Grundlagen über Zahlen

$\mathbb{N} := \{0, 1, 2, \ldots\}$	Menge der Natürlichen Zahlen
$\mathbb{N}^* := \{1, 2, 3, \ldots\}$	Menge der Natürlichen Zahlen ohne Null
$G := \{0, 2, 4, \ldots\} \equiv \{x \mid \exists\ m \in \mathbb{N} : x = 2 \cdot m\}$	Menge der Geraden Natürliche Zahlen
$U := \{1, 3, 5, \ldots\} \equiv \{x \mid \exists\ m \in \mathbb{N} : x = 2 \cdot m + 1\}$	Menge der Ungeraden Natürliche Zahlen
$\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$	Menge der Ganzen Zahlen
$\mathbb{Q} := \{\frac{z}{n} \mid z, n \in \mathbb{Z} \wedge n \neq 0\}$	Menge der Rationalen Zahlen
$\mathbb{R} := \{x \mid x \text{ ist eine Zahl}\}$	Menge der Reellen Zahlen
$\mathbb{C} := \{x + yi \mid x, y \in \mathbb{R}\}$	Menge der Komplexen Zahlen

Formeln

B-adische Darstellung $a \in \mathbb{N}^*, a = \sum_{k=0}^{l} \alpha_k B^k,$ so ist $(\alpha_l, \alpha_{l-1}, \ldots, \alpha_0)$ die B-adische Darstellung von a mit **Stellwertsystem** zur Basis B

Fakultätsfunktion $n! \equiv n \cdot n - 1 \cdot \ldots, \cdot 1$

Fibonacci $F_0 := 0,\ F_1 := 1,\ F_n := F_{n-1} + F_{n-2}$ für $n \geq 2$

Geometrische Summenformel $\sum_{j=0}^{n} r^{\ j} = \frac{r^{\ n+1} - 1}{r - 1}$

Algorithmen

Data: $a \in \mathbb{N}^*$
Result: $[\alpha_k, \ldots, \alpha_0]$
$k \leftarrow 0,$
$x \leftarrow a$ `div` $B,$
$\alpha_0 \leftarrow a$ `mod` $B,$
$L \leftarrow [\alpha_0],$
while $x \neq 0$ **do**
  $k \leftarrow k + 1,$
  $y \leftarrow x$ `div` $B,$
  $\alpha_k := x$ `mod` $B,$
  $x \leftarrow y,$
  `// füge` α_k `an den Anfang der Liste` L `hinzu,`
  $L = [\alpha_k, \ldots, \alpha_0],$
end

Algorithm 1: B-adische Darstellung

Data: $a, b \in \mathbb{Z}$
Result: $d = \text{ggT(a, b)}$
$s \leftarrow |a|,$
$t \leftarrow |b|,$
while $t \neq 0$ **do**
  $r \leftarrow s$ `mod` $t,$
  $s \leftarrow t,$
  $t \leftarrow r,$
end
$d := s$

Algorithm 2: Euklidischer Algorithmus

Data: $a, b \in \mathbb{Z}$
Result: $d = \text{ggT(a, b)}$ und $x, y \in \mathbb{Z}$ mit $xa + yb = d$
$s \leftarrow |a|$,
$t \leftarrow |b|$,
$x \leftarrow 1, y \leftarrow 0, u \leftarrow 0, v \leftarrow 1$,
while $t \neq 0$ **do**
  $q \leftarrow s$ `div` t,
  $r \leftarrow s$ `mod` t,
  $s \leftarrow t, t \leftarrow r$,
  $x \leftarrow u_{alt}$,
  $y \leftarrow v_{alt}$,
  $u \leftarrow x_{alt} - q \cdot u_{alt}$,
  $v \leftarrow y_{alt} - q \cdot v_{alt}$,
end
$d \leftarrow s$,
$x \leftarrow \text{sgn}(a) \cdot x$,
$y \leftarrow \text{sgn}(b) \cdot y$,

