Diskrete Strukturen

Andreas Surudo
Andreas.Surudo@post.rwth-aachen.de

30. August 2002

Vorwort

Dieses Skript spiegelt meine Aufzeichnungen aus der Vorlesung „Diskrete Strukturen“ bei Priv.-Doz. Yubao Guo, an der RWTH Aachen im Sommersemester 2002 wieder. Es erhebt keinerlei Anspruch auf Vollständigkeit oder Korrektheit und dient schon gar nicht als Ersatz für die Vorlesung. Falls ihr Fehler findet (und das werdet ihr) oder merkt, daß irgendetwas fehlt, dann mailt mir bitte. Ich habe (bzw. LaTeXhat) die Numerierung ein wenig geändert, da Y. Guo es nicht bewerkstelligt hat seine Numerierung durchgehend zu gestalten. Desweiteren habe ich die Definition, Sätze, etc. mit sinnvolleren Namen versehen.

Inhaltsverzeichnis

Kapitel 1

Abzählungen, Rekursionen, erzeugende Funktionen

1.1 Elementare Zählprinzipien

$\mathbf{M}$: endliche Menge
$|\mathbf{M}|$ = Anzahl der Elemente von $\mathbf{M}$
$|\mathbf{M}|$ = $n, n \in \mathbb{N} = \{1, 2, \dots\} \Leftrightarrow$ Es gibt Bijektion $f : \mathbf{M} \to \{1, 2, \dots, n\}$
Eine Menge $\mathbf{M}$ mit $|\mathbf{M}| = n$ heißt n-Menge
$|\mathbf{M}|$ = $0 \Leftrightarrow \mathbf{M} = \emptyset$

1.1 Lemma

Seien $\mathbf{A}$ und $\mathbf{B}$ zwei Mengen

1. $|\mathbf{A}| = |\mathbf{B}| \Leftrightarrow$ Es gibt eine Bijektion $f : \mathbf{A} \to \mathbf{B}$
2. $|\mathbf{A} \dot\cup \mathbf{B}| = |\mathbf{A}| + |\mathbf{B}|$ $\mathbf{A} \dot\cup \mathbf{B}$ heißt die disjunkte Vereinigung von $\mathbf{A}$ und $\mathbf{B}$, d. h. es gilt $\mathbf{A} \cap \mathbf{B} = \emptyset$
3. $|\mathbf{A} \times \mathbf{B}| = |\mathbf{A}| \cdot |\mathbf{B}|$ $\mathbf{A} \times \mathbf{B} = \{(a, b) | a \in \mathbf{A} \wedge b \in \mathbf{B}\}$ heißt das kartesische Produkt von $\mathbf{A}$ und $\mathbf{B}$

1.2 Folgerung

Seien $\mathbf{A}$ und $\mathbf{B}$ zwei endliche Mengen

$Abb(\mathbf{A}, \mathbf{B}) := \mathbf{B}^{\mathbf{A}}$ = Menge aller Abbildungen von $\mathbf{A}$ nach $\mathbf{B}$. Dann gilt $|\mathbf{B}^{\mathbf{A}}| = |\mathbf{B}|^{|\mathbf{A}|}$.

Beweis

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

$\mathbf{B}^{\mathbf{A}} \to \underbrace{\mathbf{B} \times \mathbf{B} \times \cdots \times \mathbf{B}}_{n\text{-mal}}$ ist eine Bijektion

$$\Rightarrow |\mathbf{B}^{\mathbf{A}}| = \underbrace{|\mathbf{B} \times \mathbf{B} \times \cdots \times \mathbf{B}|}_{n\text{-mal}} \overset{\text{Lemma 1.1.3}}{=} \underbrace{|\mathbf{B}| \cdot |\mathbf{B}| \cdot \cdots \cdot |\mathbf{B}|}_{n\text{--mal}} = |\mathbf{B}|^n = |\mathbf{B}|^{|\mathbf{A}|}$$

1.3 Definition (*Permutation*)

Sei $\mathbf{A}$ eine Menge
$f : \mathbf{A} \to \mathbf{A}$ heißt *Permutation* von $\mathbf{A}$, wenn f bijektiv ist.

1.4 Lemma

Sei $s_n := \{\sigma | \sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}\ bijektiv\} := Sym\{1,2,3,\ldots,n\}$ (symmetrische Gruppe vom Grad n).
Dann gilt $|s_n| = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n!$
(Bem.: $n!$ = Anzahl der Möglichkeiten eine n-Menge $\mathbf{A}$ anzuordnen)

1.5 Satz

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

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

Beweis

1. Sei $\mathbf{B} \subseteq \mathbf{A}$. $\chi_{\mathbf{B}} : \mathbf{A} \to \{0,1\}$,
   $\chi_{\mathbf{B}}(x) = \begin{cases} 1 \text{ für } x \in \mathbf{B} \\ 0 \text{ sonst} \end{cases}$ heißt charakteristische Funktion von $\mathbf{B}$, also $\mathbf{B} = \{x \in \mathbf{A} | \chi_{\mathbf{B}} = 1\}$
   $\Rightarrow$ Es gibt eine Bijektion $f : \mathcal{P}(\mathbf{A}) \to \{0,1\}^{\mathbf{A}}$ mit $f(\mathbf{B}) = \chi_{\mathbf{B}} \quad \forall\ \mathbf{B} \subseteq \mathbf{A}$
   $\Rightarrow |\mathcal{P}(\mathbf{A})| = |\{0,1\}|^{\mathbf{A}} \overset{\text{Folgerung1.2}}{=} |\{0,1\}|^{|\mathbf{A}|} = 2^n$
2. zu zeigen: $|\mathcal{P}(\mathbf{A})| = 2^n$, wenn $|\mathbf{A}| = n$
   $|\mathcal{P}(\mathbf{A})| = \sum_{k=0}^{n} |\mathcal{P}_k(\mathbf{A})| = \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} \cdot 1^k \cdot 1^{n-k} \overset{\text{Binomialsatz}}{=} (1+1)^n = 2^n$

1.6 Definition

Sei $\mathbf{A}$ eine Menge und $k \in \mathbb{N}$ mit $k \subseteq |\mathbf{A}|$
$P_k(\mathbf{A}) = \binom{A}{k} =: \{\mathbf{B} \subseteq \mathbf{A} \mid |\mathbf{B}| = k\}$ = Menge aller k-Teilmengen von $\mathbf{A}$

1.7 Bemerkung

$\mathcal{P}(\mathbf{A}) = \dot{\bigcup_{k=0}^{n}} \mathcal{P}_k(\mathbf{A}) \quad n = |\mathbf{A}|$
$\overset{\text{Lemma 1.1.2}}{\Rightarrow} |\mathcal{P}(\mathbf{A})| = |\mathcal{P}_0(\mathbf{A})| + |\mathcal{P}_1(\mathbf{A})| + \ldots + |\mathcal{P}_n(\mathbf{A})| = \sum_{k=0}^{n} |\mathcal{P}_k(\mathbf{A})|$

1.8 Lemma

Sei $\mathbf{A}$ eine Menge mit $|\mathbf{A}| = n$. Dann gilt $|\mathcal{P}_k(\mathbf{A})| = \binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$

Beweis

$|\{(b_1, b_2, \ldots, b_k) \quad b_i \in \mathbf{A} \quad b_i \neq b_j \text{ für } i \neq j\}| = n \cdot (n-1) \cdot \cdots \cdot (n-k+1)$
Es gibt $k!$ Anordnungen von $b_1, b_2 \ldots, b_k \Rightarrow |\mathcal{P}_k(\mathbf{A})| = \frac{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1)}{k!} = \binom{n}{k}$

1.9 Satz (*Pascal-Dreieck*)

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

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

Beweis

1. (durch Nachrechnen)

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

2. (kobinatorischer Beweis)

   $\binom{n}{k}$= Anzahl der k-Teilmengen von $\mathbf{A}$ mit $|\mathbf{A}| = n$
   $P_k(\mathbf{A}) = \{\mathbf{M} \subseteq \{a_1, \ldots, a_n\} \,|\, |\mathbf{M}| = k\}$ partitionieren
   $= \{\mathbf{M}' \cup \{a_n\} \,|\, \mathbf{M}' \subseteq \{a_1, \ldots, a_{n-1}\} \text{ und } |\mathbf{M}'| = k-1\} \,\dot\cup\, \{\mathbf{M}'' \subseteq \{a_1, \ldots, a_{n-1}\} \,|\, |\mathbf{M}''| = k\}$
   $\Rightarrow \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$

Die folgende Abbildung zeigt das *Pascal-Dreieck* für $n = 0, 1, \ldots, 4$

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

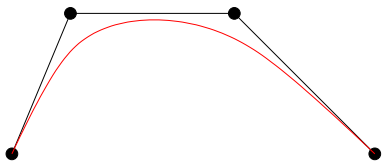
1.10 Satz (*Vandermond'sche Identität*)

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

Beweis

Sei $\mathbf{A}$ eine Menge mit $|\mathbf{A}| = n+m$, also $\mathbf{A} = \mathbf{B} \,\dot\cup\, \mathbf{C}$ mit $|\mathbf{B}| = n$ und $|\mathbf{C}| = m$
$\binom{A}{k}_l := \{x \subseteq A \,|\, |x| = k \text{ und } |x \cap \mathbf{B}| = l\}, l = 0, 1, \ldots, k$
Dann gilt: $\binom{A}{k} = \dot\bigcup_{l=0}^{k} \binom{A}{k}_l \Rightarrow \binom{m+n}{k} = |\binom{A}{k}| = \sum_{l=0}^{k} |\binom{A}{k}_l| = \sum_{l=0}^{k} \binom{n}{l}\binom{m}{k-l}$

Bezierkurven (Anwendung von Satz 1.9 und Satz 1.10 in der Computergrafik)



Bezierkurve

Freiformkurve - eine gewünschte Kurve durch möglichst wenige Punkte möglichst gut zu beschreiben

- Splines (auf Polynomen beruhend)
- Bezierkurve
  Stützstellen : $P_1, P_2, \ldots, P_n$
  $P(t) := \sum_{i=1}^{n} B_{n,i}(t) \cdot P_{i,t} \in [0,1]$
  Wobei $B_{n,i}(t) = \binom{n}{i} t^i (1-t)^{n-i}$ ←Bernsteinpolynom

Aus Satz 1.9 folgt die Rekursionsgleichung $B_{n,i}(t) = t \cdot B_{n-1,i-1}(t) + (1-t) \cdot B_{n-1,i}(t)$ Es liefert eine effiziente Berechnung der Bezierkurven.

1.11 Lemma (*Doppeltes Abzählen*)

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

s_1	:	$(s_1,t_{1,1})$	$(s_1,t_{1,2})$	$\cdots$	t_1	:	$(t_1,s_{1,1})$	$(t_1,s_{1,2})$	$\cdots$
s_2	:	$(s_2,t_{2,1})$	$\ddots$	$\ddots$	t_2	:	$(t_2,s_{2,1})$	$\ddots$	$\ddots$
$\vdots$	:	$\vdots$	$\ddots$	$\ddots$	$\vdots$	:	$\vdots$	$\ddots$	$\ddots$
s_n	:	$(s_n,t_{n,1})$	$\cdots$	$\ddots$	t_n	:	$(t_n,a_{n,1})$	$\cdots$	$\ddots$
s_i	:	$(s_i,t_{i,1})$	$(s_i,t_{i,2})$	$\cdots$	t_i	:	$(t_i,s_{i,1})$	$(t_i,s_{i,2})$	$\cdots$

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

1.12 Satz (*Schubfachprinzip*)

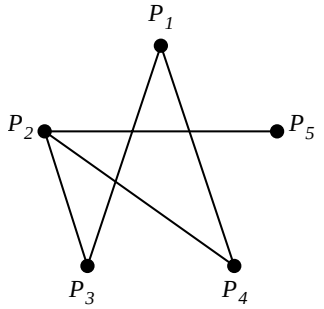
Ist $f : \mathbf{X} \to \mathbf{Y}$ eine Abbildung und gilt $|\mathbf{X}| > |\mathbf{Y}|$, so gibt es ein $y \in \mathbf{Y}$ mit $|f^{-1}(y)| \geq 2$.

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

1.13 Beispiel

1. In jeder Gruppe von 13 Personen befinden sich zwei, die im selben Monat Geburtstag haben.

2. In jeder Gruppe $\mathbf{P}$ von Personen gibt es zwei Personen, die die gleiche Anzahl von Personen in $\mathbf{P}$ kennen (Annahme: die Relation „kennen“ ist symmetrisch)



Beweis

Setze $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$ $\quad f : \mathbf{P} \to \{0, 1, 2, \ldots, n-1\}$

Fall 1: $\exists P_i \in \mathbf{P}$ mit $f(p_i) = 0 \quad \Rightarrow \quad f(p_j) \neq n-1 \quad \forall p_j \in \mathbf{P}|\{p_i\}$
d. h. $f(p) \subseteq \{\underbrace{0, 1, 2, \ldots, n-2}_{n-1 \text{ Zahlen}}\}$

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

Somit gilt $|\mathbf{P}| > |f(p)|$

Nach dem Suchubfachprinzip gibt es mindestens zwei Personen p_l und p_k mit $f(p_l) = f(p_k)$

1.14 Satz (*verallgemeinertes Schubfachprinzip)*

Ist $f : \mathbf{Y} \to \mathbf{Y}$ eine Abbildung, so gibt es ein $y \in \mathbf{Y}$ mit $|f^{-1}(y)| \geq \left\lceil \frac{|x|}{|y|} \right\rceil$.

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

Beweis („indirekt“)

Annahne: $\forall y \in \mathbf{Y} \quad |f^{-1}(y)| \leq \left\lceil \frac{|x|}{|y|} \right\rceil - 1$
$|x| = |\dot{\bigcup} f^{-1}(y)| = \sum\limits_{y \in Y} |f^{-1}(y)| \leq \cdots \leq |y| \cdot \left[\left(\frac{|x|-1}{|y|} + 1 \right) - 1 \right] = |x| - 1$

Rückblick auf Lemma 1.1 2) und 1.1 3)

$|\mathbf{A} \times \mathbf{B}| = |\mathbf{A} \cdot \mathbf{B}|$

- $\mathbf{M} = \mathbf{A}_1 \times \mathbf{A}_2 \times \ldots \times \mathbf{A}_n \Rightarrow |\mathbf{M}| = |\mathbf{A}_1| \cdot |\mathbf{A}_2| \cdot \cdots \cdot |\mathbf{A}_n| = \prod\limits_{i=1}^{n} |\mathbf{A}_i|$
  Seien $\mathbf{A}$ und $\mathbf{B}$ zwei disjunkte Mengen, so gilt $|\mathbf{A} \dot{\cup} \mathbf{B}| = |\mathbf{A}| + |\mathbf{B}|$
- Seien $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ paarweise disjunkte Mengen, d. h. $\mathbf{A}_i \cap \mathbf{A}_j = \emptyset$ für $i, j \in \{1, 2, \ldots, n\}$ mit $i \neq j$ und $\mathbf{S} = \mathbf{A}_1 \cup \mathbf{A}_2 \cup \ldots \cup \mathbf{A}_n = \bigcup\limits_{i=1}^{n} \mathbf{A}_i \Rightarrow |\mathbf{S}| = |\mathbf{A}_1| + |\mathbf{A}_2| + \ldots + |\mathbf{A}_n| = \sum\limits_{i=1}^{n} |\mathbf{A}_i|$

Problem: Sei $\mathbf{S} = \mathbf{A}_1 \cup \ldots \cup \mathbf{A}_n$, wobei $\mathbf{A}_1, \ldots, \mathbf{A}_n$ nicht unbedingt paarweise disjunkt sind.
$|\mathbf{S}| = ?$

Triviale Beispiele

- Für zwei Mengen $\mathbf{A}_1$ und $\mathbf{A}_2$ gilt
  $|\mathbf{A}_1 \cup \mathbf{A}_2| = |\mathbf{A}_1| + |\mathbf{A}_2| - |\mathbf{A}_1 \cap \mathbf{A}_2|$
- Für drei Mengen $\mathbf{A}_1, \mathbf{A}_2$ und $\mathbf{A}_3$ gilt
  $|\mathbf{A}_1 \cup \mathbf{A}_2 \cup \mathbf{A}_3| = |\mathbf{A}_1| + |\mathbf{A}_2| + |\mathbf{A}_3| - |\mathbf{A}_1 \cap \mathbf{A}_2| - |\mathbf{A}_1 \cap \mathbf{A}_3| - |\mathbf{A}_2 \cap \mathbf{A}_3| + |\mathbf{A}_1 \cap \mathbf{A}_2 \cap \mathbf{A}_3|$

1.15 Satz (*Prinzip der Inklusion und Exklusion / Siebformel)*

Für endliche Menge $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ gilt
$|\bigcup\limits_{i=1}^{n} \mathbf{A}_i| = \sum\limits_{r=1}^{n} (-1)^{r-1} \sum\limits_{1 \leq i < \ldots < i_c \leq n} |\bigcap\limits_{j=1}^{r} \mathbf{A}_{i,j}|$

Beweis
Sei $a \in \bigcup\limits_{i=1}^{n} \mathbf{A}_i$ beliebig

1. Auf der linken Seite ist a genau einmal gezählt
2. Zu zeigen: Auf der rechten Seite wird a auch genau einmal gezählt

Ausnahme: $a \in \mathbf{A}_{t_j} \quad j = 1, 2, \ldots, l$ und $a \notin \bigcup\limits_{i=1}^{n} \mathbf{A}_i \setminus \bigcup\limits_{j=1}^{l} \mathbf{A}_{t_j}$

Dann wird a in der Summe $\sum\limits_{1 < i_1 < \ldots < i_c \leq n} |\bigcap\limits_{j=1}^{r} \mathbf{A}_{i,j}|$ genau $\binom{l}{r}$ mal gezählt, denn $\{t_1, t_2, \ldots, t_l\}$ enthält genau $\binom{l}{r}$ $r-$Teilmengen.

$$\Rightarrow a \text{ ist auf der rechten Seite } \sum_{r=1}^{l} (-1)^{r-1} \binom{l}{r} = 1 + \left[-1 + \sum_{r=1}^{l} (-1)^{r-1} \binom{l}{r} \right]$$
$$= 1 - \sum_{r=0}^{l} (-1)^r \binom{l}{r} (-1)^r \cdot 1^{l-r}$$

$$\begin{aligned} &= 1 - (-1+1)^l \\ &= 1 \qquad\qquad \text{mal gezählt.} \end{aligned}$$

1.16 Beispiel (*Siebformel*)

Sei $k \in \mathbb{N}$ und $\mathbf{M}_k = \{n \in \mathbb{N} | 1 \leq n \leq 100 \wedge n \text{ teilt } k\}$

Bestimmen Sie $|\mathbf{M}_2 \cup \mathbf{M}_3 \cup \mathbf{M}_5|$ = Anzahl der durch 2, 3 oder 5 teilbaren.

