

Inhaltsverzeichnis

| | | |
|----------|--|-----------|
| 0 | Der Vektorraum \mathbb{R}^n | 5 |
| 0.1 | Satz (Rechenregeln in \mathbb{R}^n) | 6 |
| 0.2 | Definition | 7 |
| 0.3 | Beispiele | 7 |
| 0.4 | Satz | 8 |
| 0.5 | Beispiel | 9 |
| 0.6 | Definition | 10 |
| 0.7 | Beispiel | 11 |
| 0.9 | Definition | 13 |
| 0.10 | Beispiel | 13 |
| 0.11 | Satz | 15 |
| 0.12 | Satz | 16 |
| 0.13 | Definition | 17 |
| 0.14 | Beispiel | 17 |
| 0.15 | Satz | 18 |
| 0.16 | Satz | 19 |
| 0.17 | Definition | 19 |
| 0.18 | Satz (Basisergänzungssatz) | 19 |
| 0.19 | Korollar | 19 |
| 0.20 | Definition | 20 |
| 0.21 | Beispiele | 20 |
| 1 | Algebraische Strukturen | 21 |
| 1.1 | Definition | 21 |
| 1.2 | Beispiele | 21 |
| 1.3 | Definition | 22 |
| 1.4 | Bemerkung | 23 |
| 1.5 | Bemerkung | 23 |
| 1.6 | Proposition | 23 |
| 1.7 | Beispiel | 24 |
| 1.8 | Satz | 26 |

| | |
|--|-----------|
| 1.9 Beispiel | 27 |
| 1.10 Beispiel | 27 |
| 1.11 Satz (Gleichungslösen in Gruppen) | 28 |
| 1.12 Beispiel | 28 |
| 1.13 Definition | 29 |
| 1.14 Beispiele | 29 |
| 1.15 Proposition | 30 |
| 1.16 Bemerkung | 30 |
| 1.17 Definition | 31 |
| 1.18 Beispiel | 31 |
| 1.19 Proposition (Nullteilerfreiheit in Körpern) | 31 |
| 1.20 Definition | 31 |
| 1.21 Satz und Definition | 32 |
| 1.22 Bemerkung | 33 |
| 1.23 Definition | 33 |
| 1.24 Satz | 33 |
| 1.25 Korollar | 33 |
| 1.26 Bemerkung | 34 |
| 1.27 Definition | 35 |
| 1.28 Satz | 35 |
| 1.29 Beispiel | 36 |
| 1.30 Korollar | 36 |
| 1.31 Definition | 37 |
| 1.32 Beispiel | 37 |
| 1.33 Satz | 37 |
| 1.34 Korollar | 38 |
| 1.35 Bemerkung | 38 |
| 1.36 Fundamentalsatz der Algebra | 39 |
| 2 Vektorräume | 39 |
| 2.1 Definition | 39 |
| 2.2 Beispiel | 39 |
| 2.3 Proposition | 41 |

| | | |
|------|---|----|
| 2.4 | Definition | 41 |
| 2.5 | Proposition | 41 |
| 2.6 | Beispiel | 42 |
| 2.7 | Proposition | 42 |
| 2.8 | Definition | 42 |
| 2.9 | Satz | 43 |
| 2.10 | Definition | 43 |
| 2.11 | Beispiel | 43 |
| 2.12 | Definition | 44 |
| 2.13 | Beispiel | 44 |
| 2.14 | Bemerkung | 46 |
| 2.15 | Satz !!! | 46 |
| 2.16 | Definition | 46 |
| 2.17 | Beispiel | 47 |
| 2.18 | Satz (Existenz von Basen) | 48 |
| 2.19 | Lemma | 48 |
| 2.20 | Satz (Austauschsatz von Steinitz) | 49 |
| 2.21 | Korollar | 49 |
| 2.22 | Satz | 50 |
| 2.23 | Definition | 51 |
| 2.24 | Korollar | 51 |
| 2.25 | Beispiel | 51 |
| 2.26 | Satz | 52 |
| 2.27 | Definition | 53 |
| 2.28 | Beispiel | 53 |
| 2.29 | Definition | 55 |
| 2.30 | Satz | 55 |
| 2.31 | Bemerkung | 56 |
| 2.32 | Bemerkung | 56 |
| 2.33 | Satz | 57 |
| 2.34 | Beispiel | 58 |

| | | |
|----------|----------------------------|-----------|
| 3 | Lineare Abbildungen | 59 |
| 3.1 | Definition | 59 |
| 3.2 | Bemerkung | 59 |
| 3.3 | Beispiel | 59 |

Abbildungsverzeichnis

| | | |
|---|--|----|
| 1 | Ein Vektor dargestellt durch seinen Ortsvektor | 6 |
| 2 | Vektoraddition durch Parallelogrammbildung | 6 |
| 3 | Gerade dargestellt durch Vektoren | 8 |
| 4 | Eindimensionale Unterräume im \mathbb{R}^2 | 54 |

Ende des SS 2015

0 Der Vektorraum \mathbb{R}^n

$$n \in \mathbb{N} \quad \mathbb{R}^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_i \in \mathbb{R} \right\}$$

Spaltenvektoren der Länge n : $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = (a_1, \dots, a_n)^t$

a_1, \dots, a_n Komponente der Spaltenvektoren.

Wie bei Matrizen:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix} \quad \begin{array}{l} \text{(Multiplikation entspricht der Matri-} \\ \text{zenmultiplikation und ist nicht mög-} \\ \text{lich falls } n > 1) \end{array}$$

Multiplikation eines Spaltenvektors mit einer Zahl (Skalar)

$$a \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} aa_1 \\ \vdots \\ aa_n \end{pmatrix}$$

Addition+Abbildung : $\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}^n$

\mathbb{R}^n mit Addition und Multiplikation mit Skalaren : \mathbb{R} -Vektorraum

Die Vektoren im $\mathbb{R}^1 (= \mathbb{R})$, \mathbb{R}^2 und \mathbb{R}^3 entsprechen Punkten auf der Zahlengerade, Ebene, dreidimensionalen Raums. Punkte des $\mathbb{R}^2, \mathbb{R}^3$ lassen sich identifizieren mit, Ortsvektoren Pfeile mit Beginn in 0 (Komp = 0) und Ende im entsprechenden Punkt

Addition von Spaltenvektoren entspricht der Addition von Ortsvektoren entsprechend der Parallelogrammregel. Multiplikation mit Skalaren a :

Streckung (falls $|a| > 1$)

Stauchung (falls $0 \leq |a| \leq 1$)

Richtungspunkt, falls $a < 0$

Abbildung 1: Ein Vektor dargestellt durch seinen Ortsvektor

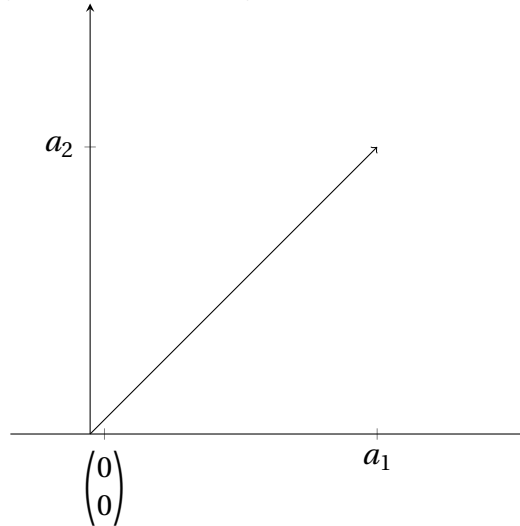
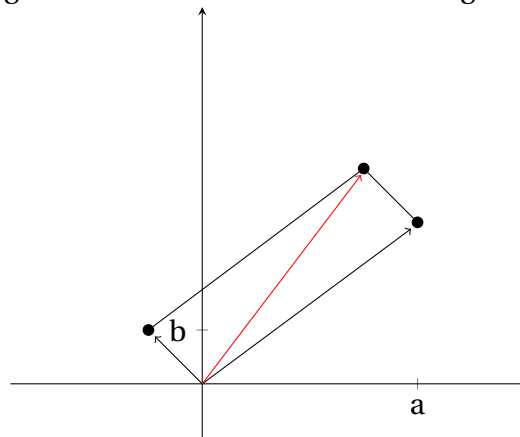


Abbildung 2: Vektoraddition durch Parallelogrammbildung



0.1 Satz (Rechenregeln in \mathbb{R}^n)

Seien $u, v, w \in \mathbb{R}^n$, $a, b \in \mathbb{R}$ Dann gilt:

a)

$$(1.1) \quad u + (v + w) = (u + v) + w$$

$$(1.2) \quad v + 0 = 0 + v = v, \text{ wobei } 0 \text{ Nullvektor}$$

$$(1.3) \quad v + -v = 0$$

$$(1.4) \quad u + v = v + u$$

$$(2.1) \quad (a + b)v = av + bv$$

$$(2.2) \quad a(u + v) = au + av$$

$$(2.3) \quad (a \cdot b)v = a(bv)$$

$$(2.4) \quad 1v = v$$

 \mathbb{R}^n kommutative

Gruppe

b) $0 \cdot v = 0$ und $a \cdot 0 = 0$

Beweis folgt aus entsprechenden Rechenregeln in 0

0.2 Definition

Eine nicht-leere Teilmenge $\mathcal{U} \subset \mathbb{R}^n$ heißt *Unterraum* (oder *Teilraum* von \mathbb{R}^n), falls gilt:

(1) $\forall u_1, u_2 \in \mathcal{U} : u_1 + u_2 \in \mathcal{U}$ (Abgeschlossenheit bezüglich +)(2) $\forall u \in \mathcal{U} \forall a \in \mathbb{R} : au \in \mathcal{U}$ (Abgeschlossenheit bezüglich Mult. mit Skalaren) \mathcal{U} enthält Nullvektor $\{0\}$ Unterraum von \mathbb{R}^n (Nullraum) \mathbb{R}^n ist Unterraum von \mathbb{R}

0.3 Beispiele

a) $0 \neq v \in \mathbb{R}^2 \quad G = \{av : a \in \mathbb{R}\}$ ist Unterraum von \mathbb{R}^n

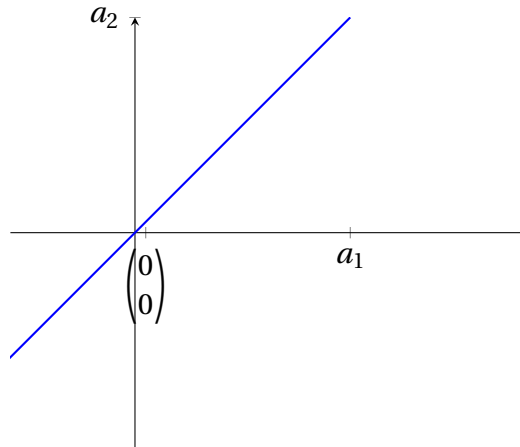
$$(a_1 v, a_2 v \in G, (a_1 +$$

$$a_2)v \in G \quad 2.1 \text{ in } 0.2$$

$$av \in G, b \in \mathbb{R} (ba)v \in G)$$

$G =$ Ursprungsgerade durch $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und $v = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} n = 2:$

Abbildung 3: Gerade dargestellt durch Vektoren

b) $v, w \in \mathbb{R}^n$ $E = \{av + bw : a, b \in \mathbb{R}\}$ ist Unterraum von \mathbb{R}^n $v = o, w = o : E = \{o\}$ $v \neq o \quad w \notin \{av : a \in \mathbb{R}\}$ $E = \mathbb{R}^2 \quad n = 3 : \text{Ebene durch } \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ und durch } v, w$ Ist $w \in \{av : a \in \mathbb{R}\}$, so ist $E = G$ (aus a))c) $v, w \neq o$ $G' = \{w + av : a \in \mathbb{R}\}$ $[v \in G' \Leftrightarrow \exists a \in \mathbb{R} : w + av \in o \Leftrightarrow \exists a \in \mathbb{R} : w = (-a)v \in G]$ **0.4 Satz**Seien $\mathcal{U}_1, \mathcal{U}_2$ Unterräume von \mathbb{R}^n a) $\mathcal{U}_1 \cap \mathcal{U}_2$ ist Unterraum von \mathbb{R}^n b) $\mathcal{U}_1 \cup \mathcal{U}_2$ ist im Allgemeinen KEIN Unterraum von \mathbb{R}^n c) $\mathcal{U}_1 + \mathcal{U}_2 := \{u_1 + u_2 : u_1 \in \mathcal{U}_1, u_2 \in \mathcal{U}_2\}$ (Summe von \mathcal{U}_1 und \mathcal{U}_2) ist Unterraum von \mathbb{R}^n .

