Mathematik III - Wintersemester 14/15

18. Februar 2015

Inhaltsverzeichnis

1 Algebraische Strukturen mit einer Verknüpfung HALBGRUPPEN, MONOIDE, GRUPPEN

1.1 Definition

Sei $X \neq \emptyset$ eine Menge.

Eine *Verknüpfung* oder (abstrakte) Multiplikation auf X ist eine Abbildung

$$\begin{aligned} \bullet : \quad & X \times X \to X \\ & (a,b) \mapsto a \bullet b \end{aligned}$$

$\underset{(ab)}{a \bullet b}$ heißt *Produkt* von a und b, muss aber mit der üblichen Multiplikation von Zahlen nichts zu tun haben.

Beschreibung bei endlichen Mengen oft durch Multiplikationstafeln.

1.2 Beispiel

a) $X = \{a,b\}$

$\bullet$	a	b
a	b	b
b	a	a

$(a \bullet a) \bullet a = b \bullet a = a$
$a \bullet (a \bullet a) = a \bullet b = b$ $\quad \to$ nicht assoziativ

b) $X = \mathbb{Z}^-$ $(= \{0,-1,-2,\dots\})$
Die normale Multiplikation ist auf $\mathbb{Z}^-$ keine Verknüpfung!
(zum Beispiel ist $(-2) \cdot (-3) = 6 \notin \mathbb{Z}^-$)
Aber auf $X = \mathbb{N}, X = \mathbb{Z}$ oder $X = \{1\}, X = \{0,1\}$

1.3 Definition

Sei $H \neq \emptyset$ eine Menge mit Verknüpfung.

$(H, \bullet)$ heißt *Halbgruppe*, falls gilt:

$$\forall a,b,c \in H : (a \bullet b) \bullet c = a \bullet (b \bullet c) \qquad \text{(Assoziativgesetz (AG))}$$

1.4 Bemerkung

AG sagt aus: bei endlichen Produkten ist die Klammerung irrelevant, z.B.

$(a \cdot b) \cdot (c \cdot d) = ((a \cdot b) \cdot c) \cdot d = (a \cdot (b \cdot c)) \cdot d$ (usw.)

Deshalb werden Klammern meistens weggelassen.

Die Reihenfolge der Elemente ist i.A. relevant!

1.5 Beispiel

a) $(\mathbb{N}, \bullet), (\mathbb{Z}, \bullet), (\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ [1] sind Halbgruppen.
   Ebenso $(\mathbb{N},+), (\mathbb{Z},+), (\mathbb{Q},+), (\mathbb{R},+)$ [2]

b) $(\mathbb{Q}\backslash\{0\},:)$ [3] ist *keine* Halbgruppe, denn z.B. $\begin{array}{rcl}(12:6):2 & = & 1\\ 12:(6:2) & = & 4\end{array}$

c) vgl. Vorlesung Theoretische Informatik
   $A \neq \emptyset$ endliche Menge ("Alphabet")
   $A^+ = \cup_{n\in N} A^n$ = Menge aller endlichen Wörter über A
   (z.B. $A = \{a,b\}$, dann ist z.B. $\underbrace{(a,a,b)}_{aab} \in A^3$)
   Verknüpfung: Konkatenation (Hintereinanderschreiben)
   z.B. $aab \bullet abab = aababab$
   $A^* = A^+ \cup \{\lambda\}$ $\quad\lambda$ (oder ϵ) ist das leere Wort
   Es gilt: $\lambda \cdot w = w \cdot \lambda = w \; \forall w \in A^*$
   $(A^+, \bullet), (A^*, \bullet)$ *Worthalbgruppe* über A

d) $M \neq \emptyset$ Menge, Abb(M,M): Menge aller Abbildungen $M \to M$ mit $\circ$ (Komposition) ist Halbgruppe.

e) (WICHTIG)
   $n \in \mathbb{N}$, $\mathbb{Z}_n = \{0,1,\ldots,n-1\}$
   Verknüpfung: $\begin{array}{l}\oplus : a \oplus b := (a+b) \bmod n\\ \odot : a \odot b := \;(a \cdot b) \bmod n\end{array}$
   $(\mathbb{Z}_n,\oplus), (\mathbb{Z}_n,\odot)$ sind Halbgruppen.

1.6 Definition

Eine Halbgruppe $(H, \bullet)$ heißt *kommutativ*, falls gilt:

$$\forall a,b \in H \; : \; a \cdot b = b \cdot a \qquad \text{(Kommutativgesetz, KG)}$$

1.7 Beispiel

Beispiele 1.5 a), e) sind kommutative Halbgruppen.
(hallo ≠ ollah, ab ≠ ba, Worthalbgruppe nicht kommutativ)

[1] $\bullet$ normale Multiplikation
[2] + normale Addition
[3] : normale Division

1.8 Definition

Sei $(H, \bullet)$ Halbgruppe, $\varnothing \neq U \subseteq H$

U heißt *Unterhalbgruppe* von H, falls $u \cdot v \in U \ \forall u, v \in U$ gilt.

$(U, \odot)$ ist dann selbst Halbgruppe.

1.9 Beispiel

$(\mathbb{Z}, +)$ Halbgruppe

G = Menge aller gerade ganzen Zahlen $\subseteq \mathbb{Z}$
$(G, +)$ ist Unterhalbgruppe von $(\mathbb{Z}, +)$

U = Menge aller ungerade Zahlen $\subseteq \mathbb{Z}$
$(U, +)$ ist <u>keine</u> Unterhalbgruppe!

1.10 Lemma

Eindeutigkeit des neutralen Elements:

Sei $(H, \bullet)$ Halbgruppe, $e_1, e_2 \in H$ mit $^{(*)}e_1 \cdot x = x \cdot e_1 = x$ und $^{(**)}e_2 \cdot x = x \cdot e_2 = x \ \forall x \in H$

Dann ist $e_1 = e_2$

Beweis. $e_1 \overset{(**)}{=} e_1 \cdot e_2 \overset{(*)}{=} e_2$ □

1.11 Definition

Eine Halbgruppe $(H, \bullet)$ heißt *Monoid*, falls $e \in H$ existiert mit $e \cdot x = x \cdot e = x \ \forall x \in H$

e heißt *neutrales Element* / Einselement / Eins in H.
Schreibweise: $(H, \bullet, e)$

Für additive Verknüpfung oft 0 für e (Nullelement)
multiplikative 1

Nach 1.10 ist das neutrale Element eindeutig!

1.12 Beispiele

a) $(\mathbb{N}, \bullet)$ Monoid mit $e = 1$
$(\mathbb{N}, +)$ kein Monoid
$(\mathbb{N}_0, +)$ Monoid mit $e = 0$
$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ Monoide mit $e = 0$
$(\mathbb{Z}, \bullet), (\mathbb{N}_0, \bullet), (\mathbb{Q}, \bullet), (\mathbb{R}, \bullet)$ Monoide mit $e = 1$

b) $(\mathrm{Abb}(M, M), \circ)$ Monoid, $e = \mathrm{id}$

c) $(\mathbb{Z}_n, \oplus)$ Monoid, $e = 0$
$(\mathbb{Z}_n, \odot)$ Monoid, $e = 1$

d) $(A^*, \bullet)$ Monoid, $e = \lambda$ (halloλ = λhallo = hallo)

1.13 Definition

Sei $(M, \bullet, e)$ Monoid. Eine Teilmenge $\emptyset \neq U \subseteq M$ heißt *Untermonoid* von M, falls U mit $\bullet$ selbst ein Monoid mit neutralem Element e ist (also $e \in U$)

1.14 Lemma

Eindeutigkeit des inversen Elements:

Sei $(H, \bullet, e)$ Monoid und es gebe zu jedem Element $h \in H$ Elemente $x, y \in H$ mit $h \cdot x \overset{(*)}{=} e \overset{(**)}{=} y \cdot h$.

Dann ist $x = y$

Beweis. $y = y \cdot e \overset{(*)}{=} y \cdot (h \cdot x) \overset{(AG)}{=} (y \cdot h) \cdot x \overset{(**)}{=} e \cdot x = x$ □

1.15 Definition

(i) $(H, \bullet, e)$ Monoid, $h \in H$

Falls ein $x \in H$ existiert mit $hx = xh = e$, so nennt man h *invertierbar* und x das *Inverse* zu h, bez. h^{-1} (bei additiven Verknüpfungen oft auch $-h$)

Nach 1.14 ist h^{-1} eindeutig bestimmt!

Es gilt: e ist immer invertierbar, $e^{-1} = e$

(ii) Ein Monoid $(G, \bullet, e)$ heißt *Gruppe*, falls jedes Element in G invertierbar ist.

(iii) Für eine endliche Gruppe G heißt die Anzahl der Elemente in G die *Ordnung* von G, $|G|$

1.16 Bemerkung

$(H, \bullet, e)$ Monoid.

Sei G die Menge aller invertierbaren Elemente von H, dann ist $(G, \bullet, e)$ eine Gruppe.

Es gilt: e invertierbar $(e^{-1} = e)$

und falls g invertierbar, dann ist auch g^{-1} invertierbar: $(g^{-1})^{-1} = g$

falls g, h invertierbar, dann auch $g \cdot h$: $\quad (g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

1.17 Beispiele

a) $(\mathbb{N}_0, +, 0)$ ist keine Gruppe aber $(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0), (\mathbb{R}, +, 0)$ sind Gruppen.

b) $(\mathbb{Z}, \bullet, 1)$ ist keine Gruppe.
Die Menge der invertierbaren Elemente ist $\{1, -1\}$, diese bilden eine Gruppe.

c) $(\mathbb{Q}, \bullet, 1)$ ist keine Gruppe, aber $(\mathbb{Q}\backslash\{0\}, \bullet, 1), (\mathbb{R}\backslash\{0\}, \bullet, 1)$ sind Gruppen.

d) A^* ist keine Gruppe, nur λ ist invertierbar.

1.18 Beispiele

a) $(\mathbb{Z}_n, \oplus, 0)$ ist Gruppe (was ist das Inverse zu $x \in \mathbb{Z}_n$? Siehe PÜ1, A9)

b) Sei $n \geq 2$. $(Z_n, \odot, 1)$ ist Monoid aber keine Gruppe.

Wann ist ein Element aus Z_n invertierbar bezüglich $\odot$?

$$\begin{aligned} z \in \mathbb{Z}_n \text{ invertierbar} \quad &\Leftrightarrow \quad \exists x \in \mathbb{Z}_n : z \odot x = 1 \\ &\Leftrightarrow \quad \exists x \in \mathbb{Z} : (z \cdot x) \bmod n = 1 \\ &\Leftrightarrow \quad \exists x, q \in \mathbb{Z} : z \cdot x = q \cdot n + 1 \\ &\Leftrightarrow \quad \exists x, q \in \mathbb{Z} : z \cdot x + (-q \cdot n) = 1 \\ &\overset{\text{Mathe I}}{\Leftrightarrow} \quad \mathrm{ggT}(z, n) = 1 \end{aligned}$$

also sind nur zu n teilerfremde Elemente invertierbar!

(vgl. $(Z_6, 0, 1)$: $0, 2, 3, 4$ nicht invertierbar, $1, 5$ invertierbar)

Bezeichnung:

$$Z_n^* = \{z \in \mathbb{Z}_n \mid \mathrm{ggT}(z, n) = 1\}$$

ist Gruppe bezüglich $\odot$ (vgl. Bemerkung **??**) mit Ordnung $|Z_n^*| = \varphi(n)$ ("phi von n", Eulersche φ-Funktion) = Anzahl aller $z \in \mathbb{N}$, die teilerfremd zu n sind und $1 \leq z \leq n$.

$\varphi(3) = 2, \varphi(4) = 2, \varphi(7) = 6$

Wie berechnet man das Inverse von $z \in \mathbb{Z}_n^*$?

Mathe I, Erweiterter Euklidischer Algorithmus (WHK, S. 80/81) liefert zu z und n ($\mathrm{ggT}(z, n) = 1$) Zahlen $s, t \in \mathbb{Z}$ mit

$$\begin{aligned} & z \cdot s + n \cdot t = 1 \\ \Rightarrow \quad & (z \cdot s) \bmod n = 1 \\ \Rightarrow \quad & (z^{-1}) = s \bmod n \end{aligned}$$

Beispiel:

$n = 8$: $(\mathbb{Z}_8, \odot)$, $z = 5$ ist invertierbar, $\mathrm{ggT}(8, 5) = 1$

EEA: $5 \cdot (-3) + 8 \cdot 2 = 1 \Rightarrow z^{-1} = -3 \bmod 8 \Rightarrow z^{-1} = 5$

c) $\mathrm{Abb}(M, M)$: invertierbare Elemente sind genau die *bijektiven* Abbildungen auf $M, \mathrm{Bij}(M)$ (Mathe I)

Speziell: $M = \{1, 2, \ldots, n\}$, dann heißt $\mathrm{Bij}(M)$ die symmetrische Gruppe von Grad n, S_n

$|S_n| = n!$, Elemente heißen Permutationen.

Bsp: $n = 2$

$$S_2 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}}_{\mathrm{id}}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$n = 3$

$$S_3 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{\mathrm{id}}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$$

$$\pi \circ \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ \varrho \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ (nicht kommutativ!)}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \pi,\ \varrho^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

1.19 Satz (Gleichungen lösen in Gruppen)

Sei G Gruppe, $a, b \in G$

(i) Es gibt genau ein $x \in G$ mit $ax = b$ (nämlich $x = a^{-1}b$)

(ii) Es gibt genau ein $y \in G$ mit $ya = b$ (nämlich $y = ba^{-1}$)

(iii) Ist $\underset{ya=yb}{ax = bx}$ für ein $\underset{y\in G}{x \in G}$, dann gilt $a = b$ (Kürzungsregel)

Beweis. (i) • $x = a^{-1}$ ist Lösung (prüfe $ax = b$):

$a \cdot \underbrace{a^{-1}b}_{x} \overset{\text{AG}}{=} (a \cdot a^{-1}) \cdot b = e \cdot b = b$

• Es gibt genau eine Lösung:
Es gelte $ax = b$
$\Rightarrow x = ex = (a^{-1}a)x \overset{\text{AG}}{=} a^{-1}(ax) = a^{-1}b$

(ii) analog

(iii) Multipliziere von $\underset{\text{links}}{\text{rechts}}$ mit $\underset{y^{-1}}{x^{-1}}$

□

1.20 Beispiel

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ - Was ist x?

$a \cdot x = b \Leftrightarrow x = a^{-1} \cdot b$

$$x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

1.21 Definition

$(G, \cdot)$ Gruppe, $\emptyset \neq U \subseteq G$ Teilmenge.

U heißt *Untergruppe* von G ($U \leqslant G$), falls U bzgl. $\cdot$ selbst eine Gruppe ist.

Insbesondere gilt dann: $\forall u, v \in U$ ist $u \cdot v \in U$.
e von G ist auch neutrales Element in U. (*)
Inversen in U sind die gleichen wie in G.

(*) Angenommen e ist neutrales Element in G, aber f neutrales Element in U, f^{-1} Inverses von f in G.
Dann ist $f^{-1} \cdot f = f \cdot f^{-1} = e$ und $f \cdot f = f$.
$\Rightarrow f = e \cdot f = (f^{-1} \cdot f) \cdot f = f^{-1} \cdot (f \cdot f) = f^{-1} \cdot f = e$

1.22 Beispiele

a) $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +)$

b) $(\{-1, 1\}, \cdot) \leqslant (\mathbb{Q}\backslash\{0\}, \cdot) \leqslant (\mathbb{R}\backslash\{0\}, \cdot)$

c) $(e, \cdot)$ ist Untergruppe jeder beliebigen Gruppe mit Verknüpfung $\cdot$ und neutralem Element e.

d) $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3$, $\pi^{-1} = \pi, \pi^{-1} \circ \pi = \mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
$\Rightarrow (\pi, \mathrm{id}) \leqslant S_3$

1.23 Satz und Definition

G Gruppe, $U \leqslant G$

(i) Durch $x \sim y \Leftrightarrow x \cdot y^{-1} \in U$
$x + (-y) \in U$ (bei additiver Verknüpfung)
wird auf G eine Äquivalenzrelation definiert

Beweis

$\sim$ ist reflexiv: $x \sim x$ gilt $\forall x \in G$, denn $x \cdot x^{-1} = e \in U$ ✓

$\sim$ ist symmetrisch: $x \sim y \Rightarrow y \sim x$
Sei $x \sim y$, also $x \cdot y^{-1} \in U$ (zzg.: $y \sim x$, also $y \cdot x^{-1} \in U$)
dann ist $y \cdot x^{-1} = (x \cdot y^{-1})^{-1} \in U$, da auch $x \cdot y^{-1} \in U$.

$\sim$ ist transitiv: $x \sim y, y \sim z \Rightarrow x \sim z$
Sei $x \sim y$, also $x \cdot y^{-1} \in U$ und $y \sim z$, also $y \cdot z^{-1} \in U$ (zzg.: $x \sim z$, d.h. $x \cdot z^{-1} \in U$)
$x \cdot z^{-1} = xez^{-1} = x(y^{-1}y)z^{-1} = (\underbrace{x \cdot y^{-1}}_{\in U}) \cdot (\underbrace{y \cdot z^{-1}}_{\in U}) \in U$, also $x \sim z$. □

(ii) Für $x \in G$ ist $Ux = \{u \cdot x \mid u \in U\}$ die Äquivalenzklasse von x bzgl. $\sim$ und heißt *Rechtsnebenklasse* von U in G.

