α	0	30	45	60	90	120	150	180	270	360
	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	$\frac{2\pi}{3}$	$\frac{5\pi}{6}$	π	$\frac{3\pi}{2}$	2π
$\sin(\alpha)$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$	0	-1	0
$\cos(\alpha)$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{\sqrt{3}}{2}$	-1	0	1

$\sin(-x) = -\sin(x)$ $\cos(-x) = \cos(x)$ $(\sin(x))' = \cos(x)$ $(\cos(x))' = -\sin(x)$ $\cos^2(x) + \sin^2(x) = 1$

Matrix $A \in K^{m \times n}$ mit m Zeilen und n Spalten

A symmetrisch $\Leftrightarrow A^T = A$ und A quadratisch

A stochastisch: 1) alle Zeilensummen = 1 2) alle Einträge ≥ 0

Matrixprodukt $A \in K^{(n \times m)}$ und $B \in K^{(m \times r)} \Rightarrow AB = C \in K^{(n \times r)}$

mit $c_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj}$ $\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 0+3 & 0+4 \\ 2+9 & 4+12 \end{pmatrix}$ $AB \neq BA$

Rechenregel Assoziativität $A \cdot B \cdot C = (A \cdot B) \cdot C = A \cdot (B \cdot C)$

Distributivität $A(B+C) = AB + AC$ $(A+B)C = AC + BC$

Einheitsmatrix $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ $I_n \cdot A = A = A \cdot I_n$ $I_n^T = I_n$

$(A^T)^T = A$ $(A+B)^T = A^T + B^T$ $(AB)^T = B^T A^T$ $(\lambda A)^T = \lambda A^T$ $\lambda^T = \lambda$

Invertieren $(A \mid I_n) \rightsquigarrow (I_n \mid B)$ mit $A^{-1} = B$ $(AB)^{-1} = B^{-1} A^{-1}$

$$\left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1m} & 1 & & 0 \\ \vdots & & \vdots & & \ddots & \\ a_{n1} & \cdots & a_{nm} & 0 & & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & & 0 & b_{11} & \cdots & b_{1m} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & b_{n1} & \cdots & b_{nm} \end{array}\right)$$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

LGS (Lineare Gleichungssystem)

a) genau eine Lösung (homogen) $rg(A) = n$ linear unabhängig

$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 2 \\ 0 & 1 & -4 & -4 \\ 0 & 0 & -5 & -3 \end{array}\right) \rightsquigarrow L = \left\{\left(\frac{12}{5}, -\frac{8}{5}, \frac{3}{5}\right)^T\right\}$ invertierbar $\det(A) \neq 0$

b) unendlich viele Lösungen (homogen) $rg(A) < n$ linear abhängig

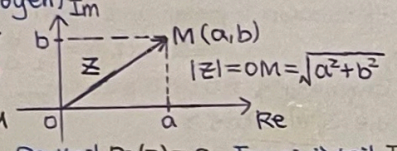
$\left(\begin{array}{cc|c} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right) \rightsquigarrow L = \{(1-2\lambda, \lambda) \mid \lambda \in \mathbb{R}\}$ nicht invertierbar $\det(A) = 0$

$= \left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} -2 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R}\right\}$ #freiParameter = $n - rg(A)$

Nullzeilen

c) keine Lösung (inhomogen)

$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow L = \varnothing$ Widerspruch



Komplexe Zahlen $i^2 = -1$

$z = a + ib \in \mathbb{C}, a, b \in \mathbb{R}$ Realteil $Re(z) = a$ Imaginärteil $Im(z) = b$

konjungierte $\bar{z} = a - ib$ $z + \bar{z} = 2a = 2\,Re(z)$ $z - \bar{z} = 2ib = 2i\,Im(z)$

$|z| = \sqrt{a^2+b^2} = \sqrt{z\bar{z}} = |\bar{z}|$ $|z|^2 = z\bar{z} = (a+ib)(a-ib) = a^2 + b^2$

$|z_1 z_2| = |z_1| \cdot |z_2|$ $|z_1 + z_2| \leq |z_1| + |z_2| \Rightarrow$ Dreiecksungleichung

$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

$z^{-1} = \frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2} = \frac{\bar{z}}{|z|^2}$

Gruppe $(G, *)$

Abgeschlossenheit $*: G \times G \to G$

Assoziativität $(a*b)*c = a*(b*c)$ $\forall a,b,c \in G$

Existenz eines neutralen Elements $a \cdot e = a = e \cdot a$ $\forall a \in G$ $\exists e \in G$

Existenz des Inversen $a \cdot a^{-1} = e$ $\forall a \in G$ $\exists a^{-1} \in G$

Gruppe ist abelsch falls $a * b = b * a$ $\forall a, b \in G$

Körper $(K, +, \cdot)$

$(K, +)$ und $(K \setminus \{0\}, \cdot)$ ist jeweils eine abelsche Gruppe

$a \cdot (b+c) = a \cdot b + a \cdot c$

Vektorraum

$(V, +, \cdot)$ ist ein K-Vektorraum wobei K ist ein Körper

1) $(V, +)$ ist abelsche Gruppe

2) $\forall a, b \in K, \forall v, w \in V$ Menge V mit 2 Abbildungen

$\begin{cases} a \cdot (v+w) = av + aw & +: V \times V \to V, (v,w) \to v+w \\ (a+b) \cdot v = av + bv & \cdot: K \times V \to V, (a,v) \to a \cdot v \\ (a \cdot b) \cdot v = a \cdot (b \cdot v) \end{cases}$

3) $\forall v \in V: 1 \cdot v = v$

Unterraum $U \subseteq V$

$\begin{cases} U \neq \varnothing \\ \forall v, w \in U \to v + w \in U \\ \forall v \in U \text{ und } a \in K \to a \cdot v \in U \\ (0 \in U \text{ ist ein notwendiges Kriterium} \end{cases}$

→ Lösungsmenge L eines homogenen LGS ist Untervektorraum

U_1 und U_2 sind Untervektorräume

→ $U_1 \cap U_2$ ist auch ein Unterraum

→ $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1 \text{ und } u_2 \in U_2$ ist ein Unterraum

Erzeugte Unterraum $\langle S \rangle$

der kleinste Unterraum von V, der S als Teilmenge enthält

die Menge aller Linearkombinationen von Vektoren in S

jeder Unterraum von V, der S enthält, enthält auch $\langle S \rangle$

Linearkombination $w = \sum_{i=1}^{n} \lambda_i v_i$ mit Vektoren $\{v_1, \ldots, v_n\}$

$w = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 \Rightarrow \begin{pmatrix} | & | & | \\ v_1 & v_2 & v_3 \\ | & | & | \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = w \Rightarrow L = \left\{\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix}^T\right\}$

Lineare Unabhängigkeit $\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n = 0$

→ linear unabhängig $\lambda_1 = \ldots = \lambda_n = 0$

→ linear abhängig nicht alle $\lambda_i = 0$

- Methode 1: LGS spaltenweise aufstellen und lösen $\left(\begin{array}{ccc|c} | & | & | & | \\ v_1 & v_2 & v_3 & 0 \\ | & | & | & | \end{array}\right)$
- Methode 2: Matrix zeilenweise aufstellen $\begin{pmatrix} -v_1- \\ -v_2- \\ -v_3- \end{pmatrix}$ Rang bestimmen $\begin{cases} \text{lin unabhängig} & rg = \#\text{Zeilen} \\ \text{lin abhängig} & rg < \#\text{Zeilen} \end{cases}$

$B = \{b_1, \ldots, b_m\}$ ist ein Basis von V mit $\dim(V) = n$

1) $m = n$ 2) B ist linear unabhängig 3) $b_i \in V$ $\forall i \in \{1, \ldots, m\}$

Lineare Abbildung

$\dim K^{m \times n} = m \cdot n$ $\dim K[X] = \infty$ $\dim K[X]_n = n+1$ $\dim K[X]_{\leq n} = n+1$ $\dim \mathbb{R}^{\mathbb{R}} = \infty$ $\dim \mathbb{R}^n = n$

$f: V \to W$ ist linear ① $f(0) = 0$ ② $f(\lambda v + w) = \lambda f(v) + f(w)$

$\begin{cases} \forall x, y \in V & f(v+w) = f(v) + f(w) \\ \forall x \in V \text{ und } k \in K & f(\lambda v) = \lambda \cdot f(v) \end{cases}$

Kern: Menge der Vektoren in V, die auf 0 abgebildet (Unterraum von V)

$\ker(f) = \{v \in V \mid f(v) = 0\} \subseteq V$ ⇒ kern ist Lösungsmenge von $Ax = 0$

$Ker(f) = \{0\} \Leftrightarrow \dim(ker(f) = \{0\}) = 0 \Leftrightarrow rg = n \Leftrightarrow f$ injektiv

$\dim(Ker(A)) = n - rg(A) = \#\text{Nullzeilen} \leq \dim(V)$

Bild: Menge der Bilder (Unterraum von W)

$Bild(f) = \{f(v) \mid v \in V\} \subseteq W$ surjektiv $\dim(Bild(f)) = \dim(W)$

$\dim(Bild(f)) = rg(A) \leq \dim(W)$ injektiv $\dim(Bild(f)) = \dim(V) = n$

bijektiv $\dim(Bild(f)) = \dim(V) = \dim(W)$

Dimensionsformel $\dim(V) = \dim(Ker(f)) + \dim(Bild(f))$

$\dim(U \cap V) = \dim(U) + \dim(V) - \dim(U + V)$

Basis des Zeilenraums: 1) Matrix A in Zeilenstufenform bringen u. umformen 2) verbleibende Nicht-Nullzeilen als Spalten schreiben

→ **Basis des Kerns:** Basis der Lösungsmenge von $Ax = 0$

Basis des Spaltenraums = Basis des Bildes: 1) transponiere A zu A^T 2) bringe A^T in Zeilenstufenform und umformen 3) verbleibende Nicht-Nullzeilen als Spalten schreiben

Spaltenraum der Abbildungsmatrix A = Bild der linearen Abbildung f_A

$rg(A) = \dim(Bild(A)) = \dim(\text{Spaltenraum von } A) = \dim(\text{Zeilenraum von } A^T)$

$rg(A^T) = \dim(Bild(A^T)) = \dim(\text{Spaltenraum von } A^T)$

F_3^4 ⇒ 4-dimensional Vektorraum Mächtigkeit = a^b

⇒ Menge $\{0, 1, 2\}$ $\begin{cases} a = \#\text{Elemente einer Menge} = 3 \\ b = \dim(Bild) \text{ oder } b = \dim(Kern) \end{cases}$

Isomorphismus = bijektive lineare Abbildung $\varphi: V \to W$

im Fall $\dim(V) = \dim(W)$, lineare Abbildung durch quadratische Matrix

f Isomorphismus $\Leftrightarrow$ $Kern(f) = \{0\} \Leftrightarrow rg(A) = n$ 展现

$\Leftrightarrow f$ bijektiv $\Leftrightarrow f$ injektiv $\Leftrightarrow f$ surjektiv

Invertierbarkeit (nur bei quadratischen Matrix)

A invertierbar $\Leftrightarrow \exists B \in K^{n \times n}$ $AB = I_n$ oder auch $BA = I_n$

$\Leftrightarrow rg(A) = n \Leftrightarrow A$ regulär $\Leftrightarrow \det(A) \neq 0 \Leftrightarrow 0 \neq$ EW von A

$\Leftrightarrow Kern(A) = 0 \Leftrightarrow \dim(Kern(A)) = 0 \Leftrightarrow$ LGS $Ax = b$ eindeutig lösbar $\Leftrightarrow$ Zeilen und Spalten linear unabhängig

$\Leftrightarrow f$ bijektiv $\Leftrightarrow f$ injektiv $\Leftrightarrow f$ surjektiv

A nicht invertierbar $\Leftrightarrow rg(A) < n \Leftrightarrow \det(A) = 0 \Leftrightarrow$ singulär

$\Leftrightarrow \dim(Kern(A)) \geq 1 \Leftrightarrow$ existiert EW = 0

Darstellungsmatrix

Seien V und W endlich dimensionale K-Vektorraum mit Basen

$B = \{b_1, \ldots, b_n\}$ und $C = \{c_1, \ldots, c_n\}$, $\varphi: V \to W$

$D_{C,B}(\varphi) = \left(\begin{array}{ccc} | & | & | \\ {}_C\varphi(b_1) & {}_C\varphi(b_2) & \ldots \; {}_C\varphi(b_n) \\ | & | & | \end{array}\right)$

b_i als Input für Abbildung φ eingeben, dann output in Form der Basis C darstellen

Basiswechselmatrix B, B' Basen von V, $S = S_{B,B'}$, $\varphi: V \to V$ linear

$D_{B'}(\varphi) = S^{-1} D_B(\varphi) S = S_{B,B'}^{-1} D_B(\varphi) S_{B,B'} = S_{B',B} D_{B,B}(\varphi) S_{B,B'}$

Basistransformation B, B' von V, C, C' von W, $\varphi: V \to V$ linear

$D_{C',B'}(\varphi) = S_{C',C} D_{C,B}(\varphi) S_{B,B'} = S_{C,C'}^{-1} D_{C,B}(\varphi) S_{B,B'}$

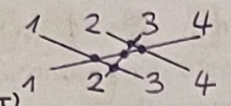
$A, B \in K^{n \times n}$ sind ähnlich $B = S^{-1} A S$ und $\det(A) = \det(B)$

$A, B \in K^{m \times n}$ sind äquivalent $B = T^{-1} A S$

$p = ax^2 + bx + c$ $x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Fehlstand $i<j$ aber $\sigma(i)>\sigma(j)$ $\quad \sigma(1,2,3,4)\to(3,4,2,1)$

f = # Fehlstände = Schnittstellen = 5



Signum $\operatorname{sgn}(\sigma)=(-1)^f=(-1)^5=-1$

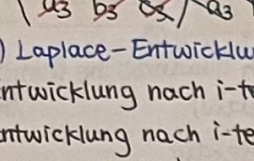
Determinanten $\operatorname{sgn}(\sigma\tau)=\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$

1) Leibniz-Formel (nur für quadratische Matrix)

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

2) für 2x2 Matrix $\det\begin{pmatrix}a&b\\c&d\end{pmatrix}=ad-bc$

3) für 3x3 Matrix



$$\det\begin{pmatrix}a_1&b_1&c_1\\a_2&b_2&c_2\\a_3&b_3&c_3\end{pmatrix}=\begin{matrix}a_1b_2c_3+b_1c_2a_3+c_1a_2b_3\\-a_3b_2c_1-b_3c_2a_1-c_3a_2b_1\end{matrix}$$

4) Laplace-Entwicklung

Entwicklung nach i-te Zeile $\det(A)=\sum_{j=1}^{n}(-1)^{i+j}a_{ij}\det(A_{ij})$

Entwicklung nach i-te Spalte $\det(A)=\sum_{i=1}^{n}(-1)^{i+j}a_{ij}\det(A_{ij})$

$$\begin{pmatrix}a_1&b_1&c_1&d_1\\a_2&b_2&c_2&d_2\\a_3&b_3&c_3&d_3\\a_4&b_4&c_4&d_4\end{pmatrix}$$ Entwicklung nach 1. Spalte

$$\det(A)=a_1\cdot\det\begin{pmatrix}b_2&c_2&d_2\\b_3&c_3&d_3\\b_4&c_4&d_4\end{pmatrix}-a_2\cdot\det\begin{pmatrix}b_1&c_1&d_1\\b_3&c_3&d_3\\b_4&c_4&d_4\end{pmatrix}+a_3\cdot\det\begin{pmatrix}b_1&c_1&d_1\\b_2&c_2&d_2\\b_4&c_4&d_4\end{pmatrix}-a_4\cdot\det\begin{pmatrix}b_1&c_1&d_1\\b_2&c_2&d_2\\b_3&c_3&d_3\end{pmatrix}$$

5) Dreiecksmatrix $\det(A)=\prod_{i=1}^{n}a_{ii}$ (Produkt der Diagonalwerte)

6) Blockmatrix $\det\begin{pmatrix}A&C\\0&B\end{pmatrix}=\det(A)\cdot\det(B)$ A und $B\in K^{n\times n}$

Rechenregel

$A,B\in K^{n\times n}$

$\det(\lambda\cdot A)=\lambda^n\det(A)$

$\det(AB)=\det(A)\det(B)=\det(B)\det(A)=\det(BA)$

$\det(A^T)=\det(A)$

$\det(A^k)=\det(A)^k$

Vertauschen zweier Zeilen/Spalten $\det(A')=-\det(A)$

Multiplikation einer Zeile/Spalte mit Skalar λ $\det(A')=\lambda\cdot\det(A)$

Addition des Vielfachen einer Zeile/Spalte zu einer anderen $\det(A')=\det(A)$

$A\in K^{n\times n}$ hat 2 gleiche Zeilen/Spalten $\det(A)=0$

A hat Nullzeilen/Nullspalten $\det(A)=0$

Diagonalisierung für quadratische Matrix $A\in K^{n\times n}$

$Av=\lambda v$ mit Eigenvektor $v\neq 0$ und Eigenwert λ

Charakteristisches Polynom einer Matrix $A\in K^{n\times n}$

$\chi_A=\det(x\cdot I_n-A)=\det(A-xI_n)=(x-\lambda_1)^{ma_1}\cdots(x-\lambda_r)^{ma_r}$

algebraische Vielfachheit $ma(\lambda_i)$

geometrische Vielfachheit $mg(\lambda_i)=\dim(\ker(\lambda_i I_n-A))=n-rg$

für $1\le i\le r$ gilt: $1\le mg(\lambda_i)\le ma(\lambda_i)$

diagonalisierbar $\Leftrightarrow$ $ma(\lambda_i)=mg(\lambda_i)$ $\forall i\in\{1,\dots,r\}$

$E_{\lambda_i}=\operatorname{Kern}(\lambda_i I_n-A)$

$B=\left\{\begin{pmatrix}v_1\\1\end{pmatrix},\begin{pmatrix}v_2\\1\end{pmatrix},\begin{pmatrix}v_3\\1\end{pmatrix}\right\}$

$S=\begin{pmatrix}v_1&v_2&v_3\\1&1&1\end{pmatrix}$

$E_{\lambda_1}=\operatorname{Kern}(\lambda_1 I_n-A)=\left\langle\begin{pmatrix}v_1\\1\end{pmatrix}\right\rangle$

$E_{\lambda_2}=\operatorname{Kern}(\lambda_2 I_n-A)=\left\langle\begin{pmatrix}v_2\\1\end{pmatrix}\right\rangle$

$E_{\lambda_3}=\operatorname{Kern}(\lambda_3 I_n-A)=\left\langle\begin{pmatrix}v_3\\1\end{pmatrix}\right\rangle$

Diagonalmatrix $D=\operatorname{diag}(\lambda_1,\lambda_2,\lambda_3)=S^{-1}AS$

Reihenfolge der λ_i in D ist nicht eindeutig (egal)

aber Reihenfolge in S und in D muss entsprechend

alle Eigenwerte unterschiedlich $\Rightarrow$ diagonalisierbar

jede Diagonalmatrix ist diagonalisierbar

Skalarprodukt von $v=\begin{pmatrix}v_1\\\vdots\\v_n\end{pmatrix}$ und $w=\begin{pmatrix}w_1\\\vdots\\w_n\end{pmatrix}$

