

WS 2005/06

# Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik  
TU München

<http://www14.in.tum.de/lehre/2005WS/ds/>

Wintersemester 2005/06

# Kapitel 0 Organisatorisches

- Vorlesungen:
  - Di 8:30–10:00 (MW2001), Fr 8:30–10:00 (MW1801)
- Übung:
  - 2SWS Tutorübung: bitte anmelden unter <https://grundstudium.in.tum.de/>
- Umfang:
  - 4V+2TÜ, 8 ECTS-Punkte
- Sprechstunde:
  - Fr 11:00–12:00 oder nach Vereinbarung

- Übungsleitung:
  - Dr. W. Meixner, MI 03.09.040 ([meixner@in.tum.de](mailto:meixner@in.tum.de))  
Sprechstunde: Fr 10:15–11:00 oder nach Vereinbarung
- Sekretariat:
  - Frau Schmidt, MI 03.09.052 ([schmiann@in.tum.de](mailto:schmiann@in.tum.de))
- Webseite:

<http://www14.in.tum.de/lehre/2005WS/ds/>

- Übungsaufgaben und Klausur:
  - Ausgabe jeweils am Freitag in der Vorlesung
  - Abgabe eine Woche später
  - Besprechung in der Tutorübung
- Klausur:
  - Zwischenklausur (50% Gewicht) am 10. Dezember 2005
  - Endklausur (50% Gewicht) am 11. Februar 2006
  - Wiederholungsklausur am 22. April 2006
  - bei den Klausuren sind *keine* Hilfsmittel außer einem handbeschriebenen DIN-A4-Blatt zugelassen
  - Zulassungsvoraussetzung (außer für Studierende im Diplomstudiengang Informatik) sind 40% der erreichbaren Hausaufgabenpunkte
  - vorauss. 12 Übungsblätter, das letzte am 27. Januar 2006, jedes 40 Punkte

# 1. Ziel der Vorlesung

Der Zweck dieser Vorlesung ist der Erwerb der Grundlagen

- beim Umgang mit logischen, algebraischen und algorithmischen Kalkülen,
- beim Lösen kombinatorischer Problemstellungen,
- bei der quantitativen Betrachtung der Effizienz von Lösungsmethoden und Algorithmen

## 2. Wesentliche Inhalte

- Wiederholung grundlegender Begriffe der Mengenlehre und der Aussagenlogik
- Algebraische Strukturen (elementare Grundlagen aus der Gruppen-, Ring- und Körpertheorie)
- Kombinatorik (elementare Zählmethoden und kombinatorische Identitäten)
- Graphen und Algorithmen (grundlegende Definitionen, elementare Algorithmen)

### 3. Literatur



Steger, Angelika:

*Diskrete Strukturen, Band 1: Kombinatorik, Graphentheorie, Algebra.*

Springer, 2001



Gries, David und Schneider, Fred B.:

*A Logical Approach to Discrete Math.*

Springer, 1993



Aigner, Martin:

*Diskrete Mathematik.*

Vieweg, 1999 (3. Auflage)

-  Kreher, Donald L. und Stinson, Douglas R.:  
*Combinatorial Algorithms: Generation, Enumeration, and Search.*  
CRC Press, 1999
-  Rosen, Kenneth H.:  
*Discrete Mathematics and Its Applications.*  
McGraw-Hill, 1995
-  Graham, Ronald L., Knuth, Donald E. und Patashnik, Oren:  
*Concrete Mathematics: A Foundation for Computer Science.*  
Addison-Wesley, 1994
-  Pemmaraju, Sriram und Skiena, Steven:  
*Computational Discrete Mathematics: Combinatorics and Graph Theory with Mathematica*  
Cambridge University Press, 2003

# Kapitel I Einleitung, Grundlagen

## 1. Was sind Diskrete Strukturen?

Der relativ junge Begriff „Diskrete Strukturen“ oder auch „Diskrete Mathematik“ umfasst Kombinatorik, Graphentheorie, Optimierung, Algorithmik und einiges mehr. Das Gebiet beschäftigt sich mit **wohlunterschiedenen** Objekten.

Wohlunterschieden sind z. B. die Elemente der Menge  $\mathbb{N}$  der natürlichen Zahlen, jedoch nicht die Elemente der reellen Zahlen  $\mathbb{R}$ . Diskret bedeutet insbesondere, dass die betrachteten Mengen im Allgemeinen **endlich** oder **abzählbar unendlich** sind.

## 2. Zusammenwirken mit / Abgrenzung von anderen Bereichen

Letztlich werden fast alle Bereiche der Mathematik benutzt; andererseits hat die Diskrete Mathematik großen Einfluss auf zahlreiche Bereiche der Mathematik und Informatik. Gelegentlich werden jedoch andere als die gebräuchlichen methodischen Grundlagen benötigt, z. B. da die betrachteten Funktionen im Allgemeinen nicht stetig sind.

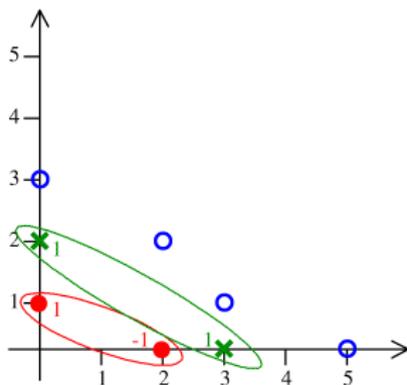
## Beispiel 1

Polynome als Funktionen (mit Ableitung, Tangenten, ...) sind nicht unbedingt Stoff der Diskreten Mathematik; ein Beispiel für eine **diskrete Betrachtung** sind dagegen die sogenannten *Newton-Polytope*:

$$\begin{array}{ll} y - x^2: & y^2 + x^3: \\ +y \mapsto (1; 0; 1) & +y^2 \mapsto (1; 0; 2) \\ -x^2 \mapsto (-1; 2; 0) & +x^3 \mapsto (1; 3; 0) \end{array}$$

Die Monome über  $\{x, y\}$  werden also als (Faktor;  $x$ -Potenz;  $y$ -Potenz) dargestellt.

## Beispiel 2



Die blauen Kreise entstehen durch Vektoraddition der grünen Kreuze und der roten Punkte und stellen die Polytope des Produkts

$$(y - x^2) (y^2 + x^3) = y^3 + yx^3 - y^2x^2 - x^5$$

dar (Minkowski-Addition).

### 3. Komplexität: Ein warnendes Beispiel

$$\begin{aligned}(k+2) \cdot & \left( 1 - (wz + h + j - q) \right)^2 \\ & - \left( (gk + 2g + k + 1)(h + j) + h - z \right)^2 \\ & - \left( 2n + p + q + z - e \right)^2 \\ & - \left( 16(k+1)^3(k+2)(n+1)^2 + 1 - f^2 \right)^2 \\ & - \left( e^3(e+2)(a+1)^2 + 1 - o^2 \right)^2 \\ & - \left( (a^2 - 1)y^2 + 1 - x^2 \right)^2 \\ & - \left( 16r^2y^4(a^2 - 1) + 1 - u^2 \right)^2 \\ & - \left( n + l + v - y \right)^2 \\ & - \left( \left( (a + u^2(u^2 - a))^2 - 1 \right) (n + 4dy)^2 + 1 - (x + cu)^2 \right)^2\end{aligned}$$

$$\begin{aligned}
& - \left( (a^2 - 1)l^2 + 1 - m^2 \right)^2 \\
& - \left( q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x \right)^2 \\
& - \left( z + pl(a - p) + t(2ap - p^2 - 1) - pm \right)^2 \\
& - \left( ai + k + 1 - l - i \right)^2 \\
& - \left( p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m \right)^2 \Big)
\end{aligned}$$

Die positiven Werte, die dieses Polynom mit  $(a, \dots, z) \in \mathbb{N}_0^{26}$  annimmt, sind genau alle Primzahlen.

Deshalb empfiehlt sich oft die Verwendung eines symbolischen Mathematikprogramms, z. B. Maple.

## 4. Mathematische und notationelle Grundlagen

### 4.1 Mengen

#### Beispiel 3

$$A_1 = \{2, 4, 6, 8\};$$

$$A_2 = \{0, 2, 4, 6, \dots\} = \{n \in \mathbb{N}_0; n \text{ gerade}\}$$

#### Bezeichnungen:

$x \in A \Leftrightarrow A \ni x$	$x$ Element $A$
$x \notin A$	$x$ nicht Element $A$
$B \subseteq A$	$B$ Teilmenge von $A$
$B \subsetneq A$	$B$ echte Teilmenge von $A$
$\emptyset$	leere Menge, dagegen:
$\{\emptyset\}$	Menge mit leerer Menge als Element

# Spezielle Mengen:

- $\mathbb{N} = \{1, 2, \dots\}$
- $\mathbb{N}_0 = \{0, 1, 2, \dots\}$
- $\mathbb{Z}$  = Menge der ganzen Zahlen
- $\mathbb{Q}$  = Menge der Brüche (rationalen Zahlen)
- $\mathbb{R}$  = Menge der reellen Zahlen
- $\mathbb{C}$  = Menge der komplexen Zahlen
- $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$  Restklassen bei Division durch  $n$
- $[n] = \{1, 2, \dots, n\}$

# Operationen auf Mengen:

- $|A|$  Kardinalität der Menge  $A$
- $A \cup B$  Vereinigungsmenge
- $A \cap B$  Schnittmenge
- $A \setminus B$  Differenzmenge
- $A \Delta B := (A \setminus B) \cup (B \setminus A)$  symmetrische Differenz
- $A \times B := \{(a, b); a \in A, b \in B\}$  kartesisches Produkt
- $A \uplus B$  Disjunkte Vereinigung: die Elemente werden nach ihrer Herkunft unterschiedlich gekennzeichnet
- $\bigcup_{i=0}^n A_i$  Vereinigung der Mengen  $A_0, A_1, \dots, A_n$
- $\bigcap_{i \in I} A_i$  Schnittmenge der Mengen  $A_i$  mit  $i \in I$
- $P(M) := 2^M := \{N; N \subseteq M\}$  Potenzmenge der Menge  $M$

## Beispiel 4

Für  $M = \{a, b, c, d\}$  ist

$$P(M) = \{ \emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \\ \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \\ \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \\ \{a, b, c, d\} \\ \}$$

## Satz 5

Die Menge  $M$  habe  $n$  Elemente,  $n \in \mathbb{N}$ . Dann hat  $P(M)$   $2^n$  Elemente!

### Beweis:

Sei  $M = \{a_1, \dots, a_n\}$ ,  $n \in \mathbb{N}$ . Um eine Menge  $L \in P(M)$  (d.h.  $L \subseteq M$ ) festzulegen, haben wir für jedes  $i \in [n]$  die (unabhängige) Wahl,  $a_i$  zu  $L$  hinzuzufügen oder nicht. Damit ergeben sich  $2^{|[n]|} = 2^n$  verschiedene Möglichkeiten. □

### Bemerkungen:

- 1 Der obige Satz gilt auch für  $n = 0$ , also die leere Menge  $M = \emptyset$ .
- 2 Die leere Menge ist in jeder Menge **als Teilmenge** enthalten.
- 3  $P(\emptyset)$  enthält **als Element** genau  $\emptyset$  (also  $P(\emptyset) \neq \emptyset$ ).

## 4.2 Relationen und Abbildungen

Seien  $A_1, A_2, \dots, A_n$  Mengen. Eine Relation über  $A_1, \dots, A_n$  ist eine Teilmenge

$$R \subseteq A_1 \times A_2 \times \dots \times A_n = \prod_{i=1}^n A_i$$

Andere Schreibweise (Infixnotation) für  $(a, b) \in R$ :  $aRb$ .

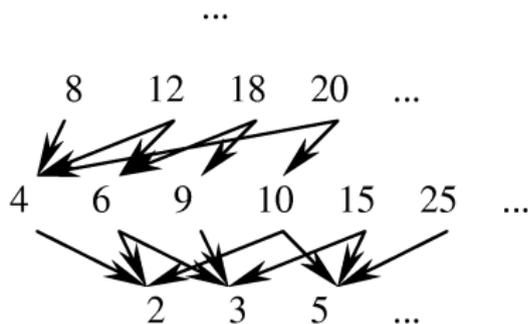
Eigenschaften von Relationen ( $R \subseteq A \times A$ ):

- reflexiv:  $(a, a) \in R \quad \forall a \in A$
- symmetrisch:  $(a, b) \in R \Rightarrow (b, a) \in R \quad \forall a, b \in A$
- asymmetrisch:  $(a, b) \in R \Rightarrow (b, a) \notin R \quad \forall a, b \in A$
- antisymmetrisch:  $[(a, b) \in R \wedge (b, a) \in R] \Rightarrow a = b \quad \forall a, b \in A$
- transitiv:  $[(a, b) \in R \wedge (b, c) \in R] \Rightarrow (a, c) \in R \quad \forall a, b, c \in A$
- Äquivalenzrelation: reflexiv, symmetrisch und transitiv
- Partielle Ordnung (aka *partially ordered set*, *poset*): reflexiv, antisymmetrisch und transitiv

## Beispiel 6

$(a, b) \in R$  sei  $a|b$  „ $a$  teilt  $b$ “,  $a, b \in \mathbb{N}$ .

Die graphische Darstellung ohne reflexive und transitive Kanten heißt **Hasse-Diagramm**:



Die Relation  $|$  stellt eine *partielle Ordnung* dar.

## Definition 7

Sei  $R \subseteq A \times B$  eine **binäre** Relation. Dann heißt

$$\{a \in A; (\exists b \in B)[(a, b) \in R]\}$$

das **Urbild** der Relation  $R$  und

$$\{b \in B; (\exists a \in A)[(a, b) \in R]\}$$

das **Bild** der Relation  $R$ .

## Definition 8

Sei  $R \subseteq A \times B$  eine **binäre** Relation. Dann heißt

$$R^{-1} := \{(b, a); (a, b) \in R\}$$

die **inverse Relation** zu  $R$ .

## Definition 9

Seien  $R \subseteq A \times B$  und  $S \subseteq B \times C$  binäre Relationen. Dann heißt

$$R \circ S := \{(a, c) \in A \times C; (\exists b \in B)[(a, b) \in R \text{ und } (b, c) \in S]\}$$

das **Produkt** der Relationen  $R$  und  $S$ . Es wird oft auch einfach durch  $RS$  bezeichnet.

## Satz 10

Das Relationenprodukt  $\circ$  ist *assoziativ* und *distributiv über  $\cup$  und  $\cap$* .

Beweis:

Hausaufgabe!



## Definition 11

Sei  $R \subseteq A \times A$  eine binäre Relation. Dann ist

- 1  $R^0 := \{(a, a); a \in A\}$  ( $=: \text{Id}_A$ )
- 2  $R^{n+1} := R^n \circ R$  für  $n \in \mathbb{N}_0$

## Beispiel 12

Sei  $\text{Kind}$  die Relation

$$\{(k, v); k \text{ ist Kind von } v\}$$

Dann bezeichnet  $\text{Kind}^2$  die **Enkel**-Relation.

## Definition 13

Sei  $R \subseteq A \times A$  eine binäre Relation.

- 1 Dann ist der reflexive (symmetrische, transitive) Abschluss (auch als reflexive, symmetrische bzw. transitive Hülle bezeichnet) die kleinste (im mengentheoretischen Sinn) Relation, die  $R$  enthält und reflexiv (symmetrisch, transitiv) ist.
- 2 Die transitive Hülle von  $R$  wird oft mit  $R^+$  bezeichnet.
- 3 Die reflexive transitive Hülle von  $R$  wird gewöhnlich mit  $R^*$  bezeichnet.

## Beispiel 14

Die transitive Hülle der Relation „die Mutter von  $k$  ist  $m$ “ ist die Menge der Tupel  $(k', m')$ , so dass gilt:

$k'$  hat seine Mitochondrien von  $m'$  geerbt.

## 4.3 Funktionen

Sei  $f : A \rightarrow B$  eine *Funktion* von  $A$  nach  $B$  (also eine Relation mit genau einem Paar  $(f(a), a) \quad \forall a \in A$ ).

(Eine solche Relation heißt auch **rechtseindeutig** und **rechtstotal**.)

- Das *Urbild* von  $b \in B$ :  $f^{-1}(b) = \{a \in A; f(a) = b\}$ .
- Schreibweisen:  $(A' \subseteq A, B' \subseteq B)$ 
  - $f(A') = \bigcup_{a \in A'} \{f(a)\}$
  - $f^{-1}(B') = \bigcup_{b \in B'} f^{-1}(b)$
- Sind  $f : A \rightarrow B$  und  $g : B \rightarrow C$  Funktionen, so ist ihre Komposition  $g \circ f$  gemäß der entsprechenden Definition für das Relationenprodukt definiert.

## Eigenschaften von $f : A \rightarrow B$ :

- $f$  injektiv:  $(\forall b \in B) \left[ |f^{-1}(b)| \leq 1 \right]$
- $f$  surjektiv:  $(\forall b \in B) \left[ |f^{-1}(b)| \geq 1 \right]$
- $f$  bijektiv:  $(\forall b \in B) \left[ |f^{-1}(b)| = 1 \right]$ , d.h. injektiv und surjektiv
- Ist  $f : A \rightarrow B$  eine Bijektion, dann ist auch  $f^{-1}$  eine bijektive Funktion.

## Eigenschaften von $f : A \rightarrow B$ :

Existiert eine Bijektion von  $A$  nach  $B$ , haben  $A$  und  $B$  *gleiche Kardinalität*.

Warnung: Es gibt  $A, B$  mit  $A \subsetneq B$ , aber  $|A| = |B|$ !

Beispiel 15 ( $|\mathbb{Z}| = |\mathbb{N}_0|$ )

$$f : \mathbb{Z} \ni z \mapsto \begin{cases} 2z & z \geq 0 \\ -2z - 1 & z < 0 \end{cases} \in \mathbb{N}_0$$

Sei  $R$  eine Relation über  $A$ ,  $\tilde{R}$  eine Relation über  $B$ .

- Eine Funktion  $f : A \rightarrow B$  heißt **Homomorphismus** von  $R$  nach  $\tilde{R}$ , falls gilt:

$$(a_1, \dots, a_k) \in R \Rightarrow (f(a_1), \dots, f(a_k)) \in \tilde{R}$$

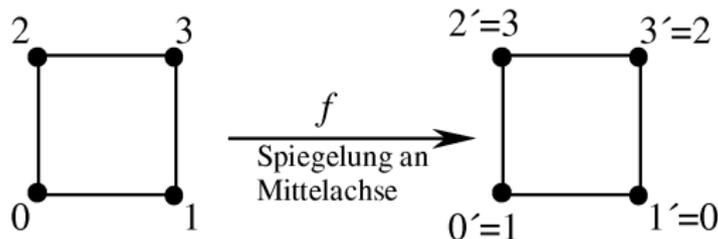
- Eine Bijektion  $f : A \rightarrow B$  heißt **Isomorphismus** zwischen  $R$  und  $\tilde{R}$ , falls gilt:

$$(a_1, \dots, a_k) \in R \iff (f(a_1), \dots, f(a_k)) \in \tilde{R}$$

## Beispiel 16

Relation: Kanten eines Graphen

$$E = \{\{0, 1\}, \{0, 2\}, \{1, 3\}, \{2, 3\}\}$$



$$E' = f(E) = \{\{0', 1'\}, \{0', 2'\}, \{1', 3'\}, \{2', 3'\}\}$$

$f$  ist ein Isomorphismus.

# Schreibweisen für wichtige Funktionen:

- $\lfloor \cdot \rfloor : \mathbb{R} \rightarrow \mathbb{Z}$   
 $\mathbb{R} \ni x \mapsto \lfloor x \rfloor := \max\{y \in \mathbb{Z}; y \leq x\} \in \mathbb{Z}$   
(„untere Gaußklammer“, „*floor*“, „*entier*“)
- $\lceil \cdot \rceil : \mathbb{R} \rightarrow \mathbb{Z}$   
 $\mathbb{R} \ni x \mapsto \lceil x \rceil := \min\{y \in \mathbb{Z}; y \geq x\} \in \mathbb{Z}$   
(„obere Gaußklammer“, „*ceiling*“)

## Beispiel 17

$$\lfloor \pi \rfloor = 3, \lfloor -\pi \rfloor = -4, \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 0 & x \in \mathbb{Z} \\ 1 & \text{sonst} \end{cases}$$

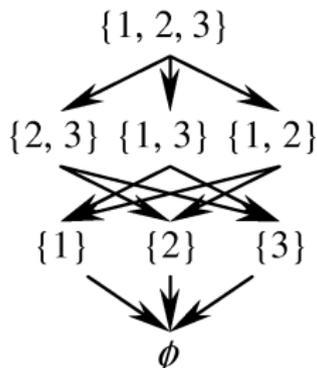
## 4.4 Partielle Ordnungen

Sei  $(S, \preceq)$  eine partielle Ordnung.

### Beispiel 18

$S = P(A)$ ,  $\preceq \equiv \subseteq$ ,  $A = \{1, 2, 3\}$

Hassediagramm:



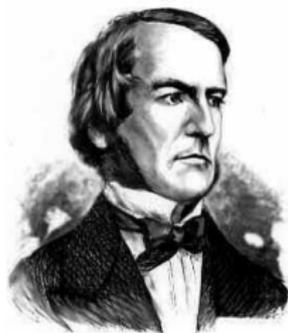
# Eigenschaften partieller Ordnungen:

- $a, b \in S$  heißen **vergleichbar** (bzgl.  $\preceq$ ), falls  $a \preceq b$  oder  $b \preceq a$ , sonst **unvergleichbar**.
- Ein Element  $a \in S$  heißt **minimal**, falls  $(\nexists b \in S)[b \neq a \wedge b \preceq a]$ .
- Ein Element  $a \in S$  heißt **maximal**, falls  $(\nexists b \in S)[b \neq a \wedge a \preceq b]$ .
- Eine partielle Ordnung heißt **linear** oder **vollständig**, falls sie keine unvergleichbaren Elemente enthält (z. B.  $(\mathbb{N}_0, \leq)$ ).

## 4.5 Boolesche Ausdrücke und Funktionen

Oft ordnen wir Aussagen über irgendwelche Gegebenheiten die Werte *true* oder *false* zu. Daneben verwenden wir auch Verknüpfungen solcher Aussagen mittels Operatoren wie z.B. „und“, „oder“, oder der Negation.

Der [Boolesche Aussagenkalkül](#) stellt für dieses Vorgehen einen formalen Rahmen dar.



George Boole

lived from 1815 to 1864

**Boole** approached logic in a new way reducing it to a simple algebra, incorporating logic into mathematics. He also worked on differential equations, the calculus of finite differences and general methods in probability.

[more on George Boole](#)

Wir betrachten nun die Menge  $\{t, f\}$  (manchmal auch  $\{1, 0\}$  oder  $\{0, 1\}$  oder  $\{1, -1\}$ ), deren Elemente für *true* und *false* stehen.

## (Unäre und) binäre Verknüpfungen boolescher Werte

		$\equiv$															
		$n \neq$															
		$a$															
		$n$															
		$o$															
		$r$															
		$\vee$	$\Leftarrow$	$\Rightarrow$	$=$	$\wedge$	$d$	$\neq$									
<i>t</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>f</i>								
<i>t</i>	<i>f</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>f</i>	<i>f</i>	<i>f</i>	<i>f</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>f</i>	<i>f</i>	<i>f</i>	<i>f</i>	
<i>f</i>	<i>t</i>	<i>t</i>	<i>t</i>	<i>f</i>	<i>f</i>	<i>t</i>	<i>t</i>	<i>f</i>	<i>f</i>	<i>t</i>	<i>t</i>	<i>f</i>	<i>f</i>	<i>t</i>	<i>t</i>	<i>f</i>	
<i>f</i>	<i>f</i>	<i>t</i>	<i>f</i>	<i>t</i>	<i>f</i>	<i>t</i>	<i>f</i>	<i>t</i>	<i>f</i>	<i>t</i>	<i>f</i>	<i>t</i>	<i>f</i>	<i>t</i>	<i>f</i>	<i>t</i>	

## Bemerkungen:

- 1 Die Bedeutung von  $\equiv$  (und damit  $\not\equiv$ ) ist klar.  $\equiv$  wird oft, vor allem in Beweisen, auch als

$\Leftrightarrow$

geschrieben (im Englischen: iff, if and only if).

- 2 Für zwei boolesche Aussagen  $A$  und  $B$  ist  $A \Rightarrow B$  falsch genau dann wenn  $A = t$  und  $B = f$ .
- 3  $A \Rightarrow B$  ist damit äquivalent mit  $\neg A \vee B$ .
- 4  $A \Rightarrow B$  ist damit auch äquivalent mit  $\neg B \Rightarrow \neg A$ .

## Wichtige Beobachtung:

Gilt also (oder beweisen wir korrekt)  $A \Rightarrow f$  (also: „aus der Bedingung/Annahme  $A$  folgt ein Widerspruch“), so ist  $A$  falsch!

## 4.6 Beweistechniken

Die meisten mathematischen Behauptungen sind von der Form

$$A \Rightarrow B \text{ bzw. } A_1, \dots, A_k \Rightarrow B.$$

Um  $A \Rightarrow B$  zu beweisen, können wir zeigen:

- 1 Unter der Annahme  $A$  können wir  $B$  zeigen (**direkter Beweis**).
- 2 Unter der Annahme  $\neg B$  können wir  $\neg A$  zeigen (**indirekter Beweis**).
- 3 Unter der Annahme  $\neg B$  können wir einen Widerspruch zeigen (**Widerspruchsbeweis**).

## Beispiel 19 (Direkter Beweis)

### Satz 20

Sei  $n \in \mathbb{N}_0$  ungerade, dann ist auch  $n^2$  ungerade.

#### Beweis:

$$n \in \mathbb{N}_0 \text{ ungerade} \Rightarrow (\exists m \in \mathbb{N}_0) [n = 2m + 1] \Rightarrow n^2 = (2m + 1)^2 = \underbrace{4m^2 + 4m}_{\text{gerade}} + 1 \Rightarrow n^2 \text{ ungerade.} \quad \square$$

$\underbrace{\hspace{10em}}_{\text{ungerade}}$

## Beispiel 21 (Indirekter Beweis)

### Satz 22

Sei  $n \in \mathbb{N}_0$ . Falls  $n^2$  gerade ist, dann ist auch  $n$  gerade.

#### Beweis:

Die Aussage ist gleichbedeutend mit „Falls  $n \in \mathbb{N}_0$  ungerade, dann ist auch  $n^2$  ungerade.“

Diese Aussage wurde in Satz 20 bewiesen. □

## Beispiel 23 (Beweis durch Widerspruch)

Wir nehmen an, dass die zu zeigende Aussage falsch ist und führen diese Annahme zu einem Widerspruch.

### Satz 24

$\sqrt{3}$  ist irrational, d. h.  $\sqrt{3} \notin \mathbb{Q}$

#### Beweis:

Widerspruchsannahme:  $\sqrt{3} \in \mathbb{Q}$ .

$$\Rightarrow \sqrt{3} = \frac{p}{q}, p, q \in \mathbb{N}, \text{ggT}(p, q) = 1 \quad (*)$$

$$\Rightarrow 3q^2 = p^2 \Rightarrow 3|p \Rightarrow (\exists k \in \mathbb{N}_0) [p = 3k]$$

$$\Rightarrow 3q^2 = 9k^2 \Rightarrow q^2 = 3k^2 \Rightarrow 3|q \Rightarrow 3|\text{ggT}(p, q)$$

Das ist ein Widerspruch zu (\*). □

## Vollständige Induktion

Wir wollen zeigen, dass eine Aussage  $P(n)$  für alle  $n \in \mathbb{N}_0$  gilt.

Wir zeigen zunächst den **Induktionsanfang**, also  $P(0)$ , und folgern dann aus der **Induktionsvoraussetzung**, also der Annahme  $P(n)$  bzw. den Annahmen  $P(0), P(1), \dots, P(n)$ , die Behauptung  $P(n + 1)$ .

## Beispiel 25

## Satz 26

$$\sum_{i=0}^n i = \frac{n \cdot (n + 1)}{2}$$

Beweis:

Induktionsanfang:  $n = 0$  trivial  $0 = 0$

Induktionsannahme:  $P(n)$ , also Satz richtig für  $n$

Induktionsschluss:

$$\begin{aligned}\sum_{i=0}^{n+1} i &= \sum_{i=0}^n i + n + 1 \stackrel{\text{(IV)}}{=} \frac{n \cdot (n + 1)}{2} + n + 1 = \\ &= \frac{2 \cdot (n + 1) + n \cdot (n + 1)}{2} = \frac{(n + 1)(n + 2)}{2}\end{aligned}$$

Dies ist  $P(n + 1)$ , die Behauptung für  $n + 1$ . □

# Das Schubfachprinzip (*pigeon hole principle*)

## Satz 27

Sei  $f : X \rightarrow Y$ , sei  $\infty > |X| > |Y| \geq 1$ , dann

$$(\exists y \in Y) [|f^{-1}(y)| \geq 2]$$

## Beweis:

Sei  $|X| = n$ ,  $|Y| = m$ , damit  $n > m$ . Widerspruchsannahme: Kein  $y \in Y$  hat mehr als ein Urbild in  $X$ . Die Bilder der ersten  $m$  Elemente aus  $X$  müssen dann notwendigerweise verschieden sein. Damit hat jedes  $y \in Y$  ein Urbild in  $X$ . Da  $f$  total ist, muss das Bild des  $(m + 1)$ -ten Elements aus  $X$  dann als Bild ein Element aus  $Y$  haben, das bereits Bild eines anderen  $x \in X$  ist. Dies ist ein Widerspruch zur Annahme. □

## Beispiele:

- Seien 13 oder mehr Personen in einem Raum. Dann haben mindestens 2 der Personen im gleichen Monat Geburtstag.

- Behauptung: In jeder Menge  $P$  von Personen ( $|P| \geq 2$ ) gibt es immer mindestens 2 Personen, die gleich viele (andere) Personen in der Menge kennen („kennen“ symmetrische Relation).

## Beweis:

- 1 Überlegung: Sei  $n = |P|$ . Wir betrachten die Abbildung  $P \ni p \mapsto \# \text{ Personen, die } p \text{ kennt} \in \{0, \dots, n-1\}$
- 2 Weitere Überlegung:
  - 1 0 kommt als Bild nicht vor (jeder kennt mindestens eine andere Person).  
 $\Rightarrow |\text{Urbildmenge}| = n > |\text{Bildmenge}| = n-1$ . Das Schubfachprinzip liefert die Behauptung.
  - 2 0 kommt als Bild vor.  
 $\Rightarrow$  Es gibt also (wegen der Symmetrie) mindestens eine Person, die kein anderer kennt. Also ist der Wertebereich der Funktion  $\subseteq \{0, 1, \dots, n-2\}$ . Das Schubfachprinzip liefert nunmehr ebenfalls den Beweis.



# Das verallgemeinerte Schubfachprinzip

## Satz 28

Sei  $f : X \rightarrow Y$ ,  $\infty > |X| \geq |Y| \geq 1$ . Dann existiert ein  $y \in Y$ , so dass

$$|f^{-1}(y)| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil .$$

## Beweis:

Es gilt  $|X| = \left| \bigcup_{y \in Y} f^{-1}(y) \right| = \sum_{y \in Y} |f^{-1}(y)|$ . Das zweite „=“ gilt, da die  $f^{-1}(y)$  alle paarweise disjunkt sind!

Widerspruchsannahme:

$$(\forall y \in Y) \left[ |f^{-1}(y)| \leq \left\lceil \frac{|X|}{|Y|} \right\rceil - 1 \right]$$

Da

$$\left\lceil \frac{|X|}{|Y|} \right\rceil - 1 \leq \frac{|X| + |Y| - 1}{|Y|} - 1 = \frac{|X| - 1}{|Y|}$$

folgt mit der Widerspruchsannahme

$$|X| = \sum_{y \in Y} |f^{-1}(y)| \leq |Y| \cdot \frac{|X| - 1}{|Y|} = |X| - 1$$

Dies stellt einen Widerspruch dar. □

# Ein Beispiel aus der Ramsey-Theorie:

## Satz 29

*In jeder Menge von 6 Personen gibt es 3 Personen, die sich gegenseitig kennen, oder 3 Personen, von denen keiner die beiden anderen kennt.*

## Beweis:

$P = \{p_1, p_2, \dots, p_6\}$ . Betrachte die Abbildung

$$\begin{aligned} &\{2, \dots, 6\} \rightarrow \{0, 1\} \\ &\{2, \dots, 6\} \ni i \mapsto \begin{cases} 1 & \text{„}p_1 \text{ kennt } p_i\text{“} \\ 0 & \text{„}p_1 \text{ kennt } p_i \text{ nicht“} \end{cases} \end{aligned}$$

Aus dem **verallgemeinerten Schubfachprinzip** folgt: Es gibt mindestens 3 Leute  $\in \{p_2, \dots, p_6\}$ , die  $p_1$  kennen, oder es gibt mindestens 3 Leute, die  $p_1$  nicht kennen.

Wir betrachten die erste Alternative, die zweite ist analog. O. B. d. A. kennt  $p_1$   $p_2$ ,  $p_3$  und  $p_4$ .

### 1. Fall:

$(\exists p_i, p_j \in \{p_2, p_3, p_4\}) [i \neq j \text{ und } p_i \text{ kennt } p_j]$ , z. B.  $i = 2, j = 4$ . Dann erfüllen  $\{p_1, p_i, p_j\}$  den ersten Teil der Behauptung.

### 2. Fall: (Komplement des 1. Falls!)

$(\forall p_i, p_j \in \{p_2, p_3, p_4\}) [i \neq j \Rightarrow p_i \text{ kennt } p_j \text{ nicht}]$ . Dann erfüllen  $\{p_2, p_3, p_4\}$  den zweiten Teil der Behauptung. □

## Beispiel 30 (Indirekter Beweis, Wohlordnungseigenschaft)

### Satz 31

Sei  $S$  eine endliche Menge  $\neq \emptyset$ , und sei  $f : S \rightarrow S$  eine Abbildung von  $S$  in  $S$ . Dann gilt:

$$(\exists r \in \mathbb{N})[f^r(S) = f(f^r(S))].$$

Dabei ist  $f^0 : S \rightarrow S$  als die Identität auf  $S$  und, für alle  $n \in \mathbb{N}_0$ ,  $f^{n+1}$  als  $f \circ f^n$  definiert.

## Beweis:

Falls  $f$  bijektiv ist, dann erfüllt  $r = 1$  die Behauptung. Wir nehmen daher an, dass  $f$  nicht bijektiv ist, also  $f(S) \subsetneq S$ . Man beachte, dass für alle  $m \in \mathbb{N}_0$  gilt, dass  $f^{m+1}(S) \subseteq f^m(S)$ !

**Weitere Annahme:** Für alle  $m \in \mathbb{N}_0$  gilt  $f^{m+1}(S) \subsetneq f^m(S)$ .

In diesem Fall hätte die Menge  $\{|f^m(S)|; m \in \mathbb{N}_0\} \subseteq \mathbb{N}_0$  kein *kleinstes Element*, da stets  $|f^{m+1}(S)| < |f^m(S)|$ .

**Widerspruch zur Wohlordnungseigenschaft!**

Sei also  $m \in \mathbb{N}$  minimal mit der Eigenschaft

$$f^{m+1}(S) = f^m(S) .$$

Dann erfüllt  $r = m$  die Behauptung. □

## Beispiel 32

### Satz

Sei  $n \in \mathbb{N}$ ,  $n \geq 3$  und  $n$  ungerade. Dann lässt sich  $n$  als Differenz zweier Quadratzahlen darstellen.

### Beweis:

Falls  $n = x^2 - y^2$  mit  $x, y \in \mathbb{N}$ ,  $x > y$ , dann gilt  $n = (x - y)(x + y)$ .

Sei nun  $s := x + y$  und  $t := x - y$ . Dann ist

$$s > t > 0$$

$$n = s \cdot t$$

$$x = (s + t)/2$$

$$y = (s - t)/2$$

Also müssen  $s$  und  $t$  beide gerade oder beide ungerade sein.

## Beweis (Forts.):

Da

$$s > t > 0$$

$$n = s \cdot t$$

$$x = (s + t)/2$$

$$y = (s - t)/2$$

kann man für ungerades  $n$  stets  $s := n$  und  $t := 1$  setzen und erhält damit  $x = (n + 1)/2$  und  $y = (n - 1)/2$ , die die Behauptung erfüllen! □

## Bemerkungen:

- 1 Falls  $n$  eine ungerade Primzahl ist, sind  $s$  und  $t$  eindeutig bestimmt und es gibt genau eine Lösung für  $x$  und  $y$ .
- 2 Für allgemeine  $n$  kann es mehr als eine Lösung geben, z.B. für  $n = 15$

$$s = 5, t = 3 \text{ und } 15 = 16 - 1, \text{ oder}$$
$$s = 15, t = 1 \text{ und } 15 = 64 - 49.$$

- 3 Auch für gerade  $n$  kann es Lösungen geben, z.B.

$$8 = 9 - 1$$
$$48 = 7^2 - 1^2$$
$$48 = 8^2 - 4^2$$

## 4.7 Einige Sprechweisen

- ① Wir sagen  
„Eine Bedingung/Eigenschaft  $A$  ist **hinreichend** für eine Eigenschaft  $B$ “,  
falls

$$A \Rightarrow B.$$

- ② Wir sagen  
„Eine Bedingung/Eigenschaft  $A$  ist **notwendig** für eine Eigenschaft  $B$ “,  
falls

$$A \Leftarrow B \text{ (bzw. } B \Rightarrow A \text{ )}.$$

- ③ Wir sagen  
„Eine Bedingung/Eigenschaft  $A$  ist **notwendig und hinreichend** für eine Eigenschaft  $B$ “,  
falls

$$A \Leftrightarrow B \text{ (bzw. } A \equiv B \text{ )}.$$

## 4.8 Folgen und Grenzwerte

$R$  bezeichne einen Bereich wie z.B.  $\mathbb{R}$ ,  $\mathbb{Q}$ ,  $\mathbb{N}_0$ , oder  $\mathbb{Z}$ .

### Definition 33

- ① Sei  $k \in \mathbb{N}_0 \cup \{-1\}$ . Eine **endliche Folge** reeller (bzw. rationaler, natürlicher, ganzer) Zahlen

$$(a_i)_{0 \leq i \leq k}$$

ist eine Abbildung

$$\{0, 1, \dots, k\} \ni i \mapsto a_i \in R.$$

- ② Eine **unendliche Folge**

$$(a_n)_{n \geq 0}$$

ist eine Abbildung

$$\mathbb{N}_0 \ni n \mapsto a_n \in R.$$

Sei  $(a_n)_{n \geq 0}$  eine reelle Folge.

① Sei  $a \in \mathbb{R}$ . Wir sagen

„Die Folge  $(a_n)_{n \geq 0}$  konvergiert für  $n \rightarrow \infty$  nach  $a$ “,  
und schreiben

$$\lim_{n \rightarrow \infty} a_n = a,$$

falls gilt:

$$(\forall \epsilon > 0 \exists n_\epsilon \in \mathbb{N} \forall n \geq n_\epsilon)[|a_n - a| < \epsilon].$$

② Wir sagen

„Die Folge  $(a_n)_{n \geq 0}$  konvergiert für  $n \rightarrow \infty$  gegen  $+\infty$ “,  
und schreiben

$$\lim_{n \rightarrow \infty} a_n = +\infty,$$

falls gilt:

$$(\forall M \in \mathbb{N} \exists n_M \in \mathbb{N} \forall n \geq n_M)[a_n > M].$$

## Beispiel 34

Sei für  $n \in \mathbb{N}$   $a_n := \frac{1}{n} \sin n$ .

Behauptung:

Die Folge  $(a_n)_{n \in \mathbb{N}}$  konvergiert (für  $n \rightarrow \infty$ ) gegen 0.

Beweis:

Sei  $\epsilon > 0$ . Wähle  $N \in \mathbb{N}$ ,  $N > \epsilon^{-1}$ . Dann gilt für  $n \geq N$ :

$$|a_n - 0| = \frac{1}{n} |\sin n| \leq \frac{1}{n} \cdot 1 \leq \frac{1}{N} < \epsilon.$$



## Bemerkungen:

- 1 Falls es für eine Folge  $(a_n)_{n \in \mathbb{N}}$  kein  $a \in \mathbb{R}$  gibt, so dass

$$\lim_{n \rightarrow \infty} a_n = a,$$

so sagen wir, „die Folge  $(a_n)_{n \geq 0}$  **divergiert** für  $n \rightarrow \infty$ “.

- 2 Konvergenz gegen  $-\infty$  wird entsprechend definiert.
- 3 Für Funktionen  $f : \mathbb{N}_0 \rightarrow \mathbb{R}$  wird das Konvergenzverhalten (bzw.  $\lim_{n \rightarrow \infty} f(n)$ ) analog definiert (indem man die Folge  $(f(n))_{n \in \mathbb{N}_0}$  betrachtet!).

## 4.9 Das Wachstumsverhalten von Funktionen

Die **Groß-O-Notation** wurde von **D. E. Knuth** in der Algorithmenanalyse eingeführt. Sie wurde ursprünglich von **Paul Bachmann** (1837–1920) entwickelt und von **Edmund Landau** (1877–1938) in seinen Arbeiten verbreitet.