Also (Eigenschaften von Äquivalenzklassen siehe Mathe I):

(a) $Ux = Uy \Leftrightarrow x \sim y$, also $x \cdot y^{-1} \in U$

(b) $x, y \in G$, dann ist entweder $Ux = Uy$ oder $Ux \cap Uy = \emptyset$

Beweis

(a) Sei $x \sim y \Rightarrow y \sim x \Rightarrow y \cdot x^{-1} \in U \Rightarrow y = y(x^{-1} \cdot x) = \underbrace{(y \cdot x^{-1})}_{\in U} x \in Ux$

(b) Sei $y \in Ux$, dann zeige: $x \sim y$
$y \in Ux \Rightarrow y = u \cdot x$ für ein $u \in U$
$\Rightarrow x \cdot y^{-1} = x \cdot (ux)^{-1} = x \cdot x^{-1} \cdot u^{-1} = u^{-1} \in U$
Es wurde gezeigt, dass $x \sim y$ gilt.

$\square$

1.24 Beispiel

$G = (\mathbb{Z}, +), 3\mathbb{Z} = \{\dots, -3, 0, 3, 6, \dots\}$
$U = (3\mathbb{Z}, +) \leqslant G$ (ÜA, Blatt 2)
Inverses zu y in $(\mathbb{Z}, +)$ ist $-y$.
$x \sim y \Leftrightarrow \underbrace{x \cdot y^{-1} \in U}_{\text{bzw.: } x - y \in U}$

$x = 0 : U + 0 = \{u + 0 \mid u \in U\} = \{\dots, -3, 0, 3, 6, \dots\} = U = 3\mathbb{Z}$

$x = 1 : U + 1 = \{u + 1 \mid u \in U\} = \{\dots, -2, 1, 4, 7, 10, \dots\} = 3\mathbb{Z} + 1$

$x = 2 : U + 2 = \{u + 2 \mid u \in U\} = \{\dots, -1, 2, 5, 8, 11, \dots\} = 3\mathbb{Z} + 2$

$x = 3 : U + 3 = U + 0 = 0$

$\dots$

1.25 Lemma

G Gruppe, U endliche Untergruppe von G, $x \in G$

Dann ist $|U| = |Ux|$

Beweis

$$\text{Abb } \varphi : \begin{array}{ccc} U & \to & Ux \\ u & \mapsto & ux \end{array}$$

ist surjektiv und injektiv (falls $u_1 x = u_2 x$, dann ist $u_1 = u_2$ (Satz 1.19 (iii), Kürzungsregel))

Also ist φ bijektiv, also U, Ux gleich mächtig.

1.26 Theorem (Satz von Lagrange)

G endliche Gruppe, $U \leqslant G$

Dann gilt $|U|$ ist Teiler von $|G|$ und $q = \frac{|G|}{|U|}$ ist die Anzahl der Rechtsnebenklassen von U in G

Beweis

Seien $Ux_1, \dots, Ux_q$ die q verschiedenen Rechtsnebenklassen von U in G

$$\text{Mathe I \& 1.23} \Rightarrow G = \bigcup_{i=1}^{q} Ux_i \text{ (disjunkte Vereinigung der Äquivalenzklassen)}$$

$$\Rightarrow |G| = \sum_{i=1}^{q} \underbrace{|Ux_i|}_{|U|} \overset{1.25}{=} q \cdot |U|$$

1.27 Definition

$(G, \bullet, e)$ Gruppe, $a \in G$

Definiere
$$\begin{array}{lll} a^0 & := & e \\ a^1 & := & a \\ a^m & := & a^{m-1} \cdot a \quad \text{für } m \in \mathbb{N} \\ a^m & := & (a^{-m})^{-1} \quad \text{für } m \in \mathbb{Z}^- \end{array}$$

(Potenzen von a)

Bei additiver Schreibweise:
$$\begin{array}{lll} 0 \cdot a & = & e \\ 1 \cdot a & = & a \\ m \cdot a & = & \begin{cases} (m-1) \cdot a + a & \text{für } m \in \mathbb{N} \\ (-m) \cdot (-a) & \text{für } m \in \mathbb{Z}^- \end{cases} \end{array}$$

1.28 Satz

G, a wie oben

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

(ii) $a^m \cdot a^n = a^{m+n} \quad \forall m, n \in \mathbb{Z}$

(iii) $(a^m)^n = a^{m \cdot n} \quad \forall m, n \in \mathbb{Z}$

Beweis

(i) $m \in \mathbb{N} : (a^{-1})^m \cdot a^m = \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_{m \text{ mal}} \cdot \underbrace{a \cdot \dots \cdot a \cdot a}_{m \text{ mal}} = e$

$\Rightarrow (a^{-1})^m = (a^m)^{-1}$ (Inverses von a^m)

nach Definition ist $a^{-m} = (a^{-1})^m$

$\Rightarrow$ (i) gilt $\forall m \in \mathbb{N}$

$m = 0: \ e = e = e$ ✓

$m \in \mathbb{Z}^-$: dann ist $-m \in \mathbb{N}$

Wende den bewiesenen Teil an auf a^{-1} statt a und $-m$ statt m, Behauptung folgt.

(ii), (iii) per Induktion und mit (i) □

1.29 Satz und Definition

G endliche Gruppe, $g \in G$

(i) Es existiert eine kleinste natürliche Zahl n mit $g^n = e$, diese heißt die *Ordnung* $\mathrm{o}(g)$ von G

(ii) Die Menge $\left\{g^0 = e, g^1 = g, g^2, \dots, g^{n-1}\right\}$ ist eine Untergruppe von G, die von g erzeugte zyklische Gruppe $< g >$

Es gilt $\mathrm{o}(g) = |< g >| = n$ teilt $|G|$

(iii) $g^{|G|} = e$

Bemerkung: Eine endliche Gruppe heißt *zyklisch*, falls sie von einem Element erzeugt werden kann.

Beweis

(i) G endlich $\Rightarrow \exists i, j \in \mathbb{N}, i > j$ mit $g^i = g^j$ (Schubfachschluss -*Editor*)

Dann ist $g^{i-j} \overset{1.28ii)}{=} g^i \cdot g^{-j} \overset{1.28}{=} \underbrace{g^i}_{=g^j} \cdot (g^j)^{-1} = e$

(ii) Das Produkt zweier Elemente aus $< g >$ liegt wieder in $< g >$

Neutrales Element ist $g^0 = e$

Inverses Element zu g^i ist $(g^i)^{-1} = g^{n-i}$

$\Rightarrow < g > \leqslant G$

(iii) Satz von Lagrange (1.26): $n = \mathrm{o}(g) = |< g >| \;\Big|\; |G|$

Also ist $|G| = n \cdot k$ für ein $k \in \mathbb{N}$

$g^{|G|} = g^{n \cdot k} = (g^n)^k = e^k = e$

$\square$

1.30 Beispiel

$(\mathbb{Z}_3 \backslash \{0\}, \odot, 1)$

$g = 1$: $< 1 >= \left\{g^0 = 1^0 = 1\right\}$, $\mathrm{o}(1) = 1$

$g = 2$: $< 2 >= \left\{g^0 = 1, g^1 = 2\right\}$, $\mathrm{o}(2) = 2$

$(\mathbb{Z}_5 \backslash \{0\}, \odot, 1)$

$g = 2$: $< 2 >= \left\{2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 3\right\}$, $\mathrm{o}(2) = 4$

1.31 Korollar

(i) Satz von Euler

Sei $n \in \mathbb{N}, a \in \mathbb{Z}, \text{ggT}(a,n) = 1$
Dann ist

$$a^{\varphi(n)} \equiv 1(\mod n)$$

(ii) Kleiner Satz von Fermat

Ist p eine Primzahl, $a \in \mathbb{Z}, p \nmid a$, dann gilt

$$a^{p-1} \equiv 1(\mod p)$$

1.32 Beweis

a) Wir können annehmen, dass $1 \leq a < n$ (denn $a^{\varphi(n)} \bmod n = (a \bmod n)^{\varphi(n)}$)
wegen $\text{ggT}(a,n) = 1$ ist $a \in \mathbb{Z}_n^*$, das ist eine endliche Gruppe.
$\overset{1.29(iii)}{\Rightarrow} a^{|\mathbb{Z}_n^*|} = 1(= e) \qquad a \odot a \odot \ldots$
$\Rightarrow a^{\varphi(n)} \equiv 1(\mod n) \qquad a \cdot a \cdot \ldots$

b) Folgt aus (i) ($n = p$, $\varphi(p) = -1$)

2 Algebraische Strukturen mit 2 Verknüpfungen: Ringe und Körper

2.1 Definition

Sei $R \neq \emptyset$ eine Menge mit zwei Verknüpfungen $+$ und $\bullet$.

(i) Wir nennen $(R, +, \cdot)$ einen *Ring*, falls gilt:

  (a) $(R, +)$ ist eine abelsche Gruppe (Eselsbrücke: KAIN)
  Das neutrale Element bezeichnen wir hier mit 0, das zu $a \in \mathbb{R}$ Inverse mit $-a$ (schreibe auch $a - b$ für $a + (-b)$).

  (b) $(R, \cdot)$ ist eine Halbgruppe.

  (c) Es gelten die Distributivgesetze:
  $a \cdot (b + c) = (a \cdot b) + (a \cdot c) = ab + ac$
  $(a + b) \cdot c = (a \cdot c) + (b \cdot c) = ac + bc \qquad \forall a, b, c \in R$

(ii) Ein Ring $(R, +, \cdot)$ heißt *kommutativ* falls $\cdot$ ebenfalls kommutativ ist, also falls $\forall a, b \in \mathbb{R} : a \cdot b = b \cdot a$

(iii) Ein Ring $(R, +, \cdot)$ heißt *Ring mit Eins*, falls $(R, \cdot)$ ein Monoid ist mit neutralen Element $1 \neq 0$ $(\forall a \in R : a \cdot 1 = 1 \cdot a = a)$.

(iv) Ist $(R, +, \cdot)$ Ring mit Eins, dann heißen die bezüglich $\cdot$ invertierbaren Elemente *Einheiten*. Das zu a bezügliche $\cdot$ invertierbare Element bezeichnen wir mit a^{-1}.
R^* := Menge der Einheiten in R.

2.2 Beispiel

a) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit Eins (1)
$\mathbb{Z}^* = \{1, -1\}$, $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ ebenso
$\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}, \mathbb{R}^* = \mathbb{R}\backslash\{0\}$.

b) $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring ohne Eins

c) trivialer Ring $(\{0\}, +, \cdot)$ ohne Eins

d) $n \in \mathbb{N}, n \geq 2, (\mathbb{Z}_n, \oplus, \odot)$ kommutativer Ring mit Eins

e) $(\mathbb{R}^n, \underbrace{+\,,\,\cdot}_{\text{Komponentenweise}})$; allgemein: $R_1, \ldots, R_n$ Ringe, dann $R_1, \times \cdots \times R_n$ Ring.

f) $M_n(\mathbb{R})$ - Menge aller $n \times n$-Matrizen über $\mathbb{R}$, mit Matrixaddition und -multiplikation ist Ring mit Eins (=E_n), nicht kommutativ für $n \geq 2$.

2.3 Satz (Rechnen mit Ringen)

Sei $(R, +, \cdot)$ ein Ring, $a, b, c \in R$. Dann gilt:

(i) $a \cdot 0 = 0 \cdot a = 0$

(ii) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$

(iii) $(-a) \cdot (-b) = a \cdot b$

Beweis

(i) $a \cdot 0 = a \cdot (0 + 0) \underset{2.1(3)}{=} a \cdot 0 + a \cdot 0$
addiere $-(a \cdot 0)$ (Inverses von $a \cdot 0$) auf beiden Seiten, erhalte $0 = a \cdot 0$
Analog $0 \cdot a = 0$

(ii) $(-a) \cdot b + a \cdot b \underset{2.1(3)}{=} (-a + a) \cdot b = 0 \cdot b \overset{(i)}{=} 0$
also ist $(-a \cdot b)$ Inverses zu $a \cdot b$, also $= -(a \cdot b)$.
Analog $a \cdot (-b) = -(a \cdot b)$

(iii) $(-a) \cdot (-b) \underset{(ii)}{=} -(a \cdot (-b)) \underset{(ii)}{=} -(-(a \cdot b)) = a \cdot b$

□

2.4 Bemerkung

a) In jedem Ring mit Eins sind 1 und -1 Einheiten (denn $(-1) \cdot (-1) = 1$, siehe 2.3(iii))
Es kann mehr geben (z.B. in $\mathbb{Z}_5$ usw.). Es kann auch $-1 = 1$ gelten (z.B. in $(\mathbb{Z}_2, \oplus, \odot)$)

b) 0 kann nach 2.3(i) nie Einheit sein (da $1 \neq 0$)

c) In einem kommutativen Ring R gilt der *Binomialsatz*,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \quad (n \in \mathbb{N}, a, b \in R)$$

2.5 Definition

Ein kommutativer Ring $(K, +, \cdot)$ heißt *Körper*, wenn jedes Element $0 \neq x \in K$ eine Einheit ist, also wenn

$$K^* = K \backslash \{0\}$$

2.6 Beispiele

a) $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ sind Körper. $(\mathbb{Z}, +, \cdot)$ ist kein Körper.

b) vgl. Beispiel 1.18 b)

$$\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n \mid \mathrm{ggT}(z, n) = 1\}$$

ist Gruppe bezüglich $\odot$

$\Rightarrow (\mathbb{Z}_n, \oplus, \odot)$ ist genau dann ein Körper, wenn n eine Primzahl ist.

2.7 Satz (Rechnen im Körper, Nullteilerfreiheit)

Sei $(K, +, \cdot)$ ein Körper, $a, b \in K$

Dann gilt

$$a \cdot b = 0 \Leftrightarrow a = 0 \text{ oder } b = 0$$

Gegenbeispiel: $(\mathbb{Z}_6, \oplus, \odot)$ ist kein Körper. Hier gilt $2 \odot 3 = 0$, aber weder $2 = 0$, noch $3 = 0$

Beweis

"$\Leftarrow$": klar: $0 \cdot b = 0$ oder $a \cdot 0 = 0$ (Satz 2.3 (i), Rechenregeln für Ringe)

"$\Rightarrow$": Sei $a \cdot b = 0$. Angenommen $a \neq 0$ (d.h. a hat Inverses)

Dann ist
$$\begin{aligned} b &= 1 \cdot b = (a^{-1} \cdot a) \cdot b \\ &= a^{-1} \cdot (a \cdot b) \\ &= a^{-1} \cdot 0 \\ &\overset{2.3(i)}{=} 0 \end{aligned}$$

□

2.8 Definition

Seien $(R, +, \cdot)$ und $(\tilde{R}, \boxplus, \boxdot)$ Ringe.

(i) $\varphi : R \to \tilde{R}$ heißt (Ring-)*Homomorphismus*, falls gilt:

$$\varphi(\underbrace{x+y}_{\in R}) = \underbrace{\varphi(x)}_{\in \tilde{R}} \boxplus \underbrace{\varphi(y)}_{\in \tilde{R}} \quad \text{und} \quad \varphi(x \cdot y) = \varphi(x) \boxdot \varphi(y) \quad \forall x, y \in R$$

2.9 Beispiel

$\varphi(\mathbb{Z},+,\cdot) \to (\mathbb{Z}_n,\oplus,\odot)$
$x \mapsto x \bmod n$ ist Ringhomomorphismus (kein Isomorphismus), da φ nicht injektiv ist, z.B. $n = 5 : \varphi(1) = \varphi(6) = \varphi(11) \dots$

2.10 Satz (Chinesischer Restsatz)

Seien $m_1,\dots,m_n \in \mathbb{N}$ paarweise teilerfremd, $M := m_1 \cdot \ldots \cdot m_n,\ \ a_1,\dots,a_n \in \mathbb{Z}$
Dann existiert ein x, $0 \le x < M$ mit

$$\begin{array}{lll} x & \equiv & a_1 \quad (\bmod m_1) \\ x & \equiv & a_2 \quad (\bmod m_2) \\ \dots & & \\ x & \equiv & a_n \quad (\bmod m_n) \end{array}$$

Beweis

Für jedes $i \in \{1,\dots,n\}$ 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 $t_i \cdot m_i + s_i \cdot M_i = 1$
Setze $e_i := s_i \cdot M_i$, dann gilt:

$$\begin{array}{l} e_i \equiv 1 \quad (\bmod m_i) \\ e_i \equiv 0 \quad (\bmod m_j) \quad (j \neq i) \end{array}$$

Die Zahl $x := \sum_{i=1}^{n} a_i e_i (\bmod M)$ ist dann die Lösung der simultanen Kongruenz. $\square$

2.11 Beispiel

a) Finde $0 \le x < 60$ mit $x \equiv \begin{cases} 2 & (\bmod 3) \\ 3 & (\bmod 4) \\ 2 & (\bmod 5) \end{cases}$

$M = 3 \cdot 4 \cdot 5 = 60$

$$\begin{array}{lll} M_1 = \frac{60}{3} = 20 & 7 \cdot 3 + (-1) \cdot 20 = 1 & \Rightarrow e_1 = -20 \\ M_2 = \frac{60}{4} = 15 & 4 \cdot 4 + (-1) \cdot 15 = 1 & \Rightarrow e_2 = -15 \\ M_3 = \frac{60}{5} = 12 & 5 \cdot 5 + (-2) \cdot 12 = 1 & \Rightarrow e_3 = -24 \end{array}$$

$x = (2 \cdot (-20) + 3 \cdot (-15) + 2 \cdot (-24)) \bmod 60 = 47$

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

(a) Berechne $2^{1000} \bmod 3, 5, 7, 11$

$$\begin{array}{lcrcl} 2^{1000} \bmod 3 & = & (-1)^{1000} \bmod 3 & = & 1 \\ 2^{1000} \bmod 5 & = & 4^{500} \bmod 5 = (-1)^{500} \bmod 5 & = & 1 \\ 2^{1000} \bmod 7 & = & 2^{3\cdot 333+1} \bmod 7 = (8^{333} \cdot 2) \bmod 7 = (1 \cdot 2) \bmod 7 & = & 2 \\ 2^{1000} \bmod 11 & = & 2^{5\cdot 200} \bmod 11 = 32^{200} \bmod 11 = (-1)^{200} \bmod 11 & = & 1 \end{array}$$

(b) Suche $0 \leq x < 1155$ mit $x \equiv \begin{cases} 1 & (\bmod 3) \\ 1 & (\bmod 5) \\ 2 & (\bmod 7) \\ 1 & (\bmod 11) \end{cases}$

Der chinesische Restsatz liefert $x = 331$

2.12 Bemerkung

Man kann auch zeigen, dass die Lösung x aus Satz 2.10 eindeutig ist:

Durch $\psi : \begin{array}{l} \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n} \\ \quad x \mapsto (x \bmod m_1, \ldots, x \bmod m_n) \end{array}$

wird ein Ringisomophismus definiert:

ψ ist surjektiv (zu jedem n-Tupel aus $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ gibt es eine Lösung x, siehe Restsatz) und es gilt:

$\underbrace{|\mathbb{Z}_M|}_{M} = \underbrace{|\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}|}_{m_1 \cdot \cdots \cdot m_n = M}$

also ist ψ bijektiv, also auch injektiv, also ist Lösung x eindeutig.

