Bild nicht verfügbar![width=6cm]TUD.png

Lineare Algebra und Analytische Geometrie

Wintersemester 2012 bis Sommersemester 2013

Vorlesung von Prof. Dr. Ulrich Brehm

Modul MATH-SEGY-LAAG | Stand des Skripts: 1. November 2018
Ursprünglicher Verfasser: Jack-William Jentzsch

Inhaltsverzeichnis

1 Mengen und Aussagenlogik

Die Grundlage dieses mathematischen Gebietes ist die **Mengenlehre**. Diese kann als Sprache der Mathematik verwendet werden.

1.1 Mengen

Die Menge ist ein mathematisches Objekt und beinhaltet Elemente. Eine *Menge* A ist eine Zusammenfassung bestimmter, wohl-unterscheidbarer Objekte a unserer Anschauung oder unseres Denkens zu einem Ganzen. Diese Objekte heißen *Elemente* der Menge. Man schreibt $a \in A$, sofern a Element der Menge A ist, andernfalls $a \notin A$. Schreibweise:

$a \in M$ (a ist ein Element von M)
$a \notin M$ (a ist kein Element von M)

Zwei Mengen A und B sind genau dann gleich, wenn sie **dieselben** Elemente enthalten. Schreibweise:

$A = B$ (gleiche Mengen)
$A \neq B$ (ungleiche Mengen)

1.1.1 Teilmengen

A ist **Teilmenge** von B genau dann, wenn für alle $a \in A$ stets $a \in B$ gilt. (Enthält die Möglichkeit der Gleichheit).

1.1.2 Schreibweisen für Mengen

$\{1, 2, 3\} = \{1, \frac{4}{2}, 2, 3\}$
Mengen können auch Mengen als Elemente enthalten. Zahlen werden widerum als Mengen definiert.

1.1.3 Die leere Menge

Menge ohne Elemente. Schreibweise: $\emptyset$ statt $\{\}$.

Symbol	Bedeutung
$\{\emptyset\}$	eine nichtleere Menge, Menge mit einem Element, Menge mit der leeren Menge enthalten, Anschauung: Ein Sack mit einem leeren Sack drin.)
$\{\{\emptyset\}\}$	Menge mit der Menge der leeren Menge
$\{\emptyset, \{\emptyset\}\}$	Menge mit zwei Elementen

1.1.4 Bezeichnung für einige Mengen

Symbol	Bedeutung
$\mathbb{N} = \{1; 2; 3; 4; \ldots\}$	natürliche Zahlen
$\mathbb{N}_0 = \{0; 1; 2; 3; 4; \ldots\}$	natürliche Zahlen mit 0
$\{q, \ldots, l\}$	Die natürlichen Zahlen lückenlos von q bis l
$\{a, b, q, \ldots, l, c, d, e\}$	Die Zahlen a, b, c, d, e und die natürlichen Zahlen lückenlos von q bis l
$\mathbb{Z} = \{-2; -1; 0; 1; 2; \ldots\}$	ganze Zahlen
$\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$	rationale Zahlen
$\mathbb{R}$ = siehe Vollständigkeitsaxiom	reelle Zahlen (Beispiele: $\sqrt{2}, \pi$)
$\mathbb{C} = \mathbb{R} \times \mathbb{R}$	komplexe Zahlen (Beispiele: $i, 1 - i, \sqrt{3} + 2i$)

1.1.5 Aussonderung durch Eigenschaften

Gegeben ist die Menge aller x, die Elemente von A sind und die Eigenschaft E haben. Schreibweisen:
$\{x \in A \text{ und } E(x)\}$
$\{x \in A \,|\, E(x)\}$
Beispiel: $\{x \in \mathbb{N} \,|\, x \text{ ist gerade und } x < 5\} = \{2, 4\}$

1.2 Aussagenlogik mit Mengen

1.2.1 Wahrheitstabellen

w ... wahr
f ... falsch

Keine Aussage ist: Diese Aussage ist falsch.
Seien a und b Aussagen (w oder f), dann gilt:

a	b	$a \wedge b$	$a \vee b$	exklusiv oder	$a \longrightarrow b$	$a \longleftrightarrow b$	$\neg a$
		und	oder	entweder a oder b	wenn a, dann b	a gilt genau dann, wenn b gilt	nicht a
w	w	w	w	f	w	w	f
w	f	f	w	w	f	f	f
f	w	f	w	w	w	f	w
f	f	f	f	f	w	w	w

1.2.2 Quantoren

$\forall x \in A\colon E(x)$	für alle x in A gilt $E(x)$
$\exists x \in A\colon E(x)$	es gibt ein x in A, für das $E(x)$ gilt
$\exists! x \in A\colon E(x)$	es gibt genau ein x in A, für das $E(x)$ gilt
$\forall x \in \mathbb{N}\colon \exists y \in \mathbb{N}\colon y \geq x$	für jedes x in $\mathbb{N}$ gibt es ein y in $\mathbb{N}$, für das $y \geq x$ gilt: wahre Aussage
$\exists y \in \mathbb{N}\colon \forall x \in \mathbb{N}\colon y \geq x$	es gibt eine natürliche Zahl, welche größer ist als alle anderen Zahlen: falsche Aussage
$\forall x \in \emptyset\colon E(x)$	für alle Elemente der leeren Menge gilt $E(x)$: Immer wahr, da die leere Menge keine Elemente hat, für die die Aussage hätte überprüft werden müssen
$\exists x \in \emptyset\colon E(x)$	es gibt ein x als Element der leeren Menge mit $E(x)$: ist falsch, da es nicht mal ein Element geben kann für das die Aussage zutreffen könnte

1.2.3 Mengentheoretische Operationen

$A \cap B := \{x \,|\, x \in A \wedge x \in B\}$	Durchschnitt von A und B, Gesprochen: A geschnitten B.
$A \cup B := \{x \,|\, x \in A \vee x \in B\}$	Vereinigung von A und B, Gesprochen: A vereinigt B.
$A \setminus B := \{x \,|\, x \in A \wedge x \notin B\}$	Relatives Komplement, Gesprochen: A ohne B.

1.2.4 Schreibweise

:= ... Der Ausdruck auf der linken Seite wird durch den auf der rechten Seite definiert.

links wird ein neues Symbol, oder bereits bekannte Objekte neu arrangiert. Auf der rechten Seite

wird dann erklärt was dieses Arrangement bedeuted. Es kann eventuell zusätzlich notwendig sein zu zeigen dass die rechte Seite wohldefiniert ist, d.h. definiert ist.

1.2.5 Rechenregeln

Idempotenz	$A \cap A = A$	$A \cup A = A$
Kommutativgesetz	$A \cap B = B \cap A$	$A \cup B = B \cup A$
Assoziativgesetz	$A \cap (B \cap C) = (A \cap B) \cap C$	$A \cup (B \cup C) = (A \cup B) \cup C$
Distributivgesetz	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Absorptionsgesetz	$A \cap (A \cup B) = A$	$A \cup (A \cap B) = A$

Die Beweise dieser Aussagen werden durch Wahrheitstabellen erbracht.

1.2.6 Das Venn-Diagramm

Das Venn-Diagramm ist eine **Darstellungsmöglichkeit von Mengen**. Hier einige Beispiele:

Bild nicht verfügbar!AoderBr.png	Bild nicht verfügbar!AundB.png	Bild nicht verfügbar!AundAoderC.png
Abbildung 1: $B \cup C$	Abbildung 2: $A \cap B$	Abbildung 3: $A \cap (B \cup C)$

1.2.7 Echte Teilmengen

Eine Menge A ist eine **echte Teilmenge** von B, wenn Folgendes gilt:
$A \subset B :\Leftrightarrow A \subseteq B \wedge A \neq B$

1.2.8 Konventionen der Logik

Das Symbol $\neg$ bindet stärker als $\wedge$ und $\vee$ und diese stärker als $\rightarrow$ und $\leftrightarrow$. Zum Beispiel ist der Ausdruck $\neg a \wedge b \rightarrow c$ so geklammert: $((\neg a) \wedge b) \rightarrow c$.

1.2.9 Logische Ausdrücke

Ein logischer Ausdruck heißt **allgemeingültig**, wenn er stets wahr ist, egal wie die Wahrheitstabelle der Aussagevarianten sind und egal welche Prädikate für die Prädikatsymbole und welche Mengen für die Mengensymbole eingesetzt werden. Zwei Ausdrücke A und B heißen **äquivalent**, geschrieben $A \Leftrightarrow B$, falls $A \leftrightarrow B$ allgemeingültig ist. A impliziert B, geschrieben $A \Rightarrow B$, falls $A \rightarrow B$ allgemeingültig ist. Im Allgemeinen gilt:

$a \vee \neg a$	$\Leftrightarrow$	wahr
$\neg\neg a$	$\Leftrightarrow$	a
$(a \rightarrow b)$	$\Leftrightarrow$	$b \vee \neg a$ (Ausdruck auch wahr, wenn a nicht wahr ist)
$(a \rightarrow b) \wedge (b \rightarrow a)$	$\Leftrightarrow$	$a \leftrightarrow b$
$\neg(a \vee b)$	$\Leftrightarrow$	$\neg a \wedge \neg b$
$\neg(a \wedge b)$	$\Leftrightarrow$	$\neg a \vee \neg b$
$\neg(\exists x \in A\colon E(x))$	$\Leftrightarrow$	$\forall x \in A\colon \neg E(x)$
$\neg(\forall x \in A\colon E(x))$	$\Leftrightarrow$	$\exists x \in A\colon \neg E(x)$

Achtung: Die folgenden Aussageformen sind paarweise nicht äquivalent:
$(a \rightarrow b) \rightarrow c$
$a \rightarrow (b \rightarrow c)$
$(a \rightarrow b) \wedge (b \rightarrow c)$

1.2.10 Der mathematische Beweis

Zwischen mathematischen Aussagen gelten die Schreibweisen $\Rightarrow$, $\Leftarrow$ und $\Leftrightarrow$. In Beweisen will man **Ketten von Schlüssen** ziehen. Beispiele:

$a \wedge (a \to b)$	$\Rightarrow$	b	Aus a folgt b, wobei a wahr ist. Daraus folgt: b ist wahr.
$\neg b \wedge (a \to b)$	$\Rightarrow$	$\neg a$	Aus a folgt b, wobei b nicht wahr ist. Daraus folgt: a ist nicht wahr.
$(a \to b) \wedge (b \to c)$	$\Rightarrow$	$a \to c$	Aus a folgt b und aus b folgt c. Daraus folgt: aus a folgt c.
$(a \vee b) \wedge (a \to c) \wedge (b \to c)$	$\Rightarrow$	c	Wenn a oder b und aus beiden c folgt, dann gilt c.

Schreibweise: $\langle A \Rightarrow B \Rightarrow C \rangle :\Leftrightarrow \langle A \Rightarrow B \wedge B \Rightarrow C \rangle$

1.2.11 Die Potenzmenge

Die Menge $\mathcal{P}(A) := \{B \mid B \subseteq A\}$ aller Teilmengen von A wird als **Potenzmenge** von A bezeichnet. Daraus folgt, dass die leere Menge $\emptyset$ und die Menge A Elemente der Potenzmenge $\mathcal{P}(A)$ sind. Die Potenzmenge $\mathcal{P}(A)$ einer n-elementigen Menge A besitzt 2^n Elemente. Beispiel: $\mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$.

- Jede Menge hat genau eine Potenzmenge $\mathcal{P}(A)$, z. B. $\mathcal{P}(\{1,2\}) = \{\{1\}, \{2\}, \{1,2\}, \emptyset\}$
- Die leere Menge ist Element jeder Potenzmenge: $\emptyset \in \mathcal{P}(X)$
- Jede Menge ist Teilmenge von sich selbst: $X \in \mathcal{P}(X)$
- Die Potenzmenge der leeren Menge enthält nur die leere Menge. $\mathcal{P}(\emptyset) = \mathcal{P}(\{\}) = \{\{\}, \{\}\} = \{\emptyset\}$
- Von endlichen Mengen ist die Potenzmenge endlich. Die Anzahl der Elemente der Potenzmenge einer endlichen Menge lässt sich so berechnen:

$\|\|x\|\| = 2$	...	Menge x mit genau zwei Elementen
$\|\|x\|\| < \infty$	...	endliche Menge
$\|\|\mathcal{P}(x)\|\| = 2^{\|\|x\|\|} = 2^{\|\|2\|\|} = 4$	...	Berechnung der Anzahl der Elemente der Potenzmenge

  Der Beweis wird durch vollständige Induktion erbracht.

1.2.12 Durchschnittsmenge/Schnittmenge

Sei M eine Menge von Mengen, dann gilt (für $M \neq \emptyset$):

$\bigcap M = \{x \mid \forall A \in M \colon x \in A\}$ [1].

Ein Beispiel:
$\bigcap\{\{1,2,3\}, \{2,3,7\}, \{\{2,7\}, 3\}\} = \{1,2,3\} \cap \{2,3,7\} \cap \{\{2,7\}, 3\} = \{3\}$.

Andere Schreibweise: $\bigcap\{M_i \mid i \in I\} = \{x \mid \forall i \in I \colon x \in M_i\}$. (... I: Indexmenge)
Beispiel: $I := \{1,2,3,4\}$
$\bigcap\{B_1, B_2, B_3, B_4\} = \{x | \forall i \in \{1,2,3,4\}; x \in B_i\} = \{x | x \in B_1 \wedge x \in B_2 \wedge x \in B_3 \wedge x \in B_4\}$

[1] Menge aller x, die in jeder Menge A des Mengensystems liegen

1.2.13 Vereinigungsmenge

$\bigcup M = \{x \mid \exists A \in M : x \in A\}$. [2]

Andere Schreibweise: $\bigcup\{M_i | i \in I\} = \{x \mid \exists i \in I : x \in M_i\}$.

1.2.14 Das Tupel

Definiere $(a, b) := \{\{a\}, \{a, b\}\}$. (a, b) heißt ein **geordnetes Paar** oder 2-Tupel oder nur Tupel, wobei zwei geordnete Paare (a, b) und (a', b') genau dann gleich sind, wenn $a = a' \wedge b = b'$. (Leichte Übung)

1.2.15 Das kartesische Produkt

Das kartesische Produkt zweier Mengen A und B ist definiert als $A \times B := \{(a, b) \mid a \in A, b \in B\}$.
$A^2 := A \times A$.
Beispiel: $\{1, 2\} \times \{1, 2, 3\} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$ [3]

1.2.16 Feststellung 1: Aussagenlogik

Sei M eine nichtleere Menge von Mengen, dann gilt:

- $A \cup (\cap M) = \cap\{A \cup B \mid B \in M\}$
- $A \cap (\cup M) = \cup\{A \cap B \mid B \in M\}$

Beweis:

$$
\begin{array}{lll}
x \in A \cap (\cup M) & \Leftrightarrow & x \in A \wedge x \in \bigcup M \\
& \Leftrightarrow & x \in A \wedge (\exists B \in M : x \in B) \\
& \Leftrightarrow & \exists B \in M : (x \in A \wedge x \in B) \\
& \Leftrightarrow & \exists B \in M : (x \in A \cap B) \\
& \Leftrightarrow & x \in \cup\{A \cap B \mid B \in M\} \\
& \text{also} & A \cap (\cup M) = \cup\{A \cap B \mid B \in M\} \ \blacksquare
\end{array}
$$

Eine Feststellung ist eine Tatsache, welche bewiesen wird, es aber nicht verdient, Satz genannt zu werden.

[2] Für ein x gilt: es gibt ein A in M, sodass $x \in A$.
[3] Beachte: $(a, b) \neq (b, a)$, falls $a \neq b$.

2 Relationen und Abbildungen

2.1 Relationen

Definition: Seien A, B Mengen. Eine Teilmenge $R \subseteq A \times B$ heißt eine Relation zwischen A und B. Falls $A = B$, dann heißt R eine Relation auf A.
Schreibweise: statt $(a, b) \in R$ schreibt man auch oft aRb. z.B. die Relation "$\leqslant$": $a \leqslant b$ statt $(a, b) \in \leqslant$

2.1.1 Beispiele für Relationen

a)	Die Gleichheitsrelation auf A (Diagonale)	$\triangle A := \{(a, a) \mid a \in A\}$
b)	Die Teilerrelation auf $\mathbb{Z}$ (ganze Zahlen)	$R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ teilt } n\}$ geschrieben: $m \mid n$ (d. h. $\frac{n}{m} \in \mathbb{Z}$) (d. h. es gibt ein $a \in \mathbb{Z}$: $n = am$)
c)	Die Kleinerrelation auf $\mathbb{R}$	$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$
d)	Die Relation 'liegt auf' zwischen der Menge der Punkte der Ebene und der Menge der Geraden der Ebene.	$\{(p, g) \mid p$ ist Punkt der Ebene, g ist Gerade der Ebene und p liegt auf $g\}$

2.1.2 Veranschaulichung einer Relation

Relation (Menge von geordneten Paaren): $\{(1, 1), (2, 1), (2, 3), (3, 1), (3, 4), (1, 3)\}$ (= Relation auf der Menge $\{1, 2, 3, 4\}$.
Bild nicht verfügbar![width=4cm]Folie1.png
Abbildung 4: Veranschaulichung als Pfeildiagramm

Ein Pfeil geht von a nach b genau dann, wenn $(a, b) \in R$ ist. Die Mengen A und B sind getrennt gezeichnet. Die Menge kann auch nur einmal dargestellt werden, wenn $A = B$:
Bild nicht verfügbar![width=4cm]UE1.png
Abbildung 5: $A = B$

(A, R) heißt dann auch ein **gerichteter Graph** (ohne Mehrfachkanten) und A ist die Menge der Ecken des Graphen und R die Menge der Kanten. Anwendung:

- Straßennetz (Kanten := Straßen, Ecken := Kreuzungen)
- Transportnetz

Bild nicht verfügbar![width=4cm]Folie3.png
Abbildung 6: Veranschaulichung als Tabelle

Falls insbesondere $A, B \subseteq \mathbb{R}$, dann stellt man den Graphen als Teilmenge der Ebene dar. Zum Beispiel $xRy \Leftrightarrow x \leq y$.

Bild nicht verfügbar![width=4cm]UE2.png
Abbildung 7: $xRy \Leftrightarrow x \leq y$

Bild nicht verfügbar![width=4cm]Folie5.png
Abbildung 8: $xRy \Leftrightarrow x^2 + y^2 \leq 1$
Kreisscheibe

Bild nicht verfügbar![w
Abbildung 9: $xRy \Leftrightarrow x$
Kreislinie

2.1.3 Definitionen und Feststellungen: Eigenschaften von Relationen

Def.	Seien $R \subseteq A \times B$, $S \subseteq B \times C$. Dann definiere: $R^{-1} := \{(b,a) \in B \times A \mid (a,b) \in R\}$ (R wird vertauscht) $S \circ R := \{(a,c) \in A \times C \mid \exists b \in B\colon (a,b) \in R \wedge (b,c) \in S\}$ (lies: S nach R) Bild nicht verfügbar![width=4cm]Folie7.png Abbildung 10: $S \circ R$ (Gestrichelte Linie)
$\triangle_A$	Diagonale von A
reflexiv	Sei R eine Relation auf A, dann heißt R reflexiv, falls $\triangle_A \subseteq R$, d. h., falls für alle $a \in A$ gilt $(a,a) \in R$
symmetrisch	falls $R = R^{-1}$, d. h. falls für alle $a, b \in R$ gilt: $(a,b) \in R \Rightarrow (b,a) \in R$
antisymetrisch	falls $R \cap R^{-1} \subseteq \triangle_A$, d. h. für alle $a, b \in R$ gilt: $\langle (a,b) \in R \wedge (b,a) \in R \rangle 4 \Rightarrow a = b$
transitiv	falls $R \circ R \subseteq R$, d. h. für alle $a, c \in R$ gilt: $(a,b) \in R$ und $(b,c) \in R \Rightarrow$ $(a,c) \in R$

Es gilt nicht: symetrisch $\Leftrightarrow \neg$ antisymetrisch.
Eine Relation R auf M heißt **Äquivalenzrelation**, falls sie reflexiv, symmetrisch und transitiv ist. Eine Relation R auf M heißt eine **Ordnungsrelation** (auch Halbordnung, partielle Ordnung) wenn sie reflexiv, antisymmetrisch und transitiv ist (Teilmengenrelation: $A \subseteq B$) Falls zusätzlich für alle $a, b \in A$ gilt: $(a,b) \in R$ oder $(b,a) \in R$, dann heißt R eine **Totalordnung**.

Beispiel: Teilmengenrelation $\subseteq$ auf $\mathcal{P}(M)$

2.1.4 Definitionen: Einschränkung von Relationen

Sei $R \subseteq A \times B$ eine zweistellige Relation. Die Einschränkung der Relation R auf C und D ist definiert durch:

$$R|_C^D := R \cap (C \times D) \qquad R|_C := R|_C^A \qquad R|^D := R|_B^D$$

2.1.5 Partiell geordnete Mengen

Sei M eine Menge und $\leq$ eine Ordnungsrelation auf M, dann heißt $(M, \leq)$ eine **partiell geordnete Menge**. Falls $\leq$ sogar eine Totalordnung auf M ist, dann heißt $(M, \leq)$ eine **total geordnete Menge** (linear geordnete Menge, Kette). Bezeichnung: $y \geq x$ bedeutet $x \leq y$. Beispiele für partiell geordnete Mengen:

1)	$(\mathcal{P}(M), \subseteq)$	Teilmengenrelation
2)	$(\mathbb{N}, \mid)$	$\{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ teilt } b\}$
3)	$(\mathbb{R}, \leq)$	ist total geordnet ($\leq$ wie üblich)

Definition: Sei $(M, \leq)$ eine partiell geordnete Menge und $S \subseteq M$ und $y \in M$, dann heißt $x \in M$:

kleinstes Element	falls	$\forall y \in M\colon x \leq y$
größtes Element	falls	$\forall y \in M\colon y \leq x$
maximales Element	falls	$\forall y \in M\colon (x \leq y \Rightarrow x = y)$
minimales Element	falls	$\forall y \in M\colon (x \geq y \Rightarrow x = y)$
obere Schranke von S	falls	$\forall s \in S\colon s \leq x$
untere Schranke von S	falls	$\forall s \in S\colon x \leq s$
Infimum von S	falls	x die größte untere Schranke von S ist.
Supremum von S	falls	x die kleinste obere Schranke von S ist.
Oberer Nachbar von y	falls	$y \leq x \wedge x \neq y \wedge \forall z \in M\colon y \leq z \leq x \Rightarrow z = x \vee z = y$ (nichts zwischen x und y)
Unterer Nachbar von y	analog	

Sei $x, y \in M$: Falls $x \leq y$ oder $y \leq x$, dann heißen x und y **vergleichbar**, sonst unvergleichbar.
$(M, \leqslant)$ heißt ein Verband, falls für je zwei Elemente x, $y \in M$ gilt: Das Supremum von $\{x, y\}$ und das Infimum von $\{x, y\}$ existieren.

2.1.6 Graphische Darstellung von endlichen partiell geordneten Mengen als Hasse-Diagramm

Man symbolisiert die Elemente durch Punkte und beschreibt die Relation 'ist oberer Nachbar' durch Kanten die von unten nach oben gehen.

Bild nicht verfügbar![width=4cm]BnA.png Abbildung 11: b ist oberer Nachbar von a.
Bild nicht verfügbar![width=4cm]AW.png Abbildung 12: Hasse-Diagramm der Relation $(\{1,2,3,4\}, \leq$).
Bild nicht verfügbar![width=4cm]BW.png Abbildung 13: Teiler von 6 (2 kein Teiler von 3).
Bild nicht verfügbar![width=4cm]CW.png Abbildung 14: Beliebiges Hasse-Diagramm.

Gegeben ist $S = \{b, c\}$. Im Folgenden ist a die größte untere Schranke von S, also Infimum. Es gibt kein Supremum, also keine kleinste obere Schranke von S:
Bild nicht verfügbar![width=4cm]Diag1.png Abbildung 15: $S = \{b, c\}$.

Im Folgenden ist c sowohl minimal, als auch maximal:
Bild nicht verfügbar![width=4cm]Diag2.png Abbildung 16: c als minimales und maximales Element.

Im Folgenden hat S keine untere Schranke und damit auch kein Infimum:
Bild nicht verfügbar![width=4cm]Diag3.png Abbildung 17: S ohne Infimum.

Eventueller 3D-Eindruck ist irrelevant, nur Höhe auf Papier zählt.

2.1.7 Feststellung 2: Größtes Element

> Das größte Element bzw. das kleinste Element einer partiell geordneten Menge ist eindeutig (falls es existiert), folglich sind auch Supremum und Infimum eindeutig bestimmt, falls sie existieren.
>
> Beweis:
> Seien Y_1 und Y_2 größte Elemente, dann folgt $Y_1 \leq Y_2$ und $Y_2 \leq Y_1$, also $Y_1 = Y_2$ (antisymmetrisch). D. h. das größte Element ist eindeutig. (Eindeutigkeit des kleinsten Elements analog.) ■

Bezeichnungen: Falls sie existieren bezeichne $\max M$ das größte, und $\min M$ das kleinste Element von M. Für $S \subseteq M$ bezeichne $\sup S$ das Supremum und $\inf S$ das Infimum.

2.1.8 Feststellung 3: Maximales Element

In einer endlich partiell geordneten Menge $(M, \subseteq)$ mit $M \neq \emptyset$ gibt es stets minimale und maximale Elemente (mindestens eins).

Beweis:
$M \neq \emptyset$, also gibt es ein Element a. Starte mit diesem, wähle ein echt größeres und davon wieder ein echt größeres. Da M endlich ist, bricht das Verfahren ab, d.h. nach endlich vielen Schritten wählt man ein Element, das kein echt größeres Element besitzt und damit maximal ist. (Minimales Element analog).
■

2.2 Abbildungen

(= Zuordnungen, oder Funktion)

2.2.1 Definition und Schreibweise

Seien A, B Mengen. Eine Abbildung f von A nach B, geschrieben $f\colon A \to B$, ist eine Relation $f \subseteq A \times B$, sodass für jedes $a \in A$ genau ein $b \in B$ existiert mit $(a, b) \in f$. Schreibweise: $b = f(a)$ für $(a, b) \in f$, auch $b = fa$, wenn aus dem Zusammenhang klar ist was gemeint ist. Zur Definition der Abbildung gehört die Angabe der Menge A (der **Definitionsbereich** oder die Quelle), der Menge B (der **Wertevorrat** oder das Werteziel) und der Relation f (die **Zuordnungsvorschrift**). Formal werden Abbildungen als Tripel (f, A, B) definiert.
Die Relation $\{(a, f(a)) \mid a \in A\}$ heißt auch der **Graph der Abbildung**. Wenn $b = f(a)$, dann heißt b das Bild von a unter f und a ein Urbild von b unter f.

2.2.2 Konvention

Die Schreibweise $f\colon A \to B$ bzw. $A \xrightarrow{f} B$ soll bedeuten, dass A, B Mengen und f eine Abbildung ist. Schreibweise:

$$\begin{array}{ll} f\colon & A \to B \\ & a \mapsto f(a) \end{array}$$

Hier ist a ein Variablensymbol für Elemente von A, das Symbol $\mapsto$ bezeichnet die Zuordnung der Elemente.

Beispiele:

$$\begin{array}{lll} f\colon & \mathbb{R} \to \mathbb{R} & \text{und} \quad g\colon \quad \mathbb{R} \to [0, \infty) \\ & t \mapsto t^2 & \qquad\quad t \mapsto t^2 \end{array}$$

Die beiden Abbildungen f, g sind verschieden, obwohl die Relationen übereinstimmen, weil die Wertevorräte verschieden sind.

Bild nicht verfügbar![width=9cm]Graf1.png Abbildung 18: Graf von f.

$$\begin{array}{lll} h\colon & \mathbb{R} \to \mathbb{R} & \text{keine Abbildung,} \quad \mathbb{R} \setminus \{0\} \to \mathbb{R} \text{ ist Abbildung} \\ & t \mapsto \frac{1}{t} & \qquad\qquad\qquad\quad t \mapsto \frac{1}{t} \end{array}$$

2.2.3 Identische Abbildung

Die identische Abbildung $M \to M$ bezeichnet die durch $\mathrm{id}(x) = x$ definierte Abbildung von M nach M. Sie heißt die identische Abbildung und wird auch mit id_M bezeichnet (bzw. id, falls aus dem Kontext klar ist, dass es um M geht). Die Relation ist $\triangle_M = \{(x, x) \mid x \in M\}$.

2.2.4 Feststellung 4: Komposition mehrerer Abbildungen

Seien $f\colon A \to B$ und $g\colon B \to C$ Abbildungen, dann ist die Relation $g \circ f$ (gesprochen g nach f) eine Abbildung in A nach C, d. h. wir können schreiben $g \circ f\colon A \to C$ ($A \xrightarrow{f} B \xrightarrow{g} C$). $g \circ f$ heißt die **Komposition** von g nach f. Es gilt: $(g \circ f)(a) = g(f(a))$.

Beweis:
Sei $a \in A$, dann gibt es genau ein $b \in B$ mit $(a, b) \in f$ und zu diesem genau ein $c \in C$ mit $(b, c) \in g$. Also ist dieses c das einzige Element in C mit $(a, c) \in g \circ f$.■

Nach Schreibweise ist $b = f(a)$, $c = g(b)$, also $c = g(f(a))$ und $c = (g \circ f)(a)$.

2.2.5 Feststellung 5: Rechnen mit Kompositionen

Wenn $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$ Abbildungen sind, dann ist $h \circ (g \circ h) = (h \circ g) \circ f$ eine Abbildung von A nach D.■

Beweis:
Hausaufgabe

2.2.6 Eigenschaften von Abbildungen

Eine Abbildung $f\colon A \to B$ heißt ...

injektiv	falls	für alle $a_1, a_2 \in A$ gilt $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$, d.h. falls jedes Element aus B höchstens ein Urbild hat.
surjektiv	falls	für alle $b \in B$ mindestens ein $a \in A$ existiert, mit $f(a) = b$, d. h. falls jedes Element aus B mindestens ein Urbild hat.
bijektiv	falls	f injektiv und surjektiv ist, d. h. falls jedes Element aus B genau ein Urbild hat.

2.2.7 Fortsetzung

Sei $f\colon A \to X$ eine Funktion. Eine Fortsetzung g von f ist wenn $g\colon B \to Y$, $A \subseteq B$ und $\forall x \in A\colon f(x) = g(x)$

2.2.8 Feststellung 6: Umkehrabbildung

Sei $f\colon A \to B$ eine bijektive Abbildung, dann ist die Relation f^{-1} eine Abbildung von B nach A, also $f^{-1}\colon B \to A$ mit $f^{-1}(b) = a \Leftrightarrow f(a) = b$.
Die Abbildung f^{-1} heißt dann die **Umkehrabbildung** (inverse Abbildung) von f. Es gilt dann ferner:

- f^{-1} ist bijektiv
- $(f^{-1})^{-1} = f$
- $f^{-1} \circ f = id_A$
- $f \circ f^{-1} = id_B$

Beweis: klar, bzw. sehr einfach.■

2.2.9 Die leere Funktion

Bemerkung: Es gibt genau eine Abbildung $\emptyset \to B$, diese wird die leere Funktion genannt und mit $\emptyset_B$ bezeichnet. Sie ist leer: $\emptyset_B = \emptyset$

Beispiele:
Bild nicht verfügbar![width=3cm]Abb1.png Abbildung 19: jedes wird hinten erreicht: f ist surjektiv, f ist nicht injektiv.
Bild nicht verfügbar![width=3cm]Abb2.png Abbildung 20: weder surjektiv noch injektiv.
Bild nicht verfügbar![width=3cm]Abb3.png Abbildung 21: bijektiv.
Bild nicht verfügbar![width=3cm]Abb4.png Abbildung 22: keine Abbildung.
Bild nicht verfügbar![width=3cm]Abb5.png Abbildung 23: keine Abbildung.

2.2.10 Definition und Schreibweise von Abbildungen

Sei $f\colon A \to B$ eine Abbildung und $\widetilde{A} \subseteq A$, dann bezeichne $f[\widetilde{A}] := \{f(a) \mid a \in \widetilde{A}\}$. $f[\widetilde{A}]$ heißt das Bild von $\widetilde{A}$ unter f (oder Bildmenge). Falls keine Missverständnisse zu befürchten sind, schreibt man auch $f(\widetilde{A})$ für $f[\widetilde{A}]$ (genau: falls $A \cap \mathcal{P}(A) = \emptyset$).

Entsprechend für $\widetilde{B} \subseteq B$ definiere $f^{-1}[\widetilde{B}] := \{a \in A \mid f(a) \in \widetilde{B}\}$. $f^{-1}[\widetilde{B}]$ heißt das vollständige Urbild von $\widetilde{B}$ unter f (oder Urbildmenge).
Falls keine Missverständnisse zu befürchten sind, schreibt man auch $f^{-1}(\widetilde{B})$, statt $f^{-1}[\widetilde{B}]$.
Beispiel: $A := \{\emptyset, \{\emptyset\}\}$, $\mathcal{P}(A) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
Was heißt jetzt $f(\{\emptyset\})$?
Für jede Menge A gibt es genau eine Abbildung mit $\emptyset \to A$. Diese wird die leere Funktion $\emptyset_A$ genannt. $\emptyset_A := (\emptyset, A, \emptyset)$

2.3 Äquivalenzrelation

werden oft mit $\sim$ bezeichnet.

2.3.1 Definition

Sei $\sim$ eine **Äquivalenzrelation** auf M und $a \in M$, dann gilt:

$$[a]_\sim := \{x \in M \mid x \sim a\} = \{x \in M \mid (x, a) \in \sim\} \quad \text{(Menge aller } x \text{ die zu } a \text{ äquivalent sind)}$$

heißt die Äquivalenzklasse von a bezüglich $\sim$. Schreibe $[a]$, falls klar ist, was $\sim$ ist. Es gilt:

$$(x, a) \in \sim \Leftrightarrow x \sim a \Leftrightarrow x \in [a]$$

Des Weiteren definiere:

$$M/\sim := \{[a]_\sim \mid a \in M\} \quad \text{(Menge aller Äquivalenzklassen)}$$

heißt die Faktormenge von M bezüglich $\sim$. Also die Menge der **Äquivalenzklassen**. Definiere die Abbildung

$$\text{nat}_\sim \colon M \to M/\sim$$
$$\text{nat}_\sim(a) := [a]_\sim$$

Sie heißt die natürliche Abbildung.

Beispiel:
Gegeben ist die Menge aller Studenten. Jedem Student wird eine Übungsgruppe zugeordnet. Die Äquivalenzklassen sind diese Übungsgruppen.

2.3.2 Satz 1: Aussagen über Äquivalenzrelation

Sei $M \neq \emptyset$, dann gilt:

- Sei $\sim$ eine Äquivalenzrelation auf M, dann gilt für alle $a, b \in M$:
  - wenn $[a] \neq [b]$, dann gilt $[a] \cap [b] = \emptyset$ (Wenn die Übungsgruppen verschieden sind, dann haben sie kein gemeinsames Element, oder ein Baustein kann nicht in zwei farbsortierten Häufen sein).
  - $[a] = [b] \Leftrightarrow a \sim b$. Ferner gilt:
    - $a \in [a]$, also insbesondere $[a] \neq \emptyset$
    - $M = \bigcup\{[a] \mid a \in M\}$
- Sei $m \subseteq \mathcal{P}(M)$, sodass gilt:
  - $\emptyset \notin m$ (i)
  - $A \cap B = \emptyset$, für alle $A, B \in m$ mit $A \neq B$. (ii)
  - $\bigcup m = M$ (iii)

Dann gibt es genau eine Äquivalenzrelation $\sim$ auf M. sodass $m = M/\sim$.

Definition:
$m \subseteq \mathcal{P}(M)$ heißt eine Zerlegung von M (oder eine Klasseneinteilung), falls m (i), (ii) und (iii) erfüllt.

Satz 1 besagt also, dass für jede Äquivalenzrelation $\sim$ auf M die zugehörige Faktormenge $M/\sim$ eine Zerlegung von M ist. Genauer handelt es sich bei der Zuordnung $\sim \mapsto M/\sim$ um eine Bijektion von der Menge der Äquivalenzrelationen auf M in die Menge der Zerlegungen von M.
Beweis:

- Da $\sim$ reflexiv ist, ist $a \in [a]$, also sehen wir $[a] \neq \emptyset$ und $M = \bigcup\{[a] \mid a \in M\}$. Sei $a \sim b$, wenn $x \in [a]$ ist, dann ist $x \sim a$, also $x \sim b$ (Transitivität), also $x \in [b]$, d. h. $[a] \subseteq [b]$ und genauso $[b] \subseteq [a]$ (da $b \sim a$ wegen $\sim$ symmetrisch). Insgesamt: $a \sim b \Rightarrow [a] = [b]$. Sei $[a] = [b]$, dann ist $a \in [b]$, also $a \sim b$. Insgesamt: $a \sim b \Leftrightarrow [a] = [b]$.

Sei nun $[a] \cap [b] \neq \emptyset$, dann wähle $x \in [a] \cap [b]$. Dann ist $x \sim a$ und $x \sim b$, also $[x] = [a]$ und $[x] = [b]$ also $[a] = [b]$.

- Erfülle $m \subseteq \mathcal{P}(M)$ die Voraussetzung. Definiere eine Relation $\sim := \bigcup\{A \times A \mid A \in m\} \subseteq M \times M$ also $a \sim b \Leftrightarrow \exists A \in m \colon a \in A \wedge b \in A$.

Zu zeigen: $\sim$ ist eine Äquivalenzrelation.

reflexiv	Sei $a \in M$. Wegen (iii) gibt es ein $A \in m$ mit $a \in A$, also $(a, a) \in A \times A \subseteq \sim$.
symmetrisch	Seien $a, b \in M$ mit $a \sim b$. Dann gibt es ein $A \in m$ mit $a \in A \wedge b \in A$, also $b \sim a$.
transitiv	Seien $a, b \in M$ mit $a \sim b$ und $b \sim c$. Dann gibt es $A, B \in m$ mit $a \in A \wedge b \in A \wedge b \in B \wedge c \in B$, also $b \in A \cap B$, also wegen (ii) $A = B$, also $a \sim c$.■

Beispiel:
informell: Gegeben ist eine Menge von farbigen Bauklötzen. Die Bauklötze werden nach Farbe sortiert. Jetzt hat jeder Haufen genau eine Farbe und zwar die gleiche die auch ein einzelner Bauklotz aus dem Haufen hat.
formaler: Gegeben ist eine Menge von Bauklötzen und eine Menge von Farben. Jedem Bauklotz wird eine Farbe zugeordnet. Sortiere die Klötze nach Farbe. Der nächste Satz wird beweisen, dass es nur eine Möglichkeit gibt den Häufen eine Farbe zuzuordnen sodass die Farbe eines Steines die gleiche ist wie der Haufen in dem er sich befindet.

2.3.3 Satz 2: Abbildungssatz

Sei $f\colon A \to B$ eine Abbildung, dann definiere auf A die Relation $\sim_f$ durch
$a_1 \sim_f a_2 :\Leftrightarrow f(a_1) = f(a_2)$.

Feststellung: $\sim_f$ ist eine Äquivalenzrelation, wie man sich sofort überlegt.

Sei $f\colon A \to B$ eine Abbildung und $\sim := \sim_f$, dann gibt es genau eine Abbildung $\widetilde{f}\colon A/\sim \to B$, sodass $f = \widetilde{f} \circ \mathrm{nat}$, wobei $\mathrm{nat}\colon A \to A/\sim$ die natürliche Abbildung sei. Ferner gilt:

- $\widetilde{f}$ ist injektiv.
- falls f surjektiv ist, dann ist $\widetilde{f}$ sogar bijektiv.
  Beispiel: Bauklotz $\to$ Farbe: Bauklötze werden nach Farben sortiert. Jeder Haufen wird einer Farbe zugeordnet. Bijektiv: Jeder Haufen wird einer Farbe zugeordnet und jede Farbe kommt vor.

Beweis:
Eindeutigkeit: Gelte $\widetilde{f} \circ \mathrm{nat} = f = \hat{f} \circ \mathrm{nat}$. Zu zeigen: $\widetilde{f} = \hat{f}$. Sei $x \in A/\sim_f$, dann gibt es ein $a \in A$ mit $[a] = \mathrm{nat}(a) = x$. Also $\widetilde{f}(x) = \widetilde{f}(\mathrm{nat}(a)) = f(a) = \hat{f}(\mathrm{nat}(a)) = \hat{f}(x)$, also $\widetilde{f} = \hat{f}$.

Existenz: Definiere $\widetilde{f}([a]) := f(a)$. Zu zeigen: $\widetilde{f}$ ist wohldefiniert, d. h. repräsentantenunabhängig, d. h. zu zeigen: $[a_1] = [a_2] \Rightarrow \widetilde{f}([a_1]) = \widetilde{f}([a_2])$.

$[a_1] = [a_2] \Rightarrow a_1 \sim a_2 \Rightarrow f(a_1) = f(a_2)$. (Nach Definition von $\sim$).

- $\widetilde{f}$ injektiv: Zu zeigen: $\widetilde{f}(x_1) = \widetilde{f}(x_2) \Rightarrow x_1 = x_2$. Sei $\widetilde{f}(x_1) = \widetilde{f}(x_2)$. Nach Definition von $A/\sim$ gibt es $a_1, a_2 \in A$ mit $x_1 = [a_1] = \mathrm{nat}(a_1), x_2 = [a_2] = \mathrm{nat}(a_2)$ also $f(a_1) = \widetilde{f}(\mathrm{nat}(a_1)) = \widetilde{f}(x_1) = \widetilde{f}(x_2) = \widetilde{f}(\mathrm{nat}(a_1)) = f(a_2)$, also $a_1 \sim a_2$, also $x_1 = [a_1]_\sim = [a_2]_\sim = x_2$.
- falls $f = \widetilde{f} \circ \mathrm{nat}$ surjektiv ist, dann ist $\widetilde{f}$ surjektiv, also insgesamt bijektiv: $A \xrightarrow{f} B \xrightarrow{g} C \to g(f(A)) = (g \circ f)(A)$.■

2.3.4 Das Auswahlaxiom

Definition: Eine Folge in M (M Menge) ist eine Abbildung $f\colon \mathbb{N} \to M$. Schreibweise: $(x_i)_{i\in\mathbb{N}}$ bedeutet $f(i) =: x_i$.

Feststellung

Falls $A \neq \emptyset$ und $f\colon A \to B$ injektiv ist, dann gibt es eine Abbildung $g\colon B \to A$ mit $g \circ f = id_A$.

Frage: Sei $f\colon A \to B$ surjektiv, gibt es dann eine Abbildung $g\colon B \to A$ mit $f \circ g = id_B$?

Beweisanfang: Sei $b \in B$ Wähle aus $f^{-1}(\{b\})(\neq \emptyset)$ ein Element $\alpha \in f^{-1}(\{b\})$ beliebig und definiere $g(b) := \alpha$ usw. Dann gilt: $(f \circ g)(b) = b$. Falls B endlich ist, ist der Beweis okay. Falls B unendlich ist bedeuted eine solche Auswahl die Existenz einer gewissen (unendlichen) Menge nähmlich $g \subseteq B \times A$, die nicht durch eine Aussage definiert ist.

Definition: Sei $M \neq \emptyset$ eine Menge und m eine Zerlegung von M. Eine Auswahlmenge von m ist eine Teilmenge $A \subseteq M$, sodass für alle $B \in m$ der Durchschnitt $A \cap B$ genau ein Element enthält. Auswahlaxiom: Für jede Menge $M \neq \emptyset$ und jede Zerlegung m von M gibt es eine Auswahlmenge. Äquivalent zum Auswahlaxiom ist wegen Satz 1: Für jede Menge M und jede Äquivalenzrelation $\sim$ auf M gibt es ein vollständiges **Repräsentantensystem** A von $M/\sim$, d. h. A enthält aus jeder Äquivalenzklasse (bezüglich $\sim$) genau ein Element.

Beispiel: Eine Klassenstufe wählt einen Klassensprecher. Die Menge der Klassensprecher einer Schule ist ein vollständiges Repräsentantensystem.

2.3.5 Satz 3: Anwendung des Auswahlaxioms

Die folgende Aussage ist äquivalent zur Gültigkeit des Auswahlaxioms: $(*)$ Zu jeder surjektiven Abbildung $f\colon A \to B$ gibt es eine Abbildung $g\colon B \to A$ mit $f \circ g = id_B$.