### Definition 35 (Groß-O-Notation)

- $f(n) \in \mathcal{O}(g(n))$  (für  $n \rightarrow \infty$ ) genau dann, wenn  $\exists c > 0$ ,  $n_0 \in \mathbb{N}$ , so dass

$$(\forall n \geq n_0) \quad [|f(n)| \leq c \cdot g(n)]$$

„ $f$  wächst bis auf einen konstanten Faktor nicht schneller als  $g$ “

- $f(n) \in o(g(n))$  (für  $n \rightarrow \infty$ ) genau dann, wenn  $\forall c > 0$   $\exists n_0 \in \mathbb{N}$ , so dass

$$(\forall n \geq n_0) \quad [|f(n)| < c \cdot g(n)]$$

„ $f$  wächst echt langsamer als  $g$ “

- $f(n) \in \Omega(g(n))$  (für  $n \rightarrow \infty$ ) genau dann, wenn  $\exists c > 0$ ,  $n_0 \in \mathbb{N}$ , so dass

$$(\forall n \geq n_0) [ |f(n)| \geq c \cdot g(n) \geq 0 ]$$

„ $f$  wächst bis auf einen konstanten Faktor nicht langsamer als  $g$ “

- $f(n) \in \omega(g(n))$  (für  $n \rightarrow \infty$ ) genau dann, wenn  $\forall c > 0$   $\exists n_0 \in \mathbb{N}$ , so dass

$$(\forall n \geq n_0) [ |f(n)| > c \cdot g(n) \geq 0 ]$$

„ $f$  wächst echt schneller als  $g$ “

- $f(n) \in \Theta(g(n))$  (für  $n \rightarrow \infty$ ) genau dann, wenn

$$f(n) \in \mathcal{O}(g(n)) \text{ und } f(n) \in \Omega(g(n))$$

„ $f$  wächst (bis auf konstante Faktoren) genauso schnell wie  $g$ “

- $f(n) \in \Omega_\infty(g(n))$  genau dann, wenn  $\exists c > 0$ , so dass für unendlich viele  $n \in \mathbb{N}$

$$|f(n)| \geq c \cdot g(n) \geq 0.$$

- $f(n) \in \omega_\infty(g(n))$  genau dann, wenn  $\forall c > 0 \exists$  unendlich viele  $n \in \mathbb{N}$  mit

$$|f(n)| > c \cdot g(n) \geq 0.$$

## Bemerkungen:

- 1 Man schreibt oft, aber **logisch unsauber**  $f(n) = \mathcal{O}(g(n))$ .
- 2 Oft werden nur Funktionen  $\mathbb{N}_0 \rightarrow \mathbb{N}_0$  betrachtet (oder  $\mathbb{N} \rightarrow \mathbb{N}_0$ ); dann sind die Absolutbeträge überflüssig.
- 3 Manchmal werden auch Funktionen  $\mathbb{R} \rightarrow \mathbb{R}$  oder das Verhalten für  $x \rightarrow a$  betrachtet.
- 4 **Achtung:** Die Notation für  $\Omega$  und  $\Omega_\infty$  ist in der Literatur nicht eindeutig; im Zweifelsfall muss auf die jeweilige Definition geachtet werden!

## Beispiel 36

Behauptung:  $n! \in O(n^n)$

Beweis:

$$(\forall n \in \mathbb{N}) [n! = n(n-1) \cdots 2 \cdot 1 \leq 1 \cdot n^n]$$



## Beispiel 37

Behauptung:  $\log n! \in O(n \log n)$

Beweis:

$$(\forall n \in \mathbb{N}) [\log n! = \log n + \log(n-1) + \dots + \log 1 < 1 \cdot n \cdot \log n]$$

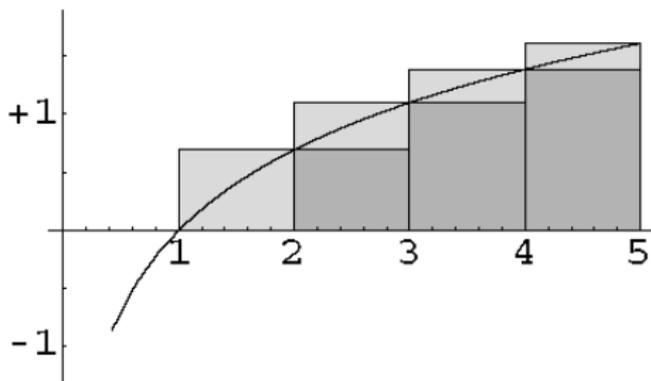


## Beispiel 38

Behauptung:  $n! = O\left((n+1) \cdot e \cdot \left(\frac{n}{e}\right)^n\right)$

Beweis:

$$(\forall n > 0) \left[ \sum_{k=1}^{n-1} \ln k < \int_1^n \ln x \, dx < \sum_{k=2}^n \ln k < \int_1^{n+1} \ln x \, dx \right]$$



Es ist

$$\int_1^n \ln x \, dx = (x \cdot \ln x - x) \Big|_1^n = n \cdot \ln n - n + 1$$

und

$$\int_1^{n+1} \ln x \, dx = (n+1) \cdot \ln(n+1) - n$$

Also:

$$(\forall n \in \mathbb{N}) \left[ n \cdot \ln n - n + 1 < \ln n! < (n+1) \cdot \ln(n+1) - n \right]$$

und damit

$$\frac{n^n}{e^{n-1}} \leq n! \leq \frac{(n+1)^{n+1}}{e^n}$$

oder:

$$e \cdot \left(\frac{n}{e}\right)^n \leq n! \leq (n+1) \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{n}\right)^n \leq (n+1) \cdot e \cdot \left(\frac{n}{e}\right)^n$$

□

# Die Stirling'sche Formel

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

oder mit anderen Worten:

$$n! = \sqrt{2\pi n} \cdot \left( \frac{n}{e} \right)^n \cdot (1 + o(1))$$

## Beispiel 39 (Polynome)

Sei

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0; \quad a_i \in \mathbb{R}, \quad a_n \neq 0.$$

Behauptung:  $f(x) = \mathcal{O}(x^n)$ .

Beweis:

$$\begin{aligned} \forall x \geq 1: \quad |f(x)| &\leq \left| \sum_{i=0}^n a_i \cdot x^i \right| \leq \sum_{i=0}^n |a_i| \cdot x^i \\ &\leq x^n \cdot \left( \sum_{i=0}^n |a_i| x^{i-n} \right) \leq x^n \cdot \underbrace{\sum_{i=0}^n |a_i|}_{=:c} \end{aligned}$$

□

# Kapitel II Algebraische Grundlagen

## 1. Algebren

### 1.1 Grundbegriffe

#### Definition 40

Eine **Algebra** besteht aus einer Trägermenge  $S$  und einer Menge  $\Phi$  von Operationen auf  $S$  (der Operatorenmenge). Dabei gilt: Jeder Operator ist eine (totale) Abbildung

$$S^m \rightarrow S$$

der Stelligkeit (Arität, **arity**)  $m \in \mathbb{N}_0$ .

- Nullstellige Operatoren sind **Konstanten**, z. B.  $0$ ,  $\perp$ .
- Einstellige Operatoren sind **unäre** Operatoren, z. B.  $x \mapsto 2^x$ ,  
 $x \mapsto \neg x$ ,  $A \mapsto 2^A$ .
- Zweistellige Operatoren sind **binäre** Operatoren, z. B.  
 $(x, y) \mapsto \max\{x, y\}$ ,  $(x, y) \mapsto \text{ggT}(x, y)$ ,  $(x, y) \mapsto x + y$ .
- Dreistellige Operatoren sind **ternäre** Operatoren, z. B.  
 $(x, y, z) \mapsto \mathbf{if\ } x \mathbf{\ then\ } y \mathbf{\ else\ } z \mathbf{\ fi}$

## Beispiel 41

Sei  $U$  eine Menge,  $F$  die Menge der Funktionen von  $U \rightarrow U$ .  
 $(F, \circ)$  ist eine Algebra mit  $\circ$  als **Komposition** von Funktionen.

## Beispiel 42

Boolesche Algebra:

$\langle \{t, f\}, \{t, f, \neg, \wedge, \vee\} \rangle$  ist eine (endliche) Algebra.

## 1.2 Eigenschaften

### Signatur einer Algebra

#### Definition 43

Die **Signatur** einer Algebra besteht aus der Liste der Stelligkeiten der Operatoren.

## Beispiel 44

$\langle \mathbb{B}, \{t, f, \neg, \wedge, \vee\} \rangle$  (Boolesche Algebra,  $\mathbb{B} = \{t, f\}$ ): 0, 0, 1, 2, 2

$$\neg : \mathbb{B} \rightarrow \mathbb{B}$$

$$\wedge : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$$

$$\vee : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$$

## Beispiel 45

$\langle 2^U, \{U, \emptyset, -, \cap, \cup\} \rangle$ : 0, 0, 1, 2, 2

$$- : 2^U \rightarrow 2^U$$

$$\cap : 2^U \times 2^U \rightarrow 2^U$$

$$\cup : 2^U \times 2^U \rightarrow 2^U$$

Diese beiden Algebren haben dieselbe Signatur; die Trägermenge ist unwesentlich, es kommt nur auf die Reihenfolge der Stelligkeiten an.

## Einselement, Nullelement, Inverses

Sei  $\langle S, \circ \rangle$  eine Algebra,  $\circ$  beliebiger zweistelliger Operator.

### Definition 46

- Ein Element  $1 \in S$  heißt **linkes** (bzw. **rechtes**) **Einselement** für den Operator  $\circ$ , falls

$$(\forall a \in S) \quad 1 \circ a = a \quad (\text{bzw. } a \circ 1 = a)$$

$1$  heißt **Einselement**, falls es linkes und rechtes Einselement ist.

- Ein Element  $0 \in S$  heißt **linkes** (bzw. **rechtes**) **Nullelement** für den Operator  $\circ$ , falls

$$(\forall a \in S) \quad 0 \circ a = 0 \quad (\text{bzw. } a \circ 0 = 0)$$

$0$  heißt **Nullelement**, falls es linkes und rechtes Nullelement ist.

- Sei  $1$  Einselement. Für  $a \in S$  heißt  $a^{-1} \in S$  **Rechtsinverses** von  $a$ , falls

$$a \circ a^{-1} = 1$$

Analog: **Links inverses**

## Beispiel 47

Betrachte  $F(U)$ , d. h. die Menge aller Abbildungen  $U \rightarrow U$ . Dann gilt (mit der Komposition als Operator):

- $f \in F(U)$  hat genau dann ein **Rechtsinverses**, wenn  $f$  **surjektiv** ist.

$$f \circ f^{-1} = id$$

(Wähle für  $f^{-1}$  irgendeine Funktion  $g$ , so dass gilt:  $g(x)$  wird von  $f$  auf  $x$  abgebildet.)

- $f \in F(U)$  hat genau dann ein **Linksinverses**, wenn  $f$  **injektiv** ist.

$$f^{-1} \circ f = id$$

(Wähle für  $f^{-1}$  irgendeine Funktion  $g$ , so dass gilt:  $f(x)$  wird von  $g$  auf  $x$  abgebildet.)

Ist  $f$  bijektiv, dann stimmen die beiden  $f^{-1}$  aus (1) und (2) überein.

## Satz 48

Falls  $c$  linkes Einselement ist und  $d$  rechtes Einselement (bezüglich des binären Operator  $\circ$ ), dann ist

$$c = d .$$

Beweis:

$$d = c \circ d = c .$$



## Satz 49

*Falls  $c$  linkes Nullelement und  $d$  rechtes Nullelement (bezüglich  $\circ$ ) ist, dann ist*

$$c = d .$$

Beweis:

$$c = c \circ d = d .$$



## Beispiel 50

Betrachte  $\langle \{b, c\}, \{\bullet\} \rangle$  mit

$\bullet$		$b$	$c$
$b$		$b$	$b$
$c$		$c$	$c$

Es gilt:  $b$  und  $c$  sind linke Nullelemente, und  $b$  und  $c$  sind rechte Einselemente.

# Abgeschlossenheit

## Definition 51

Sei  $\langle S, \Phi \rangle$  eine Algebra,  $T$  eine Teilmenge von  $S$ .

- $T$  ist unter den Operatoren in  $\Phi$  **abgeschlossen (stabil)**, falls ihre Anwendung auf Elemente aus  $T$  wieder Elemente aus  $T$  ergibt.
- $\langle T, \Phi \rangle$  heißt **Unteralgebra** von  $\langle S, \Phi \rangle$ , falls  $T \neq \emptyset$  und  $T$  unter den Operatoren  $\in \Phi$  abgeschlossen ist.

## Beispiel 52

- $\langle \mathbb{N}_0, + \rangle$  ist **Unteralgebra** von  $\langle \mathbb{Z}, + \rangle$
- $\langle \{0, 1\}, \cdot \rangle$  ist **Unteralgebra** von  $\langle \mathbb{N}_0, \cdot \rangle$
- $\langle \{0, 1\}, + \rangle$  ist **keine Unteralgebra** von  $\langle \mathbb{Z}, + \rangle$ , da sie nicht abgeschlossen ist ( $1 + 1 = 2$ ).

## 2. Morphismen

Seien  $A = \langle S, \Phi \rangle$  und  $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$  zwei Algebren mit derselben Signatur.

### 2.1 Isomorphismus

#### Definition 53

Eine Abbildung

$$h : S \rightarrow \tilde{S}$$

heißt ein **Isomorphismus** von  $A$  nach  $\tilde{A}$ , falls

- $h$  bijektiv ist und
- $h$  mit den in  $\Phi$  und  $\tilde{\Phi}$  einander entsprechenden Operatoren vertauschbar ist (**kommutatives Diagramm**):

$$\begin{array}{ccc} S^m & \xrightarrow{\circ} & S \\ (h, \dots, h) \downarrow & & \downarrow h \\ \tilde{S}^m & \xrightarrow{\tilde{\circ}} & \tilde{S} \end{array}$$

$h$  ist also ein Isomorphismus gdw

- $h(c) = \tilde{c}$  für alle nullstelligen Operatoren (Konstanten)  $c$
- $h(u(x)) = \tilde{u}(h(x))$  für alle unären Operatoren  $u \in \Phi$ ,  $\forall x \in S$
- $h(b(x, y)) = \tilde{b}(h(x), h(y))$  für alle binären Operatoren  $b \in \Phi$ ,  $\forall x, y \in S$

Notation:  $A \cong \tilde{A}$ : „ $A$  isomorph zu  $\tilde{A}$ “, d. h. es existiert ein Isomorphismus von  $A$  nach  $\tilde{A}$  (und von  $\tilde{A}$  nach  $A$ ).

Ein Isomorphismus von  $A$  nach  $A$  heißt **Automorphismus**.

Zur Vereinfachung der Notation schreiben wir statt  $\langle S, \{o_1, \dots, o_k\} \rangle$  auch

$$\langle S, o_1, \dots, o_k \rangle ,$$

solange keine Verwechslung zu befürchten ist.

## Beispiel 54

$\langle \mathbb{N}_0, + \rangle$  und  $\langle 2 \cdot \mathbb{N}_0, + \rangle$  ( $2 \cdot \mathbb{N}_0$ : gerade Zahlen) mit

$$h : \mathbb{N}_0 \ni n \mapsto 2 \cdot n \in 2\mathbb{N}_0$$

ist ein Isomorphismus zwischen den beiden Algebren.

## Beispiel 55

$\langle \mathbb{R}^+, \cdot \rangle$  und  $\langle \mathbb{R}, + \rangle$  ( $\mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}$ )

$$h : \mathbb{R}^+ \ni x \mapsto \log x \in \mathbb{R}$$

ist ein Isomorphismus (der sog. **Rechenschieberisomorphismus**)

## Satz 56

*Ein Algebra-Isomorphismus bildet Einselemente auf Einselemente, Nullelemente auf Nullelemente und Inverse auf Inverse ab.*

### Beweis:

Sei die Abbildung  $h : S \rightarrow \tilde{S}$  ein Isomorphismus von  $A = \langle S, \Phi \rangle$  nach  $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$ .

Sei  $1$  ein rechtes Einselement für den Operator  $\circ \in \Phi$  in  $A$ . Dann gilt für alle  $\tilde{b} \in \tilde{S}$ :

$$\tilde{b} \circ h(1) = h(b) \circ h(1) = h(b \circ 1) = h(b) = \tilde{b}$$

Also ist  $h(1)$  ein rechtes Einselement in  $\tilde{A}$ . Die Argumentation für linke Einselemente, Nullelemente und Inverse ist analog.  $\square$

## 2.2 Homomorphismus

### Definition 57

Eine Abbildung

$$h: S \rightarrow \tilde{S}$$

heißt ein **Homomorphismus** von  $A$  nach  $\tilde{A}$ , falls  $h$  mit den in  $\Phi$  und  $\tilde{\Phi}$  einander entsprechenden Operatoren vertauschbar ist.

## Beispiel 58

$\langle \mathbb{N}_0, + \rangle$  und  $\tilde{A} = \langle \mathbb{Z}_m, +_{(m)} \rangle$  mit  $+_{(m)}$  als Addition modulo  $m$ .

$$h: \mathbb{N}_0 \ni n \mapsto n \bmod m \in \mathbb{Z}_m$$

ist ein (surjektiver) Homomorphismus ( $\mathbb{Z}_m = \{0, 1, \dots, m - 1\}$ ).

## Beispiel 59

$\langle \Sigma^*, \circ \rangle$  und  $\langle \mathbb{N}_0, + \rangle$  mit  $\Sigma^*$  Menge der endlichen Zeichenreihen über dem Alphabet  $\Sigma$ .

$$h: \Sigma^* \ni \sigma \mapsto |\sigma| \in \mathbb{N}_0$$

mit  $|\sigma|$  der Länge der Zeichenreihe ist ein Homomorphismus.

## Satz 60

Sei  $h$  ein Homomorphismus von  $A = \langle S, \Phi \rangle$  nach  $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$ .  
Dann ist  $\langle h(S), \tilde{\Phi} \rangle$  eine Unteralgebra von  $\tilde{A}$ .

Beweis:

Offensichtlich. □

### 3. Halbgruppen

#### Definition 61

Eine **Halbgruppe** ist eine Algebra  $\langle S, \circ \rangle$  mit einem assoziativen binären Operator  $\circ$ , d. h. für alle  $a, b, c \in S$  gilt:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

#### Beispiel 62

$\langle \Sigma^*, \circ \rangle$ : Menge der endlichen Zeichenreihen über dem Alphabet  $\Sigma$ , mit Konkatination als  $\circ$ .

#### Beispiel 63

$S \subseteq \mathbb{R}$ ,  $\langle S, \max \rangle$ : Da die Maximumbildung assoziativ ist, ist  $\langle S, \max \rangle$  eine Halbgruppe.

## Beispiel 64

$\langle \{b, c\}, \circ \rangle$  mit

$\circ$	$b$	$c$
$b$	$b$	$b$
$c$	$c$	$c$

Auch diese Operation ist assoziativ.

Beweis:

$$c = c \circ (c \circ c) = (c \circ c) \circ c = c$$

$$b = b \circ (c \circ c) = (b \circ c) \circ c = b$$

$$c = c \circ (b \circ c) = (c \circ b) \circ c = c$$

$$c = c \circ (c \circ b) = (c \circ c) \circ b = c$$

$$b = b \circ (b \circ b) = (b \circ b) \circ b = b$$

$$c = c \circ (b \circ b) = (c \circ b) \circ b = c$$

$$b = b \circ (c \circ b) = (b \circ c) \circ b = b$$

$$b = b \circ (b \circ c) = (b \circ b) \circ c = b$$



## 3.1 Unterhalbgruppen

### Definition 65

Sei  $\langle S, \circ \rangle$  eine Halbgruppe,  $\emptyset \neq T \subseteq S$ .  $\langle T, \circ \rangle$  heißt **Unterhalbgruppe**, falls es eine Unteralgebra ist.

## 3.2 Abelsche Halbgruppen

### Definition 66

Eine Halbgruppe  $\langle S, \circ \rangle$  heißt **abelsch**, falls  $\circ$  symmetrisch (kommutativ) ist. Also

$$a \circ b = b \circ a \quad \forall a, b \in S$$

## 4. Monoide

### Definition 67

Ein **Monoid**  $\langle S, \circ, 1 \rangle$  ist eine Halbgruppe  $\langle S, \circ \rangle$  mit (linkem und rechtem) Einselement 1. Eine Algebra  $\langle T, \circ \rangle$ ,  $T \subseteq S$  heißt **Untermonoid** von  $\langle S, \circ, 1 \rangle$ , wenn  $\langle T, \circ \rangle$  eine Halbgruppe mit Einselement ist.

### Beispiel 68

$\langle \mathbb{N}_0, \max \rangle$  ist ein Monoid mit 0 als Einselement, ein Untermonoid davon ist  $\langle \{0, 1\}, \max \rangle$ .

### Beispiel 69

$\langle \Sigma^*, \circ \rangle$ , mit  $\circ$  Konkatenation von Zeichenreihen und der leeren Zeichenreihe  $\varepsilon$  als Einselement ist ein Monoid.

## 5. Gruppen

### 5.1 Grundlagen

#### Definition 70

Eine **Gruppe** ist eine Algebra  $\langle S, \circ, 1 \rangle$  mit folgenden Eigenschaften:

- Der Operator  $\circ$  ist assoziativ.
- 1 ist Einselement  $\in S$ .
- Für jedes  $b \in S$  existiert  $b^{-1} \in S$  mit

$$b \circ b^{-1} = 1 = b^{-1} \circ b$$

*(Existenz des Inversen).*

## Beispiel 71

$\langle \mathbb{Z}_n, +_{(n)}, 0 \rangle$  ist **nicht** Untergruppe von  $\langle \mathbb{Z}, +, 0 \rangle$ , da  $+_{(n)}$  nicht die Restriktion (Einschränkung) von  $+$  auf  $\mathbb{Z}_n$  ist. Beide sind aber Gruppen.

## Beispiel 72

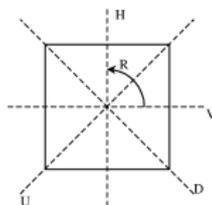
$\langle \mathbb{R}, \cdot, 1 \rangle$  oder  $\langle \mathbb{Q}, \cdot, 1 \rangle$  sind keine Gruppen! Zu dem Element  $0 \in \mathbb{Q}$  gibt es kein inverses Element.

$\langle \mathbb{R} \setminus \{0\}, \cdot, 1 \rangle$  bzw.  $\langle \mathbb{Q} \setminus \{0\}, \cdot, 1 \rangle$  sind Gruppen.

## Beispiel 73

Automorphismengruppe des Quadrats

○ ist die **Komposition** von Abbildungen

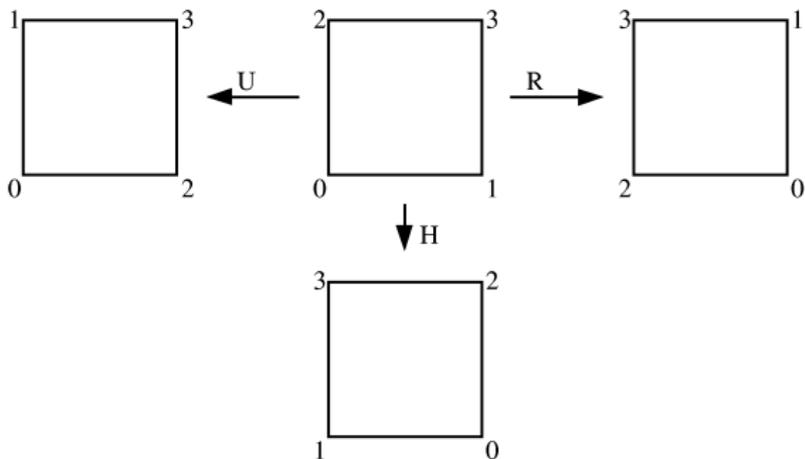


$I$  identische Abbildung,

$R$  Rotation um  $90^\circ$  gegen den Uhrzeigersinn

$H$  horizontale Spiegelung,  $V$  vertikale Spiegelung,

$D$  Spiegelung an der fallenden Diagonale,  $U$  Spiegelung an der steigenden.



Die Abbildungen  $I, R, R^2, R^3, H, V, D, U$  bilden die Automorphismengruppe des Quadrats.

## Verknüpfungstafel:

$\circ$	$I$	$R$	$R^2$	$R^3$	$H$	$V$	$D$	$U$
$I$	$I$	$R$	$R^2$	$R^3$	$H$	$V$	$D$	$U$
$R$	$R$	$R^2$	$R^3$	$I$	$D$	$U$	$V$	$H$
$R^2$	$R^2$	$R^3$	$I$	$R$	$V$	$H$	$U$	$D$
$R^3$	$R^3$	$I$	$R$	$R^2$	$U$	$D$	$H$	$V$
$H$	$H$	$U$	$V$	$D$	$I$	$R^2$	$R^3$	$R$
$V$	$V$	$D$	$H$	$U$	$R^2$	$I$	$R$	$R^3$
$D$	$D$	$H$	$U$	$V$	$R$	$R^3$	$I$	$R^2$
$U$	$U$	$V$	$D$	$H$	$R^3$	$R$	$R^2$	$I$

## Satz 74

Sei  $\langle S, \circ, 1 \rangle$  eine Gruppe. Dann gilt:

- für alle  $a \in S$ :  $a = (a^{-1})^{-1}$  (*Involutionsgesetz*)
- für alle  $a, a', b \in S$  (*Kürzungsregel*):

$$a \circ b = a' \circ b \Rightarrow a = a'$$

$$b \circ a = b \circ a' \Rightarrow a = a'$$

- für alle  $a, x, b \in S$  (*eindeutige Lösbarkeit linearer Gleichungen*):

$$a \circ x = b \iff x = a^{-1} \circ b$$

$$x \circ a = b \iff x = b \circ a^{-1}$$

- für alle  $a, b, c \in S$  (*Injektivität der Operation  $\circ$* ):

$$a \neq b \iff a \circ c \neq b \circ c \iff c \circ a \neq c \circ b$$

- für alle  $a, b \in S$  (*Surjektivität der Operation  $\circ$* ):

$$(\exists x)(a \circ x = b) \text{ und } (\exists y)(y \circ a = b)$$

## Beweis:

Wir beweisen lediglich:  $a \circ c = b \circ c \iff a = b$ . Rest: Übung

$\Leftarrow$ : Dass

$$a = b \Rightarrow a \circ c = b \circ c$$

gilt, ist offensichtlich.

$\Rightarrow$ : Sei  $a \circ c = b \circ c$ .

$$\begin{aligned} b &= b \circ (c \circ c^{-1}) = (b \circ c) \circ c^{-1} \stackrel{\text{n.V.}}{=} (a \circ c) \circ c^{-1} \\ &= a \circ (c \circ c^{-1}) = a \end{aligned}$$

□

## 5.2 Potenzen

### Definition 75

Sei  $\langle S, \circ, 1 \rangle$  eine Gruppe,  $a \in S$ . Man definiert:

- 1  $a^0 := 1$
- 2  $a^n := a \circ a^{n-1} = a^{n-1} \circ a \quad \forall n \geq 1$
- 3  $a^{-n} := (a^{-1})^n$

### Satz 76

Sei  $\langle S, \circ, 1 \rangle$  eine Gruppe. Dann gilt für alle  $m, n \in \mathbb{Z}$ ,  $a \in S$ :

- 1  $a^m \circ a^n = a^{m+n}$
- 2  $(a^n)^m = a^{m \cdot n}$
- 3  $a^m = a^n \iff a^{m-n} = 1$

Beweis:

Übung!



## 5.3 Ordnung eines Gruppenelements

### Definition 77

Sei  $G = \langle S, \circ, 1 \rangle$  eine Gruppe mit dem Einselement 1. Sei  $a \in G$  (genauer:  $a \in S$ ) ein Gruppenelement,  $a \neq 1$ . Dann ist die **Ordnung**  $\text{ord}(a)$  von  $a$  das minimale  $r \in \mathbb{N}$ , so dass

$$a^r = 1.$$

Falls kein solches  $r$  existiert, dann ist  $\text{ord}(a) := \infty$ . Falls gewünscht, kann man auch  $\text{ord}(1) := 1$  definieren.

### Beispiel 78

$\langle \mathbb{Z}, +, 0 \rangle$ :  $\text{ord}(1) = \infty$ .

## Satz 79

Sei  $G$  eine endliche Gruppe; dann hat auch jedes Element in  $G$  endliche Ordnung.

### Beweis:

Betrachte die Abbildung

$$\mathbb{N}_0 \ni i \mapsto a^i \quad a \in G \text{ beliebig } \neq 1$$

Also gibt es (**pigeon hole principle**) minimale  $k$  und  $j$ ,  
 $0 \leq j \leq k - 1$ , so dass

$$a^j = a^k.$$

Daraus folgt:

$$a^{k-j} = a^0 = 1.$$

Da  $k$  minimal gewählt wurde, folgt  $j = 0$  und  $\text{ord}(a) = k$ . □

## Beispiel 80

Betrachte  $\langle \mathbb{Z}_{12}, +_{12}, 0 \rangle$ :

$a$	0	1	2	3	4	5	6	7	8	9	10	11
$\text{ord}(a)$	-	12	6	4	3	12	2	12	3	4	6	12

## 5.4 Untergruppen

### Definition 81

Eine Unteralgebra  $\langle T, \circ, 1 \rangle$  einer Gruppe  $G = \langle S, \circ, 1 \rangle$  heißt **Untergruppe** von  $G$ , falls  $\langle T, \circ, 1 \rangle$  eine Gruppe ist.

**Bemerkung:** Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

### Beispiel 82

$\langle \mathbb{N}_0, +, 0 \rangle$  ist Unteralgebra von  $\langle \mathbb{Z}, +, 0 \rangle$ , aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

### Satz 83

*Eine Unteralgebra (bzgl.  $\circ$ ) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung  $^{-1}$  abgeschlossen ist.*

### Beweis:

Folgt sofort aus der Definition. □

## Satz 84

Jede Unteralgebra (bzgl.  $\circ$ ) einer *endlichen* Gruppe ist eine Untergruppe.

### Beweis:

Sei  $\langle T, \circ, 1 \rangle$  eine Unteralgebra einer endlichen Gruppe  $\langle S, \circ, 1 \rangle$ . Sei  $b \in T$ ,  $b \neq 1$ . Dann gilt:

$$\text{ord}(b) \in \mathbb{N} \setminus \{1\}$$

Sei  $m := \text{ord}(b)$ . Dann gilt:

$$1 = b^m = b^{m-1} \circ b = b \circ b^{m-1}$$

d. h.  $b^{m-1} \in T$  ist das Inverse zu  $b$ . □

## Satz 85

- Sei  $G = \langle S, \circ, 1 \rangle$ ,  $b \in G$  und sei

$$S_b := \{b^m; m \in \mathbb{Z}\} \subseteq S$$

die von  $b$  erzeugte Untergruppe von  $G$ .  $S_b$  ist die kleinste Untergruppe, die  $b$  enthält.

- Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).
- Seien  $G_1 = \langle S_1, \circ, 1 \rangle$  und  $G_2 = \langle S_2, \circ, 1 \rangle$  Untergruppen von  $G = \langle S, \circ, 1 \rangle$ . Dann ist auch

$$G_1 \cap G_2 = \langle S_1 \cap S_2, \circ, 1 \rangle$$

eine Untergruppe von  $G$ .

Beweis:

Trivial, lediglich zur letzten Behauptung:

$$a \in S_1 \cap S_2 \Rightarrow a^{-1} \in S_1 \wedge a^{-1} \in S_2 \Rightarrow a^{-1} \in S_1 \cap S_2.$$



## 5.5 Nebenklassen und Normalteiler

### Definition 86

Sei  $H = \langle T, \circ, 1 \rangle$  eine Untergruppe von  $G = \langle S, \circ, 1 \rangle$  und sei  $b \in G$ . Dann heißt

$$T \circ b := \{c \circ b; c \in T\} =: H \circ b$$

eine **rechte Nebenklasse** von  $H$  in  $G$  und

$$b \circ T := \{b \circ c; c \in T\} =: b \circ H$$

eine **linke Nebenklasse** von  $H$  in  $G$  (**engl.: coset**).

Die Anzahl verschiedener Nebenklassen von  $H$  in  $G$  heißt der **Index** von  $H$  in  $G$ :

$$\text{ind}(H) = \text{ind}_G(H).$$

$H$  heißt **Normalteiler** von  $G$ , falls

$$H \circ b = b \circ H \quad \forall b \in G$$

d. h.  $H$  ist Normalteiler genau dann, wenn  $\forall b \in G : H = b \circ H \circ b^{-1}$   
(„konjugiert“).

## Beispiel 87

Betrachte  $\langle \mathbb{Z}_{12}^*, \cdot_{12}, 1 \rangle = \langle \{1, 5, 7, 11\}, \cdot_{12}, 1 \rangle$ . Dann gilt: Die Untergruppe  $\langle \{1, 5\}, \cdot_{12}, 1 \rangle$  ist Normalteiler (folgt aus Definition).

## Satz 88

Sei  $H$  Untergruppe von  $G$ ,  $b \in G$ . Dann ist die Kardinalität von  $H \circ b$  gleich der Kardinalität von  $H$  (ebenso für  $b \circ H$ ).

## Beweis:

Folgt aus der Kürzungsregel: Betrachte die Abbildung

$$H \ni h \mapsto h \circ b \in H \circ b.$$

Diese Abbildung ist surjektiv und injektiv (Kürzungsregel!):

$$h_1 \circ b = h_2 \circ b \Rightarrow h_1 = h_2$$



## Satz 89

Sei  $H$  Untergruppe von  $G$ . Dann bildet die Menge der rechten (linken) Nebenklassen von  $H$  eine *Partition* (Zerlegung einer Menge in disjunkte Teilmengen) von  $G$ .

### Beweis:

Klar ist, dass

$$G \subseteq \bigcup_{b \in G} H \circ b$$

Seien  $b, c \in G$  mit  $H \circ b \cap H \circ c \neq \emptyset$ , etwa  $h_1 \circ b = h_2 \circ c$ . Dann ist

$$H \circ c = H \circ h_2^{-1} \circ h_1 \circ b = H \circ b$$



# Eigenschaften von Nebenklassen:

$H$  sei Untergruppe von  $G$ ,  $b, c \in G$ .

- Zwei Nebenklassen  $H \circ b$  und  $H \circ c$  sind entweder identisch oder disjunkt.
- Für alle  $b \in G$  gilt  $|H \circ b| = |H|$ .

## Satz 90 (Lagrange)

Sei  $G$  eine endliche Gruppe und  $H$  eine Untergruppe in  $G$ . Dann

- 1 haben alle Nebenklassen von  $H$  in  $G$  gleich viele Elemente;
- 2 ist  $|G| = \text{ind}_G(H) \cdot |H|$ ;
- 3 teilt  $|H|$  die Kardinalität  $|G|$  von  $G$  ganzzahlig.

Beweis:

- 1 siehe oben;
- 2 folgt aus Satz 89;
- 3 folgt aus 2.



Mehr zu [Joseph-Louis Lagrange!](#)

## 5.6 Satz von Fermat

### Satz 91

Sei  $b \in \mathbb{N}_0$  und  $p \in \mathbb{N}$  eine Primzahl. Dann gilt:

$$b^p \equiv b \pmod{p}, \text{ (falls } b \not\equiv 0 \pmod{p} : b^{p-1} \equiv 1 \pmod{p})$$

(gemeint ist: die Gleichung  $b^p = b$  gilt modulo  $p$ )

## Beweis:

$$\mathbb{Z}_p^* := \{n \in \{1, \dots, p-1\}; \text{ggT}(n, p) = 1\}$$

1. Fall:  $b = 0$ :  $0^p = 0 \bmod p$

2. Fall:  $1 \leq b < p$ : Betrachte  $S_b = \langle \{b^0, b^1, \dots, b^{\text{ord}(b)-1}\}, \cdot \rangle$ .

$S_b$  ist Untergruppe von  $\mathbb{Z}_p^*$ .

Lagrange:  $(\text{ord}(b) =) |S_b| \mid |\mathbb{Z}_p^*| (= p-1)$

$$\Rightarrow (\exists q \in \mathbb{N})[q \cdot \text{ord}(b)] = p-1$$

Da  $b^{\text{ord}(b)} = 1$  (Einselement) ist, gilt:

$$b^p = b^{p-1} \cdot b = b^{q \cdot \text{ord}(b)} \cdot b = 1^q \cdot b = b \bmod p$$

3. Fall:  $b \geq p$ : Dann gilt:

$$(\exists q, r \in \mathbb{N}_0, 0 \leq r < p)[b = q \cdot p + r].$$

Damit:

$$b^p = (q \cdot p + r)^p \stackrel{(*)}{=} r^p \bmod p \stackrel{(**)}{=} r \bmod p = b \bmod p$$

(\*) Binomialentwicklung, die ersten  $p$  Summanden fallen weg, da jeweils  $= 0 \bmod p$ ;

(\*\*) Fall 1 bzw. 2



# Die umgekehrte Richtung

## Satz 92

Sei  $n \in \mathbb{N}$ ,  $n \geq 2$ . Dann gilt:

$$b^{n-1} \equiv 1 \pmod{n} \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \implies n \text{ ist prim.}$$

## Beweis:

[durch Widerspruch] **Annahme:**  $r|n$  für ein  $r \in \mathbb{N}$ ,  $r > 1$ . Dann

$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \stackrel{\text{n.V.}}{\equiv} 0 \pmod{n},$$

also

$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n.$$

Daraus folgt aber, dass  $r|1$ ,  $n$  also keinen nichttrivialen Teiler besitzen kann. □

# Pierre de Fermat (1601–1665)



## Definition 93 (Eulersche phi-Funktion)

Sei  $n \in \mathbb{N}$ ,  $n > 1$ . Dann bezeichnet

$$\varphi(n) := |\mathbb{Z}_n^*|$$

die Anzahl der zu  $n$  teilerfremden Reste.

## Satz 94

Sei  $n \in \mathbb{N}$ ,  $n > 1$ . Dann gilt in der Gruppe  $\langle \mathbb{Z}_n^*, \times_n, 1 \rangle$ :

$$b^{\varphi(n)} = 1 \text{ für alle } b \in \mathbb{Z}_n^* .$$

## Beweis:

Folgt sofort aus dem Satz von Lagrange (Satz 90)! □

# Leonhard Euler (1707–1783)



# Leonhard Euler (1707–1783)



## 5.7 Zyklische Gruppen

### Definition 95

Eine Gruppe  $G = \langle S, \circ, 1 \rangle$  heißt **zyklisch**, wenn es ein  $b \in G$  gibt, so dass

$$G = S_b$$

wobei  $S_b = \langle \{b^i | i \in \mathbb{Z}\}, \circ, 1 \rangle$ .

### Satz 96

*Sei  $G$  eine zyklische Gruppe. Falls  $G$  unendlich ist, ist  $G$  zu  $\langle \mathbb{Z}, +, 0 \rangle$  isomorph; falls  $G$  endlich ist, dann ist  $G$  isomorph zu  $\langle \mathbb{Z}_m, +_m, 0 \rangle$  für ein  $m \in \mathbb{N}$ .*

## Beweis:

1. Fall: Sei  $G$  unendlich. Wir wissen:  $G = \{b^i | i \in \mathbb{Z}\}$  für ein geeignetes  $b \in G$ , nach Voraussetzung. Betrachte die Abbildung

$$h : \mathbb{Z} \ni i \mapsto b^i \in G$$

Behauptung:  $h$  ist bijektiv.

Nach Voraussetzung ist  $h$  surjektiv.

Die Injektivität beweisen wir mittels Widerspruch.

**Annahme:**  $(\exists i, j, i \neq j)[b^i = b^j]$

Daraus folgt:

$$b^{i-j} = 1$$

Daher ist  $G$  endlich, es gilt nämlich:

$$G \subseteq \{b^k; 0 \leq k < |i - j|\}$$

Dies ist ein Widerspruch zur Annahme,  $G$  sei unendlich!

## Beweis (Forts.):

### 2. Fall: $G$ endlich:

Wiederum ist die Abbildung  $h$  nach Voraussetzung surjektiv.

Nach dem Schubfachprinzip

$$(\exists i, j, i \neq j)[b^i = b^j] .$$

Nach der Kürzungsregel können wir  $j = 0$  wählen. Falls  $i > 0$  und  $i$  minimal gewählt wird, folgt sofort

$$G \text{ isomorph } \langle \mathbb{Z}_i, +_i, 0 \rangle .$$



## Satz 97

*Jede Untergruppe einer zyklischen Gruppe ist wieder zyklisch.*

## Beweis:

Sei  $G$  zyklisch,  $H \subseteq G$  Untergruppe von  $G$ .

1. Fall:  $|G| = \infty$ , also  $G \cong \langle \mathbb{Z}, +, 0 \rangle$  ( $\cong$  isomorph).

Sei  $H'$  die durch den Isomorphismus gegebene Untergruppe von  $\langle \mathbb{Z}, +, 0 \rangle$ , die  $H$  entspricht.

Zu zeigen ist:  $H'$  ist zyklisch.

Sei  $i := \min\{k \in H'; k > 0\}$ .

Die Behauptung ist:

$$H = S_i.$$

Es gilt sicher:

$$S_i \subseteq H'.$$

Falls ein  $k \in H' \setminus S_i$  existiert, folgt  $k \bmod i \in H'$ . Dies stellt einen Widerspruch zur Wahl von  $i$  dar. Also ist  $H' = S_i$ , damit ist gezeigt, dass  $H$  zyklisch ist.

