

# **Lineare Algebra I und II**

Skript zur Vorlesung von Prof. Dr. Carl-Friedrich Bödigheimer

Wintersemester 2014/2015, Sommersemester 2015

Stand: 17. April 2015

**Hinweis:**

Im Sommersemester (ab etwa Kapitel 5) wird dieses Skript erstellt von Jürgen Kanzler.

Fehler, Korrekturen oder sonstige Anmerkungen zum Skript können gern an [s6jukanz@uni-bonn.de](mailto:s6jukanz@uni-bonn.de) geschickt werden.

# Inhaltsverzeichnis

<b>1</b>	<b>Gleichungssysteme</b>	<b>7</b>
1.1	Rechnen im $\mathbb{R}^n$	7
1.1.1	Algebraische Aspekte	7
1.1.2	Geometrische Aspekte	8
1.1.3	Lineare Gleichungssysteme	9
1.1.4	Struktur der Lösungsmenge	10
1.1.5	Gauß-Algorithmus	11
<b>2</b>	<b>Körper und Vektorräume</b>	<b>13</b>
2.1	Körper	13
2.1.1	Körperaxiome und Unterkörper	13
2.1.2	Komplexe Zahlen	14
2.1.3	Endliche Körper	14
2.1.4	Inverse in $\mathbb{F}_p$	15
2.1.5	Charakteristik eines Körpers	15
2.2	Vektorräume	16
2.2.1	Vektorraumaxiome	16
2.2.2	Unterraum	17
2.2.3	Körperwechsel	18
2.3	Lineare Abbildungen	18
2.3.1	Morphismen	22
<b>3</b>	<b>Basen und Dimension</b>	<b>23</b>
3.1	Erzeugendensystem	23
3.2	Lineare Unabhängigkeit	24
3.3	Basen	25
3.4	Dimension	30
3.5	Prinzip der linearen Fortsetzung	32
3.6	Koordinaten	34
3.7	Isomorphieinvarianten	35
<b>4</b>	<b>Matrizen</b>	<b>40</b>
4.1	Rechnen mit Matrizen	40
4.2	Matrizen und lineare Abbildungen	44
4.3	Basiswechsel	48
4.4	Spaltenumformungen	50
4.5	Spezielle Matrizen	50
4.6	Normalformen	53
<b>5</b>	<b>Gruppen</b>	<b>54</b>
5.1	Symmetrische Gruppen	55
5.2	Untergruppen	56
5.3	Homomorphismen	59
5.3.1	Vorwärtsschichten/ Rückwärtsschichten von Gruppenstrukturen	62
5.3.2	Einige wichtige Isomorphismen	63
5.4	Produkte	64
5.5	Direkte Summen von Vektorräumen	65
5.5.1	Externe direkte Summe	65
5.5.2	Interne direkte Summe	66
5.6	Quotientenvektorräume	67
5.7	Normale Untergruppen	70

5.8 Quotientengruppen . . . . .	72
<b>6 Determinanten</b>	<b>76</b>
6.1 Einleitung . . . . .	76
6.2 Axiomatische Definition . . . . .	76
<b>Stichwortverzeichnis</b>	<b>80</b>



## Überblick

1. Lineare Gleichungssysteme
2. Vektorräume (und Körper)
3. Basen, Dimensionen, lineare Unabhängigkeit
4. Lineare Abbildungen und Matrizen
5. Gruppen, Ringe und Algebren
6. Determinanten
7. Eigenwerte und Eigenvektoren
8. Normalenform
9. Skalarprodukt
10. Hauptachsentransformationen

## Achtung:

Diese Version des Skriptes ist nicht vollständig korrigiert! Verbesserungsvorschläge, Rechtschreibfehler und inhaltliche Fehler dürfen gerne an [linaskript@tauradian.de](mailto:linaskript@tauradian.de) geschickt werden. Wir freuen uns über Rückmeldung!

## Vorwort

### Lineare Algebra:

- Theorie der linearen Gleichungssysteme
- Theorie der Vektorräume und linearen Abbildungen
- Theorie der Matrizen und Vektoren
- Unbekannte / Variablen  $x$  kommen nur zur ersten Potenz vor
- Keine gemischten Terme  $x_i \cdot x_j$

# 1 Gleichungssysteme

## 1.1 Rechnen im $\mathbb{R}^n$

### 1.1.1 Algebraische Aspekte

**Definition 1.1.1.** Grundkörper  $\mathbb{R} = \text{reelle Zahlen}$

**Definition 1.1.2.** Der  $\mathbb{R}^n = \mathbb{R} \times \dots \times \mathbb{R}$  besteht aus Elementen, die man sich auf zwei Weisen vorstellt:

- (i) Zahlentupel = Zeilenvektoren:  $x = (x_1, \dots, x_n)$
- $x_i =$  Einträge, Koordinaten, Komponenten  
z.B. Punkte im  $\mathbb{R}^3 : P = (x_1, x_2, x_3)$

- (ii) Spaltenvektoren:  $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

Für beide Auffassungen gibt es nun Operationen, wir notieren sie für einen Spaltenvektor:

- Addition:  $x + y = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$
- Skalierung:  $\lambda \in \mathbb{R} : \lambda \cdot x = \begin{pmatrix} \lambda \cdot x_1 \\ \vdots \\ \lambda \cdot x_n \end{pmatrix}$
- Nullvektor:  $0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

**Unterschied:** Wird bei der Matrizenmultiplikation deutlich werden.

### **Satz 1.1.3. Rechenregeln**

$$x + (y + z) = (x + y) + z$$

$$x + y = y + x$$

$$x + 0 = x$$

$$-x = (-1) \cdot x$$

$$\lambda(\mu x) = (\lambda\mu)x$$

$$(\lambda + \mu) \cdot x = \lambda x + \mu x$$

### **Definition 1.1.4. Skalarprodukt**

$$\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$$

Für  $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$  und  $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$  definiert man ein sogenanntes **Skalarprodukt**:  $(x, y) \mapsto \langle x, y \rangle :=$

$$x_1 y_1 + \dots + x_n y_n$$

$\langle x, y \rangle$  ist linear in  $x$  (bei festem  $y$ ) und linear in  $y$  (bei festem  $x$ ). Das nennt man bilinear.

**Satz 1.1.5. Rechenregeln**

$$\begin{aligned} \langle x, y \rangle &= \langle y, x \rangle \\ \langle x + x', y \rangle &= \langle x, y \rangle + \langle x', y \rangle \\ \langle x, y + y' \rangle &= \langle x, y \rangle + \langle x, y' \rangle \\ \langle 0, y \rangle &= 0 \\ \langle \lambda x, y \rangle &= \lambda \cdot \langle x, y \rangle \\ \langle x, \mu y \rangle &= \mu \cdot \langle x, y \rangle \\ (\forall y : \langle x, y \rangle = 0) &\implies x = 0 \end{aligned}$$

*Beweis.* Angenommen  $x \neq 0 \implies \exists i : x_i \neq 0$ .

Setze  $y = \begin{pmatrix} 0 \\ \vdots \\ i \\ \vdots \\ 0 \end{pmatrix}$ , also  $y_j = \begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases}$

Dann gilt  $0 = \langle x, y \rangle = x_i \cdot y_i = x_i$ . Widerspruch. □

Das waren algebraische Aspekte (unabhängig von  $\mathbb{R}$ , gilt in jedem Körper  $\mathbb{K}$  bzw. in seinem Spaltenvektorraum  $K^n$ )

**1.1.2 Geometrische Aspekte**

**Definition 1.1.6.**

- *Betrag:*  $\|x\| := \sqrt{\langle x, x \rangle} = \sqrt{x_1^2 + x_2^2 + \dots}$ . Diese Formel ist die Verallgemeinerung des Satzes des Pythagoras im  $\mathbb{R}^n$
- *Winkelmessung:*  $\cos(x, y) = \frac{\langle x, y \rangle}{\|x\| \cdot \|y\|}$ , ( $x, y \neq 0$ )

- *Matrix* = rechteckiges Zahlenschema  $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$

Der erste Index zählt die Zeilen, der zweite Index zählt die Spalten.

Spalte:  $S_j(A)$   $j$ -te Spalte

Zeile:  $Z_i(A)$   $i$ -te Zeile

- *Nullmatrix* alle Einträge 0
- *Skalierung* von Matrizen:  $\lambda \cdot A =$  jedes Element mit Lambda multiplizieren
- Addition, Subtraktion von Matrizen erfolgt komponentenweise:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

Die Matrix  $A \in \mathbb{R}^{mn}$  kann als Riesenspaltenvektor oder Riesenzeilenvektor oder Mittelweg mit  $n$  Spalten und  $m$  Zeilen aufgefasst werden.

Das Produkt einer  $(m \times n)$ -Matrix  $A$  mit einem Spaltenvektor  $x$  liefert einen neuen Spaltenvektor:

$$A \cdot x = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n \end{pmatrix}$$

**Satz 1.1.7.** Wir betrachten die Multiplikation mit einem festem  $A$  als Funktion als Funktion  $T_A : \mathbb{R}^n \rightarrow \mathbb{R}^m, x \mapsto Ax$ .

- $T_A(0) = 0$
- $T_A(\lambda x) = \lambda T_A(x)$
- $T_A(x' + x'') = T_A(x') + T_A(x'')$

### 1.1.3 Lineare Gleichungssysteme

**Definition 1.1.8.** Ein lineares Gleichungssystem (LGS) ist ein System von  $m$  Gleichungen in  $n$  Unbekannten  $x_1, \dots, x_n$  der Art:

$$\begin{array}{ll} (G_1) & a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ \vdots & \vdots \\ (G_m) & a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{array}$$

Die  $a_{ij}$  mit  $i = 1, \dots, m$  und  $j = 1, \dots, n$  heißen Koeffizienten die  $b_i = 1, \dots, m$  heißen Werte des LGS. Wichtig: alles ist durchnummeriert.

#### Kompakte Schreibweise

$A = (a_{ij}) =$  Matrix der Koeffizienten

$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} =$  Spaltenvektor der Unbekannten

$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} =$  Spaltenvektor der Werte

$A \cdot x = b$

#### Notation:

Gegeben  $A$  und  $b$

$(A|b) =$  erweiterte Matrix

**Definition 1.1.9.** Ein  $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ , der simultan alle Gleichungen löst, heißt Lösung des LGS.

$$\mathcal{L}(A|b) := x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n | Ax = b \subseteq \mathbb{R}^n$$

*Bemerkung.* 1.  $A \in \mathbb{R}^{n \times m}, x \in \mathbb{R}^n, b \in \mathbb{R}^m$

2. Alles ist durchnummeriert

3. Es ist möglich, dass alle Koeffizienten = 0 sind:  $A = 0$  ("triviales" LGS)

$$\mathcal{L}(0|b) = \begin{cases} \mathbb{R}^n, & b = 0 \\ \emptyset, & b \neq 0 \end{cases}$$

4. Es ist möglich, dass eine Zeile von  $A$  null ist.

$$b_j = 0 \implies \text{Diese Gleichung ist überflüssig, } b \neq 0 \implies \mathcal{L}(A|b) = \emptyset$$

5. Es kann sein, dass eine Spalte von  $A$  null ist

$$a_{1i} = a_{2i} = \dots = 0 \implies x_i \text{ "überflüssig"}$$

**Definition 1.1.10.** Ist  $b = 0$ , so heißt das LGS  $(A|0)$  homogen. Ist  $b \neq 0$  so heißt das LGS inhomogen.

*Bemerkung.* Was hat das alles mit  $T_A : \mathbb{R}^n \rightarrow \mathbb{R}^m$  zu tun?

$$x \mapsto y := A \cdot x$$

1.  $(A|b)$  hat eine Lösung (d.h.  $\mathcal{L}(A|b) \neq \emptyset$ ) genau dann, wenn  $b \in \text{Bild}(T_A) = T_A(\mathbb{R}^n) = \text{Wertemenge}$  gibt, es also ein  $x \in \mathbb{R}^n$  mit  $T_A(x) = b$  gibt.

2.  $0 \in \mathcal{L}(A|0)$  (d.h.  $\mathcal{L}(A|0) \neq \emptyset$ )

Ein homogenes System hat immer mindestens eine Lösung, nämlich die triviale Lösung  $x = 0$ .

### 1.1.4 Struktur der Lösungsmenge

**Satz 1.1.11.** (*homogener Fall*)

(i)  $(A|0)$  hat immer die triviale Lösung

(ii)  $x \in \mathcal{L}(A|0) \implies \lambda x \in \mathcal{L}(A|0)$

(iii)  $x, x' \in \mathcal{L}(A|0) \implies x + x' \in \mathcal{L}(A|0)$

**Satz 1.1.12.** (*inhomogener Fall*)

(i)  $x, x' \in \mathcal{L}(A|b) \implies x - x' \in \mathcal{L}(A|0)$

(ii) Sei  $\bar{x} \in \mathcal{L}(A|b)$

Dann gibt es zu jeder anderen Lösung  $x \in \mathcal{L}(A|b)$  genau eine Lösung  $\xi$  des homogenen Systems mit  $x = \bar{x} + \xi$

*Beweis.* (i)  $x, x' \in \mathcal{L}(A|b) \implies Ax = b, Ax' = b$

$$Ax - Ax' = b - b = 0$$

$$A(x - x') = 0$$

$$\text{Also } x - x' \in \mathcal{L}(A|0)$$

(ii) Es gilt  $A\bar{x} = b$

Ist  $x \in \mathcal{L}(A|b)$ , also  $Ax = b$ , so haben wir nach (i)  $x - \bar{x} = \xi \in \mathcal{L}(A|0)$

$$\text{Also: } x = \bar{x} + \xi$$

Und  $\xi$  ist eindeutig bestimmt:  $x - \bar{x} = \xi$

$$\begin{aligned} x - \bar{x} &= \xi' \\ \implies \xi &= \xi' \end{aligned}$$

□



1. Suche in den Spalten  $S_j(A)$  in der Reihenfolge  $j = q + 1, \dots, n$  einen Eintrag  $a_{ij} \neq 0$  in der Reihenfolge  $i = p + 1, \dots, m$ .
  - Gibt es kein solchen  $a_{ij}$ , so gehe zu ENDE.
  - Sei  $a_{ij} \neq 0$  mit  $j$  minimal unter  $q < j \leq n$  und  $i$  minimal unter  $p < i \leq m$
2. Vertausche Zeile  $i$  mit Zeile  $p + 1$
3. Subtrahiere von Zeile  $i + 1$  das  $\frac{a_{p+1,q}}{a_{p,q}}$ -fache der Zeile  $p$ .  
Subtrahiere von Zeile  $i + 2$  das  $\frac{a_{p+2,q}}{a_{p,q}}$ -fache der Zeile  $p$ .  
...  
Subtrahiere von Zeile  $m$  das  $\frac{a_{m,q}}{a_{p,q}}$ -fache der Zeile  $p$ .
4. Setze  $p \rightarrow p + 1, q \rightarrow j$ .
  - Ist  $p = m$  oder  $q = n$ , gehe zu ENDE
  - Sonst gehe zu 1.

ENDE.

Ausgabe:  $(A'|b')$  in Zeilenstufenform.

*Bemerkung.* Man nennt das  $a_{ij}$  in 1. ein Pivotelement .

**Satz 1.1.14.** *Jedes LGS  $(A|b)$  wird durch den Gauß-Algorithmus in ein äquivalentes LGS  $(A'|b')$  mit gleicher Lösungsmenge überführt.*

- Beweis.*
1. Zunächst ist offensichtlich, dass für  $A = 0$  das LGS  $(0|b)$  bereits in Zeilenstufenform ist, und zwar für die konstante Treppenfunktion  $\tau(0) = \tau(1) = \dots = \tau(n) = 0$ . Wie führen den Beweis durch Induktion über  $m$ .
  2. Für  $m = 1$  und  $A \neq 0$  sei  $a_{11} = \dots = a_{1j-1} = 0$  und  $a_{1j} \neq 0$ . Dann ist  $A$  bereits in Zeilenstufenform mit  $\tau(0) = \dots = \tau(j-1) = 0$  und  $\tau(j) = \dots = \tau(n) = 1$ .
  3. Für  $m > 1$  führt ein erster Durchlauf des Gauß-Algorithmus für  $A \neq 0$  an einem ersten Pivotelement  $a_{i_1 j_1} \neq 0$ . Nach Vertauschen und den Subtraktionen haben wir ein System und eine partiell definierte Treppenfunktion. Der zweite Durchlauf des Gauß-Algorithmus ist eigentlich ein erster Durchlauf auf das neue System. Dieses hat noch  $m - 1$  Zeilen. Nach Induktion wird es in Zeilenstufenform überführt.

□

# 2 Körper und Vektorräume

## 2.1 Körper

### 2.1.1 Körperaxiome und Unterkörper

**Definition 2.1.1.** Ein *Körper* ist eine Menge  $\mathbb{K}$  mit zwei Verknüpfungen  $+$  (Addition),  $\cdot$  (Multiplikation), die die folgenden Eigenschaften erfüllen:

- Addition  $\mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$ 
  1.  $a + (b + c) = (a + b) + c$  (Assoziativität)
  2.  $a + b = b + a$  (Kommutativität)
  3. Es gibt ein neutrales Element der Addition  $\tilde{x} \in \mathbb{K}$ , sodass für alle  $x \in \mathbb{K}$  gilt  $\tilde{x} + x = x$ . Dieses bezeichnen wir mit 0.
  4. Zu jedem Element  $x \in \mathbb{K}$  gibt es ein Element  $-x \in \mathbb{K}$ , sodass  $x + (-x) = 0$ . (Existenz von additiv Inversen)
- Multiplikation  $\mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$ 
  5.  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  (Assoziativität)
  6.  $a \cdot b = b \cdot a$  (Kommutativität)
  7. Es gibt ein neutrales Element der Multiplikation  $\tilde{x} \in \mathbb{K}$ , sodass für alle  $x \in \mathbb{K}$  gilt  $\tilde{x} \cdot x = x$ . Dieses Element bezeichnen wir mit 1.
  8. Zu jedem Element  $x \in \mathbb{K}$  gibt es ein Element  $x^{-1} \in \mathbb{K}$ , sodass  $x \cdot x^{-1} = 1$ . (Existenz von multiplikativ Inversen)
- Zusammenhang zwischen Addition und Multiplikation
  9.  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  (Distributivität)
  10.  $1 \neq 0$

**Definition 2.1.2.** Eine Teilmenge  $\mathbb{K}' \subseteq \mathbb{K}$  eines Körpers  $\mathbb{K}$  nennen wir *Unterkörper*, wenn sie die folgenden Eigenschaften erfüllt:

1.  $x, y \in \mathbb{K}' \Rightarrow x + y \in \mathbb{K}', x \cdot y \in \mathbb{K}'$  (Abgeschlossenheit bezüglich Addition und Multiplikation)
2.  $0, 1 \in \mathbb{K}'$
3.  $x \in \mathbb{K}' \Rightarrow -x \in \mathbb{K}'$
4.  $x \in \mathbb{K}' \Rightarrow x^{-1} \in \mathbb{K}'$

*Bemerkung.* Wie wir es aus der Schule gewohnt sind, schreiben wir vereinfachend  $x - y$  statt  $x + (-y)$  und  $\frac{x}{y}$  statt  $x \cdot y^{-1}$ . Dies sind jedoch erstmal nur Notationen, da wir keine Verknüpfung  $-$ , oder  $/$  definiert haben.

**Beispiel 2.1.3.** Beispiele für Körper, die uns allen geläufig sind sind die reellen Zahlen  $(\mathbb{R}, +, \cdot)$ , die rationalen Zahlen  $(\mathbb{Q}, +, \cdot)$ , oder auch die komplexen Zahlen  $(\mathbb{C}, +, \cdot)$ , welche wir im nächsten Abschnitt definieren werden. Ein Beispiel für einen Teilkörper von  $\mathbb{R}$ , der nicht der Körper rationalen Zahlen ist, ist  $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ , wobei  $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$

## 2.1.2 Komplexe Zahlen

**Definition 2.1.4.** Der Körper der *komplexen Zahlen*  $\mathbb{C}$  besteht aus der Menge  $\mathbb{R}^2$  zusammen mit den Verknüpfungen

- $(x, y) + (x', y') = (x + x', y + y')$
- $(x, y) \cdot (x', y') = (x \cdot x' - y \cdot y', x \cdot y' + x' \cdot y)$

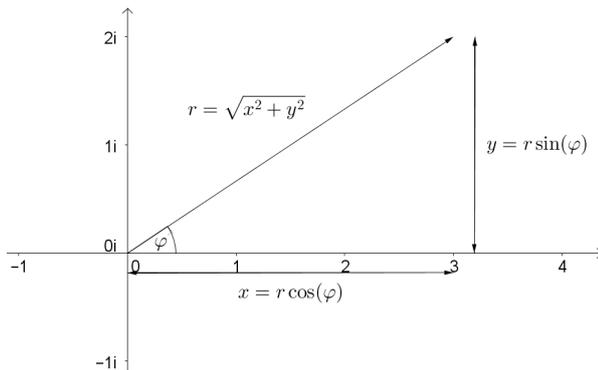
Es ist:

- $0_{\mathbb{C}} = (0, 0)$
- $1_{\mathbb{C}} = e_1 = (1, 0)$
- $-(x, y) = (-x, -y)$
- $(x, y)^{-1} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$

wie sich jeweils leicht nachrechnen lässt. Des weiteren stellen wir fest, dass  $(e_2)^2 = (0, 1)^2 = (-1, 0)$  und nennen  $e_2$  die *imaginäre Einheit*  $i$ . Wir schreiben  $(x, y) = x + iy$ .

Dass für Addition und Multiplikation die gewünschten Eigenschaften (Assoziativität, Kommutativität, Distributivität) gelten lässt sich leicht nachrechnen.

**Definition 2.1.5.**  $z = (x, y) \in \mathbb{C}$  kann als Zahl in der Gaußschen Zahlenebene interpretiert werden, die durch einen Winkel und eine Länge definiert ist.



mit  $0 \leq \varphi < 2\pi$  und  $r = \sqrt{x^2 + y^2}$  ist diese Darstellung eindeutig, wobei

$$\begin{aligned}x &= r \cos(\varphi) \\y &= r \sin(\varphi)\end{aligned}$$

$r$  und  $\varphi$  nennen wir die *Polarkoordinaten* von  $z$ . Wir schreiben  $z = (r; \phi)$

## 2.1.3 Endliche Körper

*Bemerkung.* Nachdem alle Körper, die uns bis hier hin begegnet sind unendlich viele Elemente hatten wollen wir nun versuchen zu einer Primzahl  $p$  einen Körper mit genau  $p$  Elementen, also einen endlichen Körper zu finden.

**Definition 2.1.6.** Man kann zeigen, dass es zu gegebenen  $n, z \in \mathbb{Z}, n > 1$  eindeutige Zahlen  $a, r \in \mathbb{Z}$  gibt mit  $0 \leq r < n$ , sodass  $z = an + r$ . Dies ist die Division durch  $n$  mit Rest  $r$ . Für ein gegebenes  $n$  wollen wir alle Zahlen als gleich auffassen, bei denen  $r$  gleich ist und sie in einer Menge zusammenfassen. Wir bezeichnen die Menge

$$[z] = \{z' \in \mathbb{Z} \mid z' = a'n + r, a' \in \mathbb{Z}\} = \{z' \in \mathbb{Z} \mid z' - z \text{ ohne Rest durch } n \text{ teilbar}\}$$

als die *Restklasse von  $z$  modulo  $n$* . Und nennen  $z' \in [z]$  *Repräsentant* der Restklasse.

### 2.1.4 Inverse in $\mathbb{F}_p$

**Satz 2.1.7.** Es seien  $a, b \in \mathbb{N}$  mit  $0 < b < a$ , dann gilt:

1. Der  $ggT(a, b)$  ist der letzte nicht verschwindende Rest  $r_n$  der folgenden Kette von Divisionen-mit-Rest

$$a = q_1 b + r_1 \quad \text{mit} \quad 0 \leq r_1 < b; q_1, r_1 \in \mathbb{N}$$

$$b = q_2 r_1 + r_2 \quad \text{mit} \quad 0 \leq r_2 < r_1; q_2, r_2 \in \mathbb{N}$$

$$r_1 = q_3 r_2 + r_3$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad \text{mit} \quad 0 \leq r_n < r_{n-1}; q_n, r_n \in \mathbb{N}$$

$$r_{n-1} = q_{n+1} r_n \quad \text{mit} \quad q_{n+1} \in \mathbb{N}$$

2. Es gibt  $\alpha, \beta \in \mathbb{Z}$  mit der Eigenschaft

$$ggT(a, b) = \alpha a + \beta b.$$

*Beweis.*

1. Da die  $r_i$  strikt fallend, denn  $b > r_1 > r_2 > \dots > r_n > r_{n+1} = 0$ , bricht der Algorithmus ab. Ist  $t \in \mathbb{Z}$  ein Teiler von  $a$  und  $b$ , so ist  $t$  auch Teiler von  $r_1$  und damit auch von  $r_2$  usw. bis schließlich  $r_n$ .

Umgekehrt gilt: Ist  $t$  Teiler von  $r_n$ , so auch von  $r_{n-1}, r_{n-2}$ , usw. bis  $a$  und  $b$ .

2. Löse die Gleichung rückwärts auf und setze ein. □

### 2.1.5 Charakteristik eines Körpers

Bisher konnte man den Eindruck gewinnen als läge  $\lambda \in \mathbb{N}$  in  $\mathbb{K}$ , da öfters schon so gerechnet wurde. Dies ist nicht so. Zwar gilt  $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ , aber  $\mathbb{N} \subset \mathbb{Z}$  sind keine Teilmenge von  $\mathbb{F}_p$ . Daher soll von jetzt an als Vereinbarung gelten, dass für  $n \in \mathbb{Z}$  und  $x \in \mathbb{K}$  gilt

$$nx := x + x + \dots + x \text{ (n-mal)}.$$

Dies ist also nicht die Multiplikation von Körperelementen. Nun das Ganze etwas genauer in folgender

**Definition 2.1.8.** Für jedes  $n \in \mathbb{Z}$  gilt:

$$\varepsilon_0 := 0$$

$$\varepsilon_1 := 1$$

$$\varepsilon_{n+1} := \varepsilon_n + 1 \quad (n \geq 1)$$

$$\varepsilon_n := -\varepsilon_{-n} \quad (n \leq -1)$$

Also

$$\varepsilon_n := n \cdot 1$$

**Definition 2.1.9.** Falls kein  $\varepsilon_n = 0$  mit  $n > 0$ , so hat  $\mathbb{K}$  die *Charakteristik* 0, und schreibt

$$\text{char}(\mathbb{K}) = 0.$$

Andernfalls nennt man das kleinste  $n \geq 1$  mit  $\varepsilon_n = 0$  die *Charakteristik* von  $\mathbb{K}$ , schreibe

$$\text{char}(\mathbb{K}) = n.$$

**Beispiel 2.1.10.** 1.  $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$

2.  $\text{char}(\mathbb{F}_p) = p$  ( $p$  ist eine Primzahl)

*Bemerkung.* Ist  $\text{char}(\mathbb{K}) = 0$ , so ist  $\mathbb{Q}$  ein Unterkörper.

Denn

$$\mathbb{Q} \longrightarrow \mathbb{K}$$

$$\frac{n}{m} \longmapsto \varepsilon_n \cdot \varepsilon_m^{-1},$$

so ergibt sich  $\varepsilon_a + \varepsilon_b = \varepsilon_{a+b}$  und  $\varepsilon_a \cdot \varepsilon_b = \varepsilon_{ab}$  und somit erhält man ein  $\mathbb{K}' = \{x - \varepsilon_n \cdot \varepsilon_m^{-1} \mid n, m \in \mathbb{Z} \wedge m \neq 0\}$  mit  $\varepsilon_0 = 0$  und  $\varepsilon_1 = 1$ .

**Definition 2.1.11.** Eine Funktion  $\phi : \mathbb{K} \rightarrow \mathbb{K}'$  zwischen zwei Körpern heißt *Körperhomomorphismus*, falls gilt

1.  $\phi(x + y) = \phi(x) + \phi(y)$
2.  $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$
3.  $\phi(0) = 0$  und damit auch  $\phi(-x) = -\phi(x)$
4.  $\phi(1) = 1$  und damit auch  $\phi(x^{-1}) = \phi(x)^{-1}$ , falls  $\phi$  injektiv und  $x \neq 0$

**Beispiel 2.1.12.**  $\mathbb{R} \hookrightarrow \mathbb{C}$  mit  $x \mapsto (x, 0)$  ist ein *Körperisomorphismus* auf einem Unterkörper.

**Satz 2.1.13.** Ist  $\text{char}(\mathbb{K}) > 0$ , so ist  $\text{char}(\mathbb{K})$  eine Primzahl.

*Beweis.* Sei  $\text{char}(\mathbb{K}) = n$  mit  $n > 0$  und  $n = a \cdot b$  mit  $a, b \in \mathbb{N}$  sowie  $1 < a, b < n$ . Das heißt  $n$  ist keine Primzahl. Dann wäre  $0 = \varepsilon_n = \varepsilon_a \cdot \varepsilon_b$  mit  $\varepsilon_a, \varepsilon_b \neq 0$  und somit gäbe es einen Nullteiler.  $\square$

## 2.2 Vektorräume

### 2.2.1 Vektorraumaxiome

Im folgenden Abschnitt ist mit  $\mathbb{K}$  immer ein Körper gemeint.

**Definition 2.2.1.** Ein *Vektorraum*  $V$  über  $\mathbb{K}$  ist eine Menge mit einer Verknüpfung und einer Operation.

**Addition:**

$$+ : V \times V \rightarrow V \text{ mit } (x, y) \mapsto x + y$$

**Skalierung:**

$$\cdot : \mathbb{K} \times V \rightarrow V \text{ mit } (\lambda, x) \mapsto \lambda \cdot x$$

mit den folgenden Eigenschaften:

1.  $\forall x, y \in V : x + y = y + x$
2.  $\forall x, y, z \in V : x + (y + z) = (x + y) + z$
3.  $\exists 0 \in V \forall x \in V : x + 0 = x = 0 + x$
4.  $\forall x \in V \exists -x : x + (-x) = 0 = (-x) + x$
5.  $\forall x \in V, \forall \lambda, \mu \in \mathbb{K} : \lambda \cdot (\mu \cdot x) = (\lambda \cdot \mu) \cdot x$
6.  $\forall x \in V : 1 \cdot x = x$
7.  $\forall \lambda \in \mathbb{K}, \forall x, y \in V : \lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$
8.  $\forall x \in V, \forall \lambda, \mu \in \mathbb{K} : (\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$

**Proposition 2.2.2.** 1.  $0 \cdot x = 0$

2.  $\lambda \cdot 0 = 0$

3.  $(-1) \cdot x = -x$

4.  $\forall \lambda \in \mathbb{K} \forall x \in V : \lambda \cdot x = 0 \implies \lambda = 0 \text{ oder } x = 0$

*Beweis.* Übungsaufgabe □

**Beispiel 2.2.3.**

1.  $\mathbb{K}^n$  mit  $n > 0$  ist ein Vektorraum. Denn die Addition ist definiert durch  $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix}$

und die Skalierung durch  $\lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda \cdot x_1 \\ \vdots \\ \lambda \cdot x_n \end{pmatrix}$ . Die Eigenschaften sind leicht nachzuprüfen.

2. Insbesondere ist  $\mathbb{K}^0 = \{0\}$  der *triviale* Vektorraum und  $\mathbb{K}^1$  Vektorraum über sich selbst.

3. Auch  $Mat_{m,n}(\mathbb{K})$  mit festem  $m, n \in \mathbb{N}$  ist ein Vektorraum. Auch hier lassen sich Addition und Skalierung sowie deren Eigenschaften leicht nachweisen.

*Bemerkung.* Vektorräume über  $\mathbb{Q}$ ,  $\mathbb{R}$  bzw.  $\mathbb{C}$  nennt man *rational*, *reell* bzw. *komplex*.

## 2.2.2 Unterraum

Sei  $V$  im Folgenden ein  $\mathbb{K}$ -Vektorraum.

**Definition 2.2.4.** Eine Teilmenge  $U \subset V$  heißt *Unterraum* von  $V$ , falls gilt

1.  $u, u' \in U \implies u + u' \in U$  (abgeschlossen unter der Addition)
2.  $\lambda \in \mathbb{K} u \in U \implies \lambda \cdot u \in U$  (abgeschlossen unter Skalierung)

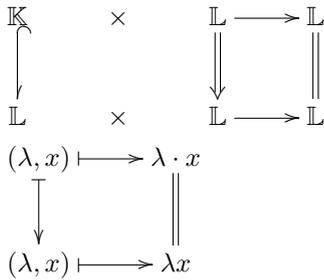
*Bemerkung.* Sei  $u \in U$  beliebig und  $\lambda = 0$ , dann folgt daraus  $0 \cdot u = 0 \in U$ .

**Beispiel 2.2.5.**

1.  $U = 0 = \{0\}$  ist Unterraum in jedem Vektorraum.
2.  $V = \mathbb{K}^n$ ,  $i = 1, \dots, n$   $U_i := \{x = (x_1, \dots, x_n) \in \mathbb{K}^n \mid x_i = 0\}$  ist Unterraum von  $V$ .  
 $U_I := \{x = (x_1, \dots, x_n) \in \mathbb{K}^n \mid x_i = 0 \text{ für } i \in I\}$   $I \subset 1, \dots, n$  ist Unterraum von  $V$ .
3.  $V = \mathbb{K}^n$   $U = \{x = (x_1, \dots, x_n) \in \mathbb{K}^n \mid x_1 + x_2 + \dots + x_n = 0\}$  ist Unterraum von  $V$ .
4.  $v \in V$   $U = \{tv \mid t \in \mathbb{K}\}$  ist Unterraum von  $V$ . Diesen Unterraum bezeichnet man auch als *Spann* bzw. *lineares Erzeugnis* von  $v$ . Manchmal nennt man ihn auch *lineare Hülle* von  $v$ . Doch dazu später mehr.
5. Sei  $u, v, w \in V$ , dann ist  $U = Span(u, v, w) = \{x = \lambda u + \mu v + \nu w \in V \mid \lambda, \mu, \nu \in \mathbb{K}\}$
6.  $(A|0)$  sei homogenes LGS und  $A \in Mat_{m,n}(\mathbb{K})$ , dann ist  $\mathbb{L}(A|0) \subset \mathbb{K}^n$  ein Unterraum.
7.  $U_1, U_2$  seien Unterräume von  $V$ , dann ist auch  $U = U_1 \cap U_2$  ein Unterraum von  $V$ . Allgemeiner:  
 $U_i \subset V \ i \in I \implies U := \bigcap_{i \in I} U_i$ .  $I$  muss nicht endlich sein. **Achtung!** Die Vereinigung von Unterräumen sind im Allgemeinen keine Unterräume mehr. Als einfaches Beispiel dafür dienen hier die beiden Koordinatenachsen des  $\mathbb{R}^2$  als Unterräume. Addiert man nämlich  $(1, 0)$  aus dem x-Achsen-Unterraum zu  $(0, 1)$  aus dem y-Achsen-Unterraum, so erhält man  $(1, 1)$ .  $(1, 1)$  liegt aber nicht in der Vereinigung von den beiden Koordinatenachsen. **Achtung!** Auch das mengenmäßige Komplement ist im Allgemeinen kein Unterraum. Das orthogonale Komplement allerdings schon.  
Denn sei  $V = \mathbb{R}^n$  und  $n = \begin{pmatrix} n_1 \\ \vdots \\ n_n \end{pmatrix}$ , dann ist  $U = \{x \in \mathbb{R}^n \mid x_1 n_1 + \dots + x_n n_n = 0\}$

8.