- d) $\mathcal{U}_1 \subseteq \mathcal{U}_1 + \mathcal{U}_2$ $\mathcal{U}_2 \subseteq \mathcal{U}_1 + \mathcal{U}_2$ und $\mathcal{U}_1 + \mathcal{U}_2$ ist der kleinste Unterraum von \mathbb{R}^n , der \mathcal{U}_1 und \mathcal{U}_2 enthält. (d.h ist w Unterraum von \mathbb{R}^n mit $\mathcal{U}_1, \mathcal{U}_2 \subseteq w$, so $\mathcal{U}_1 + \mathcal{U}_2 \subseteq w$)

Beweis. a) ✓

b) c)

□

0.5 Beispiel

- a) ??b) $G_1 = \{av : a \in \mathbb{R}\}$

$$G_2 = \{aw : a\}$$

$$G_1 + G_2 = E$$

- b) \mathbb{R}^3

$$E_1 = \left\{ r \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + s \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} : r, s \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} r \\ 0 \\ s \end{pmatrix} : r, s \in \mathbb{R} \right\}$$

$$E_2 = \left\{ t \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + u \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

$$= \left\{ \begin{pmatrix} u \\ t+u \\ u \end{pmatrix} \right\}$$

$E_1 + E_2$ Unterräume von \mathbb{R}^3 (10.3.b)

$$E_1 \cap E_2 = ?$$

$$v \in E_1 \cap E_2 \Leftrightarrow v = \begin{pmatrix} r \\ 0 \\ s \end{pmatrix} = \begin{pmatrix} u \\ t+u \\ u \end{pmatrix} \Leftrightarrow r = u, t+u = 0, s = u$$

$$E_1 \cap E_2 = \left\{ \begin{pmatrix} u \\ 0 \\ u \end{pmatrix} : u \in \mathbb{R} \right\}$$

$$= \left\{ u \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} : u \in \mathbb{R} \right\}$$

$$E_1 + E_2 = ?$$

$$E_1 + E_2 = \mathbb{R}^3, \text{ denn :}$$

Es gilt sogar:

$$\mathbb{R}^3 = E_1 + G_2, \text{ wobei}$$

$$G_2 = \left\{ t \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} : t \in \mathbb{R} \right\} \subseteq E_{@}$$

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

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = (x - y) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + (z - y) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} x - y \\ 0 \\ z - y \end{pmatrix} + \begin{pmatrix} y \\ y \\ y \end{pmatrix}$$

0.6 Definition

a) $v_1, \dots, v_m \in \mathbb{R}^n, a_1, \dots, a_m \in \mathbb{R}$

Dann heit $a_1 v_1 + \dots + a_m v_m = \sum_{i=1}^m a_i v_i$

Linearkombination von v_1, \dots, v_m (mit Koeffizienten a_1, \dots, a_m).

[Zwei formal verschiedene Linearkombinationen der gleichen v_1, \dots, v_m knnen den gleichen Vektor darstellen

$$1 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 3 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 2 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 4 \\ 5 \end{pmatrix}]$$

b) Ist $M \subseteq \mathbb{R}^n$, so ist der von M *erzeugte* (oder *aufgespannte*) Unterraum $\langle M \rangle_{\mathbb{R}}$ (oder $\langle M \rangle$) die Menge aller (endlichen) Linearkombinationen, die man mit Vektoren aus M bilden kann.

$$\langle M \rangle_{\mathbb{R}} = \left\{ \sum_{i=1}^n a_i v_i : n \in \mathbb{N}, a_i \in \mathbb{R}, v_i \in M \right\} \text{ falls } M \neq \emptyset$$

$$\langle \emptyset \rangle_{\mathbb{R}} := \{\emptyset\}$$

$$M = \{v_1, \dots, v_m\}, \text{ so}$$

0.7 Beispiel

$$\text{a) } e_i = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \in \mathbb{R}^n$$

$$\langle e_1, \dots, e_n \rangle = \mathbb{R}^n$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 e_1 + x_2 e_2 + \dots + x_n e_n$$

$$\text{b) } \mathcal{U} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \right\rangle_{\mathbb{R}}$$

Ist $\mathcal{U} = \mathbb{R}^3$?

Für welche $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ gibt es geeignete Skalare $a, b, c \in \mathbb{R}$ mit $a \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + b \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} +$

$$c \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}?$$

$$a + 3b + 2c = x$$

$$2a + 2b + 3c = y$$

$$3a + b + 4c = z$$

LGS für die Unbekannten a, b, c mit variabler rechter Seite : Gauß

$$\begin{pmatrix} 1 & 3 & 2 & x \\ 2 & 2 & 3 & y \\ 3 & 1 & 4 & z \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & 2 & x \\ 2 & -4 & -1 & y-2x \\ 0 & -8 & -2 & z-3x \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 3 & 2 & x \\ 0 & 1 & \frac{1}{4} & \frac{2x-y}{4} \\ 0 & 0 & 0 & x-2y+z \end{pmatrix}$$

LGS ist lösbar $\Leftrightarrow x-2y+z=0$.

Dass heißt $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathcal{U} \Leftrightarrow x-2y+z=0$

$$\mathcal{U} = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} : x-2y+z=0, x, y, z \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} x \\ y \\ -x+2y \end{pmatrix} : x, y \in \mathbb{R} \right\}$$

$$\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \in \mathcal{U}$$

Lösungen des LGS: c frei wählen, b, a ergeben sich, (falls $x-2y+z=0$) z.B

$$c=0, b=\frac{1}{2}x-\frac{1}{4}y, a=x-3b=-\frac{1}{2}x+\frac{3}{4}y$$

Ist $x-2y+z=0$, so ist

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \left(-\frac{1}{2}x + \frac{3}{4}y\right) \begin{pmatrix} x \\ y \\ z \end{pmatrix} + \left(\frac{1}{2}x - \frac{1}{4}y\right) \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \frac{5}{4} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \frac{1}{4} \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$$

$$\mathcal{U} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \right\rangle_{\mathbb{R}}$$

$$\begin{array}{rcl} 6x^2 & -3xy & +y^3 = 5 \\ 7x^3 & +3x^2y^2 & -xy = 7 \end{array}$$

0.9 Definition

$v_1, \dots, v_n \in \mathbb{R}^n$ heißen *linear abhängig*, falls $a_1, \dots, a_n \in \mathbb{R}$ existieren, *nicht alle* $= 0$, mit $a_1 v_1 + \dots + a_n v_n = 0$.

Gibt es solche Skalare nicht, so heißen v_1, \dots, v_m *linear unabhängig* (d.h. aus $a_1 v_1 + \dots + a_n v_n = 0$ folgt $a_1 = \dots = a_n = 0$).

(Entsprechend $\{v_1 \dots v_n\}$ linear abhängig/linear unabhängig)

Per Definition : \emptyset ist linear unabhängig.

0.10 Beispiel

a) $\sigma + v \in \mathbb{R}^n$ Dann ist v linear unabhängig:

Zu zeigen : Ist $av = \sigma \Rightarrow a = 0$

Sei $v = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ Da $v \neq \sigma$,

existiert mindestens ein i mit $b_i \neq 0$.

Angenommen $\sigma v = \begin{pmatrix} 0b_1 \\ \vdots \\ 0b_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \sigma$.

Dann $ab_i = 0$ Da $b_i \neq 0$, folgt $a = 0$.

σ ist linear abhängig:

$$1 \cdot \sigma = \sigma$$

b) $v_1 = \sigma, v_2, \dots, v_m$ ist linear abhängig :

$$\sigma = 1 \cdot \sigma + 0 \cdot v_2 + \dots + 0 \cdot v_m$$

c) $v, w \in \mathbb{R}^n$

$$v \neq \sigma \neq w$$

v, w sind linear

① abhängig \Leftrightarrow

② $v \in \langle w \rangle_{\mathbb{R}} \Leftrightarrow$

③ $w \in \langle v \rangle_{\mathbb{R}} \Leftrightarrow$

④ $\langle v \rangle_{\mathbb{R}} = \langle w \rangle_{\mathbb{R}}$

①

v, w linear abhängig $\rightarrow \exists a_1, a_2 \in \mathbb{R}$, nicht beide $= 0$, $a_1 v + a_2 w = \sigma$. Dann beide $(a_1, a_2) \neq 0$

$$a_1 v = -a_2 w \mid \cdot \frac{1}{a_1}$$

$$v = -\frac{-a_2}{-a_1} w \in \langle w \rangle_{\mathbb{R}} \textcircled{2}$$

②

$v \in \langle w \rangle_{\mathbb{R}}$ dass heißt $v = aw$ für ein $a \in \mathbb{R}$ Dann $a \neq 0$, da $v \neq \sigma$. $w = \frac{1}{a} \cdot v \in \langle v \rangle_{\mathbb{R}} \textcircled{3}$

③

$w = bv$ für ein $b \in \mathbb{R} b \neq 0$, da $w \neq \sigma$.

$$aw \in \langle w \rangle_{\mathbb{R}} \Rightarrow aW = (ab)v \in \langle v \rangle_{\mathbb{R}}$$

$$\langle w \rangle_{\mathbb{R}} \subseteq \langle v \rangle_{\mathbb{R}}$$

$$w = \frac{1}{b} w \text{ Dann analog } \langle v \rangle_{\mathbb{R}} \subseteq \langle w \rangle_{\mathbb{R}}$$

$$\text{Also } \langle v \rangle_{\mathbb{R}} = \langle w \rangle_{\mathbb{R}} \textcircled{4}$$

④

$v \in \langle v \rangle_{\mathbb{R}} = \langle w \rangle_{\mathbb{R}}$, dass heißt.

$v = a \cdot w$ für ein $a \in \mathbb{R}$

$a \cdot v + (-a)w = \sigma \Rightarrow v, w$ sind linear abhängig ①

$$\text{d) } e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \in \mathbb{R}^n$$

e_1, \dots, e_n sind linear unabhängig.

$$\sigma = a_1 e_1 + \dots a_n e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_2 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow a_1 = a_2 = \dots = a_n = 0$$

e) $\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -3 \\ 1 \end{pmatrix}, \begin{pmatrix} 6 \\ 2 \end{pmatrix}$ sind linear abhängig \mathbb{R}^2 :

Gesucht sind alle $a_i, b_i \in \mathbb{R}$ mit $a \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} + b \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix} + c \cdot \begin{pmatrix} 6 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

Führt auf LGS für a,b,c:

$$\begin{pmatrix} 1 & -3 & 6 & 0 \\ 2 & 1 & 2 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -3 & 6 & 0 \\ 0 & 7 & -10 & 0 \end{pmatrix}$$

c ist frei wählbar

f) $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$ sind linear abhängig in \mathbb{R}^3 ,

$$10.8b) : \frac{5}{4} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \frac{1}{4} \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} + (-1) \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

0.11 Satz

Seien $v_1, \dots, v_n \in \mathbb{R}^n$

a) v_1, \dots, v_m sind linear abhängig ①

$$\Leftrightarrow \exists i \dots v_i = \sum_{\substack{j=1 \\ j \neq i}}^m b_j v_j \text{ ②}$$

$$\Leftrightarrow \exists i : \langle v_1, \dots, v_m \rangle_{\mathbb{R}} = \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m \rangle_{\mathbb{R}} \text{ ③}$$

b) v_1, \dots, v_m sind linear unabhängig \Leftrightarrow Jedes $v \in \langle v_1, \dots, v_m \rangle_{\mathbb{R}}$ lässt sich auf *genau eine* Weise als Linearkombination von v_1, \dots, v_m schreiben.

c) Sind v_1, \dots, v_m linear unabhängig und es existiert $v \in \mathbb{R}^n$ mit $v \notin \langle v_1, \dots, v_m \rangle_{\mathbb{R}}$ dann sind auch v_1, \dots, v_m, v linear unabhängig

Beweis. a) ① \Rightarrow ②

v_1, \dots, v_m sind linear abhängig

$\Rightarrow \exists a_1, \dots, a_m$ nicht alle = 0,

$$a_1 v_1 + \dots + a_m v_m = 0$$

Sei $a_i \neq 0$

$$a_i v_i = \sum_{\substack{j=1 \\ j \neq i}}^m -a_j v_j$$

$$v_i = \sum_{\substack{j=1 \\ j \neq i}}^m -\frac{a_j}{a_i} v_j \quad (2)$$

$$(2) \Rightarrow (3)$$

Klar: $\langle v_1, \dots, v_{i-1}, v_{i+1}, v_m \rangle_{\mathbb{R}} \subseteq \langle v_1, \dots, v_m \rangle_{\mathbb{R}}$

Zeige \supseteq $v = \langle v_1, \dots, v_m \rangle_{\mathbb{R}}$, d.h.

$$v = \sum_{j=1}^m a_j v_j = \sum_{\substack{j=1 \\ j \neq i}}^m a_j v_j + a_i \left(\sum_{\substack{j=1 \\ j \neq i}}^m b_j v_j \right) = \sum_{\substack{j=1 \\ j \neq i}}^m (a_j + a_i b_j) v_j \in \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m \rangle_{\mathbb{R}} \quad (2)$$

$$(3) \Rightarrow (1)$$

$v_i \in \langle v_1, \dots, v_m \rangle_{\mathbb{R}} = \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m \rangle_{\mathbb{R}}$, dass heißt es existiert

$a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_m \in \mathbb{R}$ mit

$$v_i = \sum_{\substack{j=1 \\ j \neq i}}^m a_j v_j$$

$\Rightarrow \sigma = a_1 v_1 + \dots + a_{i-1} v_{i-1} + (-1) v_i + a_{i+1} v_{i+1} + \dots + a_m v_m$ v_1, \dots, v_m linear abhängig □

0.12 Satz

Sind $v_1, \dots, v_{n+1} \in \mathbb{R}^n$, so

v_1, \dots, v_{n+1} linear abhängig.

(Insbesondere ist $m > n$ und $v_i, v_m \in \mathbb{R}^n$, so sind v_1, \dots, v_m linear abhängig)

Beweis. Suche alle $a_1, \dots, a_{n+1} \in \mathbb{R}$ mit $a_1 v_1 + \dots + a_{n+1} v_{n+1} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

Führt zu LGS für a_1, \dots, a_{n+1} mit Koeffizientenmatrix $(v_1, \dots, v_{n+1}) = A$

Frage: Hat $A \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^n$ nicht triviale Lösung?

