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

1.1 Elementare Zählprinzipien

M: endliche Menge
$|M| = n,\ n \in \mathbb{N} = \{1, 2, ...\}$ ⇔ Es gibt eine Bijektion f: M $\longrightarrow \{1, 2, ...\}$
Eine Menge M mit $|M|$= n heißt n-Menge.
$|M| = 0 \Leftrightarrow M = \varnothing$

Lemma 1.1
Seien A und B zwei Mengen
a) $|A| = |B| \Leftrightarrow$ Es gibt eine Bijektion f: A $\longrightarrow B$
b) $|A \uplus B| = |A| + |B|$
 A ⊎ B heißt die disjunkte Vereinigung von A und B, d.h. es gilt A ∩ B = ∅
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. $f : A \longrightarrow A$ heißt die Permutation von A, wenn f bijektiv ist.

Lemma 1.4
Sei $S_n = \{a \mid a : \{1, 2, ...\ n\} \longrightarrow \{1, 2, ...\ n\}\ bijektiv\} = Sym\ \{1, 2, ...\ n\}$ (Symmetrische Gruppe)
Dann gilt: $|S_n| = n \cdot (n-1) \cdot (n-2)\ ...\ 2 \cdot 1$ = 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. $|A| = n \Longrightarrow |P(A)| = 2^n, wobei\ P(A) = \{B \mid B \subseteq A\}$ die Potenzmenge von A ist.

Definition 1.6
Sei A eine Menge und k ∈ ℕ mit k ≤ $|A|$
$P_k(A) = \binom{A}{k} =: \{B \subseteq A \mid\ |B| = k\}$ = Menge aller k-Teilmengen von A

Bemerkung 1.7
P(A) = $\biguplus_{k=0}^{n} P_k(A),\ n = |A|$
$\Longrightarrow |P(A)| = |P_0(A)| + |P_1(A)| +\ ...\ + |P_n(A)| = \sum_{k=0}^{n} |P_k(A)|$

Lemma 1.8
Sei A eine Menge mit $|A|$ = n. Dann gilt:

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

Satz 1.9 (Pascal-Dreieck)
Für alle n, k ∈ 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≤ S×T eine Relation. Dann gilt

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

Satz 1.12 (Schubfachprinzip)
Sei $f : X \to Y$ eine Abbildung und es gilt $|X| > |Y|$, so gibt es ein y ∈ 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 $f : X \to Y$ eine Abbildung, so gibt es ein y∈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) $|A \times B| = |A| \cdot |B|$
- $M = A_1 \times A_2 \times \ ... \ \times A_n \Longrightarrow |M| = |A_1| \cdot |A_2| \cdot \ ... \ \cdot |A_n|$

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

b) Seien A und B zwei disjunkte Mengen, so gilt $|A \uplus B| = |A| + |B|$
- Seien $A_1, A_2, \ ... \ A_n$ paarweise disjunkte Mengen (d.h. $A_i \cap A_j = \varnothing$ für $i, j \in \{1, 2, \ ... \ n\}$ *mit* $i \neq j$) und S = $A_1 \cup A_2 \cup \ ... \ A_n = \uplus_{i=1}^{n} A_i$

$$\Longrightarrow |A| = |A_1| + |A_2| + \ ... \ + |A_n| = \sum_{i=1}^{n} |A_i| \ (Summenregel)$$

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

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

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

$$|M_2 \cap M_3 \cap M_5| = |M_2| + |M_3| + |M_5| - \underbrace{|M_2 \cap M_3|}_{M_6} - \underbrace{|M_2 \cap M_5|}_{M_{10}} - \underbrace{|M_3 \cap M_5|}_{M_{15}}$$
$$+ \underbrace{|M_2 \cap M_3 \cap M_5|}_{M_{30}}$$

$$|M_2 \cap M_3 \cap M_5| = \lfloor \tfrac{100}{2} \rfloor + \lfloor \tfrac{100}{3} \rfloor + \lfloor \tfrac{100}{5} \rfloor - \lfloor \tfrac{100}{6} \rfloor - \lfloor \tfrac{100}{10} \rfloor - \lfloor \tfrac{100}{15} \rfloor + \lfloor \tfrac{100}{30} \rfloor$$
$= 50 + 33 + 20 - 16 - 10 - 6 + 3$

$= 74$

1.2 Mengenpartitionen

Definition 1.17
Sei 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 = $A_1 \uplus A_2 \uplus\ ...\ \uplus A_k\ mit\ A_i = \varnothing\ für\ i \in \{1, 2,\ ...\ n\}$ so heißt $P = \{A_1, A_2,\ ...\ A_k\}$ eine k-Partition von M.
- $Part_k(M) := \{P \mid P\ ist\ eine\ k-Partition\ von\ M\}$
- Stirlingzahlen zweiter Art:
  $S_{n,k} := |Part_k(M)|\ für\ n, k \geq 0\ und\ S_{0,0} := 0$
  $S_{n,k} := \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ = Anzahl der k-Partitionen einer n-Menge

Beispiel 1.18
1) $M = \{1, 2, 3, 4\}$
   $Part_1(M) = \{\{M\}\}$
   $Part_2(M) = \{\{\{1\}, \{2, 3, 4\}\}, \{\{2\}, \{1, 3, 4\}\}, \{\{3\}, \{1, 2, 4\}\}, \{\{4\}, \{1, 2, 3\}\},$
   $\{\{1, 2\}, \{3, 4\}\}, \{\{1, 3\}, \{2, 4\}\}, \{\{1, 4\}, \{2, 3\}\}\}$

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

2) Für $n \geq 1$ gilt:
   $S_{n,0} = 0,\ \ S_{n,1} = 1,\ \ S_{n,n-1} = \binom{n}{2},\ \ S_{n,n} = 1$
   Ist $k > n$, so gilt $S_{n,k} = 0$

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 1.20
Seien 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
$|Inj(M,N)| = n^{\underline{m}} = n \cdot (n-1) \cdot\ ...\ \cdot (n-(m-1)$
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:
$S_n = Sym\{1, 2,\ ...\ ,\ n\ \} := \{a : \{1, 2,\ ...\ ,\ n\} \longrightarrow \{1, 2,\ ...\ n\} \mid a\ bijektiv\}$
$|S_n| = n!$
• 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) ∘ (8) ∘ (6 9 11 10)

Definition 1.22
Ein k-Zyklus $(i_1, i_2, i_3,\ ...\ i_k)$ ist eine Permutation $\sigma \in S_n$ *mit* $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3,\ ...\ \sigma(i_k - 1) = i_k, \sigma(i_k) = i_1$ *und* $\sigma(i) = i$ *für* $i \notin \{i_1, i_2,\ ...\ i_k\}$ *wobei* $\{i_1, i_2,\ ...\ i_k\} \subseteq \{1, 2,\ ...\ n\}$

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) ≠ (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=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 $\{1,2,...,n\}$,
die genau k Zyklen haben, heißt Stirlingzahl erster Art, bezeichnet mit $s_{n,k}$ oder $\begin{bmatrix} n \\ k \end{bmatrix}$.
Z.B. in obigen Beispiel gilt:

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

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

Satz 1.25 (Stirling-Dreieck erster Art)

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

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: $a_0, a_1, a_2, ..., a_n = (a_n)_{n\in\mathbb{N}_0}$
Wir führen eine neue Schreibweise für $(a_n)_{n\in\mathbb{N}_0}$:
$a_0 + a_1x + a_2x^2 + ... + a_2x^n + ... = \sum\limits_{n=0}^{\infty} a_nx^n$ = 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):= $\sum\limits_{k=0}^{\infty} a_nx^n = (a_n)_{n\in\mathbb{N}_0}$

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

Bemerkung 1.28

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

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

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

3) Für k $\in \mathbb{N}$ gilt: $\sum\limits_{n=0}^{\infty} a_n x^{kn} = (b_i)_{i\in\mathbb{N}_0} \quad b_i = \begin{cases} 0 & , i \neq kn \ \forall \ n \in \mathbb{N}_0 \\ a_n & , i = kn \ f\ddot{u}r \ n \in \mathbb{N}_0 \end{cases}$

z.B. k=2: $\sum\limits_{n=0}^{\infty} a_n x^{2n} = a_0 + 0x + a_2x^2 + 0x^3 + a_4x^4 + ...$

4) Unterschiede zwischen

Potenzreihen aus der Analysis und	formalen Potenzreihen
- $f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$	- A(x)= $\sum\limits_{n=0}^{\infty} a_n x^n = (a_n)_{n\in\mathbb{N}_0}$
- 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)= $\sum\limits_{n=0}^{\infty} a_n x^n$, B(x)= $\sum\limits_{n=0}^{\infty} b_n x^n$.

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:

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

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

Beispiel 1.31
Es gilt $x^m \cdot x^n = x^{m+n} \quad m, n \in \mathbb{N}_0$

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 $1 = 1 \cdot x^0 = (1, 0, 0, ...)$

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

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

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

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 $\Longleftrightarrow$ es gilt

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

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

$$\begin{aligned} \Longleftrightarrow a_0 b_0 &= 1 && n = 0 \\ a_0 b_1 + a_0 b_0 &= 0 && n = 1 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0 && n = 2 \end{aligned}$$

Ist A invertierbar, so muß $a_0 \neq 0$. Umgekehrt ist $a_0 \neq 0$, so definiere
$b_0 = \frac{1}{a_0} \in K$
$b_n = -\frac{1}{a_0}(a_1 b_{n-1} + a_2 b_{n-2} + \ \dots\ + a_n b_0)$ rekursiv für $\in \mathbb{N}_0$

Beispiel 1.37
1) A = 1 - cx $= \sum_{n=0}^{\infty} a_n x^n$ mit $a_0 = 1, \quad a_1 = -c, \quad a_2 = a_3 = \ \dots\ = 0$
Bestimme A^{-1}

Lösung: Sei $A^{-1} = \sum_{n=0}^{\infty} b_n x^n$. Dann gilt:
$a_0 b_0 = 1 \Longrightarrow b_0 = 1$
$a_0 b_1 + a_1 b_0 = 0 \Longleftrightarrow 1 \cdot b_1 - c \cdot 1 = 0 \Longrightarrow b_1 = c$
$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \Longrightarrow b_2 = c^2$
$\dots \Longrightarrow b_n = c^n$

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

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

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

Definition 1.38
Die Abbildung D: K[[x]] $\longrightarrow$ K[[x]] mit $\sum_{n=0}^{\infty} a_n x^n \longrightarrow \sum_{n+1}^{\infty}(n+1)\ a_{n+1} x^n$ heißt formale Ableitung.
(Bemerkung: D: K[[x]] $\longrightarrow$ K[[x]] ist eine Operation auf Folgen:
D: $a_0,\ a_1,\ a_2,\ \dots\ a_n,\ \dots \longrightarrow a_1,\ 2a_2,\ 3a_3,\ \dots\ na_n,\ \dots$)

Lemma 1.39
D: K[[x]] $\longrightarrow$ K[[x]] ist k-linear und es gilt:
a) $D(x^n) = nx^{n-1}$, $n \geq 1$
b) $D(A \cdot B) = D(A) \cdot B + A \cdot B(A)$

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, ...	$\sum_{n=0}^{\infty} n x^n$	$\frac{x}{(1-x)^2}$
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
$$\mathrm{F(n) = F(n - 1) + F(n - 2)}, \qquad \mathrm{n} \geq 2 \text{ und } \mathrm{F(1) = 1} \text{ und } \mathrm{F(0) = 0}$$
oder $$\mathrm{F(n) = T}\big(\lfloor \tfrac{n}{2} \rfloor\big) + \mathrm{T}\big(\lceil \tfrac{n}{2} \rceil\big), \qquad \mathrm{n} \geq 2 \text{ und } \mathrm{T(1) = 1}$$
vokommen. Für die Bestimmung der Laufzeit von Algorithmen spielt das Lösen von Rekursionsgleichungen eine zentrale Rolle.

