Lineare Algebra und Analytische Geometrie

Manuel Kauers
nach einer Vorlesung von
Prof. Dr. W. Weil

21. Oktober 2000

Inhaltsverzeichnis

1 Mengen, Abbildungen, Relationen

Der Begriff der Menge wird hier naiv abgeleitet und nicht axiomatisch eingeführt.

Def. 1 Eine „Zusammenfassung von Objekten" heißt *Menge*. Für jedes Objekt muß feststehen, ob es zur Menge M gehört ($o \in M$) oder nicht ($o \notin M$). Zwei Mengen A, B heißen *gleich*, falls gilt:

$$\forall \quad a: \qquad a \in A \quad \Longleftrightarrow \quad a \in B$$

Die Objekte in der Menge heißen *Elemente* der Menge.

Bem. Eine Menge, deren Elemente Mengen sind, heißt *Mengensystem*

Axiom 1 Für jede Menge M gelte: $M \notin M$.

Def. 2

1. $\emptyset := \{\}$ heißt *leere* Menge.
2. Sei A eine Menge. $|A|$ bezeichnet die Anzahl der Elemente von A. Ist A nicht endlich, so schreiben wir $|A| = \infty$.
3. Sei A eine Menge. Eine Menge B heißt *Teilmenge* von A, falls gilt:

   $$\forall \quad a \in B: \qquad a \in A.$$

   Schreibweise in diesem Fall: $B \subseteq A$.

Bem.

- Für jede Menge A gilt $A \subseteq A$ und $\emptyset \subseteq A$.
- Für zwei Mengen A, B gilt:

$$A = B \qquad \Longleftrightarrow \qquad A \subseteq B \quad \wedge \quad B \subseteq A$$

- Statt $A \subseteq B$ schreibt man auch $B \supseteq A$.

Bsp.

- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- $\{1,5,7\} \subseteq \{1,5,6,7\}$

Def. 3 Sei M eine Menge. Die Menge

$$\mathcal{P}(M) := \{A : A \subseteq M\}$$

heißt *Potenzmenge* von M.

Bsp. Sei $M = \{1,2,3\}$. Dann ist

$$\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, M\}$$

Def. 4 Seien A, B Mengen. Dann heißt

$$A \cup B := \{x : x \in A \ \vee \ x \in B\}$$

die *Vereinigung* von A und B,

$$A \cap B := \{x : x \in A \ \wedge \ x \in B\}$$

der *Schnitt* von A und B,

$$A \setminus B := \{x \in A : x \notin B\}$$

die *Differenz* von A und B und

$$A \Delta B := (A \setminus B) \cup (B \setminus A)$$

die *symmetrische Differenz* von A und B.

Satz 1 Es seien A, B, C Mengen. Dann gilt:

1. $(A \cup B) \cup C = A \cup (B \cup C)$,
   $(A \cap B) \cap C = A \cap (B \cap C)$
2. $A \cup B = B \cup A$,
   $A \cap B = B \cap A$
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$,
   $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$

Def. 5 Sei $\emptyset \neq \mathcal{M}$ ein Mengensystem. Dann heißt

$$\bigcup_{M \in \mathcal{M}} M := \{x : \exists\ M \in \mathcal{M} :\ x \in M\}$$

die *Vereinigung* aller M aus $\mathcal{M}$ und

$$\bigcap_{M \in \mathcal{M}} M := \{x : \forall\ M \in \mathcal{M} :\ x \in M\}$$

der *Schnitt* aller M aus $\mathcal{M}$.

Satz 2 Sei $\emptyset \neq \mathcal{M}$ ein Mengensystem, A eine Menge. Dann gilt:

$$A \cup \Big(\bigcup_{B \in \mathcal{M}} B \Big) = \bigcup_{B \in \mathcal{M}} (A \cup B), \qquad A \cap \Big(\bigcap_{B \in \mathcal{M}} B \Big) = \bigcap_{B \in \mathcal{M}} (A \cap B)$$

$$A \cup \Big(\bigcap_{B \in \mathcal{M}} B \Big) = \bigcap_{B \in \mathcal{M}} (A \cup B), \qquad A \cap \Big(\bigcup_{B \in \mathcal{M}} B \Big) = \bigcup_{B \in \mathcal{M}} (A \cap B)$$

$$A \setminus \Big(\bigcap_{B \in \mathcal{M}} B \Big) = \bigcap_{B \in \mathcal{M}} (A \setminus B), \qquad A \setminus \Big(\bigcup_{B \in \mathcal{M}} B \Big) = \bigcup_{B \in \mathcal{M}} (A \setminus B)$$

Bem. Für $|\mathcal{M}| = 2$ ergibt sich hieraus Satz 1 als Spezialfall.

Def. 6 Es seien $A_1, \ldots, A_n$ Mengen. Dann heißt die Menge

$$A_1 \times \cdots \times A_n := \{(x_1, \ldots, x_n) : x_i \in A_i \ (i = 1, \ldots, n)\}$$

das *karthesische Produkt* von $A_1, \ldots, A_n$. Gilt $A_1 = \cdots = A_n$, so schreibt man für diese Menge auch A_1^n.

Def. 7 Seien A, B Mengen und $M \subseteq A \times B$ mit

1. $\forall\, x \in A \ \forall\, y_1, y_2 \in B : \quad ((x, y_1) \in M \ \wedge \ (x, y_2) \in M) \implies y_1 = y_2$
2. $\forall \quad x \in A \quad \exists \quad y \in B : \qquad (x, y) \in M$

Dann definiert M eine *Abbildung* (oder *Funktion* oder *Transformation* oder einen *Operator*) von A nach B, Schreibweise: $f : A \to B$. M heißt *Graph* von f .

Def. 8 Sei $f : A \to B$ eine Abbildung mit Graph M.

1. A heißt *Definitionsbereich* von f, B heißt *Wertebereich* von f.
2. Für $C \subseteq A$ heißt
   $$f(C) := \{y \in B : \ \exists\, x \in C : \ (x, y) \in M\}$$
   das *Bild* von C unter f.
3. Für $C \subseteq B$ heißt
   $$f^{-1}(C) := \{x \in A : \ \exists\, y \in C : (x, y) \in M\}$$
   das *Urbild* von C unter f.

Bem.

- Man schreibt $f(x)$ für das (einzige) Element der Menge $f(\{x\})$.
- Stets gilt $f(A) \subseteq B$.
- Ein $y \in f(A)$ kann mehrere Urbilder $x \in A$ haben. Umgekehrt existiert jedoch zu jedem $x \in A$ genau ein $y \in f(A)$ mit $f(x) = y$.

Def. 9 Sei $f : A \to B$ eine Abbildung.

1. f heißt *surjektiv* $:\Longleftrightarrow f(A) = B$.
2. f heißt *injektiv* $:\Longleftrightarrow \forall \quad x \in A: \qquad |f^{-1}(x)| = 1$
3. f heißt *bijektiv* $:\Longleftrightarrow f$ ist surjektiv und injektiv.

Bsp. Seien $f: \mathbb{R} \to \mathbb{R}$, $g: \mathbb{R} \to \mathbb{R}$ und $h: \mathbb{N} \to \mathbb{Z}$ definiert durch

$$\begin{aligned} f(x) &= (x-1)^2, \\ g(x) &= x(x-1)(x+1), \\ h(x) &= \begin{cases} \frac{x-1}{2} & \text{falls } x \text{ gerade} \\ -\frac{x}{2} & \text{falls } x \text{ ungerade} \end{cases} \end{aligned}$$

Dann gilt: f ist weder injektiv noch surjektiv, g ist surjektiv, aber nicht injektiv und h ist bijektiv.

Def. 10

1. Sei A eine Menge. Dann heißt

   $$\mathrm{id}_A : A \to A, \qquad \mathrm{id}_A(x) := x \quad (x \in A)$$

   die *Identität* auf A.
2. Sei $f: A \to B$ und $C \subseteq A$. Dann heißt

   $$f|_C : C \to B, \qquad f|_C(x) := f(x) \quad (x \in C)$$

   Einschränkung (oder *Restriktion*) von f auf C.
3. Sei $f: A \to B$ bijektiv. Dann heißt

   $$f^{-1} : B \to A, \qquad f^{-1}(x) = y \quad (x = f(y))$$

   die *Umkehrabbildung* von f.
4. Seien $f: A \to B$ und $g: B \to C$ Abbildungen. Dann heißt

   $$g \circ f : A \to C, \qquad (g \circ f)(x) := g(f(x)) \quad (x \in A)$$

   die *Komposition* (oder *Verkettung*) von f und g.

Satz 3 Sei $f: A \to B$ eine Abbildung. Dann gilt:

1. f ist injektiv $\Longleftrightarrow \exists \quad g: B \to A: \qquad g \circ f = \mathrm{id}_A$
2. f ist surjektiv $\Longleftrightarrow \exists \quad g: B \to A: \qquad f \circ g = \mathrm{id}_B$

Def. 11 Sei A eine Menge. Eine Abbildung

$$R : A \times A \to \{\text{„wahr“}, \text{„falsch“}\}$$

heißt *Relation*. Gilt für $x, y \in A$ $R(x,y) =$ „wahr“, so schreibt man xRy.

Bsp. Auf $\mathbb{R}$ sind $\geq, >, =$ Relationen. Auf $\mathbb{N}$ ist die Teilerbeziehung eine Relation (vgl. Seite 15).

Def. 12 Eine Relation $\leq$ auf einer Menge A heißt *Ordnungsrelation,* falls gilt:

1. $\forall \quad x \in A: \qquad x \leq x$
2. $\forall \quad x, y \in A: \qquad x \leq y \ \wedge \ y \leq x \quad \Longrightarrow \quad x = y$
3. $\forall \quad x, y, z \in A: \qquad x \leq y \ \wedge \ y \leq z \quad \Longrightarrow \quad x \leq z$

In diesem Fall heißt $(A, \leq)$ *geordnete* Menge. Gilt außerdem

$$\forall \quad x, y \in A: \qquad x \leq y \quad \vee \quad y \leq x$$

so heißt $\leq$ *Totalordnung* und $(A, \leq)$ heißt *total geordnete Menge.*

Bsp.

- $(\mathbb{R}, \leq)$ ist eine Totalordung.
- Für eine Menge A ist $(\mathcal{P}(A), \subseteq)$ eine Totalordnung.

Def. 13 Eine Relation $\sim$ auf einer Menge A heißt *Äquivalenzrelation,* falls gilt:

1. $\forall \quad x \in A: \qquad x \sim x$
2. $\forall \quad x, y \in A: \qquad (x \sim y \quad \Longrightarrow \quad y \sim x)$
3. $\forall \quad x, y, z \in A: \qquad (x \sim y \ \wedge \ y \sim z \quad \Longrightarrow \quad x \sim z)$

In diesem Fall heißt für $x \in A$

$$[x]_\sim := \{y \in A : \ x \sim y\}$$

Äquivalenzklasse von x. x heißt *Repräsentat* von $[x]_\sim$.

$$A/_\sim := \bigcup_{x \in A} [x]_\sim$$

heißt *Faktormenge* (oder *Quotientenmenge*). Ein Mengensystem $\mathcal{M} = A/_\sim$ heißt *Partition* (oder *Klasseneinteilung*) von A.

Bsp.

- $=$ ist eine Äquivalenzrelation.
- Sei $k \in \mathbb{N}$ fest. Dann wird durch

  $$x \sim y \qquad :\Longleftrightarrow \qquad |x - y| \text{ teilbar durch } k$$

  für $x, y \in \mathbb{Z}$ eine Äquivalenzrelation erklärt.

Satz 4 Sei $\sim$ eine Äquivalenzrelation auf A und $x, y \in A$. Dann gilt:

1. $[x]_\sim \neq \emptyset$
2. $[x]_\sim \neq [y]_\sim \quad \Longleftrightarrow \quad [x]_\sim \cap [y]_\sim = \emptyset$
3. $\bigcup_{x \in A} [x]_\sim = A$

4. Ist $\mathcal{M} \neq \emptyset$ ein Mengensystem paarweiser disjunkter Mengen mit

$$\bigcup_{M \in \mathcal{M}} M = A$$

Dann gibt es eine Äquivalenzrelation $\sim$ auf A mit $\mathcal{M} = {}^{A}\!/_{\sim}$

Satz 5 Sei $f : A \to B$ eine Abbildung. Dann wird durch

$$x \sim y \quad :\Longleftrightarrow \quad f(x) = f(y)$$

eine Äquivalenzrelation auf A erklärt. Statt ${}^{A}\!/_{\sim}$ schreibt man hierfür ${}^{A}\!/_{f}$

2 Gruppen

Def. 14 Eine Abbildung $\circ : A \times A \to A$ heißt *Verknüpfung*. Statt $\circ(x, y)$ schreibt man $x \circ y$. Eine Verknüpfung $\circ$ heißt *assoziativ* $:\Longleftrightarrow$

$$\forall \quad x, y, z \in A : \qquad (x \circ y) \circ z = x \circ (y \circ z).$$

Sie heißt *kommutativ* $:\Longleftrightarrow$

$$\forall \quad x, y \in A : \qquad x \circ y = y \circ x.$$

Def. 15 Ist $A \neq \emptyset$ und $\circ$ eine assoziative Verknüpfung auf A. Dann heißt $(A, \circ)$ *Halbgruppe*. Ist $\circ$ zusätzlich kommutativ, so heißt $(A, \circ)$ *kommutative* Halbgruppe (oder ABEL*sche Halbgruppe*).

Bem.

- Statt $(A, \circ)$ bezeichnet man oft einfacher A als Halbgruppe. Dies setzt voraus, daß klar ist, um welche Verknüpfung es sich handelt.
- Ist $(A, \circ)$ eine Halbgruppe, so schreibt man für $x, y, z \in A$ auch $x \circ y \circ z$ statt $(x \circ y) \circ z$. Außerdem sei für $k \in \mathbb{N}$ definiert

$$x^k := \underbrace{x \circ x \circ \cdots \circ x}_{k \text{ mal}}$$

Bsp.

- $(\mathbb{R}, +)$ und $(\mathbb{R}, \cdot)$ sind Halbgruppen.
- Für $A \neq \emptyset$ sind $(\mathcal{P}(A), \cup)$, $(\mathcal{P}(A), \cap)$ und $(\mathcal{P}(A), \Delta)$ Halbgruppen

Def. 16 Sei A eine Menge und $\circ$ eine Verknüpfung auf A. $(A, \circ)$ heißt *Gruppe*, falls gilt:

1. $(A, \circ)$ ist Halbgruppe
2. $\exists \quad e \in A \quad \forall \quad x \in A : \qquad x \circ e = e \circ x = x$
3. $\forall \quad x \in A \quad \exists \quad x^{-1} \in A : \qquad x^{-1} \circ x = x \circ x^{-1} = e$

Eine Gruppe $(A, \circ)$ heißt ABEL*sch*, falls gilt: $(A, \circ)$ ist ABELsche Halbgruppe.

Das Element e aus (2) heißt *Neutralelement* auf A bezüglich $\circ$ und das Element x^{-1} in (3) heißt *Inverses* von x bezüglich $\circ$.

Bem.

- In ABELschen Gruppen wählt man oft $+$ („plus") als Verknüpfungssymbol. Statt e schreibt man dann 0 („Null") , statt x^{-1} schreibt man $-x$ („minus x") und statt $x + (-y)$ schreibt man $x - y$.
- Statt $(A, \circ)$ bezeichnet man oft einfacher A als Gruppe. Dies setzt voraus, daß klar ist, um welche Verknüpfung es sich handelt.

Bsp. $(\mathbb{R}, +)$ ist eine ABELsche Gruppe. Für $A \neq \emptyset$ ist $(\mathcal{P}(A), \Delta)$ eine ABELsche Gruppe. Im letzten Fall ist $\emptyset$ das Neutralelement und zu $B \in \mathcal{P}(A)$ ist $B^{-1} = B$ das Inverse.

Satz 6 Sei $(A, \circ)$ eine Halbgruppe. Dann gilt:

$$(A, \circ) \text{ ist Gruppe} \quad \Longleftrightarrow \quad \forall\, x, y \in A\ \exists\, z, \tilde{z} \in A: \quad x \circ z = y \ \wedge\ \tilde{z} \circ x = y$$

Ist $(A, \circ)$ Gruppe, so sind $z, \tilde{z}$ eindeutig bestimmt.

Bsp. Sei $A = \{0, 1\}$. Auf A sei eine Verknüpfung $+$ definiert durch

$+$	0	1
0	0	0
1	0	1

Dann ist $(A, +)$ eine Gruppe.

Def. 17 Seien $(A, \circ)$ und $(B, *)$ Gruppen. Weiter sei $B \subseteq A$ und es gelte

$$\forall \quad x, y \in B: \qquad x * y = x \circ y.$$

Dann heißt $(B, *)$ *Untergruppe* von $(A, \circ)$.

Satz 7 (Untergruppenkriterium) Es sei $(A, \circ)$ eine Gruppe und $B \subseteq A$. e sei das Neutralelement von $(A, \circ)$. Es gilt: $(B, \circ)$ ist Untergruppe von $(A, \circ)$ $\Longleftrightarrow$

$$e \in B \qquad \wedge \qquad \forall \quad x, y \in B: \qquad x^{-1} \in B \quad \wedge \quad x \circ y \in B$$

Bem. Andere Darstellung von Satz 7: $(B, \circ)$ ist Untergruppe von $(A, \circ)$ $\Longleftrightarrow$

$$B \neq \emptyset \qquad \wedge \qquad \forall \quad x, y \in B: \qquad x \circ y^{-1} \in B.$$

Bsp. $(\mathbb{Q}, +)$ ist Untergruppe von $(\mathbb{R}, +)$, denn es gilt $\mathbb{Q} \subseteq \mathbb{R}$ und es gilt $\mathbb{Q} \neq \emptyset$ und

$$\forall \quad x, y \in \mathbb{Q} : x - y \in \mathbb{Q}.$$

Def. 18 Es seien $(A, \circ)$ und $(\tilde{A}, *)$ Gruppen. $f : A \to \tilde{A}$ heißt (*Gruppen-*) *Homomorphismus* $:\Longleftrightarrow$

$$\forall \quad x, y \in A : \qquad f(x \circ y) = f(x) * f(y)$$

Ist f zusätzlich bijektiv, so heißt f (*Gruppen-*) *Isomorphismus* In diesem Fall heißen $(A, \circ)$ und $(\tilde{A}, *)$ zueinander *isomorph*, Schreibweise:

$$(A, \circ) \cong (\tilde{A}, *).$$

Ist f ein Isomorphismus und $(\tilde{A}, *) = (A, \circ)$, so heißt f (*Gruppen-*) *Automorphismus*

Satz 8 Es seien $(A, \circ)$ und $(\tilde{A}, *)$ Gruppen. $f : A \to \tilde{A}$ sei ein Homomorphismus. e sei das Neutralelement in A und $\tilde{e}$ das Neutralelement in $\tilde{A}$. Es gilt:

1. $f(e) = \tilde{e}, \forall \quad x \in A : \qquad (f(x))^{-1} = f(x^{-1})$
2. $(f(A), *)$ ist Untergruppe von $(\tilde{A}, *)$,

   $$\text{Kern}\, f := \{x \in A : \ f(x) = \tilde{e}\}$$

   ist Untergruppe von A.
3. $$\begin{array}{ccc} f \text{ ist surjektiv} & \Longleftrightarrow & f(A) = \tilde{A} \\ f \text{ ist injektiv} & \Longleftrightarrow & \text{Kern}\, f = \{e\} \end{array}$$

Def. 19 Es sei $(A, \circ)$ eine Gruppe und $(B, \circ)$ eine Untergruppe von $(A, \circ)$. $(B, \circ)$ heißt *Normalteiler* von $(A, \circ)$ $:\Longleftrightarrow$

$$\forall \quad x \in A \quad \forall \quad y \in B : \qquad x \circ y \circ x^{-1} \in B$$

Bsp.

- A und $\{e\}$ sind Normalteiler von A.
- Ist $f : A \to B$ ein Homomorphismus, so ist Kern f Normalteiler von A.
- Von einer ABELschen Gruppe ist jede Untergruppe Normalteiler.

