Diskrete Strukturen

Ilja Bezrukov
SS2001

16. Mai 2001

Kapitel 1

Abzählungen, Rekursionen, erzeugende Funktionen

1.1 Elementare Zählprinzipien

Sei M eine endliche Menge
$|M|$=Anzahl der Elemente von M
$|A| = n \in \mathbf{N} = \{1, 2, 3, \dots\}$
$\Leftrightarrow$ es gibt eine Bijektion $\alpha : A \to \{1, \dots, n\}$
$|A| = 0 \Leftrightarrow A = \emptyset$

1.1.1 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 $A \cap B = \emptyset$

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

1.1.2 Folgerung:

Abb.$(A, B) = B^A$ =Menge aller Abbildungen von A nach B
$|B^A| = |B|^{|A|}$
Beweis:$|A| = n$
$|B| = m, A = \{a_1, \dots, a_n\} B^A \to \underbrace{B \times B \times \cdots \times B}_{n}$
$f \mapsto (f(a_1), f(a_2), f(a_n))$ ist eine Bijektion.
$|B^A| = |B \times B \times \cdots \times B| \underset{\text{Lemma 1c}}{=} |B|^n$

1.1.3 Definition:

$f : A \to A$ heisst Permutation von A, wenn f bijektiv.
$S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} | \sigma \text{ bijektiv}\}$
Heisst auch Symmetrische Gruppe von Grad n.

1.1.4 Lemma 2:

$|S_n| = n! = 1 \cdot 2 \cdots n$
(=Anzahl der Möglichkeiten, eine n-Menge A anzuordnen). Siehe LAI.

1.1.5 Satz 1:

Die Anzahl der Teilmengen einer n-Menge A ist 2^n.
$|A| = n \Rightarrow |P(A)| = 2^n$
dabei ist $|P(A) = \{B | B \subseteq A\}$Potenzmenge von A.
$P(A) = \{\{1, 2\}, \{1\}, \{2\}, \emptyset\}$. Beispiel: $A = \{1, 2\}$.
Beweis: $P(A) \to \{0, 1\}^A$
$B \to \chi_b$ characteristische Funktion von B, definiert durch $\chi_B(x) = \begin{cases} 1 & \text{für} x \in B \\ 0 & \text{sonst} \end{cases}$
ist Bijektion.
$B = \{x \in A | \chi_B(x) = 1\} |P(A)| = ||\{0, 1\}^A| = 2^{|A|}$.

1.1.6 Definition:

$P_k(A) = \binom{A}{k}$ =Menge aller k-Teilmengen von A. $= \{B \subseteq A || B| = k\}$
Bem: $P(A) = \dot{\bigcup}_{k=0}^{n} P_k(A)$
$|A| = n$
Also nach Lemma 1 ist $|P(A)| = \sum_{k=0}^{n} |P_k(A)|$

1.1.7 Lemma 3

$|P_k(A)| = |\binom{A}{k}| = \binom{n}{k} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k!}$ falls $|A| = n$.
Beweis: $B = \{b_1, \ldots, b_k\}, |b| = k, b_i \neq b_j \text{für} i \neq j, b_i \in A$
$|\{(b_1, \ldots, b_k) | b_i \in A, b_i \neq b_j \text{für} i \neq j\}| = n(n-1) \cdots (n-k+1)$.
Es gibt k! Anordnungen von $\{b_1, \ldots, b_k\}$.
2.Beweis von Satz 1(Binomialsatz): $|A| = n$
$|P(A)| = \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k \cdot 1^{n-k} = (1+1)^n$.

1.1.8 Satz 2:

a) Pascaldreieck
$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ fr $k \geq 1, n \geq k$
. Beweis: $n \geq 1, |A| = n, \binom{n}{k}$ =Anzahl der k-Teilmengen von A.
$b \in A$
$\binom{A}{k} = \{X \subseteq A | b \notin X\} \cup \underbrace{\{X \subseteq A || X| = k, b \in X\}}_{M}$