### 2.2.3 Körperwechsel



## 2.3 Lineare Abbildungen

Im folgenden bezeichne  $\mathbb{K}$  einen Körper;  $V$  und  $W$  seien Vektorräume über  $\mathbb{K}$  (Man sagt auch:  $\mathbb{K}$ -Vektorräume).

**Definition 2.3.1.** Eine Funktion  $f : V \rightarrow W$  ist eine *lineare Abbildung*, falls gilt:

- (i)  $f(0) = 0$
- (ii)  $f(x + y) = f(x) + f(y)$ , mit  $x, y \in V$
- (iii)  $f(\lambda x) = \lambda f(x)$ , mit  $\lambda \in \mathbb{K}, x \in V$ .

Hierbei folgt (i) offensichtlich aus (iii):  $f(0) = f(0 \cdot 0) = 0 \cdot f(0) = 0$ .

Lineare Abbildungen sind die zentralen Objekte der linearen Algebra; man könnte diese auch als Studium der linearen Abbildungen bezeichnen. Wir betrachten nun einige Beispiele:

- Beispiel 2.3.2.**
1. Die Multiplikation einer Matrix  $A$  mit einem Vektor  $x$ , wie wir sie bereits direkt zu Beginn eingeführt haben, ist eine lineare Abbildung:  $V = \mathbb{K}^n; W = \mathbb{K}^m; A \in \text{Mat}_{m,n}(\mathbb{K})$   
 $f = T_A : \mathbb{K}^n \rightarrow \mathbb{K}^m, x \mapsto A \cdot x$
  2. Für ein  $A \in \text{Mat}_{m,n}(\mathbb{K})$  haben wir ein lineares Gleichungssysteme studiert. Ein Ergebnis war  $W = \mathcal{L}(A|0) \subseteq \mathbb{K}^n$ , die Lösungsmenge im homogenen Fall ist ein Untervektorraum. Mit  $r = \text{rg}(A)$  und  $l = n - r$  erhalten wir die bekannte Parameterdarstellung des Lösungsraums als lineare Abbildung:

$$\begin{aligned}
 f : \mathbb{K}^l &\longrightarrow \mathcal{L}(A|0) \\
 u &\longmapsto L(u)
 \end{aligned}$$

Diese lineare Abbildung ist außerdem bijektiv. (Eine solche Abbildung nennt man auch *Isomorphismus*.)

3. Geometrische Beispiele: Drehung, Streckung, Scherung und Spiegelung im  $\mathbb{R}^2$  lassen sich als Matrizenmultiplikation darstellen und sind somit lineare Abbildungen.

$$f = T_A : \mathbb{R}^2 \rightarrow \mathbb{R}^2, x \mapsto A \cdot x$$

Die zur Drehung um  $\phi$  assoziierte Matrix ist

$$A = \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix}$$

Die Matrix zur Streckung um  $\lambda_1$  entlang der  $x$ -Achse und um  $\lambda_2$  entlang der  $y$ -Achse ist:

$$A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}; \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \lambda_1 \cdot x \\ \lambda_2 \cdot y \end{pmatrix}$$

Bei der Scherung bleibt eine Achse erhalten, in diesem Beispiel die  $x$ -Achse:

$$A = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}; \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ \alpha x + y \end{pmatrix}$$

Zur Spiegelung an der  $y$ -Achse betrachte man

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} -x \\ y \end{pmatrix}$$

die Spiegelung an der Winkelhalbierenden ist gegeben durch

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ x \end{pmatrix}$$

Auch die Projektion ist eine lineare Abbildung. Jeder Vektor  $v \in V = \mathbb{R}^2$  kann eindeutig geschrieben werden als  $v = w + w'$  mit  $w \in W$  und einem Vektor  $w'$ , der auf der Geraden liegt, die von  $\tilde{w}'$  aufgespannt wird. Die Projektion  $\pi : \mathbb{R}^2 = V \rightarrow W, w + w' = v \rightarrow w$  ist eine (surjektive!) lineare Abbildung.

#### 4. Analytische Beispiele

Auf dem Vektorraum  $V = C^{q+1}(\mathbb{R})$  der  $(q+1)$ -mal stetig differenzierbaren reellen Funktionen (mit der Addition  $(f+g)(x) := f(x) + g(x), f, g \in V$ ) ist die Ableitung eine lineare Abbildung:

$$D : C^{q+1}(\mathbb{R}) \longrightarrow C^q(\mathbb{R}) \\ f \mapsto f'$$

Hierbei bezeichnet  $f'(x) = \frac{d}{dx}f(x)$  die Ableitung von  $f$  nach  $x$ . Wegen der bekannten Ableitungsregeln, dass die Ableitung der Summe gleich der Summe der Ableitungen ist, und dass die Ableitung einer skalierten Funktion gleich der skalierten Ableitung ist, sind Ableitungen lineare Abbildungen. Insbesondere gilt für beliebig oft differenzierbare Funktionen ( $q = \infty$ ):

$$D : C^\infty(\mathbb{R}) \longrightarrow C^\infty(\mathbb{R}) \\ f \mapsto f'$$

Auf dem Vektorraum  $V = L^1([0, 1])$  der über  $[0, 1]$  integrierbaren Funktionen ist die Integration eine lineare Abbildung.

$$I : L^1([0, 1]) \longrightarrow \mathbb{R} \\ f \mapsto \int_b^a f(x) dx$$

mit  $a, b \in [0, 1]$ . Hier gilt die analoge Regel, dass das Integral einer Summe gleich der Summe der Integrale ist.

Betrachten wir als letztes Beispiel  $V = \mathcal{F}_{konv}$ , den Vektorraum der reellen konvergenten Folgen  $a = (a_0, a_1, \dots)$ . Die Grenzwertbildung ist eine lineare Abbildung:

$$\lim : V = \mathcal{F}_{konv} \longrightarrow \mathbb{R} \\ a = (a_n) = (a_0, a_1, \dots) \mapsto \lim_{n \rightarrow \infty} a_n$$

Die Summe zweier konvergenter Folgen ist wieder eine konvergente Folge, also ist die Grenzwertbildung eine lineare Abbildung:

$$(a_n) \mapsto \lim a_n, b_n \mapsto \lim b_n \\ (a_n) + (b_n) \mapsto \lim a_n + \lim b_n.$$

**Proposition 2.3.3.** *Es seien  $U, V, W$  Vektorräume über  $\mathbb{K}$ , dann gilt:*

- (i) Die Identität  $\text{id}_V : V \rightarrow V, x \mapsto x$  ist linear.
- (ii) Sind  $f : U \rightarrow V$  und  $g : V \rightarrow W$  lineare Abbildungen, dann auch die Verknüpfung  $g \circ f : U \rightarrow W$ .
- (iii) Die Nullabbildung  $0 : V \rightarrow W, x \mapsto 0$  ist eine lineare Abbildung.
- (iv) Sind  $f, f'$  lineare Abbildungen, dann ist auch  $\lambda f$ , definiert durch  $(\lambda f)(x) = \lambda f(x)$ , mit  $\lambda \in \mathbb{K}$ , wieder eine lineare Abbildung.

(v) Genauso ist auch  $f + f'$  mit  $(f + f')(x) = f(x) + f'(x)$  eine lineare Abbildung. Beides folgt einfach aus der Tatsache, dass  $f$  und  $f'$  lineare Abbildungen sind ( $f'$  ist nicht die Ableitung von  $f$ !).

(vi) Sei  $f : V \rightarrow W$  eine lineare bijektive Abbildung. Dann ist auch die Umkehrabbildung  $f^{-1} : W \rightarrow V$  linear.

*Beweis von Proposition (vi).* Zu zeigen:  $f^{-1}(x + y) = f^{-1}(x) + f^{-1}(y)$ . Seien  $x, y \in W$ . Da  $f$  bijektiv ist gilt:  $\exists! x', y' \in V : x = f(x'), y = f(y')$ ; „ $\exists!$ “ bedeutet „es gibt eindeutig“. Dann folgt mit der Linearität von  $f$ :

$$f^{-1}(x + y) = f^{-1}(f(x') + f(y')) = f^{-1}(f(x' + y')) = x' + y' = f^{-1}(x) + f^{-1}(y)$$

Damit haben wir die Bedingung (ii) aus Definition 2.3.1 verifiziert. Wir zeigen nun Bedingung (iii): Sei  $\lambda \in \mathbb{K}$ . Zu zeigen:  $f^{-1}(\lambda x) = \lambda f^{-1}(x)$ . Auch dies folgt mit  $x'$  wie oben aus der Linearität von  $f$ :

$$f^{-1}(\lambda x) = f^{-1}(\lambda f(x')) = f^{-1}(f(\lambda x')) = \lambda x' = \lambda f^{-1}(x)$$

□

**Definition 2.3.4.** Sei  $f : V \rightarrow W$  eine lineare Abbildung zwischen zwei Vektorräumen.

- (i) Die Teilmenge von  $W$   $\text{im}(f) = f(V) := \{x \in W \mid x = f(x') \text{ für } x' \in V\} \subseteq W$  heißt *Bild von  $f$*  (engl. *image*).
- (ii) Die Teilmenge von  $V$   $\text{ker}(f) = f^{-1}(0) := \{x \in V \mid f(x) = 0\} \subseteq V$  heißt *Kern von  $f$*  (engl. *kernel*).

**Proposition 2.3.5.** Sei  $f : V \rightarrow W$  eine lineare Abbildung zwischen zwei Vektorräumen.

- (i) Das Bild  $\text{im}(f)$  ist ein Untervektorraum in  $W$ .
- (ii) Der Kern  $\text{ker}(f)$  ist ein Untervektorraum in  $V$ .
- (iii) Ist  $b \in \text{im}(f)$  und etwa  $f(\xi) = b$ , so ist  $f^{-1}(b)$  ein affiner Unterraum und zwar  $f^{-1}(b) = \text{ker}(f) + \xi$ .

Ein Spezialfall von (iii) ist, dass die Lösungsmenge eines linearen Gleichungssystems im inhomogenen Fall ein affiner Unterraum ist.

*Beweis.* (i) Seien  $x, y \in \text{im}(f)$ , sodass  $x = f(x'), y = f(y')$  für  $x', y' \in V$ . Daraus folgt, dass  $x + y = f(x') + f(y') = f(x' + y')$ . Also liegt  $x + y$  im Bild von  $f$ .

(ii) Seien  $x, y \in V$  mit  $f(x) = f(y) = 0$ , also  $x, y \in \text{ker}(f)$ . Dann gilt  $f(x + y) = f(x) + f(y) = 0$ . Damit liegt auch  $x + y$  im Kern von  $f$ .

(iii) Sei  $b \in \text{im}(f)$  mit  $f(\xi) = b$ . Für  $x \in V$  mit  $f(x) = b$  gilt:

$$f(x - \xi) = f(x) - f(\xi) = b - b = 0$$

Also liegt  $x - \xi$  im Kern von  $f$ .

□

**Beispiel 2.3.6.** Betrachten wir wieder die Matrizenmultiplikation:  $f = T_A : \mathbb{K}^n \rightarrow \mathbb{K}^m, x \mapsto T_A(x) = A \cdot x$  mit  $A \in \text{Mat}_{m,n}(\mathbb{K})$ .

- $\text{ker}(T_A) = T_A^{-1}(0) = \mathcal{L}(A|0)$ . Der Kern ist der Lösungsraum des assoziierten linearen Gleichungssystems im homogenen Fall.
- $\text{im}(T_A) = \{b \in \mathbb{K}^m \mid \mathcal{L}(A|b) \neq \emptyset\}$ . Das Bild ist die Menge der Vektoren, für die das assoziierte lineare Gleichungssystem im inhomogenen Fall lösbar ist.
- Falls  $b \in \text{im}(T_A)$  mit etwa  $T_A(\xi) = b$ , so ist  $T_A^{-1}(b) = \mathcal{L}(A|b) = \mathcal{L}(A|0) + \xi$ , der Lösungsraum des inhomogenen und lösbaren Falls.

**Beispiel 2.3.7.** Die *komplexe Konjugation*  $\bar{\phantom{x}}$  ist ein Beispiel für eine Abbildung, die  $\mathbb{R}$ -linear, aber nicht  $\mathbb{C}$ -linear ist.

$$\begin{aligned} \bar{\phantom{x}} : \mathbb{C} &\rightarrow \mathbb{C} \\ z = x + iy &\mapsto \bar{z} = x - iy \end{aligned}$$

Die komplexe Konjugation  $\bar{\phantom{x}}$  ist ein Körperisomorphismus, denn

$$\bar{0} = 0; \bar{1} = 1; \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2; \overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2 \text{ (Multiplikativität).}$$

$\mathbb{C}$ -Linearität würde bedeuten  $\overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2$ . Die Abbildung kann also nicht sowohl ein Körperisomorphismus sein als auch  $\mathbb{C}$ -linear. Da die komplexe Konjugation multiplikativ ist, ist sie lediglich  $\mathbb{R}$ -linear:

$$\overline{\lambda z} = \lambda \bar{z} \Leftrightarrow \lambda = \bar{\lambda} \Leftrightarrow \lambda \in \mathbb{R} = \text{Fix}(\bar{\phantom{x}})$$

**Definition 2.3.8.** Seien  $V, W$  Vektorräume über  $\mathbb{K}$ . Eine Funktion  $f : V \rightarrow W$  heißt *affin*, falls es eine lineare Abbildung  $\varphi : V \rightarrow W$  gibt, und ein  $b \in W$  mit  $f(x) = \varphi(x) + b$ .

**Beispiel 2.3.9.**

1. Die Translation  $\tau_b : W \rightarrow W$  mit  $0 \neq b \in W, w \mapsto w + b$  ist immer eine affine Abbildung
2. Die Abbildung  $f(x) = mx + b$  mit  $m \in \mathbb{K}$  ist eine affine Abbildung. *Achtung!*: In der Schule und der Analysis werde solche Funktionen als lineare Funktionen bezeichnet. In der linearen Algebra sind dies aber im allgemeinen affine Funktionen!
3. Wir betrachten die Parameterdarstellung der Lösungsmenge  $\mathcal{L}(A|b)$  eines Linearen Gleichungssystems  $(A|b)$  der Größe  $m \times n$ , wobei  $A \in \text{Mat}_{m,n}(\mathbb{K}), b \in \mathbb{K}^n, r = \text{rg}(A), l = n - r$   
Es sei  $L^0$  die Parameterdarstellung für den homogenen Fall, also

$$L^0 : \mathbb{R}^l \rightarrow \mathcal{L}(A|b); U = (U_0, U_1, \dots, U_r) \mapsto L^0(U) = (U_0, L_1, U_1, L_2, U_2, \dots, L_r, U_r)$$

wobei  $L_1 = L_1(U_1, U_2, \dots, U_r), L_2 = L_2(U_2, U_3, \dots, U_r), \dots, L_r = L_r(U_r)$  Nun suchen wir uns irgend eine Lösung  $\xi \in \mathcal{L}A|b$  des inhomogenen Gleichungssystems. Für den Lösungsraum des inhomogenen Gleichungssystems gilt nun:

$$L = L^0 + \xi; L(U) = L^0(U) + \xi$$

4. Es sei  $f$  eine affine Abbildung. Offenbar ist  $f(0) = b$  die Translationskonstante, während  $f(x) - b = \Phi(x)$  der so genannte lineare Anteil ist. Damit hat man für affine Abbildungen folgende Gleichungen:

$$\begin{aligned} f(\lambda x) - b &= \lambda(f(x) - b) \\ f(x + y) - b &= (f(x) - b) + (f(y) - b) = f(x) + f(y) - 2b \end{aligned}$$

5. Ist  $f$  eine lineare Abbildung, so ist  $\text{Im}(f) \subseteq W$  ein linearer Unterraum.  
Ist  $f$  eine affine Abbildung, so ist  $\text{Im}(f) \subseteq W$  ein affiner Unterraum.

**Proposition 2.3.10.** Es sei  $\mathbb{K} \subseteq \mathbb{L}$  ein Unterkörper von  $\mathbb{L}$  (genau wie  $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ ) und  $V$  ein Vektorraum über  $\mathbb{L}$ . Wir wissen, dass  $V$  dann auch ein  $\mathbb{K}$ -Vektorraum ist. Es kommt aber vor, dass eine Funktion  $f : V \rightarrow W$  zwar linear ist, wenn man  $V$  als  $\mathbb{K}$ -Vektorraum betrachtet, es jedoch nicht ist, wenn man  $V$  als  $\mathbb{L}$ -Vektorraum betrachtet.

**Beispiel 2.3.11.** Ein Beispiel für die eben genannten Funktionen ist die komplexe Konjugation über  $\mathbb{R}$  und  $\mathbb{C}$ .

$$\bar{\phantom{x}} : \mathbb{C} \rightarrow \mathbb{C}; x + iy = z \mapsto \bar{z} = x - iy$$

Diese Abbildung ist  $\mathbb{R}$ -Linear, da man leicht nachrechnen kann, dass  $\lambda(x, y) \mapsto (x, -y)$ . Sie ist jedoch nicht  $\mathbb{C}$ -Linear, wie man leicht am Beispiel der Multiplikation mit  $i$  sieht. Es ist:

$$i \cdot \overline{(x, y)} = i \cdot (x, -y) = (x, y) \neq (-x, -y) = \overline{(-y, x)} = \overline{i \cdot (x, y)}$$

Abgesehen von der Linearität bei Multiplikation mit einer komplexen Zahl besitzt die komplexe Konjugation aber viele nützliche Eigenschaften. Für  $z_1, z_2 \in \mathbb{C}$  gilt nämlich

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$$

$$\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$$

$$\overline{0} = 0, \overline{1} = 1$$

$$z^{-1} = \frac{\overline{z}}{|z|^2}$$

### 2.3.1 Morphismen

**Definition 2.3.12.** Es sei  $f : V \rightarrow W$  eine lineare Abbildung, dann heißt  $f$

Monomorphismus, wenn  $f$  injektiv

Epimorphismus, wenn  $f$  surjektiv

Isomorphismus, wenn  $f$  bijektiv Endomorphismus, wenn  $V = W$  Automorphismus, wenn  $V = W$ ,  $f$  bijektiv

**Proposition 2.3.13.** *Es seien  $f : V \rightarrow W$ ,  $g : W \rightarrow U$  linear. Dann gilt*

- $f$  ist ein Monomorphismus  $\Leftrightarrow \ker(f) = 0$
- $g \circ f$  ist ein Monomorphismus  $\Leftrightarrow f$  ist ein Monomorphismus
- $g \circ f$  ist ein Epimorphismus  $\Leftrightarrow f$  ist ein Epimorphismus

# 3 Basen und Dimension

## 3.1 Erzeugendensystem

**Definition 3.1.1.** Es sei  $V$  ein  $\mathbb{K}$ -Vektorraum,  $v, e_1, e_2, \dots, e_n \in V$ ,  $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{K}$  und

$$v = \lambda_1 e_1 + \dots + \lambda_n e_n \tag{*}$$

Wir nennen (\*) eine Linearkombination (der  $e_1, \dots, e_n$  über  $\mathbb{K}$ ), oder eine lineare Darstellung von  $v$  (durch  $e_1, \dots, e_n$  über  $\mathbb{K}$ ). Ist  $v = 0$ , so nennt man (\*) eine lineare Relation zwischen den  $e_1, \dots, e_n$  (über  $\mathbb{K}$ ). Sind alle  $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$ , so nennt man (\*) eine triviale Linearkombination, oder triviale Darstellung von  $v = 0$ , oder eine triviale Relation.

**Definition 3.1.2.** Es sei  $\xi \subseteq V$  eine Teilmenge von  $V$ . Dann heißt

$$Span(\xi) := \{v \in V \mid \text{Es gibt endlich viele } e_1, \dots, e_n \in \xi \text{ und } \lambda_1, \dots, \lambda_n \in \mathbb{K} \text{ so dass } v = \lambda_1 e_1 + \dots + \lambda_n e_n\}$$

Der Spann, oder das lineare Erzeugnis von  $\xi$  in  $V$ . Wir vereinbaren, dass  $Span(\emptyset) = \{0\} = 0$ .

**Beispiel 3.1.3.** 1. Ist  $\xi = \{0\}$ , so ist  $Span(\xi) = 0$

2. Ist  $u \in V, \neq 0$ , so ist  $Span(\{u\})$  die von  $u$  aufgespannte Gerade.

3. Sind  $u_1, u_2 \neq 0$  nicht kollinear, also weder  $u_1 \in Span(u_2)$  noch  $u_2 \in Span(u_1)$ , so ist  $Span(u_1, u_2)$  eine Ebene.

4. Ist  $V = \mathbb{K}^n$ , so nennen wir  $e_i = (0, 0, \dots, \underset{i\text{-te Stelle}}{1}, \dots, 0)$  den  $i$ -ten Einheitsvektor. Für  $0 \leq m \leq n$  ist  $\xi_m = \{e_1, \dots, e_m\}$  und  $Span(\xi_m) = \mathbb{K}^m \subseteq \mathbb{K}^n$ , wobei einfach die letzten  $n - m$  Koordinaten 0 sind.

5. Ist  $V = \mathbb{R}, \mathbb{K} = \mathbb{Q}, \xi = \{1, \sqrt{2}\}$ , so ist  $Span(\xi) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{2}]$

6. Sind  $U_i \subseteq V, i \in I$  Untervektorräume eines Vektorraumes  $V$  und ist  $\xi = \bigcup_{i \in I} U_i$ , so nennen wir  $Span(\xi) = \bigoplus_{i \in I} U_i$  die Interne Summe der  $U_i$

**Proposition 3.1.4.** Es Sei  $\xi \subseteq V$  eine Teilmenge von  $V$

1.  $0 \in Span(\xi)$
2.  $\xi \subseteq Span(\xi)$  insbesondere ist  $Span(V) = V$
3.  $Span(U) = U$ , falls  $U$  ein UVR ist
4.  $Span(Span(U)) = Span(U)$
5.  $Span(\xi)$  ist der kleinste UVR von  $V$ , der  $\xi$  enthält.
6.  $Span(\xi)$  ist der Durchschnitt aller UVR von  $V$  welche  $\xi$  enthalten.

**Definition 3.1.5.** Eine Teilmenge  $\mathcal{E}$  heißt Erzeugendensystem von  $V$ , falls gilt:  $Span(\mathcal{E}) = V$ .  $V$  heißt endlich erzeugt, falls es ein endliches Erzeugendensystem gibt.

Uns interessiert dabei jedoch nur das kleinste Erzeugendensystem, beziehungsweise das minimale Erzeugendensystem.

**Lemma 3.1.6.** Ist  $\mathcal{E}$  ein EZS von  $V$  und  $0 \neq \lambda \in \mathbb{K}, e \in \mathcal{E}$ , dann ist auch  $\mathcal{E}' = (\mathcal{E} - \{e\}) \cup \{\lambda \cdot e\}$  mit  $\mathcal{E} = \{e_1, \dots, e_i, \dots\}$   
 $\Downarrow \mathfrak{M}_i[\lambda]$   
 $\mathcal{E}' = \{e_1, \dots, \lambda e_i, \dots\}$

### 3.2. Lineare Unabhängigkeit

*Beweis.*  $v = \lambda_1 e_1 + \dots + \lambda_n e_n$   
 $v = \lambda_1 e_1 + \dots + \frac{\lambda_i}{\lambda} \lambda_i e_i + \dots + \lambda_n e_n$

□

**Lemma 3.1.7.** Sei  $\mathcal{E} = \{e_1, e_2, \dots, e_i, \dots, e_j, \dots\}$  ein EZS. Dann ist  $\mathcal{E}' = (\mathcal{E} - \{e_i\}) \cup \{e_i + e_j\}$  wieder ein EZS.

$\mathcal{E} = \{e_1, \dots, e_i, \dots, e_j, \dots\}$   
 $\Downarrow \mathfrak{A}_j$   
 $\mathcal{E}' = \{e_1, \dots, e_i + e_j, \dots, e_j, \dots\}$

*Beweis.*  $v = \lambda_1 e_1 + \dots + \lambda_i e_i + \dots + \lambda_n e_n$   
 $= \lambda_1 e_1 + \dots + \lambda_i (e_i + e_j) + \dots + (\lambda_j - \lambda_i) e_j + \dots + \lambda_n e_n$

□

**Lemma 3.1.8.** Sei  $\mathcal{E}$  ein EZS von  $V$ . Es gäbe in  $\mathcal{E}$  eine nicht-triviale Relation, dh. es gibt  $e_i, \dots, e_n \in \mathcal{E}, \lambda_1, \dots, \lambda_n \in \mathbb{K}$  wobei nicht alle  $\lambda_i = 0$  und es gelte  $0 = \lambda_1 e_1 + \dots + \lambda_i e_i + \dots + \lambda_n e_n$  und etwa  $\lambda_i \neq 0$ . Dann ist  $\mathcal{E}' = \mathcal{E} - \{e_i\}$  wieder ein EZS von  $V$ .

*Beweis.* Es gilt:

$e_i = -\frac{1}{\lambda_i} (\lambda_1 e_1 + \dots + \lambda_i \hat{e}_i + \dots + \lambda_n e_n)$

$[*] = -\frac{1}{\lambda_i} (\lambda_1 e_1 + \dots + \lambda_{i-1} e_{i-1} + \lambda_{i+1} e_{i+1} + \dots + \lambda_n e_n)$

d.h.  $e_i \in \text{Span}(\mathcal{E}) = \text{Span}(\mathcal{E} - e_i)$

Also: wenn immer  $e_i$  in einer Darstellung eines  $v \in V$  vorkommt gilt:

$v = \alpha_{i_1} e_{i_1} + \dots + \alpha_{i_k} e_{i_k} + \dots + \alpha_{i_m} e_{i_m}$   
 $\Downarrow$   
 $= \alpha_{i_1} e_{i_1} + \dots + \alpha[*] + \dots + \alpha_{i_m} e_{i_m}$

□

## 3.2 Lineare Unabhängigkeit

$V =$  Vektorraum über  $\mathbb{K}$

$\mathcal{B} \subseteq V$  Teilmenge

**Definition 3.2.1.**  $\mathcal{B}$  heißt *linear unabhängig* in  $V$ , falls gilt:

$b_1, \dots, b_n \in \mathcal{B}$  sind paarweise verschieden und  $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ .

Wenn  $\lambda_1 b_1 + \dots + \lambda_n b_n = 0$  gilt, dann nur deshalb, weil  $\lambda_1 = \dots = \lambda_n = 0$ .

*Bemerkung.*  $\mathbb{B}$  ist NICHT "von" etwas unabhängig! Es IST linear unabhängig.

*Bemerkung.* Oder: Jedes  $b$  ist VON ALLEN ANDEREN linear unabhängig.

( $\Leftrightarrow b$  kann nicht als Linearkombination der anderen geschrieben werden  $\Leftrightarrow b \notin \text{Span}(\mathcal{B}, \{b\})$ )

*Bemerkung.* Man sagt: Es gibt keine nicht-triviale Relation unter den Elementen von  $\mathcal{B}$ .

*Bemerkung.* Die Eigenschaft linearer Unabhängigkeit kommt in der Menge  $\mathcal{B}$  vor, nicht in ihren Elementen.

*Bemerkung.*  $v$  ist linear unabhängig von  $\mathcal{B} \Leftrightarrow v \notin \text{Span}(\mathcal{B})$ .

$v$  ist linear abhängig von  $\mathcal{B} \Leftrightarrow v \in \text{Span}(\mathcal{B})$ .

*Bemerkung.*  $0 \notin \mathcal{B}$ , falls  $\mathcal{B}$  linear unabhängig.

Denn sonst  $0 = \lambda \cdot 0, \lambda \neq 0$  z.B. für  $\lambda = 1$

*Bemerkung.* Wir setzen  $\mathcal{B} = \emptyset$  ist linear unabhängig.

**Beispiel 3.2.2.**  $\mathcal{B} = \{b\}$  ist linear unabhängig  $\Leftrightarrow b \neq 0$ . Jede Relation müsste lauten  $\lambda \cdot b = 0$

**Beispiel 3.2.3.**  $\mathcal{B} = \{b_1, b_2\}$  ist linear unabhängig  $\Leftrightarrow b_1, b_2 \neq 0$  mit  $b_1, b_2$  nicht kollinear

$b_1 = \lambda_2 b_2$

$b_2 = \lambda_1 b_1$

Beides ist nicht möglich, da  $\mu_1 b_1 + \mu_2 b_2 = 0$

**Beispiel 3.2.4.**  $V = \mathbb{K}$ ,  $\mathcal{B} = \{e_1, \dots, e_m\}$ ,  $m \leq n$ , Standardeinheitsvektoren  $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ , wobei 1 an  $i$ -ter Stelle steht.  
 $\mathcal{B}$  ist linear unabhängig.

Angenommen  $\lambda_1 e_1 + \dots + \lambda_m e_m = 0 \Rightarrow \lambda_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \dots + \lambda_m \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 0$

- 1. Koordinate  
 $\lambda_1 \cdot 1 + \lambda_2 \cdot 0 + \dots + \lambda_m \cdot 0 = 0 \Rightarrow \lambda_1 = 0$
- 2. Koordinate  
 $\lambda_1 \cdot 0 + \lambda_2 \cdot 1 + \dots + \lambda_m \cdot 0 = 0 \Rightarrow \lambda_2 = 0$
- $\vdots$
- m. Koordinate  
 $\lambda_1 \cdot 0 + \dots + \lambda_m \cdot 1 = 0 \Rightarrow \lambda_m = 0$

**Satz 3.2.5.**  $\mathcal{B} \subset V$  ist genau dann linear unabhängig, wenn jedes  $v \in \text{Span}(\mathcal{B})$  genau eine (oder eine eindeutige) Darstellung als Linearkombination besitzt.  
 $v = \lambda_1 b_1 + \dots + \lambda_n b_n$  für ein geeignetes  $b_1, \dots, b_n \in \mathcal{B}$ , und  $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ .

*Beweis.* Angenommen wir hätten zwei Darstellungen

$$v = \lambda_{i_1} b_{i_1} + \dots + \lambda_{i_n} b_{i_n}$$

$$v = \lambda_{j_1} b_{j_1} + \dots + \lambda_{j_m} b_{j_m}$$

Dann gilt:

$$0 = v - v = \lambda_{i_1} b_{i_1} + \dots + \lambda_{i_n} b_{i_n} - \lambda_{j_1} b_{j_1} + \dots + \lambda_{j_m} b_{j_m}$$

Wir fassen zusammen und kürzen weg. Deshalb können wir folgendes annehmen:

alle  $b_{i_r}$  und  $b_{j_r}$  sind paarweise verschieden und alle  $\lambda_{i_r}$  und  $\lambda_{j_r} \neq 0$

Sind die Darstellungen verschieden, so gibt es mindestens ein  $b_{i_k} = b_{j_l}$ , aber  $\lambda_{i_k} \neq \lambda_{j_l}$ .

Dann ist die rechte Seite eine nicht triviale Relation. Aber  $\mathcal{B}$  war als linear unabhängig angenommen.

Widerspruch! □

$$V = P_n(\mathbb{K}) \ni p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

$a_i \in \mathbb{K}$   $p'(x) := a_1 + 2a_2 x + \dots + n a_n x^{n-1}$  ist die formale Ableitung

$$W = P_{n-1}(\mathbb{K}) \qquad P_\infty(\mathbb{K}) = \mathbb{K}[x]$$

$$\qquad \qquad \qquad P_\infty(\mathbb{K}) = \mathbb{K}[x]$$

$\mathcal{B} = \{1, x, x^2, \dots, x^n\} \subseteq P_n(\mathbb{K})$  sind Stammpolynome.  $\mathcal{B}$  ist ein EZS und linear unabhängig.

### 3.3 Basen

**Definition 3.3.1.** Eine Teilmenge  $\mathcal{B} \subseteq V$  eines VR-V über  $\mathbb{K}$  heißt *Basis von V*, falls  $\mathcal{B}$  ein EZS und linear unabhängig ist.

*Bemerkung.* Eine Basis ist ein minimales EZS und ein maximales linear unabhängiges System.

**Beispiel 3.3.2.**  $V = \mathbb{K}^n$ ,  $\mathcal{B} = \{e_1, \dots, e_n\}$

**Beispiel 3.3.3.**  $V = P(\mathbb{K}) : \mathcal{B} = 1, x, x^2, \dots, x^n$

$$V = \mathbb{C}/\mathbb{C} \quad \mathcal{B} = \{1\}$$

$$V = \mathbb{C}/\mathbb{R} \quad \mathcal{B} = \{e_1, e_2\}$$

$$V = \mathbb{C}/\mathbb{K} = \mathbb{Q} \quad \mathcal{B} = ?$$

$\mathcal{B} = \{\log 2, \log 3, \log 5, \dots\}$  ist ein EZS und somit linear unabhängig.