Satz 9 Sei $(A, \circ)$ eine Gruppe und $(B, \circ)$ eine Untergruppe von A. Dann sind folgende Aussagen äquivalent:

1. B ist Normalteiler von A.
2. $\forall \quad x \in A : \qquad B = \{x \circ b \circ x^{-1}, b \in B\}$
3. $\forall \quad x \in A : \qquad \{x \circ b, b \in B\} = \{b \circ x, b \in B\}$
4. $\forall \quad x, \tilde{x}, y, \tilde{y} \in A : \qquad x \circ \tilde{x}^{-1} \in B \ \wedge \ y \circ \tilde{y}^{-1} \in B \implies x \circ y \circ \tilde{y}^{-1} \circ \tilde{x} \in B$

Satz 10 Sei $(A, \circ)$ eine Gruppe und $(B, \circ)$ eine Untergruppe von $(A, \circ)$. Für $x, y \in A$ wird durch

$$x \sim y \quad :\Longleftrightarrow \quad x \circ y^{-1} \in B$$

eine Äquivalenzrelation definiert. Auf ${}^{A}\!/_{B} := {}^{A}\!/_{\sim}$ wird durch

$$[x]_\sim \cdot [y]_\sim := [x \circ y]_\sim \qquad (x, y \in A)$$

eine Verknüpfung $\cdot$ definiert. $({}^{A}\!/_{B}, \cdot)$ ist eine Gruppe.

Bem.

- Damit durch $\cdot$ eine Verknüpfung definiert ist, muß die Definition repräsentantenunabhängig sein. Dies ist genau dann der Fall, wenn $(B, \circ)$ Normalteiler von $(A, \circ)$ ist.
- $({}^{A}\!/_{B}, \cdot)$ heißt *Faktorgruppe* (oder *Quotientengruppe*)

Satz 11 (Homomorphiesatz für Gruppen) Seien $(A, \circ)$ und $(\tilde{A}, *)$ Gruppen und $f : A \to \tilde{A}$ ein Homomorphismus. Dann gilt:

1. Die *kanonische Abbildung*

   $$k : A \to {}^{A}\!/_{\text{Kern } f}, \qquad k(x) = [x]_\sim$$

   ist ein Homomorphismus
2. Es gibt einen injektiven Homomorphismus

   $$\tilde{f} : {}^{A}\!/_{\text{Kern } f} \to \tilde{A}$$

   mit $f = \tilde{f} \circ k$.
3. Ist f surjektiv, so gilt

   $$({}^{A}\!/_{\text{Kern } f}, \cdot) \cong (\tilde{A}, *)$$

Bem. Insbesondere gilt stets ${}^{A}\!/_{\text{Kern } f} \cong f(A)$

3 Symmetrische Gruppen

Es sei $B \neq \emptyset$ eine Menge und

$$S_B := \{f : B \to B : f \text{ bijektiv}\} \subseteq B^B$$

$(S_B, \circ)$ ist eine Gruppe. Das Neutralelement ist id_B und zu $f \in S_B$ ist f^{-1} das Inverse. Die Gruppe $(S_B, \circ)$ heißt *symmetrische Gruppe* von B. Im Folgenden sei $B = \{1, \ldots, m\}$. Statt S_B schreiben wir S_m. Die Elemente von S_m heißen *Permutationen*, Schreibweise:

$$\pi = \begin{pmatrix} 1 & \cdots & m \\ \pi(1) & \cdots & \pi(m) \end{pmatrix}$$

Satz 12 Es gilt $|S_m| = m!$.

Bsp. Betrachte $S_3 = \{\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6\}$ mit

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Wegen

$$\pi_2 \circ \pi_4 = \pi_6 \neq \pi_5 = \pi_4 \circ \pi_2$$

ist S_3 keine ABELsche Gruppe.

Def. 20 Seien $i < j \leq m$. Eine Permutation $\tau^{(i,j)} \in S_m$ der Form

$$\tau^{(i,j)} = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & m \\ 1 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & m \end{pmatrix}$$

heißt *Transposition* (oder *Vertauschung*)

Satz 13 Jede Permutation $\pi \in S_m$ läßt sich als Verkettung endlich vieler Transpositionen darstellen.

Bsp. Sei $\pi \in S_6$ definiert durch

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 4 & 1 \end{pmatrix}.$$

Dann gilt:

$$\pi = \tau^{(1,6)} \circ \tau^{(4,5)} \circ \tau^{(1,4)} \circ \tau^{(2,3)}$$

Ebeso gilt:

$$\pi = \tau^{(1,4)} \circ \tau^{(4,6)} \circ \tau^{(2,3)} \circ \tau^{(1,5)}$$

Damit gilt: Die Darstellung einer Permutation als Verkettung von Transpositionen ist nicht eindeutig.

Def. 21 Sei $\pi \in S_m$. Jedes Paar $(i,j) \in \{1, \dots, m\}^2$ mit $i < j$ und $\pi(i) > \pi(j)$ heißt *Fehlstand* von π. $F(\pi)$ sei die Anzahl der Fehlstände einer Permutation. $F(\pi)$ heißt *Fehlstandszahl*

Bsp. Sei $\pi \in S_4$ definiert durch

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

π hat die Fehlstände $(1,2), (1,3), (1,4)$ und $(2,3)$. Damit ist $F(\pi) = 4$.

Satz 14 Seien $\pi, \sigma \in S_m$. Dann gilt:

1. $\prod_{1 \leq i < j \leq m} \dfrac{\pi(j) - \pi(i)}{j - i} = (-1)^{F(\pi)}$

2. $(-1)^{F(\pi \circ \sigma)} = (-1)^{F(\sigma)} \cdot (-1)^{F(\pi)}$

3. $(-1)^{F(\pi)} = (-1)^{F(\pi^{-1})}$

4. $F(\tau^{(i,j)}) = 2(j-i) - 1$

Def. 22 $\pi \in S_m$ heißt gerade, wenn es eine Darstellung von π als Verkettung einer geraden Anzahl von Permutationen ist

Bem. Die Verkettung zweier gerader Permutationen ist wieder gerade. Wegen $(\tau^{(i,j)})^{-1} = \tau^{(i,j)}$ ist auch die Inverse einer geraden Permutation wieder gerade. Damit gilt: Die Menge aller geraden Permutationen ist eine Untergruppe von S_m.

4 Körper und Ringe

Def. 23 Seien A eine Menge und $+, \cdot$ Verknüpfungen auf A. A heißt *Körper*, falls gilt:

1. $(A, +)$ ist eine ABELsche Gruppe. Ihr Neutralelement heißt *Null* (0).

2. $(A \setminus \{0\}, \cdot)$ ist eine ABELsche Gruppe. Ihr Neutralelement heißt *Eins* (1).

3. $\forall \quad x, y, z \in A: \qquad x \cdot (y + z) = x \cdot y + x \cdot z$

Bem.

- Die Verknüpfung $+$ („plus“) bezeichnet man als *Addition*. Hier schreibt man $-x$ für das Inverse und $y - x$ statt $y + (-x)$. Die Verknüpfung $\cdot$ („mal“) bezeichnet man als *Multiplikation*. Hier schreibt man $\frac{1}{x}$ für das Inverse und $\frac{y}{x}$ statt $y \cdot \frac{1}{x}$. Ferner schreibt man xy statt $x \cdot y$.

- Jeder Körper besitzt mindestens zwei Elemente (0 und 1).

- Ist A ein Körper, so gilt:

$$\forall \quad x \in A: \qquad x \cdot 0 = 0 \cdot x = 0$$

Bsp.

- $\mathbb{Q}$ und $\mathbb{R}$ sind Körper

- $A := \{x + \sqrt{2}y, x, y \in \mathbb{Q}\}$ ist bezüglich reeller Addition und Multiplikation ein Körper.

- Sei $A := \{0, 1\}$ und die Verknüpfungen $+$ und $\cdot$ definiert durch

$+$	0	1
0	0	1
1	1	0

,

$\cdot$	0	1
0	0	0
1	0	1

Dann ist $(A, +, \cdot)$ ein Körper.

Def. 24 Es seien $(A, +, \cdot)$ und $(\tilde{A}, \circ, *)$ Körper und $f : A \to \tilde{A}$ eine Abbildung. Es gelte

1. $f(x + y) = f(x) \circ f(y) \qquad (x, y \in A)$
2. $f(x \cdot y) = f(x) * f(y) \qquad (x, y \in A \setminus \{0\})$

Dann heißt f *(Körper-)Homomorphismus.* Ist f zusätzlich bijektiv, so heißt f *(Körper-)Isomorphismus.* Ist f Isomorphismus von $(A, +, \cdot)$ nach $(\tilde{A}, \circ, *)$ so heißen $(A, +, \cdot)$ und $(\tilde{A}, \circ, *)$ zueinander *isomorph.* Schreibweise in diesem Fall:

$$(A, +, \cdot) \cong (\tilde{A}, \circ, *).$$

Gilt zusätzlich $(A, +, \cdot) = (\tilde{A}, \circ, *)$, so heißt f *(Körper-)Automorphismus.*

Bem.

- Alle Körper mit q Elementen ($q \in \mathbb{N}$) sind zueinander isomorph. Für diese Körper verwendet man das Symbol $\mathbb{F}_q$.
- Wir verwenden das Symbol $\mathbb{K}$ im Folgenden für einen allgemeinen Körper.

Bsp. (Komplexe Zahlen) Wir betrachten die Menge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ und die darauf definierten Verknüpfungen $+$ und $\cdot$ mit

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} := \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \end{pmatrix},$$

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} := \begin{pmatrix} a_1 b_1 - a_2 b_2 \\ a_1 b_2 + a_2 b_1 \end{pmatrix}$$

$(\mathbb{R}^2, +, \cdot)$ ist ein Körper. Das Neutralelement in $(\mathbb{R}^2, +)$ ist $(0, 0)$, das Neutralelement in $(\mathbb{R}^2 \setminus \{(0, 0)\}, \cdot)$ ist $(1, 0)$.

In der Darstellung (x, y) heißt x *Realteil* und y *Imaginärteil.* Statt (x, y) schreibt man auch $x + \mathrm{i}y$. Mit dieser Darstellung läßt sich in $(\mathbb{R}^2, +, \cdot)$ rechnen wie in $\mathbb{R}$ unter Berücksichtigung von

$$\mathrm{i}^2 = -1$$

Wir bezeichnen $(\mathbb{R}^2, +, \cdot)$ als Körper der *komplexen Zahlen* und verwenden dafür das Symbol $\mathbb{C}$.

Def. 25 Sei A eine Menge und $+$ und $\cdot$ Verknüpfungen auf A. $(A, +, \cdot)$ heißt *Ring* $:\Longleftrightarrow$

1. $(A, +)$ ist ABELsche Gruppe
2. $(A, \cdot)$ ist Halbgruppe
3. $\forall \; x, y, z \in A: \quad x \cdot (y + z) = x \cdot y + x \cdot z$
   $\forall \; x, y, z \in A: \quad (x + y) \cdot z = x \cdot z + y \cdot z$

Ist $(A, \cdot)$ zusätzlich kommutativ, so heißt $(A, +, \cdot)$ *kommutativer* Ring. Hat $(A, \cdot)$ ein Neutralelement, so heißt $(A, +, \cdot)$ Ring *mit Eins*.

Bsp.

- Jeder Körper ist ein kommutativer Ring mit Eins.
- $\mathbb{Z}$ ist ein kommutativer Ring mit Eins.
- Ist $A \neq \emptyset$, so ist $(\mathcal{P}(A), \Delta, \cap)$ ein kommutativer Ring mit Eins.

5 Restklassenkörper

In diesem Paragraphen betrachten wir Körper und Ringe mit endlich vielen Elementen. Es sei $m \in \mathbb{N}$. Für $x, y \in \mathbb{Z}$ sei die Äquivalenzrelation $\sim$ definiert durch:

$$x \sim y \qquad :\Longleftrightarrow \qquad \frac{x-y}{m} \in \mathbb{Z}$$

Def. 26 Die Äquivalenzklassen bezüglich der oben definierten Äquivalenzrelation $\sim$ heißen *Restklassen*. Statt $\mathbb{Z}/_{\sim}$ schreibt man $\mathbb{Z}_m$.

Bem. Es gilt

$$\mathbb{Z}_m = \{[0]_\sim, \ldots, [m-1]_\sim\}$$

Satz 15 Auf $\mathbb{Z}_m$ werden für $x, y \in \mathbb{Z}$ durch

$$[x]_\sim + [y]_\sim := [x+y]_\sim$$

und

$$[x]_\sim \cdot [y]_\sim := [x \cdot y]_\sim$$

Verknüpfungen definiert. Es gilt: $(\mathbb{Z}_m, +)$ ist eine ABELsche Gruppe mit Neutralelement $[0]_\sim$, $(\mathbb{Z}_m, \cdot)$ ist eine kommutative Halbgruppe mit Neutralelement $[1]_\sim$. $(\mathbb{Z}_m, +, \cdot)$ ist ein kommutativer Ring mit Eins.

Bem. Die Definition der Verknüpfung ist repräsentatenunabhängig.

Bsp.

- $\mathbb{Z}_2 = \{[0]_\sim, [1]_\sim\}$ mit

$$[0]_\sim = \{2z, z \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

$$[1]_\sim = \{1+2z, z \in \mathbb{Z}\} = \{\ldots, -3, -1, 1, 3, \ldots\}$$

- In $\mathbb{Z}_{15}$ gilt $[137]_\sim = [2]_\sim$, denn wegen

$$135 = 9 \cdot 15 + 2$$

ist $137 \sim 2$

Satz 16 Es gilt:

$$\forall \quad m \in \mathbb{N}: \qquad (\mathbb{Z}_m, +, \cdot) \text{ ist Körper} \qquad \Longleftrightarrow \qquad m \text{ ist Primzahl}$$

Bem. Statt $x \sim y$ schreibt man auch

$$x \equiv y \bmod m \qquad \text{oder} \qquad x =_m y$$

Sprechweise: „x ist *kongruent* y *modulo* m“.

Satz 17 Seien $a, b \in \mathbb{Z}$, $b \neq 0$. Dann gilt

$$\exists \quad k \in \mathbb{Z}, \quad r \in \{0, \ldots, |b| - 1\}: \qquad a = kb + r.$$

k und r sind eindeutig bestimmt. Ist $r = 0$, so heißt b *Teiler* von a, Schreibweise $b \mid a$. Ist

$$A := \{d \in \mathbb{N} : d \mid a\} \qquad \text{und} \qquad B := \{d \in \mathbb{N} : d \mid b\},$$

dann heißt

$$\mathrm{ggT}(a, b) := \max(A \cap B)$$

der *größte gemeinsame Teiler* von a und b. Ist $\mathrm{ggT}(a, b) = 1$, so heißen a und b *teilerfremd*

Satz 18 (EUKLIDischer Algorithmus) Seien $a, b \in \mathbb{Z}$, $b \neq 0$. Die Iteration

$$r_{j-2} := k_j \cdot r_{j-1} + r_j$$

mit $r_2 = a, r_1 = b$ und k_j, r_j die eindeutig bestimmten Zahlen aus obigem Satz, terminiert und liefert $\mathrm{ggT}(a, b)$.

Bsp. gesucht: $\mathrm{ggT}(24, 614)$ EUKLIDischer Algorithmus:

$$\begin{aligned} 614 &= 25 \cdot 24 + 14 \\ 24 &= 1 \cdot 14 + 10 \\ 14 &= 1 \cdot 10 + 4 \\ 10 &= 2 \cdot 4 + 4 \\ 4 &= 2 \cdot 2 \end{aligned}$$

Damit gilt $\mathrm{ggT}(24, 614) = 2$

Satz 19 Seien $a, b \in \mathbb{Z}$. Dann gilt: a, b teilerfremd $\Longleftrightarrow$

$$\exists \quad x, y \in \mathbb{Z}: \qquad ax + by = 1$$

Def. 27 Sei $M := \{k \in \{1, \ldots, m\} : ggT(k, m) = 1\}$. Die Funktion

$$\varphi : \mathbb{N} \to \mathbb{N}, \qquad \varphi(m) := |M|$$

heißt EULER*sche φ-Funktion*

Satz 20 Sei $m \in \mathbb{N}$, $x_1, \ldots, x_{\varphi(m)} \in \{1, \ldots, m\}$ seien zu m teilerfremd. Weiter sei $B \subseteq \mathbb{Z}_m$ definiert durch

$$B = \{[x_1]_\sim, \ldots, [x_{\varphi(m)}]_\sim\}$$

Dann gilt: $(B, \cdot)$ ist eine ABELsche Gruppe.

Satz 21 (Satz von FERMAT-EULER) Seien $a, m \in \mathbb{N}$ mit $\mathrm{ggT}(a, m) = 1$. Dann gilt:

$$a^{\varphi(m)} \equiv 1 \bmod m$$

Satz 22 Sei $m \in \mathbb{N}, m > 1$. Dann gilt: Es gibt endlich viele Primzahlen $p_1, \ldots, p_k$ mit

$$\prod_{i=1}^{k} p_i = m$$

Satz 23 Sei $m \in \mathbb{N}, m > 1$. $p_1, \ldots, p_m$ seien die Primzahlen aus obigem Satz. Dann gilt:

$$\varphi(m) = m \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Satz 24 (Chinesischer Restsatz) Seien $m_1, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd und

$$a_i \in \{0, \ldots, m_i - 1\} \qquad (i = 1, \ldots, k)$$

Gesucht ist ein $x \in \mathbb{N}_0$ mit

$$x \equiv a_i \bmod m_i \qquad (i = 1, \ldots k).$$

Es gilt:

$$x = \prod_{i=1}^{k} m_i \cdot \sum_{i=1}^{k} n_i \frac{a_i}{m_i},$$

wobei $n_i \in \{0, \ldots, m_i - 1\}$ $(i = 1, \ldots, k)$ durch

$$\frac{n_i}{m_i} \cdot \prod_{i=1}^{k} m_i \equiv 1 \bmod m_i$$

festgelegt ist.

Bem. Dieser Paragraph war ein Beispiel aus der Zahlentheorie, das häufig Anwendung in der Kryptographie findet.

6 Matrizen

Def. 28 Seien $n, m \in \mathbb{N}$. Elemente der Menge $\mathbb{K}^n$ heißen *Tupel*, ein Element der Menge $\mathbb{K}^{m\times n} := (\mathbb{K}^n)^m$ heißt (m,n)-*Matrix*. Schreibweisen:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, \qquad (a_{ij} \in \mathbb{K},\ i = 1,\dots,m,\ j = 1,\dots,n)$$

oder $A = ((a_{ij}))$ oder $A = ((a_{ij}))_{m\times n}$ oder $A = (a_{ij})$ oder $A = (a_1|\dots|a_n)$, $(a_i \in \mathbb{K}^m)$ oder

$$A = \begin{pmatrix} a_1 \\ \hline \vdots \\ \hline a_m \end{pmatrix}, \qquad (a_i \in \mathbb{K}^n, 1 \le i \le m).$$

Bem.

- m bezeichnet die *Zeilen* (erster Index), n die *Spalte* (zweiter Index) der Matrix.
- Die Begriffe Zeilen, Spalten, Diagonale, symmetrische oder quadratische Matrix werden in ihrer anschaulichen Bedeutung verwendet. Als *Nebendiagonale* bezeichnet man die Elemente $a_{i-1,i}$ $(i = 2,\dots,n)$ oder die Elemente $a_{i+1,i}$ $(i = 1,\dots,n-1)$. Die Definition von Diagonalen und Nebendiagonalen ist nur für quadratische Matrizen sinnvoll. Eine Matrix der Form

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

  heißt *obere Dreiecksmatrix*. Eine Matrix der Form

$$A = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ a_{1n} & \cdots & \cdots & a_{nn} \end{pmatrix}$$

  heißt *untere Dreiecksmatrix*.

- Die (n,n)-Matrix

$$E_n := I := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

heißt *Einheitsmatrix*. Andere Darstellung: $I = ((\delta_{ij}))$ mit

$$\delta_{ij} := \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Diese Darstellung von I wird als KRONECKER-*Symbol* bezeichnet.

