Mathematik III

Marius Hobbhahn, Florian Friedrich

18. Januar 2017

Inhaltsverzeichnis

1 Vektorräume

Bemerkung: 1.1-1.10 identisch mit 8.1-8.10 aus Mathematik 2, SS16

1.1 Definition (Reelle Vektorräume)

Ein $\mathbb{R}$-Vektorraum V ist eine nichtleere Menge, deren Elemente Vektoren genannt werden (Bezeichnung mittels kleiner lateinischer Buchstaben, $v, w, x, y, ...$), auf der eine Addition $+$ definiert ist, $+\colon V \times V \to V$; und eine Multiplikation mit reellen Zahlen ('Skalare') (Bezeichnung mittels kleiner griechischer Buchstaben $\alpha, \beta, \gamma, \lambda, \mu, ...$), $\cdot\colon \mathbb{R} \times V \to V$, so dass gilt:

(1.1) $u + v + w = u + (v + w) \qquad \forall u, v, w \in V$

(1.2) Es existiert ein Vektor $\mathcal{O} \in V$ ('Nullvektor') mit $v + \mathcal{O} = \mathcal{O} + v = v \qquad \forall v \in V$

(1.3) Zu jedem $v \in V$ existiert ein Vektor $-v \in V$ mit $v + (-v) = \mathcal{O}$

(1.4) $u + v = v + u \qquad \forall u, v \in V$

(Diese Eigenschaften (1.1) bis (1.4) kann man zusammenfassen als '$(V, +)$ ist eine kommutative Gruppe').

(2.1) $\overset{\text{Addition in } \mathbb{R}}{(\lambda + \mu)} \cdot v = \lambda \cdot v \overset{\text{Addition in } V}{+} \mu \cdot v \qquad \forall \lambda, \mu \in \mathbb{R}, v \in V$

(2.2) $\lambda(v + w) = \lambda v + \lambda w \qquad \forall \lambda \in \mathbb{R}, v, w \in V$

(2.3) $\overset{\text{Multiplikation in } \mathbb{R}}{(\lambda \cdot \mu)} \cdot v = \lambda \cdot \overset{\text{Multiplikation mit Skalar}}{(\mu \cdot v)} \qquad \forall \lambda, \mu \in \mathbb{R}, v \in V$

(2.4) $1 \cdot v = v \qquad \forall v \in V$

1.2 Beispiel

a) trivialer Vektorraum Nullraum: $V = \{\mathcal{O}\}$
Es gilt $\mathcal{O} + \mathcal{O} \coloneqq \mathcal{O}, \quad \lambda \cdot \mathcal{O} \coloneqq \mathcal{O} \qquad \forall \lambda \in \mathbb{R}$

b) $V = \mathbb{R}^n$, Raum aller 'Spaltenvektoren' der Länge n über $\mathbb{R}$, Elemente haben die Form $\begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix}$ mit $x_1, ..., x_n \in \mathbb{R}$.

$$\mathcal{O} = \begin{pmatrix} 0 \\ ... \\ 0 \end{pmatrix}, \quad \begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ ... \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ ... \\ x_n + y_n \end{pmatrix}, \quad \lambda \cdot \begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda \cdot x_1 \\ ... \\ \lambda \cdot x_n \end{pmatrix}$$

c) $\mathbb{R}$ ist ein $\mathbb{R}$-Vektorraum.
Vektoren: reelle Zahlen.
Skalare: reelle Zahlen.
$\mathcal{O} = 0$

d) Funktionenraum:
$M \neq \emptyset$ Menge. $V = \mathcal{F}(M, \mathbb{R}) := \{f \colon M \to \mathbb{R}\}$
Menge der auf M definierten reellen Funktionen.
Für $f, g \in V, \quad \lambda \in \mathbb{R}$ sei

- $f + g \colon M \to \mathbb{R}, \quad (f + g)(x) = f(x) + g(x) \quad \forall x \in M$
- $\lambda \cdot f \colon M \to \mathbb{R}, \quad (\lambda \cdot f)(x) = \lambda \cdot f(x) \quad \forall x \in M$

Dann ist V mit $\mathbb{R}, +, \cdot$ ein Vektorraum. Nullvektor ist $f = 0 \colon M \to \mathbb{R}, \quad f(x) = 0 \qquad \forall x \in M$.
(kurz: $f \equiv 0$, identisch Null)

1.3 Lemma

Sei V ein $\mathbb{R}$-Vektorraum, $v \in V, \quad \lambda \in \mathbb{R}$

a) $0 \cdot v = \mathcal{O}$

b) $\lambda \cdot \mathcal{O} = \mathcal{O}$

c) Zu jedem $v \in V$ ist der Vektor $-v$ aus (1.3) in 1.1 eindeutig bestimmt.

d) $(-1) \cdot v = -v$

Beweis

a)

$$\begin{aligned}
\mathcal{O} \overset{(1.3)}{=} \overbrace{\underbracket{0 \cdot v}}^{x} + \overbrace{(-0 \cdot v)}^{-x} = \underbracket{(0 + 0)}v + (-0 \cdot v) & \\
&\overset{(2.1)}{=} (0 \cdot v + 0 \cdot v) + (-0 \cdot v) \\
&\overset{(1.1)}{=} 0 \cdot v + (0 \cdot v + (-0 \cdot v)) \\
&\overset{(1.3)}{=} 0 \cdot v + \mathcal{O} \\
&\overset{(1.2)}{=} 0 \cdot v
\end{aligned}$$

b) Wie a), starte mit $\mathcal{O} = \lambda \cdot \mathcal{O} + (-\lambda \cdot \mathcal{O})$, erhalte $\mathcal{O} = \lambda \cdot \mathcal{O}$

d)

$$\begin{aligned}
\underbrace{v + (-1 \cdot v)} &= 1 \cdot v + (-1 \cdot v) \\
&\overset{(2.1)}{=} (1 + (-1))v \\
&= 0 \cdot v \\
&\overset{a)}{=} \mathcal{O} \\
&\overset{(1.3)}{=} v + (-v)
\end{aligned}$$

Addiere auf beiden Seiten $-v$:

$$\underbrace{v + (-1)v} + (-v) = v + (-v) + (-v)$$

$$\Rightarrow -1 \cdot v = -v$$

c) Angenommen, zu $v \in V$ gibt es $-v$ und $-v'$ mit $v+(-v) = \mathcal{O}$ und $v+(-v') = \mathcal{O}$. Dann ist $v + (-v) = v + (-v') \overset{+(-v)\text{auf beiden Seiten}}{\Rightarrow} -v = -v'$

$\square$

1.4 Definition (Untervektorraum)

Sei V ein $\mathbb{R}$-Vektorraum.
Eine Teilmenge $U \subseteq V$, $\quad U \neq \emptyset$ heißt Unter(vektor)raum von V, falls U bezüglich der Addition auf V und der Multiplikation mit Skalaren selbst ein Vektorraum ist.

1.5 Beispiel

a) $V = \mathbb{R}^2, \quad U = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$ ist Unterraum von V

b) $V = \mathbb{R}^2, \quad U = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\}$ ist kein Unterraum von V, z.B. (1.2) ist verletzt, Addition funktioniert auch nicht: $\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix} \notin U$

c) $V = \mathbb{R}^2, \quad U = \left\{ \begin{pmatrix} \lambda \\ 0 \end{pmatrix} \middle| \lambda \in \mathbb{R} \right\}$ ist ein Unterraum von V (prüfe alle Eigenschaften von Definition 1.1) $\rightarrow$ umständlich, einfacher geht es mit Definition 1.6

1.6 Satz (Unterraumkriterium)

Sei V ein $\mathbb{R}$-Vektorraum, sei $\emptyset \neq U \subseteq V$.
Dann ist U Unterraum von V genau dann, wenn gilt ($\Leftrightarrow$):

(1) $v \in U, \quad \lambda \in \mathbb{R} \Rightarrow \lambda \cdot v \in U$

(2) $v, w \in U \Rightarrow v + w \in U$

(oder äquivalent: $\forall v, w \in U, \forall \lambda, \mu \in \mathbb{R}$ ist $\lambda \cdot v + \mu \cdot w \in U$)
Man sagt: U ist abgeschlossen bezüglich der Vektoraddition und der Multiplikation mit Skalaren.

Beweis

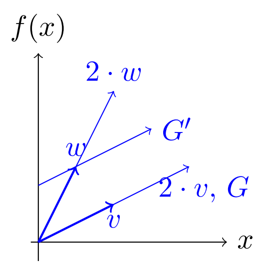
$\Rightarrow$ ist klar, da U laut Definition 1.4 selbst Vektorraum

$\Leftarrow$ rechne die Vektorraumaxiome nach (Definition 1.1, also z.B. $\mathcal{O} \in U$,...)

$\square$

1.7 Beispiel

a)
V ist ein $\mathbb{R}$-Vektorraum, $\mathcal{O} \neq v \in V$.
Dann ist $G = \{\lambda \cdot v | \lambda \in \mathbb{R}\}$ ein Unterraum.
$V = \mathbb{R}^2, \mathbb{R}^3$: G ist Gerade durch Nullpunkt (geometrisch), z.B.
$v = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, w = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$
Aber: $G' = \{w + \lambda \cdot v | \lambda \in \mathbb{R}, \quad w \in V\}$ ist kein Unterraum für $w \neq \mu \cdot v, \quad \mu \in \mathbb{R}$.
Warum? Z.B. $\mathcal{O} \notin G'$



b) $V = \mathbb{R}^3, \qquad U_1 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 | x_1 + x_2 - x_3 = 0 \right\}$ ist Unterraum. Wir zeigen (1), (2) aus 1.6:

– $U_1 \neq \emptyset$, z.B. $\mathcal{O} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \in U_1$, denn $\overset{x_1}{0} + \overset{x_2}{0} - \overset{x_3}{0} = 0$

(1) Sei $\lambda \in \mathbb{R}$, $\quad v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \in U_1$, d.h. $v_1 + v_2 - v_3 = 0$

Prüfe: Ist $\lambda \cdot v \in U_1$? $\lambda \cdot v = \begin{pmatrix} \lambda \cdot v_1 \\ \lambda \cdot v_2 \\ \lambda \cdot v_3 \end{pmatrix}$

$$\begin{aligned} \lambda \cdot v_1 + \lambda \cdot v_2 - \lambda \cdot v_3 &= \lambda(v_1 + v_2 - v_3) \\ &= \lambda \cdot 0 \\ &= 0 \end{aligned}$$

Also ist $\lambda \cdot v \in U_1$

(2) Seien $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$, $\quad w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \in U_1$, d.h. $v_1 + v_2 - v_3 = 0$, $\quad w_1 + w_2 - w_3 = 0$. Gilt $v + w \in U_1$? $v + w = \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \\ v_3 + w_3 \end{pmatrix}$

$$\begin{aligned} (v_1 + w_1) + (v_2 + w_2) - (v_3 + w_3) &= \underbrace{(v_1 + v_2 - v_3)}_{=0} + \underbrace{(w_1 + w_2 - w_3)}_{=0} \\ &= 0 \end{aligned}$$

Also $v + w \in U_1$

– Geometrische Interpretation:

$$\begin{aligned} U_1 &= \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_1 + x_2 \end{pmatrix} \middle| \; x_1, \quad x_2 \in \mathbb{R} \right\} \\ &= \left\{ x_1 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \middle| \; x_1, \quad x_2 \in \mathbb{R} \right\} \end{aligned}$$

D.h. U_1 ist die Ebene durch $O = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ mit den Richtungsvektoren $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$

c) $U_2 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 \;\middle|\; x_1 + x_2 - x_3 = 1 \right\}$ ist kein Unterraum. Z.B. $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} =$
$\mathcal{O} \notin U_2$: $0 + 0 - 0 = 0 \neq 1$.

Anderes Argument: Sei $\lambda \in \mathbb{R}$, $\quad x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in U_2$, d.h. $x_1 + x_2 - x_3 = 1$.

Gilt $\lambda \cdot x \in U_2$? $\lambda \cdot x = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \lambda x_3 \end{pmatrix}$

$$\begin{aligned} \lambda x_1 + \lambda x_2 - \lambda x_3 &= \lambda \underbrace{(x_1 + x_2 - x_3)}_{=1} \\ &= \underbrace{\lambda = 1}_{\text{nur für } \lambda=1} \end{aligned}$$

$\Rightarrow$ nicht erfüllt für $\lambda \neq 1$.
Geometrische Interpretation:

$$\begin{aligned} U_2 &= \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_1 + x_2 - 1 \end{pmatrix} \;\middle|\; x_1, \quad x_2 \in \mathbb{R} \right\} \\ &= \left\{ \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} + x_1 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \;\middle|\; x_1, \quad x_2 \in \mathbb{R} \right\} \end{aligned}$$

Ebene durch $\begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$ mit Richtungsvektoren $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$

d) $U_3 = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 \;\middle|\; x_1^2 + x_2^2 + x_3^2 \leq 1 \right\}$ ist kein Unterraum, z.B.

$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in U_3, \qquad 1^2 + 0^2 +^2 \leq 1 \quad \checkmark$, aber

$2 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \notin U_3$, denn $2^2 + 0^2 + 0^2 \not\leq 1$
Geometrische Interpretation:

U_3 ist eine Kugel um $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ mit Radius 1

e) $I \subseteq \mathbb{R}$ Intervall
Menge $C(I)$ (C: continuous, stetig) der stetigen Funktionen auf I ist Unterraum von $\mathcal{F}(I, \mathbb{R})$ (vgl. Beispiel 1.2d)).
Menge der diffbaren Funktionen auf I ist Unterraum von $C(I)$.

1.8 Satz

V ist ein $\mathbb{R}$.Vektorraum, U_1, U_2 sind Unterräume von V.

a) $U_1 \cap U_2 = \{u \in V | u \in U_1 \wedge u \in U_2\}$ ist Unterraum von V.

b) $U_1 + U_2 \coloneqq \{u_1 + u_2 | u_1 \in U_1 \wedge u_2 \in U_2\}$ <u>Summe</u> von U_1, U_2 ist Unterraum von V
(das ist nicht die Vereinigung $U_1 \cup U_2$!)

Beweis

Prüfe Unterraumkriterium 1.6

a) Übung: Prüfe $\mathcal{O} \in U_1 \cap U_2$? ✓, (1), (2)

b)
- $U_1 + U_2 \neq \emptyset$, denn $U_1 + U_2 \ni \mathcal{O} = \underbrace{\mathcal{O}}_{\in U_1} + \underbrace{\mathcal{O}}_{\in U_2}$
- Seien $v = u_1 + u_2, \quad u_1 \in U_1, \quad u_2 \in U_2$ und
$w = u_1' + u_2', \quad u_1' \in U_1, \quad u_2' \in U_2$,
also $v, w \in U_1 + U_2$ und $\lambda, \mu \in \mathbb{R}$.

$$\Rightarrow \qquad \begin{aligned} \lambda v + \mu v &= \lambda(u_1 + u_2) + \mu(u_1' + u_2') \\ &= \underbrace{\lambda u_1 + \mu u_1'}_{\in U_1} + \underbrace{\lambda u_2 + \mu u_2'}_{\in U_2} \qquad \in U_1 + U_2 \end{aligned}$$

1.9 Bemerkung

a) lässt sich für unendlich viele Unterräume ausweiten

b) lässt sich für endlich viele Unterräume ausweiten

- $U_1 \cup U_2$ ist im Allgemeinen <u>kein</u> Unterraum

1.10 Beispiel

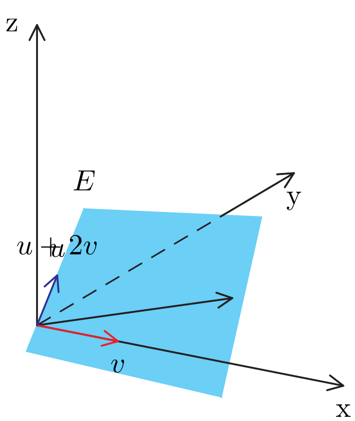
- $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{R}^2 \qquad G_1 = \{\lambda v | \lambda \in \mathbb{R}\}$
- $w = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \in \mathbb{R}^2 \qquad G_2 = \{\mu w | \mu \in \mathbb{R}\}$

(vgl. 1.7a), Geraden durch $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, Unterräume

- $G_1 + G_2$ ist Ebene
- $G_1 \cap G_2$ ist $\mathcal{O} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

1.11 Beispiel

18.10.16



- $u = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$
- $v = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$
- $E = \left\{ \lambda_1 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \middle| \lambda_1, \lambda_2 \in \mathbb{R} \right\}$

- E $\subseteq \mathbb{R}^3$ ist Untervektorraum (UVR) und wird <u>aufgespannt/erzeugt</u> von u und v. Man nennt $\left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \right\}$ <u>Erzeugendensystem</u> von E.
- D.h. $w \in E \Leftrightarrow \exists \lambda_1, \lambda_2 \in \mathbb{R} : w = \underbrace{\lambda_1 \cdot u + \lambda_2 \cdot v}_{\text{Linearkombination von } u \text{ und } v}$

- $w \notin E$, z.B. $w = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ ergibt:

  $$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \lambda_1 \cdot u + \lambda_2 \cdot v = \lambda_1 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$$

  $$\Rightarrow \left.\begin{array}{l} \text{Letzte Zeile: } 1 = \lambda_1 \\ \text{Zweite Zeile: } 0 = \lambda_1 \end{array}\right\} \lightning$$

  $$\Rightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \notin E$$

Fortsetzung Bsp. 1.11

(Nachtrag vom 19.10.2016)

a) $E = \left\langle \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \right\rangle_{\mathbb{R}}$

b) $\mathbb{R}^n$ wird erzeugt von $e_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, wobei j die Stelle ist, an der der Vektor 1 ist.

$$R^n = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, ..., \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\rangle_{\mathbb{R}} \text{ "kanonische Einheitsvektoren"}$$

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = v_1 \cdot e_1 + v_2 \cdot e_2 + ... + e_n \cdot v_n$$

c) Spannen $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ den $\mathbb{R}^2$ auf?

Wenn ja, dann muss für $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \qquad \alpha, \beta \in \mathbb{R}$ existieren mit

$$\begin{aligned}
& & \alpha \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \beta \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} &= \begin{pmatrix} x \\ y \end{pmatrix} \\
\Leftrightarrow & & \alpha + \beta &= x \\
& & \alpha + 2\beta &= y \\
\Rightarrow & & \alpha &= x - \beta \\
& & &= y - 2\beta \\
\Leftrightarrow & & \beta &= y - x \\
& & \alpha &= 2x - y
\end{aligned}$$

$\Rightarrow$ Allg. $\begin{pmatrix} x \\ y \end{pmatrix} = (2x - y) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + (y - x) \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} \Rightarrow \mathbb{R}^2 = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\rangle_{\mathbb{R}}$

d) Spannen $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ und $\begin{pmatrix} 3 \\ 6 \end{pmatrix}$ den $\mathbb{R}^2$ auf?

Nein, denn $\begin{pmatrix} 3 \\ 6 \end{pmatrix}$ ist $3 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} \Rightarrow \left\langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \end{pmatrix} \right\rangle_{\mathbb{R}} = \left\langle \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\rangle_{\mathbb{R}} = \left\{ \lambda \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} \,\middle|\, \lambda \in \mathbb{R} \right\} \subsetneq \mathbb{R}^2$

e) $\left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle_{\mathbb{R}} = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\rangle_{\mathbb{R}} = \mathbb{R}^2$, d.h. Erzeugendensysteme sind <u>nicht</u> eindeutig!

f) $\left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right\rangle_{\mathbb{R}} = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\rangle_{\mathbb{R}}$, da $\begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

D.h. $M = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right\}$ ist kein <u>minimales</u> Erzeugendensystem des $\mathbb{R}^2$, denn $v \in M$ kann immer dargestellt werden als Linearkombination von Vektoren aus $M \setminus v$.

Man sagt: $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ sind <u>linear abhängig</u>.

1.12 Definition (Linearkombination, Erzeugendensystem)

V : $\mathbb{R}$-VR (V ist Vektorraum in den reellen Zahlen)

(i) $v_1, ..., v_m \in V$ und $\lambda_1, ..., \lambda_m \in \mathbb{R}$
Der Vektor $\lambda_1 \cdot v_1 + ... + \lambda_m \cdot v_m$ heißt Linearkombination von $v_1, ..., v_m$.

(ii) Sei $M \subseteq V$. Dann ist

$$\langle M \rangle_{\mathbb{R}} = \left\{ \textstyle\sum_{k=1}^{n} \lambda_k \cdot v_k \;\middle|\; \lambda_k \in \mathbb{R}, v_k \in M, n \in \mathbb{N} \right\}$$

der von M aufgespannte/erzeugte UVR von V

Vereinbarung: $\langle \emptyset \rangle = \{0\}$
Schreibweise: $M = \{v_1, ..., v_m\}$
$\langle M \rangle_{\mathbb{R}} = \langle v_1, ..., v_m \rangle_{\mathbb{R}}$

(iii) Ist $V = \langle M \rangle_{\mathbb{R}}$, so heißt M ein Erzeugendensystem von V. V heißt endlich erzeugt, falls es ein endliches Erzeugendensystem gibt.

1.13 Bemerkung

$M \subseteq V \Rightarrow \langle M \rangle_{\mathbb{R}}$ ist der kleinste UVR von V, der M enthält.

Beweis

- $\langle M \rangle_{\mathbb{R}}$ ist UVR. erfüllt Kriterien von 1.6, daher klar:
  1.6 2) erfüllt. $u \in \langle M \rangle_{\mathbb{R}} \Rightarrow u = \lambda_1 \cdot v_1 + ... + \lambda_n \cdot v_n \quad (M = \{v_1, ..., v_n\})$
  $\Rightarrow \lambda \cdot u = \underbrace{\lambda\lambda_1}_{\in \mathbb{R}} \cdot v_1 + ... + \underbrace{\lambda\lambda_n}_{\in \mathbb{R}} \cdot v_n$
  1.6 3) ähnlich.

- Angenommen U ist der kleinste UVR, so dass $M \subseteq U$.
  Z. z.: $\langle M \rangle_{\mathbb{R}} = U$.
  Wegen 1.6 enthält U alle Linearkombinationen von Vektoren aus M.
  $\Rightarrow \langle M \rangle_{\mathbb{R}} \subseteq U \Rightarrow U$ kann nicht kleiner sein als $\langle M \rangle_{\mathbb{R}} \Rightarrow \langle M \rangle_{\mathbb{R}} = U$ $\square$

Ergänzung zu 1.13

19.10.16

Bsp: $M = \left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\} \Rightarrow \langle M \rangle_{\mathbb{R}} = \left\{ \lambda \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\}$ Gerade

- $\langle M \rangle_{\mathbb{R}} \supseteq M$

- $E = \left\{ \lambda_1 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \middle| \lambda_1, \lambda_2 \in \mathbb{R} \right\} \supseteq M$

$\langle M \rangle_{\mathbb{R}}$ Gerade, E Ebene, d.h. E ist größer als $\langle M \rangle_{\mathbb{R}}$
$\langle M \rangle_{\mathbb{R}}$ ist der kleinste UVR von $\mathbb{R}^3$, der M enthält.