**Beispiel 3.3.4.** Anwendung:  $(A | 0) =$  homogenes LGS,  $m \times n$  über  $\mathbb{K}$

Annahme: Die Matrix ist bereits in ZSF

$$\begin{pmatrix} 0 & 0 & * & \dots & \dots & \dots & \dots & \dots & \dots & * \\ 0 & * & * & \dots & \dots & \dots & \dots & \dots & \dots & * \\ \vdots & 0 & * & \dots & \dots & \dots & \dots & \dots & \dots & * \\ \vdots & \vdots & 0 & \dots & 0 & * & \dots & \dots & \dots & * \\ \vdots & \vdots & \vdots & \dots & \vdots & 0 & * & \dots & \dots & * \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$$

1. Zeile =  $a_1$

2. Zeile =  $a_2$

⋮

letzte Zeile vor Nullzeilen =  $a_r$

$r = \text{rang}(A)$ ,  $\pi_j =$  Pivotelemente,  $j_1, \dots, j_r =$  Sprungstellen der Treppenfunktion

1. Behauptung: Die ersten  $r$  Zeilen  $a_1, \dots, a_r$  sind linear unabhängige Vektoren in  $\mathbb{K}^n$ .

2. Behauptung: Die Pivotspalten  $j_1, \dots, j_r$  sind linear unabhängig in  $\mathbb{K}^m$ .

Anwenden:  $a_1, \dots, a_m \in V = \mathbb{K}^n$ ,  $U = \text{Span}(a_1, \dots, a_n)$

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \Rightarrow \text{Zeilenstufenform mit Treppenfunktion}$$

Gesucht ist eine Basis.

Nachtrag:

**Lemma 3.3.5.**  $\mathcal{E} \subseteq V$ .  $\text{Span}(\mathcal{E})$  ist der kleinste ("kleinste obere Schranke") Untervektorraum von  $V$ , der  $\mathcal{E}$  enthält.

*Beweis.* Alle UVR von  $V$  bilden einen "Verband" = Menge  $X$  mit einer *Ordnungsrelation*.

D.h. wir haben:

zwischen je zwei  $x_1, x_2 \in X$  kann eine Relation gelten  $x_1 \leq x_2$  oder nicht. Es muss nicht Vergleichbarkeit herrschen. Es kann sein, dass weder  $x_1 \leq x_2$  noch  $x_2 \leq x_1$  gilt.  $\square$

**Beispiel 3.3.6.**  $X = \mathbb{R}, x_1 \leq x_2$  mit der uns bekannten Bedeutung.

Hier:

$x_1 \leq x_2$  oder  $x_2 \leq x_1$  oder beides ( $\Rightarrow x_1 = x_2$ )

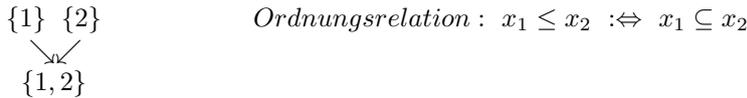
Dies nennt man eine *totale* oder *lineare Ordnung*.

**Beispiel 3.3.7.**  $M =$  Menge,  $\mathfrak{X} = \text{Pot}(M) =$  Potenzmenge =  $\mathcal{P} =$  Menge aller Teilmengen von  $M$ .

$$M = \{1, 2\}$$

$$\mathfrak{X} = \emptyset$$





**Beispiel 3.3.8.**  $\mathfrak{X} = \mathbb{N}$ ,  $a \leq b \Leftrightarrow a$  ist Teiler von  $b$ .  
 Es müssen folgende Axiome gelten:

1. Reflexivität:  $x \leq y$
2. Transitivität:  $x \leq y \wedge y \leq z \Rightarrow x \leq z$

Ein maximales Element in  $\mathfrak{X}$  ist ein  $x \in \mathfrak{X}$ , sodass gilt:  $x \geq x_0 \Rightarrow x = x_0$

**Beispiel 3.3.9.**  $V = VR$  über  $\mathbb{K}$ ,  $\mathfrak{X} =$  Menge der linear unabhängigen Teilmengen von  $V$ , Ordnungsrelation = Inklusion

**Lemma 3.3.10.** Zorn'sches Lemma

garantiert ein maximales  $\mathcal{B} \in \mathfrak{X}$ . Es ist dann leicht zu zeigen:  $\mathcal{B}$  ist auch ein EZS.

*Beweis.* Angenommen, das ist nicht so. D.h. es gibt ein UVR  $W$  mit  $\mathcal{E} \subseteq W \subsetneq \text{Span}(\mathcal{E})$ .

Dann gibt es ein  $x \in \text{Span}(\mathcal{E})$  mit  $x \notin W$ , also gibt es geeignete  $e_1, \dots, e_n \in \mathcal{E}$  und  $\lambda_1, \dots, \lambda_n \in \mathbb{K}$  mit  $x = \lambda_1 e_1 + \dots + \lambda_n e_n$ .

Es ist aber:

alle  $e_i \in W$

alle  $\lambda e_i \in W$

ABER  $x = \lambda_1 e_1 + \dots + \lambda_n e_n \in W \Rightarrow$  Widerspruch! □

**Beispiel 3.3.11.**  $\text{Span}(\mathcal{E})$  ist der Durchschnitt aller UVR, die  $\mathcal{E}$  enthalten.

*Beweis.* Sei  $U_\alpha (\alpha \in I)$ : alle UVR in  $V$  mit  $\mathcal{E} \subseteq U_\alpha$ . Nach (1) und (2) ist  $\text{Span}(\mathcal{E})$  ein solches  $U_\alpha$ . Also gilt:

$$\bigcup_{\alpha \in I} U_\alpha \subseteq \text{Span}(\mathcal{E}).$$

$$\text{Sei } x = \lambda_1 e_1 + \dots + \lambda_n e_n \in \text{Span}(\mathcal{E}) \text{ d.h. } e_i \in \bigcap_{\alpha \in I} U_\alpha. \quad \square$$

Nachtrag:

**Lemma 3.3.12.** Ist  $\mathcal{B}$  eine Basis,  $b_i \in \mathcal{B}, 0 \neq \lambda \in \mathbb{K}$ , dann ist  $\mathcal{B}' = (\mathcal{B} - \{b_i\} \cup \{\lambda \cdot b_i\})$  wieder eine Basis.

*Beweis.* Aus Lemma 3.2 und Lemma 3.17. □

**Lemma 3.3.13.** Ist  $\mathcal{B}$  eine Basis,  $b_i, b_j \in \mathcal{B}$ , dann ist  $\mathcal{B}' = (\mathcal{B} - \{b_i\} \cup \{b_i + b_j\})$  wieder eine Basis.

*Beweis.* Aus Lemma 3.3 und Lemma 3.18. □

**Lemma 3.3.14.** Austauschatz von Steinitz

Es sei  $\mathcal{B} = \{b_1, \dots, b_i, \dots\}$  eine Basis von  $V$  und sei  $b \in V$  mit einer Darstellung

$$b = \beta_1 b_1 + \dots + \beta_i b_i + \dots + \beta_n b_n \text{ für } \beta_1, \dots, \beta_n \in \mathbb{K} \text{ und etwa } \beta_i \neq 0.$$

Dann ist  $\mathcal{B}' = (\mathcal{B} - \{b_i\} \cup \{b\})$  wieder eine Basis.

*Beweis.* Sei  $v \in V$  dargestellt durch  $v = \lambda_1 b_1 + \dots + \lambda_i b_i + \dots + \lambda_n b_n$ .

O.B.d.A. nehmen an:  $n = m$  (Ergänzung durch Nullterme, falls  $n \neq m$ )

Dann können wir schreiben:

$$v = (\lambda_1 - \frac{\beta_1 \lambda_i}{\beta_i}) b_1 + \dots + \hat{b}_i + \dots + (\lambda_n - \frac{\beta_n \lambda_i}{\beta_i}) b_n$$

$$\text{weil } b_i = -\frac{\beta_1}{\beta_i} b_1 - \dots - \frac{\beta_{i-1}}{\beta_i} b_{i-1} - 1 - \frac{\beta_{i+1}}{\beta_i} b_{i+1} - \dots - \frac{\beta_n}{\beta_i} b_n$$

D.h.  $v$  ist auch darstellbar durch  $\mathcal{B}'$ . Ist  $\alpha_1 b_1 + \dots + \alpha_i b_i + \dots + \alpha_n b_n = 0$  eine Relation in  $\mathcal{B}'$ , so erhalten wir durch Einsetzen von  $b$  daraus eine Relation in  $\mathcal{B}$ :

$$(\alpha_1 - \alpha_i \beta_1) b_1 + \dots + \alpha_i \beta_i b_i + \dots + (\alpha_n - \alpha_i \beta_n) b_n = 0$$

Weil  $\mathcal{B}$  linear unabhängig, muss dies eine triviale Relation sein, also

$$\alpha_1 - \alpha_i \beta_1 = 0$$

$\vdots$   
 $\alpha_i \beta_i = 0 \quad \Rightarrow \alpha_i = 0 \rightarrow \text{Also } \alpha_k = 0 \text{ auch für } \alpha_1, \dots, \alpha_n$   
 $\vdots$   
 $\alpha_n - \alpha_i \beta_n = 0$   
 Deshalb ist  $\mathcal{B}'$  linear unabhängig. □

**Satz 3.3.15. Existenzsatz von Basen**  
 Jeder Vektorraum besitzt eine Basis

*Bemerkung.* Wir zeigen dies hier nur für endlich abzählbar erzeugte VR über  $\mathbb{K}$ , denn dafür genügt die gewöhnliche Induktion. Für VR, die überabzählbar erzeugt sind, braucht man "transfinite Induktion". Eine Variante ist das *Zorn'sche Lemma*, welches zum Auswahlaxiom und zum Wohlordnungssatz äquivalent ist. (siehe Aufgabe 35)

*Beweis.* (Im endlichen oder abzählbaren Fall)

Wir wählen ein abzählbares EZS  $\mathcal{E} = \{e_1, e_2, \dots, e_k, \dots\}$ . (Ist  $V$  endlich erzeugt, so läuft  $k$  nur bis zu diesem einen endlichen  $n$ .) Wir betrachten technisch (algorithmisch)  $\mathcal{E}$  als eine geordnete Folge.

Wir setzen  $\mathcal{E}_l := \emptyset$

$\mathcal{E}_k := \{e_1, \dots, e_k\}$  für  $k = 1, \dots, (n), \dots$

Algorithmus (Basisauswahlverfahren)

$\mathcal{B} := \emptyset$

$$\mathcal{B}_k := \begin{cases} \mathcal{B}_{k-1} & \text{falls } b_k \in \text{Span}(\mathcal{B}_{k-1}) \\ \mathcal{B}_{k-1} \cup b_k & \text{falls } b_k \notin \text{Span}(\mathcal{B}_{k-1}) \end{cases}$$

(Falls  $V$  endlich erzeugt wird, so läuft  $k$  nur bis  $n$ .)

1.  $\mathcal{B}_k \subseteq \mathcal{B}_{k-1}$  - nach Konstruktion
2.  $\text{Span}(\mathcal{B}_k) = \text{Span}(\mathcal{E}_k)$  - nach Konstruktion und Induktion
3.  $\mathcal{B}_k$  ist linear unabhängig - nach Induktion, mit Lemma 3.19.

$$\text{Wir setzen } \mathcal{B} = \begin{cases} \bigcup_{k=0}^n & \text{falls } V \text{ endlich erzeugt ist} \\ \bigcup_{k=0}^{\infty} & \text{falls } V \text{ abzählbar unendlich ist} \end{cases}$$

4.  $\mathcal{B}$  ist ein EZS:

Ist  $v \in V$  durch die ersten  $k : e_1, \dots, e_k$  darstellbar, also  $v = \lambda_1 b_1 + \dots + \lambda_k b_k$ , so ist  $v \in \text{Span}(\mathcal{E}_k) =_2 \text{Span}(\mathcal{B}_k) \subseteq_1 \text{Span}(\mathcal{B})$

5.  $\mathcal{B}$  ist linear unabhngig.

Gibt es eine Relation zwischen (endlich vielen) Elementen in  $\mathcal{B}$ , so liegen diese bereits in einem  $\mathcal{B}_N$ , weil es nur endlich viele sind.

$$e_1 \in \mathcal{B}_{k_1}$$

$$e_2 \in \mathcal{B}_{k_2}$$

$\vdots$

$$e_l \in \mathcal{B}_{k_l}$$

$$\Rightarrow e_1, \dots, e_l \in \mathcal{B}_N, \quad N = \max\{k_1, \dots, k_n\}$$

Aber nach 3) ist  $\mathcal{B}_N$  linear unabhängig. □

**Bemerkung:**

Das Basisauswahlverfahren (BAV) aus dem Basisexistenzsatz ist im Wesentlichen ein Algorithmus:

EINGABE: Geordnetes EZS  $\mathcal{E} = \{e_1, \dots, e_n, \dots\}$  (endlich oder abzählbar)

ABFRAGE: Ist  $e_{k+1} \in \text{Span}(\{e_1, \dots, e_k\})$ ?

Wenn nein füge ihn zur Basis hinzu.

Wenn ja füge es nicht zur Basis hinzu und betrachte  $e_{k+2}$

AUSGABE: Geordnete Basis  $\mathcal{B} \subseteq \mathcal{E}$

**Beispiele:**

1)  $V = \text{Pol}(\mathbb{R})$  (Die Polynomfunktionen  $f: \mathbb{R} \rightarrow \mathbb{R}$ ).

Wähle als EZS die Stammpolynome  $\mathcal{E} = \{1, X, X^2, \dots, X^n, \dots\}$ .

Behauptung:  $X^{n+1} \notin \text{Span}(1, \dots, X^n)$  (Dies ist für Polynome trivial aber noch lange nicht für Polynomfunktionen!)

Um dies zu zeigen nutzen wir einen Trick der universal einsetzbar ist:

Gäbe es eine Linearkombination, so dass

$$X^{n+1} = \sum_{k=0}^n a_k X^k \quad (3.1)$$

so könnte man (1) n-mal differenzieren (bei Polynomfunktionen wendet man formales Differenzieren an) und erhält

$$(n+1)!X = a_n n! \quad (3.2)$$

Damit wäre aber bereits, wenn  $X=0$  in (2) eingesetzt wird

$$0 = a_n n! \Rightarrow a_n = 0 \quad (3.3)$$

setzt man nun (3) in (1) ein und iteriert das Verfahren, erhält man, dass alle  $a_i = 0$  sind, womit aber  $X^{n+1} = 0$  wäre, was definitiv nicht der Fall ist.

2) Analog sieht man ein, dass  $\mathcal{B} = \{e^{a_k x} | k \in \mathbb{N} \text{ und } a_k \in \mathbb{R}\}$  linear unabhängig in  $C^\infty(\mathbb{R})$  ist.

3) Wiederum Analog sieht man ein, dass  $\mathcal{B} = \{\sin(a_k x) | k \in \mathbb{N} \text{ und } a_k \in \mathbb{R}\}$  linear unabhängig ist.

4) Sei  $V$  der Raum stetiger stückweise affiner Funktionen  $f: [0; 1] \rightarrow \mathbb{R}$  mit  $0=f(0)=f(1)$

So ist  $\mathcal{B} = \{Z_\xi | Z_\xi(x) : [0; 1] \rightarrow \mathbb{R}; Z_\xi = \begin{cases} \frac{x}{\xi} & 0 \leq x \leq \xi \\ \frac{x-1}{\xi-1} & \xi \leq x \leq 1 \end{cases}; \xi \in \mathbb{R}\}$  eine Basis.

Es ist sehr selten, dass eine überabzählbare Basis explizit angegeben werden kann, da es im Allgemeinen sehr schwer ist mit überabzählbarer Dimension (siehe Abschnitt 3.4) zu arbeiten. So ist für  $C^\infty(\mathbb{R})$  keine Hamel-Basis bekannt.

**Satz 3.3.16** (Basisergänzungssatz). *Sei  $V$  ein endlich oder abzählbar erzeugter  $K$ -Vektorraum. So kann jede linear unabhängige Teilmenge  $\mathcal{B}' \subseteq V$  zu einer Basis ergänzt werden.*

*Beweis.* Wähle ein beliebiges geordnetes Erzeugendensystem  $\mathcal{E} = \{e_1, \dots, e_n, \dots\}$ , welches nach dem Basisexistenzsatz definitiv existiert und wegen Abzählbarkeit auch geordnet werden kann.

So ist offensichtlich  $\mathcal{E}' = \{b_1, \dots, b_n, e_1, \dots, e_n, \dots\}$  erneut ein Erzeugendensystem. Wird nun BAV auf  $\mathcal{E}'$  angewandt, so werden die  $b_i$  zuerst betrachtet und wegen linearer Unabhängigkeit als Basisvektoren gewählt. Somit gilt für die letztendliche Basis  $\mathcal{B}' \subseteq \mathcal{B}$ .  $\square$

**Beispiele:**(BAV)

1)  $V = K^n$ ;  $\mathcal{E} = \{e_1, e_1 + e_2, e_1 + e_2 + e_3, \dots, e_1 + e_2 + \dots + e_n\}$   
 $\mathcal{B}' = \{2e_2\} \mapsto \mathcal{B} = \{2e_2, e_1, e_1 + e_2 + e_3, e_1 + e_2 + e_3 + e_4, \dots\}$

2)  $V = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ ;  $K = \mathbb{Q}$ ;  $\mathcal{E} = \{2, 2\sqrt{2}\}$   
 $\mathcal{B}'_1 = \{1 + \sqrt{2}\} \mapsto \mathcal{B}_1 = \{1 + \sqrt{2}, 2\}$   
 $\mathcal{B}'_2 = \{3\} \mapsto \mathcal{B}_2 = \{3, 2\sqrt{2}\}$

## 3.4 Dimension

Unser Ziel wird es sein die Dimension eines Vektorraumes durch die Kardinalität einer Basis des Vektorraumes zu definieren.

Doch dafür müssen wir uns zunächst überzeugen, dass solch ein Dimensionsbegriff wohldefiniert ist. Nach dem Basisexistenzsatz besitzt jeder Vektorraum zumindest eine Basis, dies bereitet uns also keine Probleme. Allerdings haben wir in den Übungen eingesehen, dass ein Vektorraum sehr viele Basen besitzt.

Zwar hat  $\mathbb{F}_2$  genau eine Basis, dieser ist aber auch der einzige neben dem trivialen Nullvektorraum mit nur einer Basis. So besitzt  $\mathbb{F}_3$  zwei Basen,  $(\mathbb{F}_2)^2$  hat drei Basen und  $(\mathbb{F}_7)^3$  besitzt bereits 5.630.688 Basen.

Noch deutlicher wird das Problem im  $\mathbb{R}^d$ . Denn nach dem Basisergänzungssatz kann man eine Basis konstruieren, indem man zunächst einen beliebigen von Null verschiedenen Vektor wählt, und daraufhin immer wieder von den vorher gewählten linear unabhängige Vektoren hinzufügt. So ergibt sich für die Menge aller geordneten Basen des  $\mathbb{R}^d$  folgende Darstellung  $\prod_{k=1}^{d-1} \{\mathbb{R}^d \setminus \mathbb{R}^k\}$  Womit  $\mathbb{R}^d$  sogar überabzählbar viele Basen besitzt.

Also stellt sich die Frage, ob alle Basen gleich mächtig sind.

**Proposition 3.4.1.** *Sei  $V$  ein von  $n$  Vektoren (insbesondere endlich) erzeugter Vektorraum, dann sind  $n+1$  Vektoren linear abhängig.*

*Beweis.* Es sei  $\mathcal{E} = \{e_1, e_2, \dots, e_n\}$  ein Erzeugendensystem in  $V$ . So folgt die Behauptung induktiv:

Induktionsverankerung: Für  $n=0$  ist  $\mathcal{E} = \{\}$  womit  $V = \text{Span}(\{\}) = 0$  ist.

Induktionsschritt: Seien  $v_1, \dots, v_n, v_{n+1} \in V$  beliebige aber verschiedene Vektoren. So besitzt jedes  $v_i$  folgende Darstellung:

$$v_i = \sum_{j=1}^n \omega_{i,j} e_{i,j} \text{ mit } \omega_{i,j} \in K$$

Zu Zeigen ist, dass eine nicht-triviale Relation  $0 = \sum_{k=1}^{n+1} \lambda_k v_k$  existiert, also dass mindestens ein  $\lambda_k \neq 0$  ist. Betrachte  $\lambda_k$  als Unbekannte in einem wie folgt konstruierten LGS:

$$\text{Es gelte : } 0 = \sum_{i=1}^{n+1} \lambda_i v_i = \sum_{i=1}^{n+1} \sum_{j=1}^n \omega_{i,j} e_{i,j}$$

setze  $\omega'_{i,j} := \omega_{j,i}$

Womit sich ein LGS des Ranges  $r \leq n$  ergibt, also min. eine freie Variable  $\lambda_k$  enthält. Womit wiederum das LGS eine nichttriviale Lösung besitzt.  $\square$

Nun können wir folgenden gewünschten Satz formulieren:

**Satz 3.4.2** (Dimensionssatz). *Sei  $V$  ein endlich erzeugter Vektorraum und  $\mathcal{B} = \{b_1, \dots, b_n\}$  sowie  $\mathcal{B}' = \{b'_1, \dots, b'_m\}$  zwei Basen in  $V$ , dann sind  $\mathcal{B}$  und  $\mathcal{B}'$  schon gleich mächtig (bzw.  $n=m$ ).*

*Beweis.*  $\mathcal{B}$  ist ein Erzeugendensystem in  $V$  mit  $n$  Vektoren. Nach Proposition 1 sind  $n+1$  Vektoren linear Abhängig, womit  $m \leq n$ . Analog für  $\mathcal{B}'$ .

Somit ist  $n=m$ .  $\square$

Also können wir nun unseren angestrebten Dimensionsbegriff definieren:

**Definition 3.4.3** (Dimension). Sei  $\mathcal{B}$  eine Basis in  $V$ , wobei  $V$  ein  $K$ -Vektorraum ist. So definiere:

$$\dim_K(V) := |\mathcal{B}|$$

Als die Dimension von  $V$ .

### Beispiele:

1) Sei  $K$  ein Körper so ist  $\dim_K(K^n) = n$

2)  $\dim_{\mathbb{R}}(\mathbb{C}) = 2$

3) Nach Übung sind  $\log(p_i)$  für beliebige Primzahlen  $p_i$  linear unabhängig in  $\mathbb{R}$  als  $\mathbb{Q}$ -Vektorraum. Also

ist  $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$ .

Dies ist zwar etwas informell, da es wie bereits erwähnt mehrere Arten der Unendlichkeit gibt. Es wird sich herausstellen, dass jene Dimension sogar überabzählbar ist.

Hier sieht man auch, dass unsere geometrische Vorstellung des Dimensionsbegriffes bei manchen Vektorräumen versagt, da  $\mathbb{R}$  als  $\mathbb{Q}$ -Vektorraum so zu sagen unendlich viele Richtungen besitzt, so stellt z.B. jedes  $\log(p_i)$  und jedes  $\sqrt{a}$  für ein  $a \neq n^2$  mit  $a, n \in \mathbb{N}$  eine Richtung dar.

4) Sei  $K[X]$  ein Polynomring über  $K$ , so ist  $\dim_K(K[X]) = |\mathbb{N}|$  also abzählbar.

Denn wähle als Basis  $\mathcal{B} = \{1, X, X^2, \dots, X^n, \dots\}$ .

5) Sei  $\mathbb{A}$  der Raum stetiger stückweise affiner Funktionen auf dem Intervall  $[0;1]$  mit  $f(0)=0$  und  $f(1)=0$ . So ist  $\dim_{\mathbb{R}}(\mathbb{A}) = |\mathbb{R}|$  also überabzählbar.

6) Sei  $\mathbb{E}$  der Untervektorraum des Vektorraumes der glatten Funktionen über  $\mathbb{R}$  aufgespannt von  $e^{ax}$ . So ist  $\dim_{\mathbb{R}}(\mathbb{E}) = |\mathbb{R}|$  also auch überabzählbar.

### Bemerkung:

Was wir in der linearen Algebra eine Basis nennen heißt im allgemeinen Hamel-Basis. Denn in anderen Gebieten der Mathematik treten andere Basisbegriffe auf. So arbeitet die Analysis oftmals in bzw. mit Räumen überabzählbarer Dimension, wie  $C^\infty(\mathbb{R})$ , wobei es für solche im allgemeinen sehr schwer ist eine Hamel-Basis anzugeben. Also betrachten Analytiker lediglich approximative Basen, die sogenannte Hilbert-Basis, bei der sich zwar nicht jedes Element des Vektorraumes als (endliche) Linearkombination der Basisvektoren schreiben lässt, wohl aber beliebig gut durch eine Linearkombination der Basisvektoren approximiert werden kann. Beispiele sind Fourier-Reihen, welche glatte periodische Funktionen durch Überlagerungen von  $\sin$  und  $\cos$  approximieren. Und der Weierstraß'sche Approximationssatz garantiert, dass glatte Funktionen durch Polynomfunktionen approximiert werden können.

Für die Algebra reicht eine Hilbertbasis jedoch nicht aus!

Die folgende Proposition mag trivial erscheinen –und bei Vektorräumen ist sie es tatsächlich–, aber wenn man sich beispielsweise mit Gruppen beschäftigt, gilt die analoge Aussage nicht.

**Proposition 3.4.4.** Für einen Unterraum  $U \subseteq V$  eines endlich-erzeugten Vektorraums gilt immer  $\dim(U) \leq \dim(V)$ .

*Beweis.* Sei  $\mathcal{B}$  eine Basis von  $U$ , dann ergänze sie zu einer Basis  $\mathcal{B}'$  von  $V$ , also  $\mathcal{B} \subseteq \mathcal{B}'$ . Dann ist  $\dim(U) = |\mathcal{B}| \leq |\mathcal{B}'| = \dim(V)$   $\square$

**Proposition 3.4.5.** Es seien  $U', U''$  Untervektorräume von  $V$  ( $V$  wieder endlich-erzeugt) mit  $U := U' \cap U''$  und  $\tilde{U} := U' + U''$ . Dann gilt  $\underbrace{\dim(\tilde{U})}_{n+m+k} = \underbrace{\dim(U')}_{k+n} + \underbrace{\dim(U'')}_{k+m} - \underbrace{\dim(U)}_k$ .

*Beweis.* Wir wählen eine Basis  $\mathcal{B}$  für  $U$ . Wir ergänzen einmal zu einer Basis  $\mathcal{B}' \supset \mathcal{B}$  von  $U'$  und  $\mathcal{B}'' \supset \mathcal{B}$  von  $U''$ . Außerdem setzen wir  $\tilde{\mathcal{B}} = \mathcal{B}' \cup \mathcal{B}''$ . Die Beziehungen sind im folgenden kommutativen Diagramm dargestellt:

$$\begin{array}{ccc}
 U'' & \hookrightarrow & \tilde{U} & = & U' + U'' & & \mathcal{B}'' & \subseteq & \tilde{\mathcal{B}} \\
 \uparrow & & \uparrow & & & & \cup & & \cup \\
 U' \cap U'' & \hookrightarrow & U & & & & \mathcal{B}' \cap \mathcal{B}'' & = & \mathcal{B} \subseteq \mathcal{B}'
 \end{array}$$

*Behauptung:*  $\tilde{\mathcal{B}}$  ist eine Basis für  $\tilde{U}$ .  $\mathcal{B}'$  ist offensichtlich ein Erzeugendensystem für  $\tilde{U}$ . Betrachte die linear-unabhängige Menge  $\mathcal{B}'$  und das Erzeugendensystem  $\mathcal{E} := \tilde{\mathcal{B}} = \mathcal{B}' \cup \{b'_1, \dots, b'_{m-k}\}$  von  $\tilde{U}$  und wende das Basisauswahlverfahren an:

$b'_1 \notin \text{span}(\mathcal{B}')$ , also Fügen wir  $b'_1$  hinzu;  $b'_2 \notin \text{span}(\mathcal{B}' \cup \{b'_1\})$ , wir fügen  $b'_2$  hinzu, und so weiter. Das heißt, das Basisauswahlverfahren liefert uns hier tatsächlich  $\tilde{\mathcal{B}}$ .  $\square$

**Beispiel 3.4.6.** 1. Seien  $\mathbb{K} \subseteq \mathbb{L}$  Körper. Sei  $\Lambda = \{\lambda_1, \dots, \lambda_l\}$  eine Basis von  $\mathbb{L}$  als  $\mathbb{K}$ -Vektorraum. Ist  $V$  ein  $\mathbb{L}$ -Vektorraum mit Basis  $\mathcal{B}_{\mathbb{L}} = \{b_1, \dots, b_n\}$  (als  $\mathbb{L}$ -Vektorraum!), dann ist

$$\mathcal{B}_{\mathbb{K}} := \Lambda \cdot \mathcal{B}_{\mathbb{L}} = \{\lambda_1 b_1, \dots, \lambda_l b_1, \lambda_1 b_2, \dots, \lambda_l b_2, \dots, \lambda_1 b_n, \dots, \lambda_l b_n\}$$

eine Basis von  $V$  als  $\mathbb{K}$ -Vektorraum. Insbesondere gilt:

$$\dim_{\mathbb{K}} V = \underbrace{\dim_{\mathbb{K}} \mathbb{L}}_l \cdot \underbrace{\dim_{\mathbb{L}} V}_n$$

Konkret heißt das, wenn wir  $\mathbb{K} = \mathbb{R}$  und  $\mathbb{L} = \mathbb{C}$  betrachten:  $\Lambda = \{1, i\}, l = 2$ . Also:  $\dim_{\mathbb{R}} V = 2 \cdot \dim_{\mathbb{C}} V$

2. Wir betrachten  $V = \mathbb{C}^n$  als  $\mathbb{C}$ - und als  $\mathbb{R}$ -Vektorraum:

$$\mathcal{B}_{\mathbb{C}} = \{e_1, \dots, e_n\}; e_k = (0, \dots, 0, \underbrace{1}_{\boxed{k}}, 0, \dots, 0)$$

$$\mathcal{B}_{\mathbb{R}} = \{e_1, ie_1, e_2, ie_2, \dots, e_n, ie_n\}; ie_k = (0, \dots, 0, \underbrace{i}_{\boxed{k}}, 0, \dots, 0)$$

3. Wir betrachten  $V = \mathbb{C}[X]$  der komplexen Polynome in  $X$ , wieder zunächst als Vektorraum über  $\mathbb{C}$  und dann über  $\mathbb{R}$ :

$$\mathcal{B}_{\mathbb{C}} = \{1, X, X^2, \dots, X^n, \dots\} \text{ Stammpolynome}$$

$$\mathcal{B}_{\mathbb{R}} = \{1, i, X, iX, \dots, X^n, iX^n, \dots\}$$

**Beispiel 3.4.7.** es sei  $\mathbb{L}$  ein *endlicher* Körper (etwa  $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5, \dots, \mathbb{F}_p$ ). Weil  $\mathbb{L}$  endlich ist, muss  $\text{char}(\mathbb{L}) = p$  ( $p$  eine Primzahl) sein. Wie in Definition 2.1.9 setzen wir

$$\varepsilon_0 := 0, \varepsilon_1 := 1, \varepsilon_{n+1} := \varepsilon_n + 1$$

Also gilt  $\varepsilon_p = 0$ .

*Behauptung:*  $\mathbb{K} := \{\varepsilon_0, \dots, \varepsilon_{p-1}\}$  bilden einen Unterkörper, der isomorph ist zu  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . Zu zeigen:  $\mathbb{F}_p \hookrightarrow \mathbb{L}, r \mapsto \varepsilon_r, 0 \leq r < p$ . Es gilt  $-\varepsilon_k = \varepsilon_{p-k}, \varepsilon_n + \varepsilon_m = \varepsilon_{n+m}$ . Das multiplikative Inverse  $\varepsilon_k^{-1}$  ist durch den euklidischen Algorithmus eindeutig bestimmt.

$\mathbb{L}$  hat als Vektorraum über  $\mathbb{K}$  eine endliche Basis  $\mathcal{B} = \{b_1, \dots, b_n\}$ . Da jedes  $v \in \mathbb{L}$  genau eine Darstellung  $v = \lambda_1 b_1 + \dots + \lambda_n b_n$  hat, sind insgesamt  $p^n$  Elemente möglich: Für jeden der  $n$  Koeffizienten  $\lambda_1 \dots \lambda_n$  gibt es jeweils  $p$  Wahlmöglichkeiten, da  $\lambda_i \in \mathbb{K}$ . Daraus folgt, dass

$$|\mathbb{L}| = p^n$$

Es gibt also insbesondere keinen Körper mit etwa sechs Elementen.

### 3.5 Prinzip der linearen Fortsetzung

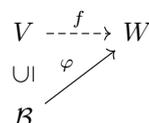
Das Prinzip der linearen Fortsetzung besagt, dass eine lineare Abbildung durch die Werte auf einer Basis vollständig bestimmt ist. Dieser „Trick“ ist hilfreich, da man statt unendlicher Systeme endliche Basen betrachten kann. Außerdem können wir die Werte auf einer Basis vorgeben, und dann wissen, dass es eine solche lineare Abbildung gibt.

**Proposition 3.5.1.** Seien  $V, W$  zwei Vektorräume über einem Körper  $\mathbb{K}$ .

(i) Für ein Erzeugendensystem  $\mathcal{E}$  von  $V$  gilt: Sind  $f, g : V \rightarrow W$  zwei lineare Abbildungen und gilt  $f(e) = g(e)$  für alle  $e \in \mathcal{E}$ , dann gilt  $f = g$  (d.h.  $\forall v \in V : f(v) = g(v)$ ).

(ii) Für eine linear-unabhängige Menge  $\mathcal{B}$  in  $V$  gilt: Ist  $\varphi : \mathcal{B} \rightarrow W, b \mapsto \varphi(b)$  eine beliebige Funktion, so gibt es eine lineare Fortsetzung  $f : V \rightarrow W$ , das heißt eine lineare Abbildung  $f$  mit der Eigenschaft  $f|_{\mathcal{B}} = \varphi$  (d.h.  $f(b) = \varphi(b), b \in \mathcal{B}$ ).

Im kommutativen Diagramm:



(iii) Aus (i) und (ii) folgt dann: Für eine Basis  $\mathcal{B}$  von  $V$  gilt: Jede Funktion  $\varphi : \mathcal{B} \rightarrow W$  besitzt genau eine lineare Fortsetzung  $f : V \rightarrow W$  (d.h.  $f|_{\mathcal{B}} = \varphi$ ).

