

---

**RWTH Aachen**  
**Sommersemester 2002**  
**Diskrete Strukturen**  
**Priv.-Doz. Dr. Y. Guo**

郭余宝

---

**Mitschrift von Mark Wiesemann,**  
**Florian Schröder, Volker Krause,**  
**Tobias Lohmann und Christian Lücking**  
Stand: 7. März 2003

---

Hinweise auf evt. Fehler bitte an  
[post@mark-wiesemann.de](mailto:post@mark-wiesemann.de)

---



# Vorwort

Ja, guten Tag, meine Damen und Herren!

Dieses Skript basiert auf unserer Mitschrift der Vorlesung „Diskrete Strukturen“ im Sommersemester 2002 an der RWTH Aachen (Priv.-Doz. Dr. Y. Guo). Es handelt sich nicht um eine offizielle Veröffentlichung des Lehrstuhls C für Mathematik.

Wir übernehmen keine Gewähr für die Fehlerfreiheit und Vollständigkeit des Skripts. Korrekturen können an [post@mark-wiesemann.de](mailto:post@mark-wiesemann.de) geschickt werden.

Wir bedanken uns bei Dr. Guo für die zur Verfügung gestellten Chinesischen Bezeichnungen und Namen.

Volker Krause  
Tobias Lohmann  
Christian Lücking  
Florian Schröder  
Mark Wiesemann

7. März 2003



# Inhaltsverzeichnis

<b>Vorwort</b>	<b>iii</b>
<b>1 Abzählung, Rekursion, erzeugende Funktionen</b>	<b>1</b>
§ 1 Elementare Zählprinzipien	1
1.1 Lemma (Mengen)	1
1.2 Folgerung	1
1.3 Definition (Permutation)	2
1.4 Lemma	2
1.5 Satz (Potenzmenge)	2
1.6 Definition (Teilmengen)	2
1.7 Bemerkung	2
1.8 Lemma	3
2. Beweis von Satz 1.5	3
1.9 Satz (Pascal-Dreieck)	3
1.10 Satz (Vandermonde'sche Identität)	3
Bezierkurven (Anwendung der Sätze 1.9 und 1.10 in der Computergraphik)	4
1.11 Lemma (Doppeltes Abzählen)	4
1.12 Satz (SCHUBFACHPRINZIP)	4
1.13 Beispiel (Schubfachprinzip)	5
1.14 Satz (verallgemeinertes Schubfachprinzip)	5
Rückblick auf Lemma 1.1 (c) und (b)	6
1.15 Satz (Prinzip der INKLUSION und EXKLUSION, SIEBFORMEL)	6
1.16 Beispiel	7
§ 2 Mengenpartitionen	7
1.17 Definition (Partition)	7
1.18 Beispiel	7
1.19 Satz (STIRLING-DREIECK ZWEITER ART)	8
1.20 Satz	8
1.21 Satz	9
§ 3 Permutationen	9
1.22 Definition (Zyklus)	10
1.23 Bemerkung (Zyklen)	10
Beispiel	10
1.24 Definition (Stirlingzahl)	10
Beispiel	10
1.25 Satz (Stirling-Dreieck erster Art)	10
1.26 Bemerkung	11
§ 4 Erzeugende Funktionen (formale Potenzreihen)	11
1.27 Definition (erzeugende Funktion)	11
1.28 Bemerkung	11
1.29 Definition (Faltung / Konvolution)	12
1.30 Lemma (Verschieben von Folgegliedern)	12
1.31 Beispiel	13
1.32 Satz	13
1.33 Bemerkung	13
1.34 Lemma	13

1.35	Beispiel (Code mit variabler Wortlänge zum Komprimieren von Daten)	14
1.36	Satz (Inversion von Potenzreihen)	14
1.37	Beispiel	15
1.38	Definition (Ableitung)	15
1.39	Lemma	15
1.40	Folgerung	15
	Neuer Beweis zum Beispiel 1.37 (2)	16
1.41	Folgerung	16
1.42	Bemerkung	16
	Formale Potenzreihen und ihre erzeugenden Funktionen (vgl. Tabelle 1.2)	16
§ 5	Rekursionsgleichungen	16
	Einige grundlegende algorithmische Verfahren	16
1.43	Definition (Rekursionsgleichung)	17
1.44	Beispiel	17
1.45	Beispiel	18
1.46	Beispiel (Fibonacci-Zahlen)	18
1.47	Bemerkung (Goldener Schnitt)	19
1.48	Satz	20
	Schema zum Lösen von (homogenen) linearen Rekursionsgleichungen	20
1.49	Beispiel	21
1.50	Beispiel (Catalan-Zahlen)	21
1.51	Lemma	22
1.52	Satz	22
<b>2</b>	<b>Graphentheorie</b>	<b>25</b>
§ 1	Grundbegriffe der Graphentheorie	25
2.1	Definition (Graph)	25
2.2	Beispiel	25
2.3	Bemerkung (leerer Graph)	27
2.4	Definition (Ecken eines Graphen)	27
2.5	Beispiel	27
2.6	Satz (Handschlaglemma, Euler 1736)	28
2.7	Folgerung	28
2.8	Lemma	28
2.9	Definition (isomorphe Graphen)	28
2.10	Beispiel	28
2.11	Definition (Darstellung von Graphen)	29
2.12	Beispiel	29
2.13	Satz (Adjazenz und Inzidenzmatrix)	29
2.14	Definition (Teilgraph)	30
2.15	Definition (zusammenhängender Graph)	30
2.16	Satz	30
2.17	Folgerung	31
2.18	Satz	31
2.19	Satz	32
§ 2	Bäume	32
2.20	Definition (Bäume und Wälder)	32
2.21	Lemma	32
2.22	Satz	33
2.23	Definition (Wurzelbaum)	33
2.24	Definition (balancierter Wurzelbaum)	34
2.25	Definition (binärer Baum)	34
2.26	Satz	34
2.27	Folgerung	35

2.28	Definition (Gerüst eines Graphen) . . . . .	35
2.29	Satz . . . . .	35
2.30	Satz (Cayley's Tree Formular) . . . . .	36
§ 3	Matching in Graphen . . . . .	37
2.31	Definition (Matching in Graphen) . . . . .	37
2.32	Beispiel . . . . .	37
2.33	Bemerkung (Maximum-Matching) . . . . .	38
2.34	Definition (bipartite Graphen) . . . . .	39
2.35	Beispiel . . . . .	39
2.36	Satz (König, 1916) . . . . .	39
2.37	Satz (König-Hall) . . . . .	39
2.38	Folgerung (König, 1916) . . . . .	40
2.39	Folgerung (König, 1916) . . . . .	40
2.40	Definition (Multipartite Graphen) . . . . .	40
§ 4	Hamiltonsche Graphen . . . . .	40
2.41	Definition (Hamiltonkreis / Hamiltonweg) . . . . .	40
2.42	Beispiel . . . . .	41
	Bemerkung . . . . .	41
2.43	Satz (notwendige Bedingung) . . . . .	41
2.44	Satz (Ore 1960, hinreichende Bedingung) . . . . .	42
2.45	Folgerung (Ore, 1960) . . . . .	42
2.46	Folgerung (Diac, 1952) . . . . .	42
2.47	Bemerkung . . . . .	42
§ 5	Eulersche Graphen . . . . .	42
	Vorbemerkung (Königsberger-Problem) . . . . .	42
2.48	Definition (Eulertour, Kantenzug) . . . . .	43
2.49	Definition (eulersch, semi-eulersch) . . . . .	43
2.50	Beispiel . . . . .	43
2.51	Satz (Euler, 1736) . . . . .	44
2.52	Folgerung . . . . .	44
2.53	Bemerkung . . . . .	44
§ 6	Planare Graphen . . . . .	44
2.54	Definition (einbettbarer / planarer Graph) . . . . .	45
2.55	Satz (Eulersche Polyederformel) . . . . .	45
2.56	Satz . . . . .	46
2.57	Beispiel . . . . .	46
2.58	Definition (Unterteilungsgraph) . . . . .	46
2.59	Satz (Kuratowski, 1930) . . . . .	46
2.60	Definition (Färbung) . . . . .	46
2.61	Beispiel . . . . .	47
2.62	Satz (VIERFARBENVERMUTUNG, Guthrie 1852) . . . . .	47
2.63	Bemerkung . . . . .	47
§ 7	Digraphen . . . . .	48
2.64	Definition (Digraph) . . . . .	48
2.65	Konvention . . . . .	48
2.66	Definiton (Teildigraph) . . . . .	48
2.67	Definition . . . . .	50
2.68	Definition (Turnier) . . . . .	51
2.69	Satz (Redei, 1934) . . . . .	51
2.70	Satz (Moon, 1966) . . . . .	51
2.71	Bemerkung . . . . .	52

<b>3</b>	<b>Algebraische Strukturen</b>	<b>53</b>
§ 1	Universelle Algebren	53
3.1	Definition (Operation)	53
3.2	Definition (Algebra)	53
3.3	Beispiel	53
3.4	Definition (neutrale Elemente)	54
3.5	Beispiel	54
3.6	Lemma	54
3.7	Beispiel (vgl. Beispiel 3.3(2))	54
3.8	Definition (inverse Elemente)	55
3.9	Definition (Halbgruppe)	55
3.10	Definition (Monoid)	55
3.11	Definition (Gruppe)	55
3.12	Definition (abelsche Algebren)	55
3.13	Definition (Ring)	55
3.14	Definition (Körper)	56
3.15	Definition (boolesche Algebren)	56
3.16	Beispiel	56
§ 2	Unteralgebra, Homomorphismen, Kongruenz	57
3.17	Definition (Unteralgebra)	57
3.18	Definition (Untergruppe, Teilring / Unterring)	57
3.19	Beispiel	57
3.20	Lemma	57
3.21	Definition (erzeugte Unteralgebra)	58
3.22	Beispiel	58
3.23	Definition (Algebra-Homomorphismus)	58
3.24	Beispiel	58
3.25	Definition (Isomorphismus)	59
3.26	Beispiel	59
3.27	Lemma	59
3.28	Lemma	59
3.29	Beispiel	60
3.30	Definition (Kongruenzrelation)	60
3.31	Beispiel	60
3.32	Satz (Homomorphiesatz)	60
3.33	Beispiel	61
§ 3	Ringe und Ideale	62
3.34	Lemma	62
3.35	Definition (Ideal)	62
3.36	Satz	63
3.37	Satz	63
3.38	Beispiel (vgl. Beispiel 3.28)	63
3.39	Beispiel	63
§ 4	Größte gemeinsame Teiler	64
3.40	Definition (Integritätsbereich)	64
3.41	Beispiel	64
3.42	Definition (größter gemeinsamer Teiler)	64
3.43	Bemerkung	64
§ 5	Eindeutige Primfaktorzerlegung	65
3.44	Definition (irreduzibel)	65
3.45	Beispiel	65
3.46	Beispiel	65
3.47	Definition (Primfaktor-Zerlegung)	65
3.48	Bemerkung	65

3.49	Definition (Hauptidealring) . . . . .	65
3.50	Satz . . . . .	65
3.51	Definition (Euklidischer Ring) . . . . .	66
3.52	Beispiel . . . . .	66
3.53	Satz . . . . .	66
3.54	Folgerung . . . . .	66
3.55	Bemerkung . . . . .	66
3.56	Satz . . . . .	66
3.57	Satz (Primzahlen) . . . . .	67
3.58	Bemerkung . . . . .	67
3.59	Satz („kleiner Fermat“) . . . . .	67
3.60	Definition (eulersche $\varphi$ -Funktion) . . . . .	67
3.61	Lemma . . . . .	67
3.62	Satz (Euler) . . . . .	68
3.63	Lemma . . . . .	68
3.64	Satz (Euklidischer Algorithmus) . . . . .	68
3.65	Definition (normiert) . . . . .	68
3.66	Folgerung . . . . .	68
3.67	Satz . . . . .	69
3.68	Beispiel . . . . .	69
3.69	Bemerkung . . . . .	70
§ 6	Endliche Körper . . . . .	70
	Vorbemerkungen . . . . .	70
3.70	Folgerung . . . . .	70
	Bemerkung . . . . .	70
3.71	Satz . . . . .	71
3.72	Satz . . . . .	71
3.73	Beispiel (Fortsetzung von Beispiel 3.68) . . . . .	71
<b>Tabellenverzeichnis</b>		<b>73</b>
<b>Abbildungsverzeichnis</b>		<b>75</b>
<b>Index</b>		<b>77</b>



# 1 Abzählung, Rekursion, erzeugende Funktionen

## § 1 Elementare Zählprinzipien

$M$ : endliche Menge

$|M|$  = Anzahl der Elemente von  $M$

$|M| = n, n \in \mathbb{N} = \{1, 2, \dots\} \Leftrightarrow$  Es gibt eine Bijektion  $f: M \rightarrow \{1, 2, \dots, n\}$ .

Eine Menge  $M$  mit  $|M| = n$  heißt  $n$ -Menge.

$|M| = 0 \Leftrightarrow M = \emptyset$  (leere Menge).

### 1.1 Lemma (Mengen)

Seien  $A$  und  $B$  zwei Mengen.

(a)  $|A| = |B| \Leftrightarrow$  Es gibt eine Bijektion  $f: A \rightarrow B$ .

(b)  $|A \uplus B| = |A| + |B|$ ;  $A \uplus B$  heißt die DISJUNKTE VEREINIGUNG von  $A$  und  $B$ , d.h. es gilt:

$A \cap B = \emptyset$  (vgl. Abbildungen 1.1 und 1.2).

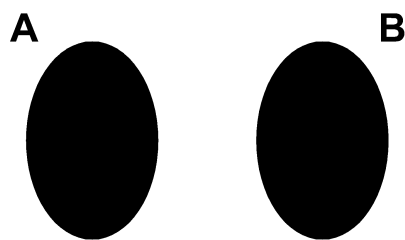


Abbildung 1.1: Disjunkte Vereinigung von  $A$  und  $B$  ( $A \uplus B$ )

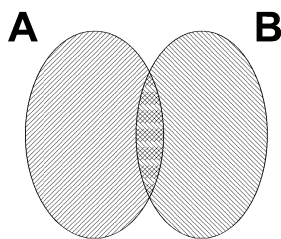


Abbildung 1.2: Vereinigung von  $A$  und  $B$  ( $A \cup B$ )

(c)  $|A \times B| = |A| \cdot |B|$

$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$  heißt KARTESISCHES PRODUKT von  $A$  und  $B$ . □

### 1.2 Folgerung

Seien  $A$  und  $B$  zwei endliche Mengen.

$\text{Abb}(A, B) := B^A$  = Menge aller Abbildungen von  $A$  nach  $B$ .

Dann gilt:  $|B^A| = |B|^{|A|}$ .

**Beweis**

Seien  $|A| = n$  und  $|B| = m$ , also  $A = \{a_1, a_2, \dots, a_n\}$ .

$B^A \rightarrow \underbrace{B \times B \times \dots \times B}_{n\text{-mal}}$  ist eine Bijektion.

$$\Rightarrow |B^A| = |\underbrace{B \times B \times \dots \times B}_{n\text{-mal}}| \stackrel{1.1(c)}{=} \underbrace{|B| \cdot |B| \cdot \dots \cdot |B|}_{n\text{-mal}} = |B|^n = |B|^{|A|}. \quad \square$$

**1.3 Definition (Permutation)**

Sei  $A$  eine Menge.

$f : A \rightarrow A$  heißt PERMUTATION von  $A$ , wenn  $f$  bijektiv ist. □

**1.4 Lemma**

Sei  $S_n := \{\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \text{ bijektiv}\} := \text{Sym}\{1, 2, \dots, n\}$  (SYMMETRISCHE GRUPPE vom Grad  $n$ ).

Dann gilt:  $|S_n| = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1 = n!$

(Bemerkung:  $n!$  = Anzahl der Möglichkeiten, eine  $n$ -Menge anzuordnen.)

**Beweis**

s. Lineare Algebra I □

**1.5 Satz (Potenzmenge)**

Die Anzahl der Teilmengen einer  $n$ -Menge  $A$  ist  $2^n$  (d.h.  $|A| = n \Rightarrow |P(A)| = 2^n$ , wobei  $P(A) = \{B \mid B \subseteq A\}$  die POTENZMENGE von  $A$  ist).

(Beispiel:  $A = \{1, 2\}$ ,  $P(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ )

**Beweis**

Sei  $B \subseteq A$ .

$$\chi_B : A \rightarrow \{0, 1\}, \chi_B(x) = \begin{cases} 1 & \text{für } x \in B \\ 0 & \text{sonst} \end{cases}$$

heißt CHARAKTERISTISCHE FUNKTION von  $B$ .

$$B = \{x \in A \mid \chi_B(x) = 1\}.$$

$\Rightarrow$  Es gibt eine Bijektion  $f : P(A) \rightarrow \{0, 1\}^A$  mit  $f(B) = \chi_B$  für alle  $B \subseteq A$ .

$$\Rightarrow |P(A)| = |\underbrace{\{0, 1\}^A}_{\text{Folg. 1.2}}| = |\{0, 1\}|^{|A|} = 2^n. \quad \square$$

**1.6 Definition (Teilmengen)**

Sei  $A$  eine Menge und  $k \in \mathbb{N}$  mit  $k \leq |A|$ .

$$P_k(A) = \binom{A}{k} =: \{B \subseteq A \mid |B| = k\} = \text{Menge aller } k\text{-Teilmengen von } A. \quad \square$$

**1.7 Bemerkung**

$$P(A) = \biguplus_{k=0}^n P_k(A), n = |A|.$$

$$\stackrel{\text{Lemma 1.1(b)}}{\implies} |P(A)| = |P_0(A)| + |P_1(A)| + \dots + |P_n(A)| = \sum_{k=0}^n |P_k(A)|. \quad \square$$

**1.8 Lemma**

Sei  $A$  eine Menge mit  $|A| = n$ . Dann gilt:

$$|P_k(A)| = \binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

**Beweis**

$$|\{\underbrace{(b_1, b_2, \dots, b_k)}_{\text{geordnetes } k\text{-Tupel}} \mid b_i \in A, b_i \neq b_j \text{ für alle } i \neq j\}| = n \cdot (n-1) \cdot (n-2) \cdots (n-k+1).$$

Es gibt  $k!$  Anordnungen von  $b_1, b_2, \dots, b_k$ .

$$\Rightarrow |P_k(A)| = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{k!} = \binom{n}{k}. \quad \square$$

**2. Beweis von Satz 1.5**

Zu zeigen:  $|P(A)| = 2^n$ , wenn  $|A| = n$ .

$$|P(A)| = \sum_{k=0}^n |P_k(A)| = \sum_{k=0}^n \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} \cdot 1^k \cdot 1^{n-k} \stackrel{\text{Binomialsatz}}{=} (1+1)^n = 2^n. \quad \square$$

**1.9 Satz (Pascal-Dreieck)**

Für alle  $n, k \in \mathbb{N}$  mit  $n > k$  gilt (vgl. Abbildung 1.3):

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

**Beweis 1 (durch Nachrechnen)**

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \dots = \binom{n}{k}, \text{ s. Analysis für Informatiker.}$$

**Beweis 2 (kombinatorisch)**

$$\binom{n}{k} = \text{Anzahl der } k\text{-Teilmengen von } A \text{ mit } |A| = n.$$

$$P_k(\underbrace{A}_{=\{a_1, a_2, \dots, a_n\}}) = \{M \subseteq \{a_1, a_2, \dots, a_n\} \mid |M| = k\} \text{ (partitionieren)}$$

$$= \{M' \cup \{a_n\} \mid M' \subseteq \{a_1, a_2, \dots, a_n\} \text{ und } |M'| = k-1\} \uplus \{M'' \subseteq \{a_1, a_2, \dots, a_{n-1}\} \mid |M''| = k\}$$

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

				1					$n = 0$
				1	1				$n = 1$
			1	2	1				$n = 2$
		1	3	3	1				$n = 3$
	1	4	6	4	1				$n = 4$
1	5	10	10	5	1				$n = 5$

Abbildung 1.3: Pascal-Dreieck für  $n = 0, 1, \dots, 5$

**1.10 Satz (Vandermonde'sche Identität)**

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

**Beweis**

Sei  $A$  eine Menge mit  $|A| = n + m$ , also  $A = B \uplus C$  mit  $|B| = n$  und  $|C| = m$ .

$$\binom{A}{k}_l = \{X \subseteq A \mid |X| = k \text{ und } |X \cap B| = l\}_{l=0,1,\dots,k}$$

Dann gilt:  $\binom{A}{k} = \bigsqcup_{l=0}^k \binom{A}{k}_l$   
 $\Rightarrow \binom{m+n}{k} = \left| \binom{A}{k} \right| = \sum_{l=0}^k \left| \binom{A}{k}_l \right| = \sum_{l=0}^k \binom{n}{l} \binom{m}{k-l}$  □

**Bezierkurven** (Anwendung der Sätze 1.9 und 1.10 in der Computergraphik)

- FREIFORMKURVE: eine gewünschte Kurve soll durch möglichst wenige Punkte möglichst gut beschrieben werden.
- SPLINES: beruhen auf Polynomen
- BÉZIERKURVE: Stützstellen  $P_1, P_2, \dots, P_n$

$$P(t) := \sum_{i=1}^n B_{n,i}(t) \cdot P_i, t \in [0, 1], \text{ wobei } B_{n,i}(t) = \binom{n}{i} \cdot t^i \cdot (1-t)^{n-i} \text{ (BERNSTEINPOLYNOM)}$$

Satz 1.9  $\Rightarrow$  Rekursionsgleichung

$$B_{n,i}(t) = t \cdot B_{n-i,i-1}(t) + (1-t) \cdot B_{n-i,i}(t)$$

Sie liefert eine effiziente Berechnung der Bézierkurve. □

**1.11 Lemma** (Doppeltes Abzählen)

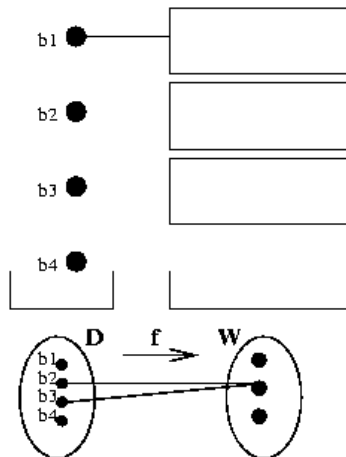
Seien  $S$  und  $T$  Mengen und  $R \subseteq \underbrace{S \times T}_{:=\{(s,t) \mid s \in S \wedge t \in T\}}$  eine Relation.

$$\begin{array}{l} s_1 : (s_1, t_{1,1}), (s_1, t_{1,2}), (s_1, t_{1,3}) \\ s_2 : (s_2, t_{2,1}), (s_2, t_{2,2}) \\ \vdots \\ s_n : (s_n, t_{n,1}) \end{array} \quad \left| \quad \begin{array}{l} t_i : (t_i, s_{i,1}), (t_i, s_{i,2}) \\ \vdots \end{array} \right.$$

Dann gilt:  $|R| = \sum_{s \in S} |\{t \in T \mid (s,t) \in R\}|$  (Zeilensumme)

$$= \sum_{t \in T} |\{s \in S \mid (s,t) \in R\}|$$
 (Spaltensumme) □

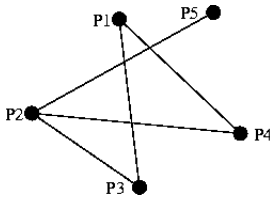
**1.12 Satz** (SCHUBFACHPRINZIP)



Ist  $f : X \rightarrow Y$  eine Abbildung und gilt  $|X| > |Y|$ , so gibt es ein  $y \in Y$  mit  $|f^{-1}(y)| \geq 2$ .  
 (Verteilt man  $n$  Elemente auf  $m$  Fächer, wobei  $n > m$  ist, so gibt es mindestens ein Fach, das 2 Elemente enthält.) □

### 1.13 Beispiel (Schubfachprinzip)

- (1) In jeder Gruppe von 13 Personen befinden sich zwei, die im selben Monat Geburtstag haben.  
 (2) In jeder Gruppe  $P$  von Personen gibt es immer zwei Personen, die die gleiche Anzahl von Personen in  $P$  kennen.  
 (Annahme: Die Relation „kennen“ ist symmetrisch.) □



#### Beweis

Setze:  $P = \{p_1, p_2, \dots, p_n\}$   
 $f : P \rightarrow \{0, 1, 2, \dots, n-1\}$

Fall 1:  $\exists p_i \in P$  mit  $f(p_i) = 0$   
 $\Rightarrow f(p_j) \neq n-1, \forall p_j \in P \setminus \{p_i\}$   
 $\Rightarrow f(p) \subseteq \underbrace{\{0, 1, 2, \dots, n-2\}}_{n-1 \text{ Zahlen}}$

Fall 2:  $\forall p_i \in P$  mit  $f(p_i) \neq 0$   
 $\Rightarrow f(p) \subseteq \underbrace{\{1, 2, 3, \dots, n-1\}}_{n-1 \text{ Zahlen}}$

Somit gilt:  $|P| > |f(p)|$ .  
 Nach dem Schubfachprinzip gibt es mindestens zwei Personen  $p_l$  und  $p_k$  mit  $f(p_l) = f(p_k)$ . □

### 1.14 Satz (verallgemeinertes Schubfachprinzip)

Ist  $f : X \rightarrow Y$  eine Abbildung, so gibt es ein  $y \in Y$  mit  $|f^{-1}(y)| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil$   
 (Beispiel: Verteilt man 7 Bücher auf 3 Fächer, so gibt es mindestens ein Fach, das 3 Bücher enthält etc.)

#### Beweis (indirekt)

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

$$|X| = \left| \bigsqcup_{y \in Y} f^{-1}(y) \right| = \sum_{y \in Y} |f^{-1}(y)| \leq |Y| \cdot \left( \left\lceil \frac{|X|}{|Y|} \right\rceil - 1 \right) \leq |Y| \cdot \left( \left( \left\lceil \frac{|X|-1}{|Y|} \right\rceil + 1 \right) - 1 \right) = |X| - 1 \quad \text{↯}$$

**Rückblick auf Lemma 1.1 (c) und (b)**

$$|A \times B| = |A| \cdot |B|$$

- $M = A_1 \times A_2 \times \dots \times A_n$

$$\Rightarrow |M| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n| = \prod_{i=1}^n |A_i| \text{ (Produktregel)}$$

Seien A und B zwei disjunkte Mengen so gilt:  $|A \uplus B| = |A| + |B|$

- Seien  $A_1, A_2, \dots, A_n$  paarweise disjunkte Mengen (d.h.  $A_i \cap A_j = \emptyset$  für  $i, j \in \{1, 2, \dots, n\}$  mit  $i \neq j$ ) und  $S = A_1 \cup A_2 \cup \dots \cup A_n = \biguplus_{i=1}^n A_i \Rightarrow |S| = |A_1| + |A_2| + \dots + |A_n| = \underbrace{\sum_{i=1}^n |A_i|}_{\text{Summenregel}}$

**Problem:**

Sei  $S = A_1 \cup A_2 \cup \dots \cup A_n$ , wobei  $A_1, \dots, A_n$  nicht unbedingt paarweise disjunkt sind.  
 $|S| = ?$

**Triviale Beispiele:**

- Für zwei Mengen  $A_1$  und  $A_2$ :

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

- Für drei Mengen  $A_1, A_2$  und  $A_3$ :

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \quad \square$$

**1.15 Satz (Prinzip der INKLUSION und EXKLUSION, SIEBFORMEL)**

Für endliche Mengen  $A_1, A_2, \dots, A_n$  gilt:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{r=1}^n (-1)^{r-1} \sum_{1 \leq i_1 < \dots < i_r \leq n} \left| \bigcap_{j=1}^r A_{i_j} \right|$$

**Beweis**

Sei  $a \in \bigcup_{i=1}^n A_i$  beliebig.

