Diskrete Strukturen
Sommersemester 2001
Prof. Dr. H. Pahlings

geLaTeXt von

Stefan Schiffer (dr.stf@web.de),
Claus Richterich (claus@richterich.net),
Kay-Uwe Hüll (huekay@web.de)

31. August 2001

Vorwort

Dieses Dokument wurde erstellt mit LaTeX2 ϵ und enthält die Vorlesungsinhalte der Vorlesung "Diskrete Strukturen" bei Professor Dr. H. Pahlings im SS 2001 an der RWTH-Aachen. Der Text spiegelt die von den Autoren aufgezeichneten Inhalte wieder. Wir können daher die Vollständigkeit nicht gewährleisten. Diese Mitschrift kann und soll in keiner Weise den Besuch der Vorlesung und der Übungen ersetzen sondern kann diesen allenfalls ergänzen. Sollten irgendwelche Fehler oder Unstimmigkeiten auftauchen, oder sollten Inhalte fehlen, bitte ich um Benachrichtigung unter der angegebenen Adresse. Das Dokument darf frei weitergegeben und kopiert werden, dies bezieht sich sowohl auf die PDF-Datei als auch auf Ausdrucke. Veränderungen an Inhalten sind nur nach ausdrücklicher Genehmigung der Autoren erlaubt. Eine kommerzielle Verwertung ist untersagt. Wir können leider für Beschädigungen o.ä., die durch diese Daten - auch indirekt - hervorgerufen wurden, keine Haftung übernehmen. Die aktuelle - weitestgehend fehlerbereinigte - Version dieses Dokuments kann von meiner Homepage runtergeladen werden.
Für Kritik, Verbesserungsvorschläge und insbesondere Korrekturen sind die Autoren jederzeit offen.
Aus gegebenem Anlass möchten wir hier allen (und es waren leider nur sehr wenige), die uns Korrekturvorschläge und Anmerkungen geschickt haben, ganz herzlich danken.

Vorabversion, Stand: 31. August 2001

Stefan Schiffer,
(dr.stf@web.de)

Claus Richterich,
(claus@richterich.net)

Kay-Uwe Hüll,
(huekay@web.de)

Homepage: http://www.drstf.de/

Zitat der Woche:
Die Mehrheit bringt der Mathematik Gefühle entgegen, wie sie nach Aristoteles durch die Tragödie geweckt werden sollen, nämlich Mitleid und Furcht. Mitleid mit denen, die sich mit der Mathematik plagen müssen, und Furcht: dass man selbst einmal in diese gefährliche Lage geraten könne.
(Paul Epstein (1883 - 1966))

Inhaltsverzeichnis

Kapitel 1

Abzählungen, Rekursionen, erzeugende Funktionen

§ 1 Elementare Zählprinzipien

$$\begin{aligned} M &= \text{endliche Menge} \\ |M| &= \text{Anzahl der Elemente von } M \end{aligned}$$

(in dieser Vorlesung werden fast nur endliche Mengen behandelt)
Alle endlichen sowie abzählbaren Mengen nennt man diskret (z.B. $\mathbb{N}$, $\mathbb{Z}$). Mengen die nicht diskret sind, nennt man kontinuierlich.

$$\begin{aligned} |A| = n \in \mathbb{N} = \{1, 2, 3, \ldots, n\} &\Leftrightarrow \text{Es gibt eine Bijektion } \alpha : A \longrightarrow \{1, 2, \ldots, n\} \\ |A| = 0 &\Leftrightarrow A = \emptyset \end{aligned}$$

Lemma 1

a.) $|A| = |B| \Leftrightarrow$ Es gibt Bijektion $\alpha : A \longrightarrow B$

b.) $|A \dot\cup B| = |A| + |B|$
($\dot\cup$ ist die **disjunkte Vereinigung**, d.h. es gilt $A \cap B = \emptyset$)

c.) $|A \times B| = |A| \cdot |B|$
$A \times B = \{(a, b) \mid a \in A, b \in B\}$

Folgerung 1

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

$$|B^A| = |B|^{|A|}$$

Beweis
Sei $|A| = n$, $A = \{a_1, a_2, \ldots, a_n\}$, $|B| = m$

$$\begin{array}{rcl} B^A & \longrightarrow & \underbrace{B \times B \times \ldots \times B}_{\text{n-mal}} \\ f & \longmapsto & (f(a_1), f(a_2), \ldots, f(a_n)) \end{array}$$

ist Bijektion

$$|B^A| = |B \times B \times \ldots \times B| \underset{\text{Lemma 1 c)}}{=} |B|^n$$

■

Definition 1 (Permutation, symmetrische Gruppe)

$$f : A \longrightarrow A$$

heißt **Permutation** von A, wenn f bijektiv ist.

$$\begin{array}{rcl} S_n & = & \{\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} \mid \sigma \text{ bijektiv } \} \\ & = & \mathrm{Sym}\{1, \ldots, n\} \\ & = & \textbf{symmetrische Gruppe} \text{ vom Grad n} \end{array}$$

Lemma 2

$$|S_n| = n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$$

gibt die Anzahl der Möglichkeiten an, die Elemente einer n**-Menge** A, d.h eine Menge A mit $|A| = n$, anzuordnen.
siehe Lineare Algebra I

$$\begin{array}{rcl} \sigma & \longmapsto & (\sigma(1), \sigma(2), \ldots, \sigma(n)) \\ S_n & \longrightarrow & \{(i_1, i_2, \ldots, i_n) \mid i_j \in \underline{n}, i_j \neq i_k \text{ für } j \neq k\} \\ & & \text{(Bilder müssen verschieden sein)} \\ & & = \{\ldots \mid \{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}\} \end{array}$$

$$|S_n| = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$$

Satz 1
Die Anzahl der Teilmengen einer n-Menge (Menge mit n Elementen) A ist 2^n.

$$|A| = n, \quad |\mathcal{P}(A)| = 2^n$$

dabei ist $\mathcal{P}(A)$ die Menge aller Teilmengen von A

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

genannt **Potenzmenge** von A.

Beispiel 1

$$A = \{1, 2\}, \quad \mathcal{P}(A) = \{\{1, 2\}, \{1\}, \{2\}, \emptyset\}$$

Beweis (1. Beweis von Satz 1)

$$\begin{aligned} \mathcal{P}(A) &\longrightarrow \{0,1\}^A \qquad (= \mathrm{Abb}(A, \{0,1\})) \\ B &\longrightarrow \chi_B \textbf{ charakteristische Funktion} \text{ von B definiert durch} \end{aligned}$$

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

ist Bijektion

$$B = \{x \in A \mid \chi_B(x) = 1\}$$
$$|\mathcal{P}(A)| = \left|\{0,1\}^A\right| = 2^{|A|} (= 2^n)$$

■

Definition 2

$$\begin{aligned} \mathcal{P}_k(A) &= \binom{A}{k} \\ &= \text{ Menge aller } k\text{-Teilmengen von } A \\ &= \{B \subseteq A \mid |B| = k\} \end{aligned}$$

Bemerkung

$$\begin{aligned} \mathcal{P}(A) &= \dot{\bigcup}_{k=0}^{n} \mathcal{P}_k(A) \\ |A| &= n \end{aligned}$$

Also nach Lemma 1 ist

$$|\mathcal{P}(A)| = \sum_{k=0}^{n} |\mathcal{P}_k(A)|$$

Lemma 3
Für $|A| = n$ gilt:

$$\begin{aligned} |\mathcal{P}_k(A)| &= \left|\binom{A}{k}\right| = \binom{n}{k} \qquad (= \textbf{Binomialkoeffizient}) \\ &= \frac{n(n-1)(n-2)\ldots(n-k+1)}{k!} \\ (&= \frac{n!}{k!(n-k)!}) \end{aligned}$$

Beweis

$$B = \{b_1, b_2, \ldots, b_k\}, \quad |B| = k, \quad b_i \neq b_j \text{ für } i \neq j, b_i \in A$$
$$|\{(b_1, b_2, \ldots, b_k) \mid b_i \neq b_j \text{ für } i \neq j, b_i \in A\}| = n(n-1)(n-2)\ldots(n-k+1)$$

Es gibt $k!$ Anordnungen von $\{b_1, b_2, \ldots, b_k\}$.

■

Beweis (2. Beweis von Satz 1)
Sei $|A| = n$, dann

$$|\mathcal{P}(A)| = \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n$$

(Zitat:"`Das ist der berühmte Satz von Binom ;-)`")

■

Satz 2

a.) **Pascal'sches Dreieck**

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \quad \text{für } k \geq 1, n \geq k$$

b.) **van-der-Mond'sche Identität**

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

Beweis

a.) Sei A Menge mit $|A| = n \geq 1$ mit

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

Sei $b \in A$, dann

$$\begin{aligned}\binom{A}{k} &= \{X \subseteq A \mid |X| = k, b \notin X\} \dot\cup \underbrace{\{X \subseteq A \mid |X| = k, b \in X\}}_{M} \\ &= \binom{A \setminus \{b\}}{k} \dot\cup M\end{aligned}$$

$$\begin{aligned} M &\longrightarrow \binom{A \setminus \{b\}}{k-1} \\ X &\longrightarrow X \setminus \{b\} \qquad \text{ist Bijektion}\end{aligned}$$

$$\left|\binom{A}{k}\right| = \binom{n-1}{k} + \binom{n-1}{k-1}$$

■

b.)

$$|A| = m+n \qquad A = B \dot\cup C \qquad |B| = m \qquad |C| = n$$

$$\binom{A}{k}_l = \{X \subseteq A \mid |X| = k, |X \cap B| = l\}$$

$$l = 0, 1, \ldots, k$$

$$\binom{A}{k} = \dot\bigcup_{l=0}^{k} \binom{A}{k}_l$$

$$\binom{m+n}{k} = \left|\binom{A}{k}\right| = \sum_{l=0}^{k} \underbrace{\left|\binom{A}{k}_l\right|}_{\binom{m}{l}\binom{n}{k-l}}$$

■

20.04.MMI

$$|M| = n \in \mathbb{N}_0 = \{0, 1, \ldots\}$$

$$\binom{M}{k} = \begin{cases} \{A \subseteq M \mid |A| = k\} & \text{für } 0 \le k \le n \\ \emptyset & \text{für } k > n, k < 0 \end{cases}$$

$$\begin{aligned} \left|\binom{M}{k}\right| &= \binom{n}{k} \\ &= \frac{n(n-1)\ldots(n-k+1)}{k!} \qquad k \ge 0 \\ &= \frac{n!}{k!(n-k)!} \qquad n \ge k \ge 0 \end{aligned}$$

Folie:

Pascal'sches Dreieck

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

Rekursion: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \qquad (n, k > 0)$

Lemma 4 (Elementare Zählprinzipien)

a.) **Doppeltes Abzählen**
Ist $R \subseteq M \times N$, so ist

$$\begin{aligned} |R| &= \sum_{a \in M} |\{b \in N \mid (a,b) \in R\}| \\ &= \sum_{b \in N} |\{a \in M \mid (a,b) \in R\}| \end{aligned}$$

b.) **Schubfachprinzip** ([en] pigeonhole principle)
Sei $|M| > |N|$. Ist $f : M \to N$, so ist f nicht injektiv, d.h.

$$\exists\, b \in \mathbb{N} \text{ mit } |f^{-1}(b)| = |\{a \in M \mid f(a) = b\}| > 1$$

c.) **Inklusion-Exklusion-Prinzip**
Seien $A_1, \ldots, A_n \subseteq M$.

$$\begin{aligned} \left| \bigcup_{i=1}^{n} A_i \right| &= \sum_{i=1}^{n} |A_i| - \sum_{i_1 < i_2} |A_{i_1} \cap A_{i_2}| + \sum_{i_1 < i_2 < i_3} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \ldots \\ &= \sum_{j=1}^{n} (-1)^{j-1} \sum_{1 \le i_1 < \ldots < i_j \le n} \left| A_{i_1} \cap \ldots \cap A_{i_j} \right| \end{aligned}$$

Beweis (zu c))
Sei $A \subseteq M$

$$\begin{aligned} \chi_A : M &\longrightarrow \{0,1\} \\ x &\longmapsto \begin{cases} 1: & \text{wenn } x \in A \\ 0: & \text{sonst} \end{cases} \end{aligned}$$

$$|A| = \sum_{x \in M} \chi_A(x)$$

$$\chi_{A_1 \cup \ldots \cup A_n}(x) = \sum_{j=1}^{n} (-1)^{j-1} \sum_{1 \le i_1 < \ldots < i_j \le n} \chi_{A_1 \cup \ldots \cup A_n}(x)$$

Daraus folgt die Beh. durch Summation über M: $\sum_{x \in M}$

Ist

a.) $x \notin A_1 \cup \ldots \cup A_n$, so ist linke Seite(*) $= 0$
rechte Seite(*) $= 0$

b.) $x \in A_1 \cup \ldots \cup A_n$, so ist linke Seite (*) $= 1$

x liege in genau $k(\geq 1)$ Teilmengen $A_1, \ldots, A_n$
$x \in A_{j_1} \cap \ldots \cap A_{j_k} \quad j_1 \leq \ldots \leq j_k$
dann ist $\chi_{A_{i_1} \cap \ldots \cap A_{i_j}}(x) = 1$
$\Leftrightarrow \{i_1, \ldots, i_j\} \subseteq \{j_1, \ldots, j_k\}$
Rechte Seite (*) $= \underbrace{\sum_{j=1}^{n} (-1)^{j-1} \binom{k}{j}}_{(1-1)^k} = 1$

■

§ 2 Partitionen

Definition 1
Eine **Partition** P von einer Menge M ist eine Zerlegung von M in eine Vereinigung von disjunkten nichtleeren Teilmengen ("**Blöcke**" genannt). Genauer:

$$P = \{A_1, \ldots, A_k\}$$

heißt Partition von M, wenn

$$M = A_1 \dot\cup \ldots \dot\cup A_k \text{ und } A_i \neq \emptyset \text{ für } i = 1, \ldots, k.$$

$$\text{Part}_k(M) := \{P \mid P \text{ ist Partition von } M, |P| = k\}$$

ist die Menge der k-**Partitionen** der Menge M.

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

heißen **Stirling-Zahlen 2. Art**. Es gilt:

$$S_{0,0} = 1$$

Beispiel 1

$$\begin{aligned} S_{n,0} &= 0 \quad n \geq 1 \\ S_{n,1} &= 1 \quad n \geq 1 \\ S_{n,k} &= 0 \quad \text{für } k > n \\ S_{n,n} &= 1 \\ S_{n,n-1} &= \binom{n}{2} \end{aligned}$$

Satz 1
Es gilt für $1 \leq k \leq n$:

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

25.04.MMI

Sei im Folgenden M eine endliche Menge mit $|M| = n > 0$.

$$\begin{aligned} \text{Part}_k(M) &= \{P = \{A_1 \dots A_n\} \mid \emptyset \neq A \quad A_i \subseteq M \quad M = A_1 \dot\cup \dots \dot\cup A_k\} \\ \text{Part}_1(M) &= \{\{M\}\} \\ \text{Part}_2(\{1,2,3,4\}) &= \{\{\{1\},\{2,3,4\}\},\{\{2\},\{1,3,4\}\},\{\{3\},\{1,2,4\}\},\{\{4\},\{1,2,3\}\}, \\ &\quad \{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\} \\ \text{Part}_2(M) &= \{\{A, M\backslash\{A\}\} \mid A \subset M, \quad A \neq \emptyset, \quad M \neq A\} \\ |\text{Part}_2(M)| &= \underbrace{1/2}_{(*)} \underbrace{(2^n - 2)}_{(**)} = 2^{n-1} - 1 \end{aligned}$$

(*) weil es jedes Element doppelt gibt z.B. $\{\{1,2\},\{3,4\}\} = \{\{3,4\},\{1,2\}\}$
(**) Potenzmenge $-\emptyset - M$

$S_{n,k} = |\text{Part}_k(M)|$ nennt man **Stirling-Zahlen 2. Art**

Beweis (Satz 1)
Sei $a \in M$ und $|M| = n \geq 1$
$\text{Part}_k(M) = X_1 \dot\cup X_2$ wobei

$$\begin{aligned} X_1 &= \{P \in \text{Part}_k(M) \mid \{a\} \notin P\} \\ X_2 &= \{P \in \text{Part}_k(M) \mid \{a\} \in P\} \\ X_2 &= \{P = \{\{a\}, B_1, \dots, B_{k-1}\} \mid \{B_1, \dots, B_{k-1}\} \in \text{Part}_{k-1}(M \setminus \{a\}) \\ |X_2| &= S_{n-1,k-1} \end{aligned}$$

Ist $P \subset X_1$ dann erhält man durch Löschen von a eine Partition $\{B_1, \dots, B_k\}$ von $M \setminus \{a\}$. Umgekehrt erhalten wir zu jeder $\{B_1, \dots, B_k\} \in \text{Part}_k(M \setminus \{a\})$ genau k verschiedene Partitonen aus X_1 nämlich:

$$\{\{\{a\} \dot\cup B_1, B_2, \dots, B_k\}, \dots, \{B_1, B_2, \dots, B_k \dot\cup \{a\}\}\}$$

$$|X_1| = k \cdot S_{n-1,k}$$

■

Bemerkung

a.) $\{\text{Partitionen von } M\} \leftrightarrow \{ \text{ Äquivalenzrelation auf } M\}$

b.) Ist $f : M \to N$ eine surjektive Abbildung

$$\begin{aligned} \text{für } b \in N \quad f^{-1}(b) &= \{a \in M \mid f(a) = b\} \neq \emptyset \\ M &= \dot{\bigcup_{b \in N}} f^{-1}(b) \end{aligned}$$

c.) Ist $f : M \to N$ eine surjektive Abbildung

$$P_f = \{f^{-1}(b) \mid b \in N\} \in \text{Part}_{|N|}(M)r$$

Satz 2

Ist $|M| = m, \quad |N| = n, \quad |\text{Abb}(M, N) = |N^M| = n^m$, so ist
die Anzahl der injektiven Abbildungen $M \longrightarrow N$

$$|\underbrace{\text{Inj}(M, N)}| = n^{\underline{m}} = n \cdot (n-1) \ldots (n-m+1),$$

und die Anzahl der surjektiven Abbildungen $M \longrightarrow N$

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

Beweis

a.) siehe § 1

b.) Sei $M = \{a_1, \ldots, a_m\}$ jede Abbildung $f : M \longrightarrow N$ ist gegeben durch
$f(a_1) = b_1 \ldots f(a_m) = b_m \in N$
f injektiv $\Leftrightarrow b_i \neq b_j$ für $i \neq j$
Für b_1 gibt es n Möglichkeiten $b_1 \in N$
b_2 gibt es $n-1$ Möglichkeiten $b_2 \in N \backslash \{b_1\}$
$\vdots$
b_m gibt es $n-m+1$ Möglichkeiten $b_m \in N \backslash \{b_1 \ldots b_{m-1}\}$

c.) Ist $f : M \to N$ surjektiv
$P_f = \{f^{-1}(b) \mid b \in N\} \in \text{Part}_n(M) = \{A_1, \ldots, A_n\}$
$P_f = P_g \Leftrightarrow g = \sigma \cdot f$ mit $\sigma \in \text{Sym}N$ [Permutation der Bilder]
$|\text{Surj}(M, N)| = S_{m,n} \cdot n!$

■

Beispiel 2
$\mathrm{Surj}(\underbrace{\{1,2,3\}}_{M}, \underbrace{\{1,2\}}_{N})$
$|\mathrm{Surj}(M,N)| = 6 = 2! \cdot S_{3,2}$

Bemerkung

$$\mathrm{Abb}(M,N) = \bigcup_{A \subseteq N} \mathrm{Surj}(M,A)$$

f kann man auffassen als surjektive Abbildung

$$f : M \to \mathrm{Bild}(f) = \{\underbrace{f(a)}_{N} \mid a \in M\} \subseteq N$$

$$\begin{aligned} n^m = |\mathrm{Abb}(M,N)| &= \sum_{A \subseteq N} |\mathrm{Surj}(M,A)| \\ &= \sum_{k=0}^{n} \sum_{A \subseteq \binom{N}{k}} |\mathrm{Surj}(M,A)| \\ &= \sum_{k=0}^{n} \binom{n}{k} \cdot k! \cdot S_{m,k} \\ &= \sum_{k=0}^{n} \frac{n^{\underline{k}}}{k!} \cdot k! \cdot S_{m,k} \end{aligned} \tag{1.1}$$

Satz 3

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

§ 3 Permutationen

$$\begin{aligned} S_n &= \mathrm{Sym}(\underline{n}) = \{\sigma : \{1,\dots,n\} \to \{1,\dots,n\} \mid \sigma \text{ bijektiv}\} \\ S_n &= n! \end{aligned}$$

Jedes $\sigma \in S_n$ kann durch eine Wertetabelle angegeben werden:

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

Bemerkung
$(S_n, \circ)$ ist eine Gruppe. $\sigma_1, \sigma_2 \in S_n$

$$\begin{aligned} \sigma_1 \circ \sigma_2 : \{1 \ldots, n\} &\longrightarrow \{1, \ldots, n\} \\ x &\longmapsto \sigma_1(\sigma_2(x)) \end{aligned}$$

$$\sigma = \sigma \circ \sigma$$

Definition 1
Ein k-**Zyklus** $(i_1, \ldots, i_k) = \sigma \in S_n$ ist eine **Permutation** mit $(i_1, \ldots, i_k) \in \{1, \ldots, n\}^k$

$$\begin{aligned} \sigma \in S_n \text{ mit } \sigma(i_1) &= i_2 \\ \sigma(i_2) &= i_3 \\ &\vdots \\ \sigma(i_{k-1}) &= i_k \\ \sigma(i_k) &= i_1 \end{aligned}$$

und $\sigma(i) = i$ für $i \notin \{i_1, \ldots, i_k\}$

Beispiel 1
σ wie oben. Dann ist $\sigma = (1, 4, 2, 3, 7, 6) \circ (5, 9) \circ (8)$

Bemerkung
Jedes $\sigma \in S_n$ läßt sich als Produkt von Zyklen schreiben.

Beispiel 2
$S_3 = \{\underbrace{(1)(2)(3)}_{\text{id}}, (1)(2,3), (2)(1,3), (3)(1,2), (1,2,3), (1,3,2)\}$

Definition 2
Die **Stirling-Zahlen 1. Art** $s_{n,k}$ geben die Anzahl der Permutationen von $\{1, \ldots, n\}$ an, die genau k (disjunkte) Zyklen haben.

$$\begin{aligned} s_{3,1} &= 2 \\ s_{3,2} &= 3 \\ s_{3,3} &= 1 \end{aligned}$$

27.04.MMI

Definition 3
Ein **(r)-Zyklus** $\zeta = (i_1, \ldots, i_r)$ ist eine Permutation $\zeta \in S_n$ mit „Ziffernmenge“

$$Z(\zeta) = \{i_1, \ldots, i_r\} \text{ mit } |Z(\zeta)| = r \text{ und}$$

$$\begin{aligned} \zeta(i_1) &= i_2 \\ \zeta(i_2) &= i_3 \\ &\vdots \\ \zeta(i_r) &= i_1 \end{aligned}$$

und $\zeta(i) = i$ für $i \notin Z(\zeta)$.

$$\mathrm{Perm}_k(\underline{n}) = \{\sigma \in S_n | \sigma = \zeta_1 \circ \ldots \circ \zeta_k \text{ mit } Z(\zeta_1) \dot\cup \ldots \dot\cup Z(\zeta_k) = \{1, \ldots, n\} = \underline{n}\}$$

Bemerkung

a.) $(i_1 \ldots i_r) = (i_2 \ldots i_r i_1) = \ldots = (i_r i_1 \ldots i_{r-1})$

b.) ζ_1, ζ_2 disjunkt, d.h. $Z(\zeta_1) \cap Z(\zeta_2) = \emptyset \Rightarrow \zeta_1 \circ \zeta_2 = \zeta_2 \circ \zeta_1$
z.B. $(1\,2) \circ (3\,4) = (3\,4) \circ (1\,2)$, aber
$(1\,2) \circ (2\,3) = (1\,2\,3) \neq (23) \circ (1\,2) = (1\,3\,2)$

Definition 4
$s_{n,k} = |\mathrm{Perm}_k(\underline{n})|$ mit $n, k \geq 1$ und $s_{0,0} = 1$ nennt man **Stirling-Zahlen 1. Art**.

Lemma 1

a.) $s_{n,k} = 0$ für $k > n$

b.) $s_{n,n} = 1$ für $n \in \mathbb{N}_0$

c.) $s_{n,1} = (n-1)!$

denn:
zu b) $\mathrm{Perm}_n(\underline{n}) = \{(1) \circ (2) \circ \ldots \circ (n) = \mathrm{id}\}, |\mathrm{Perm}_n(\underline{n})| = 1$
zu c) $\mathrm{Perm}_1(\underline{n}) = \{(n\, i_2 \ldots i_n) \mid \quad |\{i_2, \ldots, i_n\}| = n-1\}, \quad |\mathrm{Perm}_1(\underline{n})| = (n-1)!$

Satz 1
Für $n, k \in \mathbb{N}$ gilt:

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

Beweis
Sei

$$\begin{aligned} X &= \mathrm{Perm}_k(\underline{n}) = X_1 \dot\cup X_2 \\ X_1 &= \{\sigma \in X \mid \sigma(n) = n\} \\ &= \{\sigma = (n) \circ \zeta_1 \circ \ldots \circ \zeta_{n-1} \mid \zeta_1 \circ \ldots \circ \zeta_{k-1} \in \mathrm{Perm}_{k-1}(\underline{n-1})\} \end{aligned}$$

Es ist offensichtlich, dass $|X_1| = s_{n-1,k-1}$

$$X_2 \;=\; \{\sigma \in X \mid \sigma(n) \neq n\}$$

Jedes $\sigma \in X_2$ liefert durch Löschen von n eine Permutation

$$\tau \;=\; \underbrace{(i_1 \ldots i_{r_1}) \circ (i_{r_1+1} \ldots i_{r_1+r_2}) \circ \ldots \circ (i_{r_1+r_2+\ldots+r_{k-1}+1} \ldots i_{n-1})}_{k \text{ Zyklen der Längen } r_1,r_2,\ldots,r_k \text{ aus } \mathrm{Perm}_k(\underline{n-1})}$$

Umgekehrt liefert jedes solche $\tau \in \mathrm{Perm}_k(\underline{n-1})$ genau $n-1$ Elemente σ aus X_2, indem wir vor
i_1 n einfügen
i_2 n einfügen
$\vdots$
i_{n-1} n einfügen

Wir haben dann

$$(n\, i_1 \ldots i_{r_1}) \circ (i_{r+1} \ldots) \circ \ldots$$
$$(i_1\, n \ldots i_{r_1}) \circ (i_{r+1} \ldots) \circ \ldots$$
$$\ldots$$
$$|X_2| = (n-1)|\mathrm{Perm}_k(\underline{n-1})| = (n-1)s_{n-1,k}$$

■

Beispiel 3
Wir suchen $s_{4,3}$, also die Anzahl der Elemente S_4, die aus 3 Zyklen bestehen.

$$\mathrm{Perm}_3(\underline{4}) = \{(1\,2)(3)(4), (1\,3)(2)(4), (1\,4)(2)(3), (2\,3)(1)(4), (2\,4)(1)(3), (3\,4)(1)(2)\}$$

also $s_{4,3} = 6$.

