Inhaltsverzeichnis

Komplexe Zahlen

Konstellation von $\mathbb{C}$:

$R^2 = \{(a,b)|a,b \in \mathbb{R}\}$

$(0,1)^2 = -1$

"imaginäre Einheit:"

$(0,1) = i$

Andere Notation:

$(a,b) \in R^2 = (a,0) + (0,b) = (a,0) + (0,1) \cdot (b,0) = a + i \cdot b$

$\mathbb{C} = \{a + ib|a,b \in \mathbb{R}\}$

Addition:

$(a + ib) + (c + id) = (a + c) + i(b + d)$

Multiplikation:

$(a + ib) \cdot (c + id) = ac + i^2bd + i(ad + bc) = ac - bd + i(ad + bc)$

Begriffe:

$Z = a + ib \in \mathbb{C}$, $a,b \in \mathbb{R}$

$a = Re(\mathbb{Z})$

$b = Im(\mathbb{Z})$

wenn $a = 0 \rightarrow Z$ rein imaginär

$Z = a + ib \rightarrow \overline{Z} = a - ib$

$\overline{Z}$ ist die zu Z konjugierte komplexe Zahl

Nützliches:

$Z \cdot \overline{Z} = (a + ib) \cdot (a - ib) = a^2 + b^2$

$|Z| = \sqrt[2]{a^2 + b^2}$

$\overline{Z + W} = \overline{Z} + \overline{W}$

$\overline{Z \cdot W} = \overline{Z} \cdot \overline{W}$

$Re(Z) = \frac{1}{2}(Z + \overline{Z})$

$Im(Z) = \frac{1}{2i}(Z - \overline{Z})$

Dreiecksgleichung:

$Z, W \in \mathbb{C} \Rightarrow |Z + W| \leq |Z| + |W|$

Invertieren: (komplexe Zahl aus Nenner raus bekommen)

$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{ac+bd+i(cb-ad)}{c^2+d^2}$

Polarkoordinaten

Form: $Z = r(\cos\varphi + i\sin\varphi)$

mit Radius $r \in \mathbb{R}$ und Winkel $\varphi \in\,]-\pi, \pi]$

Umrechnung:

- $Z = a + ib$

1. $r = \sqrt{a^2 + b^2}$
2. $\varphi = \begin{cases} \arccos\frac{a}{r}, b \geq 0 \\ -\arccos\frac{a}{r}, b < 0 \end{cases}$
3. $Z = r \cdot (\cos\varphi + i\sin\varphi)$

- $cos\varphi = \frac{a}{r}$
- $sin\varphi = \frac{b}{r}$

Multiplikation:

$Z_1 = r_1(\cos(\varphi_1) + i\sin(\varphi_1))$

$Z_2 = r_2(\cos(\varphi_2) + i\sin(\varphi_2))$

$Z_1 \cdot Z_2 = r_1 \cdot r_2 \cdot (\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$

Potenzen:

$Z = r \cdot (\cos(\varphi) + i\sin(\varphi))$

$Z^n = r^n \cdot (\cos(n \cdot \varphi) + i\sin(n \cdot \varphi))$

Wurzeln:

$\sqrt[n]{Z}$ hat genau n Lösungen

$Z_k = \sqrt[n]{r} \cdot (\cos\frac{\varphi+2\pi\cdot k}{n} + i\sin\frac{\varphi+2\pi\cdot k}{n})$

mit $n =$ “Wurzelexponent”,

$r =$ “Radius”,

$k =$ “k-te Lösung der Wurzel von 0 bis $n-1$

Lineare Gleichungssysteme

Vereinfachte Schreibweise als Matrix:

$$\overbrace{\begin{matrix} a_{11}x_1 & + & \cdots & + & a_{1n}x_1 & = & b_1 \\ \vdots & + & \ddots & + & \vdots & = & \vdots \\ a_{m1}x_n & + & \cdots & + & a_{mn}x_n & = & b_m \end{matrix}}^{linearesGleichungssystem\ LGS} \Rightarrow \underbrace{\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)}_{(A|b)} \Rightarrow \cdots$$

$$\cdots \Rightarrow \left(\begin{array}{cccc|c} * & \cdots & \cdots & * & * \\ 0 & * & \cdots & * & \vdots \\ \vdots & 0 & * & * & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \star \end{array}\right) \Rightarrow \cdots \Rightarrow \overbrace{\left(\begin{array}{ccccc|c} 1 & * & \cdots & * & * \\ 0 & 1 & * & * & * \\ 0 & 0 & 1 & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{array}\right)}^{reduzierteZeilenstufenform}$$

$*$: unbekannter Wert

$*$: 0

$\star$: wenn $\neq 0$ gibt es keine Lösung

Umformen in ZNF:

$$\text{Elementare Zeilenumformungen} \begin{cases} \text{Vertauschen zweier Zeilen} \\ \text{Multiplikation einer Zeile mit } \lambda \neq 0 \\ \text{Addition des } \lambda\text{-fachen eines Zeile zu einer anderen} \end{cases}$$

Rang einer Matrix

Matrix M auf ZSF bringen

$\Rightarrow$ Anzahl an nicht null Zeilen = Rang von $M = rg(M)$

Das Kriterium für Lösbarkeit:

- Das System ist genau dann lösbar, wenn: $rg(A) = rg(A|b)$
- ist das LGS lösbar, so gilt: Anzahl frei wählbaren Vraiablen $= n - r$

$n =$ Anzahl der variablen und $r = rg(A)$

- ist das System (A|b) lösbar, so gilt: $\exists_1$ lsg $\Leftrightarrow n = r$

Matrix

$$A = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1a} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{ma} \end{pmatrix}}_{n \text{ Spalten}} \left.\vphantom{\begin{pmatrix} a \\ \vdots \\ a \end{pmatrix}}\right\} m \text{ Zeilen}$$

Stelle (i, j) : i-te Zeile | j-te Spalte

$$\underbrace{\begin{matrix} \mathbb{R}^{m\times n} & = \{(a_{ij})_{m,n} | a_{ij} \in \mathbb{R}\} \Rightarrow & \text{"reelle Matrix"} \\ \mathbb{C}^{m\times n} & = \{(a_{ij})_{m,n} | a_{ij} \in \mathbb{C}\} \Rightarrow & \text{"komplexe Matrix"} \end{matrix}}_{\Rightarrow K(körper)^{m\times n} = \{(a_{ij})_{m,n} | a_{ij} \in K\}}$$

