LinA Spickzettel

Gruppenaxiome: $(K, \#)$

$\forall a,b,c \in K$:

- Assoziativität: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
- neutrales Element: $a\cdot e = e\cdot a = a$
- inverses Element: $a\cdot a^{-1} = a^{-1}\cdot a = e$

Abelsche (Kommutative) Gruppe:

- Kommutativität: $a\cdot b = b\cdot a$

Körper: $(K,+,\cdot)$

$(K,+)$ Abelsche Gruppe $(e=0)$

$(K,\cdot)$ Abelsche Gruppe $(e=1)$

Distributivität:

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

$a = q\cdot b + r$

$ggT(a,b)=1 \Rightarrow a \nmid b$

$a|b \wedge b|c \Rightarrow a|c$

$a\cdot b|c \Rightarrow a|b \vee b|c$

Eukl. Algorithmus

$ggT(168,36)$

$168 \bmod 36 = 24$

$36 \bmod 24 = 12$

$24 \bmod 12 = 0 \Rightarrow = 12$

$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

$(a\cdot b) \bmod m = ((a \bmod m)\cdot(b \bmod m)) \bmod m$

RSA:

p, q Prim

$n = p\cdot q$

e teilerfremd zu m : $d := e^{-1} \pmod m$: $m = (p-1)(q-1)$

crypt $y = x^e \bmod n$: decrypt $x = y^d \bmod m$

Relationen: $R \subseteq A \times B$

- reflexiv: $(a,a) \in R$
- symmetrisch: $(a,b)\in R \curvearrowright (b,a) \in R$
- antisymmetrisch: $(a,b)\in R \wedge (b,a) \in R$
- asymmetrisch: $(a,b) \in R \Rightarrow a=b$? $(b,a) \notin R$
- transitiv: $(a,b)\in R, (b,c)\in R \Rightarrow (a,c) \in R$

Kleiner Fermat:

$a^p \equiv a \pmod p$

$a^{p-1} \equiv 1 \pmod p$

Untergruppe: $G \subseteq (K,\#)$

- $(a\cdot b) \in G$
- $a \in G \Rightarrow a^{-1} \in G$

$G \neq \emptyset$

Vektorraum: V über $(K,+,\cdot)$

+: Assoziativität

+: neutrales Element

+: inverses Element

+: Kommutativ

$\cdot$: $k\cdot(h\cdot\vec{a}) = (k\cdot h)\cdot\vec{a}$

$\cdot$: $1\cdot\vec{a} = \vec{a}$

$\cdot$: $k\cdot(\vec{a}+\vec{b}) = k\cdot\vec{a} + k\cdot\vec{b}$

$\cdot$: $(k\cdot h)\cdot\vec{a} = k\cdot\vec{a} + h\cdot\vec{a}$

Normen:

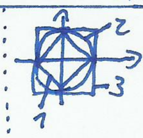
$\|\vec{a}\|_1 = \sum_i |a_i|$

$\|\vec{a}\|_2 = \sqrt{\sum_i a_i^2}$

$\|\vec{a}\|_3 = \max\{a_i\}$: $\|\vec{a}\| \geq 0$

$\|k\cdot\vec{a}\| = |k|\cdot\|\vec{a}\|$

$\|\vec{a}+\vec{b}\| \leq \|\vec{a}\| + \|\vec{b}\|$



Cauchy-Schwarzsche Ungleichung:

$\left(\sum a_i b_i\right)^2 \leq \left(\sum a_i^2\right)\cdot\left(\sum b_i^2\right)$

$\left|\sum a_i b_i\right| \leq \|\vec{a}\|\cdot\|\vec{b}\|$

Untervektorraum: $U \subseteq V$

- $U \neq \emptyset$
- $(k\cdot\vec{u}) \in U$

UVR für K

- $(\vec{u}+\vec{v}) \in U$

U_1, U_2 UVR von V:

$\dim(U_1+U_2) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2)$

$\dim(U_1 \oplus U_2) = \dim(U_1) + \dim(U_2)$

Lineare Hülle: $\mathrm{span}(a_1,\dots,a_n) = \sum_i \lambda_i \cdot a_i$

wenn $a_1,\dots,a_n$ lin. unabhängig &

$\mathrm{span}(a_1,\dots,a_n) = V \Rightarrow a_1,\dots,a_n$ Basis von V

$\Rightarrow \dim(V) = n$

Skalarprodukt:

$\langle\vec{a},\vec{b}\rangle = \vec{a}\cdot\vec{b} = |\vec{a}|\cdot|\vec{b}|\cdot\cos\varphi$

$\vec{a} \perp \vec{b} \Leftrightarrow \vec{a}\cdot\vec{b} = 0$

$\langle A\cdot\vec{a},\vec{b}\rangle = \langle\vec{a}, A^T\cdot\vec{b}\rangle$

für $\mathbb{R}_n[X]$:

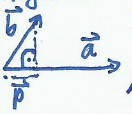
$\langle\vec{a},\vec{b}\rangle := \int_{-1}^{1} p_a(x)\cdot q_b(x)\,dx$

für $\mathbb{C}$:

$\langle\vec{a},\vec{b}\rangle := \sum_{i=1}^{n} a_i\cdot\overline{b_i}$

Projektion:

$\vec{p} = \left(\vec{b}\cdot\frac{\vec{a}}{|\vec{a}|}\right)\cdot\frac{\vec{a}}{|\vec{a}|} = \frac{\vec{b}\cdot\vec{a}}{|\vec{a}|^2}\cdot\vec{a}$



Auf UVR mit Basis W_n (ONB)

$\vec{P}_{U_0}(v) = \vec{r}_0 + \sum_{i=1}^{k} \frac{\langle\vec{v}-\vec{r}_0,\vec{w}_i\rangle}{\langle\vec{w}_i,\vec{w}_i\rangle}\vec{w}_i$

$U_0 = \vec{r}_0 + U$

LGS:

L: Lösungsmenge $A\cdot\vec{x} = \vec{b}$

$L \neq \emptyset \Rightarrow b \in \mathrm{span}(\vec{a}_1,\dots,\vec{a}_n)$

$|L| = 1 \Rightarrow \vec{a}_1,\dots,\vec{a}_n$ lin. unabhängig

Lineare Abbildung: $f(\lambda\cdot a) = \lambda\cdot f(a)$

$f(a+b) = f(a) + f(b)$ bijektiv

Drehmatrizen:

2D: $R(\alpha) = \begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}$

$R_x(\alpha) = \begin{pmatrix}1 & 0 & 0\\ 0 & \cos\alpha & -\sin\alpha\\ 0 & \sin\alpha & \cos\alpha\end{pmatrix}$; $R_y(\alpha) = \begin{pmatrix}\cos\alpha & 0 & \sin\alpha\\ 0 & 1 & 0\\ -\sin\alpha & 0 & \cos\alpha\end{pmatrix}$; $R_z(\alpha) = \begin{pmatrix}\cos\alpha & -\sin\alpha & 0\\ \sin\alpha & \cos\alpha & 0\\ 0 & 0 & 1\end{pmatrix}$

Matrizen-Rechenregeln:

- $(\lambda\cdot A)\cdot B = \lambda\cdot(A\cdot B) = A\cdot(\lambda\cdot B) = \lambda\cdot A\cdot B$
- $(A\cdot B)\cdot C = A\cdot(B\cdot C) = A\cdot B\cdot C$
- $(A+B)\cdot C = A\cdot C + B\cdot C$
- $(A+B)^T = A^T + B^T$
- $(\lambda\cdot A)^T = \lambda\cdot A^T$
- $(A^T)^T = A$

