Mathematik III

23.11.2016

Inhaltsverzeichnis

1 Vektorräume

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

1.1 Definition (Reelle Vektorräume)

Ein <u>$\mathbb{R}$-Vektorraum V</u> ist eine nichtleere Menge, deren Elemente <u>Vektoren</u> 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 $\mathcal{O} \in V$ ('<u>Nullvektor</u>') 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. $V = \mathcal{F}(M, \mathbb{R}) \coloneqq \{f \colon M \to \mathbb{R}\}$
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 8.1 eindeutig bestimmt.

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

Beweis

a)

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

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

d)

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

Addiere auf beiden Seiten $-v$:

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

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

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 $U \subseteq V$, $U \neq \emptyset$ 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) $V = \mathbb{R}^2$, $U = \{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$ ist Unterraum von V

b) $V = \mathbb{R}^2$, $U = \{\begin{pmatrix} 1 \\ 2 \end{pmatrix}\}$ 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) $V = \mathbb{R}^2$, $U = \{\begin{pmatrix} \lambda \\ 0 \end{pmatrix} | \lambda \in \mathbb{R}\}$ ist ein Unterraum von V (prüfe alle Eigenschaften von Definition 8.1) $\rightarrow$ umständlich, einfacher geht es mit 8.6

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

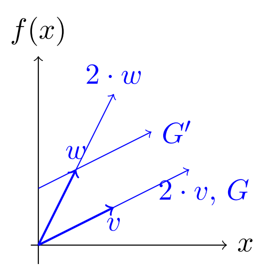
$\Rightarrow$ ist klar, da U laut Definition 8.4 selbst Vektorraum

$\Leftarrow$ rechne die Vektorraumaxiome nach (Definition 8.1, 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) $V = \mathbb{R}^3, \qquad U_1 = \{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 | x_1 + x_2 - x_3 = 0\}$ ist Unterraum. Wir zeigen (1), (2) aus 8.6:

– $U_1 \neq \emptyset$, 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:

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

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) $U_2 = \{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 | x_1 + x_2 - x_3 = 1\}$ 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:

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

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) $U_3 = \{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3 | x_1^2 + x_2^2 + x_3^2 \leq 1\}$ 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 $2^2 + 0^2 + 0^2 \nleq 1$

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 8.2d)).
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 $U_1 \cap U_2$!)

Beweis

Prüfe Unterraumkriterium 8.6

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

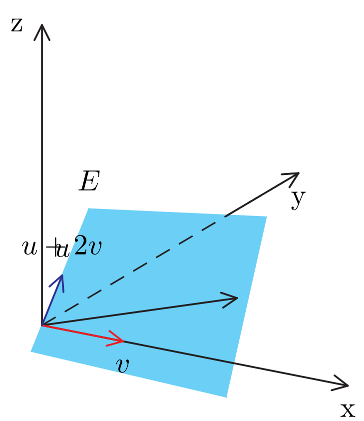
- $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{R}^2$ $\qquad G_1 = \{\lambda v | \lambda \in \mathbb{R}\}$
- $w = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \in \mathbb{R}^2$ $\qquad G_2 = \{\mu w | \mu \in \mathbb{R}\}$

(vgl. 8.7a), 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



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

- E $\subseteq \mathbb{R}^3$ ist Untervektorraum (UVR) und wird <u>aufgespannt/erzeugt</u> von u und v. Man nennt $\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \}$ <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) $E = \langle \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \rangle_{\mathbb{R}}$

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.

$R^n = \langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix}, ..., \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \rangle_{\mathbb{R}}$ "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. $\begin{pmatrix} x \\ y \end{pmatrix} = (2x - y) \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} + (y - x) \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} \Rightarrow \mathbb{R}^2 = \langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix} \rangle_{\mathbb{R}}$

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

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

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

D.h. $M = \{\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}\}$ 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 <u>Linearkombination</u> von $v_1, ..., v_m$.

