

Diskrete Strukturen

Mitschrift von M.Sondermann und P.Elftmann

SS 2002

Vorwort

Dies ist eine Mitschrift der Vorlesung 'Diskrete Strukturen' des Sommersemesters 2002 bei Priv.-Doz. Dr. Guo. Es erhebt keinerlei Anspruch auf Korrektheit und Vollständigkeit und stellt keine offizielle Veröffentlichung des Lehrstuhls dar. Bei Fehlern, Verbesserungsvorschlägen oder sonstigen Anregungen wird um eine Email an eine der unten angegebenen Adressen.

Patrick Elftmann, patrick.elftmann@post.rwth-aachen.de
Matthias Sondermann, matthias.sondermann@post.rwth-aachen.de

Letzte Änderung : 19.Juli 2002

Inhaltsverzeichnis

1	Abzählung, Rekursion, erzeugende Funktion	4
1.1	Elementare Zählprinzipien	4
1.2	Mengenpartitionen	6
1.3	Permutationen	7
1.4	Erzeugende Funktionen (formale Potenzreihen)	8
1.5	Rekursionsgleichungen	13
2	Graphentheorie	19
2.1	Grundbegriffe der Graphentheorie	19
2.2	Darstellung von Graphen	21
2.3	Bäume	24
2.4	Matchings in Graphen	28
2.5	Hamilton-Graphen	30
2.6	Eulersche Graphen	32
2.7	Planare Graphen	33
2.8	Digraphen	36
3	Algebraische Strukturen	39
3.1	universelle Algebren	39
3.2	Unteralgebra, Homomorphismus, Konvergenz	41
3.3	Ringe und Ideale	45
3.4	Größter gemeinsamer Teiler	46
3.5	Eindeutige Primfaktorzerlegung	47
3.6	Endliche Körper	51

1 Abzählung, Rekursion, erzeugende Funktion

1.1 Elementare Zählprinzipien

M: endliche Menge

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

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

$|M| = 0 \Leftrightarrow M = \emptyset$

Lemma 1.1

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 $A \cap B = \emptyset$

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

$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$ heißt das kartesische Produkt von A und B

Folgerung 1.2

Seien A und B zwei endliche Mengen. Abbildung $(A, B) = B^A =$ Menge alle Abbildungen von A nach B. Dann gilt $|B^A| = |B|^{|A|}$

Definition 1.3

Sei A eine Menge. $f: A \rightarrow A$ heißt die Permutation von A, wenn f bijektiv ist.

Lemma 1.4

Sei $S_n = \{a \mid a: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \text{ bijektiv}\} = \text{Sym}\{1, 2, \dots, n\}$ (Symmetrische Gruppe)

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

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

Satz 1.5

Die Anzahl der Teilmengen einer n-Menge A ist 2^n ,

d.h. $|A| = n \implies |P(A)| = 2^n$, wobei $P(A) = \{B \mid B \subseteq A\}$ die Potenzmenge von A ist.

Definition 1.6

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

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

Bemerkung 1.7

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

$\implies |P(A)| = |P_0(A)| + |P_1(A)| + \dots + |P_n(A)| = \sum_{k=0}^n |P_k(A)|$

Lemma 1.8

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

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

Satz 1.9 (Pascal-Dreieck)

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

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

Satz 1.10 (Vandermonde'sche Identität)

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

Lemma 1.11 (doppeltes Abzählen)

Seien S und T Mengen $R \subseteq S \times T$ eine Relation. Dann gilt

$$|R| = \underbrace{\sum_{s \in S} |\{t \in T \mid (s, t) \in R\}|}_{\text{Zeilensumme}} = \underbrace{\sum_{t \in T} |\{s \in S \mid (s, t) \in R\}|}_{\text{Spaltensumme}}$$

Satz 1.12 (Schubfachprinzip)

Sei $f : X \rightarrow Y$ eine Abbildung und es gilt $|X| > |Y|$, so gibt es ein $y \in Y$ mit $|f^{-1}(y)| \geq 2$.

Text: Verteilt man n Elemente auf m Fächer, wobei $n > m$ ist, so gibt es mindestens ein Fach, das zwei Element enthält.

Beispiele 1.13

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 mindestens zwei Personen, die die gleiche Anzahl von Personen in P kennen, die Relation ist also symmetrisch.

Satz 1.14 (verallgemeineretes Schubfachprinzip)

Sei $f : X \rightarrow Y$ eine Abbildung, so gibt es ein $y \in Y$ mit $|f^{-1}(y)| \geq \lceil \frac{|X|}{|Y|} \rceil$

Text: Verteilt man 7 Bücher auf 3 Fächer, so gibt es mindestens 1 Fach, das 3 Bücher enthält.

Einschub : Rückblick auf Lemma 1.1c) und 1.1b)

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

• $M = A_1 \times A_2 \times \dots \times A_n \implies |M| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$

$$= \prod_{i=1}^n |A_i| \text{ (Produktregel)}$$

b) 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 $S = A_1 \cup A_2 \cup \dots \cup A_n = \uplus_{i=1}^n A_i$

$$\implies |S| = |A_1| + |A_2| + \dots + |A_n| = \sum_{i=1}^n |A_i| \text{ (Summenregel)}$$

Satz 1.15 (Prinzip der Inklusion und Exklusion / Siebformel)Für endliche Mengen A_1, A_2, \dots, A_n gilt:

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

Beispiel 1.16Sei $k \in \mathbb{N}$ und $M_k = \{n \in \mathbb{N} \mid 1 \leq n \leq 100, n \text{ teilt } k\}$ Bestimmen Sie $|M_2 \cap M_3 \cap M_5|$ (Anzahl die durch 2 oder 3 oder 5 teilbaren natürlichen Zahlen ≤ 100)Lösung: $|M_k| = \lfloor \frac{100}{k} \rfloor$, da genau k -te natürliche Zahl durch k teilbar ist.

$$\begin{aligned} |M_2 \cap M_3 \cap M_5| &= |M_2| + |M_3| + |M_5| - \underbrace{|M_2 \cap M_3|}_{M_6} - \underbrace{|M_2 \cap M_5|}_{M_{10}} - \underbrace{|M_3 \cap M_5|}_{M_{15}} \\ &\quad + \underbrace{|M_2 \cap M_3 \cap M_5|}_{M_{30}} \end{aligned}$$

$$\begin{aligned} |M_2 \cap M_3 \cap M_5| &= \lfloor \frac{100}{2} \rfloor + \lfloor \frac{100}{3} \rfloor + \lfloor \frac{100}{5} \rfloor - \lfloor \frac{100}{6} \rfloor - \lfloor \frac{100}{10} \rfloor - \lfloor \frac{100}{15} \rfloor + \lfloor \frac{100}{30} \rfloor \\ &= 50 + 33 + 20 - 16 - 10 - 6 + 3 \\ &= 74 \end{aligned}$$

1.2 Mengenpartitionen

Definition 1.17Sei M eine Menge mit $|M| = n$

- Eine Partition P von M ist eine Zerlegung von M in eine Vereinigung von disjunkten nichtleeren Teilmengen.
- Gilt $M = A_1 \uplus A_2 \uplus \dots \uplus A_k$ mit $A_i = \emptyset$ für $i \in \{1, 2, \dots, n\}$ so heißt $P = \{A_1, A_2, \dots, A_k\}$ eine k -Partition von M .
- $Part_k(M) := \{P \mid P \text{ ist eine } k\text{-Partition von } M\}$
- Stirlingzahlen zweiter Art:

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

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

Beispiel 1.181) $M = \{1, 2, 3, 4\}$

$$Part_1(M) = \{\{M\}\}$$

$$Part_2(M) = \{\{\{1\}, \{2, 3, 4\}\}, \{\{2\}, \{1, 3, 4\}\}, \{\{3\}, \{1, 2, 4\}\}, \{\{4\}, \{1, 2, 3\}\}, \{\{1, 2\}, \{3, 4\}\}, \{\{1, 3\}, \{2, 4\}\}, \{\{1, 4\}, \{2, 3\}\}\}$$

Im Allgemeinen:

$$|Part_2(M)| = \frac{1}{2}(2^n - 2) \text{ für } |M| = n$$

2) Für $n \geq 1$ gilt:

$$S_{n,0} = 0, \quad S_{n,1} = 1, \quad S_{n,n-1} = \binom{n}{2}, \quad S_{n,n} = 1$$

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

Satz 1.19 (Stirling Dreieck zweiter Art)Für alle $k, n \in \mathbb{N}$ mit $1 \leq k \leq n$ gilt:

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

Stirling-Dreieck zweiter Art

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

Satz 1.20Seien M und N Mengen mit $|M| = m$ und $|N| = n$

- a) $|Abb(M, N)| = |N|^M = n^m$ (s. Folgerung 1.2)
- b) Menge aller injektiven Abbildungen von M nach N
 $|Inj(M, N)| = n^{\underline{m}} = n \cdot (n-1) \cdot \dots \cdot (n-(m-1))$
- c) Menge aller surjektiven Abbildungen von M nach N
 $|Surj(M, N)| = n! \cdot S_{m,n}$

Satz 1.21

$$n^m = \sum_{k=0}^n n^{\underline{k}} S_{m,k} \quad m, n \in \mathbb{N}$$

1.3 Permutationen

Wiederholung:

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

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

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 3 & 7 & 2 & 1 & 9 & 5 & 8 & 11 & 6 & 10 \end{pmatrix}$$

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

Definition 1.22

Ein k -Zyklus $(i_1, i_2, i_3, \dots, i_k)$ ist eine Permutation $\sigma \in S_n$ mit $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ und $\sigma(i) = i$ für $i \notin \{i_1, i_2, \dots, i_k\}$ wobei $\{i_1, i_2, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$

Bemerkung 1.23

- 1) Ein Zyklus ist nur durch die Reihenfolge der Elemente innerhalb des Zyklus bestimmt.
 z.B. $(1\ 2\ 4\ 6) = (2\ 4\ 6\ 1) = (4\ 6\ 1\ 2) = (6\ 1\ 2\ 4)$ aber $(1\ 2\ 4\ 6) \neq (1\ 2\ 6\ 4)$
- 2) Jedes $\sigma \in S_n$ läßt sich als Produkt von Zyklen schreiben.
 (Beispiel s. oben)

Einschub : Beispiel

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

$$S_3 = \{(1)(2)(3), (1)(23), (2)(13), (3)(12), (123), (132)\}, |S_3| = 3!$$

Definition 1.24

Die Anzahl der Permutationen von $\{1, 2, \dots, n\}$,

die genau k Zyklen haben, heißt Stirlingzahl erster Art, bezeichnet mit $s_{n,k}$ oder $\left[\begin{matrix} n \\ k \end{matrix} \right]$.

Z.B. in obigen Beispiel gilt:

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

$$s_{n,0} = 0 \quad \forall n \in \mathbb{N}, s_{0,0} = 1$$

Satz 1.25 (Stirling-Dreieck erster Art)

$$\forall k, n \in \mathbb{N} \text{ mit } n \geq k \geq 1 \text{ gilt: } s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}$$

Stirling Dreieck erster Art

n = 0				1			
n = 1			0	1			
n = 2			0	1	1		
n = 3			0	2	3	1	
n = 4			0	6	11	6	1

Bemerkung 1.26

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

1.4 Erzeugende Funktionen (formale Potenzreihen)

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

$$a_n = a_{n-1} + a_{n-2}, a_1 = 1, a_0 = 0$$

Um die Lösungen zu finden, brauchen wir erzeugende Funktionen.

Rekursionsgleichungen beschreiben unendliche Folgen: $a_0, a_1, a_2, \dots, a_n = (a_n)_{n \in \mathbb{N}_0}$

Wir führen eine neue Schreibweise für $(a_n)_{n \in \mathbb{N}_0}$:

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

Definiton 1.27

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

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

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

Bemerkung 1.28

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

$(\delta_{k,n} = \begin{cases} 1 & , n=k \\ 0 & , \text{sonst} \end{cases}$ heißt Kronecker-Symbol)

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

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

z.B. $k=2$: $\sum_{n=0}^{\infty} a_n x^{2n} = a_0 + 0x + a_2 x^2 + 0x^3 + a_4 x^4 + \dots$

4) Unterschiede zwischen

Potenzreihen aus der Analysis und formalen 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 neue Schreibweise der Folge $(a_n)_{n \in \mathbb{N}_0}$ |
| - Funktion von x | - i.a. nichts einzusetzen |
| - Konvergenzfrage | - keine Konvergenzfrage |

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

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

Definition 1.29

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

• Addition:

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

• Multiplikation:

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

Faltung oder Konvolution der Folgen $(a_n)_{n \in \mathbb{N}_0}$ und $(b_n)_{n \in \mathbb{N}_0}$ (Cauchy-Produkt aus der Analysis)

$$a \cdot \sum_{n=0}^{\infty} a_n x^n := \sum_{n=0}^{\infty} a \cdot a_n x^n$$

Lemma 1.30 (verschieben von Folgengliedern)

$$x^m \cdot \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} a_{n-m} x^n = (b_n)_{n \in \mathbb{N}_0}$$

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

Beispiel 1.31

Es gilt $x^m \cdot x^n = x^{m+n}$ $m, n \in \mathbb{N}_0$

Satz 1.32

a) $K[[x]]$ ist ein K -Vektorraum

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

Bemerkung 1.33

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

Lemma 1.34

Im $K[[x]]$ 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:

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

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

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

Seien $Bu := \{a, b, c\}$

$Zi := \{0, 1\}$

Für $k \in \mathbb{N}$ sei $W_k := \{\text{Folgen aus } i \text{ Buchstaben gefolgt von } k - i \text{ Zahlen} \mid 1 < i < k\}$
(z.B. $ab0 \in W_3$, $abb0010 \in W_7$, $abc11 \in W_5$)

Es gilt: $W_k := |W_k| = \sum_{i=1}^{k-1} 3^i \cdot 2^{k-i} = \underbrace{\sum_{i=0}^k 3^i \cdot 2^{k-i}}_{:=c_k} - 2^k - 3^k = \dots$

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

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

$$\dots = \sum_{i=0}^k 3^i \cdot 2^{k-i} - 2^k - 3^k = (3^{k+1} - 2^{k+1}) - 2^k - 3^k = 2 \cdot 3^k - 2^k$$

Satz 1.36 (Inversion von Potenzreihen)

Genau dann ist $A = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ invertierbar, wenn $a_0 = 1$ ist.

