# Inhaltsverzeichnis

# Kapitel 1

# Abzählung, Rekursionen, erzeug. Funktionen

## 1.1 Elementare Zählprinzipien

(18.04.01)

M bezeichnet endliche Menge
$|M|$ = Anzahl der Elemente von M
$|A| = n \in \mathbb{N} = \{1, 2, 3, \ldots\} \Leftrightarrow$ Es gibt eine Bijektion $\alpha : A \to \{1, \ldots, n\}$
$|A| = 0 \Leftrightarrow A = \emptyset$

**Lemma 1:**

a) $|A| = |B| \Leftrightarrow$ Es gibt eine Bijektion $\alpha : A \to B$

b) $|A \dot\cup B| = |A| + |B|, A \dot\cup B$ disjunkte Vereinigung, d.h. es gilt $A \cap B = \phi$

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

**Folgerung:** Abb(A,B) $= B^A =$ Menge aller Abbildungen von A nach B
$|B^A| = |B|^{|A|}$

**Beweis:**

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

$$B^A \to \underbrace{B \times B \times \ldots \times B}_{n-mal}$$

$$f \to (f(a_1), f(a_2), \ldots, f(a_n)) \text{ ist Bijektion}$$

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

**Def.:** $f : A \to A$ heisst Permutation von A, wenn f bijektiv
$S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \mid \sigma \text{ bijektiv}\} = Sym\{1, \ldots, n\}$
"symmetrische Gruppe vom Grad n"

**Lemma 2:** $|S_n| = n! = 1 \cdot 2 \cdot \ldots \cdot n$ (= Anzahl der Möglichkeiten, eine n-Menge A (d.h. Menge A mit $|A| = n$) anzuordnen) (s. Lin. Alg. I)

**Beweis:**

$$\sigma \mapsto (\sigma(1), \ldots, \sigma(n))$$

$$S_n \to \{(i_1, \ldots, i_n) \mid i_j \in \underline{n}, i_j \neq i_k \text{ für } j \neq k\} \text{ (bijektiv)}$$
$$= \{(i_1, \ldots, i_n) \mid \{i_1, \ldots, i_n\} = \{1, \ldots, n\}\}$$
$$|S_n| = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$$

**Satz 1:** Die Anzahl der Teilmengen einer n-Menge A ist $2^n$
$|A| = n, |P(A)| = 2^n$ , dabei ist $P(A) = \{B \mid B \subseteq A\}$ Potenzmenge von A

**Beispiel:** A = {1,2} , P(A) = {{1,2}, {1}, {2}, ∅}

**Beweis:** $P(A) \to \{0,1\}^A$ (= Abb(A, {0,1}))
$B \mapsto \chi_B$ charakteristische Funktion von B definiert durch

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

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

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

**Bemerkung:**

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

Also nach Lemma 1 ist

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

**Lemma 3:**

$$|P_k(A)| = \left|\binom{A}{k}\right| = \binom{n}{k} \text{Binomialkoeffizient} = \frac{n(n-1)\ldots(n-k+1)}{k!} \text{ , falls } |A| = n$$

**Beweis:**

$$B = \{b_1, \ldots, b_k\}, |B| = k, b_i \neq b_j \text{ für } i \neq j, b_i \in A$$
$$|\{(b_1, \ldots, b_k) | b_i \in A, b_i \neq b_j \text{ für } i \neq j\}| = n(n-1)\ldots(n-k+1)$$
Es gibt k! Anordnungen von $\{b_1, \ldots, b_k\}$

**2. Beweis von Satz 1:** (Binomialsatz)

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

**Satz 2:**

a) (Pascal-Dreieck)

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

b) (Vandermondesche Identität)

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

**Beweis:** 1.) $n \geq 1, |A| = n, \binom{n}{k}$= Anzahl der k-Teilmengen von $A, b \in A$

$$\binom{A}{k} = \{X \in A | b \notin X, |X| = k\} \dot\cup \underbrace{\{X \subseteq A | b \in X, |X| = k\}}_{=:M} = \binom{A\backslash\{b\}}{k} \dot\cup M$$

$$\begin{matrix} M \to \binom{A\backslash\{b\}}{k-1} \\ X \mapsto X\backslash\{b\} \end{matrix} \text{ ist Bijektion}$$

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

2.) $|A| = m + n, A = B \dot\cup C, |B| = m, |C| = n$

$$\binom{A}{k}_l = \{X \subseteq A || X| = k, |X \cap B| = l\}, l = 0, 1, \ldots, k$$

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

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

(20.04.01)

$|M| = n \in \mathbb{N}_0 = \{0, 1, \ldots\}$
$\binom{M}{k} = A \subseteq M || A| = k = \emptyset$ für $k > n, k < 0$
$\left|\binom{M}{k}\right| = \binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!}$ für $k \geq 0$
$= \frac{n!}{k!(n-k)!}$ für $n \geq k \geq 0$

**Lemma 4:**

a) [Doppeltes Abzählen] Ist $R \subseteq M \times N$, so ist

$$|R| = \sum_{a \in M} |\{b \in N | (a, b) \in R\}| = \sum_{b \in N} |a \in M | (a, b) \in R|$$

b) [Schubfachprinzip] $|M| > |N|$, Ist $f : M \to N$, so ist f nicht injektiv, d.h. $\exists\, b \in N$ mit $|f^{-1}(b)| = |\{a \in M | f(a) = b\}| > 1$

c) [Inklusions-Exklusions-Prinzip] $A_1, \ldots, A_n \subseteq M$

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{i_1 < i_2} |A_{i_1} \cap A_{i_2}| + \sum_{i_1 < i_2 < i_3} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \ldots$$

$$= \sum_{j=1}^{n} (-1)^{j-1} \sum_{1 \leq i_1 < \ldots < i_j \leq n} |A_{i_1} \cap \ldots \cap A_{i_j}|$$

**Beweis zu 3.):** $A \subseteq M, \chi_A : M \to \{0, 1\} : x \mapsto \begin{cases} 1 & \text{falls } x \in A \\ 0 & \text{sonst} \end{cases}$

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

$$\chi_{A_1\cup\ldots\cup A_n}(x) = \sum_{j=1}^{n}(-1)^{j-1} \sum_{1\le i_1<\ldots<i_j\le n} \chi_{A_{i_1}\cap\ldots\cap A_{i_j}}(x) \tag{1.1}$$

Daraus folgt Beh. durch Summation über M
Ist i) $x \notin A_1 \cup \ldots \cup A_n$ , so ist: Linke Seite von (1.1) = 0, Rechte Seite = 0
ii) $x \in A_1 \cup \ldots \cup A_n$ , so ist: Linke Seite = 1
$x$ liege in genau $k$ Teilmengen $(k \geq 1) A_1, \ldots, A_n$, d.h.

$$x \in A_{j_1} \cap \ldots \cap A_{j_k}, j_1 < \ldots < j_k$$

dann ist

$$\chi_{A_{i_1}\cap\ldots\cap A_{i_j}}(x) = 1 \Leftrightarrow \{i_1, \ldots, i_j\} \leq \{j_1, \ldots, j_k\}$$

$$\text{Rechte Seite } = \sum_{j=1}^{n}(-1)^{j-1}\binom{k}{j} = 1 - \underbrace{\sum_{j=0}^{k}(-1)^{j}\binom{k}{j}}_{(1-1)^k} = 1$$

## 1.2 Partition

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

$P = \{A_1, \ldots, A_k\}$ Partition von $M$ , wenn $M = A_1 \dot\cup \ldots \dot\cup A_k$ und $A_i \neq \emptyset$ für $i = 1, \ldots, k$

$Part_k(M) := \{P | P \text{ ist Partition von } M \text{ , } |P| = k\}$ Menge der $k$-Partitionen von $M$

$S_{n,k} = |Part_k(M)|$ falls $|M| = n$ und $n, k \geq 0$ "Stirling-Zahlen 2. Art"

$S_{0,0} = 1$

**Beispiele:** $S_{n,0} = 0$ , $n \geq 1$
$S_{n,1} = 1$ , $n \geq 1$
$S_{n,k} = 0$ , $k > n$
$S_{n,n} = 1$
$S_{n,n-1} = \binom{n}{2}$

**Satz 1:** Es gilt für $1 \leq k \leq n$

$$S_{n,k} = S_{n-1,k_1} + k \cdot S_{n-1,k}$$

(25.04.01)

(Wiederholung)

$M$ endliche Menge, $|M| = n > 0$
$Part_k(M) = \{P = \{A_1, \ldots, A_k | \emptyset \neq A_i \subseteq M, M = A_1 \dot\cup \ldots \dot\cup A_k\}\}$
$Part_1(M) = \{\{M\}\}$
$Part_2\{1,2,3,4\} = \{\{\{1\},\{2,3,4\}\},\{\{2\},\{\{1,3,4\}\},\{\{3\},\{1,2,4\}\},\{\{4\},\{1,2,3\}\},$
$\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$
$Part_2(M) = \{\{A, M\backslash A\} | \emptyset \neq A \subset M, A \neq M\}, |Part_2(M)| = \frac{1}{2}(2^n - 2) = 2^{n-1} - 1$
$S_{n,k} = |Part_k(M)|$ für $|M| = n$ "Stirlingzahlen 2. Art"

**Satz 1:** Für $n \geq k \geq 1$ gilt:

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

(Ende Wiederholung)

**Beweis:** $a \in M, |M| = n \geq 1, Part_k(M) = X_1 \dot\cup X_2$, wobei

$$X_1 = \{P \in Part_k(M) | \{a\} \notin P\}, X_2 = \{P \in Part_k(M) | \{a\} \in P\}$$

$$\Rightarrow X_2 = \{P = \{\{a\}, B_1, \ldots, B_{k-1}\} | \{B_1, \ldots, B_{k-1}\} \in Part_{k-1}(M \backslash a)\}$$

$$\Rightarrow |X_2| = S_{n-1,k-1}$$

Ist $P \in X_1$, dann erhält man durch Löschen von $a$ eine Partition $\{B_1, \ldots, B_k\}$ von M $\backslash a$. Umgekehrt erhalten wir zu jedem $\{B_1, \ldots, B_k\} \in Part_k(M \backslash a)$ genau $k$ verschiedene Partitionen aus $X$, nämlich $\{\{a\}, B_1, B_2, \ldots, B_k\}, \ldots, \{B_1, B_2, \ldots, B_k \cup \{a\}\}$
$|X_1| = k \cdot S_{n-1,k}$ Bez. bei Knuth: $S_{n,k} = \left\{ \begin{array}{c} n \\ k \end{array} \right\}$

**Bem:**

a) {Partitionen von M} $\leftrightarrow$ {Äquivalenzrelationen auf M} (Bijektion)

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

$$b \in N, f^{-1}(b) = \{a \in M | f(a) = b\} \neq 0$$

$$\Rightarrow M = \dot{\bigcup_{b \in N}} f^{-1}(b), P_f = \{f^{-1}(b) | b \in N\} \in Part_{|N|} M$$

**Satz 2:** Ist $|M| = m$ und $|N| = n$, dann gilt:

a) $|Abb(M, N)| = |N^M| = n^m$

b) $| \underbrace{Inj(M, N)} | = n^{\underline{m}} = n(n-1)\ldots(n-m+1)$ "n hoch m fallend"
Menge aller inj. Abb.

c) $| \underbrace{Surj(M, N)} | = n! S_{m,n}$
Surj. Abb.

**Beweis:**

a) s. Kapitel 1.1

b) $M = \{a_1, \ldots, a_m\}$ Jede Abb. $f : M \to N$ ist gegeben durch
$$\begin{array}{r} f(a_1) = b_1 \in N \\ \vdots \\ f(a_m) = b_m \in N \end{array}$$

$f$ injektiv $\Leftrightarrow b_i \neq b_j$ für $i \neq j$

$$\begin{array}{cc} \text{Für } b_1 \text{ gibt es } n \text{ Möglichkeiten} & b_1 \in N \\ \text{Für } b_2 \text{ gibt es } n-1 \text{ Möglichkeiten} & b_2 \in N \backslash \{b_1\} \\ \vdots & \vdots \\ \text{Für } b_m \text{ gibt es } n-m+1 \text{ Möglichkeiten} & b_m \in N \backslash \{b_1, \ldots, b_{m-1}\} \end{array}$$

c) $f : M \to N$ surjektiv

$$P_f = \{f^{-1}(b) | b \in N\} \in Part_n(M)$$

$$= \{A_1, \ldots, A_n\}$$

$$P_f = P_g \Leftrightarrow g = \sigma \cdot f \text{ mit } \sigma \in S_n \text{ (orig.: } SymN \text{ )}$$

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

**Beispiel:** $Surj(\underbrace{\{1,2,3\}}_{M}, \underbrace{\{1,2\}}_{N})$

$$|Surj(M,N)| = S_{3,2} \cdot 2! = 6$$

**Bemerkung:**

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

$f$ kann man auffassen als surj. Abb.

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

$$n^m = |Abb(M,N)| = \sum_{A \subseteq N} |Surj(M,A)| = \sum_{k=0}^{n} \sum_{A \in \binom{N}{k}} |Surj(M,A)|$$

$$= \sum_{k=0}^{n} \binom{n}{k} k! S_{m,k} = \sum_{k=0}^{n} \frac{n^{\underline{k}}}{k!} k! S_{m,k}$$

**Satz 3:** $n^m = \sum_{k=0}^{n} n^{\underline{k}} S_{m,k}$ für $m, n \in \mathbb{N}$

## 1.3 Permutationen

$$S_n = Sym(\underline{n}) = \{\sigma : \{1,\ldots,n\} \to \{1,\ldots,n\} | \sigma bij.\}$$

$$|S_n| = n!$$

Jedes $\sigma \in S_n$ kann durch eine Wertetabelle angegeben werden, z.B.:

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

**Bemerkung:** $(S_n, \circ)$ ist eine Gruppe.

$$\sigma_1, \sigma_2 \in S_n$$

$$\sigma_1 \circ \sigma_2 : \{1,\ldots,n\} \to \{1,\ldots,n\} : x \mapsto \sigma_1(\sigma_2(x))$$

$$\sigma^2 = \sigma \circ \sigma$$

**Definition:** Ein k-Zyklus $(i_1,\ldots,i_k) = \sigma \in S_n$ ist eine Permutation mit folgender Eigenschaft:

$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$ und $\sigma(i) = i$, falls $i \notin \{i_1,\ldots,i_k\}$

$$\text{mit } \{i_1,\ldots,i_k\} \in \{1,\ldots,n\}$$

**Beispiel:** $\sigma$ wie im Beipiel oben:

$$\sigma = (142376) \circ (59)(8)$$

(8) kann auch weggelassen werden

**Bemerkung:** Jedes $\sigma \in S_n$ lässt sich als Produkt von Zyklen schreiben.

**Beispiel:**

$$S_3 = \{\underbrace{(1)(2)(3)}_{id}, (1)(23), (2)(13), (3)(12), (123), (132)\}$$

**Definition:** Die Stirling-Zahlen $s_{n,k}$ 1. Art geben die Anzahl der Permutationen von {1,. . . , n} an, die genau k (disjunkte) Zyklen haben, z.B.: $s_{3,1} = 2, s_{3,2} = 3, s_{3,3} = 1$

(27.04.01)

**Definition:** Ein r-Zyklus $\zeta = (i_1, \ldots, i_r)$ ist eine Permutation $\zeta = s_n$ mit "Ziffernmenge" $Z(\zeta) = \{i_1, \ldots, i_r\}$ mit $|Z(\zeta)| = r$ und $\zeta(i_1) = i_2, \zeta(i_2) = i_3, \ldots, \zeta(i_r) = i_1$ und $\zeta(i) = i für i \notin Z(\zeta)$

$$Perm_k(\underline{n}) = \{\sigma \in s_n | \sigma = \zeta_1 \circ \ldots \circ \zeta_k \text{ mit } Z(\zeta_1) \dot{\cup} \ldots \dot{\cup} Z(\zeta_k) = \{1, \ldots, n\} = \underline{n}\}$$

**Bemerkung:**

a)

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

$$(1234) = (2341) = (3412) = (4123)$$

b) $\zeta_1, \zeta_2$ disjunkt, d. h. $Z(\zeta_1) \cap Z(\zeta_2) = \emptyset \Rightarrow \zeta_1 \circ \zeta_2 = \zeta_2 \circ \zeta_1$ z.B.:

$$\begin{array}{ccc} (12) \circ (34) & = & (34) \circ (12) \\ (12) \circ (23) & \neq & (23) \circ (12) \\ = & & = \\ (123) & & (132) \end{array}$$

**Definition:**

$$s_{n,k} = |Perm_k(\underline{n})| \text{ mit } n, k \geq 1 \text{ , "Stirling-Zahlen 1. Art"}$$

$$s_{0,0} = 1, s_{o,k} = 0 \text{ für } k > 0$$

**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 2.) $Perm_n(\underline{n}) = \{(1) \circ (2) \circ \ldots \circ (n) = id\}$
zu 3.) $Perm_1(\underline{n}) = \{(n i_2 \ldots i_n) || \{i_2, \ldots, i_n\}| = n-1\}$ $|Perm_1(\underline{n})| = (n-1)!$

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

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

**Beweis:**

$$X = Perm_k(\underline{n}) = X_1 \dot{\bigcup} X_2 \text{ , für } n \geq 1$$

$$X_1 = \{\sigma \in X | \sigma(n) = n\} = \{sigma = (n) \circ \zeta_1 \circ \ldots \circ \zeta_{k-1} | \zeta_1 \circ \ldots \circ \zeta_{k-1} \in Perm_{k-1}(\underline{n-1})\}$$

$$|X_1| = s_{n-1,k-1}$$

$$X_2 = \{\sigma \in X | \sigma(n) \notin n\}$$

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

$$\tau = \underbrace{(i_1 \ldots i_r) \circ (i_{r_1+1} \ldots i_{r1+r_2}) \circ \ldots \circ (i_{r_1+r_{k-1}+1} \ldots i_{n-1})}_{\text{k-Zyklen der Länge } r_1, r_2 \ldots r_k \in Perm_k(\underline{n-1})}$$

Umgekehrt liefert jedes solche $\tau \in Perm_k(\underline{n-1})$ genau n - 1 Elemente $r$ aus $X_2$, indem wir vor

$$\begin{array}{cccc} i_1 & n & einfügen & \Rightarrow & (ni_1 \ldots i_{r_1}) \circ (i_{r_1+1} \ldots) \ldots \\ i_2 & n & einfügen & \Rightarrow & (i_1 n \ldots i_{r_1}) \circ (i_{r_1+1} \ldots) \ldots \\ \vdots & & \vdots & \vdots & \vdots \\ i_{n-1} & n & einfügen & \vdots & \vdots \end{array}$$

$$|X_2| = (n-1)|Perm_k(\underline{n-1})| = (n-1)s_{n-1,k}$$

**Beispiel:**

$$Perm_3(\underline{4}) = \{(12)(3)(4), (13)(2)(4), (14)(2)(3), (23)(1)(4), (24)(1)(3), (34)(1)(2)\}$$

$$n = 4, X_1 = \{(12)(3)(4), (13)(2)(4), (23)(1)(4)\}$$

$$\sigma \in X_2 \text{ liefert } (1)(2)(3) = (2)(1)(3) = (3)(1)(2)$$

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

$$(41)(2)(3) = (14)(2)(3), (1)(42)(3) = (24)(1)(3), (1)(2)(43) = (34)(1)(2)$$

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

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

Um solche Rekursionen explizit zu lösen, brauchen wir

## 1.4 Formale Potenzreihen (erzeugende Funktionen)

$$(a_n)_{n \in \mathbb{N}_0} = (a_0, a_1, a_2, \ldots)$$

$\sum_{n=0}^{\infty} a_n x^n$ „formaler Ausdruck" , x = „Unbestimmte"

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

**Definition:**

$$K[[x]] := \left\{ \sum_{n=0}^{\infty} a_n x^n | a_n \in K \right\} \text{ und } \sum_{n=0}^{\infty} a_n x^n = (a_n)_{n \in \mathbb{N}_0}$$

$$x^n := (a_j)_{j\in\mathbb{N}_0} \text{ mit } a_j = \begin{cases} 1 & j = n \\ 0 & \text{sonst} \end{cases}, n \in \mathbb{N}_0$$

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

$$k \in \mathbb{N}, \sum_{n=0}^{\infty} a_n x^{kn} := (b_j)_{j\in\mathbb{N}_0} \text{ mit } b_j = \begin{cases} a_n & j \neq kn \text{ für ein } n \in \mathbb{N}_0 \\ 0 & j \neq kn \end{cases}$$

**Warnung:**

a)

$$A = A(x) = \underbrace{\sum_{n=0}^{\infty} a_n x^n}_{\text{ist keine Summe!}} \in K[[x]]$$

Es gibt keine unendlichen Summen!

b) In eine formale Potenzreihe $A$ kann man i. Allg. nichts einsetzen

(02.05.01)

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

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

$$\sum_{n=0}^{\infty} a_n x^n = (a_n)_{n\in\mathbb{N}_0} \quad \begin{matrix} \text{formale Potenzreihe (in X)} \\ \text{erzeugende Funktion der Folge } (a_n)_{n\in\mathbb{N}_0} \end{matrix}$$

[zum Vergleich: $1,125 = \frac{9}{8} \in \mathbb{Q}$]

$$x^m = (\delta_{m,n})_{n\in\mathbb{N}_0} \text{ mit } \delta_{m,n} = \begin{cases} 1 & \text{für } m = n \\ 0 & \text{sonst} \end{cases} \quad \text{„Kronecker-Symbol"}$$

**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 zum + in Satz 1)

$$\left( \sum_{i=0}^{\infty} a_i x^i \right) \left( \sum_{j=0}^{\infty} b_j x^j \right) := \sum_{k=0}^{\infty} \left( \sum_{i+j=k}^{\infty} a_i b_j \right) x^k$$

$$= \sum_{k=0}^{\infty} \left( \sum_{i=0}^{\infty} a_i b_{k-i} \right) x^k$$

, 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
- (M1)(*) (A · B) · C = A · (B · C)
- (M2)(*) A · B = B · A
- (M3) Es gibt $1 \in K[[x]]$ mit 1 · A = A für alle A $\in K[[x]]$
- (M4)(*) Es gilt A · (B + C) = (A · B) + (A · C)

(*) Für alle A, B, C $\in K[[x]]$

**Beweis:** Durch Nachrechnen

Eins-Element ist $1 \cdot x^0 = 1$

Allgemeiner gilt:
**Lemma 1:**

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

In der ,,Folgensprache" bedeutet dies

$$x^m \cdot (a_0, a_1, \ldots) = (0, 0, \ldots, 0, a_0, a_1, \ldots)$$

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

**Beweis:**

$$x^m \cdot \sum_{n=0}^{\infty} a_n x^n = \sum_{k=0}^{\infty} \underbrace{\left( \sum_{i=0}^{k} \underbrace{\underbrace{\delta_{m,i}}_{=0 \text{ für } i \neq m} \underbrace{a_{k-i}}_{\text{, insbes. wenn } i \leq k \leq m}}_{=0 \text{ falls } k<m \qquad =a_{k-m} \text{ falls } k \geq m} \right)}_{} x^k \text{ , mit } x^m = (\delta_{m,n})_{n \in \mathbb{N}}$$

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

**Folgerung:** $x^m x^n = x^{m+n}$

**Beispiel:**

$$(1 - cx) \cdot \sum_{i=0}^{\infty} c^i x^i \text{ für } c \in K$$

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

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

**Bemerkung und Definition:** Ist in einem komm. Ring mit Eins $A \cdot B = 1$, so ist $B$ durch $A$ eindeutig bestimmt und wird mit $B = A^{-1} = \frac{1}{A}$ bezeichnet
(Ebenso ist $A = B^{-1} = \frac{1}{B}$) und A (und auch B) heissen invertierbar.