Beweis:
Gelte das Auswahlaxiom. Zeige, dass dann $f\colon A \to B$ surjektiv.

Betrachte $\{\{\{(a,b) \mid a \in f^{-1}(b)\}\} \mid b \in B\}$. Dies ist eine Zerlegung der Relation $f \subseteq A \times B$. Sei G eine Auswahlmenge dieser Zerlegung (also insbesondere $G \subseteq f$). Dann ist $g := G^{-1}$ die gesuchte Abbildung $g\colon B \to A$, denn zu jedem $b \in B$ gibt es genau ein $a \in A$ mit $(a,b) \in G$ und das ist äquivalent zu $f(a) = b$, weil $(a,b) \in G \subseteq f$, also $f \circ g = id_B$.

Umgekehrt: Gelte $(*)$ und sei $\sim$ eine Äquivalenzrelation auf M, dann betrachte nat$\colon M \to M/\sim$ ist surjektiv. Nach (*) gibt es eine Abbildung $g\colon M/\sim \to M$ mit nat $\circ\, g = id_{M/\sim}$. $g(M/\sim)$ ist die gesuchte Auswahlmenge.■

2.3.6 Allgemeines kartesisches Produkt

Definition: Sei $(M_i)_{i\in I}$ eine Familie von Mengen, formal: $M\colon I \to m,\ i \mapsto M_i$ Abbildung, $M_i := M(i)$ für $i \in I$, m ist Menge von Mengen. Es gilt:

$\prod_{i\in I} M_i := \{x\colon I \to \bigcup_{i\in I} M_i \mid x \text{ Abbildung, sodass für alle } i \in I \text{ stets } x(i) \in M_i \text{ gilt}\}$.

Schreibweise:
x_i für $x(i)$

Die k-te Projektion (für $k \in I$) ist definiert durch $p_k\colon \prod_{i\in I} M_i \to M_k$ mit $p_k(x) := x(k) = x_k$ für alle $x \in \prod_{i\in I} M_i$.

Beispiel: Für $I = \mathbb{N}, M_i = \mathbb{R}$ ist $\prod_{i\in I} M_i = \prod_{i\in\mathbb{N}} \mathbb{R} =: \mathbb{R}^{\mathbb{N}}$ = die Menge aller Folgen reeller Zahlen.

Definition:

$$\underbrace{A \times \cdots \times A}_{n-\text{mal}} := A^n := \Pi_{i\in\{1,\ldots,n\}} A$$

Schreibweise für ein $x = \{(1,x_1),\ldots,(n,x_n)\} \in A^n$:

$$(x_1,\ldots,x_n)$$

2.3.7 Satz 4: Kartesisches Produkt (mit AC)

AC (= Auswahlaxiom) ist äquivalent zu: Alle kartesischen Produkte von Familien nichtleerer Mengen ist nicht leer. Der Beweis ist sehr einfach.■

2.3.8 Zornsches Lemma (mit AC)

Sei $(M, \leq)$ eine nichtleere partiell geordnete Menge, sodass jede Kette in M eine obere Schranke hat. Dann gibt es (mindestens) ein maximales Element in M.

Zur Erinnerung: eine Kette in M ist eine Teilmenge die bezüglich $\leq$ linear geordnet ist.■

2.3.9 Definition: Wohlordnung

Eine Totalordnung (lineare Ordnung) $\leq$ auf einer Menge M heißt eine Wohlordnung (und $(M, \leq)$ eine wohlgeordnete Menge), falls jede nichtleere Teilmenge ein kleinstes Element hat.

Beispiel: $(\mathbb{N}, \leq)$ ist wohlgeordnet.

2.3.10 Wohlordnungssatz (mit AC)

Auf jeder Menge M gibt es eine **Wohlordnung**. Behauptung: Sowohl das zornsche Lemma, als auch der Wohlordnungssatz sind zu AC äquivalent.

Beweis:
lang und schwierig.■

Wohlordnungssatz $\Rightarrow$ (AC): Sei m eine Zerlegung von M, sei $\leq$ eine Wohlordnung auf M, dann ist $\{\min A \mid A \in m\}$ eine Auswahlmenge.

Definition: Zwei Mengen A, B heißen gleichmächtig, geschrieben $|A| = |B|$ (oder $\operatorname{card} A = \operatorname{card} B$), falls es eine bijektive Abbildung $f\colon A \to B$ gibt.

Feststellung:

Offensichtlich gilt für alle Mengen A, B, C:

i)	$\lvert A\rvert = \lvert A\rvert$	Beweis:	id_A
ii)	$\lvert A\rvert = \lvert B\rvert \Rightarrow \lvert B\rvert = \lvert A\rvert$	Beweis:	$f\colon A \to B$ bijektiv $\Rightarrow f^{-1}\colon B \to A$ bijektiv
iii)	$\lvert A\rvert = \lvert B\rvert \wedge \lvert B\rvert = \lvert C\rvert \Rightarrow \lvert A\rvert = \lvert C\rvert$	Beweis:	f, g bijektiv $\Rightarrow g \circ f$ bijektiv ■

2.3.11 Mächtigkeiten

Eine Menge B heißt mächtiger oder gleichmächtig in Relation zu einer Menge A, falls es eine injektive Abbildung $f\colon A \to B$ gibt. Geschrieben $|A| \leq |B|$ (oder $\operatorname{card} A \leq \operatorname{card} B$).

Feststellung:

Offenbar gilt:
i) $|A| \leq |A|$
ii) $|A| = |B| \Rightarrow |A| \leq |B|$
iii) $|A| \leq |B| \wedge |B| \leq |C| \Rightarrow |A| \leq |C|$ ■

2.3.12 Bernsteins Mächtigkeitssatz

Wenn es injektive Abbildungen $f\colon A \to B, g\colon B \to A$ gibt, dann gibt es eine bijektive Abbildung $h\colon A \to B$. Also $|A| \leq |B| \wedge |B| \leq |A| \Rightarrow |A| = |C|$.

Beweis:
Konstruieren Sie eine bijektive Abbildung $h\colon A \to B$, sodass $h(a) = b \Rightarrow f(a) = b \vee g(b) = a$) (Fallunterscheidung).■

2.3.13 Satz: Vergleichbarkeit (mit AC)

Für je zwei Mengen A, B gilt: $|A| \leq |B|$ oder $|B| \leq |A|$.■

Feststellung:

Für alle Mengen M gilt $|M| \leq |\mathcal{P}(M)|$ (klar: $a \mapsto \{a\}$). Es gilt: $|M| \neq |\mathcal{P}(M)|$.

Bezeichnung: Statt $|A| \leq |B| \wedge |A| \neq |B|$ schreibt man auch $|A| < |B|$. (Beispiel: Es gilt, dass $|M| < |\mathcal{P}(M)|$) ■

Feststellung:

Falls AC gilt, dann gilt: Wenn es eine surjektive Abbildung $f\colon A \to B$ gibt, dann gilt $|B| \leq |A|$.

Beweis:
Folgt aus Satz 3.

Bemerkung:
Es gilt: $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ (Vergl. Analysis).■

2.3.14 Frage/Hypothese zum AC

Gibt es eine Menge A mit $|\mathbb{N}| < |A| < |\mathcal{P}(\mathbb{N})|$? Es stellt sich heraus (P. Cohen 1963): Die Nichtexistenz einer solchen Menge ist unabhängig von den übrigen Axiomen der Mengenlehre (einschl. Auswahlaxiom).

(CH) Kontinuumshypothese: Es gibt keine Menge A mit $|\mathbb{N}| < |A| < |\mathcal{P}(\mathbb{N})|$.
(GCH) verallgemeinerte Kontinuumshypothese: Für jede unendliche Menge M gilt: Es gibt keine Menge A mit $|M| < |A| < |\mathcal{P}(M)|$.
Satz: (GCH) $\Rightarrow$ (AC).

2.3.15 Axiomensystem Zermelo-Fraenkel mit AC (ZFC)

- Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente enthalten.
- Sei M eine Menge und $P(x)$ ein Prädikat (Aussageform), das für jedes $x \in M$ entweder wahr oder falsch ist, dann ist $\{x \in M \mid P(x)\}$ eine Menge.
- Wenn A, B Mengen sind, dann ist $\{A, B\}$ eine Menge.
- Wenn m eine Menge von Mengen ist, dann ist $\bigcup m$ eine Menge.
- Wenn M eine Menge ist, dann ist die Potenzmenge von M eine Menge.
- Unendlichkeitsaxiom: Es gibt eine Menge M, für die gilt:
  - $\emptyset \in M$
  - falls $x \in M$, dann ist auch $x \cup \{x\} \in M$
- AC (Auswahlaxiom)
- Fundierung: Es gibt keine unendlich absteigende Kette bezüglich der Elementrelation, d. h. eine Folge $(M_i)_{i\in\mathbb{N}}$ mit $M_{i+1} \in M_i$ für alle $i \in \mathbb{N}$ ist ausgeschlossen.

Sei $n \in \mathbb{N}_0$, dann bezeichne:

- $\underline{n} := \{0, \ldots, n-1\}$
- $\underline{0} = \emptyset$
- $\underline{1} = \{\emptyset\}$
- $\underline{2} = \{\emptyset, \{\emptyset\}\}$
- $\underline{3} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
- ...

2.3.16 Endlichkeit

Eine Menge heißt endlich, falls es ein $n \in \mathbb{N}_0$ gibt, mit $|M| = |\underline{n}|$. Statt $|M| = |\underline{n}|$ schreibt man auch $|M| = n$. M heißt unendlich, falls M nicht endlich ist.

2.3.17 Sätze zu endlichen Mengen

Feststellung

Seien $n, m, \widetilde{n} \in \mathbb{N}_0$.

- a) Falls $|M| = n$ und $|M| = m$ dann folgt $n = m$.
- b) Falls $|M| = n$ und $\widetilde{M} \subseteq M$ mit $\widetilde{M} \neq M$, dann gibt es ein $\widetilde{n} < n$ mit $|\widetilde{M}| = \widetilde{n}$.
- c) Falls M_1 und M_2 endlich sind, dann gilt: $|M_1 \cup M_2| = |M_1| + |M_2| - |M_1 \cap M_2|$.
- d) Falls M endlich ist und $|M| = |N|$ und $f\colon M \to N$ eine Abbildung ist, dann gilt: f ist injektiv genau dann, wenn f surjektiv ist.

Beweis:
a), b), c) sind klar und formal mit vollständiger Induktion nachweisbar.

zu d)
Sei $f\colon M \to N$ injektiv, dann ist:

$$f|^M := \begin{array}{l} M \to f(M) \\ x \mapsto f(x) \end{array}$$

bijektiv. Also $|N| = |M| = |f(M)|$ (nach Voraussetzung). Also folgt: $f(M) \subseteq N$, also $f(M) = N$ (wegen b)), also f bijektiv. Rückbeweis ist ähnlich.

Schreibweise: $|\mathbb{N}| = \aleph_0$ (sprich: aleph Null)■

Satz mit abzählbarem AC

Falls M unendlich ist, dann gilt $|\mathbb{N}| \leq |M|$.

Idee:
Wähle nacheinander verschiedene Elemente $x_1, x_2, x_3, \ldots$ aus M aus, also $x_n \in M \setminus \{x_1, \ldots x_{n-1}\}$. Entweder gibt es ein $m \in \mathbb{N}$ mit $\{x_1, \ldots x_m\} = M$, dann wäre M endlich ($|M| = m$), oder andernfalls ist $f\colon \mathbb{N} \to M$ und $f(n) := x_n$ eine injektive Abbildung, also $|\mathbb{N}| \leq |M|$.■

2.3.18 Abzählbare Mengen

Definition: Eine Menge M heißt abzählbar, falls $|M| \leq |\mathbb{N}|$. M heißt **abzählbar unendlich**, falls gilt $|M| = |\mathbb{N}|$. M heißt **überabzählbar**, falls $|\mathbb{N}| < |M|$ (Sagt man, dass M abzählbar sei, meint man also: M ist endlich oder abzählbar unendlich).

Folgerung mit AC:
Eine Menge ist genau dann unendlich, wenn es eine injektive Abbildung $f\colon M \to M$ gibt, die nicht surjektiv ist.

Beispiele:

1) $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = n + 1$ ist injektiv aber nicht surjektiv.
2) $|\mathbb{N}| = |2\mathbb{N}|$ $2\mathbb{N} := \{2n \mid n \in \mathbb{N}\}$: Menge der geraden natürlichen Zahlen ist gleichmächtig zur Menge aller natürlichen Zahlen.

Beispiel:
Gegeben sei ein Hotel mit unendlich vielen Zimmern. Das Hotel ist voll belegt. Es kommt ein Reisebus mit abzählbar unendlich vielen Fahrgästen. Um Platz zu schaffen, wird jeder Gast im Hotel auf das Zimmer mit der doppelten Zimmernummer verlegt.

Feststellung:

$\mathbb{N} \times \mathbb{N}$ ist abzählbar unendlich.■

Feststellung:

$\mathbb{N}^n$ für $n \in \mathbb{N}$ ist auch abzählbar.■

Feststellung:

Sei $m \subseteq \mathcal{P}(M)$ und gelte m ist abzählbar und jedes Element von m ist abzählbar, dann ist auch $\cup m$ abzählbar, d. h. abzählbare Vereinigungen von abzählbaren Mengen sind abzählbar. ■

3 Algebraische Grundstrukturen

Gruppen, Ringe, Körper

3.1 Gruppe

Definition: Eine Gruppe $(G, \circ)$ ist eine **Menge G zusammen mit einer Abbildung** $\circ\colon G \times G \to G, (a, b) \mapsto a \circ b$, sodass gilt:

- i) Für alle $a, b, c \in G$ gilt: $a \circ (b \circ c) = (a \circ b) \circ c$ (Assoziativgesetz)
- ii) Es gibt ein Element $e \in G$ mit $a \circ e = a = e \circ a$ für alle $a \in G$ ($e :=$ neutrales Element).
- iii) Für alle $a \in G$ gibt es ein $b \in G$ mit $a \circ b = e = b \circ a$ ($b :=$ zu a inverses Element).

Definition: Falls $(G, \circ)$ eine Gruppe ist und zusätzlich gilt:

- iv) $a \circ b = b \circ a$ für alle $a, b \in G$ (Kommutativgesetz), dann heißt G eine abelsche[4] Gruppe.

3.1.1 Feststellung 7: Gruppeneigenschaften

Sei $(G, \circ)$ eine Gruppe, dann gilt:

- Es gibt genau ein neutrales Element $e_G \in G$, $e := e_G$ mit $ea = ae = a$ für alle $a \in G$. e heißt also das neutrale Element von G (bezüglich $\circ$).
- $ba = e \Rightarrow ab = e$ für alle $a, b \in G$.
- Das Inverse ist eindeutig, meist geschrieben als a^{-1}.
- Für alle $a, b \in G$ gilt: $(ab)^{-1} = b^{-1}a^{-1}$ mit $(a^{-1})^{-1} = a$.
- Für alle $a, x, y \in G$ gilt: $(ax = ay \Rightarrow x = y)$ und $(xa = ya \Rightarrow x = y)$.

Beweis:

- angenommen e, e' seien neutrale Elemente, dann folgt $e = ee' = e'$.
- Nach ii) b) gibt es ein $c \in G$ mit $cb = e$ also $ab = (ea)b = ((cb)a)b = (c(ba))b = ceb = cb = e$.
- Sei a, $b \in G$. Angenommen $ba = ca = e$ wegen ii) folgt $ab = ac = e$, also $b = eb = (ca)b = c(ab) = ce = c$.
- $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}(a^{-1}a)b) = b^{-1}eb = b^{-1}b = e$ also $b^{-1}a^{-1} = (ab)^{-1}$. Weiter: $aa^{-1} = a^{-1}a = e$, also $a = a(a^{-1})^{-1}$.
- $ax = ay \Rightarrow x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = ey = y$. $xa = ya \Rightarrow x = y$ analog.■

Schreibweise: In abelschen Gruppen bezeichnet man oft die Verknüpfung mit $+$, das neutrale Element mit 0 statt e und das Inverse von a mit $-a$.

[4] nach Nils Abel

3.1.2 Beispiele für Gruppen

- Sei M eine Menge. Sei $\mathrm{S}(M) := \{f\colon M \to M \mid f \text{ bijektiv }\}$, dann ist $(\mathrm{S}(M), \circ)$ eine Gruppe (mit $\circ$ Komposition von Abbildungen). Sie heißt auch die **symmetrische Gruppe** auf M. Insbesondere bezeichne $S_n := \mathrm{S}(\{1, \ldots, n\})$.

Definition:
Eine Abbildung $M \times M \to M, (a, b) \mapsto ab$ heißt eine **Verknüpfung** auf M. Sie heißt assoziativ, falls für alle $a, b, c \in M$ gilt: $a(bc) = (ab)c$.

3.1.3 Halbgruppe

Eine Halbgruppe $(M, \circ)$ ist eine Menge M mit einer **assoziativen Verknüpfung**.

Beispiele:

$(\mathrm{S}(M), \circ)$	Gruppe
$(\mathbb{N}, +)$	Halbgruppe
$(\mathbb{Z}, +)$	Gruppe
$(\mathbb{Q}, \cdot)$	Halbgruppe
$(\mathbb{Q} \setminus \{0\}, \cdot)$	Gruppe

Sei Σ eine Menge (Alphabet). Σ^* ist die Menge aller Wörter (endliche Folgen von Buchstaben, also Elementen von Σ). Das leere Wort besteht aus keinem Buchstaben. Das Hintereinanderschreiben der Worte als Verknüpfung ist eine Halbgruppe.

3.1.4 Feststellung: Beklammerung bei inversen Verknüpfungen

Sei $M \times M \to M$ eine Verknüpfung. Dann gilt: Jeder Ausdruck mit beliebiger sinnvoller Beklammerung beschreibt dasselbe Element, d. h. man kann die Klammern weglassen, falls keine Missverständnisse zu erwarten sind. $(ab)(cd) = a(b(cd))$

Beweis:
wird weggelassen (einfach, aber langwierig)

Beispiele:

- $\cup : \mathcal{P}(M) \times \mathcal{P}(M) \to \mathcal{P}(M)$ ist eine assoziative Verknüpfung.
- $Abb(M, M) \times Abb(M, M) \to Abb(M, M)$ mit $(f, g) \mapsto f \circ g$ ist eine assoziative Verknüpfung. Die Menge der Abbildungen von M nach M genannt M^M.

Beispiel:
$M := \{0, 1, 2\}$, $(\{\} \cup \{1\}) \cup \{2, 3\} = \{\} \cup (\{1\} \cup \{2, 3\})$ Beispiel:
$f(x) = x^2$, $g(x) = 2x$, $h(x) = 3x$
$((f \circ g) \circ h)(x) = (2(3x))^2 = (f \circ (g \circ h))(x)$

Bezeichnung:
Sei $(G, \circ)$ eine Gruppe, $A, B \subseteq G$. Dann bezeichne $AB := \{ab \mid a \in A, b \in B\}$ das Komplexprodukt. $A^{-1} := \{a^{-1} \mid a \in A\}$. Für $a \in G$ schreibe aB für $\{a\}B$ und Ba für $B\{a\}$.■

3.1.5 Untergruppen

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Eine Untergruppe U (geschrieben $U \trianglelefteq G$.) ist eine Teilmenge von G, sodass gilt:

1) $e \in U$
2) $x \in U \Rightarrow x^{-1} \in U \quad (\Leftrightarrow \quad U^{-1} = U)$
   $(x^{-1} \in U \Rightarrow x \in U$ wegen $(x^{-1})^{-1} = x)$
3) $x, y \in U \Rightarrow xy \in U \quad (\Leftrightarrow \quad UU = U)$

Die Äquivalenzen sind einfach zu zeigen.

3.1.6 Feststellung 8: Gruppe mit Einschränkung

Sei $(G, \circ)$ eine Gruppe, U eine Untergruppe, dann ist $(U, \circ|^U_{U\times U})$ eine Gruppe, wobei $\circ|^U_{U\times U}$ die Einschränkung der Abbildung $\circ\colon G \times G \to G$ auf $U \times U$ und U ist.
Beweis:
Für $x, y \in U$ ist $x\circ|^U_{U\times U})y \in U$, wegen 3.1.5 3). $\circ|^U_{U\times U}$ ist also wieder eine Funktion.

Bemerkung:
Man schreibt dann wieder $\circ$ statt $\circ|^U_{U\times U}$.■

3.1.7 Links- und Rechtsnebenklasse

Sei $(G, \circ)$ eine Gruppe, U eine Untergruppe. $a \in G$:
aU heißt dann eine **Linksnebenklasse** von U.
Ua heißt dann eine **Rechtsnebenklasse** von U.

3.1.8 Feststellung 9: Gruppe mit Äquivalenzrelation

Sei $(G, \circ)$ eine Gruppe, U eine Untergruppe. Dann gilt:

a) Die Relation $\sim$ definiert durch $a \sim b :\Leftrightarrow aU = bU$ ist eine Äquivalenzrelation auf G.
b) Für alle $a, b \in U$ sind äquivalent:
i) $aU = bU$
ii) $b \in aU$
iii) $a^{-1}b \in U$
c) Die Äquivalenzklasse von a bezüglich $\sim$ ist aU. ($[a]_\sim = aU$)

Beweis:

a) klar
b) *i)* $\Rightarrow$ *ii)*: $b = be \in bU \Rightarrow b \in bU \overset{bU=aU}{\Rightarrow} b \in aU$
ii) $\Rightarrow$ *iii)*: $b \in aU \Rightarrow a^{-1}b \in a^{-1}(aU) = eU = U$
oder: $b \in aU \Rightarrow b \in \{au | u \in U\} \Rightarrow \exists u \in U : au = b \Rightarrow$
$\exists u \in U : u = a^{-1}b \Rightarrow a^{-1}b \in \{u | u \in U\}$
iii) $\Rightarrow$ *i)*: $a^{-1}b \in U \Rightarrow (a^{-1}b)U \subseteq UU = U \Rightarrow bU = a((a^{-1}b)U) \subseteq aU$
$aU \subseteq bU$ entsprechend:
$a^{-1}b \in U \Rightarrow ((a^{-1})b)^{-1} = (b^{-1}a) \in U^{-1} = U$ also $bU \subseteq aU$
c) $a \in aU$ $[a]_\sim \overset{\text{Def}}{=} \{x \in G \mid x \sim a\} = \{x \in G \mid xU = aU\}$
$\overset{b)}{=} \{x \in G \mid x \in aU\} = aU$ ■

3.1.9 Definition: Normalteiler

$U \subseteq G$ heißt ein Normalteiler von G, falls gilt: U ist Untergruppe von G und für alle $a \in G$ gilt: $aU = Ua$. Geschrieben $U \lhd G$.

3.1.10 Feststellung 10: Normalteiler

a) Eine Untergruppe U ist genau dann ein Normalteiler von G, wenn $aUa^{-1} = U$ für alle $a \in G$ gilt.
b) Wenn $(G, \bullet)$ abelsch ist, dann ist jede Untergruppe von $(G, \bullet)$ ein Normalteiler von $(G, \bullet)$.
c) $\{e\}$ und G sind Normalteiler von G.■
d) Sei $U \subseteq G$ eine Untergruppe. Aus $aUa^{-1} \subseteq U$ für alle $a \in G$ folgt, dass U ein Normalteiler ist. Damit ist auch
$a^{-1}Ua = (a^{-1})U(a^{-1})^{-1} \subseteq U$ (ersetze a durch a^{-1}),
also $a \cdot (a^{-1}Ua) \cdot a^{-1} = U \subseteq aUa^{-1}$

3.1.11 Definition: Gruppenhomomorphismus

Seien $(G, \circ), (H, \bullet)$ Gruppen. Ein **(Gruppen-)Homomorphismus** $f\colon G \to H$ ist eine Abbildung, sodass $f(x \circ y) = f(x) \bullet f(y)$ für alle $x, y \in G$.
Ein **Isomorphismus** ist ein bijektiver Homomorphismus. Falls $(G, \circ) = (H, \bullet)$, dann heißt ein Isomorphismus $f\colon G \to G$ ein **Automorphismus** von G.

Beispiel:

$$\exp\colon \quad \begin{array}{l} \mathbb{R} \to \mathbb{R}_+ \\ x \mapsto e^x \end{array} \qquad \mathbb{R}_+ := \{x \in \mathbb{R} \mid x > 0\} = (0, \infty)$$

ist ein Gruppenhomomorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{R}_+, \cdot)$. Da $e^{x+y} = e^x e^y$.■

3.1.12 Feststellung 11: Gruppenhomomorphismus und neutrales Element

Wenn $f\colon G \to H$ ein Gruppenhomomorphismus ist, dann gilt $f(e) = e'$ und $f(a^{-1}) = f(a)^{-1}$ (e bzw. e' neutrales Element von G bzw. H).

Beweis 1:
$e' f(e) = f(e) = f(ee) = f(e)f(e) \Rightarrow e' = f(e)$

Beweis 2:
$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e' = f(a)(f(a))^{-1} \Rightarrow f(a^{-1}) = (f(a))^{-1}$ ■

3.1.13 F 1.6:

Seien $(G_1, \star)$, $(G_2, \bullet)$ und $(G_3, \cdot)$ Gruppen und
$f\colon G_1 \to G_2$, $f\colon G_2 \to G_3$ Homomorphismen. Dann ist $(g \circ f)\colon G_1 \to G_3$ ein Homomorphismus

Beweis:
Für alle $x, y \in G$ gilt:
$(g \circ f)(x \star y) = g(f(x \star y)) \overset{f \text{ Hom.}}{=} g(f(x) \bullet g(x)) \overset{g \text{ Hom.}}{=} g(f(x)) \cdot g(f(y)) = (g \circ f)(x) \cdot (g \circ f)(y)$

3.1.14 Definition: Isomorphie zwischen Gruppen

Zwei Gruppen $(G, \circ), (H, \bullet)$ heißen isomorph, geschrieben $G \cong H$, falls es einen Isomorphismus $f\colon G \to H$ gibt. f^{-1} ist dann ebenfalls ein Isomorphismus. (Aufgabe)

3.1.15 Definition und Folgerung:

Sei $(G, \cdot)$ eine Gruppe. Bezeichne $\mathrm{Aut}(G) := \{f \mid f\colon G \to G \text{ Automorphismus}\}$. $(\mathrm{Aut}(G), \circ)$ ist dann eine Untergruppe von $(\mathrm{S}(G), \circ) = (\{f\colon G \to G \mid f \text{ bijektiv }\}, \circ)$.

3.1.16 Definition und Proposition(wichtige Feststellung): Faktorgruppe

Sei $(G, \cdot)$ eine Gruppe und N ein Normalteiler. Bezeichne $G/N := \{a \cdot N \mid a \in G\}$ die Menge der Linksnebenklassen. Dann ist: $(*)$

$$(a \cdot N) \cdot (b \cdot N) \underbrace{=}_{\text{nach def } N \text{ Normalteiler}} (a \cdot N) \cdot (N \cdot b) \underbrace{=}_{\text{assoziativ, weil } N \text{ Gruppe}} a \cdot (N \cdot N) \cdot b$$

$$\underbrace{=}_{\text{da } N \text{ Untergruppe: } N \cdot N = N} a \cdot N \cdot b \underbrace{=}_{\text{nach def } N \text{ Normalteiler}} (a \cdot b) \cdot N$$

Die Linke Seite hängt nicht von der Auswahl der Repräsentanten ab. Folglich gilt:
$\bullet\colon G/N \times G/N \to G/N, ((a \cdot N), (b \cdot N)) \mapsto (a \cdot b)N$, $((a \cdot N) \bullet (b \cdot N) := (a \cdot N) \cdot (b \cdot N))$ ist eine wohldefinierte Verknüpfung. Ferner gilt für diese Verknüpfung das Assoziativgesetz, $e \cdot N = N$ ist das neutrale Element und $a^{-1} \cdot N$ das inverse Element von $a \cdot N$ in G/N. $(a^{-1} \cdot N) \cdot (a \cdot N) = (a^{-1} a \cdot N) = N$.

Also ist $((G/N), \bullet)$ eine Gruppe und $\mathrm{nat}\colon G \to G/N$ mit $\mathrm{nat}(x) := x \cdot N$ ein Homomorphismus, denn $\mathrm{nat}(x \cdot y) = (x \cdot y) \cdot N \overset{(*)}{=} (x \cdot N) \cdot (y \cdot N) = \mathrm{nat}(x) \cdot \mathrm{nat}(y) = \mathrm{nat}(x) \bullet \mathrm{nat}(y)$.

$(G/N, \bullet)$ heißt die Faktorgruppe von G modulo N und $\mathrm{nat}\colon G \to G/N$ der natürliche Homomorphismus. $N \subseteq G$ sei immernoch ein Normalteiler.

nat	$G \to G/N$	der natürliche Homomorphismus
	$g \mapsto g \cdot N$	

Beispiel:
Sei $n \in \mathbb{Z}$. Die zyklische Gruppe Z_n ist die Faktorgruppe von $(\mathbb{Z}, +)$ modulo $n\mathbb{Z}$, also $Z_n := (\mathbb{Z}/n\mathbb{Z}, +)$. $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ ist eine Untergruppe von $(\mathbb{Z}, +)$. $n\mathbb{Z}$ ist Normalteiler, da $(\mathbb{Z}, +)$ abelsch ist.

Schreibweise:
Für $u, v, w, n \in \mathbb{Z}$. $u + v \equiv w \bmod n$ bedeutet

$$n|((u + v) - w), \quad \text{d. h. } (u + (n\mathbb{Z})) + (v + (n\mathbb{Z})) = (w + (n\mathbb{Z}))$$

Beispiel:

$$Z_5 = \mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$$

Kurzschreibweise:

$$Z_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$$

Also zum Beispiel

$$[2]_5 + [3]_5 = 2 + 5\mathbb{Z} + 3 + 5\mathbb{Z} = 2 + 5\mathbb{Z} + 3 + 5\mathbb{Z} = 5 + 5\mathbb{Z} = 5\mathbb{Z} = [0]_5$$

in $Z_5 (2 + 3 \equiv 0 \bmod 5)$.

Z_{12} entspricht dem Ziffernblatt auf einer Analoguhr.
Die zyklische Gruppe Z_n hat genau n Elemente: $n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, n-1+n\mathbb{Z}$ oder $[0]_n, [1]_n, \ldots [n-1]_n$.

3.1.17 Feststellung und Definition: Produkt zweier Gruppen

Das Produkt zweier Gruppen $(G, *), (H, \star)$ ist die Gruppe $(G \times H, \circ)$ mit $(g_1, h_1) \circ (g_2, h_2) := (g_1 * g_2, h_1 \star h_2)$.

Der Beweis, dass dies eine Gruppe ist, erfolgt durch einfaches Nachrechnen, z. B. (e, e') ist das neutrale Element, wenn e das neutrale Element in G ist und e' das neutrale Element in H ist. $(a, b)^{-1} = (a^{-1}, b^{-1})$ ist das inverse Element.

3.1.18 Feststellung: Projektion

Die Projektionen P_1, P_2 aus $(G \times H, \circ)$ sind Homomorphismen.
$P_1((g_1,h_1)\circ(g_2,h_2)) = P_1(g_1 * g_2, h_1 \star h_2) = g_1 * g_2 = P_1(g_1,h_1) * P_1(g_1,h_2)$.
$P_2((g_1,h_1)\circ(g_2,h_2)) = P_2(g_1 * g_2, h_1 \star h_2) = h_1 \star h_2 = P_2(g_1,h_1) * P_2(g_1,h_2)$.

$P_1 \colon G \times H \to G, (g,h) \mapsto g$
$P_2 \colon G \times H \to H, (g,h) \mapsto h$

Die Beschreibung einer Verknüpfung kann durch eine Verknüpfungstabelle erfolgen:
Bild nicht verfügbar![width=2cm]Z3.png Abbildung 24 :Verknüpfungstabelle: Z_3.■

Seien im Folgenden $(G,\cdot),(H,\cdot)$ Gruppen, $e \in G, e' \in H$ neutrale Elemente.

3.1.19 Proposition 12: Untergruppen und Normalteiler

Sei $f \colon G \to H$ ein Homomorphismus von $(G,\cdot)$ nach $(H,\cdot)$.

a) Sei $U \subseteq G$ eine Untergruppe. Dann ist $f(U) \subseteq H$ eine Untergruppe.
b) Sei $V \subseteq H$ eine Untergruppe. Dann ist $f^{-1}(V) \subseteq G$ eine Untergruppe.
c) Sei $N \subseteq H$ ein Normalteiler. Dann ist $f^{-1}(N) \subseteq G$ ein Normalteiler.

Beweis:

a) Seien $v_1, v_2 \in f(U)$. Dann gibt es $u_1, u_2 \in U$ mit $v_1 = f(u_1)$,
$v_2 = f(u_2)$ also $v_1 v_2 = f(u_1)f(u_2) = f(u_1 u_2) \in f(U)$, da $u_1 u_2 \in U$,
wegen Untergruppe.
$e' = f(e) \in f(U)$ und $v^{-1} = f(u)^{-1} = f(u^{-1}) \in f(U)$
(vergl. Feststellung 11, $v = f(u)$).
b) Seien $u_1, u_2 \in f^{-1}(V)$, d. h. $f(u_1) \in V, f(u_2) \in V$, also $u_1 u_2 \in f^{-1}(V)$,
da $f(u_1 u_2) = f(u_1)f(u_2) \in V$.
$u_1^{-1} \in f^{-1}(V)$, da $f(u_1^{-1}) = f(u_1)^{-1} \in V, e \in f^{-1}(V)$, da $f(e) = e' \in V$,
$\Rightarrow f^{-1}(V) \subseteq G$ ist eine Untergruppe.
c) Sei $N \subseteq H$ ein Normalteiler. Dann ist $f^{-1}(N) \subseteq G$ eine Untergruppe
(nach b)). Für alle $a \in G, x \in f^{-1}(N)$ gilt außerdem
$f(axa^{-1}) = f(a)f(x)f(a)^{-1} \in f(a)Nf(a)^{-1} = N$,
also $axa^{-1} \in f^{-1}(N)$, also ist $af^{-1}(N)a^{-1} \subseteq N$, also $f^{-1}(N)$ ist
Normalteiler von G.■

3.1.20 Definition: Kern

Sei $f \colon G \to H$ ein Homomorphismus, $e' \in H$ neutrales Element.
$\ker(f) := f^{-1}(\{e'\}) = \{a \in G \mid f(a) = e'\}$ heißt der Kern von f. Der Kern besteht also aus allen Elementen von G, die auf das neutrale Element e' von H abgebildet werden.

Eselsbrücke: Im Kern sind alle Elemente die über f stolpern und hinfallen.
Feststellung

Nach Proposition 12 c) ist $\ker(f)$ ein Normalteiler in G.■

Bemerkung:
Wir betrachten den Homomorphismus

$$\varphi\colon G \to Aut(G), a \mapsto (x \mapsto axa^{-1}).$$

$$a(xy)a^{-1} = ax(e)ya^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})(aya^{-1})$$

$\varphi(G) \subseteq Aut(G)$ ist nach Proposition 12 a) eine Untergruppe. Die Automorphismen $\varphi(G)$ heißen innere Automorphismen, d. h. $f \in Aut(G)$ ist genau dann ein **innerer Automorphismus**, wenn es ein $a \in G$ gibt mit $f(x) = axa^{-1}$ für alle $x \in G$.

3.1.21 Feststellung 13: Innerer Automorphismus

Sei $U \subseteq G$ eine Untergruppe, dann gilt: U ist genau dann ein Normalteiler von G, wenn $f(U) = U$ für alle inneren Automorphismen $f\colon G \to G$.

Beweis:
$f(U) = U$ für alle inneren Automorphismen $\Leftrightarrow aUa^{-1} = U$ für alle $a \in G \overset{3.1.10d)}{\Leftrightarrow} U$ ist ein Normalteiler von G.■

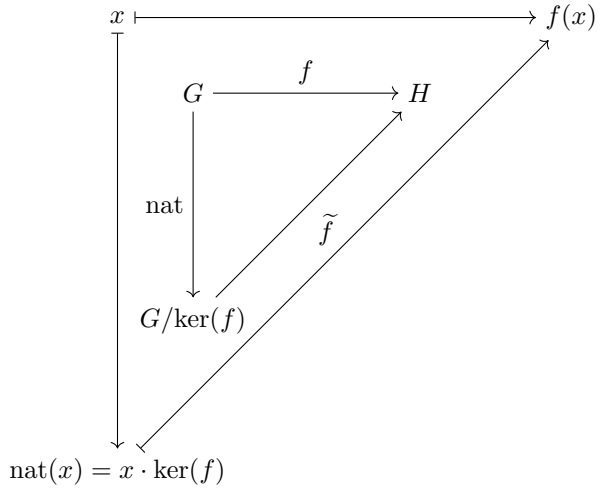
3.1.22 Feststellung 14: Natürlicher Homomorphismus

Sei N ein Normalteiler und $\mathrm{nat}\colon G \to G/N$ der natürliche Homomorphismus. Dann gilt: $\ker(\mathrm{nat}) = N$.

Beweis: (N ist Neutrales Element in $(G/N, \cdot)$)
$a \in \ker(\mathrm{nat}) \Leftrightarrow a \in \mathrm{nat}^{-1}(\{eN\}) \Leftrightarrow \mathrm{nat}(a) \in \{eN\} \Leftrightarrow \mathrm{nat}(a) = eN \Leftrightarrow aN = N \Leftrightarrow a \in N$.■

3.1.23 Satz 5: Der Homomorphiesatz

Sei $f\colon G \to H$ ein Homomorphismus ($(G,\cdot)$, $(H,\cdot)$ Gruppen). Dann gibt es genau einen Homomorphismus $\widetilde{f}$ von $(G/\ker(f), \overset{3.1.16}{\bullet})$ nach $(H,\cdot)$ mit $\widetilde{f}\circ\mathrm{nat} = f$, wobei $\mathrm{nat}(x) = x\cdot\ker(f)$ der natürliche Homomorphismus ist. Ferner ist $\widetilde{f}$ injektiv. Falls f surjektiv ist, dann ist $\widetilde{f}$ ein Isomorphismus.



Beweis: Zunächst ist

$$x \sim_f a \Leftrightarrow f(x) = f(a) \Leftrightarrow e_H = f(x)^{-1}f(a) = f(x^{-1}a)$$
$$\overset{\text{Def. Kern}}{\Leftrightarrow} x^{-1}a \in \ker(f) \overset{\text{F9. b)}}{\Leftrightarrow} x \in a\cdot\ker(f)$$

wodurch für alle $a \in G$:

$$\mathrm{nat}(a) = a\cdot\ker(f) = \{x \in G \mid x \in a\cdot\ker(f)\} = \{x \in G \mid x \sim_f a\} = [a]_{\sim_f} = \mathrm{nat}_{\sim_f}(a)$$

was wiederum

$$G/\ker(f) = \{a\cdot\ker(f) \mid a \in G\} = \{[a]_{\sim_f} \mid a \in G\} = G/{\sim_f}$$

ergibt. Wir können den Abbildungssatz verwenden (Satz 2). Also gibt es genau eine Abbildung $\widetilde{f}$ mit $\widetilde{f}\circ\mathrm{nat}_{\sim_f} = f$, wobei die natürliche Abbildung nat $\sim_f$ definiert ist durch: $\mathrm{nat}_{\sim_f}(a) = [a]_{\sim_f}$. Ferner gilt:

$$\begin{aligned}\widetilde{f}(a\cdot\ker(f) \overset{3.1.14}{\bullet} b\cdot\ker(f)) &= \widetilde{f}(ab\cdot\ker(f)) = \widetilde{f}(\mathrm{nat}(ab)) = f(ab)\\ &= f(a)\cdot f(b) = \widetilde{f}(a\cdot\ker(f))\cdot\widetilde{f}(b\cdot\ker(f))\end{aligned}$$

Also ist $\widetilde{f}$ ein Homomorphismus. Die übrigen Behauptungen folgen aus dem Abbildungssatz.■

3.1.24 Definition Index

Sei G eine **endliche Gruppe**. Dann heißt $|G|$ die Ordnung von G (die Anzahl der Elemente von G). Sei $U \subseteq G$ eine Untergruppe. Definiere durch $G/U := \{aU \mid a \in G\}$ die Menge der Linksnebenklassen. $[G : U] := |G/U|$ heißt der Index von U in G. Achtung: $(G/U, \overset{3.1.14}{\bullet})$ ist nur dann eine Gruppe, wenn U ein Normalteiler ist!

3.1.25 Feststellung 15: Ordnung

Definiere für alle $a \in G$ die bijektiven Abbildungen $a\cdot\_ : G \to G, x \mapsto ax$. Also gilt für die Untergruppe $U \subseteq G$, dass $|U| = |aU|$ für alle $a \in G$. Nach Feststellung 9 bilden die Linksnebenklassen eine Zerlegung von G. Sei $\{a_iU | i \in I\}$ diese Zerlegung, wobei $|I| = |G/U|$. Dann $|G| = \left|\dot{\bigcup}_{i\in I}\{a_iU\}\right| = \sum_{i\in I}|a_iU| = \sum_{i\in I}|U| = |U|\sum_{i\in I}1 = |U| \cdot |I| = |U| \cdot |G/U|$
Also $|G| = |U| \cdot |G/U|$, d. h. die Ordnung von G ist gleich dem Produkt der Ordnung von U und dem Index von U in G. Insbesondere sind $|U|, |G/U|$ Teiler von $|G|$. Die Anzahl der Elemente einer Gruppe ist gleich der Anzahl der Linksnebenklassen mal ihre jeweils gleich große Größe.■

3.1.26 Feststellung 16: Durchschnitt von Untergruppen

a) Sei $\mathfrak{M}$ eine nicht-leere Menge von Untergruppen von G, dann ist der Durchschnitt $\bigcap \mathfrak{M}$ eine Untergruppe von G.
b) Sei $\mathfrak{M}$ ein Normalteiler in G, dann ist $\bigcap \mathfrak{M}$ ein Normalteiler von G.

Beweis: einfache Übung. ■

3.1.27 Definition: Erzeugte Untergruppe

Sei $(G, \cdot)$ eine Gruppe und $M \subseteq G$ eine Teilmenge, dann bezeichne $\langle M\rangle := \bigcap\{U \mid M \subseteq U \trianglelefteq G\}$. $\langle M\rangle$ ist nach Definition die **kleinste Untergruppe** von G die M enthält. $\langle M\rangle$ heißt die von M erzeugte Untergruppe von G.

Analog: Von M erzeugte Normalteiler ist $\bigcap\{N \subseteq |M \subseteq N \lhd G\}$

Beispiel:
$\langle\emptyset\rangle = \{e\}$
In $Z_{12} = \mathbb{Z}/12\mathbb{Z}$ ist $\langle\{[3]\}\rangle = \{[0], [3], [6], [9]\}, [12] = [0]$ in Z_{12}

Schreibweise:
Schreibe auch $\langle a, \ldots, z\rangle$ für $\langle\{a, \ldots, z\}\rangle$.

3.1.28 Definition: Bezeichnung

Für $a \in G, n \in \mathbb{N}$ bezeichne $a^n := \underbrace{a \cdots a}_{n\text{-mal}}$
$a^0 := e$ (neutrales Element)
$a^{-n} := (a^{-1})^n$

3.1.29 Feststellung 17: Surjektiver Gruppenhomomorphismus

Für $a \in G$, wobei $(G, \cdot)$ Gruppe, ist $f\colon \mathbb{Z} \to \langle a \rangle, n \mapsto a^n$ ein surjektiver Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\langle a \rangle, \cdot)$. (eigentlich $(\langle a \rangle, \cdot|)$)

Beweis:
$a^{n+m} = a^n a^m$
f surjektiv: $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ klar.
Formal: mit Induktion ■

3.1.30 Definition: Endliche Ordnung

Sei $a \in G$. Falls es $m \in \mathbb{N}$ gibt, mit $a^m = e$, dann heißt a von endlicher Ordnung und die **kleinste Zahl** $n \in \mathbb{N}$ mit $a^n = e$ heißt die Ordnung von a, geschrieben: $\text{ord}(a) = n$.

Beispiel:
In Z_{12} hat [3] die Ordnung 4. In $(\mathbb{Z}, +)$ hat 1 keine endliche Ordnung.

Schreibweise:
In $(G, +)$ schreibt man $n \cdot a$ für $\underbrace{a + \ldots + a}_{n\text{-mal}}$.
Bemerkung:
Falls $\text{ord}(a) = n$ ist, dann ist $\ker(f) = n\mathbb{Z}$ für $f\colon \mathbb{Z} \to \langle a \rangle$ mit $m \mapsto a^m$ (Beweis klar).