Beweis: A ist invertierbar \iff es gilt

$$B = \sum_{n=0}^{\infty} b_n x^n \text{ mit } A \cdot B = 1$$

$$A \cdot B = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} \right) x^n = 1 \iff \sum_{k=0}^n a_k b_{n-k} = \begin{cases} 1 & , \text{ für } n=0 \\ 0 & , \text{ sonst} \end{cases}$$

$$\iff \begin{array}{ll} a_0 b_0 = 1 & n = 0 \\ a_0 b_1 + a_1 b_0 = 0 & n = 1 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 & n = 2 \end{array}$$

Ist A invertierbar, so muß $a_0 \neq 0$. Umgekehrt ist $a_0 \neq 0$, so definiere

$$b_0 = \frac{1}{a_0} \in K$$

$$b_n = -\frac{1}{a_0} (a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_n b_0) \text{ rekursiv für } n \in \mathbb{N}_0$$

Beispiel 1.37

- 1) $A = 1 - cx = \sum_{n=0}^{\infty} a_n x^n$ mit $a_0 = 1, a_1 = -c, a_2 = a_3 = \dots = 0$
Bestimme A^{-1}

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

$$a_0 b_0 = 1 \implies b_0 = 1$$

$$a_0 b_1 + a_1 b_0 = 0 \iff 1 \cdot b_1 - c \cdot 1 = 0 \implies b_1 = c$$

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

$$\dots \implies b_n = c^n$$

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

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

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

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

Definition 1.38

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

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

$$D: a_0, a_1, a_2, \dots, a_n, \dots \rightarrow a_1, 2a_2, 3a_3, \dots, na_n, \dots)$$

Lemma 1.39

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

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

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

Folgerung 1.40

Ist $A \in K[[x]]$ invertierbar, so ist $D(A^{-1}) = -\frac{D(A)}{A^2}$

Beweis: $A \cdot A^{-1} = 1 \quad D(1) = 0$

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

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

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

Neuer Beweis zum Beispiel 1.37 2)

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

$$D(A^{-1}) = \sum_{n=0}^{\infty} (n+1)c^{n+1}x^n$$

$$\implies D(A^{-1}) = \frac{D(A)}{A^2} = -\frac{c}{(1-cx)^2} = \sum_{n=0}^{\infty} (n+1)c^{n+1}x^n$$

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

Folgerung 1.41

Für $m \in \mathbb{N}$ gilt:

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

Bemerkung 1.42

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

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

Formale Potenzreihe 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, ...	$\sum_{n=0}^{\infty} nx^n$	$\frac{x}{(1-x)^2}$
c^n	1, c, c^2 , ...	$\sum_{n=0}^{\infty} c^n x^n$	$\frac{1}{1-cx}$
n^2	0, 1, 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, $\frac{1}{2}$, ...	$\sum_{n=0}^{\infty} \frac{1}{n} x^n$	$\ln \frac{1}{1-x}$
$\frac{1}{n!}$	1, 1, $\frac{1}{2}$, ...	$\sum_{n=0}^{\infty} \frac{1}{n!} x^n$	e^x

1.5 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 den Lösungen der Teilprobleme die Lösung von P

Binäre Suche; Mergesort; der euklidische Algorithmus

- dynamische Programmierung (Optimierungsprobleme)
- Greedy-Algorithmus

Bei der Analyse von Algorithmen können Funktionen der Form

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

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

vorkommen. Für die Bestimmung der Laufzeit von Algorithmen spielt das Lösen von Rekursionsgleichungen eine zentrale Rolle.

Lineare Rekursion

Definition 1.43

Eine Rekursionsgleichung der Form

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

mit der Anfangsbedingung $a_i = b_i, i = 0, 1, \dots, k-1$ heißt lineare Rekursionsgleichung k-ter Ordnung.

- Gilt $b_k = 0$, so ist a_n eine homogene lineare Rekursionsgleichung
- Gilt $b_k \neq 0$, so ist a_n eine inhomogene lineare Rekursionsgleichung

Beispiel 1.44

1) Spezialfall der homogenen linearen Rekursionsgleichung $a_n = c \cdot a_{n-1}, \quad n \geq 1, \quad a_0 = b_0$

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

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

Lösung der Gleichung $a_n = b_0 c^n$

2) $a_n = c \cdot a_{n-1} + b_1, \quad n \geq 1, \quad a_0 = b_0, \quad c, b_0, b_1$ Konstante

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

Beweis: (Induktion über n)

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

$n \rightarrow n + 1$:

1. Fall: $c \neq 1$. Es gilt:

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

2. Fall: $c = 1$. Es gilt:

$$\begin{aligned} a_n &= a_{n-1} + b_1 \\ &= (b_0 + (n-1)b_1) + b_1 \\ &= b_0 + n b_1 \end{aligned}$$

Beispiel 1.45

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

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

Beispiel 1.46 (Fibonacci-Zahlen)

Ein Kaninchen bringt ab seinem zweiten Lebensmonat jeden Monat ein weiteres Kaninchen zur Welt. Falls Kaninchen unsterblich wären, wieviele Kaninchen gibt es aus einem einzigen Kaninchen nach n Monaten (F_n)?

Antwort: $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 1 + 1 = 2, F_4 = 2 + 1 = F_3 + F_2$

$$\implies F_n = F_{n-1} + F_{n-2}$$

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 Funktion

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

$$= F_0 x^0 + F_1 x^1 + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) x^n$$

$$= F_0 x^0 + F_1 x^1 + \sum_{n=2}^{\infty} F_{n-1} x^n + \sum_{n=2}^{\infty} F_{n-2} x^n$$

$$= F_0 x^0 + F_1 x^1 + x \cdot \sum_{n=1}^{\infty} F_n x^n + x^2 \cdot \sum_{n=0}^{\infty} F_n x^n$$

$$= F_0 x^0 + F_1 x^1 + x \cdot \underbrace{\sum_{n=0}^{\infty} F_n x^n}_{=F} - F_0 x^0 + x^2 \cdot \sum_{n=0}^{\infty} F_n x^n$$

$$= F_0 x^0 + F_1 x^1 + xF - F_0 x^0 + x^2 F \quad \text{mit } F_0 = 0 \text{ und } F_1 = 1$$

$$= x + xF + x^2 F$$

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

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

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

Somit gilt: $F_n = a\alpha^n + b\beta^n$

$$\begin{aligned} \text{Wegen } \frac{x}{1-x-x^2} &= \frac{x}{\frac{5}{4} - (x + \frac{1}{2})^2} \\ &= \frac{x}{\left(\frac{\sqrt{5}}{2} - (x + \frac{1}{2})\right) \cdot \left(\frac{\sqrt{5}}{2} + (x + \frac{1}{2})\right)} \\ &= \frac{\frac{1}{\sqrt{5}}}{1 - \frac{\sqrt{5}+1}{2} \cdot x} + \frac{-\frac{1}{\sqrt{5}}}{1 - \frac{1-\sqrt{5}}{2} \cdot x} \end{aligned}$$

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

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

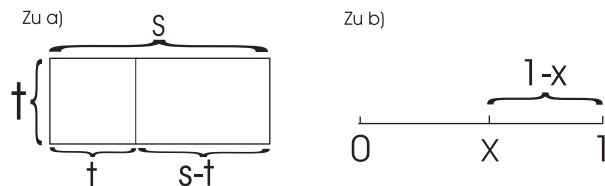
Bemerkung 1.47 (goldener Schnitt)

Die Zahl $\frac{1+\sqrt{5}}{2} = \theta$ heißt goldener Schnitt und taucht bei verschiedenen Untersuchungen auf, z.B.:

a) Bedingung: $\frac{s}{t} = \frac{t}{s-t} = \left(\frac{1}{\frac{s}{t}-1}\right)$, setze $\frac{s}{t} = x$, dann gilt:

$$x = \frac{1}{x-1} \Leftrightarrow x^2 - x - 1 = 0 \Leftrightarrow x_{1,2} = \frac{1 \pm \sqrt{5}}{2} \quad \text{Somit ist } x = \frac{\sqrt{5}-1}{2} = \frac{2}{1+\sqrt{5}} = \frac{1}{\theta} \text{ b)}$$

$$\frac{1}{x} = \frac{x}{1-x}, \quad 0 \leq x \leq 1 \quad \text{Es gilt: } \frac{x}{x-1} = \frac{1}{x} \Leftrightarrow x_{1,2} = \frac{-1 \pm \sqrt{5}}{2} \leftarrow x = \frac{\sqrt{5}-1}{2} = \frac{2}{1+\sqrt{5}} = \frac{1}{\theta} \approx 0,618$$



Satz 1.48

$a_n = c_1 a_{n-1} + c_2 a_{n-2}$ für $n \geq 2$ und $a_1 = b_1, a_0 = b_0$
 Seien α, β zwei Lösungen der Gleichung $x^2 - c_1 x - c_2 = 0$ und

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

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

Schema zum Lösen von (homogenen) linearen Rekursionsgleichungen

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

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1} + \sum_{n=k}^{\infty} a_n x^n \\ &= b_0 + b_1 x + b_2 x^2 + \dots + b_{k-1} x^{k-1} + \sum_{n=k}^{\infty} (c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}) x^n \\ &= b_0 + b_1 x + b_2 x^2 + \dots + b_{k-1} x^{k-1} + \underbrace{\sum_{n=k}^{\infty} c_1 a_{n-1} x^n}_{=c_1 x \sum_{n=k}^{\infty} a_{n-1} x^{n-1}} + \sum_{n=k}^{\infty} c_2 a_{n-2} x^2 + \dots + \sum_{n=k}^{\infty} c_k a_{n-k} x^k \\ &= b_0 + b_1 x + b_2 x^2 + \dots + b_{k-1} x^{k-1} + c_1 x (A(x) - \sum_{i=0}^{k-2} a_i x^i) + c_2 x^2 (A(x) - \sum_{i=0}^{k-2} a_i x^i + \dots) \end{aligned}$$

3. Auflösen nach A(x)

$$A(x) = \frac{d_0 + d_1x + \dots + d_{k-1}x^{k-1}}{1 - c_1x - c_2x^2 - \dots - c_kx^k} \text{ für geeignete } d_0, d_1, \dots, d_{k-1}$$

4. Partialbruchzerlegung der rechten Seite (in \mathbb{C} , Aff)

Sei $1 - c_1x - c_2x^2 - \dots - c_kx^k = (1 - \alpha_1x)^{\alpha_1} - (1 - \alpha_2x)^{\alpha_2} - \dots - (1 - \alpha_kx)^{\alpha_k}$ mit $\sum_{i=1}^t m_i = k$ und sei

$$A(x) = \frac{d_0 + d_1x + \dots}{1 - c_1x - c_2x^2 - \dots - c_kx^k} = \frac{g_1(x)}{(1 - \alpha_1x)^{m_1}} + \dots + \frac{g_t(x)}{(1 - \alpha_tx)^{m_t}} = \sum_{i=1}^t \frac{g_i(x)}{(1 - \alpha_ix)^{m_i}}$$

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

$$A(x) = \sum_{j=1}^t \frac{g_j(x)}{(1 - \alpha_jx)^{m_j}} = \sum_{n=0}^{\infty} g_n x^n$$

Beispiel 1.49

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

Lösung: Sei $A(x) = \sum_{n=0}^{\infty} a_n x^n$, dann gilt:

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

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

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

Beispiel 1.50 (Catalan-Zahlen)

Klammer : ()

Klamerkette : (()) () , () ()

Zulässige Klamerkette: An jeder Stelle der Klammerkette ist die Anzahl der bis zu dieser Stelle vorkommenden öffnenden Klammern grösser oder gleich der Anzahl der bisher vorkommenden schließenden Klammern und zum Schluss sollen die beiden Zahlen gleich sein.

$|\{\text{Zulässige Klammerkette mit } 2n \text{ Klammern}\}| := C_n$

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

$$c_0 = 1$$

$$c_1 = 1 : ()$$

$$c_2 = 2 : () () , (())$$

$$c_3 = 5 : () () () , () (()) , (()) () , (() ()) , ((()))$$

Lemma 1.51

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

Beweis: ($\underbrace{\quad \quad \quad}_{\text{zulässige Klammerkette mit } 2(k-1) \text{ Klammern}}$ $\underbrace{\quad}_{2k}$ $\underbrace{\quad \quad \quad}_{\text{zulässige Klammerkette mit } 2n-2k \text{ Klammern}}$)

$A_k : \{ \text{zulässige Klammerkette mit } 2n \text{ Klammern deren erste öffnende Klammer an der Position } 2k \text{ geschlossen wird} \}$

$$|A_k| = c_{k-1} \cdot c_{n-k}$$

$$\Rightarrow c_n = |\cup_{k=1}^n A_k| = \sum_{k=1}^n |A_k| = \sum_{k=1}^n c_{k-1} \cdot c_{n-k}$$

Lemma 1.52

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

Beweis: Sei $c(x) = \sum_{n=0}^{\infty} c_n x^n$. Dann gilt:

$$\begin{aligned} c(x) &= c_0 x^0 + \sum_{n=1}^{\infty} c_n x^n \\ &\stackrel{1.51}{=} c_0 + \sum_{n=1}^{\infty} (\sum_{k=1}^n c_{k-1} \cdot c_{n-k}) x^n \\ &= c_0 + x \sum_{n=1}^{\infty} (\sum_{k=1}^n c_{k-1} \cdot c_{n-k}) x^{n-1} \\ &\stackrel{t=n-1}{=} c_0 + x \sum_{t=0}^{\infty} (\sum_{k=1}^{t+1} c_{k-1} \cdot c_{(t+1)-k}) x^{n-1} \\ &\stackrel{s=k-1}{=} c_0 + x \sum_{t=0}^{\infty} (\sum_{s=0}^t c_s \cdot c_{(t-s)}) x^t \\ &\stackrel{1.29}{=} c_0 + x \cdot c(x) \cdot c(x) \end{aligned}$$

Somit gilt:

$$xc^2(x) - c(x) = -1$$

$$x^2 c^2(x) - xc(x) = -x$$

$$\stackrel{q.E.}{\Rightarrow} (xc(x) - \frac{1}{2})^2 = \frac{1}{4} - x \quad (= \frac{1}{4}(1 - 4x))$$

$$\Rightarrow xc(x) - \frac{1}{2} = \pm \frac{1}{2}(1 - 4x)^{\frac{1}{2}}$$

$$\sum_{n=0}^{\infty} c_n x^{n+1} = xc(x) = \frac{1}{2}(1 \pm (1 - 4x)^{\frac{1}{2}})$$

$$\stackrel{1.42}{=} \frac{1}{2}(1 \pm \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} (-4x)^n)$$

$$= \frac{1}{2}(1 \pm (1 + \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n))$$

$$c_0 x + c_1 x^2 + \dots = \frac{1}{2}(1 \pm (1 + \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n))$$