2.13 Korollar

$M = m_1 \cdot \cdots \cdot m_n$, m_i paarweise teilerfremd.
Dann ist $\varphi(M) = \varphi(m_1) \cdot \ldots \varphi(m_n)$, insbesondere:

$n = p_1^{a_1} \cdot \cdots \cdot p_k^{a_k}$ (p_i Primzahlen, $a_1 > 0, p_i \neq p_j$ für $i \neq j$)

Beweis

Nach 2.12 ist $\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ mittels ψ
$\Rightarrow x$ Einheit $\Leftrightarrow \psi(x) = (x \bmod m_1, \ldots, x \bmod m_n)$ Einheit
$\Leftrightarrow x \bmod m_i$ Einheit $\forall i = 1 \ldots n$
$\Rightarrow \varphi(M) = \varphi(m_1) \cdot \cdots \cdot \varphi(m_n)$
$\varphi(p^a) \underbrace{=}_{\text{Überlegen}} p^a - p^{a-1} = p^{a-1}(p-1)$

2.14 Definition

Sei K Körper mit Nullelement 0 und Einselement 1:

(i) Ein *Polynom über K* ist Ausdruck $f = a_0 x^0 + a_1 x^1 + \cdots + a_n x^n$, $n \in \mathbb{N}_0, a_i \in K$.
a_i heißen *Koeffizienten* des Polynoms.

(a) Ist $a_i = 0$, so kann man $0 \cdot x^i$ bei der Beschreibung weglassen.

(b) Statt $a_0 x^0$ schreibt auch a_0

(c) Sind alle $a_i = 0$, so schreibt man $f = 0$, das Nullpolynom.

(d) Ist $a_i = 1$, so schreibt man x^i statt $1 \cdot x^i$

(e) Die Reihenfolge der $a_i x^i$ kann verändert werden, ohne dass das Polynom sich verändert ($x^4 + 2x^3 + 3 = 2x^3 + 3 + x^4$)

(ii) Zwei Polynome f und g sind *gleich*, wenn ($f = 0$ und $g = 0$) oder ($f = a_0 + a_1x^1 + \cdots + a_nx^n$, $g = b_0 + b_1x^1 + \cdots + b_mx^m, a_n \neq 0, b_m \neq 0$ und $n = m$, $a_i = b_i$ für $i = 0, \ldots, n$) gilt.

(iii) Die Menge aller Polynome über K bezeichnet man als $K[x]$

2.15 Beispiel

a) $\underbrace{f}_{f(x)} = 3x^2 + \frac{1}{2}x - 1 \in \mathbb{Q}[x] \wedge f \in \mathbb{R}[x]$

b) $g = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$

Wir wollen in $K[x]$ wie in einem Ring rechnen können. Wir brauchen dazu + und · für Polynome.

2.16 Satz und Definition

K Körper, dann wird $K[x]$ zu einem kommutativen Ring mit Eins durch folgende Verknüpfungen:

$f = \underbrace{\sum_{i=0}^{n} a_i x^i}_{\text{z.B. } x+2}, \quad g = \underbrace{\sum_{j=0}^{m} b_j x^j}_{x^3+2x+1},$

dann

$$f + g = \underbrace{\sum_{i=0}^{\max(m,n)} (a_i + b_i)x^i}_{x^3+3x+3}$$

$$f \cdot g = \sum_{i=0}^{n+m} c_i x^i$$

$$\text{mit } c_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0 = \sum_{j=0}^{i} a_j b_{i-j} \qquad \text{(Faltungsprodukt)}$$

(setze a_i mit $i > n$ bzw. b_j mit $j > m$ gleich 0)

- Einselement: $f = 1$ ($a_0 = 1, a_j = 0$ für $j \geq 1$)
- Nullelement: $f = 0$

$K[x]$ heißt der *Polynomring* in einer Variablen über K.
Beweis: Ringeigenschaften nachrechnen.

2.17 Bemerkung

Die +-Zeichen in der Beschreibung der Polynome entsprechen der Ring-Addition der *Monome* $a_0, ax, a_2x^2, \dots, a_nx^n$

2.18 Beispiel

a) in $\mathbb{Q}[x], \mathbb{R}[x]$ Addition, Multiplikation klar

b) in $\mathbb{Z}_3[x]$: $f = 2x^3 + 2x + 1$, $g = 2x^3 + x$

$$\begin{aligned} f + g &= x^3 + 1 \\ f \cdot g &= (2x^3 + 2x + 1)(2x^3 + x) \\ &= x^6 + 2x^4 + x^4 + 2x^2 + 2x^3 + x \\ &= x^6 + 2x^3 + 2x^2 + x \end{aligned}$$

c) in $\mathbb{Z}_2[x]$: $f = x^2 + 1$, $g = x + 1$

$$\begin{aligned} f + g &= x^2 + x \\ f + f &= 0 \\ g \cdot g &= x^2 + 1 \end{aligned}$$

2.19 Definition

Sei $0 \neq f \in K[x]$

$f = a_0 + a_1x + \cdots + a_nx^n$ mit $a_n \neq 0$

Dann heißt n der *Grad* von f Grad(f)

Grad(0) := $-\infty$
Grad$(f) = 0$ *für konstante Polynome* $\neq 0$

2.20 Satz

K Körper, $f, g \in K[x]$

Dann ist Grad$(f \cdot g)$ = Grad(f) + Grad(g)

(Konvention: $-\infty + (-\infty) = -\infty + n = -\infty$)

Beweis

Stimmt für $f = 0$ oder $g = 0$

$$\begin{aligned} f &= a_0 + a_1x^1 + \ldots + a_nx^n && \text{mit} \quad a_n \neq 0 \\ g &= b_0 + b_1x^1 + \ldots + b_mx^m && \text{mit} \quad b_m \neq 0 \\ f \cdot g &= (\ldots) \cdot (\ldots) = \ldots + \underbrace{(a_nb_n)}_{\substack{\neq 0, \\ \text{(siehe Satz 2.7 Nullteilerfreiheit in Körpern)}}} \cdot x^{n+m} \end{aligned}$$

Höhere Potenzen mit Koeffizienten $\neq 0$ gibt es nicht

$\Rightarrow \text{Grad}(f \cdot g) = n + m$

2.21 Korollar

K Körper, dann $K[x]^* = \{f \in K[x] \mid \text{Grad}(f) = 0\}$,

d.h. nur die konstanten Polynome $\neq 0$ sind in $K[x]$ bezüglich $\cdot$ invertierbar.

$$\underbrace{f}_{\text{Grad } n} \cdot \underbrace{f^{-1}}_{\text{müsste Grad } -n \text{ haben}} = \underbrace{1}_{\text{Grad } 0} \leftarrow \text{geht nicht}$$

2.22 Definition

Sei $b \in K$

$\varphi_b : K[x] \to K,\ f := \sum_{i=0}^{n} a_i x^i \mapsto f(b) := \sum_{i=0}^{n} a_i b^i$

ist ein surjektiver Ringhomomorphismus, der sogenannte *Auswertungshomomorphismus* an der Stelle b.

(setze b für x ein)

2.23 Definition

K Körper, $f, g \in K[x]$

f teilt g, $f|g$, falls ein $q \in K[x]$ existiert mit $g = q \cdot f$

(Nach 2.20 ist dann $\text{Grad}(f) \leq \text{Grad}(g)$, falls $g \neq 0$)

2.24 Definition (Division mit Rest)

K Körper, $0 \neq f \in K[x],\ g \in K[x]$

Dann existieren eindeutig bestimmte Polynome $q, r \in K[x]$ mit $g = q \cdot f + r$ und $\text{Grad}(r) < \text{Grad}(f)$.

Bezeichnung:

$$r =: g \bmod f$$
$$q =: g \operatorname{div} f$$

Beweis

Vgl. Mathe I für $\mathbb{Z}$, siehe z.B. WHK Satz 4.69

2.25 Beispiel

a)

$$g = x^4 + 2x^3 - x + 2 \quad \in \mathbb{Q}[x]$$
$$f = 3x^2 - 1 \quad \in \mathbb{Q}[x]$$

Rechne:

$$\begin{array}{l}
\Big(x^4 + 2x^3 \qquad - x \ + 2\Big) : \Big(3x^2 - 1\Big) = \frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{9} + \dfrac{-\frac{1}{3}x + \frac{19}{9}}{3x^2 - 1} \\
\underline{- x^4 \qquad + \frac{1}{3}x^2} \\
\qquad 2x^3 + \frac{1}{3}x^2 - x \\
\qquad \underline{- 2x^3 \qquad + \frac{2}{3}x} \\
\qquad\qquad \frac{1}{3}x^2 - \frac{1}{3}x + 2 \\
\qquad\qquad \underline{- \frac{1}{3}x^2 \qquad + \frac{1}{9}} \\
\qquad\qquad\qquad - \frac{1}{3}x + \frac{19}{9}
\end{array}$$

b)

$$g = x^4 + x^2 + 1 \qquad f = x^2 + x \quad \in \mathbb{Z}_2[x]$$

Rechne:

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

2.26 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 Nullstelle von f).

Beweis

"$\Rightarrow$" sei f durch $(x - a)$ teilbar, d.h.

$$f = q \cdot (x - a) \Rightarrow f(a) = q(a) \cdot (\underbrace{a - a}_{0}) = 0 \quad q \in K$$

"$\Leftarrow$" Division mit Rest: $f = q(x - a) + r$, wobei $\text{Grad}(r) < \underbrace{\text{Grad}(x - a)}_{1}$

$\Rightarrow r$ ist konstantes Polynom (Grad 0) oder Nullpolynom (Grad $(-\infty)$) also $r \in K$

$$0 = f(a) = q(a) \cdot 0 + r \Rightarrow r = 0$$

$\square$

2.27 Definition

K Körper

(i) Ein Polynom dessen höchster von 0 verschiedener Koeffizient gleich 1 ist, heißt normiert.

(ii) $g, h \in K[x]$, nicht beide 0

$f \in K[x]$ heißt *größter gemeinsamer Teiler* von g und h ($f = \mathrm{ggT}(g, h)$), falls f normiertes Polynom von maximalem Grad ist, das g und h teilt.

(iii) $g, h \in K[x] \setminus \{0\}$ beide nicht 0

$f \in K[x]$ heißt *kleinstes gemeinsames Vielfaches* von g und h ($f = kgV(g, h)$), falls f normiertes Polynom von kleinstem Grad ist, das von g und h geteilt wird.

2.28 Bemerkung

a) $f = \sum_{i=0}^{n} a_i x^i, a_n \neq 0$, dann ist $a_n^{-1} f = x^n + \dots$ normiertes Polynom.

(z.B.: $f = 3x^2 + x + 7 \in \mathbb{R}[x]$)

dann $\frac{1}{3} f = x^2 + \frac{x}{3} + \frac{7}{3}$ normiert.

In $\mathbb{Z}_{11}[x]$: $\underbrace{4}_{\text{Inverses von 3, denn } 3 \cdot 4 = 12 \equiv 1 \pmod{11}} f = x^2 + 4x_6$ normiert.

b) $\mathrm{kgV}(g, h)$ existiert und ist eindeutig:

$$\begin{aligned}
\text{sei } f_1 &= \mathrm{kgV}(g, h), \; f_2 = \mathrm{kgV}(g, h) \\
&\Rightarrow g, h | f_1, \quad g, h | f_2 \\
&\Rightarrow g, h | (f_1 - f_2)
\end{aligned}$$

c) $\mathrm{ggT}(g, h)$ existiert. Beweis Eindeutigkeit wie in $\mathbb{Z}$ (Mathe I), folgt aus.

2.29 Satz (von Bezout)

K Körper, $g, h \in K[x]$, nicht beide 0.

Dann existieren $s, t \in K[x]$, sodass

$$f = s \cdot g + t \cdot h$$

ein ggT von g und h ist.

(Beweis: EEA in $K[x]$, später)

2.30 Satz

Euklidischer Algorithmus in $K[x] \to$ siehe „Blatt”

2.31 Satz

EEA in $K[x] \to$ siehe „Blatt”

2.32 Beispiel

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

2.33 Definition

k Körper. Ein Polynom $p \in K[x]$, Grad$(p) \geq 1$ (d.h. $p \neq 0$, p nicht konst., also keine Einheit) heißt *irreduzibel*, falls gilt:

Ist $p = f \cdot g$ ($f, g \in K[x]$), so ist Grad$(f) = 0$ oder Grad$(g) = 0$ (d.h. f oder g ist konst. Polynom).

Bemerkung: $p = a \cdot a^{-1} \cdot p$ für $a \in K\backslash\{0\}$ geht immer.

2.34 Beispiel

a) $ax + b$ ($a \neq 0$) ist irreduzibel in $K[x]$ für jeden Körper K

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

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

d) $x^2 + 1 \in \mathbb{R}[x]$ ist irreduzibel

e) $x^2 + 1 \in \mathbb{Z}_5[x]$ ist nicht irreduzibel:
$(x^2 + 1) = (x + 2) \cdot (x + 3) = (x^2 + 3x + 2x + 1) = (x^2 + 1)$
$2 \Rightarrow (x^2 + 1)$ ist teilbar durch $(x - 2) \hat{=} (x + 3)$

2.35 Abschlussbemerkung

a) Irreduzibel Polynome in $K[x]$ entsprechen den Primzahlen in $\mathbb{Z}$. Man kann zeigen: $f = \sum_{i=0}^{n} a_i x^i \in K[x]$, $a_n \neq 0, n \geq 1$.
Dann existieren eindeutig bestimmte irreduzibel Polynome $p_1, \ldots, p_e$ und natürlichen Zahlen $m_1, \ldots, m_e \in \mathbb{N}$ mit $f = a_n \cdot p_1^{m_1} \cdot \ldots \cdot p_e^{m_e}$

b) Gegeben: Primzahl p, dann gibt es Körper mit p Elementen:
$(\mathbb{Z}_p, \oplus, \odot)$

Man kann zeigen: zu jeder Primzahlpotenz p^a gibt es Körper mit p^a Elementen, diesen konstruiert man über irreduzible Polynome in $\mathbb{Z}_p[x]$.

3 Der Körper der $\mathbb{C}$ der Komplexen Zahlen

3.1 Definition

Eine komplexe Zahl $\mathbb{C}$ ist von der Form $z = x + i \cdot y$ mit $x, y \in \mathbb{R}$ und einer „Zahl” i mit $i^2 = -1$ („imaginäre Einheit”). x heißt Realteil von z, $x =$Re z
y heißt Imaginärteil, $y =$Im z.

Die Menge aller komplexen Zahlen bezeichnen wie mit $\mathbb{C}$ und definieren auf $\mathbb{C}$ Addition und Multiplikation wie folgt:

Für $z = x + iy$ und $w = a + ib$ ist
$z + w := (x + a) + i(y + b)$,
$z - w := (x - a) + i(y - b)$ und
$z \cdot w := (xa - yb) + i(xb + ya)$.

Erläuterung zur Multiplikation: $((x + iy)(a + ib) = xa + xib + iya + i^2yb = (xa - yb) + i(xb + ya)$.

Mit diesen Verknüpfungen ist $\mathbb{C}$ ein Körper:

a) AG, kG, DG: nachrechnen

b) $0 = 0 + i \cdot 0$

c) additiv Inverses: $-z = -x - iy$

d) $1 = 1 + i \cdot 0$

e) multiplikativ Inverses: $z^{-1} = \frac{1}{z} = \frac{1}{x+iy} = \frac{1}{x+iy} \cdot \frac{x-iy}{x-iy} = \frac{x-iy}{x^2+y^2} = \underbrace{\frac{x}{x^2 + y^2}}_{\in\mathbb{R}} + i \cdot \underbrace{\frac{-y}{x^2 + y^2}}_{\in\mathbb{R}}$

Man nennt für $z = x + iy$ die Zahl $\overline{z} = x - iy$ die zu z *konjugiert komplexe Zahl* und $|z| := \sqrt{x^2 + y^2}$ den *Betrag* von z.

