von  $\langle \mathbb{Z}, + \rangle$ .
2. Es seien  $S =_{\text{def}} \{ n \in \mathbb{N} \mid n \text{ ist gerade} \}$  und  $S' =_{\text{def}} \mathbb{N} \setminus S$ . Dann sind  $\langle S, + \rangle$  und  $\langle S, \cdot \rangle$  Unteralgebren von  $\langle \mathbb{N}, + \rangle$  bzw.  $\langle \mathbb{N}, \cdot \rangle$ . Außerdem ist auch  $\langle S', \cdot \rangle$  eine Unteralgebra von  $\langle \mathbb{N}, \cdot \rangle$ ;  $\langle S', + \rangle$  ist dagegen keine Unteralgebra von  $\langle \mathbb{N}, + \rangle$ .

**Proposition 4.10** *Es sei  $h : S \rightarrow \tilde{S}$  ein Homomorphismus von  $A = \langle S, f_1, \dots, f_t \rangle$  nach  $\tilde{A} = \langle \tilde{S}, \tilde{f}_1, \dots, \tilde{f}_t \rangle$ . Dann ist  $\langle h(S), \tilde{f}_1, \dots, \tilde{f}_t \rangle$  eine Unteralgebra von  $\tilde{A}$ .*

**Beweis:** Wir müssen die Abgeschlossenheit der Menge  $h(S)$  unter  $\tilde{f}_1, \dots, \tilde{f}_t$  zeigen, d.h., für jeden Operator  $\tilde{f}_i$  (der Stelligkeit  $m_i$ ) muss für alle  $\tilde{a}_1, \dots, \tilde{a}_{m_i} \in h(S)$  wiederum

$\tilde{f}_i(\tilde{a}_1, \dots, \tilde{a}_{m_i}) \in h(S)$  gelten. Es sei  $\tilde{a}_j \in h(S)$ , d.h., es gibt ein  $a_j \in S$  mit  $h(a_j) = \tilde{a}_j$ . Somit gilt:

$$\tilde{f}_i(\tilde{a}_1, \dots, \tilde{a}_{m_i}) = \tilde{f}_i(h(a_1), \dots, h(a_{m_i})) = h(f_i(a_1, \dots, a_{m_i})) \in h(S)$$

Damit ist die Proposition bewiesen. ■

**Definition 4.11** *Es seien  $A = \langle S, f_1, \dots, f_t \rangle$  und  $\tilde{A} = \langle \tilde{S}, \tilde{f}_1, \dots, \tilde{f}_t \rangle$  zwei Algebren mit gleicher Signatur.*

1. *Eine Algebra  $h : S \rightarrow \tilde{S}$  heißt (Algebra-)Isomorphismus von  $A$  nach  $\tilde{A}$ , falls  $h$  bijektiv und ein Homomorphismus von  $A$  nach  $\tilde{A}$  ist.*
2.  *$A$  und  $\tilde{A}$  heißen isomorph (symbolisch:  $A \simeq \tilde{A}$ ), falls ein Isomorphismus von  $A$  nach  $\tilde{A}$  existiert.*
3. *Gilt  $A = \tilde{A}$ , so heißt ein Isomorphismus von  $A$  nach  $A$  Automorphismus auf  $A$ .*

### Beispiele:

1. Für  $A =_{\text{def}} \langle \mathbb{N}, + \rangle$  und  $\tilde{A} =_{\text{def}} \langle \{ 2n \mid n \in \mathbb{N} \}, + \rangle$  ist  $h : n \mapsto 2n$  ein Isomorphismus von  $A$  nach  $\tilde{A}$ .
2. Für  $A =_{\text{def}} \langle \mathbb{R}_{>0}, \cdot \rangle$  und  $\tilde{A} =_{\text{def}} \langle \mathbb{R}, + \rangle$  ist  $h : \mathbb{R}_{>0} \rightarrow \mathbb{R} : x \mapsto \ln x$  (wegen  $\ln(x \cdot y) = \ln x + \ln y$ ) ein Isomorphismus von  $A$  nach  $\tilde{A}$ .
3. Auf  $A =_{\text{def}} \langle \mathbb{Z}_3, +_3 \rangle$  ist durch die Abbildung

$$h : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3 : n \mapsto \begin{cases} 0, & \text{falls } n = 0 \\ 2, & \text{falls } n = 1 \\ 1, & \text{falls } n = 2 \end{cases}$$

ein Automorphismus gegeben.

4. Auf  $A =_{\text{def}} \langle \mathbb{Z}_5^*, +_5 \rangle$  mit  $\mathbb{Z}_5^* =_{\text{def}} \{1, 2, 3, 4\}$  ist durch die Abbildung

$$h : \mathbb{Z}_5^* \rightarrow \mathbb{Z}_5^* : n \mapsto \begin{cases} 1, & \text{falls } n = 1 \\ 3, & \text{falls } n = 2 \\ 2, & \text{falls } n = 3 \\ 4, & \text{falls } n = 4 \end{cases}$$

ein Automorphismus gegeben.