Koeffizienten von x^0 ist gleich 0 \implies - als Vorzeichen

$$\begin{aligned}
\text{D.h. } c_0x + c_1x^2 + \dots &= -\frac{1}{2} \left(\sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n \right) \\
c_n &= -\frac{1}{2} \binom{\frac{1}{2}}{n+1} (-4)^{n+1} \\
&= -\frac{1}{2} \cdot \frac{\frac{1}{2} \cdot (\frac{1}{2}-1) \dots (\frac{1}{2}-n)}{(n+1)!} \cdot (-1)^{n+1} \cdot 4^{n+1} \\
&= (-1)^{n+2} \cdot \frac{(\frac{1}{2}-1) \dots (\frac{1}{2}-n)}{(n+1)!} \cdot 4^n \\
&= \frac{(2-1) \cdot (4-1) \dots (2n-1)}{(n+1)! \cdot n!} \cdot 2^n \cdot n! \\
&= \frac{(1 \cdot 3 \dots (2n-1)) (2 \cdot 4 \dots (2n))}{(n+1)! \cdot n! \cdot n!} \\
&= \frac{1}{n+1} \cdot \frac{(2n)!}{n! \cdot n!} \\
&= \frac{1}{n+1} \binom{2n}{n}
\end{aligned}$$

Schema zum Lösen von (allgemeinen) Rekursionsgleichungen

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

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

Berechne $a_n \quad n \geq k$ explizit

- 1) Aufstellen der erzeugenden Funktion

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

- 2) Umformen $\sum_{n=0}^{\infty} a_n x^n$, so daß Anfangswerte und Rekursionsgleichung eingesetzt werden können
- 3) Weiter umformen, bis auf der rechten Seite die noch vorhandene unendliche Summe (und mit allen vorkommenden Folgenglieder 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 der Tabelle in Bemerkung 1.42)
- 6) Ablesen der expliziten Darstellung für die a_n (durch Koeffizientenvergleich)

2 Graphentheorie

2.1 Grundbegriffe der Graphentheorie

Definition 2.1

Ein Graph ist ein Paar $G = (V, E)$, wobei V eine endliche Menge und

$E \subseteq \binom{V}{2} := \{\{x, y\} \mid x, y \in V, x \neq y\}$ ist

Die Elemente von V heißen Ecken (oder Punkte, Knoten; engl.: Vertices)

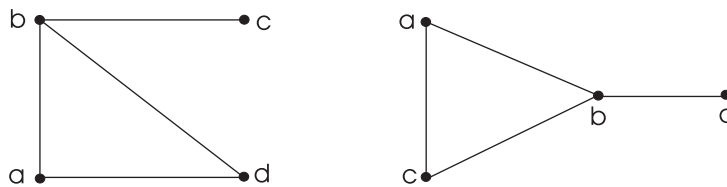
Die Elemente von E heißen Kanten (engl.: Edges)

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

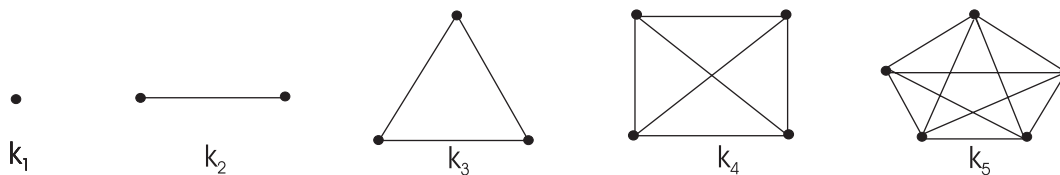
Ein Graph $G = (V, E)$ wird i. a. durch ein Diagramm dargestellt, indem man jede Ecke $x \in V$ durch einen Punkt repräsentiert und zwei Ecken $x, y \in V$ genau dann durch eine Linie verbunden werden, wenn $xy \in E$ ist.

Beispiel 2.2

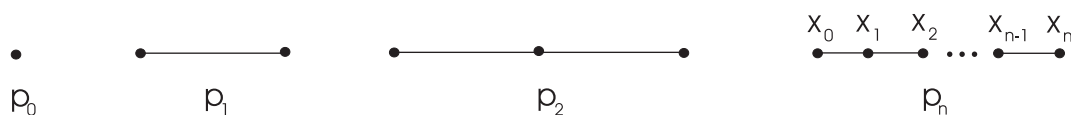
1) $G = (\{a, b, c, d\}, \{ab, bc, ca, bd\})$



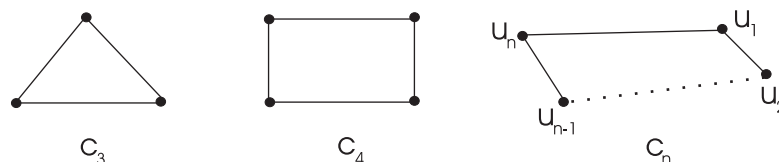
2) Vollständige Graphen $K_n = (V, \binom{V}{2})$ mit $|V| = n$



3) Wege



4) Kreis



$$C_n = U_1 U_2 \dots U_n U_1$$

5) Gittergraphen $M_{m,n}$:

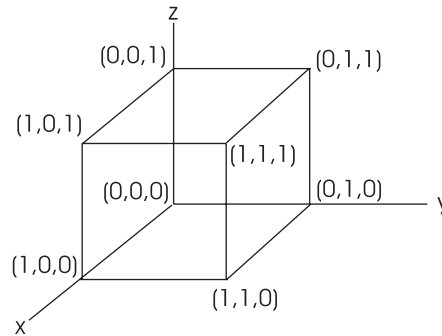


$m \cdot n$ Ecken werden wie in einem Gitter mit m Zeilen und n Spalten verbunden.

6) d-dimensionale Hyperwürfel Q_d

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

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



Bemerkung 2.3

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 Nullgraph

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

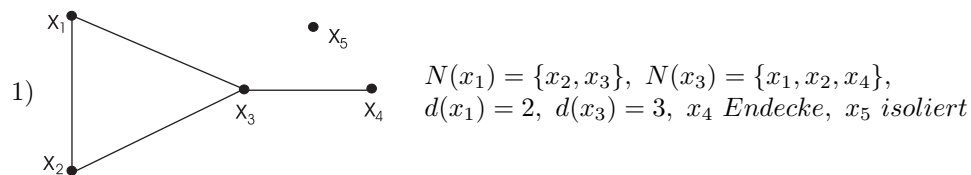
- x und y heißen Endecken von e
- e indiziert mit den Ecken x und y
- x und y sind durch e verbunden
- x und y heißen benachbart oder adjezent

Defintion 2.4

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

- $N(x) = \{y \in V \mid xy \in E\}$ heißt die Nachbarschaft von x in G
- $d_G(x) = |N(x)|$ 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-regulärer Graph*.

Beispiel 2.5



1)

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

$$d(x_1) = 2, \quad d(x_3) = 3, \quad x_4 \text{ *Endecke*, } x_5 \text{ *isoliert*}$$

2) C_n ist 2-regulär

Satz 2.6 (Handschlaglemma, Euler 1736)

$$\text{Sei } G=(V,E), \text{ dann gilt } \sum_{x \in V} d(x) = 2 \cdot |E|$$

Beweis: In $\sum_{x \in V} d(x)$ wird jede Kante \overline{xy} genau zweimal gezählt. Auf der rechten Seite ebenfalls.

Folgerung 2.7

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

Beweis: nach Satz 2.6

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

Lemma 2.8

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

Definiton 2.9

Seien $G=(V,E)$ und $G'=(V',E')$ zwei Graphen. G ist isomorph zu G' ($G \cong G'$)

⇔ ∃ eine bijektive Abbildung $\phi: V \rightarrow V'$ mit $xy \in E \Leftrightarrow \phi(x)\phi(y) \in E'$

Beispiel 2.10

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 numeriert.

2.2 Darstellung von Graphen

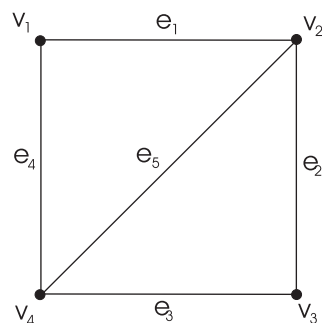
Defintion 2.11

Ist $G=(V,E)$ ein markierter Graph mit $V=\{v_1, \dots, v_n\}$ und $E=\{e_1, \dots, e_m\}$, so gilt:

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

$I=(b_{ij}) \in \{0, 1\}^{n \times m}$ mit $b_{ij} = \begin{cases} 1 & \text{, falls } v_i e_j \text{ inz.} \\ 0 & \text{, sonst} \end{cases}$ heißt die Inzidenzmatrix von G

Beispiel 2.12



$$A_G = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad I_G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$I \cdot I^t = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 3 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & 3 \end{pmatrix} = A + \text{diag} \underbrace{(2, 3, 2, 3)}_{d(v_1), d(v_2), d(v_3), d(v_4)} \quad (\text{Gradfolge von } G)$$

Satz 2.13

Sei $G=(V,E)$ mit $V=\{v_1, v_2, \dots, v_n\}$. Ist A die Adjazenzmatrix und I die Inzidenzmatrix von G , so gilt:

$$I \cdot I^t = A + \text{diag}(d(1), d(2), \dots, d(n))$$

Beweis: Für $i \neq j$:

$$(I \cdot I^t)_{ij} = \sum_{k=1}^m b_{ik} b_{jk} = \begin{cases} 1 & , \text{ falls } v_i v_j \in E \\ 0 & , \text{ sonst} \end{cases} := a_{ij}$$

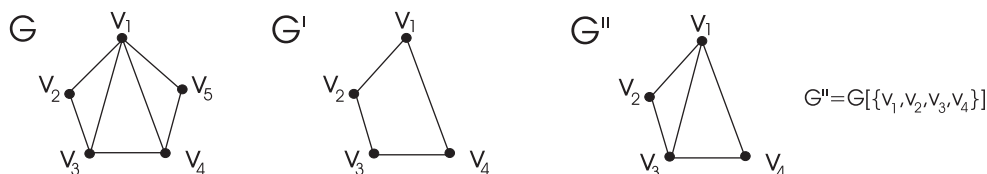
Für $i=j$:

$$(I \cdot I^t)_{ii} = \sum_{k=1}^m b_{ik} b_{ik} = \underbrace{\sum_{k=1}^m b_{ik}}_{i\text{-te Zeile von } I} = d(v_i)$$

Definition 2.14

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: $G' \cap G$
- $G[V'] := (V', E \cap \binom{V'}{2})$ heißt der von V' indizierte Teilgraph
z.B.



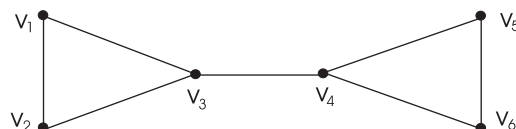
Definition 2.15

- 1) Sei $G=(V,E)$. G heißt zusammenhängend, wenn zwischen je zwei Ecken $x, y \in V$ ein Weg von x nach y existiert.
- 2) In einem nicht zusammenhängenden Graphen heißt jeder maximale (bzgl. Anzahl von Ecken und Kanten) zusammenhängende Teilgraph eine 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 zusammenhängend

- 3) Sie $G=(V,E)$ zusammenhängende. Eine Ecke $x \in V$ heißt Schnittecke falls $G[V \setminus \{x\}]$ nicht mehr zusammenhängend ist.
Eine Kante $k \in E$ heißt Brücke, falls $(V, E \setminus \{k\})$ nicht mehr zusammenhängend ist.
Beispiel



Im Beispiel sind v_3 und v_4 Schnittecken und die Kante v_3v_4 eine Brücke

Satz 2.16

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

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

Beweis: (Induktion über $m = |E|$)

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

- $m \rightarrow m + 1$:

Sie $|E| = m + 1$ 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'_k die Komponenten von G'

$$\begin{aligned} G = G' + e \rightarrow \kappa(G) &= \begin{cases} \kappa(G') & , \text{ falls } e \text{ keine Bücke von } G \text{ ist} \\ \kappa(G') - 1 & , \text{ falls } e \text{ eine Brücke von } G \text{ ist} \end{cases} \\ &\geq \underbrace{(|V| - m)}_{\kappa(G')} - 1 = |V| - (m + 1) \\ &= |V| - |E| \end{aligned}$$

Folgerung 2.17

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

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

Satz 2.18

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

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

so ist G zusammenhängend.

Beweis: (Indirekt)

Annahme: G ist nicht zusammenhängend

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

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

$$m = |E(G_1)| + |E(G_2)| + \dots + |E(G_k)|$$

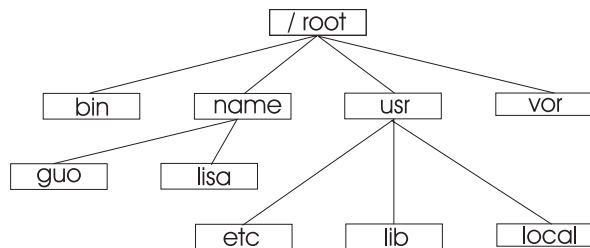
$$\begin{aligned} &\stackrel{2.17}{=} \frac{n_1(n_1-1)}{2} + \frac{n_2(n_2-1)}{2} + \dots + \frac{n_k(n_k-1)}{2} \\ &= \frac{1}{2}((n_1^2 + n_2^2 + \dots + n_k^2) - (n_1 + n_2 + \dots + n_k)) \\ &= \frac{1}{2}((n_1 + \dots + n_k)^2 - 2 \sum_{1 \leq i < j \leq k} (n_i n_j - n)) \\ &\leq \frac{1}{2}(n^2 - 2n_1 \underbrace{(n_2 + n_3 + \dots + n_k)}_{=n-n_1} - n) \\ &\leq \frac{1}{2}(n^2 - 2(n-1) - n) \\ &= \frac{1}{2}(n^2 - 3n + 2) \\ &= \frac{1}{2}(n-1)(n-2) \end{aligned}$$

Widerspruch zur Annahme, d.h. G ist zusammenhängend

Satz 2.19

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

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

2.3 Bäume**Definition 2.20**

Ein Baum ist ein zusammenhängender Graph ohne Kreise.