- (1) Auf der linken Seite wird  $a$  genau einmal gezählt.
- (2) Zu zeigen: Auf der rechten Seite wird  $a$  auch genau einmal gezählt.

Annahme:  $a \in A_{t_j}, j = 1, 2, \dots, l$  und  $a \notin \bigcup_{i=1}^n A_i \setminus \bigcup_{j=1}^l A_{t_j}$

Dann wird  $a$  in der Summe  $\sum_{1 \leq i_1 < \dots < i_r \leq n} \left| \bigcap_{j=1}^r A_{i_j} \right|$  genau  $\binom{l}{r}$ -mal gezählt. Denn:  $\{t_1, t_2, \dots, t_l\}$  enthält genau  $\binom{l}{r}$   $r$ -Teilmengen, s. Lemma 1.8.

$\Rightarrow a$  ist auf der rechten Seite genau

$$\sum_{r=1}^l (-1)^{r-1} \binom{l}{r} = 1 + \left( -1 + \sum_{r=1}^l (-1)^{r-1} \binom{l}{r} \right) = 1 - \sum_{r=0}^l (-1)^r \binom{l}{r}$$

$$= 1 - \sum_{r=0}^l \binom{l}{r} (-1)^r \cdot 1^{l-r} = 1 - \underbrace{(-1+1)^l}_{=0} = 1$$

mal gezählt. □

### 1.16 Beispiel

Sei  $k \in \mathbb{N}$  und  $M_k = \{n \in \mathbb{N} \mid 1 \leq n \leq 100, k \text{ teilt } n\}$ .

Bestimmen Sie:

$|M_2 \cup M_3 \cup M_5|$  (Anzahl der durch 2 oder 3 oder 5 teilbaren natürlichen Zahlen  $\leq 100$ )

**Lösung:**

$|M_k| = \lfloor \frac{100}{k} \rfloor$ , da genau jede  $k$ -te natürliche Zahl durch  $k$  teilbar ist.

$$\begin{aligned} |M_2 \cup M_3 \cup M_5| &= |M_2| + |M_3| + |M_5| - \underbrace{|M_2 \cap M_3|}_{=M_6} - \underbrace{|M_2 \cap M_5|}_{=M_{10}} - \underbrace{|M_3 \cap M_5|}_{=M_{15}} \\ &\quad + \underbrace{|M_2 \cap M_3 \cap M_5|}_{=M_{30}} \\ &= \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{5} \right\rfloor - \left\lfloor \frac{100}{6} \right\rfloor - \left\lfloor \frac{100}{10} \right\rfloor - \left\lfloor \frac{100}{15} \right\rfloor + \left\lfloor \frac{100}{30} \right\rfloor \\ &= 50 + 33 + 20 - 16 - 10 - 6 + 3 \\ &= 74 \end{aligned} \quad \square$$

## § 2 Mengenpartitionen

### 1.17 Definition (Partition)

Sei  $M$  eine Menge mit  $|M| = n$ .

- Eine PARTITION  $P$  von  $M$  ist eine Zerlegung von  $M$  in eine Vereinigung disjunkter nichtleerer Teilmengen.
- Gilt  $M = A_1 \uplus A_2 \uplus \dots \uplus A_k$  mit  $A_i \neq \emptyset$  für  $i \in \{1, 2, \dots, k\}$ , so heißt  $P = \{A_1, A_2, \dots, A_k\}$  eine  $k$ -Partition von  $M$ .
- $\text{Part}_k(M) := \{P \mid P \text{ ist eine } k\text{-Partition von } M\}$ .
- STIRLINGZAHLEN zweiter Art:

$$S_{n,k} := |\text{Part}_k(M)| \text{ für } n, k \geq 0 \text{ und } S_{0,0} := 1$$

$$S_{n,k} =: \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \text{Anzahl der } k\text{-Partitionen einer } n\text{-Menge.}$$

□

### 1.18 Beispiel

(1)  $M = \{1, 2, 3, 4\}$

$$\text{Part}_1(M) = \{M\}$$

$$\text{Part}_2(M) = \{\{\{1\}, \{2, 3, 4\}\}; \{\{2\}, \{1, 3, 4\}\}; \{\{3\}, \{1, 2, 4\}\}; \{\{4\}, \{1, 2, 3\}\}; \{\{1, 2\}, \{3, 4\}\};$$

$$\{\{1, 3\}, \{2, 4\}\}; \{\{1, 4\}, \{2, 3\}\}\}$$

$$= \{\{A, M \setminus A\} \mid A \subseteq M, A \neq \emptyset, A \neq M\} \text{ für } |M| = n.$$

Im Allgemeinen:

$$|\text{Part}_2(M)| = \frac{1}{2}(2^n - 2), \text{ für } |M| = n$$

(2) Für  $n \geq 1$  gilt:

$$S_{n,0} = 0$$

$$S_{n,1} = 1$$

$$S_{n,n-1} = \binom{n}{2}$$

$$S_{n,n} = 1$$

Ist  $k > n$ , so gilt  $S_{n,k} = 0$ . □

### 1.19 Satz (STIRLING-DREIECK ZWEITER ART)

Für alle  $k, n \in \mathbb{N}$  mit  $1 \leq k \leq n$  gilt

$$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$$

**Beweis** (kombinatorisch)

Sei  $A = \{a_1, a_2, \dots, a_n\}$ . Dann gilt:

$$\begin{aligned} \text{Part}_k(A) &= \underbrace{\{P \in \text{Part}_k(A) \mid \{a_n\} \in P\}}_{=\{P' \cup \{a_n\} \mid P' \in \text{Part}_{k-1}\{a_1, \dots, a_{n-1}\}\}} \cup \underbrace{\{P \in \text{Part}_k(A) \mid \{a_n\} \notin P\}}_{=\{\{\{a_n\} \cup B_1, B_2, \dots, B_k\}, \{B_1, \{a_n\} \cup B_2, B_3, \dots, B_k\}, \dots, \\ &\quad \{B_1, \dots, B_{k-1}, \{a_n\} \cup B_k\} \mid \{B_1, B_2, \dots, B_k\} \in \text{Part}_k\{a_1, a_2, \dots, a_{n-1}\}\}} \\ \Rightarrow |\text{Part}_k(A)| &= |\text{Part}_{k-1}\{a_1, \dots, a_{n-1}\}| + k \cdot |\text{Part}_k\{a_1, a_2, \dots, a_{n-1}\}|, \\ \Rightarrow S_{n,k} &= S_{n-1,k-1} + k \cdot S_{n-1,k}. \end{aligned} \quad \square$$

				1		$n = 0$
			0	1		$n = 1$
		0	1	1		$n = 2$
	0	1	3	1		$n = 3$
0	1	7	6	1		$n = 4$

Abbildung 1.4: Rekursion für die Stirlingzahlen 2. Art (Stirling-Dreieck 2. Art)

### 1.20 Satz

Seien  $M$  und  $N$  Mengen mit  $|M| = m$  und  $|N| = n$ . Dann gilt:

(a)  $|\text{Abb}(M, N)| = |N|^{|M|} = n^m$  (siehe Folgerung 1.2)

(b) Menge aller injektiven Abbildungen von  $M$  nach  $N$ :

$$|\text{Inj}(M, N)| = n^{\underline{m}} = n \cdot (n-1) \cdot \dots \cdot (n-(m-1)) \text{ („}n \text{ hoch } m \text{ fallend“)}$$

(c) Menge aller surjektiven Abbildungen von  $M$  nach  $N$ :

$$|\text{Surj}(M, N)| = n! \cdot S_{m,n}$$

**Beweis**

Sei  $M = \{a_1, a_2, \dots, a_m\}$

(b)  $f : M \rightarrow N$  injektiv  $\Leftrightarrow f(a_i) \neq f(a_j)$  für  $i \neq j$

Somit gibt es für  $f(a_1)$   $n$  Abbildungsmöglichkeiten, für  $f(a_2)$  entsprechend  $n-1$  Möglichkeiten usw.

Für  $f(a_m)$  bleiben letztendlich  $n-(m-1)$  Möglichkeiten.

Nach der Produktregel folgt die Behauptung.

(c) Sei  $N = \{b_1, b_2, \dots, b_n\}$ ,  $f : M \rightarrow N$  surjektiv.

$$\{\{a \in M \mid f(a) = b_j\} \mid j = 1, \dots, n\} \in \text{Part}_n(M)$$

Für eine feste  $n$ -Partition von  $M$  permutiert man die Elemente in  $N$ .

⇒ Eine  $n$ -Partition von  $M$  entspricht  $n!$  surjektiven Abbildungen, d.h.:

$$\underbrace{|\text{Part}_k(M)|}_{=S_{m,k}} \cdot n! = |\text{Surj}(M, N)|$$

Also:  $|\text{Surj}(M, N)| = n! \cdot S_{m,k}$  □

**1.21 Satz**

$$n^m = \sum_{k=0}^n n^k \cdot S_{m,k} \text{ mit } m, n \in \mathbb{N}.$$

**Beweis**

Seien  $M$  und  $N$  Mengen mit  $|M| = m$  und  $|N| = n$ . Dann gilt:

$$\text{Abb}(M, N) = \bigsqcup_{A \subseteq N} \text{Surj}(M, A)$$

D.h. man kann  $f : M \rightarrow N$  als surjektive Abbildung von  $M$  nach  $f(M)$  auffassen.

$$\begin{aligned} n^m = |\text{Abb}(M, N)| &= \sum_{A \subseteq N} |\text{Surj}(M, A)| \\ &= \sum_{k=0}^n \left( \sum_{A \subseteq \binom{N}{k}} |\text{Surj}(M, A)| \right) \\ &= \sum_{k=0}^n \left( \sum_{A \subseteq \binom{N}{k}} k! \cdot S_{m,k} \right) \\ &= \sum_{k=0}^n \binom{N}{k} \cdot k! \cdot S_{m,k} \\ &= \sum_{k=0}^n \frac{n^k}{k!} \cdot k! \cdot S_{m,k} \\ &= \sum_{k=0}^n n^k \cdot S_{m,k} \end{aligned}$$
□

**§ 3 Permutationen**

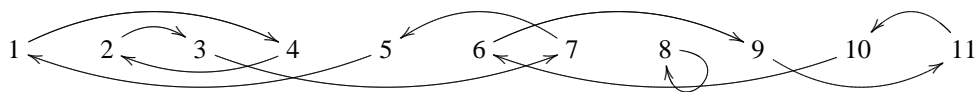
**Wiederholung**

$$S_n = \text{Sym}\{1, 2, \dots, n\} := \{a : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \mid a \text{ bijektiv} \}$$

$$|S_n| = n!$$

Jede Permutation  $\alpha \in S_n$  kann man durch eine Wertetabelle angeben.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 3 & 7 & 2 & 1 & 9 & 5 & 8 & 11 & 6 & 10 \end{pmatrix} \begin{matrix} i \\ \alpha(i) \end{matrix}$$



$$(1 \ 4 \ 2 \ 3 \ 7 \ 5) \circ (6 \ 9 \ 11 \ 10) \circ (8)$$
□

### 1.22 Definition (Zyklus)

Ein  $k$ -ZYKLUS  $(i_1 i_2 i_3 \dots i_k)$  ist eine Permutation  $\alpha \in S_n$  mit

$$\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_{k-1}) = i_k, \alpha(i_k) = i_1 \text{ und } \alpha(i) = i \text{ für alle } i \notin \{i_1, i_2, \dots, i_k\},$$

wobei  $\{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$ . □

### 1.23 Bemerkung (Zyklen)

(1) Ein Zyklus ist nur durch die Reihenfolge der Elemente innerhalb des Zyklus bestimmt.

$$\text{Z.B. ist } (1 \ 2 \ 4 \ 6) = (2 \ 4 \ 6 \ 1) = (4 \ 6 \ 1 \ 2) = (6 \ 1 \ 2 \ 4),$$

$$\text{aber } (1 \ 2 \ 4 \ 6) \neq (1 \ 2 \ 6 \ 4).$$

(2) Jedes  $\alpha \in S_n$  lässt sich als Produkt von Zyklen schreiben. (Beispiel s. o.) □

#### Beispiel

$$M = \{1, 2, 3\}, S_n = \text{Sym}\{1, 2, 3\}$$

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

$$|S_3| = 3! \quad \square$$

### 1.24 Definition (Stirlingzahl)

Die Anzahl der Permutationen von  $\{1, 2, \dots, n\}$ , die genau  $k$  Zyklen haben, heißt STIRLINGZAHL ERSTER ART, bezeichnet mit  $s_{n,k}$  oder  $\begin{bmatrix} n \\ k \end{bmatrix}$ .

$$s_{n,k} = 0 \text{ für } k > n$$

$$s_{n,0} = 0 \text{ für } n \in \mathbb{N}$$

$$s_{0,0} := 1 \quad \square$$

#### Beispiel

Nach dem oberen Beispiel gilt:

$$s_{3,1} = 2, s_{3,2} = 3, s_{3,3} = 1$$

### 1.25 Satz (Stirling-Dreieck erster Art)

Für alle  $k, n \in \mathbb{N}$  mit  $n \geq k \geq 1$  gilt:

$$s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$$

#### Beweis (kombinatorisch)

Beispiel:  $M = \{1, 2, 3, 4\}$ , Permutationen von  $M$  mit genau 3 Zyklen:

$$\{(1 \ 2) (3) (4), (1 \ 3) (2) (4), (14) (2) (3), (2 \ 3) (1) (4), (2 \ 4) (1) (3), (3 \ 4) (1) (2)\}$$

$$\{\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_k \mid \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_k \text{ Permutation von } \{1, 2, \dots, n\} \text{ mit genau } k \text{ Zyklen}\}$$

$$\{\sigma'_1 \circ \sigma'_2 \circ \dots \circ \sigma'_{k-1} \mid \sigma'_1 \circ \sigma'_2 \circ \dots \circ \sigma'_{k-1} \text{ Permutation von } \{1, 2, \dots, n-1\} \text{ mit genau } k-1 \text{ Zyklen}\}$$

$$\biguplus_{i=1}^{n-1} \{\sigma''_1 \circ \sigma''_2 \circ \dots \circ \sigma''_k \mid \sigma''_1 \circ \sigma''_2 \circ \dots \circ \sigma''_k \text{ Permutation von } (\{1, 2, \dots, n-1\} \setminus \{i\}) \cup \{(i, n)\} \text{ als eine Zahl}\}$$

$$\Rightarrow s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k} \quad \square$$

				1				$n = 0$
			0	1	1			$n = 1$
		0	1	3	3	1		$n = 2$
	0	2	6	11	6	1		$n = 3$
0	24	60	120	155	105	35	1	$n = 4$
								$n = 5$

Abbildung 1.5: Rekursion für die Stirlingzahlen 1. Art (Stirling-Dreieck 1. Art)

**1.26 Bemerkung**

$$\sum_{k=1}^n s_{n,k} = n! \quad \square$$

**§ 4 Erzeugende Funktionen (formale Potenzreihen)**

Bei der Komplexitätsanalyse von Algorithmen entstehen oft Rekursionsgleichungen, z.B.:

$$a_0 = 0$$

$$a_1 = 1$$

$$a_n = a_{n-1} + a_{n-2}$$

$$a_n = (a_{n-2} + a_{n-3}) + a_{n-2} = 2a_{n-2} + a_{n-3} = \dots$$

Um die Lösung zu finden, brauchen wir „erzeugende Funktionen“.

Rekursionsgleichungen beschreiben unendliche Folgen:

$$(a_n)_{n \in \mathbb{N}} = a_0, a_1, a_2, \dots, a_n, \dots$$

Wir führen eine neue Schreibweise für die Folge  $(a_n)_{n \in \mathbb{N}}$  ein:

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots = \sum_{n=0}^{\infty} a_nx^n \text{ („formale Potenzreihe“)}$$

**1.27 Definition (erzeugende Funktion)**

Sei  $K$  ein Körper (z.B.  $K = \mathbb{R}, \mathbb{C}$ ) und  $(a_n)_{n \in \mathbb{N}_0} \in K^\infty$  eine Folge. Die formale Potenzreihe

$$A(x) := \sum_{n=0}^{\infty} a_nx^n$$

heißt ERZEUGENDE FUNKTION der Folge  $(a_n)_{n \in \mathbb{N}_0}$ , also:

$$A(x) := \sum_{n=0}^{\infty} a_nx^n = (a_n)_{n \in \mathbb{N}_0}$$

$$K[[x]] = \left\{ \sum_{n=0}^{\infty} a_nx^n \mid a_n \in K \forall n \in \mathbb{N}_0 \right\} \quad \square$$

**1.28 Bemerkung**

(1) Für  $k \in \mathbb{N}_0$  gilt:  $x^k = (a_n)_{n \in \mathbb{N}_0}$  mit  $a_n = \begin{cases} 1, & \text{für } n = k \\ 0, & \text{sonst} \end{cases}$ .

$$\left( \delta_{n,k} = \begin{cases} 1, & n = k \\ 0, & \text{sonst} \end{cases} \text{ heißt KRONECKER-SYMBOL} \right)$$

$$x^k = (\delta_{k,n})_{n \in \mathbb{N}_0}$$

(2) Für  $m \in \mathbb{N}_0$  gilt:  $\sum_{n=m}^{\infty} a_n x^n = (b_j)_{j \in \mathbb{N}_0}$  mit  $b_j = \begin{cases} 0 & , j = 0, 1, \dots, m-1 \\ a_j & , j \geq m \end{cases}$ .

(3) Für  $k \in \mathbb{N}$  gilt:  $\sum_{n=0}^{\infty} a_n x^{kn} = (b_i)_{i \in \mathbb{N}_0}$  mit  $b_i = \begin{cases} 0 & , i \neq kn \forall n \in \mathbb{N}_0 \\ a_n & , i = kn \text{ für ein } n \in \mathbb{N}_0 \end{cases}$ .

(4) Unterschiede zwischen Potenzreihen aus der Analysis und formalen Potenzreihen / erzeugenden Funktionen (s. Tabelle 1.1):

Tabelle 1.1: Unterschiede zwischen Potenzreihen aus der Analysis und formalen Potenzreihen / erzeugenden Funktionen

Potenzreihen aus der Analysis	Formale Potenzreihen
$f(x) = \sum_{n=0}^{\infty} a_n x^n$	$A(x) = \sum_{n=0}^{\infty} a_n x^n = (a_n)_{n \in \mathbb{N}_0}$
unendliche Summe	keine Summe, nur eine neue Schreibweise der Folge $(a_n)_{n \in \mathbb{N}_0}$
Funktion von $x$	i.A. nichts einzusetzen
Konvergenzfrage	keine Konvergenzfrage

(5) Seien  $(a_n)_{n \in \mathbb{N}_0}$  und  $(b_n)_{n \in \mathbb{N}_0}$  zwei Folgen und  $A(x) = \sum_{n=0}^{\infty} a_n x^n, B(x) = \sum_{n=0}^{\infty} b_n x^n$ . Dann gilt:

$$A(x) = B(x) \Leftrightarrow a_n = b_n \forall n \in \mathbb{N}_0$$

Im Folgenden werden wir für die formale Potenzreihen Addition, Multiplikation, Division, Ableitung usw. definieren. □

### 1.29 Definition (Faltung / Konvolution)

Sei  $K$  ein Körper und  $(a_n)_{n \in \mathbb{N}_0}$  und  $(b_n)_{n \in \mathbb{N}_0} \in K^{\infty}, a \in K$ .

(1) Addition „+“:  $\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n := \sum_{n=0}^{\infty} (a_n + b_n) x^n, x_n = (a_n + b_n)_{n \in \mathbb{N}_0}$

(2) Multiplikation „·“:  $\left( \sum_{n=0}^{\infty} a_n x^n \right) \cdot \left( \sum_{n=0}^{\infty} b_n x^n \right) := \sum_{n=0}^{\infty} \left( \sum_{k=0}^n a_k b_{n-k} \right) x^n$

FALTUNG oder KONVOLUTION der Folge  $(a_n)_{n \in \mathbb{N}_0}$  und  $(b_n)_{n \in \mathbb{N}_0}$   
(Cauchy-Produkt aus der Analysis)

(3)  $a \cdot \sum_{n=0}^{\infty} a_n x^n := \sum_{n=0}^{\infty} a \cdot a_n x^n$  □

### 1.30 Lemma (Verschieben von Folgengliedern)

$$x^m \cdot \sum_{n=0}^{\infty} a_n x^n = \sum_{n=m}^{\infty} a_{n-m} x^n$$

(D.h.:  $x^m \cdot (a_0, a_1, a_2, \dots) = (\underbrace{0, \dots, 0}_{m\text{-mal}}, a_0, a_1, a_2, \dots)$ .)

**Beweis**

$$\begin{aligned}
 x^m \cdot \sum_{n=0}^{\infty} a_n x^n &= \left( \sum_{n=0}^{\infty} \delta_{m,n} x^n \right) \cdot \left( \sum_{n=0}^{\infty} a_n x^n \right) \quad (x^m = (\delta_{m,n})_{n \in \mathbb{N}_0}) \\
 &= \sum_{n=0}^{\infty} \left( \sum_{k=0}^n \delta_{m,k} a_{n-k} \right) x^n \\
 &= \sum_{n=m}^{\infty} a_{n-m} x^n \quad \square
 \end{aligned}$$

**1.31 Beispiel**

Es gilt:

$$x^m \cdot x^n = x^{m+n} \text{ mit } m, n \in \mathbb{N}_0 \quad \square$$

**1.32 Satz**

Sei  $K$  ein Körper

(a)  $K[[X]]$  ist ein  $K$ -Vektorraum.

(b)  $(K[[X]], +, \cdot)$  ist ein kommutativer Ring mit Null  $0 = 0 \cdot x^0$  und Eins  $1 = 1 \cdot x^0 = (1, 0, 0, \dots)$ .

**Beweis**

(a) siehe Lineare Algebra

(b) durch Nachrechnen □

**1.33 Bemerkung**

Gilt  $A \cdot B = 1$  in einem kommutativen Ring mit Eins, so ist  $B$  durch  $A$  eindeutig bestimmt und es wird  $B = A^{-1} = \frac{1}{A}$  bezeichnet (ebenso  $A = B^{-1} = \frac{1}{B}$ ) und  $A$  (und auch  $B$ ) heißt INVERTIERBAR. □

**1.34 Lemma**

In  $K[[X]]$  ist  $\sum_{i=0}^{\infty} c^i x^i$  für jedes  $c \in K$  invertierbar und

$$\sum_{i=0}^{\infty} c^i x^i = \frac{1}{1 - cx}$$

**Beweis**

$$\begin{aligned}
 (1 - cx) \sum_{i=0}^{\infty} c^i x^i &= \sum_{i=0}^{\infty} c^i x^i - cx \sum_{i=0}^{\infty} c^i x^i \\
 &= \sum_{i=0}^{\infty} c^i x^i - c \sum_{i=0}^{\infty} c^i x^{i+1} \\
 &= \sum_{i=0}^{\infty} c^i x^i - \sum_{i=0}^{\infty} c^{i+1} x^{i+1} \\
 &= \sum_{i=0}^{\infty} c^i x^i - \sum_{k=0}^{\infty} c^k x^k \\
 &= c^0 \cdot x^0 \\
 &= 1
 \end{aligned}$$

(Bemerkung: Wegen  $\frac{1}{1-cx} = \sum_{i=0}^{\infty} c^i x^i$  ist  $\frac{1}{1-cx}$  eine formale Potenzreihe.) □

### 1.35 Beispiel (Code mit variabler Wortlänge zum Komprimieren von Daten)

Seien  $B_n := \{a, b, c\}$  und  $Z := \{0, 1\}$ .

Für  $k \in \mathbb{N}$  sei  $W_k := \{\text{Folgen aus } i \text{ Buchstaben gefolgt von } k-i \text{ Ziffern} \mid 1 < i < k\}$ .

(Z.B.:  $\underbrace{ab0}_{\in W_3}, \underbrace{abb0010}_{\in W_7}, \underbrace{abc11}_{\in W_5}$ )

Es gilt:

$$W_k = |W_k| = \sum_{i=1}^{k-1} 3^i \cdot 2^{k-i} = \sum_{k=0}^k \underbrace{3^i 2^{k-i}}_{:=c_k} - 2^k - 3^k = (3^{k+1} - 2^{k+1}) - 2^k - 3^k = 2 \cdot 3^k - 2^k$$

#### Behauptung

$$c_k = 3^{k+1} - 2^{k+1}$$

#### Beweis

$$\begin{aligned} \sum_{k=0}^{\infty} c_k x^k &= \sum_{k=0}^{\infty} \left( \sum_{i=0}^k 3^i 2^{k-i} \right) x^k \\ &= \left( \sum_{i=0}^{\infty} 3^i x^i \right) \left( \sum_{i=0}^{\infty} 2^i x^i \right) \\ &= \frac{1}{1-3x} \cdot \frac{1}{1-2x} \\ &= \frac{3}{1-3x} - \frac{2}{1-2x} \\ &= 3 \cdot \left( \sum_{k=0}^{\infty} 3^k x^k \right) - 2 \cdot \left( \sum_{k=0}^{\infty} 2^k x^k \right) \\ &= \sum_{k=0}^{\infty} \underbrace{(3^{k+1} - 2^{k+1})}_{:=c_k} x^k \end{aligned} \quad \square$$

### 1.36 Satz (Inversion von Potenzreihen)

Genau dann ist  $A = \sum_{n=0}^{\infty} a_n x^n \in K[[X]]$  invertierbar, wenn  $a_0 \neq 0$  ist.

#### Beweis

$A$  ist invertierbar  $\Leftrightarrow$  es gibt  $B = \sum_{n=0}^{\infty} b_n x^n$  mit  $A \cdot B = 1$

$$\begin{aligned} A \cdot B = \sum_{n=0}^{\infty} \left( \sum_{k=0}^n a_k b_{n-k} \right) x^n = 1 &\Leftrightarrow \sum_{k=0}^n a_k b_{n-k} = \begin{cases} 1 & , \text{ für } n = 0 \\ 0 & , \text{ sonst} \end{cases} \\ &\Leftrightarrow \begin{array}{ll} a_0 b_0 = 1 & n = 0 \\ a_0 b_1 + a_1 b_0 = 0 & n = 1 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 & n = 2 \\ \vdots & \vdots \end{array} \end{aligned}$$

Ist  $A$  invertierbar, so muss  $a_0 \neq 0$  sein. Umgekehrt ist  $a_0 \neq 0$ , so definiere:

$$b_0 = \frac{1}{a_0} \in K, \quad b_n = -\frac{1}{a_0} (a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_n b_0) \text{ rekursiv, } n \in \mathbb{N}. \quad \square$$

### 1.37 Beispiel

(1)  $A = 1 - cx = \sum_{n=0}^{\infty} a_n x^n$  mit  $a_0 = 1, a_2 = -c, a_3 = a_4 = \dots = 0$

Bestimme  $A^{-1}$ .

Lösung: Sei  $A^{-1} = \sum_{n=0}^{\infty} b_n x^n$ . dann gilt:  $a_0 b_0 = 1 \Rightarrow b_0 = 1$

$$a_0 b_1 + a_1 b_0 = 0 \Leftrightarrow 1 \cdot b_1 - c \cdot 1 = 0 \Rightarrow b_1 = c \dots b_n = c^n$$

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \Rightarrow b_2 = c^2$$

Also:  $\frac{1}{1-cx} = \sum_{n=0}^{\infty} c^n x^n$  („geometrische Reihe“)

(2)  $\frac{1}{(1-cx)^2} = \frac{1}{1-cx} \cdot \frac{1}{1-cx} = \left( \sum_{n=0}^{\infty} c^n x^n \right) \cdot \left( \sum_{n=0}^{\infty} c^n x^n \right) = \sum_{n=0}^{\infty} \left( \sum_{k=0}^n \underbrace{c^k c^{n-k}}_{:=c^n} \right) x^n = \sum_{n=0}^{\infty} (n+1) c^n x^n$

Insbesondere:  $\frac{c}{(1-cx)^2} = \sum_{n=0}^{\infty} (n+1) c^{n+1} x^n$  (Ableitung?) □

### 1.38 Definition (Ableitung)

Die Abbildung  $D : K[[X]] \rightarrow K[[X]]$  mit  $\sum_{n=0}^{\infty} a_n x^n \rightarrow \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n$  heißt FORMALE ABLEITUNG.