$\mathbb{1} = E_n$

- $A\cdot\mathbb{1} = \mathbb{1}\cdot A = A$
- $(A\cdot B)^{-1} = B^{-1}\cdot A^{-1}$
- $A^{P+Q} = A^P\cdot A^Q$
- $A^{-P} = (A^{-1})^P$

Trafo:

$D_{AB}(f) = T_{BB^*}\cdot D_{AB}\cdot T_{AA^*}$

$\mathrm{Ker}(A) = \{\vec{x} : A\cdot\vec{x} = \vec{0}\}$

$\mathrm{defekt}(A) = \dim(\mathrm{Ker}(A))$

$\mathrm{rang}(A) = \dim(\mathrm{Im}(A))$

Anzahl lin. unabhängiger Zeilen oder Spalten

$\mathrm{rang}(A) \leq \min(m,n)$

$\mathrm{rang}(A) = \mathrm{rang}(A^T)$

Gram-Schmidt-Verfahren: $\vec{w}_1,\dots,\vec{w}_n \to \vec{v}_1,\dots,\vec{v}_n$

$\vec{v}_1 = \|\vec{v}_1\|$, $\vec{v}_2 = \left\|\vec{w}_2 - \frac{\vec{v}_1\cdot\vec{w}_2}{\vec{v}_1\cdot\vec{v}_1}\cdot\vec{v}_1\right\|$

$\vec{v}_3 = \left\|\vec{w}_3 - \frac{\vec{v}_1\cdot\vec{w}_3}{\vec{v}_1\cdot\vec{v}_1}\cdot\vec{v}_1 - \frac{\vec{v}_2\cdot\vec{w}_3}{\vec{v}_2\cdot\vec{v}_2}\cdot\vec{v}_2\right\|$, $\vec{v}_n = \left\|\vec{w}_n - \sum \frac{\vec{v}_i\cdot\vec{w}_n}{\vec{v}_i\cdot\vec{v}_i}\cdot\vec{v}_i\right\|$

Determinanten-Rechenregeln

- $\det(A\cdot B) = \det(A)\cdot\det(B)$
- $\det(A+B) \neq \det(A) + \det(B)$
- $\det(A^{-1}) = \det(A)^{-1}$

A invertierbar falls $\det(A) \neq 0$

1.) Vertauschen von Zeilen: $A' = -\det A$

2.) Skalarmultiplikation: $A' = \lambda\cdot\det(A)$

3.) Addieren d. λ-fachen: $A' = \det(A)$

$A\cdot\vec{x} = \lambda\cdot\vec{x}$

$(A - \lambda E_n)\cdot\vec{x} = 0$

$\det(A-\lambda E_n) = 0 = \chi_A(\lambda)$

Nullstellen von χ_A

EW & EV

$\mathrm{Eig}(A,\lambda) = \mathrm{Ker}(A - \lambda E_n)$

$\mathrm{Eig}(A,\lambda) = \{\vec{x} : A\cdot\vec{x} = \lambda\cdot\vec{x}\}$

$\mathrm{diag}(A) = P^{-1}\cdot A\cdot P$

$P = (v_1\ v_2 \cdots v_n)$, $V_n = \mathrm{Eig}(A,\lambda_n)$

falls $\lambda_1 \neq \lambda_2 \Rightarrow$

$\mathrm{Eig}(A,\lambda_1) \cap \mathrm{Eig}(A,\lambda_2) = \emptyset$

Definitheit:

positiv definit:

$x^T A\cdot x > 0$ (semidef. "$\geq$")

negativ definit: $x^T\cdot A\cdot x < 0$ (semidefinit "$\leq$")

$\Rightarrow$ Vorzeichen der EW

Bzw. $\langle\vec{v},\vec{v}\rangle > 0$, usw. ..

Orthogonalmatrix: $\langle A\cdot\vec{x}, A\cdot\vec{y}\rangle = \langle\vec{x},\vec{y}\rangle$