Wir gehen nun vor wie im Beweis. X_1 bildet hier die Menge der Zyklen, die 4 als 1-Zyklus enthalten:

$$X_1 = \{(1\,2)(3)(4), (1\,3)(2)(4), (2\,3)(1)(4)\}$$

Lösche die 4 in allen anderen Zyklen:

$$(1\,\not{4})(2)(3) = (2\,\not{4})(1)(3) = (3\,\not{4})(1)(2)$$

umgekehrt liefert $\tau = (1)(2)(3)$ durch Einsetzen der 4:

$$\begin{aligned}(4\,1)(2)(3) &= (1\,4)(2)(3)\\ (1)(4\,2)(3) &= (1)(2\,4)(3)\\ (1)(2)(4\,3) &= (1)(2)(3\,4)\end{aligned}$$

also ist dann

$$s_{4,3} = |X_1| + |X_2| = 3 + (4-1)\cdot 1 = 6$$

§ 4 Formale Potenzreihen (erzeugende Funktionen)

Bei der Komplexitätsanalyse von Algorithmen entstehen oft Rekursionsgleichungen wie z.B.

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

Um solche Rekursionen explizit zu lösen brauchen wir „**erzeugende Funktionen**“.

Haben wir nun eine solche Folge

$$(a_n)_{n\in\mathbb{N}_0} = (a_0, a_1, \ldots),$$

dann konstruieren wir daraus einen formalen Ausdruck

$$\sum_{n=0}^{\infty} a_n x^n,$$

wobei x eine „Unbestimmte“ ist, die wir aber als „Blackbox“ betrachten, d.h. wir werden “da nie etwas einsetzen”.

Sei K ein beliebiger Körper, z.B. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_2$.

Definition 1

$$K[\![x]\!] := \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in K \right\}$$

und

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

Für $n, k \in \mathbb{N}_0$ gilt:

$$\begin{aligned}
x^n &= (a_j)_{j\in\mathbb{N}_0} \text{ mit } a_j = \begin{cases} 1 & \text{wenn } j = n \\ 0 & \text{sonst} \end{cases} \\
\sum_{n=m}^{\infty} a_n x^n &= (b_j)_{j\in\mathbb{N}_0} \text{ mit } b_j = \begin{cases} a_j & \text{für } j \geq m \\ 0 & \text{sonst} \end{cases} \\
\sum_{n=0}^{\infty} a_n x^{kn} &= (b_j)_{j\in\mathbb{N}_0} \text{ mit } b_j = \begin{cases} a_n & \text{für } j = kn \\ 0 & \text{sonst(wenn } j \neq kn) \end{cases}
\end{aligned}$$

Beispiel 1

Seien $a_n = n!$, $k = 2$,

$$\sum_{n=0}^{\infty} a_n x^{kn} = 1 + 1!x^2 + 2!x^4 + 3!x^6 + \ldots = (1, 0, 1!, 0, 2!, \ldots)$$

$$b_4 = 2! = a_2$$

02.05.MMI

K sei ein Körper $\quad \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_2$.

$$K[\![x]\!] = \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in K \right\}$$

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

formale Potenzreihe (in x)
erzeugende Funktion der Folge $(a_n)_{n \in \mathbb{N}_0}$.
[Zum Vergleich $\quad 1,125 = \frac{9}{8} \in \mathbb{Q}$]

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

$$\delta_{m,n} = \begin{cases} 1 & \text{für } m = n \\ 0 & \text{sonst} \end{cases}$$

genannt **Kronecker-Symbol**.

Satz 1
Definiert man

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n := \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

und für $a \in K$

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

so wird $K[\![x]\!]$ ein K-Vektorraum.

Beweis
s. LA I

■

Satz 2
Definiert man (zusätzlich zu + in Satz 1)

$$\begin{aligned} (\sum_{i=0}^{\infty} a_i x^i) \cdot (\sum_{j=0}^{\infty} b_j x^j) &= \sum_{k=0}^{\infty} (\sum_{i+j=k} a_i b_j) x^k \\ &= \sum_{k=0}^{\infty} (\sum_{i=0}^{k} a_i b_{k-i}) x^k \end{aligned}$$

so ist $(K[\![x]\!], +, \cdot)$ ein **kommutativer Ring mit Eins**, d.h.

(A1) $(A+B)+C = A+(B+C)$ (*)

(A2) $A+B = B+A$ (*)

(A3) Es gibt $0(=0\cdot x^0)$ mit $0+A=A$ für alle $A \in K[\![x]\!]$

(A4) Zu $A \in K[\![x]\!]$ existiert $-A \in K[\![x]\!]$ mit $A+(-A)=0$

(M) $(A\cdot B)\cdot C = A\cdot(B\cdot C)$ (*)

(Kom) $A\cdot B = B\cdot A$ (*)

(Eins) Es gilt $1 \in K[\![x]\!]$ und $1\cdot A = A$ für alle $A \in K[\![x]\!]$

(D) Es gilt $A\cdot(B+C) = A\cdot B + A\cdot C$ (*)

(*) für alle $A, B, C \in K[\![x]\!]$.

Beweis
Durch Nachrechnen ;)

Einselement ist $1\cdot x^0 = 1$

Allgemein gilt:

Lemma 1

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

In der **Folgensprache** bedeutet dies

$$x^m \cdot (a_0, a_1, a_2, \ldots) = (\underbrace{0, 0, \ldots, 0}_{m \text{ Stück}}, a_0, a_1, a_2, \ldots)$$

Die Multiplikation mit x^m bewirkt ein Verschieben der Folge $(a_n)_{n\in\mathbb{N}_0}$ um m Stellen nach rechts.

Beweis

$$x^m \cdot \sum_{n=0}^{\infty} a_n \cdot x^n \underset{Def}{=} \sum_{k=0}^{\infty} \Big(\sum_{i=0}^{k} \underbrace{\delta_{m,i} \cdot a_{k-i}}_{0 \text{ für } i\neq m, \text{ insbesondere stets wenn } i\leq k<m} \Big) x^k = \sum_{n=m}^{\infty} (a_{n-m} x^n)$$

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

folgerung

$$x^m \cdot x^n = x^{m+n}$$

Beispiel 2
Für $c \in K$ gilt:

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

Definition 2 (und Bemerkung)
Ist in einem kommutativen Ring mit Eins

$$A \cdot B = 1,$$

so ist B durch A (und A durch B) eindeutig bestimmt und wird mit $B = A^{-1} = \frac{1}{A}$ (bzw. $A = B^{-1} = \frac{1}{B}$) bezeichnet.
A (und B) heißen **invertierbar**.

Beweis
Eindeutigkeit

Ist $A \cdot B = 1$ und $A \cdot C = 1$, so folgt

$$C = C \cdot 1 = C \cdot (A \cdot B) = (C \cdot A) \cdot B = 1 \cdot B = B$$

Beispiel 3
In $\mathbb{Z}$ sind nur 1 und -1 invertierbar.

Folgerung 1
In $K[\![x]\!]$ ist $\sum_{i=0}^{\infty} c^i x^i$ für $c \in K$ invertierbar und

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

Frage: Ist $\frac{1}{1-cx}$ eine **formale Potenzreihe**?

Gegenfrage: Ist $\frac{1}{0{,}5} \in \mathbb{Z}$?

Beispiel 4 (Code mit variabler Wortlänge)
(zum Komprimieren von Daten)

Sei

$$Bu = \{a, b, c\}, \qquad Zi = \{0, 1\}$$

$$W_k = \{ \text{ Folgen aus } 0 < i < k \text{ Buchstaben gefolgt von } k - i \text{ Ziffern } \},$$

$$Co_n = \bigcup_{k=2}^{n} W_k$$

Inhaltlich noch nicht korrekt:

z.B. $aa1|bc0001|ac1 \in W_k$ (die „|“ sind zur genauren Kenntlichmachung der Wortgrenzen)

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

Behauptung

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

Beweis:

$$\begin{aligned} c = \sum_{k=0}^{\infty} c_k x^k \quad &= \quad \left(\sum_{i=0}^{\infty} 3^i x^i \right) \left(\sum_{j=0}^{\infty} 2^j x^j \right) \\ &\underset{\text{(Folg. 2)}}{=} \quad \frac{1}{1-3x} \cdot \frac{1}{1-2x} \\ &= \quad \frac{\alpha}{1-3x} + \frac{\beta}{1-2x} \\ &= \quad \frac{\alpha(1-2x) + \beta(1-3x)}{(1-3x)(1-2x)} \end{aligned}$$

$$\begin{aligned} \alpha(1-2x) + \beta(1-3x) &= 1 \\ \alpha + \beta &= 1 \\ -2\alpha - 3\beta &= 0 \\ -\beta &= 2 \\ \alpha &= 3 \end{aligned}$$

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

Satz 3
Genau dann ist

$$A = \sum_{n=0}^{\infty} a_n x^n \in K[\![x]\!]$$

invertierbar, wenn $a_0 \neq 0$ ist.

Beweis
A invertierbar $\Leftrightarrow$ Es gibt $B = \sum_{i=0}^{\infty} b_i \cdot x^i$ mit $A \cdot B = 1$.

$$\begin{aligned} & \sum_{k=0}^{\infty} (\sum_{i=0}^{k} a_i b_{k-i}) x^k = 1 \\ \Leftrightarrow \quad & \sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} 1 & \text{für } k = 0 \\ 0 & \text{sonst} \end{cases} \\ \Leftrightarrow \quad & a_0 b_0 = 1 \quad k = 0 \\ & a_1 b_0 + a_0 b_1 = 0 \quad k = 1 \\ & a_2 b_0 + a_1 b_1 + a_0 b_2 = 0 \quad k = 2 \\ & \dots \end{aligned}$$

Ist B invertierbar, so muss $a_0 \neq 0$, sonst ist die Gleichung für $k = 0$ nicht erfüllbar.

Umgekehrt ist $a_0 \neq 0$ so zu definieren, dass $b_0 = a_0^{-1} \in K$ und $b_n = \frac{1}{a_0}(-a_1 b_{n-1} - \ldots - a_n b_0)$ rekursiv.

04.05.2001

$$\begin{aligned} K[\![x]\!] &= \{\sum_{a=0}^{\infty} a_n x^n \mid a_n \in K\} \text{ formale Potenzreihen} \\ K[x] &= \{\sum_{a=0}^{\infty} a_n x^n \mid a_n \in K \text{ und } a_n \neq 0 \text{ nur für endlich viele n}\} \\ &= \left\{\sum_{a=0}^{r} a_n x^n \mid a_n \in K, r \in \mathbb{N}_0\right\} \end{aligned}$$

Zu $K[x]$ gibt es "**Einsetzungshomomorphismen**". Ist dagegen $A \in K[\![x]\!]$, so kann man in A im Allgemeinen nichts einsetzten.

In $K[x]$ sind nur die Polynome vom Grad 0 invertierbar, dagegen:

Satz 3 nochmal

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

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) \cdot \left(\sum_{n=0} x^n\right) = \sum_{n=0}^{\infty} \underbrace{\left(\sum_{i=0}^{n} a_i b_{n-i}\right)}_{S_{n,0}} x^n$$

$$\text{mit } S_{n,0} = \begin{cases} 1 & n = 0 \\ 0 & \text{sonst} \end{cases}$$

Dann ist $(b_0, b_1, \ldots)$ Lösung des folgenden Gleichungssystems

$$\begin{aligned} a_0 x_0 &= 1 \\ a_1 x_0 + a_0 x_1 &= 0 \\ a_2 x_0 + a_1 x_1 + a_0 x_2 &= 0 \end{aligned}$$

Beispiel 5

$a_0 = 1, a_1 = -c \in K, a_2 = a_3 = \ldots = 0$

$$A = 1 - cx$$

$$\begin{aligned} x_0 &= 1 \\ -cx_0 + x_1 &= 0 \Rightarrow x_1 = c \\ -cx_1 + x_2 &= 0 \Rightarrow x_2 = cx_1 = c^2 \ldots x_n = c^n \end{aligned}$$

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

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

Beispiel 6

$$\begin{aligned} \left(\sum_{n=0}^{\infty} c^n x^n\right)^2 &\underset{Satz2}{=} \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} c^i c^{n-i}\right) x^n \\ &= \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} c^n\right) x^n \\ &= \sum_{n=0}^{\infty} (n+1) c^n x^n \end{aligned}$$

linke Seite: $\left(\frac{1}{1-cx}\right)^2 = \frac{1}{(1-cx)^2}$

Folgerung 2

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

allgemein:

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

Beweis Übung!

Definition 3
Die Abbildung $D : K[\![x]\!] \longrightarrow K[\![x]\!]$

$$\sum_{n=0}^{\infty} a_n x^n \longrightarrow \sum_{n=0}^{\infty}(n+1)a_{n+1}x^n$$

heißt **formale Ableitung**

Lemma 2
$D : K[\![x]\!] \to K[\![x]\!]$ ist k-linear und es gilt:

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

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

Folgerung 3
Ist $A \in K[\![x]\!]$ invertierbar, so ist

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

Beweis

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

$$0 = D(A \cdot A^{-1}) = A \cdot D(A^{-1}) + D(A) \cdot A^{-1} \text{ nach Lemma 1 b}$$

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

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

Beispiel 7
$A = 1 - cx \in K[\![x]\!] \quad A^{-1} = \sum_{n=0}^{\infty} c^n x^n$

$$\begin{aligned} D(A^{-1}) &= \sum_{n=0}^{\infty}(n+1)c^{n+1}x^n \quad D(A) = -c \\ &= -\frac{D(A)}{A^2} = \frac{c}{(1-cx)^2} \quad c \neq 0 \\ \frac{1}{(1-cx)^2} &= \sum_{n=0}^{\infty}(n+1)c^n x^n \end{aligned}$$

neuer Beweis von Folgerung 2.

§ 5 Lösen von Rekursionsgleichungen

Beispiel 1
Die **Fibonacci-Zahlen** F_n sind (für $n \in \mathbb{N}$) so definiert:

$$F_0 = 0 \quad F_1 = 1$$

$$(*) \qquad F_n = F_{n-1} + F_{n-2} \quad \text{für alle } n \geq 2$$

z.B. $F_2 = 1 \quad F_3 = 2 \quad F_4 = 3 \quad F_5 = 5 \quad \ldots$
Sei

$$\begin{aligned} F = F(x) &= \sum_{n=0}^{\infty} F_n x^n \\ &= F_0 x^0 + F_1 x + \sum_{n=2}^{\infty} \underbrace{(F_{n-1} + F_{n-2})}_{\text{benutzte (*)}} x^n \\ &= F_0 x^0 + F_1 x + \sum_{n=2}^{\infty} F_{n-1} x^n + \sum_{n=2}^{\infty} F_{n-2} x^n \\ &= F_0 x^0 + F_1 x + x \underbrace{\sum_{n=1}^{\infty} F_n x^n}_{F - F_0 x 0} + x^2 \underbrace{\sum_{n=0}^{\infty} F_n x^n}_{F} \\ &= F_0 x^0 + F_1 x + xF + x^2 F - xF_0 x^0 \end{aligned}$$

$F_0 = 0 \quad F_1 = 1$

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

$$F(1 - x - x^2) = x$$

$$F = \frac{x}{1 - x - x^2} \quad K = \mathbb{C}$$

suche $\alpha, \beta \in K$ und $a, b \in K$, so daß:

$$\frac{x}{1-x-x^2} = \frac{a}{1-\alpha x} + \frac{b}{1-\beta x}$$

dann folgt:

$$\sum f_n x^n = F = a\sum_{n=0}^{\infty} \alpha^n x^n + b\sum_{n=0}^{\infty} \beta^n x^n$$

$$= \sum_{n=0}^{\infty} (a\alpha^n + b\beta^n) x^n$$

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

09.05.2001

Fibonacci Zahlen

$$\begin{aligned} F_0 &= 0 \qquad F_1 = 1 \\ F_n &= F_{n-1} + F_{n-2} \\ F &= F(x) = \sum_{n=0}^{\infty} F_n x^k \\ F &= \frac{x}{1-x-x^2} = \frac{a}{1-\alpha x} + \frac{b}{1-\beta x} \qquad a, b, \alpha, \beta \in \mathbb{C} \\ F_n &= a\alpha^n + b\beta^n \end{aligned}$$

Satz 1 (Partialbruchzerlegung)
K sei ein Körper

$$g = (1-\alpha_1 x)^{m_1} \dots (1-\alpha_r x)^{m_r} \qquad \in K[x] \qquad \alpha_i \neq 0 \forall i$$

$f \in K[x]$ Grad $f <$ Grad g
Dann gibt es $f_i \in K[x]$ Grad $f_i < m_i$ mit

$$\begin{aligned} \frac{f}{g} &= \frac{f_1}{(1-\alpha_1 x)^{m_1}} + \dots + \frac{f_r}{(1-\alpha_r x)^{m_r}} \\ \frac{f_i}{(1-\alpha_i x)^{m_i}} &= \frac{\alpha_{i_1}}{(1-\alpha_i x)} + \frac{\alpha_{i_2}}{(1-\alpha_i x)^2} + \dots + \frac{\alpha_{i_{m_i}}}{(1-\alpha_i x)^{m_i}} \end{aligned}$$

(Beweis siehe "Algebraische Strukturen")

Bemerkung
Ist g wie in Satz 1, so sind die α_i^{-1} Nullstellen von g.

Definition 1
Ist $g = \sum_{i=0}^{n} a_i x^i$ mit $a_n \neq 0$, so sei

$$g^R = \sum_{i=0}^{n} a_{n-i} x^i$$

reflektiertes Polynom

Beispiel 2

$$\begin{aligned} g &= 1 + 2x + 3x^2 \\ g^R &= x^2 + 2x + 3 \end{aligned}$$

Lemma 1
Es gilt $g(\alpha) = 0$ mit $\alpha \neq 0 \Leftrightarrow g^R(\alpha^{-1}) = 0$

Beweis
Sei $\alpha \neq 0$ in K

$$\begin{aligned} 0 = g(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \quad &\Leftrightarrow \quad 0 = \alpha^{-n} g(\alpha) = \sum_{i=0}^{n} a_i \alpha^{i-n} \\ &\Leftrightarrow \quad 0 = \sum_{j=0}^{n} a_{n-j} \alpha^{-j} \qquad j = n - i; i = n - j \\ &\Leftrightarrow \quad g^R(\alpha^{-1}) = 0 \end{aligned}$$

Satz 2 (Fundamentalsatz der Algebra)
Ist

$$g = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x] \qquad \text{mit } a_n \neq 0$$

, so gibt es

$$\alpha_1, \ldots \alpha_n \in \mathbb{C} \text{ mit } g = a_n (x - \alpha_1) \ldots (x - \alpha_n)$$

.
(ohne Beweis)

Folgerung 1
Ist $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x]$ und $a_n \neq 0, a_0 \neq 0$, so gibt es $\alpha_1, \ldots, \alpha_n$ mit

$$f = a_0 (1 - \alpha_1 x) \ldots (1 - \alpha_n x)$$

denn nach Satz 2

$$\begin{aligned} f^R &= a_0(x-\alpha_1)\dots(x-\alpha_n) \\ f = (f^R)^R &= x^n\left(\frac{1}{x}-\alpha_1\right)\dots\left(\frac{1}{x}-\alpha_1\right) \\ &= (1-\alpha_1 x)\dots(1-\alpha_n x) \end{aligned}$$

Beispiel 3 (Fortsetzung)

$$F = \frac{x}{1-x-x^2} = \frac{f}{g}$$
$$g^R = x^2 - x - 1 = (x-\alpha_1)(x-\alpha_2)$$
$$\alpha_1 = \frac{1+\sqrt{5}}{2} \qquad \frac{1-\sqrt{5}}{2}$$

α_1 heisst **goldener Schnitt**

$$\begin{aligned} g &= (1-\alpha_1 x)(1-\alpha_2 x) \\ \frac{f}{g} &= \frac{x}{1-x-x^2} = \frac{a}{1-\alpha_1 x} + \frac{b}{1-\alpha_2 x} \qquad \text{mit } a,b \in \mathbb{C} \text{ existiert nach Satz 1} \\ \frac{x}{1-x-x^2} &= \frac{a(1-\alpha_2 x)+b(1-\alpha_1 x)}{(1-\alpha_1 x)(1-\alpha_2 x)} \end{aligned}$$

$$\begin{aligned} x &= a+b-(a\alpha_2+b\alpha_1)x \\ & a+b=0 \Rightarrow b=-a \end{aligned}$$

$$\begin{aligned} a\alpha_2 - b\alpha_1 &= -1 \\ a\alpha_2 + a\alpha_1 &= -1 \\ a &= \frac{-1}{\alpha_1-\alpha_2} \end{aligned}$$

$$a = +\frac{1}{\sqrt{5}} \qquad b = -\frac{1}{\sqrt{5}}$$

$$\begin{aligned} F_n &= a\alpha_1^n + b\alpha_2^n \\ &= \sqrt{5}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \underbrace{\left(\frac{1-\sqrt{5}}{2}\right)^n}_{-1< \quad <0}\right] \end{aligned}$$

für n ungerade:

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

Verfahren zum Lösen von linearen Rekursionen (mit konstanten Koeffizienten)
Geg:

$$a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k} \qquad n \geq k$$

mit gegebenem $c_i \in \mathbb{C}$ und Anfangsbedingung:

$$a_i = b_i \qquad \text{für } i = 0, 1, \ldots, k-1 \qquad b_i \in \mathbb{C} \text{ gegeben}$$

$$\begin{aligned} A &:= \sum_{n=0}^{\infty} a_n x^n \\ &= \sum_{i=0}^{k-1} a_i x^i + \sum_{n=k}^{\infty} (c_1 a_{n-1} + \ldots + c_k a_{n-k}) x^n \\ &= \sum_{i=0}^{k-1} b_i x^i + c_1 x \cdot (A - \sum_{i=0}^{k-1} b_i x^i) + c_2 x^2 \cdot (A - \sum_{i=0}^{k-2} b_i x^i) + \ldots + c_k x^k A \end{aligned}$$

Auflösen nach A:

$$A = \frac{f}{1 - c_1 x - \ldots - c_k x^k}$$

mit $f = b_0 + (b_1 - c_1 b_0)x + \ldots + (b_k - c_1 b_{k-1} - \ldots - c_k b_0)x^k$
Partialbruchzerlegung

$$\begin{aligned} A &= \sum_{i=1} \frac{f_i}{(1 - \alpha_i x)^{m_i}} \\ mit \quad f_i &= \sum_{j=0}^{m_{i-1}} f_{ij} x^i \\ &= \sum_{i=1}^{n} \sum_{j=0}^{m_{i-1}} f_{ij} \sum_{n-j}^{\infty} \binom{n+m-1}{k} \alpha_i^{n-j} x^n \end{aligned}$$

Bemerkung
Die α_i im Verfahren erhält man als Nullstellen des reflektierten Polynoms

$$g^R = x^k - c_1 x^{k-1} - \ldots - c_{k-1} x - c_k$$

Die f_{ij} kann man durch die Anfangsbedingungen bestimmen.

Beispiel 4

$$\begin{aligned} a_n &= a_{n-1} + a_{n-2} \\ g &= 1 - x - x^2 \\ g^R &= x^2 - x - 1 = (x - \alpha_1)(x - \alpha_2) \qquad \alpha_1 \neq \alpha_2 \\ a_n &= a\alpha^n + b\beta^n \end{aligned}$$

$$\begin{aligned} n &= 0 \qquad a_0 = 0 = a + b \\ n &= 1 \qquad a_1 = 1 = a\alpha + b\beta \end{aligned}$$

Beispiel 5

$$\begin{aligned} \mathcal{C}_n &= \{\text{zulässige Klammerungen mit } 2n \text{ Klammern}\} \\ C_n &= \text{Anzahl } (\mathcal{C}_n) = |\mathcal{C}_n| \\ C_0 &= 1 \\ C_1 &= 1 \\ C_2 &= 2 \\ C_3 &= 5 \\ &\dots \\ C_n &= n - \text{te } \textbf{Catalan-Zahl} \end{aligned}$$

$\mathcal{C}_n^{(k)} = \{$ Zeichenkette aus $\mathcal{C}_n$, bei der die erste Klammer an der Position $2k$ geschlossen wird $\}$.

$$\begin{aligned} \mathcal{C}_n &= \dot{\bigcup_{k=1}^{n}} \mathcal{C}_n^{(k)} \\ |\mathcal{C}_n| = C_n &= \sum_{k=1}^{n} c_{k-1} c_{n-k} \qquad n \geq 1 \\ C &= \sum_{n=0}^{\infty} c_n x^n \\ &= \underbrace{C_0 x^0}_{=1} + \sum_{n=1}^{\infty} c_n x^n \\ &= 1 + \sum_{n=1}^{\infty} \left(\sum_{k=1}^{n} c_{k-1} c_{n-k} \right) x^n \\ &= 1 + (x \cdot C) \cdot C \\ C &= 1 + x \cdot C^2 \end{aligned}$$

$$\begin{aligned} x^2C^2 - xC + x &= 0 \\ x^2C^2 - xC + \frac{1}{4} &= -x + \frac{1}{4} \\ \left(xC - \frac{1}{2}\right)^2 &= -x + \frac{1}{4} \\ xC - \frac{1}{2} &= \pm\sqrt{-x + \frac{1}{4}} \\ xC &= \frac{1}{2}(1 \pm \sqrt{1-4x}) \end{aligned}$$

11.05.MMI

Satz 3
Ist K ein Körper mit $1 + 1 \neq 0$ (d.h. char$K \neq 2$), dann gibt es zu jeder Potenzreihe

$$A = \sum_{i=0}^{\infty} a_i x^i \in K[\![x]\!] \text{ ein } B = \sum_{i=0}^{\infty} b_i x^i \in K[\![x]\!] \text{ mit } B^2 = A$$

genau dann, wenn a_0 in K ein Quadrat ist.

Beweis

$$B^2 = \sum_{n=0}^{\infty} \underbrace{\left(\sum_{k=0}^{n} b_k b_{n-k}\right)}_{a_n} x^n = A$$

genau dann, wenn (für alle $n = 0, 1, \ldots$)

$$\begin{aligned} b_0^2 &= a_0 \qquad b_0 = \overset{+}{\underset{-}{}} b (\neq 0) \\ b_0 b_1 + b_1 b_0 = 2 b_0 b_1 &= a_1 \qquad b_1 = \frac{1}{2b_0} \cdot a_1 \\ &\ldots \\ b_n &= (a_n - \sum_{k=1}^{n-1} b_n b_{n-k}) \frac{1}{2b_0} \end{aligned}$$

¿¿ Hier scheint noch was zu fehlen :(¡¡

§ 6 Die Polynommethode

Satz 1
Ist K ein Körper und $0 \neq f \in K[x]$ mit

$$f = \sum_{k=0}^{n} a_k x^k \qquad a_n \neq 0,$$

so hat f höchstens n Nullstellen.