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

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

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

**Folgerung:** 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:** Code mit variabler Wortlänge (zum Komprimieren von Daten, z.B. ,,compress", ,,gzip")
Bu = {a, b, c} , Zi = {0, 1}
$W_k$ ={Folgen aus $0 < i < k$ Buchstaben gefolgt von $k - i$ Ziffern} , $k \in \mathbb{N}$

$$Co_n = \bigcup_{k=2}^{n} W_k \text{ , z.B. } aa1|bc0001|ac1$$

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

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

$$C = \sum_{k=0}^{\infty} c_k x^k = \left(\sum_{i=0}^{\infty} 3^i x^i\right)\left(\sum_{j=0}^{\infty} 2^j x^j\right)$$

$$= \frac{1}{1-3x} \cdot \frac{1}{1-2x} = \frac{1}{(1-3x)(1-2x)}$$

$$\text{Ansatz: } = \frac{\alpha}{1-3x} + \frac{\beta}{1-2x} = \frac{\alpha(1-2x) + \beta(1-3x)}{(1-3x)(1-2x)}$$

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

$$\Rightarrow C = \sum_{k=0}^{\infty} c_k x^k = \frac{3}{1-3x} - \frac{2}{1-2x}$$

$$C = \sum_{k=0}^{\infty} c_k x^k = 3\sum_{i=0}^{\infty} B^i x^i - 2\sum_{i=0}^{\infty} 2^i x^i = \sum_{i=0}^{\infty} \underbrace{(3^{i+1} - 2^{i+1})}_{=c_i} x^i$$

**Satz 3:**

$$A = \sum_{n=0}^{\infty} a_n x^n \in K[[x]] \text{ ist invertierbar } \Leftrightarrow a_0 \neq 0$$

**Beweis:**

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

$$\sum_{k=0}^{\infty} \left( \sum_{i=0}^{k} a_i b_{k-i} \right) x^k = 1 \Leftrightarrow \sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} 1 & \text{für } k = 0 \\ 0 & \text{sonst} \end{cases}$$

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

Ist $B$ invertierbar, so muss $a_0 \neq 0$ sein, sonst ist die Gleichung für $k = 0$ nicht erfüllbar.
Umgekehrt ist $a_0 \neq 0$, so definiere $b_o = a_0^{-1} \in K$ und $b_n = \frac{1}{a_0}(-a_1 b_{n-1} - \ldots - a_n b_0)$ rekursiv.

(04.05.01)

(Wiederholung)

$$K[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n | a_n \in K \right\} \text{ „formale Potenzreihen"}$$

$$K[x] = \left\{ \sum_{n=0}^{\infty} a_n x^n | a_n \in K \text{ und } a_n \neq 0 \text{ nur für endlich viele n} \right\}$$

$$= \left\{ \sum_{n=0}^{r} a_n x^n | a_n \in K, r \in \mathbb{N}_0 \right\} \text{ „Polynomring"}$$

- In $K[x]$ gibt es „Einsetzungshomophismen", dagegen: Ist $A \in K[[x]]$, so kann man in $A$ i. Allg. nichts einsetzen.
- In K[x] sind nur die Polynome vom Grad = 0 invertierbar, dagegen:

**Satz 3:**

$$A = \sum_{n=0}^{\infty} a_n x^n \in K[[x]] \text{ ist invertierbar } \Leftrightarrow a_0 \neq 0$$

$$\left( \sum_{n=0}^{\infty} a_n x^n \right) \left( \sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left( \sum_{i=0}^{n} a_i b_{n-i} \right) x^n = 1 = 1 \cdot x^0 \Leftrightarrow \sum_{i=0}^{n} a_i b_{n-i} = \delta_{n,0} = \begin{cases} 1 & \text{für } n = 0 \\ 0 & \text{sonst} \end{cases}$$

Dann ist $(b_0, b_1, b_2, \ldots)$ Lösung des folgenden Gleichungssystems:

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

usw.
lösbar $\Leftrightarrow a_0 \neq 0$

(Ende Wiederholung)

**Beispiel:** $a_0 = 1, a_1 = -c \in K, a_2 = a_3 = \ldots = 0, A = 1 - cx$

$$\begin{array}{lll} 1 \cdot x_0 = 1 & \Leftrightarrow & x_0 = 1 \\ -cx_0 + x_1 = 0 & \Leftrightarrow & x_1 = c \\ -cx_1 + x_2 = 0 & \Leftrightarrow & x_2 = c^2 \\ \vdots & \vdots & x_n = c^n \end{array}$$

**Folgerung 1:**

$$\frac{1}{1-cx} = \sum_{n=0}^{\infty} c^n x^n \text{ ,,Geometrische Reihe"}$$

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

**Beispiel:**

$$\left(\sum_{n=0}^{\infty} c^n x^n\right)^2 = \sum_{n=0}^{\infty}\left(\sum_{i=0}^{\infty} c^i c^{n-i}\right)x^n = \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} c^n\right)x^n = \sum_{n=0}^{\infty}(n+1)c^n x^n$$

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

**Folgerung 2:**

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

**Allgemeiner:**

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

**Beweis:** Übung

**Definition:** Die Abbildung

$$D : K[[x]] \to K[[x]] : \sum_{n=0}^{\infty} a_n x^n \mapsto \sum_{n=0}^{\infty}(n+1)a_{n+1}x^n$$

heisst ,,formale Ableitung".

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

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

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

**Beweis:** Nachrechnen

**Folgerung 3:** Ist $A \in K[[x]]$ invertierbar, so mit $D(A^{-1}) = -\frac{D(A)}{A^2}$

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

$$0 = D(A \cdot A^{-1}) = A \cdot D(A^{-1}) + D(A) \cdot A^{-1} \text{ nach Lemma 2 (2)}$$

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

**Beispiel:**

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

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

$$\overset{Folg.}{=} -\frac{D(A)}{A^2} = \frac{c}{(1-cx)^2}, \text{ o.B.d.A. } c \neq 0$$

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

$\Rightarrow$ neuer Beweis der Folgerung

## 1.5 Lösen von Rekursionsgleichungen

**Beispiel:** Die Fibonacci-Zahlen $F_n$ sind (für $n \in \mathbb{N}_0$) so definiert

$$F_0 = 0, F_1 = 1$$

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

$$\text{z.B. } F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, \ldots$$

$$\text{Sei } F = F(x) = \sum_{n=0}^{\infty} F_n x^n = F_0 + F_1 x + \sum_{n=2}^{\infty} F_n x^n$$

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

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

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

$$= F_0 + F_1 x + x \cdot F + x^2 \cdot F - F_0 x^0 x$$

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

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

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

Sei 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

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

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

(09.05.01)

(Wiederholung)

Fibonacci-Zahlen

$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

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

$$F = \frac{x}{1 - x - x^2} = \frac{a}{1 - \alpha x} + \frac{b}{1 - \beta x}, a, b, \alpha, \beta \in \mathbb{C}$$

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

(Ende Wiederholung)

**Satz 1:**(Partial-Bruchzerlegung)

$K$ sei ein Körper, $g = (1-\alpha_1 x)^{m_1} \dots (1-\alpha_r x)^{m_r} \in K[x]$ mit $\alpha_i \neq 0$ für alle $i$

$$f \in K[x], Grad\ f < Grad\ g$$

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

$$\frac{f}{g} = \frac{f_1}{(1-\alpha_1 x)^{m_1}} + \dots + \frac{f_r}{(1-\alpha_r x)^{m_r}}$$

$$\frac{f_i}{(1-\alpha_i x)^{m_i}} = \frac{a_{i1}}{1-\alpha_i x} + \frac{a_{i2}}{(1-\alpha_i x)^2} + \dots + \frac{a_{im_i}}{(1-\alpha_i x)^{m_i}}$$

**Beweis:** s. Alg. Strukturen

**Bemerkung:** Ist $g$ wie in Satz 1, so sind die $(\alpha_i)^{-1}$ Nullstellen von $g$.

**Definition:** Ist

$$g = \sum_{i=0}^{n} a_i x^i \text{ mit } a_n \neq 0,$$

so sei

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

das reflektierte Polynom.

**Beispiel:** $g = 1 + 2x + 3x^2 \Rightarrow g^R = x^2 + 2x + 3$

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

**Beweis:** Sei $\alpha \neq 0$ in $K$

$$0 = g(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \Rightarrow 0 = \alpha^{-n} g(\alpha) = \sum_{i=0}^{n} a_i \alpha^{i-n} \text{ , setze: } j = n - i \Leftrightarrow i = n - j$$

$$\Leftrightarrow 0 = \sum_{j=0}^{n} a_{n-j} \alpha^{-j}$$

$$\Leftrightarrow 0 = g^R(\alpha^{-1})$$

**Bemerkung:** $g^R(x) = x^n g(x^{-1})$

**Satz 2:** („Fundamentalsatz der Algebra") Ist

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

so gibt es $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ mit

$$g = a_n (x - \alpha_1) \dots (x - \alpha_n)$$

(ohne Beweis)

**Folgerung:** Ist

$$f = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x], a_n \neq 0, a_0 \neq 0,$$

so gibt es $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ mit

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

denn nach Satz 2 ist

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

$$\Rightarrow f = \left(f^R\right)^R = x^n(\frac{1}{x} - \alpha_1) \ldots (\frac{1}{x} - \alpha_n) = (1 - \alpha_1 x) \ldots (1 - \alpha_n x)$$

Fortsetzung des Beispiels

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

$$g^R = x^2 - x - 1 = (x - \alpha_1)(x - \alpha_2)$$

$$\alpha_1 = \frac{1 + \sqrt{5}}{2}, \alpha_2 = \frac{1 - \sqrt{5}}{2}$$

$\alpha_1$ heisst „Der Goldene Schnitt"

$$g = (1 - \alpha_1 x)(1 - \alpha_2 x), \frac{f}{g} = \frac{x}{1 - x - x^2} = \frac{a}{1 - \alpha_1 x} + \frac{b}{1 - \alpha_2 x}$$

mit $a, b \in \mathbb{C}$ ex. nach Satz 1

$$\frac{x}{1 - x - x^2} = \frac{a(1 - \alpha_2 x) + b(1 - \alpha_2 x)}{(1 - \alpha_1 x)(1 - \alpha_2 x)}$$

$$x = a + b - (a\alpha_2 + b\alpha_1)x$$

$$a + b = 0 \Rightarrow b = -a$$

$$a\alpha_2 - b\alpha_1 = -1 \Rightarrow a\alpha_2 + a\alpha_1 = -1$$

$$\Rightarrow a = \frac{-1}{\alpha_1 + \alpha_2} = \frac{1}{\sqrt{5}}, b = \frac{-1}{\sqrt{5}}$$

$$F_n = a\alpha_1^n + b\alpha_2^n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right]$$

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)

**Gegeben:** $a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k}, n \geq k$ mit gegebenen $c_i \in \mathbb{C}$
und Anfangsbedingung: $a_i = b_i$ für $i = 0, 1, \ldots k-1, b_i \in \mathbb{C}$ gegeben.

$$A := \sum_{n=0}^{\infty} a_n x^n = \sum_{i=0}^{k-1} a_i x^i + \sum_{n=k}^{\infty} (c_1 a_{n-1} + \ldots + c_k a_{n-k}) x^n$$

$$= \sum_{i=0}^{k-1} b_i x^i + c_1 x \left( A - \sum_{i=0}^{k-2} b_i x^i \right) + c_2 x^2 \left( A - \sum_{i=0}^{k-2} b_i x^i \right) + \ldots + c_k x^k A$$

Auflöesen nach A:

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

mit

$$f = b_0 + (b_1 - c_1 b_0)x + \ldots + (b_{k-1} - c_1 b_{k-2} - \ldots - c_{k-1} b_0)x^{k-1}$$

Partialbruchzerlegung:

$$A = \sum_{i=1}^{r} \frac{f_i}{(1 - \alpha_i x)^{m_i}} \text{ mit } f_i = \sum_{j=0}^{m_i - 1} f_{ij} x^j$$

$$A = \sum_{i=1}^{r} \sum_{j=0}^{m_i - 1} f_{ij} \sum_{n=j}^{\infty} \binom{n+m-1}{n} \alpha_i^{n-j} x^n$$

**Bemerkung:** Die $\alpha_i$ im Verfahren erhält man als Nullstelle 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 Anfangsbestimmungen bestimmen.

**Beispiel:**

$$a_n = a_{n-1} = a_{n-2}, g = 1 - x - x^2$$

$$g^R = x^2 - x - 1 = (x - \alpha_1)(x - \alpha_2), \alpha_1 \neq \alpha 2$$

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

$$n = 0 : a_0 = 0 = a + b$$

$$n = 1 : a_1 = 1 = a\alpha + b\beta$$

**Beispiel:**$\mathcal{C}_n = \{$ zulässige Klammerungen mit $2n$ Klammern $\}$

$$c_n = |\mathcal{C}_n|, c_0 = 1, c_1 = 1, c_2 = 2[\mathcal{C}_2 = \{(()), ()()\}]$$

$$c_3 = 5, c_n = \text{ n-te Catalan-Zahl}$$

$\mathcal{C}_n^{(k)} = \{$ Zeichenketten (aus $\mathcal{C}_n$ , bei der die 1. Klammer an der Position 2k geschlossen wird$\}$

$$\mathcal{C}_n = \dot{\bigcup_{k=1}^{n}} \mathcal{C}_n^{(k)}, |\mathcal{C}_n| = c_n = \sum_{k=1}^{n} c_{k-1} c_{n-k} \text{ für } n \geq 1$$

$$C = \sum_{n=0}^{\infty} c_n x^n = c_0 + \sum_{n=1}^{\infty} c_n x^n = 1 + \sum_{n=1}^{\infty} \left( \sum_{k=1}^{n} c_{k-1} c_{n-k} \right) x^n = 1 + (xC)C$$

$$C = 1 + xC^2$$

$$x^2 C^2 - xC + x = 0$$

$$x^2 C^2 - xC + \frac{1}{4} = -x + \frac{1}{4}$$

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

$$xC - \frac{1}{2} = \pm \sqrt{-x + \frac{1}{4}}$$

$$xC = \frac{1}{2} \left( 1 \pm \sqrt{1 - 4x} \right)$$

**Satz 3:** Ist $K$ ein Körper mit $1+1 \neq 0$ (d.h. $charK \neq 0$) gibt es zu $0 \neq A = \sum_{i=0}^{\infty} a_i x_i$ ein $B = \sum_{i=0}^{\infty} b_i x^i$ mit $B^2 = A$ genau dann, wenn $a_0$ in $K$ ein Quadrat ist.

(11.05.01)

**Satz 3:**(Wiederholung) ...gibt es zu $0 \neq A = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ ein $B = \sum_{n=0}^{\infty} b_n x^n \in K[[x]]$ mit $B^2 = A$ genau dann, wenn es ein $b_0 \neq 0$ gibt mit $b^2 = a_0 (\neq 0)$

**Beweis:**

$$B^2 = \sum_{n=0}^{\infty} \left( \sum_{k=0}^{n} b_k b_{n-k} \right) x^n = A \;\Leftrightarrow\; \sum_{k=0}^{n} b_k b_{n-k} = a_n \text{ für alle } n \in \{0, \ldots, n\}$$

Also:

$$\begin{array}{cll} b_0^2 & = a_0 & b_0 = \pm b (\neq 0) \\ b_0 b_1 + b_1 b_0 = 2 b_0 b_1 & = a_1 & b_1 = \frac{1}{2b_0} a_1 \\ b_0 b_2 + b_1 b_1 + b_2 b_0 & = a_2 & b_2 = (a_2 - b_1^2) \cdot \frac{1}{2b_0} \end{array}$$

Ist also $a_0 \neq 0$ und $a_0 = b^2$, so definiere induktiv

$$b_0 = b, b_n = \left( a_n - \sum_{k=1}^{n-1} b_k b_{n-k} \right) \cdot \frac{1}{2b_0}$$

Dann ist $B^2 = A$.
Umkehrung ist klar.
Im Beispiel war $B \in K[[x]]$ und $B^2 = 1 - 4x \Rightarrow B = (1-4x)^{\frac{1}{2}}$

## 1.6 Die Polynommethode

**Satz 1:** Ist $K$ ein Körper und $0 \neq f \in K[x]$ (also $f = \sum_{i=0}^{n} a_i x^b, a_n \neq 0$), so hat $f$ höchstens $n$ Nullstellen.

**Beweis:** s. LA I

**Folgerung:** Ist

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

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 $f = g$, d.h. $a_i = b_i$ für alle $i = 0, \ldots, n$.

**Beweis:** folgt aus Satz 1; betrachte $f - g$ , $Grad(f-g) \leq n$, also $f - g = 0$

Im folgenden sei $K$ ein Körper mit $\mathbb{Q} \leq K$
**Definition:**

$$x^{\underline{n}} = x(x-1)\ldots(x-n+1) \in K[x]$$

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

[Beachte: $n! \neq 0, x^{\underline{n}} = 1, \binom{x}{k} = 1$]

**Beispiel:**

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

In 1.2 Satz 3

$$m^n = \sum_{k=0}^{m} S_{n,k} m^{\underline{k}} = \sum_{k=0}^{n} S_{n,k} m^{\underline{k}} \tag{1.2}$$

$S_{n,k}$ Stirling-Zahlen 2.Art
für $n \geq k > m$ gilt $m^{\underline{k}} = m(m-1)\ldots\cdot 1 \cdot 0(\cdot - 1 \cdot \ldots) = 0$
für $n < k \leq m$ gilt $S_{n,k} = 0$
Setze

$$f = x^n, g = \sum_{k=0}^{n} S_{n,k} x^{\underline{k}}$$

$\Rightarrow f(m) = g(m)$ für alle $m \in \mathbb{N}$ wegen 1.2

**Satz 2:** Ist $\mathbb{Q} \leq K$ Körper, so gilt

a)

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

b)

$$x^{\underline{n}} = \sum_{k=0}^{n} (-1)^{n-k} s_{n,k} x^k \text{ , wobei } s_{n,k} \text{ Stirlingzahlen 1.Art}$$

**Beweis:** von 1.: s.o., benutze Satz 1
von 2.: Induktion: Übung, benutze $s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$

**Bemerkung:** $(x^n)_{n\in\mathbb{N}_0}$ und $(x^{\underline{n}})_{n\in\mathbb{N}_0}$ sind $K$-Basen des $K$-Vektorraums $K[x]$ und $[S_{n,k}]_{n,k\in\mathbb{N}_0}$ und $[(-1)^{n-k}s_{n,k}]$ sind Basiswechselmatrizen, also invers zueinander.