3.1.31 Feststellung 18: Anwendung des Homomorphiesatzes

Falls $\operatorname{ord}(a) = n$ ist, dann ist $\langle a \rangle \cong Z_n$.

Beweis:
Folgerung aus dem Homomorphiesatz mit $f\colon \mathbb{Z} \to \langle a \rangle$, $m \mapsto a^m$ und weil $\ker(f) = n\mathbb{Z}$.

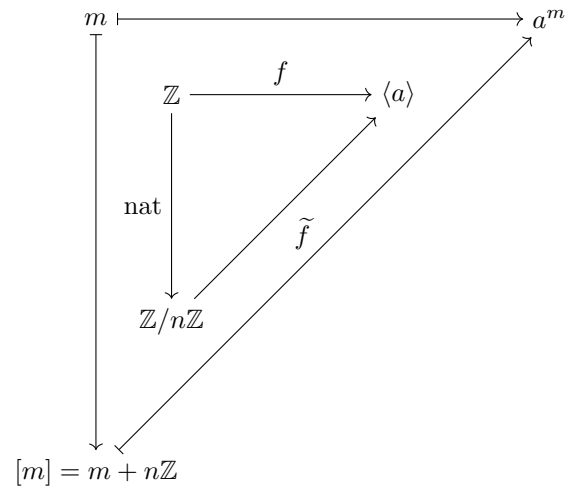


Abbildung 26■

Insbesondere folgt aus Feststellung 18, dass $\langle a \rangle = \{a^0, \ldots, a^{n-1}\}$ und $a^i = a^j \Leftrightarrow i - j \in n\mathbb{Z} \Leftrightarrow i \equiv j \bmod n$, wobei $n := \operatorname{ord}(a)$.

Eine einelementig erzeugte Gruppe G, d. h. es gibt $a \in G$ mit $\langle a \rangle = G$ heißt eine zyklische Gruppe. Wir haben gezeigt, dass eine zyklische Gruppe isomorph ist zu Z_n (für ein $n \in \mathbb{N}$) oder zu $(\mathbb{Z}, +)$

3.1.32 Die symmetrische und die alternierende Gruppe

$S_n := S(\{1, \ldots, n\})$
$S(M) = \{f \mid f\colon M \to M, f \text{ bijektiv}\}$
$(S(M), \circ)$ bildet eine Gruppe.

Definition:
Sei $M \neq \emptyset$. Ein Element $\pi \in \mathrm{S}(M)$ heißt ein **(endlicher) Zyklus**, wenn es endlich viele paarweise verschiedene Elemente $x_1, \ldots, x_m \in M$ gibt, sodass $\pi(x_1) = x_2, \ldots, \pi(x_i) = x_{i+1}$ für $i = 1, \ldots, m-1$ und $\pi(x_m) = x_1$ und $\pi(x) = x$ für alle $x \in M \setminus \{x_1, \ldots, x_m\}$. Man definiert dann $(x_1, \ldots, x_m) := \pi$ und die Länge des Zyklus als m.
Beispiel:
Kinder auf dem Schulhof. Es gibt einen Kreis in dem manche Kinder stehen. Jedes Kind nimmt den Platz seines Nachbarn ein. Kinder außerhalb des Kreises bleiben auf ihrem Platz.

3.1.33 Zyklus

Ein Zyklus der Länge 2 heißt eine **Transposition**. Zwei Zyklen $(x_1, \ldots, x_m)$ und $(y_1, \ldots, y_n)$ heißen elementfremd, wenn $\{x_1, \ldots, x_m\} \cap \{y_1, \ldots, y_n\} = \emptyset$ gilt.

Bemerkung:
Nach Definition ist $(x_1, \ldots, x_m) = (x_2, \ldots, x_m, x_1) = \ldots = (x_{i+1}, \ldots, x_m, x_1, \ldots, x_i) = \ldots$ für $i = 1, \ldots, m-1$

3.1.34 Permutationen

Sei M eine endliche Menge. Die Elemente von $\mathrm{S}(M)$ heißen **Permutationen** von M.
Die Zweizeilenform:

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

Des weiteren wird die Komposition als Produkt geschrieben und bezeichnet ($\circ := \cdot$).
Darstellung einer Permutation als Produkt von elementfremden Zyklen als Beispiel:

$(1, 3, 6, 4)(2)(5, 7)$

3.1.35 Feststellung 19: Eigenschaften von Permutationen

a) Jede Permutation einer endlichen Menge ist das Produkt (Komposition) von elementfremden Zyklen.
b) Das Produkt von zwei elementfremden Zyklen ist unabhängig von der Reihenfolge der Zyklen.
c) Die Darstellung nach a) ist eindeutig, bis auf die Reihenfolge der Zyklen, $(x_1, \ldots, x_k) = (x_2, \ldots, x_k, x_1) = \ldots$ und auf die Angabe von 1-Zyklen (Identitäten).■

Definition:
Ein n-Zyklus ist ein Zyklus der Länge n.

Beispiel:
Das Produkt von zwei Permutationen (schreibe sie direkt hintereinander statt $\circ$) wird als Abbildung aufgefasst, also zuerst wird die rechtsstehende Abbildung angewandt.
$[(1, 3, 7)(2, 4)(5, 6)] \cdot [(1, 4, 5)(2, 6)] = (1, 2, 5, 3, 7)(4, 6)$.

3.1.36 Feststellung 19.2:

a) Ein Zyklus der Länge m ist als Produkt von $(m-1)$ Transpositionen darstellbar.
b) Jede Permutation (einer endlichen Menge) ist als Produkt von Transpositionen darstellbar.

Beweis:
$(x_1, \ldots, x_m) = (x_1, x_m) \cdots (x_1, x_2)$

3.1.37 Vollständige Induktion

Sei A ein Prädikat für natürliche Zahlen. Falls $A(1)$ wahr ist (Induktionsanfang) und falls für alle $n \in \mathbb{N}$ gilt: Falls $A(n)$ wahr ist, dann ist auch $A(n+1)$ wahr. Dann gilt $\forall n \in \mathbb{N}$: $A(n)$ also $A(n)$ ist für alle n wahr.

3.1.38 Feststellung 20

Sei $\pi \in S_n$ das Produkt von t Transposition. In der Darstellung von π als Produkt elementfremder Zyklen, in dem jedes Fixelement ($\pi(x) = x$) als 1-Zyklus aufgeführt ist, bezeichne $Z(\pi)$ als die Zahl aller Zyklen und $g(\pi)$ als die Zahl der Zyklen gerader Länge. Dann gilt: $g(\pi) \equiv n - Z(\pi) \equiv t \bmod 2$.

Beweisidee:
$Z(\pi) - g(\pi)$ ist die Anzahl der Zyklen ungerader Länge, also
$Z(n) - g(n) \equiv n \bmod 2$
$n - Z(\pi) \equiv -g(\pi) \equiv g(\pi) \bmod 2$

Durch vollständige Induktion nach t wird gezeigt: für das Produkt π von t Transposition gilt: $t \equiv n - Z(\pi) \bmod 2$.

Beweis: $\mathrm{Z}(\pi) - \mathrm{g}(\pi)$ ist die Anzahl der Zyklen ungerader Länge.
Einschub: n lässt sich als Summe schreiben: $n = n_1 + n_2$, n_1 die Anzahl der Zahlen die in geraden Zyklen vorkommen, n_2 die Anzahl Zahlen die in ungeraden Zyklen vorkommen. $n_1 \equiv 2 \wedge n \equiv n_1 + n_2 \Rightarrow n \equiv 2 + n_2 \Rightarrow n \equiv n_2$
$\forall j \in \{1, \ldots, \mathrm{Z}(\pi) - \mathrm{g}(\pi)\}$ gilt: der ungerade Zyklus z_j hat $m_j \equiv 1 (\Leftrightarrow$ m_j ungerade) Zahlen
$n_2 = \sum_{j=1}^{\mathrm{Z}(\pi)-\mathrm{g}(\pi)} m_j \equiv \sum_{j=1}^{\mathrm{Z}(\pi)-\mathrm{g}(\pi)} 1 = \mathrm{Z}(\pi) - \mathrm{g}(\pi) \Rightarrow n \equiv n_2 \equiv \mathrm{Z}(\pi) - \mathrm{g}(\pi)$
Einschub Ende
Also $\mathrm{Z}(\pi) - \mathrm{g}(\pi) \equiv n \bmod 2$,
Durch vollständige Induktion nach t wird gezeigt: Für das Produkt π von t Transposition gilt: $t \equiv n - \mathrm{Z}(\pi) \bmod 2$
Induktionsanfang: ($t = 0$) Dann ist $\pi = \mathrm{id}$, also $\mathrm{Z}(\pi) = n \Leftrightarrow n - \mathrm{Z}(\pi) = 0 \equiv 0 = t$
($t = 1$) Dann ist π eine Transposition, also $\mathrm{Z}(\pi) = n - 1$
Induktionsannahme: Gelte die Behauptung für das Produkt π von t Transpositionen, also $n - \mathrm{Z}(\pi) \equiv t \bmod 2$
Induktionsschluss: Sei $\pi' := (y_1, y_2) \cdot \pi$
Zu zeigen $n - \mathrm{Z}(\pi') \equiv t + 1 \bmod 2$ d.h. zu zeigen $\mathrm{Z}(\pi') - \mathrm{Z}(\pi) \equiv 1 \bmod 2$
Sei π als Produkt von elementfremden Zyklen **inklusive 1-Zyklen** dargestellt (vgl. F1.14c)
Dann müssen die y_1 und y_2 schon in Zyklen vorkommen.
1.Fall: y_1, y_2 kommen in demselben Zyklus vor, sagen wir in $(u_1, \ldots, u_m)$, o.B.d.A. $y_1 = u_1$, $y_2 = u_r$ (für ein $1 < r \leqslant m$), dann gilt:

$$(y_1, y_2)\cdot(\underset{\|}{y_1}, u_2, \ldots, u_{r-1}, \underset{\|}{y_2}, u_{r+1}, \ldots, u_m) = (\underset{\|}{y_1}, u_2, \ldots, u_{r-1})(\underset{\|}{y_2}, u_{r+1}, \ldots, u_m)$$
$$\begin{matrix} \| \\ u_1 \end{matrix} \qquad \begin{matrix} \| \\ u_r \end{matrix} \qquad \begin{matrix} \| \\ u_1 \end{matrix} \qquad \begin{matrix} \| \\ u_r \end{matrix}$$

also aus einem Zylus werden zwei Zyklen, also $\mathrm{Z}(\pi') - \mathrm{Z}(\pi) = 1 \equiv 1 \mod 2$
2. Fall: y_1, y_2 kommen in verschiedenen Zyklen vor, sagen wir in $(u_1, \ldots, u_r)$, $(v_1, \ldots, v_s)$ und $u_1 = y_1$, $v_1 = y_2$ o.B.d.A.
Dann gilt:

$$(y_1, y_2)(\underset{\|}{y_1}, u_2, \ldots, u_r)(\underset{\|}{y_2}, v_2, \ldots, v_s) = (\underset{\|}{y_1}, u_2, \ldots, u_r, \underset{\|}{y_2}, v_2, \ldots, v_s)$$
$$\begin{matrix} \| \\ u_1 \end{matrix} \qquad \begin{matrix} \| \\ v_1 \end{matrix} \qquad \begin{matrix} \| \\ u_1 \end{matrix} \qquad \begin{matrix} \| \\ v_1 \end{matrix}$$

also aus zwei Zyklen wird ein Zyklus, also $\mathrm{Z}(\pi') - \mathrm{Z}(\pi) = -1 \equiv 1 \bmod 2$

3.1.39 Satz 6 und Definition: Signum

Die Abbildung sign: $S_n \to \{1, -1\}$ mit $\text{sign}(\pi) = (-1)^{g(\pi)}$ ist ein Gruppenhomomorphismus in $(\{-1, 1\}, \cdot) \cong Z_2$.

sign(π) heißt das Signum von π. Es sind äquivalent:

(i) $\text{sign}(\pi) = 1$ (aufpassen: 1 ist ungerade)
(ii) Es gibt eine Darstellung von π als Produkt einer geraden Anzahl von Transpositionen.
(iii) Jede Darstellung von π als Produkt von Transpositionen enthält eine gerade Anzahl von Transpositionen.
(iv) $g(\pi)$ ist gerade.

Beweis:
Da $g(\pi)$ in einer Darstellung von π als Produkt elementfremder Zyklen (im Wesentlichen) eindeutig ist (Feststellung 19), ist $g(\pi)$ wohldefiniert und $g(\pi) \equiv t \bmod 2$ (Feststellung 20). Daraus folgt dann:
$(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$
$(i) \Leftrightarrow (iv)$ ist trivial.
sign ist ein Homomorphismus: Falls π als Produkt von t Transpositionen und τ als Produkt von s Transpositionen darstellbar ist, dann ist $\pi \cdot \tau$ ein Produkt von $t + s$ Transpositionen, also $\text{sign}(\pi\tau) = (-1)^{s+t} = (-1)^t(-1)^s = \text{sign}(\pi)\,\text{sign}(\tau)$.■

3.1.40 Feststellung und Definition: Alternierende Gruppe

Sei sign: $S_n \to \{1, -1\}$. $A_n := \ker(\text{sign}) = \{\pi \in S_n | \,\text{sign}(\pi) = 1\}$. Nach Feststellung 20 und Satz 6 ist A_n ein Normalteiler von S_n (Kern eines Homomorphismus). A_n heißt die alternierende Gruppe. Eine Permutation $\pi \in S_n$ heißt gerade, falls $\text{sign}(\pi) = 1$ ist (d. h. falls $\pi \in A_n$). π heißt ungerade, falls π nicht gerade ist. Falls $n \geq 2$ hat die A_n den Index 2 in S_n Es gibt genau 2 Linksnebenklassen, weil die jede Permutation entweder gerade oder ungerade ist.

Es gilt: $|S_n| = n(n-1)(n-2)\cdots 1 = n!$ also nach Feststellung 15: $|A_n| = \frac{1}{2}n!$ (für $n \geq 2$).■

Achtung:
Ein Zyklus gerader Länge ist eine ungerade Permutation und ein Zyklus ungerader Länge ist eine gerade Permutation.

Beispiel:
$\text{sign}((1,3,2,5)(2,4,1)(3,7))((4,5,6)(1,2,4,7))^{-1} =$
$\text{sign}((1,3,2,5)(2,4,1)(3,7))(\text{sign}((4,5,6)(1,2,4,7)))^{-1} =$
$\text{sign}(1,3,2,5)\,\text{sign}(2,4,1)\,\text{sign}(3,7)(\text{sign}(4,5,6)\,\text{sign}(1,2,4,7))^{-1} =$

$(-1)(1)(-1)((1)(-1))^{-1} = (-1)^{-1} = -1$

Beachte: sign ist ein Homomorphismus.

3.1.41 Definition: konjugiert

Sei $(G, \cdot)$ eine Gruppe. Zwei Elemente $x, y \in G$ heißen zueinander konjugiert, wenn es ein $a \in G$ gibt mit $y = axa^{-1}$, d. h. es gibt einen inneren Automorphismus, der x in y abbildet.

Zwei Untergruppen U_1, U_2 heißen zueinander konjugiert, falls es ein $a \in G$ gibt, mit $U_2 = aU_1a^{-1}$.

3.2 Ringe und Körper

3.2.1 Definition: Ring

Ein Ring $(R, +, \cdot)$ besteht aus einer **Menge R und zwei Verknüpfungen** $+\colon R \times R \to R$ **und** $\cdot\colon R \times R \to R$, sodass für alle $a, b, c \in R$ gilt:

1)	$(R, +)$ ist eine abelsche Gruppe.	
2)	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	Assoziativgesetz
3)	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$	Distributivgesetze
	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	

Konvention:
$\cdot$ bindet stärker als $+$, d. h. z. B. bedeutet $a \cdot b + a \cdot c = (a \cdot b) + (a \cdot c)$.

Bezeichnung:
Das neutrale Element bezüglich $+$ wird mit 0 bezeichnet. Das inverse Element bzgl. $+$ wird mit $-a$ bezeichnet.

3.2.2 Definition: Ringeigenschaften

Sei $(R, +, \cdot)$ ein Ring.

- R heißt kommutativ, falls $ab = ba$ für alle $a, b \in R$.
- R heißt ein (Ring) mit Eins bzw. unitär, falls es ein Element $1 \in R$ gibt und $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.
- R heißt ein (Ring) ohne Eins, falls es R nicht ein Ring mit Eins ist.
- R heißt nullteilerfrei, falls für alle $a, b \in R$ gilt: $ab = 0 \Rightarrow (a = 0 \vee b = 0)$.
- R heißt ein Schiefkörper, falls $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.
- R heißt ein Körper, falls $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe.
- R heißt ein Integritätsbereich, falls R ein nullteilerfreier kommutativer Ring mit Eins ist wobei außerdem $1 \neq 0$. $(\{\{0\}, \{((0,0),0)\}, \{((0,0),0)\}\})$ soll ausgeschlossen werden, denn wenn es ein $a \neq 0$ gibt, dann folgt $a \cdot 1 = a \neq 0 = a \cdot 0$)

3.2.3 Feststellung 21: Ringeigenschaft

Für einen Ring $(R, +, \cdot)$ gilt: Es gibt mindestens ein Element in R.
Beweis: $(R, +)$ ist eine Gruppe.

Für einen Körper $(K, +, \cdot)$ gilt: Es gibt mindestens zwei Elemente in K.
Beweis: $(K, +)$ und $(K \setminus \{0\}, +)$ sind Gruppen.

3.2.4 Feststellung 21: Ringeigenschaft

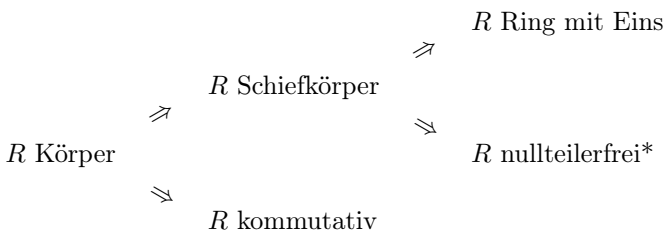
In einem Ring gilt: $a \cdot 0 = 0 = 0 \cdot a$ für alle $a \in R$, denn $0 + a \cdot 0 = a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0$, also $0 = a \cdot 0$ ($0 \cdot a = 0$ analog). ■

3.2.5 Beispiele für Ringe

$(\mathbb{N}, +, \cdot)$	kein Ring, weil $(\mathbb{N}, +)$ keine Gruppe
$(\mathbb{Z}, +, \cdot)$	Ring, kommutativ, mit Eins, nullteilerfrei, Integritätsbereich, kein Schiefkörper
$(\mathbb{Q}, +, \cdot)$	Körper
$(\mathbb{R}, +, \cdot)$	Körper
$(\mathbb{C}, +, \cdot)$	Körper der komplexen Zahlen
$(2\mathbb{Z}, +, \cdot)$	kommutativer Ring ohne Eins
$(\{0\}, +, \cdot)$	trivialer Ring, kommutativer Ring mit Eins (Die Eins ist 0), kein Schiefkörper, da $(\emptyset, \cdot)$ keine Gruppe, insbesondere kein Integritätsbereich

3.2.6 Feststellung 22: Ringarten

Nach Definition gilt für einen Ring $(R, +, \cdot)$:



* Sei $ab = 0$ und o.b.d.A $a \neq 0$, dann gibt es a^{-1}, also ist $b = 1b = a^{-1}(ab) = a^{-1}0 = 0$.■

3.2.7 Definition: Ringhomomorphismus

Seien $(R, \oplus_R, \odot_R), (S, \oplus_S, \odot_S)$ Ringe. Eine Abbildung $f\colon R \to S$ heißt ein Ringhomomorphismus, falls für alle $a, b \in R$ gilt: $f(a \oplus_R b) = f(a) \oplus_S f(b)$ und $f(a \odot_R b) = f(a) \odot_S f(b)$. Ein bijektiver Ringhomomorphismus ist ein Ringisomorphismus.

Zwei Ringe heißen isomorph, falls es einen Isomorphismus zwischen ihnen gibt. Geschrieben: $(R, \oplus_R, \odot_R) \cong (S, \oplus_S, \odot_S)$.
Falls $f\colon R \to S$ ein Ringhomomorphismus ist. dann ist $f^{-1}\colon S \to R$ ebenfalls ein Ringisomorphismus.
Nach Definition ist ein Ringhomomorphismus insbesondere auch ein Gruppenhomomorphismus $(R, +)$ und $(R, \oplus)$

3.2.8 Definition: Kern

Falls $f\colon R \to S$ ein Ringhomomorphismus ist, dann heißt $\ker(f) := f^{-1}(\{r \in R \mid f(r) = 0\})$ der Kern von f.

3.2.9 Definition: Unterring

Sei $(R, +, \cdot)$ ein Ring. $S \subseteq R$ heißt ein Unterring, falls $0 \in S$ und falls für alle $a, b \in S$ gilt: $a + b \in S, -a \in S, ab \in S$.

3.2.10 Definition: Unterkörper

Sei $(K, +, \cdot)$ ein Körper. Ein Körper $(L, +|^L_{L\times L}, \cdot|^L_{L\times L})$ heißt ein Unterkörper von $(K, +, \cdot)$, wenn $\{0_K, 1_K\} \subseteq L \subseteq K$.

3.2.11 Definition: Produkt

Das Produkt von zwei Ringen R, S ist definiert als $(R \times S, +, \cdot)$ mit

$$(r_1, s_1) + (r_2, s_2) = (\underbrace{r_1 + r_2}_{\in R}, \underbrace{s_1 + s_2}_{\in S})$$

Beispiel: $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ nicht nullteilerfrei:

$$(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$$

3.2.12 Folgerung: Produkt von Ringen

Das Produkt von zwei Ringen ist ein Ring. Beweis Übung. Z. B.: Assoziativgesetz Multiplikation

$$\begin{aligned}((r_1, s_1) \cdot (r_2, s_2)) \cdot (r_3, r_3) &= (r_1 \cdot r_2, s_1 \cdot s_2) \cdot (r_3, s_3) \\ &= ((r_1 \cdot r_2) \cdot r_3, (s_1 \cdot s_2) \cdot s_3) \\ &= (r_1 \cdot (r_2 \cdot r_3), s_1 \cdot (s_2 \cdot s_3)) \\ &= (r_1, s_1) \cdot (r_2 \cdot s_3, r_2 \cdot s_3) \\ &= (r_1, s_1)((r_2, s_2) \cdot (r_3, s_3))\end{aligned}$$

3.2.13 Definition: Ideal

Sei $(R, +, \cdot)$ ein Ring. $I \subseteq R$ heißt ein Ideal, falls $(I, +|)$ eine Untergruppe von $(R, +)$ ist (also $0 \in I, a + b \in I, -a \in I$) und für alle $a, b \in I, r \in R$ gilt: $ra \in I, ar \in I$. Insbesondere sind Ideale auch Unterringe.

3.2.14 Beispiel

Die Menge der Geraden Zahlen ist mit $+$ und $\cdot$ ein Ideal.
Gerade Zahlen addiert sind gerade. $(a + b = 2\tilde{a} + 2\tilde{b} = 2(\tilde{a} + \tilde{b}))$
Eine gerade Zahl mal eine beliebig Zahl ist gerade. $(ar = (2\tilde{a})r = 2(\tilde{a}r))$

3.2.15 Definition und Proposition: Faktorring

Sei $(R,+,\cdot)$ ein Ring und I ein Ideal. Dann setze $R/I = \{a+I \mid a \in R\}$. $(R,+)$ abelsch $\Rightarrow (I,+)$ Normalteiler. $(R/I,+)$ ist eine abelsche Gruppe (Faktorgruppe von $(R,+)$ modulo I). Definiere $\cdot\colon R/I \times R/I \to R/I$ durch $(a+I)(b+I) = ab+I$.

Diese Verknüpfung ist wohldefiniert: Sei $a,\widetilde{a},b,\widetilde{b} \in R$ Aus $a+I = \widetilde{a}+I, b+I = \widetilde{b}+I$ folgt: $a-\widetilde{a} \in I, b-\widetilde{b} \in I$, weil:

$$\begin{aligned} & a+I = \widetilde{a}+I \\ \Leftrightarrow\ & \{a+i \mid i \in I\} = \{\widetilde{a}+j \mid j \in I\} \\ \Leftrightarrow\ & \exists i,j \in I\colon a+i = \widetilde{a}+j \\ \Leftrightarrow\ & \exists i,j \in I\colon a-\widetilde{a} = i-j \\ \Leftrightarrow\ & a-\widetilde{a} \in I \qquad (i-j \in I, \text{ da } (I,+) \text{ ist Gruppe}) \end{aligned}$$

Also $(a-\widetilde{a})b \in I$ und $\widetilde{a}(b-\widetilde{b}) \in I$, dann $ab-\widetilde{a}\widetilde{b} = (a-\widetilde{a})b + \widetilde{a}(b-\widetilde{b}) \in I$, also $ab+I = \widetilde{a}\widetilde{b}+I$.

Assoziativgesetz für $\cdot$ und Distributivgesetze für I folgen direkt aus denen in R.

Damit ist $(R/I,+,\cdot)$ ein Ring und $\mathrm{nat}\colon R \to R/I$ mit $\mathrm{nat}(a) := a+I$ ein Ringhomomorphismus mit. $(R/I,+,\cdot)$ heißt der Faktorring modulo I.

$$\begin{aligned} \ker(\mathrm{nat}) &= \mathrm{nat}^{-1}(0+I) \\ &= \{x \in R \mid x+I = I\} \\ &= \{x \in R \mid \exists i,j \in I\colon x+i = j\} \\ &= \{x \in R \mid \exists i,j \in I\colon x = \underbrace{j-i}_{\in I}\} \\ &= I \end{aligned}$$

3.2.16 Feststellung: Kern als Ideal

Sei $f\colon R \to S$ ein Ringhomomorphismus. Dann ist $\ker(f)$ ein Ideal in R.

Beweis:
$\ker(f) = f^{-1}(\{r \in R \mid f(r) = 0\})$ Untergruppe von $(R,+)$ schon gezeigt. Aus $r \in R, a \in \ker(f)$ folgt $f(ra) = f(r)f(a) = f(r)\cdot 0 = 0$, also $ra \in \ker(f)$. ($ar \in \ker(f)$ analog).

Beispiel:
Für $n \in \mathbb{Z}$ ist $n\mathbb{Z}$ ein Ideal in $(\mathbb{Z},+,\cdot)$ (klar).
$(Z_n,+,\cdot)$ mit Z_n $(= \mathbb{Z}/n\mathbb{Z})$ ist der Restklassenring von $\mathbb{Z}$ modulo $n\mathbb{Z}$.
Multiplikation in Z_n: $[a]_n[b]_n = [ab]_n, [a]_n = a+n\mathbb{Z}$.■

Sei $n \in \mathbb{Z}$. $(Z_n,+,\cdot)$ ist ein kommutativer Ring mit Eins $(= [1]_n)$. Frage: Wann ist Z_n nullteilerfrei?

Beispiel:
Z_6 ist nicht nullteilerfrei, denn $[2]_6[3]_6 = [6]_6 = [0]_6$

3.2.17 Feststellung 23: Nullteilerfreiheit

Z_n ist genau dann nullteilerfrei, wenn n eine Primzahl ist.

Beweis:
Falls $n \geq 2$ keine Primzahl ist, dann gibt es $m_1, m_2 \in \mathbb{N} \setminus \{1\}$ mit $n = m_1 m_2$ und damit ist $[m_1]_n [m_2]_n = [m_1 m_2]_n = [n]_n = [0]_n$, aber $[m_1]_n \neq [0]_n, [m_2] \neq [0]_n$ also Z_n nicht nullteilerfrei.

Falls n eine Primzahl ist, dann ist Z_n nullteilerfrei, denn falls n eine Primzahl ist, folgt aus $n \mid a \cdot b$ (n teilt $a \cdot b$) die Aussage $n \mid a \vee n \mid b$.

$$[a]_n \cdot [b]_n = [ab]_n = [0]_n \Rightarrow [a]_n = [0]_n \vee [b]_n = [0]_n$$

3.2.18 Feststellung

Ein endlicher Integritätsbereich ist ein Körper. Insbesondere is Z_n ist genau dann ein Körper, wenn n eine Primzahl ist.
Beweis:
Sei R ein endlicher Integritätsbereich. Es gilt $R \neq \{0\}$. Betrachte die Abbildung

$$\begin{aligned} a \cdot \_ \colon R &\to R \\ b &\mapsto a \cdot b \end{aligned}$$

Für $a \neq 0$ ist diese Abbildung injektiv, denn für b_1, $b_2 \in R$ gilt:

$$\begin{aligned} a \cdot b_1 = a \cdot b_2 &\Rightarrow a \cdot (b_1 - b_2) = 0 \\ &\Rightarrow a = 0 \vee b_1 - b_2 = 0 \\ &\Rightarrow b_1 = b_2 \qquad\qquad (\text{wegen } a \neq 0) \end{aligned}$$

Für eine endlich Menge gilt, dass jede injektive Abbildung $f \colon R \to R$ bijektiv ist, also gibt es ein $b \in R$ mit $a \cdot b = 1$, also $b = a^{-1}$ Also $(R, +, \cdot)$ ein Körper. (Beachte $R \setminus \{0\} \neq \emptyset$)

Bezeichnung:
Sei $(R, +, \cdot)$ ein Ring, $r \in R, m \in \mathbb{Z}$. Dann definiere $\cdot' \colon \mathbb{Z} \times R \to R$ durch:

$$\begin{aligned} 0 \cdot' r &:= 0 \\ m \cdot' r &:= \underbrace{r + r + r + \cdots + r}_{m\text{-mal}} && \text{für } m \in \mathbb{N} : \\ m \cdot' r &:= (-m) \cdot' (-r) && \text{für } m \in \mathbb{Z} \setminus \mathbb{N} \setminus \{0\} \end{aligned}$$

Außerdem definere:
$r^m = \underbrace{r \cdot' \ldots \cdot' r}_{m\text{-mal}}$ für $m \in \mathbb{N}$
Konvention:
Schreibe wieder $\cdot$ statt $\cdot'$.
$\cdot$ bindet stärker als $+$.
also z. B.: $2r + 3s = r + r + s + s + s$

Rechenregeln:
Es gilt für $m, n \in \mathbb{Z}, r, s \in R$:
$(m + n)r = mr + nr$
$(\underbrace{mn}_{\in\mathbb{Z}}) \underbrace{\cdot}_{\cdot:\mathbb{Z}\times R\to R} (\underbrace{rs}_{\in R}) = (mr)(ns)$
(folgt aus dem Distributivgesetz, vollständiger Induktion und Fallunterscheidung) ■

3.2.19 Definition: Charakteristik

Sei K ein Körper. Dann definiere

$$\text{char}(K) := \begin{cases} 0, & \text{falls für alle } n \in \mathbb{N} \text{ stets } n \cdot 1_K \neq 0_K \text{ gilt} \\ p, & \text{falls } p \text{ die kleinste natürliche Zahl mit } p \cdot 1_K = 0_K \text{ ist} \end{cases}$$

K heißt dann ein Körper mit der Charakteristik $\text{char}(K)$.

Die Charakteristik gibt also an, wie oft man das neutrale Element der Multiplikation mit sich selbst addieren muss, damit sich die 0 ergibt.

Beispiele:
$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sind Körper der Charakteristik 0. $(Z_p, +, \cdot)$ für p Primzahl ist ein Körper der Charakteristik p.

3.2.20 Feststellung 24: Charakteristik und Primzahl

Sei K ein Körper der Charakteristik $p \neq 0$. Dann ist p eine Primzahl.

Beweis:
Angenommen p wäre keine Primzahl. Dann wähle $p = n_1 n_2$ mit $n_1, n_2 \in \{2, \ldots, p-1\}$. Es gilt: $0 = p \cdot 1 = (n_1 n_2) \cdot 1 = (n_1 \cdot 1)(n_2 \cdot 1)$ (weil das Distributivgesetz gilt). Da K nullteilerfrei ist, folgt $n_1 \cdot 1 = 0$ oder $n_2 \cdot 1 = 0$. Da n_1, $n_2 < p$ ist dies ein Widerspruch zur Minimalität von p.■

3.2.21 Feststellung:

In einem Körper K der Charakteristik $p \neq 0$ betrachte:

$$\{0_K, 1_K, 1_K + 1_K, 3 \cdot 1_K, \ldots, \underbrace{(p-1)}_{\in\mathbb{N}} \cdot 1_K\}$$

Dies ist ein Unterkörper von K. Denn

$(n \cdot 1) + (m \cdot 1) = (n + m) \cdot 1 = k \cdot 1$, falls $n + m \equiv k \mod p$.
$-n \cdot 1 = (p - n) \cdot 1$, $(n \cdot 1) \cdot (m \cdot 1) = (n \cdot m) \cdot 1$
Inverse von $n \cdot 1$ (mit $n \neq 0 \mod p$) in K ist $m \cdot 1$ mit $(n \cdot m) \equiv 1 \mod p$
Dieser Unterkörper von K mit p Elementen, heißt der Primkörper von K. Der Primkörper ist der kleinstemögliche Unterkörper.

4 Vektorräume

4.1 Unterräume, lineare Unabhängigkeit, Basis, Dimension

4.1.1 Definition: Vektorraum

Seien $(K, +, \cdot)$ ein Körper, $(V, \oplus)$ eine abelsche Gruppe und $\odot\colon K \times V \to V$ eine Abbildung. $V := (V, \oplus, \odot)$ heißt ein Vektorraum über K oder K-**Vektorraum**, falls für alle $x, y \in V, \lambda, \mu \in K$ gilt:

1) $\lambda(x \oplus y) = (\lambda \odot x) \oplus (\lambda \odot y)$
2) $(\lambda + \mu) \odot x = (\lambda \odot x) \oplus (\mu \odot x)$
3) $(\lambda \cdot \mu) \odot x = \lambda \odot (\mu \odot x)$
4) $1 \odot x = x$

Bezeichnung:
Man nennt die Elemente von V Vektoren und die Elemente von K Skalare.

4.1.2 Bemerkung und Konvention

$\odot$ und $\cdot$ bindet stärker als $\oplus$ und $+$, also $\lambda \odot x + (\lambda + \lambda \cdot \lambda) \odot y = (\lambda \odot x) \oplus ((\lambda + (\lambda \cdot \lambda)) \odot y)$.

verwende griechische Buchstaben für Skalare und Vektoren für lateinische. Statt $\oplus$ und $\odot$ schreibe $+$ bzw. $\cdot$. Welche Operation dann gemeint ist, ergibt sich dann aus dem Kontext, also:

1) $\lambda(x + y) = \lambda x + \lambda y$
2) $(\lambda + \mu)x = \lambda x + \mu x$
3) $(\lambda\mu)x = \lambda(\mu x)$
4) $1x = x$

Nicht definiert ist zum Beispiel:

$$\underbrace{\lambda}_{\in K} + \underbrace{x}_{\in V}$$

4.1.3 Besonders wichtige Beispiele und Schreibweisen für Vektoren

Sei $(K, +, \cdot)$ ein Körper, $n \in \mathbb{N}$. Definiere

$$V := K^n \qquad \left(= \underbrace{K \times \cdots \times K}_{n\text{-mal}} = \Pi_{i \in \{1,\ldots,n\}} K \right)$$

$$+\colon V \times V \to V$$
$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) \mapsto (a_1 + b_1, \ldots, a_n + b_n)$$

$$\cdot\colon K \times V \to V$$
$$\lambda(a_1, \ldots, a_n) \mapsto (\lambda a_1, \ldots, \lambda a_n)$$

$K^n := (V, +, \cdot)$ ist der (n-dimensionale) Standardvektorraum. Durch einfaches Nachrechnen ergibt sich sofort, dass $(V, +)$ eine abelsche Gruppe ist und dass 1), 2), 3), 4) gelten und somit der Standardvektorraum ein Vektorraum ist. Später werden wir zeigen, dass bestimmte „endlich dimensionale“ Vektorräume „isomorph“ zu K^n sind.

Sei $(K, +, \cdot)$ ein Körper. Dann ist $(K, +, \cdot)$ auch ein Vektorraum, ähnlich zu K^1.

4.1.4 Schreibweise

Man schreibt üblicherweise die Elemente von K^n als $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ statt $(a_1, \ldots, a_n)$. $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ nennt man **Spaltenvektor** und $(a_1, \ldots, a_n)$ **Zeilenvektor**.

4.1.5 Geometrische Interpretation

$\mathbb{R}^2$ kann man als Menge der Punkte der Ebene auffassen (bezüglich eines Koordinatensystems).

Bild nicht verfügbar![width=4cm]R21.pngAbbildung 28

Bild nicht verfügbar![width=4cm]R22.pngAbbildung 29

4.1.6 Physikalische Bedeutung

Vektorielle Größen, z. B. Geschwindigkeit (Vektoren im $\mathbb{R}^3$), Skalare Größen, z. B. Masse, Länge, Betrag der Geschwindigkeit.

4.1.7 Höherdimesionale Bedeutung

Auch sehr hohe Dimensionen haben anschauliche Interpretation: Beispielsweise hat eine Bank n Konten. Zu jedem Zeitpunkt gibt ein Vektor die Verteilung des Geldes auf die einzelnen Accounts an. Eine Einzahlung enspricht dann der Addition eines Vektors, bei dem ein Eintrag positive ist und der Rest 0.
Frage: Was ist ein Vektor?
Antwort: Ein Element eines Vektorraums.

4.1.8 Feststellung 25: Rechenregeln

Sei V ein K-Vektorraum. Dann gilt für alle $\lambda \in K, x \in V$:

1) $\lambda 0_V = 0_V$ ($0_V \in V$ neutrales Element bezüglich $\oplus$)
2) $0_K x = 0_V$ ($0_K \in K$ neutrales Element bezüglich $+$)
3) $\lambda(-x) = -(\lambda x) = (-\lambda)x$ ($-x$ inverses Element bezüglich $\oplus$)
4) $\lambda x = 0_V \Rightarrow x = 0_V \vee \lambda = 0_K$

Beweis:

1) $\lambda 0_V + 0_V = \lambda(0_V) = \lambda(0_V + 0_V) = \lambda 0_V + \lambda 0_V \Rightarrow 0_V = \lambda 0_V$
2) $0_K x + 0_K x = (0_K + 0_K)x = 0_K x = 0_K x + 0_V \Rightarrow 0_K x = 0_V$
3) $\lambda x + \lambda(-x) = \lambda(x - x) = \lambda 0_V = 0_V$, also $\lambda(-x) = -(\lambda x)$
   $(-\lambda)x + \lambda x = (-\lambda + \lambda)x = 0_K x = 0_V$, also $(-\lambda)x = -(\lambda x)$
4) Sei $\lambda \neq 0_K$ und $\lambda x = 0_V$.
   $0_V = \lambda^{-1} 0_V = \lambda^{-1}(\lambda x) = (\lambda^{-1}\lambda)x = 1x = x$, also $x = 0_V$ ■

4.1.9 Definition: Linearer Untervektorraum

Sei V ein K-Vektorraum und $U \subseteq V$. Dann heißt U ein linearer Untervektorraum (kurz: Unterraum) von V, falls gilt: $(U, +)$ ist eine Untergruppe von $(V, +)$, (also insbesondere $0 \in U$), und für alle $\lambda \in K$ folgt aus $u \in U$ stets $\lambda u \in U$. ($\Leftrightarrow K \cdot U \subseteq U$)

4.1.10 Feststellung 26: Unterraumkriterium

Folgende Aussagen sind äquivalent für eine Teilmenge $U \subseteq V$ (V ein K-Vektorraum):

i) $U \subseteq V$ ist ein Unterraum.
ii) $U \neq \emptyset$ und für alle $x, y \in U, \lambda \in K$ gilt: $x + y \in U$ und $\lambda x \in U$.
iii) $+$ bzw. $\cdot$ lassen sich einschränken zu den Abbildungen $+ \colon U \times U \to U$ bzw. $\cdot \colon K \times U \to U$ und U ist mit diesen Operationen ein K-Vektorraum.

Beweis durch Ringschluss:
i) $\Rightarrow$ *iii)*
Wegen *i)* ist $(U, +)$ eine Untergruppe von $(V, +)$. (Diese ist auch abelsch) Also ist $+|^{U}_{U \times U}$ eine Funktion. Nach Definition von Unterraum ist $K \cdot U \subseteq U$. Somit ist auch die Einschränkung $\cdot|^{U}_{K \times U}$ eine Funktion. Die Gesetze 1) bis 4) aus der Definition des Vektorraums gelten für alle $x, y \in V, \lambda, \mu \in K$, da $(V, +, \cdot)$ ein K-Vektorraum ist, also gelten die Gesetze auch für $x, y \in U \subseteq V$.

iii) $\Rightarrow$ *ii)*
Für $\lambda \in K, x, y \in U$ gilt: $\lambda x \in U$ (wegen $\cdot \colon K \times U \to U$),
$x + y \in U$ (wegen $+ \colon U \times U \to U$),
$U \neq 0$, da $(U, +)$ abelsche Gruppe.

ii) $\Rightarrow$ *i)*
Wegen $U \neq \emptyset$ gibt es ein $u \in U$. Dann ist wegen ii) und Feststellung 25: $-u = (-1)u \in U$ und $0 = u - u = u + (-u) \in U$, ferner gilt für alle $x, y \in U \colon x + y \in U, -x = (-1)x \in U$, also ist $(U, +)$ eine Untergruppe in $(V, +)$ und für alle $\lambda \in K, x \in U$ gilt $\lambda x \in U$. Damit ist U ein Unterraum.■

Sei $(V, +, \cdot)$ im Weiteren ein K-Vektorraum.

4.1.11 Feststellung 27: Durchschnitt und Summe von Unterräumen

a) Sei Ψ eine nichtleere Menge von Unterräumen von V. Dann ist $\bigcap \Psi$ ein Unterraum von V.
b) Seien U_1, U_2 Unterräume von V. Dann ist $U_1 + U_2 := \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$ ein linearer Untervektorraum von V.

Beweis:
Entfällt, einfache Übung.■

4.2 Linearkombination von Vektoren, lineare Hülle, Basis

4.2.1 Definition: Linearkombination

Seien $v_1, \ldots, v_m \in V$. Ein Vektor $v \in V$ heißt eine Linearkombination von $v_1, \ldots, v_m$, wenn es $\lambda_1, \ldots, \lambda_m \in K$ gibt mit $v = \lambda_1 v_1 + \ldots + \lambda_m v_m = \sum_{i=1}^{n} \lambda_i v_i$ (i läuft von 1 bis n).

Für eine nichtleere Teilmenge $M \subseteq V$ ist $v \in V$ eine Linearkombination von Vektoren aus M, falls es ein $n \in \mathbb{N}, v_1, \ldots, v_n \in M$ gibt, sodass v eine Linearkombination von $v_1, \ldots, v_m$ ist.

4.2.2 Definition: Lineare Hülle

Sei $M \subseteq V$.
$\mathrm{Lin}(M) := \{v \in V \mid v \text{ ist eine Linearkombination von Vektoren aus } M\}$
$= \{v \in V \mid \exists n \in \mathbb{N}\ \exists v_1, \ldots, v_n \in M\ \exists \lambda_1, \ldots, \lambda_n : v = \sum_{i=0}^{n} \lambda_i v_i\}$
$\mathrm{Lin}(\emptyset) := \{0\}$

$\mathrm{Lin}(M)$ heißt lineare Hülle von M in V oder der von M **aufgespannte lineare Unterraum**.
Es gilt:

$$M \subseteq \mathrm{Lin}(M)$$
$$\mathrm{Lin}(M) = \mathrm{Lin}(\mathrm{Lin}(M))$$
$$M \subseteq P \Rightarrow \mathrm{Lin}(M) \subseteq \mathrm{Lin}(P)$$
$$v \in \mathrm{Lin}(M \setminus \{v\}) \Rightarrow \mathrm{Lin}(M \setminus \{v\}) = \mathrm{Lin}(M)$$
$$\mathrm{Lin}(A) + \mathrm{Lin}(B) = \mathrm{Lin}(A \cup B)$$

4.2.3 Satz 7

$\mathrm{Lin}(M) = \bigcap\{U \mid M \subseteq U \wedge U \text{ ist ein Unterraum von } V\}$

Beweis:
Für $M = \emptyset$ gilt die Behauptung offensichtlich. Sei $M \neq \emptyset$.