Lineare Rekursion
Definition 1.43
Eine Rekursionsgleichung der Form
$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ \dots\ + c_k a_{n-k} + b_k \qquad \forall n \geq k$$
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 $\quad a_n = c \cdot a_{n-1}, \ \ n \geq 1, \ \ a_0 = b_0$
  $a_1 = c \cdot a_0 = c \cdot b_0$
  $a_2 = c \cdot a_1 = c \cdot c \cdot b_0 = c^2 b_0$
  Lösung der Gleichung $a_n = b_0 c^n$

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

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

n $\longrightarrow$ n + 1:
1. Fall: c $\neq$ 1. Es gilt:
$$\begin{aligned} a_n &= c a_{n-1} + b_1 = c\left(b_0 c^{n-1} + b_1 \cdot \tfrac{c^{n-1}-1}{c-1}\right) + b_1 \\ &= b_0 c^n + b_1 \left(\tfrac{c^n - 1}{c-1} + 1\right) \\ &= b_0 c^n + b_1 \cdot \tfrac{c^n - 1}{c-1} \end{aligned}$$

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

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

$$
\begin{aligned}
\text{Sei F} = \text{F(x)} &= \sum_{n=0}^{\infty} F_n x^n \\
&= F_0x^0 + F_1x^1 + \sum_{n=2}^{\infty}(F_{n-1} + F_{n-2})x^n \\
&= F_0x^0 + F_1x^1 + \sum_{n=2}^{\infty} F_{n-1}x^n + \sum_{n=2}^{\infty} F_{n-2}x^n \\
&= F_0x^0 + F_1x^1 + x \cdot \sum_{n=1}^{\infty} F_nx^n + x^2 \cdot \sum_{n=0}^{\infty} F_nx^n \\
&= F_0x^0 + F_1x^1 + x \cdot \underbrace{\sum_{n=0}^{\infty} F_nx^n}_{=F} - F_0x^0 + x^2 \cdot \sum_{n=0}^{\infty} F_nx^n \\
&= F_0x^0 + F_1x^1 + xF - F_0x^0 + x^2F \qquad mit\ F_0 = 0\ und\ F_1 = 1 \\
&= x + xF + x^2F
\end{aligned}
$$

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

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

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

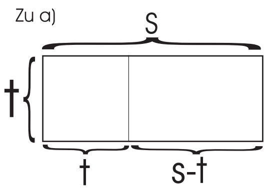
Somit gilt: $F_n = a\alpha^n + b\beta^n$

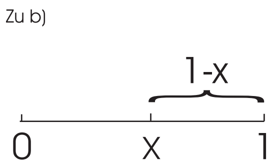
$$
\begin{aligned}
\text{Wegen } \frac{x}{1-x-x^2} &= \frac{x}{\frac{5}{4} - \left(x + \frac{1}{2}\right)^2} \\
&= \frac{x}{\left(\frac{\sqrt{5}}{2} - \left(x + \frac{1}{2}\right)\right) \cdot \left(\frac{\sqrt{5}}{2} + \left(x + \frac{1}{2}\right)\right)} \\
&= \frac{\frac{1}{\sqrt{5}}}{1 - \frac{\sqrt{5}+1}{2}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

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

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

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: $\frac{s}{t} = \frac{t}{s-t} = (\frac{1}{\frac{s}{t}-1})$, setze $\frac{s}{t} = x$, dann gilt:
$x = \frac{1}{x-1} \Leftrightarrow x^2 - x - 1 = 0 \Leftrightarrow x_{1,2} = \frac{1\pm\sqrt{5}}{2}$ Somit ist x=$\frac{\sqrt{5}-1}{2} = \frac{2}{1+\sqrt{5}} = \frac{1}{\theta}$ b) $\frac{1}{x} = \frac{x}{1-x}$, $0 \leq x \leq 1$ 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≥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=$\begin{cases} \frac{b_0 - b_0\beta}{\alpha-\beta} & \text{, falls } \alpha \neq \beta \\ b_0 & \text{, falls } \alpha = \beta \end{cases}$ $B = \begin{cases} \frac{b_1 - b_0\alpha}{\alpha-\beta} & \text{, falls } \alpha \neq \beta \\ b_0 & \text{, falls } \alpha = \beta \end{cases}$

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

Schema zum Lösen von (homogenen) linearen Rekursionsgleichungen
$a_n = c_1 a_{n-1} + c_2 a_{n-2} + ... + c_k a_{n-k}$ für n≥k mit $a_i = b_i$ für i=0,1,...,k-1

1. Aufstellen der erzeugenden Funktion
   A(x)=$\sum\limits_{n=0}^{\infty} a_n x^n$

2. Anwendung der Rekursionsgleichung

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

3. Auflösen nach A(x)

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

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

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

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

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

$$A(x) = \sum_{j=1}^{t} \frac{g_i(x)}{(1-\alpha_ix)^{m_i}} = \sum_{n=0}^{\infty} g_nx^n$$

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)=$\sum\limits_{n=0}^{\infty} a_nx^n$, dann gilt:

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

$$= a_0 + a_1x + a_2x^2 + 5x\sum_{n=3}^{\infty} a_{n-1}x^{n-1} - 7x^2\sum_{n=3}^{\infty} a_{n-2}x^{n-2} + 3x^2\sum_{n=3}^{\infty} a_{n-3}x^{n-3}$$

$$= 1 + 5 + 19x^2 + 5x(A(x) - (1+5x)) - 7x^2(A(x) - 1) + 3x^3A(x) \ \Rightarrow$$

$$A(x) = \tfrac{1+x^2}{1-5x+7x^2-3x^3} = \tfrac{1+x^2}{(1-x)^2(1-3x)} = \tfrac{\frac{1}{2}x-\frac{3}{2}}{(1-x)^2} + \tfrac{\frac{5}{2}}{1-3x} = \tfrac{1}{2}(x-3)\tfrac{1}{(1-x)^2} + \tfrac{5}{2} \cdot \tfrac{1}{1-3x}$$

$$= \tfrac{1}{2}(x-3)\sum_{n=0}^{\infty}\binom{n+1}{1}x^n + \tfrac{5}{2}\sum_{n=0}^{\infty}(3x)^n = 1 + 5x + \sum_{n=2}^{\infty}(\tfrac{5}{2}3^n - n - \tfrac{3}{2})x^n \ \Rightarrow$$

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

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.

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

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

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

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

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:

$c(x) = c_0 x^0 + \sum_{n=1}^{\infty} c_n x^n$

$\overset{1.51}{=} c_0 + \sum_{n=1}^{\infty} (\sum_{k=1}^{n} c_{k-1} \cdot c_{n-k}) x^n$

$= c_0 + x \sum_{n=1}^{\infty} (\sum_{k=1}^{n} c_{k-1} \cdot c_{n-k}) x^{n-1}$

$\overset{t=n-1}{=} c_0 + x \sum_{t=0}^{\infty} (\sum_{k=1}^{t+1} c_{k-1} \cdot c_{(t+1)-k}) x^{n-1}$

$\overset{s=k-1}{=} c_0 + x \sum_{t=0}^{\infty} (\sum_{s=0}^{t} c_s \cdot c_{(t-s)}) x^t$

$\overset{1.29}{=} c_0 + x \cdot c(x) \cdot c(x)$

Somit gilt:

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

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

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

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

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

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

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

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

Koeffizienten von x^0 ist gleich 0 $\Longrightarrow$ - als Vorzeichen

D.h. $c_0x + c_1x^2 + ... = -\frac{1}{2}(\sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n}(-4)^n x^n)$

$$\begin{aligned}
c_n &= -\tfrac{1}{2}\binom{\frac{1}{2}}{n+1}(-4)^{n+1} \\
&= -\tfrac{1}{2} \cdot \tfrac{\frac{1}{2}\cdot(\frac{1}{2}-1)\ ...\ (\frac{1}{2}-n)}{(n+1)!} \cdot (-1)^{n+1} \cdot 4^{n+1} \\
&= (-1)^{n+2} \cdot \tfrac{(\frac{1}{2}-1)\ ...\ (\frac{1}{2}-n)}{(n+1)!} \cdot 4^n \\
&= \tfrac{(2-1)\cdot(4-1)\ ...\ (2n-1)}{(n+1)!\cdot n!} \cdot 2^n \cdot n! \\
&= \tfrac{(1\cdot 3\ ...\ (2n-1))\ (2\cdot 4\ ...\ (2n))}{(n+1)!\cdot n!\cdot n!} \\
&= \tfrac{1}{n+1} \cdot \tfrac{(2n)!}{n!\cdot n!} \\
&= \tfrac{1}{n+1}\binom{2n}{n}
\end{aligned}$$

Schema zum Lösen von (allgemeinen) Rekursionsgleichungen

Rekursionsgleichung $a_n = f(a_{n-1}, a_{n-2},\ ...\ a_{n-k})\ \ n \geq k.$
Anfangswerte $a_i = b_i\ \ i = 0, 1, 2\ ...\ k-1$
Berechne $a_n\ \ n \geq k$ explizit

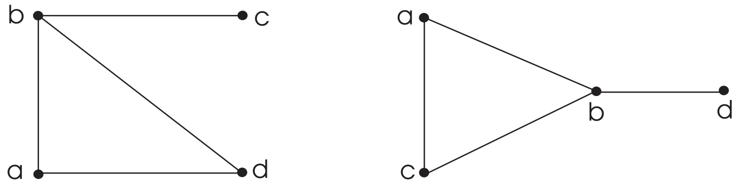
1) Aufstellen der erzeugenden Funktion
   A(x) = $\sum_{n=0}^{\infty} a_n x^n$
2) Umformen $\sum_{n=0}^{\infty} a_n x^n$, so daß Anfangswerte und Rekursionsgleichung eingesetzt werden können
3) Weiter umformen, bis auf der rechten Seite die noch vorhandene unendliche Summe (und mit allen vorkommenden Folgeglieder 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

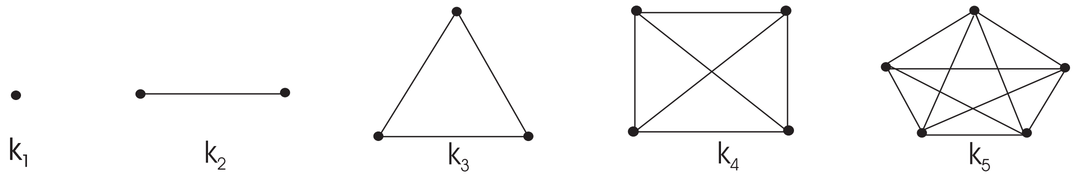
2.1 Grundbegriffe der Graphentheorie

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.