In 1.1 Satz 1

$$\binom{m+n}{k} = \sum_{l=0}^{k} \binom{m}{l}\binom{n}{k-l} \text{ mit } m,n,k \in \mathbb{N}$$

spezialisiere

$$\binom{(j+1)\cdot m}{k} = \sum_{l=0}^{k} \binom{m}{l}\binom{j\cdot m}{k-l} \text{ mit } m,k,j \in \mathbb{N} \tag{1.3}$$

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

nach Satz 1 (Folg.); wegen 1.3 stimmen L.S. und R.S. für $\infty$ viele m überein.

**Satz 3:** Für $c \in K (K \geq \mathbb{Q}, K$ 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)

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

b)

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

**Beweis:**

a) Induktion nach $j$
Für $j=1$ Beh. klar per Def.
Für $j \geq 1$

$$\left((1+cx)^{\frac{1}{m}}\right)^j + 1 = \left((1+cx)^{\frac{1}{m}}\right)^j (1+cx)^{\frac{1}{m}} \overset{Ind.Ann.}{=} \left(\sum_{n=0}^{\infty} \binom{\frac{j}{m}}{n} c^n x^n\right)\left(\sum_{n=0}^{\infty} \binom{\frac{1}{m}}{n} c^n x^n\right)$$

$$= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \binom{\frac{j}{m}}{k} c^k \binom{\frac{1}{m}}{n-k} c^{n-k}\right) x^n$$

$$= \sum_{n=0}^{\infty} \underbrace{\left(\sum_{k=0}^{n} \binom{\frac{j}{m}}{k}\binom{\frac{1}{m}}{n-k}\right)}_{\text{nach Satz 2 } = \binom{j+1}{n}} c^n x^n$$

b) Wende 1. an für $j=m$

$$\left((1+cx)^{\frac{1}{m}}\right)^m = \sum_{n=0}^{\infty} \underbrace{\binom{1}{n}}_{\begin{array}{l}=1 \text{ für } n=0\\ =1 \text{ für } n=1\\ =0 \text{ für } n>1\end{array}} c^n x^n = 1+cx$$

(16.05.01)

**Polynommethode**

Ausgangspunkt: Gleichung gültig für alle $m,n \in \mathbb{N}$, z.B.

$$\binom{2m}{n} = \sum_{k=0}^{m} \binom{m}{k}\binom{m}{n-k}$$

Gesucht: Polynome $f,g \in K[x], K \geq \mathbb{Q}$ mit $f(m) =$ L.S. und $g(m) =$ R.S.
Satz 1 impliziert dann $f=g$ und es gilt für alle $z \in K f(z) = g(z)$
Im Beispiel:

$$f = \binom{2x}{n} = \frac{1}{n!}(2x)(2x-1)\dots(2x-n+1)$$

$$g = \sum_{k=0}^{n} \binom{x}{n}\binom{x}{n-k}$$

Also:

$$\binom{2z}{n} = \sum_{k=0}^{n} \binom{z}{k}\binom{z}{n-k} \text{ , für -stellialle } z \in \mathbb{C} \quad [z \in \mathbb{C}^{n\times n}]$$

z.B.: $z = \frac{1}{2}$

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

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

**Beispiel:** (Forts. von 1.5 Catalan-Zahlen)
$\mathcal{C}_n$ = Anzahl der regulären Klammerungen mit 2n Klammern
oder Anzahl der binären Suchbäume mit n Knoten

$$\mathcal{C}_0 = 1, \mathcal{C}_1 = 1, \mathcal{C}_2 = 2, \mathcal{C}_3 = 5$$

$$\mathcal{C}_n = \sum_{k=0}^{n-1} \mathcal{C}_k \; \mathcal{C}_{n-1+k}, n \geq 1$$

$$\mathcal{C} = \sum_{k=0}^{\infty} \mathcal{C}_n x^n = 1 + x\mathcal{C}^2 \quad | \cdot x$$

$$\left(x\mathcal{C} - \frac{1}{2}\right)^2 = \frac{1}{4}(1 - 4x)$$

$$x\mathcal{C} - \frac{1}{2} = \pm\frac{1}{2}(1 - 4x)^{\frac{1}{2}}$$

$$\sum_{n=1}^{\infty} \mathcal{C}_{n-1} x^n = x\mathcal{C} = \frac{1}{2}\left(1 \pm \sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n} - 4^n x^n\right)$$

Koeffizient von $x^0 = 0$, also gilt - als Vorzeichen

$$\mathcal{C}_n = -\frac{1}{2}\binom{\frac{1}{2}}{n+1}(-4)^{n+1} = -\frac{1}{2}(-1)^{n+1}4^{n+1}\frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)\ldots(\frac{1}{2}-n)}{(n+1)!}$$

$$= -\frac{1}{2}2^{n+1}(-1)^1\frac{1 \cdot 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)}{(n+1)!}$$

$$= \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) \cdot 2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2n}{(n+1)! \cdot n!} = \frac{1}{n+1} \cdot \frac{2n!}{n! \cdot n!} = \frac{1}{n+1}\binom{2n}{n}$$

# Kapitel 2

# Algebraische Strukturen

## 2.1 Universelle Algebren

**Definition 1:** Ist $M$ ein Menge, so heisst eine Abbildung

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

eine $n$-stellige Operation mit $n = s(f)$.
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. $(n_i = s(f_i), I$ 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 gilt:

$$(a \circ b) \circ c = a \circ (b \circ c) \text{ für alle } a, b, c \in M$$

**Beispiel:** $A =$ Menge ('Alphabet')

$$w = W(A) = \{(a_1, \ldots, a_k) | a_i \in A, n \in \mathbb{N}_0\} \quad \text{„Worte in A"}$$

$$w \times w \to w : (a_1, \ldots, a_n), (b_1, \ldots, b_m) \to (a_1, \ldots, a_n, b_1, \ldots, b_m)$$

**Definition 3:** Ein Monoid ist eine Algebra $(M, \circ, e)$ vom Typ (2,0) mit $(M, \circ)$ ist eine Halbgruppe und $e \circ a = a \circ e = a$ für alle $a \in M$. $e$ heisst „neutrales Element".

**Definition 3 (alt.):** Ein Monoid ist eine Halbgruppe $(M, \circ)$ und es gibt $e \in M$ 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 Monoid und $g \circ g^{-1} = g^{-1} \circ g = e$ für alle $g \in G$. Gilt zusätzlich $g_1 \circ g_2 = g_2 \circ g_1$ für alle $g_1, g_2 \in G$, so heisst $G = (G, \circ, ^{-1}, e)$ abelsche (oder kommutative) Gruppe.

**Beispiel:** $S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} | \sigma \text{ bijektiv}\}$
$(S_n, \circ, ^{-1}, (1))$ ist eine (nicht-abelsche) Gruppe (für $n \geq 3$).
$(\mathbb{Z}, +, -, 0)$ ist eine abelsche Gruppe.

**Definition 5:** $(R, +, -, 0, \cdot, 1)$ vom Typ (2, 1, 0, 2, 0) heisst ein ,,Ring mit Eins", wenn folgendes gilt:

- $(R, +, -, 0)$ ist eine abelsche Gruppe
- $(R, \cdot, 1)$ ist ein Monoid
- $\begin{array}{l}(a+b)\cdot c = a\cdot c + b\cdot c \\ a\cdot(b+c) = a\cdot b + a\cdot c\end{array}$ für alle $a, b, c \in R$

Gilt zusätzlich $a \cdot b = b \cdot a$ für alle $a, b \in R$, so heisst $(R, \ldots)$ 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 $1 \neq 0$ , so heisst $(R, \ldots)$ (kommutativer) Körper.

**Beispiele:** $(\mathbb{Z}, +, -, 0, 1, \cdot)$ ist ein kommutativer Ring
$(\mathbb{Q}, +, -, 0, 1, \cdot)$, $(\mathbb{R}, +, -, 0, 1, \cdot)$, $(\mathbb{C}, +, -, 0, 1, \cdot)$ und $(\mathbb{F}_2, +, -, 0, 1, \cdot)$ sind Körper.
$(K^{n\times n}, +, -, 0, I_n, \cdot)$ ist nichtkommutativer Ring mit Eins, wobei $I_n$ die Einheitsmatrix bezeichnet, mit $n > 1$.
$K[x]$ ist der Polynomring und $K[[x]]$ der Ring der formalen Potenzreihen.

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

- $(V, +, -, 0)$ ist eine abelsche Gruppe
- $\alpha(v + w) = \alpha(v) + \alpha(w)$ , $\alpha \in K; v, w \in V$
- $1 \in K$ , $1(v) = v$
- $(\alpha + \beta)(v) = \alpha(v) + \beta(v)$ , $\beta \in K$
- $(\alpha \cdot \beta)(v) = (\alpha(\beta(v))n$-stellige Operation

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

- $(M, +, -, 0)$ ist abelsche Gruppe
- $\alpha(v + w) = \alpha(v) + \alpha(w)$ , $\alpha \in R; v, w \in M$
- $1(v) = v$
- $(\alpha + \beta)(v) = \alpha(v) + \beta(v)$ , $\beta \in R$
- $(\alpha \cdot \beta)(v) = \alpha(\beta(v))$

(18.05.01)

Der kleinste Ring ist $\{0\}$ mit $0 = 1, + = \cdot$ usw.
Der kleinste Körper ist $\mathbb{F}_2 = \{0, 1\}$

## 2.2 Unteralgebren, Homomorphismen, Kongruenzen

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

**Definition 1:** $\mathbf{U} \leq \mathbf{A}$ Unteralgebra
$f_i(u_1, \ldots, u_{n_i}) \in \mathbf{U}$ für alle $u_1, \ldots, u_{n_i} \in \mathbf{U}, i \in I$
(insbes. ist $n_i = 0$, also $f_i \in \mathbf{A}$, so muss $f_i \in U$

**Bemerkung:** Ist $\mathbf{U} \leq \mathbf{A}$, so ist $(U, (f_{i|U^{n_i}})_{i\ inI})$ Algebra vom Typ T

**Beispiel:**

a) $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ Gruppe
$\mathbf{U} \leq \mathbf{G} \Leftrightarrow \mathbf{U}$,,Untergruppe" $\Leftrightarrow (u, u' \in \mathbf{U} \Rightarrow u \cdot u' \in \mathbf{U}, u^{-1} \in \mathbf{U}, 1 \in \mathbf{U})$

b) $\mathbf{V} = (V, +, -, 0, K)$ K-Vektorraum
$\mathbf{U} \leq \mathbf{V} \Leftrightarrow \mathbf{U}$ Untervektorraum = Teilraum

c) $\mathbf{R}$ Ring ,$\mathbf{U} \leq \mathbf{R}$ , $\mathbf{U}$ Teilring = Unterring

**Lemma 1:** $\mathbf{U}_j \leq \mathbf{A}$ für $j \in J$ = Indexmenge

$$\Rightarrow \bigcap_{j\in J} \mathbf{U}_j \leq \mathbf{A}$$

**Definition 2:** $M \subset A$ Teilmenge

$$< M >= \bigcap \{U | M \leq U \leq A\}$$

= das ,,Erzeugnis" aus M oder die von M erzeugte Unteralgebra

**Beispiel:**

a) $V$ K-VR, $v_1, \ldots, v_n \in V$

$$< \{v_1, \ldots, v_n\} >= \left\{ \sum_{i=1}^{n} \alpha_i v_i | \alpha_i \in K \right\}$$

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

$$< g >=< \{g\} >= \{g^i | i \in \mathbb{Z}\}, \text{ wobei } g^i = \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{i mal} & \text{für } i > 0 \\ 1 & \text{für } i = 0 \\ \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{-i mal} & \text{für } i < 0 \end{cases}$$

$$< \{g_1, \ldots, g_n\} >= \left\{ a_1 \cdot \ldots \cdot a_m | m \in \mathbb{N}, a_j \in \{g_1, \ldots, g_n, g_1^{-1}, \ldots, g_n^{-1}\} \right\}$$

**Definition 3:** Seien $\mathbf{A} = (A, (f_i)_{i\in I})$ und $\mathbf{A'}, (f_i')_{i\in I})$ Algebren vom gleichen Typ $\mathrm{T} = (n_i)_{i\in I}$, so heisst eine Abbildung $\phi : \mathbf{A} \to \mathbf{A'}$ ein (Algebren-)Homomorphismus, wenn $f_i' : (\phi(a_1), \ldots, \phi(a_{n_i})) = \phi(f_i(a_1, \ldots, a_{n_i}))$

[Insbesondere $\phi(f_i) = f_i'$, falls $n_i = 0, d.h. f_i \in A$]
Ist zusätzlich $\phi$ bijektiv, so heisst $\phi$ ein Isomorphismus.

$$\mathbf{A} = \mathbf{A'} \overset{def}{\Leftrightarrow} \text{ Es gibt Isomorphismus } \phi : \mathbf{A} \to \mathbf{A'}$$

**Beispiel:**

a) $V, W$ K-VR

$$\phi : V \to W \text{ Homomorphismus } \Leftrightarrow \phi \text{ ist K-Linear, d.h.}$$

$$\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$$
$$\phi(-v) = -\phi(v)$$
$$\phi(0) = 0$$
$$\phi(\alpha \cdot v) = \alpha \cdot \phi(v)$$

b) $G_1, G_2$ Gruppen; $(G_1, \cdot, ^{-1}, 1), (G_2, *, ', e)$
$\phi : G_1 \to G_2$ Homomorphismus

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

**Bemerkung:** Hier folgen (ii) und (iii) aus (i)

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

$$a_1 \sim a_1', \ldots, a_{n_i} \sim a_{n_i}' \Rightarrow f_i(a_1, \ldots, a_{n_i}) \sim f_i(a_i', \ldots, a_{n_i}')$$

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

**Beispiel:** $(G, \cdot, ^{-1}, 1)$ Gruppe, $\sim$ Äquivalenzrelation auf G

$$\sim \text{ Kongruenz } \Leftrightarrow \left[ \begin{array}{c} a \sim a' \\ b \sim b' \end{array} \right. \Rightarrow \begin{array}{c} a \cdot b \sim a' \cdot b' \\ a^{-1} \sim a'^{-1} \end{array}$$

**Homomorphiesatz:**

a) Es sei $\sim$ Kongruenzrelation auf A, dann wird die Menge der Äquivalenzklassen

$A/\sim = \{[a]_\sim | a \in A\}$ ,wobei $[a]_\sim = \{a' \in A | a' \sim a\}$ Äquivalenzklasse von a,

eine Algebra vom Typ T mit $\overline{f_i}([a_1]_\sim, \ldots, [a_{n_i}]_\sim) := f_i(a_1, \ldots, a_{n_i})$ und
$\pi = \pi_\sim : A \to A/\sim : a \mapsto [a]_\sim$ ist surjektiver Homomorphismus.

b) Ist $\phi : \mathbf{A} \to \mathbf{B}$ ein Homomorphismus, so wird durch

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

eine Kongruenzrelation auf $\mathbf{A}$ definiert und

$$Bild(\phi) = \phi(A) := \{\phi(a) | a \in A\}$$

ist Unteralgebra von B und es gibt einen Isomorphismus

$$\overline{\phi} : \mathbf{A}/\sim \to Bild(\phi) : [a]_\sim \mapsto \phi(a)$$

**Bemerkung:** Kennt man also alle Kongruenzen auf **A**, so kennt man bis auf Isomorphie alle homomorphen Bilder von **A**.

**Beweis:** Nachrechnen!
Nicht vergessen, zu zeigen, die Operationen $\overline{f_i}$ sind wohldefiniert

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

$$[a_i] = [a_i'] \Rightarrow R.S. = f_i(a_1', \ldots, a_{n_i}')$$

Dies gilt gerade, weil $\sim$ Kongruenz.

**Beispiel:** $V$ K-VR, $\phi : V \to W$ Homomorphismus

$$v \sim v' \overset{perDef.}{\Leftrightarrow} \phi(v) = \phi(v') \Leftrightarrow \phi(v - v') = 0$$

$$\Leftrightarrow v - v' \in Kern\phi = U \leq V$$

$[v]_\sim = v + U$, insbesondere: $[0]_\sim = U = Kern\phi$

(23.05.01)

$\mathbf{A} = (A, (f_i)_{i \in I})$ 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

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

zur Algebra vom Typ T mit

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

Faktoralgebra

$$A \to A/\sim : a \mapsto [a]_\sim \text{ Surj. Homomorphismus von Algebren}$$

**Beispiel:** V K-VR und $\sim$ Kongruenzrelation

$$[0]_\sim = U \text{ Teilraum von V}$$

$$[a]_\sim = a + U = \{a + U | u \in U\}$$

$$V/\sim =: V/U$$

## 2.3 Ringe und Ideale

$R = (R, +, -, 0, \cdot, 1)$ sei Ring (Typ = (2, 1, 0, 2, 0)), d.h.

- $(R, +, -, 0)$ abelsche Gruppe
- $(R, \cdot, 1)$ Monoid und
- $(a + b)c = ac + bc$
- $a(b + c) = ab + ac$

**Lemma 1:** In einem Ring R gelten

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

b) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b); b \in R$

c) $-(-a) = a$

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

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

Was gibt es in Ringen für Kongruenzrelationen? Sei $\sim$ eine Kongruenzrelation auf R, setze $I = [0]_\sim = \{a \in R | a \sim 0\}$
Dann folgt für $a, a', b, b' \in R; a \sim a'; b \sim b'$

$$(a + b) \sim (a' + b')$$

$$a \cdot b \sim a' \cdot b'$$

$$-a \sim -a'$$

$$a \sim a' \Leftrightarrow a - a' \sim a' - a' = 0 \Leftrightarrow a - a' \in I = [0]_\sim$$

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

Welche Eigenschaft hat $I = [0]_\sim$?
Ist

$$\begin{array}{ccccc} u, v \in I & \Rightarrow & u \sim 0, v \sim 0 & \Rightarrow & u + v \sim 0 \text{ also: } u + v \in I \\ & & -u \sim -0 = 0 & \Rightarrow & -u \in I \end{array}$$

Ist $a \in R, u \in I$, 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 $a \cdot u \in I$ und $u \cdot a \in I$.