Lösung: $|\mathbf{M}_k| = \left\lfloor \frac{100}{k} \right\rfloor$, die genau k-te natürliche Zahl durch k teilbar ist.

$$\begin{aligned} |\mathbf{M}_2 \cup \mathbf{M}_3 \cup \mathbf{M}_5| &= |\mathbf{M}_2| + |\mathbf{M}_3| + |\mathbf{M}_5| - |\underbrace{\mathbf{M}_2 \cap \mathbf{M}_3}_{\mathbf{M}_6}| - |\underbrace{\mathbf{M}_2 \cap \mathbf{M}_5}_{\mathbf{M}_{10}}| - |\underbrace{\mathbf{M}_3 \cap \mathbf{M}_5}_{\mathbf{M}_{15}}| + |\underbrace{\mathbf{M}_2 \cap \mathbf{M}_3 \cap \mathbf{M}_5}_{\mathbf{M}_{30}}| \\ &= \left\lfloor \tfrac{100}{2} \right\rfloor + \left\lfloor \tfrac{100}{3} \right\rfloor + \left\lfloor \tfrac{100}{5} \right\rfloor - \left\lfloor \tfrac{100}{6} \right\rfloor - \left\lfloor \tfrac{100}{10} \right\rfloor - \left\lfloor \tfrac{100}{15} \right\rfloor + \left\lfloor \tfrac{100}{30} \right\rfloor \\ &= 50 + 33 + 20 - 16 - 10 - 6 + 3 \\ &= 74 \end{aligned}$$

1.2 Mengenpartitionen

1.17 Definition (*Partition*)

Sei $\mathbf{M}$ eine Menge mit $|\mathbf{M}| = n$

- Eine *Partition* $\mathbf{P}$ von $\mathbf{M}$ ist eine Zerlegnung von $\mathbf{M}$ in eine Vereinigung von disjunkten nichtleeren Teilmengen
- Gilt $\mathbf{P} = \mathbf{A}_1 \dot\cup \mathbf{A}_2 \dot\cup \cdots \dot\cup \mathbf{A}_k$ mit $\mathbf{A}_i \not\subseteq \emptyset$ für $i \in \{1, 2, \ldots, n\}$, so heißt $\mathbf{P} = \{\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_k\}$ eine k-Partition von $\mathbf{M}$
- $Part_k(M) := \{\mathbf{P} | \mathbf{P} \text{ ist eine } k\text{-Partition von } \mathbf{M}\}$
- Stirlingzahlen zweiter Art:
  $S_{n,k} := |Part_k(\mathbf{M})|$ für $n, k \geq 0$ und $S_{0,0} := 1$
  $S_{n,k} =: \left\{ {n \atop k} \right\}$ gibt die Anzahl der k-Partitionen einer n-Menge an

1.18 Beispiel

1. $\mathbf{M} = \{1, 2, 3, 4\}$

   $$\begin{aligned} Part_1(\mathbf{M}) &= \Big\{\big\{\{1,2,3,4\}\big\}\Big\} \\ Part_2(\mathbf{M}) &= \Big\{\big\{\{1\},\{2,3,4\}\big\}, \big\{\{2\},\{1,3,4\}\big\}, \big\{\{3\},\{1,2,4\}\big\}, \big\{\{4\},\{1,2,3\}\big\}, \\ &\quad \big\{\{1,2\},\{3,4\}\big\}, \big\{\{1,3\},\{2,4\}\big\}, \big\{\{1,4\},\{2,3\}\big\}\Big\} \\ &= \big\{\{\mathbf{A}, \mathbf{M} \setminus \mathbf{A}\} | \mathbf{A} \subseteq \mathbf{M} \quad \mathbf{A} \neq \emptyset \quad \mathbf{A} \neq \mathbf{M}\big\} \end{aligned}$$

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

2. Für $n \geq 1$ gilt: $S_{n,0} = 0 \quad S_{n,1} = 1 \quad S_{n,n-1} = \binom{n}{2} \quad S_{n,n} = 1$

1.19 Satz (*Stirling-Dreieck zweiter Art*)

Für alle $k, m \in \mathbb{N}$ mit $1 \leq k \leq n$ gilt $S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$

Beweis (kombinatorisch)

Sei $\mathbf{A} = \{a_1, a_2, \ldots, a_n\}$

Dann gilt $Part_k(\mathbf{A}) = \underbrace{\{\mathbf{P} \in Part_k(\mathbf{A}) | \{a_n\} \in \mathbf{P}\}}_{\left\{\mathbf{P}' \cup \{a_n\} | \mathbf{P}' \in Part_{k-1}(\{a_1, a_2, \ldots, a_{n-1}\})\right\}} \cup \underbrace{\{\mathbf{P} \in Part_k(\mathbf{A}) | \{a_n\} \notin \mathbf{P}\}}_{\left\{\left\{\{a_1\} \cup B_1, B_2, \ldots, B_k\right\}, \left\{B_1, \{a_n\} \cup B_2, B_3, \ldots, B_k\right\}, \ldots, \left\{B_1, \ldots, B_{k-1}, \{a_n\} \cup B_n\right\} | \{B_1, \ldots, B_k\} \in Part_k(\{a_1, a_2, \ldots, a_{n-1})\right\}}$

$$\begin{array}{cccccccccc} \Rightarrow & |Part_k(\mathbf{A})| & = & |Part_{k-1}(\{a_1, a_2, \ldots, a_{n-1}\})| & + & k & \cdot & |Part_k(\{a_1, a_2, \ldots, a_{n-1}\})| \\ \text{d. h.} & S_{n,k} & = & S_{n-1,k-1} & + & k & \cdot & S_{n-1,k} \end{array}$$

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

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

1.20 Satz

Seien $\mathbf{M}$ und $\mathbf{N}$ Mengen mit $|\mathbf{M}| = m$ und $|\mathbf{N}| = n$, so gilt

1. $|Abb(\mathbf{M}, \mathbf{N})| = |\mathbf{N}|^{|\mathbf{M}|} = n^m$ (siehe Folgerung 1.2)
2. $|Inj(\mathbf{M}, \mathbf{N})| = n^{\underline{m}} = n \cdot (n-1) \cdot \cdots \cdot (n-(m-1))$ (n hoch m fallend)
3. $|Surj(\mathbf{M}, \mathbf{N})| = n! \cdot S_{m,n}$

Beweis

Sei $\mathbf{M} = \{a_1, a_2, \ldots, a_m\}$

1. klar
2. $f : \mathbf{M} \to \mathbf{N}$ injektiv $\Leftrightarrow f(a_i) \neq f(a_j)$ für $i \neq j$
3. Sei $\mathbf{N} = \{b_1, b_2, \ldots, b_n\}$ $\quad f : \mathbf{M} \to \mathbf{N}$ surjektiv.
   $\left\{\{a \in \mathbf{M} | f(a) = b_j\} | j = 1, \ldots, n\right\} \ni Part_k(\mathbf{M})$
   Für eine feste n-Partition von $\mathbf{M}$ permutiert man die Elemente in $\mathbf{N}$

   $\Rightarrow$ Eine n-Partition von $\mathbf{M}$ entspricht $n!$ surjektiven Abbildungen, d. h.
   $\underbrace{|Part_n(\mathbf{M})|}_{S_{m,n}} \cdot n! = |\text{surj}(\mathbf{M}, \mathbf{N})|$. Also $|\text{surj}(\mathbf{M}, \mathbf{N})| n! \cdot S_{m,n}$.

1.21 Satz

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

Beweis

Seien $\mathbf{M}$ und $\mathbf{N}$ Mengen mit $|\mathbf{M}| = m$ und $|\mathbf{N}| = n$

Dann gilt $Abb(\mathbf{M}, \mathbf{N}) = \dot{\bigcup}_{\mathbf{A} \subseteq \mathbf{N}} Surj(\mathbf{M}, \mathbf{A})$, d. h. man kann $f : \mathbf{M} \to \mathbf{N}$ als surjektive Abbildung von $\mathbf{M}$ nach $f(\mathbf{M})$.

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

1.3 Permutationen

Wiederholung: $S_n = Sym\{1,2,\ldots,n\} := \{\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\} | \sigma \textit{ bijektiv}\} \quad |S_n| = n!$
Jede Permutation $\sigma \in S_n$ kann man durch eine Wertetabelle angeben:

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

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

1.22 Definition (k-*Zyklus*)

Ein k-Zyklus $(i_1, i_2, \ldots, i_k)$ ist eine Permutation $\sigma \in S_n$ mit

- $\sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k,\ \sigma(i_k) = i_1$ und
- $\sigma(i) = i$ für $i \notin \{i_1, i_2, \ldots, i_k\}$ wobei $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$

1.23 Bemerkung

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

   Beispiel: $(1\ 2\ 4\ 6) = (2\ 4\ 6\ 1) = (4\ 6\ 1\ 2) = (6\ 1\ 2\ 4)$ aber $(1\ 2\ 4\ 6) \neq (1\ 2\ 6\ 4)$

2. Jedes $\sigma \in S_n$ läßt sich als Produkt von Zyklen schreiben. (Beispiel s. o.)

1.24 Definition (*Stirlingzahlen erster Art*)

Die Anzahl der Permutationen von $\{1, 2, \ldots, n\}$, die genau k Zyklen haben, heißt Stirlingzahl erster Art, bezeichnet mit $s_{n,k}$ oder $\left[{n \atop k}\right]$.

Beispiel: $\mathbf{M} = \{1,2,3\} \quad S_n = Sym\{1,2,3\}$
$S_3 = \{(1)(2)(3), (1)(2\ 3), (2)(1\ 3), (3)(1\ 2), (1\ 2\ 3), (1\ 3\ 2)\} \quad |S_3| = 3!$

$s_{3,1} = 2 \quad s_{3,2} = 3 \quad s_{3,3} = 1$
$s_{n,k} = 0 \quad$ für $k > n$
$s_{n,0} = 0 \quad$ für $n \in \mathbb{N}$
$s_{0,0} := 1$

1.25 Satz (*Stirling-Dreieck erster Art)*

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

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

Beweis (kombinatorisch)

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

$$\{(1\ 2)(3)(4), (1\ 3)(2)(4), \underbrace{(1\ 4)(2)(3)}_{i=1}, (2\ 3)(1)(4), \underbrace{(2\ 4)(1)(3)}_{i=2}, \underbrace{(3\ 4)(1)(2)}_{i=3}\}$$

$\{\sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_n | \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_k$ Permutation von $\{1,2,\ldots,n\}$ mit genau k Zyklen$\} =$
$\{\sigma_1' \cdot \sigma_2' \cdot \cdots \cdot \sigma_n' | \sigma_1' \cdot \sigma_2' \cdot \cdots \cdot \sigma_{k-1}'$ Permutation von $\{1,2,\ldots,n-1\}$ mit genau $k-1$ Zyklen$\}$
$\bigcup_{i=1}^{n-1} \{\sigma_1'' \cdot \sigma_2'' \cdot \cdots \cdot \sigma_n'' | \sigma_1'' \cdot \sigma_2'' \cdot \cdots \cdot \sigma_k''$ Permutation von $(\{1,2,\ldots,n-1\} | \{i\}) \cup \{(i,n)\}\}$
$\Rightarrow s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}$

Rekursion für die Stirlingzahlen erster Art (Stirling-Dreieck erster Art)

					1							$n=0$
				0		1						$n=1$
			0		1		1					$n=2$
		0		2		3		1				$n=3$
	0		6		11		6		1			$n=4$
0		24		50		35		10		1		$n=5$

1.26 Bemerkung

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

1.4 Erzeugende Funktionen (Formale Potenzreihen)

Bei der Komplexitätsanalyse von Algorithmen entstehen oft Rekursionsgleichungen.

Beispiel: $a_n = a_{n-1} + a_{n-2} \qquad a_1 = 1 \quad a_0 = 0$
$= (a_{n-2} + a_{n-3}) + a_{n-2} = 2a_{n-2} + a_{n-3} = \ldots$

Um die Lösungen zu finden, brauchen wir *erzeugende Funktionen*. Rekursionsgleichungen beschreiben unendliche Folgen:
$(a_n)_{n\in\mathbb{N}} = a_0, a_1, a_2, \ldots, a_n, \ldots$
$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots = \sum_{n=0}^{n} a_n x^n$ „formale Potenzreihe“

1.27 Definition (*erzeugende Funktion)*

Sei K ein Körper (z. B. $K = \mathbb{R}, \mathbb{C}$) und $(a_n)_{n\in\mathbb{N}} \in K^\infty$ eine Folge.
Die formale Potenzreihe $A(x) := \sum_{a=1}^{\infty} a_n x^n$ heißt *erzeugende Funktion* der Folge $(a_n)_{n\in\mathbb{N}_0}$, also $A(x) = \sum_{n=0}^{\infty} a_n x^n = (a_n)_{n\in\mathbb{N}_0}$.
$K[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n | a_n \in K \quad \forall n \in \mathbb{N} \right\}$

1.28 Bemerkung

1. Für $k \in \mathbb{N}_0$ gilt $x^k = (a_n)_{n\in\mathbb{N}_0}$ mit $a_n = \begin{cases} 1 & n = k \\ 0 & \text{sonst} \end{cases}$
   $\left(\delta_{k,n} = \begin{cases} 1 & n = k \\ 0 & \text{sonst} \end{cases} \text{ heißt } \textit{Kronecker-Symbol}\right)$
   $x^k = (\delta_{k,n})_{n\in\mathbb{N}_0}$

2. $\sum\limits_{n=1}^{\infty} a_n x^n = (b_j)_{j\in\mathbb{N}_0}$
   $(a_n x^n + a_{n+1}x^{n+1} + \ldots = 0 + 0x + \ldots + 0x^{n-1} + a_n x^n + a_{n+1}x^{n+1} + \ldots)$

3. Für $k \in \mathbb{N}$ gilt: $\sum\limits_{n=0}^{\infty} a_n x^{kn} = (b_i)_{i\in\mathbb{N}_0}$ $\quad b_i = \begin{cases} 0 & i \neq kn \quad \text{für alle } n \in \mathbb{N}_0 \\ a_n & i = kn \quad \text{für ein } n \in \mathbb{N}_0 \end{cases}$
   z. B. $k = 2 : \sum\limits_{n=0}^{\infty} a_n x^{2n} = \underbrace{a_0}_{b_0} + \underbrace{0x}_{b_1} + a_1x^2 + 0x^3 + \underbrace{a_2x^4}_{b_4}$

4. Unterschiede zwischen

Potenzreihen aus der Analysis	formale Potenreihen (erzg. Fkt)
$f(x) = \sum\limits_{n=0}^{\infty} a_n x^n$	$A(x) = \sum\limits_{n=0}^{\infty} a_n x^n = (a_n)_{n\in\mathbb{N}_0}$
• unendliche Summe	• Keine Summe, nur eine neue Schreibweise der Folge $(a_n)_{n\in\mathbf{N}_0}$
• Funktion von x	• Im Allgemeinen nichts einsetzen
• Konvergenzfrage	• Keine Konvergenzfrage

5. Seien $(a_n)_{n\in\mathbb{N}_0}$ und $(b_n)_{n\in\mathbb{N}_0}$ zwei Folgen und $A(x) = \sum\limits_{n=0}^{\infty} a_n x^n$ und $B(x) = \sum\limits_{n=0}^{\infty} b_n x^n$.
   Dann gilt $A(x) = B(x) \Leftrightarrow a_n = b_n \quad \forall n \in \mathbb{N}_0$

1.29 Definition

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

- Addition „+“
  $\sum\limits_{n=0}^{\infty} a_n x^n + \sum\limits_{n=0}^{\infty} b_n x^n := \sum\limits_{n=0}^{\infty} (a_n + b_n)x^n = (a_n + b_n)_{n\in\mathbb{N}_0}$
- Multiplikation „·“
  - $(\sum\limits_{n=0}^{\infty} a_n x^n) \cdot (\sum\limits_{n=0}^{\infty} b_n x^n) := \sum\limits_{n=0}^{\infty} (\sum\limits_{n=0}^{n} a_k b_{n-k})x^n$
    Faltung oder Konvolution der Folgen $(a_n)_{n\in\mathbb{N}_0}$ und $(b_n)_{n\in\mathbb{N}_0}$ (Cauchy-Produt aus der Analysis)
  - $a \cdot \sum\limits_{n=0}^{\infty} a_n x^n := \sum\limits_{n=0}^{\infty} a \cdot a_n x^n$

1.30 Lemma (*Verschieben von Folgegliedern*)

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

(d. h. $x^m \cdot (a_0, a_1, a_2, \ldots) = (\underbrace{\overset{b_0}{0}, \ldots, \overset{b_{m-1}}{0}}_{m-\text{mal}}, \overset{b_m}{a_0}, \overset{b_{m+1}}{a_1}, \ldots)$

Beweis

$$\begin{aligned} x^m \cdot \sum_{n=0}^{\infty} a_n x^n &= (\sum_{n=0}^{\infty} \delta_{m,n} x^n) \cdot (\sum_{n=0}^{\infty} a_n x^n) \\ &= \sum_{n=0}^{\infty} (\sum_{k=0}^{n} \delta_{m,n} a_{n-k}) x^n \\ &= \sum_{n=m}^{\infty} a_{n-m} x^n \end{aligned}$$

1.31 Beispiel

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

1.32 Satz

Sei K ein Körper

- $K\big[[x]\big]$ ist ein K-Vektorraum
- $(K\big[[x]\big], +, \cdot)$ ist ein kommutativer Ring mit Null ($0 = 0 \cdot x^n$) und Eins ($1 = 1 \cdot x^0 = (1, 0, 0, \ldots)$)

1.33 Bemerkung

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

1.34 Lemma

In $K\big[[x]\big]$ 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

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

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

1.35 Beispiel (*Code mit Variabler Wortlänge zum Komprimieren von Daten*)

Seien $Bu := \{a, b, c\}$ und $Zi := \{0, 1\}$. Für $k \in \mathbb{N}$ sei $W_k := \{$Folgen aus i Buchstaben gefolgt von $k - i$ Ziffern $\mid 1 < i < k\}$. (z. B. $\underbrace{ab0}_{\in W_3}, \underbrace{abb0010}_{\in W_7}, \underbrace{abc11}_{\in W_5}$).

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

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

Beweis

$$\begin{aligned}
\sum_{k=1}^{\infty} c_k x^k &= \sum_{k=0}^{\infty} (\sum_{i=0}^{k} 3^i \cdot 2^{k-i}) x^k \\
&= (\sum_{i=0}^{\infty} 3^i \cdot x^i) \cdot (\sum_{i=0}^{\infty} 2^i \cdot x^i) \\
&\overset{\text{Lemma1.34}}{=} \frac{1}{1-3x} \cdot \frac{1}{1-2x} \\
&= \frac{3}{1-3x} - \frac{2}{1-2x} \\
&= 3 \cdot \left(\sum_{k=0}^{\infty} 2^k \cdot x^k \right) \\
&= \sum_{k=0}^{\infty} \underbrace{(3^{k+1} - 2^{k+1})}_{:=C_k} x^k
\end{aligned}$$

1.36 Satz (*Inversion von Potenzreihen*)

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

Beweis

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

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

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

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

1.37 Beispiel

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

  Bestimme A^{-1}

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

  $$\begin{aligned}
  & a_0 b_0 = 1 && \Rightarrow\ b_0 = 1 \\
  & a_0 b_1 + a_1 b_0 = 0 \Leftrightarrow 1 \cdot b_1 - c \cdot 1 = 0 && \Rightarrow\ b_1 = c \\
  & a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 && \Rightarrow\ b_2 = c^2 \\
  & \vdots && \Rightarrow\ \vdots \\
  & \vdots && \Rightarrow\ b_n = c^n
  \end{aligned}$$

  Also: $\frac{1}{1-cx} = \sum_{n=0}^{\infty} c^n x^n$

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

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

1.38 Definition

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

Bemerkung: $D : K\big[[x]\big] \to K\big[[x]\big]$ ist eine Operation auf Folgen:
$D : (a_0, a_1, a_2, \ldots, a_n, \ldots) \to (\underset{\shortparallel}{a_1}, \underset{\shortparallel}{2a_2}, \ldots, \underset{\shortparallel}{na_n}, \ldots)$
$\qquad\qquad\qquad\qquad\qquad\quad x^0 \quad x^1 \qquad\qquad x^{n-1}$

1.39 Lemma

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

1. $D(x^n) = nx^{n-1}$
2. $D(A \cdot B) = D(A) \cdot B + A \cdot D(B)$

1.40 Folgerung

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

Beweis

$$\begin{aligned} A \cdot A^{-1} = 1 \quad &\Rightarrow 0 = D(1) = D(A \cdot A^{-1}) = D(A) \cdot A^{-1} + A \cdot D(A^{-1}) \\ &\Rightarrow A \cdot D(A^{-1}) = -D(A) \cdot A^{-1} \\ &\Rightarrow D(A^{-1}) = -\tfrac{D(A)}{A^2} \end{aligned}$$

1.41 Folgerung

Für $m \in \mathbb{N}$ gilt: $\boxed{\frac{1}{(1-cx)^m} = \sum_{n=0}^{\infty} \binom{n+m-1}{m-1} c^n x^n}$

1.42 Bemerkung

- Erzeugende Funktionen kann man im Prinzip wie ganz normale Funktionen (aus der Analysis) betrachten
- Falls es zu einer Funktion F (aus der Analysis) eine Potenzreihe gibt, dann kann man diese durch Taylorentwicklung um die Null beschreiben:
  $F(x) = \sum_{n=0}^{\infty} \frac{F^{(n)}(0)}{n!} x^n := \Big(\frac{F^{(n)}(0)}{n!}\Big)_{n \in \mathbb{N}}$
- Formale Potenzreihen und ihre erzeugenden Funktionen

a_n	Folge	Potenzreihe	erzeugende Funktion
1	$1,1,1,1,\ldots$	$\sum_{n=0}^{\infty} x^n$	$\frac{1}{1-x}$
n	$0,1,2,3,\ldots$	$\sum_{n=0}^{\infty} nx^n$	$\frac{x}{(1-x)^2}$
c^n	$1,c,c^2,c^3,\ldots$	$\sum_{n=0}^{\infty} c^n x^n$	$\frac{1}{1-cx}$
n^2	$0,1,4,9,\ldots$	$\sum_{n=0}^{\infty} n^2 x^2$	$\frac{x(1+x)}{(1-x)^3}$
$\binom{r}{n}$	$1,r,\binom{r}{2},\binom{r}{3}$	$\sum_{n=0}^{\infty} \binom{r}{n} x^n$	$\frac{1}{(1+x)^n}$
$\binom{r+n}{n}$	$1,r+1,\binom{r+2}{2},\binom{r+3}{3}$	$\sum_{n=0}^{\infty} \binom{r+n}{n} x^n$	$\frac{1}{(1-x)^{r+1}}$
$\frac{1}{n}$	$0,1,\frac{1}{2},\frac{1}{3},\ldots$	$\sum_{n=0}^{\infty} \frac{1}{n} x^n$	$ln\frac{1}{1-x}$
$\frac{1}{n!}$	$1,1,\frac{1}{2},\frac{1}{6},\ldots$	$\sum_{n=0}^{\infty} \frac{1}{n!} x^n$	e^x

Für $r \in \mathbb{R}$ definiert man:

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

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \quad \forall\, n \in \mathbb{N} \longrightarrow (1+x)^y = \sum_{k=0}^{\infty} \binom{y}{k} x^k \quad \forall\, y \in \mathbb{R}$$

1.5 Rekursionsgleichungen

Einige grundlegende algorithmische Verfahren:

- Divide and Conquer-Algorithmus
  Idee: - teile das zu lösende Problem P in kleinere Teilprobleme auf (Divide)
  - löse die Teilprobleme (Conquer)
  - berechne aus den Lösungen der Teilprobleme die Lösung von P (Conquer)

- dynamische Programmierung (Optimierungsprobleme)

- Greedy-Algorithmen

- Bei der Analyse von Algorithmen kommen Funktionen der Form
  $F(n) = F(n-1) + F(n-2) \quad n \geq 2$ und $F(1) = 1,\ F(0) = 0$ oder
  $T(n) = T(\lfloor \frac{n}{2} \rfloor) + T(\lceil \frac{n}{2} \rceil) \quad n \geq 2$ und $T(1) = 1$
  vor. Für die Bestimmung der Laufzeit von Algorithmen spielt das Lösen von Rekusionsgleichungen eine zentrale Rolle.