Ein Graph, dessen Komponenten Bäume sind, heißt Wald.

Lemma 2.21

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 Endecken und besitzen den Grad 1. Ansonsten wären Kreise vorhanden und T kein Baum.

Satz 2.22

Sei $G=(V,E)$ ein Graph mit $|V| = n$. Die folgenden Aussagen sind äquivalent

- 1) G ist ein Baum
- 2) G ist zusammenhängend und kreisfrei
- 3) G ist zusammenhängend und $|E| = n - 1$
- 4) G ist kreisfrei und $|E| = n - 1$
- 5) Zwischen je zwei Ecken u und $v \in V$ 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 minimal zusammenhängend
(d.h. G ist zusammenhängend und jede Kante von G ist eine Brücke)

Beweis: 2) \Rightarrow 1) \Rightarrow 3) \Rightarrow 4) \Rightarrow 5) \Rightarrow 6) \Rightarrow 7) \Rightarrow 2)

Wir zeigen nur 1) \Rightarrow 3)

(Induktion über $n = |V|$)

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

$n \rightarrow n + 1$:

Lemma 2.21 $\Rightarrow G$ enthält eine Edecke $x \in V$.

Dann ist der Graph $G - x := G[V \setminus \{x\}]$ ein Baum mit n Ecken, also $|E(G - x)| = n - 1$

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

Defintion 2.23

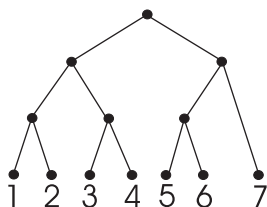
Ein Wurzelbaum $T=(V,E)$ ist ein Baum, in dem eine Ecke $v \in V$ als Wurzel ausgezeichnet wird. Es sei x ein Ecke im Wurzelbaum T mit Wurzel w .

- Jede Ecke y auf dem eindeutig bestimmten Weg von w nach x heißt Vorgänger von x
- Sei y ein Vorgänger von x mit $x \neq y$, so heißt x Nachfolger von y
- Sind $xy \in E(T)$, so heißen sie unmittelbarer Nachfolger bzw. Vorgänger
- Ein geordneter Baum ist ein Wurzelbaum, in dem für die unmittelbaren Nachfolger jeder Ecke eine Ordnung festgelegt ist

Defintion 2.24

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

Ein Wurzelbaum T der Tiefe t heißt balanciert, wenn jede Edecke von t auf Niveau t oder $t-1$ ist. Z.B. ein Fussballturnier mit 7 Mannschaften



Definition 2.25

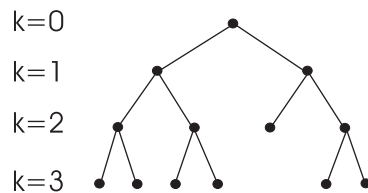
Es sei $T=(V,E)$ ein Wurzelbaum mit Wurzel $w \in V$.

- T heißt binärer Baum, wenn jede Ecke höchstens zwei unmittelbare Nachfolger hat.
- T heißt vollständiger binärer Baum, wenn jede Ecke zwei unmittelbare Nachfolge hat oder keinen.

Satz 2.26

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 $0 \leq k \leq t$. Es gilt: $\sum_{k=0}^t P_k = n$

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

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

Folgerung 2.27

Sei $T=(V,E)$ ein binärer Baum mit der Tiefe t und $|V|=n$. Dann gilt $t \geq \lceil \log_2(\frac{n+1}{2}) \rceil$

Beweis: Übung

Definition 2.28

Ein Teilgraph T eines zusammenhängenden Graphen G heißt Gerüst von G, wenn T ein Baum mit $V(T)=V(E)$ ist.



Satz 2.29

Jeder zusammengehörige 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

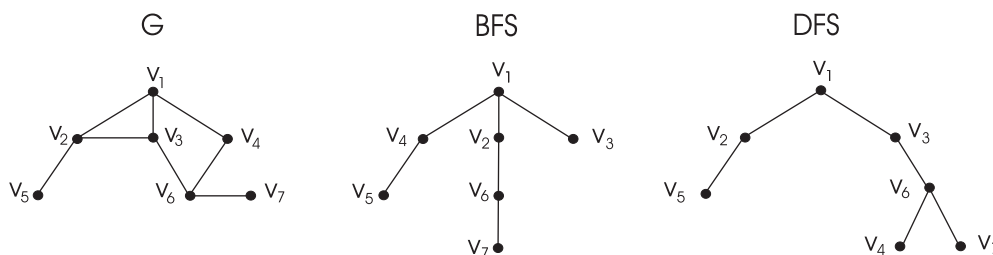
$C=v_0v_1v_2...v_nv_0$ und nehme eine beliebige Kante von C raus.

Z.B. $G'=(V,E\setminus\{v_0v_1\})$ ist 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)

Beide haben den Aufwand $O(|V| + |E|)$.



Adjenzliste

- 1 : 2,3,4
- 2 : 1,3,5
- 3 : 1,2
- 4 : 1,6
- 5 : 2
- 6 : 3,4,7
- 7 : 6

Vor- und Nachteile (Adjenzmatrix vs. Adjenzliste)

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

$f(x)=\Theta(g(n))=f(n)$ wächst genauso schnell wie $g(n)$

Satz 2.30 (Cayley's Tree Formular)

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

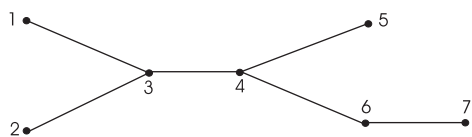
Beweis:

Baum T auf $V = \{1, 2, \dots, n\} \xleftrightarrow{\text{bijektiv}} P(T) = (t_1, t_2, \dots, t_{n-2}) \in V^{n-2}$, Prüfcode von T

Algorithmus \rightarrow

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

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



$i \leftarrow 1$

while $|V| > 2$ do begin

 bestimme die Ecken V im Baum T mit der kleinsten Markierung

$t_i \leftarrow$ Nachbar von V im Baum T

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

$i \leftarrow i + 1$

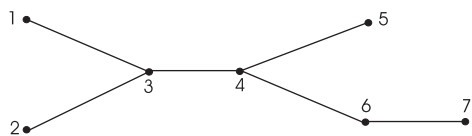
end

Algorithmus \leftarrow

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

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

z.B. $(3, 3, 4, 4, 6)$



$S \leftarrow \emptyset$

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 $e_{n-1} := \{1, 2, \dots, n\} \setminus S t_{n-2}$ in den Graphen ein.

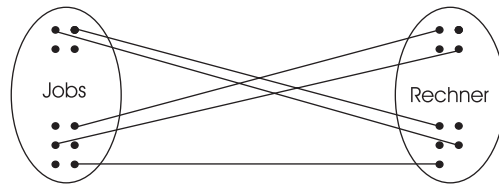
\implies Behauptung

2.4 Matchings in Graphen

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

Gesucht: eine Verteilung von den Jobs auf die Rechner, so daß möglichst viele Jobs gleichzeitig bearbeitet werden können.

In der Graphentheorie können wir das obige Problem wie folgt formulieren:



$J_l R_k \in E(G) \leftrightarrow R_k$ erfüllt die Leistungsanforderung von Job J_l

Gesucht ist dann die Kantenmenge $M \subseteq E(G)$, so daß keine zwei Kanten aus M einen gemeinsame Endecke haben.

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

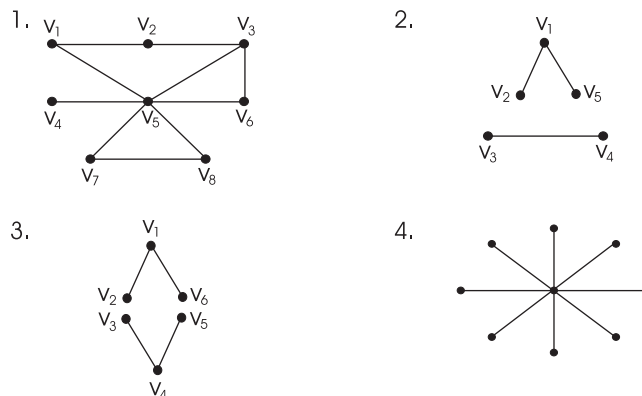
Definition 2.31

Sei $G=(V,E)$ ein Graph. Eine Kantenmenge $M \subseteq E(G)$ heißt Matching von G , wenn

$V(K_1) \cap V(K_2) = \emptyset \quad \forall K_1, K_2 \in M$ und $K_1 \neq K_2$

- Ein Matching M von G heißt maximal, wenn es in G kein Matching M' gibt mit $M \subsetneq M'$
- Ein Matching M heißt Maximum-Matching, wenn es in G kein Matching M'' gibt mit $|M| < |M''|$
- Ein Matching heißt perfekt, wenn $V(M) = V(G)$

Beispiele 2.32



Bemerkung 2.33

Für jeden Graphen $G=(V,E)$ gilt: 1) Jedes perfektes Matching ist ein Maximum-Matching

2) Für jedes Matching M ist $|V(M)| = 2|M|$

3) Für ein perfektes Matching M von G gilt $2|M| = |V(G)|$

4) G hat ein perfektes Matching $\implies |V(G)|$ ist gerade

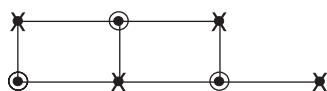
Bemerkung 2.34

Ein Graph $G=(V,E)$ heißt bipartit, wenn man $V(G)$ in zwei disjunkte Mengen A und B zerlegen kann, so daß $G[A]$ und $G[B]$ Nullgraphen (ohne Kanten) sind.

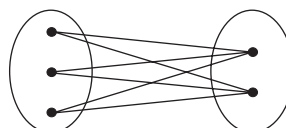
- A, B heißen Partitions Mengen
- vollständig bipartiter Graph $K_{p,q}$: Ein bipartiter Graph $(A \uplus B, E)$ mit $|A| = p$ und $|B| = q$ und $xy \in E$ für alle $x \in A$ und $y \in B$

Beispiele 2.35

1.



2.

**Satz 2.36**

Ein Graph G ist bipartit $\iff G$ hat keine Kreise ungerader Länge.

Satz 2.37 (König-Hall)

Sei $G=(A \uplus B, E)$ ein bipartiter Graph. G besitzt ein Matching M mit $|M| = |A| \iff |N(S)| \geq |S|$ für alle $S \subseteq A$

Beweis:

 \implies trivial \impliedby (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 $U(a) := \{x \in V(G) \mid \text{mid } x \text{ ist durch einen } M\text{-alternierenden Weg mit } a \text{ verbunden}\}$ M ist ein Maximum-Matching $\implies U(a) \subseteq V(M)$ Setze $A'=(U(a) \cap A) \cup \{a\}$ und $B'=(U(a) \cap B)$ Dann gilt $B'=N(A')$ und $|B'|=|A'|-1 \rightarrow |A'|=|B'|+1=|N(A')|+1>|N(A')| \rightarrow$ Widerspruch**Folgerung 2.38** (König, 1916)

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

Beweis:

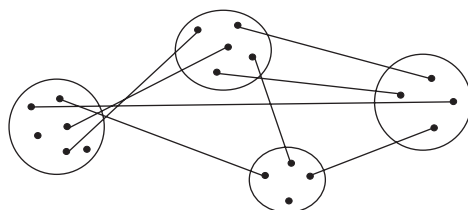
1. $|A|=|B|$ 2. $|N(S)| \geq |S| \forall S \subseteq A$ 3. (1.+2.) + Satz 2.37 \rightarrow Behauptung**Folgerung 2.39** (König, 1916)

Ein r -regulärer bipartiter Graph läßt sich in r kantendisjunkte perfekte Matchings zerlegen.

Beweisidee: sukzessives Anwenden von Folgerung 2.38

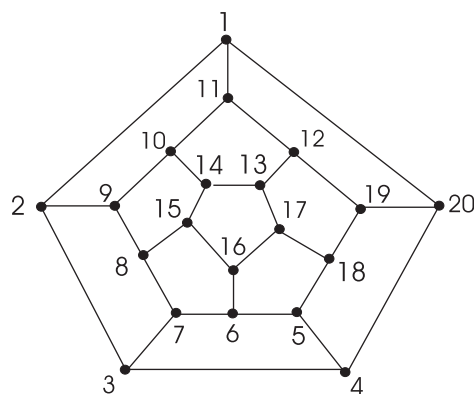
Definition 2.40 (multipartite Graphen)

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.



2.5 Hamilton-Graphen

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



Definition 2.41

Sei $G=(V,E)$.

Ein Kreis C in G heißt Hamilton-Kreis, falls $V(C)=V(G)$.

Ein Weg W in G heißt Hamilton-Weg, falls $V(W)=V(G)$.

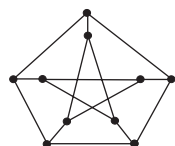
Enthält G einen Hamilton-Kreis, so heißt G hamiltonscher Graph.

Enthält G einen Hamilton-Weg, so heißt G semi-hamiltonscher Graph.

Beispiel 2.42

1. K_n , $n \geq 3$ ist hamiltonsch.
2. D_{20} ist hamiltonsch (Skizze siehe oben).

3. Petersen-Graph ist nicht hamiltonsch, aber semi-hamiltonsch.



Satz 2.43 (notwendige Bedingung)

Ist G ein Hamilton-Graph, so gilt für jede nicht leere Eckenmenge $S \subseteq V(G)$:

$\kappa(G-S) \leq |S|$ (Anmerkung: κ =Anz. der Komponenten)

Beweis: trivial

Satz 2.44 (Ora, 1960)

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:

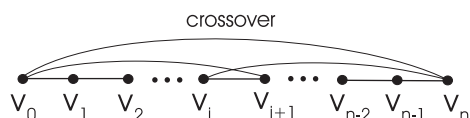
G ist hamiltonsch $\iff G+uv$ ist hamiltonsch.

Beweis: (wichtig)

\implies trivial

\impliedby indirekt:

Ann.: $G+uv$ hamiltonsch, aber G nicht, dann enthält jeder Hamiltonkreis von $G+uv$ die Kante uv .