2. Fall:  $|G| < \infty$ : Der Beweis läuft analog.



## 5.8 Transformationsgruppen

### Definition 98

Eine **Transformationsgruppe** ist eine Gruppe von bijektiven Abbildungen einer Menge  $U$  auf sich selbst mit der **Komposition**  $\circ$  als binärem Operator:

$$g \circ f : U \ni x \mapsto g(f(x)) \in U$$

### Satz 99 (Darstellungssatz für Gruppen)

*Jede Gruppe ist isomorph zu einer Transformationsgruppe.*

## Beweis:

Sei  $G = \langle S, \circ, 1 \rangle$ ,  $g \in G$ . Betrachte die Abbildung

$$\tilde{g} : S \ni a \mapsto g \circ a \in S$$

Aus der Kürzungsregel und der Existenz eines Inversen folgt, dass  $\tilde{g}$  eine bijektive Abbildung ist.

Wir betrachten nun  $\tilde{G} := \langle \tilde{S}, \circ, \tilde{1} \rangle$  mit  $\tilde{S} = \{\tilde{g}; g \in G\}$ . Die Abbildung

$$\tilde{\phantom{g}} : S \ni g \mapsto \tilde{g} \in \tilde{S}$$

ist ein Gruppenisomorphismus. Für  $h, g \in G$  gilt:

$$(\widetilde{h \circ g})(a) = (h \circ g) \circ a = h \circ (g \circ a) = h \circ \tilde{g}(a) = \tilde{h}(\tilde{g}(a)) = (\tilde{h} \circ \tilde{g})(a)$$

□

## 5.9 Permutationsgruppen

### Definition 100

Eine **Permutation** ist eine bijektive Abbildung einer endlichen Menge auf sich selbst; o. B. d. A. sei dies die Menge

$U := \{1, 2, \dots, n\}$ .

$S_n$  (**Symmetrische Gruppe** für  $n$  Elemente) bezeichnet die Menge aller Permutationen auf  $\{1, 2, \dots, n\}$ .

Sei nun  $\pi \in S_n$ . Es existiert folgende naive Darstellung:

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

Kürzer schreibt man auch

$$\pi = \left( \pi(1) \ \pi(2) \ \pi(3) \ \dots \ \pi(n-1) \ \pi(n) \right)$$

Sei  $a \in \{1, 2, 3, \dots, n\}$ . Betrachte die Folge

$$a = \pi^0(a), \pi^1(a), \pi^2(a), \pi^3(a), \dots$$

Aus dem Schubfachprinzip und der Kürzungsregel folgt, dass es ein minimales  $r = r(a)$  mit  $r \leq n$  gibt, so dass  $\pi^r(a) = a$ . Damit bildet

$$\left( a = \pi^0(a) \ \pi^1(a) \ \pi^2(a) \ \pi^3(a) \ \dots \ \pi^{r-1}(a) \right)$$

einen **Zyklus** der Permutation  $\pi \in S_n$ .

Umgekehrt liefert

$$(a \ \pi^1(a) \ \pi^2(a) \ \pi^3(a) \ \dots \ \pi^{r-1}(a))$$

eine zyklische Permutation der Zahlen

$$\{a, \pi^1(a), \pi^2(a), \pi^3(a), \dots, \pi^{r-1}(a)\} \subseteq \{1, 2, \dots, n\} .$$

## Satz 101

Sei  $\pi = (a_0 \ a_1 \ a_2 \ \dots \ a_{n-1})$  eine zyklische Permutation von  $\{1, 2, \dots, n\}$ , also

$$\pi: a_i \mapsto a_{(i+1) \bmod n}$$

Dann gilt:

- 1  $\pi^k(a_i) = a_{(i+k) \bmod n}$
- 2  $\pi$  hat die Ordnung  $n$ .

Beweis:

- 1 Leicht durch Induktion zu zeigen.
- 2 Aus 1. folgt:  $\pi^n = \pi^0 = id$ . Wäre  $\text{ord } \pi = m < n$ , dann hätte der Zyklus die Form  $(a_0 \ a_1 \ a_2 \ \dots \ a_{m-1})$  und  $a_m$  wäre gleich  $a_0$ , was einen Widerspruch zur Voraussetzung darstellt.

□

## Satz 102

*Jede Permutation aus  $S_n$  kann als Komposition (von endlich vielen) disjunkten Zyklen dargestellt werden.*

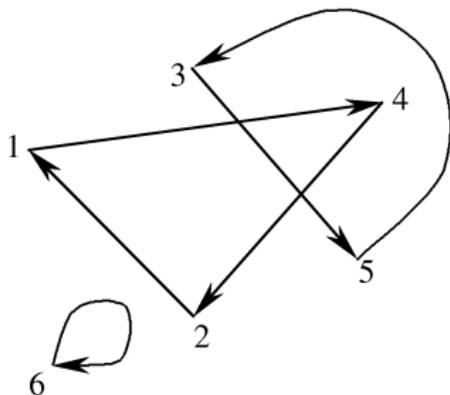
Beweis:

Übung!



## Beispiel 103

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



In diesem Beispiel ist (6) ein **Fixpunkt** und (3 5) eine **Transposition** (eine Permutation, die nur 2 Elemente vertauscht und alle anderen auf sich selbst abbildet).

**Bemerkung:**

Disjunkte Zyklen können vertauscht werden.

**Korollar 104**

*Die Ordnung einer Permutation  $\pi$  ist das kgV der Längen ihrer Zyklen.*

## 6. Boolesche Algebren

### 6.1 Definitionen

Eine **Boolesche Algebra** ist eine Algebra

$$\langle S, \oplus, \otimes, \sim, 0, 1 \rangle,$$

$\oplus, \otimes$  sind binäre,  $\sim$  ist ein unärer Operator, 0 und 1 sind Konstanten. Es gilt:

- 1  $\oplus$  und  $\otimes$  sind assoziativ und kommutativ.
- 2 0 ist Einselement für  $\oplus$ , 1 ist Einselement für  $\otimes$ .
- 3 für  $\sim$  gilt:

$$b \oplus \sim b = 1$$

$$b \otimes \sim b = 0 \quad \forall b \in S.$$

- 4 Distributivgesetz:

$$b \otimes (c \oplus d) = (b \otimes c) \oplus (b \otimes d)$$

$$b \oplus (c \otimes d) = (b \oplus c) \otimes (b \oplus d)$$

## Bemerkung:

Eine boolesche Algebra ist keine Gruppe, weder bezüglich  $\oplus$  ( $b \oplus \sim b = 1$ ) noch bezüglich  $\otimes$ .

## Beispiel 105

- $\langle \mathbb{B}, \vee, \wedge, \neg, F, T \rangle$
- $\langle 2^U, \cup, \cap, \bar{\phantom{x}}, \emptyset, U \rangle$
- $\langle \{1, 2, 3, 6\}, \text{kgV}, \text{ggT}, x \mapsto \frac{6}{x}, 1, 6 \rangle$

# George Boole (1815–1864)



George Boole

lived from 1815 to 1864

**Boole** approached logic in a new way reducing it to a simple algebra, incorporating logic into mathematics. He also worked on differential equations, the calculus of finite differences and general methods in probability.

## Satz 106 (Eigenschaften Boolescher Algebren)

① *Idempotenz:*

$$(\forall b \in S) \left[ b \oplus b = b \quad \wedge \quad b \otimes b = b \right]$$

② *Nullelement:*

$$(\forall b \in S) \left[ b \oplus 1 = 1 \quad \wedge \quad b \otimes 0 = 0 \right]$$

③ *Absorption:*

$$(\forall b, c \in S) \left[ b \oplus (b \otimes c) = b \quad \wedge \quad b \otimes (b \oplus c) = b \right]$$

④ *Kürzungsregel:*

$$(\forall b, c, d \in S) \left[ \begin{array}{l} (b \oplus c = b \oplus d) \wedge (\sim b \oplus c = \sim b \oplus d) \Leftrightarrow c = d \\ (b \otimes c = b \otimes d) \wedge (\sim b \otimes c = \sim b \otimes d) \Leftrightarrow c = d \end{array} \right]$$

## Satz 106 (Forts.)

5 *eindeutiges Komplement:*

$$(\forall b, c \in S) \left[ b \oplus c = 1 \wedge b \otimes c = 0 \iff c = \sim b \right]$$

6 *Involution:*

$$(\forall b \in S) \left[ \sim (\sim b) = b \right]$$

7 *Konstanten:*

$$\sim 0 = 1 \quad \sim 1 = 0$$

8 *De-Morgan-Regeln:*

$$(\forall b, c, d \in S) \left[ \begin{array}{l} \sim (b \oplus c) = \sim b \otimes \sim c \\ \sim (b \otimes c) = \sim b \oplus \sim c \end{array} \right]$$

Augustus de Morgan (1806–1871)

Wir zeigen zunächst die Teilbehauptung 7:

$$\sim 0 = 1 \quad \sim 1 = 0$$

**Beweis:**

Mit  $b = 0$  folgt aus den Eigenschaften 2 und 3 Boolescher Algebren sofort

$$\sim 0 = 1 ,$$

und ebenso mit  $b = 1$

$$\sim 1 = 0 ,$$

womit wir Behauptung 7 gezeigt haben. □

Folgende Hilfsbehauptung ist sehr nützlich:

$$1 = 1 \oplus (0 \otimes 1) = (1 \oplus 0) \otimes (1 \oplus 1) = 1 \otimes (1 \oplus 1) = 1 \oplus 1 .$$

Beweis:

[Es werden nur Teile des Satzes bewiesen.]

1

$$b \oplus b = (1 \otimes b) \oplus (1 \otimes b) = (1 \oplus 1) \otimes b = 1 \otimes b = b$$

2

$$b \oplus 1 = b \oplus (b \oplus (\sim b)) = (b \oplus b) \oplus (\sim b) = b \oplus (\sim b) = 1$$

3

$$b \oplus (b \otimes c) = (b \otimes 1) \oplus (b \otimes c) = b \otimes (1 \oplus c) = b \otimes 1 = b$$



## Beobachtung:

Die Eigenschaften treten in Paaren auf, die durch Vertauschen von  $\oplus$  und  $\otimes$  und von 0 und 1 ineinander übergehen. Solche Eigenschaften heißen **dual** zueinander.

Da die Axiome unter Dualität abgeschlossen sind, folgt:

Das Duale eines Satzes ist wieder ein Satz.

## Definition 107

Sei  $A = \langle S, \oplus, \otimes, \sim, 0, 1 \rangle$  eine endliche Boolesche Algebra. Dann definiert man:

$$a \leq b \iff a \otimes b = a$$

$$a < b \iff a \leq b \wedge a \neq b$$

## Satz 108

Durch  $\leq$  ist auf  $A$  eine partielle Ordnung definiert, d. h. eine reflexive, antisymmetrische und transitive Relation.

Beweis:

- (a) **Reflexivität:** Zu zeigen ist, dass für alle  $a \in S$  gilt  $a \leq a$ , d. h.  $a \otimes a = a$  (Idempotenzgesetz bzgl.  $\otimes$ )
- (b) **Antisymmetrie:** Sei  $a \leq b \wedge b \leq a$ . Damit gilt:  $a \otimes b = a$  und  $b \otimes a = b$  nach Definition. Damit:

$$a = a \otimes b = b \otimes a = b$$

- (c) **Transitivität:** Sei  $a \leq b \wedge b \leq c$ , dann gilt:  $a \otimes b = a$  und  $b \otimes c = b$ . Es ist zu zeigen, dass  $a \leq c$ , d.h.  $a \otimes c = a$ .

$$a \otimes c = (a \otimes b) \otimes c = a \otimes (b \otimes c) = a \otimes b = a$$



## 6.2 Atome

### Definition 109

Ein Element  $a \in S$ ,  $a \neq 0$  heißt ein **Atom**, i. Z.  $\text{atom}(a)$ , falls

$$(\forall b \in S \setminus \{0\}) [b \leq a \Rightarrow b = a].$$

### Satz 110

*Es gilt:*

- 1  $\text{atom}(a) \Rightarrow (\forall b \in S) [a \otimes b = a \vee a \otimes b = 0]$
- 2  $\text{atom}(a) \wedge \text{atom}(b) \wedge a \neq b \Rightarrow a \otimes b = 0$
- 3 *Falls gilt:*  $(\forall a \in S)[\text{atom}(a) \Rightarrow a \otimes b = 0]$ , *dann*  $b = 0$ .

## Beweis:

[Wir zeigen nur die erste Teilbehauptung]

- 1 Sei  $a$  ein Atom. Nach Voraussetzung gilt (mit  $a \otimes b$  statt  $b$ ):

$$a \otimes b \neq 0 \implies (a \otimes b \leq a \implies a \otimes b = a)$$

Da aber  $a \otimes b \leq a$  ist (Übungsaufgabe!), folgt

$$(a \otimes b = 0) \vee (a \otimes b = a).$$



## Satz 111 (Darstellungssatz)

Jedes Element  $x$  einer *endlichen* Booleschen Algebra  $\langle S, \oplus, \otimes, \sim, 0, 1 \rangle$  lässt sich in eindeutiger Weise als  $\oplus$ -Summe von *Atomen* schreiben:

$$x = \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a$$

## Beweis:

Es gilt:

$$x \otimes \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a \stackrel{\text{D-G.}}{=} \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} (x \otimes a) \stackrel{\text{Satz 110}}{=} \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a$$

Setze

$$y := \bigoplus_{\substack{a \in S \\ \text{atom}(a) \\ a \otimes x \neq 0}} a.$$

## Beweis (Forts.):

Wir haben gezeigt:

$$x \otimes y = y$$

Ebenso gilt:

$$x \otimes (\sim y) = 0 \quad (\text{Übungsaufgabe!})$$

Zusammen:

$$\begin{aligned} x &= x \otimes (y \oplus (\sim y)) \\ &\stackrel{\text{D-G.}}{=} (x \otimes y) \oplus (x \otimes (\sim y)) \\ &= y \oplus 0 = y \end{aligned}$$

## Beweis (Forts.):

Zur Eindeutigkeit: Sei (Widerspruchsannahme)

$$0 \neq x = \bigoplus_{a \in S_1} a = \bigoplus_{a \in S_2} a,$$

wobei  $S_1, S_2 \subseteq S$ ,  $S_1 \neq S_2$  zwei verschiedene Teilmengen von Atomen aus  $S$  sind.

O. B. d. A. gelte  $S_1 \cap S_2 = \emptyset$  — wenn nicht, dann bilde die Schnittmenge mit  $\overline{(S_1 \cap S_2)}$ .

## Beweis (Forts.):

Dann gilt:

$$\begin{aligned}x &= x \otimes x = \left( \bigoplus_{a \in S_1} a \right) \otimes \left( \bigoplus_{a \in S_2} a \right) \\ &= \bigoplus_{\substack{a \in S_1 \\ a' \in S_2}} \underbrace{a \otimes a'}_{=0} \\ &\stackrel{\text{Satz 110 (2)}}{=} \bigoplus_{\substack{a \in S_1 \\ a' \in S_2}} 0 = 0,\end{aligned}$$

was ein Widerspruch zur Annahme ist. □

## Korollar 112

Jede **endliche** Boolesche Algebra mit  $n$  Atomen enthält genau  $2^n$  Elemente.

## Korollar 113

Jede **endliche** Boolesche Algebra  $A = \langle S, \oplus, \otimes, \sim, 0, 1 \rangle$  mit  $n$  Atomen ist **isomorph** zur Potenzmengenalgebra

$$\mathcal{P}_n := \langle 2^{\{1, \dots, n\}}, \cap, \cup, \bar{\phantom{x}}, \emptyset, \{1, \dots, n\} \rangle$$

## Beweis:

Seien  $a_1, \dots, a_n$  die Atome von  $A$ . Definiere die Abbildung

$$h : S \ni \bigoplus_{i \in I} a_i \mapsto I \in 2^{\{1, \dots, n\}}$$

Diese Abbildung ist ein Isomorphismus (leicht nachzurechnen).  $\square$

# Kapitel III Ringe und Körper

## 1. Definitionen und Beispiele

### Definition 114

Eine Algebra  $A = \langle S, \oplus, \odot, 0, 1 \rangle$  mit zwei zweistelligen Operatoren  $\oplus$  und  $\odot$  heißt ein **Ring**, falls

- R1.  $\langle S, \oplus, 0 \rangle$  eine abelsche Gruppe mit neutralem Element  $0 \in S$  ist,
- R2.  $\langle S, \odot, 1 \rangle$  ein Monoid mit neutralem Element  $1 \in S$  ist und
- R3.  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$  für alle  $a, b, c \in S$ ,  
 $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$  für alle  $a, b, c \in S$ ,  
(man sagt:  $\oplus$  und  $\odot$  sind **distributiv**).

## Definition 115

Eine Algebra  $A = \langle S, \oplus, \odot, 0, 1 \rangle$  mit zwei zweistelligen Operatoren  $\oplus$  und  $\odot$  heißt **Körper** (engl. **field**), falls

- K1.  $\langle S, \oplus, 0 \rangle$  eine abelsche Gruppe mit neutralem Element  $0 \in S$  ist,
- K2.  $\langle S \setminus \{0\}, \odot, 1 \rangle$  eine abelsche Gruppe mit neutralem Element  $1 \in S$  ist und
- K3.  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$  für alle  $a, b, c \in S$ .

## Beispiele 116

- Die Algebra der ganzen Zahlen  $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$  ist ein **kommutativer** Ring.
- Für  $n \in \mathbb{N}$ ,  $n > 1$ , ist die Algebra der Restklassen bzgl. Division durch  $n$ , also  $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1 \rangle$  ein **kommutativer** Ring.
- Die Menge der  $n \times n$ -Matrizen ( $n \geq 1$ ) mit Einträgen aus  $\mathbb{Z}$  ist ein **im Allgemeinen nicht kommutativer** Ring.

## Beispiele 117

- $\mathbb{Q}$  (die Menge der rationalen Zahlen) ist ein Körper.
- Ebenso  $\mathbb{R}$  und  $\mathbb{C}$ .
- Die Restklassenalgebra  $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1 \rangle$  ist für alle  $n$ , die **prim** sind, ein Körper.

## 2. Eigenschaften von Körpern

### Satz 118

In jedem Körper  $K$  gilt:

$$a \cdot 0 = 0 \cdot a = 0 \quad \text{für alle } a \in K .$$

### Beweis:

Es sei  $a$  ein beliebiges Element aus  $K$ . Dann folgt aus den Axiomen:

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + a \cdot 0 - a \cdot 0 = a \cdot (0 + 0) - a \cdot 0 \\ &= a \cdot 0 - a \cdot 0 = 0 . \end{aligned}$$



**Bemerkung:** Satz 118 gilt sogar in Ringen.

## Definition 119

Sei  $R$  kommutativ. Ein  $a \in R$ ,  $a \neq 0$ , heißt **Nullteiler**, falls es ein  $b \in R$  gibt,  $b \neq 0$ , so dass  $ab = 0$ .

## Satz 120

In jedem Körper  $K$  gilt für alle  $a, b \in K$ :

$$ab = 0 \quad \implies \quad a = 0 \quad \text{oder} \quad b = 0.$$

(Man sagt: Körper sind *nullteilerfrei*.)

## Beweis:

Angenommen  $ab = 0$ . Falls  $a \neq 0$ , so existiert ein multiplikatives Inverses  $a^{-1}$  von  $a$ . Unter Verwendung von Satz 118 folgt damit:

$$b = 1 \cdot b = a^{-1}ab = a^{-1} \cdot 0 = 0.$$



## 2.1 Größter gemeinsamer Teiler (ggT)

### Definition 121

- Seien  $a, b \in \mathbb{N}$ . Dann heißt  $d \in \mathbb{N}$  der **größte gemeinsame Teiler** ( $\text{ggT}(a, b)$ ), falls gilt:
  - ①  $d|a$  und  $d|b$ ;
  - ② falls  $d' \in \mathbb{N}$ ,  $d'|a$  und  $d'|b$ , dann gilt  $d'|d$ .
- Sind  $a_1, \dots, a_n \in \mathbb{N}$ ,  $n \geq 3$ , dann definieren wir

$$\text{ggT}(a_1, \dots, a_n) := \text{ggT}(\text{ggT}(a_1, \dots, a_{n-1}), a_n).$$

## Satz 122

Seien  $a, b \in \mathbb{N}$ . Dann gibt es  $c, d \in \mathbb{Z}$ , so dass

$$c \cdot a + d \cdot b = \text{ggT}(a, b).$$

## Beweis:

Sei o.B.d.A.  $a > b$ . Der **Euklidische Algorithmus** (fortgesetzte ganzzahlige Division mit Rest) (**Euklid von Alexandria**, ca. 325–265 v. Chr.) liefert eine Folge

$$r_0 := a = q_2 \cdot b + r_2 \quad , \text{ mit } 0 < r_2 < b, q_2, r_2 \in \mathbb{N}_0$$

$$r_1 := b = q_3 \cdot r_2 + r_3 \quad , \text{ mit } 0 < r_3 < r_2, q_3, r_3 \in \mathbb{N}_0$$

$$r_2 = q_4 \cdot r_3 + r_4 \quad , \text{ mit } 0 < r_4 < r_3, q_4, r_4 \in \mathbb{N}_0$$

$\vdots$

$$r_{m-3} = q_{m-1} \cdot r_{m-2} + r_{m-1} \quad , \text{ mit } 0 < r_{m-1} < r_{m-2} \quad (*)$$

$$r_{m-2} = q_m \cdot r_{m-1} + r_m \quad , \text{ mit } 0 = r_m < r_{m-1}$$

Dann gilt  $r_{m-1} | a$  und  $r_{m-1} | b$  sowie  $\text{ggT}(a, b) | r_{m-1}$ .

Also  $r_{m-1} = \text{ggT}(a, b)$ .

Rückwärtiges iteratives Ersetzen von  $r_{m-2}, r_{m-3}, \dots$  in Gleichung (\*) entsprechend den vorhergehenden Gleichungen liefert die gewünschte Darstellung. □

## Satz 123

Bezeichnet man mit  $+_n$  und  $\cdot_n$  die Addition bzw. Multiplikation modulo  $n$ , so gilt:

$$\langle \mathbb{Z}_n, +_n, \cdot_n \rangle \text{ ist ein Körper} \iff n \text{ ist Primzahl.}$$

### Beweis:

Die Axiome **K1** und **K3** sind durch die Addition und Multiplikation modulo  $n$  offensichtlich erfüllt. Wir haben bereits gesehen, dass  $a$  modulo  $n$  genau dann ein multiplikatives Inverses hat, wenn  $a$  und  $n$  teilerfremd sind, also

$$\text{ggT}(a, n) = 1.$$

Falls  $n$  prim ist, gilt dies für alle  $a$ ,  $1 \leq a < n$ .

Umgekehrt kann  $\text{ggT}(a, n) = 1$  für alle  $a$ ,  $1 \leq a < n$  nur gelten, falls  $n$  prim ist. □

## 2.2 Multiplikative Gruppe endlicher Körper

### Satz 124

In jedem endlichen Körper  $K$  ist die multiplikative Gruppe  $K^* = K \setminus \{0\}$  zyklisch, d.h. es gibt ein Element  $g \in K^*$  mit  $K^* = \{1, g, g^2, \dots, g^{|K|-2}\}$ .

### Beweis:

Es gilt:  $\text{ord}(a) < \infty$  für alle  $a \in K^*$ . Sei  $a$  ein Element in  $K^*$  mit maximaler Ordnung:

$$\max\{\text{ord}(b) \mid b \in K^*\} = \text{ord}(a).$$

Es ist zu zeigen, dass  $\text{ord}(a) = |K| - 1$ . Dazu betrachten wir das Polynom  $x^{\text{ord}(a)} - 1$ , das Grad  $\text{ord}(a)$  hat.

Für jedes  $b \in K^*$  gilt, dass  $\text{ord}(b) \mid \text{ord}(a)$  (da sonst  $ab$  größere Ordnung als  $a$  hätte). Also ist jedes Element von  $K^*$  eine Nullstelle des obigen Polynoms. Da ein Polynom vom Grad  $k$  höchstens  $k$  verschiedene Nullstellen haben kann (warum?), folgt daraus  $\text{ord}(a) \geq |K^*| = |K| - 1$ . □

## 2.3 Primitive Elemente

### Definition 125

Sei  $K$  ein endlicher Körper. Ein Element  $a$ , das die multiplikative Gruppe  $K^* = K \setminus \{0\}$  erzeugt, nennt man **primitives Element**.

### Beispiel 126

In  $\mathbb{Z}_5^*$  sind sowohl 2 als auch 3 primitive Elemente:

$$\begin{array}{ll} 2^0 = 1 & 3^0 = 1 \\ 2^1 = 2 & 3^1 = 3 \\ 2^2 = 4 & 3^2 = 4 \\ 2^3 = 3 & 3^3 = 2 \\ (2^4 = 1 & 3^4 = 1) \end{array}$$

**Bemerkung:**  $\langle \mathbb{Z}_4, +_4, \cdot_4, 0, 1 \rangle$  ist **kein** Körper!

### Beispiel 127

Setzt man  $K = \{0, 1, a, b\}$  und definiert eine Addition und Multiplikation wie folgt:

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

so bildet  $\langle K, \oplus, \odot, 0, 1 \rangle$  einen Körper (Übung!).

## 3. Polynome

### 3.1 Definition und Grundlagen

#### Definition 128

Sei  $R$  ein (kommutativer) Ring. Ein **Polynom** über  $R$  in der Variablen  $x$  ist eine Funktion  $p$  der Form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

wobei  $n \in \mathbb{N}_0$ ,  $a_i \in R$  und  $a_n \neq 0$ .

$n$  heißt der **Grad** des Polynoms,  $a_0, \dots, a_n$  seine **Koeffizienten**.

$R[x]$  bezeichnet die Menge der Polynome über dem Ring  $R$  in der Variablen  $x$ .

## Bemerkungen:

- 1 Das Nullpolynom  $p(x) = 0$  hat Grad 0.
- 2 Formal kann das Polynom  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  auch mit der Folge  $(a_0, a_1, \dots, a_n)$  gleichgesetzt werden.

## Beispiel 129

- $p(x) = x^2 - 2x + 1$  ist ein Polynom vom Grad 2.
- Eine lineare Funktion  $f(x) = ax + b$  mit  $a \neq 0$  ist ein Polynom vom Grad 1.
- Konstante Funktionen  $f(x) = c$  sind Polynome vom Grad 0.

## 3.2 Rechnen mit Polynomen

### Berechnung des Funktionswertes

Um den Wert eines Polynoms an einer bestimmten Stelle  $x_0 \in R$  zu bestimmen, verwendet man besten das sogenannte **Hornerschema**:

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \\ &= ((\dots (((a_n x + a_{n-1})x + a_{n-2})x + \dots)x + a_1)x + a_0. \end{aligned}$$

Hat man die Koeffizienten in einem Array  $a[0..n]$  abgespeichert, kann man den Funktionswert  $p(x_0)$  daher wie folgt berechnen:

```
begin  
   $p \leftarrow a[n]$   
  for  $i = n-1$  downto  $0$  do  
     $p \leftarrow p \cdot x_0 + a[i]$   
  end  
  return( $p$ )  
end
```

### **Beobachtung:**

Für die Auswertung eines Polynoms vom Grad  $n$  genügen damit  $O(n)$  Multiplikationen und Additionen.

## Addition

Die Summe zweier Polynome  $a(x) = a_n x^n + \dots + a_1 x + a_0$  und  $b(x) = b_n x^n + \dots + b_1 x + b_0$  ist definiert durch

$$(a + b)(x) = c_n x^n + \dots + c_1 x + c_0, \quad \text{wobei } c_i = a_i + b_i .$$

## Bemerkungen:

- An sich fehlende Koeffizienten sind gleich 0 gesetzt.
- Für den Grad des Summenpolynoms gilt

$$\text{grad}(a + b) \leq \max\{\text{grad}(a), \text{grad}(b)\} .$$

## Beispiel 130

- 1 Für  $a(x) = x^2 - 3x + 5$  und  $b(x) = 4x + 2$  ergibt sich  
 $(a + b)(x) = x^2 + x + 7$ .  
Hier gilt  $\text{grad}(a + b) = 2 = \text{grad}(a)$ .
- 2 Für  $a(x) = x^3 + 1$  und  $b(x) = -x^3 + 1$  ergibt sich hingegen  
 $(a + b)(x) = 2$  und somit  
 $\text{grad}(a + b) = 0 < 3 = \max\{\text{grad}(a), \text{grad}(b)\}$ .

### Beobachtung:

Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad  $\leq n$  lässt sich in  $O(n)$  arithmetischen Schritten berechnen.

## Multiplikation

Das Produkt zweier Polynome  $a(x) = a_n x^n + \dots + a_1 x + a_0$  und  $b(x) = b_m x^m + \dots + b_1 x + b_0$  erhält man durch Ausmultiplizieren und anschließendes Sortieren und Zusammenfassen der Koeffizienten. Also

$$(a \cdot b)(x) = c_{n+m} x^{n+m} + \dots + c_1 x + c_0, \quad \text{wobei } c_i = \sum_{j=0}^i a_j b_{i-j}.$$

Für den Grad des Produktpolynoms gilt

$$\text{grad}(a \cdot b) = \text{grad}(a) + \text{grad}(b),$$

falls  $R$  nullteilerfrei ist, ansonsten

$$\text{grad}(a \cdot b) \leq \text{grad}(a) + \text{grad}(b).$$

## Beispiel 131

Für  $a(x) = x^2 - 3x + 5$  und  $b(x) = 4x + 2$  ergibt sich

$$\begin{aligned}(a \cdot b)(x) &= (1 \cdot 4)x^3 + (1 \cdot 2 + (-3) \cdot 4)x^2 + \\ &\quad ((-3) \cdot 2 + 5 \cdot 4)x + 5 \cdot 2 \\ &= 4x^3 - 10x^2 + 14x + 10.\end{aligned}$$

Man sagt auch, dass die Koeffizienten

$$c_i = \sum_{j=0}^i a_j b_{i-j}$$

des Produktpolynoms durch **Faltung** der Koeffizientenfolgen von  $a(x)$  und  $b(x)$  entstehen.

### **Beobachtung:**

Das Produkt zweier Polynome vom Grad  $\leq n$  lässt sich in Zeit  $O(n^2)$  berechnen.

Es gibt dafür aber auch schnellere Algorithmen!

## Division

Für diesen Abschnitt setzen wir voraus, dass der Koeffizientenring ein Körper ist. Betrachte das Schema

$$\begin{array}{r} 2x^4 + x^3 + \phantom{0x^2} + \phantom{0x} + \phantom{0} \quad x + 3 \text{ div } x^2 + x - 1 = 2x^2 - x + 3 \\ - (2x^4 + 2x^3 - 2x^2) \\ \hline \phantom{2x^4} - x^3 + 2x^2 + \phantom{0x} + \phantom{0} \quad x + 3 \\ - (-x^3 - x^2 + x) \\ \hline \phantom{2x^4} \phantom{-x^3} 3x^2 + \phantom{0x} + \phantom{0} \quad 3 \\ - (3x^2 + 3x - 3) \\ \hline \phantom{2x^4} \phantom{-x^3} \phantom{3x^2} - 3x + 6 \end{array}$$

## Satz 132

Zu je zwei Polynomen  $a(x)$  und  $b(x)$ ,  $b \neq 0$ , gibt es eindeutig bestimmte Polynome  $q(x)$  und  $r(x)$ , so dass

$$a(x) = q(x)b(x) + r(x) \text{ und } r = 0 \text{ oder } \text{grad}(r) < \text{grad}(b).$$

## Beispiel 133

Im vorhergehenden Schema war das

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{q(x)} \cdot \underbrace{(x^2 + x - 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}$$

## Beweis:

Gilt  $\text{grad}(a) < \text{grad}(b)$ , so kann man  $q = 0$  und  $r = a$  setzen. Sei also  $\text{grad}(a) \geq \text{grad}(b)$ .

Induktion über  $\text{grad}(a)$ :

Ist  $\text{grad}(a) = 0$ , so folgt aus  $\text{grad}(a) \geq \text{grad}(b)$ , dass  $a$  und  $b$  beides konstante Funktionen sind. Also  $a(x) = a_0$  und  $b(x) = b_0$  mit  $b_0 \neq 0$ . Wir können daher  $q(x) = a_0/b_0$  und  $r(x) = 0$  setzen.

## Beweis (Forts.):

Ist  $\text{grad}(a) = n > 0$  und  $\text{grad}(b) = m, m \leq n$ , und

$$\begin{aligned} a(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, & a_n \neq 0, \\ b(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0, & b_m \neq 0 \end{aligned}$$

so setzen wir

$$\tilde{a}(x) = a(x) - (a_n/b_m)x^{n-m} \cdot b(x).$$

Dann gilt  $\text{grad}(\tilde{a}) < \text{grad}(a)$ .

Nach Induktionsannahme gibt es daher Polynome  $\tilde{q}(x)$  und  $\tilde{r}(x)$  mit  $\tilde{a}(x) = \tilde{q}(x) \cdot b(x) + \tilde{r}(x)$ , mit  $\tilde{r}(x) = 0$  oder  $\text{grad}(\tilde{r}) < \text{grad}(b)$ . Es gilt

$$a(x) = (a_n/b_m)x^{n-m}b(x) + \tilde{q}(x)b(x) + \tilde{r}(x) =: q(x)b(x) + r(x).$$

## Beweis (Forts.):

Um die **Eindeutigkeit** zu beweisen, nehmen wir an, es gäbe für Polynome  $a$  und  $b$  zwei Darstellungen wie im Satz angegeben. Also  $q \cdot b + r = a = \hat{q} \cdot b + \hat{r}$  und somit auch

$$(q - \hat{q}) \cdot b = (r - \hat{r}).$$

Falls  $q \neq \hat{q}$ , ist die linke Seite ein Polynom vom Grad  $\geq \text{grad}(b)$ . Da die rechte Seite aus der Differenz zweier Polynome vom Grad kleiner als  $\text{grad}(b)$  besteht, Widerspruch! Also ist  $q = \hat{q}$  und damit auch  $r = \hat{r}$ .



### Beobachtung:

Für zwei Polynome  $a$  und  $b$  von Grad höchstens  $n$  kann man die Polynome  $q$  und  $r$  aus Satz 132 wie im Beispiel bestimmen. Da sich der Grad des Polynoms in jeder Zeile verringert, benötigen wir also höchstens  $n$  Multiplikationen von Polynomen mit Konstanten und  $n$  Subtraktionen von Polynomen vom Grad höchstens  $n$ .

Insgesamt ergibt sich:

Die Division zweier Polynome vom Grad  $\leq n$  lässt sich in Zeit  $O(n^2)$  berechnen.

### Beobachtung:

Falls der führende Koeffizient des Divisorpolynoms gleich 1 ist, lässt sich die Division auch über einem Ring  $R$  durchführen.

### 3.3 Nullstellen von Polynomen

#### Definition 134

Eine **Nullstelle** eines Polynoms  $p$  ist ein Wert  $x_0$  mit  $p(x_0) = 0$ .

#### Lemma 135

*Sei  $p \in R[x]$ ,  $x_0 \in R$  eine Nullstelle von  $p$ . Dann ist  $p(x)$  ohne Rest durch  $x - x_0$  teilbar.*

#### Beweis:

Nach Satz 132 gibt es Polynome  $q$  und  $r$  mit

$p(x) = q(x) \cdot (x - x_0) + r(x)$  und  $\text{grad}(r) < \text{grad}(x - x_0) = 1$ ,  
also  $\text{grad}(r) = 0$ , d.h.  $r(x) = r_0$ . Wegen

$p(x_0) = q(x_0) \cdot (x_0 - x_0) + r_0 = r_0$  muss also  $r_0$  gleich Null sein.

D.h.,  $p(x) = q(x) \cdot (x - x_0)$ . □

## Satz 136 (Fundamentalsatz der Algebra)

*Jedes Polynom  $p \neq 0$  mit Grad  $n$  hat höchstens  $n$  Nullstellen.*

### Beweis:

Wir zeigen den Satz durch Induktion über den Grad des Polynoms.

Ist  $p$  ein Polynom mit Grad 0, so ist die Aussage wegen der Annahme  $p \neq 0$  offenbar richtig.

Ist  $p$  ein Polynom mit Grad  $n > 0$ , so hat  $p$  entweder keine Nullstelle (und die Aussage ist somit trivialerweise richtig) oder  $p$  hat mindestens eine Nullstelle  $a$ . Dann gibt es nach Lemma 135 eine Darstellung  $p(x) = q(x) \cdot (x - a)$  mit  $\text{grad}(q) = n - 1$ . Nach Induktionsannahme hat  $q$  höchstens  $n - 1$  und somit  $p$  höchstens  $n$  Nullstellen. □

## Beispiele 137

- Das Polynom  $x^2 - 1 = (x + 1)(x - 1)$  über  $\mathbb{R}$  hat zwei Nullstellen  $x = +1$  und  $x = -1$  in  $\mathbb{R}$ .
- Das Polynom  $x^2 + 1$  hat keine einzige reelle Nullstelle.
- Das Polynom  $x^2 + 1$  hat die beiden komplexen Nullstellen  $x = i$  und  $x = -i$ , wobei  $i$  die imaginäre Einheit bezeichnet, also  $i = \sqrt{-1}$ .

**Bemerkung:**  $\mathbb{C}$  ist **algebraisch abgeschlossen**, da jedes Polynom  $\in \mathbb{C}[x]$  vom Grad  $\geq 1$  mindestens eine Nullstelle  $\in \mathbb{C}$  hat;  $\mathbb{R}$  und  $\mathbb{Q}$  sind **nicht** algebraisch abgeschlossen.

### 3.4 Partialbruchzerlegung

#### Beispiel 138

Finde zu  $\frac{g}{f} = \frac{x^2+1}{(x-1)^2(x-2)}$  Polynome  $p, q$  mit  $\text{grad}(p) < 2$ ,  $\text{grad}(q) < 1$  und

$$\frac{x^2 + 1}{(x - 1)^2(x - 2)} = \frac{p}{(x - 1)^2} + \frac{q}{x - 2}. \quad (*)$$

Die r.S. von (\*) heißt **Partialbruchzerlegung** von  $\frac{g}{f}$ .

Ansatz:  $p(x) = ax + b$ ,  $q(x) = c$ .

$$\frac{p}{(x - 1)^2} + \frac{q}{x - 2} = \frac{(x - 2) \cdot p + (x - 1)^2 \cdot q}{(x - 1)^2(x - 2)}.$$

Durch Vergleich mit (\*) erhält man

$$\begin{aligned}x^2 + 1 &= (ax + b)(x - 2) + c(x - 1)^2 \\ &= (a + c)x^2 + (b - 2a - 2c)x + c - 2b.\end{aligned}$$

Koeffizientenvergleich liefert folgendes lineares Gleichungssystem:

$$\begin{aligned}a + c &= 1 \\ b - 2a - 2c &= 0 \\ c - 2b &= 1\end{aligned}$$

Dieses hat die eindeutige Lösung  $a = -4$ ,  $b = 2$ ,  $c = 5$ . Somit gilt:

$$\frac{x^2 + 1}{(x - 1)^2(x - 2)} = \frac{-4x + 2}{(x - 1)^2} + \frac{5}{x - 2}.$$

## Satz 139 (Partialbruchzerlegung)

Seien  $f, g \in K[x]$  ( $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ) Polynome mit  $\text{grad}(g) < \text{grad}(f)$ , und es gelte

$$f(x) = (x - \alpha_1)^{m_1} \cdot \dots \cdot (x - \alpha_r)^{m_r}$$

mit  $\mathbb{N} \ni m_i \geq 1$  und paarweise verschiedenen  $\alpha_i \in K$  ( $i = 1, \dots, r$ ). Dann gibt es eindeutig bestimmte Polynome  $g_1, \dots, g_r \in K[x]$  mit  $\text{grad}(g_i) < m_i$ , so dass gilt:

$$\frac{g}{f} = \frac{g_1}{(x - \alpha_1)^{m_1}} + \dots + \frac{g_r}{(x - \alpha_r)^{m_r}}.$$

## Beweis:

Induktion nach  $r$ . Für  $r = 1$  ist nichts zu zeigen. Es gelte  $r > 1$ . Sei  $\tilde{f} = (x - \alpha_2)^{m_2} \cdot \dots \cdot (x - \alpha_r)^{m_r}$ . Dann gilt  $f = (x - \alpha_1)^{m_1} \tilde{f}$ . Sei  $d = \text{grad}(f)$  und  $\tilde{d} = \text{grad}(\tilde{f})$ . Es genügt nun, Folgendes zu zeigen:

**Zwischenbehauptung:** Es gibt eindeutig bestimmte Polynome  $A, B \in K[x]$  mit  $\text{grad}(A) < m_1$ ,  $\text{grad}(B) < \tilde{d}$ , so dass

$$\frac{g}{f} = \frac{A}{(x - \alpha_1)^{m_1}} + \frac{B}{\tilde{f}} \quad (1)$$

gilt.

(Wendet man auf  $\frac{B}{\tilde{f}}$  die Induktionsbehauptung an, so folgt die Behauptung des Satzes.)

Gleichung (1) ist äquivalent zu

$$A\tilde{f} + B(x - \alpha_1)^{m_1} = g. \quad (2)$$

Wir machen den Ansatz:  $A = \sum_{i=0}^{m_1-1} a_i x^i$ ,  $B = \sum_{j=0}^{\tilde{d}-1} b_j x^j$ .

Durch Koeffizientenvergleich mit (2) erhalten wir folgendes inhomogene lineare Gleichungssystem bestehend aus  $d$  Gleichungen in den Unbestimmten  $a_{m_1-1}, \dots, a_0, b_{\tilde{d}-1}, \dots, b_0$ :

$$M \cdot \begin{pmatrix} a_{m_1-1} \\ \vdots \\ a_0 \\ b_{\tilde{d}-1} \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} c_{d-1} \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ c_0 \end{pmatrix}, \quad (3)$$

wobei  $M$  eine  $d \times d$ -Matrix ist, und  $g = \sum_{i=0}^{d-1} c_i x^i$ . Wir haben die Zwischenbehauptung bewiesen, wenn wir zeigen können, dass die Matrix  $M$  invertierbar ( $\det M \neq 0$ ) ist. Dazu benötigen wir das folgende Lemma.