**Proposition 4.12** *Ein Isomorphismus  $h$  von  $A = \langle S, \circ \rangle$  nach  $\tilde{A} = \langle \tilde{S}, \tilde{\circ} \rangle$  bildet neutrale Elemente auf neutrale Elemente und inverse Elemente auf inverse Elemente ab.*



**Beweis:** (nur für Rechtsneutralität) Es sei  $e \in S$  rechtsneutral für  $\circ$ . Dann gilt für  $b \in \tilde{S}$

$$b \tilde{\circ} h(e) = h(h^{-1}(b)) \tilde{\circ} h(e) = h(h^{-1}(b) \circ e) = h(h^{-1}(b)) = b.$$

Somit ist  $h(e)$  ein rechtsneutrales Element von  $\tilde{A}$ .

Analoge Argumentationen können für linksneutrale, neutrale, rechtsinverse, linksinverse, inverse Elemente geführt werden. Damit ist die Proposition bewiesen. ■

**Proposition 4.13** *Gibt es einen Isomorphismus  $h$  von  $A = \langle S, \circ \rangle$  nach  $\tilde{A} = \langle \tilde{S}, \tilde{\circ} \rangle$ , so gibt es einen Isomorphismus  $\tilde{h}$  von  $\tilde{A} = \langle \tilde{S}, \tilde{\circ} \rangle$  nach  $A = \langle S, \circ \rangle$ .*

**Beweis:** Wir definieren  $\tilde{h} =_{\text{def}} h^{-1}$ . Da  $h : S \rightarrow \tilde{S}$  bijektiv ist, gibt es  $\tilde{h} : \tilde{S} \rightarrow S$  stets und  $\tilde{h}$  ist ebenfalls bijektiv. Weiterhin gilt für  $a, b \in \tilde{S}$ :

$$\begin{aligned} \tilde{h}(a \tilde{\circ} b) &= \tilde{h}(h(h^{-1}(a)) \tilde{\circ} h(h^{-1}(b))) \\ &= \tilde{h}(h(h^{-1}(a) \circ h^{-1}(b))) \\ &= h^{-1}(h(h^{-1}(a) \circ h^{-1}(b))) \\ &= h^{-1}(a) \circ h^{-1}(b) \\ &= \tilde{h}(a) \circ \tilde{h}(b) \end{aligned}$$

Somit ist  $\tilde{h}$  ein Homomorphismus und mithin ein Isomorphismus. Damit ist die Proposition bewiesen. ■

## 4.2 Algebrentypen

### 4.2.1 Algebren mit einer Verknüpfung

Wir betrachten die folgenden drei Eigenschaften für eine Algebra  $A = \langle S, \circ \rangle$ :

- (E1) : Die Verknüpfungen  $\circ$  ist assoziativ.
- (E2) : Es gibt ein neutrales Element  $e \in S$ .
- (E3) : Jedes Element  $a \in S$  besitzt ein eindeutiges inverses Element.

Natürlich kann für eine Algebra die Eigenschaft (E3) nur gelten, wenn auch (E2) gilt.

**Definition 4.14** *Es sei  $A = \langle S, \circ \rangle$  eine Algebra mit binärer Verknüpfung  $\circ$ . Dann wird  $A$  einer der folgenden Namen zugewiesen, je nachdem welche der Eigenschaften (E1), (E2) oder (E3) gelten:*

Name	(E1)	(E2)	(E3)
Gruppoid			
Halbgruppe	X		
Monoid	X	X	
Gruppe	X	X	X
Loop		X	X
Gruppoid mit 1		X	

**Definition 4.15** *Ein Gruppoid  $\langle S, \circ \rangle$  heißt abelsch, falls  $a \circ b = b \circ a$  für alle  $a, b \in S$  gilt, d.h.,  $\circ$  ist kommutativ.*

### Beispiele:

1. Die Algebra  $A =_{\text{def}} \langle \{a, b\}, \circ \rangle$  mit dem durch die Verknüpfungstabelle

$\circ$	$a$	$b$
$a$	$b$	$a$
$b$	$b$	$b$

gegebenen Operator  $\circ$  ist lediglich ein nicht-abelscher Gruppoid, denn  $\circ$  ist nicht assoziativ (wegen  $(a \circ b) \circ a = a \circ a = b$  und  $a \circ (b \circ a) = a \circ b = a$ ) und  $A$  besitzt kein neutrales Element ( $b$  ist zwar rechtsneutral aber nicht linksneutral;  $a$  ist weder rechts- noch linksneutral). Die Kommutativität gilt ebenfalls nicht für  $\circ$  (wegen  $a \circ b \neq b \circ a$ ).

2.  $\langle \mathbb{N}_+, + \rangle$  ist eine abelsche Halbgruppe, aber kein Monoid.
3.  $\langle \mathbb{N}, + \rangle$  ist ein abelscher Monoid, aber keine Gruppe.

4.  $\langle \mathbb{Z}, + \rangle$  ist eine abelsche Gruppe.
5.  $\langle \mathbb{Z}, - \rangle$  ist ein nicht-abelscher Gruppoid.
6.  $\langle \Sigma^*, \circ \rangle$  ist ein nicht-abelscher Monoid.
7. Die Algebra  $A =_{\text{def}} \langle \{e, a, b\}, \circ \rangle$  mit dem durch die Verknüpfungstabelle

$\circ$	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$e$	$b$
$b$	$b$	$b$	$e$

gegebenen Operator  $\circ$  ist ein abelscher Loop, denn  $\circ$  ist nicht assoziativ (wegen  $a \circ (b \circ b) = a \circ e = a$  und  $(a \circ b) \circ b = b \circ b = e$ ),  $e$  ist das neutrale Element und jedes Element ist zu sich selbstinvers. Die Kommutativität von  $\circ$  folgt aus der Symmetrie der Verknüpfungstabelle entlang der Diagonale von links oben nach rechts unten.