$\langle v,w\rangle=v^Tw=\sum_{i=1}^{n}v_iw_i\in K$

$\left\langle\begin{pmatrix}v_1\\v_2\\v_3\end{pmatrix},\begin{pmatrix}w_1\\w_2\\w_3\end{pmatrix}\right\rangle=v_1w_1+v_2w_2+v_3w_3$

$\to v$ und w orthogonal falls $\langle v,w\rangle=0$

$\to$ orthogonales Komplement eines UVR $U\subseteq K^n$

$U^\perp=\{v\in K^n\mid\langle u,v\rangle=0\ \forall u\in U\}$

Eigenschaften

1) Bilinearität: $\forall v,w,v',w'\in V$ und $\forall\lambda\in K$ gilt

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

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

2) Symmetrie: $\langle v,w\rangle=\langle w,v\rangle$ $\forall v,w\in V$

3) nicht ausgeartet: $(K^n)^\perp=\{0\}$

$\to$ nur der Nullvektor steht auf allen Vektoren senkrecht

4) Nicht-Negativität: für $K=\mathbb{R}$: $\langle v,v\rangle\ge 0$ $\forall v\in\mathbb{R}^n$

Euklidische Länge von $v\in\mathbb{R}^n$: $|v|=\sqrt{\langle v,v\rangle}$

$\to |v+w|\le|v|+|w|$ (Dreiecksgleichung)

$\to |av|=|a|\cdot|v|$

$\to v\neq 0\Rightarrow|v|>0$

$\to |\langle v,w\rangle|\le|v|\cdot|w|$ (Schwarzsche Gleichung)

Orthonormalsystem (linear unabhängig)

1) v_i und v_j für $i\neq j$ orthogonal 2) $|v_i|=1$ für alle i

Orthonormalbasis (ONB): Orthonormalsystem + Basis

Orthonormierungsverfahren von Gram und Schmidt (Orthonormalbasis)

Input: UVR $U=\langle u_1,\dots,u_n\rangle$ Output: ONB $B=\langle b_1,\dots,b_n\rangle$

$b_1=\frac{1}{|u_1|}\cdot u_1$ $\quad b_{k+1}=\frac{1}{|b'_{k+1}|}\cdot b'_{k+1}$ mit $b'_{k+1}=u_{k+1}-\sum_{i=1}^{k}\langle u_{k+1},b_i\rangle b_i$

$b_2=\frac{1}{|b_2'|}\cdot b_2'$ mit $b_2'=u_2-\langle u_2,b_1\rangle b_1$

$b_3=\frac{1}{|b_3'|}\cdot b_3'$ mit $b_3'=u_3-\langle u_3,b_1\rangle b_1-\langle u_3,b_2\rangle b_2$

$b_n=\frac{1}{|b_n'|}\cdot b_n'$ mit $b_n'=u_3-\langle u_3,b_1\rangle b_1-\langle u_3,b_2\rangle b_2-\dots-\langle u_3,b_{n-1}\rangle b_{n-1}$

Lineare Code $C\le F_K^n$ als (n,k) Code $\quad F_2^5\ (x_1,x_2)\to(x_1,x_2,x_1,x_2,x_1+x_2)$

$\begin{pmatrix}c_1\\\vdots\\c_n\end{pmatrix}=G\cdot\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix}$

C: Codewort — Länge von C: $n=5$

G: Generatormatrix — Informationsrate: $\frac{k}{n}=\frac{2}{5}$

x: Informationswort — Redundanz: $n-k=5-2=3$

Generatormatrix $G=\begin{pmatrix}I_k\\A\end{pmatrix}$ mit $A\in K^{(n-k)\times k}$ $\quad G=\begin{pmatrix}1&0\\0&1\\1&0\\0&1\\1&1\end{pmatrix}$ I_2

Parity-Check-Matrix $P=(-A\ I_{n-k})\in K^{(n-k)\times n}$

$P\cdot G=(-A\ I_{n-k})\cdot\begin{pmatrix}I_k\\A\end{pmatrix}=0$

$P\cdot c=P\cdot(c'+f)=0$ für alle $c\in C$

$\dim(C)=n-(n-k)=k$

$P=\left(\begin{array}{ccc|ccc}-1&0&1&0&0\\0&-1&0&1&0\\-1&-1&0&0&1\end{array}\right)=\left(\begin{array}{ccc|ccc}1&0&1&0&0\\0&1&0&1&0\\1&1&0&0&1\end{array}\right)$

in F_2 $1+1\equiv 0$ $0+1\equiv 1$ $-1\equiv 1$ $2\equiv 0$

Hamming Gewicht von c # Stelle $\neq 0$ $w(c)=|\{i\in\{1,\dots,n\}\mid c_i\neq 0\}|$ für $c=(c_1,\dots,c_n)\in K^n$

Hamming Abstand von c und c' # Unterschiedsstelle $d(c,c')=w(c-c')=|\{i\in\{1,\dots,n\}\mid c_i\neq c'_i\}|$ für $c,c'\in K^n$

Hamming Abstand von C

$d(C)=\min\{d(c,c')\mid c,c'\in C,\ c\neq c'\}$ für eine Teilmenge $C\subseteq K^n$

$=\min\{w(c)\mid c\in C\setminus\{0\}\}$ für ein Untervektorraum C

$d(C)=2e+1\Rightarrow$ C ist e-fehlerkorrigierend

$d(C)=2e+2\Rightarrow$ C ist e-fehlerkorrigierend und (e+1)-fehlererkennend

Symmetrische Matrix $A\in\mathbb{R}^{n\times n}$ $\quad A=\begin{pmatrix}a&b\\b&c\end{pmatrix}$ $\det=ac-b^2$ $\operatorname{spur}=a+c$

- positiv definit, falls alle Eigenwerte >0 ($\to$ Maximum) — >0 — /
- positiv semidefinit, falls alle Eigenwerte ≥ 0 — $=0$ — ≥ 0
- negativ definit, falls alle Eigenwerte <0 ($\to$ Minimum) — >0 — <0
- negativ semidefinit, falls alle Eigenwerte ≤ 0 — $=0$ — ≤ 0
- indefinit, falls sowohl positive als auch negative Eigenwerte gibt — <0 — /

Komplexe Zahlen - Kartesische Koordinaten

Addition $(a, b) + (c, d) = (a + c, b + d)$

Multiplikation $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$

Rechenregel

- Die Assoziativgesetze: $[(a, b) \dot{+} (c, d)] \dot{+} (e, f) = (a, b) \dot{+} [(c, d) \dot{+} (e, f)]$.
- Die Kommutativgesetze: $(a, b) \dot{+} (c, d) = (c, d) \dot{+} (a, b)$.
- Das Distributivgesetz: $(a, b) \cdot [(c, d) + (e, f)] = (a, b) \cdot (c, d) + (a, b) \cdot (e, f)$.
- Es gibt ein Einselement: $(1, 0)$ erfüllt $(1, 0) \cdot (c, d) = (c, d) \quad \forall (c, d) \in \mathbb{R}^2$.
- Es gibt ein Nullelement: $(0, 0)$ erfüllt $(0, 0) + (c, d) = (c, d) \quad \forall (c, d) \in \mathbb{R}^2$.
- Es gibt inverse Elemente: Zu $(a, b) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ ist $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) \in \mathbb{R}^2$ invers zu (a, b), denn

$$(a, b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2}\right) = (1, 0).$$

  Man schreibt $(a, b)^{-1}$ für das Inverse zu (a, b).
- Es gibt entgegengesetzte Elemente: Zu $(a, b) \in \mathbb{R}^2$ ist $(-a, -b) \in \mathbb{R}^2$ entgegengesetzt zu (a, b), denn

$$(a, b) + (-a, -b) = (0, 0).$$

  Man schreibt $-(a, b)$ für das Entgegengesetzte zu (a, b).

Kurzschreibweise **a = (a,0)**

Imaginäre Einheit **i = (0,1)** $\mathrm{i}^2 = \mathrm{i} \cdot \mathrm{i} = (0 + 1\mathrm{i}) \cdot (0 + 1\mathrm{i}) = -1$

Addition $(a + b\mathrm{i}) + (c + d\mathrm{i}) = a + c + \mathrm{i}(b + d)$

Multiplikation $(a + \mathrm{i}b) \cdot (c + \mathrm{i}d) = a\,c + \mathrm{i}^2 b\,d + \mathrm{i}b\,c + \mathrm{i}a\,d = a\,c - b\,d + \mathrm{i}(a\,d + b\,c)$

Begriffe und Tatsachen zu komplexen Zahlen

Gegeben ist eine komplexe Zahl $z = a + \mathrm{i}b \in \mathbb{C}, a, b \in \mathbb{R}$.

- Man nennt
  - $\mathrm{Re}(z) = a \in \mathbb{R}$ den **Realteil** von z und
  - $\mathrm{Im}(z) = b \in \mathbb{R}$ den **Imaginärteil** von z.
- Die komplexen Zahlen $0 + \mathrm{i}b$ nennt man **rein imaginär.**

- Zwei komplexe Zahlen sind genau dann gleich, wenn Real- und Imaginärteil gleich sind, d. h.

$$a + \mathrm{i}b = c + \mathrm{i}d \;\Leftrightarrow\; a = c \text{ und } b = d.$$

- Man nennt $\overline{z} = a - ib$ die **zu** z **konjugierte** komplexe Zahl. Die Zahl $\overline{z}$ entsteht aus z durch Spiegelung an der reellen Achse. Insbesondere gilt:
  - $\overline{z} = z \Leftrightarrow \mathrm{Im}(z) = 0 \Leftrightarrow z \in \mathbb{R}$.
  - $z\overline{z} = (a + ib)(a - ib) = a^2 + b^2 \in \mathbb{R}$.
  - Für $z_1,\ z_2 \in \mathbb{C}$ gelten die Rechenregeln:

$$\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2 \qquad \text{und} \qquad \overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2.$$

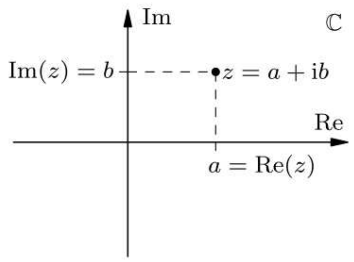
Addition $\overline{z+\omega} = \overline{z} + \overline{\omega}$

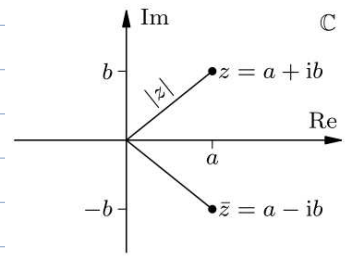
$$\overline{z+\omega} = \overline{a+ib+c+id} = \overline{(a+c)+i(b+d)} = (a+c)-i(b+d)$$
$$\overline{z}+\overline{\omega} = a-ib+c-id = a+c-i(b+d)$$

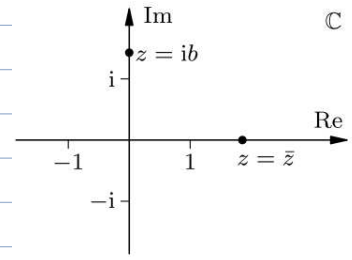
Multiplikation $\overline{z \cdot \omega} = \overline{z} \cdot \overline{\omega}$

- $\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z})$.
- $\mathrm{Im}(z) = \frac{1}{2\mathrm{i}}(z - \overline{z})$.

$|z| \geq \mathrm{Re}(z)$ bzw $\mathrm{Im}(z)$







- Man nennt den Ausdruck

$$|\bar{z}| = |z| = \sqrt{a^2 + b^2} = \sqrt{z\,\overline{z}} \in \mathbb{R}_{\geq 0}$$

den **Betrag** oder die **Länge** von z.

- In $\mathbb{C}$ gilt die **Dreiecksungleichung:**

$$|z_1 + z_2| \leq |z_1| + |z_2| \text{ für alle } z_1,\ z_2 \in \mathbb{C}.$$

Betrag ist multiplikativ

$|z\,\omega| = |z|\,|\omega|$

$$|(a+ib)(c+id)| = |ac - bd + i(ad+bc)| = (ac-bd)^2 + (ad+bc)^2$$
$$|a+ib)|\,|c+id| = (a^2+b^2)\,(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

Betrag ist nicht additiv

$|z+\omega| \leq |z| + |\omega|$

$|i-i| = 0$
$|i| + |-i| = 2$

$$|z+\omega|^2 = (z+\omega)\overline{(z+\omega)}$$
$$= (z+\omega)(\bar{z}+\bar{\omega})$$
$$= z\bar{z} + z\bar{\omega} + \omega\bar{z} + \omega\bar{\omega}$$
$$= |z|^2 + 2Re(z\bar{\omega}) + |\omega|^2$$

$\leq$

$$(|z| + |w|)^2$$
$$= |z|^2 + 2|z|\,|\omega| + |\omega|^2$$
$$= |z|^2 + 2|z|\,|\bar{\omega}| + |\omega|^2$$
$$= |z|^2 + 2|z\bar{\omega}| + |\omega|^2$$

$$\frac{2+\mathrm{i}}{1-\mathrm{i}} = \frac{2+\mathrm{i}}{1-\mathrm{i}} \cdot \frac{1+\mathrm{i}}{1+\mathrm{i}} = \frac{1+3\mathrm{i}}{2} = \frac{1}{2} + \frac{3}{2}\mathrm{i} \qquad \text{und} \qquad \frac{1}{\mathrm{i}} = \frac{1}{\mathrm{i}} \cdot \frac{(-\mathrm{i})}{(-\mathrm{i})} = -\mathrm{i}.$$

Fundamentalsatz von Algebra

$$p = a_n x^n + \cdots + a_1 x + a_0 \quad \rightarrow \quad p = a_n (x - z_1)^{\nu_1} \cdots (x - z_k)^{\nu_k}$$

Nullstellen **Vielfachheiten**

Rezept: Tipps zum Bestimmen von Nullstellen von Polynomen

- **Mitternachtsformel:** Ist $p = ax^2 + bx + c$ ein Polynom mit $a,\ b,\ c \in \mathbb{C}$, so sind

$$z_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathbb{C}$$

die Nullstellen von p, und es gilt $p = a(x - z_1)(x - z_2)$. Beachte hierbei:

- $\sqrt{-r} = \mathrm{i}\sqrt{r}$ für $r \in \mathbb{R}_{>0}$ und
- $\sqrt{a + b\mathrm{i}}$ erhält man mit der Formel: Die Wurzeln $w_{1,2}$ aus $z = a + \mathrm{i}b$ lauten im Fall $b \geq 0$:

$$w_{1,2} = \pm \left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \mathrm{i} \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}} \right)$$

bzw. im Fall $b < 0$:

$$w_{1,2} = \pm \left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} - \mathrm{i} \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}} \right).$$

- Ist $z \in \mathbb{C}$ eine Nullstelle des **reellen** Polynoms $p = a_n x^n + \cdots + a_1 x + a_0$ mit $a_0,\ a_1, \ldots, a_n \in \mathbb{R}$, so ist auch $\overline{z} \in \mathbb{C}$ eine Nullstelle von p.
- Kann man eine Nullstelle $z \in \mathbb{C}$ des Polynoms p vom Grad n erraten? Falls ja, so kann man diese mit der Polynomdivision *wegdividieren:*

$$p(z) = 0 \ \Leftrightarrow \ p = (x - z)\, q$$

mit einem Polynom q vom Grad $n - 1$.

$x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i})$ **Nullstellen** $\pm i$

$x^2 - 1 = (x + 1)(x - 1)$ **Nullstellen** ± 1

Für das Polynom $p = x^2 + x + 1$ gilt

$$z_{1,2} = \frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2}$$

$$\sqrt{-3} = \sqrt{3 \cdot (-1)} = \sqrt{3 (\mathrm{i})^2} = \sqrt{3}\,\mathrm{i}$$

$$z_1 = -\frac{1}{2} + \frac{\sqrt{-3}}{2} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\,\mathrm{i}$$

$$z_2 = -\frac{1}{2} - \frac{\sqrt{-3}}{2} = -\frac{1}{2} - \frac{\sqrt{3}}{2}\,\mathrm{i}$$

$$p = x^2 + x + 1 = \left(x - \left(\tfrac{-1}{2} + \tfrac{\sqrt{3}\mathrm{i}}{2}\right)\right)\left(x - \left(\tfrac{-1}{2} - \tfrac{\sqrt{3}\mathrm{i}}{2}\right)\right)$$

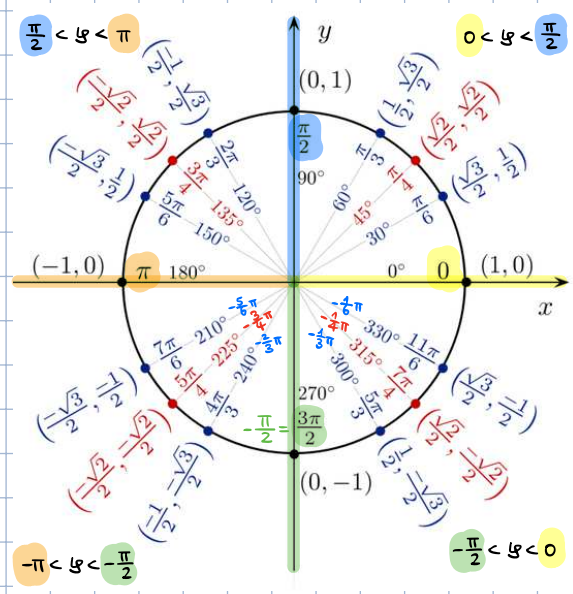
Bogenmaß	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	$\frac{2\pi}{3}$	$\frac{3\pi}{4}$	$\frac{5\pi}{6}$	π
Winkel	$0°$	$30°$	$45°$	$60°$	$90°$	$120°$	$135°$	$150°$	$180°$
$\sin x$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
$\cos x$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{\sqrt{2}}{2}$	$-\frac{\sqrt{3}}{2}$	-1

Polardarstellung

Die komplexen Zahlen bilden die sogenannte **Gauß'sche Zahlenebene** $\mathbb{C}$. Jede komplexe Zahl $z = a + ib$ ist durch ihre kartesischen Koordinaten (a, b) eindeutig beschrieben. Man kann aber jeden Punkt $z \neq 0$ aus $\mathbb{C}$ auch durch **Polarkoordinaten** (r, φ) eindeutig beschreiben. Dabei ist (beachte die Abb. 8.1)

- $r = \sqrt{a^2 + b^2} = |z| \in \mathbb{R}_{>0}$ die Länge bzw. der Betrag von z und
- $\varphi \in (-\pi, \pi]$ der Winkel, der von z und der positiven reellen Achse eingeschlossen wird.

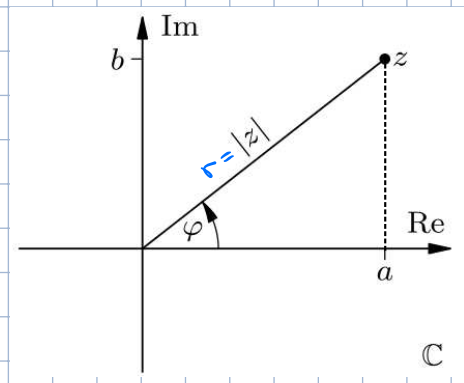
Man nennt $\varphi \in (-\pi, \pi]$ das **(Haupt-)Argument** von z und schreibt dafür $\varphi = \arg(z)$.