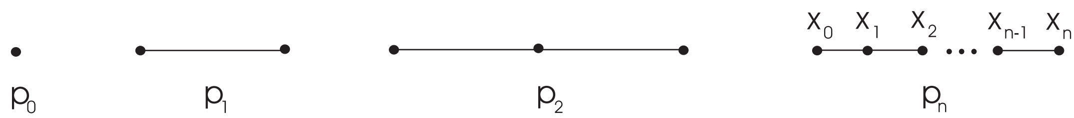
Beispiel 2.2
1) G = ($\{a, b, c, d\}, \{ab, bc, ca, bd\}$)



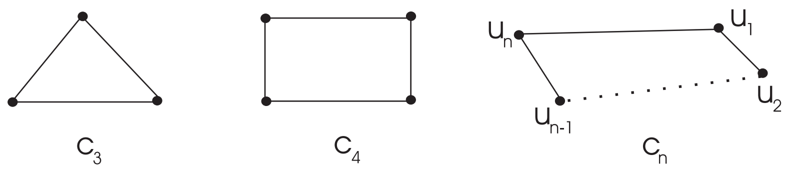
2) Vollständige Graphen K_n = (V, $\binom{V}{2}$) mit $|V|$ = n



3) Wege

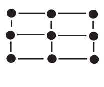


4) Kreis



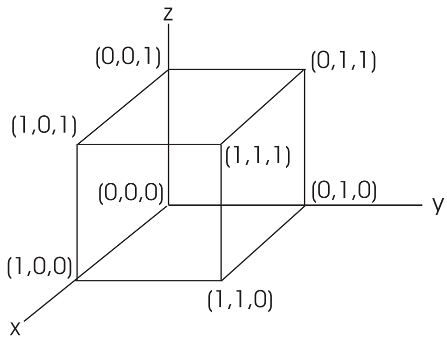
$C_n = U_1U_2 \ ... \ U_nU_1$

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(Qd) := die Menge aller 0-1 Folgen der Länge d
E(Qd) := $\{xy \mid x, y \in V(Qd)\}$ x und y unterscheiden sich genau in einer Stelle

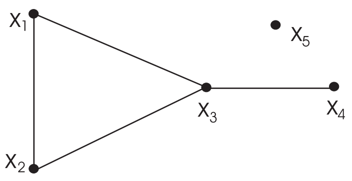


Bemerkung 2.3
1) In dieser Vorlesung betrachten wir nur Graphen ohne Mehrfachkanten und ohne Schleifen
- Ein Graph ohne Schleifen heißt Multigraph
- Ein Graph ohne Schleifen und ohne Mehrfachkanten heißt schlichter Graph
- G = $(\varnothing, \varnothing)$ heißt leerer Graph
- G = (V, $\varnothing$) heißt 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.
- δ(G) = $\min\limits_{x \in V} d(x)$, $\quad \triangle(G) = \max\limits_{x \in V} d(x)$
  ist $\delta(G) = \triangle(G)$=k, so heißt G k-regulärer Graph.

Beispiel 2.5

1) 

$N(x_1) = \{x_2, x_3\},\ N(x_3) = \{x_1, x_2, x_4\},$
$d(x_1) = 2,\ d(x_3) = 3,\ x_4\ Endecke,\ x_5\ isoliert$

2) C_n ist 2-regulär

Satz 2.6 (Handschlaglemma, Euler 1736)

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

Beweis: In $\sum\limits_{x \in V} d(x)$ 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
$\Longrightarrow$ 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' ($G \cong G'$)
$\Leftrightarrow$ $\exists$ eine bijektive Abbildung $\phi: \ V \to V'$ mit xy $\in$ E $\Leftrightarrow$ $\phi(y) \in E'$

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.

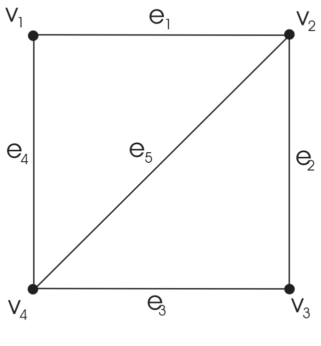
2.2 Darstellung von Graphen

Defintion 2.11
Ist G=(V,E) ein markierter Graph mit V=$\{v_1, ..., v_n\}$ und E=$\{e_1, ..., e_m\}$, 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 Adjezenzmatrix von G

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

Beispiel 2.12



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

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

Satz 2.13
Sei G=(V,E) mit V=$\{v_1, v_2, ..., v_n\}$. Ist A die Adjezenzmatrix und I die Inzidenzmatrix von G, so gilt:
$I \cdot I^t$=A + diag(d(1),d(2),...,d(n))

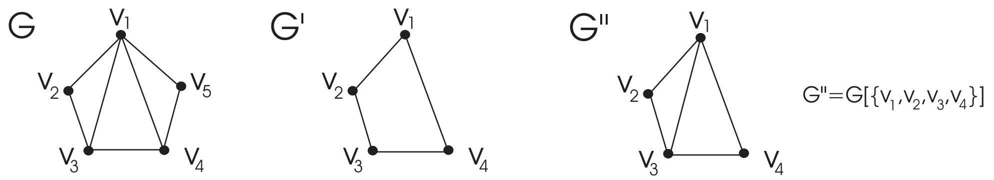
Beweis: Für $i \neq j$:

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

Für i=j:

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

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.

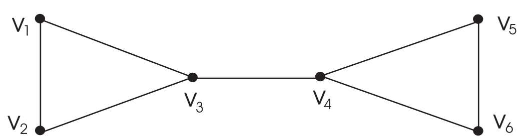


Definition 2.15
1) Sei G=(V,E). G heißt zusammenhängend, wenn zwischen je zwei Ecken x, y $\in$ V ein Weg von x nach y existiert.
2) In einem nicht zusammenhängenden Graphen heißt jeder maximale (bzgl. Anzahl von Ecken und Kanten) zusammenhängende Teilgraph eine Zusammenhangskomponente ode Komponente.
   - Sind G_1, ... G_k die Komponenten von G, so gilt:

$$G = \bigcup_{i=1}^{k} G_i$$

   κ(G) := Anzahl der Komponenten von G
   κ(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 $v_3 v_4$ eine Brücke

Satz 2.16
Sei G=(V,E). Dann gilt:

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

Beweis: (Induktion über m = $|E|$)
• m = 0: κ(G) = $|V|$
also κ(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:
κ(G') $\geq |V| - |E|\setminus\{e\}$ = $|V|$ - ((m + 1) - 1) = $|V|$ - m
Seien $G'_1, G'_2,$ ... G'_k die Komponenten von G'

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

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

= $|V|$ - $|E|$

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 $G_1,$ ... G_k die Komponenten von G mit $|V(G_i)| = n_i$ i = 1, ... k
Dann gilt k $\geq$ 2 und $n_1 + n_2 +$ ... n_k = n

m = $|E(G_1)| + |E(G_2)| +$ ... $+ |E(G_k)|$

$\overset{2.17}{=} \frac{n_1(n_1-1)}{2} + \frac{n_2(n_2-1)}{2} + \ ... \ + \frac{n_k(n_k-1)}{2}$

$= \frac{1}{2}((n_1^2 + n_2^2 + \ ... \ + n_k^2) - (n_1 + n_2 + \ ... \ + n_k))$

$= \frac{1}{2}((n_1 + \ ... \ n_k)^2 - 2\sum_{1 \leq i < j \leq k}(n_i n_j - n))$

$\leq \frac{1}{2}(n^2 - 2n_1(\underbrace{n_2 + n_3 + \ ... \ + n_k}_{=n-n_1}) - n)$

$\leq \frac{1}{2}(n^2 - 2(n-1) - n)$

$= \frac{1}{2}(n^2 - 3n + 2)$

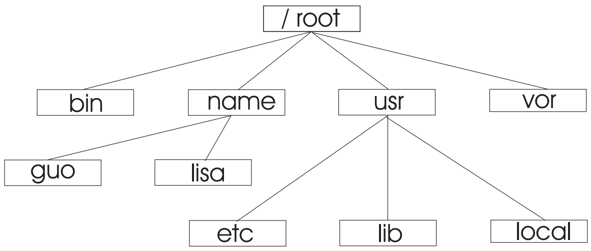
$= \frac{1}{2}(n-1)(n-2)$

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)

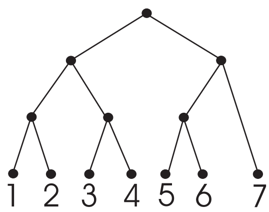
Beweis: Sei p = $v_0 v_1$ ... v_k ein längster Weg in T.
Dann sind v_0 und v_k zwei Endecken und besitzen den Grad 1. Ansonsten wären Kreise vorhanden und T kein Baum.

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 Kreifrei 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 $\subsetneqq$ 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 Endecke 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

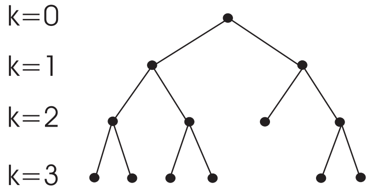
Defintion 2.23
Ein Wurzelbaum T=(V,E) ist ein Baum, in dem eine Ecke v∈V als Wurzel ausgezeichnet wird. Es sei x ein Ecke im Wurzelbaum T mit Wurzel w.
- Jede Ecke y auf dem eindeutig bestimmten Weg von w nach x heißt Vorgänger von x
- Sei y ein Vorgänger von x mit x≠y, so heißt x Nachfolger von y
- Sind xy∈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 depth(T) eines Wurzelbaumes T ist die maximale Länge eines Weges von der Wurzel zu einer Endecke.
Ein Wurzelbaum T der Tiefe t heißt balanciert, wenn jede Endecke 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∈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.