**Korollar 3.5.2.** Es gibt eine Bijektion zwischen den Funktionen von  $\mathcal{B}$  nach  $W$  und den linearen Abbildungen von  $V$  nach  $W$ .

$$\begin{aligned} \text{Funkt}(\mathcal{B}, W) &= W^{\mathcal{B}} \xrightarrow{\cong} \text{lin}_{\mathbb{K}}(V, W) = \text{Hom}_{\mathbb{K}}(V, W) \\ &\quad \varphi \longmapsto f \\ \varphi &:= f|_{\mathcal{B}} \longleftarrow f \end{aligned}$$

*Beweis.* (i) Sei  $v$  dargestellt durch  $\mathcal{E}$ , etwa

$$v = \lambda_1 e_1 + \dots + \lambda_n e_n$$

Dann rechnet man einfach nach:

$$\begin{aligned} f(v) &= f(\lambda_1 e_1 + \dots + \lambda_n e_n) \\ &= \lambda_1 \underbrace{f(e_1)}_{=} + \dots + \lambda_n \underbrace{f(e_n)}_{=} \\ &= \lambda_1 \underbrace{g(e_1)}_{=} + \dots + \lambda_n \underbrace{g(e_n)}_{=} \\ &= g(\lambda_1 e_1 + \dots + \lambda_n e_n) \\ &= g(v) \end{aligned}$$

(ii) Auf  $\mathcal{B} = \{b_1, \dots, b_n\}$  seien Werte  $w_i = \varphi(b_i)$  vorgegeben. wir ergänzen  $\mathcal{B}$  zu einer Basis  $\mathcal{B}' \supseteq \mathcal{B}$  von  $V$ :

$$\mathcal{B}' = \{b_1, \dots, b_n, \underbrace{b'_1, \dots, b'_m}_{\text{ergänzt}}\}$$

Wir schreiben  $v = \lambda_1 b_1 + \dots + \lambda_n b_n + \lambda'_1 b'_1 + \dots + \lambda'_m b'_m$ . Wir wählen  $w_{n+1}, \dots, w_{n+m}$  beliebig in  $W$  (z.B.  $= 0$ ). Dann definieren wir:

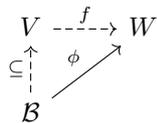
$$f(v) = \lambda_1 w_1 + \dots + \lambda_n w_n + \lambda'_1 w_{n+1} + \dots + \lambda'_m w_{n+m}$$

Wir stellen fest:

1. Damit ist  $f : V \rightarrow W$  für jedes  $v$  definiert, denn für jedes  $v$  gibt es eine Darstellung.
2.  $f$  ist wohldefiniert, weil die Darstellung von  $v$  eindeutig ist.
3.  $f$  ist linear.
4.  $f|_{\mathcal{B}} = \varphi$  auf  $\mathcal{B}$

□

$V$  Sei ein  $\mathbb{K}$ -Vektorraum.  $\mathcal{B} \subseteq V$



$f$  ist linear,  $\phi$  entspricht dann einer beliebigen Funktion.

$$\text{Funkt}(\mathcal{B}, W) = W^{\mathcal{B}} \longrightarrow \text{Lin}_{\mathbb{K}}(V, W) = \text{Hom}_{\mathbb{K}}(V, W); \quad \phi \longleftrightarrow f$$

1.  $\mathcal{E}$  ist Erzeugendensystem  
 $f, g : V \longrightarrow W$   
 $f|_{\mathcal{E}} = g|_{\mathcal{E}} \implies f = g$
2.  $\mathcal{B}$  ist linear-unabhängig  $\forall \phi : \mathcal{B} \longrightarrow W \exists! f : V \longrightarrow W$  linear  $f|_{\mathcal{B}} = \phi$
3.  $\mathcal{B}$  ist eine Basis  $\forall \phi : \mathcal{B} \longrightarrow W \exists! f : V \longrightarrow W$  linear  $f|_{\mathcal{B}} = \phi$

**Beispiel 3.5.3.**  $V = \mathbb{C}, \mathbb{K} = \mathbb{C}$

## 3.6 Koordinaten

$V$  ist endlich erzeugter Vektorraum über  $\mathbb{K}$ .

$\mathcal{B} = (b_1, \dots, b_n)$  ist geordnete Basis.

Sei  $V \ni v = \lambda_1 b_1 + \dots + \lambda_n b_n$  und  $v = \lambda'_1 b_1 + \dots + \lambda'_n b_n$ , dann ist  $\lambda_1 = \lambda'_1, \dots, \lambda_n = \lambda'_n$  (eindeutige Darstellung).

**Definition 3.6.1.** Falls  $\mathcal{B}$  eine fest gewählte Basis ist, dann gibt es *Koordinaten* bzgl.  $\mathcal{B}$ . Definiert durch

$$K_{\mathcal{B}} : V \longrightarrow \mathbb{K}^n$$

$$v \longmapsto (\lambda_1, \dots, \lambda_n),$$

falls  $v = \lambda_1 b_1 + \dots + \lambda_n b_n$ .

$K_{\mathcal{B}}^i(v) = \lambda_i$  ist die  $i$ -te Koordinate.

$$K_{\mathcal{B}}(v) = (K_{\mathcal{B}}^1(v), \dots, K_{\mathcal{B}}^n(v))$$

**Satz 3.6.2.**  $K_{\mathcal{B}}$  ist ein Isomorphismus.

*Beweis.*

1. zz.  $K_{\mathcal{B}}$  ist bijektiv:

$(\lambda_1, \dots, \lambda_n) \longmapsto v = \lambda_1 b_1 + \dots + \lambda_n b_n$  Rückrichtung ist klar nach Konstruktion (siehe Definition).

2. zz.  $K_{\mathcal{B}}$  ist linear:

$$K_{\mathcal{B}}(0) = (0, \dots, 0) = 0$$

Seien  $v, v' \in V$ .

Dann gilt  $K_{\mathcal{B}}(v) + K_{\mathcal{B}}(v') = K_{\mathcal{B}}(v + v')$ , denn  $(\lambda_1 b_1 + \dots + \lambda_n b_n) + (\lambda'_1 b_1 + \dots + \lambda'_n b_n) = (\lambda_1 + \lambda'_1) b_1 + \dots + (\lambda_n + \lambda'_n) b_n$

Sei  $\alpha \in \mathbb{K}$  und  $v \in V$ .  $K_{\mathcal{B}}(\alpha v) = \alpha K_{\mathcal{B}}(v)$ , denn  $\lambda_1 \alpha b_1 + \dots + \lambda_n \alpha b_n = \alpha(\lambda_1 b_1 + \dots + \lambda_n b_n)$

□

**Beispiel 3.6.3.** 1. Wenn  $V = \mathbb{K}^n$  und  $\mathcal{B} = (b_1, \dots, b_n)$  Standardbasis, dann ist  $K_{\mathcal{B}}(v) = v$ , also  $K_{\mathcal{B}} = id$ .

Denn  $v = (v_1, \dots, v_n) = v_1 e_1 + \dots + v_n e_n$ .

2. Wenn  $V = \mathbb{R}^2$  und  $\mathcal{B} = (b_1, b_2) = ((1, 0), (1, 1))$ , dann ist  $v = (1, 1) = 1b_1 + 1b_2 = 1(1, 0) + 1(1, 1)$

3. Wenn  $V = P_n(\mathbb{K}) \cong$  Vektorraum der Polynome vom Grad  $\leq n$  und  $\mathcal{B} = \{1, X, X^2, \dots, X^n\}$ . Dann ist  $p(X) = a_0 + a_1 X + \dots + a_n X^n$ ,  $K_{\mathcal{B}} = (a_0, \dots, a_n)$

Es stellt sich nun die Frage, was tun, wenn  $V$  nicht endlich erzeugt ist?

- wähle auch hier Basis  $\mathcal{B}$
- was wäre auf der rechten Seite  $\mathbb{K}^{\mathcal{B}}$  oder  $\mathbb{K}^{|\mathcal{B}|}$   $W^{\mathcal{B}}$  ist die Menge aller Funktionen  $\phi : \mathcal{B} \longrightarrow W$
- $\mathbb{K}^{\mathcal{B}}$  ist in der Tat zu groß für unsere Zwecke

Besser: Teilraum  $\mathbb{K}(\mathcal{B})$  ist frei von  $\mathcal{B}$  erzeugter Vektorraum.  $\mathbb{K}^{\mathcal{B}} \cong$  Menge aller Funktionen von  $\mathcal{B}$  nach  $\mathbb{K}$  ist das kartesische Produkt aller Faktoren  $\mathbb{K}$ , Indexmenge  $\mathcal{B}$

$\prod \mathbb{K}_b \cong$  alle mit  $\mathcal{B}$  indizierten Familien  $(\lambda_b \mid b \in \mathcal{B}) \longleftrightarrow \phi : \mathcal{B} \longrightarrow \mathbb{K}; b \longmapsto \lambda_b$ . Im Falle  $\mathcal{B}$  abzählbar, so wäre dies dann die Folge  $(\lambda_1, \lambda_2, \dots)$

Unterraum  $\mathbb{K}(\mathcal{B}) \subseteq \mathbb{K}^{\mathcal{B}}$  aller Funktionen  $\phi : \mathcal{B} \longrightarrow \mathbb{K}$  mit  $\lambda_i \in \mathbb{K}$  und  $\phi(b) = 0$  für fast alle  $b \in \mathcal{B}$ , d.h. die Menge  $\text{supp}(\phi) \cong$  Menge der Träger von  $\phi = \{b \in \mathcal{B} \mid \phi(b) \neq 0\}$  endlich.

$$\text{supp}(\alpha\phi) = \text{supp}(\phi), \alpha \neq 0$$

$$\text{supp}(\phi_1 + \phi_2) \subseteq \text{supp}(\phi_1) \cup \text{supp}(\phi_2)$$

$\mathbb{K}(\mathcal{B})$  ist eine  $\mathbb{K}$ -VR.

Basis? Standardbasis?

**Definition 3.6.4.** Für jedes  $b \in \mathcal{B}$  ist die *charakteristische Funktion* definiert durch:

$$\mathcal{X}_b : \mathcal{B} \longrightarrow \mathbb{K}$$

$$b' \longmapsto \delta_{bb'} = \begin{cases} 1, & b' = b, \\ 0, & b' \neq b. \end{cases}$$

$\phi \in \mathbb{K}(\mathcal{B})$

$\text{supp}(\phi) = \{b_1, \dots, b_n\}$

$\phi = \phi(b_1)\mathcal{X}_{b_1} + \dots + \phi(b_n)\mathcal{X}_{b_n}$   $X = \{\mathcal{X}_b \mid b \in \mathcal{B}\}$  ist ein Erzeugendensystem und linear-unabhängig  $\alpha_1\mathcal{X}_{b_1} + \dots + \alpha_n\mathcal{X}_{b_n} = 0$

Einsetzen  $b = b_1, b_2$ , dann  $\alpha_1\mathcal{X}_{b_1}(b_1) = 1$   $\mathcal{B} \longleftarrow X$

$b \longmapsto \mathcal{X}_b$

Dann  $\mathcal{B} \cong X \subseteq \mathbb{K}(\mathcal{B})$  und  $\dim_{\mathbb{K}}\mathbb{K}(\mathcal{B}) = |\mathcal{B}|$

**Beispiel 3.6.5.**  $\mathcal{B} = \{1, \dots, n\}$ ,  $\mathbb{K}(\mathcal{B}) \cong \mathbb{K}^n$ ;  $e_i \longmapsto \mathcal{X}_i$

Koordinaten:  $K_{\mathcal{B}} : V \longrightarrow K(\mathcal{B})$ ,  $v = \lambda_1 b_1 + \dots + \lambda_n b_n$  eine Darstellung durch gewisse  $b_1, \dots, b_n \in \mathcal{B}$ . (das ist nicht abgezählt)

$v \mapsto \mathcal{X}_v = \lambda_1\mathcal{X}_{b_1} + \dots + \lambda_n\mathcal{X}_{b_n}$ ,  $\text{supp}(\mathcal{X}_v) \subseteq \{b_1, \dots, b_n\}$

$\phi \longmapsto v' = \phi(b'_1)b'_1 + \dots + \phi(b'_m)b'_m$ ,  $\text{supp}(\phi) = \{b'_1, \dots, b'_m\}$

**Satz 3.6.6.**  $\mathbb{K}_{\mathcal{B}} : V \longrightarrow \mathbb{K}(\mathcal{B})$  ist ein Isomorphismus.

$A$  ist Menge,  $\mathbb{K}(A)$  frei von  $A$  erzeugter  $\mathbb{K}$ -VR,  $\phi : A \longrightarrow \mathbb{K}$ ,  $\text{supp}(\phi)$  endlich,  $\Psi \circ l_A = \Psi|_A = l_B \circ \psi$ .  $\Psi$  soll lineare Abbildung werden mit der Eigenschaft

$$\begin{array}{ccc} A & \xleftarrow{l_A} & \mathbb{K}(A) \\ \downarrow \psi & \searrow \phi & \downarrow l_B \circ \psi \\ B & \xleftarrow{l_B} & \mathbb{K}(B) = W \end{array}$$

## 3.7 Isomorphieinvarianten

**Definition 3.7.1.** Zwei Vektorräume  $V$  und  $W$  (über  $\mathbb{K}$ ) heißen *isomorph*, wenn es einen Isomorphismus  $f : V \rightarrow W$  gibt. Wir schreiben  $V \cong W$

**Satz 3.7.2.** *Isomorphie ist eine Äquivalenzrelation.*

*Beweis.* •  $f = id_V$  ist ein Isomorphismus von  $V$  nach  $V$ , sodass für alle Vektorräume  $V$  gilt  $V \cong V$

- Ist  $f : V \rightarrow W$  ein Isomorphismus, so ist auch  $f^{-1} : W \rightarrow V$  ein Isomorphismus. Also gilt für Zwei Vektorräume  $V, W$ :  $V \cong W \Leftrightarrow W \cong V$
- Sind  $f : V \rightarrow W$  und  $g : W \rightarrow X$  zwei Isomorphismen, so ist auch  $g \circ f$  ein Isomorphismus. Für  $V, W, X$  gilt also  $V \cong W, W \cong X \Rightarrow V \cong X$

□

Was ist eine Isomorphieinvariante? Das ist eine "Größe"  $\gamma$  (z.B. eine Zahl, ein Zahlenpaar, eine Angabe Ja/Nein), welche man einem Vektorraum zuordnen kann, so dass gilt:

$$V \cong W \Rightarrow \gamma(V) = \gamma(W)$$

Gilt auch die Umkehrung, so nennt man  $\gamma$  vollständig.

**Beispiel 3.7.3.** • Betrachten wir alle Rechtecke in der Ebene und als Äquivalenzrelation die Kongruenz. Da  $R \equiv R' \Leftrightarrow \text{Seitenlängen}(a, b) = (a', b')$  ist  $(a, b)$  eine vollständige Kongruenzinvariante.

- Wählen wir statt der Seitenlängen  $(a, b)$  den Flächeninhalt  $vol$ , oder die Diagonallänge  $\gamma_2$  wählt, so ist dies eine Kongruenzinvariante, aber keine vollständige.

- Betrachten wir als Äquivalenzrelation die Ähnlichkeit, so ist  $(a, b)$  keine Invariante. Wohl aber  $\gamma'_0(\mathbb{R}) = \frac{a}{b}$

Wir werden für  $\gamma = \dim_{\mathbb{K}}$  wählen und sogar mehr zeigen.

**Proposition 3.7.4.** Sei  $f : V \rightarrow W$  linear

1. Ist  $\xi \subseteq V$  ein Erzeugendensystem und  $f$  epimorph, so ist  $\xi' = f(\xi)$  ein Erzeugendensystem von  $W$ .
2. Ist  $\mathcal{B}$  linear unabhängig und  $f$  monomorph, so ist  $\mathcal{B}' = f(\mathcal{B})$  linear unabhängig.

*Beweis.* 1. Es sei  $w \in W$ , also etwa  $w = f(v)$  für ein  $v \in V$ . Wir können  $v$  schreiben als

$$v = \lambda_1 e_1 + \dots + \lambda_n e_n$$

für geeignete  $e_1, \dots, e_n \in \xi, \lambda_1, \dots, \lambda_n \in \mathbb{K}$  denn  $\xi$  ist EZS für  $V$ . Dann gilt  $w = f(v) = \lambda_1 f(e_1) + \dots + \lambda_n f(e_n)$  also ist  $w \in \text{Span}(\xi')$

2. Angenommen, wir hätten eine nicht-triviale Relation zwischen Elementen in  $\mathcal{B}'$ , also etwa

$$\lambda_1 f(b_1) + \dots + \lambda_n f(b_n) = 0$$

mit nicht alle

$$\lambda_1, \dots, \lambda_n$$

null. Dann hätten wir auch

$$f(\lambda_1 b_1 + \dots + \lambda_n b_n) = 0$$

und weil  $f$  monomorph ist, auch

$$\lambda_1 b_1 + \dots + \lambda_n b_n = 0$$

$\mathcal{B}$  war aber als linear unabhängig vorausgesetzt

□

**Korollar 3.7.5.** Es sei  $f : V \rightarrow V'$  ein Isomorphismus. Ist  $\mathcal{B} \subseteq V$   $\left\{ \begin{array}{l} \text{Erzeugendensystem} \\ \text{linear unabhängig} \\ \text{eine Basis} \end{array} \right.$ , so ist auch

$$\mathcal{B}' = f(\mathcal{B}) \subseteq V' \left\{ \begin{array}{l} \text{Erzeugendensystem} \\ \text{linear unabhängig} \\ \text{eine Basis} \end{array} \right.$$

*Beweis.* Beweis folgt aus der Proposition. □

**Satz 3.7.6.**  $V \cong V' \Leftrightarrow \dim_{\mathbb{K}}(V) = \dim_{\mathbb{K}}(V')$

*Beweis.* " $\Rightarrow$ ": Ist  $f : V \rightarrow V'$  ein Isomorphismus und  $\mathcal{B}$  irgendeine Basis von  $V$ , so ist nach dem Korollar  $f(\mathcal{B})$  eine Basis von  $V'$ . Da  $f$  bijektiv ist, sind  $\mathcal{B}$  und  $f(\mathcal{B}) = \mathcal{B}'$  gleich mächtig, also  $\dim_{\mathbb{K}}(V) = |\mathcal{B}| = |\mathcal{B}'| = \dim_{\mathbb{K}}(V')$ .

" $\Leftarrow$ ": Aus  $\dim_{\mathbb{K}}(V) = \dim_{\mathbb{K}}(V')$  folgt, dass je zwei Basen  $\mathcal{B}$  von  $V$  bzw.  $\mathcal{B}'$  von  $V'$  gleich mächtig sind. Wir wählen eine Bijektion  $\varphi : \mathcal{B} \rightarrow \mathcal{B}'$  und definieren  $\Phi = \mathbb{K}(\varphi) : \mathbb{K}(\mathcal{B}) \rightarrow \mathbb{K}(\mathcal{B}')$  durch  $\Phi(x) = x \circ \varphi : \mathcal{B}' : \mathcal{B}' \xrightarrow{\varphi^{-1}} \mathcal{B} \xrightarrow{x} \mathbb{K}$  einen Isomorphismus  $\Phi$ . Insgesamt haben wir dann

$$\begin{array}{ccc} V & \xrightarrow{\mathbb{K}_{\mathcal{B}}} & \mathbb{K}(\mathcal{B}) \\ \downarrow f & & \downarrow \Phi = \mathbb{K}(\varphi) \\ V' & \xrightarrow{\mathbb{K}_{\mathcal{B}'}} & \mathbb{K}(\mathcal{B}') \end{array}$$

Nun definieren wir  $f := \mathbb{K}_{\mathcal{B}'}^{-1} \circ \mathbb{K}(\varphi) \circ \mathbb{K}_{\mathcal{B}}$ . Dies ist ein Isomorphismus; er macht

das obige Diagramm kommutativ.

□

*Bemerkung.* Dieses  $f$  ist nicht *kanonisch*, was so viel heißt wie: es ist nicht der einzige Isomorphismus, er hängt von vielen Wahlen ab:

- Wahl von  $\mathcal{B}$
- Wahl von  $B'$
- Wahl von  $\varphi$

Rang:  $rg(A) = rg(T_A) = rg(L_{\mathfrak{B}\mathfrak{A}}(A))$

$$T_A : \mathbb{K}^n \rightarrow \mathbb{K}^m$$

$$f = L_{\mathfrak{B}\mathfrak{A}}(A) : V \rightarrow W \quad \dim(V) = n \quad \dim(W) = m$$

**Satz 3.7.7.**  $rg(A) = rg(T_A) = rg(L_{\mathfrak{B}\mathfrak{A}}(A))$

*Beweis.* Für die erste Gleichheit wenden wir die Dimensionsformel an:

$$\dim(W(A)) = \dim(\text{Im}(T_A)) = n - \dim(\mathcal{L}(A|0)) = r = rg(A)$$

Für die zweite Gleichheit beachte man

$$\begin{array}{ccc} V & \xrightarrow{f = L_{\mathfrak{B}\mathfrak{A}}} & W \\ K_{\mathfrak{A}} \downarrow \cong & & \cong \downarrow K_{\mathfrak{B}} \\ & \xrightarrow{T_A} & \end{array}$$

Wobei  $f = L_{\mathfrak{B}\mathfrak{A}} = K_{\mathfrak{B}}^{-1} \cdot T_A \cdot K_{\mathfrak{A}}$

Aber

1)  $K_{\mathfrak{B}}(\text{Im}(f)) = \text{Im}(T_A)$

2)  $K_{\mathfrak{B}} : \text{Im}(f) \xrightarrow{\cong} \text{Im}(T_A)$

Beweis fertig mit Lemma 1(1). □

Allgemein:

**Lemma 3.7.8.** 
$$\begin{array}{ccc} \text{Es sei } Ker(f) \subseteq V & \xrightarrow{f} & W \supseteq Im(f) \\ \varphi \downarrow \cong & \downarrow \varphi & \downarrow \psi \quad \downarrow \cong \\ Ker(f') \subseteq V' & \xrightarrow{f'} & W' \supseteq Im(f') \end{array}$$

ein kommutatives Diagramm,

dh.  $\psi \circ f = f' \circ \varphi$  sind  $\varphi$  und  $\psi$  Isomorphismen, dann gilt:

1.  $Im(f)$  wird von  $\psi$  isomorph auf das  $Im(f')$  abgebildet.
2.  $Ker(f)$  wird von  $\varphi$  isomorph auf den  $Ker(f')$  abgebildet.

*Beweis.* zu 2.

$$v \in V, f(v) = 0 \Leftrightarrow \psi(f(v)) = 0 = f'(\varphi(v))$$

$$v \in Ker(f) \Rightarrow \varphi(v) \in Ker(f')$$

Umgekehrt  $v' \in Ker(f')$  also  $f'(v') = 0$ .

Weil  $\varphi$  surjektiv ist, ist  $v' = \varphi(v)$  für ein  $v \in V$ .

$$\text{Dh. } 0 = f'(\varphi(v)) = \psi(f(v)).$$

Weil  $\psi$  monomorph ist, folgt  $f(v) = 0$ , also  $v \in Ker(f)$ . □

**Lemma 3.7.9.** 
$$\begin{array}{ccc} V & \xrightarrow{f} & W \xrightarrow[\psi]{\cong} W \\ \varphi \uparrow \cong & & \\ V & & \end{array}$$

1.  $Ker(f) = Ker(\psi \circ f)$  (aber i.A.  $Im(f) \neq Im(\psi \circ f)$ )
2.  $Im(f \circ \varphi) = Im(f)$  (aber i.A.  $Ker(f) \neq Ker(f \circ \varphi)$ )

*Bemerkung.* zu 4.2

a)  $V$  fest,  $\mathbb{K}$  fest

$$\begin{array}{ccc} \downarrow & W \rightarrow & Hom_{\mathbb{K}}(V, W) \\ V \downarrow \varphi & & \downarrow \varphi_* = Hom_{\mathbb{K}}(V, \varphi) \\ \varphi \circ \downarrow & Y \rightarrow & Hom_{\mathbb{K}}(V, Y) \end{array}$$

Wieder erhält man ein Funktor.

kovariant:  $W = Y : (id_W)_* = id_{Hom_{\mathbb{K}}(V,W)}$  (induzierte Abbildung)  
 $id_* = id$  (aber nicht die gleiche Identität!)

b)  $W$  fest,  $\mathbb{K}$  fest

$$\begin{array}{c} \swarrow \circ \psi \\ X \rightarrow Hom_{\mathbb{K}}(X, W) \ni f \circ \psi = \psi^*(f) \end{array}$$

$$\begin{array}{ccc} W & \downarrow \psi & \uparrow \psi^* = Hom_{\mathbb{K}}(\psi, W) \\ \swarrow \circ f & V \rightarrow Hom_{\mathbb{K}}(V, W) \ni f & \end{array}$$

Ein Funktor  $VR_{/\mathbb{K}} \rightarrow VR_{/\mathbb{K}}$

Kontravariant

$$1. X = V \quad (id_V)^* = id_{Hom_{\mathbb{K}}(V,W)}$$

$$2. (\varphi_2 \circ \varphi_1)^* = \varphi_1^* \circ \varphi_2^*$$

=====

# 4 Matrizen

## 4.1 Rechnen mit Matrizen

Mit  $\mathbb{K}$  bezeichnen wir wie immer einen Körper, mit  $M = \text{Mat}_{m,n}(\mathbb{K})$  die Menge der  $m \times n$  Matrizen über  $\mathbb{K}$ . Für eine Matrix schreiben wir  $A = (a_{ij})$ , mit dem *Zeilenindex*  $i = 1, \dots, m$  und dem *Spaltenindex*  $j = 1, \dots, n$ .

### Addition

$$\begin{aligned} + : M \times M &\longrightarrow M \\ (A, B) = ((a_{ij}), (b_{ij})) &\longmapsto C = (c_{ij}) = (a_{ij} + b_{ij}) \end{aligned}$$

Die Matrix mit allen Einträgen gleich Null heißt *Nullmatrix*  $0_{m,n} = 0$ .

Es gilt:

- 1)  $A + B = B + A$
- 2)  $A + (B + C) = (A + B) + C$
- 3)  $A + 0 = A = 0 + A$
- 4) zu jedem  $A \in M$  gibt es ein Negatives  $-A = (-a_{ij})$  mit  $A + (-A) = 0$

### Skalierung

$$\begin{aligned} \mathbb{K} \times M &\longrightarrow M \\ (\lambda, A) &\longmapsto \lambda A = (\lambda a_{ij}) \end{aligned}$$

Es gilt:

- 5)  $\lambda(\mu A) = (\lambda\mu)A$
- 6)  $\lambda(A + B) = \lambda A + \lambda B$   $(\lambda + \mu)A = \lambda A + \mu A$
- 7)  $1 \cdot A = A$ ;  $(-1) \cdot A = -A$
- 8)  $0 \cdot A = 0$ ;  $\lambda \cdot 0 = 0$

### Einheitsmatrizen und Elementarmatrizen

Matrizen der Form  $\tilde{E}^{kl} = (\tilde{e}_{ij}^{kl})$  ( $i = 1, \dots, m; j = 1, \dots, n; k = 1, \dots, m; l = 1, \dots, n$ ) mit

$$\tilde{e}_{ij}^{kl} = \begin{cases} 1 & \text{falls } (i, j) = (k, l) \\ 0 & \text{falls } (i, j) \neq (k, l) \end{cases}$$

heißen *Einheitsmatrizen*.

$$\tilde{E}^{kl} = \begin{matrix} & & & \boxed{l} \\ \boxed{k} & \begin{pmatrix} 0 & \vdots & & \\ \dots & 1 & & \\ 0 & & & 0 \end{pmatrix} \end{matrix}$$

Matrizen der Form  $E^{kl} = \mathbb{1} + \tilde{E}^{kl}$  ( $k \neq l$ ) heißen *Elementarmatrizen*.

**Satz 4.1.1.** (i)  $\text{Mat}_{m,n}(\mathbb{K})$  ist ein  $\mathbb{K}$ -Vektorraum.

(ii)  $\mathcal{B} = \{\tilde{E}^{kl} | k = 1, \dots, m; l = 1, \dots, n\}$  ist eine Basis.

(iii)  $\dim_{\mathbb{K}}(\text{Mat}_{m,n}(\mathbb{K})) = m \cdot n$

*Beweis.* (i) folgt aus 1) bis 8).

(ii)

$$A = (a_{ij}) = \begin{matrix} a_{11}\tilde{E}^{11} & +a_{12}\tilde{E}^{12} & +\dots & +a_{1n}\tilde{E}^{1n} \\ +a_{21}\tilde{E}^{21} & +\dots & & \\ \vdots & & & \\ +a_{m1}\tilde{E}^{m1} & +\dots & & +a_{mn}\tilde{E}^{mn} \end{matrix} = \sum_{i,j} a_{ij}\tilde{E}^{ij}$$

Also ist  $\mathcal{B}$  ein Erzeugendensystem. Für die lineare Unabhängigkeit von  $\mathcal{B}$  schreibe man eine mutmaßliche Relation

$$0 = \begin{matrix} \lambda_{11}\tilde{E}^{11} & +\dots & +\lambda_{1n}\tilde{E}^{1n} \\ \vdots & & \\ +\lambda_{m1}\tilde{E}^{m1} & +\dots & +\lambda_{mn}\tilde{E}^{mn} \end{matrix}$$

mit  $m \cdot n$  Termen. Also erhalten wir  $m \cdot n$  Gleichungen für jede Stelle  $(i, j)$ :

$$0 = \lambda_{ij} \cdot \tilde{e}_{ij}^{ij} = \lambda_{ij}$$

Also sind alle  $\lambda_{ij} = 0$ .

(iii) folgt aus (ii).

□

### Multiplikation von Matrizen

$$\begin{matrix} \text{Mat}_{m,k}(\mathbb{K}) \times \text{Mat}_{k,n}(\mathbb{K}) & \xrightarrow{\quad} & \text{Mat}_{m,n}(\mathbb{K}) \\ A, B & \longmapsto & A \cdot B = AB =: C \\ (a_{ij}), (b_{jl}) & & \longmapsto (c_{il}) \end{matrix}$$

mit  $c_{il} := \sum_{s=1}^k a_{is}b_{sl}; i = 1, \dots, m; l = 1, \dots, n$ .

Es gilt:

- 1)  $A \cdot (B \cdot C) = (A \cdot B) \cdot C$
- 2)  $A \cdot (B + C) = AB + AC$   
 $(A + B) \cdot C = AC + BC$
- 3)  $\lambda(A \cdot B) = (\lambda A)B = A(\lambda B)$
- 4)  $\underset{m,k}{0} \cdot \underset{k,n}{A} = \underset{m,n}{0}; \underset{m,k}{A} \cdot \underset{k,n}{0} = \underset{m,n}{0}$

**Lemma 4.1.2.** i) Ist die  $i$ -te Zeile  $Z_i(A) = 0$ , so auch die  $i$ -te Zeile  $Z_i(AB)$ , für alle  $B$ .

ii) Ist die  $j$ -te Spalte  $S_j(B) = 0$ , so auch  $S_j(AB)$ , für alle  $A$ .

**Achtung!!!** Das Matrizenprodukt ist im Allgemeinen **nicht** kommutativ:

$$AB \neq BA$$

**Beispiel 4.1.3.**

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ Spiegelung an der } y\text{-Achse}$$

$$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ Spiegelung an der } x\text{-Achse}$$

$$AB = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ Spiegelung an der Hauptdiagonalen}$$

$$BA = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \text{ Spiegelung an der Nebendiagonalen}$$

**Spezielle Produkte**

a)  $m = 1, n = 1, k$  beliebig: Skalarprodukt  $\langle A, B \rangle$

$$\underbrace{(a_1, \dots, a_k)}_A \cdot \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}}_B = \underbrace{a_1 b_1 + \dots + a_k b_k}_C$$

b)  $k = 1; m, n$  beliebig:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}_A (b_1, \dots, b_n)_B = \begin{pmatrix} a_1 b_1 & \dots & a_1 b_n \\ \vdots & \ddots & \vdots \\ a_m b_1 & \dots & a_m b_n \end{pmatrix}_C$$

mit  $\text{rg}(C) = 1$

c)  $n = 1; m, k$  beliebig,  $A \in \text{Mat}_{m,k}(\mathbb{K})$

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

Lineare Gleichungssysteme mit  $m$  Gleichungen und  $k$  Unbekannten.

*Bemerkung.* Eine  $(n \times n)$ -Matrix heißt *quadratisch*.

**Einsmatrix**

Die quadratische  $(n \times n)$ -Matrix der Form

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

mit den Einträgen 1 entlang der Diagonale und 0 sonst, heißt *Einsmatrix*  $\mathbb{1} = \mathbb{1}_n$ . Es gilt (für  $A \in \text{Mat}_{mn}(\mathbb{K})$ ):

1)

$$\begin{matrix} \mathbb{1}_m & \cdot & A & = & A \\ m \times m & & m \times n & & m \times n \end{matrix}$$

2)

$$\begin{matrix} A & \cdot & \mathbb{1}_n & = & A \\ m \times n & & n \times n & & m \times n \end{matrix}$$

Also ist  $\mathbb{1}$  ein beidseitiges neutrales Element.

**Achtung!** Nicht jede  $(n \times n)$ -Matrix besitzt ein Inverses!

**Definition 4.1.4.** Sei  $A \in \text{Mat}_{m,n}(\mathbb{K})$ .

- 1) Eine Matrix  $B \in \text{Mat}_{n,m}(\mathbb{K})$  heißt *Rechtsinverses* zu  $A$ , falls gilt:  $A \cdot B = \mathbb{1}_m$ .
- 2) Eine Matrix  $C \in \text{Mat}_{n,m}(\mathbb{K})$  heißt *Linksinverses* zu  $A$ , falls gilt:  $C \cdot A = \mathbb{1}_n$ .
- 3) Eine quadratische Matrix  $A \in \text{Mat}_{n,n}(\mathbb{K})$  heißt *invertierbar*, falls es ein  $\tilde{A} \in \text{Mat}_{n,n}(\mathbb{K})$  gibt mit  $A \cdot \tilde{A} = \tilde{A} \cdot A = \mathbb{1}_n$ .

*Bemerkung.* Existiert im Fall 3) ein Inverses, so ist es eindeutig bestimmt. (Aber Rechts- und Linksinverse sind *nicht* eindeutig bestimmt.)