## Lemma 140

Seien  $\tilde{A}, \tilde{B} \in K[x]$  Polynome mit  $\text{grad}(\tilde{A}) \geq 1$  und  $\text{grad}(\tilde{B}) \geq 1$ .  
Gibt es dann Polynome  $A, B \in K[x]$ ,  $A \neq 0$  oder  $B \neq 0$ , mit  
 $\text{grad}(A) < \text{grad}(\tilde{A})$ ,  $\text{grad}(B) < \text{grad}(\tilde{B})$  und

$$A\tilde{B} + B\tilde{A} = 0,$$

so sind  $\tilde{A}$  und  $\tilde{B}$  nicht teilerfremd.

### Beweis:

Dies folgt sofort aus der Eindeutigkeit der Primfaktorzerlegung.  $\square$

## Beweis (Forts.):

Nun zurück zum Beweis von Satz Satz:partial. Angenommen

$\det(M) = 0$ . Dann würde es einen Vektor

$x = (a_{m_1-1}, \dots, a_0, b_{\tilde{d}-1}, \dots, b_0)^t \neq 0$  mit  $M \cdot x = 0$  geben, d.h.

es würde Polynome  $A = \sum_{i=0}^{m_1-1} a_i x^i$  und  $B = \sum_{j=0}^{\tilde{d}-1} b_j x^j$ ,  $A \neq 0$

oder  $B \neq 0$ , geben mit  $\text{grad}(A) < m_1 - 1$ ,

$\text{grad}(B) < \tilde{d} - 1 = \text{grad}(\tilde{f})$  und  $A\tilde{f} + B(x - \alpha_1)^{m_1} = 0$ .

Nach Lemma 140 wären dann  $\tilde{f}$  und  $(x - \alpha_1)^{m_1}$  nicht teilerfremd.

Dies ist jedoch ein Widerspruch zur Voraussetzung. Damit ist

Satz Satz:partial bewiesen. □

## 3.5 Schnelle Fouriertransformation (FFT, DFT)

### 3.5.1 Grundlagen

Ein Polynom  $P = \sum_i a_i x^i \in \mathbb{C}[x]$  vom Grad  $\leq n$  ist eindeutig durch seine Koeffizienten  $a_i$  bestimmt, d.h. man hat eine Bijektion

$$\{\text{Polynome} \in \mathbb{C}[x] \text{ vom Grad} \leq n\} \rightarrow \mathbb{C}^{n+1}$$

$$P_{\vec{a}} = \sum_{i=0}^n a_i x^i \mapsto \vec{a} = (a_0, \dots, a_n).$$

Problem:  $P_{\vec{a}} \cdot P_{\vec{b}} = P_{\vec{c}}$  mit  $\vec{c} = (c_0, \dots, c_{2n})$ ,  $c_k = \sum_i a_{k-i} b_i$ , und die naive Berechnung von  $\vec{c}$  benötigt  $\Theta(n^2)$  Operationen.

**Bemerkung:**  $\vec{c} = \vec{a} * \vec{b}$  mit  $c_k = \sum_i a_{k-i} b_i$  ist die **Faltung** von  $\vec{a}$  und  $\vec{b}$ .

Es gibt noch eine weitere eindeutige Darstellung eines Polynoms.

### Lemma 141

Seien  $P = \sum_{i=1}^n a_i x^i$  und  $Q = \sum_{j=0}^n b_j x^j$  Polynome ( $\in \mathbb{C}[x]$ ) vom Grad  $\leq n$  und seien  $\omega_0, \dots, \omega_n \in \mathbb{C}$  paarweise verschiedene Elemente. Dann gilt:

$$P = Q \iff P(\omega_i) = Q(\omega_i) \quad \text{für alle } i = 0, \dots, n.$$

### Beweis:

„ $\Rightarrow$ “: Klar.

„ $\Leftarrow$ “: Es gelte  $P(\omega_i) = Q(\omega_i)$  für  $i = 0, \dots, n$ . Dann ist jedes  $\omega_i$  eine Nullstelle des Polynoms  $P - Q$ . Da  $\text{grad}(P - Q) \leq n$  gilt, folgt  $P - Q = 0$  aus Satz Satz:fundalg. □

Man kann leicht zeigen, dass es zu jedem Tupel  $(b_0, \dots, b_n) \in \mathbb{C}^{n+1}$  (genau) ein Polynom  $f \in \mathbb{C}[x]$  vom Grad  $\leq n$  gibt, mit  $f(\omega_i) = b_i$  für  $i = 0, \dots, n$  (z.B. das **Newton'sche Interpolationspolynom**, benannt nach **Sir Isaac Newton** (1643–1727)).

Somit erhalten wir eine weitere Bijektion:

$$\begin{aligned} \{\text{Polynome } \in \mathbb{C}[x] \text{ vom Grad } \leq n\} &\rightarrow \mathbb{C}^{n+1} \\ P &\mapsto (P(\omega_0), \dots, P(\omega_n)) \end{aligned}$$

Vorteil:

$$\begin{aligned} P \times Q &\mapsto (P(\omega_0)Q(\omega_0), \dots, P(\omega_n)Q(\omega_n)) = \\ &\quad (P(\omega_0), \dots, P(\omega_n)) \cdot (Q(\omega_0), \dots, Q(\omega_n)). \end{aligned}$$

Multiplikation benötigt nur  $O(n)$  Operationen. „ $\cdot$ “ auf der rechten Seite bezeichnet hier das komponentenweise (**Hadamard**) Vektorprodukt (**Jacques S. Hadamard** (1865–1963)).

Problem: Bijektion i.a. zu komplex.

### Definition 142

Ein  $\omega \in \mathbb{C}$  heißt **primitive  $n$ -te Einheitswurzel**, wenn  $\omega^k \neq 1$  für alle  $k = 1, \dots, n-1$  und  $\omega^n = 1$  gilt, d.h.  $\text{ord}(\omega) = n$  in  $\mathbb{C}^* = \mathbb{C} \setminus 0$ .

**Bemerkung:** Es ist  $\omega = e^{2i\pi/n}$  eine primitive  $n$ -te Einheitswurzel.

### Definition 143

Sei  $\omega \in \mathbb{C}$  eine primitive  $n$ -te Einheitswurzel,  $n \in \mathbb{N}$ . Die Abbildung

$$\mathcal{F}_{n,\omega} : \mathbb{C}^n \rightarrow \mathbb{C}^n, \\ \vec{a} = (a_0, \dots, a_{n-1}) \mapsto (P_{\vec{a}}(1), P_{\vec{a}}(\omega), \dots, P_{\vec{a}}(\omega^{n-1}))$$

heißt **diskrete Fouriertransformation**; wir schreiben auch kurz  $\mathcal{F}$  für  $\mathcal{F}_{n,\omega}$ .

Die Fouriertransformation ist nach **Jean Baptiste Joseph Fourier** (1768–1830) benannt.

## Bemerkung:

$\mathcal{F}$  is nach Lemma 141 und anschließender Bemerkung eine Bijektion.

### Lemma 144

Für  $\vec{a}, \vec{b} \in \mathbb{C}^n$  gilt

$$\mathcal{F}(\vec{a} * \vec{b}) = \mathcal{F}(\vec{a}) \cdot \mathcal{F}(\vec{b}).$$

### Beweis:

Es gilt

$$\begin{aligned}\mathcal{F}(\vec{a}) \cdot \mathcal{F}(\vec{b}) &= (P_{\vec{a}}(1)P_{\vec{b}}(1), P_{\vec{a}}(\omega)P_{\vec{b}}(\omega), \dots, P_{\vec{a}}(\omega^{n-1})P_{\vec{b}}(\omega^{n-1})) \\ &= (P_{\vec{c}}(1), P_{\vec{c}}(\omega), \dots, P_{\vec{c}}(\omega^{n-1})) \\ &= \mathcal{F}(\vec{c}), \quad \text{mit } \vec{c} = \vec{a} * \vec{b}.\end{aligned}$$



Idee: Berechne  $\vec{a} * \vec{b}$  vermöge  $\mathcal{F}^{-1}(\mathcal{F}(\vec{a}) \cdot \mathcal{F}(\vec{b}))$ . Die komponentenweise Multiplikation  $\mathcal{F}(\vec{a}) \cdot \mathcal{F}(\vec{b})$  benötigt nur  $O(n)$  Operationen.

Jedoch:  $\mathcal{F}$  ist eine lineare Abbildung  $\mathcal{F}(\vec{a}) = \Omega \cdot \vec{a}$ , mit  $\Omega = (\omega^{kl})_{0 \leq l, k \leq n-1}$ . Die Matrixmultiplikation benötigt aber  $\Omega(n^2)$  Operationen (also keine offensichtliche Verbesserung im Vergleich zur klassischen Polynom-Multiplikation)!

Ausweg: "Divide and Conquer"!!!

### 3.5.2 Berechnung der diskreten Fouriertransformation (FFT)

Sei  $n = 2^k$  eine 2er-Potenz. Zerlege  $\vec{a} = (a_0, \dots, a_{n-1})$  in einen

geraden Anteil  $\vec{a}_g = (a_0, a_2, \dots, a_{n-2})$  und einen  
ungeraden Anteil  $\vec{a}_u = (a_1, a_3, \dots, a_{n-1})$

Dann gilt:

$$P_{\vec{a}}(x) = P_{\vec{a}_g}(x^2) + xP_{\vec{a}_u}(x^2).$$

#### Beispiel 145

Sei  $\vec{a} = (1, 2, 4, 8)$ , also  $P_{\vec{a}}(x) = 1 + 2x + 4x^2 + 8x^3$ . Damit ist  
 $\vec{a}_g = (1, 4)$  und  $\vec{a}_u = (2, 8)$ , also

$$\begin{aligned} P_{\vec{a}_g}(x^2) + xP_{\vec{a}_u}(x^2) &= 1 \cdot (x^2)^0 + 4 \cdot (x^2)^1 + x \cdot (2 \cdot (x^2)^0 + 8 \cdot (x^2)^1) \\ &= 1 + 2 \cdot x + 4 \cdot x^2 + 8 \cdot x^3 \end{aligned}$$

## Lemma 146

Ist  $\mathcal{F}_{\frac{n}{2}, \omega^2}(\vec{a}_g) = (c_0, \dots, c_{\frac{n}{2}-1})$  und  $\mathcal{F}_{\frac{n}{2}, \omega^2}(\vec{a}_u) = (d_0, \dots, d_{\frac{n}{2}-1})$ ,  
so gilt  $\mathcal{F}_{n, \omega}(\vec{a}) = (e_0, \dots, e_{n-1})$  mit

$$\begin{aligned}e_i &= P_{\vec{a}}(\omega^i) \\&= P_{\vec{a}_g}(\omega^{2i}) + \omega^i P_{\vec{a}_u}(\omega^{2i}) \\&= c_i + \omega^i d_i \\e_{\frac{n}{2}+i} &= P_{\vec{a}}(\omega^{\frac{n}{2}+i}) \\&= P_{\vec{a}_g}(\omega^{2(\frac{n}{2}+i)}) + \omega^{\frac{n}{2}+i} P_{\vec{a}_u}(\omega^{2(\frac{n}{2}+i)}) \\&= c_i + \omega^{\frac{n}{2}+i} d_i\end{aligned}$$

für  $i = 0, \dots, \frac{n}{2} - 1$ .

Bem.:  $\omega^2$  ist primitive  $\frac{n}{2}$ -te Einheitswurzel. Natürlich ist  $\omega^{2\frac{n}{2}} = 1$ .

Dies liefert folgenden **Divide-and-Conquer**-Algorithmus:

DFT( $\vec{a}, \omega$ )

Eingabe:  $\vec{a} = (a_0, \dots, a_{n-1})$ ,  $n = 2^k$ ,  $\omega$

Ausgabe:  $\mathcal{F}_{n,\omega}(\vec{a}) = (e_0, \dots, e_{n-1})$

if  $n = 1$  then  $e_0 := a_0$

else

$\vec{a}_g := (a_0, a_2, \dots, a_{n-2})$

$\vec{a}_u := (a_1, a_3, \dots, a_{n-1})$

$(c_0, \dots, c_{\frac{n}{2}-1}) := \text{DFT}(\vec{a}_g, \omega^2)$

$(d_0, \dots, d_{\frac{n}{2}-1}) := \text{DFT}(\vec{a}_u, \omega^2)$

for  $i = 0$  to  $\frac{n}{2} - 1$  do

$e_i := c_i + \omega^i d_i$

$e_{\frac{n}{2}+i} := c_i + \omega^{\frac{n}{2}+i} d_i$

endfor

endif

return( $e_0, \dots, e_{n-1}$ )

## Satz 147

Der Algorithmus DFT berechnet  $\mathcal{F}_{n,\omega}(\vec{a})$  auf Eingabe  $n = 2^k$ ,  $\vec{a}$ ,  $\omega$  in  $T(n) = O(n \log n)$  Operationen.

### Beweis:

Aus dem Algorithmus erhält man folgende Rekursion

$$T(n) = 2T(n/2) + cn$$

mit einer Konstante  $c > 0$  und  $T(1) = 1$ . Mit  $n = 2^k$  folgt

$$\begin{aligned} T(2^k) &= 2T(2^{k-1}) + cn = 2(2T(2^{k-2}) + cn/2) + cn \\ &= \dots = 2^\ell T(2^{k-\ell}) + \ell cn \end{aligned}$$

Speziell für  $\ell = k$  gilt  $T(2^k) = kc2^k + 2^k T(1)$ , und wir erhalten  $T(2^k) = O(2^k k) = O(n \log n)$ . □

### 3.5.3 Berechnung der inversen diskreten Fouriertransformation

#### Satz 148

Es gilt

$$\mathcal{F}_{n,\omega}^{-1} = \frac{1}{n} \mathcal{F}_{n,\omega^{-1}}.$$

**Bemerkung:**  $\omega^{-1}$  ist ebenso eine primitive  $n$ -te Einheitswurzel. Zum Beweis von Satz 148 benötigen wir folgendes Lemma:

#### Lemma 149

*Ist  $\omega$  eine primitive  $n$ -te Einheitswurzel, so gilt*

$$\sum_{j=0}^{n-1} \omega^{kj} = 0$$

*für alle  $k = 1, \dots, n - 1$ .*

## Beweis:

Für jedes  $a \in \mathbb{C}$ ,  $a \neq 1$ , gilt  $\sum_{j=0}^{n-1} a^j = \frac{a^n - 1}{a - 1}$ . Speziell für  $a = \omega^k$  ist  $a^n = \omega^{kn} = 1$ , ( $k = 1, \dots, n - 1$ ).  $\square$

Nun zum Beweis von Satz 148.

## Beweis:

Sei  $\vec{e} = \mathcal{F}_{n,\omega}(\vec{a}) = (e_0, \dots, e_{n-1})$ . Wir zeigen, dass gilt:

$$\frac{1}{n} \mathcal{F}_{n,\omega^{-1}}(\vec{e}) = \vec{a}$$

$$\begin{aligned} P_{\vec{e}}(\omega^{-k}) &= \sum_{j=0}^{n-1} e_j \omega^{-kj} = \sum_{j=0}^{n-1} P_{\vec{a}}(\omega^j) \omega^{-kj} \\ &= \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} a_i \omega^{ij} \omega^{-kj} = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} \omega^{(i-k)j} = n a_k, \end{aligned}$$

denn nach Lemma 149 ist  $\sum_{j=0}^{n-1} \omega^{(i-k)j} = 0$ , falls  $i \neq k$ .

Im Fall  $i = k$  gilt  $\sum_{j=0}^{n-1} \omega^{(i-k)j} = n$ .  $\square$

## 3.6 Restklassen in Polynomringen

### 3.6.1 Einführung und Definitionen

Der Begriff der Restklasse stammt ursprünglich aus der Teilbarkeitslehre in  $\mathbb{Z}$ ; ( $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$  ist ein kommutativer Ring).

#### Definition 150

Sei  $n$  eine fest gewählte ganze Zahl  $\neq 0$ . Für jedes  $\ell \in \mathbb{Z}$  heißt die Menge

$$[\ell]_n := \{m \in \mathbb{Z} : m - \ell \text{ ist durch } n \text{ teilbar}\}$$

die Restklasse von  $\ell$  modulo  $n$ .

# Bemerkungen

- ① Für  $\ell, m \in \mathbb{Z}$  gilt:

$$m \in [\ell]_n \iff m \bmod n = \ell \bmod n.$$

Gilt  $m \in [\ell]_n$ , so schreibt man auch  $m \equiv \ell \pmod{n}$  und spricht „ $m$  kongruent  $\ell$  modulo  $n$ “.

- ② Es gilt  $[\ell]_n = \{\ell + kn : k \in \mathbb{Z}\} =: \ell + n\mathbb{Z} =: \ell + (n)$ .
- ③ Da es genau  $n$  verschiedene Reste  $0, 1, \dots, n-1$  gibt, gibt es auch genau  $n$  verschiedene Restklassen  $[0]_n, [1]_n, \dots, [n-1]_n$ .

# Bemerkungen

- 4 Kongruenz modulo  $n$  definiert auf  $\mathbb{Z}$  eine Äquivalenzrelation  $\sim_n: m \sim_n \ell : \iff n \text{ teilt } m - \ell$ , und  $[\ell]_n$  ist die Äquivalenzklasse von  $\ell$ .
- 5 Auf der Menge aller Restklassen  $[\ell]_n$  kann man Addition und Multiplikation wie folgt definieren

$$[\ell]_n + [m]_n := [\ell + m]_n, \quad [\ell]_n \cdot [m]_n := [\ell \cdot m]_n,$$

und erhält einen kommutativen Ring; er heißt der **Restklassenring  $\mathbb{Z}$  modulo  $n$**  und wird mit  $\mathbb{Z}/(n)$ , oder  $\mathbb{Z}/n\mathbb{Z}$  bezeichnet.

- 6 Die Abbildung  $(\mathbb{Z}/(n), +, \cdot) \rightarrow (\mathbb{Z}_n, +_n, \cdot_n), [\ell]_n \mapsto$  „Rest der Division von  $\ell$  durch  $n$ “ ist ein Ringisomorphismus.

Restklassen können auch im Polynomring  $K[x]$  ( $K$  ein Körper) gebildet werden.

### Definition 151

Sei  $g \in K[x]$  ein Polynom,  $\text{grad}(g) \geq 1$ . Für jedes  $f \in K[x]$  heißt die Menge

$$[f]_g := \{h \in K[x] : h - f \text{ ist durch } g \text{ teilbar}\}$$

die Restklasse von  $f$  modulo  $g$ .

**Bemerkung:** Wie in  $\mathbb{Z}$  gilt nun auch im Polynomring  $K[x]$ :

- 1  $h \in [f]_g \iff h$  und  $f$  haben bei Polynomdivision durch  $g$  denselben Rest.
- 2  $[f]_g = \{f + hg : h \in K[x]\} =: f + (g)$  mit  $(g) := \{hg : h \in K[x]\} =$  Menge aller Polynome, die durch  $g$  teilbar sind.

- ③ „Kongruenz modulo  $g$ “ definiert auf  $K[x]$  eine Äquivalenzrelation  $\sim_g: h \sim_g f \iff h - f$  ist durch  $g$  teilbar, und  $[f]_g$  ist die Äquivalenzklasse von  $f$ .
- ④ Auf der Menge aller Restklassen  $[f]_g$  kann man Addition und Multiplikation wie folgt definieren

$$[f]_g + [h]_g := [f + h]_g, \quad [f]_g \cdot [h]_g := [f \cdot h]_g,$$

und erhält einen kommutativen Ring; er heißt der Restklassenring  $K[x]$  modulo  $g$  und wird mit  $K[x]/(g)$  bezeichnet.

### 3.6.2 Eigenschaften von Restklassenringen

Teilt man Polynome durch ein fest gewähltes Polynom  $g$ ,  $\text{grad}(g) \geq 1$ , so treten als Reste sämtliche Polynome vom Grad  $< d = \text{grad}(g)$  auf. Deshalb setzen wir

$$K[x]_d := \{h \in K[x] : \text{grad}(h) < d\},$$

und definieren auf  $K[x]_d$  Addition  $+_g$  und Multiplikation  $\cdot_g$  wie folgt:

Mit  $\text{Rem}(f)$  bezeichnen wir den Rest der Polynomdivision von  $f$  durch  $g$ .

$$f +_g h := f + h, \quad f \cdot_g h := \text{Rem}(f \cdot h).$$

Man prüft leicht nach, dass  $(K[x]_d, +_g, \cdot_g)$  ein kommutativer Ring ist.

## Satz 152

Sei  $g \in K[x]$  ein Polynom,  $d = \text{grad}(g) \geq 1$ . Dann ist die Abbildung

$$(K[x]/(g), +, \cdot) \rightarrow (K[x]_d, +_g, \cdot_g), \quad [f]_g \mapsto \text{Rem}(f)$$

ein Ringisomorphismus, die Umkehrabbildung ist gegeben durch  $r \mapsto [r]_g$ .

## Beweis:

Es gilt

1

$$[f]_g = [0]_g \iff g|f \iff \text{Rem}(f) = 0$$

2

$$\begin{aligned} [f]_g + [h]_g &= [f + h]_g \mapsto \text{Rem}(f + h) = \\ &\text{Rem}(f) + \text{Rem}(h) = \text{Rem}(f) +_g \text{Rem}(h) \end{aligned}$$

3

$$\begin{aligned} [f]_g \cdot [h]_g &= [f \cdot h]_g \mapsto \text{Rem}(f \cdot h) \\ &= \text{Rem}(\text{Rem}(f) \cdot \text{Rem}(h)) = \text{Rem}(f) \cdot_g \text{Rem}(h). \end{aligned}$$

Aus (1) - (3) folgt, dass obige Abbildung wohldefiniert, injektiv und ein Ringhomomorphismus ist; sie ist auch surjektiv, denn für  $f \in K[x]_d$  ist  $\text{Rem}(f) = f$ . □

## Satz 153

Sei  $K$  ein Körper mit  $n$  Elementen, und sei  $g \in K[x]$ ,  
 $d = \text{grad}(g) \geq 1$ . Dann besitzt  $K[x]/(g)$  genau  $n^d$  Elemente.

### Beweis:

Nach Satz 152 ist  $|K[x]/(g)| = |K[x]_d|$ , und offensichtlich gilt  
 $|K[x]_d| = n^d$ . □

## Definition 154

Ein Polynom  $g \in K[x]$  heißt **irreduzibel**, falls  $\text{grad}(g) \geq 1$  gilt und aus  $g = g_1 \cdot g_2$  mit  $g_1, g_2 \in K[x]$  stets  $\text{grad}(g_1) = 0$  oder  $\text{grad}(g_2) = 0$  folgt; ansonsten heißt  $g$  **reduzibel**.

## Satz 155

Sei  $g \in K[x]$ ,  $\text{grad}(g) \geq 1$ . Dann gilt:

$K[x]/(g)$  ist ein Körper  $\Leftrightarrow g$  ist irreduzibel.

### Beweis:

“ $\Rightarrow$ ” Sei  $K[x]/(g)$  ein Körper. Angenommen,  $g$  ist **nicht** irreduzibel.

Dann gibt es  $g_1, g_2 \in K[x]$  mit  $g = g_1 \cdot g_2$  und  $\text{grad}(g_1), \text{grad}(g_2) \geq 1$ .

Da  $d := \text{grad}(g) = \text{grad}(g_1) + \text{grad}(g_2)$ , folgt  $\text{grad}(g_1) < d$  und  $\text{grad}(g_2) < d$ . Also gilt  $[g_1]_g \neq [0]_g$  und  $[g_2]_g \neq [0]_g$ .

Jedoch ist

$$[g_1]_g \cdot [g_2]_g = [g_1 g_2]_g = [g]_g = [0]_g,$$

d.h.  $[g_1]_g$  und  $[g_2]_g$  sind **Nullteiler**. In einem Körper gibt es jedoch keine Nullteiler (vgl. Satz 120).

## Beweis (Forts.):

“ $\Leftarrow$ ” Sei  $g$  irreduzibel, und sei  $[f]_g \neq [0]_g$  gegeben.

$[f]_g \neq [0]_g$  bedeutet, dass  $f$  nicht durch  $g$  teilbar ist. Da  $g$  irreduzibel ist, sind  $f$  und  $g$  daher teilerfremd.

Somit existieren Polynome  $p, q \in K[x]$  mit  $pf + qg = 1$ , und es folgt

$$\begin{aligned} [p]_g \cdot [f]_g &= [pf]_g = [1 - qg]_g = [1]_g - \underbrace{[qg]_g}_{=[0]_g} \\ &= [1]_g \cdot \end{aligned}$$

Also ist  $[p]_g = ([f]_g)^{-1}$ .



## 3.7 Konstruktion endlicher Körper

### Satz 156

Zu jeder Primzahl  $p$  und zu jeder natürlichen Zahl  $n \geq 1$  gibt es einen endlichen Körper mit  $p^n$  Elementen; dieser wird mit  $GF(p^n)$  bezeichnet ( $GF = \mathbf{G}$ alois  $\mathbf{F}$ ield, nach *Evariste Galois* (1811–1832)).

Beweis:

$n = 1$ :  $\mathbb{Z}_p = GF(p)$  ist ein Körper mit  $p$  Elementen.

$n > 1$ : Sei  $K = \mathbb{Z}_p$ . Sei  $g \in K[x]$  ein *irreduzibles* Polynom vom Grad  $n$  (zur Existenz eines solchen Polynoms: siehe Bemerkung unten).

Nach Satz 155 ist  $K[x]/(g)$  ein Körper, und nach Satz 153 hat  $K[x]/(g)$  genau  $p^n$  Elemente.

□

## Satz 157

Je zwei endliche Körper mit  $p^n$  Elementen sind *isomorph*.

### Beweis:

siehe geeignetes Textbuch zur Algebra oder Zahlentheorie,  
ebenfalls bzgl. der Existenz irreduzibler Polynome! □

## Beispiel 158

Wir betrachten den Fall  $K = \mathbb{Z}_3 = GF(3)$  und  $p(x) = x^2 + 1$ .

Der Ring  $\mathbb{Z}_3[x]/(p)$  besteht also aus allen Polynomen in  $\mathbb{Z}_3[x]$  vom Grad  $\leq 1$ :

$$\mathbb{Z}_3[x]/(p) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\} .$$

Bemerkung zur Notation: Wir schreiben hier (und auch sonst) das Polynom  $f$  statt der Restklasse  $[f]_g$ .

Das Polynom  $p$  ist irreduzibel. **Wieso?**

## Beispiel 159

Für  $K = \mathbb{Z}_2 = GF(2)$  und  $p(x) = x^2 + x + 1$  gilt in ähnlicher Weise

$$\mathbb{Z}_2[x]/(p) = \{0, 1, x, x + 1\}.$$

Für die Addition und Multiplikation modulo  $p$  ergibt sich

$+_p$	0	1	$x$	$x + 1$	$\cdot_p$	0	1	$x$	$x + 1$
0	0	1	$x$	$x + 1$	0	0	0	0	0
1	1	0	$x + 1$	$x$	1	0	1	$x$	$x + 1$
$x$	$x$	$x + 1$	0	1	$x$	0	$x$	$x + 1$	1
$x + 1$	$x + 1$	$x$	1	0	$x + 1$	0	$x + 1$	1	$x$

Aus diesen beiden Tabellen folgt, dass  $\mathbb{Z}_2[x]/(p)$  mit den angegebenen Verknüpfungen  $+_p$  und  $\cdot_p$  einen Körper mit **4 Elementen** bildet (den wir schon früher gesehen haben).

## Beispiel 160

Für  $K = \mathbb{Z}_2$  und  $q(x) = x^2 + 1$  gilt wiederum

$$\mathbb{Z}_2[x]/(q) = \{0, 1, x, x + 1\} .$$

Für die Addition und Multiplikation modulo  $q$  ergibt sich nunmehr jedoch

$+_q$	0	1	$x$	$x + 1$
0	0	1	$x$	$x + 1$
1	1	0	$x + 1$	$x$
$x$	$x$	$x + 1$	0	1
$x + 1$	$x + 1$	$x$	1	0

$\cdot_q$	0	1	$x$	$x + 1$
0	0	0	0	0
1	0	1	$x$	$x + 1$
$x$	0	$x$	1	$x + 1$
$x + 1$	0	$x + 1$	$x + 1$	0

Aus der zweiten Tabelle folgt, dass  $\mathbb{Z}_2[x]/(q) \setminus \{0\}$  bzgl.  $\cdot_q$  keine Gruppe bildet. Der Grund ist, dass  $q$  nicht irreduzibel ist.

### 3.8 Redundante Datenspeicherung und Fehlerkorrektur

Seien natürliche Zahlen  $k, t$  und  $s$  so gewählt, dass

$$k + 2t \leq 2^s - 1.$$

Sei weiter  $K = GF(2^s)$ , und seien  $c_0, \dots, c_{k-1} \in K$ . Wir fassen die  $c_i$  sowohl als Elemente von  $K$  als auch (in frei festzulegender, eindeutiger Weise) als *Binärwörter der Länge  $s$*  auf.

Sei weiter  $\alpha$  ein primitives Element in  $K = GF(2^s)$  (existiert nach Satz 124) und seien

$$g(x) := \prod_{i=1}^{2t} (x - \alpha^i),$$

$$c(x) := \sum_{i=0}^{k-1} c_i x^i, \text{ und}$$

$$d(x) = \sum_{i=0}^{k+2t-1} d_i x^i := g(x) \cdot c(x).$$

Wir sagen, dass der Vektor der Koeffizienten von  $d(x)$  den Vektor  $(c_0, \dots, c_{k-1})$  **kodiert** (**Reed-Solomon-Code**  $RS(s, k, t)$ ).

## Satz 161

Für jedes  $s \in \mathbb{N}$  und  $k, t \in \mathbb{N}$  mit  $k + 2t \leq 2^s - 1$  ist der Reed-Solomon-Code  $RS(s, k, t)$  *t-fehlerkorrigierend* und *2t-fehlererkennend*.

Das bedeutet, dass, falls bei der Übertragung des Vektors der  $d_i$  nicht mehr als  $2t$  der  $d_i$ 's verändert werden, dies **erkannt** werden kann. Werden höchstens  $t$  der  $d_i$ 's verändert, so können die ursprünglichen  $d_i$ 's sogar **rekonstruiert** werden.

## Beweis:

Sei  $(f_0, \dots, f_{k+2t-1})$  der sich nach der Übertragung ergebende Code-Vektor, sei  $e_i := f_i - d_i$  für  $i = 0, \dots, k + 2t - 1$ , und seien

$$e(x) := \sum_{i=0}^{k+2t-1} e_i x^i \quad \text{und} \quad f(x) := \sum_{i=0}^{k+2t-1} f_i x^i .$$

Dann gilt  $f(x) = d(x) + e(x)$ , und es folgt

$$f(\alpha^i) = e(\alpha^i) \quad \text{für alle } 1 \leq i \leq 2t .$$

## Beweis (Forts.):

In Matrixschreibweise sieht dies wie folgt aus:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{2(k+2t-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(k+2t-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t} & \alpha^{4t} & \alpha^{6t} & \dots & \alpha^{2t(k+2t-1)} \end{pmatrix} \cdot \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{k+2t-2} \\ e_{k+2t-1} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}.$$

Falls nur  $e_{i_1}, \dots, e_{i_r}$  ungleich 0 sind, fallen Spalten weg und es ergibt sich

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_r} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_r} \\ \alpha^{3i_1} & \alpha^{3i_2} & \dots & \alpha^{3i_r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2ti_1} & \alpha^{2ti_2} & \dots & \alpha^{2ti_r} \end{pmatrix} \cdot \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix}.$$

## Beweis (Forts.):

Immer wenn die Anzahl  $r$  der Spalten  $\leq$  der Anzahl  $2t$  der Zeilen ist, hat diese Matrix vollen Spaltenrang (Vandermonde-Matrix).

- Wenn  $(e(\alpha^i) =) f(\alpha^i) = 0$  für  $i = 1, \dots, 2t$ , dann ist  $e_i = 0$  für alle  $i$  eine Lösung, und zwar dann die einzige (Spaltenrang).
- Falls  $\leq t$  Fehler aufgetreten sind, können wir entsprechende  $e_{i_j}$  eindeutig bestimmen (z.B. durch Probieren) und damit die  $d_i$  rekonstruieren.



## 4. Die elementaren Zählfunktionen

### 4.1 Untermengen

#### Definition 162 (Binomialkoeffizienten)

$$\binom{n}{0} := 1 \quad \forall n \in \mathbb{N}_0$$

$$\binom{n}{k} := 0 \quad n < k, n \in \mathbb{N}_0, k \in \mathbb{N}$$

$$\binom{n}{k} := \binom{n-1}{k} + \binom{n-1}{k-1} \quad \text{sonst} \quad (n, k \in \mathbb{N})$$

## Satz 163

Sei  $N$  eine Menge mit  $|N| = n$  Elementen. Die Menge aller  $k$ -elementigen Untermengen von  $N$  wird bezeichnet mit

$$\binom{N}{k}.$$

Es gilt:

$$\left| \binom{N}{k} \right| = \binom{|N|}{k} = \binom{n}{k}.$$

## Beweis:

Seien  $n, k \geq 0, a \in N$ .

①

$\binom{n}{0}$  und  $k > n$  sind klar.

② Definiere

$$S_a := \left\{ A \in \binom{N}{k}; a \in A \right\},$$
$$\tilde{S}_a := \left\{ A \in \binom{N}{k}; a \notin A \right\}.$$

## Beweis (Forts.):

- ③ Damit gilt

$$S_a \cup \tilde{S}_a = \binom{N}{k}, \quad S_a \cap \tilde{S}_a = \emptyset.$$

$$|S_a| = \left| \binom{N \setminus \{a\}}{k-1} \right| = \binom{n-1}{k-1} \quad (\text{per Induktion})$$

$$|\tilde{S}_a| = \left| \binom{N \setminus \{a\}}{k} \right| = \binom{n-1}{k} \quad (\text{per Induktion})$$

Daraus folgt

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



## Zwischenbemerkung zur Nomenklatur:

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

## 4.2 Partitionen von Mengen und Zahlen

### 4.2.1 Ungeordnete Partitionen

#### 1. Mengenpartitionen

Sei  $N$  eine Menge der Kardinalität  $n$  und sei  $k \in \mathbb{N}_0$ . Eine Zerlegung von  $N$  in  $k$  nichtleere, paarweise disjunkte Teilmengen heißt eine  **$k$ -Partition** von  $N$ . Die einzelnen Teilmengen heißen auch **Klassen**. Ihre Anzahl wird mit

$$S_{n,k}$$

bezeichnet (die sog. **Stirling-Zahlen der 2. Art**).

## Beispiel 164

$$N = \{1, 2, 3, 4, 5\}, k = 2$$

$$\begin{array}{ll} \{1\} \cup \{2, 3, 4, 5\} & \{1, 2\} \cup \{3, 4, 5\} \\ \{2\} \cup \{1, 3, 4, 5\} & \{1, 3\} \cup \{2, 4, 5\} \\ \{3\} \cup \{1, 2, 4, 5\} & \{1, 4\} \cup \{2, 3, 5\} \\ \{4\} \cup \{1, 2, 3, 5\} & \{1, 5\} \cup \{2, 3, 4\} \\ \{5\} \cup \{1, 2, 3, 4\} & \{2, 3\} \cup \{1, 4, 5\} \\ & \{2, 4\} \cup \{1, 3, 5\} \\ & \{2, 5\} \cup \{1, 3, 4\} \\ & \{3, 4\} \cup \{1, 2, 5\} \\ & \{3, 5\} \cup \{1, 2, 4\} \\ & \{4, 5\} \cup \{1, 2, 3\} \end{array}$$

$$\Rightarrow S_{5,2} = 15.$$

Weiter gilt:  $S_{n,1} = 1, S_{n,2} = \text{Übung}, S_{n,n} = 1.$

## 2. Zahlpartitionen

Sei

$$\mathbb{N}_0 \ni n = n_1 + n_2 + \dots + n_k$$

mit  $n_1, \dots, n_k \in \mathbb{N}$  und  $n_1 \geq n_2 \geq \dots \geq n_k$ .

Eine solche Zerlegung heißt ***k*-Partition** der Zahl  $n$ .

Die Anzahl aller *k*-Partitionen von  $n \in \mathbb{N}$  wird mit

$$P_{n,k}$$

bezeichnet.

## Beispiel 165

$$n = 8, k = 4.$$

$$8 = 5 + 1 + 1 + 1$$

$$= 4 + 2 + 1 + 1$$

$$= 3 + 3 + 1 + 1$$

$$= 3 + 2 + 2 + 1$$

$$= 2 + 2 + 2 + 2$$

$$\Rightarrow P_{8,4} = 5$$

## 4.2.2 Geordnete Partitionen

### 1. Mengenpartitionen

Seien  $N, n, k$  wie vorher. Eine (beliebig) *geordnete*  $k$ -Menge  $\subseteq N$  heißt  $k$ -Permutation aus  $N$ . Ihre Anzahl ist

$$n \cdot (n - 1) \cdots (n - k + 1) = n^{\underline{k}}$$

(„ $n$  hoch  $k$  fallend“, „fallende Fakultät“).

Analog:

$$n^{\overline{k}} := n \cdot (n + 1) \cdots (n + k - 1)$$

Überlegung: Jede  $k$ -Menge aus  $N$  ergibt  $k!$   $k$ -Permutationen. Also

$$\binom{n}{k} \cdot k! = n^{\underline{k}}$$

oder:

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

Eine  $k$ -Mengenpartition ergibt

$$k! \cdot S_{n,k}$$

geordnete  $k$ -Mengenpartitionen (Die Klassen sind (beliebig) *untereinander* geordnet, aber nicht *in sich*!).

## 2. Zahlpartitionen

Eine geordnete Zahlpartition ist gegeben durch

$$\mathbb{N} \ni n = n_1 + n_2 + \dots + n_k; \quad n_1, \dots, n_k \in \mathbb{N}$$

Betrachte folgende graphische Darstellung:



Wähle aus den  $n - 1$  Trennstellen  $k - 1$  aus. Jede der  $\binom{n-1}{k-1}$  Wahlmöglichkeiten ergibt eine eindeutig bestimmte geordnete  $k$ -Zahlpartition und umgekehrt.

Ihre Anzahl ist also

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

## 4.3 Multimengen

### Beispiel 166

$$M := \{1, 2, 2, 3, 5, 5, 5\} \quad |M| = 7$$

### Satz 167

Die Anzahl der  $k$ -Multimengen (also Multimengen der Kardinalität  $k$ ) aus  $N$  ( $|N| = n$ ) ist

$$\binom{n+k-1}{k} = \frac{n^{\overline{k}}}{k!} = \frac{(n+k-1)^{\overline{k}}}{k!}.$$

## Beweis:

Sei o.B.d.A.  $N = \{1, \dots, n\}$ . Betrachte eine Multimenge  $\{a_1, a_2, \dots, a_k\}$  der Kardinalität  $k$ . Sei o.B.d.A.  $a_1 \leq a_2 \leq \dots \leq a_k$ . Definiere die Ersetzung  $f$ :

$$f : \begin{array}{ccc} a_1 & a_1 & \geq 1 \\ a_2 & a_2 + 1 & \\ a_3 & a_3 + 2 & \\ \vdots & \vdots & \\ a_k & a_k + k - 1 & \leq n + k - 1 \end{array}$$

Das Ergebnis unter  $f$  ist eine Menge  $\subseteq [n + k - 1]$ . Die Anzahl der Möglichkeiten auf der rechten Seite beträgt  $\binom{n+k-1}{k}$ , und die durch  $f$  gegebene Zuordnung ist offensichtlich bijektiv.  $\square$

## Andere Beweisvariante:

### Beweis:

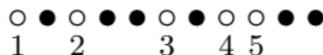
$$\begin{array}{ccccccccccc} 0 & 1 & & 0 & 2 & & & & & 1 & & 0 \\ \circ & \circ & \bullet & \circ & \circ & \bullet & \bullet & \circ & \dots & \circ & \bullet & \circ \\ 1 & 2 & & 3 & 4 & & & & & n-1 & & n \end{array}$$

Von  $n + k$  Kugeln werden  $k$  schwarz gefärbt; die erste darf nicht schwarz gefärbt werden. Also bleiben  $n$  weiße Kugeln übrig, darunter die erste.

Jede dieser weißen Kugeln zählt nun als sooft ausgewählt, wie unmittelbar rechts davon schwarze Kugeln stehen. Es werden also aus  $n$  weißen Kugeln  $k$  ausgewählt (mit Wiederholung).  $\square$

## Beispiel 168

Darstellung zu obigem Beispiel:



Zugehörige Multimenge:

$$\{1, 2, 2, 3, 5, 5\}$$

## 4.4 Anzahl von Abbildungen

Betrachte Funktionen von  $N$  (Urbildraum) nach  $R$  (Bildraum),  
 $|N| = n, |R| = r$  mit  $n, r \in \mathbb{N}_0$ .