Beweis (siehe LA I)

Folgerung 1
Sind

$$f = \sum_{i=0}^{n} a_i x^i, \qquad g = \sum_{i=0}^{n} b_i x^i \in K[x]$$

und ist

$$f(\alpha_i) = g(\alpha_i) \text{ für alle } \alpha_i \in M \subseteq K \text{ mit } |M| \geq n+1$$

so gilt

$$f = g, \text{ d.h. } a_i = b_i \forall i = 0, 1, \ldots.$$

Beweis
Folgt aus Satz 1; betrachte $f - g$, $\text{grad}(f-g) \leq n$, also $f - g = 0$.

Definition 1
Sei K ein Körper mit $\mathbb{Q} \subseteq K$, dann ist „x hoch n fallend“ definiert durch

$$x^{\underline{n}} = x(x-1)...(x-n+1) \in K[x], \text{ und}$$

„x über n“ durch

$$\binom{x}{n} = \frac{1}{n!} \cdot x^{\underline{n}} \qquad \in K[x]$$

mit

$$x^{\underline{0}} = 1 \text{ und } \binom{x}{0} = 1.$$

Beispiel 1

$$\binom{x}{1} = x, \qquad \binom{x}{2} = \frac{1}{2}x(x-1)$$

Nach §2 Satz 3, gilt

$$\begin{aligned} m^n &= \sum_{k=0}^{m} S_{n,k} m^{\underline{k}} \\ &= \sum_{k=0}^{n} S_{n,k} m^{\underline{k}}, \text{ denn} \end{aligned}$$

für $n \geq k \geq m$ gilt $m^{\underline{k}} = m(m-1) \cdot \ldots \cdot 0 \cdot [\ldots] = 0$

für $n < k \leq m$ gilt $S_{n,k} = 0$

$$\begin{aligned} \text{Setze } f &= x^n \qquad (*) \\ g &= \sum_{k=0}^{n} S_{n,k} x^{\underline{k}} \end{aligned}$$

$f(m) = g(m)$ für alle $m \in \mathbb{N}$ wegen (*)

Satz 2
Ist $\mathbb{Q} \subseteq K$ Körper, so gilt

a)
$$x^n = \sum_{k=0}^{n} S_{n,k} x^{\underline{k}}$$

b)
$$x^{\underline{n}} = \sum_{k=0}^{n} (-1)^{n-k} s_{n,k} x^k$$

Beweis (Übung)
a) siehe unten, benutze Satz 1

b) Benutze Induktion über $s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}$

Bemerkung

$$(x^n)_{n \in \mathbb{N}_0} \text{ und } (x^{\underline{n}})_{n \in \mathbb{N}_0}$$

sind K-Basen des K-Vektorraums $K[x]$ und

$$[S_{n,k}]_{n,k \in \mathbb{N}_0} \text{ und } [(-1)^{n-k} s_{n,k}]_{n,k \in \mathbb{N}_0}$$

sind **Basiswechselmatrizen**, also invers zueinander.

In § 1 Satz **??** haben wir die van-der-Mond'sche Gleichung eingeführt/bewiesen.

$$\binom{m+n}{k} = \sum_{l=0}^{k} \binom{m}{l} \binom{n}{k-l} \qquad \begin{array}{l} \forall\, m, n, k \in \mathbb{N} \\ \text{wegen kombinatorischem} \\ \text{Beweis} \end{array}$$

spezialisiert gilt

$$(*) \qquad \binom{(j+1)m}{k} = \sum_{l=0}^{k} \binom{m}{l} \binom{j*m}{k-l} \qquad j \in \mathbb{N}, \quad m, n \in \mathbb{Z}$$

$$\binom{(j+1)x}{k} = \sum_{l=0}^{k} \binom{x}{l}\binom{j*x}{k-l} \qquad \in K[x]$$

nach Satz 1 (bzw. Folgerung **??**) wegen (*) stimmen linke und rechte Seite für ∞ viele m überein.

Satz 3
Für $c \in K$ ($\mathbb{Q} \subseteq K, K$ Körper) und $m \in \mathbb{N}$ setze

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

dann gilt für $1 \leq j \leq m, j \in \mathbb{N}$

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

b)
$$((1+cx)^{\frac{1}{m}})^m = 1+cx$$

Beweis
a) Induktion über j:

$$\begin{aligned} j=1 &\quad \text{Behauptung, klar} \\ j \geq 1 &\quad ((1+cx)^{\frac{1}{m}})^{j+1} = ((1+cx)^{\frac{1}{m}})^j (1+cx)^{\frac{1}{m}} \\ &= \sum_{n=0}^{\infty} (\sum_{k=0}^{n} \binom{\frac{j}{m}}{k} c^k \binom{\frac{1}{m}}{n-k} c^{n-k}) x^n \\ &= \sum_{n=0}^{\infty} (\underbrace{\sum_{k=0}^{n} \binom{\frac{j}{m}}{k}\binom{\frac{1}{m}}{n-k}}_{\binom{\frac{j+1}{m}}{k} nach \S 6 Satz 2}) c^n x^n \end{aligned}$$

b) Wende a) an für $j = m$

16.05.MMI

Ausgangspunkt für die Polynommethode ist, dass eine Gleichung wie

$$(*) \qquad \binom{2m}{n} = \sum_{k=0}^{n} \binom{m}{k}\binom{m}{n-k}$$

gültig ist für alle $m, n \in \mathbb{N}$. Gesucht sind die Polynome $f, g \in K[x]$ mit $K \supseteq \mathbb{Q}$ mit

$$\begin{aligned} f(m) &= LS(*) \\ g(m) &= RS(*) \end{aligned}$$

wobei $LS(*)$ die linke Seite und $RS(*)$ die rechte Seite von der Gleichung $(*)$ meinen

Satz 1 impliziert dann $f = g$ und es gilt für alle $z \in K$

$$f(z) = g(z)$$

Im Beispiel ist

$$\begin{aligned} f &= \binom{2x}{n} = \frac{1}{n!}(2x)(2x-1)\cdot \ldots \cdot (2x-n+1) \\ g &= \sum_{k=0}^{n} \binom{x}{k}\binom{x}{n-k}, \text{ also} \\ \binom{2z}{n} &= \sum_{k=0}^{n} \binom{z}{k}\binom{z}{n-k} \qquad \forall\, z \in \mathbb{C} \quad [\text{bzw. } z \in \mathbb{C}^{n\times n}] \end{aligned}$$

Sei etwa $z = \frac{1}{2}$, dann ist

$$\sum_{k=0}^{n} \binom{\frac{1}{2}}{k} \cdot \binom{\frac{1}{2}}{n-k} = \binom{1}{n} = \begin{cases} 1 & \text{für } n = 0, 1 \\ 0 & n > 1 \end{cases}$$

$$\left(\sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} c^n x^n\right)^2 = 1 + cx =: (1+cx)^{\frac{1}{2}}.$$

Beispiel 2 (Fortsetzung von §5 Catalanzahlen)

$$\begin{aligned} C_n &= \text{Anzahl der regulären Klammerungen mit } 2n \text{ Klammern} \\ &= \text{Anzahl der binären Suchbäume mit } n \text{ Knoten} \end{aligned}$$

$$C_0 = 1, \quad C_1 = 1, \quad C_2 = 2$$

$$
\begin{aligned}
C_n &= \sum_{k=0}^{n-1} C_k C_{n-1+k}, \qquad n \geq 1 \\
C = \sum_{n=0}^{\infty} C_n x^n &= 1 + xC^2 \qquad | \cdot x \\
\Leftrightarrow (xC - \frac{1}{2})^2 &= \frac{1}{4}(1-4x) \\
\Leftrightarrow xC - \frac{1}{2} &= \pm\frac{1}{2}(1-4x)^{\frac{1}{2}} \\
\Leftrightarrow \sum_{n=1}^{\infty} \underbrace{C_{n-1}}_{\text{Koeff.}} x^n = xC &= \frac{1}{2}\left(1 \pm \frac{1}{2}\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}(-4)^n x^n\right)
\end{aligned}
$$

Da der Koeffizient von x^0 $C_{n-1} = 0$, gilt $-$ als Vorzeichen und durch Koeffizientenvergleich gilt:

$$
\begin{aligned}
C_n &= -\frac{1}{2}\binom{\frac{1}{2}}{n+1}(-4)^{n+1} \\
&= -\frac{1}{2}(-1)^{n+1} \cdot 4^{n+1} \cdot \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)\cdot\ldots\cdot(\frac{1}{2}-n)}{(n+1)!} \\
&= -\frac{1}{2}2^{n+1}(-1)^1 \cdot \frac{1\cdot 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)}{(n+1)!} \cdot \frac{n!}{n!} \\
&= \frac{1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)\cdot 2\cdot 4\cdot\ldots(2n)}{(n+1)!n!} \\
&= \frac{1}{n+1}\cdot\frac{(2n)!}{n!n!} \\
&= \frac{1}{n+1}\binom{2n}{n}
\end{aligned}
$$

Kapitel 2

Algebraische Strukturen

§ 1 Universelle Algebren

Definition 1
Ist M eine Menge so heißt eine Abbildung

$$f : M^n = M \times \cdots \times M \to M$$

eine **n-stellige Operation** $n = s(f)$. Da $M^0 = \{\emptyset\}$, ist eine 0-stellige Operation vollständig beschrieben durch ein Element $a = f(\emptyset)$ aus M. Eine **universelle Algebra** vom Typ $(n_i)_{i\in I}$ ist $(M, (f_i)_{i\in I})$, wobei f_i eine n_i-stellige Operation auf M ist [$n_i = s(f_i)$ und I Indexmenge].

Bemerkung
2-stellige Operationen werden meist durch $+, \cdot, \circ, \ldots$ bezeichnet [Infix Notation $+(a, b) = a + b$].

Definition 2
Eine **Halbgruppe** ist eine **Algebra** $(H, \circ)$ vom Typ(2), bei der $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in H$ gilt.

Beispiel 1
A = Menge ("Alphabet") $\quad W(A) = \{(a_1, \ldots, a_n) \mid a_i \in A, n \in \mathbb{N}_0\}$ ("Worte in A")
$W \times W \to W$
$(a_1, \ldots, a_n), (b_1, \ldots, b_m) \to (a_1, \ldots, a_n, b_1, \ldots, b_m)$

Definition 3
Ein **Monoid** ist eine Algebra $(M, \circ, e)$ vom Typ$(2, 0)$ mit:

a.) $(M, \circ)$ ist eine Halbgruppe und

b.) für alle $a \in M$ $\quad e \circ a = a \circ e = a$ $\qquad$ e heißt **neutrales Element**

Definition 3 alt

Ein Monoid ist eine Halbgruppe $(M, \circ)$ mit:
Es gilt $e \in M$ mit $e \circ a = a \circ e = a$ für alle $a \in M$

Bemerkung
Sind $(H, \circ, e)$ und $(H, \circ, f)$ Monoide, (mit gleicher Verknüpfung $\circ$) so gilt $e = f$. d.h. das **neutrale Element** eines Monoids ist eindeutig bestimmt.

$$e = e \circ f = f$$

Definition 4
Eine **Gruppe** ist eine Algebra vom Typ$(2, 1, 0)$ $(G, \circ, ^{-1}, e)$, bei der folgende Regeln gelten $(G, \circ, e)$ ist ein Monoid und:
$g \circ g^{-1} = g^{-1} \circ g = e$ $\qquad$ für alle $g \in G$
Gilt zusätzlich $g_1 \circ g_2 = g_2 \circ g_1$ $\qquad$ für alle $g_1, g_2 \in G$,
so heißt $G = (G, \circ, ^{-1}, e)$ **abelsche Gruppe** oder **kommutative Gruppe**.

Beispiel 2

a.) $S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \mid \sigma \text{ bijektiv}\}$ $(S_n, \circ, ^{-1}, \underbrace{(1)}_{id})$

ist eine (nicht abelsche) Gruppe (für $n \geq 3$)

b.) $(\mathbb{Z}, +, -, 0)$
ist eine abelsche Gruppe

Definition 5
$(R, +, -, 0, \cdot, 1)$ vom Typ$(2, 1, 0, 2, 0)$ heißt ein **Ring (mit Eins)**, wenn $(R, +, -, 0)$ abelsche Gruppe und $(R, \cdot, 1)$ Monoid ist und folgendes gilt:

$$\begin{aligned} (a + b) \cdot c &= a \cdot c + b \cdot c \qquad \forall a, b, c \in R \\ a \cdot (a + c) &= a \cdot b + a \cdot c \end{aligned}$$

Gilt zusätzlich $a \cdot b = b \cdot a$ für alle $a, b \in R$ so heißt $(R, +, -, 0, \cdot, 1)$ **kommutativer Ring**.
Gilt zusätzlich zu jedem $a \in R \backslash \{0\}$ gibt es ein $a^{-1} \in R$ mit $a \cdot a^{-1} = a^{-1} \cdot a = 1$ und gilt $1 \neq 0$, so heißt $(R, +, -, 0, \cdot, 1)$ **kommutativer Körper**.

Beispiel 3
$(\mathbb{Z}, +, -, 0, \cdot, 1)$ ist kommutativer Ring
$(\mathbb{Q}, +, -, 0, \cdot, 1)$ sind Körper
$(\mathbb{R}, +, -, 0, \cdot, 1)$
$(\mathbb{C}, +, -, 0, \cdot, 1)$
$(\mathbb{F}_2, +, -, 0, \cdot, 1)$
$(K^{n\times n}, +, -, 0, \underbrace{E_n}_{\text{Einheitsmatrix}}, \cdot)$ ist nicht kommutativer Ring mit Eins
$K[x]$ Polynomring
$K[\![x]\!]$ Ring der formalen Potenzreihen

Definition 6
Ein **Vektorraum** über einem Körper K ist eine Algebra $(V, +, -, \cdot, K)$ vom Typ$(2, 1, 0, (1)_{i\in K})$ wobei $(V, +, -, \cdot)$ abelsche Gruppe ist.

$$\begin{array}{rrcll} & \alpha(v+w) & = & \alpha(v)+\alpha(w) & \alpha \in K \quad v, w \in V \\ 1 \in K & 1(v) & = & v & \\ & (\alpha+\beta)(v) & = & \alpha(v)+\beta(v) & \beta \in K \\ & (\alpha\cdot\beta)(v) & = & \alpha(\beta(v)) & \end{array}$$

Definition 7
Ist $(R, +, -, 0, \cdot, 1)$ Ring (mit Eins) so ist ein **R-Modul** eine Algebra $(M, +, -, \cdot, R)$ vom Typ$(2, 1, 0, (1)_{i\in R})$ wobei:

$$\begin{array}{rcll} \alpha(v+w) & = & \alpha(v)+\alpha(w) & \alpha \in R \\ 1(v) & = & v & v \in M \\ (\alpha+\beta)(v) & = & \alpha(v)+\beta(v) & \alpha, \beta \in R \\ (\alpha\cdot\beta)(v) & = & \alpha(\beta(v)) & v, w \in M \end{array}$$

§ 2 Unteralgebren, Homomorphismen, Kongruenzen

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

Definition 1
Die Algebra $U \subseteq A$ heißt **Unteralgebra** (im Zeichen $U \leq A$) genau dann, wenn

$$f_i(u_1, \ldots, u_{n_i}) \in U \text{ für alle } u_1, \ldots, u_{n_i} \in U, i \in I.$$

Insbesondere gilt: ist $n_i = 0$, also $f_i \in A$, so muß $f_i \in U$.

Bemerkung
Ist $U \leq A$, so ist $(U, (f_i|_U{}^{n_i})_{i\in I})$ Algebra vom Typ T.

Beispiel 1

a) Sei $G = (G, \cdot, ^{-1}, 1)$ Gruppe.

$$\begin{aligned} U \leq G &\Leftrightarrow U \text{ Untergruppe} \\ &\Leftrightarrow (u, u' \in U \Rightarrow u \cdot u' \in U, u^{-1} \in U, 1 \in U) \end{aligned}$$

b) Sei $V = (V, +, -, \underline{0}, K)$ ein K-Vektorraum.

$$U \leq V \Leftrightarrow U \textbf{ Untervektorraum} = \textbf{Teilraum}$$

c) Sind R Ring und $U \leq R$, so ist U ein **Teilring** (auch: **Unterring**) von R.

Lemma 1

$$U_j \leq A \text{ für } j \in J \text{ (= unendliche Indexmenge)} \Rightarrow \bigcap_{j \in J} U_j \leq A$$

Beweis (trivial)

Definition 2

Ist $M \subseteq A$, dann ist

$$\begin{aligned} \langle M \rangle &= \bigcap \{U | M \leq U \leq A\} \\ &= \textbf{Erzeugnis von } M, \text{ die von } M \textbf{ erzeugte Unteralgebra}. \end{aligned}$$

Beispiel 2

a) V ist K-Vektorraum, $v_1, \ldots, v_n \in V$.

$$\langle \{v_1, \ldots, v_n\} \rangle = \left\{ \sum_{i=1}^{n} \alpha_i v_i \mid \alpha_i \in K \right\}$$

b) $G = (G, \cdot, ^{-1}, 1)$ sei Gruppe, $g \in G$

$$\langle g \rangle = \langle \{g\} \rangle = \{g^i | i \in \mathbb{Z}\}, \text{ wobei}$$

$$g^i = \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{i \text{ mal}} & \text{für } i > 0 \\ 1 & \text{für } i = 0 \\ \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{-i \text{ mal} (-i > 0)} & \text{für } i < 0 \end{cases}$$

$$\langle \{g_1, \ldots, g_n\} \rangle = \left\{ a_1 \ldots a_m \mid m \in \mathbb{N}, a_j \in \{g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}\} \right\}$$

Definition 3
Sind $A = (A, (f_i)_{i\in I})$ und $A' = (A', (f'_i)_{i\in I})$ Algebren vom gleichen Typ $T = (n_i)_{i\in I}$ so heißt eine Abbildung

$$\varphi : A \to A'$$

ein (Algebra-) **Homomorphismus**, wenn

$$f'_i(\varphi(a_1), \ldots, \varphi(a_{n_i})) = \varphi(f_i(a_1, \ldots, a_{n_i}))$$

[insbesondere ist $\varphi(f_i) = f'_i$ falls $n_i = 0$, d.h. $f_i \in A$].

Ist zusätzlich φ bijektiv, so heißt φ ein **Isomorphismus**.

$$A \cong A' \underset{def}{\Leftrightarrow} \exists \text{ Isomorphismus } \varphi : A \to A'$$

Beispiel 3

a) V, W sind K-Vektorräume.

$$\varphi : V \to W \text{ Homomorphismus} \Leftrightarrow \varphi \text{ ist } K\text{-linear}$$

$$\begin{aligned} [\varphi(v_1 + v_2) &= \varphi(v_1) + \varphi(v_2) \text{ und} \\ \varphi(-v) &= -\varphi(v) \\ \varphi(\alpha \cdot v) &= \alpha \cdot \varphi(v) \\ \varphi(0) &= 0 \qquad] \end{aligned}$$

b) Seien $G_1 = (G_1, \cdot, ^{-1}, 1)$ und $G_2 = (G_2, *, ', e)$,

$$\varphi : G_1 \to G_2 \text{ Homomorphismus.}$$

(i) $\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2), \forall g_1, g_2 \in G_1$
(ii) $\varphi(g^{-1}) = \varphi(g)', g \in G_1$
(iii) $\varphi(1) = e$

Gilt (i) für alle g_i, so kann man (ii) und (iii) daraus folgern.

Definition 4
Eine **Äquivalenzrelation** $\sim$ heißt eine **Kongruenzrelation** auf der Algebra A, wenn folgendes gilt:

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

d.h. $\sim$ ist mit allen Verknüpfungen f_i verträglich.

Beispiel 4
Sei $(G, \cdot, ^{-1}, 1)$ Gruppe, $\sim$ eine Äquivalenzrelation auf G.

$\sim$ ist Kongruenzrelation $\Leftrightarrow (a \sim a', b \sim b' \Rightarrow (a \cdot b \sim a' \cdot b'$ und $a^{-1} \sim a'^{-1}$ und $1 \sim 1))$

Satz 1 (Homomorphiesatz)

a) Es sei $\sim$ Kongruenzrelation auf A. Dann ist die Menge der Äquivalenzklassen

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

wobei $[a]_\sim = \{a' \in A \mid a' \sim a\}$ die Äquivalenzklasse von a bezeichnet, eine Algebra von Typ T mit

$$\overline{f_i}([a_1]_\sim, \ldots, [a_{n_i}]_\sim) := [f_i(a_1, \ldots, a_{n_i})]$$

und

$$\begin{aligned} \pi = \pi_\sim : \quad A &\to A/_\sim \\ a &\mapsto [a]_\sim \end{aligned}$$

ist surjektiver Homomorphismus.

b) Ist $\varphi : A \to B$ ein Homomorphismus, so wird durch $a \sim a' \Leftrightarrow \varphi(a) = \varphi(a')$ eine Kongruenzrelation auf A definiert und

$$\text{Bild}(\varphi) = \varphi(A) := \{\varphi(a) \mid a \in A\}$$

ist Unteralgebra von B und es gibt einen Isomorphismus

$$\begin{aligned} \overline{\varphi} : \quad A/_\sim &\to \text{Bild}(\varphi) \\ [a]_\sim &\mapsto \varphi(a) \end{aligned}$$

Kennt man also alle Kongruenzrelationen auf A, so kennt man bis auf Isomorphie alle homomorphen Bilder von A.

Beweis (Nachrechnen!)
zu zeigen ist, dass die Operationen $\overline{f_i}$ wohldefiniert sind, d.h.

$$\overline{f_i}([a_1]_\sim, \ldots, [a_{n_i}]_\sim) = f_i(a_1, \ldots, a_{n_i})$$

Es kann sein, dass $[a_i] = [a_i']$, dann muß auch

$$\overline{f_i}([a_1]_\sim, \ldots, [a_{n_i}]_\sim) = f_i(a_1', \ldots, a_{n_i}')$$

gelten, weil $\sim$ eine Kongruenzrelation ist.

Beispiel 5
Seien V ein K-Vektorraum und $\varphi : V \to W$ ein Homomorphismus.

$$\begin{aligned} v \sim v' &\underset{def}{\Leftrightarrow} \varphi(v) = \varphi(v') \\ &\Leftrightarrow \varphi(v - v') = 0 \\ &\Leftrightarrow v - v' \in \mathrm{Kern}(\varphi) = U \leq V \end{aligned}$$

$$[v]_\sim = v + U$$

,

$$[\underline{0}]_\sim = U = \mathrm{Kern}(\varphi)$$

23.05.MMI

$A = (A, f_i)_{i \in I})$ Algebra vom Typ $T = (n_i)_{i \in I}$
Eine Äquivalenzrelation $\sim$ auf A heisst **Kongruenzrelation**, wenn für alle j

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

Dann wird

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

zu Algebra vom Typ T mit

$$\overline{f_i}([a_1]_\sim, \ldots, [a_{n_i}]_\sim) = [f_i(a_1, \ldots, a_{n_i})]_\sim$$

genannt **Faktoralgebra**:

$$\begin{aligned} A &\to A/_\sim \\ a &\to [a]_\sim \end{aligned}$$

surjektiver Homomorphismus von Algebren.

Beispiel 6
V K-Vektorraum und $\sim$ Kongruenzrelation

$$\begin{aligned} [0]_\sim &= U \qquad \text{Teilraum von } U \\ [a]_\sim &= a + U = \{a + u \mid u \in U\} \\ V/_\sim &=: V/_U \end{aligned}$$

§ 3 Ringe und Ideale

$R = (R, +, -, 0, \cdot, 1)$ sei Ring (mit Eins)
(Typ $= (2, 1, 0, 2, 0)$)
d.h. $(R, +, -, 0)$ abelsche Gruppe
$(R, \cdot, 1)$ Monoid und

$$\begin{aligned} (a+b)\cdot c &= a\cdot c + b\cdot c \\ (a\cdot(b+c)) &= a\cdot b + a\cdot c \end{aligned}$$

Lemma 1
In einem Ring R gelten:

a.) $a \cdot 0 = 0 \cdot a = 0$ für alle $a \in R$

b.) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ für alle $a, b \in R$

c.) $-(-a) = a$

d.) $-(a + b) = (-a) + (-b)$

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

Was gibt es in Ringen für Kongruenzrelationen auf R ?
Setze $\mathcal{I} = [0]_\sim = \{a \in R \mid a \sim 0\}$
Daraus folgt für $a, a' \in R$

$$\begin{aligned} a \sim a' \\ b \sim b' \end{aligned} \qquad \Rightarrow \begin{aligned} a+b &\sim a'+b' \\ a\cdot b &\sim a'\cdot b' \\ -a &\sim -a' \end{aligned}$$

$$\begin{aligned} a \sim a' &\Leftrightarrow a - a' \sim a' - a' = 0 \\ &\Leftrightarrow a - a' \in \mathcal{I} = [0]_\sim \end{aligned}$$

Also: Die Kongruenz $\sim$ ist vollständig beschrieben durch $\mathcal{I} = [0]_\sim$

Welche Eigenschaften hat $\mathcal{I} = [0]_\sim$?

$$\begin{aligned} u, v \in \mathcal{I} \Rightarrow \qquad & u \sim 0 \Rightarrow && u + v \sim 0 \\ & v \sim 0 && \text{also } u + v \in \mathcal{I} \\ & \text{und } -u \sim -0 = 0 && -u \in \mathcal{I} \end{aligned}$$

Ist $a \in R, u \in \mathcal{I}$, d.h. $u \sim 0, a \sim a$, also $a \cdot u \sim a \cdot 0 = 0$ und $u \cdot a \sim 0 \cdot a = 0$ also $a \cdot u \in \mathcal{I}$ und $u \cdot a \in \mathcal{I}$.

Definition 1
$\mathcal{I} \subseteq R$ (R Ring) heisst **Ideal** (Im Zeichen $\mathcal{I} \trianglelefteq R$) wenn $0 \in \mathcal{I}$ und

$$\begin{aligned} a, b \in \mathcal{I} &\Rightarrow a + b \in \mathcal{I} \text{ und } -a \in \mathcal{I} \\ a \in R, u \in \mathcal{I} &\Rightarrow a \cdot u \in \mathcal{I} \text{ und } u \cdot a \in \mathcal{I} \end{aligned}$$

Satz 1
Ist $\sim$ eine Kongruenzrelation auf R, so ist

$$\mathcal{I} = [0]_\sim \trianglelefteq R$$

Umgekehrt: Ist $\mathcal{I} \trianglelefteq R$, so wird durch

$$a \sim a' \underset{def}{\Leftrightarrow} a - a' \in \mathcal{I}$$

eine Kongruenzrelation definiert.
[Dabei $[0]_\sim = \mathcal{I}, [a] = a + \mathcal{I} = \{a + u \mid u \in \mathcal{I}\}$]
Man schreibt

$$R/_\sim = R/_\mathcal{I}$$

(Es gibt genausoviele Kongruenzrelationen, wie es Teilräume gibt.)

Beweis
1. Teil s.o.