1.43 Definition (*Lineare Rekusion*)

Eine Rekursiongleichung der Form $\boxed{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} + b_k \quad \forall\, n \geq k}$ mit der Anfangsbedingungen $a_i = b_i \quad i = 0,1,\ldots,k-1$ heißt lineare Rekusionsgleichung k-ter Ordnung

- Gilt $b_k = 0$, so heißt die Gleichung eine homogene lineare Rekursionsgleichung

- Gilt $b_k \neq 0$, so heißt die Gleichung eine inhomogene lineare Rekursionsgleichung

1.44 Beispiel

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

$$\begin{array}{lcll} a_1 & = & c \cdot a_0 & = & c \cdot b_0 \\ a_2 & = & c \cdot a_1 = c \cdot c \cdot b_0 & = & c^2 \cdot b_0 \\ & \vdots & & & \end{array}$$

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

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

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

Beweis (Induktion über n)

$\mathbf{n = 1}$:

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

$\mathbf{n \Rightarrow n + 1}$:

1. Fall $(c \neq 1)$ **:**

$$\begin{array}{lcl} a_n & = & c \cdot a_{n-1} + b_1 \\ & = & c\big(b_0 \cdot c^{n-1} + b_1 \cdot \frac{c^{n-1} - 1}{c-1}\big) + b_1 \\ & = & b_0 \cdot c^n + b_1\big(\frac{c^n - c}{c-1} + 1\big) \\ & = & b_0 \cdot c^n + b_1 \cdot \frac{c^n - 1}{c-1} \end{array}$$

1. Fall $(c = 1)$ **:**

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

1.45 Beispiel

$a_n :=$ Anzahl der Wörter mit der Länge n über $\{a, b\}$, die keine zwei aufeinanderfolgenden a's enthalten

z. B. :

$$\begin{array}{lcll} a_1 & = & 2 & (a, b) \\ a_2 & = & 3 & (ab, ba, bb) \\ a_3 & = & 5 & (aba, abb, bab, bba, bbb) \\ & \vdots & & \end{array}$$

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

1.46 Beispiel (*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 nach n Monaten (F_n)?

Antwort:

$$\begin{array}{lcll} F_0 & = & 0 & \\ F_1 & = & 1 & \\ F_2 & = & 1 & \\ F_3 & = & 1 + 1 & = \quad F_2 + F_1 \\ F_4 & = & 2 + 1 & = \quad F_3 + F_2 \\ & \vdots & & \\ F_n & = & F_{n-1} + F_{n-2} & \end{array}$$

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

Fibonacci-Zahlen.

Numerisch berechnen wir F_n mit Hilfe von erzeugenden Funktionen.

$$\begin{aligned}
F &= F(x) = \sum_{n=0}^{\infty} F_n x^n \\
&= F_0x^0 + F_1x^1 + \sum_{n=2}^{\infty}(F_{n-1}+F_{n-2})x^n \\
&= F_0x^0 + F_1x^1 + \underbrace{\sum_{n=2}^{\infty} F_{n-1}x^n}_{x\cdot\sum_{n=1}^{\infty}F_nx^n} + \underbrace{\sum_{n=2}^{\infty} F_{n-2}x^n}_{x^2\cdot\underbrace{\sum_{n=0}^{\infty}F_nx^n}_{:=F}} \\
&\qquad\qquad \underbrace{x\cdot\sum_{n=0}^{\infty}(F_nx^n - F_0x^0)}_{x\cdot F - F_0 x} \\
&= F_0x^0 + F_1x^1 + x\cdot F - F_0\cdot x + x^2\cdot F \\
&= x + x\cdot F + x^2\cdot F \\
\Rightarrow F &= \tfrac{x}{1-x-x^2}
\end{aligned}$$

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

$$\begin{aligned}
\sum_{n=0}^{\infty} F_n x^n = F &= \tfrac{a}{1-\alpha x} + \tfrac{b}{1-\beta x} \\
&= a\cdot\sum_{n=0}^{\infty}\alpha^n x^n + b\cdot\sum_{n=0}^{\infty}\beta^n x^n \\
&= \sum_{n=0}^{\infty}(a\cdot\alpha^n + b\cdot\beta^n)x^n
\end{aligned}$$

Somit gilt $\boxed{F_n = a\cdot\alpha^n + b\cdot\beta^n}$

Wegen $\frac{x}{1-x-x^2} \overset{q.E.}{=} \frac{x}{\frac{5}{4}\cdot(x+\frac{1}{2})^2}$

$$\begin{aligned}
&= \frac{x}{\left[\frac{\sqrt{5}}{2}-(x+\frac{1}{2})\right]\cdot\left[\frac{\sqrt{5}}{2}+(x+\frac{1}{2})\right]} \\
&\overset{?}{=} \frac{\cdot}{\frac{\sqrt{5}-1}{2}-x} + \frac{\cdot}{\frac{\sqrt{5}+1}{2}+x} \qquad \text{Partialbruchzerlegnung} \\
&= \frac{\frac{1}{\sqrt{5}}}{1-\frac{1+\sqrt{5}}{2}x} + \frac{-\frac{1}{\sqrt{5}}}{1-\frac{1-\sqrt{5}}{2}x}
\end{aligned}$$

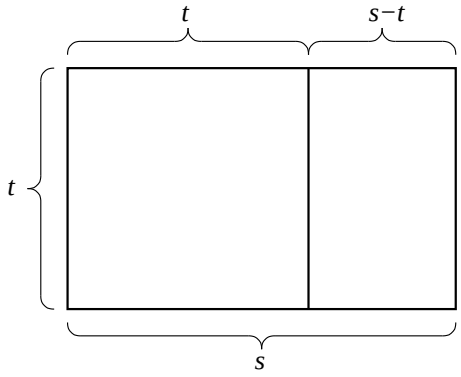
d.h. $\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}, \quad a = \frac{1}{\sqrt{5}}, \quad b = -\frac{1}{\sqrt{5}}$

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

1.47 Bemerkung

Die Zahl $\sigma = \frac{1+\sqrt{5}}{2} = 1,61803398875$ heißt goldener Schnitt und taucht bei verschiedenen Untersuchungen auf.

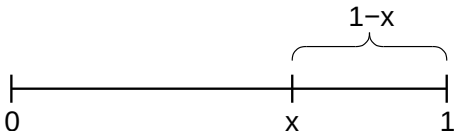
1.



$\frac{s}{t} = \frac{t}{s-t} = \frac{1}{\frac{s}{t}-1}$

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 $x = \frac{s}{t} = \frac{1+\sqrt{5}}{2}$

2.



$\frac{1}{x} = \frac{x}{1-x}$

Es gilt:
$\frac{x}{1-x} = \frac{1}{x} \Leftrightarrow x^2 + x - 1 = 0 \Leftrightarrow x = \frac{-1 \pm \sqrt{5}}{2} \Rightarrow x = \frac{\sqrt{5}-1}{2} = \frac{2}{1+\sqrt{5}} = \frac{1}{\sigma} \approx 0.618$

1.48 Satz

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

Seien α, β zwei Lösungen der Gleichung $x^2 - c_1 x - c_2 = 0$
und $A = \begin{cases} \frac{b_0 - \beta b_0}{\alpha - \beta} & \alpha \neq \beta \\ \frac{b_1 - \alpha b_0}{\alpha} & \alpha = \beta \end{cases} \qquad B = \begin{cases} \frac{b_1 - \alpha b_0}{\alpha - \beta} & \alpha \neq \beta \\ b_0 & \alpha = \beta \end{cases}$

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

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

Schema zum Lösen von (homogenen) linearen Regressionsgleichungen

$a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2} + \ldots + c_k \cdot a_{n-k}$ für $n \geq k$ mit $a_i = b_i$ für $i = 0, 1, \ldots, k-1$

1. **Aufstellen der erzeugenden Funktion**

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

2. **Anwendung der Rekursionsgleichung**

$$\begin{aligned}
A(x) &= a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1} + \sum_{n=k}^{\infty} a_n x^n \\
&= b_0 + b_1x + b_2x^2 \ldots + b_{k-1}x^{k-1} + \sum_{n=k}^{\infty} (c_1a_{n-1} + \ldots + c_ka_{n-k})x^n \\
&= b_0 + b_1x + \ldots + b_{k-1}x^{k-1} \\
&\quad + \underbrace{\sum_{n=k}^{\infty} c_1a_{n-1}x^n}_{c_1x\underbrace{\sum_{n=k}^{\infty} a_{n-1}x^{n-1}}_{A(x)-\sum_{i=0}^{k-2} a_ix^i}} + \underbrace{\sum_{n=k}^{\infty} c_2a_{n-2}x^n}_{c_2x^2\underbrace{\sum_{n=k}^{\infty} a_{n-2}x^{n-2}}_{A(x)-\sum_{i=0}^{k-3} a_ix^i}} + \ldots + \underbrace{\sum_{n=k}^{\infty} c_ka_{n-k}x^n}_{c_kx^k\underbrace{\sum_{n=k}^{\infty} a_{n-k}x^{n-k}}_{A(x)}} \\
&= b_0 + b_1x + \ldots + b_{k-1}x^{k-1} \\
&\quad + c_1x\Big(A(x) - \sum_{i=0}^{k-2} a_ix^i\Big) + c_2x^2\Big(A(x) - \sum_{i=0}^{k-3} a_ix^i\Big) + \ldots + c_kx^k \cdot A(x)
\end{aligned}$$

3. **Auflösen nach A(x)**

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

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

Sei $1 - c_1x - c_2x^2 - \ldots - c_kx^k = (1-\alpha_1x)^{m_1} \cdot (1-\alpha_2x)^{m_2} \cdot \ldots \cdot (1-\alpha_tx)^{m_t}$ mit $\sum_{i=1}^{t} m_i = k$

Und sei
$$\begin{aligned}
A(x) &= \tfrac{d_0+d_1x+\ldots+d_{k-1}x^{k-1}}{1-c_1x-c_2x^2-\ldots-c_kx^k} \\
&= \tfrac{g_1(x)}{(1-\alpha_1x)^{m_1}} + \ldots + \tfrac{g_t(x)}{(1-\alpha_tx)^{m_t}} \\
&= \sum_{i=1}^{t} \tfrac{g_i(x)}{(1-\alpha_ix)^{m_i}}
\end{aligned}$$

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

5. **Nach Tabelle in Bemerkung 1.42:**

$A(x) = \sum_{i=1}^{t} \frac{g_i(x)}{(1-\alpha_ix)^{m_i}} = \sum_{i=1}^{t} g_i(x)\Big(\sum_{n=0}^{\infty} \binom{n+m_i-1}{m_i-1}(\alpha_ix)^n\Big) = \sum_{n=0}^{\infty} q_nx^n$

Dann gilt: $a_n = q_n, \quad n \geq k$

1.49 Beispiel

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

Lösung

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

Dann gilt:

$$\begin{aligned}
A(x) &= a_0 + a_1x + a_2x^2 + \sum_{n=3}^{\infty}(5a_{n-1} - 7a_{n-2} + 3a_{n-3})x^n \\
&= a_0 + a_1x + a_2x^2 + 5x\Big(\sum_{n=3}^{\infty} a_{n-1}x^{n-1} - 7x^2 \cdot \sum_{n=3}^{\infty} a_{n-2}x^{n-2} + 3x^3 \sum_{n=3}^{\infty} a_{n-3}x^{n-3}\Big) \\
&= 1 + 5x + 19x^2 + 5x\big(A(x) - (1+Sx)\big) - 7x^2\big(A(x) - 1\big) + 3x^3 \cdot A(x) \\
\Rightarrow \quad A(x) &= \tfrac{1+x^2}{1-Sx+7x^2-3x^3} \\
&= \tfrac{1+x^2}{(1-x)^2(1-3x)} \\
&= \tfrac{\frac{1}{2}x-\frac{3}{2}}{(1-x)^2} + \tfrac{\frac{5}{2}}{1-3x} \\
&= \tfrac{1}{2}(x-3)\tfrac{1}{(1-x)^2} + \tfrac{5}{2} \cdot \tfrac{1}{1-3x} \\
&= \tfrac{1}{2}(x-3)\sum_{n=0}^{\infty}\tbinom{n+1}{1}x^n + \tfrac{5}{2}\sum_{n=0}^{\infty}(3x)^n \\
&= 1 + 5x + \sum_{n=2}^{\infty}\left(\tfrac{5}{2} \cdot 3^n - n - \tfrac{3}{2}\right)x^n \\
\Rightarrow a_n &= \tfrac{5}{2} \cdot 3^n - n - \tfrac{3}{2}, \quad n \geq 2
\end{aligned}$$

1.50 Beispiel (*Catalan-Zahlen*)

In einer zulässigen Klammerkette ist an jeder Stelle der Kette die Anzahl der bis dahin vorkommenden öffnenden Klammern grösser oder gleich der bis dahin vorgekommenen schließenden Klammern und öffnende und schließende Klammer sind von der Anzahl her gleich.

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

z. B. :

$$\begin{aligned}
C_0 &= 1 \\
C_1 &= 1 \quad \{()\} \\
C_2 &= 2 \quad \{()(),(())\} \\
C_3 &= 5 \quad \{()()(),((())),(())(),()(()),(()())\} \\
&\vdots
\end{aligned}$$

Frage: $C_n = ?$

1.51 Lemma (*Rekursionsformel für Catalan-Zahlen*)

$$\boxed{C_n = \sum_{k=1}^{n} C_{k-1}C_{n-k} \qquad n \geq 1}$$

Beweis

$$(\quad \overbrace{(\ldots)}^{\text{zulässige Klammerkette mit } 2(k-1) \text{ Klammern}} \quad \underset{2k}{\underset{\uparrow}{)}} \quad \underbrace{(\ldots)}_{\text{zulässige Klammerkette mit } 2n-2k \text{ Klammern}}$$

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

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

$\Rightarrow C_n = |\dot{\bigcup}_{k=1}^{n} A_k| = \sum_{k=1}^{n} |A_k| = \sum_{k=1}^{n} C_{k-1} \cdot C_{n-k}$

1.52 Satz (*explizite Darstellung der Catalan-Zahlen*)

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

Beweis

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

Dann gilt:
$$\begin{aligned}
c(x) &= C_0 x^0 + \sum_{n=1}^{\infty} C_n x^n \\
&\overset{Lemma 1.51}{=} C_0 + \sum_{n=1}^{\infty} \Big(\sum_{k=1}^{n} C_{k-1} \cdot C_{n-k} \Big) x^n \\
&= C_0 + x \cdot \sum_{n=1}^{\infty} \Big(\sum_{k=1}^{n} C_{k-1} \cdot C_{n-k} \Big) x^{n-1} \\
&\overset{t=n-1}{=} C_0 + x \cdot \sum_{t=0}^{\infty} \Big(\sum_{k=1}^{t+1} C_{k-1} \cdot C_{\underbrace{(t+1)-k}_{t-(k-1)}} \Big) x^t \\
&\overset{s=k-1}{=} C_0 + x \cdot \sum_{t=0}^{\infty} \Big(\sum_{s=0}^{t} C_s \cdot C_{t-s} \Big) x^t \\
&\overset{Def 1.29}{=} \underset{\| \; 1}{C_0} + x \cdot c(x) \cdot c(x)
\end{aligned}$$

Somit gilt:
$$\begin{aligned}
x \cdot c^2(x) - c(x) &= -1 \\
x^2 \cdot c^2(x) - x \cdot c(x) &= -x \\
\overset{q.E.}{\Rightarrow} \quad \big(x \cdot x(x) - \tfrac{1}{2}\big)^2 &= \tfrac{1}{4} - x \qquad \big(= \tfrac{1}{4}(1-4x) \big) \\
\Rightarrow \quad x \cdot c(x) - \tfrac{1}{2} &= \pm \tfrac{1}{2} \sqrt{1-4x}
\end{aligned}$$

$$\begin{aligned}
\sum_{n=0}^{\infty} C_n x^{n+1} &= x \cdot \underbrace{c(x)}_{\sum_{n=0}^{\infty} C_n x^n} \\
&= \tfrac{1}{2} \cdot \Big[1 \pm \sqrt{1-4x} \Big] \\
&\overset{Bem.1.42}{=} \tfrac{1}{2} \cdot \Big[1 \pm \sum_{n=0}^{\infty} \tbinom{\frac{1}{2}}{n} (-4x)^n \Big] \\
0 + C_0 x + C_1 x^2 + \ldots &= \tfrac{1}{2} \cdot \Big[1 \pm \big(1 + \sum_{n=1}^{\infty} \tbinom{\frac{1}{2}}{n} (-4)^n x^n \big) \Big]
\end{aligned}$$

Der Koeffizient von x^0 ist gleich $0 \Rightarrow$ „ $-$ “ als Vorzeichen, d. h.

$C_0 x + C_1 x^2 + \ldots = -\frac{1}{2} \cdot \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n$

$$\begin{aligned}
\Rightarrow \quad C_n &= -\tfrac{1}{2} \cdot \tbinom{\frac{1}{2}}{n+1} (-4)^{n+1} \\
&= -\tfrac{1}{2} \cdot \tfrac{\frac{1}{2} \cdot (\frac{1}{2}-1) \cdot \ldots \cdot \frac{1}{2} \cdot (\frac{1}{2}-n)}{(n+1)!} \cdot (-1)^{n+1} \cdot 4^n \\
&= (-1)^{n+2} \tfrac{(\frac{1}{2}-1) \cdot \ldots \cdot \frac{1}{2} \cdot (\frac{1}{2}-n)}{(n+1)!} \cdot 4^n \\
&= \tfrac{(2-1)(4-1) \cdots (2n-1)}{(n+1) \cdot n!} \cdot \overbrace{2^n \cdot n!}^{(2\cdot 1)(2\cdot 2) \cdots (2 \cdot n)} \\
&= \frac{\overbrace{\big[1 \cdot 3 \cdot \ldots \cdot (2n-1)\big] \big[2 \cdot 4 \cdot \ldots \cdot (2n)\big]}^{(2n)!}}{(n+1) \cdot n! \cdot n!} \\
&= \tfrac{1}{n+1} \cdot \tfrac{(2n)!}{n! \cdot n!} \\
&= \tfrac{1}{n+1} \tbinom{2n}{n}
\end{aligned}$$

Schema zum Lösen von allgemeinen Regressionsgleichungen

Gegeben sei die Rekursionsgleichung $a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k})$ für $n \geq k$ mit den Anfangswerten $a_i = b_i,\ i = 0, 1, \ldots, k-1$.

Berechne a_n für $n \geq k$ explizit:

1. Aufstellen der erzeugenden Funktion: $A(x) = \sum_{n=0}^{\infty} a_n x^n$
2. $A(x) = \sum_{n=0}^{\infty} a_n x^n$ umformen, so daß Anfangswerte und Rekursionsgleichung eingesetzt werden können.
3. Weiter umformen, bis af der rechten Seite die noch vorhandenen unendlichen Summen (und mit ihnen alle Vorkommen von Folgegliedern 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)

Kapitel 2

Graphentheorie

2.1 Grundbegriffe der Graphentheorie

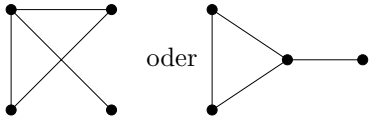
2.1 Definition (*Graph*)

Ein *Graph* ist ein Paar $G = (V, E)$, wobei V eine endliche Menge und $E \subseteq \binom{V}{2} := \big\{\{x, y\} | x, y \in V,\ x \neq y\big\}$ ist. Die Elemente von V heißen *Ecken* (oder Punkte/Knoten; engl. *vertexes*) und die Elemente von E heißen *Kanten* (engl. *edges*). Statt $\{x, y\} \in E$ schreiben wir auch $xy \in E$.

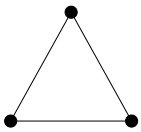
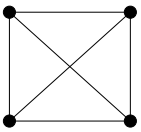
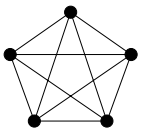
Ein Graph $G = (V, E)$ wird i. A. durch ein Diagramm dargestellt, in dem man jede Ecke $x \in V$ durch einen Punkt repräsentiert und zwei Ecken $x, y \in V$ genau durch eine Linie verbunden werden, wenn $xy \in E$ ist.