*Beweis.* Seien  $\tilde{A}, \tilde{\tilde{A}}$  zwei Inverse zu  $A$ , also  $A\tilde{A} = \mathbb{1}$ ,  $A\tilde{\tilde{A}} = \mathbb{1}$ . Nach Distributivität gilt:

$$A(\tilde{A} - \tilde{\tilde{A}}) = A\tilde{A} - A\tilde{\tilde{A}} = 0$$

Wenn wir diese Gleichung nun von links mit  $\tilde{A}$  multiplizieren, erhalten wir:

$$0 = \tilde{A} \cdot 0 = \tilde{A}A(\tilde{A} - \tilde{\tilde{A}}) = \mathbb{1} \cdot (\tilde{A} - \tilde{\tilde{A}})$$

. Damit folgt  $\tilde{A} = \tilde{\tilde{A}}$ . □

**Notation** Ist  $A$  invertierbar, so nennen wir das (eindeutig bestimmte) Inverse  $A^{-1}$ .

**Lemma 4.1.5.** *i) Ist  $A$  invertierbar, so auch  $A^{-1}$  und  $(A^{-1})^{-1} = A$ .*

*ii) Sind  $A$  und  $B$  invertierbar, so auch  $AB$  und  $(AB)^{-1} = B^{-1}A^{-1}$ . (Man beachte die Reihenfolge!)*

*iii) Ist  $A$  invertierbar und  $\lambda \in \mathbb{K}, \lambda \neq 0$ , so auch  $\lambda A$  und  $(\lambda A)^{-1} = \frac{1}{\lambda}A^{-1}$ .*

*Beweis.* klar. □

**Beispiel 4.1.6.**  $(A_1 \cdots A_r)^{-1} = A_r^{-1} \cdots A_1^{-1}$

**Satz 4.1.7.** Eine  $(n \times n)$ -Matrix  $A$  ist invertierbar genau dann, wenn ihr Rang  $\text{rg}(A) = n$ , also maximal.

**Definition 4.1.8** (Transponieren).

$$\begin{aligned} \top : \text{Mat}_{m,n}(\mathbb{K}) &\longrightarrow \text{Mat}_{n,m}(\mathbb{K}) \\ (a_{ij}) = a &\longmapsto A^\top := (a_{ji}) \\ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} &\longmapsto \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{nm} \end{pmatrix} \end{aligned}$$

Es gilt:

- 1)  $(A^\top)^\top = A$
- 2)  $(A + B)^\top = A^\top + B^\top$
- 3)  $(\lambda A)^\top = \lambda \cdot A^\top$
- 4)  $0^\top = 0$
- 5)  $\mathbb{1}_n^\top = \mathbb{1}_n$
- 6)  $(AB)^\top = B^\top A^\top$
- 7) Ist  $A$  invertierbar, so auch  $A^\top$  mit  $(A^\top)^{-1} = (A^{-1})^\top$ .

**Beispiel 4.1.9.**

$$\begin{array}{ll}
 x = (x_1, \dots, x_n) \in \mathbb{K}^n & \text{Zeilenvektor} \\
 x^\top = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \text{Spaltenvektor} \\
 x \cdot y^\top = \langle x, y \rangle & x, y \text{ Zeilenvektoren} \\
 x^\top \cdot y = \langle x, y \rangle & x, y \text{ Spaltenvektoren}
 \end{array}$$

## 4.2 Matrizen und lineare Abbildungen

Wir haben bereits gesehen, dass die Multiplikation einer  $(m \times n)$ -Matrix  $C$  mit einem  $(n \times 1)$ -Spaltenvektor  $x \in K^n$  einen  $(m \times 1)$ -Spaltenvektor ergibt und dass dies eine lineare Abbildung ist:

$$\begin{aligned}
 T_C : K^n &\rightarrow K^m \\
 x &\mapsto Cx
 \end{aligned}$$

Rechenregeln:

1.  $T_C(0) = 0$
2.  $T_C(\lambda x) = \lambda T_C(x)$
3.  $T_C(x + x') = T_C(x) + T_C(x')$

Sei  $V$  ein  $K$ -Vektorraum mit geordneter Basis  $A = (a_1, \dots, a_n)$ ,  $\dim V = n$ ,  $W$  ein  $K$ -Vektorraum mit geordneter Basis  $B = (b_1, \dots, b_m)$ ,  $\dim W = m$  und  $f : V \rightarrow W$  eine lineare Abbildung.

Dann ist  $f$  durch  $f(A)$  vollkommen bestimmt, also durch  $f(a_1), \dots, f(a_n) \in W$ .

Jedes  $f(a_j)$  ist bestimmt durch seine Koeffizienten bzgl. der Basis  $B$ :

$$f(a_j) = \sum_{i=1}^m \lambda_{ij} b_i$$

Also ist  $f$  durch die  $\lambda_{ij}$  vollkommen bestimmt. Diese  $\lambda_{ij}$  fasse man zu einer Matrix  $\Lambda = (\lambda_{ij}) \in \text{Mat}_{m,n}(K)$  zusammen und notiere:

1.  $K_B(f(a_j)) = (\lambda_{1j}, \dots, \lambda_{mj}) = S_j(\Lambda) = \Lambda e_j$  (j-te Spalte)
2.  $a_j = K_A^{-1}(e_j)$

Damit haben wir  $K_B \circ f = T_\Lambda \circ K_A$ :

$$\begin{array}{ccc}
 V & \xrightarrow{f} & W \\
 K_A \downarrow & & \downarrow K_B \\
 K^n & \xrightarrow{T_\Lambda} & K^m
 \end{array}
 \qquad
 \begin{array}{ccc}
 a_j & \longmapsto & f(a_j) \\
 \downarrow & & \downarrow \\
 e_j & \longmapsto & S_j(\Lambda)
 \end{array}$$

$$\begin{aligned}
 \implies f &= K_B^{-1} \circ T_\Lambda \circ K_A \\
 T_\Lambda &= K_B \circ f \circ K_A^{-1}
 \end{aligned}$$

Bei festgewählten Basen  $A$  und  $B$  bestimmt  $f$  eine Matrix  $\Lambda$  und damit  $T_\Lambda$  und umgekehrt bestimmt  $\Lambda$  das  $T_\Lambda$  und damit  $f$ .

**Definition 4.2.1.** Wir definieren zwei Funktionen:

$$M_{BA} : \text{Hom}_K(V, W) \rightarrow \text{Mat}_{m,n}(K)$$

$$f \mapsto C = (c_{ij})$$

mit  $c_{ij} = K_B(f(a_j))$  und

$$L_{BA} : \text{Mat}_{m,n}(K) \rightarrow \text{Hom}_K(V, W)$$

$$C \mapsto f = K_B^{-1} \circ T_C \circ K_A$$

**Beispiel 4.2.2.**

1.  $f = 0 : M_{BA}(0) = 0$   
 $C = 0 : L_{BA}(0) = 0$
2.  $V = W, A = B:$   
 $f = \text{id} : M_{AA}(\text{id}) = \mathbb{1}$   
 $C = \mathbb{1} : L_{AA}(\mathbb{1}) = \text{id}$
3.  $V = W = \mathbb{R}^2, A = (e_1, e_2), B = (e_1, e_2 + e_1), f = \text{id} :$   
 $M_{BA}(\text{id}) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$
4.  $V = W = \mathbb{R}^2, A = (e_1, e_2), B = (e_1, e_2 + e_1), C = \mathbb{1} :$   
 $L_{BA}(\mathbb{1}) = ((x, y) \mapsto (x, -x + y))$  (Scherung)
5.  $V = K^n, W = K^m, A = (e_1, \dots, e_n), B = (e_1, \dots, e_m) :$   
 $M_{BA}(T_C) = C, L_{BA}(C) = T_C$ , denn  $K_A = \text{id}, K_B = \text{id}$

**Satz 4.2.3.** Sei  $A$  bzw.  $B$  eine Basis für  $V$  bzw.  $W$ .  $M_{BA}$  und  $L_{BA}$  sind zueinander invers und linear, d.h. sie sind Isomorphismen von Vektorräumen.

$$\text{Hom}(V, W) \begin{matrix} \xrightarrow{M_{BA}} \\ \xleftarrow{L_{BA}} \end{matrix} \text{Mat}_{m,n}(K)$$

Seien  $V = K^n, W = K^m$  und  $A$  und  $B$  die Standardbasen von  $V, W$ . Nun betrachte man die Funktionen

$$L_{BA} = T : \text{Mat}_{n,m}(K) \rightarrow \text{Hom}(K^n, K^m)$$

$$C \mapsto K_B^{-1} \circ T_C \circ K_A = T_C$$

**Lemma 4.2.4.**  $T$  ist linear und multiplikativ, d.h.  $T_0 = 0, T_{\lambda C} = \lambda T_C, T_{A+B} = T_A + T_B$ , sowie für  $n = m$  gilt  $T_{\mathbb{1}} = \text{id}$  und  $T_{A^{-1}} = T_A^{-1}$ , als auch  $T_{AB} = T_A T_B$  für passende  $A$  und  $B$ .

Die Beweise reduzieren sich auf Rechenregeln für Matrizen.

Es sei  $\varphi : W \rightarrow Y$  eine feste lineare Abbildung. Dann haben wir die Postkomposition

$$V \begin{matrix} \xrightarrow{f} W \xrightarrow{\varphi} Y \\ \searrow \varphi \circ f \nearrow \end{matrix}$$

und können dies als Funktion

$$\varphi_* = \text{Hom}_K(V, \varphi) : \text{Hom}_K(V, W) \rightarrow \text{Hom}_K(V, Y)$$

$$f \mapsto \varphi \circ f$$

betrachten.

Entsprechend sei  $\psi : X \rightarrow V$  eine feste lineare Abbildung. Dann haben wir die Präkomposition

$$X \begin{matrix} \xrightarrow{\psi} V \xrightarrow{f} W \\ \searrow f \circ \psi \nearrow \end{matrix}$$

und können dies als Funktion

$$\begin{aligned}\psi^* = \text{Hom}_K(\psi, W) : \text{Hom}_K(V, W) &\rightarrow \text{Hom}_K(X, W) \\ f &\mapsto f \circ \psi\end{aligned}$$

betrachten.

**Lemma 4.2.5.**  $\varphi_* : \text{Hom}_K(V, W) \rightarrow \text{Hom}_K(V, Y)$  ist linear:

1.  $\varphi_*(0) = 0$
2.  $\varphi_*(\lambda f) = \lambda \varphi_*(f)$
3.  $\varphi_*(f + g) = \varphi_*(f) + \varphi_*(g)$
- 1':  $\varphi \circ 0 = 0$
- 2':  $\varphi \circ (\lambda f) = \lambda(\varphi \circ f)$
- 3':  $\varphi \circ (f + g) = (\varphi \circ f) + (\varphi \circ g)$

**Lemma 4.2.6.**  $\psi^* : \text{Hom}_K(V, W) \rightarrow \text{Hom}_K(V, Y)$  ist linear:

1.  $\psi^*(0) = 0$
2.  $\psi^*(\lambda f) = \lambda \psi^*(f)$
3.  $\psi^*(f + g) = \psi^*(f) + \psi^*(g)$
- 1':  $0 \circ \psi = 0$
- 2':  $(\lambda f) \circ \psi = \lambda(f \circ \psi)$
- 3':  $(f + g) \circ \psi = (f \circ \psi) + (g \circ \psi)$

*Beweis.* (Lemma 4.2.5).

$$\begin{aligned}\varphi_*(0) &= \varphi \circ 0 = 0 \\ (\varphi_*(\lambda f))(x) &= (\varphi \circ (\lambda f))(x) \\ &= \varphi(\lambda f(x)) = \lambda \varphi(f(x)) \\ &= \lambda((\varphi \circ f)(x)) = \lambda(\varphi_*(f)(x)) \\ (\varphi_*(f + g))(x) &= (\varphi \circ (f + g))(x) = \varphi((f + g)(x)) \\ &= \varphi(f(x) + g(x)) = \varphi(f(x)) + \varphi(g(x)) \\ &= (\varphi \circ f)(x) + (\varphi \circ g)(x) = \varphi_*(f)(x) + \varphi_*(g)(x)\end{aligned}$$

□

*Beweis.* (Satz 4.2.3). Sei  $M = M_{BA}$ ,  $L = L_{BA}$ ,  $f \in \text{Hom}(V, W)$  und  $x \in V$ .

$$\begin{aligned}L(M(f)) &= K_B^{-1} \circ T_{M(f)} \circ K_A \\ &= K_B^{-1} \circ K_B \circ f \circ K_A^{-1} \circ K_A = f \\ M(L(C))(x) &= M(K_B^{-1} \circ T_C \circ K_A)(x) \\ &= K_B(K_B^{-1} \circ T_C \circ K_A)K_A^{-1}(x) = T_C(x) = Cx \\ \implies M(L(C)) &= C\end{aligned}$$

Also  $L \circ M = \text{id}$  und  $M \circ L = \text{id}$ .

Es genügt, die Linearität von  $L$  zu zeigen. Dies folgt mithilfe der gerade bewiesenen Lemmata:

$$\begin{aligned} L(\lambda C) &= K_B^{-1} \circ T_{\lambda C} \circ K_A \\ &= K_B^{-1} \circ (\lambda T_C) \circ K_A \\ &= \lambda(K_B^{-1} \circ T_C \circ K_A) \\ &= \lambda L(C) \end{aligned}$$

$$\begin{aligned} L(A + B) &= K_B^{-1} \circ T_{A+B} \circ K_A \\ &= K_B^{-1} \circ (T_A + T_B) \circ K_A \\ &= K_B^{-1} \circ T_A \circ K_A + K_B^{-1} \circ T_B \circ K_A \\ &= L(A) + L(B) \end{aligned} \quad \square$$

**Basis für  $\text{Hom}_K(V, W)$**

Da  $L_{BA}$  ein Isomorphismus ist, können wir die Basis  $\tilde{E}^{kl}$  der StandardEinheitsmatrizen nach  $\text{Hom}(V, W)$  schicken und erhalten

$$f^{kl} : V \rightarrow W, a_j \mapsto \begin{cases} b_k & , \text{ falls } j = l \\ 0 & , \text{ falls } j \neq l \end{cases}$$

Nach Konstruktion gilt nun

$$\begin{aligned} L_{BA}(\tilde{E}^{kl}) &= f^{kl} \\ M_{BA}(f^{kl}) &= \tilde{E}^{kl} \end{aligned}$$

In Lemma 4.2.4 haben wir für die Funktion  $T$  auch schon multiplikative Eigenschaften aufgelistet, daraus folgt

$$\begin{aligned} M_{AA}(\text{id}) &= \mathbb{1} \\ L_{AA}(\mathbb{1}) &= \text{id} \end{aligned}$$

Für die multiplikativen Eigenschaften von  $M$  und  $L$  betrachten wir drei Vektorräume  $V, W$  und  $Z$  mit geordneten Basen  $A \subseteq V, B \subseteq W$  und  $C \subseteq Z$  Dann haben wir

$$\begin{aligned} \text{Hom}(W, Z) \times \text{Hom}(V, W) &\rightarrow \text{Hom}(V, Z) \\ \text{Mat}_{l,m}(K) \times \text{Mat}_{m,n}(K) &\rightarrow \text{Mat}_{l,n}(K) \end{aligned}$$

$$\begin{aligned} f, g &\mapsto f \circ g \\ A, B &\mapsto A \cdot B \end{aligned}$$

**Satz 4.2.7.**

$$\begin{aligned} M_{AA}(\text{id}) &= \mathbb{1} \\ L_{AA}(\mathbb{1}) &= \text{id} \end{aligned}$$

$$\begin{aligned} M_{CA}(f \circ g) &= M_{CB}(f) \cdot M_{BA}(g) \\ L_{CA}(A \cdot B) &= L_{CB}(A) \circ L_{BA}(B) \end{aligned}$$

*Beweis.* Die ersten beiden Ausgaben wurden bereits bewiesen, bei den anderen genügt es, diese für  $L$  zu beweisen.

$$\begin{aligned} L_{CA}(AB) &= K_C^{-1} \circ T_{AB} \circ K_A \\ &= K_C^{-1} \circ T_A \circ T_B \circ K_A \\ &= K_C^{-1} \circ T_A \circ K_B \circ K_B^{-1} \circ T_B \circ K_A \\ &= L_{CB}(A) \circ L_{BA}(B) \end{aligned} \quad \square$$

**Korollar 4.2.8.**  $f : V \rightarrow W$  ist genau dann ein Isomorphismus, wenn  $M_{BA}(f)$  invertierbar ist; in diesem Fall ist  $M_{BA}(f^{-1}) = M_{BA}(f)^{-1}$ .

$C \in \text{Mat}_{m,n}(K)$  ist genau dann invertierbar, wenn  $L_{BA}(C)$  ein Isomorphismus ist; in diesem Fall ist  $L_{AB}(C^{-1}) = L_{BA}(C)^{-1}$ , und speziell ist  $L_{AB}(\mathbb{1}) = L_{BA}(\mathbb{1})^{-1}$ .

### 4.3 Basiswechsel

Angenommen, wir haben bislang einer linearen Abbildung  $f : V \rightarrow W$  bzgl. der Basen  $A \subseteq V$  und  $B \subseteq W$  eine Matrix zugeordnet, nämlich  $C = M_{BA}(f)$ . Wie ändert sich  $C$ , wenn wir andere Basen  $A'$  und  $B'$  nehmen?

Wir benutzen Satz 4.2.7 zweimal:

$$\begin{array}{ccc} W & \xleftarrow{f} & V \\ \text{id} \downarrow & & \uparrow \text{id} \\ W & \xleftarrow{f} & V \end{array} \quad \begin{array}{ccc} B & \xleftarrow{M_{BA}(f)} & A \\ M_{B'B}(\text{id}) \downarrow & & \uparrow M_{AA'}(\text{id}) \\ B' & \xleftarrow{M_{B'A'}(f)} & A' \end{array}$$

$$\begin{aligned} C' &= M_{B'A'}(f) = M_{B'A'}(\text{id} \circ f \circ \text{id}) \\ &= M_{B'B}(\text{id}) \cdot M_{BA}(f) \cdot M_{AA'}(\text{id}) \\ &= M_{B'B}(\text{id}) \cdot M_{BA}(f) \cdot M_{A'A}(\text{id})^{-1} \\ &= \Omega_{B'B} \cdot C \cdot \Omega_{A'A}^{-1} \end{aligned}$$

Die Matrix  $\Omega = \Omega_{A'A}$  heißt Basiswechsellmatrix für den Wechsel von  $A$  nach  $A'$ . Ihre  $j$ -te Spalte  $S_j(\Omega_{A'A})$  enthält die Koeffizienten, um  $a_j$  durch die  $a'_1, \dots, a'_k$  darzustellen:

$$\begin{aligned} a_j &= \sum_{k=1}^n \omega_{kj} \cdot a'_k \\ K_{A'}(a_j) &= (\omega_{1j}, \dots, \omega_{nj}) = S_j(\Omega) \end{aligned}$$

**Proposition 4.3.1.**

1.  $\Omega_{AA} = \mathbb{1}$
2.  $\Omega_{A'A} = \Omega_{AA'}^{-1}$
3.  $\Omega_{A''A'} \cdot \Omega_{A'A} = \Omega_{A''A}$
4. Es sei  $A$  eine Basis von  $V$  und  $D$  eine invertierbare Matrix in  $\text{Mat}_n(K)$ . Dann gibt es eine Basis  $A'$  von  $V$  mit  $\Omega_{A'A} = D$ .

*Beweis.*  $\varphi = L_{AA}(D) : V \rightarrow V$  ist ein Automorphismus. Also ist  $A' = (\varphi^{-1}(a_1), \dots, \varphi^{-1}(a_n))$  wieder eine Basis, wenn  $A = (a_1, \dots, a_n)$  war. Dann haben wir

$$\begin{aligned} D &= M_{AA}(\varphi) = M_{AA'}(\varphi) \cdot M_{A'A}(\text{id}) \\ &= M_{A'A}(\varphi^{-1}) \cdot \Omega_{A'A} \\ &= \mathbb{1} \cdot \Omega_{A'A} = \Omega_{A'A} \end{aligned} \quad \square$$

### Normalformen

Wir werden noch sehen, dass wir die zu einer linearen Abbildung  $f : V \rightarrow W$  bzgl. zweier Basen  $A \subseteq V$  und  $B \subseteq W$  gehörende Matrix  $C = M_{BA}(f)$  durch geschickte Wahl von  $A$  und  $B$  auf eine sehr einfache Form bringen können.

Anders gesagt, multipliziert man eine Matrix  $C$  von links und rechts mit invertierbaren Matrizen  $R$  und  $S$ , dann kann man  $C' = RCS$  auf sehr einfache Form

$$C' = \begin{pmatrix} \mathbb{1}_r & 0_{r,n-r} \\ 0_{m-r,r} & 0_{m-r,n-r} \end{pmatrix}$$

bringen, wobei  $r = \text{rg}(f) = \text{rg}(C)$  der Rang von  $C$  ist.

Interessanter ist, wenn  $C$  eine  $n \times n$ -Matrix ist, die also zu einem Endomorphismus  $f : V \rightarrow V$  bzgl. einer Basis  $A$  gehört, also  $C = M_{AA}(f)$ . Dann kann man sich auf simultane Basiswechsel beschränken und versucht, durch geschickte Wahl von  $A$  die Matrix  $C$  möglichst einfach zu machen.

Anders gesagt, man multipliziert  $C$  von links mit  $R$  und von rechts mit  $R^{-1}$ , also  $C' = RCR^{-1}$ . Dies nennt man eine Konjugation. Daran kann man nun viel mehr ablesen.

Und als drittes wird man dann noch die zulässigen  $R$  einschränken und nur mit speziellen  $R$  konjugieren.

**Lemma 4.3.2.** *Es sei  $f : V \rightarrow W$  linear und es seien  $\psi : V \rightarrow V$  und  $\phi : W \rightarrow W$  Automorphismen. Dann gilt:*

$$(i) \ker(\phi \circ f \circ \psi) = \psi^{-1}(\ker(f))$$

$$(ii) \text{im}(\phi \circ f \circ \psi) = \phi(\text{im}(f))$$

**Lemma 4.3.3.** *Sei  $M \in \text{Mat}_{m,n}(\mathbb{K})$ ,  $A \in \text{Mat}_{m,m}(\mathbb{K})$  und  $B \in \text{Mat}_{n,n}(\mathbb{K})$  sowie  $A$  und  $B$  invertierbar. Dann gilt:*

$$(i) \mathcal{L}(AMB|0) = \ker(T_{AMB}) = T_B^{-1}(\mathcal{L}(M|0)) = T_{B^{-1}}(\mathcal{L}(M|0)) = B^{-1}(\mathcal{L}(M|0)) \\ := \{B^{-1}x \mid x \in \mathcal{L}(M|0)\}$$

$$(ii) \mathcal{W}(AMB) = T_A(\mathcal{W}(M)) = A\mathcal{W}(M) = \{y \in \mathbb{K}^m \mid \mathcal{L}(AMB|y) \neq \emptyset\}$$

### Beweis:

Das erste Lemma war eine Übungsaufgabe, das zweite folgt aus dem ersten Lemma mit Isomorphismen

$$M_{\mathfrak{B}\mathfrak{A}} : \text{Hom}_{\mathbb{K}}(V, W) \xrightarrow{\cong} \text{Mat}_{m,n}(\mathbb{K}) \quad : L_{\mathfrak{B}\mathfrak{A}}$$

**Korollar 4.3.4** ( $\rightarrow$  Übungsaufgabe 55).  $(i) \text{rg}(\phi \circ f \circ \psi) = \text{rg}(f)$

$$(ii) \text{rg}(AMB) = \text{rg}(M)$$

**Beweis:** Wir wissen bereits aus Lemma 1:

$\ker(\phi \circ f \circ \psi) = \psi^{-1}(\ker(f))$ , also ist  $\dim(\ker(\phi \circ f \circ \psi)) = \dim(\psi^{-1}(\ker(f))) = \dim(\ker(f))$ , weil  $\psi^{-1}$  ein Isomorphismus ist. Weiter gilt nach der Dimensionsformel:

$$n = \dim(V) = \dim(\text{im}(f)) + \dim(\ker(f)) = \dim(\text{im}(\phi \circ f \circ \psi)) + \dim(\ker(\phi \circ f \circ \psi)),$$

daraus folgt sofort die Behauptung  $\text{rg}(f) = \text{rg}(\phi \circ f \circ \psi)$ . □

## 4.4 Spaltenumformungen

Wir kennen für Zeilen folgende Umformungen:

$\mathfrak{M}_i[\lambda] :$	$Mat_{m,n}(\mathbb{K}) \rightarrow Mat_{m,n}(\mathbb{K})$	Multiplikation der $i$ -ten Zeile mit $\lambda$
$\mathfrak{A}_{ij} :$	$Mat_{m,n}(\mathbb{K}) \rightarrow Mat_{m,n}(\mathbb{K})$	Addition der $j$ -ten zur $i$ -ten Zeile
$\mathfrak{B}_{ij} :$	$Mat_{m,n}(\mathbb{K}) \rightarrow Mat_{m,n}(\mathbb{K})$	Vertauschen der $i$ -ten und $j$ -ten Zeile

Analog gilt für Spaltenumformungen:

$\mathfrak{M}'_i[\lambda] :$	$Mat_{m,n}(\mathbb{K}) \rightarrow Mat_{m,n}(\mathbb{K})$	Multiplikation der $i$ -ten Spalte mit $\lambda$
$\mathfrak{A}'_{ij} :$	$Mat_{m,n}(\mathbb{K}) \rightarrow Mat_{m,n}(\mathbb{K})$	Addition der $j$ -ten zur $i$ -ten Spalte
$\mathfrak{B}'_{ij} :$	$Mat_{m,n}(\mathbb{K}) \rightarrow Mat_{m,n}(\mathbb{K})$	Vertauschen der $i$ -ten und $j$ -ten Spalte

### Voller Gaußalgorithmus

**Satz 4.4.1.** Jede Matrix  $A \in Mat_{m,n}(\mathbb{K})$  mit  $rg(A) = r$  kann durch Zeilen- und Spaltenumformungen in eine Form wie  $\begin{pmatrix} \mathbb{1} & 0 \\ 0 & 0 \end{pmatrix}$  gebracht werden.

**Beweis:**

- (1) Der einfache Gauß-Algorithmus, das heißt wenn nur Zeilenumformungen benutzt werden, bringt  $A$  zunächst auf die Form
- (2) Durch Vertauschen der Spalten  $j_1, \dots, j_r$  auf die Plätze  $1, \dots, r$ , also durch ein "nach vorne ziehen", erhalten wir
- (3) Dividieren der Spalte 1 durch  $\pi_1, \dots$ , Spalte  $r$  durch  $\pi_r$ , erhalten wir
- (4) Als letzten Schritt werden alle Spalten "ausgeräumt"

## 4.5 Spezielle Matrizen

Sei im Folgenden  $n$  fest gewählt.

a) **Elementarmatrizen**

Für  $1 \leq k \neq l \leq n$  sei

$$E^{kl} = \mathbb{1}_n + \tilde{E}^{kl} = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ & & & \ddots \\ 0 & & & & 1 \end{pmatrix}$$

die Elementarmatrix. Dann ist  $E^{kl}$  invertierbar mit  $(E^{kl})^{-1} = \mathbb{1} - \tilde{E}^{kl}$ , denn es gilt

$$(\mathbb{1} + \tilde{E}^{kl})(\mathbb{1} - \tilde{E}^{kl}) = \mathbb{1}^2 - (\tilde{E}^{kl})^2 = \mathbb{1} - 0 = \mathbb{1}.$$

Etwas allgemeiner gilt für  $0 \neq \lambda \in \mathbb{K} :$   $E^{kl}[\lambda] = \mathbb{1} + \lambda \tilde{E}^{kl}$ ,

$$E^{kl}[\lambda] : \begin{array}{l} e_k \mapsto e_k \\ e_l \mapsto e_l + \lambda e_k \\ e_i \mapsto e_i (i \neq k, l) \end{array}$$

Geometrisch betrachtet erhalten wir Scherungen:

$$n = 2 : \quad E^{12}[\lambda] = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

**Lemma 4.5.1.** Für die Elementarmatrizen gelten

- (1)  $E^{kl}[0] = \mathbb{1}$
- (2)  $E^{kl}[\lambda] \cdot E^{kl}[\mu] = E^{kl}[\lambda + \mu]$ , insbesondere  
 $(E^{kl}[\lambda])^s = E^{kl}[s\lambda]$
- (3)  $E^{kl}[\lambda]^{-1} = E^{kl}[-\lambda]$
- (4)  $E^{ij}[\lambda] \cdot E^{kl}[\mu] E^{ij}[-\lambda] \cdot E^{kl}[-\mu] = \mathbb{1}$ ,  $i \neq l, j \neq k$
- (5)  $E^{ij}[\lambda] \cdot E^{jl}[\mu] \cdot E^{ij}[-\lambda] \cdot E^{jl}[-\mu] = E^{il}[\lambda\mu]$ ,  $i \neq l$
- (6)  $E^{ij}[\lambda] \cdot E^{ki}[\mu] \cdot E^{ij}[-\lambda] \cdot E^{ki}[-\mu] = E^{kj}[-\lambda\mu]$ ,  $j \neq k$
- (7)  $(E^{ij}[1] \cdot E^{ji}[1]^{-1} \cdot E^{ij}[1])^4 = \mathbb{1}$

**Beweis:**

Man kann solche Formeln durch Nachrechnen beweisen, oder man kontrolliert, dass beide Seiten auf den Standardeinheitsvektoren  $e_1, \dots, e_n$  das gleiche tun. Eine gute Methode ist auch folgende: Man rechnet das im kleinsten Fall  $n = 2$  oder einem anderen kleinen Wert nach, und nennt die kleinen Matrizen kurz  $e^{ij}[\lambda]$ . Dann sieht man schnell, dass die Gleichungen auch für die durch  $\mathbb{1}$  ergänzte große Elementarmatrix

$$E^{ij}[\lambda] = \begin{pmatrix} e^{ij}[\lambda] & 0 \\ 0 & \mathbb{1} \end{pmatrix}$$

gelten. Und zum Schluss benutzt man  $E^{ij}[\lambda] = P E^{ij} P^{-1}$  für ein geeignetes  $P$ , wenn  $k, l$  beliebig ist.  $\square$   
*Bemerkung.* Ausdrücke der Form  $aba^{-1}b^{-1}$  nennt man einen *Kommutator*.

#### b) Streckungsmatrizen

Sei  $k = 1, \dots, n$  und  $\lambda \in \mathbb{K}$ . Dann definieren wir die Streckungsmatrix als

$$D_k[\lambda] = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & \lambda & \\ 0 & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

**Lemma 4.5.2.** Es gilt

- (1)  $D_k[1] = \mathbb{1}$
- (2)  $D_k[\lambda] \cdot D_k[\mu] = D_k[\lambda\mu]$ , insbesondere  
 $D_k[\lambda]^s = D_k[\lambda^s]$
- (3)  $D_k[\lambda]$  ist genau dann invertierbar, wenn  $\lambda \neq 0$  ist, und in diesem Fall ist  $D_k[\lambda]^{-1} = D_k[\frac{1}{\lambda}]$
- (4)  $D_i[\lambda] \cdot D_j[\mu] = D_j[\mu] \cdot D_i[\lambda]$

#### c) Diagonalmatrizen

Matrizen der Form  $D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} =: D[\lambda_1, \dots, \lambda_n]$  heißen Diagonalmatrizen.

**Lemma 4.5.3.** Es gilt

- (1)  $D[\lambda_1, \dots, \lambda_n] = D[\lambda_1] \cdot \dots \cdot D[\lambda_n]$
- (2)  $D[1, \dots, 1] = \mathbb{1}$
- (3)  $D[\lambda_1, \dots, \lambda_n] \cdot D[\mu_1, \dots, \mu_n] = D[\lambda_1\mu_1, \dots, \lambda_n\mu_n]$
- (4)  $D[\lambda_1, \dots, \lambda_n]$  ist genau dann invertierbar, wenn  $\lambda_1, \dots, \lambda_n \neq 0$ , in diesem Fall ist  $D[\lambda_1, \dots, \lambda_n]^{-1} = D[\lambda_1^{-1}, \dots, \lambda_n^{-1}]$

d) **Permutationsmatrizen**

Eine *Permutation* auf den Ziffern  $1, \dots, n$  ist eine Bijektion  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ , zusammen mit einer Abbildung

$$f_\sigma : \mathbb{K}^n \rightarrow \mathbb{K}^n, \quad e_k \mapsto e_{\sigma(k)},$$

die also eine Permutation der Standardbasis darstellt. Die dazugehörige Matrix sei

$$P_\sigma = M_{SS}(F_\sigma).$$

Sie hat in jeder Zeile  $i$  genau einen von Null verschiedenen Eintrag, und zwar an der Stelle  $j = \sigma^{-1}(i)$  eine 1, und sie hat in jeder Spalte  $j$  genau einen von Null verschiedenen Eintrag, und zwar an der Stelle  $i = \sigma(j)$  eine 1.

**Beispiel 4.5.4.**

-  $\sigma = id$

- Transposition  $(i\ j) : i \mapsto j, \quad j \mapsto i, \quad k \mapsto k$  für  $k \neq i, j$

**Lemma 4.5.5.** *Es gilt*

(1)  $P_{id} = \mathbb{1}$

(2)  $P_\sigma \cdot P_\tau = P_{\sigma\circ\tau}$

(3)  $P_\sigma$  ist invertierbar und es ist  $P_\sigma^{-1} = P_{\sigma^{-1}}$

(4)  $P_{(i\ j)}^{-1} = P_{(i\ j)}$  für eine Transposition  $(i\ j)$

**Lemma 4.5.6.**

1.  $P_\sigma E^{ij}[\lambda] P_\sigma^{-1} = E^{\sigma(i)\sigma(j)}[\lambda]$
2.  $P_\sigma D_k[\lambda] P_\sigma^{-1} = P_{\sigma(k)}[\lambda]$
3.  $P_\sigma D(\lambda_1, \dots, \lambda_k) P_\sigma^{-1} = D(\lambda_{\sigma^{-1}(1)}, \dots, \lambda_{\sigma^{-1}(k)})$
4.  $P_\sigma P_\varepsilon P_\sigma^{-1} = P_{\sigma\varepsilon\sigma^{-1}}$
5.  $D_j[\lambda^{-1}] E^{ij}[\mu] D_i[\lambda] = E_{ij}[\lambda\mu]$

Was bewirken diese Matrizen?