3.2 Beispiel

a) $z = 2 + 3i$ mit $\mathrm{Re}(z) = 2$ und $\mathrm{Im}(z) = 3$.
$\overline{z} = 2 - 3i, |z| = \sqrt{2^2 + 3^2} = \sqrt{13}$
$z \cdot \overline{z} = (2 + 3i) \cdot (2 - 3i)$
$= 4 - 6i + 6i - 9i^2 = 4 + 9 = 13$

b) $w = 1 + i = 1 + 1 \cdot i$: $\mathrm{Re}(w) = 1, \mathrm{Im}(w) = 1, \overline{w} = 1 - i,\ |w| = \sqrt{1^2 + 1^2} = \sqrt{2}$

c) Selbst nachrechnen: $u = 7 = 7 + 0 \cdot i,\ v = 5i = 0 + 5i$

d) $u + w + z = 7 + (1 + i) + (2 + 3i) = 10 + 4i$
$u \cdot w = 7 \cdot (1 + i) = 7 + 7i$
$\frac{w}{z} = \frac{1+i}{2+3i} = \frac{(1+i)\cdot(2-3i)}{4+9} = \frac{2-3i+2i=3i^2}{13} = \frac{5-i}{13} = \frac{5}{13} - \frac{1}{13}i$

3.3 Bemerkung: komplexe Zahlenebene

Man kann $\mathbb{C}$ veranschaulichen in der „Gaußschen Zahlenebene”:
Betrachte $z = x + iy$ als Punkt $(x|y)$ in $\mathbb{R}^2$:

3.4 Satz (Eigenschaften)

a) $$\left.\begin{aligned} \overline{w+z} &= \overline{w} + \overline{z} \\ \overline{w \cdot z} &= \overline{w} \cdot \overline{z} \\ \overline{\left(\frac{w}{z}\right)} &= \frac{\overline{w}}{\overline{z}} \quad (z \neq 0) \\ \overline{\overline{z}} &= z \end{aligned}\right\} \mathbb{C} \to \mathbb{C}, z \mapsto \overline{z} \text{ ist Körperisomorphismus}$$

b) $Re(z) = \frac{z+\overline{z}}{2}, Im(z) = \frac{z-\overline{z}}{2i}$

c) $|z| \geq 0,\ |z| = 0$ nur für $z = 0$

d) $|z| = |\overline{z}| = \sqrt{z \cdot \overline{z}}$

e) $|w \cdot z| = |w| \cdot |z|$

f) $|w + z| \leq |w| + |z|$ (Dreiecksungleichung)
$|w + z| \geq \Big||w| - |z|\Big|$

Beweis

z.B.: d) sei $z = x + iy \quad x, y \in \mathbb{R}$
$\Rightarrow \overline{z} = x - iy, \quad |z| = \sqrt{x^2 + y^2}$
$|\overline{z}| = \ldots$

3.5 Bemerkung

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

b) Mann kann jede quadratische Gleichung $ax^2 + bx + c$ $(a, b, c \in \mathbb{R})$ in $\mathbb{C}$ lösen:
$x_{1|2} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$
Jedes $b^2 - 4ac < 0$ ist, schreibe:
$\frac{-b\pm\sqrt{4ac-b^2}\cdot i}{2a}$

c) Es gilt sogar: Fundamentalsatz der Algebra:
Jedes Polynom $f \in \mathbb{C}[x]$ vom Grad $n \geq 1$ hat genau n Nullstellen in $\mathbb{C}$.

3.6 Polarkoordinaten

Eine andere Möglichkeit, komplexe Zahlen zu beschreiben:

Angabe von Winkel (φ) und Abstand r zum Nullpunkt.
Zu jedem $z \in \mathbb{C}$ gibt es ein eindeutig bestimmtes $r \leq 0$ und ein $\varphi \in \mathbb{R}$ mit $z = r(\cos\varphi + i \cdot \sin\varphi)$ (Polarkoordinatendarstellung von z) und zwar ist $r = |z| = \sqrt{x^2 + y^2}$ für $z = x + iy$, $\frac{x}{r} = \cos\varphi$, $\frac{y}{r} = \sin\varphi$:

$$\begin{aligned} z &= x + iy \\ &= r \cdot \cos\varphi + i \cdot r \cdot \sin\varphi \\ &= r \cdot (\cos\varphi + i \cdot \sin\varphi) \end{aligned}$$

Aus den Additionstheoremen für sin, cos folgt (PÜ6):

$$\begin{aligned} z_1 \cdot z_2 &= |z_1| \cdot |z_2| \cdot (\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)) \\ z^2 &= |z|^2 \cdot (\cos(2\varphi) + i \cdot \sin(2\varphi)) \\ \pm\sqrt{z} &= \sqrt{|z|} \cdot (\cos(\frac{\varphi}{2}) + i \cdot \cos(\frac{\varphi}{2})) \end{aligned}$$

3.7 Beispiel

a) $z_1 = 1,\ r_1 = 1,\ \varphi_1 = 0 \Rightarrow z_1 = 1 \cdot (\cos 0 + i \cdot \sin 0)$

b) $z_2 = i,\ r_2 = 1,\ \varphi_2 = \frac{\pi}{2} \Rightarrow z_2 = 1 \cdot (\cos\frac{\pi}{2} + i \cdot \sin\frac{\pi}{2})$

c) $z_3 = 1 + i,\ r_2 = \sqrt{2},\ \varphi_2 = \frac{\pi}{4} \Rightarrow z_3 = \sqrt{2} \cdot (\cos\frac{\pi}{4} + i \cdot \sin\frac{\pi}{4})$

3.8 Definition/Schreibweise

$e^{i\varphi} := \cos\varphi + i \cdot \sin\varphi$

$z = \underbrace{r}_{\text{Betrag}} \cdot e^{i\varphi}$

3.9 Bemerkung

Statt Defintion 3.8:

Man kann auch die Definition von Folgen, Konvergenz, Grenzwert von $\mathbb{R}$ auf $\mathbb{C}$ übertragen, alles aus Mathe II (Analysis!), u.a. auch Potenzreihen, insbesondere die Exponentialfunktion definieren.
Für alle $z \in \mathbb{C}$ konvergiert $\sum_{k=0}^{\infty} \frac{z^k}{k!} := \exp(z),\ e^z$
Mit den Methoden aus Mathe III - „2. Teil" kann man dann zeigen, dass

$$e^{it} = \cos t + i \cdot \sin t\ \forall t \in \mathbb{R} \text{ (Eulersche Formel)}$$

$$z_1 \cdot z_2 = (r_1 \cdot r_2) \cdot (\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)) = \underline{(r_1 \cdot r_2) \cdot e^{i(\varphi_1 + \varphi_2)}}$$

3.10 Beispiele

a) $1 \cdot e^{i \cdot 0} = 1$

b) $e^{i\pi} = -1$ (und: $e^{i\pi} + 1 = 0$ ☺)

c) $2 \cdot e^{2\pi} = 2$

d) ...

3.11 Bemerkung

$\mathbb{C}$ hat alle algrebraischen und analystischen Eigenschaften wie $\mathbb{R}$ (oder besser), außer:

Es gibt auf $\mathbb{C}$ keine vollständige Ordnung $\leq$, die mit $+$ und $\cdot$ verträglich ist, d.h. für die gelten würde:

$$a \leq b, c \leq d \Rightarrow a + c \leq b + d$$
$$a \leq b, r \geq 0 \Rightarrow ra \leq rb$$

4 Wiederholung und Erweiterung der linearen Algebra aus Mathe II

4.1 Beispiel

a) $K = \mathbb{Z}, V_1 = \mathbb{Z}_2^2 = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} : x_1, x_2 \in \mathbb{Z}_2 \right\}$

V_1 hat 4 Elemente: $\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$\mathcal{O} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, d.h. $-\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$\forall v \in V : 0 \cdot v = \mathcal{O} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und $1 \cdot v = v$

b) $K = \mathbb{Z}_5, V_2 = \mathbb{Z}_5^3 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \right\}$

$v = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, w = \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} \in \mathbb{Z}_5^3$

$-v = \begin{pmatrix} 0 \\ 4 \\ 3 \end{pmatrix}, -w = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}, v + w \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$

$1 \cdot w = w, 2 \cdot w = \begin{pmatrix} 1 \\ 4 \\ 3 \end{pmatrix}, 3 \cdot w = \cdots$

$|V| = 5 \cdot 5 \cdot 5 = 125$

c) $U = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in V_1 : x_1 \oplus x_2 = 0 \right\}$ ist UR von V_1

- $U = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \neq \emptyset$
- Sei $u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \in U$, d.h. $u_1 \oplus u_2 = 0$

$\Rightarrow$ für $\lambda \cdot u = \begin{pmatrix} \lambda u_1 \\ \lambda u_2 \end{pmatrix}$ gilt $\lambda u_1 \oplus \lambda u_2 = \lambda \cdot \underbrace{(u_1 \oplus u_2)}_{0} = 0$

d) $\mathbb{Z}_3^3$:

$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ l.a.; $\begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$ l.u.; $\begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$ sind l.a.

e) Kanonische Basis von V_2 (Bsp. b)):

$B_1 = \underbrace{\left\{ e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}}_{\text{geordnete Basis}}$, $\dim V_2 = 3$

z.B.: $\begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix} = \alpha \cdot e_1 + \beta \cdot e_2 + \gamma \cdot e_3$ mit $\alpha = 2,\ \beta = 3,\ \gamma = 1$ und $\alpha,\ \beta,\ \gamma$ sind die kartesischen Koordinaten.

Eine andere (geordnete) Basis, z.B.:

$B_2 = \left\{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \right\}$

Zeige Vektoren sind linear unabhängig:

$\alpha \cdot \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} + \beta \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \gamma \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = O$

$\Rightarrow \cdots \Rightarrow \cdots \Rightarrow \alpha = \beta = \gamma = 0$

Koordinaten von $\begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$ in B_2?

Stelle LGS auf und löse es ...

4.2 Definition

$A \in M_{n,n}(K)$ heißt *invertierbar*, falls $\exists A^{-1} \in M_{n,n}(K)$ mit $A^{-1} \cdot A = A \cdot A^{-1} = E_n$

5 Lineare Abbildungen

5.1 Definition

Seien V, W K-Vektorräume.

a) $\varphi : V \to W$ heißt *lineare* Abbildung (VR-Homomorphismus), falls:

- $\forall v_1, v_2 \in V : \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ (Additivität)
- $\forall v \in V, \forall \lambda \in K : \varphi(\lambda \cdot v) = \lambda \cdot \varphi(v)$ (Homogenität)

b) Ist die lineare Abbildung $\varphi : V \to W$ bijektiv, so heißt φ *Isomorphismus*, V und W heißen dann *isomorph*, $V \cong W$.

5.2 Bemerkung

$\varphi : V \to W$ ist eine lineare Abbildung:

a) $\varphi(O) = O$

b) $\varphi\left(\sum_{i=1}^{n} \lambda_i v_i\right) = \sum_{i=1}^{n} \lambda_i \varphi(v_i)$

5.3 Beispiel

a) Nullabbildung:
$\varphi : V \to W, v \mapsto O$

b) $\varphi : V \to V, v \mapsto \lambda v$ für jedes festes $\lambda \in K$ ist lineare Abbildung ($\lambda = 1 : \varphi = \mathrm{id}_V$)

c) $\varphi : \mathbb{R}^3 \to \mathbb{R}^3, \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_2 \\ z_3 \end{pmatrix}$ ist eine lineare Abbildung (Spiegelung an x_1, x_2-Ebene)

d) $\varphi : \mathbb{R}^2 \to R^2, \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} (x_1)^2 \\ x_2 \end{pmatrix}\right)$ ist nicht linear

$v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \lambda = 3 :$

$\varphi(3v) = \varphi\left(\begin{pmatrix} 3 \\ 6 \end{pmatrix}\right) = \begin{pmatrix} 9 \\ 6 \end{pmatrix} \neq \begin{pmatrix} 3 \\ 9 \end{pmatrix} = 3 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 3 \cdot \varphi\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = 3 \cdot \varphi(v)$

5.4 Satz

$A \in M_{m,n}(K)$

Dann ist $\varphi : K^n \to K^m$, $x \mapsto Ax$

eine lineare Abbildung

Beweis

folgt aus Rechenregeln für Matrizen:

$$\begin{aligned}\varphi(x+y) = A(x+y) &= Ax + Ay \\ &= \varphi(x) + \varphi(y)\end{aligned}$$

$$\begin{aligned}\varphi(\lambda \cdot x) = A(\lambda x) &= \lambda A x \\ &= \lambda \varphi(x)\end{aligned}$$

□

Alle bisherigen Beispiele waren von dieser Form!
5.3

a) $A = 0 = Nullmatrix$

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

c) $A = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$

Es gilt ($\to$ später):
alle lineare Abbildungen $K^n \to K^m$ sind von der Form in 5.4

5.5 Satz

$\varphi : V \to W$ lineare Abbildung

(i) $U \subseteq V$ UR von V
$\Rightarrow \varphi(U) \subseteq W$ UR von W und $\varphi(V)$ (Bild von V) ist UR von W

(ii) falls $\dim(U)$ endlich : $\dim(\varphi(U)) \leq \dim(U)$

Beweis

(i) $U \subseteq V$ Unterraum, d.h. für $u, v \in U$ ist $\lambda u + \mu v \in U$
$\varphi(U) = \{\varphi(u) | u \in U\}$ ist auch UR:
für $\varphi(u), \varphi(v) \underset{\text{lin. Abb.}}{=} \varphi(\lambda u + \mu v) \in \varphi(U)$
außerdem ist $\varphi(U) \neq \emptyset$, da $\varphi(O) = O$

(ii) $v_1, \ldots, v_k$ Basis von U
$\Rightarrow \varphi(u_1), \cdots, \varphi(u_k)$ ist Erzeugendensystem von $\varphi(U)$
$\Rightarrow$ enthält Basis (Mathe II)
$\Rightarrow$ Behauptung □

5.6 Definition

$\varphi : V \to W$ lineare Abbildung, V endlich dimensional
Dann heißt die $\dim(\varphi(V))$ der Rang von φ, $\mathrm{rg}(\varphi)$.

5.7 Definition/Satz

$\varphi : V \to W$ lineare Abbildung

(i) $\ker(\varphi) := \{v \in V \mid \varphi(v) = O\}$
(alle Vektoren die von φ auf O abgebildet werden)
heißt der Kern von φ und ist ein UR von V.

(ii) φ : injektiv $\Leftrightarrow \ker(\varphi) = \{O\}$

Beweis

(i) $\ker(\varphi)$ ist UR:

- $\ker(\varphi) \neq \emptyset$, da $\varphi(O) = O$
- seien $u, v \in \ker(\varphi)$, d.h. $\varphi(u) = O, \varphi(v) = O$, seien $\lambda, \mu \in K$
$\Rightarrow \lambda u + \mu v \in \ker(\varphi)$, dann:
$\varphi(\lambda u + \mu v) \underset{\text{lin. Abb.}}{=} \lambda \cdot \underbrace{\varphi(u)}_{O} + \mu \cdot \underbrace{\varphi(v)}_{O} = O$

(ii) "$\Rightarrow$"
$\varphi(O) = O$, wegen Injektivität kann kein weiteres Element auf O abgebildet werden.
"$\Leftarrow$"
Angenommen es gibt $v_1, v_2 \in V$ mit $\varphi(v_1) = \varphi(v_2)$, dann ist $O = \varphi(v_1) - \varphi(v_2)$
$= \varphi(v_1 - v_2)$ (lineare Abbildung!)
$\Rightarrow v_1 - v_2 = O$ (nur O wird auf O abgebildet)
$\Rightarrow v_1 = v_2$
$\Rightarrow \varphi$ injektiv

□

5.8 Beispiel

$\varphi : \mathbb{R}^3 \to \mathbb{R}^3$, $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \to \begin{pmatrix} x_1 \\ 2x_1 \\ x_1 + x_2 + 2x_3 \end{pmatrix}$ ist lineare Abbildung

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

$U = \langle e_2, e_3 \rangle, \quad \dim(U) = 2$

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

$\varphi(U) = \langle \varphi(e_2), \varphi(e_3) \rangle = \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle = x_3\text{-Achse}$

$\varphi(e_2) = \varphi(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad \varphi(e_3) = \varphi(\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}) = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}$

$\dim(\varphi(U)) = 1$

5.9 Satz

V, W K-VR, $\dim(V) = n$

$\{v_1, \ldots, v_n\}$ Basis von V
$w_1, \ldots, w_n$ Vektoren aus W (nicht notwendig verschieden)

Dann $\exists!$ lineare Abbildung

$\varphi : V \to W$ mit $\varphi(v_i) = w_i\ (i = 1, \ldots, n)$

und zwar:

$$\left.\begin{array}{l} \varphi : V \to W \\ v = \sum_{i=1}^n \lambda_i v_i \mapsto \sum_{i=i}^n \lambda_i w_i \end{array}\right\} *$$

D.h.: wenn man weiß, wie die Basisvektoren abgebildet werden, dann kennt man die lineare Abbildung vollständig.