Gauß:

$$\left(\mathbf{A} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \rightarrow \right)$$

□

0.13 Definition

Sei \mathcal{U} ein Unterraum von \mathbb{R}^n

$B \subseteq \mathcal{U}$ heißt Basis von \mathcal{U} falls:

(1) $\langle B \rangle_{\mathbb{R}} = \mathcal{U}$

(2) B ist linear unabhängig

($\mathcal{U} = \{\sigma\}, B = \emptyset$)

0.14 Beispiel

a) e_1, \dots, e_n ist Basis von \mathbb{R}^n (kanonische Basis)

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i$$

$$\begin{pmatrix} a_i \\ \vdots \\ a_n \end{pmatrix} = \sum_{i=1}^n a_i e_i$$

b) $\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ ist Basis von \mathbb{R}^2 :

Sei $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$. Gesucht: $a, b \in \mathbb{R}$ mit $a \begin{pmatrix} 1 \\ 2 \end{pmatrix} + b \begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$

LGS mit variabler rechter Seite

$$\begin{array}{rcl} 1a & +3b & = x \\ 2a & +2b & = y \end{array}$$

Gauß:

$$\begin{pmatrix} 1 & 3 & x \\ 2 & 2 & y \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & x \\ 0 & -4 & y-2x \end{pmatrix}$$

Eindeutige Lösung: $b = -\frac{1}{4}y + \frac{1}{2}x$ $a = x - 3b = x + \frac{3}{4}y - \frac{3}{2}x = -\frac{1}{2}x + \frac{3}{4}y$

$$\text{z.B. } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = -\frac{1}{2} \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 3 \\ 2 \end{pmatrix} \in \mathbb{R}^2 \langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix} \rangle$$

$\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ sind linear unabhängig nach 0.10c)

$$\left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix} \right\} \text{ Basis.}$$

$$\text{c) } \mathcal{U} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \right\rangle_{\mathbb{R}}$$

$$\begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \frac{5}{4} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \frac{1}{4} \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$$

$$\mathcal{U} = \left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \right\rangle_{\mathbb{R}}$$

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \text{ linear unabhängig (0.10c)}$$

$$\left\{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \right\} \text{ Basis von } \mathcal{U}$$

0.15 Satz

Jeder Unterraum \mathcal{U} des \mathbb{R}^n besitzt eine Basis.

Beweis. Ist $\mathcal{U} = \{\sigma\}$, so $b = \emptyset$.

Sei also $\mathcal{U} \neq \{\sigma\}$.

v_1 ist linear unabhängig.

$\langle v_1 \rangle_{\mathbb{R}} \subseteq \mathcal{U}$.

Ist $\mathcal{U} = \langle v_1 \rangle_{\mathbb{R}}$, so ist $\{v_1\}$ Basis von \mathcal{U}

Ist $\langle v_1 \rangle_{\mathbb{R}} \subsetneq \mathcal{U}$.

Sei $v_2 \in \mathcal{U} \setminus \langle v_1 \rangle_{\mathbb{R}}$.

Nach 0.11c) ist $\{v_1, v_2\}$ linear unabhängig. Ist $\langle v_1, v_2 \rangle = \mathcal{U}$, so ist $\{v_1, v_2\}$ Basis von \mathcal{U} .

Ist $\langle v_1, v_2 \rangle_{\mathbb{R}} \subsetneq \mathcal{U}$ so wähle v_3 usw.

Es existiert $m \neq n$ mit $\langle v_1, \dots, v_m \rangle_{\mathbb{R}} = \mathcal{U}$ und v_1, \dots, v_m sind linear unabhängig.

(Denn noch 0.12 gibt es im \mathbb{R}^n keine $n+1$ linear unabhängige Vektoren) \square

0.16 Satz

Je zwei Basen B_1, B_2 eines Unterraums \mathcal{U} des \mathbb{R}^n enthalten die gleiche Anzahl von Vektoren $|B_1| = |B_2|$.

Insbesondere:

Je zwei Basen des \mathbb{R}^n enthalten n Vektoren

0.17 Definition

Ist \mathcal{U} Unterraum von \mathbb{R}^n , B Basis von \mathcal{U} , $|B| = m$.

Dann ist m die *Dimension* von \mathcal{U} , $\dim(\mathcal{U}) = m$.

$\dim(\mathbb{R}^n) = n$, $\dim(\mathcal{U}) \neq n$.

0.18 Satz (Basisergänzungssatz)

Sei \mathcal{U} Unterraum der \mathbb{R}^n , $M \subseteq \mathcal{U}$ eine Menge m linear unabhängiger Vektoren.

Dann lässt sich M zu einer Basis von \mathcal{U} ergänzen.

Beweis. Analog zu 0.15 \square

0.19 Korollar

Ist \mathcal{U} Unterraum des \mathbb{R}^n und $\dim(\mathcal{U}) = n$, dann ist $\mathcal{U} = \mathbb{R}^n$

Beweis. Sei B Basis von \mathcal{U} , also $|B| = n$.

Nach 0.18 (dort mit $\mathcal{U} = \mathbb{R}^n$, $M = B$) lässt sich B zu Basis B' von \mathbb{R}^n ergänzen.

$$\dim(\mathbb{R}^n) = n \Rightarrow |B'| = n.$$

Also $B = B'$

$$\mathbb{R}^n = \langle B' \rangle_{\mathbb{R}} = \langle B \rangle_{\mathbb{R}} = \mathcal{U}$$

□

0.20 Definition

Ist \mathcal{U} Unterraum von \mathbb{R}^n , $B = (u_1 \dots, u_m)$ eine geordnete Basis von \mathcal{U} . Nach 0.11b), lässt sich jeder Vektorraum $\mathcal{U} = \langle B \rangle_{\mathbb{R}}$ *eindeutig* als Linearkombination

$$\mathcal{U} = \sum_{i=1}^m a_i u_i \quad , a_i \in \mathbb{R}$$

schreiben.

$(a_1 \dots, a_m)$ heißen *Koordinaten* von u bzgl. der Basis B .

0.21 Beispiele

a) $B(e_1 \dots, e_m)$ kanonische Basis von \mathbb{R}^n .

Koordinaten von $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{R}^n$ bzgl. B :

$(a_1 \dots, a_n)$ *kartesische* Koordinaten.

(Rene Descartes, 1596-1650)

Anfang des WS 2015/16

1 Algebraische Strukturen

13.10.2015

1.1 Definition

Sei $X \neq \emptyset$. Eine *Verknüpfung* auf X ist :

$$\begin{cases} X \times X & \longrightarrow X \\ (a, b) & \longrightarrow a \star b \end{cases} \quad (\text{'Produkt' von a und b})$$

\star ist Platzhalter für andere Verknüpfungssymbole, die in speziellen Beispielen auftreten können.

1.2 Beispiele

a) Addition $+$ und Multiplikation \cdot sind Verknüpfungen auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Multiplikation ist *keine* Verknüpfung auf der Menge der negativen ganzen Zahlen.

b) Division ist keine Verknüpfung auf \mathbb{N} . Division ist Verknüpfung auf $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$

c) $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$ ($n \in \mathbb{N}$)

$$a \oplus b := (a + b) \bmod n \quad n \in \mathbb{Z}_n$$

$$a \odot b := (a \cdot b) \bmod n \quad n \in \mathbb{Z}_n$$

Verknüpfungen auf \mathbb{Z}_n

$$n = 7: \quad 5 \odot 6 = 2$$

$$5 \oplus 6 = 4$$

$$n = 2: \quad \mathbb{Z}_n = \{0, 1\}$$

$$0 \oplus 0 = 0, 1 \oplus 0 = 1, 0 \oplus 1 = 1, 1 \oplus 1 = 0$$

$$\odot = \cdot$$

d) M Menge, $X =$ Menge aller Abbildungen $M \longrightarrow M$. Verknüpfung auf X : Hintereinanderausführung von Abbildungen: \circ

$$(f, g): M \longrightarrow M, \text{ So } f \circ g: M \rightarrow M$$

$$(f \circ g)(m) = f(g(m)) \in M, m \in M$$

Im Allgemeinen ist $g \circ f \neq f \circ g$

e) $X = \{0, 1\}$

2-stellige Aussagen, Junktoren wie $\wedge, \vee, \text{XOR}, \Rightarrow, \Leftrightarrow$ heißen Verknüpfungen auf X . 0 entspricht f, 1 entspricht w.

$$0 \vee 0 = 0, 1 \vee 0 = 1, 0 \vee 1 = 1, 1 \vee 1 = 1$$

$$0 \wedge 0 = 0, 0 \wedge 1 = 0, 1 \wedge 0 = 0, 1 \wedge 1 = 1 \text{ (= 'Multiplikation')}$$

$$0 \text{ XOR } 0 = 0, 1 \text{ XOR } 0 = 1, 0 \text{ XOR } 1 = 1, 1 \text{ XOR } 1 = 0 \text{ (= Addition mod 2)}$$

f) $X = M_n(\mathbb{R})$ = Menge der $n \times n$ - Matrizen über \mathbb{R} .

Matrizenaddition ist Verknüpfung auf X .

Matrizenmultiplikation ist Verknüpfung auf X .

g) M Menge. X Menge aller endlichen Folgen von Elementen aus M ('Wörter' über M).

Verknüpfung: Hintereinanderausführung zweier Folgen (Konkatenation).

$$M = \{0, 1\}, w_1 = 1101, w_2 = 001$$

$$w_1 w_2 = 110111$$

$$w_2 w_1 = 0011101$$

1.3 Definition

Sei $X \neq \emptyset$ eine Menge mit Verknüpfung \star .

a) X , genauer (X, \star) ist *Halbgruppe*, falls $(a \star b) \star c = a \star (b \star c)$ für alle $a, b, c \in X$.
(Assoziativgesetz)

b) (X, \star) heißt *Monoid*, falls (X, \star) Halbgruppe ist und ein $e \in X$ existiert mit $e \star a = a$ und $a \star e = a$ für alle $a \in X$. e heißt *neutrales Element* (später, e ist eindeutig bestimmt).

c) Sei (X, \star) ein Monoid. Ein Element $a \in X$ heißt *invertierbar*, falls $b \in X$ existiert (abhängig von a) mit $a \star b = b \star a = e$. b heißt *inverses Element* (das *Inverse*) zu a (später: wenn b existiert, so ist es eindeutig bestimmt).

d) Monoid (X, \star) heißt *Gruppe*, falls jedes Element in X bezüglich \star invertierbar ist.

- e) Halbgruppe, Monoid, Gruppe (X, \star) bezüglich kommutativ (oder *abelsch*) falls $a \star b = b \star a$ für alle $a, b \in X$ (Kommutativgesetz).

(Nach: Abel, 1802-1829)

14.10.2015

«««< HEAD

1.4 Bemerkung

In Halbgruppe liefert jede sinnvolle Klammerung eines Produktes mit endlich vielen Faktoren das gleiche Element. =====

1.5 Bemerkung

In Halbgruppe liefert jede sinnvolle Klammerung eines Produktes mit endlich vielen Faktoren das gleiche Element.

»»»> dbd12bd4a4b0c211913e023b2cc43fbc6e314244

(n = 4)

$$(a \star (b \star c)) \star d \underset{\text{AG}^1}{=} ((a \star b) \star c) \star d \underset{\text{AG}^1}{=} (a \star b) \star (c \star d) \underset{\text{AG}^1}{=} a \star (b \star (c \star d)) \underset{\text{AG}^1}{=} a \star ((b \star c) \star d)$$

Klammern werden daher meist weggelassen.

$a^n = a \star \dots \star a$ "Potenzen eindeutig definiert"
 $\xleftarrow[n \in \mathbb{R}]{n}$

1.6 Proposition

- In einem Monoid (X, \star) ist das neutrale Element eindeutig bestimmt.
- Ist (X, \star) Monoid und ist $a \in X$ invertierbar, so ist das Inverse zu a eindeutig bestimmt. Bezeichnung: a^{-1}
- Ist (X, \star) Monoid und wenn $a, b \in X$ invertierbar sind, so auch $a \star b$.
 $(a \star b)^{-1} = b^{-1} \star a^{-1}$
- Die Menge der invertierbaren Elemente in einem Monoid (X, \star) bilden bezüglich \star eine Gruppe.

¹Assoziativgesetz

Beweis. a) Angenommen: e_1, e_2 sind neutrale Elemente. Dann:

$$e_1 = e_1 \star e_2 = e_1 \star e_2 = e_2 \quad \neq$$

b) Angenommen a hat 2 inverse Elemente b_1, b_2 also.

$$\begin{aligned} a \star b_1 &= e, b_2 \star a = e \\ b_1 &= e \star b_1 = (b_2 \star a) \star b_1 = b_2 \star (a \star b_1) = b_2 \star e = b_2 \quad \neq \end{aligned}$$

c)

$$(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star e \star a^{-1} = e$$

Analog: $(b^{-1} \star a^{-1}) \star (a \star b) = e$

Also: $(a \star b)^{-1} = b^{-1} \star a^{-1}$

d) \mathcal{J} = Menge der inversen Elemente in (X, \star) ,

$e \in \mathcal{J}$, dann $e \star e = e$, dass heißt $e^{-1} = e$, \star ist Verknüpfung auf \mathcal{J} .

Zu zeigen: $a, b \in \mathcal{J} \Rightarrow a \star b \in \mathcal{J}$ Folgt aus c).

Assoziativgesetz gilt in \mathcal{J} , $a \in \mathcal{J} \Rightarrow a^{-1} \in \mathcal{J}$, denn $(a^{-1})^{-1} = a$ □

Bemerkung: Multiplikation mit a^{-1} macht Multiplikation mit a (Verknüpfung) rückgängig.