$A = B \Leftrightarrow$ gleich viele Spalten UND gleich viele Zeilen UND gleiche Einträge an den gleichen Stellen

Besondere Matrizen

- $m \times 1 : \text{S} = \begin{pmatrix} S1 \\ \vdots \\ S_m \end{pmatrix}$ Spaltenvektor
- $1 \times n : Z = \begin{pmatrix} Z1 & \cdots & Z_n \end{pmatrix}$ Zeilenvektor
- $m \times n : 0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ Nullmatrix
- $m = n$: <u>quadratische Matrix</u>

Diagonalmatrix: $diag(\lambda_1 \dots \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$

$$\text{Einheitsmatrix: } E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

$$\text{Obere } \Delta\text{-Matrix: } O = \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix}$$

$$\text{Untere } \Delta\text{-Matrix: } U = \begin{pmatrix} * & 0 & \cdots & 0 \\ * & * & \ddots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ * & * & \cdots & * \end{pmatrix}$$

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in K^{m \times n} = \begin{pmatrix} \overrightarrow{S_1}, & \cdots & \overrightarrow{S_n} \end{pmatrix} = \begin{pmatrix} Z_1 \\ \vdots \\ Z_m \end{pmatrix}$$

Rechenoperationen

<u>Transponieren:</u>

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}$$

Symmetrische Matrix: $A^T = A$

<u>Addieren:</u>

$A = (a_{ij})_{m,n}$, $B = (b_{ij})_{m,n}$

$A + B = (a_{ij} + b_{ij})_{m,n}$

$A = (a_{ij}) = -(-a_{ij}) = -(-A)$

<u>Skalare Multiplikation (Vervielfachen:)</u>

$A = (a_{ij})_{m,n} \in \mathbb{K}^{m \times n}$

$\lambda \in \mathbb{K}$

$\Rightarrow \lambda A = (\lambda a_{ij})$

<u>Multiplikation:</u>

$$Z = (Z_1, \cdots, Z_n) \quad , \quad S = \begin{pmatrix} S_1 \\ \vdots \\ S_n \end{pmatrix}$$

$Z \cdot S = \sum_{i=1}^{n} Z_i S_i$

$$\Downarrow$$

$$A = \begin{pmatrix} Z_1 \\ \vdots \\ Z_m \end{pmatrix} \in \mathbb{K}^{m \times n} \quad , \quad B = \begin{pmatrix} S_1 & \cdots & S_p \end{pmatrix} \in \mathbb{K}^{n \times p}$$

$$A \cdot B := \begin{pmatrix} Z_1 \cdot S_1 & Z_1 \cdot S_2 & \cdots & Z_1 S_p \\ Z_2 \cdot S_1 & Z_2 \cdot S_2 & \cdots & Z_2 S_p \\ \vdots & \vdots & \ddots & \vdots \\ Z_m \cdot S_1 & Z_m \cdot S_2 & \cdots & Z_m \cdot S_p \end{pmatrix} \in K^{m \times p}$$

$A \cdot B \neq B \cdot A \leftarrow$ keine Kommutativität

$A^k = \underbrace{A \cdot A \cdots A}_{k}$

$A^0 := E_n$

<u>Invertieren:</u>

$A \in K^{n \times n} \quad , \quad B = A^{-1}$

$A \cdot B = E_n = B \cdot A$

Nicht jede Matrix invertierbar!

$$B = \begin{pmatrix} \vec{S_1} & \dots & \vec{S_n} \end{pmatrix} \quad , \quad e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

$$A \cdot B = A \cdot \begin{pmatrix} \vec{S_1} & \dots & \vec{S_n} \end{pmatrix} = \begin{pmatrix} A\vec{S_1} \cdots A\vec{S_n} S_n \end{pmatrix} = \begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} = E_n$$

löse so:

$$(A|E_n) \Rightarrow \cdots \text{el. ZUF} \cdots \Rightarrow (E_n|A^{-1})$$

Elementarmartizen

Permutationsmatrizen (Vertauschen von Zeilen):

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}$$
$$P \cdot A = \begin{pmatrix} 1 & 1 & 1 \\ 3 & 3 & 3 \\ 2 & 2 & 2 \end{pmatrix}$$
$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Multiplikation einer Zeile mit $\lambda \neq 0$:

$$D_k(\lambda) = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & 1 & 0 & 0 & \ddots & 0 \\ 0 & \ddots & 0 & \lambda & 0 & \ddots & 0 \\ 0 & \ddots & 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \leftarrow k$$

Addition des λ-fachen der l-ten Zeile zur k-ten Zeile:

$$N_{kl}(\lambda) = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \lambda & \vdots \\ 0 & \ddots & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \leftarrow \lambda \text{ an der } k\text{-ten Zeile und } l\text{-ten Spalte}$$

Rechenregeln Matrizen

Addition:

$A + B = B + A$	Kommutativität
$(A + B) + C = (A + B) + C$	Assoziativität
$(\mu \cdot \lambda)A = \mu(\lambda \cdot A)$	
$0 + A = A = A = 0$	Neutrales Element
$E_n A = A$	
$\forall A \exists B : A + B = 0$	Inverses Element
$B = -A$	
$\lambda(A + B) = \lambda A + \lambda B$	Distributivität

Transposition:

$(A + B)^T = A^T + B^T$	Summe
$(\lambda A)^T = \lambda A^T$	Skalarmultiplikation
$(A^T)^T = A$	Zweifache Transposition
$(AB)^T = B^T A^T$	Produkt
$(A^{-1})^T = (A^T)^{-1}$	Inverses

Multiplikation:

$\exists A, B : AB \neq BA$	nicht kommutativ!
$(AB)C = A(BC)$	Assoziativität
$\exists E \in E_n : EA = A$	Neutrales Element
$A(B + C) = AB + AC$	Distributivität
$(B + C)A = BA + CA$	
$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$	Inverses

Gruppen

G nichtleere Menge mit innerer Verknüpfung $\cdot$

$\cdot : G \times G \to G$

$(G, \cdot)$ heißt Gruppe, wenn:

$$\left.\begin{array}{r} \forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c) \\ \exists e \in G : e \cdot a = a = a \cdot e \quad \forall a \in G \\ \forall a \in G \exists b \in G : a \cdot b = e = b \cdot a \end{array} \right\| \begin{array}{l} \text{Assoziativgesetz} \\ \text{neutrales Element} \\ \text{inverses Element} \end{array}$$