Beweis

Für φ aus * gilt:

- φ ist linear
- $\varphi(v_i) = w_i$
  $\varphi(v_1) = \varphi(1 \cdot v_1 + 0 \cdot v_2 + \ldots + 0 \cdot v_n) = 1 \cdot w_1 + 0 \cdot w_2 + \ldots + 0 \cdot w_n = 1 \cdot w_1 = w_1$ usw.
- φ ist eindeutig.

  Angenommen $\exists\ \psi : V \to W$ lin. Abb. mit $\psi(v_i) = w_i\ \forall i = 1 \ldots n$

  Dann ist $\psi(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i (\psi(v_i)) = \sum_{i=1}^n \lambda_i w_i = \varphi(\sum_{i=1}^n \lambda_i v_i)$ $\square$

5.10 Beispiel

$V = \mathbb{R}^2, \varphi$ Drehung um Winkel α $(0 \leq \alpha < 2\pi)$ um Nullpunkt gegen den Uhrzeigersinn.

φ ist lin. Abb.:
$\varphi(\alpha_1 + \alpha_2) = \varphi(\alpha_1) + \varphi(\alpha_2)$
$\varphi(\lambda\alpha) = \lambda\varphi(\alpha)$

$\varphi : e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$

$e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$

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

$$\begin{aligned} \varphi : x \mapsto\ & x_1 \cdot \varphi(e_1) + x_2 \cdot \varphi(e_2) \\ &= x_1 \cdot \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} + x_2 \cdot \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix} \\ &= \begin{pmatrix} x_1 \cdot \cos\alpha - x_2 \cdot \sin\alpha \\ x_1 \cdot \sin\alpha + x_2 \cdot \cos\alpha \end{pmatrix} \\ &= A \cdot x \end{aligned}$$

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

5.11 Satz (Dimensionsformel)

V endl. dim. K-VR, $\varphi : V \to W$ lin. Abb.

Dann gilt:
$\dim(V) = \dim(\ker(\varphi)) + \underbrace{\mathrm{rg}(\varphi)}_{\dim(\varphi(V))}$

Beweis

Sei $u_1, \ldots, u_k$ Basis von $\ker(\varphi)$

Ergänze zu Basis $u_1, \ldots, u_n$ von V (Mathe 2, Basisergänzungssatz)

Setze $U := \langle u_{k+1}, \ldots, u_n \rangle$

Dann ist $\ker(\varphi) \cap U = \{O\}$,
d.h. kein Element außer O liegt in U,
also hat die Abb. $\varphi|_U$ den

$\ker(\varphi|_U) = \{O\}$,

ist damit nach Satz 5.7 (ii) injektiv.
Deshalb ist $\dim(U) = \dim(\varphi(U))$.

Außerdem ist $\varphi(U) = \varphi(V)$
$\Rightarrow \dim(V) = \dim(\ker(\varphi)) + \underbrace{\dim(U)}_{\dim(\varphi(U)) = \dim(\varphi(V)) = \mathrm{rg}(\varphi)}$

□

5.12 Korollar

V, W endlich. dim. K-VR mit $\dim V = \dim W$,
$\varphi : V \to W$ lin. Abb.

Dann sind folgende Aussagen äquivalent:

(i) φ ist surjektiv

(ii) φ ist injektiv

(iii) φ ist bijektiv

Beweis

$\dim V = \dim W = n$

Nach 5.11 gilt:
$n = \dim(\ker(\varphi)) + \mathrm{rg}(\varphi)$

Also: $\underbrace{\mathrm{rg}(\varphi) = n}_{\varphi \text{ surjektiv}} \Leftrightarrow \underbrace{\dim(\ker(\varphi))}_{\varphi \text{ injektiv (Satz 5.7)}} = 0$

$\Rightarrow$ Beh. □

5.13 Zusammenhang lin. Abb. und hom. LGS, Matrizen, Rang

- homogenes LGS: $A \in M_{m,n}(K)$ gesucht:
  Menge aller $x \in K^n$ mit $Ax = O$
- lin. Abb. dazu:
  $\varphi : K^n \to K^m, x \mapsto Ax$
  Dann ist der Lösungsraum des homogenen LGS = $\ker(\varphi)$

Dimensionsformel:

$\underbrace{\dim(\ker(\varphi))}_{\dim(\text{Lösungsraum LGS})} = \underbrace{\dim(K^n)}_{n} - \underbrace{rg(\varphi)}_{\dim(\varphi(K^n))}$

$$\begin{aligned} \varphi(K^n) &= \langle \varphi(e_1), \cdots, \varphi(e_n) \rangle_K \\ &= \langle Ae_1, \cdots, Ae_n \rangle \end{aligned}$$

(Ae_i ist gerade die i-te Spalte S_i von A)

$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$

Also:
$\mathrm{rg}(\varphi) = \dim\left(\langle s_1, \cdots, s_n \rangle_K\right)$ = Maximale Anzahl linear unabhängiger Spalten von A.

Also: dim(Lösungsraum) = $n-$ Spaltenrang von A

Mathe II: dim(Lösungsraum) = $n-$ Zeilenrang von A

$\Rightarrow$ für beliebige $A \in M_{m,n}(K)$ gilt:

$$\begin{aligned}\text{Zeilenrang von } A &= \text{Spaltenrang von } A\\ &= \text{Zeilenrang von } A\end{aligned}$$

$\Rightarrow$ für beliebigen $A \in M_{m,n}(K)$ gilt:

$$\begin{aligned}&= \text{Rang von A}\\ &= \text{rg}(\varphi) \text{ mit } \varphi \text{ wie oben}\end{aligned}$$

6 Matrizen und lineare Abbildungen

6.1 Definition

Seien V, W endlich dimensionale VR mit geordneter Basis

$$\mathcal{B} = (v_1, \cdots, v_n) \text{ von } V$$

und

$$C = (w_1, \cdots, w_m) \text{ von } W$$

Sei

$$\varphi : V \to W \text{ lineare Abbildung}$$

Stelle die Bilder $\underbrace{\varphi(v_1)}_{\in W}, \ldots, \underbrace{\varphi(v_n)}_{\in W}$ bzgl. Basis C dar:

$$\begin{aligned}\varphi(v_1) &= a_{11} \cdot w_1 + \cdots + a_{m1} w_m\\ &\vdots\\ \varphi(v_n) &= a_{1n} \cdot w_1 + \cdots + a_{mn} w_m\end{aligned}$$

Dann heißt die $m \times n$ Matrix

$$A_\varphi^{\mathcal{B},C} := \begin{pmatrix} a_{11} \cdots a_{1n} \\ \vdots \quad\quad \vdots \\ a_{m1} \cdots a_{mn}\end{pmatrix} \text{ (Spalte } i \text{ enthält Koordinaten von } \varphi(v_i) \text{ bzgl. } C)$$

die *Darstellungsmatrix* von φ bzgl. der Basen $\mathcal{B}$ und C
(Schreibweise für den Fall $\mathcal{B} = C$, dann auch $A_\varphi^{\mathcal{B}}$)

Bemerkung: φ durch $A_\varphi^{\mathcal{B},C}$ eindeutig bestimmt, vgl. 5.7

6.2 Beispiel

a)

$$V = W = \mathbb{R}^2, \quad \mathcal{B} = \mathcal{C} = (e_1, e_2) = \left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$$

$$\varphi : V \to V, \quad v \mapsto 2v$$

$$A_\varphi^{\mathcal{B},\mathcal{C}} = A_\varphi^{\mathcal{B}} = ?$$

$$\left.\begin{aligned}\varphi\left(\begin{pmatrix}1\\0\end{pmatrix}\right) &= \begin{pmatrix}2\\0\end{pmatrix} = \underline{2}\begin{pmatrix}1\\0\end{pmatrix} + \underline{0}\begin{pmatrix}0\\1\end{pmatrix}\\ \varphi\left(\begin{pmatrix}0\\1\end{pmatrix}\right) &= \begin{pmatrix}0\\2\end{pmatrix} = \underline{0}\begin{pmatrix}1\\0\end{pmatrix} + \underline{2}\begin{pmatrix}0\\1\end{pmatrix}\end{aligned}\right\} A_\varphi^{\mathcal{B}} = \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$$

andere Basis $\mathcal{D} = \left(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\right) \quad A_\varphi^{\mathcal{B},\mathcal{D}}$

$$\left.\begin{aligned}\varphi\left(\begin{pmatrix}1\\0\end{pmatrix}\right) &= \begin{pmatrix}2\\0\end{pmatrix} = \underline{2}\begin{pmatrix}1\\2\end{pmatrix} - \underline{2}\begin{pmatrix}0\\2\end{pmatrix}\\ \varphi\left(\begin{pmatrix}0\\1\end{pmatrix}\right) &= \begin{pmatrix}0\\2\end{pmatrix} = \underline{0}\begin{pmatrix}1\\2\end{pmatrix} + \underline{1}\begin{pmatrix}0\\2\end{pmatrix}\end{aligned}\right\} A_\varphi^{\mathcal{B},\mathcal{D}} = \begin{pmatrix}2 & 0\\ -2 & 1\end{pmatrix}$$

b) $V = W$ mit $\dim V = n$, $\mathcal{B}$ bel. Basis, $\varphi = id_V$, dann ist:

$$A_\varphi^{\mathcal{B}} = E_n$$

c) $V = W = \mathbb{R}^2$, $\mathcal{B} = \mathcal{C} = (e_1, e_2)$

φ Drehung um Nullpunkt um α gegen Uhrzeigersinn

$$\Rightarrow A_\varphi^{\mathcal{B}} = \begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}$$

Vgl. Beispiel 5.10

d) $V = W = \mathbb{R}^2$, $\mathcal{B} = (e_1, e_2)$

φ : Spiegelung an der $\underbrace{\langle e_1\rangle}_{x_1-\text{Achse}}$, d.h. $\varphi : \begin{pmatrix}x_1\\x_2\end{pmatrix} \mapsto \begin{pmatrix}x_1\\-x_2\end{pmatrix} \quad A_\varphi^{\mathcal{B}} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$

andere Basis $\mathcal{B}' = \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\end{pmatrix}\right)$

$A_\varphi^{\mathcal{B},\mathcal{B}'} = ?$

$$\varphi\left(\begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1\\0\end{pmatrix} = a_{11}\begin{pmatrix}1\\1\end{pmatrix} + a_{21}\begin{pmatrix}1\\-1\end{pmatrix}$$
$$\varphi\left(\begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}0\\-1\end{pmatrix} = a_{12}\begin{pmatrix}1\\1\end{pmatrix} + a_{22}\begin{pmatrix}1\\-1\end{pmatrix}$$

$\Rightarrow$ LGS, ausrechnen, erhalte:

$$A_\varphi^{\mathcal{B},\mathcal{B}'} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

e) andersherum:

$V = W = \mathbb{R}, \quad \mathcal{B} = (e_1, e_2)$

$A_\varphi^{\mathcal{B}} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

Was ist $\varphi\left(\begin{pmatrix} 7 \\ -5 \end{pmatrix}\right)$

$\varphi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$

$\varphi\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 4 \end{pmatrix} = \varphi\left(7\begin{pmatrix} 1 \\ 0 \end{pmatrix} - 5\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = 7\varphi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) - 5\varphi\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = 7\begin{pmatrix} 1 \\ 5 \end{pmatrix} + (-5)\begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} -3 \\ 1 \end{pmatrix}$

Gegeben:

Koordinaten eines Punktes bzgl. Basis $\mathcal{B}$ (z.B. Roboterkoordinaten), Abbildung φ

Gegeben:

Koordinaten dieses Punktes bzgl. Basis C (Weltkoordinatensystem) $\rightarrow$ später

Koordinaten des mit φ abgebildeten Punktes bzgl. C $\rightarrow$ jetzt

6.3 Satz

$V, W, \mathcal{B}, C, \varphi$ wie in 6.1

Sei $v \in V, K_B(v)$ sei Koordinatenvektor von v bzgl. $\mathcal{B}$ (enthält Koordinaten von v bzgl. $\mathcal{B}$)

Dann lässt sich der Koordinatenvektor von $\varphi(v)$ bzgl. C berechnen als

$$K_C(\varphi(v)) = A_\varphi^{\mathcal{B},C} \cdot K_{\mathcal{B}}(v)$$

Beweis: nacher

6.4 Beispiel

$\dim(V) = 3 \quad \mathcal{B} = (v_1, v_2, v_3) \quad \varphi : V \to W$
$\dim(W) = 2 \quad C = (w_1, w_2)$

mit

$$A_\varphi^{\mathcal{B},C} \begin{pmatrix} 1 & 1 & -2 \\ 2 & 0 & 3 \end{pmatrix}$$

$v = \underline{5} \cdot v_1 \underline{-2} \cdot v_2 + \underline{4} \cdot v_3$, d.h. Koordinaten von v bzgl. $\mathcal{B}$ sind $5, -2, 4$

$$K_{\mathcal{B}} = \begin{pmatrix} 5 \\ -2 \\ 4 \end{pmatrix}$$

Was sind Koordinaten von $\varphi(v)$ in Basis C?

$$K_C = \begin{pmatrix} 1 & 1 & -2 \\ 2 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ -2 \\ 4 \end{pmatrix} = \begin{pmatrix} -5 \\ 22 \end{pmatrix}$$

d.h. $\varphi(v) = -5 \cdot w_1 + 22 \cdot w_2$

Beweis

$$A_{\varphi}^{\mathcal{B},C} = \begin{pmatrix} a_{11} \cdots a_{1n} \\ \vdots \\ a_{m1} \cdots a_{mn} \end{pmatrix}, \quad v = \sum_{i=0}^{n} \lambda_i v_i, \quad K_{\mathcal{B}}(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

$$A_{\varphi}^{\mathcal{B},C} \cdot K_{\mathcal{B}}(v) = \begin{pmatrix} \sum\limits_{i=1}^{n} a_{1i} \lambda_i \\ \vdots \\ \sum\limits_{i=1}^{n} a_{mi} \lambda_i \end{pmatrix}$$

$$\begin{aligned} \varphi(v) &= \varphi\left(\sum \cdots\right) \\ &= \sum_{i=1}^{n} \lambda_i \underbrace{\varphi(v_i)}_{\sum_{k=1}^{m} a_{ki} w_k} \\ &= \sum_{k=1}^{m} \underbrace{\left(\sum_{i=1}^{n} \lambda_i a_{ki}\right)}_{\text{Koordinaten von } \varphi(v) \text{ bzgl. } C} \cdot w_k \end{aligned}$$

$$K_{\varphi}(\varphi(v)) = \begin{pmatrix} \sum\limits_{i=1}^{n} \lambda_i a_{1i} \\ \vdots \\ \sum\limits_{i=1}^{n} \lambda_i a_{mi} \end{pmatrix}$$

□

6.5 Bemerkung / Korollar zu 6.3

Der Koordinatenvektor kann als Bild der "Koordinatenabbildung"
$K_B : V \to K^n$
$v = \sum_{i=0}^{n} \lambda v_i \mapsto \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$
aufgefasst werden, dann erhalte folgende Übersicht

$$\begin{array}{lccc} & V & \xrightarrow{\varphi} & W \\ (\text{dim V=n, Basis B}) & \downarrow K_B & & \downarrow K_C \quad (\text{dim W=m, Basis C}) \\ & K^n & \xrightarrow{\text{Multiplikation mit } A_\varphi^{B,C}} & K_m (*) \end{array}$$

(*): $\underbrace{K_C \varphi(v))}_{(*)} = A_\varphi^{B,C} K_B(v)$ Damit folgt:
jede lin. Abb $K^n \to K^m$ (K Körper) ist von der Form $\varphi(x) = Ax$ für ein $A \in M_{m,n}(K)$

Beweis:

Benutze kanonische Basis von K^n bzw. K^m. Dann stimmen Elemente von K^n bzw. K^m mit ihren Koordinatenvektoren bzgl. Basis überein, Beh. folgt aus 6.3

6.6 Satz (Eigenschaften der Darstellungsmatrix)

U, V, W VR mit Basen B, C, D
$\varphi_1, \varphi_2, \varphi : U \to V, \Psi : V \to W$

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

b) $A_{\lambda\varphi}^{B,C} = \lambda \cdot A_\varphi^{B,C}$ $(\lambda \in K)$

c) $A_{\Psi\circ\varphi}^{B,D} = A_\Psi^{C,D} \cdot A_\varphi^{B,C}$

(D.h.: Der Hintereinanderausführung von lin. Abb. entspricht das Matrixprodukt der Darstellungsmatrizen)

Beweis:

Übungsaufgabe

□

Folgerung:

6.7 Satz:

V ein K-VR, dim(V)=n, Basis B
$\varphi : V \to V$ lin. Abb. mit A_φ^B
Dann gilt:
φ invertierbar (bij.) $\Leftrightarrow$ A_φ^B invertierbar und $A_{\varphi^{-1}}^B$ ist dann = $(A_\varphi^B)^{-1}$

Beweis:

"$\Rightarrow$" Sei φ invertierbar, d.h. $\exists \varphi^{-1}$
Dann ist $A^B_\varphi \cdot A^B_{\varphi^{-1}} \underbrace{=}_{(6.6)} A^B_{\varphi \circ \varphi^{-1}} = A^B_{id} = E_n$
analog $A^B_{\varphi^{-1}} = A^B_\varphi$

"$\Leftarrow$" Sei A^B_φ invertierbar, d.h. $\exists Y$ mit $A^B_\varphi \cdot Y = Y \cdot A^B_\varphi = E_n$
Dann ist Y Abbildungsmatrix für eine eindeutig bestimmte lineare Abbildung $\Psi : V \to V$, $Y = A^B_\Psi$
$\overset{(6.6)}{\Rightarrow} A^B_{\varphi \circ \Psi} = A^B_\varphi \cdot A^B_\Psi = E_n$
d.h. $\varphi \circ \Psi = \Psi \circ \varphi = idv \Rightarrow \varphi$ ist bij. (invertierbar.)

