Eberhard Karls Universität Tübingen

Mathematik für Informatiker III

Wintersemester 2019/2020

Dr. Britta Dorn

Mitschrieb von
Felix Pfeiffer

14. Februar 2020

Inhaltsverzeichnis

1 Lineare Abbildungen

Definition 1.1. *Lineare Abbildung, VR-Isomorphismus*

Seien V, W K-Vektorräume (K Körper)

a) $\varphi\colon V \to W$ heiß lineare Abbildung (VR-Homomorphismus) falls

   (i) $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2) \quad \forall v_1, v_2 \in V$ (Additivität)

   (ii) $\varphi(\lambda v) = \lambda * \varphi(v) \quad \forall v \in V, \lambda \in K$ (Homogenität)

   gilt.

b) Ist die lin. Abb. $\varphi\colon V \to W$ bijektiv, so heißt φ Isomorphismus, V und W heißen dann isomorph, $V \cong W$

Bemerkung 1.2.

$\varphi\colon V \to W$ lin. Abb.

a) $\varphi(\vec{0}) = \vec{0} \quad (\varphi(\lambda\vec{0}) = \lambda * \varphi(\vec{0}))$

b) $\varphi(\sum_{i=0}^{n} \lambda_i v_i) = \sum_{i=0}^{n} \lambda_i \varphi(v_i)$ (d.h. LK in V wurden in LK in W überführt)

Beispiel 1.3.

a) Nullabbildung: $\varphi\colon V \to W \quad v \mapsto \vec{0}$ ist linear

b) $\varphi\colon V \to V \quad v \mapsto \lambda v$ für festes $\lambda \in K$ ist linear $\quad (\lambda = 1 : \varphi = id_v)$

c) $\varphi\colon \mathbb{R}^3 \to \mathbb{R}^3 \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_2 \\ -x_3 \end{pmatrix}$ Spiegelung an x_1x_2-Ebene ist lin. Abb.

d) $\varphi\colon \mathbb{R} \to \mathbb{R} \quad x \mapsto x + 1$ nicht linear

e) $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2 \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1^2 \\ x_2 \end{pmatrix}$ nicht linear

Satz 1.4.

Sei $A \in M_{m,n}(K)$ eine Matrix. Dann ist $\varphi\colon K^n \to K^m \quad x \mapsto A * x$ eine lineare Abbildung
Beweis:
Folgt aus den Rechenregel für Matrizen (Distributivgesetz) Mathe II:
$\varphi(x + y) = A(x + y) = Ax + Ay = \varphi(x) + \varphi(y)$
$\varphi(\lambda x) = A(\lambda x) = \lambda * Ax = \lambda * \varphi(x)$
Alle bisherigen Beispiele waren in dieser Form.
1.3

a) $A = 0$ =Nullmatrix

b) $A = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda \end{pmatrix} = \lambda * E_n$

c) $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in M_{3,3}(\mathbb{R})$

Es gilt (später) ALLE lin. Abb. $K^n \to K^m$ sind in der Form 1.4 also Matrizen

Satz 1.5. *Eigenschaften des Bilds einer lin. Abb.*

Sei $\varphi\colon V \to W$ lin. Abb.

a) $U \subseteq V$ Untervektorraum von V, dann ist $\underbrace{\varphi(U)}_{\text{Bild von } U} \subseteq W$ UR von W

b) Falls $dim(U) < \infty$: $dim(\varphi(U)) \leq dim(U)$

Beweis:

a) $\varphi(U)$ ist UR
   - $\varphi(\vec{0}) \overset{1.2}{=} \varphi(\vec{0}) \in \varphi(U)$
   - Seien $u, v \in U, \lambda \in K$ Dann sind $\varphi(u), \varphi(v) \in \varphi(U)$ und damit
     $\varphi(u) + \varphi(v) \overset{\text{lin. Abb.}}{=} \varphi(u + v) \in \varphi(U)$

b) $\{u_1, ..., u_k\}$ Basis von U
   $\overset{\varphi \text{ lin.}}{\Rightarrow} \{\varphi(u_1, ..., \varphi(u_k)\}$ Erzeugendensystem von $\varphi(U)$
   $\Rightarrow$ enthält Basis
   $\Rightarrow$ Beh.

Definition 1.6. *Rang einer lin. Abb.*

$\varphi\colon V \to W$ lin. Abb. $dimV < \infty$

a) $Ker\varphi := \{v \in V \mid \varphi(v) = \vec{0}\}$ (alle Vektoren, die von φ uf $\vec{0}$ abgebildet werden) heißt der <u>Kern von φ</u> und ist eun UR von V.

b) φ ist injektiv $\Leftrightarrow Ker\varphi = \{\vec{0}\}$

Beweis:

a) UR-Kriterium
   - $\varphi(\vec{0}) \overset{=}{1.2} \vec{0} = \vec{0} \in Ker\varphi$
   - Seien $u, v \in Ker\varphi$ d.h. $\varphi(u) = \varphi(v) = \vec{0}$ und $\lambda, \mu \in K$.
     $\varphi(\lambda u + \mu v) \overset{=}{\text{lin. Abb.}} \lambda * \underbrace{\varphi(u)}_{\vec{0}} + \mu * \underbrace{\varphi(v)}_{\vec{0}} = \vec{0}$

     $\Rightarrow \lambda u + \mu v \in Ker\varphi$
     $\Rightarrow Ker\varphi$ UR

b) "$\Rightarrow$"
   $\varphi(\vec{0}) = \vec{0}$ (1.2), wegen Injektivität kann kaein weiteres Element auf $\vec{0}$ abg. werden.
   "$\Leftarrow$"
   Sei $Ker\varphi = \{\vec{0}\}$, zeige φ inj.
   Ang. es gibt $v_1, v_2 \in V$ mit $\varphi(v_1) = \varphi(v_2)$.
   Dann ist $\vec{0} = \varphi(v_1) - \varphi(v2) \overset{\text{lin. Abb.}}{=} \varphi(v_1 - v_2) = \vec{0}$
   $\Rightarrow v_1 - v_2 = \vec{0}$ (nur $\vec{0}$ wurd auf $\vec{0}$ abg. laut Vorr.)
   $\Rightarrow v_1 = v_2$
   $\Rightarrow \varphi$ inj.

Definition 1.7. *Rang einer lin. Abb.*

$\varphi\colon V \to W$

a) $Ker\varphi := \{v \in V \mid \varphi(v) = \vec{0}\}$ (alle Vektoren, die von φ auf $\vec{0}$ abgebildet werden) heißt der Kern von φ und ist ein UR von V.

b) φ ist injektiv $\Leftrightarrow Ker\varphi = \{\vec{0}\}$

Beispiel 1.8.

$\varphi\colon \mathbb{R}^3 \to \mathbb{R}^3 \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ 2x_1 \\ x_1 + x_2 + 2x_3 \end{pmatrix}$ lin. Abb., zugehörige Matrix $A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix}$

Betracete UR $U =< e_2, e_3 >$, $dimU = 2$

$\varphi(U)?$, $dim\varphi(U)?$, $Ker\varphi?$

- $\varphi(U) =< \varphi(e_2), \varphi(e_3) > \qquad \varphi(e_2) = \varphi \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \varphi(e_3) = \varphi \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$

  $=< \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} >=< \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} >= x_3$-Achse

- $dim\varphi(U) = 1$

- $Ker\varphi$: für welche $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3$ gilt $\varphi\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$?

  Löse LGS!

  $$\begin{array}{ccccccc} x_1 & & & & & = & 0 \\ 2x_1 & & & & & = & 0 \\ x_1 & + & x_2 & + & 2x_3 & = & 0 \\ \hline \end{array}$$

  $\Rightarrow x_1 = 0, x_2 - 2x_3$

  $\Rightarrow Ker\varphi = \{ \begin{pmatrix} 0 \\ -2\lambda \\ \lambda \end{pmatrix} \mid \lambda \in \mathbb{R}\}$

Satz 1.9.

Seien V, W K-VR, $dimV = n$
$\{v_1, ..., v_n\}$ Basis von V, $w_1, ..., w_n$ Vektoren aus W (nicht notw. verschieden)
Dann $\exists!$ lin. Abb. $\varphi\colon V \to W$ mit $\varphi(v_1) = w, \forall i \in \{1,,,.,n\}$ und zwar

$$\varphi\colon V \to W \qquad v = \underbrace{\sum_{i=1}^{n} \lambda_i v_i}_{\text{LK der } v_i} \mapsto \underbrace{\sum_{i=1}^{n} \lambda_i w_i}_{\text{LK der } w_i} \qquad (w_i = \varphi(v_i))$$

D.h. wenn man weiß, wie die Basisvektoren abgeb. werden, so kennt man die lin. Abb. vollständing.
Beweis:
Für jedes φ gilt:

- φ ist linear
- $\varphi(v_i) = w_i$
- φ ist eindeutig: ang. es gibt $\Psi\colon v \to W$ linear mit $\Psi(v_i) = w_i \quad \forall i$
  Dann ist $\Psi(\underbrace{\sum_{i=1}^{n} \lambda_i v_i}_{v \in V}) \overset{\text{lin. Abb.}}{=} \sum_{i=1}^{n} \lambda_i \Psi(v_i) = \sum_{i=1}^{n} \lambda_i w_i = \varphi(\sum_{i=1}^{n} \lambda_1 v_i)$

Beispiel 1.10.

$V = \mathbb{R}^2, \varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$ Drehung um Winkel α $(0 \leq \alpha \leq 2\pi)$ um Nullpunkt, gg. Uhrzeigersinn.
φ ist lin. Abb.
Darstellung mit Matrix A?
Basisvektoren:

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \overset{\varphi}{\mapsto} \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \overset{\varphi}{\mapsto} \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$$

Allg. Vektor: $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$\varphi(x) = x_1 * \varphi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) + x_2 * \varphi\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) \qquad$ SATZ 1.9!

$= x_1 * \varphi\left(\begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}\right) + x_2 * \varphi\left(\begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}\right) = \begin{pmatrix} x_1 * \cos\alpha - x_2 * \sin\alpha \\ x_1 * \sin\alpha + x_2 * \cos\alpha \end{pmatrix}$

$= Ax$ mit $A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$

Drehung um $\alpha = 0°$ $\quad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Drehung um $\alpha = 90° = \frac{\pi}{2}$ $\quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Satz 1.11. *Dimensionssatz für lin. Abb.*

V, W K-VR, $\quad dimV = n \quad \varphi\colon V \to W$ lin. Abb.
Dann gilt $dimV = dim(Ker\varphi) + \underbrace{rg(\varphi)}_{dim\varphi(V)}$

Beweis:
Sei $\{u_1, ..., u_k\}$ Basis von $Ker\varphi$. Ergänze zu Basis $\{u_1, ..., u_n\}$ von V (Basisergänzungssatz) und setze $U := < u_{k+1}, ..., u_n >_K$
Basis $< u_{k+1}, ..., u_n > \quad u_1, ..., u_k = U$
Da $Ker\varphi \cap U = \{\vec{0}\}$ und $V = Ker\varphi + U$, ist $dimV = dim(Ker\varphi) + dimU$
zeige: $dimU \overset{(1)}{=} dim\varphi(U) \overset{(2)}{=} \underbrace{dim\varphi(V)}_{rg\varphi}$

$(1) Ker\varphi \cap U = \{\vec{0}\} \Rightarrow Ker(\varphi(u)) = \{\vec{0}\} \overset{1.7\text{ b)}}{\Rightarrow} \varphi \mid u$ injektiv $\Rightarrow dimU = dim\varphi(U)$
$(2) dim\varphi(U) = dim\varphi/V)$, da $\varphi/V) = \varphi(U + Ker\varphi) \overset{\varphi \text{ lin.}}{=} \varphi(U) + \underbrace{\varphi(Ker\varphi)}_{\vec{0}} = \varphi(U)$

Korollar 1.12.

V, W K-VR mit $dimV = dimW = n$
$\varphi\colon V \to W$ lin. Abb.
Dann sind äquivalent.

a) φ surjektiv

b) φ injektiv

c) φ bijektiv

Beweis:
$1.11 \Rightarrow n = dim(Ker\varphi) + rg(\varphi)$
φ surj. $\Leftrightarrow rg\varphi = n \Leftrightarrow dim(Ker\varphi) = 0 \Leftrightarrow \varphi$ inj.

2 Matritzen und Lineare Abbildungen

Definition 2.1. *Darstellungsmatrix*

Seien V, W endlich dim VR mit geordneten Basen $\mathcal{B} = (v_1, ..., v_n\}$ (von V) und $\mathcal{C} = (w_1, ..., w_n)$ (von W)
Sei $\varphi \colon V \to W$ lin. Abb.
Stelle die Bilder $\underbrace{\varphi(v_1), ..., \varphi(v_n)}_{\in W}$ bezgl. der Basis $\mathcal{C}$ dar:

$\varphi(v_1) = a_{11} * w_1 + \ldots + a_{m1} * w_m$
$\vdots$
$\varphi(v_n) = a_{1m} * w_1 + \ldots + a_{mn} * w_m$

Dann heißt die $m \times n$ Matrix $A_\varphi^{\mathcal{B},\mathcal{C}} := \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{mn} & \ldots & a_{mn} \end{pmatrix}$
(Spalte i erhält die Koordinaten von $\varphi(v_i)$ bzgl. $\mathcal{C}$)
(Schreibeweise: auch A_φ (falls $\mathcal{B}, \mathcal{C}$) $\quad A_\varphi^{\mathcal{B}}$(falls $V = W, \mathcal{B} = \mathcal{C}$))
(Bem.: φ ist durch $A_\varphi^{\mathcal{B},\mathcal{C}}$ eindeutig best. vgl. SATZ 1.9)

Beispiel 2.2.

a) $V = W = \mathbb{R}^2, \quad \mathcal{B} = \mathcal{C} = (e_1, e_2) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$
$\varphi \colon V \to V, \quad v \mapsto 2v$ (Streckung Faktor 2)
$\varphi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 0 \end{pmatrix} = 2e_1 + 0e_2$
$\varphi\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 2 \end{pmatrix} = 0e_1 + 2e_2$
$A_\varphi^{\mathcal{B},\mathcal{C}} = A_\varphi^{\mathcal{B}} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
andere Basis $\mathcal{D} = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right)$
$\varphi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 0 \end{pmatrix} = 2 * \begin{pmatrix} 1 \\ 2 \end{pmatrix} - 2 * \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
$\varphi\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 2 \end{pmatrix} = 0 * \begin{pmatrix} 1 \\ 2 \end{pmatrix} + 1 * \begin{pmatrix} 0 \\ 2 \end{pmatrix}$
$A_\varphi^{\mathcal{B},\mathcal{D}} = \begin{pmatrix} 2 & 0 \\ -2 & 1 \end{pmatrix}$

b) $V = W$ mit $\dim V = n, \quad \mathcal{B}$ bel. Basis
$\varphi = id_v$, dann ist $A_\varphi^{\mathcal{B},\mathcal{B}} = A_\varphi^{\mathcal{B}} = E_n$

c) $V = W = \mathbb{R}^2, \quad \mathcal{B} = \mathcal{C} = (e_1, e_2)$
φ Drehung um Nullp. um Winkel α
$\Rightarrow A_\varphi^{\mathcal{B}} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$, vgl. Bsp. 1.10

d) $V = W = \mathbb{R}^2, \quad \mathcal{B} = (e_1, e_2)$
φ Spiegelung an $< e_1 >$ (x_1-Achse), d.h.:
$\varphi\colon \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ -x_2 \end{pmatrix}$
$A_\varphi^\mathcal{B} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
andere Basis: $\mathcal{B}' = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right)$
$A_\varphi^{\mathcal{B}'} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\varphi\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 0 * \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 1 * \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
$\varphi\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1 * \begin{pmatrix} 1 \\ 1 \end{pmatrix} + 0 * \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
$A_\varphi^{\mathcal{B},\mathcal{B}'} =?$
$\varphi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = a_{11} * \begin{pmatrix} 1 \\ 1 \end{pmatrix} + a_{21} * \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
$\varphi\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = a_{12} * \begin{pmatrix} 1 \\ 1 \end{pmatrix} + a_{22} * \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
$\rightarrow$ LGS lösen, erhalte $A_\varphi^{\mathcal{B},\mathcal{B}'} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$
d.h.: dieselbe lin. Abb. φ hat i.A. bzgl. anderer Wahl der Basen andere Darst. matrix!

e) umgekehrt:
$V = W = \mathbb{R}^2, \quad \mathcal{B} = (e_1, e_2)$
$A_\varphi^\mathcal{B} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$
was macht φ? was ist z.B. $\varphi\left(\begin{pmatrix} 7 \\ -5 \end{pmatrix} \right)$
geg.: Koord. eines Punktes btzl. einer Basis $\mathcal{B}$ von V. (z.B. Roboterkoord.), lin. Abb $\varphi\colon V \rightarrow W$
ges.: Koord. dieses Punktes (z.B. Weltkoord.) bzgl. Basis $\mathcal{C}$ von W $\quad\rightarrow$ später (Basiswechselmatrix)
Koord. des mit φ abg. Punktes bzgl. $\mathcal{C}$ $\quad\rightarrow$ jetzt

Satz 2.3. *Koordinatenvektorberechnung*

$V, W, \mathcal{B}, \mathcal{C}, \varphi$ wie in 2.1
Sei $v \in V$,
$\kappa_\mathcal{B}(v)$ <u>Koordinatenvektor</u> von v bzgl. $\mathcal{B}$ (enthält Koord. von v bzgl. $\mathcal{B}$)
Dann lässt sich der Koordinatenvektor von $\varphi(v)$ bzgl. $\mathcal{C}$ berechnen als

$$\underbrace{\kappa_\mathcal{C}(\varphi(v))}_{\varphi(v) \text{ in } \mathcal{C}} = \underbrace{A_\varphi^{\mathcal{B},\mathcal{C}}}_{\text{wie werden Bilder der Basiswechselmatrix } \mathcal{B} \text{ in } \mathcal{C} \text{ dargestellt?}} * \underbrace{\kappa_\mathcal{B}(v)}_{\text{welche Koord. von } v \text{ in } \mathcal{B}}$$

Beweis:

$A^{\mathcal{B},\mathcal{C}}|varphi = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \\ a_{m1} & & a_{mn} \end{pmatrix} \quad v = \sum_{i=1}^n \lambda_i v_i \quad (\lambda_i \in \kappa)$

$\kappa_{\mathcal{B}}(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$

$A_\varphi^{\mathcal{B},\mathcal{C}} * \kappa_{\mathcal{B}}(v) = \begin{pmatrix} \sum_{i=1}^n a_{1i}\lambda_i \\ \vdots \\ \sum_{i=1}^n a_{mi}\lambda_i \end{pmatrix}$

$\varphi(v) = \varphi(\sum_{i=1}^n \lambda_i v_i)$
$= \sum_{i=1}^n \lambda_i \quad \underbrace{\varphi(v_i)}_{\sum_{k=1}^m a_{ki} w_k} \quad$ (linear)

$= \sum_{k=1}^m (\underbrace{\sum_{i=1}^n \lambda_i a_{ki}}_{\text{Koord. von } \varphi(v) \text{ bzgl. } \mathcal{C}}) * w_k$

Also $\kappa_{\mathcal{C}}(\varphi(v)) = \begin{pmatrix} \sum_{i=1}^n \lambda_i a_{1j} \\ \vdots \\ \sum_{i=1}^m \lambda_i a_{mi} \end{pmatrix} = A_\varphi^{\mathcal{B},\mathcal{C}} * \kappa_{\mathcal{B}}(v)$

Beispiel 2.4.