Damit haben wir für jede komplexe Zahl $z \neq 0$ die zwei Darstellungsmöglichkeiten:

$$z = \begin{cases} (a, b) \text{ kartesische Koordinaten} \\ (r, \varphi) \text{ Polarkoordinaten} \end{cases}.$$

- $z = 1$. Hier gilt $(a, b) = (1, 0)$ und $(r, \varphi) = (1, 0)$.
- $z = \mathrm{i}$. Hier gilt $(a, b) = (0, 1)$ und $(r, \varphi) = (1, \pi/2)$.
- $z = -1$. Hier gilt $(a, b) = (-1, 0)$ und $(r, \varphi) = (1, \pi)$.
- $z = -\mathrm{i}$. Hier gilt $(a, b) = (0, -1)$ und $(r, \varphi) = (1, -\pi/2)$.
- $z = -1 - \mathrm{i}$. Hier gilt $(a, b) = (-1, -1)$ und $(r, \varphi) = (\sqrt{2}, -3\pi/4)$.
- $z = -1 + \mathrm{i}$. Hier gilt $(a, b) = (-1, 1)$ und $(r, \varphi) = (\sqrt{2}, 3\pi/4)$.



$\cos\varphi = \frac{a}{r} \Rightarrow a = r\cos\varphi$

$\sin\varphi = \frac{b}{r} \Rightarrow b = r\sin\varphi$

$z = a + \mathrm{i}b = r\,(\cos\varphi + \mathrm{i}\sin\varphi)$

Umrechnungsformeln

- **kartesisch → polar:** Gegeben ist $z = a + \mathrm{i}b \neq 0$, $a, b \in \mathbb{R}$. Dann:

$$\left.\begin{aligned} r &= \sqrt{a^2 + b^2} \\ \varphi &= \begin{cases} \arccos(a/r), \text{ falls } b \geq 0 \\ -\arccos(a/r), \text{ falls } b < 0 \end{cases} \end{aligned}\right\} \Rightarrow z = r\left(\cos(\varphi) + \mathrm{i}\sin(\varphi)\right).$$

- **polar → kartesisch:** Gegeben ist $z = r\left(\cos(\varphi) + \mathrm{i}\sin(\varphi)\right)$, $r, \varphi \in \mathbb{R}$. Dann:

$$\left.\begin{aligned} a &= r\cos(\varphi) \\ b &= r\sin(\varphi) \end{aligned}\right\} \Rightarrow z = a + \mathrm{i}b.$$

Multiplikation

$$\left.\begin{aligned} z_1 &= r_1\left(\cos(\varphi_1) + \mathrm{i}\sin(\varphi_1)\right) \\ z_2 &= r_2\left(\cos(\varphi_2) + \mathrm{i}\sin(\varphi_2)\right) \end{aligned}\right\} \Rightarrow z_1 \cdot z_2 = r_1 r_2\left(\cos(\varphi_1 + \varphi_2) + \mathrm{i}\sin(\varphi_1 + \varphi_2)\right)$$

Additionstheoremen des Sinus und Cosinus

$$z_1 z_2 = r_1 r_2\left[\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i\left(\cos\varphi_1\sin\varphi_2 + \sin(\varphi_1)\cos(\varphi_2)\right)\right]$$

Moivre'sche Formel

Für jede komplexe Zahl $z = (\cos(\varphi) + \mathrm{i}\sin(\varphi)) \in \mathbb{C}\setminus\{0\}$ und jede natürliche Zahl $n \in \mathbb{N}$

Potenz

$$\left(\cos(\varphi) + \mathrm{i}\sin(\varphi)\right)^n = \cos(n\varphi) + \mathrm{i}\sin(n\varphi)$$

$$z^n = r^n\left(\cos(\varphi) + \mathrm{i}\sin(\varphi)\right)^n = r^n\left(\cos(n\varphi) + \mathrm{i}\sin(n\varphi)\right)$$

n-te Wurzel

$$z_k = \sqrt[n]{r}\left(\cos\left(\frac{\varphi + 2k\pi}{n}\right) + \mathrm{i}\sin\left(\frac{\varphi + 2k\pi}{n}\right)\right),\ k = 0,\ 1, \ldots, n-1$$

Lineare Gleichungssystem (LGS)

$$\begin{aligned} a_{11}x_1 &+ \cdots + a_{1n}x_n &&= b_1 \\ a_{21}x_1 &+ \cdots + a_{2n}x_n &&= b_2 \\ &\vdots && \vdots \\ a_{m1}x_1 &+ \cdots + a_{mn}x_n &&= b_m \end{aligned} \quad \text{mit} \quad a_{ij}, b_i \in \begin{cases} \mathbb{R} & \text{(reelles LGS)} \\ \mathbb{C} & \text{(komplexes LGS)} \end{cases}$$

Zeilenindex
Variablenindex

Matrixschreibweise

$$\longleftrightarrow \quad \overbrace{\underbrace{\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)}_{\text{erw. Koeffizientenmatrix } (A \mid b)}}^{\text{Koeffizientenmatrix } A} .$$

Ein n-**Tupel** $(\ell_1, \ldots, \ell_n) \in \mathbb{R}^n$ heißt **Lösung** des LGS, falls für alle $i = 1, \ldots, m$ gilt:

$$a_{i1}\,\ell_1 + \cdots + a_{in}\,\ell_n = b_i .$$

Das Gauß'sche Eliminationsverfahren

Elementare Zeilenumformungen

- Vertauschen zweier Zeilen.
- Multiplikation einer Zeile mit einem $\lambda \neq 0$.
- Addition eines λ-Fachen einer Zeile zu einer anderen Zeile.

Rang einer Matrix

$$M \rightsquigarrow M' = \left(\begin{array}{ccccc} * & * & * & * & * \\ & * & * & * & \vdots \\ & & * & * & * \\ 0 & & & & 0 \end{array}\right) \begin{array}{l} \Big\} \; r \text{ Zeilen ungleich } 0 \ldots 0 \\ \qquad \text{Rang von } M \quad r = \operatorname{rg}(M) \\ \Big\} \; s - r \text{ Zeilen gleich } 0 \ldots 0, \end{array}$$

Zeilenstufenform

$$\begin{array}{l} ax + by = c \\ a'x + b'y = c' \end{array} \rightarrow \begin{array}{lcll} ax & + & by & = c \\ \underbrace{(a' + \lambda a)}_{=0}\,x & + & (b' + \lambda b)y & = c' + \lambda c \end{array}$$

Lösbarkeit und Lösungsmenge

a) Eindeutig lösbar (eindeutige Lösung)

→ keine Widerspruchzeile
→ Variablen-Anzahl = Gleichung-Anzahl
→ ohne Nullzeilen $\operatorname{rg}(A) = n$

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 2 \\ 2 & 2 & -1 & 1 \\ 3 & 4 & 2 & 2 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 1 & 2 & 2 \\ 0 & 1 & -4 & -4 \\ 0 & 0 & -5 & -3 \end{array}\right)$$

$$L = \{(12/5,\ -8/5,\ 3/5)\}$$

homogenes LGS

b) unendlich viele Lösungen

→ keine Widerspruchzeile
→ Variablen-Anzahl > Gleichung-Anzahl
→ mindestens eine Nullzeile

Anzahl der freien Parameter $= n - \operatorname{rg}(A)$

$$\begin{array}{l} 2x + 4y = 2 \\ 3x + 6y = 3 \\ 5x + 10y = 5 \end{array} \leftrightarrow \left(\begin{array}{cc|c} 2 & 4 & 2 \\ 3 & 6 & 3 \\ 5 & 10 & 5 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

$$L = \{(1 - 2\lambda, \lambda) \mid \lambda \in \mathbb{R}\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} -2 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

c) nicht lösbar (leere Lösung)

inhomogenes LGS

→ eine Widerspruchzeile

$$\begin{array}{l} x + 2y + 3z = 4 \\ 2x + 4y + 6z = 10 \end{array} \leftrightarrow \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 2 & 4 & 6 & 10 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 2 \end{array}\right) \quad L = \emptyset.$$

ungleich 0

Matrizen

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = (a_{ij})_{m,n} = (a_{ij})$$

m Zeilen

Eintrag / Koeffizient

n Spalten

reelle Matrix $\mathbb{R}^{m\times n} = \{(a_{ij})_{m,n} \mid a_{ij} \in \mathbb{R}\}$

komplexe Matrix $\mathbb{C}^{m\times n} = \{(a_{ij})_{m,n} \mid a_{ij} \in \mathbb{C}\}$

Gleichheit $A = (a_{ij})$ und $B = (b_{ij})$ $\Leftrightarrow$ A und B gleich viele Zeilen und Spalten haben, $a_{ij} = b_{ij}$ für alle i, j gilt

Besondere Matrizen

- Die $m \times 1$-Matrizen bzw. $1 \times n$-Matrizen

$$s = \begin{pmatrix} s_1 \\ \vdots \\ s_m \end{pmatrix} \in \mathbb{K}^{m\times 1} = \mathbb{K}^m \text{ bzw. } z = (z_1, \dots, z_n) \in \mathbb{K}^{1\times n}$$

  heißen **Spalten** oder **Spaltenvektoren** bzw. **Zeilen** oder **Zeilenvektoren.**

- Die Matrix

$$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \in \mathbb{K}^{m\times n}$$

  heißt $m \times n$-**Nullmatrix.**

- Ist $m = n$, also $A \in \mathbb{K}^{n\times n}$, so heißt A **quadratische Matrix.** Die wichtigsten quadratischen Matrizen sind:
  - **Diagonalmatrizen:**

$$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \operatorname{diag}(\lambda_1, \dots, \lambda_n),$$

  - die $n \times n$-**Einheitsmatrix** $E_n = \operatorname{diag}(1, \dots, 1)$ mit den **Standardeinheitsvektoren** als Spalten:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \in \mathbb{K}^n,$$

  - **obere** und **untere Dreiecksmatrizen**

$$O = \begin{pmatrix} * & \dots & * \\ & \ddots & \vdots \\ 0 & & * \end{pmatrix} \text{ und } U = \begin{pmatrix} * & & 0 \\ \vdots & \ddots & \\ * & \dots & * \end{pmatrix}.$$

Rechenoperation

- **Transponieren:** Zu $A = (a_{ij}) \in \mathbb{K}^{m\times n}$ bezeichnet $A^\top = (a_{ji}) \in \mathbb{K}^{n\times m}$ die **zu** A **transponierte Matrix** oder das **Transponierte** von A:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \xrightarrow{\text{Transponieren}} A^\top = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}.$$

- **Addition:** Zu zwei Matrizen $A = (a_{ij}),\ B = (b_{ij}) \in \mathbb{K}^{m\times n}$ bezeichnet $A + B = (a_{ij} + b_{ij}) \in \mathbb{K}^{m\times n}$ die **Summe:**

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \cdots & a_{1n}+b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & \cdots & a_{mn}+b_{mn} \end{pmatrix}.$$

- **Multiplikation mit Skalaren:** Zu $\lambda \in \mathbb{K}$ und $A = (a_{ij}) \in \mathbb{K}^{m\times n}$ bezeichnet $\lambda \cdot A = (\lambda\, a_{ij}) \in \mathbb{K}^{m\times n}$ das **skalare Vielfache** von A:

$$\lambda \cdot \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} = \begin{pmatrix} \lambda\, a_{11} & \cdots & \lambda\, a_{1n} \\ \vdots & \ddots & \vdots \\ \lambda\, a_{m1} & \cdots & \lambda\, a_{mn} \end{pmatrix}.$$

- **Multiplikation von Matrizen:** Zu zwei Matrizen $A = (a_{ij}) \in \mathbb{K}^{m\times n}$ und $B = (b_{jk}) \in \mathbb{K}^{n\times p}$ bezeichnet $A \cdot B = (\sum_{j=1}^{n} a_{ij} b_{jk})_{ik} \in \mathbb{K}^{m\times p}$ das **Produkt:**

Spaltenanzahl$_A$ = Zeilenanzahl$_B$

$$A \cdot B = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix} \cdot (s_1, \ldots, s_p) = \begin{pmatrix} z_1 \cdot s_1 & \ldots & z_1 \cdot s_p \\ \vdots & & \vdots \\ z_m \cdot s_1 & \ldots & z_m \cdot s_p \end{pmatrix}.$$

- Wir setzen außerdem für jedes $A \in \mathbb{K}^{n\times n}$ und $k \in \mathbb{N}$:

$$A^k = \underbrace{A \cdot A \cdot \ldots \cdot A}_{k\text{-mal}} \quad \text{und} \quad A^0 = E_n.$$

quadratische Matrix A

symmetrisch, falls $A^\top = A$

schiefsymmetrisch, falls $A^\top = -A$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{pmatrix} \qquad \begin{pmatrix} 0 & 2 & 3 \\ -2 & 0 & 5 \\ -3 & -5 & 0 \end{pmatrix}$$

$(m \times n) \cdot (n \times p) = m \times p$

Matrizenmultiplikation nicht kommutativ $\quad (A+B)^2 \neq A^2 + 2AB + B^2$

Elementarmatrix

Die Multiplikation einer Elementarmatrix E von links an eine Matrix A bewirkt

- die Vertauschung von k-ter und l-ter Zeile, falls $E = P_{kl}$,
- die Vervielfachung der k-ten Zeile mit λ, falls $E = D_k(\lambda)$,
- die Addition des λ-Fachen der l-ten Zeile zur k-ten Zeile, falls $E = N_{kl}(\lambda)$,

$$P_{kl}\begin{pmatrix}\vdots\\ z_k\\ \vdots\\ z_l\\ \vdots\end{pmatrix} = \begin{pmatrix}\vdots\\ z_l\\ \vdots\\ z_k\\ \vdots\end{pmatrix}, \quad D_k(\lambda)\begin{pmatrix}\vdots\\ z_k\\ \vdots\\ z_l\\ \vdots\end{pmatrix} = \begin{pmatrix}\vdots\\ \lambda z_k\\ \vdots\\ z_l\\ \vdots\end{pmatrix}, \quad N_{kl}(\lambda)\begin{pmatrix}\vdots\\ z_k\\ \vdots\\ z_l\\ \vdots\end{pmatrix} = \begin{pmatrix}\vdots\\ z_k + \lambda z_l\\ \vdots\\ z_l\\ \vdots\end{pmatrix}.$$

$$P_{kl} = \begin{pmatrix} & & & k & & l & & \\ & & & \downarrow & & \downarrow & & \\ 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 0 & & 1 & & & \\ & & & \ddots & & & & \\ & & 1 & & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \end{pmatrix} \quad = P_{kl}$$

$$D_k(\lambda) = \begin{pmatrix} & & & k & & & \\ & & & \downarrow & & & \\ 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \quad = D_k(\lambda)$$

$$N_{kl}(\lambda) = \begin{pmatrix} & & & k & & l & & \\ & & & \downarrow & & \downarrow & & \\ 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & \lambda & & & \\ & & & \ddots & & & & \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \end{pmatrix} \quad = N_{kl}(\lambda)$$

Matrix invertieren

Mit $E_n = (e_1, \ldots, e_n)$ und $X = (s_1, \ldots, s_n)$ lautet $A\,X = E_n$

$A\,X = (A\,s_1, \ldots, A\,s_n) = (e_1, \ldots, e_n)$, also $A\,s_i = e_i$ für $i = 1, \ldots, n$.

Rezept: Invertieren einer Matrix

Eine Matrix $A \in \mathbb{K}^{n\times n}$ ist genau dann invertierbar, wenn $\operatorname{rg}(A) = n$ gilt.
Ist $A \in \mathbb{K}^{n\times n}$ invertierbar, so erhält man das Inverse A^{-1} durch simultanes Lösen von n Gleichungssystemen:

(1) Notiere die erweiterte Koeffizientenmatrix $(A \mid E_n)$.
(2) Führe elementare Zeilenumformungen durch, bis links die reduzierte Zeilenstufenform E_n erreicht ist:

$$(A \mid E_n) \rightsquigarrow \ldots \rightsquigarrow (E_n \mid B).$$

(3) Es gilt dann $B = A^{-1}$.

$\operatorname{rg}(A) < n$ **falls gibts Nullzeilen -> Matrix A ist nicht invertierbar**

Rechenregel

Sind $A, B, C \in \mathbb{K}^{m\times n}$ und $\lambda, \mu \in \mathbb{K}$, so gelten:

- Die **Vektorraumaxiome:** (Addition)
  - $A + B = B + A$,
  - $(A + B) + C = A + (B + C)$,
  - $A + 0 = A$,
  - $A + (-A) = 0$,
  - $(\lambda\mu)A = \lambda(\mu A)$,
  - $1 \cdot A = A$,
  - $(\lambda + \mu)A = \lambda A + \mu A$,
  - $\lambda(A + B) = \lambda A + \lambda B$.

- Die Regeln für das Transponieren:
  - $(A + B)^\top = A^\top + B^\top$,
  - $(\lambda A)^\top = \lambda A^\top$,
  - $(A^\top)^\top = A$.

Sind $A, B, C \in \mathbb{K}^{n\times n}$ quadratische Matrizen,

- Die Regeln für die Multiplikation:
  - $(AB)C = A(BC)$,
  - $A(B + C) = AB + AC$,
  - $(A + B)C = AC + BC$,
  - $E_n \cdot A = A = A \cdot E_n$,
  - $(AB)^\top = B^\top A^\top$.

- Die Regeln für das Invertieren:
  - $(A^{-1})^{-1} = A$,
  - $(AB)^{-1} = B^{-1}A^{-1}$

- Die zwei wichtigen Regeln für die Inversen von 2×2- bzw. Diagonalmatrizen:
  - $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \Rightarrow A^{-1} = \frac{1}{ad-bc}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, falls $ad - bc \neq 0$,
  - $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n) \Rightarrow D^{-1} = \operatorname{diag}(\lambda_1^{-1}, \ldots, \lambda_n^{-1})$, falls $\lambda_1, \ldots, \lambda_n \neq 0$.