□

Fragen: Wann ist eine Matrix (lineare Abbildung) invertierbar?
Wie berechnet man inverse?

6.8 Satz:

$A \in M_{n,n}(K)$
Dann gilt: A ist invertierbar $\Leftrightarrow \underbrace{\mathrm{rg}(A) = n}_{\text{d.h. alle Zeilen/Spalten sind l.u.}}$

Beweis:

Betrachte $\varphi : K^n \to K^n$ mit $\varphi(x) = Ax$
Dann ist $A = A^B_\varphi$ (B Basis von K^n)
A invertierbar $\overset{(6.7)}{\Leftrightarrow}$ φ invertierbar (bij.)
A invertierbar $\overset{(5.12)}{\Leftrightarrow}$ φ surjektiv
A invertierbar $\Leftrightarrow \mathrm{rg}(\varphi) = n$
A invertierbar $\overset{(5.13)}{\Leftrightarrow} \mathrm{rg}(A) = n$

□

6.9 Berechnung von Inversen

$\to$ Blatt (Gauß) + Bsp.

Gesehen: Darstellungsmatrix hängt von der Wahl der Basen ab. Wie ändert sie sich, wenn man Basen ändert? Dieser Vorgang wird als Basistransformation bezeichnet.

Dazu:

6.10 Definition/Satz:

Sei V ein VR, $B = (v_1, \ldots, v_n)$ und $B' = (v'_1, \ldots, v'_n)$ Basis von V
Schreiben v'_i als LK der Basisvektoren von B$(i = 1 \ldots n)$, also

$v_1' = s_{11}v_1 + \dots + s_{n1}v_n$
$v_n' = s_{1n}v_1 + \dots + s_{nn}v_n$

Dann heißt $S_{B,B'} = \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ \vdots & \vdots & \dots & \vdots \\ s_{n1} & s_{n2} & \dots & s_{nn} \end{pmatrix}$ Basiswechselmatrix

Ihre Spalten sind die Koordinatenvektoren der Basisvektoren von B' bzgl. B

Analog:
Stelle v_k als LK der Basisvektoren von B' das ($v_k = \sum_{l=1}^n t_{lk}v_l'$)
erhalte so $S_{B',B} (= (t_{lk})_{l,k=1\dots n})$
Es gilt $(S_{B,B'})^{-1} = (S_{B',B})$
(nachrechnen: $S_{B,B'} \cdot S_{B',B} = E_n$)

6.11 Satz: Koordinaten umrechnen

V mit B, B' wie in 6.10, $v \in V$

Dann ist $K_{B'}(v) = S_{B',B} \cdot K_B(v)$

Beweis:

$v = \sum_{k=1}^n \lambda_k \cdot \underbrace{v_k}_{\sum_{l=1}^n t_{lk}v_l'}$, also $K_B(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$

also $V = \sum_{l=1}^n \underbrace{\left(\sum_{k=1}^n \lambda_k t_{lk} \right)}_{\text{neue Koordinaten (bzgl. B')}} \cdot \underbrace{v_l'}_{\in B'}$

6.12 Beispiel

$V = \mathbb{R}^2,\ B = (e_1, e_2),\ B' = \left(v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right)$

$S_{B,B'} = \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix},\ v_1 = 1 \cdot e_1 + 1 \cdot e_2,\ v_2 = 1 \cdot e_1 - 2 \cdot e_2$

$S_{B',B} = (S_{B,B'})^{-1} = (\dots \text{ Gauß } \dots) = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{1}{3} \end{pmatrix}$

$i = \begin{pmatrix} 3 \\ 6 \end{pmatrix}\ K_B(u) = \begin{pmatrix} 3 \\ 6 \end{pmatrix}\ (u = 3 \cdot e_1 + 6 \cdot 3_2)$

Koordinaten von u in Basis B'?

$K_{B'}(u) = S_{B',B} \cdot K_B(u) = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{1}{3} \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 6 \end{pmatrix} = \frac{4}{-1}$

(also ist $u = 4 \cdot v_1 - 1 \cdot v_2$)

Mit der Basiswechselmatrix kann man auch Darstellungsmatrizen umrechnen:

6.13 Satz: Darstellungsmatrizen umrechnen

$\varphi : V \to W$ 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 $v \in V$
nach 6.3:
$A_\varphi^{B',C'} \cdot K_{B'}(v) = K_{C'}(\varphi(v))$
Koordinatenwechsel nach C (6.11): $= S_{C',C} \cdot K_\varphi(v))$
6.3: $= S_{C',C} \cdot A_\varphi^{B,C} \cdot K_B(v)$
Koordinatenwechsel nach B' (6.11): $S_{C',C} \cdot A_\varphi^{B,C} \cdot s_{B,B'} \cdot K_{B'}(v)$

□

6.14 Korollar

$\varphi : V \to V$ lin. Abb.
B, B' Basen von V. $S := S_{B,B'}$
$\Rightarrow A_\varphi^{B'} = S^{-1} A_\varphi^B S$

6.15 Beispiel

V, B, B' wie in 6.12
φ : Spiegelung an der x_1-Achse
$\Rightarrow A_\varphi^B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$A_\varphi^{B'} \overset{=}{6.14} \begin{pmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{1}{3} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & \frac{4}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix}$

7 Determinanten

7.1 Definition

$A \in M_n(K) \quad i, j \in \{1, \ldots, n\}$
$A_{ij} \in M_{n-1}(K)$ sei die Matrix, die man aus A durch Streichen der i-ten Zeile und der j-ten Spalte erhält.

z.B. $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \quad A_{11} = \begin{pmatrix} 5 & 6 \\ 8 & 9 \end{pmatrix} \quad A_{32} = \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}$

7.2 Definition: Determinante, rekursive Def.

$A \in M_n(K)$

$n = 1$ $A = (a)$, dann $\det(A) := a$

$n > 1$

$$\begin{aligned} det(A) :&= \sum_{j=1}^{n} (-1)^{1+j} a_{1j} \cdot \det(A_{1j}) \\ &= a_{11} \cdot \det(A_{11} - a_{12} \cdot \det(A_{12}) \\ &+ a_{13} \cdot \det(A_{13} - a_{14} \cdot \det(A_{14}) \\ &+ \cdots - \ldots \\ &\cdots + / - a_{1n} \cdot \det(A_{1n}) \end{aligned}$$

$\det(A)$ heißt **Determinante** von A
(Formel heißt auch ”Entwicklung nach der 1. Zeile” → später)

7.3 Beispiel

a) $\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}$

b) $\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11} \cdot (a_{22} \cdot a_{33} - a_{23} \cdot a_{32} - a_{12} \cdot (a_{21} \cdot a_{33} - a_{23} \cdot a_{31}) + a_{13} \cdot (a_{21} \cdot a_{32} - a_{22} \cdot a_{31}) = \ldots$
Regel von Sarrus:
$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{pmatrix}$ Diagonalen von links oben nach rechts unten addieren, Diagonalen von rechts oben nach links unten subtrahieren

c) für $n \times n$-Matrix erhalte $n!$ Summanden (nicht schön! $n = 5 : 120$, $n = 10 : 3.6$Mio)

d) Ist A eine obere oder untere Dreiecksmatrix ist, so lässt sich $\det(A)$ einfach berechnen:
$A = \begin{pmatrix} a_{11} & & & & \\ a_{21} & a_{22} & & & \\ \ldots & \ldots & \ldots & & \\ a_{n1} & \ldots & \ldots & \ldots & a_{nn} \end{pmatrix}$, $\det(A) = a_{11} \cdot a_{22} \cdot \cdots \cdot a_{nn}$
klar für $n = 1$: $A = (a)$
$n > 1$: $\det(A) = a_{11} \cdot \det(B) - \underbrace{a_{12}\det()}_{0} + \underbrace{\ldots}_{0}$, B: A ohne erste Spalte und erste Zeile
Beweis durch Induktion

e) damit klar: $\det(E_n) = 1$

7.4 Entwicklungssatz von Laplace

$A \in M_n(K)$

a) Entwicklung nach der i-ten Zeile:
für $i \in \{1, \ldots, n\}$ gilt:

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

b) Entwicklung nach der j-ten Spalte:

für $i \in \{1, \ldots, n\}$ gilt:

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

$$(-1)^{i+j} \rightsquigarrow \begin{pmatrix} + & - & + & - & + & \ldots \\ - & + & - & + & \ldots & \\ + & - & + & \ldots & & \\ \ldots & & & & & \end{pmatrix}$$

7.5 Beispiel

$A = \begin{pmatrix} 2 & 1 & 1 \\ -1 & 0 & 3 \\ 2 & 0 & 4 \end{pmatrix} \in M_3(\mathbb{R})$

Mit Definition 7.2 (Entwicklung nach der 1. Zeile):

$\det(A) = 2 \cdot \det \begin{pmatrix} 0 & 3 \\ 0 & 4 \end{pmatrix} - 1 \cdot \det \begin{pmatrix} -1 & 3 \\ 2 & 4 \end{pmatrix} + 1 \cdot \det \begin{pmatrix} -1 & 0 \\ 2 & 0 \end{pmatrix} = 2 \cdot 0 - 1 \cdot (-10) + 1 \cdot 0 = 10$

oder: Entwicklung nach der 3. Zeile:

$\det(A) = 2 \cdot \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} - 0 \cdot \det(\ldots) + 4 \cdot \det \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} = 2 \cdot 3 - 0 + 4 \cdot 1 = 10$

oder (besser): Entwicklung nach der 2. Spalte:

$\det(A) = -1 \cdot \det \begin{pmatrix} -1 & 3 \\ 2 & 4 \end{pmatrix} + 0 \cdot \det(\ldots) - 0 \cdot \det(\ldots) = -1 \cdot (-10) = 10$

Also: Es ist geschickt, nach einer Spalte oder Zeile zu entwickeln, in der viele Nullen stehen.

Falls es wenig Nullen gibt: Zuerst Gauß anwenden (Auchtung: det. ändert sich dabei eventuell!)

7.6 Bemerkung

Aus 7.4 folgt $\det(A) = \det(A^T)$

7.7 Satz (Eigenschaften der Determinanten)

$A, B \in M_n(K), s_1, \dots, s_n$ Spalten von A, $s'_i \in K^n, \lambda \in K$

(D1) $\det(s_1, \dots, \underbrace{s_i + s'_i}_{i}, \dots, s_n) = \det(s_1, \dots, s_i, \dots, s_n) + \det(s_1, \dots, s'_i, \dots, s_n)$

(D2) Beim Vertauschen zweier Spalten von A ändert sich das Vorzeichen von $\det(A)$

(D3) $\det(s_1, \dots, \underbrace{\lambda \cdot s_i}_{i}, \dots, s_n) = \lambda \cdot \det(s_1, \dots, s_i, \dots, s_n)$

(Beweis D1-D3 folgt aus 7.2 & 7.4)

(D4) $\det(\lambda \cdot A) = \det(\lambda s_1, \dots, \lambda s_n) \overset{(D3)}{=} \lambda^n \cdot \det(A)$

(D5) Ist eine Spalte von A gleich O, so ist $\det(A) = 0$

(D6) Besitzt A zwei identische Spalten, so ist $\det(A) = 0$
(Vertausche identische Spalten, erhalte Matrix $A' = A$. Nach (D2): $\det(A) = -\det(A') = -\det(A)$. Dies ist nur möglich, falls $\det(A) = 0$ (oder in Körper mit $1 + 1 = 0$. Hier anders beweisen!))

(D7) $\det(s_1, \dots, \underbrace{s_i + \lambda s_j}_{i}, \dots, s_n) = \det(A) \quad (i \neq j)$

mit D1, D3, D6

(D8) $\det(A \cdot B) = \det(A) \cdot \det(B)$

Analog mit Zeilen statt Spalten!

Vorsicht: Im Allgemeinen ist $\det(A + B) \neq \det(A) + \det(B)$

7.8 Bemerkung / Beispiel

Also: Erzeuge mit Gaußelimination viele Nulleinträge (! D2, D3: det ändert sich)

D7: det bleibt, entwickele nach guter Zeile / Spalte, oder bringe Matrix auf obere/untere $\triangle$-Form

z.B.

$$\det\begin{pmatrix} 0 & 1 & 2 \\ -2 & 0 & 3 \\ 2 & -2 & 3 \end{pmatrix} \overset{z_1 \leftrightarrow z_2}{=} -\det\begin{pmatrix} -2 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & -2 & 3 \end{pmatrix} \overset{III = 2 \cdot II + III}{=} -\det\begin{pmatrix} -2 & 0 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 7 \end{pmatrix} = -(-2) \cdot 1 \cdot 7 = 14$$

7.9 Satz (Charakterisietung invertierbarer Matrizen über det)

$A \in M_n(K)$ ist invertierbar $\Leftrightarrow \det(A) \neq 0$

In diesem Fall gilt:

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

Beweis

"$\Rightarrow$": Sei A invertierbar, d.h. $\exists A^{-1}$ mit $A \cdot A^{-1} = A^{-1} \cdot A = E_n$

$\Rightarrow \underbrace{\det(A \cdot A^{-1})}_{(D8):\det(A)\cdot\det(A^{-1})} = \det(E_n) = 1$

$\Rightarrow \det(A) \neq 0$ und $\det(A^{-1}) = (\det(A))^{-1}$

"$\Leftarrow$": Sei A nicht invertierbar.

$\Rightarrow \mathrm{rg}(A) < n$

$\overset{6.8}{\Rightarrow}$ Spalten von A sind l.a.

d.h. $\exists i$ mit $s_i = \sum_{k=1k\neq i}^{n} \lambda_k s_k$ (s_i als LK der anderen Spalten)

$\det(A) \overset{(D7)}{=} \det(s_1, \ldots, s_i - \sum \lambda_k s_k, \ldots, s_n)$
$= \det(s_1, \ldots, O, \ldots, s_n) \overset{(D5)}{=} 0$

7.10 Bemerkung

Berechnung von A^{-1} mittels 6.9 (Gauß mit $(A \mid E_n)$) oder auch mittels det, vgl. Übungsblatt 10, A1

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \Rightarrow A^{-1} = \frac{1}{\det A} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

8 Eigenwerte und Eigenvektoren

8.1 Definition

Sei $A \in M_n(K)$.

Ein Skalar $\lambda \in K$ heißt *Eigenwert* von A, wenn es einen Vektor $O \neq x \in K^n$ gibt („nicht-trivial", d.h. $\neq 0$) mit

$$A \cdot x = \lambda x$$

Jedes solche x heißt dann ein zu λ gehöriger *Eigenvektor* von A und $\mathrm{Eig}(\lambda) = \mathrm{Eig}_A(\lambda) = \{x \in K^n | Ax = \lambda x\}$ (alle zu λ gehör. EV & der Nullvektor O) der λ zugeordnete *Eigenraum*.

8.2 Satz

$\lambda \in K$ ist Eigenwert von $A \in M_n(K) \Leftrightarrow \det(A - \lambda \cdot E_n) = 0$,

und die zu λ gehörigen Eigenvektoren sind genau die nichttrivialen Lösungen des LGS.

$[A - \lambda \cdot E_n]x = O$, also $\mathrm{Eig}_A(\lambda) = \ker(A - \lambda \cdot E_n)$.

Beweis

$Ax = \lambda x \Leftrightarrow Ax = \lambda \cdot E_n \cdot x \Leftrightarrow (A - \lambda E_n)x = O$

Also: λ Eigenwert von $A \Leftrightarrow (A - \lambda \cdot E_n)x = O$ hat noch andere Lösungen als $x = O$

$\underbrace{\Leftrightarrow}_{\text{Mathe III}} \operatorname{rg}(A - \lambda \cdot E_n) < n$

$\underbrace{\Leftrightarrow}_{6.8} (A - \lambda \cdot E_n)$ nicht invertierbar

$\underbrace{\Leftrightarrow}_{7.9} \det(A - \lambda \cdot E_n) = 0$

x Eigenvektor $\Leftrightarrow x \neq O$ und $(A - \lambda \cdot E_n)x = O$

8.3 Definition

Für $A \in M_n(K)$ heißt $p_a(\lambda) := det(A - \lambda \cdot E_n)$ das *charakteristische Polynom* von A.

8.4 Beispiel

$A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} \in M_2(\mathbb{R}$

Eigenwerte, Eigenvektoren, Eig(A), $p_A(\lambda)$?