Bemerkung:  $D : K[[X]] \rightarrow K[[X]]$  ist eine Operation auf Folgen:

$$D : a_0, a_1, a_2, \dots, a_n, \dots \rightarrow \underbrace{a_1}_{x^0}, \underbrace{2 \cdot a_2}_{x^1}, 3 \cdot a_3, \dots, \underbrace{n \cdot a_n}_{x^{n-1}}, \dots$$
 □

### 1.39 Lemma

$D : K[[X]] \rightarrow K[[X]]$  ist  $K$ -linear und es gilt:

(a)  $D(x^n) = nx^{n-1}, n \geq 1$

(b)  $D(A \cdot B) = D(A) \cdot B + A \cdot D(B)$

#### Beweis

Nachrechnen! □

### 1.40 Folgerung

Ist  $A \in K[[X]]$  invertierbar, so ist

$$D(A^{-1}) = -\frac{D(A)}{A^2}$$

#### Beweis

$$A \cdot A^{-1} = 1, D(1) = 0$$

$$\Rightarrow 0 = D(1) = D(A \cdot A^{-1}) = D(A) \cdot A^{-1} + A \cdot D(A^{-1})$$

$$\Rightarrow A \cdot D(A^{-1}) = -D(A) \cdot A^{-1}$$

$$\Rightarrow D(A^{-1}) = -\frac{D(A)}{A^2}$$
 □

**Neuer Beweis zum Beispiel 1.37 (2)**

$$A = 1 - cx \in K[[X]], A^{-1} := \sum_{n=0}^{\infty} c^n x^n = \frac{1}{1 - cx}, D(A) = -c$$

$$D(A^{-1}) \stackrel{\text{Def. 1.38}}{=} \sum_{n=0}^{\infty} (n+1)c^{n+1}x^n$$

$$\stackrel{\text{Folgerung 1.40}}{\Rightarrow} D(A^{-1}) = -\frac{D(A)}{A^2} = -\frac{-c}{(1 - cx)^2} = \sum_{n=0}^{\infty} (n+1)c^{n+1}x^n$$

$$\Rightarrow \frac{1}{(1 - cx)^2} = \sum_{n=0}^{\infty} (n+1)c^n x^n \quad \square$$

**1.41 Folgerung**

Für  $m \in \mathbb{N}$  gilt:

$$\frac{1}{(1 - cx)^m} = \sum_{n=0}^{\infty} \binom{n+m-1}{m-1} c^n x^n$$

**Beweis**

Übung. □

**1.42 Bemerkung**

- Erzeugende Funktionen kann man im Prinzip wie ganz normale Funktionen (in der Analysis) behandeln.
- Falls es zu einer Funktion  $F$  (aus der Analysis) eine Potenzreihe gibt, dann kann man diese durch Taylor-Entwicklung um die Null beschreiben:

$$F(x) = \sum_{n=0}^{\infty} \frac{F^{(n)}(0)}{n!} x^n := \left( \frac{F^{(n)}(0)}{n!} \right)_{n \in \mathbb{N}_0} \quad \square$$

**Formale Potenzreihen und ihre erzeugenden Funktionen (vgl. Tabelle 1.2)**

Für  $r \in \mathbb{R}$  definiert man (verallgemeinerte Binomialkoeffizienten):

$$\binom{r}{0} = 1, \binom{r}{k} = \frac{r \cdot (r-1) \cdot (r-2) \cdots (r-k+1)}{k!} \quad \forall k \in \mathbb{N}$$

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k, n \in \mathbb{N}$$

$$\stackrel{\text{verallg.}}{\Rightarrow} (1+x)^y = \sum_{k=0}^{\infty} \binom{y}{k} x^k, y \in \mathbb{R}. \quad \square$$

**§ 5 Rekursionsgleichungen****Einige grundlegende algorithmische Verfahren**

- Divide and Conquer-Algorithmen

Idee:

- teile das zu lösende Problem  $P$  in kleinere Teilprobleme auf (Divide)
- löse die Teilprobleme
- berechne aus dem Lösungen der Teilprobleme die Lösung von  $P$  (Conquer)

Tabelle 1.2: Formale Potenzreihen und ihre erzeugenden Funktionen

$a_n$	Folge	Potenzreihe	erzeugende Funktion
1	1, 1, 1, ...	$\sum_{n=0}^{\infty} x^n$	$\frac{1}{1-x}$
$n$	0, 1, 2, ...	$\sum_{n=0}^{\infty} nx^n$	$\frac{1}{(1-x)^2}$
$c^n$	1, $c$ , $c^2$ , ...	$\sum_{n=0}^{\infty} c^n x^n$	$\frac{1}{1-cx}$
$n^2$	0, 1, 2, 4, ...	$\sum_{n=0}^{\infty} n^2 x^n$	$\frac{x(1+x)}{(1-x)^3}$
$\binom{r}{n}$	1, $r$ , $\binom{r}{2}$ , ...	$\sum_{n=0}^{\infty} \binom{r}{n} x^n$	$\frac{1}{(1+x)^r}$
$\binom{r+n}{n}$	1, $r+1$ , $\binom{r+2}{2}$ , ...	$\sum_{n=0}^{\infty} \binom{r+n}{n} x^n$	$\frac{1}{(1-x)^{r+1}}$
$\frac{1}{n}$	0, 1, $\frac{1}{2}$ , ...	$\sum_{n=1}^{\infty} \frac{1}{n} x^n$	$\ln \frac{1}{1-x}$
$\frac{1}{n!}$	1, 1, $\frac{1}{2}$ , ...	$\sum_{n=0}^{\infty} \frac{1}{n!} x^n$	$e^x$

Beispiele: Binäre Suche, Merge-Sort, euklidischer Algorithmus

- dynamische Programmierung (Optimierungsprobleme)
- Greedy-Algorithmus

Bei der Analyse von Algorithmen kommen Funktionen der Form

$$F(n) = F(n-1) + F(n-2), n \geq 2 \text{ und } F(1) = 1, F(0) = 0$$

oder

$$T(n) = T\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + T\left(\left\lceil \frac{n}{2} \right\rceil\right), n \geq 2 \text{ und } T(1) = 1$$

vor. Für die Bestimmung der Laufzeit (Anzahl der Rechenschritte) von Algorithmen spielt das Lösen von Rekursionsgleichungen eine zentrale Rolle.  $\square$

### 1.43 Definition (Rekursionsgleichung)

Eine Rekursionsgleichung der Form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} + b_k \quad \forall n \geq k \quad (*)$$

mit den Anfangsbedingungen  $a_i = b_i, i = 0, 1, \dots, k-1$ , heißt LINEARE REKURSIONSGLEICHUNG  $k$ -ter Ordnung.

Gilt  $b_k = 0$ , so heißt (\*) eine HOMOGENE LINEARE REKURSIONSGLEICHUNG.

Gilt  $b_k \neq 0$ , so heißt (\*) eine INHOMOGENE LINEARE REKURSIONSGLEICHUNG.  $\square$

### 1.44 Beispiel

(1) Spezialfall der homogenen linearen Rekursionsgleichung:

$$a_n = c \cdot a_{n-1}, n \geq 1, a_0 = b_0$$

$$a_1 = c \cdot a_0 = c \cdot b_0$$

$$a_2 = c \cdot a_1 = c \cdot c \cdot b_0 = c^2 \cdot b_0$$

$$\text{Lösung der Gleichung: } a_n = b_0 \cdot c^n$$

(2) Spezialfall der inhomogenen linearen Rekursionsgleichung:

$$a_n = c \cdot a_{n-1} + b_1, n \geq 1, a_0 = b_0 \text{ mit } c, b_0, b_1 \text{ konstant}$$

Behauptung:

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

Beweis (durch Induktion über  $n$ ):

$$n = 1: a_1 = c \cdot \underbrace{a_0}_{=b_0} + b_1 = \begin{cases} b_0 \cdot c^1 + b_1 \cdot \frac{c^1 - 1}{c - 1} & , \text{ falls } c \neq 1 \\ b_0 + 1 \cdot b_1 & , \text{ falls } c = 1 \end{cases}$$

$$n \mapsto n + 1:$$

1. Fall:  $c \neq 1$ :

$$\begin{aligned} a_n &= c \cdot a_{n-1} + b_1 = c \cdot \left( b_0 \cdot c^{n-1} + b_1 \cdot \frac{c^{n-1} - 1}{c - 1} \right) + b_1 \\ &= b_0 \cdot c^n + b_1 \cdot \left( \frac{c^n - 1}{c - 1} + 1 \right) = b_0 \cdot c^n + b_1 \cdot \frac{c^n - 1}{c - 1} \end{aligned}$$

2. Fall:  $c = 1$ :

$$a_n = a_{n-1} + b_1 = (b_0 + (n-1) \cdot b_1) + b_1 = b_0 + n \cdot b_1 \quad \square$$

### 1.45 Beispiel

$a_n$  := Anzahl der Wörter mit der Länge  $n$  über  $\{a, b\}$ , die keine zwei aufeinander folgende  $a$ 's enthalten.  
(Z.B.:  $a_1 = 2$  (a, b),  $a_2 = 3$  (ab, ba, bb))

$$a_n = a_{n-1} + a_{n-2}, n \geq 3 \quad \square$$

### 1.46 Beispiel (Fibonacci-Zahlen)

Ein Kaninchen bringt ab seinem zweiten Lebensmonat jeden Monat ein weiteres Kaninchen zur Welt. Falls Kaninchen unsterblich wären, wie viele Kaninchen werden durch ein einziges Kaninchen nach  $n$  Monaten geboren ( $F_n$ )?

Antwort:  $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 1 + 1 = 2, F_4 = 1 + 2 = 3, \dots, F_n = F_{n-1} + F_{n-2}$

Die Zahlen  $F_n$  für  $n \in \mathbb{N}_0$  definiert durch  $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$  für  $n \geq 2$  heißen FIBONACCI-ZAHLEN.

Nun berechnen wir  $F_n$  explizit mit Hilfe der erzeugenden Funktionen:

$$\begin{aligned} F &= F(x) = \sum_{n=0}^{\infty} F_n \cdot x^n \\ &= F_0 \cdot x^0 + F_1 \cdot x^1 + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) \cdot x^n \\ &= F_0 \cdot x^0 + F_1 \cdot x^1 + \sum_{n=2}^{\infty} F_{n-1} \cdot x^n + \sum_{n=2}^{\infty} F_{n-2} \cdot x^n \\ &= F_0 \cdot x^0 + F_1 \cdot x^1 + x \cdot F - F_0 \cdot x + x^2 \cdot F \\ &\quad \underbrace{=}_{F_0=0, F_1=0} x + x \cdot F + x^2 \cdot F \end{aligned}$$

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

Seien nun  $\alpha, \beta, a, b \in \mathbb{C}$  mit  $\frac{x}{1-x-x^2} = \frac{a}{1-\alpha \cdot x} + \frac{b}{1-\beta \cdot x}$ .

Dann gilt:

$$\sum_{n=0}^{\infty} F_n \cdot x^n = F = \frac{a}{1-\alpha \cdot x} + \frac{b}{1-\beta \cdot x} = a \cdot \sum_{n=0}^{\infty} \alpha^n x^n + b \cdot \sum_{n=0}^{\infty} \beta^n x^n = \sum_{n=0}^{\infty} (a \cdot \alpha^n + b \cdot \beta^n) \cdot x^n$$

Somit gilt:

$$F_n = a \cdot \alpha^n + b \cdot \beta^n$$

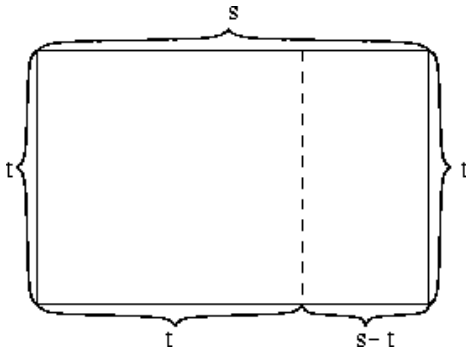
$$\begin{aligned} \text{Wegen } \frac{x}{1-x-x^2} & \stackrel{\text{quadr. Ergänzung}}{=} \frac{x}{\frac{5}{4} - (x + \frac{1}{2})^2} = \frac{x}{\left[\frac{\sqrt{5}}{2} - (x + \frac{1}{2})\right] \cdot \left[\frac{\sqrt{5}}{2} + (x + \frac{1}{2})\right]} \\ & = \frac{?}{\left(\frac{\sqrt{5}-1}{2} - x\right)} + \frac{?}{\left(\frac{\sqrt{5}+1}{2} + x\right)} \quad (\text{Partialbruchzerl.}) \\ & = \frac{\frac{1}{\sqrt{5}}}{1 - \frac{\sqrt{5}+1}{2} \cdot x} + \frac{-\frac{1}{\sqrt{5}}}{1 - \frac{1-\sqrt{5}}{2} \cdot x} \end{aligned}$$

$$\text{D.h.: } \alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}, a = \frac{1}{\sqrt{5}}, b = -\frac{1}{\sqrt{5}}$$

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

### 1.47 Bemerkung (Goldener Schnitt)

Die Zahl  $\frac{1+\sqrt{5}}{2} = \Theta$  heißt GOLDENER SCHNITT. Diese Zahl taucht bei verschiedenen Untersuchungen auf, z.B.:



(1)

Bedingung:

$$\frac{s}{t} = \frac{t}{s-t} \left( = \frac{1}{\frac{s}{t}-1} \right), \quad 0 < t < s$$

Setze:  $\frac{s}{t} = x$ . Dann gilt:

$$x = \frac{1}{x-1} \Leftrightarrow x^2 - x - 1 = 0 \Leftrightarrow x_{1,2} = \frac{1 \pm \sqrt{5}}{2}$$

$$\text{Somit ist } x \left( = \frac{s}{t} \right) = \frac{1+\sqrt{5}}{2}$$



(2) 0

$$\frac{1}{x} = \frac{x}{1-x}, \quad 0 < x < 1$$

$$\text{Es gilt: } \frac{x}{1-x} = \frac{1}{x} \Leftrightarrow x^2 + x - 1 = 0 \quad (pq\text{-Formel}) \Leftrightarrow x_{1,2} = \frac{-1 \pm \sqrt{5}}{2}$$

$$\Rightarrow x = \frac{\sqrt{5}-1}{2} = \frac{2}{1+\sqrt{5}} = \frac{1}{\vartheta} \approx 0,618 \quad \square$$

### 1.48 Satz

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} \text{ für } a_1 = b_1, a_0 = b_0$$

Seien  $\alpha, \beta$  zwei Lösungen der Gleichung  $x^2 - c_1 x - c_2 = 0$  und

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

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

Dann gilt:

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

#### Beweis

Induktion über  $n$ , analog zum Beweis von Beispiel 1.44 (2). □

### Schema zum Lösen von (homogenen) linearen Rekursionsgleichungen

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} \text{ für } n \geq k$$

mit  $a_i = b_i$  für  $i = 0, 1, \dots, k-1$

#### (1) Aufstellen der erzeugenden Funktion:

$$A(x) = \sum_{n=0}^{\infty} a_n x^n$$

#### (2) Anwendung der Rekursionsgleichung:

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1} + \sum_{n=k}^{\infty} a_n x^n \\ &= b_0 + b_1 x + \dots + b_{k-1} x^{k-1} + \sum_{n=k}^{\infty} (c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}) x^n \\ &= b_0 + b_1 x + \dots + b_{k-1} x^{k-1} + \sum_{n=k}^{\infty} c_1 a_{n-1} x^n + \sum_{n=k}^{\infty} c_2 a_{n-2} x^n + \dots + \sum_{n=k}^{\infty} c_k a_{n-k} x^n \\ &= b_0 + b_1 x + \dots + b_{k-1} x^{k-1} + c_1 x \sum_{n=k}^{\infty} a_{n-1} x^{n-1} + c_2 x^2 \sum_{n=k}^{\infty} a_{n-2} x^{n-2} + \dots + c_k x^k \sum_{n=k}^{\infty} a_{n-k} x^{n-k} \\ &= b_0 + b_1 x + \dots + b_{k-1} x^{k-1} + c_1 x \cdot \left( A(x) - \sum_{i=0}^{k-2} a_i x^i \right) + c_2 x^2 \cdot \left( A(x) - \sum_{i=0}^{k-3} a_i x^i \right) + \dots \\ &= b_0 + b_1 x + \dots + b_{k-1} x^{k-1} + c_1 x \left( A(x) - \sum_{i=0}^{k-2} a_i x^i \right) + c_2 x^2 \left( A(x) - \sum_{i=0}^{k-3} a_i x^i \right) + \dots + c_k x^k \cdot A(x) \end{aligned}$$

#### (3) Auflösen nach A(x):

$$A(x) = \frac{d_0 + d_1 x + \dots + d_{k-1} x^{k-1}}{1 - c_1 x - c_2 x^2 - \dots - c_k x^k} \text{ für geeignete } d_0, d_1, \dots, d_{k-1}.$$

(4) **Partialbruchzerlegung der rechten Seite** (in  $\mathbb{C}$ , vgl. AfI, 9. Übung, Aufgabe 8)

Sei  $1 - c_1x - c_2x^2 - \dots - c_kx^k = (1 - \alpha_1 \cdot x)^{m_1} \cdot (1 - \alpha_2 \cdot x)^{m_2} \dots (1 - \alpha_t \cdot x)^{m_t}$  mit  $\sum_{i=1}^t m_i = k$  und sei:

$$A(x) = \frac{d_0 + d_1x + \dots + d_{k-1}x^{k-1}}{1 - c_1x - \dots - c_kx^k} = \frac{g_1(x)}{(1 - \alpha_1x)^{m_1}} + \dots + \frac{g_t(x)}{(1 - \alpha_tx)^{m_t}} = \sum_{i=1}^t \frac{g_i(x)}{(1 - \alpha_ix)^{m_i}}$$

Wobei  $g_i(x)$  ein Polynom mit Grad  $\leq m_i - 1$  für  $i = 1, \dots, t$  ist.

(5) **Nach Tabelle 1.2:**

$$A(x) = \sum_{i=1}^t \frac{g_i(x)}{(1 - \alpha_ix)^{m_i}} = \sum_{i=1}^t g_i(x) \left( \sum_{n=0}^{\infty} \binom{n + m_i - 1}{m_i - 1} \cdot (\alpha_ix)^n \right) \underbrace{=}_{\text{umformen}} \sum_{n=0}^{\infty} g_n \cdot x^n$$

Dann gilt:  $a_n = g_n, n \geq k$

□

### 1.49 Beispiel

$$a_n = 5a_{n-1} - 7a_{n-2} + 3a_{n-3}, n \geq 3 \text{ mit } a_0 = 1, a_1 = 5, a_2 = 19$$

**Lösung:**

Sei  $A(x) = \sum_{n=0}^{\infty} a_n x^n$ . Dann gilt:

$$\begin{aligned} A(x) &= a_0 + a_1x + a_2x^2 + \sum_{n=3}^{\infty} (5a_{n-1} - 7a_{n-2} + 3a_{n-3})x^n \\ &= a_0 + a_1x + a_2x^2 + 5x \left( \sum_{n=3}^{\infty} a_{n-1}x^{n-1} \right) - 7x^2 \left( \sum_{n=3}^{\infty} a_{n-2}x^{n-2} \right) + 3x^3 \left( \sum_{n=3}^{\infty} a_{n-3}x^{n-3} \right) \\ &= a_0 + a_1x + a_2x^2 + 5x(A(x) - (a_0 + a_1x)) - 7x^2(A(x) - a_0) + 3x^3A(x) \\ &= 1 + 5x + 19x^2 + 5x(A(x) - (1 + 5x)) - 7x^2(A(x) - 1) + 3x^3A(x) \\ \Rightarrow A(x) &= \frac{1 + x^2}{1 - 5x + 7x^2 - 3x^2} = \frac{1 + x^2}{(1 - x)^2(1 - 3x)} \\ &= \frac{\frac{1}{2}x - \frac{3}{2}}{(1 - x)^2} + \frac{\frac{5}{2}}{1 - 3x} \\ &= \frac{1}{2}(x - 3) \cdot \frac{1}{(1 - x)^2} + \frac{5}{2} \frac{1}{1 - 3x} \\ &= \frac{1}{2}(x - 3) \cdot \sum_{n=0}^{\infty} \overbrace{\binom{n+1}{1}}^{=n+1} x^n + \frac{5}{2} \sum_{n=0}^{\infty} (3x)^n \\ &= 1 + 5x + \sum_{n=2}^{\infty} \left( \frac{5}{2} 3^n - n + \frac{3}{2} \right) x^n \end{aligned}$$

$$\Rightarrow a_n = \frac{5}{2} \cdot 3^n - n - \frac{3}{2}, n \geq 2$$

□

### 1.50 Beispiel (Catalan-Zahlen)

Klammer:  $( \quad , \quad )$  (2 Klammern)

öffnende schließende  
Klammerketten:  $(( ))( ), ( )(), ()(())$

Zulässige Klammerkette:

An jeder Stelle der Klammernkette ist die Anzahl der bis zu dieser Stelle vorkommenden öffnenden Klammern  $\geq$  Anzahl der bis zu dieser Stelle vorkommenden schließenden Klammern und zum Schluss sollen beide Anzahlen gleich sein.

$C_n := | \{ \text{zulässige Klammernketten mit } 2n \text{ Klammern} \} |$

Frage:  $C_n = ?$ ,  $n \in \mathbb{N}$

$$\begin{aligned} c_0 &:= 1 \\ c_1 &:= 1 \quad () \\ c_2 &:= 2 \quad (()), ()() \\ c_3 &:= 5 \quad ()(), (()), (()), ()(), (())() \end{aligned} \quad \square$$

### 1.51 Lemma

$$c_n = \sum_{k=1}^n c_{k-1} \cdot c_{n-k}, n \geq 1$$

**Beweis**

$$\left( \underbrace{\quad \quad \quad}_{\text{zulässige } 2(k-1) \text{ Klammern}} \right) \cdot \underbrace{\quad \quad \quad}_{\text{zulässige } 2n-2k \text{ Klammern}}$$

$A_k := \{ \text{zulässige Klammernkette mit } 2n \text{ Klammern, dessen erste öffnende Klammer an der Position } 2k \text{ geschlossen wird} \}$

$$\Rightarrow | \bigsqcup_{k=1}^n A_k | = \sum_{k=1}^n | A_k | = \sum_{k=1}^n c_{k-1} \cdot c_{n-k} \quad \square$$

### 1.52 Satz

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

**Beweis**

Sei  $c(x) = \sum_{n=0}^{\infty} c_n \cdot x^n$

Dann gilt:

$$\begin{aligned} c(x) &= c_0 x^0 + \sum_{n=1}^{\infty} c_n x^n \\ &\stackrel{\text{Lemma}}{=} c_0 + \sum_{n=1}^{\infty} \left( \sum_{k=1}^n c_{k-1} c_{n-k} \right) x^n \\ &= c_0 + x \sum_{n=1}^{\infty} \left( \sum_{k=1}^n c_{k-1} c_{n-k} \right) x^{n-1} \\ &\stackrel{t=n-1}{=} c_0 + x \sum_{t=0}^{\infty} \left( \sum_{k=1}^{t+1} c_{k-1} c_{(t+1)-k} \right) x^t \\ &\stackrel{s=k-1}{=} c_0 + x \sum_{t=0}^{\infty} \left( \sum_{s=0}^t c_s c_{t-s} \right) x^t \\ &\stackrel{\text{Def. 1.29}}{=} c_0 + x \cdot c(x) \cdot c(x) \end{aligned}$$

Somit gilt:

$$x c^2(x) - c(x) = -1 \quad | \cdot x$$

$$\begin{aligned}
 x^2 c^2(x) - c(x) &= -x \\
 \Rightarrow (xc(x) - \frac{1}{2})^2 &= \frac{1}{4} - x \\
 \Rightarrow xc(x) - \frac{1}{2} &= \pm \frac{1}{2}(1 - 4x)^{\frac{1}{2}} \\
 \underbrace{\sum_{n=0}^{\infty} c_n x^{n+1}}_{0+c_0x+c_1x^2+\dots} &= x \underbrace{c(x)}_{\sum_{n=0}^{\infty} c_n x^n} = \frac{1}{2}(1 \pm (1 - 4x)^{\frac{1}{2}}) \\
 &= \frac{1}{2} [1 \pm \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n] \\
 \text{Tabelle 1.2} \\
 &= \frac{1}{2} \cdot \underbrace{(1 \pm 1 + \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n \cdot x^n)}_{\text{Koeffizient von } x^6 \text{ ist } 0 \Rightarrow, - \text{ als Vorzeichen}}
 \end{aligned}$$

Das heißt:

$$\begin{aligned}
 c_0x + c_1x^2 + \dots &= -\frac{1}{2} \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n+1} (-4)^n x^n \\
 \Rightarrow c_n &= -\frac{1}{2} \binom{\frac{1}{2}}{n+1} (-4)^{n+1} \\
 &= -\frac{1}{2} \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)\dots(\frac{1}{2}-n)}{(n+1)!} (-1)^{n+1} 4^{n+1} \\
 &= (-1)^{n+2} \frac{(\frac{1}{2}-1)(\frac{1}{2}-2)\dots(\frac{1}{2}-n)}{(n+1)!} 4^n \\
 &= \frac{(2-1)(4-1)\dots(2n-1)}{(n+1)n!} 2^n n! \\
 &= \frac{[1 \cdot 3 \cdot \dots \cdot (2n-1)][2 \cdot 4 \cdot \dots \cdot 2n]}{(n+1)n!n!} \\
 &= \frac{1}{n+1} \frac{(2n)!}{n!n!} \\
 &= \frac{1}{n+1} \binom{2n}{n} \quad \square
 \end{aligned}$$

### Schema zum Lösen von (allgemeinen) Rekursionsgleichungen

$a_n = f(a_{n-1}, a_{n-2}, \dots, a_{n-k}), n \geq k \leftarrow$  Rekursionsgleichung

$a_i = b_i, i = 0, 1, 2, \dots, k-1 \leftarrow$  Anfangswerte

Berechne  $a_n, n \geq k$  explizit:

- (1) Aufstellen der erzeugenden Funktion  $A(x) = \sum_{n=0}^{\infty} a_n x^n$ .
- (2) Forme  $\sum_{n=0}^{\infty} a_n x^n$  so um, dass Anfangswerte und Rekursionsgleichung eingesetzt werden können.
- (3) Weiter umformen, bis auf der rechten Seite die noch vorhandenen unendlichen Summen (und mit ihnen alle Vorkommen von Folgigliedern  $a_n$ ) durch  $A(x)$  ersetzt werden können.
- (4) Auflösen der erhaltenen Gleichung nach  $A(x)$ . Dadurch erhält man eine Gleichung der Form  $A(x) = g(x)$ , wobei  $g$  eine (hoffentlich einfache) Funktion ist.
- (5) Umschreiben der Funktion  $g$  als formale Potenzreihe (z.B. durch Partialbruchzerlegung und / oder durch Nachschlagen in 1.2).
- (6) Ablesen der expliziten Darstellung für die  $a_n$  (durch Koeffizientenvergleich). □



## 2 Graphentheorie

### § 1 Grundbegriffe der Graphentheorie

#### 2.1 Definition (Graph)

Ein GRAPH ist ein Paar  $G = (V, E)$ , wobei

- $V$  eine endliche Menge,
- $E \subseteq \binom{V}{2} := \{\{x, y\} \mid x, y \in V, x \neq y\}$

ist.