### 4.2.2 Algebren mit zwei Verknüpfungen

**Definition 4.16** Eine Algebra  $A = \langle S, +, \cdot \rangle$  der Signatur  $(2, 2)$  heißt Ring, falls folgende Bedingungen gelten:

1.  $\langle S, + \rangle$  ist eine abelsche Gruppe mit neutralem Element  $0 \in S$ .
2.  $\langle S, \cdot \rangle$  ist ein Monoid mit neutralem Element  $1 \in S$ .
3. Für alle  $a, b, c \in S$  gilt:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}$$

D.h.,  $+$  und  $\cdot$  sind distributiv.

#### Beispiele:

1.  $\langle \mathbb{Z}, +, \cdot \rangle$  ist ein Ring.
2.  $\langle \{\mathbf{w}, \mathbf{f}\}, \oplus, \wedge \rangle$  ist ein Ring.
3.  $\langle \{\mathbf{w}, \mathbf{f}\}, \oplus, \vee \rangle$  ist kein Ring, denn die Distributivität gilt nicht.
4. Die univariaten ganzzahligen Polynome bilden einen Ring.

**Definition 4.17** Eine Algebra  $A = \langle S, +, \cdot \rangle$  der Signatur  $(2, 2)$  heißt Körper, falls folgende Bedingungen gelten:

1.  $\langle S, + \rangle$  ist eine abelsche Gruppe mit neutralem Element  $0 \in S$ .
2.  $\langle S \setminus \{0\}, \cdot \rangle$  ist eine abelsche Gruppe mit neutralem Element  $1 \in S$ .
3. Für alle  $a, b, c \in S$  gilt

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}$$

D.h.,  $+$  und  $\cdot$  sind distributiv.

**Beispiele:**

1.  $\langle \mathbb{Z}, +, \cdot \rangle$  ist kein Körper.
2.  $\langle \{\mathbf{w}, \mathbf{f}\}, \oplus, \wedge \rangle$  ist ein Körper.
3. Die univariaten ganzzahligen Polynome bilden keinen Körper, denn es gibt kein ganzzahliges Polynom  $p(x)$  mit  $x \cdot p(x) = 1$ .
4.  $\langle \mathbb{Q}, +, \cdot \rangle$ ,  $\langle \mathbb{R}, +, \cdot \rangle$  und  $\langle \mathbb{C}, +, \cdot \rangle$  sind Körper.

### 4.2.3 Algebren mit drei Operatoren

**Definition 4.18** Eine Algebra  $A = \langle S, +, \cdot, \bar{\phantom{x}} \rangle$  der Signatur  $(2, 2, 1)$  heißt boolesche Algebra, falls folgende Bedingungen gelten:

1.  $\langle S, + \rangle$  ist ein abelscher Monoid mit neutralem Element  $0 \in S$ .
2.  $\langle S, \cdot \rangle$  ist ein abelscher Monoid mit neutralem Element  $1 \in S$ .
3. Für alle  $a \in S$  gilt  $a + \bar{a} = 1$  und  $a \cdot \bar{a} = 0$ .
4. Für alle  $a, b, c \in S$  gilt:

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ a + (b \cdot c) &= (a + b) \cdot (a + c) \end{aligned}$$

**Beispiele:**

1.  $\langle \{\mathbf{w}, \mathbf{f}\}, \vee, \wedge, \neg \rangle$  ist eine boolesche Algebra.
2.  $\langle \mathcal{P}(A), \cup, \cap, \bar{\phantom{x}} \rangle$  ist eine boolesche Algebra (für beliebiges  $A$ ).

## 4.3 Gruppen\*

Zur Erinnerung: Eine Gruppe  $\langle G, \circ \rangle$  ist ein Gruppoid mit den folgenden Eigenschaften:

- (G1) Die Verknüpfung  $\circ$  ist assoziativ auf  $G$ .
- (G2) Es gibt ein neutrales Element  $e \in G$ .
- (G3) Für jedes Element  $a \in G$  gibt es ein Inverses  $a^{-1} \in G$ .

Im Folgenden werden wir eine Gruppe  $\langle G, \circ \rangle$  mit der Trägermenge  $G$  identifizieren.

**Theorem 4.19** *Es seien  $G$  eine Gruppe,  $a, b, c \in G$  und  $x, y \in G$ . Dann gilt:*

1. Involutionsregel:

$$a = (a^{-1})^{-1}$$

2. Kürzungsregeln:

$$a \circ b = c \circ b \iff a = c$$

$$b \circ a = b \circ c \iff a = c$$

3. Eindeutige Lösbarkeit linearer Gleichungen:

$$a \circ x = b \iff x = a^{-1} \circ b$$

$$x \circ a = b \iff x = b \circ a^{-1}$$

**Beweis:** (*Involutionsregel*) Wir definieren  $b =_{\text{def}} (a^{-1})^{-1}$ , d.h.,  $b$  ist das inverse Element von  $a^{-1}$  in  $G$ . Dann gilt

$$b = b \circ e = b \circ (a^{-1} \circ a) = (b \circ a^{-1}) \circ a = e \circ a = a$$