V mit $\dim V = 3$, Basis $\mathcal{B} = (v_1, v_2, v_3)$
W mit $\dim W = 2$, Basis $\mathcal{B} = (w_1, w_2)$
$\varphi\colon V \to W$ mit $A_\varphi^{\mathcal{B},\mathcal{C}} = \begin{pmatrix} 1 & 1 & -2 \\ 2 & 0 & 3 \end{pmatrix}$
z.B. $v = 5v_1 - 2v_2 + 4v_3$

Koord. von v bzgl. $\mathcal{B}$ sind also $5, -2, 4 \quad \kappa_{\mathcal{B}}(v) = \begin{pmatrix} 5 \\ -2 \\ 4 \end{pmatrix}$

Was sind die Koord. von $\varphi(v)$ in Basis $\mathcal{C}$?

$\kappa_{\mathcal{C}}(\varphi(v)) = \begin{pmatrix} 1 & 1 & -2 \\ 2 & 0 & 3 \end{pmatrix} * \begin{pmatrix} 5 \\ -2 \\ 4 \end{pmatrix} = \begin{pmatrix} -5 \\ 22 \end{pmatrix}$

(d.h. $\varphi(v) = -5 * w_1 + 22 * w_2$, Koord sind $-5, 22$)

Bemerkung 2.5. *Korollar zu 2.3*

Der Koord. vektor kann als Bild des "Koord. ab."

$\kappa_{\mathcal{B}}\colon V \to K^n \quad v = \sum_{i=1}^n \lambda_i v_i \mapsto \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$

aufgfasst werden, dann erhalte folg. Übersicht:

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "\kappa_{\mathcal{B}}"] & W \arrow[d, "\kappa_{\mathcal{C}}"] \\ K^n \arrow[r, "\text{Mult mit } A_\varphi^{\mathcal{B},\mathcal{C}}"] & K^m \end{tikzcd}$$

$\dim W = m$ Basis $\mathcal{C}$

<u>Damit folgt.</u>
<u>Jede</u> lin. Abb $K^n \to K^m$ (K Körper) ist von der Form $\varphi(x) = Ax$ für ein $A \in M_{m,n}(K)$
<u>Beweis:</u>
Benutze kanon. Basis bon K^n bzw. K^m. Damit stimmen El. von K^n bzw. K^m mit ihren Koord. vektoren bzgl. Basis überein,
Beh. folgt mit 2.3: $\underbrace{K_{\mathcal{C}}(\varphi(v))}_{=\varphi(v)} = A_\varphi^{\mathcal{B},\mathcal{C}} \underbrace{\kappa_{\mathcal{B}}(v)}_{=v}$ also $\varphi(v) = A_\varphi^{\mathcal{B},\mathcal{C}} v$

Satz 2.6. *Eigenschaften der Darstellungsmatrix*

$V; W; U$ VR mit Basen $\mathcal{B}, \mathcal{C}, \mathcal{D}$
$\varphi, \varphi_1, \varphi_2\colon V \to W$
$\Psi\colon W \to V$ lin. Abb.
Dann gilt:

a) $A_{\varphi_1+\varphi_2}^{\mathcal{B},\mathcal{C}} = A_{\varphi_1}^{\mathcal{B},\mathcal{C}} + A_{\varphi_2}^{\mathcal{B},\mathcal{C}}$

b) $A_{\lambda\varphi}^{\mathcal{B},\mathcal{C}} = \lambda * A_{\varphi}^{\mathcal{B},\mathcal{C}}$

c) $A_{\Psi\circ\varphi}^{\mathcal{B},\mathcal{C}} = A_{\Psi}^{\mathcal{B},\mathcal{C}} * A_{\varphi}^{\mathcal{B},\mathcal{C}}$

(d.h.: Das Matrixprodukt der Darstellungsmatrix entspricht der Hintereinanderausführung von lin. Abb.)
<u>Beweis:</u>
Übungsaufgabe

Folgerung 2.7.

V K-VR, $\dim V = n$, $\mathcal{B}$ Basis, $\varphi\colon V \to V$ linear ist Darstellungsmatrix $A_\varphi^\mathcal{B}$
Dann: φ invertierbar $\Leftrightarrow A_\varphi^\mathcal{B}$ invertierbar und $A_{\varphi^{-1}}^\mathcal{B} = (A_\varphi^\mathcal{B})^{-1}$

<u>Beweis:</u>
$(\Rightarrow)$ Zeige $(A_\varphi^\mathcal{B}) * (A_{\varphi^{-1}}^\mathcal{B}) = E_n$
φ inv. bar. $\Rightarrow A_\varphi^\mathcal{B} * A_{\varphi^{-1}}^\mathcal{B} \overset{2.6}{==} A_{\underbrace{\varphi \circ \varphi^{-1}}_{id}} = E_n$
Analog: $(A_{\varphi^{-1}}^\mathcal{B}) * (A_\varphi^\mathcal{B}) = E_n$
$(\Leftarrow)$ Sei nun $A_\varphi^\mathcal{B}$ inv. bar.
$\Rightarrow \exists \gamma \in M_n(\kappa)\colon A_\varphi^\mathcal{B} * \gamma = \gamma * A_\varphi^\mathcal{B} = E_n$
γ ist Darstellungsmatrix für eine eindeutig def. lin. Abb. $\Psi\colon V \to V$ (siehe 2.1), d.h. $\gamma = A_\Psi^\mathcal{B}$
$$\Rightarrow \begin{cases} E_n = A_\varphi^\mathcal{B} * A_\Psi^\mathcal{B} \overset{2.6}{=} A_{\varphi\circ\Psi}^\mathcal{B} \\ E_n = A_\Psi^\mathcal{B} * A_\varphi^\mathcal{B} \overset{2.6}{=} A_{\Psi\circ\varphi}^\mathcal{B} \end{cases}$$
$\Rightarrow \varphi \circ \Psi = \Psi \circ \varphi = id_v$
$\Rightarrow \varphi$ besitzt Inverse Ψ

Satz 2.8. *Wdh. Mathe II*

$A \in M_n(\kappa)$ inv. bar. $\Leftrightarrow rg(A) = n$

<u>Beweis:</u>
$2.1 \Rightarrow A = A_\varphi^\mathcal{E}$ für eine end. best. lin. Abb. $\varphi\colon K^n \to K^m$ $(\varphi(v) = A * v)$
A inv. bar. $\overset{2.7}{\Leftrightarrow} \varphi$ inv. bar.
$\Leftrightarrow \varphi$ bijketiv
$\overset{1.12}{\Leftrightarrow}$ surjektiv
$\Leftrightarrow rg(\varphi) = n$
$\Leftrightarrow rg(A) = n$

Beispiel 2.9.

$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \Rightarrow rg(A) = 1 \Rightarrow A$ nicht inv. bar.
$B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow rg(B) = 2 \Rightarrow B$ inv. bar.

Beispiel 2.10. *Berechnung von A^{-1} (Wdh. Mathe II)*

Bsp.: $A = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$

Suche Matrix X, die $AX = E_n$ löst.

$AX = E_n \Leftrightarrow A \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\Leftrightarrow \underbrace{A \begin{pmatrix} x_{11} \\ x_{21} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}}_{(*)}$ und $\underbrace{A \begin{pmatrix} x_{12} \\ x_{22} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{(**)}$

Wende dazu Gauß-Algorithmus simultan auf die LGS $(*)$ und $(**)$ an. Das Ergebnis lässt sich direkt ablesen, wenn auf der linken Seite des LGS statt der Stufenform die Einheitsmatrix steht.

$$\left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{array}\right) \overset{II=I-2II}{\Rightarrow} \left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 0 & -5 & 1 & -2 \end{array}\right) \overset{(-\frac{1}{5})II}{\Rightarrow} \left(\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 0 & 1 & -\frac{1}{5} & \frac{2}{5} \end{array}\right)$$

$$\overset{I=I-II}{\Rightarrow} \left(\begin{array}{cc|cc} 2 & 0 & \frac{6}{5} & -\frac{2}{5} \\ 0 & 1 & -\frac{1}{5} & \frac{2}{5} \end{array}\right) \overset{\frac{1}{2}I}{\Rightarrow} \left(\begin{array}{cc|cc} 1 & 0 & \frac{3}{5} & -\frac{1}{5} \\ 0 & 1 & -\frac{1}{5} & \frac{2}{5} \end{array}\right)$$

$X = \begin{pmatrix} \frac{3}{5} & -\frac{1}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix} = A^{-1}$

Bemerkung: $A_\varphi^{\mathcal{B},\mathcal{C}}$ hängt von der Wahl der Basen $\mathcal{B}, \mathcal{C}$ ab.

Wie kann man einen Basiswechsel berechnen?

Beispiel 2.11.

Geg.: Basen $B' = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 7 \end{pmatrix}\right), \quad B = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}\right).$

Aufgabe: Die Koord von $\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix}$ eines Vektors $v \in \mathbb{R}^2$ bzgl. B' sind gegeben.

Wie erhält man die Kooord. von v bzgl. B?

$v = \lambda_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 4 \\ 7 \end{pmatrix} = \mu_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \mu_2 \begin{pmatrix} 2 \\ 3 \end{pmatrix}$

Geg.: λ_1 und λ_2 Koord. bzgl. B'

Ges.: μ_1 und μ_2 Koord. bzgl. B

$I: \quad \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}: \quad \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \underbrace{-1}_{\mu_1} * \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \underbrace{1}_{\mu_2} * \begin{pmatrix} 2 \\ 3 \end{pmatrix}$

$II: \quad \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}: \quad \begin{pmatrix} 4 \\ 7 \end{pmatrix} = \underbrace{2}_{\mu_1} * \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \underbrace{1}_{\mu_2} * \begin{pmatrix} 2 \\ 3 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$

$\begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \to \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$

$\overset{1.9}{\Rightarrow} \qquad \underbrace{\begin{pmatrix} -1 & 2 \\ 1 & 1 \end{pmatrix}}_{\text{Basiswechselmatrix } S_{B,B'} \text{ (Def. 2.12)}} \qquad \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}$

Definition 2.12. *Basistransformation*

V VR, $B = \{v1, ..., v_n)$, $B' = \{v'_1, ..., v'_n\}$ Basen von V
Schreibe v'_i als Linearkombination der Vektoren aus B:
$v'_1 = s_{11}v_1 + \ldots + s_{n1}v_n$
$\vdots$
$v'_n = s_{1n}v_1 + \ldots + s_{nn}v_n$
Dann heißt

$$S_{B,B'} = \begin{pmatrix} s_{11} & \ldots & s_{1n} \\ \vdots & & \vdots \\ s_{n1} & \ldots & s_{nn} \end{pmatrix}$$

Basiswechselmatrix
Spalte i enthält die Koord. von v' bzgl. Basis B.

Satz 2.13. *Umrechnung von Koordinaten*

V, B, B' wie in 2.12. Für $v \in V$ ist $K_B(v) = S_{B,B'}K_{B'}(v)$

Beweis: Sei $K_{B'}(v) = \begin{pmatrix} \lambda_1 \\ \ldots \\ \lambda_n \end{pmatrix}$

$\Rightarrow v = \sum_{k=1}^n \lambda_k \underbrace{v'_k}_{=\sum_{e=1}^n s_{ek} * v_e \text{ Def 2.12}}$

$v = \sum_{e=1}^n (\underbrace{\sum_{k=1}^n \lambda_k s_{ek}}_{\mu_e = \text{ Koord. von Basis } B}) * v_e$

Satz 2.14. *Umrechnung von Darstellungsmatritzen*

$\varphi\colon V \to W$ lin. Abb., $B.B'$ Basen von V, C, C' Basen von W.
$\Rightarrow A_\varphi^{B',C'} = S_{C',C}A_\varphi^{B,C}S_{B,B'}$

Beweis: Sei $v \in V$.
$\Rightarrow A_\varphi^{B',C'} * K_{B'}(v) \overset{2.3}{=} K_{C'}(\varphi(v))$
$\overset{2.13}{=} S_{C',C} * K_C(\varphi(v))$
$\overset{2.3}{=} S_{C',C} * A_\varphi^{B,C} * K_B(v)$
$\overset{2.13}{=} S_{C',C} * A_\varphi^{B,C} * S_{B,B'} * K_{B'}(v)$

Lemma 2.15.

V VR, B, B' Basen $\Rightarrow S_{B,B'} = (S_{B',B})^{-1}$
Beweis:
Sei $v \in V$
$S_{B,B'} * S_{B',B} * K_B(v) \overset{2.13}{=} S_{B,B'} * K_{B'} \overset{2.13}{=} K_B(v)$
$\Rightarrow S_{B,B'} * S_{B',B} = E_n$

Korollar 2.16.

$\varphi\colon V \to V$ linear, B, B' Basen von V
$S := S_{B,B'}$
$\overset{2.14}{\Rightarrow} A_\varphi^{B'} = \underbrace{S^{-1}}_{\overset{2.15}{=} S_{B',B}} A_\varphi^B \underbrace{S}_{S_{B,B'}}$

Beispiel 2.17.

Wie sieht Darstellungsmatrix einer Drehung $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$ um $\frac{\pi}{2}$ bzgl. $B = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$ aus?

$A_\varphi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ Drehung um $\frac{\pi}{2}$ bzgl. $E = (e_1, e_2)$

$A_\varphi^B = S_{B,E} A_\varphi S_{E,B}$

Es ist $S_{E,B} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow S_{B,E} = (S_{B,E})^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$

$\Rightarrow A_\varphi^B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix}$

3 Orthogonale und unitäre Matritzen

Wiederholung Mathe II 3.1. *Mathe II*

Norm, Skalarprodukt, endl. VR, ONS, ONB, Gram.Schmidt $\Rightarrow$ Folien

Definition 3.2. *Orthogonale Matrix*

Eine Matrix $A \in M_n(\mathbb{R})$ heißt orthogonal, falls ihre Spaltenvektoren ein ONB des $\mathbb{R}^n$. bilden.

Beispiel 3.3.

im $\mathbb{R}^2$

a) $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist orth. (Bem.: $\det E_n = 1$)

b) $R = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ $(\alpha \in \mathbb{R})$
$$\begin{matrix} \uparrow & \uparrow \\ s_1 & s_2 \end{matrix}$$
$(s_1|s_2) = (\cos\alpha)(-\sin\alpha) + \sin\alpha\cos\alpha = 0$
$(s_1|s_1) = (s_2|s_2) = \cos^2\alpha + \sin^2\alpha = 1$
s_1, s_2 bilden Also ONS, sind damit (Bem.: 8.8 in Mathe II) l.n.
$\Rightarrow$ bilden ONB (da $\dim \mathbb{R}^2 = 2$, 2 l.n. Vektoren sind schon Basis)
(Bem.: $\det R = 1$)

c) $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Bt orth., aber keine Rotation:
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}$, S ist Spiegelung an 1. Winkelhalbierenden (vertauscht x- und y-Koord.)
(Bem.: $\det S = -1$)

Satz 3.4. *Eigenschaften orthogonaler Matrizen*

Für eine orthogonale Matrix $A \in M_n(\mathbb{R})$ gilt:

a) $A^T A = E_n$

b) A ist inv. bar. mit $A^{-1} = A^T$
(→ zugehörige lin. Abb. ist bij.)

c) $\|Av\| = \|v\|$ (zugehörige lin. Abb. ist 'lLängentreu")

d) $|\det A| = 1$

e) A hat nur Eigenwerte mit Betrag 1

Beweis:

a) seien $s_1, ..., s_n$ Spalten von A.
A orth. $\Rightarrow s_1, ..., s_n$ ONB $\Rightarrow (s_i|s_j) = \begin{cases} 1 & \text{für } i = j \\ 0 & i \neq j \end{cases}$
$\Rightarrow A^T A = E_n$

b) folgt aus a)

c) $\|Av\|^2 = (Av \mid Av)$
$= (Av)^T Av$
$= v^T \underbrace{A^T A}_{E_n} Av$
$= v^T E_n v$
$= v^T v$
$= v \mid v)$
$= \|v\|^2$

d) $1 = \det E_n = \det(A^T A)$
$= \det A^T * \det A$
$= \det A * \det A$
$= (\det A)^2$
$\Rightarrow \det A = \pm 1$

e) Sei $\lambda \in W$ von A, d.h. $\exists v \neq 0$ mit $Av = \lambda v$.
Dann ist $\|v\| = \|Av\|$
$= \|\lambda v\|$
$= |\lambda| \|v\|$
$\Rightarrow |\lambda| = 1$

Definition 3.5. *orthogonale Gruppe*

$O(n) := \{A \in M_n(\mathbb{R} \mid A \text{ orth } \}$, die orthogonale Gruppe, und
$SO(n) := O^+(n) = \{A \in O(n) \mid \det A = 1\}$, die spezielle orth. Gruppe,
sind Untergruppen der allgemein linearen Gruppe
$OL(n, \mathbb{R}) := \{A \in M_n(\mathbb{R}) \mid A \text{ inv. bar } \}$

Definition 3.6. *orthogonale Abbildung*

Sei allgemeines V ein eukildischer VR mit Skalarprodukt $(. \mid .)$,
B ein ONB von V, $\quad \varphi \colon V \to V$ lin. Abb.
φ heißt orthogonale Abb., wenn
$(\varphi(v) \mid \varphi(w)) = (v \mid w) \quad \forall v, w \in V$ gilt.
Die Eigenschaften aus 3.4 gelten dann für A_φ^B und analog für φ.

Satz 3.7. *orthogonale Abbildung im 2-dim euklidschen Vektorraum*

Sei V ein 2-dim VR, B ONB, φ orth. Abb. auf V ($\varphi\colon V \to V$ orth. Abb.)
$A = A_\varphi^B$

a) Ist $\det A = 1$, so ist $A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ für $\alpha \in \mathbb{R}$,
φ ist Drehung/Rotation um Winkel α um Nullpunkt.

b) Ist $\det A = -1$, so ist $A = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$ für $\alpha \in \mathbb{R}$,
Dann gibt es eine ONB $\mathcal{C} = (w_1, w_2)$ von V, so dass $A_\varphi^\mathcal{C} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
φ ist Spiegelung an der Achse $< w_1 >$.

<u>Beweis:</u>
$\rightarrow$ Folien

Bemerkung 3.8. *orthogonale Abbildung im 3-dim euklifschen Vektorraum*

Sei V ein 3-dim VR, $\varphi\colon V \to V$ orth. Abb.
Dann tritt einer der folgenden Fälle auf:

a) Es ex. ONB $B = (v_1, v_2, v_3)$, so dass
$A = A_\varphi^B = \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & -1 \end{pmatrix}$ für $\alpha \in \mathbb{R}$
$\det A = -1$
(φ ist Drehspiegelung: Drehung um Achse $< v_3 >$ und Spiegelung an Ebene $< v_1, v_2 >$

Spezialfälle:

a) $\alpha = \pi$: $A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
(Achsen-)Spiegelung an $< v_3 >$

b) $\alpha = 0$: $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$
(Ebenen-)Spiegelung an $< v_1, v_2 >$

c) $\alpha = \pi$: $A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$
Punktspiegelung an Nullpunkt.

Bemerkung 3.9. *Affine Abbildungen, homogene Koordinaten*

a) Für geometrische Anwendungen reichen lin. Abb. oft nicht aus, z.B. Translation (Verschiebung) um Vektor $b \in V$:
$t\colon V \to V, \quad v \mapsto v + b$
nicht linear für $b \neq 0$

b) Die Komposition einer lin. Abb. mit einer Translation heißt affine Abbildung
$\alpha\colon V \to V, \quad v \mapsto \varphi(v) + b = (t \circ \varphi)(v)$ mit φ lin. Abb., $v \in V$

c) Affine Abb. bilden UR nicht unbedingt auf UR ab, sondern auf sogenannte affine UR der Form
$U + b = \{u + b \mid u \in U\}$ mit U UR, $b \in V$
(z.B. Geraden/Ebenen, die nicht unbedingt durch 0 gehen)

d) Affine Abb. auf n-dim eukl. VR lassen sich nicht durch $n \times n$-Matrizen beschreiben.
Es gibt aber Beschreibungen durch $(n+1) \times (n+1)$-Matrizen, sog. homogene Koordinaten
($\to$ Robotik, Computergrafik, ...)