„$\subseteq$“:
Zu zeigen: Jede Linearkombination aus M ist in jedem der Unterräume über die der Schnitt in der rechten Menge gebildet wird enthalten.
Sei also $m \in \mathbb{N}, v_1, \ldots, v_m \in M, \lambda_1, \ldots, \lambda_m \in K$ und U ein Unterraum mit $M \subseteq U \subseteq V$.
Wegen $M \subseteq U$ gilt $v_i \in U$ für $i = 1, \ldots, m$.
Nach Definition linearer Unterraum für U folgt erst

$$\lambda_i v_i \in U \text{ für } i = 1, \ldots, m$$

und mit trivialer vollständiger Induktion auch, dass die Summe enthalten ist:

$$\sum_{i=1}^{m} \lambda_i v_i \in U$$

Somit ist die Linearkombination auch im Schnitt enthalten.

„$\supseteq$“:
Zeige die (logisch stärkere) Aussage:

$$M \subseteq \mathrm{Lin}(M) \wedge \mathrm{Lin}(M) \text{ ist ein Unterraum von } V$$

denn nach Definition vom Schnitt folgt dann, dass der Schnitt auf der rechten Seite ein Teilmenge von $\mathrm{Lin}(M)$ sein muss. Zeige Eigenschaften aus Folgerung 26 ii):

- $0 \in \mathrm{Lin}(M)$, da $0 = 0v$ für $v \in M \neq \emptyset$ beliebig, somit $\mathrm{Lin}(M) \neq \emptyset$
- Sei

$$m, n \in \mathbb{N},$$
$$v_1, \ldots, v_m, v_{m+1}, \ldots, v_{m+n} \in M,$$
$$\lambda_1, \ldots, \lambda_{m+n}, \lambda \in K.$$

  Dann gilt:

$$\lambda \left(\sum_{i=1}^{m} \lambda_i v_i \right) = \sum_{i=1}^{m} (\lambda \lambda_i) v_i \in \mathrm{Lin}(M)$$

  und

$$\left(\sum_{i=1}^{m} \lambda_i v_i \right) + \left(\sum_{i=m+1}^{m+n} \lambda_i v_i \right) = \sum_{i=1}^{m+n} \lambda_i v_i \in \mathrm{Lin}(M)$$

Nach Feststellung 27 ist $\mathrm{Lin}(M)$ also ein Unterraum von V und $\mathrm{Lin}(M)$ ist der kleinste Unterraum (bezüglich $\subseteq$) von V, welcher M enthält.

4.2.4 Definition: Erzeugendensystem

$M \subseteq V$ heißt ein **Erzeugendensystem** von V, falls $\mathrm{Lin}(M) = V$.

Beispiel:
$\mathrm{Lin}\left(\left\{\begin{pmatrix}1\\-2\end{pmatrix}\right\}\right) = \left\{\begin{pmatrix}\lambda\\-2\lambda\end{pmatrix}\middle|\lambda \in \mathbb{R}\right\} \subseteq \mathbb{R}^2$
geometrisch: Gerade durch $\begin{pmatrix}0\\0\end{pmatrix}$ und $\begin{pmatrix}1\\-2\end{pmatrix}$.
Analog im $\mathbb{R}^3$ (Raum), z. B. $\mathrm{Lin}\left(\left\{\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}\right\}\right) = \left\{\begin{pmatrix}\lambda\\\lambda+\mu\\\mu\end{pmatrix}\middle|4\lambda, \mu \in \mathbb{R}\right\}$
Ebene die durch die drei Punkte $\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}$ beschrieben wird.

4.2.5 Definition: linear unabhängig

Eine Teilmenge $M \subseteq V$ heißt **linear unabhängig** (Abkürzung: l. u.), falls für je endlich viele paarweise verschiedene Vektoren $v_1, \ldots, v_m \in M$ und $\lambda_1, \ldots, \lambda_m \in K$ aus $\sum_{i=1}^{m} \lambda_i v_i = 0$ stets $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$ folgt. Analog ausgedrückt: Es gibt keine nichttriviale Linearkombination von Elementen aus M, die 0 ergibt.

Ein geordnetes Tupel $(v_1, \ldots, v_m)$ mit $v_i \in V$ für $i = 1, \ldots, m$ heißt linear unabhängig, wenn die Menge $\{v_1, \ldots, v_m\}$ linear unabhängig ist und die Vektoren $v_1, \ldots, v_m$ paarweise verschieden sind.

Eine Menge (bzw. ein Tupel) von Vektoren heißt **linear abhängig**, falls sie nicht linear unabhängig ist.

$x \in V$ heißt linear abhängig von M, falls $x \in \mathrm{Lin}(M)$.

4.2.6 Feststellung 28: Lineare Unabhängigkeit

Die folgenden Aussagen sind äquivalent für $M \subseteq V$:

i) M ist linear unabhängig
ii) Für alle $v \in M$ gilt: $v \notin \text{Lin}(M \setminus \{v\})$ (kein Vektor $v \in M$ lässt sich als Linearkombination der übrigen Vektoren aus M darstellen).

Beweis:
$(i) \Rightarrow (ii)$: Zu zeigen: $\neg(ii) \Rightarrow \neg(i)$.

Angenommen $v \in M \cap \text{Lin}(M \setminus \{v\})$. Dann gibt es $v_1, \ldots, v_m \in M \setminus \{v\}$ und $\lambda_1, \ldots, \lambda_m \in K$ mit $v = \sum_{i=1}^{m} \lambda_i v_i$. Ohne Beschränkung der Allgemeinheit (o.B.d.A.) seien die Vektoren $v_1, \ldots, v_m$ paarweise verschieden (wegen $\lambda u + \mu u = (\lambda + \mu)u$). Daraus folgt $0 = -(1)v + \sum_{i=1}^{m} \lambda_i v_i$. Dies ist jedoch eine nichttriviale Linearkombination von Elementen aus M zu 0, also ist M linear abhängig.

$(ii) \Rightarrow (i)$: Zu zeigen: $\neg(i) \Rightarrow \neg(ii)$.
Angenommen $0 = \sum_{i=1}^{m} \lambda_i v_i$ mit $v_i \in M$ paarweise verschieden und mindestens ein $\lambda_i \neq 0$. O.B.d.A. sei $\lambda_1 \neq 0$ (ggf. umnummerieren, Reihenfolge ändern). Dann ist $\lambda_1 v_1 = \sum_{i=2}^{m} (-\lambda_i) v_i$, also $v_1 = \sum_{i=2}^{m} (\lambda_1^{-1}(-\lambda_i)) v_i \in \text{Lin}(M \setminus \{v_1\})$. Also gilt $\neg(ii)$.■

Beispiele:

- $\emptyset$ ist linear unabhängig.
- Falls $0 \in M$, dann ist M linear abhängig ($1 \cdot 0 = 0$ nichttriviale Linearkombination zu 0).
- Falls in $(v_1, \ldots, v_m)$ ein Vektor doppelt vorkommt, dann ist das Tupel linear abhängig.
- Falls $v \in M$ und $\lambda v \in M$ für ein $\lambda \neq 1$ dann ist M linear abhängig: $v \neq \lambda v$ wegen $\lambda \neq 1$ und $\lambda v + (-1)(\lambda v) = 0$, da $-1 \neq 0$.

4.2.7 Feststellung 29: Lineare Unabhängigkeit

Sei $M \subseteq V$ linear unabhängig und $x \in V \setminus \mathrm{Lin}(M)$. Dann ist $M \cup \{x\}$ linear unabhängig.

Beweis:
Sei $0 = \sum_{i=1}^{m} \lambda_i x_i + \lambda x$ mit $x_i \in M$ paarweise verschieden und $\lambda_1, \ldots, \lambda_m, \lambda \in K$.
Zu zeigen: $\lambda_1 = \cdots = \lambda_m = \lambda = 0$.

Fall 1:
$\lambda = 0$. Dann ist wegen M linear unabhängig $\lambda_1 = \lambda_2 = \ldots = \lambda_m = 0$.

Fall 2: $\lambda \neq 0$. Dann ist

$$\lambda x = -\sum_{i=1}^{m} \lambda_i x_i$$
$$\Rightarrow x = \sum_{i=1}^{m} (-\lambda^{-1}\lambda_i) x_i \in \mathrm{Lin}(M)$$

im Widerspruch zu $x \in V \setminus \mathrm{Lin}(M)$. Wodurch dieser Fall nicht eintreten kann.
■

4.2.8 Definition: Basis

$M \subseteq V$ heißt **Basis** von V, falls M ein **linear unabhängiges Erzeugendensystem** von V ist.

Ein Tupel $(b_1, \ldots, b_m)$ von Vektoren in V heißt eine geordnete Basis von V, falls die b_i paarweise verschieden sind und $\{b_1, \ldots, b_n\}$ eine Basis von V ist.

4.2.9 Satz 8: Charakterisierung einer Basis

Die folgenden Aussagen sind äquivalent für eine Menge $M \subseteq V$:

(i) M ist eine Basis von V
(ii) M ist ein minimales (bezüglich $\subseteq$) Erzeugendensystem von V.
(iii) M ist eine maximale (bezüglich $\subseteq$) linear unabhängige Menge in V.

Beweis:
$(i) \Rightarrow (ii)$: Sei M eine Basis. Dann ist M ein linear unabhängiges Erzeugendensystem. Untersuche $\widetilde{M} \subsetneq M$ wobei $v \in M \setminus \widetilde{M}$. Wegen Feststellung 28 gilt $v \notin \mathrm{Lin}(M \setminus \{v\})$. Wegen $v \notin \widetilde{M}$ gilt außerdem $\widetilde{M} \subseteq M \setminus \{v\}$ und damit auch $\mathrm{Lin}(\widetilde{M}) \subseteq \mathrm{Lin}(M \setminus \{v\})$. Daraus folgt $v \notin \mathrm{Lin}(\widetilde{M})$. Deshalb ist $\widetilde{M}$ kein Erzeugendensystem von V.

$(ii) \Rightarrow (i)$: Sei M ein minimales Erzeugendensystem. Dann ist $M \setminus \{v\}$ für $v \in M$ kein Erzeugendensystem, also $\mathrm{Lin}(M\setminus\{v\}) \neq V$. Wäre $v \in \mathrm{Lin}(M\setminus\{v\})$, dann auch $\mathrm{Lin}(M \setminus \{v\}) = \mathrm{Lin}(M) = V$ was ein Wiederspruch ist. Also $v \notin \mathrm{Lin}(M \setminus \{v\})$. Mit Feststellung 28 folgt dann dass M linear unabhängig ist und somit eine Basis.

$(i) \Rightarrow (iii)$: Sei M eine Basis. Dann ist M linear unabhängig
Angenommen $M \subsetneq \widetilde{M}$ ($\widetilde{M}$ echte Obermenge) wäre linear unabhängig. Sei $v \in \widetilde{M} \setminus M \subseteq \widetilde{M}$. Dann ist laut Feststellung 28 $v \notin \mathrm{Lin}(\widetilde{M}) \supseteq \mathrm{Lin}(M)$ im Widerspruch zu $\mathrm{Lin}(M) = V$.

$(iii) \Rightarrow (i)$: Angenommen $\mathrm{Lin}(M) \neq V$, dann wähle $v \in V \setminus \mathrm{Lin}(M)$. Dann ist nach Feststellung 29 $M \cup \{v\}$ linear unabhängig im Widerspruch zur Maximalität von M.■

4.2.10 Beispiel: Standardbasis

Die Vektoren $e_1 := \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, e_2 := \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}, \ldots, e_n := \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}$ in K^n bilden eine Basis von K^n, wobei $0, 1 \in K$, die zwei neutralen Elemente sind. $(e_1, \ldots, e_n)$ heißt die Standardbasis von K^n.

Beweis:
$\begin{pmatrix}a_1\\\vdots\\a_n\end{pmatrix} = \begin{pmatrix}a_1 \cdot 1 + 0 + \ldots + 0\\\vdots\\0 + \ldots + 0 + a_n \cdot 1\end{pmatrix} = a_1 \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} + \ldots + a_n \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix} = \sum_{i=1}^{n} a_i e_i$, also ist $\{e_1, \ldots, e_n\}$ ein Erzeugendensystem. Aus $\sum_{i=1}^{n} a_i e_i = \begin{pmatrix}a_1\\\vdots\\a_n\end{pmatrix} = \begin{pmatrix}0\\\vdots\\0\end{pmatrix}$ folgt $a_1 = a_2 = \cdots = a_n = 0$, also ist $\{e_1, \ldots, e_n\}$ linear unabhängig.

4.2.11 Beispiel: Der Vektorraum K^I

Sei I eine Menge und K ein Körper. $K^I := \{f\colon I \to K \mid f \text{ Abbildungen}\} = \Pi_{i\in I} K$ (allgemeines kartesisches Produkt) mit den Operationen $+\colon K^I \times K^I \to K^I$ und $\cdot\colon K \times K^I \to K^I$, die durch $(f+g)(i) := f(i) + g(i)$ bzw. $(\lambda f)(i) := \lambda f(i)$ für alle $i \in I$ definiert sind, ist ein K-Vektorraum.

Beweis:
Klar (einfaches Nachrechnen).

$K^{(I)} := \{f \in K^I | f(i) = 0_K$ für alle bis auf endlich viele $i \in I\}$ ist ein Unterraum von K^I. $\{e_i \mid i \in I\}$ mit

$$e_i \in K^{(I)}$$
$$e_i(j) := \begin{cases} 1, & \text{für } j = i \\ 0, & \text{sonst} \end{cases}$$

ist eine Basis von $K^{(I)}$.
Bemerkung:
Falls I endlich ist, ist $K^{(I)} = K^I$. Außerdem $K^\emptyset = \{ \underbrace{\emptyset_K}_{\text{leere Abbildung}} \}$ (der Nullvektorraum).

K^I ist eine Verallgemeinerung von K^n mit $n \in \mathbb{N}$. Jetzt kann (veranschaulicht gesehen) ein Vektor $v \in K^I$ auch unendlich viele Einträge haben. Ein Vektor $v \in K^{(I)}$ hat endlich aber beliebig viele Einträge. Falls $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$, dann gilt:

$$K^I = \Pi_{i\in I} K = \Pi_{i\in\{1,\ldots,n\}} K = K^n$$

4.2.12 Satz 9: (mit AC und zornschem Lemma)

Sei $M \subseteq V$ linear unabhängig und sei E mit $M \subseteq E \subseteq V$ ein Erzeugendensystem von V. Dann gibt es eine Basis B von V mit $M \subseteq B \subseteq E \subseteq V$. Insbesondere gilt: Jeder Vektorraum hat eine Basis (setze $M := \emptyset, E := V$).

Beweis:
Sei $\mathfrak{M} := \{S \mid M \subseteq S \subseteq E \text{ und } S \text{ ist linear unabhängig}\}$. $\mathfrak{M}$ ist somit eine Auswahl an linear unabhängigen Teilmengen. Es gilt $\mathfrak{M} \neq \emptyset$, da $M \in \mathfrak{M}$. Außerdem ist $(\mathfrak{M}, \subseteq)$ eine partiell geordnete Menge.
Sei $L \subseteq \mathfrak{M}$ eine nichtleere Kette (d. h. bezüglich $\subseteq$ linear geordnete Teilmenge). Wir wollen zeigen, dass $\bigcup L \in \mathfrak{M}$ gilt. $M \subseteq \bigcup L \subseteq E$ ist klar. Zu zeigen: $\bigcup L$ ist linear unabhängig. Seien $v_1, \ldots, v_n \in \bigcup L$ paarweise verschieden und $\lambda_1, \ldots, \lambda_n \in K$ mit $\sum_{i=1}^{n} \lambda_i v_i = 0$. Für alle $i = 1, \ldots, n$ gibt es dann ein S_i mit $v_i \in S_i \in L$. Da L bezüglich $\subseteq$ linear geordnet ist, gilt das Gleiche auch für die Teilmenge $\{S_1, \ldots, S_n\}$. Deshalb können wir o.B.d.A. annehmen, dass $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n$ gilt. Daraus folgt $v_1, \ldots, v_n \in S_n$. Da S_n als Element von $\mathfrak{M}$ linear unabhängig ist, folgt $\lambda_1 = \cdots = \lambda_n = 0$. Also ist $\bigcup L$ linear unabhängig. Damit ist $\bigcup L$ eine obere Schranke von L in $(\mathfrak{M}, \subseteq)$.

Da somit jede Kette in $(\mathfrak{M}, \subseteq)$ eine obere Schranke besitzt, folgt aus dem zornschen Lemma die Existenz eines maximalen Elementes $B \in \mathfrak{M}$. Angenommen es gilt $\mathrm{Lin}(B) \subsetneq \mathrm{Lin}(E) = V$. Dann gibt es ein $v \in \mathrm{Lin}(E)$ mit $v \notin \mathrm{Lin}(B)$. Bei der Darstellung von v als Linearkombination muss mindestens ein Vektor $e \in E \setminus B$ dabei sein, sonst wäre $v \in \mathrm{Lin}(B)$. Also ist $e \in V \setminus \mathrm{Lin}(B)$ und B linear unabhängig. Somit ist $B \cup \{e\}$ nach Feststellung 29 linear unabhängig und es gilt außerdem $M \subseteq B \cup \{e\} \subseteq E$, also $B \cup \{e\} \in \mathfrak{M}$. Wegen $B \subsetneq B \cup \{e\}$ ist dies ein Widerspruch zur Maximalität von B. Daraus folgt $\mathrm{Lin}(B) = V$. Somit ist B ein linear unabhängiges Erzeugendensystem, also eine Basis.■

Bemerkung:
Falls E endlich ist, dann braucht man im Beweis von Satz 9 nicht das zornsche Lemma, da dann die Menge $\mathfrak{M}$ ebenfalls endlich ist und eine nichtleere endliche partiell geordnete Menge stets maximale Elemente enthält.

4.2.13 Definition: Lineare Abbildungen

Seien V, W K-Vektorräume. Eine Abbildung $f\colon V \to W$ heißt linear, falls für alle $x, y \in V, \lambda \in K$ gilt: $f(x + y) = f(x) + f(y), f(\lambda x) = \lambda f(x)$. Ein Isomorphismus $f\colon V \to W$ ist eine bijektive lineare Abbildung. V und W heißen isomorph, geschrieben $V \cong W$, wenn es einen Isomorphismus $f\colon V \to W$ gibt. Eine lineare Abbildung $f\colon V \to V$ heißt auch ein Endomorphismus.

Bemerkung:
$f(0_V) = f(0_K x) = 0_K f(x) = 0_W$
$f(-x) = f((-1)x) = (-1)f(x) = -f(x)$ für $f\colon V \to W$ linear.

Eine lineare Abbildung ist insbesondere auch ein Gruppenhomomorphismus von $(V, +)$ nach $(W, +)$.

4.2.14 Beispiel und Definition: Projektion

Die Projektionen $p_i\colon K^n \to K$ mit $p_i \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} := a_i$ ist linear für $i \in \{1, \ldots, n\}$. Die Projektionen $p_i\colon K^I \to K$ mit $p_i(f) := f(i)$ sind linear für $i \in I$.

Beweis:
klar:

$$p_i(\lambda f) = (\lambda f)(i) = \lambda(f(i)) = \lambda(p_i(f))$$
$$p_i(f+g) = (f+g)(i) = f(i) + g(i) = p_i(f) + p_i(g)$$

4.2.15 Feststellung 30 und Definition: Eigenschaften linearer Abbildungen

a) Wenn $f\colon U \to V$, $g\colon V \to W$ lineare Abbildungen sind, dann ist $g \circ f\colon U \to W$ linear.
b) Wenn $f\colon V \to W$ ein Isomorphismus ist, dann ist $f^{-1}\colon W \to V$ ebenfalls linear und ein Isomorphismus.
c) Falls $U_1 \subseteq U$ ein Unterraum ist und $f\colon U \to V$ linear, dann ist $f(U_1)$ ein Unterraum von V.
d) Falls $V_1 \subseteq V$ ein Unterraum ist und $f\colon U \to V$ linear, dann ist $f^{-1}(V_1)$ ein Unterraum von U. Insbesondere ist $\ker(f) := f^{-1}(\{0\}) = \{u \in U \mid f(u) = 0\}$ ein Unterraum von U. $\ker(f)$ heißt der Kern von f.
e) Eine lineare Abbildung $f\colon U \to V$ ist genau dann injektiv, wenn $\ker(f) = \{0\}$.

Beweis: 9zu e):

„⇒“: Sei f injektiv. Dann folgt für beliebige $x \in U$ mit $f(x) = \underbrace{f(0)}_{=0}$, dass $x = 0$ gilt. Damit ist $\ker(f) = \{x \in U \mid f(x) = 0\} = \{0\}$.
„⇐“: Sei $\ker(f) = \{0\}$. Dann folgt aus $f(x) = f(y)$, dass $f(x-y) = f(x) - f(y) = 0$, also $x - y \in \underbrace{\ker(f)}_{=\{0\}}$, wodurch wiederum $x - y = 0$, was $x = y$ zur Folge hat. ■

Bezeichnung:
Für $U \subseteq V$ und $\lambda\colon U \to K, u \mapsto \lambda_u$ ist die Summe $\sum\limits_{u \in U} \lambda_u u$ definiert, falls $\{u \in U \mid \lambda_u \neq 0_K\}$ endlich ist. Lasse Summanden der Form $0u$ weg und beachte, dass endliche Summen unabhängig von der Reihenfolge der Summanden sind. Kommentar: $\sum\limits_{u \in \emptyset} \lambda_u u := 0_V$.

4.2.16 Feststellung 31: Raum der Linearkombinationen

Sei $M \subseteq V$. P sei die Interpretation von $\Lambda \in K^{(M)}$ als Linearkombination aus Vektoren aus M. Sie ist definiert durch:

$$P\colon K^{(M)} \to V$$
$$P(\Lambda) := \sum_{u \in M} \Lambda(u) \cdot u$$

wobei alternativ $\Lambda(u) = p_u(\Lambda)$ und p_u Projektionen sind. Dann gilt:

a) P ist linear.
b) P ist injektiv $\Leftrightarrow$ M ist linear unabhängig.
c) $P\left(K^{(M)}\right) = \mathrm{Lin}(M)$, also insbesondere P surjektiv $\Leftrightarrow \mathrm{Lin}(M) = V$.
d) P ist ein Isomorphismus $\Leftrightarrow$ M ist eine Basis von V.
Also $V \cong K^{(M)}$, falls M eine Basis.

Bemerkung:
b) $\wedge$ c) bedeutet anders ausgedrückt: M ist linear unabhängig $\Leftrightarrow$ $P\colon \mathrm{Lin}(M) \to V$ injektiv $\Leftrightarrow$ jeder Vektor in $\mathrm{Lin}(M)$ lässt sich eindeutig (bis auf die Reihenfolge der Summanden und Summanden der Form $0b$) als Linearkombination von paarweise verschiedenen Vektoren aus M ausdrücken.

d) bedeutet: M ist genau dann eine Basis von V, wenn sich jeder Vektor in V eindeutig als Linearkombination von Vektoren aus M darstellen lässt. Mit Satz 9 (mit AC) folgt: Jeder Vektorraum V ist isomorph zu einem Vektorraum der Form $K^{(M)}$ (M Menge). Also für V K-Vektorraum und B Basis ist V isomorph zum Vektorraum der Linearkombinationen aus B.

Beweis:
a)

$$\begin{aligned} P(\Lambda + \mathrm{M}) &= \sum_{u \in M} (\Lambda + \mathrm{M})(u) \cdot u \\ &= \sum_{u \in M} (\Lambda(u) + \mathrm{M}(u)) \cdot u && \text{Definition } +\colon K^{(M)} \times K^{(M)} \to K^{(M)} \\ &= \sum_{u \in M} \Lambda(u) \cdot u + \sum_{u \in M} \mathrm{M}(u) \cdot u \\ &= P(\Lambda) + P(\mathrm{M}) \end{aligned}$$

$$\begin{aligned} P(\lambda\Lambda) &= \sum_{u \in M} (\lambda\Lambda)(u) \cdot u \\ &= \sum_{u \in M} \lambda(\Lambda(u)) \cdot u && \text{Definition } \cdot\colon K \times K^{(M)} \to K^{(M)} \\ &= \lambda \sum_{u \in M} \Lambda(u) \cdot u \\ &= \lambda P(\Lambda) \end{aligned}$$

b)

$$P \text{ injektiv} \Leftrightarrow \underbrace{\{\Lambda \in K^{(M)} \mid P(\Lambda) = 0_V\}}_{=\ker(P)} = \{0_{K^{(M)}}\}$$

$$\Leftrightarrow \forall \Lambda \in K^{(M)}: \quad \underbrace{P(\Lambda)}_{=\sum_{u\in M} \Lambda(u)\cdot u} = 0 \Rightarrow \Lambda = 0_{K^{(M)}}$$

$\Leftrightarrow$ in jeder Linearkombination von verschiedenen Elementen aus M, die 0_V ergibt, sind alle Koeffizienten 0_K

$\Leftrightarrow M$ linear unabhängig

c)

$$P\left(K^{(\emptyset)}\right) = P(\{\emptyset_V\}) = \{P(\emptyset_V)\} = \left\{\sum_{u\in\emptyset} \emptyset_V(u)\cdot u\right\} = \{0_V\} = \text{Lin}(\emptyset)$$

Sei $M \neq \emptyset$.
„$\supseteq$“: Jede Linearkombination aus M lässt sich als Linearkombination von paarweise verschiedenen Elementen schreiben. Sei $\sum_{i=1}^{m} \lambda_i u_i \in \text{Lin}(M)$ mit $u_i \in M$ paarweise verschieden. Definiere Λ durch $\Lambda(u_i) := \lambda_i$ für $i \in \{1, \ldots, m\}$ und $\Lambda(u) := 0$ für $u \in M \setminus \{u_1, \ldots, u_m\}$. Dann ist $\Lambda \in K^{(M)}$ und somit

$$\sum_{i=1}^{m} \lambda_i u_i = \sum_{u\in M} \Lambda(u)\cdot u \in P\left(K^{(M)}\right)$$

„$\subseteq$“: Ausdrücke der Form $\sum_{u\in M} \Lambda(u)\cdot u$ für $\Lambda \in K^{(M)}$ sind in $\text{Lin}(M)$. (Summanden $0\cdot u$ weglassen, restliche Summanden sind endlich).

d)
P Isomorphismus $\Leftrightarrow P\left(K^{(M)}\right) = V$ und $\ker(P) = \{0\} \Leftrightarrow M$ ist ein Erzeugendensystem und M ist linear unabhängig $\Leftrightarrow M$ ist eine Basis.■

4.2.17 Satz 10: Basisaustauschsatz

Seien B, C Basen von V. Sei $b \in B$. Dann ist $C \setminus \text{Lin}(B \setminus \{b\}) \neq \emptyset$ und für alle $c \in C \setminus \text{Lin}(B \setminus \{b\})$ ist $(B \setminus \{b\}) \cup \{c\}$ eine Basis von V.

Beweis:
Da B eine Basis von V ist, ist B ein minimales Erzeugendensystem (Feststellung 28), also $\text{Lin}(B \setminus \{b\}) \subsetneq V$. C kann keine Teilmenge von $\text{Lin}(B \setminus \{b\})$ sein, denn sonst:

$$\begin{aligned} & C \subseteq \text{Lin}(B \setminus \{b\}) \\ \Rightarrow & \text{Lin}(C) \subseteq \text{Lin}(B \setminus \{b\}) \\ \Rightarrow & V = \text{Lin}(C) \subseteq \text{Lin}(B \setminus \{b\}) \subsetneq V \end{aligned}$$

also $C \nsubseteq \text{Lin}(B \setminus \{b\})$, d. h. $C \setminus \text{Lin}(B \setminus \{b\}) \neq \emptyset$. Sei $c \in C \setminus \text{Lin}(B \setminus \{b\})$. Dann ist $(B \setminus \{b\}) \cup \{c\}$ linear unabhängig (Feststellung 29). Da B eine Basis ist, gibt es $b_1, \ldots, b_m \in B \setminus \{b\}$ paarweise verschieden und $\lambda_1, \ldots, \lambda_m, \lambda \in K$ mit $c = \sum_{i=1}^{m} \lambda_i b_i + \lambda b$. Es gilt $\lambda \neq 0$ wegen $c \notin \text{Lin}(B \setminus \{b\})$ und damit

$$b = \lambda^{-1} \left(c - \sum_{i=1}^{m} \lambda_i b_i \right) = \lambda^{-1} c + \sum_{i=1}^{m} (-\lambda_i \lambda^{-1}) b_i$$

also $b \in \text{Lin}((B \setminus \{b\}) \cup \{c\})$. Aus dem und $\text{Lin}(B) = V$ folgt

$$\text{Lin}((B \setminus \{b\}) \cup \{c\}) = \text{Lin}(B \cup \{c\}) = V$$

■

4.2.18 Definition: endlich-dimensional

V heißt endlich-dimensional, falls V eine **endliche Basis** hat. (geschrieben: $\dim V < \infty$). Falls V nicht endlich-dimensional ist, dann heißt V unendlich-dimensional (geschrieben: $\dim V = \infty$).

4.2.19 Satz 11 und Definition: Dimensionen von Vektorräumen

Sei V endlich-dimensional. Dann haben je zwei Basen von V dieselbe (endliche) Zahl n von Elementen. Diese Zahl heißt die Dimension von V, geschrieben: $\dim V = n$.

Beweis:
Sei B eine endliche Basis von V und C irgendeine Basis von V. Dann können wir nacheinander jedes Element von B nach dem Basisaustauschsatz durch ein Element aus C ersetzen und erhalten so eine Basis $C' \subseteq C$ von V mit $|B| = |C'|$. Da C eine Basis ist, ist C ein minimales Erzeugendensystem (laut Feststellung), also $C' = C$, also $|B| = |C'| = |C|$.■

Bemerkung:
Sei I endlich, dann: $\dim K^I = |I|$

Bemerkung:
Wegen Satz 9 und Satz 11 sind äquivalent:

i) V ist unendlich dimensional.
ii) V hat eine unendliche Basis.
iii) jede Basis von V ist unendlich.

Beweis:
i) $\Leftrightarrow$ V ist nicht endlich-dimensional. $\Leftrightarrow$ V hat keine endlich Basis. $\Leftrightarrow$ jede Basis von V ist unendlich. $\Leftrightarrow$ iii)
iii) $\overset{\text{Satz } 9}{\Rightarrow}$ V hat eine Basis und sie ist unendlich. $\Rightarrow$ ii)
$\neg$ iii) $\Leftrightarrow$ Es gibt eine endliche Basis. $\overset{\text{Satz } 11}{\Leftrightarrow}$ Jede Basis ist endlich. $\Leftrightarrow \neg$ ii)

4.2.20 Satz 12: endlich-dimensional

Jeder Unterraum U eines endlich dimensionalen Vektorraums V ist endlich-dimensional und es gilt:
a) $\dim U \leq \dim V$
b) $\dim U = \dim V \Leftrightarrow U = V$

Beweis:
Sei $\dim V = n$. Sei B eine Basis von U. U ist linear unabhängig. Nach Satz 9 gibt es eine Basis C von V mit $B \subseteq C \subseteq V$ und $|C| = n$ (nach Satz 11). Also $\dim U = |B| \leq |C| = n = \dim V$ und falls $=$ gilt, dann ist $B = C$, also $U = \text{Lin}(B) = \text{Lin}(C) = V$. ■

4.2.21 Feststellung 32: lineare Unabhängigkeit

Sei $A \subseteq V$ linear unabhängig, $B, C \subseteq A$ mit $B \cap C = \emptyset$. Dann ist $\mathrm{Lin}(B) \cap \mathrm{Lin}(C) = \{0\}$.

Beweis:
Sei $x \in \mathrm{Lin}(B) \cap \mathrm{Lin}(C)$. Dann gibt es $\lambda_i \in K, \mu_j \in K$ mit $i = 1, \ldots, n$, $j = 1, \ldots, m$, $b_i \in B, c_j \in C$ paarweise verschieden mit $x = \sum_{i=1}^{n} \lambda_i b_i = \sum_{i=1}^{m} \mu_i c_i$, also $0 = \sum_{i=1}^{n} \lambda_i b_i + \sum_{j=1}^{m} -\mu_j c_j$. Da $b_i, c_j \in A$ und A linear unabhängig folgt $\lambda_i = 0$ für alle $i = 1, \ldots, n$, und $\mu_i = 0$ für alle $j = 1, \ldots, m$, also $x = 0$.■

4.2.22 Satz 13 und Definition: Komplementärräume (mit AC, falls $\dim V = \infty$)

Zu jedem Unterraum $U \subseteq V$ gibt es einen Unterraum W mit $U \cap W = \{0\}$ und $U + W = V$. Ein solcher Unterraum W heißt ein zu U komplementärer Unterraum.

Beweis:
Sei A eine Basis von $U = \mathrm{Lin}(A)$. Nach Satz 9 gibt es eine Basis B von V mit $A \subseteq B \subseteq V$. Definiere $W := \mathrm{Lin}(B \setminus A)$. Dann ist $U \cap W = \{0\}$ (vgl. Feststellung 32). Außerdem:

$$U + W = \mathrm{Lin}(A) + \mathrm{Lin}(B \setminus A) = \mathrm{Lin}(A \cup B \setminus A) = \mathrm{Lin}(B) = V$$

4.2.23 Feststellung 33: Kardinalitäten

Sei $\dim V = n < \infty$.

a) Falls $M \subseteq V$ linear unabhängig, dann ist $|M| \leqslant n$.
b) Falls $E \subseteq V$ ein Erzeugendensystem von V ist, dann ist $n \leqslant |E|$.

Beweis:
a) Sei M linear unabhängig. Dann gibt es nach Satz 9 der Existenz einer Basis eine Basis B von V mit $M \subseteq B$ also $|M| \leqslant |B| = n$.
b) Sei E ein Erzeugendensystem. Dann gibt es nach Satz 9 eine Basis B von V mit $B \subseteq E$ also $n = |B| \leqslant |E|$.

4.2.24 Bemerkung

Seien $x_1, \ldots, x_m \in V$ paarweise verschieden. Dann gilt: Falls $M \subseteq \{x_1, \ldots, x_m\}$ eine maximal linear unabhängige Teilmenge ist, dann ist M eine Basis von $\mathrm{Lin}(\{x_1, \ldots, x_m\})$, wie wir in Beweis von Satz 8 gezeigt haben. Folglich gilt: $\dim \mathrm{Lin}(\{x_1, \ldots, x_m\}) = |M|$ d. h. $\dim \mathrm{Lin}(\{x_1, \ldots, x_m\})$ ist die Anzahl der Elemente einer maximalen linear unabhängigen Teilmenge von M.

4.2.25 Satz 14: Dimensionssatz für lineare Unterräume

Seien U, W Unterräume von V mit $\dim V < \infty$. Dann gilt: $\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$.

Beweis:
Sei $m := \dim(U \cap W)$ und $(a_1, \ldots, a_m)$ eine Basis von $U \cap W$. Ergänze einerseits zu einer Basis $(a_1, \ldots, a_m, b_1, \ldots, b_r)$ von U und andererseits zu einer Basis $(a_1, \ldots, a_m, c_1, \ldots, c_s)$ von W (jeweils paarweise verschiedene Vektoren). Wir wollen zeigen, dass dann $(a_1, \ldots, a_m, b_1, \ldots, b_r, c_1, \ldots, c_s)$ eine Basis von $U+W$ ist, hieraus würde folgen:

$$\dim(U + W) = m + r + s = \underbrace{(m + r)}_{=\dim U} + \underbrace{(m + s)}_{=\dim W} - \underbrace{m}_{=\dim(U \cap W)}$$

Zunächst ist $B := \{a_1, \ldots, a_m, b_1, \ldots, b_r, c_1, \ldots, c_s\}$ ein Erzeugendensystem von $U + W$:

$$\begin{aligned}
\mathrm{Lin}(B) &= \mathrm{Lin}(\{a_1, \ldots, a_m, b_1, \ldots, b_r, c_1, \ldots, c_s\}) \\
&= \mathrm{Lin}(\{a_1, \ldots, a_m, b_1, \ldots, b_r\} \cup \{a_1, \ldots, a_m, c_1, \ldots, c_s\}) \\
&= \mathrm{Lin}(\{a_1, \ldots, a_m, b_1, \ldots, b_r\}) + \mathrm{Lin}(\{a_1, \ldots, a_m, c_1, \ldots, c_s\}) \\
&= U + V
\end{aligned}$$

Noch zu zeigen: B ist linear unabhängig. Sei

$$0 = \underbrace{\sum_{i=1}^{m} \lambda_i a_i}_{=:a} + \underbrace{\sum_{i=1}^{r} \mu_i b_i}_{=:b} + \underbrace{\sum_{i=1}^{s} \beta_i c_i}_{=:c}$$

$a \in U \cap W, b \in U, c \in W$. Dann gilt $b = -a - c \in W$ und insgesamt $b = -a - c \in U \cap W$. Da $(a_1, \ldots, a_m)$ Basis von $U \cap W$ ist, kann b als Linearkombination der a_i dargestellt werden. D.h. es gilt $b = \sum_{i=1}^{m} \gamma_i a_i$. Daraus folgt $0 = a + b + c = \sum_{i=1}^{m} (\lambda_i + \gamma_i) a_i + \sum_{i=1}^{s} \beta_i c_i$. Wegen $(a_1, \ldots, a_m, c_1, \ldots, c_s)$ linear unabhängig folgt wiederum $\beta_1 = \ldots = \beta_s = 0$. Eingesetzt ergibt dies $0 = \sum_{i=1}^{m} \lambda_i a_i + \sum_{i=1}^{r} \mu_i b_i$. Da auch $(a_1, \ldots, a_m, b_1, \ldots, b_r)$ linear unabhängig erhalten wir $\lambda_1 = \ldots = \lambda_m = \mu_1 = \ldots = \mu_s = 0$. Damit ist B linear unabhängig und deshalb eine Basis von $U + W$.■

4.2.26 Feststellung 34: Direkte Summe

Seien $U_1, \ldots, U_m \subseteq V$ Unterräume und $U = U_1 + \ldots + U_m$. Dann sind folgende Aussagen äquivalent:

i) $U_i \cap W_i = \{0\}$ für $i = 1, \ldots, m$, wobei $W_i := U_1 + \ldots + U_{i-1} + U_{i+1} + \ldots + U_m$.

ii) Aus $u_1 + \ldots + u_m = 0$ mit $u_i \in U_i$ für $i = 1, \ldots, m$ folgt $u_1 = \ldots = u_m = 0$.

iii) Jedes $u \in U$ lässt sich eindeutig schreiben als $u = u_1 + \ldots + u_m$ mit $u_i \in U_i$ für $i = 1, \ldots, m$.

Bemerkung:
Falls eine (und damit alle) der Bedingungen (i), (ii), (iii) erfüllt ist, nennt man U auch direkte Summe der Unterräume und schreibt $U = U_1 \oplus \ldots \oplus U_m$.■

Bemerkung:

- Im Fall $m = 2$ ist $U = U_1 \oplus U_2 \Leftrightarrow U_1 \cap U_2 = \{0\}$ und $U = U_1 + U_2$.
- Falls $(b_1, \ldots, b_m)$ eine (geordnete) Basis von V ist, dann ist $V = Kb_1 \oplus \ldots \oplus Kb_m$ (folgt direkt aus der Definition einer Basis).

4.2.27 Feststellung 35: Dimension der direkten Summe

Bemerkung:
Seien $U_1, U_2, U_3 \subseteq V$ Unterräume. Dann gilt: $(U_1 \oplus U_2) \oplus U_3 = U_1 \oplus (U_2 \oplus U_3)$. Die linke Seite enthält die Aussagen $U_1 \cap U_2 = \{0\}$ und $(U_1 + U_2) \cap U_3 = \{0\}$. Daraus folgt (Übungsaufgabe) $U_1 \cap (U_2 + U_3) = \{0\}$ und damit dann auch $U_2 \cap (U_1 + U_3) = \{0\}$ (vertausche die Rolle von U_1 und U_2).

Falls $\dim U_i = \infty$ für ein $i \in \{1, \ldots, m\}$. Dann ist $\dim(U_1 \oplus \ldots \oplus U_m) = \infty$.
Seien nun die U_i endlich dimensional. Dann gilt

$$\dim(U_1 \oplus \ldots \oplus U_m) = \dim U_1 + \ldots + \dim U_m.$$

Beweis:
Es reicht die Behauptung für $m = 2$ zu zeigen. (trivial vollständige Induktion)
Nach Dimensionssatz gilt:

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \underbrace{\dim(U_1 \cap U_2)}_{= \dim\{0\} = 0}$$

4.2.28 Feststellung 36 und Definition: Produktraum

Seien $W_1, \ldots, W_m$ K-Vektorräume. Dann ist

$$W := W_1 \times \ldots \times W_m$$

mit komponentenweiser Addition und Multiplikation mit Skalaren ein K-Vektorraum. Er heißt der Produktraum von $W_1, \ldots, W_m$.

$$\lambda(x_1, \ldots, x_m) + (y_1, \ldots, y_m) = (\lambda x_1 + y_1, \ldots, \lambda x_m + y_m)$$

Sei $p_i \colon W \to W_i$ mit

$$p_i(x_1, \ldots, x_m) := x_i$$

definiert. Die Projektionen p_i sind linear und surjektiv. Es gilt:

$$W = W_1' \oplus \ldots \oplus W_m',$$

wobei

$$W_i' := \{(0, \ldots, 0, \underbrace{x_i}_{\text{an der } i\text{-ten Stelle}}, 0, \ldots, 0) \mid x_i \in W_i\}.$$

Offensichtlich ist $W_i' \cong W_i$. Man schreibt auch $W = W_1 \oplus \ldots \oplus W_m$ für $W_1 \times \ldots \times W_m$ und nennt dies die (äußere) direkte Summe von $W_1, \ldots, W_m$.■

4.2.29 Feststellung 37: Vektorräume und Isomorphieeigenschaften

Seien U, V, W K-Vektorräume und $f \colon U \to V$ und $g \colon V \to W$ ein Isomorphismen (bijektive lineare Abbildung). Dann sind f^{-1} und $f \circ g$ Isomorphismen.

Beweis:

$$\begin{aligned} f^{-1}(x + \lambda y) &= f^{-1}(\underbrace{f(f^{-1}(x))}_{=x} + \lambda \underbrace{f(f^{-1}(y))}_{=y}) && f \text{ bijektiv} \\ &= f^{-1}(f(f^{-1}(x) + \lambda f^{-1}(y))) && f \text{ linear} \\ &= f^{-1}(x) + \lambda f^{-1}(y) && f \text{ bijektiv} \end{aligned}$$

$$\begin{aligned} (f \circ g)(x + \lambda y) &= f(g(x + \lambda y)) \\ &= f(g(x) + \lambda g(y)) \\ &= f(g(x)) + \lambda f(g(y)) \\ &= (f \circ g)(x) + \lambda (f \circ g)(y) \end{aligned}$$

Bemerkung:
Wenn $f \colon V \to W$ ein Isomorphismus ist, dann übertragen sich alle Begriffe und Eigenschaften (die

mittels + und $\cdot$ definierbar sind).

Beispiele:

- B Basis von $V \Rightarrow f(B)$ Basis von W.
- $M \subseteq V$ linear unabhängig $\Rightarrow f(M) \subseteq W$ linear unabhängig
- $\dim V = n \Rightarrow \dim W = n$.
- ...

4.2.30 Definition: Rang

Sei $\dim V = n, \dim W = m, f\colon V \to W$ lineare Abbildung. Dann heißt

$$\mathrm{Rang}(f) := \dim(f(V))$$

der Rang von f.