- Auf $\mathbb{K}^{m\times n}$ wird die Addition komonentenweise definiert. $(\mathbb{K}^{m\times n}, +)$ ist damit eine ABELsche Gruppe. Darin ist die *Nullmatrix* $((0))$ das Neutralelement und zu $((a_{ij})) \in \mathbb{K}^{m\times n}$ ist $((-a_{ij}))$ das Inverse.

Def. 29 Seien $A \in \mathbb{K}^{m\times n}, B \in \mathbb{K}^{n\times k}$. Dann heißt $C := ((c_{ij})) \in \mathbb{K}^{m\times k}$ mit

$$c_{ij} := \sum_{l=1}^{n} a_{il} b_{kl} \qquad (i = 1, \ldots, m; j = 1, \ldots, k)$$

das *Produkt* von A und B.

Bem.

- Beachte, daß die Matrizen „passend“ sein müssen.
- Die so definierte Matrizenmultiplikation ist i.A. keine Verknüpfung, da die Abgeschlossenheit verletzt ist.

Bsp. Sei $A \in \mathbb{R}^{2\times 3}, B \in \mathbb{R}^{3\times 2}$ mit

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

Dann gilt

$$\begin{aligned} A \cdot B &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} (1\cdot 0 + 2\cdot 1 + 3\cdot 0) & (2\cdot 1 - 1\cdot 2 + 3\cdot 1) \\ (3\cdot 0 + 2\cdot 1 + 1\cdot 0) & (3\cdot 2 - 2\cdot 1 + 1\cdot 1) \end{pmatrix} \\ &= \begin{pmatrix} 2 & 3 \\ 2 & 5 \end{pmatrix}, \\ B \cdot A &= \begin{pmatrix} 0 & 2 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 4 & 2 \\ -2 & 0 & 2 \\ 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

Satz 25 Seien A, B, C Matrizen, für die folgenden Operationen definiert sind. Dann gilt:

1. $(AB)C = A(BC)$,
2. $(A + B)C = AC + BC$, $A(B + C) = AB + AC$,
3. $IA = A = AI$.

Satz 26 Für $n \in \mathbb{N}$ ist $(\mathbb{K}^{n\times n}, +, \cdot)$ ein (nichtkommutativer) Ring mit Eins.

Bem. Es gibt kein $n \geq 2$, für das $(\mathbb{K}^{n\times n}, +, \cdot)$ kommutativ oder gar Körper ist.

Def. 30 Sei $A \in \mathbb{K}^{n\times n}$. Existiert ein $A^{-1} \in \mathbb{K}^{n\times n}$ mit $A \cdot A^{-1} = I$, so heißt A *regulär* (oder *invertierbar*). Ist A nicht regulär, so heißt A *singulär* .

Bem.

- Die Menge

  $$GL(\mathbb{K}, n) := \{A \in \mathbb{K}^{n\times n} : \ A \text{ ist regulär}\}$$

  ist eine Gruppe bezüglich Matrizenmultiplikation. Sie heißt *allgemeine lineare Gruppe.*

- Sei $A = ((a_{ij})) \in \mathbb{K}^{m\times n}$. $A^\top := ((b_{ij})) \in \mathbb{K}^{n\times m}$ mit

  $$b_{ij} := a_{ji} \qquad (i = 1, \ldots, m, \ j = 1, \ldots, n)$$

  heißt die zu A *transponierte* (oder *gespiegelte*) Matrix. Es gilt:

  $$\begin{aligned} (A^\top)^\top &= A \\ (A+B)^\top &= A^\top + B^\top \\ (A \cdot B)^\top &= B^\top \cdot A^\top \\ (A^{-1})^\top &= (A^\top)^{-1} \end{aligned}$$

  Ist A symmetrisch, so gilt $A = A^\top$.

Def. 31 Seien $A = ((a_{ij})) \in \mathbb{K}^{m\times n}$, $c \in \mathbb{K}$. Dann ist $c \cdot A$ definiert durch $((c \cdot a_{ij}))$

Bem. Statt eines Grundkörpers $\mathbb{K}$ kann man zur Definition von Matrizen auch allgemeiner kommutative Ringe mit Eins zugrundelegen. Die Sätze und Definitionen dieses Paragraphen gelten dann analog.

7 Polynome

Def. 32 Sei $(a_n)_{n=0}^\infty$ eine Folge in $\mathbb{K}$ mit

$$\exists \quad n_0 \in \mathbb{N}_0 \quad \forall \quad n \geq n_0 : \qquad a_n = 0.$$

Dann heißt $p := (a_n)_{n=0}^\infty$ *Polynom* über $\mathbb{K}$. $\operatorname{Grad} p := n_0$ heißt *Grad* von p. Für das *Nullpolynom* $\mathbf{0} := (0, 0, 0, \ldots)$ sei Grad $\mathbf{0} := -1$. Es sei

$$\mathbb{K}[x] := \{(a_n) \in \mathbb{K}^{\mathbb{N}} : (a_n) \text{ ist Polynom}\}$$

Für $p \in \mathbb{K}[x]$ und ein spezielles $x_0 \in \mathbb{K}$ heißt

$$p(x_0) := \sum_{n=0}^{\infty} a_n x_0^n$$

Auswertung von p an der Stelle x_0. Ist $p(x_0) = 0$, so heißt x_0 *Nullstelle* von p.

Bem. Statt $(a_0, a_1, a_2, \ldots)$ verwendet man auch die Schreibweise

$$a_0 + a_1 x + a_2 x^2 + \ldots.$$

Def. 33 Seien $p := (a_n)_{n=0}^{\infty}, q := (b_n)_{n=0}^{\infty} \in \mathbb{K}[x]$. Dann wird durch

$$p + q := (c_n)_{n=0}^{\infty}, \qquad c_i = a_i + b_i \quad (i \in \mathbb{N}_0)$$

eine Addition $+$ und durch

$$p \cdot q := (c_n)_{n=0}^{\infty}, \qquad c_i = \sum_{k=0}^{i} a_k b_{i-k} \quad (i \in \mathbb{N}_0)$$

eine Multiplikation $\cdot$ auf $\mathbb{K}[x]$ definiert.

Bem. Für $p, q \in \mathbb{K}[x], x \in \mathbb{K}$ gilt:

$$p(x) \cdot q(x) = (p \cdot q)(x), \qquad p(x) + q(x) = (p+q)(x)$$

Satz 27 $(\mathbb{K}[x], +, \cdot)$ ist ein kommutativer Ring mit Eins.

Satz 28 Seien $p, q \in \mathbb{K}[x]$, $q \neq \mathbf{0}$. Dann gilt:

$$\exists \quad r, s \in \mathbb{K}[x], \;\; \operatorname{Grad} r < \operatorname{Grad} q : \qquad p = s \cdot q + r$$

Bem. Sei $p \in \mathbb{K}[x], x_0 \in \mathbb{K}$. Dann gilt:

$$p(x_0) = 0 \qquad \Longleftrightarrow \qquad \exists \quad s \in \mathbb{K}[x] : \qquad p = (x - x_0) \cdot s$$

Satz 29 (Fundamentalsatz der Algebra) Sei $p \in \mathbb{C}[x]$ mit $\operatorname{Grad} p > 1$. Dann gilt: p hat (mindestens) eine Nullstelle.

Def. 34 Seien $s, p \in \mathbb{K}[x]$. s heißt *Teiler* von p $:\Longleftrightarrow$

$$\exists \quad r \in \mathbb{K}[x] : \qquad p = s \cdot r$$

Schreibweise in diesem Fall: $s \mid r$ (Sprechweise: „s teilt r"). Sind $p, q \in \mathbb{K}[x]$, ist

$$T := \{s \in \mathbb{K}[x] : \quad s \mid p \;\wedge\; s \mid q\}$$

und gilt

$$\forall \quad s \in T : \qquad \operatorname{Grad} s \leq 0$$

dann heißen p und q zueinander *teilerfremd*

Satz 30 Seien $p, q \in \mathbb{K}[x]$. Dann gilt: p, q sind teilerfremd $\Longleftrightarrow$

$$\exists \quad s, r \in \mathbb{K}[x] : \qquad r \cdot p + s \cdot q = 1$$

8 Der Gauss-Algorithmus

Wir betrachten ein *lineares Gleichungssystem*. Für vorgegebene $a_{ij}, b_i \in \mathbb{K}$ werden $x_j \in \mathbb{K}$ $(1 \le i \le m, 1 \le j \le n)$ gesucht mit:

$$\begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ \vdots & & \ddots & & \vdots & & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array}$$

Solche Lineare Gleichungssysteme lassen sich durch

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

als Matrizenmultiplikation darstellen. Einfacher läßt sich das Gleichungssystem als *erweiterte Matrix* darstellen durch

$$\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right).$$

Ist $b_1 = \cdots = b_m = 0$, so heißt das Gleichungssystem *homogen* und wird nur durch die Matrix $((a_{ij}))$ dargestellt.

Def. 35 Zwei lineare Gleichungssysteme heißen *äquivalent*, wenn sie die selbe Lösungsmenge haben.

Satz 31 Seien $AX = B$ und $CX = D$ zwei lineare Gleichungssysteme. Dann gilt: Die Gleichungssysteme sind äquivalent $\Longleftrightarrow$ $(A|B)$ kann durch endlich viele *elementare Zeilenumformungen* in $(C|D)$ umgewandelt werden. Als elementare Zeilenumformungen gelten dabei:

1. Vertauschen zweier Zeilen,
2. Multiplikation einer Zeile mit $c \in \mathbb{K} \setminus \{0\}$,
3. Addition des c-fachen einer Zeile zu einer anderen $(c \in \mathbb{K})$.

Geht $(A|B)$ durch eine elementare Zeilenumformung in $(C|D)$ über, so schreibt man: $(A|B) \rightsquigarrow (C|D)$

Bsp. Betrachte das lineare Gleichungsssystem

$$\begin{array}{rcrcrcrcrcr} -2x_1 & + & 4x_2 & - & 2x_3 & - & x_4 & + & 4x_5 & = & -3 \\ 4x_1 & - & 8x_2 & + & 3x_3 & - & 3x_4 & + & x_5 & = & 2 \\ x_1 & - & 2x_2 & + & x_3 & - & x_4 & + & x_5 & = & 0 \\ x_1 & - & 2x_2 & & & - & 3x_4 & + & 4x_5 & = & a \end{array}$$

Wir lösen das Gleichungssystem nach dem Verfahren von Gauss:

$$\left(\begin{array}{rrrrr|r} -2 & 4 & -2 & -1 & 4 & -3 \\ 4 & -8 & 3 & -3 & 1 & 2 \\ 1 & -2 & 1 & -1 & 1 & 0 \\ 1 & -2 & 0 & -3 & 4 & a \end{array}\right) \rightsquigarrow \left(\begin{array}{rrrrr|r} 1 & -2 & 1 & -1 & 1 & 0 \\ 4 & -8 & 3 & -3 & 1 & 2 \\ -2 & 4 & -2 & -1 & 4 & -3 \\ 1 & -2 & 0 & -3 & 4 & a \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{rrrrr|r} 1 & -2 & 1 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 & -3 & 2 \\ 0 & 0 & 0 & -3 & 6 & -3 \\ 0 & 0 & -1 & -2 & 3 & a \end{array}\right) \rightsquigarrow \left(\begin{array}{rrrrr|r} 1 & -2 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 3 & -2 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & -3 & 6 & a+2 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{rrrrr|r} 1 & -2 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 3 & -2 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 & a+1 \end{array}\right)$$

Diese Darstellung heißt *Treppennormalform*. Sie steht für das Gleichungssystem

$$\begin{array}{rcrcrcrcrcr} x_1 & - & 2x_2 & + & x_3 & - & x_4 & + & x_5 & = & 0 \\ & & & & x_3 & - & x_4 & + & 3x_5 & = & -2 \\ & & & & & & x_4 & - & 2x_5 & = & 1 \\ & & & & & & & & 0 & = & a+1 \end{array}$$

Aus dieser Darstellung läßt sich ablesen: Das lineare Gleichungssystem ist nur lösbar für $a = -1$. In diesem Fall gilt:

$$\begin{array}{rl} & x_5 \text{ ist beliebig, sei } x_5 := s \\ \Longrightarrow & x_4 = 1 + 2x_5 = 1 + 2s \\ \Longrightarrow & x_3 = -2 + x_4 - 3x_5 = -1 - s \\ \Longrightarrow & x_2 \text{ ist beliebig, sei } x_2 := t \\ \Longrightarrow & x_1 = 2x_2 - x_3 + x_4 - x_5 = 2 + 2t + 2s \end{array}$$

Damit ist für beliebige $s, t \in \mathbb{R}$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 2+2t+2s \\ t \\ -1-s \\ 1+2s \\ s \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} + s \begin{pmatrix} 2 \\ 0 \\ -1 \\ 2 \\ 1 \end{pmatrix} + t \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

eine Lösung des linearen Gleichungssystems.

Satz 32 (Gauss-Algorithmus) Sei $AX = B, A \in \mathbb{K}^{m \times n}, B \in \mathbb{K}^{m \times 1}$ ein lineares Gleichungssystem. Dann liefert der folgende Algorithmus die Treppennormalform der erweiterten Matrix $C := (A|B) := ((c_{ij}))$

Schritt A:

IF $\exists \quad i \in \{1, \ldots, m\}: \qquad c_{i1} \neq 0$ THEN

vertausche gegebenenfalls die Zeilen in A so, daß $c_{11} \neq 0$

`ELSE`

gehe zu Schritt C

Schritt B:

Multipliziere Zeile 1 mit $(c_{11})^{-1}$

`FOR` $i = 2, \ldots, m$

addiere das $(-c_{i1})$-fache von Zeile 1 zu Zeile i

Schritt C:

`IF` $c_{11} = 0$ `THEN`

$$C := \begin{pmatrix} c_{12} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m2} & \cdots & c_{mn} \end{pmatrix} \qquad \in \mathbb{K}^{m \times (n-1)}$$

`ELSE IF` $c_{11} = 1$ `THEN`

$$C := \begin{pmatrix} c_{22} & \cdots & c_{2n} \\ \vdots & \ddots & \vdots \\ c_{m2} & \cdots & c_{mn} \end{pmatrix} \qquad \in \mathbb{K}^{(m-1) \times (n-1)}$$

`ELSE` Ende.

Dieser Algorithmus liefert die Treppennormalform von $(A|B)$:

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

Aus dieser Darstellung kann man wie im obigen Beispiel die Lösung(en) des linearen Gleichungssystems ablesen.

Def. 36 Sei $A \in \mathbb{K}^{m \times n}$, $\tilde{A}$ sei die Treppennormalform von A. k sei die Anzahl der Zeilen i in $\tilde{A}$ mit

$$a_{i1} = a_{i2} = \cdots = a_{in} = 0$$

Dann heißt $\operatorname{Rang} A := n - k$ der *Rang* von A.

9 Vektorräume

Def. 37 Sei V eine Menge und

$$+ : V \times V \to V, \qquad \cdot : \mathbb{K} \times V \to V$$

seien Abbildungen. Es gelte:

1. $(V,+)$ ist ABELsche Gruppe
2. $\forall \quad a,b \in \mathbb{K}, \mathbf{x}, \mathbf{y} \in V:$

$$\begin{aligned} a \cdot (\mathbf{x} + \mathbf{y}) &= a\mathbf{x} + a\mathbf{y} \\ (a+b) \cdot \mathbf{x} &= a\mathbf{x} + b\mathbf{x} \end{aligned}$$

3. $\forall \quad a,b \in \mathbb{K}, \mathbf{x} \in V: \qquad a(b\mathbf{x}) = (ab)\mathbf{x}$
4. $1 \cdot \mathbf{x} = \mathbf{x}$

Dann heißt $(V,+,\cdot)$ (oder auch V) *Vektorraum* über $\mathbb{K}$ (oder $\mathbb{K}$-Vektorraum). Die Elemente von V heißen *Vektoren*. Das Neutralelement in V bezüglich $+$ heißt *Nullvektor*. Die Elemente von $\mathbb{K}$ bezeichnet man als *Skalare*.

Bem. Die Abbildung $+$ ist eine Verknüpfung. Sie wird als *Vektoraddition* bezeichnet. Eine Abbildung der Form $\cdot$ wird als *äußere Verknüpfung* bezeichnet. Hier heißt $\cdot$ *Skalarmultiplikation*

Bsp.

- Für $n \in \mathbb{N}$ ist $V = \mathbb{K}^n$ ein Vektorraum, wenn $+$ und $\cdot$ komponentenweise erklärt werden.
- Für $n,m \in \mathbb{N}$ ist $V = \mathbb{K}^{m \times n}$ ebenfalls ein Vektorraum. Man kann $\mathbb{K}^{n \times n}$ mit $\mathbb{K}^{nm}$ identifizieren. Deshalb brauchen $\mathbb{K}^{n \times 1}, \mathbb{K}^{1 \times n}$ und $\mathbb{K}^n$ als Vektorräume nicht unterschieden zu werden.
- $V := \mathbb{K}[x]$ ist ein Vektorraum, wenn $+$ und $\cdot$ komponentenweise erklärt werden.
- $\mathbb{K}$ selbst ist ein Vektorraum.
- Sei $A \neq \emptyset$ und $V := \mathbb{K}^A$. Addition sei durch

  $$(f+g)(x) := f(x) + g(x) \qquad (x \in \mathbb{K}, f,g \in V)$$

  und Skalarmultiplikation durch

  $$(af)(x) := a(f(x)) \qquad (a, x \in \mathbb{K}, f \in V)$$

  definiert. Dann ist V ein Vektorraum.

Def. 38 Sei V ein $\mathbb{K}$-Vektorraum, $\mathbf{x}_1, \ldots, \mathbf{x}_k \in V$, $a_1, \ldots, a_k \in \mathbb{K}$. Dann heißt

$$\mathbf{x} = \sum_{i=1}^{k} a_i \mathbf{x}_i$$

Linearkombination von $\mathbf{x}_1, \ldots, \mathbf{x}_k$

Satz 33 Sei V ein $\mathbb{K}$-Vektorraum. Dann gilt:

1. $\forall \quad a \in \mathbb{K}: \qquad a\mathbf{0} = \mathbf{0}$
2. $\forall \quad \mathbf{x} \in V: \qquad 0\mathbf{x} = \mathbf{0}$

3. $a\mathbf{x} = \mathbf{0} \iff a = 0 \vee \mathbf{x} = \mathbf{0}$

4. $\forall \ \mathbf{x} \in V: \quad (-1)\cdot\mathbf{x} = -\mathbf{x}$

Def. 39 Sei V ein $\mathbb{K}$-Vektorraum und $\emptyset \neq U \subseteq V$. Ist U mit den auf V definierten Verknüpfungen $+$ und $\cdot$ ein Vektorraum, so heißt U *Untervektorraum* (oder *(linearer) Unterraum* oder *Teilraum*) von V.

Satz 34 Sei V ein $\mathbb{K}$-Vektorraum und $\emptyset \neq U \subseteq V$. Es gilt: U ist Untervektorraum von V $\iff$

$$\forall \ \mathbf{x}, \mathbf{y} \in U, a, b \in \mathbb{K}: \qquad a\mathbf{x} + b\mathbf{y} \in U$$

Bsp.

- Zu jedem Vektorraum V sind V und $\{\mathbf{0}\}$ Untervektorräume.
- Die Lösungsmenge eines homogenen linearen Gleichungssystems mit n Unbekannten ist Untervektorraum des $\mathbb{K}^n$.
- Sei $A \neq \emptyset$, $a \in A$.

  $$U := \{f \in \mathbb{K}^A : \ f(a) = 0\}$$

  ist Untervektorraum von $\mathbb{K}^A$.

Satz 35 Der Schnitt beliebig vieler Untervektorräume ist ein Untervektorraum.

Def. 40 Sei V ein $\mathbb{K}$-Vektorraum und $A \subseteq V$. Dann heißt

$$[A] := \bigcap_{\substack{U \text{ UVR von } V \\ A \subseteq U}} U$$

die *lineare Hülle* von A. Statt $[\{\mathbf{x}_1, \ldots, \mathbf{x}_k\}]$ schreibt man auch $[\mathbf{x}_1, \ldots, \mathbf{x}_k]$. Sprechweise: „$\mathbf{x}_1, \ldots, \mathbf{x}_k$ erzeugen U" (oder „$\mathbf{x}_1, \ldots, \mathbf{x}_k$ spannen U auf"). Ist U ein Untervektorraum von V und $[A] = U$, dann heißt A *Erzeugendensystem* von U.