2. Teil Sei $\mathcal{I} \subseteq R$ beliebig gegeben und $\sim$ definiert durch

$$a \sim a' \Leftrightarrow a - a' \in \mathcal{I}$$

1. Beh $\sim$ ist Äquivalenzrelation

(i) Reflexivität:
$a \sim a$ gilt, weil $a - a = 0 \in \mathcal{I}$

(ii) Symmetrie:
$a \sim b \Rightarrow b \sim a$ gilt, weil gilt:

$$a - b \in \mathcal{I} \Rightarrow -(a - b) \in \mathcal{I} = b - a \in \mathcal{I} \trianglelefteq R \qquad \text{d.h.} b \sim a$$

(iii) Transitivität:
$a \sim b$ und $b \sim c \Rightarrow a \sim c$ gilt, weil $a - b \in \mathcal{I}$ und $b - c \in \mathcal{I}$ impliziert $a - b + (b - c) \in \mathcal{I} = a - c \in \mathcal{I}$ d.h. $a \sim c$.

2. Beh $\sim$ ist sogar Kongruenzrelation

$$\begin{array}{lll} a \sim a' & \Rightarrow & a + b \sim a' + b' \quad \text{(i)} \\ b \sim b' & \text{zu zeigen} & -a \sim -a' \quad \text{(ii)} \\ & & a \cdot b \sim a' \cdot b' \quad \text{(iii)} \end{array}$$

(i)

$$\begin{array}{rcl} a - a' \in \mathcal{I} & \Rightarrow & a - a' + b - b' \in \mathcal{I} \\ b - b' \in \mathcal{I} & & a + b - (a' + b') \in \mathcal{I} \\ & & a + b \sim a' + b' \end{array}$$

(ii)

$$\begin{array}{rcl} a \sim a' \in \mathcal{I} \text{ also } a - a' \in \mathcal{I} & \Rightarrow & -(a - a') \in \mathcal{I} \\ & & -a - (-a') \in \mathcal{I} \\ & & -a \sim -a' \end{array}$$

(iii)

$$\begin{array}{lll} a - a' \in \mathcal{I} \quad \text{dann folgt} & & (a - a') \cdot b \in \mathcal{I} \\ b - b' \in \mathcal{I} & & a' \cdot (b - b') \in \mathcal{I} \\ & & \\ \text{und auch} & & (a - a')b + a'(b - b') \in \mathcal{I} \\ & & ab - a'b' \in \mathcal{I} \\ & \text{d.h.} & ab \sim a'b' \end{array}$$

Satz 2
Ist R kommutativer Ring ($a \cdot b = b \cdot a \qquad \forall a, b \in R$) und $d \in R$ beliebig, so ist

$$R \cdot d = \{a \cdot d \mid a \in R\} \trianglelefteq R$$

ein Ideal, das **von d erzeugte Hauptideal**.
Es ist $R \cdot d = R \Rightarrow d$ ist invertierbar in $(R, \cdot, 1)$ [d.h. $\exists d' \in R$ mit $d \cdot d' = 1$]

Beweis
zu zeigen:

(i) $0 \in R \cdot d$

(ii) $u, v \in R \cdot d \Rightarrow u + v \in R \cdot d$ und $-u \in R \cdot d$

(iii) $c \in R, u \in R \cdot d \Rightarrow c \cdot u \in R \cdot d$

zu (i) $0 \in R \cdot d$, weil $0 = 0 \cdot d$ (siehe Lemma 1a)

zu (ii) $u, v \in R \cdot d$ bedeutet $u = a \cdot d$ und $v = b \cdot d$ mit $a, b \in R$
dann folgt:

$$\begin{aligned} u + v &= a \cdot d + b \cdot d = \underbrace{(a + b)}_{\in R} \cdot d \in R \cdot d \\ -u &= -a \cdot d = \underbrace{(-a)}_{\in R} \cdot d \in R \cdot d \end{aligned}$$

zu (iii) $u \in R \cdot d$ und $c \in R$, d.h. $u = a \cdot d$ mit $a \in R$
dann folgt:

$$c \cdot u = c(a \cdot d) = \underbrace{(c \cdot a)}_{\in R} \cdot d \in R \cdot d$$

Wann ist $R \cdot d = R$?
Sei d invertierbar in $(R, \cdot, 1)$, d.h. es gelten $d' \in R$ und $d \cdot d' = 1$
dann gilt für $a \in R$

$$a = a \cdot 1 = a \cdot d \cdot d' = \underbrace{(a \cdot d')}_{\in R} \cdot d \in R \cdot d$$

also

$$R \subseteq R \cdot d$$

Umgekehrt sei $R = R \cdot d$
dann ist $1 \in R \cdot d$, d.h. $\exists d' \in R$ mit $1 = d \cdot d'$, d.h. d ist invertierbar.

Beispiel 1

$$\begin{array}{rcll} R & = & \mathbb{Z} & m \in \mathbb{N} \\ m\mathbb{Z} & \trianglelefteq & \mathbb{Z} & \\ \mathbb{Z}_m & = & \mathbb{Z}/_{m\mathbb{Z}} = \mathbb{Z}/_{\sim_m} & \\ & = & \{[a]_\sim \mid a \in \mathbb{Z}\} & \end{array}$$

$\sim = \sim_m$ definiert durch:

$$a \sim b \Leftrightarrow a - b \in m\mathbb{Z}$$

$$[a]_\sim = [a]_m = a + m\mathbb{Z} = \{a + m \cdot z \mid z \in \mathbb{Z}\}$$

$$\begin{array}{rcl} \mathbb{Z} & \to & \mathbb{Z}_m \\ a & \mapsto & [a]_m \end{array}$$

ist surjektiver Ringhomomorphismus

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

dann ist $a \in \mathbb{Z}$ beliebig $\underbrace{\lfloor \frac{a}{m} \rfloor}_{= \text{grösste ganze Zahl} \leq \frac{a}{m}}$ (untere Gaussklammer).

$$i = a - \lfloor \frac{a}{m} \rfloor m \in \{0, 1, \ldots, m-1\}$$

dann ist

$$[a]_m = [i]$$

Bemerkung
statt

$$a \sim_m b \text{ für } a, b \in \mathbb{Z}$$

schreibt man oft

$$\Leftrightarrow a \equiv b \bmod m$$
$$\Leftrightarrow [a]_m = [b]_m \text{ in } \mathbb{Z}$$

Beispiel 2

$$R = \mathbb{Z} \qquad m = 3$$

$$\begin{aligned} [0]_m &= \{0, 3, -3, 6, -6, \ldots\} \\ [1]_m &= \{1, 4, -2, 7, -5, \ldots\} \\ [2]_m &= \{2, 5, -1, 8, -4, \ldots\} \\ \mathbb{Z}_3 = \mathbb{Z}/_{3\mathbb{Z}} &= \{\underset{=0}{[0]_3}, \underset{=1}{[1]_3}, \underset{=1+1}{[2]_3}\} \end{aligned}$$

Konvention
In jedem kommutativen Ring R schreibt man

$$1 + 1 = 2, 1 + 1 + 1 = 3, \ldots$$

allgemein:

$$a \in R, \qquad \underbrace{a + \ldots + a}_{r-mal} =: r \cdot a \text{ in } R$$

z.B. $2 + 2 = 1$ in $\mathbb{Z}_3$
genauer $[2]_3 + [2]_3 = [1]_3$

Beispiel 3
keine ganze Zahl der Form $7 + n \cdot 8$ ist eine Summe von 3 Quadratzahlen in $\mathbb{Z}$ (für $n \in \mathbb{Z}$)

Beweis
Annahme:

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

Betrachte

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}_8 = \mathbb{Z}/_{8\mathbb{Z}} \\ z &\mapsto [z]_8 \end{aligned}$$

ist Homomorpismus.
Dann folgt

$$\begin{aligned} \varphi(z) &= \varphi(a^2) + \varphi(b^2) + \varphi(c^2) \\ [z]_8 &= \varphi(a)^2 + \varphi(b)^2 + \varphi(c)^2 \\ &= a'^2 + b'^2 + c'^2 \qquad a', b', c' \in \mathbb{Z}_8 \end{aligned}$$

in $\mathbb{Z}_8$ gilt:

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

Quadrate in $\mathbb{Z}_8$ sind $0, 1, 4$.
Summe von 3 Quadraten sind:

$$\begin{aligned} 0 &= 0^2 + 0^2 + 0^2 \\ 1 &= 1^2 + 0^2 + 0^2 \\ 2 &= 1^2 + 1^2 + 0^2 \\ 3 &= 1^2 + 1^2 + 1^2 \\ 4 &= 2^2 + 0^2 + 0^2 \\ 5 &= 2^2 + 1^2 + 0^2 \\ 6 &= 2^2 + 1^2 + 1^2 \end{aligned}$$

7 ist in $\mathbb{Z}_8$ keine Summe von 3 Quadraten.
Also ist die Annahme falsch.

Beispiel 4
Pseudozufallszahlen

Gesucht sind Zufallszahlen in $\{0, 1, \ldots, m-1\}$ für ein $m \in \mathbb{N}$.

25.05.MMI

$$\mathbb{Z}_m = \mathbb{Z}/_{m\mathbb{Z}} = \{[a]_m \mid a \in \mathbb{Z}\}$$
$$[a]_m = \{n + mz \mid z \in \mathbb{Z}\} = a + m\mathbb{Z}$$
$$[a]_m = [b]_m \Leftrightarrow b - a \in m\mathbb{Z}$$
$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$
$$[a]_m \overset{+}{\cdot} [b]_m = [a \overset{+}{\cdot} b]_m$$

Konvention $1 = [1]_m$
$k = \underbrace{1 + 1 + \ldots + 1}_{\text{k-mal}} = [k]_m$ in $\mathbb{Z}_m$

Beispiel 5
Pseudozufallszahlen
$n \in \mathbb{N}$ $\{0, 1, \ldots, m-1\}$ $\mathbb{Z}_m$

$$\begin{aligned} z_0 &= 0 \qquad \text{Startwert [Datum } \cdot \text{ Uhrzeit]} \\ z_n &= a \cdot z_{n-1} + c \qquad \text{in } \mathbb{Z}_m \qquad n \geq 1 \end{aligned}$$

Eigentlich $[z_n]_m = [a]_m[z_{n-1}]_m + [c]_m$ mit geeigneten a und c in $\mathbb{Z}_m$.
Jede solche Folge $(z_n)_{n\in\mathbb{N}_0}$ wird periodisch werden

$$\begin{aligned} z_j &= z_{j+k} \Rightarrow \\ z_{j+1} &= z_{j+k+1} \end{aligned}$$

Bestimme a, c so daß Periode $k = m$ ist, aber bitte nicht $a = c = 1$

$$\begin{aligned} F &= \sum_{n=0}^{\infty} z_n x^n = z_0 + \sum_{n=1}^{\infty} (a \cdot z_{n-1} + c) x^n \in \mathbb{Z}_m[\![x]\!] \\ &= a \cdot x \cdot F + c \cdot \frac{x}{1-x} \qquad [z_0 = 0] \\ F &= c \cdot \frac{x}{1-x} \cdot \frac{1}{1-ax} = c \cdot \frac{x}{1-x} \cdot \sum_{n=0}^{\infty} a^n x^n \\ &= c \sum_{n=1}^{\infty} (1 + a + a^2 + \ldots + a^{n-1}) x^n \end{aligned}$$

Also $z_n = c(1 + a + \ldots + a^{n-1})$ für $n \geq$ in $\mathbb{Z}_m a$ und c so zu bestimmen , daß Periode m

$$\begin{aligned} \mathbb{Z}_m &= \{z_0, z_1, \ldots, z_{m-1}\} \qquad z_m = z_0 \\ \text{Also:} \qquad &= \{\underbrace{c(1 + a + \ldots + a^{n-1})}_{=1 \text{ für ein n}} \mid n = 1, \ldots, m\} \end{aligned}$$

Also muß c in $\mathbb{Z}_m$ invertierbar ["$ggT(c, m) = 1$ in $\mathbb{Z}$"] $a^m = 1$ in $\mathbb{Z}_m$
(Fortsetzung folgt [§8 Beispiel 7])

§ 4 Größter gemeinsamer Teiler, Euklidische Ringe

Bemerkung
Ist $m \in \mathbb{N}$ keine Primzahl, so ist

$$m = p \cdot q \qquad \text{mit } 1 < p, q < m$$

dann ist

$$[p]_m \cdot [q]_m = [p \cdot q]_m = [m]_m = 0 \text{ in } \mathbb{Z}_m$$

aber $[p]_m \neq 0$ und $[q]_m \neq 0$ weil $1 < p, q < m$

Definition 1
Ist R ein kommutativer Ring und ist $a \neq 0 \neq b$ aber $a \cdot b = 0$, so heißen a, b **Nullteiler**.
R heißt **Integritätsbereich**, wenn R ein kommutativer Ring (mit 1) und R keine Nullteiler enthält. [Insbesondere gilt dann: $a \cdot b = 0 \Longrightarrow a = 0$ oder $b = 0$]

Beispiel 1
$\mathbb{Z}, K[x], K[\![x]\!], \mathbb{Z}[x], K$ Körper , ... sind Integritätsbereiche
kein Integritätsbereich ist $\mathbb{Z}_4, \mathbb{Z}_m$ für m ist keine Primzahl.

Definition 2
$a, b \in R \qquad a \mid b \Leftrightarrow \exists z \in R$ mit $b = a \cdot z \qquad$ (lies: "a teilt b")
$d \in R$ heißt ein **größter gemeinsamer Teiler** von a und b "in Zeichen $d \in ggT(a, b)$", wenn $d \mid a$ und $d \mid b$ und zusätzlich gilt aus $c \mid a$ und $c \mid b$ folgt $c \mid d$.

Bemerkung
Ist u in $(R, \cdot, 1)$ invertierbar "u ist **Einheit** in R" so gilt $u \mid a$ für alle $a \in R$ denn $a = u \cdot (u^{-1} \cdot a)$

Beispiel 2
In $\mathbb{Z}$ sind nur 1 und -1 Einheiten
$ggT(4, 6) \ni -2, 2$

Bemerkung
$d \in ggT(a, b)$ in R und u Einheit in $R \Rightarrow u \cdot d \in ggT(a, b)$ umgekehrt, sind d und $d' \in ggT(a, b)$ so gilt:

$$\begin{array}{lll} & d' \mid d & \text{weil } d \in ggT(a,b) \\ \text{und} & d \mid d' & \text{weil } d' \in ggT(a,b) \end{array}$$

$$\begin{array}{llllll} \text{d.h.} & \exists v & \in & R & d' = dv & \\ & \exists v' & \in & R & d = d'v' & \end{array}$$

$$\begin{array}{rcll} d' & = & d(v' \cdot v) & \text{also} \\ d'(1 - v'v) & = & 0 & \end{array}$$

Also, da R Integritätsbereich, folgt $d' = 0$ und dann auch $d = 0$ oder $(1 - v'v) = 0$ d.h. $v'v = 1$ und v, v' sind Einheiten in R.
Also $d, d' \in ggT(a, b) \Rightarrow d' = u \cdot d$ für eine Einheit $u \in R$.
Also $ggT's$ sind nur bis auf eine Einheit (d.h. Multiplikation mit einer Einheit) in R bestimmt.

Wie findet man $ggT(a,b)$? [Nicht in jedem Integritätsbereich gibt es $ggT(a,b)$ für alle a,b] In $\mathbb{Z}$ oder $K[x]$ findet man $ggT(a,b)$ mit dem Euklidischen Algorithmus.

Definition 3
Ein Integritätsbereich R zusammen mit δ heißt ein **[Norm-] Euklidischer Ring** wenn:

$$\begin{aligned} \delta : R \setminus \{0\} &\to \mathbb{N}_0 \\ [\delta : R &\to \mathbb{N}_0 \qquad \text{mit } \delta(0)=0 \text{ und } \delta(ab)=\delta(a)\cdot\delta(b)] \qquad (*) \end{aligned}$$

mit folgenden Eigenschaften. In $a,b \in R$ mit $b \neq 0$ existiert stets ein $q \in R$ und $r \in R$ mit

$$a = q \cdot b + r \text{ wobei } r = 0 \text{ oder } \delta(r) < \delta(b)$$

Beispiel 3
$(\mathbb{Z}, ||)$ ist (Norm-) euklidisch wobei:

$$\mid a \mid = \begin{cases} a & : \quad a \geq 0 \\ -a & : \quad a < 0 \end{cases}$$

$$(*)\delta(a) = 0 \Leftrightarrow a = 0$$

Beispiel 4
$R = (K[x], \text{Grad})$ ist euklidischer Ring

$$\mathbb{Q}[x] = x^5 + x^3 + 1 = (2x^3 + 2x)\underbrace{(\frac{1}{2}x^2)}_{q} + \underbrace{1}_{r}$$

$R = (K[x], \delta)$ ist Normeuklidisch

$$\delta(f) = \begin{cases} 2^{\text{Grad } f} & : \quad f \neq 0 \\ 0 & : \quad f = 0 \end{cases}$$

Satz 1
Ist (R, δ) euklidischer Ring, so gibt es zu $a,b \in R$ stets ein $d \in ggT(a,b)$ und es gibt $y,z \in R$ mit:

$$d = a \cdot y + b \cdot z$$

30.05.MMI

Beweis (Euklidischer Algorithmus)
Ist $b = 0$, so setze $d = a$ und z.B. $y = 1, z = 0$.

Ist umgekehrt $b \neq 0$ existieren $q_1, r_1 \in R$ mit

$$\begin{array}{lll} a = b \cdot q_1 + r_1 & \text{mit } [\ r_1 = 0 \text{ oder }] & \delta(r_1) < \delta(b) \\ b = q_2 \cdot r_1 + r_2 & \text{mit } [\ r_2 = 0 \text{ oder }] & \delta(r_2) < \delta(r_1) \\ r_1 = q_3 \cdot r_2 + r_3 & \text{mit } [\ r_3 = 0 \text{ oder }] & \delta(r_3) < \delta(r_2) \end{array}$$

...

nach endlich vielen, [spätestens $\delta(b) + 1$] Schritten wegen $\delta(b) > \delta(r_1) > \ldots > \delta(r_n) \geq 0$

$r_{n-2} = q_n \cdot r_{n-1} + r_n \quad \text{mit} \quad \delta(r_n) < \delta(r_{n-1})$

$r_{n-1} = q_{n+1} \cdot r_n$

setze $b = q_0$ und $a = r_{-1}$

Behauptung: $\exists y_j, z_j$ mit

$$r_n = y_j r_{n-j-1} + z_j r_{n-j} \text{ für } j = 1, 2, \ldots, n$$

denn für $j = 1$ setzen wir $y_1 = 1$ und $z_1 = -q_n$.

Schritt von j auf $j + 1$:

$$r_{n-j-2} = q_{n-j} r_{n-j-1} + r_{n-j}$$

$$y_{j+1} = z_j \qquad z_{j+1} = y_j - q_{n-j} z_j$$

Dass $r_n \in ggT(a, b)$ ist [da $y = y_n, z = z_n$] folgt aus $ggT(a.b) = ggT(b, a - qb)$.

Lemma 1

$$ggT(a, b) = ggT(b, a - qb)$$

Beweis
Zeige

$$d \mid a, b \longrightarrow d \mid b, a - qb$$

denn: $a = d \cdot a_1$, $b = d \cdot b_1$ mit $a_1, b_1 \in R \Rightarrow b = db_1, a - qb = da_1 - qdb_1 = d(a_1 - qb_1)$, d.h. $d \mid b, a - qb$.

Satz 2
Ist (R, δ) euklidischer Ring und $a, b \in R$, dann

$$[b]_a = b + a \cdot R = R/_{aR}$$

genau dann invertierbar (oder auch eine „Einheit“) wenn

$$1 \in ggT(a, b)$$

Beweis

a) angenommen $1 \in ggT(a, b)$. Nach Satz 1 gibt es $y, z \in R$ mit

$$1 = y \cdot a + z \cdot b$$

$$z \cdot b - 1 = (-y) \cdot a \in Ra$$

$$[z]_a \cdot [b]_a = [zb]_a = [1]_a = 1 \text{ (Einselement von } R/_{Ra} \text{)}$$

$$\text{d.h.} [b]_a^{-1} = [z]_a$$

b) Sei $[b]_a$ invertierbar in $R/_{Ra}$, d.h. $\exists z \in R$ mit $[b]_a^{-1} = [z]_a$
also gilt $[b]_a[z]_a = 1$ und für ein $y \in R$:

$$b \cdot z - 1 = y \cdot a$$

$$bz - ya = 1$$

Gelte $d|a, b$, dann folgt

$$d|bz - ya, \text{ also } d \mid 1$$

Also ist d Einheit in R, also gilt $1 \in ggT(a, b)$.

Folgerung 1
Ist $m \in \mathbb{N}$ so ist $[c]_m$ in $\mathbb{Z}_m = \mathbb{Z}/_{mZ}$ invertierbar genau dann, wenn $1 \in ggT(c, m)$.

Ist R ein kommutativer Ring, so wird die Menge der Einheiten in R mit R^* bezeichnet.

$$R^* = \{a \in R \mid \exists a^{-1} \in R \text{ mit } a \cdot a^{-1} = 1\}$$

Beispiel 5

$$\begin{aligned}
\mathbb{Z}_6 &= \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\} \\
\mathbb{Z}_6^* &= \{[1]_6, [5]_6\} \\
\mathbb{Z}_8 &= \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [8]_8, [7]_8\} \\
\mathbb{Z}_8^* &= \{[1]_8, [3]_8, [5]_8, [7]_8\}
\end{aligned}$$

Definition 4

$$|\mathbb{Z}_m^*| = \varphi(m) \qquad \text{für } m \in \mathbb{N}$$

φ heißt Eulersche φ-Funktion.

$\varphi(m)$ gibt die Anzahl der zu m teilerfremden Zahlen in $\{1, \ldots, m-1\}$ an.

z.B.

$$\varphi(6) = 2$$

$$\varphi(8) = 4$$

Folgerung 2
$\mathbb{Z}_m = \mathbb{Z}/_{m\mathbb{Z}}$ ist für $m \in \mathbb{N}$ genau dann ein Körper, wenn m eine Primzahl ist.

Beweis:

$\mathbb{Z}_1 = \mathbb{Z}/_{1\mathbb{Z}} = \{[0]_1\} = \{0\}$ ist kein Körper.

Ist $m > 1$ keine Primzahl, so gilt $m = a \cdot b$ mit $1 < a, b < m$, was bedeutet, daß $[a]_m \cdot [b]_m = [m]_m = [0]_m = 0$ ist, obwohl $[a]_m \neq 0$ und $[b]_m \neq 0$.

Also ist $\mathbb{Z}/_{m\mathbb{Z}}$ kein Integritätsbereich (es gibt Nullteiler), also kein Körper.

Ist umgekehrt m eine Primzahl, so ist für jedes Element $a \in \mathbb{N}$ mit $1 \leq a < m$

$$1 \in ggT(a, m)$$

also nach Folgerung 1 (Satz 2) ist $[a]_m$ invertierbar. Also hat jedes $[a]_m \neq 0$ in $\mathbb{Z}_m$ ein Inverses.

Satz 3
Ist (R, δ) ein euklidischer Ring und ist $I \trianglelefteq R$, so gibt es ein $a \in R$ mit $I = R \cdot a$. D.h. in einem euklidischen Ring gibt es nur Hauptideale. Er wird auch als Hauptidealring bezeichnet.

Beweis:

Ist $I = \{0\}$ das Nullideal, so ist $I = R \cdot 0$.

Es sei nun $I \neq \{0\}$ ein Ideal in R und

$$m = \min\{\delta(y) \mid y \in I \setminus \{0\}\} \subseteq \mathbb{N}_0$$

und es sei $m = \delta(a)$ für ein $a \in I \setminus \{0\}$.

Behauptung: $I = R \cdot a$

Beweis:

$\supseteq$ Da $a \in I$ gilt $y \cdot a \in I$ für jedes $y \in R$, also $R \cdot a \subseteq I$.

$\subseteq$ Sei $b \in I$ beliebig, da $a \neq 0$ existieren $q, r \in R$ mit

$$b = q \cdot a + r \qquad \text{mit } r = 0 \text{ oder } \delta(r) < \delta(a)$$

$$r = \overbrace{b}^{\in I} - \underbrace{q \cdot \overbrace{a}^{\in I}}_{\in I} \in I$$

$\delta(r) < \delta(a)$ ist unmöglich, weil

$$\delta(a) = \min\{\delta(y) \mid y \in I \setminus \{0\}\}$$

Also folgt $r = 0$, d.h. $b \in Ra$, also $I \subseteq Ra$.

Folgerung 3
Jedes Ideal von $\mathbb{Z}$ ist von der Form $I = \mathbb{Z}m$ mit $m \in \mathbb{N}_0$. Jedes homomorphe Bild von $\mathbb{Z}$ ist isomorph zu $\mathbb{Z}_m = \mathbb{Z}/_{m\mathbb{Z}}$ für $m \in \mathbb{Z}$ oder $\mathbb{Z}(\cong \mathbb{Z}_0 = \mathbb{Z}/_{0\mathbb{Z}})$.

§ 5 Eindeutige Primfaktorzerlegung

R sei ein Integritätsbereich (kommutativer Ring ohne Nullteiler, d.h. $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$), dann definiert man

01.06.MMI

Definition 1

$$p \in R \textbf{ irreduzibel } \Leftrightarrow p \neq 0, p \notin R^* \text{ und } p = a \cdot b \Rightarrow a \in R^* \text{ oder } b \in R^*$$

Lemma 1
(R, δ) euklidischer Ring, p irreduzibel $\Rightarrow p|a \cdot b \Rightarrow p|a$ oder $p|b$

Beweis
Angenommen $p|ab$, dann:
Ist p kein Teiler von a, so ist $1 \in ggT(p, a)$ und es gibt deshalb $y, z \in R$ mit $1 = yp + za$. Multipliziert man dies mit b, so erhält man:

$$b = ypb + zab.$$

Da p sowohl ab als auch ybp teilt, muß es auch b teilen.

Satz 1
Ist (R, δ) ein Normeuklidischer Ring, dann hat jedes $a \in R\backslash\{0\}$ eine Darstellung der Form:

$$a = u \cdot p_1 \dots p_r \qquad \text{mit } u \in R^*, p_i \text{ irred.}$$

Gilt auch

$$a = v \cdot q_1 \dots q_s \qquad \text{mit } v \in R^*, q_i \text{ irred.}$$

so gilt $r = s$ und es gibt Permutation $\sigma \in S_r$ mit $q_i = u_i p_{\sigma(i)}$ mit $u_i \in R^*$.