1.14 Definition (Lineare Unabhängigkeit)

- $V: \quad \mathbb{R} - VR, \quad v_1, ..., v_n$ heißen <u>linear unabhängig</u>, wenn gilt:

$$\left.\begin{array}{l} \lambda_1 \cdot v_1 + ... + \lambda_m \cdot v_m = 0 \\ \lambda_1, ..., \lambda_m \in \mathbb{R} \end{array}\right\} \Rightarrow \underbrace{\lambda = \lambda_2 = ... = \lambda_m = 0}_{\text{einzige Lösung!}}$$

- $M \subseteq V$ heißt linear unabhängig, wenn gilt:
  Für beliebiges $m \in \mathbb{N}$ und $v_1, ..., v_m \in M$ paarweise verschieden sind $v_1, ..., v_m$ linear unabhängig

- Ist in obigen beiden Fällen (mindestens) $\lambda_i \neq 0$, dann sind die Vektoren linear abhängig

1.15 Beispiel

a) $\mathcal{O}$ ist linear abhängig, da $\lambda \cdot \mathcal{O} = 0 \qquad \forall \lambda \neq 0$

b) Sind $\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -5 \end{pmatrix}$ linear abhängig in $\mathbb{R}^2$?
$\lambda_1 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix} + \lambda_3 \cdot \begin{pmatrix} 1 \\ -5 \end{pmatrix} = \mathcal{O}$
$\begin{cases} \text{I} & \lambda_1 - 3\lambda_2 + \lambda_3 & = 0 \\ \text{II} & 2\lambda_1 + \lambda_2 - 5\lambda_3 & = 0 \end{cases}$ Erfüllt für $\lambda_1 = \lambda_2 = \lambda_3 = 0$. Aber hier gibt es noch die Lösung: $\lambda_1 = 2, \quad \lambda_2 = \lambda_3 = 1$!
$\Rightarrow$ Vektoren sind linear abhängig

c) $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ linear unabhängig (l.u.) in $\mathbb{R}^3$

d) $v \neq \mathcal{O}, \quad v \in V, \quad v$, ist linear unabhängig
Angenommen es existiert $\lambda \neq 0$ mit $\lambda \cdot v = 0$.
$\Rightarrow v = (\frac{1}{\lambda} \cdot \lambda) \cdot v = \frac{1}{\lambda} \cdot (\lambda \cdot v) = \mathcal{O}$ ↯

e)

$$\begin{aligned} v, w \text{ linear abhängig } &\Leftrightarrow v = \lambda w \text{ , für ein } \lambda \in \mathbb{R} \\ &\Leftrightarrow v \in \langle w \rangle_{\mathbb{R}} \end{aligned}$$

f) In $V = \mathcal{F}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} |\ \text{f Abbildung}\}$ sind die Vektoren

- $f(x) = x, \quad g(x) = x^2$ linear unabhängig
- $f(x) = \sin^2(x), \quad g(x) = \cos^2(x), \quad h(x) = 2$ linear abhängig:

$$\begin{aligned} 2 &= 2 \cdot (\sin^2 x + \cos^2 x) \\ &= 2 \sin^2 x + 2 \cos^2 x \\ 0 &= \underbrace{2}_{\lambda_1} \sin^2 x + \underbrace{2}_{\lambda_2} \cos^2 x \underbrace{-1}_{\lambda_3} \cdot 2 \end{aligned}$$

1.16 Satz

$M = \{v_1, ..., v_n\} \subseteq V$

(i) M linear unabhängig $\Leftrightarrow$ Zu jedem $v \in \langle M \rangle_{\mathbb{R}}$ gibt es eindeutig bestimmte $\lambda_1, ... \lambda_n \in \mathbb{R} : v = \sum_{i=1}^n \lambda_i \cdot v_i$

(ii) M linear unabhängig, $v \notin \langle M \rangle_{\mathbb{R}} \Rightarrow M \cup \{v\}$ linear unabhängig

Beweis

(i) ($\Leftarrow$) $\mathcal{O} \in \langle M \rangle_{\mathbb{R}} \Rightarrow \exists$ eindeutig bestimmte $\lambda_1, ..., \lambda_m \in \mathbb{R}$:
$$\mathcal{O} = \lambda_1 \cdot v_1 + ... + \lambda_n \cdot v_n$$
Gleichung erfüllt für $\lambda_1 = ... = \lambda_n = 0$ (eindeutige Lösung)

($\Rightarrow$) Sei M linear unabhängig, $v \in \langle M \rangle_{\mathbb{R}}$
Angenommen $v = \sum_{i=1}^n \lambda_i \cdot v_i = \sum_{i=1}^n \mu_i \cdot v_i$
$$\Leftrightarrow \sum_{i=1}^n \underbrace{(\lambda_i - \mu_i)}_{=0,\text{ da } M \text{ linear unabhängig}} \cdot v_i = \mathcal{O}$$
$$\Rightarrow \lambda_i = \mu_i \qquad \forall i = 1, ..., n$$

(ii) Z.z.: $\sum_{i=1}^n \lambda_i \cdot v_i + \lambda \cdot v = \mathcal{O} \Rightarrow \lambda_i = 0 \quad \forall i, \lambda = 0$
Annahme: $\lambda \neq 0 \Rightarrow v = \underbrace{-\frac{\lambda_1}{\lambda}}_{\in \mathbb{R}} \cdot v_1 - ... - \frac{\lambda_n}{\lambda} \cdot v_n$
$$\Rightarrow v \in \langle M \rangle_{\mathbb{R}} \lightning. \text{ Also } \lambda = 0$$
$\lambda_i = 0$, weil M linear unabhängig. $\square$

1.17 Satz

$M \subseteq V$ linear unabhängig genau dann, wenn gilt:

$$N \subseteq M, \quad \langle N\rangle_{\mathbb{R}} = \langle M\rangle_{\mathbb{R}} \Rightarrow N = M$$

In Worten: Man kann von M keinen Vektor weglassen, ohne dass der von M aufgespannte Raum sich verkleinert.

Beweis

($\Rightarrow$) Sei $M \subseteq V$ linear unabhängig.
Angenommen: Man kann doch aus M Vektoren weglassen, d.h.

$$N \subseteq M, \quad \langle N\rangle_{\mathbb{R}} = \langle M\rangle_{\mathbb{R}} \text{ und } N \neq M$$

$$\begin{aligned}
N \neq M &\Rightarrow \exists x \in M \setminus N && \text{(da } N \subseteq M\text{)} \\
&\Rightarrow \exists v_1, ..., v_n \in N && \text{paarweise verschieden und} \\
&\quad\ \exists \lambda_1, ..., \lambda_n \in \mathbb{R} && \text{so dass} \\
&\quad\ x = \lambda_1 v_1 + ... + \lambda_n v_n && \text{(da } \langle N\rangle_{\mathbb{R}} = \langle M\rangle_{\mathbb{R}}\text{)} \\
&\Rightarrow \lambda_1 v_1 + ... + \lambda_n v_n - x = \mathcal{O} \\
&\quad\ \underbrace{v_1, ..., v_n}_{\in N}, \quad \underbrace{x}_{\in M \setminus N} \ \text{paarweise verschieden}
\end{aligned}$$

Da $N \subseteq M$, ist $\underbrace{v_1, ..., v_n, x}_{\text{linear abhängig}} \in M \Rightarrow M$ linear abhängig↯
Also muss $N = M$ gelten.

($\Leftarrow$) Sei M linear abhängig.
Z.z. Man kann Vektoren aus M weglassen, d.h.:

$$\exists N \subseteq M, \quad \langle N\rangle_{\mathbb{R}} = \langle M\rangle_{\mathbb{R}} \text{ und } N \neq M$$

$$\begin{aligned}
M \text{ linear abhängig} \Rightarrow\ & \exists n \in \mathbb{N} \quad \exists v_1, ..., v_n \in M \\
& \exists \lambda_1, ..., \lambda_n \in \mathbb{R} \text{ (mit } \lambda_i \neq 0 \text{ für ein i)} \\
& \lambda_1 \cdot v_1 + ... + \lambda_n \cdot v_n = 0
\end{aligned}$$

O.B.d.A: $\lambda_1 \neq 0 \Rightarrow v_1 = -\frac{\lambda_2}{\lambda_1} \cdot v_2 - \frac{\lambda_3}{\lambda_1} \cdot v_3 - ... - \frac{\lambda_n}{\lambda_1} \cdot v_n$
Setze $N = M \setminus \{v_1\} \Rightarrow N \neq M$
Da v_1 Linearkombination von $v_2, ..., v_n$ folgt:
Jede Linearkombination von $v_1, ..., v_n$ lässt sich ausdrücken als Linearkombination von $v_2, ..., v_n \Rightarrow \langle N\rangle_{\mathbb{R}} = \langle M\rangle_{\mathbb{R}}$ □

Basis und Dimension

25.10.16

Ein minimales Erzeugendensystem heißt Basis.

1.18 Definition (Basis)

V endlich erzeugter $\mathbb{R}$-VR. Eine endliche Menge $B \subseteq V$ heißt Basis, falls

- $\langle B \rangle_{\mathbb{R}} = V$ und
- B linear unabhängig.

Für $V = \{\mathcal{O}\}$ ist $B = \emptyset$ die Basis.

1.19 Beispiel

a) $\{e_1, ..., e_n\}$ ist Basis von $\mathbb{R}^n$ ('Standard-/kanonische Basis')

b) Basis ist nicht eindeutig.

$$B_1 = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \qquad B_2 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\}$$

$$\Rightarrow \langle B_1 \rangle_{\mathbb{R}} = \langle B_2 \rangle_{\mathbb{R}}, \text{ da: } \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ und } \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \langle B_2 \rangle_{\mathbb{R}} \Rightarrow \mathbb{R}^2 = \langle B_1 \rangle_{\mathbb{R}} \subseteq \langle B_2 \rangle_{\mathbb{R}}$$

1.20 Satz (Existenz von Basen)

V endlich erzeugter $\mathbb{R}$-VR $\Rightarrow$ Jedes endliche Erzeugendensystem enthält Basis.

Beweis

Sei $M \subseteq V$ endlich, $\langle M \rangle_{\mathbb{R}} = V$

- M linear unabhängig $\rightarrow$ fertig
- M linear abhängig $\overset{1.17}{\Rightarrow}$ Man kann aus M einen Vektor $v \in M$ weglassen, so dass $\langle M \setminus \{v\} \rangle_{\mathbb{R}} = V = \langle M \rangle_{\mathbb{R}}$. Nach endlich vielen Schritten liefert das Verfahren eine Basis. $\square$

Fragen

- Basis nicht eindeutig. Sind alle Basen gleich groß?
- geg. $w = \begin{pmatrix} \frac{1}{3} \\ 0 \\ 1 \end{pmatrix} \in \mathbb{R}^3, \qquad S = \{e_1, e_2, e_3\}$. Wie kann man w zu einer Basis ergänzen? Welche Vektoren aus S sind geeignet?

$$w = \frac{1}{3}e_1 + e_3 = \{\underbrace{w, e_1, e_3}_{\text{linear abhängig}}\} \text{ keine Basis, aber}$$

$$\{\underbrace{w, e_1, e_2}_{\text{linear unabhängig}}\} \text{ Basis und } \{w, e_2, e_3\} \text{ Basis}$$

1.21 Satz (Austauschlemma)

V endlich erzeugter $\mathbb{R}$-VR. Gegeben: $w \in V, \quad w \neq \mathcal{O}, \quad w = \sum_{i=1}^n \lambda_i v_i$, wobei $B = \{v_1, ..., v_n\} \subseteq V$ Basis von V.
$\Rightarrow \underbrace{\big(B \setminus \{v_j\}\big) \cup \{w\}}_{(\star)}$ Basis, falls $\underbracket{\lambda_j \neq 0}$

Beweis

Z.z: $(\star)$ ist Basis.

1) $(\star)$ ist linear unabhängig.
   Z.z:

$$\sum_{i \neq j} \mu_i v_i + \mu w = 0 \Rightarrow \mu_i = 0 \text{ und } \mu = 0$$

$$\begin{aligned}
\sum_{i \neq j} \mu_i v_i + \mu w &= \sum_{i \neq j} \mu_i v_i + \mu\bigg(\sum_{i=1}^n \lambda_i v_i\bigg) \\
&= \sum_{i \neq j} (\mu_i + \mu\lambda_i) v_i + \mu\lambda_j v_j \\
&= 0
\end{aligned}$$

$$\begin{aligned}
B = \{v_1, ..., v_n\} \text{ Basis } &\Rightarrow \mu\lambda_j = 0 \text{ und } \mu_i + \mu\lambda_i = 0 \quad \forall i \neq j \\
\underbracket{\lambda_j \neq 0} &\Rightarrow \mu = 0 \Rightarrow \mu_i + \underbrace{\mu\lambda_i}_{=0} = \mu_i = 0 \quad \forall i \neq j
\end{aligned}$$

2) $(\star)$ erzeugt V.

$$\begin{aligned} && w = \lambda_j v_j + \sum_{i \neq j}^{\lambda_i v_i} && |: \lambda_j, \text{ da } \lambda_j \neq 0 \\ \Leftrightarrow && v_j = \frac{1}{\lambda_j} w - \sum_{i \neq j} \frac{\lambda_i}{\lambda_j} v_i \\ \Rightarrow && v_j \in \langle (B \setminus \{v_j\}) \cup \{w\} \rangle_{\mathbb{R}} \\ \Rightarrow && \langle (B \setminus \{v_j\}) \cup \{w\} \rangle_{\mathbb{R}} = \langle B \cup \{w\} \rangle_{\mathbb{R}} = V \end{aligned}$$

1.22 Satz (Steinitz'scher Austauschsatz)

Geg. $w_1, ..., w_m \in V$ linear unabhängig, $\{v_1, ..., v_n\}$ Basis von V.
Es folgt:

a) Aus den n Vektoren $v_1, ..., v_n$ kann man $n - m$ Vektoren auswählen, die mit $w_1, ..., w_m$ eine Basis bilden.

b) $m \leq n$

Beweis

a) 1) $w_1 \in V \Rightarrow w_1 = \sum_{i=1}^{n} \lambda_i v_i$
Wären alle $\lambda_i = 0$, dann wäre auch $w_1 = 0$. Da $\mathcal{O} \in V$ linear abhängig ist, wäre also auch $w_1, ..., w_m$ linear abhängig. E
Also: Mindestens ein $\lambda_i \neq 0$
O.B.d.A. $\lambda_1 \neq 0$ (sonst umnummerieren) $\overset{1.20}{\Rightarrow}$ $\{w_1, v_2, ..., v_n\}$ ist Basis von V

2) $w_2 \in V \Rightarrow \mu_1 w_1 + \sum_{i=2}^{n} \mu_i v_i$
Wären alle $\mu_2, ..., \mu_n = 0$, so wäre $w_2 = \mu_1 w_1$, also auch w_1, w_2 linear abhängig. E, da $\{w_1, ..., w_m\}$ linear unabhängig.
$\Rightarrow$ Mindestens ein $\mu_i \neq 0, \quad i \in \{2, ..., n\}$
O.B.d.A. $\mu_2 \neq 0 \overset{1.20}{\Rightarrow} \{w_1, w_2, v_3, ..., v_n\}$ Basis von V

□

b) $\rightarrow$ Übung

1.23 Korollar

V endlich erzeugter $\mathbb{R}$-VR

i) Je zwei Basen von V enthalten gleich viele Elemente.

ii) Basisergänzungssatz
Jede linear unabhängige Teilmenge von V lässt sich zu einer Basis von V ergänzen.

Beweis

i) $B, \tilde{B}$ Basen
B linear unabhängig $\overset{1.22b)}{\Rightarrow} |B| \leq |\tilde{B}|$
$\tilde{B}$ linear unabhängig $\overset{1.22b)}{\Rightarrow} |\tilde{B}| \leq |B|$
$\Rightarrow |B| = |\tilde{B}|$

ii) Wähle beliebige Basis von V und tausche aus(1.22a)).

1.24 Satz

V endlich erzeugter $\mathbb{R}$-VR, $B \subseteq V$.
Dann sind äquivalent:

i) B ist Basis

ii) B ist maximale linear unabhängige Menge in V

iii) B ist minimales Erzeugendensystem

Beweis

i)⇒ii) Wegen 1.23 (linear unabhängige Menge zu Basis ergänzen, alle Basen gleich groß)

ii)⇒i) (Bzw. ¬i)⇒ ¬ii).) B keine Basis, B linear unabhängig
$\Rightarrow \langle B \rangle_{\mathbb{R}} \subsetneq V \Rightarrow \exists v \in V \setminus \langle B \rangle_{\mathbb{R}} \colon B \cup \{v\}$ linear unabhängig

i)⇒iii) Satz 1.17

□

1.25 Definition (Dimension)

26.10.16

V : $\mathbb{R}$-VR

i) Ist V endlich erzeugbar, B Basis von V, $\quad |B| = n$ so hat V die Dimension n, $\dim(V) = n$

ii) Ist V nicht endlich erzeugbar, so heißt V unendlichdimensional.

1.26 Korollar

$\dim V = n, B \subseteq V, |B| = n$.
Dann ist B Basis von V, wenn B linear unabhängig oder $\langle B \rangle_{\mathbb{R}} = V$

Beweis

Folgt aus 1.24

1.27 Beispiel

a) $\{e_1, ..., e_n\}$ Basis von $\mathbb{R}^n \Rightarrow \dim(\mathbb{R}^n) = n$

b) $\langle \emptyset \rangle_{\mathbb{R}} = \{\mathcal{O}\} \Rightarrow dim(\{\mathcal{O}\}) = 0$

c) Bilden $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$ Basis von V?
Ja, weil linear unabhängig (siehe Korollar 1.26).

d) $V = \mathbb{R}^4, U = \left\langle u_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, u_2 = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} \right\rangle_{\mathbb{R}}$
u_1, u_2 linear unabhängig $\Rightarrow \dim(U) = 2$
Ergänze u_1, u_2 zu Basis von $V = \mathbb{R}^4$

- 1. Möglichkeit (Austauschlemma + Steinitz)
  $\{e_1, e_2, e_3, e_4\}$ Basis von $\mathbb{R}^4$
  $u_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} = e_1 + 2e_2 + e_4 \Rightarrow \{u_1, e_2, e_3, e_4\}$ Basis von $\mathbb{R}^4$

$$u_2 = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} = 2e_2 + e_3 \Rightarrow \{u_1, u_2, e_3, e_4\} \text{ Basis von } \mathbb{R}^4$$

(Basis könnte auch anders aussehen, nur beispielhaft dargestellt)

- 2. Möglichkeit (1.16)

  * $e_1 \notin U$ ($\star$)(nachrechnen)
    $\overset{1.16}{\Rightarrow} \{u_1, u_2, e_1\}$ linear unabhängig
  * $e_4 \notin \langle\{u_1, u_2, e_1\}\rangle_{\mathbb{R}}$ (nachrechnen)
    $\overset{1.16}{\Rightarrow} \{u_1, u_2, e_1, e_4\}$ linear unabhängig und damit Basis (Korollar 1.26)

  ($\star$) Angenommen:

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \lambda_1 \cdot u_1 + \lambda_2 \cdot u_2$$

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} I & 1 = \lambda_1 \\ II & 0 = 2\lambda_1 + 2\lambda_2 \\ III & 0 = \lambda_2 \\ IV & 0 = \lambda_1 \quad ⚡ \text{ zu I} \end{cases}$$

$$\Rightarrow e_1 \notin \langle\{u_1, u_2\}\rangle_{\mathbb{R}} \Rightarrow \{u_1, u_2, e_1\} \text{ linear unabhängig}$$

1.28 Satz (Dimensionssatz)

V $\mathbb{R}$-VR, $\dim(V) = n$

i) $U \subseteq V$ ist UVR $\Rightarrow \dim(U) \leq n$

ii) $U \subseteq W \subseteq V, \qquad U, W$ sind UVR mit $\dim(U) = \dim(W) \Rightarrow U = W$

iii) $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$

Beweis

i) Basis von U kann man zu Basis von V ergänzen $\Rightarrow \dim(U) \leq \dim(V)$

ii) $\dim(U) = \dim(W) \overset{U \subseteq W}{\Rightarrow}$ Basis von U auch Basis von $W \Rightarrow U = W$

iii) Sei $\{v_1, ..., v_k\}$ Basis von $U \cap W$
Ergänze $\{v_1, ..., v_k\}$ zu

a) Basis $\{v_1, ..., v_k, u_{k+1}, ..., u_m\}$ von U

b) Basis $\{v_1, ..., v_k, w_{k+1}, ..., w_l\}$ Basis von W

<u>Behauptung:</u> $B = \{v_1, ..., v_k, w_{k+1}, ..., w_l, u_{k+1}, ..., u_m\}$ Basis von $U + W$

1) B linear unabhängig
Sei
$$\overbrace{\lambda_1 v_1 + ... + \lambda_k v_k}^{=v} + \overbrace{\mu_{k+1} u_{k+1} + ... + \mu_m u_m}^{=u} + \overbrace{\gamma_{k+1} w_{k+1} + ... + \gamma_l w_l}^{=w} = 0$$
$\lambda_i, \mu_j, \gamma_r \in \mathbb{R}$

Es ist $w \in U \cap W$, da

* $w = \underbrace{\gamma_{k+1} w_{k+1}}_{\in W} + ... + \underbrace{\gamma_l w_l}_{\in W} \in W$
* $w = -\underbrace{u}_{\in U} - \underbrace{v}_{\in U} \in U$

Also: $w \in U \cap W$.

$\Rightarrow \exists \alpha_1, ..., \alpha_k \in \mathbb{R} : w = \alpha_1 v_1 + ... + \alpha_k v_k$
$\Rightarrow w = \gamma_{k+1} w_{k+1} + ... + \gamma_l w_l = \alpha_1 v_1 + ... + \alpha_k v_k$
$\Rightarrow \gamma_{k+1} w_{k+1} + ... + \gamma_l w_l - \alpha_1 v_1 - ... - \alpha_k v_k = 0$
$\{v_1, ..., v_k, w_{k+1}, ..., w_l\}$ linear unabhängig
$\Rightarrow \gamma_{k+1} = ... = \gamma_l = \alpha_1 = ... = \alpha_k = 0$
$\Rightarrow w = \mathcal{O}$ und $v + u + w = v + u = \lambda_1 v_1 + ... + \lambda_k v_k + \mu_{k+1} u_{k+1} + ... + \mu_m u_m = 0$
$\{v_1, ..., v_k, u_{k+1}, ..., u_m\}$ linear unabhängig (Basis von U)
$\Rightarrow \lambda_1 = ... = \lambda_k = \mu_{k+1} = ... = \mu_m = 0$

2) $\langle B \rangle_{\mathbb{R}} = U + W$, da:

* $\langle B \rangle_{\mathbb{R}} \subseteq U + W$ (da $\underbrace{u + v}_{\in U} + \underbrace{w}_{\in W} \in U + W$)

- $U \subseteq \langle B \rangle_{\mathbb{R}}$ (da Basis von U in B)

- $W \subseteq \langle B \rangle_{\mathbb{R}}$

$\Rightarrow U + W \subseteq \langle B \rangle_{\mathbb{R}}$

$\square$

1.29 Bemerkung (Koordinaten)

Geg.: Basis $\{v_1, ..., v_n\}$ von V, Vektor $u \in V$
$\Rightarrow u = \lambda_1 v_1 + ... + \lambda_n v_n$
λ_i eindeutig und heißen Koordinaten von u bezüglich der Basis B.
z.B.: $\begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 3 \begin{pmatrix} \frac{1}{3} \\ 0 \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}$ hat Koordinaten 1,1,3 bezüglich
$B = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{3} \\ 0 \\ 1 \end{pmatrix} \right\}$

2 Matrizen und lineare Gleichungssysteme

02.11.16

2.1 Beispiel

- Ein Bauer besitzt Kühe und Gänse
- Insgesamt 18 Tiere mit 40 Beinen
- Frage: Wieviele der Tiere sind Kühe?

<u>Lineares Gleichungssystem (LGS):</u> $* \begin{cases} I: & k+g &= 18 \\ II: & 4k+2g &= 40 \quad \Leftrightarrow \quad 2k+g=20 \end{cases}$

$$\Rightarrow g = 20 - 2k = 18 - k \Leftrightarrow k = 2 \Rightarrow g = 16$$

<u>Vektorenschreibweise von $*$:</u>

$$\begin{pmatrix} k+g \\ 4k+2g \end{pmatrix} = \begin{pmatrix} 18 \\ 40 \end{pmatrix} \text{ oder } k \begin{pmatrix} 1 \\ 4 \end{pmatrix} + g \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 18 \\ 40 \end{pmatrix}$$

<u>Matrixschreibweise:</u>

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 4 & 2 \end{pmatrix}}_{\text{Matrix}} \cdot \begin{pmatrix} k \\ g \end{pmatrix} = \begin{pmatrix} 18 \\ 40 \end{pmatrix}$$

2.2 Definition (Matrix)

Allgemeines lineares Gleichungssystem:
Gegeben:

- Unbekannte $x_1, ..., x_n \in \mathbb{R}, n \in \mathbb{N}$
- $m \in \mathbb{N}$ Gleichungen
- Koeffizienten $a_{ij} \in \mathbb{R}, i = 1, ..., m; j = 1, ..., n$

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n = b_2 \\ \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n = b_m \end{array}$$

Matrixschreibweise:
$Ax = b$ mit

- $A = \begin{array}{c} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \leftarrow \text{Zeile} \\ \quad\uparrow \\ \quad\text{Spalte} \end{array}$

- $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$

- $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{R}^m$

Man schreibt $A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$ oder nur $A = (a_{ij})$, wenn m, n schon bekannt.

- $a_{ij} \in \mathbb{R}$ - Eingänge der Matrix A
- A - reelle $m \times n$- Matrix
- $\mathcal{M}_{m,n}(\mathbb{R})$ - Menge aller reellen $m \times n$ - Matrizen
- $\mathcal{M}_{n,n}(\mathbb{R}) = M_n(\mathbb{R})$ - quadratische Matrizen

$(**)$ Dabei ist
$Ax \coloneqq x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + x_2 \begin{pmatrix} a_{12} \\ \vdots \\ a_{m2} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1m} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \\ \vdots \quad + \quad \vdots \quad + \quad \vdots \quad + \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n \end{pmatrix} \in \mathbb{R}^m$

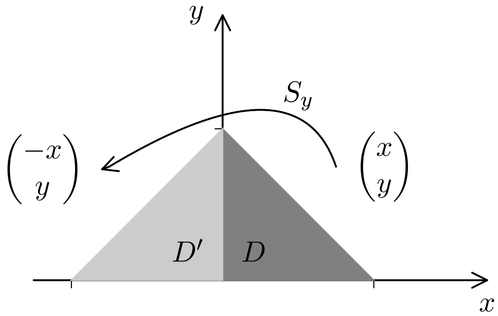
2.3 Bemerkung

Aus $(**)$ ergibt sich: $A : \mathbb{R}^n \to \mathbb{R}^m, x \longmapsto A \cdot x$ für $A \in \mathcal{M}_{m,n}(\mathbb{R})$
A bildet Vektoren auf Vektoren ab.