4.2.31 Satz 16: Dimensionssatz für lineare Abbildungen

Sei $f\colon V \to W$ eine lineare Abbildung und $\dim(V) < \infty$. Dann sind $f(V)$ und $\ker(f)$ endlich dimensional und

$$\dim(V) = \dim(f(V)) + \dim(\ker(f)),$$

also

$$\dim(V) = \mathrm{Rang}(f) + \dim(\ker(f)).$$

Beweis:
$\ker(f) \subseteq V$, also nach Satz 12 $\dim(\ker(f)) \leqslant \dim(V) < \infty$. Nach Satz 13 gibt es einen zu $\ker(f)$ komplementären Unterraum $U \subseteq V$ mit

$$\ker(f) \cap U = \{0\} \text{ und } U + \ker(f) = V.$$

Sei $f|_U^{f(V)}$ die Einschränkung von f auf U und $f(V)$. Dann ist

$$\ker\left(f|_U^{f(V)}\right) = \ker(f|^{f(V)}) \cap U = \ker(f) \cap U = \{0\}$$

und

$$\begin{aligned} f(V) &= f(U + \ker(f)) \\ &= f(U) + f(\ker f) \\ &= f(U) \\ &= f|_U^{f(V)}(U). \end{aligned}$$

Also ist $f|_U^{f(V)}$ bijektiv, womit $\dim(U) = \dim(f(V))$, wodurch nach Dimensionssatz linearer Unterräumne dann gilt:

$$\dim(V) = \underbrace{\dim(U)}_{=\dim(f(V))} + \dim(\ker(f)) - \dim(\underbrace{U \cap \ker(f)}_{=\{0\}}) = \dim(f(V)) + \dim(\ker(f)).$$

$\mathrm{Rang}\, f = \dim f(V)$ nach Definition.■

4.2.32 Feststellung 38 und Definition: Basisisomorphismus

Sei $B = (b_1, \ldots, b_n)$ eine geordnete Basis von V (also $\dim V = n$). Dann ist die Abbildung $i_B \colon K^n \to V$ mit

$$i_B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \sum_{i=1}^{n} x_i b_i$$

ein Isomorphismus. Er heißt der zu B gehörige Basisisomorphismus.

Beweis:
i_B linear ist klar. i_B ist bijektiv, da wegen $(b_1, \ldots, b_n)$ Basis von V gilt: Jeder Vektor $v \in V$ hat eine eindeutige Darstellung als $v = \sum_{i=1}^{n} x_i b_i$ mit $x_i \in K$.
Die Umkehrabbildung ${i_B}^{-1} \colon V \to K^n$ heißt die Koordinatenabbildung von V zur Basis B, also ${i_B}^{-1}(v) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, wenn $v = \sum_{i=1}^{n} x_i b_i$ die eindeutig bestimmte Darstellung von v als Linearkombination der $b_1, \ldots, b_n$ ist.■
Bemerkung: $i_B(e_i) = \sum_{k=1}^{n} e_{ik} b_k = b_i$

Alternativer Beweis zu Feststellung 38: Laut Feststellung 31 ist $V \cong K^B$ mit P als Isomorphismus. Zeige $K^B \cong K^{\{1,\ldots,n\}} = K^n$. Definiere $f \colon K^B \to K^{\{1,\ldots,n\}}$ für alle $x \in K^B$ und $i \in \{1, \ldots, n\}$:

$$f(x)(i) := x(b_i)$$

f ist ein Isorphismus und somit auch $i_B = P^{-1} \circ f^{-1}$.

4.2.33 Feststellung 39: Isomorphie von Vektorräumen

a) Jeder n-dimensionale K-Vektorraum V ist isomorph zu K^n.
b) Zwei endlich-dimensionale K-Vektorräume V und W sind genau dann isomorph, wenn sie dieselben Dimensionen haben.

Beweis:

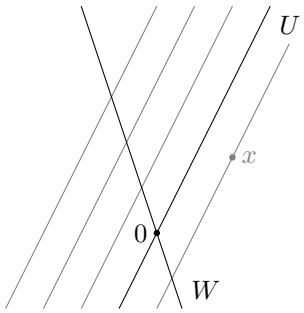
a) Es gibt eine Basis $B = (b_1, \ldots, b_n)$ von V und nach Feststellung 38 ist dann $V \cong K^n$.
b) $V \cong W \Rightarrow \dim V = \dim W$ klar, $\dim V = \dim W = n \Rightarrow V \cong K^n \cong W$.■

4.2.34 Quotientenvektorraum

Sei V ein K-Vektorraum und $U \subseteq V$ ein Unterraum. $(V, +)$ ist eine abelsche Gruppe, $(U, +)$ eine Untergruppe. Betrachte die Faktorgruppe $(V/U, +)$ und den natürlichen Homomorphismus $\mathrm{nat} \colon V \to V/U$, $V/U := \{a + U \mid a \in V\}$. Definiere $\cdot K \times V/U \to V/U$ durch

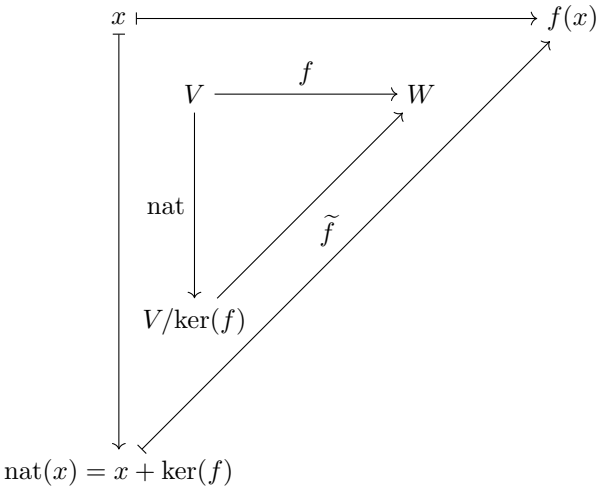
$$\lambda \cdot (x + U) := (\lambda x) + U$$

(Für $\lambda \neq 0$ ist $\lambda\cdot(x+U) = \lambda\cdot U$, aber nicht für $\lambda = 0$) Damit wird $(V/U, +, \cdot)$ ein K-Vektorraum. Er heißt der Quotientenvektorraum von V nach U. $\mathrm{nat}\colon V \to V/U$ wird damit eine lineare Abbildung.
Begründung: Für $\lambda, \mu \in K$, $x + y \in V/U$, $y + U \in V/U$:
$(\lambda+\mu)\cdot(x+U) = (\lambda+\mu)\cdot x+U = (\lambda x+\mu x)+U = (\lambda x+U)+(\mu x+U) = \lambda\cdot(x+U)+\mu\cdot(x+U)$
$\lambda \cdot (x + U + y + U) = ((\lambda x) + U) + ((\lambda y) + U)$
$\mathrm{nat}(\lambda x) = \lambda x + U = \lambda \cdot (x + U) = \lambda \cdot \mathrm{nat}(x)$
Veranschaulichung:
Beispiel: $V = \mathbb{R}^2$, U 1-dimensionaler linearer Unterraum.
$V/U = \{x + U | x \in V\}$ Menge der zu U parallel Geraden.
W ein zu U komplementärer Unterraum als vollständiges Repräsentantensystem von V/U

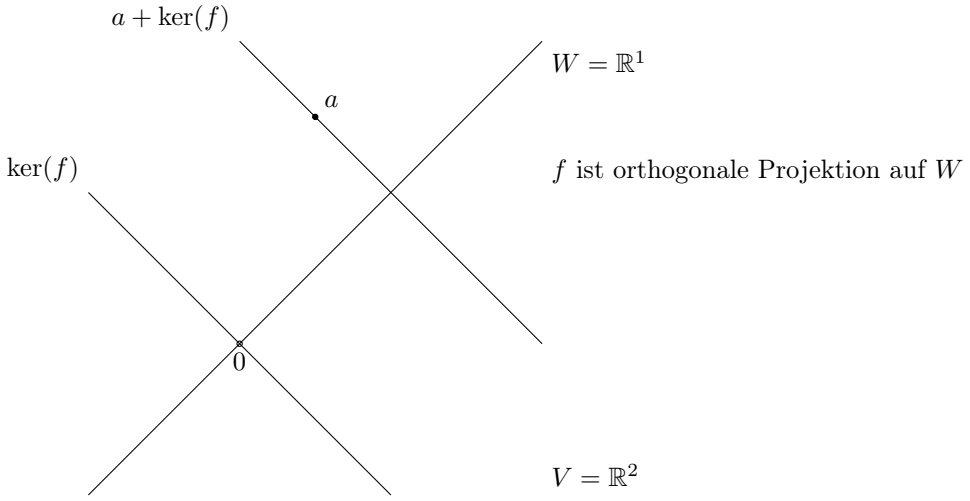


4.2.35 Satz 2.19: Homomorphiesatz für Vektorräume

Seien V, W K-Vektorräume und $f\colon V \to W$ eine lineare Abbildung. Dann gibt es genau eine lineare Abbildung $\tilde{f}\colon V/\ker(f) \to W$ mit $f = \tilde{f} \circ \mathrm{nat}$, $V/\ker(f) := \{a + \ker(f) \mid a \in V\}$. f ist injektiv und falls f surjektiv ist, dann ist $\tilde{f}$ ein Isomorphismus



Beweis: Nach dem Homomorphiesatz 1.9 für Gruppen gibt es genau einen Gruppenhomomorphismus von $(V/\ker(f), +)$ nach $(W, +)$ mit $f = \tilde{f} \circ \mathrm{nat}$. Für jedes $x \in V$, $\lambda \in K$ gilt: $\tilde{f}(\lambda \cdot (x + \ker(f))) = \tilde{f}(\lambda\cdot x+\ker(f)) = \tilde{f}(\mathrm{nat}(\lambda\cdot x)) = (\tilde{f}\circ\mathrm{nat})(\lambda\cdot x) = f(\lambda\cdot x) \overset{f \text{ linear}}{=} \lambda f(x) = \lambda\tilde{f}(\mathrm{nat}(x)) = \lambda\tilde{f}(x + \ker(f))$ Damit ist f eine lineare Abbildung.



4.2.36 Feststellung 40: lineare Fortsetzung

Falls $\dim V = \infty$ mit AC für b). Sei V, W K-Vektorräume, $B \subseteq V$ und $f\colon B \to W$ eine Abbildung.

a) Falls B eine Basis von V ist, dann gibt es genau eine lineare Fortsetzung $f'\colon V \to W$ von f (Fortsetzung heißt $f'(b) = f(b)$ für alle $b \in B$)
b) Falls B linear unabhängig ist, dann gibt es mindestens eine lineare Fortsetzung $f'\colon V \to W$ von f.
c) Falls $\mathrm{Lin}(B) = V$, dann gibt es höchstens eine (d. h. entweder genau eine oder gar keine) lineare Fortsetzung $f'\colon V \to W$ von f.

Beweis:
Eindeutigkeit von a) c): Sei $\mathrm{Lin}(B) = V$ und f'', $f'\colon V \to W$ linear mit $f'(b) = f(b) = f''(b)$ für alle $b \in B$. Jeder Vektor $v \in V$ lässt sich schreiben als $\sum_{i=1}^{n} \lambda_i b_i$, damit

$$f'(v) = f'\left(\sum_{i=1}^{n} \lambda_i b_i\right) = \sum_{i=1}^{n} \lambda_i f'(b_i) = \sum_{i=1}^{n} \lambda_i f''(b_i) = f''(v)$$

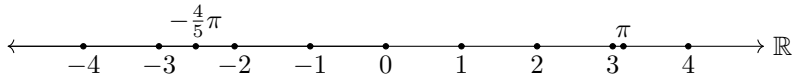
Also ist f' eindeutig bestimmt.

a) Falls B eine Basis ist, dann ist $v = \sum\limits_{b \in B} \lambda_b b$ eindeutig bestimmt.
$f'(v) := \sum\limits_{b \in B} \lambda_b f(b)$ ist somit wohldefiniert. Es gilt $f'(b) = 1 \cdot f(b) = f(b)$.
Linearität: Übung.
b) Setze B nach Satz 8 (Mengen zu Basen mit AC) zu einer Basis $\bar{B}$ von V fort und definiere $\bar{f}\colon \bar{B} \to V$ durch
$$\bar{f}(b) := \begin{cases} f(b) & , \text{falls } b \in B \\ 0 & , \text{falls } b \in \bar{B} \setminus B \end{cases}$$
Setze $\bar{f}$ gemäß a) eindeutig zu einer linearen Abbildung $f'\colon V \to W$ fort.■

Sei K ein Körper, L ein Unterkörper. Dann können wir K als L-Vektorraum auffassen. Bezeichne ihn L^K

$$\cdot : L \times K \to K$$
$$(\lambda, x) \mapsto \lambda \cdot x$$

Beispiel $K := \mathbb{R}$, $L := \mathbb{Q}$:



4.2.37 Satz 15: Charakterisierung endlicher Körper

1)
Sei K ein endlicher Körper. Dann gilt: $|K| = p^n$, wobei $p = \operatorname{char} K$ ist, also p eine Primzahl und $n \in \mathbb{N}$, nämlich $n = \dim_{L^K}$, wobei L der Primkörper von K ist.

2)
Sei p eine Primzahl und $q = p^n$. Dann gibt es bis auf Isomorphie genau einen Körper $(K, +, \cdot)$ mit q Elementen. Ferner gilt: $(K, +) \cong (\underbrace{Z_p \times \ldots \times Z_p}_{n\text{-mal}}, +) = (Z_p^n, +)$. $(K \setminus \{0\}, \cdot) \cong (Z_{q-1}, +)$.

Beweis:
zu 1)
$L = \{0, 1, 2, \ldots, p-1\} \cong Z_p$ ist der kleinste Unterkörper von K. Es gilt $K \cong Z_p^n$ und damit $|K| = |Z_p^n| = |Z_p|^n = p^n$.

Die übrigen Aussagen werden in der Vorlesung „Algebra und Zahlentheorie' bewiesen." ■

5 Matrizen und lineare Abbildungen

5.1 Matrizen

5.1.1 Definition: Matrix

Eine **Matrix** ist ein Schema der Form

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

wobei $m, n \in \mathbb{N}$ und $a_{ij} \in K$ für $i = 1, \ldots, m, j = 1, \ldots, n$. Zum Beispiel:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} & a_{18} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} & a_{28} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} & a_{37} & a_{38} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} & a_{47} & a_{48} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & a_{56} & a_{57} & a_{58} \\ a_{61} & a_{62} & & a_{64} & a_{65} & a_{66} & a_{67} & a_{68} \\ a_{71} & a_{72} & a_{73} & a_{74} & a_{75} & a_{76} & a_{77} & a_{78} \end{pmatrix}$$

Freie Stellen bedeuten $0 \in K$. A heißt eine Matrix über K mit m Zeilen und n Spalten oder eine $m \times n$-**Matrix mit Koeffizienten in** K. (Sprich: „m Kreuz n“) A heißt vom Typ $m \times n$. a_{ij} nennt man den Koeffizienten der Matrix an der Stelle (i, j).

Eine **quadratische Matrix** ist eine $(m \times n)$-Matrix mit $m = n$ (also eine $n \times n$-Matrix). Sehr formal kann man eine Matrix als Abbildung $A\colon \{1, \ldots, m\} \times \{1, \ldots, n\} \to K$ mit $(i, j) \mapsto a_{ij}$ definieren. Die Menge aller $m \times n$-Matrizen über K wird mit $K^{m,n}$ bezeichnet:

$$K^{m,n} := K^{\{1,\ldots,m\} \times \{1,\ldots,n\}}$$

Statt $K^{m,n}$ schreibt man manchmal auch $K^{m \times n}$.

Damit ergibt sich sofort, dass $K^{m,n}$ ein K-Vektorraum ist mit Dimension

$$\dim K^{m,n} = \dim K^{\{1,\ldots,m\} \times \{1,\ldots,n\}} = |\{1, \ldots, m\} \times \{1, \ldots, n\}| = m \cdot n$$

Somit ist

$$K^{m,n} \cong K^{m \cdot n}$$

wobei Addition und Multiplikation mit Skalaren komponentenweise definiert sind.

5.1.2 Rechnen mit Matrizen

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} := \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{pmatrix}$$

$$\lambda \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} := \begin{pmatrix} \lambda a_{11} & \cdots & \lambda a_{1n} \\ \vdots & \ddots & \vdots \\ \lambda a_{m1} & \cdots & \lambda a_{mn} \end{pmatrix}$$

Kurzschreibweise:
$(a_{ij}) := (a_{ij})_{ij} := (a_{ij})_{1 \leqslant i \leqslant m, 1 \leqslant i \leqslant n} = A$, $B = (b_{ij})$, $A + B = (a_{ij} + b_{ij})$, $\lambda A = (\lambda a_{ij})$. Die Kurzschreibweise nur verwenden, wenn aus dem Kontext klar ist, dass (a_{ij}) eine $m \times n$-Matrix ist.

Die Menge der Matrizen, die genau einen Koeffizienten 1 haben und bei denen alle anderen Koeffizienten 0 sind, bilden eine Basis von $K^{m,n}$.

5.1.3 Blockmatrizen

Seien $A_{i,j}$ Matrizen, sodass für alle $i, j, k, l, m, n, o, p, q \in \mathbb{R}$ mit $i, k \leqslant m$ sowie $j, l \leqslant n$ gilt, dass

$$A_{i,j} \in K^{o,p} \Leftrightarrow A_{k,l} \in K^{q,r}$$

falls $i = k \wedge p = r$ oder $j = l \wedge o = q$ ist.
Blockmatrizen entsteht durch zusammensetzen der $A_{i,j}$ Matrizen.

$$B = \begin{bmatrix} A_{11} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \cdots & A_{m,n} \end{bmatrix}$$

Die Kastenklammern weisen auf eine Blockmatrix hin.

5.1.4 Bemerkung und Konvention

$(m \times 1)$-Matrizen heißen auch Spaltenvektoren
$(1 \times n)$-Matrizen heißen auch Zeilenvektoren
(1×1)-Matrizen werden auch als Skalare, d. h. Körperelemente, aufgefasst

Wir wollen im Weiteren K^m als Menge von $(m \times 1)$-Matrizen auffassen.

5.1.5 Bezeichnungen

Sei

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

eine $m \times n$-Matrix. Die Vektoren

$$a_j := \begin{matrix} | \\ a_j \\ | \end{matrix} := \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in K^m \cong K^{m,1}$$

heißen die **Spaltenvektoren** der Matrix A. Schreibweise:

$$A = \begin{bmatrix} | & & | \\ a_1 & \cdots & a_n \\ | & & | \end{bmatrix} =: (a_1, \ldots, a_n)$$

d. h. ein n-Tupel von Vektoren in K^m wird auch als $m \times n$-Blockmatrix aufgefasst. Entsprechend heißen

$$a'_i := \begin{matrix} - \\ a'_n \\ - \end{matrix} := (a_{i1}, \ldots, a_{in}) \in K^n \cong K^{1,n}$$

die **Zeilenvektoren** von A Schreibweise:

$$A = \begin{bmatrix} - & a'_1 & - \\ & \vdots & \\ - & a'_m & - \end{bmatrix} =: \begin{pmatrix} a'_1 \\ \vdots \\ a'_m \end{pmatrix}$$

Ein m-Tupel von Zeilenvektoren wird als $m \times n$-Blockmatrix aufgefasst.

5.1.6 Definition: transponierte Matrix

Die **transponierte Matrix** A^T entsteht durch Vertauschen der Spalten mit den Zeilen, d. h.:

$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}^T := \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}$, also wenn $A \in K^{m,n}$ dann ist $A^T \in K^{n,m}$.

Beispiel: $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$

5.2 Matrixbeschreibung linearer Abbildungen

Seien $B = (b_1, \ldots, b_n)$, bzw. $C = (c_1, \ldots, c_m)$ geordnete Basen der K-Vektorräume V bzw. W (also $\dim V = n, \dim W = m$) und $f\colon V \to W$ eine lineare Abbildung. Dann ist f nach Feststellung 40 durch die Angabe der Bildvektoren $f(b_1), \ldots, f(b_n)$ eindeutig bestimmt. Jeden dieser Bildvektoren kann man eindeutig in der Form

$$f(b_j) = \sum_{i=1}^{m} a_{ij} c_i \tag{1}$$

schreiben, mit $a_{ij} \in K$, für $i = 1, \ldots, m, j = 1, \ldots, n$.

Wir nennen die $(m \times n)$-Matrix ${}_B^C M_f = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} =: A$ die **Matrix von f bezüglich der geordneten Basen B und C.**

Andererseits kann man die $a_{ij} \in K$ ($i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}$) beliebig vergeben und erhält eine eindeutig bestimmte lineare Abbildung f_A, für die (1) gilt (vgl. Feststellung 40). ${}_B^C f_A$ nennt man die durch die Matrix $A \in K^{m,n}$ **beschriebene lineare Abbildung bezüglich der Basen B und C.** Es gilt dann also

$$f\left(\sum_{j=1}^{n} x_j b_j\right) = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} x_j c_i \tag{2}$$

Beweis:

$$f\left(\sum_{j=1}^{n} x_j b_j\right) = \sum_{j=1}^{n} f(x_j b_j) = \sum_{j=1}^{n} x_j f(b_j) \overset{(1)}{=} \sum_{j=1}^{n} x_j \sum_{i=1}^{m} a_{ij} c_i = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} x_j c_i$$

Wir haben also eine natürliche Bijektion zwischen der Menge der linearen Abbildungen $f\colon V \to W$ (V mit Basis B, W mit Basis C, $\dim V = n$, $\dim W = m$) und $K^{m,n}$.
Besonders einfach ist die Situation, wenn $V = K^n$, $W = K^m$ gilt und die Basen B, C die Standardbasen sind, d. h. $B = (e_1, \ldots, e_n)$, $C = (e_1, \ldots, e_m)$.

$$f\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = f\left(\sum_{j=1}^{n} x_j e_j\right) \overset{(2)}{=} \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} x_j e_i = \sum_{i=1}^{m} \underbrace{\left(\sum_{j=1}^{n} a_{ij} x_j\right)}_{\in K} e_i = \begin{pmatrix} \sum_{j=1}^{n} a_{1j} x_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj} x_j \end{pmatrix} \tag{3}$$

Wenn $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = f(x)$, dann ist also

$$y_i = \sum_{j=1}^{n} a_{ij} x_j. \tag{4}$$

Insbesondere gilt für $k \in \{1, \ldots, n\}$, dass

$$f(e_k) = \begin{pmatrix} \sum_{j=1}^{n} a_{1j} e_{kj} \\ \vdots \\ \sum_{j=1}^{n} a_{mj} e_{kj} \end{pmatrix} = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix} \tag{5}$$

d. h. das Bild des k-ten Standardbasisvektors e_k ist gleich dem k-ten Spaltenvektor der zugehörigen Matrix, d. h. a_{ij} ist die i-te Komponente des Bildes von e_j unter f:

$$a_{ij} = p_i(f(e_j)) \tag{6}$$

Wir haben also in natürlicher Weise eine Bijektion zwischen der Menge der linearen Abbildungen $f\colon K^n \to K^m$ und der Menge der $(m \times n)$-Matrizen über K bezüglich der Standardbasen. Ist $A \in K^{m,n}$, dann soll die durch A beschriebene lineare Abbildung f_A bzgl. der Standardbasen mit demselben Symbol $A := f_A$ bezeichnet werden, d. h. die Matrix wird als lineare Abbildung $K^n \to K^m$ aufgefasst. Damit ist $Ax = A(x) = f_A(x) = y$ und mit (3):

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} \tag{7}$$

Umgekehrt gilt für die Matrix M_f zur linearen Abbildung $f\colon K^n \to K^m$ bzgl. der Standardbasen:

$$M_f = (f(e_1), \ldots, f(e_n))$$

Wenn $A = \begin{pmatrix} a_1' \\ \vdots \\ a_m' \end{pmatrix}$ mit $a_i' = (a_{i1}, \ldots, a_{in})$ und $(a_{i1}, \ldots, a_{in}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \sum_{k=1}^{n} a_{ik} x_k$ dann ist

$$Ax = \begin{pmatrix} a_1' x \\ \vdots \\ a_m' x \end{pmatrix}$$

Für lineare Abbildungen $g\colon K^n \to K^m$ und $f\colon K^m \to K^l$ ist die Komposition $f \circ g$ definiert. Da wir Matrizen als lineare Abbildungen auffassen und umgekehrt, ist damit das Produkt von Matrizen $A \in K^{l,m}, B \in K^{m,n}$ erklärt als Komposition der zugehörigen Abbildungen. Definiere $AB \in K^{l,n}$ durch

$$AB := M_{f_A \circ f_B} \tag{8}$$

5.2.1 Das Produkt von Matrizen

Für Matrizen $A = (a_{ij}) \in K^{l,m}, B = (b_{ij}) \in K^{m,n}$ ist das Produkt $C := AB$, $C = (c_{ij}) \in K^{l,n}$, durch

$$c_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj} \tag{9}$$

mit $1 \leq i \leq l$ und $\leq j \leq n$ gegeben.

Beweis:

$$\begin{aligned} c_{ij} &\overset{(6)}{=} p_i(f_C(e_j)) = p_i(f_{AB}(e_j)) \overset{(8)}{=} p_i(f_{C_{f_A \circ f_B}}(e_j)) \\ &= p_i((f_A \circ f_B)(e_j)) = p_i(f_A(f_B(e_j))) \\ &\overset{(5)}{=} p_i\left(f_A\begin{pmatrix} b_{1j} \\ \vdots \\ b_{mj} \end{pmatrix}\right) \overset{(3)}{=} p_i\begin{pmatrix} \sum_{k=1}^{m} a_{1k}b_{kj} \\ \vdots \\ \sum_{k=1}^{m} a_{lk}b_{kj} \end{pmatrix} = \sum_{k=1}^{m} a_{ik}b_{kj} \end{aligned}$$

Bemerkung:
(7) ist ein Spezialfall von (9). ($n = 1$)

Also:

$$AB = \begin{bmatrix} — & a_1' & — \\ & \vdots & \\ — & a_m' & — \end{bmatrix} \begin{bmatrix} | & & | \\ a_1 & \cdots & a_n \\ | & & | \end{bmatrix} = (a_i' b_j)_{1 \leqslant i \leqslant l, 1 \leqslant j \leqslant n}$$

Beispiel:

$$\begin{pmatrix} 1 & 2 & 0 \\ 3 & 0 & 4 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 5 & 8 \\ 1 & 8 \end{pmatrix} = \begin{pmatrix} 1\cdot 2 + 2\cdot 5 + 0\cdot 1 & 1\cdot 0 + 2\cdot 8 + 0\cdot 8 \\ 3\cdot 2 + 0\cdot 5 + 4\cdot 1 & 3\cdot 0 + 0\cdot 8 + 4\cdot 8 \end{pmatrix} = \begin{pmatrix} 12 & 16 \\ 10 & 32 \end{pmatrix}$$

Falksches Schema:

$$\begin{array}{cc} & B \\ A & AB \end{array}$$

$$\begin{array}{cc} & \begin{bmatrix} 2 & 0 \\ 5 & 8 \\ 1 & 8 \end{bmatrix} \\ \begin{bmatrix} 1 & 2 & 0 \\ 3 & 0 & 4 \end{bmatrix} & \begin{bmatrix} 12 & 16 \\ 10 & 32 \end{bmatrix} \end{array}$$

Matrix zur identischen Abbildung $\mathrm{id}\colon K^n \to K^n$ ist:

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

Matrix zur i-ten Projektion $p_i\colon K^n \to K$ ist: (1 an der i-ten Stelle)

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} = e_i^T$$

Was für Abbildungen beschreibt die 1×1-Matrix

$$f_{(a)}\colon K \to K$$

$$x \mapsto ax$$

Der Spaltenvektor $v \in K^m$ aufgefasst als $m \times 1$-Matrix beschreibt die Abbildung $K \to K^m$ mit $x \mapsto xv$.

Beispiel:

$$\lambda \cdot E_n = \begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix} \text{ mit } x \mapsto \lambda x.$$

Geometrisch beschreibt dies eine Streckung um den Faktor λ (für $\lambda < 0$ Streckung mit $|\lambda|$ mit anschliessender Spiegelung am Punkt 0.

Es gilt (wenn die Produkte definiert sind): $A(BC) = (AB)C$. Beweis ist klar, da das Assoziativgesetz für die zugehörigen linearen Abbildungen gilt und wir die natürlichen Bijektionen zwischen der $K^{m,n}$ und der Menge der linearen Abbildungen $K^n \to K^m$ haben und das Produkt von Matrizen dem Produkt der linearen Abbildungen entspricht.
Beweis:

$$A(BC) = A(M_{f_B \circ f_C}) = M_{f_A \circ f_{\left(M_{f_B \circ f_C}\right)}} = M_{f_A \circ (f_B \circ f_C)}$$
$$(AB)C = (M_{f_A \circ f_B})C = M_{f_{\left(M_{f_A \circ f_B}\right)} \circ f_C} = M_{(f_A \circ f_B) \circ f_C}$$

Beispiel:

$$\begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \begin{pmatrix} 3 & -6 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ aber } \begin{pmatrix} 3 & -6 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} -8 & -27 \\ 3 & 9 \end{pmatrix}$$

Dieses Beispiel zeigt, dass für quadratische $(n \times n)$-Matrizen A, B gelten kann:

1) $AB \neq BA$
2) $AB = 0$, aber $A \neq 0$, $B \neq 0$, $BA \neq 0$

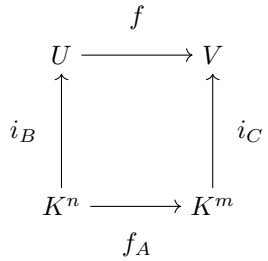
Beispiel:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, A^2 = AA = 0 \text{ aber } A \neq 0$$

5.2.2 Beziehung zwischen linearer Funktion und Matrix

Seien U und V endlich dimensionale K-Vektorräume und $f\colon U \to V$ eine lineare Abbildung. $A \in K^{m,n}$ eine Matrix. Des Weiteren sei:

$$B = (b_1, \ldots, b_n) \text{ geordnete Basis von } U, \quad \dim U = n$$
$$C = (c_1, \ldots, c_m) \text{ geordnete Basis von } V, \quad \dim V = m$$



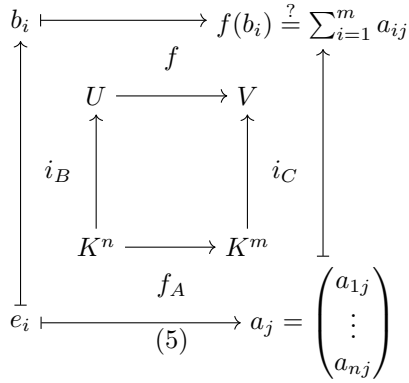
i_B und i_C sind die Basisisomorphismen. f_A ist die lineare Abbildung zur Matrix A **bezüglich der Standardbasen**. Es gilt dann:

$$\begin{aligned} & f & = & \; i_C \circ f_A \circ {i_B}^{-1} \\ \Leftrightarrow \quad & f(b_j) & = & \sum_{i=1}^{m} a_{ij} c_i \end{aligned}$$

Dies ist gleichbedeutend mit: $f \circ i_B = i_C \circ f_A$ gilt genau dann, wenn A die Matrix zu f ist **bezüglich der Basen B und C**:

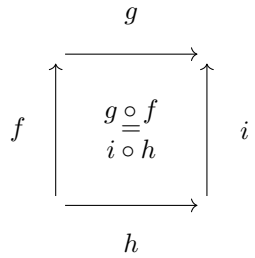
$$f \circ i_B = i_C \circ f_A \Leftrightarrow A = {}_B^C M_f$$

Beweis:
Nach Feststellung 40 Lineare Fortsetzung sind die Funktionen $f \circ i_B$ und $i_C \circ A$ gleich, genau dann wenn sie die Elemente der Standardbasis gleich abbilden.

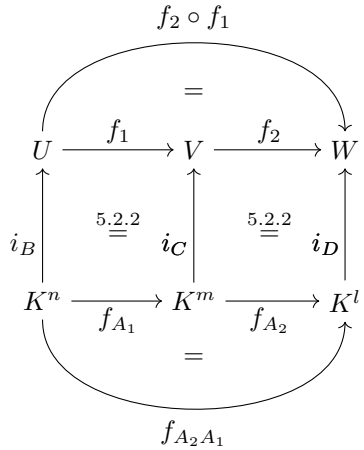


5.2.3 kommutive Diagramme

Man sagt ein Diagramm von Abbildungen ist kommutativ, wenn für je zwei gerichtete Abbildungswege von Pfeilen mit derselben Quelle und demselben Ziel gleich abbilden.



Seien $f_1 \colon U \to V$, $f_2 \colon V \to W$ lineare Abbildungen. Sei $A_1 := {}_B^C M_{f_1}$ die Matrix von f_1 bez. B und C. $A_2 := {}_C^D M_{f_2}$ die Matrix von f_2 bez. C und D. Dann ist das folgende Diagramm von linearen Abbildungen kommutativ:



Wobei i_B, i_C, i_D die Basisisomorphismen sind. f_{A_1} ist die zugehörige lineare Abbildung zur Matrix A_1 bezüglich der Standardbasen. Der vorherige Satz ergibt $f_1 \circ i_B = i_C \circ f_{A_1}$ und $f_2 \circ i_C = i_D \circ f_{A_2}$.

Es folgt:

$$\begin{aligned}(f_2 \circ f_1) \circ i_B &= f_2 \circ (i_C \circ f_{A_1}) \\ &= (i_D \circ f_{A_2}) \circ f_{A_1} \\ &= i_D \circ f_{A_2 A_1}\end{aligned}$$

Damit folgt aus dem vorherigen Satz, dass A_2A_1 die Matrix von $f_2 \circ f_1$ bezüglich der Basen B und D ist. Also

$${}^{D}_{B}M_{f_2 \circ f_1} = \left({}^{D}_{C}M_{f_2}\right)\left({}^{C}_{B}M_{f_1}\right)$$

5.2.4 Bemerkung

Für

$$A = \begin{bmatrix} | & & | \\ a_1 & \cdots & a_n \\ | & & | \end{bmatrix}$$

gilt:

$$\sum_{j=1}^{n} \lambda_j a_j = \sum_{j=1}^{n} \lambda_j \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = \sum_{j=1}^{n} \begin{pmatrix} a_{1j}\lambda_j \\ \vdots \\ a_{mj}\lambda_j \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} a_{1j}\lambda_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj}\lambda_j \end{pmatrix} \overset{(7)}{=} A \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

Somit

$$AK^n = \{Ax | x \in K^n\} = \mathrm{Lin}\{a_1, \ldots, a_n\}$$

5.2.5 Rang einer Matrix

Sei $A \in K^{m,n}, A = (a_1, \ldots, a_n)$ (a_i Spaltenvektoren von A). Dann heißt

$$\mathrm{Rang}(A) := \dim \mathrm{Lin}\{a_1, \ldots, a_n\}$$

der Rang von A.

5.2.6 Feststellung 41

Sei $\dim V = n, \dim W = m, f\colon V \to W$ linear, seien B und C Basen von V bzw. W und A die Matrix von f bez. B und C. Dann gilt:

$$\mathrm{Rang}(f) = \mathrm{Rang}(A)$$

Beweis:
i_B, i_C sind Isomorphismen. $A = {i_C}^{-1} \circ f \circ i_B$ und $\mathrm{Lin}\{a_1, \ldots, a_n\} = \{Ax | x \in K^n\}$, also $\mathrm{Rang}(A) = \dim({i_C}^{-1} \circ f \circ i_B)(K^n) = \dim({i_C}^{-1}(f(V))) = \dim f(V) = \mathrm{Rang}(f)$, da der Isomorphismus ${i_C}^{-1}$ die Dimension bewahrt.■

5.2.7 Feststellung 42

Es gilt: Rang(A) ist die Anzahl der Spaltenvektoren eines maximalen linear unabhängigen System von verschiedenen Spaltenvektoren der Matrix, also für $a_{i_1}, \ldots, a_{i_r}$ ist $(a_{i_1}, \ldots, a_{i_r})$ linear unabhängig und jeder weitere Spaltenvektor von A ist davon linear abhängig.

Beweis:
$\{a_1, \ldots, a_n\}$ ist ein Erzeugendensystem des Unterraums $\mathrm{Lin}\{a_1, \ldots, a_n\}$. Daher gibt es eine Basis $B \subseteq \{a_1, \ldots, a_n\}$ (Satz 9, ohne AC, da $\dim W < \infty$). Diese Basis hat Rang(A) Elemente und ist ein maximal linear unabhängiges System.

5.2.8 Feststellung 42: Dimensionen und lineare Abbildungen

Sei $f\colon V \to W$ linear und $\dim V < \infty$. Dann gilt:

a)	f injektiv	$\Leftrightarrow$	$\mathrm{Rang}\, f = \dim V$
b)	f surjektiv	$\Leftrightarrow$	$\mathrm{Rang}\, f = \dim W$
c)	f bijektiv	$\Leftrightarrow$	$\mathrm{Rang}\, f = \dim W = \dim V$
d)	$\mathrm{Rang}\, f \leq \dim V$	und	$\mathrm{Rang}\, f \leq \dim W$

Beweis:
klar mit Satz 16 und f injektiv $\Leftrightarrow \ker f = \{0\}$, $f(V) = W \Leftrightarrow \dim f(V) = \dim W$ (wegen $\dim V < \infty$).■

Bemerkung:
Falls $\dim V = \dim W < \infty$, dann gilt: f injektiv $\Leftrightarrow f$ surjektiv.

5.2.9 Feststellung 42': für Matrizen formuliert

Sei $A \in K^{m,n}$. Die lineare Abbildung $A\colon K^n \to K^m$ ist

a)	A injektiv	$\Leftrightarrow$	$\mathrm{Rang}\, A = n$
b)	A surjektiv	$\Leftrightarrow$	$\mathrm{Rang}\, A = m$
c)	f bijektiv	$\Leftrightarrow$	$\mathrm{Rang}\, A = n = m$ (quadratische Matrix)
d)	$\mathrm{Rang}\, A \leq n$	und	$\mathrm{Rang}\, A \leq m$ ■

5.2.10 Definition: invertierbar

Eine Matrix $A \in K^{m,n}$ heißt invertierbar, falls es eine Matrix A^{-1} gibt, mit $A^{-1}A = AA^{-1} = E$.
$A \in K^{m,n}$ ist also genau dann invertierbar, wenn $\mathrm{Rang}\, A = n = m$.

5.2.11 Definition: Endomorphismenmenge

Bezeichne $End(V) := \{f: V \to V | f \text{ lineare Abbildung}\}$ die Menge der Endomorphismen von V.

5.2.12 Feststellung 43: Aussagenäquivalenz Dimensionen und lineare Abbildungen

Sei $f: V \to V$ linear und $\dim V = n < \infty$. Dann sind äquivalent:

a) f ist ein Automorphismus von V (d. h. $f: V \to V$ ist bijektiv)
b) $\operatorname{Rang} f = n$
c) f ist injektiv
d) f ist surjektiv
e) es gibt ein $g \in End(V)$ mit $g \circ f = id$
f) es gibt $h \in End(V)$ mit $f \circ h = id$

Beweis:
klar mit Feststellung 42. ■

5.2.13 Feststellung 43': Entsprechend für quadratische Matrizen

Sei $A \in K^{n,n}$. Dann sind äquivalent:

a) A ist invertierbar
b) $\operatorname{Rang} A = n$
c) $A: K^n \to K^n$ ist injektiv
d) $A: K^n \to K^n$ ist surjektiv
e) es gibt $B \in K^{n,n}$ mit $BA = E_n$ (Einheitsmatrix)
f) es gibt $C \in K^{n,n}$ mit $AC = E_n$ (Einheitsmatrix)

Beweis:
klar mit Feststellung 42. ■

5.2.14 Definition und Feststellung 43: Vektorräume und Homomorphismen

$Hom(V,W) := \{f: V \to W | f \text{ lineare Abbildung}\}$ mit $(f+g)(x) := f(x) + g(x)$ für $x \in V, f, g \in Hom(V,W)$. $(\lambda f)(x) := \lambda f(x)$ für $x \in V, \lambda \in K, f \in Hom(V,W)$ ist ein K-Vektorraum (also insbesondere $f + g \in Hom(V,W), \lambda f \in Hom(V,W)$ für $f, g \in Hom(V,W)$).

Beweis:
einfaches Nachrechnen ■

5.2.15 Feststellung 44: Rechenregeln mit Hom

Für alle $f_1, f_2 \in Hom(U,V), g_1, g_2 \in Hom(V,W), \lambda \in K$ gilt:

- $g_1 \circ (f_1 + f_2) = g_1 \circ f_1 + g_1 \circ f_2$
- $(g_1 + g_2) \circ f_1 = g_1 \circ f_1 + g_2 \circ f_1$
- $(\lambda g_1) \circ f_1 = \lambda(g_1 \circ f_1)$
- $g_1 \circ (\lambda f_1) = \lambda(g_1 \circ f_1)$

Beweis:
einfaches Nachrechnen. Anwendung der linearen Abbildung auf $u \in U$.

Beispiel:
$(g_1 \circ (f_1 + f_2)(u) = g_1((f_1 + f_2)(u)) = g_1(f_1(u) + f_2(u)) = g_1(f(u)) + g_1(f(u)) = (g_1 \circ f_1)(u) + (g_1 \circ f_2)(u)$ für alle $u \in U$. also $g_1 \circ (f_1 + f_2) = (g_1 \circ f_1) + (g_1 \circ f_2)$■

5.2.16 Feststellung 45: Rechenregeln mit Hom

Seien B, C geordnete Basen von V bzw. W und $\dim V < \infty, \dim W < \infty$. Seien $f_1 \colon V \to W$, $f_2 \colon V \to W$ lineare Abbildungen, $\lambda \in K$. Seien A_1 bzw. A_2 die Matrizen von f_1 bzw. f_2 bezüglich B und C. Dann ist $A_1 + A_2$ die Matrix von $f_1 + f_2$ bezüglich B und C und λA die Matrix von λf_1 bezüglich B und C.

Beweis:
klar, einfaches Nachrechnen. ■

5.2.17 Feststellung 46: Abhängigkeiten und Dimensionen

Falls $\dim V = U$, $\dim W = m$, dann ist $Hom(V,W) \cong K^{m,n}$.

Beweis:
wähle in V bzw. W geordnete Basen, wende Feststellung 45 an. ■

5.3 Rechenregeln für Matrizen

5.3.1 Feststellung 47: Rechenregeln

Seien $A_1, A_2 \in K^{m,n}, B_1, B_2 \in K^{m,n}$. Dann gilt:

- $(B_1 + B_2)A_1 = B_1A_1 + B_2A_1$
- $B_1(A_1 + A_2) = B_1A_1 + B_1A_2$
- $(\lambda B_1)A_1 = \lambda(B_1A_1)$
- $B_1(\lambda A_1) = \lambda(B_1A_1)$

Beweis: direkte Folgerung aus Feststellung 45 und 44 bezüglich der Standardbasen. ■

5.3.2 Definition: Algebra

Sei K ein Körper. Ein Ring R mit 1, der gleichzeitig ein K-Vektorraum ist, sodass $\lambda(gf) = (\lambda g)f = g(\lambda f)$ für alle $\lambda \in K, f, g \in R$ gibt, heißt eine Algebra (mit 1) über K, kurz K-Algebra. Also ist $K^{m,n}$ eine K-Algebra.

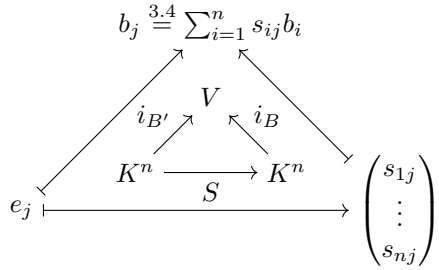
5.3.3 Definition: Übergangsmatrix

Seien $B = (b_1, \ldots, b_n)$, $B' = (b'_1, \ldots, b'_n)$ (geordnete) Basen von V. Dann kann man die Basiselemente in B' darstellen, d. h. es gibt eindeutig bestimmte $s_{ij} \in K$ und

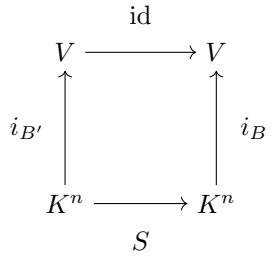
$$b'_j = \sum_{i=1}^{h} s_{ij} b_i \tag{3.6}$$

Die Matrix $S = (s_{ij})_{i,j}$ heißt die Übergangsmatrix von B nach B'.

Bemerkung:
Nach Definition der Übergangsmatrix ist das folgende Diagramm kommutativ:



Das heißt $i_{b'} = i_b \cdot s$ oder $s = i_b^{-1} \circ i_b$, also ist s invertierbar und $s^{-1} = i_b'^{-1} \cdot i_b$. i_b, i'_b sind die Basisisomorphismen der übergangsmatrix von B' nach B.