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

$\implies S \cap T = \emptyset$ (sonst 'crossover') und $|S \cup T| \leq n-1 < n$

$d(u)+d(v) = |S|+|T| - |S \cap T| + |S \cap T| < n \implies$ Widerspruch

Folgerung 2.45 (Ore, 1960)

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

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

Beweisidee: Kanten hinzufügen $\implies K_n$

Folgerung 2.46 (Dirac, 1952)

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

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

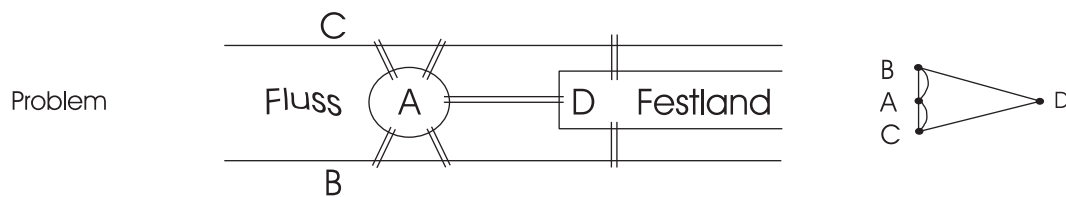
Bemerkung 2.47

1. Anwendung: Das Problem eines Handlungsreisenden (TSP=Travelling Salesman Problem)

2. Das Entscheidungsproblem, enthält G einen Hamiltonkreis?

Das Problem ist NP-vollständig (siehe theoretische Informatik)

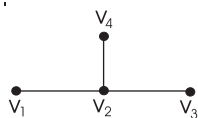
2.6 Eulersche Graphen



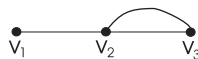
Definition 2.48

- Sei $G=(V,E)$ ein zusammenhängender Graph $x_0x_1\dots x_k$ mit $x_i \in V$ und mit $x_ix_{i+1} \in E(G)$ heißt eine Kantenfolge der Länge k .
- Eine Kantenfolge mit paarweise verschiedenen Kanten heißt Kantenzug, z.B.

1.



2.



1. $v_1v_2v_3v_2v_4$ Kantenfolge aber kein Kantenzug
2. $v_1v_2v_4v_2$ Kantenzug

Nur in diesem Abschnitt werden wir auch die Multigraphen studieren.

- Ein Kantenzug Z mit $E(Z)=E(G)$ heißt eulerscher Kantenzug.
- Ein geschlossener eulerscher Kantenzug heißt Eulertour.

Definition 2.49

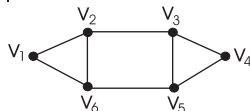
Sei $G=(V,E)$ zusammenhängend mit $|V| \geq 2$.

G heißt semi-eulersch, falls G einen eulerschen Kantenzug enthält.

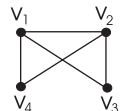
G heißt eulersch, falls G eine Eulertour enthält.

Beispiel 2.50

1.



2.



1. $G_1 : v_1v_2v_3v_4v_5v_6v_2v_5v_3v_6v_1$
 2. $G_2 : v_1v_2v_3v_1v_4v_2$
- G_1 ist eulersch, G_2 ist semi-eulersch

Satz 2.51 (Euler 1736)

Sei $G=(V,E)$ zusammenhängend und $|V| \geq 2$. Dann gilt:

G ist eulersch \iff der Grad jeder Ecke ist gerade

Beweis:

\implies trivial

\impliedby Sei $z=x_0x_1\dots x_t$ ein längster Kantenzug in G . Dann haben wir:

1. $x_t = x_0$
2. z ist eine Eulertour von G

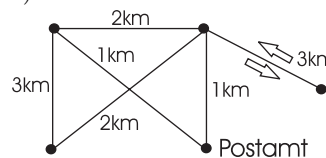
Folgerung 2.52

Ein zusammenhängender Graph $G=(V,E)$ mit $|V| \geq 2$ ist semi-eulersch \iff

G besitzt 2 oder keine Ecke ungeraden Grades

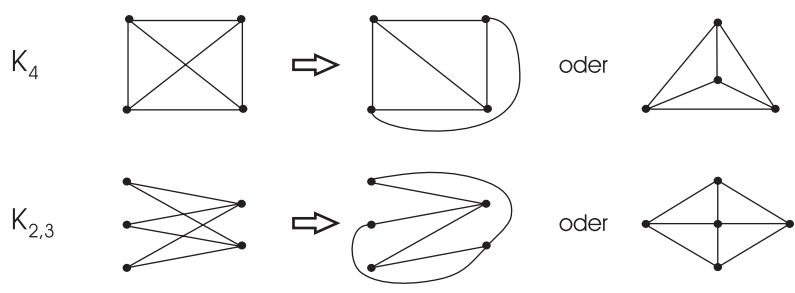
Bemerkung 2.53

- Für eulersche Graphen gibt es einen effizienten Algorithmus (Fleury's Algorithmus mit $O(|E(G)|)$, eine Eulertour zu konstruieren.
- 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 dann 'bewerteter Graph')
 Gesucht wird eine geschlossene Kantenfolge Z von minimaler Gesamtlänge mit $E(Z)=E(G)$, z.B.



2.7 Planare Graphen

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

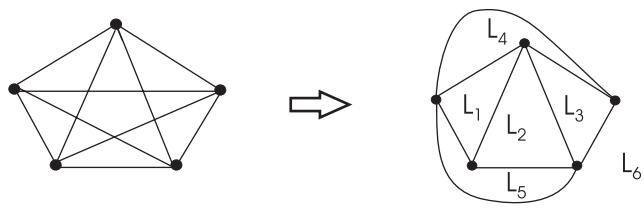


Definition 2.54

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

- G heißt einbettbar in den \mathbb{R}^2 : wenn ein Paar φ, φ' gibt, so daß gilt:
 $\varphi: V \rightarrow \mathbb{R}^2$ injektiv
 $\varphi': E \rightarrow J = \{\text{bild}(e) \mid e:[0,1] \rightarrow \mathbb{R}^2 \text{ stetig und injektiv}\}$; $\text{bild}(e) = \text{Jordankurve}$
 mit $\varphi'(uv) = \text{bild}(e)$, $e=uv \in E(G)$
 und $\varphi(u) = e(0)$
 $\varphi(v) = e(1)$
 und $\varphi'(e_1) \cap \varphi'(e_2) = v(e_1) \cap v(e_2)$, $e_1, e_2 \in E(G)$
- G heißt planar, wenn G in \mathbb{R}^2 einbettbar ist.
- Ein ebener Graph (oder eine Landkarte) ist eine Einbettung in \mathbb{R}^2 eines planaren Graphen (in Zeichen: (G, φ, φ'))
- Ist (G, φ, φ') ein ebener Graph, so heißen die Zusammenhangskomponenten von $\mathbb{R}^2 \setminus \cup_{e \in E} \varphi'(e)$ die Gebiete (oder Länder) von (G, φ, φ')

z.B.



$$l(G) = \text{Anzahl der Länder von } G$$

$$l = 6, \quad |v| = 5, \quad |E| = 9$$

Satz 2.55 (Eulersche Polyederformel, 1752)

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

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

Beweis: (Induktion über $m = |E| \geq |V| - 1$) (Folgerung 2.17)

$m = |V| - 1$: G ist ein Baum
 $1 = (|V| - 1) - |V| + 2$

$m \rightarrow m+1$: G zusammenhängend, $|E(G)| = m + 1 \geq |V|$
Satz 2.22 G enthält mindestens einen Kreis c
 Sei nun $e \in E(c)$ beliebig. Dann gilt:
 $|E(G - e)| = m$ und
 $l(G - e) = m - |V| + 2$
 Durch die Entfernung von e verschmelzen die beiden Länder auf den
 zwei Seiten von e zu einem.
 $\Rightarrow l(G - e) = m - |V| + 2$
 $l(G) = |E(G)| - |V| + 2$

Bemerkung:

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

Satz 2.56

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

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

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 zwei Länder.

$$\Rightarrow 3|L| \leq 2|E| \stackrel{\text{Satz 2.55}}{=} \frac{2}{3}|E| \geq l(G) = |E| - |V| + 2$$

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

Beispiel 2.57

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

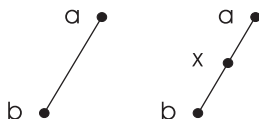
2) $K_{3,3}$ ist nicht planar, denn $K_{3,3}$ ist c_3 -frei und für c_3 -freie planare Graphen $G=(V,E)$ mit $|V| \geq 3$ gilt: $|E| \leq 2|V| - 4$

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

Definition 2.58

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

Wir sagen e wird unterteilt, wenn wir zu H eine neue Ecke x hinzufügen und die Kante e durch zwei neue Kanten ax und xb ersetzen.



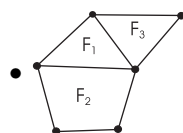
Ein Graph H heißt Unterteilungsgraph von G , wenn man H aus G durch sukzessives Unterteilen von Kanten gewinnt.

Satz 2.59

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

Definition 2.60 (Vierfarbenproblem)

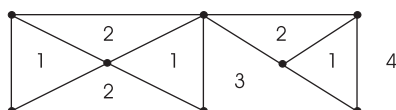
Sei G ein Landkarte



Zwei verschiedene Länder F_1 und F_2 heißen benachbart, wenn es eine Kante gibt, die sowohl zum Rand von F_1 und 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 eine p -Färbung von G , wenn $h(F_1) \neq h(F_2)$ für zwei verschiedene benachbarte Länder F_1 und F_2 .
 Man sagt auch, daß sich die Landkarte G mit p Farben färben läßt.

Beispiel 2.61



Satz 2.62 (Vierfarbenvermutung, Guthrie 1852)

Jede Landkarte läßt sich mit vier Farben färben

Beweis: (N. Robertson et al. 1997)

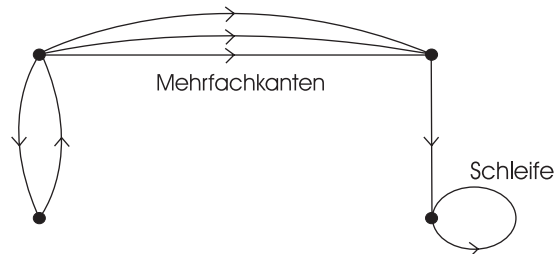
Bemerkung 2.63

- 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 $\mathbb{R}^2 S^n$)
- 2) Das Problem der Kantenfärbung
- 3) Das Problem der Eckenfärbung

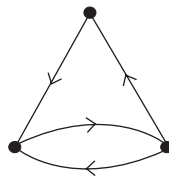
2.8 Digraphen

Definition 2.64

Ein Digraph D besteht aus einer endlichen und nicht-leeren Eckenmenge V (engl. vertex set) und einer Bogenmenge $A \subseteq V \times V$ (engl. arcs) von geordneten Eckenpaaren, in Zeichen $D=(V,A)$



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

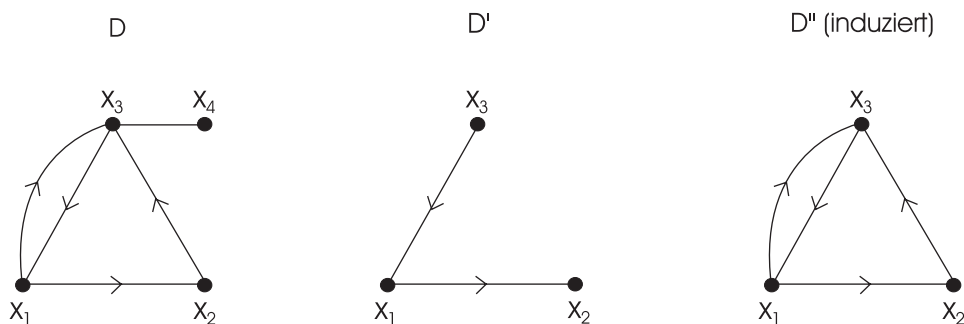


Definition 2.65

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

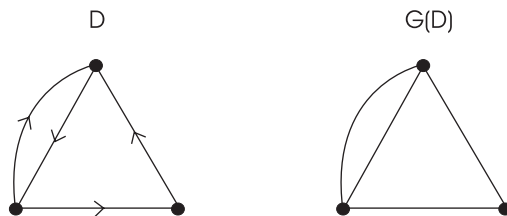
- $D' = (V', A')$ heißt Teildigraph von D , wenn $V' \subseteq V$ und $A' \subseteq A \cap (V' \times V')$ sind, in Zeichen $D' \subseteq D$
- Ein Teildigraph $D' = (V', A')$ heißt ein von V' induzierter Teildigraph, wenn $A' = A \cap (V' \times V')$, in Zeichen $D' = D[V']$

z.B.



- Orientierte Kantenfolge der Länge p in D
 $F := x_0x_1x_2 \dots x_p \quad x_i \in V(D), \quad i=0, 1, \dots, p$
 $x_ix_{i+1} \in A(D), \quad i=0, 1, \dots, p-1$
 z.B. in D ist $x_3x_1x_2x_3x_1x_3$ eine orientierte Kantenfolge
- orientierter Kantenzug := orientierter Kantenfolge mit paarweise verschiedenen Bögen
 z.B. $x_3x_1x_3x_4$
- orientierter Weg := orientierte Kantenfolge mit paarweise verschiedenen Ecken
 z.B. $x_3x_1x_2$
- Geschlossener Kantenfolge := ...

- Geschlossener Kantenzug := ...
- Geschlossener Kreis der Länge q := Eine geschlossene Kantenfolge der Länge q mit genau q Ecken
- Geschlossener Kantenfolge := ...
z.B. $x_1x_2x_3x_1$ 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 D 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:
 $N^+(x) = \{y \mid xy \in A(D)\}$
 $N^-(x) = \{w \mid wx \in A(D)\}$
 $d^+ = |N^+(x)|, \quad \delta^+(D) = \min\{d^+ \mid x \in V(D)\}$
 $\Delta^+(D) = \max\{d^+ \mid x \in V(D)\}$
 $d^- = |N^-(x)|, \quad \delta^-(D) = \min\{d^- \mid x \in V(D)\}$
 $\Delta^-(D) = \max\{d^- \mid x \in V(D)\}$
- Der untergeordnete Graph von D (in Zeichen $G(D)$) ist $G(D) = (V(D), \{xy \mid xy \in A(D)\})$

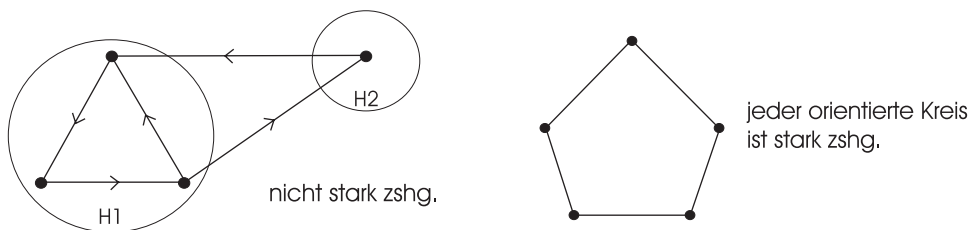


Definition 2.66

Sei G ein Digraph

Eine stark zusammenhängende Komponente H von D ist ein maximaler Teilgraph von D , so daß H für zwei beliebige Ecken $u, v \in V(H)$ einen orientierten Weg $\text{vin } u$ nach v enthält.