Matrizen können nicht nur zur Lösung von LGS verwendet werden, sondern auch in der Geometrie:

2.4 Beispiel:

a) Spiegelung S_y ain $\mathbb{R}^2$ an y-Achse



$S_y : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -x \\ y \end{pmatrix} \quad x, y \in \mathbb{R}$

$S_y : \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$

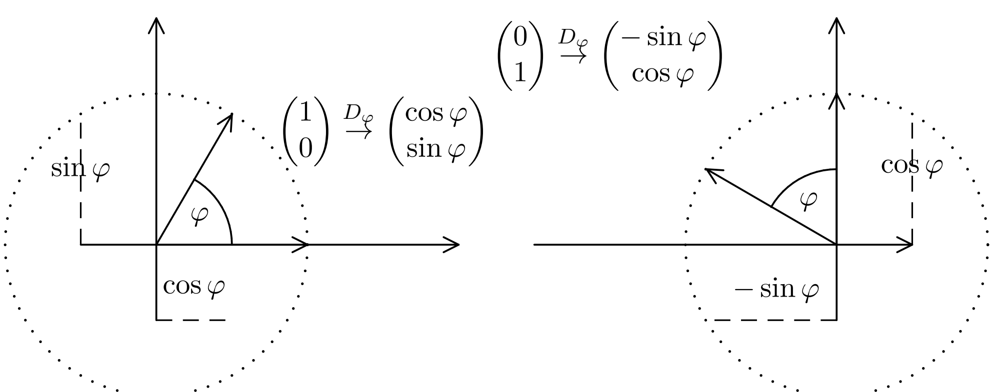
$S_y \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} s_{11} + s_{12} \\ s_{21} + s_{22} \end{pmatrix} = \begin{pmatrix} -x \\ y \end{pmatrix}$

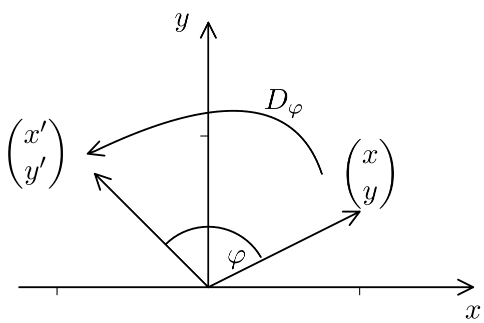
$\Rightarrow s_{11} = -1 \quad s_{12} = 0 \quad s_{21} = 0 \quad s_{22} = 1$

$S_y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

S_y bildet D auf D' ab.

b) Drehung D_φ um $\varphi \in [0, 2\pi)$
Vorüberlegung am Einheitskreis:





$D_\varphi : \begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} x' \\ y' \end{pmatrix}$
$D_\varphi = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}$
$\Rightarrow D_\varphi \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} d_{11} \\ d_{21} \end{pmatrix} = \begin{pmatrix} \cos\varphi \\ \sin\varphi \end{pmatrix}$ und
$D_\varphi \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} d_{12} \\ d_{22} \end{pmatrix} = \begin{pmatrix} -\sin\varphi \\ \cos\varphi \end{pmatrix}$
$\Rightarrow D_\varphi = (D_\varphi \cdot e_1, D_\varphi \cdot e_2) = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$

2.5 Bemerkung

Aus Beispiel 2.4 b) und Definition 2.2 ergibt sich:

$A \cdot e_j = 1 \cdot \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \qquad$ (j-te Spalte von $A \in \mathcal{M}_{m,n}(\mathbb{R})$)

$\Rightarrow A = (\underbrace{A_{e_1}, A_{e_2}, ..., A_{e_n}}_{\text{Spalten}})$

2.6 Satz

$A \in \mathcal{M}_{m,n}(\mathbb{R}) \qquad x, y \in \mathbb{R}^n$

i) $A(\lambda x) = \lambda(A \cdot x) \qquad \lambda \in \mathbb{R}$

ii) $A(x+y) = Ax + Ay$

Beweis

i)

$$\begin{aligned} A(\lambda x) &= (\lambda x_1) \underbrace{A \cdot e_1}_{\text{1. Spalte}} + (\lambda x_2) A e_2 + ... + (\lambda x_n) \underbrace{Ae_n}_{n\text{-te Spalte}} \\ &= \lambda[x_1(Ae_1) + ... + x_n(Ae_n)] \\ &= \lambda(Ax) \end{aligned}$$

ii) Übung

2.7 Beispiel (Folien 02.11.2016)

a) $A \cdot x = (D_\pi \circ S_y) \cdot x = D_\pi \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ -x_2 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \overset{A}{\mapsto} \begin{pmatrix} x_1 \\ -x_2 \end{pmatrix} \qquad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

b) Berechnung Matrixprodukt (Verknüpfung) $A \cdot B$

$$\begin{aligned}
\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} e & f \\ g & h \end{pmatrix}}_{B} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big[\underbrace{x_1 \begin{pmatrix} e \\ g \end{pmatrix} + x_2 \begin{pmatrix} f \\ h \end{pmatrix}}_{\in \mathbb{R}^2} \Big] \\
&\overset{2.6}{=} \quad x_1 \Big[\underbrace{e \begin{pmatrix} a \\ c \end{pmatrix} + g \begin{pmatrix} b \\ d \end{pmatrix}}_{\in \mathbb{R}^2} \Big] + x_2 \Big[\underbrace{f \begin{pmatrix} a \\ c \end{pmatrix} + h \begin{pmatrix} b \\ d \end{pmatrix}}_{\in \mathbb{R}^2} \Big] \\
&= \underbrace{\begin{pmatrix} ea + gb & fa + hb \\ ec + gd & fc + hd \end{pmatrix}}_{\text{Matrixprodukt } A \cdot B} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}
\end{aligned}$$

2.8 Definition (Matrixprodukt)

$A = (a_{ij}) \in \mathcal{M}_{m,n}(\mathbb{R}) \qquad B = (b_{ij}) \in \mathcal{M}_{m,n}(\mathbb{R})$

$$\begin{aligned}
A \cdot B &= (c_{ik}) \quad \in \mathcal{M}_{m,l}(\mathbb{R}) \\
c_{ik} &= (i\text{-te Zeile von } A) \cdot (k\text{-te Spalte von } B) \\
&= a_{i1} b_{1k} + a_{i2} b_{2k} + \cdots + a_{in} b_{nk} \\
&= \sum_{j=1}^{n} a_{ij} b_{jk}
\end{aligned}$$

(Skalarprodukt)

2.9 Beispiel

08.11.16

$A = \begin{pmatrix} \underline{1} & \underline{0} & \underline{-1} \\ 2 & -3 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & \underline{2} & -1 \\ 0 & \underline{0} & 0 \\ 0 & \underline{1} & 0 \end{pmatrix}, \qquad A \cdot B = \begin{pmatrix} 1 & \underline{1} & -1 \\ 2 & 3 & -2 \end{pmatrix}$

$B \cdot A$ nicht definiert!

2.10 Satz + Definition

$\mathcal{M}_{m,n}(\mathbb{R})$ ist Vektorraum mit

- $A + B = (a_{ij} + b_{ij}) \qquad A, B \in \mathcal{M}_{m,n}(\mathbb{R})$
- $\lambda \cdot A = (\lambda a_{ij}) \qquad A \in \mathcal{M}_{m,n}(\mathbb{R}), \lambda \in \mathbb{R}$

Beweis: Siehe Hausaufgabe 03 Aufgabe 4a)

2.11 Beispiel

$A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 0 & 2 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & -3 \\ 1 & 0 & 1 \end{pmatrix}$

$A + B = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \qquad (-2) \cdot A = \begin{pmatrix} -2 & -4 & -6 \\ 2 & 0 & -4 \end{pmatrix}$

2.12 Definition (Matrizentransponierung)

i) $A \in \mathcal{M}_{m,n}(\mathbb{R}), \quad A = (a_{ij})$.
Die zu A transponierte Matrix (Tauschen von Zeilen und Spalten):

$$A^T = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix} \in \mathcal{M}_{m,n}(\mathbb{R})$$

z.B.: $A = \begin{pmatrix} 1 & 2 & 0 \\ -1 & 1 & 2 \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} 1 & -1 \\ 2 & 1 \\ 0 & 2 \end{pmatrix}$

Eine Matix heißt symmetrisch, wenn $A = A^T$, z.B.:

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 3 & 4 \\ 0 & 4 & -1 \end{pmatrix}$$

ii)
- Nullmatrix: $\mathcal{O}_{m,n} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in \mathcal{M}_{m,n}(\mathbb{R})$
- Einheitsmatrix (nur Hauptdiagonale): $E_n = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$

2.13 Beispiel

a) $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 0 \\ 3 & 0 \end{pmatrix}$

$A \cdot B = \begin{pmatrix} 5 & 0 \\ 5 & 0 \end{pmatrix} \neq B \cdot A = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix}$ Matrixmultiplikation nicht kommutativ!

b) $A \in \mathcal{M}_{m,n}(\mathbb{R})$
$A \cdot E_n = A$ und $E_m \cdot A = A$

3 Gruppen

3.1 Beispiel (Wiederholung zu Permutationen)

Geg.: Menge $\{A, B, C\}$
Anordnungen: ABC, CAB, ACB, ... $\to 3 \cdot 2 \cdot 1 = 3!$ Möglichkeiten
Jede Anordnung kann man auffassen als eineindeutige (bijektive) Abbildung
$\pi : \{A, B, C\} \to \{A, B, C\}$

π :

x	A	B	C
$\pi(x)$	A	C	B

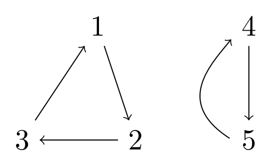
3.2 Definition (Permutation)

- Eine Permutation ist eine eineindeutige Abbildung einer endlichen Menge auf sich selbst. Im Allgemeinen verwendet man die Menge $\{1, ..., n\}$ und schreibt eine Permutation π als Wertetabelle $\pi = \begin{pmatrix} 1 & ... & n \\ \pi(1) & ... & \pi(n) \end{pmatrix}$ oder als geordnete Liste der Werte $\pi = \pi(1)...\pi(n)$
- $\mathscr{S}_n$- Menge aller Permutationen von $\{1, ..., n\}$, $\quad |\mathscr{S}_n| = n!$

Beispiel: $\mathscr{S}_2 = \{\mathrm{id}, (AB)\} = \{\mathrm{id}, (12)\}, \quad |\mathscr{S}_2| = 2! = 2$
mit $\mathrm{id} = \begin{pmatrix} AB \\ AB \end{pmatrix}, \qquad \pi = \begin{pmatrix} AB \\ BA \end{pmatrix}$

3.3 Beispiel

- $M = \{1, 2, ..., 5\}$
  $\pi = \pi(1)...\pi(5) = 23154$
  oder $\pi = \begin{pmatrix} 12345 \\ 23154 \end{pmatrix}$
- $\mathrm{id(i)} = i \qquad \forall i \in \{1, .., n\}$



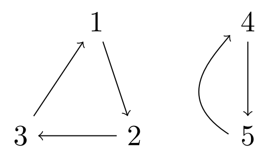
Graph der Permutation

3.4 Bemerkung

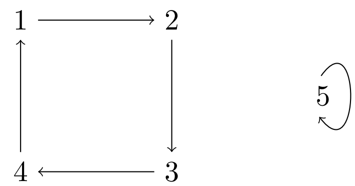
In Literatur oft Zyklenschreibweise:
Zyklus $(a_1 a_2 ... a_k)$ bedeutet $\pi(a_i) = a_{i+1}$ und $\pi(a_k) = a_1$
z.B.: $\pi = (123)(45)$

Verknüpfung von Permutationen

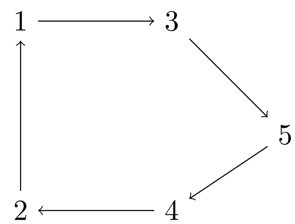
3.5 Beispiel



$$\pi = \begin{pmatrix} 12345 \\ 23154 \end{pmatrix} = (123)(45)$$



$$\sigma = \begin{pmatrix} 12345 \\ 23415 \end{pmatrix} = (1234)(5)$$



$$\pi\sigma = \begin{pmatrix} 12345 \\ 31524 \end{pmatrix} = (13542)$$

3.6 Bemerkung

a) Die Verknüpfung von 2 Permutationen π, σ ist wieder Permutation η mit $\eta(i) = \pi \circ \sigma(i) = \pi(\sigma(i))$

b) Fixpunkte mit $\pi(i) = i$ lässt man weg, z.B. $\underbrace{(123)(4)}_{\in \mathscr{S}_4} = (123)$

c) Jede Permutation kann als Produkt disjunkter Zyklen geschrieben werden, z.B.: $(34) \underset{\text{Verkettung } \circ}{\cdot} (345) = (3)(45) = (45)$.
Zwei Zyklen heißen <u>disjunkt</u>, wenn $\{a_1 ... a_k\} \cap \{b_1 ... b_j\} = \emptyset$.

d) Permutationen sind nur in sehr seltenen Fällen kommutativ:
$(123)(23) = (12) \neq (23)(123) = (13)$

e) Zyklendarstellung nicht eindeutig, z.B.:
$(123) = (231)$ oder $(34)(12) = (12)(34)$

3.7 Beispiel

09.11.16

Symmetrie-operationen des Rechtecks	Identität	Spiegelung y-Achse	Spiegelung x-Achse	Drehung 180°
	$\begin{array}{\|cc\|}\hline D & C \\ A & B \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline C & D \\ B & A \\ \hline\end{array}$	$\begin{array}{\|cc\|}\hline A & B \\ \hline D & C \\ \hline\end{array}$	$\begin{array}{\|cc\|}\hline B & A \\ C & D \\ \hline\end{array}$
als Matrix	$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$S_y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$S_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$D_\pi = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
als Permutation der Ecken	id	$\pi = (AB)(CD)$	$\sigma = (AD)(BC)$	$\eta = (AC)(BD)$

Verknüpfungstafel

$\underset{\cdot}{Matrixmultiplikation}$	E_2	S_y	S_x	D_π
E_2	E_2	S_y	S_x	D_π
S_y	S_y	E_2	D_π	S_x
S_x	S_x	D_π	E_2	S_y
D_π	D_π	S_x	S_y	E_2

3.8 Definition (Grundbegriffe)

- Seien X, Y nichtleere Mengen, Eine Verknüpfung ' $\cdot$ ' ist eine Abbildung

$$X \times X \to Y \qquad (a, b) \to a \cdot b \qquad (\leftarrow \text{'Produkt' von a und b})$$

- Eine Menge $X \neq \emptyset$ heißt <u>abgeschlossen</u> bzgl. einer Verknüpfung ' $\cdot$ ', falls $a \cdot b \in X \qquad \forall a, b \in X$.
  Beispiel: $X = \{-1, 1\}$ mit '$\cdot$' Addition $\Rightarrow (-1) \cdot (1) = -1 + 1 = 0$

Die Menge $\{id, \pi, \sigma, \eta\}$ aus Beispiel 3.7 ist abgeschlossen bzgl. der Verkettung von Permutationen

Bemerkung

Die Verknüpfung von Elementen einer endlichen Menge stellt man anhand der Verknüpfungstafel dar, siehe Beispiel 3.7.

3.9 Definition (Gruppe)

a) Eine Gruppe ist ein Paar $(G, \cdot)$ mit Menge $G \neq \emptyset$ und einer Verknüpfung $\cdot : \underbrace{G \times G \to G}_{\text{abgeschlossen!}}$, die folgende Eigenschaften erfüllt:

   1) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$ Assoziativität
   2) $\exists e \in G : a \cdot e = e \cdot a = a \quad \forall a \in G$ Neutralelement
   3) $\forall a \in G \quad \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$ Inverse

   Falls zusätzlich

   4) $a \cdot b = b \cdot a \quad \forall a, b \in G$ Kommutativität

   gilt, dann heißt G abelsche Gruppe.

b) $|G|$ heißt Ordnung der Gruppe G.

3.10 Beispiel

a) $(\{e\}, \cdot)$ ist Gruppe

b) $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ mit ' $+$ ' ist abelsche Gruppe. Inverse zu a ist -a.

c) $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ mit ' $\cdot$ ' keine Gruppen. Problem: 0 besitz keine Inverse, weil $0 \cdot a = 1$ ↯

$\Rightarrow$ $\mathbb{R}, \mathbb{Q}$ mit ' $\cdot$ ' Gruppen, wenn man 0 weglässt

d) Einzige endliche Gruppen von reellen Zahlen:

   - $(\{1\}, \cdot)$ bzw. $(\{0\}, +)$
   - $(\{1, -1\}, \cdot)$

   Für weitere endliche Gruppen muss man Restklassen (Beispiel 3.12) Matrizen oder Permutationen betrachten

e) $\mathscr{S}_2 = \{\mathrm{id}, (12)\}$ und
   $\mathscr{S}_3 = \{\mathrm{id}, (12), (23), (13), (123), (132)\}$ sind Gruppen (s. 3.11)

f) $V_4 = \{\mathrm{id}, \pi, \sigma, \eta\}$ aus Beispiel 3.7 ist die Symmetriegruppe des Rechtecks und heißt 'Kleinsche Vierergruppe' (V_4 Gruppe: s. 3.16 e).

3.11 Satz

$\mathscr{S}_n$ ist eine <u>nicht</u> abelsche Gruppe. (Name: Symmetrische Gruppe)

Beweis

- assoziativ: $\pi, \sigma, \eta \in \mathscr{S}_n \Rightarrow \underbrace{(\pi \cdot \sigma) \cdot \eta}_{\text{Verknüpfung von Abbildungen}} = \overset{\text{bijektive Abbildungen}}{\pi \overset{\uparrow}{\cdot} (\sigma \overset{\uparrow}{\cdot} \eta)}$

- Neutralelement: id, denn
  $\mathrm{id} \cdot \pi = \pi \cdot \mathrm{id} = \pi \qquad \forall \pi \in \mathscr{S}_n$

- Inverse: Alle Pfeile eines Zyklus werden umgedreht, d.h. die Zyklen werden rückwärts gelesen:

$$\begin{tikzcd}
 & 1 \arrow[dr] & & & & 1 \arrow[dl] & \\
3 \arrow[ur] & & 2 \arrow[ll] & \longrightarrow & 3 \arrow[rr] & & 2 \arrow[ul]
\end{tikzcd}$$

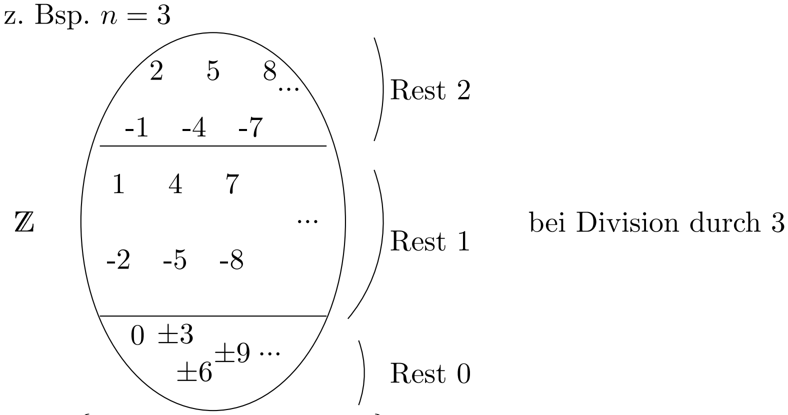
  $\pi = (123)$ $\qquad$ $\pi^{-1} = (132)$
  Fixpunkte und 2er-Zyklen ändern sich dabei nicht:
  $\sigma = (1678)(23) \Rightarrow \sigma^{-1} = (1876)(23)$
  Setzt man die Pfeile von den Graphen π und π^{-1} zusammen, ändert sich nichts, d.h. $\pi \cdot \pi^{-1}(i) = i \Rightarrow \pi \cdot \pi^{-1} = \mathrm{id} = \pi \cdot \pi^{-1}$

- nicht abelsch: Bemerkung 3.6d)

3.12 Beispiel

Restklassen modulo $n : \mathbb{Z}_n = \{0, 1, ..., n-1\}$,

z. Bsp. $n = 3$



$\mathbb{Z}_3 = \{ \underbrace{0, \quad 1, \quad 2}_{\text{Restklassen, Repräsentanten}} \}$

a) $(\mathbb{Z}_n, \oplus)$ mit $a \oplus b = a + b \mod n$. Z.B. in $\mathbb{Z}_3$ ist $2 \oplus 1 = 0$

<u>$(\mathbb{Z}_n, \oplus)$ ist abelsche Gruppe:</u>

- abgeschlossen: $a + b \mod n \in \{0, ..., n-1\}$
- assoziativ: $a + (b + c) \mod n = (a + b) + c \mod n$
- Neutralelement: $a + 0 \equiv 0 + a \equiv a \pmod{n}$
- Inverse zu $a \in \mathbb{Z}_n$: Für welches $b \in \mathbb{Z}_n$ ist $a + b \mod n = 0$?
  Wähle b so, dass $a + b = n$, falls $a \neq 0$ (sonst b = 0)
  z.B. in $\mathbb{Z}_3 : a = 1 \Rightarrow b = 2, \quad a = 2 \Rightarrow b = 1, \quad a = 0, b = 0$
- kommutativ: $a + b \mod n = b + a \mod n$

b) $(\mathbb{Z}_n, \odot)$ mit $a \odot b = ab \mod n$
Ist i.A. keine Gruppe:

- assoziativ ✓
- Neutralelement: $e = 1$ ✓

– Aber: 0 hat keine Inverse! Es gibt kein $a \in \mathbb{Z}_n$: $\underbrace{0 \cdot a \mod n}_{0} = 1$ ($\lightning$)

Hat $z \neq 0$ eine Inverse bzgl. $\odot$?

$\bar{z}$ invers zu z, wenn $\bar{z} \cdot z \equiv 1 \pmod n$
z.B. in $\mathbb{Z}_{15}$ gilt:

* $2 \cdot 8 = \quad 16 \equiv 1 \pmod{15}$, d.h. 2 und 8 sind zueinander invers
* Alle Vielfachen von 5 haben Rest $0, 5, 10$, d.h.
$k \cdot 5 \mod 15 \in \{0, 5, 10\} \quad \forall k \in \mathbb{Z} \Rightarrow 5$ hat kein Inverses

Allgemein:

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

Beweis von *

'$\Leftarrow$' Lemma von Bézout/Erweiterter Euklidischer Algorithmus (EEA):
$a, b \in \mathbb{Z} \Rightarrow \exists s, t \in \mathbb{Z} : \text{ggT}(a, b) = s \cdot a + t \cdot b$
Hier: $a = z, \quad b = n, \quad s = \bar{z}, \quad t = -q$

'$\Rightarrow$' Übung (Übungsblatt 5, A1c)

Also: Nur die zu n teilerfremden Zahlen in $\mathbb{Z}_n$ haben Inverse. Z.B.: In $\mathbb{Z}_{15}$ sind $1, 2, 4, 7, 8, 11, 13, 14$ bzgl. $\odot$ invertierbar.
Bezeichnung: $\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n \mid \text{ggT}(z, n) = 1\}$ ist Gruppe mit Ordnung $|\mathbb{Z}_n^*| = \varphi(n)$ (Eulersche φ–Funktion, $\varphi(n)$ ist Anzahl der zu n teilerfremden Zahlen zwischen 1 und n).