**Proposition 4.5.7.** *Sei  $A \in Mat_{m,n}(\mathbb{K}), \lambda \neq 0$*

1.  $E^{ij}A = \mathfrak{A}'_{ij}(A)$  Addition der  $j$ -ten Zeile zur  $i$ -ten
2.  $D_i[\lambda]A = \mathfrak{M}'_i[\lambda](A)$  Multiplikation der  $i$ -ten Zeile mit  $\lambda$
3.  $P_{ij}A = \mathfrak{B}'_{ij}(A)$  Vertauschen der  $i$ -ten und  $j$ -ten Zeile

**Proposition 4.5.8.** *Sei  $A \in Mat_{m,n}(\mathbb{K}), E^{ij}, D_i[\lambda], P_{\sigma(j)} \in Mat_{n,m}(\mathbb{K}), \lambda \neq 0$*

1.  $AE^{ij} = \mathfrak{A}'_{ij}(A)$  Addition der  $j$ -ten Zeile zur  $i$ -ten
2.  $AD_i[\lambda] = \mathfrak{M}'_i[\lambda](A)$  Multiplikation der  $i$ -ten Zeile mit  $\lambda$
3.  $AP_{\sigma(j)} = \mathfrak{B}'_{ij}(A)$  Vertauschen der  $i$ -ten und  $j$ -ten Zeile

Man stellt also fest:

1. Der vollständige Gauß-Algorithmus, angewandt auf  $A$ , ist nichts anderes als sukzessives Multiplizieren von links oder rechts mit Elementarmatrizen, Streck- oder Vertauschmatrizen. Gauß macht aus der Matrix  $A$  die Matrix  $A' = ZAS$ , wobei  $Z$  das Produkt aller verwendeten Elementar-, Streck- und Vertauschmatrizen ist, in der richtigen Reihenfolge sortiert nach Zeilen- und Spaltenumformungen. Hier ist  $r = rg(A)$ .

2.  $A$  sei quadratisch und invertierbar.

In diesem Fall kommt man ohne Spaltenumformungen aus.  $A$  wird durch Linksmultiplikation mit  $Z$  zu  $A' = \mathbb{1} Z$  ist gleich  $A^{-1}$ . **Wichtig:** Man muss nicht wissen, ob  $A$  invertierbar ist, der Algorithmus bricht vorher ab.

**Beispiel 4.5.9.**  $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Linksmultiplikation mit  $E_{21}[-3]$  liefert:

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

Linksmultiplikation mit  $E^{12}[1]$  liefert:

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

Linksmultiplikation mit  $D_2[-\frac{1}{2}]$  liefert schließlich das Inverse  $A^{-1}$ . Die Inverse Matrix steht nun da, wo ursprünglich die Einheitsmatrix stand und an Stelle von  $A$  steht nun die Einheitsmatrix.

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

## 4.6 Normalformen

Sei im Folgenden  $f : V \rightarrow W$  lineare Abbildung zwischen zwei Vektorräumen  $V$  mit  $\dim(V) = n$  und  $W$  mit  $\dim(W) = m$ , sei weiter der  $rg(f) = r$ . Setze  $V' := Ker(f)$  mit Basis  $\mathcal{A}'' = (a''_1, \dots, a''_{n-r})$ . Ergänze nun  $\mathcal{A}''$  zu eine Basis  $\mathcal{A}$  von  $V$ , also  $\mathcal{A} = (\mathcal{A}', \mathcal{A}'') = (a'_1, \dots, a'_r, a''_1, \dots, a''_{n-r})$ . Dann gilt: (1)  $f(a''_i) = 0$  mit  $i = 1, \dots, n - r$ . Das ist klar, denn Elemente im Kern werden auf Null geschickt.

(2) Setze  $\mathcal{B}' := f(\mathcal{A}') = (f(a'_1), \dots, f(a'_r))$ .  $\mathcal{B}'$  ist eine geordnete Basis von  $im(f) \subseteq W$ .

Warum ist das so?  $0 = \lambda_1 f(a'_1) + \dots + \lambda_r f(a'_r) = f(\lambda_1 a'_1 + \dots + \lambda_r a'_r)$ , da gleich Null muss  $v' = (\lambda_1 a'_1 + \dots + \lambda_r a'_r) \in Ker(f)$ .  $v'$  ist mit der Basis des Kerns darstellbar  $v' = \mu_1 a''_1 + \dots + \mu_{n-r} a''_{n-r}$ . Daraus folgt, dass  $0 = (-\lambda_1) a'_1 + \dots + (-\lambda_r) a'_r + \mu_1 a''_1 + \dots + \mu_{n-r} a''_{n-r}$  und somit gelten muss, dass alle  $\lambda_1 = \dots = \lambda_r = 0$  und  $\mu_1 = \dots = \mu_{n-r} = 0$ . Ergänze zu einer Basis  $\mathcal{B} = (\mathcal{B}', \mathcal{B}'') = (f(a'_1), \dots, f(a'_r), b_1, \dots, b_{n-r})$ . Dann ist

$$M_{\mathcal{B}, \mathcal{A}}(f) = \left( \begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array} \right)$$

**Satz 4.6.1.** Für jede lineare Abbildung  $f : V \rightarrow W$  zwischen Vektorräumen gibt es Basen  $\mathcal{A}$  in  $V$  und  $\mathcal{B}$  in  $W$ , so dass gilt

$$M_{\mathcal{B}, \mathcal{A}}(f) = \left( \begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array} \right) \text{ mit } r = rg(f)$$

Insbesondere gilt: Wenn  $f$  ein Isomorphismus ist und  $m = n$  (d.h.  $V$  und  $W$  haben gleiche Dimension), dann ist  $M_{\mathcal{B}, \mathcal{A}}(f) = \mathbb{1}_n$

*Beweis.* nach obiger Konstruktion. □

**Satz 4.6.2.** Für jede Matrix  $M \in Mat_{m,n}(\mathbb{K})$  gibt es invertierbare Matrizen  $A, B$  mit

$$BMA = \left( \begin{array}{c|c} \mathbb{1}_r & 0 \\ \hline 0 & 0 \end{array} \right)$$

Insbesondere gilt: Wenn  $M$  invertierbar ist, so ist  $BMA = \mathbb{1}$

*Beweis.*

1. Gauß-Algorithmus mit  $B = Z$  Produkt der Zeilenumformungen und  $A = S$  Produkt der Spaltenumformungen.
2.  $M_{\mathcal{B}, \mathcal{A}} : Hom(V, W) \longleftrightarrow Mat_{m,n}(\mathbb{K}) : L$ .  $\mathcal{A}$  ist Basiswechselmatrix in  $V$  und  $\mathcal{B}$  ist Basiswechselmatrix in  $W$ .

□

# 5 Gruppen

Wir haben schon etliche Gruppen gesehen und wollen diesen Begriff nun axiomatisieren.

**Definition 5.0.3.** Eine *Gruppe*  $G$  ist eine nicht-leere Menge mit einer Verknüpfung, genannt *Multiplikation*

$$\begin{aligned} \mu : G \times G &\longrightarrow G \\ (x, y) &\longmapsto \mu(x, y) = x \cdot y = xy, \end{aligned}$$

so dass folgende drei Axiome erfüllt sind:

(G1) *Assoziativgesetz*: Für alle  $x, y, z \in G$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

(G2) *Neutrales Element*: Es gibt ein Element  $1 \in G$  so dass für alle  $x \in G$

$$x \cdot 1 = 1 \cdot x = x.$$

(G3) *Inverse Elemente*: Für jedes  $x \in G$  gibt es ein  $x^{-1} \in G$ , so dass

$$x \cdot x^{-1} = x^{-1}x = 1.$$

Gilt zusätzlich das

(G4) *Kommutativgesetz*: Für alle  $x, y \in G$  gilt  $x \cdot y = y \cdot x$ .

so nennt man  $G$  *kommutativ* oder *abelsch*.

## Notation

1) Das Produkt wird meist ohne Punkt  $xy$  geschrieben und das Inverse  $x^{-1}$ . Wir werden gleich sehen, dass es zu jedem  $x$  *nur ein Inverses* gibt. Das neutrale Element wird oft auch mit  $e$  bezeichnet.

2) In einer abelschen Gruppe schreibt man das Produkt oft (aber nicht immer) als Addition  $x + y$ , das neutrale Element als 0, und das Inverse als  $-x$ . Die Axiome lauten dann

$$\begin{aligned} x + (y + z) &= (x + y) + z \\ x + 0 &= 0 + x = x \\ x + (-x) &= (-x) + x = 0 \\ x + y &= y + x \end{aligned}$$

**Lemma 5.0.4.** *Gilt*

$$\begin{aligned} x \cdot y_1 = y_1 \cdot x = 1 \quad \text{und} \\ x \cdot y_2 = y_2 \cdot x = 1, \end{aligned}$$

so ist  $y_1 = y_2$ .

*Beweis.* Wir benötigen nur

$$\begin{aligned} (1) \quad x \cdot y_1 = 1 \quad \text{und} \\ (2) \quad y_2 \cdot x = 1, \end{aligned}$$

denn

$$y_1 \stackrel{(G2)}{=} 1 \cdot y_1 \stackrel{(2)}{=} (y_2 x) y_1 \stackrel{(G1)}{=} y_2 (x y_1) \stackrel{(1)}{=} y_2 \cdot 1 \stackrel{(G2)}{=} y_2$$

□

**Lemma 5.0.5.**

$$\begin{aligned} (1) \quad & 1^{-1} = 1 \\ (2) \quad & (x^{-1})^{-1} = x \\ (3) \quad & (xy)^{-1} = y^{-1}x^{-1} \end{aligned}$$

**Beispiel 5.0.6.** 1)  $G = \mathbb{Z}$  mit der Addition (abelsch).

2)  $G = \mathbb{K}$  mit der Addition (abelsch)

3)  $G = \mathbb{K}^* := \mathbb{K} \setminus \{0\}$  mit der Multiplikation (abelsch)

4)  $G = V$  Vektorraum mit Addition (abelsch)

5)  $G = \mathbb{Z}/n$  mit der Addition (abelsch)

6) *Allgemeine lineare Gruppe*  $G = \text{GL}_n(\mathbb{K})$  Gruppe der invertierbaren  $n \times n$ - Matrizen über  $\mathbb{K}$  (nicht-abelsch für  $n \geq 2$ )

$$A \in \underbrace{\text{GL}_n(\mathbb{C}) \supseteq \text{GL}_n(\mathbb{R}) \supseteq \text{GL}_n(\mathbb{Q}) \supseteq \text{GL}_n(\mathbb{Z})}_{\substack{A^{-1} \text{ hat wieder Einträge im Unterkörper } \mathbb{K}' \subseteq \mathbb{K} \quad \text{Warum ist } A^{-1} \text{ wieder ganzzahlig?}}$$

7)  $G = \text{GL}(V) = \text{Aut}_{\mathbb{K}}(V) = \{f : V \rightarrow V \mid f \text{ linear und bijektiv}\}$  *Automorphismen* von  $V$  (nicht abelsch für  $\dim V > 1$ ).

8) *Diedergruppen*  $G = \{\text{Drehungen und Spiegelungen eines regelmäßigen } n\text{-Ecks}\} = D_{2n}$

9) Drehungen (ohne Spiegelungen) der 5 platonischen Körper (Tetraeder, Würfel, Oktaeder, Dodekaeder, Ikosaeder)

Die *Ikosaedergruppe* hat 60 Elemente:

12 Ecken

30 Kanten

20 Flächen (Dreiecke)

Euler-Zahl  $\chi = 12 - 30 + 20 = 2$

- 6 Geraden durch antipodische Ecken: Drehungen um  $72^\circ, 144^\circ, 216^\circ, 288^\circ \rightsquigarrow 6 \cdot 4 = 24$
- 10 Geraden durch antipodische Flächenmittelpunkte: Drehungen um  $120^\circ, 240^\circ \rightsquigarrow 10 \times 2 = 20$
- 15 Geraden durch antipodische Kantenmittelpunkte: Drehungen um  $180^\circ \rightsquigarrow 15 \cdot 1 = 15$
- identische Abbildung  $\rightsquigarrow 1$

## 5.1 Symmetrische Gruppen

**Definition 5.1.1** (Symmetrische Gruppe). Für eine beliebige Menge  $X$  nennt man

$$\text{Sym}(X) = \{f : X \rightarrow X \text{ bijektiv}\}$$

die *symmetrische Gruppe von X*. Für  $X = \{1, \dots, n\}$  schreibt man  $S_n = \mathfrak{S}_n = \text{Sym}(\{1, \dots, n\})$ . Es gilt  $|\mathfrak{S}_n| = n!$ .

**Spezielle Elemente:**

- Die *Transposition*  $(ij) \in \mathfrak{S}_n$  vertauschen nur zwei Elemente  $i \neq j, 1 \leq i, j \leq n$  und lässt alle anderen fix.
- $(ij)^{-1} = (ij) = (ji)$ .
- *Zykel*:  $i_1, \dots, i_k$  seien paarweise verschiedene Elemente in  $\{1, \dots, n\}$ . Wir definieren  $(i_1 i_2 \dots i_k) \in \mathfrak{S}_n$  durch  $i_1 \mapsto i_2 \mapsto i_3 \mapsto \dots \mapsto i_k \mapsto i_1$  und  $i \mapsto i$  für alle anderen Elemente.
- $k = 1$ :  $(i_1) = 1$ .
- $(i_1 i_2 \dots i_k)^{-1} = (i_k i_{k-1} \dots i_2 i_1)$ .
- $(i_1 i_2 \dots i_k) = (i_2 i_3 \dots i_k i_1) = (i_3 i_4 \dots i_k i_1 i_2) = \dots$  ( Jeder Zykel der Länge  $k$  hat  $k$  Notationen.)

- $\mathfrak{S}_n$  ist nicht abelsch für  $n \geq 3$ :

$$(12)(23) = (123)$$

$$(23)(12) = (132)$$

**Lemma 5.1.2.** *Jedes  $\pi \in \mathfrak{S}_n$  lässt sich eindeutig als Produkt von disjunkten Zykeln schreiben:*

$$\pi = (a_1 \dots a_k)(b_1 \dots b_l)(c_1 \dots c_m) \cdots (x_1 \dots x_r)$$

*Dabei ist die Reihenfolge der  $r$  Zykeln nicht bestimmt, weil disjunkte Zykeln vertauschen; die Reihenfolge der Elemente in einem Zykel ist bis auf zyklische Vertauschung eindeutig bestimmt.*

*Beweis.* Wir schreiben  $X = \{1, \dots, n\}$ .

Wir beginnen mit dem Element 1 und verfolgen seine Bahn

$$1 = a_1 \xrightarrow{\pi} a_2 \xrightarrow{\pi} \dots \xrightarrow{\pi} a_{k+1} = 1;$$

weil wir nur endlich-viele Möglichkeiten haben, muss für ein  $k \geq 1$  wieder  $1 = a_{k+1}$  erscheinen;  $k$  sei minimal mit dieser Eigenschaft. Ist  $k = 1$ , so ist 1 ein Fixpunkt von  $\pi$  und wir brauchen den Zykel  $(a_1)$  gar nicht zu notieren; ansonsten haben wir einen ersten Zykel  $(a_1 \dots a_k)$ .

Wir setzen  $\mathfrak{A} = \{a_1, \dots, a_k\}$  und betrachten die Menge  $X \setminus \mathfrak{A}$ . Ist diese Menge leer, sind wir fertig. Sonst wählen wir das kleinste Element  $b_1$  und verfolgen seine Bahn

$$b_1 \xrightarrow{\pi} b_2 \xrightarrow{\pi} \dots \xrightarrow{\pi} b_{l+1} = b_1.$$

Diese kann die Bahn von  $a_1$  nicht kreuzen, liegt also ganz in  $X \setminus \mathfrak{A}$ . Ist  $l = 1$ , so brauchen wir den Zykel  $(b_1)$  nicht zu notieren; sonst haben wir den Zykel  $(b_1 \dots b_l)$ . Wir schreiben  $\mathfrak{B} = \{b_1, \dots, b_l\}$ .

Wir machen so weiter, als nächstes mit  $X \setminus (\mathfrak{A} \cup \mathfrak{B})$ , bis ganz  $X$  ausgeschöpft ist. □

**Definition 5.1.3.** Wir definieren den *Zykeltyp* von  $\pi \in \mathfrak{S}_n$  als

$$\text{Typ}(\pi) = (t_1, \dots, t_n),$$

wobei  $t_i$  die Anzahl der Zykeln der Länge  $i$  und  $t_1$  die Anzahl der Fixpunkte von  $\pi$  ist. Wir haben dann

$$n = 1t_1 + 2t_2 + \dots + nt_n.$$

**Beispiel 5.1.4.** 1)  $\pi = (ij)$  Transposition hat  $\text{Typ}(\pi) = (n - 2, 1, 0, \dots, 0)$ .

2)  $\pi = 1$  hat  $\text{Typ}(1) = (n, 0, 0, \dots, 0)$ .

3)  $\pi = (1375462)(8)(910)$  hat  $\text{Typ}(\pi) = (1, 1, 0, 0, 0, 0, 1, 0)$ .

**Lemma 5.1.5.** *Jeder Zykel ist ein Produkt von Transpositionen:*

$$(i_1 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-2} i_{k-1})(i_{k-1} i_k)$$

**Korollar 5.1.6.** *Jede Permutation ist ein Produkt von Transpositionen.*

**Lemma 5.1.7.**  $\sigma(i_1 \dots i_k)\sigma^{-1} = (\sigma(i_1)\sigma(i_2) \dots \sigma(i_k))$ .

## 5.2 Untergruppen

**Definition 5.2.1.** Eine Teilmenge  $H \subseteq G$  einer Gruppe  $G$  heißt *Untergruppe*, wenn sie folgende Eigenschaften hat:

(U1)  $1 \in H$ .

(U2)  $g \in H \Leftrightarrow g^{-1} \in H$ .

(U3)  $g_1, g_2 \in H \Rightarrow g_1 g_2 \in H$ .

Wir notieren Untergruppen mit  $H \leq G$ .

**Beispiel 5.2.2.**

1)  $H = 1 =: 1 \leq G$  ist die *triviale* Untergruppe.

- 2)  $n\mathbb{Z} = \{a \in \mathbb{Z} \mid a \text{ ist durch } n \text{ teilbar}\} \leq \mathbb{Z}$   
 3)  $\mathbb{S}^0 = \{\pm 1\} = \{x \in \mathbb{R}^\times \mid |x| = 1\} \leq \mathbb{R}^\times$   
 4)  $\mathbb{S}^1 = \{z \in \mathbb{C}^\times \mid |z| = 1\} \leq \mathbb{C}^\times$ .  
 5)  $\mathbb{S}^3 = \{z \in \mathbb{H} \cong \mathbb{R}^4 \mid |z| = 1\} \cong \mathbb{H}^\times$ , wobei  $\mathbb{H}$  die Gruppe der Quaternionen bezeichnet.  
 6)  $\mu_n = \{z \in \mathbb{C}^\times \mid z^n = 1\} \leq \mathbb{C}^\times$  Gruppe der  $n$ -ten Einheitswurzeln  
 7)  $H = \{1, (ij)\} \leq \mathfrak{S}_n$  für  $n \geq 2$ ;  $H' = \{\sigma \in \mathfrak{S}_n \mid \sigma(k) = k\} \leq \mathfrak{S}_n$   
 8)  $\mathrm{GL}_n(\mathbb{Z}) \leq \mathrm{GL}_n(\mathbb{Q}) \leq \mathrm{GL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{C})$   
 9)  $\mathrm{SL}_2(\mathbb{K}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{K}) \mid ad - bc = 1 \right\} \leq \mathrm{GL}_2(\mathbb{K})$  für  $\mathbb{K}$  Körper oder  $\mathbb{K} = \mathbb{Z}$   
 10)  $H = \{A \in \mathrm{GL}_n(\mathbb{K}) \mid A^\top = A^{-1}\}$  ist eine Untergruppe, denn  $\mathbb{1}^\top = \mathbb{1}^\top$  und  $(AB)^\top = B^\top A^\top = B^{-1}A^{-1} = (AB)^{-1}$ .  
 11) Sei  $V$  ein Vektorraum und sei  $0 \neq v \in V$ . Dann sind

$$H = \{f \in \mathrm{GL}(V) \mid f(v) = v\} \quad \text{und} \\ H' = \{f \in \mathrm{GL}(V) \mid \exists \lambda \in \mathbb{K}^\times : f(u) = \lambda u\}$$

Untergruppen von  $\mathrm{GL}(V)$ . Ein  $f \in H$  lässt das Erzeugnis von  $v$  ( $\langle v \rangle$ ) *punktweise* fest. Ein  $f \in H'$  lässt hingegen nur den von  $v$  erzeugten Unterraum invariant, denn  $f(\langle v \rangle) = \langle v \rangle \Leftrightarrow \exists \lambda \neq 0 : f(v) = \lambda v$ , wobei letzteres eine *Eigenwertgleichung* ist. Wir haben also  $H \leq H'$ .

Allgemeiner betrachten wir für einen Untervektorraum  $U \subseteq V$  die Untergruppen

$$H = \{f \in \mathrm{GL}(V) \mid \forall u \in U : f(u) = u\} \quad \text{und} \\ H' = \{f \in \mathrm{GL}(V) \mid f(U) = U\}$$

von  $\mathrm{GL}(V)$ , für die gilt  $H \leq H'$ .

- 12) Die Menge der Diagonalmatrizen  $\mathcal{D} = \{D[\lambda_1, \dots, \lambda_n] \mid \lambda_1, \dots, \lambda_n \neq 0\}$  sind mit der Matrizenmultiplikation eine Gruppe. Die Menge aller *zentralen Matrizen*  $\mathcal{Z} = \{D[\lambda, \dots, \lambda] \mid \lambda \neq 0\}$  eine Untergruppe:  $\mathcal{Z} \leq \mathcal{D}$ . Die zentralen Matrizen sind besonders wichtig, da sie das *Zentrum* der Gruppe  $\mathrm{GL}_n(\mathbb{K})$  sind, das heißt, sie vertauschen mit allen Matrizen.  
 13) Die Menge der Permutationsmatrizen  $\mathcal{P} = \{P_\sigma \mid \sigma \in \mathfrak{S}_n\}$  ist eine Untergruppe der  $\mathrm{GL}_n(\mathbb{K})$ :  $P_1 = \mathbb{1}$ ,  $P_{\alpha\beta} = P_\alpha P_\beta$ .  
 14) Die Menge der *oberen Dreiecksmatrizen*  $\mathcal{T}^+$ , also der Matrizen der Form

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

ist abgeschlossen bezüglich der Matrixmultiplikation und daher eine Untergruppe der  $\mathrm{GL}_n$ . Die entsprechende Aussage gilt auch für die Menge der *unteren Dreiecksmatrizen*  $\mathcal{T}^-$ .

- 15) Für den Tetraeder  $\mathcal{T}$  ist die Gruppe der Rotationen eine Untergruppe der Symmetrien (also Rotationen und Spiegelungen):

$$\mathrm{Rot}(\mathcal{T}) = \mathcal{T} \leq \mathcal{T}' = \mathrm{Sym}(\mathcal{T}')$$

Die analoge Aussage gilt für alle platonischen Körper.

**Definition 5.2.3.** (i) Die Kardinalität einer Gruppe  $G$  heißt ihre *Ordnung*  $|G|$ .

- (ii) Sei  $g \in G$ . Die kleinste natürliche Zahl  $s$  mit  $g^s = 1$  nennt man die *Ordnung* von  $g$ , falls so ein  $s$  existiert; falls nicht, so heißt  $g$  von *unendlicher Ordnung*.

*Notation:*  $\mathrm{ord}(g) = 1, 2, \dots, \infty$ .

*Bemerkung.* • Die Kardinalität von  $G$  kann überabzählbar sein (z.B.  $G = \mathbb{S}^1$ ).

- Ordnung hat hier nichts mit Ordnungsrelationen zu tun.

**Beispiel 5.2.4.**

1. In der Übungsaufgabe 56 haben wir gefunden:

$$A = \begin{pmatrix} \cos \frac{2\pi}{s} & -\sin \frac{2\pi}{s} \\ \sin \frac{2\pi}{s} & \cos \frac{2\pi}{s} \end{pmatrix} \quad \text{ord}(A) = s$$

$$A = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \quad \text{ord}(A) = \infty \text{ für } \frac{2\pi}{\alpha} \notin \mathbb{Q}$$

2. Für ein festes  $g \in G$  betrachten wir die Untergruppe aus allen ganzzahligen Potenzen von  $g$ :

$$H := \{1, g^{\pm 1}, g^{\pm 2}, \dots, g^{\pm n}, \dots\} \leq G$$

Es gilt  $|H| = \text{ord}(g)$ .

3. Wir betrachten die symmetrische Gruppe  $\mathfrak{S}_n$ . Die Ordnung eines  $k$ -Zykels  $g = (i_1 i_2 \dots i_k)$  ist  $\text{ord}(g) = k$ . Wenn  $g$  das Produkt disjunkter  $k$ - und  $l$ -Zykel ist, gilt:

$$g = (i_1 \dots i_k)(j_1 \dots j_l) \Rightarrow \text{ord}(g) = \text{kgV}(k, l).$$

Produkte nicht-disjunkter Zykel muss man erst als Produkte disjunkter Zykel ausdrücken.

**Definition 5.2.5.** Für jede Teilmenge  $\mathcal{E} \subseteq G$  einer Gruppe sei  $H := \langle \mathcal{E} \rangle$  die Menge aller endlichen Produkte von Elementen und ihren Inversen in  $\mathcal{E}$

$$g = e_1^{l_1} e_2^{l_2} \dots e_i^{l_i} \dots e_n^{l_n} \quad l_i \in \mathbb{Z},$$

wobei die  $e_i$  *nicht* verschieden sein müssen! (Nur wenn  $G$  abelsch ist, kann man verlangen, dass die  $e_i$  verschieden sind.)  $H$  heißt die von  $\mathcal{E}$  erzeugte Untergruppe. Ist  $H = \langle \mathcal{E} \rangle = G$ , so heißt  $\mathcal{E}$  ein *Erzeugendensystem* für  $G$ .

**Beispiel 5.2.6.**

- $G = \mathbb{Z}/n = \{\underline{0}, \underline{1}, \dots, \underline{n-1}\}, \mathcal{E} = \{\underline{1}\}$ , wir können jede Restklasse als Summe  $\underline{1} + \underline{1} + \dots$  schreiben. Ein anderes Erzeugendensystem wäre zum Beispiel  $\mathcal{E} = \{\underline{2}, \underline{3}\}$ , da die Differenz  $\pm 1$  ist.
- $G = \mathfrak{S}_n, \mathcal{E} = \{(ij) \mid 1 \leq i < j \leq n\}$ , denn jede Permutation lässt sich als Produkt von Transpositionen schreiben. Es reicht sogar  $\{(i(i+1)) \mid 1 \leq i < n\}$ , da  $\sigma(i(i+1))\sigma^{-1} = (\sigma(i)\sigma(i+1)) = (kl)$  für ein  $\sigma$  mit  $\sigma(i) = k, \sigma(i+1) = l$ .
- $G = GL_n(\mathbb{K})$ : Ein Erzeugendensystem der allgemeinen linearen Gruppe ist die Vereinigung von Elementarmatrizen, Streckungsmatrizen und Permutationsmatrizen.

*Bemerkung.* Beim linearen Erzeugnis  $\text{span}(\mathcal{E})$  in einem Vektorraum wird außer der Addition und dem Negativen auch die Skalierung benutzt.

Sei  $\mathfrak{B} = \{b_1, \dots, b_n\} \subseteq V$  Basis des  $\mathbb{R}$ -Vektorraums  $V$ . Dann ist

$$\langle \mathfrak{B} \rangle = \{v = k_1 b_1 + \dots + k_n b_n \mid k_1, \dots, k_n \in \mathbb{Z}\}$$

nur eine additive Untergruppe von  $V$ , aber *kein* Untervektorraum; man nennt  $\langle \mathfrak{B} \rangle$  auch ein *Gitter*.

Nun noch ein paar wichtige Untergruppen:

**Definition 5.2.7.** Das *Zentrum*  $\text{Zen}(G)$  einer Gruppe  $G$  ist die Untergruppe

$$\text{Zen}(G) := \{z \in G \mid \forall g \in G : zg = gz\},$$

also die Elemente, die mit allen kommutieren.

Die *Kommutatoruntergruppe*  $\text{Kom}(G) = [G, G]$  ist die von allen *Kommutatoren*  $[x, y] := xyx^{-1}y^{-1}$  ( $x, y \in G$  beliebig) erzeugte Untergruppe. Beachte:

- $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$
- $[x, y][a, b]$  ist in der Regel *kein* Kommutator (deshalb nimmt man das Erzeugnis).

- Abgeschlossen bezüglich Konjugieren:

$$\gamma[x, y]\gamma^{-1} = \gamma xyx^{-1}y^{-1}\gamma^{-1} = (\gamma x\gamma^{-1})(\gamma y\gamma^{-1})(\gamma x^{-1}\gamma^{-1})(\gamma y^{-1}\gamma^{-1}) = [\gamma x\gamma^{-1}, \gamma y\gamma^{-1}]$$

**Beispiel 5.2.8.**

1.  $G$  abelsch:  $\text{Zen}(G) = G$ , denn die Gruppe ist kommutativ;  $\text{Kom}(G) = 1$ , da  $xy = yx \Leftrightarrow [x, y] = 1$ .
2. Für  $G = \text{GL}_n(\mathbb{K})$  ist  $\text{Zen}(G) = \{D[\lambda, \dots, \lambda] \mid 0 \neq \lambda \in \mathbb{K}\} \cong \mathbb{K}^\times$ . Dies Matrizen nennt man *zentrale Matrizen*, vergleiche Übungsaufgabe 63.
3.  $G = \mathfrak{S}_n, n \geq 3$ :  $\text{Zen}(G) = 1$
4. Für drei verschiedene Indizes  $1 \leq i, j, k \leq n$  gilt

$$[E^{ii}[\lambda], E^{jk}[\mu]] = E^{jk}[\lambda\mu]$$

Für  $n \geq 3$  erzeugen die Kommutatoren also alles:  $\text{Kom}(\text{GL}_n(\mathbb{K})) = \text{GL}_n(\mathbb{K})$

### 5.3 Homomorphismen

**Definition 5.3.1.** Eine Funktion  $f : G \rightarrow G'$  zwischen zwei Gruppen  $G, G'$  heißt *Homomorphismus*, falls gilt:

1.  $f(1) = 1$ ,
2.  $f(xy) = f(x)f(y)$  für alle  $x, y \in G$ .

*Bemerkung.*

- Es gilt  $f(x^{-1}) = f(x)^{-1}$
- $\text{ord}(f(x))$  teilt  $\text{ord}(x)$ , falls  $\text{ord}(x)$  endlich; insbesondere hat  $f(x)$  endliche Ordnung, wenn  $x$  endliche Ordnung hat.
- Isomorphismus:  $f$  bijektiv  $\xrightarrow{\cong}$   
 Epimorphismus:  $f$  surjektiv  $\rightarrow$   
 Monomorphismus:  $f$  injektiv  $\hookrightarrow$   
 Endomorphismus:  $G = G'$   
 Automorphismus:  $G = G'$  und  $f$  Isomorphismus

**Beispiel 5.3.2.**

1. Für festes  $n$ :  $G = \mathbb{Z} \rightarrow G' = \mathbb{Z}, f(x) = nx$   
 $n \neq 0$ : mono,  $n = \pm 1$ : iso
2.  $\rho_n : \mathbb{Z} \rightarrow \mathbb{Z}/n, \rho_n(x) = \underline{x}$  Restklasse modulo  $n$ , epi
3.  $\exp : (\mathbb{R}, +) \rightleftarrows (\mathbb{R}_{>0}, \cdot) : \ln$
4.  $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{S}^1, \cdot), t \mapsto e^{2\pi it}$
5.  $f : V \rightarrow V' f$  linear, insb. gilt:  $f(x + y) = f(x) + f(y)$
6. Die Homomorphismen

$$G = \text{GL}(V) \begin{array}{c} \xrightarrow{M_{\mathcal{A}\mathcal{A}}} \\ \xleftarrow{L_{\mathcal{A}\mathcal{A}}} \end{array} G' = \text{GL}_n(\mathbb{K}) \quad (\dim_{\mathbb{K}}(V) = n, \mathcal{A} \subset V \text{ Basis}),$$

sind beide Isomorphismen.

7.  $\varepsilon : \mathbb{Z} \rightarrow \mathbb{K}, \varepsilon(n) = \varepsilon_n = (1 + \dots + 1)$   $n$ -mal  
 $\varepsilon(0) = 0, \varepsilon(n + m) = \varepsilon(n) + \varepsilon(m)$
8.  $\mathbb{Z}/n \rightarrow \mu_n, k \mapsto \zeta_n^k, \zeta_n = \exp(\frac{2\pi i}{n})$

9.  $(\mathbb{R}, +) \xrightarrow{\exp} (\mathbb{R}_{>0}, \cdot)$   $\exp(x + y) = \exp(x) \exp(y)$   
Umkehrfunktion:  $\log(xy) = \log(x) + \log(y)$
10.  $P : \mathfrak{S}_n \rightarrow \mathbb{P}_n =$  Gruppe der Permutationsmatrizen,  $\sigma \mapsto P_\sigma$
11.  $D : (\mathbb{K}^\times)^n \rightarrow \mathbb{D} =$  Gruppe der Diagonalmatrizen,  $(\lambda_1, \dots, \lambda_n) \mapsto D(\lambda_1, \dots, \lambda_n)$
12. Für  $g \in G$  haben wir einen Homomorphismus  $f_g : \mathbb{Z} \rightarrow G$ ,  $k \mapsto g^k$ . Falls  $\text{ord}(g) = n$ , so ist auch  $\mathbb{Z}/n \rightarrow G, \bar{k} \mapsto g^k$  ein Homomorphismus.

**Definition 5.3.3** (Signum). Auf den symmetrischen Gruppen definieren wir eine wichtige Funktion

$$\text{sign} : \mathfrak{S}_n \rightarrow \{\pm 1\}, \text{sign}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

1. Warum ist  $\text{sign}(\sigma) = \pm 1$ ?
2. Ein Paar  $(i, j)$  mit  $1 \leq i < j \leq n$  und  $\sigma(i) > \sigma(j)$  nennt man einen **Fehlstand** von  $\sigma$ .
3. Hat  $\sigma$  genau  $k$  Fehlstände ( $0 \leq k \leq \frac{n(n-1)}{2}$ ), so gilt

$$\prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)) = (-1)^k \prod_{1 \leq i < j \leq n} |\sigma(j) - \sigma(i)| = (-1)^k \prod_{1 \leq i < j \leq n} |j - i| = (-1)^k \prod_{1 \leq i < j \leq n} (j - i),$$

weil in den beiden mittleren Produkten die gleichen Faktoren in eventuell anderer Reihenfolge vorkommen. Also ist  $\text{sign}(\sigma) = (-1)^k$  bestimmt durch die Anzahl der Fehlstände.