Definition 3.10. *Skalarprodukt über $\mathbb{C}$-Vektorräume*

Sei V ein $\mathbb{C}$-VR, Eine Abb. $(* \mid *)\colon V \times V \to \mathbb{C}$, heißt hier Skalarprodukt, wenn sie folg Eig. für alle $u, v, w \in V, \quad \lambda \in \mathbb{C}$ erfüllt:

(1) konjungiertsymmetrisch (hermitesch):
$(u \mid v) = \overline{(v \mid u)}$

(2) semilinear im 1. Argument:
$\lambda u \mid v = \bar{\lambda}(u \mid v)$,
$(u + v \mid w) = (u + w) + (v \mid w)$
linear im 2. Argument:
$(u \mid \lambda v) = \lambda(u \mid v)$
$(u \mid v + w) = (u \mid v) + (u \mid w)$

(3) positiv definit:
$(v \mid v) \geq 0$ und $(v \mid v) = 0 \Leftrightarrow v = \vec{0}$
V mit $(* \mid *)$ nennt man auch Prä-Hilbertraum

Beispiel 3.11. *Standardskalarprodukt auf $\mathbb{C}^n$*

für $u, v \in \mathbb{C}^n$ ist $(u \mid v = \sum_{i=0}^{n} \bar{u}_i v_i = \bar{u}^T v$
z.B. $\left(\begin{pmatrix} i \\ 1+2i \end{pmatrix} \begin{pmatrix} 0 \\ 5 \end{pmatrix}\right) = -i * 0 + (1-3i)5 = 5 - 15i \left(\begin{pmatrix} i \\ 1+3i \end{pmatrix} \begin{pmatrix} i \\ 1+3i \end{pmatrix}\right)$
$= (-i, 1-3i) \begin{pmatrix} i \\ 1+3i \end{pmatrix} = (-i)i + (1-3i)(1+3i) = ... \in \mathbb{R}$

Definition 3.12. *unitäre Matritzen*

Eine Matrix $Q \in M_n(\mathbb{C})$ heißt unitär wenn ihre Spalten eine ONB des $\mathbb{C}^n$ bilden. (bzgl. Skalarprodukt aus 3.11)
$U(n) := \{Q \in M_n(\mathbb{C} \mid Q \text{unitär}\}$ - unitäre Gruppe,
$SU(n) := \{Q \in U(n) \mid detQ = 1\}$ - spezielle unit. Gruppe (Untergruppe von $GL(n, \mathbb{C})$, analog zu Beweis 3.5)

Satz 3.13. *Eigenschaften unitäre Matritzen*

Für $Q \in U(n)$ gilt

a) $\bar{Q}^T Q = E_n$ (nach Schreibweise Q^* für $\bar{Q}^T$ üblich, <u>Adjungierte</u> Q^H für $\bar{Q}^T$ üblich von Q)

b) Q ist inv. bar. mit $Q^{-1} = \bar{Q}^T$

c) $||Q * v|| = ||v||$ (Norm aus Skalarprodukt), (auch $(Q * v \mid Qv) = (v \mid v)$)

d) $|detQ| = 1$ (Achtung nicht nur $\pm$ 1, auch komplexe Zahlen mit Betrag 1)

e) Die Eigenwerte von Q haben Betrag 1.

Beweis:
wie für Satz 3.4.

Beispiel 3.14.

a) $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, b) $\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$ sind unitär
c) jede orth. Matrix ist unitär (über $\mathbb{C}$ betrachtet)

Beispiel 3.15. *symmetrische und hermitesche Matritzen*

a) $A \in M_n(\mathbb{R})$ heißt <u>symmetrisch</u>, falls $A = A^T$ gilt, d.h. $\underbrace{(Ax \mid y)}_{Ax)^T y = x^T A^T y =} = \underbrace{(x \mid Ay)}_{x^T Ay} \forall x, y \in \mathbb{R}^n$

b) $A \in M_n(\mathbb{C}$ heißt hermitesch, falls $A = \bar{A}^T$ gilt, d.h. $\underbrace{(Ax \mid y)}_{\bar{(}Ax)^T = \bar{x}^T A^T y =} = \underbrace{(x \mid Ay)}_{\bar{x}^T Ay}$

Beispiel 3.16.

a) $\begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \in M_2(\mathbb{R})$ symmetrisch

b) $\begin{pmatrix} 1 & i \\ -i & 0 \end{pmatrix} \in M_2(\mathbb{C})$ hermitesch

Satz 3.17. *EV/EW von hermiteschen Matritzen*

Sei $A \in M_n(\mathbb{C})$ hermitesch, dann gilt:

a) A besitzt nur reelle EW.

b) EV zu verschiedenen EW sind orthogonal.

Beweis:

a) Sei λ EW von A mit EV x, d.h. (*) $Ax = \lambda x, x \neq \vec{0}$
Dann ist $\lambda(x \mid x) \overset{3.10}{=} (x \mid \lambda x) \overset{(*)}{=} (x \mid Ax) \overset{3.15}{=} (Ax \mid x) \overset{(*)}{=} (\lambda x \mid x) \overset{3.10}{=} \bar{\lambda}(x \mid x)$
wegen $x \neq \vec{0}$ ist $(x \mid x) \neq 0$ also $\lambda = \bar{\lambda}$, also λ reell.

b) Seien $\lambda_1 \neq \lambda_2$ EW von A mit EV x_1, x_2, d.h. $Ax_1 = \lambda_1 x_1 \quad Ax_2 = \lambda_2 x_2$
Wegen a) sind λ_1, λ_2 reell.
Dann ist $\lambda_1(x_1 \mid x_2) \overset{3.10}{=} (\lambda_1 x_1 \mid \ x_2) \overset{(*)}{=} (Ax_1 \mid x_2) \overset{3.15}{=} (x_1 \mid Ax_2) \overset{(*)}{=} (x_1 \mid \lambda_2 x_2) \overset{3.10}{=} \lambda_2(x_1 \mid x_2)$
$\Leftrightarrow \lambda_1(x_1 \mid x_2) - \lambda_2(x_1 \mid x_2) = 0$
$\Leftrightarrow \underbrace{(\lambda_1 - \lambda_2)}_{\neq 0, \text{ da } \lambda_1 \neq \lambda_2} *(x_1 \mid x_2) = 0$
$\Rightarrow (x_1 \mid x_2) = 0$, d.h. x_1, x_2 orthogonal

Korollar 3.18. *EV/EW symm. Matr.*

Satz 3.17 gilt ebenso für symm. Matritzen.

Beispiel 3.19.

$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \in M_2(\mathbb{R})$ ist symm. hermitesch
mit (nachrechnen)
EW $\lambda_1 = 0, \lambda_2 = 5$ (beide reell)
EV sin z.B. $x_1 = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ EV zu $\lambda_1 = 0, x_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ EV zu $\lambda_2 = 5$ sind orthogonal

Definition 3.20. *orthogonale / unitäre Diagonalisierbarkeit*

$A \in M_n(\mathbb{R})$ heißt <u>orthogonal diagonalisierbar</u> falls es eine orthogonale Matrix $Q \in M_n(\mathbb{R})$ und eine Diagonalmatrix $D \in M_n(\mathbb{R})$ gibt, sodass $A = Q^T DQ$
(durch Umformen: $D = QAQ^T$)
$A \in M_n(\mathbb{C})$ heißt <u>unitär diagonalisierbar</u> falls es eine unitäre Matrix $U \in M_n(\mathbb{C})$ und eine Diagonalmatrix $D \in M_n(\mathbb{C})$ gibt, sodass $A = \bar{U}^T DU$
(durch Umformen: $D = UA\bar{U}^T$)

Satz 3.21.

Eine orthogonal diagonalisierbare Matrix $A \in M_n(\mathbb{R})$ ist symmetrisch.
Beweis;
Sei $A = Q^T DQ$ wie in 3.20.
$\Rightarrow A^T = (Q^T DQ)^T = Q^T D^T (Q^T)^T = Q^T DQ = A$
Im Gegensatz dazu ist eine unitär diagonalisierbare Matrix nicht unbedingt hermitesch. Es gilt aber:

Satz 3.22.

Ist $A \in M_n(\mathbb{C})$ unitär diagonalisierbar mit <u>reeller</u> Diagonalmatrix, so ist A hermitesch.
Beweis:
Sei $A = \bar{U}^T DU$ mit $\bar{D} = D$ (D reell)
$\Rightarrow \bar{A}^T = \overline{(\bar{U}^T DU)^T} = \bar{U}^T \bar{D}^T \overline{(\bar{U}^T)} = \bar{U}^T DU = A$

Satz 3.23. *Hauptachsentransformation*

a) Sei $A \in M_n(\mathbb{R})$ symm.
   Dann ist A orthogonal diagonalisierbar d.h. $A = Q^T DQ \quad (Q \in \mathcal{O}(b), D$ Diagonalmatrix)

b) Sei $A \in M_n(\mathbb{C})$ hermitesch.
   Dann ist A unitär diagonalisierbar mit reeller Diagonalmatrix, d.h. $A = \bar{U}^T DU$
   ($U \in \mathcal{U}(n), D \in M_n(\mathbb{R})$ Diagonalmatrix)

Beweis von a):
Induktion über n:
<u>IA:</u> $n = 1$, dann ist $A = (a) = D \quad (A = (1) * (a) * (1)$, orthogonal diagonalisierbar)
<u>IS:</u> (fpr $n \geq 2)n - 1 \to n$
<u>IV:</u> Die Aussage gelte für symm. Matrix $A \in M_n(\mathbb{R})$:
<u>I. Behh.:</u> Dann ist auch $A \in M_n(\mathbb{R})$, $\quad A$ symmetrisch orthogonal diagonalisierbar
Sei $A \in M_n(\mathbb{R})$, symmetrisch
$\Rightarrow A$ besitzt EW λ (reell), zugehöriger EV sei v_1, o.B.d.A. normiert ($||v_1|| = 1$)
Ergänze $v <_1$ zu ONB $(v_1, ..., v_n)$ von $\mathbb{R}^n$ (Gram-Schmidt)
Sei Q Matrix mit Spalten $v_1, ..., v_n$.
Q ist dann orthogonal.
Setzt $B = Q^T AQ$
Dann ist $B^T = (Q^T AQ)^T = Q^T A^T (Q^T)^T = Q^T AQ = B$, also ist B symmetrisch.
Es gilt $Qe_1 = v_1$ (1. Spalte von Q ist v_1) $\quad$ (*)
und damit auch $e_1 = Q^T v_1 \quad$ (**)
$\Rightarrow$ 1. Spalte von B ist $Be_1 = Q^T AQe_1$

$$\overset{(*)}{=} Q^T Av_1 \overset{\lambda\ \text{EW}}{=} Q^T \lambda v_1 = \lambda Q^T v_1 \overset{(**)}{=} \lambda e_1 = \begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

B symmetrisch $\Leftrightarrow$ 1. Zeile von B ist $(\lambda, 0, ..., 0) \Rightarrow B = \begin{pmatrix} \lambda & 0 \cdots & 0 \\ 0 & & \\ \vdots & \widetilde{B} & \\ 0 & & \end{pmatrix}$

$\overset{\text{IV.}}{\Rightarrow} \exists \widetilde{P} \in M_{n-1}(\mathbb{R})$ orthogonal, sodass $\widetilde{B} = \widetilde{P}^T \widetilde{D} \widetilde{P} \quad \widetilde{P}$ Diagonalmatrix
(bzw. $\widetilde{D} = \widetilde{P} \widetilde{B} \widetilde{P}^T$)

setzt $P := \begin{pmatrix} 1 & 0 \cdots & 0 \\ 0 & & \\ \vdots & \widetilde{P} & \\ 0 & & \end{pmatrix} \in M_n(\mathbb{R})$

$\Rightarrow P$ auch orthogonal und

$$P^TBP = \begin{pmatrix} \lambda & 0 \cdots & 0 \\ 0 & & \\ \vdots & \tilde{D} & \\ 0 & & \end{pmatrix} =: D \text{ ist ebenfalls Diagonalmatrix} \in M_n(\mathbb{R})$$

Mit Q und P ist auch QP orthogonal. Dann ist $(QP)^T\, A(QP)$

$= \underbrace{P^T \quad \underbrace{Q^TAQ}_{=B \text{ war so definiert}} \quad P}_{=D}$

d.h. A ist orthogonal diagonalisierbar

Beweis von b) folgt analog.

Beispiel 3.24. *vgl. 3.19 Bsp.*

$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \in M_2(\mathbb{R})$ symm. $\overset{3.23}{\Rightarrow}$ orth. diag. bar.

$\lambda_1 = 5, \lambda_2 = 0$

$v_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, v_2 = \begin{pmatrix} -2 \\ 1 \end{pmatrix} \in V$ (sind orthogonal)

normiere EV$*||v_1|| = \sqrt{1^2 * 2^2} = \sqrt{5} = ||v_2||$

$v_1' = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \qquad v_2' = \frac{1}{\sqrt{5}} \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ bilden ONB von $\mathbb{R}^2$.

(Achtung, falls EV zu nicht verschiedenen EW. Muss sie erst orthog. machen $\to$ Gram-Schmidt!)

setze $Q = ((v_1')(v_2')) = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$

$Q^T = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$

$D = \begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$

Dann ist $A = QDQ^T$

$= \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix} \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$

$= \frac{1}{5} \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 5 & 10 \\ 0 & 0 \end{pmatrix}$

$= \frac{1}{5} \begin{pmatrix} 5 & 10 \\ 10 & 20 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$

Exkurs 1

(Mehr zu $\mathbb{C}$ (Wdhlg. u. Neues))

1) In $\mathbb{C}$ existiert $\sqrt{-1}$: $\pm i$, d.h. $x^2+1=0$ ist lösbar in $\mathbb{C}$,
x^2+1 als Polynom in $\mathbb{C}[x]$ zerfällt in Linearfaktoren:
$x^2+1=(x+i)(x-i)$

2) Mann kann jede quadrat. Gl. $ax^2+bx+c \quad (a,b,c \in \mathbb{R}$ in $\mathbb{C}$ lösen:
$x_{1/2} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$ falls $b^2-4ac<0$, schreibe $\frac{-b\pm\sqrt{4ac-b^2}*i}{2a}$
(Bsp.: $x^2+x+2=0 \quad x_{1/2}=\frac{-1\pm\sqrt{1^2-4*1*2}}{2}=\frac{-1\pm\sqrt{-7}}{2}=\frac{-1\pm i\sqrt{7}}{2}$

3) Fundamentalsatz der Algebra:
jedes Polynom $f\in\mathbb{C}[x]$ vom Grad >1 hat <u>genau</u> n Nullstellen in $\mathbb{C}$
(D.h. es zerfällt in n Linearfaktoren)

4) $\mathbb{C}$ hat alle algebraischen und analytischen Eigenschaften wie $\mathbb{R}$ (oder besser), außer:
Es gibt auf $\mathbb{C}$ keine vollst. Ordnung $\leq$, die mit $+$ und $*$ verträglich ist.
(d.h. für die gelten würde: $a\leq b, c\leq d \Rightarrow a+c\leq b+d \quad a\leq b, r\geq 0 \Rightarrow ra\leq rb$)

5) <u>Polarkoordinaten</u>
Andere Möglichkeit komplexe Zahlen zu beschreiben:
$z=x+iy$ (Koordinatensystem im $\mathbb{R}^2$) Angabe vom Winkel φ und Abstand zum Nullpunkt.
Zu jedem $z=x+iy\in\mathbb{C}$ gibt es ein eindeutig best. $r\geq 0\in\mathbb{R}$ und ein $\varphi\in\mathbb{R}$
(nicht eind., φ im Bogenmaß) mit $z=r*(\cos\varphi+i*\sin\varphi)$
(Polarkoordinatendarstellung von z) und zwar ist $r=|z|=\sqrt{x^2+y^2}$
$\frac{x}{r}=\cos\varphi, \frac{y}{r}=\sin\varphi \Rightarrow z=x+iy=r*\cos\varphi+i(r*\sin\varphi)=r(\cos\varphi+i*\sin\varphi)$
Aus den Additionstheoremen aus $\sin, \cos$ folgt, $z_1*z_2=r_1*r_2(\cos(\varphi_1+\varphi_2)+i*\sin(\varphi_1+\varphi_2))$
$z^2=r^2(\cos(2\varphi)+i*\sin(2\varphi))$
$\pm\sqrt{z}=\pm\sqrt{r}(\cos(\frac{\varphi}{2})+i*\sin(\frac{\varphi}{2}))$ usw.
<u>Bsp.:</u>

a) $z_1=1=1+i*0$
$r_1=1, \varphi_1=0$
$z_1=1*(\underbrace{\cos 0}_{1}+i*\underbrace{\sin 0}_{0})$

b) $z_2=i=0+1*i$
$r_2=1, \varphi_2=\frac{\pi}{2}$

c) $z_3=1+i$
$r_3=\sqrt{2}, \varphi_3=\frac{\pi}{4}$

<u>Definition / Schreibweise:</u>
$e^{i\varphi}:=\cos\varphi+i*\sin\varphi$
$z=\underbrace{r}_{\text{Betrag}} *e^{(i\varphi)\to\text{Winkel}}$(Argument)
(Idee: für $z\in\mathbb{C}$ konvergiert $\sum_{k=0}^{\infty}\frac{z^k}{k!}=exp(z)=e^z$, also $e^{i\varphi}=\sum_{k=0}^{\infty}\frac{(i\varphi)^k}{k!}$
Es gilt: $i^0=1, i^1=i, i^2=-i^3=-i, i^4=i^0$

$$\to \sum_{k=0}^{\infty}\frac{(i\varphi)^k}{k!}=\underbrace{\sum_{k=0}^{\infty}(-1)^k*\frac{\varphi^{2k}}{(2k)!}}_{\cos\varphi}+i*\underbrace{\sum_{k=0}^{\infty}(-1)^k*\frac{\varphi^{2k+1}}{(2k+1)!}}_{\sin\varphi}$$

Bsp.:

a) $e^{i0} = 1$

b) $e^{i\pi} = -1$

c) $2e^{i\frac{\pi}{4}}, 3e^{-i\frac{\pi}{2}}$

d) $z = r_1 * e^{i\varphi_1}, w = r_2 * e^{i\varphi_2} \in \mathbb{C}$
$zw = r_1 * r_2 * e^{i(\varphi_1+\varphi_2)}$ (Beträge werden multipliziert, Argumente werden addiert)
$\frac{z}{w} = \frac{r_1}{r_2} * e^{i(\varphi_1-\varphi_2)} \quad (w \neq 0)$
$z^n = r^n * e^{n*i*\varphi} \quad (n \in \mathbb{N})$

e) n-te Einheitswurzeln:
in $\mathbb{R}$: Wie viele Lösungen besitzt die Gleichung $x^n = 1$? $\quad (n \in \mathbb{N})$
n ungerade: eine $(x = 1)$
n gerade: zwei $(x_1 = 1, x_2 = -1)$
in $\mathbb{C}$:
Die Gleichung $z^n = 1$ besitzt n verschiedene Lösungen $z_0, z_1, ..., z_{n-1}$, nämlich
$z_k = e^{\frac{2\pi i}{n}*k} \quad (k = 0, 1, ..., n-1)$ diese werden als die n-te Einheitswurzeln bezeichnet.
Nachrechnen:
für jedes z_k muss gelten: $(z_k)^n = 1$
$(z_k)^n = (e^{\frac{2\pi i}{n}*k}) = e^{2\pi ik} = \underbrace{(e^{2\pi i})}_{1}{}^k = 1$
Bsp: $n = 3$, dritte Einheitswurzeln.
Löse $z^3 = 1$ in $\mathbb{C}$:
$z_0 = e^{\frac{2\pi i}{3}*0} = e^0 = 1,$
$z_1 = e^{\frac{2\pi i}{3}*1} \quad \frac{2}{3}\pi \widehat{=} \frac{2}{3}180° = 120°$
$z_2 = e^{\frac{2\pi i}{3}*1} \quad \frac{3}{4}\pi \widehat{=} 240°$