Die anderen Regeln sind ähnlich zu beweisen. Damit ist der Satz bewiesen. ■

Wir führen einige Schreibweisen ein für eine Gruppe  $G$ ,  $a \in G$  und  $n \in \mathbb{N}$ :

$$\begin{aligned} a^0 &=_{\text{def}} e \\ a^n &=_{\text{def}} a \circ a^{n-1} \quad \text{für } n \geq 1 \\ a^{-n} &=_{\text{def}} (a^{-1})^n \end{aligned}$$

Hierbei heißt  $a^n$  die  $n$ -te Potenz von  $a$ . Zu beachten ist, dass  $a^{-n}$  wohldefiniert ist:

$$(a^{-1})^n = (a^{-1})^n \circ (a^n \circ (a^n)^{-1}) = ((a^{-1})^n \circ a^n) \circ (a^n)^{-1} = e \circ (a^n)^{-1} = (a^n)^{-1}$$

Im Allgemeinen gelten folgende Rechenregeln für alle  $m, n \in \mathbb{Z}$  und  $a \in G$ :

$$\begin{aligned} a^m \circ a^n &= a^{m+n} \\ (a^n)^m &= a^{m \cdot n} \\ a^m = a^n &\iff a^{m-n} = e \end{aligned}$$

**Definition 4.20** Es seien  $G$  eine Gruppe und  $a \in G$ . Die Ordnung  $\text{ord}(a)$  von  $a$  ist die kleinste Zahl  $r \in \mathbb{N}_+$  mit  $a^r = e$ . Falls kein solches  $r$  existiert, dann definieren wir  $\text{ord}(a) =_{\text{def}} \infty$ .

**Beispiele:**

1. In  $\langle \mathbb{Z}, + \rangle$  gilt  $\text{ord}(0) = 1$  und  $\text{ord}(n) = \infty$  für alle  $n \in \mathbb{Z} \setminus \{0\}$ .
2. In  $\langle \mathbb{Z}_{12}, +_{12} \rangle$  sind die Ordnungen für die Elemente der folgenden Tabelle zu entnehmen:

$a$	0	1	2	3	4	5	6	7	8	9	10	11
$\text{ord}(a)$	1	12	6	4	3	12	2	12	3	4	6	12

**Proposition 4.21** Es sei  $G$  eine endliche Gruppe. Dann hat jedes Element in  $G$  eine endliche Ordnung.

**Beweis:** Es sei  $a \in G$ . Dann sind alle Elemente  $a^0, a^1, \dots, a^{|G|}$  ebenfalls Elemente von  $G$ . Da  $G$  nur  $|G|$  Elemente enthält, sind unter diesen  $|G|+1$  Elementen mindestens zwei gleiche Elemente  $a^k$  und  $a^j$  mit  $k \neq j$ . Wir wählen  $k$  minimal mit  $a^k = a^j$  für  $0 \leq j \leq k-1$ . Es gilt  $a^{k-j} = e$ . Da  $k$  minimal ist, muss  $j = 0$  gelten. Mithin gilt  $a^k = e$  und somit  $\text{ord}(a) = k$ . Damit ist die Proposition bewiesen. ■

**Lemma 4.22** Es seien  $G$  eine Gruppe und  $a \in G$  mit  $\text{ord}(a) < \infty$ . Dann gilt:

$$a^k = e \iff \text{ord}(a) | k$$

**Beweis:** Wir zeigen beide Richtungen einzeln.

( $\Rightarrow$ ) Mit  $k = s \cdot \text{ord}(a) + r$  für  $r, s \in \mathbb{N}$  mit  $0 \leq r < \text{ord}(a)$  folgt:

$$e = a^k = a^{s \cdot \text{ord}(a) + r} = (a^{\text{ord}(a)})^s \circ a^r = e^s \circ a^r = e \circ a^r = a^r$$

Wegen  $r < \text{ord}(a)$  gilt  $r = 0$ . Somit gilt  $k = s \cdot \text{ord}(a)$  bzw.  $\text{ord}(a) | k$ .

( $\Leftarrow$ ) Mit  $k = s \cdot \text{ord}(a)$  gilt  $a^k = (a^{\text{ord}(a)})^s = e^s = e$ .

Damit ist das Lemma bewiesen. ■

**Lemma 4.23** *Es sei  $G$  eine abelsche Gruppe. Es seien  $a, b \in G$  Elemente endlicher, teilerfremder Ordnung, d.h.,  $\text{ord}(a), \text{ord}(b) < \infty$  und  $\text{ggT}(\text{ord}(a), \text{ord}(b)) = 1$ . Dann gilt:*

$$\text{ord}(a \circ b) = \text{ord}(a) \cdot \text{ord}(b)$$

**Beweis:** Da  $G$  abelsch ist, gilt:

$$(a \circ b)^{\text{ord}(a) \cdot \text{ord}(b)} = (a^{\text{ord}(a)})^{\text{ord}(b)} \circ (b^{\text{ord}(b)})^{\text{ord}(a)} = e^{\text{ord}(b)} \circ e^{\text{ord}(a)} = e$$

Nach Lemma 4.22 gilt mithin  $\text{ord}(a \circ b) \mid \text{ord}(a) \cdot \text{ord}(b)$ .

