

# **Mathematik für Informatiker II**

## **2009**

Tony Lemke

21. Juni 2009



# Inhaltsverzeichnis

<b>I Grundstrukturen der linearen Algebra</b>	<b>5</b>
<b>IV.1 Gruppen, Ringe, Körper</b>	<b>6</b>
Definition Verknüpfung . . . . .	6
Beispiel . . . . .	6
Definition Gruppe . . . . .	6
Beispiel . . . . .	7
Bemerkung . . . . .	7
Definition Untergruppe . . . . .	7
Bemerkung . . . . .	7
Definition . . . . .	7
Beispiel 4.1.1 . . . . .	8
Satz 4.1.2 . . . . .	8
Definition Ring . . . . .	9
Definition Körper . . . . .	10
Beispiel 4.1.3 . . . . .	11
Beispiel 4.1.4 . . . . .	11
Satz 4.1.5 Division mit Rest . . . . .	12
Beispiel . . . . .	13
Beispiel . . . . .	13
Lemma 4.1.6 . . . . .	13
Definition . . . . .	14
Fundamentalsatz der Algebra [Gauss 1799] . . . . .	14
Korollar 4.1.7 . . . . .	14
Lemma 4.1.7 . . . . .	14
Beispiel . . . . .	14
Korollar 4.1.9 . . . . .	14
<b>IV.2 Vektorräume</b>	<b>16</b>
Definition 4.2.1 . . . . .	16
Rechenregeln 4.2.2 in $K$ -Vektorraum $V$ . . . . .	16
Beispiel 4.2.3 . . . . .	17
Definition 4.2.4 . . . . .	18
Beispiel 4.2.5 . . . . .	18
Definition 4.2.6 . . . . .	19

Beispiel . . . . .	20
Definition 4.2.7 . . . . .	20
Beispiel 4.2.8 . . . . .	21
Definition 4.2.9 . . . . .	22
Beispiel . . . . .	22
Satz . . . . .	22
Basisauswahlsatz . . . . .	23
Beispiel . . . . .	23
Satz 4.2.11 . . . . .	23
<b>IV.3 Multiplikation von Matrizen und Vektoren</b>	<b>25</b>
Definition . . . . .	25
Beispiel . . . . .	25
Zahlenbeispiele . . . . .	26
Satz 4.3.1 . . . . .	27
Definition . . . . .	28
Definition . . . . .	28
Definition . . . . .	29
Satz 4.3.2 . . . . .	29
Anmerkung . . . . .	30

**Teil I**

**Grundstrukturen der linearen  
Algebra**

# IV.1 Gruppen, Ringe, Körper

## Definition Verknüpfung

Sei  $G$  Menge. **Verknüpfung** auf  $G$ :

Vorschrift, die zwei Elementen  $a, b \in G$  ein neues Element  $a * b \in G$  zuordnet, d.h. Abbildung

$$\begin{aligned} * : G \times G &\rightarrow G \\ (a, b) &\mapsto a * b \end{aligned}$$

## Beispiel

- a)  $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R}_+$  ( $:= \{x \in \mathbb{R} : x \geq 0\}$ ) mit Addition oder Multiplikation als Verknüpfung, d.h. man kann für  $a, b \in G$

$$a * b := a \cdot b \text{ oder } a * b := a + b$$

definieren (Reihenfolge egal)

- b)  $X$  Menge,  $G := \text{Abb}(X, X) := \{f : X \rightarrow X, f \text{ Abbildung}\}$   
Definiere für  $f, g \in G$ :

$$f * g = f \circ g \in G \quad \text{Reihenfolge **nicht** egal}$$

## Definition Gruppe

Menge  $G$  mit Verknüpfung  $*$  heißt **Gruppe**, falls die folgenden (Gruppen-)Axiome erfüllt sind:

(G1)  $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$  (Assoziativgesetz)

(G2) Es gibt ein  $e \in G$  (neutrales Element), sodass

a)  $e * a = a \quad \forall a \in G$

b)  $\forall a \in G : a' * a = e$

Die Gruppe heißt abelsche (oder kommutativ), falls **zusätzlich**

$$a * b = b * a \quad \forall a, b \in G$$

**Häufig abkürzend:**  $a \cdot b$  oder  $ab$  anstelle  $a*b$

## Beispiel

$\mathbb{Z}, \mathbb{Q}$  und  $\mathbb{R}$  mit  $+$  sind Gruppen.  $\mathbb{R}_+ \setminus \{0\}$  mit  $\cdot$  ist Gruppe, aber  $\mathbb{Z}$  mit  $\cdot$  zum Beispiel **nicht** (denn in  $\mathbb{Z}$  ist 1 neutrales Element bezüglich  $\cdot$ , aber für  $a \in \mathbb{Z}$  ist  $\frac{1}{a} \notin \mathbb{Z}$ ).

$\mathbb{N}_0$  mit  $+$  ist auch keine Gruppe (denn neutrales Element ist 0, aber für  $a \in \mathbb{N}$  ist  $-a \in \mathbb{N}$  mit  $a + (-a) = 0$ ).

## Bemerkung

Für eine Gruppe mit  $*$  ist neutrales Element  $e \in G$  **eindeutig** bestimmt und es gilt auch  $a * e = a \forall a \in G$ .

Auch das inverse Element ist eindeutig bestimmt: Wir bezeichnen diese für  $a \in G$  mit  $a^{-1}$  und es gilt  $a * a^{-1} = a^{-1} * a = e$

## Definition Untergruppe

$G' \subset G$  mit  $G' \neq \emptyset$  ist:

$$\begin{aligned} a, b \in G' &\Rightarrow a * b \in G' \\ a \in G' &\Rightarrow a^{-1} \in G' \end{aligned}$$

Insbesondere ist  $G'$  mit  $*$  wieder Gruppe (insbesondere ist  $e \in G'$ )

## Bemerkung

Betrachte  $G = \{a_1, a_2\}$  (zwei Elemente)  $\Rightarrow$  ein Element muss das neutrale Element sein, d.h.  $a_1 := e$ , setze  $a := a_2$ . Mit dem Gruppenaxiom folgt:  $a^{-1} = a$ , also  $a \cdot a = e$

$*$	$e$	$a$	Symmetrie $\Rightarrow$ abelsche Gruppe
$e$	$e$	$a$	
$a$	$a$	$e$	

## Definition

$G$  mit  $\cdot$  und  $H$  mit  $\odot$  Gruppen.

Eine Abbildung  $\varphi : G \rightarrow H$  heißt (Gruppen-)Homomorphismus, falls

$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b) \quad \forall a, b \in G,$$

wobei  $\varphi$  eine lineare Abbildung ist.

Homomorphismus heißt **Isomorphismus**, falls  $\varphi$  bijektiv.