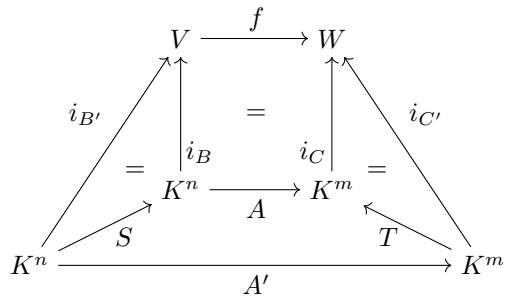
Also ist S die Matrix zur Abbildung $id\colon V \to V$ bebzüglich der Basen B' und B.

5.3.4 Satz 17: Transformation der Matrix zu einer linearen Abbildung bei Wechsel der Basen

Sei $\dim V = n$, $\dim W = m$, B und B' seien Basen von V, C und C' seien Basen von W und $f\colon V \to W$ eine lineare Abbildung. Sei A die Matrix von f bezüglich der Basen B und C und A' dieMatrix von f bezüglich B' und C', dann gilt $A' = T^{-1}AS$, wobei S die übergangsmatrix von B nach B' und T die Übergangsmatrix von C nach C' ist.

Beweis:
$A' = i_C'^{-1} \circ f \circ i_B' = (i_C T)^{-1} \circ f \circ (i_B \circ S) = T^{-1}(i_c^{-1} f i_B)S = T^{-1}AS$ ■

Als Diagramm:



Bei Endomorphismen $f\colon V \to V$ wird man im Allgemeinen f ür V jedes Mal dieselbe Basis B wählen. Statt 'A ist die Matrix von F bezüglich B und B' sagt man 'A ist die Matrix von f bezüglich B'.

5.3.5 Satz 17': Spezialfall von Satz 17

Seien B, B' Basen von V, $n = \dim V$ und f eine lineare Abbildung $f\colon V \to V$. Sei A die Matrix von f bezüglich B. Sei A' die Matrix von f bezüglich B', dann ist $A' = S^{-1}AS$, wobei S die Übergangsmatrix von B nach B' ist. ■

5.3.6 Satz 17': Spezialfall von Satz 17

Seien $B = (b_1, \ldots, b_n)$ und $C = (c_1, \ldots, c_n)$ Basen von K^n und $f\colon K^n \to K^n$ linear. Sei $E = (e_1, \ldots, e_n)$ die Standardbasis (als Matrix Einheitsmatrix E). Dann ist C die Übergangsmatrix von E nach C. Entsprechend istB^{-1} die Übergangsmatrix von B nach E, also $B^{-1}C$ die Übergangsmatrix von B nach C.
Bild nicht verfügbar![width=5cm]SS1.png Abbildung 36
Bild nicht verfügbar![width=5cm]SS2.png Abbildung 37

$$\begin{array}{ccccc} C = i_C & \nearrow & V & \nwarrow & i_C = C \\ & K^n & \xrightarrow[C]{} & K^n & \end{array}$$

C ist die Übergangsmatrix von E nach C.

$$\begin{array}{ccccc} C = i_C & \nearrow & V & \nwarrow & i_B = B \\ & K^n & \xrightarrow[B^{-1}C]{} & K^n & \end{array}$$

■

Beispiel:
f Spiegelung an der Geraden $R\begin{pmatrix}1\\1\end{pmatrix}$ in R^2.
$f(e_1) = e_2, f(B_1) = b_1, f(e_2) = e_1, f(b_2) = -b_2$
Bild nicht verfügbar![width=5cm]SS3.png Abbildung 38
Also ist bezüglich der Standardbasis die Matrix von $f\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$. Also ist die Matrix von f bezüglich Basis $B = (b_1, b_2) = (\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}-1\\1\end{pmatrix})$ ist $\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$. $B^{-1} = \begin{pmatrix}0,5 & 0,5\\-0,5 & 0,5\end{pmatrix}$, denn $\begin{pmatrix}1 & -1\\1 & 1\end{pmatrix} \cdot \begin{pmatrix}0,5 & 0,5\\-0,5 & 0,5\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$.
$BAB^{-1} = \begin{pmatrix}1 & -1\\1 & 1\end{pmatrix} \cdot \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} \cdot \begin{pmatrix}0,5 & 0,5\\-0,5 & 0,5\end{pmatrix} = \begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \cdot \begin{pmatrix}0,5 & 0,5\\-0,5 & 0,5\end{pmatrix} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$
Bild nicht verfügbar![width=7cm]SS4.png Abbildung 39

6 Lineare Gleichungssysteme

Sei K ein Körper. Wir betrachten das lineare Gleichungssystem * (LGS)

$$\begin{array}{llll} a_{11}x_1 & +a_{12}x_2 & +\ldots+ & a_{1n}x_n & = b_1 \\ a_{21}x_1 & +a_{22}x_2 & +\ldots+ & a_{2n}x_n & = b_2 \\ a_{m1}x_1 & +a_{m2}x_2 & +\ldots+ & a_{mn}x_n & = b_m \end{array} \tag{4.1}$$

* von m Gleichungen mit n unbekannten $x_1, \ldots, x_n$, wobei $a_{ij} \in K$ (für $i = 1, \ldots, m, j = 1, \ldots, n$) und $b_1, \ldots, b_m \in K$ gegeben sind und alle n-Tupel $\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \in K^n$ gesucht sind, die das Gleichungssystem lösen.

In Matrizenschreibweise:

$$Ax = b \tag{4.2}$$

Gegeben:
$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in K^{m,n}, b \in K^m$

Gesucht:
Alle $x \in K^n$ mit $Ax = b$. Jedes $x \in K^n$ mit $Ax = b$ heißt eine Lösung des LGS (4.1) bzw. (4.2). Gesucht $\{x \in K^n | Ax = b\}$, d. h. gesucht ist das vollständige Urbild des Vektors $b \in K^m$ unter der linearen Abbildung $A\colon K^n \to K^n$.

6.1 Satz 18: Lösungsmenge bei LGS I

Das LGS $Ax = b$ von m Gleichungen und n Unbekannten (d. h. $A \in K^{m,n}$) hat für jedes $b \in K^m$:

a)	höchstens eine Lösung	$\Leftrightarrow$	Rang $A = n$	A injektiv
b)	mindestens eine Lösung	$\Leftrightarrow$	Rang $A = m$	A surjektiv
c)	genau eine Lösung	$\Leftrightarrow$	Rang $A = n = m$	A bijektiv

$Ax = b$ hat eine Lösung $\Leftrightarrow b \in BildA = \text{Lin}\{a_1, \ldots, a_n\}$ wobei $A = (a_1, \ldots, a_n)$. Es gilt $b \in \text{Lin}\{a_1, \ldots, a_n\} \Leftrightarrow \text{Lin}\{a_1, \ldots, a_n\} = \text{Lin}\{a_1, \ldots, a_n, b\}$. ■

6.2 Definition: erweiterte Matrix

Bezeichne (A, b) die erweiterte Matrix $(A, b) = (a_1, \ldots, a_n, b)$. Es gilt $\text{Lin}\{a_1, \ldots, a_n\} = \text{Lin}\{a_1, \ldots, a_n, b\} \Leftrightarrow \text{Rang } A = \dim\{a_1, \ldots, a_n\} = \dim\{a_1, \ldots, a_n, b\} = \text{Rang}(A, b)$. Es folgt Satz 19.

6.3 Satz 19: Lösungsmenge bei LGS II

Das lineare Gleichungssystem $Ax = b$ von m Gleichungen und n Unbekannten hat

a) mindestens eine Lösung $\Leftrightarrow$ $\operatorname{Rang} A = \operatorname{Rang}(A, b)$
b) genau eine Lösung $\Leftrightarrow$ $\operatorname{Rang} A = \operatorname{Rang}(A, b) = n$
c) keine Lösung $\Leftrightarrow$ $\operatorname{Rang} A \neq \operatorname{Rang}(A, b)$

■

6.4 Struktur der Lösungsmenge

6.4.1 Definition: homogen und inhomogen

Das LGS $Ax = b$ heißt **homogen**, wenn $b = 0$ und **inhomogen**, wenn $b \neq 0$ Wenn das LGS $Ax = b$ gegeben ist, dann heißt $Ax = 0$ das zugehörige homogene LGS. Die Lösungsmenge des homogenen LGS $Ax = 0$ ist $\{x \in K^n | x \in K^m | Ax = 0\} = \ker A$, also ein linearer Unterraum.

6.4.2 Feststellung 48: Lösung eines LGS

Sei $u \in K^n$ eine Lösung des LGS $Ax = b$ (also $Au = b$). Dann gilt: $v \in K^n$ ist genau dann eine Lösung des LGS $Ax = b$, wenn $v - u \in \ker A$, d. h. wenn $v - u$ eine Lösung des zugehörigen homogenen LGS $Ax = 0$ ist.

Beweis:
$\Rightarrow$
u und v seien Lösungen des LGS $Ax = b$ also $Au = b$, $Av = b$ also $A(v - u) = Av - Au = b - b = 0$

$\Leftarrow$
Aus $Au = b$ und $A(v - u) = 0$ folgt $Av = A(u + (v - u)) = Au + A(u - u) = b + 0 = b$ ■

Aus Feststellung 48 und Satz 19 folgt Satz 20.

6.4.3 Satz 20: Struktur der Lösungsmenge eines LGS

Die Lösungsmenge des LGS $Ax = b$ ist

a) ϕ , falls $\operatorname{Rang} A \neq \operatorname{Rang}(A, b)$
b) $\{u\} + \ker A := \{u + w | w \in \ker A\}$, wobei n eine beliebige Lösung des LGS $Ax = b$ ist und falls $\operatorname{Rang} A = \operatorname{Rang}(A, b)$

■

Die allgemeine Lösung (Menge aller Lösungen) des inhomogenen LGS $Ax = b$ ist die Summe aus einer speziellen Lösung u des inhomogenen LGS $Ax = b$ und der allgemeinen Lösung des zugehörigen homogenen LGS $Ax = b$, falls das inhomogene LGS überhaupt lösbar ist.

6.4.4 Definition: affiner Unterraum

Eine Teilmenge $M \subseteq V$ heißt ein **affiner Unterraum** von V, falls $M = \phi$ oder es ein $v \in M$ gibt, sodass $U := M \neq \{-v\}$ ein linearer Unterraum von V ist, also $M = \{v\} + U$.

$$\dim M := \begin{cases} -1 & \text{, falls } M = \phi \\ \dim U & \text{, falls } M = \{v\} + U \end{cases}$$

Die Dimension ist sinnvoll, da U unabhängig von der Wahl von $v \in M$ ist (nachrechnen). U heißt der zu M gehörige lineare Unterraum.

Beispiel:
Die nulldimensionalen affinen Unterräume sind die eindimensionalen Teilmengen von V (Punkte).

6.4.5 Satz 20'

a) Die Lösungsmenge eines LGS ist ein affiner Unterraum.
b) Falls es eine Lösung des LGS $Ax = b$ gibt, dann ist die Dimension des Lösungsraums $n - \operatorname{Rang} A$ (wobei $A \in K^{m,n}$, d. h. $n =$ Zahl der Unbekannten).

Beweis:
a) Unformulierung von Satz 20.
b) Nach Satz 20 ist der zugehörige lineare Unterraum $\ker A$. Nach Dimensionssatz für lineare Abbildungen ist
$\operatorname{Rang} A + \dim \ker A = n$ ($A\colon K^n \to K^n$) also $\ker A = n - \operatorname{Rang} A$.■

6.5 Der Gauss-Algorithmus zur Lösung von LGS

Zur Lösung von homogenen LGS $Ax = 0$ betrachte Matrix A. Zur Lösung von inhomogenen LGS $Ax = b$ betrachte die erweiterte Matrix (A, b).

6.5.1 Umformung des LGS

Typ 1 Addition eines Vielfachen einer Gleichung zu einer anderen Gleichung.
$p_{ij}^{(\lambda)}$: Addiere zur j-ten Gleichung das λ-fache der i-ten Gleichung.
Typ 2 Vertauschen von zwei Gleichungen
p_{ij}: Vertausche die i-te Gleichung mit der j-ten Gleichung
Typ 3 Multiplikation einer Gleichung mit dem Faktor $\lambda \in K \setminus \{0\}$.
$r_i^{(\lambda)}$: Multipliziere die i-te Gleichung mit λ.

Nach einer Umformung vom Typ 1 ist offenbar jede Lösung des gegebenen LGS auch eine Lösung des neuen LGS und umgekehrt, denn die Umformung $p_{ij}^{(\lambda)}$ und damit $p_{ij}^{(-\lambda)}$ wieder rückgangig gemacht. Die Umformungen ändern die Lösungsmenge des LGS nicht.

$c_{ij} \neq 0$. Ziehe von der r-ten Gleichung (Zeile) $r \neq i$ das $\frac{c_{rj}}{c_{ij}}$-fache der i-ten Zeile ab. Also $\widetilde{c}_{rs} = c_{rs} - \frac{c_{rj}}{c_{ij}} c_{is}$ für $r \neq i$. $\widetilde{d}_r = d_r - \frac{c_{rj}}{c_{ij}} d_i$. Insbesondere $\widetilde{c}_{rj} = c_{rj} - \frac{c_{rj}}{c_{ij}} c_{ij} = 0$.

Starte mit der **erweiterten Matrix** (A, b). Das Verfahren bricht ab, wenn in jeder Zeile, die nicht aus lauter Nullen besteht (auf der linken Seite), gibt es mindestens einen Eintrag $\neq 0$, so dass

in der entsprechenden Spalte alle übrigen Glieder 0 sind. Die rechte Spalte zählt dafür nicht mit. c_{ij} heißt das Pivot-Element des Austauschschritts. Diese Form ist durch Umformung vom Typ 1 stehts erreichbar.

6.5.2 Beispiel des Verfahrens

										x_1	x_2	x_3	x_4	rechte Seite
(1)			x_2	+	x_3	+	x_4	=	1	0	1	1	1	1
(2)	x_1	+	$2x_2$	+	$3x_3$	+	$7x_4$	=	1	1	2	3	7	1
(3)	$2x_1$	+	$3x_2$	+	x_3			=	0	2	3	1	0	0
(4)	$-x_1$	+	$5x_2$			+	$2x_4$	=	0	-1	5	0	2	0
(1')			x_2	+	x_3	+	x_4	=	1	0	1	1	1	1
(3')		−	x_2	−	$5x_3$	−	$14x_4$	=	-2	0	-1	-15	-14	-2
(4')			$7x_2$	+	$3x_3$	+	$9x_4$	=	1	0	7	3	9	1
(3")				−	$4x_3$	−	$13x_4$	=	-1	0	0	-4	-13	-1
(4")				−	$4x_3$	+	$2x_4$	=	-6	0	0	-4	2	-6
(4"')							$15x_4$	=	-5	0	0	0	15	-5

(4"') $\Rightarrow x_4 = -\frac{5}{15} = -\frac{1}{3}$, einsetzen in (3") $\Rightarrow -4x_3 + \frac{13}{3} = -1 \Rightarrow -4x_3 = -\frac{16}{3} \Rightarrow x_3 = \frac{4}{3}$, einsetzen in (1') $\Rightarrow x_2 + \frac{4}{3} - \frac{1}{3} = 1 \Rightarrow x_2 = 0$, einsetzen in (2) $\Rightarrow x_1 + 2 \cdot 0 + 3\frac{4}{3} - 7\frac{1}{3} = 1 \Rightarrow x_1 = 1 - 4 + \frac{7}{3} \Rightarrow x_1 = -\frac{2}{3}$.

6.5.3 Nachtlösbarkeit eines LGS

Wenn bei der Umformung des LGS eine Gleichung der Form $0 = \widetilde{b}_i$ entsteht und $\widetilde{b}_i \neq 0$, dann nicht lösbar.

6.5.4 weiteres Beispiel

Nach den Zeilenumformen von Typ 1 sei die erweiterte Matrix:

(1)	0	1	2	4	2
(2)	1	2	0	1	2
(3)	1	1	1	1	1
(4)	0	0	0	0	0

Lösung durch suksesives Einsetzen. Gleichung $0 = 0$ weglassen. Frei wählbare Variablen x_2, x_5.

(1) $2x_3 + 4x_5 = 2 \Rightarrow x_3 = 1 - 2x_5$, (3) einsetzen $\Rightarrow x_1 + x_2 + (1 - 2x_5) + x_5 = 1 \Rightarrow x_1 = -x_2 + x_5$
(2) einsetzen $\Rightarrow (-x_2 + x_5) + 2x_2 + 2x_4 + x_5 = 2 \Rightarrow x_2 + 2x_4 + 2x_5 = 2 \Rightarrow x_4 = 1 - 0,5x_2 - x_5$

Lösungsmenge

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_5 \end{pmatrix} \;\middle|\; x_1 = -x_2 + x_5, x_3 = 1 - 2x_5, x_4 = 1 - 0,5x_2 - x_5 \right\} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} + R \begin{pmatrix} -1 \\ 1 \\ 0 \\ -0,5 \\ 0 \end{pmatrix} + R \begin{pmatrix} 1 \\ 0 \\ -2 \\ -1 \\ 1 \end{pmatrix}$$

Was bewirken die Zeilenumformungen der Matrix:

Typ 1:

$$q_{ij}^{(\lambda)} \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{i1} & \cdots & a_{in} \\ a_{j1} & \cdots & a_{jn} \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{i1} & \cdots & a_{in} \\ a_{j1} + \lambda a_{i1} & \cdots & a_{jn} + \lambda a_{in} \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

Dies ist gerade die Multiplikation der Matrix von links mit $Q_{ij}^{(\lambda)} = \begin{pmatrix} 1 & \cdots & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ 0 & \cdots & \cdots & 1 \end{pmatrix}$. $Q_{ij}^{(\lambda)} \in K^{m,n}, a_{ij} = \lambda, a_{kk} = 1, a_{kk} = 0$ sonst.$A \mapsto Q_{ij}^{(\lambda)} \cdot A$

Beispiel:
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lambda & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ \lambda a_{11} + a_{31} & \lambda a_{12} + a_{32} & \lambda a_{13} + a_{33} \end{pmatrix} = Q_{13}^{(\lambda)}$$
Typ 2:
Vertausche i-te Zeile mit j-ter Zeile ($i \neq j$). Multiplikation von A von links mit
$$p_{ij} := \begin{pmatrix} 1 & \cdots & \cdots & \cdots & \cdots \\ \cdots & 0 & \cdots & 1 & \cdots \\ \cdots & \cdots & 1 & \cdots & \cdots \\ \cdots & 1 & \cdots & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix} \in K^{m,n}$$
$(Q_{ij}^{(\lambda)})^{-1} = Q_{ij}^{(-\lambda)}$ zu Typ 1
$p_{ij}^{-1} = p_{ij}$ zu Typ 2

Typ 3:
Multiplikation der i-ten Zeile mit $\lambda \neq 0$.

6.5.5 Inversion von $(n \times n)$-Matrizen

Ziel: Durch elementare Zeilenumformung aus A die Einheitsmatrix machen, d. h. $TA|TE$, $TE = E \Rightarrow T = A^{-1}$.

Beispiel

A				E			
1	2	2	1	1	0	0	0
1	0	2	0	0	1	0	0
3	2	0	1	0	0	1	0
1	1	0	0	0	0	0	1
1	0	2	1	1	0	0	-1
1	0	2	0	0	1	0	0
1	0	0	1	0	0	1	-2
1	1	0	0	0	0	0	1
1	0	2	0	1	0	-1	1
1	0	2	0	0	1	0	0
1	0	0	1	0	0	1	-2
1	1	0	0	0	0	0	1
0	0	2	0	1	0	-1	1
1	0	0	0	-1	1	1	-1
1	0	0	1	-1	1	1	-1
1	1	0	0	0	0	0	1
0	0	2	0	1	0	-1	1
1	0	0	0	-1	1	1	-1
0	0	0	1	1	-1	-1	1
0	1	0	0	1	-1	-1	2

Mit Typ 2 und Typ 3 Zeilenumformung (vertauschen der Reihenfolge von Zeilen und Multiplikation von Zeilen mit $\lambda \in K \setminus \{0\}$ ergibt sich:

1	0	0	0	-1	1	1	-1
0	1	0	0	1	-1	-1	2
0	0	1	0	0,5	0	$-0,5$	0,5
0	0	0	1	1	-1	-1	1

E				A^{-1}			

$$A^{-1} = \begin{pmatrix} -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 2 \\ 0,5 & 0 & -0,5 & 0,5 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Falls bei den Umformungen auf der linken Seite eine Zeile 0 entsteht, dann ist A nicht invertierbar.

6.5.6 Die transponierte Matrix

$\begin{pmatrix} a_{11} & \cdots & a_{m1} \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}^T = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ Also $A \in K^{m,n} \Leftrightarrow A \in K^{n,m}$.

Beispiel

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

6.5.7 Feststellung 49: Rechenregeln

a) $(A_1 + A_2)^T = A_1^T + A_2^T$
b) $\lambda A)^T = \lambda A^T$
c) $(A^T)^T = A$
d) $(AB)^T = B^T A^T$
e) Falls $A \in K^{m,n}$ invertierbar, dann ist $(AT)^{-1} = (A^{-1})^T$

Beweis:
a), b), c) unmittelbar klar.

zu d)

$$(\begin{pmatrix} \widetilde{a_1} \\ \cdots \\ \widetilde{a_m} \end{pmatrix} \begin{pmatrix} b_1 & \cdots & b_l \end{pmatrix})^T = \begin{pmatrix} \widetilde{a_1} b_1 & \cdots & \widetilde{a_1} b_l \\ \cdots & & \\ \widetilde{a_m} b_1 & \cdots & \widetilde{a_m} b_l \end{pmatrix}^T =$$

$$\begin{pmatrix} b_1^T \widetilde{a_1}^T & \cdots & b_l^T \widetilde{a_1}^T \\ \cdots & & \\ b_1^T \widetilde{a_m}^T & \cdots & b_l^T \widetilde{a_m}^T \end{pmatrix} = \begin{pmatrix} b_1^T \\ \cdots \\ b_l^T \end{pmatrix} \begin{pmatrix} \widetilde{a_1}^T & \cdots & \widetilde{a_m}^T \end{pmatrix}$$

zu e)
$B = A^{-1} \Leftrightarrow AB = E = BA \Rightarrow B^T A^T = E^T = E = A^T B^T$ also $B^T = (A^T)^{-1}$.■

Bemerkung:
Mit a) bis c) folgt $A \mapsto A^T$ ist ein Isomorphismus zwischen den K-Vektorräumen $K^{m,n}$ und $K^{n,m}$.

Wir können auch entsprechend Spaltenumformungen definieren (nicht geeignet für LGS). Sei $A \in K^{m,n}$.

Typ 1' Addiere das λ-fache der i-ten Spalte zur j-ten Spalte.
Also Matrix $A = (Q_{ij}^{(\lambda)} A^T)^T = A(Q_{ij}^{(\lambda)}))^T = AQ_{ji}^{(\lambda)}$.

Typ 2' Vertausche die i-te Spalte mit der j-ten Spalte.
$A' = (P_{ij} A^T)^T = AP_{ij}^T = AP_{ij}$. (Bemerkung: $P_{ij}^T = P_{ij} = P_{ji}^T = P_{ji}$) $A \mapsto AP_{ji}$.

Typ 3' Multipliziere die i-te Spalte mit λ.
$(R_i^{(\lambda)})^T = R_i^{(\lambda)}$ $A \mapsto AR_i^{(\lambda)}$.

6.5.8 Feststellung 50

Der Rang einer Matrix A ändert sich nicht bei Zeilen- oder Spaltenumformung der Typen 1, 2, 3 bzw. 1', 2', 3'.

Beweis:
Sei $A \in K^{m,n}$ mit $\operatorname{Rang} A = \dim(BildA)$, $BildA := \{Ax | x \in K^n\}$. Die betrachteten Zeilen- bzw. Spaltenumformungen sind Multiplikationen mit invertierten Matrizen von links bzw. rechts. Andererseits gilt $\operatorname{Rang} A = \operatorname{Rang} BA = \operatorname{Rang} AC$ wenn $B \in K^{m,n}$ bzw. $C \in K^{n,n}$ invertierbar sind, dann invertierbare Matrizen entsprechend Isomorphismen. Diese bewahren die Dimension von Unterräumen. Zur Rangbestimmung einer Matrize kann man also Zeilen- und Spaltenumformungen (vom Typ 1,2,3,1',2',3') verwenden um eine Matrix zu erhalten, deren Rang man direkt ablesen kann.
■

6.5.9 Satz 21

Sei $A \in K^{m,n}, r = \operatorname{Rang} A$. Dann gibt es invertierbare Matrizen $B \in K^{m,n}, C \in K^{n,n}$ sodass $BAC = \begin{pmatrix} 1 & \cdots & 0 & 0 & \\ \cdots & 1 & \cdots & \cdots & \\ 0 & \cdots & 1 & \cdots & \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$

Beweis:
Wir können folgende Gestalt erreichen. Mit Typ 1: In jeder Zeile $\neq 0$ gibt es einen Koeffizienten $\neq 0$, sodass in der entsprechenden Spalte sonst nur 0-en stehen, danach mit Typ 3: Diese Koeffizienten $\neq 0$ können als 1 gewählt werden, danach mit Vertauschen von Zeilen (Typ 2) und mit Vertauschen von Spalten (Typ 2') die Gestalt $\begin{pmatrix} E_r & A' \\ 0 & 0 \end{pmatrix}$, schliesslich mit Typ 1' die Gestalt $\begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots \\ 0 & \cdots & 1 & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$. Der Rang der Matrix $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$ ist r, also gleich dem Rang von A (da die Zeilen- und Spaltenumformungen den Rang nicht verändern. ■

Folgerung:
Für eine linerae Abbildung $f\colon V \to W$ mit $\dim V = n, \dim W = m, \dim(f(V)) = r$ (Rang) gibt es geordnete Basen von V bzw. W (im allgemeinen verschiedene Basen), sodass f bezüglich dieser Basen die Matrix $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \in K^{m,n}$ hat.

6.5.10 Satz 21

Für jede matrix A gilt $\operatorname{Rang} A = \operatorname{Rang} A^T$

Beweis:
Nach Satz 21 gibt es invertierbare Matrizen B, C mit $BAC = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$.
Also $\operatorname{Rang} A = \operatorname{Rang}(BAC) = r = \operatorname{Rang} \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = \operatorname{Rang}(BAC)^T = \operatorname{Rang}(C^T A^T B^T) = \operatorname{Rang} A^T$, da B^T, C^T nach Feststellung 49 e) invertierbar sind. ■

6.5.11 Definition: regulär und singulär

Invertierbare Matrizen nennt man auch regulär. Nichtinvertierbare quadratische Matrizen nennt man singulär.

6.5.12 Definition: lineare Gruppe

Sei V ein K-Vektorraum. Dann bezeichne $GL(V) := \{f\colon V \to V | f \text{ linear und bijektiv}\}$ = Menge der Automorphismen von V. $GL(V)$ ist mit $\circ$ (Komposition von Abbildungen) eine Gruppe. Sie heißt die (allgemeine) lineare Gruppe von V (general linear group). Statt $GL(K^n)$ schreibt man auch $GL(n, K)$. Offenbar gilt $(GL(n, K) \cong \{A \in K^{n,n} | A \text{ invertierbar}\}$ mit Matrixmultiplikation wegen der natürlichen Bijektion zwischen linearen Abbildungen $K^n \Rightarrow K^n$ und $(n \times n)$-Matrizen.

6.5.13 Definition: obere Dreiecksmatrix

Eine obere Dreiecksmatrix ist eine matrix der Form $A \in K^{n,n}$ mit $a_{ij} = 0$ für $i > j$, also $A = \begin{pmatrix} a_{11} & a_{1n} \\ 0 & a_{nn} \end{pmatrix}$.

6.5.14 Definition: untere Dreiecksmatrix

Eine untere Dreiecksmatrix ist eine Matrix der Form $A \in K^{n,n}$ mit $a_{ij} = 0$ für $i < j$, also $A = \begin{pmatrix} a_{11} & 0 \\ a_{n1} & a_{nn} \end{pmatrix}$.

6.5.15 Definition: Diagonalmatrix

Eine Diagonalmatrix ist eine Matrix der Form $A \in K^{n,n}$ mit $a_{ij} = 0$ für $i \neq j$, also $A = \begin{pmatrix} a_{11} & 0 \\ 0 & a_{nn} \end{pmatrix}$.

6.5.16 Bezeichnungen

Eine Untergruppe von $GL(n, K)$: Bezeichne

$\Delta_n^O := \{A \in GL(n, K) | A \text{ ist obere Dreicksmatrix}\}$
$\Delta_n^U := \{A \in GL(n, K) | A \text{ ist untere Dreicksmatrix}\}$
$D_n := \{A \in GL(n, K) | A \text{ ist Diagonalmatrix}\}$
$\widetilde{\Delta}_n^O := \{A \in \Delta_n^O | a_{ii} = 1 \text{ für } i = 1, \ldots, n\}$
$\widetilde{\Delta}_n^U := \{A \in \Delta_n^U | a_{ii} = 1 \text{ für } i = 1, \ldots, n\}$

6.5.17 Feststellung 51

Falls A eine obere oder eine untere Dreiecksmatrix ist, dann gilt $A \in GL(n,K) \Leftrightarrow \prod_{i=1}^{n} a_{ii} \neq 0$.

Beweis:
Nachrechnen

Als Hasse-Diagramm:
Bild nicht verfügbar![width=4cm]MHD.png
Abbildung 40: Veranschaulichung als Hassediagramm
■

6.5.18 Feststellung 52

a) $\Delta_n^O, \Delta_n^U, D_n, \widetilde{\Delta}_n^O, \widetilde{\Delta}_n^U$ sind Untergruppen von $GL(n,K)$.
b) $\widetilde{\Delta}_n^O = \langle \{Q_{ij}^{(\lambda)} | 1 \leq j < i \leq n, \lambda \in K\} \rangle$
$\widetilde{\Delta}_n^U = \langle \{Q_{ij}^{(\lambda)} | 1 \leq j < i \leq n, \lambda \in K\} \rangle$
$D_n = \langle \{R_i^{(\lambda)} | 1 \leq i \leq n, \lambda \in K \setminus \{0\}\} \rangle$
$\Delta_n^O = \langle \widetilde{\Delta}_n^O \cup D_n \rangle$
$\Delta_n^U = \langle \widetilde{\Delta}_n^U \cup D_n \rangle$
$\langle \cdot \rangle$ = erzeugte Untergruppe

Beweis:
Nachrechnen. ■

6.6 Permutationsmatrizen

Eine Permutationsmatrize ist eine Matrize $P \in K^{n,n}$ bei der in jeder Zeile und jeder Spalte genau ein Koeffizient 1 steht und alle anderen 0 sind. Es gibt also eine Permutation $\sigma \in S_n$ ($S_n :=$ symetrische Gruppe der Permutationen von $\{1,\ldots,n\}$, sodass $P = P_\sigma := (e_{\sigma(1)}, e_{\sigma(2)}, \ldots, e_{\sigma(n)})$. e_j ist der j-te Standardbasisvektor. Also $P_\sigma \; e_i = e_{\sigma(i)}$.

Folglich gilt: $P_{\tau\sigma} e_i = e_{\tau\sigma(i)} = P_\tau e_{\sigma(i)} = P_\tau P_\sigma e_i$ für $i = 1,\ldots,n$, also $P_{\tau\sigma} = P_\tau P_\sigma$.

Offenbar gilt $P_\sigma = E_n \Leftrightarrow \sigma = id$. Die Abbildung $\sigma \mapsto P_\sigma$ ist also eine Abbildung $S_n \to GL(n,K)$ und ist ein injektiver Gruppenhomomorphismus von S_n in $GL(n,K)$.

6.6.1 Satz 22

Jede invertierbare Matrix $A \in K^{n,n}$ lässt sich in der Form $A = BPC$ schreiben, wobei $B \in \Delta_n^U$, $C \in \Delta_n^O$ und P eine Permutationsmatrix ist.

Beweis:
Nachrechnen. ■

6.6.2 Feststellung 53

a) Jede reguläre Matrix ist das Produkt von Elementarmatrizen.
b) Jede reguläre $n \times n$-Matrix ist sogar von der Form $BR_n^{(d)}$, wobei B das Produkt von Elementarmatrizen vom Typ 1 is und $d \in K \setminus \{0\}$.

Beweis:
a)
Gaussalgorithmus (vgl. auch Beweis Feststellung 48).

b)
Frage: Ist d durch A eindeutig bestimmt?
■

Geometrisch (im Fall $K = R$) Typ 1 Elementarmatrizen. $Q_{ij}^{(\lambda)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & \lambda_{ij} & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

$Q_{ij}^{(\lambda)}$ ist eine Scherung.

Bild nicht verfügbar![width=6cm]Scherung.png Abbildung 41: Scherung

Die Scherung ändert das Volument nicht (bei jedem vernünftigen Volumenbegriff).

7 Detarminanten

Sei K ein Körper und $A \in K^{n,n}$.

7.1 Detarminantenfunktion

Eine Abbildung $d\colon K^{n,n} \to K$ heißt eine Determinantenfunktion, wenn sie folgende Eigenschaften hat:

(i) sie ist multilinear, d. h. linear in jeder Spalte. Dies ist definiert als: Für jedes $1 \leq i \leq n$ gilt: $d(a_1, \ldots, a_{i-1}, \lambda a_i + \mu b_i, a_{i+1}, \ldots, a_n) = \lambda d(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n + \mu d(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n)$, d. h. für jedes $1 \leq i \leq n$ und feste aber beliebige $a_j \in K^n (j \neq 1)$ ist die Abbildung $a \mapsto d(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n)$ eine lineare Abbildung von K^n nach K.

(ii) $d(a_1, \ldots, a_i, \ldots, a_i, \ldots, a_n) = 0$, d. h. wenn zwei Spaltenvektoren übereinstimmen, dann ist $d(A) = 0$.

(iii) $d(E_n) = 1$

7.2 Feststellung 54

Sei $d\colon K^{n,n} \to K$ eine Detarminantenfunktion. Für alle $\lambda \in K, A = (a_1, \ldots, a_n) \in K^{n,n}$ gilt:

1) $d(a_1, \ldots, a_{i-1}, a_i + \lambda a_j, \ldots, a_n) = d(a_1, \ldots, a_{i-1}, a_i, \ldots, a_n)$ für $i \neq j$, d. h. $d(A) = d(AQ_{ji}^{(\lambda)}$, d. h. $d(A)$ ändert sich nicht, wenn man ein Vielfaches einer Spalte zu einer anderen addiert (Typ 1'), also wegen (iii) folgt $d(Q_{ji}^{(\lambda)}) = 1$.
2) $d(a) = -d(AP_{ij})$ $(i \neq j)$, d. h. $d(A)$ wird mit -1 multipliziert, wenn man zwei Spalten vertauscht.
3) $d(AR_i^{(\lambda)}) = \lambda d(A)$, insbesondere (mit (iii)) $d(R_i^{(\lambda)} = \lambda$.

Beweis:
1)
$d(a_1, \ldots, a_{i-1}, a_i + \lambda a_j, a_{i+1}, \ldots a_n) = d(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots a_n) + \lambda d(a_1, \ldots, a_{i-1}, a_j, a_{i+1}, \ldots a_n) = d(a_1, \ldots, a_n)$

2)
$0 = d(a_1, \ldots, a_i + a_j, \ldots, a_i + a_j, \ldots a_n) = d(a_1, \ldots, a_i, \ldots, a_i, \ldots a_n) + d(a_1, \ldots, a_j, \ldots, a_j, \ldots a_n) + d(a_1, \ldots, a_j, \ldots, a_i, \ldots a_n) + d(a_1, \ldots, a_i, \ldots, a_j, \ldots a_n) = d(a_1, \ldots, a_j, \ldots, a_i, \ldots a_n) + d(a_1, \ldots, a_i, \ldots, a_j, \ldots a_n)$ also $d(a_1, \ldots, a_i, \ldots, a_j, \ldots a_n) = -d(a_1, \ldots, a_j, \ldots, a_i, \ldots a_n)$

3)
$d(a_1, \ldots, a_{i-1}, \lambda a_i, a_{i+1}, \ldots a_n) = \lambda d(a_1, \ldots, a_n)$■

7.3 Feststellung 55: Eindeutigkeit

Es gibt höchstens eine Detarminantenfunktion $d\colon K^{n,n} \to K$ und $d(A) = 0$, falls A singulär (nicht invertierbar) ist.

Beweis:
Falls A regulär ist, dann lässt sich A als Produkt von Elementarmatrizen schreiben, also wegen Feststellung 54 und (iii) eindeutig bestimmt. Bemerkung: In Feststellung 53 gilt dann $d(A) = d$. Falls A nicht regulär ist, dann lässt sich A schreiben als $A = CE_rB$ mit $E_r = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ mit $r = \operatorname{Rang} A < n$ und B, C reguläre Matrizen.
$d(C, E_r, B) = 0$, dann nach elementarer Spaltenumformung erhählt man aus A die Matrix der Form CE_r. Diese enthählt $n - r > 0$ Spalten mit 0-Vektor, also $d(CE_r) = 0$ (wegen (i)). ■

8 Glossar der Definitionen

Die Bedeutung der verwendeten Symbole ergibt sich aus dem Kontext. Aus Gründen der Übersichtlichkeit wird auf deren Definition verzichtet. Alle Definitionen sind im Skript erläutert und umfassend dargestellt.

Mathematisches Objekt	Definition
Echte Teilmenge	$A \subset B := A \subseteq B \wedge A \neq B$
Potenzmenge	$\mathcal{P}(A) = \{B \colon B \subseteq A\}$
Durchschnittsmenge	$\cap M = \{x / \quad \forall A \in M \colon x \in A)$
Vereinigungsmenge	$\cup M = \{x / \quad \exists A \in M \colon x \in A\}$
kartesisches Produkt	$A \times B \colon \{(a,b) / a \in A, b \in B\}$
Relation	$R \subseteq A \times B$
Umkehrrelation	$R^{-1} = \{(b,a) \in B \times A, (a,b) \in R, (b,c) \in R\}$
Verknüpfung von Relationen (Komposition)	$S \circ R := \{(a,b) \in A \times C, \quad \exists b \in B \colon (a,b) \in R, (b,c) \in S\}$
Identische Abbildung	$\triangle_M = \{(x,x) \vert x \in M\}$
Umkehrabbildung	$f^{-1}(b) = a \Leftrightarrow f(a) = b$
Äquivalenzrelation von a	$[a]_\sim := \{x \in M \vert x \sim a\}$
Menge der Äquivalenzklassen	$M / \sim := \{[a] \vert a \in M\}$
Äquivalenzrelation	$a_1 \sim_f a_2 \colon f(a_1) = f(a_2)$
Symetrische Gruppe	$\mathrm{S}(M) := \{f \colon M \to M \vert f \text{ bijektiv }\}$
Gruppenhomomorphismus	$f(x \circ y) = f(x) \bullet f(y)$
Kern von f	$\ker f := f^{-1}(\{e'\}) = \{a \in G \vert f(a) = e'\}$
Ringhomomorphismus	$f(a+b) = f(a) \ddot{+} f(b)$ und $f(a \cdot b) = f(a) \ddot{\cdot} f(b)$
Faktorring	$R/_I = \{a + I \vert a \in R\}.\ (R/_I, +)$
Vektorraum	$V = K^n = \underbrace{K \times K \times \ldots K}_{n\text{-mal}}$
Linearkombination	$v = \lambda_1 u_1 + \ldots + \lambda_m u_m = \sum_{i=1}^{n} \lambda_1 u_1$
K^I-Vektorraum	$K^I := \{f \colon I \to K \vert f \text{ Abbildungen}\}$
$K^{(I)}$	$K^{(I)} := \{f \in K^I \vert f(i) = 0 \vert \text{für alle bis auf endlich viele } i\}$
Rang von f	$\mathrm{Rang}(f) := \dim(f(v))$
Rang von $A \in K^{m,n}$	$\mathrm{Rang}(A) := \dim \mathrm{Lin}\{a_1, \ldots, a_n\}$
Menge aller Endomorphismen	$End(V) := \{f \colon V \to V \vert f \text{ lineare Abbildung}\}$

9 Gleichungsverzeichniss

Nummer	Gleichung
3.1	$f(b_j) = \sum_{i=1}^{m} a_{ij} c_i$
3.2	$f(\sum_{j=1}^{m} x_j b_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_j c_i$
3.3	$y_i = \sum_{j=1}^{n} a_{ij} x_j$
3.4	$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x1 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 & \dots & a_{1n}x_n \\ \dots & \dots & \dots \\ a_{m1}x_1 & \dots & a_{mn}x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{m} a_{1j}x_j \\ \sum_{j=1}^{n} a_{mj}x_j \end{pmatrix}$
3.5	$c_{ij} = \sum_{k=1}^{m} a_{ij} b_{ij}$
3.6	$b'_j = \sum_{i=1}^{h} s_{ij} b_i$
4.1	$\begin{array}{llll} a_{11}x_1 & +a_{12}x_2 & +\ldots+ & a_{1n}x_n = b_1 \\ a_{21}x_1 & +a_{22}x_2 & +\ldots+ & a_{2n}x_n = b_2 \\ a_{m1}x_1 & +a_{m2}x_2 & +\ldots+ & a_{mn}x_n = b_m \end{array}$
4.2	$Ax = b$

10 Hinweise

10.1 Allgemeine Information

Das Skript deckt den Stoff der Vorlesung ab, enthält aber wenig Beispiele, wie sie in den Übungen behandelt werden.

10.2 Symbolik des Skripts

Feststellungen und mathetamtische Beweise (Sätze) sind im Rahmen aufgeführt. Die wichtigsten Definitionen und Gleichungen sind graun unterlegt. Schlagwörter sind im Fettdruck dargestellt.

11 Quelle des Materials

Dieses Skript ist eine Vorlesungsmitschrift des Moduls **MATH-SEGY-LAAG**: Lineare Algebra. Die Vorlesung wurde von **Prof. Ulrich Brehm** gehalten. Es liegt dem handgeschriebenen Vorlesungsskript von Prof. Dr. Ulrich Brehm zu Grunde.

Telefon 0351-463-34168
E-Mail ulrich.brehm@tu-dresden.de

11.1 Weitere Quellen

- `http://www.youtube.com/watch?v=_WsozSzbUTc`): Die Potenzmenge - Teil 1
- `http://www.youtube.com/watch?v=Mw275rRDsxY&feature=relmfu`): Die Potenzmenge - Teil 2
- `http://tu-dresden.de/tulogosw.png`: Logo der Technischen Universität Dresden (TUD)

11.2 Verwendete Programme

- LaTeX
- Microsoft Photo Draw
- Microsoft Power Point

12 Überarbeitungen

Im Skriptupdate vom 1. November 2018wurden folgende Dinge überarbeitet und korrigiert:

- Mengen und Aussagenlogik
- Relationen und Abbildungen (soweit wie besprochen)
- Matrizen (soweit wie besprochen)
- Gleichungsdarstellung
- Farbunterlegungen

Innoffizielles Skript orientiert an die LAAG-Vorlesung von Professor Brehm

von Studenten für Studenten

SoSe 2015, laskei, Version 6

Inhaltsverzeichnis

5 Benutzte Sachverhalte aus LAAG 1

Satz 5.1. *Hier kommt der Satz 3.1' hier. Das hat mit Übergangsmatrizen bzw. Darstellung von linearen Abbildungen in verschiedenen Basen zu tun.*

Satz 5.2 (Dimensionssatz)**.** *Seien V, W K-Vektorräume,* $\dim V < \infty$ *und $f\colon V \to W$ eine lineare Abbildung. Dann gilt* $\dim V = \dim(\ker f) + \dim f(V)$.

F 5.3. *Sei $f\colon V \to W$ eine lineare Abbildung zwischen Vektorräumen. Dann ist f genau dann injektiv, wenn f invertierbar ist.*

Satz 5.4. *Sei $f: V \to W$ eine lineare Abbildung zwischen endlich-dimensionalen Vektorräumen. Dann ist f genau dann injektiv, wenn* $\det f \neq 0$*, wobei* det *definiert ist für die zu f zugehöige Matrix bezüglich irgendeiner Basis.*

Satz 5.5 (Entwicklungssatz für Determinanten)**.** *Denke dir hier den Entwicklungssatz für Determinanten.*

6 Eigenwerte und Eigenvektoren

Sei K ein Körper, V ein K-Vektorraum.

Definition 6.1. Zwei quadratische Matrizen A, A' heißen ähnlich oder konjugiert (zueinander), geschrieben: $A \approx A'$, wenn es eine invertierbare Matrix S gibt, mit $A' = S^{-1}AS$.