Gruppen

Die Menge mit der Verknüpfung $\circ$ heißt Gruppe, wenn die folgende Eigenschaften erfüllt:

1. A **ist in** $\circ$ **abgeschlossen** $\quad \forall a, b \in A : a \circ b \in A$
2. **Die Einschränkung von** $\circ$ **auf** A **ist assoziativ** $\quad \forall a, b, c \in A : (a \circ b) \circ c = a \circ (b \circ c)$
3. A **besitzt ein neutrales Element bezüglich** $\circ$ $\quad \exists e \in A : \forall a \in A : a \circ e = a = e \circ a$
4. **Jedes Element aus** A **besitzt ein inverses Element bezüglich** $\circ$ $\quad \forall a \in A : \exists a^{-1} \in A : a \circ a^{-1} = e = a^{-1} \circ a$

Untergruppen

Sind $(G, *)$ eine Gruppe und H eine Teilmenge von G, so ist H dann eine Untergruppe von G, wenn gilt:

1. H **ist nicht die leere Menge**
2. **Für alle** $x \in H$ **ist zugleich** $x^{-1} \in H$
3. **Aus** $x, y \in H$ **folgt stets** $(x \circ y) \in H$

Ordnung von Gruppenelemente

Sei G eine Gruppe mit neutralen Element e, und es sei $a \in \mathbb{G}$

a) falls $Ord(a) = |\langle a\rangle| = \infty$, **dann** $a^i \neq a^j, i \neq j$

b) falls $Ord(a) \in \mathbb{N}$, **so gilt** $Ord(a) = |\langle a\rangle| = n$ **(n ist die kleinst natürliche Zahl, für** $a^n = e$ **gilt**

(i) $\langle a\rangle = \{e, a_1, \ldots, a^{n-1}\}$ $\quad s = nq + r \quad \Rightarrow \quad a^{qn+r} = (a^n)^q \cdot a^r = e^q * a^r = e * a^r = a^r,\ r \in \{0, 1, \ldots, n-1\}$

(ii) **Für** $s \in \mathbb{N} : a^s = e \Leftrightarrow n|s$ **(n ist Teiler von s)** $\quad s = nq \quad \Rightarrow \quad a^s = a^{nq} = (a^n)^q = e^q = e$

Satz von Lagrange: Für jede Untergruppe (H, o) einer endlichen Gruppe (G, o) gilt: $|H|$ teilt $|G|$

-> folgt: Für alle Elemente $a \in G$ einer endlichen Gruppe (G, o) gilt: $ord(a)$ teilt $|G|$

Satz von Euler: Sind $a, n \in \mathbb{N}$ zueinander teilerfremd, dann gilt: $a^{\varphi(n)} \equiv_n 1$ bzw. $a^{|G|} \equiv_n e$

Ringe

Eine Algebra $(A, \oplus, \odot)$ mit zwei inneren Verknüpfungen heißt Ring, falls folgendes gilt:

- $(A, \oplus)$ ist eine kommutative Gruppe mit neutralem Element $0 \in A$ (additive Gruppe)
- $(A, \odot)$ ist ein Monoid mit neutralem Element $1 \in A$ (multiplikatives Monoid) bzw. $ae = a = ea$
- assoziativ $(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$
- $\oplus$ und $\odot$ sind distributiv, d.h. für alle $a, b, c \in A$ gilt: $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$
  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$
- $(A, \odot)$ ist (nur manchmal) kommutativ, falls $a \cdot b = b \cdot a$ gilt

Körper

Eine Algebra $(A, \oplus, \odot)$ mit zwei Operatoren heißt Körper, falls folgendes gilt:

- $(A, \oplus)$ ist eine kommutative Gruppe mit neutralem Element $0 \in A$ (additive Gruppe)
- $(A \backslash \{0\}, \odot)$ ist eine kommutative Gruppe mit neutralem Element $1 \in A$ (multiplikatives Monoid)
- $\oplus$ und $\odot$ sind distributiv, d.h. für alle $a, b, c \in A$ gilt: $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$

Körper -> Ring mit Eigenschaft: $\mathbb{R}^* = \mathbb{R} \backslash \{\bar{0}\}$ jedes Element ungleich 0 -> invertierbar

z.B. $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ da $\bar{2} \cdot \bar{4} = \bar{8} = \bar{0}$, $\bar{6}$ enthält Faktor $\bar{2}$

Ringe vs Körper

1. Alle Elemente eines Körpers (außer die 0) haben Inverse bzgl. $\odot$, die eines Ringes nur manchmal.
2. $\odot$ ist bei Körpern immer kommutativ, bei Ringen nur manchmal.
3. Körper sind immer nullteilerfrei, Ringe nur manchmal.

Nullteiler

Sei $(R, \oplus, \odot)$ ein Ring. Zwei Elemente $a, b \in R$ mit $a, b \neq 0$ heißen Nullteiler, falls $a \odot b = 0$ gilt

Falls R keine Nullteiler besitzt, nennt man R nullteilerfrei

a ist teilerfremd zu n, dann ist a invertierterbar, sonst nicht invertierbar

Einheitengruppe $\mathbb{R}^\times = \{a \in \mathbb{R} \mid \text{a ist invetierbar})\} = \{a \in \mathbb{R} \mid \exists b \in \mathbb{R} \cdot a \cdot b = b \cdot a = 1\}$

Menge aller multiplikativ invertierbaren Elemente von R mit Einselement 1 bildet Einheitengruppe

Restklassen modulo n

Für $n \in \mathbb{N}$ ist additive Gruppe $(\mathbb{Z}_n, +_n, \cdot_n)$ ein kommutativer, endlicher Ring -> "Restklassenring modulo n"

$(\mathbb{Z}_n, +_n, \cdot)$ ist ein Körper $\iff$ n ist Primzahl p $\quad \mathbb{Z}_p^* = \left\{\overline{1}, \overline{2}, \overline{3}, \cdots, \overline{p-1}\right\} = \mathbb{Z}_p \backslash \{\overline{0}\}$

$\bar{a} := a + n\mathbb{Z} = \{a, a+n, a+2n, a+3n \ldots, a-2n, a-n\}$

$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ -> Restklassen modulo n

n=5 $\quad \overline{3} + \overline{4} = \overline{7} \equiv_5 \overline{2}$ $\quad \overline{3} \cdot \overline{4} = \overline{12} \equiv_5 \overline{2}$

$a \equiv b \,(mod\, n) \iff n \mid a-b$ und $\bar{a} = \bar{b}$ $\quad a + n\mathbb{Z} = b + n\mathbb{Z}$

"a konjugiert b modulo n": falls a, b den gleichen Rest bei Division durch n mit Rest haben

Prime Restklassengruppen modulo n (a und b muss nicht prim sein)

a und b sind teilerfremd (relativ prim) -> haben keine gemeinsame Teiler außer 1

$\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n \mid \bar{a} \text{ ist invertierbar }\} = \left\{\bar{a} \in \mathbb{Z}_n \mid \exists \bar{b} \in \mathbb{Z}_n : \bar{a}\bar{b} = 1\right\} = \{\bar{a} \in \mathbb{Z}_n \mid ggT(a,b) = 1\}$

Verknüpfungstafel von Ringen

additive Gruppe n = 6

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

multiplikative Gruppe n = 6

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

1 und 5 sind teilerfremd zu 6 → invertierbar

Erweiterte euklidische Algorithmus (Lemma von Bézout)

Für zwei beliebige natürliche Zahlen $a, b \in N_0$ existieren ganze Zahlen $r, s \in \mathbb{Z}$

$ggT(a,b) = \bar{a} * \bar{r} + \bar{b} * \bar{s} = d \qquad \mathbb{Z}_n^* = |\{\bar{a} \in \mathbb{Z}_n^* \mid ggT(a,b) = 1\} \qquad a^{-1} = r$

Die eulersche Phi-Funktion gibt die Anzahl der Elemente in $\mathbb{Z}_n^*$ an

$\varphi(n) := |\mathbb{Z}_n^*| = |\{a \in \{1, \ldots, n\} \mid ggT(a,n) = 1\}| = n \prod_{p \in \mathbb{P}: p|n} \left(1 - \frac{1}{p}\right)$

Für Primzahl p gilt $\varphi(p) := p - 1$

Für Primzahlen p, q gilt $\varphi(pq) := (p-1)(q-1)$

Der kleine Satz von Fermat: Sei p prim

$\forall a \in \mathbb{Z}$ mit $ggT(a,p) = 1$ gilt $a^{p-1} \equiv 1 \bmod p$

$\forall a \in \mathbb{Z}$ gilt $a^p \equiv a \bmod p$

Rechnen mit Kongruenzen

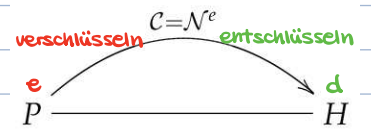
Für beliebige $a, b, n \in \mathbb{N}$ gilt:

1. $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$,
2. $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$,
3. $(a \cdot b) \bmod (a \cdot n) = a \cdot (b \bmod n)$.

$$\begin{matrix} a \equiv b \ (\bmod n) \\ c \equiv d \ (\bmod n) \end{matrix} \Rightarrow \begin{matrix} a + c \equiv b + d \ (\bmod n) \\ ac \equiv bd \ (\bmod n) \end{matrix}$$

Kryptosystem

Das Pohlig-Hellman-Verfahren (Nachricht chiffrieren und dechiffrieren)



Der Sender $\mathcal{P}$ verschlüsselt seine Nachricht mit dem geheimen Schlüssel e mit $ggT(e, p-1) = 1$ und sendet diesen Geheimtext $\mathcal{C}$ an $\mathcal{H}$

-- Verschlüsselungsfunktion $f : \mathcal{N} \times \mathcal{K} \to \mathcal{C}$ definiert durch $f(\mathcal{N}, e) = f_e(\mathcal{N}) = \mathcal{N}^e$ für $e \in \mathcal{K}$

Der Empfänger $\mathcal{H}$ entschlüsselt den Geheimtext $\mathcal{C}$ mithilfe der Zahl d mit $de \equiv 1(\bmod p-1)$ und erhält so den Klartext $\mathcal{N}$

-- Entschlüsselungsfunktion $g : \mathcal{C} \times \mathcal{K} \to \mathcal{N}$ definiert durch $g(\mathcal{C}, d) = g_d(\mathcal{C}) = \mathcal{C}^d = \mathcal{N}^{ed} = \mathcal{N}$ für $d \in \mathcal{K}$

Das RSA-Verfahren (Modifikation des Pohlig-Hellman-Verfahrens)

Besonderheit: Der Schlüssel e und Gemientext $\mathcal{C}$ ist öffentlich zuganglich, aber nur R kennt den geheimen Schlüssel d

Will der Sender $\mathcal{S}$ an den Empfänger $\mathcal{R}$ eine Nachricht $\mathcal{N}$ senden, so sucht $\mathcal{S}$ in einem öffentlichen Verzeichnis den öffentlichen Schlüssel e von $\mathcal{R}$, wendet ihn auf seinen Klartext $\mathcal{N}$ an und sendet dann $\mathcal{R}$ den so erhaltenen Geheimtext $\mathcal{C} = e(\mathcal{N})$. Der Emptänger $\mathcal{R}$ hat einen geheimen Schlüssel d. Mit ihm kann er aus dem Geheimtext $\mathcal{C}$ den Klartext $\mathcal{N}$ wiederherstellen $\mathcal{N} = d(e(\mathcal{N}))$

Beispiel-Beweis

R wählt zwei Primzahlen $p \neq q$ und berechnet $n := pq,\ \varphi(n) = (p-1)(q-1)$

R wählt ein $e \in \mathbb{N}$ mit $\mathrm{ggT}(e, \varphi(n)) = 1$ und berechnet $d \in \mathbb{N}$ mit $ed \equiv 1(\bmod \varphi(n)) = 1 + r * \varphi(n) = 1 + r(p-1)(q-1)$

$$\begin{matrix} a^{ed} \equiv a^{1+r(p-1)(q-1)} \equiv a\left(a^{p-1}\right)^{r(q-1)} \equiv a(\bmod p) & \longrightarrow & p \mid a^{ed} - a \\ a^{ed} \equiv a^{1+r(p-1)(q-1)} \equiv a\left(a^{q-1}\right)^{r(p-1)} \equiv a(\bmod q) & \longrightarrow & q \mid a^{\mathrm{ed}} - a \end{matrix} \Rightarrow$$

Da p und q verschiedene Primzahlen sind,

$pq \mid a^{ed} - a$ **, d.h.** $a^{ed} \equiv a(\bmod n)$

Der Empfänger $\mathcal{R}$ R erhält den Geheimtext $\mathcal{C} = \mathcal{N}^e \in \mathbb{Z}_n$ und berechnet mit geheimen Schlüssel d den Klartext $\mathcal{C}^d = \mathcal{N}^{\mathrm{ed}} = \mathcal{N} \in \mathbb{Z}_n$

Vektorräume

Eine nichtleere Menge V mit einer Addition $+$ und einer Multiplikation $\cdot$ heißt ein **Vektorraum über** $\mathbb{K}$ oder ein $\mathbb{K}$**-Vektorraum,** wenn für alle $u, v, w \in V$ und für alle $\lambda, \mu \in \mathbb{K}$ gilt:

(1)	$v + w \in V, \quad \lambda v \in V,$	(Abgeschlossenheit)
(2)	$u + (v + w) = (u + v) + w,$	(Assoziativität)
(3)	Es gibt ein Element $0 \in V:$ $\quad v + 0 = v$ für alle $v \in V,$	(Nullelement)
(4)	Es gibt ein Element $v' \in V:$ $\quad v + v' = 0$ für alle $v \in V,$	(negatives Element)
(5)	$v + w = w + v$ für alle $v, w \in V,$	(Kommutativität)
(6)	$\lambda (v + w) = \lambda v + \lambda w,$	(Distributivität)
(7)	$(\lambda + \mu) v = \lambda v + \mu v,$	(Distributivität)
(8)	$(\lambda \mu) v = \lambda (\mu v),$	(Assoziativität)
(9)	$1 \cdot v = v.$	

Nullvektor

inverse Vektor

Rechenregeln

$0\, v = 0$ und $\lambda\, 0 = 0.$

$\lambda\, v = 0 \;\Rightarrow\; \lambda = 0$ oder $v = 0.$

Vier wichtigste Beispiele von K-Vektorräume

Menge für alle natürliche Zahlen $n \in \mathbb{N}$

$$\mathbb{K}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, \ldots, x_n \in K \right\}$$

Vektoraddition $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$

Multiplikation mit Skalaren $\lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$

Nullvektor $0 = (0, \ldots, 0)^\top$

inverse Vektor $v = (v_1, \ldots, v_n)^\top$ -> $-v = (-v_1, \ldots, -v_n)^\top$

Menge aller $m \times n$ - Matrizen über $\mathbb{K}$

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

Vektoraddition $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$

Multiplikation mit Skalaren $\lambda \cdot (a_{ij}) = (\lambda a_{ij})$

Nullvektor **Nullmatrix** $0 = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$

inverse Vektor $v = (a_{ij})$ -> $-v = (-a_{ij})$

Menge aller Polynome über $\mathbb{K}$

$\mathbb{K}[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid n \in \mathbb{N}_0, a_i \in \mathbb{K}\}$

Vektoraddition $\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$

Multiplikation mit Skalaren $\lambda \cdot \sum a_i x^i = \sum (\lambda a_i) x^i$

Nullvektor **Nullpolynom** $\sum 0 x^i$

inverse Vektor $p = \sum a_i x^i$ -> $-p = \sum (-a_i) x^i$

Menge aller Abbildungen von $\mathbb{M}$ nach $\mathbb{K}$

$\mathbb{K}^M = \{f \mid f : M \to \mathbb{K}$ Abbildung $\}$

Vektoraddition $f + g : \begin{cases} M & \to \mathbb{K} \\ x & \mapsto f(x) + g(x) \end{cases}$

Multiplikation mit Skalaren $\lambda \cdot f : \begin{cases} M & \to \mathbb{K} \\ x & \mapsto \lambda f(x) \end{cases}$

Nullvektor $0 : \begin{cases} M \to \mathbb{K} \\ x \mapsto 0 \end{cases}$

inverse Vektor $f : \begin{cases} M \to \mathbb{K} \\ x \mapsto f(x) \end{cases}$ -> $-f : \begin{cases} M \to \mathbb{K} \\ x \mapsto -f(x) \end{cases}$

Rezept: Nachweis für Untervektorraum

Gegeben ist eine Teilmenge U eines Vektorraums V. Begründe:

(1) $0 \in U$,
(2) $u, v \in U \Rightarrow u + v \in U$,
(3) $u \in U, \lambda \in \mathbb{K} \Rightarrow \lambda u \in U$.

Die Teilmenge U von V ist dann ein Untervektorraum von V und als solcher ein $\mathbb{K}$-Vektorraum.

Linearekombinationen

Sind $v_1, \ldots, v_n \in V$ verschiedene Vektoren eines $\mathbb{K}$-Vektorraums V und $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$

so nennt man den Vektor $v = \lambda_1 v_1 + \cdots + \lambda_n v_n = \sum_{i=1}^{n} \lambda_i v_i \in V$ eine Linearkombination von $v_1, \ldots, v_n$

Rezept: Darstellen eines Vektors als Linearkombination

Gegeben sind Vektoren v und $v_1, \ldots, v_n$ eines gemeinsamen $\mathbb{K}$-Vektorraums V. Um zu prüfen, ob v eine Linearkombination von $v_1, \ldots, v_n$ und v als Linearkombination dieser Vektoren zu schreiben ist, gehe man wie folgt vor:

(1) Mache den Ansatz $\lambda_1 v_1 + \cdots + \lambda_n v_n = v$ in den Unbestimmten $\lambda_1, \ldots, \lambda_n$.
(2) Entscheide, ob die Gleichung in (1) eine Lösung $\lambda_1, \ldots, \lambda_n$ hat oder nicht.
Falls ja, so ist v eine Linearkombination von $v_1, \ldots, v_n$, nächster Schritt.
Falls nein, so ist v keine Linearkombination von $v_1, \ldots, v_n$.
(3) Bestimme eine Lösung $\lambda_1, \ldots, \lambda_n$ der Gleichung in (1) und erhalte die gesuchte Darstellung für v.

Im Fall $V = \mathbb{K}^n$ liefert der Ansatz in (1) ein lineares Gleichungssystem (falls eindeutig lösbar -> v Linearkombination)

Im Fall $V = \mathbb{K}^{m \times n}$ liefert der Ansatz in (1) einen Koeffzientenvergleich von Matrizen (falls eindeutig lösbar -> v Linearkombination)

Im Fall $V = \mathbb{K}[x]$ liefert der Ansatz in (1) einen Koeffzientenvergleich von Polynomen (falls eindeutig lösbar -> v Linearkombination)

Im Fall $V = \mathbb{K}^M$ liefert der Ansatz in (1) einen Wertevergleich von Funktionen (nicht lösbar -> keine Linearkombination)

span(X) =

Erzeugnis von X (lineare Hille von X) $\langle X \rangle = \left\{ \sum_{i=1}^{n} \lambda_i v_i \mid n \in \mathbb{N}, \lambda_1 \ldots, \lambda_n \in \mathbb{K}, v_1, \ldots, v_n \in X \right\} \subseteq V$

Definition: die Menge aller Linearkombinationen von X (eine nichtleere Teilmenge eines $\mathbb{K}$-Vektorraums V)

$X \subseteq \langle X \rangle$

$\langle X \rangle$ ist ein Untervektorraum von V

$\langle X \rangle$ ist der kleinste Untervektorraum U von V mit $X \subseteq U$

$\langle X \rangle$ ist der Durchschnitt aller Untervektorraume von V, die X enthalten $\langle X \rangle = \bigcap_{\substack{UVR \text{ von } v \\ X \subseteq U}} U$

Ist X endlich, also $X = \{v_1, \ldots, v_n\}$, so gilt $\langle X \rangle = \langle v_1, \ldots, v_n \rangle = \left\{ \sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in \mathbb{K} \right\} = \mathbb{K}v_1 + \cdots + \mathbb{K}v_n$

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

$\langle X \rangle = U$ -> **X erzeugt den Vektorraum U oder X ist ein Erzeugendensystem von U**

Lineare (Un-)Abhängigkeit

- Vektoren $v_1 \dots, v_n \in V$ heißen linear unabhängig, wenn für jede echte Teilmenge $T \subsetneq \{v_1, \dots, v_n\}$ gilt $\langle T \rangle \subseteq \langle v_1, \dots, v_n \rangle$

- Vektoren $v_1 \dots, v_n \in V$ heißen linear abhängig, wenn sie nicht linear unabhängig sind, gilt:

linear abhängig $\Leftrightarrow$ $\exists T \subsetneq \{v_1, \dots, v_n\}$ mit $\langle T \rangle = \langle v_1, \dots, v_n \rangle$

Rezept: Nachweis der linearen (Un-)Abhängigkeit

Gegeben ist eine Teilmenge $X \subseteq V$ des $\mathbb{K}$-Vektorraums V mit dem Nullvektor 0_V. Wir untersuchen die Menge X auf lineare (Un-)Abhängigkeit:

(1) Mache den Ansatz $\lambda_1 v_1 + \dots + \lambda_n v_n = 0_V$ mit $\lambda_1, \dots, \lambda_n \in \mathbb{K}$, wobei
   - $X = \{v_1, \dots, v_n\}$, falls X endlich ist, bzw.
   - $v_1, \dots, v_n \in X$ eine beliebige endliche Wahl von Elementen aus X ist, falls X nicht endlich ist.