Algorithm 3: Erweiterter Euklidischer Algorithmus

Mengen und Abbildungen

Abbildungen

Funktion	Eine Abbildung f von M nach N	M heißt Definitionsbereich
	ordnet jedes $x \in M$ <u>eine</u> $y \in N$ zu	$f : M \to N, x \mapsto y$
Bild	$Bild(f) := \{y \mid \exists\, x \in M : f(x) = y\}$	Wertebereich
Urbild	$Urbild(f) := \{x \mid \exists\, y \in N : f^{-1}(y) = x\} \subseteq M$	
Injektivität	$\forall\, x, x' \in M : f(x) = f(x') \Rightarrow x = x'$	
Surjektivität	$\forall\, y \in N : \exists\, x \in M : f(x) = y$	
Bijektivität	$\forall\, x \in M : \exists\, y \in N : f(x) = y \wedge f^{-1}(y) = x$	f ist Injektiv und Surjektiv
Umkehrfunktion	Sei $f : M \to N, x \mapsto y$ eine bijektive Funktion	
	$f^{-1} : N \to M, y \mapsto x$ ist die Umkehrfunktion	
Komposition	Seien f, g Funktionen mit $f : M \to N$ und	

	$g : N \to O$, dann ist $f \circ g : M \to O$	
	f, g injektiv $\Rightarrow f \circ g$ injektiv	
	f, g surjektiv $\Rightarrow f \circ g$ surjektiv	
	f, g bijektiv $\Rightarrow f \circ g$ bijektiv	$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
Abb(M, N)	$\{f \mid f : M \to N\}$	
Symm(M, N)	$\{f \mid f \in \text{Abb}(M, N), f \text{ ist bijektiv}\}$	
Identitätsabbildung	$id_M : M \to M, x \mapsto x$	

Mengen

Seien M und N zwei endliche, nicht-leere Mengen mit $m = |M|, n = |N|, \psi : M \to N$

Teilmenge	$N \subseteq M \equiv \forall\ n \in N : n \in M$
Mächtigkeit	$l = |M|, M$ hat l Elemente
n-Menge	$M = [n]$ und $M = \{m_1, m_2, \dots, m_k\}, \forall\ m_i \in M : i \in [n]$
Binäre Folgen	$\mathrm{Abb}(\mathbb{N}^*, \{0,1\})$
Char. binäre Folge	$\mathcal{X}_U : \mathbb{N}^* \to \{0,1\}, n \mapsto \begin{cases} 1, & \text{falls } n \in U \\ 0, & \text{falls } n \notin U \end{cases}$
Leere Menge	$|M| = 0 \Leftrightarrow M = \emptyset$ und für jede Menge N gilt: $\emptyset \subseteq N$
Karthesische Produkt	$M \times N := \{(x,y) \mid x \in M, y \in N\}$
Schubfachprinzip	$m > n \Rightarrow \psi$ nicht injektiv
	$m < n \Rightarrow \psi$ nicht surjektiv
Gleichmächtigkeitsregel	$m = n \Rightarrow \psi$ ist bijektiv
	Es seien $M_1, M_2, \dots, M_l$ endliche Mengen mit $M_i \cap M_j = \emptyset$
Summenregel	$\bigcup\limits_{k=1}^{l} M_k$ ist eine endliche Menge und $\left|\bigcup\limits_{k=1}^{l} M_k\right| = \sum\limits_{k=1}^{l} |M_k|$
Produktregel	$|M \times N| = |M| \cdot |N|$
Allg. Produktregel	$|\times_{k=1}^{l}| = \prod\limits_{k=1}^{l} |M_k|$
Potenzregel	$\mathrm{Abb}(M,N)$ endliche Menge und $|\mathrm{Abb}(M,N)| = |N|^{|M|}$
Potenzmenge	$\mathcal{P}(N) := \{U \mid U \subseteq N\}$ und $|\mathcal{P}(N)| = 2^{|N|}$
	$\mathcal{P}_k(N) := \{U \mid U \subseteq N \wedge |U| = k\}$
Binomialkoeffizienten	$\binom{n}{k} := |\mathcal{P}_k(n)|$ die Anzahl k-elementigen Teilmengen einer n-Menge
Unendliche Menge	$\exists\ f \in \mathrm{Abb}(\mathbb{N}^*, M) : f$ injektiv $\Rightarrow M$ ist unendlich
	$\exists\ f \in \mathrm{Abb}(\mathbb{N}^*, M) : f$ bijektiv $\Rightarrow M$ ist abzählbar unendlich
	$\exists\ f \in \mathrm{Abb}(\mathbb{N}^*, M) : f$ bijektiv und $\nexists\ g \in \mathrm{Abb}(\mathbb{N}^*, M) : g$ surjektiv
	$\Rightarrow M$ ist überabzählbar unendlich
ÜÜÜberabzählbar unendlich	$\mathcal{P}(\mathbb{R})$