Bsp.

- Es ist $[\emptyset] = \{\mathbf{0}\}$. Ist V ein $\mathbb{K}$-Vektorraum, so ist $[V] = V$. Für $\mathbf{x} \in V$ gilt

  $$[\mathbf{x}] = \{a\mathbf{x} : a \in \mathbb{K}\}$$

- Ist $V = \mathbb{R}^3$ und $\mathbf{x}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{x}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, so ist

  $$[\mathbf{x}_1, \mathbf{x}_2] = \{a_1\mathbf{x}_1 + a_2\mathbf{x}_2 : a_1, a_2 \in \mathbb{R}\} = \{\begin{pmatrix} a_1 \\ a_2 \\ 0 \end{pmatrix}, a_1, a_2 \in \mathbb{R}\} \cong \mathbb{R}^2.$$

Satz 36 Sei V ein $\mathbb{K}$-Vektorraum und $\emptyset \neq A \subseteq V$. Dann gilt:

$$[A] = \{\mathbf{x} \in V : \mathbf{x} \text{ ist Linearkombination von Vektoren aus } A\}$$

10 Lineare Abhängigkeit

Def. 41 Sei V ein $\mathbb{K}$-Vektorraum und $\mathbf{x}_1, \ldots, \mathbf{x}_k \in V$. $\mathbf{x}_1, \ldots, \mathbf{x}_k$ heißen *linear abhängig* $:\Longleftrightarrow$ Es gibt eine Linearkombination

$$\sum_{i=1}^{k} a_i \mathbf{x}_i = \mathbf{0}$$

mit mindestens einem $a_i \neq 0$ $(i = 1, \ldots, k)$. $\mathbf{x}_1, \ldots, \mathbf{x}_k$ heißen *linear unabhängig* $:\Longleftrightarrow$

$$\sum_{i=1}^{k} a_i \mathbf{x}_i = \mathbf{0} \qquad \Longleftrightarrow \qquad a_1 = \cdots = a_k = 0$$

Bem.

- Es gilt:

$$\mathbf{x}_1, \ldots, \mathbf{x}_k \text{ linear unabhängig} \quad \Longleftrightarrow \quad \neg(\mathbf{x}_1, \ldots, \mathbf{x}_k \text{ linear abhängig})$$

- Es gilt:

$$\exists\, 1 \leq i \leq k: \ \mathbf{x}_i = \mathbf{0} \quad \Longrightarrow \quad \mathbf{x}_1, \ldots, \mathbf{x}_k \text{ linear abhängig}$$
$$\exists\, 1 \leq i, j \leq k,\ i \neq j: \ \mathbf{x}_i = \mathbf{x}_j \quad \Longrightarrow \quad \mathbf{x}_1, \ldots, \mathbf{x}_k \text{ linear abhängig}$$

- Es gilt: $\mathbf{x}_1, \ldots, \mathbf{x}_k$ sind linear abhängig $\Longleftrightarrow$ $\mathbf{x}_1$ ist Linearkombination von $\mathbf{x}_2, \ldots, \mathbf{x}_k$. $\mathbf{x} \in V$ ist linear abhängig $\Longleftrightarrow$ $\mathbf{x} = \mathbf{0}$

- Seien $\mathbf{x}_1, \ldots, \mathbf{x}_k \in V$. Zur Prüfung auf Lineare Unabhängigkeit löse das lineare Gleichungssystem

$$(\mathbf{x}_1 | \ldots | \mathbf{x}_k) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

  Ist ein a_i $(i = 1, \ldots, k)$ beliebig, so sind $\mathbf{x}_1, \ldots, \mathbf{x}_k$ linear abhängig.

Bsp. Sei $V = \mathbb{R}^4$, $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \in \mathbb{R}^3$ mit

$$\mathbf{x}_1 := \begin{pmatrix} 2 \\ -3 \\ 1 \\ 4 \end{pmatrix}, \qquad \mathbf{x}_2 := \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \qquad \mathbf{x}_3 := \begin{pmatrix} -2 \\ 1 \\ -1 \\ 1 \end{pmatrix}.$$

Wegen

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

ist $a_3 = a_2 = a_1 = 0$. Damit sind $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ linear unabhängig.

Satz 37 Seien $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{K}^n$ mit $k > n$. Dann sind $\mathbf{x}_1, \ldots, \mathbf{x}_k$ linear abhängig.

Def. 42 Sei V ein $\mathbb{K}$-Vektorraum, $A \subseteq V$. A heißt *linear abhängig* $:\Longleftrightarrow$

$$\exists \quad \mathbf{x}_1, \ldots \mathbf{x}_k \in A : \qquad \mathbf{x}_1, \ldots, \mathbf{x}_k \text{ sind linear abhängig}$$

Ist A nicht linear abhängig, so heißt A linear unabhängig.

Bem.

- Sei $A = \{\mathbf{x}_1, \ldots, \mathbf{x}_k\} \subseteq V$. Dann gilt:

  $$A \text{ ist linear abhängig} \qquad \Longleftrightarrow \qquad \mathbf{x}_1, \ldots, \mathbf{x}_k \text{ sind linear abhängig}$$

- $\mathbf{0} \in A \Longrightarrow A$ ist linear abhängig.
- Ist A linear abhängig und $A \subseteq B$, so ist B linear abhängig. Ist A linear unabhängig und $B \subseteq A$, so ist B linear unabhängig.
- A ist linear abhängig $\Longleftrightarrow$

  $$\exists \quad \mathbf{x} \in A : \qquad [A] = [A \setminus \{\mathbf{x}_1\}]$$

- Sei $\mathbf{x} \in V$, $A \subseteq V$, $\mathbf{x} \notin A$. Es gilt:

  $$\mathbf{x} \notin [A] \qquad \Longleftrightarrow \qquad A \cup \{\mathbf{x}\} \text{ ist linear unabhängig}$$

11 Basis und Dimension

Def. 43 Sei V ein $\mathbb{K}$-Vektorraum.

1. Sei $A \subseteq V$ mit $[A] = V$. A heißt *minimales* Erzeugendensystem von V $:\Longleftrightarrow$

   $$\forall \quad B \subset A : \qquad [B] \neq V$$

2. Sei $A \subseteq V$ linear unabhängig. A heißt *maximal* $:\Longleftrightarrow$

   $$\forall \quad B \supset A : \qquad B \text{ ist linear abhängig}$$

3. Sei $A \subseteq V$ linear unabhängig und $[A] = V$. Dann heißt A *Basis* von V.

Satz 38 Sei V ein $\mathbb{K}$-Vektorraum und $\emptyset \neq B \subseteq V$. Dann sind folgende Aussagen äquivalent:

1. B ist Basis von V
2. B ist minimales Erzeugendensystem von V
3. B ist maximale linear unabhängige Teilmenge von V.

4. Sei $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$. Dann gilt

$$\forall \quad \mathbf{x} \in V \quad \exists \quad b_1, \ldots, b_k : \qquad \mathbf{x} = \sum_{i=1}^{k} b_i \mathbf{b}_i$$

Bsp.

- $\emptyset$ ist Basis von $\{\mathbf{0}\}$
- Sei $V = \mathbb{K}^n$ und $B = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ mit

$$\mathbf{e}_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow i\text{-te Stelle} \\ \\ \\ \\ \end{array}$$

- Zu $V = \mathbb{K}[x]$ ist

$$B = \{x^i, \ i \in \mathbb{N}_0\}$$

  eine Basis

Satz 39 Sei V ein $\mathbb{K}$-Vektorraum. $B, \tilde{B}$ seien Basen von V. Dann gilt $|B| = |\tilde{B}|$.

Satz 40 Sei V ein $\mathbb{K}$-Vektorraum und $A \subseteq V$ mit $[A] = V$ und $|A| < \infty$. Dann gilt

$$\exists \quad B \subseteq A : \qquad B \text{ ist Basis von } V$$

Bem. Ist V ein $\mathbb{K}$-Vektorraum und B Basis von V mit $|B| < \infty$. Dann gilt:

$$\forall \quad A \subseteq V, |B| = |A| : \qquad A \text{ ist Basis von } V$$

Def. 44 Sei V ein $\mathbb{K}$-Vektorraum. B sei Basis von V. Ist $|B| < \infty$, so heißt $|B|$ *Dimension* von V, Schreibweise $\dim V = |B|$. Ist B nicht endlich, so heißt V unendlich dimensional, Schreibweise $\dim V = \infty$.

Satz 41 (Basisergänzungssatz) Sei V ein $\mathbb{K}$-Vektorraum und $A \subseteq V$ linear unabhängig. Dann gilt:

$$\exists \quad B \text{ Basis von } V : \qquad A \subseteq B$$

Bem. Jeder $\mathbb{K}$-Vektorraum hat eine Basis.

Satz 42 Sei V ein $\mathbb{K}$-Vektorraum mit $\dim V = n$. U sei Untervektorraum von V. Dann gilt:

1. $\dim U \leq n$
2. $\dim U = n \quad \Longleftrightarrow \quad U = V$

Bsp. Sei $V = \mathbb{K}^{\mathbb{N}}$ und $U = \mathbb{K}[x]$. Dann ist $\dim V = \dim U = \infty$, U ist Untervektorraum von V, aber es gilt $U \neq V$

Satz 43 Sei V ein $\mathbb{K}$-Vektorraum, $W = [\mathbf{x}_1, \ldots, \mathbf{x}_k]$ ein Untervektorraum von V. $\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_k$ seien die Vektoren, die nach Anwendung des GAUSS-Algorithmus auf die Matrix

$$A = \begin{pmatrix} \mathbf{x}_1^\top \\ \hline \vdots \\ \hline \mathbf{x}_k^\top \end{pmatrix}$$

In den Zeilen der Treppennormalform stehen. Dann gilt: Die Menge aller von $\mathbf{0}$ verschiedenen Vektoren $\tilde{\mathbf{x}}_i$ $(i = 1, \ldots, k)$ bilden eine Basis von W. Es gilt $\dim W = \operatorname{Rang} A$.

Bsp. Sei $V = \mathbb{R}^5$, $W = [\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4]$ mit

$$\mathbf{x}_1 := \begin{pmatrix} 1 \\ 2 \\ -1 \\ -1 \\ -1 \end{pmatrix}, \quad \mathbf{x}_2 := \begin{pmatrix} 2 \\ -1 \\ 1 \\ 2 \\ -2 \end{pmatrix}, \quad \mathbf{x}_3 := \begin{pmatrix} 3 \\ -4 \\ 3 \\ 5 \\ -3 \end{pmatrix}, \quad \mathbf{x}_4 := \begin{pmatrix} -1 \\ 8 \\ -5 \\ 6 \\ 1 \end{pmatrix}.$$

Wegen

$$\begin{pmatrix} \mathbf{x}_1^\top \\ \mathbf{x}_2^\top \\ \mathbf{x}_3^\top \\ \mathbf{x}_4^\top \end{pmatrix} = \begin{pmatrix} 1 & 2 & -1 & -1 & -1 \\ 2 & -1 & 1 & 2 & -2 \\ 3 & -4 & 3 & 5 & -3 \\ -1 & 8 & -5 & 6 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & \frac{1}{5} & 0 & -1 \\ 0 & 1 & -\frac{3}{5} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

ist

$$B = \{ \begin{pmatrix} 5 \\ 0 \\ 1 \\ 0 \\ -5 \end{pmatrix}, \begin{pmatrix} 0 \\ 5 \\ -3 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \}$$

eine Basis von W.

Satz 44 Sei $V = \mathbb{K}^n$, $U = [\mathbf{x}_1, \ldots, \mathbf{x}_k]$ ein Untervektorraum von V. Weiter sei

$$A := (\mathbf{x}_1 | \cdots | \mathbf{x}_k)$$

Dann gilt: Die Vektoren $\mathbf{x}_j$, für die j der Index einer „Treppenstufe“ in der Normalform von A ist, bilden eine Basis von U. Weiter gilt $\dim U = \operatorname{Rang} A$.

Bsp. Sei $V = \mathbb{R}^5$, $W = [\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4]$ mit

$$\mathbf{x}_1 := \begin{pmatrix} 1 \\ 2 \\ -1 \\ -1 \\ -1 \end{pmatrix}, \quad \mathbf{x}_2 := \begin{pmatrix} 2 \\ -1 \\ 1 \\ 2 \\ -2 \end{pmatrix}, \quad \mathbf{x}_3 := \begin{pmatrix} 3 \\ -4 \\ 3 \\ 5 \\ -3 \end{pmatrix}, \quad \mathbf{x}_4 := \begin{pmatrix} -1 \\ 8 \\ -5 \\ 6 \\ 1 \end{pmatrix}.$$

Wegen

$$(\mathbf{x}_1|\mathbf{x}_2|\mathbf{x}_3|\mathbf{x}_4) = \begin{pmatrix} 1 & 2 & 3 & -1 \\ 2 & -1 & -4 & 8 \\ -1 & 1 & 3 & -5 \\ -1 & 2 & 5 & -6 \\ -1 & -2 & -3 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 & -1 \\ 0 & 1 & 2 & -2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

ist

$$B = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_4\}$$

eine Basis von W.

Satz 45 Sei $A \in \mathbb{K}^{m \times n}$. Dann gilt: Die Menge L mit

$$L := \{\mathbf{x} \in \mathbb{K}^m : A\mathbf{x} = \mathbf{0}\}$$

ist ein Untervektorraum von $\mathbb{K}^m$ und es gilt $\dim L = n - \operatorname{Rang} A$.

12 Summen- und Faktorräume

Def. 45 Sei V ein $\mathbb{K}$-Vektorraum und $A_1, \ldots, A_k \subseteq V$. Dann heißt

$$A_1 + \cdots + A_k := \sum_{i=1}^{k} A_i := \{\mathbf{x} \in V : \mathbf{x} = \sum_{i=1}^{k} \mathbf{x}_i,\ \mathbf{x}_i \in A_i\ (i = 1, \ldots, k)\}$$

die *Summe* von $A_1, \ldots, A_k$. Ist $\mathbf{x} \in V$ und $B \subseteq V$, so schreibt man statt $\{\mathbf{x}\}+B$ auch $\mathbf{x} + B$.

Bem. Es gilt $[A_1] + \cdots + [A_k] = [A_1 \cup \cdots \cup A_k]$.

Def. 46 Sei V ein $\mathbb{K}$-Vektorraum und $U_1, \ldots, U_k$ seien Untervektorräume von V. Die Summe

$$U := U_1 + \cdots + U_k$$

heißt *direkt* $:\Longleftrightarrow$

$$\forall \quad i \in \{1, \ldots, k\} : \qquad U_i \cap \sum_{\substack{j=1 \\ i \neq j}}^{k} U_j = \{\mathbf{0}\}$$

Schreibweise in diesem Fall: $U = U_1 \oplus \cdots \oplus U_k$.

Bem. Die Summe von Untervektorräumen ist ein Untervektorraum.

Satz 46 Sei V ein $\mathbb{K}$-Vektorraum und $U_1, \ldots, U_k$ seien Untervektorräume von V. Dann gilt: Die Summe $U := U_1 + \cdots + U_k$ ist direkt $\Longleftrightarrow$ Zu jedem Vektor $\mathbf{x} \in U$ ist die Darstellung

$$\mathbf{x} = \sum_{i=1}^{k} \mathbf{x}_i \qquad (\mathbf{x}_i \in U_i, i = 1, \ldots, k)$$

eindeutig.

Satz 47 Sei V ein $\mathbb{K}$-Vektorraum und U, W seien Untervektorräume von V. Dann gilt:

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

Bem. Es gilt $\dim(U\oplus W)=\dim U+\dim W$.

Def. 47 Sei V ein $\mathbb{K}$-Vektorraum. U, W seien Untervektorräume von V mit

$$V=U\oplus W$$

Dann heißt W *Komplementärraum* zu U.

Satz 48 Sei V ein $\mathbb{K}$-Vektorraum und U ein Untervektorraum von V. Dann exisitert ein Komplementärraum W zu U.

Bem. Der Komplementärraum W ist nicht eindeutig.

Def. 48 Sei V ein $\mathbb{K}$-Vektorraum, U ein Untervektorraum zu V. Für $\mathbf{x}, \mathbf{y}\in V$ sei die Äquivalenzrelation $\sim$ definiert durch

$$\mathbf{x}\sim\mathbf{y} \qquad :\Longleftrightarrow \qquad \mathbf{x}-\mathbf{y}\in U$$

Auf der Menge $V/_U := V/_\sim$ seien für $\mathbf{x}, \mathbf{y}\in V, a\in\mathbb{K}$ definiert:

$$\begin{aligned}[\mathbf{x}]_\sim+[\mathbf{y}]_\sim &:= [\mathbf{x}+\mathbf{y}]_\sim\\ a[\mathbf{x}]_\sim &:= [a\mathbf{x}]_\sim.\end{aligned}$$

Dann heißt der Vektorraum $V/_U$ *Quotientenraum* (oder *Faktorraum*) von V nach U.

Bem. Es gilt $V/_{\{\mathbf{0}\}}\cong V$ und $V/_V=\{[\mathbf{0}]_\sim\}$.

Satz 49 Sei V ein $\mathbb{K}$-Vektorraum und U ein Untervektorraum zu V. Dann gilt:

$$\dim V/_U+\dim U=\dim V.$$

Satz 50 Sei V ein $\mathbb{K}$-Vektorraum, U ein Untervektorraum von V und B Basis von U. Ist $\tilde{B}$ mit $B\subseteq\tilde{B}$ eine Basis von V, so ist

$$\{[\mathbf{x}]_\sim\in V/_U : \quad \mathbf{x}\in\tilde{B}\setminus B\}$$

eine Basis von $V/_U$.

13 Affine Unterräume

Def. 49 Sei V ein $\mathbb{K}$-Vektorraum, U ein Untervektorraum von V und $\mathbf{x}\in V$. Dann heißt

$$L:=\mathbf{x}+U$$

affiner Unterraum von U. In diesem Fall heißt $\mathbf{x}$ *Aufpunkt* und U *Richtung* (oder *Richtungsraum*) von L.

$$\dim L:=\dim U$$

heißt *Dimension* von L.

Bem.

- Ist $\dim L = 0$, so heißt L *Punkt*.
  Ist $\dim L = 1$, so heißt L *Gerade*.
  Ist $\dim L = 2$, so heißt L *Ebene*.
  Ist $\dim L = \dim V - 1$, so heißt L *Hyperebene*.

- affine Unterräume werden auch in *Parameterdarstellung* geschrieben. Ist $L = \mathbf{x}_0 + U$ und $U = [\mathbf{x}_1, \ldots, \mathbf{x}_k]$, so schreibt man

$$L = \{\mathbf{x}_0 + a_1\mathbf{x}_1 + \cdots + a_k\mathbf{x}_k, \quad a_i \in \mathbb{K}\ (i = 1, \ldots, k)\}$$

  In dieser Darstellung heißen $\mathbf{x}_1, \ldots \mathbf{x}_k$ *Richtungsvektoren* und $a_1, \ldots, a_k$ *Parameter*.

Satz 51 Sei V ein $\mathbb{K}$-Vektorraum. $\mathcal{M}$ sei eine Menge affiner Unterräume in V. Dann gilt

$$M := \bigcap_{L \in \mathcal{M}} L$$

ist leer oder ein affiner Unterraum. Ist U_L der Richtungsraum zu $L \in \mathcal{M}$, so gilt

$$U_M := \bigcap_{L \in \mathcal{M}} U_L$$

ist Richtungsraum von M.

Def. 50 Sei V ein $\mathbb{K}$-Vektorraum. Weiter seien $L_1 = \mathbf{x}_1 + U_1$ und $L_2 := \mathbf{x}_2 + U_2$ affine Unterräume von V. L_1, L_2 heißen zueinander *parallel* $:\Longleftrightarrow$

$$U_1 \subseteq U_2 \qquad \vee \qquad U_2 \subseteq U_1$$

Schreibweise in diesem Fall: $L_1 || L_2$.