D heißt stark zusammenhängend wenn D nur eine stark zusammenhängende Komponente hat z.B.



Definition 2.67

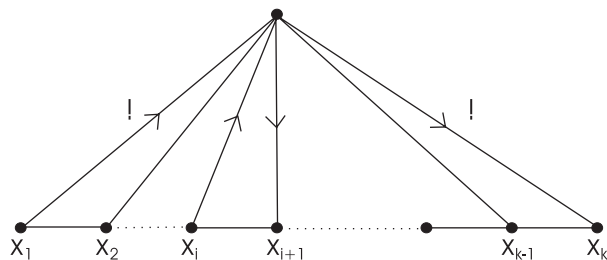
Ein Digraph heißt Turnier wenn zwischen je zwei Ecken genau ein Bogen existiert. Ein Turnier mit n Ecken heißt n -Turnier in Zeichen T_n

Satz 2.68

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 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 $x_1x_2 \dots x_ix_{i+1} \dots x_k$ ein orientierter Weg in D mit der Länge k (\Rightarrow Widerspruch!)

Satz 2.69 (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: (vollständige Induktion über p)

Bemerkung 2.70

$D=(V,A) \longleftrightarrow$ Relation A auf der Menge V

3 Algebraische Strukturen

3.1 universelle Algebren

Definition 3.1

Ist M eine Menge, so heißt eine Abbildung $f: M^n = M \times M \times \dots \times M \rightarrow M$ eine n -stellige Operation oder ein n -stelliger Operator.

- $n=s(f)$ heißt die Stelligkeit vom Operator f
- ein zweistelliger Operator heißt auch Verknüpfung (engl.: binary operation)

Definition 3.2

Eine universelle Algebra vom Typ $(h_i)_{i \in I}$ ist $(M, (f_i)_{i \in I})$, wobei f_i eine n_i -stellige Operation auf M ist, d.h. $n_i = s(f_i)$. I ist eine Indexmenge (kann unendlich sein), die Liste $(M_i)_{i \in I}$ heißt Signatur der Algebra.

Beispiel 3.3

1. Die boolesche Algebra $(\{T, F\}, \vee, \wedge, \neg)$ hat die Signatur $(2,2,1)$
2. Mit den arithmetischen Operationen $+$ und \cdot können wir unterschiedliche Algebren definieren:
 - $(\mathbb{N}, +), (\mathbb{N}, +, \cdot)$
 - (\mathbb{Z}, \cdot)
 - $(x \in \mathbb{N}, x \text{ ist Quadratwurzel}, \cdot)$
denn für $x=a^2$ und $y=b^2$ ist $xy=a^2b^2 = (ab)^2$
 - $(x \in \mathbb{N}, x \text{ ist Quadratwurzel}, +)$
ist keine Algebra
3. Σ =Menge (Alphabet)
 $\Sigma^* = \{a_1, a_2, \dots, a_n \mid a_i \in \Sigma, n \in \mathbb{N}_0\}$
 $\circ: \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ mit $(a_1, \dots, a_n) \circ (b_1, \dots, b_m) = (a_1 \dots a_n b_1 \dots b_m)$
 Σ^*, \circ ist eine Algebra
4. U = beliebige Menge
 $F(U) = \{f \mid f: U \rightarrow U\}$
 \circ : Komposition von zwei Funktionen $(f \circ g)(x) = f(g(x)) \forall x \in U$
 $(F(U), \circ)$ ist eine Algebra

Definition 3.4 (neutrales Element)

Sei (M, \circ) eine Algebra mit einem zweistelligen 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 $e \in M$ 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 links- als auch rechtsneutrales Element ist.

Beispiel 3.5

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

\circ	b	c
b	b	b
c	c	c

 $\Rightarrow b$ und c sind rechtsneutrale Elemente $\Rightarrow (\{b, c\}, \circ)$ besitzt kein n.E.

Lemma 3.6

Sei (M, \circ) eine Algebra vom Typ (2). Dann gilt:

Ist c ein linksneutrales Element und d ein rechtsneutrales Element, so ist $c=d$.

Beweis: 1. $c \cdot d = d$ und 2. $c \cdot d = c$

Eindeutigkeit des neutralen Elementes:

Annahme: e_1 und e_2 sind neutrale Elemente: $e_1 = e_1 \cdot e_2 = e_2$

Beispiel 3.7

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

Definition 3.8 (inverses Element)

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

Ein Element $x \in M$ heißt linksinverses Element von $a \in M$, falls $x \cdot a = e$

Ein Element $x \in M$ heißt rechtsinverses Element von $a \in M$, falls $a \cdot x = e$

Ein Element $x \in M$ heißt inverses Element (oder Inverse) von $a \in M$, falls x sowohl ein linksinverses als auch rechtsinverses Element ist.

Definition 3.9 (Halbgruppe)

Eine Algebra $A=(M, \circ)$ vom Typ (2) heißt Halbgruppe, falls der Operator \circ assoziativ ist, also $a \circ (b \circ c) = (a \circ b) \circ c \forall a, b, c \in M$

Definition 3.10 (Monoid)

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

M1 : A ist assoziativ

M2 : \exists ein neutrales Element $e \in M$

Definition 3.11 (Gruppe)

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

G1 : A ist assoziativ

G2 : \exists ein neutrales Element $e \in M$

G3 : jedes Element $a \in M$ besitzt ein Inverses

Definition 3.12 (abelsche Algebra)

Eine Halbgruppe (ein Monoid, eine Gruppe) $A=(M, \circ)$ heißt abelsch, falls \circ kommutativ ist.

Definition 3.13 (Ring)

Eine Algebra $A=(M, \oplus, \odot)$ mit zwei zweistelligen Operatoren \oplus und \odot heißt ein Ring, falls

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

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \text{ und}$$

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

Definition 3.14 (Körper)

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

K1 : (M, \oplus) ist eine abelsche Gruppe

K2 : (M, \odot) ist eine abelsche Gruppe

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

Definition 3.15 (boolesche Algebra)

Eine Algebra $A=(M, \oplus, \odot, \neg)$ vom Typ (2,2,1) heißt boolesche Algebra, falls

B1 : (M, \oplus) ist ein abelscher Monoid

B2 : (M, \odot) ist ein abelscher Monoid

B3 : für den Operator \neg gilt : $a \oplus (\neg a) = 1$ und $a \odot (\neg a) = 0 \forall a \in M$

B4 : die Distributivgesetze gelten

Beispiel 3.16

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

2) Sei K ein Körper, dann:

- $K[x] = \left\{ \sum_{k=0}^n a_k x^k \mid a_k \in K \right\}$ (Menge der Polynome über K)

ist ein kommutativer Ring (Polynomring)

- $K[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in K \right\}$ ist ein kommutativer Ring

mit Null $0=0x^0$ und Eins $1=1x^0$

- $K^{n \times n} = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{nn} \end{pmatrix} \mid a_{ij} \in K, 1 \leq i, j \leq n \right\}$

mit $n > 1$ ist ein nichtkommutativer Ring

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

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

Der kleinste Körper: $F_2 = \{0, 1\}$

Konvention Sei $\{K, \oplus, \odot\}$ ein Körper.

- $0 \in K$ (Null) neutrales Element bzgl. \oplus
- $1 \in K$ (Eins) neutrales Element bzgl. \odot
- $-a \in K$ Inverse zu $a \in K$ bzgl. \oplus
- $a^{-1} \in K$ Inverse zu a bzgl. \odot

3.2 Unter algebra, Homomorphismus, Konvergenz

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

Definition 3.17

$U \subseteq A$ heißt Unter algebra von A (in Zeichen $U \leq A$), falls die Operatoren f_i abgeschlossen sind, d.h.:

$$f_i(U^{n_i}) \subseteq U \quad \forall i \in I$$

$$f_i(U^{n_i}) = \{f_i(u_1, \dots, u_n) \mid u_1, \dots, u_n \in U\}$$

Definition 3.18

- Sei $G = (G, \cdot)$ eine Gruppe.

Eine Unter algebra $U \leq G$ heißt Untergruppe von G , falls (U, \cdot) eine Gruppe ist.

(d.h.: $\forall u, u' \in U$ gilt $uu' \in U$, $u^{-1} \in U$ und $1 \in U$)

- Sei $R = (R, \oplus, \odot)$ ein Ring.

Eine Unter algebra $U \leq R$ heißt Teilring (Unterring) von R , falls (U, \oplus, \odot) ein Ring ist.

Beispiel 3.19

1) $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$

2) Sei $Z_n = \{1, \dots, n-1\}$ und $+_n : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}_n$ mit $+_n(a, b) = a+b \pmod n$

z.B. $n=5 : \mathbb{Z} = \{1, 2, 3, 4, 5\}$, $+_5 : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z}_5$ mit $1+_5 2=3$, $2+_5 3=0$, $3+_5 6=4$

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

Lemma 3.20

Sei I eine Indexmenge und $U_j \leq A$ für $j \in I$.

Dann gilt: $\bigcap_{j \in I} U_j \leq A$

Definition 3.21

Sei M eine Teilung von einer Algebra A.
 $\langle M \rangle = \cap \{U \mid M \subseteq U \leq A\}$
 heißt die von M erzeugte Unteralgebra.

Beispiel 3.22

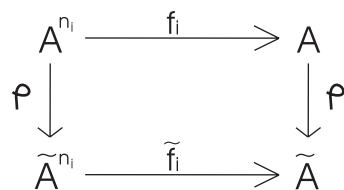
1) Sei $G=(G, \cdot)$ eine Gruppe und sei $g \in G$.
 $\langle \{g\} \rangle = \{g^i \mid i \in \mathbb{Z}\}$ (die von g erzeugte Untergruppe),

$$\text{wobei } g_i = \begin{cases} g \dots g & , \text{ falls } i > 0 \\ 1 & , \text{ falls } i = 0 \\ g^{-1} \dots g^{-1} & , \text{ falls } i < 0 \end{cases}$$

$$\langle \{g_1, \dots, g_n\} \rangle = \{a_1, \dots, a_m\}_{m \in \mathbb{N}^0}, a_j \in \{g_1, \dots, g_n, g_1^{-1}, \dots, g_n^{-1}\}$$

Definition 3.23

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 Homomorphismus von A und \tilde{A} , falls für alle $i \in I$ die Operatoren f_i und \tilde{f}_i mit φ vertauschbar sind,
 also $\tilde{f}_i(\varphi(a_1), \dots, \varphi(a_{n_i})) = \varphi(f_i(a_1, \dots, a_{n_i})) \forall a_j \in A, j = 1, \dots, n, i \in I$



Die Vertauschbarkeit bedeutet, daß man zum gleichen Ergebnis kommt, unabhängig davon , ob man 'oben herum' oder 'unten herum' läuft.

Beispiel 3.24

- 1) Sei $A=(A, (f_i)_{i \in I})$ eine Algebra und $A' \leq A$, dann ist
 $\text{id} : A' \rightarrow A$ mit $a \rightarrow a \forall a \in A'$
 ein Homomorphismus von A' nach A, oder die 'kleinere' Algebra A' ist in der 'größeren' Algebra A eingebettet, z.B.
 $A=(\mathbb{N}, +), \tilde{A}=(\mathbb{Z}, +), A \leq \tilde{A}$
 $\varphi : \mathbb{N} \rightarrow \mathbb{Z}$ mit $n \rightarrow n \forall n \in \mathbb{N}$ ist ein Homomorphismus von A nach \tilde{A}
- 2) $A=(\sum^*, \circ)$ (siehe 3.3), $\tilde{A}=(\mathbb{N}^0, +)$
 $\varphi : \sum^* \rightarrow \mathbb{N}^0$ mit $w \rightarrow |w|$ ist ein Homomorphismus von A und \tilde{A}
- 3) Sei K ein Körper und V,W zwei K-Vektorräume (siehe LA2.25)
 $\varphi : V \rightarrow W$ ist ein Homomorphismus $\Leftrightarrow \varphi$ ist k-linear
 (k-linear: $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ und $\varphi(0) = 0$ und $\varphi(\alpha v) = \alpha \varphi(v)$)

Definition 3.25

- Seien $A=(A, (f_i)_{i \in I})$ und $\tilde{A}=(\tilde{A}, (\tilde{f}_i)_{i \in I})$ Algebren vom gleichen Typ $T=(n_i)_{i \in I}$
 Eine Abbildung $\varphi : A \rightarrow \tilde{A}$ heißt Isomorphismus von A und \tilde{A} , falls
 1. φ ein Homomorphismus von A nach \tilde{A} ist und
 2. φ bijektiv ist.
 Ein bijektiver Homomorphismus heißt dann Isomorphismus.
- $A \cong \tilde{A}$ isomorph $\Leftrightarrow \exists$ ein Isomorphismus von A nach \tilde{A}
- Ein Isomorphismus einer Algebra A nach A heißt Automorphismus

Beispiel 3.26

- 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) $A=(x \in \mathbb{R} \mid x > 0 (= \mathbb{R}^+), \cdot)$, $\tilde{A} = (\mathbb{R}, +)$
 $\varphi : \mathbb{R}^+ \rightarrow \mathbb{R}$ mit $x \rightarrow \log x \forall x \in \mathbb{R}^+$ ist ein Isomorphismus,
 denn für die Logarithmusfunktion gilt: $\log(xy) = \log x + \log y \forall x, y \in \mathbb{R}^+$

\circ	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

- 3) Sei $A=(\{1, 2, 3\}, \circ)$ eine Algebra mit
 $\varphi 1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3$ ist ein Automorphismus

Lemma 3.27

Ein Isomorphismus zwischen zwei Algebren bildet neutrale Elemente auf neutrale Elemente und Inverse auf Inverse ab.