G nennt man abelsch (=kommutativ) falls:

- $ab = ba \quad \forall a, b \in G$

Untergruppen

$(G, \cdot)$ sei eine Gruppe mit neutralem Element e

$U \subseteq G$ mit:

$$\left.\left.\begin{array}{r} e \in U \\ u, v \in U \Rightarrow u \cdot v \in U \\ u \in U \Rightarrow u^{-1} \in U \end{array} \right\| \begin{array}{l} \text{neutrales Element} \\ \text{abgeschlossen} \\ \text{inverses Element} \end{array} \right\} \Rightarrow \begin{cases} U \text{ ist Untergruppe} \\ U \leq G \end{cases}$$

Von Elementen erzeugten Untergruppen

$\langle a \rangle = \{a^k \,|\, a \in G,\, k \in \mathbb{Z}\}$

- $e \in \langle a \rangle$
- $a^k, a^l \in \langle a \rangle \Rightarrow a^k \cdot a^l = a^{k+l} \in \langle a \rangle$
- $a^k a^{-k} = a^0 = e$

Ordnung eines Elements

$(G, \cdot)$ Gruppe $\rightarrow a \in G$

$\rightarrow O(a) = |\langle a \rangle| = \begin{cases} n \in \mathbb{N}, & \# \{a^k \,|\, k \in \mathbb{Z}\} \\ \infty, & sonst. \end{cases}$

$O(a) =$ kleinste Zahl n mit $a^n = e$

$\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$

$O(a) = n$

Satz über die Ordnung von Gruppenelementen:

Es sei G eine Gruppe mit neutralem Element e, und es sei $a \in G$:

(a) Falls $O(a) = \infty$, dann: $a^i \neq a^j \;\; , \; i \neq j$.

(b) Falls $O(a) \in \mathbb{N}$, so gilt: $O(a) = u =$ kleinste natürliche Zahl, für die $a^n = e$ gilt.

$a^s = e \Leftrightarrow O(a) \Big| s$

Sätze von Lagrange und Euler

Satz von Lagrange:

G sei eine endliche Gruppe, $U \leq G$

Dann:

$$|U| \Big| |G|$$

Satz von Euler:

$$a^{|G|} = e \quad \forall a \in G$$

Die Restklassen modulo n:

Gegeben: $n \in \mathbb{N}$

Betrachte: wähle $a \in \mathbb{Z}$

$$\overline{a} = \{a + nz \,|\, z \in \mathbb{Z}\}$$

Wir schließen $a, b \in \mathbb{Z}$:

$a \equiv b(mod \;\; n)$, falls a, b den gleichen Rest bei Div durch n haben:

Es gilt:

$$\left. \begin{array}{l} a = qn + r \\ b = \tilde{q}n + r \end{array} \right\} \Leftrightarrow \begin{cases} a - b & = (q - \tilde{q})n \\ & \Leftrightarrow n|(a-b) \\ & \Leftrightarrow a + n\mathbb{Z} = b + n\mathbb{Z} \\ & \Leftrightarrow \overline{a} = \overline{b} \end{cases}$$

Menge der Restklassen $\rightarrow \mathbb{Z} \Big| n\mathbb{Z} = \mathbb{Z} \Big| n = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

$|\mathbb{Z}_n| = n$

Addition:

$\overline{k}, \overline{l} \in \mathbb{Z}$

$\rightarrow \overline{k} = \overline{l} = \overline{k + l}$

Ringe

Eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$ heißt ein Ring falls gilt:

- $(R, +)$ ist abelsche Gruppe
- $\cdot$ ist assoziativ
- Distributivgesätze $a(b+c) = ab + ac$ und $(a+b)c = ac + bc \forall a, b, c \in R$
- $\exists$ Einselement: $1 \in R$: $1 \cdot a = a = a \cdot 1 \quad \forall a \in R$

Einheitengruppe (= Gruppe der invertierbaren Elemente)

Gegeben: Ring $(R, +, \cdot)$

$R^\times = \{a \in R \,|\, a \text{ ist invertierbar}\} = \{a \in R \,|\, \exists b \in R : ab = 1 = ba\}$

$R^\times$ ist die Einheitengruppe von R

Prime Restklassengruppen

$$\begin{aligned} n \in \mathbb{N} \to \mathbb{Z}_n^\times &= \{\overline{a} \text{ ist invertierbar}\} \\ &= \{\overline{a} \in \mathbb{Z}_n \,\big|\, \exists j \in \mathbb{Z}_n : \overline{a}j = 1\} \\ &= \{\overline{a} \in \mathbb{Z}_n \mid ggt(a, n) = 1\} \end{aligned}$$

$$a, b \text{ sind relativ prim/teilerfremd} \Leftrightarrow ggT(a, b) = 1$$

$(\mathbb{Z}_n, +, \cdot)$ ist körper $\Leftrightarrow n \in (\mathbb{P})$

$$\begin{array}{lll} \overline{a} \text{ invertierbar} & \Leftrightarrow \exists \overline{b} \in \mathbb{Z}_n & : \overline{a}\overline{b} = \overline{1} \\ & \Leftrightarrow \exists b \in \mathbb{Z} & : (a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z} \\ & \Leftrightarrow \exists b \in \mathbb{Z} & : n \big| ab - 1 \\ & \Leftrightarrow \exists b \in \mathbb{Z} \; \exists x \in \mathbb{Z} & : ab - 1 = nx \\ & \Leftrightarrow \exists b \in \mathbb{Z} \; \exists x \in \mathbb{Z} & : ab - nx = 1 \\ & \Rightarrow & ggT(a, n) = 1 \end{array}$$

Euklidischer Algorithmus

$a_1 = a, \; a_2 = b \mid b > 0$

Sukzessive Division mit Rest:

$$\begin{array}{rcccccl} a_1 & = & q_1 a_2 & + & a_3 & , & 0 < a_3 < a_2 \\ a_2 & = & q_2 a_3 & + & a_4 & , & 0 < a_4 < a_3 \\ \vdots & = & \vdots & + & \vdots & & \vdots \\ a_{n-2} & = & q_{n-2} a_{n-1} & + & a_n & , & 0 < a_n < a_{n-1} \\ a_{n-1} & = & q_{n-1} a_n & + & 0 & \nwarrow & \underline{a_n = ggT(a_1, a_2)} \end{array}$$