(2) Falls die Gleichung in (1) nur für $\lambda_1 = \dots = \lambda_n = 0$ möglich ist, so ist X linear unabhängig.
Falls die Gleichung in (1) für $\lambda_1, \dots, \lambda_n$ möglich ist und dabei nicht alle $\lambda_i = 0$ sind, so ist X linear abhängig.

Nullvektor 0 ist linear abhängig denn $\lambda 0 = 0$ -> $\lambda = 0$ muss nicht gelten

Ist $v \neq 0$, so ist v linear unabhangig denn $\lambda v = 0$ -> $\lambda = 0$ muss gelten

Für alle natürlichen Zahlen $n \in \mathbb{N}$ sind die Standardeinheitsvektoren $e_1, \dots, e_n$ linear unabhangig

denn $\lambda_1 e_1 + \dots + \lambda_n e_n = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ -> $\lambda_1 = \dots = \lambda_n = 0$

drei Vektoren sind linear abhangig denn $\lambda_1 v_1 + \lambda_2 v_2 + \lambda_3 v_3 = 0$ -> $\lambda = 0$ muss nicht gelten

Die (unendliche) Menge $\{1, x, x^2, x^3, \dots\} \in \mathbb{R}[x]$ ist linear unabhangig

denn $\lambda_1 x^{r_1} + \dots + \lambda_n x^{r_n} = 0$ -> beim Nullpolynom $\sum 0x^i$ gilt $\lambda_1 = \dots = \lambda_n = 0$

Die Vektoren $\sin, \cos \in \mathbb{R}^{\mathbb{R}}$ sind linear unabhangig

mit der Nullfunktion 0 gilt $\lambda_1 \cos(x) + \lambda_2 \sin(x) = 0(x) = 0$

für $x = 0$ gilt -> $\sin(0) = 0$ hat $\lambda_1 = 0$ zur Folge

für $x = \pi/2$ gilt $\lambda_1 \cos(\pi/2) + \lambda_2 \sin(\pi/2) = 0$ -> $\cos(\pi/2)$ hat $\lambda_2 = 0$ zur Folge

Basen von Vektorräumen

Eine Teilmenge B eines K-Vektorraums V heißt Basis von V, falls es gleichzeitig gilt:

1) B ein Erzeugendensystem von V ist, $\langle B \rangle = V$ **2) B linear unabhängig ist**

äquivalente Kennzeichnungen von Basen

(i) ist eine Basis von V

(ii) ist ein maximale linear unabhängige Teilmenge von V

d.h. ist linear unabhängig und für iedes $v \in V \backslash B$ ist $B \cup \{v\}$ linear abhängig

(iii) ist ein minimales Erzeugendensvstem von V

d.h. erzeugt V und für jedes $v \in B$ gilt $B \backslash \{v\}$ erzeugt V nicht)

Merkregeln (wichtige Sätze)

- **Existenzsätze:**
  - Jeder $\mathbb{K}$-Vektorraum V besitzt eine Basis.
  - Jedes Erzeugendensystem von V enthält eine Basis von V. — Basisverkürzungssatz
  - Jede linear unabhängige Teilmenge von V kann zu einer Basis ergänzt werden. — Basisergänzungssatz
- **Eindeutige Darstellbarkeit:** Ist B eine Basis von V, so ist jedes $v \in V$ bis auf die Reihenfolge der Summanden eindeutig als Linearkombination von B darstellbar, d. h. jedes $v \in V$ ist von der Reihenfolge der Summanden abgesehen auf genau eine Art und Weise in der Form

$$v = \lambda_1 b_1 + \cdots + \lambda_r b_r$$

  mit $b_1, \ldots, b_r \in B$ und $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$ darstellbar.
- **Gleichmächtigkeit von Basen:** Je zwei Basen B und B' von V haben gleich viele Elemente.
- **Dimensionsbegriff:** Ist B eine Basis des $\mathbb{K}$-Vektorraums V, so nennt man $|B|$ die **Dimension** von V. Man schreibt $\dim(V)$ für die Dimension.
- **Nützliche Regeln:**
  - Gilt $\dim(V) = n$, so bilden je n linear unabhängige Vektoren eine Basis.
  - Gilt $\dim(V) = n$, so bildet jedes Erzeugendensystem mit n Elementen eine Basis.
  - Gilt $\dim(V) = n$, so sind mehr als n Vektoren linear abhängig.
  - Ist U ein Untervektorraum von V mit $U \subsetneq V$, so gilt $\dim(U) < \dim(V)$.
  - Ist U ein Untervektorraum von V mit $\dim(U) = \dim(V)$, so gilt $U = V$.

Für jedes $n \in \mathbb{N}$ gilt $\dim(\mathbb{K}^n) = n$, da die Standardbsis/ kanonische Basis $B = \{e_1, \ldots, e_n\}$ des $\mathbb{K}^n$ genau n Elemente enthält

Für alle $m, n \in \mathbb{N}$ gilt $\dim(\mathbb{K}^{m \times n}) = m \cdot n$, da die Basis $B = \{E_{11}, E_{12}, \ldots, E_{mn}\}$ der Standardeinheitsmatrizen E_{ij} (Eins nur an der Stelle (i, j) sonst Nullen) genau mn Elemente enthält

Der Vektorraum $\mathbb{R}[x]$ der reellen Polynome hat unendliche Dimension $(\mathbb{R}[x]) = \infty$, da die Basis $B = \{1, x, x^2, \ldots\}$ nicht endlich ist

Der Vektorraum $\mathbb{R}[x]_n$ der Polynome vom Grad n hat die Dimension $n + 1$ -> $\dim(\mathbb{R}[x]_n) = n + 1$

Verkürzen eines Erzeugendensystems zu einer Basis

- Gegeben ist ein Erzeugendensystem X eines Vektorraums V. Man bestimmt dann eine Basis $B \subseteq X$ von V wie folgt:

  (1) Prüfe, ob X linear unabhängig ist.
  Falls ja: X ist eine Basis.
  Falls nein: Entferne aus X Elemente $a_1, \dots, a_r$, die Linearkombinationen anderer Elemente aus X sind, und setze $\tilde{X} = X \setminus \{a_1, \dots, a_r\}$.
  (2) Beginne mit $\tilde{X}$ anstelle von X von vorne.

Verlängern einer linear unabhängigen Menge zu einer Basis

- Gegeben ist eine linear unabhängige Teilmenge X eines Vektorraums V. Man bestimmt dann eine Basis $B \supseteq X$ von V wie folgt:

  (1) Prüfe, ob X ein Erzeugendensystem von V ist.
  Falls ja: X ist eine Basis.
  Falls nein: Wähle aus V Elemente $a_1, \dots, a_r$, sodass $X \cup \{a_1, \dots, a_r\}$ linear unabhängig ist, und setze $\tilde{X} = X \cup \{a_1, \dots, a_r\}$.
  (2) Beginne mit $\tilde{X}$ anstelle von X von vorne.

Bei Spaltenvektoren, also $X = \{v_1, \dots, v_s\}$, $v_i \in \mathbb{K}^n$, lassen sich diese zwei Aufgaben ganz einfach und mit den gleichen Methoden durchführen: Man schreibt dazu die Spalten v_i als Zeilen $v_i^\top$ in eine Matrix M und wendet elementare Zeilenumformungen an, um die Matrix auf Zeilenstufenform zu bringen:

$$M = \begin{pmatrix} v_1^\top \\ \vdots \\ v_s^\top \end{pmatrix} \rightsquigarrow M' = \begin{pmatrix} * & * & * & * & * \\ & * & * & * & \vdots \\ & & * & * & * \\ 0 & & & & 0 \end{pmatrix} \begin{matrix} \} \, r \text{ Zeilen ungleich } 0 \dots 0 \\ \} \, s - r \text{ Zeilen gleich } 0 \dots 0 \end{matrix}.$$

Dann gilt:

- Die Transponierten der ersten r Zeilen von M' bilden eine Basis $B = \{b_1, \dots, b_r\}$ von $\langle X \rangle$, die $s - r$ Spaltenvektoren, aus denen die letzten $s - r$ Nullzeilen hervorgegangen sind, sind Linearkombinationen von B. Durch die Wahl der ersten r Zeilen hat man das Erzeugendensystem auf ein linear unabhängiges Erzeugendensystem von $\langle X \rangle$ *verkürzt*.
- Ergänzt man die Matrix M' durch $n - r$ weitere Zeilen, die die Zeilenstufenform fortsetzen, so *verlängert* man die linear unabhängige Menge aus r Vektoren zu einer linear unabhängigen Menge mit n Vektoren, man *verlängert* also die linear unabhängige Menge zu einer Basis des $\mathbb{K}^n$.

Sind $a_1', \dots, a_n' \in K^m$ die Spaltenvektoren von A, so gilt: $\{a_{j_1}', \dots, a_{j_r}'\}$ ist eine Basis von $\{a_1, \dots, a_m\}$.

(1) $\{a_1, \dots, a_m\}$ ist linear unabhängig $\Leftrightarrow r = m$

(2) $\{a_1, \dots, a_m\}$ ist ein Erzeugendensystem von K^n $\Leftrightarrow r = n$

(3) $\{a_1, \dots, a_m\}$ ist eine Basis von K^n $\Leftrightarrow r = m = n$

(4) $\{b_1, \dots, b_r\} \cup \{e_j \mid j \in \{1, \dots, n\} \setminus \{j_1, \dots, j_r\}\}$ ist eine Basis von K^n

Anwendung auf Matrizen und lineare Gleichungssysteme

Wir betrachten eine $m \times n$ - Matrix $A \in \mathbb{K}^{m \times n}$ mit den Spalten $s_1, \dots s_n \in K^m$ und den Zeilen $z_1, \dots + z_m \in K^{1 \times n}$

Rang von A ($rg(A)$) = Zellenrang von A ($\dim(Z_A)$) = Spaltenrang von A ($\dim(S_A)$)

Spaltenraum von A -> Erzeugnis der Spalten von A, also $S_A = \langle s_1, \dots, s_n \rangle \subseteq \mathbb{K}^m = \{Av \mid v \in \mathbb{K}^n\}$

Zeilenraum von A -> Erzeugnis der Zeilen von A, also $Z_A = \langle z_1, \dots, z_m \rangle \subseteq \mathbb{K}^{1 \times n} = \{v^\top A \mid v \in \mathbb{K}^m\}$

Bestimmen von Zeilen-/Spalten-/ Raum/Rang

Gegeben ist die Matrix

$$A = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix} = (s_1, \dots, s_n) = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in \mathbb{K}^{m \times n}$$

- Wende auf A elementare Zeilenumformungen an und erhalte:

$$A \rightsquigarrow \dots \rightsquigarrow \begin{pmatrix} * & * & * & * & * \\ & * & * & * & \vdots \\ & & * & * & * \\ 0 & & & & 0 \end{pmatrix} =: A'.$$

00001

Dann gilt: Die von der Nullzeile verschiedenen Zeilen von A' bilden eine Basis des Zeilenraums von A, die Anzahl dieser Zeilen ist der Zeilenrang von A.

- Wende auf A *elementare Spaltenumformungen* an (analog zu den elementaren Zeilenumformungen) und erhalte:

$$A \rightsquigarrow \dots \rightsquigarrow \begin{pmatrix} * & & & & 0 \\ * & * & & & \\ * & * & * & & \\ * & \dots & \dots & * & 0 \end{pmatrix} \begin{matrix} 0 \\ 0 \\ 0 \\ 1 \end{matrix} =: A''.$$

Dann gilt: Die von der Nullspalte verschiedenen Spalten von A'' bilden eine Basis des Spaltenraums von A, die Anzahl dieser Spalten ist der Spaltenrang von A.

Kern einer Matrix

Kern(A) ≠ {0} => linear abhängig

Ist $A \in \mathbb{K}^{m \times n}$, so nennt man die Menge $\ker(A) = \{v \in \mathbb{K}^n \mid Av = 0\} \subseteq \mathbb{K}^n$ den Kern von A

-- Der Kern von A ist die Lösungsmenge des homogenen linearen Gleichungssystems $Ax = 0$

-- Der Kern einer Matrix $A \in \mathbb{K}^{m \times n}$ ist ein Untervektorraum von $\mathbb{K}^n$

-- Für eine quadratische Matrix $A \in \mathbb{K}^{n \times n}$ gilt: $\dim(\ker(A)) = n - \mathrm{rg}(A) =$ Anzahl der Nullzeilen in Zeilenstufenform

-- Das LGS $Ax = b$ mit $A \in \mathbb{K}^{m \times n}$ und $b \in \mathbb{K}^m$ ist genau dann lösbar, wenn $b \in S_A = \{Av \mid v \in \mathbb{K}^n\}$

$$\ker \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 6 & 8 \\ 3 & 6 & 9 & 12 \\ 4 & 8 & 12 & 16 \end{pmatrix} = \ker \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} 2 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 0 \\ 0 \\ -1 \end{pmatrix} \right\rangle.$$

① ② ③

$\dim(\ker(A)) = n - rg(A) = 4 - 1 = 3$

① $2 \cdot 1 + (-1) \cdot 2 + 0 \cdot 3 + 0 \cdot 4 = 0$

② $3 \cdot 1 + 0 \cdot 2 + (-1) \cdot 3 + 0 \cdot 4 = 0$

③ $4 \cdot 1 + 0 \cdot 2 + 0 \cdot 3 + (-1) \cdot 4 = 0$

Lineare Code

Bei Datenübertragung wird ein Bit wahrscheinlich fehlerhaft geschrieben, somit wird Bit-Strom $(x_1, \dots, x_k)$ redundant gesendet

-- Die Menge aller Codewörter bildet einen Unterraum des K^n

-- Eine solche Datenübertagung ist nur sinnvoll, wenn die Zuordnung des Codeworts zu einem Datenwort injektiv ist

-- Das inhomogene LGS $G \cdot x = c$ muss also für alle $c \in C$ eindeutig lösbar sein, also $rg(G) = k$

-- Die Spalten von G erzeugen C und sind linear unabhängig -> $\dim(C) = k$

Generatormatrix

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = G \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$$

Codewort Informationswort

Menge aller Codewörter

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

$C \subseteq K^n$ als (n, k)-Code

Länge von C -> n

Informationsrate -> k/n

Redundanz -> $n - k$

Wiederholungscode, bei dem alles beliebig oft wiederholt wird -> $(x_1, \dots, x_k) \mapsto (x_1, \dots, x_k, \dots\dots x_1, \dots, x_k,)$

a) 1-fehlererkennende Code: falls einmal wiederholt und der auftretende Fehler kann nach Empfang nicht korrigiert werden

b) 1-fehlerkorrigierende Code: falls mehrere-mal wiederholt und der auftretende Fehler kann nach Empfang korrigiert werden

Parity-Check-Code -> Abbildung $(x_1, \dots, x_4) \mapsto (x_1, \dots, x_4, x_1 + x_2 + x_3 + x_4)$ -> 1-fehlererkennende Code

Dekodieren

Ablauf: Das empfangene Wort $c' = (c'_1, \dots, c'_n)$ kann sich vom gesendeten Wort c durch Übertragungsfehler unterscheiden

1) Falls $c' \in C$, so wird $c = c'$ angenommen -> Auflösen des LGS $G \cdot x = c'$ -> das wahrscheinliche Informationswort $x \in K^k$

2) Falls $c' \notin C$ -> Annahme: nur wenige Fehlerbits -> sucht man $c'' \in C$, das sich von c' an möglichst wenig Koordinaten unterscheidet

-- 2a) Falls es genau ein solches c'' gibt -> $c = c''$ wird angenommen und $x \in K^k$ mit $G \cdot x = c''$ ausgegeben

-- 2b) Falls es mehrere solches c'' gibt -> Fehlermeldung

Hamming-Gewicht

Hamming-Gewicht von c (Anzahl der Stelle wo ungleich 0)

$w(c) := |\{i \in \{1, \dots, n\} \mid c_i \neq 0\}|$ **für** $c = (c_1, \dots, c_n) \in K^n$

Hamming-Abstand von c und c' (Anzahl der Stelle wo c und c' sich unterscheiden)

$d(c, c') := w(c - c') = |\{i \in \{1, \dots, n\} \mid c_i \neq c'_i\}|$ **für** $c, c' \in K^n$

Hamming-Abstand von C (das geringste Hamming-Gewicht der überhaupt vorkommen kann)

$d(C) := \min\{d(c, c') \mid c, c' \in C, c \neq c'\}$ **für eine Teilmenge** $C \subseteq K^n$

$d(C) = \min\{w(c) \mid c \in C \backslash \{0\}\}$ **für ein Unterraum** C

Sei $C \subseteq K^n$ ein Code

(a) Falls $d(C) = 2e + 1$, so ist C e-fehlerkorrigierend

(b) Falls $d(C) = 2e + 2$, so ist C e-fehlerkorrigierend und $(e + 1)$-fehlererkennend

Generatormatrix $G = \begin{pmatrix} I_k \\ A \end{pmatrix}$ mit $A \in K^{(n-k)\times k}$

Parity-Check-Matrix $P := (-AI_{n-k}) \in K^{(n-k)\times n}$

P hat den Rang $n - k$ und es gilt $P \cdot G = (-AI_{n-k}) \cdot \begin{pmatrix} I_k \\ A \end{pmatrix} = 0$

$P \cdot c = 0$ für alle $c \in C$ -> Lösungsmenge L des homogenen LGS $P \cdot x = 0$

-> hat die Dimension $\dim(C) = n - (n - k) = k$

Der (7,4)-Hamming-Code

Abbildung $(x_1, \ldots, x_4) \mapsto (x_1, x_2, x_3, x_4, x_2 + x_3 + x_4, x_1 + x_3 + x_4, x_1 + x_2 + x_4)$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{7\times 4} \qquad P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$d(C) \neq 1$