Exkurs 2

Polynomdivision (mit Rest)

1) Wdhlg. Mathe II $\rightarrow$ Folien

2) Def: $f, g \in K[x]$
   f teilt g, $\quad f \mid g$, falls $\exists q \in K[x]$ mit $g = q * f$
   (nach Gradformel ist dann $grad(f) \leq grad(g)$) (falls $g \neq 0$)

3) Satz: (division mit Rest)
   $0 \neq f \in K[x], g \in K[x]$
   Dann ex. eind. best. Polynome $q, r \in K[x]$ mit $g = q * f + r$ und $grad(r) < grad(f)$
   (Beweis wie für $\mathbb{Z}$, machen wir evtl. später)

4) Bsp.:

   a) $g = x^4 + 2x^3 - x + 2$
      $f = 3x^2 - 1 \qquad \in \mathbb{R}[x]$
      $$(x^4 + 2x^3 + 0x^2 - x + 2) : (\underbrace{x^2 - 1}_{f}) = \underbrace{(\frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{9})}_{q} + r$$
      $-(x^4 - \frac{1}{3}x^2)$

      $2x^3 + \frac{1}{3}x^2 - x + 2$
      $-(2x^3 - \frac{2}{3}x)$

      $\frac{1}{3}x^2 - \frac{1}{3}x + 2$
      $-(\frac{1}{3}x^2 - \frac{1}{9})$

      $-\frac{1}{3}x + \frac{19}{9}$

   b) $g = x^4 + x^2 + 1$
      $f = x^2 + x \qquad \in \mathbb{Z}_2[x]$
      $(x^4 + 0x^3 + x^2 + 0x + 1) : (x^2 + x) = (x^2 + x) + 1$
      $-(x^4 + x^3)$

      $x^3 + x^2 + 0x + 1$
      $-(x^3 + x^2)$

      1

5) Korollar: K Körper, $a \in K$
   $f \in K[x]$ ist genau dann durch $(x - a)$ teilbar, wenn $f(a) = 0$ ist. (d.h. a ist Nullst. von f) Beweis:
   "$\Rightarrow$" $f = q * (x - a) \Rightarrow f(a) = q(a) * \underbrace{(a - a)}_{0} = 0$
   "$\Leftarrow$" $[f(a) = 0$, zeige $(x - a) \mid f$ d.h. zeige $r = 0]$
   Div. mit Rest: $f = q * (x - a) + r \qquad$ mit $\underbrace{grad(r)}_{0, -\infty} < \underbrace{grad(x - a)}_{1}$
   $\Rightarrow r$ ist konst. Polynom, also $r \in K$ (oder 0)
   $0 = f(a) = g(a) * \underbrace{(a - a)}_{0} + r \Rightarrow r = 0$

6) Anwendungsbsp.:
   Nullstellen von $f(x) = x^3 - 6x^2 + 11x - 6 \quad \in \mathbb{R}[x]$
   $\rightarrow$ rate eine Nullstelle (falls ganzzahlig Teiler von a_0 also hier $\pm 1, \pm 2, \pm 3, \pm 6$)
   z.B. $x = 1 : f(1) = 1 - 6 + 11 - 6 = 0$
   $\Rightarrow$ Polynomdivision durch $(x-1)$ ohne Rest möglich: $(x^3 - 6x^2 + 11x - 6) : (x - 1) = \underbrace{x^2 - 5x + 6}_{\text{weitere Nullst. sind 2 und 3}}$

4 Singulärwertzerlegung

Definition 4.1. *SWZ*

Sei $A \in M_{m,n}(\mathbb{C}), rg(A) = r$
Eine Singulärwertzerlegung von A (SWZ. engl. SVD) ist ein Produkt der Form $A = U\Sigma\bar{V}^T$ mit $U \in U(m), V \in U(n)$ (unitäre Matritzen) und $\Sigma \in M_{m,n}(\mathbb{R})$ der Form $\begin{pmatrix} \sigma_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & \sigma_r & \\ & 0 & & 0 \end{pmatrix}$ mit $\sigma_1 \geq \sigma_2 \geq, ..., \geq \sigma_r > 0$ den Singulärwerten von A.
(für $A \in M_{m,n}(\mathbb{R})$ sind U, V orthogonale Matritzen)

Satz 4.2. *SWZ*

Jede Matrix besitzt ein SWZ.
Beweis: mit vollst. Ind. (vgl. H.A.T.) oder konstruktiv:
(hier nur für den Fall $A \in M_{m,n}(\mathbb{R})$ - für komplexe Matrix analog!)

1) setze $B := A^T A$, dann ist $B \in M_n(\mathbb{R})$ symmetrisch.
2) Bestimme die EW $\lambda_1, ..., \lambda_n$ von B und eine ONB aus EW $v_1, ..., v_n$ von B, dabei sei $\lambda_1 \geq \lambda_2 \geq, ..., \geq \lambda_n$.
   Es gilt:
   λ_i sind reell (3.17/3.18, da B symm.) und alle ≥ 0
   $\lambda_i = \lambda_i * \underbrace{(v_i \mid v_i)}_{1,\text{ da } v \text{ ONB}}$
   $= \lambda_i * v_i^T * v_i$
   $= v_i^T * \lambda_i * v_i$
   $= v_i^T B v_i$
   $= v_i^T (A^T A) v_i$
   $= (Av_i)^T (Av_i)$
   $= (Av_i)^T (Av_i) \geq 0$
   $\lambda_1, ..., \lambda_r > 0, \lambda_{r+1} = ... = \lambda_n = 0$, da $rg(A) = rg(B) = r$
3) für $i = 1, ..., r$ setzte $u_i := \frac{1}{\sqrt{\lambda_i}} * A * v_i$
   Diese bilden ONS:
   $(u_i \mid u_j)$
   $= \frac{1}{\sqrt{\lambda_i}} (Av_i)^T \frac{1}{\sqrt{\lambda_j}} Av_j$
   $= \frac{1}{\sqrt{\lambda_i}\sqrt{\lambda_j}} v_i^T A^T A v_j$
   $= \frac{\sqrt{\lambda_j}}{\sqrt{\lambda_i}} \underbrace{(v_i \mid v_j)} = \begin{cases} \sqrt{\frac{\lambda_j}{\lambda_i}} = 1 & \text{, falls } i = j \\ 0 & \text{, falls } i \neq j \end{cases}$
4) Ergänze zu ONB $u_1, ..., u_m$ des $\mathbb{R}^m$

5) $U := (u_1, ..., u_m)$ (u_i als Spalten) $\in M_m(\mathbb{R})$
$V := (v_1, ..., v_m)$ (v_i als Spalten) $\in M_n(\mathbb{R})$
und $\sum = (s_{ij})_{i,j} \in M_{m,n}(\mathbb{R})$ mit $s_{ij} = \begin{cases} \sqrt{\lambda_i} = 1 & \text{, für } i = j \geq r \\ 0 & \text{sonst} \end{cases}$
Dann ist $A = U \sum V^T$ SWZ von A:
- V orthogonal (nach 2))
- U orthogonal (nach 3), 4))
- $U \sum V^T = \sum_{i=1}^r \sqrt{\lambda_i} \underbrace{u_i v_i^T}_{\in M_{m,n}(\mathbb{R})} = \sum_{i=1}^r A v_i v_i^T$
$= \sum_{i=1}^n A v_i v_i^T$ ($v_{r+1}, ..., v_n$ sind EV zum EW $0 = A \sum_{i=1}^n v_i v_i^T$
$= A \underbrace{V V^T}_{=E_n, \text{ da } v_1,...,v_n \text{ ONB}}$
$=A * E_n$
$= A$

Bemerkung 4.3.

a) $ker A =< v_{r+1}, ..., v_n > Im(A) =< u_1, ..., u_r >$

b) Ist A symm., entsprechen die Singulärwerte den Beträgen der EW. Sind alle EW$\geq$0 so ist die Hauptachsentransformation (H.A.T.) $A = QDQ^T$ auch eine SWZ (analog in $\mathbb{C}$)

Beispiel 4.4.

a) $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 0 & 1 \end{pmatrix} \in M_{3,2}(\mathbb{R})$

$B = A^T A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 2 & 2 \end{pmatrix}$ symm.

EW von B: $\lambda_1 = 6, \lambda_2 = 1$

EV: $v_1 = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 1 \end{pmatrix}, v_2 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 \\ -2 \end{pmatrix}$ orth., da B symm. (normieren!)

$V = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}, \sum = \begin{pmatrix} \sqrt{6} & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$

$u_1 = \frac{1}{\sqrt{6}} A v_1 = \frac{1}{\sqrt{30}} \begin{pmatrix} 2 \\ 5 \\ 1 \end{pmatrix}$

$u_2 = \frac{1}{\sqrt{1}} A v_2 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$

ergänze zu ONB des $\mathbb{R}^3$, z.B. mittels $e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ (e_2, u_1, u_2 l.u.) mit Gram-Schmidt erhalte

$w_3 = ... = \frac{1}{\sqrt{6}} \begin{pmatrix} -2 \\ 2 \\ -1 \end{pmatrix}$

$u_3 = \frac{1}{||w_3||} w_3 = \frac{1}{\sqrt{6}} \begin{pmatrix} -2 \\ 1 \\ -1 \end{pmatrix}$

$$\Rightarrow \text{SWZ: } A = U\Sigma V^T = \begin{pmatrix} \frac{2}{\sqrt{30}} & \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{6}} \\ \frac{5}{\sqrt{30}} & 0 & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{30}} & -\frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{6}} \end{pmatrix} \begin{pmatrix} \sqrt{6} & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} \end{pmatrix}$$

Beispiel 4.5. *a) aus voherigem Bsp.*

a) $A = (2\,2\,1) \in M_{1,3}(\mathbb{R}$
$B = A^T A = \begin{pmatrix} 4 & 4 & 2 \\ 4 & 4 & 2 \\ 2 & 2 & 1 \end{pmatrix}$, enthalte EW $\lambda_1 = 2, \lambda_2 = \lambda_3 = 0$
EV $v_1 = \frac{1}{3}\begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}, v_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, v_3 = \frac{1}{3\sqrt{2}}\begin{pmatrix} 1 \\ - \\ -4 \end{pmatrix}$
$V \in M_3(\mathbb{R}) = \begin{pmatrix} v_1 & v_2 & v_3 \end{pmatrix}$
$\Sigma = (3\,0\,0)$
$u_1 = \frac{1}{3}Av_1 = \frac{1}{3}(3) = (1)$
$U \in M_1(\mathbb{R}) = (1)$
$A = U\Sigma V^T$
andere Möglichkeit:
setze $\tilde{A} = A^T = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}$, führe alle Schritte mit $\tilde{A}$ durch.
$\tilde{B} = \tilde{A}^T\tilde{A} = (9) \in M_1(\mathbb{R})$ erhalte
EW $\lambda_1 = 9$
EV $v_1 = (1)$, ist bereits ONB des $\mathbb{R}^1$
$\tilde{V} = (1)$ (entspricht dem U vorher)
$\Sigma^\sim = \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}, U^\sim$ (berechne u_1, u_2, u_3) sieht wie V vorher aus.
$\tilde{A} = \tilde{U}\tilde{\Sigma}\tilde{V}^T$
$A = \tilde{A}^T = (\tilde{U}\tilde{\Sigma}\tilde{V}^T)^T = \tilde{V}\tilde{\Sigma}^T\tilde{U}^T = U\Sigma V^T$

Definition 4.6. *Pseudoinverse*

Sei $A = U\Sigma\bar{V}^T$ eine SWZ von $A \in M_{m,n}(\mathbb{C})$. Dann heißt $A^+ = V\Sigma^+\bar{U}^T$ die Pseudoinverse (oder Moore-Penrose-Inverse) von A, wobei $\Sigma^+ \in M_{n,m}(\mathbb{R})$ aus $\Sigma \in M_{m,n}(\mathbb{R})$ entseht, indem man Σ transponiert und die Elemente $\neq 0$ invertiert, also $\Sigma^+ = (s_{ij}^+)$ mit $s_{ij}^+ = \begin{cases} \frac{1}{\sigma_i} & \text{, für } i = j, \sigma \neq 0 \\ 0 & \text{sonst} \end{cases}$

(Falls $A \in M_{m,n}(\mathbb{R})$ $\quad A^+ = V\Sigma^+U^T \in M_{n,m}(\mathbb{R})$)

Bemerkung 4.7.

Für die Pseudoinverse gilt,

a) $(A^+)^T = (A^T)^+$

b) Ist $A \in M_n(\mathbb{C})$ invertierbar so ist $A^{-1} = A^+$

c) A, ist $(A\,B)^+ \neq B^+A^+$

Bemerkung 4.8. *Pseudonormallösung*

Sei $Ax = b$ ein LGS, $A \in M_{m,n}(\mathbb{C})$.
Mathe II: $m = n, A \in M_n(\mathbb{C})$ mit A inv. bar $\Rightarrow \exists$ eindeutige Lösung (und zwar $x = A^{-1}b$)
andernfalls: keine Lösung oder mehrere Lösungen möglich
Die Pseudonormallösung x^+ des LGS ist definiert als $x^+ = A^+b$, und für x^+ gilt:

1) Die Norm des Fehlers $Ax^+ - b$ ist minimal.

2) Die Norm von x^+ ist minimal.

Insbesondere gilt: Ist das LGS eindeutig lösbar, so ist x^+ die Lösung .
Ist das LGS mehrdeutig lösbar, so ist x^+ die Lösung mit kleinster Norm.

Bemerkung 4.9. *Anwendungen von SWZ*

PCA, ML: recommender Systems,
Bioinformatik

Bemerkung 4.10. *zu 3/4*

Definitheit von Matritzen
geg.: quadrat. (evtl. symm.) Matrix $A \in M_n(\mathbb{R})$.
Für $x \in \mathbb{R}^n$ beschreibt der Ausdruck $x^T Ax$ eine sog. quadratische Form. (Polynom vom Grad 2 in den Variablen $x_1, ..., x_n$), z.B. $(x_1\ x_1\ x_3) \begin{pmatrix} 2 & -3 & 0 \\ -3 & 8 & 1 \\ 0 & 1 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} =$
$2x_1^2 + 8x_2^2 + 5x_3^2 - 3x_1x_2 - 3x_2x_1 + 1x_3x_2$
(analog für $A \in M_n(\mathbb{C})$, evtl. hermitesch, mit $\bar{x}^T Ax$)
DEF (definite, semidefinite, indefinite Matrix)
$A \in M_n(\mathbb{R})$ symm. heißt

a) positiv/negativ definit, falls $x^T Ax\ > 0 / < 0 \quad \forall x \in \mathbb{R}^n, x \neq 0$

b) positiv/negativ semidefinit, falls $x^T Ax\ \geq 0 / \leq 0 \quad \forall x \in \mathbb{R}^n$ gilt.

Erfüllt A keine dieser Eigenschaften, heißt sie indefinit.
($x^T Ax$ nimmt pos. und neg. Werte an, je nach x)
(analog für $\mathbb{C}, \bar{x}^T Ax$, A hermitesch)
Kriterien für Definitheit:
$A \in M_n(\mathbb{R})$ symm. oder $A \in M_n(\mathbb{C})$ hermitesch, ist genau dann
pos. definit wenn alle EW > 0 sind.
neg. definit wenn alle EW < 0 sind.
pos. semidefinit wenn alle EW ≥ 0 sind.
neg. semidefinit wenn alle EW ≤ 0 sind.
und indefinit, wenn pos. und neg. EW existieren.
Andere Möglichkeit über Minoren ($\rightarrow$ Entwicklungssatz von Laplace)
(Det. von kleinerer Matrix, die man durch Streichen von Zeilen/Spalten erhält)

5 Elementare Zahlentheorie

Wiederholung Mathe II 5.1.

- b Teiler von a
- Division mit Rest, mod/div

Folien

Beispiel 5.2.

$a = 22,\ b = 5,\ 22 = 4 * 5 + 2$
$22 \div 5 = 4,\ 22 \mod 5 = 2$
$a = -22,\ b = 5,\ -22 = (-5) * 5 + 3$
$-22 \div 5 = -5,\ -22 \mod 5 = 3$

Bemerkung 5.3. *Eine Anwendung von 5.2*

Sind die Stellenwertsysteme zur Basis b ($b \in \mathbb{N}, b < 1$)
($b = 2$: Binärsystem, $b = 8$: Oktalsystem, $b = 10$: Dezimalsystem, $b = 16$: Hexadezimalsystem)
Mittels Division mit Rest und vollständiger Induktion lässt sich zeigen:
Jede natürliche Zahl $n \in \mathbb{N}$ lässt sich eindeutig darstellen in der Form $n = \sum_{i=0}^{k} \underbrace{xi}_{\text{Ziffern}<b} b^i$

wobei (1): $k = 0$ für $n = 0$
$b^k \leq n < b^{k+1}$ für $n > 0$
(2) $x_i \in \mathbb{N}_o$ (Ziffern von n bzgl. b)
$0 \leq x_i \leq b - 1, \quad x_k \neq 0$ für $n \neq 0$
(b-adische Darstellung von n)
Schreibweise: $n = (x_n, ..., x_0)_b$ (oder, falls b klar, z.B. $b = 10$): $n = x_k, ..., x_0$

Beispiel 5.4.

a) $b = 2$
$9 = 1 * 2^3 + 0 * 2^2 + 0 * 2^1 + 1 * 2^0$
$(9)_{10} = (1001)_2$

b) Ziffern für $b = 16$
$0, 1, ..., 9, A, B, C, D, E, F$
$(11)_{10} = B_{16}$
$(29)_{10} = 1 * 16^1 + 13 * 16^0 = (1D)_{16}$

Verfahren 5.5. *zur Bestimmung der b-adischen Darst. von $n \in \mathbb{N}_0$*

$n_0 := n, \quad x_0 := n_0 \mod b$
$n_1 := \frac{n_0 - x_0}{b}, \quad x_1 := n_1 \mod b$
$n_2 := ...$
$n_k := \frac{n_{k-1} - x_{k-1}}{b}, \quad x_k := n_k \mod b$
solange, bis $n_k < b$) (d.h. $x_k = n_k$) Dann $n = (x_k, ..., x_0)_b$

Beispiel 5.6.

$(41)_5$ im 3er-System
$(41)_5 = 4 * 5^1 + 1 * 5^0 = (21)_{10}$
$21 \mid 3 = 0$
$\frac{21-0}{3} = 7, 7 \mod 3 = 1$
$\frac{7-1}{3} = 2, 2 < 3$, fertig $\Rightarrow (41)_5 = (210)_3$

Wiederholung Mathe II 5.7.