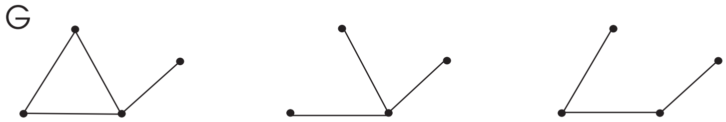
Satz 2.26
Sei T=(V,E) ein binärer Baum mit der Tiefe t und $|V|$=n. Dann gilt t+1≤n≤ $2^{n+1} - 1$
Beweis:



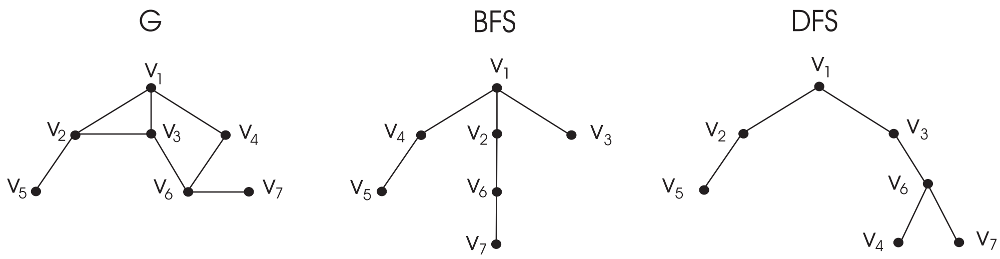
P_k:= Anzahl der Ecken auf Niveau 0≤k≤t. Es gilt: $\sum\limits_{k=0}^{t} P_k$=n
Da gilt $P_k \geq 1$ für 1≤k≤t und $P_k \leq 2P_{k-1}$ für 1≤k≤t, ist $P_k \leq 2^k$
⇒ t+1≤ $\sum\limits_{k=0}^{t} P_k \leq \sum\limits_{k=0}^{t} 2^k = 2^{t+1} - 1$

Folgerung 2.27
Sei T=(V,E) ein binärer Baum mit der Tiefe t und $|V|$=n. Dann gilt t≥ $\lceil log_2(\frac{n+1}{2})\rceil$
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=$v_0 v_1 v_2 ... v_n v_0$ und nehme eine beliebige Kante von C raus.
Z.B. G'=(V,E$\setminus\{v_0 v_1\}$) 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($|V| + |E|$).



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

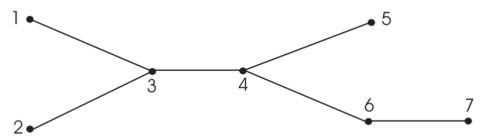
Vor- und Nachteile (Adjezenzmatrix vs. Adjenzenzliste)

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

f(x)=Θ(g(n))=f(n) wächst genauso schnell wie g(n)

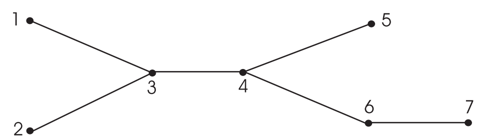
Satz 2.30 (Cayley's Tree Formular)
Sei G ein vollständiger markierter Graph mit n $\geq$ 2 Ecken. Dann besitzt G n^{n-2} verschiedene Gerüste.
Beweis:
Baum T auf V = $\{1, 2, \ ... \ n\} \overset{bijektiv}{\longleftrightarrow}$ P(T) = $(t_1, t_2, \ ... \ t_{n-2}) \in V^{n-2}$, Prüfcode von T

Algorithmus $\rightarrow$
Eingabe: Baum T=(V,E) mit V=$\{1, 2, \ ... \ n\}$
Ausgabe: Wort $(t_1, t_2, \ ... \ t_n)$ über dem Alphabet $\{1, 2, \ ... \ n\}$



i $\leftarrow$ 1
while $|V| > 2$ do begin
bestimme die Endecken V im Baum T mit der kleinsten Markierung
$t_i \leftarrow$ Nachbar von V im Baum T
T $\leftarrow \underbrace{(V(T)\backslash\{V\}, E(T)\backslash\{Vt_i\})}_{ebenfalls\ ein\ Baum}$
i $\leftarrow$ i + 1
end

Algorithmus $\leftarrow$
Eingabe: Wort $(t_1, t_2, \ ... \ t_n)$ über dem Alphabet $\{1, 2, \ ... \ n\}$
Ausgabe: Baum T = ($\{1, 2, \ ... \ n\}$, E)
z.B. (3, 3, 4, 4, 6)

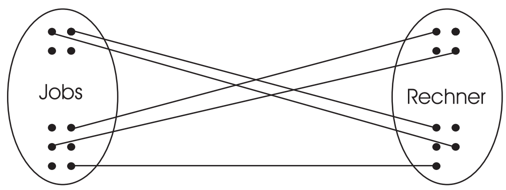


S $\leftarrow \varnothing$
for i from 1 to n-2 do begin wähle die kleinste Ecke $s_i \in \{1, 2, \ ... \ n\}\backslash$ S mit $s_i \notin \{t_i, t_{i+1}, \ ... \ t_{n-2}\}$
füge die Kante $e_i = s_i t_i$ in den Graphen ein
S $\leftarrow S \cup \{s_i\}$
end
füge die Kante $e_{n-1} := \{1, 2, \ ... \ n\}\backslash St_{n-2}$ in den Graphen ein.

$\Longrightarrow$ Behauptung

2.4 Matchings in Graphen

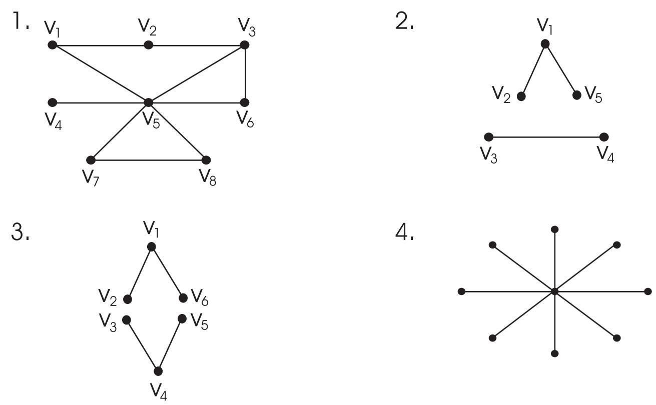
Gegeben: eine Menge von Rechnern mit verschiedenen Leistungsmerkmalen (z.B. Speicher, Geschwindigkeit, ...) und eine Menge von Jobs mit unterschiedlichen Leistungsanforderungen an die Rechner.
Gesucht: eine Verteilung von den Jobs auf die Rechner, so daß möglichst viele Jobs gleichzeitig bearbeitet werden 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) $= \varnothing \;\; \forall\, K_1, K_2 \in M$ und $K_1 \neq K_2$
- Ein Matching M von G heißt maximal, wenn es in G kein Matching M' gibt mit M $\subsetneqq M'$
- 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



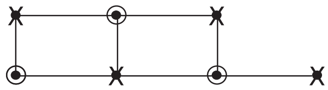
Bemerkung 2.33
Für jeden Graphen G=(V,E) gilt: 1) Jedes perfektes Matching ist ein Maximum-Matching
2) Fr jedes Matching M ist $|V(M)| = 2|M|$
3) Für ein perfektes Matching M von G gilt $2|M| = |V(G)|$
4) G hat ein perfektes Matching $\Longrightarrow |V(G)|$ ist gerade

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.

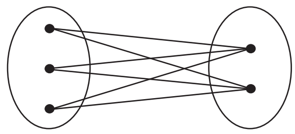
- A, B heißen Partitionsmengen
- vollständig bipartiter Graph $K_{p,q}$: Ein bipartiter Graph (A $\uplus$ B, E) mit $|A|$ = p und $|B|$ = q und xy $\in$ E für alle x $\in$ A und y in B

Beispiele 2.35

1.



2.



Satz 2.36
Ein Graph G ist bipartit $\longleftrightarrow$ G hat keine Kreise ungerader Länge.

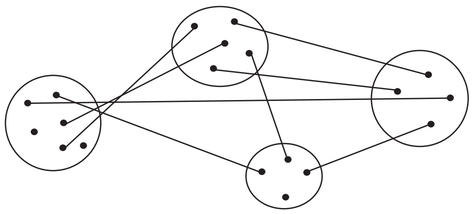
Satz 2.37 (König-Hall)
Sei G=(A $\uplus$ B, E) ein bipartiter Graph. G besitzt ein Matching M mit $|M| = |A| \longleftrightarrow |N(S)| \leq |S|$ für alle S $\subseteq$ A

Beweis:
$\Longrightarrow$ trivial
$\Longleftarrow$ (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 $\setminus V(M) \neq \varnothing$
Wähle a $\in A \setminus V(M)$ und bezeichne U(a) := $\{x \in V(G)|mid$ x ist durch einen M-alternierenden Weg mit a verbunden}
M ist ein Maximum-Matching $\Longrightarrow$ U(a) $\subseteq$ V(M)
Setze A'=(U(a)∩A)∪$\{a\}$ und B'=(U(a)∩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

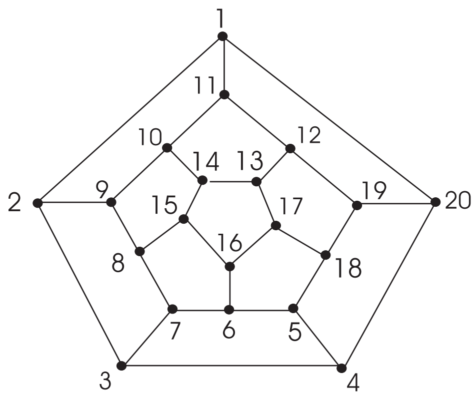
Folgerung 2.39 (König, 1916)
Ein r-regulärer bipartiter Graph läßt sich in r kantendisjunkte perfekte Matchings zerlegen.
Beweisidee: sukzessives Anwenden von Folgerung 2.38

Definition 2.40 (multipatite Graphen)
Ein Graph G=(V,E) heißt k-patit (multipatit), wenn V(G) in k disjunkte Mengen $V_1, V_2, ..., V_k$ zerlegt werden kann, so dass G(V_i) für i=1,...,k Nullgraphen sind.

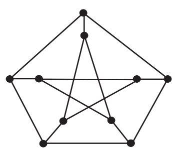


2.5 Hamilton-Graphen

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



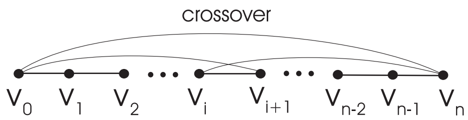
Definition 2.41
Sei G=(V,E).
Ein Kreis C in G heißt Hamilton-Kreis, falls V(C)=V(G).
Ein Weg W in G heißt Hamilton-Weg, falls V(W)=V(G).
Enthält G einen Hamilton-Kreis, so heißt G hamiltonscher Graph.
Enthält G einen Hamilton-Weg, so heißt G semi-hamiltonscher Graph.