$d(C) \neq 2$

$d(C) = min. 3$

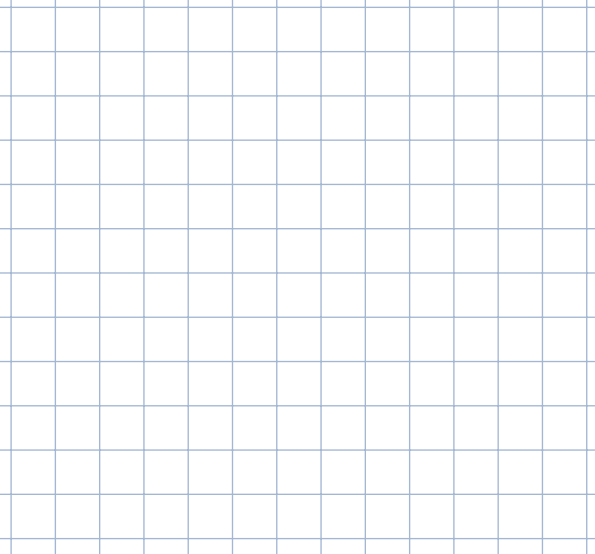
Determinanten

Symmetrische Gruppe $(S_n, \circ)$

Menge $S_n = \{\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\} \mid \sigma \text{ ist bijektiv}\}$

Die Elemente von S_n nennt man Permutationen

Mächtigkeit $|S_n| = n!$ -> Die symmetrische Gruppe hat $n!$ Elemente



Signum & Fehlstand

Die Abbildung vom Signum $\text{sgn} : S_n \to \{1, -1\}$ ist ein Homomorphismus

-> $\text{sgn}(\tau \circ \sigma) = \text{sgn}(\tau) \cdot \text{sgn}(\sigma)$ für alle $\tau, \sigma \in S_n$

-> $\text{sgn}\left(\sigma^{-1}\right) = \text{sgn}(\sigma)$ für jedes $\sigma \in S_n$

Fehlstand $(\sigma(i), \sigma(j))$ existiert, wenn für das Paar (i, j) von Indizes aus I_n einerseits $i < j$ und andererseits $\sigma(i) > \sigma(j)$ gilt

f -> Anzahl der Fehlstände -> Signum (= Vorzeichen) einer Permutation $\sigma \in S_n$ kann dadurch bestimmen $\text{sgn}(\sigma) = (-1)^f$

(Schnittstellen)

Determinante von A (Leibniz'sche Formel) $|\boldsymbol{A}| = \det(\boldsymbol{A}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$

-> Für jede quadratische Matrix $A \in R^{n \times n}$ mit Einträgen aus einem kommutativen Ring R

Im Fall $n = 1$ -> gilt $S_1 = \{\mathrm{id}\}$ für jede Matrix $\boldsymbol{A} = (a_{11}) \in R^{1 \times 1}$

-> $\operatorname{sgn}(\mathrm{id}) = 1$ somit $\det(\boldsymbol{A}) = \sum_{\sigma \in S_1} \operatorname{sgn}(\sigma) \prod_{i=1}^{1} a_{i\sigma(i)} = 1 \cdot a_{11} = a_{11}$

Im Fall $n = 2$ -> gilt $S_2 = \{\mathrm{id} = \sigma_1, \sigma_2\}$ für jede Matrix $\boldsymbol{A} = (a_{ij}) \in R^{2 \times 2}$

-> $\operatorname{sgn}(\sigma_1) = 1$ und $\operatorname{sgn}(\sigma_2) = -1$

-> somit $\det(\boldsymbol{A}) = \sum_{\sigma \in S_2} \operatorname{sgn}(\sigma) \prod_{i=1}^{1} a_{i\sigma(i)} = 1 \cdot a_{11}a_{22} + (-1) \cdot a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}$

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{pmatrix} {}^{+}a_{11} & a_{12}{}^{-} \\ a_{21} & a_{22} \end{pmatrix}$$

Im Fall $n = 3$ -> gilt $S_3 = \{\sigma_1, \dots \sigma_6\}$ für jede Matrix $\boldsymbol{A} = (a_{ij}) \in R^{3 \times 3}$

-> $\operatorname{sgn}(\sigma_1) = 1, \operatorname{sgn}(\sigma_2) = 1, \operatorname{sgn}(\sigma_3) = 1, \operatorname{sgn}(\sigma_4) = -1, \operatorname{sgn}(\sigma_5) = -1, \operatorname{sgn}(\sigma_6) = -1$

-> somit $\det(a_{ij}) = \sum_{\sigma \in S_3} \operatorname{sgn}\sigma \prod_{i=1}^{n} a_{i\sigma(i)} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - (a_{13}a_{22}a_{31} + a_{23}a_{32}a_{11} + a_{33}a_{12}a_{21})$

$$\begin{vmatrix} a_{11}a_{12}a_{13} \\ a_{21}a_{22}a_{23} \\ a_{31}a_{32}a_{33} \end{vmatrix} = {}^{+}a_{13}\begin{pmatrix} {}^{+}a_{11} & {}^{+}a_{12}{}^{-} & a_{13}{}^{-} \\ a_{23} & a_{21} & a_{22} & a_{23} \\ a_{33} & a_{31} & a_{32} & a_{33} \end{pmatrix} a_{11}{}^{-} \\ a_{21} \\ a_{31}$$

Im Fall $n \geq 4$ -> **Determinante einer $n \times n$ -Matrix rekursiv berechnen**

-> Die Berechnung der Determinante einer $n \times n$ -Matrix wird auf die Berechnung von $(n-1) \times (n-1)$ -Matrizen zurückgeführt

Für jede quadratische Matrix $A \in R^{n \times n}$ und $i, j \in \{1, \dots, n\}$ bezeichne $\boldsymbol{A}_{ij} \in R^{(n-1) \times (n-1)}$ diejenige Matrix, die aus A durch Entfernen der i-ten Zeile und j-ten Spalte entsteht

$$\boldsymbol{A} = \begin{pmatrix} & & a_{1i} & & \\ & & \vdots & & \\ a_{j1} & \cdots & a_{ji} & \cdots & a_{jn} \\ & & \vdots & & \\ & & a_{ni} & & \end{pmatrix}, \quad \boldsymbol{A}_{ji} = \begin{pmatrix} & \\ & \end{pmatrix}$$

Entwicklungssatz von Laplace: für $\boldsymbol{A} = (a_{ij}) \in R^{n \times n}$ und beliebige $i, j \in \{1, \dots, n\}$ gilt

Entwicklung nach der i-ten Zeile $\det \boldsymbol{A} = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det \boldsymbol{A}_{ij}$

Entwicklung nach der j-ten Spalte $\det \boldsymbol{A} = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det \boldsymbol{A}_{ij}$

$$\det \boldsymbol{A} = \begin{vmatrix} 4 & 2 & -3 & 4 \\ 5 & 6 & 1 & 4 \\ \mathbf{0} & \mathbf{0} & \mathbf{2} & \mathbf{0} \\ -2 & -2 & 3 & 6 \end{vmatrix} \begin{matrix} = (-1)^{1+3} \cdot \mathbf{0} \cdot \det(\boldsymbol{A}_{13}) \\ + (-1)^{2+3} \cdot \mathbf{0} \cdot \det(\boldsymbol{A}_{23}) \\ + (-1)^{3+3} \cdot \mathbf{2} \cdot \det(\boldsymbol{A}_{33}) \\ + (-1)^{4+3} \cdot \mathbf{0} \cdot \det(\boldsymbol{A}_{43}) \end{matrix} = (-1)^{3+3} \, \mathbf{2} \begin{vmatrix} 4 & 2 & 4 \\ 5 & 6 & 4 \\ -2 & -2 & 6 \end{vmatrix}$$

Determinante einer transponierten Matrix: Für jede quadratische Matrix $\boldsymbol{A} \in R^{n \times n}$ gilt $\det(\boldsymbol{A}) = \det\left(\boldsymbol{A}^{\top}\right)$

Regeln für die Determinante

-- Entsteht die Matrix B aus der Matrix $A \in R^{n \times n}$ durch Vertauschen zweier Zeilen/ Spalten, so gilt $\det(\boldsymbol{B}) = -\det(\boldsymbol{A})$

-- Hat eine Matrix $\boldsymbol{A} \in R^{n \times n}$ zwei gleiche Zeilen/ Spalten, so ist ihre Determinante null $\det(\boldsymbol{A}) = 0$

Determinantenmultiplikationssatz: Sind $A, B \in R^{n \times n}$, so gilt $\det(\boldsymbol{AB}) = \det(\boldsymbol{A}) \det(\boldsymbol{B})$

-- Die Determinante eines Produkts von Matrizen ist das Produkt der Determinanten

-> durch Anwenden des Determinantenmultiplikationssatz: $\det(\boldsymbol{A}) \det\left(\boldsymbol{A}^{-1}\right) = \det\left(\mathbf{E}_n\right) = 1$

-> Folgerung 1: Ist $A \in R^{n \times n}$ invertierbar, so ist $\det(\boldsymbol{A}) \in R$ invertierbar, und es gilt $\det\left(\boldsymbol{A}^{-1}\right) = (\det \boldsymbol{A})^{-1}$

-> Folgerung 2: Für jede Matrix $\boldsymbol{A} \in R^{n \times n}$ und jedes $k \in \mathbb{N}$ gilt $\det\left(\boldsymbol{A}^{k}\right) = (\det \boldsymbol{A})^{k}$

Die Determinante einer Dreiecksmatrix ist das Produkt der Diagonalelemente

$$\det \begin{pmatrix} a_{11} & * & \dots & * \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & a_{nn} \end{pmatrix} = \prod_{i=1}^{n} a_{ii} \qquad \det \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ * & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \dots & * & a_{nn} \end{pmatrix} = \prod_{i=1}^{n} a_{ii}$$

Blockdreiecksmatrix $M = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{B} \end{pmatrix} \in R^{n \times n}$ $\quad \boldsymbol{A} \in R^{m \times m}$ $\quad \boldsymbol{B} \in R^{(n-m)\times(n-m)}$ $\quad \boldsymbol{0} \in R^{(n-m)\times m}$ -> Nullmatrix $\quad \boldsymbol{C} \in R^{m \times (n-m)}$

Die Determinante einer Blockdreiecksmatrix ist das Produkt der Determinanten der Blöcke

$$\det \begin{pmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{B} \end{pmatrix} = \det \boldsymbol{A} \det \boldsymbol{B} = \det \begin{pmatrix} \boldsymbol{A} & \boldsymbol{0} \\ \boldsymbol{C} & \boldsymbol{B} \end{pmatrix}$$

Die Determinante nach elementaren Zeilen-/Spalten- umformungen

Für jede Matrix $A \in R^{n \times n}$ und $\lambda \in R$ gilt

(a) Entsteht A' aus A durch Vertauschen zweier Zeilen/ Spalten, so gilt $\det A' = -\det A$

(b) Entsteht A' aus A durch Addition eines Vielfachen einer Zeile/ Spalte zu einer anderen, so gilt $\det A' = \det N_{ij}(\lambda) A = \det A$

(c) Entsteht A' aus A durch Multiplikation einer Zeile/ Spalte mit einem Element $\lambda \in R$, so gilt $\det A' = \lambda \det A$

Achtung: Für Matrizen $\boldsymbol{A} \in R^{n \times n}$ und $\lambda \in R$ ist $\det(\lambda A) = \lambda^n \det(A)$

Eine Matrix $A \in R^{n \times n}$ ist invertierbar, gdw. es gilt $\det A \neq 0$

Orthogonalität

Skalarprodukt/ euklidischer Vektorraum

$\langle v, w \rangle$ ist äquivalent wie $s(v, w)$

Definition: ein reeller Vektorraum V mit einer Abbildung $\langle\ ,\ \rangle : V \times V \to \mathbb{R}, (v, w) \mapsto \langle v, w \rangle$ mit folgenden Eigenschaften

(i) bilinear, wenn für alle $v, v', w, w' \in V$ und $\lambda \in \mathbb{R}$ gilt:
-- Linearitit im 1. Argument: $\langle \lambda v + v', w \rangle = \lambda \langle v, w \rangle + \langle v', w \rangle$
-- Linearitit im 2. Argument: $\langle v, \lambda w + w' \rangle = \lambda \langle v, w \rangle + \langle v, w' \rangle$

(ii) symmetrisch, wenn für alle $v, w \in V$ gilt: $\langle v, w \rangle = \langle w, v \rangle$

(iii) positiv definit, wenn für alle $v \in V$ gilt: $\langle v, v \rangle \geq 0$ und $\langle v, v \rangle = 0 \Leftrightarrow v = 0$

für ein Vektorraum V mit euklidischem Skalarprodukt $\langle\ ,\ \rangle$

-- Länge oder Norm von $v \in V$: die reelle Zahl $\|v\| = \sqrt{\langle v, v \rangle}$

-- Abstand von v und w: die reelle Zahl $d(v, w) = \|v - w\| = \|w - v\|$

-- Winkel zwischen $v \neq 0$ und $w \neq 0$: die reelle Zahl $\measuredangle(v, w) = \arccos\left(\frac{\langle v, w \rangle}{\|v\|\|w\|}\right)$

-> Cauchy-Schwarz'sche Ungleichung: $|\langle v, w \rangle| \leq \|v\|\|w\|$ --> $-1 \leq \frac{\langle v, w \rangle}{\|v\|\|w\|} \leq 1$ und $\measuredangle(v, w) \in [0, \pi]$

-- Orthogonalität $v \perp w$: zwei Vektoren v und w senkrecht oder orthogonal, wenn $\langle v, w \rangle = 0$ gilt

Eine Teilmenge B eines euklidischen Vektorraums V mit Skalarprodukt $\langle\ ,\ \rangle$ heißt

-- Orthogonalsystem von V, wenn für alle $v, w \in B$ mit $v \neq w$ gilt $v \perp w$

-- Orthogonalbasis von V, wenn B Orthogonalsystem und Basis ist

-- Orthonormalsystem von V, wenn B Orthogonalsystem ist und $\|v\| = 1$ (normiert) für alle $v \in B$ gilt

-- Orthonormalbasis (= ONB) von V, wenn B Orthonormalsystem und Basis ist

-> Orthonormalität: B ist $ONB \Leftrightarrow \forall i, j : \langle b_i, b_j \rangle = \delta_{ij}$ mit dem Kronecker-Delta $\delta_{ij} = \begin{cases} 1, & \text{falls } i = j \\ 0, & \text{falls } i \neq j \end{cases}$

Orthogonale Zerlegung von v längs a

Ist $a \neq 0$ ein Vektor eines euklidischen Vektorraums mit dem Skalarprodukt $\langle\ ,\ \rangle$,

so lässt sich jeder Vektor $v \in V$ in der Form $v = v_a + v_{a\perp}$ mit $v_a = \lambda a = \frac{\langle v,a \rangle}{\langle a,a \rangle} a$ und $v_a \perp a$ darstellen

Bestimmen der Linearkombination bezüglich einer ONB

Ist $B = \{b_1, \ldots, b_n\}$ eine Orthonormalbasis eines euklidischen Vektorraums V bezüglich des Skalarprodukts $\langle\ ,\ \rangle$,

so erhält man für jedes $v \in V$ die Koeffizienten $\lambda_1, \ldots, \lambda_n$ der (bis auf die Reihenfolge der Summanden eindeutig bestimmten) Linearkombination $v = \lambda_1 b_1 + \cdots + \lambda_n b_n$ wie folgt: Für $i = 1, \ldots, n$ gilt $\lambda_i = \langle v, b_i \rangle$

Nachprüfen-Beispiel

$$\langle v, b_1 \rangle = \lambda_1 \underbrace{\langle b_1, b_1 \rangle}_{=1} + \lambda_2 \underbrace{\langle b_2, b_1 \rangle}_{=0} + \cdots + \lambda_n \underbrace{\langle b_n, b_1 \rangle}_{=0} = \lambda_1$$

$$\langle v, b_2 \rangle = \lambda_1 \underbrace{\langle b_1, b_2 \rangle}_{=0} + \lambda_2 \underbrace{\langle b_2, b_2 \rangle}_{=1} + \cdots + \lambda_n \underbrace{\langle b_n, b_2 \rangle}_{=0} = \lambda_2$$

Orthogonale Matrizen: eine Matrix $A \in \mathbb{R}^{n \times n}$ mit $A^\top A = E_n$

Eigenschaften

A ist invertierbar

$A^{-1} = A$

$\det(A) = \pm 1$

Die Spalten von A bilden eine ONB des $\mathbb{R}^n$

Die Zeilen von A bilden eine ONB des $\mathbb{R}^n$

Das Produkt orthogonaler Matrizen ist orthogonal

A ist längenerhaltend, d.h. $\|Av\| = \|v\|$ für jedes $v \in \mathbb{R}^n$ (euklidische Norm)

Orthonormierungsverfahren von Gram und Schmidt

Gegeben ist eine Basis $\{a_1, \ldots, a_n\}$ eines euklidischen Vektorraums V mit Skalarprodukt $\langle\ ,\ \rangle$,

Bilde die Vektoren $b_1, \ldots, b_n$ allgemein wie folgt: $b_1 = \frac{1}{\|a_1\|} a_1$, $b_{k+1} = \frac{1}{\|c_{k+1}\|} c_{k+1}$ mit $c_{k+1} = a_{k+1} - \sum_{i=1}^{k} \langle a_{k+1}, b_i \rangle b_i$

Beispiele

(1) $b_1 = \frac{1}{\|a_1\|} a_1$

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

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

(4) ...