## Beispiel 4.1.1

- a) Seien  $G = \mathbb{R}$  mit  $+$  und  $H = \mathbb{R}_+ \setminus \{0\}$  mit  $\cdot$  Gruppen  
 $\Rightarrow \exp : \mathbb{R} \rightarrow \mathbb{R}_+$  ist Isomorphismus (Homomorphismus, da  $e^{x+y} = e^x \cdot e^y$   
 $x \mapsto e^x$   
 und Isomorphismus, da  $x \mapsto e^x$  bijektiv).
- b)  $\mathbb{Z}$  mit  $+$  ist abelsche Gruppe  $\Rightarrow$  für jedes  $m \in \mathbb{Z}$  ist Abbildung

$$\begin{aligned} \varphi_m : \mathbb{Z} &\rightarrow \mathbb{Z} \\ a &\mapsto m \cdot a \end{aligned}$$

Homomorphismus, denn  $m(a+b) = ma + mb$  (hier:  $G = \mathbb{Z}$  mit  $+$  und  $H = \mathbb{Z}$  mit  $+$ ). Sein Bild  $m\mathbb{Z} := \{m \cdot a : a \in \mathbb{Z}\} \subset \mathbb{Z}$  (mit  $m = 1 \Rightarrow m\mathbb{Z} = \mathbb{Z}$  in diesem Fall zu vernachlässigen) ist **Untergruppe**, da  $ma + mb = m(a+b)$  und  $-mb = m(-b)$

- c) zyklische Gruppe mit  $m$  Elementen: Sei  $m \in \mathbb{N}$  **fest**, zu jedem  $r \in \{0, \dots, m-1\}$  betrachte  $r + m\mathbb{Z} \in \mathbb{Z} := \{r + m \cdot a : a \in \mathbb{Z}\}$  (die um  $r$  additiv verschobene Untergruppe  $m\mathbb{Z}$ )

Beispiel  $m = 2$ :  $0 + 2\mathbb{Z}$  Menge der geraden ganzen Zahlen  
 $1 + 2\mathbb{Z}$  Menge der ungeraden ganzen Zahlen

Allgemein:  $\mathbb{Z} = (0 + m\mathbb{Z}) \dot{\cup} (1 + m\mathbb{Z}) \dot{\cup} \dots \dot{\cup} ((m-1) + m\mathbb{Z})$  *disjunkte Vereinigung*

Entscheidung zu welchem  $r + m\mathbb{Z}$  eine Zahl  $a \in \mathbb{Z}$  gehört mittels Division mit Rest:  
 Ist

$$\frac{a}{m} = k + \frac{r}{m} \text{ mit } k \in \mathbb{Z} \text{ und } r \in \{0, \dots, m-1\}$$

$a \in r + m\mathbb{Z}$ , da  $a = km + r$

$\rightsquigarrow \boxed{r + m\mathbb{Z}}$  Restklasse modulo  $m$  (alle Zahlen, die bei Division durch  $m$  Rest  $r$  haben))

$a, a' \in$  derselben Restklasse, falls  $a - a'$  teilbar durch  $m$

Schreibweise:  $a \equiv a' \pmod{m}$  ( $:= \Leftrightarrow a - a'$  teilbar durch  $m$ )

Bezeichnung: Zu jedem  $a \in \mathbb{Z}$  ist  $\bar{a} := a + m\mathbb{Z}$ , seine Restklasse  $\rightsquigarrow \bar{a}$  „Repräsentant“ von  $a + m\mathbb{Z}$ . (Für  $m = 2$  sind  $\bar{0}, \bar{1}$  Repräsentanten von  $0 + 2\mathbb{Z}$  und  $1 + 2\mathbb{Z}$ )

Definiere Addition von Restklassen durch  $\bar{a} + \bar{b} := \overline{a+b}$

## Satz 4.1.2

Für  $m \in \mathbb{Z}$  ist die Menge

$$\mathbb{Z}/m\mathbb{Z} := \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$$

der Restklasse modulo  $m$  mit  $+$  wie oben definiert ist eine abelsche Gruppe, und die Abbildung

$$\begin{aligned}\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \\ a &\mapsto a + m\mathbb{Z}\end{aligned}$$

ist surjektiver Homomorphismus.

### Beweisskizze

Assoziativität und Kommutativität wird von  $\mathbb{Z}$  nach  $\mathbb{Z}/m\mathbb{Z}$  vererbt, zum Beispiel:

$$(\bar{a} + \bar{b}) + \bar{c} = \overline{(a + b) + c} = \overline{a + b + c} = \bar{a} + (\bar{b} + \bar{c})$$

Neutrales Element ist  $\bar{0}$ , da

$$\bar{0} + \bar{a} = \overline{0 + a} = \bar{a}$$

Inverses von  $\bar{a}$  ist  $\overline{-a}$ , da

$$\bar{a} + \overline{-a} = \overline{a + (-a)} = \bar{0}$$

**Bezeichnung:**  $\mathbb{Z}/m\mathbb{Z}$  heißt für  $m > 0$  durch zyklische Gruppe der Ordnung  $m$

### Beispiel Rechnen mit Restklassen:

- Stundenzeiger der Uhr  $\hat{=}$  Restklasse mod 12
- Wochentage  $\hat{=}$  Restklasse mod 7

## Definition Ring

Menge  $R$  mit zwei Verknüpfungen

$$\begin{aligned}+ : R \times R &\rightarrow R \\ (a, b) &\mapsto a + b\end{aligned}$$

$$\begin{aligned}\cdot : R \times R &\rightarrow R \\ (a, b) &\mapsto a \cdot b\end{aligned}$$

heißt Ring, falls

(R1)  $(R, +)$  ist abelsche Gruppe

(R2)  $\cdot$  ist assoziativ, d.h.:  $(a \cdot b) \cdot c = a \cdot (b \cdot c) \forall a, b, c$

(R3) Distributivgesetze  $\forall a, b, c \in \mathbb{R}$ :

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

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

Ring **kommutativ**, falls  $a \cdot b = b \cdot a \forall a, b \in R$

$1 \in R$  **Einselement**, falls  $1 \cdot a = a \cdot 1 = a \forall a \in R$

$0 \in R$  **Nullelement**, falls  $a + 0 = 0 + a = a \forall a \in R \Rightarrow 0 \cdot a = a \cdot 0 = 0$

**Beachte:** Bezüglich  $\cdot$  ist kein Inverses verlangt!

**Beispiel:**  $\mathbb{Z}, \mathbb{Q}$  und  $\mathbb{R}$  sind mit der üblichen Addition  $+$  und Multiplikation  $\cdot$  kommutative Ringe

**Spezialfall:** Ist  $R$  bezüglich  $\cdot$  kommutativ und zusätzlich  $R \setminus \{0\}$  bezüglich  $\cdot$  abelsche Gruppe, dann ist  $(R, +, \cdot)$  „Körper“

## Definition Körper

Eine Menge  $K$  mit zwei Verknüpfungen

$$+ : K \times K \rightarrow K$$

$$(a, b) \mapsto a + b$$

$$\cdot : K \times K \rightarrow K$$

$$(a, b) \mapsto a \cdot b$$

heißt „Körper“ („field“), wenn folgende Axiome gelten:

(K1)  $(K, +)$  ist abelsche Gruppe (neutrales Element  $\equiv$  Nullelement 0)  
(das zu  $a \in K$  inverse Element sei  $-a \in K$ )

(K2)  $(K^*, \cdot)$  mit  $K^* := K \setminus \{0\}$  ist abelsche Gruppe (neutrales Element: Einselement, bezeichnet mit 1; für  $a \in K^*$  bezeichne  $a^{-1}$  (oder  $\frac{1}{a}$ ), das zu  $a$  bezüglich  $\cdot$  inverse Element)