1.7 Beispiel

a) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Halbgruppen bezüglich $+$.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind bezüglich $+$ Monoide mit neutralen Element 0.

$\mathbb{N} = \{1, 2, \dots\}$ ist kein Monoid bezüglich $+$, aber \mathbb{N}_0 .

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Gruppen bezüglich $+$. Inverses Element zu a : $-a$

\mathbb{N} ist keine Gruppe bezüglich $+$, Inverse Elemente in \mathbb{N}_0 : $\{0\}$

b) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Monoide bezüglich \cdot (neutrales Element 1). Keine Gruppen (in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ist 0 nicht invertierbar).

$\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ Gruppen.

Invertierbare Elemente in $\mathbb{Z} :: \{1, -1\} \leftarrow$ Gruppe bezüglich \cdot
 \uparrow
 Eigenes Inverses

c) M Menge.

$X =$ Menge aller Abbildungen $M \longrightarrow M$ mit Hintereinanderausführung \circ als Verknüpfung.

Monoid, neutrales Element. id_M

$$f \circ id_M = f = id_M \circ f$$

$$id_M(m) = m \text{ für alle } m \in M.$$

Invertierbar sind genau die bijektiven Abbildungen $M \longrightarrow M$, Inverse = Umkehrabbildung.

$f : M \longrightarrow M$ bijektiv

$$f \circ f^{-1} = f^{-1} \circ f = id_M$$

‘Proposition’ on page 23 d): Die bijektive n Abbildung, $M \longrightarrow M$ bilden bezüglich \circ eine Gruppe

d) $M =$ Menge z.B $\{0, 1\}$, x Menge aller endlichen Folgen über m . Halbgruppe mit Verknüpfung Konkatination . Nimmt man die leere Folge mit hinzu, ist es das neutrale Element. Dann: Monoid.

e) $M_n(\mathbb{R})$ Menge der Matrizen über \mathbb{R} .

Addition: neutrales Element $0 - Matrix$, Inverse zu A ist $-A$. $(M, Addition)$ ist Gruppe

Multiplikation: $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ Halbgruppe mit neutralem Element I_m

f) $n \in \mathbb{N} \quad \mathbb{Z}_n = \{0, \dots, n-1\} \quad$ Verknüpfung \oplus

$$a \oplus b = a + b \mod n$$

(\mathbb{Z}_n, \oplus) ist Gruppe.

Assoziativgesetz: $a, b, c \in \mathbb{Z}_n$

$$\begin{aligned} (a \oplus b) \oplus c &= (a + b \mod n) \mod n \\ &= ((a + b) + c) \mod n \\ &\stackrel{\text{Mathe I}}{=} (a + (b + c)) \mod n \\ &= (a + (b + c) \mod n) \mod n \\ &\stackrel{\text{Mathe I}}{=} (a + (b \oplus c)) \mod n \\ &= (a \oplus (b \oplus c)) \end{aligned}$$

0 ist neutrales Element bezüglich \oplus

0 ist sein eigenes Inverse.

$1 \leq i \leq n$ $n - i \in \mathbb{Z}_n$ Inverses zu i

$$i \oplus (n - i)$$

$$= (i + (n - i)) \bmod n = n \bmod n = 0$$

g) $n \in \mathbb{N}, \mathbb{Z}_0$ Verknüpfung \odot $n > 1$

$$a \odot b = a \cdot b \bmod n$$

(\mathbb{Z}_n, \odot) ist Monoid

Assoziativgesetz wie bei \oplus .

1 ist neutrales Element bei \odot Keine Gruppe bezüglich \odot , denn 0 hat kein Inverses

1.8 Satz

Sei $n \in \mathbb{N}, n > 1$

a) Die Elemente in (\mathbb{Z}_n, \odot) , die invertierbar bezüglich \odot sind, sind genau diejenigen $a \in \mathbb{Z}_n$ mit $\text{ggT}(a, n) = 1$.

Für solche a bestimmt man das Inverse folgendermaßen:

Bestimme $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot n = 1$ (Erweiterter Euklidischer Algorithmus)

Dann ist $a^{-1} = s \bmod n$

b) $\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n : \text{ggT}(a, n) = 1\}$ ist Gruppe bezüglich \odot .

$|\mathbb{Z}_n^*| =: \varphi(n)$ Euler'sche φ -Funktion (Leonard Euler 1707-1783)

c) Ist p eine Primzahl so ist $(\mathbb{Z}_p \setminus \{0\}, \odot)$ eine Gruppe. *Beweis* folgt aus b)

Beweis. a) Angenommen $a \in \mathbb{Z}_n$ invertierbar bezüglich \odot

D.h es existiert $b \in \mathbb{Z}_n$ mit $a \odot b = 1$

$a \cdot b \bmod n = 1$, d.h es existiert $k \in \mathbb{Z}$ mit $a \cdot b = 1 + k \cdot n, 1 = a \cdot b - k \cdot n$

Sei $d = \text{ggT}(a, n)$:

$$d \mid a \Rightarrow d \mid a \cdot b$$

$$d \mid n \Rightarrow d \mid k \cdot n$$

$$\Rightarrow d \mid a \cdot b - k \cdot n = 1$$

$$\Rightarrow d = 1 \quad \text{ggT}(a, n) = 1.$$

Umgekehrt sei $a \in \mathbb{Z}_n$ mit $\text{ggT}(a, n) = 1$

EEA liefert $s, t \in \mathbb{Z}$ mit $s \cdot a + t \cdot n = 1$.

$$\begin{aligned}
 & (s \bmod n) \odot a &= ((s \bmod n) \cdot a) \bmod n \\
 \stackrel{\text{Mathe I}}{=} & (s \cdot a) \bmod n &= (1 - t \cdot n) \bmod n \\
 = & (1 - \underbrace{(t \cdot n) \bmod n}_{=0}) \bmod n &= 1 \bmod n = 1
 \end{aligned}$$

b) 'Proposition' on page 23 d)

□

1.9 Beispiel

$n = 24$, $a = 7$ ist invertierbar in (\mathbb{Z}_{24}, \odot)

EEA:

$$\begin{aligned}
 1 &= (-2) \cdot 24 + 7 \cdot 7 \\
 a^{-1} &= 7 \bmod 24 = 7 = a
 \end{aligned}$$

1.10 Beispiel

Sei $M = \{1, \dots, n\}$

Die Menge der bijektiven Abbildungen auf M (*Permutationen*) bilden nach 1.7c) eine Gruppe bezüglich Hintereinanderausführung \circ .

Bezeichnung: S_n *systematische Gruppe von Grad n*

Es ist $|S_n| = n!$

(Mathe I)

$$\text{z.B.: } \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$$

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

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

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

$$\varrho \circ \varrho^{-1} = id$$

$$\pi \circ \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\varrho \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

S_n ist für $n \geq 3$ nicht abelsch (nicht kommutativ)

1.11 Satz (Gleichungslösen in Gruppen)

Sei (G, \cdot) eine Gruppe $a, b \in G$ (in allgemeinen Gruppen schreibt man Verknüpfungen oft als \cdot statt \star , oft auch ab statt $a \cdot b$)

- a) Es gibt genau ein $x \in G$ mit $ax = b$ (nämlich $x = a^{-1}b$) ["Teilen durch" a von links = Multiplikation von links mit a^{-1}]
- b) Es gibt genau ein $y \in G$ mit $ya = b$ (nämlich $y = ba^{-1}$)
- c) Ist $ax = bx$ für ein $x \in G$, so ist $a = b$
Ist $ya = yb$ für ein $y \in G$, so ist $a = b$

Beweis. a) Setze $x = a^{-1}b \in G$.

$a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1})b = a \cdot b = b$ Eindeutigkeit : Sei $x \in G$ mit $ax = b$

Multiplikation beide Seiten mit a^{-1} ,

$$x = (a^{-1}a)x = a^{-1}b$$

b) analog

c) $ax = bx$ Multiplikation mit x^{-1} Dann $a = b$

□

1.12 Beispiel

- a) Suche Permutation $\xi \in S_3$ mit $\varrho \circ \xi = \pi$ (vgl. 1.10). 'Satz (Gleichungslösen in Gruppen)' on page 28a):

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

- b) 1.11c) gilt in Monoiden, die keine Gruppen sind, im Allgemeinen nicht:

Beispiel: (\mathbb{Z}_0, \odot)

$$2 \odot 3 - 0 = 3 \odot 3, \text{ aber } 2 \neq 4$$

1.13 Definition

a) $R \neq \emptyset$ Menge mit 2 Verknüpfungen $+$ und \cdot heißt *Ring*, falls

(1) $(R, +)$ ist kommutative Gruppe (neutrales Element: 0, *Nullelement*, Inverses zu a : $-a$ $b + (-a) =: b - a$)

(2) (R, \cdot) ist Halbgruppe

(3) $(a + b) \cdot c = a \cdot c + b \cdot c$ und $a \cdot (b + c) = a \cdot b + a \cdot c$ (\cdot vor $+$)
Distributivgesetz

b) Ring R heißt *kommutativer Ring* falls (R, \cdot) kommutative Halbgruppe ist.

c) Ring R heißt *Ring mit Eins*, falls (R, \cdot) Monoid, neutrales Element $1 \neq 0$ (*Eins-element*, *Eins*)

1.14 Beispiele

a) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit 1, invertierbare Elemente bezüglich \cdot sind 1 und -1 .

b) $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins.
Alle Elemente $\neq 0$ sind invertierbar bezüglich \cdot .

c) $n \in \mathbb{N}, n > 1$.

$$\mathbb{Z}_n = \{0, \dots, n-1\}$$

$(\mathbb{Z}_n, \oplus, \odot)$ ist kommutativer Ring mit Eins:

Wegen 'Beispiel' on page 24 f),g) sind nur die Distributivgesetz zu zeigen:

$$\begin{aligned} (a \oplus b) \odot c &= ((a \oplus b) \cdot c) \bmod n \\ &= (((a + b) \bmod n) \cdot c) \bmod n \\ &= ((a + b) \cdot c) \bmod n \\ \text{Mathe I} \quad &= (a \cdot c + b \cdot c) \bmod n \\ &= ((a \cdot c) \bmod n + (b \cdot c) \bmod n) \bmod n \\ \text{Mathe I} \quad &= a \odot c \oplus b \odot c \end{aligned}$$

d) $M_n(\mathbb{R}), n \times n$ -Matrizen über \mathbb{R} , mit Matrizenaddition $+$ und, Multiplikation \cdot ist Ring mit Eins.

(Folgt aus Rechenregeln für Matrizen, Mathe II) Eins : E_n $n \times n$ -Einheitsmatrix
 Für $n \geq 2$ ist $M_n(\mathbb{R})$ kein kommutativer Ring

1.15 Proposition

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

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

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

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

Beweis.

a) $0 \cdot a = (0 + 0) \cdot a \stackrel{\text{DG}^2}{=} 0 \cdot a + 0 \cdot a$
 Addiere auf beiden Seiten $-(0 \cdot a)$
 $0 = 0 \cdot a + 0 = 0 \cdot a$

b) $(-a) \cdot b + ab = ((-a) + a) \cdot b \stackrel{\text{a)}}{=} 0 \cdot b = 0$
 $\Rightarrow (-a) \cdot b = -(ab)$ Analog $a \cdot (-b) = -(ab)$

c) $(-a) \cdot (-b) \stackrel{\text{b)}}{=} -(a \cdot (-b)) \stackrel{\text{b)}}{=} -(-(a \cdot b)) = a \cdot b$

□

1.16 Bemerkung

a) In einem Ring mit Eins sind 1 und -1 bezüglich \cdot invertierbar.

$$1 \cdot 1 = 1 \quad (1^{-1} = 1)$$

$$(-1) \cdot (-1) = 1 \quad (1.15c)), \text{ dass heißt. } (-1)^{-1} = -1$$

0 ist nie bezüglich Multiplikation invertierbar, denn $0 \cdot a = 0 \neq 1$. 1.15a)

b) Es kann sein dass $1 = -1$ gilt. Zum Beispiel:

$$(\mathbb{Z}_2, \oplus, \odot) \quad 1 \oplus 1 = 0 \quad 1 = -1$$

²Distributivgesetz

1.17 Definition

Ein kommutativer Ring $(R, +, \cdot)$ mit Eins heißt *Körper*, wenn jedes Element $\neq 0$ bezüglich Multiplikation invertierbar ist.

1.18 Beispiel

a) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper, \mathbb{Z} nicht.

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

\mathbb{Z}_n ist kommutativer Ring mit 1.

‘Beispiele’ on page 29c: Die invertierbaren Elemente in \mathbb{Z}_n sind alle $a \in \mathbb{Z}_n$ mit $\text{ggT}(a, n) = 1$

1.19 Proposition (Nullteilerfreiheit in Körpern)

Ist K ein Körper, $a, b \in K$, mit $a \cdot b = 0$, so ist $a = 0$ oder $b = 0$

Beweis.

Sei $a \cdot b = 0$ Angenommen $a \neq 0$. Dann existiert $a^{-1} \in K$

$$0 \underset{1.15a)}{=} a^{-1} \cdot 0 \underset{\text{Vor.}}{=} a^{-1}(a \cdot b) = (a^{-1} \cdot a) \cdot b = b$$

□

Beispiel: $R = (\mathbb{Z}_6, \oplus, \odot)$

$$2 \odot 3 = 0 \quad 2 \neq 0, 3 \neq 0$$

1.20 Definition

Sei K ein Körper,

a) Ein (Formales) *Polynom* über K ist ein Ausdruck $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \sum_{i=0}^n a_i x^i$ wobei $n \in \mathbb{N}_0, a_i \in K$. (Manchmal $f(x)$ statt f , $+$ -Zeichen hat zunächst nichts mit einer Addition zu tun. a_i *Koeffizienten* von f)

Ist $a_i = 0$ so kann man in der Schreibweise von f $0 \cdot x^i$ auch weglassen.