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⊆V(G):
κ(G-S)≤ $|S|$ (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)≥n, dann gilt:
G ist hamiltonsch $\Longleftrightarrow$ G+uv ist hamiltonsch.

Beweis: (wichtig)
$\Longrightarrow$ trivial
$\Longleftarrow$ 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:= $\{j \mid 2 \leq j \leq n-1,\ u_j v \in E(G)\}$
⇒ S∩T=∅ (sonst 'crossover') und $|S \cup T|$ ≤n-1<n
d(u)+d(v)=$|S|$+$|T|$-$|S \cup T|$ + $|S \cap T|$ <n ⇒ Widerspruch

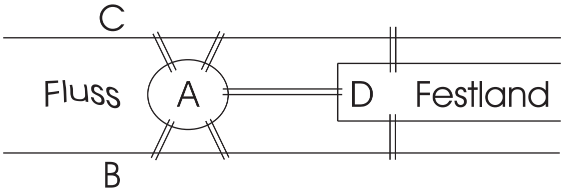
Folgerung 2.45 (Ore, 1960)
Sei G=(V,E) ein Graph mit $|V|$=n.
Gilt für alle nicht adjazentierten Ecken u,v die Ungleichung d(u)+d(v)≥n, so ist G hamiltonsch.
Beweisidee: Kanten hinzufügen ⇒ K_n

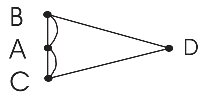
Folgerung 2.46 (Dirac, 1952)
Sei G=(V,E) ein Graph mit $|V|$=n.
Ist d(v)≥ $\frac{n}{2}$ $\forall\ v \in V(G)$, so ist G hamiltonsch.

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

Problem

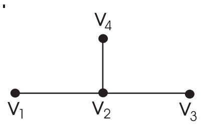




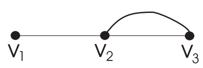
Definition 2.48

- Sei G=(V,E) ein zusammenhängender Graph $x_0x_1...x_k$ 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.

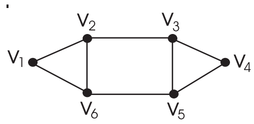
- Ein Kantenzug Z mit E(Z)=E(G) heißt eulerscher Kantenzug.
- Ein geschlossener eulerscher Kantenzug heißt Eulertour.

Definition 2.49

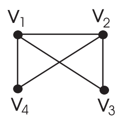
Sei G=(V,E) zusammenhängend mit $|V| \geq 2$.
G heißt semi-eulersch, falls G einen eulerschen Kantenzug enthält.
G heißt eulersch, falls G eine Eulertour enthält.

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 $\Longleftrightarrow$ der Grad jeder Ecke ist gerade

Beweis:
$\Longrightarrow$ trivial
$\Longleftarrow$ Sei z=$x_0x_1...x_t$ ein längster Kantenzug in G. Dann haben wir:

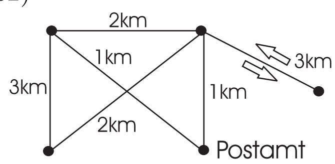
1. $x_t = x_0$
2. z ist eine Eulertour von G

Folgerung 2.52

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

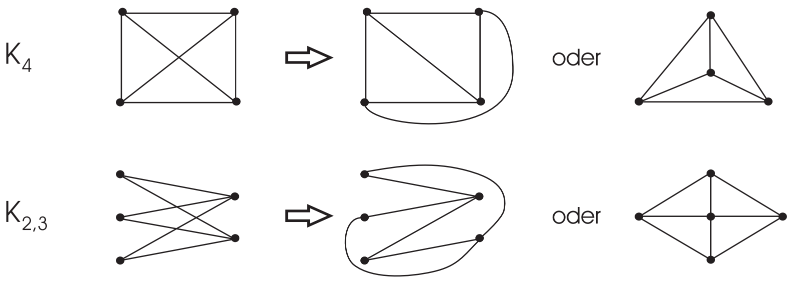
Bemerkung 2.53

- Für eulersche Graphen gibt es einen effizienten Algorithmus (Fleurys 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$\rightarrow$ $\{q \in Q \mid q > 0\}$
  (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?

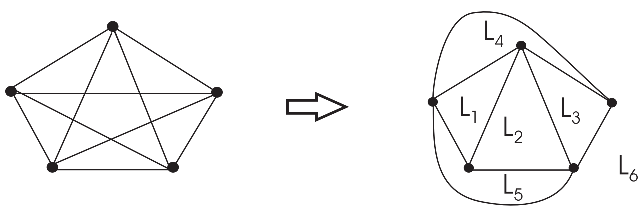


Definition 2.54

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

- G heißt einbettbar in den $\mathbb{R}^2$: wenn ein Paar φ, φ' gibt, so daß gilt:
  φ: V $\rightarrow \mathbb{R}^2$ injektiv
  φ': E $\rightarrow$ J = {bild(e) | e:[0,1] $\rightarrow \mathbb{R}^2$ stetig und injektiv} ; bild(e) = Jordankurve
  mit φ' (uv) = bild(e), e=uv $\in$ E(G)
  und φ(u) = e(0)
  φ(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 $\mathbb{R}^2 \mid \cup_{e \in E}\ \varphi'(e)$ die Gebiete (oder Länder) von (G, φ, φ')

z.B.



l(G) = Anzahl der Länder von G
$l = 6,\ |v| = 5,\ |E| = 9$

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 $\geq |V|$
$\stackrel{Satz\ 2.22}{=}$ 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 Invariation 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:

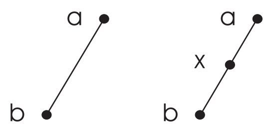
$$|E| \leq 3|V| - 6$$

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

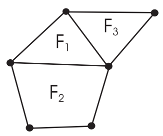
Definition 2.58
Sei G=(V,E) und e=ab $\in$ E(G)
Wir sagen e wird unterteilt, wenn wir zu H eine neue Ecke x hinzufügen und die Kante e durch zwei neue Kanten ax und xb ersetzen.



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.

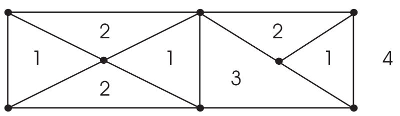
Definition 2.60 (Vierfarbenproblem)
Sei G ein Landkarte

- 

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 $\longrightarrow \{1,\ 2,\ ...\ p\}$ 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



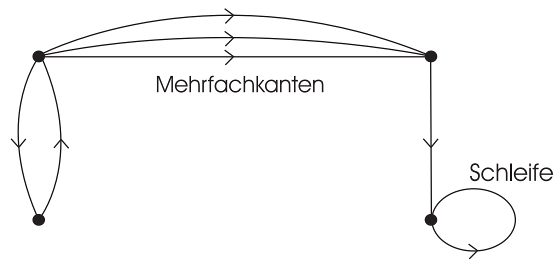
Satz 2.62 (Vierfarbenvermutung, Guthrie 1852)
Jede Landkarte läßt sich mit vier Farben färben

Beweis: (N. Robertson et al. 1997)

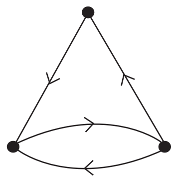
Bemerkung 2.63
1) Bei den Anwendungen planarer Graphen in der Informatik steht der algorithmsiche Aspekt im Vordergrund
Es gibt Verfahren, die in der Zeit O($|V|+|E|$) testen, ob G=(V,E) planar ist, und falls ja, diesen auch in $\mathbb{R}^2$ einbetten. (Bemerkung $\mathbb{R}^2$ S^n)
2) Das Problem der 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)

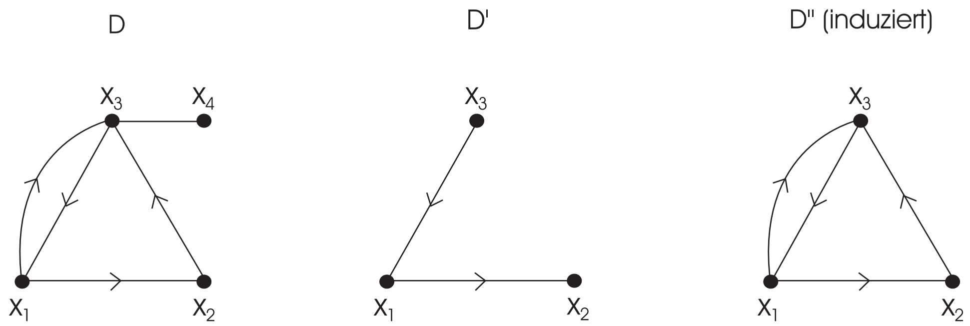


Konvention: Wir werden hier nur die schlichten Digraphen (d.h. die Digraphen ohne Schleifen und Mehrfachbögen) betrachten.



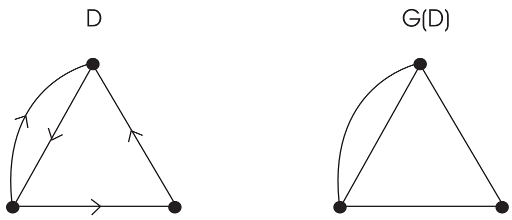
Definition 2.65
Sei D=(V,A) ein Digraph
- $D' = (V', A')$ heißt Teildigraph von D, wenn $V' \subseteq V$ und $A' \subseteq A \cap (V' \times V')$ sind, in Zeichen $D' \subseteq D$
- Ein Teildigraph $D' = (V', A')$ heißt ein von V' induzierter Teildigraph, wenn $A' = A \cap (V \times V')$, in Zeichen $D' = D[V']$

z.B.