Berechnung der Inversen in $\mathbb{Z}_n^*$:

$$\begin{aligned}
\text{EEA :} \qquad z \in \mathbb{Z}_n^* &\Rightarrow \exists s, t \in \mathbb{Z} : sz + tn = 1 \\
&\Rightarrow s \cdot z \equiv 1 \pmod n \\
&\Rightarrow s \text{ invers zu } z
\end{aligned}$$

3.13 Satz (Eigenschaften von Gruppen)

G Gruppe.

i) Das Neutralelement von G ist eindeutig.

ii) Die Inverse zu jedem $a \in G$ ist eindeutig.

iii) $a, b \in G \Rightarrow (ab)^{-1} = b^{-1} \cdot a^{-1}$

Beweis

i) Angenommen e_1, e_2 Neutralelemente
$\Rightarrow e_1 = e_1 \cdot e_2 = e_2$

ii) Angenommen $a \in G$ hat 2 Inversen x, y
$x, y \in G \Rightarrow x = x \underbrace{(ay)}_{e} = \underbrace{(xa)}_{e} y = y$

iii)
* $(ab)^{-1} \cdot (ab) \underset{\text{Vor.}}{=} (b^{-1}a^{-1})(ab) = b^{-1} \underbrace{(a^{-1}a)}_{e} b = \underbrace{b^{-1}b}_{e} = e$
* $(ab)(ab)^{-1}$ analog

$\square$

3.14 Satz (Gleichungen lösen in Gruppen)

G Gruppe, $a, b \in G$

i) $\exists! x \in G : a \cdot x = b.$ Es ist $x = a^{-1} \cdot b$

ii) $\exists! y \in G : y \cdot a = b.$ Es ist $y = b \cdot a^{-1}$

iii) $ax = bx$ für ein $x \in G \Rightarrow a = b$
bzw. $ya = yb$ für ein $y \in G \Rightarrow a = b$ (Kürzungsregel)

Beweis

i) $x = a^{-1}b$ erfüllt $ax = a(a^{-1}b) = \underbrace{(aa^{-1})}_{e} b = b$

ii) Analog zu i)

iii) $a = a \underbrace{(xx^{-1})}_{e} = (ax)x^{-1} = (bx)x^{-1} = b \underbrace{(xx^{-1})}_{e} = b$

$\square$

Untergruppen und Nebenklassen

3.15 Definition (Untergruppe)

$(G, \cdot)$ Gruppe, $\emptyset \neq U \subseteq G$.
U heißt <u>Untergruppe</u> von G ($U \leq G$), wenn U bzgl. '$\cdot$' eine Gruppe ist.

Bemerkung

22.11.2016

- Abgeschlossenheit prüfen: $\forall u, v \in U : uv \in U$
- e von G ist auch e von U
- Inversen in U gleich wie in G

(wegen Satz 3.13)

3.16 Beispiel

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

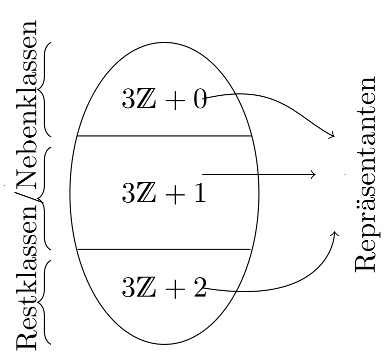
b) $(\{-1, 1\}, \cdot) \leq (\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot)$

c) $V_4 = \{\mathrm{id}, \underbrace{(AB)(CD)}_{\pi}, \underbrace{(AC)(BD)}_{\sigma}, \underbrace{(AD)(BC)}_{\eta}\} \leq \mathscr{S}_4$ (Bsp. 3.7, 3.10) weil V_4 abgeschlossen, $id \in V_4$, $\quad \gamma^{-1} = \gamma \qquad \forall \gamma \in V_4$

3.17 Beispiel

Es ist $U = 3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}$ eine Untergruppe von $(\mathbb{Z}, +)$.

- Mehr Klassen gibt es nicht, da $3\mathbb{Z} + 3 = 3\mathbb{Z} + 0$, $3\mathbb{Z} + 4 = 3\mathbb{Z} + 1$, $3\mathbb{Z} - 1 = 3\mathbb{Z} + 2$
- Repräsentanten sind nicht eindeutig, -1 auch Repräsentant von $3\mathbb{Z} + 2 = 3\mathbb{Z} - 1$
- Grundidee: Nebenklassen von U unterteilen $G = \mathbb{Z}$ in disjunkte Äquivalenzklassen. Hier: $x \sim_U y \Leftrightarrow \exists u \in 3\mathbb{Z} : u + x = y$, z.B. $4 \sim_U 10$, da $\underbrace{6}_{\in 3\mathbb{Z}} + 4 = 10$



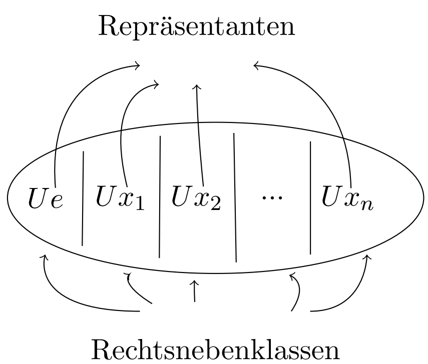
3.18 Satz + Definition (Rechtsnebenklasse, Repräsentant)

G Gruppe, $U \leq G$.

i) Für $x, y \in G : x \sim_U y :\Leftrightarrow \exists u \in U : ux = y$.
<u>Behauptung</u>: $\sim_U$ Äquivalenzrelation.

ii) $Ux := \{ux \mid u \in U\}$ (mit $x \in G$) heißt <u>Rechtsnebenklasse</u> von U in G. x heißt <u>Repräsentant</u> der Klasse Ux [Linksnebenklassen analog: xU]

iii) ${}^{G}\!/\!_{U} := \{Ux \mid x \in G\}$ Menge der Rechtsnebenklassen von U in G.
<u>Behauptung</u>: ${}^{G}\!/\!_{U}$ ist eine disjunkte Zerlegung von G in Äquivalenzklassen Ux.



Beweis

i) – $x \sim_U x$, da $\underbrace{e}_{\in U} \cdot x = x$ (Reflexivität)

– (Symmetrie)

$$\begin{aligned} x \sim_U y &\Rightarrow \exists u \in U : ux = y \\ &\Rightarrow x = \underbrace{u^{-1}}_{\in U} y = x \\ &\Rightarrow y \sim_U x \end{aligned}$$

– (Transitivität)

$$\begin{aligned} x \sim_U y,\ y \sim_U z &\Rightarrow \exists u, u' \in U : ux = y,\ u'y = z \\ &\Rightarrow u'y = u'(ux) = \underbrace{(u'u)}_{\in U} x = z \\ &\Rightarrow x \sim_U z \end{aligned}$$

iii) – $Ux = \{ux | u \in U\} = \{y \in G | \underbrace{\exists u : ux = y}_{y \sim_U x}\} = \{y \in G | y \sim_U x\} \Rightarrow Ux$ Äquivalenzklassen von $x \in G$

– Für je 2 Äquivalenzklassen Ux, Uy gilt: $Ux = Uy$ oder $Ux \cap Uy = \emptyset$ (wegen Transitivität)

3.19 Beispiel

$\mathbb{Z}_3 := {}^{\mathbb{Z}}/_{3\mathbb{Z}} = \{3\mathbb{Z}+0,\ 3\mathbb{Z}+1,\ 3\mathbb{Z}+2\} = \{3\mathbb{Z}+3,\ 3\mathbb{Z}-2,\ 3\ Z+11\}$
Man schreibt oft $\mathbb{Z}_3 = \{\underline{0}, \underline{1}, \underline{2}\}$ (wobei $\underline{j} = 3\mathbb{Z}+j$) oder einfach $\mathbb{Z}_3 = \{0, 1, 2\}$
Allgemein: $\mathbb{Z}_n := {}^{\mathbb{Z}}/_{n\cdot\mathbb{Z}}, \quad n \in \mathbb{N}$
Beobachtung in $\mathbb{Z}_3$: Ist $x \in \underline{1}, y \in \underline{2}$, dann ist immer $x + y \in \underline{0}$

3.20 Kriterium

G Gruppe, $U \leq G$.
Für je 2 beliebige Klassen, $Ux, Uy \quad (x, y \in G)$ gelte:
$x' \in Ux,\ y' \in Uy \Rightarrow x' \cdot y' \in U(xy)$

3.21 Definition (Wohldefiniertheit)

Wenn Kriterium 3.20 erfüllt ist, kann man auf ${}^{G}/_{U}$ eine Verknüpfung definieren:
$* : {}^{G}/_{U} \times {}^{G}/_{U} \to {}^{G}/_{U}$ mit
$(Ux) * (Uy) = U(\underbrace{xy}_{\text{Produkt in } G})$
Man sagt: Wenn 3.20 erfüllt, ist '$*$' <u>wohldefiniert</u>.

3.22 Beispiel

23.11.2016

a) $*$ wohldefiniert auf $(\mathbb{Z}_n, +)$ (ohne Beweis)
<u>Bemerkung:</u> $x \sim_U y \Leftrightarrow \exists u \in 3\mathbb{Z} : u + x = y$
$\Leftrightarrow x \equiv y \pmod 3$
Daraus ergibt sich die Def. aus Bsp. 3.12 mit $\mathbb{Z}_3 = \{0, 1, 2\}$ und $x \oplus y = x + y \pmod 3$

b) $U = \{\mathrm{id}, (12)\} \leq \mathscr{S}_3$. Auf ${}^{\mathscr{S}_3}/_{U}$ ist $*$ nicht wohldefiniert (Übung).

3.23 Satz (Faktorengruppe/Quotientengruppe)

$U \leq G, \quad G$ Gruppe.
Wenn '$*$' aus Def 3.21 wohldefiniert, dann ist $({}^{G}/_{U}, *)$ eine Gruppe.

(Name: Quotientengruppe/Faktorengruppe)
Beweis: Übung.
Bemerkung: G abelsch $\Rightarrow$ '$*$' immer wohldefiniert, d.h. ${}^{G}/{}_{U}$ Gruppe.

3.24 Lemma

G Gruppe, $U \leq G$, U endlich $\Rightarrow |Ux| = |U| \quad \forall x \in G$

Beweis

$\varphi : U \to Ux, \quad u \mapsto u \cdot x$ bijektiv:

- surjektiv, da $\varphi(U) = Ux$
- injektiv, da $\varphi(u_1) = \varphi(u_2) \Rightarrow u_1x = u_2x$
  $\overset{\cdot x^{-1}}{\Rightarrow} u_1 = u_2$

$\Rightarrow |U| = |Ux|$

3.25 Theorem (Lagrange)

G endliche Gruppe, $U \leq G \Rightarrow |U|$ teilt $|G|$ und $|{}^{G}/{}_{U}| = \frac{|G|}{|U|}$.

Beweis

Seien $U_{x_1}, ..., U_{x_q}$ die q verschiedenen Rechtsnebenklassen von U in G.
$\Rightarrow G = \dot{\bigcup}_{i=1}^{q} Ux_i \Rightarrow |G| = \sum_{i=1}^{q} \underbrace{|Ux_i|}_{=|U|} = q \cdot |U|.$ $\square$

Ordnung und zyklische Gruppen

3.26 Definition

$(G, \cdot)$ Gruppe, $a \in G$.
Definiere $a^0 := e, \quad a^1 := a, \quad \underbrace{a^m := (a^{m-1}) \cdot a}_{\text{für } m \in \mathbb{N}}, \quad a^m := \underbrace{(a^{-1})^{-m}}_{\text{für } m \in \mathbb{Z}^-}$
als Potenzen von $a \in G$.

3.27 Satz

G Gruppe, $a \in G$. Es gilt:

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

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

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

Beweis

i) a) m positiv:

- Inverses für a^m, wenn $m \geq 0$:
  Es ist $a^m \cdot \underbrace{(a^{-1})^m}_{\text{Inverse}} = \underbrace{a \cdot a \cdot ... \cdot a}_{\text{m-mal}} \cdot \underbrace{a^{-1} \cdot ... \cdot a^{-1}}_{\text{m -mal}} = e$
  $\Rightarrow (a^m)^{-1} = (a^{-1})^m$
- nach Definition: $a^{\overbrace{-m}^{\in \mathbb{Z}^-}} = (a^{-1})^{+m}$
  $\Rightarrow$ i) gilt für $m \geq 0$

b) m negativ:

- $a^{\overbrace{-m}^{\in \mathbb{N}}} = ((\underbrace{a^{-1}}_{\in G})^{-1})^{\overbrace{-m}^{\in \mathbb{N}}} \overset{\text{Def.}}{=} (a^{-1})^m$
- $a^{\overbrace{m}^{\in \mathbb{Z}^-}} = (a^{-}1)^{\overbrace{-m}^{\in \mathbb{N}}} \overset{\text{a)}}{=} (a^{-m})^{-1}$
  $\Rightarrow (a^m)^{-1} = ((a^{-m})^{-1})^{-1} = a^{-m}$

ii) + iii) analog mit m oder n negativ oder positiv

3.28 Satz + Definition (Ordnung, zyklische Gruppe)

G endliche Gruppe, $g \in G$.

i) Es gibt eine kleinste Zahl $n \in \mathbb{N}$ mit $g^n = e$. n heißt Ordnung $\mathcal{O}(g)$ von g.

ii) $\{g^0 = e, g^1, g^2, ..., g^{n-1}\} \leq G$ und heißt die von g erzeugte zyklische Gruppe $\langle g \rangle$.

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

Beweis

i) G endlich $\Rightarrow \exists i,j \in \mathbb{N} : g^i = g^j$ und $i > j$

$$\Rightarrow g^{\overbrace{i-j}^{\in\mathbb{N}}} = g^i g^{-j} = \underbrace{g^i}_{=g^j}(g^j)^{-1} = e$$

Wähle $n = \min\{k \in \mathbb{N} | g^k = e\}$.

ii)
- $\langle g\rangle$ abgeschlossen, da $g^m \cdot g^k = g^{m+k} \in \langle g\rangle$
- $g^0 = e \in \langle g\rangle$
- $(g^m)^{-1} = g^{-m} = \underbrace{g^n}_{e} \cdot g^{-m} \in \langle g\rangle$

iii) Lagrange: $n \mid |G| \Rightarrow n \cdot k = |G|$ für ein $k \in \mathbb{N}$

$$\Rightarrow g^{|G|} = g^{nk} = \underbrace{(g^n)}_{e}{}^k = e^k = e$$

$\square$

3.29 Bemerkung

Eine endliche Gruppe heißt zyklisch, falls sie von einem Element erzeugt wird.

Beispiel

- $(\mathbb{Z}_n, \oplus)$ zyklisch, da $1 \in \mathbb{Z}_n$ und $1^2 = 1+1 = 2$, $1^3 = 1+1+1 = 3$, ...,
  $1^n = (1^{n-1}) \cdot 1 = (n-1)+1 = n$ und $n \equiv 0 \pmod n$
  $\mathbb{Z}_n$ hat Ordnung n, da $1^n = 0$
- Drehungen, die ein regelmäßiges $n-$Eck in sich selbst überführen, sind zyklisch:
  $(ABC)^0 = id$, $(ABC) = (ABC)$, $(ABC)^2 = (ACB)$, $(ABC)^3 = id$
  $\langle (ABC)\rangle = \{\mathrm{id}, (ABC), (ACB)\} \leq \mathscr{S}_3$
- $\mathscr{S}_3$ oder V_4 nicht zyklisch.

3.30 Korollar

i) Satz von Euler:
$n \in \mathbb{N}$, $a \in \mathbb{Z}$, $\mathrm{ggT}(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$

ii) Kleiner Satz von Fermat:
p Primzahl, $a \in \mathbb{Z}$, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$

Beweis

Wir können annehmen, dass $1 \leq a < n$, denn
$a^{\varphi(n)} \mod n = \underbrace{(a \mod n)}_{\{1,\ldots,n-1\}}{}^{\varphi(n)} \mod n$

$\Rightarrow a \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^*$ endliche Gruppe $\Rightarrow a^{\overbrace{|\mathbb{Z}_n^*|}^{=\varphi(n)}} \equiv 1 \pmod{n}$
ii) Folgt aus i) für $n = p, \quad \varphi(p) = p - 1$ $\square$

4 Ringe und Körper

Grundlegende Eigenschaften

4.1 Definition (Ring)

Sei $\mathcal{R} \neq \emptyset$ eine Menge mit 2 Verknüpfungen $+$ und $\cdot$.

i) Man nennt $(\mathcal{R}, +, \cdot)$ einen Ring, wenn gilt:

   1) $(\mathbb{R}, +)$ ist abelsche Gruppe mit Neutralelement 0 und Inverse $-a$ von a.
   2) $(\mathbb{R}, \cdot)$ ist abgeschlossen und assoziativ (Halbgruppe).
   3) Distributivgesetze: $a \cdot (b + c) = ab + ac$
      $(a + b) \cdot c = ac + bc \qquad \forall a, b, c \in \mathcal{R}$

29.11.2016

ii) $(\mathcal{R}, +, \cdot)$ heißt kommutativ, falls '$\cdot$' zusätzlich kommutativ ist

iii) $(\mathcal{R}, +, \cdot)$ heißt Ring mit Eins, falls es bezüglich '$\cdot$' ein Neutralelement 1 gibt mit $a \cdot 1 = 1 \cdot a = a \qquad \forall a \in \mathcal{R}$.

iv) Ist $(\mathcal{R}, +, \cdot)$ Ring mit Eins, so heißen die bezüglich '$\cdot$' invertierbaren Elemente Einheiten.
Bezeichnung:

   – a^{-1} Inverse von a bzgl. '$\cdot$'
   – $\mathcal{R}^* :=$ Menge aller Einheiten in $\mathcal{R}$

4.2 Beispiel

a) Trivialer Ring $(\{0\}, +, \cdot)$

b) $(\mathbb{Z}, +, \cdot)$ kommutativer Ring mit Eins.
Einheiten: $1, -1 \Rightarrow \underbrace{\mathbb{Z}^* = \{-1, 1\}}_{\text{kein Ring!}}$
Ebenso $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$
mit $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ und $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

c) $(2\mathbb{Z}, +, \cdot)$ Ring, kommutativ, ohne Eins

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

e) $(\mathbb{R}^n, +, \cdot)$ kommutativer Ring mit Eins: ($\cdot$ und + Komponentenweise)
Bemerkung: $\mathcal{R}_1, ..., \mathcal{R}_n$ Ringe $\Rightarrow \mathcal{R}_1 \times ... \times \mathcal{R}_n$ Ring

f) $(M_n(\mathbb{R}), +, \cdot)$ (für $n \geq 2$) Ring mit Eins ($= E_n$). Nicht kommutativ!

4.3 Satz (Rechenregeln für Ringe)

$(\mathcal{R}, +, \cdot)$ Ring, $a, b, c \in \mathcal{R}$

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

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

iii) $(-a)(-b) = ab$

Beweis

i) Es ist $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$
Addiere $-a \cdot 0$: $\quad a \cdot 0 - a \cdot 0 = a \cdot 0 + a \cdot 0 - a \cdot 0$
$\Leftrightarrow \quad 0 = a \cdot 0$
Analog: $0 = 0 \cdot a$

ii) Es ist $(-a)b + ab = \underbrace{(-a + a)}_{=0} b = 0 \cdot b \overset{\text{i)}}{=} 0$
$\Rightarrow (-a)b$ invers zu ab und $(-a)b = -(ab)$
Analog: $a(-b) = -(ab)$

iii) $(-a)(-b) \overset{\text{ii)}}{=} -(a(-b)) \overset{\text{ii)}}{=} -(-(ab)) = ab$

$\square$

4.4 Bemerkung

a) $\mathcal{R}$ Ring mit Eins $\Rightarrow 1, -1 \in \mathcal{R}^*$
Achtung! Z.B. in $(\mathbb{Z}_2, \oplus, \odot)$ ist $1 = -1$

b) In einem kommutativen Ring gilt der binomische Lehrsatz:
$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i \cdot b^{n-i}$

c) In 4.3: Rechenregeln für Multiplikation mit additiven Inversen, z.B.: $a \cdot (-b)$
Über Addition mit multiplikativen Inversen keine Aussage möglich (z.B. keine Regel für $a^{-1} + b$).

4.5 Definition (Körper)

Ein kommutativer Ring mit Eins $(\mathcal{K}, +, \cdot)$ heißt Körper, falls $\mathcal{K}^* = \mathcal{K} \setminus \{0\}$. D.h. jedes $x \in \mathcal{K} \setminus \{0\}$ ist bezüglich '$\cdot$' invertierbar.

4.6 Beispiel

a) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ Körper [$(\mathbb{C}, +, \cdot)$ auch]
$(\mathbb{Z}, +, \cdot)$ kein Körper, da $\mathbb{Z}^* = \{1, -1\}$.

b) $\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n | \mathrm{ggT}(z, n) = 1\}$ Gruppe bezüglich '$\odot$'
$\Rightarrow (\mathbb{Z}_n, \oplus, \odot)$ Körper $\Leftrightarrow n$ Primzahl

4.7 Satz (Rechenregeln für Körper: Nullteilerfreiheit)

$(\mathcal{K}, +, \cdot)$ Körper, $a, b \in \mathcal{K}$. Dann gilt

a) alle Rechenregeln für Ringe gelten auch für Körper

b) $ab = 0 \Leftrightarrow a = 0 \vee b = 0$ [Gegenbeispiel: $(\mathbb{Z}_6, \oplus, \odot)$, weil $2 \odot 3 = 0$]

Beweis

$'\Leftarrow'$ klar (Satz 4.3i))

$'\Rightarrow'$ $ab = 0$. Angenommen $a \neq 0 \Rightarrow b = 1 \cdot b = (a^{-1}a)b = a^{-1} \underbrace{(ab)}_{=0} \overset{4.3i)}{=} 0$ $\square$

Strukturgleichheit von Ringen

4.8 Definition (Ringhomomorphismus, Ringisomorphismus)

Geg. $(\mathcal{R}, +, \cdot)$, $(\mathcal{R}', \boxplus, \boxdot)$ Ringe

i) $\psi : \mathcal{R} \to \mathcal{R}'$ heißt Ringhomomorphismus, falls $\psi(x + y) = \psi(x) \boxplus \psi(y)$ und $\psi(xy) = \psi(x) \boxdot \psi(y)$ $\forall x, y \in \mathcal{R}$

ii) Wenn ψ bijektiv ist, heißt ψ Ringisomorphismus. In diesem Fall heißen $\mathcal{R}, \mathcal{R}'$ isomorph (d.h. sie sind strukturgleich). Man schreibt $\mathcal{R} \cong \mathcal{R}'$

4.9 Beispiel

a) $\psi : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, \oplus, \odot)$
$x \mapsto x \mod n$
$x + y \to x + y \pmod n, \quad x \cdot y \to x \cdot y \pmod n$
ψ Ringhomomorphismus
Nicht injektiv: $\psi(1) = \psi(n+1) = 1$ 30.11.2016

b) $(\{w, f\}, \text{XOR}, \wedge) \cong (\mathbb{Z}_2, \oplus, \odot)$
Boolsche Algebra, siehe PÜ

Chinesischer Restsatz

4.10 Bemerkung

Gegeben: $m_1, ..., m_n \in \mathbb{N}, \quad a \in \mathbb{Z}, \quad M = m_1 \cdot ... \cdot m_n$
$\Rightarrow \underbrace{(a \mod M)}_{r} \mod m_i = a \mod m_i \quad \forall i$

Beweis

Z.z.: $r \equiv a \pmod{m_i}$
Division mit Rest:

$$
\begin{aligned}
\exists q \in \mathbb{Z} : a &= qM + r \\
&= \underbrace{\left(q \frac{M}{m_i}\right)}_{\in \mathbb{Z}, \text{ da } m_i | M} m_i + r \\
\Rightarrow a &\equiv r \pmod{m_i}
\end{aligned}
$$

□

4.11 Chinesischer Restsatz

Gegeben:

- $m_1, ..., m_n \in \mathbb{N}$ paarweise teilerfremd
- $M = m_1 \cdot ... \cdot m_n$
- $a_1, ..., a_n \in \mathbb{Z}$

Dann existiert $0 \le x < M$ mit

$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}\right\} \underline{\text{Simultane Kongruenz}}$$

Beweis

Es ist $\operatorname{ggT}\Big(m_i, \underbrace{\frac{M}{m_i}}_{M_i}\Big) = 1 \qquad \forall i \in \{1, ..., n\}$.

$\overset{\text{EEA}}{\Rightarrow} \exists\, s_i, t_i \in \mathbb{Z} : t_i m_i + s_i M_i = 1$

Setze: $e_i := s_i M_i \Rightarrow e_i \equiv \begin{cases} 1 \pmod{m_i} \\ 0 \pmod{m_j},\ j \neq i \end{cases}$

$\Rightarrow x \overset{4.10}{=} \sum_{i=1}^{n} a_i e_i \pmod{M}$ ist Lösung der simultanen Kongruenz.