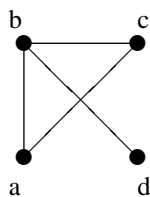
Die Elemente von  $V$  heißen ECKEN (oder PUNKTE, KNOTEN, engl. VERTICES). Die Elemente von  $E$  heißen KANTEN (engl. EDGES).

Statt  $\{x, y\} \in E$  schreiben wir auch nur  $xy \in E$ .

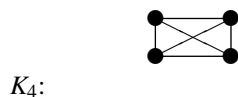
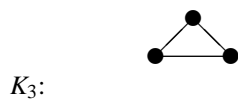
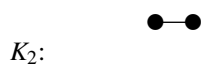
Ein Graph  $G = (V, E)$  wird i.A. durch ein Diagramm dargestellt, indem man jede Ecke  $x \in V$  durch einen Punkt repräsentiert und zwei Ecken  $x, y \in V$  genau dann durch eine Linie verbindet, wenn  $xy \in E$  ist.  $\square$

#### 2.2 Beispiel

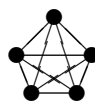
- (1)  $G = (\{a, b, c, d\}, \{ab, bc, ca, bd\})$



- (2) Vollständige Graphen :  $K_n = \left(V, \binom{V}{2}\right)$  mit  $|V| = n$

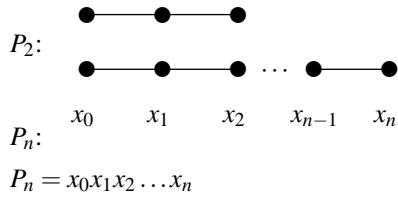


$K_5$ :

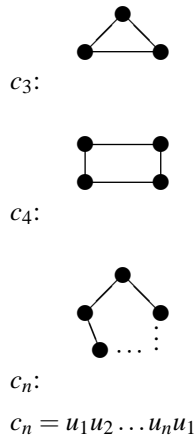


- (3) Wege:





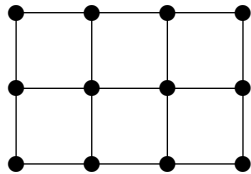
(4) Kreise:



(5) Gittergraphen:

$M_{m,n}$ :  $m \cdot n$  Ecken werden wie in einem Gitter mit  $m$  Zeilen und  $n$  Spalten verbunden.

Z.B.  $M_{3,4}$ :



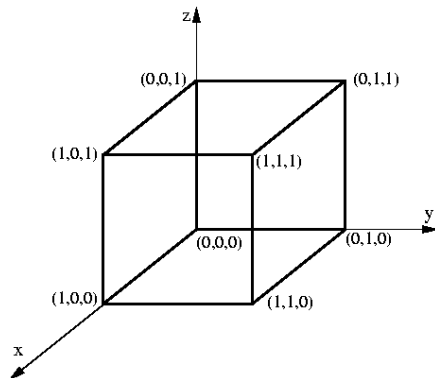
(6)  $d$ -dimensionale Hyperwürfel  $Q_d$ :

$V(Q_d)$  := die Menge aller 0-1-Folgen der Länge  $d$

$(\underbrace{0, 1, 0, 1, \dots, 0}_d \text{ Zahlen})$

$E(Q_d) := \{xy \mid x, y \in V(Q_d), x \text{ und } y \text{ unterscheiden sich an genau einer Stelle}\}$

Z.B.  $Q_3$ :



□

### 2.3 Bemerkung (leerer Graph)

(1) In dieser Vorlesung betrachten wir nur Graphen ohne MEHRFACHKANTEN und ohne SCHLEIFEN.

Ein Graph ohne Schleifen heißt MULTIGRAPH, ein Graph ohne Schleifen und ohne Mehrfachkanten heißt SCHLICHTER GRAPH.

$G = (\emptyset, \emptyset)$  heißt LEERER GRAPH.

$G = (V, \emptyset)$  heißt NULL-GRAPH.

(2) Sei  $G = (V, E)$  und  $e = xy \in E$

- $x$  und  $y$  heißen Endecken von  $e$ .
- $e$  INZIDIERT mit den Ecken  $x$  und  $y$ .
- $x$  und  $y$  sind durch  $e$  verbunden.
- $x$  und  $y$  heißen benachbart oder ADJAZENT. □

### 2.4 Definition (Ecken eines Graphen)

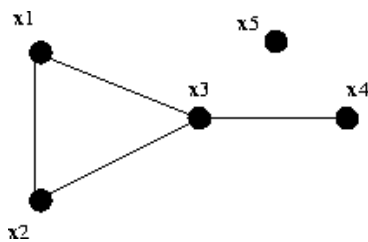
Sei  $G = (V, E)$  und  $x \in V$

- $N(x) = \{y \in V | xy \in E\}$  heißt die NACHBARSCHAFT von  $x$  in  $G$ .
- $d_G = |N(x)|$  heißt der ECKENGRAD von  $x$  in  $G$ .  
Ist  $d(x) = 1$ , so heißt  $x$  ENDECKE .  
Ist  $d(x) = 0$  so heißt  $x$  ISOLIERTE ECKE .
- $\delta(G) = \min_{x \in V} d(x)$ ,  $\Delta(G) = \max_{x \in V} d(x)$
- Ist  $\delta(G) = \Delta(G) = k$ , so heißt  $G$   $k$ -REGULÄR.  
Z.B. ist  $K_n$  ist  $(n - 1)$ -regulär. □

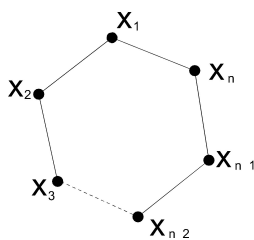
### 2.5 Beispiel

(1)  $N(x_1) = \{x_2, x_3\}, N(x_3) = \{x_1, x_2, x_4\}$

$d(x_1) = 2, d(x_2) = 2, d(x_3) = 3, d(x_4) = 1$  (Endecke),  $d(x_5) = 0$  (isoliert)



(2)  $C_n$  ist 2-regulär.



**2.6 Satz** (Handschlaglemma, Euler 1736)

Sei  $G = (V, E)$ . Dann gilt:  $\sum_{x \in V} d(x) = 2|E|$ .

**Beweis** (doppeltes Abzählen, vgl. Lemma 1.11)

In  $\sum_{x \in V} d(x)$  wird jede Kante  $x \longleftrightarrow y$  genau zwei Mal gezählt (zum ersten Mal in  $d(x)$ , zum zweiten Mal in  $d(y)$ ). Auf der rechten Seite wird jede Kante ebenfalls zweimal gezählt. □

**2.7 Folgerung**

Für jeden Graphen  $G = (V, E)$  gilt: Die Anzahl der Ecken mit ungeradem Grad ist gerade.

**Beweis**

Nach Satz 2.6 gilt:

$$\underbrace{2|E|}_{\text{gerade}} = \sum_{x \in V} d(x) = \underbrace{\sum_{\substack{x \in V \\ d(x) \text{ gerade}}} d(x)}_{\Rightarrow \text{gerade}} + \underbrace{\sum_{\substack{x \in V \\ d(x) \text{ ungerade}}} d(x)}_{\Rightarrow \text{gerade}}$$

Auf einem Empfang geben immer gerade viele Gäste ungerade vielen die Hand. □

**2.8 Lemma**

Sei  $G = (V, E)$  mit  $|V| \geq 2$ . Dann gibt es immer zwei Ecken  $x, y \in V$  mit  $d(x) = d(y)$ .

**Beweis** (Schubfachprinzip, vgl. Beispiel 1.13 (2))

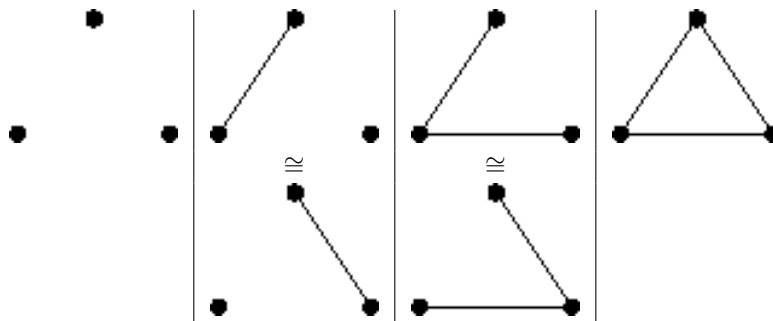
Übung. □

**2.9 Definition** (isomorphe Graphen)

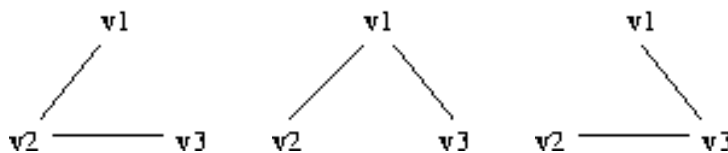
Es seien  $G = (V, E)$  und  $G' = (V', E')$  zwei Graphen.  $G$  ist ISOMORPH zu  $G'$  (in Zeichen  $G \cong G'$ )  $\Leftrightarrow$  Es gibt eine bijektive Abbildung  $\Phi : V \rightarrow V'$  mit  $xy \in E \Leftrightarrow \Phi(x)\Phi(y) \in E'$ . □

**2.10 Beispiel**

(1) Nicht-isomorphe Graphen mit 3 Ecken:



(2) Werden die Namen von Ecken (oder die Namen von Ecken und Kanten) in einem Graphen  $G = (V, E)$  berücksichtigt, so heißt der Graph MARKIERT oder NUMMERIERT, z.B:



**2.11 Definition (Darstellung von Graphen)**

Ist  $G = (V, E)$  ein markierter Graph mit  $V = \{v_1, \dots, v_n\}$  und  $E = \{e_1, \dots, e_m\}$ , so heißt die  $n \times n$ -Matrix

$A = (a_{ij}) \in \{0, 1\}^{n \times n}$  mit  $a_{ij} = \begin{cases} 1 & v_i v_j \in E \\ 0 & \text{sonst} \end{cases}$  die ADJAZENZMATRIX von  $G$ .

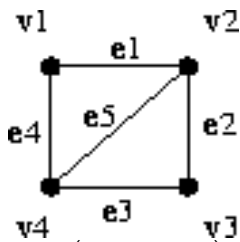
	$v_1$	$v_2$	$\dots$	$v_n$	
$v_1$	0				= A
$v_2$		0	$a_{ij}$		
$\vdots$			$\ddots$		
$v_n$				0	

Die  $n \times m$ -Matrix  $I = (b_{ij}) \in \{0, 1\}^{n \times m}$  mit  $b_{ij} = \begin{cases} 1 & \text{wenn } v_i \text{ und } e_j \text{ inzident} \\ 0 & \text{sonst} \end{cases}$  heißt INZIDENZMATRIX von  $G$ .

	$e_1$	$e_2$	$\dots$	$e_m$	
$v_1$					= I
$v_2$					
$\vdots$			$b_{ij}$		
$v_n$					

□

**2.12 Beispiel**



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

$a_{ii} = 0, i = 1, \dots, 4$   $A$  ist symmetrisch.

$$I = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Die Summe der Einträge der  $i$ -ten Zeile entspricht  $d(v_i)$ . Die Summe der Einträge jeder Spalte ist 2.

$$I_{n \times m} \cdot I_{m \times n}^T = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 3 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 3 \end{pmatrix} = A + \text{diag} \left( \underbrace{(2, 3, 2, 3)}_{(d(v_1), d(v_2), d(v_3), d(v_4))} \right)$$

□

**2.13 Satz (Adjazenz und Inzidenzmatrix)**

Sei  $G = (V, E)$  mit  $V = \{v_1, \dots, v_n\}$ . Ist  $A = (a_{ij})$  die Adjazenzmatrix und  $I = (b_{ij})$  die Inzidenzmatrix von  $G$ , so gilt:

$$I \cdot I^T = A + \text{diag}(d(v_1), \dots, d(v_n))$$

**Beweis**

Für  $i \neq j$ :  $(I \cdot I^T)_{ij} = \sum_{k=1}^m \underbrace{b_{ik} b_{jk}}_{\neq 0 \text{ nur für } e_k = v_i v_j} = \begin{cases} 1 & \text{falls } v_i v_j \in E \\ 0 & \text{sonst} \end{cases} := a_{ij}$

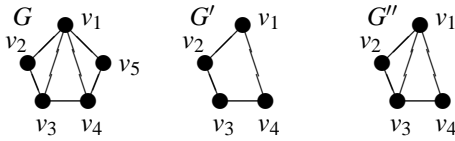
Für  $i = j$ :  $(I \cdot I^T)_{ii} = \sum_{k=1}^m \underbrace{b_{ik}b_{ik}}_{b_{ik}} = \sum_{k=1}^m \underbrace{b_{ik}}_{i\text{-te Zeilensumme von } I} = d(v_i)$  □

**2.14 Definition (Teilgraph)**

Sei  $G = (V, E)$  ein Graph und  $V' \subseteq V$ .

- $G' = (V', E')$  heißt TEILGRAPH von  $G$ , wenn  $E' \subseteq E \cap \binom{V'}{2}$  ist; in Zeichen:  $G' \subseteq G$ .
- $G[V'] := (V', E \cap \binom{V'}{2})$  heißt der von  $V'$  INDUZIERTER TEILGRAPH.

Z.B.:



$G'' = G[\{v_1, v_2, v_3, v_4\}]$  □

**2.15 Definition (zusammenhängender Graph)**

- (1) Sei  $G = (V, E)$ .  $G$  heißt ZUSAMMENHÄNGEND (zshg.), wenn zwischen je zwei Ecken  $x, y \in V$  ein Weg von  $x$  nach  $y$  existiert.
- (2)
  - In einem nicht zshg. Graphen heißt jeder maximale (bzgl. Anzahl von Ecken und Kanten) zshg. Teilgraph ZUSAMMENHANGSKOMPONENTE oder KOMPONENTE.
  - Sind  $G_1, \dots, G_k$  die Komponenten von  $G$ , so gilt:  $G = \bigcup_{i=1}^k G_i$ .
  - $\kappa(G) :=$  Anzahl der Komponenten von  $G$
  - $\kappa(G) = 1 \Leftrightarrow G$  ist zshg.
- (3) Sei  $G = (V, E)$  zshg.
  - Eine Ecke  $x \in V$  heißt SCHNITTECKE, falls  $G[V \setminus \{x\}]$  nicht mehr zshg. ist.
  - Eine Kante  $k \in E$  heißt BRÜCKE, falls  $(V, E \setminus \{k\})$  nicht mehr zshg. ist.

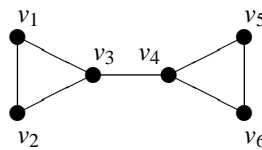


Abbildung 2.1: Beispiel: Schnittecken und Brücken

(In Abbildung 2.1 sind  $v_3$  und  $v_4$  Schnittecken und die Kante  $v_3v_4$  ist eine Brücke.) □

**2.16 Satz**

Sei  $G = (V, E)$ . Dann gilt:

$$\kappa(G) \geq |V| - |E|$$

**Beweis** (Induktion über  $m = |E|$ )

$$m = 0: \kappa(G) \geq |V| - \underbrace{|E|}_{=0}$$

$m \Rightarrow m + 1$ : Sei  $|E| = m + 1$  und  $e = ab \in E(G)$  beliebig.

Dann hat  $G' = (V, E \setminus \{e\})$  genau  $m$  Kanten und es gilt:

$$\kappa(G') \geq |V'| - |E' \setminus \{e\}| = |V| - [(m + 1) - 1] = |V| - m$$

Seien  $G'_1, G'_2, \dots, G'_{\kappa(G')}$  die Komponenten von  $G'$ .

$$G = G' + e$$

$$\Rightarrow \kappa(G) = \begin{cases} \kappa(G') & , \text{ falls } e \text{ keine Brücke von } G \text{ ist} \\ \kappa(G') - 1 & , \text{ falls } e \text{ eine Brücke von } G \text{ ist} \end{cases}$$

$$\geq \underbrace{(|V| - m)}_{\leq \kappa(G')} - 1 = |V| - (m + 1) = |V| - |E| \quad \square$$

## 2.17 Folgerung

Sei  $G = (V, E)$  zshg. mit  $n = |V|$  und  $m = |E|$ . Dann gilt:

$$n - 1 \leq m \leq \frac{n(n-1)}{2} = \binom{n}{2}$$

**Beweis**

Übung. □

## 2.18 Satz

Sei  $G = (V, E)$  mit  $n = |V|$  und  $m = |E|$ .

Gilt  $m > \underbrace{\frac{1}{2}(n-1)(n-2)}_{=\binom{n-1}{2}}$ , so ist  $G$  zshg.

**Beweis** (indirekt)

Annahme:  $G$  ist nicht zshg.

Seien  $G_1, \dots, G_k$  die Komponenten von  $G$  mit  $|V(G_i)| = n_i, i = 1, \dots, k$ .

Dann gilt:  $k \geq 2$  und  $n_1 + n_2 + \dots + n_k = n$ .

$$\begin{aligned}
 m &= |E(G_1)| + |E(G_2)| + \dots + |E(G_k)| \\
 &\leq \frac{n_1(n_1-1)}{2} + \frac{n_2(n_2-1)}{2} + \dots + \frac{n_k(n_k-1)}{2} \\
 &= \frac{1}{2} [(n_1^2 + n_2^2 + \dots + n_k^2) - (n_1 + n_2 + \dots + n_k)] \\
 &= \frac{1}{2} \left[ (n_1 + n_2 + \dots + n_k)^2 - 2 \sum_{1 \leq i < j \leq k} n_i n_j - n \right] \\
 &\leq \frac{1}{2} \left[ n^2 - 2n_1 \underbrace{(n_2 + n_3 + \dots + n_k)}_{=n-n_1} - n \right] \\
 &\leq \frac{1}{2} [n^2 - 2(n-1) - n] \\
 &= \frac{1}{2} (n^2 - 3n + 2) \\
 &= \frac{1}{2} (n-1)(n-2) \quad \zeta
 \end{aligned}$$

D.h.:  $G$  ist zshg. □

### 2.19 Satz

Ist  $G = (V, E)$  ein Graph mit  $|V| = n$  und  $|E| = m$ , so gilt:

$$m \leq \binom{n - \kappa(G) + 1}{2}$$

#### Beweis

Siehe L. Volkmann, „Diskrete Strukturen“, Satz 3.6.  
(Aus Satz 2.19 folgt Satz 2.18.) □

## § 2 Bäume

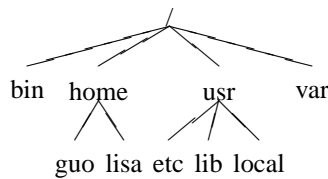


Abbildung 2.2: Beispiel für einen Baum: Dateisystem

### 2.20 Definition (Bäume und Wälder)

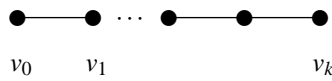
- (1) Ein BAUM ist ein zusammenhängender Graph ohne Kreise.
- (2) Ein Graph, dessen Komponenten Bäume sind, heißt WALD. □

### 2.21 Lemma

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

**Beweis**

Sei  $P = v_0 v_1 \dots v_k$  ein längster Weg in  $T$ .



Dann sind  $v_0$  und  $v_k$  zwei Eendecken. □

**2.22 Satz**

Sei  $G = (V, E)$  ein Graph mit  $|V| = n$ .

Die folgenden Aussagen sind äquivalent:

- (1)  $G$  ist ein Baum.
- (2)  $G$  ist zhsg. und kreisfrei.
- (3)  $G$  ist zhsg. und  $|E| = n - 1$ .
- (4)  $G$  ist kreisfrei und  $|E| = n - 1$ .
- (5) Zwischen je zwei Ecken  $u$  und  $v$  gibt es genau einen Weg.
- (6)  $G$  ist maximal kreisfrei (d.h.  $G$  ist kreisfrei und für alle  $E'$  mit  $E \subsetneq E'$  enthält  $(V, E')$  einen Kreis).
- (7)  $G$  ist maximal zshg. (d.h.  $G$  ist zshg. und jede Kante von  $G$  ist eine Brücke).

**Beweis**

Übung:  $(2) \stackrel{\text{Def.}}{\Leftrightarrow} (1) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (6) \Rightarrow (7) \Rightarrow (2)$

Wir zeigen nur:  $(1) \Rightarrow (3)$

Induktion über  $n$ :

$n = 2$ :  $|E| = 1 = 2 - 1 = n - 1$  ✓

$n \Rightarrow n + 1$ :

Lemma 2.21  $\Rightarrow G$  enthält eine Eendecke  $x \in V$ . Dann ist der Graph  $G - x := G[V \setminus \{x\}]$  ein Baum mit  $n$  Ecken, also:  $|E(G - x)| = n - 1$ .

$\Rightarrow |E(G)| = |E(G - x)| + 1 = (n - 1) + 1 = (n + 1) - 1$  □

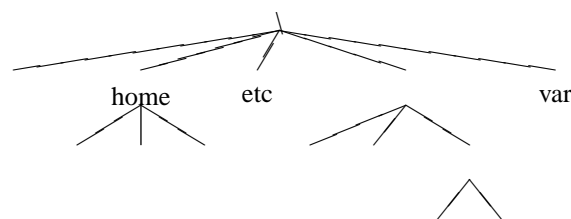
**2.23 Definition (Wurzelbaum)**

Abbildung 2.3: Beispiel für einen Wurzelbaum

Ein WURZELBAUM  $T = (V, E)$  ist ein Baum, in dem eine Ecke  $w \in V$  als Wurzel ausgezeichnet wird. Es sei  $x$  eine Ecke im Wurzelbaum  $T$  mit Wurzel  $w$ .

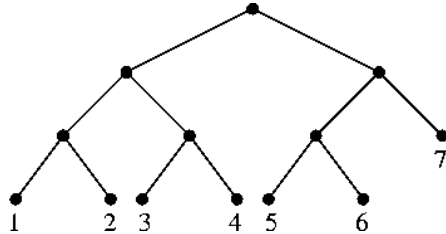
- Jede Ecke  $y$  auf dem (eindeutig bestimmten) Weg von  $w$  nach  $x$  heißt VORGÄNGER von  $x$ .
- Ist  $y$  ein Vorgänger von  $x$  und  $x \neq y$ , so heißt  $x$  NACHFOLGER von  $y$ .
- Sind  $yx \in E(T)$ , so heißt sie UNMITTELBARER VORGÄNGER bzw. UNMITTELBARER NACHFOLGER.
- Ein GEORDNETER BAUM ist ein Wurzelbaum, in dem für die unmittelbaren Nachfolger jeder Ecke eine Ordnung festgelegt ist.  $\square$

### 2.24 Definition (balancierter Wurzelbaum)

Die TIEFE  $\text{depth}(T)$  eines Wurzelbaums  $T$  ist die maximale Länge eines Weges von der Wurzel zu einer Edecke.

Ein Wurzelbaum  $T$  mit der Tiefe  $t$  heißt BALANCIERT, wenn jede Edecke von  $T$  auf Niveau  $t$  oder  $t - 1$  ist.

Z.B. Fußball-Turnier mit 7 Mannschaften:  $\square$



### 2.25 Definition (binärer Baum)

Es sei  $T = (V, E)$  ein Wurzelbaum mit der Wurzel  $w \in V$ :

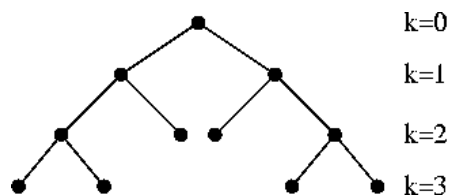
- $T$  heißt BINÄRER BAUM, wenn jede Ecke höchstens zwei unmittelbare Nachfolger hat.
- $T$  heißt VOLLSTÄNDIGER BINÄRER BAUM, wenn jede Ecke entweder zwei oder keinen unmittelbaren Nachfolger hat.  $\square$

### 2.26 Satz

Sei  $T = (V, E)$  ein binärer Baum mit der Tiefe  $t$  und  $|V| = n$ .

Dann gilt:  $t + 1 \leq n \leq 2^{t+1} - 1$ .

**Beweis**



$P_k :=$  Anzahl der Ecken auf Niveau  $k$  für  $0 \leq k \leq t$

So gilt:  $\sum_{k=0}^t P_k = n$

Da gilt:  $P_k \geq 1$  für  $1 \leq k \leq t$  und  $P_k \leq 2 \cdot P_{k-1}$  für  $1 \leq k \leq t$ , ist  $P_k \leq 2^k$

$\Rightarrow t + 1 \leq \sum_{k=0}^t 1 \leq \sum_{k=0}^t P_k \leq \sum_{k=0}^t 2^k = 2^{t+1} - 1$   $\square$

### 2.27 Folgerung

Sei  $T = (V, E)$  ein binärer Baum mit der Tiefe  $t$  und  $|V| = n$ . Dann gilt:

$$t \geq \left\lceil \log_2 \left( \frac{n+1}{2} \right) \right\rceil$$

**Beweis**

Übung. □

### 2.28 Definition (Gerüst eines Graphen)

Ein Teilgraph  $T$  eines zusammenhängenden Graphen  $G$  heißt GERÜST (SPANNENDER BAUM oder BAUMFAKTOR) von  $G$ , wenn  $T$  ein Baum mit  $V(T) = V(G)$  ist. □



### 2.29 Satz

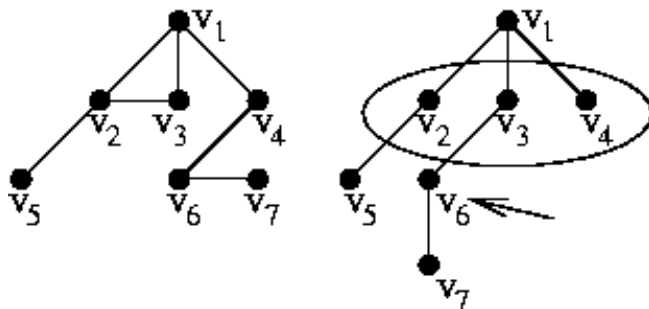
Jeder zusammenhängende Graph enthält ein Gerüst.

**Beweis**

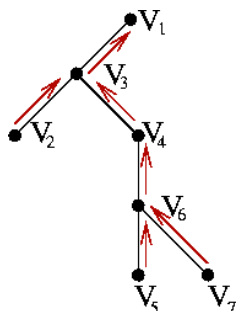
Sei  $G = (V, E)$  zusammenhängend.

(a) Enthält  $G$  keinen Kreis, so setze  $T := G$  und  $T$  ist ein Gerüst von  $G$ , sonst wähle einen Kreis  $C = v_0 v_1 v_2 \dots v_t v_0$  und wähle eine beliebige Kante von  $C$  aus (z.B. ist  $G' = (V, E) \setminus \{v_0, v_1\}$  zusammenhängend), fährt man so fort, dann erhält man einen zusammenhängenden Teilgraphen  $T$ , der kreisfrei ist. Also ist  $T$  ein Gerüst von  $G$ .

(b) Algorithmus 1: BREITENSUCHE (BFS: Breadth-First-Search)

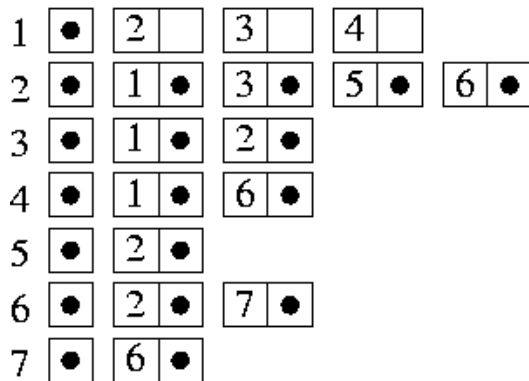


Algorithmus 2: TIEFENSUCHE (DFS: Depth-First-Search)



Die Algorithmen 1 und 2 haben eine Laufzeit von  $O(|V| + |E|)$ .