(n) $b_n = \frac{1}{\|c_n\|} c_n$ mit $c_n = a_n - \langle a_n, b_1 \rangle b_1 - \cdots - \langle a_n, b_{n-1} \rangle b_{n-1}$

Vektorprodukt und Spatprodukt

Für Vektoren $a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ und $b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$ und $c = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} \in \mathbb{R}^3$

Vektorprodukt von a und b -> $a \times b = \begin{pmatrix} a_2b_3 - b_2a_3 \\ a_3b_1 - b_3a_1 \\ a_1b_2 - b_1a_2 \end{pmatrix} \in \mathbb{R}^3$

äquivalent

Spatprodukt von a, b und c -> $[a, b, c] = \langle a \times b, c \rangle \in \mathbb{R}$

Eigenschaften

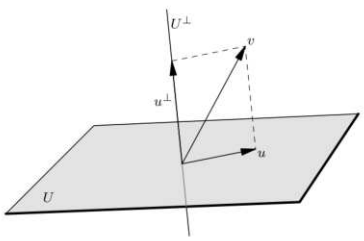
1. $\langle x, a \times b \rangle = \det(x, a, b)$ **für alle** $x \in \mathbb{R}^3$
2. **Der Vektor** $a \times b$ **steht senkrecht auf** a **und** b, $a \times b \perp a, b$
3. $\|a \times b\| = \|a\|\|b\| \sin \measuredangle(a, b) =$ **Flächeninhalt des von** a, b **aufgespannten Pallelogramms**
4. **Falls** a **und** b **linear unabhängig sind, so bilden** $a, b, a \times b$ **ein Rechtssystem, d. h.** $\det(a, b, a \times b) > 0$
5. **Für jeden Vektor** $a \in \mathbb{R}^3$ **gilt:** $a \times a = 0$
6. **Für alle** $a, b \in \mathbb{R}^3$ **gilt:** $a \times b = -b \times a$
7. $a \times b = 0 \Leftrightarrow a, b$ **sind linear abhängig**
8. $\|a \times b\|^2 + |\langle a, b \rangle|^2 = \|a\|^2\|b\|^2$
9. **Für alle** $u, v, w, x \in \mathbb{R}^3$ **gilt:**
   - **-- Grassmann-Identität** $u \times (v \times w) = \langle u, w \rangle v - \langle u, v \rangle w$
   - **-- Jacobi-Identität** $(u \times (v \times w)) + (v \times (w \times u)) + (w \times (u \times v)) = 0$
   - **-- Lagrange-Identität** $\langle u \times v, w \times x \rangle = \langle u, w \rangle \langle v, x \rangle - \langle u, x \rangle \langle v, w \rangle$
10. $[a, b, c] = \det(a, b, c)$
11. $|[a, b, c]| =$ **Volumen des von** a, b, c **aufgespannten Spates**
12. $[a, b, c] = 0 \Leftrightarrow \{a, b, c\}$ **ist linear abhängig**
13. $[a, b, c] > 0 \Leftrightarrow a, b, c$ **bilden ein Rechtssystem**

Das orthogonale Komponent

Ist U **ein Untervektorraum eines endlichdimensionalen euklidischen Vektorraums** V **Skalarprodukt** $\langle\ ,\ \rangle$

-> das orthogonale Komplement zu U **->** $U^\perp = \{v \in V \mid v \perp u$ **für alle** $u \in U\}$

Eigenschaften



- **--** $U^\perp$ **ist Untervektorraum von** V
- **--** $U^\perp \cap U = \{0\}$
- **-- Jedes** $v \in V$ **hat genau eine Darstellung der Form** $v = u + u^\perp$ **mit** $u \in U$ **und** $u^\perp \in U^\perp$
- **--** $\dim(V) = n \Rightarrow \dim\left(U^\perp\right) = n - \dim(U)$

Bestimmen des orthogonalen Komplements

Ist U **ein Untervektorraum eines endlichdimensionalen euklidischen Vektorraums** V **mit** $\dim(V) = n$

(1) Bestimme eine Basis $\{b_1 \ldots, b_r\}$ **von** U -> $\dim(U) = r$

(2) Bestimme $n - r$ **linear unabhängige Vektoren** $a_1 \ldots, a_{n-r}$ **, die zu allen** $b_1, \ldots, b_r$ **orthogonal sind**

(3) Es gilt $U^\perp = \langle a_1, \ldots, a_{n-r} \rangle$ -> $\dim\left(U^\perp\right) = n - r$

Die orthogonale Projektion von V auf U

Abbildung $p_U : \begin{cases} V & \to U \\ v = u + u^\perp & \mapsto u' \end{cases}$

Für den Vektor $u^\perp = v - u$ **gilt nämlich** $\|u^\perp\| = \|v - u\| \leq \|v - w\|$

minimaler Abstand von v zu U -> $\|u^\perp\| = \|v - u\| = \min$

u als Lösung der Minimierungsaufgabe -> **Bestimme** $u \in U$ **mit** $\|v - u\| = \min$

(i) Wähle eine Basis $\{b_1, \ldots, b_r\}$ **von** U

(ii) dann $u = Ax$ **mit** $A = (b_1, \ldots, b_r) \in \mathbb{R}^{n \times r}$ **für ein** $x = (\lambda_1, \ldots, \lambda_r)^\top \in \mathbb{R}'$

(iii) Bestimme $x \in \mathbb{R}^r$ **mit** $\|v - Ax\| = \min$

Beweis

$$\|v - w\| = \|\overbrace{v - u}^{=u^\perp} + u - w\| = \sqrt{\langle u^\perp + (u - w), u^\perp + (u - w)\rangle}$$
$$= \sqrt{\|u^\perp\|^2 + \|u - w\|^2 + 2\underbrace{\langle u^\perp, u - w\rangle}_{=0}} \geq \|u^\perp\| = \|v - u\|$$

Das lineare Ausgleichsproblem

Das lineare Ausgleichsproblem und seine Lösung

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

Gesucht: **ein Vektor** $x \in \mathbb{R}^r$, **sodass** $\|b - Ax\| = \min$

Lösung: $x \in \mathbb{R}^r$, **welches die Normalgleichung erfüllt:** $A^\top Ax = A^\top b$ **bzw.** $x = (A^\top A)^{-1} A^\top b$

-> **genau dann eindeutig lösbar, wenn der Rang von A maximal ist, d.h. wenn** $rg(A) = r$ **gilt**

Anwendung 1: Bestimmen der orthogonalen Projektion $u = p_U(b)$

(1) Wähle eine Basis $B = \{b_1, \ldots, b_r\}$ **von** U **und setze** $A = (b_1, \ldots, b_r) \in \mathbb{R}^{n \times r}$

(2) Löse das eindeutig lösbare lineare Gleichungssystem $A^\top Ax = A^\top b$ **und erhalte Lösungsvektor** $x = (\lambda_1, \ldots, \lambda_r)^\top \in \mathbb{R}^r$

(3) Es ist $u = \lambda_1 b_1 + \cdots + \lambda_r b_r$ **und der minimale Abstand von b zu U ist dann** $\|b - u\|$

Anwendung 2: Lösen eines überbestimmten linearen Gleichungssystems (mehr Gleichungen als Unbekannte $n \geq r$)

Aufgabe: Finde ein Vektor $x \in \mathbb{R}^r$, **sodass** $\|b - Ax\| = \min$ **bzw.** $Ax = b$ **mit** $A \in \mathbb{R}^{n \times r}$ **und** $b \in \mathbb{R}^n$

Eine optimale Lösung: $x \in \mathbb{R}^r$, **welches die Normalgleichung erfüllt:** $A^\top Ax = A^\top b$ **bzw.** $x = (A^\top A)^{-1} A^\top b$

x als Lösung des Koeffizientenmatrix $\left(A^\top A \mid A^\top b\right) \rightsquigarrow (E_n \mid x)$

Anwendung 3: Bestimmen einer Ausgleichsfunktion (Methode der kleinsten Quadrate)

Gegeben: n **Stützstellen** $(t_1, y_1), \ldots, (t_n, y_n)$ **und Basisfunktionen** $f_1, \ldots, f_r$

Gesucht: Eine gut approximierte Ausgleichsfunktion f, sodass der Fehler $\sum_{i=1}^n (y_i - f(t_i))^2$ **minimal wird**

(1) Setze $b = (y_1, \ldots, y_n)^\top \in \mathbb{R}^n$ **und** $A = \begin{pmatrix} f_1(t_1) & \ldots & f_r(t_1) \\ \vdots & & \vdots \\ f_1(t_n) & \ldots & f_r(t_n) \end{pmatrix} \in \mathbb{R}^{n \times r}$

$$b - Ax = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} - \lambda_1 \begin{pmatrix} f_1(t_1) \\ \vdots \\ f_1(t_n) \end{pmatrix} - \cdots - \lambda_r \begin{pmatrix} f_r(t_1) \\ \vdots \\ f_r(t_n) \end{pmatrix} = \begin{pmatrix} y_1 - f(t_1) \\ \vdots \\ y_n - f(t_n) \end{pmatrix}$$

$$\min = \|b - Ax\| = (y_1 - f(t_1))^2 + \cdots + (y_n - f(t_n))^2 = \sum_{i=1}^n (y_i - f(t_i))^2$$

(2) Löse die Normalgleichung $A^\top Ax = A^\top b$ **und erhalte** $x = (\lambda_1, \ldots, \lambda_r)^\top \in \mathbb{R}^r$

(3) Es ist $f = \lambda_1 f_1 + \cdots + \lambda_r f_r$ **die Ausgleichsfunktion**

Ausgleichsgerade

$$\left.\begin{array}{ll} f_1 : \mathbb{R} \to \mathbb{R}, f_1(x) = 1 & \forall x \in \mathbb{R} \\ f_2 : \mathbb{R} \to \mathbb{R}, f_2(x) = x & \forall x \in \mathbb{R} \end{array}\right\} \Rightarrow f(x) = \lambda_1 + \lambda_2 x$$

Ausgleichsparabel

$$\left.\begin{array}{ll} f_1 : \mathbb{R} \to \mathbb{R}, f_1(x) = 1 & \forall x \in \mathbb{R} \\ f_2 : \mathbb{R} \to \mathbb{R}, f_2(x) = x & \forall x \in \mathbb{R} \\ f_3 : \mathbb{R} \to \mathbb{R}, f_3(x) = x^2 & \forall x \in \mathbb{R} \end{array}\right\} \Rightarrow f(x) = \lambda_1 + \lambda_2 x + \lambda_3 x^2$$

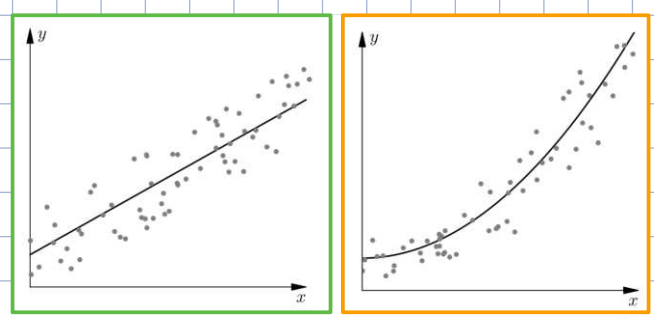


Abb. 18.1 Approximation durch eine Gerade $f = \lambda_1 + \lambda_2 t$ bzw. Parabel $f = \lambda_1 + \lambda_2 t + \lambda_3 t^2$

Lineare Abbildungen

Homomorphismus = die lineare Abbildung $f : V \to W$ -> **falls für alle** $\lambda \in \mathbb{K}$ **und alle** $v, w \in V$ **gilt** $f(\lambda v + w) = \lambda f(v) + f(w)$

Eigenschaften linearer Abbildungen

Es seien U, V **und** W **Vektorräume über einem Körper** $\mathbb{K}$

-- **Ist** $f : V \to W$ **eine lineare Abbildung, so gilt** $f(0_V) = 0_W$ **für die Nullvektoren** 0_V **von** V **bzw.** 0_W **von** W

-- **Sind** $f : V \to W$ **und** $g : W \to U$ **lineare Abbildungen, so ist die Komposition** $g \circ f : V \to U$ **auch eine lineare Abbildung**

-- **Ist** $f : V \to W$ **eine biiektive lineare Abbildung (=Isomorphismus), so ist die Umkehrabbildung** $f^{-1} : W \to V$ **eine bijektive lineare Abbildung**

Die lineare Abbildung $f_A : \mathbb{K}^n \to \mathbb{K}^m, f_A(v) = Av$

Gegeben sind Matrizen $A \in \mathbb{K}^{m \times n}$ **und** $B \in \mathbb{K}^{r \times m}$**, dann gilt:**

-- **Die Abbildung** $f_A : \mathbb{K}^n \to \mathbb{K}^n$ **mit** $f_A(v) = Av$ **ist linear**

-- **Es ist** $f_B \circ f_A = f_{BA}$ **eine lineare Abbildung von** K^n **in** K^r

-- **Es ist** $f_A : \mathbb{K}^n \to \mathbb{K}^m$ **genau dann umkehrbar, wenn** $m = n$ **und** A **invertierbar ist. In diesem Fall gilt** $f_A^{-1} = f_{A^{-1}}$

$\dim(\text{Ker}(f_A)) + \dim(\text{Bild}(f_A)) = \dim(K^n) = n$

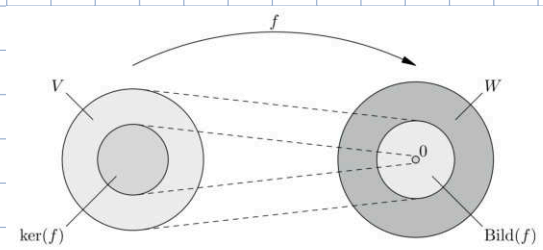
Ist $f : V \to W$ **linear, so sind Kern von** f **und Bild von** f **die Untervektorräume von** V **bzw.** W

-- **Kern von** f -> $\ker(f) = f^{-1}(\{0\}) = \{v \in V \mid f(v) = 0\} \subseteq V$

-- **Bild von** f -> $\text{Bild}(f) = f(V) = |f(v)| v \in V \,| \subseteq W$

-- **Defekt von** f $\text{def}(f) = \dim(\ker(f))$ **Dimension des Kerns**

-- **Rang von** f $\text{rg}(f) = \dim(\text{Bild}(f))$ **Dimension des Bildes**



-- **Dimensionsformel** $\dim(V) = \dim(\ker(f)) + \dim(\text{Bild}(f))$ **bzw.** $\dim(V) = \text{def}(f) + \text{rg}(f)$

-- **Die Abbildung** f **ist genau dann injektiv, wenn** $\ker(f) = \{0\}$ **bzw.** $\text{def}(f) = 0$

-- **Sind** V **und** W **endlichdimensional, so gilt im Fall** $\dim(V) = \dim(W)$ -> f **ist surjektiv** $\Leftrightarrow$ f **ist injektiv** $\Leftrightarrow$ f **ist bijektiv**

$\dim(U \cap V) = \dim(U) + \dim(V) - \dim(U + V)$

Beispiele

Für die lineare Abbildung $f : \mathbb{R} \to \mathbb{R}, f(v) = av$ **mit** $a \in \mathbb{R}$ **gilt:**

-- **Ist** $a = 0$**, so ist** $\ker(f) = \mathbb{R}$**, also , und** $\text{Bild}(f) = \{0\}$**, also** $\text{rg}(f) = 0$ -> f **weder injektiv noch surjektiv noch bijektiv**

-- **Ist** $a \neq 0$**, so ist** $\ker(f) = \{0\}$**, also** $\text{def}(f) = 0$**, und** $\text{Bild}(f) = \mathbb{P}$**, also** $\text{rg}(f) = 1$ -> -> f **injektiv, surjektiv, bijektiv**

Fur jede Matrix $A \in \mathbb{R}^{m \times n}$ **ist** $f_A : \mathbb{R}^n \to \mathbb{R}^m$**, mit** $f_A(v) = Av$ **linear. Es gilt:**

-- $\ker(f_A) = \ker(A)$ **und** $\text{def}(f_A) = n - \text{rg}(A)$

-- $\text{Bild}(f_A) = S_A$ **(-> Spaltenraum von** A**) und** $\text{rg}(f_A) = \text{rg}(A)$

Die Abbildung f_A **ist genau dann injektiv, wenn** $\text{rg}(A) = n$

Die Abbildung f_A **ist genau dann surjektiv, wenn** $\text{rg}(A) = m$

Die Abbildung f_A **ist genau dann bijektiv, wenn** $m = n$ **und** $\text{rg}(A) = n$

Für die lineare Abbildung $f : \mathbb{R}[x]_n \to \mathbb{R}[x]_n$ **mit** $f(p) = p'$ **gilt:**

-- $\ker(f) = \{p \in \mathbb{R}[x]_n \mid \deg(p) \leq 0\} = \mathbb{R}$ **, also**

-- $\text{Bild}(f) = \{p \in \mathbb{R}[x]_n \mid \deg(p) \leq n - 1\} = \mathbb{R}[x]_{n-1}$ **, also** $\text{rg}(f) = n$

Seien V und W endlich dimensionale K-Vektorräume und sei $f: V \to W$ linear. Dann gilt:

(i) f ist injektiv $\Leftrightarrow$ $\text{Kern}(f) = \{0\}$ $\Leftrightarrow$ $\dim \text{Kern}(f) = 0$ $\Leftrightarrow$ $\dim \text{Bild}(f) = \dim V$

(ii) f ist surjektiv $\Leftrightarrow$ $\text{Bild}(f) = W$ $\Leftrightarrow$ $\dim \text{Bild}(f) = \dim W$

(iii) Ist $\dim V = \dim W$, so gilt:

f ist injektiv $\Leftrightarrow$ f ist surjektiv $\Leftrightarrow$ f ist bijektiv.

Koordinatenvektoren

eine geordnete Basis des $\mathbb{K}$-Vektorraums V -> $B = (b_1, \dots, b_n)$

jeden Vektor $v \in V$ eindeutig als Linearkombination bezüglich B darstellen -> $v = \lambda_1 b_1 + \cdots + \lambda_n b_n$, wobei $\lambda_1, \dots, \lambda_n \in \mathbb{K}$

Koordinatenvektor von v bezüglich B -> ${}_Bv = (\lambda_1, \dots, \lambda_n)^\top \in \mathbb{K}^n$

für alle $\lambda \in \mathbb{K}$ und $v, w \in V$ gilt ${}_B(\lambda v + w) = \lambda {}_Bv + {}_Bw$ d.h, die bijektive Abbildung ${}_B : V \to \mathbb{K}^n, v \mapsto {}_Bv$ ist linear

Darstellungsmatrix

Es seien V und W endlichdimensionale $\mathbb{K}$-Vektorräume mit

-- $\dim(V) = n$ und $B = (b_1, \dots, b_n)$ eine Basis von V

-- $\dim(W) = m$ und $C = (c_1, \dots, c_m)$ eine Basis von W

f ist genau dann injektiv, wenn $\ker(A) = \{0\}$

f ist genau dann surjektiv, wenn $\operatorname{rg}(A) = m$

f ist genau dann bijektiv, wenn A invertierbar

Ist $f : V \to W$ linear, dann Darstellungsmatrix A von f bezüglich B und C -> $A = {}_cM(f)_B = ({}_cf(b_1), \dots, {}_cf(b_n)) \in \mathbb{K}^{m \times n}$

In der i-ten Spalte der Darstellungsmatrix steht der Koordinatenvektor des Bildes des i-ten Basisvektors

Im Sonderfall - Die linearen Abbildungen $f = f_A : \mathbb{K}^n \to \mathbb{K}^m, f_A(v) = Av$

Darstellungsmatrix $A \in \mathbb{K}^{m \times n}$ von f bezüglich E_n und E_m -> $A = {}_{E_m}M(f)_{E_n} = (f(e_1), \dots, f(e_n))$

Zusammenhang zwischen Darstellungsmatrix ${}_cM(f)_B$ und lineare Abbildung $f(v) = \lambda_1 f(b_1) + \cdots + \lambda_n f(b_n)$

$${}_cM(f)_B \, {}_Bv = ({}_cf(b_1), \dots, {}_cf(b_n)) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \lambda_1 {}_cf(b_1) + \cdots + \lambda_n {}_cf(b_n) = {}_cf(v)$$

Basistransformation

Die Darstellungsmatrix der Verkettung linearer Abbildungen

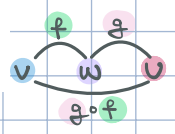
$\mathbb{K}$-Vektorraum V -> $\dim(V) = n$ und geordneter Basis $B = (b_1, \dots, b_n)$

$\mathbb{K}$-Vektorraum W -> $\dim(W) = m$ und geordneter Basis $C = (c_1, \dots, c_m)$