(K3) Distributivgesetze:  $\forall a, b, c \in K$ :

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

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

## Bemerkung

Folgende Rechenregeln gelten im Körper  $(K, +, \cdot)$ :

- $1 \neq 0 \Rightarrow \#K \geq 2$  (das heißt Körper besitzt mindestens 2 Elemente)
- $0 \cdot a = 0 = a \cdot 0 \forall a \in K$

- $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$
- $a \cdot (-b) = -(a \cdot b)$  und  $(-a) \cdot (-b) = a \cdot b$
- $ab = a\tilde{b}$  und  $a \neq 0 \Rightarrow b = \tilde{b}$

### Beispiel 4.1.3

a)  $(\mathbb{Q}, +, \cdot)$  und  $(\mathbb{R}, +, \cdot)$  sind Körper (Achtung:  $(\mathbb{Z}, +, \cdot)$  ist kein Körper, da  $\frac{1}{a} \notin \mathbb{Z}$ )

b)  $(\mathbb{C}, +, \cdot)$  **Körper** der komplexen Zahlen:  $\mathbb{C} := \mathbb{R} \times \mathbb{R}$  mit

$$+ : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$$

$$(a_1, a_2), (b_1, b_2) \mapsto (a_1 + b_1, a_2 + b_2)$$

$$\text{und } \cdot : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$$

$$(a_1, a_2), (b_1, b_2) \mapsto (a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1 - a_1 b_2, a_1 b_2 + a_2 b_1)$$

Nullelement ist  $(0, 0)$ , denn  $(a_1, a_2) + (0, 0) = (a_1 + 0, a_2 + 0) = (a_1, a_2)$

Einselement ist  $(1, 0)$ , denn  $(a_1, a_2) \cdot (1, 0) = (a_1 \cdot 1 - a_2 \cdot 0, a_1 \cdot 0 + a_2 \cdot 1) = (a_1, a_2)$

Inverses von  $(a_1, a_2) \neq (0, 0)$  ist

$$(a_1, a_2)^{-1} := \left( \frac{a_1}{a_1^2 + a_2^2}, \frac{-a_2}{a_1^2 + a_2^2} \right),$$

denn

$$\begin{aligned} (a_1, a_2)(a_1, a_2)^{-1} &= (a_1, a_2) \left( \frac{a_1}{a_1^2 + a_2^2}, \frac{-a_2}{a_1^2 + a_2^2} \right) \\ &= \left( a_1 \frac{a_1}{a_1^2 + a_2^2} - a_2 \frac{-a_2}{a_1^2 + a_2^2}, a_1 \frac{-a_2}{a_1^2 + a_2^2} + a_2 \frac{a_1}{a_1^2 + a_2^2} \right) \\ &= \left( \frac{a_1^2 + a_2^2}{a_1^2 + a_2^2}, \frac{-a_1 a_2 + a_1 a_2}{a_1^2 + a_2^2} \right) = (1, 0) \quad (\text{da } \mathbb{R} \text{ bezüglich } \cdot \text{ kommutativ}) \end{aligned}$$

### Beispiel 4.1.4

$K[t] := \{f(t) := \sum_{j=0}^n a_j t^j \text{ mit } a_0, \dots, a_n \in K\}$  (Polynome über  $K$ ; Menge aller Polynome mit Koeffizienten in  $K$ )

**Hier:**  $t$  Unbekannte (muss nicht aus  $K$  sein); alles einsetzbar, was sinnvoll ist.

$a \cdot t := (ta_1, ta_2)$  mit  $a \in \mathbb{C}, t \in \mathbb{R}$

**Monom:** alle  $a_i = 0$  außer einem

**Nullpolynom:**  $a_j \forall j$  (d.h.  $f \equiv 0$ ), d.h.  $f(t) = a_r t^r$

**Grad von  $f$ :**  $\deg f := \begin{cases} -\infty, & \text{falls } f \equiv 0 \\ \max\{r \in \mathbb{N}_0 : a_r \neq 0\}, & \text{sonst} \end{cases}$

**„Natürliche“ Addition und Multiplikation in  $K[t]$**

Sei  $f, g \in K[t]$ , d.h.z.B.:

$$f(t) := \sum_{j=0}^n a_j t^j, \quad g(t) := \sum_{j=0}^m b_j t^j$$

Definiere  $s := \max\{m, n\}$

$\Rightarrow (f + g)(t) := \sum_{j=0}^s (a_j + b_j) \cdot t^j$  (dabei vorausgesetzt, dass  $f$  oder  $g$  mit  $a'_j s = 0$  oder  $b'_j s = 0$  aufgefüllt werden können, z.B.:  $f(t) = 3 + 0t + 0t^2$ ,  $g(t) = 2 + 5t + 3t^2$   
 $\Rightarrow (f + g)(t) = (3 + 2) + 5t + 3t^2$ )

Des Weiteren:

$$\begin{aligned} (f \cdot g)(t) &= \left( \sum_{j=0}^n a_j t^j \right) \cdot \left( \sum_{k=0}^m b_k t^k \right) \\ &= \sum_{r=0}^{m+n} c_r t^r \quad \text{mit } c_r := \sum_{j+k=r} a_j b_k \end{aligned}$$

$$\text{(d.h. } c_0 = a_0 + b, \quad c_1 = a_0 b_1 + a_1 b_0, \quad c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0)$$

### Bemerkung

$K$  Körper  $\Rightarrow (K[t], +, \cdot)$  ist kommutativer Ring („Polynomring über  $K$ “)

### Beachte

Der Mangel eines Rings gegenüber einem Körper ist, dass man im Allgemeinen nicht dividieren kann, das heißt für  $f \in K[t]$  ist im Allgemeinen  $f^{-1}(t) := \frac{1}{f(t)} \notin K[t]$

### Satz 4.1.5 Division mit Rest

$f, g \in K[t], g \neq 0$

$\Rightarrow$  es gibt ein eindeutig bestimmte Polynome  $q, r \in K[t]$ , sodass  $f = q \cdot g + r$  und  $\deg r < \deg g$

## Beispiel

$$K = \mathbb{R}, f(t) := 3t^3 + 2t + 1, g(t) := t^2 - 4t$$

$$\begin{array}{r} \left( \begin{array}{r} 3t^3 \phantom{+ 2t + 1} \\ - 3t^3 + 12t^2 \end{array} \right) : (t^2 - 4t) = 3t + 12 + \frac{50t + 1}{t^2 - 4t} \\ \hline \phantom{\left( \right)} \phantom{3t^3} + 2t \\ \phantom{\left( \right)} \phantom{3t^3} \phantom{+ 2t} + 12t^2 \\ \phantom{\left( \right)} \phantom{3t^3} \phantom{+ 2t} \phantom{+ 12t^2} - 12t^2 + 48t \\ \hline \phantom{\left( \right)} \phantom{3t^3} \phantom{+ 2t} \phantom{+ 12t^2} \phantom{- 12t^2} + 48t \\ \phantom{\left( \right)} \phantom{3t^3} \phantom{+ 2t} \phantom{+ 12t^2} \phantom{- 12t^2} \phantom{+ 48t} - 50t \\ \hline \phantom{\left( \right)} \phantom{3t^3} \phantom{+ 2t} \phantom{+ 12t^2} \phantom{- 12t^2} \phantom{+ 48t} \phantom{- 50t} 50t \end{array}$$