Die Anzahl beliebiger Abbildungen  $N \rightarrow R$  ist

$$r^n .$$

Die Anzahl der injektiven Abbildungen  $N \rightarrow R$  ist

$$r^{\underline{n}} .$$

Die Anzahl der surjektiven Abbildungen  $N \rightarrow R$  („geordnete  
 $r$ -Mengenpartitionen von  $N$ “) ist

$$r! \cdot S_{n,r} .$$

Die Gesamtzahl der Abbildungen  $N \rightarrow R$  ist

$$\begin{aligned} &= r^n = \sum_{A \subseteq R} \# \text{ der surjektiven Abbildungen } N \rightarrow A \\ &= \sum_{k=0}^r \sum_{\substack{A \subseteq R \\ |A|=k}} \# \text{ der surjektiven Abbildungen } N \rightarrow A \\ &= \sum_{k=0}^r \left( \binom{r}{k} \cdot k! \cdot S_{n,k} \right) = \sum_{k=0}^r S_{n,k} \cdot r^{\underline{k}} . \end{aligned}$$

## 4.5 Zusammenfassende Darstellung

$N$  seien  $n$  Tennisbälle,  $R$  seien  $r$  Schachteln: „balls into bins“

	beliebig	injektiv	surjektiv	bijektiv ( $n = r$ )
$N$ unterscheidbar $R$ unterscheidbar	$r^n$	$r^{\underline{n}}$	$r! \cdot S_{n,r}$	$r! = n!$
$N$ nicht unterscheidbar $R$ unterscheidbar	$\frac{r^{\bar{n}}}{n!}$	$\binom{r}{n}$	$\binom{n-1}{r-1}$	1
$N$ unterscheidbar $R$ nicht unterscheidbar	$\sum_{k=1}^r S_{n,k}$	1 oder 0	$S_{n,r}$	1
$N$ nicht unterscheidbar $R$ nicht unterscheidbar	$\sum_{k=1}^r P_{n,k}$	1 oder 0	$P_{n,r}$	1

## 4.6 Abzählen von Permutationen

### 4.6.1 Stirling-Zahlen der ersten Art

#### Definition 169

Die **Stirling-Zahl der ersten Art**

$$s_{n,k}$$

gibt die Anzahl der Permutationen  $\in S_n$  mit genau  $k$  Zyklen an.

#### Einfache Beobachtungen:

- 1 für alle  $n \in \mathbb{N}$ :

$$\sum_{k=1}^n s_{n,k} = n!$$

2

$$s_{n,1} = (n-1)! = \frac{n!}{n}$$

3

$$s_{n,n-1} = \binom{n}{2}$$

4

$$s_{n,n} = 1$$

5

$$s_{n,k} = 0 \text{ für } k > n \geq 0$$

Man setzt weiterhin:

$$s_{0,0} := 1 \quad s_{n,0} := 0 \text{ für } n \in \mathbb{N} \quad s_{n,k} = 0 \text{ für } n \in \mathbb{N}_0, k < 0.$$

## 4.6.2 Typ einer Permutation

### Definition 170

Sei  $\pi$  eine Permutation von  $n$  Objekten,  $b_i(\pi)$  die Anzahl der Zyklen von  $\pi$  der Länge  $i$  ( $i = 1, \dots, n$ ) und  $b(\pi)$  die Anzahl der Zyklen von  $\pi$ , also

$$\sum_{i=1}^n i \cdot b_i(\pi) = n \quad \text{und} \quad \sum_{i=1}^n b_i(\pi) = b(\pi).$$

Dann heißt der formale Ausdruck

$$1^{b_1(\pi)} 2^{b_2(\pi)} 3^{b_3(\pi)} \dots n^{b_n(\pi)}$$

der **Typ von  $\pi$**  (Potenzen mit Exponent 0 werden gewöhnlich nicht geschrieben).

## Beispiel 171

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 6 & 2 & 7 & 1 & 8 & 3 \end{pmatrix}$$

$$= (4\ 5\ 6\ 2\ 7\ 1\ 8\ 3)$$

*als Funktionswerte*

$$= (1\ 4\ 2\ 5\ 7\ 8\ 3\ 6)$$

*in Zykelschreibweise*

Typ:  $8^1$

## Beispiel 172

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 7 & 1 & 6 & 5 & 3 & 8 \end{pmatrix}$$

$$= (2\ 4\ 7\ 1\ 6\ 5\ 3\ 8)$$

$$= (1\ 2\ 4)\ (3\ 7)\ (5\ 6)\ (8)$$

Typ:  $1^1\ 2^2\ 3^1$

## Lemma 173

*Es gibt*

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

*verschiedene Typen von Permutationen in  $S_n$ .*

Beweis:

Klar. □

## Lemma 174

Es gibt

$$\frac{n!}{b_1! \cdot b_2! \cdot \dots \cdot b_n! \cdot 1^{b_1} \cdot 2^{b_2} \cdot \dots \cdot n^{b_n}}$$

verschiedene Permutationen in  $S_n$  vom Typ  $1^{b_1} \cdot 2^{b_2} \cdot \dots \cdot n^{b_n}$  (Beachte:  $0! = 1$ ). Insbesondere gilt:

$$s_{n,k} = \sum_{\substack{(b_1, \dots, b_n) \in \mathbb{N}_0^n \\ \sum b_i = k \\ \sum i \cdot b_i = n}} \frac{n!}{b_1! \cdot b_2! \cdot \dots \cdot b_n! \cdot 1^{b_1} \cdot 2^{b_2} \cdot \dots \cdot n^{b_n}}$$

und

$$n! = \sum_{\substack{(b_1, \dots, b_n) \in \mathbb{N}_0^n \\ \sum_{i=1}^n i \cdot b_i = n}} \frac{n!}{b_1! \cdot b_2! \cdot \dots \cdot b_n! \cdot 1^{b_1} \cdot 2^{b_2} \cdot \dots \cdot n^{b_n}}.$$

## Beweis:

Sei Typ  $1^{b_1} 2^{b_2} \dots n^{b_n}$  gegeben:

$$\overbrace{(\_)(\_)\dots(\_)}^{b_1} \overbrace{(\_)(\_)\dots(\_)}^{b_2} \dots \overbrace{(\_)\dots(\_)}^{b_n (\leq 1)}$$

Insgesamt gibt es  $n$  freie Plätze. Ersetze die freien Plätze durch Permutationen aus  $S_n$ . Dafür gibt es  $n!$  Möglichkeiten.

Nun muss beachtet werden, dass

- die Zyklen der Länge  $i$  beliebig vertauschbar sind, und
- ein Zyklus der Länge  $i$  in sich  $i$ -mal zyklisch geshiftet werden kann, ohne die Permutation zu ändern.

Damit ergeben sich für die Zyklen der Länge  $i$  oben genau  $b_i! \cdot i^{b_i}$  verschiedene Anordnungen, so dass insgesamt alle Permutationen mit dem angegebenen Faktor **überzählt** werden. □

## Beispiel 175

$$s_{5,1} = \frac{5!}{1! \cdot 5^1} = 4! = 24$$

$$s_{5,2} = \sum_{\text{Typ}=1^1 4^1} 1 + \sum_{\text{Typ}=2^1 3^1} 1 = \frac{5!}{1! \cdot 1! \cdot 1^1 \cdot 4^1} + \frac{5!}{1! \cdot 1! \cdot 2^1 \cdot 3^1} = 50$$

$$s_{5,3} = \sum_{\text{Typ}=1^2 3^1} 1 + \sum_{\text{Typ}=1^1 2^2} 1 = \frac{5!}{2! \cdot 1! \cdot 1^2 \cdot 3^1} + \frac{5!}{1! \cdot 2! \cdot 1^1 \cdot 2^2} = 35$$

## 4.7 Abzählkoeffizienten

### 4.7.1 Binomialkoeffizienten

Wir hatten bereits:

1

$$\binom{n}{k} = \frac{n^k}{k!} \quad \forall n \geq k > 0$$

$$\binom{n}{0} = 1 \quad \forall n > 0$$

2

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \binom{n}{n-k} \quad \forall n \geq k > 0$$

3

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \quad \forall n \geq k > 0$$

Weiter definiert man:

1

$$n^{\underline{0}} := n^{\overline{0}} := 0! := 1 \quad \forall n \in \mathbb{C}$$

2

$$\binom{0}{0} := 1$$

3

$$x^{\underline{k}} = x \cdot (x - 1) \cdot \dots \cdot (x - k + 1)$$

$$x^{\overline{k}} = x \cdot (x + 1) \cdot \dots \cdot (x + k - 1) \quad \forall x \in \mathbb{C}, k \geq 0$$

4

$$\binom{x}{k} = \begin{cases} \frac{x^{\underline{k}}}{k!} & k \geq 0 \\ 0 & \text{sonst} \end{cases}$$

## Lemma 176

$\binom{x}{k}$  ist, für  $k \geq 0$ , ein Polynom in  $x$  vom Grad  $k$ , und es gilt auch für alle  $k \in \mathbb{Z}$  und  $x \in \mathbb{C}$

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

### Beweis:

Da für  $k \leq 0$  per Definition der Binomialkoeffizienten Gleichheit gilt, betrachten wir nur  $k > 0$ . Es ist dann

$$\binom{x}{k} = \binom{x-1}{k-1} + \binom{x-1}{k}$$

ein Polynom in  $x$  vom Grad  $\leq k$ . Für alle  $x \in \mathbb{N}$  ist dieses Polynom gleich 0. Ein Polynom einer Variablen mit unendlich vielen Nullstellen ist aber sicher identisch 0 (Fundamentalsatz der Algebra (Satz 136)).

## Beweis (Forts.):

Eine weitere Möglichkeit, den Beweis zu führen:

$$\begin{aligned}x^k &= x \cdot (x - 1)^{k-1} = (k + x - k)(x - 1)^{k-1} \\ &= k \cdot (x - 1)^{k-1} + (x - k)(x - 1)^{k-1} \\ &= k \cdot (x - 1)^{k-1} + (x - 1)^k\end{aligned}$$

Also gilt

$$\binom{x}{k} = \frac{x^k}{k!} = \frac{(x - 1)^{k-1}}{(k - 1)!} + \frac{(x - 1)^k}{k!} = \binom{x - 1}{k - 1} + \binom{x - 1}{k}.$$



# Das Pascalsche Dreieck

$\binom{n}{k}$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1	0	
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

benannt nach **Blaise Pascal** (1623–1662).

### Beobachtung:

Die Zeilensumme in der  $n$ -ten Zeile ist  $2^n$ .

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

## Lemma 177

Für die Spaltensumme bis zur  $n$ -ten Zeile gilt:

$$\sum_{m=0}^n \binom{m}{k} = \binom{n+1}{k+1} \quad \forall n, k \geq 0$$

### Beweis:

(Vollständige Induktion über  $n$ )

Induktionsanfang:  $n = 0$

$$\begin{aligned} \sum_{m=0}^0 \binom{0}{k} &= \binom{0}{k} = \begin{cases} 1 & \text{für } k = 0 \\ 0 & \text{sonst} \end{cases} \\ &\stackrel{!}{=} \binom{0+1}{k+1} = \binom{1}{k+1} = \begin{cases} 1 & \text{für } k = 0 \\ 0 & \text{sonst} \end{cases} \end{aligned}$$

## Beweis (Forts.):

Induktionsschluss:  $n \mapsto n + 1$ :

$$\begin{aligned}\sum_{m=0}^{n+1} \binom{m}{k} &= \sum_{m=0}^n \binom{m}{k} + \binom{n+1}{k} \\ &= \binom{n+1}{k+1} + \binom{n+1}{k} = \binom{n+2}{k+1}\end{aligned}$$



## Beispiel 178

$\binom{n}{k}$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

$$k = 2, n = 5 :$$

$$\sum_{m=0}^5 \binom{m}{2} = \binom{6}{3}$$

## Lemma 179

Für die Diagonalsumme gilt:

$$\sum_{k=0}^m \binom{n+k}{k} = \binom{m+n+1}{m} \quad \forall m \in \mathbb{N}, n \in \mathbb{C}$$

**Beweis:**

(Vollständige Induktion über  $m$ )

Induktionsanfang:  $m = 0$ :

$$\begin{aligned} \sum_{k=0}^0 \binom{n+k}{k} &= \binom{n}{0} = 1 \\ &\stackrel{!}{=} \binom{0+n+1}{0} = \binom{n+1}{0} = 1 \end{aligned}$$

## Beweis (Forts.):

Induktionsschluss  $m \mapsto m + 1$ :

$$\begin{aligned}\sum_{k=0}^{m+1} \binom{n+k}{k} &= \sum_{k=0}^m \binom{n+k}{k} + \binom{m+n+1}{m+1} \\ &= \binom{m+n+1}{m} + \binom{m+n+1}{m+1} \\ &= \binom{m+n+2}{m+1}\end{aligned}$$



## Beispiel 180

$\binom{n}{k}$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

$$m = 3, n = 2 :$$

$$\sum_{k=0}^3 \binom{2+k}{k} = \binom{6}{3}$$

## Beobachtungen:

- Negation

$$(-x)^{\bar{k}} = (-1)^k \cdot x^{\bar{k}}$$

- Binomialsatz

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} \cdot x^k \cdot y^{n-k}$$

## Spezialfälle des Binomialsatzes:

①  $x = y = 1$ :

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

(Beweis zur Zeilensumme!)

②  $y = 1$ :

$$(x + 1)^n = \sum_{k=0}^n \binom{n}{k} \cdot x^k$$

③  $x = -1, y = 1$ :

$$0 = (-1 + 1)^n = \sum_{k=0}^n \binom{n}{k} \cdot (-1)^k$$
$$\Rightarrow \sum_{\substack{k=0 \\ k \text{ ungerade}}}^n \binom{n}{k} = \sum_{\substack{k=0 \\ k \text{ gerade}}}^n \binom{n}{k} = 2^{n-1}$$

## Satz 181 (Vandermonde-Identität)

$$\binom{x+y}{n} = \sum_{k=0}^n \binom{x}{k} \cdot \binom{y}{n-k} \quad n \in \mathbb{N}_0, x, y \in \mathbb{C}$$

### Beweis:

Seien zunächst  $x, y \in \mathbb{N}$ .

Zur Verdeutlichung sei z. B.  $x$  die Anzahl der Wahlmänner der Demokraten und  $y$  die Anzahl der Wahlmänner der Republikaner.

$\binom{x+y}{n}$  ist dann die Anzahl der Möglichkeiten, aus  $(x+y)$  Wahlmännern  $n$  auszuwählen. Dementsprechend ist  $\binom{x}{k}$  die Anzahl der Möglichkeiten, aus  $x$  Demokraten  $k$  auszuwählen, und  $\binom{y}{n-k}$  die Anzahl der Möglichkeiten, aus  $y$  Republikanern  $(n-k)$  auszuwählen.

Damit überlegt man sich leicht, dass die Formel für  $x, y \in \mathbb{N}$  gilt.

## Beweis (Forts.):

Erweiterung auf  $x, y \in \mathbb{C}$ : Setze  $y = \text{const.}$  Damit stehen links und rechts ein Polynom  $n$ -ten Grades in  $x$ :

$$p_l(x) \stackrel{!}{=} p_r(x)$$

Für  $x \in \mathbb{Z}$  gilt:

$$p_l(x) - p_r(x) = 0$$

Dieses Polynom hat unendlich viele Nullstellen. Nach dem Fundamentalsatz der Algebra ist dann

$$p_l(x) - p_r(x) \equiv 0$$

Das heißt,  $p_l(x)$  und  $p_r(x)$  sind identisch. □

## 4.7.2 Stirling-Zahlen der ersten Art

### Lemma 182

*Mit den zusätzlichen Festlegungen*

$$s_{0,0} = 1$$

*und*

$$s_{n,k} = 0 \quad k \leq 0, n > 0$$

*gilt:*

$$s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k} \quad \forall n, k > 0.$$

## Beweis:

Für Permutationen auf  $\{1, \dots, n\}$  mit  $k$  Zyklen gilt:

**Entweder:**  $n$  bildet einen Zyklus der Länge 1:

$$\pi = \underbrace{(* \cdots *) (* \cdots *) \cdots (n)}_{\substack{\text{Permutation auf} \\ \{1, \dots, n-1\} \\ \text{mit } (k-1) \text{ Zyklen}}}$$

Dafür gibt es  $s_{n-1, k-1}$  Möglichkeiten.

## Beweis (Forts.):

**Oder:**  $n$  ist in einem Zyklus der Länge  $\geq 2$  enthalten.

Streiche  $n$  aus dieser Permutation:

$$\pi' = \underbrace{(*\downarrow \dots *\downarrow)(*\downarrow \dots *\downarrow) \dots (*\downarrow \dots *\downarrow)}_{\substack{\text{Permutation auf} \\ \{1, \dots, n-1\} \\ \text{mit } k \text{ Zyklen}}}$$

Die  $\downarrow$  bezeichnen Stellen, an denen  $n$  gestrichen worden sein könnte (immer hinter der jeweiligen Zahl, da  $(\downarrow * \dots *)$  zyklisch mit  $(* \dots * \downarrow)$  identisch ist). Dafür gibt es  $n - 1$  mögliche Stellen.

Damit ergeben sich hier  $(n - 1)s_{n-1,k}$  Möglichkeiten.

Die beiden Fälle sind disjunkt, also können die Möglichkeiten addiert werden. □

# Stirling-Dreieck der ersten Art

$s_{n,k}$	0	1	2	3	4	5	6
0	1						
1	0	1					
2	0	1	1				
3	0	2	3	1			
4	0	6	11	6	1		
5	0	24	50	35	10	1	
6	0	120	274	225	85	15	1

$$s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k} \quad \forall n, k > 0$$

Es gilt:

$$(\forall n \in \mathbb{N}) \left[ x^n = \sum_{k=0}^n (-1)^{n-k} \cdot s_{n,k} \cdot x^k \right].$$

Beweis:

(Vollständige Induktion)

Induktionsanfang:  $n = 0$

$$x^0 = 1 \stackrel{!}{=} \sum_{k=0}^0 (-1)^{0-k} s_{0,k} \cdot x^k = s_{0,0} = 1$$

## Beweis (Forts.):

Induktionsschluss:  $n \mapsto n + 1$

$$\begin{aligned}x^{n+1} &= (x - n) \cdot x^n \\ &\stackrel{\text{IA}}{=} (x - n) \cdot \sum_{k=0}^n (-1)^{n-k} \cdot s_{n,k} \cdot x^k \\ &= \sum_{k=0}^n (-1)^{n-k} \cdot s_{n,k} \cdot x^{k+1} + \sum_{k=0}^n (-1)^{n-k+1} \cdot n \cdot s_{n,k} \cdot x^k \\ &= \sum_{k=0}^{n+1} (-1)^{n-k+1} \cdot (s_{n,k-1} + n \cdot s_{n,k}) \cdot x^k \\ &= \sum_{k=0}^{n+1} (-1)^{n+1-k} \cdot s_{n+1,k} \cdot x^k\end{aligned}$$



### 4.7.3 Stirling-Zahlen der zweiten Art

#### Lemma 183

Es gilt:

$$\forall n, k \in \mathbb{N}_0 \quad S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k} .$$

#### Beweis:

Sei  $N = \{1, \dots, n\}$ .

In einer Partition von  $N$  in  $k$  Teilmengen gilt

**entweder:**  $\{n\}$  tritt als solches in der Partition auf:

$$\underbrace{N_1 \uplus N_2 \uplus \dots \uplus N_{k-1}}_{\substack{\text{Partition von} \\ \{1, \dots, n-1\} \\ \text{in } (k-1) \text{ Teilmengen}}} \uplus \{n\}$$

$\Rightarrow S_{n-1,k-1}$  Möglichkeiten

Beweis (Forts.):

oder:  $n$  ist in einem  $N_i$  mit  $\geq 2$  Elementen enthalten:

$$N_1 \uplus N_2 \uplus \dots \uplus N_k$$

Streiche  $n$ . Betrachte:

$$\underbrace{N_1 \setminus \{n\} \uplus N_2 \setminus \{n\} \uplus \dots \uplus N_k \setminus \{n\}}_{\text{Partition von } \{1, \dots, n-1\} \text{ in } k \text{ Klassen}}$$

$\Rightarrow S_{n-1,k}$  Möglichkeiten.  $n$  kann an einer von  $k$  Stellen entfernt worden sein:

$\Rightarrow$  insgesamt  $k \cdot S_{n-1,k}$  Möglichkeiten in diesem Fall. □

# Stirling-Dreieck der zweiten Art

$S_{n,k}$	0	1	2	3	4	5	6
0	1						
1	0	1					
2	0	1	1				
3	0	1	3	1			
4	0	1	7	6	1		
5	0	1	15	25	10	1	
6	0	1	31	90	65	15	1

$$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$$

## Einige Eigenschaften:

$$S_{n,1} = 1$$

$$S_{n,2} = \frac{2^n - 2}{2} = 2^{n-1} - 1$$

$$S_{n,n-1} = \binom{n}{2}$$

$$S_{n,n} = 1$$

**Bemerkung:**

Es gibt auch andere Notationen für die Stirling-Zahlen zweiter Art, z. B.: Es gibt auch andere Notationen für die Stirling-Zahlen zweiter Art, z. B.:

$$S_{n,k} = \left[ \begin{matrix} n \\ k \end{matrix} \right] = \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$$

z. B. in Graham, Knuth, Pataschnik: Concrete Mathematics

## 4.7.4 Auflistung von Permutationen

### Definition 184

Seien  $\pi = (\pi_1 \pi_2 \cdots \pi_n)$  und  $\sigma = (\sigma_1 \sigma_2 \cdots \sigma_n)$  zwei Permutationen aus  $S_n$ ,  $\pi \neq \sigma$ , als Wertevektor geschrieben (d.h.  $\pi_i = \pi(i)$  etc.). Dann heißt  $\pi$  **lexikographisch kleiner als**  $\sigma$ , geschrieben  $\pi < \sigma$ , genau dann, wenn

$$(\exists 1 \leq k \leq n)(\forall 1 \leq i < k) \left[ (\pi_i = \sigma_i) \wedge (\pi_k < \sigma_k) \right].$$

### Beispiel 185

$n = 3, N = \{1, 2, 3\}$ :

$$(1 \ 2 \ 3) < (1 \ 3 \ 2) < (2 \ 1 \ 3) < (2 \ 3 \ 1) < (3 \ 1 \ 2) < (3 \ 2 \ 1)$$

## Algorithmus zur Auflistung von $S_n$ in lexikographischer Ordnung:

Gegeben:  $N = \{1, 2, \dots, n\}$

```
appendlexlist(string praefix, set N)
  if N={a} then print(praefix  $\circ$  a)
  else
    for  $k \in N$  in aufsteigender Reihenfolge do
      appendlexlist(praefix  $\circ$   $k$ ,  $N \setminus \{k\}$ )
    od
  fi
end
```

Aufruf:  $\text{appendlexlist}(\lambda, N)$

## Beispiel 186

$n = 3, N = \{1, 2, 3\}$ :

$$(1\ 2\ 3) < (1\ 3\ 2) < (2\ 1\ 3) < (2\ 3\ 1) < (3\ 1\ 2) < (3\ 2\ 1)$$

### 4.7.5 Auflistung von Teilmengen

Sei  $N = \{0, 1, 2, \dots, n - 1\}$ ,  $|N| = n$ .

#### Definition 187

Seien  $A, B \subseteq N$ ,  $A \neq B$ . Dann heißt  $A$  **lexikographisch kleiner als**  $B$ , geschrieben  $A < B$ , wenn

$$\max\{A \Delta B\} \in B$$

#### Beispiel 188

$N = \{0, 1, 2\}$ ;

$$2^N = \{\emptyset, \{0\}, \{1\}, \{1, 0\}, \{2\}, \{2, 0\}, \{2, 1\}, \{2, 1, 0\}\}$$

## Algorithmus zur Auflistung aller Teilmengen in lexikographischer Ordnung:

- 1  $N = \{0, \dots, n - 1\}$ . Zähle die natürlichen Zahlen von 0 bis  $2^n - 1$  in Binärschreibweise auf, fülle jede Binärzahl dabei mit führenden Nullen auf  $n$  Stellen auf.
- 2 Sei  $a = a_{n-1}a_{n-2} \dots a_0$  ein Element der obigen Folge. Dann entspricht  $a$  die Teilmenge

$$N_a = N_{a_{n-1}a_{n-2} \dots a_0} = \left\{ k \in N : 0 \leq k \leq n - 1 \wedge a_k = 1 \right\}$$

## Algorithmus zur Auflistung aller Teilmengen in lexikographischer Ordnung, zweite Variante:

Sei  $n \in \mathbb{N}$ .

```
appendlexlist(set praefix, nat n)
  for k = 0, 1 do
    if k = 1 then praefix:=praefix  $\cup$  {n} fi
    if n = 0 then print(praefix)
    else
      appendlexlist(praefix, n - 1)
    fi
  od
end
```

Aufruf:  $\text{appendlexlist}(\emptyset, n - 1)$

## 4.7.6 Gray-Codes

### Definition 189

Ein **Gray-Code**  $GC(n)$ ,  $n \in \mathbb{N}$ , ist eine Permutation  $(g_0, \dots, g_{2^n-1})$  der Wörter in  $\{0, 1\}^n$ , so dass sich zwei aufeinanderfolgende Wörter  $g_i$  und  $g_{i+1}$ , für alle  $i = 0, \dots, 2^n - 1$ , in genau einer Position unterscheiden.

$GC(n)$  heißt **zyklischer Gray-Code**, falls die Bedingung auch für  $g_{2^n-1}$  und  $g_0$  gilt.

$$GC(1) := (g_{1,0}, g_{1,1}) = (0, 1)$$

$$GC(n+1) := (0 \cdot g_{n,0}, 0 \cdot g_{n,1}, \dots, 0 \cdot g_{n,2^n-1}, \\ 1 \cdot g_{n,2^n-1}, \dots, 1 \cdot g_{n,0})$$

### Beispiel 190

$$GC(3) = (000 \ 001 \ 011 \ 010 \ 110 \ 111 \ 101 \ 100)$$

## Lemma 191

- 1  $GC(n)$  hat Länge  $2^n$ .
- 2  $\{g_{n,0}, \dots, g_{n,2^n-1}\} = \{0, 1\}^n$ .
- 3 für alle  $k$  unterscheidet sich  $g_{n,k}$  von  $g_{n,(k+1) \bmod 2^n}$  in genau **einem Bit**.

Beweis:

Folgt direkt aus der Definition. □

## 4.8 Summation und Differenzenoperator

### 4.8.1 Direkte Methoden

#### 1. Indextransformation:

Sei  $i \geq 0$ , dann gilt:

$$\sum_{k=m}^n a_k = \sum_{k=m}^{k=n} a_k = \sum_{k-i=m}^{k-i=n} a_{k-i} = \sum_{k=m+i}^{k=n+i} a_{k-i} = \sum_{k=m+i}^{n+i} a_{k-i}$$

## Beispiel 192

$$S_n = 0 \cdot a + 1 \cdot a + 2 \cdot a + \cdots + n \cdot a = \sum_{k=0}^n k \cdot a$$

Indextransformation:  $k \mapsto n - k$

$$S_n = \sum_{k=0}^n (n - k) \cdot a$$

## Beispiel (Forts.)

$$S_n = \sum_{k=0}^n (n - k) \cdot a$$

also:

$$\begin{aligned} S_n &= \frac{1}{2} \left( \sum_{k=0}^n k \cdot a + \sum_{k=0}^n (n - k) \cdot a \right) \\ &= \frac{n \cdot a}{2} \cdot \sum_{k=0}^n 1 \\ &= \frac{n \cdot (n + 1)}{2} \cdot a = \binom{n + 1}{2} \cdot a \end{aligned}$$

## 2. Induktion

### Beispiel 193

$$S_n = \sum_{k=1}^n (2k - 1)$$

Nach Berechnen einiger Werte

$$S_1 = 1$$

$$S_2 = 4$$

$$S_3 = 9$$

vermutet man:

$$S_n = n^2$$

## Beispiel (Forts.)

*Behauptung:*

$$S_n = n^2$$

*Beweis durch vollständige Induktion:*

*Induktionsanfang:  $n = 1$  trivial*

*Induktionsschluss:  $n \mapsto n + 1$*

$$S_{n+1} = S_n + 2 \cdot (n + 1) - 1 \stackrel{\text{IA}}{=} n^2 + 2 \cdot n + 1 = (n + 1)^2$$

## Beispiel 194

Seien  $a_1, a_2, \dots, a_n \in \mathbb{R}^+$ .

Das arithmetische Mittel  $A$  der  $a_i$ :

$$A = \frac{1}{n} \sum_{i=1}^n a_i$$

Das geometrische Mittel  $G$  der  $a_i$ :

$$G = \sqrt[n]{\prod_{i=1}^n a_i}$$

Das harmonische Mittel  $H$  der  $a_i$ :

$$\frac{1}{H} = \frac{1}{n} \sum_{i=1}^n \frac{1}{a_i}$$

Wir wollen zeigen:  $G \leq A$ .

## Beispiel (Forts.)

*Beweis durch vollständige Induktion:*

*Induktionsanfang:  $n = 1$  trivial,  $n = 2$  durch Einsetzen:*

$$\begin{aligned}(G \leq A) &\equiv \left( \sqrt{a_1 \cdot a_2} \leq \frac{a_1 + a_2}{2} \right) \\ &\equiv (4a_1 \cdot a_2 \leq (a_1 + a_2)^2) \\ &\equiv (0 \leq a_1^2 - 2a_1a_2 + a_2^2 = (a_1 - a_2)^2)\end{aligned}$$

*Induktionsschluss:*

*Wir zeigen:*

- 1  $P_n \Rightarrow P_{n-1}$
- 2  $(P_n \wedge P_2) \Rightarrow P_{2n}$

## Beispiel (Forts.)

① Sei

$$b := \frac{1}{n-1} \sum_{i=1}^{n-1} a_i.$$

Damit:

$$\begin{aligned} \left( \prod_{i=1}^{n-1} a_i \right) \cdot \sum_{i=1}^{n-1} \frac{a_i}{n-1} &= \left( \prod_{i=1}^{n-1} a_i \right) \cdot b \stackrel{P_n}{\leq} \left( \frac{1}{n} \left( b + \sum_{i=1}^{n-1} a_i \right) \right)^n \\ &= \left( \frac{1 + \frac{1}{n-1}}{n} \cdot \sum_{i=1}^{n-1} a_i \right)^n = \left( \frac{1}{n-1} \cdot \sum_{i=1}^{n-1} a_i \right)^n \\ &\Rightarrow \prod_{i=1}^{n-1} a_i \leq \left( \frac{1}{n-1} \sum_{i=1}^{n-1} a_i \right)^{n-1} \Rightarrow P_{n-1} \end{aligned}$$

## Beispiel (Forts.)

② *Es gilt:*

$$\begin{aligned}\prod_{i=1}^{2n} a_i &= \left( \prod_{i=1}^n a_i \right) \cdot \left( \prod_{i=n+1}^{2n} a_i \right) \\ &\stackrel{P_n}{\leq} \left( \sum_{i=1}^n \frac{a_i}{n} \right)^n \cdot \left( \sum_{i=n+1}^{2n} \frac{a_i}{n} \right)^n \\ &= \left( \left( \sum_{i=1}^n \frac{a_i}{n} \right) \cdot \left( \sum_{i=n+1}^{2n} \frac{a_i}{n} \right) \right)^n \\ &\stackrel{P_2}{\leq} \left( \frac{1}{2} \sum_{i=1}^{2n} \frac{a_i}{n} \right)^{2n} = \left( \frac{1}{2n} \sum_{i=1}^{2n} a_i \right)^{2n} \\ &\Rightarrow P_{2n}\end{aligned}$$



## 4.8.2 Differenzenoperator

### Definition 195

Der Operator

$$E : f \mapsto E(f)$$

mit  $E(f)(x) := f(x + 1)$  heißt **Translationsoperator**.

$$\Delta : f \mapsto \Delta(f)$$

mit  $\Delta(f)(x) := f(x + 1) - f(x)$  heißt  
**(Vorwärts-)Differenzenoperator**.

$$\nabla : f \mapsto \nabla(f)$$

mit  $\nabla(f)(x) := f(x) - f(x - 1)$  heißt  
**(Rückwärts-)Differenzenoperator**.

Mit  $I$  als dem Identitätsoperator, (also  $I(f) = f$ ) gilt damit

$$\Delta(f) = (E - I)(f)$$

$$\nabla(f) = (I - E^{-1})(f)$$

## Beispiel 196

Sei  $a \in \mathbb{N}_0$ :

$$E^a(f)(x) = \underbrace{(E \circ E \circ \dots \circ E)}_a(f)(x) = f(x + a)$$

## Beobachtungen:

Seien  $P, Q$  Operatoren  $\in \{E, I, \Delta, \nabla\}$ , sei  $\alpha \in \mathbb{R}$ .

1

$$(P + Q)(f) = P(f) + Q(f)$$

2

$$(\alpha P)(f) = \alpha \cdot P(f)$$

3

$$(QP)(f) = Q(P(f)), \text{ i. a. } (QP)(f) \neq (PQ)(f)$$

4

$$\Delta^n = (E - I)^n = \underbrace{(E - I) \dots (E - I)}_n = \sum_{k=0}^n \left( (-1)^{n-k} \binom{n}{k} E^k \right)$$

## Satz 197

Aus (4) folgt:

$$\begin{aligned}\Delta^n(f)(x) &= \left( \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} E^k \right) (f)(x) \\ &= \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(x+k) .\end{aligned}$$

Beweis:

Klar. □

Beispiel 198

$$\Delta^2(x^3) \Big|_{x=0} = \sum_{k=0}^2 (-1)^{2-k} \binom{2}{k} k^3 = 0 - 2 + 8 = 6$$

### 4.8.3 Fallende Fakultät

#### Definition 199

Sei  $n \in \mathbb{N}$ . Dann gilt:  $\frac{x^n}{x^{n+1}} = \frac{1}{x-n}$ .

Damit für  $n = -1$  „formal“:

$$x^{-1} = \frac{1}{x+1}$$

Und für  $n$  ersetzt durch  $-n$ :

$$x^{-n} = \frac{x^{-n+1}}{x+n}$$

$$x^{-n} := \frac{1}{(x+1)(x+2)\cdots(x+n)}$$

$$x^{-n} := \frac{1}{(x-1)(x-2)\cdots(x-n)}$$

## Lemma 200

Für alle  $n \in \mathbb{Z}$  gilt:

①

$$\Delta x^n = n \cdot x^{n-1}$$

②

$$\nabla x^{\bar{n}} = n \cdot x^{\overline{n-1}}$$

## Beweis:

(Wir zeigen nur 1.)

- $n > 0$ :

$$\begin{aligned}\Delta x^n &= (x+1)^n - x^n \\ &= (x+1) \cdot x^{n-1} - (x-n+1) \cdot x^{n-1} \\ &= n \cdot x^{n-1}\end{aligned}$$

- $n = 0$ :

$$\Delta x^0 = (x+1)^0 - x^0 = 0 = 0 \cdot x^{-1}$$

## Beweis (Forts.):

- $n < 0$ . Setze  $m := -n$ :

$$\begin{aligned}\Delta x^{-m} &= (x+1)^{-m} - x^{-m} \\ &= \frac{1}{(x+2)(x+3)\cdots(x+m+1)} - \frac{1}{(x+1)\cdots(x+m)} \\ &= \frac{(x+1) - (x+m+1)}{(x+1)\cdots(x+m+1)} \\ &= -m \cdot x^{-m-1}\end{aligned}$$



## 4.8.4 Diskrete Stammfunktion

### Definition 201

Sei  $f$  so, dass  $\Delta f = g$ . Dann heißt  $f$  eine **diskrete Stammfunktion** von  $g$ . Schreibweise:  $f = \sum g$ .

### Satz 202

Sei  $f$  eine diskrete Stammfunktion von  $g$ . Dann gilt:

$$\sum_{i=a}^b g(i) = f(b+1) - f(a)$$

### Beweis:

Wegen  $\Delta f = g$  gilt  $g(i) = f(i+1) - f(i)$ , also

$$\sum_{i=a}^b g(i) = \sum_{i=a}^b (f(i+1) - f(i)) = f(b+1) - f(a).$$



## Beispiel 203

$$\sum x^n = \frac{x^{n+1}}{n+1}$$

für  $n \neq -1$ .

## Beispiel 204

Sei

$$f(x) := \sum x^{-1}.$$

Dann ist

$$f(x+1) - f(x) = x^{-1} = \frac{1}{x+1}$$

$$f(x) = \frac{1}{x} + f(x-1) = \dots = \frac{1}{x} + \frac{1}{x-1} + \dots + \frac{1}{1} + f(0)$$

Wir setzen o. B. d. A.  $f(0) = 0$ , damit

$$f(x) = H_x$$

(harmonische Reihe).

## Beispiel 205

Es ist  $\Delta a^x = a^{x+1} - a^x = (a - 1) \cdot a^x$ .

$$\Delta \frac{a^x}{(a - 1)} = a^x,$$

bzw.

$$\sum a^x = \frac{a^x}{(a - 1)} + C$$

## Beispiel 206

Was ist  $\sum_{k=0}^n k^2$ ? Es gilt:

$$x^2 = x^2 + x^1.$$

Also:

$$\begin{aligned}\sum_{k=0}^n k^2 &= \left( \sum x^2 + \sum x^1 \right) \Big|_{x=0}^{n+1} \\ &= \left( \frac{x^3}{3} + \frac{x^2}{2} \right) \Big|_{x=0}^{n+1} \\ &= \frac{(n+1) \cdot n \cdot (n-1)}{3} + \frac{(n+1) \cdot n}{2} \\ &= \frac{n \cdot (n + \frac{1}{2})(n+1)}{3}.\end{aligned}$$

## Beispiel 207

Es ist

$$x^m = \sum_{k=0}^m S_{m,k} \cdot x^k,$$

wie wir in [4.4](#) gesehen haben.

## Beispiel (Forts.)

Also:

$$\begin{aligned}\sum_{k=0}^n k^m &= \left( \sum x^m \right) \Big|_{x=0}^{n+1} \\ &= \left( \sum_{k=0}^m S_{m,k} \cdot x^k \right) \Big|_{x=0}^{n+1} \\ &= \sum_{k=0}^m S_{m,k} \cdot \left( \sum x^k \right) \Big|_{x=0}^{n+1} \\ &= \sum_{k=0}^m S_{m,k} \cdot \left( \frac{x^{k+1}}{k+1} \right) \Big|_{x=0}^{n+1} \\ &= \sum_{k=0}^m \frac{S_{m,k}}{k+1} (n+1)^{k+1}.\end{aligned}$$

*Es ergibt sich ein Polynom in  $n$  vom Grad  $m + 1$ .*

## Lemma 208 (Partielle Summation)

Es gilt:

$$\sum (f \cdot \Delta g) = f \cdot g - \sum ((Eg) \cdot \Delta f) .$$

Beweis:

$$\begin{aligned} \Delta(f \cdot g)(x) &= (f \cdot g)(x+1) - (f \cdot g)(x) \\ &= f(x+1) \cdot g(x+1) - f(x) \cdot g(x) \\ &= f(x+1) \cdot g(x+1) \\ &\quad \underbrace{-f(x) \cdot g(x+1) + f(x) \cdot g(x+1)}_{=0} - f(x) \cdot g(x) \\ &= g(x+1) \cdot (\Delta f)(x) + f(x) \cdot (\Delta g)(x) \\ &= (Eg)(x) \cdot (\Delta f)(x) + f(x) \cdot (\Delta g)(x) . \end{aligned}$$

□

## Bemerkung zur Notation:

Bei der Darstellung

$$\sum (f \cdot \Delta g) = f \cdot g - \sum ((Eg) \cdot \Delta f)$$

ist zu beachten, dass die diskrete Stammfunktion nur bis auf additive Konstanten bestimmt ist, links und rechts also eigentlich Klassen von Funktionen stehen (wie bei den Landau-Symbolen).

## Beispiel 209

Berechne

$$\sum_{k=1}^n \binom{k}{m} \cdot H_k$$

für  $m \geq 0$ . Es gilt:

$$\begin{aligned} \Delta \binom{x}{m+1} &= \binom{x+1}{m+1} - \binom{x}{m+1} \\ &= \binom{x}{m+1} + \binom{x}{m} - \binom{x}{m+1} = \binom{x}{m}. \end{aligned}$$

Partielle Summation mit  $f(x) = H_x$ ,  $\Delta g = \binom{x}{m}$  ergibt:

## Beispiel

$$\begin{aligned}\sum_{k=1}^n \binom{k}{m} \cdot H_k &= \left( \sum \binom{x}{m} \cdot H_x \right) \Big|_{x=1}^{n+1} \\ &= \left( H_x \cdot \binom{x}{m+1} \right) \Big|_{x=1}^{n+1} - \left( \sum \binom{x+1}{m+1} \cdot \frac{1}{x+1} \right) \Big|_{x=1}^{n+1} \\ &= \left( H_x \cdot \binom{x}{m+1} \right) \Big|_{x=1}^{n+1} - \left( \frac{1}{m+1} \cdot \sum \binom{x}{m} \right) \Big|_{x=1}^{n+1} \\ &= \left( H_x \cdot \binom{x}{m+1} \right) \Big|_{x=1}^{n+1} - \frac{1}{m+1} \cdot \binom{x}{m+1} \Big|_{x=1}^{n+1} \\ &= \binom{n+1}{m+1} \cdot H_{n+1} - \binom{1}{m+1} \cdot H_1 \\ &\quad - \left( \frac{1}{m+1} \binom{n+1}{m+1} - \frac{1}{m+1} \binom{1}{m+1} \right) \\ &= \binom{n+1}{m+1} \left( H_{n+1} - \frac{1}{m+1} \right) + 0.\end{aligned}$$

## Lemma 210 (Newton-Darstellung von Polynomen)

Sei  $f(x)$  ein Polynom vom Grad  $n$ . Dann gilt:

$$f(x) = \sum_{k=0}^n \frac{\Delta^k f(0)}{k!} \cdot x^k = \sum_{k=0}^n \Delta^k f(0) \binom{x}{k}.$$

**Bemerkung:** Die Newton-Darstellung entspricht offensichtlich der **Taylorreihenentwicklung** im differenzierbaren Fall.