2.2 Beispiel

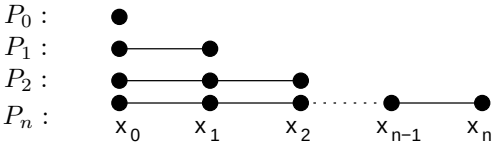
1. $C = (\{a, b, c, d\}, \{ab, bc, ca, bd\})$



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

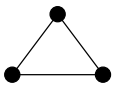
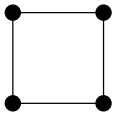
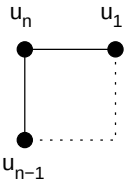
K_1:  K_2: K_3:  K_4:  K_5: 

3. Wege:



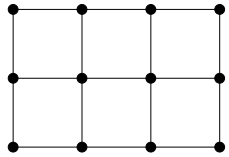
$P_n = x_0 x_1 x_2 \dots x_n$

4. Kreise:

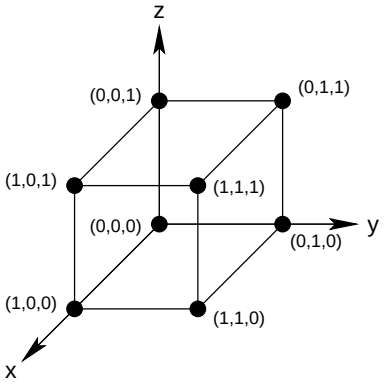
C_3 :  C_4 :  C_n : 

$C_n = u_1 u_{n-1} \dots u_n u_1$

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

$M_{3,4} =$ 

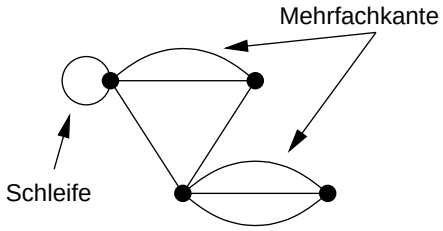
6. d-dimensionale Hyperwürfel Q_d
   $V(Q_d)$:=die Menge aller $0-1$-Folgen der Länge d
   $E(Q_d) := \{xy | x, y \in V(Q_d), x \text{ und } y \text{ unterscheiden sich an genau einer Stelle}\}$

$Q_3 =$ 

2.3 Bemerkung

1. In dieser Vorlesung betrachten wir nur Graphen ohne Mehrfachkanten und ohne Schleifen!

   - Ein Graph ohne Schleifen heißt *Multigraph*
   - Ein Graph ohne Schleifen und ohne Mehrfachkanten heißt *schlichter Graph*
   - $G = (\emptyset, \emptyset)$ heißt *leerer Graph*
   - $G = (V, \emptyset)$ heißt *Nullgraph*



Graph mit Schleife und Mehrfachkanten

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 *adjazent*

2.4 Definition (*Nachbarschaft, Eckengrad*)

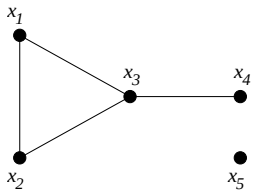
Sei $G = (V, E)$ und $x \in V$

- $N(x) = \{y \in V \,|\, xy \in E\}$ heißt die *Nachbarschaft* von x in G
- $d_G = |N(x)|$ heißt *Eckengrad* von x in G
  - Ist $d(x) = 1$, so heißt x *Endecke*
  - Ist $d(x) = 0$, so heißt x *isolierte Ecke*

- $\delta(G) = min_{x \in V} d(x) \qquad \Delta(G) = max_{x \in V} d(x)$

  Ist $\delta(G) = \Delta(G) = k$, so heißt G *k-regulärer Graph*, z. B. K_n ist $(n-1)$-regulär

2.5 Beispiel

1. 

   $N(x_1) = \{x_2, x_3\} \quad N(x_3) = \{x_1, x_2, x_4\}$
   $d(x_1) = 2$
   $d(x_2) = 2$
   $d(x_3) = 3$
   $d(x_4) = 1$ Endecke
   $d(x_5) = 0$ isolierte Ecke

2. C_n ist 2-regulär

2.6 Satz (*Handschlaglemma - Euler, 1736*)

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

Beweis (Doppeltes Abzählen)

In $\sum_{x \in V} d(x)$ wird jede Kante $xy \in V$ genau zweimal gezählt (einmal in $d(y)$ und zum zweiten Mal in $d(z)$). Auf der rechten Seite wird jede Kante ebenfalls zweimal gezählt.

2.7 Folgerung

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

Beweis

Sei $G = (V, E)$ und $V_1 = \{x \in V \mid d(x) \text{ ungerade}\}$ und $V_2 = \{x \in V \mid d(x) \text{ gerade}\} \quad (V = V_1 \dot\cup V_2)$

Nach Satz 2.6 gilt: $\underbrace{2 \cdot |E|}_{\text{gerade}} = \sum_{x \in V} d(x) = \underbrace{\sum_{x \in V} \underbrace{d(x)}_{\text{gerade}}}_{\text{gerade}} + \underbrace{\sum_{x \in V} \underbrace{d(x)}_{\text{ungerade}}}_{\text{gerade}}$

2.8 Lemma

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

Beweis

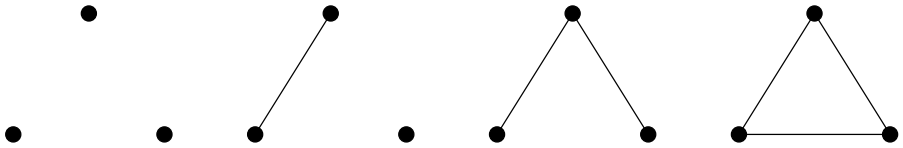
Schubfachprinzip (→ vgl. 1.13.2)

2.9 Definition (*isomorphe Graphen*)

Es seien $G = (V, E)$ und $G' = (V', E')$ zwei Graphen. G ist *isomorph* zu G' (in Zeichen $G \cong G'$) genau dann, wenn es eine bijektive Abbildung $\phi : V \to V'$ mit $xy \in E \Leftrightarrow \phi(x)\phi(y) \in E'$ gibt.

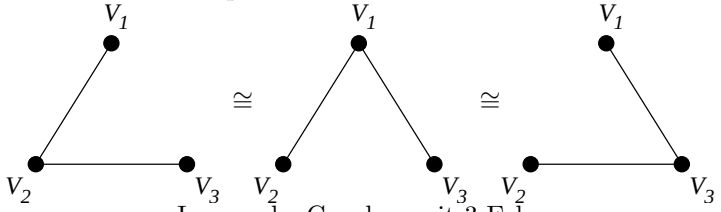
2.10 Beispiel

1.



Nicht isomorphe Graphen mit 3 Ecken

2. Werden die Namen von Ecken (und Kanten) eines Graphen berücksichtigt, so spricht man von einem *markierten* oder *benannten* Graph.



Isomorphe Graphen mit 3 Ecken

Darstellung von Graphen

2.11 Definition (*Adjazenz-, Inzidenzmatrix*)

Ist $G = (V, E)$ ein Graph mit $V = \{v_1, \ldots, v_n\}$ und $E = \{e_1, \ldots, e_m\}$, so heißt die $n \times n$-Matrix $A = (a_{ij}) \in \{0,1\}^{m \times m}$ mit $a_{ij} = \begin{cases} 1 & v_i v_j \in E \\ 0 & \text{sonst} \end{cases}$, die *Adjazenzmatrix* von G.

$$\begin{array}{c} \\ v_1 \\ v_2 \\ \vdots \\ v_n \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & \ldots & v_n \end{array} \\ \begin{pmatrix} 0 & & & \\ & 0 & a_{ij} & \\ & & \ddots & \\ & & & 0 \end{pmatrix} \end{array}$$

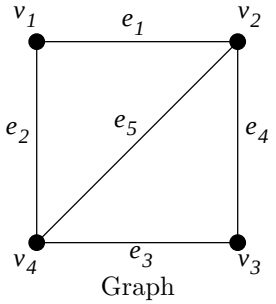
Adjazenzmatrix

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

$$\begin{array}{c} \\ v_1 \\ v_2 \\ \vdots \\ v_n \end{array} \begin{array}{c} \begin{array}{cccc} e_1 & e_2 & \ldots & e_m \end{array} \\ \begin{pmatrix} & & & \\ & b_{ij} & & \\ & & & \\ & & & \end{pmatrix} \end{array}$$

Inzidenzmatrix

2.12 Beispiel (*Adjazenz-, Inzidenzmatrix*)



Graph

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Adjazenzmatrix

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Inzidenzmatrix

2.13 Satz (*Zusammenhang von Adjazenz- und Inzidenzmatrix*)

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

$$\boxed{I \cdot I^T = A + diag\big(d(v_1), \ldots, d(v_n)\big) = A + \begin{pmatrix} v_1 & & \\ & \ddots & \\ & & v_n \end{pmatrix}}$$

Beweis

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

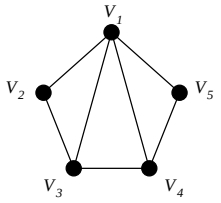
Für $i = j : (I \cdot I^T)_{ij} = \sum_{k=1}^{m} \underbrace{b_{ik} b_{jk}}_{b_{ik}} = \sum_{k=1}^{m} b_{ik}$

2.14 Definition (*Teilgraph*)

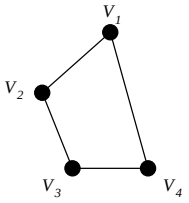
Sei $G = (V, E)$ ein Graph und $V' \subseteq V$

- $G' = (V', E')$ heißt *Teilgraph* von G, wemm $E' \subseteq E \cap \binom{V'}{2}$ ist. In Zeichen: $G' \subseteq G$
- $G[V'] := (V', E \cap \binom{V'}{2})$ heißt der von V' *induzierte Teilgraph*

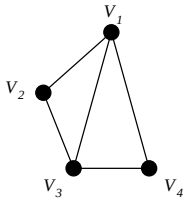
z. B.



G



G'



$G'' = G[\{V_1, V_2, V_3, V_4\}]$

2.15 Definition (*zusammenhängend, Komponenten, Schnittecke, Brücke*)

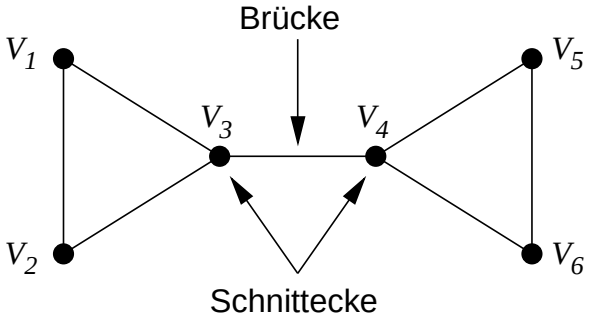
1. Sei $G = (V, E)$. G heißt *zusammenhängend*, wenn zwischen je zwei Ecken $x, y \in V$ ein Weg von x nach y existiert.

2. In einem nicht zusammenhängenden Graphen heißt jeder maximale (bzgl. Anzahl von Ecken und Kanten) zusammenhängende Teilgraph eine *Zusammenhangskomponente* oder *Komponente*.

   Sind $G_1, \ldots, G_k$ die Komponenten von G, so gilt $G = \bigcup_{i=1}^{k} G_i$.

   $\kappa(G)$:=Anzahl der Komponenten von G.
   $\kappa(G) = 1 \Leftrightarrow G$ ist zusammenhängend

3. Sei $G = (V, E)$ zusammenhängend. 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.



zusammenhängender Graph

2.16 Satz (*Anzahl der Komponenten eines Graphen*)

Sei $G = (V, E)$. Dann gilt $\kappa(G) \geq |V| - |E|$.

2.17 Folgerung

Sei $G = (V, E)$ zusammenhängend mit $n = |V|$ und $m = |E|$. Dann gilt: $\boxed{n - 1 \leq m \leq \frac{n(n-1)}{n} = \binom{n}{2}}$

2.18 Satz

Sei $G = (V, E)$ mit $|V| = n$ und $|E| = m$. Gilt $m > \frac{1}{2}(n-1)(n-2) = \binom{n-1}{2}$, so ist G zusammenhängend.

Beweis (Indirekt)

Angenommen G ist nicht zusammenhängend und seien $G_1, \ldots, G_k$ die Komponenten von G mit $|V(G_i)| = n_i$ für alle $i = 1, \ldots, k$. Dann gilt $k \geq 2$ und $n_1 + n_2 + \ldots + n_k = n$

$$
\begin{aligned}
m &= |E(G_1)| + |E(G_1)| + \ldots + |E(G_1)| \\
&\overset{2.17}{\leq} \frac{n_1(n_1-1)}{2} + \frac{n_2(n_2-1)}{2} + \ldots + \frac{n_k(n_k-1)}{k} \\
&= \frac{1}{2}\left[\left({n_1}^2 + {n_2}^2 + \ldots + {n_k}^2\right) - (n_1 + n_2 + \ldots + n_k)\right] \\
&= \frac{1}{2}\left[(n_1 + \ldots + n_k)^2 - 2\sum_{1 \leq i < j \leq k} n_i n_j - n\right] \\
&\leq \frac{1}{2}\left[n^2 - 2n_1 \underbrace{(n_2 + n_3 + \ldots + n_k)}_{n - n_1} - n\right] \\
&\leq \frac{1}{2}\left[n^2 - 2(n-1) - n\right] \\
&= \frac{1}{2}\left(n^2 - 3n + 2\right) \\
&= \frac{1}{2}(n-1)(n-2)
\end{aligned}
$$

Dies ist aber ein Widerspruch und somit folgt G ist zusammenhängend.

2.19 Satz

Ist $G = (V, E)$ ein Graph mit $|V| = n$ und $|E| = m$, so gilt: $\boxed{m \leq \binom{n - \kappa(G) + 1}{2}}$

Beweis

Siehe Lutz Volkmann: „Diskrete Strukturen“ Satz 3.6

Bemerkung

Satz 2.19 $\Rightarrow$ Satz 2.18

Bäume

2.20 Definition (*Baum, Wald*)

Ein *Baum* ist ein zusammenhängender Graph ohne Kreise. Ein *Wald* ist ein Graph, dessen Komponenten Bäume sind.

2.21 Lemma (*Endecken in Bäumen*)

Eine Endecke eines Graphen $G = (V, E)$ ist eine Ecke $x \in V$ mit $d(x) = 1$. Jeder Baum $T = (V, E)$ mit $|V| = 2$ enthält mindestens zwei Endecken.

Beweis

Sei $P = v_1 v_2 \dots v_k$ ein längster Weg in T. Angenommen es existiert ein $v \in V$, sodaß $v_k v \in E$. Dann ist $v \notin \{v_1, v_2, \dots, v_k\}$, da aus $v = v_i$ für ein $i \in \{1, 2, \dots, k-1\}$ folgt: $v_i \dots v_k v_i$ ist ein Kreis. Außerdem gilt auch nicht $v \in V \setminus \{v_1, v_2, \dots, v_k\}$, da in diesem Fall $v_1 \dots v_k v$ ein Weg wäre der länger als P ist. Es folgt also $v = v_{k-1}$ und somit $d(v_k) = 1$, womit v_k eine Endecke ist. Analog zeigt man, dass v_1 ebenfalls eine Endecke ist.

2.22 Satz

Sei $G = (V, E)$ ein Graph mit $|V| = n$ und $|E| = m$. Folgende Aussagen sind äquivalent:

1. G ist ein Baum
2. G ist zusammenhängend und kreisfrei
3. G ist zusammenhängend und $m = n - 1$
4. G ist kreisfrei und $m = n - 1$
5. Zwischen zwei Ecken von G existiert genau ein Weg
6. G ist maximal kreisfrei (d.h. durch Hinzufügen einer weiteren Kante entsteht ein Kreis)
7. G ist minimal zusammenhängend (d.h. durch Herausnehmen einer Kante zerfällt G in zwei Komponenten).

Beweis

Üblicherweise werden Beweise dieser Art geführt, indem man zeigt, daß (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (7) $\Rightarrow$ (1). Hier bietet es sich jedoch an zu zeigen, daß (2) $\Leftrightarrow$ (1) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (7) $\Rightarrow$ (2).
(2) $\Leftrightarrow$ (1) folgt unmittelbar aus der Definition von Bäumen. Wir zeigen deshalb nur exemplarisch (1) $\Rightarrow$ (3) (per Induktion über n).

Induktionsanfang: Für $n = 2$ gilt $m = 1 = 2 - 1 = n - 1$.

Induktionsschluss: Sei $n \geq 2$ und für alle Bäume $T' = (V', E')$ mit $|V'| = n$ gelte $|E'| = |V'| - 1$. Sei $T = (V, E)$ ein Baum mit $|V| = n + 1$ und x eine Endecke von G (eine Endecke existiert nach Lemma 2.21). $G - x := G[V \setminus \{x\}]$ ist ein Baum mit genau n Ecken und somit gilt nach Induktionsvoraussetzung $|E(G - x)| = n - 1$. Durch Hinzufügen von x zu $G - x$ wird auch genau eine Kante zu $G - x$ hinzugefügt ($d(x) = 1$) und somit gilt $|E(G')| = |E(G - x)| + 1 = (n - 1) + 1 = (n + 1) - 1$.

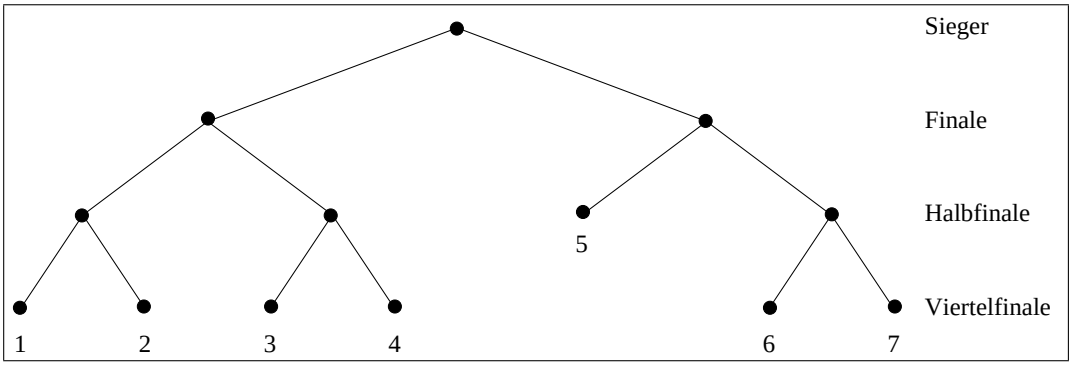
2.23 Definition (*Wurzelbaum*)

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

- Jede Ecke y auf dem Weg von w nach x heißt *Vorgänger* von x
- Ist y ein Vorgänger von x und $x \neq y$, so heißt x *Nachfolger* von y
- Ist $yx \in E(T)$, so heißt x bzw. y *unmittelbarer Nachfolger* bzw. *unmittelbarer Vorgänger*
- Ein *geordneter* Baum ist ein Wurzelbaum, in dem für die unmittelbaren Nachfolger jeder Ecke eine Ordnung festgelegt ist

2.24 Definition (*Tiefe eines Wurzelbaumes*)

Die *Tiefe* $depth(T)$ eines Wurzelbaumes T ist die maximale Länge eines Wegs von der Wurzel w zu einer Endecke.
Ein Wurzelbaum T mit der Tiefe t heißt *balanciert*, wenn jede Endecke von T auf Niveau t oder $t-1$ liegt. Z. B. ein Fussballturnier mit 7 Mannschaften:



2.25 Definition (*binärer Wurzelbaum*)

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

- T heißt *binärer* Wurzelbaum, wenn jede Ecke höchstens zwei unmittelbare Nachfolger hat
- T heißt *vollständig binärer* Wurzelbaum, wenn jede Ecke entweder genau zwei oder keine unmittelbaren Nachfolger hat

2.26 Satz (*Anzahl der Ecken in binären Bäumen*)

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

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

Beweis

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

Somit gilt $\sum_{k=0}^{t} P_k = n$. Da $1 \leq P_k \leq 2 \cdot P_{k-1}$ für $1 \leq k \leq t$ gilt, ist $P_k \leq 2^k$.

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

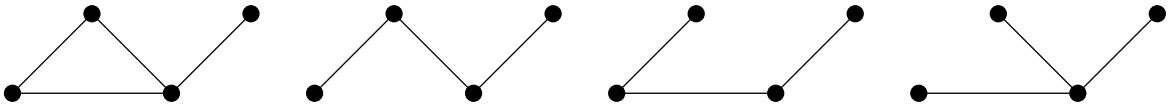
2.27 Folgerung (*Tiefe in binären Bäumen*)

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

Dann gilt $\boxed{t \geq \left\lceil ld\left(\frac{n+1}{2}\right)\right\rceil}$

2.28 Definition (*Gerüst*)

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



Graph und seine drei Gerüste

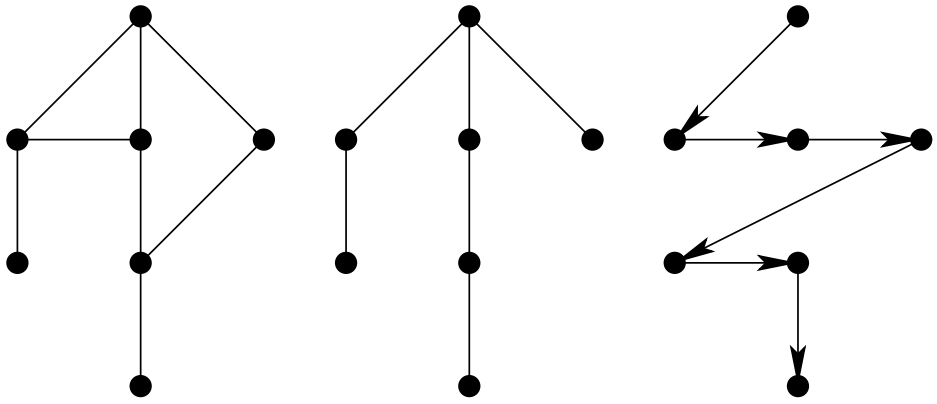
2.29 Satz

Jeder zusammenhängende Graph enthält ein Gerüst.

Beweis

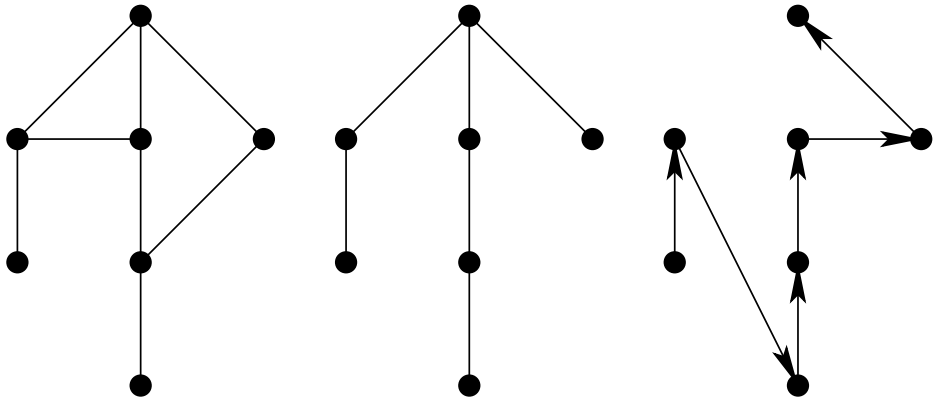
Enthält G keinen Kreis, so setze $T = G$ und T ist ein Gerüst von G. Sonst wähle einen Kreis $C = v_o v_1 v_2 \dots v_t v_0$ und nehme eine beliebige Kante von C heraus (z. B. $G' = (V, E \setminus \{v_0 v_1\})$ G' ist damit immer noch zusammenhängend) Fährt man so fort, dann erhält man einen Teilgraphen T, der kreisfrei ist. Also ist T ein Gerüst von G.