$\Rightarrow$  Also ist hier  $r(t) = 50t + 1$  und  $q(t) = 3t + 12$ ;  $\deg r = 1 < 2 = \deg g$

## Beispiel

a)  $f(t) := t^2 + 1$  hat keine Nullstellen in  $\mathbb{R}$  ( $t^2 + 1 = 0 \Leftrightarrow t^2 = -1$ )

b)  $f(t) := t^2 + 1 \in \mathbb{R}[t]$  hat zwei Nullstellen in  $\mathbb{C}$ , nämlich  $i$  und  $-i$ ,  
weil  $i^2 = -1 \Leftrightarrow i^2 + 1 = 0$  und  $(-i)^2 = i^2 = -1$

□

## Lemma 4.1.6

Sei  $\lambda \in K$  Nullstelle von  $f \in K[t]$

$\Rightarrow \exists g \in K[t]$ , sodass

-  $f(t) = (t - \lambda)g(t)$

-  $\deg g = \deg f - 1$

## Beispiel

$\mathbb{R}, f(x) := x^3 - 4x^2 + 5x - 2$  hat Nullstelle  $\lambda_1 = 1$  (Wird geraten oder durch Newton-Verfahren erhalten)

$$\Rightarrow f(x) = (x - 1)g(x)$$

Polynomdivision liefert:

$$\begin{array}{r} \left( \begin{array}{r} x^3 - 4x^2 + 5x - 2 \\ - x^3 \phantom{+ 5x} + x^2 \end{array} \right) : (x - 1) = x^2 - 3x + 2 \\ \hline \phantom{\left( \right)} \phantom{x^3} - 3x^2 + 5x \\ \phantom{\left( \right)} \phantom{x^3} \phantom{- 3x^2} + 3x \\ \hline \phantom{\left( \right)} \phantom{x^3} \phantom{- 3x^2} \phantom{+ 3x} - 2x - 2 \\ \phantom{\left( \right)} \phantom{x^3} \phantom{- 3x^2} \phantom{+ 3x} \phantom{- 2x} + 2 \\ \hline \phantom{\left( \right)} \phantom{x^3} \phantom{- 3x^2} \phantom{+ 3x} \phantom{- 2x} \phantom{+ 2} 0 \end{array}$$

also  $f(x) = (x - 1)(x^2 - 3x + 2)$  und  $\deg g = 2 = \underbrace{\deg f - 1}_3$

□

## Definition

- Vielfachheit einer Nullstelle  $\lambda$ :  
Maximales  $r$ , sodass  $f$  eine Zerlegung  $f(t) = (t - \lambda)^r \cdot g(t)$  mit  $g \in K[t]$  hat

**Beispiel:**  $f(t) = (t - 1)^3 \cdot g(t) \Rightarrow$  Vielfachheit der Nullstelle  $\lambda_1 = 1$  ist 3

- $f$  zerfällt in Linearfaktoren, falls  $f \in K[t]$  die Darstellung

$$f(t) = (t - \lambda_1)^{r_1} \cdot \dots \cdot (t - \lambda_m)^{r_m}$$

hat (d.h.  $\lambda_i$  ist Nullstelle von  $f$  mit Vielfachheit  $r_i$ )

**Beispiel:**  $f(t) = t^2 + 1$  zerfällt über  $\mathbb{R}$  **nicht** in Linearfaktoren; aber  $f(t) = t^2 - 1 = (t + 1)(t - 1)$  wohl.

## Fundamentalsatz der Algebra [Gauss 1799]

Jedes Polynom  $f \in \mathbb{C}[t]$  mit  $\deg f > 0$  hat **mindestens eine** Nullstelle in  $\mathbb{C}$

Hat  $f$  eine Nullstelle  $\Rightarrow$  Herausdividieren mit Lemma 4.1.6 und wiederhole (da  $g(t)$  wieder mindestens einen Nullstelle hat wegen Fundamentalsatz der Algebra) und  $\dots$  und kein Rest, das heißt  $\deg r = 0$

### Korollar 4.1.7

Jedes Polynom in  $\mathbb{C}[t]$  zerfällt in Linearfaktoren (heißt natürlich nicht, dass die Nullstellen reell sind)

### Lemma 4.1.7

$f \in \mathbb{R}[t]$  und  $\lambda \in \mathbb{C}$  Nullstelle von  $f$   
 $\Rightarrow \bar{\lambda} \in \mathbb{C}$  ist auch eine Nullstelle von  $f$ , und beide haben dieselbe Vielfachheit.

### Beispiel

$f(t) = t^2 + 1 \Rightarrow \lambda = i$  Nullstelle und ebenso  $\bar{\lambda} = -i$ ; beide mit Vielfachheit 1 (Nullstellen eines Polynoms mit reellen Koeffizienten sind symmetrisch bezüglich der x-Achse)

### Korollar 4.1.9

Jedes Polynom  $f \in \mathbb{R}[t]$  von **ungeradem** Grad hat mindestens eine reelle Nullstelle.

### **Begründung**

Polynom von Grad  $d$  zerfällt über  $\mathbb{C}$  in Linearfaktoren, d.h.  $r_1 + \dots + r_m = d$ , jede Nullstelle in  $\mathbb{C}$  tritt mit komplex Konjugierte auf

$\Rightarrow$  für  $f$  mit ungeradem Grad muss es einzelne reelle Nullstelle geben

## IV.2 Vektorräume

Im Folgenden:  $K = (K, +, \cdot)$  stets Körper

### Definition 4.2.1

Sei  $(K, +, \cdot)$  Körper. Eine Menge  $V$  mit der inneren Verknüpfung

$$\begin{aligned}\oplus : V \times V &\rightarrow V && \text{(Addition)} \\ (v, w) &\mapsto v \oplus w\end{aligned}$$

und einer (äußeren) Verknüpfung

$$\begin{aligned}\cdot : K \times V &\rightarrow V && \text{ („Multiplikation mit Skalaren“ oder} \\ (\lambda, v) &\mapsto \lambda \cdot v && \text{ „skalare Multiplikation“)}\end{aligned}$$

heißt  $(K)$ -Vektorraum oder Vektorraum über  $K$ , falls gilt

(V1)  $(V, \oplus)$  ist abelsche Gruppe (neutrales Element: Nullvektor oder  $\mathbf{0}$ ; Inverses von  $v \in V$  heißt Negatives, bezeichnet mit  $-v$ )

(V2) Verträglichkeit der Multiplikation mit Skalaren:

$$\begin{aligned}- (\lambda + \mu) \cdot v &= \lambda \cdot v + \mu \cdot v \\ - \lambda \cdot (v \oplus u) &= \lambda \cdot v \oplus \lambda \cdot u \\ - (\lambda \cdot \mu) \cdot v &= \lambda \cdot (\mu \cdot v), \quad 1 \cdot v = v\end{aligned}$$

**Beachte:** Eine innere Verknüpfung  $\cdot : V \times V \rightarrow ?$  ist (noch) nicht definierte  $\rightsquigarrow$  „inneres Produkt“, „Skalarprodukt“  $\cdot : V \times V \rightarrow K$  ( $\rightsquigarrow$  Euklidischer Vektorraum)

### Rechenregeln 4.2.2 in $K$ -Vektorraum $V$

- a)  $0 \cdot v = \mathbf{0}$
- b)  $\lambda \cdot \mathbf{0} = \mathbf{0}$
- c)  $\lambda \cdot v = \mathbf{0} \Rightarrow \lambda = \mathbf{0} \vee v = \mathbf{0}$
- d)  $(-1) \cdot v = -v$

### Beweis von a)

$0 \cdot v = (0 + 0) \cdot v = 0 \cdot v \oplus 0 \cdot v \Rightarrow 0 \cdot v = \mathbf{0}$ , weil  $0 \cdot v$  neutrales Element bezüglich Addition  $\oplus$  sein muss.