$= {}^{A\backslash\{b\}}_{k})\dot{\cup}M.M \to ({}^{A\backslash\{b\}}_{k-1})X \to X\backslash\{b\}$ sind bijektiv.
$|\binom{A}{k}| = \binom{n-1}{k} + \binom{n-1}{k-1}$

b) Vandermondsche Identität:
$\binom{n+m}{k} = \sum_{l=0}^{k} \binom{n}{l} \cdot \binom{m}{k-l}$.
Beweis:$|A| = m+n, |B| = m, |C| = n, A = B\dot{\cup}C$
$|\binom{A}{k}_l = \{X \subseteq A||X| = k, |x \cap B| = l\}$
$l = 0, 1, \ldots, k$
$|\binom{A}{k} = \dot{\bigcup}_{l=0}^{k}|\binom{A}{k}_l$
$|\binom{m+n}{k} = ||\binom{A}{k}| = \sum_{l=0}^{k}|\underbrace{|\binom{A}{k}_l|}_{\binom{m}{l}\binom{n}{k-l}}$

1.1.9 Lemma 4 :

a) Doppeltes Abzählen
Ist $R \subseteq M \times N$, so ist $|R| = \sum |\{b \in N|(a,b) \in R\}|, a \in M$
$= \sum_{b \in N} |\{a \in M|(a,b) \in R\}|$

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

c) Inklusion-Exklusionsprinzip $A_1, \ldots A_n \subseteq M$
$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{i_1 < i_2} |A_{i_1} \cap A_{i_2}| + \sum_{\ldots} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{i_1 < \ldots < i_j \leq n} |A_{i_1} \cap \ldots \cap A_{i_j}$
Beweis:
$A \subseteq M$
$\chi_A : m \to \{0, 1\}$
$x \mapsto \begin{cases} 1 & \text{wenn} x \in A \\ 0 & \text{sonst} \end{cases}$ $|A| = \sum_{x \in M} \chi_A(x)\,(*)\chi_{A_1 \cup \cdots \cup a_n}(x) = \sum_{j=1}^{n} \sum_{1 \leq i_1 < \ldots < i_j \leq n} \chi_{A_1 \cup \cdots \cup a_n}(x)$
Daraus folgt die Beh. durch Summation über M
$\sum_{x \in M}$:

(a) Ist $x \in A_1 \cup \ldots \cup A_n$ so ist $\begin{matrix} L.S(*) = 0 \\ R.S(*) = 0 \end{matrix}$

(b) $x \in A_1 \cup \ldots \cup A_n$so ist$L.S(*) = 1$
x liege in genau $k(\geq 1)$ Teilmengen $A_1, \ldots, A_n$,
$x \in A_{j_1} \cap \ldots \cap A_{j_k}, j_1 < \ldots < j_k$
dann ist $\chi_{A_1 \cup \cdots \cup a_n}(x) = 1 \Leftrightarrow \{i_1, \ldots, \imath_j\} \subseteq \{j_1, \ldots, j_k\}$
$R.S(*) = \sum_{j=1}^{n} (-1)^{j-1} \binom{k}{j} = 1 - \underbrace{\sum_{j=0}^{k} (-1)^j \binom{k}{j} = 1}_{(1-1)^k}$.

1.2 Partitionen

1.2.1 Definition:

Eine Partition P von M (Menge) ist eine Zerlegung von M in eine Vereinigung von disjunkten, nichtleeren Teilmengen(Blöcke genannt), genauer $P = \{A_1, \dots, A_k\}$ Partition von M, wenn $M = A_1 \dot{\cup} \dots \dot{\cup} A_k$ und $A_i \neq \emptyset$ für $i = 1, \dots, k$
$Part_K(M) := \{P | P \text{ ist Partition vom M } |P| = k\}$
$S_{n,k} = |Part_K(M)| \text{falls } |M| = n$
Stirling Zahlen 2.Art $n, k \geq 0$
$S_{0,0} = 1$
Beispiele:
$S_{n,0} = 0, n \geq 1 S_{n,1} = 1, n \geq 1 S_{n,n} = 1 S_{n,n-1} = \binom{n}{2}$

1.2.2 Satz 1:

Es gilt für $1 \leq k \leq n S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$

Beweis: $a \in M, |M| = n \geq 1$
$Part_k M = X_1 \uplus X_2$, wobei
$X_1 = \{P \in Part_k M | \{a\} \not\in P\}$
$X_2 = \{P \in Part_k M | \{a\} \in P\}$
$X_2 = \{P = \{\{a\}, B_1, \dots, B_{k-1}\} | \{B_1, \dots B_{k-1}\} \in Part_{k-1} M \backslash \{a\}\}$
$|X_2| = S_{n-1,k-1}$
Ist $P \in X_1$ dann erhält man durch löschen von a eine Partition $\{B_1, \dots, B_k\}$ von $M \backslash \{a\}$
Umgekehrt erhalten wir zu jedem $\{B_1, \dots B_k\} \in Part_k M \backslash \{a\}$ genau k verschiedene Partitionen aus X_1, nämlich $\{\{a\} \cup B_1, B_2, \dots B_k\}, \dots, \{B_1, B_2, \dots B_k \cup \{a\}\}$
$|X_1| = k \cdot S_{n-1,k}$.