$\mathbb{K}$-Vektorraum U -> $\dim(U) = r$ und geordneter Basis $D = (d_1, \dots, d_r)$

lineare Abbildungen $f : V \to W$ und $g : W \to U$

Darstellungsmatrizen ${}_cM(f)_B$ und ${}_DM(g)_C$



es gilt ${}_DM(g \circ f)_B = {}_DM(g)_C \, {}_cM(f)_B$

Basistransformationsformel (BATRAFO)

im Allgemeinen ${}_{C'}M(f)_{B'} = {}_{C'}M(\mathrm{Id} \circ f \circ \mathrm{Id})_{B'} = {}_{C'}M(\mathrm{Id}_W)_C \, {}_cM(f)_B \, {}_BM(\mathrm{Id}_V)_{B'}$

im Sonderfall - Die lineare Abbildung $f : \mathbb{K}^n \to \mathbb{K}^n, f(v) = Av$ und $A \in \mathbb{K}^{n \times n}$

${}_BM(f)_B = B^{-1}AB$ bzw. ${}_BM(\mathrm{Id})_{E_n} \, {}_{E_n}M(\mathrm{Id})_B = {}_BM(\mathrm{Id})_B = E_n$

Voraussetzung

-- lineare Abbildung $f : V \to W$

-- Basen von V -> $B = (b_1, \dots, b_n)$ und $B' = (b'_1, \dots, b'_n)$

-- Basen von W -> $C = (c_1, \dots, c_m)$ und $C' = (c'_1, \dots, c'_m)$

Darstellungsmatrizen der Identitäten $\mathrm{Id} : V \to V, \ \mathrm{Id}(v) = v$ bezüglich Basen von V -> ${}_BM(\mathrm{Id})_{B'} = ({}_Bb'_1, \cdots, {}_Bb'_n) \in \mathbb{K}^{n \times n}$

Darstellungsmatrizen der Identitäten $\mathrm{Id} : W \to W, \ \mathrm{Id}(w) = w$ bezüglich Basen von W -> ${}_{C'}M(\mathrm{Id})_C = ({}_{C'}c_1, \dots, {}_{C'}c_m) \in \mathbb{K}^{m \times m}$

${}_BM(\mathrm{Id})_A$ **Basisvektoren aus Basis A dargestellt bezüglich Basis B**

Diagonalisierung

Eigenwert und Eigenvektor von Matrizen

Gegeben ist eine quadratische Matrix $A \in \mathbb{K}^{n\times n}$, gilt $Av = \lambda v$ mit $v \neq 0$ und $\lambda \in \mathbb{K}$

-- $v \in V\backslash\{0\}$ -> ein Eigenvektor von A zum Eigenwert $\lambda \in \mathbb{K}$

-- $\lambda \in \mathbb{K}$ -> einen Eigenwert von A mit Eigenvektor $v \in V\backslash\{0\}$

Ist λ ein Eigenwert von A, so nennt man den Untervektorraum

-- $\mathrm{Eig}_A(\lambda) = \{v \in \mathbb{K}^n \mid Av = \lambda v\}$ -> den Eigenraum von A zum Eigenwert λ

-- $\mathrm{geo}(\lambda) = \dim\left(\mathrm{Eig}_A(\lambda)\right)$ -> die geometrische Vielfachheit des Eigenwerts λ

Diagonalisieren von Matrizen

Diagonalmatrix $D = B^{-1}AB$ (wenn eine Matrix $A \in \mathbb{K}^{n\times n}$ diagonalisierbar bzw. eine invertierbare Matrix $B \in \mathbb{K}^{n\times n}$ gibt)

-> diagonalisierbar gdw. -> es gibt $B = (b_1, \ldots, b_n)$ und $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ (nicht notwendig alle verschieden), mit $Ab_1 = \lambda_1 b_1, \ldots, Ab_n = \lambda_n b_n$

-- Matrix $D = \mathrm{diag}\left(\lambda_1, \ldots, \lambda_n\right)$ -> die Diagonalform zu A

-- Matrix $B = (b_1, \ldots, b_n)$ -> eine die Matrix A diagonalisierende Matrix

-- Bestimmen von D und B -> das Diagonalisieren von A

Das charakteristische Polynom einer Matrix

Das charakteristische Polynom einer Matrix $A \in \mathbb{K}^{n\times n}$ -> $\chi_A = \det\left(A - xE_n\right)$

χ_A zerfällt über $\mathbb{K}$ in Linearfaktoren mit verschiedenen $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$ -> $\chi_A = (\lambda_1 - x)^{v_1} \cdots (\lambda_r - x)^{v_r}$

-- $\lambda_1, \ldots, \lambda_r$ sind die verschiedenen Eigenwerte von A

-- χ_A hat den Grad $n\ (= v_1 + \cdots + v_r)$

-- A hat höchstens n verschiedene Eigenwerte (falls $r = n$)

-- Potenz $v_i = \mathrm{alg}\left(\lambda_i\right)$ die algebraische Vielfachheit des Eigenwerts λ_i

-- Für $1 \leq i \leq r$ gilt: $1 \leq \mathrm{geo}\left(\lambda_i\right) \leq \mathrm{alg}\left(\lambda_i\right)$

Produkt der Eigenwerte -> $\det(A) = \lambda_1 \cdots \lambda_n$

Summe der Eigenwerte -> $\mathrm{Spur}(A) = \lambda_1 + \cdots + \lambda_n$

Gemeinsamkeiten ähnlicher Matrizen $A, B \in \mathbb{K}^{n\times n}$

-- $\chi_A = \chi_B$

-- A und B haben die gleichen Eigenwerte

-- Die Eigenwerte von A und B haben die gleichen $\mathrm{alg}(\lambda)$ und $\mathrm{geo}(\lambda)$

Kriterium zur Diagonalisierbarkeit

Eine Matrix $A \in \mathbb{K}^{n\times n}$ ist genau dann mit n verschiedenen Eigenwerten diagonalisierbar, wenn

-- das charakteristische Polynom χ_A über $\mathbb{K}$ in Linearfaktoren zerfällt

-- $\mathrm{alg}(\lambda) = \mathrm{geo}(\lambda)$ für jeden Eigenwert λ von A gilt

Diagonalisieren einer Matrix $A \in \mathbb{K}^{n\times n}$

(1) Bestimme das charakteristische Polynom χ_A und zerlege dieses in Linearfaktoren $\chi_A = (\lambda_1 - x)^{v_1} \cdots (\lambda_r - x)^{v_r}$

-> Es gilt $v_1 + \cdots + v_r = n$ und Es sind $\lambda_1, \ldots, \lambda_r$ die verschiedenen Eigenwerte mit der jeweiligen algebraischen Vielfachheit $\mathrm{alg}\left(\lambda_i\right) = v_i$

ACHTUNG: Ist χ_A nicht vollständig in Linearfoktoren zerlegbar, STOP: A ist nicht diagonalisierbar, sonst weiter zu (2)

(2) Bestimme zu jedem Eigenwert λ_i durch Angabe einer Basis B_i mit $|B_i| = \mathrm{geo}\left(\lambda_i\right)$ den Eigenraum $\mathrm{Eig}_A\left(\lambda_i\right) = \ker\left(A - \lambda_i E_n\right) = \langle B_i \rangle$

ACHTUNG: Gilt $\mathrm{geo}\left(\lambda_i\right) \neq \mathrm{alg}\left(\lambda_i\right)$ für ein i, STOP: A ist nicht diagonalisierbar, sonst weiter zu (3)

(3) Ordne die Basis $B = (b_1, \ldots, b_n)$ mit $Ab_1 = \lambda_1 b_1, \ldots, Ab_n = \lambda_n b_n$ -> erhalte Diagonalform zu A bzw. $D = \mathrm{diag}\left(\lambda_1, \ldots, \lambda_n\right) = B^{-1}AB$

Diagonalisierbarkeit einer reellen symmetrischen Matrix

Diagonalisierbarkeit einer reellen symmetrischen Matrix $A \in \mathbb{R}^{n\times n}$ **mit** $A^\top = A$

-- A **ist diagonalisierbar**

-- **Alle Eigenwerte von** A **sind reell**

-- **Eigenvektoren zu verschiedenen Eigenwerten stehen senkrecht aufeinander**

--> **bezüglich des Standardskalarprodukts** $\langle v, w\rangle = v^\top w$

-- **Die** A **diagonalisierende Matrix** B **kann orthogonal gewählt werden, d.h.** $B^{-1} = B$

Numerische Berechnung von Eigenwerten und Eigenvektoren

Gerschgorinkreise

$$K_i = \{z \in \mathbb{C} || z - a_{ii} \mid \leq \sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{ij}|\},\ i = 1, \ldots, n$$

Satz von Gerschgorin: **Die** n **Eigenwerte der komplexen Matrix** $A = (a_{ij}) \in \mathbb{C}^{n\times n}$ **liegen in der Vereinigung** $\bigcup_{i=1}^{n} K_i$ **der** n **Gerschgorinkreise**

Singulärwertzerlegung

Singulärwertzerlegung von $A \in \mathbb{R}^{m\times n}$ -> $A = U\Sigma V^\top$

-- **orthogonale Matrix** $U = (u_1, \ldots, u_m) \in \mathbb{R}^{m\times m}$

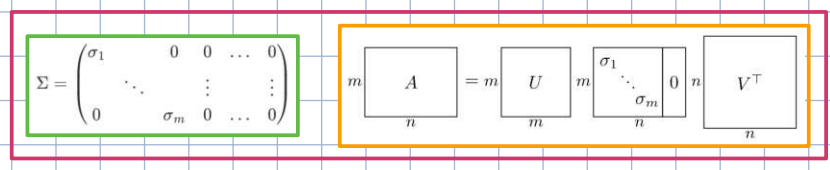
-- **orthogonale Matrix** $V = (v_1, \ldots, v_n) \in \mathbb{R}^{n\times n}$

-- **eine Diagonalmatrix** $\Sigma \in \mathbb{R}^{m\times n}$

-- **Singulärwerte** $\sigma_1, \ldots, \sigma_k$ **von** $A \in \mathbb{R}^{m\times n}$ -> $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_k \geq 0, k = \min\{m, n\}$

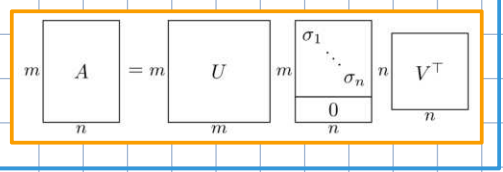
im Fall $m \leq n$

$$\Sigma = \begin{pmatrix} \sigma_1 & & 0 & 0 & \ldots & 0 \\ & \ddots & & & & \\ 0 & & \sigma_m & 0 & \ldots & 0 \end{pmatrix}$$



im Fall $n \leq m$

$$\Sigma = \begin{pmatrix} \sigma_1 & & 0 \\ & \ddots & \\ 0 & & \sigma_n \\ 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$$



Bestimmung der Singulärwertzerlegung einer Matrix

1) **Bestimme die Eigenwerte** $\lambda_1 \ldots\ldots \lambda_n$ **von** $A^\top A \in \mathbb{R}^{n\times n}$ **und ordne** $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > \lambda_{r+1} = \cdots = \lambda_n = 0$ **mit** $1 \leq r \leq n$

dann Bestimme eine $\mathrm{ONB}\ (v_1, \ldots, v_n)$ **des** R^n **aus Eigenvektoren von** $A^\top A$ -> $A^\top A v_i = \lambda_i v_i$ **und erhalte die orthogonale Matrix** V

--> **Basistransformationsformel mit den Basen** U **von** $\mathbb{R}^m$ **und** V **von** $\mathbb{R}^n$ ${}_U M(f_A)_V = {}_U M(\mathrm{Id})_{E_m E_m} M(f_A)_{E_n E_n} M(\mathrm{Id})_V = U^\top A V = \Sigma$

--> **Bild-Koordinatenvektor des** i**-ten Basisvektors steht in** i**-ten Spalte der Darstellungsmatrix, gilt** $(*)\ Av_i = \sigma_i u_i$ **für alle** $i = 1, \ldots, \min\{m, n\}$

--> **Wegen** $A^\top = V\Sigma^\top U^\top$ **hat** $A^\top$ **dieselben Singulärwerte wie** A -> **es folgt** $(**)\ A^\top u_i = \sigma_i v_i$ **für alle** $i = 1, \ldots, \min\{m, n\}$

--> **damit folgt** $A^\top A v_i \overset{(*)}{=} \sigma_i A^\top u_i \overset{(**)}{=} \sigma_i^2 v_i$ **für alle** $i = 1, \ldots n$

2) **Setze** Σ **(in Fallunterscheidung** $m \leq n$ **oder** $n \leq m$**) mit** $\sigma_i = \sqrt{\lambda_i}$ **für alle** $i = 1, \ldots, \min\{m, n\}$

3) **Bestimme** $u_1, \ldots, u_r$ **aus** $u_i = \frac{1}{\sigma_i} A v_i$ **für** $i = 1, \ldots, r$ **und ergänze im Fall** $r < m$ **die Vektoren** $u_1, \ldots, u_r$ **zu einer** ONB **bzw.** U

Definitheit

Definitheit reeller symmetrischer $n \times n$ **- Matrix** A

-- **positiv definit, falls** $v^\top A v > 0$ **für alle** $v \in \mathbb{R}^n \backslash \{0\}$ **gilt** -> Minimum

-- **negativ definit, falls** $v^\top A v < 0$ **für alle** $v \in \mathbb{R}^n \backslash \{0\}$ **gilt** -> Maximum

-- **positiv semidefinit, falls** $v^\top A v \geq 0$ **für alle** $v \in \mathbb{R}^n \backslash \{0\}$ **gilt**

-- **negativ semidefinit, falls** $v^\top A v \leq 0$ **für alle** $v \in \mathbb{R}^n \backslash \{0\}$ **gilt**

-- **indefinit, falls es Vektoren** $v, w \in \mathbb{R}^n$ **mit** $v^\top A v > 0$ **und** $w^\top A w < 0$ **gibt** -> Sattelpunkt

Feststellen der Definitheit von 2×2 **- Matrizen** $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$

1) **Bestimme** $\det(A) = ac - b^2$ **und** $\mathrm{Spur}(A) = a + c$

2) **Definitheit im Bezug auf** $\det(A)$ **und** $\mathrm{Spur}(A)$ **feststellen**

-- **Gilt** $\det(A) < 0$, **so ist** A **indetnit**

-- **Gilt** $\det(A) = 0$ **und** $\mathrm{Spur}(A) \geq 0$, **so ist** A **positiv semidefinit**

-- **Gilt** $\det(A) = 0$ **und** $\mathrm{Spur}(A) \leq 0$, **so ist** A **negativ semidefinit**

-- **Gilt** $\det(A) > 0$ **und** , **so ist** A **positiv definit**

-- **Gilt** $\det(A) > 0$ **und** $\mathrm{Spur}(A) < 0$, **so ist** A **negativ definit**

Kriterien zur Feststellung der Definitheit

Eigenwertkriterium: Eine reelle symmetrische $n \times n$ - Matrix $A \in \mathbb{R}^{n \times n}$ ist genau dann

-- positiv definit, wenn alle Eigenwerte von A positiv sind

-- negativ dehnt, wenn alle Eigenwerte von A negativ sind

-- positiv semidefinit, wenn alle Eigenwerte von A positiv oder null sind

-- negativ semidefinit, wenn alle Eigenwerte von A negativ oder null sind

-- indefinit, wenn A positive und negative Eigenwerte hat

Hauptminorenkriterium: Eine reelle symmetrische $n \times n$ - Matrix $A \in \mathbb{R}^{n \times n}$ ist genau dann

-- positiv definit, wenn alle n Hauptminoren positiv sind

-- negativ dennit, wenn die n Hauptminoren wie folgt alternierend sind: $\det(a_{ij})_{11} < 0,\ \det(a_{ij})_{22} > 0,\ \det(a_{ij})_{33} < 0, \dots$

Matrixnormen

Norm eines Vektorraums

Eine Abbildung $N : V \to \mathbb{R}$ eines $\mathbb{K}$-Vektorraums V heißt eine Norm auf V, falls gilt

(N_1) $N(v) \geq 0$ für alle $v \in V$ und $N(v) = 0 \Leftrightarrow v = 0$

(N_2) $N(\lambda v) = |\lambda| N(v)$ für alle $\lambda \in \mathbb{K}, v \in V$

(N_3) $N(v + w) \leq N(v) + N(w)$ für alle $v, w \in V$ (Dreiecksungleichung)

Einen Vektorraum mit einer Norm $(V, \|\cdot\|)$ nennt man auch normierten Vektorraum

verschiedene Normen des $\mathbb{R}^n$

1-Norm bzw. ℓ^1-Norm $\quad \|v\|_1 = N_1\left((v_1, \dots, v_n)^\top\right) = \sum_{i=1}^n |v_i| = |v_1| + \dots + |v_n|$

2-Norm bzw. euklidische Norm bzw ℓ^2-Norm $\quad \|v\|_2 = N_2\left((v_1, \dots, v_n)^\top\right) = \sqrt{\sum_{i=1}^n |v_i|^2} = \sqrt{v_1^2 + \dots + v_n^2}$

Maximumsnorm bzw. ℓ^∞-Norm $\quad \|v\|_\infty = N_\infty\left((v_1, \dots, v_n)^\top\right) = \max\{|v_i| \mid i = 1, \dots, n\}$

Die von ℓ^1-, ℓ^2 - und ℓ^∞-Norm induzierten Matrixnormen

Im Folgenden sei $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ eine quadratische Matrix

-- Die ℓ^1-Norm auf dem $\mathbb{R}^n$ induziert auf dem $\mathbb{R}^{n \times n}$ die Matrixnorm $\|\cdot\|_1$ mit $\|A\|_1 = \max\{|a_{1i}| + \dots + |a_{ni}| \mid 1 \leq i \leq n\}$ – beträgsmäßig maximale Spaltensumme

-- Die ℓ^∞-Norm auf dem $\mathbb{R}^n$ induziert auf dem $\mathbb{R}^{n \times n}$ die Matrixnorm $\|\cdot\|_\infty$ mit $\|A\|_\infty = \max\{|a_{i1}| + \dots + |a_{in}| \mid 1 \leq i \leq n\}$ – beträgsmäßig maximale Zeilensumme

-- Die ℓ^2-Norm auf dem $\mathbb{R}^n$ induziert auf dem $\mathbb{R}^{n \times n}$ die Matrixnorm $\|\cdot\|_2$ mit $\|A\|_2 = \max\{\sqrt{\mu} \mid \mu \text{ ist Eigenwert von } A^\top A\}$ – beträgsmäßig maximale Singulärwerte

erst Betrag und vergleichen

--> es ist also $\|A\|_2$ die Wurzel aus dem größten Eigenwert von $A^\top A$. Man nennt $\|\cdot\|_2$ die Spektralnorm

--> Ist $A \in \mathbb{R}^{n \times n}$ symmetrisch, $A^\top = A$, so gilt für die Spektralnorm: $\|A\|_2 = \max\{|\mu| \mid \mu \text{ ist Eigenwert von } A\}$

--> Außerdem gilt für jede Matrix $A \in \mathbb{R}^{n \times n}$ und jede von einer Vektornorm induzierte Matrixnorm $\|\cdot\|$ -> $\|A\|_2 \leq \|A\|$