Statt a_0x^0 schreibt man a_0 , statt a_1x^1 schreibt man a_1x . Sind alle $a_i = 0$, so $f = 0$, *Nullpolynom*.

Ist $a_i = 1$, so schreibt man x^i statt $1x^i$

- b) Zwei Polynome f und g sind *gleich*, wenn *entweder* $f = 0$ und $g = 0$ oder $f \neq 0$ und $g \neq 0$

$$\text{d.h. } f = \sum_{i=0}^n a_i x^i, a_n \neq 0$$

$$g = \sum_{i=0}^m a_i x^i, b_m \neq 0$$

und $n = m$ und $a_i = b_i$ für $i = 0 \dots n$

- c) Menge aller Polynome über K . $K[x]$

Wir wollen $K[x]$ zu einem Ring machen. Wie?

$$\text{Beispiel: } f = 3x^2 + 2x + 1,$$

$$g = 5x^3 + x^2 + x \in Q[x]$$

$$f + g = 5x^3 + 4x^2 + 3x + 1$$

$$f \cdot g = (3x^2 + 2x + 1) \cdot (5x^3 + x^2 + x)$$

$$= 15x^5 + 10x^4 + 5x^3 + 3x^4 + 2x^3 + x^2 + 3x^2 + 2x^2 + x$$

$$= 15x^5 + 13x^4 + 10x^3 + 3x^2 + x$$

27.10.2015

1.21 Satz und Definition

K Körper. $K[x]$ wird zu einem kommutativen Ring mit Eins durch folgenden Verknüpfungen.

$$f = \sum_{i=0}^n a_i x^i, g = \sum_{i=0}^m b_i x_i \text{ so}$$

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

$$f \cdot g = \sum_{i=0}^{n+m} c_i x^i, \text{ wobei } c_i = \sum_{j=0}^i a_j b_{i-j} \quad (\text{Faltungsprodukt})$$

In beiden Fällen sind Koeffizienten a_i mit $i > n$ bzw. b_i mit $i > m$ gleich 0 zu setzen. Das Einselement ist $1 (= 1x^0)$

Das Nullelement ist das Nullpolynom.

$$-f = \sum_{i=0}^n (-a_i) x^i$$

$(K[x], +, \cdot)$ heißt *Polynomring* in einer Variable *Beweis*: Nachrechnen

1.22 Bemerkung

$$\begin{aligned} \text{a) } f &= \sum_{i=0}^n a_i x^i \in K[x], a \in K \subseteq K[x] \\ a \cdot f &= \sum_{i=0}^n (a \cdot a_i) x^i \\ x \cdot f &= \sum_{i=0}^n a_i x^{i+1} = a_n x^{n+1} + \dots + a_0 x \end{aligned}$$

b) Das $+$ - Zeichen in der Definition der Polynome entspricht genau der Addition der *Monome* $a_i x^i$.

$$(a_0 x^0 \quad + \quad a_1 x^1) = a_0 x^0 \quad + \quad a_1 x^1$$

\uparrow Add. aus 1.21 \uparrow + aus 1.20

1.23 Definition

Sei $0 \neq f \in k[x]$, $f = \sum_{i=0}^n a_i x^i$, $a_n \neq 0$.

Dann heit n der *Grad* in f , $\text{Grad}(f) = n$

$\text{Grad}(0) := -\infty$

$\text{Grad}(f) := 0$: *Konstante Polynome* $\neq 0$

1.24 Satz

Sei K ein Krper, $f, g \in K[x]$.

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

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

Sei $f \neq 0$ und $g \neq 0$

$$f = \sum_{i=0}^n a_i x^i, a_n \neq 0, n = \text{Grad}(f)$$

$$g = \sum_{i=0}^m b_i x^i, b_m \neq 0, m = \text{Grad}(g)$$

Koeffizienten von x^{n+m} in $f \cdot g$: $a_n b_m \neq 0$
1.19

1.25 Korollar

Sei K ein Krper

- a) Genau die konstanten Polynome $\neq 0$ sind in $K[x]$ bezüglich \cdot invertierbar
Insbesondere ist $K[x]$ *kein* Körper
- b) Sind $f, g \in K[x]$ mit $f \cdot g = 0$, so ist $f = 0$ oder $g = 0$ (Nullteilerfreiheit in $K[x]$)
- c) Sind $f, g_1, g_2 \in K[x]$ mit $f \cdot g_1$ und ist $f \neq 0$, so ist $g_1 = g_2$

Beweis.

- a) Sei $f \in K[x]$ invertierbar bezüglich \cdot . Dann ist $f \neq 0$ und es existiert $g \in K[x]$ mit $f \cdot g = 1$.

Mit 1.24:

$$\begin{aligned} 0 = \text{Grad}(1) &= \text{Grad}(f \cdot g) \\ &= \text{Grad}(f) + \text{Grad}(g). \end{aligned}$$

$$\text{Also: } \text{Grad}(f) = 0 (= \text{Grad}(g))$$

Dass heißt f ist konstantes Polynom.

Ist umgekehrt $f = a \in K, a \neq 0$, so $f^{-1} = a^{-1} \in K$

- b) Folgt aus 1.24:

$$\begin{aligned} -\infty = \text{Grad}(0) &= \text{Grad}(f \cdot g) \\ &= \text{Grad}(f) + \text{Grad}(g) \end{aligned}$$

$$\Rightarrow \text{Grad}(f) = -\infty \text{ oder } \text{Grad}(g) = -\infty, \text{ d.h. } f = 0, \text{ oder } g = 0$$

- c) $f g_1 = f g_2$
 $\Rightarrow 0 = f g_1 - f g_2 = f \cdot (g_1 - g_2)$
 Da $f \neq 0$, folgt mit b)
 $g_1 - g_2 = 0$, d.h. $g_1 = g_2$

□

1.26 Bemerkung

- a) Jedem Polynom $f = \sum_{i=0}^n a_i x^i \in K[x]$

kann man eine Funktion $K \rightarrow K$ zuordnen. $a \in K \mapsto f(a) = \sum_{i=0}^n a_i a^i \in K$

(Polynomfunktion aus Analysis $K = \mathbb{R}$)

Aufgrund der Definition von Addition/Multiplikation von Polynomen gilt:

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

$$(f \cdot g)(a) = f(a) \cdot g(a)$$

Es kann passieren, dass zwei verschiedene Polynome die gleiche Funktion beschreiben.

$$\text{Z.B. } K = \mathbb{Z}_2 = \{0, 1\}$$

$$f = x^2, g = x$$

$$f \neq g$$

$$f(1) = 1 = g(1)$$

$$f(0) = 0 = g(0)$$

Über unendlichen Körpern passiert das nicht (später)

b) Schnelle Berechnung von $f(a)$:

$$f = a_0 + a_1x + \dots + a_nx^n$$

$$f(a) = a_0 + a(a_1 + a(a_2 + \dots + a(a_{n-1} + aa_n)))$$

Horner-Schema

1.27 Definition

K Körper, $f, g \in K[x]$

f teilt g ($f \mid g$) falls $q \in K[x]$ existiert mit $g = q \cdot f$ (Falls $g \neq 0 \pmod f \mid g$, so ist $\text{Grad}(f) \leq \text{Grad}(g)$ nach ‘Satz’ on page 33)

1.28 Satz

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

Dann existiert eindeutig bestimmte Polynome q, r

$$(1) \quad g = q \cdot f + r$$

$$(2) \quad \text{Grad}(r) < \text{Grad}(f)$$

(Beweis WHK, Satz 4.69)

Division mit Rest

28.10.2015

1.29 Beispiel

a) $g = x^4 + 2x^3 - x + 2, f = 3x^2 - 1, f, g \in Q[x]$

$$\begin{array}{r} (x^4 + 2x^3 - x + 2) : (3x^2 - 1) = \frac{1}{3}x^2 + \frac{2}{3}x + \frac{1}{9} + \frac{-\frac{1}{3}x + \frac{19}{9}}{3x^2 - 1} \\ \underline{-x^4 \quad + \frac{1}{3}x^2} \\ 2x^3 + \frac{1}{3}x^2 - x \\ \underline{-2x^3 \quad + \frac{2}{3}x} \\ \frac{1}{3}x^2 - \frac{1}{3}x + 2 \\ \underline{-\frac{1}{3}x^2 \quad + \frac{1}{9}} \\ -\frac{1}{3}x + \frac{19}{9} \end{array}$$

b) $g = x^4 - x^2 + 1 \quad f = x^2 + x \quad f, g \in \mathbb{Z}_3[x]$

$$\begin{array}{r} x^4 + 3x^3 + 1 : x^2 + x = x^2 + 2x \\ \underline{-(x^4 + x^3)} \\ 2x^3 + 2x^2 + 1 \\ \underline{-(2x^3 + 2x^2)} \\ 1 \leftarrow r \end{array}$$

1.30 Korollar

K Körper, $a \in K$.

$f \in K[x]$ ist genau dann durch $(x - a)$ teilbar, wenn $f(a) = 0$ (d.h. a ist Nullstelle von f)

$$[f = g \cdot (x - a), g \in K[x]]$$

Beweis.

Falls $x - a \mid f$, so existiert $q \in K[x]$ mit $f \stackrel{1.26}{=} q(x - a)$.

$$\text{Dann } f(a) = q(a) \cdot \underbrace{(a - a)}_{=0} = 0.$$

Umgekehrt: Angenommen $f(a) = 0$. Division mit Rest von f durch $x - a$:

$$f = q \cdot (x - a)r, q, r \in K[x]$$

$$\text{Grad}(r) < \text{Grad}(x - a) = 1, r \in K$$

Zeige: $r = 0$.

$$r = f - q \cdot (x - a)$$

Setze $a \in K$ ein.

$$\begin{aligned} r &= f(a) - q(a) \cdot (a - a) = 0 - 0 = 0 \\ f &= q \cdot (x - a) \end{aligned}$$

□

1.31 Definition

K Körper $a \in K$ heißt m -fache Nullstelle von $f \in K[x]$, falls $(x - a)^m \mid f$ und $(x - a)^{m+1} \nmid f$.

Dass heißt $f = q \cdot (x - a)^m$ und $q(a) \neq 0$

1.32 Beispiel

$$x^5 + x^4 + 1 \in \mathbb{Z}_3[x]$$

In \mathbb{Z}_3 hat f die Nullstelle 1

‘Korollar’ on page 36: $x - 1 (= x + 2)$ teilt f

Dividiere f durch $x - 1$:

$$f = (x^4 + 2x^3 + 2x + 2) \cdot (x - 1)$$

1.33 Satz

K Körper, $f \in K[x]$, $\text{Grad}(f) = n \geq 0$ (dass heißt $f \neq 0$).

Dann hat f höchstens n Nullstellen in K (einschließend Vielfachheit). Genauer:

Sind a_1, \dots, a_k die verschiedenen Nullstellen von f , so ist

$f = g \cdot (x - a_1)^{m_1} \cdot \dots \cdot (x - a_k)^{m_k}$, m_i Vielfachheiten der Nullstellen a_i , g hat keine Nullstelle in K

Beweis. Durch Induktion nach n .

$n = 0$: $f = a_0 \neq 0$, ohne Nullstelle. ✓

Sei $n > 0$. Behauptung sei richtig für alle Polynome von $\text{Grad} < n$.

Hat f keine Nullstellen, $g = f$ ✓

Hat f Nullstellen a_1, \dots, a_k , $k \geq 1$

so $f = q \cdot (x - a_1)^{m-1}$ (nach Definition) $q(a_1) \neq 0$.

$$\text{Grad}(q) = n - m_1 \underset{m_1 > 0}{<} n$$

Wir zeigen:

q hat genau die Nullstellen a_2, \dots, a_k mit Vielfachheiten m_2, \dots, m_k .

Klar: Jede Nullstelle von q ist Nullstelle von f , Dass heißt q hat höchstens Nullstellen a_2, \dots, a_k .

Diese Nullstellen hat q mit Vielfachheit $0 \geq n_i \geq m_i$, denn $(x - a_i)^{m_i} | q \Rightarrow (x - a_i)^{n_i} | f$

Sei $i \in \{2, \dots, k\}$. Es ist $f = s \cdot (x - a_i)^{m_i}$, $s \in K[x]$, $s(a_i) \neq 0$

$$q = q_1 \cdot (x - a_i)^{n_i}, q_1 \in K[x], q(a_i) \neq 0, \quad ((x - a_i)^0 = 1)$$

$$f = q_1(x - a_1)^{n_i} \cdot (x - a_1)^{m_1} \text{ 'Korollar' on page 33c):}$$

$$s(x - a_i)^{m_i - n_i} = q_1 \cdot (x - a_1)^{m_1}$$

Ist $m_i > n_i$, so ist $m_i - n_i > 0$

$$0 = s(a_i)(a_i - a_i)^{m_i - n_i} = q(a_i)(a_i - a_i) \neq 0E$$

Dass heißt $n_i = m_i, i = 2, \dots, k$

$$q = g(x - a_2)^{m_2} \dots (x - a_k)^{m_k}, g \text{ ohne Nullstelle in } K$$

$$f = g(x - a_1)^{m_2} \dots (x - a_2)^{m_1} \quad (\text{Nach Induktionsvoraussetzung}) \quad \square$$

1.34 Korollar

K Körper, $f, g \in K[x]$, $m = \max(\text{Grad}(f), \text{Grad}(g))$

Gibt es $m + 1$ Elemente $a_1, \dots, a_{m+1} \in K$, paarweise verschieden, mit $f(a_i) = g(a_i)$, $i = 1, \dots, m + 1$ so $f = g$.