Bem.

- $||$ ist keine Äquivalenzrelation.

- Ist $L_1 \not\subseteq L_2$ und $L_2 \not\subseteq L_1$, so gilt $L_1 \cap L_2 = \emptyset$. In diesem Fall heißen L_1, L_2 *echt* parallel.

14 Lineare Abbildungen

Def. 51 Seien V, W Vektorräume über $\mathbb{K}$ und $\Phi : V \to W$ mit

$$\forall \quad \mathbf{x}, \mathbf{y} \in V, a, b \in K : \qquad \Phi(a\mathbf{x} + b\mathbf{y}) = a\Phi(\mathbf{x}) + b\Phi(\mathbf{y})$$

Dann heißt Φ (*Vektorraum-*) *Homomorphismus* (oder *linear*). Ist Φ zusätzlich bijektiv, so heißt Φ (*Vektorraum-*) *Isomorphismus*. Ist $\Phi : V \to W$ ein Isomorphismus, so heißen V, W zueinander *isomorph*, Schreibweise in diesem Fall: $V \cong W$.

Bem.

- $\cong$ ist eine Äquivalenzrelation.
- Weitere Bezeichnungen. Sei $\Phi : V \to W$ linear. Gilt $V = W$, so heißt Φ *Endomorphismus*. Ist Φ zusätzlich bijektiv, so heißt Φ *Automorphismus*. Lineare, injektive Abbildungen heißen *Monomorphismus* und lineare, surjektive Abbildungen heißen *Epimorphismus*.
- Ist $\Phi : V \to W$ linear, so gilt: $\Phi(\mathbf{0}) = \mathbf{0}$.
- Es sei

$$\begin{aligned} \operatorname{Bild}\Phi &:= \Phi(V) \\ \operatorname{Kern}\Phi &:= \{\mathbf{x} \in V : \Phi(\mathbf{x}) = \mathbf{0}\}. \end{aligned}$$

  Es gilt: $\operatorname{Bild}\Phi$ ist Untervektorraum von W, $\operatorname{Kern}\Phi$ ist Untervektorraum von W. Weiter gilt:

$$\begin{aligned} \Phi \text{ ist surjektiv} \quad &\iff \quad \operatorname{Bild}\Phi = W \\ \Phi \text{ ist injektiv} \quad &\iff \quad \operatorname{Kern}\Phi = \{\mathbf{0}\} \end{aligned}$$

Bsp. Sei $A = (\mathbf{a}_1|\cdots|\mathbf{a}_n) \in \mathbb{K}^{m\times n}$, $\Phi : \mathbb{K}^m \to \mathbb{K}^n$ definiert durch

$$\Phi(\mathbf{x}) = A\mathbf{x} \qquad (\mathbf{x} \in V)$$

Dann ist Φ linear und es gilt:

$$\begin{aligned} \operatorname{Bild}\Phi &= [\mathbf{a}_1, \ldots, \mathbf{a}_n] \\ \operatorname{Kern}\Phi &= \{\mathbf{x} \in \mathbb{K}^n : A\mathbf{x} = \mathbf{0}\} \end{aligned}$$

Beachte: $A\mathbf{x} = \mathbf{0}$ ist ein homogenes lineares Gleichungssystem.

Satz 52 (Homomorphiesatz für Vektorräume) Es seien V, W Vektorräume über $\mathbb{K}$ und $\Phi : V \to W$ linear. Dann gilt:

1. Die *kanonische* Abbildung

$$k : V \to {}^{V}\!/_{\operatorname{Kern}\Phi}, \qquad k(\mathbf{x}) = [\mathbf{x}]_\sim$$

   ist linear.
2. Es gibt eine lineare, injektive Abbildung $\tilde{\Phi} : {}^{V}\!/_{\operatorname{Kern}\Phi} \to W$ mit $\Phi = \tilde{\Phi} \circ k$.
3. Ist Φ surjektiv, so gilt

$${}^{V}\!/_{\operatorname{Kern}\Phi} \cong W$$

Satz 53 Seien V, W Vektorräume über $\mathbb{K}$ und $\Phi : V \to W$ linear. Dann gilt:

$${}^{V}\!/_{\operatorname{Kern}\Phi} \cong \operatorname{Bild}\Phi$$

Satz 54 Sei V ein $\mathbb{K}$-Vektorraum. U, W seien Untervektorräume zu V mit $V = U \oplus W$. Dann gilt

$$V/U \cong W, \qquad V/W \cong U$$

Def. 52 Sei V ein $\mathbb{K}$-Vektorraum und $\pi : V \to V$ linear. Weiter gelte:

$$\forall \quad \mathbf{x} \in V : \qquad \pi^2(\mathbf{x}) = \pi(\mathbf{x})$$

Dann heißt π *Projektion* von V auf $\operatorname{Bild} \pi$.

Bem. Ist $\pi : V \to V$ eine Projektion, so gilt:

$$V = \operatorname{Kern} \pi \oplus \operatorname{Bild} \pi.$$

Die Umkehrung gilt im Allgemeinen nicht.

Satz 55 Es seien V, W Vektorräume über $\mathbb{K}$ und B eine Basis von V. Es sei $\tilde{\Phi} : B \to W$ eine Abbildung. Dann gilt: Durch $\tilde{\Phi}$ wird eindeutig eine lineare Abbildung $\Phi : V \to W$ definiert.

Bem. Umgekehrt ist jede lineare Abbildung durch ihre Werte auf der Basis definiert.

Satz 56 Seien V, W Vektorräume über $\mathbb{K}$, $\dim V = n$, $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ eine Basis von V und $\Phi : V \to W$ linear. Dann gilt:

1. Φ ist injektiv $\Longleftrightarrow \Phi(\mathbf{b}_1), \ldots, \Phi(\mathbf{b}_n)$ sind linear unabhängig.
2. Φ ist surjektiv $\Longleftrightarrow [\Phi(\mathbf{b}_1), \ldots, \Phi(\mathbf{b}_n)] = W$
3. Φ ist bijektiv $\Longleftrightarrow \{\Phi(\mathbf{b}_1), \ldots, \Phi(\mathbf{b}_n)\}$ ist Basis von W.

Satz 57 (Isomorphiekriterium) Seien V, W endlich dimensionale Vektorräume über $\mathbb{K}$ mit $\dim V = \dim W = n$. $\Phi : V \to W$ sei linear. Dann sind folgende Aussagen äquivalent:

1. Φ ist injektiv
2. Φ ist surjektiv
3. Φ ist bijektiv

Bem. Für $\dim V = \dim W = \infty$ gilt diese Aussage im Allgemeinen nicht mehr.

Satz 58 Seien V, W endlich dimensionale Vektorräume über $\mathbb{K}$. Dann gilt:

$$V \cong W \qquad \Longleftrightarrow \qquad \dim V = \dim W.$$

Bem. Insbesondere sind alle $\mathbb{K}$-Vektorräume V mit $\dim V = n$ isomorph zu $\mathbb{K}^n$.

Satz 59 (Dimensionssatz für lineare Abbildungen) Es seien V, W Vektorräume über $\mathbb{K}$ und $\Phi : V \to W$ linear. Dann gilt:

$$\dim \operatorname{Kern} \Phi + \dim \operatorname{Bild} \Phi = \dim W$$

15 Vektorräume linearer Abbildungen

Bem. Sind V, W Vektorräume über $\mathbb{K}$, so ist

$$W^V := \{f : V \to W\}$$

ebenfalls ein Vektorraum.

Satz 60 Es seien U, V, W Vektorräume über $\mathbb{K}$. Dann gilt:

1. Sind $\Phi : U \to V$ und $\Psi : V \to W$ linear, so ist $(\Psi \circ \Phi) : U \to W$ linear.
2. Ist $\Phi : V \to W$ ein Isomorphismus, so ist $\Phi^{-1} : W \to V$ ebenfalls ein Isomorphismus.
3. Sind $\Phi, \Psi : V \to W$ linear, $a \in \mathbb{K}$, so sind $\Phi + \Psi$ und $a\Phi$ linear.

Bem.

- Die Menge

  $$\mathrm{Hom}(V, W) := \{\Phi \in W^V : \ \Phi \text{ ist linear}\}$$

  ist ein Untervektorraum von W^V. Speziell ist

  $$\mathrm{End}\, V := \mathrm{Hom}(V, V)$$

  zusätzlich ein Ring mit Eins. Weiter gilt für $a \in K, \Phi, \Psi \in \mathrm{End}\, V$:

  $$a(\Phi \circ \Psi) = (a\Phi) \circ \Psi = \Phi \circ (a\Psi)$$

  Allgemein heißt jeder Vektorraum V, der diese Eigenschaft erfüllt und Ring mit Eins ist, *Algebra* über $\mathbb{K}$.

- Der $\mathbb{K}$-Vektorraum

  $$\mathrm{Aut}\, V := \{\Phi \in \mathrm{End}\, V : \ \Phi \text{ ist Automorphismus}\}$$

  ist bezüglich $\circ$ eine Gruppe.

Satz 61 Seien V, W endlich dimensionale Vektorräume über $\mathbb{K}$. Dann gilt:

$$\dim \mathrm{Hom}(V, W) = \dim V \cdot \dim W$$

16 Dualräume

Def. 53 Ist V ein $\mathbb{K}$-Vektorraum, so heißt

$$V^* := \mathrm{Hom}(V, \mathbb{K})$$

Dualraum von V. $\mathbf{x}^* \in V^*$ heißt *lineares Funktional* (oder *Linearform*).

Bem. Die Elemente von V^* sind Abbildungen in V.

Bsp. Sei $V = \mathbb{R}[x]$. Dann ist

$$\mathbf{x}^* : V \to \mathbb{R} : \qquad \mathbf{x}^*(\mathbf{p}) := \mathbf{p}(0) \qquad (\mathbf{p} \in V)$$

ein Element von V^*.

Satz 62 Ist V ein $\mathbb{K}$-Vektorraum, $\dim V = n$, so gilt $\dim V^* = n$ und damit $V \cong V^*$. Ist $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ Basis von V, so ist $B^* := \{\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*\}$ mit

$$\mathbf{b}_i^*(\mathbf{b}_j) := \delta_{ij} \qquad (i, j = 1, \ldots, n)$$

Basis von V^*.

Bem.

- B^* heißt die zu B *duale* Basis. $\mathbf{b}_i^* \in B^*$ heißt i-tes *Koordinantenfunktional* bezüglich B.
- Für $\mathbf{x} \in V$ und $\mathbf{x}^* \in V^*$ gilt:

$$\begin{aligned} \mathbf{x} &= \mathbf{b}_1^*(\mathbf{x})\,\mathbf{b}_1 + \cdots + \mathbf{b}_n^*(\mathbf{x})\,\mathbf{b}_n \\ \mathbf{x}^* &= \mathbf{x}^*(\mathbf{b}_1)\,\mathbf{b}_1^* + \cdots + \mathbf{x}^*(\mathbf{b}_n)\,\mathbf{b}_n^* \end{aligned}$$

Def. 54 Sei V ein $\mathbb{K}$-Vektorraum und V^* der Dualraum von V. Dann heißt

$$V^{**} := (V^*)^*$$

der *Bidualraum* von V.

Satz 63 Sei V ein $\mathbb{K}$-Vektorraum und V^{**} der Bidualraum von V. Für $\mathbf{x} \in V$ sei $\Psi : V \to V^{**}$ definiert durch:

$$\Psi(\mathbf{x}) : V^* \to \mathbb{K}, \qquad (\Psi(\mathbf{x}))(\mathbf{x}^*) := \mathbf{x}^*(\mathbf{x}) \quad (\mathbf{x}^* \in V)$$

Dann gilt: Ψ ist injektiver Homomorphismus. Ist $\dim V < \infty$, so ist Ψ Isomorphismus von V und V^{**}.

17 Darstellung linearer Abbildungen durch Matrizen

Statt einer Menge $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ verwenden wir zur Charakterisierung einer Basis fortan ein n-Tupel:

$$B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$$

Damit wird die Reihenfolge der Vektoren in der Basis festgelegt. Man spricht von einer *geordneten* Basis.

Def. 55 Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$ und $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ eine geordnete Basis von V. Für $\mathbf{x} \in V$ sei

$$\mathbf{x} = a_1\,\mathbf{b}_1 + \cdots + a_n\,\mathbf{b}_n$$

die (eindeutige) Linearkombination von $\mathbf{x}$ durch Basisvektoren aus B. Dann heißt

$$\widehat{\mathbf{x}} := \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \qquad \in \mathbb{K}^n$$

Koordinatendarstellung (oder *Koordinatenvektor*) von $\mathbf{x}$ bezüglich B. Die Koeffizienten $a_1, \ldots, a_n$ heißen *Koordinaten.*

Bem. Die Abbildung $\Phi : V \to \mathbb{K}^n$, $\Phi(\mathbf{x}) := \widehat{\mathbf{x}}$ ist ein Isomorphismus von V und $\mathbb{K}^n$.

Def. 56 Seien V, W Vektorräume über $\mathbb{K}$, $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ sei Basis von V und $\tilde{B} = (\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_n)$ sei Basis von W. Weiter sei $\Phi \in \mathrm{Hom}(V, W)$. Dann heißt

$$A_\Phi := (\widehat{\Phi(\mathbf{b}_1)}| \cdots |\widehat{\Phi(\mathbf{b}_n)}) \in \mathbb{K}^{m \times n}$$

Abbildungsmatrix von Φ bezüglich B und $\tilde{B}$.

Bem. Es gilt $\mathrm{Rang}\, A_\Phi = \dim \mathrm{Bild}\, \Phi$. Es sei $\mathrm{Rang}\, \Phi := \mathrm{Rang}\, A_\Phi$ der *Rang* von Φ.

Satz 64 Seien V, W Vektorräume über $\mathbb{K}$, $\dim V = n$, $\dim W = m$. B sei geordente Basis von V und $\tilde{B}$ geordnete Basis von W. Dann gilt: Die Abbildung

$$\Psi : \mathrm{Hom}(V, W) \to \mathbb{K}^{m \times n} : \qquad \Psi(\Phi) = A_\Phi$$

ist Isomorphismus von $\mathrm{Hom}(V, W)$ nach $\mathbb{K}^{m \times n}$.

Satz 65 Seien V, W endlich dimensionale Vektorräume über $\mathbb{K}$, B sei Basis von V und $\tilde{B}$ sei Basis von W. Weiter sei $\Phi \in \mathrm{Hom}(V, W)$ und A_Φ die Abbildungsmatrix von Φ. Dann gilt

$$\forall \quad \mathbf{x} \in V : \qquad \widehat{\Phi(\mathbf{x})} = A_\Phi \cdot \widehat{\mathbf{x}}$$

Bem. Statt direkt mit einer Abbildung zu arbeiten, erlaubt dieser Satz einen „Umweg“ über die oft einfacheren Räume $\mathbb{K}^n$ und $\mathbb{K}^m$:

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & W \\ \downarrow & & \uparrow \\ \mathbb{K}^n & \xrightarrow[A_\Phi]{} & \mathbb{K}^m \end{array}$$

Satz 66 Seien U, V, W Vektorräume über $\mathbb{K}$ mit $\dim U = k$, $\dim V = n$ und $\dim W = m$. Weiter sei $\Phi \in \mathrm{Hom}(U, V)$ und $\Phi \in \mathrm{Hom}(V, W)$. Dann gilt:

$$A_{\Psi \circ \Phi} = A_\Psi \cdot A_\Phi$$

Satz 67 Seien V, W Vektorräume über $\mathbb{K}$ mit $\dim V = \dim W = n$. Weiter sei $\Phi \in \mathrm{Hom}(V, W)$. Dann gilt:

$$\Phi \text{ ist bijektiv} \qquad \Longleftrightarrow \qquad A_\Phi \in GL(\mathbb{K}, n)$$

In diesem Fall gilt:

$$A_{\Phi^{-1}} = A_\Phi^{-1}$$

Bem. Beachte, daß $A_{\Phi^{-1}}$ Abbildungsmatrix bezüglich der Basis von W und A_Φ^{-1} Abbildungsmatrix bezüglich der Basis von V ist.

Satz 68 Sei V ein $\mathbb{K}$-Vektorraum. $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ und $\tilde{B} = (\tilde{\mathbf{b}}_1, \ldots, \tilde{\mathbf{b}}_n)$ seien Basen von V. Weiter sei

$$\mathbf{b}_j = \sum_{i=1}^{n} s_{ij} \tilde{\mathbf{b}}_i \qquad (j = 1, \ldots, n)$$

die Linearkombination der Basisvektoren aus B durch die Vektoren aus $\tilde{B}$. Ist $\widehat{\mathbf{x}}$ der Koordinatenvektor von $\mathbf{x} \in V$ bezüglich B, dann ist

$$\widehat{\widehat{\mathbf{x}}} = ((s_{ij})) \cdot \widehat{\mathbf{x}}$$

der Koordinantevektor von $\mathbf{x}$ bezüglich $\tilde{B}$.

Bem.

- Die Matrix $S = ((s_{ij})) \in \mathbb{K}^{n \times n}$ ist regulär. Sie heißt *Basiswechselmatrix*
- Sei $\dim V = n, \dim W = m$, $\Phi \in \mathrm{Hom}(V, W)$. $B, \tilde{B}$ seien Basen von V, C, $\tilde{C}$ seien Basen von W. $S \in \mathbb{K}^{n\times n}$ sei die Basiswechsematrix von B nach $\tilde{B}$ und $T \in \mathbb{K}^{m \times m}$ sei die Basiswechselmatrix von C nach $\tilde{C}$. Ist A_Φ die Abbildungsmatrix von Φ bezüglich B und C, so ist

  $$\tilde{A}_\Phi := T^{-1} A_\Phi S$$

  die Abbildungsmatrix von Φ bezüglich $\tilde{B}$ und $\tilde{C}$:

  $$\begin{tikzcd} V\ (B) \arrow[r, "A_\Phi"] \arrow[d, shift right, "S"'] & W\ (C) \arrow[d, shift right, "T"'] \\ V\ (\tilde{B}) \arrow[r, "\tilde{A}_\Phi"] \arrow[u, shift right, "S^{-1}"', "\mathrm{id}_V" near start] & W\ (\tilde{C}) \arrow[u, shift right, "T^{-1}"', "\mathrm{id}_W" near start] \end{tikzcd}$$

Def. 57 Seien $A, B \in \mathbb{K}^{m\times n}$. A und B heißen zueinander *äquivalent* $:\Longleftrightarrow$

$$\exists \quad S \in GL(\mathbb{K}, n),\ T \in GL(\mathbb{K}, m) : \qquad B = T^{-1} A S$$

Ist zusätzlich $m = n$ und $S = T$, so heißen A und B einander *ähnlich*

Bem.

- Äquivalenz und Ähnlichkeit sind Äquivalenzrelationen auf $\mathbb{K}^{m\times n}$.
- Sind $A, B \in \mathbb{K}^{m\times n}$ äquivalent, so läßt sich A durch elementare Zeilenumformungen in B überführen.
- Für $A, B \in \mathbb{K}^{m\times n}$ gilt:

  $$A, B \text{ äquivalent} \quad\Longleftrightarrow\quad \mathrm{Rang}\, A = \mathrm{Rang}\, B$$

- Sind $A, B \in \mathbb{K}^{n\times n}$ ähnlich, dann sind sie auch äquivalent.

18 Determinanten

Def. 58 Sei $A = ((a_{ij})) \in \mathbb{K}^{n\times n}$. Dann heißt

$$\det A := \sum_{\pi \in S_n} (-1)^{F(\pi)} \prod_{i=1}^{n} a_{\pi(i),i} \quad \in \mathbb{K}$$

die *Determinante* von A.

Bem.