$A - \lambda \cdot E_2 = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} - \lambda \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1-\lambda & 1 \\ -2 & 4-\lambda \end{pmatrix}$

- $p_A(\lambda) = \det \begin{pmatrix} 1-\lambda & 1 \\ -2 & 4-\lambda \end{pmatrix} = (1-\lambda)(4-\lambda)-(1\cdot(-2)) = \lambda^2-5\lambda+6 = (\lambda-2)(\lambda-3)$

- Eigenwerte von A:
  $\lambda \in W$ von A $\overset{8.2}{\Leftrightarrow} p_A(\lambda) = 0 \Leftrightarrow \lambda = 2$ oder $\lambda = 3$
  $\Rightarrow \lambda_1 = 2, \lambda_2 = 3$ Eigenwerte von A

- Eigenvektoren von A:
  x ist EV von A zum EW $\lambda_1 \Leftrightarrow x \neq O$ und $(A - \lambda_1 E_2)x = O$
  also $\begin{pmatrix} 1-2 & 1 \\ -2 & 4-2 \end{pmatrix} x = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} -1 & 1 \\ -2 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
  $\begin{pmatrix} -1 & 1 & | & 0 \\ -2 & 2 & | & 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} -1 & 1 & | & 0 \\ 0 & 0 & | & 0 \end{pmatrix}$
  $-x1 + x2 = 0$ (x_2 ist freie Variable)
  $\Leftrightarrow x_1 = x_2$
  Lösung $\left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 | x_1 = x_2 \right\}$ alternativ $=< \begin{pmatrix} 1 \\ 1 \end{pmatrix} >_{\mathbb{R}}$
  (oder wähle z.B. $x_2 = 1 \Rightarrow x_1 = 1$, also ist $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ Lösung, restliche Lösungen sind $< \begin{pmatrix} 1 \\ 1 \end{pmatrix} >_{\mathbb{R}}$)

$\mathrm{Eig}_A(\lambda_1) = \mathrm{Ker}\begin{pmatrix}-1 & 1\\ -2 & 2\end{pmatrix} =< \begin{pmatrix}1\\1\end{pmatrix} >$

x ist EV von A zum EW $\lambda_2 \Leftrightarrow x_{\neq}0$ und $\begin{pmatrix}-2 & 1\\ -2 & 1\end{pmatrix} x = \begin{pmatrix}0\\0\end{pmatrix}$

$\mathrm{Eig}_A(\lambda_2) = \mathrm{Ker}\begin{pmatrix}-2 & 1\\ -2 & 1\end{pmatrix} =< \begin{pmatrix}1\\2\end{pmatrix} >$

zu Lösung von homogenen LGS: siehe Blatt im Moodle

8.5 Anwendungen

a) Matrixpotenzen

Berechne $A^{2015} = \underbrace{A \cdot A \cdot \ldots \cdot A}_{2015 \text{ mal}}$ für $A = \begin{pmatrix}1 & 1\\ -2 & 4\end{pmatrix}$ aus Bsp. 8.4

Definiere $S := \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$, $\begin{pmatrix}1\\1\end{pmatrix}$ EV zu λ_1, $\begin{pmatrix}1\\2\end{pmatrix}$ EV zu λ_2

$S^{-1} \overset{7.10}{=} \frac{1}{\det S} \cdot \begin{pmatrix}2 & -1\\ -1 & 1\end{pmatrix} = \begin{pmatrix}2 & -1\\ -1 & 1\end{pmatrix}$

dann ist $A = S \cdot \underbrace{\begin{pmatrix}2 & 0\\ 0 & 3\end{pmatrix}}_{D} \cdot S^{-1}$, D=Diagonalmatrix (stimmt, nachrechnen!)

$\Rightarrow A^{2015} = (SDS^{-1})^{2015} = (SD\underbrace{S^{-1}) \cdot (S}_{E_2}DS^{-1}) \cdot (SDS^{-1}) \cdot \cdots \cdot (SDS^{-1})$

$= S \cdot D^{2015} \cdot S^{-1}$

$= S \cdot \begin{pmatrix}2^{2015} & 0\\ 0 & 3^{2015}\end{pmatrix} S^{-1}$

Mit lin. Abb./Darstellungsmatr. ausgedrückt:

$\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ mit $A = A_\varphi^{\mathcal{B}} = \begin{pmatrix}1 & 1\\ -2 & 4\end{pmatrix}$, $\mathcal{B}$ kanon. Basis

Bezügl. Basis $\mathcal{B}' = \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}\right)$ hat Darstellungsmatrix Diagonalgestalt $A_\varphi^{\mathcal{B}'} = \begin{pmatrix}2 & 0\\ 0 & 3\end{pmatrix}$

Bem.: nicht jede Darstellungsmatrix lässt sich auf Diagonalgestalt bringen, z.B. $A = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \in M_2(\mathbb{R})$, Drehung um 90°

$\det(A - \lambda E_2) = \det\begin{pmatrix}-\lambda & -1\\ 1 & -\lambda\end{pmatrix} = \lambda^2 + 1$, keine nullstellen in $\mathbb{R}$, also keine reelen Eigenwerte!

b)
- Physik: Schwingungen, Eigenfrequenz, Tacoma Narrows Bridge
- Googles PageRank-Algorithmus
- Eigenfaces / Zähne ...

⋮

8.6 Bemerkung

Für $A \in M_n(K)$ ist $p_A(\lambda) = \det(A - \lambda E_n) = \det \begin{pmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} - \lambda & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{n1} & \dots & \dots & a_{nm} - \lambda \end{pmatrix}$
ein Polynom vom Grad n (folgt aus Def. der Det.)
Nullstellen von $p_A(\lambda)$ sind $\in W$ von A
$\Rightarrow K = \mathbb{R} :\leq n$ Eigenwerte
$K \in \mathbb{C}$: genau n Eigenwerte (nicht notwendig verschieden)

8.7 Definition: diagonalisierbar

a) Eine Matrix $A \in M_n(K)$ heißt **diagonalisierbar**, wenn eine invertierbare Matrix $S \in M_n(K)$ existiert, so dass $A = SDS^{-1}$ gilt, wobei $D = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & \lambda_n \end{pmatrix}$ Diagonalmatrix ist. (die λ_i sind dann gerade die Eigenwerte von A, siehe 8.8)
(Bem.: Dann gilt auch $D = S^{-1}AS$)

b) für lin. Abb:
Eine lin. Abb. $\varphi : V \to V$ heißt **diagonalisierbar**, falls V eine Basis $\mathcal{B}$ aus Eigenvektoren (zur zugehörigen Darstellungsmatrix) besitzt, d.h. $A_\varphi^\mathcal{B}$ ist Diagonalmatrix.

Ist jede Matrix diagonalisierbar?

8.8 Satz: Spektralsatz

a) $A \in M_n(K)$ ist diagonalisierbar $\Leftrightarrow$ Es gibt n l.u. Eigenvektoren von A

b) Besitzt A n verschiedene Eigenwerte, so ist A diagonalisierbar.

Beweis:

a) A diagonalisierbar, d,h, $\exists S$ invertierbar mit
$S^{-1}AS = \begin{pmatrix} \lambda_1 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & \lambda_n \end{pmatrix} \Leftrightarrow AS = S \cdot \begin{pmatrix} \lambda_1 & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & \lambda_n \end{pmatrix}$
Sei $S = (s_1, \dots, s_n)$ (s=Spalten) Für die i-te Spalte s_i von S gilt dann $A_{si} = \lambda_i \cdot s_i$ $(i = 1, \dots, n)$
Also ist s_i Eigenvektor zum EW λ_i von A
S ist invertierbar $\Leftrightarrow$ Spalten $s_1, \dots, s_n$ l.u. (Satz 6.8)

b) zeige per Induktion, dass die zugehörigen Eigenvektoren linear unabhängig sind, Behauptung folgt dann aus (i)

$\square$

8.9 Bemerkung zu 8.8 (ii)

Es gib auch diagonalisierbare Matrizen, die nicht n verschiedene Eigenwerte haben!
z.B. E_n ist bereits in Diagonalform

$$E_n = \begin{pmatrix} 1 & \dots & 0 \\ 0 & \dots & 0 \\ 0 & \dots & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & \dots & 1 \end{pmatrix}}_{S} \underbrace{\begin{pmatrix} 1 & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & \dots & 1 \end{pmatrix}}_{D} \underbrace{\begin{pmatrix} 1 & \dots & 0 \\ 0 & \ddots & 0 \\ 0 & \dots & 1 \end{pmatrix}}_{S^{-1}}$$

aber alle n Ew sind 1 (mit lin. Abb. ausgedrückt: id_v ist diagonalisierbar, $A^B_{\mathrm{id}_v}$ hat n gleiche EW)

9 Norm- und Skalarprodukt

In diesem Kapitel betrachten wir nur $\mathbb{R}$-VR

9.1 Definition: Norm

Für $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{R}^n$ heißt $||v|| := (\sum_{i=1}^n v_i^2)^{\frac{1}{2}}$ die **Norm** oder **Länge**

9.2 Eigenschaften

a) $||v|| \geq 0 \;\; \forall v \in \mathbb{R}^n$
$||v|| = 0 \Leftrightarrow v = O$

b) $||\lambda v|| = |\lambda| \cdot ||v|| \; \forall \lambda \in \mathbb{R}, \forall v \in \mathbb{R}^n$

c) $||v + w|| \leq ||v|| + ||w|| \; \forall v, w \in \mathbb{R}^n$

9.3 Definition: Skalarprodukt

Sind $v, w \in \mathbb{R}^3$ Vektoren, die einen Winkel α einschließen, so heißt

$$(v|w) := ||v|| \cdot ||w|| \cdot \cos \alpha$$

das **Skalarprodukt** von v mit w.
anschaulich: $(v|w)$ = Flächeninhalt des von v und w erzeugten Projektionsrechtecks.

9.4 Eigenschaften des Skalarprodukts

seien $u, v, w \in \mathbb{R}^3, \lambda \in \mathbb{R}$

a) $(v|w) \in R$ (d.h. ist Skalar, daher der Name)

b) $(v|w) = (w|v)$ (denn: $(v|w) = ||v|| \cdot ||w|| \cdot \cos \alpha = ||w|| \cdot ||v|| \cdot \cos \alpha = (w|v)$)

c) $(\lambda \cdot v|w) = (v|\lambda \cdot w) = \lambda \cdot (v|w)$
(denn $\lambda = 0\surd$
$\lambda > 0: \ (\lambda v|w) = ||\lambda \cdot v|| \cdot ||w|| \cdot \cos\alpha = \lambda \cdot ||v|| \cdot ||w|| \cos\alpha = \lambda(v|w)$
$\lambda < 0$: Winkel zw. λv und w ist $\pi - \alpha \ \Rightarrow (\lambda v|w) = ||\lambda \cdot v|| \cdot ||w|| \cdot \cos(\pi - \alpha) = -\lambda \cdot ||v|| \cdot ||w|| \cdot (-\cos\alpha) = \lambda \cdot (v|w))$

d) $(u + v|w) = (u|w) + (v|w)$ (z.B. grafisch klarmachen)
wegen (ii) gilt (iii)&(iv) auch im 2. Argument

e) $(v|v) = ||v||^2$ (denn: $\alpha = 0 : ||v|| \cdot ||v|| \cdot 1$)

zur Berechnung:
e_1, e_2, e_3 kanon. Basisvektoren in $\mathbb{R}^3$
$(e_i|e_i) = 1, \ (e_i|e_j) = 1 \forall i \neq j$ (denn $\alpha = \frac{\pi}{2}$, Vektoren stehen senkrecht zueinander)
$v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}, \ w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \in \mathbb{R}^3$
$\Rightarrow (v|w) = (v_1e_1 + v_2e_2 + v_3 \cdot e_3|w_1e_1 + w_2e_2 + w_3e_3) \overset{(ii),(iii)}{=} v_1w_1(e_1|e_1) + v_1w_2(e_1|e_2) + v_1w_3(e_1|e_3) + \cdots = v_1w_1 + v_2w_2 + v_3w_3$
allgemein:

9.5 Definition: Standardskalarprodukt, euklidischer Vektorraum, euklidische Norm & Abstand

a) für $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}, \ w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in \mathbb{R}^3$
heißt

$$(v|w) := \sum_{j=1}^{n} v_j w_j = v^T w$$

das **Standardskalarprodukt von v mit w**

b) für beliebigen $\mathbb{R} - VR\ V$:
Eine Abb $(\cdot|\cdot) : V \times V \to \mathbb{R} \quad (v, w) \to (v, w)$ heißt **Skalarprodukt** auf V, falls $(\cdot|\cdot)$ Eigenschaften aus 9.4 erfüllt.
V heißt dann **euklidischer Vektorraum**.

c) für $v, w \in V$, V eukl. VR, so heißt

$$||v|| := +\sqrt{(v|v)}$$

die **(euklidische) Norm** von v,

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

der **(euklid) Abstand** von v und w

9.6 Beispiel

a) $v = \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}, w = \begin{pmatrix} 2 \\ 2 \\ 4 \end{pmatrix} \in \mathbb{R}^3$
$(v|w) = v^T w = -1 \cdot 2 + 2 \cdot 2 + 1 \cdot 4 = 6$
$||v|| = +\sqrt{(v|v)} = \sqrt{(-1)^2 + 2^2 + 1^2} = +\sqrt{6}$
$d(v,w) = ||v - w|| = ||\begin{pmatrix} -1-2 \\ 2-2 \\ 1-4 \end{pmatrix}|| = \sqrt{(-3)^2 + 0^2 + (-3)^2} = \sqrt{18}$
Winkel zwischen v und w:
$(v|w) = ||v|| \cdot ||w|| \cdot \cos\alpha \Leftrightarrow \cos \frac{(v|w)}{||v||\cdot||w||} = \frac{6}{\sqrt{6}\sqrt{24}} = \frac{1}{2}$
$\Rightarrow \alpha = \frac{\pi}{3}$

10 Orthogonalsysteme

10.1 Definition: orthogonal, Orthogonalsystem, Orthonormalsystem, Orthonormalbasis

V euklid. VR

a) $v, w \in V$ heißen **orthogonal** (senkrecht), $v \perp w$, fallso $(v|w) = 0$ gilt.
(d.h. $v = O$ oder $w = O$ oder winkel zw. v und w ist $\frac{\pi}{2}$) (O ist $\perp$ zu allen Vektoren)

b) $M \subseteq V$ heißt **Orthogonalsystem** (OGS), falls $(v|w) = 0\ \forall v, w \in M,\ v \neq w$, gilt.
(gilt zusätzlich $||v|| = 1\ \forall v \in M$, so heißt M **Orthonormalsystem** (ONS))

c) Ist V endlich dimensional, so heißt M **Orthogonalbasis** (ONB von V, falls M ONS und Basis von V ist.

10.2 Bemerkung

Jedes ONS ist l.u.:
$v_1, \ldots, v_k$ ONS, $\lambda_1 v_1 + \cdots + \lambda_k v_k = O$ dann ist
$0 = (v_1 | \underbrace{\lambda_1 v_2 + \cdots + \lambda_k v_k}_{0})$
$= \lambda_1 \underbrace{(v_1|v_1)}_{0} + \lambda_2 \underbrace{(v_1|v_2)}_{0} + \cdots + \lambda_k (v_1|v_k)$
$= \lambda_1$
$\Rightarrow \lambda_1 = 0$
analog für $\lambda_2, \ldots, \lambda_k$, alle =0
$\Rightarrow v_1, \ldots, v_k$ l.u.

Man kann zu jedem Unterraum eines euklidischschen VR eine ONB berechnen.
Geg.: $v_1 \ldots v_k \in V$

Ges.: $w_1, \dots, w_k \in V$ (ONS) mit $< v_1, \dots, v_k >=< w_1, \dots, w_k >$
Idee: starte mit 1. Vektor, $w_1 = v_1$
Baue w_2 aus w_1 und v_2:
$w_2 = v_2 + \lambda w_1$ mit λ so, dass $w_2 \perp w_1$.
w_1, w_2 bilden dann OGS, $\frac{w_1}{||w_1||}, \frac{w_2}{||w_2||}$ bilden dann ONS.
$w_1 \perp w_2 \Leftrightarrow (w_1|v_2 + \lambda w_1) = 0$
$\Leftrightarrow (w_1|v_2) + \lambda \underbrace{(w_1|w_1)}_{||w_1||^2} = 0$
$\Leftrightarrow \lambda = \frac{-(w_1|v_2)}{||w_1||^2}$

10.3 Satz: Orthogonalisierungsverfahren von Gram-Schmidt

geg.: $v_1, \dots, v_k \in V$
def.: $w_1, \dots, w_k \in V$ wie folgt:
$w_1 = v_1$
$w_{r+1} := v_{r+1} + \sum_{i=1}^{r} \lambda_i^{(r+1)} w_i$
mit $\lambda_i^{(r+1)} := \frac{-(w_i|v_{r+1}}{||w_i||^2}$ falls $w_i \neq 0$
und $y_1, y_2 \in V$ als $y_r := \frac{w_r}{||w_r||}$ (falls $w_r \neq O$)
Dann gilt:

a) Bricht die Iteration nach k Schritten nicht ab (d.h. $w_i \neq 0$ für $i = 1 \dots k$), so bilden $w_1, \dots, w_k$ ein OGS und $y_1, \dots, y_k$ ein ONS mit $< v_1, \dots, v_k >=< w_1, \dots, w_k >=< y_1, \dots, y_k >$

b) Bricht die Iteration nach r Schritten ab (d.h. $w_r = O$), so gilt: $v_1, \dots, v_{r-1}$ sind l.u., $v_1, \dots, v_r$ l.a.

10.4 Beispiel

$v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix} \in \mathbb{R}^3$
gesucht:

a) ONB für die Ebene $< v_1, v_2 >$

b) Vektor v_3, der diese ONB zu einer ONB von $\mathbb{R}^3$ ergänzt.