- Kongruenzrelationmodulo $m, \mathbb{Z}_m$
- Rechenregeln für $\mod$ $\rightarrow$ Folien

Beispiel 5.8.

a) Was ist $11 * 12 * 13 \mod 7$?
$11 * 12 * 13 = 1716 \equiv 1(\mod 7)$ oder:
$11 * 12 * 13 = 132 * 13 \equiv (-1)(-1) = 1 \mod 7$ oder:
$11 * 12 * 13 = 4 * 5 * 6 = 120 \equiv 1 \mod 7$ oder:
$11 * 12 * 13 \equiv (-3)(-2)(-1) = -6 \equiv 1 \mod 7$

b) welchen Rest lässt
$(214\,935)^{2019}$ bei Div. durch 7?
$(214\,935)^{2019} = (210\,000 + 4\,900 + 35 - 1)^{2019}$
$\equiv (-1)^{2019} \equiv -1 \equiv 6 \bmod 7$, d.h. Rest: 6

Bemerkung 5.9.

Es gilt
$a \equiv b(\text{mod} m), c \in \mathbb{Z} \Rightarrow c * a = c * b(\text{mod} m)$
z.B. ist $2 * 3 = 2 * 2(\text{mod} 2)$ aber
$3 \neq 2(\text{mod} 2)$
! hier jetzt nicht teilen

Beispiel 5.10.

Welche $x \in \mathbb{Z}$ erfüllen die Konguenz $2x + 1 \equiv 5(\text{mod} 6)$?
$2x + 1 \equiv 5(\text{mod} 6) \Leftrightarrow 2x \equiv 4(\text{mod} 6)$ $\quad$ ($\not\Leftrightarrow x \equiv 2(\text{mod} 6)$ $\quad$ vgl. 5.9!)
Welche $x \in \{0, ..., 5\}$ erfüllen $2x \equiv 4(\text{mod} 6)$?
$x = 2, x = 5$
$\Rightarrow$ Lösungsmenge ist $\{2 + 6k \mid k \in \mathbb{Z}\} \cup \{5 + 6k \mid k \in \mathbb{Z}\}$

Definition 5.11. *ggT,KgV*

Seine $a_1, ..., a_r \in \mathbb{Z}$

a) Ist mind, ein $a_i \neq 0$, so ist der größte gemeinsame Teiler $ggT(a_1, ..., a_r)$ die größte nat. Zahl, die alle $a_1, ..., a_r$ teilt. (engl.: gcd)

b) Sind alle $a_i \neq 0$, so ist das kleinste gemeinsame Vielfache $KgV(a_1, ..., a_r)$ die kleinste nat. Zahl, die von allen $a_1, ..., a_r$ geteilt wird. (engl.: lcm)

c) Ist $ggT(a_1, ..., a_r) = 1$, so heißen $a_1, ..., a_r)$ teilerfremd.
Ist $ggT(a_i, a_j) = 1 \quad \forall i, j, \quad i \neq j$, so heißen $a_1, ..., a_r$ paarweise teilerfremd
(Stärker, z.B. (6,10,15) teilerfremd, aber nicht paarweise teilerfremd)

Wie berechnet man der ggT zweier Zahlen? $\rightarrow$ Euklid. Alg. (365-300 v. Chr.)

Lemma 5.12.

Seien $q, v, w \in \mathbb{Z}, v \neq 0$
Dann gilt $t \mid v$ und $t \mid w \Leftrightarrow t \mid v$ und $t \mid q * v + w$

<u>Beweis:</u>
$"\Rightarrow"$
$t \mid v$, d.h. $\exists k_1 \in \mathbb{Z}$ mit $tk_1 = v$
$t \mid w$, d.h. $\exists k_2 \in \mathbb{Z}$ mit $tk_1 = w$
$\Rightarrow q * v + w = q + tk_1 + tk_2 = t\underbrace{(qk_1 + k_2)}_{\in \mathbb{Z}}$
d.h. $t \mid qv + w$

$"\Leftarrow"$
$tk_1 = v$ wie oben,
$t \mid qv + w \Rightarrow \exists k_2 \in \mathbb{Z}$ mit $tk_2 = qv + w$
$\Rightarrow w = tk_2 - qv = tk_2 - qtk_1 = t\underbrace{(k_2 - qk1)}_{\in \mathbb{Z}}$
d.h. $t \mid w$
Damit folgt: $ggT(v, w) = ggT(v, qv + w)$
Dies ist das Grundprinzip des ggT:

Seien $a, b \in \mathbb{Z}, b \neq 0, b \nmid a$
Idee: Division mi Rest macht Aufgabe kleiner!
Setze $a_0 = a, a_1 = b$, teile mit Rest:
$a_0 = q_1 a_1 + a_2 \quad a_2$ ist Rest
$a_1 = q_2 a_2 + a_3$
$\vdots$
$a_{n-1} = q_n a_n + 0$ (erstmalig Rest 0)
Dann gilt:
$ggT(a, b) = ggT(b, a)$
$= ggT(a_1, a_0)$
$= ggT(a_1, q_1 a_1 + a_2)$
$\overset{5.12}{=} ggT(a_1, a_2)$
$= ggT(a_2, q_2 a_2 + a_3)$
$\overset{5.12}{=} (a_2, a_3)$
$\vdots$
$= ggT(a_{n-1}, a_n)$
$= ggT(a_n, a_{n-1})$
$= ggT(a_n, qa_n)$
$= a_n$
Das ist der Beweis für die Korrektheit des Eukl. Alg.

Definition 5.13. *Euklidischer Algorithmus*

Algorithm 1: `Euklidischer Algorithmus`

```
Data: a, b ∈ ℤ, nicht beide=0
Result: y = ggT(a, b)
if b = 0 then
    y := |a|
end
if b | a then
    y := |b|
end
if b ≠ 0 ∧ b ∤ a then
    x := a
    y := b
    while x mod y ≠ 0 do
        r := x mod y
        x := r
        y := r
    end
end
return y
```

Beispiel 5.14.

$a = 48, b = -30$

x	y	$x \bmod y = r$
48	-30	18
-30	18	6
18	6	0

$\rightarrow ggT(48, -30) = 6$

jetzt: wichtige Darstellung des ggT:

Satz 5.15. *Bachet de Meziriac*

Seien $a, b \in \mathbb{Z}$, nicht beide $= 0$.
$\Rightarrow \exists s, t \in \mathbb{Z}$ mit $ggT(a, b) = sa + tb$
Beweis:
$\underline{b = 0}$: $ggT(a, b) = |a| = s * a + 0 * b, \quad s = \begin{cases} 1 & , a > 0 \\ -1 & , a < 0 \end{cases}$
$\underline{b \neq 0, b \mid a}$ $ggT(a, b) = |b| = 0 * a + t * b, \quad t = \begin{cases} 1 & , b > 0 \\ -1 & , b < 0 \end{cases}$
$\underline{b \neq 0, b \nmid a}$: setze $a_0 := a, a_1 := b$
Euklidischer Algorithmus:
$a_0 = q_1 a_1 + a_2$
$a_1 = q_2 a_2 + a_3$
$\vdots$
$a_{n-1} = q_n a_n + 0$
$a_n = ggT(a_0, a_1) \quad (n \geq 2$, da $a_1 \nmid a_0)$
zeigen mit Ind:
$\exists s_j, t_j \in \mathbb{Z}$ mit $a_j = s_j * a_0 + t_j * a_1 \quad j = 0, ..., n$
$\underline{\text{I.A.:}}$ $j = 0 : s_0 = 1, t_0 = 0$
$j = 1 : s_1 = 0, t_1 = 1$
$\underline{\text{IS.:}}$ $j - 1, j - 2 \rightarrow j$
$\underline{\text{IV.:}}$ Sei $j \geq 2$ und es gelte $a_{j-2} = s_{j-2} a_0 + t_{j-2} a_1 \quad a_{j-1} = s_{j-1} a_0 + t_{j-1} a_1$
Dann $j = 0, ..., n$
$a_j = a_{j-2} - q_{j-1} a_{j-1}$
$= s_{j-2} + t_{j-2} a_1 - q_{j-1}(s_{j-1} a_o + t_{j-1} a_1)$
$= \underbrace{(s_{j-2} - q_{j-1} s_{j-1})}_{:= s_j} a_0 + \underbrace{(t_{j-2} - q_{j-1} t_{j-1})}_{:= t_j} a_1$
Beh. des Satzes folgt mit $s = s_n$, $t = t_n$.
Der Beweis liefert Alg. zur Bestimmung von s und t.

Definition 5.16. *Erweiterter Euklid. Alg. (EEA)*

Eingabe: $a, b \in \mathbb{Z}$ nicht beide $= 0$
If $b = 0$ then $y := |a|, t := 0$
    if $a > 0$ then $s := 1$ else $s := -1$ endif
endif
If $b \mid a$ then $y := |b|, s := 0$
.   if $b > 0$ then $t := 1$ else $t := -1$ endif
endif
If $b \neq 0$ and $b \nmid a$ then $x := a, y := b, s_1 := 1, s_2 := 0, t_1 := 0, t_2 := 1$
    while $(x \mod y) \neq 0$ do
        $q := x \div y, r := x \mod y, s := s_1 - q s_2, t := t_1 - q t_2, s_1 := s_2, s_2 := s,$
        $t_1 := t_2, t_2 := t, x := y, y := r$
    endwhile
endif
Ausgabe: $y = ggT(a, b), s, t$ (mit $y = sa + tb$)

Beispiel 5.17.

$a = 48, b = -30$

mod	x	y	s_1	s_2	s	t_1	t_2	t	q	r
	48	-30	1	0		0	1			
$48 \mod (-30) = 18$	-30	18	0	1	1	1	1	1	-1	18
$-30 \mod 18 = 6$	18	$\underline{6}$	1	2	2	1	3	3	-2	6
$18 \mod 6 = 0$										

Also $ggT(48, -30) = 6 = 2 * 48 + 3(-30)$

Achtung: Darstellung des $ggT(a, b)$ als $sa + tb$ ist nicht eindeutig, z.B. 6=7+48+11*(-30)

Bessere Methode: (Jameel):

48=(-1)(-30)+18

-30=(-2)(18)+6

18=3*6+0 $\Rightarrow ggT(48, -30) = 6$

6=-30+2*18 = -30+2(48-30) = $\underbrace{3}_{a}$*(-30)+$\underbrace{2}_{b}$*48

Anwendungen 5.18. *des EEA*

vgl. Mathe II: wie findet man die multiplikative Inverse von $z \in \mathbb{Z}_m$

(d.h. z^{-1} mit $z * z^{-1} = 1$ in $\mathbb{Z}_m$)

Dort gezeigt: $z \in \mathbb{Z}_m$ ist invertierbar $\Leftrightarrow ggT(z, m) = 1$

EEA liefert dann zu z und m Zahlen $s, t \in \mathbb{Z}$ mit $z * s + m * t = 1 \quad (ggT(z, m)$

$\Rightarrow (z * s) \mod m = 1$

$\Rightarrow s = z^{-1} \mod m$

Bsp.: 3^{-1} in $\mathbb{Z}_7$?

EEA: 3*$\underbrace{(-2)}_{s}$+7*(1)=1 $\quad s, -2 \mod 7 = 5 = 3^{-1}$ in $\mathbb{Z}_7$

4^{-1} in $\mathbb{Z}_9$? (ex, da $ggT(4, 9) = 1$)

4*$\underbrace{(-2)}_{s}$+9*(1)=1 $\quad s, -2 \mod 9 = 7 = 4^{-1}$ in $\mathbb{Z}_9$

Korollar 5.19.

$a, b \in \mathbb{Z}$, nicht beide $= 0$, $c \in \mathbb{Z}$

a) a, b teilerfremd $\Leftrightarrow \exists s, t \in \mathbb{Z} : sa + tb = 1$

b) a, b teilerfremd $\Rightarrow$ falls $a \mid bc$, dann $a \mid c$

Beweis:

a) "$\Rightarrow$" 5.15

"$\Leftarrow$" sei $d = ggT(a, b)$, dann $d \mid a, d \mid b$

$\Rightarrow d \mid \underbrace{sa + tb}_{=1} \Rightarrow d = 1$

b) 5.15: $\exists s, t \in \mathbb{Z}$ mit $1 = sa + tb$

$\Rightarrow c = sac + tbc$

Da $a \mid a$ und $a \mid bc = a \mid \underbrace{sca + tbc}_{=0}$

Definition 5.20. *Primzahl*

Eine nat.Zahl $p > 1$ heißt Primzahl (PZ), wenn sie nur 1 und p als Teiler besitzt.
$(ggT(k, p) = 1 \forall k \leq k \leq p - 1)$

Satz 5.21. *Lemma von Euklied*

p PZ, $a_1, ..., a_k \in \mathbb{Z}, p \mid a_1 * ... * a_k \Rightarrow \exists j$ mit $p \mid a_j$

Beweis:
Induktion nach k
IA.: $k = 1$
IS.: $k - 1 \to k$ (Beh. gelte für $k - 1$)
falls $p \mid a_k$, dann fertig
falls $p \nmid a_k$, dann ist $ggT(a_k, p) = 1$ da p PZ
Nach 5.19 b) gilt dann $p \mid \underbrace{a_1 * ... * a_{k-1}}_{\text{hierfür gilt I.A. d.h.} p \mid a_j, \text{ für } j \in \{1, ..., k-1\}}$

Theorem 5.22. *Fundamentalsatz der elementaren Zahlentheorie*

Zu jeder nat. Zahl $n \geq 2$ gibt es endl. viele verschiedene Primzahlen $p_1, ..., p_k$ und nat. Zahlen $e_1, ..., e_k$ mit $n = p_1^{e_1} * ... * p_k^{e_k}$
Die p_j heißen Primfaktoren (Primteiler) von n.
Die Darstellung von n als Produkt von PZ ist bis auf die Reihenfolge eindeutig.

Beweis: Existenz
verschärfte Induktion nach n
I.A.: $n = 2$ ist PZ
I.S.: $2, 3, ..., n \to n + 1$
Sei $n \geq 2$
I.V.: Aussage gelte für $2, ..., n$
z.z.: Aussage gilt dann auch für $n + 1$
Ist $n + 1$ bereits PZ, so gilt Aussage
Ist $n + 1$ keine PZ, so ist $n + 1 = a * b$ für $a, b \in \{2, ..., n\}$
Nach I.V. sind a und b Produkt von PZ $\Rightarrow n + 1$ ist ebenfalls Prod. von PZ.

Eindeutigkeit:
Sei $n = p_1^{e_1} * ... * p_k^{e_k} = q_1^{f_1} * ... * q_m^{f_m}$
p_i, q_i PZ, p_i und q_i paarweise verschieden
$e, f \in \mathbb{N}$
Nach 5.21: jedes p_i teilt eines der q_j, d.h. $p_i = q_j$, da q_j PZ
Ebenso umgekehrt
$\Rightarrow \{p_1, ..., p_k\} = \{q_1, ..., q_m\}, k = m$
oBdA sei $p_i = q_i \quad \forall i = 1...k$
Gibt es ein l mit $e_l \neq f_l$, so sei oBdA $e_l < f_l$.
Teile beide Seiten durch $p_l^{e_l}$, erhalte $p_1^{e_1} * ... * p_{l-1}^{e_{l-1}} * p_{l+1}^{e_{l+1}} * ... * p_k^{e_k} = p_1^{f_1} * ... * p_{l-1}^{f_{l-1}} * p_l^{f_{l-e_l}} * p_{l+1}^{f_{l+1}} * ... * p_l^{f_k}$
p_l teilt rechte Seite, wegen Gleichheit also auch die linke Seite, also teilt es nach 5.21 ein p_l, $j \neq l$.
Dann gilt aber $p_l = p_j$ (da PZ) $\lightning$ (zu paarweise versch. PZ p_j) $\Rightarrow e_i = f_i \quad \forall i = 1, ..., k$

Korollar 5.23. *Euklid*

Es gibt undenlich viele PZ.
<u>Beweis:</u>
Ang., es gibt nur endlich viele PZ $p_1, ..., p_n$.
Bilde $a = p_1 * ... * p_n + 1$
<u>5.22</u> $\exists$ PZ q mit $q \mid a$
Also gilt $q = p_i$ für ein i
$\Rightarrow q \mid \underbrace{a}_{q|a} - \underbrace{p_1 * ... * p_n}_{q=p_i, q|p_1*...*p_n} = 1 \quad ↯$

Satz 5.24. *Chinesischer Restsatz*

Seien $m_1, ..., m_n \in \mathbb{N}$ paarweise teilerfremd, $M = m_1 * ... * m_n, \quad a_1, ..., a_n \in \mathbb{Z}$
Dann existiert ein x, $0 \leq x < M$ mit
$x = a_1(\text{mod} m_1)$
$x = a_2(\text{mod} m_2)$
$\vdots$
$x = a_n(\text{mod} m_n)$

<u>Beweis:</u>
Für jedes $i \in \{1, .., n\}$ sind die Zahlen m_i und $M_i = \frac{M}{m_i}$ teilerfremd.
$\Rightarrow EEA$ liefert s_i und $t_i \in \mathbb{Z}$ mit $t_i m_i + s_i M_i = 1$
setze $e_i = s_i M_i$, dann gilt:
$e_i \equiv 1 \text{ mod } m_i$
$e_i \equiv 0 \text{ mod } m_j \quad (j \neq i)$
Die Zahl $x := \sum_{i=1}^{n} a_i e_i (\text{mod} M) \quad (= (a_1 e_1)(\text{mod} M) + (a_2 e_2)(\text{mod} M) + ...)$
ist dann die Lösung der simultanen Konguenz.

Beispiel 5.25.

a) Finde $0 \leq x < 60$ mit $x = \begin{cases} 2 & \text{mod} 3 \\ 3 & \text{mod} 4 \\ 2 & \text{mod} 5 \end{cases}$
$M = 3 * 4 * 5 = 60$
$M_1 = \frac{60}{3} = 20, M_2 = \frac{60}{4} = 15, M_3 = \frac{60}{5} = 12$
EEA liefert $7 * 3 + (-1) * 20 e_1 = -20$
$4 * 4 + (-1) * 15 = 1 \quad e_2 = -15$
$5 * 5 + (-1) * 24 = 1 \quad e_1 = -24$
$\Rightarrow (2 * (-20) + 3 * (-15) + 2 * (-24)) \text{ mod } 60 = 47$

b) Was ist 2^{1000} mod $\underbrace{1155}_{3*5*7*11}$

2^{1000} mod $3 \equiv (-1)^{1000}$ mod $3 = 1$
2^{1000} mod $5 = 4^{500}$ mod $5 \equiv (-1)^{500} = 1$
2^{1000} mod $7 = 2^{3*333+1}$ mod $7 = 8^{333} * 2^1$ mod $7 \equiv 1 * 2$ mod $7 = 2$
2^{1000} mod $11 = 2^{5*200}$ mod $11 = 32^{200}$ mod $11 \equiv (-1)^{200}$ mod $11 = 1$

Suche $0 \leq x < 1155$ mit $x = \begin{cases} 1 & \text{mod} 3 \\ 1 & \text{mod} 5 \\ 2 & \text{mod} 2 \\ 1 & \text{mod} 11 \end{cases}$, denn dann ist $x \equiv 2^{1000}$ mod $\begin{matrix} 3 \\ 5 \\ 7 \\ 11 \end{matrix}$, also auch
$x \equiv 2^{1000}$ mod 1155.
$\rightarrow$ chin. Restsatz liefert $x = 331$. (nachrechnen!)

Definition 5.26. *Lösung bei chin. Restsatz ist eindeutig*

$\rightarrow$ Folien

Wiederholung Mathe II 5.27. *Eulersche φ-Funktion*

Für $n \in \mathbb{N}$ ist $\varphi(n) := |\{a \in \mathbb{N} \mid 1 \leq a \leq n \wedge ggT(a,n) = 1\}|$ die Anzahl der zu n teilerfremden Zahlen zw. 1 und n.
z.B. $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2\varphi(4) = 2, \varphi(7) = 6, p$ PZ $\varphi(p) = p - 1$

Korollar 5.28.