Folgender Satz beschreibt die Motivation dieser Definition aus dem Verhalten von Matrizen bei einem Basiswechsel:

Satz 6.2. *Für $A, A' \in K^{n,n}$ gilt $A \approx A'$ genau dann, wenn es 2 Basen B, B' von K^n gibt und einen Endomorphismus $f: K^n \to K^n$ gibt, sodass A die Matrix von f bezüglich B und A' die Matrix bezüglich B' ist.*

Beweis. „⇐“Nach 5.1 (Wähle für S die Übergangsmatrix von B nach B')
„ $\Longrightarrow$ “Wähle die Basis B beliebig und B' so, dass S die Übergangsmatrix wird. □

Satz 6.3. *$\approx$ ist eine Äquivalenzrelation auf $K^{n,n}$*

Beweis. **reflexiv** $A \approx A'$, denn $A = E_n^{-1} A E_n$

symmetrisch $A \approx A' \implies \exists S \in GL(n,K)$ mit $A' = S^{-1}AS$, also $A = SA'S^{-1} = (S^{-1})^{-1}A'S^{-1}$

transitiv $A \approx A' \wedge A' \approx A'' \implies \exists S, T \in GL(n,K) : A' = S^{-1}AS \wedge A'' = T^{-1}A'T \implies A'' = T^{-1}S^{-1}AST = (ST)^{-1}AST$

□

Sei im weiteren $f \in \mathrm{End}(V)$, d.h. $f: V \to V$ ist eine lineare Abbildung und $A \in K^{n,n}$ die zugehörige Matrix (bezüglich Standardbasis).

Definition 6.4. $\lambda \in K$ heißt ein Eigenwert (EW) von f, falls es ein $x \in V$ gibt, mit $x \neq 0$ und $f(x) = \lambda x$.
$x \in V$ heißt ein Eigenvektor (EV) von f zum Eigenwert λ, falls $x \neq 0$ und $f(x) = \lambda x$.
Sei $\lambda \in K$ ein Eigenwert von f, dann heißt $V(\lambda, f) := \{x \in V | f(x) = \lambda x\}$ der Eigenraum (ER) von f zum Eigenwert λ.
$U \subseteq V$ heißt Eigenraum von f, falls es einen Eigenwert λ von f gibt mit $U = V(\lambda, f)$.

Definition 6.5. Sei $A \in K^{n,n}$. Wir fassen A als lineare Abbildung $A\colon K^n \to K^n$ bezüglich der Standardbasis von K^n auf und damit sind die Begriffe Eigenwert, Eigenvektor, Eigenraum auf quadratischen Matrizen erklärt, also:
$\lambda \in K$ heißt ein Eigenwert von A, falls es ein $x \in K^n$ gibt mit $x \neq 0, Ax = \lambda x$
$x \in K^n$ heißt ein Eigenvektor von A zum Eigenwert λ, falls $x \neq 0$ und $Ax = \lambda x$ gilt.

F 6.6. *Sei x ein Eigenvektor von f zum Eigenwert λ. Dann ist x kein Eigenvektor zum Eigenwert $\mu \neq \lambda$, d.h. der Eigenvektor bestimmt eindeutig seinen Eigenwert.*

Beweis. Aus $f(x) = \lambda x$ und $f(x) = \mu x$ folgt $\lambda x = \mu x \implies (\lambda - \mu)x = 0 \overset{x \neq 0}{\implies} \lambda = \mu$ □

F 6.7. *Folgende Aussagen sind äquivalent:*

(i) λ *ist Eigenwert von* f.

(ii) $ker(f - \lambda\,\mathrm{id}) \neq \{0\}$

(iii) $f - \lambda\,\mathrm{id}$ *ist nicht injektiv.*

Beweis.
- „(i) $\iff$ (ii)“: $f(x) = \lambda x \iff (f - \lambda\,\mathrm{id})x = 0 \iff x \in \ker(f - \lambda\,\mathrm{id})$. Die Behauptung folgt aus der Definition von Eigenwert: λ ist Eigenwert von $f \iff \exists x \in V : x \neq 0 \wedge f(x) = \lambda x$
- „(ii) $\iff$ (iii)“: Schon gezeigt (Für $g \in \mathrm{End}(V)$ gilt: $\ker g = \{0\} \iff g$ injektiv)

□

F 6.8. *Folgende Aussagen sind äquivalent:*

(i) x *ist Eigenwert von* f *zum Eigenwert* λ.

(ii) $x \in \ker(f - \lambda\,\mathrm{id}) \wedge x \neq 0$

Beweis. $f(x) = \lambda x \iff (f - \lambda\,\mathrm{id})x = 0 \iff x \in \ker(f - \lambda\,\mathrm{id})$ □

F 6.9. *Sei* $\dim V = n < \infty$*, dann gilt:* λ *ist genau dann ein Eigenwert von* f*, wenn* $\det(f - \lambda\,\mathrm{id}) = 0$ *ist.*

Beweis. Nach Folgerung 5.3 ist $f - \lambda\,\mathrm{id}$ genau dann injektiv, wenn $f - \lambda\,\mathrm{id}$ invertierbar ist. Nach Satz 5.4 (angewendet auf die zu $f - \lambda\,\mathrm{id}$ gehörige Matrix bezüglich irgendeiner Basis) ist $f - \lambda\,\mathrm{id}$ genau dann invertierbar, wenn $\det(f - \lambda\,\mathrm{id}) \neq 0$. □

F 6.10. *Sei* $A \in K^{n,n}$*, dann ist* λ *ein Eigenwert von* A *genau dann, wenn* $\det(A - \lambda E) = 0$

Beweis. $Ax = \lambda x \iff (A - \lambda E)x = 0$. Es gibt ein $x \neq 0$ mit $(A - \lambda E)x = 0 \iff \det(A - \lambda E) = 0$ □

F 6.11. *Sei* $\dim V = n < \infty$ *und* $U = V(\lambda, f)$*. Dann gilt:* $\dim U = n - \mathrm{Rang}(f - \lambda\,\mathrm{id})$

Beweis. $U = \ker(f - \lambda\,\mathrm{id})$. Nach dem Dimensionssatz für lineare Abbildungen (5.2) gilt: $\dim U = \dim\ker(f - \lambda\,\mathrm{id}) = \dim V - \dim(f - \lambda\,\mathrm{id}) = n - \mathrm{Rang}(f - \lambda\,\mathrm{id})$ □

F 6.12. *Der Eigenraum* U *von* f *zum Eigenwert* λ *ist ein linearer Unterraum* $U \supseteq V$ *mit* $U \neq \{0\}$.

Beweis. Seien $x, y \in U, a \in K$, dann gilt: $f(x+ay) = f(x)+a\cdot f(y) = \lambda x+a\lambda y = \lambda(x + ay)$, also $x + ay \in U$. $U \neq \{0\}$, da λ Eigenwert von f ist. □

Alle Feststellungen gelten entsprechend für Matrizen $A \in K^{n,n}$.

6.1 Bestimmung der Eigenwerte und -vektoren von $A \in K^{n,n}$

1. Bestimmung der Eigenwerte: Bestimme alle $\lambda \in K$ für die $\det(A-\lambda E) = 0$ gilt.
2. Bestimmung der Eigenräume $V(\lambda, A)$ von A zum Eigenwert λ ($V = K^n$): Man löse das homogene lineare Gleichungssystem $(A - \lambda E)x = 0$ (Eigenwert λ einsetzen). Der Eigenraum ist mindestens eindimensional (wenn λ wirklich Eigenwert ist).

Zu 1:

F 6.13.

$$\det(A - \lambda E) = \begin{vmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} - \lambda \end{vmatrix}$$

ist ein Polynom n-ten Grades von λ. Genauer

$$\det(A - \lambda E) = (-1)^n \lambda^n + b_{n-1}\lambda^{n-1} + \dots + b_1\lambda + b_0$$

mit $b_0, \dots, b_{n-1}, (-1)^n \in K$. Ferner gilt: $b_0 = \det A$,$b_{n-1} = (-1)^n$ Spur A.

Beweis. Nach dem Entwicklungssatz 5.5 ist klar, dass $\det(A-\lambda E)$ ein Polynom vom Grad höchstens n in λ ist.
Der einzige Summand aus den $n!$ Summanden, die selbst Produkte sind, der λ^n enthält, ist $(a_{11} - \lambda) \cdot \dots \cdot (a_{nn} - \lambda)$. Daher ist der Koeffizient von λ^n gleich $(-1)^n$.
$b_0 = \det A$ klar (wähle $\lambda = 0$). Der einzige Term, der λ^{n-1} enthält, kommt in $(a_{11} - \lambda) \cdot \dots \cdot (a_{nn} - \lambda)$ vor, also ist der Koeffizient von λ^{n-1} $(-1)^n \cdot (a_{11} + \dots + a_{nn})$ □

Satz 6.14. *Jede Menge von Eigenvektoren zu verschiedenen Eigenwerten von f ist linear unabhängig.*

Beweis. Seien $\lambda_1, \dots, \lambda_m$ paarweise verschiedene Eigenwerte von f und x_i ein zu λ_i gehöriger Eigenvektor von f, also $x_i \neq 0$ und $f(x_i) = \lambda_i x_i$.
Beweis durch vollständige Induktion nach m:

Induktionsanfang Für $m = 1$ gilt die Behauptung, da $x_1 \neq 0$.

Induktionsschritt Sei $\sum_{i=1}^{m} a_i x_i = 0$ mit $a_1, \dots, a_m \in K$. Zu zeigen ist: $a_i = 0$ für $i = 0, \dots m$. Wende die lineare Abbildung $(f - \lambda_m id)$ auf die Gleichung

an, also:

$$0 = f(0) = (f - \lambda_m id)\left(\sum_{i=1}^{m} a_i x_i\right) = \sum_{i=1}^{m} (f - \lambda_m id)\,(a_i x_i)$$

$$= \sum_{i=1}^{m} a_i \underbrace{(\lambda_i - \lambda_m)}_{\neq 0 \text{ für } i \neq m} x_i = \sum_{i=1}^{m-1} a_i(\lambda_i - \lambda_m)x_i \overset{\text{Induktion}}{\Longrightarrow} a_1 = \cdots = a_{m-1} = 0 \Longrightarrow$$

$$a_m \lambda_m = 0 \overset{\lambda_m \neq 0}{\Longrightarrow} a_m = 0$$ □

F 6.15. *Falls* $\dim V = n < \infty$*, dann kann* $f\colon V \to V$ *höchstens* n *verschiedene Eigenwerte haben.*

Definition 6.16. $f \in \mathrm{End}(V)$ heißt diagonalisierbar, wenn es eine Basis von V aus Eigenvektoren gibt. Entsprechend heißt eine Matrix $A^{n,n}$ diagonalisierbar, falls sie ähnlich zu einer Diagonalmatrix ist, d.h. falls es $S \in GL(n, K)$ gibt, sodass $D = S^{-1}AS$ eine Diagonalmatrix ist.

Offenbar gilt:

F 6.17. $A \in K^{n,n}$ *ist genau dann diagonalisierbar, wenn es eine Basis von* K^n *aus Eigenvektoren von* A *gibt.*

Beweis. Wenn $B = (b_1, \ldots, b_n)$ eine Basis aus Eigenvektoren zu Eigenwerten $\lambda_1, \ldots, \lambda_n$ ist, dann ist die zugehörige Matrix $D = \begin{pmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ und umgekehrt. Ferner gilt $D = B^{-1}AB$ □

Wenn $B = (b_1, \ldots, b_n)$ eine Basis aus Eigenvektoren von A ist und b_i Eigenvektor zum Eigenvektor λ_i, dann ist $B^{-1}AB = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ eine Diagonalmatrix.
Das Verfahren zur Diagonalisierung/Entscheidung ob A diagonalisierbar ist:

1. Bestimme alle (verschiedenen) Nullstellen $\lambda_1, \ldots, \lambda_m$ von $\det(A - \lambda E)$.
2. Bestimme zu jedem λ_i den Eigenraum $V(\lambda_i, A)$. Wähle in jedem dieser Eigenräume eine Basis. Dann ist die Vereinigung dieser Basen der Eigenräume wegen Satz 6.14 linear unabhängig.

Falls $\sum_{i=1}^{m} \dim V(\lambda_i, A) = n (= \dim V)$, dann ist A diagonalisierbar und die Vereinigung der (gewählten) Basen der Eigenräume ist eine Basis von V.
Umgekehrt gilt: Falls A diagonalisierbar ist, dann gibt es eine Basis von V aus Eigenvektoren von A und damit gilt $\sum_{i=1}^{m} \dim V(\lambda_i, A) = n$

F 6.18. *a)* $A \in K^{n,n}$ *ist diagonalisierbar genau dann, wenn*

$$\sum_{i=1}^{m} \dim V(\lambda_i, A) = n = \dim V$$

($\lambda_1, \ldots, \lambda_m$ paarweise verschiedene Eigenwerte von A)

b) Falls $A \in K^{n,n}$ n verschiedene Eigenwerte hat, dann ist A diagonalisierbar.

Definition 6.19. $\dim V(\lambda_i, A)$ nennt man auch die geometrische Vielfachheit des Eigenwertes λ_i.

Beispiel.

- $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ hat als einzigen Eigenwert 1, die geometrische Vielfachheit ist 2.
- $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ $\det(A - \lambda E) = \left|\begin{smallmatrix} 1-\lambda & 1 \\ 0 & 1-\lambda \end{smallmatrix}\right| = (1-\lambda)^2$. Also hat A nur einen Eigenwert, nämlich 1.

  $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right) \implies x_2 = 0$. Der zugehörige Eigenraum ist also: $\{\left(\begin{smallmatrix} x \\ 0 \end{smallmatrix}\right) | x \in \mathbb{R}\}$. Die geometrische Vielfachheit des Eigenwert 1 ist 1, daher ist A nicht diagonalisierbar.
- $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$: $\det(A - \lambda E) = \det \left(\begin{smallmatrix} -\lambda & -1 \\ a & -\lambda \end{smallmatrix}\right) = \lambda^2 + 1$
  $\implies$ für $K = \mathbb{R}$ hat A keine Eigenwert, also nicht diagonalisierbar.

  $\implies$ für $K = \mathbb{C}$ hat A die 2 verschiedenen Eigenwerte $(i, -i)$, ist also diagonalisierbar über $\mathbb{C}$.

  Bemerkung: Geometrisch beschreibt A eine Drehung um 90°.
- Projektion der Ebene auf eine Gerade g: Eigenwert 1 für alle Punkte auf g ungleich 0; Eigenwert 0 für alle Punkte ungleich 0 auf h, mit h orthogonal zu g
- Spiegelung einer Ebene an einer Geraden g: Eigenwert 1 für alle Punkte auf g ungleich 0; Eigenwert -1 für alle Punkte ungleich 0 auf h, mit h orthogonal g

Beispiel. Sei A diagonalisierbar. Bestimme A^n explizit: Bestimme die Matrix S mit $D = S^{-1}AS$, mit $D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_m \end{pmatrix}$ als Diagonalmatrix,

also

$$A = SDS^{-1} \implies A^n = SD^nS^{-1} = S \begin{pmatrix} \lambda_1^n & & 0 \\ & \ddots & \\ 0 & & \lambda_m^n \end{pmatrix} S^{-1}$$

6.2 Polynomringe

$K[X]$ mit $K^{\mathbb{N}_0}$ - Polynome über einem Körper K.
Beispiel:

$$\sum_{i=0}^{n} a_i x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} a_j b_{i-j} x^i\right)$$

Definition 6.20. Wir betrachten den K-Vektorraum $K^{\mathbb{N}_0}$ als eine abelsche Gruppe mit der Multiplikation $(a_i)_{i\in\mathbb{N}_0}\cdot(b_i)_{i\in\mathbb{N}_0} = \left(\sum_{j=0}^{i} a_j b_{i-j}\right)_{i\in\mathbb{N}_0}$.
Dies ist eine kommutativer Ring mit 1. Dieser Ring wird mit $K[X]$ bezeichnet und heißt der Polynomring über K.
Bezüglich der natürlichen Basis $(e_i)_{i\in\mathbb{N}_0}$ von $K^{\mathbb{N}_0}$ gilt $e_i = X^i$, wobei $X \coloneqq e_i$ und $X^0 \coloneqq 1 = e_0$ (1-Element des Ringes).
Also lässt sich $f \in K^{\mathbb{N}_0}$ eindeutig als $f = \sum_{i=0}^{n} a_i x^i$ darstellen mit $a_n \neq 0$ (für $f \neq 0$).
Die Elemente von $K[X]$ heißen Polynome.
Das Element $a \in K$ wird (stillschweigend) mit $a \cdot e_i$ identifiziert, also $K \subseteq K[X]$.
Sei $f \neq 0$ und $f = \sum_{i=0}^{n} a_i x^i$ mit $a_n \neq 0$, dann heißt n der Grad des Polynoms f, geschrieben: $n = \operatorname{grad} f$, $\operatorname{grad} 0 \coloneqq -\infty$.

Beispiel (Warum werden Polynome nicht einfach als Funktionen definiert?). Für die Abbildung $f\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ mit $f(X) = X^2 + X$ ist $f(0) = 0$, $f(1) = 1^2 + 1 = 0$ also als Abbildung $f = 0$. Als Polynom $X^2 + X \in Z_2[X]$ ist das nicht das Nullpolynom.

Satz 6.21. *Jedem $f \in K[X]$ kann man die Abbildung $X \mapsto f(X)$ zuordnen ($X \in K$). Diese Abbildung ist genau dann injektiv, wenn K unendlich ist.*

$$K[X] \to \operatorname{Abb}(K, K)$$

Es folgen nun einige Sätze ohne Beweise über Polynomringe.
(ausführlicher mit Beweisen z.B. in Florenz: Lineare Algebra I und in Büchern mit dem Titel „Algebra “und später in der Vorlesung Algebra)

F 6.22. *Für $f, g \in K[X]$ gilt*

a) $\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g$

b) $f \cdot g = 0 \implies f = 0$ *oder* $g = 0$, *das heißt* $K[X]$ *ist nullteilerfrei.*

c) $\operatorname{grad}(f + g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\}$

d) $\operatorname{grad}(f + g) = \operatorname{grad} f$, *falls* $\operatorname{grad} g < \operatorname{grad} f$

Satz 6.23 (Division mit Rest)**.** *Seien $f, g \in K[X]$, $g \neq 0$. Dann gibt es eindeutig bestimmte $s, r \in K[X]$ mit $f = s \cdot g + r$ und* $\operatorname{grad} r < \operatorname{grad} g$.

F 6.24. *Sei $b \in K$. Dann ist $K[X] \to K$, $\sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} a_i b^i$ ein Ringhomomorphismus. Es ist der b-Einsetzungshomomorphismus. Das Bild von f wird mit $f(b)$ bezeichnet. $b \in K$ heißt Nullstelle von f, falls $f(b) = 0$.*

F 6.25. *Sei b eine Nullstelle von $0 \neq f \in K[X]$. Dann gibt es ein Polynom g mit $f = (x - b) \cdot g$.*

Beweis. Aus Satz 6.23 folgt, dass $g, r \in K[X]$ existieren mit $f = (x - b) \cdot g + r$ mit $\operatorname{grad} r < \operatorname{grad}(x - b) = 1$. Also $\operatorname{grad} r = 0 \implies r \in K$. Ferner $f(b) = 0 = (b - b)g(b) + r \implies r = 0$. □

Definition 6.26. $a \in K$ heißt m-fache Nullstelle von $f \in K[X]$ ($m \in \mathbb{N}$), falls $(x - a)^m \mid f$ und $(x - a)^{m+1} \nmid f$. Dies ist äquivalent zu $f = (x - a)^m g$ mit $g \in K[X]$ und $g(a) \neq 0$.
m ist die Vielfachheit der Nullstelle a von f

Mit Folgerung 6.25 ist klar, dass jede Nullstelle eine eindeutig bestimmte Vielfachheit hat.

F 6.27. *Sei $f \in K[X]$ und $f \neq 0$. Dann lässt sich f schreiben als*

$$f = \left(\sum_{i=1}^{k} (x - a_i)^{m_i} \right) g \qquad (m_i > 0,\ a_i \neq a_j \text{ für } i \neq j)$$

wobei g keine Nullstellen in K hat.

F 6.28. *Die geometrische Vielfachheit eines Eigenwertes λ von $A \in K^{n,n}$ ist kleiner oder gleich der algebraischen Vielfachheit von λ (= Vielfachheit der Nullstelle λ vom Polynom* $\det(A - \lambda E)$.

Beweis in der Übung.

Definition 6.29. Sei R ein Ring, $I \subseteq R$ heißt Ideal, falls

$$I \neq \emptyset \qquad \forall a, b \in I : a + b \in I \qquad \forall a \in I, r \in R : ar \in I \wedge ra \in I$$

Die Ideale sind für Ringe, was Nullteiler für Gruppen sind.

F 6.30 (Homomorphiesatz)**.** *Sei $f \colon R \to S$ ein Ringhomomorphismus. Dann ist* $\ker f$ *ein Ideal in R.*

Satz 6.31. *Sei I ein Ideal in $K[X]$. Dann existiert ein $g \in I$ mit $I = g \cdot K[X] = \{g \cdot f | f \in K[X]\}$.*

Beweis. Falls $I = \{0\}$, wähle $g = 0$. Sonst wähle $g \in I \setminus \{0\}$ mit minimalen Grad. Sei $h \in I$, dann existieren $r, s \in K[x]$ mit $h = g \cdot s + r$ mit $\operatorname{grad} r < \operatorname{grad} g \implies r = h - gs \in I \implies r = 0$, da $\operatorname{grad} g$ minimal ist in $I \setminus \{0\}$. Also $g \mid h \implies I \subseteq g \cdot K[X]$. $g \cdot K[X] \subseteq I$ ist klar. □

Bemerkung. a) Der Beweis zeigt: falls $I \neq \{0\}$ kann man g beliebig unter solchen mit kleinstem Grad wählen.

b) Falls $I \neq \{0\}$, ist g eindeutig bestimmt, wenn man fordert, dass g normiert ist.

Definition 6.32. $\sum_{i=0}^{n} a_i x^i = g \in K[X]$ heißt normiert, falls $a_n = 1$.

Definition 6.33. Sei $0 \neq f \in K[X]$. f zerfällt über K, falls $f = b \prod_i (x - a_i)^{m_i}$ mit $0 \neq b \in K$, $m_i \in \mathbb{N}$.

Definition 6.34. Falls für alle $0 \neq f \in K[X]$ aus $\operatorname{grad} f > 0$ folgt, dass f eine Nullstelle hat, nennt man K algebraisch abgeschlossen (das heißt, dass jedes Polynom zerfällt).

Satz 6.35 (Hauptsatz der Algebra)**.** $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Bemerkung. Der kleinste algebraische Abschluss von $\mathbb{Q}$ ist nicht $\mathbb{C}$, sondern abzählbar.

Satz 6.36. *Sei $p \in \mathbb{R}[X]$. Wenn $n \in \mathbb{C} \setminus \mathbb{R}$ ein Nullstelle von p ist, ist $\overline{n}$ ebenfalls eine Nullstelle von p.*
Das bedeutet, dass die nicht-reellen Nullstellen in komplex-konjugierten Paaren mit jeweils gleicher Vielfachheit vor.

6.3 Trigonalisierbarkeit

Sei V ein K-Vektorraum, $\dim V = n < \infty$, $f\colon V \to V$ linear.

Definition 6.37. Sei $A \in K^{n,n}$. Dann sei $\chi_A \in K[X], \chi_(X) = \det(XE_n - A)$. χ_A heißt charakteristisches Polynom. χ_A ist ein normiertes Polynom n-ten Grades. Beachte $\chi_A(\lambda) = \det(\lambda E_n - A) = (-1)^n \det(A - \lambda E_n)$.

F 6.38. *Ähnliche Matrizen haben dasselbe charakteristische Polynom, also $A \approx B \implies \chi_a = \chi_b$.*

Beweis. Seien $A, B \in K^{n,n}$, $A \approx B$. Dann gibt es $S \in GL(n)$ mit $B = S^{-1}AS$, also

$$\begin{aligned}\chi_B &= \det(XE_n - B) = \det(XE_n - S^{-1}AS) = \det(S^{-1}(XE_n - A)S)\\ &= \det(S^{-1})\chi_A \det(S) = \chi(A)\end{aligned}$$

□

Definition 6.39. Sei $f\colon V \to V$ eine lineare Abbildung mit V endlichem Vektorraum. Das charakteristische Polynom χ_f ist definiert als $\chi_f = \chi_A$, wobei A die Matrix von f bezüglich einer beliebigen Basis von V ist. (Nach Folgerung 6.38 ist dies wohldefiniert.)

F 6.40. *Wenn $A = \left(\begin{smallmatrix} A_1 & B \\ 0 & A_2 \end{smallmatrix}\right)$ mit A_1 und A_2 quadratischen Matrizen, dann ist $\chi_A = \chi_{A_1} \cdot \chi_{A_2}$.*

Beweis. $\chi_A = \det(XE - A) = \det\left(\begin{smallmatrix} XE - A_1 & -B \\ 0 & XE - A_2 \end{smallmatrix}\right) = \det(XE - A_1)\det(XE - A_2) = \chi_{A_1} \cdot \chi_{A_2}$ □

Definition 6.41. $A \in K^{n,n}$ heißt trigonalisierbar, falls sie ähnlich zu einer oberen Dreiecksmatrix ist.
$f \operatorname{End}(V)$ heißt trigonalisierbar, falls es eiine Basis von V gibt, sodass die Matrix von f bezüglich dieser Basis eine obere Dreiecksmatrix ist.

Satz 6.42. *Sei $f \in \operatorname{End}(V)$. f ist genau dann trigonalisierbar, wenn χ_f in Linearfaktoren zerfällt. D.h. $\chi_f(X) = \prod_i (X - \lambda_i)$ mit $\lambda_1, \dots \lambda_n \in K$.*

Beweis. Wenn f trigonalisierbar, dann gibt es eine Basis bezüglich der die Matrix A von f eine obere Dreiecksmatrix ist, also

$$A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \implies \chi_f(X) = \chi_A(X) \overset{6.40}{=} (X - \lambda_1) \cdot \dots \cdot (X - \lambda_n)$$

Nun sei $f \in \operatorname{End}(V)$, sodass χ_f in Linearfaktoren zerfällt. Beweis mit Induktion nach $n = \dim V$:

Induktionsanfang $n = 1$ Jede Matrix mit nur 1 Eintrag ist eine obere Dreiecksmatrix.

Induktionsannahme Gelte die Aussage für $n - 1$ ($n \geq 2$).

Induktionsschritt Sei $\dim V = n$. Wähle einen Eigenwert λ_1 und zugehörigen Eigenvektor x_1. Ergänze ihn zu einer Basis $(x_1, \dots, x_n)$ von V (Basisergänzungssatz). Bezüglich dieser Basis ist die Matrix von f von der Form

$$A = \begin{pmatrix} \lambda_1 & a_{12} \dots a_{1n} \\ 0 & B \end{pmatrix}$$

da $f(x_1) = Ax_1 = \lambda_1 x_1$ (nach der Definition von Eigenwert). Sei $W = \operatorname{Lin}\{x_2, \dots, x_n\}$. Sei $g \colon W \to W \in \operatorname{End}(W)$ mit Matrix B bezüglich der Basis $(x_2, \dots, v_n)$ von W. Das charakteristische Polynom von f ist $\chi_f(X) = (X - \lambda_1)\chi_B(X) = (X - \lambda_1)\chi_g(X)$. Also ist g nach Induktionsannahme trigonalisierbar, d.h. es gibt eine Basis $(y_2, \dots, y_n)$, sodass die Matrix C von g bezüglich dieser Basis eine obere Dreiecksmatrix ist. Damit ist die Matrix $\sim A$von f bezüglich der Basis $(x_1, y_2, \dots, y_n)$ von der Form ï

$$\tilde{A} = \begin{pmatrix} \lambda_1 & \tilde{a_{12}}, \dots \tilde{a_{1n}} \\ 0 & C \end{pmatrix},$$

also eine obere Dreiecksmatrix.

□

Bemerkung. Der Beweis liefert ein Verfahren die Basis und die obere Dreiecksmatrix schrittweise zu bestimmen.

Korollar 6.43. *Für $A \in K^{n,n}$ gilt: χ_A zerfällt genau dann in Linearfaktoren, wenn A trigonalisierbar ist.*

Korollar 6.44. *Jede Matrix in $K^{n,n}$ mit K algebraisch abgeschlossen, insbesondere $K = \mathbb{C}$, ist trigonalisierbar.*

6.4 Einsetzen von Matrizen in Polynome

Definition 6.45. Sei $p \in K[X]$, $p = \sum_{i=0}^{n} a_i X^i$. Für $f \in \mathrm{End}(V)$ und $A \in K^{n,n}$ definiere

$$p(f) = a_0 \,\mathrm{id}_V + a_1 f + a_2 (f \circ f) + a_3 f^3 + \dots a_n f^n$$
$$p(A) = a_0 E + a_1 A + a_2 A^2 + \dots a_n A^n$$

Es gilt

$$(p_1 \cdot p_2)(f) = p_1(f) \circ p_2(f)$$
$$(p_1 \cdot p_2)(A) = p_1(A) p_2(A)$$
$$(p_1 + p_2)(f) = p_1(f) + p_2(f)$$

Satz 6.46 (Cayley-Hamilton)**.** *Für alle $f \in \mathrm{End}(V)$ ($\dim V < \infty$) gilt $\chi_f(f) = 0 = (x \mapsto 0)$.*
Für $A \in K^{n,n}$ gilt $\chi_A(A) = 0$.

Beweis. Vorbereitung: Sei $0 \neq x \in V$. Betrachte $(x, f(x), \dots f^n(x))$. Dieses Tupel von Vektoren ist linear abhängig, da $\dim V = n < n + 1$. Sei $r \leq n$ die kleinste Zahl mit $(x, f(x), \dots f^r(x))$ linear abhängig, also $(x, f(x), \dots f^{r-1}(x))$ linear unabhängig. Dann existieren $c_0, c_1, \dots c_{r-1}$ mit $f^r(x) = \sum_{i=0}^{r-1} c_i f^i(x)$. Sei

$$U_x = \mathrm{Lin}\{x, f(x), f^2(x), \dots, f^{r-1}(x)\}$$
$$\text{mit der Basis } B = (b_1, b_2, \dots b_r) \text{ mit } f(b_i) = b_{i+1} \text{ für } i = 1, \dots r-1$$
$$\implies f(b_r) = \sum_{i=1}^{r} c_{i-1} b_1$$

Folglich ist $f(U_x) \subseteq U_x$ und die zugehörige Matrix von $f|_{U_x} : U_x \to U_x$ bezüglich der Basis B ist

$$M_x = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & c_0 \\ 1 & 0 & 0 & \dots & 0 & c_1 \\ 0 & 1 & 0 & \dots & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & c_{r-2} \\ 0 & 0 & 0 & \dots & 1 & c_{r-1} \end{pmatrix}$$
$$\implies \chi_{M_x} = x^r - c_{r-1} x^{r-1} - c_{r-2} x^{r-2} - \dots c_1 x - c_o$$
$$\implies \chi_{M_x}(f)(x) = f^r(x) - c_{r-1} f^{r-1}(x) - c_{r-2} f^{r-2}(x) - \dots c_1 f(x) - c_o x = 0$$

Zu zeigen ist nun $\chi_f(f) = 0 \iff \forall x \in V : \chi_f(f)(x) = 0$. Für $x = 0$ klar. Sei also $x \neq 0$. Dann betrachte U_x wie oben und ergänze B zu einer Basis $(b_1, \ldots, b_r, b_{r+1}, \ldots, b_n)$ von V. Die Matrix von f hat bezüglich dieser Basis die Form $A = \left(\begin{smallmatrix} M_x & C \\ 0 & D \end{smallmatrix}\right)$. Es gilt als $\chi_f = \chi_A = \chi_{M_x} \cdot \chi_D$ nach Folgerung 6.40. Also $\chi_f(f)(x) = (\chi_{A_x} \circ \chi_D(f))(x) = \chi_{M_x}(f)(\chi_D(f)(x)) = 0$, da $\chi_{M_x}(f)$ die Nullfunktion ist. □

Definition 6.47. Sei $f \in \mathrm{End}(V)$ $(dim V = n < \infty)$
Es gibt genau ein Polynom $\mu_f \in K[X]$ mit folgenden Eigenschaften:

(1) μ_f ist normiert

(2) $\mu_f(f) = 0$

(3) $\forall \varphi \in K[X]$ gilt: $\varphi(f) = 0 \Rightarrow \mu_f \mid \varphi$ (teilt)
(d.h. $\exists \psi \in K[X]$ mit $\varphi = \psi \cdot \mu_f$)

μ_f heißt das Minimalpolynom von f.

Beweis. Sei $I = \{\varphi \in K[X] \mid \varphi(f) = 0\}$ I ist ein Ideal in $K[X]$ (Kern des Homomorphismus $\varphi \mapsto \varphi(f)$)
Nach Satz 6.31 gibt es $\psi \in I$ mit $I = \psi \cdot K[X]$. Es gilt also genau ein normiertes Polynom $\mu_f \in I$ mit $I = \mu_f \cdot K[X]$, d.h. welches 3 und 2 erfüllt. □

Bemerkung. μ_f ist durch folgende Eigenschaften eindeutig bestimmt:

(I) μ_f ist normiert

(II) $\mu_f(f) = 0$

(III) μ_f hat den kleinsten Grad unter den Polynomen $\psi \neq 0$ mit $\psi(f) = 0$ (vergleiche Beweis zum Satz 6.31)

Satz 6.48. *Sei $f \in \mathrm{End}(V)$. Dann gilt:*

a) $\mu_f | \chi_f$

b) Falls a ein Eigenwert von f ist, dann ist $\mu_f(a) = 0$

c) Wenn f genau n verschiedene Eigenwerte hat, dann ist $\mu_f = \chi_f$

Beweis. a) nach Definition von μ_f und Satz 6.46 von Caley-Hamilton.

b) Sei $f(x) = ax$ für ein $x \neq 0$ und $\mu_f = b_0 + b_1 x + \cdots + b_{k-1} x^{k-1} + x^k$. Dann folgt

$$0 = \mu_f(f)(x) = \left(\sum_{i=1}^{k} b_i f^i \right)(x) = \sum_{i=0}^{k} b_i f^i(x) = \sum_{i=0}^{k} b_i a^i x = \mu_f(a) x$$

Also $\mu_f(a) = 0$.

c) Wenn f n verschiedene Eigenwerte hat, dann ist wegen b) $\operatorname{grad}(\mu_f) = n = \operatorname{grad}(\chi_f)$. Mit $\mu_f \mid \chi_f$ und μ_f, χ_f normiert folgt $\mu_f = \chi_f$. □

Bemerkung. Zu jedem Körper K gibt es einen Erweiterungskörper L (d.h. $K \subseteq L$ Unterkörper), der algebraisch abgeschlossen ist und zwar so, dass jedes Element in L Nullstelle eines Polynoms in $K[X]$ ist ($K[X] \subseteq L[X]$).
Ein socher Körper heißt der algebraische Abschluss von K. Er ist bis auf Isomorphie eindeutig bestimmt.
Beweis erfolgt später in einer Algebra-Vorlesung.

F 6.49. *Sei $A \in K^{n,n}$. Dann sind χ_A und μ_A unabhängig davon, ob man A als Matrix in $K^{n,n}$ oder in $L^{n,n}$ auffasst. (L Erweiterungskörper von K)*

Beweis. klar □

Definition 6.50. Sei $f = \sum_{i=0}^{n} a_i x^i \in K[X]$. Dann bezeichne $f' = \sum_{i=1}^{n} i a_i x^{i-1} \in K[X]$. f' heißt die (formale) Ableitung

F 6.51. *Zu $f, g \in K[X]$ gibt es genau ein normiertes Polynom h größten Grades mit $h \mid f$ und $h \mid g$, geschrieben $h = \operatorname{ggT}(f, g)$*
Ferner gilt: h lässt sich darstellen in der Form $h = \operatorname{ggT}(f, g) = uf + vg$ mit $u, v \in K[X]$

Beweis. Sei $I = \{uf + vg \mid u, v \in K[X]\}$ das von $\{f, g\}$ erzeugte Ideal. Dann gibt es nach 6.31 genau ein normiertes Polynom $h \in I$ mit $I = h \cdot K[X]$.
h kann algorithmisch mit dem Euklidischen Algorithmus gefunden werden. □

F 6.52. *Falls $\operatorname{char}(K) = 0$ und $f \in K[X]$ eine k-fache Nullstelle a hat, dann ist $(x-a)$ ein gemeinsamer Teiler von $f, f', \ldots, f^{(k-1)}$, aber a keine Nullstelle von $f^{(k)}$.*

Beweis. Vollständige Induktion nach k (Übung) □

Beispiel. $x^5 + 1 = (x+1)^5$ in $\mathbb{Z}_5$, aber $(x^5+1)' = 5x^4 = 0$ (siehe HA 4b).
Beachte, dass $\operatorname{char}(Z_5) = 5 \neq 0$.

F 6.53. *Sei $A \in K^{n,n}$. Falls $\mathrm{ggT}(\chi_A, \chi_A') = 1$, dann hat χ_A im Erweiterungskörper von K keine mehrfachen Nullstellen, also $\mu_A = \chi_A$.*

Beweis. Nutze Satz 6.52, 6.51, 6.49, die Existenz eines algebraischen Abschlusses und 6.48 c) □

6.5 Jordan'sche Normalform

Definition 6.54 (Jordanmatrix)**.** Sei $\lambda \in K$, $m \in \mathbb{N}$. Dann ist die Jordanmatrix

$$J(\lambda, m) := \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \lambda & 1 \\ & & 0 & \lambda \end{pmatrix} \in K^{m,m}$$

Also $J(\lambda, m) = \lambda E_m + J(0, m)$

Beispiel. $J(\lambda, 1) = (\lambda)$, $J(\lambda, 2) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$

Satz 6.55 (Jordan'sche Normalform)**.** *Sei V ein K-Vektorraum, $\dim V = n < \infty$, $f \in \mathrm{End}(V)$. Falls χ_f in Linearfaktoren zerfällt (z.B. für $K := \mathbb{C}$ stets der Fall), dann existiert eine Basis B von V, sodass die Matrix von f bezüglich dieser Basis die Form hat*

$$\begin{pmatrix} J(\lambda_1, m_1) & & & \mathbf{0} \\ & J(\lambda_2, m_2) & & \\ & & \ddots & \\ \mathbf{0} & & & J(\lambda_k, m_k) \end{pmatrix} \in K^{n,n}$$

Sie heißt die Jordan'sche Normalform von f. Dabei müssen die λ_i nicht verschieden sein.

Satz 6.56 (Eindeutigkeit der Jordanschen Normalform)**.** *Die Jordan'sche Normalform ist eindeutig bis auf die Reihenfolge der Jordan-Kästchen.*

Beweis. Seien $\lambda_1, \ldots, \lambda_s$ die paarweise verschiedenen Eigenwerte von f. Dabei ist s die Anzahl der Eigenwerte. Dann gehören zu λ_i genau h_i Jordan-Matrizen

(genannt Jordankästchen).

$$\begin{aligned}
&\text{zu } \lambda_1\text{: } J(\lambda_1, n_{11}), \ldots, J(\lambda_1, n_{1h_1}) \\
&\qquad\qquad \vdots \\
&\text{zu } \lambda_l\text{: } J(\lambda_l, n_{l1}), \ldots, J(\lambda_l, n_{lh_l}) \\
&\qquad\qquad \vdots \\
&\text{zu } \lambda_s\text{: } J(\lambda_s, n_{s1}), \ldots, J(\lambda_s, n_{sh_s}) \qquad\qquad (l = 1, \ldots, s)
\end{aligned}$$

O.B.d.A. sei für alle i: $n_{i1} \geq n_{i2} \geq \ldots \geq n_{ih_i}$. Die Jordankästchen eines Eigenwertes sind nach Größe geordnet. h_i ist die Anzahl der Jordankästchen zum EW λ_i.
Alle Jordankästchen zu einem Eigenwert bilden einen Jordankasten:

$$\boxed{\begin{matrix} J(\lambda_l, n_{l1}) & & \\ & \ddots & \\ & & J(\lambda_l, n_{lh_l}) \end{matrix}}$$

Die Jordanmatrix besteht aus den s Jordankästen:

$$\begin{pmatrix} \boxed{\begin{matrix} J(\lambda_1, n_{11}) & & \\ & \ddots & \\ & & J(\lambda_1, n_{1h_1}) \end{matrix}} & & \\ & \ddots & \\ & & \boxed{\begin{matrix} J(\lambda_s, n_{s1}) & & \\ & \ddots & \\ & & J(\lambda_s, n_{sh_s}) \end{matrix}} \end{pmatrix}$$

$\dim\ker(J(0,m)^k) = \min\{k, m\}$ (Beweis: Übung). $J(0,m)$ ist also nilpotent.
Es gilt $J(\lambda, m) + \mu E_m = J(\lambda + \mu, m)$
Weiterhin gilt $\dim\ker(J(\lambda, m)^k) = 0$ für $\lambda \neq 0$, da

$$\det(J(\lambda, m)) = \lambda^m \neq 0$$

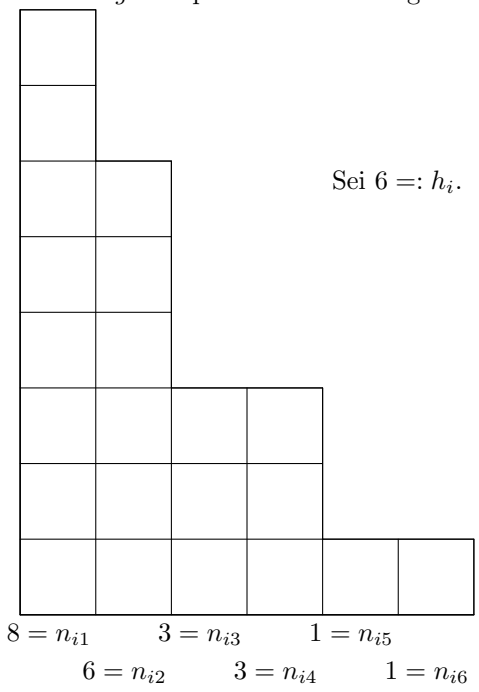
$$\det(J(\lambda, m)^k) \overset{5.4.(1)}{=} (\det(J(\lambda, m)))^k = (\lambda^m)^k = \lambda^{mk} \neq 0$$

Unter der Annahme der Existenz einer Jordan'schen Normalform für $f \in \mathrm{End}(V)$ möchten wir für jeden Eigenwert die zugehörigen n_{ij} ermitteln: Sei $A \in K^{n,n}$ die Matrix zu f in Jordan'scher Normalform. Dann bezeichne für einen Eigenwert λ_i von A und ein $j \in \mathbb{N}$:

$$m_{ij} := \dim\ker((f - \lambda_i \,\mathrm{id})^j) \overset{S3.2\&F.3.7}{=} \dim\ker((A - \lambda_i E)^j) = \sum_{t=1}^{h_i} \min\{n_{it}, j\}$$

Bemerke: m_{ij} hängt nur von j, λ und f ab. Begründung für letztes „=“: Die Jordan-Kästchen mit $\lambda \neq \lambda_i$ tragen nicht zum ker bei, die anderen werden summiert entsprechend obiger Überlegung zu $J(0,m)$. ($\det(J(\lambda-\lambda_i,m)^k) \neq 0$, für $\lambda \neq \lambda_i$) □

Bemerkung. Graphische Darstellung für die Bestimmung von n_{ij} aus m_{ij}:



Bemerkung. Da $(\forall j \in \mathbb{N})$ die m_{ij} nur von f abhängen und die n_{ij} eindeutig von den m_{ij} bestimmt werden, ist der Jordankasten eindeutig. (bis auf die Reihenfolge der Kästchen, (ist aber egal für geforderte Eindeutigkeit)) ($f = \tilde{f} \Rightarrow m_{ij} = \tilde{m}_{ij} \Rightarrow n_{ij} = \tilde{n}_{ij}$) Außerdem ist ein Algorithmus zur Bestimmung der Jordan'schen Normalform gegeben.