### Beispiel 4.2.3

a) Standardbeispiel ist der (Standard-)Vektorraum

$$V : K^n = \left\{ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in K \right\} \text{ mit}$$

$\oplus : V \times V \rightarrow V$  (komponentenweise Addition)

$$(x, y) \mapsto \begin{array}{c} x \oplus y \\ \ddots \\ \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix} \end{array}$$

$\cdot : K \times V \rightarrow V$  (Multiplikation jedes

$$(\lambda, v) \mapsto \begin{array}{c} \lambda \cdot v \\ \ddots \\ \begin{pmatrix} \lambda \cdot x_1 \\ \lambda \cdot x_2 \\ \vdots \\ \lambda \cdot x_n \end{pmatrix} \end{array} \text{ Eintrags mit Skalar})$$

b) Vektorraum der  $m \times n$ -Matrizen über  $K$

$$\begin{aligned} V := K^{m \times n} (= M(m \times n, K)) &:= \{ A = (a_{jk})_{j=1, \dots, m, k=1, \dots, n} : a_{jk} \in K \forall j, k \} \\ &= \left\{ A = (a_{jk})_{\substack{j=1, \dots, m \\ k=1, \dots, n}} : a_{jk} \in K \forall j, k \right\} \end{aligned}$$

Man ordnet Matrizen in einem rechteckigen Schema an:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

mit  $m$  Zeilen und  $n$  Spalten.

### Addition in $K^{m \times n}$

$$\begin{aligned} \oplus : K^{m \times n} \times K^{m \times n} &\rightarrow K^{m \times n} \\ (A, B) &\mapsto A \oplus B := (a_{kj} + b_{kj})_{\substack{k=1, \dots, m \\ j=1, \dots, n}} \end{aligned}$$

### Skalare Multiplikation

$$\begin{aligned} \cdot : K \times K^{m \times n} &\rightarrow K^{m \times n} \\ (\lambda, A) &\mapsto \lambda \cdot A := (\lambda \cdot a_{kj})_{\substack{k=1, \dots, m \\ j=1, \dots, n}} \end{aligned}$$

- c) Polynomring  $(K[t], +, \cdot)$  kommutativer Ring  
(innere) Addition wie in (4.1.4) b)  
(äußere) Multiplikation mit Skalaren:

$$\begin{aligned} \cdot : K \times K[t] &\rightarrow K[t] \\ (\lambda, f) &\mapsto (\lambda \cdot f)(t) := \lambda \left( \sum_{j=0}^n a_j t^j \right) = \sum_{j=0}^n (\lambda \cdot a_j) t^j \end{aligned}$$

### Definition 4.2.4

Sei  $V$   $K$ -Vektorraum und  $W \subset V$  Teilmenge.  $W$  heißt Unter(vektor)raum von  $V$ , falls

(UV1)  $W \neq 0$

(UV2)  $v, w \in W \Rightarrow v \oplus w \in W$  ( $W$  abgeschlossen bezüglich  $\oplus$ )

(UV3)  $\lambda \in K, v \in W \Rightarrow \lambda \cdot v \in W$  ( $W$  abgeschlossen bezüglich Multiplikation mit Skalaren)

Insbesondere:  $W$  mit  $\oplus, \cdot$  wieder Vektorraum (mit  $\oplus, \cdot$  aus  $V$ )

### Beispiel 4.2.5

a)

$$W = \{0\} \text{ für } W \left\{ \left( \begin{array}{c} x_1 \\ x_2 \end{array} \right) \in \mathbb{R}^2 : a_1 x_1 + a_2 x_2 = 0 \text{ für festes } a_1, a_2 \in K \right\}$$

sind Untervektorräume von  $\mathbb{R}^2$ , aber die Menge

$$\left\{ \left( \begin{array}{c} x_1 \\ x_2 \end{array} \right) \in \mathbb{R}^2 : a_1 x_1 + a_2 x_2 = b \text{ für } a_1, a_2, b \in K \text{ und } b \neq 0 \right\} =: \hat{W}$$

ist kein Untervektorraum von  $\mathbb{R}^2$ , denn  $v, w \in W$ , d.h.  $v$  so, dass

$$a_1 v_1 + a_2 v_2 = 0$$

und  $w$  so, dass

$$b_1 w_1 + b_2 w_2 = 0$$

$$\Rightarrow v \oplus w = \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \end{pmatrix} \quad \text{Zu zeigen: } v \oplus w \in W$$

$$\begin{aligned} a_1(v_1 + w_1) + a_2(v_2 + w_2) &= a_1 v_1 + a_1 w_1 + a_2 v_2 + a_2 w_2 \\ &= \underbrace{a_1 v_1 + a_2 v_2}_{=0} + \underbrace{a_1 w_1 + a_2 w_2}_{=0} = 0 \end{aligned}$$

Dagegen:  $\hat{W}$  ist kein Untervektorraum von  $\mathbb{R}^2$ , da

$$\begin{aligned} v, w \in \hat{W} \text{ bedeutet: } a_1 v_1 + a_2 v_2 &= b \\ a_1 w_1 + a_2 w_2 &= b \end{aligned}$$

$$\begin{aligned} \Rightarrow v \oplus w &= \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \end{pmatrix} \quad \text{und } a_1(v_1 + w_1) + a_2(v_2 + w_2) \\ &= \underbrace{a_1 v_1 + a_2 v_2}_{=b} + \underbrace{a_1 w_1 + a_2 w_2}_{=b} \\ &= 2b \neq b \end{aligned}$$

$$\Rightarrow v \oplus w \notin \hat{W}$$

b)

$$V = \text{Abb}(\mathbb{R}, \mathbb{R}) := \{f : \mathbb{R} \rightarrow \mathbb{R}, f \text{ Funktion}\}$$

hat Untervektorräume

$$\begin{aligned} \mathbb{R}[t]_d &:= \{f \in \mathbb{R}[t] \text{ mit } \deg f \leq d\} \subset \mathbb{R}[t] \\ &\subset \{f \in \text{Abb}(\mathbb{R}, \mathbb{R}) : f \text{ stetig}\} \subset V \end{aligned}$$

## Definition 4.2.6

Familie von Vektoren  $v^j \ v^1, \dots, v^r \in V$

$r \in V$  heißt **Linearkombination** von  $v^1, \dots, v^r$ , wenn es  $\lambda_1, \dots, \lambda_r \in K$  gibt, sodass sich  $v$  als

$$v = \lambda_1 v^1 \oplus \lambda_2 v^2 \dots \lambda_r \oplus v^r$$

darstellen lässt.