**Beispiel 5.3.4.**

1.  $\sigma = (ij)$  Transposition  $\text{sign}(\sigma) = -1$
2.  $\sigma = (123)$ ;  $\text{sign}(\sigma) = \frac{3-2}{2-1} \frac{1-2}{3-1} \frac{1-3}{3-2} = +1$

**Lemma 5.3.5.** *sign ist ein Homomorphismus:*

$$\begin{aligned} \text{sign}(1) &= 1, \\ \text{sign}(\pi \circ \sigma) &= \text{sign}(\pi) \cdot \text{sign}(\sigma) \end{aligned}$$

*Beweis.*

$$\begin{aligned} \text{sign}(\pi \circ \sigma) &= \prod_{i < j} \frac{\pi(\sigma(j)) - \pi(\sigma(i))}{j - i} \\ &= \prod_{i < j} \frac{\pi(\sigma(j)) - \pi(\sigma(i))}{\sigma(j) - \sigma(i)} \cdot \frac{\sigma(j) - \sigma(i)}{j - i} \\ &= \prod_{k < l} \frac{\pi(l) - \pi(k)}{l - k} \cdot \prod_{i < j} \frac{\sigma(j) - \sigma(i)}{j - i} \\ &= \text{sign}(\pi) \cdot \text{sign}(\sigma) \end{aligned}$$

□

**Beispiel 5.3.6.**

1.  $\sigma = (i_1 \ i_2 \ \dots \ i_k)$   $k$ -Zykel  
 $= (i_1 \ i_2)(i_2 \ i_3) \dots (i_{k-1} \ i_k)$   $k - 1$  Faktoren  
 $\text{sign}(\sigma) = (-1)^{k-1}$
2.  $\text{sign}(\sigma^{-1}) = \text{sign}(\sigma)$
3.  $\text{Typ}(\sigma) = (t_1, t_2, \dots, t_n) :$   
 $\text{sign}(\sigma) = (-1)^{t_1 \cdot 0} \cdot (-1)^{t_2 \cdot 1} \dots (-1)^{t_n \cdot n} = (-1)^{n - (t_1 + t_2 + \dots + t_n)}$

**Definition 5.3.7.** Für einen Homomorphismus  $f : G \rightarrow G'$  definieren wir

1.  $\ker(f) = \bar{f}(1) = \{x \in G \mid f(x) = 1\} \subseteq G$ , genannt der *Kern* von  $f$ .
2.  $\operatorname{im}(f) = f(G) = \{y \in G' \mid \exists x \in G f(x) = y\} \subseteq G'$  genannt das *Bild* von  $f$ .

**Lemma 5.3.8.** 1)  $\ker(f)$  ist eine Untergruppe;  $f$  ist genau dann ein Monomorphismus, wenn  $\ker(f) = 1$  ist.

2)  $\operatorname{im}(f)$  ist eine Untergruppe;  $f$  ist genau dann ein Epimorphismus, wenn  $\operatorname{im}(f) = G'$  ist.

*Beweis.* 1)  $1 \in \ker(f)$ , wegen  $f(1) = 1$ .

$$g_1, g_2 \in \ker(f) \Rightarrow f(g_1) = 1, f(g_2) = 1 \Rightarrow f(g_1 g_2) = f(g_1) f(g_2) = 1 \cdot 1 = 1$$

Ist  $f$  ein Monomorphismus, so kann nur für  $x = 1$  die Bedingung  $f(x) = 1$  gelten. Angenommen  $f(g_1) = f(g_2)$ ; dann ist  $f(g_1 g_2^{-1}) = f(g_1) f(g_2^{-1}) = f(g_1) f(g_2)^{-1} = 1$ ; also folgt aus  $\ker(f) = 1$  nun  $g_1 g_2^{-1} = 1$ , also  $g_1 = g_2$ .

2)  $1 = f(1)$ , also  $1 \in \operatorname{im}(f)$ .

Ist  $y_1 = f(x_1)$  und  $y_2 = f(x_2)$ , so ist  $f(x_1 x_2) = y_1 y_2$ . □

### Beispiel 5.3.9.

1.  $f: \mathbb{Z} \rightarrow \mathbb{Z}/n, x \mapsto \bar{x}$  Restklasse mod  $n$   
 $\ker(f) = n\mathbb{Z} \subseteq \mathbb{Z}$
2.  $\varepsilon: \mathbb{Z} \rightarrow \mathbb{K}, \varepsilon(n) = n1$   
 $\ker(\varepsilon) = 0 \Leftrightarrow \operatorname{char}(\mathbb{K}) = 0$   
 $\ker(\varepsilon) = p\mathbb{Z} \Leftrightarrow \operatorname{char}(\mathbb{K}) = p$  (Primzahl)
3.  $L_g: \mathbb{Z} \rightarrow G, f(n) = g^n$  ( $g \in G$  fest)  
 $\ker(L_g) = 0 \Leftrightarrow \operatorname{ord}(g) = \infty$   
 $\ker(L_g) = n\mathbb{Z} \Leftrightarrow \operatorname{ord}(g) = n$
4.  $L_{a,b}: (\mathbb{R}, +) \rightarrow (\mathbb{C}^\times, \cdot)$   $a, b \in \mathbb{R}, a, b > 0$   
 $L_{a,b}(t) = e^{(a+ib)t}$   
 $\operatorname{im}(L_{a,b}) = \text{Spirale (logarithmische oder Bernoulli'sche)}$
5.  $X$  Menge,  $G$  Gruppe:  $\Gamma = \operatorname{Funkt}(X, G)$  ist eine Gruppe:  
 $(\gamma_1 \gamma_2)(x) := \gamma_1(x) \gamma_2(x), 1(x) := 1, \gamma^{-1}(x) := \gamma(x)^{-1}$
6. Ist  $X$  eine Gruppe, so ist  $\operatorname{Hom}(X, G)$  i.A. keine Untergruppe:

$$\begin{aligned} (\gamma_1 \cdot \gamma_2)(xy) &= \gamma_1(xy) \gamma_2(xy) = \gamma_1(x) \gamma_1(y) \gamma_2(x) \gamma_2(y) \\ (\gamma_1 \cdot \gamma_2)(x) (\gamma_1 \cdot \gamma_2)(y) &= \gamma_1(x) \gamma_2(x) \gamma_1(y) \gamma_2(y) \end{aligned}$$

**Lemma 5.3.10.** Für einen Homomorphismus  $\phi: G \rightarrow G'$  gilt:

1.  $\phi(\operatorname{Kom}(G)) \subset \operatorname{Kom}(G')$
2.  $\operatorname{Kom}(G) \subset \ker(\phi)$ , falls  $G'$  abelsch ist.

*Beweis.* 1): Ist  $g = [x, y] = xyx^{-1}y^{-1}$  ein Kommutator, so ist  $\phi(g) = \phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = [\phi(x), \phi(y)]$  wieder ein Kommutator.

$[x, y]^{-1} = xyx^{-1}y^{-1} = yxy^{-1}x^{-1} = [y, x]$  auch Und ist  $g$  ein Produkt von Kommutatoren (und Inversen von Kommutatoren), so auch  $\phi(g)$ .

2): Ist  $G'$  abelsch, so ist  $\operatorname{Kom}(G') = 1$ , also  $\phi(\operatorname{Kom}(G)) = 1$ , also  $\operatorname{Kom}(G) \subset \ker(\phi)$ :

Oder auf Elementen:

$$\phi[x, y] = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = \phi(x)\phi(x)^{-1}\phi(y)\phi(y)^{-1} = 1. \quad \square$$

### 5.3.1 Vorwärtsschicken/ Rückwärtsschicken von Gruppenstrukturen

Ist  $(G, \cdot)$  eine Gruppe,  $X = G'$  eine bloße Menge und  $\phi : G \rightarrow X$  eine Bijektion, so kann man  $X$  derart zu einer Gruppe  $(G', *)$  machen, dass  $\phi$  ein Gruppenhomomorphismus ist.

$$\phi : (G, \cdot) \rightarrow X = G' \text{ Bijektion}$$

vorwärtsgeschobene Gruppenstruktur auf  $G'$ :

$$x * y := \phi(\phi^{-1}(x) \cdot \phi^{-1}(y))$$

$$1^* := \phi(1)$$

$$x^{-1*} := \phi(\phi^{-1}(x)^{-1})$$

$$1) \phi^{-1}(x * y) = \phi^{-1}(x) \cdot \phi^{-1}(y)$$

$$2) \phi^{-1}(1^*) = 1$$

$$3) \phi^{-1}(x^{-1*}) = \phi^{-1}(x)^{-1}$$

$$\phi^{-1} : (G', *) \xrightarrow{\sim} (G, \cdot)$$

$$1') \phi(ab) = \phi(a) * \phi(b)$$

$$2') \phi(1) = 1^*$$

$$3') \phi(a^{-1}) = \phi(a)^{-1}$$

$$\phi : (G, \cdot) \xrightarrow{\sim} (G', *)$$

Gruppenaxiome folgen aus (1-3) oder (1'-3'); man kann sie auch direkt nachprüfen:

$$\begin{aligned} x * (y * z) &= x * \phi(\phi^{-1}(y) \cdot \phi^{-1}(z)) \\ &= \phi(\phi^{-1}(x) \cdot \phi^{-1}(\phi(\phi^{-1}(y) \cdot \phi^{-1}(z)))) \\ &= \phi(\phi^{-1}(x) \cdot (\phi^{-1}y \cdot \phi^{-1}(z))) \\ &= \phi((\phi^{-1}(x) \cdot \phi^{-1}(y)) \cdot \phi^{-1}(z)) \\ &= \phi(\phi^{-1}(\phi(\phi^{-1} \cdot \phi^{-1}(y))) \cdot \phi^{-1}(z)) \\ &= \phi(\phi^{-1}(x * y) \cdot \phi^{-1}z) \\ &= (x * y * z) \end{aligned}$$

Genau analog: Zurückziehen

$$X = G' \xrightarrow{\psi} (G, \cdot) \text{ Bijektion}$$

$$x * y := \psi^{-1}(\psi(x) \cdot \psi(y))$$

$$1^* := \psi^{-1}(1)$$

$$x^{-1*} := \psi^{-1}(\psi(x)^{-1})$$

#### Beispiel 5.3.11.

1. **Tangens:**  $(\mathbb{R}, +) \xrightarrow{\tan} (\mathbb{R}, *)$   
(nicht für  $n\frac{\pi}{2}$  definiert!)

$$\tan(a + b) = \frac{\tan(a) + \tan(b)}{1 - \tan(a)\tan(b)}$$

$$x * y := \frac{x + y}{1 - xy}$$

2.  $G = \mathbb{R}$  mit Addition  
 $G' = \mathbb{R}_{>0}$  mit Multiplikation

- Das geometrische Mittel ist das mit  $\psi = \ln$  zurückgezogene arithmetisches Mittel:

$$\exp\left(\frac{\ln(x) + \ln(y)}{2}\right) = \exp\left(\frac{\ln(xy)}{2}\right) = \exp(\ln \sqrt{xy}) = \sqrt{xy}$$

- Das harmonische Mittel ist das mit  $\psi = \frac{1}{t}$  zurückgezogene arithmetische Mittel

$$G' = \mathbb{R}_{>0}, \left(\frac{x^{-1} + y^{-1}}{2}\right)^{-1} = \frac{2}{\frac{1}{x} + \frac{1}{y}} = \frac{2}{\frac{y+x}{xy}} = \frac{2xy}{x+y}$$

3.  $G = (\mathbb{R}, +) \xrightarrow{\psi=(\ )^3} G' = \mathbb{R}$   
 $x * y = (\sqrt[3]{x} + \sqrt[3]{y})^3 = x + 3\sqrt[3]{x^2y} + 3\sqrt[3]{xy^2} + y$   
 $x^{-1*} = -x$   
 $0^* = 0$  „Deformation der Addition“

### 5.3.2 Einige wichtige Isomorphismen

1.  $\mathbb{Z}/n \xrightarrow{\cong} \mu_n \xrightarrow{\cong} \text{Rot}_n \subset D_{2n}$  Diedergruppe

$$\bar{k} \mapsto \zeta_n^k \mapsto \mathcal{A}_n = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}$$

2. Gruppe mit zwei Elementen:

$$\begin{array}{ccccc} \mathbb{Z}/2 & \cong & \mathbb{S}^0 & \cong & \mathfrak{S}_2 \\ 0 & \mapsto & 1 & \mapsto & \text{id} \\ 1 & \mapsto & -1 & \mapsto & (12) \end{array}$$

3. Die folgenden Isomorphismen hängen von einer Basis  $\mathcal{A}$  von  $V$  ab ( $\dim V = n$ ):

$$\text{GL}(V) \begin{array}{c} \xrightarrow{M_{\mathcal{A}\mathcal{A}}} \\ \xleftarrow{L_{\mathcal{A}\mathcal{A}}} \end{array} \text{GL}_n(\mathbb{K})$$

4.  $\mathcal{S}_n \xrightarrow{\cong} P_n$  Permutationsmatrizen

$$\sigma \mapsto P_\sigma$$

5.  $\text{Zen}(\text{GL}_n(V)) \cong \text{Zen}(\text{GL}_n(\mathbb{K})) \cong \mathbb{K}^\times$ ,  $n \geq 3$

$$\text{Diagonalmatrizen } D_n \rightarrow (\mathbb{K}^\times)^n$$

$$D[\lambda_1, \dots, \lambda_n] \mapsto (\lambda_1, \dots, \lambda_n)$$

6. Diedergruppen:  $D_2 \cong \mathcal{S}_2$ ,  $D_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ ,  $D_6 \cong \mathcal{S}_3$

7. Platonische Gruppen:

- Tetraeder:  $\mathfrak{T} \cong \mathfrak{A}_4$
- Würfel und Oktaeder:  $\mathfrak{W} \cong \mathfrak{O} \cong \mathfrak{S}_4$
- Dodekaeder und Ikosaeder:  $\mathfrak{D} \cong \mathfrak{I} \cong \mathfrak{A}_5$

### 8. Automorphismengruppen

- a)  $\mathbb{Z} \xrightarrow{\text{id}} \mathbb{Z}$ ,  $-\text{id} : \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $n \mapsto -n$   
 $\text{Aut}(\mathbb{Z}) = \{\text{id}, -\text{id}\} \cong \mathbb{S}^0$

- b)  $\mathbb{Z}/2 \rightarrow \mathbb{Z}/2$ : nur die Identität

$$\bar{0} \mapsto \bar{0}$$

$$\bar{1} \mapsto \bar{1}$$

$$\text{Aut}(\mathbb{Z}/2) = \bar{1}$$

- c)  $\mathbb{Z}/3 \rightarrow \mathbb{Z}/3$ : außer der Identität noch  $\theta = -\text{id}$ .

$$\theta : \bar{0} \mapsto \bar{0}$$

$$\bar{1} \mapsto \bar{2}$$

$$\bar{2} \mapsto \bar{1}$$

$$\text{Aut}(\mathbb{Z}/3) \cong \mathbb{S}^0$$

## 5.4 Produkte

**Definition 5.4.1.** Gegeben seien zwei Gruppen  $G_1$  und  $G_2$ . Wir definieren eine neue Gruppe  $G = G_1 \times G_2$  mit der Multiplikation

$$\begin{aligned} (x_1, x_2) \cdot (y_1, y_2) &:= (x_1 \cdot y_1, x_2 \cdot y_2) \\ (x_1, x_2)^{-1} &:= (x_1^{-1}, x_2^{-1}) \\ 1 &:= (1, 1) \end{aligned}$$

Offenbar ist das wieder eine Gruppe und wird *direktes Produkt* genannt.

**Beispiel 5.4.2.**

1.  $V = \mathbb{K}^n = \mathbb{K}^{n_1} \times \mathbb{K}^{n_2} \quad n_1 + n_2 = n$
2.  $(\mathbb{R}^\times, \cdot) \cong (\mathbb{S}^0, \cdot) \times (\mathbb{R}_{>0}, \cdot)$   
 $x \mapsto \left(\frac{x}{|x|}, |x|\right)$
3.  $\mathbb{C}^\times \cong \mathbb{S}^1 \times \mathbb{R}_{>0}$   
 $z \mapsto \left(\frac{z}{|z|}, |z|\right)$
4.  $V \supset U_1, U_2$  Untervektorräume,  
 $V = U_1 + U_2, U_1 \cap U_2 = 0$   
 $V \cong U_1 \times U_2 =: U_1 \oplus U_2$  interne direkte Summe  
 $(u_1, u_2) \mapsto u_1 + u_2$
5. Sei  $V$  wie in 4.

$$\begin{array}{ccc} \text{GL}(V) & \supseteq & G = \{f \in \text{GL}(V) \mid f(U_1) \subseteq U_1, f(U_2) \subseteq U_2\} & \ni & f \\ & & \downarrow & & \downarrow \\ & & \text{GL}(U_1) \times \text{GL}(U_2) & \ni & (f_1, f_2) \end{array}$$

wobei  $f_i = f|_{U_i} : U_i \rightarrow U_i$ .

**Eigenschaften**

•

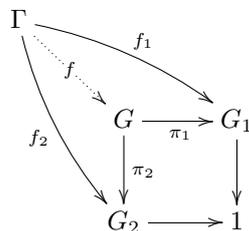
$$x_1 \xrightarrow{i_1} (x_1, 1); (1, x_2) \xleftarrow{i_2} x_2 \quad \text{Inklusionen}$$

$$\begin{array}{ccccc} & & i_1 & & \\ & & \rightarrow & & \\ G_1 & \xleftrightarrow{\quad} & G_1 \times G_2 & \xleftrightarrow{\quad} & G_2 \\ & & \xleftarrow{\pi_1} & & \xleftarrow{\pi_2} \\ & & & & \end{array}$$

$$x_1 \xleftarrow{\pi_1} (x_1, x_2) \xrightarrow{\pi_2} x_2 \quad \text{Projektionen}$$

- $G_1, G_2$  abelsch  $\implies G_1 \times G_2$  abelsch.
- Im abelschen Falle sagt man *direkte Summe* und schreibt auch  $G = G_1 \oplus G_2$ .  
 Bsp.:  $\mathbb{Z}/6 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/3$

**Proposition 5.4.3** (Universelle Eigenschaft). *Zu je zwei Homomorphismen  $f_1 : \Gamma \rightarrow G_1, f_2 : \Gamma \rightarrow G_2$  gibt es genau einen Homomorphismus  $f = (f_1, f_2) : \Gamma \rightarrow G_1 \times G_2$  mit  $f_1 = \pi_1 \circ f, f_2 = \pi_2 \circ f$ :*



Wir erhalten eine Bijektion von Mengen

$$\begin{aligned} \text{Hom}(\Gamma, G) &\xrightarrow{\cong} \text{Hom}(\Gamma, G_1) \times \text{Hom}(\Gamma, G_2) \\ f &\mapsto (\pi_1 \circ f, \pi_2 \circ f) \\ (f : \gamma \mapsto (f_1(\gamma), f_2(\gamma))) &\longleftarrow (f_1, f_2) \end{aligned}$$

## 5.5 Direkte Summen von Vektorräumen

### 5.5.1 Externe direkte Summe

**Definition 5.5.1.** Sind  $V_1, V_2$  zwei Vektorräume, so ist  $V := V_1 \times V_2$  mit

$$\begin{aligned} \text{Addition} & \quad (v_1, v_2) + (v'_1, v'_2) := (v_1 + v'_1, v_2 + v'_2) \\ \text{Null} & \quad 0 := (0, 0) \\ \text{Negative} & \quad -(v_1, v_2) = (-v_1, -v_2) \\ \text{Skalierung} & \quad \lambda(v_1, v_2) = (\lambda v_1, \lambda v_2) \end{aligned}$$

wieder ein Vektorraum. Wir schreiben  $V = V_1 \oplus V_2$ .

- Es gibt Monomorphismen (Inklusionen)

$$\begin{aligned} i_1 : V_1 &\rightarrow V, & i_2 : V_2 &\rightarrow V \\ v_1 &\mapsto (v_1, 0) & v_2 &\mapsto (0, v_2) \end{aligned}$$

und Epimorphismen (Projektionen)

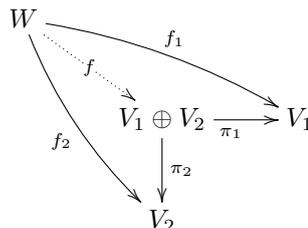
$$\begin{aligned} \pi_1 : V &\rightarrow V_1, & \pi_2 : V &\rightarrow V_2 \\ (v_1, v_2) &\mapsto v_1 & (v_1, v_2) &\mapsto v_2 \end{aligned}$$

- $\dim(V_1 \oplus V_2) = \dim(V_1) + \dim(V_2)$
- $\pi_1 \circ i_2 = 0, \pi_2 \circ i_1 = 0$
- $\pi_1 \circ i_1 = \text{id}_{V_1}, \pi_2 \circ i_2 = \text{id}_{V_2}$
- $(i_1 \circ \pi_1)^2 = (i_1 \circ \pi_1), (i_2 \circ \pi_2)^2 = (i_2 \circ \pi_2)$

**Beispiel 5.5.2.** •  $V = \mathbb{K}^n = \mathbb{K}^{n_1} \times \mathbb{K}^{n_2}$  für  $n = n_1 + n_2$

- $0 \oplus V \cong V \cong V \oplus 0$
- $V_1 \oplus (V_2 \oplus V_3) \cong (V_1 \oplus V_2) \oplus V_3$
- $V_1 \oplus V_2 \cong V_2 \oplus V_1$

**Satz 5.5.3** (Universelle Eigenschaft („Produkt“)). • Zu je zwei linearen Abbildungen  $f_1 : W \rightarrow V_1, f_2 : W \rightarrow V_2$  gibt es genau eine lineare Abbildung  $f : W \rightarrow V_1 \oplus V_2$  mit  $f_1 = \pi_1 \circ f, f_2 = \pi_2 \circ f$ :



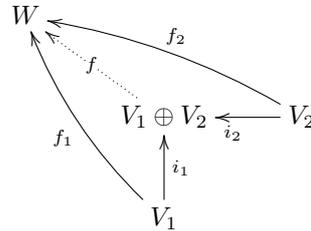
Anders gesagt:

$$\Pi : \text{Hom}(W, V_1 \oplus V_2) \longrightarrow \text{Hom}(W, V_1) \oplus \text{Hom}(W, V_2) \\ f \longmapsto (\pi_1 \circ f, \pi_2 \circ f)$$

ist eine Bijektion von Mengen.

- Darüber hinaus ist  $\Pi$  sogar linear, d.h. ein Isomorphismus von Vektorräumen.

**Satz 5.5.4** (Universelle Eigenschaft „Summe“). • Zu je zwei linearen Abbildungen  $f_1 : V_1 \rightarrow W$  und  $f_2 : V_2 \rightarrow W$  gibt es genau eine lineare Abbildung  $f : V_1 \oplus V_2 \rightarrow W$  mit  $f \circ i_1 = f|_{V_1}$  und  $f \circ i_2 = f|_{V_2} = f_2$



Anders gesagt:

$$\Sigma : \text{Hom}(V_1 \oplus V_2, W) \longrightarrow \text{Hom}(V_1, W) \oplus \text{Hom}(V_2, W)$$

$$f \longmapsto (f \circ i_1, f \circ i_2)$$

ist eine Bijektion von Mengen.

- Darüber hinaus ist  $\Sigma$  sogar linear, d.h. ein Isomorphismus von Vektorräumen.

### 5.5.2 Interne direkte Summe

**Definition 5.5.5.** Sind  $U_1, U_2 \subseteq V$  Untervektorräume und gilt  $U_1 + U_2 = V$  sowie  $U_1 \cap U_2 = 0$ , so heißt  $V$  direkte interne Summe von  $U_1$  und  $U_2$ . Wir nennen  $U_1$  und  $U_2$  komplementär (in  $V$ ).

- $i_1 : U_1 \rightarrow V, i_2 : U_2 \rightarrow V$  sind Monomorphismen.

**Proposition 5.5.6** (Universelle Eigenschaft der Summe, intern). Es sei  $V$  die interne direkte Summe von  $U_1$  und  $U_2$ .

- (i) Zu je zwei Homomorphismen  $f_1 : U_1 \rightarrow W, f_2 : U_2 \rightarrow W$  gibt es genau einen Homomorphismus  $f : V \rightarrow W$  mit  $f \circ i_1 = f|_{U_1} = f_1 : U_1 \rightarrow W$  und  $f \circ i_2 = f|_{U_2} = f_2 : U_2 \rightarrow W$ .

Anders gesagt:

$$\Sigma : \text{Hom}(V, W) \longrightarrow \text{Hom}(U_1, W) \oplus \text{Hom}(U_2, W)$$

$$f \longmapsto (f \circ i_1, f \circ i_2)$$

ist eine Bijektion von Mengen.

- (ii) Darüber hinaus ist  $\Sigma$  sogar linear, d.h. ein Isomorphismus von Vektorräumen.

**Proposition 5.5.7.** Ist  $V$  die interne direkte Summe von  $U_1$  und  $U_2$ , so ist  $V$  isomorph zur externen direkten Summe  $V \cong U_1 \oplus U_2$ .

Beweis.

$$\phi : U_1 \oplus U_2 \longrightarrow V$$

$$(u_1, u_2) \longmapsto u_1 + u_2$$

ist ein Isomorphismus:

- 1) linear
- 2) Epimorphismus wegen  $U_1 + U_2 = V$
- 3) Monomorphismus wegen  $U_1 \cap U_2 = 0$ .

□

Damit haben wir auch Projektionen  $\pi'_i : V \rightarrow U_i$  durch  $\pi'_i = \pi_i \circ \phi^{-1}$ : ist  $v$  zerlegt in  $v = u_1 + u_2$ , so ist  $\pi'_i(v) = u_i$ .

**Proposition 5.5.8.** Ist  $V = V_1 \oplus V_2$  die externe direkte Summe von  $V_1$  und  $V_2$ , so ist  $V$  die interne direkte Summe von  $U_1 = i_1(V_1) = \{(v_1, 0) \in V \mid v_1 \in V_1\}$  und  $U_2 = i_2(V_2) = \{(0, v_2) \in V \mid v_2 \in V_2\}$ .

## 5.6 Quotientenvektorräume

Es sei  $U \subseteq V$  ein Untervektorraum. Wir definieren eine Äquivalenzrelation auf  $V$ :

**Definition 5.6.1.** Zwei Vektoren  $v, v' \in V$  heißen *kongruent modulo  $U$*  genau dann, wenn  $v - v' \in U$  gilt. Notation:  $v \equiv v' \pmod{U} \iff v - v' \in U$ .

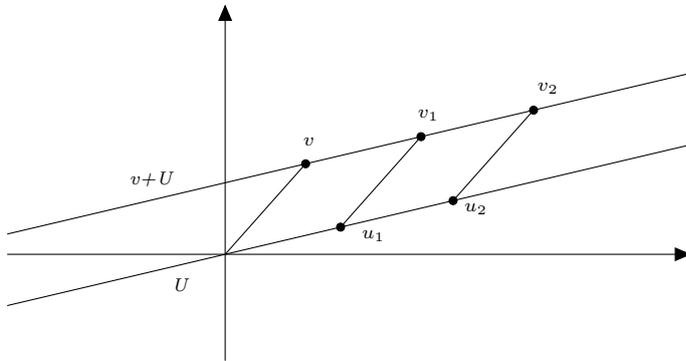
- Äquivalenzrelation

- 1)  $v \equiv v$ , da  $v - v = 0 \in U$ .
- 2)  $v \equiv v' \iff v' \equiv v$ , weil aus  $v - v' \in U$  natürlich  $v' - v \in U$  folgt.
- 3)  $v \equiv v', v' \equiv v'' \implies v \equiv v''$ , weil aus  $v - v' \in U$  und  $v' - v'' \in U$  auch  $v - v'' = (v - v') + (v' - v'') \in U$  folgt.

- Äquivalenzklassen

$$[v]_U := \{v' \in V \mid v \equiv v' \pmod{U}\}$$

**Lemma 5.6.2.**  $[v]_U = v + U$  (affiner Unterraum)



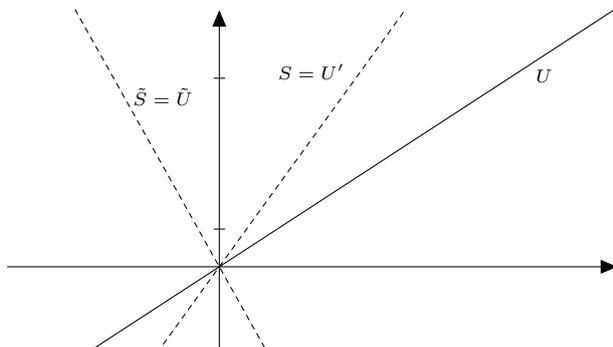
*Beweis.*

$$[v]_U \in \begin{array}{l} v' \mapsto v + (v - v') \in v + U \\ v + u \longleftarrow v + u \end{array}$$

□

- 1)  $[v]_U \neq \emptyset$ , denn  $v \in [v]_U$ .
- 2)  $[v_1]_U$  und  $[v_2]_U$  sind gleich ( $\iff v_1 \equiv v_2$ ) oder disjunkt ( $\iff v_1 \not\equiv v_2$ ).
- 3)  $V = \bigcup_{v \in V} [v]_U$ .
- 4)  $[0] = U$  ausgezeichnete Klasse

**Definition 5.6.3.** Ein „Schnitt“ oder *Repräsentantensystem* ist eine Teilmenge  $S \subseteq V$ , so dass  $S \cap [v]_U$  aus genau einem Element  $v_s$  besteht (für alle  $v \in V$ ).



**Beispiel 5.6.4.** Ist  $U'$  komplementärer Unterraum zu  $U$  (d.h.  $V = U + U', U \cap U' = 0$ ), so ist  $S = U'$  ein Schnitt;  $V$  ist in diesem Fall die interne direkte Summe von  $U$  und  $U'$ .

Für einen Schnitt  $S$  haben wir eine Bijektion

$$\begin{aligned} S &\xrightarrow{\cong} V/U = \{[v]_U \mid v \in V\} && \text{Menge der Äquivalenzklassen} \\ s &\longmapsto [s]_U \end{aligned}$$

**Definition 5.6.5.** Die Menge  $V/U$  wird wie folgt zu einem Vektorraum (über  $\mathbb{K}$ ), welcher *Quotientenvektorraum* heißt:

- Addition:

$$\begin{aligned} V/U \times V/U &\xrightarrow{+} V/U \\ [v_1]_U + [v_2]_U &:= [v_1 + v_2]_U \end{aligned}$$

- Null:  $0 := [0]_U = U$
- Skalierung  $\lambda \cdot [v]_U := [\lambda v]_U$ , also  $\lambda \cdot (v + U) := \lambda v + U$

*Beweis.* a) Wohldefiniertheit

- der Addition:

$$\begin{aligned} v_1 \equiv v'_1 \quad v_2 \equiv v'_2 &\implies v'_1 = v_1 + u_1 \quad v'_2 = v_2 + u_2 \implies v'_1 + v'_2 = v_1 + v_2 + (u_1 + u_2) \implies v'_1 + v'_2 \equiv v_1 + v_2 \end{aligned}$$

- der Skalierung:

$$v_1 \equiv v_2 \implies \lambda v_1 \equiv \lambda v_2$$

b) Vektorraumaxiome: nachrechnen.

□

**Proposition 5.6.6.** 1)  $U = 0: V/0 \cong V, [v] = v + 0 = v.$

2)  $U = V: V/V \cong 0, [v] = v + V = V.$

3) Sind  $U, U'$  komplementäre Untervektorräume von  $V$ , so ist  $V/U \cong U'$ .

*Beweis.* Wir zeigen 3): Wir haben eine Bijektion

$$\begin{aligned} S = U' &\xrightarrow{\varphi} V/U \\ u' &\longmapsto [u']_U \end{aligned}$$

Diese ist ein Isomorphismus, denn

$$\begin{aligned} u'_1 + u'_2 &\mapsto [u'_1 + u'_2]_U = [u'_1]_U + [u'_2]_U \\ \lambda u' &\mapsto [\lambda u']_U = \lambda [u']_U \end{aligned}$$

□

**Proposition 5.6.7.**  $\dim_{\mathbb{K}} V/U = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} U.$

*Beweis.* Es sei  $\{b_1, \dots, b_m\} = \mathfrak{B}'$  eine Basis von  $U'$ , die wir zu einer Basis  $\mathfrak{B} = \{b_1, \dots, b_m, b_{m+1}, \dots, b_n\}$  ergänzen.

Dann ist  $\overline{\mathfrak{B}} = \{\pi_U(b_{m+1}), \dots, \pi_U(b_n)\}$  eine Basis für  $V/U$ : es ist ein Erzeugendensystem und linear unabhängig. □

**Satz 5.6.8** (Universelle Eigenschaft). (i) Die Abbildung  $\pi_U : V \rightarrow V/U, v \mapsto [v]_U = v + U$  ist linear und surjektiv.

(ii) Für jede lineare Abbildung  $f : V \rightarrow W$  mit  $U \subseteq \ker(f)$  gibt es genau eine lineare Abbildung  $f' : V/U \rightarrow W$  mit  $f = f' \circ \pi_U.$

$$\begin{array}{ccc} U \subseteq \ker(f) \subseteq & V & \xrightarrow{f} W \\ & \downarrow \pi_U & \nearrow f_U \\ & V/U & \end{array}$$

*Beweis.* (i)  $\pi_U$  ist offenbar surjektiv und nach Konstruktion der Struktur auf  $V/U$  auch linear.

(ii) Wir setzen  $f_U([v]) = f_U(v + U) = f(v) \in W$ .

Dies ist wohldefiniert, denn

$$f(v + u) = f(v) + \underbrace{f(u)}_{=0, \text{ weil } U \subseteq \ker(f)} = f(v)$$

Weil  $\pi_U$  surjektiv ist, ist  $f_U$  eindeutig bestimmt.

□

*Bemerkung.* Der Beweis zeigt, wie man zu einer Basis von  $V/U$  kommt:

- 1) Ist  $\{b_1, b_2, \dots\} = \mathfrak{E}$  ein Erzeugendensystem von  $V$ , so ist  $\pi_U(\mathfrak{E}) = \{\pi_U(b_1), \dots\}$  ein Erzeugendensystem von  $V/U$ , aus dem man eine Basis auswählen kann.
- 2) Ist  $\mathfrak{B}'$  eine Basis von  $U$  und  $\mathfrak{B} \supseteq \mathfrak{B}'$  eine ergänzte Basis von  $V$ , so ist  $\overline{\mathfrak{B}} = \pi_U(\mathfrak{B} \setminus \mathfrak{B}')$  eine Basis von  $V/U$ .