Algorithmus 1: Breitensuche *BFS : Breadth-First-Search*



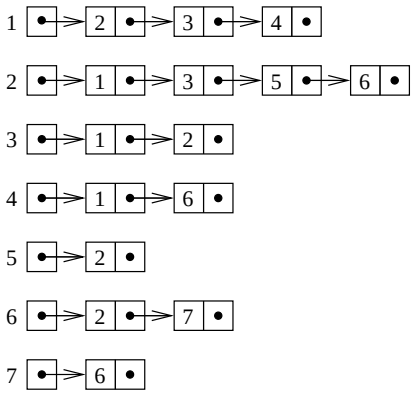
Graph Gerüst Breitensuche

Algorithmus 2: Tiefensuche *DFS : Depth-First-Search*



Graph Gerüst Tiefensuche

In der Informatik benutzt man sehr oft die Darstellung als Adjazenzliste:



Vor- und Nachteile:

	Adjazenzmatrix	Adjazenzliste
Speicherplatz	$\theta(\|V\|^2)$	$\theta(\|V\| + \|E\|)$
Prüfen ob $xy \in E$	$\theta(1)$	$\theta(min\{d(x), d(y)\})$
$N(x)$ bestimmen	$\theta(\|V\|)$	$\theta(d(x))$

2.30 Satz (*Cayley's Tree Formula*)

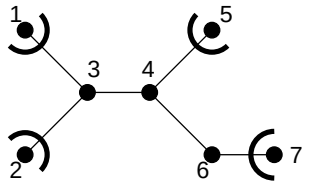
Sei G ein vollständiger markierter Graph mit $n \geq 2$ Ecken. Dann besitzt G n^{n-2} verschiedene Gerüste.

Beweis

Baum T auf $V = \{1, 2, \ldots, n\} \overset{\text{bijektiv}}{\longleftrightarrow} P(T) = \underbrace{(t_1, t_2, \ldots, t_{n-2})}_{\text{Prüfercode von} T} \in V^{n-2}$

Algorithmus „$\rightarrow$“

Eingabe: Baum $T = (V, E)$ mit $V = \{1, 2, \ldots, n\}$
Ausgabe: Wort $(t_1, t_2, \ldots, t_{n-2})$ über dem Alphabet $\{1, 2, \ldots, n\}$



$\rightarrow (3, 3, 4, 4, 6)$

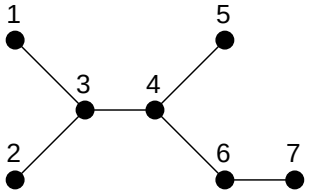
$i \leftarrow 1$
`WHILE` $|V| > 2$ `DO`

Bestimme die Endecke v im Baum T mit der kleinsten Markierung
$t_i \leftarrow$ Nachbar von v im Baum T
$T \leftarrow \big(V(T) \setminus \{v\}, E(T) \setminus \{vt_i\}\big)$
$i \leftarrow i + 1$

Algorithmus „$\leftarrow$“

Eingabe: Wort $(t_1, t_2, \ldots, t_{n-2})$ über dem Alphabet $\{1, 2, \ldots, n\}$
Ausgabe: Baum $T = (V, E)$ mit $V = \{1, 2, \ldots, n\}$

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



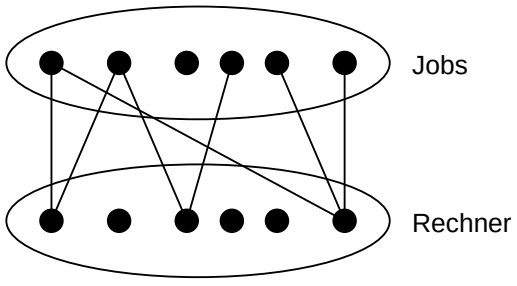
$S \leftarrow \emptyset$
`FOR` $i = 1$ `TO` $n - 2$ `DO`
Wähle die kleinste Ecke $s_i \in \{1, 2, \ldots, n\} \setminus S$ mit $s_i \notin \{t_i, t_{i+1}, \ldots, t_{n-2}\}$
Füge die Kante $e_i = s_i t_i$ in den Graphen ein
$S \leftarrow S \cup \{s_i\}$
Füge die Kante $e_{n-1} := \{1, 2, \ldots, n\} \setminus St_{n-2}$ in den Graphen ein

2.2 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

Graphentheoretisch können wir das obige Problem wie folgt formulieren:



Verteilung von Jobs auf Rechner

$J_l R_k \in E(G) \Leftrightarrow R_k$ erfüllt die Leistungsanforderungen von Job J_l

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

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

2.31 Definition (*Matching*)

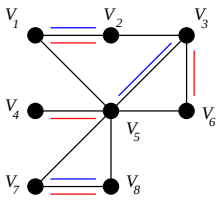
Sei $G = (V, E)$ ein Graph. Eine Kantenmenge $M \subseteq E(G)$ heißt *Matching* von G, wenn

$$\boxed{V(k_1) \cap V(k_2) = \emptyset \quad \forall k_1, k_2 \in M \quad k_1 \neq k_2}$$

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

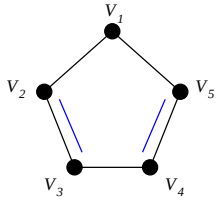
2.32 Beispiel

G_1 :



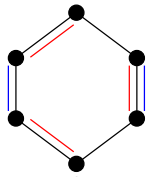
$M = \{V_1V_2, V_3V_5, V_7V_8\}$ maximal
$M = \{V_1V_2, V_3V_6, V_4V_5, V_7V_8\}$ perfekt

G_2 :



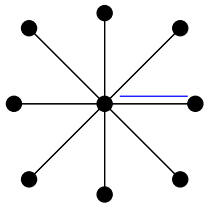
$M = \{V_2V_3, V_4V_5\}$ maximal
G_2 hat kein perfektes Matching

G_3 :



$M = \{V_2V_3, V_5V_6\}$ maximal
$M = \{V_1V_2, V_3V_4, V_5V_6\}$ perfekt

G_4 :



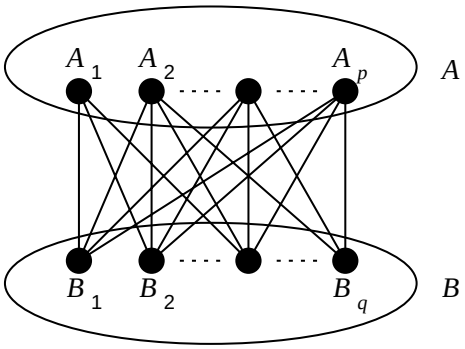
Sterngraph, hat kein perfektes und jeder beliebige Zweig ist ein maximales Matching.

2.33 Bemerkung

Für jeden Graphen $G = (V, e)$ gilt:

1. Jedes pefekte Matching ist ein Maximum-Matching
2. Für jedes Matching ist $|V(M)| = 2|M|$
3. Für ein perfektes Matching M von G gilt $2|M| = |V(G)|$
4. G hat ein perfektes Matching $\overset{\Rightarrow}{\not\Leftarrow} |V(G)|$ ist gerade

2.34 Definition (*vollständiger bipartiter Graph*)

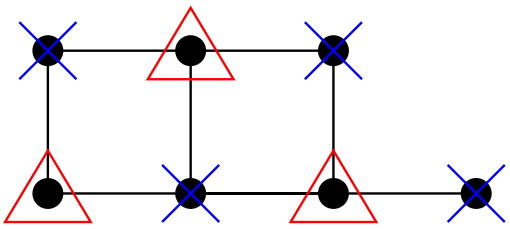


$K_{p,q}$ vollstängiger bipartiter Graph

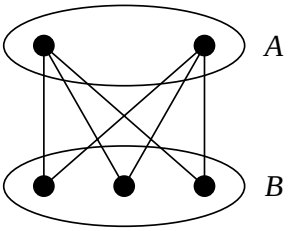
Ein Graph $G = (V, E)$ heißt *bipartit*, wenn sich $V(G)$ in zwei disjunkte Mengen A und B zerlegen läßt, so daß $G[A]$ und $G[B]$ Nullgrößen sind. A und B heißen *Partitionsmengen*. Ein vollständiger bipartiter Graph $K_{p,q}$ ist ein bipartiter Graph $(A \dot\cup B, E)$ mit $|A| = p$ und $|B| = q$ und $xy \in E$ für alle $x \in A$ und $y \in B$.

2.35 Beispiel

1)



2)



$K_{2,3}$ vollständiger bipartiter Graph

2.36 Satz (*König, 1916*)

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

2.37 Satz (*König-Hall*)

Sei $G = (A \dot\cup B, E)$ bipartit. Dann hat G ein Matching M mit $\boxed{|M| = |A| \Leftrightarrow |N(S)| \geq |S| \quad \forall S \subseteq A}$

Beweis

„$\Rightarrow$“: trivial

„$\Leftarrow$“: $U(a) := \{x \in V(G) | x$ ist durch einen M-alternierenden Weg mit a verbunden$\}$

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

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

Dann gilt: $B' = N(A')$ und $|B'| = |A'| - 1 \Rightarrow |A'| = |B'| + 1 = |N(A')| + 1 > |N(A')|$

2.38 Folgerung (*König, 1916*)

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

2.39 Folgerung (*König, 1916*)

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

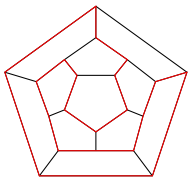
Beweis

Sukzessives Anwenden von Folgerung 2.38

2.40 Definition (*Multipartite Graphen*)

Ein Graph $G = (V, E)$ heißt k-partit (*multipartit*), wenn $V(G)$ in k disjunkte Mengen $V_1, V_2, \ldots, V_k$ zerlget werden kann, so daß $G[V_i]$ für $i = 1, \ldots, k$ Nullgraphen sind.

2.3 Hamiltonsche Graphen



3-regulärer
Dodekaeder D_{20}

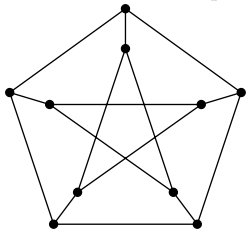
Im Jahre 1859 erfand Sir William Hamilton das Spiel „Rund um die Welt“. Dabei gilt es durch eine Menge von Städten zu reisen, wobei man jede Stadt nur einmal besucht und zum Schluß wieder am Ausgangspunkt ankommt. Die Abbildung zeigt einen Graphen mit 20 Knoten (Städten) und einen Pfad hindurch, welche die Bedingungen des Spiels erfüllt.

2.41 Definition (*Hamiltonkreis*)

Sei $G = (V, E)$. Ein Kreis C in G heißt *Hamiltonkreis*, falls $V(C) = V(G)$ ist. Ein Weg W in G heißt *Hamiltonweg*, falls $V(W) = V(G)$ ist. Enthält G einen Hamiltonkreis, so heißt G *Hamiltonscher Graph* und wenn G einen Hamiltonweg enthält, so heißt G *Semi-Hamiltonscher Graph*.

2.42 Beispiel

1. K_n mit $n \geq 3$ ist ein Hamiltonscher Graph
2. D_{20} ist ein Hamiltonscher Graph ($\rightarrow$ 2.3)
3. Der *Peterson-Graph* ist zwar nicht Hamiltonsch, aber dafür Semi-Hamiltonsch.



Bemerkung: Hamlitonsch $\overset{\rightarrow}{\not\leftarrow}$ Semi-Hamiltonsch

2.43 Satz (*Notwendige Bedingung*)

Ist G ein Hamiltonscher Graph, so gilt für jede nicht leere Eckmenge $S \subseteq V(G)$: $\boxed{\kappa(G - S) \leq |S|}$

Beweis

C sei Hamiltonkreis von G und $S = \{x_{n_1}, \ldots, x_{n_p}\}$ eine Eckmenge. Dann gilt:

$$\begin{array}{lcl} \kappa(C-\{x_{n_1}\}) & = & 1 \\ \kappa(C-\{x_{n_1},x_{n_2}\}) & \leq & 2 \\ \vdots & \leq & \vdots \\ \kappa(G-S) & \leq & \kappa(C-S)\leq |S| \end{array}$$

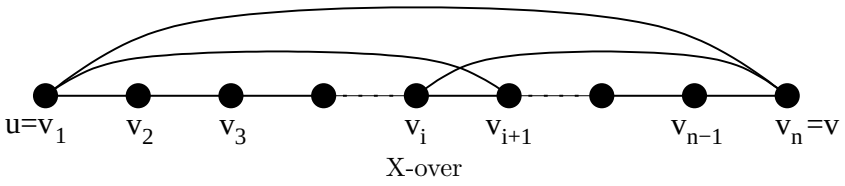
2.44 Satz (*Hinreichende Bedingung*)

Sei $G=(V,E)$ ein Graph mit $|V|=n$. Sein u und v zwei nicht adjazente Ecken mit $d(u)+d(v)\geq n$, dann gilt G ist Hamiltonsch $\Leftrightarrow G+uv$ ist Hamiltonsch.

Beweis

„$\Rightarrow$“: trivial
„$\Leftarrow$“: (indirekt)

Nehmen wir an $G+uv$ ist Hamiltonsch, aber G nicht. Dann enthält jeder Hamiltonkreis von $G+uv$ die Kante uv und ein X-over.



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

Dann folgt $S\cap T=\emptyset$, sonst hätten wir ein „X-over“ und $|S\cup T|\leq n-1\leq n$

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

Dies ist aber ein Widerspruch!

2.45 Folgerung (*Ore, 1960*)

Sei $G=(V,E)$ ein Graph mit $|V|=n$. Gilt für alle nicht adjazenten Ecken u,v die Ungleichung $d(u)+d(v)\geq n$, so ist G Hamiltonsch.

2.46 Folgerung (*Dirac, 1952*)

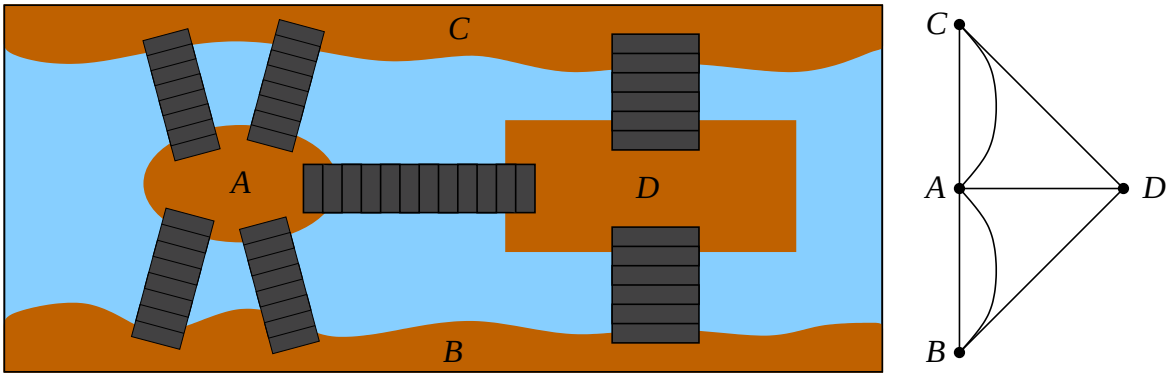
Sei $G=(V,E)$ ein Graph mit $|V|=n$. Ist $d(v)\geq\frac{n}{2}$ für alle $v\in V(G)$, so ist G Hamiltonsch.

2.47 Bemerkung

1. Hamilton-Graphen finden eine Anwendung bei der Lösung des Problems des Handlungsreisenden (*TSP: Travelling Salesman Problem*) .

2. Das Entscheidungsproblem, „enthält G einen Halbkreis?“, ist NP-vollständig (→ Informatikvorlesung(en))

2.4 Eulersche Graphen



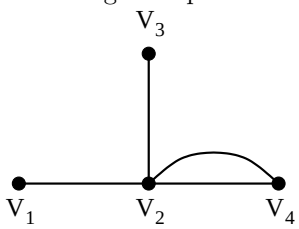
Das Königsberger Problem

2.48 Definition (*Kantenfolge, -zug, Eulertour*)

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

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

z. B.



$V_1V_2V_3V_2V_4$ Kantenfolge, aber kein Kantenzug
$V_1V_2V_4V_2$ Kantenzug

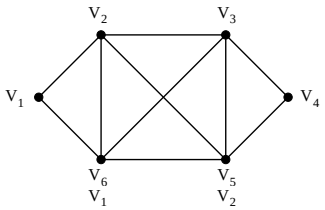
- Ein Kantenzug Z mit $E(Z) = E(G)$ heißt *Eulerscher Kantenzug*. Ein geschlossener Eulerscher Kantenzug heißt *Eulertour*.

2.49 Definition (*Eulersch, Semi-Eulersch*)

Sei $G = (V, E)$ zusammenhängend mit $|V| \geq 2$. G heißt *Semi-Eulersch*, falls G einen Eulerschen Kantenzug hat bzw. *Eulersch*, wenn G eine Eulertour hat.

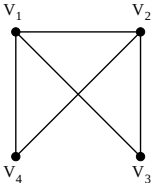
2.50 Beispiel

G_1 :



Eulertour z. B. $V_1V_2V_3V_4V_5V_6V_2V_5V_3V_6V_1$
G_1 ist Eulersch

G_2 :



Kantenzug t. B. $V_1V_2V_3V_1V_4V_2$
G_2 ist Semi-Eulersch

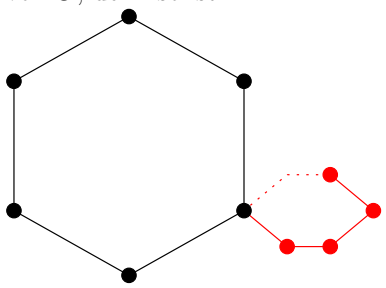
2.51 Satz

Sei $G = (V, E)$ zusammenhängend und $|V| = 2$. Dann gilt G ist Eulersch $\Leftrightarrow$ der Grad jeder Ecke ist gerade.

Beweis

„$\Rightarrow$“: trivial

„$\Leftarrow$“: Sei $z = x_0 x_1 \dots x_t$ ein längster Kantenzug in G Dann ist $x_t = x_0$ und z ist eine Eulertour von G, denn sonst:



2.52 Folgerung

Ein zusammenhängender Graph $G = (V, E)$ mit $|V| \geq 2$ ist Semi-Eulersch $\Leftrightarrow$ G besitzt zwei oder keine Ecke ungeraden Grades.

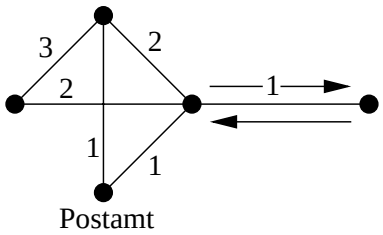
2.53 Bemerkung

1. Für Eulersche Graphen gibt es einen effizienten Algorithmus (*Fleury's Algorithmus*, mit der Komplexität $\Theta(|E(G)|)$), eine Eulertour zu konstruieren.

2. **Anwendungsbeispiel:** Chinesisches Briefträgerproblem (Kuan, 1962)

   Es geht darum einen möglichst kurzen Weg, vom Postamt aus beginnend, durch alle Anlieferstellen zu finden und zum Schluß wieder am Postamt anzukommen.

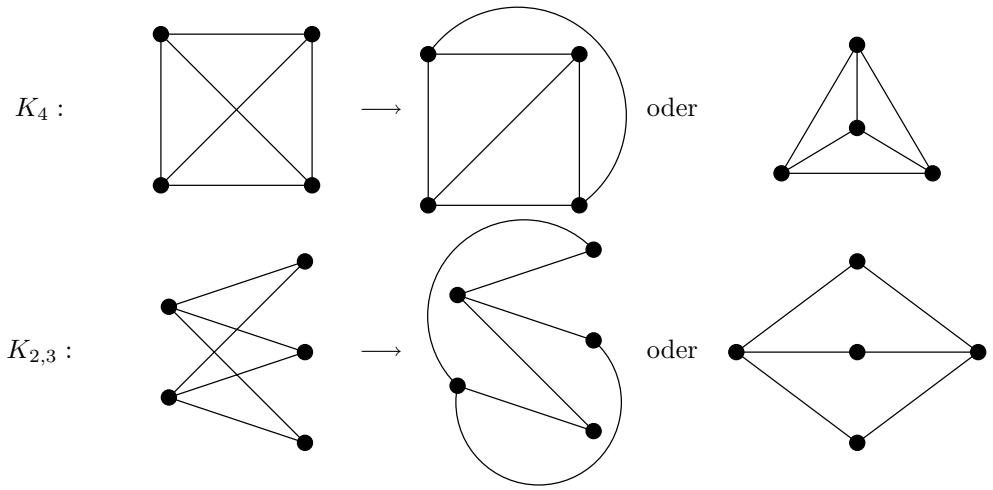
   Graphentheoretisch läßt sich dieses Problem folgendermaßen darstellen:
   Es sei $G = (V, E)$ ein zusammenhängender Graph mit einer Kantengewichtsfunktion $c : E \to \{q \in \mathbb{Q} | q > 0\}$. G heißt dann bewerteter Graph. Gesucht wird eine geschlossene Kantenfolge Z von minimaler Gesamtlänge mit $E(Z) = E(G)$.
   Beispiel:



2.5 Planare Graphen

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

Beispiele



2.54 Definition

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

1. G heißt *einbettbar* in den $\mathbb{R}^2$, wenn es ein Paar φ, φ' gibt, so daß gilt:

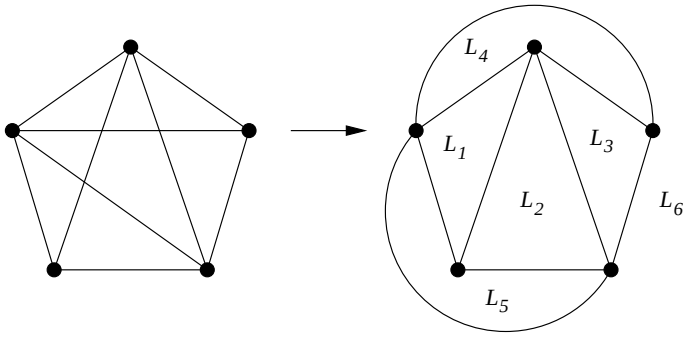
   $\varphi \quad : V \to \mathbb{R}^2$ injektiv
   $\varphi' \quad : E \to J = \{\underbrace{Bild(e) \,|\, e : [0,1] \to \mathbb{R}^2 \text{ stetig und injektiv}}_{\text{Jordankurve}}\}$

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

2. G heißt *planar*, wenn G in $\mathbb{R}^2$ einbettbar ist

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

4. Ist (G, φ, φ') ein ebener Graph, so heißen die Zusammenhangskomponenten von $\mathbb{R}^2 | \bigcup\limits_{e \in E} \varphi'(e)$ *Gebiete* (oder Länder) von (G, φ, φ').
   z. B.