Hier benutzt man gerne eine andere Darstellung (bis auf Adjazenzmatrix und Inzidenzmatrix) von Graphen im Computer: Adjazenzliste.



Vor- und Nachteile:

	Adjazenzmatrix	Adjazenzliste
Speichern	$\Theta( V ^2)$	$\Theta( V  +  E )$
$xy \in E?$	$O(1)$	$O(\min\{d(x), d(y)\})$
$N(x) = ?$	$\Theta( V )$	$\Theta(d(x))$

$d(x)$  = Grad

$N(x)$  = Nachbarschaft

$f(n) = \Theta(g(n)) = f(n)$  wächst genau so schnell wie  $g(n)$

□

### 2.30 Satz (Cayley's Tree Formular)

Sei  $G$  ein vollständig markierter Graph mit  $n \geq 2$  Ecken.  
Dann besitzt  $G$   $n^{n-2}$  verschiedene Gerüste.

#### Beweis

Baum  $T$  auf  $V = \{1, 2, \dots, n\}$

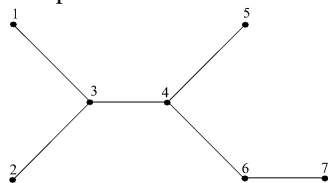
$P(T) = (t_1, t_2, \dots, t_{n-2}) \in V^{n-2}$  heißt PRÜFERCODE von  $T$ .

#### Algorithmus „ $\rightarrow$ “

Eingabe: Baum  $T = (V, E)$  mit  $V = \{1, 2, \dots, n\}$

Ausgabe: Wort  $(t_1, t_2, \dots, t_{n-2})$  über dem Alphabet  $\{1, 2, \dots, n\}$

Beispiel:



(3,3,4,4,6)

$i \leftarrow 1$

while  $|V| > 2$  do begin

  bestimme die Ecke  $v$  im Baum  $T$  mit der kleinsten Markierung;

$t_i \leftarrow$  Nachbar von  $v$  im Baum  $T$ ;

$T \leftarrow \underbrace{(V(T) \setminus \{v\}, E(T) \setminus \{vt_i\})}_{\text{ebenfalls ein Baum}}$

$i \leftarrow i + 1$

end

**Algorithmus „←“**

Eingabe: Wort  $(t_1, t_2, \dots, t_{n-2})$  über dem Alphabet  $\{1, 2, \dots, n\}$

Ausgabe: Baum  $T = (\{1, 2, \dots, n\}, E)$ .

$S \leftarrow \emptyset$

for  $i$  from 1 to  $n-2$  do begin

    wähle die kleinste Ecke  $s_i \in \{1, 2, \dots, n\} \setminus S$  mit  $s_i \notin \{t_i, t_{i+1}, \dots, t_{n-2}\}$ ;

    füge die Kante  $e_i = s_i t_i$  in den Graphen ein;

$S \leftarrow S \cup \{s_i\}$

end

füge die Kante  $e_{n-1} := \{1, 2, \dots, n\} \setminus S$  in den Graphen ein

⇒ Behauptung

□

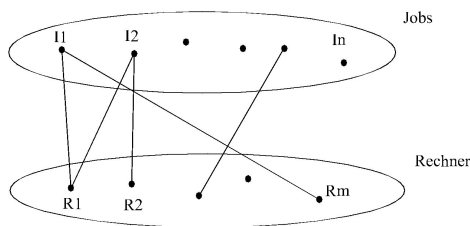
### § 3 Matching in Graphen

#### Vorbemerkungen

**Gegeben:** Eine Menge von Rechnern mit verschiedenen Leistungsmerkmalen (z.B. Geschwindigkeit, Speicher) und eine Menge von Jobs mit unterschiedlichen Leistungsanforderungen an die Rechner.

**Gesucht:** Eine Verteilung der Jobs auf die Rechner, so dass möglichst viele Jobs gleichzeitig bearbeitet werden können.

Graphentheoretisch können wir das obige Problem wie folgt formulieren:



$J_i R_k \in E(G) \Leftrightarrow R_k$  erfüllen die Leistungsanforderungen von Job  $J_i$ .

Gesucht ist dann die Kantenmenge  $M \subseteq E(G)$ , so dass keine zwei Kanten aus  $M$  eine gemeinsame Ecke haben.

**Konvention:** Sei  $G = (V, E)$  und  $M$  eine Kantenmenge,  $V(M) := \{x, y \in V(G) \mid xy \in M\}$ .

#### 2.31 Definition (Matching in Graphen)

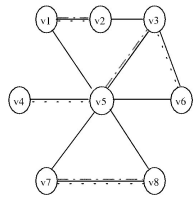
Sei  $G = (V, E)$  ein Graph.

Eine Kantenmenge  $M \subseteq E(G)$  heißt **MATCHING** von  $G$ , wenn  $V(k_1) \cap V(k_2) = \emptyset, \forall k_1, k_2 \in M, k_1 \neq k_2$

- Ein Matching  $M$  von  $G$  heißt **MAXIMAL**, wenn es in  $G$  kein Matching  $M'$  gibt mit  $M \subset M'$ .
- Ein Matching  $M$  heißt **MAXIMUM-MATCHING**, wenn es in  $G$  kein Matching  $M''$  gibt mit  $|M| < |M''|$ .
- Ein Matching  $M$  heißt **PERFEKT**, wenn  $V(M) = V(G)$ .

#### 2.32 Beispiel

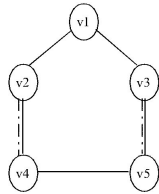
- $G_1$ :



$M = \{v_1v_2, v_3v_5, v_7v_8\}$  maximal

$M = \{v_1v_2, v_3v_6, v_4v_5, v_7v_8\}$  perfekt

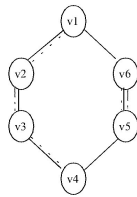
- $G_2$ :



$M = \{v_2v_4, v_3v_5\}$  maximal, Maximum-Matching

$G_2$  hat kein perfektes Matching

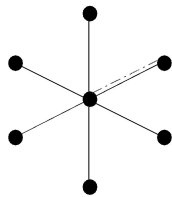
- $G_3$ :



$M = \{v_2v_3, v_5v_6\}$  maximal

$M = \{v_1v_2, v_3v_4, v_5v_6\}$  perfekt

- $G_4$ : (STERNGRAPH):



□

### 2.33 Bemerkung (Maximum-Matching)

Für jeden Graphen  $G = (V, E)$  gilt:

- (1) Jedes perfekte Matching ist ein Maximum-Matching.
- (2) Für jedes Matching  $M$  gilt:  $|V(M)| = 2 \cdot |M|$ .
- (3) Für ein perfektes Matching  $M$  von  $G$  gilt:  $2 \cdot |M| = |V(G)|$ .
- (4)  $G$  hat ein perfektes Matching.  $\Rightarrow |V(G)|$  ist gerade.

□

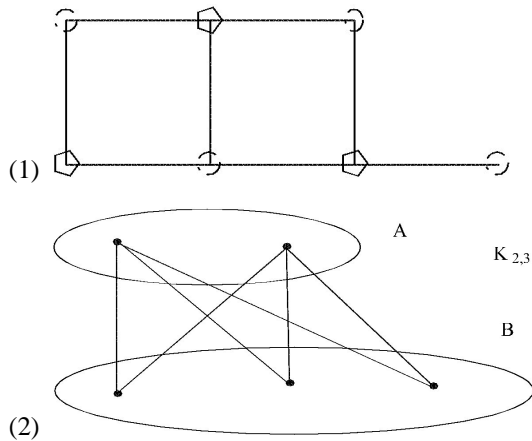
**2.34 Definition (bipartite Graphen)**

Ein Graph  $G = (V, E)$  heißt BIPARTIT, wenn  $V(G)$  in zwei disjunkte Mengen  $A$  und  $B$  zerlegt werden kann, so dass die  $G[A]$  und  $G[B]$  Nullgraphen sind.

- $A, B$  heißen PARTITIONSMENGEN.
- vollständiger bipartiter Graph:  $K_{p,q}$

□

**2.35 Beispiel**



□

**2.36 Satz (König, 1916)**

Ein Graph  $G$  ist bipartit.  $\Leftrightarrow G$  hat keinen Kreis ungerader Länge.

**Beweis**

„ $\Rightarrow$ “: trivial

„ $\Leftarrow$ “: Übung

Idee: wähle  $a \in V(G)$  fest und definiere:

$A = \{x \in V(G) \mid \text{es gibt in } G \text{ einen Weg von } a \text{ nach } x \text{ mit ungerader Länge}\}$

$B = \{y \in V(G) \mid \text{es gibt in } G \text{ einen Weg von } a \text{ nach } y \text{ mit gerader Länge}\}$

Zu zeigen:  $G = (A \uplus B, E)$ .

□

**2.37 Satz (König-Hall)**

Sei  $G = (A \uplus B, E)$  ein bipartiter Graph.

$G$  besitzt ein Matching  $M$  mit  $|M| = |A| \Leftrightarrow |N(S)| \geq |S|$  für alle  $S \subseteq A$ .

**Beweis**

„ $\Rightarrow$ “: trivial

„ $\Leftarrow$ “: (indirekt)

Sei  $|N(S)| \geq |S|$  für alle  $S \subseteq A$ . Es sei  $M$  ein Maximum-Matching von  $G$ , aber  $|M| < |A|$ .

Dann gilt:  $A \setminus V(M) \neq \emptyset$

Wähle  $a \in A \setminus V(M)$  und bezeichne:

$U(a) := \{x \in V(G) \mid x \text{ ist durch einen } M\text{-alternierenden Weg mit } a \text{ verbunden}\}$

$M$  ist ein Maximum-Matching  $\Rightarrow U(a) \subseteq V(M)$

Setze:  $A' = (U(a) \cup A) \cup \{a\}$   $B' = U(a) \cap B$

Dann gilt:  $B' = N(A')$  und  $|B'| = |A'| - 1$

$\Rightarrow |A'| = |B'| + 1 = |N(A')| + 1 > |N(A')| \nmid$

□

**2.38 Folgerung (König, 1916)**

Ist  $G = (A \uplus B, E)$  ein  $r$ -regulärer bipartiter Graph mit  $r \geq 1$ , so besitzt  $G$  ein perfektes Matching.

**Beweis**

- (1)  $|A| = |B|$
- (2)  $|N(S)| \geq |S|, \forall S \subseteq A$

**2.39 Folgerung (König, 1916)**

Ein  $r$ -regulärer bipartiter Graph lässt sich in  $r$  kantendisjunkte Matchings zerlegen.

**Beweis**

Sukzessives Anwenden von Folgerung 2.38. □

**2.40 Definition (Multipartite Graphen)**

Ein Graph  $G = (V, E)$  heißt  $k$ -PARTIT (MULTIPARTIT, wenn  $V(G)$  in  $k$  disjunkte Mengen  $V_1, V_2, \dots, V_k$  zerlegt werden kann, so dass  $G[V_i]$  für  $i = 1, \dots, k$  Nullgraphen sind. □

**§ 4 Hamiltonsche Graphen**

Im Jahr 1859 erfand Sir William Hamilton das Spiel „Rund um die Welt“.

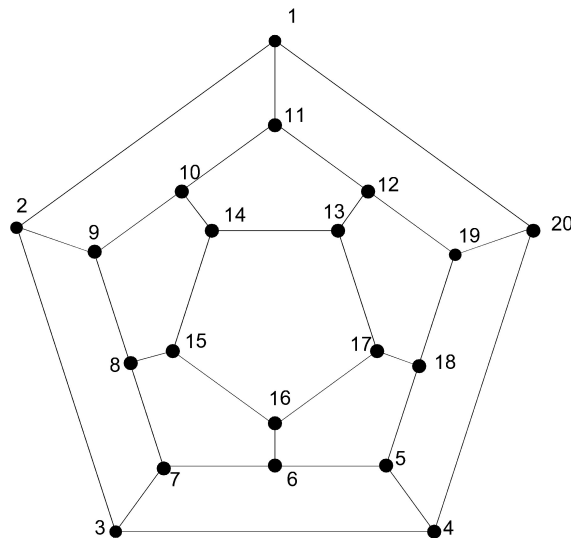


Abbildung 2.4: 3-regulärer Dodecaeder

**2.41 Definition (Hamiltonkreis / Hamiltonweg)**

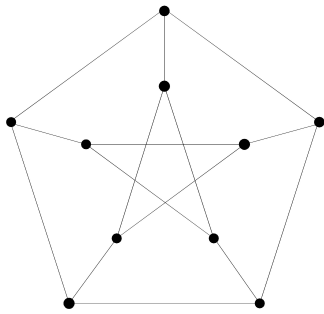
Sei  $G = (V, E)$ .

- Ein Kreis  $C$  in  $G$  heißt HAMILTONKREIS, falls  $V(C) = V(G)$
- Ein Weg  $W$  in  $G$  heißt HAMILTONWEG, falls  $V(W) = V(G)$
- Enthält  $G$  einen Hamiltonkreis, so heißt  $G$  HAMILTONSCHER GRAPH.

- Enthält  $G$  einen Hamiltonweg, so heißt  $G$  SEMI-HAMILTONSCHER GRAPH. □

### 2.42 Beispiel

- (1)  $K_n, n \geq 3$  ist hamiltonsch.
- (2)  $D_{20}$  (vgl. Abb. 2.4) ist hamiltonsch.



- (3) Peterson-Graph (vgl. Abb.) ist nicht hamiltonsch, aber semi-hamiltonsch □

### Bemerkung

hamiltonsch  $\xrightarrow{\quad}$  semi-hamiltonsch □  
 $\not\leftarrow$

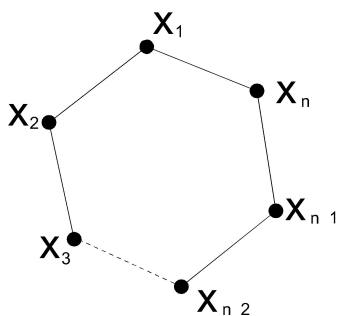
### 2.43 Satz (notwendige Bedingung)

Ist  $G$  ein hamiltonscher Graph, so gilt für jede nicht leere Eckenmenge:

$$S \subseteq V(G)$$

$$\kappa(G - S) \leq |S|$$

#### Beweis



$C$ : Hamiltonkreis von  $G$

$$S = \{x_{n1}, \dots, x_{np}\} \subseteq V(G)$$

$$\kappa(G - \{x_{n1}\}) = 1$$

$$\kappa(G - \{x_{n1}, x_{n2}\}) \leq 2$$

$\vdots$

$$\kappa(G - S) \leq \kappa(C - S) \leq |S| \quad \square$$

**2.44 Satz** (Ore 1960, hinreichende Bedingung)

Sei  $G = (V, E)$  ein Graph mit  $|V| = n$ . Sind  $u$  und  $v$  zwei nicht adjazente Ecken mit:

$$d(u) + d(v) \geq n$$

Dann gilt:

$$G \text{ ist hamiltonsch} \Leftrightarrow G + \underline{uv} \text{ ist hamiltonsch}$$

**Beweis**

„ $\Rightarrow$ “: trivial

„ $\Leftarrow$ “: (indirekt)

Annahme:  $G + uv$  hamiltonsch, aber  $G$  nicht.

Dann enthält jeder Hamiltonkreis von  $G + uv$  die Kante  $uv$ .

Seien:  $S := \{i \mid 1 \leq i \leq n-2, uv_{i+1} \in E(G)\}$

$T := \{j \mid 2 \leq j \leq n-1, v_j v \in E(G)\}$

$\Rightarrow S \cap T = \emptyset$  (sonst haben wir „crossover“),  $|S \cup T| \leq n-1 < n$

$$d(u) + d(v) = |S| + |T| = \underbrace{|S \cup T|}_{< n} + \underbrace{|S \cap T|}_{= 0} < n$$

□

**2.45 Folgerung** (Ore, 1960)

Sei  $G = (V, E)$  ein Graph mit  $|V| = n$ .

Gilt für alle nicht adjazenten Ecken  $u, v$  die Ungleichung  $d(u) + d(v) \geq n$ , so ist  $G$  hamiltonsch.

**Beweis**

Idee: Kanten hinzufügen  $\rightarrow K_n$ .

□

**2.46 Folgerung** (Diarc, 1952)

Sei  $G = (V, E)$  ein Graph mit  $|V| = n$ .

Ist  $d(v) \geq \frac{n}{2}$  für alle  $v \in V(G)$ , so ist  $G$  hamiltonsch.

□

**2.47 Bemerkung**

(1) Anwendung: Travelling-Salesman-Problem (TSP)

(2) Das Entscheidungsproblem „Enthält  $G$  einen Hamiltonkreis?“ ist *NP*-vollständig (siehe Vorlesung in Informatik).

□

**§ 5 Eulersche Graphen****Vorbemerkung** (Königsberger-Problem)

(vgl. Abbildung 2.5)

□

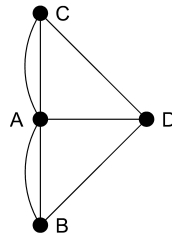


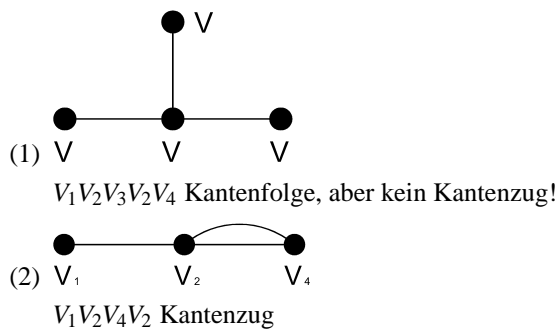
Abbildung 2.5: Das Königsberger-Problem

**2.48 Definition (Eulertour, Kantenzug)**

Sei  $G = (V, E)$  ein zusammenhängender Graph.

- $x_0x_1 \cdots x_k$  mit  $x_i \in V$  ( $0 \leq i \leq k$ ) und mit  $x_ix_{i+1} \in E(G)$  ( $0 \leq i \leq k-1$ ) heißt eine **KANTENFOLGE** der Länge  $k$ .
- Eine Kantenzug mit paarweise verschiedenen Kanten heißt **KANTENZUG**.

Zum Beispiel:



- Nur in diesem Abschnitt werden wir auch die Multigraphen, d.h. mit Mehrfachkanten studieren.
- Ein Kantenzug  $Z$  mit  $E(Z) = E(G)$  heißt **EULERSCHER KANTENZUG**.
- Ein geschlossener Eulerscher Kantenzug heißt **EULERTOUR**. □

**2.49 Definition (eulersch, semi-eulersch)**

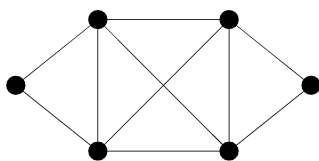
Sei  $G = (V, E)$  zusammenhängend mit  $|V| \geq 2$ .

$G$  heißt **SEMI-EULERSCH**, falls  $G$  einen eulerschen Kantenzug hat;

$G$  heißt **EULERSCH**, falls  $G$  eine Eulertour hat. □

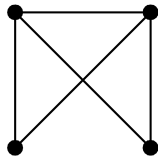
**2.50 Beispiel**

(1)  $G_1$ :



Z.B.:  $V_1V_2V_3V_4V_5V_6V_2V_5V_3V_6V_1 \Rightarrow G_1$  ist eulersch

(2)  $G_2$ :



Z.B.:  $V_1V_2V_3V_1V_4V_2 \Rightarrow G_2$  ist semi-eulersch

□

### 2.51 Satz (Euler, 1736)

Sei  $G = (V, E)$  zusammenhängend mit  $|V| \geq 2$ . Dann gilt:  
 $G$  ist eulersch.  $\Leftrightarrow$  Der Grad jeder Ecke ist gerade.

#### Beweis

„ $\Rightarrow$ “: trivial

„ $\Leftarrow$ “: Sei  $Z = x_0x_1 \cdots x_t$  ein längster Kantenzug in  $G$ .

Dann haben wir:

(1)  $x_t = x_0$

(2)  $Z$  ist eine Eulertour von  $G$ .

□

### 2.52 Folgerung

Ein zusammenhängender Graph  $G = (V, E)$  mit  $|V| \geq 2$  ist semi-eulersch, genau dann, wenn  $G$  zwei oder keine Ecke ungeraden Grades besitzt.

□

### 2.53 Bemerkung

(1) Für eulersche Graphen gibt es einen effizienten Algorithmus (Fleury's Algorithmus mit Komplexität  $O(|E(G)|)$ ), eine Eulertour zu konstruieren.

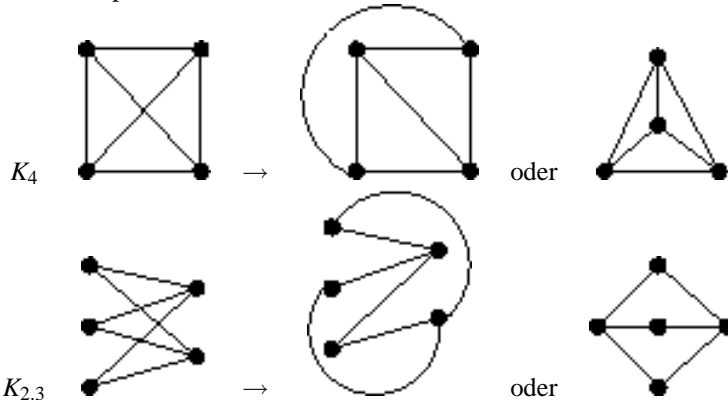
(2) Anwendungsbeispiel: Chinesisches Briefträgerproblem (Kuan, 1962): Es sei  $G = (V, E)$  ein zusammenhängender Graph mit einer Kantengewichtsfunktion  $c : E \rightarrow \{q \in \mathbb{Q} \mid q > 0\}$  ( $G$  heißt GEWICHTETER GRAPH). Gesucht wird eine geschlossene Kantenfolge  $Z$  von minimaler Gesamtlänge mit  $E(Z) = E(G)$ .

□

## § 6 Planare Graphen

### Frage

Welche Graphen kann man so in der Ebene  $\mathbb{R}^2$  zeichnen, dass sich keine zwei Kanten schneiden?



□

**2.54 Definition** (einbettbarer / planarer Graph)

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

(1)  $G$  heißt EINBETTBAR in den  $\mathbb{R}^2$ , wenn es ein Paar  $\varphi, \varphi'$  gibt, so dass gilt:

$$\varphi : V \rightarrow \mathbb{R}^2 \text{ injektiv}$$

$$\varphi' : E \rightarrow J = \{\text{Bild}(e) \mid e : [0, 1] \rightarrow \mathbb{R}^2 \text{ stetig und injektiv}\} \text{ Jordankurve mit } \varphi'(uv) = \text{Bild}(e) \text{ mit}$$

$$\begin{cases} \varphi(u) = e(0) \\ \varphi(v) = e(1) \end{cases}, e = uv \in E(G) \text{ und } \varphi'(e_1) \cap \varphi'(e_2) = V(e_1) \cap V(e_2), e_1, e_2 \in E(G).$$

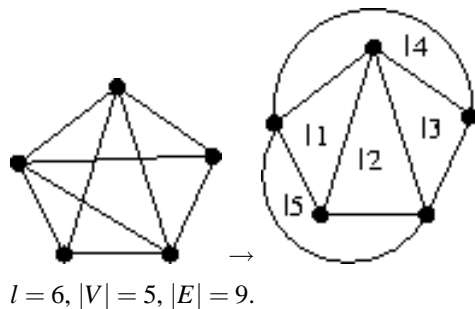
(2)  $G$  heißt PLANAR, wenn  $G$  in  $\mathbb{R}^2$  einbettbar ist.

(3) Ein EBENER Graph (oder eine LANDKARTE) ist eine Einbettung in  $\mathbb{R}^2$  eines planaren Graphen (in Zeichen:  $(G, \varphi, \varphi')$ ).

(4) Ist  $(G, \varphi, \varphi')$  ein ebener Graph, so heißen die Zusammenhangskomponenten von  $\mathbb{R}^2 \setminus \bigcup_{e \in E} \varphi'(e)$

GEBIETE (oder LÄNDER) von  $(G, \varphi, \varphi')$ .

$l(G)$  ist die Anzahl der Länder, z.B.:



□

**2.55 Satz** (Eulersche Polyederformel)

Sei  $G = (V, E)$  ein zusammenhängender ebener Graph. Dann gilt:

$$l(G) = |E| - |V| + 2$$

**Beweis** (Induktion über  $m = |E|$ )

$$m = |E| \underset{\text{Satz 2.22}}{\geq} |V| - 1$$

$m = |V| - 1$ :  $G$  ist ein Baum:

$$1 = \underbrace{(|V| - 1)}_m - |V| + 2$$

$m \rightarrow m + 1$ :

$G$  zusammenhängend und  $|E(G)| = m + 1 \geq |V| \underset{\text{Satz 2.22}}{\Rightarrow} G$  enthält mindestens einen Kreis  $C$ .

Sei nun  $e \in E(C)$  beliebig. Dann gilt:

$$|(G - e)| = m \text{ und } l(G - e) = m - |V| + 2.$$

Durch die Entfernung von  $e$  verschmelzen die beiden Länder auf den zwei Seiten von  $e$  zu einem Land.

$$\Rightarrow l(G - e) = \underbrace{m}_{+1} - |V| + 2 = \underbrace{m}_{+1} - |V| + 2$$

$$l(G) = |E(G)| - |V| + 2$$

□

**Bemerkung**

- (1) Sei  $G$  planar. Dann ist  $I(G)$  eine Invariante für verschiedene Einbettungen in  $\mathbb{R}^2$ . Daher können wir bei einem planaren Graphen von der Anzahl seiner Länder sprechen.
- (2) Jeder Graph kann im  $\mathbb{R}^3$  eingebettet werden. □

**2.56 Satz**

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

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

**Beweis**

O.B.d.A.:  $G$  ist in  $\mathbb{R}^2$  eingebettet.

$L :=$  Menge von Ländern. Jedes Land wird von mindestens 3 Kanten begrenzt und jede Kante begrenzt höchstens 2 Länder.

$$\Rightarrow 3 \cdot \underbrace{|L|}_{I(G)} \leq 2 \cdot |E| \quad \Rightarrow \quad \underbrace{\frac{2}{3} \cdot |E|}_{\text{Satz 2.55}} \geq I(G) = |E| - |V| + 2 \Rightarrow |E| \leq 3 \cdot |V| - 6 \quad \square$$

**2.57 Beispiel**

(1)  $K_5$  ist nicht planar, denn  $|E(K_5)| = \binom{5}{2} = 10 \geq 3 \cdot 5 - 6$ .

(2)  $K_{3,3}$  ist nicht planar, denn  $K_{3,3}$  ist  $C_3$ -frei und für  $C_3$ -freie planare Graphen  $G = (V, E)$  mit  $|V| \geq 3$  gilt:

$$|E| \leq 2 \cdot |V| - 4$$

Die beiden Graphen  $K_5$  und  $K_{3,3}$  sind in gewisser Weise die kleinsten nicht-planaren Graphen. □

**2.58 Definition (Unterteilungsgraph)**

Es sei  $G = (V, E)$  und  $e = ab \in E(G)$ . Wir sagen  $e$  wird unterteilt, wenn wir zu  $G$  eine neue Ecke  $x$  hinzufügen und die Kante  $e$  durch zwei neue Kanten  $ax$  und  $xb$  ersetzen.