$M = m_1 * ... * m_n, m_i$ paarw. teilerfremd (wie in 5.24)
$\varphi(M) = \varphi(m_1) * ... * \varphi(m_n)$
Insbesondere $n = p_1^{e_1} * ... * p_k^{e_k}$ (p, PZ, paarw. verschieden, $e_i > 0$)
dann $\varphi(n) = \varphi(p_1 - 1)p_1^{e_1 - 1} * ... * (p_k - 1)p_k^{e_k - 1}$
Bsp.: $\varphi(19854) ==?$
$19854 = 3^4 * 5 * 7^2$
$\Rightarrow \varphi(19854) = 2 * 3^3 * 4 * 5^0 * 6 * 7^1 = 9072$

<u>Beweis:</u> Nach Bem 5.26 ist
$\mathbb{Z}_M \tilde{=} \mathbb{Z}_m \times ... \times \mathbb{Z}_{mn}$ mittels ψ
$\Rightarrow x$ inv.bar. im Ring $\mathbb{Z}_M \Leftrightarrow \varphi(x) = (x \text{ mod } m_1, ..., x \text{ mod } m_n)$ inv. bar. im RIng $\mathbb{T}_{m1} \times ... \times \mathbb{Z}_{mn} \Leftrightarrow x$ mod m_j inv. bar. in $\mathbb{Z}_{mj}$ $\quad \forall i = 1...n$
Also $\varphi(M) = \varphi(m_1) * ... * \varphi(m_n)$
$a \in \mathbb{N} \quad \varphi(p^a) = \underbrace{p^a}_{\#\text{ Zahlen 1 bis } p^a} - \underbrace{p^{a-1}}_{=p^{a-1}*(p-1)}$ alle, die nicht teilbar zu p^a sind.
(Alle Vielfachen von p)

Wiederholung 5.29. *K[x]*

$\rightarrow$ Folien
$(K[x], x, *, 1, 0$, Grad, Gradformel, inv. El., f teilt g, DIV. mit Rest,
$f \in K[x]$ durch $(x - a)$ teilbar $\Leftrightarrow f(a) = 0)$

Definition 5.30. *normiert, ggT, KgV in K[x]*

a) $f = \sum_{i=0}^{n} a_i x^i$, grad$f = n$, heißt normiert, falls $a_n = 1$

b) $g, h \in K[x]$ nicht beide=0
$f \in K[x] = ggT(g, h)$, falls f normiertes Polynom von max. Grad ist, das g und h teilt.

c) $g, h \in K[x] \setminus \{0\}$
$f \in K[x] = KgV(g, h)$ falls f norm. Poly von kleinstem $\underbrace{\text{Grad}}_{\geq 0}$ ist, das von g und h geteilt wird.

Bemerkung 5.31.

$f = \sum_{i=0}^{n} a_i x^i, \quad a_n \neq 0,$
dann ist $a_n^{-1} f = x^n + ...$ normiertes Polynom.
+z.B. $f = 3x^2 + x + 7 \in \mathbb{R}[x]$,
dann $\frac{1}{3} f = x^2 + \frac{1}{3} x + \frac{7}{3}$ normiert.
in $\mathbb{Z}_1 1[x]$:
$4f = x^2 + 4x + 6$ normiert
(4 ist inv. El. vin 3, denn $3 * 4 = 12 \equiv 1 \bmod 11$)
Wie in $\mathbb{Z}$ lassen sich nun der euklid. Alg., der EEA und der Satz von Meziriac beweisen.

Satz 5.32. *Euklid. Alg. in K[x]*

Algorithm 2: `Euklidischer Algorithmus in` $K[x]$

Data: $g, h \in K[x]$, beide nicht 0

Result: $d = ggT(g, h), s, t$

if $h = 0$ **then**

  $y := g$

end

if $h \mid g$ **then**

  $y := h$

end

if $h \neq 0 \wedge h \nmid g$ **then**

  $x := g$

  $y := h$

  while $x \bmod y \neq 0$ **do**

    $r := x \bmod y$

    $x := y$

    $y := r$

  end

end

$d := a_n^{-1} y$ (für $y = a_n x^n + ... + a_1 x + a_0$ und $a_n \neq 0$, d.h. nomiere y)

return d $(= ggT(g, h))$

Satz 5.33. *EEA in K[x]*

Algorithm 3: `Erweiterter Euklidischer Algorithmus in` $K[x]$

Data: $g, h \in K[x]$, beide nicht 0
Result: $d = ggT(g, h), s, t$

if $h = 0$ **then**
    $y := g$
    $s := 1$
    $t := 0$
end
if $h \mid g$ **then**
    $y := h$
    $s := 0$
    $t := 1$
end
if $h \neq 0 \wedge h \nmid g$ **then**
    $x := g$
    $y := h$
    $s_2 := 1$
    $s_1 := 0$
    $s := 0$
    $t_2 := 0$
    $t_1 := 1$
    $t := 1$ **while** $x \bmod y \neq 0$ **do**
        $q := x \operatorname{div} y$
        $r := x \bmod y$
        $s := s_2 - qs_1$
        $t := t_2 - qt_1$
        $s_2 := s_1$
        $s_1 := s$
        $t_2 := t_1$
        $t_1 := t$
        $x := y$
        $y := r$
    end
end
$d := a_n^{-1} y$ (für $y = a_n x^n + ... + a_1 x + a_0$ und $a_n \neq 0$, d.h. nomiere y)
$s := a_n^{-1} s$
$t := a_n^{-1} t$ **return** d *(*$= ggT(g, h)$*)*, s, t *(mit* $d = sg + th$*)*

Satz 5.34. *von Bizout*

$g, h \in K[x]$, nicht beide 0
Dann ex. $s, t \in K[x]$, sodass
$f = s * g + t * h$ ein ggT von g und h ist.

Beispiel 5.35.

$g = x^4 + x^3 + 2x^2 + 1$
$h = x^3 + 2x^2 + x$
$g, h \in \mathbb{Z}_3[x]$

$x \bmod y$	x	y	s_2	s_1	s	t_2	t_1	t	g	r
	g	h	1	0	0	0	1	1		
$x^2 + x$	h	$x^2 + x$	0	1	1	1	$(2x + 1)$	$(2x + 1)$	$(x + 2)$	$(x^2 + x)$
$2x + 2$	$(x^2 + x)$	$(2x + 2)$	1	$(2x + 2)$	$(2x + 2)$	$(2x + 1)$	x^2	x^2	$(x + 1)$	$(2x + 2)$
0										

$(x^4 + x^3 + 2x^2 + 0x + 1) : (x^3 + 2x^2 + 2) = \underbrace{(x + 2)}_{=q}$

$-(x^4 + 2x^3 + 2x)$

$2x^3 + 2x^2 + x + 1$
$-(2x^3 + x^2 + 1)$

$\underbrace{x^2 + x}_{=r}$

$s = s_2 - 1s_1 = 1 - q * 0 = 1$
$t = t_2 - qt_1 = 0 - (x + 2) * 1 = 2x + 1$
$s_2 = s_1 = 0$
$s_1 = s = 1$
$t_2 = t_1 = 1$
$t_1 = t = (2x + 1)$
$x = y = h$
$y = r = x^2 + x$

$while(x \bmod y) \neq 0 : x = h, y = x^2 + x$
$(x^3 + 2x^2 + 0x + 2) : (x^2 + x) = \underbrace{(x + 1)}_{q}$

$-(x^3 + x^2)$

$x^2 + 2$
$-(x^2 + x)$

$\underbrace{2x + 2}_{r}$

$s = s_2 - 1s_1 = 0 - (x + 1) * 1 = 2x + 2$
$t = t_2 - qt_1 = 1 - (x + 1) * (2x + 1)$
$= 1 - (2x^2 + x + 2x + 1)$
$= 1 - (2x^2 + 1)$
$= x^2$

$s_2 = s_1 = 1$
$s_1 = s = 2x + 2$
$t_2 = t_1 = (2x + 1)$
$t_1 = t = x^2$
$x = y = x^2 + x$
$y = r = 2x + 2$

Prüfe $x \bmod y) \neq 0$?
$(x^2 + x) : (2x + 2) = 2x$
$-(x^2 + x)$

0

$d = a_n^{-1} y = \underbrace{2^{-1}}_{=2} * (2x + 2)$
$= x + 1$
$s = 2 * (2x + 2) = x + 1$
$t = 2(x^2) = x^2$

Überprüfe: $d = s * g + t * h$?
$(x + 1)(x^4 + x^3 + 2x^2 + 1) + 2x * 2(x^3 + 2x2 + 2)$
$= x^5 + x^4 + 2x^3 + x + x^4 + x^3 + 2x^2 + 1 + 2x^5 + x^4 + x^2$
$= x + 1 = d$

Definition 5.36. *irreduzible Polynome*

Ein Polynom $p \in K[x], Grad(p) \geq 1$
(d.h.: $p \neq 0, p$ nicht konstant, also nicht inv. bar.)
heßt irreduzibel, falls gilt:
Ist $p = f * g \quad (f, g \in K[x])$
so ist $Grad(f) = 0$ oder $Grad(g) = 0$
(d.h. f oder g muss konst. Polynom sein)
(Bem.: $p = a * (a^{-1} * p), \quad a \in \ K[x] \setminus \{0\}$ geht immer, es gibt also immer Teiler $\neq 1$ (konst. Poly.))

Beispiel 5.37.

a) $ax + b \quad (a \neq 0)$ ist irreduzibel in $K[x]$ für jeden Körper K
(Teiler sind nur konst. Polyn., keine von größerem Grad)

b) $x^2 - x \in \mathbb{Q}[x]$ ist irreduzibel:
ang. nicht, dann $(x^2 - 2) = (ax + b) * (cx + d)$ mit $(a, b, c, d \in \mathbb{Q}, \quad a, c \neq 0$
$(ax + b)$ hat Nullstelle $-\frac{b}{a}$,
also müsste auch $x^2 - 2$ Nullstelle $\underbrace{-\frac{b}{a}}_{\in\mathbb{Q}}$ haben
Nullstellen von $x^2 - x$ sind aber nur $\sqrt{2}$ und $-\sqrt{2}$, beide nicht in $\mathbb{Q}$

c) $x^2 - x \in \mathbb{R}[x]$ ist nicht irreduzibel:
$(x^2 - 2) = \underbrace{x + \sqrt{2}}_{\in\mathbb{R}[x]} * \underbrace{x - \sqrt{2}}_{\in\mathbb{R}[x]}$

d) $x^2 + 1 \in \mathbb{R}[x]$ ist irreduzibel,
denn $x^2 + 1$ hat keine Nullstelle in $\mathbb{R}$

e) $x^2 + 1 \in \mathbb{Z}_5[x]$ ist nicht irreduzibel:
2 und 3 sind Nullstellen:
$(x^2 + 1) = (x + \underbrace{3}_{\text{Nullst. 3}})(x + 2) = (x^2 + \underbrace{2x + 3x}_{=0} + 1)$

Abschlussbem 5.38.

a) Irred. Polyn. in $K[x]$ entspr. den PZ in $\mathbb{Z}$.
Man kann zeigen:
$f = \sum^n i = 0 a_i x^i \in K[x], \quad a_n \neq 0, n \geq 1.$
Dann ex. eind. best. irred. Polyn.
$p_1, ..., p_l$ und nat. Zahlen $e_1, ..., e_l \in \mathbb{Z}$ mit
$f = a_n * p^{e_1} * ... * p_l^{e_l}$

b) Geg.: PZ p, dann gibt es Körper mit p elementen, nämlich $(\mathbb{Z}, +, *)$
Man kann zeigen:
Zu jeder PZ Potenz p^a gibt es Körper mit p^a El., diesen konstruiert man über irred. Polynome in $\mathbb{Z}_p[x]$

6 Mehr zu Gruppen

Wiederholung Mathe II 6.1. *Gruppe, Untergruppe*

siehe Folien

Satz 6.2. *Nebenklassen von Untergruppen (UG)*

Sei $(G, *)$ Gruppe, $U \leq G$

a) Durch $x \underset{u}{\sim} y \Leftrightarrow x * y^{-1} \in U$ kurz: $(x \sim y)$
wird auf G eine Äquivalenzrelation definiert.
Beweis:
$\sim$ ist
reflexiv:: $x \sim x$ gilt $\forall x \in G$ denn $x * x^{-1} = e \in U$
symmetrisch: z.z.: $x \sim y \Rightarrow y \sim x$
Sei $x \sim y$, d.h. $xy^{-1} \in U$ dann ist $yx^{-1} = (xy^{-1})^{-1} \in U$ also ist $y \sim x$
transitiv: z.z. $x \sim y$ und $y \sim z \Rightarrow x \sim z$ Übung!

b) Für $x \in G$ ist $Ux = \{ux \mid u \in U\}$ die Äquivalenzklasse von x und heißt Rechtsnebenklasse von U in G.
Also (Eig. von Äquivalenzklassen, Mathe I)

- $Ux = Uy \Leftrightarrow x \sim y$, also $xy^{-1} \in U$
- $x, y \in G$, dann ist entweder $Ux = Uy$ oder $Ux \cap Un = \emptyset$

(Analog: Linksnebenkl.: $x \overset{u}{\sim} y \Leftrightarrow x^{-1}y \in U$
Beweis:

- sei $x \sim y$, dann zeige dass $y \in Ux$.
$x \sim y \Rightarrow y \sim x \Rightarrow yx^{-1} \in U$
$\Rightarrow y = y(x^{-1}x) = (yx^{-1})x \in Ux$

- sei $y \in Ux$, dann zeige, dass $x \sim y$ gilt:
$y \in Ux \Rightarrow y = ux$ für ein $u \in U$
$\Rightarrow xy^{-1} = x(ux)^{-1} = x * (x^{-1}u^{-1}) = u^{-1} \in U$, d.h. $x \sim y$

Beispiel 6.3.

$G = (\mathbb{Z}, +)$, $3\mathbb{Z} = \{\dots, -3, 0, 3, 6, 9, \dots\}$, $U = (3\mathbb{Z}, +) \leq G$ (vgl. Mateh II)
Inverses zu y in $(\mathbb{Z}, +)$ ist $-y$
$x \sim y \Leftrightarrow xy^{-1} \in U$, also
$x + (-y) \in U$
$x - y \in U$
$x = 0 : U + 0 = \{u + 0 \colon u \in U\} = \{\dots, -3, 0, 3, 6, 9, \dots\} = U = 3\mathbb{Z}$
$x = 1 : U + 1 = \{u + 1 \colon u \in U\} = \{\dots, -2, 1, 34, 7, 10, \dots\} = 1 + 3\mathbb{Z}$
$x = 2 : U + 2 = \{u + 2 \colon u \in U\} = \{\dots, -1, 2, 5, 8, 11, \dots\} = 2 + 3\mathbb{Z}$
$x = 3 : U + 3 = \{u + 3 \colon u \in U\} = \{\dots, 0, 3, 6, 9, 12 \dots\} = U + 0 = 3\mathbb{Z}$
$x = 4 : U + 4 = U + 1$
$\vdots$
usw.

Die Äquivalenzklassen von $3\mathbb{Z}$ in $\mathbb{Z}$ sind die Konguenzklassen vom mod3.
Allg.:
$G = (\mathbb{Z}, +)$ $U = (n\mathbb{Z}, +)$, $\quad n \in \mathbb{N}$
$x \sim y \Leftrightarrow x - y \in U$ d.h. $x - y = n * k$ für ein $k \in \mathbb{Z}$
$\Leftrightarrow x \equiv y \bmod n$
$\Leftrightarrow x \bmod n = y \bmod n$

Lemma 6.4. *Mächtigkeit von Nebenklassen*

G Gruppe, U endl. Ugr. von G, $x \in G$
Dann ist $|U| = |Ux|$

Beweis:
Abb. $\varphi\colon U \to Ux \quad u \mapsto ux$ ist surjektiv (ganz Ux wird getroffen, siehe 6.2 b))
und injektiv (falls $u_1x = u_2x$, dann ist $u_1 = u_2$ (Kürzungsrgel in Gr.)), also φ bij., also U, Ux gleichmächtig.

Theorem 6.5. *Satz von Lagrange*

G endl. Gr., $U \leq G$
Dann ist $|U|$ Teiler von $|G|$ und $q = \frac{|G|}{|U|}$ ist die Anzahl der Rechtsnebenklassen von U in G.
Beweis:
Seien $Ux_1, ..., Ux_q$ die q verschiedenen Rechtsnebenkl. von U in G.
Mathe I und 6.2
$G = \cup_{i=1}^{q} Ux_i$ (disj. Vereinigung der Äq. Kl.)
$\Rightarrow |G| = \sum_{i=1}^{q} |Ux_i| \overset{6.4}{=} q * |U|$

Definition 6.6. *Potenzen/Vielfache von Gruppenelementen*

$(G, *, e)$ Gruppe, $a \in G$
Definiere
$a^0 := e$
$a^1 := a$
$a^m := a^{m-1} * a \quad$ für $m \in \mathbb{N}$
$a^m := (a^{-1})^{-m} \quad m \in \mathbb{Z}^-$
(Be: Gr. mit additiver Verknüpfung $(G, +, e)$:
$0 * a := e$
$1 * a := a$
$$m * a := \begin{cases} (m-1) * a + a & \text{für } m \in \mathbb{N} \\ -m * (-1) & \text{für } m \in \mathbb{Z}^- \end{cases}$$

Satz 6.7.

G, a wie in 6.6

a) $(a^{-1} =^m = (a^m)^{-1} = a^{-m} \quad \forall m \in \mathbb{Z}$

b) $a^m * a^n = a^{m+n} \quad \forall m \in \mathbb{Z}$

c) $(a^m)^n = a^{m*n} \quad \forall m \in \mathbb{Z}$

Beweis:
$(a^{-1})^m * a^m = \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{m \text{ mal}} * \underbrace{a * a * \ldots * a}_{m \text{ mal}} = e$
$\Rightarrow (a^{-1} =^m = (a^m)^{-1}$
nach Def. 6.6 ist $a^{-m} = (a^{-1})^m$
$\Rightarrow$ a) gilt $\forall m \in \mathbb{N}$

- $\underline{m = 0}$ $e = e = e$
- $\underline{m \in \mathbb{Z}}$ dann ist $-m \in \mathbb{Z}$ wende bewiesenen Teil an auf a^{-1} statt a und $-m$ statt m, Beh. folgt
  b) c) per Ind. mit a)

Satz 6.8. *Ordnung, Zyklische Gruppen*

G endl. Gr. $\quad g \in G$

a) Es ex. eine kleinste nat. Zahl n mit $g^n = e$, diese heißt die Ordnung $o(g)$ von g.

b) Die Menge $\{g^0 = a, g^1 = g, g^2, \ldots, g^{n-1}\}$ ist eine Untergr. von G,
die von g erzeugte zyklische Gruppe $< g >$.
Es gilt $a(g) = | < g > | = n \mid |G|$.

c) $g^{|G|} = e$

d) Eine endl. Gr. heißt zyklisch, falls sie von einem El. erzeugt werden kann.