- Ist obiger Definition ist S_n die in Paragraph 3 eingeführte Symmetrische Gruppe und $F(\pi)$ die Fehlstandszahl von $\pi \in S_n$.
- Beachte: Determinanten sind nur für quadratische Matrizen definiert.
- Wegen $|S_n| = n!$ ist die Berechnung einer Determinante nach dieser Definition aufwendig.
- Weitere Schreibweisen:

$$|A| := \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} := \det A$$

- Spezielle Determinanten:

  $n = 1:$ $\det A = a_{11}$

  $n = 2:$ $\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11} \cdot a_{22} - a_{21} \cdot a_{12}$

  $n = 3:$ (Regel von Sarrus):

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} \\ -a_{31}a_{22}a_{13} - a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33}$$

- Ist $A = ((a_{ij})) \in \mathbb{K}^{n\times n}$ eine Dreiecksmatrix, so gilt

$$\det A = \prod_{i=1}^{n} a_{ii}.$$

  Damit gilt speziell: $\det I = 1$.

Satz 69 Sei $A \in \mathbb{K}^{n\times n}$. Dann gilt:

$$\det A = \det A^{\top}.$$

Satz 70 Sei $\Delta : (\mathbb{K}^n)^n \to \mathbb{K}$ definiert durch

$$\Delta(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \det(\mathbf{x}_1 | \cdots | \mathbf{x}_n)$$

1. Seien $j \in \{1, \ldots, n\}$, $\mathbf{x}_1, \ldots, \mathbf{x}_n, \tilde{\mathbf{x}}_j \in \mathbb{K}^n$, $a, b \in \mathbb{K}$. Dann gilt:

$$\begin{aligned} & \Delta(\mathbf{x}_1, \ldots, \mathbf{x}_{j-1}, a\mathbf{x}_j + b\tilde{\mathbf{x}}_j, \mathbf{x}_{j+1}, \ldots, \mathbf{x}_n) \\ = \; & a\Delta(\mathbf{x}_1, \ldots, \mathbf{x}_{j-1}, \mathbf{x}_j, \mathbf{x}_{j+1}, \ldots, \mathbf{x}_n) \\ + \; & b\Delta(\mathbf{x}_1, \ldots, \mathbf{x}_{j-1}, \tilde{\mathbf{x}}_j, \mathbf{x}_{j+1}, \ldots, \mathbf{x}_n) \end{aligned}$$

   Diese Eigenschaft heißt *Multilinearität*.

2. Sei $\pi \in S_n$. Dann gilt:

$$\Delta(\mathbf{x}_{\pi(1)}, \ldots, \mathbf{x}_{\pi(n)}) = (-1)^{F(\pi)} \cdot \Delta(\mathbf{x}_1, \ldots, \mathbf{x}_n)$$

3. $\Delta(\mathbf{e}_1, \ldots, \mathbf{e}_n) = 1$

4. Seien $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{K}^n$. Dann gilt:

$$\Delta(\mathbf{x}_1, \ldots, \mathbf{x}_n) = 0 \qquad \Longleftrightarrow \qquad \mathbf{x}_1, \ldots, \mathbf{x}_n \text{ sind linear abhängig}$$

Satz 71 Sei $A \in \mathbb{K}^{n \times n}$. Dann gilt:

1. A ist reguär $\Longleftrightarrow \det A \neq 0$.

2. Geht A durch Vertauschen zweier Zeilen [Spalten] in eine Matrix $\tilde{A}$ über, so gilt $\det A = -\det \tilde{A}$.

3. Geht A durch Multiplikation einer Zeile [Spalte] mit $k \in \mathbb{K} \setminus \{0\}$ in eine Matrix $\tilde{A}$ über, so gilt $k \det A = \det \tilde{A}$.

4. Geht A durch Addition des k-fachen einer Zeile [Spalte] zu einer anderen Zeile [Spalte] in eine Matrix $\tilde{A}$ über, so gilt $\det A = \det \tilde{A}$.

Satz 72 (Entwicklungssatz für Determinanten) Sei $A \in \mathbb{K}^{n \times n}$. Für $i, j = 1, \ldots, n$ sei

$$A_{i,j} := \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn} \end{pmatrix} \in \mathbb{K}^{(n-1)\times(n-1)}.$$

Dann gilt:

$$\det A = \sum_{k=1}^{n} (-1)^{k+j} a_{kj} \det A_{k,j} = \sum_{k=1}^{n} (-1)^{k+j} a_{jk} \det A_{j,k}$$

Satz 73 Seien $A, B \in \mathbb{K}^{n \times n}$. Dann gilt:

$$\det(A \cdot B) = \det A \cdot \det B$$

Bem.

- Ist $A \in GL(\mathbb{K}, n)$, so gilt:
$$\det A^{-1} = \frac{1}{\det A}$$
- Sind $A, B \in \mathbb{K}^{n \times n}$ ähnlich, so gilt
$$\det A = \det B$$
Damit haben für $\Phi \in \mathrm{Hom}(V, W)$ alle Abbildungsmatrizen dieselbe Determinante. Es sei
$$\det \Phi := \det A_\Phi$$
die *Determinante* von Φ.

Satz 74 Sei $A \in GL(\mathbb{K}, n)$ und $B = ((b_{ij})) = A^{-1}$. Dann gilt:
$$b_{ij} = (-1)^{i+j} \frac{\det A_{ji}}{\det A} \qquad (i, j = 1, \ldots, n)$$

19 Eigenwerte

Def. 59 Sei V ein $\mathbb{K}$-Vektorraum und $\Phi \in \mathrm{End}\, V$. $c \in \mathbb{K}$ heißt *Eigenwert* von $\Phi :\Longleftrightarrow$
$$\exists \quad \mathbf{x} \in V \setminus \{ \mathbf{0} \} : \qquad \Phi(\mathbf{x}) = c \cdot \mathbf{x}.$$
In diesem Fall heißt $\mathbf{x}$ *Eigenvektor* von Φ zum Eigenwert c. Ist c ein Eigenwert von Φ, so heißt
$$E_c := \mathrm{Kern}(\Phi - c \cdot \mathrm{id}_V)$$
der *Eigenraum* von Φ bezüglich c. Die Menge
$$\{c \in \mathbb{K} : \quad c \text{ ist Eigenwert von } \Phi\}$$
heißt *Spektrum* von Φ.

Bem.

- Es gilt:
$$E_c = \{ \mathbf{x} \in V : \ \mathbf{x} \text{ ist Eigenvektor zu } c\}$$
- Eigenwerte, Eigenvektoren, Eigenräume und das Spektrum einer Matrix $A \in \mathbb{K}^{n \times n}$ sind definiert durch die Eigenwerte, Eigenvektoren, Eigenräume und das Spektrum der Abbildung
$$\Phi : \mathbb{K}^n \to \mathbb{K}^n, \qquad \Phi(\mathbf{x}) = A \cdot \mathbf{x}$$

- Sind $A, B \in \mathbb{K}^{n\times n}$ einander ähnlich, dann gilt für $c \in \mathbb{K}$:

$$c \text{ ist Eigenwert von } A \quad \Longleftrightarrow \quad c \text{ ist Eigenwert von } B$$

Satz 75 Sei V ein $\mathbb{K}$-Vektorraum und $\Phi \in \operatorname{End} V$. $c_1, \ldots, c_k \in \mathbb{K}$ seien die Eigenwerte von Φ ($c_i \neq c_j$, $i \neq j$). $\mathbf{x}_i$ sei ein Eigenvektor zu c_i ($i = 1, \ldots, n$). Dann gilt:

$$\mathbf{x}_1, \ldots, \mathbf{x}_n \text{ sind linear unabhängig}$$

Satz 76 $A \in \mathbb{K}^{n\times n}$ hat höchstens n Eigenwerte.

Def. 60 Sei $A \in \mathbb{K}^{n\times n}$ Dann heißt

$$p \in \mathbb{K}[x]: \qquad p(x) = \det(A - xI)$$

das *charakteristische Polynom* von A. Ist A Abbildungsmatrix einer linearen Abbildung $\Phi \in \operatorname{End} V$, so heißt p auch das *charakteristische Polynom* von Φ.

Satz 77 Sei $A \in \mathbb{K}^{n\times n}$, $c \in \mathbb{K}$ und p das charakteristische Polynom von A. Dann gilt:

$$c \text{ ist Eigenwert von } A \qquad \Longleftrightarrow \qquad p(c) = 0$$

Ist c Eigenwert von A, so gilt

$$E_c = \{\, \mathbf{x} \in \mathbb{K}^n : \ (A - c \cdot I) \cdot \mathbf{x} \,=\, \mathbf{0} \,\}$$

Bsp. Sei $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \in \mathbb{R}^{2\times 2}$. Dann ist

$$p(x) = \begin{vmatrix} 1-x & 0 \\ 1 & 1-x \end{vmatrix} = (1-x)^2$$

das charakteristische Polynom von A. Damit ist $c = 1$ der einzige Eigenwert von A. Weiter gilt:

$$E_1 = [\begin{pmatrix} 0 \\ 1 \end{pmatrix}]$$

20 Diagonalisierbarkeit

Def. 61 Sei $A \in \mathbb{K}^{n\times n}$. A heißt *diagonalisierbar* $:\Longleftrightarrow$ A ist ähnlich zu einer Matrix $C \in \mathbb{K}^{n\times n}$ der Form

$$C = \begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_{nn} \end{pmatrix}$$

Sei V ein $\mathbb{K}$-Vektorraum und $\Phi \in \operatorname{End} V$. Φ heißt *diagonalisierbar* $:\Longleftrightarrow$ Es gibt eine diagonalisierbare Abbildungsmatrix von Φ.

Bem. Ist $\Phi \in \operatorname{End} V$ diagonalisierbar, so sind alle Abbildungsmatrizen von Φ diagonalisierbar und die Diagonalmatrix ist eindeutig.

Satz 78 Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$ und $\Phi \in \operatorname{End} V$. Dann sind folgende Aussagen äquivalent:

1. Φ ist diagonalisierbar
2. Es gibt eine Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ von V mit $\mathbf{b}_i$ ist Eigenvektor von Φ $(i = 1, \ldots, n)$
3. Für die Eigenräume $E_{c_1}, \ldots, E_{c_n}$ von Φ gilt:
$$V = E_{c_1} \oplus \cdots \oplus E_{c_n}$$
4. Für die Eigenräume $E_{c_1}, \ldots, E_{c_n}$ von Φ gilt:
$$\dim V = \dim E_{c_1} + \cdots + \dim E_{c_n}$$

Bem.

- Analoges gilt für Matrizen $A \in \mathbb{K}^{n \times n}$.
- Ist $\Phi \in \operatorname{End} V, \dim V = n$ [bzw. $A \in \mathbb{K}^{n \times n}$] und hat Φ [bzw. A] n verschiedene Eigenwerte, dann ist Φ [bzw. A] diagonalisierbar.

Satz 79 Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$ und $\Phi \in \operatorname{End} V$. p sei das charakteristische Polynom von Φ. Dann gilt: Φ ist diagonalisierbar $\Longleftrightarrow$ p läßt sich in der Form

$$p(x) = (-1)^n (x - c_1)^{r_1} \cdot \cdots \cdot (x - c_k)^{r_k}$$

schreiben $(r_i \in \mathbb{N},\ c_i \in \mathbb{K},\ (i = 1, \ldots, n),\ c_i \neq c_j\ (i \neq j))$ und es gilt

$$\dim \operatorname{Bild}(\Phi - c_i \mathrm{id}_V) = n - r_i \qquad (i = 1, \ldots, k)$$

Bem. Hat ein Polynom p eine Darstellung

$$p(x) = (-1)^n (x - c_1)^{r_1} \cdot \cdots \cdot (x - c_k)^{r_k},$$

so heißt diese Darstellung *Linearfaktorzerlegung* von p. Darin heißt r_i die *Vielfachkeit* der Nullstelle c_i, $(x - c_i)$ heißt *Linearfaktor.*

Satz 80 ist $A \in \mathbb{K}^{n \times n}$ diagonalisierbar und $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ eine Basis von $\mathbb{K}^n$ mit $A\mathbf{b}_i = c_i \mathbf{b}_i$ $(i = 1, \ldots, k)$, dann gilt für $S = (\mathbf{b}_1 | \cdots | \mathbf{b}_n) \in \mathbb{K}^{n \times n}$:

$$S^{-1}AS = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_n \end{pmatrix}$$

Bem. Die Matrix S aus obigem Satz heißt *Transformationsmatrix* und die Matrix $S^{-1}AS$ ist die Abbildungsmatrix der linearen Abbildung $\Phi : \mathbb{K}^n \to \mathbb{K}^n$, $\Phi(\mathbf{x}) = A\mathbf{x}$ bezüglich der Basis B.

Bsp. Sei $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{K}^{2\times 2}$.

- $\mathbb{K} := \mathbb{R}$. Das charakteristische Polynom $p(x) = x^2 + 1$ läßt sich nicht in Linearfaktoren zerlegen. p hat also keine Nullstellen, damit hat A keine Eigenwerte und A ist nicht diagonalisierbar.

- $\mathbb{K} := \mathbb{C}$. Das charakteristische Polynom p zerfällt in Linearfaktoren:

  $$p(x) = (\mathrm{i} - x)(-\mathrm{i} - x).$$

  Damit sind $-\mathrm{i}, \mathrm{i}$ zwei veschiedene Eigenwerte von A. Wegen $n = 2$ ist damit A diagonalisierbar.

- $\mathbb{K} := \mathbb{F}_2$. Hier gilt:

  $$p(0) = 0 + 1 = 1, \qquad p(1) = 1^2 + 1 = 2 = 0.$$

  Damit ist $c = 1$ einziger Eigenwert von A. Der Eigenraum E_1 hat die Form

  $$E_1 = [\begin{pmatrix} 1 \\ 1 \end{pmatrix}]$$

  Wegen $\dim E_1 = 1$ ist A nicht diagonalisierbar.

21 Satz von Cayley-Hamilton

Def. 62 Es sei V ein $\mathbb{K}$-Vektorraum, $p = (a_0, a_1, \ldots, a_n) \in \mathbb{K}[x]$, $\Phi \in \operatorname{End} V$. Dann sei

$$p(\Phi) := a_0 \mathrm{id}_V + a_1 \Phi + \cdots + a_n \Phi^n$$

Satz 81 (Satz von Cayley-Hamilton) Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$, $\Phi \in \operatorname{End} V$ und p das charakteristische Polynom von Φ. Dann gilt:

$$p(\Phi) = \mathbf{0}$$

Def. 63 Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$, $\Phi \in \operatorname{End} V$.

$$m = (m_0, m_1, \ldots, m_{k-1}, 1, 0, \ldots) \in \mathbb{K}[x]$$

sei das Polynom kleinsten Grades mit $m(\Phi) = \mathbf{0}$. Dann heißt m *Minimalpolynom* von Φ.

Bem.

- m ist bis auf Normierung eindeutig. Es gilt $m \neq 0$.

- Sind $A, B \in \mathbb{K}^{n\times n}$, ist m das Minimalpolynom von A und $\tilde{m}$ das Minimalpolynom von B, dann gilt:

  $$A, B \text{ sind ähnlich} \quad \Longleftrightarrow \quad m = \tilde{m}$$

Satz 82 Sei V ein $\mathbb{K}$-Vektorraum, $\Phi \in \operatorname{End} V$, m das Minimalpolynom von Φ und $q \in \mathbb{K}[x]$ mit $q(\Phi) = \mathbf{0}$. Dann gilt $m \mid q$.

Bem.

- Insbesondere teilt m das charakteristische Polynom von Φ.
- Polynome q mit $q(\Phi) = \mathbf{0}$ heißen *annullierend.*
- Für das charakteristische Polynom p gilt:

$$\forall \quad x_0 \in \mathbb{K}: \qquad m(x_0) = 0 \quad \Longleftrightarrow \quad p(x_0) = 0$$

Bsp. Sei $\Phi : \mathbb{R}^3 \to \mathbb{R}^3$, $\Phi(\mathbf{x}) = A\mathbf{x}$ mit

$$A = \begin{pmatrix} 7 & -6 & 11 \\ 0 & 1 & -1 \\ -4 & 4 & 7 \end{pmatrix}.$$

$p = -(x-1)^2(x+1)$ ist das charakteristische Polynom von A. Weil das Minimalpolynom p teilen muß, bleiben für m nur die Möglichkeiten

$$m = (x-1)(x+1) \qquad \text{oder} \qquad m = (x-1)^2(x+1)$$

Wegen

$$(A-I)(A+I) = \begin{pmatrix} 6 & -6 & 11 \\ 0 & 0 & -1 \\ -4 & 4 & -8 \end{pmatrix} \cdot \begin{pmatrix} 8 & -6 & 11 \\ 0 & 2 & -1 \\ -4 & 4 & -6 \end{pmatrix} \neq \mathbf{0}$$

ist $m = (x-1)^2(x+1)$.

22 Jordan-Normalform

Satz 83 Sei V ein $\mathbb{K}$-Vektorraum, $\Phi \in \operatorname{End} V$, $q \in \mathbb{K}[x]$. Dann gilt:

1. $\operatorname{Kern} q(\Phi)$ ist ein Φ-invarianter Untervektorraum von V, d.h.:

$$\forall \quad \mathbf{x} \in \operatorname{Kern} q(\Phi): \qquad \Phi(\mathbf{x}) \in \operatorname{Kern} q(\Phi)$$

2. Ist $r \in \mathbb{K}[x]$ mit $q \mid r$, dann gilt:

$$\operatorname{Kern} q(\Phi) \subseteq \operatorname{Kern} r(\Phi)$$

3. Ist $r \in \mathbb{K}[x]$ teilerfremd zu q, dann gilt:

$$\operatorname{Kern}(q \cdot r)(\Phi) = \operatorname{Kern} q(\Phi) \oplus \operatorname{Kern} r(\Phi)$$

Satz 84 Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$, $\Phi \in \operatorname{End} V$, $q \in \mathbb{K}[x]$ anullierend und

$$q = q_1 \cdot \dots \cdot q_k$$

eine Zerlegung von q in paarweise teilerfremde Faktoren $q_i \in \mathbb{K}[x]$ $(i = 1, \dots, k)$. Dann gilt: Die Untervektorräume

$$U_i := \operatorname{Kern} q_i(\Phi) \qquad (i = 1, \dots, k)$$

sind Φ-invariant, es gilt

$$V = U_1 \oplus \cdots \oplus U_k$$

und sind A_i die Abbildungsmatrizen von $\Phi|_{U_i}$ $(i = 1, \ldots, k)$, so gibt es eine Basis B von V, zu der die Abbildungsmatrix A_Φ von der Form

$$A = \begin{pmatrix} \boxed{A_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \boxed{A_k} \end{pmatrix}$$

ist.

Satz 85 Es sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$, $\Phi \in \operatorname{End} V$. Dann gilt: Φ ist diagonalisierbar $\Longleftrightarrow$ Das Minimalpolynom m hat die Form

$$m = (x - c_1) \cdot \cdots \cdot (x - c_k)$$

Def. 64 Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$, $\Phi \in \operatorname{End} V$. $c \in \mathbb{K}$ sei Eigenwert von Φ, $s \in \mathbb{N}$ sei die Vielfachheit der Nullstelle c im Minimalpolynom von Φ. Dann heißt

$$H_c := \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^s$$

der *Hauptraum* zu c. s heißt dann der *Index* von H_c.

Bem.

- Ist r die Vielfachheit der Nullstelle c im charakteristischen Polynom, so gilt

  $$H_c = \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^s = \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^r$$

- Es gilt $\dim H_c = r$ und

  $$p = (c - x)^r$$

  ist das charakteristische Polynom von $\Phi|_{H_c}$.

Satz 86 Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$, $\Phi \in \operatorname{End} V$, c Eigenwert von Φ. Dann gilt: s ist Index von H_c $\Longleftrightarrow$

$$s = \min_{n \in \mathbb{N}} \{\operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^n = \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^{n+1}\}$$

Bem.