Ein Graph  $H$  heißt UNTERTEILUNGSGRAPH von  $G$ , wenn man  $H$  aus  $G$  durch sukzessives Unterteilen von Kanten gewinnt. □

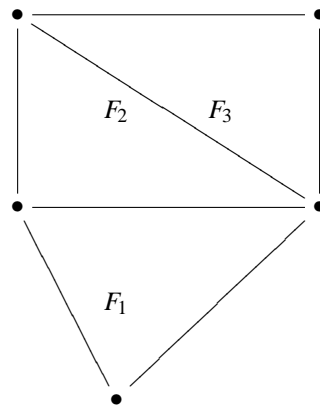
**2.59 Satz (Kuratowski, 1930)**

$G$  ist planar  $\Leftrightarrow (K_5 \text{ und Unterteilgraphen von } K_5) + (K_{3,3} \text{ und Unterteilgraphen von } K_{3,3})$  sind keine Teilgraphen von  $G$ . □

**2.60 Definition (Färbung)**

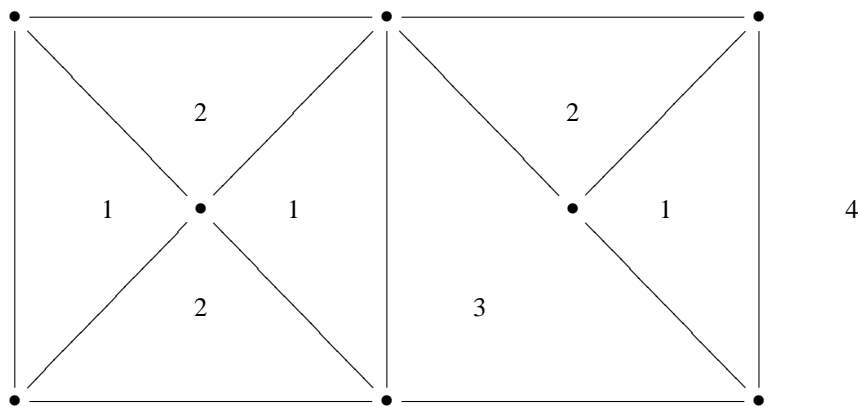
Sei  $G$  eine Landkarte.

- Zwei verschiedene Länder  $F_1$  und  $F_2$  heißen BENACHBART, wenn es eine Kante gibt, die sowohl zum Rand von  $F_1$  als auch zum Rand von  $F_2$  gehört.



- Ist  $L$  die Menge der Länder von  $G$ , so nennt man eine Abbildung  $h : L \rightarrow \{1, 2, \dots, p\}$  FÄRBUNG oder  $p$ -FÄRBUNG von  $G$ , wenn  $h(F_1) \neq h(F_2)$  für zwei verschiedene benachbarte Länder  $F_1$  und  $F_2$  gilt. Man sagt auch, dass sich die Landkarte  $G$  mit  $p$  Farben färben lässt.  $\square$

### 2.61 Beispiel



$\square$

### 2.62 Satz (VIERFARBENVERMUTUNG, Guthrie 1852)

Jede Landkarte lässt sich mit vier Farben färben.

**Beweis** (N. Robertson et al., 1997)

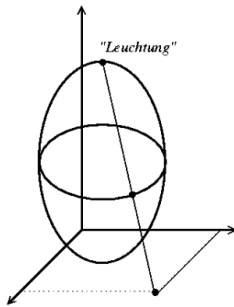
Hier nicht geführt.

### 2.63 Bemerkung

- (1) Bei den Anwendungen planarer Graphen in der Informatik steht der algorithmische Aspekt im Vordergrund.

Es gibt Verfahren, die in der Zeit  $O(|V| + |E|)$  testen, ob  $G = (V, E)$  planar ist, und falls ja, diesen auch in  $\mathbb{R}^2$  einbetten.

(Bemerkung:  $\mathbb{R}^2 \sim S^n$ )



(2) Das Problem der Kantenfärbung. (Wird hier nicht angesprochen.)

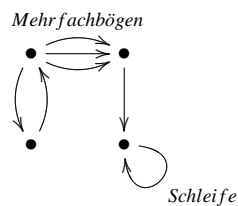
(3) Das Problem der Eckenfärbung. (Wird hier nicht angesprochen.)

## § 7 Digraphen

### 2.64 Definition (Digraph)

Ein DIGRAPH  $D$  besteht aus einer endlichen nichtleeren Eckenmenge  $V$  (engl.: vertex set) und einer Bogenmenge  $A \subseteq V \times V$  (engl.: arcs) von geordneten Eckpaaren, in Zeichen  $D = (V, A)$ .

**Beispiel**

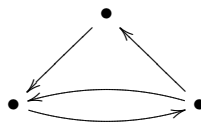


□

### 2.65 Konvention

Wir werden hier nur die schlichten Digraphen (d.h. die Digraphen ohne Schleifen und Mehrfachbögen) betrachten.

**Beispiel**



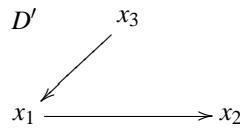
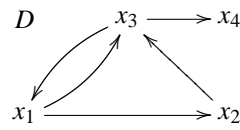
□

### 2.66 Definiton (Teildigraph)

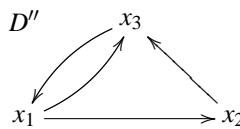
Sei  $D = (V, A)$  ein Digraph.

- $D' = (V', A')$  heißt TEILDIGRAPH von  $D$ , wenn  $V' \subseteq V$  und  $A' \subseteq A \cap (V' \times V')$  sind, in Zeichen  $D' \subseteq D$ .
- Ein Teildigraph  $D' = (V', A')$  heißt ein von  $V'$  INDUZIERTER TEILDIGRAPH, wenn  $A' = A \cap (V' \times V')$ , in Zeichen  $D' = D[V']$ .

**Beispiel**



$D' \subseteq D$



$D'' = D[\{x_1, x_2, x_3\}]$

ORIENTIERTE KANTENFOLGE der Länge  $p$  in  $D$ :

$F := x_0x_1x_2 \dots x_p$  mit  $x_i \in V(D), i = 0, 1, \dots, p$  und  $x_i, x_{i+1} \in A(D), i = 0, 1, \dots, p - 1$

**Beispiel**

In  $D$  ist  $x_3x_1x_2x_3x_1x_3$  ist eine orientierte Kantenfolge.

ORIENTIERTER KANTENZUG ist definiert als orientierte Kantenfolge mit paarweise verschiedenen Bögen

**Beispiel**

$x_3x_1x_3x_4$  (in  $D$ )

ORIENTIERTER WEG ist definiert als orientierte Kantenfolge mit paarweise verschiedenen Ecken

**Beispiel**

$x_3x_1x_2$  (in  $D$ )

- GESCHLOSSENE KANTENFOLGE (selbsterklärend)
- GRSCHLOSSENER KANTENZUG (selbsterklärend)
- ORIENTIERTER KREIS der Länge  $q$  ist definiert als geschlossene Kantenfolge der Länge  $q$  mit genau  $q$  Ecken.

**Beispiel**

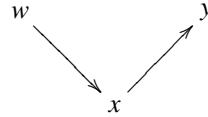
$x_1x_2x_3x_1$  ist ein 3-Kreis in  $D$

- EULERTOUR in  $D$ : Ein geschlossener Kantenzug  $Z$  in  $D$  mit  $A(Z) = A(D)$ .
- HAMILTONSCHER WEG von  $D$ : Ein Weg  $W$  in  $P$  mit  $V(W) = V(D)$ .
- HAMILTONSCHER KREIS von  $D$ : Ein Kreis  $C$  in  $D$  mit  $V(D) = V(C)$ .

- Für  $x \in V(D)$  definieren wir:

$$N^+(x) = \{y \mid xy \in A(D)\}$$

$$N^-(x) = \{w \mid wx \in A(D)\}$$



$$d^+(x) = |N^+(x)|$$

$$\delta^+(D) = \min\{d^+(x) \mid x \in V(D)\}$$

$$\Delta^+(D) = \max\{d^+(x) \mid x \in V(D)\}$$

$$d^-(x) = |N^-(x)|$$

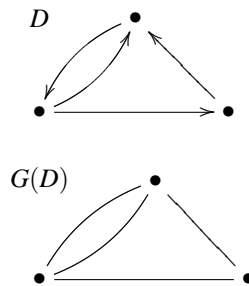
$$\delta^-(D) = \min\{d^-(x) \mid x \in V(D)\}$$

$$\Delta^-(D) = \max\{d^-(x) \mid x \in V(D)\}$$

- UNTERGEORDNETER GRAPH von  $D$  (in Zeichen  $G(D)$ ):

$$G(D) = (V(D), \underbrace{\{xy \mid xy \in A(D)\}}_{\text{Kante}})$$

**Beispiel**



□

**2.67 Definition**

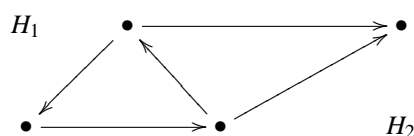
Sei  $D$  ein Digraph.

Eine STARK ZUSAMMENHÄNGENDE KOMPONENTE  $H$  von  $D$  ist ein maximaler Teildigraph von  $D$ , so dass  $H$  für zwei beliebige Ecken  $u, v \in V(H)$  einen orientierten weg von  $u$  nach  $v$  enthält.

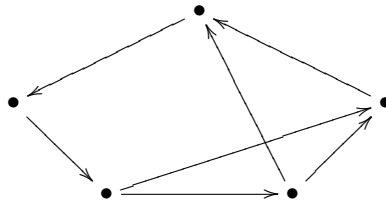
$D$  heißt STARK ZUSAMMENHÄNGEND, wenn  $D$  nur eine stark zusammenhängende Komponente hat.

**Beispiel**

(1) nicht stark zusammenhängend:



(2) stark zusammenhängend:

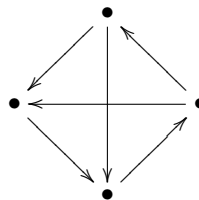


□

**2.68 Definition (Turnier)**

Ein Digraph heißt TURNIER, wenn zu je zwei Ecken genau ein Bogen existiert.  
 Ein Turnier mit  $n$  Ecken heißt  $n$ -Turnier, in Zeichen:  $T_n$ .

**Beispiel**



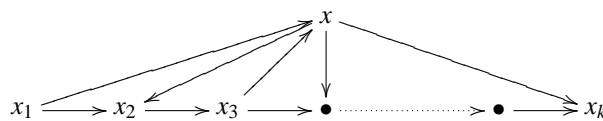
□

**2.69 Satz (Redei, 1934)**

Jedes Turnier besitzt einen orientierten Hamiltonschen Weg.

**Beweis**

Sei  $T_n$  ein Turnier und sei  $W = x_1x_2 \dots x_k$  ein längster orientierter Weg der Länge  $k - 1$  in  $T_n$ .  
 Annahme:  $k < n$



Sei  $x \in V(T_n) \setminus V(W)$ .

Dann haben wir:  $x_1 \rightarrow x \rightarrow x_k$ .

$\Rightarrow \exists i \in \{1, 2, \dots, k - 1\}$  mit  $x_i \rightarrow x \rightarrow x_{i+1}$

So ist  $x_1x_2 \dots x_i x x_{i+1} \dots x_k$  ein orientierter Weg in  $D$  mit der Länge  $k$ .  $\zeta$

□

**2.70 Satz (Moon, 1966)**

Ist  $T_n$  ein stark zusammenhängendes Turnier, so liegt jede Ecke von  $T_n$  auf einem  $p$ -Kreis für alle  $p \in \{3, 4, \dots, n\}$

**Beweis**

Per vollständiger Induktion über  $p$ .

□

### 2.71 Bemerkung

$D_{\text{(Schleifen)}} = (V, A) \leftrightarrow$  Relation  $A$  auf der Menge  $V$

□

# 3 Algebraische Strukturen

## § 1 Universelle Algebren

### 3.1 Definition (Operation)

Ist  $M$  eine Menge, so heißt eine Abbildung

$$f : M^n := \underbrace{M \times M \times \dots \times M}_{n\text{-mal}} \rightarrow M$$

eine  $n$ -stellige OPERATION oder ein  $n$ -stelliger OPERATOR.

- $n = s(f)$  heißt die STELLIGKEIT vom Operator  $f$ .
- Ein zweistelliger Operator (d.h.  $f : M \times M \rightarrow M$ ) heißt auch VERKNÜPFUNG (engl. binary operation). □

### 3.2 Definition (Algebra)

Eine UNIVERSELLE ALGEBRA<sup>1</sup> vom Typ  $(n_i)_{i \in I}$  ist  $(M, (f_i)_{i \in I})$ , wobei  $f_i$  eine  $n_i$ -stellige Operation auf  $M$  ist (d.h.  $n_i = s(f_i)$ ) und  $I$  eine Indexmenge ist (die auch unendlich sein kann). Die Liste  $(n_i)_{i \in I}$  heißt SIGNATUR der Algebra  $(M, (f_i)_{i \in I})$ . □

### 3.3 Beispiel

(1) Die boolesche Algebra  $(\{T, F\}, \underbrace{\vee}_{=f_1}, \underbrace{\wedge}_{=f_2}, \underbrace{\neg}_{=f_3})$  hat die Signatur  $(2, 2, 1)$ .

$\vee$	$T$	$F$		$\wedge$	$T$	$F$		$\neg$	$T$	$F$
$T$	$T$	$T$		$T$	$T$	$F$		$\neg$	$T$	$F$
$F$	$T$	$F$		$F$	$F$	$F$		$\neg$	$F$	$T$

(2) Mit den üblichen arithmetischen Operationen wie „+“ und „·“ können wir unterschiedliche Algebren definieren.

- $(\mathbb{N}, +)$  und  $(\mathbb{N}, +, \cdot)$  sind Algebren.
- $(\mathbb{Z}, \cdot)$  ist eine Algebra.
- $(\underbrace{\{x \in \mathbb{N} \mid x \text{ ist Quadratzahl}\}}_{:=M}, \cdot)$  ist eine Algebra, denn für  $x = a^2$  und  $y = b^2$  gilt:  
 $x \cdot y = a^2 \cdot b^2 = (a \cdot b)^2$ , d.h.  $\cdot : M \times M \rightarrow M$ .
- $(\{x \in \mathbb{N} \mid x \text{ ist Quadratzahl}\}, +)$  ist keine Algebra, denn die Summe von  $4 = 2^2$  und  $9 = 3^2$  ist z.B. keine Quadratzahl.



<sup>1</sup>Algebra auf Chinesisch:

(3)  $\Sigma$  = Menge (Alphabet)

$\Sigma^* = \{(a_1, a_2, \dots, a_n) \mid a_i \in \Sigma, n \in \mathbb{N}_0\}$  (Wörter über  $\Sigma$ )

$\circ : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$  mit  $(a_1 a_2 \dots a_n) \circ (b_1 b_2 \dots b_m) = (a_1 a_2 \dots a_n b_1 b_2 \dots b_m)$

$(\Sigma^*, \circ)$  ist eine Algebra.

(4)  $U$ : eine beliebige Menge

$F(U) := \{f \mid f : U \rightarrow U\}$

$\circ$ : Komposition von zwei Funktionen, also  $(f \circ g)(x) = f(g(x)) \forall x \in U$

$(F(U), \circ)$  ist eine Algebra. □

### 3.4 Definition (neutrale Elemente)

Sei  $(M, \circ)$  eine Algebra mit zweistelligem Operator „ $\circ$ “.

Ein Element  $e \in M$  heißt LINKSNEUTRALES ELEMENT für den Operator „ $\circ$ “, falls  $e \circ a = a \forall a \in M$ .

Ein Element  $a \in M$  heißt RECHTSNEUTRALES ELEMENT für den Operator „ $\circ$ “, falls  $a \circ e = a \forall a \in M$ .

Ein Element  $e \in M$  heißt NEUTRALES ELEMENT für den Operator „ $\circ$ “, falls  $e$  sowohl ein linksneutrales als auch ein rechtsneutrales Element ist, also:  $e \circ a = a \circ e = a \forall a \in M$ . □

### 3.5 Beispiel

$(\{b, c\}, \circ)$  mit

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

- $b \circ b = b$  und  $c \circ b = c \Rightarrow b$  ist ein rechtsneutrales Element.
- $b \circ c = b$  und  $c \circ c = c \Rightarrow c$  ist ein rechtsneutrales Element.
- $b \circ b = b$  und  $b \circ c = b \Rightarrow b$  ist kein linksneutrales Element.

Also hat  $(\{b, c\}, \circ)$  kein neutrales Element. □

### 3.6 Lemma

Sei  $(M, \circ)$  eine Algebra vom Typ (2), d.h.  $\circ$  ist eine zweistellige Verknüpfung. Dann gilt:

Ist  $c$  ein linksneutrales Element ( $*$ ) und  $d$  ein rechtsneutrales Element ( $\triangle$ ), so ist  $c = d$ .

Insbesondere gilt: Jede Algebra  $(M, \circ)$  vom Typ (2) enthält höchstens ein neutrales Element ( $\diamond$ ).

#### Beweis

$(*) \Rightarrow c \circ d = d$

$(\triangle) \Rightarrow c \circ d = c$

$\Rightarrow d = c$

Eindeutigkeit des neutralen Elements ( $\diamond$ ):

Annahme:  $e_1$  und  $e_2$  sind zwei neutrale Elemente.

$e_1 = e_1 \circ e_2 = e_2$  □

### 3.7 Beispiel (vgl. Beispiel 3.3(2))

- $(\mathbb{N}_0, +)$  hat ein neutrales Element „0“, denn  $x + 0 = 0 + x = 0 \forall x \in \mathbb{N}$ .
- $(\mathbb{Z}, \cdot)$  hat ein neutrales Element „1“.
- $(\mathbb{N}_0, +, \cdot)$  hat ein neutrales Element „0“ bzgl. „+“ und ein neutrales Element „1“ bzgl. „ $\cdot$ “. □

**3.8 Definition (inverse Elemente)**

Sei  $(M, \circ)$  eine Algebra vom Typ (2) mit neutralem Element  $e$ .

Ein Element  $x \in M$  heißt LINKSINVERSES ELEMENT von  $a \in M$ , falls  $x \circ a = e$ .

Ein Element  $x \in M$  heißt RECHTSINVERSES ELEMENT von  $a \in M$ , falls  $a \circ x = e$ .

Ein Element  $x \in M$  heißt INVERSES ELEMENT (oder INVERSE) von  $a \in M$ , falls  $x$  sowohl ein linksinverses als auch ein rechtsinverses Element ist.  $\square$

**Wichtige Algebren mit genau einer zweistelligen Verknüpfung****3.9 Definition (Halbgruppe)**

Eine Algebra  $A = (M, \circ)$  mit einem zweistelligen Operator  $\circ$  heißt HALBGRUPPE, falls der Operator  $\circ$  assoziativ ist, also:

$$a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in M$$

Z.B. ist  $(\Sigma^*, \circ)$  in Beispiel 3.3 eine Halbgruppe.  $\square$

**3.10 Definition (Monoid)**

Eine Algebra  $A = (M, \circ)$  vom Typ (2) heißt MONOID, falls gilt:

(M1)  $\circ$  ist assoziativ (d.h.  $A = (M, \circ)$  ist eine Halbgruppe)

(M2)  $\exists$  ein neutrales Element  $e \in M$   $\square$

**3.11 Definition (Gruppe)**

Eine Algebra  $A = (M, \circ)$  vom Typ (2) heißt GRUPPE, falls gilt:

(G1)  $\circ$  ist assoziativ

(G2)  $\exists$  ein neutrales Element  $e \in M$

(G3) jedes Element  $a \in M$  besitzt eine Inverse  $\square$

**3.12 Definition (abelsche Algebren)**

Eine Halbgruppe (ein Monoid, eine Gruppe)  $A = (M, \circ)$  heißt ABELSCH, falls  $\circ$  kommutativ ist, also:  $a \circ b = b \circ a \quad \forall a, b \in M$ .  $\square$

**Wichtige Algebren mit mehreren Verknüpfungen****3.13 Definition (Ring)**

Eine Algebra  $A = (M, \oplus, \odot)$  mit zwei zweistelligen Operatoren  $\oplus$  und  $\odot$  heißt RING, falls gilt:

(R1)  $(M, \oplus)$  ist eine abelsche Gruppe mit neutralem Element  $0 \in M$

(R2)  $(M, \odot)$  ist ein Monoid mit neutralem Element  $1 \in M$

(R3)  $\oplus$  und  $\odot$  sind distributiv, also:

- $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \quad \forall a, b, c \in M$
- $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a) \quad \forall a, b, c \in M$   $\square$

**3.14 Definition (Körper)**

Eine Algebra  $A = (M, \oplus, \odot)$  mit zwei zweistelligen Operatoren  $\oplus$  und  $\odot$  heißt KÖRPER, falls gilt:

(K1)  $(M, \oplus)$  ist eine abelsche Gruppe mit neutralem Element  $0 \in M$

(K2)  $(M \setminus \{0\}, \odot)$  ist eine abelsche Gruppe mit neutralem Element  $1 \in M$

(K3)  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \forall a, b, c \in M$

Körper sind z.B.  $(\mathbb{R}, +, \cdot)$  und  $(\mathbb{C}, +, \cdot)$ . □

**3.15 Definition (boolesche Algebren)**

Eine Algebra  $A = (M, \oplus, \odot, \neg)$  vom Typ  $(2, 2, 1)$  heißt BOOLESCHE ALGEBRA, falls gilt:

(B1)  $(M, \oplus)$  ist ein abelsches Monoid mit neutralem Element  $0 \in M$

(B2)  $(M, \odot)$  ist ein abelsches Monoid mit neutralem Element  $1 \in M$

(B3) •  $a \oplus (\neg a) = 1 \forall a \in M$

•  $a \odot (\neg a) = 0 \forall a \in M$

(B4)  $\oplus$  und  $\odot$  sind distributiv, also:

•  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \forall a, b, c \in M$

•  $a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c) \forall a, b, c \in M$  □

**3.16 Beispiel**

(1)  $(\mathbb{Z}, +, \cdot)$  ist ein KOMMUTATIVER RING, d.h.  $(\mathbb{Z}, +, \cdot)$  ist ein Ring und zusätzlich gilt:  $a \cdot b = b \cdot a$   $\forall a, b \in \mathbb{Z}$ .

(2) Sei  $K$  ein Körper, dann gilt:

•  $K[X] := \left\{ \sum_{k=0}^n a_k X^k \mid a_k \in K, n \in \mathbb{N}_0 \right\}$  (Menge der Polynome über  $K$ )  
ist kommutativer Ring (POLYNOMRING).

•  $K[[X]] := \left\{ \sum_{k=0}^{\infty} a_k X^k \mid a_k \in K \right\}$  ist ein kommutativer Ring (mit Null  $0 = 0 \cdot X^0$  und Eins  $1 = 1 \cdot X^0$ , vgl. Satz 1.32)

•  $K^{n \times n} := \left\{ \left( \begin{array}{ccc} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{array} \right) \mid a_{ij} \in K, 1 \leq i, j \leq n \right\}$  mit  $n > 1$  ist ein nicht kommutativer Ring (mit Null  $\underline{0}$  und Eins  $E_n$ )

(3)  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  sind Körper

(4) • Der kleinste Ring:  $\{0\}$  mit  $0 = 1$  und  $+ = \cdot$

• Der kleinste Körper:  $\mathbb{F}_2 = \{0, 1\}$  □

**Konvention**

Sei  $(K, \oplus, \odot)$  ein Körper:

- $0 \in K$  (Null), neutrales Element bezüglich  $\oplus$
- $1 \in K$  (Eins), neutrales Element bezüglich  $\odot$
- $-a$ : Inverses von  $a \in K$  bezüglich  $\oplus$
- $a^{-1}$ : Inverses von  $a \in K \setminus \{0\}$  bezüglich  $\odot$

□

**§ 2 Untereralgebra, Homomorphismen, Kongruenz**

Es sei  $A = (A, (f_i)_{i \in I})$  eine Algebra vom Typ  $T = (n_i)_{i \in I}, n_i = s(f_i)$ .

**3.17 Definition (Untereralgebra)**

$U \subseteq A$  heißt **UNTERALGEBRA** von  $A$ , in Zeichen  $U \leq A$ , falls die Operatoren  $f_i, i \in I$  abgeschlossen sind, d.h.

$$\underbrace{f_i(U^{n_i})}_{\{f_i(u_1, u_2, \dots, u_{n_i}) \mid u_1, u_2, \dots, u_{n_i} \in U\}} \subseteq U \quad \forall i \in I$$

□

**3.18 Definition (Untergruppe, Teilring / Unterring)**

- Sei  $G = (G, \cdot)$  eine Gruppe.  
Eine Untermenge  $U \leq G$  heißt **UNTERGRUPPE** von  $G$ , falls  $(U, \cdot)$  eine Gruppe ist. (D.h. für alle  $u, u' \in U$  gilt:  $u \cdot u' \in U, u^{-1} \in U$  und  $1 \in U$ .)
- Sei  $R = (R, \oplus, \odot)$  ein Ring.  
Eine Untereralgebra  $U \leq R$  heißt **TEILRING (UNTERRING)** von  $R$ , falls  $(U, \oplus, \odot)$  ein Ring ist.

□

**3.19 Beispiel**

- (1)  $(\mathbb{Z}, +)$  ist eine Untergruppe von  $(\mathbb{Q}, +)$ .
- (2) Sei  $Z_n := \{0, 1, \dots, n-1\}$  und  $+_n : \mathbb{N} \times \mathbb{N} \rightarrow Z_n$  mit  $+_n(a, b) = a + b \pmod n$   
( $+_n$  Addition modulo  $n$ )  
Z.B.  $n = 5$ :  
 $Z_5 = \{0, 1, 2, 3, 4\}, +_n : \mathbb{N} \times \mathbb{N} \rightarrow Z_5$

$$\begin{array}{rclcl} 1 & +_5 & 2 & = & 3 \\ 2 & +_5 & 3 & = & 0 \\ 3 & +_5 & 6 & = & 4 \\ 78 & +_5 & 100 & = & 3 \end{array}$$

Dann ist  $(Z_n, +_n)$  keine Untergruppe von  $(\mathbb{Z}, +)$ , da sich hier die Operatoren unterscheiden.

□

**3.20 Lemma**

Sei  $J$  eine Indexmenge und  $U_j \leq A$  für  $j \in J$ . Dann gilt:

$$\bigcap_{j \in J} U_j \leq A$$

□

**3.21 Definition** (erzeugte Unteralgebra)

Sei  $M$  eine Teilmenge von einer Algebra  $A$ .

$$\langle M \rangle = \bigcap \{U \mid M \subseteq U \leq A\}$$

heißt die von  $M$  ERZEUGTE UNTERALGEBRA. □

**3.22 Beispiel**

(1) Sei  $G = (G, \cdot)$  eine Gruppe und sei  $g \in G$ .

$\langle \{g\} \rangle = \{g^i \mid i \in \mathbb{Z}\}$  (die von  $g$  erzeugte Untergruppe), wobei:

$$g^i := \begin{cases} \overbrace{g \cdots g}^{i\text{-mal}} & , \text{ falls } i > 0 \\ 1 & , \text{ falls } i = 0 \\ \underbrace{g^{-1} \cdots g^{-1}}_{-i\text{-mal}} & , \text{ falls } i < 0 \end{cases}$$

(2)  $\langle \{g_1, \dots, g_n\} \rangle = \{a_1 \cdots a_m \mid m \in \mathbb{N}_0, a_j \in \{g_1, \dots, g_n, g_1^{-1}, \dots, g_n^{-1}\}\}$  □

**3.23 Definition** (Algebra-Homomorphismus)

Seien  $A = (A, (f_i)_{i \in I})$  und  $\tilde{A} = (\tilde{A}, (\tilde{f}_i)_{i \in I})$  Algebren vom gleichen Typ  $T = (n_i)_{i \in I}$ , d.h.  $n_i = s(f_i) = s(\tilde{f}_i)$ .