## Beweis:

$f(x)$  kann eindeutig in der Form

$$f(x) = \sum_{k=0}^n b_k \cdot x^k$$

geschrieben werden ( $x^k$  ist Basis!). Damit ist nach Lemma 200 (1)

$$\Delta^i f(x) = \sum_{k=0}^n b_k \cdot k^i \cdot x^{k-i}.$$

Also gilt, dass

$$\Delta^i f(0) = b_i \cdot i! \quad \text{bzw.} \quad b_k = \frac{\Delta^k f(0)}{k!}.$$



## Beispiel 211

Es ist

$$x^n = \sum_{i=0}^n S_{n,i} \cdot x^i .$$

Also gilt auch

$$\begin{aligned} k! \cdot S_{n,k} &= \Delta^k x^n \Big|_{x=0} = (E - I)^k x^n \Big|_{x=0} \\ &= \left( \sum_{i=0}^k (-1)^{k-i} \binom{k}{i} E^i \right) x^n \Big|_{x=0} = \sum_{i=0}^k (-1)^{k-i} \cdot \binom{k}{i} \cdot i^n , \end{aligned}$$

und damit auch

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

## 4.9 Inversion

### 4.9.1 Basisfolgen

#### Definition 212

Eine Folge  $(p_0(x), p_1(x), \dots)$  von Polynomen  $p_i(x)$  heißt **Basisfolge**, falls

$$\deg(p_i) = i \quad \text{für alle } i.$$

Bemerkung:  $p_0 \neq 0$ , da wir für  $p(x) \equiv 0$  festlegen:  $\deg(p) = -1$ .

**Beobachtung:**  $(p_i(x))_{i \geq 0}$  sei eine Basisfolge. Dann kann jedes Polynom  $f(x) \in \mathbb{R}[x]$  vom Grad  $n$  eindeutig dargestellt werden als

$$f(x) = \sum_{i=0}^n f_i \cdot p_i(x)$$

mit  $f_i \in \mathbb{R}$ .

**Beweis:**

Mit Koeffizientenvergleich und vollständiger Induktion. □

## 4.9.2 Zusammenhangskoeffizienten

Seien  $(p_i(x))_{i \geq 0}$  und  $(q_i(x))_{i \geq 0}$  Basisfolgen. Dann gibt es eindeutig bestimmte Zahlen  $a_{n,k}$  und  $b_{n,k} \in \mathbb{R}$  (die sogenannten **Zusammenhangskoeffizienten**), so dass für alle  $n, k \in \mathbb{N}_0$  gilt:

1

$$q_n(x) = \sum_{k=0}^n a_{n,k} \cdot p_k(x)$$

2

$$p_n(x) = \sum_{k=0}^n b_{n,k} \cdot q_k(x)$$

### Lemma 213

Seien die  $a_{n,k}$ ,  $b_{n,k}$  wie oben,  $A = (a_{ij})_{0 \leq i, j \leq n}$  und  $B = (b_{ij})_{0 \leq i, j \leq n}$ , dann ist

$$AB = I$$

( $I$  ist die  $n + 1$ -dimensionale Einheitsmatrix.)

Beweis:

Klar. □

## Satz 214

Seien  $a_{n,k}$  und  $b_{n,k}$ ,  $n, k \in \mathbb{N}_0$ , die zu zwei Basisfolgen gehörenden Zusammenhangskoeffizienten. Dann gilt:

$$(\forall n \in \mathbb{N}_0) \left[ v_n = \sum_{k=0}^n a_{n,k} \cdot u_k \right] \iff (\forall n \in \mathbb{N}_0) \left[ u_n = \sum_{k=0}^n b_{n,k} \cdot v_k \right]$$

Beweis:

In Matrixschreibweise gilt:

$$v = (v_0, \dots, v_n)^T = A \cdot u \iff u = B \cdot v$$

Klar, da  $A = B^{-1}$ .



### 4.9.3 Die Binomialinversion

Der Binomialsatz ergibt:

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

Betrachte die beiden Basisfolgen

$$(v_k)_{k \geq 0} := (x^k)_{k \geq 0} \text{ und } (u_k)_{k \geq 0} := ((x-1)^k)_{k \geq 0}.$$

Satz 214 liefert:

$$(\forall n \in \mathbb{N}_0) \left[ v_n = \sum_{k=0}^n \binom{n}{k} \cdot u_k \iff u_n = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} \cdot v_k \right]$$

Für „Puristen“: Ersetze  $u_n$  durch  $(-1)^n \cdot u_n$ . Dann gilt:

$$\begin{aligned} (\forall n \in \mathbb{N}_0) \left[ v_n = \sum_{k=0}^n (-1)^k \binom{n}{k} \cdot u_k \right] &\iff \\ (\forall n \in \mathbb{N}_0) \left[ u_n = \sum_{k=0}^n (-1)^k \binom{n}{k} \cdot v_k \right] \end{aligned}$$

## Beispiel 215

Sei  $d(n, k)$  die Anzahl der Permutationen  $\in S_n$  mit genau  $k$  Fixpunkten.

$$D_n := d(n, 0) .$$

(Die Anzahl der sog. **derangements**).

$$n! = \sum_{k=0}^n d(n, k) = \sum_{k=0}^n \binom{n}{k} D_{n-k} \stackrel{k \mapsto n-k}{=} \sum_{k=0}^n \binom{n}{k} D_k$$

## Beispiel (Forts.)

Mit der Binomialinversion gilt:

$$\begin{aligned}D_n &= \sum_{k=0}^n (-1)^{n-k} \cdot \binom{n}{k} \cdot k! \\&= n! \cdot \sum_{k=0}^n \left( (-1)^{n-k} \frac{n^k}{n!} \right) \\&= n! \cdot \sum_{k=0}^n \left( (-1)^{n-k} \cdot \frac{1}{(n-k)!} \right) \\&= n! \cdot \sum_{k=0}^n \frac{(-1)^k}{k!} .\end{aligned}$$

Daraus ergibt sich, dass

$$\lim_{n \rightarrow \infty} \frac{D_n}{|S_n|} = \frac{1}{e} .$$

## 4.9.4 Stirling-Inversion

Betrachte die Basisfolgen  $(x^n)_{n \geq 0}$  und  $(x^n)_{n \geq 0}$ .

$$x^n = \sum_{k=0}^n S_{n,k} \cdot x^k$$

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

Daraus lässt sich die **Stirling-Inversion** ableiten:

$$(\forall n \in \mathbb{N}_0) \left[ v_n = \sum_{k=0}^n S_{n,k} \cdot u_k \iff u_n = \sum_{k=0}^n (-1)^{n-k} s_{n,k} \cdot v_k \right]$$

## 4.10 Erzeugende Funktionen

### Definition 216

Zu einer Folge  $(a_i)_{i \geq 0}$  mit  $a_i \in \mathbb{R}$  ist die zugehörige (gewöhnliche) erzeugende Funktion die formale Potenzreihe

$$A(z) = \sum_{i=0}^{\infty} a_i \cdot z^i .$$

**Beobachtungen:** Die formalen Potenzreihen bilden einen Ring:

$$A(z) \pm B(z) = \sum_{i \geq 0} (a_i \pm b_i) z^i$$

$$c \cdot A(z) = \sum_{i \geq 0} (c \cdot a_i) z^i$$

Hier gilt folgende Produktformel:

$$A(z) \cdot B(z) = \sum_{n \geq 0} \left( \sum_{k=0}^n a_k \cdot b_{n-k} \right) \cdot z^n$$

(Konvolution von  $A(z)$  und  $B(z)$ )

## Satz 217

Eine formale Potenzreihe

$$A(z) = \sum_{n \geq 0} a_n \cdot z^n$$

besitzt ein **multiplikatives Inverses** genau dann, wenn  $a_0 \neq 0$ .

Beweis:

Annahme: Sei

$$B(z) = \sum_{n \geq 0} b_n \cdot z^n$$

ein solches Inverses. Dann muss  $A(z) \cdot B(z) = 1$  sein, also auch  $a_0 \cdot b_0 = 1$ , damit  $a_0 \neq 0$ . Daher muss  $b_0 = a_0^{-1}$  sein.

## Beweis (Forts.):

Seien induktiv  $b_0, b_1, \dots, b_{n-1}$  bereits bestimmt. Dann folgt aus

$$[z^n] \left( A(z) \cdot B(z) \right) = \sum_{k=0}^n a_k \cdot b_{n-k} = 0, n \geq 1$$

(dabei bezeichnet  $[z^n](\dots)$  den Koeffizienten von  $z^n$  in  $(\dots)$ )  
folgende Formel:

$$b_n = \frac{-1}{a_0} \sum_{k=1}^n a_k \cdot b_{n-k}$$

Also ist  $b_n$  und damit per Induktion  $B(z)$  eindeutig bestimmt.  $\square$

## Beispiel 218

Geometrische Reihe:

$$A(z) = \sum_{n \geq 0} z^n$$

Es gilt  $A(z) \cdot (1 - z) = 1$ , da

$$\begin{aligned} A(z) \cdot (1 - z) &= A(z) - z \cdot A(z) \\ &= (1 + z + z^2 + \dots) - (z + z^2 + z^3 + \dots) = 1 \end{aligned}$$

Also:

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

## Satz 219

*Einige wichtige Erzeugendenfunktionen:*

1

$$\sum_{n \geq 0} z^n = \frac{1}{1 - z}$$

2

$$\sum_{n \geq 0} (-1)^n \cdot z^n = \frac{1}{1 + z}$$

3

$$\sum_{n \geq 0} z^{2n} = \frac{1}{1 - z^2}$$

4

$$\sum_{n \geq 0} \binom{a}{n} z^n = (1+z)^a, \quad a \in \mathbb{C}$$

5

$$\sum_{n \geq 0} \binom{c+n-1}{n} z^n = \frac{1}{(1-z)^c} = (1-z)^{-c}$$

6

$$\sum_{n \geq 0} \binom{m+n}{n} z^n = \frac{1}{(1-z)^{m+1}}$$

7

$$\sum_{n \geq 0} \frac{z^n}{n!} = e^z$$

8

$$\sum_{n \geq 1} \frac{(-1)^{n+1} z^n}{n} = \ln(1 + z)$$

## Beweis:

- 1 s. o.
- 2 Setze in (1)  $z \mapsto -z$ .
- 3 Setze in (1):  $z \mapsto z^2$ .
- 4 Der Fall  $a \in \mathbb{N}_0$  wird durch den Binomialsatz gezeigt, für allgemeine  $a$  verweisen wir auf die *Analysis*.

5

$$\begin{aligned}\sum_{n \geq 0} \binom{c+n-1}{n} z^n &= \sum_{n \geq 0} \binom{-c}{n} (-1)^n z^n \\ &= \sum_{n \geq 0} \binom{-c}{n} (-z)^n \\ &\stackrel{(4)}{=} (1-z)^{-c}\end{aligned}$$

- 6 Setze in (5)  $c := m - 1$ .



## Beispiel 220

Sei

$$A(z) = \sum_{n \geq 0} a_n \cdot z^n, m \in \mathbb{N}_0.$$

Dann ist

$$z^m \cdot A(z) = \sum_{n \geq 0} a_n \cdot z^{n+m} = \sum_{n \geq m} a_{n-m} \cdot z^n.$$

## Beispiel (Forts.)

Damit gilt

$$\begin{aligned} \frac{z^m}{(1-z)^{m+1}} &\stackrel{\text{Satz 219 (6)}}{=} z^m \cdot \sum_{n \geq 0} \binom{m+n}{n} \cdot z^n \\ &= \sum_{n \geq 0} \binom{m+n}{n} z^{m+n} = \sum_{n \geq m} \binom{n}{n-m} z^n \\ &\stackrel{(*)}{=} \sum_{n \geq 0} \binom{n}{n-m} \cdot z^n. \end{aligned}$$

(\*) Das Gleichheitszeichen gilt, da für  $n < m$

$$\binom{n}{n-m} = 0$$

ist.

## 4.11 Auflösung von Rekursionsgleichungen

### Beispiel 221

$$a_0 = 2$$

$$a_n = 2 \cdot a_{n-1} + 2^n \quad \text{für alle } n \geq 1$$

*lineare inhomogene Rekursionsgleichung 1. Ordnung*

$$a_n = 2 \cdot a_{n-1} + 2^n$$

$$a_{n-1} = 2 \cdot a_{n-2} + 2^{n-1} \quad | \cdot (-2)$$

---

$$a_n - 2 \cdot a_{n-1} = 2 \cdot a_{n-1} - 4 \cdot a_{n-2} + 2^n - 2 \cdot 2^{n-1}$$

$$\Rightarrow 0 = a_n - 4 \cdot a_{n-1} + 4 \cdot a_{n-2}$$

*lineare homogene Rekursionsgleichung 2. Ordnung*

## Beispiel (Forts.)

Zu dieser linearen Rekursionsgleichung

$$a_n - 4 \cdot a_{n-1} + 4 \cdot a_{n-2} = 0$$

gehört das folgende *charakteristische Polynom*:

$$(x - 2)^2 = x^2 - 4 \cdot x + 4 = 0$$

Später wird gezeigt, dass die  $a_n$  hier von der Form

$$a_n = (c_1 \cdot n + c_2) \cdot 2^n \quad c_1, c_2 \in \mathbb{C}$$

sind. Aus den Anfangsbedingungen ( $a_0 = 2, a_1 = 6$ ) ergibt sich  $c_1 = 1$  und  $c_2 = 2$ . Damit gilt

$$a_n = (n + 2) \cdot 2^n \quad \forall n \geq 0$$

## Beispiel (Forts.)

*Man zeigt auch allgemein, dass*

$a_n = (c_1 \cdot n + c_2) \cdot 2^n$  folgende Bedingung erfüllt:

$$a_n - 4a_{n-1} + 4a_{n-2} = 0 \quad (c_1, c_2 \in \mathbb{C}).$$

## Beispiel 222

Sei  $(a_0, a_1, a_2) = (0, 1, 2)$  und

$$a_n = a_{n-1} - a_{n-2} + a_{n-3} \quad \forall n \geq 3$$

(also  $(a_i)_{i \geq 0} = (0, 1, 2, 1, 0, 1, 2, 1, \dots)$ ). Das zugehörige charakteristische Polynom ist

$$\begin{aligned} x^3 - x^2 + x - 1 = 0 &= (x - 1)(x^2 + 1) \\ &= (x - 1)(x - i)(x + i). \end{aligned}$$

Setze nun  $a_n = c_1 \cdot 1^n + c_2 \cdot i^n + c_3 \cdot (-i)^n$ . Durch Einsetzen der Anfangsbedingungen erhält man dann  $c_1 = 1$  und  $c_2 = c_3 = -\frac{1}{2}$ , also

$$a_n = 1 - \frac{1}{2}(i^n + (-i)^n).$$

## Satz 223

Sei  $(q_1, q_2, \dots, q_d)$  eine gegebene Folge,  $q_i \in \mathbb{C}$ ,  $d \geq 1$ ,  $q_d \neq 0$ . Sei weiter

$$q(z) := 1 + q_1z + q_2z^2 + \dots + q_dz^d$$

Das *reflektierte Polynom* dazu ist

$$q^R(z) := z^{\deg(q)} \cdot q\left(\frac{1}{z}\right) = z^d + q_1z^{d-1} + q_2z^{d-2} + \dots + q_d$$

(Bemerkung:  $q^R(z)$  ist das *charakteristische Polynom*). Seien  $\{\alpha_i\}_{1 \leq i \leq k}$  die verschiedenen Nullstellen von  $q^R$ , sei  $d_i$  die Vielfachheit von  $\alpha_i$ . Damit ist

$$\sum_{i=1}^k d_i = d.$$

## Satz 223 (Forts.)

Gelten diese Bedingungen, so sind für eine Folge  $(f_n)_{n \geq 0}$ , mit

$$F(z) := \sum_{n \geq 0} f_n z^n$$

der zugehörigen Erzeugendenfunktion, die folgenden Aussagen äquivalent:

- 1 **Lineare Rekursion:** ( $d$  ist die *Ordnung* der Rekursion)

$$(\forall n \in \mathbb{N}) \left[ f_{n+d} + q_1 \cdot f_{n+d-1} + q_2 \cdot f_{n+d-2} + \dots + q_d \cdot f_n = 0 \right]$$

- 2 **Erzeugende Funktion:**

$$F(z) = \frac{p(z)}{q(z)}$$

für ein Polynom  $p(z)$  vom Grad  $< d$ .

## Satz 223 (Forts.)

- ③ **Partialbruchzerlegung:** *Es gibt Polynome  $g_i$ ,  $\deg(g_i) < d_i$  für  $i = 1, \dots, k$ , so dass*

$$F(z) = \sum_{i=1}^k \frac{g_i(z)}{(1 - \alpha_i z)^{d_i}}$$

- ④ **Explizite Darstellung:** *Es gibt Polynome  $p_i$ ,  $\deg(p_i) < d_i$ , so dass*

$$(\forall n \geq 0) \left[ f_n = \sum_{i=1}^k p_i(n) \cdot \alpha_i^n \right]$$

## Beweis:

Betrachte die komplexen Vektorräume

$$V_k = \{(f_n)_{n \geq 0} : (f_n)_{n \geq 0} \text{ erfüllt Eigenschaft } k\}$$

mit  $k \in \{1, 2, 3, 4\}$ . Es gilt:

$$\dim(V_1) = d$$

$$\dim(V_2) = d \text{ (} p \text{ hat } d \text{ frei wählbare Koeffizienten)}$$

$$\dim(V_3) = \sum_{i=1}^k d_i = d \text{ (} g_i \text{ hat } d_i \text{ frei wählbare Koeffizienten)}$$

$$\dim(V_4) = \sum_{i=1}^k d_i = d \text{ (} p_i \text{ hat } d_i \text{ frei wählbare Koeffizienten)}$$

Um zu zeigen  $V_i = V_j$ , genügt es daher,  $V_i \subseteq V_j$  zu zeigen.

## Beweis (Forts.):

- $V_1 = V_2$ : Sei  $(f_n)_{n \geq 0} \in V_2$ . Wir wissen, dass

$$F(z) = \sum_{n \geq 0} f_n \cdot z^n = \frac{p(z)}{q(z)}.$$

Es ist

$$\tilde{F}(z) = (1 + q_1z + q_2z^2 + \dots + q_dz^d) \cdot \sum_{n \geq 0} f_n z^n = p(z)$$

mit  $\deg(p) \leq d - 1$ , also  $[z^{d+n}]p(z) = 0$  für alle  $n \geq 0$ .

Betrachte für  $n \geq 0$

$$[z^{d+n}]\tilde{F}(z) = f_{n+d} + f_{n+d-1}q_1 + \dots + f_nq_d = 0.$$

Damit gilt, dass

$$(f_n)_{n \geq 0} \in V_1,$$

also  $V_2 \subseteq V_1$ , und damit  $V_1 = V_2$ .

## Beweis (Forts.):

- $V_2 = V_3$ : Sei  $(f_n)_{n \geq 0} \in V_3$ , also

$$F(z) = \sum_{i=1}^k \frac{g_i(z)}{(1 - \alpha_i z)^{d_i}}.$$

Zu zeigen ist, dass

$$F(z) = \frac{p(z)}{q(z)}.$$

Betrachte hierzu

$$\prod_{i=1}^k (1 - \alpha_i z)^{d_i}.$$

Wir wissen, dass

$$q^R(z) = \prod_{i=1}^k (z - \alpha_i)^{d_i}.$$

## Beweis (Forts.):

Weiter gilt, dass

$$q^R(z) = z^d \cdot q\left(\frac{1}{z}\right),$$

also

$$\begin{aligned} q(z) &= \left(q^R(z)\right)^R = \left(\prod_{i=1}^k (z - \alpha_i)^{d_i}\right)^R \\ &= z^d \cdot \prod_{i=1}^k \left(\frac{1}{z} - \alpha_i\right)^{d_i} \\ &= \prod_{i=1}^k (1 - \alpha_i z)^{d_i}. \end{aligned}$$

## Beweis (Forts.):

Daraus erhält man (durch Bilden des Hauptnenners)

$$F(z) = \frac{\sum_{i=1}^k \left( g_i(z) \cdot \prod_{\substack{j=1 \\ j \neq i}}^k (1 - \alpha_j z)^{d_j} \right)}{\prod_{i=1}^k (1 - \alpha_i z)^{d_i}} = \frac{p(z)}{q(z)}.$$

Es ist damit

$$\deg(p(z)) < d_i + \sum_{\substack{j=1 \\ j \neq i}}^k d_j = d,$$

also  $V_3 \subseteq V_2$  und damit  $V_2 = V_3$ .

- $V_3 = V_4$ : Sei

$$(f_n)_{n \geq 0} \in V_3.$$

Zu zeigen ist, dass

$$(f_n)_{n \geq 0} \in V_4.$$

Es gilt, dass

$$F(z) = \sum_{i=1}^k \frac{g_i(z)}{(1 - \alpha_i z)^{d_i}} \quad \deg(g_i(z)) < d_i .$$

Aus Satz 6 (5) wissen wir, dass

$$\frac{1}{(1-x)^c} = \sum_{n \geq 0} \binom{c+n-1}{n} \cdot x^n.$$

Damit gilt, dass

$$\begin{aligned}\frac{1}{(1 - \alpha_i z)^{d_i}} &= \sum_{n \geq 0} \binom{d_i + n - 1}{n} \cdot (\alpha_i z)^n \\ &= \sum_{n \geq 0} \binom{d_i + n - 1}{n} \cdot \alpha_i^n z^n .\end{aligned}$$

## Beweis (Forts.):

Mit

$$g_i(z) = g_{i,0} + g_{i,1}z + \dots + g_{i,d_i-1}z^{d_i-1} = \sum_{j=0}^{d_i-1} g_{i,j}z^j$$

gilt:

$$\frac{g_i(z)}{(1 - \alpha_i z)^{d_i}} = \sum_{n \geq 0} \left( \sum_{j=0}^{d_i-1} g_{i,j} \cdot \binom{d_i + n - j - 1}{n - j} \cdot \alpha_i^{n-j} \right) \cdot z^n$$

## Beweis (Forts.):

Also gilt auch, dass

$$F(z) = \sum_{i=1}^k \frac{g_i(z)}{(1 - \alpha_i z)^{d_i}}$$
$$= \sum_{n \geq 0} \left( \underbrace{\sum_{i=1}^k \sum_{j=0}^{d_i-1} \alpha_i^{-j} \cdot g_{i,j} \cdot \binom{n + d_i - j - 1}{d_i - 1} \cdot \alpha_i^n}_{p_i(n)} \right) \cdot z^n$$

Betrachte nun

$$f_n = [z^n]F(z) = \sum_{i=1}^k p_i(n) \cdot \alpha_i^n.$$

Es gilt, dass  $\deg(p_i(n)) \leq d_i - 1$ , und damit ist auch  $(f_n)_{n \geq 0} \in V_4$ , also  $V_3 = V_4$ . □

**Anwendung:** Sei eine homogene Rekursion gegeben, z. B.

$$F_{n+2} = F_{n+1} + F_n \quad F_0 = 0, F_1 = 1$$

- ① Drücke die Rekursion in einer einzigen Formel aus, inklusive der Anfangsbedingungen. Wie immer ist  $F_n = 0$  für  $n < 0$ .  $F_n = F_{n-1} + F_{n-2}$  gilt auch für  $n = 0$ , aber für  $n = 1$  ist  $F_1 = 1$ , die rechte Seite jedoch 0. Also ist die vollständige Rekursion

$$F_n = F_{n-1} + F_{n-2} + \delta_{n,1},$$

mit

$$\delta_{n,m} = \begin{cases} 1 & n = m \\ 0 & \text{sonst} \end{cases}$$

- 2 Interpretiere die Gleichung aus 1. mit Hilfe von erzeugenden Funktionen. Wir wissen schon, dass Indexerniedrigung einer Multiplikation mit einer Potenz von  $z$  entspricht. Also erhalten wir:

$$\begin{aligned}F(z) &= \sum F_n z^n \\ &= \sum F_{n-1} z^n + \sum F_{n-2} z^n + \sum \delta_{n,1} z^n \\ &= z \cdot F(z) + z^2 \cdot F(z) + z\end{aligned}$$

- 3 Löse die Gleichung in  $F(z)$ . Das ist leicht:

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

- ④ Drücke die rechte Seite als formale Reihe aus und ermittle daraus die Koeffizienten. Dies ist der schwierigste Schritt. Zunächst schreiben wir  $1 - z - z^2$  in der Form  $1 - z - z^2 = (1 - \alpha z)(1 - \beta z)$  und ermitteln dann durch Partialbruchzerlegung die Konstanten  $a$  und  $b$ , so dass gilt:

$$\frac{1}{(1 - \alpha z)(1 - \beta z)} = \frac{a}{1 - \alpha z} + \frac{b}{1 - \beta z} .$$

Es ergibt sich z.B.

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

Es gilt:

$$\begin{aligned} F(z) &= z \left( \frac{a}{1 - \alpha z} + \frac{b}{1 - \beta z} \right) \\ &= z \left( a \sum_{n \geq 0} \alpha^n z^n + b \sum_{n \geq 0} \beta^n z^n \right) \\ &= \sum_{n \geq 1} (a\alpha^{n-1} + b\beta^{n-1}) z^n \end{aligned}$$

und somit

$$\begin{aligned} F_n &= a\alpha^{n-1} + b\beta^{n-1} \\ &= \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right), \end{aligned}$$

nachdem man die Konstanten  $a$  und  $b$  etwa aus den Gleichungen für  $F_0$  und  $F_1$  bestimmt hat.

## 4.12 Das Master-Theorem

Bei der Analyse von **Divide-and-Conquer**-Verfahren stößt man oft auf Rekursionen, die sich nicht als lineare Rekursionen formulieren lassen. So führt der Mergesort-Algorithmus in der Standardvariante zu der Rekursionsgleichung

$$C_n = C_{\lfloor n/2 \rfloor} + C_{\lceil n/2 \rceil} + n \quad \text{für alle } n > 1 \quad \text{und } C_1 = 0.$$

Löst man allgemein ein Problem der Größe  $n$  dadurch, dass man es in  $a$  Teilprobleme der Größe höchstens  $n/b$  aufteilt, so erhält man für die Laufzeit  $T(n)$  eine Rekursion der Form

$$T(n) = a \cdot T(n/b) + f(n),$$

wobei  $f(n)$  die Laufzeit für die Aufteilung in Teilprobleme und für das Zusammenfügen der Lösungen der Teilprobleme ist.

## Satz 224 (Master-Theorem)

Seien  $a \in \mathbb{N}$ ,  $b > 1$  und  $C \geq 0$  Konstanten, und sei  $f(n)$  eine nichtnegative Funktion. Weiter seien  $c_1(n), \dots, c_a(n)$  Funktionen mit  $|c_i(n)| \leq C$  für alle  $1 \leq i \leq a$  und  $n \in \mathbb{N}_0$ . Ist dann  $T(n)$  eine Funktion, die für  $n = 1$  gleich 0 ist und die für  $n \geq 1$  die Rekursionsgleichung

$$T(n) = T(n/b + c_1(n)) + \dots + T(n/b + c_a(n)) + f(n)$$

erfüllt, dann gilt

$$T(n) = \begin{cases} \Theta(n^{\log_b a}), & \text{falls } f(n) = O(n^{\log_b a - \epsilon}) \text{ für ein } \epsilon > 0, \\ \Theta(n^{\log_b a} \log n), & \text{falls } f(n) = \Theta(n^{\log_b a} \cdot \log^\delta n) \text{ f. } \delta > 0, \\ \Theta(f(n)), & \text{falls } f(n) = \Omega(n^{\log_b a + \epsilon}) \text{ für ein } \epsilon > 0. \end{cases}$$

Für den Beweis des Master-Theorems verweisen wir auf die Literatur, z.B. in:

- 1 Verma, Rakesh M.:

*A general method and a master theorem for divide-and-conquer recurrences with applications.*

J. Algorithms **16**, 1 (1994), pp. 67–79

- 2 Roura, Salvador:

*An improved master theorem for divide-and-conquer recurrences.*

Proceedings of the 24th International Colloquium on Automata, Languages and Programming, ICALP'97 (Bologna, Italy, July 7-11, 1997). LNCS **1256** (1997), pp. 449–459

## Satz 225 (“Baby-Version” des MT)

Wenn die Funktion  $T$  für  $x < 1$  gleich 0 ist und wenn für  $x \geq 1$  die Rekursion

$$T(x) = aT(x/b) + x$$

gilt (also  $T(1) = 1$ ), dann gilt für  $n = b^t$  eine ganzzahlige Potenz von  $b$ :

$$T(n) = (1 + o(1)) \cdot \begin{cases} \frac{b}{b-a}n, & \text{falls } a < b, \\ n \log_b n, & \text{falls } a = b, \\ \frac{a}{a-b}n^{\log_b a}, & \text{falls } a > b. \end{cases}$$

## Beweis:

Zuerst wenden wir die Rekursionsgleichung so oft an, bis wir die Anfangsbedingung erreichen. Wir haben also

$$\begin{aligned}T(n) &= n + aT(n/b) \\&= n + a\frac{n}{b} + a^2T(n/b^2) \\&= n + a\frac{n}{b} + a^2\frac{n}{b^2} + a^3T(n/b^3) \\&= \dots \\&= n + a\frac{n}{b} + a^2\frac{n}{b^2} + \dots + a^tT(n/b^t),\end{aligned}$$

wobei  $t = \log_b n$ . Also

$$T(n) = n \left( 1 + \frac{a}{b} + \dots + \frac{a^t}{b^t} \right)$$

Beweis (Forts.):

**Fallunterscheidung:**

$a < b$ : In diesem Fall konvergiert die Summe und wir erhalten:

$$T(n) \leq n \sum_{k \geq 0} \left(\frac{a}{b}\right)^k = \frac{b}{b-a} n .$$

$a = b$ : In diesem Fall ist die Lösung

$$T(n) = n (\log_b n + 1) = (1 + o(1)) \cdot n \log_b n .$$

## Beweis (Forts.):

$a > b$ : Wir erhalten:

$$\begin{aligned} T(n) &= n \left( \frac{a}{b} \right)^t \left( 1 + \frac{b}{a} + \dots + \frac{b^t}{a^t} \right) \\ &\leq n \frac{a}{a-b} \left( \frac{a}{b} \right)^t \\ &= \frac{a}{a-b} a^{\log_b n} \\ &= \frac{a}{a-b} n^{\log_b a}, \end{aligned}$$

da  $t = \log_b n$ .



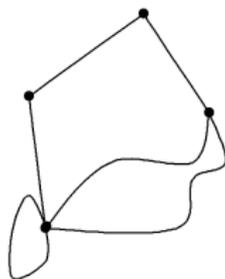
# Kapitel IV Graphen und Algorithmen

## 1. Grundlagen

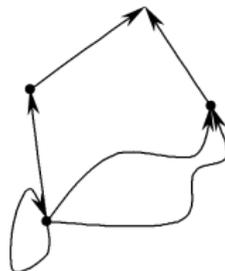
### Definition 226

Ein Graph  $G = (V, E)$  besteht aus einer Menge  $V$  von Knoten (aka Ecken, engl. **vertex**, **vertices**) und einer (Mehrfach-)Menge  $E \subseteq V \times V$  von Paaren  $(u, v) \in V \times V$ , genannt Kanten (engl. **edges**).

Ein Graph heißt **ungerichteter** Graph, falls für alle  $(u, v) \in E$  auch  $(v, u) \in E$  ist. Man schreibt dann  $E$  auch als Menge von ungeordneten Paaren  $\{u, v\}$  von Kanten.



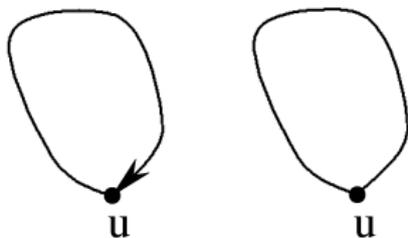
Ein Graph heißt ein **gerichteter** Graph, falls  $E$  (wie in obiger Definition) eine Menge von geordneten Paaren  $(u, v)$  ist.



## 1.1 Schlingen

### Definition 227

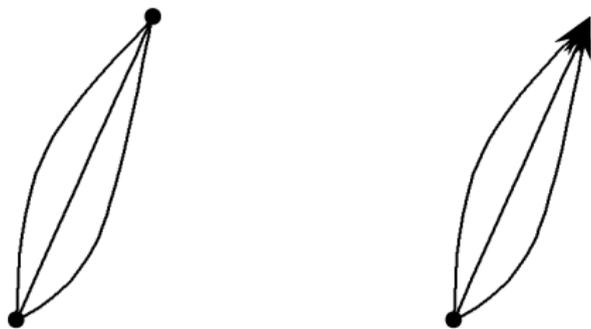
Eine **Schlinge** ist eine Kante der Form  $(u, u)$  bzw.  $\{u, u\}$ .



## 1.2 Mehrfachkanten

### Definition 228

Ist  $E$  eine Multimenge (d. h. Kanten treten mit Vielfachheit auf), sind die Kanten mit Vielfachheit 2 oder größer **Mehrfachkanten**.



Ein Graph, der Mehrfachkanten enthält, heißt auch **Multigraph**.

## 1.3 Einfache Graphen

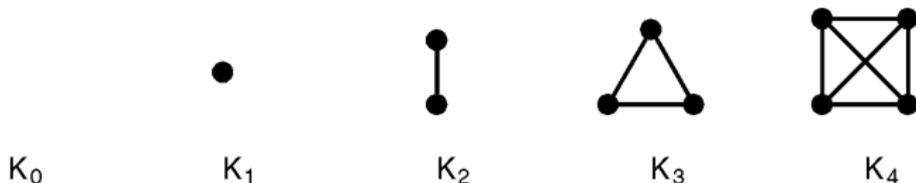
### Definition 229

Ein Graph heißt **einfach**, falls er keine Schlingen oder Mehrfachkanten enthält.

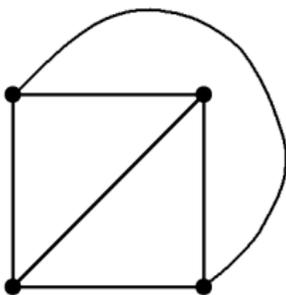
### Definition 230

Ein Graph  $G = (V, E)$  ( $=: K_n$ ) mit  $|V| = n$  Knoten heißt **vollständig** (**der vollständige Graph mit  $n$  Knoten**), falls  $E = \{\{u, v\}; u, v \in V, u \neq v\}$  bzw.  $E = \{(u, v); u, v \in V, u \neq v\}$ .

### Beispiel 231



Der  $K_4$  lässt sich auch kreuzungsfrei zeichnen:



Für die Anzahl der Kanten in einem vollständigen Graphen (und damit für die **maximale** Anzahl von Kanten in einem einfachen Graphen) gilt:

$$|E| = \binom{n}{2} = \frac{n \cdot (n - 1)}{2}$$

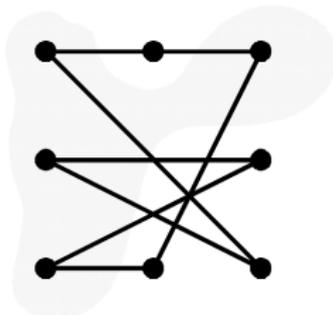
## 1.4 Bipartiter Graph

### Definition 232

Ein Graph heißt **bipartit**, falls sich  $V$  in  $V_1 \uplus V_2$  mit  $V_1 \neq \emptyset \neq V_2$  so partitionieren lässt, dass gilt:

$$(\forall e \in E) [e \in (V_1 \times V_2) \cup (V_2 \times V_1)]$$

### Beispiel 233 ( $C_8$ , Kreis mit 8 Knoten)



**Bemerkung:**

Schreibweise für bipartite Graphen:

$$G = (V_1, V_2, E)$$

## 1.5 Vollständiger bipartiter Graph

### Definition 234

Ein bipartiter Graph  $G = (V_1, V_2, E)$  heißt **vollständig**, falls  $E = V_1 \times V_2 \cup V_2 \times V_1$ .

(Notation:  $K_{m,n}$  mit  $m = |V_1|, n = |V_2|$ )

### Beispiel 235



$K_{1,1}$



$K_{1,2}$



$K_{3,3}$

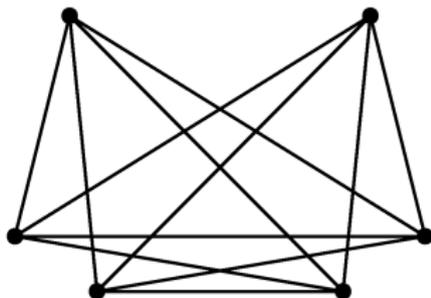
## 1.6 $k$ -partiter Graph

### Definition 236

Ein Graph heißt  $k$ -partit ( $k \in \mathbb{N}, k \geq 2$ ), falls es eine Partition  $V = V_1 \uplus V_2 \uplus \dots \uplus V_k$  mit  $V_i \neq \emptyset, i = 1, \dots, k$  gibt, so dass

$$(\forall e \in E) [e \in V_i \times V_j; 1 \leq i, j \leq k, i \neq j]$$

### Beispiel 237 (Vollständiger tripartiter Graph $K_{2,2,2}$ )



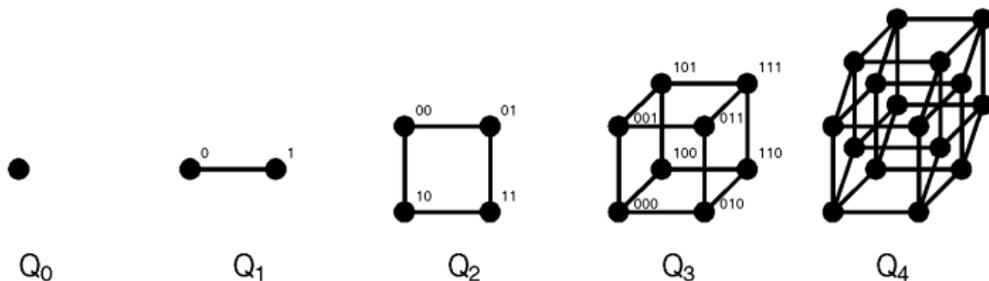
## 1.7 (Binärer) Hyperwürfel

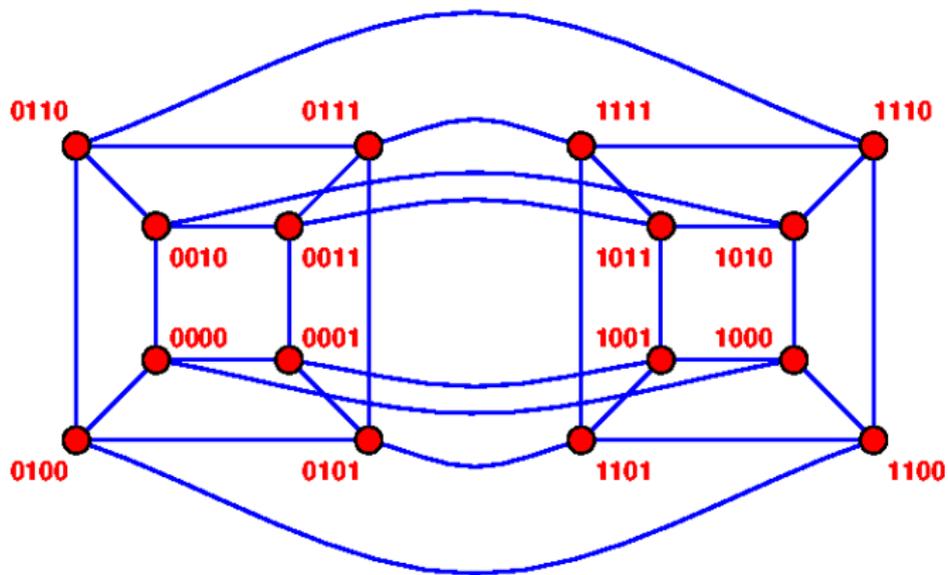
### Definition 238

Ein Graph  $G = (V, E)$  heißt  $n$ -dimensionaler binärer Hyperwürfel (aka  $Q_n$ ), falls  $V = V_n = \{0, 1\}^n$  mit

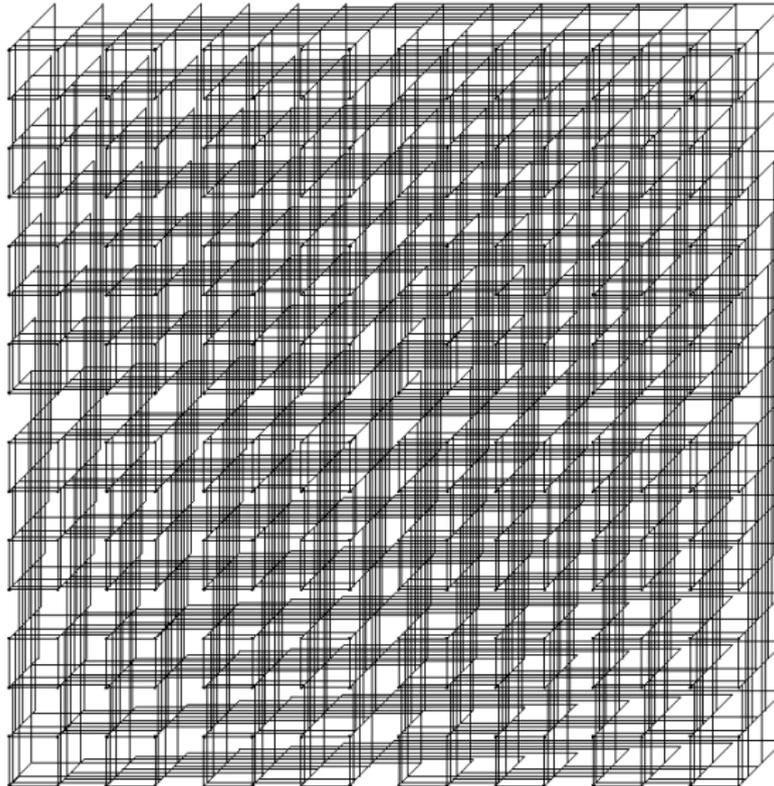
$$E = \left\{ \{v, w\} \in V_n^2; \text{Hamming-Abstand}(v, w) = 1 \right\}.$$

### Beispiel 239





$Q_4$ : 4-dimensionaler Hyperwürfel



$Q_8$ : 8-dimensionaler Hyperwürfel

Für die Anzahl der Knoten in  $Q_n$  gilt:

$$|V| = 2^n$$

Für die Anzahl der Kanten in  $Q_n$  gilt:

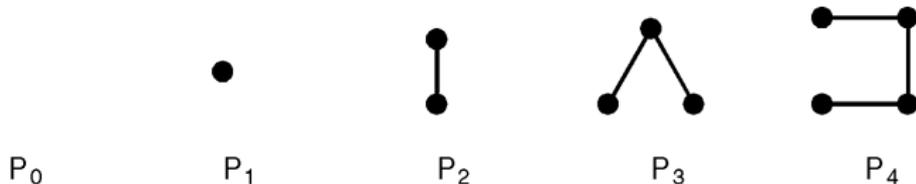
$$|E| = n \cdot \frac{2^n}{2} = n \cdot 2^{n-1}$$

## 1.8 Pfade

### Definition 240

- 1 Ein Pfad der Länge  $n$  ist eine Folge  $(v_1, v_2, \dots, v_n)$  von Knoten eines Graphen  $G = (V, E)$ , so dass  $(v_i, v_{i+1}) \in E$  für alle  $i = 1, \dots, n - 1$ .
- 2 Der Graph  $P_n$  ist der Graph  $(V, E)$  mit  $V = \{v_1, \dots, v_n\}$  und  $E = \{(v_i, v_{i+1}); i = 1, \dots, n - 1\}$ .