$\exists r, s \in \mathbb{Z} : ra + sb = a_n \quad \Leftarrow$ erweiterter euklidischer Algorithmus

Erweiterte Euklidischer Algorithmus

Der Erweiterte Euklidischer Algorithmus findet zwei weitere Zahlen $s, t \in R$ die eine Linearkombination bilden, die folgende Gleichung erfüllt:

$$s \cdot a + t \cdot b = \text{ggT}(a, b)$$

Berechnung

Bei dem Erweiterten Euklidischen Algorithmus wird die bisherige Folge r_x um drei weitere (q_x, s_x, t_x) erweitert, welche mit der folgenden Formeln bestimmt werden

$$q_{x+1} := \left\lfloor \frac{r_{x-1}}{r_x} \right\rfloor$$

$$r_{x+1} := \begin{cases} a & \text{wenn } x = 0, \\ b & \text{wenn } x = 1 \\ r_{x-1} - q_x \cdot r_x & \end{cases}$$

$$s_{x+1} := \begin{cases} 1 & \text{wenn } x = 0, \\ 0 & \text{wenn } x = 1 \\ s_{x-1} - q_x \cdot s_x & \end{cases} \longrightarrow \begin{aligned} \text{ggT}(a, b) &= r_n \\ &= s_n \cdot a + t_n \cdot b \end{aligned} \quad \text{mit } r_{n+1} = 0$$

$$t_{x+1} := \begin{cases} 0 & \text{wenn } x = 0, \\ 1 & \text{wenn } x = 1 \\ t_{x-1} - q_x \cdot t_x & \end{cases}$$

Eulersche φ-Funktion:

Man nennt $\varphi(n) = \#\{a \in \{1, \ldots, n\} \mid ggT(a, n) = 1\}$

$\varphi(n) = \left|\mathbb{Z}_n^\times\right|$

$\varphi(p) = p - 1 \quad \forall p \in \mathbb{P}$

kleiner Satz von Fermat

Es sei $p \in \mathbb{P}$ dann gilt: $\forall a \in \mathbb{Z} : a^p \equiv a(mod\ p)$

Das Pohlig Hellman Verfahren

$$\underline{p = \text{(große) Primzahl} \;\|\; \mathcal{N} = \text{ Klartext} \mid \mathcal{N} \in \mathbb{Z}_p^\times \;\|\; e, d = \text{ Schlüssel}}$$

Wähle $e \in \mathbb{N}$ mit $ggT(e, p-1) = 1$

Bestimme d mit:

$$\begin{aligned} ed &\equiv 1(mod\ p-1) \\ ed &= 1 + r(p-1) \\ 1 &= ed - r(p-1) \end{aligned}$$

$$\Rightarrow \text{euklidischer Algorithmus}$$

Verschlüsseln:

$$\mathcal{C} = \mathcal{N}^e$$

Entschlüsseln:

$$\mathcal{C}^d = (\mathcal{N}^e)^d = \mathcal{N}^{ed} = \mathcal{N}^{1+r(p-1)} = \mathcal{N}^1 \cdot (\mathcal{N}^{(p-1)})^r \overset{\text{Satz von Euler - Fermat}}{=} N$$

Wähle p am besten mit $\frac{p-1}{2}$ auch prim $\leftarrow$ sichere Primzahl

RSA-Verfahren:

Vorbereitung des Empfängers (Erzeugers der Schlüssel):

1. wähle große $p, q \in \mathbb{P} \ : \ p \neq q$ und $p \pm 1, q \pm 1$ müssen große Primteiler haben
2. setze $n = p \cdot q$
3. $\left|\mathbb{Z}_n^\times\right| = \left|\{a \in \{1, \ldots, n\} \mid ggT(a, n) = 1\}\right| = \varphi(n) = \varphi(p \cdot q) = (p-1)(q-1)$
4. wähle $e \in \{1, \ldots, n\} \ : \ ggT(e, \varphi(n)) = 1$
5. berechne $d \ : \ e \cdot d \equiv 1(mod \ \varphi(n))$
6. veröffentliche Schlüssel (n, e)

Verschlüsselung des Senders:

$$\mathcal{C} \equiv \mathcal{N}^e \ (mod \ n)$$

Entschlüsselung des Empfängers:

$$\mathcal{N} \equiv \mathcal{C}^d \ (mod \ n)$$

Vektorräume

Körper

Ein Ring K $(K, +, \cdot)$ mit:

1. K ist kommutativ
2. $\exists$ Einselement $1 \ : \ 1 \cdot \lambda = \lambda = \lambda \cdot 1 \quad \forall \lambda \in K$
3. Jedes $\lambda \neq 0$ ist invertierbar $\Leftrightarrow \ K^\times = K \setminus \{0\}$

V heißt ein K-Vektorraum falls $\forall \lambda, \mu \in K \ , \ \forall u, v, w \in V \ :$

$$\left.\begin{array}{l} 1.\ v + w \in V \ , \ \lambda \cdot v \in V \\ 2.\ u + (v + w) = (u + v) + w \\ 3.\ \exists 0 \in V \ : \ 0 + v = v \\ 4.\ \exists v' \in V \ : \ v + v' = 0 \\ 5.\ u + v = v + u \end{array}\right\} (V, +) \ : \ \text{abelsche Gruppe}$$

$$\left.\begin{array}{l} 6.\ \lambda(u + v) = \lambda u + \lambda v \\ 7.\ (\lambda + \mu)v = \lambda v + \mu v \\ 8.\ (\lambda\mu)v = \lambda(\mu v) \\ 9.\ 1v = v \end{array}\right\} \quad \text{Verträglichkeitsgesetze}$$

Sprechweisen und Regeln

Vektor: Element eines Vektorraumes

Nullvektor: 0-Element des Vektorraumes

Entgegengesetzte Vektoren (Negative): $-v \quad \to w + (-v) = w - v$

$K = \mathbb{R}$: reeller Vektorraum

$K = \mathbb{C}$: komplexer Vektorraum

$\lambda \in K$: Skalare

3 Regeln:

$0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v \ \Big| - (0v)$

$0 = 0 \cdot v$

$\lambda \cdot 0 = \lambda(0+0) = \lambda \cdot 0 + \lambda \cdot 0$

$0 = \lambda \cdot 0$

$\lambda \cdot v = 0 \iff \lambda = 0 \vee v = 0$

Untervektorräume

V sei ein K-Vektorraum

$U \subseteq$ heißt Untervektorraum, falls U wieder ein K-Vektorraum ist

d.h.