Mit dieser 2. Bemerkung sieht man, dass dies auch für unendlich-dimensionale Vektorräume gilt.

**Satz 5.6.9.** *Jeder Untervektorraum  $U \subset V$  besitzt einen komplementären Unterraum  $U'$ :*

$$(1) \quad U + U' = V \qquad (2) \quad U \cap U' = 0$$

*Beweis.* Wie oben.

□

**Satz 5.6.10.** *Es sei  $f : V \rightarrow W$  eine lineare Abbildung. Dann ist*

$$\begin{array}{ccc} V/\ker(f) & \xrightarrow{\cong} & \text{im}(f) \\ [v] & \mapsto & f(v) \end{array}$$

ein Isomorphismus.

**Korollar 5.6.11.** *Sei  $f : V \rightarrow W$  eine lineare Abbildung. Ist  $U'$  komplementär zu  $\ker(f) = U$ , so ist*

$$\varphi = f|_{U'} : U' \longrightarrow W' := \text{im}(f)$$

ein Isomorphismus.

**Beispiel 5.6.12.** Wir betrachten ein lineares Gleichungssystem  $Ax = b$  mit  $A \in \text{Mat}_{m,n}(\mathbb{K})$ ,  $b \in \mathbb{K}^m$ . Sei

$$f = T_A : \mathbb{K}^n \longrightarrow \mathbb{K}^m, x \mapsto Ax,$$

und  $V = \mathbb{K}^n$ ,  $W = \mathbb{K}^m$ .

•

$$U = \begin{array}{l} \mathcal{L}(A \mid 0) = \ker(T_A) = 0 + U \quad \text{Lösungen des homogenen Systems (linearer Unterraum)} \\ \mathcal{W}(A) = \text{im}(T_A) \cong V/\mathcal{L}(A \mid 0) \end{array}$$

- $v + U = \mathcal{L}(A \mid b)$ , falls  $f(v) = b$  ( $\Leftrightarrow b \in \mathcal{W}(A)$ ) (affiner Unterraum)
- $\emptyset = \mathcal{L}(A \mid b)$ , falls es kein  $v \in V$  mit  $f(v) = b$  gibt ( $\Leftrightarrow b \notin \mathcal{W}(A)$ ).
- $V$  ist zerlegt in die affinen Unterräume  $v + U = \mathcal{L}(A \mid f(v))$  einer davon ist  $U = \mathcal{L}(A \mid 0)$ .
- Ist  $U'$  komplementär zu  $U$  so besitzt jeder affine Raum einen eindeutigen Repräsentanten

$$u' + \mathcal{L}(A \mid 0) = \mathcal{L}(A \mid f(u'))$$

## 5.7 Normale Untergruppen

Sei  $G$  eine Gruppe. Wir betrachten für ein festes  $\gamma \in G$  die Funktion

$$I_\gamma : G \rightarrow G, \quad I_\gamma(g) = \gamma g \gamma^{-1},$$

welche *Konjugation mit  $\gamma$*  heißt.

(1)  $I_\gamma$  ist ein Homomorphismus von  $G$ , denn

$$\begin{aligned} I_\gamma(1) &= \gamma \cdot 1 \cdot \gamma^{-1} = 1, \\ I_\gamma(xy) &= \gamma xy \gamma^{-1} = \gamma x \gamma^{-1} \gamma y \gamma^{-1} = I_\gamma(x) I_\gamma(y) \end{aligned}$$

(2)  $I_1 = \text{id}_G$ , denn  $I_1(x) = 1x1^{-1} = x$ .

$$\begin{aligned} I_\alpha \circ I_\beta &= I_{\alpha\beta}, \text{ denn } I_\alpha(I_\beta(x)) = \alpha\beta x \beta^{-1} \alpha^{-1} = (\alpha\beta)x(\alpha\beta)^{-1}. \\ I_\alpha^{-1} &= I_{\alpha^{-1}}. \end{aligned}$$

(3) Also ist  $I_\gamma : G \rightarrow G$  ein Automorphismus für jedes  $\gamma \in G$ .

(4) Und  $I : G \rightarrow \text{Aut}(G), \gamma \mapsto I_\gamma$  ist ein Homomorphismus.

(5) Ist  $\gamma \in \text{Zen}(G)$ , so ist  $I_\gamma = \text{id}_G$ ; und umgekehrt. Also ist  $\text{Zen}(G) = \ker(I)$ .

Insbesondere ist  $I_\gamma = \text{id}$  für alle  $\gamma \in G$  wenn  $G$  abelsch ist.

Man nennt die  $I_\gamma$  *innere Automorphismen* von  $G$ . Sie bilden eine Untergruppe  $\text{Inn}(G) \leq \text{Aut}(G)$ .

Selbst eine abelsche Gruppe wie  $\mathbb{Z}/n$  kann nicht-innere Automorphismen haben:

$$\alpha : \mathbb{Z}/3 = \{\underline{0}, \underline{1}, \underline{2}\} \rightarrow \mathbb{Z}/3, \quad \underline{0} \mapsto \underline{0}, \underline{1} \mapsto \underline{2}, \underline{2} \mapsto \underline{1}$$

Es ist  $\text{Inn}(\mathbb{Z}/3) = 1$  und  $\text{Aut}(\mathbb{Z}/3) = \{\text{id}, \alpha\}$ .

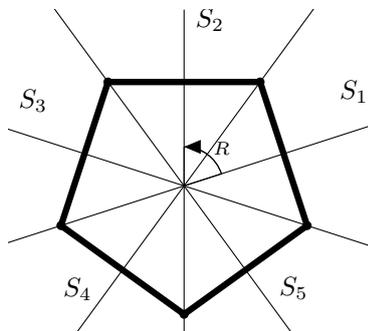
**Definition 5.7.1.** Eine Untergruppe  $H \subset G$  heißt *normal* (oder ein *Normalteiler*, am besten „selbstkonjugiert“), falls  $I_\gamma(H) = H$  gilt für alle  $\gamma \in G$ .

Für eine Untergruppe  $H$  von  $G$  ist

$$I_\gamma(H) = \gamma H \gamma^{-1} = \{\gamma h \gamma^{-1} \mid h \in H\} \leq G$$

wieder eine Untergruppe von  $G$ , und zwar isomorph zu  $H$ , aber vielleicht verschieden von  $H$ . Für einen Normalteiler ist hingegen  $I_\gamma(H) = H$ .

**Beispiel 5.7.2.** 1)  $G = D_{2n}$  Diedergruppe mit Spiegelungen  $S_1, \dots, S_n$  mit  $S_i^2 = 1$  und Rotation  $R$  mit  $R^n = 1$ .



- $H_i := \{1, S_i\}$  ist nicht normal, da  $RH_iR^{-1} = H_{i+1}$  wegen  $RS_iR^{-1} = S_{i+1}$
- $\text{Rot}_n = \{1, R, R^2, \dots, R^{n-1}\}$  ist normal, denn  $S_iRS_i^{-1} = R^{-1}$ .

2) In einer abelschen Gruppe  $G$  ist jede Untergruppe normal.

3) In  $G = \mathfrak{S}_n$  ist  $H = \{1, (1, 2)\}$  nicht normal, denn  $(2, 3)H(2, 3) = \{1, (1, 3)\}$ .

4)  $\text{Inn}(G)$  ist normal in  $\text{Aut}(G)$ .

5) Die *alternierende Gruppe*  $\mathfrak{A}_n := \{\sigma \in \mathfrak{S}_n \mid \text{sign } \sigma = 1\} = \ker(\text{sign})$  ist normal in  $\mathfrak{S}_n$ .

*Beweis.* Sei  $\sigma \in \mathfrak{A}_n$ . Dann ist für alle  $g \in \mathfrak{S}_n$

$$\begin{aligned}\text{sign}(g\sigma g^{-1}) &= \text{sign}(g) \text{sign}(\sigma) \text{sign}(g^{-1}) \\ &= \text{sign}(g) \cdot 1 \cdot \text{sign}(g)^{-1} = 1\end{aligned}$$

□

Also ist mit  $\sigma$  auch  $g\sigma g^{-1}$  wieder in  $\mathfrak{A}_n$ , für alle  $g \in \mathfrak{S}_n$ .

Das letzte Beispiel lässt sich verallgemeinern:

**Lemma 5.7.3.** *Ist  $\varphi : G \rightarrow G'$  ein Homomorphismus, so ist  $\ker(\varphi)$  normal in  $G$ .*

*Beweis.* Sei  $x \in \ker(\varphi)$ , also  $\varphi(x) = 1$ . Dann gilt für jedes  $g \in G$ :

$$\begin{aligned}\varphi(gxg^{-1}) &= \varphi(g)\varphi(x)\varphi(g^{-1}) \\ &= \varphi(g) \cdot 1 \cdot \varphi(g)^{-1} = 1\end{aligned}$$

Also ist auch  $gxg^{-1} \in \ker(\varphi)$ . □

*Bemerkung.* Es gibt Gruppen, die (außer  $H = 1, H = G$ ) keine normalen Untergruppen haben; diese nennt man *einfache* Gruppen (weil sie in einem gewissen Sinne unzerlegbar sind). Z.B ist die alternierende Gruppe  $\mathfrak{A}_n$  einfach für  $n \geq 5$ .

**Definition 5.7.4.** (i) Zwei Elemente  $g_1, g_2 \in G$  heißen *konjugiert*, wenn es ein  $\gamma \in G$  gibt mit  $\gamma g_1 \gamma^{-1} = g_2$ . Notation:  $g_1 \sim g_2$ .

(ii) Zwei Untergruppen  $H_1, H_2 \leq G$  heißen *konjugiert*, wenn es ein  $\gamma \in G$  gibt mit  $\gamma H_1 \gamma^{-1} = H_2$ . Notation:  $H_1 \sim H_2$ .

a) Konjugiertheit ist eine Äquivalenzrelation für Elemente:

- $g \sim g$ , denn  $I_1(g) = g$ .
- $g_1 \sim g_2 \implies \exists \gamma \in G : \gamma g_1 \gamma^{-1} = g_2 \Leftrightarrow \exists \gamma' = \gamma^{-1} g_1 = \gamma^{-1} g_2 \gamma = \gamma' g_2 \gamma'^{-1} \implies g_2 \sim g_1$ .
- $g_1 \sim g_2, g_2 \sim g_3 \implies \exists \gamma : \gamma g_1 \gamma^{-1} = g_2$ , also  $\exists \gamma' : \gamma' g_2 \gamma'^{-1} = g_3$  und somit  $\gamma \gamma' g_1 \gamma'^{-1} \gamma^{-1} = (\gamma \gamma') g_1 (\gamma \gamma')^{-1} = g_3$ , d.h.  $g_1 \sim g_3$ .

b) Konjugierte Elemente haben gleiche Ordnung. Ist nämlich  $g_1^n = 1$  und  $\gamma g_1 \gamma^{-1} = g_2$ , so ist

$$g_2^n = (\gamma g_1 \gamma^{-1})^n = \gamma g_1 \gamma^{-1} \gamma g_1 \gamma^{-1} \dots \gamma g_1 \gamma^{-1} = \gamma g_1^n \gamma^{-1} = \gamma \gamma^{-1} = 1,$$

also ist die Ordnung von  $g_2$  höchstens so groß wie die Ordnung von  $g_1$ . Die Rückrichtung ist analog.

c) Ist  $\varphi : G \rightarrow G'$  ein Homomorphismus und  $g_1 \sim g_2$ , so auch  $\varphi(g_1) \sim \varphi(g_2)$ :

$$g_1 \sim g_2 \implies \exists \gamma : \gamma g_1 \gamma^{-1} = g_2 \implies \varphi(\gamma g_1 \gamma^{-1}) = \varphi(\gamma) \varphi(g_1) \varphi(\gamma)^{-1} = \varphi(g_2)$$

d) Konjugiertheit ist eine Äquivalenzrelation auf der Menge der Untergruppen von  $G$ .

e) Konjugierte Untergruppen sind isomorph.

**Beispiel 5.7.5.** (1)  $G = \mathfrak{S}_n$ :  $\alpha \sim \beta \Leftrightarrow \text{Typ}(\alpha) = \text{Typ}(\beta)$ .

(2)  $G = D_{2n}$ : Ist  $n$  ungerade, so sind alle Spiegelungen  $S_i$  zueinander konjugiert. Ist  $n$  gerade, so zerfallen die Spiegelungen in zwei Konjugationsklassen.

(3) In einer abelschen Gruppe ist jedes Element nur zu sich selbst konjugiert; ebenso für Untergruppen.

(4) In jeder Gruppe ist das neutrale Element 1 nur zu sich selbst konjugiert; ebenso die Untergruppen  $H = 1, H = G$ .

## 5.8 Quotientengruppen

Es sei  $G$  eine Gruppe und  $H \leq G$  eine Untergruppe.

**Definition 5.8.1.** Für ein  $g \in G$  ist seine *Linksnebenklasse* die Teilmenge

$$gH = \{x = gh \mid h \in H\} \subset G,$$

und seine *Rechtsnebenklasse* die Teilmenge

$$Hg = \{y = hg \mid h \in H\} \subset G.$$

*Bemerkung.* (1) Für  $g \in H$  ist  $gH = Hg = H$ .

(2) Im Allgemeinen ist  $gH \neq Hg$ , und keine der beiden Nebenklassen ist eine Untergruppe (außer wenn  $g \in H$ ).

(3)  $G$  zerfällt sowohl in Links- als auch Rechtsnebenklassen, was man wie folgt sieht:

(4) Wir können zwei Äquivalenzrelationen  $\equiv_H, {}_H\equiv$  auf  $G$  definieren:

$$\begin{aligned} x_1 \equiv_H x_2 &\Leftrightarrow \exists h \in H : x_1 h = x_2 \\ &\Leftrightarrow x_1^{-1} x_2 \in H \end{aligned}$$

$$\begin{aligned} x_1 {}_H\equiv x_2 &\Leftrightarrow \exists h \in H : x_1 = h x_2 \\ &\Leftrightarrow x_1 x_2^{-1} \in H \end{aligned}$$

Für die Äquivalenzklassen  $[x]_H$  bzw.  ${}_H[x]$  gilt:

$$[x]_H = xH \quad \text{und} \quad {}_H[x] = Hx.$$

**Lemma 5.8.2.**  $|gH| = |H|$ .

*Beweis.*  $x = gh \mapsto g^{-1}x$  ist eine Bijektion. □

Da alle Äquivalenzklassen somit gleichmächtig sind, ist die Mächtigkeit von  $G$  gleich der Mächtigkeit von  $H$  mal der Anzahl der Äquivalenzklassen; die letzte Anzahl nennt man den *Index* von  $H$  in  $G$ , geschrieben  $[G : H]$ .

**Korollar 5.8.3.** Für eine endliche Gruppe gilt: die Ordnung einer Untergruppe  $H$  ist immer ein Teiler der Gruppenordnung:

$$|G| = |H| \cdot [G : H]$$

**Lemma 5.8.4.**  $H \leq G$  ist genau dann normal, wenn  $gH = Hg$  für alle  $g \in G$  gilt.

*Beweis.* klar (Übung). □

**Beispiel 5.8.5.** Wir betrachten in  $G = \mathfrak{S}_3$  die Untergruppen  $H = \{1, \langle 1, 2 \rangle\}$ ,  $N = \{1, \langle 1, 2, 3 \rangle = z, \langle 1, 3, 2 \rangle = z^2\}$  und listen sämtliche Links- und Rechtsnebenklassen auf, indem wir in den Spalten der folgenden Tabelle für jedes Element  $\sigma$  von  $\mathfrak{S}_3$  mit  $\times, \circ$  bzw.  $\otimes$  markieren, ob  $\sigma$  zur jeweiligen Linksnebenklasse, Rechtsnebenklasse bzw. zu beiden gehört.

$\times$	1	$\langle 1, 2 \rangle$	$\langle 1, 3 \rangle$	$\langle 2, 3 \rangle$	$\langle 1, 2, 3 \rangle$	$\langle 1, 3, 2 \rangle$	$\circ$
$1H$	$\otimes$	$\otimes$					$H1$
$\langle 1, 2 \rangle H$	$\otimes$	$\otimes$					$H \langle 1, 2 \rangle$
$\langle 1, 3 \rangle H$			$\otimes$		$\times$	$\circ$	$H \langle 1, 3 \rangle$
$\langle 2, 3 \rangle H$				$\otimes$	$\circ$	$\times$	$H \langle 2, 3 \rangle$
$\langle 1, 2, 3 \rangle H$			$\times$	$\circ$	$\otimes$		$H \langle 1, 2, 3 \rangle$
$\langle 1, 3, 2 \rangle H$			$\circ$	$\times$		$\otimes$	$H \langle 1, 3, 2 \rangle$
$1N$	$\otimes$				$\otimes$	$\otimes$	$N1$
$\langle 1, 2 \rangle N$		$\otimes$	$\otimes$	$\otimes$			$N \langle 1, 2 \rangle$
$\langle 1, 2 \rangle N$		$\otimes$	$\otimes$	$\otimes$			$N \langle 1, 3 \rangle$
$\langle 2, 3 \rangle N$		$\otimes$	$\otimes$	$\otimes$			$N \langle 2, 3 \rangle$
$\langle 1, 2, 3 \rangle N$	$\otimes$						$N \langle 1, 2, 3 \rangle$
$\langle 1, 3, 2 \rangle N$	$\otimes$				$\otimes$	$\otimes$	$N \langle 1, 3, 2 \rangle$

Man erkennt insbesondere, dass  $N$  ein Normalteiler ist,  $H$  aber nicht.

Es sei nun  $H \trianglelefteq G$  eine normale Untergruppe. Dann konstruieren wir eine neue Gruppe  $\Gamma := G/H = H \backslash G$  genannt *Quotientengruppe*, wie folgt:

- als Menge besteht  $\Gamma$  aus allen Linksnebenklassen (oder Rechtsnebenklassen)  $gH$  für  $g \in G$ . (Ist  $G$  endlich, so sind dies  $[G : H] = \frac{|G|}{|H|}$  Elemente
- als neutrales Element  $1 = 1_\Gamma$  nehmen wir  $1H = H$ .
- als Multiplikation setzen wir

$$g_1 \cdot g_2H := (g_1g_2)H.$$

- als Inverse setzen wir

$$(gH)^{-1} := g^{-1}H$$

Zu zeigen ist nur die Wohldefiniertheit der Multiplikation; alle Gruppenaxiome folgen dann sofort.

Seien  $g'_1 = g_1h_1$  und  $g'_2 = g_2h_2$  (für  $h_1, h_2 \in H$ ) andere Repräsentanten der gleichen Linksnebenklassen, so haben wir:

$$\begin{aligned} g'_1g'_2 &= g_1h_1g_2h_2 \\ &= g_1g_2 \underbrace{g_2^{-1}h_1g_2}_{\tilde{h} \in H, \text{ weil } H \text{ normal}} \\ &= g_1g_2\tilde{h}h_2. \end{aligned}$$

Also repräsentieren  $g'_1g'_2$  und  $g_1g_2$  die gleiche Nebenklasse.

**Proposition 5.8.6.** *Sei  $H \trianglelefteq G$ . Dann gilt:*

i)  $\Gamma = G/H$  ist eine Gruppe.

ii)

$$\pi = \pi_H^G : G \longrightarrow G/H, \quad g \longmapsto gH$$

ist ein Epimorphismus (genannt kanonische Projektion).

iii)  $\ker(\pi) = H$ .

*Beweis.* klar nach vorausgegangener Konstruktion. □

**Satz 5.8.7** (Universelle Eigenschaft). *Es sei  $H \trianglelefteq G$  eine normale Untergruppe und  $\varphi : G \rightarrow G'$  ein Homomorphismus. Dann sind äquivalent:*

(i)  $\ker(\varphi) \supseteq H$ .

(ii) Es gibt einen Homomorphismus  $\bar{\varphi} : \Gamma = G/H \rightarrow G'$  mit  $\varphi = \bar{\varphi} \circ \pi$ .

$$\begin{array}{ccccc} K \subset & \longrightarrow & G & \xrightarrow{\varphi} & G' \\ \uparrow & & \parallel & & \uparrow \bar{\varphi} \\ H \subset & \longrightarrow & G & \xrightarrow{\pi} & \Gamma \end{array}$$

*Beweis.* (i)  $\Rightarrow$  (ii): Wir definieren  $\bar{\varphi}(gH) := \varphi(g)$ .

$\bar{\varphi}$  ist wohldefiniert, denn aus  $g' = gh$  ( $h \in H$ ) folgt mit (i):

$$\bar{\varphi}(g'H) = \varphi(g') = \varphi(gh) = \varphi(g) \underbrace{\varphi(h)}_{=1} = \varphi(g) = \bar{\varphi}(gH).$$

Offenbar ist  $\varphi = \bar{\varphi} \circ \pi$ .

(i)  $\Leftarrow$  (ii) : Gibt es ein  $\bar{\varphi} : G/H \rightarrow G'$  mit  $\varphi = \bar{\varphi} \circ \pi$ , so folgt sofort für jedes  $h \in H$ :

$$\varphi(h) = \bar{\varphi}(\pi(h)) = \bar{\varphi}(1) = 1,$$

also  $H \leq \ker(\varphi)$ . □

**Satz 5.8.8.** Für jeden Homomorphismus  $\varphi : G \rightarrow \tilde{G}$  gilt:

$$G/\ker(\varphi) \cong \text{im}(\varphi).$$

*Beweis.* Mit Satz 5.8.7 ( $G' = \text{im}(\varphi), H = K = \ker(\varphi), \varphi' = \varphi|_{G'} : G' \rightarrow G'$ ) wissen wir, dass es ein  $\bar{\varphi}$  gibt mit  $\varphi = \bar{\varphi} \circ \pi$ .

$$\begin{array}{ccc} K = \ker(\varphi) \hookrightarrow G & \xrightarrow{\varphi'} & \text{im}(\varphi) = G' \leq G \\ & \downarrow \pi & \nearrow \bar{\varphi} \\ & G/K & \end{array}$$

$\bar{\varphi}$  ist also surjektiv.  $\bar{\varphi}$  ist auch injektiv, denn aus  $\bar{\varphi}(g_1K) = \bar{\varphi}(g_2K)$ , also  $\varphi(g_1) = \varphi(g_2)$ , folgt  $g_2^{-1}g_1 \in K$ , also  $g_1K = g_2K$ . □

**Beispiel 5.8.9.** 1) Die Homomorphismen  $\text{id} : G \rightarrow G$  und  $1 \rightarrow G$  zeigen  $G/G \cong 1$  (triviale Gruppe) und  $G/1 \cong G$ .

2) Wegen

$$\mathfrak{A}_n = \ker(\text{sign}) \hookrightarrow \mathfrak{S}_n \xrightarrow{\text{sign}} \mathbb{S}^0 = \{\pm 1\},$$

ist  $\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{S}^0$ .

3) Sei  $G = \mathbb{Z}/n = \{0, 1, \dots, n-1\}$  eine zyklische Gruppe und  $k \cdot l = n$ . Dann haben wir Isomorphismen

$$H = \{0, k, 2k, \dots, (l-1)k\} \xrightarrow{\cong} \mathbb{Z}/l, \underline{xk} \mapsto \underline{x}, (x = 0, 1, 2, \dots, l-1)$$

und

$$\psi : G/H \xrightarrow{\cong} \mathbb{Z}/k, gH \mapsto \underline{g}, (g = 0, 1, \dots, k-1).$$

4) Ist  $G = G_1 \times G_2$  ein direktes Produkt, so ist  $H = G_1 \times 1 = \ker(\pi_{G_2})$  normal und da die Projektion  $\pi_{G_2} : G \rightarrow G_2$  surjektiv ist, erhalten wir einen Isomorphismus

$$\psi : \begin{array}{ccc} G/H & \xrightarrow{\cong} & G_2 \\ \underbrace{(g_1, g_2)H}_{(1, g_2)H} & \mapsto & g_2. \end{array}$$

5) Wir haben gesehen, dass in der Diedergruppe  $G = D_{2n}$  die Untergruppe  $H = \text{Rot}_n \cong \mathbb{Z}/n$  der Rotationen um Winkel  $\frac{360^\circ}{n} \cdot k, k = 0, 1, \dots, n-1$  normal ist. Wir erhalten einen Isomorphismus

$$G/H \xrightarrow{\cong} \mathbb{S}^0$$

$$gH \mapsto \begin{cases} +1, & \text{falls } g \in \text{Rot}_n \\ -1, & \text{falls } g \notin \text{Rot}_n \text{ (also Spiegelung oder Produkt aus Spiegelung und Rotation)}. \end{cases}$$

6) Für die allgemeine lineare Gruppe  $G = \text{GL}_n(\mathbb{K})$  ist die Untergruppe der Diagonalmatrizen  $H = \text{Zen}(G) = \{D[\lambda, \dots, \lambda] \mid \lambda \neq 0\}$  ein Normalteiler und

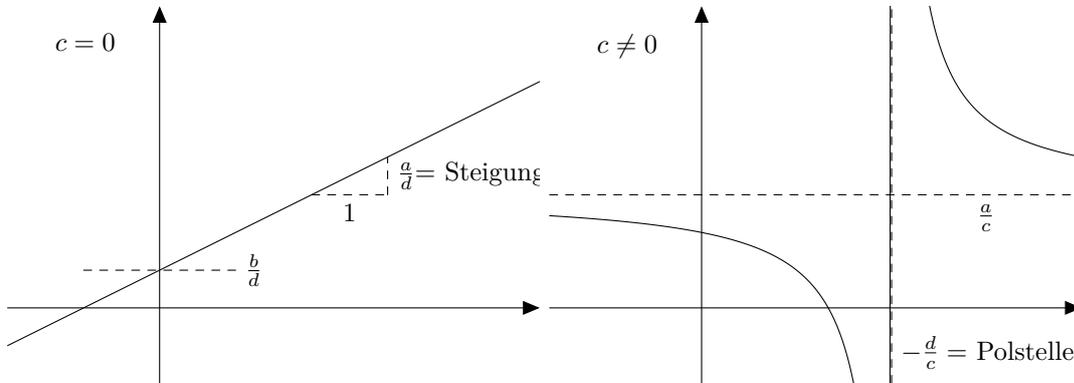
$$\text{PGL}_n(\mathbb{K}) := \text{GL}_n(\mathbb{K})/\text{Zen}(\text{GL}_n(\mathbb{K}))$$

ist die *allgemeine projektive Gruppe*.

7) Möbius-Gruppe

$$\mathfrak{M}(\mathbb{R}) := \left\{ f : \mathbb{R} \cup \infty \rightarrow \mathbb{R} \cup \infty \mid f(x) = \frac{ax + b}{cx + d}, \text{ für } a, b, c, d \in \mathbb{R} \text{ mit } ad - bc \neq 0 \right\}$$

Dabei setzen wir  $f(\infty) := \frac{a}{c}$ , insbesondere  $f(\infty) = \infty$ , falls  $c = 0$  und  $f(-\frac{d}{c}) = \infty$ , falls  $c \neq 0$ .



$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f_M(x) = \frac{ax + b}{cx + d}$$

Es gilt:

$$f_{\mathbb{1}} = \text{id} \\ f_{M_1 \cdot M_2} = f_{M_1} \circ f_{M_2}$$

$$\begin{array}{ccc} \text{Zen}(\text{GL}_2(\mathbb{R})) & \longrightarrow & \text{GL}_2(\mathbb{R}) \xrightarrow{\pi} \mathfrak{M}(\mathbb{R}) \\ \cong \downarrow & & \downarrow \cong \\ \mathbb{R}^\times & & \text{PGL}_2(\mathbb{R}) \end{array}$$

Analoge Betrachtungen können wir für  $\mathfrak{M}(\mathbb{C})$  durchführen.

8) Affine Gruppen

$$G = \text{Aff}(\mathbb{R}) = \{\text{affine Abbildungen } f : \mathbb{R} \rightarrow \mathbb{R}\} = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f(x) = ax + b, a \neq 0\}$$

Diejenigen  $f \in \text{Aff}(\mathbb{R})$  mit  $b = 0$  bilden die Untergruppe der invertierbaren linearen Abbildungen, welche isomorph ist zu  $\text{GL}_1(\mathbb{R}) \cong \mathbb{R}^\times$  (multiplikativ).

Für  $a = 1$  erhalten wir die Untergruppe der Translationen  $\text{Trans}(\mathbb{R}) \cong \mathbb{R}^\times$  (additiv).

Es gibt eine Bijektion

$$\text{Aff}(\mathbb{R}) \longrightarrow \mathbb{R} \times \mathbb{R}^\times, f \longmapsto (b, a),$$

aber diese ist *kein* Isomorphismus von Gruppen, wenn man rechts die Gruppenstruktur des direkte Produkts  $\mathbb{R} \times \mathbb{R}^\times$  nimmt. Stattdessen muss man rechts wie folgt multiplizieren:

$$(b', a') \cdot (b, a) := (a'b + b', a'a).$$

Diese Gruppenstruktur nennt man ein *semidirektes Produkt*.

- $\text{Trans}(\mathbb{R}) \trianglelefteq \text{Aff}(\mathbb{R})$  ist eine normale Untergruppe.
- $\text{GL}_1(\mathbb{R}) \leq$  ist eine nicht-normale Untergruppe.
- $\text{GL}_1(\mathbb{R})$  ist auch eine Quotientengruppe:

$$\text{Trans}(\mathbb{R}) \twoheadrightarrow \text{Aff}(\mathbb{R}) \xrightarrow{\pi} \text{Aff}(\mathbb{R}) / \text{Trans}(\mathbb{R}) \cong \text{GL}_1(\mathbb{R}),$$

$\longleftarrow s$

Dabei ist  $\pi(f) := a$  und  $s(a) := (x \mapsto ax)$  und damit  $\pi \circ s = \text{id}$ .

- Analog:  $\text{Aff}(\mathbb{R}^n)$ .

# Stichwortverzeichnis

- affine Abbildung, 21
- affine Gruppen, 75
- affiner Unterraum, 20
- Allgemeine lineare Gruppe, 55
- alternierende Gruppe, 70
- Austauschsatz von Steinitz, 27
- Automorphismus, 22
  - eines Vektorraums, 55
  - innerer, 70
  
- Basis, 25
- Basisauswahlverfahren, 28
- Basisergänzungssatz, 29
- Basiswechselmatrix, 48
- Bild
  - einer linearen Abbildung, 20
  - eines Gruppenhomomorphismus, 61
  
- Charakteristik
  - eines Körpers, 15
- charakteristische Funktion, 35
  
- Determinantenfunktion, 76
  - normierte, 78
- Diagonalmatrix, 51
- Diedergruppe, 55
- Dimension, 30
- Dimensionssatz, 30
- direkte Summe
  - externe, 65
  - interne, 64, 66
  - von Gruppen, 64
- direktes Produkt von Gruppen, 64
  
- Einheitsmatrix, 40
- Einsmatrix, 42
- Elementarmatrix, 40
- endlich erzeugt, 23
- Endomorphismus, 22
- Epimorphismus, 22
- Erzeugendensystem, 23
  - einer Gruppe, 58
  
- Fehlstand einer Permutation, 60
- Funktorkontravarianter, 39
  - kovarianter, 39
  
- Gauß-Algorithmus, 11
  - voller, 50
- Gaußsche Zahlenebene, 14
  
- Gitter, 58
- Gruppe, 54
  - einfache, 71
  
- homogenes LGS, 10
- Homomorphismus
  - von Körpern, 16
  - von Gruppen, 59
  
- Ikosaedergruppe, 55
- Index, 72
- inhomogenes LGS, 10
- interne direkte Summe, 64
- interne Summe, 23
- invertierbare Matrix, 43
- Isomorphie
  - von Vektorräumen, 35
- Isomorphismus, 22
  
- Körper, 13
- Körperhomomorphismus, 16
- Kern
  - einer linearen Abbildung, 20
  - eines Gruppenhomomorphismus, 61
- Kommutator, 51
- Kommutatoruntergruppe, 58
- komplementäre Untervektorräume, 66
- Kongruenz modulo eines Untervektorraums, 67
- Konjugation
  - komplexe, 21
  - mit einem Gruppenelement, 70
  - einer Matrix, 49
- konjugiert
  - konjugierte Gruppenelemente, 71
  
- linear unabhängig, 24
- lineare Abbildung, 18
- lineare Darstellung, 23
- lineare Hülle, 17
- lineare Relation, 23
- lineares Erzeugnis, 17, 23
- Linearkombination, 23
- Links inverses
  - einer Matrix, 43
- Linksnebenklasse, 72
  
- Möbius-Gruppe, 75
- maximales Element, 27
- Monomorphismus, 22
  
- Normalteiler, 70

- Ordnung
  - einer Gruppe, 57
  - eines Gruppenelements, 57
  - lineare, 26
  - totale, 26
- Ordnungsrelation, 26
- Permutationsmatrix, 52
- Pivotelement, 12
- Polarkoordinaten, 14
- Postkomposition, 45
- Potenzmenge, 26
- Präkomposition, 45
- Produkt
  - direktes, 64
- Produktsatz für Determinanten, 78
- Quotientengruppe, 73
- Quotientenvektorraum, 68
- Rang
  - einer Matrix, 11
- Rechtsinverses
  - einer Matrix, 43
- Rechtsnebenklasse, 72
- Regel von Sarrus, 77
- Repräsentant
  - einer Restklasse, 14
- Repräsentantensystem, 67
- Restklasse, 14
- Scherungsinvarianz, 76
- Schnitt, 67
- semidirektes Produkt, 75
- Signum einer Permutation, 60
- Skalarprodukt, 7
- Spaltenmultiplikatitivität, 76
- Spann, 17, 23
- Sprungstelle
  - einer Treppenfunktion, 11
- Streckungsmatrix, 51
- symmetrische Gruppe, 55
- Translation, 21
- transponierte Matrix, 43
- Transposition, 52, 55
- Treppenfunktion, 11
- universelle Eigenschaft
  - der direkten Summe, 66
  - des direkten Produkts, 64
  - direkte Summe, 66
  - des Quotienten, 68
  - Produkt, 65
  - Quotientengruppe, 73
- Untergruppe, 56
  - erzeugte, 58
  - normale, 70
- Unterkörper, 13
- Unterraum, 17
- Vektorraum, 16
- Verband, 26
- Zeilenstufenform, 11
- zentrale Matrix, 59
- Zentrum
  - einer Gruppe, 58
- Zorn'sches Lemma, 27
- Zykel, 55
- Zykeltyp, 56