Beweis:

a) G endl. $\Rightarrow \exists i, j \in \mathbb{N}, i > j$ mit $g^i = g^j$
Dann ist $g^{j-j} = g^i + g^{-j} = g^i (g^j)^{-1} = g^i * (g^j)^{-1} = e$

b)
- Produkt zweier El. aus $< g >$ liegt wieder in $< g >$ (also abgeschl.)
- neutr. El. ist $g^0 = e$
- inv. El. zu g^i ist $(g^i)^{-1} = g^{n-1}$
  $g^i * g^{n-1} = g^{1+n-i} = g^n = e$
  $\Rightarrow < g > \leq G$
- Satz von Lagrange (6.6) sagt $n = o(g) = | < g > | \mid |G|$, also ist $|G| = n * k$ für ein $k \in \mathbb{N}$.
  $g^{|G|} = g^{n*k} = (g^n)^k = e^k = e$

Beispiel 6.9.

a) $(\mathbb{Z}_3 \setminus \{0\}, *) = \{1, 2\}$

b) In $(\mathbb{Z}_3 \setminus \{0\}, *)$
$g = 1 \quad < 1 >= \{1^0 = 1, 1^1 = 1, 1^2 = 1\} = \{1\}, o(1) = 1$
$g = 2 \quad < 2 >= \{2^0 = 1, 2^1 = 2, 2^2 = 1\} = \{1, 2\}, o(2) = 2$
ist $< 2 >= \{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 \equiv 3, 2^4 \equiv 1\} = \{1, 2, 3, 4\} = \mathbb{Z}_5 \setminus \{0\}, o(2) = 4$
d.h. $\mathbb{Z}_5 \setminus \{0\}$ ist zykl. Gr. mit erzeugendem El. 2

Korollar 6.10.

a) <u>SATZ von EULER:</u>
Sei $n \in \mathbb{N}, a \in \mathbb{Z}, ggT(a, n) = 1$
Dann ist $a^{\varphi(n)} \equiv 1(\text{mod} n)$

b) <u>kleiner SATZ von FERMAT:</u>
Ist p eine Primzahl, $a \in \mathbb{Z}, p \nmid a$, dann gilt: $a^{p-1} \equiv (\text{mod} p)$

<u>Beweis:</u>

a) Wir können annehmen, dass $1 \leq a < n$ gilt (denn $a^{\varphi(n)} \bmod n = (a \bmod n)^{\varphi(n)}$).
Wegen $ggT(a, n) = 1$ ist $a \in \mathbb{Z}_n^*$, das ist endl. Gruppe
$\overset{6.8c)}{\Rightarrow} a^{|\mathbb{Z}_n^*|} = 1$
$\Rightarrow a^{\varphi(n)} \equiv 1(\text{mod} n)$

b) folgt aus a)
$(n = p, \varphi(p) = p - 1)$

7 Kurzer Ausflug in die Kryptologie

Definition 7.1. *Kryptologie*

$\underbrace{\text{Krypto}}_{\text{gehiem}}\underbrace{\text{logie}}_{\text{Lehre}}$
- die Wissenschaft die sich mit Verschlüsselung befasst.

Definition 7.2. *Setting*

Personen A und B wollen auf geheime Weise kommunizieren
Alice, Bob (Charlie oder Carol) schicken Nachrichten
Eve ließt Nachrichten, kann sie aber nicht verändern
Mallory verändert Nachrichten

Lösung: Kryptosystem
Sender: Nachricht m (plaintext/Klartext) + Ke (encryption Key) = c (cyphertext/Chiffrentext)
Empfänger: $c + Kd$ (decription Key) $= m$

Definition 7.3. *Symmetrische Verfahren*

→ Folien

Problem:
Wie tauschen A und B den Schlüssel aus?
Lösung:

Definition 7.4. *Asymmetrische Verschlüsselung, Public Key Kryptografie*

a) Idee: Verschlüsselung ohne Schlüsselaustausch
1. m mit Schlüssel von A verschlüsseln, und an B schicken
2. B verschlüsselt m zusätzlich noch mit eigenem Schlüssel, und schickt m wieder an A zurück
3. A entfernt Schloss A, und schickt m wider an B zurück
4. B entfernt eigenen Schlüssel und kann m lesen.

oder einfacher:
1. B schickt Schloss an A
2. A verschlüsselt m mit Schloss von B, und schickt m wieder an B
3. B kann eigenes Schloss entfernen und m lesen

b) Public Key Verfahren:
Bob (will Nachricht empf.) besitzt 2 Schlüssel:
   - öffentl. Schlüssel (public key) zum verschlüsseln non Nachrichten
   - geheimer Schlüssel (private Key) zum entschlüsseln der Nachricht

c) Realisierung: Einwegfunktionen → Folien

d) Das RSA-Verfahren (Rivest, Shamir, Adleman, 1997)
Bob (Schlüsselerzeugung)
1. wählt zwei große PZ, p, q, bildet $n = p * q$
2. berechnet $\varphi(n) = (p-1) * (q-1)$
3. wählt e teilerfremd zu $\varphi(n)$
4. bestimmt $0 < d < \varphi(n)$ mit $ed \bmod \varphi(n) = 1$ (EEA: d ist Inverse zu $e \bmod \varphi(n)$)
(dann gilt: $\underbrace{ed = k * \varphi(n) + 1 \text{ für ein } k \in \mathbb{Z}}_{(*)}$)
5. publickey: (n, e), privatekey: d

Alice (Verschlüsseln)
1. Nachricht m, gegeben als Zahl, $0 \leq m < n$ (sonst in Blöcke zerlegen)
2. berechnet $c = m^e \bmod n$
3. sendet c an Bob

Bob (Entschlüsseln)
1. berechnet $c^d \bmod n = m$

Korrektheit:
$c^d = (m^e)^d = m^{ed}$
$\overset{(*)}{=} m^{k\varphi(n)+1}$
$= m^{k\varphi(n)} + m^1$
$= (m^{\varphi(n)})^k * m \equiv 1 \bmod n$ Satz von Euler 6.10 a)
$= m (\mathrm{mod} n)$

e) Bsp/Übung

f) Sicherheit von RSA

g) wie findet man große PZ? (Bitlänge 500 $\widehat{=}$ 150 stellige Zahl)

- wähle zufällige Zahl im gewünschten Größenbereich
- prüfe alle "kleinen" PZ $< 10^6$ (Liste) als Teiler
- weiter mit PZ-Test
- keine PZ: starte erneut Test positiv: mit hoher Wahrscheinlichkeit PZ gefunden

Nach wie vielen Versuchen findet man so PZ?
Primzahlsatz:
$\underbrace{\pi(x)}_{\text{Anz. PZ} \leq x} \sim \frac{x}{\ln x}$
d.h. Erwartung nach $\ln(10^{150}) = 150 * \ln(10) \approx 350$ vielen Versuchen trifft man auf PZ.
Die meisten PZ-Tests beruhen auf dem kl. Satz von Fermat: (6.10 b))
$n \in \mathbb{N}, n \geq 2 \quad n$ PZ $\Leftrightarrow a^{n-1} \equiv 1 \bmod n$ für alle $2 \leq a < n$.
D.h.: findet man einn a mit $a^{n-1} \not\equiv 1 \bmod n$, so ist n keine PZ

8 Mehrdimensionale Analysis

Bisher (Mathe I): Folgen, Fkt. auf $\mathbb{R}$ (Punkte sind reelle Zahlen)
Jetzt: auf $\mathbb{R}^n$, Punkte sind Vektoren mit n Einträgen

Definition 8.1. *Norm, Betrag*

a) Sei $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$, Norm/Betrag von x:
$\|x\| = +\sqrt{x^T x} = +\sqrt{x_1^2 + \ldots + x_n^2}$

b) Abstand von $x, y \in \mathbb{R}^n$ ist $d(x, y) := \|x - y\|$

Definition 8.2. *offene Mengen*

a) Für $x \in \mathbb{R}^n$ und $\epsilon > 0$ heißt $K(x_o, \epsilon) := \{x \in \mathbb{R}^n \mid \|x_n - x_0\| < \epsilon\}$ die offene ϵ-Kugel von x_0.
$K(\begin{pmatrix} 2 \\ 2 \end{pmatrix}, 1)$ Mittelpunkt ist $(2, 2)$. Alle Punkte mit Abstand < 1 liegen in Kugel. In $\mathbb{R}^2$ ist das ein Kreis, in $\mathbb{R}^3$ eine Kugel.

b) Eine Menge $D \subseteq \mathbb{R}^n$ heißt offen, falls es zu jedem $x \in D$ ein $\epsilon > 0$ ex. mit $K(x, \epsilon) \subseteq D$
$\{x \in \mathbb{R}^n \mid \|x\| \leq 1\}$ nicht offen
$\{x \in \mathbb{R}^n \mid \|x\| < 1\}$ offen da Rand nicht definiert

Definition 8.3. *Folgen, Konvergenz*

Seien $x_k \quad (k = 1, 2, ...)$ Punkte im $\mathbb{R}^n$ und $(x_k)_{k \in \mathbb{N}}$ Folge im $\mathbb{R}^n$
$(x_k)_{k \in \mathbb{N}}$ konvergiert gegen $a \in \mathbb{R}^n$
($x_k \overset{k \to \infty}{\longrightarrow}$ oder $\lim_{x \to \infty} x_k = a$) wenn gilt:
$\forall \epsilon > 0 \quad \exists N \in \mathbb{N}$ sodass $\|x_k - a\| < \epsilon \quad \forall k > N$.

Es gilt $(x_k)_{k \in \mathbb{N}} = \left(\begin{pmatrix} x_1^{(k)} \\ \vdots \\ x_n^{(k)} \end{pmatrix} \right) \longrightarrow a = \begin{pmatrix} a_n \\ \vdots \\ a_n \end{pmatrix} \Leftrightarrow$ Komponenten $x_i^{(k)} \longrightarrow a_i \quad \forall i = 1 \ldots n$

Die aus Mathe I beka. Begriffe (Divergenz, Nullfolge, ...) und Rechenregeln für Folgen gelten analog im $\mathbb{R}^n$

Beispiel 8.4.

$\begin{pmatrix} 2 + \frac{1}{k} \\ (1 + \frac{1}{k})^k \end{pmatrix} \overset{k \to \infty}{\longrightarrow} \begin{pmatrix} 2 \\ e \end{pmatrix}$

$\begin{pmatrix} k \\ \frac{1}{k} \\ 3 \end{pmatrix}_{k \in \mathbb{N}}$ konv. nicht

Definition 8.5. *Reelle Fkt.* $\mathbb{R}^n \to \mathbb{R}^m$

a) Eine reelle Funktion von mehreren Veränderlichen $f\colon D \subseteq \mathbb{R}^n \to \mathbb{R}^m$
$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix}$ ordnet einem Vektor $x \in D \subseteq \mathbb{R}^n$
einen Vektor $f(x) = f(x_1, ..., x_n) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix} \in \mathbb{R}^m$ zu.
(f hängt also von n Veränderten/Veränderlichen ab)

b) Je nach Dimension von Def. und Bildberich unterscheidet man:
$m = 1 \quad f\colon D \subseteq \mathbb{R}^n \to \mathbb{R}$ skalare Fkt.
Skalare Fkt. auf $\mathbb{R}^2 \quad (m = 2)$ lassen sich grafisch wie folgt darstellen:
Für $f\colon \mathbb{R}^2 \to \mathbb{R}$ zeichne entweder

- den Graphen $\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid x, y \in \mathbb{R}, z = f(x, y)\}$ als Fläche im $\mathbb{R}^3$
- sog. Höhenlinien/Niveauflächen $\{(x, y) \mid f(x, y) = c\} \subseteq \mathbb{R}^2$ für mehrere $c \in \mathbb{R}$ fest gewählt.

$m > 1 \quad f\colon D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ Vektorwertige Fkt.
$n = 1 \quad f\colon D \subseteq \mathbb{R} \to \mathbb{R}^m$ parametrisierte Kurve
($m = 2$: ebene Kurve, $m = 3$: Kurve im Raum)

Definition 8.6. *Stetigkeit*

a) Skalare Fkt.: $f\colon D \subseteq \mathbb{R}^n \to \mathbb{R}$ heißt stetig in $a_0 \in D$, wenn für alle Folgen $(a_k)_{k\in\mathbb{N}}$ in D mit $\lim_{k\to\infty} a_k = a_0$ gilt: $\lim_{k\to\infty} f(a_k) = f(a_0)$
f heißt stetig auf D, falls f stetig $\forall a_0 \in D$ ist.

b) Vektorwertige Fkt.: $f\colon D \subseteq \mathbb{R}1n \to \mathbb{R}^m, \quad x \mapsto \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix}$ heißt stetig in a_0/stetig auf D
wenn alle $f_i\colon D \to \mathbb{R} \quad (1 \leq i \leq m, f_i$ sind stetige Fkt.) in a_0/auf D stetig sind.

c) "*" wie in Mathe I gilt: Summen, Produkte, Quotienten, Kompositionen stetiger Funktionen sind stetig.

Beispiel 8.7.

a) $f\colon \mathbb{R}^n \to \mathbb{R} \quad f(x_1,...,x_n) = x_i$ ist stetig in a_0 (gilt für alle $a_0 \in \mathbb{R}^n$

Sei $(a_k)_{k\in\mathbb{N}}$ Folge im $\mathbb{R}^n$ mit $a_k := \begin{pmatrix} a_1^{(k)} \\ \vdots \\ a_n^{(k)} \end{pmatrix} \overset{k\to\infty}{\longrightarrow} a_0 = \begin{pmatrix} a_1^{(0)} \\ \vdots \\ a_n^{(0)} \end{pmatrix}$

Dann ist $\lim_{k\to\infty} f(a_k) = \lim_{k\to\infty} f(a_1^{(k)},...,a_n^{(k)}) = \lim_{k\to\infty} a_i^{(k)} = a_j^{(0)}$
und $f(a_0) = f(a_1^{(0)},...,a_n^{(0)}) = a_i^{(0)}$ wegen "*" sind dann auch alle Polynomfkt. stetig (z.B. $f(x,y) = 3x^2y^2 + 4xy^2 + 7x - 3$)

b) $f\colon \mathbb{R}^2 \to \mathbb{R}$

$f(x,y) = \begin{cases} \frac{(x+y)^2}{xy} & \text{, falls } (x,y) \neq (0,0) \\ 0 & \text{, falls } (x,y) = (0,0) \end{cases}$

ist stetig im $\mathbb{R}^2 \setminus \{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$ (wegen a und "*")

Verhalten in $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$?

Betrachte Folge $(a_k)_{k\in\mathbb{N}}$ mit $a_k = \begin{pmatrix} \frac{1}{k} \\ \frac{1}{k} \end{pmatrix} \overset{k\to\infty}{\longrightarrow} \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$f(a_k) = f(\frac{1}{k}, \frac{1}{k}) = \frac{(\frac{1}{k}+\frac{1}{k})^2}{\frac{1}{k}*\frac{1}{k}} = \frac{(\frac{2}{k})^2}{\frac{1}{k^2}} = \frac{4}{k^2} * \frac{k^2}{1} = 4$ also $\lim_{k\to\infty} f(a_k) = 4$

aber $f(a_0) = f(0,0) = 0$ also f nicht stetig in $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$

(auch die Def. $f(0,0) = 4$ hätte f nicht stetig gemacht, betrachte darum z.B. die Folge $(a_k) = \begin{pmatrix} \frac{1}{k} \\ \frac{1}{k} \end{pmatrix} \to \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ dann ist $f(a_k) = 4.5 \neq f(a_0) = 4$)

Definition 8.8. *partielle Ableitung*

Sei $D \subseteq \mathbb{R}^n$ offen, $f\colon D \to \mathbb{R}^m, a = (a_1,...,a_n)^T \in D$

a) $f(x_1,...,x_n) = \begin{pmatrix} f_1(x_1,...,x_n) \\ f_m(x_1,...,x_n) \end{pmatrix}$

heißt <u>an der Stelle a partiell nach x_j</u> ($j \in \{1,...,n\}$ <u>differenzierbar</u>, falls für jede Fkt. $f\colon \mathbb{R}^n \to \mathbb{R}$ gilt:
Die skalare Fkt. $f_i(a_1,...,a_{j-1},x_j,a_{j+1},...,a_n)$ linear Veränderlichen ("partielle Fkt.", alle x_k bis x_j durch entsprechendes a_k ersetzt.) ist an der Stelle a_j diff.bar, d.h.
$\lim_{h\to\infty} \frac{f_i(a_1,...,a_{j-1},a_j+h,a_{j+1},...,a_n)-f(a_1,...,a_n)}{h}$
ex. für alle $1 \leq i \leq m$.

b) Dieser Grenzwert heißt dann <u>partielle Ableitung</u> fon f_i nach x_j an der Stelle a, $\frac{\partial f_i}{\partial x_j}(a)$

c) Sind alle f_i nach allen x_j part. diff. in a, so heißt <u>f partiell diffbar</u> und man definiert die <u>Jacobimatrix</u> von f an der Stelle a durch $f'(a) := \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(a) & \cdots & \frac{\partial f_1}{\partial x_n}(a) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_1}(a) & \cdots & \frac{\partial f_m}{\partial x_n}(a) \end{pmatrix} \in M_{m,n}(\mathbb{R})$

d) Für skalare Fkt. ($m = 1$) besteht $f'(a)$ nur aus einer Zeile. Man bez. dann den Vektor

$f'(a)^T = \begin{pmatrix} \frac{\partial f}{\partial x_1}(a) \\ \vdots \\ \frac{\partial f}{\partial x_n}(a) \end{pmatrix} = \nabla f(a) = \mathrm{Grad} f(a) \in \mathbb{R}^n$ als <u>Gradient von f</u> im Punkt a.

Beispiel 8.9.

a) $f\colon \mathbb{R}^2 \to \mathbb{R}, \quad f(x,y) = 3xy + 4y$
$\frac{\partial f}{\partial x}(x,y) = \lim_{h\to 0} \frac{f((x+h),y)-f(x,y)}{h} = \lim_{h\to 0} \frac{3(x+h)y+4y-(3xy+4y)}{h} = \lim_{h\to 0} \frac{3hy}{h} = 3y$
kurz: sehe y als Konstante an, leite nach x ab!
$\frac{\partial f}{\partial y}(x,y) = 3x + 4$

b) $f\colon \mathbb{R}^3 \to \mathbb{R}, \quad f(x,y,z) = e^x + y^2 + xz$
$\frac{\partial f}{\partial x}(x,y,z) = e^x + 0 + z$
$\frac{\partial f}{\partial y}(x,y,z) = 0 + 2y + 0$
$\frac{\partial f}{\partial z}(x,y,z) = 0 + 0 + x$
$f'(x,y,z) = \begin{pmatrix} e^x + z & 2y & x \end{pmatrix}$
$f'(0,0,0) = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$
$\nabla f(x,y,z) = \begin{pmatrix} e^x + z \\ 2y \\ x \end{pmatrix}$

c) $f\colon \mathbb{R}^3 \to \mathbb{R}^2$
$f(x,y,z) = \begin{pmatrix} x + y \\ xyz \end{pmatrix}$
$f'(x,y,z) = \begin{pmatrix} 1 & 1 & 0 \\ yz & xz & xy \end{pmatrix}$
$f'(0,0,1) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

d) Bild:

Bemerkung 8.10.

a) Der Gradient zeigt in der Richtung des steilsten Anstiegs einer Fkt. in einem gegebenen Punkt.
Er steht senkrecht auf den Höhenlinien.

b) Ex. für f alle part. Abl. (d.h. Tangenten in Richtung x_j ex. $\forall j$), so muss f nicht stetig sein!
Mathe I: f diffbar. $\Rightarrow$ f stetig.
Mathe III: f diffbar. $\not\Rightarrow$ f stetig.
(Ü: am Bsp.: 8.7 b) ausprobieren)

Definition 8.11. *totale Differenzierbarkeit*

Sei $D \subseteq \mathbb{R}^n$ offen, $a \in D$
$f\colon D \to \mathbb{R}^m$ heißt in a (total) differenzierbar, wenn f in a partiell diffbar ist und geschrieben werden kann als
"*" $\underbrace{f(x)}_{f(x_1,\ldots,x_n)\in\mathbb{R}^m} = \underbrace{f(a)}_{\in\mathbb{R}^m} \underbrace{f\prime(a)}_{\in M_{m,n}(\mathbb{R})} \underbrace{(x-a)}_{\in\mathbb{R}^n} + \underbrace{R(x)}_{\in\mathbb{R}^m},$
wobei $R\colon D \to \mathbb{R}^m$ Abb. mit $\lim_{x\to a} \frac{\|R(x)\|}{\|x-a\|} = 0$ gilt.
f heißt (total) diffbar, wenn f in jedem Punkt von D diffbar ist.
(Für $n = 1, m = 1$ ist Def. 8.11 die Def. der Differenzierbarkeit aus Mathe I, denn
$f(x) = f(a) + f'(a)(x-a) + R(x)$
$\Leftrightarrow \frac{f(x)-f(a)}{x-a} = f'(a) + \underbrace{\frac{R(x)}{x-a}}_{\to 0 \text{ für } x\to a}$
"*" bedeutet: man kann f in der Nähe von a (da $(R(x)$ nahe a klein wird) durch
$g(x) = f(a) + f'(a)(x-a)$ ersetzen.
g heißt die lineare Approximation / Tangentialebene von f in a.