**Definition:** $I \subseteq R$ ($R$ Ring) heisst Ideal (als Zeichen: $I \trianglelefteq R$), wenn

$$a \in I \text{ und } a, b \in I \Rightarrow a + b \in I \text{ und } -a \in I$$

$$a \in R, u \in I \Rightarrow a \cdot u \in I \text{ und } u \cdot a \in I$$

**Satz 1:** Ist $\sim$ eine Kongruenzrelation auf R, so ist $I = [0]_\sim \trianglelefteq R$.
Umgekehrt: Ist $I \trianglelefteq R$, so wird durch

$$a \sim a' \overset{Def.}{\Leftrightarrow} a - a' \in I$$

eine Kongruenzrelation definiert.
(dabei $[0]_\sim = I, [a]_{sim} = a + I = \{a + u | u \in I\}$)
Man schreibt $R/\sim = R/I$

**Beweis:** 1. Teil: s.o. 2. Teil: Sei $I \trianglelefteq R$ beliebig gegeben und $\sim$ definiert durch $a \sim a' \Leftrightarrow a - a' \in I$

a) **Behauptung:** $\sim$ ist Äquivalenzrelation

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

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

$$a - b \in I \Rightarrow -(a - b) = b - a \in I, \text{ d.h. } b \sim a$$

(iii) Transitivität: $a \sim b, b \sim c \Rightarrow a \sim c$ gilt, weil

$$\begin{array}{lcl} a - b \in I & & (a - b) + (b - c) \in I \\ b - c \in I & \text{impliziert} & = \\ & & a - c \in I, \text{ d.h. } a \sim c \end{array}$$

b) **Behauptung:** $\sim$ ist sogar Kongruenzrelation, d.h. zu zeigen:

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

(i)

$$a - a' \in I, b - b' \in I \Rightarrow (a - a') + (b - b') \in I$$

$$\Rightarrow (a+b) - (a'+b') \in I, \text{ d.h. } (a+b) \sim (a'+b')$$

(ii)

$$a \sim a' \text{ also } a - a' \in I \Rightarrow -(a - a') \in I \Rightarrow -a - (-a') \in I, \text{ d.h. } -a \sim -a'$$

(iii)

$$a - a' \in I, \text{ dann folgt } (a - a')b \in I$$

$$b - b' \in I, \text{ dann folgt } a'(b - b') \in I$$

$$\text{und } (a - a')b + a(b - b') = ab - a'b' \in I, \text{ d.h. } ab \sim a'b'$$

**Satz 2:** Ist $R$ kommutativer Ring ($a \cdot b = b \cdot a$ , für alle $a, b \in R$) und $d \in R$ beliebig, so ist $Rd = \{a \cdot d | a \in R\} \trianglelefteq R$ ein Ideal, das von $d$ erzeugte Hauptideal.
Es ist $Rd = R \Leftrightarrow d$ ist invertierbar in $(R, \cdot, 1)$, d.h. $\exists d' \in R$ mit $dd' = 1$

**Beweis:** Zu zeigen:

a) $0 \in R$

b) $u, v \in Rd \Rightarrow u + v \in Rd$ und $-u \in Rd$

c) $c \in R, u \in Rd \Rightarrow c \cdot u \in Rd$

a)

$$0 \in Rd \text{ , weil } 0 = 0 \cdot d \text{ (s. Lemma 1)}$$

b)

$$u, v \in Rd \text{ bedeutet } u = a \cdot d, v = b \cdot d \text{ mit } a, b \in R$$

dann folgt

$$u + v = ad + bd = \underbrace{(a+b)}_{\in R} d \in Rd$$

$$-u = \underbrace{-a}_{\in R} d \in Rd$$

c)

$$u \in Rd \text{ , d.h. } u = a \cdot d \text{ mit } a \in R$$

dann folgt

$$c \cdot u = c(ad) = \underbrace{(ca)}_{\in R} d \in Rd$$

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

$$a = a \cdot 1 = a \cdot d' \cdot d = \underbrace{(a \cdot d')}_{\in R} d \in Rd \text{ , also } R \subseteq Rd$$

umgekehrt sei $R = Rd$, dann ist $1 \in Rd$, d.h. $\exists d' \in R$ mit $1 = dd'$, d.h. $d$ ist invertierbar.

**Beispiel:** $R = \mathbb{Z}, m \in \mathbb{N}$

$$m\mathbb{Z} \trianglelefteq \mathbb{Z}, \mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\sim_m = \{[a]_\sim | a \in \mathbb{Z}\}$$

$$\sim = \sim_m \text{ definiert durch } a \sim b \Leftrightarrow a - b \in m\mathbb{Z}$$

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

$$\mathbb{Z} \to \mathbb{Z}_m : a \mapsto [a]_m \text{ ist surj. Ringhomomorphismus}$$

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\} \text{ , denn ist } a \in \mathbb{Z} \text{ beliebig}$$

$$i = a - \left\lfloor \frac{a}{m} \right\rfloor m \in \{0, 1, \ldots, m-1\} \text{ , dann ist } [a]_m = [i]$$

**Bemerkung:** Statt $a \sim_m b$ für $a, b \in \mathbb{Z}$ schreibt man oft

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

**Beispiel:** $R = \mathbb{Z}, m = 3$

$$[0]_m = \{0, 3, -3, 6, -6, \ldots\}$$

$$[1]_m = \{1, 4, -2, 7, -5, \ldots\}$$

$$[2]_m = \{2, 5, -1, 8, -4, \ldots\}$$

$$\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z} = \{[0]_3 = 0, [1]_3 = 1, [2]_3 = 1 + 1\}$$

**Konvention:** In jedem kommutativen Ring $R$ schreibt man $1+1 = 2, 1+1+1 = 3$ allgemein: $a \in R, \underbrace{a + \ldots + a}_{r} =: r \cdot a$,
z.B. $2 + 2 = 1$ in $\mathbb{Z}_3$, genauer: $[2]_3 + [2]_3 = [4]_3 = [1]_3$

**Beispiel:** Behauptung: Keine ganze Zahl der Form $7 + n \cdot 8$ ist eine Summe von 3 Quadraten in $\mathbb{Z}$ (für $n \in \mathbb{Z}$)

**Beweis:** Annahme: $z = z + n \cdot 8 = a^2 + b^2 + c^2$ für $a, b, c \in \mathbb{Z}$
Betrachte: $\varphi : \mathbb{Z} \to \mathbb{Z}_8 = \mathbb{Z}/8\mathbb{Z} : z \mapsto [z]$ Homomorphismus Dann folgt:

$$\varphi(z) = \varphi(a^2) + \varphi(b^2) + \varphi(c^2)$$

$$[z]_8 = \varphi(a)^2 + \varphi(b)^2 + \varphi(c)^2$$
$$= a'^2 + b'^2 + c'^2; a', b', c' \in \mathbb{Z}$$

in $\mathbb{Z}_8$:

| z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $z^2$ | 0 | 1 | 4 | 1 | 0 | 1 | 4 | 1 |

Quadrate sind 0, 1, 4 $\Rightarrow$ Summen von 3 Quadraten sind: $0 = 0^2 + 0^2 + 0^2$
$1 = 1^2 + 0^2 + 0^2$
$2 = 1^2 + 1^2 + 0^2$

$3 = 1^2 + 1^2 + 1^2$
$4 = 2^2 + 0^2 + 0^2$
$5 = 2^2 + 1^2 + 0^2$
$6 = 2^2 + 1^2 + 1^2$
$\Rightarrow$ 7 ist in $\mathbb{Z}$ keine Summe von 3 Quadraten. Also war die Annahme falsch.

(25.05.01)

**Beispiel:** Pseudozufallszahlen $m \in \mathbb{N}, \mathbb{Z} = \{0, 1, \ldots, m-1\}$

$$z_0 = 0 \text{ Startwert (z.B. [Datum } \cdot \text{ Uhrzeit]}_m$$

$$z_n = a_{n-1} + c \text{ in } \mathbb{Z}_m$$

eigentlich: $[z_n]_m = [a]_m[z_{n-1}]_m + [c]_m$ mit *geeigneten* a und c in $\mathbb{Z}_n$

Jede solche Folge $(z_n)_{n \in \mathbb{N}_0}$ wird periodisch werden.

$$z_j = z_{j+k} \Rightarrow z_{j+1} = z_{j+k+1}$$

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

$$F = \sum_{n=0}^{\infty} z_n x^n = z_0 + \sum_{n=1}^{\infty} z_n x^n = z_0 + \sum_{n=1}^{\infty} (a z_{n-1} + c) x^n \in \mathbb{Z}_m[[x]]$$

$$= axF + c\frac{x}{1-x} \text{ , da } z_0 = 0$$

$$F = c\frac{x}{1-x} \cdot \frac{1}{1-ax} = c\frac{x}{1-x} \sum_{n=0}^{\infty} a^n x^n = c \sum_{n=1}^{\infty} (1 + a + \ldots + a^{n-1}) x^n$$

Also $z_n = c(1 + a + \ldots + a^{n-1})$ für $n \geq 1$ in $\mathbb{Z}_m$
$a$ und $c$ zu bestimmen, dass Periode in $\mathbb{Z} = \{z_0, z_1, \ldots, z_{m-1}\}, z_m = z_0$
Also $= \{\underbrace{c(1 + a + \ldots + a^{n-1})}_{\text{insbes. } =1 \text{ für ein } n} | n = 1, \ldots, m\}$
Also muss $c$ in $\mathbb{Z}_m$ invertierbar sein [ggT($c$,$m$) $= 1$ in $\mathbb{Z}$], $a^m = 1$ in $\mathbb{Z}_m$
(Fortsetzung folgt)

## 2.4 Grösste gemeinsame Teiler, Euklidische Ringe

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

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

Dann ist

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

aber

$$[p]_m \neq 0, [q]_m \neq 0 \text{ , weil } 1 < p, q < m$$

**Definition:** 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) ist und $R$ keine Nullteiler enthält.
(insbes. gilt dann: $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$)

**Beispiele:** $\mathbb{Z}, K[x], K[[x]], \ldots$ ($K$ Körper) sind Integritätsbereiche
Kein Integritätsbereich ist $\mathbb{Z}_0, \mathbb{Z}_4, \ldots, \mathbb{Z}_m$ für $m$ nicht Primzahl

Im Folgenden sei $R$ ein Integritätsbereich

**Definition:** $a, b \in R, a|b$ „a teilt b" $\Leftrightarrow \exists z \in R$ mit $b = a \cdot z$
$d \in R$ heisst ein grösster gemeinsamer Teiler von $a$ und $b$ "in Zeichen $d \in ggT(a, b)$", wenn $d|a$ und $d|b$ und zusätzlich gilt aus $c|a$ und $c|b$ folgt $c|d$

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

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

**Bemerkung:** $d \in ggT(a, b)$ in $R$ und $u$ Einheit in $R \Rightarrow u \cdot d \in ggT(a, b)$
umgekehrt: Sind $d, d' \in ggT(a, b)$, so gilt $d'|d$ und $d|d'$, d.h.

$$\begin{array}{ll} \exists v \in R & d' = d \cdot v \quad \Rightarrow d' = d' \cdot v' \cdot v \\ \exists v' \in R & d = d' \cdot v' \end{array}$$

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

Wie findet man $ggT(a, b)$?
(**Bemerkung:** 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:** Ein Integritätsbereich $R$ zusammen mit $\delta$ heisst ein (Norm-)Euklidischer Ring, wenn $\delta : R \backslash \{0\} \to \mathbb{N}_0$

$$[\delta : R \to \mathbb{N}_0 \text{ mit } \delta(a) = 0 \Leftrightarrow a = 0 \text{ und } \delta(ab) = \delta(a) \cdot \delta(b)]$$

mit folgender Eigenschaft:
Zu $a, b \in R$ 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:**

$$(\mathbb{Z}, ||) \text{ ist (norm-)euklidisch, wobei } |a| = \begin{cases} a & a \geq 0 \\ -a & a < 0 \end{cases}$$

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

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

$$R = (K[x], \delta) \text{ ist normeuklidisch, mit } \delta(f) = \begin{cases} 2^{Grad\ f} & f \neq 0 \\ 0 & f = 0 \end{cases}$$

**Satz 1:** Ist $(R, \delta)$ 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

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

**Beweis:** (Euklidischer Algorithmus)

(30.05.01)

**Definition:** $(R, \delta)$ euklidischer Ring, wenn $R$ Integritätsbereich und $\delta : R\backslash\{0\} \to \mathbb{N}_0$ mit

Zu $a, b \in R, b \neq 0$ gibt es stets $q, r \in R$ mit $a = qb + r$ wobei $r = 0$ oder $\delta(r) = \delta(b)$

**Beispiel:** $(\mathbb{Z}, |)$ oder $(K[x], Grad)$

**Satz 1:** In einem euklidischen Ring $(R, \delta)$ gibt es zu $a, b \in R$ stets ein $d \in ggT(a, b)$ und es ist

$$d = ya + zb \text{ für } y, z \in R$$

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

$$\begin{array}{rccc} & a = bq_1 + r_1 & [\text{mit } r_1 = 0 \text{ oder}] & \delta(r_1) < \delta(b) \\ \text{sonst } (b \neq 0) \text{ ex. } q_1, r_1 \in R \text{ mit} & b = q_2 r_1 + r_2 & \text{mit} & \delta(r_2) < \delta(r_1) \\ & r_1 = q_3 r_2 + r_3 & \text{mit} & \delta(r_3) < \delta(r_2) \end{array}$$

nach endlich vielen (sp“atestens $\delta(b) + 1$) Schritten wegen $\delta(b) > \delta(r_1) > \ldots \geq 0$

$$r_{n-2} = q_n r_{n-1} + r_n, \delta(r_n) < \delta(r_{n-1})$$

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

[setze $b = r_0$ und $a = r_{-1}$]

**Behauptung:** Es gilt $y_j, z_j$ mit

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

, denn für $j = 1$ setze $y_1 = 1$ und $z_1 = -q_n$

Schritt $j \mapsto j + 1$:

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

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

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

**Lemma 1:**

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

**Beweis:** Zeige: $d|a, b \Rightarrow d|b, a - qb$
denn $a = da_1, b = db_1$ mit

$$a_1, b_1 \in R \Rightarrow \begin{array}{c} b = db_1 \\ a - qb = d(a_1 - qb_1) \end{array}$$

d.h. $d|b, a - qb$

**Satz 2:** Ist R$(R, \delta)$ euklidischer Ring, $a, b \in R$
Dann ist $[b]_a = b + a \cdot R = R/aR$ genau dann invertierbar (”Einheit”), wenn $1 \in ggT(a, b)$

**Beweis:**

a) Angenommen $1 \in ggTa, b$
Nach Satz 1 gibt es $y, z \in R$ mit $1 = ya + zb$

$$zb - 1 = (-y)a \in Ra$$

$$[zb]_a = [1]_a$$

$$= [z]_a [b]_a = 1 \text{ Einselement von } R/aR$$

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

b) Sei $[b]_a$ invertierbar in $R/aR$, d.h. $\exists z \in R [b]_a^{-1} = [z]_a$, also $[b]_a[z]_a = 1$

$$bz - 1 = ya \text{ für ein } y \in R$$

$$bz - ya = 1$$

Sei $d|a, b \Rightarrow d|ay, bz \Rightarrow d|bz - ay = 1 \Rightarrow d$ ist Einheit in $R$, also ist $1 \in ggT(a, b)$

**Folgerung:** Ist $m \in \mathbb{N}$, so ist

$$[c]_m \text{ in } \mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \text{ invertierbar genau dann, wenn } 1 \in ggT(c, m)$$

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

$$R^* = \{a \in R | \exists a^{-1} \in R \text{ mit } aa^{-1} = 1\}$$

**Beispiel:**

$$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$$

$$\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$$

$$\mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$$

**Definition:**

$$|\mathbb{Z}_m^*| =: \varphi(m) \text{ für } m \in \mathbb{N}, \varphi \text{ heißt Eulersche } \varphi\text{-Funktion}$$

z.B. $\varphi(6) = 2, \varphi(8) = 4$ ( $\varphi(m)$ = Anzahl der zu $m$ teilerfremden Zahlen in $\{1, \ldots, m-1\}$)

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

**Beweis:** $\mathbb{Z}_1 = \mathbb{Z}/1\mathbb{Z} = \{[0]_1\} = \{0\}$ kein Körper
Ist $m > 1$ keine Primzahl, so ist $m = a \cdot b$ mit $1 < a, b < m$
Dann ist $[a]_m[b]_m = [m]_m = [0]_m = 0$
also ist $\mathbb{Z}/m\mathbb{Z}$ kein Integritätsbereich (es gibt Nullteiler), also kein Körper.
Umgekehrt ist $m$ Primzahl, so ist für jedes $a \in \mathbb{N}$ mit $1 \leq a < m$
$1 \in ggT(a, m)$, also nach Folgerung (Satz 2) $[a]_m$ ist invertierbar.
Also jedes $[a] \neq 0$ in $\mathbb{Z}_m$ hat Inverses.

**Satz 3:** Ist $(R, \delta)$ euklidischer Ring und ist $I \trianglelefteq R$, so gibt es $a \in R$ mit $I = Ra$.
D.h. in einem euklidischen Ring gibt es nur Hauptideale
"Ein euklidischer Ring ist ein Hauptidealring"

**Beweis:** Ist $I = \{0\}$ das Nullideal, so ist $I = R \cdot 0$
Es sei nun $I \neq \{0\}$ ein Ideal in $R$

$$\emptyset \neq \{\delta(y) | y \in I \backslash \{0\}\} \subseteq \mathbb{N}_0$$

$$m = Min\{\delta(y) | y \in I \backslash \{0\}\} \subseteq \mathbb{N}_0 \text{ und es sei } m = \delta(a) \text{ für ein } a \in I \backslash \{0\}$$

**Behauptung:** $I = Ra$

**Beweis:**

a) Da $a \in I$, gilt $ya \in I$ für jedes $y \in R$, also gilt $Ra \subseteq I$

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

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

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

$\delta(r) < \delta(a)$ ist unmöglich, weil $\delta(a) = Min\{\delta(y) | y \in I \backslash \{0\}\}$
Also folgt $r = 0$, d.h. $b \in Ra, I \subseteq Ra$

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

## 2.5 Eindeutige Primfaktorzerlegung

$R$ sei ein Integritätsbereich (kommutativer Ring mit $a \cdot b = 0 \Rightarrow a = 0$ oder $b = 0$)

**Definition:** $p \in R$ heisst irreduzibel, wenn

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

**Beispiel:** In $\mathbb{Z}$: $p$ ist irreduzibel $\Leftrightarrow$ $p$ ist Primzahl oder $-p$ ist Primzahl

**Lemma 1:** Ist $(R, \delta)$ euklidischer Ring und $p$ irreduzibel, so folgt:

$$p|ab \Rightarrow p|a \text{ oder } p|b$$

**Beweis:** Angenommen $p|ab$ und $p \not| a$
Zu zeigen: $p \not| b$
Da $p \not| a$ folgt $1 \in ggT(a, p)$
Nach Satz 1, Kapitel 4 gibt es $y, z \in R$ mit

$$1 = ya + zp$$

$$b = y \underbrace{ab}_{p|} + \underbrace{zbp}_{p|}$$

Also $p|b$

$(R, \delta)$ Normeuklidisch, wenn $\delta : R \rightarrow \mathbb{N}_0$ mit

$$\delta(a) = 0 \Rightarrow a = 0 \text{ und } \delta(ab) = \delta(a)\delta(b) \text{ und}$$

Zu $a, b \in R, b \neq 0$ ex. $q, r \in R$ mit

$$a = qb + r \text{ mit } \delta(r) < \delta(q)$$

**Beispiele:** $(\mathbb{Z}, ||)$
$(K[x], \delta), \delta(f) = z^{Gradf} = 0$ falls $f = 0$

**Folgerung:** Ist $(R, \delta)$ normeuklidisch, so gilt

$$a \in R^* \Rightarrow \delta(a) = 1$$

denn aus $1 \cdot 1 = 1$ folgt

$$\delta(1) = \delta(1)\delta(1) \in \mathbb{N}$$

$$\delta(1) = 1$$

aus $a \cdot a^{-1} = 1$ folgt

$$\delta(a)\delta(a^{-1}) = 1 \text{ oder } \delta(a) = 1$$

(01.06.01)

$$p \in R \text{ irreduzibel } \Leftrightarrow \ p \neq 0, p \in R^*$$

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

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

**Satz 1:** Ist $(R, \delta)$ normeuklidischer Ring, dann hat jedes $a \in R\backslash\{0\}$ eine Darstellung in der Form $a = u \cdot p_1 \cdot \ldots \cdot p_r$ und $u \in R^*, p_i$ irreduzibel
Gilt auch $a = vq_1 \ldots q_s$ mit $v \in R^*, q_i$ irreduzibel, so gilt $v = s$ und es gibt eine Permutation $\sigma \in S_r$ mit $q_i = u_i p_{\sigma(i)}$ mit $u_i \in R^*$

**Beweis:**

a) Existenz, Induktion nach $\delta(n)$

$$\delta(n) = 1 \Rightarrow \ a \in R^*$$

$$(1 = qa + r \text{ mit } \delta(n) < \delta(a) = 1$$

$$\delta(r) = 0 \Rightarrow \ r = 0 (\delta \text{ Norm})$$

$$q = a^{-1}, a \in R^*)$$

a = u , r = 0
$\delta(a) > 1$: Ist $a$ irreduzibel, so $a = d \cdot a$
sonst $a = b \cdot c$ und $c \notin R^*$

$$\delta(a) = \delta(b) \cdot \delta(c) \text{ und } \delta(a) > \delta(b), \delta(c) > 1$$

Nach Ind.Ann.

$$b = up_1 \ldots p_l, u \in R^*, p_i \text{ irreduzibel}$$

$$c = u' p_{l+1} \ldots p_r, u' \in R^*, p_i \text{ irreduzibel}$$

$$a = bc = \underbrace{uu'}_{\in U^*} p_1 \ldots p_r$$

b) Eindeutigkeit

$$a = up_1 \ldots p_r; p_i, q_j \text{ irreduzibel}$$

$$= vq_1 \ldots q_r; u, v \in R^*$$

Induktion nach $Min(r, s) = r$

$$r = 0 \text{ dann } a \in R^*, s = 0 \text{ und } u = v = a$$

$$r > 0, p_r|a = vq_1 \ldots q_s$$

Nach Lemma 1 (mehrfach angewandt) gibt es $j$ mit

$$p_r|q_j \text{ œ} j = s$$

$$q_s = u_r p_r \text{ dabei } u_r \in R^*$$

$$0 = a - a = p_r \underbrace{(up_1 \cdot \ldots \cdot p_{r-1} - vu_r q_1 \cdot \ldots \cdot q_{s-1})}_{=0}$$

Nach Ind.Ann. $r - 1 = s - 1$ und bei passender Sortierung ist

$$q_i = u_i p_i \text{ mit } u_i \in R^*$$

**Corrolar:**

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

$$a = up_1 \ldots p_r; p_i \text{ Primzahl } ; u \in \{1, -1\}$$

$\Rightarrow$

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

$$f = uf_1 \ldots f_r \text{ mit } u \in K^* \text{ und } f_i \text{ irreduzibel und normiert}$$

**Definition:**

$$f = \sum_{i=o}^{n} a_i x^i \text{ heisst normiert (engl. monic), wenn } a_n = 1$$

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

$$R/fR = \{[g]_f | g \in R, \delta(g) < \delta(f)\} \cup \{0\}$$

oder

$$[g]_f = g + fR (= \{g + fz | z \in R\})$$

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

**Beweis:**

a)

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

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

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

$$g \cdot r = q \cdot f \in fR$$

$$[q]_f = [r]_f$$

Nach Definition ist

$$R/fR = \{[g]_f | g \in R\} = \{[g]_f | g \in R, \delta(g) < \delta(f)\} \cup \{0\}$$

b) Behauptung: Ist $f$ irreduzibel, dann ist $R/fR$ ein Körper.
**Beweis:**

(i) Sei $0 \neq [g]_f \in R/fR$, zu zeigen: $[g]_f$ hat Inverses

$$f \not| g; 1 \in ggT(f,g) \text{ weil } f \text{ irreduzibel}$$

Es gibt $1 = yf + zg$ mit $y, z \in R$

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

$$\Rightarrow [g]_f \text{ invertierbar mit } [g]_f^{-1} = [z]_f$$

Also ist $R/fR$ Körper.