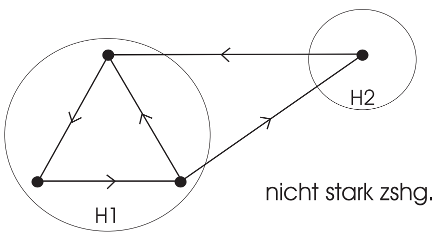


- Orientierte Kantenfolge der Länge p in D
  F := $x_0 x_1 x_2$ ... x_p $\quad$ $x_i \in V(D)$, i=0, 1, ... p
  $x_i x_{i+1} \in A(D)$, i=0, 1, ... p-1
  z.B. in D ist $x_3 x_1 x_2 x_3 x_1 x_3$ eine orientierte Kantenfolge
- orientierter Kantenzug := orientierter Kantenfolge mit paarweise verschiedenen Bögen
  z.B. $x_3 x_1 x_3 x_4$
- orientierter Weg := orientierte Kantenfolge mit paarweise verschiedenen Ecken
  z.B. $x_3 x_1 x_2$
- 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 ∈ V(D) definieren wir:
N^+(x) = $\{y \mid xy \ \in A(D)\}$
N^-(x) = $\{w \mid wx \ \in A(D)\}$
$d^+ = |N^+(x)|, \qquad \delta^+(D) = min\{d^+ \mid x \ \in V(D)\}$
$\qquad\qquad\qquad \Delta^+(D) = max\{d^+ \mid x \in V(D)\}$
$d^- = |N^-(x)|, \qquad \delta^-(D) = min\{d^- \mid x \ \in V(D)\}$
$\qquad\qquad\qquad \Delta^-(D) = max\{d^- \mid x \in V(D)\}$
• Der untergeordnete Graph von D (in Zeichen G(D)) ist G(D) = (V(D), $\{xy \mid xy \ \in A(D)\}$)



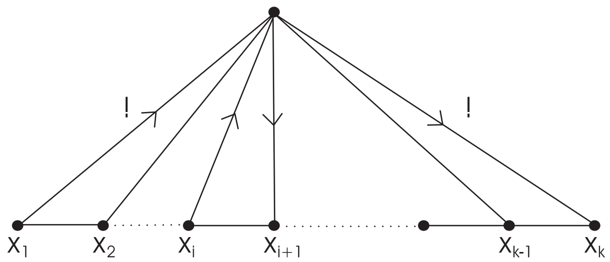
Definition 2.66
Sei G ein Digraph
Eine stark zusammenhängende Komponente H von D ist ein maximaler Teilgraph von D, so daß H für zwei beliebige Ecken u, v ∈ V(H) einen orientierten Weg vin u nach v enthält.
D heißt stark zusammenhängend wenn D nur eine stark zusammenhängende Komponente hat
z.B.



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 = $x_1 x_2$ ... x_k ein längster orientierter Weg in T_n
Annahme: k < n



Sei x $\in$ V(T_n) $\setminus$ V(W)
Dann haben wir $x_1 \longrightarrow x \longrightarrow x_k$
$\Rightarrow \exists i \in \{1, 2,\ ...\ k-1\}$ mit $x_i \longrightarrow x \longrightarrow x_{i+1}$
So ist $x_1 x_2$ ... $x_i x x_{i+1}$ ... 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 einen p-Kreis für alle p $\in \{3, 4,\ ...\ n\}$
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: $M^n = M \times M \times ... \times M$ →M eine n-stellige Operation oder ein n-stelliger Operator.
• n=s(f) heißt die Stelligkeit vom Operator f
• ein zweistelliger Operator jeißt 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 · können wir unterschiedliche Algebren definieren:
• (ℕ,+), (ℕ,+,·)
• (ℤ,·)
• $(x \in \mathbb{N},\ x\ ist\ Quadratwurzel, \cdot)$
denn für x=a^2 und y=b^2 ist xy=$a^2b^2 = (ab^2)$
• $(x \in \mathbb{N},\ x\ ist\ Quadratwurzel, +)$
ist keine Algebra
3. Σ=Menge (Alphabet)
Σ^*=$\{a_1, a_2, ..., a_n \mid a_i \in \Sigma,\ n \in \mathbb{N}_0\}$
$\circ : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ mit $(a_1, ..., a_n) \circ (b_1, ..., b_m) = (a_1...a_nb_1...b_m)$
$\Sigma^*, \circ$ ist eine Algebra
4. U = beliebige Menge
F(U)=$\{f \mid f :\ U \rightarrow U\}$
∘ : Komposition von zwei Funktionen (f∘g)(x))f(g(x)) $\forall x \in$U
(F(U),∘) ist eine Algebra

Definition 3.4 (neutrales Element)
Sei (M,∘) eine Algebra mit einem zweistelligen Operator ∘.
Ein Element e∈M heißt linksneutrales Element für den Operator ∘, falls e∘a=a $\forall a \in M$
Ein Element e∈M heißt rechtsneutrales Element für den Operator ∘, falls a∘e=a $\forall a \in M$
Ein Element e∈M heißt neutrales Element für den Operator ∘, falls e sowohl links- als auch rechtsneutrales Element ist.

Beispiel 3.5
$(\{b, c\}, \circ)$ mit $\begin{array}{c|cc} \circ & b & c \\ \hline b & b & b \\ c & c & c \end{array}$ ⇒ b und c sind rechtsneutrale Elemente ⇒ $(\{b, c\}, \circ)$ besitzt kein n.E.

Lemma 3.6
Sei (M,∘) eine Algebra vom Typ (2). Dann gilt:
Ist c ein linksneutrales Element un d ein rechtsneutrales Element, so ist c=d.

Beweis: 1. c·d=d und 2. c·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. ·

Definition 3.8 (inverses Element)
Sei (M,∘) eine Algebra vom Typ (2) und mit neutralem Element e.
Ein Element x∈M heißt linksinverses Element von a∈M, falls x·a=e
Ein Element x∈M heißt rechtsinverses Element von a∈M, falls a·x=e
Ein Element x∈M heißt inverses Element (oder Inverse) von a∈M, falls x sowohl ein linksinverses als auch rechtsinverses Element ist.

Definition 3.9 (Halbgruppe)
Eine Algebra A=(M,∘) vom Typ (2) heißt Halbgruppe, falls der Operator ∘ assoziativ ist, also a∘(b∘c)=(a∘b)∘c ∀ a,b,c ∈M

Definition 3.10 (Monoid)
Eine Algebra A=(M,∘) vom Typ (2) heißt Monoid, falls
M1 : A ist assoziativ
M2 : ∃ ein neutrales Element e∈M

Definition 3.11 (Gruppe)
Eine Algebra A=(M,∘) vom Typ (2) heißt Gruppe, falls
G1 : A ist assoziativ
G2 : ∃ ein neutrales Element e∈M
G3 : jedes Element a∈M besitzt ein Inverses

Definition 3.12 (abelsche Algebra)
Eine Halbgruppe (ein Monoid, eine Gruppe) A=(M,∘) heoßt abelsch, falls ∘ kommutativ ist.

Definition 3.13 (Ring)
Eine Algebra A=(M,⊕,⊙) mit zwei zweistelligen Operatoren ⊕ und ⊙ heißt ein Ring, falls
R1 : (M,⊕) ist eine abelsche Gruppe mit neutralem Element 0∈M
R2 : (M,⊙) ist ein Monoid mit neutralem Element 1∈M
R3 : ⊕ und ⊙ sind distributiv, also
a⊙(b⊕c) = (a⊙b)⊕(a⊙c) und
(b⊕c)⊙a = (b⊙a)⊕(c⊙a) ∀ a,b,c ∈M

Definition 3.14 (Körper)
Eine Algebra A=(M,⊕,⊙) mit zwei zweistelligen Operatoren ⊕ und ⊙ heißt Körper, falls
K1 : (M,⊕) ist eine abelsche Gruppe
K2 : (M,⊙) ist eine abelsche Gruppe
K3 : a⊙(b⊕c) = (a⊙b)⊕(a⊙c) ∀ a,b,c ∈M

Definition 3.15 (boolesche Algebra)
Eine Algebra A=(M,⊕,⊙,¬) vom Typ (2,2,1) heißt boolesche Algebra, falls
B1 : (M,⊕) ist ein abelscher Monoid
B2 : (M,⊙) ist ein abelscher Monoid
B3 : für den Operator ≠ gilt : a⊕(≠a)=1 und a⊙(≠a)=0 ∀a∈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]={$\sum\limits_{k=0}^{n} a_k x^k \mid a_k \in K\}$ (Menge der Polynome über K)
  ist ein kommutativer Ring (Polynomring)
- K[[x]]={$\sum\limits_{n=0}^{\infty} a_n x^n \mid a_n \in K\}$ ist ein kommutativer Ring
  mit Null 0=0x^0 und Eins 1=1x^0
- $K^{n\times n} = \{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{1n} & \cdots & a_{nn} \end{pmatrix} \mid a_{ij} \in K,\ 1 \leq i,j \leq n\}$

  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 Unteralgebra, 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 Unteralgbera von A (in Zeichen U$\leq$A), falls die Operatoren f_i abgeschlossen sind, d.h.:
$f_i(U^{n_i}) \subseteq U \ \forall i \in I$
$f_i(U^{n_i}) = \{f_i(u_1, ..., u_n) \mid u_1, ..., u_n \in U\}$

Definition 3.18
- Sei G=(G,$\cdot$) eine Gruppe.
  Eine Unteralgebra 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 Unteralgebra 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 $Z_n = \{1, ..., n-1\}$ und $+_n \ : \ \mathbb{N} \times \mathbb{N} \to \mathbb{Z}_n$ mit $+_n$(a,b)=a+b(mod n)
   z.B. n=5 : $\mathbb{Z} = \{1, 2, 3, 4, 5\}$, $+_5 \ : \ \mathbb{N} \times \mathbb{N} \to \mathbb{Z}_5$ 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: $\bigcap\limits_{j\in I} U_j$ $\leq$A

Definition 3.21
Sei M eine Teilung von einer Algebra A.
$< M >= \cap\{U \mid M \subseteq U \leq A\}$
heißt die von M erzeugte Unteralgebra.

Beispiel 3.22
1) Sei G=(G,·) eine Gruppe und sei g∈G.
$< \{g\} >= \{g \mid i \in \mathbb{Z}\}$ (die von g erzeugte Untergruppe),

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

$< \{g_1, ..., g_n\} >=\{a_1, ..., a_m\}_{m\in\mathbb{N}^0},\ a_j \in \{g_1, ...g_n, g_1^{-1}, ..., g_n^{-n}\}$

Definition 3.23
Seien A=(A,$(f_i)_{i\in I}$) und $\tilde{A} = (\tilde{A}, (\tilde{f}_1)_{i\in I})$ Algebren vom gleichen Typ T=$(n_i)_{i\in I}$, d.h. n_i=s(f_i)=s($\tilde{f}_i$)
Eine Abbildung $\varphi : A \to \tilde{A}$ heißt Homomorphismus von A und $\tilde{A}$, falls für alle i∈I die Operatoren f_i und $\tilde{f}_i$ mit φ vertauschbar sind,
also $\tilde{f}_i(\varphi(a_1), ..., \varphi(a_{n_i})) = \varphi(f_i(a_1, ..., a_{n_i}))\ \forall a_j \in A,\ j = 1, ..., n,\ i \in I$

$$\begin{tikzcd} A^{n_i} \arrow[r, "f_i"] \arrow[d, "\varphi"'] & A \arrow[d, "\varphi"] \\ \tilde{A}^{n_i} \arrow[r, "\tilde{f}_i"] & \tilde{A} \end{tikzcd}$$