Bemerkung:

1. { Partitionen von M } $\leftrightarrow$ { Äquivalenzrelationen auf M }
2. Ist $f : M \to N$ eine surjektive Abb $f^{-1}(b) = \{a \in M | f(a) = b\} \neq \emptyset, b \in M$
   $M = \bigcup_{b \in N} f^{-1}(b)$
   $P_f = \{f^{-1}(b) | b \in N\} \in Part_{|N|} M$

1.2.3 Satz 2:

Ist $|M| = m, |N| = n$

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

2. $|\underbrace{Inj(M,N)}_{\text{Injektive Abb.}}| = n^{\underline{m}} = n(n-1)\cdots(n-m+1)$ n nach m fallend

3. $|\underbrace{Surj(M,N)}_{\text{Surjektive Abb.}}| = n!S_{m,n}$

<u>Beweis:</u>

1. siehe 1

2. $M = \{a_1,\dots,a_m\}$ Jede Abb. $f : M \to N$ ist gegeben durch $f(a_1) = b_1 \in N \dots f(a_m) = b_m \in N$
   f injektiv $\Leftrightarrow b_i \neq b_j$ für $i \neq j$
   für b_1 gibt es n Möglichkeiten $b_1 \in N$
   für b_2 gibt es n-1 Möglichkeiten $b_2 \in N\backslash\{b_1\}$
   $\dots$
   für b_m gibt es n-m+1 Möglichkeiten $b_m \in N\backslash\{b_1,\dots b_{m-1}\}$

3. $f : M \to N$ surjektiv
   $P_=\{f^{-1}(b)|b \in N\} \in Part_n M = \{A_1,\dots A_n\}$
   $P_f = P_g \Leftrightarrow g = \sigma \circ f$ mit $\sigma \in Sym\ N$
   $|Surj(M,N)| = S_{m,n} \cdot n!$

1.2.4 <u>Satz 3:</u>

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

<u>Beweis:</u>
$Abb(M,N) = \bigcup_{A\subseteq N} Surj(M,A)$
f kann man auffasen als surj. Abb. $f : M \to Bild(f) = \{f(a) \in N|a \in M\} \subseteq N$
$n^m = |Abb(M,N)| = \sum_{A\subseteq N} |surj(M,A)|$
$= \sum_{k=0}^{n} \sum_{A\in\binom{N}{k}} |Surj(M,A)| = \sum_{k=0}^{n} k! \cdot S_{m,k}$
$= \sum_{k=0}^{n} \frac{n^{\underline{k}}}{k!} S_{m,k}$

1.3 Permutationen

$S_n = Sym(\underline{n}) = \{\sigma : \{1,\dots,n\} \to \{1,\dots,n\}|\sigma \text{ bijektiv}\}$
$|S_n| = n!$
jedes $\sigma \in S_n$ kann durch eine Wertetabelle angegeben werden:

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

1.3.1 <u>Bemerkung:</u>

$(S_n,\cdot)$ ist eine Gruppe. $\sigma_1 \circ \sigma_2 : \{1,\dots,n\} \to \{1,\dots,n\},\ x \mapsto \sigma_1(\sigma_2(x))$

1.3.2 Definition:

Ein k-Zyklus $(i_1, \ldots, i_k) = \sigma \in S_n, \{i_1, \ldots, i_k\} \in \{1, \ldots, n\}$ ist eine Permutation mit
$\sigma(i_1) = i_2\sigma(i_2) = i_3 \cdots \sigma(i_{k-1}) = i_k\sigma(i_k) = i_1$
und $\sigma(i) = i$ für $i \not\in \{i_1, \ldots, i_k\}$

1.3.3 Beispiel:

σ wie oben
$\sigma = (1\ 4\ 2\ 3\ 7\ 6) \circ (5\ 9) \circ (8)$

1.3.4 Bemerkung:

Jedes $\sigma \in S_n$ lässt sich als Produkt von Zyklen schreiben.
Beispiel: $S_3 = \{(1)(2)(3), (1)(2\ 3), (2), (1\ 3), (3)(1\ 2), (1\ 2\ 3), (1\ 3\ 2)\}$

1.3.5 Definition:

Die Stirlingzahlen $s_{n,k}$ 1.Art geben die Anzahl der Permutationen von $\{1, \ldots, n\}$ an, die genau k (disjunkte) Zyklen haben.