- $0 \in U$
- $u, v \in U \Rightarrow u + v \in U$
- $\lambda \in K, u \in U \Rightarrow \lambda u \in U$

Linearkombinationen

$v_1, \ldots, v_n \in V$, $\lambda_1, \ldots, \lambda_n \in K$

wenn gilt:

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n = \sum_{i=1}^{n} \lambda_i v_i \in V$$

ist v eine Linearkombination von $v_1, \ldots, v_n$

Das Erzeugnis von X

Geg.: V : K-Vektorraum $\quad x \subseteq V$

$$\begin{aligned} Setze: \langle X \rangle &= lin(X) = span(X) \\ &= \left\{ \sum_{i=1}^{n} \lambda_i v_i \;\middle|\; \lambda_i \in K,\ v_i \in X,\ n \in \mathbb{N} \right\} \\ &= Kv_1 + \ldots + Kv_n \\ &= \text{Menge aller endlichen Linearkombinationen von Elementen aus } X \\ &= \text{Erzeugnis von } X \\ &= \text{lineare Hülle von } X \end{aligned}$$

- $\langle X \rangle \leq V \ \leftrightarrow \ \langle X \rangle$ ist ein Untervektorraum von V

Definition:

$X = \emptyset \rightarrow \langle \emptyset \rangle = \{0\}$

Lineare Unabhängigkeit:

Geg.: K-Vektorraum V

$v_1, \ldots, v_n \in V$ heißen linear unabhängig, falls:

$\forall T \subsetneq \{v_1, \ldots, v_n\} \ \Rightarrow \ \langle T \rangle \subsetneq \langle v_1, \ldots, v_n \rangle \leftarrow$ "keins unnötig"

Das Kriterium für lineare Unabhängigkeit:

Gegeben: $v_1, \ldots, v_n \in V$, $0_v \in V$

Ansatz:

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0_v$$

Falls:

$$\exists_1 \text{Lsg.} \ \Rightarrow v_1, \ldots, v_n \text{ linear unabhängig}$$

Basen von Vektorräumen

Ist V ein K-Vektorraum, so nennt man $B \leq V$ eine Basis von V, falls:

- B linear unabhängig
- B erzeugt V

Merkregeln

- Jeder K-Vektorraum hat eine Basis
- $\begin{aligned} B \leq V \text{ ist eine Basis von } V \quad &\Leftrightarrow B \text{ ist eine maixmal-linear-unabhängige Teilmenge von } V \\ &\Leftrightarrow B \text{ ist minimales Erzeugendensystem von } V \end{aligned}$
- Jede linear unabhängige Menge von V kann man zu einer Basis ergänzen
- Jedes Erzeugendensystem von V kann zu einer Basis verkürzt werden
- Ist B eine Basis von V, so kann jedes $v \in V$ als genau eine Weise bzgl. B dargestellt werden:

$$v = \lambda_1 b_1 + \ldots + \lambda_n b_n$$

- Je zwei Basen von V haben die gleiche Mächtigkeit : B_1, B_2 Basen von $V \Rightarrow |B_1| = |B_2|$

- Die Dimension eines Vektorraumes V:

Wähle Basis B von V

$$dim(V) = |B| = \begin{cases} n \\ \infty \end{cases}$$

- Ist V ein Vektorraum der Dimension n: $dim(V) = n$:

Dann:

- Jede linear unabhängige Menge mit n Elementen ist eine Basis
- Jedes Erzeugendensystem mit n Elementen ist eine Basis
- Mehr als n Vektoren sind immer linear abhängig

- $U \leq V \Rightarrow dim(U) \leq dim(V)$
- $U \leq V \wedge dim(U) = dim(V) \Rightarrow U = V$
- $dim(\mathbb{R}[x]_n) = n + 1$

Anwendung in Linearen Gleichungssystemen

$$A \in K^{m \times n} = (a(ij)) = \begin{pmatrix} s_1 & \ldots & s_n \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix}$$

$$\begin{array}{r|l} S_A = \langle s_1, \ldots, s_n \rangle = \text{Spaltenraum von } A & Z_A = \langle z_1, \ldots, z_m \rangle = \text{Zeilenraum von } A \\ dim(S_A) = \text{Spaltenrang von } A & dim(Z_A) = \text{Zeilenrang von } A \end{array}$$

$rg(A) =$ Zeilenrang $=$ Spaltenrang $\forall A \in K^{m \times n}$

Spaltenraum

$A = \begin{pmatrix} s_1 & \dots & s_n \end{pmatrix} \in K^{m\times n}$

$$\begin{aligned} \langle s_1,\dots,s_n\rangle &= \left\{ \sum_{i=1}^n \lambda_i s_i \;\middle|\; \lambda_i \in K \right\} \\ &= \left\{ \begin{pmatrix} s_1 & \dots & s_n \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \;\middle|\; \lambda_1,\dots,\lambda_n \in K \right\} \\ &= \{A\cdot x \mid x \in K^n\} \end{aligned}$$

$Ax = 0$: $(A|0) \to ZSF$

$$\left. \begin{matrix} \text{Lösungsraum von } A\cdot x = 0 \\ Kern(A) \\ ker(A) \end{matrix} \right\} \leq K^n$$

$$dim(Kern(A)) = n - rg(A)$$

Lineare codes

datenübertragung: Bits $\to x_1, x_2, x_3, \dots$

Strom von Bits über gestörten Kanal

$p \approx 10^{-6}$ falsches Bit wird übertragen

$$G = \text{Generatormatrix}$$

$$G = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \\ \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \end{pmatrix} \Bigg| \text{ Wiederholungsmatrix}$$

$$G = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 1 \\ \\ 1 & 1 & \cdots & 1 \end{pmatrix} \Bigg| \text{ Parity-Check Matrix}$$

Die Menge $C := \left\{ G \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \middle| \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \in K^k \right\} \leq K$

heißt (n,k)-Code:

$$\begin{aligned} n &= \text{Länge} \\ n-k &= \text{Redundanz} \\ \\ dim(C) &= k \\ \frac{k}{n} &= \text{Informationsrate} \\ rg(G) &= k \end{aligned}$$

Wie läuft das Dekodieren ab?