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'≤A, dann ist
id : A' → A mit a→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=(ℕ,+), $\tilde{A} = (\mathbb{Z}, +)$, A≤A'
φ : ℕ → ℤ mit n→n ∀n∈ ℕ ist ein Homomorphismus von A nach $\tilde{A}$
2) A=($\sum^*, \circ$) (siehe 3.3), $\tilde{A} = (N^0, +)$
$\varphi : \sum^* \to \mathbb{N}^0$ mit w→ $|w|$ ist ein Homomorphismus von A und $\tilde{A}$
3) Sei K ein Körper und V,W zwei K-Vektorräume (siehe LA2.25)
φ : V→W ist ein Homomorphismus ⇔ φ ist k-linear
(k-kinear: $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ *und* $\varphi(0) = 0$ *und* $\varphi(\alpha v) = \alpha\varphi(v)$)

Definition 3.25
- Seien A=(A,$(f_i)_{i\in I}$) und $\tilde{A} = (\tilde{A}, (\tilde{f}_1)_{i\in I})$ Algebren vom gleichen Typ T=$(n_i)_{i\in I}$
  Eine Abbildung φ : A→ $\tilde{A}$ 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≅ $\tilde{A}$ isomorph ⇔ ∃ ein Isomorphismus von A nach $\tilde{A}$
- Ein Isomorphismus einer Algebra A nach A heißt Automorphismus

Beispiel 3.26
1) A=(ℕ,+), $\tilde{A} = (\{2n \mid n \in \mathbb{N}\}, +)$
$\varphi : \mathbb{N} \to \{2n \mid n \in \mathbb{N}\}$ mit n→2n ∀n∈ ℕ ist ein Isomorphismus von A nach $\tilde{A}$
2) A=($x \in \mathbb{R} \mid x > 0$ (= $\mathbb{R}^+$), ·), $\tilde{A} = (\mathbb{R}, +)$
$\varphi : \mathbb{R}^+ \to \mathbb{R}$ mit x→logx ∀x∈ $\mathbb{R}^+$ ist ein Isomorphismus,
denn für die Logarithmusfunktion gilt: log(xy)=log x + log y ∀x,y∈ $\mathbb{R}^+$

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

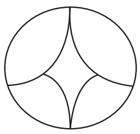
$\circ$	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

φ 1→2, 2→1, 3→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: φ : A ← $\tilde{A} = \varphi^{-1}$

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



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

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

Beispiel 3.29
ℤ und m ∈ ℕ
$\sim_m$: a $\sim_m$ b ⇔ m | a-b d.h. a ≡ b (modulo m)

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

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

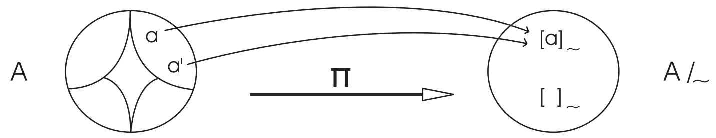
Definition 3.30
Sei A=(A,$(f_i)_{i \in I}$) eine Algebra. Eine Äquivalenzrelation ∼ auf A heißt eine Kongurenzrelation auf A, wenn ∼ mit allen f_i verträglich ist, d.h.

$$a_1 \sim a_1', \; ... \; a_{n_i} \sim a_{n_i}' \to f_i(a_1 \; ... \; a_{n_i}) \sim f_i(a_1' \; ... \; a_{n_i}')$$

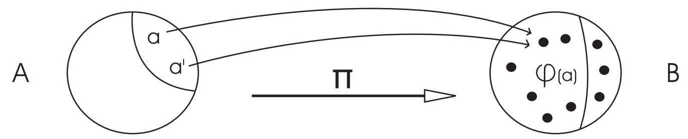
Beispiel 3.31
Sei G=(G, $\cdot$) eine Gruppe und sei $\sim$ eine Äquivalenzrelation auf G.
$\sim$ Kongurenz $\Leftrightarrow a \sim a', b \sim b' \rightarrow a \cdot b \sim a' \cdot b'$ mit $a^{-1} \sim (a')^{-1}$

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 Kongurenzrelation auf A

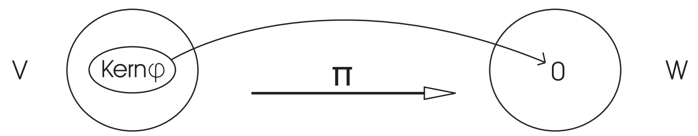
a) Für jedes a $\in$ A bezeichnen wir mit $[a]_\sim = \{a' \in A \mid a' \sim a\}$ die Äquivalenzklasse von a
Dann wird die Menge der Äquivalenzklassen A/$\sim$:= $\{[a]_\sim \mid a \in A\}$ eine Algebra vom Typ $(n_i)_{i \in I}$ mit $\tilde{f}([a_1]_\sim, [a_2]_\sim, \ \ldots\ , [a_{n_i}]_\sim) := [f_i(a_1 \ \ldots\ a_{n_i}]_\sim$ und
$\pi_\sim : A \rightarrow$ A/$\sim$ mit $a \rightarrow [a]_\sim$ ist ein surjektiver Homomorphismus (Epismorphismus)



b) Ist $\varphi : A \rightarrow B$ ein Homomorphismus, so wird dann $a \sim a' \leftrightarrow \varphi(a) = \varphi(a')$
eine Kongurenzrelation 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 $\forall v, v' \in V$
$v \sim v' \Leftrightarrow \varphi(v) = \varphi(v')$
$\Leftrightarrow \varphi(v) - \varphi(v') = O$
$\Leftrightarrow \varphi(v - v') = 0$ (da φ k-linear)
$\Leftrightarrow v - v' \in Kern\ \varphi \leq V$
also, $[v]_\sim = v + Kern\ \varphi \quad \forall v \in V$
$[o]_\sim = Kern\ \varphi$



3.3 Ringe und Ideale

Erinnerung an Definition 3.13
Eine Algebra R=(R,+,·) vom Typ (2,2) ist ein Ring, falls,
• (R,+) eine abelsche Gruppe mit $0 \in$ R
• (R, ·) ein Monoid mit $1 \in$ R
• + und · sind distributiv

Lemma 3.34
1) a · 0 = 0 · a = 0 $\forall a \in$ R
2) a · (-b) = (-a) · b = - (a · b) $faa, b \in$ R
3) -(-a) = a $\forall a \in$ R
4) -(a+b) = (-a) + -(b) $\forall a, b \in$ 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 $\in [o]_\sim$. 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,+,·= 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 · u $\in$ I und u · a $\in$ I

Satz 3.36
Ist $\sim$ eine Kongurenzrelation 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 Kongurenzrelation definiert
(Dabei ist $[o]_\sim = I$, $[a]_\sim = a + I$)
Schreibweise: R/I := R/$\sim$
Beweis: (Übung)

Satz 3.37
Ist R ein kommutativer Ring und d $\in$ R beliebig. Dann gilt:
1) R·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, ·) d.h. $\exists d' : dd' = 1$
Beweis: (Übung)

Beispiel 3.38 (vgl. Beispiel 3.29)
R=(ℤ,+,·) und m $\in N$, $\sim = \sim_m$
Dann ist mℤ $\trianglelefteq$ ℤ und 1ℤ = ℤ
Konvention: In einem kommutativen Ring schreibt man $\underbrace{a + a + \ \dots \ + a}_{k-mal} = k \cdot a$

Beispiel 3.39
Zeigen Sie: Keine ganze Zahl der Form 7 + n·8 ist die Summe von 3 Quadraten in $\mathbb{Z}$ für n $\in \mathbb{Z}$
Beweis: (Indirekt)
Annahme: z = 7 + n·8 = $a^2 + b^2 + c^2$ für a,b $\in \mathbb{Z}$
Betrachte: $\varphi : \mathbb{Z} \to \mathbb{Z}_8, \quad z \to [z]_8$ (φ Homomorphismus)
$\Rightarrow \varphi(z) = \varphi(a^2) + \varphi(b^2) + \varphi(c^2) = \varphi(a)^2 + \varphi(b)^2 + \varphi(c)^2 = [7]_8$ wobei $\varphi(a), \varphi(b), \varphi(b) \in \mathbb{Z}_8$

In $\mathbb{Z}_8$:

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

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 $\supseteq$ Integrittsbereich $\supseteq$ 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 · q mit 1 < p,q < m, dann ist
$[p]_m \cdot [q]_m = [p \cdot q]_m = [m]_m = [0]_m = 0$ in $\mathbb{Z}_m$, aber: $[p]_m \neq 0$ und $[q]_m \neq 0$, weil $1 < p \cdot q < m$

Definition 3.40
Sei R=(R,+,·) ein kommutativer Ring. Sind a $\neq$ 0 und b $\neq$ 0, aber a · b = 0, so heißt a und b Nullteiler.
R heißt Integritätsbereich, falls R keine Nullerteiler 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 m nicht Primzahl

Definition 3.42
Sei R ein Integritätsbereich.
1) a | b $\Leftrightarrow \exists c \in R, \quad$ b = a · c (a teilt b)
   (a $\nmid$ b $\Leftrightarrow \nexists c \in R, \quad$ b = a · c)
2) d $\in$ R heißt ein gröster gemeinsamer Teiler von a, b $\in$ R (in Zeichen: d $\in$ ggT(a,b)), wenn
   - d | a und d | b
   - (c | a und c | d) $\Rightarrow$ c | d

Bemerkung 3.43
Sei R=(R,+,·) 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. ggT(4,10) = {-2,2}
2) Ist u $\in$ R eine Einheit in R, so gilt auch u | a für alle a $\in$ R, denn a=u(u^{-1}a)

3) d $\in$ ggT(a,b) in R und u $\in R^*$ $\Rightarrow u \cdot d \in$ ggT(a,b), denn umgekehrt kann man zeigen:
   d, $d' \in$ ggT(a,b) $\Rightarrow d'$ = ud für ein u $\in R^*$
4) Guo: Nicht in jedem Integritätsbereich gilt ggT(a,b)={1}
   Bemerkung: = nicht jede Ampel ist immer Rot!?
   Richtig?: In keinem Integritätsbereich gilt ggT(a,b) $\neq \varnothing$ 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:
a) I ist ein Integritätsbereich
b) I^*={-1,1}
c) $|\alpha|^2$=4 $\Rightarrow \alpha$ ist irreduzibel
d) 4 = 2·2 = (1+$\sqrt{-3}$)(1-$\sqrt{-3}$) zwei verschiedene Primfaktorzerlegungen von 4 in I
Frage: Welche Integirtätsbereiche 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
1) a = $p_1 \cdot \ ... \ \cdot p_r$, p_i irreduzibel
2) a = $q_1 \cdot \ ... \ \cdot q_s$, 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, ... s

Bemerkung 3.48
Hat a $\in$ R eine eindeutige Zerlegung, so ist a $\in$ R$\setminus(\{0\} \cup R^*)$ denn:
$0 = a_1 \cdot \ ... \ \cdot a_\alpha \Rightarrow \exists a_i = 0$, aber 0 ist nicht irreduzibel
u = $a_1 \cdot \ ... \ \cdot a_\beta \Rightarrow 1 = a_1(\underbrace{u^{-1}a_2 \cdot \ ... \ \cdot a_\beta}_{a^{-1}})$, aber Einheit ist nicht irreduzibel

Zwei spezielle Ringe: Haupidealringe $\supseteq$ 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$\backslash\{0\} \rightarrow \mathbb{N}_0$
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 δ: R $\rightarrow \mathbb{N}_0$

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

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

a = q $\cdot$ b + r mit grad(r) < grad(b)
$x^5 + x^3 + 1 = (2x^3 + x)(\frac{1}{2}x^2 + \frac{1}{4}) + (-\frac{1}{4}x + 1)$

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

Satz 3.53
Ein Euklidischer Ring R ist ein Hauptidealring. Somit hat jedes Element a $\in$ R$\backslash(\{0\} \cup R^*)$ in R eine eindeutige Primfaktorzerlegung.