1.3.6 Definition:

Ein (r) Zyklus $\zeta = (i_1, \ldots, i_r)$ ist eine Permutation $\zeta \in S_n$ mit Ziffernmenge
$Z(\zeta) = \{i_1, \ldots, i_r\}$ mit $|Z(\zeta) = r$
$Per_k(\underline{n}) = \{\sigma \in S_n | \sigma = \zeta_1 \circ \ldots \circ \zeta_k$ mit $Z(\zeta_1) \uplus \ldots \uplus Z(\zeta_k) = \{1, \ldots, n\} = n\}$.

1.3.7 Bemerkung:

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

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

1.3.8 Definition:

$s_{n,k} = |Perm_k(\underline{n})|\ n, k \geq 1$
$s_{0,0} = 1\ s_{0,k} = 0,\ k > 0$
Stirling-Zahlen 1. Art.

1.3.9 Lemma 1:

a) $s_{n,k} = 0$ für $k > n$

b) $s_{n,n} = 1$ für $n \in \mathbf{N}_0 Perm_n \underline{n} = \{(1) \circ (2) \circ \cdots \circ (n) = id\}$

c) $s_{n,1} = (n-1)!$
$Perm_1(\underline{n}) = \{(n\ i_2 \ldots i_n) |\ |\{i_2, \ldots, \imath_n\}| = n-1\}$
$|\ | = (n-1)!$

1.3.10 Satz 1

für $n, k \in \mathbf{N}$ gilt $s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$
Beweis:
$X = Perm_k(\underline{n}) = X_1 \uplus X_2$
$X_1 = \{\sigma \in X | \sigma(n) = n\} = \{\sigma = (n) \circ \zeta_1 \circ \ldots \circ \zeta_{k-1} | \zeta_1 \circ \ldots \circ \zeta_{k-1} \in Perm_{k-1}(\underline{n-1})\}$
$|X_1| = s_{n-1,k-1}$
$X_2 = \{\sigma \in X | \sigma(n) \neq n\}$
Jedes $\sigma \in X_2$ liefert durch Streichen von n eine Permutation
$\tau : \underbrace{(i_1 \ldots i_r)(i_{r_1+1} \ldots i_{r_1+r_2}) \cdots (\imath_{r_1+r_{k-1}+1}\ i_{n-1})}$
k Zyklen der Länge $r_1, r_2, \ldots, r_k \in Perm_k(\underline{n-1})$
Umgekehrt liefert jedes solches $\tau \in Perm_k(\underline{n-1})$ genau n-1 Elemente aus X_2 indem wir
vor $i_1, i_2, \imath_{n-1}$ n einfügen:
$(n\ i_1 \ldots i_r)(i_{r_1+1} \ldots i_{r_1+r_2}) \cdots (\imath_{r_1+r_{k-1}+1}\ i_{n-1})$
$(i_1\ n \ldots i_r)(i_{r_1+1} \ldots i_{r_1+r_2}) \cdots (\imath_{r_1+r_{k-1}+1}\ i_{n-1}) \cdots |X_2| = (n-1)\ |Perm_k(\underline{n-1})| = (n-1)s_{n-1,k}$

1.4 Formale Potenzreihen(erzeugende Funktionen)

Bei der Komplexitätsanalyse von Algorhytmen entstehen oft Rekursionsgleichungen, z.B. $a_n = a_{n-1} + a_{n-2}$
Um solche Rekursionen explizit zu lösen, brauchen wir erzeugende Funktionen.
$(a_n)_{n \in \mathbf{N_0}} = (a_0, a_1, a_2, \ldots)$
$\sum_{n=0}^{\infty} a_n x^n$ formaler Ausdruck, x unbestimmte