- Analog gilt: s ist Index von H_c

  $$\begin{aligned} &\Longleftrightarrow \quad s = \min_{n \in \mathbb{N}} \{\dim \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^n = \dim \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^{n+1}\} \\ &\Longleftrightarrow \quad s = \min_{n \in \mathbb{N}} \{\dim \operatorname{Bild}(\Phi - c \cdot \mathrm{id}_V)^n = \dim \operatorname{Bild}(\Phi - c \cdot \mathrm{id}_V)^{n+1}\} \\ &\Longleftrightarrow \quad s = \min_{n \in \mathbb{N}} \{\operatorname{Rang}(\Phi - c \cdot \mathrm{id}_V)^n = \operatorname{Rang}(\Phi - c \cdot \mathrm{id}_V)^{n+1}\} \end{aligned}$$

- Ist $H_c = V$, so gilt:

$$s = \min_{n \in \mathbb{N}} \{ (\Phi - c \cdot \mathrm{id}_V)^n = \mathbf{0} \}$$

Def. 65 Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$, $\Phi \in \operatorname{End} V$, c sei Eigenwert von Φ. Dann heißt $A \in \mathbb{K}^{m \times m}$ mit

$$A = \begin{pmatrix} c & 0 & \cdots & \cdots & 0 \\ 1 & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & c \end{pmatrix}$$

JORDAN-*Kästchen* der Länge m zum Eigenwert c. Ist s der Index des Hauptraumes H_c, so heißt B mit

$$B = \begin{pmatrix} \boxed{A_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \boxed{A_k} \end{pmatrix}$$

JORDAN-*Block* zum Eigenwert c. Dabei sind $A_1, \ldots, A_k$ JORDAN-Kästchen, und zwar je

$2 \dim \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^l - \dim \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^{l+1} - \dim \operatorname{Kern}(\Phi - c \cdot \mathrm{id}_V)^{l-1}$

Kästchen der Länge l ($l = 1, \ldots, s$).

Satz 87 (JORDAN-Normalform) Sei V ein $\mathbb{K}$-Vektorraum, $\dim V = n$ und $\Phi \in \operatorname{End} V$.

$$p(x) = (-1)^n (x - c_1)^{r_1} \cdot \cdots \cdot (x - c_k)^{r_k} \qquad (c_i \neq c_j,\ i \neq j)$$

sei das charakteristische Polynom und

$$m(x) = (x - c_1)^{s_1} \cdot \cdots \cdot (x - c_k)^{s_k}$$

das Minimalpolynom von Φ. Weiter sei A_{c_i} JORDAN-Block zum Eigenwert c_i ($i = 1, \ldots, k$). Dann gibt es eine Basis B von V, bezüglich der die Abbildungsmatrix A_Φ die Form

$$A_\Phi = \begin{pmatrix} \boxed{A_{c_1}} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \boxed{A_{c_k}} \end{pmatrix}$$

hat. Weiter gilt: Im JORDAN-Block A_{c_i} zum Eigenwert c_i treten insgesamt E_{c_i} JORDAN-Kästchen auf. Mindestens eines davon hat die Länge s_i, keines ist länger.

Bem.

- A_Φ heißt JORDAN-*Normalform* von Φ, B heißt JORDAN-*Basis* von Φ. A_Φ ist bis auf die Reihenfolge der JORDAN-Kästchen eindeutig.

- Bestimmung der JORDAN-Basis: Setze

$$U_0 := \{\mathbf{0}\}, \qquad U_j := \mathrm{Kern}(\Phi - c \cdot \mathrm{id}_V)^j \quad (j = 1, \ldots, s).$$

Stelle H_c als direkte Summe dar durch:

$$\begin{array}{ccccccccccc} H_c = & U_{s-1} & \oplus & W_1 & & & & & & & \\ & U_{s-1} & = & U_{s-2} & \oplus & W_2 & & & & & \\ & & & U_{s-2} & = & U_{s-3} & \oplus & W_3 & & & \\ & & & & & & \ddots & \ddots & \ddots & & \\ & & & & & & & U_2 & = & E_c \oplus & W_{s-1} \end{array}$$

Sei $B_1 = (\mathbf{b}^1_1, \ldots, \mathbf{b}^1_{q_1})$ eine Basis von W_1. Als Basis von W_2 wird

$$B_2 = (\mathbf{b}^2_1, \ldots, \mathbf{b}^2_{q_1})$$

mit

$$\mathbf{b}^2_i := (\Phi - c \cdot \mathrm{id}_V)(\mathbf{b}^1_i) \qquad (i = 1, \ldots, q_1)$$

gewählt. Als Basis von W_3 wird

$$B_3 := (\mathbf{b}^3_1, \ldots, \mathbf{b}^3_{q_3})$$

mit

$$\mathbf{b}^3_i := (\Phi - c \cdot \mathrm{id}_V)(\mathbf{b}^2_i) \qquad (i = 1, \ldots, q_2)$$

gewählt, usw. Wir erhalten für die Ergänzungsräume W_i folgende Basen:

$$\begin{array}{lllllllll} B_1 = (\mathbf{b}^1_1, & \mathbf{b}^1_2, \ldots, & \mathbf{b}^1_{q_1}) & & & & & & \\ \downarrow & \downarrow & \downarrow & & & & & & \\ B_2 = (\mathbf{b}^2_1, & \mathbf{b}^2_2, \ldots, & \mathbf{b}^2_{q_1}, & \mathbf{b}^2_{q_1+1}, \ldots, & \mathbf{b}^2_{q_2}) & & & & \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & & & & \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & & & \\ B_s = (\mathbf{b}^s_1, & \mathbf{b}^s_2, \ldots, & \mathbf{b}^2_{q_1}, & \mathbf{b}^s_{q_1+1}, \ldots & \mathbf{b}^s_{q_2}, & \mathbf{b}^s_{q_2+1}, \ldots, & \mathbf{b}^s_{q_{s-1}+1}, \ldots, & \mathbf{b}^s_{q_s}) \end{array}$$

Die Anordung der Vektoren entlang der Pfeile, also

$$B := (\mathbf{b}^1_1, \mathbf{b}^2_1, \ldots, \mathbf{b}^s_1, \mathbf{b}^1_2, \ldots\ldots)$$

ist die JORDAN-Basis.

Bsp.

- Sei $B = (\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$ eine Basis von V, $\Phi \in \operatorname{End} V$ definiert durch

$$\begin{array}{rcrcrcr} \Phi(\mathbf{b}_1) & := & 3\mathbf{b}_1 & - & \mathbf{b}_2 & + & \mathbf{b}_3 \\ \Phi(\mathbf{b}_2) & := & 4\mathbf{b}_1 & & & + & 2\mathbf{b}_3 \\ \Phi(\mathbf{b}_3) & := & 3\mathbf{b}_1 & - & \mathbf{b}_2 & + & 3\mathbf{b}_3 \end{array}$$

Bezüglich B hat Φ die Abbildungsmatrix

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

$p(x) = -(x-2)^3$ ist das charakteristische Polynom und $m(x) = (x-2)^3$ das Minimalpolynom von Φ. Es gilt

$$\dim E_2 = 3 - \operatorname{Rang}(A - 2I) = 3 - 2 = 1$$

Da Φ nur einen Eigenwert hat, hat die JORDAN-Normalform von Φ nur einen JORDAN-Block. Wegen $\dim E_2 = 1$ enthält der JORDAN-Block nur ein JORDAN-Kästchen. Seine Länge muß maximal sein (also 3, dies deckt sich mit der Vielfachheit der Nullstelle im Minimalpolynom). Damit ist

$$A_\Phi = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

die JORDAN-Normalform von A. Gesucht ist nun die JORDAN-Basis $\tilde{B}$.

$$\begin{array}{rcl} U_3 & := & \operatorname{Kern}(\Phi - 2\cdot \mathrm{id}_V)^3 = H_c = V \\ U_2 & := & \operatorname{Kern}(\Phi - 2\cdot \mathrm{id}_V)^2 \\ U_1 & := & \operatorname{Kern}(\Phi - 2\cdot \mathrm{id}_V) = E_2 \end{array}$$

Es gilt:

$$\begin{array}{rcll} U_2 & = & [\mathbf{b}_1, \mathbf{b}_2 - \mathbf{b}_3], & q_2 := \dim U_2 = 2 \\ U_1 & = & [\mathbf{b}_1 - \mathbf{b}_2 + \mathbf{b} - 3], & q_1 := \dim U_1 = 1 \end{array}$$

Mit $W_1 = [\mathbf{b}_2]$ ergibt sich

$$U_3 = U_2 \oplus W_1.$$

Damit folgt für $W_2 := [(\Phi - 2\mathrm{id}_V)(\mathbf{b}_2)] = [4\mathbf{b}_1 - 2\mathbf{b}_2 + 2\mathbf{b}_3]$:

$$U_2 = U_1 \oplus W_2.$$

Es ist $((\Phi - 2\mathrm{id}_V)^2(\mathbf{b}_2)) = (2\mathbf{b}_1 - 2\mathbf{b}_2 + 2\mathbf{b}_3)$ Basis von $U_1 = E_2$. Damit sind

$$\begin{array}{rcl} B_1 & = & (\mathbf{b}_2) \\ B_2 & = & (4\mathbf{b}_1 - 2\mathbf{b}_2 + 2\mathbf{b}_3) \\ B_3 & = & (2\mathbf{b}_1 - 2\mathbf{b}_2 + 2\mathbf{b}_3) \end{array}$$

die Basen der Ergänzungsräume. Damit ist

$$\tilde{B} := (\mathbf{b}_2, 4\,\mathbf{b}_1 - 2\,\mathbf{b}_2 + 2\,\mathbf{b}_3, 2\,\mathbf{b}_1 - 2\,\mathbf{b}_2 + 2\,\mathbf{b}_3)$$

die JORDAN-Basis. Bezüglich dieser Basis hat Φ also die Abbildungsmatrix $\tilde{A}$. Insbesondere ist

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

die Basiswechselmatrix. Probe:

$$\begin{aligned} S^{-1}AS &= \begin{pmatrix} 0 & 1 & 1 \\ \frac{1}{2} & 0 & -\frac{1}{2} \\ -\frac{1}{2} & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 4 & 3 \\ -1 & 0 & -1 \\ 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 4 & 2 \\ 1 & -2 & -2 \\ 0 & 2 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix} = \tilde{A}. \end{aligned}$$

- Sei $A \in \mathbb{R}^{12\times 12}$ mit $p = (2-x)^{12}$ als charakteristisches Polynom. Es gelte:

$$\begin{array}{ll} \text{Rang}(A-2I) = 7 & \text{Rang}(A-2I)^2 = 4 \\ \text{Rang}(A-2I)^3 = 2 & \text{Rang}(A-2I)^4 = 0 \end{array}$$

Durch diese Informationen ist die JORDAN-Normalform von A festgelegt: $c = 2$ ist 12-facher Eigenwert von p. Damit ist $H_c = \mathbb{R}^{12} = V$. Aus $\text{Rang}(A-2I)^4 = 0$ folgt $s = 4$, also ist

$$m(x) = (x-2)^4$$

das Minimalpolynom von A. Weiter gilt:

$$E_2 = U_1 \subset U_2 \subset U_3 \subset U_4 = H_c$$

Für die Dimensionen der Räume gilt:

$$\begin{aligned} \dim U_1 &= 12 - 7 = 5 \\ \dim U_2 &= 12 - 4 = 8 \\ \dim U_3 &= 12 - 2 = 10 \\ \dim U_4 &= 12. \end{aligned}$$

Wegen $\dim E_2 = 5$ gibt es 5 JORDAN-Kästchen, nämlich:

$$2\dim U_4 - \dim U_5 - \dim U_3 = 24 - 12 - 10 = 2$$

Kästchen der Länge 4,

$$2\dim U_3 - \dim U_4 - \dim U_2 = 20 - 12 - 8 = 0$$

Kästchen der Länge 3,

$$2\dim U_2 - \dim U_3 - \dim U_1 = 16 - 10 - 5 = 1$$

Kästchen der Länge 2 und

$$2 \dim U_1 - \dim U_2 - \dim U_0 = 10 - 8 - 0 = 2$$

Kästchen der Länge 1. Damit ist

$$\tilde{A} = \begin{pmatrix} 2 & 0 & 0 & 0 & & & & & & & & \\ 1 & 2 & 0 & 0 & & & & & & & & \\ 0 & 1 & 2 & 0 & & & & & & & & \\ 0 & 0 & 1 & 2 & & & & & & & & \\ & & & & 2 & 0 & 0 & 0 & & & & \\ & & & & 1 & 2 & 0 & 0 & & & & \\ & & & & 0 & 1 & 2 & 0 & & & & \\ & & & & 0 & 0 & 1 & 2 & & & & \\ & & & & & & & & 2 & 0 & & \\ & & & & & & & & 1 & 2 & & \\ & & & & & & & & & & 2 & \\ & & & & & & & & & & & 2 \end{pmatrix}$$

die JORDAN-Normalform von A.

23 Skalarprodukte

Def. 66 Sei V ein $\mathbb{R}$-Vektorraum und $\beta : V \times V \to \mathbb{R}$ eine Abbildung mit:

1. $\forall \quad a, b \in \mathbb{R},\ \mathbf{x}, \mathbf{y}, \mathbf{z} \in V : \quad \beta(\mathbf{x}, a\mathbf{y} + b\mathbf{z}) = a\beta(\mathbf{x}, \mathbf{y}) + b\beta(\mathbf{x}, \mathbf{z})$
2. $\forall \quad \mathbf{x}, \mathbf{y} \in V : \qquad \beta(\mathbf{x}, \mathbf{y}) = \beta(\mathbf{y}, \mathbf{x})$
3. $\forall \quad \mathbf{x} \in V \setminus \{\mathbf{0}\} : \qquad \beta(\mathbf{x}, \mathbf{x}) > 0$

Dann heißt β *Skalarprodukt* (oder *inneres Produkt*) auf V. Schreibweise:

$$\beta(\mathbf{x}, \mathbf{y}) =: \langle \mathbf{x}, \mathbf{y} \rangle$$

Ist $\langle \cdot, \cdot \rangle$ ein Skalarprodukt auf V, so heißt $(V, \langle \cdot, \cdot \rangle)$ EUKLID*ischer* Vektorraum (oder *Vektorraum* mit Skalarprodukt*)*

Bem.

- Skalarprodukte können allgemeiner auf allen total geordneten Körpern definiert werden. Die folgenden Sätze gelten dann analog.
- Ein Skalarprodukt β ist linear in beiden Komponenten. Eine solche Abbildung heißt *multilinear.* Eigenschaft (2) heißt *Symmetrie* und Eigenschaft (3) heißt *Positiv-Definitheit.* Ein Skalarprodukt ist damit eine symmetrische, positiv definite, 2-fach multilineare Abbildung $V \times V \to \mathbb{R}$.

Bsp.

- Sei $V = \mathbb{R}^n$. Dann ist durch

$$\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{i=1}^{n} x_i y_i$$

für $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n$ ein Skalarprodukt definiert. Dieses Skalarprodukt heißt *Standardskalarprodukt.* Ist in einem EUKLIDischen Vektorraum kein Skalarprodukt angegeben, so ist dieses gemeint.

- Auf $V = \mathbb{R}^2$ wird für $\mathbf{x} = (x_1, x_2)$ und $\mathbf{y} = (y_1, y_2)$ durch

$$\langle \mathbf{x}, \mathbf{y} \rangle := x_1 y_1 - (x_1 y_2 + x_2 y_1) + 2 x_2 y_2$$

ein Skalarprodukt definiert.

- Sei $V = C([a, b])$. Für jedes (feste) $s \in V$ wird durch

$$\langle g, h \rangle := \int_a^b g(t) h(t) s(t) dt \qquad (g, h \in V)$$

ein Skalarprodukt erklärt. s heißt *Gewichtsfunktion.*

Def. 67 Sei V ein $\mathbb{R}$-Vektorraum, $\langle \cdot, \cdot \rangle$ ein Skalarprodukt auf V. $\mathbf{x}, \mathbf{y} \in V$ heißen zueinander *orthogonal* $:\Longleftrightarrow$

$$\langle \mathbf{x}, \mathbf{y} \rangle = 0$$

Schreibweise in diesem Fall: $\mathbf{x} \perp \mathbf{y}$. $A, B \subseteq V$ heißen *orthogonal* $:\Longleftrightarrow$

$$\forall \quad \mathbf{x} \in A, \mathbf{y} \in B : \qquad \mathbf{x} \perp \mathbf{y}.$$

Schreibweise in diesem Fall: $A \perp B$. Statt $\{\mathbf{x}\} \perp B$ schreibt man auch $\mathbf{x} \perp B$. Für $A \subseteq V$ heißt

$$A^{\perp} := \{\mathbf{x} \in V : \mathbf{x} \perp A\}$$

das *orthogonale Komplement* von A.

Bem. Für $A \subseteq V$ gilt:

- $A^{\perp}$ ist Untervektorraum von V.
- $A^{\perp} = [A]^{\perp} = [A^{\perp}]$.
- $A^{\perp} \cap [A] = \{\mathbf{0}\}$
- $[A] \subseteq (A^{\perp})^{\perp}$

Def. 68 Sei V ein $\mathbb{R}$-Vektorraum. Eine Abbildung $\|\cdot\| : V \to \mathbb{R}$ mit

1. $\forall \quad \mathbf{x} \in V : \qquad \|\mathbf{x}\| \geq 0$ und $\|\mathbf{x}\| = 0 \Longleftrightarrow \mathbf{x} = \mathbf{0}$
2. $\forall \quad \mathbf{x} \in V, c \in \mathbb{R} : \qquad \|c\mathbf{x}\| = |c| \|\mathbf{x}\|$

3. $\forall \quad \mathbf{x}, \mathbf{y} \in V: \qquad \|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$

heißt *Norm* (oder *Länge*) auf V.

Bem.

- Ist $\langle \cdot, \cdot \rangle$ ein Skalarprodukt auf V, so wird durch

$$\|\mathbf{x}\| := \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} \qquad (\mathbf{x} \in V)$$

  eine Norm definiert.

- Eigenschaft (3) in obiger Definition bezeichnet man auch als *Dreiecksungleichung*.

- Die Abbildung

$$d : V \times V \to \mathbb{R}, \qquad d(\mathbf{x}, \mathbf{y}) := \|\mathbf{x} - \mathbf{y}\|$$

  heißt *Metrik* auf V. Für $\mathbf{x}, \mathbf{y} \in V$ heißt $d(\mathbf{x}, \mathbf{y})$ der *Abstand* (oder die *Distanz*) zwischen $\mathbf{x}$ und $\mathbf{y}$.

Satz 88 Sei V ein $\mathbb{R}$-Vektorraum, $\langle \cdot, \cdot \rangle$ ein Skalarprodukt und $\|\cdot\|$ die zum Skalarprodukt $\langle \cdot, \cdot \rangle$ gehörige Norm. Dann gilt:

1. die Cauchy-Schwarzsche Ungleichung:

$$\forall \quad \mathbf{x}, \mathbf{y} \in V: \qquad |\langle \mathbf{x}, \mathbf{y} \rangle| \leq \|\mathbf{x}\| \cdot \|\mathbf{y}\|,$$

   und $|\langle \mathbf{x}, \mathbf{y} \rangle| = \|\mathbf{x}\| \cdot \|\mathbf{y}\| \iff \mathbf{x}, \mathbf{y}$ linear abhängig.

2. die *Parallelogrammidentität*:

$$\forall \quad \mathbf{x}, \mathbf{y} \in V: \qquad \|\mathbf{x} + \mathbf{y}\|^2 + \|\mathbf{x} - \mathbf{y}\|^2 = 2\|\mathbf{x}\|^2 + 2\|\mathbf{y}\|^2$$

3. $4\langle \mathbf{x}, \mathbf{y} \rangle = \|\mathbf{x} + \mathbf{y}\|^2 - \|\mathbf{x} - \mathbf{y}\|^2$

Bem. Eine Norm $\|\cdot\|$ wird genau dann von einem Skalarprodukt induziert, wenn die Parallelogrammgleichung erfüllt ist. In diesem Fall wird das Skalarprodukt durch Eigenschaft (3) eindeutig festgelegt.

Def. 69 Sei V ein $\mathbb{R}$-Vektorraum, $\langle \cdot, \cdot \rangle$ ein Skalarprodukt auf V, $\|\cdot\|$ die zu $\langle \cdot, \cdot \rangle$ gehörige Norm. Die Zahl $\omega \in [0, \pi]$ mit

$$\cos \omega = \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{\|\mathbf{x}\| \cdot \|\mathbf{y}\|} \qquad (\mathbf{x}, \mathbf{y} \in V \setminus \{\mathbf{0}\})$$

heißt *Winkel* zwischen $\mathbf{x}$ und $\mathbf{y}$.

Bem.