1. Fall $c' \in C$:

$$\text{Dekodiere} : G \cdot x = c' \quad \Rightarrow \quad x \in k^k$$

2. Fall: $c' \notin C$:

$$\text{Suche } c'' \text{, das sich von } c' \text{ möglichst wenig unterscheidet:}$$

$$\begin{array}{c|c} \exists_1 c'' & \exists c''_1, \ldots c''_n \ : \ c''_1, \ldots, c''_n \text{ paarweise disjunkt} \\ \text{nächstes } c' \text{ an } c'' \text{wählen und wie in Fall 1 dekodieren} & \text{Nachricht neu senden lassen} \end{array}$$

Hamming Gewicht und Abstand

Für $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in K^n$ ist das <u>Hamming-Gewicht:</u>

$$w(c) = \left| \left\{ i \in \{1, \ldots, n\} \middle| c_i \neq 0 \right\} \right|$$

Für $c, c' \in K^n$ ist der <u>Hamming-Abstand:</u>

$$d(c,c') = w(c-c') = \left| \left\{ i \in \{a, \ldots, n\} \middle| c_i \neq c'_i \right\} \right.$$

Für $C \subseteq K^n$ gilt:

$$\begin{array}{rclcl} d(C) & = & min\Big\{ d(c,c') & \Big| & c, c' \in C, \ c \neq c' \Big\} \\ d(C) & = & min\Big\{ w(c) & \Big| & c \in C \setminus \{0\} \Big\} \end{array}$$

Lineare Codes (Fortsetzung)

$d(c,c'') \leq d(c,c') + d(c',c'')$

Es sei $C \in K^n$ ein Code:

$$\begin{array}{r|l} d(C) = 2e+1 & d(C) = 2e+2 \\ & \\ C \text{ ist } e\text{-fehlerkorrigierend} & C \text{ ist } e\text{-fehlerkorrigierend} \\ & C \text{ ist } (e+1)\text{-fehlererkennend} \end{array}$$

Die Kontrollmatrix (Parity Check Matrix)

$G = \begin{pmatrix} E_k \\ A \end{pmatrix} \in K^{n \times k}$

$P = \begin{pmatrix} -A & E_{n-k} \end{pmatrix} \in K^{(n-1) \times n}$

Es gilt:

$$P \cdot G = 0$$

Damit:

- $Pc = 0 \forall c \in C$
- $dim(C) = dim(\text{Lösungsraum } Px = 0) = n - (n-k) = k$

$$C = \text{"Lösungsmenge } Px = 0\text{"}$$

Vorbereitung auf Determinante

Die symmetrische Gruppe:

Menge aller Permutationen (=Bijektionen) von $\{1, 2, \dots, n\} = I_n$

$S_n = \left\{\sigma : I_n \to I_n \middle| \sigma \text{ bijektiv}\right\}$

$\left|S_n\right| = n!$

Verknüpfung: Komposition (Hintereinanderausführung):

$f \circ g = f(g(x))$

Das Signum (Vorzeichen) einer Permutation:

Wir nennen (j, i) einen Fehlstand der Permutation σ, falls

$$i < j, \text{ aber } \sigma(i) > \sigma(j)$$

Hat σ f Fehlstände, so setze $sgm(\sigma) = (-1)^f$

Es gilt:

$f = \#\text{Fehlstände von } \sigma \leftarrow$ ist ein Homomorphismus:

$sgm(\sigma \circ \tau) = sgm(\sigma) \cdot sgm(\tau) \quad \forall \sigma, \tau \in S_n$

$$\begin{aligned} sgm(\sigma \circ \tau) &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\ &= \underbrace{\prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}}_{sgm(\sigma)} \cdot \underbrace{\prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i}}_{sgm(\tau)} \end{aligned}$$

Die Determinante berechnen:

Für jede quadratische Matrix $A \in K^{n \times n}, K körper$, heißt

$$|A| = det(A) = \sum_{\sigma \in S_n} sgm(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

die Determinante von A (Leibniz'sche Formel).

$$\left(\text{Permanente von } A = per(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}\right)$$

- $\left|diag(\lambda_1, \dots, \lambda_n)\right| = \prod_{i=1}^{n} \lambda_i \leftarrow$ gilt auch für obere- und untere- Δ-Matrizen
- $det(A) = det(A^T) \;\; \forall A \in K^{n \times n}$

- Determinantenmultiplikationssatz:

$$det(A \cdot B) = det(A) \cdot det(B) \;\; \forall A, B \in K^{n \times n}$$

- $det(A^{-1}) = \frac{1}{det(A)}$
- $det(A^k) = det(A)^k$

Laplace'scher Entwicklungssatz:

Vorab:

Streichungsmatrix:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,m} & a_{2,m} & \cdots & a_{n,m} \end{pmatrix} \to \underbrace{A_{1,1} = \begin{pmatrix} a_{2,2} & \cdots & a_{2,n} \\ \vdots & \ddots & \vdots \\ a_{2,m} & \cdots & a_{n,m} \end{pmatrix}}_{A_{i,j} \to \text{Zeile } i \text{ und Spalte } j \text{ weglassen}}$$

$$A = (a_{i,j}) \to det(A) = \begin{cases} \displaystyle\sum_{j=1}^{n} (-1)^{i+j} \cdot a_{i,j} \cdot det(A_{i,j}) & \text{Entwicklung nach } i\text{-ter Zeile} \\ \displaystyle\sum_{i=1}^{n} (-1)^{i+j} \cdot a_{i,j} \cdot det(A_{i,j}) & \text{Entwicklung nach } j\text{-ter Spalte} \end{cases}$$

Determinante und elementare Zeilenumformungen

$P_{i,j}$ = Permutationsmatrix

$$det(P_{i,j} \cdot A) = det(P_{i,j}) \cdot det(A) = -det(A)$$

$D_i(\lambda)$ = Multiplikation einez Zeile mit λ

$$det(D_i(\lambda) \cdot A) = det(D_i(\lambda)) \cdot det(A) = \lambda \cdot det(A)$$

$N_{i,j}(\lambda)$ = Addition des λ-fachen der j-ten Zeile zur i-ten Zeile

$$det(N_{i,j}(\lambda) \cdot A) = det(N_{i,j}(\lambda)) \cdot det(A) = det(A)$$

$det(\lambda \cdot A) = \lambda^n \cdot det(A) \; \forall A \in K^{n \times n}$

Blockdiagonalmatrizen

A, B quadratisch $\to \begin{vmatrix} A & C \\ 0 & B \end{vmatrix} = \begin{vmatrix} A & 0 \\ C & B \end{vmatrix} = |A| \cdot |B|$

$$det(A) \neq 0 \Leftrightarrow A \text{ invertierbar } \forall A \in K^{n \times n}$$