Algebraische Grundstrukturen

	$\circ : M \times M \to M$	
	$(a,b) \mapsto c$	
Assoziativität	$\forall\ a,b,c \in M : a \circ (b \circ c) \circ b = (a \circ b) \circ c$	
Kommutativität	$\forall\ a,b \in M : a \circ b = b \circ a$	
Distributivität	$\forall\ a,b,c \in M : a \odot (b \oplus c) = a \odot b \oplus a \odot c$	$\mathbf{DG}_1$
	$\forall\ a,b,c \in M : (a \oplus b) \odot c = a \odot b \oplus b \odot c$	$\mathbf{DG}_2$
Neutrales Element	$\exists\ e \in M : \forall\ a \in M : e \circ a = a = a \circ e$	
Inverses Element	$\forall\ a \in M : \exists\ a^{-1} \in M : a \circ a^{-1} = e$	

	AG	NE	IE	KG
Monoid	$\times$	$\times$		
Gruppe	$\times$	$\times$	$\times$	
Kommutative Gruppe	$\times$	$\times$	$\times$	$\times$

Einheitengruppe $E(R) := \{x \mid x \in M \wedge \exists y \in M : x \odot y = e\}$

(Trivialer) Ring $(M, \oplus, \odot, n, e)$ ist ein Ring falls:
$(M, \oplus, n)$ ist eine kommutative Gruppe
$(M, \oplus, e)$ ist ein Monoid
es gelten die Distributivgesetze für $\odot, \oplus$

Nicht-trivialer Ring M ist Ring und $|M| \geq 2$

Integritätsbereich M ist ein Ring und $\forall\ a, b \in M : a \odot b = n \Rightarrow a = n \vee b = n$

Schiefkörper $\forall\ a \in M : a \neq 0 : \exists\ a' \in M : a \odot a' = e$

Körper M ist ein Körper falls M ein kommutativer Schiefkörper ist

Relationen

Sei R eine Relation auf M $(R \subseteq M \times M)$

Eigenschaften

Reflexivität $\forall\ x \in M : (x, x) \in R$

Symmetrie $\forall\ (x, y) \in R : (y, x) \in R$

Transitivität $\forall\ (a, b), (b, c) \in R : (a, c) \in R$

Äquivalenzrelation R ist eine Äquivalenzrelation $\Leftrightarrow$ R ist reflexiv, symmetrisch und transitiv

Äquivalenzklasse $[a]_R := \{x \mid x \in M \wedge (a, x) \in R\}$
$M/R := \{x \mid [x]_R\}$ die Menge aller Äquivalenzklassen von R

Repräsentant $x \in [a]_R$

Repräsentantensystem $\{x \mid x$ ist ein Repräsentant$\}$

Restklassenring/Körper

Addition $[x]_n + [y]_n := [x + y]_n$

Multiplikation $[x]_n \cdot [y]_n := [x \cdot y]_n$

Additiv Inverse $[x]_n + [n - x]_n = [x + (n - x)]_n = [n]_n = [0]_n$

Multiplikativ Inverse $[x]_n \cdot [x']_n = [1]_n$

Kongruent $x \equiv_n y \Leftrightarrow x \bmod n = y \bmod n$

Vektorräume, Matrizen und Polynome

Defintion Vektorraums

Sei $(V, \oplus, 0_V)$ eine komm. Gruppe und $(\mathbb{K}, +, \cdot, 0, 1)$ ein Körper mit $\substack{*:\mathbb{K}\times V\to V \\ (\lambda,v)\to\lambda * v}$

$\mathbb{K}$-Vektorraum $(V, \oplus, 0_V, *)$

Vektoren $v \in V, v = (v_1, \ldots, v_n)$

Linearkombination $lin(v_1, \ldots, v_k) = \sum_{i=1}^{k} \lambda_i v_i$ — $\lambda_i, \ldots, \lambda_k \in \mathbb{K}, v_1, \ldots, v_k \in V$

Matrix $A = \begin{pmatrix} A_{11} & A_{12} & \ldots & A_{1n} \\ A_{21} & A_{22} & \ldots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \ldots & A_{mn} \end{pmatrix} \in \mathbb{K}^{m,n}$ — $A = (A_{ij})_{\substack{i=1,\ldots,m, \\ j=1,\ldots,n}}$

Einheitsmatrix $E = (E_{ij}), E_{ij} = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases}$ — Auch kanonische Basis

Inverse Matrix $AA^{-1} = E = A^{-1}A$ — A ist invertierbar

Matrixaddition $A + B = (A_{ij} + B_{ij})_{\substack{i=1,\ldots,m, \\ j=1,\ldots,n}}$