- Für je zwei Vektoren $\mathbf{x}, \mathbf{y} \in V \setminus \{\mathbf{0}\}$ ist ω eindeutig festgelegt.

- Sind $\mathbf{x}, \mathbf{y}$ zueinander orthogonal, so ist $\omega = \frac{\pi}{2}$ der Winkel zwischen $\mathbf{x}$ und $\mathbf{y}$.

Def. 70 Die Menge

$$l^2 := \{(a_n)_{n=0}^{\infty} \in \mathbb{R}^{\mathbb{N}_0} : \sum_{n=0}^{\infty} a_n^2 < \infty\}$$

heißt *Standard*-HILBERT-*Raum*.

Bem.

- l^2 ist ein Untervektorraum von $\mathbb{R}^{\mathbb{N}_0}$ und $\mathbb{R}[x]$ ist ein Untervektorraum von l^2.
- Für $\mathbf{x} = (x_0, x_1, \ldots)$, $\mathbf{y} = (y_0, y_1, \ldots) \in l^2$ wird durch

$$\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{n=0}^{\infty} x_n y_n$$

ein Skalarprodukt auf l^2 definiert.

Def. 71 Sei $A \in \mathbb{R}^{n \times n}$. A heißt *positiv definit* $:\Longleftrightarrow$

$$\forall \quad \mathbf{x} \in \mathbb{R}^n \setminus \{\mathbf{0}\} : \qquad \mathbf{x}^\top A \mathbf{x} > 0$$

Satz 89 Sei V ein $\mathbb{R}$-Vektorraum, $\dim V = n$, B eine geordnete Basis von V. Dann gilt: $\beta : V \times V \to \mathbb{R}$ ist ein Skalarprodukt $\Longleftrightarrow$

$$\exists \quad A \in \mathbb{R}^{n \times n} \quad \forall \quad \mathbf{x}, \mathbf{y} \in V : \qquad \beta(\mathbf{x}, \mathbf{y}) = \mathbf{x}^\top A \mathbf{y}.$$

Satz 90 Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch. Dann gilt:

1. A ist diagonalisierbar.
2. Sind c_1, c_2 Eigenwerte von A ($c_1 \neq c_2$) und ist $\mathbf{x}_1$ Eigenvektor zu c_1 und $\mathbf{x}_2$ Eigenvektor zu c_2, so gilt: $\mathbf{x}_1 \perp \mathbf{x}_2$.

Satz 91 Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch. Dann gilt: A ist positiv definit $\Longleftrightarrow$ Alle Eigenwerte von A sind positiv.

Satz 92 Sei $A = ((a_{ij})) \in \mathbb{R}^{n \times n}$ symmetrisch. Dann sind folgende Aussagen äquivalent:

1. A ist positiv definit.
2. $\exists \quad B \in GL(\mathbb{R}, n) : \qquad A = B^\top B$.
3. Für $k = 1, \ldots, n$ gilt:

$$\begin{vmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{kk} \end{vmatrix}$$

Bem.

- Die Darstellung $B^\top B$ aus (2) heißt CHOLESKY-*Zerlegung* von A.
- Die Determinanten aus (3) heißen *Hauptminoren* von A.

24 Orthonormalbasen

Def. 72 Sei V ein EUKLIDischer Vektorraum und $A \subseteq V$. A heißt *Orthogonalsystem* $:\Longleftrightarrow$

1. $\mathbf{0} \notin A$
2. $\forall \quad \mathbf{x}_1, \mathbf{x}_2 \in A,\ \mathbf{x}_1 \neq \mathbf{x}_2 : \qquad \mathbf{x}_1 \perp \mathbf{x}_2.$

Gilt zusätzlich

$$\forall \quad \mathbf{x} \in A : \qquad \|\mathbf{x}\| = 1,$$

so heißt A *Orthonormalsystem.* Sei B Basis von V.

1. B heißt *Orthogonalbasis* $:\Longleftrightarrow$ B ist Orthogonalsystem.
2. B heißt *Orthonormalbasis* (ONB) $:\Longleftrightarrow$ B ist Orthonormalsystem.

Bem. Ist $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ Basis von V, dann gilt:

$$B \text{ ist Orthonormalbasis} \qquad \Longleftrightarrow \qquad \langle \mathbf{b}_i, \mathbf{b}_j \rangle = \delta_{ij} \quad (i, j = 1, \ldots, n)$$

Satz 93 Sei V ein EUKLIDischer Vektorraum, $A \subseteq V$ sei ein Orthogonalsystem. Dann gilt: A ist linear unabhängig.

Satz 94 Sei V ein endlich dimensionaler EUKLIDischer Vektorraum. Dann existiert eine Orthonormalbasis von V.

Bem. Ist $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ eine Basis von V, dann gewinnt man eine Orthonormalbasis mit Hilfe des GRAM-SCHMITT*schen Orthogonalisierungsverfahrens*: Setze

$$\begin{aligned}
\tilde{\mathbf{b}}_1 &:= \mathbf{b}_1, \\
\tilde{\mathbf{b}}_2 &:= \mathbf{b}_2 - \frac{\langle \mathbf{b}_2, \tilde{\mathbf{b}}_1 \rangle}{\|\tilde{\mathbf{b}}_1\|^2} \cdot \tilde{\mathbf{b}}_1, \\
&\vdots \qquad \vdots \\
\tilde{\mathbf{b}}_n &:= \mathbf{b}_n - \sum_{i=1}^{n-1} \frac{\langle \mathbf{b}_n, \tilde{\mathbf{b}}_i \rangle}{\|\tilde{\mathbf{b}}_i\|^2} \cdot \tilde{\mathbf{b}}_i.
\end{aligned}$$

Dann ist

$$\tilde{B} := \left(\frac{\tilde{\mathbf{b}}_1}{\|\tilde{\mathbf{b}}_1\|}, \ldots, \frac{\tilde{\mathbf{b}}_n}{\|\tilde{\mathbf{b}}_n\|}\right)$$

eine Orthonormalbasis von V. Wendet man dieses Verfahren auf ein Erzeugendensystem von V an, so bilden alle Vektoren $\tilde{\mathbf{b}}_i \neq \mathbf{0}$ eine Orthonormalbasis von V.

Satz 95 Sei V ein EUKLIDischer Vektorraum und $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ eine Orthonormalbasis von V. Dann gilt:

1. $\forall \quad \mathbf{x} \in V: \qquad \mathbf{x} = \sum_{i=1}^{n} \langle \mathbf{x}, \mathbf{b}_i \rangle \mathbf{b}_i$

2. $\forall \quad \mathbf{x}, \mathbf{y} \in V: \qquad \langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} \langle \mathbf{x}, \mathbf{b}_i \rangle \cdot \langle \mathbf{y}, \mathbf{b}_i \rangle$

Bem. Ist V ein EUKLIDischer Vektorraum und $A \subseteq V$ ein Orthonormalsystem, dann gilt die BESSEL*sche Ungleichung*:

$$\forall \quad \mathbf{x} \in V: \qquad \|\mathbf{x}\|^2 \geq \sum_{\mathbf{y} \in A} \langle \mathbf{x}, \mathbf{y} \rangle^2$$

Das Orthonormalsystem A heißt *vollständig*, wenn die PARSEVALL*sche Gleichung* gilt:

$$\forall \quad \mathbf{x} \in V: \qquad \|\mathbf{x}\|^2 = \sum_{\mathbf{y} \in A} \langle \mathbf{x}, \mathbf{y} \rangle^2$$

25 Orthogonalprojektionen

Def. 73 Sei V ein EUKLIDischer Vektorraum. Eine Projektion $\pi \in \operatorname{End} V$ heißt *Orthogonalprojektion* $:\Longleftrightarrow$

$$\forall \quad \mathbf{x} \in V: \qquad (\pi(\mathbf{x}) - \mathbf{x}) \perp \pi(\mathbf{x})$$

In diesem Fall heißt $\pi(\mathbf{x})$ *Orthogonalprojektion* von $\mathbf{x}$ auf $\operatorname{Bild} \pi$.

Bem. Für eine Projektion $\pi \in \operatorname{End} V$ gilt:

$$\pi \text{ ist Orthogonalprojektion} \qquad \Longleftrightarrow \qquad \operatorname{Kern} \pi \perp \operatorname{Bild} \pi.$$

Satz 96 Sei V ein EUKLIDischer Vektorraum und U ein Untervektorraum von V. Es gilt: Es gibt eine Orthogonalprojektion π auf $U \Longleftrightarrow V = U \oplus U^\perp$. In diesem Fall ist π durch U eindeutig bestimmt und es gilt $U = (U^\perp)^\perp$.

Satz 97 Sei V ein EUKLIDischer Vektorraum und U ein endlich dimensionaler Untervektorraum von V. Dann existiert die Orthogonalprojektion π auf U und es gilt $V = U \oplus U^\perp$.

Satz 98 Sei V ein EUKLIDischer Vektorraum, U ein Untervektorraum von V und $\pi \in \operatorname{End} V$ mit $\operatorname{Bild} \pi \subseteq U$. Dann gilt: π ist Orthogonalprojektion auf U $\Longleftrightarrow$

$$\forall \quad \mathbf{x} \in V \quad \forall \quad \mathbf{y} \in U: \qquad \|\mathbf{x} - \pi(\mathbf{x})\| \leq \|\mathbf{x} - \mathbf{y}\|$$

Bem. Ist π Orthogonalprojektion auf U, so heißt

$$d(\mathbf{x}, U) := \|\mathbf{x} - \pi(\mathbf{x})\|$$

der *Abstand* (oder die *Distanz*) von $\mathbf{x}$ zu U. Allgemeiner: Sind $A, B \subseteq U$, so heißt

$$d(A, B) := \inf_{\substack{\mathbf{x} \in A \\ \mathbf{y} \in B}} \|\mathbf{x} - \mathbf{y}\|$$

der *Abstand* (oder die *Distanz*) von A zu B. Diese Definition stimmt mit der obigen überein.

26 Adjungierte Abbildungen

Def. 74 Seien V, W endlich dimensionale Vektorräume. $\Phi \in \mathrm{Hom}(V, W)$ und $\Psi \in \mathrm{Hom}(W, V)$ heißen zueinander *adjungiert* $:\Longleftrightarrow$

$$\forall \quad \mathbf{x} \in V \quad \forall \quad \mathbf{y} \in W: \qquad \langle \Phi(\mathbf{x}), \mathbf{y} \rangle = \langle \mathbf{x}, \Psi(\mathbf{y}) \rangle$$

Bem.

- Beachte, daß in obiger Definition links das Skalarprodukt in V und rechts das Skalarprodukt in W steht.
- Zu $\Phi \in \mathrm{Hom}(V, W)$ gibt es höchstens eine adjungierte Abbildung. Diese bezeichnen wir mit Φ^*.

Satz 99 (RIEZscher Darstellungssatz) Sei V ein EUKLIDischer Vektorraum, $\dim V < \infty$ und $\mathbf{x}^* \in V^*$. Dann gilt:

$$\exists_1 \quad \mathbf{x}_0 \in V \quad \forall \quad \mathbf{x} \in V: \qquad \mathbf{x}^*(\mathbf{x}) = \langle \mathbf{x}, \mathbf{x}_0 \rangle$$

Satz 100 Seien V, W endlich dimensionale EUKLIDische Vektorräume. Dann gilt:

$$\forall\ \Phi \in \mathrm{Hom}(V, W)\ \exists\ \Phi^* \in \mathrm{Hom}(W, V): \quad \Phi, \Phi^* \text{ sind zueinander adjungiert}$$

Bem.

- Damit existiert ein basisunabhängiger Isomorphismus von V nach V^*. Ist B Basis von V, so gilt:

$$B \hat{=} B^* \qquad \Longleftrightarrow \qquad B \text{ ist Orthonormalbasis in } V.$$

- Ist A_Φ die Abbildungsmatrix von $\Phi \in \mathrm{Hom}(V, W)$, so gilt:

$$A_{\Phi^*} = A_\Phi^\top$$

Satz 101 Seien V, W EUKLIDische Vektorräume, Φ, Ψ Homomorphismen und $a \in \mathbb{R}$. Dann gilt:

1. $(\Phi^*)^* = \Phi$
2. $(a\Phi)^* = a\Phi^*$
3. $(\Phi + \Psi)^* = \Phi^* + \Psi^*$
4. $(\Phi \circ \Psi)^* = \Psi^* \circ \Phi^*$

Def. 75 Sei V ein EUKLIDischer Vektorraum und $\Phi \in \mathrm{End}\, V$. Φ heißt *selbstadjungiert* $:\Longleftrightarrow$

$$\forall \quad \mathbf{x}, \mathbf{y} \in V: \qquad \langle \Phi(\mathbf{x}), \mathbf{y} \rangle = \langle \mathbf{x}, \Phi(\mathbf{y}) \rangle$$

Φ heißt *antiselbstadjungiert* $:\Longleftrightarrow$

$$\forall \quad \mathbf{x}, \mathbf{y} \in V: \qquad \langle \Phi(\mathbf{x}), \mathbf{y} \rangle = -\langle \mathbf{x}, \Phi(\mathbf{y}) \rangle$$

Bem. Ist $\dim V < \infty$ und B eine Orthonormalbasis von V, dann gilt für $\Phi \in \operatorname{End} V$:

$$\Phi \text{ ist selbstadjungiert} \quad \Longleftrightarrow \quad A_\Phi \text{ ist symmetrisch}$$

Satz 102 Sei V ein EUKLIDischer Vektorraum, $\dim V < \infty$, $\Phi \in \operatorname{End} V$. Dann gilt: Φ ist selbstadjungiert $\Longleftrightarrow$ Es gibt eine Orthonormalbasis aus Eigenvektoren von Φ.

Def. 76 $A \in \mathbb{R}^{n\times n}$ mit $A^\top A = I$ heißt *orthogonal*. $A, B \in \mathbb{R}^{n\times n}$ heißen *orthogonal äquivalent* $:\Longleftrightarrow$

$$\exists \quad S \in \mathbb{R}^{n\times n} \text{ orthogonal :} \qquad B = S^\top AS.$$

Satz 103 Sei $A \in \mathbb{R}^{n\times n}$. Dann gilt: A ist symmetrisch $\Longleftrightarrow$ A ist orthogonal äquivalent zu einer Diagonalmatrix.

27 Isometrien

Def. 77 Seien V, W EUKLIDische $\mathbb{R}$-Vektorräume, $\Phi \in \operatorname{Hom}(V, W)$. Φ heißt *Isometrie* (oder *orthogonale Abbildung*) $:\Longleftrightarrow$

$$\forall \quad \mathbf{x}, \mathbf{y} \in V: \qquad \langle \Phi(\mathbf{x}), \Phi(\mathbf{y})\rangle = \langle \mathbf{x}, \mathbf{y}\rangle$$

Bem.

- Beachte, daß in obiger Definition links das Skalarprodukt in W und rechts das Skalarprodukt in V steht.
- Jede Isometrie ist injektiv
- Ist $\Phi \in \operatorname{Hom}(V, W)$ surjektiv (also bijektiv), so heißen V und W zueinander *isometrisch isomorph*.

Satz 104 Seien V, W EUKLIDische Vektorräume und $\Phi \in \operatorname{Hom}(V, W)$. Dann sind folgende Aussagen äquivalent:

1. Φ ist Isometrie
2. $\forall \quad \mathbf{x} \in V: \qquad \|\Phi(\mathbf{x})\| = \|\mathbf{x}\|$
3. $\forall \quad \mathbf{x}, \mathbf{y} \in V: \qquad d(\Phi(\mathbf{x}), \Phi(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$

Satz 105 Seien V, W EUKLIDische Vektorräume mit $\dim V = \dim W = n$ und $\Phi \in \operatorname{Hom}(V, W)$. Dann sind folgende Aussagen äquivalent:

1. Φ ist Isometrie.
2. Ist $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ eine Orthonormalbasis in V, so ist $(\Phi(\mathbf{b}_1), \ldots, \Phi(\mathbf{b}_n))$ eine Orthonormalbasis in W.
3. $\Phi^* \circ \Phi = \mathrm{id}_V$ und $\Phi \circ \Phi^* = \mathrm{id}_W$
4. Ist B eine Orthonormalbasis von V und $\tilde{B}$ eine Orthonormalbasis in W, dann ist die Abbildungsmatrix von Φ bezüglich B und $\tilde{B}$ orthogonal.

Def. 78 Sei V ein EUKLIDischer Vektorraum, $\dim V < \infty$ und $\Phi \in \operatorname{End} V$ eine Isometrie. Dann heißt Φ *Drehung*. Ist $\det \Phi = 1$, so heißt die Drehung *eigentlich*, ist $\det \Phi = -1$, so heißt sie *uneigentlich* . Uneigentliche Drehungen heißen auch *Drehspiegelung*

Bem.

- Außer ± 1 kann die Determinante von Φ keine Werte annehmen.
- Die Menge

  $$O(n) := \{A \in \mathbb{R}^{n\times n} : \ |\det A| = 1\}$$

  ist eine Gruppe, sie heißt *orthogonale Gruppe*. Die Menge

  $$SO(n) := \{A \in \mathbb{R}^{n\times n} : \ \det A = 1\}$$

  ist eine Untergruppe von $O(n)$ und heißt *spezielle* orthogonale Gruppe.

Satz 106 Sei V ein EUKLIDischer Vektorraum, $\dim V = n$, $\Phi \in \operatorname{End} V$. Dann gilt: Φ ist Isometrie $\Longleftrightarrow$ Es gibt eine Orthonormalbasis von V, bezüglich der A_Φ die Form

$$A_\Phi = \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & -1 & & & & & & & \\ & & & & \ddots & & & & & & \\ & & & & & -1 & & & & & \\ & & & & & & \cos\omega_1 & -\sin\omega_1 & & & \\ & & & & & & \sin\omega_1 & \cos\omega_1 & & & \\ & & & & & & & & \ddots & & \\ & & & & & & & & & \cos\omega_k & -\sin\omega_k \\ & & & & & & & & & \sin\omega_k & \cos\omega_k \end{pmatrix}$$

hat mit $\omega_i \in (0, \pi)$ $(i = 1, \ldots, k)$.

Bsp. Sei $\Phi : \mathbb{R}^3 \to \mathbb{R}^3$ eine Drehung mit $\det \Phi = 1$ und

$$\Phi(\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}) = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \qquad \Phi(\begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}) = \frac{1}{3}\begin{pmatrix} -2 \\ 1 \\ 7 \end{pmatrix}$$

Die Drehachse $[\mathbf{x}_1]$ steht senkrecht auf $\Phi(\mathbf{x}) - \mathbf{x}$ $(\mathbf{x} \in V)$. Damit gilt:

$$\mathbf{x}_1 \perp \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \qquad \mathbf{x}_1 \perp \begin{pmatrix} 1 \\ -5 \\ 4 \end{pmatrix}$$

$$\Longrightarrow \quad [\mathbf{x}_1] = [\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}] \qquad \Longrightarrow \quad \mathbf{x}_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Zur Bestimmung des Drehwinkels ω werden die Vektoren $\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$ orthogonal auf die Drehebene $[\mathbf{x}_1^\top]$ projeziert. Dabei ist zu beachten, daß die Vektoren

$$\mathbf{u} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \qquad \text{und} \qquad \mathbf{v} = \begin{pmatrix} 1 \\ -5 \\ 4 \end{pmatrix}$$

eine Basis von $[\mathbf{x}_1^\top]$ bilden. Damit ist

$$\pi_u(\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}) = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \qquad \text{und} \qquad \pi_v(\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}) = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

Damit gilt:

$$\begin{aligned} & \cos\omega = \frac{1}{2} \cdot \langle \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \rangle = \frac{1}{2} \\ \Longrightarrow \quad & \sin\omega = \frac{1}{2}\sqrt{3} \end{aligned}$$

Die Normalform lautet also

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

Die Transformationsmatrix S hat die Form

$$S = \frac{1}{6} \begin{pmatrix} 2\sqrt{3} & 0 & 4\sqrt{6} \\ 2\sqrt{3} & 3\sqrt{2} & -\sqrt{6} \\ 2\sqrt{3} & -3\sqrt{2} & -\sqrt{6} \end{pmatrix}$$

Index