Eine Abbildung  $\varphi : A \rightarrow \tilde{A}$  heißt (ALGEBRA-)HOMOMORPHISMUS von  $A$  nach  $\tilde{A}$ , falls für alle  $i \in I$  die Operatoren  $f_i$  und  $\tilde{f}_i$  mit  $\varphi$  vertauschbar sind, also:

$$\tilde{f}_i(\varphi(a_1), \dots, \varphi(a_{n_i})) = \varphi(f_i(a_1, \dots, a_{n_i})) \quad \forall a_j \in A, j = (1, \dots, n_i), i \in I$$

Die Vertauschbarkeit bedeutet, dass man zum gleichen Ergebnis kommt, unabhängig davon, ob man im Diagramm „oben herum“ oder „unten herum“ läuft. □

**3.24 Beispiel**

(1) Sei  $A = (A, (f_i)_{i \in I})$  eine Algebra und  $A' \leq A$ . Dann ist:

$$\text{id} : A' \rightarrow A \text{ mit } a \rightarrow a \quad \forall a \in A'$$

ein Homomorphismus von  $A'$  nach  $A$ .

(Abbildung fehlt)

Oder die „kleinere“ Algebra  $A'$  ist in die „größere“ Algebra  $A$  eingebettet.

Z.B.:  $A = (\mathbb{N}, +), \tilde{A} = (\mathbb{Z}, +), A \leq \tilde{A}$ :

$$\varphi : \mathbb{N} \rightarrow \mathbb{Z} \text{ mit } n \rightarrow n \quad \forall n \in \mathbb{N}$$

ist ein Homomorphismus von  $A$  nach  $\tilde{A}$ .

(2)  $A = (\Sigma^*, \circ)$  (siehe Beispiel 3.3)

$\tilde{A} = (\mathbb{N}_0, +)$

$\varphi : \Sigma^* \rightarrow \mathbb{N}_0$  mit  $w \rightarrow |w| \quad \forall w \in \Sigma^*$  ist auch ein Homomorphismus von  $A$  nach  $\tilde{A}$

(3) Sei  $K$  ein Körper und  $V, W$  zwei  $K$ -Vektorräume (siehe Lineare Algebra I, Def. (2.25)). Dann gilt:

$$\varphi : V \rightarrow W \text{ ist ein Homomorphismus} \Leftrightarrow \varphi \text{ ist } k\text{-linear, d.h.:}$$

- $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$
- $\varphi(-v) = -\varphi(v)$
- $\varphi\left(\begin{smallmatrix} 0 \\ \in V \end{smallmatrix}\right) = \begin{smallmatrix} 0 \\ \in W \end{smallmatrix}$
- $\varphi(\alpha \cdot v) = \alpha \cdot \varphi(v)$

$$v \in V, \alpha \in K$$

□

### 3.25 Definition (Isomorphismus)

Seien  $A \cong (A, (f_i)_{i \in I})$  und  $\tilde{A}(\tilde{A}, (\tilde{f}_i)_{i \in I})$  zwei Algebren vom gleichen Typ  $(n_i)_{i \in I}$ . Eine Abbildung  $\varphi : A \rightarrow \tilde{A}$  heißt ISOMORPHISMUS von  $A$  nach  $\tilde{A}$ , falls:

- (1)  $\varphi$  ein Homomorphismus von  $A$  nach  $\tilde{A}$  ist,
- (2)  $\varphi$  bijektiv ist.

Ein bijektiver Homomorphismus heißt dann Isomorphismus.

$A = \tilde{A} \Leftrightarrow \exists$  einen Isomorphismus von  $A$  nach  $\tilde{A}$  (ISOMORPH).

Ein Isomorphismus von einer Algebra  $A$  nach  $A$  heißt AUTOMORPHISMUS.

□

### 3.26 Beispiel

(1)  $A = (\mathbb{N}, +), \tilde{A} = (\{2n \mid n \in \mathbb{N}\}, +)$

$\varphi : \mathbb{N} \rightarrow \{2n \mid n \in \mathbb{N}\}$  mit  $n \rightarrow 2n \forall n \in \mathbb{N}$  ist ein Isomorphismus von  $A$  nach  $\tilde{A}$ .

(2)  $A = (\underbrace{\{x \in \mathbb{R} \mid x > 0\}}_{:= \mathbb{R}^+}, \cdot), \tilde{A} = (\mathbb{R}, +)$

$\varphi : \mathbb{R}^+ \rightarrow \mathbb{R}$  mit  $x \rightarrow \log(x) \forall x \in \mathbb{R}^+$  ist ein Isomorphismus, denn für die Logarithmus-Funktion gilt:

$$\log(x \cdot y) = \log(x) + \log(y) \forall x, y \in \mathbb{R}^+$$

(3) Sei  $A = (\{1, 2, 3\}, \cdot)$  eine Algebra mit:

o	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

$\varphi : 1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3$  ist ein Automorphismus.

□

### 3.27 Lemma

Ein Isomorphismus zwischen zwei Algebren bildet neutrale Elemente auf neutrale Elemente und inverse Elemente auf inverses Element ab.

□

### 3.28 Lemma

Ist  $\varphi$  ein Isomorphismus der Algebra  $A$  in die Algebra  $\tilde{A}$ , so gibt es auch einen Isomorphismus  $(\varphi^{-1})$  von  $\tilde{A}$  nach  $A$ .

$$\begin{array}{l} \varphi : A \rightarrow \tilde{A} \\ A \leftarrow \tilde{A} : \varphi^{-1} \end{array}$$

□

**Erinnerung** (an Lineare Algebra, Definition (1.33))

Sei  $M$  eine Menge.

- RELATION  $R$  auf  $M$  ist eine Teilmenge  $R \subseteq M \times M$  und heißt ÄQUIVALENZRELATION, falls  $R$  reflexiv und symmetrisch und transitiv ist.

- Äquivalenzrelation auf  $M$ :

$$M/R := \underbrace{\text{Menge der Äquivalenzklassen von } R}_{\subseteq P(M)} \quad \square$$

**3.29 Beispiel**

$\mathbb{Z}$  und  $m \in \mathbb{N}$

$\sim_m: a \sim_m b \Leftrightarrow m \mid a - b$ , d.h.  $a \equiv b \pmod{m}$

$$\mathbb{Z} := \underbrace{\{k \cdot m \mid k \in \mathbb{Z}\}}_{[0]_{\sim_m}} \cup \underbrace{\{k \cdot m + 1 \mid k \in \mathbb{Z}\}}_{[1]_{\sim_m}} \cup \dots \cup \underbrace{\{k \cdot m + (m-1) \mid k \in \mathbb{Z}\}}_{[m-1]_{\sim_m}}$$

$$\begin{aligned} \mathbb{Z}_m &= \{[0]_{\sim_m}, [1]_{\sim_m}, \dots, [m-1]_{\sim_m}\} \\ &= \mathbb{Z}/m\mathbb{Z} \\ &= \{[a]_{\sim_m} \mid a \in \mathbb{Z}\} \\ &= \{\{a + m\mathbb{Z} \mid z \in \mathbb{Z}\} \mid a \in \mathbb{Z}\} \\ &= \{a + m\mathbb{Z} \mid a \in \mathbb{Z}\} \end{aligned} \quad \square$$

**3.30 Definition** (Kongruenzrelation)

Sei  $A = (A, (f_i)_{i \in I})$  eine Algebra.

Eine Äquivalenzklasse  $\sim$  auf  $A$  heißt eine KONGRUENZRELATION auf  $A$ , wenn  $\sim$  mit allen  $f_i$  verträglich ist, d.h.:

$$a_1 \sim a'_1, \dots, a_{n_i} \sim a'_{n_i} \Rightarrow f_i(a_1, \dots, a_{n_i}) \sim f_i(a'_1, \dots, a'_{n_i}) \quad \square$$

**3.31 Beispiel**

Sei  $G = (G, \cdot)$  eine Gruppe und sei  $\sim$  eine Äquivalenzrelation auf  $G$ .

$\sim$  Kongruenz  $\Leftrightarrow a \sim a', b \sim b' \Rightarrow a \cdot b \sim a' \cdot b'$  und  $a^{-1} \sim (a')^{-1}$ . □

**3.32 Satz** (Homomorphiesatz)

Sei  $A = (A, (f_i)_{i \in I})$  eine Algebra vom Typ  $(n_i)_{i \in I}$ ,  $n_i = s(f_i)$  und sei  $\sim$  eine Kongruenzrelation auf  $A$ .

(a) Für jedes  $a \in A$  bezeichnen wir mit:

$$[a]_{\sim} = \{a' \in A \mid a' \sim a\}$$

die Äquivalenzklasse von  $a$ .

Dann wird die Menge der Äquivalenzklassen

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

eine Algebra vom Typ  $(n_i)_{i \in I}$  mit

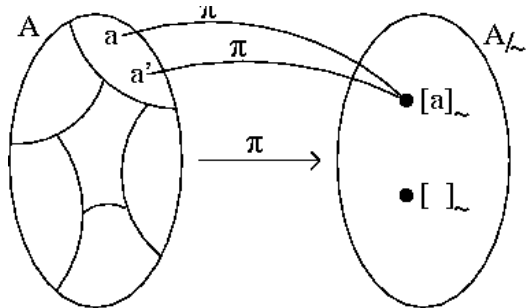
$$\bar{f}_i([a_1]_{\sim}, \dots, [a_{n_i}]_{\sim}) := [f_i(a_1, \dots, a_{n_i})]_{\sim}$$

und

$$\pi_{\sim} : A \rightarrow A/\sim \text{ mit } a \rightarrow [a]_{\sim}$$

ist ein surjektiver Homomorphismus.

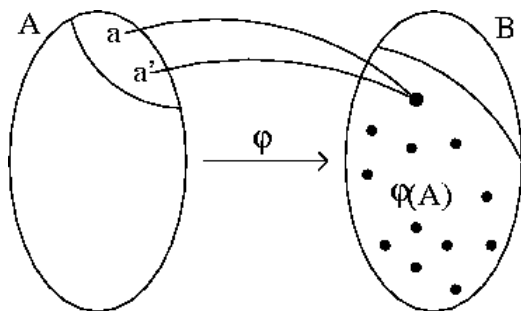
Epimorphismus



(b) Ist  $\varphi : A \rightarrow B$  ein Homomorphismus, so wird durch:

$$a \sim a' \Leftrightarrow \varphi(a) = \varphi(a')$$

eine Kongruenzrelation auf  $A$  definiert.



Außerdem gilt:

- $\varphi(A)$  ist eine Unteralgebra von  $B$ .
- Es gibt einen Isomorphismus  $\bar{\varphi} : A/\sim \rightarrow \varphi(A), [a]_{\sim} \rightarrow \varphi(a)$ .

### Beweis

Nachrechnen. □

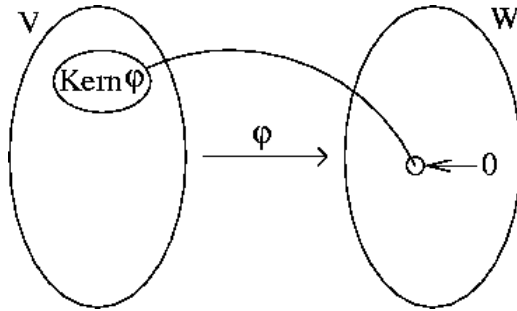
### 3.33 Beispiel

Sei  $K$  ein Körper, seien  $V, W$  zwei  $K$ -Vektorräume und sei  $\varphi : V \rightarrow W$  ein Homomorphismus.

$$\begin{aligned} \forall v, v' \in V : v \sim v' &\Leftrightarrow \varphi(v) = \varphi(v') \\ &\stackrel{\text{Def.}}{\Leftrightarrow} \varphi(v) - \varphi(v') = 0 \\ &\stackrel{\text{Beispiel 3.24}}{\Leftrightarrow} \varphi(v - v') = 0 \\ &\stackrel{\varphi \text{ ist } k\text{-linear}}{\Leftrightarrow} v - v' \in \text{Kern}(\varphi) \leq V \end{aligned}$$

Also:

$$\begin{aligned} [v]_{\sim} &= v + \text{Kern}(\varphi) \quad \forall v \in V \\ [0]_{\sim} &= \text{Kern}(\varphi) \end{aligned} \quad \square$$



### § 3 Ringe und Ideale

#### Erinnerung an Definition 3.13

Eine Algebra  $R = (R, +, \cdot)$  vom Typ (2,2) ist ein Ring, falls gilt:

- $(R, +)$  ist eine abelsche Gruppe mit  $0 \in R$
- $(R, \cdot)$  ist ein Monoid mit  $1 \in R$
- $+$  und  $\cdot$  sind distributiv

□

#### 3.34 Lemma

Sei  $R$  ein Ring. Dann gilt:

- (1)  $a \cdot 0 = 0 \cdot a = 0 \quad \forall a, b \in R$
- (2)  $a \cdot (-b) = (-a) \cdot b = -(a \cdot b) \quad \forall a, b \in R$
- (3)  $-(-a) = a \quad \forall a \in R$
- (4)  $-(a+b) = (-a) + (-b) \quad \forall a, b \in R$

Schreibweise:  $a - b = a + (-b)$

Sei  $\sim$  eine Kongruenzrelation auf  $R$ .

Wir betrachten die Teilmenge  $[0]_{\sim} := \{a \in R \mid a \sim 0\}$

$$a \sim a' \stackrel{-a' \sim -a'}{\iff} \underbrace{a + (-a')}_{=a-a'} \sim \underbrace{a' + (-a')}_{=a'-a'=0} \stackrel{\text{Kongruenz}}{\iff} a - a' \in [0]_{\sim}$$

$\Rightarrow \sim$  ist vollständig beschrieben durch  $[0]_{\sim}$ .

Seien  $u, v \in [0]_{\sim}$ . Dann gilt:

$$u \sim 0, v \sim 0 \Rightarrow u + v \sim 0 \Rightarrow u + v \in [0]_{\sim}$$

□

#### 3.35 Definition (Ideal)

Sei  $R = (R, +, \cdot)$  ein Ring,

$I \subseteq R$  heißt IDEAL<sup>2</sup> (in Zeichen  $I \trianglelefteq R$ ), falls gilt:

- $0 \in I$
- $a, b \in I \Rightarrow a + b \in I, -a \in I$
- $a \in R, u \in I \Rightarrow a \cdot u \in I$  und  $u \cdot a \in I$

□

<sup>2</sup>Ideal auf Chinesisch: 理想

### 3.36 Satz

Ist  $\sim$  eine Kongruenzrelation auf  $R$ , so ist  $I = [0]_{\sim} \trianglelefteq R$ .

Umgekehrt: Ist  $I \trianglelefteq R$ , so wird durch  $a \sim a' \Leftrightarrow a - a' \in I$  eine Kongruenzrelation definiert.

(Dabei ist  $[0]_{\sim} = I$  und  $[a]_{\sim} = a + I$ .) Schreibweise:  $R/I := R/\sim$

□

### 3.37 Satz

Ist  $R$  ein kommutativer Ring und  $d \in R$  beliebig. Dann gilt:

(1)  $R \cdot d = \{a \cdot d \mid a \in R\} \trianglelefteq R$  ist ein Ideal

( $R \cdot d$  heißt auch das von  $d$  erzeugte HAUPTIDEAL.)

(2)  $R \cdot d = R \Leftrightarrow d$  ist invertierbar in  $(R, \cdot)$ , d.h.  $\exists d' : d \cdot d' = 1$

□

### 3.38 Beispiel (vgl. Beispiel 3.28)

$R = (\mathbb{Z}, +, \cdot)$  und  $m \in \mathbb{N}$ ,  $\sim = \sim_m$

Dann ist  $m\mathbb{Z} \trianglelefteq \mathbb{Z}$  und  $1\mathbb{Z} = \mathbb{Z}$ .

□

### Konvention

In einem kommutativen Ring schreibt man:

$$\underbrace{a + a + \dots + a}_{k\text{-mal}} = k \cdot a$$

□

### 3.39 Beispiel

Zeigen Sie: Keine ganze Zahl der Form  $7 + n \cdot 8$  ist die Summe von 3 Quadraten in  $\mathbb{Z}$  für  $n \in \mathbb{Z}$ .

**Beweis** (indirekt)

Annahme:  $z = 7 + n \cdot 8 = a^2 + b^2 + c^2$ , für  $a, b, c \in \mathbb{Z}$

Betrachte:  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_8, z \rightarrow [z]_8$

$R$  Homomorphismus (vgl. Satz 3.31(a))

$$\begin{aligned} \Rightarrow \varphi(z) &= \varphi(a^2) + \varphi(b^2) + \varphi(c^2) \\ &= \varphi(a)^2 + \varphi(b)^2 + \varphi(c)^2 \\ &\stackrel{!}{=} [7]_8 \end{aligned}$$

Wobei:  $\varphi(a), \varphi(b), \varphi(c) \in \mathbb{Z}_8$ .

In  $\mathbb{Z}_8$ :

$x$	0	1	2	3	4	5	6	7
$x^2$	0	1	4	1	0	1	4	1

$\Rightarrow$  Quadrate in  $\mathbb{Z}_8$  sind: 0, 1, 4, ...

$\Rightarrow$  Summen von drei Quadraten in  $\mathbb{Z}_8$  sind nicht gleich 7

$\Rightarrow$  Behauptung

□

## § 4 Größte gemeinsame Teiler

Ring  $\supseteq$  kommutativer Ring  $\supseteq$  Integritätsbereich  $\supseteq$  Hauptidealring

$\supseteq$  Euklidischer Ring  $\begin{cases} (\mathbb{Z}, +, \cdot) & \text{Primzahlen} \\ K[X] & \text{Polynomring} \end{cases}$

- Natürliche Zahlen  $p \geq 2$ , für die 1 und  $p$  die einzigen positiven Teiler sind, nennt man PRIMZAHLEN, z.B. 2, 3, 5, 7, 11, 13, 17,  $\dots$ , 1 ist keine Primzahl!
- Ist  $m \in \mathbb{N}$  keine Primzahl und  $m > 1$  mit  $m = p \cdot q$  mit  $1 < p, q < m$ , dann gilt:  
 $[p]_m \cdot [q]_m = [p \cdot q]_m = [m]_m = [0]_m = 0$  in  $\mathbb{Z}_m$ , aber  $[p]_m \neq 0$  und  $[q]_m \neq 0$ , weil  $1 < p, q < m$ .  $\square$

### 3.40 Definition (Integritätsbereich)

Sei  $R = (R, +, \cdot)$  ein kommutativer Ring. Sei  $a \neq 0$  und  $b \neq 0$ , aber  $a \cdot b = 0$ , so heißen  $a$  und  $b$  NULLTEILER.

$R$  heißt INTEGRIÄTSBEREICH<sup>3</sup>, falls  $R$  keine Nullteiler enthält, d.h.  $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ .  $\square$

### 3.41 Beispiel

- (1)  $\mathbb{Z}$  ist ein Integritätsbereich.
- (2)  $\mathbb{Z}[X]$  ist ein Integritätsbereich.
- (3) Sei  $K$  ein Körper. Dann sind  $K[X]$  und  $K[[X]]$  Integritätsbereiche.
- (4)  $\mathbb{Z}_4$  ist kein Integritätsbereich, denn  $[2]_4 \cdot [2]_4 = [0]_4$ .  
 $\mathbb{Z}_m$  ist kein Integritätsbereich, wenn  $m$  keine Primzahl ist.  $\square$

### 3.42 Definition (größter gemeinsamer Teiler)

Sei  $R$  ein Integritätsbereich.

- (1)  $a \mid b \Leftrightarrow \exists c \in R$  mit  $b = a \cdot c$ . In Worten: „ $a$  teilt  $b$ “.  
 $a \nmid b \Leftrightarrow \nexists c \in R$  mit  $b = a \cdot c$ .
- (2)  $d \in R$  heißt ein GRÖSSTER GEMEINSAMER TEILER von  $a, b \in R$ , in Zeichen:  $d \in \text{ggT}(a, b)$ , wenn:
  - $d \mid a$  und  $d \mid b$ .
  - $(c \mid a \wedge c \mid b) \Rightarrow c \mid d$   $\square$

### 3.43 Bemerkung

Sei  $R = (R, +, \cdot)$  ein Integritätsbereich. Jedes Element  $u \in R$  heißt EINHEIT in  $R$ , falls  $u^{-1}$  existiert.

$$R^* = \{u \in R \mid \exists u^{-1} \in R \text{ mit } u \cdot u^{-1} = 1\}$$

- (1) In  $\mathbb{Z}$  sind nur  $-1$  und  $1$  Einheiten, z.B.  $\text{ggT}(4, 10) = \{-2, 2\}$ .
- (2) Ist  $u \in R$  eine Einheit in  $R$ , so gilt  $u \mid a \forall a \in R$ , denn  $a = u(u^{-1}a)$ .
- (3) Ist  $d \in \text{ggT}(a, b)$  in  $R$  und  $u \in R^* \Rightarrow u \cdot d \in \text{ggT}(a, b)$ .  
 Umgekehrt kann man zeigen:  $d, d' \in \text{ggT}(a, b) \Rightarrow d' = u \cdot d$  für ein  $u \in R^*$ .
- (4) Nicht in jedem Integritätsbereich gilt:  $\text{ggT}(a, b) = \{1\}$ .  $\square$

<sup>3</sup>Integritätsbereich auf Chinesisch:

整环

## § 5 Eindeutige Primfaktorzerlegung

### 3.44 Definition (irreduzibel)

Sei  $R$  ein Integritätsbereich.  $p \in R$  und  $p \neq 0$  und  $p \notin R^*$  heißt IRREDUZIBEL, falls gilt:

$$p = a \cdot b \Rightarrow a \in R^* \vee b \in R^*$$

□

### 3.45 Beispiel

$p \in \mathbb{Z}$  ist irreduzibel  $\Leftrightarrow p$  oder  $-p$  ist eine Primzahl.

□

### 3.46 Beispiel

Sei  $I = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ . Dann gilt:

(a)  $I$  ist ein Integritätsbereich.

(b)  $I^* = \{-1, 1\}$

(c)  $|\alpha|^2 = 4 \Rightarrow \alpha$  ist irreduzibel.

(d)  $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$  (zwei verschiedene Primfaktorzerlegungen in  $I$ )

□

### Frage

Welche Integritätsbereiche  $R$  haben die Eigenschaft, dass jedes  $a \in R \setminus (\{0\} \cup R^*)$  eine eindeutige Primfaktorzerlegung hat?

□

### 3.47 Definition (Primfaktor-Zerlegung)

Sei  $R$  ein Integritätsbereich.  $a \in R$  hat eine eindeutige (PRIMFAKTOR-)ZERLEGUNG, falls gilt:

$a = p_1 \cdot \dots \cdot p_r$  mit  $p_i$  irreduzibel und  $a = q_1 \cdot \dots \cdot q_s$  mit  $q_i$  irreduzibel  $\Rightarrow r = s$  und mit passender Umsortierung ist  $q_i = u_i p_i$  mit  $u_i \in R^*$  für  $i = 1, \dots, s$ .

□

### 3.48 Bemerkung

Hat  $a \in R$  eine eindeutige Zerlegung, so ist  $a \in R \setminus (\{0\} \cup R^*)$ , denn  $0 = a_1 \cdot \dots \cdot a_\alpha \Rightarrow \exists a_i = 0$  aber  $0$  ist nicht irreduzibel und  $u = a_1 \cdot \dots \cdot a_\beta \Rightarrow 1 = a_1 (u^{-1} a_2 \cdot \dots \cdot a_\beta)$ , aber Einheit ist nicht irreduzibel. □

## Zwei spezielle Ringe: Hauptidealring $\supseteq$ Euklidischer Ring

### 3.49 Definition (Hauptidealring)

Ein Integritätsbereich  $R$  heißt HAUPTIDEALRING, wenn jedes Ideal  $I$  von  $R$  ein Hauptideal ist, d.h.  $\exists d \in R$  mit  $I = R \cdot d$ .

□

### 3.50 Satz

Sei  $R$  ein Hauptidealring.

Dann hat jedes  $a \in R \setminus (\{0\} \cup R^*)$  in  $R$  eine eindeutige Primfaktorzerlegung.

□

### 3.51 Definition (Euklidischer Ring)

Ein Integritätsbereich  $R$  heißt ein EUKLIDISCHER RING, falls gilt:

- (1)  $\exists \delta$  mit  $R \setminus \{0\} \rightarrow \mathbb{N}_0$
- (2) Zu  $a, b \in R$  mit  $b \neq 0$  existiert  $q, r \in R$ , so dass  $a = qb + r$  mit  $\delta(r) < \delta(b)$ .

Ein Euklidischer Ring  $(R, \delta)$  heißt NORM-EUKLIDISCHER RING, wenn:

$$\delta : R \rightarrow \mathbb{N}_0 \text{ mit } \begin{cases} \delta(a) = 0 & \Leftrightarrow a = 0 \\ \delta(a \cdot b) = \delta(a) \cdot \delta(b) \end{cases} \quad \square$$

### 3.52 Beispiel

$$(1) (\mathbb{Z}, |\cdot|) \text{ ist ein Norm-Euklidischer Ring, wobei } |a| = \begin{cases} a & , \text{ falls } a \geq 0 \\ -a & , \text{ falls } a < 0 \end{cases}$$

(2) Sei  $K$  ein Körper.  $R = (K[X], \text{grad})$  ist ein Euklidischer Ring.

$$R = (K[X], \delta) \text{ mit } \delta(f) = \begin{cases} \text{grad}(f) & , f \neq 0 \\ 0 & , f = 0 \end{cases} \text{ ist ein Norm-Euklidischer Ring.} \quad \square$$

### 3.53 Satz

Ein Euklidischer Ring  $R$  ist ein Hauptidealring. Somit hat jedes  $a \in R \setminus (\{0\} \cup R^*)$  in  $R$  eine eindeutige Primfaktorzerlegung. □

### 3.54 Folgerung

In  $\mathbb{Z}$  hat jedes  $a \in \mathbb{Z} \setminus \{0\}$  eine eindeutige Primfaktorzerlegung in der Form:

$$a = \mu p_1 \cdots p_k, p_i \text{ Primzahl und } \mu \in \mathbb{Z}^* = \{-1, 1\}$$

#### Beweis

Beispiel 3.52(1) und Satz 3.53 □

### 3.55 Bemerkung

Aus Folgerung 3.54 folgt der FUNDAMENTALSATZ DER ARITHMETIK.

Jede Zahl  $n \in \mathbb{N}$  mit  $n \geq 2$  läßt sich eindeutig als Produkt von Primzahlen darstellen:

$$n = p_1^{t_1} \cdot p_2^{t_2} \cdots p_k^{t_k}$$

Wobei  $p_1 < p_2 < \cdots < p_k$  Primzahlen sind und  $t_1, \dots, t_k \in \mathbb{N}$ . □

### 3.56 Satz

Es gibt unendlich viele Primzahlen.

#### Beweis (indirekt)

Annahme:  $p_1, \dots, p_k$  sind alle Primzahlen,  $k \in \mathbb{N}$ .

Setze:  $n = p_1 \cdot p_2 \cdots p_k + 1$  (\*)

$\Rightarrow n$  ist keine Primzahl.