Skalarprodukt

$V \times V \to \mathbb{R}$, V ist ein $\mathbb{R}$-Vektorraum

$\langle \cdot, \cdot \rangle$ heißt Skalarprodukt wenn:

- **Bilinearität:** $\forall v, w, v', w' \in V$, $\forall \lambda \in \mathbb{R}$

$$\langle \lambda v + v', w \rangle = \lambda \langle v, w \rangle + \langle v', w \rangle$$

$$\langle v, \lambda w + w' \rangle = \lambda \langle v, w \rangle + \langle v, w' \rangle$$

- **Symmetrie:** $\forall v, w \in V$

$$\langle v, w \rangle = \langle w, v \rangle$$

- **Positive Definitheit:** $\forall v \in V$

$$\langle v, v \rangle \geq 0$$

$$\langle v, v \rangle = 0 \Leftrightarrow v = 0$$

Wichtige Skalarprodukte

- **kanonisches/standard Skalarprodukt:**

$V = \mathbb{R}^n, v, w \in V$

$$\langle v, w \rangle := v^T w$$

- **Skalarprodukt mit Matrix:** $A = \mathbb{R}^{n \times n}$, $v, w \in \mathbb{R}^n$

$$\langle v, w \rangle_A := v^T A w$$

$n = 2 \Rightarrow A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\langle v, w \rangle_A = a \cdot {v_1}^2 + (b + c) \cdot v_1 \cdot v_2 + d \cdot {v_2}^2$$

- **Polynom Skalarprodukt:** $p, q \in \mathbb{R}[x]$

$$\langle p, q \rangle := \int_a^b p(x) \cdot q(x) dx$$

Begriffe:

- Euklidescher Vektorraum: $\mathbb{R}$-Vektorraum mit Skalarprodukt
- Länge/Betrag/Norm eines Vektors: $v \in V$

$$||v|| := \sqrt{\langle v, v \rangle}$$

- Distanz/Abstand: $v, w \in V$

$$d(v, w) := ||v - w||$$

- Winkel $\forall v, w \in V$, $v, w \neq 0$ mit Cauchy-Schwarzschen Ungleichung:

$$\sphericalangle(v, w) := \arccos \frac{\langle v, w \rangle}{||v|| \cdot ||w||} \in [0, \pi]$$

Orthogonalität

$v \perp w \mid v, w \in V$ falls:

$$\langle v, w \rangle = 0$$

$B \subseteq V$

$$\underbrace{\overbrace{b_i \perp b_j \; \forall i \neq j \quad \wedge \quad b_i, b_j \in B}^{\text{Orthogonalsystem}} \;\; \wedge \;\; ||b_i|| = 1 \; \forall b_i \in B}_{\text{Ortholnormalsystem}}$$

Falls B eine Basis von V ist: **Orthogonalbasis/Orthonormalbasis**

Normieren:

$v \in V \setminus \{0\}$

$$\hat{v} = \frac{1}{||v||} \cdot v$$

Orthogonale Zerlegung von Vektoren:

$v, a \; \neq 0 | \; v, a \in V$

gesucht: $v_a, v_{a^\perp} | v = v_a + v_{a^\perp} \wedge v_a \perp v_{a^\perp}$

$$v_a = \frac{\langle v, a \rangle}{\langle a, a \rangle} \cdot a$$

$$v_{a^\perp} = v - v_a$$

Linearkombinationen bezüglich Orthonormalbasen:

$B = \{b_1, \ldots, b_n\}$ ist ONB von V

Linearkombination zu $v \in V$ finden:

$$\lambda_i = \langle b_i, v \rangle \; \forall i \in \{1, \ldots, n\}$$

Orthogonale Matrizen:

$A \in \mathbb{R}^{n \times n}$ heißt orthogonal falls: $A^T A = E_n$

A sei orthogonal:

- $A^{-1} = A^T$
- $A^T A = A A^T = E_n$
- $det(A) = \pm 1$
- Zeilen bzw. Spalten von A bilden eine ONB des $\mathbb{R}^n$
- $||Av|| = ||v||$

Gram-Schmidt'sches Orthonormalisierungsverfahren

Basis $A = \{a_1, a_2, \dots, a_n\}$ eines euklidischen Vektorraumes V

$b_1 = \frac{1}{||a_1||} \cdot a_1$

$b_2 = \frac{1}{||c_2||} \cdot c_2$ mit $c_2 = a_2 - \langle a_2, b_1 \rangle \cdot b_1$

$b_3 = \frac{1}{||c_3||} \cdot c_3$ mit $c_3 = a_3 - \langle a_3, b_2 \rangle \cdot b_2 - \langle a_3, b_1 \rangle \cdot b_1$

$b_n = \frac{1}{||c_n||} \cdot c_n$ mit $c_n = a_n - \langle a_n, b_1 \rangle \cdot b_1 - \dots - \langle a_n, b_{n-1} \rangle \cdot b_{n-1}$

allgemein:

$$b_{k+1} = \frac{1}{||c_{k+1}||} \cdot c_{k+1} \text{ mit } c_{k+1} = a_{k+1} - \sum_{i=1}^{k} \langle a_{k+1}, b_i \rangle \cdot b_i$$

Vektorprodukt

nur im $\mathbb{R}^3$

$a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}, \ b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$

$$a \times b = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix} \Rightarrow a, b \perp a \times b$$

Orthogonale Projektion

Orthogonales Komplement

V ist ein euklidischer Vektorraum über $\mathbb{R}$ mit Skalarprodukt $\langle \cdot, \cdot \rangle$

$U \leq V$

orthogonales Komplement zu U:

$$U^\perp = \{v \in V \mid v \perp u \ \forall u \in U\}$$

- $U^\perp \leq V$
- $U \cap U^\perp = \{0\}$
- $\exists_1$ Darstellung der Form $v = u + u^\perp \ \ \forall v \in V \mid u \in U, \ u^\perp \in U^\perp$