Angenommen  $\text{ord}(a \circ b) < \text{ord}(a) \cdot \text{ord}(b)$ . Dann gibt es eine Primzahl  $p \geq 2$  mit

$$\text{ord}(a \circ b) \mid \frac{\text{ord}(a) \cdot \text{ord}(b)}{p}.$$

Da  $\text{ord}(a)$  und  $\text{ord}(b)$  teilerfremd sind, kann  $p$  nur eine der beiden Ordnungen teilen. Ohne Beeinträchtigung der Allgemeinheit gelte  $p \mid \text{ord}(a)$ . Somit folgt

$$e = (a \circ b)^{\frac{\text{ord}(a) \cdot \text{ord}(b)}{p}} = a^{\frac{\text{ord}(a) \cdot \text{ord}(b)}{p}} \circ (b^{\text{ord}(b)})^{\frac{\text{ord}(a)}{p}} = a^{\frac{\text{ord}(a) \cdot \text{ord}(b)}{p}}$$

und mithin gilt nach Lemma 4.22 auch

$$\text{ord}(a) \mid \frac{\text{ord}(a) \cdot \text{ord}(b)}{p}$$

Wegen  $p \nmid \text{ord}(b)$  folgt:

$$\text{ord}(a) \mid \frac{\text{ord}(a)}{p}$$

Dies ist jedoch ein Widerspruch. Somit gilt  $\text{ord}(a \circ b) = \text{ord}(a) \cdot \text{ord}(b)$  und das Lemma ist bewiesen. ■

**Lemma 4.24** *Es seien  $G$  eine endliche, abelsche Gruppe und  $a \in G$  ein Element maximaler Ordnung, d.h.  $\text{ord}(a) = \max\{\text{ord}(b) \mid b \in G\}$ . Dann gilt  $\text{ord}(b) \mid \text{ord}(a)$  für alle  $b \in G$ .*

**Beweis:** Zum Beweis mittels Widerspruch nehmen wir an, dass  $b$  ein Element in  $G$  mit  $\text{ord}(b) \nmid \text{ord}(a)$  ist. Dann gibt es eine Primzahl  $p \geq 2$  mit:

$$p^i \mid \text{ord}(a), \quad p^{i+1} \nmid \text{ord}(a), \quad p^{i+1} \mid \text{ord}(b)$$

Wir definieren  $a' =_{\text{def}} a^{p^i}$  und  $b' =_{\text{def}} b^{\frac{\text{ord}(b)}{p^{i+1}}}$  und bestimmen die Ordnungen von  $a'$  und  $b'$ :

$$\begin{aligned} \text{ord}(a') &= \frac{\text{ord}(a)}{p^i}, & \text{denn } (a')^{\frac{\text{ord}(a)}{p^i}} &= \left(a^{p^i}\right)^{\frac{\text{ord}(a)}{p^i}} = a^{\text{ord}(a)} = e \\ \text{ord}(b') &= p^{i+1}, & \text{denn } (b')^{p^{i+1}} &= \left(b^{\frac{\text{ord}(b)}{p^{i+1}}}\right)^{p^{i+1}} = b^{\text{ord}(b)} = e \end{aligned}$$

Da  $p^{i+1} \nmid \text{ord}(a)$  sind  $\frac{\text{ord}(a)}{p^i}$  und  $p^{i+1}$  teilerfremd. Somit folgt aus Lemma 4.23

$$\text{ord}(a' \circ b') = \text{ord}(a') \cdot \text{ord}(b') = p \cdot \text{ord}(a) > \text{ord}(a).$$

Dies ist jedoch ein Widerspruch zur Maximalität der Ordnung von  $a$  und das Lemma ist bewiesen. ■

**Definition 4.25** Eine Unteralgebra  $\langle H, \circ \rangle$  einer Gruppe  $\langle G, \circ \rangle$  heißt Untergruppe von  $G$ , falls  $\langle H, \circ \rangle$  eine Gruppe ist.

**Proposition 4.26** Es seien  $G$  eine Gruppe und  $H$  eine Untergruppe von  $G$ . Dann sind die neutralen Elemente von  $G$  und  $H$  identisch.

**Beweis:** Es seien  $e_H$  ein neutrales Element von  $H$  und  $e_G$  ein neutrales Element von  $G$ . Es gilt  $e_H \circ e_H = e_H$  und  $e_G \circ e_H = e_H$ , d.h.,  $e_H \circ e_H = e_G \circ e_H$ . Nach der Kürzungsregel für  $G$  gilt  $e_H = e_G$ . ■

**Proposition 4.27** Jede Unteralgebra einer endlichen Gruppe ist eine Untergruppe.

**Beweis:** Es sei  $\langle H, \circ \rangle$  ein Unteralgebra der endlichen Gruppe  $\langle G, \circ \rangle$ . Die Assoziativität überträgt sich von  $H$  auf  $G$ . Für die Existenz des neutralen Elementes und der inversen Elemente sei  $b \in H$ . Da  $H$  abgeschlossen ist unter  $\circ$ , gilt  $b^n \in H$  für alle  $n \in \mathbb{N}$ . Nach Proposition 4.21 hat  $b$  eine endliche Ordnung in  $G$ . Definiere  $m =_{\text{def}} \text{ord}(b)$ . Dann gilt  $e = b^m \in H$  und  $e = b \circ b^{m-1}$ . Somit gehört das neutrale Element  $e$  zu  $H$  und  $b^{m-1}$  ist das inverse Element zu  $b$ . ■

**Korollar 4.28** Ist  $G$  eine endliche Gruppe und sind  $H$  und  $K$  Untergruppen von  $G$ , so ist  $H \cap K$  eine Untergruppe von  $G$ .