$l(G)$:=Anzahl der Gebiete (oder Länder) von G
$l = 6 \quad |V| = 5 \quad |E| = 9$

2.55 Satz (*Eulersche Polyederformel, 1752*)

Sei $G = (V, E)$ ein zusammenhängender ebener Graph. Dann gilt: $\boxed{l(G) = |E| - |V| + 2}$

Beweis (Induktion über $m = |E| \overset{2.17}{\geq} |V| - 1$)

$m = |V| - 1$: G ist ein Baum
$1 = (\underbrace{|V| - 1}_{m}) - |V| + 2 \quad \surd$

$m \to m + 1$: Da G zusammenhängend ist und $|E(G)| = m + 1 \geq |V| \overset{\text{Satz } 2.22}{\Rightarrow} G$ 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.

$$\begin{array}{rrcll} \Rightarrow & l(G-e) & = & m - |V| + 2 & \mid +1 \\ & l(G) & = & |E(G)| - |V| + 2 & \end{array}$$

Bemerkung

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

2.56 Satz

Für jeden planaren Graphen $G = (V, E)$ mit $|V| \geq 3$ gilt: $\boxed{|E| \leq 3 \cdot |V| - 6}$

Beweis

o.B.d.A. G ist in $\mathbb{R}^2$ eingebettet, $l :=$Menge von Ländern

Jedes Land wird von mindestens 3 Kanten begrenzt und jede Kante begrenzt höchstens 2 Länder

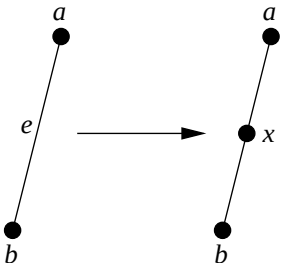
$$\Rightarrow 3 \cdot \underbrace{|L|}_{l(G)} \leq 2 \cdot |E| \overset{\text{Satz } 2.55}{\Rightarrow} \tfrac{2}{3} \cdot |E| \geq l(G) = |E| - |V| + 2 \Rightarrow |E| \leq 3 \cdot |V| - 6$$

2.57 Beispiel

1. K_5 ist nicht planar, denn $|E(K_5)| = \binom{5}{2} = 10 \not\leq 3 \cdot 5 - 6$
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 $|E| \leq 2 \cdot |V| - 4$

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

2.58 Definition (*Unterteilungsgraph*)



Es sei $G = (V, E)$ und $e = ab \in E(G)$. Wir sagen e wird *unterteilt*, wenn wir zu G eine neue Ecke x hinzufügen und die Kante e durch zwei neue Kanten ax und xb ersetzen.
Ein Graph H heißt *Unterteilungsgraph* von G, wenn man H aus G durch sukzessives Unterteilen von Kanten erhält.

2.59 Satz (*Kuratowski, 1936*)

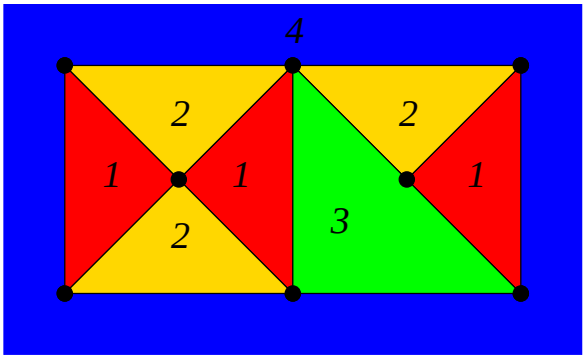
G ist planar $\Leftrightarrow$ $\boxed{\begin{array}{c}(K_5 \text{ und Unterteilungsgraphen von } K_5) \\ + \\ (K_{3,3} \text{ und Unterteilungsgraphen von } K_{3,3})\end{array}}$ sind keine Teilgraphen von G

2.60 Definition (*Färbung*)

Sei G eine Landkarte.

- Zwei verschiedene Länder F_1 und F_2 heißen *benachbart*, wenn es eine Kante gibt, die sowohl zum Rand von F_1, als auch zum Rand von F_2 gehört.
- Ist L die Menge der Länder von G, so nennt man eine Abbildung $H : L \to \{1, 2, \ldots, p\}$ *Färbung* oder p-Färbung von G, wenn $h(F_1) \neq h(F_2)$ für zwei verschiedene benachbarte Länder F_1 und F_2 gilt. Man sagt auch, daß sich die Landkarte G mit p Farben färben läßt.

2.61 Beispiel (*Färbung*)



2.62 Satz (*Vierfarbvermutung*)

Jede Landkarte läßt sich mit vier Farben färben.

Beweis

N. Robertson, 1997

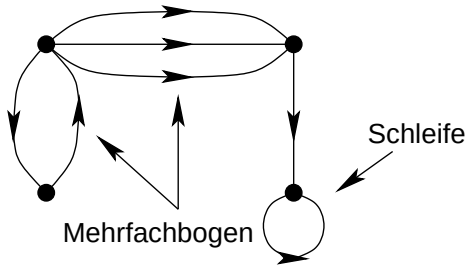
2.63 Bemerkung

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

2.6 Digraphen

2.64 Definition (*Digraph*)

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



Digraph

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

2.65 Definition

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

- $D' = (V', A')$ heißt *Teilgraph* von D, wenn $V \subseteq V$ und $A' \subseteq A \cap (V' \times V')$ sind, in Zeichen $D' \subseteq D$.
- Ein Teilgraph $D' = (V', A')$ heißt ein von V' *induzierter* Teilgraph, wenn $A' = A \cap (V' \times V')$, in Zeichen $D' = D[V']$.
- Orientierte Kantenfolge der Länge p in D: $F : x_0x_1x_2 \dots x_p$ mit $x_i \in V(D), \quad i = 0, 1, \dots, p$ und $x_ix_{i+1} \in A(D), \quad i = 0, 1, \dots, p-1$
- Orientierter Kantenzug:= Orientierte Kantenfolge mit paarweise verschiedenen Bögen
- Orientierter Weg:= Orientierte Kantenfolge mit paarweise verschiedenen Ecken
- Geschlossene Kantenfolge:=...
- Orientierter Kreis der Länge q:= Eine geschlossene Kantenfolge mit der Länge q mit genau q Ecken
- Eulertour in D:= Ein geschlossener Kantenzug Z in D mit $A(Z) = A(D)$
- Hamiltonscher Weg von D:= Ein Weg W in D mit $V(W) = V(D)$
- Hamiltonscher Kreis von D:= Ein Kreis C in D mit $V(D) = V(C)$
- Für $x \in V(D)$ definieren wir:
  $N^+(x) = \{y | xy \in A(D)\}$
  $N^-(x) = \{w | wx \in A(D)\}$
  $d^+(x) = |N^+(x)| \qquad \delta^+(D) = min\{d^+(x) | x \in V(D)\}$
  $\Delta^+(D) = max\{d^+(x) | x \in V(D)\}$
  $d^-(x) = |N^-(x)| \qquad \delta^-(D) = min\{d^-(x) | x \in V(D)\}$
  $\Delta^-(D) = max\{d^-(x) | x \in V(D)\}$
- Der untergeordnete Graph von D ist $G(D) = (V(D), \{\underbrace{xy}_{\text{Kante}} \mid \underbrace{xy}_{\text{Bogen}} \in A(D)\})$ (in Zeichen $G(D)$)

2.66 Definition

Eine *stark zusammenhängende Komponente* H von D ist ein maximaler Teilgraph von D, sodaß H für zwei beliebige Ecken $u, v \in V(H)$ einen orientierten Weg von u nach v enthält. D heißt stark zusammenhängend, wenn D nur eine stark zusammenhängende Komponente hat.

2.67 Definition (*Turnier*)

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.

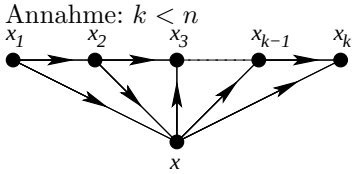
2.68 Satz (*Redei, 1934*)

Jedes Turnier besitzt einen orientierten Hamiltonschen Weg.

Beweis

Sei T_n ein Turnier und sei $W = \underbrace{x_1 x_2 \dots x_k}_{\text{Länge } k-1}$ ein längster orientierter Weg in T_n.

Annahme: $k < n$



Sei $x \in V(T_n) \setminus V(W)$. Dann haben wir $x_1 \to x \to x_k \Rightarrow \exists i \in \{1, \dots, k-1\}$ mit $x_i \to x \to x_{i+1}$
So ist $x_1 x_2 \dots x_i x x_{i+1} \dots x_k$ ein orientierter Weg in T_n mit der Länge k. Widerspruch!

2.69 Satz

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

Beweis (vollständige Induktion über p)

2.70 Bemerkung

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

Kapitel 3

Algebraische Strukturen

3.1 Universelle Algebren

3.1 Definition (*n-stellige Operation*)

Ist $\mathbf{M}$ eine Menge, so heißt eine Abbildung $f : \mathbf{M}^n := \underbrace{\mathbf{M} \times \mathbf{M} \times \ldots \times \mathbf{M}}_{n-\text{mal}} \to \mathbf{M}$ eine *n-stellige Operation* oder ein *n-stelliger Operator*.

- $n = s(f)$ heißt *Stelligkeit* vom Operator f
- Ein zweistelliger Operator (d. h. $f : \mathbf{M} \times \mathbf{M} \to \mathbf{M}$) heißt auch *Verknüpfung* (engl. *binary operation*)

3.2 Definition (*Universelle Algebra, Indexmenge, Signatur*)

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

3.3 Beispiel

1. Die *boolesche Algebra* $(\{\text{T,F}\}, \vee, \wedge, \neg)$ hat Signatur $(2, 2, 1)$.

$\vee$	T	F
T	T	T
F	T	F

Oder

$\wedge$	T	F
T	T	F
F	F	F

Und

$\neg$T:=F
$\neg$F:=T

Negation

2. Mit den üblichen arithmetischen Operationen wie „+“ und „·“ können wir unterschiedlische Algebren definieren:
   - $(\mathbb{N}, +)$, $(\mathbb{N}, +, \cdot)$
   - $(\mathbb{Z}, \cdot)$
   - $(\{x \in \mathbb{N} \mid x \text{ ist Quadratzahl}\}, \cdot)$
     (denn für $x = a^2$ und $y = b^2$ ist $x \cdot y = a^2 \cdot b^2 = (a \cdot b)^2$, d. h. $\cdot : \mathbf{M} \times \mathbf{M} \to \mathbf{M}$)
   - $(\{x \in \mathbb{N} \mid x \text{ ist Quadratzahl}\}, +)$ ist keine Algebra, denn die Summe von $4 = 2^2$ und $9 = 3^2$ ist keine Quadratzahl.
3. Sei Σ eine Menge, auch *Alphabet* genannt. Dann heißen $\Sigma^* = \{(a_1 a_2 \ldots a_n) \mid a_i \in \Sigma, n \in \mathbb{N}_0\}$ die *Wörter* über dem Alphabet Σ.
   $\bullet : \Sigma^* \times \Sigma^* \to \Sigma^*$ mit $(a_1 a_2 \ldots a_n) \bullet (b_1 b_2 \ldots b_n) = (a_1 \ldots a_n b_1 \ldots b_n)$
   $(\Sigma^*, \bullet)$ ist eine Algebra

4. Sei $\mathbf{U}$ eine beliebige Menge und $F(\mathbf{U}) := \{f \mid f : \mathbf{U} \to \mathbf{U}\}$. $\circ$: *Komposition* von zwei Funktionen, also $(f \circ g)(x) = f(g(x))$ für alle $x \in \mathbf{U}$
$(F(\mathbf{U}), \circ)$ ist eine Algebra

3.4 Definition (*Neutrale Elemente*)

Sei $(\mathbf{M}, \circ)$ eine Algebra mit einem zweistelligen Operator „$\circ$“.

- Ein Element $e \in \mathbf{M}$ heißt *linksneutrales Element* für den Operator „$\circ$“, falls $e \circ a = a \quad \forall a \in \mathbf{M}$.
- Ein Element $e \in \mathbf{M}$ heißt *rechtsneutrales Element* für den Operator „$\circ$“, falls $a \circ e = a \quad \forall a \in \mathbf{M}$.
- Ein Element $e \in \mathbf{M}$ heißt *neutrales Element* für den Operator „$\circ$“, falls e sowohl ein linksneutrales, als auch ein rechtsneutrales Element ist, also $e \circ a = a \circ e = a \quad \forall a \in \mathbf{M}$.

3.5 Beispiel

Sei $(\{b, c\}, \circ)$ eine Algebra mit der Verknüpfung

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

$\left.\begin{array}{l} b \circ b = b \\ c \circ b = c \end{array}\right\} \Rightarrow b$ ist ein rechtsneutrales Element

$\left.\begin{array}{l} b \circ c = b \\ c \circ c = c \end{array}\right\} \Rightarrow c$ ist ein rechtsneutrales Element

$\left.\begin{array}{l} b \circ b = b \\ b \circ c = b \end{array}\right\} \Rightarrow b$ ist <u>kein</u> linksneutrales Element

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

3.6 Lemma

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

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

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

Beweis

$\left.\begin{array}{ll} \star & \Rightarrow c \circ d = d \\ \triangle & \Rightarrow c \circ d = c \end{array}\right\} \Rightarrow c = d$

♡ Eindeutigkeit des neutralen Elements :

Annahme: e_1 und e_2 sind zwei neutrale Elemente
$e_1 \overset{e_2 r}{=} e_1 \circ e_2 \overset{e_2 l}{=} e_2$

3.7 Beispiel (*siehe Beispiel 3.3*)

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

3.8 Definition (*Inverse Elemente*)

Sei $(\mathbf{M}, \circ)$ eine Algebra vom Typ (2) und neutralem Element e.

- Ein Element $x \in \mathbf{M}$ heißt *linksinverses Element* von $a \in \mathbf{M}$, falls $x \circ a = e$
- Ein Element $x \in \mathbf{M}$ heißt *rechtsinverses Element* von $a \in \mathbf{M}$, falls $a \circ x = e$
- Ein Element $x \in \mathbf{M}$ heißt *inverses Element* (oder *Inverses*) von $a \in \mathbf{M}$, falls x sowohl ein linksinverses Element, als auch ein rechtsinverses Element von a ist.

3.9 Definition (*Halbgruppe*)

Eine Algebra $\mathbf{A} = (\mathbf{M}, \circ)$ mit einem zweistelligen Operator $\circ$ vom Typ (2) heißt *Halbgruppe*, falls der Operator $\circ$ assoziativ ist, also $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in \mathbf{M}$.

z. B. $(\Sigma^*, \circ)$ im Beispiel 3.3 ist eine Halbgruppe

3.10 Definition (*Monoid*)

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

$M1:$ $\circ$ assoziativ ist (d. h. $\mathbf{A} = (\mathbf{M}, \circ)$ ist eine Halbgruppe) und

$M2:$ ein neutrales Element $e \in \mathbf{M}$ existiert

3.11 Definition (*Gruppe*)

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

$G1:$ $\circ$ assoziativ ist (d. h. $\mathbf{A} = (\mathbf{M}, \circ)$ ist eine Halbgruppe) und

$G2:$ ein neutrales Element $e \in \mathbf{M}$ existiert und

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

3.12 Definition (*Abelsche Algebra*)

Eine Halbgruppe (ein Monoid, eine Gruppe) $\mathbf{A} = (\mathbf{M}, \circ)$ heißt *abelsch*, falls $\circ$ kommutativ ist, also $a \circ b = b \circ a \quad \forall a, b \in \mathbf{M}$.

3.13 Definition (*Ring*)

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

$R1:$ $\mathbf{A} = (\mathbf{M}, \oplus)$ eine abelsche Gruppe mit neutralem Element $0 \in \mathbf{M}$ ist und

$R2:$ $\mathbf{A} = (\mathbf{M}, \odot)$ ein Monoid mit neutralem Element $1 \in \mathbf{M}$ ist und

$R3:$ $\oplus$ und $\odot$ sind distributiv, also $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ und $(b \oplus c) \odot c) = (b \odot a) \oplus (c \odot a)$ $\forall a, b, c \in \mathbf{M}$

3.14 Definition (*Körper*)

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

$K1:$ $\mathbf{A} = (\mathbf{M}, \oplus)$ eine abelsche Gruppe mit neutralem Element $0 \in \mathbf{M}$ ist und

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

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

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

3.15 Definition (*boolesche Algebra*)

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

$B1:$ $\mathbf{A} = (\mathbf{M}, \oplus)$ ein abelsches Monoid mit neutralem Element $0 \in \mathbf{M}$ ist und

$B2:$ $\mathbf{A} = (\mathbf{M}, \odot)$ ein abelsches Monoid mit neutralem Element $1 \in \mathbf{M}$ ist und

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

$B4:$ das Distributivgesetz gilt: $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \quad \forall a, b, c \in \mathbf{M}$
$a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c) \quad \forall a, b, c \in \mathbf{M}$

3.16 Beispiel

1. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring, d. h. $(\mathbb{Z}, +, \cdot)$ ist ein Ring und zusätzlich gilt $a \cdot b = b \cdot a \quad \forall a, b \in \mathbb{Z}$
2. Sei $\mathbf{K}$ ein Körper, dann ist
   - $\mathbf{K}[x] := \left\{ \sum_{k=0}^{n} a_k x^k \,\middle|\, a_k \in \mathbf{K},\ n \in \mathbb{N}_0 \right\}$* ein kommutativer Ring (Polynomring)
   - $\mathbf{K}[\![x]\!] := \left\{ \sum_{n=0}^{\infty} a_n x^n \,\middle|\, a_n \in \mathbf{K} \right\}$ ein kommutativer Ring mit Null $0 = 0 \cdot x^0$ und Eins $1 = 1 \cdot x^0$ (vgl. Satz 1.32)
   - $\mathbf{K}^{n \times n} := \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \,\middle|\, a_{ij} \in \mathbf{K},\ 1 \le i,\ j \le n \right\}$ mit $n > 1$ ein nicht-kommutativer Ring (mit Null $\underline{0}$ und Eins E_n†)
3. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper
4. Der kleinsten Ring: $\{0\}$ mit „0“ = „1“ und „ + “ = „ $\cdot$ “
   Der kleinste Körper: $\mathbb{F}_2 = \{0, 1\}$

Konvention

Sei $(\mathbf{K}, \oplus, \odot)$ ein Körper

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

3.2 Unteralgebren, Homomorphismen, Kongruenzen

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

3.17 Definition (*Unteralgebra*)

$\mathbf{U} \subseteq \mathbf{A}$ heißt Unteralgebra von $\mathbf{A}$ (in Zeichen $\mathbf{U} \le \mathbf{A}$), falls die Operatoren f_i abgeschlossen sind, d. h. $\{f_i(u_1, \ldots, u_{n_i}) |\, u_1, \ldots, u_n \in \mathbf{U}\} = f_i(\mathbf{U}^{n_i}) \subseteq \mathbf{U}$ für alle $i \in \mathbf{I}$

*Menge der Polynome über $\mathbf{K}$
†Einheitsmatrix

3.18 Definition (*Untergruppe, Teilring*)

- Sei $\mathbf{G} = (\mathbf{G}, \cdot)$ eine Gruppe.
  Eine Unteralgebra $\mathbf{U} \leq \mathbf{G}$ heißt *Untergruppe* von $\mathbf{G}$, falls $(\mathbf{U}, \cdot)$ eine Gruppe ist. (d. h. für alle $u, u' \in \mathbf{U}$ gilt: $u \cdot u' \in \mathbf{U},\ u^{-1} \in \mathbf{U}$ und $\underline{1} \in \mathbf{U}$)
- Sei $\mathbf{R} = (\mathbf{R}, \oplus, \odot)$ ein Ring.
  Eine Unteralgebra $\mathbf{U} \leq \mathbf{R}$ heißt *Teilring* oder *Unterring* von $\mathbf{R}$, falls $(\mathbf{U}, \oplus, \odot)$ ein Ring ist.