1.4.1 Definition:

Sei K ein Körper, z.B. $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{F_2}$
$K[[x]] := \{\sum_{n=0}^{\infty} a_n x^n | a_n \in K\}$ und $\sum_{k=0}^{\infty} a_n x^n = (a_n)_{n \in \mathbf{N}_0} x^n := (a_j)_{j \in \mathbf{N}_0}$
mit $a_j = \begin{cases} 1 & \text{für} j = n \\ 0 & \text{sonst} \end{cases}$
$\sum_{n=m}^{\infty} a_n x^n = (b_j)_{j \in \mathbf{N}_0}$ mit $b_j = \begin{cases} a_j & \text{für} j \geq n \\ 0 & \text{sonst} \end{cases}$

$$\sum_{n=0}^{\infty} a_k x^{kn} = (b_j)_{j \in \mathbf{N}_0} \text{ mit } b_j = \begin{cases} 0 & \text{wenn } j \neq kn \\ a_n & \text{wenn } j = kn \end{cases}$$

1.4.2 Satz 1:

Definiert man

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

2. 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: Siehe LAI :-).

1.4.3 Satz 2:

Definert man, (zusätzlich zu $+$, siehe Satz 1)
$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{j=0}^{\infty} a_j x^j\right) := \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j\right) x^k = \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k$
so ist $(K[[x]], +, \cdot)$ ein kommutatiover 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 $0 + A = A \forall A \in K[[x]]$
(A4) zu $A \in K[[x]] \exists -A \in K[[x]]$ mit $A + -A = 0$
(M) $(A \cdot B) \cdot C = A \cdot (B \cdot C)*$
(Komm) $A \cdot B = B \cdot A*$
(Eins) Es gilt $1 \in K[[x]]$ mit $1 \cdot A = A \; \forall A \in K[[x]]$
(D) Es gilt $A \cdot (B + C) = A \cdot B + A \cdot C*$

$*: \; \forall A, B, C \in K[[x]]$
Einselement ist $1 \cdot x^0 = 1$

1.4.4 Lemma 1:

$x^m \cdot \sum_{n=0}^{\infty} a_n x^n = \sum_{n=m}^{\infty} a_{n-m} x^n$
In der Folgesprache bedeutet dies $x^m \cdot (a_0, a_1, \ldots) = (0, 0, 0, \ldots, 0, a_1, a_2, \ldots)$
Multiplikation mit x^m bewirkt Verschieben der Folge $(a_n)_{n \in 0}$ um m Stellen nach rechts.

1.4.5 Folgerung:

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

1.4.6 Beispiel:

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

1.4.7 Bem. 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.
[also $A = B^{-}1 = \frac{1}{B}$]und A (und auch B) heisst invertierbar.
Beweis: Ist $A \cdot B = 1$ und $A \cdot C = 1$, so folgt $C = C \cdot 1 = C(A \cdot B) = (\underbrace{A \cdot C}_{=1}) \cdot B = B$
Beispiele: In $\mathbf{Z}$ sind nur 1 und -1 invertierbar.

1.4.8 Folgerung:

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

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

[Ist $\frac{1}{1-cx}$ eine Formale Potenzreihe?
Gegenfrage: ist $\frac{1}{0{,}5} \in \mathbf{Z}$?]

1.4.9 Beispiel:

Code mit variabler Wortlänge (Komprimieren von Daten)
$Bu = \{a, b, c\}$
$Zi = \{0, 1\}$
$W_k = \{$Folgen aus $0 < i < k$ Buchstaben gefolgt von $k - i$ Ziffern $\} Co_n = \bigcup_{k=2}^{n} W_k$
z.B.$aa1|bc0001|ac1|$
$w_k = |W_k| = \sum_{i=1}^{k-1} 3^i 2^{k-i} = \underbrace{\sum_{i=o}^{k-1} 3^i 2^{k-i}}_{c_k} -2^k - 3^k$
Beh: $c_k = 3^{k+1} - 2^{k+1}$
$c \cdot \sum_{k=0}^{\infty} c_k x^k = (\sum_{i=0}^{\infty} 3^i x^i)(\sum_{j=0}^{\infty} 2^j x^j)$
$\underset{\text{Folg.1}}{=} \frac{1}{1-3x} \cdot \frac{1}{1-2x} = \frac{1}{(1-3x)(1-2x)}$
Ansatz:
$= \frac{\alpha}{1-3x)} + \frac{\beta}{(1-2x)} = \frac{\alpha(1-2x)+\beta(1-3x)}{(1-3x)(1-2x)}$
$\alpha(1 - 2x) + \beta(1 - 3x) = 1$
$\beta = -2, \alpha = 3$
$c = \sum_{k=0}^{\infty} c_k x^k = \frac{3}{(1-3x)} - \frac{2}{(1-2x)}$
$c = \sum_{k=0}^{\infty} c_k x^k = 3 \cdot \sum_{i=0}^{\infty} 3^i x^i - 2 \cdot \sum_{i=0}^{\infty} 2^i x^i$
$= \sum_{i=0}^{\infty} (\underbrace{3^{i+1} - 2^{i+1}}_{c_i}) x^i$