**Beweis:**  $H \cap K$  ist abgeschlossen unter den Gruppenoperationen. ■

**Korollar 4.29** Es seien  $G$  eine endliche Gruppe und  $a \in G$  ein beliebiges Element. Dann ist  $S_a =_{\text{def}} \{e, a, a^2, \dots, a^{\text{ord}(a)-1}\}$  die kleinste Untergruppe von  $G$ , die  $a$  enthält.



**Beweis:**  $S_a$  ist abgeschlossen unter den Gruppenoperationen. Jede Unter algebra, die  $a$  enthält, muss auch  $a^n$  für  $n \in \mathbb{N}$  enthalten. ■

**Definition 4.30** Eine Gruppe  $G$  heißt zyklisch, falls es ein  $b \in G$  gibt mit  $G = \{b^i \mid i \in \mathbb{Z}\}$ . Das Element  $b$  heißt erzeugendes Element (bzw. Generator) von  $G$ .

**Beispiele:**

1.  $\langle \mathbb{Z}, + \rangle$  ist zyklisch mit 1 als erzeugendem Element.
2.  $\langle \mathbb{Z}_n, +_n \rangle$  ist zyklisch mit 1 als erzeugendem Element.

**Korollar 4.31** Für eine endliche, zyklische Gruppe  $G$  mit dem Generator  $b \in G$  gilt  $|G| = \text{ord}(b)$ .

**Theorem 4.32** Es sei  $G$  eine zyklische Gruppe.

1. Ist  $|G| = \infty$ , so ist  $G$  isomorph zu  $\langle \mathbb{Z}, + \rangle$ .
2. Ist  $|G| = m < \infty$ , so ist  $G$  isomorph zu  $\langle \mathbb{Z}_m, +_m \rangle$ .

**Beweis:** (nur endliche Gruppen) Es sei  $G$  zyklisch mit erzeugendem Element  $b$  und endlich, d.h.,  $|G| = m$  für  $m \in \mathbb{N}_+$ . Somit ist  $G = \{b^i \mid i \in \{0, 1, \dots, m-1\}\}$  mit  $\text{ord}(b) = m$ . Wir definieren die folgende Abbildung:

$$h : \mathbb{Z}_m \rightarrow G : i \mapsto b^i$$

Dann ist  $h$  bijektiv (wegen  $|\mathbb{Z}_m| = |G|$ ) und es gilt:

$$\begin{aligned} h(i) \circ h(j) &= b^i \circ b^j \\ &= b^{i+j} \\ &= b^{s \cdot m + \text{mod}(i+j, m)} \\ &= e^s \circ b^{\text{mod}(i+j, m)} \\ &= b^{\text{mod}(i+j, m)} \\ &= b^{i+m \cdot j} \\ &= h(i +_m j) \end{aligned}$$

Damit ist das Theorem bewiesen. ■

**Beispiel:**  $\langle \mathbb{Z}_5^*, \cdot_5 \rangle$  ist eine zyklische Gruppe mit erzeugendem Element 2:

$$\{2^0, 2^1, 2^2, 2^3\} = \{1, 2, 4, 3\}$$

Somit gilt  $\langle \mathbb{Z}_5^*, \cdot_5 \rangle \cong \langle \mathbb{Z}_4, +_4 \rangle$  mittels der Abbildung:

$$0 \mapsto 1, \quad 1 \mapsto 2, \quad 2 \mapsto 4, \quad 3 \mapsto 3$$

Die *eulersche Phi-Funktion*  $\varphi : \mathbb{N}_+ \rightarrow \mathbb{N}_+$  ist definiert als:

$$\varphi(n) =_{\text{def}} |\mathbb{Z}_n^*|$$

Mit anderen Worten:  $\varphi(n)$  ist die Anzahl der zu  $n$  teilerfremden Zahlen.

**Lemma 4.33** *Es sei  $G$  eine endliche Gruppe mit  $|G| = n$ . Dann gilt  $\text{ord}(a)|n$  für alle Elemente  $a \in G$ .*

**Theorem 4.34 (Euler)** *Für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  und für alle  $a \in \mathbb{Z}_n^*$  gilt*

$$\text{mod}(a^{\varphi(n)}, n) = 1.$$

**Beweis:** Es sei  $a \in \mathbb{Z}_n^*$  mit  $k =_{\text{def}} \text{ord}(a)$ . Nach Lemma 4.33 gilt  $k|\varphi(n)$  und wir erhalten

$$\text{mod}(a^{\varphi(n)}, n) = \text{mod}(a^{k \cdot \frac{\varphi(n)}{k}}, n) = \text{mod}(1^{\frac{\varphi(n)}{k}}, n) = 1.$$

Damit ist das Theorem bewiesen. ■

**Theorem 4.35 (Fermat)** *Für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  gilt:*

$$n \text{ ist eine Primzahl} \iff \text{mod}(a^{n-1}, n) = 1 \text{ für alle } a \in \mathbb{Z}_n \setminus \{0\}$$

**Beweis:** Wir zeigen beide Richtungen einzeln.

( $\Rightarrow$ ) Es sei  $n$  eine Primzahl. Dann gilt  $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$  und  $\varphi(n) = n - 1$ . Nach Theorem 4.34 gilt somit  $\text{mod}(a^{n-1}, n) = 1$  für alle  $a \in \mathbb{Z}_n \setminus \{0\}$ .