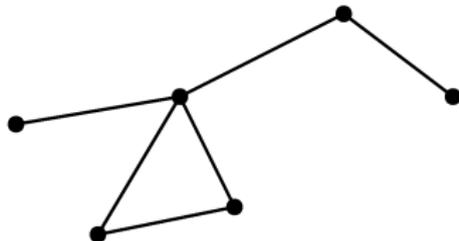
### Beispiel 241



## Definition 242

Ein Pfad heißt **einfach**, falls alle Knoten paarweise verschieden sind.

Beispiel 243 (Pfad, aber *nicht einfacher* Pfad der Länge 7)



## 1.9 Kreise

### Definition 244

Ein Graph  $G = (V, E)$  heißt (einfacher) Kreis der Länge  $n$  (i. Z.  $C_n, n \geq 3$ ), falls  $V = \{v_0, \dots, v_{n-1}\}$  und  $E = \{\{v_i, v_{(i+1) \bmod n}\}; i = 0, \dots, n - 1\}$ .

## 1.10 Gitter

### Definition 245

Ein Graph  $G = (V, E)$  heißt ein  $m$ - $n$ -Gitter (zweidimensionales Gitter mit den Seitenlängen  $m$  und  $n$ , i. Z.  $M_{m,n}$ ), falls  $V = \{1, \dots, m\} \times \{1, \dots, n\}$  und

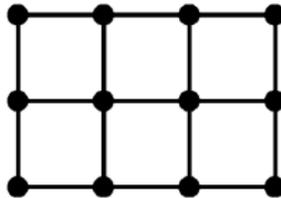
$$\underbrace{\{(i, j), (k, l)\}} \in E \iff |i - k| + |j - l| = 1$$

Kante zwischen  
Knoten  $(i, j)$   
und Knoten  $(k, l)$

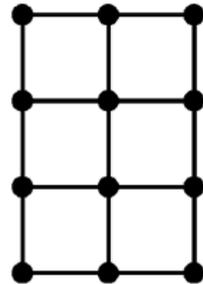
## Beispiel 246



$M_{1,2}$



$M_{3,4}$



$M_{4,3}$

## 1.11 Torus

### Definition 247

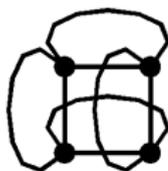
Ein Graph  $G = (V, E)$  heißt **zweidimensionaler Torus** (pl. Tori) mit den Seitenlängen  $m$  und  $n$ , falls  $V = \{1, \dots, m\} \times \{1, \dots, n\}$  und

$$\{(i, j), (k, l)\} \in E \iff |i - k| \bmod m + |j - l| \bmod n = 1$$

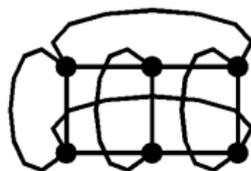
### Beispiel 248



$T_{1,2}$



$T_{2,2}$

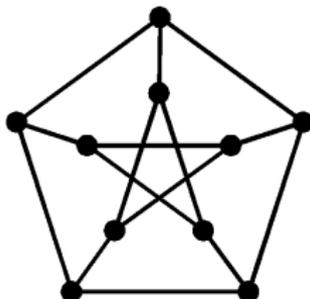


$T_{2,3}$

## 1.12 Petersen-Graph

### Definition 249

Der folgende Graph heißt **Petersen-Graph**:



## 2. Definitionen für ungerichtete Graphen

### 2.1 Pfade und Kreise

#### Definition 250

Ein **Pfad (Weg)** in einem Graphen ist eine Folge von Knoten  $v_0, v_1, \dots, v_k$  mit  $\{v_i, v_{i+1}\} \in E, i = 0, \dots, k - 1$ .

Ein Pfad heißt **einfach**, wenn alle  $v_i$  paarweise verschieden sind.

Ein **Kreis** ist ein Pfad, bei dem gilt:  $v_0 = v_k$ .

Ein Kreis heißt **einfach**, wenn die Knoten  $v_0, \dots, v_{k-1}$  paarweise verschieden sind.

## 2.2 Isomorphe Graphen

### Definition 251

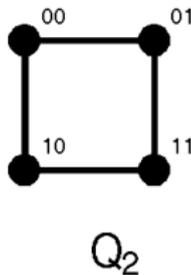
Zwei Graphen  $G_i = (V_i, E_i)$ ,  $i = 1, 2$  heißen **isomorph**, falls es eine Bijektion  $\varphi : V_1 \rightarrow V_2$  gibt, so dass gilt:

$$(\forall v, w \in V_1) \left[ \{v, w\} \in E_1 \iff \{\varphi(v), \varphi(w)\} \in E_2 \right].$$

### Beispiel 252

$K_{2,2} \cong C_4 \cong Q_2$  oder  $T_{4,4,4} \cong Q_6$

### Beispiel 253



## 2.3 Adjazenz

### Definition 254

Sei  $G = (V, E)$ ,  $u, v \in V$  und  $\{u, v\} \in E$ . Dann heißen  $u$  und  $v$  **adjazent** (aka **benachbart**).  $u$  und  $v$  sind **Endknoten** von  $\{u, v\}$ ;  $u$  und  $v$  sind **inzident** zur Kante  $\{u, v\}$ . Zwei Kanten heißen **adjazent**, falls sie einen Endknoten gemeinsam haben.

## 2.4 Nachbarschaft

### Definition 255

Sei  $u \in V$ .

$$N(u) := \{v \in V; u \neq v, \{u, v\} \in E\}$$

heißt die **Nachbarschaft** von  $u$ .

$d(u) := \deg(u) := |N(u)|$  heißt **Grad** von  $u$ .

Falls  $d(u) = 0$ , so heißt  $u$  **isoliert**.

## 2.5 Gradfolge

### Definition 256

Sei  $V = \{v_1, \dots, v_n\}$  so, dass

$$d(v_1) \geq d(v_2) \geq \dots \geq d(v_n).$$

Dann heißt  $(d(v_1), d(v_2), \dots, d(v_n))$  die **Gradfolge** von  $G$ .

### **Bemerkung:**

Isomorphe Graphen haben dieselbe Gradfolge.

## Satz 257

Sei  $G = (V, E)$ . Dann gilt:

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

Beweis:

$\sum d(v)$  zählt Halbkanten. □

## Korollar 258

*In jedem Graphen ist die Anzahl der Knoten mit ungeradem Grad gerade.*

## 2.6 Reguläre Graphen

### Definition 259

Ein Graph  $G = (V; E)$  heißt *k-regulär* genau dann, wenn

$$(\forall v \in V) \left[ d(v) = k \right].$$

### Beispiel 260

$Q_k$  ist *k-regulär*;  $T_{m_1, \dots, m_k}$  ist *2k-regulär*.

## 2.7 Teilgraphen

### Definition 261

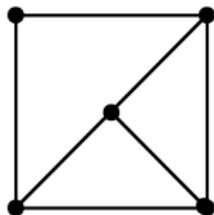
- ①  $G' = (V', E')$  heißt **Teilgraph** von  $G = (V, E)$ , falls

$$V' \subseteq V \quad \wedge \quad E' \subseteq E.$$

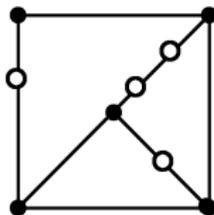
- ② Ein Graph  $H = (\bar{V}, \bar{E})$  heißt **Unterteilung** von  $G = (V, E)$ , falls  $H$  aus  $G$  dadurch entsteht, dass jede Kante  $\{v, w\} \in E$  durch einen Pfad  $v = \bar{v}_0, \bar{v}_1, \dots, \bar{v}_k = w$  ersetzt wird. Dabei sind  $\bar{v}_1, \dots, \bar{v}_{k-1}$  jeweils neue Knoten.

## Beispiel 262 (Unterteilung)

G:



H:



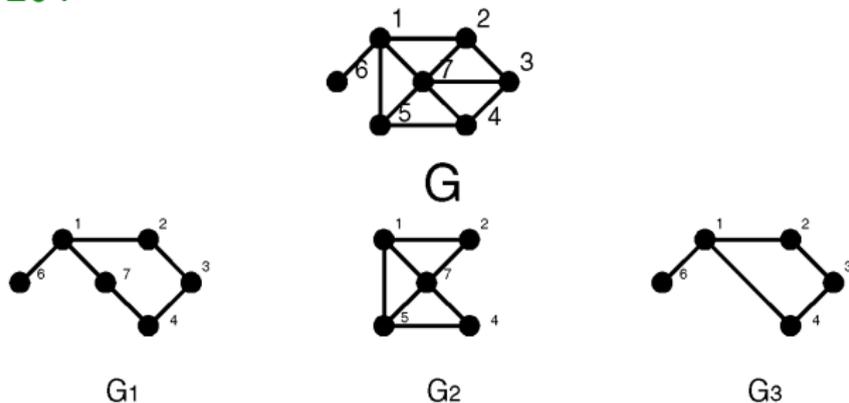
**Bemerkung:** (Satz von Kuratowski) Ein Graph ist genau dann nicht planar, wenn er eine Unterteilung des  $K_5$  oder des  $K_{3,3}$  als Teilgraph enthält.

## 2.8 Induzierte Teilgraphen

### Definition 263

Ein Graph  $G' = (V', E')$  heißt (knoten-)induzierter Teilgraph von  $G = (V, E)$ , falls  $G'$  Teilgraph von  $G$  ist und  $E' = E \cap (V' \times V')$ .

### Beispiel 264

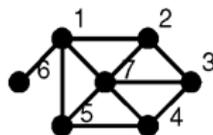


$G_1$  ist Teilgraph von  $G$ , aber nicht knoteninduziert;  $G_2$  ist der von  $\{1, 2, 4, 5, 7\}$  induzierte Teilgraph;  $G_3$  ist nicht Teilgraph von  $G$ .

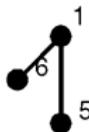
Sei  $V' \subseteq V$ . Dann bezeichnet  $G \setminus V'$  den durch  $V \setminus V'$  induzierten Teilgraphen von  $G$ .

### Beispiel 265

$$G_4 = G \setminus \{2, 3, 4, 7\}$$



G



G<sub>4</sub>

## 2.9 Erreichbarkeit

### Definition 266

Sei  $G = (V, E)$ ;  $u, v \in V$ .  $v$  heißt von  $u$  aus in  $G$  **erreichbar**, falls  $G$  einen Pfad mit Endknoten  $u$  und  $v$  enthält.

### Satz 267

Die Relation  $R \subseteq V \times V$  mit

$$uRv \iff \text{„}v \text{ ist von } u \text{ aus in } G \text{ erreichbar“}$$

ist eine Äquivalenzrelation.

### Beweis:

Es ist leicht zu sehen, dass  $R$  reflexiv, symmetrisch und transitiv ist. □

## 2.10 Zusammenhangskomponenten

Die Äquivalenzklassen der Erreichbarkeitsrelation heißen **Zusammenhangskomponenten** von  $G$ .  $G$  heißt **zusammenhängend**, falls  $G$  aus genau einer Zusammenhangskomponente besteht.

## 2.11 Bäume

### Definition 268

Ein Graph  $G = (V, E)$  heißt **Baum**, falls  $G$  zusammenhängend und kreisfrei ist.

## Satz 269

*Die folgenden Aussagen sind äquivalent:*

- 1  $G = (V, E)$  ist ein nichtleerer Baum.
- 2  $V \neq \emptyset$  und für je zwei Knoten  $u, v \in V$  mit  $u \neq v$  gibt es genau einen einfachen Pfad zwischen  $u$  und  $v$ .
- 3  $G$  ist zusammenhängend und  $|V| = |E| + 1$ .

## Beweis:

1.  $\Rightarrow$  2.

Seien  $u, v \in V$ ,  $u \neq v$ . Da  $G$  zusammenhängend ist, muss mindestens ein Pfad zwischen  $u$  und  $v$  existieren.

Widerspruchssannahme: Es gibt zwei verschiedene Pfade zwischen  $u$  und  $v$ .



Dann gibt es einen Kreis in  $G$ , was einen Widerspruch zur Annahme darstellt.

## Beweis (Forts.):

2.  $\Rightarrow$  3. Beweis durch Induktion:

Dass  $G$  zusammenhängend und  $V$  nichtleer sein muss, ist klar. Für  $|E| = 0$  gilt  $|V| = 1$  (Induktionsanfang).

$G$  muss einen Knoten mit Grad 1 enthalten: Wähle  $u \in V$  beliebig. Wähle einen Nachbarn  $u_1$  von  $u$ . Falls  $\deg(u_1) > 1$ , wähle einen Nachbarn  $u_2 \neq u$  von  $u_1$  usw. Da  $V$  endlich und  $G$  zusammenhängend und kreisfrei ist (sonst gäbe es ein Knotenpaar mit zwei verschiedenen einfachen Pfaden dazwischen), kommt man so schließlich zu einem Blatt (Knoten mit Grad 1).

Entfernt man dieses Blatt (sowie die inzidente Kante) und wendet auf den entstehenden Graphen die IV an, erhält man:

$$(|V| - 1) - 1 = |E| - 1$$

Damit ist bewiesen, dass  $|V| = |E| + 1$ .

## Beweis (Forts.):

3.  $\Rightarrow$  1.

Sei nun  $G$  zusammenhängend mit  $|V| = |E| + 1$ .

Zu zeigen:  $G$  ist kreisfrei.

Widerspruchsannahme:  $G$  enthält einen einfachen Kreis  
 $C = (V_C, E_C)$ .

Da wir  $G$  aufbauen können, indem wir die Knoten in  $V \setminus V_C$  mit jeweils einer neuen Kante hinzufügen und zum Schluss noch eventuell übrig gebliebene Kanten hinzufügen, gilt:

$$|V| = |V_C| + |V \setminus V_C| \leq |E_C| + |E \setminus E_C| = |E|$$

Das ist ein Widerspruch zur Voraussetzung  $|V| = |E| + 1$ .



## Korollar 270

Seien  $T = (V, E)$  ein Baum mit  $|V| = n$  und  $(d_1, d_2, \dots, d_n)$  die Gradfolge von  $T$ , dann gilt:

$$\sum_{i=1}^n d_i = 2 \cdot |E| = 2n - 2$$

## 2.12 Spann­b­ume

### Definition 271

Ein Teilgraph  $T = (V', E')$  von  $G = (V, E)$  hei­ft **Spannbaum** von  $G$ , falls  $T$  ein Baum und  $V' = V$  ist.

## Satz 272 (Arthur Cayley, 1889)

Sei  $t(n)$  die Anzahl der verschiedenen markierten Bäume mit Knotenmenge  $\{1, \dots, n\}$ . Dann gilt:

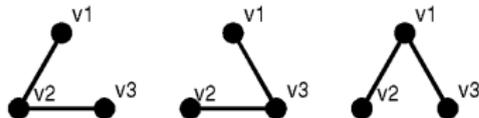
$$t(n) = n^{n-2}$$

### Beispiel 273

•  $n = 2$ :

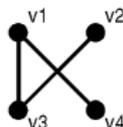
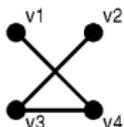
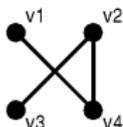
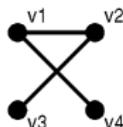
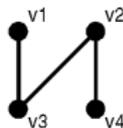
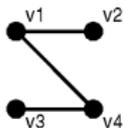
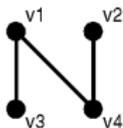
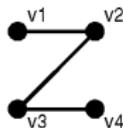
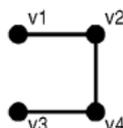
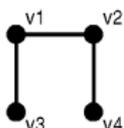
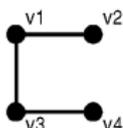
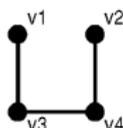
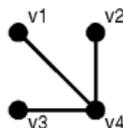
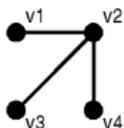
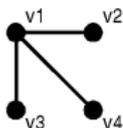
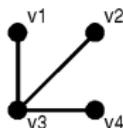


•  $n = 3$ :



## Beispiel (Forts.)

- $n = 4$ :



## Beweis:

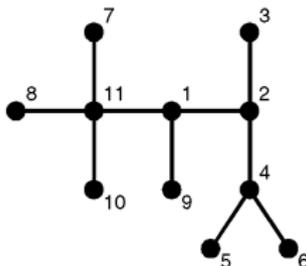
Wir geben eine Bijektion zwischen der Menge  $\mathcal{T}(n)$  der markierten Spannbäume mit  $n$  Knoten und der Menge  $\{1, \dots, n\}^{n-2}$  an. (Diese Bijektion geht auf **H. Prüfer** zurück; man bezeichnet sie deshalb auch als **Prüfer-Code**.)

## Beweis (Forts.):

Sei  $T \in \mathcal{T}(n)$ . Konstruiere  $(a_1, \dots, a_{n-2})$ ,  $a_i \in \{1, \dots, n\}$  wie folgt:

```
for  $i = 1$  to  $n - 2$  do  
   $v_i :=$  Blatt mit minimalem Index  
   $a_i :=$  Index des Nachbarn von  $v_i$  in  $T$   
   $T := T \setminus \{v_i\}$   
od
```

## Beispiel 274



Prüfer-Code:  $(2, 4, 4, 2, 1, 11, 11, 1, 11)$

## Beweis (Forts.):

Sei  $(a_1, \dots, a_{n-2})$  ein gegebener Prüfer-Code; sei  $f_i$  sei die Anzahl des Auftretens von  $i$  in  $(a_1, \dots, a_{n-2})$ . Wenn ein Blatt, das Nachbar von  $a_i$  ist, im Algorithmus gestrichen wird, ist  $a_i$  nicht das kleinste Blatt, sondern innerer Knoten:

$$d(a_i) \geq f_i + 1$$

Da

$$n - 2 = \sum_{i=1}^n f_i \leq \sum_{i=1}^n (d(v_i) - 1) = 2n - 2 - n = n - 2$$

gilt

$$(\forall i) \left[ f_i = d(a_i) - 1 \right]$$

Also ergeben sich aus den  $f_i$  die Knotengrade. Insbesondere sind die Knoten mit  $f_i = 0$  (also die, die nicht im Code auftauchen), genau die Blätter des Baumes.

## Beweis (Forts.):

**Umkehrabbildung:** Gegeben  $(a_1, \dots, a_{n-2})$

for  $i=1$  to  $n$  do

$d(v_i) := f_i + 1$

od

$B := \emptyset; T := \emptyset$

for  $i=1$  to  $n-2$  do

$b := \min_{1 \leq j \leq n} \{j; j \notin \{a_i, a_{i+1}, \dots, a_{n-2}\} \cup B\}$

füge Kante  $(b, a_i)$  zu  $T$  hinzu

$B := B \cup \{b\}$

od

füge letzte Kante zu  $T$  gemäß der Gradbedingung hinzu

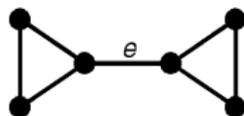


## 2.13 Brücken

### Definition 275

Eine Kante  $e$  eines Graphen  $G = (V, E)$  heißt **Brücke**, falls  $G' = (V, E \setminus \{e\})$  mehr Zusammenhangskomponenten hat als  $G$ .

### Beispiel 276

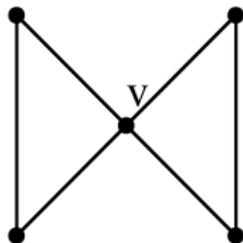


### Beobachtung:

Eine Kante  $e$  ist genau dann eine Brücke, wenn es keinen einfachen Kreis gibt, der  $e$  enthält.

**Anmerkung:** (ohne Definition)

Der Knoten  $v$  in der folgenden Abbildung ist ein Artikulationsknoten:



## 2.14 Abstand

### Definition 277

Seien  $u, v$  zwei Knoten und  $P$  ein Pfad in  $G$  von  $u$  nach  $v$  mit einer minimalen Anzahl  $k$  von Kanten. Dann heißt

$$d(u, v) := k$$

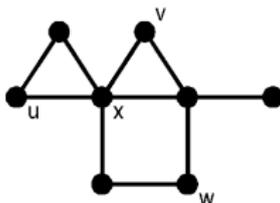
der **Abstand** von  $u$  und  $v$  in  $G$ .

Wir setzen  $d(u, v) := \infty$ , falls  $u$  und  $v$  in verschiedenen Zusammenhangskomponenten von  $G$  liegen.

$$D(G) := \max\{d(u, v); u, v \in V\}$$

heißt der **Durchmesser** des Graphen  $G$ .

## Beispiel 278



$$d(u, v) = 2, \quad d(u, w) = 3, \quad d(u, x) = 1, \quad D(G) = 3.$$

**Beobachtung:**

$d$  erfüllt die Dreiecksungleichung, ist also eine Metrik:

$$d(u, v) \leq d(u, w) + d(w, v)$$

## 2.15 Adjazenzmatrix

### Definition 279

Sei  $G = (V, E)$ ,  $V = \{v_1, \dots, v_n\}$ . Dann heißt

$$A = (a_{ij})_{1 \leq i, j \leq n} \quad \text{mit } a_{ij} = \begin{cases} 1 & \text{falls } \{v_i, v_j\} \in E \\ 0 & \text{sonst} \end{cases}$$

die **Adjazenzmatrix** von  $G$ .

### Beobachtungen:

- Für ungerichtete Graphen ist die Adjazenzmatrix symmetrisch.
- Gibt es keine Schlingen, so sind alle Diagonalelemente null.

## Satz 280

Sei  $A$  die Adjazenzmatrix von  $G = (V, E)$ ,  $|V| = n$ , und sei

$$\begin{aligned} A^0 &:= I, \\ A^{i+1} &:= A^i \cdot A \quad \text{für alle } i \geq 0. \end{aligned}$$

Dann gilt für

$$A^k = (a_{ij}^{(k)})_{1 \leq i, j \leq n} :$$

$a_{i,j}^{(k)}$  ist die Anzahl verschiedener Pfade der Länge  $k$  in  $G$  von  $v_i$  nach  $v_j$ .

## Beweis:

Induktion nach  $k$ :

Induktionsanfang:  $k = 0$  und  $k = 1$  sind trivial.

Induktionsschluss:  $k \mapsto k + 1$

$a_{il}^{(k)}$  ist nach Induktionsvoraussetzung die Anzahl verschiedener Pfade der Länge  $k$  von  $v_i$  nach  $v_l$ .

Die Anzahl verschiedener Pfade von  $v_i$  nach  $v_j$  der Länge  $k + 1$  lässt sich wie folgt berechnen:

$$\sum_{l=1}^n a_{il}^{(k)} \cdot a_{lj} = a_{ij}^{(k+1)}$$



### Bemerkung:

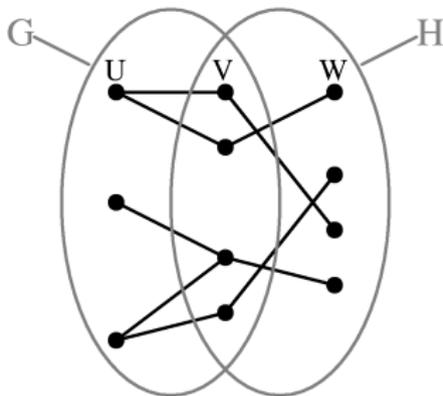
Adjazenzmatrix von bipartiten Graphen

Sei  $G = (U, V, E)$  mit  $U = \{u_1, \dots, u_n\}$  und  $V = \{v_1, \dots, v_m\}$  ein bipartiter Graph. Dann heißt

$$A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \quad \text{mit } a_{ij} = \begin{cases} 1 & \text{falls } \{u_i, v_j\} \in E \\ 0 & \text{sonst} \end{cases}$$

die Adjazenzmatrix von  $G$ .

Werden zwei bipartite Graphen zusammengesetzt, zum Beispiel:



berechnet sich die Adjazenzmatrix  $A'$  des bipartiten Graphen  $G' = (U, W, E')$ , mit

$$\{u, w\} \in E' \iff (\exists v \in V)[\{u, v\} \text{ in } G \text{ und } \{v, w\} \text{ in } H]$$

als das **boolesche** Produkt  $A_G \cdot A_H$ .

## Definition 281

Seien  $A \in \mathbb{B}^{m,k}$ ,  $B \in \mathbb{B}^{k,n}$  zwei boolesche Matrizen, interpretiert als 0, 1-Matrizen. Dann ist das boolesche Produkt  $C = AB$  der beiden Matrizen gegeben durch

$$c_{i,j} = \bigvee_{l=1}^k a_{i,l} \wedge b_{l,j} \quad \text{für } i \in [m], j \in [n]$$

## 2.16 Inzidenzmatrix

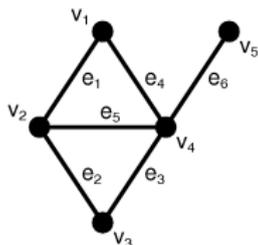
### Definition 282

Sei  $G = (V, E)$  mit  $V = \{v_1, \dots, v_n\}$  und  $E = \{e_1, \dots, e_m\}$ .  
Dann heißt

$$B = (b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \quad \text{mit} \quad b_{i,j} = \begin{cases} 1 & \text{falls } v_i \in e_j \\ 0 & \text{sonst} \end{cases}$$

die **Inzidenzmatrix** von  $G$ .

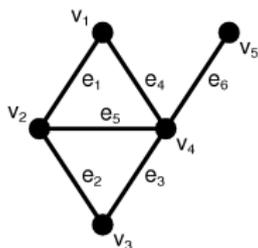
## Beispiel 283 (Adjazenz- und Inzidenzmatrix)



Adjazenzmatrix:

$$A = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 & v_5 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{matrix}$$

## Beispiel (Adjazenz- und Inzidenzmatrix)



Inzidenzmatrix:

$$B = \begin{array}{c} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \\ \left( \begin{array}{cccccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right) \end{array}$$

## Beobachtung:

$$B \cdot B^T = \begin{pmatrix} d(v_1) & & & \\ & d(v_2) & & \\ & & \ddots & \\ 0 & & & d(v_n) \end{pmatrix} + A$$

## 3. Definitionen für gerichtete Graphen

### 3.1 Digraph

#### Definition 284

Ein **Digraph** (aka gerichteter Graph, engl. *directed graph*)  $G = (V, A)$  besteht aus einer Knotenmenge  $V$  und einer Menge  $A \subseteq V \times V$  von geordneten Paaren, den **gerichteten** Kanten.

## 3.2 Grad

### Definition 285

- $d^-(v)$  ist der **Aus-Grad** von  $v$ , d. h. die Anzahl der Kanten mit Anfangsknoten  $v$ .
- $d^+(v)$  ist der **In-Grad** von  $v$ , d. h. die Anzahl der Kanten mit Endknoten  $v$ .
- $d(v) = d^-(v) + d^+(v)$  ist der **(Gesamt-)Grad** von  $v$ .

## Beobachtung:

$$\sum_{v \in V} d^-(v) = \sum_{v \in V} d^+(v) = |A|$$

### 3.3 Adjazenzmatrix

#### Definition 286

Sei  $G = (V, A)$  ein Digraph mit  $V = \{v_1, \dots, v_n\}$ . Dann heißt

$$C = (c_{ij})_{1 \leq i, j \leq n} \quad \text{mit} \quad c_{ij} = \begin{cases} 1 & \text{falls } (v_i, v_j) \in A \\ 0 & \text{sonst} \end{cases}$$

die **Adjazenzmatrix** von  $G$ .

### 3.4 Inzidenzmatrix

#### Definition 287

Sei  $G = (V, A)$  ein einfacher(!) Digraph mit  $V = \{v_1, \dots, v_n\}$  und  $A = \{e_1, \dots, e_m\}$ . Dann heißt

$$B = (b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \text{ mit } b_{ij} = \begin{cases} 1 & \text{falls } v_i \text{ Endknoten von } e_j \\ -1 & \text{falls } v_i \text{ Anfangsknoten von } e_j \\ 0 & \text{sonst} \end{cases}$$

die **Inzidenzmatrix** von  $G$ .

## Beobachtung:

$$B \cdot B^T = \begin{pmatrix} d(v_1) & & & \\ & d(v_2) & & \\ & & \ddots & \\ 0 & & & d(v_n) \end{pmatrix} - A'$$

Diese Matrix heißt **Laplacesche Matrix**. Dabei ist, für alle  $i, j$ , der Eintrag  $a'_{i,j}$  die Anzahl der im zu  $G$  gehörigen **ungerichteten** Graphen zwischen  $v_i$  und  $v_j$  verlaufenden Kanten. Enthält  $G$  keine antiparallelen Kanten, ist damit  $A'$  gleich der Adjazenzmatrix dieses ungerichteten Graphen.

**Beobachtung:** Die Laplacesche Matrix ist symmetrisch.

## 3.5 Gerichteter Pfad

### Definition 288

Eine Folge  $(u_0, u_1, \dots, u_n)$  mit  $u_i \in V$  für  $i = 0, \dots, n$  heißt **gerichteter Pfad**, wenn

$$(\forall i \in \{0, \dots, n-1\}) \left[ (u_i, u_{i+1}) \in A \right].$$

Ein gerichteter Pfad heißt **einfach**, falls alle  $u_i$  paarweise verschieden sind.

## 3.6 Gerichteter Kreis

### Definition 289

Ein gerichteter Pfad  $(u_0, u_1, \dots, u_n)$  heißt **gerichteter Kreis**, wenn  $u_0 = u_n$ .

Der gerichtete Kreis heißt **einfach**, falls  $u_0, u_1, \dots, u_{n-1}$  alle paarweise verschieden sind.

## 3.7 dag

### Definition 290

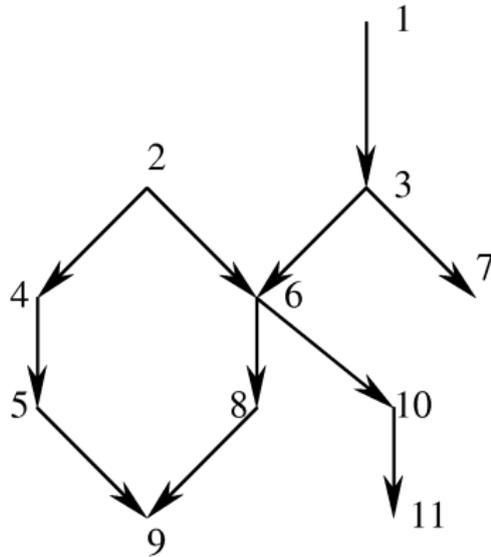
Ein Digraph, der keinen gerichteten Kreis enthält, heißt *directed acyclic graph*, kurz *dag*.

In einem *dag* heißen Knoten mit In-Grad 0 *Quellen*, Knoten mit Aus-Grad 0 *Senken*.

Eine Nummerierung  $i : V \rightarrow \{1, \dots, |V|\}$  der Knoten eines *dags* heißt *topologisch*, falls für jede Kante  $(u, v) \in A$  gilt:

$$i(u) < i(v).$$

## Beispiel 291



Algorithmus zur topologischen Nummerierung:

```
while  $V \neq \emptyset$  do  
    nummeriere eine Quelle mit der nächsten Nummer  
    streiche diese Quelle aus  $V$   
od
```

## 3.8 Zusammenhang

### Definition 292

Ein Digraph heißt **zusammenhängend**, wenn der zugrundeliegende ungerichtete Graph zusammenhängend ist.

## 3.9 Starke Zusammenhangskomponenten

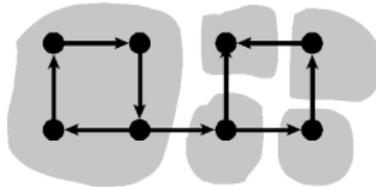
### Definition 293

Sei  $G = (V, A)$  ein Digraph. Man definiert eine Äquivalenzrelation  $R \subseteq V \times V$  wie folgt:

$$uRv \iff \left\{ \begin{array}{l} \text{es gibt in } G \text{ einen gerichteten Pfad von } u \text{ nach } v \\ \text{und einen gerichteten Pfad von } v \text{ nach } u. \end{array} \right.$$

Die von den Äquivalenzklassen dieser Relation induzierten Teilgraphen heißen die **starken Zusammenhangskomponenten von  $G$** .

## Beispiel 294



## 4. Durchsuchen von Graphen

Gesucht sind Prozeduren, die alle Knoten (eventuell auch alle Kanten) mindestens einmal besuchen und möglichst effizient sind.

### 4.1 Tiefensuche, Depth-First-Search

Sei  $G = (V, E)$  ein ungerichteter Graph, gegeben als Adjazenzliste.

algorithm DFS

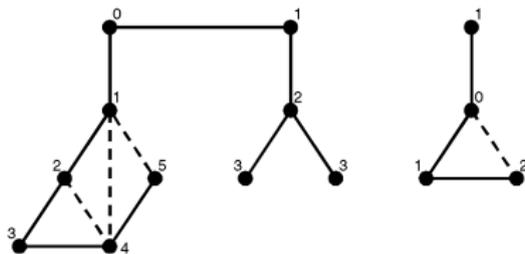
```
void proc DFSvisit(node  $v$ )  
  visited[ $v$ ] := true  
  pre[ $v$ ] := ++precount  
  for all  $u \in$  adjacency_list[ $v$ ] do  
    if not visited[ $u$ ] then  
      type[( $v, u$ )] := 'Baumkante'  
      parent[ $u$ ] :=  $v$   
      DFSlevel[ $u$ ] := DFSlevel[ $v$ ]+1  
      DFSvisit( $u$ )  
    elsif  $u \neq$  parent[ $v$ ] then  
      type[( $v, u$ )] := 'Rückwärtskante'  
    fi  
  od  
  post[ $v$ ] := ++postcount  
end proc
```

## Fortsetzung

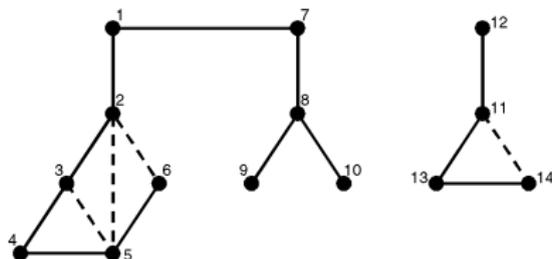
```
co Initialisierung: oc  
for all  $v \in V$  do  
    visited[ $v$ ] := false  
    pre[ $v$ ] := post[ $v$ ] := 0  
od  
precount := postcount := 0  
for all  $v \in V$  do  
    if not visited[ $v$ ] then  
        DFSlevel[ $v$ ] := 0  
        parent[ $v$ ] := null  
        DFSvisit( $v$ )  
    fi  
od  
end
```

## Beispiel 295 (gestrichelt sind Rückwärtskanten)

DFS-Level:

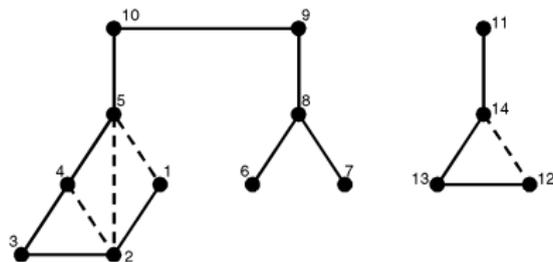


Präorder-Nummer:



## Beispiel (Fortsetzung)

*Postorder-Nummer:*



**Beobachtung:** Die Tiefensuche konstruiert einen Spannwald des Graphen. Die Anzahl der Bäume entspricht der Anzahl der Zusammenhangskomponenten von  $G$ .

### Satz 296

*Der Zeitbedarf für die Tiefensuche ist (bei Verwendung von Adjazenzlisten)*

$$O(|V| + |E|) .$$

### Beweis:

Aus Algorithmus ersichtlich. □

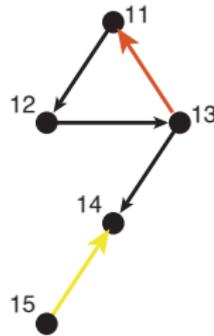
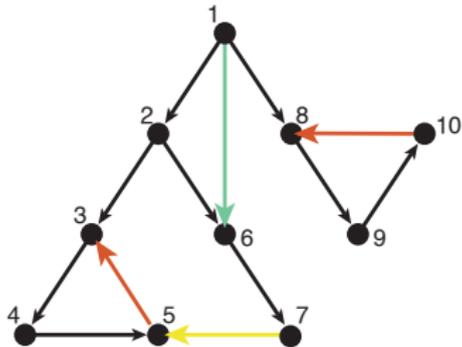
**Tiefensuche im Digraphen:** Für gerichtete Graphen verwendet man obigen Algorithmus, wobei man die Zeilen

```
elseif  $u \neq \text{parent}[v]$  then  
     $\text{type}[(v, u)] := \text{'Rückwärtskante'}$   
fi
```

ersetzt durch

```
elseif  $\text{pre}[u] > \text{pre}[v]$  then  
     $\text{type}[(v, u)] := \text{'Vorwärtskante'}$   
elseif  $\text{post}[u] \neq 0$  then  
     $\text{type}[(v, u)] := \text{'Querkannte'}$   
else  
     $\text{type}[(v, u)] := \text{'Rückwärtskante'}$   
fi
```

## Beispiel 297 (Präorder-Nummer)



## 4.2 Breitensuche, Breadth-First-Search

Sei  $G = (V, E)$  ein ungerichteter Graph, gegeben mittels Adjazenzlisten.

```

algorithm BFS
  for all  $v \in V$  do
    touched[ $v$ ] := false
    bfsNum[ $v$ ] := 0
  od
  count := 0
  queue :=  $\emptyset$ 
  for all  $v \in V$  do
    if not touched[ $v$ ] then
      bfsLevel[ $v$ ] := 0
      parent[ $v$ ] := null
      queue.append( $v$ )
      touched[ $v$ ] := true
    while not empty(queue) do
       $u$  := remove_first(queue)
      bfsNum[ $u$ ] := ++count
    
```

## Fortsetzung

```
for all  $w \in \text{adjacency\_list}[u]$  do  
    if not touched[w] then  
        type[( $u, w$ )] := 'Baumkante'  
        parent[w] :=  $u$   
        bfsLevel[w] := bfsLevel[u]+1  
        queue.append( $w$ )  
        touched[w] := true  
    elsif not  $w = \text{parent}[u]$  then  
        type[( $u, w$ )] := 'Querkante'  
    fi  
od  
od  
fi  
od  
end
```

## Beobachtungen:

- 1 Die Breitensuche konstruiert einen Spannwald.
- 2 Der Spannwald besteht genau aus den Baumkanten im Algorithmus.
- 3  $(u, v)$  ist Querkante  $\Rightarrow |\text{bfsLevel}(u) - \text{bfsLevel}(v)| \leq 1$

## Satz 298

*Der Zeitbedarf für die Breitensuche ist (bei Verwendung von Adjazenzlisten)*

$$O(|V| + |E|) .$$

**Beweis:**

Aus Algorithmus ersichtlich.



## 4.3 Matroide

### Definition 299

Sei  $S$  eine endliche Menge,  $U \subseteq 2^S$  eine Teilmenge der Potenzmenge von  $S$ . Dann heißt  $M = (S, U)$  ein **Matroid** und jedes  $A \in U$  heißt **unabhängige Menge**, falls gilt:

- 1  $\emptyset \in U$
- 2  $A \in U, B \subseteq A \implies B \in U$
- 3

$$A, B \in U, |B| = |A| + 1 \\ \implies (\exists x \in B \setminus A) \left[ (A \cup \{x\}) \in U \right]$$

Jede bezüglich  $\subseteq$  maximale Menge in  $U$  heißt **Basis**.