4.12 Beispiel

a) $m_1 = 3, \quad m_2 = 4, \quad m_3 = 5 \Rightarrow M = 60$

Finde $x \in [0, 60)$ mit $x \equiv \begin{cases} 2 \pmod 3 & (= a_1) \\ 3 \pmod 4 & (= a_2) \\ 2 \pmod 5 & (= a_3) \end{cases}$

Es ist

- $M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$
- $M_2 = \frac{60}{4} = 15$
- $M_3 = \frac{60}{5} = 12$

EEA:

- $7 \cdot \overbrace{3}^{m_1} + \underbrace{(-1) \cdot \overbrace{20}^{M_1}}_{e_1} = 1$
- $4 \cdot \overbrace{4}^{m_2} + \underbrace{(-1) \cdot \overbrace{15}^{M_2}}_{e_2} = 1$

$$- 5 \cdot \overbrace{5}^{m_3} \underbrace{+(-2) \cdot \overbrace{12}^{M_3}}_{e_3} = 1$$

$$\Rightarrow x = [2 \cdot (-20) + 3 \cdot (-15) + 2 \cdot (-24)] \mod 60 = -133 \mod 60 = 47$$

b) Was ist $2^{1000} \mod \underbrace{1155}_{= \underset{m_1}{3} \cdot \underset{m_2}{5} \cdot \underset{m_3}{7} \cdot \underset{m_4}{11}}$?

1) Berechne $2^{1000} \mod 3, 5, 7$ und 11
   - $2^{1000} \mod 3 = (-1)^{1000} \mod 3 = 1 = a_1$
   - $2^{1000} \mod 5 = 4^{500} \mod 5 = (-1)^{500} = 1 = a_2$
   - $2^{1000} \mod 7 = \underbrace{2^3}_{=8}{}^{\cdot 333+1} \mod 7 = 1 \cdot 2 \mod 7 = 2 = a_3$
   - $2^{1000} \mod 11 = \underbrace{2^5}_{=32}{}^{\cdot 200} \mod 11 = (-1)^{200} = 1 = a_4$

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

   Chinesischer Restsatz: $x = 331$

4.13 Satz (Eindeutigkeit Chines. Restsatz)

Die Lösung x aus 4.11 ist eindeutig.

Beweis

Z.z.: $\psi : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}, \quad x \mapsto (x \mod m_1, ..., x \mod m_n)$ ist bijektiv (Ringisomorphismus)

- ψ Ringhomomorphismus:

$$\begin{aligned} \psi(x \oplus y) &= \psi(x + y \mod M) \\ &= ((x + y \mod M) \mod m_1, ..., (x + y \mod M) \mod m_n) \\ &\overset{4.10}{=} (x + y \mod m_n, \ ..., \ x + y \mod m_n) \\ &= \psi(x) \oplus \psi(y) \end{aligned}$$

  Analog mit $\psi(x \odot y) = \psi(x) \odot \psi(y)$

- ψ surjektiv:
  Zu jedem n-Tupel aus $\underbrace{\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}}_{\ni(a_1,...,a_n)}$ gibt es Lösung $x \in \mathbb{Z}_M$ (4.11).

- ψ injektiv:
  Da $|\mathbb{Z}_M| = |\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}| \Leftrightarrow M = m_1 \cdot ... \cdot m_n$
  D.h. kein Element word doppelt 'getroffen'

$\Rightarrow \psi$ bijektiv, also Isomorphismus $\square$

4.14 Beispiel

Gilt $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$? Nein.
z.B. $\underbrace{\mathbb{Z}_2^* = \{1\}}_{\varphi(2=1)}$, $\underbrace{\mathbb{Z}_4^* = \{1, 3\}}_{\varphi(4)=2}$
Aber: $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ und $4 = \varphi(8) \neq \varphi(2) \cdot \varphi(4)$

4.15 Korollar

- $M = m_1 \cdot .... \cdot m_n$ mit m_i paarweise teilerfremd und $m_i \in M$
  $\Rightarrow \varphi(M) = \varphi(m_1) \cdot ... \cdot \varphi(m_n)$

- Insbesondere:
  $M = p_1^{a_1} \cdot ... \cdot p_k^{a_k}, \quad p_i \in \mathbb{P}$ (Primzahl), $p_i \neq p_j$ für $i \neq j, \quad a_i \in \mathbb{N}$
  $\Rightarrow \varphi(M) = (p_1 - 1)p_1^{a_1-1} \cdot ... \cdot (p_k - 1)p_k^{a_k-1}$

Beweis

Wegen 4.13 ist $\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$ mittels ψ.
$\Rightarrow x$ Einheit $\Leftrightarrow \psi(x) = (x \mod m_1, ..., x \mod m_n)$ Einheit
$\Leftrightarrow x \mod m_i$ Einheit $\forall i \Rightarrow \varphi(M) = \varphi(m_1) \cdot ... \cdot \varphi(m_n)$
Es ist $\varphi(p^a) = \underbrace{p^a}_{|\mathbb{Z}_{p^a}|} - \underbrace{p^{a-1}}_{\text{Vielfache von p in } \mathbb{Z}_{p^a}} = (p-1)p^{a-1}$

a	$\lvert\mathbb{Z}_{p^a}\rvert$	Vielfache von p	$\varphi(p^a) = \lvert\mathbb{Z}_{p^a}^*\rvert$
1	p	$0 \cdot p = 0$	$p - 1 = p^1 - p^0$
2	p^2	$k \cdot p, \underbrace{0 \leq k \leq p-1}_{p \text{ Möglichkeiten}}$	$p^2 - p^1$
3	p^3	$kp + k'p^2, \underbrace{0 \leq k, k' \leq p-1}_{p^2 \text{ Möglichkeiten}}$	$p^3 - p^2$

$\square$

Polynomringe

06.12.2016

In Mathe I wurde für den Ring $(\mathbb{Z}, +, \cdot)$ folgendes eingeführt:

- Division mit Rest
- Erweiterter Euklidischer Algorithmus
- kgV, ggT, Primzahlzerlegung

4.16 Definition (Polynom)

$\mathcal{K}$ - Körper mit Nullelement $\mathcal{O}$ und Einselement $\mathbb{1}$.

i) Ein <u>Polynom</u> über $\mathcal{K}$ ist ein Ausdruck $f = \underbrace{a_0 x^0}_{a_0} + \underbrace{a_1 x^1}_{a_1 x} + ... + a_n x^n$ mit $n \in \mathbb{N}$, $a_i \in \mathcal{K}$ Koeffizienten von f (auch $f(x)$ anstatt f).
Ist $a_i = 0 \quad \forall \{1, ..., n\}$, so schreibt man $f = 0$ (Nullpolynom)

ii) $\mathcal{K}[x]$ = Menge aller Polynome über $\mathcal{K}$ in einer Variablen x

iii) $f, g \in \mathcal{K}[x]$ sind gleich, wenn gilt

   a) $f = a_0 + ... + a_n x^n$
   $g = b_0 + ... + b_m x^m$ mit $a_n \neq 0,\ b_m \neq 0$
   $\Rightarrow m = n$ und $a_i = b_i \quad \forall i = 1, ..., n$
   oder

   b) $f = 0$ und $g = 0$

4.17 Beispiel

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

b) $g = x^7 + x^2 \in \mathbb{Z}_2[x]$, d.h. Koeffizienten $\in \{0, 1\}$

4.18 Satz + Definition

$\mathcal{K}$ Körper.
$\mathcal{K}[x]$ ist kommutativer Ring mit Eins. Dabei ist für $f = \sum_{i=0}^{n} a_i x^i$,
$g = \sum_{j=0}^{m} b_j x^j$

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

- $f \cdot g = (a_0 + a_1 x + ... + a_n x^n)(b_0 + b_1 x + ... + b_m xm)$
  $= \underbrace{a_0 \cdot b_0}_{c_0} + \underbrace{(a_0 \cdot b_1 + a_1 \cdot b_0)}_{c_1} x + ... + \underbrace{a_n b_m}_{c_{n+m}} x^{n+m}$
  mit $c_i = \sum_{k=0}^{i} a_k \cdot b_{i-k}$ (Faltungsprodukt)
  [Anmerkung: $a_i = 0 = b_j$ für $i > n$ bzw. $j > m$]
- Einselement: $f = 1$
- Nullelement $f = 0$

$\mathcal{K}[x]$ heißt der Polynomring in einer Variablen über $\mathcal{K}$.

Beweis

Ringeigenschaften nachrechnen □

4.19 Bemerkung

- $a_0,\ a_1 x,\ a_2 x^2, ...,\ a_n x^n$ heißen Monome
- $a_n x^n$ heißt Leitterm von $f = a_0 + ... + a_n x^n$ mit $a_n \neq 0$

4.20 Beispiel

In $\mathbb{Z}_3[x]$:
$f = 2x^3 + 1, \quad g = x - 1 = x + 2$, da $-1 \equiv 2 \pmod 3$

- $f + g = 2x^3 + x + \underbrace{1 + 2}_{\equiv 0 \pmod 3} = 2x^3 + x$
- $f \cdot g = (2x^3 + 1)(x + 2) = 2x^4 + x + \underbrace{4x^3}_{\equiv 1 \pmod 3} + 2 = 2x^4 + x + x^3 + 2$

Grad eines Polynoms

4.21 Definition

$f \in \mathcal{K}[x], \quad f = a_0 + ... + a_n x^n \qquad a_n \neq 0$
n heißt der Grad von f, $\mathrm{grad}(f) = n$
$\mathrm{grad}(0) = -\infty, \quad \mathrm{grad}(g) = 0$, falls g konstant

4.22 Satz

$\mathcal{K}$ Körper, $f, g \in \mathcal{K}[x]$.
$\Rightarrow \mathrm{grad}(f \cdot g) = \mathrm{grad}(f) + \mathrm{grad}(g)$
<u>Konvention:</u> $\quad -\infty - \infty = -\infty = -\infty + n = -\infty$

Beweis

- Stimmt für $f = 0$ oder $g = 0$
- Angenommen die Leitterme von f bzw. g sind $a_n x^n$ bzw. $b_m x^m$ mit $a_n \neq 0, \quad b_m \neq 0$.
  $\Rightarrow \mathrm{grad}(f) = n, \quad \mathrm{grad}(g) = m$ und $\underbrace{a_n \cdot b_m}_{\neq 0,\text{ da } \mathcal{K} \text{ Körper (4.7)}} x^{n+m}$ ist Leitterm von $f \cdot g$
  $\Rightarrow \mathrm{grad}(fg) = n + m$ $\square$

4.23 Korollar (Inversen in $\mathcal{K}[x]$)

$\mathcal{K}[x]^* = \{f \in \mathcal{K}[x] \mid \mathrm{grad}(f) = 0\}$ (nur konstante Polynome $\neq 0$ invertierbar)

Beweis

$$f \cdot f^{-1} = 1 \Rightarrow \mathrm{grad}(ff^{-1}) = \mathrm{grad}(f) + \mathrm{grad}(f^{-1}) \overset{4.22}{=} \mathrm{grad}(1) = 0$$
$$\Leftrightarrow \mathrm{grad}(f) = \mathrm{grad}(f^{-1}) = 0$$ $\square$

Polynomdivision mit Rest

4.24 Bemerkung

Für $b \in \mathcal{K}$ ist $f(b) = \sum_{i=0}^{n} a_i \cdot b^i$, falls $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathcal{K}[x]$.
Man kann zeigen, dass $\psi_b : \mathcal{K}[x] \to \mathcal{K}$, $f \mapsto f(b)$ ein surjektiver Homomorphismus ist.

4.25 Definition

$\mathcal{K}$ Körper, $f, g \in \mathcal{K}[x]$.
$f|g$, falls $q \in \mathcal{K}[x]$ existiert mit $g = gf$ (nach 4.22: $\mathrm{grad}(f) \leq \mathrm{grad}(g)$).

4.26 Satz (Division mit Rest in $\mathcal{K}[x]$)

$\mathcal{K}$ Körper, $f \in \mathcal{K}[x], \quad 0 \neq g \in \mathcal{K}[x]$.
Dann existieren eindeutig bestimmte Polynome $q, r \in \mathcal{K}[x]$ mit $f = qg + r$ und

$\operatorname{grad}(r) < \operatorname{grad}(g)$.
Bezeichnung: $r = f \mod g, \quad q = f \operatorname{div} g$

Beweis

vgl. Mathe I für $\mathbb{Z}$, Literatur $\square$

4.27 Beispiel

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

$$
\begin{array}{rrrrrl}
\big(x^4 & +2x^3 & & -x & +2\big) & : \big(3x^2-1\big) = \frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{9} + \frac{-\frac{1}{3}x+\frac{19}{9}}{3x^2-1}\\
-x^4 & & +\frac{1}{3}x^2 & & & \\
\hline
& 2x^3 & +\frac{1}{3}x^2 & -x & & \\
& -2x^3 & & +\frac{2}{3}x & & \\
\hline
& & \frac{1}{3}x^2 & -\frac{1}{3}x & +2 & \\
& & -\frac{1}{3}x^2 & & +\frac{1}{9} & \\
\hline
& & & -\frac{1}{3}x & +\frac{19}{9} &
\end{array}
$$

Mit $\frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{9} = q$ und $-\frac{1}{3}x + \frac{19}{9} = r$ (Rest).
Aufhören bei $\operatorname{grad}(r) < \operatorname{grad}(g)$!

4.28 Korollar

$\mathcal{K}$ Körper, $a \in \mathcal{K}, \quad f \in \mathcal{K}[x]$

$$\underbrace{(x-a)}_{\text{teilt f restlos}} \mid f \Leftrightarrow f(a) = 0$$ 07.12.2016

Beweis

($\Rightarrow$) $\exists q \in \mathcal{K}[x] : f = q(x-a) \Rightarrow f(a) = q(a)\underbrace{(a-a)}_{0} = 0$

($\Leftarrow$) Division mit Rest: $f = q(x-a) + r$, $\operatorname{grad}(r) < \operatorname{grad}(x-a) \quad$ (da $q|f$)
$\Rightarrow \operatorname{grad}(r) \leq 0$, d.h. $r = c \neq 0$ konstant oder $r = 0$
$0 = f(a) = q(a)\underbrace{(a-a)}_{=0} + r(a) \Rightarrow r = 0$ $\square$

Euklidischer Algorithmus in $\mathcal{K}[x]$

4.29 Definition (Normiertheit)

$\mathcal{K}$ Körper.

i) $f = a_0 + ... + a_n x^n \in \mathcal{K}[x], \quad a_n \neq 0$ heißt <u>normiert</u>, wenn $a_n = 1$

ii) $g, h \in \mathcal{K}[x], \quad g, h$ nicht beide 0.
$f = \text{ggT}(g, h)$, falls $f \in \mathcal{K}[x]$ normiertes Polynom von maximalem Grad ist, das g und h teilt.

iii) $g, h \in \mathcal{K}[x] \setminus \{0\}$.
$f = \text{kgV}(g, h)$, falls $f \in \mathcal{K}[x]$ ein normiertes Polynom von minimalem Grad ist, das von g und h geteilt wird.

4.30 Bemerkung

a) $g = x, \quad h = x + 1 \in \mathbb{Q}[x]$

- $g | x(x+1), \quad h | x(x+1)$
- $g | 2x(x+1), \quad h | 2x(x+1)$
- $\text{kgV}(g, h) = x(x+1) = x^2 + x$, da $2x^2 + 2x$ nicht normiert!
  $\rightarrow$ Normierung macht Ergebnisse eindeutig.

b) Normierung erfolgt, indem man durch Koeffizienten des Leitterms 'teilt':
$f = a_n x^n + ... + a_0 \Rightarrow a_n^{-1} \cdot f = \underbrace{x^n + ... + a_n^{-1} a_0}_{\text{normiert}}$

c) $\text{kgV}(g, h)$ existiert und ist eindeutig.

- Existenz: $g | gh, \quad h | gh$ (gh gemeinsames Vielfaches)
- Eindeutig : $f_1 = \text{kgV}(g, h), \quad f_2 = \text{kgV}(g, h)$
  $\Rightarrow g, h | f_1$ und $g, h | f_2$
  $\Rightarrow g, h | (f_1 - f_2)$
  f_1, f_2 normiert und von gleichem (minimalen) Grad.
  $\Rightarrow \text{grad } (f_1 - f_2) < \text{grad } (f_1)$
  $\Rightarrow f_1 - f_2 = 0$, denn sonst wäre $\text{kgV}(g, h) = f_1 - f_2$ ↯zur Minimalität des Grades
  $\Rightarrow$ kgV eindeutig.

d) $\text{ggT}(g, h)$ existiert und ist eindeutig. Beweis folgt wie in Mathe I für $\mathbb{Z}$ aus:

4.31 Lemma von Bézout

$g, h \in \mathcal{K}[x]$ nicht beide gleich 0.
$\Rightarrow \exists s, t \in \mathcal{K}[x] : sg + th = \text{ggT}(g, h)$

Beweis

Siehe 4.33 (EEA).

Beweis Eindeutigkeit von ggT

$f = \text{ggT}(g, h), \quad f' = \text{ggT}(g, h)$
$(f, f'$ Funktionen desselben Grades und normiert$)$
$\Rightarrow \exists s', t' \in \mathcal{K}[x] : f' = s' \cdot g + t' \cdot h$

$f|g \wedge f|h \Rightarrow f|f'$
$\Rightarrow \exists q \in \mathcal{K}[x] : f' = qf$
$\Rightarrow \text{grad}(f') = \text{grad } (q) + \text{grad } (f)$

$\text{grad } (f) = \text{grad } (f') \Rightarrow \text{grad } (q) = 0$
$\text{grad } (q) = 0 \Rightarrow q = c \neq 0, \quad c \in \mathcal{K}$
$\Rightarrow f' = cf$
f, f' normiert $\Rightarrow c = 1$ $\square$

4.32 Satz: Euklidischer Algorithmus EA in $\mathcal{K}[x]$

Eingabe: $g, h \in \mathcal{K}[x]$, nicht beide gleich 0
if $h = 0$ **then**
    $y \coloneqq g$
end if
if $h|g$ **then**
    $y \coloneqq h$
end if
if $h \neq 0 \wedge h \nmid g$ **then**
    $x \coloneqq g, \quad y \coloneqq h$
    while $(x \mod y) \neq 0$ **do**
        $r \coloneqq x \mod y$
        $x \coloneqq y, \quad y \coloneqq r$
    end while

end if
$d := a_n^{-1} y$ (Normierung von y, siehe 4.30)
Ausgabe: $d = \mathrm{ggT}(g, h)$

Beweis

Wie für $\mathbb{Z}$ in Mathe I.
Hinweis: $d|g$ und $d|h \Leftrightarrow d|(g \mod h)$ und $d|h$.
Begründung: $g = qh + (g \mod h)$.

4.33 Satz: Erweiterter Euklidischer Algorithmus EEA in $\mathcal{K}[x]$

Eingabe: $g, h \in \mathcal{K}[x]$, nicht beide gleich 0
if $h = 0$ **then**
  $y := g, \quad s := 1, \quad t := 0$
end if
if $h|g$ **then**
  $y := h, \quad s := 0, \quad t := 1$
end if
if $h \neq 0 \wedge h \nmid g$ **then**
  while $(x \mod y) \neq 0$ **do**
    $q := x \operatorname{div} y, \quad r := x \mod y$
    $s := s_1 - q s_2, \quad t := t_1 - q t_2$
    $s_1 := s_2, \quad s_2 := s$
    $t_1 := t_2, \quad t_2 := t$
    $x := y, \quad y := r$
  end while
end if
$d := a_n^{-1} y$ (Normierung von y, siehe 4.30)
$s := a_n^{-1} s, \quad t := a_n^{-1} t$ (Normierung von s, t, siehe 4.30)
Ausgabe: $d = \mathrm{ggT}(g, h), \quad s, t$ für $\mathrm{ggT}(g, h) = sh + tg$

4.34 Beispiel

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

x	y	s_1	s_2	s	t_1	t_2	t	q	r
g	h	1	0		0	1			
h	$x^2 + x$	0	1	1	1	$2x + 1$	$2x + 1$	$x + 2$	$x^2 + x$
$x^2 + x$	$\underbrace{2x + 2}_{\text{ggT unnormiert}}$	1	$2x + 2$	$2x + 2$	$2x + 1$	x^2	x^2	$x + 1$	$2x + 2$

NR: (Achtung: Polynomdivision in $\mathbb{Z}_3[x]$, nicht normale Polynomdivision!)

- $$\begin{array}{l}
(x^4 + x^3 + 2x^2 \qquad +1) \;:\; (x^3 + 2x^2 + 2) = \overbrace{x + 2}^{q} \\
\underline{-x^4 - 2x^3 \qquad\quad -2x} \\
\qquad 2x^3 + 2x^2 + x + 1 \\
\qquad \underline{-2x^3 - x^2 \qquad - 1} \\
\qquad\qquad x^2 + x \qquad\qquad (= r)
\end{array}$$

- $$\begin{array}{l}
(x^3 + 2x^2 \qquad + 2) : \; (x^2 + x) = x + 1 \\
\underline{-x^3 - x^2} \\
\qquad x^2 \qquad +2 \\
\qquad \underline{-x^2 - x} \\
\qquad\qquad 2x + 2 \qquad\qquad (= r)
\end{array}$$

- $t = 1 - (x + 1)(2x + 1) = 1 - (2x^2 + 1) = x^2$

- $$\begin{array}{l}
(x^2 + x) : \; (2x + 2) = 2^{-1}x \\
\underline{-x^2 - x} \\
\qquad\quad 0
\end{array}$$

- Normierung von y:

$$\begin{aligned}
d &= a_n^{-1} y = 2^{-1}(2x + 2) \\
&= x + 1 \\
s &= 2^{-1}(2x + 2) = x + 1 \\
t &= 2^{-1} \cdot x^2 = 2x^2, \text{ da } 2^{-1} = 2
\end{aligned}$$

- Probe:

$$\begin{aligned} d = sg + th &= (x+1)(x^4 + x^3 + 2x^2 + 1) + (2x^2)(x^3 + 2x^2 + 2) \\ &= x^5 + x^4 + 2x^3 + x + x^4 + x^3 + 2x^2 + 1 + 2x^5 x^4 + x^2 \\ &= 3x^5 + 3x^4 + 3x^3 + 3x^2 + x + 1 \\ &= 0x^5 + 0x^4 + 0x^3 + 0x^2 + x + 1 \\ &= x + 1 = \mathrm{ggT}(g, h) \end{aligned}$$

Primelemente in $\mathcal{K}[x]$

<u>Primelemente</u> sind Polynome, die sich nicht als Produkt von zwei Polynomen vom Grad ≥ 1 darstellen lassen. So ist z.B. $2x^2 + 2x = 2x(x+1)$ kein Primelement, jedoch sind die Faktoren $2x$ und $x+1$ Primelemente.