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

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

der <u>von M aufgespannte/erzeugte UVR</u> 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 <u>Erzeugendensystem</u> von V. V heißt <u>endlich erzeugt</u>, 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: $M = \{\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\} \Rightarrow \langle M \rangle_{\mathbb{R}} = \{\lambda \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} | \lambda \in \mathbb{R}\}$ Gerade

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

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

$\langle M \rangle_{\mathbb{R}}$ 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 linear unabhängig, 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 $v = \sum_{i=1}^n \lambda_i \cdot v_i = \sum_{i=1}^n \mu_i \cdot v_i$

$$\begin{aligned} &\Leftrightarrow \sum_{i=1}^n \underbrace{(\lambda_i - \mu_i)}_{=0, \text{ da } M \text{ linear unabhängig}} \cdot v_i = \mathcal{O} \\ &\Rightarrow \lambda_i = \mu_i \qquad \forall i = 1, ..., n \end{aligned}$$

(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) Basisi ist nicht eindeutig.
$B_1 = \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\}, \qquad B_2 = \{\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}$
$\Rightarrow \langle B_1 \rangle_{\mathbb{R}} = \langle B_2 \rangle_{\mathbb{R}}$, da: $\begin{pmatrix}1\\0\end{pmatrix} = 2\begin{pmatrix}1\\1\end{pmatrix} - \begin{pmatrix}1\\2\end{pmatrix}$ 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 andlich 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.
$\Rightarrow \underbrace{(B \setminus \{v_j\}) \cup \{w\}}_{(\star)}$ Basis, falls $\underline{\lambda_j \neq 0}$

Beweis

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

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

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

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

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

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) $V = \mathbb{R}^4, U = \langle u_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, u_2 = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} \rangle_{\mathbb{R}}$
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:

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

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

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

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

1.28 Satz (Dimensionssatz)

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

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

ii) $U \subseteq W \subseteq V$, $\quad U, W$ 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

Behauptung: $B = \{v_1, ..., v_k, w_{k+1}, ..., w_l, u_{k+1}, ..., u_m\}$ 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
$B = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{3} \\ 0 \\ 1 \end{pmatrix} \}$

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?

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

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

Vektorenschreibweise von $*$:

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

Matrixschreibweise:

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

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

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

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

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

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

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

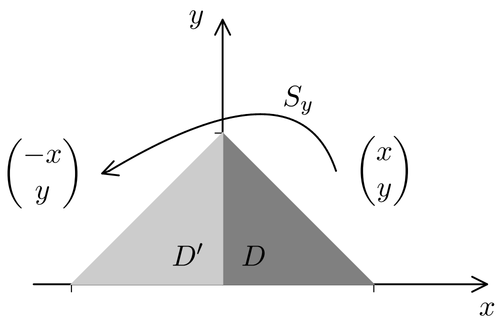
2.3 Bemerkung

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



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

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

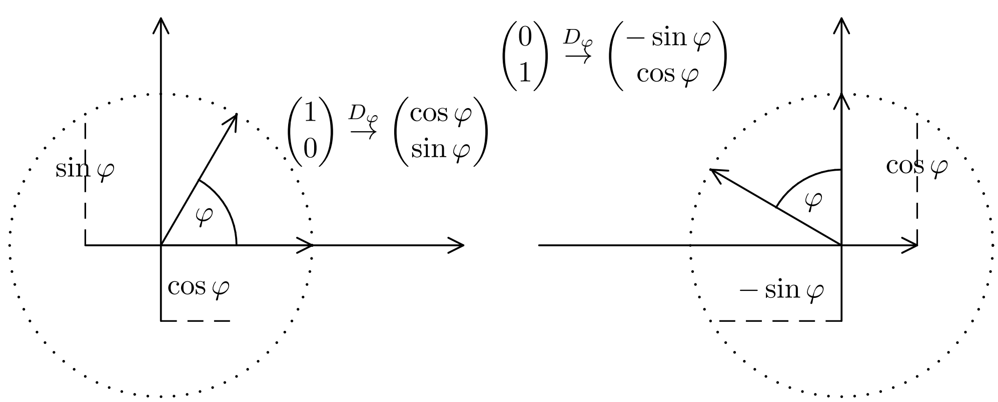
$S_y \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} s_{11} + s_{12} \\ s_{21} + s_{22} \end{pmatrix} = \begin{pmatrix} -x \\ y \end{pmatrix}$