Bezeichnung  $\text{span}\{v^1, \dots, v^r\} := \{v \in V : v \text{ ist Linearkombination von } v^1, \dots, v^r\}$

Es gilt:  $v^1, \dots, v^r \in V$

$\Rightarrow \text{span}\{v^1, \dots, v^r\} \subseteq V$  ist Untervektorraum

Genauer:  $\text{span}\{v^1, \dots, v^r\}$  ist der **kleinste** Untervektorraum von  $V$ , der  $v^1, \dots, v^r$  enthält.

## Beispiel

$V = \mathbb{R}^2, K = \mathbb{R}$

$$\text{a) } v^1 := \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \quad v^2 := \begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

$$\text{span}\{v^1\} = \{v \in V : v_2 = 0\}$$

$$\text{span}\{v^2\} = \{v \in V : v_1 = 0\}$$

$$\text{span}\{v^1, v^2\} = V (= \mathbb{R}^2), \text{ da sich jedes } v \in V \text{ als}$$

$$v = \lambda_1 v^1 + \lambda_2 v^2$$

darstellen lässt.

$$\text{b) } v^0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad v^1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad v^2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\Rightarrow \text{span}\{v^1\} \subset V$$

$$\text{span}\{v^0, v^1, v^2\} = V = \text{span}\{v^0, v^2\} = \text{span}\{v^0, v^1\}$$

$$\text{Beispiel } w = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}, \text{ Finde } \lambda_0, \lambda_1 \in \mathbb{R}, \text{ sodass } w = \lambda_0 v^0 + \lambda_1 v^1$$

$\rightsquigarrow$  „Darstellung“ von  $V$  über  $\text{span}$  nicht „eindeutig“

$\rightsquigarrow$  „Effiziente“ Darstellung, das heißt: Darstellung mit maximaler Anzahl aufspannender Vektoren

## Definition 4.2.7

Sei  $V$   $K$ -Vektorraum. Eine Familie von Vektoren  $(v^j)_{j \in I}$  ( $I$  Indexmenge) heißt **linear unabhängig**, falls

$$\sum_{j \in I} \lambda_j v^j = \mathbf{0} \Rightarrow \lambda_j = 0 \text{ für alle } j \in I,$$

ansonsten linear abhängig.

## Beispiel 4.2.8

a)  $K = \mathbb{R}, v = \mathbb{R}^n$

Betrachte die **Einheitsvektoren**

$$e^1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e^2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e^n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

wobei der Index die Stelle der 1 angibt.

Die Familie  $(e^j)_{j=1, \dots, n}$  ist linear unabhängig, denn:

Es gelte:  $\sum_{j=1}^n \lambda_j e^j = \mathbf{0}$ ; zu Zeigen:  $\lambda_j = 0 \forall j = 1, \dots, n$

### Beweis

$$\begin{aligned} \sum_{j=1}^n \lambda_j e^j &= \lambda_1 e^1 + \lambda_2 e^2 + \dots + \lambda_n e^n = \mathbf{0} \\ \Leftrightarrow \lambda_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \lambda_n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} &= \mathbf{0} \\ &\Leftrightarrow \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \mathbf{0} \end{aligned}$$

Mit derselben Argumentation kann man auch zeigen, dass eine beliebige Teilmenge von  $(e^j)_{j=1, \dots, n}$  auch linear unabhängig ist.

b)  $K = \mathbb{R}, V = \mathbb{R}[t] = \left\{ f(t) = \sum_{j=0}^n a_j t^j : a_j \in \mathbb{R} \right\}$

Betrachte die Monome  $(t^j)_{j=0, \dots, n}$ . Diese sind linear unabhängig, denn: Es gelte

$$\sum_{j=0}^n a_j t^j = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n \equiv 0 \quad ((d.h. :) = 0 \forall t)$$

$$\Rightarrow a_0 = 0, a_1 = 0, \dots, a_n = 0$$

(Oder: Grad des Polynoms links und rechts anschauen)

## Definition 4.2.9

Eine Familie  $\mathcal{B} = (v^j)_{j \in I}$  in einem Vektorraum  $V$  heißt **Erzeugendensystem** von  $V$ , wenn

$$V = \text{span} \left( v^j \right)_{j \in I}$$

d.h. jedes  $v \in V$  lässt sich als Linearkombination der  $v^j$  ( $j \in I$ ) schreiben, d.h. jedes  $v \in V$  hat Darstellung

$$v = \sum_{j \in I} \lambda_j v^j$$

mit irgendwelchen  $\lambda_j \in K$ .

Die Familie  $\mathcal{B} = (v^j)_{j \in I}$  heißt **Basis** von  $V$ , falls

- $B$  ein Erzeugendensystem ist **und**
- die Vektoren in  $B$  sind linear unabhängig

Ist  $B = \{v^1, \dots, v^n\}$  eine Basis von  $V$ , so heißt

$$\begin{array}{ll} \#B = n & =: \dim V \\ \text{(Länge der Basis)} & \text{(Dimension des Vektorraums)} \end{array}$$

Falls  $B$  keine **endliche** Basis ist (d.h. keine Basis endlicher Länge), so setzen wir  $\dim V := \infty$

## Beispiel

a)  $K = \mathbb{R}$ ,  $V = \mathbb{R}^n$

$B = \{e^1, \dots, e^n\}$  Einheitsvektoren bilden Basis von  $\mathbb{R}^n$  und  $\dim \mathbb{R}^n = n$  („kanonische Basis“)

Dagegen ist  $\{e^1, 2e^1, e^2, \dots, e^n\}$  keine Basis, aber ein Erzeugendensystem von  $V$ , aber es ist eine Basis von  $W := \{v \in \mathbb{R}^n : v_1 = 0\}$  (erste Komponente jedes Vektors verschwindet).

b)  $K = \mathbb{R}$ ,  $V = \mathbb{R}[t]$

Die Monome  $(t^j)_{j=0, \dots, n}$  bilden eine Basis für  $V$ , d.h. alle Polynome werden von Monomen erzeugt und Monome sind linear unabhängig. Da Polynomgrad beliebig sein kann, gilt  $\dim \mathbb{R}[t] = \infty$ .

## Satz

Jeder Vektorraum besitzt eine Basis.

## Beweis

Bei  $\dim V < \infty$  konstruktiv nach Basisauswahlsatz.

## Basisauswahlsatz

Aus jedem endlichen Erzeugendensystem (d.h. Erzeugendensystem von  $V$  existiert mit endlich vielen Vektoren) kann man eine Basis auswählen.

Inbesondere hat jeder Vektorraum  $V$  mit  $\dim V < \infty$  eine endliche Basis.

## Beispiel

$K = \mathbb{R}, V = \mathbb{R}^n$

Betrachte  $\{e^1, 2e^1, e^2, 2e^2, \dots, e^n, 2e^n, e^1 + e^2\}$ . Dies ist Erzeugendensystem von  $\mathbb{R}^n$ , alle Vektoren linearabhängig  $\rightsquigarrow$  streiche alle linearen Abhängigkeiten, aber stelle sicher, dass  $\text{span}\{\dots\} = V$

$\Rightarrow \{e^1, 2e^1, e^2, 2e^2, \dots, e^n, 2e^n, e^1 + e^2 \setminus 2e^1, 2e^2, \dots, 2e^n, e^1 + e^2\}$  ist Basis, sowie  $\{e^1, 2e^1, e^2, 2e^2, \dots, e^n, 2e^n, e^1 + e^2 \setminus e^1, e^2, \dots, e^n, e^1 + e^2\}$ .