Lemma 3.28

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

Erinnerung an LA (Definition 1.33)
 Sei M eine Menge.



- Relation R auf M ist eine Teilmenge $R \subseteq M \times M$
- Relation R auf M heißt Äquivalenzrelation, falls R reflexiv, symmetrisch und transitiv
- Äquivalenzrelation auf M

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

Beispiel 3.29

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

$\sim_m : a \sim_m b \Leftrightarrow m \mid a-b$ d.h. $a \equiv b$ (modulo m)

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

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

Definition 3.30

Sei $A=(A, (f_i)_{i \in I})$ eine Algebra. Eine Äquivalenzrelation \sim auf A heißt eine Kongruenzrelation auf A , wenn \sim mit allen f_i verträglich ist, d.h.

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

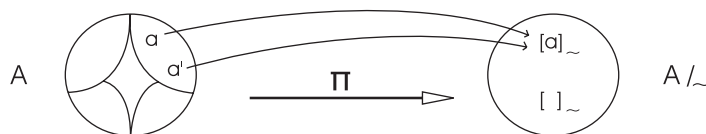
Beispiel 3.31

Sei $G=(G, \cdot)$ eine Gruppe und sei \sim eine Äquivalenzrelation auf G .
 \sim Kongruenz $\Leftrightarrow a \sim a', b \sim b' \rightarrow a \cdot b \sim a' \cdot b'$ mit $a^{-1} \sim (a')^{-1}$

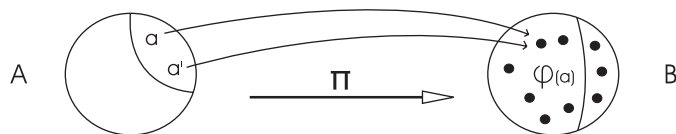
Satz 3.32

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 $\tilde{f}([a_1]_{\sim}, [a_2]_{\sim}, \dots, [a_{n_i}]_{\sim}) := [f_i(a_1 \dots a_{n_i})]_{\sim}$ und
 $\pi_{\sim} : A \rightarrow A/\sim$ mit $a \rightarrow [a]_{\sim}$ ist ein surjektiver Homomorphismus (Epimorphismus)



- b) Ist $\varphi : A \rightarrow B$ ein Homomorphismus, so wird dann $a \sim a' \Leftrightarrow \varphi(a) = \varphi(a')$
 eine Kongruenzrelation auf A definiert
 und $\varphi(A)$ ist eine Unteralgebra von B
 und es gibt einen Isomorphismus $\tilde{\varphi} : A/\sim \rightarrow \varphi(A)$, $[a]_{\sim} \rightarrow \varphi(a)$
 Beweis: (Nachrechnen)



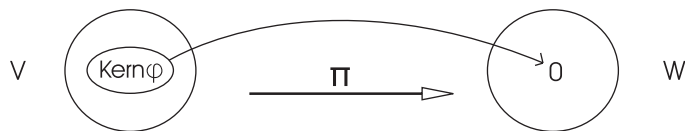
Beispiel 3.33

Sei K ein Körper und seien V, W zwei K -Vektorräume.

$\varphi : V \rightarrow W$ ist ein Homomorphismus $\forall v, v' \in V$

$$\begin{aligned} v \sim v' &\Leftrightarrow \varphi(v) = \varphi(v') \\ &\Leftrightarrow \varphi(v) - \varphi(v') = 0 \\ &\Leftrightarrow \varphi(v - v') = 0 \text{ (da } \varphi \text{ k-linear)} \\ &\Leftrightarrow v - v' \in \text{Kern } \varphi \leq V \end{aligned}$$

also, $[v]_{\sim} = v + \text{Kern } \varphi \quad \forall v \in V$
 $[0]_{\sim} = \text{Kern } \varphi$



3.3 Ringe und Ideale

Erinnerung an Definition 3.13

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

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

Lemma 3.34

- 1) $a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in R$
- 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 den Teilring $[0]_{\sim} := \{a \in R \mid a \sim 0\}$

- $a \sim a' \Leftrightarrow \underbrace{a + (-a')}_{a-a'} \sim \underbrace{a' + (-a')}_{a'-a'=0}$
 $\Leftrightarrow a - a' \in [0]_{\sim}$

Also, \sim ist vollständig beschrieben durch $[0]_{\sim}$

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

Definition 3.35

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

$I \subseteq R$ heißt Ideal (in Zeichen $I \trianglelefteq R$),

wenn $0 \in I$

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

Satz 3.36

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 $[0]_{\sim} = I, [a]_{\sim} = a + I$)

Schreibweise: $R/I := R/\sim$

Beweis: (Übung)

Satz 3.37

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
(Rd heißt das von d erzeugte Hauptideal)
- 2) $Rd = R \Leftrightarrow d$ ist invertierbar in (R, \cdot) d.h. $\exists d' : dd' = 1$

Beweis: (Übung)

Beispiel 3.38 (vgl. Beispiel 3.29)

$R=(\mathbb{Z},+,\cdot)$ 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 $\underbrace{a + a + \dots + a}_{k\text{-mal}} = k \cdot a$

Beispiel 3.39

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 $a, b \in \mathbb{Z}$

Betrachte: $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_8, z \rightarrow [z]_8$ (φ Homomorphismus)

$$\Rightarrow \varphi(z) = \varphi(a^2) + \varphi(b^2) + \varphi(c^2) = \varphi(a)^2 + \varphi(b)^2 + \varphi(c)^2 = [7]_8 \text{ wobei } \varphi(a), \varphi(b), \varphi(c) \in \mathbb{Z}_8$$

$$\text{In } \mathbb{Z}_8: \begin{array}{c|cccccccc} x & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline x^2 & 0 & 1 & 4 & 1 & 0 & 1 & 4 & 1 \end{array}$$

also, Quadrate in \mathbb{Z}_8 sind 0, 1, 4

Summe von drei Quadraten in \mathbb{Z}_8 sind nicht gleich 7

\Rightarrow Behauptung

3.4 Größter gemeinsamer Teiler

(Ring \supseteq kommutativer Ring \supseteq Integritätsbereich \supseteq Hauptideal \supseteq Euklidischer Ring)

Natürliche Zahlen $p \geq 2$, für die 1 und p die einzigen Teiler sind, nennt man Primzahlen.

z.B. 2, 3, 5, 7, 11, 13, 17, ...

Ist $m \in \mathbb{N}$ keine Primzahl und $m > 1$, so ist $m = p \cdot q$ mit $1 < p, q < m$, dann ist

$$[p]_m \cdot [q]_m = [p \cdot q]_m = [m]_m = [0]_m = 0 \text{ in } \mathbb{Z}_m, \text{ aber: } [p]_m \neq 0 \text{ und } [q]_m \neq 0, \text{ weil } 1 < p \cdot q < m$$

Definition 3.40

Sei $R=(R, +, \cdot)$ ein kommutativer Ring. Sind $a \neq 0$ und $b \neq 0$, aber $a \cdot b = 0$, so heißt a und b Nullteiler.

R heißt Integritätsbereich, falls R keine Nullteiler enthält (d.h. $ab=0 \Rightarrow a=0$ oder $b=0$)

Beispiel 3.41

1) \mathbb{Z} ist ein Integritätsbereich

2) $\mathbb{Z}[x]$ ist ein Integritätsbereich

3) Sei K ein Körper. Dann sind $K[x]$ und $K[[x]]$ (Menge aller formalen Potenzreihen)

Integritätsbereiche

4) \mathbb{Z}_4 ist kein Integritätsbereich, denn $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4 = 0$ in \mathbb{Z}_4

\mathbb{Z}_6 ist kein Integritätsbereich

\mathbb{Z}_n ist kein Integritätsbereich für n nicht Primzahl

Definition 3.42

Sei R ein Integritätsbereich.

1) $a \mid b \Leftrightarrow \exists c \in R, b = a \cdot c$ (a teilt b)

($a \nmid b \Leftrightarrow \nexists c \in R, b = a \cdot c$)

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 $d \mid b$

• ($c \mid a$ und $c \mid b$) $\Rightarrow c \mid d$

Bemerkung 3.43

Sei $R=(R, +, \cdot)$ ein Integritätsbereich. Jedes Element $u \in R$ heißt Einheit in R , falls u^{-1} existiert.

$$R^* = \{u \in R \mid \exists u^{-1} \in R \text{ mit } uu^{-1} = 1\}$$

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 auch $u \mid a$ für alle $a \in R$, denn $a = u(u^{-1}a)$

- 3) $d \in \text{ggT}(a,b)$ in R und $u \in R^* \Rightarrow u \cdot d \in \text{ggT}(a,b)$, denn umgekehrt kann man zeigen:
 $d, d' \in \text{ggT}(a,b) \Rightarrow d' = ud$ für ein $u \in R^*$
- 4) Guo: Nicht in jedem Integritätsbereich gilt $\text{ggT}(a,b)=\{1\}$
 Bemerkung: = nicht jede Ampel ist immer Rot!?
 Richtig?: In keinem Integritätsbereich gilt $\text{ggT}(a,b) \neq \emptyset$ außer im Nullring mit $0=1$

3.5 Eindeutige Primfaktorzerlegung

Definition 3.44

Sei R ein Integritätsbereich. $p \in R$ mit $p \neq 0$ und $p \notin R^*$ heißt irreduzibel wenn $p=ab \Rightarrow a \in R^*$ oder $b \in R^*$

Beispiel 3.45

$p \in \mathbb{Z}$ ist irreduzibel $\Leftrightarrow p$ oder $-p$ ist eine Primzahl

Beispiel 3.46

Sei $I = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$. Dann gilt:

- I ist ein Integritätsbereich
 - $I^* = \{-1, 1\}$
 - $|\alpha|^2 = 4 \Rightarrow \alpha$ ist irreduzibel
 - $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ zwei verschiedene Primfaktorzerlegungen von 4 in I
- Frage: Welche Integritätsbereiche R haben die Eigenschaften, daß jedes $a \in R \setminus (\{0\} \cup R^*)$ eine eindeutige Primfaktorzerlegung hat?

Definition 3.47

Sei R ein Integritätsbereich. $a \in R$ hat eine eindeutige (Primfaktor)Zerlegung, wenn

- $a = p_1 \cdot \dots \cdot p_r$, p_i irreduzibel
 - $a = q_1 \cdot \dots \cdot q_s$, q_i irreduzibel
- $\Rightarrow r=s$ und mit passender Umsortierung ist $q_i = u_i p_i$ mit $u_i \in R^*$ $i=1, 2, \dots, s$

Bemerkung 3.48

Hat $a \in R$ eine eindeutige Zerlegung, so ist $a \in R \setminus (\{0\} \cup R^*)$ denn:

$$0 = a_1 \cdot \dots \cdot a_\alpha \Rightarrow \exists a_i = 0, \text{ aber } 0 \text{ ist nicht irreduzibel}$$

$$u = a_1 \cdot \dots \cdot a_\beta \Rightarrow 1 = a_1 \underbrace{(u^{-1} a_2 \cdot \dots \cdot a_\beta)}_{a^{-1}}, \text{ aber Einheit ist nicht irreduzibel}$$

Zwei spezielle Ringe: Hauptidealringe \supseteq Euklidische Ringe

Definition 3.49

Ein Integritätsbereich R heißt Hauptidealring, wenn jedes Ideal I von R ein Hauptideal ist, d.h. $\exists d \in R: I = Rd$

Satz 3.50

Sei R ein Hauptidealring. Dann hat jedes $a \in R \setminus (\{0\} \cup R^*)$ in R eine eindeutige Primfaktorzerlegung. (ohne Beweis)

Definition 3.51

Ein Integritätsring R heißt Euklidischer Ring, wenn

1) $\exists \delta: R \setminus \{0\} \rightarrow \mathbb{N}_0$

2) zu $a, b \in R$ mit $b \neq 0$ existiert $q, r \in R$, so daß $a = q \cdot b + r$ mit $\delta(r) < \delta(b)$

Ein Euklidischer Ring (R, δ) heißt Norm-Euklidischer Ring, wenn $\delta: R \rightarrow \mathbb{N}_0$

mit $\begin{cases} \delta(a) = 0 \Leftrightarrow a = 0 \text{ und} \\ \delta(a \cdot b) \leq \delta(a) + \delta(b) \end{cases}$

Beispiel 3.52

1) $(\mathbb{Z}, | \cdot |)$ ist ein 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.

z.B. $\delta(x^5 + x^3 + 1) = 5$ $\underbrace{x^5 + x^3 + 1}_{:=a}, \underbrace{2x^3 + x}_{:=b} \in \mathbb{Q}[x]$

$a = q \cdot b + r$ mit $\text{grad}(r) < \text{grad}(b)$

$$x^5 + x^3 + 1 = (2x^3 + x)\left(\frac{1}{2}x^2 + \frac{1}{4}\right) + \left(-\frac{1}{4}x + 1\right)$$

3) $R = (K[x], \delta)$ mit $\delta(f) = \begin{cases} 2\text{grad}(f) & , f \neq 0 \\ 0 & , f = 0 \end{cases}$ ist Norm-Euklidischer Ring

Satz 3.53

Ein Euklidischer Ring R ist ein Hauptidealring. Somit hat jedes Element $a \in R \setminus (\{0\} \cup R^*)$ in R eine eindeutige Primfaktorzerlegung.

• Euklidischer Ring $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$

Folgerung 3.54

In \mathbb{Z} hat jedes $a \in \mathbb{Z} \setminus \{0\}$ eine eindeutige Primfaktorzerlegung in der Form $a = u p_1 \dots p_k$, p_i Primzahl und $u \in \mathbb{Z}^* = \{-1, 1\}$. Beweis: Beispiel 3.52 und Satz 3.53.

Bemerkung 3.55

Aus der 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: $n = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$, wobei $p_1 < p_2 < \dots < p_k$ Primzahlen sind und $t_1, \dots, t_k \in \mathbb{N}$

Satz 3.56

Es gibt unendlich viele Primzahlen.