4.35 Definition (Primelemente = irreduzible Polynome)

13.12.2016

$p \in \mathcal{K}[x]$ mit $\mathrm{grad}(p) \geq 1$ heißt <u>irreduzibel</u>, falls gilt:

$$\forall f, g \in \mathcal{K}[x] : p = f \cdot g \text{ ist } \mathrm{grad}(f) = 0 \text{ oder } \mathrm{grad}(g) = 0$$

4.36 Beispiel

a) $x + 1, \quad 2x \in \mathbb{R}[x]$ irreduzibel.
Allg.: $ax + b \quad (a \neq 0)$ irreduzibel in $\mathcal{K}[x]$

b) $x^2 - 2 \in \mathbb{Q}[x]$ ist irreduzibel:
Angenommen nicht, dann $x^2 - 2 = \underbrace{(ax+b)}_{\text{Nullstelle:}-\frac{b}{a}} \underbrace{(cx+d)}_{\text{Nullstelle:}-\frac{d}{c}} \qquad (a, c \neq 0)$
$\Rightarrow x^2 - 2$ hat auch Nullstelle $-\frac{b}{a} \in \mathbb{Q}$ ↯
Widerspruch: Nullstelle von $x^2 - 2$ sind aus $\mathbb{R}$

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

d) $x^2 + 1$ hat in $\mathbb{R}$ keine Nullstelle und ist somit irreduzibel in $\mathbb{R}[x]$.
<u>Anmerkung:</u> In $\mathbb{C}[x]$ ist $x^2 + 1$ kein Primelement (siehe Kapitel 5)

e) $x^2 + 1 = (x+2)(x+3)$ in $\mathbb{Z}_5[x]$
$\rightarrow$ nicht irreduzibel in $\mathbb{Z}_5[x]$

4.37 Satz

$f \in \mathcal{K}[x]$, $\operatorname{grad}(f) \geq 1$. Dann sind äquivalent:

(1) f irreduzibel

(2) $g, h \in \mathcal{K}[x], f|g \cdot h \Rightarrow f|g \vee f|h$

Beweis

(1) $\Rightarrow$ (2)

$$\begin{aligned} \text{Angenommen } f \nmid g &\overset{(1)}{\Rightarrow} \operatorname{ggT}(f,g) = 1 \\ &\overset{\text{Bézout}}{\Rightarrow} \exists s,t \in \mathcal{K}[x] : sf + tg = 1 \\ &\Rightarrow sfh + tgh = h \\ &\text{Wissen:} f|fsh \text{ und } f|tgh \quad (f|gh \text{ Voraussetzung von (2)}) \\ &\Rightarrow f|h \end{aligned}$$

(2) $\Rightarrow$ (1)

Angenommen $f = gh$. Zeigen: $\operatorname{grad}(h) = 0$.

$$\begin{aligned} f = gh &\overset{(2)}{\Rightarrow} f|g \vee f|h \quad \text{O.B.d.A: } f|g \\ &\Rightarrow \operatorname{grad}(f) \underset{f|g}{\leq} \operatorname{grad}(g) \underset{h \neq 0}{\leq} \operatorname{grad}(h) + \operatorname{grad}(g) = \operatorname{grad}(\underbrace{h \cdot g}_{=f}) \end{aligned}$$

(damit müssen also alle '$\leq$' sein: '$=$')

$\Rightarrow \operatorname{grad}(h) = 0$

$\square$

4.38 Korollar

$f \in \mathcal{K}[x]$, $\operatorname{grad}(f) = n \geq 1$. Dann:

1) f hat höchstens n Nullstellen $a_1, ..., a_k \in \mathcal{K}$

2) $f = (x - a_1) \cdot ... \cdot (x - a_k) \cdot \bar{f}$ mit $\operatorname{grad}(\bar{f}) = \operatorname{grad}(f - k)$.
[f normiert, $k = n \Rightarrow f = (x - a_1) \cdot ... \cdot (x - a_n)$]

Beweis

$\underline{n = 1}$: $f = ax + b$ hat Nullstelle $-a^{-1}b$

$\underline{n > 1}$: Hat f keine Nullstelle, so fertig. Sonst:
Sei a Nullstelle $\Rightarrow f = (x-a)g, \quad \text{grad}(g) = n-1$.
Sei $b \neq a$ weitere Nullstelle $\Rightarrow (x-b)|(x-a)g$
$x - b$ irreduzibel, $(x-b) \not|(x-a) \Rightarrow (x-b)|g$
$\Rightarrow b$ Nullstelle von g

Per Induktion hat $g \quad n-1$ Nullstellen. Behauptung folgt. □

4.39 Satz

$f \in \mathcal{K}[x]$ mit Leitterm $a_n x^n, \quad n \geq 1$
$\Rightarrow$ Es existieren eindeutig bestimmte irreduzible Polynome $p_1, ..., p_l$ und $m_1, ..., m_l \in \mathbb{N}$ mit $f = a_n p_1^{m_1} \cdot ... \cdot p_l^{m_l}$

Beweis

Wie in $\mathbb{Z}$. □

4.40 Bemerkung

$(\mathbb{Z}_n, \oplus, \odot)$ Körper $\Leftrightarrow n$ Primzahl
Analog in $\mathcal{K}[x]$:
Sei $f \in \mathcal{K}[x], \quad \text{grad}(f) = n$
$(\mathcal{K}[x]_n, +, \odot_f)$ mit

- $\mathcal{K}[x]_n := \{g \in \mathcal{K}[x] \mid \text{grad}(g) < n\}$
- $g \odot_f h = (g \cdot h) \mod f$

ist kommutativer Ring mit Eins.

$\mathcal{K}[x]_n^* = \{g \in \mathcal{K}[x]_n \mid \text{ggT}(g, f) = 1\}$

Man kann zeigen:

a) $\mathbb{Z}_p[x]_n$ Körper der Ordnung $p^n \Leftrightarrow f$ irreduzibel, p Primzahl.

b) Jeder endliche Körper hat Primzahlpotenzordnung und ist durch seine Ordnung bis auf Isomorphie eindeutig festgelegt.

5 Komplexe Zahlen

Problem (16 Jhdt.):

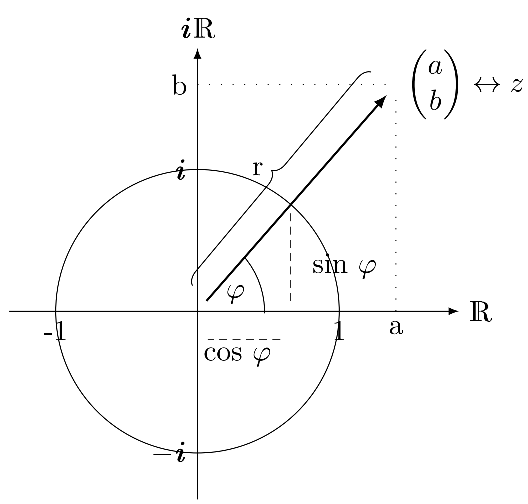
- Gleichungen wie z.B. $x^2 = -1$ haben keine reelle Lösung. Dagegen hat $x^2 = -1$ imaginäre Lösungen ('imaginaires' - Descartes) $x_{1/2} = \pm\sqrt{-1}$
- $x^4 = 1$ hat zwei reelle Lösungen $x = \pm 1$ und zwei imaginäre Lösungen $x = \pm\sqrt{-1}$
- $x^2 + 2x + 2$ hat die imaginären Lösungen $-1 \pm \sqrt{-1}$

5.1 Definition

- $\boldsymbol{i} := \sqrt{-1}$ heißt <u>imaginäre Einheit</u> (Euler 1777)
- $\mathbb{C} := \{a + b\boldsymbol{i} \mid a, b \in \mathbb{R}\}$ Menge der komplexen Zahlen
- Für $z = a + b\boldsymbol{i}$ heißt $\mathrm{Re}(z) := a$ <u>Realteil</u> von z und $\mathrm{Im}(z) := b$ <u>Imaginärteil</u> von z

Gaußsche Zahlenebene und Polarkoordinaten

5.2 Gaußsche Zahlenebene (1831)



Beobachtung: $a + b\boldsymbol{i} \leftrightarrow \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$

('korrespondiert eineindeutig zu')

$r = \sqrt{a^2 + b^2}$
$a = r \cdot \cos(\varphi)$
$b = r \cdot \sin(\varphi)$

Daraus ergibt sich die Darstellung in Polarkoordinaten:
$r \geq 0, \quad \varphi \in [0, 2\pi)$ bzw. $(r, \varphi) \in [0, \infty) \times [0, 2\pi)$
$\Rightarrow a + b\boldsymbol{i} = r(\cos(\varphi) + \boldsymbol{i}\sin(\varphi))$

5.3 Definition

14.12.2016

Für $z = a + b\boldsymbol{i} \in \mathbb{C}$ ist $|z| := \sqrt{a^2 + b^2}$ der Betrag von z.

5.4 Bemerkung

Jede Zahl $z = a + b\boldsymbol{i} \in \mathbb{C} \setminus \{0\}$ lässt sich durch den Winkel $\varphi \in [0, 2\pi)$ und durch den Betrag $|z|$ eineindeutig darstellen: $z = |z| \underbrace{(\cos(\varphi) + \boldsymbol{i}\sin(\varphi))}_{e^{i\varphi}}$

5.5 Formel von Euler

$e^{\boldsymbol{i}\varphi} = \cos(\varphi) + \boldsymbol{i}\sin(\varphi), \quad \varphi \in \mathbb{R}$

Beweisidee (später mit Taylorreihen)

$$\underbrace{\sum_{k=0}^{\infty} \frac{(\boldsymbol{i}\varphi)^k}{k!}}_{\text{später: } e^{i\varphi}} = \underbrace{\sum_{k=0}^{\infty} (-1)^k \cdot \frac{\varphi^{2k}}{(2k)!}}_{\cos(\varphi),\ \text{gerade } k} + \boldsymbol{i} \cdot \underbrace{\sum_{k=0}^{\infty} (-1)^k \cdot \frac{\varphi^{2k+1}}{(2k+1)!}}_{\sin(\varphi),\ \text{ungerade } k}$$

Anmerkung: $\boldsymbol{i}^0 = 1, \quad \boldsymbol{i}^1 = \boldsymbol{i}, \quad \boldsymbol{i}^2 = -1, \quad \boldsymbol{i}^3 = -\boldsymbol{i}, \quad \boldsymbol{i}^4 = \boldsymbol{i}^0 = 1$
$\Rightarrow \langle \boldsymbol{i} \rangle$ zyklische Gruppe der Ordnung 4

5.6 Bemerkung

Damit ergibt sich für $z \in \mathbb{C}$ die Darstellung $z = |z|e^{\boldsymbol{i}\varphi}, \quad \varphi$ wie in Abbildung 5.2

5.7 Bemerkung

$e^{\boldsymbol{i}\varphi}$ liegt für $\varphi \in \mathbb{R}$ auf dem Einheitskreis, d.h. $\varphi \to e^{\boldsymbol{i}\varphi}$ ist Kreisfunktion. Für Frequenzanalyse (Fourierreihen):
t... Zeit, $\omega \in \mathbb{Z}$... Frequenz.
Dann beschreibt $e^{\boldsymbol{i}(t \cdot 2\pi)\omega}$ eine Schwingung, z.B.:

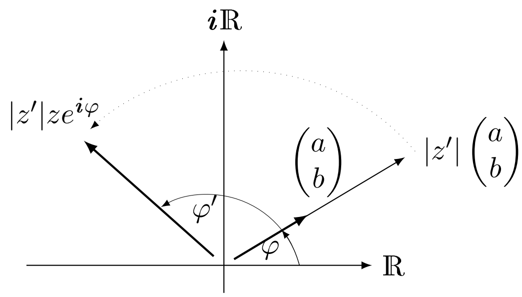
- $\omega = 1$: in einer Zeiteinheit (ZE) wird Einheitskreis 1 mal durchlaufen
- $\omega = k$: in einer ZE wird Einheitskreis k mal durchlaufen

Verknüpfungen auf $\mathbb{C}$

1) $(\mathbb{C}, +) \cong (\mathbb{R}^2, +)$, d.h. $(a + b\boldsymbol{i})(a' + b'\boldsymbol{i}) = (a + a') + (b + b')\boldsymbol{i}$ (Vektoraddition)

2) Wie wählt man Multiplikation, so daß $\mathbb{C}$ Körper wird?
Man möchte, dass Potenzregel gilt, z.B:
$e^{\boldsymbol{i}\varphi} \cdot e^{\boldsymbol{i}\varphi'} = e^{\boldsymbol{i}(\varphi+\varphi')} \Leftrightarrow$
$(\cos\varphi + \boldsymbol{i}\sin\varphi)(\cos\varphi' + \boldsymbol{i}\sin\varphi') = \cos(\varphi+\varphi') + \boldsymbol{i}\sin(\varphi+\varphi')$
Damit scheidet die komponentenweise Multiplikation aus. Mit den üblichen Rechenregeln aus $\mathbb{R}$:
$(\cos\varphi + \boldsymbol{i}\sin\varphi)(\cos\varphi' + \boldsymbol{i}\sin\varphi') =$
$\underbrace{\cos\varphi\cos\varphi' - \sin\varphi\sin\varphi'}_{\cos(\varphi+\varphi')} + \boldsymbol{i}\underbrace{(\sin\varphi\cos\varphi' + \cos\varphi\sin\varphi')}_{\sin(\varphi+\varphi')}$

Für $z = a + b\boldsymbol{i} = |z|e^{\boldsymbol{i}\varphi}$ und $z' = a' + b'\boldsymbol{i} = |z'|e^{\boldsymbol{i}\varphi'}$ ist das Produkt $zz' = z|z|e^{\boldsymbol{i}\varphi'} = |z'||z|e^{\boldsymbol{i}(\varphi+\varphi')}$ eine Drehstreckung des Vektors $\begin{pmatrix} a \\ b \end{pmatrix}$



3) Die Inverse einer Drehstreckung $re^{\boldsymbol{i}\varphi}$ ist dann eine Stauchung $\frac{1}{\varphi}$ verknüpft mit einer Drehung um $-\varphi$:
$z = re^{\boldsymbol{i}\varphi} \Leftrightarrow z^{-1} = \frac{1}{r}e^{\boldsymbol{i}-\varphi}$, da $zz^{-1} = r\frac{1}{r}e^{\boldsymbol{i}(\varphi-\varphi)} = 1 \cdot e^0 = 1$

In der Schreibweise $z = a + b\boldsymbol{i}, \quad z' = a' + b'\boldsymbol{i}$ ergibt sich:
$zz' = (a + b\boldsymbol{i})(a' + b'\boldsymbol{i}) = aa' - bb' + (ab' + ba')\boldsymbol{i}$, denn
$a = r\cos\varphi, \quad b = r\sin\varphi, \quad a' = r'\cos\varphi', \quad b' = r'\sin\varphi'$.

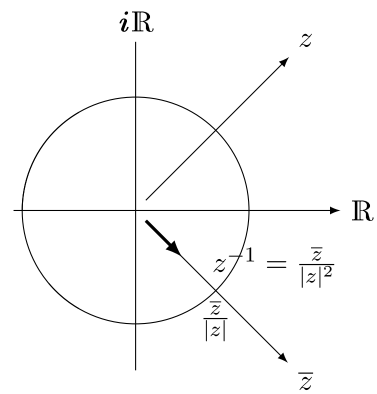
Für $z = a + b\boldsymbol{i} \in \mathbb{C}$ ist die Inverse
$z^{-1} = \frac{1}{a+b\boldsymbol{i}} = \frac{a-b\boldsymbol{i}}{(a+b\boldsymbol{i})(a-b\boldsymbol{i})} = \frac{a-b\boldsymbol{i}}{a^2-\boldsymbol{i}^2b^2} = \frac{a-b\boldsymbol{i}}{a^2+b^2}$

5.8 Definition

Falls $z = a + b\boldsymbol{i} \in \mathbb{C}$, heißt $\bar{z} := a - b\boldsymbol{i}$ die zu z Konjugierte.

5.9 Bemerkung

- Es folgt $z^{-1} = \frac{\bar{z}}{|z|^2}$
- $z \cdot \bar{z} = |z|^2 \in \mathbb{R}$



5.10 Satz

$(\mathbb{C}, +, \cdot)$ mit

- $(a + b\boldsymbol{i}) + (a' + b'\boldsymbol{i}) = (a + a') + (b + b')\boldsymbol{i}$ und
- $(a + b\boldsymbol{i})(a' + b'\boldsymbol{i}) = aa' - bb' + (ab' + a'b)\boldsymbol{i}$

ist ein Körper.

Nullelement: $\mathcal{O} = 0 + 0\boldsymbol{i}$
Einselement: $\mathbb{1} = 1 + 0\boldsymbol{i}$

Beweis

Nachrechnen. $\square$

Beispiel

- $(1 + \boldsymbol{i}) = \sqrt{2}e^{\boldsymbol{i} \cdot \frac{\pi}{4}}$
- $(2 + \boldsymbol{i})(3 - 4\boldsymbol{i}) = 6 + 4 + (3 - 8)\boldsymbol{i} = 10 - 5\boldsymbol{i}$
- $\frac{\boldsymbol{i}+1}{2\boldsymbol{i}-1} = \frac{(\boldsymbol{i}+1)(2\boldsymbol{i}+1)}{\underbrace{(2\boldsymbol{i} - 1)}_{z}\underbrace{(2\boldsymbol{i} + 1)}_{\bar{z}}} = \frac{1-2+\boldsymbol{i}(2+1)}{2^2+1^2} = -\frac{1}{5} + \frac{3}{5}\boldsymbol{i}$

5.11 Rechenregeln (Konjunktion, Betrag)

$w, z \in \mathbb{C}$

a) $\overline{w \pm z} = \overline{w} \pm \overline{z}$
$\overline{w \cdot z} = \overline{w} \cdot \overline{z}$
$\bar{\bar{z}} = z$
$\Rightarrow z \mapsto \bar{z}$ Körperisomorphismus

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

c) $|z| \geq 0$, $|z| = 0 \Leftrightarrow z = 0$ (positive Definitheit)

d) $|z| = |\bar{z}| = \sqrt{z\bar{z}}$

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

f) $|w + z| \leq |w| + |z|$ Dreiecksungleichung
$|w - z| \geq |w| - |z|$ (Beweis: Übung)

5.12 Bemerkung

a) Alternative Konstruktion von $\mathbb{C}$.:
4.40: $\mathcal{K}[x]_n$ wird Körper, wenn man durch irreduzibles Polynom f vom Grad n teilt (Modulorechnung).
Mit $\mathcal{K} = \mathbb{R}$, $n = 2$, $f = x^2 + 1$ ist

$$\begin{aligned}(a + bx) \odot_f (a' + b'x) &= aa' + bb'x^2 + (ab' + ba')x \quad \bmod f \\ &= (aa' - bb') + (ab' + ba')x\end{aligned}$$

Statt x schreibt man $\boldsymbol{i}$, $\boldsymbol{i}^2 = -1$

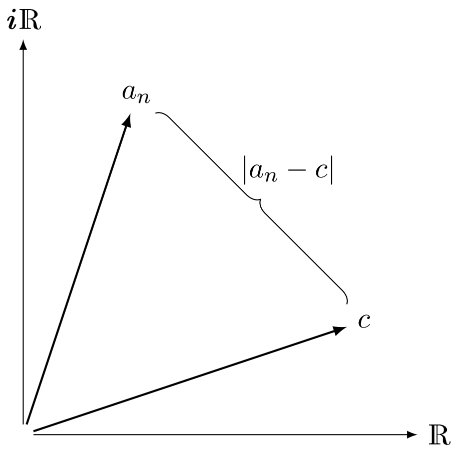
b) $x^2 + 1 = (x - \boldsymbol{i})(x + \boldsymbol{i})$ ist nicht irreduzibel in $\mathbb{C}[x]$.
Tatsächlich besitzt in $\mathbb{C}$ jede quadratische Gleichung 2 Lösungen.

Allgemein: Fundamentalsatz der Algebra:
$f \in \mathbb{C}[x]$, $a_n x^n$ Leitterm, $n \geq 1$.
$\Rightarrow f$ hat genau n Nullstellen $b_1, ..., b_n$ (nicht notw. verschieden) mit
$f = a_n(x - b_1) \cdot ... \cdot (x - b_n)$
Das heißt, lineare Polynome $ax+b$ mit $a \neq 0$ sind die einzigen Primelemente in $\mathbb{C}[x]$.

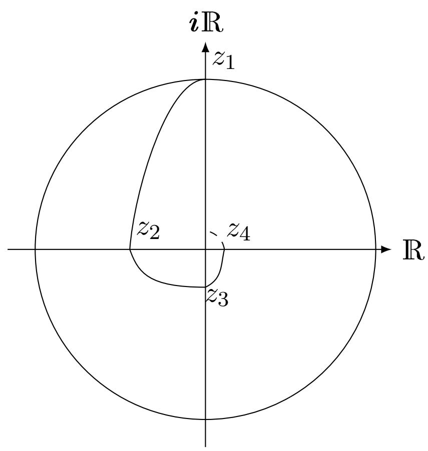
20.12.2016

c) Wurzelberechnung: $z = |z|(\cos\varphi + i\sin\varphi)$
$\Rightarrow \pm\sqrt{z} = \pm\sqrt{|z|}(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2})$, da
$(e^{i\psi})^2 = e^{i2\psi} = e^{i\psi} \cdot e^{i\psi}$

d) Übertragung des Grenzwertes von Folgen/Funktionen in $\mathbb{R}$ auf Folgen in $\mathbb{C}$:



$a_n \to c, \quad a_n, c \in \mathbb{C} \Leftrightarrow \forall \epsilon > 0\ \exists n_0 \in \mathbb{N}\ \forall n \geq n_0 : \quad \underbrace{|a_n - c|}_{\text{Abstand von a und c}} \quad < \epsilon$



$z_n = \frac{1}{n} e^{in\frac{\pi}{2}} \Rightarrow z_n \overset{n\to\infty}{\to} 0$

$z_1 = e^{\boldsymbol{i}\frac{\pi}{2}} = \boldsymbol{i}$
$z_2 = \frac{1}{2} e^{\boldsymbol{i}\pi} = -0.5$
...

- Konvergenz von Reihen in $\mathbb{C}$
- Aus absoluter Konvergenz folgt Konvergenz (mit $\triangle$-Ungleichung)
  $\sum_{n=1}^{\infty} z_n$ ist absolut konvergent, wenn $\sum_{n=1}^{\infty} |z_n|$ konvergiert.
  Beispiel: $\underbrace{\sum_{k=0}^{\infty} \frac{z^k}{k!}}_{\text{später } = e^z}$ konvergiert $\forall z \in \mathbb{C}$, insbesondere für $z = \boldsymbol{i}\varphi$ (5.5)

e) $\mathbb{C}$ hat alle analytischen Eigenschaften von $\mathbb{R}$, außer:
Auf $\mathbb{C}$ gilt es keine vollständige Ordnung $\leq$, die mit $+$ und $\cdot$ verträglich wäre, d.h. für die gelten würde

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

Wdh. zu $\mathbb{C}$ (falls Skizzen aus der Vorlesung gewünscht: Mail schreiben, wird dann hinzugefügt)

- Komplexe Zahl: $z = a + bi, a, b \in \mathbb{R}, i^2 = -1$
  Im Folgenden ist $z = a + bi, z' = a' + b'i \in \mathbb{C}$
  z.B. $x^2 + 2x + 3$ hat in $\mathbb{C}$ Nst.
  $x_{1/2} = \frac{-2 \pm \sqrt{4-12}}{2} = -1 \pm \sqrt{2}i$

- Es gibt 2 Darstellungen:

  1) $z = a + bi, z.B. z = 2 + 2i$
     $|z| = \sqrt{a^2 + b^2} = \sqrt{8}$
  2) Polarkoordinaten:
     $z = |z|e^{i\varphi}\ z^* = \cos(\frac{\pi}{4}) \cdot i \sin(\frac{\pi}{4}) = e^{i\frac{\pi}{4}}$
     $\Rightarrow z = |z|z^* = \sqrt{8}e^{i\frac{\pi}{4}}$

- Formel von Euler $e^{i\varphi} = \cos(\varphi) + i \sin(\varphi)$

- Addition: $z + z' = a + a' + (b + b')i$
  Man sieht hier : $|z + z'| \leq |z| + |z'|$

- Multiplikation:

$$\begin{aligned} zz' &= (a + bi)(a' + b'i) \\ &= aa' - bb' + (ab' + a'b)i \\ &= |z||z'|e^{i\varphi}e^{i\varphi'} \\ &= |z||z'|e^{i(\varphi+\varphi')} \end{aligned}$$

- (Drehstreckung)
  z.B.:
  $1 + i = \sqrt{2}e^{i\frac{\pi}{4}}$
  $\frac{1}{2} + \frac{\sqrt{3}}{2}i = e^{i\frac{\pi}{3}}$
  $(1 + i)(\frac{1}{2} + \frac{\sqrt{3}}{2}i) = \frac{1-\sqrt{3}}{2} + \frac{1+\sqrt{3}}{2}i = \sqrt{2}e^{i(\frac{7\pi}{12})}$
  (Drehung um 60° von $1 + i$)

- $\bar{z} = a - bi$
  $z\bar{z} = (a+bi)(a-bi) = a^2 + b^2 = |z|^2$
  z.B. $z = 1 + 3i, \bar{z} = 1 - 3i, z\bar{z} = 1 + 9 \Rightarrow |z| = \sqrt{10}$

6 Lineare Abbildungen

Bemerkung

Ein $\mathcal{K}-$VR besitzt Skalare $\lambda \in \mathcal{K}$, $\mathcal{K}$ Körper.
Bisher $\mathcal{K} = \mathbb{R}$.
Speziell: $\mathcal{K}^n = \{v = (v_1, ..., v_n) \mid v_i \in \mathcal{K} \;\; \forall i = 1, ..., n\}$ ist $\mathcal{K}-$Vektorraum.
$\mathbb{Z}_2^2$ ist $\mathbb{Z}_2-$Vektorraum:
$\mathbb{Z}_2^2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$

- $v + w = \begin{pmatrix} v_1 + w_1 \mod 2 \\ v_2 + w_2 \mod 2 \end{pmatrix} \qquad v, w \in \mathbb{Z}_2^2$
- $\lambda v = \begin{pmatrix} \lambda v_1 \mod 2 \\ \lambda v_2 \mod 2 \end{pmatrix} \qquad \lambda \in \mathbb{Z}_2, \quad v \in \mathbb{Z}_2^2$
- Nullelement: $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$

6.1 Definition

V, W $\mathcal{K}-$Vektorräume.

i) $\varphi : V \to W$ heißt lineare Abbildung, falls

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

   b) $\varphi(\lambda v) = \lambda \varphi(v) \quad \forall v \in V \;\; \forall \lambda \in \mathcal{K}$

ii) Ist die lineare Abbildung $\varphi : V \to W$ bijektiv, so heißt φ (Vektorraum-)Isomorphismus, man schreibt $V \cong W \quad (V$ isomorph zu $W)$

Bemerkung

Erfüllt φ Bedingung i), so heißt φ auch (Vektorraum-)Homomorphismus.