1.4.10 Satz 3:

Genau dann ist $A = \sum_{n=0}^{infty} a_n x^n \in K[[x]]$ invertierbar, wenn $a_0 \neq 0$ ist.
Beweis: A ist invertierbar$\Leftrightarrow$ $\exists\, B = \sum_{i=0}^{\infty} b_i x^i$ mit $A \cdot B = 1$
$\sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k = 1 \Leftrightarrow \sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} 1 & \text{für} k = 0 \\ 0 & \text{sonst} \end{cases}$

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

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 $b_0 = a_0^{-1} \in K$ und $b_n = \frac{1}{a_0} \cdot (-a_1 b_{n-1} -$

$\cdots - a_n b_0)$ rekursiv.

$K[[x]] = \{\sum_{n=0}^{\infty} a_n x^n | a_n \in K\}$ Formale Potenzreihen
$K[x] = \{\sum_{n=0}^{\infty} a_n x^n | a_n \in K$ und $a_n \neq 0$ nur für endl.viele n $\}$
$= \{\sum_{n=0}^{r} a_n x^n | a_n \in K, r \in N_0\}$ Polynomring

- zu $K[x]$ gibt es einen Einsetzungshomomorphismus, ist $A \in K[[x]]$, so kann man in A im Allgemeinen nichts einsetzen.
- In $K[x]$ sind nur die Polynome vom Grad=0 invertierbar.

1.4.11 Satz 3:

$A = \sum_{n=0}^{\infty} a_n x^n \in K[[x]]$ ist invertierbar genau dann, wenn $a_0 \neq 0$ ist.
$(\sum_{n=0}^{\infty} a_n x^n) \cdot (\sum_{n=0}^{\infty} b - n x^n) = \sum_{n=0}^{\infty} \underbrace{\left(\sum_{i=0}^{n} a_i b_{n-i}\right)}_{=1=1x^0 \Leftrightarrow \delta_{n,0} x^n}$
Dann ist $(b_0, b_1, b_2, \ldots)$ Lösung des folgendes Gleichungssystems:

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

Lösbar $\Leftrightarrow a_0 \neq 0$

1.4.12 Beispiel:

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

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

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

1.4.13 Beispiel:

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

1.4.14 Folgerung:

$$\begin{aligned}
\frac{1}{(1-cx)^2} &= \sum_{n=0}^{\infty} (n+1)c^n x^n \\
\text{allgemeiner } \frac{1}{(1-cx)^m} &= \sum_{n=0}^{\infty} \binom{n+m-1}{m-1} c^n x^n
\end{aligned}$$

1.4.15 Definition:

Die Abbildung

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

heisst *formale Ableitung*

1.4.16 Lemma 1:

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

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

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

1.4.17 Folgerung:

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

$$\begin{aligned} A \cdot A^{-1} &= 1 \qquad D(1) = 0 \\ 0 = D(A \cdot A^{-1} &= A \cdot D(A^{-1}) + D(A) \cdot A^{-1} \text{ nach Lemma 1.b} \\ -D(A) \cdot A^{-1} &= D(A^{-1}) \cdot A \end{aligned}$$

1.4.18 Beispiel:

$$\begin{aligned} A &= 1 - cx \;\in K[[x]] \\ A^{-1} &= \sum_{n=0}^{\infty} c^n x^n \\ D(A^{-1}) &= \sum_{n=0}^{\infty} (n+1)c^{n+1}x^n \qquad D(A) = -c \\ &\underset{\text{Folg.}}{=} -\frac{D(A)}{A^2} = \frac{c}{(1-cx)^2} \qquad c \neq 0 \text{ O.b.d.A.} \\ \frac{1}{(1-cx)^2} &= \sum_{n=0}^{\infty} (n+1)c^n x^n \end{aligned}$$

neuer Beweis der Folgerung

1.5 Lösen von Rekursionsgleichungen

1.5.1 Beispiel:

Die Fibonacci-Zahlen F_n sind (für $n \in_0$) so definert:

$$F_0 = 0 \qquad F_1 = 1$$
$$(*) \qquad \mathrm{F}_n = F_{n-1} + F_{n-2} \qquad \forall n \geq 2$$