Insbesondere: Ist K unendlich, $f, g \in K[x]$ mit $f(a) = g(a)$ für alle $a \in K$, so ist $f = g$

Beweis. $f - g \in K[x]$, $\text{Grad}(f - g) \leq m$.

$f - g$ hat $m + 1$ Nullstellen a_1, \dots, a_{m+1}

$$1.33 \quad f - g = 0, f = g \quad \square$$

1.35 Bemerkung

Über $\mathbb{Q}, \mathbb{R}, \mathbb{Z}_p$ (p Primzahl) gibt es Polynome beliebig hohen Grades ohne Nullstellen

Über \mathbb{Q}, \mathbb{R} : $(x^2 + 1)^m$ hat $\text{Grad}(2m)$, keine Nullstellen in \mathbb{Q}, \mathbb{R}

über \mathbb{Z}_p z.B. $(x^p - x + 1)^m$ hat $\text{Grad } pm$, ohne Nullstellen (ohne Beweis)

1.36 Fundamentalsatz der Algebra

Ist $f \in \mathbb{C}[x]$, $f \neq 0$ so ist $(f = a_n x^n + \dots + a_0)$

$f = a_n(x-c_1)^{m_1} \dots (x-c_k)^{m_k}$, $a_n, c_1, \dots, c_k \in \mathbb{C}$ (Nullstellen mit Vielfachen m_1, m_2)

$m_1 + \dots + m_k = \text{Grad}(f)$

$\text{Grad}(f) = n$ f hat n Nullstellen (einschließend Vielfachheit)

2 Vektorräume

3.11.2015

2.1 Definition

Sei K ein Körper. Ein K -Vektorraum V besitzt Verknüpfung $+$ bezüglich derer eine kommutative Gruppe ist (Neutrales Element 0 , Nullvektor, Inverses zu $v \in V : -v$). Außerdem existiert Abbildung $K \times V \rightarrow V$

$(a, v) \mapsto av, a \in K, v \in V$

(„Multiplikation“ von Elementen aus V , („Vektoren“) mit Körperelementen („Skalare“)), so dass gilt:

$(a + b)v = av + bv$ für alle $a, b \in K, v \in V$

$a(v + w) = av + aw$ für alle $a \in K, v, w \in V$

$(ab)v = a(bv)$ für alle $a, b \in K, v \in V$

$1v = v$ für alle $v \in V$.

2.2 Beispiel

a) K Körper, $n \in \mathbb{N}$

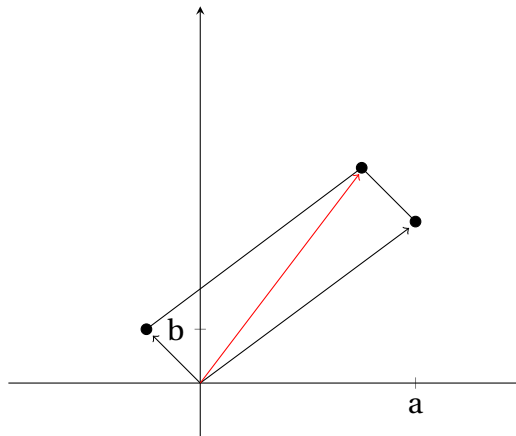
$K^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_i \in K \right\}$ ist K -Vektorraum bezüglich $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}$

$a \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} aa_1 \\ \vdots \\ aa_n \end{pmatrix}$ für alle $a \in K, \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in K^n$. Raum der Spaltenvektoren der Länge n über K .

Entsprechend: Raum der Zeilenvektoren, $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = (a_1, \dots, a_n)^t$

Für $K = \mathbb{R} : \mathbb{R}^n$

$n = 2, 3$ Elemente aus $\mathbb{R}^2, \mathbb{R}^3$, identifizierbar mit Ortsvektor der Ebene oder des 3-dimensionalen Raumes.



b) Sei K ein Körper Polynomring $K[x]$ ist ein K -Vektorraum, bezüglich

- Addition von Polynomen
- Multiplikation von Körperelementen mit Polynomen

$$a \left(\sum_{i=0}^n a_i x^i \right) := \sum_{i=0}^n (a a_i) x^i \in K[x]$$

(Multiplikation von Polynomen mit Polynom Grad ≤ 0)

2.1 folgt aus den Ringeigenschaften von $K[x]$

c) K Körper. $V = \text{Abbildung } (K, K) = \{ \alpha : K \rightarrow K : \alpha \text{ Abbildung} \}$ Addition auf V

$\alpha + \beta \in V (\alpha + \beta)(x) = \alpha(x) + \beta(x)$ für alle $x \in K$

Skalare Multiplikation:

$a \in \mathbb{R}, \alpha \in V (a\alpha)(x) = a \cdot \alpha(x)$ Für alle $x \in K$

Nachrechnen : Damit wird V ein K -Vektorraum

2.3 Proposition

K Körper, $V, K - VR$

a) $a \cdot \sigma = \sigma$

b) $0 \cdot v = \sigma$

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

a,b,c Für alle $v \in V$

2.4 Definition

K Körper, $V, K - VR$.

$\emptyset + U \subseteq V$ heißt *Unterraum* (*Untervektorraum*, oder *Teilraum*) von V , falls U bezüglich Addition auf V und der skalaren Multiplikation mit Elementen aus K selbst K Vektorraum ist.

2.5 Proposition

U ist Unterraum von V

\Leftrightarrow

(1) $u_1 + u_2 \in U$ für alle $u_1, u_2 \in U$

(2) $au \in U$ für alle $u \in U, a \in K$
(Nullvektor in U = Nullvektor in V)

Beweis. $\Rightarrow \checkmark \Leftarrow$: Da $U \neq \emptyset$, existiert $u \in U$.

$\sigma = 0 \cdot u \in U$

$u \in U \Rightarrow -u = (-1)u \in U$

Mit (1): $(U, +)$ ist kommutative Gruppe. Restliche Axiome gelten auch für U, K .

□

2.6 Beispiel

- a) $V - K - VR$, so ist V Unterraum von V .
und $\{0\}$ ist Unterraum von V (*Nullraum*)
- b) Betrachte $K[x]$ als $K - VR$. (2.2).
Sei $n \in \mathbb{N}_0$.
 $U = \{f \in K[x] : \text{Grad}(f) \leq n\}$ Unterraum von $K[x]$

2.7 Proposition

Seien U_1, U_2 Unterräume von K -VR V .

- a) $U_1 \cap U_2$ ist Unterraum
- b) $U_1 + U_2 := \{u_1 + u_2 : u_1 \in U_1, u_2 \in U_2\}$ ist Unterraum von V (*Summe* von Unterräumen)
- c) $U_1 + U_2$ ist der kleinste Unterraum von V , der $U_1 \cup U_2$ enthält.
- d) $U_1 \cap U_2$ ist im Allgemeinen kein Unterraum.
Beweis: 0.4

2.8 Definition

V K -VR

- a) $v_1, \dots, v_m \in V, a_1, \dots, a_m \in K$

Dann heißt

$$a_1 v_1 + \dots + a_m v_m = \sum_{i=1}^m a_i v_i \in V$$

Linearkombination von v_1, \dots, v_m (mit Koeffizienten a_1, \dots, a_m).

[Beachte: Zwei formell verschiedene Linearkombinationen derselben Vektoren können den gleichen Vektor darstellen z.B. in \mathbb{R}^2 :

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

- b) Ist $M \subseteq V$, so ist der von M erzeugte oder aufgespannte Unterraum $\langle M \rangle_K$ (oder kurz $\langle M \rangle$) die Menge aller endlichen Linearkombination, die man mit Vektoren aus M bilden kann:

$$\langle M \rangle = \left\{ \sum_{i=1}^n a_i v_i : n \in \mathbb{N}, a_i \in K, v_i \in M \right\}$$

$$\langle \emptyset \rangle_K := \{\emptyset\}$$

$$M = \{v_1, \dots, v_m\} : \langle M \rangle = \langle v_1, \dots, v_m \rangle$$

- c) Ist $\langle M \rangle_K = V$, so heißt M Erzeugungssystem

2.9 Satz

V K -VR, $M \subseteq V$

- a) $\langle M \rangle_K$ ist Unterraum von V
- b) $\langle M \rangle_K$ ist der kleinste Unterraum von V , der M enthält.
Insbesondere: Sind U_1, U_2 Unterräume von V , so ist $\langle U_1 \cup U_2 \rangle_K = U_1 + U_2$
Beweis: 0.7

2.10 Definition

V K -VR V heißt endlich erzeugt, falls es eine endliche Teilmenge $M \subseteq V$ gibt mit $V = \langle M \rangle_K$

2.11 Beispiel

- a) $K^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_i \in K \right\}$
 K^n ist endlich erzeugt.

$$e_1, \dots, e_n \text{ Einheitsvektor } e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i$$

$$K^n = \langle e_1, \dots, e_n \rangle_K, \text{ denn } \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1 e_1 + \dots + a_n e_n$$

- b) $K[x]$ als K -Vr ist nicht endlich erzeugt. Angenommen es existiert $f_1, \dots, f_n \in K[x]$ mit $K[x] = \langle f_1, \dots, f_n \rangle_K$.

Sei $t, \max \text{Grad}(f_i) \in \mathbb{N}_0 \cup \{-\infty\}$

Dann haben alle Polynome in $\langle f_1, \dots, f_n \rangle_K$ höchstens Grad t . Also $x^{t+1} \in K[x] \setminus \langle f_1, \dots, f_n \rangle_K$

$M = \{1, x, x^2, x^3, \dots\} = \{x^i : i \in \mathbb{N}_0\}$

$$K[x] = \langle M \rangle_K. \quad f = \sum_{n=0}^t a_i x^i$$

- c) $n \in \mathbb{N}. \quad U = \{f \in K[x] : \text{Grad}(f) = n\}$

Unterraum von $K[x]$, endlich erzeugt

2.12 Definition

Sei V K -VR, $v_1, \dots, v_m \in V$ heißen *linear abhängig*, wenn es $a_1, \dots, a_n \in K$, *nicht alle* $= 0$, gibt mit

$$a_1 v_1 + \dots + a_m v_m = \sigma$$

(Beachte: Immer mit $0 \cdot v_1 + \dots + 0 \cdot v_m = \sigma$, aber bei linearer Abhängigkeit soll es noch eine andere Möglichkeit geben) Andernfalls nennt man v_1, \dots, v_m *linear unabhängig*:

(D.h. aus $a_1 v_1 + \dots + a_m v_m = \sigma$ folgt $a_1 = \dots = a_m = 0$)

Entsprechend: $\{v_1, \dots, v_m\}$ linear abhängig, linear unabhängig.

\emptyset per Definition linear unabhängig. Klar: Teilmenge von linear unabhängigen Vektoren wieder linear unabhängig

2.13 Beispiel

- a) σ ist linear abhängig: $1 \cdot \sigma = \sigma$

- b) $v, w \in V, v \neq \sigma \neq w$.

Wann sind v und w linear abhängig?

v, w linear abhängig $\Rightarrow \exists a, b \in K$, nicht beide $= 0$ mit $a \cdot v + b \cdot w = \sigma$

Angenommen: $a \neq 0$ $a \cdot v = -b \cdot w \mid a^{-1}$ (K Körper)

$$v = 1 \cdot v = (a^{-1}a)v = a^{-1}(av) = a^{-1}(-bw) = (-a^{-1}b)w \in \langle w \rangle_K = \{cw : c \in K\}$$

$$d \in K$$

$$dv = (-da^{-1}b)w \in \langle w \rangle_K$$

$$\langle v \rangle_K \subseteq \langle w \rangle_K$$

Dann auch $b \neq 0$.

Angenommen $b = 0$, $a \cdot v = -0w = \sigma$

$$v = a^{-1}\sigma = \sigma E \text{ Vertausche Rollen von } v, w : \langle w \rangle_K \subseteq \langle v \rangle_K$$

$$v \in \langle w \rangle_K$$

$$v, w \text{ linear abhängig} \Leftrightarrow \langle v \rangle_K = \langle w \rangle_K$$

Beweis. $\Rightarrow \checkmark$

$$\Leftarrow v \in \langle v \rangle_K = \langle w \rangle_K$$

$$\Rightarrow v = c \cdot w \text{ für ein } c \in K.$$

$$\Rightarrow \sigma = -v + c \cdot w = (-1)v + c \cdot w$$

$$\Rightarrow v, w \text{ linear abhängig.} \quad \square$$

c) $e_1, \dots, e_n \in K^n$ sind linear unabhängig.

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = a_1 e_1 + \dots + a_n e_n = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

$$\Rightarrow a_1 = \dots = a_n = 0.$$

d) $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} \in \mathbb{R}^3$ linear abhängig, linear unabhängig? Für welche $a, b, c \in \mathbb{R}$

$$\text{gilt } a \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + b \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} + c \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}?$$

Führt auf LGS für die unbekannten a, b, c

$$1a \quad 3b \quad 2c = 0$$

$$2a \quad 2b \quad 3c = 0$$

$$3a \quad 1b \quad 4c = 0$$

Gauß:

$$\begin{pmatrix} 1 & 3 & 2 & 0 \\ 2 & 2 & 3 & 0 \\ 3 & 1 & 4 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & -4 & -1 & 0 \\ 0 & -8 & -2 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 1 & 0.25 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$c \text{ frei wählbar, } b = -\frac{1}{4}c \quad a = -3b - 2c = -\frac{3}{4}c - 2c = -\frac{5}{4}c$$

$$\text{z.B. } c = 4, b = -1, a = -5$$

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

Vektoren sind linear abhängig.