## Satz 4.2.11

Sei  $\mathcal{B} = \{v^1, \dots, v^n\}$  Familie von Vektoren in  $K$ -Vektorraum  $V \neq \{0\}$ . Dann ist **äquivalent**:

- (i)  $\mathcal{B}$  ist eine **Basis**, das heißt: ein lineares unabhängiges Erzeugendensystem
- (ii)  $\mathcal{B}$  ist ein **unverkürzbares** Erzeugendensystem (das heißt kein Vektor darf weggelassen werden)
- (iii) Zu jedem  $v \in V$  gibt es **eindeutige**  $\lambda_1, \dots, \lambda_n \in K$ , sodass  $v$  die Darstellung

$$v = \lambda_1 v^1 + \lambda_2 v^2 + \dots + \lambda_n v^n$$

(das heißt  $\mathcal{B}$  ist Erzeugendensystem **und** eindeutige Darstellung)

- (iv)  $\mathcal{B}$  ist **unverlängerbar** unabhängig, das heißt für jedes  $v \in V$  wird

$$\mathcal{B} \cup \{v\} = \{v^1, \dots, v^n, v\}$$

linear abhängig.

**Beispiel für (iv)**

$V = \mathbb{R}^2$ ,  $\mathcal{B} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$  mit  $v := \begin{pmatrix} 1 \\ 1 \end{pmatrix}$  wäre

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

linear abhängig.

**Beweis**

[Fi] §1.5.2

## IV.3 Multiplikation von Matrizen und Vektoren

Im folgenden stets  $K$  Körper und  $j, k, m, n, p, q, r, s \in \mathbb{N}$

### Definition

Sei

$$A \in K^{m \times n} = \left\{ A = (a_{jk})_{\substack{1 \leq j \leq m \\ 1 \leq k \leq n}}, a_{jk} \in K \forall K \right\}$$

$$B \in K^{n \times p} = \left\{ B = (b_{jk})_{\substack{1 \leq j \leq n \\ 1 \leq k \leq p}}, b_{jk} \in K \forall K \right\}$$

Definiere Matrixprodukt  $AB := A \cdot B =: C \in K^{m \times p}$

$$C = (c_{jk})_{\substack{1 \leq j \leq m \\ 1 \leq k \leq p}} \text{ durch } c_{jk} := \sum_{r=1}^n a_{jr} b_{rk} = a_{j1} b_{1k} + \dots + a_{jn} b_{nk}$$

für  $1 \leq j \leq m, 1 \leq k \leq p$

Das heißt:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1p} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{np} \end{pmatrix} = \begin{pmatrix} \circ & \square & & \\ \circ & & & \square \end{pmatrix}$$

**Beachte:** Die „innere“ Matrixdimension  $n$  muss übereinstimmen, damit  $AB$  sinnvoll definiert.

**Spezialfall:**  $m = n = p$ : quadratische Matrix

### Beispiel

a)  $m = 1, p = 1, n \in \mathbb{N}$  beliebig

$$A = (a_{11}, \dots, a_{1n}) \in \mathbb{R}^{1 \times n}, B = \begin{pmatrix} b_{11} \\ \vdots \\ b_{n1} \end{pmatrix} \in \mathbb{R}^{n \times 1}$$

$$\Rightarrow AB = (a_{11}, \dots, a_{1n}) \cdot \begin{pmatrix} b_{11} \\ \vdots \\ b_{n1} \end{pmatrix} = a_{11}b_{11} + \dots + a_{1n}b_{n1} \in \mathbb{R}^{1 \times 1}$$

b)  $m, p \in \mathbb{N}$  beliebig,  $n = 1$

$$A = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} \in \mathbb{R}^{m \times 1}, B = (b_{11}, \dots, b_{1p}) \in \mathbb{R}^{1 \times p}$$

$$\Rightarrow AB = \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} \cdot (b_{11}, \dots, b_{1p}) = \begin{pmatrix} a_{11}b_{11} & \dots & a_{11}b_{1p} \\ a_{21}b_{11} & \dots & a_{21}b_{1p} \\ \vdots & & \vdots \\ a_{m1}b_{11} & \dots & a_{m1}b_{1p} \end{pmatrix}$$

c)  $m, n \in \mathbb{N}$  beliebig,  $p = 1$  (Multiplikation einer Matrix mit einem Vektor)  
 $A \in \mathbb{R}^{m \times n}, v \in \mathbb{R}^n (= \mathbb{R}^{n \times 1})$

$$\begin{aligned} \Rightarrow Av &= \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} a_{11}v_1 + \dots + a_{1n}v_n \\ \vdots \\ a_{m1}v_1 + \dots + a_{mn}v_n \end{pmatrix} \\ &=: \begin{pmatrix} w_1 \\ \dots \\ w_n \end{pmatrix} =: w \in \mathbb{R}^n \end{aligned}$$

### Typisch:

- $A \in K^{m \times n}, B \in K^{n \times p} \Rightarrow AB \in K^{m \times p}$
- $A \in K^{m \times n}, v \in K^n \Rightarrow Av \in K^m$

### Zahlenbeispiele

$$\text{a) } \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}}_{\in \mathbb{R}^{2 \times 2}} \underbrace{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}}_{\in \mathbb{R}^{2 \times 3}} = \underbrace{\begin{pmatrix} 1 & 0 & 5 \\ 1 & 0 & 1 \end{pmatrix}}_{\in \mathbb{R}^{2 \times 3}}$$

$$\text{b) } \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}}_{\in \mathbb{R}^{2 \times 2}} \underbrace{\begin{pmatrix} 1 & 2 \\ 0 & 3 \\ 1 & 4 \end{pmatrix}}_{\in \mathbb{R}^{3 \times 2}} \text{ nicht definiert}$$

$$\text{c) } \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}}_{\in \mathbb{R}^{2 \times 3}} \underbrace{\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}}_{\in \mathbb{R}^{3 \times 1}} = \underbrace{\begin{pmatrix} 6 \\ 5 \end{pmatrix}}_{\in \mathbb{R}^{2 \times 1}}$$

$$\text{d) } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

### Allgemein

$E \in \mathbb{R}^{n \times n}$  mit  $E = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix}$ , d.h.  $E = (\delta_{jk})_{1 \leq j, k \leq n}$  mit

$$\delta_{jk} = \begin{cases} 1, & \text{falls } j = k \\ 0, & \text{sonst} \end{cases} \quad \text{Kronecker-Symbol}$$

heißt **Einheitsmatrix**.

### Achtung:

Selbst wenn  $m = n = p$ , ist die Multiplikation im Allgemeinen nicht kommutativ.

### Beispiel

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow AB \neq BA$$

### Satz 4.3.1

Für alle  $A \in K^{m \times n}$ ,  $B \in K^{n \times p}$ ,  $C \in K^{p \times q}$  gilt

$$(AB)C = A(BC)$$

### Beweis

Vorraussetzungen an die Dimension erfüllt.