Lösung:

a) $w_1 = v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$
$r = 1, w_{r+1} = w_2$
$w_2 = v_2 + \sum_{i=1}^{1} \lambda_i^{(2)} = v_2 + \lambda_1^{(2)} w_1$
mit $\lambda_1^{(2)} = \frac{-(w_1|v_2)}{||w_1||^2}$

$(w_1|v_2) = 1 \cdot 1 + 1 \cdot 3 + 0 \cdot 2 = 4$
$||w_1||^2 = 1^2 + 1^2 = 2$

$$\Rightarrow w_2 = \begin{pmatrix}1\\3\\2\end{pmatrix} - \frac{4}{2} \cdot \begin{pmatrix}1\\1\\0\end{pmatrix} = \begin{pmatrix}-1\\1\\2\end{pmatrix}$$

$$\Rightarrow \text{OGB} \left\{\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}-1\\1\\2\end{pmatrix}\right\}$$

$$\Rightarrow \text{ONB} \left\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\end{pmatrix}, \frac{1}{\sqrt{6}}\begin{pmatrix}-1\\1\\2\end{pmatrix}\right\}$$

b) Vektor, der $\{w_1, w_2\}$ zu Basis ergänzt, ist z.B.

$$v_3 = \begin{pmatrix}1\\0\\0\end{pmatrix}$$

(denn z.B. so zeigen: $\det\begin{pmatrix}1 & -1 & 1\\1 & 1 & 0\\0 & 2 & 0\end{pmatrix} = 1 \cdot \det\begin{pmatrix}1 & 1\\0 & 2\end{pmatrix} = 1 \cdot 2 \neq 0 \Rightarrow w_1, w_2, w_3$ l.u.)

$$w_2 = v_3 - \frac{(w_1|v_3)}{||w_1||^2} \cdot w_1 - \frac{(w_2|v_3)}{||w_2||^2} \cdot w_2 = \begin{pmatrix}1\\0\\0\end{pmatrix} - \frac{1}{2} \cdot \begin{pmatrix}1\\1\\0\end{pmatrix} + \frac{1}{6} \cdot \begin{pmatrix}-1\\1\\2\end{pmatrix} = \begin{pmatrix}\frac{1}{3}\\-\frac{1}{3}\\\frac{1}{3}\end{pmatrix},$$

$||w_3|| = \sqrt{\frac{1}{3}}$

$$y_3 = \sqrt{3}\begin{pmatrix}\frac{1}{3}\\-\frac{1}{3}\\\frac{1}{3}\end{pmatrix}$$

10.5 Definition: orthogonale Matrix

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

10.6 Beispiel

$\mathbb{R}^2$:

$$A = \begin{pmatrix}\cos\alpha & -\sin\alpha\\\underbrace{\sin\alpha}_{s_1} & \underbrace{\cos\alpha}_{s_2}\end{pmatrix} \quad (\alpha \in \mathbb{R}) \text{ ist orthogonal}$$

$(s_1|s_2) = \cos\alpha \cdot (-\sin\alpha) + \sin\alpha \cdot \cos\alpha = 0$
$||s_1|| = ||s_2|| \sqrt{\cos^2\alpha + \sin^2\alpha} = 1$

10.7 Satz: Eigenschaften von orthogonalen Matrizen

Sei $A \in M_n(\mathbb{R})$ orthogonal

a) $A^T A = E_n$

b) A invertierbar, $A^{-1} = A^T$

c) $||Av|| = ||v||$ (zugehörige Abb. ist ”Längentreu“)

d) $|\det A| = 1$

Beweis:

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

b) folgt aus (i)

c) $||Av||^2 = (Av|Av) = (Av)^T \cdot Av = v^T A^T Av \overset{(i)}{=} v^T E_n v = v^T v = (v|v) = ||v||^2$

d) $1 = \det E_n \overset{(i)}{=} \det(A^T A) = \det(A^T) \cdot \det(A) = \det(A) \cdot \det(A) = (\det(A))^2$

11 Mehrdimensionale Analysis

Siehe Blatt im Moodle (11.1 bis 11.12)

11.13 Beispiel

a) $f : \mathbb{R}^2 \to \mathbb{R}$
$f(x,y) = e^x + y^2$
$\underbrace{f'(x,y}_{\text{Jacobimatrix}} = \begin{pmatrix} \frac{\partial f}{\partial x}(x,y) & \frac{\partial f}{\partial y}(x,y) \end{pmatrix} = \begin{pmatrix} e^x & 2y \end{pmatrix}$
$f'(0,0) = \begin{pmatrix} 1 & 0 \end{pmatrix}$
$\nabla f(x,y) = \begin{pmatrix} e^x \\ 2y \end{pmatrix}$

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

Siehe Blatt im Moodle (11.14 bis 11.21)

11.22 Definition: (total)differenzierbar, affin-linear

$D \subseteq \mathbb{R}^n$ offen, $a \in D$
$f : D \to \mathbb{R}^m$ heißt **(total)differenzierbar in a** wenn f in a partiell differenzierbar ist und geschrieben werden kann als $f(x) = f(a) + f'(a)(x-a) + \epsilon(x)$ mit $\epsilon : D \to \mathbb{R}^m$ mit $\lim\limits_{x \to a} \frac{||\epsilon(x)||}{||x-a||} = 0$ (d.h. ϵ wird klein nahe a)
($n = m = 1$, erhalte Definition der Differenzierbarkeit aus Mathe II)
Anschaulich:
f kann in der nähe von a durch die **affin-lineare** Abbildung $x \mapsto \underbrace{f(a)}_{\text{konst.}} + \underbrace{\underbrace{f'(a)}_{\text{Matrix}}(x-a)}_{\text{linear}}$ beschrieben werden

11.23 Definition: Richtungsableitung

$D \subseteq \mathbb{R}^n$ offen, $f : D \to \mathbb{R}$, $a \in D$
$v \in \mathbb{R}^n$ mit $||v|| = 1$
f heißt **in a differenzierbar in Richtung v** wenn $\lim\limits_{h \to 0} \frac{f(a+hv)-f(a)}{h}$ ex.
Der Grenzwert heißt dann **Richtungsabtleitung** von f in Richtung v im Punkt a.
Bez.: $\frac{\partial f}{\partial v}(a)$

11.24 Bemerkung

$\frac{\partial f}{\partial x_j}$ ist die Richtungsableitung von f in Richtung $e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ (1 an Stelle j)

11.25 Satz

sei $f : D \subseteq \mathbb{R}^n \to \mathbb{R}$ (total)differenzeirbar in $a \in D$
Dann ex. in a alle Richtungsableitungen und für alle $v \in \mathbb{R}^n$ mit $||v|| = 1$ gilt:

$$\frac{\partial f}{\partial v}(a) = f'(a) \cdot v$$

Die Richtungsableitug stellt den Anstieg von f an der Stelle a in Richtung v dar.

Beweis:
f differenzierbar, d.h. $f(x) = f(a) + f'(a) \cdot (x-a) + \epsilon(x)$
$\overset{x=a+h\cdot v}{\Rightarrow} f(a + h \cdot v) = f(a) + f \cdot (a) \cdot (a + h \cdot v - a) + \epsilon(a + h \cdot v)$
$\overset{h \neq 0}{\Rightarrow} \frac{f(a+hv-f(a)}{h} = \frac{f'(a)\cdot(hv)}{h} + \frac{\epsilon(a+hv)}{h}$
$\frac{\partial f}{\partial v} = \lim\limits_{h \to 0} \frac{f(a+hv)-f(a)}{h} = f'(a) \cdot v$

□

11.26 Beispiel

a) Anstieg von $f(x,y) = x^2 + y^2$ im Punkt $a = \begin{pmatrix}1\\1\end{pmatrix}$ in Richtung $v = \begin{pmatrix}\sin\alpha\\ \cos\alpha\end{pmatrix}$ $(||v|| = 1)$

$\frac{\partial f}{\partial v}(1,1) = f'(1,1) \cdot \begin{pmatrix}\sin\alpha\\ \cos\alpha\end{pmatrix} = \begin{pmatrix}2 & 2\end{pmatrix} \cdot \begin{pmatrix}\sin\alpha\\ \cos\alpha\end{pmatrix} = 2 \cdot \sin\alpha + 2 \cdot \cos\alpha$

b) $f(x,y) = 2x^2 + y^2,\ \ a = \begin{pmatrix}\frac{1}{2}\\ \frac{1}{2}\\ \frac{3}{4}\end{pmatrix}$ Punkt auf "Gebirge"

gesucht: Richtung $v = \begin{pmatrix}v_1\\ v_2\end{pmatrix}$, in der die Tangente an den Graph von f die Steigung $\frac{3}{\sqrt{2}}$ hat.

$\frac{\partial f}{\partial v}\left(\frac{1}{2},\frac{1}{2}\right) = f'\left(\frac{1}{2},\frac{1}{2}\right) = \begin{pmatrix}2 & 1\end{pmatrix}\begin{pmatrix}v_1\\ v_2\end{pmatrix} = 2v_1 + v_2 \overset{!}{=} \frac{3}{\sqrt{2}}$ und $||v|| = 1$, d.h. $v_1^2 + v_2^2 = 1$

Gleichungssystem lösen...

ergibt $v = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}$ und $v = \begin{pmatrix}\frac{7}{5\sqrt{2}}\\ \frac{1}{5\sqrt{2}}\end{pmatrix}$

11.27 Bemerkung

Es gilt: $\frac{\partial f}{\partial v}(a) = f'(a) \cdot v = (\nabla f)^T \cdot v = ||\nabla f(a)|| \cdot ||v|| \cdot \cos\alpha$, α: Winkel zw. ∇f und v
$\Rightarrow$ Richtungsableitung: $\frac{\partial f}{\partial v}(a)$ ist am größten, wenn $\cos\alpha = 1$, also $\alpha = 0$ ist, d.h. wenn der Richtungsvektor v in Richtung des Gradienten zeigt.
Der Gradient zeigt also immer in die Richtung des steilsten Anstiegs der Funktion.

Jetzt wieder 1-dimensionale Analysis:

12 Taylorpolynome und Taylorreihe

12.1 Definition

$I \subseteq \mathbb{R}$ Intervall, $x_0 \in I,\ f : I \to \mathbb{R}$

a) $f^{(0)} := f$
$f^{(1)} = f'$, falls f diffbar auf I
$\vdots$
$f^{(n)} = (f^{(n-1)})'$, falls $f^{(n-1)}$ diffbar auf I
(f **n-mal differenzierbar**, $f^{(n)}$ **n-te Ableitung**

b) f heißt **unendlich oft differenzierbar**, falls f n-mal diffbar $\forall n \in \mathbb{N}$.
(Bez. auch $f^{(1)} = f', f^{(2)} = f'', \dots$)

12.2 Beispiel

a) $f(x) = x^2$ ∞ oft diffbar
$f'(x) = 2x,\ f''(x) = 2,\ f^{(n)} = 0 \forall n \geq 3$

b) $f(x) = e^x$
$f^{(n)}(x) = e^x \forall n \in \mathbb{N}_0$

c) $f(x) = \begin{cases} \frac{1}{2}x^2 & x \geq n \\ -\frac{1}{2}x^2 & x < 0 \end{cases}$
$f'(x) = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases} = |x|$, nicht diffbar in $x = 0$

d) $f : \mathbb{R}^+ \to \mathbb{R}^+,\ f(x) = x^\alpha \quad (\alpha \in \mathbb{R})$
$f'(x) = \alpha \cdot x^{\alpha-1}$
$f^{(n)} = \alpha \cdot (\alpha - 1) \cdot \dots \cdot (\alpha - n + 1) \cdot x^{\alpha-n} = n! \underbrace{\binom{\alpha}{n}}_{\text{binom.}} \cdot x^{\alpha-n} \quad \forall n \in \mathbb{N}_0$

12.3 Motivation

Polynome sind besonders einfach zu handhaben.
Wir wollen komplizierte Funktionen möglichst gut mittels Polynome beschreiben / annähern.
Damit zwei Funktionen „ähnlich” sind, sollten nicht nur ihre Funktionswerte in einigen Punkten übereinstimmen, sondern möglichst auch ihre Ableitung in diesen Punkten.

gegeben: Funktion $f : I \to \mathbb{R},\ x_o \in I$
gesucht: Polynom $T_n(x)$ vom Grad n, das f gut annähert, insbesondere an der Stelle x_0.
Wie muss T_n aussehen?

für $n = 0$: (Grad 0, d.h. $T_0(x)$ ist Gerade)
$T_0(x) = f(x_0)$ (dann wenigstens Übereinstimmung in x_0):
$T_0(x_0) f(x_0)$

für $n = 1$: $T_1(x) = f(x_0) + f'(x_0) \cdot (x - x_0)$ Polynome vom Grad 1 $\surd$
$T_1(x_0) = f(x_0) + f'(x_0)$ (Übereinstimmung in x_0) $\surd$
$T_1'(x) = f'(x_0)$
$\Rightarrow T_1'(x_0) = f'(x_0)$ (Übereinstimmung der 1. Ableitung in x_0)

für $n = 2$: $t_2(x) = f(x_0) + f'(x_0) \cdot (x - x_0) + \frac{1}{2} \cdot f''(x_0) \cdot (x - x_0)^2$ Polynom vom Grad 2 $\surd$
$T_2(x_0) = f(x_0) + 0 + 0$ (Übereinstimmung in x_0) $\surd$
$T_2'(x) = f'(x_0) + 2 \cdot \frac{1}{2} \cdot f''(x_0) \cdot (x - x_o)^1 = f'(x_0) + f''(x_0)(x - x_0)$
$T_2''(x) = f''(x_0)$
$T_2'(x_0) = f'(x_0)$
$T_2''(x_0) = f''(x_0)$ $T-2$ und f stimmen in 1. und 2. Ableitung an der Stelle x_0 überein.

12.4 Definition: Taylorpolynom

$F : I \to \mathbb{R}$ n-mal differenzierbar auf I, $x_0 \in I$
Dann heißt

$$T_n(x) := \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x - x_0)^k$$

das **n-te Taylorplynome von f**, entwickelt um den Punkt $x_0 \in I$.
oben für $n = 0, 1, 2$ gesehen:
Für $T_n(x)$ gilt: $T_n(x_n) = f(x_n)$ und $T_n^{(k)}(x_0) = f^{(k)}(x_0)$ für $k = 1 \dots n$

$T_n(x)$ nähert also f an. Wie gut?

12.5 Satz: Formel von Taylor mit Lagrange-Restglied

$f : I \to \mathbb{R}$ (n-1)-mal differenzierbar auf I, $x_0 \in I$
Sei $R_n(x) := f(x) - T_n(x)$
der Fehler zwischen f un dem n-ten Taylorpolynom von f entwickelt um den Punkt x_0. ("Restglied")
Dann gibt es zu jedem $x \in I$ eine Stelle ξ zwischen x_0 und x, so dass

$$R_n(x) = \frac{f^{(n+1)}(\xi)}{n+1} \cdot (x - x_0)^{n+1}$$

(Merkregel: (n+1)-ter Term von $t_{n+1}(x)$ mit ξ statt x_0)
also ist f darstellbar durch das n-te Taylorpolynom mittels

$$f(x) = \underbrace{\sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!}(x - x_0)^k}_{\text{Polynom vom Grad n}} + \underbrace{\frac{f^{(n+1)}(\xi)}{(n+1)!}}_{R_n(x)}(x - x_0)^{n+1}$$

(Taylorentwicklung von f an der Stelle X_0)

Beweis:
Sei $g(x) = (x - x_)^{n+1}$
Es gilt $R_n^{(k)}(x_0) = 0$ und $g^{(k)}(x_0) = 0 \; \forall k = 0 \dots n$
$\frac{R(x)}{g(x)} = \frac{R(x)-R(x_0)}{g(x)-g(x_0)} \overset{*}{=} \frac{R'(\xi_1)}{g'(\xi_1)}$ für ein ξ_1 zwischen x und x_0 (*: 2. Mittelwertsatz aus Mathe II)
$= \frac{R'(\xi_1)-R'(x_0)}{g'(\xi_1)-g'(x_0)} \overset{*}{=} \frac{R''(\xi_2)}{g''(\xi_2)}$ für ein ξ_2 zw. ξ_1 und x_0
$= \dots = \frac{R^{(n+1)}(\xi_{n+1})}{g^{(n+1)}(\xi_{n+1})} = \frac{f^{(n+1)}(\xi_{n+1})}{(n+1)!}$ für ein ξ_{n+1} zwischen ξ_n und x_0
setze $\xi = \xi_{n+1}$, Behauptung folgt

12.6 Bemerkung

a) Der Satz besagt:
   $f(x)$ kann bis auf $R_n(x)$ als Polynom n-ten Grades dargestellt werden.
   Je größer n, desto besser sollte diese Annäherung sein. Insbesondere ist interessant: gilt $R_n(x) \to 0$ für $n \to \infty$?

b) Es gibt auch andere Darstellungen des Restglieds, z.B: mit Integral.

12.7 Beispiel

a) $f(x) = e,\ x_0 = 0$
$f^{(k)} = e^x\ \forall k \in \mathbb{N}_0$
$f^{(k)}(x_0) = e^0 = 1$
$\Rightarrow T_n(x) = \sum_{k=0}^n \frac{f^{(k)}(0)}{k!}(x-0)^k = \sum_{k=0}^n \frac{1}{k!}x^k$
$\Rightarrow \underbrace{e^x}\ f(x) = \underbrace{\sum_{k=0}^{n} \frac{x^k}{k!}}_{T_n(x)} + \underbrace{\frac{e^\xi}{(n+1)!} \cdot x^{n+1}}_{R_n(x)}$ (ξ zwischen 0 und x)
e^ξ ist beschränkt durch e^0 oder e^x, $\frac{x^{n+1}}{(n+1)!} \to 0$ für $n \to \infty$
Also:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}\ \ \forall x \in \mathbb{R}$$