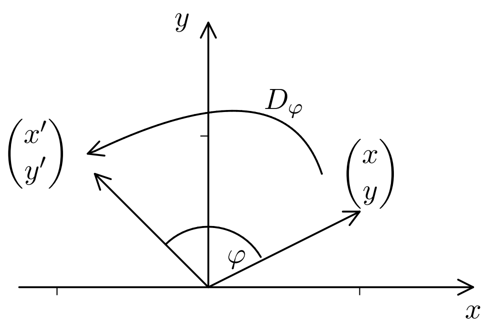
$\Rightarrow s_{11} = -1 \quad s_{12} = 0 \quad s_{21} = 0 \quad s_{22} = 1$

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

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 Def 2.2 ergibt sich:

$A \cdot e_j = 1 \cdot \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ (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)

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

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) $A \cdot B$

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

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, ... $\rightarrow 3 \cdot 2 \cdot 1 = 3!$ Möglichkeiten
Jede Anordnung kann man auffassen als eineindeutige (bijektive) Abbildung
$\pi : \{A, B, C\} \rightarrow \{A, B, C\}$

$$\pi : \begin{array}{c|c|c|c} \text{x} & \text{A} & \text{B} & \text{C} \\ \hline \pi(x) & \text{A} & \text{C} & \text{B} \end{array}$$

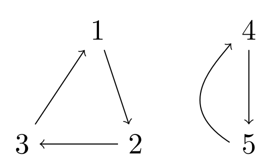
3.2 Definition (Permutation)

- Eine <u>Permutation</u> 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: $\mathscr{S}_2 = \{\text{id}, (AB)\} = \{\text{id}, (12)\}, \quad |\mathscr{S}_2| = 2! = 2$
mit $\text{id} = \begin{pmatrix} AB \\ AB \end{pmatrix}, \qquad \pi = \begin{pmatrix} AB \\ BA \end{pmatrix}$

3.3 Beispiel

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



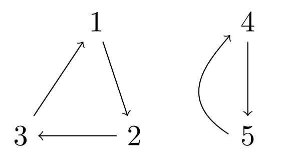
Graph der Permutation

3.4 Bemerkung

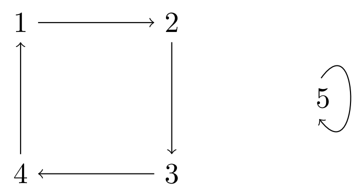
In Literatur oft <u>Zyklenschreibweise</u>:
Zyklus $(a_1 a_2 ... a_k)$ bedeutet $\pi(a_i) = a_{i+1}$ und $\pi(a_k) = a_1$
z.B.: $\pi = (123)(45)$

Verknüpfung von Permutationen

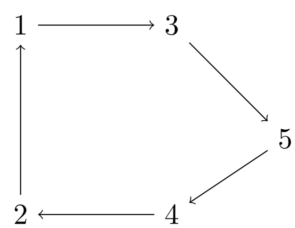
3.5 Beispiel



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



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



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

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 disjunkt, 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°
	D C A B	C D B A	A B D C	B A C D
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

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

Falls zusätzlich

4) $a \cdot b = b \cdot a \qquad \forall a, b \in G \qquad$ 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 $0 \cdot a = 1 \lightning$

$\Rightarrow$ $\mathbb{R}, \mathbb{Q}$ 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:

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

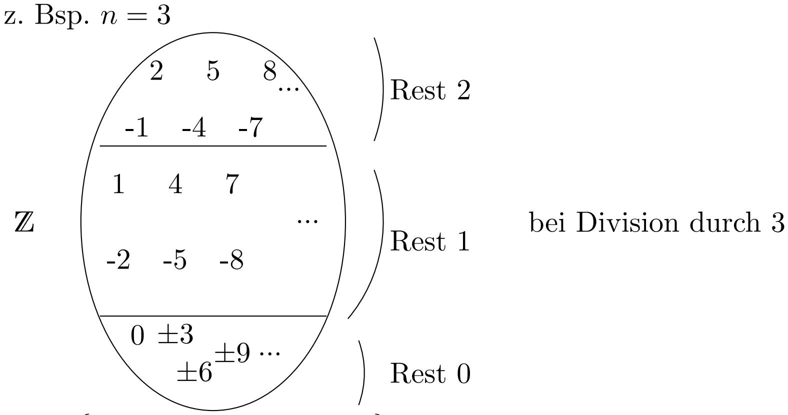
  $\pi = (123) \qquad\qquad \pi^{-1} = (132)$
  Fixpunkte und 2er-Zyklen ändern sich dabei nicht:
  $\sigma = (1678)(23) \Rightarrow \sigma^{-1} = (1876)(23)$
  Setzt man die Pfeile von den Graphen π und π^{-1} zusammen, ändert sich nichts, d.h. $\pi \cdot \pi^{-1}(i) = i \Rightarrow \pi \cdot \pi^{-1} = \mathrm{id} = \pi \cdot \pi^{-1}$
- nicht abelsch: Bem. 3.6d)

15.11.2016

3.12 Beispiel

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

z. Bsp. $n = 3$



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

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

$\underline{(\mathbb{Z}_n, \oplus) \text{ ist abelsche Gruppe:}}$

- 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 $a \in \mathbb{Z}_n$: $\underbrace{0 \cdot a \mod n}_{0} = 1$ (↯)

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 $\mathbb{Z}_1 5$ 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:

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

Beweis von *

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

'⇒' 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: $\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n \mid \operatorname{ggT}(z, n) = 1\}$ ist Gruppe mit Ordnung $|\mathbb{Z}_n^*| = \varphi(n)$ (Eulersche $\varphi-$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 3.13)

3.16 Beispiel

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

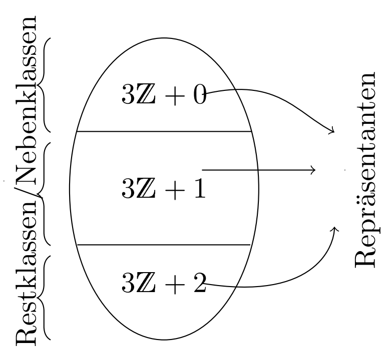
b) $(\{-1, 1\}, \cdot) \leq (\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot)$

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 $\underbrace{6}_{\in 3\mathbb{Z}} + 4 = 10$



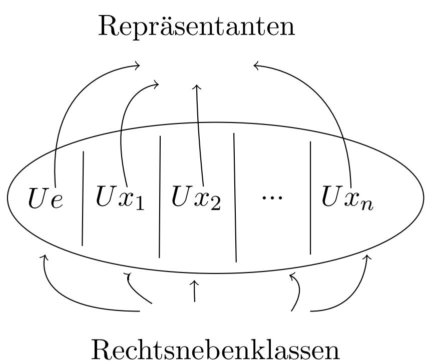
3.18 Satz + Definition (Rechtsnebenklasse, Repräsentant)

G Gruppe, $U \leq G$.

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

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

iii) ${}^{G}/_{U} := \{Ux \mid x \in G\}$ Menge der Rechtsnebenklassen von U in G.
Behauptung: ${}^{G}/_{U}$ 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 $j = 3\mathbb{Z} + j$) 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 $\varphi(u_1) = \varphi(u_2) \Rightarrow u_1 x = u_2 x$
  $\overset{\cdot x^{-1}}{\Rightarrow} u_1 = u_2$

$\Rightarrow |U| = |Ux|$

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:

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

* $a^{\overbrace{m}^{\in \mathbb{Z}^-}} = (a^-1)^{\overbrace{-m}^{\in \mathbb{N}}} \stackrel{\text{a)}}{=} (a^{-m})^{-1}$
$\Rightarrow (a^m)^{-1} = ((a^{-m})^{-1})^{-1} = a^{-m}$

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 <u>endlich</u> $\Rightarrow \exists i, j \in \mathbb{N} : g^i = g^j$ 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 $k \in \mathbb{N}$

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

□

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

4.1 Definition

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 assoziativ.

   3) Distributivgesetze: $a \cdot (b + c) = ab + ac$
      $(a + b) \cdot c = ac + bc \qquad \forall a, b, c \in \mathcal{R}$