Beispiel 8.12. *Gleichung der Tangentialebene*

an $f\colon \mathbb{R}^2 \to \mathbb{R}, \quad f(x,y) = x^2 + y^2$ in $a = \begin{pmatrix}1\\2\end{pmatrix}$
$g(x) = f(a) + f'(a)(x-a)$
$g(x) = 5 + (2\ \ 4)\begin{pmatrix}x-1\\y-2\end{pmatrix}$ $\qquad f'(x,y) = (2x\ \ 2y) \Rightarrow f'(1,2) = (2\ \ 4)$
$g(x,y) = 5 + 2(x-1) + 4(y-2)$
$= 5 + 2x - 2 + 4y - 8$
$= 2x + 4y - 5$

Satz 8.13. *Diffbar / Stetigkeit*

Ist $f\colon D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ diffbar in $a \in D$, so ist f auch stetig in a.
Beweis:
$\lim_{x\to a} f(x) \overset{\text{diffbar}}{=} \lim_{x\to a}(f(a) + \underbrace{f'(a)(x-a)}_{\text{beschr } \to 0} + \underbrace{R(x)}_{\to 0}) = f(a)$, also f stetig.

Bemerkung 8.14.

Für part. Abb. gilt:
wenn alle part. Abb. von $f\colon D \subseteq \mathbb{R}^n \to \mathbb{R}^m$ ex. und stetig sind, dann ist f diffbar.
Also: part. Abl. ex. und stetig $\overset{8.14}{\Rightarrow}$ f diffbar $\overset{8.13}{\Rightarrow}$ f stetig

Bemerkung 8.15. *Ableitungsregeln*

Die aus Mathe I bekannten Ableitungsregel gelten weiterhin:
Sei $D \subseteq \mathbb{R}^n$ offen, $f, g\colon D \to \mathbb{R}^m$ in $a \in D$ differenzierbar, sei $\lambda \in \mathbb{R}$. Dann sind auch $f+g, \lambda f, f^T g$ in a diffbar und es gilt.

a) $(f+g)'(a) = f'(a) + g'(a)$

b) $(\lambda f)'(a) = \lambda f'(a)$

c) $(f^T g)'(a) = f(a)^T g'(a) + g(a)^T f'(a)$

Weiter gilt auch die Kettenregel:
Seien $D_1 \subseteq \mathbb{R}^n, D_2 \subseteq \mathbb{R}^d$ offen, $g\colon D_1 \to D_2$ diffbar in $a \in D_1, f\colon D_2 \to \mathbb{R}^m$ diffbar in $g(a) \in D_2$.
Dann ist $f \circ g\colon D_1 \to \mathbb{R}^m$ diffbar in a mit $(f \circ g)'(a) = f'(g(a)) * g'(a)$

Beispiel 8.16.

$f\colon \mathbb{R}^2 \to \mathbb{R}, \quad f(x,y) = x^2 + 3y$
$h\colon \mathbb{R} \to \mathbb{R}^2, \quad h(t) = \begin{pmatrix} \cos t \\ t \end{pmatrix}$
$f \circ h\colon \mathbb{R} \to \mathbb{R}$
$(f \circ h)(t) = f(h(t)) = f\begin{pmatrix} \cos t \\ t \end{pmatrix} = \cos^2 t + 3t$
$(f \circ h)'(t) = (\text{direkt Mathe I}) = 2 * \cos t(-\sin t) + 3$
oder Kettenregel: $(f \circ h)'(t) = f'(g(t)) * h'(t)$
$= (2\cos t \;\; 3) * \begin{pmatrix} -\sin t \\ 1 \end{pmatrix}$
$= -2\cos t \sin t + 3$

$f'(x,y) = (2x \;\; 3)$
$h'(t) = \begin{pmatrix} -\sin t \\ 1 \end{pmatrix}$

Definition 8.17. *Richtungsableitung*

Sei $f\colon D \subseteq \mathbb{R}^n \to \mathbb{R}, \quad a \in D, \quad v \in \mathbb{R}^n$ mit $|v\| = 1$
f heißt in a diffbar in Richtung v, wenn $\lim_{n\to 0} \frac{f(a+h*v)-f(a)}{h}$ ex.
Der GW heißt dann die Richtungsableitung von von f in Richtung v im Punkt a,
$\frac{\partial f}{\partial v}(a)$ ($\widehat{=}$ Anstieg von f an Stelle a in Richtung v)
Für diffbare Fkt. ex. alle Richtungsbaleitungen und es gilt $\frac{\partial f}{\partial v}(a) = f'(a) * v$
$= \|f'(a)\| * \|v\| * \cos\alpha$
$\Rightarrow \frac{\partial f}{\partial v}(a)$ wird am größten, wenn $\cos\alpha = 1$, also $\alpha = 0$ ist.
D.h., wenn v in Richtung des Gradienten zeigt $(f'(a)^T = \nabla f(a))$
$\Rightarrow$ Der Gradient zeigt also immer in die Richtung des steilsten Anstiegs der Fkt.! (vgl. 8.10)

Definition 8.18. *Stetig differenzierbare Funktionen*

Sei $D \subseteq \mathbb{R}^n$ offen, $f\colon D \to \mathbb{R}$

a) f heißt stetig differenzierbar, wenn f überall in D partiell differenzierbar ist und die partiellen Ableitungen $\frac{\partial f}{\partial x_j}(j = 1, ..., n)$ alle in D stetig sind.

b) f heißt 2-mal stetig differenzierbar, wenn f stetif diffbar und außerdem auch alle partiellen Ableitungen $\frac{\partial f}{\partial x_j}(j = 1, ..., n)$ stetig differenzierbar sind.
Die partielle Ableitung $\frac{\partial f}{\partial x_j}$ nach x_k wird mit $\frac{\partial^2 f}{\partial x_k \partial x_j}$ bezeichnet.
Statt $\frac{\partial^2 f}{\partial x_j \partial x_j}$ schreibt man auch $\frac{\partial^2}{(\partial x_j)^2}$

c) Analog s-mal stetig differenzierbar $\frac{\partial^s f}{\partial x_{js} ... \partial x_{j1}}$

Beispiel 8.19.

$f\colon \mathbb{R}^2 \to \mathbb{R}, \quad f(x, y) = 3y + xy^2$
$\frac{\partial f}{\partial x}(x, y) = y^2 \quad \frac{\partial f}{\partial y}(x, y) = 3 + 2xy$
$\frac{\partial^2 f}{\partial x \partial x}(x, y) = 0 \quad \frac{\partial^2 f}{\partial y \partial x} = 2y \quad \frac{\partial^2 f}{\partial x \partial y} = 2y \quad \frac{\partial^2 f}{\partial y \partial y} = 2x$

Satz 8.20. *Satz von Schwarz*

Sei $D \subseteq \mathbb{R}^n$ offen, $f\colon D \to \mathbb{R}$ s-mal stetig differenzierbar.
Dann ist $\frac{\partial^2 f}{\partial x_k \partial x_j} = \frac{\partial^2 f}{\partial x_j \partial x_k}$ für alle $j, k \in \{1, ..., n\}$
(D.h.: Die Reihenfolge spielt beim mehrfachen partiellen Ableiten keine Role!)
Beweis mit dem 1. Mittelwertsatz der Differentialrechnung.

Definition 8.21. *Hessematrix*

Sei $D \subseteq \mathbb{R}^n$ offen, $f\colon D \to \mathbb{R}$ 2-mal stetig differenzierbar, $a \in D$.
Dann heißt $H_f(a) := (\frac{\partial^2 f}{\partial x_j \partial x_k}(a))_{\substack{i=1,...,n \\ k=1,..,n}}$

$$= \begin{pmatrix} \frac{\partial^2}{\partial x_1 \partial x_1}(a) & \frac{\partial^2}{\partial x_1 \partial x_2}(a) & \cdots & \frac{\partial^2}{\partial x_1 \partial x_n}(a) \\ \frac{\partial^2}{\partial x_2 \partial x_1}(a) & \frac{\partial^2}{\partial x_2 \partial x_2}(a) & \cdots & \frac{\partial^2}{\partial x_2 \partial x_n}(a) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2}{\partial x_n \partial x_1}(a) & \frac{\partial^2}{\partial x_n \partial x_2}(a) & \cdots & \frac{\partial^2}{\partial x_n \partial x_n}(a) \end{pmatrix}$$

die Hessematrix von f an der stelle a.
Nach dem Satz von Schwarz (8.20) ist $H_f(a)$ symmetrisch!

Beispiel 8.22.

$f\colon \mathbb{R}^2 \to \mathbb{R}, \quad f(x, y) = e^x + xy, \quad a = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
$\frac{\partial f}{\partial x} = e^x + y \quad \frac{\partial f}{\partial y} = x$
$\frac{\partial^2 f}{\partial y \partial x} = e^x \quad \frac{\partial^2 f}{\partial y \partial y} = 1 = \frac{\partial^2 f}{\partial x \partial y} \quad \frac{\partial f}{\partial y \partial y} = 0$
$H_f(x, y) = \begin{pmatrix} e^x & 1 \\ 1 & 0 \end{pmatrix}, \quad H_f(a) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

Definition 8.23. *lokale Extrema*

Sei $D \subseteq \mathbb{R}^1, \quad f\colon D \to \mathbb{R}, \quad a \in D$ a heißt <u>Stelle eines lokalen Minimums (Maximums)</u>, wenn ein $\epsilon > 0$ ex. mit $f(n) \leq f(x) \quad \forall x \in K(a, \epsilon) \cap D$
$(f(a) \geq f(x))$

Satz 8.24. *Notwendige Bedingung für lokale Extremstellen*

Sei f wie oben, D offen. Wenn $a \in D$ Stelle eines lokalen Extremums ist und in a die part. Abl. ex., dann ist
$\nabla f(a) = (\vec{0} = \text{Nullindex} \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
$(f(a =^T = (0...0) = 0^T)$
<u>Beweis:</u>
Sei a lok. Extremstelle von f.
Betrachte $K(a, \epsilon) \leq D$
Die Fkt. $\varphi\colon (-\epsilon, \epsilon) \to \mathbb{R}$
$\varphi(t) = f(a + t * e_K) \quad K = \{1, ..., n\}$
besitzt bei $t = 0$ ein lokales Extremum.
$(\varphi(0) = f(a)$, kleiner oder größer als die Pkt. Werte drumrum)
$\overset{\text{Mathe I}}{\Rightarrow} \quad \underbrace{\varphi(0) = 0}_{\lim_{n \to \infty} \frac{f(a + h * e_K) + f(a)}{h} = \frac{\partial f}{\partial x_K}(a)}$

Satz 8.25. *Hinreichende Bedingung für lokale Extremstellen*

Sei f wie oben, 2-mal stetig diffbar. $a \in D$
und $\nabla f(a) = \vec{0}$ (mam sagt a ist kritischer Punkt von f)
Dann gilt:

a) $H_f(a)$ pos. definit $\Rightarrow a$ ist Stelle eines lokalen Minimums
(alle EW von $H_f(a) \geq 0$)

b) $H_f(a)$ neg. definit $\Rightarrow a$ ist Stelle eines lokalen Maximums
(alle EW von $H_f(a) < 0$)

c) $H_f(a)$ indefinit $\Rightarrow a$ ist Sattelpunkt
(Sowohl pos. als auch neg. EW) (keine Extremstelle)

(Hat $H_f(a)$ nur EW≥ 0 oder nur ≤ 0 und kommt 0 als EW vor, so ist (noch) keine Aussage möglich)
<u>Beweis:</u>
$H_f(a)$ ist pos. definit $\Rightarrow H_f(x)$ pos. definit für alle $x \in K(a, \xi)$
Für diese x gilt (mehrdim. Satz von Taylor ($\to$ Folien))
$\exists \xi \in (0, 1)$ mit $f(x) = f(a) + \underbrace{f'(a) * (x - a) + \frac{1}{2}(x - a)^T * H_f(a + \xi(x - a)) * (x - a)}_{0, \text{ da } H_f(x) \text{ pos. definit} \quad y^T H_f(a) > 0}$
$\geq f(a)$, also ist a Stelle eins der Min.
(Max. analog)

Beispiel 8.26.

$f\colon \mathbb{R}^2 \to \mathbb{R}$

a) $f(x,y) = x^2 + y^2$
   $f'(x,y) = (2x \quad 2y)... = (0 \quad 0) \Rightarrow x = 0, y = 0$ der kritische Punkt $(0,0)^T$
   $H_f(x,y) = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, H_f(0,0) = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
   EW: $2 > 0 \overset{8.25}{\Rightarrow}$ lok. Minimum bei $(0,0)^T$

Beispiel 8.27.

a) ... 7.26

b) $f\colon \mathbb{R}^2 \to \mathbb{R}, \quad f(x,y) = x^2 + y^2$
   $f'(x,y) = (2x \quad -2y) = (0 \quad 0)$
   $\Rightarrow x = y = 0$, krit Punkt $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
   $H_f(x,y) = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}, \quad H_f(0,0) = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$
   EW: $2, -2 \Rightarrow$ Sattelpunkt in $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$

c) $f(x,y) = x^2 + y^4 + 2x$ ergibt krit. Punkt $\begin{pmatrix} -1 \\ 0 \end{pmatrix}$
   $H_f(-1,0) = \begin{pmatrix} 2 & 0 \\ 0 & -0 \end{pmatrix}$, EW: $2, 0$
   $\Rightarrow$ keine Aussage möglich

d) $f(x, y = 3xy - x^3 - y^3$ ergibt krit. Punkte: $\underbrace{\begin{pmatrix} 0 \\ 0 \end{pmatrix}}_{\text{Sattelp.}}$ und $\underbrace{\begin{pmatrix} 1 \\ 1 \end{pmatrix}}_{\text{lok. Max. stelle}}$
   $f(1,1) = 3 - 1 - 1 = 1$

Beispiel 8.28. *Extrema unter Nebenbedingungen (NB)*

Lösen von Extremwertaufgaben wenn es zusätzliche Bedingungen gibt.

a) Geg. $U \in \mathbb{R}$, welches Rechteck (Seiten x, y) mit Umfang U hat max. Fläche?
   d.h. Max. stekke der Fkt. $f(x,y) = x * y$ (Fläche)
   unter der NB dass $2x + 2y = U$ (constraints)
   d.h. finde Max. stelle von $f\colon \mathbb{R}^2 \to \mathbb{R}$ auf der Menge
   $A := \{(x,y) \in \mathbb{R}^2 \mid 2x + 2y = U, \quad x, y \geq 0\}$ ($\widehat{=}$ Gerade in $\mathbb{R}$)

b) Post: Paket, $L + B + H \leq 200$ cm will Volumen maximieren

c) Milchmädchenproblem

Definition 8.29. *lok. Extr. bzgl. A*

Seien $D, A \subseteq \mathbb{R}^n, \quad D \to \mathbb{R}, \quad a \in D \cap A$
Dann heißt a Stelle eines lokalen Maximums (Min.) von f bzgl. A wenn es ein $\epsilon > 0$ gibt mit $f(a) \geq f(x) \quad \forall x \in K(a,\epsilon) \cup A$

Beispiel 8.30.

Welcher Punkt auf der Hyperbel $xy = 3$ ist dem Nullpunkt am nächsten?
D.h. Minimieren $f(x,y) = \sqrt{x^2+y^2}$ (Abstanf von $\begin{pmatrix}0\\0\end{pmatrix}$ unter der NB $x * y = 3$
$\rightarrow$ Applet, Knet,...

Satz 8.31. *Lagrangesche Multiplikationsregel*

Sei $D \subseteq \mathbb{R}^n$ offen, $f\colon D \to \mathbb{R}$, $g\colon D \to \mathbb{R}^d$ $(d < n)$ stetig diffbar
Sei $A := \{x \in D \mid g(x))\vec{0}\}$ Nebenbedingung
Sei weiter $a \in D$ mit $Rang(g'(a)) = d$ (Jacobimatrix von g in a hat Rang d, d.h. alle Zeilen sind l.u.)
Ist a Stelle eines lok. Extremums von f bzgl. A (unter der NB von A), dann ex. $\lambda_1, ..., \lambda_d \in \mathbb{R}$, so dass für die Fkt.
$F\colon D \to \mathbb{R}$, $F(x) = f(x) + \lambda_a, ..., \lambda_d) * g(x)$ gilt:
$F'(a) = \vec{0}^T$ $(\nabla F(a) = 0)$
$\lambda_1, ..., \lambda_d$ heißen Lagrange Multiplikatoren.
Ist die NB skalar, d.h. $g\colon D \to \mathbb{R}$ $(d = 1)$, so lautet der Satz:
Ist a lok. Extr. st. von f unter der NB $g(x) = 0$ dann gilt:
$(F(x) = f(x) + \lambda * g(x), \qquad \underbrace{F'(a)}_{f'(x)+\lambda * g'(x)=\vec{0}^T} = \vec{0}^T$
$\nabla f(a) + \lambda * \nabla g(a) = \vec{0}$
für ein $\lambda \in \mathbb{R}$, d.h. $\nabla f, \nabla g$ sind parallel

Beispiel 8.32.

a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x,y) = 3x + 2y$
   $A = \{\begin{pmatrix}x\\y\end{pmatrix} \mid x^2 + y^2 = 1\}$
   d.h. $f\colon \mathbb{R}^2 \to \mathbb{R}$, $g(x,y) = 1 + x^2 - y^2$ $(= 0)$
   $F(x,y) = 3x + 2y + \lambda(1 - x^2 - y^2)$
   $\frac{\partial F}{\partial x} F(x,y) = 3 - 2\lambda x \overset{!}{=} 0$ I
   $\frac{\partial F}{\partial y} F(x,y) = 2 - 2\lambda y \overset{!}{=} 0$ II
   NB: III: $1 - x^2 - y^2 = 0$
   löse 3 Gl. erhalte $\lambda^2 = \frac{13}{4}$, $y = \pm\frac{2}{\sqrt{13}}$, $\lambda = \pm\frac{3}{\sqrt{13}}$
   mögl. Extr. stl sind also $a_1 = (\frac{3}{\sqrt{13}}, \frac{2}{\sqrt{13}})^T$, $a_2 = (-\frac{3}{\sqrt{13}}, -\frac{2}{\sqrt{13}})^T$
   $f(a_1) = \sqrt{13}$, $f(a_2) = -\sqrt{13}$ $\leftarrow$ Extremwerte

b) $\rightarrow$ Skript