Bestimmung des orthogonalen Komplement

$U \leq V, \ dim(V) = n, \ dim(U) = r$

$U = \langle a_1, \dots, a_r \rangle$

ergänze basis $B_u = \{a_1, \dots, a_n\}$ zu Basis von V:

$$B_V = \{a_1 \dots, a_r, a_{r+1}, \dots, a_n\}$$

Bilde ONB $B = \{b_1, \dots, b_r, b_{r+1}, \dots, b_n\}$ von V wobei $\{b_1, \dots, b_r\}$ ONB von U

$$U^\perp = \{b_{r+1}, \dots, b_n\}$$

Orthogonale Projektion

$$P_U : \begin{cases} V & \to & U \\ v = u + u^{\perp} & \to & u \end{cases}$$

V euklidischer Vektorraum mit Untervektorraum $U \leq V$

$dim(V) = n$

$dim(U) = v$

noch machen ahh

Bestimme $u = P_u(v)$

$$\begin{aligned} ||v - w||^2 &= ||\overbrace{v - u}^{=u^{\perp}} + u - w||^2 \\ &= \big\langle u^{\perp} + (u - w),\ u^{\perp} + (u - w)\big\rangle \\ &= ||u^{\perp}||^2 + ||u - w||^2 + 2\langle u^{\perp}, u - w\rangle \\ &\geq ||u^{\perp}||^2 = ||v - u||^2 \end{aligned}$$

$$u = \underset{w \in U}{min} ||v - w||$$

Ausrechnen:

$V = \mathbb{R}^n$, $U \leq V$, $U = \langle b_1, \ldots, b_r\rangle \mid b_i \in \mathbb{R}^n$

$u = \lambda_1 b_1 + \ldots + \lambda_r b_r$

Bilde Matrix $A = (b_1, \ldots, b_r) \in \mathbb{R}^{n \times r}$

$u = (b_1, \ldots, b_r) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_r \end{pmatrix} = A \cdot \underbrace{\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_r \end{pmatrix}}_{=:x}$

$\to ||v - u|| = ||v - Ax|| = min$

Das Lineare Ausgleichsproblem

Gegeben: $A \in \mathbb{R}^{n \times r},\ r \leq n,\ b \in \mathbb{R}^n$

Gesucht: $x \in \mathbb{R}^r : ||b - Ax|| = min$

Lösung: Finde x als Lösung des LGS $A^T Ax = A^T b =$ "Normalgleichung"

Anwendungen

Orthogonale Projektion bestimmen

Bestimme orthogonale Projektion von $u = P_U(v)$

$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^{n \times 1},\ \ U = \langle b_1, b_2, \cdots, b_r\rangle,\ \ A = (b_1, b_2, \ldots, b_r) \in \mathbb{R}^{n \times r}$

$x = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_r \end{pmatrix} \in \mathbb{R}^{r \times 1}$

$$A^TAx = A^Tv$$
$$\Downarrow$$
$$\left(\begin{array}{c|c} A^TA & A^Tv \end{array} \right)$$
$$\Downarrow$$
$$\left(\begin{array}{c|c} E_r & x \end{array} \right)$$
$$\Downarrow$$
$$u = A \cdot x$$
$$u = \lambda_1 \cdot b_1 + \lambda_2 + b_2 + \ldots + \lambda_r \cdot b_r$$

$d = ||v - u||$

Lösen Überbestimmter linearer Gleichungssysteme

$Ax = b$ nicht lösbar mit mehr Gleichungen als Unbekannten

Ersatzlösung: $||b - Ax|| = min$

$$\begin{array}{rcl} ||b - Ax|| & = & min \\ & \Downarrow & \\ A^TAx & = & A^Tb \\ & \vdots & \end{array}$$

Methode der kleinsten Quadrate

Gegeben: “Punktwolke”

Gesucht: besste Aproximation durch Ausgleichsfuntion

Basisfunktionen: $f_1, f_2, \ldots, f_r$ bestimmt durch Anwender

Bsp.:

$$y = \beta_1 + \beta_2 x + \beta_3 x^2 \quad \rightarrow \quad f_1(x) = 1,\ f_2(x) = x,\ f_3(x) = x^2$$

$$f = f_1 + f_2 + \ldots + f_r$$

Dann minimiere:

$$(y_1 - f(t_1))^2 + \ldots + (y_n - f(t_n))^2 = min$$

$$A = \begin{pmatrix} f_1(t_1) & \cdots & f_r(t_1) \\ \vdots & \ddots & \vdots \\ f_1(t_n) & \cdots & f_r(t_n) \end{pmatrix},\ \ b = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix},\ \ x = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_r \end{pmatrix}$$

$$f = \lambda_1 f_1 + \ldots + \lambda_r f_r$$
$$||b - Ax|| = min$$
$$A^TAx = Ab$$
$$\vdots$$

lineare Abbildung

V, W K-Vektorräume

Eine Abbildung $f : v \rightarrow w$ heißt Homomorphismus

falls gilt: $\forall \lambda \in K\ \forall v, w \in V$:

$$\left. \begin{array}{rcl} f(\lambda v) & = & \lambda f(v) \\ f(v + w) & = & f(v) + f(w) \end{array} \right\} \Leftrightarrow f(\lambda v + w) = \lambda f(v) + f(w)$$

- $f : v \to w$ linear, $f : w \to u$ linear $\Rightarrow g \circ f$ linear
- $f : v \to w$ linear $\Rightarrow f(0) = 0$
- $f : v \to w$ linear und bijektiv $\Rightarrow f^{-1} : w \to v$

Bild und Kern

$f : V \to W$ linear.

$$\begin{array}{rcll|rcl} ker(f) & = & \{v \in V \mid f(v) = 0\} & \leq V & dim(ker(f)) & = & def(f) \\ Bild(f) & = & \{f(v) \mid v \in V\} & \leq W & dim(Bild(f)) & = & rg(f) \end{array}$$

Dimensionsformel

$f : v \to w$ linear

$$dim(V) = def(f) + rg(f)$$

$$f \text{ injektiv } \Leftrightarrow ker(f) = \{0\}$$

$$f \text{ injektiv} \Leftrightarrow f \text{ surjektiv } \Leftrightarrow f \text{ bijektiv}$$

Koordinatenvektoren

V endlich dimensionaler K-Vektorraum mit geordneter Basis $B = (v_1, \ldots, v_n)$

$v \in V \Rightarrow \exists_1$ Darstellung

$$v = \underbrace{\lambda_1 v_1 + \ldots + \lambda_n v_n}_{v_1, \ldots, v_n} \to_B v = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$