Beweis

a) Existenz:
Induktion nach $\delta(a)$
$\delta(a) = 1 \Rightarrow a \in R^*$

$[1 = qa + r$ mit $\delta(u) < \delta(a) = 1$
$\delta(r) = 0 \Leftrightarrow r = 0 \qquad (\delta \text{ Norm }) \qquad q = a^{-1} \qquad a \in R^*]$

$\delta(a) > 1$:
Ist a irreduzibel, so $a = 1 \cdot a$. Sonst $a = b \cdot c$ und $b, c \notin R^*$ $\delta(a) = \delta(b) \cdot \delta(c)$ und

$\delta(b), \delta(c) > 1$ und $< \delta(a)$
Nach Induktionsannahme:

$$\begin{aligned} b &= u \cdot p_1 \dots p_l \qquad u \in R^*, p_i \text{ irred.} \\ c &= u' \cdot p_{l+1} \dots p_r \qquad u' \in R^*, p_i \text{ irred.} \\ a &= b \cdot c = \underbrace{u \cdot u'}_{\in R^*} \cdot p_1 \dots p_r \end{aligned}$$

b) Eindeutigkeit:

$$\begin{aligned} a &= u \cdot p_1 \dots p_r \qquad p_i, q_j \text{ irred.} \\ &= v \cdot q_1 \dots q_s \qquad u, v \in R^* \end{aligned}$$

Induktion nach $Min(r, s) = r$:
$r = 0$, dann $a \in R^*, s = 0$ und $u = v = a$
$r > 0$, $p_r | a = v q_1 \dots q_s$
Nach Lemma 1 (mehrfach angewandt) gibt es j mit $p_r | q_j$
oBdA $j = s$
$q_s = u_r p_r$ dabei $u_r \in R^*$

$$0 = a - a = p_r \underbrace{(u p_1 \dots p_{r-1} - (v u_r) q_1 \dots q_{s-1})}_{=0}$$

Nach Induktionsannahme $r - 1 = s - 1$ und bei passender Sortierung ist $q_i = u_i p_i$ mit $u_i \in R^*$.

Korrollar

a) In $\mathbb{Z}$ hat jedes $a \in \mathbb{Z} \backslash \{0\}$ ein eindeutige Darstellung (bis auf Reihenfolge der Faktoren) in der Form

$$a = u p_1 \dots p_r \qquad p_i \text{ Primzahl }, u \in \{-1, 1\}$$

b) Ist K Körper, so hat jedes $f \in K[x] \backslash \{0\}$ eine (bis auf Reihenfolge) eindeutige Darstellung in der Form

$$f = u f_1 \dots f_r \qquad \text{mit } u \in K^* \text{ und } f_i \text{ irred. und normiert}$$

Definition 2
$f = \sum_{i=0}^{n} a_i x^i$ heisst **normiert** (engl. **monic**) wenn $a_n = 1$.

Satz 2
Es sei (R, δ) euklidischer Ring und $0 \neq f \in R$
so ist

$$R/_{f \cdot R} = \{[g]_f \mid g \in R, \delta(g) < \delta(f)\} \cup \{\underline{0}\}$$

wobei

$$[g]_f = g + fR (= \{g + f \cdot z \mid z \in R\})$$

Es ist $R/_{f \cdot R}$ Körper $\Leftrightarrow$ f irreduzibel.

Beweis

a)

$$[g_1]_f = [g_2]_f \Leftrightarrow g_1 - g_2 \in fR$$

Da (R, δ) euklidischer Ring und $f \neq 0$, gibt es zu jedem beliebigen $g \in R$ stets ein $q, r \in R$ mit

$$\begin{aligned} g &= q \cdot f + r \qquad \text{wobei } r = 0 \text{ oder } \delta(r) < \delta(f) \\ g - r &= q \cdot f \qquad \in fR \\ [g]_f &= [r]_f \end{aligned}$$

Nach Definition ist

$$\begin{aligned} R/_{fR} &= \{[g]_f \mid g \in R\} \\ &= \{[g]_f \mid g \in R, \delta(g) < \delta(f)\} \cup \{0\} \end{aligned}$$

b) Ist f irreduzibel. Beh: $R/_{fR}$ ist Körper

(i) Sei $0 \neq [g]_f$ aus $R/_{fR}$.
Zu zeigen: $[g]_f$ hat Inverses.
$f \not| g \qquad 1 \in ggT(f, g)$, weil f irreduzibel ist.
Es gibt $y, z \in R$ mit $1 = y \cdot f + z \cdot g$ mit $y, z \in R$

$$1 = [1]_f = \underbrace{[y \cdot f]_f}_{=0} + [z]_f \cdot [g]_f$$

Also ist $[g]_f$ invertierbar: $[g]_f^{-1} = [z]_f$.
Also ist $R/_{fR}$ Körper.

(ii) Es sei f nicht irreduzibel
$f = a \cdot b$ mit $a, b \notin R^*$
$0 = [f]_f = [a \cdot b]_f = [a]_f \cdot [b]_f$
Wäre $[a]_f = 0$, so wäre $f | a = f \cdot a_1 \qquad a_1 \in R$
$f = a \cdot b = f \underbrace{a_1 \cdot b}_{\Rightarrow b \in R^*}$ Widerspruch $\lightning$
Also $[a]_f = 0$ und $[b]_f = 0$
also ist $R/_{fR}$ kein Integritätsbereich und damit erst recht kein Körper.
Schliesslich: Ist $f \in R^*$, so ist $R/_{fR} = R/_R = \{0\}$ und $R/_{fR}$ kein Körper.

Beispiel 1

$$R = \mathbb{Z}_2[x] \qquad \mathbb{Z}_2 = \{0,1\} \cong \mathbb{Z}/_{2\mathbb{Z}}$$
$$f = x^2 + x + 1 \qquad \in R \qquad \delta(g) = \text{ Grad}g$$
$$R/_{fR} = \{[g]_f \mid g \in R, \text{ Grad } g < 2\} \cup \{0\}$$

	$-\infty$	0
Polynome vom Grad	0 in $\mathbb{Z}_2[x]$	1
	1 in $\mathbb{Z}_2[x]$	x, $x+1$

$|R/_{fR}| = 4$

$$R/_{fR} = \{[0],[1],[x],[x+1]\}$$

$\cdot$	0	1	$[x]$	$[x+1]$
0	0	0	0	0
1		1	$[x]$	$[x+1]$
$[x]$			$[x+1]$	1
$[x+1]$				$[x]$

$[x][x] = [x^2] = [x+1]$
NR: $x^2 = \underbrace{(x^2+x+1)}_{f} \cdot \underbrace{1}_{q} + \underbrace{x+1}_{r}$

$[x][x+1] = [x^2+x] = [1]$
NR: $x^2 + x = \underbrace{(x^2+x+1)}_{f} \cdot \underbrace{1}_{q} + 1$

$[x+1][x+1] = [x^2+1] = [x]$
$[x+1] = [x]^{-1}$

Also $\mathbb{Z}_2[x]/(x^2+x+1)\mathbb{Z}_2[x]$ ist Körper mit 4 Elementen

Beispiel 2
$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{[0]_4,[1]_4,[2]_4,[3]_4\}$ ist ein Ring mit 4 Elementen kein Körper!

$$[2]_4[2]_4 = [4]_4 = 0$$
$$[3]_4[3]_4 = [9]_4 = 1$$

NR $9 = 4*2+1 \Rightarrow [9]_4 = [1]_4$

13.06.MMI

(R,S) sei euklidischer Ring z.B. $(\mathbb{Z},|\quad|)$ $(K[x],\text{Grad})$ K Körper.

- Division mit Rest

- euklidischer Algorithmus zu $a,b \in R$ gibt es $d \in ggT(a,b) \quad d = ya + zb$ mit $y,z \in R$

Folgerung 1
R/qR ist Körper $\Leftrightarrow$ q irreduzibel in R

$$\begin{array}{lcll} q \in R \text{ irreduzibel} & \Leftrightarrow & q & \neq & 0 \\ & & q & \notin & R^* \\ & & q & = & a \cdot b \Rightarrow a \in R^* \text{ oder } b \in R^* \end{array}$$

Beispiel 3
$\mathbb{Z}/p\mathbb{Z}$ Körper $\Leftrightarrow$ p Primzahl $p \in \mathbb{N}$

$$\begin{array}{rcl} \mathbb{Z}_p & = & \mathbb{Z}/p\mathbb{Z} \text{ ist Körper mit } p \text{ Elementen falls } p \text{ Primzahl} \\ \mathbb{Z}_{p^2} & = & \mathbb{Z}/p^2\mathbb{Z} \text{ ist Ring mit } p^2\text{-Elementen aber kein Körper} \end{array}$$

Beispiel 4
$R = K[x]$ K Körper $R/fR = \{[g]_f \mid q \in K[x]\}$

$$\begin{array}{rcl} [g]_f & = & g + fK[x] \\ [g]_f & = & [h]_f \Leftrightarrow g - h \in fK[x] = q \cdot f \text{ mit } q \in K[x] \end{array}$$

$R/fR = K[x]/fK[x] = \{[\sum_{i=0}^{n-1} a_i x^i]_f \mid a_i \in K\}$ falls Grad $f = n \geq 1$

Bemerkung
Ist $K = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ [Körper mit p Elementen p Primzahl] und ist $f \in K[x]$ und Grad $f = n \geq 1$. Dann ist:

$$\begin{array}{rcl} \mid K[x]/fK[x] \mid & = & p^n \\ K[x]/fK[x] & = & \{[a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}]_f \mid a_i \in \mathbb{Z}_p\} \end{array}$$

und $K[x]/fK[x]$ Körper $\Leftrightarrow$ f ist irreduzibel.

Beispiel 5
$K = \mathbb{Z}_2$ $\underbrace{f = x^3 + x + 1 \in K[x]}_{\text{irreduzibel}}$

$$\begin{array}{rcl} L & = & K[x]/fK[x] \text{ ist ein Körper mit 8 Elementen} \\ & = & \{[a_0 + a_1 x + a_2 x^2]_f \mid a_0, a_1, a_2 \in \mathbb{Z}_2\} \end{array}$$

Die Element von L werden durch 3 Bits dargestellt.

$$[a_0 + a_1 x + a_2 x^2]_f \rightarrow a_0 a_1 a_2$$

$$\begin{array}{rcll} \alpha & = & [x]_f & \leftrightarrow 010 \\ \alpha^2 & = & [x^2]_f & \leftrightarrow 001 \\ \alpha^3 & = & [x^3]_f = [x+1]_f & \leftrightarrow 110 \quad \text{NR: } x^3 = (x^3 + x + 1) + x + 1 \\ \alpha^4 & = & [x^3 \cdot x]_f = [x^2 + x]_f & \leftrightarrow 011 \\ \alpha^5 & = & [x^4 \cdot x]_f = [x^3 + x^2]_f = [x^2 + x + 1]_f & \leftrightarrow 111 \quad \text{NR: } x^3 + x^2 = (x^3 + x + 1) + x^2 + x + 1 \\ \alpha^6 & = & [x^3 + x^2 + x]_f = [x^2 + 1]_f & \leftrightarrow 101 \\ \alpha^7 & = & [x^3 + x]_f = [1]_f & \leftrightarrow 100 \\ \alpha^8 & = & \alpha & \end{array}$$

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

$$\alpha^3 \cdot \alpha^2 = \alpha^5$$

$$\alpha^3 \cdot \alpha^5 = \alpha^8 = \alpha^7 \cdot \alpha = \alpha$$

$$\alpha^3 + \alpha^5 = \alpha^3(1 + \alpha^2) = [x^2]_f = \alpha^2$$

§ 6 Der chinesische Restsatz

$R_1, \ldots, R_r$ seien Ringe; dann wird $R = R_1 \times \ldots \times R_r = \{(a_1, \ldots a_r) \mid a_i \in R_i\}$ zu einem Ring $R = (R, +, -, 0, \cdot, 1)$ mit:

$$\begin{aligned}(a_1, \ldots, a_r) \dot{+} (b_1, \ldots, b_r) &= (a_1 \dot{+} b_1, \ldots, a_r \dot{+} b_r)\\ -(a_1, \ldots, a_r) &= (-a_1, \ldots, -a_r)\\ 0 &= (0, \ldots, 0)\\ 1 &= (1, \ldots, 1)\end{aligned}$$

Lemma 1
Ist R euklidischer Ring und sind $q_1, q_2 \in R$ mit $1 \in ggT(q_1, q_2)$ [d.h. q_1, q_2 sind teilerfremd], so gilt $q_1|a$ und $q_2|q \Longrightarrow q_1 \cdot q_2|a$

Beweis

$$\begin{aligned}1 &= yq_1 + zq_2 \quad y, z \in R\\ a &= ayq_1 + azq_2\end{aligned}$$

Nach Voraussetzung ist $a = q_1a_1$ und $a = q_2a_2$

$$\begin{aligned}a &= ya_2q_1q_2 + za_1q_1q_2\\ &= q_1q_2 \cdot (ya_2 + za_1)\end{aligned}$$

Bemerkung
$4|12$ und $6|12$ in $\mathbb{Z}$, aber $4 \cdot 6 \not| 12$

Satz 1
Ist R euklidischer Ring und sind $q_1, \ldots, q_r \in R$ paarweise teilerfremd, d.h. $1 \in ggT(q_i, q_j)$ für $i \neq j$.
Dann gilt für $m = q_1 \cdot \ldots \cdot q_r$

$$R/mR \cong R/q_1R \times \ldots \times R/q_rR$$

$$\psi: \quad [a]_m \to ([a]_{q_1}, \ldots, [a]_{q_r})$$

[dabei ist $[a]_m = a + mR$ und $[a]_{q_i} = a + q_iR$]

Beweis

$$\begin{aligned} \hat{\psi} : R &\to R/q_1R \times \ldots \times R/q_rR \\ a &\to ([a]_{q_1}, \ldots, [a]_{q_r}) \qquad \text{ist Isomorphismus} \end{aligned}$$

ist offenbar ein Ringhomomorphismus mit $Kern$:

$$\begin{aligned} Kern\hat{\psi} &= \{a \in R \mid \hat{\psi}(a) = o\} \\ &= \{a \in R \mid [a]_{q_1} = 0, \ldots, [a]_{q_r} = 0\} \\ &= \{a \in R \mid q_1 \mid a, \ldots, q_r \mid a\} \\ &= \{a \in R \mid m = q_1 \ldots q_r \mid a\} \qquad \text{mehrfache Anwendung von Lemma1} \\ &= mR \end{aligned}$$

Nach Homomorphiesatz aus §1

$$\begin{aligned} \psi : \quad R/mR &\cong \text{Bild}\hat{\psi} \\ [a]_m &\to \hat{\psi}(a) = ([a]_{q_1}, \ldots, [a]_{q_r}) \end{aligned}$$

zu zeigen:

$$Bild\psi = R/q_iR \times \ldots R/q_rR$$

Beweis
Wir finden Umkehrabbildung

$$\eta : R/q_1R \times \ldots \times R/q_rR \to R/mR$$

mit $\psi \circ \eta = id_{\to R}$
dazu setzte $q_i' = \frac{m}{q_i} = q_1 \ldots q_{i-1}q_{i+1} \ldots q_r$

$$\begin{aligned} 1 &\in ggt(q_i, q_i') \qquad \text{weil } q_1, \ldots, q_r \text{ paarweise teilerfremd} \\ 1 &= y_iq_i + z_iq_i' \\ [1]_{q_i} &= [z_iq_i']_{q_i} \end{aligned}$$

definiere $\eta([a_1]_{q_1}, \ldots, [a_r]_{q_r}) = [\sum_{i=1}^r a_iq_i'z_i]_m \qquad a_i \in R$ Dann gilt:

$$\begin{aligned} \psi\eta([a_1]_{q_1}, \ldots, [a_r]_{q_r}) &= \psi[\sum_{i=1}^r a_iz_iq_i']_m \\ &= \sum_{i=1}^r (\underbrace{[a_iz_iq_i']_{q_1}}_{=0 \text{ für } i\neq 1}, \ldots, \underbrace{[a_iz_iq_i']_{q_r}}_{=0 \text{ für } i\neq r}) \\ &= ([a_1z_1q_1']_{q_1}, \ldots, [a_rz_rq_r']_{q_r}) \\ &= ([a_1]_{q_1}, \ldots, [a_r]_{q_r}) \end{aligned}$$

also $\psi\eta = id$ und psi ist surjektiv.

15.06.MMI

Beispiel 1
Seien $R = \mathbb{Z}, m = 60 = 3 \cdot 4 \cdot 5$. Dann sind

$$\begin{aligned} q_1 = 3 \quad & q_1' = 20, \text{ weil } 3 \cdot 20 = 60 \\ q_2 = 4 \quad & q_2' = 15, \text{ weil } 4 \cdot 15 = 60 \\ q_3 = 5 \quad & q_3' = 12, \text{ weil } 5 \cdot 12 = 60 \end{aligned}$$

Suche nun y_i, z_i, für die gilt

$$1 = y_i \cdot q_i + z_i \cdot q_i'$$

$$\begin{aligned} 1 &= 7 \cdot 3 + \underbrace{(-1)}_{z_1} \cdot 20 \\ 1 &= (-11) \cdot 4 + \underbrace{3}_{z_1} \cdot 15 \\ 1 &= 5 \cdot 5 + \underbrace{(-2)}_{z_1} \cdot 12 \end{aligned}$$

Es ist also

$$\mathbb{Z}_{60} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$$

Berechne nun z.B. $[43]_{60} \cdot [35]_{60}$

$$\begin{aligned} [43]_{60} \cdot [35]_{60} &= \eta([43]_3, [43]_4, [43]_5) \cdot \eta([35]_3, [35]_4, [35]_5) \\ &= \eta([1]_3, [3]_4, [3]_5) \cdot \eta([2]_3, [3]_4, [0]_5) \\ &= \eta([1]_3 \cdot [2]_3, [3]_4 \cdot [3]_4, [3]_5 \cdot [0]_5) \\ &= \eta([2]_3, [1]_4, [0]_5) \\ &= [\underbrace{2 \cdot (-1) \cdot 20}_{a_1 \cdot z_1 \cdot q_1'} + \underbrace{1 \cdot 3 \cdot 15}_{a_2 \cdot z_2 \cdot q_2'} + \underbrace{0 \cdot (-2) \cdot 12}_{a_3 \cdot z_3 \cdot q_3'}]_{60} \\ &= [5]_{60} \end{aligned}$$

Folgerung 1 (chinesischer Restsatz)
Sind $q_1, \ldots, q_r$ paarweise teilerfremde ganze Zahlen, in Zeichen $q_k \in \mathbb{Z}, k \in \{1, \ldots, r\}$ und $1 \in \text{ggT}(q_i, q_j)$ für $i \neq j$ mit $i, j \in \{1, \ldots, r\}$, mit $m = q_1 \cdot \ldots \cdot q_r$ und sind $a_1, \ldots, a_r \in \mathbb{Z}$ beliebig, so gibt es stets genau ein $a \in \{0, \ldots, m-1\}$ mit

$$a \equiv a_i \mod q_i \qquad \text{für } i = 1, \ldots, r.$$

(Die Menge aller $a \in \mathbb{Z}$ mit $a \equiv a_i \mod q_i$ ist gerade $[a]_m = a + m\mathbb{Z}$.)

Beweis
Wende Satz 1 an mit $R = \mathbb{Z}$. Da ψ surjektiv ist, gibt es zu $[a_1]_{q_1}, \ldots, [a_r]_{q_r}$ für beliebige $a_1, \ldots, a_r \in \mathbb{Z}$ stets ein $[a]_m \in \mathbb{Z}/_{m\mathbb{Z}}$ mit

$$\psi([a]_m) = ([a_1]_{q_1}, \ldots, [a_r]_{q_r})$$

$[a]_m$ ist eindeutig bestimmt, weil ψ auch injektiv ist.

$$\begin{aligned} \psi([a]) &= ([a]_{q_1}, \ldots, [a]_{q_r}) \\ &= ([a_1]_{q_1}, \ldots, [a_r]_{q_r}) \end{aligned}$$

da (für $i = 1, \ldots, m$)

$$[a]_{q_i} = [a_i]_{q_i}$$

gilt

$$a \equiv a_i \mod q_i$$

Folgerung 2
Sind $q_1, \ldots, q_r$ paarweise teilerfremde ganze Zahlen, in Zeichen $q_k \in \mathbb{Z}, k \in \{1, \ldots, r\}$ und $1 \in \mathrm{ggT}(q_i, q_j)$ für $i \neq j$ mit $i, j \in \{1, \ldots, r\}$, mit $m = q_1 \cdot \ldots \cdot q_r$ und sind $a_1, \ldots, a_r \in \mathbb{Z}$ beliebig, so gilt

$$[a]_m \in (R/_{mR})^*,$$

$$\text{d.h.}[a]_m \text{ ist Einheit (also invertierbar) } \Leftrightarrow [a]_{q_i} \in (R/_{q_i R})^*, i = 1, \ldots, r$$

Also

$$|(R/_{mR})^*| = \prod_{i=1}^{r} |(R/_{q_i R})^*|.$$

Beweis
Ein Isomorphismus ψ bildet Einheiten auf Einheiten ab, weil für $v = u^{-1}$

$$\psi(1) = \psi(uv) = \psi(u)\psi(v) = 1,$$

also

$$\psi(v) = \psi(u)^{-1}$$

$$(R/_{q_1 R} \times \ldots \times R/_{q_r R})^* = (R/_{q_1 R})^* \times \ldots \times (R/_{q_r R})^*$$

§ 7 Eulersche φ-Funktion und Moebius-Inversion

Satz 1
Ist φ die Eulersche φ-Funktion, d.h.

$$\varphi(m) = |\mathbb{Z}_m^*| = |\{j \in \{1, \ldots, m\} \mid 1 \in \mathrm{ggT}(j, m)\}|$$

und $m = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$ mit $p_i \neq p_j$ für $j \neq i$ und p_i Primzahlen und $n_i \in \mathbb{N}$, so ist

$$\varphi(m) = p_1^{n_1-1}(p_1 - 1) \cdot \ldots \cdot p_r^{n_r-1}(p_r - 1).$$

Beispiel 1

$$\varphi(60) = \varphi(4 \cdot 3 \cdot 5) = \varphi(2^2 \cdot 3 \cdot 5) = \underbrace{2}_{2^1(2-1)} \cdot 2 \cdot 4 = 16$$

$$\varphi(1) = 1 = |\{j \in \{1\} \mid 1 \in \mathrm{ggT}(1, 1)\}| = |\{1\}| = 1$$

Beweis
Wende Folgerung 2 (§6) an mit $R = \mathbb{Z}$ und $q_i = p_i^{n_i}$ dann gilt

$$\varphi(m) = |\mathbb{Z}_m^*| = \prod_{i=1}^{r} |\mathbb{Z}_{q_i}^*| = \prod_{i=1}^{r} \varphi(p_i^{n_i})$$

Bleibt noch zu zeigen, dass für $n \in \mathbb{N}$ und p Primzahl

$$\varphi(p^n) = p^{n-1}(p - 1).$$

Bestimmte $j \in \{1, \ldots, p^n\}$ erfüllen $1 \notin \mathrm{ggT}(j, p^n)$

$$\Leftrightarrow p|j \Leftrightarrow j \in \{p, 2p, 3p, \ldots, p^{n-1} \cdot p\} = M$$

Die Anzahl der teilerfremden Zahlen zu p in $\{1, \ldots, p^n\}$

$$\begin{aligned} \varphi(p^n) &= |\{k \in \{1, \ldots, p^n\} \mid 1 \in \mathrm{ggT}(k, p^n)\}| \\ &= p^n - |M| = p^n - p^{n-1} = p^{n-1}(p - 1) \end{aligned}$$

Bemerkung
Die Formel

$$\varphi(m) = p_1^{n_1-1}(p_1 - 1) \cdot \ldots \cdot p_r^{n_r-1}(p_r - 1)$$

aus Satz 1 lässt sich auch so schreiben:

$$\begin{aligned}\varphi(m) &= m(1-\frac{1}{p_1})\cdot\ldots\cdot(1-\frac{1}{p_r}) \\ &= \frac{m}{1}-(\frac{m}{p_1}+\ldots+\frac{m}{p_r})+\sum_{i<j}\frac{m}{p_ip_j}-+\ldots(-1)^r\frac{m}{p_1\ldots p_r}\end{aligned}$$

Definition 1

$$\mu(d)=\begin{cases}1 & \text{für } d=1\\ (-1)^r & \text{für } d=p_1\cdot\ldots\cdot p_r \text{ mit } p_i \text{ Primzahl}, p_i\neq p_j \text{ für } j\neq i\\ 0 & \text{wenn für eine Primzahl} p \text{ gilt } p^2|d\end{cases}$$

Die Funktion $\mu:\mathbb{N}\longrightarrow\mathbb{Z}$ heißt Möbiusfunktion.

Folgerung 1

$$\varphi(m)=\sum_{d|m(d\in\mathbb{N})}\mu(d)\cdot\frac{m}{d}$$

Lemma 1
Es gilt für die Möbiusfunktion

$$\sum_{d|m,d\in\mathbb{N}}\mu(d)=\begin{cases}1 & \text{für } m=0\\ 0 & \text{sonst}\end{cases}.$$

[Man kann dies als rekursieve Formel deuten

$$\begin{aligned}\mu(1) &= 1\\ \mu(m) &= -\sum_{d|m,1\leq d<m}\mu(d)]\end{aligned}$$

Beweis
Für $m=1$ ist $\varphi(m)=\varphi(1)=1$. Sei also $m>1$, dann hat m genau eine Primfaktorzerlegung $m=p_1^{n_1}\cdot\ldots\cdot p_r^{m_r}$ mit $p_i\neq p_j$ für $i\neq j$ und p_i Primzahlen.

$$\begin{aligned}d|m &\Rightarrow d=p_1^{m_1}\cdot\ldots\cdot p_r^{m_r} \text{ mit } 0\leq m_i\leq n_i.\\ d|m \text{ und } \mu(d)\neq 0 &\Rightarrow m_i\in\{0,1\}\end{aligned}$$

$$\{d|m\mid\mu(d)\neq 0\}\longleftrightarrow\{\text{Teilmenge von } p=\{p_1,\ldots,p_r\}\}$$

$$\prod_{p\in M}p\longleftrightarrow M$$

$$\sum_{d|m,d\in\mathbb{N}} \mu(d) = \sum_{d|m,\mu(d)\neq 0} \mu(d) = \sum_{M\subseteq P} \mu\left(\prod_{p\in M} p\right)$$
$$= \sum_{j=0}^{r} \sum_{M}$$

Satz 2 (Möbiusinversion)
Sei $f : \mathbb{N} \longrightarrow \mathbb{Z}$ eine beliebige Abbildung und dazu

$$g(m) = \sum_{d|m,d\in\mathbb{N}} f(d)$$

die „summatorische Funktion zu f“. Dann gilt

$$f(m) = \sum_{d|m,d\in\mathbb{N}} \mu(d) g\left(\frac{m}{d}\right)$$

Beweis

$$\sum_{d|m} \mu(d) g(\frac{m}{d}) = \sum_{d|m} \mu(d) \left(\sum_{c|\frac{m}{d}} f(c)\right)$$
$$= \sum_{c|m} \left(\sum_{d|\frac{m}{c}} \mu(d)\right) f(c) = f(m)$$

denn nach Lemma 1 ist

$$\sum_{d|\frac{m}{c}} \mu(d) = \begin{cases} 0 & \text{für } \frac{m}{c} \neq 1 \\ 1 & \text{für } c = m \end{cases}$$

20.06.MMI

§ 8 Gruppen und Untergruppen

$(G, \cdot) = (G, \cdot, ^{-1}, 1)$ sei Gruppe

Beispiel 1

a) R Ring $\Rightarrow (R, +, -, 0)$ abelsche Gruppe
$(\mathbb{Z}, +)$ Gruppe
$(\mathbb{Z}_m, +)$ $\quad |\mathbb{Z}_m| = m \in \mathbb{N}$

b) $(S_n, \circ)$ = **symmetrische Gruppe**
$S_n = \{$ Permutationen von $\{1, \ldots, n\}$ $\}$

c) $GL_n(K) = \{A \in K^{n \times n} \mid detA \neq 0\}$ K Körper

Beweis
Ist R Ring und ist

$$R^* = \{a \in R \mid \exists a^{-1} \in R \text{ mit } a \cdot a^{-1} = a^{-1} \cdot a = 1\}$$

so ist $(R^*, \cdot)$ ein Gruppe, die **Einheitengruppe von** R
[allgemeiner: $(M, \cdot, 1)$ Monoid $\Rightarrow M^* = \{$ invertierbare Elemente in M $\}$ $(M^*, \cdot, 1)$ Gruppe]

Beispiel 2
$m \in \mathbb{N}$
$\mathbb{Z}_m^* = \{[a]_m \mid 1 \in ggT(a, m)\}$,
$(\mathbb{Z}_m^*)$ heisst **prime Restklassengruppe modulo** m
$|\mathbb{Z}_m^*| = \varphi(m)$ φ ist Eulersche Funktion.