2.14 Bemerkung

Man kann auch für unendliche Mengen $M \subseteq V$ lineare Unabhängigkeit definieren.

Jede endliche Teilmenge von M ist linear unabhängig. Zum Beispiel $\{x^i : i \in \mathbb{N}_0\}$ linear unabhängig in $K[x]$.

2.15 Satz !!!

V K -VR, v_1, \dots, v_m sind linear abhängig

$$1. \Leftrightarrow \exists i : v_i = \sum_{\substack{j=1 \\ j \neq i}}^m b_j v_j \text{ für geeignete } b_j \in K$$

$$\Leftrightarrow \exists i : \langle v_1, \dots, v_m \rangle_K = \langle v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m \rangle_K$$

$$2. v_1, \dots, v_m \text{ linear unabhängig}$$

$$\Leftrightarrow \text{jedes } v \in \langle v_1, \dots, v_m \rangle \text{ lässt sich als } v_1, \dots, v_m \text{ schreiben.}$$

$$3. \text{ Sind } v_1, \dots, v_m \text{ linear unabhängig und ist } v \notin \langle v_1, \dots, v_m \rangle_K, \text{ so sind } v_1, v_m, v \text{ linear unabhängig.}$$

Beweis. Wie in 0.11, aber $v_1, \dots, v_m \in V$

□

2.16 Definition

Sei V endliche erzeugter K -VR.

Eine endliche Teilmenge $B \subseteq V$ heit *Basis* von V , falls

(1) $V\langle B \rangle_K$

(2) B linear unabhängig

($V = \{\sigma\} : \emptyset$ ist Basis von V)

2.17 Beispiel

a) e_1, \dots, e_n Basis K^n (*kanonische Basis*)

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1 e_1 + \dots + a_n e_n$$

b) $\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \end{pmatrix}, K = \mathbb{Z}_5 :$

$$3 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = 3 \begin{pmatrix} 1 \\ 2 \end{pmatrix} - \begin{pmatrix} 3 \\ 1 \end{pmatrix} = 3 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + 4 \begin{pmatrix} 3 \\ 1 \end{pmatrix} \text{ bilden Basis von } \mathbb{Z}_7^2$$

Lineare Unabhängigkeit:

$$a \begin{pmatrix} 1 \\ 2 \end{pmatrix} + b \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Führt auf LGS für a,b:

$$1 \cdot a + 3 \cdot b = 0$$

$$2 \cdot a + 1 \cdot b = 0$$

Gauß-Algorithmus (funktioniert über jedem Körper K)

$$\begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & 0 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow{II \cdot 4} \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$b = 0, a + 3b = 0, a = 0$$

$$\left\langle \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix} \right\rangle_{\mathbb{Z}_7} = \mathbb{Z}_7^2$$

$$\text{Sei } \begin{pmatrix} c \\ d \end{pmatrix} \in \mathbb{Z}_7^2$$

Gesucht sind $a, b \in \mathbb{Z}_7$

Gauß:

$$1 \cdot a + 3 \cdot b = c$$

$$2 \cdot a + 1 \cdot b = d$$

$$\begin{pmatrix} 1 & 3 & c \\ 2 & 1 & d \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 & c \\ 0 & 2 & d-2c \end{pmatrix} \xrightarrow{II \cdot 4} \begin{pmatrix} 1 & 3 & c \\ 0 & 2 & 4d-2c \end{pmatrix}$$

$$b = 4d - c = 4d + 6c$$

$$a = c - 3b = 4c + 2d$$

$$\begin{pmatrix} c \\ d \end{pmatrix} = (4c + 2d) \begin{pmatrix} 1 \\ 2 \end{pmatrix} + (4d + 6c) \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

2.18 Satz (Existenz von Basen)

Sei V endliches Erzeugter K -VR. Dann enthält jedes endliche Erzeugendensystem von V eine Basis von V .

Beweis. Sei $M \subseteq V$ endlich mit $V = \langle M \rangle_K$. Ist M linear unabhängig, so ist M Basis ✓

ist M linear abhängig, so existiert nach 2.15a)

$v \in M$ mit $V = \langle M \rangle_K = \langle M \setminus \{v\} \rangle_K$

Da M endlich, endet dieses Verfahren mit Basis □

2.19 Lemma

V endlich erzeugter K -VR

$B = \{v_1, \dots, v_n\}$ Basis von V . Sei $\sigma \neq w \in V$.

Dann $w = \sum_{j=1}^n a_j v_j, a_j \in K$.

Ist $a_i \neq 0$, so ist $(B \setminus \{v_i\}) \cup \{w\}$ wieder eine Basis von V

$$\text{Beweis. } w = \sum_{j=1}^n a_j v_j \Rightarrow a_i v_i = w - \sum_{\substack{j=1 \\ j \neq i}}^n a_j v_j$$

$$\Rightarrow v_i = a_i^{-1}(a_i v_i) = a_i^{-1} w + \sum_{\substack{j=1 \\ j \neq i}}^n (a_i^{-1} a_j) v_j$$

$$v_i \in \langle (B \setminus \{v_i\}) \cup \{w\} \rangle_K$$

$$V = \langle B \rangle_K = \langle B \cup \{w\} \rangle_K \stackrel{2.15}{=} \langle B \setminus \{v_i\} \cup \{w\} \rangle_K$$

Zeige $(B \setminus \{v_i\}) \cup \{w\}$ ist linear unabhängig:

$$\text{Angenommen } \sigma = \sum_{\substack{j=1 \\ j \neq i}}^6 c_j v_j + c w = \sum_{\substack{j=1 \\ j \neq i}}^6 c_i v_j + \sum_{\substack{j=1 \\ j \neq i}}^6 c a_j v_j = \sum_{\substack{j=1 \\ j \neq i}}^6 (c_j + c a_j) v_j + c a_i v_i$$

v_1, \dots, v_n linear unabhängig

$\Rightarrow (1) ca_i = 0$ und

(2) $c_j + ca_j = 0$ für alle $j \neq i$

(1) $ca_i = 0, a_i \neq 0 \Rightarrow c = 0$

(2) $c_j = 0$ für alle $j \neq i$.

Fertig. □

2.20 Satz (Austauschsatz von Steinitz)

(Ernst Steinitz, 1871-1928, Kiel)

V endlich erzeugter K -VR, B Basis von V , M endliche linear unabhängige Teilmenge von V . Dann existiert $C \subseteq B$ mit $|C| = |M|$, so dass $(B \setminus C) \cup M$ Basis von V ist.

Insbesondere $|M| \leq |B|$.

Beweis. Sei $|M| = k$

Induktionsnach k .

$k = 0$ ✓

$k > 0$. Sei $M = \tilde{M} \cup \{w\}$, $|\tilde{M}| = k - 1$

Induktionsvoraussetzung: Existiert $\tilde{C} \subseteq B$ mit $|\tilde{C}| = |\tilde{M}|$ und $(B \setminus \tilde{C}) \cup \tilde{M}$ ist Basis von V

$$w = \sum_{u \in B \setminus \tilde{C}} a_u u + \sum_{v \in \tilde{M}} a_v v$$

Mindestens eines der a_u ist $\neq 0$, denn sonst $w = \sum_{v \in \tilde{M}} a_v v$, also $M = \tilde{M} \cup \{w\}$

linear abhängig E

Also sei $a_i \neq 0$ für ein $u \in B \setminus \tilde{C}$.

Nach 2.19 ist $(B \setminus C) \cup M$ Basis von V wobei $c = \tilde{C} \cup \{w\}$.

Fertig. □

2.21 Korollar

V endlich erzeugte K -VR

a) Je zwei Basen von V enthalten gleich viele Vektoren

b) Jede linear unabhängige Teilmenge von V ist endlich

c) (Basisergänzungssatz)

Jede linear unabhängige Menge von Vektoren lässt sich zu Basis ergänzen.

Beweis. a) B, \tilde{B} Basen von V .

$$2.20: |B| \leq |\tilde{B}|$$

$$: |\tilde{B}| \leq |B|$$

$$\text{Also } |B| = |\tilde{B}|.$$

b) Angenommen V enthält unendlich linear abhängige Teilmenge M , Sei B Basis von V . Wähle $M_0 \subset M$ mit M_0 endlich, $|M_0| > |B|$.

Nach Voraussetzung ist M_0 linear abhängig Widerspruch zu 2.20

c) Sei M linear unabhängige Teilmenge von V . Nach b) ist M endlich.

Sei B eine Basis von V 2.20: $\exists c \subseteq B, |c| = |M|$ so dass $\underbrace{(B \setminus c)}_{\text{Basisergänzung}} \cup M$ Basis. \square

Basisergänzung

2.22 Satz

V endlich erzeugter K -VR,

$B \subseteq V$. Dann sind äquivalent:

(1) B ist Basis von V

(2) B ist maximal unabhängige Teilmenge von V

(3) B ist minimales Erzeugendensystem von V (d.h. $\langle B \setminus \{w\} \rangle_K \neq V$ für alle $w \in B$.)

Beweis. (2) \Rightarrow (1)

Angenommen $\langle B \rangle_K \neq V$

Sei $v \in V \setminus \langle B \rangle_K$.

2.15c): $B \cup \{v\}$ linear abhängig \nexists . $\langle B \rangle_K = V$ B ist Basis

(1) \Rightarrow (2): Angenommen $B \subseteq C$, C linear unabhängig.

2.21 c ist endlich.

2.20 $|c| \leq |B|$ Daher $B = c$.

(3) \Rightarrow (1). Angenommen B ist linear abhängig

2.15a): $\exists w \in B : V = \langle B \rangle_K = \langle B \setminus \{w\} \rangle_K \not\Rightarrow$

B ist linear unabhängig also Basis.

(1) \Rightarrow (3). Angenommen $\exists w \in B$ mit $\langle B \setminus \{w\} \rangle_K = V_i = \langle B \rangle_K$

2.15a): B ist linear abhängig $\not\Rightarrow$

□

2.23 Definition

V K -VR.

a) Ist V endlich erzeugt, B ist Basis von V , $|B| = n$, so hat V Dimension n ,
 $\dim_K(V) = n$ (oder einfach $\dim(V) = n$)

b) (V heißt nicht endlich erzeugt, so heißt V *unendlich-dimensional*)
 (Also endlich erzeugt = endlich-dimensional)

2.24 Korollar

V K -VR, $\dim_K(V) = n$, $B \subseteq V, |B| = n$

a) Ist B linear unabhängig, dann ist B Basis.

b) Ist $\langle B \rangle_K = V$, dann ist B Basis

Beweis: Folgt aus 2.22

2.25 Beispiel

a) $\dim_K(K^n) = n$, da e_1, \dots, e_n Basis.

b) $V = \mathbb{R}^4$

$$U = \left\langle \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} \right\rangle$$

$\begin{matrix} = u_1 & = u_2 \end{matrix} \quad \mathbb{R}$

u_1, u_2 sind linear unabhängig.

$$a \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} + b \begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \text{ nur für } a, b = 0$$

$\{u_1, u_2\}$ Basis von U $\dim_{\mathbb{R}}(U) = 2$.

Ergänze u_1, u_2 zu Basis von $V = \mathbb{R}^4$:

Erste Möglichkeit:

e_1, e_2, e_3, e_4 kanonische Basis des \mathbb{R}^4

$$U_1 = 1e_1 + 2e_2 + 0e_3 + 1e_4$$

2.19: U_1, e_3, e_4 Basis von \mathbb{R}^4

$$U_2 = au_1 + be_2 + ce_3 + de_4 =$$

$$\begin{pmatrix} 0 \\ 2 \\ 1 \\ 0 \end{pmatrix} = a \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ b \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ c \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ d \end{pmatrix} \quad c = 1$$

2.19: u_1, u_2, e_3, e_4 Basis von \mathbb{R}^4

Zweite Möglichkeit:

2.15c):

v_1, \dots, v_m linear unabhängig

$$v \notin \langle v_1, \dots, v_m \rangle \Rightarrow v_1, \dots, v_m \text{ linear unabhängig. } U = \left\{ \begin{pmatrix} a \\ 2a+2b \\ b \\ a \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

$e_1 \notin U$ (1. Koordinate \neq 4. Koordinate)

2.15c) U_1, U_2, e_1 linear unabhängig.

$\langle u_1, u_2, e_1 \rangle = ?$

$$U_1 := \left\{ \begin{pmatrix} a+c \\ 2a+2b \\ b \\ a \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

$e_2 \notin U$

2.15c): u_1, U_2, e_1, e_2 linear unabhängig

2.24: $\{u_1, u_2, e_1, e_2\}$ Basis von \mathbb{R}^4

2.26 Satz

V K -VR, $\dim_K(V) = n$.

a) Ist U Unterraum von V , so ist $\dim_K(U) \leq n$. Ist $\dim_K(U) = n$, so ist $U = V$.

b) (Dimensionenformel)

U, W Unterräume von V , so gilt:

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

A, B endliche
Mengen

$$(|A \cup B| = |A| + |B| - |A \cap B|)$$

Beweis. a) Ergänze Basis von U zu Basis von V . (2.21c)

b) Basis von $U \cup W \rightarrow$ Basis von U

\rightarrow Basis von w (WHK 9.23)

□

2.27 Definition

V K -VR, $\dim_K(V) = n$, $B = (v_1, \dots, v_n)$ geordnete von V .