6.2 Bemerkung

i) $\varphi(\mathcal{O}) = \mathcal{O}$

ii) $\varphi(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i \varphi(v_i)$

6.3 Beispiel

a) Nullabbildung $\varphi : V \to W, \quad v \mapsto \mathcal{O}$ linear

b) $\varphi : V \to V, \quad v \mapsto \mu v$ für festes $\mu \in \mathcal{K}$ linear

c) $\varphi : \mathbb{R}^3 \to \mathbb{R}^3, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_2 \\ -x_3 \end{pmatrix}$ Spiegelung an x_1x_2- Ebene, linear

d) $\varphi : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1^2 \\ x_2 \end{pmatrix}$ nicht linear [$x \mapsto x^2$ nicht linear]

6.4 Bemerkung

$A \in \mathcal{M}_{m,n}(\mathcal{K}), \quad \mathcal{K}$ Körper $\overset{2.6}{\Rightarrow} \varphi : \mathcal{K}^n \to \mathcal{K}^m, \quad v \mapsto Av$ linear
Zeigen später: Alle linearen Abbildungen $\varphi : \mathcal{K}^n \to \mathcal{K}^m$ lassen sich durch Matrix $A \in \mathcal{M}_{m,n}(\mathcal{K})$ darstellen.

Kern und Rang

Motivation

Gegeben: LGS $Ax = b$ mit $A \in \mathcal{M}_{m,n}(\mathcal{K}), \quad b \in \mathcal{K}^m$
Gesucht: Lösung $x \in \mathcal{K}^n$
z.B.: $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}$

Spezielle Lösung: $x_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. Da $A \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, ist auch

$$\underbrace{A \begin{pmatrix} 1 \\ 0 \\ \lambda \end{pmatrix}}_{\text{Gerade}} = A\left(x_0 + \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix} \right) = \underbrace{Ax_0}_{b} + \underbrace{A \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix}}_{\mathcal{O}} = b \Rightarrow \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix} \text{ ist Lösung von } Ax = b$$

$$\Rightarrow H' = \left\{ \begin{pmatrix} 1 \\ 0 \\ \lambda \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\}, \quad H = \left\{ \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\} \text{ (s.u.)}$$

6.5 Definition

$Ah = \mathcal{O}, \quad h \in \mathcal{K}^n$ heißt homogenes LGS.

$\underbrace{H}_{\ker A\text{ , vgl. 6.8}} := \{h \in \mathcal{K}^n \mid Ah = \mathcal{O}\}$ Lösungsraum des homogenen LGS.

6.6 Satz

21.12.2016

Angenommen, es existiert eine Lösung x_0 von $Ax = b$. Dann ist
x Lösung $\Leftrightarrow x = x_0 + h, \quad h \in H$

Beweis

($\Rightarrow$) x Lösung $\Rightarrow \mathcal{O} = Ax - Ax_0 = A(\underbrace{x - x_0}_{=:h}) \Rightarrow h \in H$

($\Leftarrow$) $x = x_0 + h, \quad h \in H \Rightarrow Ax = A(x_0 + h) = Ax_0 + \underbrace{Ah}_{=\mathcal{O}} = b$ $\square$

Bemerkung

- Wenn x Lösung von $Ax = b$, so setzt sich x zusammen aus spezieller Lösung x_0+Lösung von homogenem LGS.
- Anzahl Lösungen von $Ax = b$ ist gleich der Anzahl der Lösungen von $Ax = \mathcal{O}$ dim(Lösungsraum) = dim(H)
- H heißt Kern von A

6.7 Satz

$\varphi : V \to W$ linear

i) $U \leq V$ UVR $\Rightarrow \underbrace{\varphi(U)}_{\text{Bild von } U} \leq W$ UVR von W.

ii) $\dim\,(U) < \infty \Rightarrow \dim\,(\varphi(U)) \leq \dim\,(U)$

Beweis

i) – $\mathcal{O} \in U \Rightarrow \varphi(\mathcal{O}) = \mathcal{O} \in \varphi(U)$
– $v, w \in U \Rightarrow \varphi(v) + \varphi(w) = \varphi(\underbrace{v + w}_{\in U}) \in \varphi(U)$

- $\lambda \in \mathcal{K}, \quad v \in U \Rightarrow \lambda\varphi(v) = \varphi(\underbrace{\lambda v}_{\in U}) \in \varphi(U)$

ii) $\varphi : V \to W$ linear
$\{u_1, ..., u_k\}$ Basis von U $[u \in U \Rightarrow u = \lambda_1 u_1 + ... + \lambda_k u_k]$
$\Rightarrow \{\varphi(u_1), ..., \varphi(u_k)\}$ Erzeugendensystem von U, enthält Basis von U $\Rightarrow$ Behauptung □

6.8 Definition

i) $\varphi : V \to W$ linear, $\dim(V) < \infty$.
Dann heißt $\dim(\underbrace{\varphi(V)}_{\text{UVR wegen 6.7}})$ Rang von φ, $\text{rg}(\varphi)$.
Im Beispiel (Motivation) ist $\text{rg}(A) = 2$, weil die Matrix auf eine Ebene abbildet.

$$Av = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix} v_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ a_{32} \end{pmatrix} v_2 + \underbrace{\begin{pmatrix} a_{13} \\ a_{23} \\ a_{33} \end{pmatrix}}_{\mathcal{O}} v_3$$

ii) $\varphi : V \to W$ linear.
$\ker(\varphi) = \{v \in V \mid \varphi(v) = \mathcal{O}\}$ heißt Kern von φ.
Im Beispiel (Motivation) ist $H = \left\{ \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix} \middle| \lambda \in \mathbb{R} \right\} = \ker(A)$, da jeder Gerade dieser Form auf den Nullvektor, $\mathcal{O}$, abgebildet wird.

6.9 Satz

$\varphi : V \to W$ linear

i) $\ker(\varphi)$ ist UVR von V

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

Beweis

i)
- $\varphi(\mathcal{O}) = \mathcal{O} \Rightarrow \mathcal{O} \in \ker(\varphi)$
- $u, v \in \ker(\varphi) \Rightarrow \underbrace{\varphi(u)}_{=\mathcal{O}} + \underbrace{\varphi(v)}_{=\mathcal{O}} = \mathcal{O} = \varphi(u + v) \Rightarrow u + v \in \ker(\varphi)$
- $\lambda \in \mathcal{K}, v \in \ker(\varphi) \Rightarrow \mathcal{O} = \lambda\varphi(v) = \varphi(\lambda v) \Rightarrow \lambda v \in \ker(\varphi)$

ii) (⇒) φ injektiv, $\varphi(\mathcal{O}) = \mathcal{O}$.
Da φ injektiv, kannn kein weiteres Element auf $\mathcal{O}$ abgebildet werden.

(⇐) Angenommen, $\varphi(v_1) = \varphi(v_2) \quad v_1, v_2 \in V$
$\Rightarrow \mathcal{O} = \varphi(v_1) - \varphi(v_2) = \varphi(v_1 - v_2)$
$\Rightarrow v_1 - v_2 = \mathcal{O}$, da $\ker(\varphi) = \{\mathcal{O}\}$
$\Rightarrow v_1 = v_2$ □

6.10 Beispiel

$$A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \varphi : \mathbb{R}^3 \to \mathbb{R}^3, \quad x \mapsto Ax$$

- $\mathbb{R}^3 = \langle e_1, e_2, e_3 \rangle_{\mathbb{R}} \Rightarrow \varphi(\mathbb{R}^3) = \langle \varphi(e_1), \varphi(e_2), \varphi(e_3) \rangle_{\mathbb{R}} = \left\langle \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\rangle_{\mathbb{R}} =$
  $\left\langle \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} \right\rangle_{\mathbb{R}}$
  $\Rightarrow \mathrm{rg}(\varphi) = 2$

- $\varphi(x) = \mathcal{O} \Leftrightarrow Ax = \mathcal{O} \Leftrightarrow x = \begin{pmatrix} 0 \\ 0 \\ \lambda \end{pmatrix}, \quad \lambda \in \mathbb{R}$

  $\ker(\varphi) = H = \left\{ \lambda \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\}$

Bemerkung

$\dim(\ker(\varphi))$	$+\mathrm{rg}(\varphi)$	$= \dim(\mathbb{R}^3)$
1	+2	=3

6.11 Satz

V, W sind $\mathcal{K}-$Vektorräume, $\dim(V) = n$
Gegeben: $\{v_1, ..., v_n\}$ Basis von V, $w_1, ..., w_n \in W$ nicht notw. verschieden

$\exists!$ lin.Abb. $\varphi : V \to W$ mit $\varphi(v_i) = w_i \; \forall i$,
und zwar

$$(\triangle) \qquad v = \sum_{i=1}^{n} \lambda_i v_i \xrightarrow{\varphi} w = \sum_{i=1}^{n} \lambda_i \underbrace{\varphi(v_i)}_{w_i}$$

Das heißt: Wenn man weiß, wie die Basisvektoren abgebildet werden, dann kennt man die lineare Abbildung vollständig. (vgl. Bemerkung 2.5 + Beispiel 2.4b))

Beweis

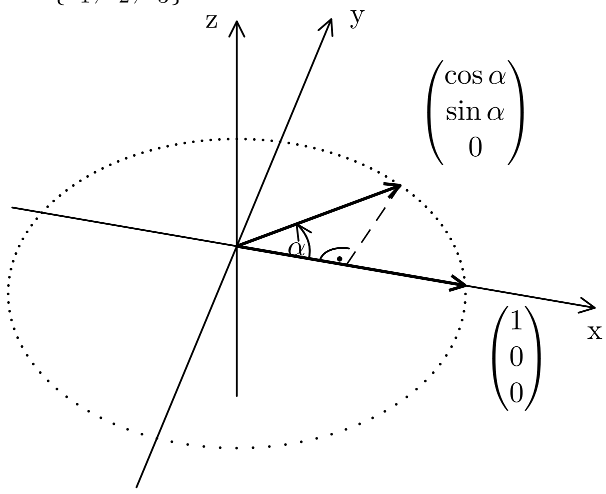
Für φ aus $(\triangle)$ gilt:

- φ linear ✓
- $\varphi(v_i) = w_i \ \forall i$✓
- φ eindeutig: Angenommen es gibt $\psi : V \to W$ linear mit $\psi(v_i) = w_i \Rightarrow$
  $\psi\Bigl(\underbrace{\sum_{i=1}^{n} \lambda_i v_i}_{v}\Bigr) = \sum_{i=1}^{n} \lambda_i \underbrace{\psi(v_i)}_{=w_i} = \varphi\Bigl(\underbrace{\sum_{i=1}^{n} \lambda_i v_i}_{v}\Bigr)$

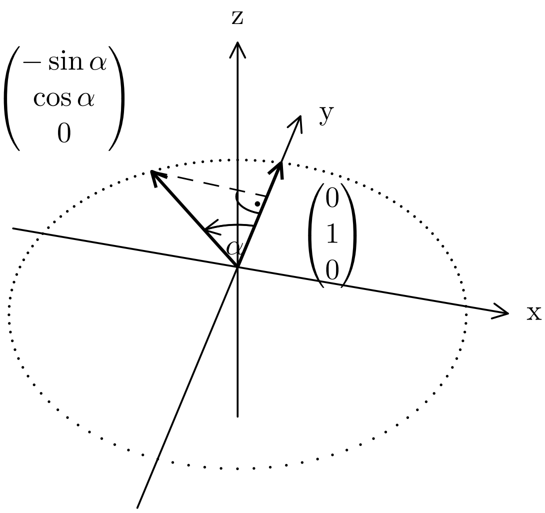
$\square$

6.12 Beispiel

$\varphi : \mathbb{R}^3 \to \mathbb{R}^3$ Drehung um Winkel α um $z-$Achse.
$B = \{e_1, e_2, e_3\}$



$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} \cos\alpha \\ \sin\alpha \\ 0 \end{pmatrix}$$



$$\begin{pmatrix}-\sin\alpha\\ \cos\alpha\\ 0\end{pmatrix} \qquad \begin{pmatrix}0\\1\\0\end{pmatrix}$$

$$\begin{pmatrix}0\\1\\0\end{pmatrix} \overset{\varphi}{\to} \begin{pmatrix}-\sin\alpha\\ \cos\alpha\\ 0\end{pmatrix}$$

$$\begin{pmatrix}0\\0\\1\end{pmatrix} \overset{\varphi}{\to} \begin{pmatrix}0\\0\\1\end{pmatrix}$$

$$A = (Ae_1,\ Ae_2,\ Ae_3) = \begin{pmatrix}\cos\alpha & -\sin\alpha & 0\\ \sin\alpha & \cos\alpha & 0\\ 0 & 0 & 1\end{pmatrix}, \text{ vgl. Bsp. 2.4b}$$

6.13 Beispiel

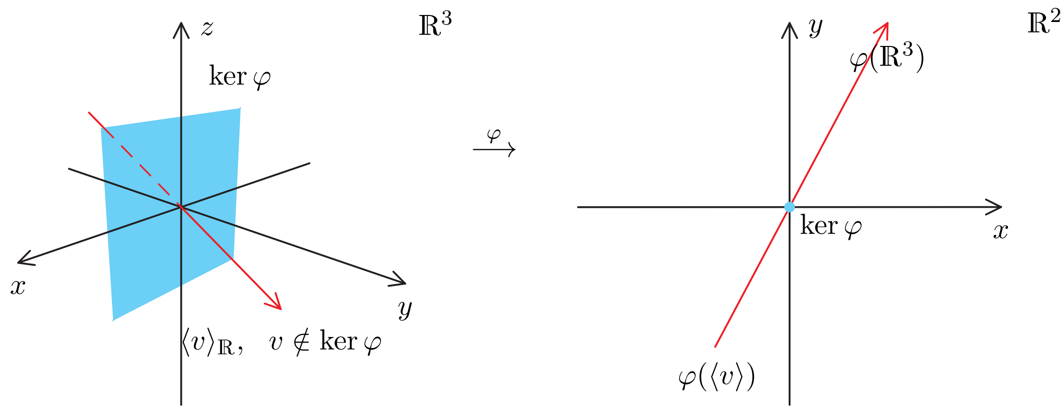
10.01.2017

$\varphi : \mathbb{R}^3 \to \mathbb{R}^2, \quad v \mapsto Av, \quad A = \begin{pmatrix}1 & 2 & 0\\ 2 & 4 & 0\end{pmatrix}$

- $\ker(\varphi) = \left\langle \begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}2\\-1\\0\end{pmatrix} \right\rangle_{\mathbb{R}}$
- Bild von $\mathbb{R}^3$:

$$\begin{aligned}\varphi(\mathbb{R}^3) &= \langle \varphi(e_1), \varphi(e_2), \varphi(e_3)\rangle_{\mathbb{R}}\\ &= \left\langle \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\4\end{pmatrix}, \begin{pmatrix}0\\0\end{pmatrix} \right\rangle_{\mathbb{R}}\\ &= \left\langle \begin{pmatrix}1\\2\end{pmatrix} \right\rangle_{\mathbb{R}}\end{aligned}$$

  - $\varphi : \ker(\varphi) \to \{\mathcal{O}\}$
  - $v \notin \ker(\varphi) \Rightarrow \varphi(v) \neq 0$



6.14 Satz (Dimensionsformel)

V, W $\mathcal{K}-$Vektorräume, $dim(V) = n$, $\varphi : V \to W$ lineare Abbildung.
Dann ist

$$\dim(V) = \underbrace{\dim(\ker\varphi)}_{\text{'Defekt von }\varphi'} + \operatorname{rg}(\varphi)$$

Beweis:

Sei $\{u_1, ..., u_k\}$ Basis von $\ker\varphi$. Ergänze zu Basis $\{u_1, ..., u_n\}$ von V und setze $U := \langle u_{k+1}, ..., u_n\rangle_{\mathcal{K}}$
Da $\ker\varphi \cap U = \{\mathcal{O}\}$ und $V = U + \ker\varphi$, ist

$$\dim(V) = \dim(\ker\varphi) + \dim(U) - \underbrace{\dim(U \cap \ker\varphi)}_{=0}$$

Zeige: $\dim(U) \overset{1)}{=} \dim(\varphi(U)) \overset{2)}{=} \underbrace{\dim(\varphi(V))}_{\operatorname{rg}(\varphi)}$

1)

$$\begin{aligned}\ker\varphi \cap U = \{\mathcal{O}\} &\Rightarrow \ker(\varphi/_U) = \{\mathcal{O}\}\\ &\overset{6.9}{\Rightarrow} \varphi/_U \text{ injektiv}\\ &\Rightarrow \dim(U) = \dim(\varphi(U))\end{aligned}$$

$$\left[\text{Bem:}\quad \{u_{k+1,\dots,u_n}\}\text{Basis von } U \quad \overset{\varphi/_U \text{ injektiv}}{\Rightarrow} \{\varphi(u_{k+1}),\dots,\varphi(u_n)\} \text{ Basis von } \varphi(U)\right]$$

2)

$$\begin{aligned}\dim(\varphi(U)) &= \dim(\varphi(V)),\ \text{da}\\ \varphi(V) &= \varphi(U + \ker(\varphi))\\ &\overset{\varphi \text{ linear}}{=} \varphi(U) + \underbrace{\varphi(\ker(\varphi))}_{\{\mathcal{O}\}}\\ &= \varphi(U)\end{aligned}$$

6.15 Korollar

V, W $\mathcal{K}-$Vekorräume mit $\dim(V) = \dim(W) = n$, $\varphi : V \to W$ lineare Abbildung.
Dann sind äquivalent:

i) φ surjektiv,

ii) φ injektiv,

iii) φ bijektiv.

Beweis

$6.14 \Rightarrow n = \dim(\ker\varphi) + \mathrm{rg}\varphi$
φ surjektiv $\Leftrightarrow \mathrm{rg}\varphi = n \Leftrightarrow \dim(\ker\varphi) = 0 \overset{6.9}{\Leftrightarrow} \varphi$ injektiv $\square$

Lösungen von LGS, Rang von Matrizen

Gegeben: LGS mit $Ax = b$, $A \in \mathcal{M}_{m,n}(\mathcal{K})$, $b \in \mathcal{K}^m$, $\mathcal{K}$ Körper.
Gesucht: $\mathcal{L} := \{x \in \mathcal{K}^n \mid Ax = b\}$ Lösungsraum

Sei $x_0 \in \mathcal{L}$ eine spezielle Lösung.
$\overset{6.6}{\Rightarrow} \mathcal{L} = x_0 + \ker\varphi, \quad \varphi : \mathcal{K}^n \to \mathcal{K}^m, \quad x \mapsto Ax$
D.h. Größe von $\mathcal{L}$ gegeben durch $\dim(\ker\varphi)$.

6.16 Bemerkung

$\dim(\ker\varphi) = n - \underbrace{\mathrm{rg}\varphi}_{=\dim(\varphi(\mathcal{K}^n))}$ (6.14)

$\varphi(\mathcal{K}^n) = \langle \varphi(e_1), ..., \varphi(e_n)\rangle_{\mathcal{K}} = \langle \underbrace{Ae_1, ...Ae_n}_{\text{Spalten von } A}\rangle_{\mathcal{K}}$

$\Rightarrow$ rgφ = Anzahl der linear unabhängigen Spalten von A = Spaltenrang von A

Man kann zeigen: Spaltenrang von A = Zeilenrang von A (Anzahl linear unabhängiger Zeilen von A)
Insgesamt: $\dim(\ker\varphi) = n-$ Spaltenrang von $A = n-$ Zeilenrang von A

7 Lineare Abbildungen und Matrizen

Erinnerung

(1.29): Ein Vektor hat bezüglich unterschiedlicher Basen unterschiedliche Linearkombinationen und damit auch unterschiedliche Koordinaten, z.B.
$v = \begin{pmatrix} 4 \\ 3 \end{pmatrix} \in \mathbb{R}^2$ hat bezüglich $B = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$ die Linearkombination $\begin{pmatrix} 4 \\ 3 \end{pmatrix} = \underbrace{3}_{\lambda_1} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \underbrace{1}_{\lambda_2} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, das heißt $\lambda_1 = 3$ und $\lambda_2 = 1$ sind die Koordinaten von v bezüglich der Basis B. Bezüglich der Standardbasis hat v die Koordinaten $\begin{pmatrix} 4 \\ 3 \end{pmatrix} = \underbrace{4} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \underbrace{3} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

7.1 Definition (Koordinatenvektor)

V $\mathcal{K}-$Vektorraum, $B \subseteq V$ Basis, $B = \{v_1, ..., v_n\}$.

Wenn $v \in V$ und $v = \lambda_1 v_1 + ... + \lambda_n v_n$, dann heißt $\mathrm{K}_B(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \mathcal{K}^n$

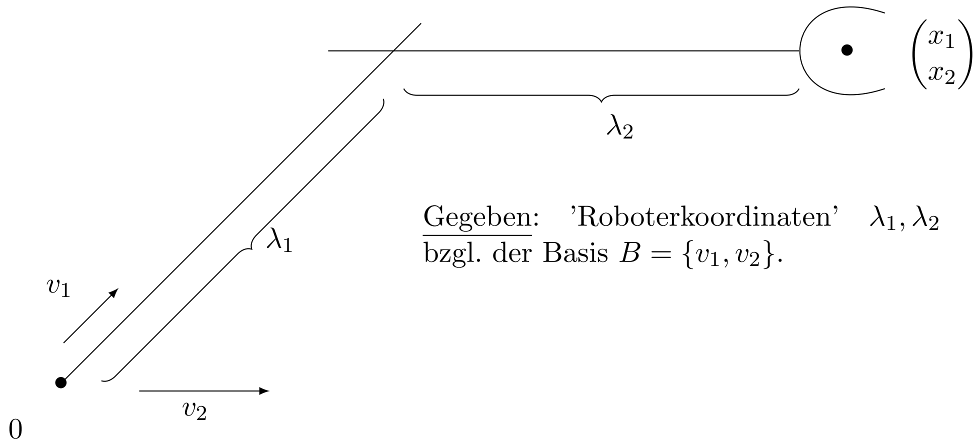
Koordinatenvektor von v bezüglich der Basis B.

$$\left[\text{Im Beispiel oben ist } \mathrm{K}_B\left(\begin{pmatrix} 4 \\ 3 \end{pmatrix} \right) = \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix}. \right]$$

Basistransformationen

Umrechnung von Koordinaten bezüglich verschiedener Basen.

7.2 Beispiel



<u>Gegeben</u>: 'Roboterkoordinaten' λ_1, λ_2 bzgl. der Basis $B = \{v_1, v_2\}$.

1) <u>Gesucht</u>: 'Weltkoordinaten' $(x_1, x_2)^T$ bzgl. Basis $C = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$.

   Es ist $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix}$

   Mit z.B.: $\lambda_1 = 3, \quad \lambda_2 = 1$:

$$\Rightarrow \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}_{\substack{\text{Basiswechselmatrix} \\ S_{BC}\ (7.3)}} \cdot \underbrace{\begin{pmatrix} 3 \\ 1 \end{pmatrix}}_{\substack{\text{Koordinaten} \\ \text{bzgl. } B}} = \underbrace{\begin{pmatrix} 4 \\ 3 \end{pmatrix}}_{\substack{\text{Koordinaten bzgl. } C, \\ \text{Position des Greifarms}}}$$

11.01.2017

2) <u>Gesucht</u>: Koordinaten μ_1, μ_2 bezüglich Basis $D = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right\}$.

   Es ist $\mu_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \mu_2 \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

   $\lambda_1 = 1, \quad \lambda_2 = 0 : \begin{pmatrix} 1 \\ 1 \end{pmatrix} = (-1) \begin{pmatrix} 1 \\ 2 \end{pmatrix} + 1 \begin{pmatrix} 2 \\ 3 \end{pmatrix}$

   $\lambda_1 = 0, \quad \lambda_2 = 1 : \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (-3) \begin{pmatrix} 1 \\ 2 \end{pmatrix} + 2 \begin{pmatrix} 2 \\ 3 \end{pmatrix}$

   Daraus ergibt sich in Matrixschreibweise:

$$\underbrace{\begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix}}_{\substack{\text{Basiswechselmatrix} \\ S_{B,D}}} \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}$$

Z.B.: $\lambda_1 = 3, \quad \lambda_2 = 1 \Rightarrow \begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} -6 \\ 5 \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix}$ = Koordinaten (-vektor) bzgl. D

7.3 Definition (Basiswechselmatrix)

V Vektorraum, $B = \{v_1, ..., v_n\}, \quad C = \{w_1, ..., w_n\}$ Basen von V.
Schreibe v_i als Linearkombination der Vektoren aus C :
$v_1 = s_{11}w_1 + ... + s_{n1}w_n$
$\vdots$
$v_n = s_{1n}w_1 + ... + s_{nn}w_n$

Dann heißt die Matrix $S_{B,C} = \begin{pmatrix} s_{11} & \cdots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{n1} & \cdots & s_{nn} \end{pmatrix}$ <u>Basiswechselmatrix von Basis B nach C</u>.
Spalte i enthält die Koordinaten von v_i bzgl. C.