Definition 1
Ist $H \leq G$ **Untergruppe** von G
[also $H \leq G$ mit $1 \in H$ und $a, b \Rightarrow a^{-1} \cdot b \in H$]
und $g \in G$, so heisst die Menge

$$g \cdot H = \{g \cdot h \mid h \in H\}$$

Linksnebenklasse (von g bezüglich H).

Lemma 1
Ist $H \leq G$ $(G, \cdot)$ Gruppe, so wird durch

$$g \sim g' \Leftrightarrow g^{-1} \cdot g \in H$$

eine Äquivalenzrelation auf G definiert, und

$$[g]_\sim = g \cdot H$$

Beweis
$\sim$-Reflexivität: gilt, weil $1 = g^{-1} \cdot g \in H$ $\forall g$
$\sim$-Symmetrie: gilt, weil $g \sim g'$ bedeutet, dass $g^{-1} \cdot g' \in H \Rightarrow (g^{-1} \cdot g')^{-1} \in H \Leftrightarrow g'^{-1} \cdot g \in H \Leftrightarrow g \sim g'$
$\sim$-Transitivität: gilt, denn

Seien $g \sim g'$ also $g^{-1} \cdot g' \in H$
$g' \sim g''$ also $g'^{-1} \cdot g'' \in H$

$\Rightarrow$ $g^{-1} \cdot g'' = g' \cdot g^{-1} \cdot g'^{-1} \cdot g'' \in H$ also $g \sim g'' \in H$.

Folgerung 1
Die Linksnebenklassen von H in G bilden eine Partition.

Satz 1 (Satz von Lagrange)
Es sei $(G, \cdot)$ Gruppe mit $|G| < \infty$ und $H \leq G$, dann ist

$$|G| = |H| \cdot [G : H]$$

wobei

$$\begin{aligned} [G:H] &= \text{Anzahl der Linksnebenklassen von } H \text{ in } G \\ &= \textbf{Index} \text{ von } H \text{ in } G \\ |H| &= \text{Anzahl der Elemente von } H \\ &= \textbf{Ordnung} \text{ von } H \end{aligned}$$

Insbesondere ist $|H| \mid |G|$.

Beweis

$$G = g_1 H \dot\cup \ldots \dot\cup g_r H$$

(nach Lemma 1 bzw. Folgerung 1), weil $|G| < \infty$

ψ_i: $\begin{array}{ccc} H & \to & g_i \cdot H \\ h & \mapsto & g_i \cdot h \end{array}$

ψ_i ist injektiv, weil $g_i \cdot h = g_i \cdot h'$ für $h, h' \in H \Rightarrow h = g_i^{-1} \cdot g_i \cdot h = g_i^{-1} g_i \cdot h' = h'$
ψ_i ist surjektiv, weil jedes Element aus $g_i \cdot H$ von der Form $g_i \cdot h = \psi_i(h)$ ist.
Also ist ψ_i bijektiv. $|H| = |g_i \cdot H|$

$$|G| = \sum_{i=1}^{r} |g_i \cdot H| = |H| \cdot r$$

und $r = [G : H]$.

Definition 2
Ist $g \in G$ und $(G, \cdot)$ eine Gruppe, so sei

$$< g >= \{g^j \mid j \in \mathbb{Z}\}$$

die von g **erzeugte Untergruppe** von G.
$| < g > | = ord(g)$ heisst **Ordnung** von g
G heisst **zyklisch**, wenn es $g \in G$ gibt mit $G =< g >$.

Beispiel 3

a) $(\mathbb{Z}_n, +)$
[beachte: $(G,+)$ Gruppe $g \in G \qquad < g >= \{j \cdot g \mid j \in \mathbb{Z}\}$]
$\mathbb{Z}_n =< 1 >$ ist zyklisch von der Ordnung n.

b) $(\mathbb{Z}_{12}^*, \cdot)$
$\mathbb{Z}_{12}^* = \{1,5,7,11\} \qquad j = [j]_{12}$

$$\begin{array}{rll} 5^2 = 1 & \text{in } \mathbb{Z}_{12} & | < 5 > | = 2 \\ 7^2 = 1 & \text{in } \mathbb{Z}_{12} & | < 7 > | = 2 \\ 11^2 = 1 & \text{in } \mathbb{Z}_{12} & | < 11 > | = 2 \\ (\mathbb{Z}_{12}^*, \cdot) & \text{nicht zyklisch} & | < 1 > | = 1 \end{array}$$

c) $(\mathbb{Z}_7^*, \cdot)$
$\mathbb{Z}_7^* = \{1,2,3,4,5,6\} \qquad j = [j]_7$

g	1	2	3	4	
g^2		4	2	2	
g^3		1	6	1	in $\mathbb{Z}_7^*$
			5		
			1		

$< 3 >= G$
$ord(3) = 6$
$ord(2) = 3$
$ord(6) = 2$
(in $\mathbb{Z}_7^*$)

Satz 2

Ist $(G,\cdot)$ eine zyklische Gruppe mit $|G| = m$, $G =< g >$, so ist $m = ordg = Min\{j \in \mathbb{N} \mid g^j = 1\}$ und $g^j = 1 \Leftrightarrow ord(g) \mid j$ und $ord(g^j) = \frac{m}{d}$ mit $1 \leq d \in ggT(j,m)$. G hat zu jedem Teiler t von m genau eine Untergruppe U mit $|U| = t$ und zwar

$$\begin{aligned} U &= \langle g^{\frac{m}{t}} \rangle \\ < g^j > &= G \Leftrightarrow 1 \in ggT(j,m) \\ m &= \sum_{\substack{d \mid m \\ d \in \mathbb{N}}} \varphi(d) \end{aligned}$$

$\varphi(d)$ = Anzahl der Elemente in G mit Ordnung d.

Beweis

Da $|G| = d < \infty$ gibt es $i < j$ mit $i,j \in \mathbb{N}$ und $g^i = g^j$, dann folgt

$$g^h = 1 \qquad \text{für } h = j - i \in \mathbb{N}$$

Sei $n = Min\{k \in \mathbb{N} \mid g^k = 1\}$. Dann ist $|\{1, g, \ldots, g^{n-1}\}| = n$.
Ist $j \in \mathbb{Z}$, so gibt es $q, r \in \mathbb{Z}$ mit $j = q \cdot n + r$ und $r \in \{0, 1, \ldots, n-1\}$.
Es folgt $g^j = \underbrace{(g^n)^q}_{=1} \cdot g^r = g^r \in \{1, g, \ldots, g^{n-1}\}$.
Also $G = \{1, g, \ldots, g^{n-1}\}$ $\quad n = m$
und $g^j = 1 \Leftrightarrow r = 0 \Leftrightarrow j = q \cdot n \Leftrightarrow n|j$.
$(g^i)^j = g^{ij} = 1 \Leftrightarrow m|ij \Leftrightarrow \frac{m}{d}|j$ für $d \in ggT(i, m)$. Also $ord(g^i) = \frac{m}{d}$
Sei $U \leq G$ $\quad |U| = t$ nach Lagrange ist $t|m$.
Sei $d = Min\{j \in \mathbb{N} \mid g^j \in U\}$

Beh:

$$< g^d >= U$$

Bew: $\subseteq$: trivial

$\supseteq$: Sei $g^j \in U$ beliebig. Es gibt dazu $q, r \in \mathbb{Z}$ mit $j = q \cdot d + r$ und $r \in \{0, \ldots, d-1\}$
$g^j \in U$ $\quad (g^d)^q = g^{qd} \in U$
also $g^{j-qd} = g^r \in U$ also $r = 0$
$g^j = (g^d)^q \in < g^d >$
$ord(g^d) = |U| = t = \frac{m}{d}$

Also $U =< g^{\frac{m}{t}} >$.
$< g^i >= G \Leftrightarrow ord(g^i) = m \Leftrightarrow 1 \in ggT(m, i)$.

Folgerung 2
Ist $|G| = n$ und $g \in G$, $(G, \cdot)$ Gruppe, so ist $g^n = 1$

Beweis
$< g > \leq |G| = n$
$ord(g) = |\langle g \rangle| \,|\, |G| = n = ord(g) \cdot q$
$1 = g^{ord(g)}$ also $1 = 1^q = g^{ord(g) \cdot q} = g^n$

Satz 3 (Satz von Euler)
Für $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $1 \in ggT(a, n)$ gilt:

$$a^{\varphi(n)} = 1 \mod n$$

Beweis
$[a]_n \in \mathbb{Z}_n^*$ nach Voraussetzung.
$1 = [a]_n^{|\mathbb{Z}_n^*|} = [a]_n^{\varphi(n)} = [a^{\varphi(n)}]_n$
d.h. $n|a^{\varphi(n)} - 1$

Beispiel 4
Was sind die letzen drei Ziffern von

$$b = 7^{123785648801}?$$

Antwort: 007.

Bew: $b \equiv 7 \mod 1000$
$ggT(7, 1000) = 1 \qquad 7^{\varphi(1000)} = 1 \mod 1000$

$$\begin{aligned} \varphi(1000) &= \varphi(10^3) = \varphi(2^3 \cdot 5^3) \\ &= 2^2 \cdot (5-1) \cdot 5^2 = 400 \\ 7^{400} &\equiv 1 \mod 1000 \\ 123\ldots801 &= q \cdot 400 + 1 \\ b &= 7 \mod 1000 \end{aligned}$$

Satz 4 (kleiner Satz von Fermat)
Ist p Primzahl und $a \in \mathbb{Z}$ beliebig, so ist

$$a^p \equiv a \mod p$$

Beweis
$p|a$ dann auch $p|a^p$ und $p|a^p - a$

$p \not| a$ und es gilt $1 \in ggT(p, a)$.
nach Euler $a^{\varphi(p)} \equiv 1 \mod p$.
mit $\varphi(p) = p - 1$ gilt dann
$a^{p-1} \equiv 1 \mod p$ und durch Multiplikation mit a also $a^p \equiv a \mod p$

22.06.MMI

Folgerung 3 (Primzahltest)
Ist $p \in \mathbb{N}$ und gibt es $1 < a < p$ mit $a^{p-1} \not\equiv 1 \mod p$, so ist p keine Primzahl.

Beweis
Wäre p eine Primzahl, so wäre $\varphi(p) = p - 1$ und $1 \in \mathrm{ggT}(a, p)$ und nach Satz von Euler oder Fermat:

$$a^{\varphi(p)} = a^{p-1} = 1 \mod p$$

Beispiel 5

$$f_i = 2^{(2^i)} + 1$$

i	0	1	2	3	4	5 . . . 11	12 . . . 23
f_i	3	5	17	257	65537	keine Primzahl	

Für $i = 5, \ldots, 11$ sind die Faktoren bekannt.

Wende Folgerung (Primzahltest) an mit $a = 3$

$$[a^{f_5-1}]_{f_5} = [a^{(2^{32})}]_{f_5}$$

mit 32 Multiplikationen und < 32 Divisionen mit Rest

$$= [302906160]_{f_5} \neq [1]_{f_5}$$

Also ist f_5 keine Primzahl.

Beispiel 6 (zu Satz 2)
Seien $G = \langle g \rangle$ mit $|G| = 12$. Dann ist

			$\varphi(d)$
$\operatorname{ord} g^i = 12$	für	$i = 1, 5, 7, 11$	4
$\operatorname{ord} g^i = 6$	für	$i = 2, 10$	2
$\operatorname{ord} g^i = 4$	für	$i = 3, 9$	2
$\operatorname{ord} g^i = 3$	für	$i = 4, 8$	2
$\operatorname{ord} g^i = 2$	für	$i = 6$	1
$\operatorname{ord} g^i = 1$	für	$i = 12$	1

Satz 5
Äquivalent sind für eine endliche Gruppe G mit $|G| = m$

a) G ist zyklisch

b) für $1 \leq d | m$ ist $\big|\{g \in G \mid g^d = 1\}\big| = d$

c) für $1 \leq d | m$ ist $|\{g \in G \mid \operatorname{ord} g = d\}| = \varphi(d)$

$a) \Rightarrow b)$: Sei $1 \leq d$ mit $d|m$.

$$\left|\{g \in G \mid g^d = 1\}\right| = |\{g \in G \mid (ord g)|d\}| \underset{Satz2}{=} \sum_{\substack{c|d \\ c\in\mathbb{N}}} \varphi(c) = d$$

$b) \Rightarrow c)$: Sei $|G| = m$, G beliebig, $1 \leq d|m$

Beweis

$$f(d) = |\{g \in G \mid \operatorname{ord} g = d\}|$$

$$d \underset{Vor.b)}{=} \left|\{g \in G \mid g^d = 1\}\right| = \sum_{\substack{c|d \\ c\in\mathbb{N}}} f(c)$$

mit Hilfe der Möbiusinversion ist

$$f(d) = \sum_{\substack{c|d \\ c\in\mathbb{N}}} \mu(c)\frac{d}{c} = \varphi(c)$$

$c \Rightarrow a)$: $\varphi(m) \geq 1$, also gibt es nach Vor. C) ein Element g mit $\langle g\rangle = G$

Beispiel 7 (Pseudozufallszahlen Fortsetzung von Beispiel 5 in §§ 3)

$$\begin{aligned} z_0 &= 0 \qquad \text{in } \mathbb{Z}_m \\ z_n &= az_{n-1} + c \end{aligned}$$

a und c sind so zu bestimmen, dass

$$(*)Z_m = \{[z_n]_m \mid 0 < n < m-1\}$$

Wende den chinesischen Restsatz an

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_r^{k_r}}$$

falls $m = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ mit $p_i \neq p_j$ Primzahlen für $i \neq j$
(*) gilt genau dann, wenn

$$\mathbb{Z}_{p_i^{k_i}} = \{[z]_{p_i^{k_i}} \mid 0 < n < p_i^{k_i} - 1\} \qquad \text{für } i = 1, 2, \ldots, r$$

OBdA $m = p^k$ für eine Primzahl.

In §§ 3 ist die Rekursion aufgelöst worden durch:

$$z_n = c(a^0 + a^1 + \ldots + a^{n-1}) \text{ in } \mathbb{Z}_m$$

(*) gilt außerdem genau dann, wenn c eine Einheit ist, d.h. $c \in \mathbb{Z}_m^*$ und

$$\mathbb{Z}_m = \left\{(1 + a + \ldots + a^{n-1}) \mid 0 < n < m - 1\right\}$$

Insbesondere folgt

$$\begin{aligned} 0 &= (1 + a + \ldots + a^{m-1}) \\ 0 &= (1 + a + \ldots + a^{m-1})(a - 1) = a^m - 1 \end{aligned}$$

Also muß gelten

$$a^m = 1$$

also ist

$$a \in \mathbb{Z}_m^*$$

und es gilt

$$\operatorname{ord} a | m = p^k$$

und nach Lagrange

$$\operatorname{ord} a || \mathbb{Z}_m^*| = \varphi(m) = p^{k-1}(p - 1)$$

also

$$\operatorname{ord} a | p^{k-1}.$$

Angenommen $p \neq 2$: Zeige $\mathbb{Z}_{p^k}^*$ ist zyklisch und

$$\operatorname{ord}[p + 1]_m = p^{k-1}$$

also

$$[a]_m = [p + 1]_m^j$$

also

$$p | a - 1$$

Folgerung 4
Damit (*) gilt, (d.h. alle Elemente getroffen werden) müssen a und c die folgenden Bedingungen erfüllen:

(i) $1 \in \operatorname{ggT}(m, c)$

(ii) Ist $2 \neq p|m$, so muss $p|a-1$ gelten.

(iii) [Ist $2|m$, so muss $2^2|a-1$

umgekehrt folgt aus (i), (ii), (iii) die Bedingung (*)]

Dies kann man genauer in Knuth, The art of computer programming II, Kapitel 1 nachlesen.

Es sei $(G, \cdot, ^{-1}, 1)$ eine beliebige Gruppe und $\sim$ eine Kongruenzrelation, d.h.

$$\begin{aligned} \sim & \text{ ist } \text{Äquivalenzrelation} \\ a \sim b & \Rightarrow a^{-1} \sim b^{-1} \\ a \sim b, c \sim d & \Rightarrow a \cdot c \sim b \cdot d \forall a, b, c, d \end{aligned}$$

Setze $H = [1]_\sim = \{h \in G \mid h \sim 1\}$.
Weil $\sim$ reflexiv ist und $1 \in H$, gilt:
Sei $h \in H$, also $h \sim 1$, so folgt

$$h^{-1} \sim 1^{-1} = 1, \text{ also } h^{-1} \in H$$

Seien $h, h' \in H$, also $h \sim 1$ und $h' \sim 1$, dann

$$h \cdot h' \sim 1 \cdot 1 = 1, \text{ also } h \cdot h' \in H$$

Also ist $H \leq G$ „Untergruppe“.
Seien $h \in H, g \in G$, also $h \sim 1, g \sim g$. Es folgt

$$\left.\begin{array}{rcl} h \cdot g & \sim & 1 \cdot g = g \\ g^{-1} & \sim & g^{-1} \end{array}\right\} \Rightarrow g^{-1}(h \cdot g) \sim g^{-1} g = 1$$

Es folgt $g^{-1} \cdot h \cdot g \in H$.

Definition 3
Eine Untergruppe $H \leq G$ heißt „**Normalteiler**“, (in Zeichen $H \triangleq G$,) wenn für alle $g \in G, h \in H$

$$g^{-1} h g \in H$$

oder:

$$g^{-1} H g = H \qquad \forall g \in G$$

oder:

$$H \cdot g = g \cdot H \qquad \forall g \in G$$

wobei $H \cdot g$ die Rechts- und $g \cdot H$ die Linksnebenklasse sind.

Satz 6
Ist $\sim$ eine Kongruenzrelation auf G, so ist

$$[1]_\sim = H \triangleq G.$$

Umgekehrt ist $H \triangleq G$, so wird durch

$$a \sim b \underset{def}{\Leftrightarrow} a^{-1}b \in H$$

eine Kongruenzrelation definiert.

Beispiel 8
Sei $G = S_3$ eine symmetrische Gruppe.

$$H = S_3 = \{1, (12), (23), (13), (123), (132)\}$$

$|G| = 1 \cdot 2 \cdot 3 = 6$ 6
$\langle(12)\rangle = \{1, (12)\}$ 3
$\langle(123)\rangle = \{1, (123), (132)\}$ 2
An alle: wie geht das hier weiter? In meinen Aufzeichnungen stimmt irgendwas nicht!!!!!

Bemerkung
Ist G abelsch und $H \leq G$, so ist

$$H \triangleq G$$

04.07.MMI

K endlicher Körper, in der Regel ist $K = \mathbb{Z}_2$ ($K = GF(2^m)$).

Ein **linearer** (n, k)**-Code** ist ein Teilraum C von K^n mit dim $C = k$

$$d(v, w) = |\{i \mid v_i \neq w_i\}| = d(v - w, 0)$$

C wird im Allgemeinen durch eine **Generator-Matrix** $G(c)$ angegeben.

$G(C) \in K^{k \times n}$ mit Basisvektoren von C in den Zeilen.

Kontrollmatrix $H = H(C) \in K^{n-k,n}$

$$C = \{c \in K^n \mid H \cdot c^T = 0\}$$

Für ein $c' \in K^n$ nennt man Hc'^T **Syndrom**.

$$Hc'^T = 0 \Leftrightarrow c' \in C$$

C ist ein zylklischer Code genau dann, wenn c linearer (n, k)-Code mit

$$c = (c_0, c_1, \ldots, c_{n-1} \in C \Rightarrow \mathcal{V}(c) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$$

$$\begin{aligned} \Psi : K^n &\longrightarrow K[x]/_{(x^n-1)K[x]} = K[x]/_{(x^n-1)} \\ (c_0, \ldots, c_{n-1}) &\longmapsto \left[\sum_{i=0}^{n-1} c_i x^i\right]_{x^n-1} \end{aligned}$$

$$\Psi(\mathcal{V}(c)) = [x]_{x^n-1}\Psi(c)$$

Bemerkung
$C \subseteq K^n$ linearer Code ist zyklisch genau dann, wenn

$$\Psi(c) \trianglelefteq K[x]/_{x^n-1}$$

Was sind die Ideale in $K[x]/_{x^n-1}$?
Angenommen

$$I \trianglelefteq K[x]/_{x^n-1}$$

$$\begin{aligned} J &= \{f \in K[x] \mid [f]_{x^n-1} \in I\} \trianglelefteq K[x] \\ &= g \cdot K[x] \text{ für ein } g \in K[x] \end{aligned}$$

$$x^n -^{\in} J, \text{also } g | x^n - 1$$

Lemma 2
Ist C ein zyklischer (n, k)-Code mit $c \neq 0$, so gibt ef ein normiertes **Generatorpolynom** $g \in K[x]$ mit $g|x^n - 1$ von C mit

$$\Psi(c) = \{[f \cdot g]_{x^n-1} \mid f \in K[x]\} \trianglelefteq K[x]/_{x^n-1}$$

Es ist

$$\operatorname{grad} g = n - k$$

Es gibt genauso viele zyklische Codes der Länge n wie $x^n - 1$ in $K[x]$ an Teilern hat.

Beispiel 9
$K = \mathbb{Z}_2 \qquad n = 7 = 2^3 - 1$

$$x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

Wähle $g = (x^3 + x + 1)$.

$$
\begin{array}{rcl}
 & & \begin{array}{ccccccc} 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{array} \\
G(C) & = & \left[\begin{array}{ccccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right] \begin{array}{l} \leftrightarrow [g]_{x^7} \\ \leftrightarrow [xg]_{x^7} \\ \leftrightarrow [x^2g]_{x^7} \\ \leftrightarrow [x^3g]_{x^7} \end{array} \\
 & & 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad \leftrightarrow \quad [x^4g]_{x^7} = [g]_{x^7} + [xg]_{x^7-1} + [x^2g]_{x^7-1}
\end{array}
$$

$$\dim C = 4 = 7 - \operatorname{grad} g$$

Beweis
$x^n - 1 = g \cdot h$ mit $h = \sum_{i=0}^{k} h_i x^i \qquad h_i = 1.$

$$\operatorname{grad} g + \operatorname{grad} h = \operatorname{grad} g + k = n$$

$$[g], [xg], \ldots, [x^{k-1}g] \text{ in } K[x]/_{x^n-1} \text{ linear unabhängig}$$

$$0 = [x^n - 1] = [gh] = [x^k g + \sum_{i=0}^{k-1} h_i x^i g]$$

$$[x^k g] = -\sum_{i=0}^{k-1} h_i [x^i g] \in \langle [g], [xg], \ldots, [x^{k-1}g] \rangle$$

$$\dim C = k$$

im Beispiel:

$$
\begin{array}{rcl}
x^7 - 1 & = & g \cdot h = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1) \\
h & = & (x+1)(x^3 + x^2 + 1) \\
 & = & x^4 + \not{x}^3 + \not{x}^3 + x^2 + x + 1 \\
 & = & x^4 + x^2 + x + 1
\end{array}
\tag{2.1}
$$

Nachricht	Codierung	Senden	Empfangen
$w = 1001 = 1 + x^3$	$c = w \cdot g =$	$c = 1100101$	$c' = 1101101 =$
	$(1 + x^3)(^+x + x^3) =$		$1 + x + x^3 + x^4 + x^6$
	$1 + \not{x}^3 + x + x^4 + \not{x}^3 + x^6$		

Fehlererkennung/Korrektur: Teile mit Rest durch g oder äquivalent setze in c' das Element $\alpha = [x]_g \in K[x]/_g$ ein.

29.06.MMI

§ 9 Endliche Körper und Codes

Satz 1
Ist K endlicher Körper, so gilt

a) $p = Min\{j \in \mathbb{N} \mid j \cdot 1 = \underbrace{1 + \ldots + 1}_{j} = 0\}$ ist eine Primzahl und $\mid K \mid = p^n$ für $n \in \mathbb{N}$.

p heißt **Charakteristik** von K und es gilt $p \cdot a = 0$ und $(a+b)^p = a^p + b^p$ für alle $a, b \in K$

b) Die multiplikative Gruppe $(K^*, \cdot)$ ist zyklisch

Beweis
a) $\psi : \begin{array}{c} \mathbb{Z} \to K \\ j \to j \cdot 1 \end{array}$ ist Ringhomorphismus

$Bild(\psi) \cong \mathbb{Z}/_{Kern(\psi)}$ Homomorphiesatz
$Kern(\psi) \triangleq \mathbb{Z}$ also existiert $p \in \mathbb{N}$ mit $Kern(\psi) = p\mathbb{Z}$

$$p = Min\{j \in \mathbb{N} \mid j1 = 0\}$$

Wäre p keine Primzahl, so hätte $Bild\psi \cong \mathbb{Z}/_{p\mathbb{Z}}$ Nullteiler. $\not\swarrow$ $K \geq K_p = Bild\psi \cong Z_p$
$\swarrow$
Körper K kann man als K_p-Vektorraum auffassen $dim_{K_p} K = n$ so hat K p^n Elemente $\mid K \mid = p^n$.

$$a \in K \qquad p \cdot a = p \cdot 1a = 0 \cdot a = 0$$

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j \cdot b^{p-j}$$

für $j = 1, 2, \ldots, p-1$ ist $p \mid \binom{p}{j} = \frac{p \cdot (p-1) \ldots (p-j+1)}{1 \cdot 2 \ldots j}$

$$\begin{array}{lrcl} \text{da} & pa^j b^{b-j} & = & 0 \quad \text{in } K \\ \text{ist} & \binom{p}{j} a^j b^{b-j} & = & 0 \quad \text{für } j = 1, 2, \ldots . p-1 \end{array}$$

also $(a+b)^p = a^p + b^p$

b) $\mid K \mid = p^n$ dann ist $\mid K^* \mid = p^n - 1$. Nach Lagrange gilt für jedes $\alpha \in K*$:

$$\alpha^{p^n - 1} = 1$$

Also ist jedes $\alpha \in K^*$ Nullstelle von

$$x^{p^n - 1} - 1 = \prod_{\alpha \in K^*} (x - \alpha) \in K[x]$$

Ist $m| \mid K^* \mid = p^n - 1 = m \cdot q$ mit $q \in \mathbb{N}$. So ist:

$$x^{p^n-1} - 1 = (x^m - 1)(1 + x^m + \ldots + x^{(q-1)m})$$

Also hat $x^m - 1$ im K^* genau m Nullstellen:

$$\mid \{\alpha \in K^* \mid \alpha^m = 1\} \mid = m$$

Nach §8 Satz 3 folgt K^* ist zyklisch.