(ii) Es sei $f$ nicht irreduzibel

$$f = ab \text{ mit } a, b \notin R^*$$

$$0 = [f]_f = [a]_f \cdot [b]_f$$

Wäre $[a]_f = 0$, so wäre

$$f/a = fa_1, a_1 \in R$$

$$f = ab = fa_1 b \Rightarrow b \in R^* \text{ Widerspruch!}$$

Also ist $R/fR$ kein Integritätsbereich, also erst recht kein Körper.
Schliesslich: Ist $f \in R^*$, so ist $R/fR = R/R = \{0\}$ und $R/fR$ kein Körper.

**Beispiel:**

$$R = \mathbb{Z}_2[x], \mathbb{Z}_2 = \{0,1\} \cong \mathbb{Z}/2\mathbb{Z}$$

$$f = x^2 + x + 1 \in R, \delta(g) = Grad g$$

$$R/fR = \{[g]_f | g \in R, Grad g < 2\} \cup \{0\}$$

Polynome vom $Grad 0$ in $\mathbb{Z}_2[x]$: 1
Polynome vom $Grad 1$ in $\mathbb{Z}_2[x]$: $x, x+1$
$|R/fR| = 4$
$R/fR = \{[0]_f, [1]_f, [x]_f, [x+1]_f\}$

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

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

**Beispiel:**

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

$$[2]_4[2]_4 = [4]_4 = 0$$

$$[3]_4[3]_4 = [9]_4 = 1$$

(13.06.01)

$(R, \delta)$ Euklidischer Ring
z.B. $(\mathbb{Z}, ||), (K[x], Grad) K$ Körper
Division mit Rest
eukl. Algorithmus: Zu $a, b \in R$ gibt es $d \in ggT(a, b)$

$$d = ya + zb \text{ mit } y, z \in R$$

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

$$(q \in R \text{ irred. } \Leftrightarrow \ q \neq 0, q \notin R^*, q = a \cdot b \Rightarrow a \in R^* \text{ oder } b \in R^*)$$

z.B.:

$$\mathbb{Z}/p\mathbb{Z} \text{ Körper } \Leftrightarrow \ p \text{ Primzahl, } p \in \mathbb{N}$$

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \text{ ist Körper mit } p \text{ Elementen, falls } p \text{ Primzahl}$$

$$\mathbb{Z}_{p^2} = \mathbb{Z}/p^2\mathbb{Z} \text{ ist Ring mit } p^2 \text{ Elementen, kein Körper}$$

**Beispiel:**

$$R = K[x], K \text{ Körper}$$

$$R/fR = \{[g]_f | g \in K[x]\}$$

$$[g]_f = g + fK[x]$$

$$[g]_f = [h]_f \Leftrightarrow \ g - h \in fK[x] \Leftrightarrow \ g - h = g \cdot f \text{ mit } q \in K[x]$$

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

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

$$|K[x]/fK[x]| = p^n$$

$$K[x]/fK[x] = \{[a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}]_f | a_i \in \mathbb{Z}_p\}$$

$$\text{und } K[x]/fK[x] \text{ Körper } \Leftrightarrow \ f \text{ ist irreduzibel}$$

**Beispiel:**

$$K = \mathbb{Z}_2, f = x^3 + x + 1 \in K[x] \text{ irreduzibel (s. Aufgabe 27)}$$

$$L = K[x]/fK[x] \text{ ist Körper mit 8 Elementen}$$

$$= \{[a_0 + a_1 x + a_2 x^2]_f | a_0, a_1, a_2 \in \mathbb{Z}_2\}$$

Die Elemente von $L$ werden durch 3 Bits dargestellt

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

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

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

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

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

$$\alpha^5 = \alpha^4 \cdot \alpha = [x^3 + x^2]_f = [x^2 + x + 1]_f \leftrightarrow \ 111 \text{ , da } x^3 + x^2 = x^3 + x + 1 + x^2 + x + 1$$

$$\alpha^6 = \alpha^5 \cdot \alpha = [x^3 + x^2 + x]_f = [x^2 + 1]_f \leftrightarrow \ 101 \text{ , da } x^3 + x^2 + x = x^3 + x + 1 + x^2 + 1$$

$$\alpha^7 = \alpha^6 \cdot \alpha = [x^3 + x]_f = [1]_f \leftrightarrow \ 100$$
$$\alpha^8 = \alpha$$

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

$$\alpha^3 \cdot \alpha^2 = \alpha^5$$
$$\alpha^3 \cdot \alpha^5 = \alpha^8 = \alpha^7 \cdot \alpha = \alpha$$
$$\alpha^3 + \alpha^5 = [x^2]_f = \alpha^2$$

## 2.6 Der Chinesische Restsatz

$R_1, \ldots, R_r$ seien Ringe; dann wird

$$R = R_1 \times \ldots \times R_r = \{(a_1, \ldots, a_r) | a_i \in R_i\}$$

zu einem Ring $R = (R, +, -, 0, \cdot, 1)$ mit

$$(a_1, \ldots, a_r) + (b_1, \ldots, b_r) = (a_1 + b_1, \ldots, a_r + b_r)$$
$$(a_1, \ldots, a_r) \cdot (b_1, \ldots, b_r) = (a_1 \cdot b_1, \ldots, a_r \cdot b_r)$$
$$-(a_1, \ldots, a_r) = (-a_1, \ldots, -a_r)$$
$$0 = (0, \ldots, 0)$$
$$1 = (1, \ldots, 1)$$

**Lemma 1:** Ist $R$ euklidischer Ring und sind $q_1, q_2 \in R$ mit $1 \in ggT(q_1, q_2)$, "d.h. $q_1, q_2$ teilerfremd", so gilt

$$q_1 | a \text{ und } q_2 | a \Rightarrow q_1 \cdot q_2 | a$$

**Beweis:**

$$1 = yq_1 + zq_2; y, z \in R$$
$$a = ayq_1 + azq_2$$

Nach Voraussetzung ist $a = q_1 a_1, a = q_2 a_2$

$$a = yq_1 q_2 a_2 + za_1 q_1 q_2 = q_1 q_2 (ya_2 + za_1)$$

**Bemerkung:** $4|12$ und $6|12$ in $\mathbb{Z}$, aber $4 \cdot 6 \not| 12$, da $ggT(4, 6) = 2 \neq 1$

**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 $m = q_1 \ldots q_r$

$$R/mR = R/q_1 R \times \ldots \times R/q_r R$$
$$\psi : [a]_m \mapsto ([a]_{q_1}, \ldots, [a]_{q_r})$$

(dabei ist $[a]_m = a + mR, [a]_{q_i} = a + q_i R$)

**Beweis:**

$$\overset{\wedge}{\psi}: R \to R/q_1 R \times \cdot \times R/q_r R : a \mapsto ([a]_{q_1}, \ldots, [a]_{q_r})$$

ist offenbar ein Ringhomomorphismus, mit

$$Kern \overset{\wedge}{\psi} = \{a \in R | \overset{\wedge}{\psi}(a) + 0\}$$

$$= \{a \in R | [a]_{q_1} = 0, \ldots, [a]_{q_r} = 0\}$$

$$= \{a \in R | q_1 | a, \ldots, q_r | a\}$$

$$= \{a \in R | m = q_1 \ldots q_r | a\} \text{ mehrfache Anwendung von Lemma 1}$$

$$= mR$$

Nach Homomorphiesatz aus 2.1

$$\psi : R/mR \cong Bild \overset{\wedge}{\psi} : [a]_m \to \overset{\wedge}{\psi}(a) = ([a]_{q_1}, \ldots, [a]_{q_r})$$

z.z. $Bild\psi = R/q_1R \times \ldots \times R/q_rR$

**Beweis:** Wir finden Umkehrabb. $\eta : R/q_1R \times \ldots \times R/q_rR = \overline{R}$ mit $\psi \cdot \eta = id_{\overline{R}}$ dazu setze

$$q_i' = \frac{m}{q_i} = q_1 \ldots q_{i-1} q_{q+1} \ldots q_r$$

$$1 \in ggT(q_i, q_i') \text{ weil } q_1, \ldots, q_r \text{ paarweise teilerfremd}$$

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

$$([1]_{q_i} = [z_i q_i']_{q_i})$$

Definiere

$$\eta([a_1]_{q_1}, \ldots, [a_r]_{q_r}) = \left[\sum_{i=1}^{r} a_i q_i' z_i\right]_m, a_i \in R$$

Dann gilt

$$\psi \circ \eta([a_1]_{q_1}, \ldots, [a_r]_{q_r}) = \psi\left[\sum_{i=1}^{r} a_i z_i q_i'\right]_m = \sum_{i=1}^{r} ( \underbrace{[a_i z_i q_i']_{q_1}}_{=0 \text{ für } i \neq 1}, \ldots, \underbrace{[a_i z_i q_i']_{q_r}}_{=0 \text{ für } i \neq r} )$$

$$([a_1 z_1 q_1']_{q_1}, \ldots, [a_r z_r q_r'])$$

$$([a_1]_{q_1}, \ldots, [a_r z_r q_r']_{q_r})$$

$$([a_1]_{q_1}, \ldots, [a_r]_{q_r}) \text{ also } \psi \circ \eta = id$$

**Beispiel:**

$$R = \mathbb{Z}, m = 60 = 3 \cdot 4 \cdot 5$$

$$q_1 = 3, q_1' = 20$$

$$q_2 = 4, q_2' = 15$$

$$q_3 = 5, q_3' = 12$$

$$1 = 7 \cdot 3 + \underbrace{(-1)}_{z_1} \cdot 20, 1 = (-11) \cdot 4 + \underbrace{(3)}_{z_2} \cdot 15, 1 = 5 \cdot 5 + \underbrace{(-2)}_{z_3} \cdot 12$$

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

$$[43]_{60} \cdot [35]_{60} \to ([1]_3, [3]_4, [3]_5) \cdot ([2]_3, [3]_4, [0]_5)$$

$$= ([2]_3, [1]_4, [0]_5) \to [2 \cdot (-1) \cdot 20 + 1 \cdot 3 \cdot 15 + 0 \cdot (-2) \cdot 12]_{60}$$

$$= [-40 + 45]_{60} = [5]_{60}$$

$$\Rightarrow [43]_{60} \cdot [35]_{60} = [5]_{60}$$

**Folgerung:** (Chinesischer Restsatz)
Sind $q_1, \ldots, q_r$ paarweise teilerfremde ganze Zahlen und $m = q_1 \cdot \ldots \cdot q_r$ und sind $a_1, \ldots, a_r \in \mathbb{Z}$ beliebig, so gibt es genau ein $a \in \{0, 1, \ldots, m-1\}$ mit $a \equiv a_i \bmod q_i$ für $i = 1, \ldots, r$, d.h. $q_i | a - a_i$

(15.06.01)

**Satz 1:** $R$ euklidischer Ring, $m = q_1 \ldots q_r$

$$1 \in ggT(q_i, q_j), i \neq j$$

$$\psi : R/mR \rightarrow R/q_1R \times \ldots \times R/q_rR : [a]_m \rightarrow ([a]_{q_1}, \ldots, [a]_{q_r}) \text{ ist Isomorphismus}$$

**Folgerung:** (Chinesischer Restsatz)
Ist $m = q_1 \ldots q_r \in \mathbb{N}, 1 \in ggT(q_i, q_j)$ für $i \neq j$, dann gibt es zu $a_1, \ldots, a_r \in \mathbb{Z}$ beliebig stets genau ein $a \in \{0, \ldots, m-1\}$ mit

$$a \equiv a_i \bmod q_i \text{ für } i = 1, \ldots, n \tag{2.1}$$

(Die Menge aller $a \in \mathbb{Z}$ mit (2.1) ist gerade $[a]_m = a + m\mathbb{Z}$)

**Beweis:** Wende Satz 1 an mit $R = \mathbb{Z}$
Da $\psi$ 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 $[a]_m \in \mathbb{Z}/a\mathbb{Z}$ mit

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

$[a]_m$ eindeutig, weil $\psi$ auch injektiv.

$\psi([a]) = ([a]_{q_1}, \ldots, [a]_{q_r}) = ([a_1]_{q_1}, \ldots, [a_r]_{q_r})$ , da $[a]_{q_1} = [a_i]_{q_i}, a \equiv a_i \bmod q_i, i = 1, \ldots, r$

In $[a]_m$ existiert genau ein $a$ mit $0 \leq a \leq m-1$

**Folgerung 2:** Voraussetzung und Bezeichnung wie in Satz 1. Dann gilt

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

Also

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

**Beweis:** Ein Isomorphismus $\psi$ bildet Einheiten auf Einheiten ab, weil

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

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

$$R/q_iR \times \ldots \times R/q_rR)^* = (R/q_iR)^* \times \ldots \times (R/q_rR)^*$$

## 2.7 Die Eulersche Phi-Funktion und Möbius-Inversion

**Satz 1:** Ist $\phi$ die Eulersche $\phi$-Funktion, d.h.

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

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

$$\phi(m) = p_1^{n_1 - 1}(p_1 - 1) \ldots p_r^{n_r - 1}(p_r - 1) \tag{2.2}$$

**Beispiel:**

$$\phi(60) = \phi(3 \cdot 4 \cdot 5) = \phi(3 \cdot 2^2 \cdot 5) = 2 \cdot 2 \cdot 4 = 16$$
$$\phi(1) = 1 = |\{j \in \{1\} | ggT(1, 1) = 1\}| = |\{1\}| = 1$$

**Beweis:** Wende Folgerung 2 aus 2.6 an mit $R = \mathbb{Z}, q_i = p_i^{n_i}$

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

Nur zu zeigen: $\phi(p^n) = p^{n-1}(p-1)$ mit $n \in \mathbb{N}, p$ Primzahl

$$j \in \{1, \ldots, p^n\} \text{ erfüllt } 1 \notin ggT(j, p^n) \Leftrightarrow p | j \Leftrightarrow j \in \{p, 2p, \ldots, (p^{n-1}) \cdot p\} = M$$

$$\psi(p^n) = |\{j \in \{1, \ldots, p^n\} | 1 \in ggT(j, p^n)\}| = p^n - |M|| = p^n - p^{n-1} = p^{n-1}(p-1)$$

**Bemerkung:** Die Formel (2.2) aus Satz 1 lässt sich auch so schreiben:

$$\phi(m) = m \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_r})$$
$$= \frac{m}{1} - (\frac{m}{p_1} + \ldots + \frac{m}{p_r}) + \prod_{i<j} \frac{m}{p_i p_j} - + \ldots + (-1)^r \frac{m}{p_1 \ldots p_r}$$

**Definition:**

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

$\mu : \mathbb{N} \to \mathbb{Z}$ "Möbiusfunktion"

**Folgerung:**

$$\phi(m) = \sum_{d|m} \mu(d) \frac{m}{d}$$

**Lemma 1:** Es gilt für die Möbiusfunktion

$$\sum_{d|m} \mu(d) = \begin{cases} 1 & m = 1 \\ 0 & \text{sonst} \end{cases}$$

Man kann dies als rekursive Formel deuten:

$$\mu(1) = 1, \mu(m) = - \sum_{d|m, 1 \leq d < m} \mu(d)$$

**Beweis:**$\phi(1) = 1$
Also sei $m > 1$:

$$m = p_1^{n_1} \dots p_r^{n_r}, p_i \neq p_j \text{ für } i \neq j, p_i \text{ Primzahlen}$$

$$d|m \Rightarrow d = p_1^{m_1} \dots p_r^{m_r} \text{ mit } 0 \leq m_i \leq n_i$$

$$d|m \text{ und } \mu(d) \neq 0 \Rightarrow m_i \in \{0, 1\}$$

$$\{d|m \text{ mit } \mu(d) \neq 0\} \leftrightarrow \{ \text{ Teilmengen von } P = \{p_1, \dots, p_r\}\}$$

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

$$\sum_{d|m} \mu(d) = \sum_{\substack{d|m \\ \mu(d)\neq 0}} \mu(d) = \sum_{M \subset P} \mu(\prod_{p \in M} p)$$

$$= \sum_{j=0}^{r} \sum M \leq \binom{p}{j} \underbrace{\mu(\prod_{p \in M} p)}_{=(-1)^j} = \sum_{j=1}^{r} \binom{r}{j} (-1)^j \overset{Kap.1}{=} (1-1)^R = 0$$

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

$$g(m) := \sum_{d|m} f(d) \text{ "Summatorische Funktion zu f"}$$

Dann gilt

$$f(m) = \sum_{d|m} \mu(d) g(\frac{m}{d}) \tag{2.3}$$

**Beweis:**

$$\sum_{d|m} \mu(d) g(\frac{m}{d}) = \sum_{d|m} \mu(d) \sum_{c|\frac{m}{d}} f(c) = \sum_{c|m} \underbrace{\left( \sum_{d|\frac{m}{c}} \mu(d) \right)}_{\substack{nach\ Lemma\ 1 \\ \begin{matrix} =0 & für\ \frac{m}{c} \neq 1 \\ =1 & für\ c=m \end{matrix}}} f(c) = f(m)$$

(20.06.01)

## 2.8 Gruppen und Untergruppen

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

**Beispiele:**

a)

$$R \text{ Ring} \Rightarrow (R, +, -, 0) \text{ Abelsche Gruppe}$$

$$(\mathbb{Z}, +) \text{ Gruppe}$$

$$(\mathbb{Z}_m, +), |\mathbb{Z}_m| = m \in \mathbb{N}$$

b)

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

c)

$$GL_n(K) = \{A \in K^{n \times n} | det\ A \neq 0\}, K \text{ Körper}$$

**Bemerkung:** Ist $R$ Ring und ist

$$R^* = \{a \in R | \exists a^{-1} \in R \text{ mit } aa^{-1} = a^{-1}a = 1\}$$

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

**Beispiel:**

d)

$$\mathbb{Z}_m^* = \{[a]_m | 1 \in ggT(a, m)\}, m \in \mathbb{N}$$

"prime Restklassengruppe modulo m"

$$|\mathbb{Z}_m^*| = \varphi(m), \varphi \text{ Eulersche Funktion}$$

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

$$g \cdot H = \{gh | h \in H\}$$

Linksnebenklasse (von $g$ bezüglich $H$) , beachte: $(G, \cdot)$

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

$$g \sim g' \overset{Def.}{\Leftrightarrow} g^{-1}g' \in H$$

eine Äquivalenzrelation auf $G$ definiert und

$$[g]_\sim = gH$$

**Beweis:**

- $\sim$ Reflexivität: gilt, weil $1 = g^{-1}g \in H$ für alle $g$
- $\sim$ Symmetrie: gilt, weil

  $g \sim g'$ bedeutet $g^{-1}g' \in H \Rightarrow H \ni (g^{-1}g')^{-1} = g'^{-1}g \in H \Leftrightarrow\ g' \sim g$