3.19 Beispiel

1. $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$
2. Sei $\mathbf{Z}_n := \{0, 1, \ldots, n-1\}$ und $+_n : \mathbb{N} \times \mathbb{N} \to \mathbf{Z}_n$ mit $+_n(a, b) = (a + b)\ mod\ n \quad \forall a, b \in \mathbb{N}$

   z. B. $n = 5:$ $\quad \mathbf{Z}_5 = \{0, 1, 2, 3, 4\} \quad +_5 : \mathbb{N} \times \mathbb{N} \to \mathbf{Z}_5$

   $1 +_5 2 = 3 \quad 2 +_5 3 = 0 \quad 3 +_5 6 = 4$

   Dann ist $(\mathbf{Z}_n, +_n)$ keine Untergruppe von $(\mathbb{Z}, +)$, da sich dir Operatoren unterscheiden: z. B. $2 + 3 = 5$, aber $2 +_5 3 = 0$

3.20 Lemma

Sei $\mathbf{J}$ eine Indexmenge und $\mathbf{U}_j \leq \mathbf{A}$ für $j \in \mathbf{J}$. Dann gilt $\bigcap\limits_{j \in \mathbf{J}} \mathbf{U}_j \leq \mathbf{A}$

3.21 Definition (*erzeugte Unteralgebra*)

Sei $\mathbf{M}$ eine Teilmenge von einer Algebra $\mathbf{A}$.

$\langle \mathbf{M} \rangle = \bigcap \{\mathbf{U} \,|\, \mathbf{M} \subseteq \mathbf{U} \leq \mathbf{A}\}$ heißt die von $\mathbf{M}$ erzeugte Unteralgebra.

3.22 Beispiel

1. Sei $\mathbf{G} = (\mathbf{G}, \circ)$ eine Gruppe und sei $g \in \mathbf{G}$ und $\langle \{g\} \rangle = \{g^i \,|\, i \in \mathbb{Z}\}$, die von g erzeugte Unteralgebra, wobei $g^i := \begin{cases} \overbrace{g \circ \cdots \circ g}^{i\text{-mal}} & \text{falls } i > 0 \\ 1 & \text{falls } i = 0 \\ \underbrace{g^{-1} \circ \cdots \circ g^{-1}}_{-i\text{-mal}} & \text{falls } i < 0 \end{cases}$
2. $\langle \{g_1, \ldots, g_n\} \rangle = \left\{a_1, \ldots, a_m \,|\, m \in \mathbb{N}_0,\ a_j \in \{g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}\}\right\}$

3.23 Definition (*Homomorphismus*)

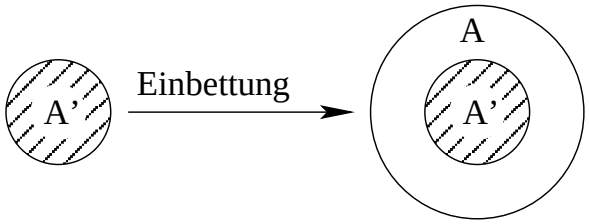
Seien $\mathbf{A} = (\mathbf{A}, (f_i)_{i \in \mathbf{I}})$ und $\widetilde{\mathbf{A}} = (\widetilde{\mathbf{A}}, (\widetilde{f}_i)_{i \in \mathbf{I}})$ Algebren vom gleichen Typ $\mathbf{T} = (n_i)_{i \in \mathbf{I}}$, d. h. $n_i = s(f_i) = s(\widetilde{f}_i)$.
Eine Abbildung $\varphi : \mathbf{A} \to \widetilde{\mathbf{A}}$ heißt (Algebra-)*Homomorphismus* von $\mathbf{A}$ nach $\widetilde{\mathbf{A}}$, falls für alle $i \in \mathbf{I}$ die Operatoren f_i und $\widetilde{f}_i$ mit φ vertauschbar sind, also $\widetilde{f}_i(\varphi(a_1), \ldots, \varphi(a_{n_i})) = \varphi(f_i(a_1, \ldots, a_{n_i}))$ für alle $a_i \in \mathbf{A}$, $j = 1, \ldots, n$ und $i \in \mathbf{I}$.

$$\begin{array}{ccc} \mathbf{A}^{n_i} & \xrightarrow{f_i} & \mathbf{A} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ \widetilde{\mathbf{A}}^{n_i} & \xrightarrow{\widetilde{f}_i} & \widetilde{\mathbf{A}} \end{array}$$

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

3.24 Beispiel

1. Sei $\mathbf{A} = (\mathbf{A}, (f_i)_{i\in\mathbf{I}})$* eine Algebra und $\mathbf{A}' \leq \mathbf{A}$. Dann ist id : $\mathbf{A}' \to \mathbf{A}$ mit $a \to a$ für alle $a \in \mathbf{A}'$ ein Homomorphismus von $\mathbf{A}'$ nach $\mathbf{A}$, oder: die „kleinere“ Algebra $\mathbf{A}'$ ist in die „größere“ Algebra $\mathbf{A}$ eingebettet:



   z. B. $\mathbf{A} = (\mathbb{N}, +)$ $\widetilde{\mathbf{A}} = (\mathbb{Z}, +)$ $\mathbf{A} \leq \widetilde{\mathbf{A}}$

   $\varphi : \mathbb{N} \to \mathbb{Z}$ mit $n \to n$ $\forall n \in \mathbb{N}$ ist ein Homomorphismus von $\mathbf{A}$ nach $\widetilde{\mathbf{A}}$

2. $\mathbf{A} = (\sum^*, \bullet)$ $\widetilde{\mathbf{A}} = (\mathbb{N}_0, +)$

   $\varphi : \sum^* \to \mathbb{N}_0$ mit $w \to |w|$† $\forall w \in \sum^*$ ist ein Homomorphismus von $\mathbf{A}$ nach $\widetilde{\mathbf{A}}$

3. Sei $\mathbf{K}$ ein Körper und $\mathbf{V}, \mathbf{W}$ zwei $\mathbf{K}$-Vektorräume.

   $\varphi : \mathbf{V} \to \mathbf{W}$ ist ein Homomorphismus $\Leftrightarrow$ φ ist k-linear

   d. h.

   - $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ $\forall v_1, v_2 \in \mathbf{V}$
   - $\varphi(-v) = -\varphi(v)$ $\forall v \in \mathbf{V}$
   - $\varphi(0 \in \mathbf{V}) = 0 \in \mathbf{W}$
   - $\varphi(\alpha \cdot v) = \alpha \cdot \varphi(v)$ $\forall \alpha \in \mathbf{K}, v \in \mathbf{V}$

3.25 Definition (*Isomorphismus, Automorphismus*)

Seien $\mathbf{A} = (\mathbf{A}, (f_i)_{i\in\mathbf{I}})$ und $\widetilde{\mathbf{A}} = (\widetilde{\mathbf{A}}, (\widetilde{f}_i)_{i\in\mathbf{I}})$ Algebren vom gleichen Typ $\mathbf{T} = (n_i)_{i\in\mathbf{I}}$.
Eine Abbildung $\varphi : \mathbf{A} \to \widetilde{\mathbf{A}}$ heißt *Isomorphismus* von $\mathbf{A}$ nach $\widetilde{\mathbf{A}}$, falls

1. φ ein Homomorphismus von $\mathbf{A}$ nach $\widetilde{\mathbf{A}}$ ist und
2. φ bijektiv ist.

Ein bijektiver Homomorphismus heißt *Isomorphismus*.

$\mathbf{A} \cong \widetilde{\mathbf{A}}$ ($\mathbf{A}$ *isomorph* zu $\widetilde{\mathbf{A}}$) $\Leftrightarrow \exists$ *Isomorphismus* von $\mathbf{A}$ nach $\widetilde{\mathbf{A}}$

Ein Isomorphismus einer Algebra $\mathbf{A}$ nach $\mathbf{A}$ heißt *Automorphismus*.

3.26 Beispiel (*Isomorphismus, Automorphismus*)

1. $\mathbf{A} = (\mathbb{N}, +)$ $\widetilde{\mathbf{A}} = (\{2n \,|\, n \in \mathbb{N}\}, +)$ $\varphi : \mathbb{N} \to \{2n \,|\, n \in \mathbb{N}\}$ mit $n \to 2n$ $\forall n \in \mathbb{N}$ ist ein Isomorphismus von $\mathbf{A}$ nach $\widetilde{\mathbf{A}}$
2. $\mathbf{A} = (\mathbb{R}^+, \cdot)$ $\widetilde{\mathbf{A}} = (\mathbb{R}, +)$ $\varphi : \mathbb{R}^+ \to \mathbb{R}$ mit $x \to \log x$ $\forall x \in \mathbb{R}^+$ ist ein Isomorphismus für die Logarithmusfunktion. Es gilt: $\log(x \cdot y) = \log x + \log y$ $\forall x, y \in \mathbb{R}^+$

*siehe Beispiel 3.3
†Länge des Wortes „w“

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

0	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

$\varphi : 1 \to 2, \quad 2 \to 1, \quad 3 \to 3$ ist ein Automorphismus

3.27 Lemma

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

3.28 Lemma

Ist φ ein Isomorphismus der Algebra $\mathbf{A}$ in die Algebra $\widetilde{\mathbf{A}}$, so gibt es auch einen Isomorphismus φ^{-1} von $\widetilde{\mathbf{A}}$ nach $\mathbf{A}$.

$$\begin{array}{rcccl} \varphi & : & \mathbf{A} & \to & \widetilde{\mathbf{A}} \\ & & \mathbf{A} & \leftarrow & \widetilde{\mathbf{A}} \quad : \quad \varphi^{-1} \end{array}$$

Erinnerung an Lineare Algebra

Sei $\mathbf{M}$ eine Menge.

- Eine *Relation* $\mathbf{R}$ auf $\mathbf{M}$ ist eine Teilmenge $\mathbf{R} \subseteq \mathbf{M} \times \mathbf{M}$.
- Eine Relation $\mathbf{R}$ auf $\mathbf{M}$ heißt *Äquivalenzrelation*, falls $\mathbf{R}$ reflexiv, symmetrisch und transitiv ist.
- $\mathbf{M}/_{\mathbf{R}} := \underbrace{\text{Menge der Äquivalenzklassen von } \mathbf{R}}_{\subseteq \mathcal{P}(\mathbf{M})}$

3.29 Beispiel

Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$

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

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

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

3.30 Definition (*Kongruenzrelation*)

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

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

3.31 Beispiel

Sei $\mathbf{G} = (\mathbf{G}, \circ)$ eine Gruppe und sei $\sim$ eine Äquivalenzrelation auf $\mathbf{G}$.

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

3.32 Satz (*Homomorphiesatz*)

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

1. Für jedes $a \in \mathbf{A}$ bezeichnen wir mit $[a]_\sim = \{a' \in \mathbf{A} \mid a' \sim a\}$ die Äquivalenzklasse von a. Dann wird die Menge der Äquivalenzklassen $\mathbf{A}/_\sim =: \{[a]_\sim \mid a \in \mathbf{A}\}$ eine Algebra vom Typ $(n_i)_{i \in \mathbf{I}}$ mit $\overline{f_i}([a_1]_\sim, [a_2]_\sim, \ldots, [a_n]_\sim) := [f_i(a_1, a_2, \ldots, a_{n_i})]_\sim$ und $\pi_\sim : \mathbf{A} \to \mathbf{A}/_\sim$ mit $a \to [a]_\sim$ ist ein *surjektiver Homomorphismus*, bzw. *Epimorphismus*.

2. Ist $\varphi : \mathbf{A} \to \mathbf{B}$ ein Homomorphismus, so wird dann durch $a \sim a' \Leftrightarrow \varphi(a) = \varphi(a')$ eine Kongruenzrelation auf $\mathbf{A}$ definiert

   - und $\varphi(\mathbf{A})$ ist eine Unteralgebra von $\mathbf{B}$
   - und es gibt einen Isomorphismus $\overline{\varphi} : \mathbf{A}/_\sim \to \varphi(\mathbf{A})$ mit $[a]_\sim \to \varphi(a)$

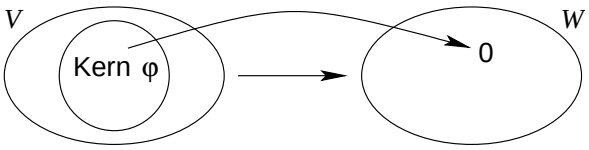
3.33 Beispiel

Sei $\mathbf{K}$ ein Körper und seinen $\mathbf{V}, \mathbf{W}$ zwei $\mathbf{K}$-Vektorräume.

$\varphi : \mathbf{V} \to \mathbf{W}$ ist ein Homomorphismus

$$\begin{aligned} \forall v, v' \in \mathbf{V} : v \sim v' &\overset{\text{def}}{\Longleftrightarrow} && \varphi(v) = \varphi(v') \\ &\Longleftrightarrow && \varphi(v) - \varphi(v') = 0 \\ &\overset{\text{Beispiel 3.24 3.}}{\underset{\varphi \text{ ist } k\text{-linear}}{\Longleftrightarrow}} && \varphi(v - v') = 0 \Leftrightarrow v - v' \in \operatorname{Kern} \varphi \leq \mathbf{V} \end{aligned}$$

also $[v]_\sim = v + \operatorname{Kern} \varphi \quad \forall v \in \mathbf{V}$ und $[0]_\sim = \operatorname{Kern} \varphi$



3.3 Ringe und Ideale

Erinnerung an Definition 3.13
Eine Algebra $\mathbf{R} = (\mathbf{R}, +, \cdot)$ vom Typ $(2, 2)$ ist ein Ring, falls

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

3.34 Lemma

Sei $\mathbf{R}$ ein Ring.

1. $a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in \mathbf{R}$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b) \quad \forall a, b \in \mathbf{R}$

3. $-(-a) = a \quad \forall a \in \mathbf{R}$
4. $-(a+b) = (-a) + (-b) \quad \forall a, b \in \mathbf{R}$

Sei $\sim$ eine Kongruenzrelation auf $\mathbf{R}$. Wir betrachten die Teilmenge $[0]_\sim := \{a \in \mathbf{R} \mid a \sim 0\}$.

- $a \sim a' \quad \overset{-a' \sim -a'}{\Leftrightarrow} \quad \underbrace{a + (-a')}_{a-a'} \sim \underbrace{a' + (-a')}_{0}$
  $\Leftrightarrow \quad a - a' \in [0]_\sim$
  Also ist $\sim$ vollständig beschrieben durch $[0]_\sim$
- Seien $u, v \in [0]_\sim$. Dann gilt: $u \sim 0, \quad v \sim 0 \Rightarrow u + v \in [0]_\sim$

3.35 Definition (*Ideal*)

Sei $\mathbf{R} = (\mathbf{R}, +, \cdot)$ ein Ring. $\mathbf{I} \subseteq \mathbf{R}$ heißt *Ideal* (in Zeichen $\mathbf{I} \trianglelefteq \mathbf{R}$), wenn

- $\underline{0} \in \mathbf{I}$
- $a, b \in \mathbf{I} \Rightarrow a + b \in \mathbf{I}$
- $-a \in \mathbf{I}, \quad a \in \mathbf{R}, \quad u \in \mathbf{I} \Rightarrow a \cdot u \in \mathbf{I}$ und $u \cdot a \in \mathbf{I}$

3.36 Satz

Ist $\sim$ eine Kongruenzrelation auf $\mathbf{R}$, so ist $\mathbf{I} = [0]_\sim \trianglelefteq \mathbf{R}$.
Umgekehrt: Ist $\mathbf{I} \trianglelefteq \mathbf{R}$, so wird durch $a \sim a' :\Leftrightarrow a - a' \in \mathbf{I}$ eine Kongruenzrelation definiert.
(Dabei ist $[0]_\sim = \mathbf{I}$ und $[a]_\sim = a + \mathbf{I}$)

Schreibweise: $\mathbf{R}/_{\mathbf{I}} := \mathbf{R}/_\sim$

3.37 Satz (*Hauptideal*)

Ist $\mathbf{R}$ ein kommutativer Ring und $d \in \mathbf{R}$ beliebig, dann ist

1. $\mathbf{R}d = \{a \cdot d \mid a \in R\} \trianglelefteq \mathbf{R}$ ein Ideal* und
2. $\mathbf{R}d = \mathbf{R} \Leftrightarrow d$ invertierbar in $(\mathbf{R}, \cdot)$, d. h. es gibt ein d' mit $d \cdot d' = 1$

3.38 Beispiel (vgl. Beispiel 3.29)

Sei $\mathbf{R} = (\mathbb{Z}, +, \cdot)$ und $m \in \mathbb{N}, \quad \sim = \sim_m$. Dann ist $m\mathbb{Z} \in \mathbb{Z}$ und $1\mathbb{Z} = \mathbb{Z}$

Konvention: In einem kommutativen Ring schreibt man $\underbrace{a + a + \ldots + a}_{k-\text{mal}} = k \cdot a$

3.39 Beispiel

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

Beweis (indirekt)

Annahme: $z = 7 + n \cdot 9 = a^2 + b^2 + c^2$ für $a, b, c \in \mathbf{Z}$

*$\mathbf{R}d$ heißt das von d erzeugte Hauptideal

Betrachte $\varphi : \mathbb{Z} \to \mathbb{Z}_8, \quad z \to [z]_8$
$\Rightarrow \varphi(z) = \varphi(a^2) + \varphi(b^2) + \varphi(c^2) = \varphi(a)^2 + \varphi(b)^2 + \varphi(c)^2 \stackrel{!}{=} [7]_8$, wobei $\varphi(a), \varphi(b), \varphi(c) \in \mathbb{Z}_8$

In $\mathbb{Z}_8$:

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

Also sind Quadrate in $\mathbb{Z}_8$ $0, 1, 4$ und die Summen von drei Quadraten in $\mathbb{Z}_8$ sind nicht gleich 7
$\Rightarrow$ Behauptung

3.4 Größte gemeinsame Teiler

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

z. B. 2 3 5 7 11 13 17 19 23 29 31 usw.

Ist $m \in \mathbb{N}$ keine Primzahl und $m > 1$, so ist $m = p \cdot q$ mit $1 < p, q < m$, dann ist $[p]_m \cdot [p]_m = [p \cdot q]_m = [m]_m = [0]_m = 0$ in $\mathbb{Z}_m$, aber $[p]_m \neq 0$ und $[q]_m \neq 0$, weil $1 < p \cdot q < m$.

3.40 Definition (*Nullteiler, Integritätsbereich*)

Sei $\mathbf{R} = (\mathbf{R}, +, \cdot)$ ein kommutativer Ring. Sind $a \neq 0$ und $b \neq 0$, aber $a \cdot b = 0$, so heißen a und b *Nullteiler.*

$\mathbf{R}$ heißt *Integritätsbereich*, falls $\mathbf{R}$ keine Nullteiler enthält (d. h. $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$)

3.41 Beispiel

1. $\mathbb{Z}$ ist ein Integritätsbereich
2. $\mathbb{Z}[x]$ ist ein Integritätsbereich
3. Sei $\mathbf{K}$ ein Körper. Dann sind $\mathbf{K}[x]$ und $\mathbf{K}\big[[x]\big]$ Integritätsbereiche
4. $\mathbb{Z}_4$ ist kein Integritätsbereich, denn: $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4 = 0$ in $\mathbb{Z}_4$

   $\mathbb{Z}_m$ ist kein Integritätsbereich, wenn m keine Primzahl ist

3.42 Definition (*größter gemeinsamer Teiler*)

Sei $\mathbf{R}$ ein Integritätsbereich

1. $a \mid b \Leftrightarrow \exists c \in \mathbf{R} : b = a \cdot c$
   $a \nmid b \Leftrightarrow \nexists c \in \mathbf{R} : b = a \cdot c$

2. $d \in \mathbf{R}$ heißt ein *größter gemeinsamer Teiler* von $a, b \in \mathbf{R}$ (in Zeichen: $d \in \mathrm{ggT}(a, b)$), wenn
   - $d \mid a$ und $d \mid b$
   - $(c \mid a$ und $c \mid b) \Rightarrow c \mid d$

3.43 Bemerkung (*Einheit*)

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

$\mathbf{R}^* = \{u \in \mathbf{R} \mid \exists u^{-1} \in \mathbf{R}$ mit $u \cdot u^{-1} = 1\}$

1. In $\mathbb{Z}$ sind nur -1 und 1 Einheiten z. B. $\mathrm{ggT}(4, 10) = \{-2, 2\}$

2. Ist $u \in \mathbf{R}$ eine Einheit in $\mathbf{R}$, so gilt $u \mid a$ für alle $a \in \mathbf{R}$, denn $a = u(u^{-1}a)$
3. Ist $d \in \mathrm{ggT}(a,b)$ in $\mathbf{R}$ und $u \in \mathbf{R}^* \Rightarrow u \cdot d \in \mathrm{ggT}(a,b)$
   Umgekehrt kann man zeigen: $d, d' \in \mathrm{ggT}(a,b) \Rightarrow d' = u \cdot d$ für ein $u \in \mathbf{R}^*$
4. Nicht in jedem Integritätsbereich gilt $\mathrm{ggT}(a,b) = \{1\}$

3.5 Eindeutige Primfaktorzerlegung

3.44 Definition (*irreduzibeler Integritätsbereich*)

Sei $\mathbf{R}$ ein Integritätsbereich. $p \in \mathbf{R}$ mit $p \neq 0$ und $p \notin \mathbf{R}^*$ heißt *irreduzibel*, wenn

$$p = a \cdot b \Rightarrow a \in \mathbf{R}^* \text{ oder } b \in \mathbf{R}^*$$

3.45 Beispiel

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

3.46 Beispiel

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

a) $\mathbf{I}$ ist ein Integritätsbereich

b) $\mathbf{I}^* = \{-1, 1\}$

c) $|\alpha|^2 = 4 \Rightarrow \alpha$ ist irreduzibel

d) $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ (2 verschiedene Primfaktorzerlegungen von 4 in $\mathbf{I}$

Frage: Welche Integritätsbereiche $\mathbf{R}$ haben die Eigenschaft, daß jedes $a \in \mathbf{R} \setminus (\{0\} \cup \mathbf{R}^*)$ eine eindeutige Primfaktorzerlegung hat?