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

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

$$
\begin{aligned}
&= F_0x^0 + f_1x + \sum_{n=2}^{\infty} F_{n-1}x^n + \sum_{n=2}^{\infty} F_{n-2}x^n \\
&= F_0x^0 + F_1x + x \cdot \sum_{n=1}^{\infty} F_nx^n + x^2 \cdot \underbrace{\sum_{n=0}^{\infty} F_nx^n}_{F} \\
&= F_0x^0 + F_1x + xF + x^2F - xF_0x^0 \\
F &= x + xF + x^2F \\
& \quad F(1-x-x^2) = x \\
F &= \frac{x}{1-x-x^2}
\end{aligned}
$$

suche $\alpha, \beta \in K$ und $a, b \in K$ so dass $\frac{x}{1-x-x^2} = \frac{a}{1-\alpha x} + \frac{b}{1-\beta x}$

1.5.2 Satz 1: Partialbruchzerlegung

K seie ein Körper

$$
\begin{aligned}
g &= (1-\alpha_1 x)^{m_1} \cdot \dots \cdot (1-\alpha_r x)^{m_r} \qquad \in K[x] \ \alpha_i \neq 0 \forall i \\
& \quad f \in K[x] \text{Grad } f < \text{Grad } g \\
& \quad \text{Dann gibt es } f_i \in K[x] \text{ Grad } f_i < m_i \\
\text{mit } \frac{f}{g} &= \frac{f_i}{(1-\alpha_1 x)} m_1 + \dots + \frac{f_r}{(1-\alpha_r x)} m_r \\
\frac{f_i}{(1-\alpha_i x)^{m_i}} &= \frac{a_{i_1}}{1-\alpha_i x)} + \frac{a_{i_2}}{(1-\alpha_i x)^2} + \dots + \frac{a_{m_i}}{(1-\alpha_i x)^{m_i}}
\end{aligned}
$$

1.5.3 Bemerkung:

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

1.5.4 Definition:

$$\text{Ist } g = \sum_{i=0}^{n} a_i x^i \text{mit } a_n \neq 0 \text{,so sei } g^R = \sum_{i=0}^{n} a_{n-i} x^i$$

das *reflektierte Polynom*

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

1.5.5 Lemma 1:

es gilt $g(\alpha) = 0$ mit $\alpha \neq 0 \Leftrightarrow g^R(\alpha^{-1}) = 0$
Beweis: Sei $\alpha \neq 0$ in K

$$0 = g(\alpha) \quad = \quad \sum_{i=0}^{n} a_i \cdot \alpha^i \Rightarrow 0 = \alpha^{-n} g(\alpha)$$

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

1.5.6 Bemerkung:

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

1.5.7 Satz 2: Fundamentalsatz der Algebra

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

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

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

1.5.8 Folgerung:

$$\text{Ist } f = \sum_{i=0}^{n} a_i x^i \in \mathbf{C} \text{ und } a_n \neq 0, a_0 \neq 0$$

so gibt es $\alpha_1, \ldots, \alpha_n$ mit

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

denn nach Satz 2 gilt

$$\begin{aligned} f^R &= a_0(x-\alpha_1)\cdots(x-\alpha_n) \\ f = (f^R)^R &= x^n(1/x-\alpha_1)\cdots(1/x-\alpha_n) \\ &= (1-\alpha_1 x)\cdots(1-\alpha_n x) \end{aligned}$$

Fortsetzung des Fibonacci-Beispiels

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

1.5.9 Verfahren zum Lösen von linearen Rekursionen

(mit konstanten Koeffizienten)

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

mit gegebenen $c_i \in \mathbf{C}$

und Anfangsbed. $a_i = b_i$ für $i = 0, 1, \ldots, k-1 \qquad b_i \in \mathbf{C}$ gegeben.