7.4 Satz (Koordinaten umrechnen)

V, B, C wie in 7.3.

Für $v \in V$ ist $\mathrm{K}_C(v) = S_{BC} \cdot \mathrm{K}_B(v)$

Beweis

$$
\begin{aligned}
v &= \sum_{k=1}^{n} \lambda_k \cdot \underbrace{v_k}_{\sum_{l=1}^{n} S_{lk} w_l \ (7.3)} \Rightarrow \mathrm{K}_B(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \\
&= \sum_{l=1}^{n} \Big(\sum_{k=1}^{n} \lambda_k \cdot s_{lk} \Big) w_l \\
&= \mu_l \qquad \text{(Koordinaten in Basis } C\text{)}
\end{aligned}
$$

$\square$

Darstellungsmatrizen

7.5 Beispiel

Skizze: Siehe 7.2.
Roboter soll folgende Operation $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ ausführen:

$$\varphi\Big(\begin{pmatrix}x_1\\x_2\end{pmatrix}\Big) = 2\begin{pmatrix}x_1\\x_2\end{pmatrix}$$

<u>Gegeben</u>: Aktuelle Position $\begin{pmatrix}x_1\\x_2\end{pmatrix}$, $B = \Big\{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}\Big\}$, $C = \Big\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}\Big\}$

<u>Gesucht</u>: λ_1, λ_2, so dass Greifarm in neuer Position $\varphi\Big(\begin{pmatrix}x_1\\x_2\end{pmatrix}\Big) = 2\begin{pmatrix}x_1\\x_2\end{pmatrix}$.

Methode aus 7.3:

$$\left.\begin{aligned}\varphi\Big(\begin{pmatrix}1\\0\end{pmatrix}\Big) &= \begin{pmatrix}2\\0\end{pmatrix} = 0\cdot\begin{pmatrix}1\\1\end{pmatrix} + 2\begin{pmatrix}1\\0\end{pmatrix}\\ \varphi\Big(\begin{pmatrix}0\\1\end{pmatrix}\Big) &= \begin{pmatrix}0\\2\end{pmatrix} = 2\cdot\begin{pmatrix}1\\1\end{pmatrix} - 2\begin{pmatrix}1\\0\end{pmatrix}\end{aligned}\right\}\to \text{Matrixschreibweise:}$$

$$\underbrace{\begin{pmatrix}0 & 2\\2 & -2\end{pmatrix}}_{A_\varphi^{C,B}\ \text{(Def. 7.6)}} \cdot \underbrace{\begin{pmatrix}x_1\\x_2\end{pmatrix}}_{\text{aktuelle Pos. bzgl. C}} = \underbrace{\begin{pmatrix}\lambda_1\\\lambda_2\end{pmatrix}}_{\substack{\text{Koord. bzgl. B,}\\ \text{nachdem } \varphi \text{ ausgeführt wurde}}} = \mathrm{K}_B\Bigg(\varphi\Big(\begin{pmatrix}x_1\\x_2\end{pmatrix}\Big)\Bigg)$$

Z.B. Greifarm in $\begin{pmatrix}x_1\\x_2\end{pmatrix} = \begin{pmatrix}1\\3\end{pmatrix}$ soll nach $\varphi\Big(\begin{pmatrix}3\\1\end{pmatrix}\Big) = \begin{pmatrix}6\\2\end{pmatrix}$ bewegt werden. Dazu muss man λ_1, λ_2 auf $\begin{pmatrix}\lambda_1\\\lambda_2\end{pmatrix} = \begin{pmatrix}0 & 2\\2 & -2\end{pmatrix}\cdot\begin{pmatrix}3\\1\end{pmatrix} = \begin{pmatrix}2\\4\end{pmatrix}$ einstellen.

Probe: $\underbrace{\lambda_1}_{=2}\begin{pmatrix}1\\1\end{pmatrix} + \underbrace{\lambda_2}_{=4}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}6\\2\end{pmatrix} = \varphi\Big(\begin{pmatrix}3\\1\end{pmatrix}\Big)$ ✓

7.6 Definition (Darstellungsmatrix)

V, W Vektorraum endlicher Dimension mit Basen $B = \{v_1, ..., v_n\}$ von V und $C = \{w_1, ..., w_m\}$ von W. $\varphi : V \to W$ lineare Abbildung.
Schreibe $\varphi(v_i)$ als Linearkombination der Vektoren aus C:

$\varphi(v_1) = \boxed{a_{11}w_1 + \cdots + a_{m1}w_m}$

$\vdots$

$\varphi(v_n) = a_{1n}w_1 + ... + a_{mn}w_m$

Dann heißt $A_\varphi^{B,C} = \begin{pmatrix}a_{11} & \cdots & a_{1n}\\ \vdots & \ddots & \vdots\\ a_{m1} & \cdots & a_{mn}\end{pmatrix}$ <u>Darstellungsmatrix von φ</u> bzgl. B und C.

Schreibweisen:

1) $A_\varphi^{B,B} = A_\varphi^B$
2) Falls $B = \{e_1, ..., e_n\} = C$, (also $V = W$), schreibe A_φ

$$\left[\text{Bem.: } \varphi \text{ durch } A_\varphi^{B,C} \text{ eindeutig bestimmt.}\right]$$

7.7 Satz

V, W, B, C, φ wie in 7.6
Gegeben: $v \in V$, $\mathrm{K}_B(v)$.

Dann ist $\mathrm{K}_C(\varphi(v)) = A_\varphi^{B,C} \cdot \mathrm{K}_B(v)$

Beweis

- $\mathrm{K}_B(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}, \quad A_\varphi^{B,C} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$

  $A_\varphi^{B,C} \cdot \mathrm{K}_B(v) = \begin{pmatrix} \sum_{i=1}^n a_{1i}\lambda_i \\ \vdots \\ \sum_{i=1}^n a_{mi}\lambda_i \end{pmatrix}$

- $\varphi(v) = \varphi(\sum_{i=1}^n v_i\lambda_i) = \sum_{i=1}^n \lambda_i \cdot \underbrace{\varphi(v_i)}_{=\sum_{k=1}^m a_{ki}w_k \ (7.6)}$

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

$$\Rightarrow \mathrm{K}_C(\varphi(v)) = \begin{pmatrix} \sum_{i=1}^n \lambda_i a_{1i} \\ \vdots \\ \sum_{1=i}^n \lambda_i a_{mi} \end{pmatrix} \qquad \square$$

7.8 Beispiel

Gegeben: Basis $B = \{v_1, v_2, v_3\}$ von V und Basis $C = \{w_1, w_2\}$ von W,
$\varphi : V \to W$ mit $A_\varphi^{B,C} = \begin{pmatrix} 1 & 1 & -2 \\ 2 & 0 & 3 \end{pmatrix}$.
Angenommen, $v \in V$ mit $\mathrm{K}_B(v) = \begin{pmatrix} 5 \\ -2 \\ 4 \end{pmatrix}$.

$$\Rightarrow \underbrace{\mathrm{K}_C(v)}_{\substack{\text{Koordinaten bzgl. } C,\\ \text{nachdem } \varphi \text{ ausgeführt wurde}}} = \begin{pmatrix} 1 & 1 & -2 \\ 2 & 0 & 3 \end{pmatrix} \cdot \mathrm{K}_B(\varphi(v)) = \begin{pmatrix} -5 \\ 22 \end{pmatrix}$$

Bemerkung

17.01.2017

In 7.3 und 7.6 haben die Basisvektoren von $B = \{v_1, .., v_n\}$ und $C = \{w_1, ..., w_m\}$ eine bestimmte Reihenfolge (Nummerierung). Man sagt es sind <u>geordnete Basen</u> und schreibt dafür $B = (v_1, ..., v_n)$, $\quad C = (w-1, ..., w_m)$, um anzuzeigen, dass die Basiselemente nicht vertauscht werden dürfen.

Beispiel

$$B = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right), \quad C = \left(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right)$$

$$\Rightarrow S_{B,C} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \text{ da:}$$

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 0 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = 0 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

7.9 Beispiel

In 7.5 ist $A_\varphi^{C,B} = \underbrace{S_{C,B}}_{2)} \cdot \underbrace{A_\varphi^C}_{1)}$

1) Streckung im Faktor 2 bezüglich $C = \{e_1, e_2\}$
   $A_\varphi^C = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

2) Basiswechssel von C nach $B = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$

$\begin{pmatrix}1\\0\end{pmatrix} = 0 \cdot \begin{pmatrix}1\\1\end{pmatrix} + 1 \cdot \begin{pmatrix}1\\0\end{pmatrix}$
$\begin{pmatrix}0\\1\end{pmatrix} = 1 \cdot \begin{pmatrix}1\\1\end{pmatrix} + (-1) \cdot \begin{pmatrix}1\\0\end{pmatrix}$
$\Rightarrow S_{C,B} = \begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}$
Probe:
$\underbrace{\begin{pmatrix}0 & 1\\1 & -1\end{pmatrix}}_{S_{C,B}} \cdot \underbrace{\begin{pmatrix}2 & 0\\0 & 2\end{pmatrix}}_{A_\varphi^C} = \underbrace{\begin{pmatrix}0 & 2\\2 & -2\end{pmatrix}}_{A_\varphi^{C,B}}$

7.10 Satz (Umrechnen von Darstellungsmatrizen)

$\varphi : V \to W$ lineare Abbildung, B, B' Basen von V, $\quad C, C'$ Basen von W.

$\Rightarrow A_\varphi^{B',C'} = S_{C,C'} \cdot A_\varphi^{B,C} \cdot S_{B',B}$

$\Big[$Bemerkung: in 7.9: $A_\varphi^{C,B} = S_{C,B} \cdot A_\varphi^{C,C} \cdot S_{C,C}$ mit $S_{C,C} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = E_2$ ist 'Spezialfall'.$\Big]$

Beweis:

Sei $v \in V$.

$$\begin{aligned} A_\varphi^{B',C'} \cdot K_{B'}(v) &\overset{7.7}{=} K_{C'}(\varphi(v)) \\ &\overset{7.4}{=} S_{C,C'} \cdot \overbrace{K_C(\varphi(v))} \\ &\overset{7.7}{=} S_{C,C'} \cdot \overbrace{A_\varphi^{B,C} \cdot \underline{K_B(v)}} \\ &\overset{7.4}{=} S_{C,C'} \cdot A_\varphi^{B,C} \cdot \underline{S_{B',B} \cdot K_{B'}(v)} \end{aligned}$$

$\square$

7.11 Bemerkung zu Darstellungsmatrizen

V bzw. W K-VR mit Basen $B = \{v_1, .., v_n\}$ bzw. $C = \{w_1, ..., w_n\}, \varphi : V \to W$ lin. Abbildung.
Für $v \in W$ kann $K_B(v)$ aufgefasst werden als Bild der Koordinatenabbildung.

$K_B : V \to K^n, v = \sum_{i=1}^{n} \lambda_i v_i \mapsto \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$

Daraus ergibt sich folgendet Übersicht:

$$\begin{tikzcd}
V \arrow[r, "\varphi"] \arrow[d, "\mathrm{K}_B"'] & W \arrow[d, "\mathrm{K}_C"] \\
\mathcal{K}^m \arrow[r, "A_\varphi^{BC}"'] & \mathcal{K}^n
\end{tikzcd}$$

$\Rightarrow$ Jede lineare Abbildung $\varphi : \mathcal{K}^n \to \mathcal{K}^m$ ($\mathcal{K}$ Körper) ist von der Form $\varphi(x) = A \cdot x$ für eine geeignete Matrix $A \in \mathcal{M}_{m,n}(\mathcal{K})$.

Beweis

Wenn $V = \mathcal{K}^n$ und $W = \mathcal{K}^m$, benutze für B und C kanonische Basis.

$\Rightarrow K_C(\varphi(v)) = \varphi(v) \overset{7.4}{=} A_\varphi^{B,C} \cdot K_B(v) = \underbrace{A_\varphi^{B,C} \cdot v}_{\text{Matrix} \cdot \text{Vektor}}$ $\square$

7.12 Satz (Eigenschaften von Darstellungsmatrizen)

U, V, W Vektorräume mit Basen B, C, D; $\quad \varphi, \psi$ lineare Abbildungen.

i) Sei $\varphi, \psi : V \to W$. Dann ist
$A_{\varphi+\psi}^{B,C} = A_\varphi^{B,C} + A_\psi^{B,C}$

ii) Sei $\varphi : U \to W$. Dann ist
$A_{\lambda\varphi}^{B,C} = \lambda A_\varphi^{B,C}, \quad \lambda \in \mathcal{K}$

iii) Sei $\varphi : U \to V, \quad \psi : V \to W$. Dann ist
$A_{\psi\circ\varphi}^{B,D} = A_\psi^{C,D} \cdot A_\varphi^{B,C}$

[Bemerkung: Verknüpfung linearer Abbildungen entspricht dem Matrixprodukt der Darstellungsmatrizen.]

7.12 hier ohne Beweis.

Matrixinversen

Erinnerung

(4.2): $\mathcal{M}_n(\mathcal{K})$ mit Matrixaddition und -multiplikation ist ein Ring mit Eins ($= E_n$).
D.h. $A \in \mathcal{M}_n(\mathcal{K})$ kann Inverse A^{-1} besitzen.
Für A^{-1} gilt: $A \cdot A^{-1} = A^{-1}A = E_n$.

Fragen:

- Welche $A \in \mathcal{M}_n(\mathcal{K})$ besitzen Inverse $A^{-1} \in \mathcal{M}_n(\mathcal{K})$?
- Wie berechnet man A^{-1}?

7.13 Beispiel

$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$ hat Inverse $A^{-1} = \begin{pmatrix} 0 & 1 \\ \frac{1}{2} & 0 \end{pmatrix}$, da:
$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2$

7.14 Bemerkung

Idee: $A \in \mathcal{M}_n(\mathcal{K})$ kann als Darstellungsmatrix A_φ^B der linearen Abbildung $\varphi : \mathcal{K}^n \to \mathcal{K}^n, \quad \varphi(v) = Av$ bezüglich Basis B aufgefasst werden.

7.15 Satz

V $\mathcal{K}$-Vektorraum, $\dim(V) = n$, B Basis, $\varphi : V \to V$ linear mit Darstellungsmatrix A_φ^B. Dann:

$$\varphi \text{ invertierbar} \Leftrightarrow A_\varphi^B \text{ invertierbar}$$

Das heißt: $A_{\varphi^{-1}}^B = (A_\varphi^B)^{-1}$

Beweis

($\Rightarrow$) Zeige: $(A_\varphi^B) \cdot (A_{\varphi^{-1}}^B) = E_n$
φ invertierbar $\Rightarrow A_\varphi^B \cdot A_{\varphi-1}^B \overset{7.12}{=} A_{\varphi\circ\varphi^{-1}}^B = E_n$
Analog: $A_{\varphi^{-1}}^B \cdot A_\varphi^B = E_n$

$(\Leftarrow)$ Sei nun A_φ^B invertierbar.

$$\begin{aligned}
&\Rightarrow \exists Y \in \mathcal{M}_n(\mathcal{K}) : A_\varphi^B \cdot Y = Y \cdot A_\varphi^B = E_n \\
&\overset{7.14}{\Rightarrow} Y = A_\psi^B \text{ mit } \psi(v) = Y \cdot v \\
&\Rightarrow \begin{cases} E_n = A_\varphi^B \cdot A_\psi^B \overset{7.12}{=} A_{\varphi\circ\psi}^B \\ E_n = A_\psi^B \cdot A_\varphi^B \overset{7.12}{=} A_{\psi\circ\varphi}^B \end{cases} \\
&\Rightarrow \varphi \circ \psi = \psi \circ \varphi = id_v \\
&\Rightarrow \varphi \text{ hat Inverse } \psi
\end{aligned}$$

□

7.16 Satz

18.01.2017

$$A \in \mathcal{M}_n(\mathcal{K}) \text{ invertierbar} \Leftrightarrow \underbrace{\mathrm{rg}(A) = n}_{\substack{\text{d.h. alle Spalten \& Zeilen} \\ \text{linear unabhängig}}}$$

Beweis

$7.14 \Rightarrow A = A_\varphi^B$ für $\varphi : \mathcal{K}^n \to \mathcal{K}^n, \quad \varphi(v) = Av$

$$\begin{aligned}
A \text{ invertierbar } &\overset{7.15}{\Leftrightarrow} \varphi \text{ invertierbar} \\
&\Leftrightarrow \varphi \text{ bijektiv} \\
&\overset{6.15}{\Leftrightarrow} \varphi \text{ surjektiv} \\
&\Leftrightarrow \mathrm{rg}(\varphi) = n \\
&\overset{6.16}{\Leftrightarrow} \mathrm{rg}(A) = n
\end{aligned}$$

□

7.17 Beispiel

$A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \Rightarrow \mathrm{rg}(A) = 1 \Rightarrow A$ nicht invertierbar

$A = \underbrace{\begin{pmatrix} 1 & -1 \\ 2 & 0 \end{pmatrix}}_{\in \mathcal{M}_2(\mathbb{R})} \Rightarrow \mathrm{rg}(A) = 2 \Rightarrow$ A invertierbar (weil Rang voll).

7.18 Berechnung der Matrixinverse (A^{-1})

Gegeben: Quadratische Matrix $A0 \begin{pmatrix} a_{11} & ... & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & ... & a_{nn} \end{pmatrix} \in \mathcal{M}_n(\mathcal{K})$, $\mathcal{K}$ Körper. Gesucht: Matrixinverse $A^{-1} \in \mathcal{M}_n(\mathcal{K})$.

Voraussetzungen

Das sogenannte Gauß-Jordan-Verfahren zur Berechnung der Matrixinversen baut auf der Berechnung der Lösungen von Gleichungssystemen $Ax = b$ mit **quadratischer** Matrix A auf. Deswegen werden zunächst einige Regeln angegeben, die zur Lösung linearer Gleichungssysteme benutzt werden. Dabei wird im Folgenden das LGS mit Hilfe der erweitertern Koeffizientenmatrix $(A|b)$ beschrieben: Wenn $b = (b_1, ..., b_n)^T \in \mathcal{K}^n$ schreibt man $(A|b) = \left(\begin{array}{ccc|c} a_{11} & ... & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & ... & a_{nn} & b_n \end{array}\right)$.
Die Lösungsmenge des LGS ändert sich nicht, wenn man an $(A|b)$ folgende elementaren Zeilenumformungen aus dem Gaußverfahren durchführt:

1. Erweiterung einer Zeile mit einem Skalar $\lambda \in \mathcal{K}, \quad \lambda \neq 0$,
2. Addition von Zeilen
3. Tauschen von Zeilen.

Gauß-Jordan-Algorithmus

Im Unterschied zum Gauß-Algorithmus bringt man das LGS $Ax = b$ nicht auf Dreiecksform, sondern man formt die Zeilen so um, dass A zur Einheitsmatrix E_n wird. Dabei wird b automatisch zum Lösungsvektor x umgeformt: Man erhält das System $(E_n|x)$.

Berechnung der Inversen A^{-1}

Zur Berechnung der Inversen muss nun das System $AX = E_n$ gelöst werden. Man erreicht dies, indem der Gauß-Jordan-Algorithmus simultan auf die n LGS $Ay = e_j, \quad j = 1, ..., n$ angewendet wird. Dazu stellt man das System $(A|E_n)$ auf. Durch Zeilenumformungen überführt man nun A in die Einheitsmatrix, wobei die rechte Seite in die Lösungsmatrix X überführt wird. Man erhält so das System $(E_n|X)$ mit $X = A^{-1}$.

[Anmerkung: Das Verfahren zeigt auch, ob A überhaupt eine Inverse besitzt. Besitzt A keine Inverse, so kann man A nicht in die Einheitsmatrix umformen.]

Beispiel

Gegeben: $A = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$
Algorithmus zur Berechnung von A^{-1} erweitert den Gauß-Algorithmus zur Lösung von LGS.
z.B. $Ax = b$ mit $b = \begin{pmatrix} 10 \\ 15 \end{pmatrix}$
Gauß-Jordan-Verfahren:

$$\begin{pmatrix} 2 & 1 & 10 \\ 1 & 3 & 15 \end{pmatrix} \xrightarrow{II=I-2\cdot II} \begin{pmatrix} 2 & 1 & 10 \\ 0 & -5 & 20 \end{pmatrix} \xrightarrow{-\frac{1}{5}\cdot II} \begin{pmatrix} 2 & 1 & 10 \\ 0 & 1 & 4 \end{pmatrix} \xrightarrow{I=I-II} \begin{pmatrix} 2 & 0 & 6 \\ 0 & 1 & 4 \end{pmatrix} \xrightarrow{\frac{1}{2}} \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \end{pmatrix}$$

$\Rightarrow x = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ Lösung
Für Inverse: Suche Matrix, die $A \cdot X = E_n$ löst.

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

Wende Gauß-Jordan-Algorithmus simultan auf LGS (*) und (**) an.

$$\begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{pmatrix} \xrightarrow{II=I-2II} \begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & -5 & 1 & -2 \end{pmatrix} \xrightarrow{-\frac{1}{5}II} \begin{pmatrix} 2 & 1 & 1 & 0 \\ 0 & 1 & -\frac{1}{5} & \frac{2}{5} \end{pmatrix} \xrightarrow{I=I-II} \begin{pmatrix} 2 & 0 & \frac{6}{5} & -\frac{2}{5} \\ 0 & 1 & -1\frac{1}{5} & \frac{2}{5} \end{pmatrix} \xrightarrow{\frac{1}{2}I}$$
$$\begin{pmatrix} 1 & 0 & \frac{3}{5} & -\frac{1}{5} \\ 0 & 1 & -\frac{1}{5} & \frac{2}{5} \end{pmatrix} \Rightarrow \begin{pmatrix} \frac{3}{5} & -\frac{1}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix} = X = A^{-1}$$

7.19 Lemma

V $\mathcal{K}$-Vektorraum, B, C Basen $\Rightarrow S_{B,C} = (S_{C,B})^{-1}$

Beweis

Sei $v \in V$.
$S_{C,B} \cdot S_{B,C} \cdot K_B(v) = S_{C,B} \cdot K_C(v) = K_B(v) = E_n$ $\square$

7.20 Beispiel

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

Aus 7.2: $S_{B,C} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, aus 7.9: $S_{C,B} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$

Tatsächlich ist $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

7.21 Korollar

$\varphi : V \to V, \quad B, C$ Basen von $V, \quad S := S_{B,C}$

$\Rightarrow A_\varphi^C = S A_\varphi^B S^{-1}$

Beweis

$S A_\varphi^B S^{-1} \overset{7.19}{=} S_{B,C} A_\varphi^{B,B} S_{C,B} = A_\varphi^{C,C} = A_\varphi^C$ □

7.22 Beispiel

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

Wie sieht Darstellungsmatrix von einer Drehung $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ um den Winkel $\frac{\pi}{2}$ bzgl. B aus?

Wissen: $D_{\frac{\pi}{2}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = A_\varphi^C$ Drehung um $\frac{\pi}{2}$ bzgl. C

$$\begin{aligned} A_\varphi^B &= S_{C,B} \underbrace{D_{\frac{\pi}{2}}}_{A_\varphi^{C,C}} S_{B,C} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix} \end{aligned}$$

8 Determinanten

7.16 : $A \in \mathcal{M}_n(\mathcal{K})$ invertierbar $\Leftrightarrow \mathrm{rg}(A) = n$
In diesem Kapitel werden invertierbare Matrizen mit Hilfe der Determinante charakterisiert.
Das ist einfacher zu implementieren.

8.1 Definition

$A \in \mathcal{M}_n(\mathcal{K}), \quad i, j \in \{1, ..., n\}. \quad A_{i,j} \in \mathcal{M}_{n-1}(\mathcal{K})$ sei die Matrix, die man aus A durch Streichen der $i-$ten Zeile und $j-$ten Spalte erhält.

z.B.: $A = \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & -1 \\ -2 & 1 & 1 \end{pmatrix} \Rightarrow A_{2,3} = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$

8.2 Definition (Rekursive Definition der Determinante)

$A \in \mathcal{M}_n(\mathcal{K})$.

$\underline{n = 1:}\quad A = (a), \det(A) := a \in \mathcal{K}$

$\underline{n \geq 2}:\quad$ Entwicklung nach der 1. Zeile (7.4):

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix}$$

$$\det(A) = +a_{11} \cdot \det(A_{1,1}) - a_{12} \cdot \det(A_{1,2}) + a_{13} \cdot \det(A_{1,3}) \pm ...(-1)^{n+1} a_{1n} \cdot \det(A_{1,n})$$
$$= \sum_{j=1}^{n} (-1)^{1+j} a_{1j} \cdot \det(A_{1j})$$

8.3 Beispiel

a) $\det \begin{pmatrix} 1 & 1 \\ 2 & -3 \end{pmatrix} = 1 \cdot (-3) - 1 \cdot 2 = -5$