Bem. 3.48  $\Rightarrow n = p_{n_1}^{t_1} \cdot p_{n_2}^{t_2} \cdots p_{n_s}^{t_s}$  mit  $p_{n_1} < \cdots < p_{n_s}$  Primzahlen und  $t_i \in \mathbb{N}$  (\*\*)

$$\stackrel{*}{\Rightarrow} p_{n_1} \mid n - 1$$

$$\stackrel{**}{\Rightarrow} p_{n_1} \mid n$$

$\Rightarrow$  unmöglich  $\zeta$  □

### 3.57 Satz (Primzahlen)

Für alle  $n \in \mathbb{N}$  gilt:

$$\underbrace{\pi(n)}_{\text{\# der Primzahlen } \leq n} = (1 + \underbrace{o(1)}_{\rightarrow 0, n \rightarrow \infty}) \cdot \frac{n}{\ln(n)}$$

□

### 3.58 Bemerkung

Wie findet man Primzahlen?

(1) Finde alle Primzahlen  $\leq n$ :

Z.B.:  $n = 36$

1	<del>2</del>	3	<del>4</del>	5	<del>6</del>	7	<del>8</del>	9
<del>10</del>	11	<del>12</del>	13	<del>14</del>	<del>15</del>	<del>16</del>	17	<del>18</del>
19	<del>20</del>	<del>21</del>	<del>22</del>	23	<del>24</del>	<del>25</del>	<del>26</del>	<del>27</del>
<del>28</del>	29	<del>30</del>	31	<del>32</del>	<del>33</del>	<del>34</del>	<del>35</del>	<del>36</del>

$$\pi(36) = 11$$

Weiterhin:  $\pi(49) = 15$  und  $\pi(100) = 25$ .

Man schreibt alle Zahlen von 2 bis  $n$  auf und wendet dann den folgenden Algorithmus an:

for  $i$  from 2 to  $\sqrt{n}$  do begin

    falls  $i$  ungestrichen, streiche alle Vielfachen  $2i, 3i, \dots$  von  $i$

end

Die am Ende übrig gebliebenen ungestrichenen Zahlen sind dann genau die Primzahlen  $\leq n$ .

(2) Finde große Primzahlen:

Randomisierte Verfahren der derzeit effizientesten Primzahltester (vgl. Wahrscheinlichkeitstheorie und Statistik). □

### 3.59 Satz („kleiner Fermat“)

Für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  gilt:

$$n \text{ Primzahl} \Leftrightarrow a^{n-1} \equiv 1 \pmod{n} \quad \forall a \in \mathbb{Z} \setminus \{0\}$$

□

### 3.60 Definition (eulersche $\varphi$ -Funktion)

$\varphi : \mathbb{N} \rightarrow \mathbb{N}$  mit  $\varphi(n) := |\mathbb{Z}_n^*|$  heißt EULERSCHE  $\varphi$ -FUNKTION, wobei:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \setminus \{0\} \mid \text{ggT}(n, a) = 1\}$$

□

### 3.61 Lemma

Ist  $n = p_1^{t_1} \cdots p_k^{t_k}$  mit  $p_1 < p_2 < \cdots < p_k$  Primzahlen, so gilt folgendes:

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

□

**3.62 Satz (Euler)**

Für alle  $n \in \mathbb{N}$  mit  $n \geq 2$  gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \forall a \in \mathbb{Z}_n^+$$

(Bemerkung: Satz 3.57  $\stackrel{n \text{ Primzahl}}{\implies}$  Satz 3.50)  
 $\varphi(n)=n-1$

Berechne  $ggT(a, b)$  für  $a, b \in \mathbb{Z} = (\mathbb{Z}, +, \diamond)$

- Euklidischer Algorithmus (vgl. Übung 11):

$$? = ggT(729, 153)$$

- Primfaktorzerlegung:

$$729 = 3^6$$

$$153 = 3^2 \cdot 17$$

$$\Rightarrow ggT(729, 153) = 9$$

- Division mit Rest:

$$729 = 4 \cdot 153 + 117$$

$$153 = 1 \cdot 117 + 36$$

$$117 = 3 \cdot 36 + 9$$

$$36 = 4 \cdot 9 + 0$$

$$\Rightarrow ggT(729, 153) = 9$$

□

**3.63 Lemma**

Sind  $m, n \in \mathbb{N}$  mit  $m \leq n$  und  $m \nmid n$ , so gilt:

$$ggT(m, n) = ggT(n \bmod m, m)$$

**Beweis**

Übung.

□

**3.64 Satz (Euklidischer Algorithmus)**

Seien  $a_0, a_1 \in \mathbb{N}$  mit  $a_0 \geq a_1$

Man bestimmt sukzessive  $q_i, a_i \in \mathbb{N}$  wie folgt:

$$a_0 = q_1 a_1 + a_2 \text{ mit } 0 < a_2 < a_1$$

$$a_1 = q_2 a_2 + a_3 \text{ mit } 0 < a_3 < a_2$$

⋮

$$a_{k-1} = q_{k-1} a_{k-1} + a_k \text{ mit } 0 < a_k < a_{k-1}$$

Dann gilt:  $a_k = ggT(a_0, a_1)$ .

□

**3.65 Definition (normiert)**

Ein Polynom  $f = \sum_{k=0}^n a_k x^k$  heißt **NORMIERT**, wenn  $a_n = 1$ .

□

**3.66 Folgerung**

Ist  $K$  ein Körper, so hat jedes Polynom  $f \in K[x] \setminus \{0\}$  eine eindeutige Zerlegung (bis auf die Reihenfolge der Faktoren) in der Form:

$$f = u f_1 \cdot f_2 \cdot \dots \cdot f_r, n \in K^* \text{ und } f_i \text{ ist irreduzibel und normiert.}$$

**Beweis**

Beispiel 3.52 und Satz 3.53

□

**3.67 Satz**

Es sei  $(R, \delta)$  ein euklidischer Ring und  $0 \neq f \in R$ , so ist:

$$R/fR = \{[g]_f \mid g \in R, \delta(g) < \delta(f)\} \cup \{0\}$$

wobei  $[g]_f = g + fR = \{g + fZ \mid z \in R\}$

Es ist  $R/fR$  Körper.  $\Leftrightarrow f$  ist irreduzibel.

**Beweis**

Da  $(R, \delta)$  ein euklidischer Ring ist und  $f \neq 0$  gibt es zu einem beliebigen  $g \in R$  stets  $q, r \in R$  mit  $g = q \cdot f + r$  mit  $r = 0$  oder  $\delta(r) < \delta(f)$ .

$\Rightarrow g - r = q \cdot f \in R$ , also:  $[g]_f = [r]_f$ .

Nach Definition gilt:

$$R/fR = \{[g]_f \mid g \in R\} = \{[g]_f \mid g \in R, \delta(g) < \delta(f)\} \cup \{0\}$$

Nun zeigen wir:  $R/fR$  ist ein Körper  $\Leftrightarrow f$  ist irreduzibel.

„ $\Leftarrow$ “: (Ist  $f$  irreduzibel, so ist  $R/fR$  ein Körper.)

Sei  $0 \neq [g]_f \in R/fR$ . Zu zeigen.  $[g]_f^{-1}$  existiert.

$f$  ist irreduzibel  $\Rightarrow f \nmid g \Rightarrow 1 \in \text{ggT}(f, g)$

$$\Rightarrow \exists y, z \in R : 1 = yf + zg$$

Ü11, A2

$$\Rightarrow \underbrace{[1]_f}_{=1} = \underbrace{[yf]_f}_{=0} + [z]_f \cdot [g]_f$$

$1 = [z]_f \cdot [g]_f \Rightarrow [g]_f$  ist invertierbar mit  $[g]_f^{-1} = [z]_f$ .

Also:  $R/fR$  ist ein Körper.

„ $\Rightarrow$ “: (Ist  $R/fR$  ein Körper, so ist  $f$  irreduzibel.)

Wir zeigen: Sei  $f$  nicht irreduzibel, dann ist  $R/fR$  kein Körper.

$f$  ist nicht irreduzibel  $\Rightarrow \exists a, b \in R \setminus R^* : f = a \cdot b$

$$\underbrace{[f]_f}_{=0} = [a \cdot b]_f = [a]_f \cdot [b]_f$$

Wäre  $[a]_f = 0$ , so gälte  $f \mid a$ , d.h.  $\exists a_1 \in R : a = f \cdot a_1$

$$\Rightarrow f = a \cdot b = f \cdot \underbrace{a_1 \cdot b}_{=1 \in R^*} \Rightarrow a_1 \cdot b = 1 \Rightarrow b \in R^* \nmid$$

Also:  $[a]_f \neq 0$ .

Analog kann man zeigen:  $[b]_f \neq 0$ .

Insgesamt ist  $R/fR$  kein Integritätsbereich.

$R/fR$  ist kein Körper.

(Bemerkung: Ist  $f \in R^*$ , so ist  $R/fR = R/R = \{0\}$  kein Körper.)

□

**3.68 Beispiel**

Sei  $K = \mathbb{Z}_2 = \{0, 1\}$ . Dann ist  $K$  ein Körper

$(\mathbb{Z}_2[x], \delta)$  mit  $\delta(g) = \text{grad}(g)$  für  $g \in \mathbb{Z}_2[x]$  ist ein euklidischer Ring.

Gegeben ist  $f = x^3 + x + 1 \in \mathbb{Z}_2[x]$ . Dann ist  $f$  irreduzibel.

$\mathbb{Z}_2[x]/f\mathbb{Z}_2[x] = \{[a_0 + a_1x + a_2x^2]_f \mid a_0, a_1, a_2 \in \mathbb{Z}_2\}$  ist ein Körper mit 8 Elementen, die durch 3 Bits dargestellt werden:

$$[a_0 + a_1x + a_2x^2]_f \leftrightarrow a_0a_1a_2$$

$$\alpha = [x]_f \leftrightarrow 010$$

$$\alpha^2 = [x^2]_f \leftrightarrow 001$$

$$\alpha^3 = [x^3]_f = [x+1]_f \leftrightarrow 110$$

$$\text{denn: } x^3 = (x+1) + \underbrace{(x^3+x+1)}_{:=f} \cdot 1$$

$$\alpha^4 = \alpha^3 \cdot \alpha = [x^2+x]_f = [x+1]_f \leftrightarrow 011$$

$$\alpha^5 = \alpha^4 \cdot \alpha = [x^3+x^2]_f = [x^2+x+1]_f \leftrightarrow 111$$

$$\text{denn: } x^3+x^2 = \underbrace{(x^2+x+1)}_{:=g} + \underbrace{(x^3+x+1)}_{:=f}$$

$$\alpha^6 = \alpha^5 \cdot \alpha = [x^3+x^2]_f = [x^2+x+1]_f \leftrightarrow 101$$

$$\text{denn: } x^3+x^2+x = \underbrace{(x^2+1)}_{:=g} + \underbrace{(x^3+x+1)}_{:=f}$$

$$\alpha^7 = \alpha^6 \cdot \alpha = [x^3+x]_f = [1]_f \leftrightarrow 100$$

$$\alpha^8 = \alpha$$

□

### 3.69 Bemerkung

Ist  $\alpha^i = \beta$ , so schränkt man  $i = \log_\alpha(\beta)$  ein („diskreter Logarithmus“).

□

## § 6 Endliche Körper

### Vorbemerkungen

Unendliche Körper:

$(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$

Endliche Körper:

(1)  $(\mathbb{Z}_2, +_2, \cdot_2)$ , wobei  $+_n : a+_n b := (a+b) \bmod n$ ,  $\cdot_n : a \cdot_n b := (a \cdot b) \bmod n$ .

$$|\mathbb{Z}_2| = 2$$

(2)  $(\mathbb{Z}_2[x]/f\mathbb{Z}_2[x], +_f, \cdot_f)$  mit  $f = x^3+x+1$  (vgl. Beispiel 3.68),

wobei  $+_f : g+_f h := (g+h) \bmod f$ ,  $\cdot_f : g \cdot_f h := (g \cdot h) \bmod f$ .

$$|\mathbb{Z}_2[x]/(x^3+x+1)\mathbb{Z}_2[x]| = |\{[a_0+a_1x+a_2x^2]_f \mid a_0, a_1, a_2 \in \mathbb{Z}_2\}|$$

$$= |\{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}| = 2^3$$

Wir werden uns in diesem Abschnitt mit der Konstruktion von endlichen Körpern beschäftigen.

Anwendung: CD-Spieler.

Aus Satz 3.67 erhalten wir sofort die Folgerung 3.70.

□

### 3.70 Folgerung

(1)  $(\mathbb{Z}_n, +_n, \cdot_n)$  ist ein Körper  $\Leftrightarrow n$  ist Primzahl.

(2) Sei  $K$  ein Körper und  $f \in K[x]$ . Dann gilt:

$(K[x]/fK[x], +_f, \cdot_f)$  ist ein Körper  $\Leftrightarrow f$  ist irreduzibel über  $K[x]$

(D.h.:  $f = g \cdot h \Leftrightarrow \text{grad}(g) = 0$  oder  $\text{grad}(h) = 0$ )

□

### Bemerkung

$p^k$ ,  $p$  Primzahl,  $k \in \mathbb{N}$ .

Bis auf Isomorphie kann man einen endlichen Körper mit  $p^k$  vielen Elementen konstruieren.

Wenn ja: ist die Konstruktion eindeutig?

□

**3.71 Satz**

- (1) Für ein  $n \in \mathbb{N}$  gibt es einen Körper mit  $n$  Elementen  $\Leftrightarrow n = p^k$  für eine Primzahl  $p$  und ein  $k \in \mathbb{N}$ .
- (2) Sind  $K_1$  und  $K_2$  zwei endliche Körper mit  $|K_1| = |K_2|$ , so gilt  $K_1 \cong K_2$ .  
(GALOISKÖRPER (engl. galois field) mit  $p^k$  Elementen,  $\text{GF}(p^k)$ : der (bis auf Isomorphie) eindeutige endliche Körper mit  $p^k$  Elementen.)

Mit Folgerung 3.70 und Satz 3.71 kann man alle endlichen Körper konstruieren. □

**3.72 Satz**

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

Z.B. (vgl. Beispiel 3.68):

$$(\mathbb{Z}_2[x]/(x^3 + x + 1)\mathbb{Z}_2[x])^* = \underbrace{\langle [x]_f \rangle}_{\text{GENERATOR}}$$

• Effiziente Implementierung:

Sei  $p$  eine Primzahl.

$$k = 1: \text{GF}(p) \cong (\mathbb{Z}_p, +_p, \cdot_p)$$

$$k > 1: \text{GF}(p^k) \cong \mathbb{Z}_p[x]/f\mathbb{Z}_p[x], f \text{ irreduzibel mit } \text{grad}(f) = k.$$

$$\left( \mathbb{Z}_p[x]/f\mathbb{Z}_p[x] = \left\{ \sum_{i=0}^{k-1} a_i x^i \mid a_i \in \mathbb{Z}_p \right\} \sim a_0 a_1 \cdots a_{k-1}, a_i \in \mathbb{Z}_p, i = 0, 1, \dots, k-1 \right)$$

D.h.: Wir können die Elemente in  $\mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$  in kanonischer Weise durch Zeichenketten  $a_0 a_1 \cdots a_{k-1}$  mit  $a_i \in \mathbb{Z}_p$  kodieren.

• Addition von zwei Polynomen:

$$a(x) \longleftrightarrow a_0 a_1 \cdots a_{k-1}$$

$$b(x) \longleftrightarrow b_0 b_1 \cdots b_{k-1}$$

$$c(x) \longleftrightarrow c_0 c_1 \cdots c_{k-1}, c_i = (a_i + b_i) \text{ mod } p$$

• Multiplikation von zwei Polynomen:

(a)  $c(k) = a(x) \cdot b(x) = (\dots) \cdot (\dots)$  ausrechnen, dann den Rest modulo  $f$  bestimmen  $\rightarrow$  relativ aufwendig

(b)  $a(x) \cdot \sum_{i=0}^{k-1} b_i x^i = a(x) \cdot b_0 + x \cdot (a(x) \cdot b_1 + x \cdot (\dots + x \cdot (a(x) \cdot b_{k-2} + x \cdot a(x) \cdot b_{k-1})))$  □

**3.73 Beispiel (Fortsetzung von Beispiel 3.68)**

$p = 2, k = 3, f = x^3 + x + 1 \in \mathbb{Z}_2[x]$  irreduzibel.

$\mathbb{Z}_2[x]/(x^3 + x + 1)\mathbb{Z}_2[x]$	Kurzdarstellung
0	000
1	100
$x$	010
$1+x$	110
$x^2$	001
$1+x^2$	101
$x+x^2$	011
$1+x+x^2$	111

Seien nun  $a(x) = x + x^2$  und  $b(x) = 1 + x + x^2$ . Dann gilt:

$$a(x) \cdot b(x) = a(x) \cdot \underbrace{b_0}_1 + x \cdot (a(x) \cdot \underbrace{b_1}_1 + x \cdot a(x) \cdot \underbrace{b_2}_1)$$

Aufgabe	Realisierung	Ergebnis
Berechne $a(x) \cdot b_2$	$b_2 = 1$ , also $a(x) \cdot b_2 = a(x)$	0110
Multipliziere mit $x$	Shift nach rechts	0011
Berechne Rest modulo $f$	XOR mit $f = 1101$	1110
Addiere $a(x) \cdot b_1$	$b_1 = 1$ , also XOR mit $a = 0110$	1000
Multipliziere mit $x$	Shift nach rechts	0100
Berechne Rest modulo $f$	letztes Bit = 0	–
Addiere $a(x) \cdot b_0$	$b_0 = 1$ , also XOR mit $a = 0110$	0010

Aus der letzten Zeile können wir das Ergebnis ablesen:

$$a(x)_f \cdot b(x) = x^2$$

Test:

$$\begin{aligned} (x+x^2) \cdot (1+x+x^2) &= x+x^2+x^3+x^2+x^3+x^4 \\ &= x + \underbrace{2x^2}_{=0} + \underbrace{2x^3}_{=0} + x^4 \\ &= x+x^4 \\ &= x^2 + x \cdot \underbrace{(x^3+x+1)}_{=f} \end{aligned}$$

Nach Satz 3.72 gibt es für jedes Polynom  $t(x) \in \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$  ein  $l_t \in \{0, 1, \dots, p^{k-2}\}$  mit  $t(x) = \alpha^{l_t}$ .

In Beispiel 3.68 gilt:  $\alpha = [x]_f$ .

$$a(x) = x+x^2 = \alpha^4, \quad b(x) = 1+x+x^2 = \alpha^5.$$

$$\text{Dann gilt: } a(x) \cdot_f b(x) = \alpha^{l_a} \cdot \alpha^{l_b} = \alpha^{(l_a+l_b) \bmod p^{k-1}} = \alpha^4 \cdot \alpha^5 = \alpha^{9 \bmod 2^3-1} = \alpha^2 = x^2.$$

Wie speichert man Daten auf CDs?

⇒ „READ-SOLOMON-CODE“ (endliche Körper)

1	0	1	...	...	0	1	...	...	0	1
---	---	---	-----	-----	---	---	-----	-----	---	---

s Bits                      s Bits                      s Bits

= 1 Block

k Blöcke

— ENDE —

## Tabellenverzeichnis

1.1	Unterschiede zwischen Potenzreihen aus der Analysis und formalen Potenzreihen / erzeugenden Funktionen . . . . .	12
1.2	Formale Potenzreihen und ihre erzeugenden Funktionen . . . . .	17



## Abbildungsverzeichnis

1.1	Disjunkte Vereinigung von $A$ und $B$ ( $A \uplus B$ ) . . . . .	1
1.2	Vereinigung von $A$ und $B$ ( $A \cup B$ ) . . . . .	1
1.3	Pascal-Dreieck für $n = 0, 1, \dots, 5$ . . . . .	3
1.4	Rekursion für die Stirlingzahlen 2. Art (Stirling-Dreieck 2. Art) . . . . .	8
1.5	Rekursion für die Stirlingzahlen 1. Art (Stirling-Dreieck 1. Art) . . . . .	11
2.1	Beispiel: Schnittecken und Brücken . . . . .	30
2.2	Beispiel für einen Baum: Dateisystem . . . . .	32
2.3	Beispiel für einen Wurzelbaum . . . . .	33
2.4	3-regulärer Dodecaeder . . . . .	40
2.5	Das Königsberger-Problem . . . . .	43



# Index

- abelsch, 55
- Ableitung
  - formale, 16
- adjazent, 27
- Adjazenzmatrix, 29
- Algebra
  - universelle, 53
- Algebra-Homomorphismus, 58
- Äquivalenzrelation, 60
- Automorphismus., 59
  
- Bézierkurve, 4
- balanciert, 34
- Baum, 32
  - binärer, 34
    - vollständiger, 34
  - geordneter, 34
  - spannender, 35
  - Wurzel-, 33
- Baumfaktor, 35
- benachbart, 46
- Bernsteinpolynom, 4
- binärer Baum, 34
- Binomialkoeffizienten
  - verallgemeinerte, 17
- bipartit, 39
- boolesche Algebra, 56
- Brücke, 30
- Breitensuche, 35
  
- charakteristische Funktion, 2
  
- Digraph, 48
  - schlichter, 48
  - stark zusammenhängender, 50
  - Teil-, 48
- disjunkte Vereinigung, 1
  
- ebener, 45
- Ecke
  - End-, 27
  - isolierte, 27
- Ecken, 25
- Eckengrad, 27
- edges, 25
- einbettbar, 45
  
- Einheit, 64
- Element
  - inverses, 55
  - linksinverses, 55
  - linksneutrales, 54
  - neutrales, 54
  - rechtsinverses, 55
  - rechtsneutrales, 54
- Endecke, 27
- erzeugende Funktion, 12
- erzeugte Unteralgebra, 58
- Euklidischer Ring, 66
- eulersch, 43
- eulersche  $\varphi$ -Funktion, 67
- eulerscher Kantenzug, 43
- Eulertour, 43, 49
- Exklusion, 6
  
- Färbung, 47
  - p-, 47
- Faltung, 13
- Fibonacci-Zahlen, 19
- formale Ableitung, 16
- Freiformkurve, 4
- Fundamentalsatz der Arithmetik, 66
- Funktion
  - charakteristische, 2
  - erzeugende, 12
  
- Galoiskörper, 71
- Gebiete, 45
- Generator, 71
- geordneter Baum, 34
- Gerüst, 35
- geschlossene Kantenfolge, 49
- gewichteter Graph, 44
- Goldener Schnitt, 20
- größter gemeinsamer Teiler, 64
- Graph, 25
  - bipartiter, 39
  - ebener, 45
  - einbettbarer, 45
  - gewichteter, 44
  - hamiltonscher, 40
  - isomorpher, 28

- k-partiter, 40
- leerer, 27
- markierter, 28
- Multi-, 27
- multipartiter, 40
- Null-, 27
- numerierter, 28
- planarer, 45
- schlichter, 27
- semi-hamiltonscher, 41
- untergeordneter, 50
- Unterteilungs-, 46
- vollständiger, 25
- zusammenhängender, 30
- geschlossener Kantenzug, 49
- Gruppe, 55
  - Symmetrische, 2
  - Unter-, 57
- Halbgruppe, 55
- Hamiltonkreis, 40
- hamiltonscher Graph, 40
- Hamiltonscher Kreis, 49
- Hamiltonscher Weg, 49
- Hamiltonweg, 40
- Hauptideal, 63, 65
- Hauptidealring, 65
- homogene lineare Rekursionsgleichung, 18
- Homomorphismus, 58
  - Algebra-, 58
- Ideal, 62
  - Haupt-, 63
- induzierter Teildigraph, 48
- induzierter Teilgraph, 30
- inhomogene lineare Rekursionsgleichung, 18
- Inklusion, 6
- Integritätsbereich, 64
- Inverse, 55
- inverses Element, 54
- invertierbar, 14
- Inzidenzmatrix, 29
- inzidiert, 27
- irreduzibel, 65
- isolierte Ecke, 27
- isomorph, 28, 59
- Isomorphismus, 59
- k-partit, 40
- k-regulär, 27
- Körper, 56
- Kanten, 25
  - Mehrfach-, 27
- Kantenfolge, 43
  - geschlossene, 49
  - orientierte, 49
- Kantenzug, 43
  - eulerscher, 43
  - geschlossener, 49
  - orientierter, 49
- kartesisches Produkt, 1
- Knoten, 25
- kommutativer Ring, 56
- Komponente, 30
  - stark zusammenhängende, 50
- Kongruenzrelation, 60
- Konvolution, 13
- Kreis
  - Hamiltonscher, 49
  - orientierter, 49
- Kronecker-Symbol, 12
- Länder, 45
- Landkarte, 45
- leerer Graph, 27
- lineare Rekursionsgleichung, 18
- linksinverses Element, 55
- linksneutrales Element, 54
- markiert, 28
- Matching, 37
  - maximales, 37
  - Maximum-, 37
  - perfektes, 37
- maximal, 37
- Maximum-Matching, 37
- Mehrfachkanten, 27
- Monoid, 55
- Multigraph, 27
- multipartit, 40
- Nachbarschaft, 27
- Nachfolger, 34
  - unmittelbarer, 34
- neutrales Element, 54
- Norm-Euklidischer Ring, 66
- normiert, 68
- Null-Graph, 27
- Nullteiler, 64
- nummeriert, 28
- Operation, 53
- Operator, 53
- orientierte Kantenfolge, 49
- orientierter Kantenzug, 49
- orientierter Kreis, 49
- orientierter Weg, 49
- Partition, 7
- Partitions Mengen, 39

- 
- Pascal-Dreieck, 3
  - perfekt, 37
  - Permutation, 2
  - planar, 45
  - Polynomring, 56
  - Potenzmenge, 2
  - Prüfercode, 36
  - Primfaktor-Zerlegung, 65
  - Primzahl, 64
  - Produkt
    - kartesisches, 1
  - Punkte, 25
  
  - Read-Solomon-Code, 72
  - rechtsinverses Element, 55
  - rechtsneutrales Element, 54
  - Rekursionsgleichung
    - lineare, 18
      - homogene, 18
      - inhomogene, 18
  - Relation, 60
    - Äquivalenz-, 60
    - Kongruenz-, 60
  - Ring, 55
    - Euklidischer, 66
    - kommutativer, 56
    - Norm-Euklidischer, 66
    - Polynom-, 56
    - Teil-, 57
    - Unter-, 57
  
  - Schleifen, 27
  - schlichter Graph, 27
  - Schnittecke, 30
  - Schubfachprinzip, 5
  - semi-eulersch, 43
  - semi-hamiltonscher Graph, 41
  - Siebformel, 6
  - Signatur, 53
  - spannender Baum, 35
  - Splines, 4
  - stark zusammenhängend, 50
  - stark zusammenhängende Komponente, 50
  - Stelligkeit, 53
  - Sterngraph, 38
  - Stirling-Dreieck zweiter Art, 8
  - Stirlingzahl
    - erster Art, 11
  - Stirlingzahl erster Art, 11
  - Stirlingzahlen, 8
  - Symmetrische Gruppe, 2
  
  - Teildigraph, 48
    - induzierter, 48
  - Teiler
    - größter gemeinsamer, 64
  - Teilgraph
    - induzierter, 30
  - Teilring, 57
  - Tiefe, 34
  - Tiefensuche, 35
  - Turnier, 51
    - n-, 51
  
  - universelle Algebra, 53
  - unmittelbarer Nachfolger, 34
  - unmittelbarer Vorgänger, 34
  - Unteralgebra, 57
    - erzeugte, 58
  - untergeordneter Graph, 50
  - Untergruppe, 57
  - Unterring, 57
  - Unterteilungsgraph, 46
  
  - Vereinigung
    - disjunkte, 1
  - Verknüpfung, 53
  - vertices, 25
  - Vierfarbenvermutung, 47
  - vollständiger binärer Baum, 34
  - Vorgänger, 34
    - unmittelbarer, 34
  
  - Wald, 32
  - Weg
    - Hamiltonscher, 49
    - orientierter, 49
  - Wurzelbaum, 33
    - balancierter, 34
  
  - Zerlegung
    - Primfaktor-, 65
    - zusammenhängend, 30
  - Zusammenhangskomponente, 30
  - Zyklus, 10
-