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

Folgerung 3.54
In $\mathbb{Z}$ hat jedes a$\in \mathbb{Z}\backslash\{0\}$ eine eindeutige Primfaktorzerlegung in der Form a=$up_1...p_k$, 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}...p_k^{t_k}$, wobei $p_1 < p_2 < ... < p_k$ Primzahlen sind und $t_1, ..., t_k \in \mathbb{N}$

Satz 3.56
Es gibt unendlich viele Primzahlen.

Beweis (indirekt):
Annahme: $p_1, ..., p_k$ sind alle Primzahlen, k$\in \mathbb{N}$
Setze n=$p_1...p_k + 1$ ($\otimes$) $\Rightarrow$ n ist keine Primzahl $\Rightarrow$ n=$p_{n_1}^{t_1}...p_{n_s}^{t_s}$ mit $p_{n_1} < ... < p_{n_s}$ Primzahlen, $t_i \in \mathbb{N}$ ($\otimes\otimes$) $\overset{\otimes}{\Longrightarrow} p_{n_1} \mid n - 1 \overset{\otimes\otimes}{\Longrightarrow} \Longrightarrow$ unmöglich (Widerspruch)

Satz 3.57 (Primzahlsatz)
$\forall n \in \mathbb{N}$ gilt: $\sharp$ der Primzahlen $\leq$ n, wobei $\sharp$ 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 √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:

$$n\ Primzahl \iff a^{n-1} \equiv 1 (mod\ n)\ \forall a \in \mathbb{Z}_n \backslash \{0\}$$

Definition 3.60
φ: $\mathbb{N} \rightarrow \mathbb{N}$ mit φ(n)=$|\mathbb{Z}_n^*|$
heißt eulersche φ-Funktion, wobei $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \backslash \{0\} \mid ggT(n,a) = 1\}$

Lemma 3.61
Ist n=$p_1^{t_1}...p_k^{t_k}$, $p_1 < ... < p_k$ Primzahlen, so gilt folgendes:

$$\varphi(n) \ = \ \prod_{i=1}^{k} (p_i - 1) p_i^{t_1 - 1}$$

Satz 3.62 (Euler)
$\forall n \in \mathbb{N}$ mit n$\geq$2 gilt: $a^{\varphi(n)} \ \equiv \ 1 (mod\ n)$ $\forall$a$\in \mathbb{Z}_n^+$

Bemerkung: Satz 3.62 $\overset{n\ Primz.}{\Longrightarrow}$ Satz 3.59

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

Beispiel ggT(729,153)
1. Primfaktorzelegung
   729 = 3^6 und 153 = $3^2 \cdot 17 \Longrightarrow$ 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$\in$ggT(729,153)
$\Rightarrow$ d$\in$ggT(117,153)
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:

$$ggT(m,n) \ = \ ggT(n\ mod\ m, m)$$

Beweis: Übung

Satz 3.64 (Euklidischer Algorithmus)
Seien $a_0, a_1 \in \mathbb{N}$ mit $a_0 \geq a_1$
Man bestimmt sukzessiv $a_i, q_i \in \mathbb{N}$
$a_0 \ = \ q_1 a_1 + a_2$ mit $0 \leq a_2 \leq a_1$
$a_1 \ = \ q_2 a_2 + a_3$ mit $0 \leq a_3 \leq a_2$
$\vdots$
$a_{k-2} = q_{k-1} a_{k-1} + a_k$ mit $0 \leq a_k \leq a_{k-1}$
$a_{k-1} = q_k a_k + 0$
Dann gilt a_k=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∈K[x]$\setminus\{0\}$ eine eindeutige Zerlegung
(bis auf Reihenfolge der Faktoren) der Form:
f=u$f_1 f_2 ... f_r$, u∈ K^* und f_i irreduzibel und normiert.

Beweis: Beispiel 3.52(2) + Satz 3.53

Satz 3.67
Es sei (R,δ) ein Euklidischer Ring und 0$\neq f$ ∈R, so ist:
$R/_{fR}= \{[g]_f \mid g \in R \;\; f(g) < \delta(f) \cup \{0\}\}$, wobei $[g]_f = g + fR = \{g + fZ \mid Z \in \mathbb{R}\}$
Es ist $R/_f R$ Körper ⇔ f ist irreduzibel.

Beispiel 3.68
Sei K=$\mathbb{Z}_2$ ein Körper. $(\mathbb{Z}_2[x], \delta)$ mit $\delta(g) = grad(g)$ für g∈ $\mathbb{Z}_2[x]$ ist ein euklidischer Ring.

Gegeben ist f=$x^3 + x + 1 \in \mathbb{Z}_2[x]$, dann ist f irreduzibel
$\mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]} = \{[a_0 + a_1 x + a_2 x^2]_f \mid a_0 a_1 a_2 \in \mathbb{Z}_2\}$ ist ein Körper mit 8 Elementen, die durch 3 Bits dargestellt werden.
$[a_0 + a_1 x + a_2 x^2]_f \ \sim \ a_0 a_1 a_2$

α=$[x]_f \ \sim$ 010
α^2=$[x^2]_f \ \sim$ 001
α^3=$[x+1]_f \ \sim$ 110, denn $x^3 = x + 1 + (x^3 + x + 1)1$
α^4=$\alpha^3\alpha$=$[x^2 + x]_f \ \sim$ 011
α^5=$\alpha^4\alpha$=$[x^3 + x^2]_f$=$[x^2 + x + 1]_f \ \sim$ 111
α^6=$\alpha^5\alpha$=$[x^3 + x^2 + x]_f$=$[x^2 + 1]_f \ \sim$ 101
α^7=$\alpha^6\alpha$=$[x^3 + x]_f$=$[1]_f \ \sim$ 100
α^8=α

Bemerkung 3.69
Ist α^i=β, 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) $(Z_2, +_2, \cdot_2)$
wobei $+_n: \ a +_n b = (a+b) mod\ n$ und $\cdot_2: \ a \cdot_2 b = (ab) mod\ n$
2) $(Z_2[x]/_{fZ_2[x]}, +_f, \cdot_f)$ mit f=x^3+x+1
wobei $+_f: \ g +_f h = (g+h) mod\ f$ und $\cdot_f: \ g \cdot_f h = (gh) mod\ f$
$|(Z_2[x]/(x^3+x+1)Z_2[x])| \ = \ |\{(a_0+a_1x+a_2x^2)_f \mid a_o, a_1, a_2 \in Z_2\}|$
$= |\{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}|$=$2^3$
Aus Satz 3.67 erhalten wir sofort:

Folgerung 3.70
1) $(Z_n, +_n, \cdot_n)$ 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 $\Rightarrow$ grad(g)=0 oder 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, 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 $K^* = <a> = \ \{1, a, a^2, \ ...\ a^{|k|-2}\}$
z.B. $(\mathbb{Z}_2[x]/(x^3+x+1)\mathbb{Z}_2[x])^* = <[x]_f>$ $\quad$ ($<[x]_f>$ = Generator)

Effiziente Implementierung
Sei p eine Primzahl.
k=1 $\quad$ GF(p) $= (\mathbb{Z}_p, +_p, \cdot_p)$
k>1 $\quad$ GF(p^k) $= \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$, $\quad$ f ist irreduzibel mit grad(f)=k
$=: \{\sum_{i=0}^{k-1} a_i x^i \mid a_i \in \mathbb{Z}_p\} \sim a_0a_1 \ ...\ a_{k-1}, \quad a_i \in \mathbb{Z}_p$, $\;$ i=0, 1 ... k-1
d.h. wir können die Elemente in $\mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ in kanonischer Weise durch Zeichenketten $a_0a_1 \ ...\ a_{k-1}$ mit $a_i \in \mathbb{Z}_p$ kodieren.

Addition von zwei Polynomen:
a(x) $\sim \ a_0a_1 \ ...\ a_{k-1}$ +
b(x) $\sim \ b_0b_1 \ ...\ b_{k-1}$ =
c(x) $\sim \ c_0c_1 \ ...\ c_{k-1} \ \ c_i = (a_i+b_i)$ mod 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) $\cdot \sum_{i=0}^{k-1} b_i x^i = a(x) \cdot b_o + x(a(x)b_1 + x(... + x(a(x) \cdot b_{k-2} + xa(x) \cdot b_{k-1})))$

Beispiel 3.73 (Fortsetzung von Beispiel 3.68)
p=2, k=3, f=$x^3 + x + 1 \in \mathbb{Z}_2[x]$ irreduzibel

$\mathbb{Z}_2[x] \backslash (x^3 + x + 1)\mathbb{Z}_2[x]$	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)·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)·b_2	b_2=1, also a(x)·b_2=a(x)	0110
Multipliziere mit x	Shift nach rechts	0011
Berechne Rest mod f	XOR mit f=1101	1110
Addiere a(x)·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)·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) $= x^2$
Test: $(x + x^2)(1 + x + x^2) = x + x^2 + x^3 + x^2 + x^3 + x^4$

$$= x + \underbrace{2x^2}_{mod 2=0} + \underbrace{2x^3}_{mod 2=0} + x^4$$

$$= x + x^4 = x^2 + x(x^3 + x + 1)$$

c) Nach Satz 3.72 gilt es für jedes Polynom t(x) $\in \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ ein $l_t \in \{0, 1, \ ... \ p^k - 2\}$ mit t(x)=α^{l_t}
In Beispiel 3.68 gilt $\alpha = [x]_f$
$a(x) = x + x^2 = \alpha^4, \ b(x) = 1 + x + x^2 = \alpha^5$
Dann gilt a(x)$\cdot_f$b(x) $= \alpha^{l_a} \cdot \alpha^{l_b} = \alpha^{(l_a + l_b) mod \ p^k - 1} = \alpha^4 \cdot \alpha^5 = \alpha^{9 \ mod \ 2^3 - 1} = \alpha^2 = x^2$

Index