- $\sim$ Transitivität:

$$\text{Seien } \begin{array}{lll} g \sim g' & \text{also} & g^{-1}g' \in H \\ g' \sim g'' & \text{also} & g'^{-1}g'' \in H \end{array}$$

$$H \ni g^{-1}g'g'^{-1}g'' = g^{-1}g'', \text{ also } g \sim g''$$

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

$$g' = g \cdot h \in gH$$

**Folgerung:** Die Linksnebenklassen von $H$ in $G$ bilden eine Partition.

**Satz:**(von Lagrange) Ist $(G, \cdot)$ Gruppe mit $|G| < \infty$ und $H \leq G$, dann ist

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

wobei $[G : H]$ = Anzahl der Linksnebenklassen von $H$ in $G$ = "Index von $H$ in $G$"
$|H|$ = Anzahl der Elemente von $H$ = "Ordnung von H"
Insbesondere gilt: $|H| \mid |G|$

**Beweis:** $G = g_1 H \dot{\cup} \ldots \dot{\cup}\, g_r H$ (nach Lemma 1 bzw. Folgerung) $|G| < \infty$

$$\psi_i : H \to g_i H : h \mapsto\ g_i h$$

$\psi_i$ ist injektiv, weil $g_i h = g_i h'$ für $h, h' \in H$

$$\Rightarrow h = g_i^{-1} g_i h - g_i^{-1} g_i h' = h'$$

$\psi_i$ ist surjektiv: jedes Element aus $g_i H$ ist von der Form $g_i h = \psi_i(h)$
Also ist $\psi_i$ bijektiv $|H| = |g_i H|$

$$|G| = \sum_{i=1}^{r} |g_i H| = |H| \cdot r \text{ und } r = [G : H]$$

**Definition:** Ist $g \in G, (G_i)$ Gruppe, so sei

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

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

**Beispiele:**

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

b) $(\mathbb{Z}_{12}^*, \cdot)$

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}, j = [j]_{12}$$
$$5^2 = 1 \text{ in } \mathbb{Z}_{12}, | < 5 > | = 2$$
$$7^2 = 1, | < 7 > | = 2$$
$$11^2 = 1, | < 11 > | = 2$$
$$| < 1 > | = 1$$

$(\mathbb{Z}_{12}^*, \cdot)$ ist nicht zyklisch.

c) $(\mathbb{Z}_7^*, \cdot)$

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

| $g$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $g^2$ | 1 | 4 | 2 | 2 | 4 | 1 |
| $g^3$ | 1 | 1 | 6 | 1 | 6 | 6 |
| $g^4$ | 1 | 2 | 4 | 4 | 2 | 1 |
| $g^5$ | 1 | 4 | 5 | 2 | 3 | 6 |
| $g^6$ | 1 | 1 | 1 | 1 | 1 | 1 |

$$ord(2) = 3, ord(3) = 6, ord(6) = 2 \text{ in } \mathbb{Z}_7^*$$

$$< 3 >= G$$

**Satz 2:** Ist $(G, \cdot)$ eine zyklische Gruppe und $|G| = m, G =< g >$, so ist

$$m = ord(g) = Min\{j \in \mathbb{N} | g^j = 1\}$$

und

$$g^j = 1 \Leftrightarrow \ ord(g)|j$$

und

$$ord(g^j) = \frac{m}{d} \text{ mit } 1 \leq d \in ggT(j, m)$$

$G$ hat zu jedem Teiler $t$ von $m$ genau eine Untergruppe $U$ mit $|U| = t$ und zwar

$$U = g^{\frac{m}{t}}, < g^j >= G \Leftrightarrow \ 1 \in ggT(j, m), m = \sum_{d|m} \varphi(d)$$

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

**Beweis:** Da $|G| = m < \infty$ gibt es $i < j$ mit

$$g^i = g^j; i, j \in \mathbb{N}$$

dann folgt

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

Sei $n = Min\{k \in \mathbb{N} | g^k = 1\}$ Dann ist $|\{1, g, \ldots, g^{n-1}\}| = n$
Ist $j \in \mathbb{Z}$, so gibt es $q, r \in \mathbb{Z}$ mit

$$j = qn + r \text{ und } r \in \{0, \ldots, n-1\}$$

Es folgt

$$g^j = \underbrace{(g^n)^q}_{=1} \cdot g^r = g^r \in \{1, g, \ldots, g^{n-1}\}$$

Also

$$G = \{1, g, \ldots, g^{n-1}\}, n = m$$

und

$$g^j = 1 \Leftrightarrow \ r = 0 \Leftrightarrow \ j = qn \Leftrightarrow \ n|j$$

$$(g^i)^j = g^{ij} = 1 \Leftrightarrow \ m|ij \Leftrightarrow \ \frac{m}{d}|j \text{ für } d \in ggT(i, m)$$

Also $ord(g^i) = \frac{m}{d}$
Sei $U \leq G, |U| = t$ , nach Lagrange gilt: $t|m$
Sei $d = Min\{j \in \mathbb{N} | g^j \in U\}$

**Behauptung:** $< g^d >= U$
$\subseteq$ : trivial

$\supseteq$ : Sei $g^J \in U$ beliebig
Es gibt dazu $q, r \in \mathbb{Z}$ mit

$$j = qd + r \text{ und } r \in \{0, \ldots, d-1\}$$

$$g^j \in U, (g^d)^q = g^{dq} \in U$$

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

**Beweis:**

$$< g > \leq |G| = n$$

$$ord(g) = | < g > | | |G| = n = ord(g) \cdot q$$

$$1 = g^{ord(g)}, \text{ also } 1 = 1^q = g^{ord(g) \cdot q} = g^n$$

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

$$a^{\varphi(n)} \equiv 1 \bmod n$$

**Beweis:** $[a]_n \in \mathbb{Z}_n^*$ nach Voraussetzung

$$1 = [a]_n^{|\mathbb{Z}_n^*|} = [a_n]_n^{\varphi(n)} = [a^{\varphi(n)}]_n$$

d.h. $n | a^{\varphi(n)} - 1$

**Beispiel:** Was sind die letzten 3 Ziffern von $b = 7^{123785648801}$?
Antwort: 007

**Beweis:** $b \equiv 7 \bmod 1000$

$$ggT(7, 1000) = 1 \Rightarrow 7^{\varphi(1000)} \equiv 1 \bmod 1000$$

$$\varphi(1000) = \varphi(10^3) = \varphi(2^3 \cdot 5^3) = (2-1) \cdot 2^2 \cdot (5-1) \cdot 5^2 = 400$$

$$\Rightarrow 7^{400} \equiv 1 \bmod 1000$$

$$123785648801 = q \cdot 400 + 1$$

$$b \equiv 7 \bmod 1000$$

**Kleiner Satz von Fermat:**(nicht: "Satz vom kleinen Fermat")
Ist $p$ Primzahl und $a \in \mathbb{Z}$ beliebig, so ist

$$a^p = a \bmod p$$

**Beweis:** Falls $p | a$ , dann auch $p | a^p$ und $p | a^p - a$
sonst $p \not| a$ und $1 \in ggT(p, a)$

$$\text{nach Euler } a^{\varphi(p)} \equiv 1 \bmod p$$

$$\varphi(p) = p - 1 \Rightarrow a^{p-1} \equiv 1 \bmod p \Leftrightarrow a^p \equiv a \bmod p$$

(22.06.01)

**Satz** von Lagrange:

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

**Satz 2:** Ist $G =< g >, |G| = m$, so ist

$$ord\ g = | < g > | = Min\{j | g^j = 1\}$$

$$ord\ g^i = \frac{m}{d}, d \in ggT\{m, i\}$$

$$|\{g^i | ord\ g^i = d\}| = \varphi(d) \text{ für } d|m$$

**Folgerung:** $g \in G, G$ beliebig, $|G| = m < \infty$

$$\Rightarrow g^{|G|} = 1$$

**Satz von Euler:**

$$G = \mathbb{Z}_m^* \Rightarrow a^{\varphi(m)} = 1, \forall a \in \mathbb{Z}_m^*$$

**Kl. Satz von Fermat:** Spezialfall $m = p$ Primzahl

(Ende Wiederholung)

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

**Beweis:** Wäre $p$ Primzahl, so wäre $\varphi(p) = p - 1$ und $1 \in ggT(a, p)$ und nach Euler oder Fermat

$$a^{p-1} = 1 \bmod p$$

**Beispiel:**

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

| | | | | | | Faktoren bekannt | |
|---|---|---|---|---|---|---|---|
| $i$ | 0 | 1 | 2 | 3 | 4 | $\overbrace{5 \ldots 11}$ | $\ldots 23$ |
| $f_i$ | 3 | 5 | 17 | 257 | 65537 | keine Primzahl | |

Wende Folgerung an mit $a = 3$

$$[a^{f_i - 1}]_{f_5} = [a^{(2^{32})}]_{f_5}$$

mit 32 Multiplikationen und $< 32$ Divisionen mit Rest

$$= [302906160]_{f_5} \neq [1]_{f_5}$$

$\Rightarrow f_5$ keine Primzahl

**Beispiel** zu Satz 2: $G =< g >, |G| = 12$
dann ist

$$\left.\begin{array}{lll} d = ord\ g^i & = 12 \text{ für } i = 1, 5, 7, 11 & , \varphi(d) = 4 \\ ord\ g^i & = 6 \text{ für } i = 2, 10 & , \varphi(d) = 2 \\ ord\ g^i & = 4 \text{ für } i = 3, 9 & , \varphi(d) = 2 \\ ord\ g^i & = 3 \text{ für } i = 4, 8 & , \varphi(d) = 2 \\ ord\ g^i & = 2 \text{ für } i = 6 & , \varphi(d) = 1 \\ ord\ g^i & = 1 \text{ für } i = 12 & , \varphi(d) = 1 \end{array}\right\} \sum = 12$$

**Satz 5:** Äquivalent sind für eine endliche Gruppe $G$ mit $|G| = m$

a) $G$ ist zyklisch

b) für $1 \leq d|m$ ist $|\{g \in G | g^d = 1\}| = d$

c) für $1 \leq d|m$ ist $|\{g \in G | ord\ g = d\}| = \varphi(d)$

**Beweis:** a) $\Rightarrow$ b)
Sei $1 \leq d|m$

$$|\{g \in G | g^d = 1\}| = |\{g \in G | ord\ g | d\}| \overset{\text{Satz 2}}{=} \varphi(d) = \sum_{c|d} \varphi(c) = d$$

b) $\Rightarrow$ c) jetzt $|G| = m, G$ beliebig, $1 \leq d|m$

$$f(d) = |\{g \in G | ord g = d\}|$$

$$d \overset{\text{Vor.}}{=} |\{g \in G | g^d = 1\}| = \sum_{c|d} f(c)$$

Möbiusinversion

$$f(d) = \sum_{c|d} \mu(c) \frac{d}{c} = \varphi(c)$$

c) $\Rightarrow$ a) $\varphi(m) \geq 1$, also gibt es nach Vor. c) ein Element $g$ mit $< g >= G$

**Beispiel:** (Pseudozufallszahlen, Fortsetzung von 2.3)

$$z_0 = 0, z_n = a z_{n-1} + c \text{ in } \mathbb{Z}_m$$

$a$ und $c$ sind so zu bestimmen, daß

$$\mathbb{Z}_m = \{[z_n]_m | 0 < n < m - 1\} \tag{2.4}$$

Wende Chin. Restsatz an

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_r^{k_r}}$$

falls

$$m = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}, p_i \neq p_j \text{ für } i \neq j, p_i \text{ Primzahl}$$

(2.4) gilt genau dann, wenn

$$\mathbb{Z}_{p_i^{k_i}} = \{[z_n]_{p_i^{k_i}} | 0 < n < p_i^{k_i} - 1\} \text{ für } i = 1, 2, \ldots, r$$

OBdA: $m = p^k$ für eine Primzahl $p$
In 2.3 war Rekursion aufgelöst

$$z_n = c(1 + a + \ldots + a^{n-1}) \text{ in } \mathbb{Z}_n$$

$$(2.4) \Leftrightarrow c \in \mathbb{Z}_n^* \text{ und } \mathbb{Z}_m = \{(1 + a + \ldots + a^{n-1}) | 0 < n < m - 1\}$$

Insbesondere folgt

$$0 = (1 + a + \ldots + a^{m-1})$$

$$0 = (1 + a + \ldots + a^{m-1})(a - 1) = a^m - 1$$

Also $a^m = 1$, also $a \in \mathbb{Z}_m^*$, also $ord\ a | m$ und nach Lagrange:

$$ord\ a |\ |\mathbb{Z}_m^*| = \varphi(m) \cdot p^{k-1} \cdot (p - 1)$$

also $ord\ a | p^{k-1}$

Fall: $p \neq 2$
Zeige: $\mathbb{Z}_{p^k}^*$ ist zyklisch.

$$ord\ [p+1]_m = p^{k-1}$$

also

$$[a]_m = [p+1]_m^j$$

also

$$p | a - 1$$

**Folgerung:** Damit (2.4) gilt, müssen $a$ und $c$ die folgenden Bedingungen erfüllen

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

b) Ist $2 \neq p | m$, so muß $p | a - 1$

c) Ist $2 | m$, so muß $4 | a - 1$

Umgekehrt folgt aus a) bis c): $a$ und $c$ erfüllen (2.4)
(siehe auch: Knuth, The art of computer programming II, Kap. I)

Es sei $(C, \cdot, ^{-1}, 1)$ beliebige Gruppe und $\sim$ sei eine Kongruenzrelation, d.h. $\sim$ ist Äquivalenzrelation und

$$a \sim b \Rightarrow a^{-1} \sim b^{-1}$$

$$a \sim b, c \sim d \Rightarrow a \cdot c \sim b \cdot d$$

für alle $a, b, c, d \in G$
Setze

$$H := [1]_\sim = \{h \in G | h \sim 1\}$$

weil $\sim$ reflexiv, ist $1 \in G$.
Ist $h \in H$, also $h \sim 1$, so folgt $h^{-1} \sim 1^{-1} = 1$, also $h^{-1} \in H$
Sind $h, h' \in H$, also $h \sim 1$ und $h' \sim 1$, so folgt $h \cdot h' \sim 1 \cdot 1 = 1$, d.h. $h \cdot h' \in H$
Also ist $H \leq G$ "Untergruppe" Sei $h \in H, g \in G$, also $h \sim 1, g \sim g$
dann folgt

$$h \cdot g \sim 1 \cdot g = g$$

$$g^{-1} \sim g^{-1}$$

und hieraus

$$g^{-1} \cdot (h \cdot g) \sim g^{-1} \cdot g = 1$$

also

$$g^{-1} \cdot h \cdot g \in H$$

**Definition:** Eine Untergruppe $H$ von $G$ heißt Normalteiler, (in Zeichen "$H \trianglelefteq G$"), wenn für alle $g \in G, h \in H$ gilt

$$g^{-1} \cdot h \cdot g \in H$$

oder

$$g^{-1} \cdot H \cdot g = H$$

oder

$$H \cdot g = g \cdot H$$

Dabei ist: $g \cdot H$ Linksnebenklasse, $H \cdot g$ Rechtsnebenklasse

**Satz 6:** Ist $\sim$ eine Kongruenzrelation auf $G$, so ist

$$[1]_\sim = H \trianglelefteq G$$

Umgekehrt ist $H \trianglelefteq G$, so wird durch

$$a \sim b \overset{\text{Def.}}{\Leftrightarrow} a^{-1} \cdot b \in H$$

eine Kongruenzrelation definiert.

**Beispiel:** $G = S_3$ sym. Gruppe

$$G = \{1, (12), (23), (13), (123), (132)\}$$

$$|G| = 6 = 2 \cdot 3$$

(Hier bekam Hr. Pahlings einen LISP-Anfall und klammerte alles, was sich mit 3 Zahlen schreiben lässt. Wer das ganze logisch sinnvoll aufschreiben konnte, möge sich bei mir melden. Danke.)

$$H nicht \trianglelefteq G$$

$$H \cdot < (123) >= 1 \cdot H = H \cdot 1$$

$$(12)H = G \backslash H = H(12)$$

$$< (123) > \trianglelefteq G$$

**Bemerkung:** Ist $G$ abelsch und $H \leq G$, so ist $H \trianglelefteq G$

## 2.9 Euklidische Körper und Codes

**Satz 1:**

a) Ist $K$ euklidischer Körper, so gilt:

$$p = Min\{j \in \mathbb{N} | j \cdot 1 = \underbrace{1 + \ldots + 1}_{j} = 0\}$$

ist eine Primzahl und $|K| = p^n$.
$p$ heißt Charakteristik von K und es gilt

$$p \cdot a = 0 \text{ und } (a+b)^p = a^p + b^p \text{ für alle } a, b, \in K$$

b) Die multiplikative Gruppe $(K^*, \cdot)$ ist zyklisch

**Beweis:**

a) $\psi : \mathbb{Z} \to K : j \mapsto j \cdot 1$ ist Ringhomomorphismus
$Bild\ \psi \simeq \mathbb{Z}/Kern\ \psi$ Homomorphiesatz
$Kern\ \psi \trianglelefteq \mathbb{Z}$, also existiert $p \in \mathbb{N}$ mit $Kern\ \psi = p\mathbb{Z}$

$$p = Min\{j \in \mathbb{N} | j \cdot 1 = 0\}$$

Wäre $p$ keine Primzahl, so hätte $Bild\ \psi \simeq \mathbb{Z}/p\mathbb{Z}$ Nullteiler. Widerspruch!

$$K \geq K_p = Bild\ \psi \simeq \mathbb{Z}_p$$

Körper $K$ kann man also als $K_p$-Vektorraum auffassen , $dim_{K_p} K = n$
so hat $K$ $p^n$ Elemente, d.h. $|K| = p^n$

$$a \in K, p \cdot a = p \cdot 1 \cdot a = 0 \cdot a = 0$$

$$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j b^{p-j}$$

für $j = 1, 2, \cdot, p-1$ ist

$$p|\binom{p}{j} = \frac{p(p-1) \cdot \ldots \cdot (p-j+1)}{1 \cdot 2 \cdot \ldots \cdot j}$$

da $pa^j b^{p-j} = 0$ in $K$, ist $\binom{p}{j} a^j b^{p-j} = 0$ für $j = 1, 2, \ldots, p-1$
also $(a+b)^p = a^p + b^p$

b) $|K| = p^n$, dann ist $|K^*| = p^n - 1$
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 $m \mid |K^*| = p^n - 1 = m \cdot q$ mit $q \in \mathbb{N}$, so ist

$$x^{p^n-1} - 1 = (x^m - 1)(1 + x^m + \cdot + x^{(q-1)m})$$

Also hat $x^m - 1$ in $K^*$ genau $m$ Nullstellen

$$|\{\alpha \in K^* | \alpha^m = 1\}| = m$$

Nach Kap. 2.8, Satz 3 folgt $K^*$ ist zyklisch.