Jedes $v \in V$ hat *eindeutige* Darstellung $v = \sum_{i=1}^n a_i v_i \quad a_i \in K \quad 2.15b)$

(a_1, a_n) (in dieser Anordnung) heißen *Koordinaten* von V bezüglich B) Insbesondere v_i hat Koordinaten $(0, \dots, 0, 1, 0, \dots, 0)$

2.28 Beispiel

a) $V = K^n, (e_1, \dots, e_n) = B$ kanonische Basis.

Koordinaten von $v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ bezüglich $B: (a_1, \dots, a_n)$

Kartesische Koordinaten

(R. Decartes, 1596-1650)

b) $V = \mathbb{Q}^3, B = \left(\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right)$

B ist geordnete Basis von V . (nachprüfen)

Koordinaten von $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ bezüglich B :

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + a_2 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$$

Gauß Algorithmus:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & -2 & 1 & -2 \\ 0 & 1 & 2 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & -0.5 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & -0.5 & 1 \\ 0 & 0 & 2.5 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & -0.5 & 1 \\ 0 & 0 & 1 & -0.4 \end{pmatrix}$$

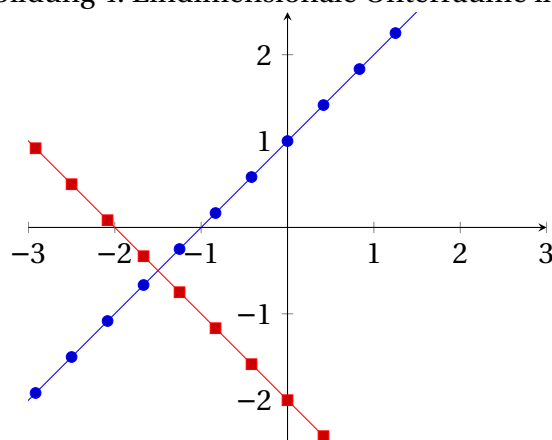
$$a_3 = -0,4$$

$$a_2 = 0.8$$

$$a_1 = 0.2$$

Koordinaten von $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ bezüglich $B \left(\frac{1}{5}, \frac{4}{5}, -\frac{2}{5} \right)$

Abbildung 4: Eindimensionale Unterräume im \mathbb{R}^2



2.29 Definition

V K -VR, U Unterraum von V , $w \in V$. Dann heißt $w + U := \{w + u : u \in U\}$ *affiner Unterraum* von v .

($w +$ ist im allgemeinen kein Untervektorraum)

$$\dim(w + u) := \dim(U)$$

2.30 Satz

V K -VR, U, W Unterräume von V ,

- a) $w + U$ ist Unterraum ①
 $\Leftrightarrow W \in U$ ②
 $\Leftrightarrow w + U = U$ ③
- b) Ist $v \in w + U$, so ist $v + U = w + U$
- c) Sind $v_1 + U, v_2 + W$ affine Unterräume, so ist entweder $(v_1 + U) \cap (v_2 + W) = \emptyset$ oder es existiert $v \in V$ mit $(v_1 + U) \cup (v_2 + W) = v + (U \cup W)$ affiner Unterraum.

Beweis. ③ \Rightarrow ① \checkmark

a) ① \Rightarrow ②

$$w + U \text{ Unterraum} \Rightarrow \sigma \in w + U$$

$$\Rightarrow \exists u \in U \text{ mit } w + u = \sigma$$

$$\Rightarrow w = -u \in U$$

② \Rightarrow ③: $w \in U, w + U \subseteq U$ (da U Unterraum)

$$\text{Sei } u \in U. \text{ Dann } u - w \in U \quad u = w + (u - w) \in w + U$$

b) $v \in w + U, v = w + u$ für ein $u \in U$

$$v + U = w + \underbrace{u + U}_{=U \text{ nach a)}} = w + U$$

c) Angenommen $(v_1 + U) \cup (v_2 + W) \neq \emptyset$

$$\text{Sei } v \in (v_1 + U) \cup (v_2 + W)$$

Nach b) $v + U = v_1 + U$

$$v + W = v_2 + W$$

$$\begin{aligned}(v_1 + U) \cup (v_2 + W) &= (v + U) \cup (v + W) \\ &= v + (U \cap W)\end{aligned}$$

$\supseteq \checkmark$

$\subset x \in (v + U) \cup (v + W), x = v + u = v + w, u \in U, w \in W$
 $u - w \in U \cap W.$

$$x = v + u = v + (U \cap W)$$

□

2.31 Bemerkung

affine Unterräume:

spezielle Rolle von σ ist aufgehoben. Zur Beschreibung eines $x \in K^n$ kann man jeden Punkt p als „Nullpunkt“ wählen und dann die Koordinaten von x bezüglich einer nach p „verschobenen“ Basis berechnen. p hat Koordinaten (p_1, \dots, p_n) bezüglich Basis v_1, \dots, v_n

Ursprüngliche Koordinatensystem I : σ, v_1, \dots, v_n

Neues Koordinatensystem II: $:p, v_1 + p, \dots, v_n + p$

x hat Koordinaten (a_1, \dots, a_n) bezüglich I

\Rightarrow Koordinaten von x bezüglich II = $(a_1 - p_1, \dots, a_n - p_n)$
 $=$ Koordinaten von $x - p$ bezüglich I

x hat Koordinaten (a'_1, \dots, a'_n) bezüglich II

$\Rightarrow x$ hat Koordinaten $(a'_1 + p_1, \dots, a'_n + p_n)$ bezüglich I. (Robotik)

2.32 Bemerkung

a) In Mathe II:

$x \times m$ über $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Das geht auch bei den Körpern K .

Addition, Multiplikation mit Skalaren, Matrixmultiplikation werden analog definiert.

Es gelten die gleichen Rechenregeln wie in (Mathe II, 9.5 www.ffgti.org)

b) In Mathe II, wurden Matrizen verwendet zur Beschreibung von LGS $\begin{matrix} A \\ m \times n \end{matrix} x =$

$$\begin{matrix} b \\ n \times 1 \end{matrix} x =$$

Analog: LGS über beliebigen Körpern K . GaußAlgorithmus funktioniert analog.

$$(a_1, \dots, a_n), a_1 \neq 0 \\ \rightarrow (1, a_1^{-1}, a_2, \dots)$$

(K Körper!)

2.33 Satza) Die Menge der Lösungen eines *homogenen* LGS.

$$A \cdot x = 0$$

$$(A \in \mathcal{M}_{n,m}(K), x \in K^m \\ 0 \text{ ist Nullvektor in } K^n)$$

b) Ist das *inhomogene* LGS

$$A \cdot x = b$$

lösbar und ist $x_0 \in K^n$ eine spezielle Lösung (d.h. $A \cdot x_0 = b$), so erhält man alle Lösungen von $A \cdot x = b$ durch $\{x_0 + y : Ay = 0\}$, y = Zugehöriges homogenes LGS.

Ist U der Lösungsraum von $Ax = 0$, so ist die Lösungsmenge von $Ax = B$ gerade der affine Unterraum $x_0 + U$ von K^n

Beweis. a) Folgt aus Rechenregeln für Matrizen: $x_1, x_2 \in K^m$ Lösungen von $A \cdot x = 0$.

$$A(x_1 + x_2) = Ax_1 + Ax_2 = 0 + 0 = 0$$

 $x_1 + x_2$ Lösung. $a \in K$.

$$A(a \cdot x_1) = a \cdot (Ax_1) = a \cdot 0 = 0$$

 $a \cdot x_1$ Lösung.Null-Lösung existiert. b) $Ax_0 = b$. Sei $y \in K^m$ mit $Ay = 0$.

$$A \cdot (x_0 + y) = Ax_0 + Ay = b + 0 = b$$

 $x_0 + y$ ist Lösung von $Ax = b$ Zeige: Jede Lösung von $Ax = b$ ist von der Form $x_0 + y$ für ein y mit $Ay = 0$.Sei x Lösung von $Ax = b$.

$$x = x_0 + (x - x_0)$$

$$A(x - x_0) = Ax - Ax_0 = b - b = 0$$

□

2.34 Beispiel

gegebenes LGS:

$$\begin{array}{rrrrr} x_1 & +x_2 & +x_3 & -x_4 & = 0 \\ x_1 & -2x_2 & & x_4 & = 1 \end{array}$$

Über \mathbb{Q} :

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 0 \\ 1 & -2 & & 1 & \end{pmatrix}$$

Gauß:

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 0 \\ 1 & -2 & & 1 & \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & -1 & 0 \\ 0 & -3 & -1 & 2 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & -1 & 0 \\ 0 & 1 & \frac{1}{3} & -\frac{2}{3} & -\frac{1}{3} \end{pmatrix}$$

x_3, x_4 Frei wählbar.

Zugehöriges homogenes System:

$$\begin{pmatrix} 1 & 1 & 1 & -1 & 0 \\ 1 & -2 & & 1 & \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & -1 & 0 \\ 0 & 1 & \frac{1}{3} & -\frac{2}{3} & -\frac{1}{3} \end{pmatrix}$$

Lösungsmenge = Unterraum.

Basis des Lösungsraum:

Setze die frei wählbaren x_4, x_3 .

- $x_4 = 1, x_3 = 0 \rightsquigarrow$ Lösung $\begin{pmatrix} * \\ * \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} ** \\ ** \\ 1 \\ 0 \end{pmatrix}$
- $x_4 = 0, x_3 = 1 \rightsquigarrow$ Lösung

Jede Lösung $d \cdot \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ 0 \\ c \end{pmatrix} + \begin{pmatrix} -\frac{2}{3} \\ -\frac{1}{3} \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} * \\ * \\ c \\ d \end{pmatrix}$

Lösungsraum vom zugehörigen homogenen LGS:

$$\left\langle \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -\frac{2}{3} \\ -\frac{1}{3} \\ 1 \\ 0 \end{pmatrix} \right\rangle$$

3 Lineare Abbildungen

3.1 Definition

V, W, K -VR

a) $\alpha : V \longrightarrow$ heißt (K -) *lineare Abbildung* (oder *Vektorraum-Homomorphismus*)

falls:

$$\text{Additivitat} \quad \leftarrow (1) \quad \alpha(u + v) = \alpha(u) + \alpha(v) \text{ fur alle } u, v \in V$$

$$\text{Homogenitat} \quad \leftarrow (2) \quad \alpha(kv) = k\alpha(v) \text{ fur alle } k \in K, v \in V$$

3.2 Bemerkung

$\alpha : V \rightarrow W$ lineare Abbildung.

a) $\alpha(\sigma) = \sigma$

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

Beweis. a) $\alpha(\sigma) = \alpha(\sigma + \sigma) = \alpha(\sigma)$

b) Definition + Induktion nach n . □

3.3 Beispiel

a) Nullabbildung $\alpha : V \rightarrow W$

$$\alpha(v) = 0 \text{ fur alle } v \in V$$

b) $c \in K$

$$\alpha : V \rightarrow V, \alpha(v) = c \cdot v \text{ lineare Abbildung } c = 1 : \text{ id}_V$$

c) $\zeta : \begin{cases} \mathbb{R}^3 & \longrightarrow \mathbb{R}^3 \\ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} & \mapsto \begin{pmatrix} 3 \\ x_1 \\ x_2 \end{pmatrix} - x_3 \end{cases}$

Spiegelung an der $\{x_1, x_2\}$ -Ebene in \mathbb{R}^3

$$\text{d) } \alpha = \begin{cases} \mathbb{R}^2 & \rightarrow \mathbb{R}^n \\ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} & \rightarrow x_1^2 \end{cases}$$

nicht linear

Index

- Abbildung, 21
- abelsch, 23
- affine Unterräume, 56
- affiner Unterraum, 55
- Assoziativgesetz, 22
- aufgespannte Unterraum, 43

- Basis, 46
- Basisergänzungssatz, 50

- Dimension, 51
- Dimensionenformel, 53
- Distributivgesetz, 29
- Division mit Rest, 35

- Einheitsvektor, 43
- Einselement, 29
- endlich erzeugt, 43
- Erweiterter Euklidischer
 Algorithmus, 26
- Erzeugungssystem, 43
- Euler'sche φ -Funktion, 26

- geordnete Basis, 53
- Grad, 33
- Gruppe, 22

- Halbgruppe, 22
- homogenen, 57
- Horner-Schema, 35

- inhomogene, 57
- Inverse, 22

- inverses Element, 22
- invertierbar, 22

- K-Vektorraum, 39
- kanonische Basis, 47
- Kartesische Koordinaten, 53
- Koeffizienten, 31
- kommutativer Ring, 29
- Kommutativgesetz, 23
- Komponente, 5
- Konkatenation, 22
- Konstante Polynome, 33
- Koordinaten, 53
- Körper, 31

- linear abhängig, 44
- linear unabhängig, 44
- Linearkombination, 10, 42

- Matrizenaddition, 22, 29
- Matrizenmultiplikation, 5, 22, 29
- Monoid, 22
- Monome, 33

- neutrales Element, 22
- Nullelement, 29
- Nullpolynom, 31
- Nullpunkt, 56
- Nullraum, 7, 42
- Nullteilerfreiheit, 31, 34
- Nullvektor, 39

- Ortsvektoren, 5

Parallelogrammregel, 5
Permutationen, 27
Polynom, 31
Polynomring, 32

Ring, 29
Ring mit Eins, 29

Spaltenvektoren, 5, 39
systematische Gruppe, 27

Teilraum, 41

unendlich-dimensional, 51
Unterraum, 7, 41
Untervektorraum, 41

Vektor, 6
Vektorraum, 5
Verknüpfung, 21
Verknüpfungssymbole, 21

Zahlengerade, 5