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

Auflösen nach A

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

$$mit$$

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

Es wird jetzt eine *Partialbruchzerlegung* durchgeführt:

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

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

Die α_i im Verfahren erhält man als Nullstellen des reflektierten Polynoms

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

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

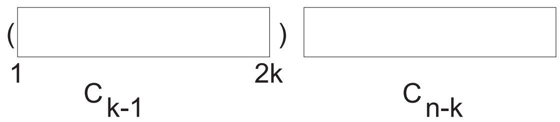
1.5.10 Beispiel:Catalanzahlen

$\mathbf{C}_n$ ={zulässige Klammerungen mit 2n Klammern }

$$C_n \quad = \quad |\mathbf{C}_n|$$

$$\begin{aligned}
C_0 &= 1 \\
C_1 &= 1 \qquad () \\
C_2 &= 2 \qquad ()(), (()) \\
C_3 &= 5 \\
C_n &= \text{n-te Catalanzahl}
\end{aligned}$$

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



$$\begin{aligned}
\mathbf{C_n} &= \biguplus_{k=1}^{n} \mathbf{C}_n^{(k)} \\
|\mathbf{C_n}| = C_n &= \sum_{k=1}^{n} C_{k-1}C_{n-k} \qquad n \geq 1 \\
C &= \sum_{n=0}^{\infty} C_n x^n \\
&= C_0 + \sum_{n=1}^{\infty} C_n x^n \\
&= 1 + \sum_{n=1}^{\infty} \left(\sum_{k=1}^{n} C_{k-1}C_{n-k} \right) x^n \\
&= 1 + (x \cdot C) \cdot C \\
C &= 1 + x \cdot c^2 \qquad \cdot x \\
& x^2C^2 - xC + x = 0 \\
& x^2C^2 - xC + 1/4 = -x + 1/4 \\
& ((Cx - 1/2)^2 = -x + 1/4 \\
xC - 1/2 &= \pm\sqrt{-x + 1/4} \\
xC &= 1/2 \cdot (1 \pm \sqrt{1 - 4x})
\end{aligned}$$

1.5.11 <u>Satz 3:</u>

$$0 \neq A = \sum_{n=0}^{\infty} a_n x^n \in K[[x]] \text{ein } B = \sum_{n=0}^{\infty} b_n x^n \in K[[x]] \text{ mit } B^2 = A$$

genau dann, wenn es ein $b \neq 0$gibt mit $B^2 = a_0 \quad (\neq 0)$

1.6 Die Polynommethode

1.6.1 Satz 1

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

$$f = \sum_{i=0}^{n} a_i x^i \qquad a_n \neq 0$$

so hat f höchstens n Nullstellen.

1.6.2 Folgerung:

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

und ist $f(\alpha_i) = g(\alpha_i)$ für alle $\alpha_i \in M \subseteq K$ mit $|M| \geq n+1$
so gilt $f = g$, d.h. $a_i = b_i \forall i = 0, \ldots, n$.
Beweis: folgt aus Satz1; betrachte $f - g$ Grad$(f-g) \leq n$ also $f - g = 0$.

Im folgenden sei K ein Körper mit
$Q \subseteq K$

1.6.3 Definition:

$$x^{\underline{n}} = x(x-1)\cdots(x-n+1) \in K[x] \binom{x}{n} = \frac{1}{n!} x^{\underline{n}} \qquad \in K[x] x^{\underline{0}} = 1 \binom{x}{0} = 1$$

Beispiel:
In 1.2.4 Satz 3:

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

$$= \sum_{k=0}^{n} S_{n,k} m^{\underline{k}} \tag{1.1}$$

für $n \geq k > m$ gilt $m^{\underline{k}} = m(m-1)\cdots 0(\ldots) = 0$
für $n < k \leq m$ gilt $S_{n,k} = 0$

$$\begin{aligned} \text{Setze } f &= x^n \\ g &= \sum_{k=0}^{n} S_{n,k} x^{\underline{k}} \\ f(m) &= g(m) \quad \forall m \in \mathbf{N} \text{ wegen } (1.1) \end{aligned}$$

1.6.4 Satz 2:

Ist $\mathbf{Q} \subseteq K$ Körper, so gilt

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

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

1.6.5 Bemerkung:

$(x^n)_{n\in\mathbf{N}_0}$ und $(x^{\underline{n}})_{n\in\mathbf{N}_0}$
sind K-Basen des K-Vektorraums K[x] und

$$[S_{n,k}]_{n,k\in\mathbf{N}_0}$$

$$\left[(-1)^{n-k} s_{n,k}\right]_{n,k\in\mathbf{N}_0}$$

sind Basiswechselmatrizen, also invers zu einander.