( $\Leftarrow$ ) Es sei  $1 \leq p < n$  ein Teiler von  $n$ . Wir wollen zeigen, dass  $p = 1$  gilt. Nach Voraussetzung gilt  $\text{mod}(p^{n-1}, n) = 1$  und folglich  $p^{n-1} - 1 = k \cdot n = k \cdot k' \cdot p$  für geeignete  $k, k' \in \mathbb{Z}$ . Damit  $p$  sowohl  $p^{n-1}$  als auch 1 teilt, muss  $p = 1$  gelten. Somit besitzt  $n$  keine von 1 verschiedenen Teiler. Mithin ist  $n$  eine Primzahl.

Damit ist das Theorem bewiesen. ■

## 4.4 Endliche Körper\*

Zur Erinnerung: Ein Körper  $K = \langle K, +, \cdot \rangle$  ist eine Algebra mit:

(K1)  $\langle K, + \rangle$  ist eine abelsche Gruppe mit dem neutralen Element 0, wobei inverse Elemente mit  $-a$  für  $a \in S$  bezeichnet werden.

(K2)  $\langle K \setminus \{0\}, \cdot \rangle$  ist eine abelsche Gruppe mit dem neutralen Element 1, wobei inverse Elemente mit  $a^{-1}$  für  $a \in S \setminus \{0\}$  bezeichnet werden.

(K3) Es gelten die Distributivgesetze für alle  $a, b, c \in K$ :

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}$$

Wie im Falle von Gruppen identifizieren wir einen Körper mit seiner Trägermenge  $K$ .

**Beispiele:**

1.  $\mathbb{Q}, \mathbb{R}$  und  $\mathbb{C}$  (mit den üblichen Operationen) sind Körper.
2.  $\langle \mathbb{Z}_2, +_2, \cdot_2 \rangle$  ist ein Körper.
3.  $\langle \mathbb{Z}_4, +_4, \cdot_4 \rangle$  ist kein Körper, denn:  $2 \cdot_4 2 = 0 \notin \mathbb{Z}_4 \setminus \{0\}$

**Proposition 4.36** *In jedem Körper  $K$  gilt für alle  $a \in K$ :*

$$a \cdot 0 = 0 \cdot a = 0$$

**Beweis:** Es sei  $a \in K$ . Aus den Distributivgesetzen erhalten wir:

$$\begin{aligned} 0 + (a \cdot 0) &= a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0) \\ 0 + (0 \cdot a) &= 0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a) \end{aligned}$$

Mit Hilfe der Kürzungsregeln für Gruppen folgt  $0 = a \cdot 0 = 0 \cdot a$ . Damit ist die Proposition bewiesen. ■

**Proposition 4.37** *In jedem Körper  $K$  gilt für alle  $a, b \in K$ :*

$$a \cdot b = 0 \implies a = 0 \text{ oder } b = 0$$

(Wir sagen auch: Körper sind nullteilerfrei.)

**Beweis:** Es gelte  $a \cdot b = 0$ . Wir unterscheiden zwei Fälle:

- 1. Fall: Es sei  $a = 0$ . Dann gilt die Aussage.
- 2. Fall: Es sei  $a \neq 0$ . Dann gibt es ein multiplikatives Inverse  $a^{-1} \in K \setminus \{0\}$ . Somit gilt nach Voraussetzung und Proposition 4.36:

$$b = 1 \cdot b = a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$$

Damit ist die Proposition bewiesen. ■

**Theorem 4.38** Für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  gilt:

$$\langle \mathbb{Z}_n, +_n, \cdot_n \rangle \text{ ist ein Körper} \iff n \text{ ist eine Primzahl}$$

**Beweis:**  $\langle \mathbb{Z}_n, +_n \rangle$  ist für alle  $n \geq 2$  eine abelsche Gruppe; Distributivgesetze gelten offensichtlich. Wir müssen noch zeigen, wann  $\langle \mathbb{Z}_n \setminus \{0\}, \cdot_n \rangle$  eine (abelsche) Gruppe ist.

( $\Leftarrow$ ) Ist  $n$  eine Primzahl, so gilt  $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$ . Somit ist  $\langle \mathbb{Z} \setminus \{0\}, \cdot_n \rangle$  eine Gruppe.

( $\Rightarrow$ ) Wir zeigen die Kontraposition. Es sei  $n$  also keine Primzahl. Somit gibt es ein  $a \in \mathbb{Z} \setminus \{0\}$  mit  $\text{ggT}(a, n) > 1$ , d.h.,  $a \notin \mathbb{Z}_n^*$ . Es sei  $a \in \mathbb{Z} \setminus \{0\}$  minimal mit  $\text{ggT}(a, n) > 1$ . Dann gilt  $a|n$ . Es gibt somit  $b \in \mathbb{Z} \setminus \{0\}$  mit  $a \cdot b = n$  bzw.  $a \cdot_n b = 0$ . Somit ist  $\langle \mathbb{Z}_n \setminus \{0\}, \cdot_n \rangle$  kein Gruppoid, also auch keine Gruppe.

Damit ist das Theorem bewiesen. ■

Für einen Körper  $K$  bezeichnen wir mit  $K^* =_{\text{def}} K \setminus \{0\}$  die *multiplikative Gruppe*.