**Bemerkung:** Ist $f \in \mathbb{Z}_p[x]$ irreduzibel in $Grad\ f = n$, 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

$$Irr_n(\mathbb{Z}_p) = \{f \in \mathbb{Z}_p[x] | f \text{ irred.}, Grad\ f = n, f \text{ normiert}\}$$

so ist für jedes $n \in \mathbb{N}$

$$x^{p^n} - x = \prod_{d|n} \prod_{f \in Irr_d(\mathbb{Z}_p)} f \in \mathbb{Z}_p[x] \tag{2.5}$$

$$N_n(p) = |Irr_n(\mathbb{Z}_p)| = \frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}$$

**Folgerung:** Zu jeder Primzahlpotenz $p^n$ gibt es einen Körper $K$ mit $|K| = p^n$

**Beispiel:** p = 2 , n = 3

$$x^{2^3} - x = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

**Beweis zu Satz 2:**

a) **Behauptung:** Ist $f$ irreduzibel $\in \mathbb{Z}_p[x]$ und $Grad\ f = d|n$, so ist $f|x^{p^n} - x$
**Beweis:** $K = \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$ ist Körper und $|K| = p^d$

$$\alpha^{p^d-1} = 1, \alpha^{p^d} = \alpha \text{ für alle } \alpha \in K*$$

Speziell für $\alpha = [x]_f$ erhält man

$$[x^{p^d}]_f = [x]_f \text{ also } f|x^{p^d} - x$$

(wie in Satz 1) wenn $d|n$, so ist

$$x^{p^d} - 1|x^{p^n} - x$$

b) **Behauptung:** Ist $f \in \mathbb{Z}_p[x]$ irred. und $f|x^{p^n} - x$, so ist

$$d = Grad\ f|n$$

**Beweis:** $n = qd + r$ mit $0 \leq r < d, q \in \mathbb{Z}$
**Behauptung:** $r = 0, K = K[x]/fK[x], |K| = p^d$

$$[x]_f^{p^d} = [x]_f \text{ wie in a)}$$

Außerdem:

$$[x]_f^{p^n} = [x]_f$$

weil nach Voraussetzung $f|x^{p^n} - x$
daher

$$[x]_f^{p^n} = [x]_f \text{ wobei } n = dq + r$$

$$K \ni \left[\sum_{i=0}^{d-1} a_i x^i\right]_f^{p^r} = \left(\sum_{i=0}^{d-1} [a_i x^i]_f\right)^{p^r}$$

nach Satz 1 a)

$$= \sum_{i=0}^{d-1} [a_i^{p^r} x^{i p^r}]_f = \left[\sum_{i=0}^{d-1} a_i (x^{p^r})^i\right]_f = \underbrace{\left[\sum_{i=0}^{d-1} a_i x^i\right]_f}_{\alpha}$$

jedes $\alpha \in K$ erfüllt $\alpha^{p^r} = \alpha$, ist also Nullstelle von $x^{p^r} - x$, hat aber höchstens $Grad\ (x^{p^r} - x)$ Nullstellen. Also $r = 0$
**Behauptung:** Es gibt kein irreduzibles Polynom $f \in \mathbb{Z}_p[x]$ mit

$$f^2|x^{p^n} - x$$

**Beweis:** Angenommen

$$x^{p^n} - x = f^2 \cdot g = f \cdot (f \cdot g)$$

Wende formale Ableitung an

$$D(x^{p^n} - x) = p^n x^{p^n-1} - 1 = -1 \text{ in } \mathbb{Z}_p[x]$$

$$D(f \cdot (fg)) = f \cdot D(fg) + D(f) \cdot fg = f(D(fg) + D(f) \cdot g)$$

Also $f| - 1$ , $f$ Einheit in $\mathbb{Z}_p[x]$ nicht irred.

c) Damit ist 2.5 bewiesen, berechne *Grad*

$$Grad\ (x^{p^n} - x) = p^n = \sum_{d|n} \sum_{f \in Irr_d(\mathbb{Z}_p)} Grad\ f = \sum_{d|n} N_d(p)d$$

$$p^n = \sum_{d|n} dN_n(p)$$

und Kap. 2.7 Möbiusinversion

$$nN_n(p) = \sum_{d|n} \mu(d) p^{\frac{n}{d}}$$

Beweis der Folgerung:

$$N_n(p) = \frac{1}{n}\left[1p^n + \sum_{1 \neq d|n} \mu(d)p^{\frac{n}{d}}\right], \mu(d) \in \{0, 1, -1\}$$

$$\geq \frac{1}{n}\left[p^n - \sum_{1 \neq d|n} p^{\frac{n}{d}}\right] \geq \frac{1}{n}[p^n - (p + p^2 + \ldots + p^{n-1})] > 0$$

**Satz 3:** Je zwei Körper mit $p^n$ Elementen sind isomorph. Bezeichnung für einen Körper mit $p^n$-Elementen ist $GF(p^n)$ ("Galois-Feld")

**Beweis:** Ist $f \in Irr_n(\mathbb{Z}_p)$ und $K$ ein beliebiger Körper mit $|K| = p$
**Behauptung:**

$$K \simeq \mathbb{Z}_p[x]/f\mathbb{Z}_p[x]$$

**Beweis:** Nach Satz 2 enthält $K$ eine Nullstelle von $f$

$$\psi : \mathbb{Z}_p[x]/f\mathbb{Z}_p[x] \to K : \left[\sum_{i=0}^{n-1} a_i x^i\right]_f \mapsto \sum_{i=0}^{n-1} a_i \alpha^i, a_i \in \mathbb{Z}_p$$

ist Isomorphismus.

Anwendungen von endl. Körpern, z.B. Kodierungstheorie
**Problem:** Nachricht $\overset{Kodierung}{\to}$ Codeworte $\overset{Senden}{\to}$ Codeworte + Fehler $\overset{Dekodierung}{\to}$
**Aufgabe:** Bestimme Code so, daß $k$ Fehler korrigiert oder erkannt werden
linearer $(n, k)$-Code = Teilraum C von $\mathbb{Z}_2^n$ der Dimension $k$

$$v, w \in \mathbb{Z}_2^n \Rightarrow d(x, y) = |\{i \in \{1, \ldots, n\} | v_i \neq w_i\}| \text{"Hamming-Abstand"}$$

$$d = Min\{d(v, w) | v, w \in C\} = \text{ Minimaldistanz von } C$$

Ist $d = 2e+1$ , so kann $C$ bis zu $e$ Fehler korrigieren und bis zu $2e$ Fehler entdecken.

(04.07.01)

$K$ 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 $dim\ C = k$

$$d(v, w) = |\{i | v_i \neq w_i\}| = d(v - w, 0)$$

$C$ wird durch Generatormatrix $G(C)$ angegeben, $G(C) \in K^{k \times n}$ mit Zeilen = Basisvektoren von C
Kontrollmatrix $H = H(C) \in K^{n-k,n}$

$$C = \{c \in K^n | H \cdot c^{tr} = 0\}$$

(In LA I wurde die Transponierte mit $^{tr}$ bezeichnet, dies übernehme ich, da die meisten Leser wohl auch LA I gehört haben. Das Zeichen $^T$ wurde damals im Bereich der Orthogonalräume verwendet. Anm. des Autors)
Ist $c' \in K^n$ gegeben, dann ist $c'$ genau dann ein Codewort, wenn $Hc'^{tr} = 0$ , $Hc'^{tr}$ heißt Syndrom
$C$ zyklischer Code $\Leftrightarrow$ $C$ linearer $(n,k)$-Code mit

$$c = (c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow V(c) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$$

$$\psi : K^n \rightarrow K[x]/(x^n-1)K[x] = K[x]/(x^n-1) : (c_0, \ldots, c_{n-1}) \mapsto \left[\sum_{i=0}^{n-1} c_i x^i\right]_{(x^n-1)}$$

$$\psi(v(c)) = [x]_{(x^n-1)} \cdot \psi(c)$$

**Bemerkung:** $C \leq K^n$ linearer Code ist zyklisch $\Leftrightarrow$ $\psi(c) \trianglelefteq K[x]/(x^n-1)$ (Ideal)
Was sind die Ideale in $K[x]/(x^n-1)$?
Angenommen $I \trianglelefteq K[x]/(x^n-1)$

$$J = \{f \in K[x] | [f]_{x^n-1} \in I\} \trianglelefteq K[x]$$

$$= gK[x] \text{ für ein } g \in K[x]$$

$$x^n - 1 \in J \text{ , also } g | x^n - 1$$

**Lemma 1:** Ist $C$ ein zyklischer $(n,k)$-Code ($C \neq \{0\}$), so gibt es ein normiertes $g \in K[x]$ mit $g|x^n-1$ "Generatorpolynom" von $C$ mit

$$\psi(c) = \{[f \cdot g]_{x^n-1} | f \in K[x]\} \leq K[x]/(x^n-1)$$

Es ist $Grad\ g = n - k$
Es gibt genau soviele zyklische Codes der Länge $n$ wie $x^n - 1$ in $K[x]$ an Teilern hat.

**Beispiel:** $K = \mathbb{Z}_2, n = 7 = 2^3 - 1$

$$x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$$

Wähle $g = x^3 + x + 1$

$$G(C) = \begin{bmatrix} 1101000 \\ 0110100 \\ 0011010 \\ 0001101 \end{bmatrix} \begin{matrix} \rightarrow [g]_{x^7-1} \\ \rightarrow [xg]_{x^7-1} \\ \rightarrow [x^2g]_{x^7-1} \\ \rightarrow [x^3g]_{x^7-1} \end{matrix}$$

Beachte: $1000110 \rightarrow [x^4g]_{x^7-1} = [g] + [xg] + [x^2g]$

$$dim\ C = 4 = 7 - Grad\ g$$

**Beweis:**(des Lemmas)

$$x^n - 1 = gh \text{ mit } h = \sum_{i=0}^{k} h_i x^i, h_k = 1$$

$$Grad\ g + k = n$$

$$[g], [xg], \ldots, [x^{k-1}g] \text{ in } K[x]/x^n - 1 \text{ lin. unabh.}$$

$$0 = [x^n - 1] = [gh] = [x^k g + \sum_{i=0}^{k-1} h_i x^i g] = [x^k g]$$

$$= -\sum_{i=0}^{k-1} h_i [x^i g] \in < [g], [xg], \ldots, [x^{k-1} g] >$$

$$dim\ C = k$$

**Beispiel:**

$$x^7 - 1 = g \cdot h, h = (x+1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$$

$$[x^4 g] = [g] + [xg] + [x^2 g]$$

$C$ hat Minimaldistanz 3
Nachricht sei $w = 1001 = 1 + x^3$
Codierung: $C = w \cdot g = (1 + x^3)(1 + x + x^3) = x^6 + x^4 + x + 1 = 1100101$
Senden $\rightarrow$ Empfangen: $c' = 1101101 = x^6 + x^4 + x^3 + x + 1$
Fehlerkorrektur/erkennung: Teile mit Rest durch $g$. Äquivalent: Setze in $c'$ das Element $\alpha = [x]_g \in K[x]/(g)$ ein.

$$c'(\alpha) = 1 + [x]_g + [x^3]_g + [x^4]_g + [x^6]_g = [x^6 + x^4 + x^3 + x + 1]_g$$

$$= x^3(x^3 + x + 1) + x + 1 = [x+1]_g = \alpha^j, j = \lg_\alpha [x+1] = 3$$

Fehler an Position 3
$c' = c + e$ , Fehlerpolynom $e = x^i$
$c'(\alpha) = \underbrace{c(\alpha)}_{=0} + \alpha^j$ , falls nur ein Fehler gemacht wurde
Korrektur: $c'' = c' + x^3 \leftrightarrow$ 1100101 = $c$ $w'$: teile $c$ durch $g$ , $c = g(1+x^4)$ , $w = 1001$

**Bemerkung:** Ist $L = GF(p^n)$, so gilt für jedes $\beta \in L$, $(K[x]/(f), f$ irred. $\in K[x]$ vom $Grad\ n)$

$$\beta^{p^n} = \beta \text{ , d.h. } x^{p^n} - x = \prod_{\beta \in L} (x - \beta) \in L[x]$$

$$= \prod_{d|n} \prod_{f \in Irr_d(K)} f, Irr_d(K) = \{f \in K[x], Grad\ f = d, f \text{ irred.}, f \text{ normiert}\}$$

Also: Zu jedem $\beta$ ex. genau ein normiertes, irred. Polynom (vom $Grad\ d|n$) mit $f(\beta) = 0$
Dieses (eindeutig bestimmte) Polynom heißt Minimalpolynom von $\beta$, in Zeichen: $f_\beta \in K[x]$

$$L^* = L \backslash \{0\} = < \alpha > \text{ für ein } \alpha \in L$$

**Satz 1:** Ist $n = p^r - 1$ ,($p$ Primzahl, $p = 2$), $t < n - 1, t \in \mathbb{N}$
$L = GF(p^n)$ und $L^* = < \alpha >$

$$g = kgV\{f_{\alpha^i} | 1 \leq i \leq t\} \in K[x]$$

dann ist $g | x^n - 1$ und ist $C$ der zyklische Code mit Generatorpolynom $g$ hat Minimaldistanz $\geq t + 1$

**Beispiel:** (s.o.)

$$n = 7 = 2^3 - 1, g = x^3 + x + 1 = f_\alpha = f_{\alpha^2}$$

$$\alpha = [x]_g \in K[x]/(g) = L, < \alpha > = L^*$$

Setze $t = 2$

$$g = kgV\{f_\alpha, f_{\alpha^2}\}$$

Also Minimaldistanz von $C$ ist nach Satz $1 \geq t + 1 = 3$

**Beweis:**

$$g = \sum_{i=0}^{m} g_i x^i = kgV\{f_\alpha, \ldots, f_{\alpha^t}\}$$

$$\psi(C) = \{[f]_{x^n-1} |\ g|f \Leftrightarrow\ f(\alpha) = f(\alpha^2) = \ldots = f(\alpha^t) = 0\}$$

Also

$$C = (c_0, \ldots, c_{n-1}) = \sum_{i=0}^{n-1} c_i x^i \in C \Leftrightarrow c(\alpha) = c(\alpha^2) = \ldots + c(\alpha^t) = 0$$

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \ldots & (\alpha^2)^{n-1} \\ \vdots & & & & \vdots \\ 1 & \alpha^t & \alpha^{2t} & \ldots & \alpha^{(n-1)t} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} c(\alpha) \\ c(\alpha) \\ \vdots \\ c(\alpha^t) \end{bmatrix} = 0$$

Angenommen $Jc \in C$ mit $\alpha(c, 0) \leq t, c_i = 0$ außer für $i \notin \{j_1, \ldots, j_t\}, 0 \leq j_1 < \ldots < j_t \leq n - 1$

$$\underbrace{\begin{bmatrix} \alpha^{j_1} & \alpha^{j_2} & \ldots & \alpha^{j_t} \\ \alpha^{2j_1} & \alpha^{2j_2} & \ldots & \alpha^{2j_t} \\ \vdots & & & \vdots \\ \alpha^{tj_1} & \alpha^{tj_2} & \ldots & \alpha^{tj_t} \end{bmatrix}}_{M} \begin{bmatrix} c_{j_1} \\ \vdots \\ c_{j_t} \end{bmatrix} = 0$$

$$det\ M = \alpha^{j_1} \cdot \alpha^{j_2} \ldots \alpha^{j_t} det \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \ldots & \alpha^{j_t} \\ \vdots & & & \vdots \\ \alpha^{j_1(t-1)} & & \ldots & \alpha^{j_t(t-1)} \end{bmatrix} = \alpha^{j_1} \ldots \alpha^{j_t} \prod_{j_i < j_k} (\alpha^{j_i} - \alpha^{j_k} \neq 0$$

$\Rightarrow c = 0$

(06.07.01)

**Definition:** Ein Reed-Solomon Code der Länge $n = 2^r - 1$ über $K \leq GF(2^r)$ mit Plandistanz (designed distance) $t$ ist ein Code

$$C = \{c = [c_0, \ldots, c_{n-1} | c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^t) = 0\}$$

wobei $< \alpha >= (GF(2^r))^*$

**Bemerkung:** $C$ ist ein zyklischer Code mit Generatorpolynom $g = kgV(f_{\alpha^i} | 1 \leq i \leq t)$
$f_{\alpha^i} \in K[x]$ Minimalpolynom von $\alpha^i$
$C$ hat Minimaldistanz $\geq t + 1$
Ist $t = 2t'$, so kann $C$ $t'$ Fehler korrigieren oder $2t'$ Fehler erkennen.

**Beispiel:** $K = \mathbb{Z}_2, n = 15 = 2^4 - 1$

$$x^{15} - 1 = (x+1)(x^2+x+1)\underbrace{(x^4+x+1)}_{f}(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

$$GF(2^4) = K[x]/(x^4 + x + 1), \alpha = [x]_f$$

$$f_\alpha = x^4 + x + 1 = f_{\alpha^2} = f_{\alpha^4}, ord\ \alpha = 15$$

$$f_{\alpha^3} = x^4 + x^3 + x^2 + x + 1, ord\ \alpha^3 = 5$$

$$\alpha^3 \text{ Nullstelle von } x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$$

$g_1 = f_\alpha \cdot f_{\alpha^3} = x^8 + \ldots$ ist Generatorpolynom eines zyklischen Codes $C_1, (15, 7)$-Code

$$dim\ C_1 = 7, |C_1| = 2^7$$

$$C = \{c = [c_0, \ldots, c_{n-1}] | c(\alpha) = c(\alpha^2) = c(\alpha^3) = c(\alpha^4)\}$$

Minimaldistanz $\geq 5$ , also 2 Fehler korrigierend

$$ord\ \alpha^5 = 3 \text{ , also ist } \alpha^5 \text{ Nullstelle von } x^3 + 1 = (x+1)(x^2 + x + 1)$$

$$f_{\alpha^5} = x^2 + x + 1$$

$$f_{\alpha^6} = f_{\alpha^3}$$

Setzt man $g_2 = f_\alpha \cdot f_{\alpha^3} \cdot f_{\alpha^5} = x^{10} + \ldots$ , so ist $g_2$ Generatorpolynom eines Codes $C_2, (15, 5)$-Code

$$dim\ C_2 = 5 \text{ , Minimaldistanz } \geq 7$$

Bei CD's werden Reed-Solomon Codes verwendet mit $n = 2^8 - 1$ und Plandistanz 5

Um Fehlerbündel zu korrigieren, speichere Information in $N \times n$-Matrizen und transponiere (oder sende spaltenweise)

# Kapitel 3

# Graphen

## 3.1 Grundbegriffe

**Definition 1:** Ein Graph $G = (V, E)$ ist eine endliche, nichtleere Menge $V$ (von "Knoten" oder "Vertices") mit $E \subseteq \binom{V}{2} = \{M \subseteq V | \, |M| = 2\}$ Die Elemente von $E$ heißen Kanten ("edges")

**Beispiele:**

a) $V_n = (V = \{1, \ldots, n\}, \binom{V}{2})$ vollständiger Graph mit $n$ Kanten

b) $V = \{1, 2, 3, 4\}, E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 1\}, \{2, 4\}\}$
Beschreibung eines Vierecks mit zusätzlicher Diagonale zwischen 2 und 4

**Definition:** Ist $G = (V, E)$ ein nummerierter Graph

$$V = \{v_1, \ldots, v_n\}, E = \{e_1, \ldots, e_m\}$$

so heißt die 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, 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

**Beispiel:** (Fortsetzung von b)

$$A = \begin{bmatrix} 0101 \\ 1011 \\ 0101 \\ 1110 \end{bmatrix}$$

**Allgemein:** $A$ ist immer symmetrisch und die Hauptdiagonale besteht aus Nullen.

$$B = \begin{bmatrix} 10010 \\ 11001 \\ 01100 \\ 00111 \end{bmatrix}$$

$$B \cdot B^{tr} = \begin{bmatrix} 2101 \\ 1311 \\ 0121 \\ 1113 \end{bmatrix} = A + diag(2,3,2,3)$$

**Definition:** Ist $G = (V, E)$ Graph und $v \in V$, so sei

$$d(v) = deg(v) = |\{e \mid v \in e\}| \text{ Grad des Knoten } v$$

Im Beispiel b) ist $d(1) = 2, d(2) = 3, d(3) = 2, d(4) = 3$

**Bemerkung:** Ist $A$ Adjazenzmatrik und $B$ Inzidenzmatrix eines nummerierten Graphen, so ist

$$B \cdot B^{tr} = A + diag(d(v_1), \ldots, d(v_n))$$

**Beweis:** Für $i \neq j$:

$$(BB^{tr})_{ij} = \left( \sum_{k=1}^{m} \underbrace{b_{ik} b_{jk}}_{\neq 0 \text{ nur für } e_k = \{v_i, v_j\}} \right)_{ij} = A_{ij}$$

Für $i = j$:

$$(BB^{tr})_{ij} = \sum_{k=1}^{m} b_{ik} b_{ik} = \sum_{k=1}^{m} \underbrace{b_{ik}}_{=1 \Leftrightarrow\ v_i \in e_k}$$

**Variationen:**

- Multigraphen ("Mehrfachkanten"): $A_{ij}$ kann größer als 1 werden
- Graphen mit Schleifen: $A_{ii}$ kann $\neq 0$ sein
- Gerichtete Graphen: $(V, E)$, wobei

$$E \subseteq V \times V = \{ \underbrace{(v_1, v_2)}_{\text{Kante von } v_1 \textbf{ nach } v_2} \mid v_1, v_2 \in V \}$$

  Dann ist $A$ nicht notwendig symmetrisch.