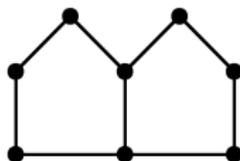
Nach 3. haben je zwei Basen gleiche Kardinalität. Diese heißt der **Rang**  $r(M)$  des Matroids.

## Beispiel 300

Linear unabhängige Vektoren in einem Vektorraum.

## Beispiel 301

$G$  sei folgender Graph:



$S$  = Menge der Kanten von  $G$

$U$  = Menge der kreisfreien Teilmengen von  $S$

## 4.4 Greedy-Algorithmus

Sei  $M = (S, U)$  ein Matroid,  $w : S \rightarrow R$  eine Gewichtsfunktion.

```
algorithm greedy( $S, U, w$ )  
   $B := \emptyset$   
  while ( $|B| < r(M)$ ) do  
    sei  $x \in \{y \in S \setminus B; B \cup \{y\} \in U\}$  mit  
      minimalem Gewicht  
     $B := B \cup \{x\}$   
  od  
end
```

## Satz 302

*Der Greedy-Algorithmus liefert eine Basis minimalen Gewichts.*

## Beweis:

Aus der Definition des Matroids (1.) folgt, dass die leere Menge  $\emptyset$  eine unabhängige Menge ist.

Aus 3. folgt, dass in der while-Schleife wiederum nur unabhängige Mengen generiert werden.

Daher ist  $B$  am Ende des Algorithmus eine Basis (da inklusionsmaximal). Es bleibt zu zeigen, dass die gefundene Basis minimales Gewicht besitzt.

Sei also  $B = \{b_1, \dots, b_r\}$  die vom Algorithmus gelieferte Basis. Sei  $b_1, \dots, b_r$  die Reihenfolge der Elemente, in der sie der Greedy-Algorithmus ausgewählt hat. Dann gilt

$$w(b_1) \leq w(b_2) \leq \dots \leq w(b_r).$$

## Beweis (Forts.):

Sei weiter  $B' = \{b'_1, \dots, b'_r\}$  eine minimale Basis, und es gelte o. B. d. A.

$$w(b'_1) \leq w(b'_2) \leq \dots \leq w(b'_r) .$$

Sei  $i \in \{1, \dots, r\}$ . Gemäß Eigenschaft 3 für Matroide folgt, dass es ein  $b' \in \{b'_1, \dots, b'_i\}$  gibt, so dass  $\{b_1, \dots, b_{i-1}, b'\} \in U$ .

Damit ist  $w(b_i) \leq w(b'_i)$  (für alle  $i$ ), und daher wegen der Minimalität von  $B'$

$$w(b_i) = w(b'_i) \quad \text{für alle } i .$$



## 4.5 Minimale Spannbäume

### Satz 303

Sei  $G = (V, E)$  ein zusammenhängender, ungerichteter Graph,  $F \subseteq 2^E$  die Menge der kreisfreien Teilmengen von  $E$ . Dann ist  $M = (E, F)$  ein Matroid mit Rang  $|V| - 1$ .

### Beweis:

Es sind die drei Eigenschaften eines Matroids zu zeigen.

- 1  $\emptyset$  ist kreisfrei und daher in  $F$  enthalten.
- 2 Ist  $A$  kreisfrei und  $B$  eine Teilmenge von  $A$ , dann ist auch  $B$  kreisfrei.

## Beweis (Forts.):

- 3 Sind  $A$  und  $B$  kreisfrei,  $|B| = |A| + 1$ , dann existiert ein  $b \in B$ , so dass  $A \cup \{b\}$  kreisfrei ist:

Wir betrachten die Walder  $(V, A)$  (mit  $|A|$  Kanten und  $|V| - |A|$  Zusammenhangskomponenten) und  $(V, B)$  (mit  $|B|$  Kanten und  $|V| - |B|$  Zusammenhangskomponenten). Diese Bedingungen lassen zwei Moglichkeiten zu:

- 1 Es existiert eine Kante  $e$  in  $B$ , die zwei Zusammenhangskomponenten in  $(V, A)$  verbindet. Damit ist  $A \cup \{e\}$  kreisfrei.
- 2 Alle Kanten in  $B$  verlaufen innerhalb der Zusammenhangskomponenten in  $(V, A)$ .  $(V, A)$  besitzt jedoch eine Zusammenhangskomponente mehr als  $(V, B)$ . Daher muss es eine Zusammenhangskomponente in  $(V, A)$  geben, deren Knoten nicht in  $(V, B)$  auftauchen, was einen Widerspruch darstellt.



## Kruskals Algorithmus:

```
algorithm kruskal
  sortiere  $E$  aufsteigend:  $w(e_1) \leq \dots \leq w(e_m)$ .
   $F := \emptyset$ 
   $i := 0$ 
  while  $|F| < |V| - 1$  do
     $i++$ 
    if  $F \cup \{e_i\}$  kreisfrei then
       $F := F \cup \{e_i\}$ 
    fi
  od
end
```

## Satz 304

Kruskals Algorithmus bestimmt (bei geeigneter Implementierung) einen minimalen Spannbaum für  $G = (V, E)$  in Zeit  $O(|E| \cdot \log(|V|))$ .

### Beweis:

Die Korrektheit folgt aus Satz 303.

Zur Laufzeit:

Die Sortierung von  $E$  nach aufsteigendem Gewicht benötigt

$$O(|E| \cdot \log(|E|)),$$

z. B. mit Heapsort oder Mergesort.

Da  $|E| \leq (|V|)^2$ , gilt auch

$$O(|E| \cdot \log(|V|))$$

als Zeitbedarf für das Sortieren.

## Implementierung des Tests auf Kreisfreiheit:

Repräsentation der Zusammenhangskomponenten:

Feld  $Z$ :  $Z[i]$  ist die Zusammenhangskomponente des Knoten  $i$ .

Feld  $N$ :  $N[j]$  ist die Anzahl der Knoten in der Zusammenhangskomponente  $j$ .

Feld  $M$ :  $M[j]$  ist eine Liste mit den Knoten in der Zusammenhangskomponente  $j$ .

```
co Initialisierung oc  
for all  $i \in V$  do  
     $Z[i] := i$   
     $N[i] := 1$   
     $M[i] := (i)$   
od  
co Test auf Kreisfreiheit oc  
sei  $e := \{i, j\}$ 
```

## Fortsetzung

```
co  $F \cup \{e\}$  kreisfrei  $\Leftrightarrow Z[i] \neq Z[j]$  oc  
if  $Z[i] \neq Z[j]$  then  
  if  $N[Z[i]] \leq N[Z[j]]$  then  
     $BigSet := Z[j]$   
     $SmallSet := Z[i]$   
  else  
     $BigSet := Z[i]$   
     $SmallSet := Z[j]$   
  fi  
   $N[BigSet] := N[BigSet] + N[SmallSet]$   
  for all  $k \in M[SmallSet]$  do  
     $Z[k] := BigSet$   
  od  
  hänge  $M[SmallSet]$  an  $M[BigSet]$  an  
fi
```

## Beweis (Forts.):

Zeitbedarf für den Test:  $O(1)$  für jede Abfrage, damit dafür insgesamt

$$O(|E|).$$

Zeitbedarf für das Umbenennen der Zusammenhangskomponenten: Nach jedem Umbenennen befindet sich ein Knoten in einer mindestens doppelt so großen Zusammenhangskomponente. Daher ist die Anzahl der Umbenennungen je Knoten  $\leq \log(|V|)$ . Für das Umbenennen aller Knoten benötigt man dann

$$O(|V| \cdot \log(|V|)).$$



**Bemerkung:**

Es gibt Algorithmen für minimale Spannbäume der Komplexität  $O(m + n \cdot \log n)$   
und, für dünnbesetzte Graphen, der Komplexität  $O(m \cdot \log^* n)$ ,  
wobei

$$\log^* x = \min_{n \in \mathbb{N}} \left\{ n : \underbrace{\log(\log(\dots \log(x) \dots))}_n < 1 \right\}.$$

## 5. Spezielle Pfade

### 5.1 Eulersche Pfade und Kreise

#### Definition 305

Ein Pfad bzw. Kreis in einem Graphen (Digraphen) heißt **eulersch**, wenn er jede Kante des Graphen genau einmal enthält.

Ein Graph (Digraph) heißt **eulersch**, wenn er einen eulerschen Kreis enthält.

#### Satz 306

*Ein Graph besitzt genau dann einen eulerschen Kreis (Pfad), wenn er zusammenhängend ist und alle (alle bis auf zwei) Knoten geraden Grad haben.*

## Beweis:

„ $\Rightarrow$ “

Ein eulerscher Graph muss notwendigerweise zusammenhängend sein. Die Knotengrade müssen gerade sein, da für jede zu einem Knoten (auf dem eulerschen Kreis) hinführende Kante auch eine von diesem Knoten weiterführende Kante existieren muss, da sonst der eulersche Kreis nicht fortgeführt werden kann.

## Beweis (Forts.):

„ $\Leftarrow$ “

Konstruktion des eulerschen Kreises: Man suche einen beliebigen Kreis im Graphen (muss aufgrund der Voraussetzungen existieren). Sind noch Kanten unberücksichtigt, suche man auf dem Kreis einen Knoten, der zu noch nicht verwendeten Kanten inzident ist.

Nach Voraussetzung muss sich wieder ein Kreis finden lassen, der vollständig aus noch nicht berücksichtigten Kanten besteht. Diesen füge man zum bereits gefundenen Kreis hinzu, worauf sich ein neuer Kreis ergibt.

Dieses Verfahren läßt sich fortführen, bis keine Kanten mehr unberücksichtigt sind und damit ein eulerscher Kreis gefunden ist.



## Satz 307

*Ein Digraph besitzt genau dann einen eulerschen Kreis (Pfad), wenn er stark zusammenhängend ist und für alle Knoten der In-Grad gleich dem Aus-Grad ist (wenn für einen Knoten  $\text{In-Grad} = \text{Aus-Grad} - 1$ , für einen weiteren Knoten  $\text{In-Grad} = \text{Aus-Grad} + 1$  gilt und für alle anderen Knoten der In-Grad gleich dem Aus-Grad ist).*

### Beweis:

Der Beweis ist analog zum Beweis des vorhergehenden Satzes. □

## Algorithmus zum Finden eines eulerschen Kreises:

```
algorithm Eulerian_Circle( $V, E$ )  
   $EC := \emptyset$   
  select  $v = v_0 \in V$   
  do  
     $C := \emptyset$   
    while  $N(v) \neq \emptyset$  do  
      select  $w \in N(v)$   
       $E := E \setminus \{v, w\}$   
       $C := C \cup \{v, w\}$   
      if  $N(v) \neq \emptyset$  then  $Q.add(v)$  fi  
       $v := w$   
    od  
  co Neuer Kreis oc  
  if  $C \neq \emptyset$  then  $EC := EC \cup C$  fi
```

## Fortsetzung

```
if not empty( $Q$ ) then  
     $v := Q.remove()$   
fi  
until  $E = \emptyset$   
end
```

Laufzeit des Algorithmus:  $\Theta(|E|)$ .

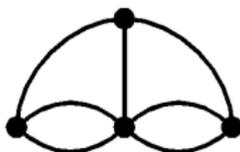
Laufzeit der while-Schleife:  $O(|E|)$ , der do-until-Schleife ohne Durchlaufen der while-Schleife:  $O(|V|)$  und damit ebenfalls  $O(|E|)$ , da der Graph zusammenhängend ist.

## 5.2 Hamiltonsche Pfade

Ein Pfad (Kreis) in einem Graphen (Digraphen) heißt **hamiltonsch**, wenn er jeden Knoten genau einmal enthält.

Ein Graph (Digraph) heißt **hamiltonsch**, wenn er einen hamiltonschen Kreis enthält.

### Beispiel 308 (Das Königsberger Brückenproblem)



Dieser Graph besitzt einen hamiltonschen Kreis, aber weder einen eulerschen Kreis noch einen eulerschen Pfad.

Die Aufgabe, einen hamiltonschen Kreis zu finden, ist wesentlich schwerer als einen eulerschen Kreis zu finden; es ist ein  $\mathcal{NP}$ -vollständiges Problem.

## 6. Kürzeste Wege

Gegeben sind ein (Di)Graph  $G = (V, E)$  und eine Gewichtsfunktion  $w : E \rightarrow \mathbb{R}^+ \cup \{+\infty\}$ . O. B. d. A. sei  $G$  vollständig, damit auch zusammenhängend.

Sei  $u = v_0, v_1, v_2, \dots, v_n = v$  ein Pfad in  $G$ . Die Länge dieses Pfades ist

$$\sum_{i=0}^{n-1} w(v_i, v_{i+1}).$$

$d(u, v)$  sei die Länge eines kürzesten Pfades von  $u$  nach  $v$ .

## Problemstellungen:

- 1 Gegeben  $u, v \in V$ , berechne  $d(u, v)$ .
- 2 Gegeben  $u \in V$ , berechne für alle  $v \in V$  die Länge  $d(u, v)$  eines kürzesten Pfades von  $u$  nach  $v$  (sssp, single source shortest path).
- 3 Berechne für alle  $(u, v) \in V^2$  die kürzeste Entfernung  $d(u, v)$  (apsp, all pairs shortest path).

## 6.1 Der Floyd-Warshall-Algorithmus für apsp

Gegeben sind ein (Di)Graph  $G = (V, E)$  und eine Gewichtsfunktion  $w : E \rightarrow \mathbb{R}^+ \cup \{+\infty\}$ . Sei o. B. d. A.  $V = \{0, \dots, n-1\}$ . Eine Gewichtsmatrix ist wie folgt definiert:

$$D = (w(v_i, v_j))_{\substack{0 \leq i < n \\ 0 \leq j < n}}$$

Ziel ist es, eine  $n \times n$ -Matrix mit den Einträgen

$$d_{ij} = \text{Länge eines kürzesten Weges von } i \text{ nach } j$$

zu berechnen. Dazu werden induktiv Matrizen  $D^{(k)}$  mit Einträgen

$$d_{ij}^{(k)} = \left( \begin{array}{l} \text{Länge eines kürzesten Weges von } i \text{ nach } j, \\ \text{so dass alle inneren Knoten } < k \text{ sind} \end{array} \right)$$

erzeugt.

```

algorithm Floyd
  for  $i=0$  to  $n-1$  do
    for  $j=0$  to  $n-1$  do
       $D^0[i, j] := w(v_i, v_j)$ 
    od
  od
  for  $k=0$  to  $n-1$  do
    for  $i=0$  to  $n-1$  do
      for  $j=0$  to  $n-1$  do
         $D^{k+1}[i, j] := \min\{D^k[i, j],$ 
                                $D^k[i, k]+D^k[k, j]\}$ 
      od
    od
  od
end

```

## Satz 309

*Der Floyd-Algorithmus berechnet für alle  $u, v \in V^2$  die Länge eines kürzesten Weges zwischen  $u$  und  $v$ , und zwar mit Zeitbedarf  $\Theta(n^3)$  und Platzbedarf  $\Theta(n^2)$ .*

### Beweis:

Ersichtlich aus Algorithmus.



## Bemerkungen:

- 1 Zur Bestimmung der eigentlichen Pfade (und nicht nur der Entfernungen) muss bei der Minimum-Bestimmung jeweils das  $k$  gespeichert werden.
- 2 Der Algorithmus funktioniert auch, wenn *negative Kantengewichte* vorhanden sind, es jedoch keine *negativen Kreise* gibt.
- 3 Die Erweiterung auf Digraphen ist offensichtlich.

## 6.2 Dijkstras Algorithmus für sssp

Gegeben sind ein (Di)Graph  $G = (V, E)$ , ein Knoten  $s \in V$  und eine Gewichtsfunktion  $w : E \rightarrow \mathbb{R}^+ \cup \{\infty\}$ .

algorithm Dijkstra

$F := V \setminus \{s\}$

for all  $v \in F$  do  $d[v] := w(s, v)$  od

co  $d[s] = 0$  oc

while  $F \neq \emptyset$  do

bestimme  $v \in F$  mit  $d[v]$  minimal

$F := F \setminus \{v\}$

for all  $w \in N(v)$  do

$d[w] := \min\{d[w], d[v] + w(v, w)\}$

od

od

end

## Satz 310

*Dijkstras Algorithmus berechnet  $d(s, v)$  für alle  $v \in V$ ; der Zeitaufwand ist  $O(n^2)$ , der Platzbedarf  $O(n + m)$ .*

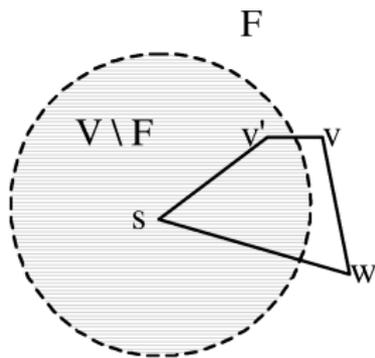
### Beweis:

Zeit- und Platzbedarf sind aus dem Algorithmus ersichtlich. Die Korrektheit zeigen wir mit einem Widerspruchsbeweis:

Annahme:  $v$  sei der erste Knoten, so dass  $d(s, v)$  falsch (d. h. zu groß) berechnet wird.

## Beweis (Forts.):

Diese Situation illustriert folgendes Bild:



Nach Annahme muss dann gelten:

$$d(w) + w(w, v) < d(s, v') + d(v', v) = d(v) .$$

Damit wäre  $d(w)$  aber kleiner als  $d(v)$ , und der Algorithmus hätte  $w$  und nicht  $v$  gewählt. □

### **Bemerkung:**

Mit besseren Datenstrukturen (**priority queues** – z. B. **Fibonacci heaps**) kann Dijkstras Algorithmus so implementiert werden, dass er z. B. in Zeit  $O(m + n \cdot \log n)$  läuft.

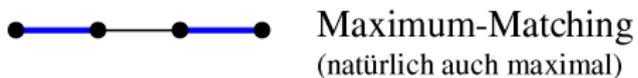
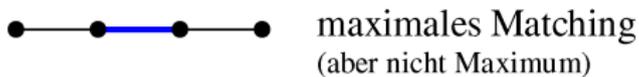
## 7. Matchings

### Definition 311

Sei  $G = (V, E)$  ein Graph.

- 1  $M \subseteq E$  heißt **Matching**, falls alle Kanten in  $M$  paarweise disjunkt sind.
- 2  $M$  heißt **maximales Matching**, falls es kein Matching  $M'$  in  $G$  gibt mit  $M \subsetneq M'$ .
- 3  $M$  heißt **Matching maximaler Kardinalität** (aka **Maximum Matching**), falls es in  $G$  kein Matching  $M'$  mit  $|M'| > |M|$  gibt.
- 4  $m(G)$  ist die Kardinalität eines Maximum Matchings in  $G$ .

## Beispiel 312



## 7.1 Matchings in bipartiten Graphen

### Satz 313 („Heiratssatz“)

Sei  $G = (U, V, E)$  ein bipartiter Graph. Dann ist  $m(G) = |U|$  genau dann, wenn gilt:

$$(\forall A \subseteq U) [|A| \leq |N(A)|]$$

Beweis:

„ $\Rightarrow$ “

Offensichtlich.

„ $\Leftarrow$ “

Sei  $M$  ein Maximum Matching in  $G$ .

Annahme: Ein Knoten  $u = u_0 \in U$  sei in  $M$  ungematcht.

Wir beginnen in  $u_0$  eine BFS, wobei wir in den ungeraden Schichten (also von  $U$  aus) nur ungematchte und in den geraden Schichten (also von  $V$  aus) nur gematchte Kanten verwenden. Querkanten bleiben außer Betracht.

**Fall 1:** Die BFS findet in  $V$  einen ungematchten Knoten  $v$ . Dann stoppen wir.

**Fall 2:** Nach Vollendung einer geraden Schicht (mit gematchten Kanten) sind alle Blätter des BFS-Baums gematcht. Seien  $U'$  (bzw.  $V'$ ) die Knoten des aktuellen BFS-Baums in  $U$  (bzw.  $V$ ). Gemäß Annahme ist  $|U'| > |V'|$ , die alternierende BFS kann also fortgesetzt werden. Da  $G$  endlich ist, muss schließlich Fall 1 eintreten.

## Beweis (Forts.):

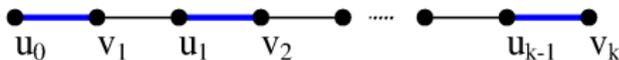
„ $\Leftarrow$ “ (Fortsetzung)

Also existiert per Konstruktion ein Pfad wie in folgender Abbildung:



Ein solcher Pfad, bei dem sich gematchte und ungematchte Kanten abwechseln, heißt **alternierender** Pfad. Sind, wie hier, Anfangs- und Endknoten ungematcht, heißt der Pfad auch **augmentierend**.

Vertauscht man auf diesem Pfad gematchte und ungematchte Kanten, erhält man dadurch ein Matching  $M'$  mit  $|M'| = |M| + 1$ , was wiederum einen Widerspruch darstellt:



## Definition 314

Man definiert für einen bipartiten Graphen  $G = (U, V, E)$  die Kenngröße:

$$\delta := \delta(G) := \max_{A \subseteq U} \{|A| - |N(A)|\}$$

Da bei der Maximumsbildung auch  $A = \emptyset$  sein kann, ist  $\delta \geq 0$ .

## Satz 315

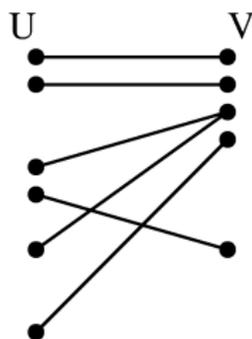
*Es gilt:*

$$m(G) = |U| - \delta .$$

## Beweis:

Dass  $m(G) \leq |U| - \delta$  gilt, ist offensichtlich. Wir zeigen nun noch, dass auch  $m(G) \geq |U| - \delta$  gilt, damit ist der Satz bewiesen.

Betrachte folgenden Graphen:



Man fügt nun  $\delta$  neue Knoten hinzu. Von diesen gehen Kanten zu allen Knoten in  $U$ , so dass ein  $K_{|U|,\delta}$  entsteht.

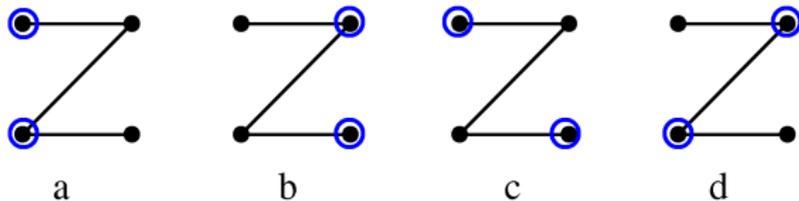
### Beweis (Forts.):

Der neue Graph erfüllt die Voraussetzungen des Heiratssatzes.  
Damit gibt es im neuen Graphen ein Matching  $M'$  mit  $|M'| = |U|$ .  
Daraus folgt, dass es im alten Graphen ein Matching der  
Kardinalität  $\geq |U| - \delta$  geben muss. □

## Definition 316

$D \subseteq U \uplus V$  heißt **Träger** oder **Knotenüberdeckung** (*vertex cover*, *VC*) von  $G$ , wenn jede Kante in  $G$  zu mindestens einem  $u \in D$  inzident ist.

## Beispiel 317



In den Fällen a, b und d sind Träger gezeigt, in c nicht.

## Satz 318

*Es gilt:*

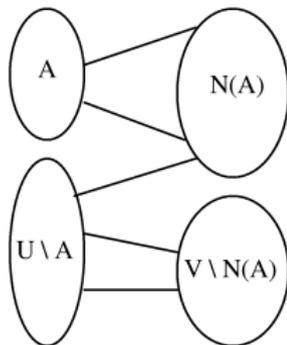
$$\max\{|M|; M \text{ Matching}\} = \min\{|D|; D \text{ Träger}\}$$

## Beweis:

„ $\leq$ “ Offensichtlich.

„ $\geq$ “ Für ein geeignetes  $A \subseteq U$  gilt

$$m(G) = |U| - \delta(G) = |U \setminus A| + |N(A)|:$$



$(U \setminus A) \cup N(A)$  ist Träger von  $G$ .



Sei

$$M = (m_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$$

eine (quadratische) Matrix mit  $m_{ij} \geq 0$ . Alle Zeilen- und Spaltensummen von  $M$  seien gleich  $r > 0$ .

Man ordnet nun  $M$  den bipartiten Graphen  $G = (U, V, E)$  zu mit

$$U = \{u_1, \dots, u_n\}, V = \{v_1, \dots, v_n\} \text{ und } \{u_i, v_j\} \in E \Leftrightarrow m_{ij} > 0.$$

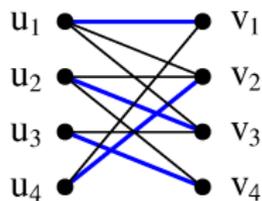
Ein Matching in  $G$  entspricht einer Menge von Positionen in  $M$ , die alle in verschiedenen Zeilen und Spalten liegen.

## Beispiel 319

Die Matrix

$$\begin{pmatrix} \boxed{3} & 1 & 1 & 0 \\ 0 & 1 & \boxed{2} & 2 \\ 0 & 0 & 2 & \boxed{3} \\ 2 & \boxed{3} & 0 & 0 \end{pmatrix}$$

entspricht dem Graphen



### Bemerkung:

Ein Träger  $D$  von  $G$  ist also eine Menge von Zeilen und Spalten von  $M$ , die zusammen alle Einträge  $m_{ij} > 0$  enthalten.

### Definition 320

Eine Menge von Positionen (in  $M$ ), die alle in verschiedenen Zeilen und in verschiedenen Spalten liegen, heißt **Diagonale** von  $M$ .

Eine Diagonale der Größe  $n$  muss in  $M$  existieren, denn falls  $M$  keine solche Diagonale hat, gibt es nach Satz 318  $e$  Zeilen und  $f$  Spalten mit  $e + f < n$ , die zusammen alle Einträge  $> 0$  von  $M$  enthalten.

Die Gesamtsumme der Einträge in  $M$  wäre dann

$$n \cdot r = \sum_{i,j} m_{ij} \leq (e + f) \cdot r < r \cdot n,$$

was offensichtlich ein Widerspruch ist.

Sei  $c_1$  der minimale Eintrag  $> 0$  in  $M$ , und sei  $P_1$  die zu einer Diagonale der Größe  $n$  gehörige Permutationsmatrix (d. h. Einträge  $= 1$  an den Positionen der Diagonale,  $0$  sonst).

Dann gilt:

$$M_1 := M - c_1 P_1$$

ist eine  $n \times n$ -Matrix mit allen Zeilen- und Spaltensummen  $= r - c_1$ . Die Matrix  $M_1$  enthält damit mehr Nullen als  $M$ .

Damit haben wir gezeigt:

## Satz 321

Sei  $M$  wie oben. Dann gibt es für ein geeignetes  $k$  Konstanten  $c_i > 0$  und Permutationsmatrizen  $P_i$ ,  $i = 1, \dots, k$ , so dass gilt

$$M = \sum_{i=1}^k c_i P_i \quad \sum_{i=1}^k c_i = r .$$

## 7.2 Konstruktion optimaler Matchings

### Satz 322

Ein Matching  $M$  ist genau dann Maximum, wenn es dazu keinen augmentierenden Pfad gibt.

#### Beweis:

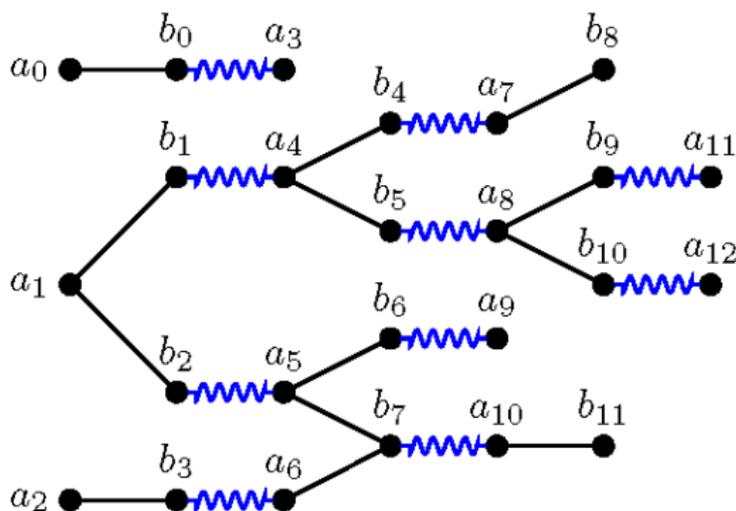
„ $\Rightarrow$ “ Offensichtlich.

„ $\Leftarrow$ “ Sei  $M$  ein Matching, zu dem es keinen augmentierenden Pfad gibt. Annahme,  $M$  sei kein Maximum Matching, es existiere ein Maximum Matching  $M'$ . Betrachte nun  $M \Delta M'$ . Die Zusammenhangskomponenten dieses Graphen sind alternierende Pfade und Kreise gerader Länge. Da  $|M'| > |M|$  gilt, muss es einen alternierenden Pfad mit ungerader Länge geben, der mit Kanten aus  $M'$  beginnt und endet. Dies ist aber ein *augmentierender* Pfad.



Der Algorithmus zur Konstruktion optimaler Matchings ist eine parallele (simultane) alternierende Breitensuche.

### Beispiel 323 (Konstruktion im bipartiten Graph)



## Ergebnisse und Erweiterungen:

	bipartit	allgemein
ungewichtet	$O(\sqrt{ V } \cdot  E )$	$O(\sqrt{ V } \cdot  E )$
gewichtet	$O( V  \cdot ( E  +  V  \cdot \log( V )))$	$O( V  \cdot  E  \cdot \log( V ))$

Siehe auch:

Zvi Galil: Efficient algorithms for finding maximum matchings in graphs, ACM Computing Surveys 18 (1986), pp. 23–38

## 7.3 Reguläre bipartite Graphen

### Lemma 324

Sei  $G = (U, V, E)$  ein  $k$ -regulärer bipartiter Graph ( $k \in \mathbb{N}$ ). Dann hat  $G$  ein perfektes Matching.

### Beweis:

Sei  $A \subseteq U$  und  $B = N(A) \subseteq V$ . Dann ist  $|A| \leq |B|$ , da ja alle von  $A$  ausgehenden Kanten in  $B$  enden und, falls  $|B| < |A|$ , es in  $B$  damit einen Knoten mit Grad  $> k$  geben müsste.  $\square$

### Korollar 325

Sei  $G = (U, V, E)$  ein  $k$ -regulärer bipartiter Graph ( $k \in \mathbb{N}$ ). Dann lässt sich  $E$  als disjunkte Vereinigung von  $k$  perfekten Matchings darstellen.

## 7.4 Transversalen

### Definition 326

Sei  $G = (U, V, E)$  ein bipartiter Graph,  $M$  ein Matching in  $G$ , und  $A \subseteq U$  die in  $M$  gematchte Teilmenge der Knotenmenge  $U$ . Dann heißt  $A$  eine **Transversale** in  $G$ .

### Satz 327

Sei  $G = (U, V, E)$  ein bipartiter Graph,  $\mathcal{T} \subseteq 2^U$  die Menge der Transversalen in  $G$ . Dann ist  $(U, \mathcal{T})$  ein Matroid.

### Beweis:

Die ersten beiden Bedingungen für ein Matroid sind klarerweise erfüllt:

- 1  $\emptyset \in \mathcal{T}$
- 2  $B \subset A, A \in \mathcal{T} \Rightarrow B \in \mathcal{T}$

## Beweis (Forts.):

Seien nun  $A$  und  $A'$  Transversalen mit den zugehörigen Matchings  $M$  und  $M'$ , und sei  $|A'| = |A| + 1$ , also auch  $|M'| = |M| + 1$ . Betrachte  $M' \Delta M$ .

Dann muss  $M' \Delta M$  (mindestens) einen Pfad ungerader Länge enthalten, der mit einer Kante in  $M'$  beginnt und mit einer Kante in  $M$  endet (und dazwischen abwechselnd Kanten in  $M$  bzw.  $M'$  enthält). Dieser Pfad ist ein augmentierender Pfad bzgl.  $M$ , und einer der beiden Endpunkte liegt in  $A' \setminus A$ , kann also zu  $A$  hinzugenommen werden. □

## Anwendung: gewichtetes Zuweisungsproblem, Variante 1

$n$  Nutzer wollen jeweils auf eine aus einer nutzerspezifischen Teilmenge von insgesamt  $m$  Ressourcen zugreifen. Jede Ressource kann aber nur von höchstens einem Nutzer in Anspruch genommen werden. Der Wert einer Zuweisung von Ressourcen zu (interessierten) Nutzern ergibt sich als die Summe

$$\sum_{i \in A} w_i ,$$

wobei die Zuweisung einem Matching in dem durch Nutzer, Ressourcen und Zugriffswünsche gegebenen Graphen entspricht,  $w_i \in \mathbb{R}^+$  ein Gewicht für jeden Nutzer  $i \in \{1, \dots, n\}$  ist, und  $A$  die durch die Zuweisung (das Matching) bedachte Teilmenge der Nutzer ist.

## 7.5 Gewichtetes Matching in bipartiten Graphen

Wir betrachten nun eine zweite Variante eines **Zuweisungsproblems**, das durch bipartite Graphen  $G = (U, V, E)$  mit einer Gewichtsfunktion  $w : E \rightarrow \mathbb{R}^+$  gegeben ist. Das Gewicht eines Matchings  $M \subseteq E$  ist dann

$$\sum_{e \in M} w(e) .$$

Wir können o.B.d.A. annehmen, dass  $|U| = |V| (= n)$  und  $G$  vollständig bipartit (also  $G = K_{n,n}$ ) ist, indem wir zunächst die kleinere der beiden Mengen  $U$  und  $V$  mit zusätzlichen Knoten auffüllen und dann die fehlenden Kanten durch Kanten mit Gewicht 0 ersetzen.

Damit suchen wir in  $G$  *optimale perfekte Matchings*. Wir können das Problem, ein perfektes Matching **maximalen** Gewichts zu finden, reduzieren auf das Problem, ein perfektes Matching **minimalen** Gewichts zu bestimmen, indem wir jedes Gewicht  $w(e)$  durch

$$\max_{e \in E} w(e) - w(e)$$

ersetzen.

Wir nehmen daher an, dass wir o.B.d.A. ein perfektes Matching minimalen Gewichts in  $(G, w)$  suchen.

Für die folgende Diskussion nehmen wir zur Vereinfachung weiter an, dass alle Gewichte  $\in \mathbb{N}_0$  sind.

Sei

$$W = (w_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$$

die zu  $(G, w)$  gehörige Gewichtsmatrix, und sei

$$P = (p_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$$

eine Permutationsmatrix (d.h., jede Zeile und jede Spalte von  $P$  enthält genau eine 1 und ansonsten nur Einträge 0).

Die Permutationsmatrix  $P$  entspricht einem perfekten Matching  $M$  in  $G$  mit Gewicht

$$\sum_{i,j} p_{ij} w_{ij} .$$

## Beobachtung:

Wenn wir von jedem Element einer Zeile (oder Spalte) in  $W$  einen festen Betrag  $p$  subtrahieren, verringert sich das Gewicht eines jeden perfekten Matchings  $M$  um diesen Betrag  $p$ , die relative Ordnung (nach Gewicht) unter den perfekten Matchings bleibt bestehen, insbesondere gehen optimale Matchings wieder in optimale Matchings über.

Wir führen nun solche Zeilen- und Spaltenumformungen durch, um eine **Diagonale** mit möglichst vielen Einträgen  $= 0$  zu erhalten.

## Beispiel 328

Sei

$$W = \begin{pmatrix} 9 & 11 & 12 & 11 \\ 6 & 3 & 8 & 5 \\ 7 & 6 & 13 & 11 \\ 9 & 10 & 10 & 7 \end{pmatrix}$$

Nachdem wir von jeder Zeile das minimale Gewicht subtrahieren, erhalten wir

$$W' = \begin{pmatrix} 0 & 2 & 3 & 2 \\ 3 & 0 & 5 & 2 \\ 1 & 0 & 7 & 5 \\ 2 & 3 & 3 & 0 \end{pmatrix}$$

## Beispiel (Forts.)

$$W' = \begin{pmatrix} 0 & 2 & 3 & 2 \\ 3 & 0 & 5 & 2 \\ 1 & 0 & 7 & 5 \\ 2 & 3 & 3 & 0 \end{pmatrix}$$

*Nachdem wir von jeder Spalte das minimale Gewicht subtrahieren, erhalten wir*

$$W'' = \begin{pmatrix} 0 & 2 & 0 & 2 \\ 3 & 0 & 2 & 2 \\ 1 & 0 & 4 & 5 \\ 2 & 3 & 0 & 0 \end{pmatrix}$$

## Beispiel (Forts.)

Diese Matrix enthält eine Diagonale der Größe 3 mit Einträgen = 0:

$$W'' = \begin{pmatrix} \boxed{0} & 2 & 0 & 2 \\ 3 & 0 & 2 & 2 \\ 1 & \boxed{0} & 4 & 5 \\ 2 & 3 & \boxed{0} & 0 \end{pmatrix}$$

Aus Satz 318 folgt, dass die maximale Länge einer 0-Diagonale gleich der minimalen Anzahl von Zeilen und Spalten ist, die alle 0en bedecken.

Falls wir noch keine 0-Diagonale der Länge  $n$  haben, iterieren wir folgenden Algorithmus:

- 1 finde eine minimale Anzahl von  $e$  Zeilen und  $f$  Spalten ( $e + f < n$ ), die zusammen alle Einträge  $= 0$  enthalten;
- 2 sei  $w$  das Minimum der nicht überdeckten Elemente;
- 3 subtrahiere  $w$  von den  $n - e$  nicht überdeckten Zeilen;
- 4 addiere  $w$  zu den  $f$  überdeckten Spalten.

Die Gewichte ändern sich also wie folgt:

- 1 um  $-w$ , falls  $(i, j)$  nicht überdeckt ist;
- 2 um 0, falls  $(i, j)$  von einer Zeile *oder* Spalte überdeckt ist, aber nicht beides;
- 3 um  $+w$ , falls  $(i, j)$  von einer Zeile *und* einer Spalte überdeckt ist.

Insbesondere sind die resultierenden Gewichte wieder  $\geq 0$ .  
Die Anzahl der doppelt (von Zeilen *und* Spalten) überdeckten Positionen ist  $e \cdot f$ , die Anzahl der nicht überdeckten Positionen ist

$$n^2 - n(e + f) + ef .$$

Der resultierende Gewichtsunterschied ist daher

$$\begin{aligned} \Delta w &= (ef)w - (n^2 - n(e + f) + ef)w \\ &= (n(e + f) - n^2)w < 0 \end{aligned}$$

Damit muss unsere Iteration enden und wir finden eine 0-Diagonale der Länge  $n$ , entsprechend einer optimalen Zuordnung.

## Beispiel (Forts.)

In unserem Beispiel ergibt sich

$$W'' = \begin{pmatrix} \boxed{0} & \boxed{2} & \boxed{0} & \boxed{2} \\ 3 & \boxed{0} & 2 & 2 \\ 1 & \boxed{0} & 4 & 5 \\ \boxed{2} & \boxed{3} & \boxed{0} & \boxed{0} \end{pmatrix}$$

Der Algorithmus bestimmt  $w = 1$ :

$$\Rightarrow \begin{pmatrix} \boxed{0} & 2 & 0 & 2 \\ \boxed{2} & \boxed{-1} & 1 & 1 \\ \boxed{0} & -1 & 3 & 4 \\ 2 & 3 & 0 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 3 & \boxed{0} & 2 \\ 2 & \boxed{0} & 1 & 1 \\ \boxed{0} & 0 & 3 & 4 \\ 2 & 4 & 0 & \boxed{0} \end{pmatrix}$$

## Beispiel (Forts.)

In dem durch die Matrix

$$W = \begin{pmatrix} 9 & 11 & \boxed{12} & 11 \\ 6 & \boxed{3} & 8 & 5 \\ \boxed{7} & 6 & 13 & 11 \\ 9 & 10 & 10 & \boxed{7} \end{pmatrix}$$

gegebenen bipartiten Graphen hat also das durch die markierten Kanten gegebene perfekte Matching minimales Gewicht.

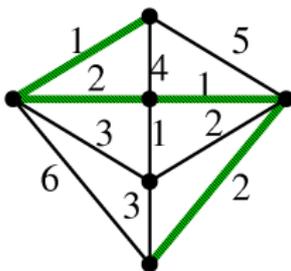
**Bemerkung:** Bei geeigneter Implementierung ist die Laufzeit des Algorithmus  $O(n^3)$ .

## 7.6 Das Problem des chinesischen Postboten

Gegeben ist ein zusammenhängender, gewichteter Multigraph  $G = (V, E, w)$ .

Gesucht ist ein Kreis minimalen Gewichts, der jede Kante mindestens einmal enthält.

Beispiel 329 (In der optimalen Lösung werden die dickeren grünen Kanten zweimal verwendet)



**Algorithmus:** Sei  $U$  die Menge der Knoten ungeraden Grades,  $|U| = 2k$ .

- 1 Bestimme  $d(u, v)$  für alle  $u, v \in U$ .
- 2 Bestimme auf dem  $K_{2k}$  mit Kantengewichtung  $w(\{u, v\}) = d(u, v)$  ein perfektes Matching  $M$  minimalen Gewichts.
- 3 Füge die den Kanten in  $M$  entsprechenden kürzesten Pfade in  $G$  ein und bestimme im resultierenden Graphen einen Eulerkreis. Dieser ist eine Lösung.