Setze  $D := AB$ ,  $D$  hat Einträge  $D = (d_{jk})_{\substack{1 \leq j \leq n \\ 1 \leq k \leq p}}$  mit  $d_{jk} = \sum_{r=1}^n a_{jr} b_{rk}$

$F := DC$  hat Einträge  $(f_{js})_{\substack{1 \leq j \leq m \\ 1 \leq s \leq q}}$  mit  $f_{js} = \sum_{r=1}^p d_{jr} c_{rs}$

$$\begin{aligned}
\Rightarrow f_{js} &= \sum_{r=1}^p d_{jr} c_{rs} = \sum_{k=1}^p \left( \sum_{r=1}^n a_{jr} b_{rk} \right) c_{ks} \\
&= \sum_{r=1}^n a_{jr} \underbrace{\sum_{k=1}^p b_{rk} c_{ks}}_{:=g_{rs}} \quad \text{Einträge von } G := BC \\
&= \sum_{r=1}^n a_{jr} g_{rs} = \text{Einträge von } A(BC)
\end{aligned}$$

Weiter gilt:

$$\begin{aligned}
\forall A \in K^{m \times n}, B, C \in K^{n \times p} \\
A \cdot (B + C) &= A \cdot B + A \cdot C \\
\forall A, B \in K^{m \times n}, C \in K^{n \times p} \\
(A + B) \cdot C &= A \cdot C + B \cdot C
\end{aligned}$$

## Definition

$A \in K^{n \times n}$  (quadratisch!) heißt **invertierbar**, falls es ein  $X \in K^{n \times n}$  gibt mit

$$A \cdot X = X \cdot A = I \quad (\text{Einheitsmatrix})$$

Bezeichnung:  $X = A^{-1}$ , d.h.  $A \cdot A^{-1} = A^{-1} \cdot A = I$

**Inverse ist eindeutig**, denn: Annahme: es gibt  $X, Y \in K^{n \times n}$  mit  $AX = I = XA$  und  $AY = I = YA$

$$\Rightarrow \mathbf{X} = XI = X(AY) = (XA)Y = IY = Y$$

Seien  $A, B \in K^{n \times n}$  invertierbar  $\Rightarrow AB$  invertierbar und es gilt  $(AB)^{-1} = B^{-1}A^{-1}$ . Hierbei ist die Reihenfolge zu beachten!

## Beweis

$A, B$  invertierbar, d.h.  $A \cdot A^{-1} = A^{-1} \cdot A = I$  und  $B \cdot B^{-1} = B^{-1} \cdot B = I$

$$\Rightarrow (B^{-1}A^{-1})(AB) = B^{-1} \underbrace{(A^{-1}A)}_{=I} B = B^{-1}B = I$$

$$\Rightarrow (AB)(B^{-1}A^{-1}) = A \underbrace{(BB^{-1})}_{=I} A^{-1} = I$$

## Definition

Die Menge  $GL(n, K) := \{A \in K^{n \times n}, A \text{ invertierbar}\}$  heißt *General Linear Group*, da sie mit der Matrixmultiplikation und  $I$  als neutralem Element eine Gruppe bildet (aber im Allgemeinen keine abelsche Gruppe)

## Definition

Für  $A \in K^{m \times n}$  mit  $A = (a_{jk})_{\substack{1 \leq j \leq m \\ 1 \leq k \leq n}}$  heißt

$$A^T := (a_{kj})_{\substack{1 \leq k \leq n \\ 1 \leq j \leq m}} \in K^{n \times m} = \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \dots & a_{mn} \end{pmatrix}$$

die zu  $A$  **transponierte** Matrix. (Andere Bezeichnung:  $A^t$ )

Für  $v \in K^n (= K^{n \times 1})$ ,  $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$  ist  $v^T = (v_1, \dots, v_n) \in K^{1 \times n}$

## Beachte

- Für  $v \in K^n$  ist  $vv^T \in K^{n \times n}$   $vv^T = \begin{pmatrix} v_1v_1 & \dots & v_1v_n \\ \vdots & & \vdots \\ v_nv_1 & \dots & v_nv_n \end{pmatrix}$

-  $v^T v \in K$ ,  $v^T v = \sum_{j=1}^n v_j^2 = \|v\|_2^2$  (Skalarprodukt von Vektoren)

Insbesondere ist  $\frac{vv^T}{v^T v}$  wohldefiniert, da  $\frac{vv^T}{v^T v} = \underbrace{\frac{1}{v^T v}}_{\text{Skalar}} \cdot \underbrace{vv^T}_{\text{Matrix}}$ , aber  $\frac{v^T v}{vv^T}$  nicht wohldefiniert.

## Satz 4.3.2

i)  $A \in K^{m \times n} \Rightarrow (A^T)^T = A$

ii)  $A, B \in K^{m \times n} \Rightarrow (A + B)^T = A^T + B^T$

iii)  $A \in K^{m \times n}, B \in K^{n \times p}$

$\Rightarrow (AB)^T = B^T A^T$  (Hierbei ist die Reihenfolge zu beachten!)

## Beweis (iii)

$AB =: C \in K^{m \times p}$  mit  $c_{jk} = \sum_{r=1}^n a_{jr} b_{rk}$ ,  $1 \leq j \leq m$ ,  $1 \leq k \leq p$   
 $\Rightarrow C^T = (\tilde{c}_{jk})_{\substack{1 \leq j \leq p \\ 1 \leq k \leq m}} \in K^{p \times m}$  mit

$$\tilde{c}_{jk} = c_{kj} = \sum_{r=1}^n a_{kr} b_{rj} \quad \text{und} \quad \underbrace{\underbrace{B^T}_{\in K^{p \times n}} \underbrace{A^T}_{\in K^{n \times m}}}_{\in K^{p \times m}} \quad \text{hat Einträge} \quad (B^T A^T)_{ls} = \sum_{r=1}^n b_{rl} a_{sr} \\ = \sum_{r=1}^n a_{sr} b_{rl} = c_{sl}$$

### Folgerung

Für  $A \in K^{n \times n}$  invertierbar ist auch  $A^T$  invertierbar und es gilt  $(A^T)^{-1} = (A^{-1})^T$

### Beweis

$$(A^{-1})^T A^T = (A A^{-1})^T = I^T = I \quad \text{und} \quad A^T (A^{-1})^T = (A^{-1} A)^T = I^T = I$$

Daraus folgt:  $(A^T)^{-1} = (A^{-1})^T$  □

### Anmerkung

- $Q \in \mathbb{C}^{n \times n}$  mit  $Q$  invertierbar **unitär**, falls  $Q^{-1} = \overline{Q}^T$
- $Q \in \mathbb{R}^{n \times n}$  mit  $Q$  invertierbar heißt **orthogonal**, falls  $Q^{-1} = Q^T$ . „Orthogonal“ bedeutet: für zwei beliebige Zeilen oder Spalten  $q^j, q^k$  gilt:

$$(q^j)^T q^k = \delta_{jk} = \begin{cases} 1, & \text{falls } j = k \\ 0, & \text{sonst} \end{cases}$$

### Wichtige Anwendung

lineare Gleichungssysteme: gegeben:  $A \in K^{m \times n}, b \in K^m$   
 gesucht:  $x \in K^n$ , sodass  $Ax = b$

Zur Lösung: Gauß-Elimination, QR-Zerlegung