Bemerkung
Ist $f \in \mathbb{Z}_p[x]$ irreduzibel und $\text{grad}(f) = n$ so ist $\mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ Körper mit p^n Elementen.

Frage: "Gibt's das immer?"

Satz 2
Ist p Primzahl und $\text{Irr}_n(\mathbb{Z}_p) = \{f \in \mathbb{Z}_p[x] \mid f \text{ irreduzibel, grad}f = n \text{ und normiert}\}$ so ist für jedes $n \in N$:

$$(*) \qquad x^{p^n} - x = \prod_{d|n} \prod_{f \in \text{Irr}_d(\mathbb{Z}_p)} f \qquad \in \mathbb{Z}_{p[x]}$$

$$N_n(p) = \mid \text{Irr}_n(\mathbb{Z}_p) \mid = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}$$

Folgerung 1
Zu jeder Primzahl p^n gibt es einen Körper K mit $\mid K \mid = p^n$.

Beispiel 1
$p = 2 \qquad n = 3$

$$x^{2^3} - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

Beweis Behauptung
a) Ist f irreduzibel $\in \mathbb{Z}_p[x]$ und $\text{grad}f = d|n$ so ist $f|x^{p^n} - x$

Beweis
$K = \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ ist Körper und $\mid K \mid = p^d$

$$\begin{aligned} \alpha^{p^{d-1}} &= 1 \qquad \text{für alle } x \in K^* \\ \alpha^{p^\alpha} &= \alpha \end{aligned}$$

Speziell für $\alpha = [x]_f$ erhält man:

$$[x^{p^d}]_f = [x]_f \text{ also } f|x^{p^d} - x$$

[wie im Satz 1] wenn $d|n$ so ist:

$$x^{p^d} - x | x^{p^n} - x$$

Behauptung

b) Ist $f \in \mathbb{Z}_p[x]$ irreduzibel und $f | x^{p^n} - x$, so ist $d = \text{grad} f | n$

Beweis

$r = 0 \qquad K = K[x]/fK[x] \qquad | K | = p^d$

$$[x]_f^{p^d} = [x]_f \qquad \text{wie in a)}$$

außerdem $[x]_f^{p^n} = [x]_f$ weil nach Vorraussetzung $f | x^{p^n} - 1$. Daher $[x]_f^{p^r} = [x]_f$ weil $n = dq + r$.

$$\begin{aligned} K \ni [\sum_{i=0}^{d-1} a_i x^i]_f^{p^r} &= (\sum_{i=0}^{d-1} [a_i x^i]_f)^{p^r} \qquad \text{nach Satz 1 a)} \\ &= \sum_{i=0}^{d-1} a_i (x^{p^r})^i]_f \\ &= [\underbrace{\sum_{i=0}^{d-1} a_i x^i}_{\alpha}]_f \end{aligned}$$

für $\alpha \in K$ erfüllt $\alpha^{p^r} = \alpha$ ist also Nullstelle von $x^{p^r} - x$ hat aber höchtens $\text{grad}(x^{p^r} - x)$ Nullstellen. Also $r = 0$.

Behauptung

c) Es gibt kein irreduziebles Ploynom $f \in \mathbb{Z}_p[x]$ und $f^2 | x^{p^n} - x$

Beweis

Angenommen $x^{p^n} - x = f^2 \cdot g = f \cdot (f \cdot g)$. Wende formale Ableitung an:

$$D(x^{p^n} - x) = p^n x^{p^n - 1} - 1 = -1 \qquad \text{in } \mathbb{Z}_p[x]$$

$$f | D(f \cdot fg) = f \cdot D(fg) + D(f) \cdot fg$$

Also $f | -1$. f ist Einheit in $\mathbb{Z}_p[x]$ und nicht irreduzibel.

d) Damit ist (*) bewiesen, brechne grad

$$\begin{aligned} \text{grad}(x^{p^n}) &= p^n \\ &= \sum_{d|n} \sum_{f \in \text{Irr}_d(\mathbb{Z}_p)} \text{grad} f \\ &= \sum_{d|n} N_d(p) \cdot d \\ p^n &= \sum_{d|n} N_d(p) \cdot d \end{aligned}$$

Nach §7 Möbiusinversion

$$nN_n(p) = \sum_{d|n} \mu(d) p^{\frac{n}{d}}$$

Beweis (Folgerung 1)

$$\begin{aligned} N_0(p) &= \frac{1}{n}[1p^n + \sum_{d|n;\ d\neq 1} \mu(d) p^{\frac{n}{d}}] \qquad \mu(d) \in \{0, 1, -1\} \\ &\geq \frac{1}{n}[p^n - \sum_{d|n} p^{\frac{n}{d}}] \\ &\geq \frac{1}{n}[p^n - (p + p^2 + \ldots + p^{n-1}] > 0 \end{aligned}$$

Satz 3
Je zwei Körper mit p^n Elementen sind isomorph. $GF(p^n)$ Bezeichnung für einen Körper mit p^n Elementen **Galois Feld**.

Beweis
Ist $f \in \mathrm{Irr}_n(\mathbb{Z}_p)$ und K ein beliebiger Körper mit $\mid K \mid 0p^n$.

Behauptung
$K \equiv \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$

Beweis
Nach Satz 2 enthält K eine Nullstelle α von f:

$$\Psi : [\sum_{i=0}^{n-1} a_i x^i]_f \to \sum_{i=0}^{n-1} a_i x^i \qquad a_i \in \mathbb{Z}_p$$

$$\mathbb{Z}_p/f\mathbb{Z}_p[x] \to K$$

Ψ ist ein Isomorphismus

$$\begin{aligned} c'(\alpha) &= 1 + [x]_g + [x^3]_g + [x]_g^4 + [x]_g^6 \\ &= [x^6 + x^4 + x^3 + x + 1]_g \end{aligned}$$

Anwendungen von endlichen Körpern ist z.B. die Kodierungstheorie.

$$\begin{aligned} x^6 + x^4 + x^3 + x + 1 &= (x^3 + x + 1)x^3 + x + 1 \\ &= [x + 1]_g \qquad [\neq 0] \\ &= \alpha^j \text{ mit } j = \log_\alpha [x + 1] \\ &\Rightarrow \quad j = 3 \end{aligned}$$

Haben also einen Fehler an Position 3, falls nur *ein* Fehler gemacht wurde.

$$c' = c + e,$$

Problem:

$$\boxed{\text{Nachricht}} \overset{Codierung}{\longrightarrow} \boxed{\text{Codewort}} \overset{Senden+Fehler}{\longrightarrow} \boxed{\text{Codewort + Fehler}} \overset{Decodierung}{\longrightarrow}$$

Aufgabe: Finde Code so, daß k Fehler korrigiert oder erkannt werden.
wobei $c \in C$ und $e = x^j$ das Fehlerpolynom ist.

$$c'(\alpha) = \underbrace{c(\alpha)}_{=0} + \alpha^j = \alpha^j$$

Korrektur:

$$c'' = c' + x^3 \leftrightarrow 1100101 = c$$

Um nun das dekodierte w' zu erhalten (das empfangene Wort), teile c durch g:

$$c = g(1 + x^4) \Rightarrow w = 1001$$

Bemerkung
Ist $L = GF(p^n)$, so gilt für jedes $\beta \in L$ $[K[x]/_{(f)} f \in K[x]$ irreduzibel vom Grad $n]$

$$\beta^{p^n} = \beta, \text{d.h.}$$

$$\begin{aligned} x^{p^n} &= \prod_{p \in L} (x - \beta) \in L[x] \\ &= \prod_{d|n} \prod_{f \in \mathrm{Irr}_d(K)} f \end{aligned}$$

wobei

$$\mathrm{Irr}_d(K) = \{f \in K[x] \mid \operatorname{grad} f = d, f \text{ irreduzibel }, f \text{ normiert}\}$$

Also: Zu jedem β existiert genau ein normiertes irreduzibles Polynom (von grad $d|n$) mit $f(\beta) = 0$.
Dieses (eindeutig) bestimmte Polynom heißt **Minimalpolynom** von *beta*, in Zeichen $f_\beta \in K[x]$.

$$L^* = L \setminus \{0\} = \langle \alpha \rangle \text{ für ein } \alpha \in L.$$

Satz 4
Es sei $n = p^r - 1$ (p Primzahl $p = 2$), $t < n - 1$, $L = GF(p^r)$, $L^* = \langle\alpha\rangle$ und

$$g = \mathrm{kgV}\{f_{a^i} \mid 1 \leq i \leq t\},$$

dann ist $g|x^n - 1$ und ist C der zyklische Code mit Generatorpolynom g und hat Minimaldistanz $\geq t + 1$.

Beispiel 2
Voraussetzungen wie in Beispiel 1, also $n = 7 = 2^3 - 1$ und

$$g = x^3 + x + 1 = f_\alpha = f_{\alpha^2}$$

$$\alpha = [x]_g \in K[x]/_{(g)} = L \qquad \langle\alpha\rangle) = L^*$$

Setze $t = 2$, $g = \mathrm{kgV}\{f_\alpha, f_{\alpha^2}\}$.
Also ist die Minimaldistanz von C nach Satz 4 $\geq t + 1 = 3$.

Beweis
Satz **??**

$$g = \sum_{1=0}^{m} g_i x^i = \mathrm{kgV}\{f_\alpha, \ldots, f_{\alpha^t}\}$$

$$\psi(c) = \{[f]_{x^n-1} \mid g|f\}$$

wobei $g|f \Leftrightarrow f(\alpha) = f(\alpha^2) = \ldots = f(\alpha^t) = 0$.

$$\begin{aligned} \text{Also } c &= (c_0, \ldots, c_{n-1}) \\ &= \sum_{i=0}^{n-1} c_i x^i \in C \Leftrightarrow \begin{matrix} c(\alpha) = 0 \\ c(\alpha^2) = 0 \\ \vdots \\ c(\alpha^t) = 0 \end{matrix} \end{aligned}$$

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & (\alpha^2) & (\alpha^2)^2 & \ldots & (\alpha^2)^{n-1} \\ \vdots & & & & \vdots \\ 1 & (\alpha^t) & (\alpha^t)^2 & \ldots & (\alpha^t)^{n-1} \end{bmatrix} \cdot \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} c(\alpha) \\ c(\alpha^2) \\ \vdots \\ c(\alpha^t) \end{bmatrix} = 0$$

Angenommen $\exists c \in C mitd(c, \underline{0}) \leq t$, dann sind alle $c_i = 0$ außer für $i \notin \{j_1, \ldots, j_t\}, 0 \leq j_1 < \ldots < j_t \leq n - 1$

$$\underbrace{\begin{bmatrix} \alpha^{j_1} & \alpha^{j_2} & \ldots & \alpha^{j_t} \\ \alpha^{1j_1} & \alpha^{2j_2} & \ldots & \alpha^{2j_t} \\ \vdots & & & \vdots \\ \alpha^{tj_1} & \alpha^{tj_2} & \ldots & \alpha^{tj_t} \end{bmatrix}}_{M} \cdot \begin{bmatrix} c_{j_1} \\ c_{j_2} \\ \vdots \\ c_{j_t} \end{bmatrix} = \underline{0}$$

$$\begin{aligned}
\det M &= \alpha^{j_1}\alpha^{j_2}\cdot\ldots\cdot\alpha^{j_1}\det \underbrace{\begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \ldots & \alpha^{j_t} \\ \vdots & & & \vdots \\ \alpha^{j_1(t-1)} & \alpha^{j_2(t-1)} & \ldots & \alpha^{j_t(t-1)} \end{bmatrix}}_{\text{van der Mondsche Matrix}} \\
&= \alpha^{j_1}\alpha^{j_2}\cdot\ldots\cdot\alpha^{j_1}\prod_{j_i<j_k}(\alpha^{j_i}-\alpha^{j_k}) \neq 0 \\
&\Rightarrow \quad c = 0.
\end{aligned}$$

■

06.07.MMI

Definition 1
Ein **Reed-Solomon-Code** der Länge $n = 2^r - 1$ über $K \leq GF(2^r)$ mit **Plandistanz** (**designed distance**) t ist ein Code

$$C = \{c = [c_0, \ldots, c_{n-1}] \mid c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^t) = 0\}$$

wobei $< \alpha >= (GF(2^r))^*$

Bemerkung
C ist **zyklischer Code** mit **Generatorpolynom** $g = kgV(f_{\alpha^i} \mid 1 \leq i \leq t)$ $\quad f_{\alpha^i} \in K[x]$ ist Minmalpolynom von α^i. C hat **Minimaldistanz** $\geq t + 1$.

$$\mathrm{Irr}_d(K) = \{f \in K[x] \mid \operatorname{grad} f = d, f \text{ irreduzibel}, f \text{ normiert}\}$$

Also existiert zu jedem β genau ein normiertes irreduzibles Polynom (vom Grad $d|n$) mit $f(\beta) = 0$.

Dieses (eindeutig) bestimmte Polynom heißt Minimalpolynom von β, in Zeichen

$$f_\beta \in K[x]$$

$$L^* = L \setminus \{0\} = \langle\alpha\rangle \text{ für ein } \alpha \in L$$

Satz 5
Seien $n = p^r - 1$ (p Primzahl, $p = 2$), $t < n - 1$, $L = GF(p^r)$ und $L^* = \langle\alpha\rangle$ und

$$g = \mathrm{kgV}\{f_{\alpha^i} \mid 1 \leq i \leq t\},$$

dann ist $g|x^n - 1$ und ist C der zyklische Code mit Generatorpolynom g mit einer **Minimaldistanz** $\geq t + 1$.

Beispiel 3
Siehe oben. $n = 7 = 2^3 - 1$, $g = x^3 + x^+1 = f_\alpha = f_{\alpha^2}$

$$\alpha = [x]_g \in K[x]/_{(g)} = L\langle\alpha\rangle = L^*$$

Setze $t = 2, g = \text{kgV}\{f_\alpha, f_{\alpha^2}\}$. Also ist nach Satz 5 die Minimaldistanz von $C \leq t + 1 = 3$.

Ist $t = 2t'$, so kann C t' Fehler korrigieren oder $2t'$ Fehler erkennen.

Beispiel 4
$K = \mathbb{Z}_2 \qquad n = 15 = 2^4 - 1$

$$X^{15} - 1 = (X+1)(X^2+X+1)\underbrace{(X^4+X+1)}_{=f;\alpha=[x]_f}(X^4+X^3+1)(X^4+X^3+X^2+X+1)$$

$$\begin{aligned} GF(2^4) &= K[x]/_{(X^4+X+1)} \\ & f_\alpha = X^4+X+1 = f_{\alpha^2} = f_{\alpha^4} \qquad ord\alpha = 15 \\ & f_{\alpha^3} = X^4+X^3+X^2+X+1 \qquad ord\alpha^3 = 5 \end{aligned}$$

α^3 ist Nullstelle von $X^5 + 1 = (X+1)(X^4+X^3+X^2+X+1)$
$g_1 = f_\alpha \cdot f_{\alpha^3} = X^8 + \ldots$ ist Generatorpolynom eines zyklischen Codes C_1

$$(15, 7) - \text{Code} \qquad dim C_1 = 7 \qquad |C_1| = 2^7$$

$$C = \{c = [c_0, \ldots, c_{n-1}] \mid c(\alpha) = c(\alpha^2) = c(\alpha^3) = c(\alpha^4)\}$$

Minimaldistanz ≥ 5 2 Fehler korrigierend
$f_{\alpha^5} = X^2 + X + 1 \qquad ord\alpha^5 = 3$ also ist α^5 Nullstelle von $X^3 - 1 = (X-1)(X^2+X+1)$
$f_{\alpha^6} = f_{\alpha^3}$

Setzt man $g_2 = f_\alpha \cdot f_{\alpha^3} \cdot f_{\alpha^5} = X^{10}$, so ist g_2 Generatorpolynom eines Codes C_2

$$(15, 5) - \text{Code} \qquad dim C_2 = 5$$

Minimaldistanz ≥ 7

Bei CDs werden Reed-Solomon Codes verwandt. $n = 2^8 - 1$ und Plandistanz ist 5.

Fehlerbündel korrigieren:
Speichere Informationen in $N \times n$-Matrizen und transponiere (oder sende spaltenweise)

$$N \begin{bmatrix} c_0 & \ldots & c_{n-1} \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots \end{bmatrix}$$

Kapitel 3

Graphen

06.07.MMI
(Fortsetzun

§ 1 Grundbegriffe

Definition 2
Ein Graph $G = (V, E)$ ist eine endliche nicht leere Menge V von **Knoten** (= **vertices**) mit einer Menge $E \subseteq \binom{V}{2} = \{M \subseteq V \mid |M| = 2\}$. Die Elemente von E heißen **Kanten** (= **edges**).

Beispiel 5

a)
$$V_n = (V = \{1, \ldots, n\}, \binom{V}{2})$$
ist der **vollständige Graph** mit n Knoten.

b)
$$V = \{1, 2, 3, 4\} \qquad E = (\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 1\}, \{2, 4\})$$
[Bild von $G = (V, E)$]

Definition 3
Ist $G = (V, E)$ ein **numerierter Graph**
$$V = \{v_1, \ldots, v_n\} \qquad E = \{e_1, \ldots, e_m\},$$
so heißt die $n \times n$-Matrix
$$A = [a_{ij}] \in \mathbb{Z}^{n \times n} \text{ mit } a_{ij} = \begin{cases} 1 & \text{für } \{v_i, v_j\} \in E \\ 0 & \text{sonst} \end{cases}$$
Adjazenzmatrix von G. [immer gilt $a_{ii} = 0$]

Und die Matrix

$$B = [b_{ij}] \in \mathbb{Z}^{n\times m} \text{ mit } b_{ij} = \begin{cases} 1 & \text{für } v_i \in e_j \\ 0 & \text{sonst} \end{cases}$$

Inzidenzmatrix von G.
Im Beispiel b):

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

allgemein
A ist immer symetrisch und die Diagonale besteht aus Nullen.

$$B = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$B \cdot B^T = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} = A + diag(2,3,2,3)$$

Definition 4

Ist $G = (V, E)$ Graph und $v \in V$, so sei $d(v) = deg(v) = |\{e \mid v \in e\}|$ **Grad** des Knotens v
Im Beispiel b) ist $d(1) = 2, d(2) = 3, d(3) = 2, d(4) = 3$.

Bemerkung

Ist A die Adjazenzmatrix und B die Inzidenzmatrix eines numerierten Graphen, so ist

$$B \cdot B^T = A + diag(d(v_1), \ldots, d(v_n))$$

Beweis

Für $i \neq j$:

$$\begin{aligned} (BB^T)_{i,j} &= (\sum_{k=1}^{m} \underbrace{\underbrace{b_{ik}b_{jk}}_{=0 \text{ außer für } v_i \in e_k \text{ und } v_j \in e_k}}_{\neq 0 \text{ nur für } e_k = \{v_i, v_j\}})_{ij} \\ &= A_{ij} \end{aligned}$$

Für $i = j$:

$$\begin{aligned} (BB^T)_{ii} &= \sum_{k=1}^{m} b_{ik}b_{ik} = \sum_{k=1}^{m} \underbrace{b_{ik}}_{=1 \Leftrightarrow v_i \in e_k} \\ &= d(v_i) \end{aligned}$$

Variationen:

Multigraph Mehrfachkanten
[Bild]
A_{ij} kann > 1 sein.

Graphen mit Schleifen [Bild]
A_{ii} kann $\neq 0$ sein.

gerichteter Graph $G = (V, E)$, wobei

$$E \subseteq V \times V = \{ \underbrace{(v_1, v_2)}_{\text{Kante von } v_1 \text{ nach } v_2} \mid v_1, v_2 \in V\}$$

Dann ist die Adjazenzmatrix nicht symetrisch.

Lemma 1
Handschlaglemma (Euler)
Ist (V, E) ein Graph (im Sinne von Definition 1), so gilt

$$\sum_{v \in V} d(v) = 2|E|$$

Beweis

$$\sum_{v \in V} d(v) = \sum_{i=1}^{n} \sum_{j=1}^{m} b_{ij} = \sum_{j=1}^{m} \underbrace{\sum_{i=1}^{n} b_{ij}}_{=2} = 2m = 2|E|$$

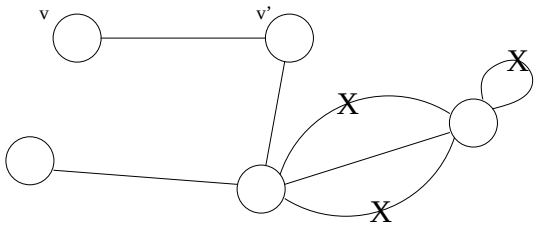
mit

$$V = \{v_1, \ldots, v_n\} \qquad E = \{e_1, \ldots, e_m\} \qquad [b_{ij}] = \text{ Inzidenzmatrix}$$

11.07.MMI

$G = (V, E)$ $\quad \emptyset \neq V$ endliche Menge von Knoten

$$E \subseteq \binom{V}{2} = \{\{v, w\} \mid v \neq v' \in V\}$$



$[d(v) = 1, d(v') = 2$, keine Mehrfachkanten$]$

$$d(v) =\mid \{e \in E \mid v \in E\} \mid$$

Lemma 2
Handschlaglemma (Euler)

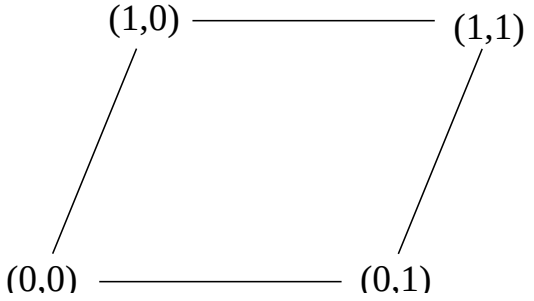
$$\sum_{v \in V} d(v) = 2 \mid E \mid$$

Definition 5
$G = (V, E)$ heißt k-**regulär**, wenn $d(v) =$ für alle $v \in V$.

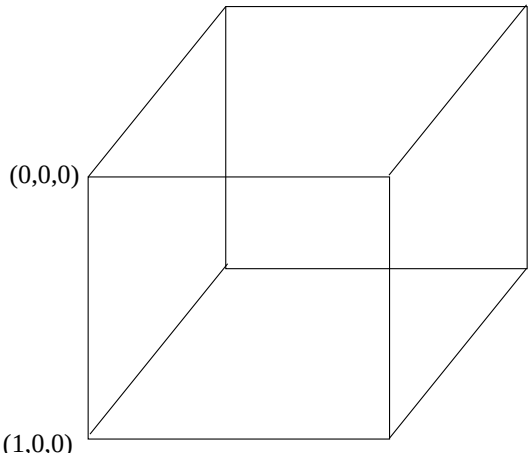
Beispiel 6
a) $V_n = K_n = (V, (\binom{V}{2}))$ $\quad \mid V \mid = n$ ist $(n-1)$-regulär.

b)

$$\begin{aligned} Q_n &= n - dim \textbf{ Hyperkubus} \\ &= (\mathbb{Z}_2^n, E_n) \\ E_n &= \{\{v, v'\} \mid v \neq v' \in \mathbb{Z}_2^n, \quad \underbrace{d(v, v')}_{\text{Hamming-Abstand}} = 1\} \end{aligned}$$



Q_2

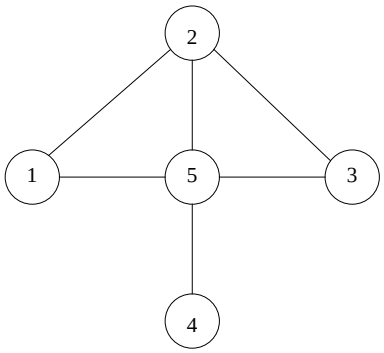


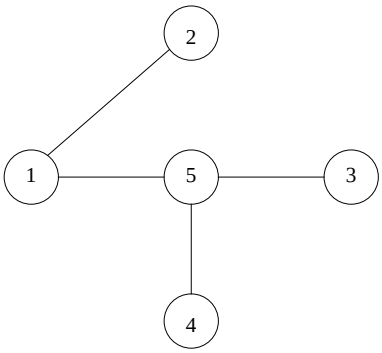
Q_3

Q_n ist n-regulär:

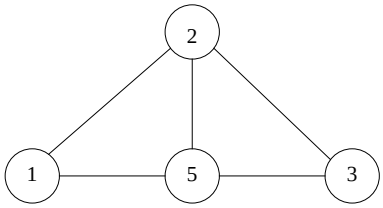
$$\begin{aligned} |\,\mathbb{Z}_2\,|^n \cdot n &= 2\cdot |\,E\,| \\ |\,E\,| &= n\cdot 2^{n-1} \end{aligned}$$

Definition 6
Ist $G=(V,E)$ ein Graph, so ist $G'=(V',E')$ ein **Teilgraph** von G, wenn $V'\subseteq V$ und $\binom{E'\subseteq E\cap(V}{2)}$. G' heißt **induzierter Teigraph**, wenn $\binom{E'=E\cap(V}{2)}$ in Zeichen $G'=G[V']$.





Teilgraph



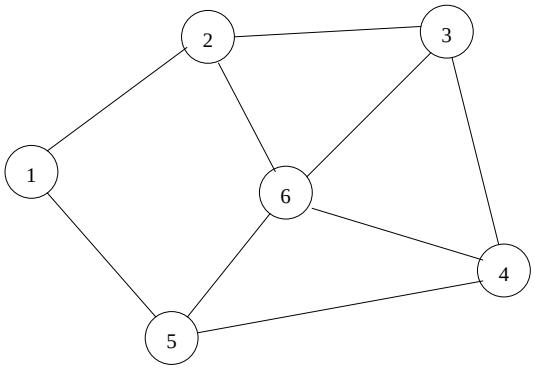
$G[\{1,2,3,5\}]$

§ 2 Wege und Kreise

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

Definition 7

- Ein **Weg** (**Kantenzug**) von v nach v' in V der Länge l ist eine Folge
$$w=(w_0,w_1,\ldots,w_l) \text{ mit } w_i\in V \text{ und } w_0=vw_l=v'$$
$$E(w)=\{\{w_{i-1},w_i\}\mid 1\le i\le l\}\subseteq E$$
- w heißt **Pfad** von v bach v', wenn $w_i\neq w_j$ für $i\neq j$
- w heißt **Kreis**, wenn $w_0=w_l$ und $w_i\neq w_j$ für $i\neq j$, $0\le i,j\le l-1$ und $l\ge 3$



Kreis: $(1,2,6,4,5,1)$, Weg: $1,2,6,3,4,6,5)$, aber kein Pfad.

Definition 8
$G = (V, E)$ heißt **zusammenhängend**, wenn es zu $v, v' \in V$ stets einen Pfad v nach v' gibt.

Bemerkung

a) Gibt es einen Weg von v nach nach v' in G, so auch einen Pfad.