3.47 Definition (*eindeutige (Primfaktor-)Zerlegung*)

Sei $\mathbf{R}$ ein Integritätsbereich. $a \in \mathbf{R}$ hat eine *eindeutige (Primfaktor-)Zerlegung*, wenn

$$\left.\begin{array}{ll} 1)\ a = p_1, \ldots, p_r & p_i \text{ irreduzibel} \\ 2)\ a = q_1, \ldots, q_s & q_i \text{ irreduzibel} \end{array}\right\} \Rightarrow \begin{array}{l} r = s \text{ und mit passender Sortierung ist} \\ q_i = u_i p_i \text{ mit } u_i \in \mathbf{R}^* \text{ für } i = 1, \ldots, s \end{array}$$

3.48 Bemerkung

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

$0 = a_1 \cdot \ldots \cdot a_\alpha \Rightarrow \exists a_i = 0$, aber 0 ist nicht irreduzibel
$u = a_1 \cdot \ldots \cdot a_\beta \Rightarrow 1 = a_1(\underbrace{u^{-1} \cdot a_2 \cdot \ldots \cdot a_\beta}_{a^{-1}})$, aber Einheit ist nicht irreduzibel

3.49 Definition (*Hauptidealring*)

Ein Integritätsbereich $\mathbf{R}$ heißt *Hauptidealring*, wenn jedes Ideal $\mathbf{I}$ von $\mathbf{R}$ ein Hauptideal ist, d.h. $\exists d \in \mathbf{R}$ mit $\mathbf{I} = \mathbf{R} \cdot d$

3.50 Satz

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

3.51 Definition (*Euklidscher Ring*)

Ein Integritätsbereich $\mathbf{R}$ heißt ein *Euklidscher Ring*, wenn

1. $\exists \delta : \mathbf{R} \setminus \{0\} \to \mathbb{N}_0$
2. Zu $a, b \in \mathbf{R}$ mit $b \neq 0$ existiert $q, r \in \mathbf{R}$, so daß $a = q \cdot b + r$ mit $\delta(r) < \delta(b)$

Ein Euklidscher Ring $(\mathbf{R}, \delta)$ heißt *Norm-Euklidscher Ring*, wenn

$$\delta : \mathbf{R} \to \mathbb{N}_0 \text{ mit } \begin{cases} \delta(a) = 0 \Leftrightarrow a = 0 \\ \delta(a \cdot b) = \delta(a) \cdot \delta(b) \end{cases}$$

3.52 Beispiel

1. $(\mathbb{Z}, |\cdot|)$ ist ein (Norm-)Euklidscher Ring, wobei $|a| = \begin{cases} a & \text{falls } a \geq 0 \\ -a & \text{falls } a < 0 \end{cases}$
2. Sei $\mathbf{K}$ ein Körper. $(\mathbf{R} = \mathbf{K}[x], \text{grad})$ ist ein Euklidscher Ring
3. $\mathbf{R} = (\mathbf{K}[x], \delta)$ mit $\delta(f) = \begin{cases} 2^{\text{grad}(f)} & \text{falls } f \neq 0 \\ 0 & \text{falls } f = 0 \end{cases}$ ist ein Norm-Euklidscher Ring

3.53 Satz

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

- **Euklidscher Ring $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$ (Primzahlen)**

3.54 Folgerung (*eindeutige Primfaktorzerlegung*)

In $\mathbb{Z}$ hat jedes $a \in \mathbb{Z} \setminus \{0\}$ eine *eindeutige Primfaktorzerlegung* in der Form $a = u \cdot p_1 \cdot \ldots \cdot p_k$ mit p_i Primzahl und $u \in \mathbb{Z}^* = \{-1, 1\}$

Beweis

Beispiel 3.52 1.
Satz 3.53

3.55 Bemerkung (*Fundamentalsatz der Arithmetik*)

Aus Folgerung 3.54 folgt der „*Fundamentalsatz der Arithmetik*“.

Jede Zahl $n \in \mathbb{N}$ mit $n \geq 2$ läßt sich eindeutig als Produkt von Primzahlen darstellen. $n = p_1^{t_1} \cdot \ldots \cdot p_k^{t_k}$, wobei $p_1 < \ldots < p_k$ Primzahlen sind und $t_1, \ldots, t_k \in \mathbb{N}$

3.56 Satz

Es gibt unendlich viele Primzahlen.

Beweis (indirekt)

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

Setze: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$ $(\star)$

$\Longrightarrow$ $n$ist keine Primzahl

$\overset{3.55}{\Longrightarrow}$ $n = p_{n_1}^{t_1} \cdot p_{n_2}^{t_2} \cdot \ldots \cdot p_{n_k}^{t_k}$ mit $p_{n_1} < \ldots < p_{n_k}$ Primzahlen und $t_i \in \mathbb{N}$ $(\star\star)$

$\left.\begin{array}{l} \overset{(\star)}{\Longrightarrow} \; p_{n_1} \mid n-1 \\ \overset{(\star\star)}{\Longrightarrow} \; p_{n_1} \mid n \end{array}\right\}$ unmöglich

3.57 Satz (*Primzahlsatz*)

Für alle $n \in \mathbb{N}$ ist die Anzahl der Primzahlen $\pi(n) = (1 + o(1)) \cdot \frac{n}{\ln(n)} \leq n$

3.58 Bemerkung (*Wie findet man Primzahlen?*)

1. **Finde alle Primzahlen kleiner** n

   z. B. $n = 36$ $\pi(36) = 11$

~~1~~	[2]	[3]	~~4~~	[5]	~~6~~	[7]	~~8~~	~~9~~
~~10~~	[11]	~~12~~	[13]	~~14~~	~~15~~	~~16~~	[17]	~~18~~
[19]	~~20~~	~~21~~	~~22~~	[23]	~~24~~	~~25~~	~~26~~	~~27~~
~~28~~	[29]	~~30~~	[31]	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~

   Man schreibe alle Zahlen von 2 bis n auf und wende den folgenden Algorithmus an:

   `FOR` i=2 `TO` $\sqrt{n}$ `DO`
   Falls i nicht gestrichen, streiche alle Vielfachen von i

   Die am Ende übrig gebliebenen ungestrichenen Zahlen sind genau die Primzahlen kleiner n.

2. **Finden großer Primzahlen**

   randomisierte Verfahren der derzeit effizientesten Primzahlentester (vgl. *Stochastik*)

• • Der Satz von Fermat

3.59 Satz („*kleiner Fermat*“)

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

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

3.60 Definition (*Eulersche φ-Funktion*)

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

3.61 Lemma

Ist $n = p_1^{t_1} \cdot \ldots \cdot p_k^{t_k}$ mit $p_1 < p_2 < \ldots < p_k$ Primzahlen, so gilt

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

3.62 Satz (*Euler*)

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

Bemerkung: Satz 3.62 $\overset{n \text{ Primzahl}}{\underset{\varphi(n)=n-1}{\Longrightarrow}}$ Satz 3.59

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

z. B. $? = \mathrm{ggT}(729, 153)$

- Euklidscher Algorithmus (vgl. Übung 11)
- Primfaktorzerlegung

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

- Division mit Rest

$$\begin{array}{rcrcrcl} 729 & = & 4 & \cdot & 153 & + & 117 \\ 153 & = & 1 & \cdot & 117 & + & 36 \\ 117 & = & 3 & \cdot & 36 & + & 9 \\ 36 & = & 4 & \cdot & 9 & + & 0 \end{array}$$

$\Rightarrow \mathrm{ggT}(729, 153) = 9$

3.63 Lemma

Sind $m, n \in \mathbb{N}$ mit $m \leq n$ und $m \nmid n$, so gilt $\boxed{\mathrm{ggT}(m, n) = \mathrm{ggT}(n \bmod m, m)}$

3.64 Satz (*Euklidscher Algorithmus*)

Seien $a_0, a_1 \in \mathbb{N}$ mit $a_0 \geq a_1$. Man bestimmt sukzessive $q_i, a_i \in \mathbb{N}$ wie folgt

$$\begin{array}{rcrcrcll} a_0 & = & q_1 & \cdot & a_1 & + & a_2 & \text{mit } 0 < a_2 < a_1 \\ a_1 & = & q_2 & \cdot & a_2 & + & a_3 & \text{mit } 0 < a_3 < a_2 \\ \vdots & = & \vdots & \cdot & \vdots & + & \vdots & \\ a_{k-2} & = & q_{k-1} & \cdot & a_{k-1} & + & a_k & \text{mit } 0 < a_k < a_{k-1} \\ a_{k-1} & = & q_k & \cdot & a_k & + & 0 & \end{array}$$

$\Rightarrow \mathrm{ggT}(a_0, a_1) = a_k$

Euklidscher Ring $\mathbf{K}[x]$

3.65 Definition (*normiertes Polynom*)

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

3.66 Folgerung

Ist $\mathbf{K}$ ein Körper, so hat jedes Polynom $f \in \mathbf{K}[x] \setminus \{0\}$ eine eindeutige Zerlegung (bis auf die Reihenfolge der Faktoren) in der Form $f = u \cdot f_1 f_2 \ldots f_r$ mit $u \in \mathbf{K}^*$ und f_i irreduzibel und normiert.

Beweis

Beispiel 3.52 (2) und Satz 3.53

3.67 Satz

Es sei $(\mathbf{R}, \delta)$ ein euklidscher Ring mit $0 \neq f \in \mathbf{R}$, so ist $\mathbf{R}/_{f\mathbf{R}} = \{[g]_t \mid g \in \mathbf{R}, \delta(g) < \delta(f)\} \cup \{0\}$, wobei $[g]_t = g + f\mathbf{R} = \{g + fz \mid z \in \mathbf{R}\}$. Es ist $\mathbf{R}/_{f\mathbf{R}}$ Körper $\Leftrightarrow$ f ist irreduzibel.

Beweis

Da $(\mathbf{R}, \delta)$ ein Euklidscher Ring ist und $f \neq 0$, gibt es zu einem beliebigen $q \in \mathbf{R}$ stets $q, r \in \mathbf{R}$ mit $g = q \cdot f + r$ mit $r = 0$ oder $\delta(r) < \delta(f) \Rightarrow g - r = q \cdot f \in \mathbf{R}$, also $[g]_f = [r]_f$.
Nach der Definition ist $\mathbf{R}/_{f\mathbf{R}} = \{[g]_f \mid g \in \mathbf{R}\} = \{[g]_f \mid g \in \mathbf{R}, \delta(g) < \delta(f)\} \cup \{0\}$

Nun zeigen wir: $\mathbf{R}/_{f\mathbf{R}}$ ist ein Körper $\Leftrightarrow$ f irreduzibel

„$\Rightarrow$“: (Ist f irreduzibel, so ist $\mathbf{R}/_{f\mathbf{R}}$ ein Körper)

Sei $0 \neq [g]_f \in \mathbf{R}/_{f\mathbf{R}}$.

Zu zeigen: $[g]_f^{-1}$ existiert

f ist irreduzibel $\Rightarrow f \nmid g \Rightarrow 1 \in \mathrm{ggT}(f, g)$

$$\overset{\text{Ü11/A2}}{\Rightarrow} \quad \exists y, z \in \mathbf{R}: \quad 1 = y \cdot f + z \cdot g$$
$$\Rightarrow \quad \underbrace{[1]_f}_{=1} = \underbrace{[y \cdot f]_f}_{=0} + [z]_f \cdot [g]_f$$
$$\overset{1=[z]_f \cdot [g]_f}{\Rightarrow} \quad [g]_f \text{ ist invertierbar mit } [g]_f^{-1} = [z]_f, \text{ also ist } \mathbf{R}/_{f\mathbf{R}} \text{ ein Körper}$$

„$\Leftarrow$“: (Ist $\mathbf{R}/_{f\mathbf{R}}$ ein Körper, so ist f irreduzibel)

Wir zeigen: Sei f nicht irreduzibel, dann ist $\mathbf{R}/_{f\mathbf{R}}$ kein Körper

f ist nicht irreduzibel $\Rightarrow \exists a, b \in \mathbf{R} \setminus \mathbf{R}^*: f = a \cdot b, \ \underbrace{[f]_f}_{=0} = [a \cdot b]_f = [a]_f \cdot [b]_f$

wäre $[a]_f = 0$, so wäre $f \mid a$, d. h. $\exists a_1 \in \mathbf{R}$ mit $a = f \cdot a_1$
$\Rightarrow f = a \cdot b = f \cdot \underbrace{a_1 \cdot b}_{=1} \Rightarrow a_1 \cdot b = 1 \Rightarrow b \in \mathbf{R}^* \Rightarrow$ Widerspruch!

Also ist $[a]_f \neq 0$. Analog kann man zeigen: $[b]_f \neq 0$.

Insgesamt ist $\mathbf{R}/_{f\mathbf{R}}$ kein Integritätsbereich $\Rightarrow$ $\mathbf{R}/_{f\mathbf{R}}$ ist kein Körper

Bemerkung: Ist $f \in \mathbf{R}^*$, so ist $\mathbf{R}/_{f\mathbf{R}} = \mathbf{R}/_{\mathbf{R}} = \{0\}$ kein Körper

3.68 Beispiel

Sei $\mathbf{K} = \mathbb{Z}_2 = \{0, 1\}$. Dann ist $\mathbf{K}$ ein Körper. $(\mathbb{Z}_2[x], \delta)$ mit $\delta(g) = \mathrm{grad}(g)$ für $g \in \mathbf{Z}_2[x]$ ist ein euklidscher 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 können.

$$
\begin{array}{lcll}
 & [a_0 + a_1 x + a_2 x^2]_f & \rightsquigarrow & a_0 a_1 a_2 \\
 & & & \\
\alpha & = & [x]_f & \rightsquigarrow 010 \\
\alpha^2 & = & [x^2]_f & \rightsquigarrow 001 \\
\alpha^3 & = & [x^3]_f = [x+1]_f & \rightsquigarrow 110, \text{ denn } x^3 = x + 1 + \underbrace{(x^3 + x + 1)}_{:=f} \cdot 1 \\
\alpha^4 & = & \alpha^3 \alpha = [x^2 + x]_f & \rightsquigarrow 011 \\
\alpha^5 & = & \alpha^4 \alpha = [x^3 + x^2]_f = [x^2 + x + 1]_f & \rightsquigarrow 111, \text{ denn } x^3 + x^4 = \underbrace{(x^2 + x + 1)}_{:=g} + \underbrace{(x^3 + x + 1)}_{:=f} \cdot 1 \\
\alpha^6 & = & \alpha^5 \alpha = [x^3 + x^2 + x]_f = [x^2 + x + 1]_f & \rightsquigarrow 101, \text{ denn } x^3 + x^2 + x = x^2 + 1 + \underbrace{(x^3 + x + 1)}_{:=f} \\
\alpha^7 & = & \alpha^6 \alpha = [x^3 + x]_f = [1]_f & \rightsquigarrow 100 \\
\alpha^8 & = & \alpha &
\end{array}
$$

3.69 Bemerkung (*diskreter Logarithmus*)

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

3.6 Endliche Körper

- unendliche Körper
  - $(\mathbb{Q}, +, \cdot)$
  - $(\mathbb{R}, +, \cdot)$
  - $(\mathbb{C}, +, \cdot)$
- 1. $(\mathbb{Z}_2, +_2, \cdot_2)$, wobei $+_n : a +_n b := (a + b) \bmod n$ und $\cdot_n : a \cdot_n b := (a \cdot b) \bmod n$
     $|\mathbb{Z}_2| = 2$
  2. $(\mathbb{Z}_2[x]/_{f\mathbb{Z}_2[x]}, +_f, \cdot_f)$ mit $f = x^3 + x + 1$ (vgl. Beispiel 3.68),
     wobei $+_f : g +_f g := (g + h) \bmod f$ und $\cdot_f : g \cdot_f h := (g \cdot h) \bmod f$

     $$
     \begin{array}{lcl}
     |\mathbb{Z}_2[x]/_{(x^3+x+1)\mathbb{Z}_2[x]}| & = & |\{[a_0 + a_1 x + a_2 x^2]_f \mid a_0, a_1, a_2 \in \mathbb{Z}_2\}| \\
     & = & |\{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}| \\
     & = & 2^3
     \end{array}
     $$

Wir werden uns in diesem Abschnitt mit der Konstruktion von endlichen Körpern beschäftigen.

Aus Satz 3.67 erhalten wir sofort:

3.70 Folgerung

1. $(\mathbb{Z}_n, +_n, \cdot_n)$ ist ein Körper $\Leftrightarrow$ n ist Primzahl
2. Sei $\mathbf{K}$ ein Körper und $f \in \mathbf{K}[x]$. Dann gilt:

   $(\mathbf{K}[x]/_{f\mathbf{K}[x]}, +_f, \cdot_f)$ ist ein Körper $\Leftrightarrow$ f ist irreduzibel über $\mathbf{K}[x]$*

Bemerkung

Bis auf Isomorphie kann man einen endlichen Körper mit p^k Elementen konstruieren, wobei p eine Primzahl ist und $k \in \mathbb{N}$. Ist diese Konstruktion eindeutig?

*d. h. $f = g \cdot h \Rightarrow \text{grad}(g) = 0$ oder $\text{grad}(h) = 0$

3.71 Satz

1. Für ein $n \in \mathbb{N}$ gibt es einen Körper mit n Elementen $\Leftrightarrow n = p^k$ für eine Primzahl p und ein $k \in \mathbf{N}$
2. Sind $\mathbf{K}_1$ und $\mathbf{K}_1$ zwei Körper mit $|\mathbf{K}_1| = |\mathbf{K}_2|$, so gilt $\mathbf{K}_1 \cong \mathbf{K}_2$.
   (*Galoiskörper* mit p^k Elementen, $\mathrm{GF}(p^k)$ (engl. *Galoisfield*) der (bis auf Isomorphie) eindeutige Körper mit p^k Elementen)

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

3.72 Satz

In jedem endlichen Körper $\mathbf{K}$ ist die multiplikative Gruppe $\mathbf{K}^*$ zyklisch, d. h. es gibt ein Element $a \in \mathbf{K}^*$ mit $\mathbf{K}^* =< a >= \{1, a, a^2, \ldots, a^{|\mathbf{K}|-2}\}$.

Z. B. $\left(\mathbb{Z}_2[x]/_{(x^3+x+1)\mathbb{Z}_2[x]}\right)^* =< [x]_f >$ $\quad < [x]_f >$ heißt *Generator*

Effiziente Implementierung

Sei p eine Primzahl

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

$k > 1:$ $\mathrm{GF}(p^k) \cong \underbrace{\mathbb{Z}_p[x]/_{f\mathbb{Z}_p[x]}}$, f irreduzibel mit $\mathrm{grad}(f) = k$

$$= \left\{ \sum_{i=0}^{k-1} a_i x^i \,|\, a_i \in \mathbb{Z}_p \right\} \sim a_0 a_1 \ldots a_{k-1} \quad a_i \in \mathbb{Z}_p \quad i = 0, 1, \ldots, k-1$$

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

- Addition von zwei Polynomen

$$\begin{array}{ccc} a(x) & \rightsquigarrow & a_0 a_1 \ldots a_{k-1} \\ + & & + \\ b(x) & \rightsquigarrow & b_0 b_1 \ldots b_{k-1} \\ \| & & \| \\ c(x) & \rightsquigarrow & c_0 c_1 \ldots c_{k-1} \end{array} \quad \text{mit } c_i = (a_i + b_i) \bmod p$$

- Multiplikation von zwei Polynomen
  1. $c(x) = a(x) \cdot b(x) = \ldots$ ausrechnen, dann den Rest modulo f bestimmen – relativ aufwendig
  2. $a(x) \cdot \sum_{i=0}^{k-1} b_i x^i = a(x) \cdot b_0 + x \cdot (a(x) \cdot b_1 + x \cdot (\ldots + x \cdot (a(x) \cdot b_{k-2} + x \cdot a(x) \cdot b_{k-1})))$

3.73 Beispiel (*Fortsetzung von Beispiel 3.68*)

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

$\mathbb{Z}_2[x]/_{(x^3+x+1)\mathbb{Z}_2[x]}$	Kurzdarstellung
0	000
1	100
x	010
$1+x$	110
x^2	001
$1+x^2$	101
$x+x^2$	011
$1+x+x^2$	111

Seien nun $a(x) = x + x^2$ und $b(x) = 1 + x + x^2$
Dann gilt: $a(x) \cdot b(x) = a(x) \cdot b_0 + x(a(x) \cdot b_1 + x \cdot a(x) \cdot b_2)$

Aufgabe	Realisierung	Ergebnis
Berechne $a(x) \cdot b_2$	$b_2 = 1$, also $a(x) \cdot b_2 = a(x)$	0110
Multipliziere mit x	Shift nach rechts	0011
Berechne Rest mod f	XOR mit $f = 1101$	1110
Addiere $a(x) \cdot b_1$	$b_1 = 1$, also XOR mit $a = 0110$	1000
Multipliziere mit x	Shift nach rechts	0100
Berechne Rest mod f	letztes Bit $= 0$	0100
Addiere $a(x) \cdot b_0$	$b_0 = 1$, also XOR mit $a = 0110$	0010

Aus der letzten Zeile können wir das Ergebnis ablesen: $a(x) \cdot_f b(x) = x^2$

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

c) Nach Satz 3.72 gibt es für jedes Polynom $t(x) \in \mathbb{Z}_p[x]/_{t\mathbb{Z}_p[x]}$ ein $l_t \in \{0, 1, \ldots, p^k - 2\}$ mit $t(x) = \alpha^{l_t}$.

Im Beispiel 3.68 gilt $\alpha = [x]_f \quad a(x) = x + x^2 = \alpha^4 \quad b(x) = 1 + x + x^2 = \alpha^5$

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

Index