Skalarmultiplikation $\lambda * A = (\lambda * A_{ij})_{\substack{i=1,\ldots,m, \\ j=1,\ldots,n}}$

Matrixmultiplikation $AB = C, C_{ij} = \sum_{i=1}^{m} A_{im} \cdot B_{mj}$ — $A \in \mathbb{K}^{l,\mathbf{m}}, B \in \mathbb{K}^{\mathbf{m},n} \Rightarrow C \in \mathbb{K}^{l,n}$

Transposition $A^T = (A_{ji})_{\substack{i=1,\ldots,m, \\ j=1,\ldots,n}}$ — $A \in \mathbb{K}^{m,n} \Rightarrow A^T \in \mathbb{K}^{n,m}$

Polynome

Variablen $\overset{1}{x^0}, \overset{x}{x^1}, \ldots, x^m$

Monom $x^j, j = 0, \ldots, m$

Polynom $f(x) = \sum_{i=0}^{k} f_i x^i = f_0 + f_1 x + f_2 x^2 + \ldots + f_m x^m$ — $f_i \in \mathbb{K}$

Grad $deg(f) = m$ falls $f_m \neq 0, deg(f) + deg(g) = deg(fg)$

Leitkoeffizient f_m — $Lc(f)$

Leitmonom x^m — $Lm(f)$

Leitterm $f_m x^m$ — $Lt(f)$

Polynom-division

Data: $f(x), g(x), g(x) \neq 0$
Result: $q(x), r(x) : f(x) = q(x)g(x) + r(x)$
$q(x) \leftarrow 0$
$r(x) \leftarrow f(x)$
while $deg(r) > deg(g)$ **do**
  $h(x) \leftarrow \frac{Lc(r)}{Lc(g)} \cdot x^{deg(r)-deg(g)} // (h(x) = \frac{Lt(r)}{Lt(f)})$
  $q(x) \leftarrow q(x) + h(x)$
  $s(x) \leftarrow r(x) - h(x)g(x)$
  $r(x) \leftarrow s(x)$
end

Algorithm 4: Polynomdivision

Data: $f(x) = \sum_{i=0}^{k} f_i x^i$
Result: $f(\alpha)$
$\lambda \leftarrow f_k$
$l \leftarrow 0$
while $l < k$ **do**
  $l \leftarrow l + 1$
  $\lambda \leftarrow \lambda \cdot \alpha + f_{k-l}$
end

Algorithm 5: Hornerschema

Lineares Gleichungssysteme

Gleichungssystem
$$\begin{array}{ccccccccc} A_{11}x_1 & + & A_{12}x_2 & + & \dots & + & A_{1n}x_n & = & b_1 \\ A_{21}x_1 & + & A_{22}x_2 & + & \dots & + & A_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ A_{m1}x_1 & + & A_{m2}x_2 & + & \dots & + & A_{mn}x_n & = & b_m \end{array}$$

Zeile mit Index i $A_{i1}x_1 + A_{i2}x_2 + \ldots + A_{in}x_n = b_i$

Elementaroperation I $\underbrace{A_{i1}x_i + A_{i2}x_2 + \ldots + A_{in}x_n = b_i}_{\cdot\lambda\in\mathbb{K},\lambda\neq 0}$

$\lambda \cdot (A_{i1}x_i + A_{i2}x_2 + \ldots + A_{in}x_n = b_i)$

II $\underbrace{A_{i1}x_i + A_{i2}x_2 + \ldots + A_{in}x_n = b_i}_{+\text{ zeile } j(\cdot\lambda,\lambda\in\mathbb{K})}$

$(\lambda\cdot)(A_{i1}x_i + +A_{i2}x_2 + \ldots + A_{in}x_n + A_{jn}x_n = b_i + b_j\lambda)$

III

Lösungsmenge $\mathbb{L}_{A,b} := \{v \mid v \in \mathbb{K}^n : Av = b\}$

Homogene Lösungsraum $\mathbb{L}_{A,0} := \{v \mid v \in \mathbb{K}^n : Av = 0\}$

Eigenvektor $v \in \mathbb{K}^n : v \neq 0_{\mathbb{K}^n}$ falls $\exists\lambda \in \mathbb{K} : Av = \lambda v (\Leftrightarrow Av - \lambda Ev = 0)$

Eigenwert Der λ von hier oben

Eigenraum $E_\lambda(A) := \{v \mid v \in \mathbb{K}^n : Av = \lambda v\}$ (λ EW von A)