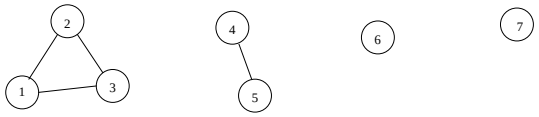
b) Definiert man auf V eine Relation

$$v \sim v' \Leftrightarrow \text{ Es gibt einen Pfad vo} v \text{ nach } v'$$

so ist $\sim$ eine Äquivalenzrelation. Sind $V_1, \ldots, V_s$ die Äquivalenzklassen bezüglich $\sim$ ist:

$$V = V_1 \dot\cup \ldots \dot\cup V_s$$
$$E = E \cap (\binom{V_1}{2}) \dot\cup \ldots \dot\cup E \cap (\binom{V_s}{2})$$

Die $G[V_i]$ induzierten Teilgraphen heißen dann **(Zusammenhangs) Komponenten** von G.



$G[\{1,2,3\}]$ $G[\{4,5\}]$ $G[\{6\}]$ $G[\{7\}]$

Satz 6
$G = (V, E)$ enthält mindestens $\mid V \mid - \mid E \mid$ Komponenten. G ist zusammenhängend, wenn $\mid E \mid \geq \mid V \mid -1$.

Beweis
Induktion nach $\mid E \mid = m$:

$m = 0$ $V = \dot\bigcup_{v_i \in V} \{v_i\}$ **Zerlegung in Komponenten**. Es gibt $\mid V \mid$ Komponenten.

$\mid E \mid = m > 0$ Sei $e \in E$ und $E' = E\ e \mid E' \mid = m - 1$. $G' = (V, E')$ hat nach Induktionsannahme $k \geq \mid V \mid -m + 1$ Komponenten. $G = (V, E)$ hat dann k oder $k - 1 \geq \mid V \mid -m$ Komponetn.

A ist Adjazenzmatrix eines **numerischen Graphen** $V = \{v_1, \ldots, v_n\}$.

$$A = [a_{ij \in \{1,\ldots,n} \text{ mit } a_{ij} \begin{cases} 1 & \text{für } \{i,j\} \in E \\ 0 & \text{sonst} \end{cases}$$

Satz 7
Ist $G = (V, E)$ nummerierster Graph mit Adjazenzmatrix A und ist:

$$A^r = \underbrace{A \cdot A \ldots \cdot A}_{r} = [a_{ij}^{(r)}] \qquad r \in N_0$$

So ist $a_{ij}^{(r)}$ = Anzahl der Wege von v_i nach v_j mit der Länge r.

Beweis
Induktion nach r:

$$r = 0 \quad A^0 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

$r > 0$

$$W_{ij}^{(r)} = \{w = (w_o, \dots w_r) \mid \text{ Weg von } v_i \text{ nach } v_j \text{ der Länge } r\}$$

$$(w_o, w_1, \dots, w_r) \to ((w_o, w_1), (w_1, \dots, w_r))$$

$$W_{ij}^{(r)} \to \dot{\bigcup}_{k=1}^{n} (W_{ik}^{(1)} \times W_{kj}^{(r-1)}) \qquad n = \mid V \mid$$

$$\begin{aligned} \mid W_{ij}^{(r)} &= \sum_{k=1}^{r} \underbrace{\mid W_{ik}^{(1)} \mid}_{a_{ik}} \underbrace{\mid W_{kj}^{(r-1)} \mid}_{a_{kj}^{r-1}} \\ &= (A \cdot A^{r-1})_{i,j} = (A^r)_{i,j} = a_{ij}^{(r)} \end{aligned}$$

Definition 9
Eine **Eulertour** in einem Graph $G = (V, E)$ ist ein "geschlossener" Weg $w = (w_o, w_1, \dots, w_m)$ mit $w_0 = w_m$ mit $E(w) = E$ und $m = \mid E \mid$. d.h. alle Kanten von G werden genau einmal durchlaufen. G heißt **eulersch**, wenn es eine Eulertour gibt.

Satz 8
Ein zusammenhängender Graph ist genau dann eulersch, wenn $d(v)$ gerade ist für alle $v \in V$.

Beweis

$\Rightarrow$ $w = (w_0, w_1, \dots, w_m)$ sei Eulertour. $E(w) = \{\{w_o, w_1\}, \{w_1, w_2\}, \dots, \{w_{m-1}, w_m\}\}$ für $v \in V$ setzte $n_v = \mid \{j \in \{0, \dots, m-1\} \; w_j = v\} \mid$ dann ist $d(v) = 2n_v \in 2\mathbb{N}$

$\Leftarrow$ Algorithmus zur Konstruktion einer Eulertour:

Bilde maximalen (d.h. nicht verlängerbaren) Weg $w = (w_0, w_1, \dots, w_r)$ mit $\mid E(w) \mid = r$. Dann muß $w_0 = w_r$ sein, dann – da $d(w_r) \in 2\mathbb{N}$ – gäbe es ein v mit $\{w_r, v\} \in E \setminus E(w)$ und man könnte w verlängern zu $(w_0, w_1, \dots, w_r, v)$

Also ist $w_0 = w_r$. Ist $E(w) = E$, so ist w eine Eulertour. Sonst gibt es $\{v, v'\} \in E \setminus E(w)$ und weil G zusammenhängend ist, $\{w_i, v\} \in E \setminus E(w)$ für ein $i \in \{0, \dots, r-1\}$. Bilde maximalen Weg $w' = (w_i = w'_0, w'_1, \dots, w'_s)$ in $(V, E \setminus E(w)$ mit $\mid E(w') \mid = s$. Wie oben ist $w'_0 = w'_s$. Ersetze w durch $w_1 = (w_0, \dots, w_i, w'_1, \dots, w'_s, w_{i+1}, \dots, w_r)$ und r durch $r + s$ und wiederhole den Algorithmus.

13.07.MMI

Beispiel 7
Gesucht seien die Eulertouren in $G = (V, E)$ mit

$$\begin{aligned} w &= (1,2,4,3,1) \\ w' &= (4,6,5,4) \\ w_1 &= (1,2,4,6,5,4,3,1) \\ w'' &= (5,3,2,5) \\ w &= (1,2,4,6,5,3,2,5,4,3,1) \text{ ist Eulertour} \end{aligned} \tag{3.1}$$

Beispiel 8
Kann man alle Dominosteine in einem Kreis/Rechteck auslegen?

$$\begin{aligned} D &= \{\{i,j\} \mid 0 \leq i,j \leq 6\}, |D| = 28 \\ V &= \{0,1,2,3,4,5,6\} \end{aligned} \tag{3.2}$$

$G' = (V, D)$ ist ein Graph mit Schleifen.

Es ist nun die Eulertour in G' gesucht, was gleichbedeutend ist mit der Suche einer Eulertour in K_7, dem vollständigen Graphen mit 7 Knoten. Dieser Graph ist 6-regulär und damit existiert nach dem Satz von Euler eine Eulertour.

Definition 10
Es sei $G = (V, E)$ ein Graph. Ein **Hamiltonpfad** (**Hamiltonkreis**) in G ist ein Pfad (bzw. Kreis), der alle Knoten V genau einmal durchläuft.

Gibt es einen Hamiltonkreis, so heißt G **hamiltonsch**, gibt es einen Hamiltonpfad in G, so heißt G **semi-hamiltonsch**.

Beispiel 9
Es gibt einen Hamiltonpfad im **Petersengraph**, aber keinen Hamiltonkreis, also nicht hamiltonsch.

Satz 9
Sei $G = (V, E)$ ein Graph mit $|V| \geq 3$. Dann gilt für $v \neq v'$ mit $\{v, v'\} \notin E$ stets

$$d(v) + d(v') \geq |V| - 1$$

so gibt es immer einen Hamiltonpfad.

i Gilt sogar

$$d(v) + d(v') \geq |V|$$

so gibt es immer einen Hamiltonkreis.

Beweis

a) Aus der Voraussetzung folgt, dass G zusammenhängend ist.

Wäre er nicht zusammenhängend, wähle $v \in V_1, v' \in V_2$ mit $V_1 \neq V_2$ Komponenten von G. Dann ist

$$d(v) \leq |V_1| - 1 \text{ und } d(v') \leq |V_2| - 1$$

$$\Rightarrow d(v) + d(v') \leq \underbrace{|V_1| + |V_2|}_{\leq |V|} \leq |V| - 2$$

b) Konstruktion eines Hamiltonpfades beginnend mit beliebiger Kante $\{w_1, w_2\} \in E$. $w = (w_1, w_2, \ldots, w_p)$ sei ein Pfad der Länge $p-1$. Ist p=n=—V—, so ist man fertig.

Gibt es $v \notin \{w_1, \ldots, w_p\} \in V$ mit $\{v, w_p\} \in E$ oder $\{v, w_1\} \in E$, so kann man w verlängern zu $(v, w_1, \ldots, w_p)$ oder $w_1, \ldots, w_p, v)$. Also können wir annehmen, es gibt kein $v \notin \{w_1, \ldots, w_p\}$ mit $\{v, w_p\} \in E$ oder $\{v, w_1\} \in E$

$$d(w_1) = k$$

Wir finden einen Kreis, der $w_1, \ldots, w_p$ enthält. Klar, wenn $\{w_1, w_p\} \in E$. Sonst ist für $j_k < p$ $\{w_{j_{i-1}}, w_p\} \in E$, so erhält man einen Kreis. Eine solche Kante muß existieren, denn sonst wäre

$$d(w_p) \leq p - q - k, \text{ also } d(w_1) + d(w_p) \leq p - 1 < |V| - 1$$

Man erhält also einen Kreis mit p Knoten.

$$\exists v \notin \{v_1, \ldots, v_p\} \text{ mit } \{v, v_j\} \in E$$

man erhält einen Pfad mit $p+1$ Knoten. Es gibt also einen Hamiltonpfad.

Unter Benutzung von $d(v_1) + d(v_n) \geq n = |V|$ erhält man wie oben einen Hamiltonkreis.

Beispiel 10
Angenommen es gibt 7 Prüfungen und kein Dozent prüft mehr als 3 mal. Der zugehörige Graph ist

$$V = \{1, \ldots, 7\} \text{ mit } |V| = 7 \text{ und } E = \{\{i, j\} \mid Pr_i \neq Pr_j\}$$

$$d(i) \geq 3$$

18.07.MMI

§ 3 Bäume und Wälder

Definition 11
Ein Graph $G = (V, E)$ heißt **Baum**, wenn er zusammenhängend ist und keine Kreise enthält.
Ein Graph, dessen sämtliche Komponenten Bäume sind, heißt **Wald**.
Ein **gewurzelter Baum** ist ein Baum zusammen mit einem ausgezeichneten Knoten (G, v_0).

Satz 10
Äquivalent sind für einen Graphen $G = (V, E)$:

a. G ist ein Baum

b. zu $v, v' \in V \quad v \neq v'$ existiert genau ein Pfad von v nach v'.

c. $|E| = |V| - 1$ und G ist zusammenhängend.

Beweis
a. $\Rightarrow$ **b.** Da G zusammenhängend ist, existiert ein Pfad von v nach v'. Gitb es 2 verschiedene Pfade, so erhielte man einen Kreis.

b. $\Rightarrow$ **a.** Nach Vorrausetzung ist G zusammenhängend. Wäre ein Kreis vorhanden, so erhielte man 2 Pfade von v_1 nach v_2, wenn $e = \{v_0, v_1\}$ im Kreis vorkommt.

a. $\Rightarrow$ **c.** Induktion

c. $\Rightarrow$ **a.** weggelassen

Satz 11
Ist $G = (V, E)$ ein zusammenhängender Graph, so enthält G einen **aufspannenden Baum** T, d.h. $T = (V, E')$ mit $E' \leq E$ (und T ist Baum).

Beweis

a. Enthält G keinen Kreis, so setze $T = G$, sonst wähle Kreis $(v_0, v_1, \ldots, v_n, v_0)$.

$G' = (V, E \backslash \{v_0, v_1\})$ ist zusammenhängend.

Iteriere.

b. Algorithmus (**Breitensuche**)
Initiere: $S = (v_0)$ $v_0 \in V$ $V' = \emptyset, E' = \emptyset$

`while` $S = (\quad)$ `do`
$v = S[1] =$ `erstes Element der Liste` S
$E'' = \{\{v, v'\} \in E \mid v' \notin V'$
$V' := V' \cup \{v' \mid \{v, v'\} \in E''\} \cup \{v\}$
$E' := E' \cup \{\{v, v'\} \in E \mid v' \notin V'\}$
`lösche` v `in der Liste` S
`hänge an` S `die Liste` $(v' \mid \{v, v'\} \in E')$ `an`
`od;`

Aufgabe: Finde alle Bäume mit Knotenmenge $V = \{v_1, v_2, \ldots, v_n\} (= \{1, 2, \ldots, n\})$
äquivalent: Finde alle aufspannenden Bäume des Graphen $(V, \binom{V}{2}) = K_n$.

$n = 2$

$n = 3$

$n = 4$

Satz 12
Cayley

Die Anzahl aller Graphen mit $V = \{1, 2, \ldots, n\}$ ist n^{n-2}.

Beweis

a. Jedem Baum T auf $V = \{1, 2, \ldots, n\}$ ist n^{n-2} wird ein Element $P(T) = (t_1, \ldots, t_{n-2}) \in V^{n-2}$, genannt **Prüfercode** von T, zugeordnet nach folgendem Algorithmus:

Gegeben: Baum T

Weg In T existiert immer ein $v_0 \in V$ mit $d(v_0) = 1$. v_0 heißt **Blatt**. Wähle einen maximalen (d.h. nicht verlängerbaren) Pfad $(v_0, v_1, \ldots, v_m)$, dann ist $d(v_0) = 1 = d(v_m)$ `for` i `in` $[1, \ldots, n-2]$ `do`
`wähle kleinstes` $v \in V$ `mit` $d(v) = 1$
`es gibt dann genau ein` $v' \in V$ `mit` $\{v, v'\} \in E$
`setze` $t_i = v'$
$V = V \backslash \{v\}$
`od;`

$P(T) = (2, 4, 2, 4, 4, 8)$
gestrichene Knoten (in dieser Reihenfolge) $1, 3, 5, 2, 6, 4$
Bem: Ist $P(T) = (t_1, \ldots, t_{n-2})$ und $n_j = |\{i \in \{1, \ldots, n-2\} \mid t_i = j\}|$ $j \in \{1, \ldots, n\}$, so $d(j) = n_j + 1$.
Umgekehrt sei $t = (t_1, \ldots, t_{n-2})$ $t_i \in \{1, \ldots, n\}$ gegeben. Wir konstruieren einen Graphen (Baum) mit folgendem Algorithmus:
`Initiere` $E' = \emptyset$
`Sei` $i = Min\{j \in V \mid j \notin T\}$
$E' := E' \cup \{\{i, t_i\}\}$
`Ersetze` t `durch` $t = (t_2, \ldots, t_{n-1})$
`Ersetze` V `durch` $V \backslash \{i\}$
`wiederhole dies bis` $t = (\quad)$
`Dann` $E' = E' \cup V$ $|V| = 2$ `hier (in diesem Stadium)`

Damit erhält man Baum T mit $P(T) = t$

Beispiel 11

$$t = (1, 3, 3, 1, 1, 4) \qquad V = \{1, 2, 3, 4, 5, 6, 7, 8\}$$

Definition 12
Zwei Graphen $G = (V, E)$ und $G' = (V', E')$ heißen **isomorph**, wenn es eine Bijektion $\psi : V \to V'$ gibt, mit $\{\{\psi(v_i), \psi(v_j)\} \mid \{v_i, v_j\} \in E\} = E'$

Isomorphieklassen von Bäumen mit n Knoten:

$n = 2$

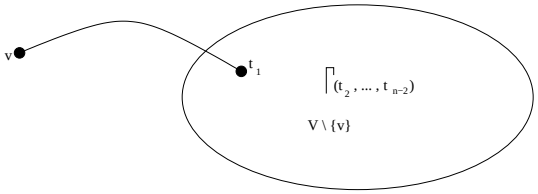
$n = 3$

$n = 4$

$n = 5$

20.07.MMI

Satz 13
Calay Die Anzahl der Bäume auf V mit $\mid V \mid = n$ ist n^{n-2}. $(t_1, \ldots, t_{n-2}) t_i \in V \mid V \mid = n$ $\Gamma_v(t_1, \ldots, t_{n-2})$



ensteht aus $\Gamma_{V \backslash \{v\}}(t_2, \ldots, t_{n-2})$ durch "Anheften" des Blattes v an t_1 wobei $v = Min\{v \in V \mid v \notin \{t_1, \ldots, t_{n-2}\}\}$

§ 4 Planare Graphen

Definition 13
Eine ebene Einbetung eines Graphen $G = (V, E)$ ist eine Paar ψ, ψ' von injektiven Abbildungen.

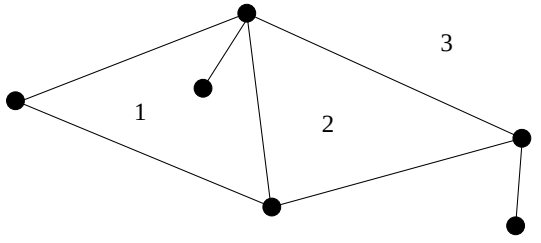
$$\psi : V \to \mathbb{R}^2$$

$$\psi' : E \to J = \{Bild \mid \epsilon : [0,1] \to \mathbb{R}^2 \text{ injektiv}\} \text{ stetig - Jordankurven}$$

$$\text{mit } \psi' \underbrace{v, v'}_{\in E} = Bild\epsilon\{\psi(v), \psi(v')\} = \{\epsilon(0), \epsilon(1)\}$$

$$\text{und } \psi'(\underbrace{v_1, v_2}_{\in E}) \wedge \psi'(\underbrace{v_3, v_4}_{\in E}) = \bigcap_{i=1}^{n} \{\psi(v_i)\}$$

G heißt planar, wenn so eine planare Einbettung gibt.



$g = 3$ Gebiete

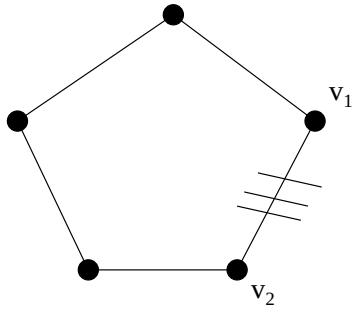
Ist (G, ψ, ψ') ein eingebetter Graph so heißen die Zusammenhangskomponeten von $\mathbb{R}^2 \setminus \bigcup_{e \in E} \psi'(e)$ **Gebiete** von (G, ψ, ψ').

Satz 14
Eulersche Polyederformel Ist (G, ψ, ψ') ein zusammmenhängender eingebetter Graph, so gilt:

$$g = \text{ Anzahl der Gebiete } = \mid E \mid - \mid V \mid + 2$$

Beweis
Induktion nach $\mid E \mid$

- $\mid E \mid = 0$ dann ist $\mid V \mid = 1$, $g = 1$
- Sei $\mid E \mid > 0$.
  - Ist G ein Baum, so ist $\mid E \mid - \mid V \mid = -1$ und $g = 1$
  - Sonst hat G einen Kreis, sei $e = \{v_1, v_2\} \in E$ Kante in einem Kreis.



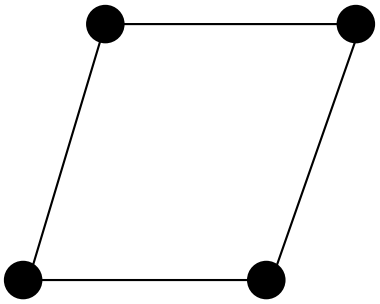
$G' = (V, E' = E\backslash\{e\})$ ist zusammenhängend und eingebettet. G' hat $g - 1$ Gebiete, wenn G genau g Gebiete hat, da e nicht mehr 2 Gebiete trennt.

$$g - 1 \underbrace{=}_{\text{Ind. Ann.}} \mid E' \mid - \mid V \mid +2 = \mid E \mid - \mid V \mid +2 - 1$$

Satz 15
Ist $G = (V, E)$ planar, so ist:

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

Beweis
Sei $\{\psi, \psi'\}$ Einbettung mit g Gebieten. Jedes Gebeit wird von mindestens § Kanten berandet. Jede Kante berandet höchstens 2 Gebiete.



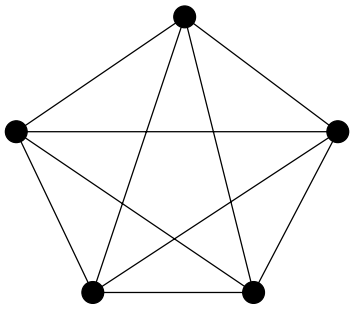
$$2 \mid E \mid \geq \mid \{(R, e) \mid R \text{ Gebiet und } \psi'(e) \in \underbrace{einlustigerbuchstaben}_{\text{Rand}} R\} \mid \geq 3g$$

Einsetzen in

$$g = \mid E \mid - \mid V \mid +2 \leq \frac{2}{2 \mid} E \mid$$

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

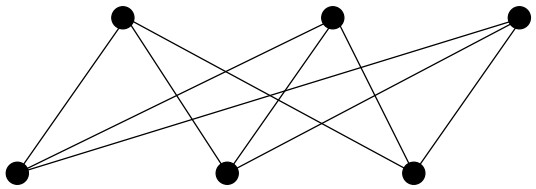
Beispiel 12
a)



K_5

$\mid E \mid = 10, \mid V \mid = 5, 3 \mid V \mid -6 = 9 \Rightarrow K_5$ ist nicht planar.

b) $K_{m,n} = (V_1 \dot{\cup} V_2, E), \mid V_1 \mid = m, \mid V_2 \mid = n, E = \{\{v_1, v_2\} \mid V - 1 \in V_1, v_2 \in V_2\}$ heißt **vollständig bipartiter Graph**.

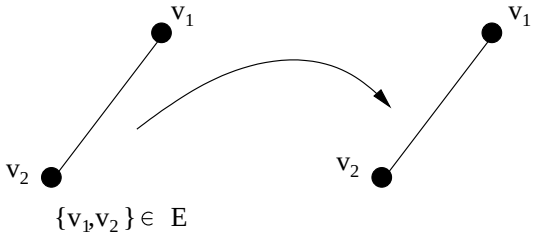


$G = K_{3,3} = (V, E)$

$\mid V \mid = 6, \mid E \mid = 9, 3 \mid V \mid -6 = 12 \Rightarrow$ Bedingung von Satz 2 ist erfüllt. In jeder Einbettung von G wird jedes Gebiet von ≥ 4 Kanten berandet (denn es gibt in G keinen Kreis der Länge 3). Der Beweis von Satz 2 liefert:

$$\begin{aligned} \mid E \mid - \mid V \mid +2 &\leq \frac{2}{4} \mid E \mid \\ 9 = \mid E \mid &\leq 2 \mid V \mid -4 = 12 - 4 = 8 \end{aligned}$$

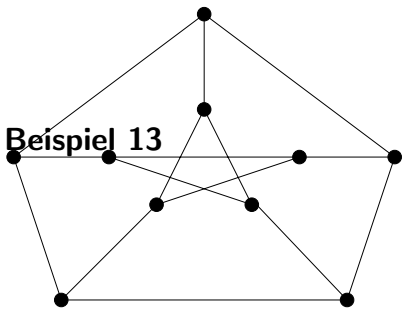
Definition 14
Graphen, die durch endlich viele Operationen der Form:



oder ihre Umkehrung "Entfernung von Knoten von Grad 2" heißen 2**-äquivalent**.

Satz 16
Kuratowski Ein Graph G ist genau dann planar, wenn er keine Teilgraphen enthält, der 2-äquivalent zu K_5 oder $K_{3,3}$ ist.

Beispiel 13



Teilgraph 2-äquivalent zu $K_{3,3}$.

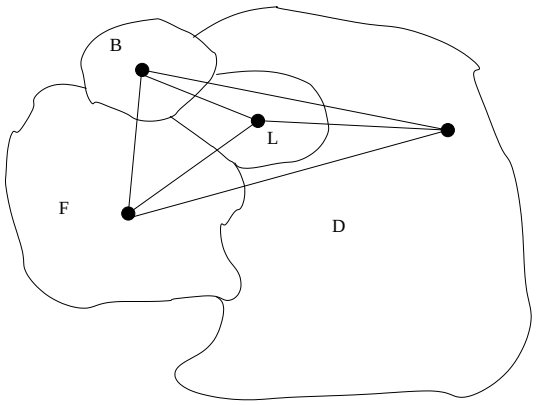
Definition 15
Eine **(Kanten-)Färbung** eines Graphen $G = (V, E)$ mit $k \in \mathbb{N}$ Farben ist eine Abbildung

$$c : V \to \{1, \ldots, k\}$$

mit $c(v) \neq c(v')$ falls $\{v, v'\} \in E$. G ist k-färbbar, wenn es eine Färbung mit k Farben gibt.

$$\chi(G) = Min\{k \mid G \text{ ist } k\text{-färbbar}\}$$

[bipartiter Graph = Graph gefärbt mit 2 Farben].
Färbung von Landkarten: "benachbachte Länder sollen verschieden gefärbt werden"



$K_4, \chi(K_4) = 4$

Satz 17
Vierfarbensatz Ist G planar, so ist $\chi(G) \leq 4$. [Appel, Hacken 1976 (Four colors suffice)]

Liebe Mitstudierenden (und natürlich die, die es werden wollen und alle anderen auch):

Wir sind auf Eure Einsendungen von **Fehlern und Korrekturen** angewiesen, um eine möglichst fehlerfreie Mitschrift anbieten zu können. Es wäre wirklich "total dufte" :) von Euch, wenn ihr uns Fehler, die Euch auffallen

zumailt/schickt/...

Kontaktaufnahme siehe erste Seite oder www.drstf.de

Anhang A

Zahlentafeln

§ 0.1 Stirling Zahlen 2. Art, $S_{n,k}$

Stirling'sches Dreieck 2. Art, $S_{n,k}$

$n\backslash k$	0	1	2	3	4	5	6
0	1						
1	0	1					
2	0	1	1				
3	0	1	3	1			
4	0	1	7	6	1		
5	0	1	15	25	10	1	
6	0	1	31	90	65	15	1

§ 0.2 Stirling Zahlen 1. Art, $s_{n,k}$

Stirling'sches Dreieck 1. Art, $s_{n,k}$

$n\backslash k$	0	1	2	3	4	5	6	7
0	1							
1	0	1						
2	0	1	1					
3	0	2	3	1				
4	0	6	11	6	1			
5	0	24	50	35	10	1		
6	0	120	274	225	85	15	1	
7	0	720	1764	1624	735	175	21	1

Anhang B

Zeichen

$\dot{\cup}$	*lies: „disjunkt vereinigt“* $A \dot{\cup} B = A \cup B \Leftrightarrow A \cap B = \emptyset$ Bsp: $A = \{a, c, e\}, B = \{b, d\}, A \dot{\cup} B = \{a, b, c, d, e\}$, denn $A \cap B = \emptyset$
$\times$	*lies: „kreuz“* $A \times B = \{(a, b) \mid a \in A, b \in B\}$
$n^{\underline{\mathrm{m}}}$	*lies: „n hoch m fallend“* $n^{\underline{\mathrm{m}}} = n \cdot (n-1) \cdot \ldots \cdot (n-m+1)$
$a \mid b$	(*lies: „‘“a* teilt *b”*) $a \mid b \Leftrightarrow \exists z \in R$ mit $b = a \cdot z$

Index