**Theorem 4.39** In jedem endlichen Körper  $K$  ist die multiplikative Gruppe  $K^*$  zyklisch.

**Beweis:** Mit  $K$  ist auch  $K^*$  endlich. Somit besitzt jedes Element von  $K^*$  eine endliche Ordnung in der Gruppe  $K^*$ . Es sei  $a \in K^*$  ein Element maximaler Ordnung. Wir müssen zeigen, dass  $\text{ord}(a) = |K^*|$  gilt. Dazu betrachten wir das Polynom

$$p(x) =_{\text{def}} x^{\text{ord}(a)} - 1.$$

Wir können nun wie folgt argumentieren:

1. Der Grad von  $p$  ist  $\text{ord}(a)$ .
2. Für alle  $b \in K^*$  gilt  $\text{ord}(b) | \text{ord}(a)$ .
3. Für alle  $b \in K^*$  gilt  $b^{\text{ord}(a)} = 1$ , d.h., alle  $b \in K^*$  sind Nullstellen von  $p$ .
4. Ein Polynom vom Grad  $\text{ord}(a)$  hat höchstens  $\text{ord}(a)$  Nullstellen, d.h.,  $\text{ord}(a) \geq |K^*|$ .

Damit folgt  $\text{ord}(a) = |K^*|$  und das Theorem ist bewiesen. ■

**Theorem 4.40** Für  $n \in \mathbb{N}$  mit  $n \geq 2$  gibt es genau dann einen Körper mit  $|K| = n$  Elementen, wenn  $n = p^k$  für eine geeignete Primzahl  $p$  sowie ein geeignetes  $k \in \mathbb{N}$  gilt. Sind  $K_1$  und  $K_2$  endliche Körper mit  $|K_1| = |K_2|$ , so gilt  $K_1 \cong K_2$ .

Der nach diesem Theorem (bis auf Isomorphie) eindeutige endliche Körper mit  $p^k$  Elementen heißt *Galoiskörper* und wird mit  $\text{GF}(p^k)$  bezeichnet.

**Beispiel:** Wir wollen den  $\text{GF}(4)$  konstruieren. Wie wir bereits wissen, ist  $\langle \mathbb{Z}_4, +_4, \cdot_4 \rangle$  kein Körper. Wir definieren also  $K =_{\text{def}} \{0, 1, a, b\}$ , wobei 0 das additive neutrale Element und 1 das multiplikative neutrale Element sind.

Zunächst legen wir die Multiplikation fest. Die zugehörige Verknüpfungstabelle erhalten wir durch Wahl von  $a$  als erzeugendes Element (mit  $a^2 = b$  und  $a^3 = 1$ ):

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

Durch die Multiplikation ergibt sich eine Verknüpfungstabelle für die Addition:

$+$	0	1	$a$	$b$
0	0	1	$a$	$b$
1	1	0	$b$	$a$
$a$	$a$	$b$	0	1
$b$	$b$	$a$	1	0

Die Einträge lassen sich wie folgt begründen:

- Die Einträge für das Nullelement 0 sind eindeutig festgelegt.
- Die Einträge für  $a$  ermitteln wir wie folgt:
  - $a + 1 \neq 1$ , denn aus  $a + 1 = 1$  folgt  $a = 0$ .
  - $a + 1 \neq a$ , denn aus  $a + 1 = a$  folgt  $1 = 0$ .
  - $a + 1 \neq 0$ , denn aus  $a + 1 = 0$  folgt  $0 = a + a^3 = a \cdot (1 + a^2) = a \cdot (1 + b)$  (wegen der Distributivgesetze), d.h.,  $1 + b = 0$  (wegen der Nullteilerfreiheit) und folglich  $1 + a = 1 + b$  bzw.  $a = b$ .

Somit gilt  $a + 1 = b$  und folglich  $a + b = a + a^2 = a \cdot (1 + a) = a \cdot b = 1$ .

- Die inversen Elemente werden eindeutig aufgeteilt.



---

# Literaturverzeichnis

---

- [GKP94] Ronald L. Graham, Donald E. Knuth und Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. 2. Auflage. Addison-Wesley Longman, Amsterdam, 1994.
- [Knu97] Donald E. Knuth. *The Art of Computer Programming. Volume 1 / Fundamental Algorithms*. 3. Auflage. Addison-Wesley, Reading, MA, 1997.
- [KP09] Bernd Kreußler und Gerhard Pfister. *Mathematik für Informatiker*. Springer-Verlag, Berlin, 2009.
- [MM06] Christoph Meinel und Martin Mundhenk. *Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen. Eine Einführung*. 3., überarbeitete und erweiterte Auflage. B. G. Teubner Verlag, Wiesbaden, 2006.
- [Ste07] Angelika Steger. *Diskrete Strukturen. Band 1: Kombinatorik-Graphentheorie-Algebra*. 2. Auflage. Springer-Verlag, Berlin, 2007.
- [SS02] Thomas Schickinger und Angelika Steger. *Diskrete Strukturen. Band 2: Wahrscheinlichkeitstheorie und Statistik*. Springer-Verlag, Berlin, 2002.
- [Wag03] Klaus W. Wagner. *Theoretische Informatik. Eine kompakte Einführung*. 2. überarbeitete Auflage. Springer-Verlag, Berlin, 2003.
- [WHK04] Manfred Wolff, Peter Hauck und Wolfgang Küchlin. *Mathematik für Informatik und Bioinformatik*. Springer-Verlag, Berlin, 2004.
- [Wil05] Herbert S. Wilf. *generatingfunctionology*. 3. Auflage. CRC Press, Boca Raton, FL, 2005.