Beweis (indirekt):

Annahme: p_1, \dots, p_k sind alle Primzahlen, $k \in \mathbb{N}$

Setze $n = p_1 \dots p_k + 1$ (\otimes) $\Rightarrow n$ ist keine Primzahl $\Rightarrow n = p_{n_1}^{t_1} \dots p_{n_s}^{t_s}$ mit $p_{n_1} < \dots < p_{n_s}$ Primzahlen,

$t_i \in \mathbb{N}$ ($\otimes \otimes$) $\Rightarrow p_{n_1} \mid n - 1 \xrightarrow{\otimes \otimes} \Rightarrow$ unmöglich (Widerspruch)

Satz 3.57 (Primzahlsatz)

$\forall n \in \mathbb{N}$ gilt: $\#$ der Primzahlen $\leq n$, wobei $\#$ der Primzahlen $= \pi(n) = (1 + o(1)) \cdot \frac{n}{\ln(n)}$

Bemerkung 3.58

Wie findet man Primzahlen?

Algorithmus:

Man schreibt alle Zahlen von 2 bis n auf und wendet dann folgenden Algorithmus an:

```

for i from 2 to  $\sqrt{n}$  do begin
  if i nicht durchgestrichen, streiche alle Vielfachen von i
end

```

Die am Ende übrig gebliebenen nicht durchgestrichenen Zahlen sind die Primzahlen $\leq n$

Finden großer Primzahlen:

randomisierte Verfahren der effizientesten Primzahltester vgl. Stochastik.

Der Satz von Fermat

Satz 3.59 (kleine Fermat)

Für alle $n \in \mathbb{N}$ mit $n \geq 2$ gilt:

$$n \text{ Primzahl} \iff a^{n-1} \equiv 1 \pmod{n} \quad \forall a \in \mathbb{Z}_n \setminus \{0\}$$

Definition 3.60

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

heißt eulersche φ -Funktion, wobei $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \setminus \{0\} \mid \text{ggT}(n, a) = 1\}$

Lemma 3.61

Ist $n = p_1^{t_1} \dots p_k^{t_k}$, $p_1 < \dots < p_k$ Primzahlen, so gilt folgendes:

$$\varphi(n) = \prod_{i=1}^k (p_i - 1) p_i^{t_i - 1}$$

Satz 3.62 (Euler)

$\forall n \in \mathbb{N}$ mit $n \geq 2$ gilt: $a^{\varphi(n)} \equiv 1 \pmod{n} \quad \forall a \in \mathbb{Z}_n^+$

Bemerkung: Satz 3.62 $\stackrel{n \text{ Primz.}}{\implies}$ Satz 3.59

Berechne $\text{ggT}(a, b)$ für $a, b \in \mathbb{Z} = (\mathbb{Z}, +, \cdot)$

Beispiel $\text{ggT}(729, 153)$

1. Primfaktorzerlegung

$$729 = 3^6 \text{ und } 153 = 3^2 \cdot 17 \implies \text{ggT}(729, 153) = 9$$

2. Division mit Rest

$$729 = 4 \cdot 153 + 117$$

$$153 = 1 \cdot 117 + 36$$

$$117 = 3 \cdot 36 + 9$$

$$36 = 4 \cdot 9$$

$$d \in \text{ggT}(729, 153)$$

$$\implies d \in \text{ggT}(117, 153)$$

$$\text{oder } 117 = 729 - 4 \cdot 153$$

Lemma 3.63

Sind $n, m \in \mathbb{N}$ mit $m \leq n$ und $m \nmid n$, so gilt:

$$\text{ggT}(m, n) = \text{ggT}(n \bmod m, m)$$

Beweis: Übung

Satz 3.64 (Euklidischer Algorithmus)

Seien $a_0, a_1 \in \mathbb{N}$ mit $a_0 \geq a_1$

Man bestimmt sukzessiv $a_i, q_i \in \mathbb{N}$

$$a_0 = q_1 a_1 + a_2 \text{ mit } 0 \leq a_2 < a_1$$

$$a_1 = q_2 a_2 + a_3 \text{ mit } 0 \leq a_3 < a_2$$

\vdots

$$a_{k-2} = q_{k-1} a_{k-1} + a_k \text{ mit } 0 \leq a_k < a_{k-1}$$

$$a_{k-1} = q_k a_k + 0$$

Dann gilt $a_k = \text{ggT}(a_0, a_1)$

Euklidischer Ring**Definition 3.65**

Ein Polynom $f = \sum_{k=0}^n a_k x^k$ heißt normiert, wenn $a_n = 1$

Folgerung 3.66

Ist K ein Körper, so hat jedes Polynom $f \in K[x] \setminus \{0\}$ eine eindeutige Zerlegung (bis auf Reihenfolge der Faktoren) der Form:

$$f = u f_1 f_2 \dots f_r, \quad u \in K^* \text{ und } f_i \text{ irreduzibel und normiert.}$$

Beweis: Beispiel 3.52(2) + Satz 3.53

Satz 3.67

Es sei (R, δ) ein Euklidischer Ring und $0 \neq f \in R$, so ist:

$$R/fR = \{[g]_f \mid g \in R, f(g) < \delta(f) \cup \{0\}\}, \text{ wobei } [g]_f = g + fR = \{g + fZ \mid Z \in R\}$$

Es ist R/fR Körper $\Leftrightarrow f$ ist irreduzibel.

Beispiel 3.68

Sei $K = \mathbb{Z}_2$ 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.

$$[a_0 + a_1x + a_2x^2]_f \sim a_0 a_1 a_2$$

$$\alpha = [x]_f \sim 010$$

$$\alpha^2 = [x^2]_f \sim 001$$

$$\alpha^3 = [x + 1]_f \sim 110, \text{ denn } x^3 = x + 1 + (x^3 + x + 1)1$$

$$\alpha^4 = \alpha^3 \alpha = [x^2 + x]_f \sim 011$$

$$\alpha^5 = \alpha^4 \alpha = [x^3 + x^2]_f = [x^2 + x + 1]_f \sim 111$$

$$\alpha^6 = \alpha^5 \alpha = [x^3 + x^2 + x]_f = [x^2 + 1]_f \sim 101$$

$$\alpha^7 = \alpha^6 \alpha = [x^3 + x]_f = [1]_f \sim 100$$

$$\alpha^8 = \alpha$$

Bemerkung 3.69

Ist $\alpha^i = \beta$, so schreibt man $i = \log_\alpha(\beta)$ (diskreter Logarithmus).

3.6 Endliche Körper

Unendliche Körper $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

Endliche Körper

1) $(\mathbb{Z}_2, +_2, \cdot_2)$

wobei $+_n : a +_n b = (a + b) \bmod n$ und $\cdot_2 : a \cdot_2 b = (ab) \bmod n$

2) $(\mathbb{Z}_2[x]/f\mathbb{Z}_2[x], +_f, \cdot_f)$ mit $f=x^3+x+1$

wobei $+_f : g +_f h = (g + h) \bmod f$ und $\cdot_f : g \cdot_f h = (gh) \bmod f$

$$|(\mathbb{Z}_2[x]/(x^3+x+1)\mathbb{Z}_2[x])| = |\{(a_0 + a_1x + a_2x^2)_f \mid a_0, a_1, a_2 \in \mathbb{Z}_2\}| \\ = |\{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}| = 2^3$$

Aus Satz 3.67 erhalten wir sofort:

Folgerung 3.70

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 Körper $\Leftrightarrow f$ irreduzibel über $K[x]$.

D.h. $f=gh \Rightarrow \text{grad}(g)=0$ oder $\text{grad}(h)=0$.

Bemerkung: p^k , p Primzahl, $k \in \mathbb{N}$

Bis auf den Isomorphismus kann man einen endlichen Körper mit p^k vielen Elementen konstruieren? Wenn ja, ist die Konstruktion eindeutig?

Satz 3.71

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 mit p^k Elementen, $\text{GF}(p^k)$ (engl. Galois field)

Mit Folgerung 3.70 und Satz 3.71 kann man alle endlichen Körper konstruieren.

Satz 3.72

In jedem endlichen Körper K ist die multiplikative Gruppe K^* zyklisch, d.h. es gibt ein Element

$a \in K^*$ mit $K^* = \langle a \rangle = \{1, a, a^2, \dots, a^{|K^*|-2}\}$

z.B. $(\mathbb{Z}_2[x]/(x^3+x+1)\mathbb{Z}_2[x])^* = \langle [x]_f \rangle$ ($\langle [x]_f \rangle = \text{Generator}$)

Effiziente Implementierung

Sei p eine Primzahl.

$k=1$ $\text{GF}(p) = (\mathbb{Z}_p, +_p, \cdot_p)$

$k>1$ $\text{GF}(p^k) = \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$, f ist irreduzibel mit $\text{grad}(f)=k$

$$=: \{\sum_{i=0}^{k-1} a_i x^i \mid a_i \in \mathbb{Z}_p\} \sim a_0 a_1 \dots a_{k-1}, \quad a_i \in \mathbb{Z}_p, \quad i=0, 1 \dots k-1$$

d.h. wir können die Elemente in $\mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ in kanonischer Weise durch Zeichenketten $a_0 a_1 \dots a_{k-1}$ mit $a_i \in \mathbb{Z}_p$ kodieren.

Addition von zwei Polynomen:

$$a(x) \sim a_0 a_1 \dots a_{k-1} +$$

$$b(x) \sim b_0 b_1 \dots b_{k-1} =$$

$$c(x) \sim c_0 c_1 \dots c_{k-1} \quad c_i = (a_i + b_i) \bmod p$$

Multiplikation von zwei Polynomen

a) $c(x) = a(x) \cdot b(x) = (\quad) \cdot (\quad)$ ausrechnen und dann den Rest modulo f bestimmen

$$b) a(x) \cdot \sum_{i=0}^{k-1} b_i x^i = a(x) \cdot b_0 + x(a(x)b_1 + x(\dots + x(a(x) \cdot b_{k-2} + xa(x) \cdot b_{k-1})))$$

Beispiel 3.73 (Fortsetzung von Beispiel 3.68)

$p=2, k=3, f=x^3 + x + 1 \in \mathbb{Z}_2[x]$ irreduzibel

$\mathbb{Z}_2[x] \setminus (x^3 + x + 1) \mathbb{Z}_2[x]$	Kurzdarstellung
0	000
1	100
x	010
$1 + x$	110
x^2	001
$x + x^2$	011
$1 + x + x^2$	111

Seien nun $a(x)=x + x^2$ und $b(x)=1 + x + x^2$

Dann gilt: $a(x) \cdot b(x) = a(x) \cdot b_0 + x(a(x) \cdot b_1 + x(a(x) \cdot b_2))$

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 mod 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 mod 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: $a(x) \cdot_f b(x) = x^2$

$$\begin{aligned} \text{Test: } (x + x^2)(1 + x + x^2) &= x + x^2 + x^3 + x^2 + x^3 + x^4 \\ &= x + \underbrace{2x^2}_{\text{mod}2=0} + \underbrace{2x^3}_{\text{mod}2=0} + x^4 \\ &= x + x^4 = x^2 + x(x^3 + x + 1) \end{aligned}$$

c) Nach Satz 3.72 gilt 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 $\alpha = [x]_f$

$$a(x) = x + x^2 = \alpha^4, \quad b(x) = 1 + x + x^2 = \alpha^5$$

$$\text{Dann gilt } a(x) \cdot_f b(x) = \alpha^{l_a} \cdot \alpha^{l_b} = \alpha^{(l_a+l_b) \text{ mod } p^k-1} = \alpha^4 \cdot \alpha^5 = \alpha^9 \text{ mod } 2^3-1 = \alpha^2 = x^2$$

Index

- Adjazenzmatrix, 21
- Algebra
 - abelsch, 40
 - universell, 39
 - Unteralgebra, 42
- algorithmische Verfahren, 13
- Automorphismus, 42

- Baum, 24
 - balanciert, 25
 - Binarbaum, 25
 - Tiefe, 25
 - vollständig, 25
- boolesche Algebra, 40

- Catalan-Zahlen, 16
- Cayleys Tree Formular, 27

- Digraph, 36
- doppeltes Abzählen, 5

- erzeugende Funktionen, 8
- Euklidischer Ring, 48
- eulersch, 32
 - semi-eulersch, 32
- Eulersche Polyederformel, 34
- Eulertour, 32, 37

- Fibonacci-Zahlen, 14
- Fleury's Algorithmus, 33
- formale Potenzreihen, 8

- Goldener Schnitt, 15
- Graph
 - eingebettet, 33
 - Gerüst, 26
 - planar, 33
 - zshg., 22
- Graphen
 - bipartit, 29
 - Gittergraphen, 19
 - multipartit, 30
 - Nachbarschaft, 20
 - vollständige, 19
- Gruppe, 40
 - Untergruppe, 41

- Halbgruppe, 40
- Hamilton-Kreis, 30
- Hamilton-Weg, 30

- hamiltonsch, 30
 - semi-hamiltonsch, 30
- Hamiltonscher Kreis, 37
- Hamiltonscher Weg, 37
- Handschlaglemma, 21
- Hauptidealring, 47
- Homomorphiesatz, 44
- Homomorphismus, 42
- Hyperwürfel, 20

- injektive Abbildungen, 7
- Inklusion und Exklusion, 6
- Integritätsbereich, 46
- inverses Element, 40
- Inversion von Potenzreihen, 11
- Inzidenzmatrix, 21
- irreduzibel, 47

- k-Partition, 6
- Kantenfolge, 32
 - orientiert, 36
- Kantenzug, 32
 - orientiert, 36
- Komponente
 - stark zshg., 37
 - Zusammenhangskomponente, 22, 33
- Körper, 40
- Kronecker-Delta, 9

- lineare Rekursion, 13

- Matching, 28
- Monoid, 40

- neutrales Element, 39

- Operator, 39

- Partition, 6
- Permutationen, 7

- Rekursionsgleichungen
 - Schema (allgemein), 18
 - Schema (homogen linear), 15
- Ring, 40

- Schubfachprinzip, 5
- Siebformel, 6
- Signatur, 39
- Stirlingzahl
 - Dreieck erster Art, 8

- Dreieck zweiter Art, 7
 - erster Art, 8
 - zweiter Art, 6
- surjektive Abbildungen, 7
- Symmetrische Gruppe, 4

- Teildigraph, 36
 - induziert, 36
- Teilgraph, 22
 - induziert, 22
- Travelling Salesman Problem, 31
- Turnier, 37
 - stark zshg., 38

- Vandermond'sche Identität, 5
- Verknüpfung, 39
- Vierfarbenproblem, 35
- Vierfarbenvermutung, 35

- Wald, 24
- Weg
 - orientiert, 36