**Lemma 1:**(Handschlag-Lemma von Euler) Ist $(V, E)$ ein Graph (im Sinne von Definition 1), so gilt

$$\sum_{v \in V} d(v) = 2 \cdot |E|$$

**Beweis:**

$$\sum_{v \in V} d(v) = \sum_{i=1}^{n} \underbrace{\sum_{j=1}^{m} b_{ij}}_{=2} = 2 \cdot m = 2 \cdot |E|$$

$$V = \{v_1, \ldots, v_n\}, E = \{e_1, \ldots, e_m\}, [b_{ij}] = \text{ Inzidenzmatrix}$$

(11.07.01)

$G = (V, E), \emptyset \neq V$ endliche Menge von "Knoten"

$$E \subseteq \binom{V}{2} = \{\{v, v'\} \mid v \neq v', v, v' \in V\}$$

$$d(v) = |\{e \in E \mid v \in e\}|$$

**Handschlag-Lemma** von Euler:

$$\sum_{v \in V} d(V) = 2\ |E|$$

**Definition:** $G = (V, E)$ heißt k-regulär, wenn $d(v) = k$ für alle $v \in V$

**Beispiel:**

a)

$$V_n = K_n = (V, \binom{V}{2})), |V| = n$$

$V_n$ ist $(n-1)$-regulär

b)

$$Q_n = n\text{-dimensionaler Hyperkubus } = (\mathbb{Z}_2^n, E_n)$$

$$E_n = \{\{v, v'\} \mid v \neq v' \in \mathbb{Z}_2^n, \underbrace{d(v, v')}_{Hammingabstand} = 1\}$$

$Q_n$ ist $n$-regulär

$$|\mathbb{Z}_2|^n \cdot n = 2 \cdot |E|, |E| = n \cdot 2^{n-1}$$

**Definition:** Ist $G = (V, E)$ ein Graph, so ist $G' = (V', E')$ ein Teilgraph/Untergraph von $G$, wenn $V' \subseteq V$ und $E' \subseteq E \cap \binom{V'}{2}$
G heißt induzierter Teilgraph, wenn $E' = E \cap \binom{V'}{2}$
$G' = G[V']$

## 3.2 Wege und Kreise

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

**Definition:** Ein Weg ("Kantenzug") von $v$ nach $v'$ in $V$ der Länge l ist eine Folge

$$W = (w_0, w_1, \ldots, w_l) \text{ mit } w_i \in V, w_0 = v, w_l = v'$$

und

$$E(W) = \{\{w_{i-1}, w_i\} \mid 1 \leq i \leq l\} \subseteq E$$

$W$ heißt Pfad von $v$ nach $v'$, wenn

$$w_i \neq w_j \text{ für } i \neq j$$

$W$ heißt Kreis, wenn

$$w_0 = w_l \text{ und } w_i \neq w_j \text{ für } i \neq j, 0 \leq i, j \leq l-1 \text{ und } l \geq 3$$

**Definition:** $G = (V, E)$ heißt zusammenhängend, wenn es zu $v, v' \in V$ stets einen Pfad von $v$ nach $v'$ gibt.

**Bemerkung:**

a) Gibt es einen Weg von $v$ nach $v'$ in $G$, so auch einen Pfad

b) Definiert man auf $V$ eine Relation

$$v \sim v' \Leftrightarrow \text{ Es gibt einen Pfad von } v \text{ nach } v'$$

so ist $\sim$ eine Äquivalenzrelation
Sind $V_1, \ldots, V_s$ die Äquivalenzklassen bezüglich $\sim$, so 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 $G$

**Satz 1:** $G = (V, E)$ enthält mindestens $|V| - |E|$ Komponenten. Ist $G$ zusammenhängend, dann ist $|E| \geq |V| - 1$

**Beweis:** Induktion nach $|E| = m$
$m = 0$ :

$$V = \dot{\bigcup_{V_i \in V}} \{V_i\} \text{ Zerlegung in Komponenten}$$

Es gibt $|V|$ Komponenten
$m > 0$ : Sei $e \in E$ und $E' = E \backslash \{e\}$, also $|E'| = m - 1$
$G' = (V, E')$ hat nach Ind. Ann. $k \geq |V| - m + 1$ Komponenten
$G = (V, E)$ hat dann $k$ oder $k - 1$, also $\geq |V| - m$ Komponenten

Adjazenzmatrix eines nummerierten Graphen

$$V = \{v_1, \ldots, v_n\}$$

$$A = [a_{ij}]_n, i, j \in \{1, \ldots, n\} \text{ mit } a_{ij} = \begin{cases} 1 & \text{für } \{i, j\} \in E \\ 0 & \textit{sonst} \end{cases}$$

**Satz 2:** Ist $G = (V, E)$ nummerierter Graph mit Adjazenzmatrix $A$ und ist

$$A^r = \underbrace{A \cdot A \cdot \ldots \cdot A}_{r} = [a_{ij}^{(r)}], r \in \mathbb{N}_0$$

so ist $a_{ij}^{(r)}$ = Anzahl der Wege von $v_i$ nach $v_j$ mit Länge $r$

**Beweis:** Induktion nach $r$
$r = 0$ :

$$A^0 = \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$$

$r > 0$ :

$$W_{ij}^{(r)} = \{w = (w_0, \ldots, w_r) \mid w = \text{ Weg von } v_i \text{ nach } v_j \text{ der Länge } r\}$$

$$(w_0, \ldots, w_r) \mapsto ((w_0, w_1), (w_1, \ldots, w_r))$$

$$W_{ij}^{(}r) \rightarrow \bigcup_{k=1}^{n} (W_{ik}^{(1)} \times W_{kj}^{(r-1)}), n = |V|$$

$$|W_{ij}^{(r)}| = \sum_{k=1}^{n} \underbrace{|W_{ik}^{(1)}|}_{=a_{ik}} \underbrace{|W_{kj}^{(r-1)}|}_{=a_{kj}^{(r-1)}} = (A \cdot A_{i,j}^{r-1} = (A^r)_{i,j} = a_{i,j}^{(r)}$$

**Definition:** Eine Eulertour in einem Graphen $G = (V, E)$ ist ein "geschlossener" Weg

$$w = (w_o, \ldots, w_m) \text{ mit } w_0 = w_m$$

mit $E(w) = E$ und $m = |E|$, d.h. alle Kanten von $G$ werden genau einmal durchlaufen.
$G$ heißt eulersch, wenn es so eine Eulertour gibt.

**Satz 3:** Ein zusammenhängender Graph ist genau dann eulersch, wenn $d(v)$ gerade ist für alle $v \in V$

**Beweis:** $\Rightarrow$ :
$w = (w_0, \ldots, w_m)$ sei eine Eulertour.

$$\Rightarrow E(w) = \{\{w_0, w_1\}, \{w_1, w_2\}, \ldots, \{w_{m-1}, w_m\}\}$$

Für $v \in V$ setze $n_v = |\{j \in \{0, \ldots, m-1\} \mid w_j = v\}|$, dann $d(v) = 2n_v \in 2\mathbb{N}$
$\Leftarrow$:
Algorithmus zur Konstruktion einer Eulertour: Bilde maximalen (d.h. nicht verlängerbaren) Weg

$$w = (w_0, w_1, \ldots, w_r) \text{ mit } E(w) = r$$

Behauptung: Dann muß $w_0 = w_r$ sein, denn da $d(w_r) \in 2\mathbb{N}$ gäbe es ein $v$ mit

$$\{w_r, v\} \in E \backslash E(w)$$

und man könnte $w$ verlängern zu $(w_0, \ldots, w_r, v\}$
Also ist $w_0 = w_r$
Ist $E(w) = E$, so ist $W$ Eulertour, sonst gibt es $\{v, v'\} \in E \backslash E(w)$ und weil $G$ zusammenhängend ist, gibt es $\{w_i, v\} \in E \backslash E(w)$ für ein $i \in \{0, \ldots, r-1\}$
Bilde maximalen Weg

$$w' = (w_i = w_0', w_1', \ldots, w_s') \text{ in } (V, E \backslash E(w)) \text{ mit } |E(w')| = s$$

wie oben ist $w_0' = w_s'$ Ersetze

$$w \text{ durch } w_1 = (w_0, \ldots, w_i, w_1', \ldots, w_s', w_{i+1}, \ldots, w_r) \text{ und } r \text{ durch } r + s$$

Wiederhole Algorithmus

(13.07.01)

**Beispiel:** Kann man alle Dominosteine in einem Rechteck auslegen?

$$D = \{\{i, j\} \mid 0 \leq i, j \leq 6\}, |D| = 28, V = \{0, 1, 2, 3, 4, 5, 6\}$$

$$G' = (V, D) \text{ Graph mit Schleifen}$$

Gesucht: Eulertour in $G'$ existiert genau dann, wenn Eulertour existiert im Graph ohne Schleifen

$$G' \text{ ohne Schleifen } = K_7 \text{ vollst. Graph mit 7 Knoten (6-regulär)}$$

Nach Satz von Euler existiert Eulertour

**Definition:** Es sei $G = (V, E)$ ein Graph. Ein Hamiltonkreis(-pfad) in $G$ ist ein Kreis (Pfad), der alle Kanten aus $V$ genau einmal durchläuft.
Gibt es einen Hamiltonkreis(-pfad), so heißt $G$ (semi-)hamiltonsch.

**Beispiel:** Der Kubus $Q_3$ ist hamiltonsch.

**Satz 4:** Sei $G = (V, E)$ Graph, $|V|geq3$
Gilt für $v \neq v'$ mit $\{v, v'\} \notin E$ stets

$$d(v) + d(v') \geq |V| - 1$$

so gibt es immer einen Hamiltonpfad.
Gilt sogar

$$d(v) + d(v') \geq |V|$$

gibt es stets einen Hamiltonkreis.

**Beweis:**

a) Aus der Voraussetzung folgt: $G$ ist zusammenhängend.
Sonst: Wähle $v \in V_1, v' \in V_2$, wobei $V_1 \neq V_2$ Komponenten sind, dann

$$d(v) \leq |V_1| - 1, d(v') \leq |V_2| - 1$$
$$\Rightarrow d(v) + d(v') \leq \underbrace{|V_1| + |V_2|}_{\leq |V|} - 2 \leq |V| - 2$$

Widerspruch!

b) Konstruktion eines Hamiltonpfads beginnend mit beliebiger Kante $\{w_1, w_2\} \in E$

$$w = (w_1, w_2, \ldots, w_p) \text{ Pfad der Länge } p - 1 \geq 1$$

Ist $p = n = |V|$, so ist man fertig.
Sonst: $v \notin \{w_1, \ldots, w_p\}$ 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

$$v \notin \{w_1, \ldots, w_p\} \text{ mit } \{v, w_p\} \in E \text{ oder } \{v, w_1\} \in E$$

**Beispiel:**

$$\{w_1, w_{j_1}\}, \ldots, \{w_1, w_{j_k}\}, 2 = j_1 < \ldots < j_k \leq p \Rightarrow d(w_1) = k$$

Wir finden einen Kreis, der $w_1, \ldots, w_p$ enthält
klar, wenn $\{w_1, w_p\} \in E$, sonst $j_k < p$
Ist $\{w_{j_i - 1}, w_p\} \in E$, so erhält man einen Kreis. Eine solche Kante muß existieren, denn sonst wäre

$$d(w_p) \leq p - 1 - k \text{ , also } d(w_1) + d(w_p) \leq p - 1 < |V| - 1$$

Man erhält also einen Kreis mit $p$ Knoten

$$\exists v \notin \{v_1, \ldots, v_p\}, \text{ so } \{v, v_j\} \in E$$

Man erhält einen Pfad mit $p + 1$ Knoten $\Rightarrow$ Es gibt einen Hamiltonpfad
$\Rightarrow$ unter Benutzung $d(v_1) + d(v_n) \geq n = |V|$, so erhält man wie oben einen Hamiltonkreis.

**Beispiel:** 7 Prüfungen, Kein Dozent prüft mehr als 3 Mal, Gibt es eine Lösung, damit kein Dozent 2 Prüfungen hintereinander machen muß?
Graph $V = \{1, \ldots, 7\}, E = \{\{i, j\} \mid Pr_i \neq Pr_j\}, d(i) \geq 3$
Es gibt Hamiltonpfad.

(18.07.01)

## 3.3 Bäume und Wälder

**Definition:** Ein Graph $G = (V, E)$ heißt ein Baum, wenn er zusammenhängend ist und keine Kreise enthält.
Ein Graph, dessen sämtliche Komponenten Bäume sind, heißt Wald.
Ein gewurzelter Baum ist ein Baum mit einem ausgezeichneten Knoten $(G, v_0)$

**Satz 1:** Äquivalent sind für einen Graphen $G = (V, E)$

a) $G$ ist einen Baum

b) Zu $v, v' \in V, v \neq v'$ 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 genau ein Pfad von $v$ nach $v'$. Gäbe es 2 verschiedene Pfade, so erhielte man einen Kreis.
b) $\rightarrow$ a): Nach Voraussetzung ist $G$ zusammenhängend. Wäre ein Kreis vorhanden, so erhielte man 2 Pfade von $v_0$ nach $v_1$, wenn $e = \{v_0, v_1\}$ im Kreis vorkommt
a) $\rightarrow$ c): Induktion
c) $\rightarrow$ a): Klar

**Satz 2:** Ist $G$ ein zusammenhängender Graph, so erhält $G$ einen aufspannenden Baum $T$, d.h. $T = (V, E')$ mit $E' \subseteq E$ und $T$ ist Baum

**Beweis:**

a) Enthält $G$ einen Kreis, so setze $T = G$, sonst wähle Kreis $(v_0, v_1, \ldots, v_n, v_0)$

$$G' = (V, E \backslash \{v_0, v_1\}) \text{ ist zusammenhängend}$$

Iteriere bis $G$ keinen Kreis mehr enthält.

b) Algorithmus (Breitensuche)
Initiiere: $S = (v_0), v_0 \in V, V' = \emptyset, E' = \emptyset$
`while` $S \neq ()$ `do`

$$v = S[1] \text{ (erstes Element der Liste)}$$
$$E'' := \{(v, v') \in E \mid v' \notin V'\}$$
$$V' := V' \cup \{v' \mid (v, v') \in E''\} \cup \{v\}$$
$$E' := E' \cup \{\{v, v'\} \in E \mid v' \in V'\}$$
$$\text{Lösche } v \text{ in der Liste } S$$
$$\text{Hänge an } S \text{ die Liste } (v' \mid \{v, v'\} \in E'')$$

`od;`

**Aufgabe:** Finde alle Bäume mit Knotenmenge $(\{v_1, \ldots, v_n\}, \{1, \ldots, n\})$
Äquivalent: Finde alle aufspannenden Bäume des Graphen $(V, \binom{V}{2}) = K_n$

$$n = 2 : Ordnung = 1$$

$$n = 3 : Ordnung = 3$$

$$n = 4 : Ordnung = 16$$

**Satz (Cayley):** Die Anzahl aller Graphen mit $V = \{1, \ldots, n\}$ ist $n^{n-2}$

**Beweis:** Jedem Baum $T$ auf $V = \{1, \ldots, n\}$ wird ein Element $P(T) = (t_1, \ldots, t_{n-2}) \in V^{n-2}$ zugeordnet. "Prüfercode" von $T$ nach folgendem Algorithmus:
Gegeben: Baum $T$
Bemerkung: 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 $d(v_0) = 1 = d(v_m)$
Algorithmus: `for i in` [1, . . . , n-2] `do`

$$\text{wähle kleinsten } v \in V \text{ mit } d(v) = 1$$

$$\text{Es gibt dann genau ein } v' \in V \text{ mit } \{v, v'\} \in E$$

$$\text{Setze } t_i := v'$$

$$V := V \backslash \{v\}$$

`od;`

**Bemerkung:** 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. Konstruiere Graphen (Baum) mit folgendem Algorithmus:
Initiiere: $E' = \emptyset$

$$\text{Sei } i = Min\{j \in V \mid j \notin t\}$$

$$E' := E' \cup \{t_i, t_1\}$$

$$\text{Ersetze } t \text{ durch } (t_2, \ldots, t_{n-1})$$

$$\text{Ersetze } V \text{ durch } V \backslash \{i\}$$

Wiederhole bis $t = ()$
Dann $E' := E' \cup V$ , beachte: $|V| = 2$
Damit erhält man Baum $T$ mit $P(T) = t$

**Definition:** Zwei Graphen $G = (V, E)$ und $G' = (V', E')$ heißen isomorph, wenn es eine Bijektion $\psi : V \to V'$ gibt mit

$$\{\{\psi(v_i), \psi(v_j)\} \mid \{v_i, v_j\} \in E\} = E'$$

(20.07.01)

**Satz (cayley):** Anzahl der Bäume auf $V$ mit $|V| = n$ ist $n^{n-2}$

$$(t_1, \ldots, t_{n-2}), t_i \in V, |V| = n$$

$$\Gamma_V(t_1, \ldots, t_{n-2}) \text{ Baum}$$

entsteht aus

$$\Gamma_{V \backslash \{v\}}(t_2, \ldots, t_{n-2})$$

durch "Anheften des Blattes $v$ an $t_1$", wobei

$$v = Min\ \{v \in V \mid v \notin \{t_1, \ldots, t_{n-2}\}\}$$

## 3.4 Planare Graphen

**Definition:** Eine ebene Einbettung eines Graphen $G = (V, E)$ ist ein Paar $\psi, \psi'$ von injektiven Abbildungen

$$\psi : V \to \mathbb{R}^2$$

$$\psi' : E \to J = \{Bild\ e \mid e : [0,1] \to \mathbb{R}^2 \text{ inj. und stetig}\} \text{ "Jordankurve"}$$

mit

$$\psi'\overbrace{\{v, v'\}}^{\in E} = Bild\ e, \{\psi(v), \psi(v')\} = \{e(0), e(1)\}$$

und

$$\psi'\{\underbrace{v_1, v_2}_{\in E}\} \wedge \psi'\{v_3, v_4\} = \bigcap_{i=1}^{n}\{\psi(v_i)\}$$

$G$ heißt planar, wenn es eine ebene Einbettung gibt.
Ist $(G, \psi, \psi')$ ein eingebetteter Graph, so heißen die Zusammenhangskomponenten von $\mathbb{R}^2 \setminus \bigcup_{e \in E} \psi'(e)$ Gebiete von $(G, \psi, \psi')$

**Satz 1:** (Eulersche Polyederformel) Ist $(G, \psi, \psi')$ ein zusammenhängender Graph, so gilt:

$$g = \text{ Anzahl der Gebiete } = |E| - |V| + 2$$

**Beweis:** Induktion nach $|E|$ (Anzahl der Kanten)

- $|E| = 0$ dann ist $|V| = 1, g = 1$
- Sei $|E| > 0$ : Ist $G$ ein Baum , so ist $|E| - |V| = -1$
  Sonst hat $G$ einen Kreis, sei $e = \{v_1, v_2\} \in E$ Kante in einem Kreis
  $G' = (V, E' = E \setminus \{e\})$ ist zusammendhängend, eingebettet
  $G'$ hat $g - 1$ Gebiete, wenn $G$ genau $g$ Gebiete hat
  $g - 1 \overset{\text{Ind.Ann.}}{=} |E'| - |V| + 2 = |E| - |V| + 2 - 1$

**Satz 2:** Ist $G = (V, E)$ planar, so ist $|E| \leq 3 \cdot |V| - 6$

**Beweis:** $\{\psi, \psi'\}$ Einbettung mit $g$ Gebieten
Jedes Gebiet wird von mindestens 3 Gebieten umrandet. Jede Kante berandet höchstens 2 Gebiete

$$2|E| \geq |\{(R, e) \mid R \text{ Gebiet und } \psi'(e) \subseteq \delta R\}| \leq 3g, e \in E$$

einsetzen in $g = |E| - |V| + 2$

$$|E| - |V| + 2 \leq \frac{2}{3}|E|$$

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

**Beispiel:**

a)

$$K_5 : |E| = 10, |V| = 5, 3|V| - 6 = 9 \Rightarrow K_5 \text{ nicht planar}$$

b)

$$K_{m,n} = (V_1 \dot{\cup} V_2, E), |V_1| = m, |V_2| = n$$

$$E = \{\{v_1, v_2\} \mid v_1 \in V_1, v_2 \in V_2\}$$

vollständiger, bipartiter Graph

$$G = K_{3,3}, |V| = 6, |E| = 9$$

$$3 \cdot \ |V| - 6 = 12$$

Bedingung von Satz 2 ist erfüllt
In jeder Einbettung von $G$ würde jedes Gebiet von $geq4$ Kanten berandet (denn es gibt in $G$ keinen Kreis der Länge 3). Der Beweis von Satz 2 liefert:

$$|E| - |V| + 2 \leq \frac{2}{4}|E|$$

$$9 = |E| \leq 2|V| - 4$$

$$12 - 4 = 8$$

**Definition:** (Zwei) Graphen, die durch endlich viele Operationen der Form

$$\rightarrow$$

oder ihre Umkehrung "Entfernung von Knoten vom Grad 2" hervorgehen, heißen 2-äquivalent.

**Satz 3:** (Kuratowski) Ein Graph $G$ ist genau dann planar, wenn er keinen Teilgraphen enthält, der 2-äquivalent ist zu $K_5$ oder $K_{3,3}$ ist.

Ohne Beweis

**Definition:** Eine ?-Färbung eines Graphen $G = (V, E)$ mit $k \in \mathbb{N}$ Farben ist eine Abbildung

$$c : V \rightarrow \{1, \ldots, k\}$$

mit $c(v) \neq c(v')$, falls $\{v, v'\} \in E$.
$G$ ist $k$-färbbar, wenn es eine Färbung mit $k$ Farben gibt.

$$\gamma(G) = Min\ \{k \mid G \text{ ist } k\text{-färbbar}\}$$

bipartiter Graph = Graph gefärbt mit 2 Farben

Färbung von Landkarten: Benachbarte Länder sollen verschieden gefärbt werden

**Satz 4:** (Vierfarbensatz) Ist $G$ planar, so ist $\gamma(G) \leq 4$

# Index