Ferner gilt, da Matrizen in der Jordan'schen Normalform Dreiecksmatrizen sind, $m_{i\,\max\{n_{ij}|j\in\mathbb{N}\}}$ die Summe der Größen der Jordankästchen zum Eigenwert λ_i ist (also größe des Jordankasten), n_{i1} die Größe des größten Jordankästchen zum Eigenwert λ_i ist und damit $J(0,n_{i1})^{n_{i1}-1} \neq 0$ und $J(0,n_{i1})^{n_{i1}} = 0$, und weil $\chi_f = \chi_A$ und $\mu_f = \mu_A$ und weil eine Basis existiert wie wir noch zeigen werden.

$$\chi_f = \prod_{i=1}^{s} (X-\lambda_i)^{m_{in_{i1}}}$$

$$\mu_f = \prod_{i=1}^{s} (X-\lambda_i)^{n_{i1}}$$

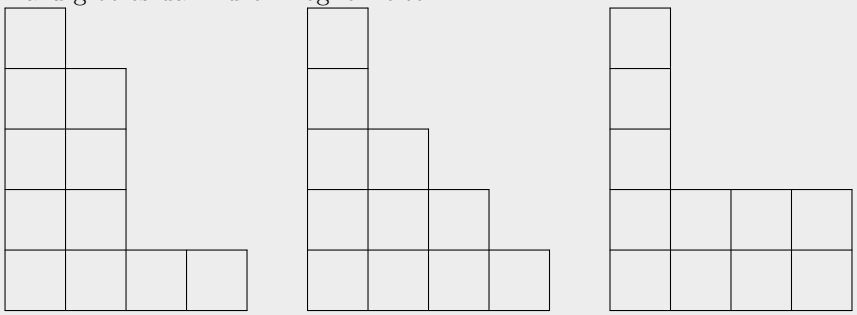
und $\chi_f = \mu_f \Leftrightarrow$ zu jedem λ_i gibt es genau ein Jordankästchen. d.h. $h_i = 1$ für alle $i = 1,\ldots,n$ sowie f ist diagonalisierbar $\Leftrightarrow n_{ij} = 1$ für alle $i = 1,\ldots n$, $j = 1,\ldots,h_i$

Beispiel. Wie viele und welche Äquivalenzklassen von Matrizen $A \in \mathbb{C}^{11,11}$ unter Ähnlichkeit gibt es, für die gilt $\mu_A = X^5$ und $\dim \ker A = 4$?
$\dim \ker A = \dim \ker(A - \underbrace{\lambda}_{=0} E)^1 = 4 \Rightarrow h = 4$

Lösung: Wegen $\mu_A = X^5$ ist 0 der einzige Eigenwert. Zu diesen wissen wir folgendes:

$\mu_A = x^5$

Dazu gibt es dann drei Möglichkeiten:



Die zugehörigen Matrizen sind (wobei $J_i := J(0, i)$):

$$\begin{pmatrix} \boxed{\begin{matrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & 1 & \\ & & & 0 & 1 \\ & & & & 0 \end{matrix}} & & & \\ & \boxed{\begin{matrix} 0 & 1 & & \\ & 0 & 1 & \\ & & 0 & 1 \\ & & & 0 \end{matrix}} & & \\ & & \boxed{0} & \\ & & & \boxed{0} \end{pmatrix}$$

$$= \begin{pmatrix} J_5 & & & 0 \\ & J_4 & & \\ & & J_1 & \\ 0 & & & J_1 \end{pmatrix}, \begin{pmatrix} J_5 & & & 0 \\ & J_3 & & \\ & & J_2 & \\ 0 & & & J_1 \end{pmatrix}, \begin{pmatrix} J_5 & & & 0 \\ & J_2 & & \\ & & J_2 & \\ 0 & & & J_2 \end{pmatrix}$$

Der Beweis zur Existenz der Jordan'schen Normalform wird nun mit mehreren Hilfssätzen vorbereitet.

Definition 6.57 (nilpotent)**.** $f \in \mathrm{End}(V)$ heißt k-stufig nilpotent ($k \in \mathbb{N}$), falls $f^k = 0$, $f^i \neq 0$ für $0 \leq i < k$.
f heißt nilpotent, falls $k \in \mathbb{N}$ existiert, sodass f k-stufig nilpotent ist.

Lemma 6.58 (Zerlegung in Unterräume)**.** *Sei* $\dim V < \infty$, $f \in \mathrm{End}(V)$. *Dann gibt es Unterräume* V_N, V_B *von* V, *sodass gilt:*

(I) $f(V_N) \subseteq V_N$ *und* $f(V_B) \subseteq V_B$

(II) $f|_{V_N}^{V_N}$ *ist nilpotent und* $f|_{V_B}^{V_B}$ *ist bijektiv*

(III) $V = V_N \oplus V_B$ *(* $:\iff V = V_N + V_B \wedge V_N \cap V_B = \{0\}$ *)*

Beweis. Sei $V_i := \ker f^i$ $(i = 1, ...)$. Dann ist $V_i \subseteq V_{i+1}$. Da $\dim V < \infty$ gibt es $k \in \mathbb{N}$ mit $V_k = V_{k+1}$. Wähle k minimal mit dieser Eigenschaft und sei $V^i := f^i(V)$. Dann ist $V^i \supseteq V^{i+1}$, da $f(V) \subseteq V \Rightarrow f^i(f(V)) \subseteq f^i(V)$. Nach Dimensionssatz für lineare Abbildungen, angewendet auf f^i, ist $\dim V_i + \dim V^i = \dim \ker f^i + \dim f^i(V) = \dim V = n$, also $V^{k+1} = V^k$. Setze $V_N := V_k = \ker f^k$, $V_B := V^k = f^k(V)$. Sei $x \in V_N$. Dann ist $f^k(f(x)) = f(\underbrace{f^k(x)}_{=0}) = 0$. Also $f(x) \in V_N$. Sei $x \in V_B$. Dann ist $x = f^k(u)$ für ein $u \in V$, also $f(x) = f(f^k(u)) = f^k(f(u))$ $(\implies$ (I)$)$
$(f|_{V_N})^k \equiv 0$, also ist $f|_{V_N}$ nilpotent (k-stufig-nilpotent).
$f(V_B) = f(f^k(V)) = f^{k+1}(V) = f^k(V) = V_B$, also ist $f|_{V_B}$ surjektiv, also $f|_{V_B}$ bijektiv (wegen $\dim V_B < \infty$) $(\implies$ (II)$)$
Sei $x \in V_B \cap V_N$. Dann ist $f^k(x) = 0 = f^k(0)$ (wegen $x \in V_N$). Da $f|_{V_B}$ bijektiv ist, folgt $x = 0$, also $V_B \cap V_N = \{0\}$. Wegen $\dim V = n = \dim V_B + \dim V_N = \dim(V_B + V_N) + \dim(V_B \cap V_N) = \dim(V_B + V_N)$ ist $V = V_B + V_N$. □

Definition 6.59 (Hauptraum zum Eigenwert λ)**.** Sei $f \in \mathrm{End}(V)$ und λ ein Eigenwert von f. Sei λ eine k-fache Nullstelle von μ_f. Dann definiere den Hauptraum von f zum Eigenwert λ als:

$$H(f, \lambda) := \bigcup_{s=1}^{\infty} \ker(f - \lambda \,\mathrm{id})^s$$

Es gilt

$$\ker(f - \mathrm{id}) \subsetneq \ker(f - \lambda\,\mathrm{id})^2 \subsetneq \cdots \subsetneq \ker(f - \lambda\,\mathrm{id})^k = H(f, \lambda)$$

vgl. Aufgabe 2a) auf dem 4. Übungsblatt.

Satz 6.60 (Zerlegung in Haupträume)**.** *Sei $f \in \mathrm{End}(V)$ und zerfalle das charakteristische Polynom χ_f in Linearfaktoren und seien $\lambda_1, \ldots, \lambda_k$ die verschiedenen Eigenwerte von f. $\chi_f = \prod_{i=1}^{k}(X - \lambda_i)^{m_i}$. Sei $V_i := H(f, \lambda_i)$. Dann gilt:*

(I) $V_i \supseteq f(V_i)$

(II) $V = V_1 \oplus \cdots \oplus V_k$

(III) Es gibt eine Basis von V bezüglich der die Matrix von f von der Form

$$\begin{pmatrix} A_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & A_k \end{pmatrix}$$

ist und $\chi_{A_i} = (X - \lambda_i)^{m_i}$

Beweis. Vollständige Induktion nach k.
Induktionsanfang: Für $k = 1$ gilt die Behauptung.
Induktionsannahme: Die Behauptung gilt für $k - 1$.
Induktionsschritt: Sei $\chi_f = (X-\lambda_1)^{m_1} \cdots (X-\lambda_k)^{m_k}$. Wende 6.58 auf $f - \lambda_1\,\mathrm{id}$ an. Dann ist $V = V_N \oplus V_B$ mit geeigneten V_N, V_B, sodass $(f - \lambda_1\,\mathrm{id})|_{V_n}$ nilpotent und $(f - \lambda_1\,\mathrm{id})|_{V_B}$ bijektiv ist mit $(f - \lambda_1\,\mathrm{id})(V_N) \subseteq V_N$ und $(f - \lambda_1\,\mathrm{id})(V_B) \subseteq V_B$. Wähle eine geordnete Basis zunächst von V_N und dann V_B. Dann ist die zugehörige Matrix von $f - \lambda_1\,\mathrm{id}$ eine Blockmatrix $\begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix}$ mit A nilpotent und B regulär und

$$\chi_{f-\lambda_1\,\mathrm{id}} = \chi_A \cdot \chi_B = \prod_{i=1}^{k}(X - \lambda_i + \lambda_1)^{m_i} = X^{m_1}\prod_{i=2}^{k}(X - \lambda_i + \lambda_1)^{m_i}$$

Da A nilpotent ($\implies$ einziger Eigenwert ist 0) und B regulär ($\implies$ 0 ist kein Eigenwert) ist, folgt $\chi_A = X^{m_1}$. Für f haben wir bezüglich derselben Basis die Matrixdarstellung $\begin{pmatrix} A + \lambda_1 E_{m_1} & 0 \\ 0 & B + \lambda_1 E_{n-m_1} \end{pmatrix}$. Auf $f|_{V_B}$ wenden wir die Induktionsannahme an und erhalten die gewünschte Zerlegung von V. □

Wir haben damit gezeigt, dass es eine geordnete Basis von V gibt bezüglich der die Matrix von f die Form $\begin{pmatrix} A_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & A_k \end{pmatrix}$ hat, wobei $\chi_{A_1} = (X - \lambda_i)^{m_i}$.

Daher reicht es für den Beweis von 6.55 die Haupträume $H(f, \lambda_i)$ einzeln und statt f die Abbildungen $(f - \lambda_i \,\mathrm{id})|_{H(f,\lambda_i)} : H(f, \lambda_i) \to H(f, \lambda_i)$, d.h. nilpotente Endomorphismen zu betrachten. Dafür nutze folgendes Lemma:

Lemma 6.61. *Sei $f \in \mathrm{End}(V)$, k-stufig nilpotent, also $f^k \equiv 0, f^{k-1} \not\equiv 0$. Sei $x_0 \in V$ mit $f^{k-1} \neq 0$. Dann ist $(x_0, f(x_0), \ldots, f^{k-2}(x_0), f^{k-1}(x_0)) =: \tilde{w}$ linear unabhängig. Sei $W := \mathrm{Lin}\ \tilde{w}$. Dann gibt es $U \subseteq V$ mit $f(U) \subseteq U$ und $V = W \oplus U$*

Beweis. Wir zeigen, dass $(x_0, f(x_0), \ldots, f^{k-1}(x_0))$ linear unabhängig ist: $f^{k-1}(x_0) \neq 0 \Rightarrow (f^{k-1}(x_0))$ ist linear unabhängig. Sei l die kleinste Zahl, sodass $f^l(x_0)$, $f^{l-1}(x_0)$, $\ldots$, $f^{k-1}(x_0)$ linear unabhängig sind. Angenommen, $l > 0$, dann wäre $f^{l-1}(x_0) = \sum_{i=l}^{k-1} \lambda_i f^i(x_0) \Rightarrow f^l(x_0) = f(f^{l-1}(x_0)) = \sum_{i=l}^{k-1} \lambda_i f^{i+1}(x_0) = \sum_{i=l+1}^{k-1} \lambda_{i-1} f^i(x_0)$ (wegen $f^k(x_0) = 0$)im Widerspruch zu $f^l(x_0), f^{l-1}(x_0), \ldots, f^{k-1}(x_0)$ linear unabhängig.
Existenz von U: Beweis mit Induktion nach k:
Falls $k = 1$ ist $f \equiv 0$ und jedes Komplement von $W = \mathrm{Lin}\{x_0\}$ hat die gewünschte Eigenschaft. Sei die Behauptung für alle $m \leq k - 1$ bewiesen. Sei $V_1 = f(V)$, $W_0 = f(V) \cap W$, $y_0 = f(x_0)$. Dann

$$f^{k-1}(V_1) = \{0\},\ W_0 = \mathrm{Lin}\{y_0, f(y_0), \ldots, f^{k-1}(y_0)\} = \mathrm{Lin}\{f(x_0), \ldots, f^{k-1}(x_0)\}$$

Nach Induktionsannahme angewendet auf $f|_{V_1} = f|_{f(V)} : V_1 \to V_1$ gibt es U_0 mit $V_1 = W_0 \oplus U_0$ mit $f(V_0) \subseteq U_0$. Sei $\tilde{U} = \{x \in V | f(x) \in U\} = f^{-1}(U_0)$. $\tilde{U}$ ist ein Unterraum von V.
Wir zeigen $V = W + \tilde{U}$. Sei $x \in V$. Dann ist $f(x) \in V_1$, also $f(x) = w + t$ mit $w \in W_0$, $t \in U_0$. Sei

$$w = \sum_{i=1}^{k-1} \lambda_i f^i(x_0) = f\left(\underbrace{\sum_{i=0}^{k-2} \lambda_{i+1} f^i(x_0)}_{=:w_1 \in W}\right)$$

Also $f(x) = f(w_1) + t$, also $t = f(x - w_1)$. Wegen $t \in U_0$ folgt $x - w_1 \in \tilde{U} = f^{-1}(U_0)$, also $x = \underbrace{w_1}_{\in W} + \underbrace{(x - w_1)}_{\in \tilde{U}} \Rightarrow V = W + \tilde{U}$.
Wir zeigen $W \cap \tilde{U} = \{0\}$. Sei $x \in W \cap \tilde{U}$. Da $x \in W \Rightarrow f(x) \in W_0$. Da $f(U_0) \subseteq U_0$ folgt aus $x \in U_0$, dass $f(x) \in U_0$, also $f(x) \in W_0 \cap U_0 = \{0\}$. Da $x \in W$ folgt

$$x = \sum_{i=0}^{k-1} \lambda_i f^i(x_0) \text{ mit } \lambda_i \in K \Rightarrow 0 = f(x) = \sum_{i=0}^{k-2} \lambda_i f^{i+1}(x_0)$$

Wegen der linearen Unabhängigkeit der $f^i(x_0)$ folgt $\lambda_0 = \lambda_1 = \ldots \lambda_{k-2} = 0 \Rightarrow x = \lambda_{k-1} f^{k-1}(x_0) \in W_0$. Also gilt wegen $x \in U_0$ auch $x = 0$, also $W \cap \tilde{U} = \{0\}$. □

Beweis der Existenz der Jordanschen Normalform. Sei nun U_1 ein Komplement zu $U_0 \oplus (W \cap \tilde{U})$ in $\tilde{U}$. Also $\tilde{U} = \underbrace{U_1 \oplus U_0}_{=:U} \oplus (W \cap \tilde{U})$. Wegen $\tilde{U} \subseteq W + U$ gilt dann $V = W + \tilde{U} = W + U$. Wegen $U \subseteq \tilde{U}$ gilt weiter $W \cap U = (W \cap \tilde{U}) \cap U = \{0\}$ und $f(U) \subseteq f(\tilde{U}) = U_0 \subseteq U$.
Sei $(u_1, ..., u_m)$ eine Basis von U, also $(f^{k-1}(x_0), \ldots, x_0, u_1, \ldots, u_m)$ eine Basis von V. Bezüglich dieser Basis hat f die Form $\begin{pmatrix} J(0,k) & 0 \\ 0 & C \end{pmatrix}$ wegen $F(U) \subseteq U$, $V = W \oplus U$. C ist ($\leq k-$stufig) nilpotent, also können wir Lemma 6.61 wiederholt anwenden und erhalten die gewünschte Darstellung. (Formal gesehen ist dieser Teil über vollständige Induktion zu beweisen.) □

7 Euklidische und unitäre Räume

Sei in diesem Kapitel $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, V ein $\mathbb{K}$-Vektorraum. Wir wollen Längen und Winkel definieren. Dazu braucht man zusätzlich Strukturen auf dem Vektorraum.

Definition 7.1. Ein Skalarprodukt (abstrakter Winkelbegriff) auf V ist eine Abbildung $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{K}$, sodass für alle $x, y, z \in V$, $\lambda \in \mathbb{K}$ gilt:

1) $\langle x, x \rangle \in \mathbb{R}$ und $\langle x, x \rangle \geq 0$

2) $\langle x, x \rangle = 0 \iff x = 0$

3) $\langle \lambda x + y, z \rangle = \lambda \langle x, z \rangle + \langle y, z \rangle$

4) $\langle x, y \rangle = \overline{\langle y, x \rangle}$

Dabei ist $\overline{a + ib} = a - ib$ für $a, b \in \mathbb{R}$, insbesondere für $\mathbb{K} = \mathbb{R}$ gilt $\langle x, y \rangle = \langle y, x \rangle$.
Für $\mathbb{K} = \mathbb{R}$ heißt V zusammen mit einem Skalarprodukt $\langle \cdot, \cdot \rangle$ ein euklidischer Raum.
Für $\mathbb{K} = \mathbb{C}$ heißt V zusammen mit einem Skalarprodukt $\langle \cdot, \cdot \rangle$ ein unitärer Raum.
$|\cdot| : \mathbb{C} \to \mathbb{C}$,
$|\lambda| := \sqrt{a^2 + b^2} = \sqrt{a^2 + b^2 - abi + abi} = \sqrt{(a + bi)(a - bi)} = \sqrt{\lambda \overline{\lambda}}$

F 7.2. *In einem euklidischen oder unitären Raum V gilt für alle $x, y, z \in V$, $\lambda \in \mathbb{K}$:*

3') $\langle x, \lambda y + z \rangle = \overline{\lambda} \langle x, y \rangle + \langle x, z \rangle$

Beweis.

$\langle x, \lambda y + z \rangle \overset{4)}{=} \overline{\langle \lambda y + z, x \rangle} \overset{3)}{=} \overline{\lambda \langle y, x \rangle + \langle z, x \rangle} = \overline{\lambda} \overline{\langle y, x \rangle} + \overline{\langle z, x \rangle} \overset{4)}{=} \overline{\lambda} \langle x, y \rangle + \langle x, z \rangle$ □

Beispiel.

1) Sei $V = \mathbb{K}^n$. Für $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ definiere $\langle x, y\rangle := \sum_{i=1}^n x_i \overline{y_i}$.
   Dies definiert ein Skalarprodukt auf $\mathbb{K}^n$ (Jeder für sich nachrechnen!). Man nennt dies das Standardskalarprodukt auf $\mathbb{R}^n$ bzw. $\mathbb{C}^n$.
   Insbesondere gilt $\mathbb{K} = \mathbb{R}$: $\langle x, y\rangle = \sum_{i=1}^n x_i y_i = x^\top y$.

2) Sei $V := \{f\colon [0,1] \to \mathbb{C} \mid f \text{ stetig}\}$ mit den Standardoperationen. Dann ist $\langle\ .\ \rangle : V \times V \to \mathbb{C}$ mit $\langle f, g\rangle := \int_0^1 f(t)\overline{g(t)}\,dt$ ein Skalarprodukt auf V.

Bemerkung. Statt $\langle x, y\rangle$ schreibt man auch oft $x \cdot y$, (x, y), $(x \mid y)$ oder $x^\top y$.

Satz 7.3 (Cauchy-Schwarz-Ungleichung)**.** *Sei $(V, \langle\cdot,\cdot\rangle)$ ein euklidischer oder unitärer Raum. Für alle $x, y \in V$ gilt dann:*

$$|\langle x, y\rangle|^2 \le \langle x, x\rangle \langle y, y\rangle$$

Ferner gilt : $|\langle x, y\rangle|^2 = \langle x, x\rangle \langle y, y\rangle \iff x, y$ linear abhängig.

Beweis. Sei o.B.d.A. $y \neq 0$ (sonst Behauptung trivial).
Setze $a := -\frac{\langle x,y\rangle}{\langle y,y\rangle}$. Dann ist

$$\begin{aligned}
0 &\overset{1)}{\le} \langle x + ay, x + ay\rangle \overset{3),3')}{=} \langle x, x\rangle + a\langle y, x\rangle + \overline{a}\langle x, y\rangle + a\overline{a}\langle y, y\rangle = \\
&= \langle x, x\rangle - \frac{\langle x, y\rangle \langle y, x\rangle}{\langle y, y\rangle} - \frac{\overline{\langle x, y\rangle}\langle x, y\rangle}{\langle y, y\rangle} + \frac{|\langle x, y\rangle|^2}{\langle y, y\rangle} = \\
&\overset{4)}{=} \frac{1}{\langle y, y\rangle}\Big(\langle x, x\rangle \langle y, y\rangle - \langle x, y\rangle \overline{\langle x, y\rangle} - \overline{\langle x, y\rangle}\langle x, y\rangle\Big) \\
&= \frac{1}{\langle y, y\rangle}\Big(\langle x, x\rangle \langle y, y\rangle - |\langle x, y\rangle|^2\Big)
\end{aligned}$$

also folgt die Ungleichung.
Mit "="genau dann, wenn $x + ay = 0$ (wegen 2)). $x + ay = x - \frac{\langle x,y\rangle}{\langle y,y\rangle} y = 0 \implies x, y$ linear abhängig.
Falls x, y linear abhängig sind, folgt "=":

$$|\langle \lambda y, y\rangle|^2 = |\lambda|^2 \left|\underbrace{\langle y, y\rangle}_{\geqslant 0}\right|^2 = \lambda\overline{\lambda}\langle y, y\rangle \langle y, y\rangle \overset{3),F7.2)}{=} \langle \lambda y, \lambda y\rangle \langle y, y\rangle .$$

□

Für unser Beispiel 2 folgt, dass für $f, g\colon [0,1] \to \mathbb{C}$ stetig gilt, dass

$$\left|\int_0^1 f(t)\overline{g(t)}\,dt\right|^2 \le \int_0^1 |f(t)|^2\,dt \int_0^1 |g(t)|^2\,dt$$

mit "="genau dann, wenn $g = 0$ oder f und g sind im $\mathbb{C}$-Vektorraum über $\{f : [0,1] \to \mathbb{C} \mid f \text{ stetig}\}$ linear unabhängig. Also es es gibt ein $a \in \mathbb{C}$ mit $f = a \cdot g$.

Definition 7.4. Eine Norm auf V ist eine Abbildung $\|\cdot\| : V \to \mathbb{R}$, sodass für alle $x, y \in V$, $\lambda \in \mathbb{K}$ gilt:

1) $\|x\| \geq 0$

2) $\|x\| = 0 \implies x = 0$

3) $\|x + y\| \leq \|x\| + \|y\|$ Dreiecksungleichung

4) $\|\lambda x\| = |\lambda| \cdot \|x\|$.

V zusammen mit einer Norm heißt ein normierter Raum.

$x = 0_V \Rightarrow \|x\| = \|0_V\| = \|0_K \cdot 0_V\| = |0_K| \cdot \|0_V\| = 0_K$

Satz 7.5. *Sei V ein euklidischer oder unitärer Raum. Dann ist durch*

$$\|x\| := \sqrt{\langle x, x\rangle} \text{ für } x \in V$$

eine Norm auf V definiert. Sie heißt die von $\langle\cdot,\cdot\rangle$ induzierte Norm.

Beweis.

1) $\|x\| \geq 0$ und reell für alle $x \in V$ definiert wegen $\langle x, x\rangle \in \mathbb{R}$ und $\langle x, x\rangle \geq 0$.
$\|x\| = 0 \overset{def}{\iff} \sqrt{\langle x, x\rangle} = 0 \iff \langle x, x\rangle = 0 \overset{2)}{\iff} x = 0$

2) $$\begin{aligned}\|x + y\|^2 = \langle x + y, x + y\rangle &= |\langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle| \\ &\leq |\langle x, x\rangle| + |\langle y, y\rangle| + 2\,|\langle x, y\rangle| \\ &\overset{7.3}{\leq} \|x\|^2 + \|y\|^2 + 2\,\|x\|\,\|y\| = (\|x\| + \|y\|)^2\end{aligned}$$

3) $\|\lambda x\| = \sqrt{\langle \lambda x, \lambda x\rangle} = \sqrt{\lambda\overline{\lambda}\,\langle x, x\rangle} = |\lambda| \cdot \|x\|$

□

7.1 Winkel in euklidischen Räumen

Motiviert elementargeometrisch in der Ebene:

Bemerkung (Kosinussatz $(x, y \neq 0)$).

$$\begin{aligned}2\,\|x\|\,\|y\|\cos\alpha &= \|x\|^2 + \|y\|^2 - \|x - y\|^2 \\ \cos\alpha &= \frac{\langle x, x\rangle + \langle y, y\rangle - \langle x - y, x - y\rangle}{2\,\|x\|\,\|y\|} = \\ &= \frac{\langle x, y\rangle + \langle y, x\rangle}{2\,\|x\|\,\|y\|} \overset{\mathbb{K}=\mathbb{R}}{=} \frac{\langle x, y\rangle}{\|x\|\,\|y\|}\end{aligned}$$

Definition 7.6. In einem euklidischen Raum definiere den Winkel zwischen zwei Vektoren x, y als α mit

$$\alpha := \arccos\left(\frac{\langle x, y\rangle}{\|x\|\,\|y\|}\right)$$

Definition 7.7. Zwei Vektoren $x, y \in V$ heißen orthogonal, falls $\langle x, y\rangle = 0$ ist.

Definition 7.8. Seien $M_1, M_2 \subseteq V$. M_1,M_2 heißen orthogonal zueinander, geschrieben $M_1 \perp M_2$, falls $\langle x, y\rangle = 0$ für alle $x \in M_1$, $y \in M_2$.
Sei $M \subseteq V$. Dann definiere

$$M^\perp := \{x \in V \mid \langle x, y\rangle = 0 \text{ für alle } y \in M\}$$

genannt das orthogonale Komplement von M.

F 7.9. *Seien $M, M_1, M_2 \subseteq V$. Dann gilt:*

a) $M^\perp = (\operatorname{Lin} M)^\perp$

b) $M^\perp$ *ist ein linearer Unterraum von* V.

c) $M_1 \subseteq M_2 \implies M_1^\perp \supseteq M_2^\perp$

d) $M^{\perp\perp} \supseteq M$

e) $M^\perp = M^{\perp\perp\perp}$

f) Seien $M_i \subseteq V$ für alle $i \in I$, $I \neq \emptyset$. Dann ist

$$\left(\bigcup_{i\in I} M_i\right)^\perp = \bigcap_{i\in I} (M_i^\perp)$$

g) Falls $\dim(\operatorname{Lin} M) < \infty$, *dann ist* $M^{\perp\perp} = \operatorname{Lin} M$.

h) Falls $\dim U < \infty$ *und* $U \subseteq V$ *linearer Unterraum, dann ist* $V = U \oplus U^\perp$.

Beweis.

a) Aus $\langle x, y_i\rangle = 0$ für $i = 1, \ldots, n$ folgt $\langle x, \sum_{i=1}^n \lambda_i y_i\rangle = 0$, wobei $\lambda_i \in \mathbb{K}$, also $M^\perp = (\operatorname{Lin} M)^\perp$.

b) Entsprechend folgt aus $\forall x_i \in M^\perp$, $(i = 1, \ldots, n)$, dass $\langle x_i, y\rangle = 0$ für $i = 1, \ldots, n$, dass $\langle \sum_{i=1}^n \lambda_i x_i, y\rangle = 0$ (mit $\lambda_i \in \mathbb{K}$). $0 \in M^\perp$, weil $\langle 0, y\rangle = 0$, für alle $y \in M$.

c) klar

d) , f), g), h) Hausaufgabe

e) folgt aus c) und d), da $M \subseteq M^{\perp\perp} \overset{c)}{\Longrightarrow} M^{\perp}2 \supseteq (M^{\perp\perp})^{\perp}$ und $(M^{\perp})^{\perp\perp} \overset{d)}{\supseteq} M^{\perp}$

□

Definition 7.10. $x \in V$ heißt normiert, falls $\|x\| = 1$. $x \neq 0$ kann man normieren: $\frac{x}{\|x\|}$.
$\left\| \frac{x}{\|x\|} \right\| \overset{7.4.3)}{=} \left| \frac{1}{\|x\|} \right| \|x\| = \frac{1}{\|x\|}\|x\| = 1$

Definition 7.11. $m \subseteq V$ (mit $m \neq \emptyset$) heißt ein Orthogonalsystem, falls $0 \notin m$ und für alle $x, y \in m$ mit $x \neq y$ gilt $\langle x, y\rangle = 0$.
$m \subseteq V$ (mit $m \neq \emptyset$) heißt ein Orthonormalsystem, falls für alle $x \in m$ gilt $\|x\| = 1$ und für alle $x, y \in m$ mit $x \neq y$ gilt $\langle x, y\rangle = 0$ (Abkürzung ON-System).
Eine Orthonormalbasis (Abkürzung ON-Basis) von V ist eine Basis von V, die ein Orthonormalsystem ist.

F 7.12. *Jedes Orthogonalsystem ist linear unabhängig.*

Beweis. Sei m ein Orthogonalsystem und $x_1, \ldots, x_n \in m$ paarweise verschieden. Gelte $\sum_{i=1}^{n} \lambda_i x_i = 0$, $\lambda_i \in \mathbb{K}$. Für jedes $k \in \{1, \ldots, n\}$ folgt

$$0 = 0 \cdot \langle 0, x_k\rangle \overset{7.4.3)}{=} \langle 0 \cdot 0, x_k\rangle = \left\langle \sum_{i=1}^{n} \lambda_i x_i, x_k \right\rangle = \sum_{i=1}^{n} \lambda_i \langle x_i, x_k\rangle = \lambda_k \langle x_k, x_k\rangle .$$

Wegen $x_k \neq 0$ ist $\langle x_k, x_k\rangle > 0$, also $\lambda_k = 0$. Dies gilt für jedes $k \in \{1, \ldots, n\}$, also ist m linear unabhängig. □

Bemerkung. Falls $e_1, \ldots, e_n \in V$ ein Orthonormalsystem ist ($e_i \neq e_j$ für $i \neq j$), dann gilt $\langle e_i, e_j\rangle = \delta_{ij} := \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$
δ_{ij} nennt man Kroneckersymbol.

Beweis. $\langle e_i, e_i\rangle = \left\langle \frac{e_i}{\|e_i\|}, \frac{e_i}{\|e_i\|} \right\rangle = \left\langle \frac{e_i}{\sqrt{\langle e_i, e_i\rangle}}, \frac{e_i}{\sqrt{\langle e_i, e_i\rangle}} \right\rangle = \frac{1}{\sqrt{\langle e_i, e_i\rangle}^2} \langle e_i, e_i\rangle$ □

F 7.13. *Sei $(e_1, \ldots, e_n)$ eine ON-Basis von V. Seien $x, y \in V$. Dann gilt $x = \sum_{i=1}^{n} \langle x, e_i\rangle e_i$, d.h. die i-te Koordinate von x bzgl. der Basis $(e_1, \ldots, e_n)$ ist $\langle x, e_i\rangle$.*
Ferner gilt für $x_i := p_i(x) = \langle x, e_i\rangle$, $y_i := \langle y, e_i\rangle$, dass $\langle x, y\rangle = \sum_{i=1}^{n} x_i \overline{y_i} =$

1.

Beweis. Sei $x = \sum_{i=1}^{n} \lambda_i e_i$. Dann ist

$$\langle x, e_i \rangle = \left\langle \sum_{j=1}^{n} \lambda_j e_j, e_i \right\rangle = \sum_{i=1}^{n} \lambda_j \underbrace{\langle e_j, e_i \rangle}_{=\delta_{ji}} = \lambda_i$$

$$\langle x, y \rangle = \left\langle \sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j \right\rangle = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i \overline{y_j} \underbrace{\langle e_j, e_i \rangle}_{=\delta_{ji}} = \sum_{i=1}^{n} x_i \overline{y_i}$$

□

Satz 7.14 (Orthonormalisierungsverfahren nach E. Schmidt)**.** *Sei* $(x_1, x_2, \dots)$ *ein endliches oder abzählbar unendliches System linear unabhängiger Vektoren aus* V*. Dann gibt es genau ein ON-System* $(e_1, e_2, \dots)$ *mit folgenden Eigenschaften:*

1) $\mathrm{Lin}\{e_1, \dots, e_k\} = \mathrm{Lin}\{x_1, \dots, x_k\}$ *für alle* $k = 1, 2, \dots$

2) $\langle x_k, e_k \rangle \in \mathbb{R}^+ = (0, \infty)$

Beweis. Die $e_1, e_2, \dots$ werden rekursiv definiert und 1), 2) und Eindeutigkeit induktiv gezeigt. Bei einem endlichen System $(x_1, \dots, x_n)$ bricht das Verfahren nach n Schritten ab.
$x_1 \neq 0$ (wegen $(x_1, x_2, \dots)$ linear unabhängig), also ist $e_1 := \frac{x_1}{\|x_1\|}$ normiert, $\mathrm{Lin}\{e_1\} = \mathrm{Lin}\{x_1\}$, und $\langle x_1, e_1 \rangle = \left\langle x_1, \frac{1}{\|x_1\|} x_1 \right\rangle = \frac{1}{\|x_1\|} \langle x_1, x_1 \rangle = \frac{1}{\sqrt{\langle x_1, x_1 \rangle}} \sqrt{\langle x_1, x_1 \rangle}^2 = \sqrt{\langle x_1, x_1 \rangle} = \|x_1\| > 0$ (reell!).
Eindeutigkeit: Aus $e_1' = c x_1$ mit $c > 0$ und $\|e_1'\| = 1$ folgt

$$1 = \langle e_1', e_1' \rangle = c\bar{c} \langle x_1, x_1 \rangle = |c|^2 \|x_1\|^2, \text{also } c = |c| = \frac{1}{\|x_1\|}.$$

Also $e_1' = e_1$.
Setze $b_{k+1} := x_{k+1} - \sum_{i=1}^{k} \langle x_{k+1}, e_i \rangle e_i$.

Dann gilt $\mathrm{Lin}\{e_1,\dots,e_k,b_{k+1}\} = \mathrm{Lin}\{x_1,\dots,x_k,x_{k+1}\}$ Ferner ist für $1 \le j \le k$

$$\begin{aligned}
\langle b_{k+1}, e_j\rangle &= \left\langle x_{k+1} - \sum_{i=1}^{k} \langle x_{k+1}, e_i\rangle\, e_i, e_j \right\rangle \\
&= \langle x_{k+1}, e_j\rangle - \left\langle \sum_{i=1}^{k} \underbrace{\langle x_{k+1}, e_i\rangle}_{\text{Skalar}} e_i, e_j \right\rangle \\
&= \langle x_{k+1}, e_j\rangle - \sum_{i=1}^{k} \langle x_{k+1}, e_i\rangle \underbrace{\langle e_i, e_j\rangle}_{\delta_{ij},\ \text{mit IA}} \\
&= \langle x_{k+1}, e_j\rangle - \langle x_{k+1}, e_j\rangle \\
&= 0 \\
&= \overline{0} \\
&= \langle b_{k+1}, e_j\rangle
\end{aligned}$$

$b_{k+1} \neq 0$, da $(x_1,\dots,x_{k+1})$ nach Voraussetzung linear unabhängig ist. Setze $e_{k+1} := \frac{b_{k+1}}{\|b_{k+1}\|}$. Es gilt

$$\|b_{k+1}\|^2 = \langle b_{k+1}, b_{k+1}\rangle = \langle x_{k+1}, b_{k+1}\rangle > 0 \text{ wegen } \langle e_i, b_{k+1}\rangle = 0 \text{ für } k = 1,\dots,n$$

Also

$$\langle x_{k+1}, e_{k+1}\rangle = \left\langle x_{k+1}, \frac{1}{\|b_{k+1}\|} b_{k+1} \right\rangle = \frac{1}{\|b_{k+1}\|} \langle x_{k+1}, b_{k+1}\rangle > 0$$

Damit ist $(e_1,\dots,e_k,e_{k+1})$ ein ON-System mit den Eigenschaften 1), 2).
Eindeutigkeit: Angenommen $(e_1,\dots,e_k,e'_{k+1})$ erfüllen 1) und 2), dann ist

$$\begin{aligned}
e_{k+1} &= \sum_{i=1}^{k} \lambda_i c e_i + c x_{k+1} \text{ mit gewissen } \lambda_i \in \mathbb{K},\ c > 0\ (\in \mathbb{R}). \\
&= c(x_{k+1} + \sum_{i=1}^{k} \lambda_i e_i)
\end{aligned}$$

wegen $\mathrm{Lin}\{e_1,\dots,e_k,e'_{k+1}\} = \mathrm{Lin}\{x_1,\dots,x_k,x_{k+1}\} = \mathrm{Lin}\{e_1,\dots,e_k,x_{k+1}\}$
Für $i = 1,\dots,k$ erhält man

$$0 = \left\langle e'_{k+1}, e_i\right\rangle = \lambda_i c + c\left\langle x_{k+1}, e_i\right\rangle, \text{ also } \lambda_i = -\left\langle x_{k+1}, e_i\right\rangle.$$

Damit ist $e'_{k+1} = c b_{k+1}$. Wegen $c > 0$ und $\left\|e'_{k+1}\right\| = 1$ folgt $c = \frac{1}{\|b_{k+1}\|}$, also $e'_{k+1} = e_{k+1}$. □

Bemerkung (zum ON-Verfahren von E. Schmidt). Bei der Berechnung von Hand ist es günstiger zunächst nur die b_i $(i = 1, 2, \dots)$ zu bestimmen:

$$b_1 := x_1,\ b_{k+1} := x_{k+1} - \sum_{i=1}^{k} \frac{\langle x_{k+1}, b_i\rangle}{\|b_i\|^2} b_i$$

Zum Schluss $e_k := \frac{b_k}{\|b_k\|}$ $(k = 1, 2, \dots)$. Beachte

$$\langle x_{k+1}, e_i \rangle e_i = \left\langle x_{k+1}, \frac{b_i}{\|b_i\|} \right\rangle \frac{b_i}{\|b_i\|} = \frac{\langle x_{k+1}, b_i \rangle}{\|b_i\|^2} b_i$$

F 7.15 (Folgerung)**.** *Sei* $\dim V = n < \infty$*. Dann kann jede ON-Basis eines Linearen Unterraums* $U \subseteq V$ *zu einer ON-Basis von* V *ergänzt werden, insbesondere hat* V *eine ON-Basis.*

Beweis. Sei $(b_1, \dots, b_k)$ eine ON-Basis von U. Dann kann diese zu einer Basis $(b_1, \dots, b_k, x_{k+1}, \dots, x_n)$ von V ergänzt werden. Anwendung des Schmidtschen Orthonormalisierungsverfahrens (Satz 7.14) bewahrt die $b_1, \dots, b_k$, $(e_i = b_i)$ und man erhält eine ON-Basis $(b_1, \dots, b_k, e_{k+1}, \dots, e_n)$. Für $U = 0$ wähle eine Basis $(x_1, \dots, x_n)$ von V. Wende Satz 7.14 darauf an. □

Frage: Wann wird eine Norm von einem Skalarprodukt induziert?
Antwort für $\mathbb{K} = \mathbb{R}$.

Satz 7.16. *Sei* V *ein normierter* $\mathbb{R}$*-Vektorraum. Dann gibt es ein Skalarprodukt* $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ *auf* V *mit* $\langle x, x \rangle = \|x\|^2$ *für alle* $x \in V$*, wenn die Parallelogrammgleichung gilt:*

$$\|x - y\|^2 + \|x + y\|^2 = 2(\|x\|^2 + \|y\|^2) \text{ für alle } x, y \in V. \qquad \text{(P)}$$

Ferner gilt: Falls die Norm von einem Skalarprodukt induziert wird, dann ist das Skalarprodukt durch die Norm eindeutig bestimmt.

Beweis. " $\Longrightarrow$ ":

$$\langle x - y, x - y \rangle + \langle x + y, x + y \rangle = 2\langle x, x \rangle + 2\langle y, y \rangle = 2(\|x\|^2 + \|y\|^2)$$

" $\Longleftarrow$ ": Eindeutigkeit: $\langle x + y, x + y \rangle - \langle x, x \rangle - \langle y, y \rangle = 2\langle x, y \rangle$, also $\langle x, y \rangle = \frac{1}{2}(\|x + y\|^2 - \|x\|^2 - \|y\|^2)$. Zur Existenz definiere $\langle x, y \rangle := \frac{1}{2}(\|x + y\|^2 - \|x\|^2 - \|y\|^2)$. Dann gilt offensichtlich: $\langle x, y \rangle = \langle y, x \rangle$, $\langle x, x \rangle = \|x\|^2 \geq 0$ und $\langle x, x \rangle = 0 \iff x = 0$. Verträglichkeit mit $+$:

$$2(\langle x + y, z \rangle - \langle x, z \rangle - \langle y, z \rangle) \overset{\text{nachrechnen}}{\underset{\dots}{=}} \overset{(P)}{=} 0$$

Verträglichkeit mit Skalarmultiplikation wird erst mit Additivität induktiv für $\lambda \in \mathbb{Z}$ gezeigt, dann für $\lambda \in \mathbb{Q}$ und über Stetigkeit für $\lambda \in \mathbb{R}$. Der Rest des Beweises wird weggelassen. □

7.2 Orthogonale und unitäre Abbildungen

Definition 7.17. Eine lineare Abbildung $f : V \to W$ zwischen euklidischen bzw. unitären Vektorräumen heißt eine orthogonale bzw. unitäre

Abbildung, falls gilt

$$\langle f(x), f(y)\rangle = \langle x, y\rangle \text{ für alle } x, y \in V$$

F 7.18. *Sei $f\colon V \to W$ eine lineare Abbildung zwischen euklidischen bzw. unitären Vektorraumäumen. Dann sind folgende Aussagen äquivalent:*

i) f *ist eine orthogonale bzw. unitäre Abbildung*

ii) $\forall x \in V : \|x\| = \|f(x)\|$

iii) $\forall x \in V : \|x\| = 1 \implies \|f(x)\| = 1$

iv) für jedes ON-System $(e_1, \dots, e_n)$ *in* V *ist* $(f(e_1), \dots, f(e_n))$ *ein ON-System in* W*.*

Ferner gilt: Falls $\dim V < \infty$*, dann ist jede der Aussagen (i)-(iv) äquivalent zu*

v) Es gibt eine ON-Basis von V*, die auf ein ON-System in* W *abgebildet wird.*

Beweis.

i) $\implies$ ii): $\|x\| = \sqrt{\langle x, x\rangle} = \sqrt{\langle f(x), f(x)\rangle} = \|f(x)\|$

ii) $\implies$ iii): klar

iii) $\implies$ ii): o.B.d.A. $x \neq 0$. Mit $e = \frac{1}{\|x\|}x$ gilt

$$x = \|x\|\, e \text{ und } \|e\| = 1 \implies \|f(x)\| = \|x\|\, \|f(e)\| = \|x\|$$

ii $\implies$ iv): Sei $(e_1, \dots, e_n)$ ein ON-System in V. Für $j \neq k$ gilt

$$\begin{aligned} 2\operatorname{Re}\langle f(e_j), f(e_k)\rangle &\overset{*}{=} \|f(e_j) + f(e_k)\|^2 - \|f(e_j)\|^2 - \|f(e_k)\|^2 \\ &= \|e_j + e_k\|^2 - \|e_j\|^2 - \|e_k\|^2 \\ &= 2\operatorname{Re}\langle e_j, e_k\rangle = 0 \end{aligned}$$

$*$ wegen

$$\begin{aligned} \|x + y\|^2 &= \langle x + y, x + y\rangle \\ &= \langle x, x\rangle + \langle y, y\rangle + \overbrace{\langle x, y\rangle + \langle y, x\rangle}^{z+\overline{z}=2\operatorname{Re} z} \\ &= \|x\|^2 + \|y\|^2 + 2\operatorname{Re}\langle x, y\rangle \end{aligned}$$

Falls $\mathbb{K} = \mathbb{C}$: $\operatorname{Im}\langle f(e_j), f(e_k)\rangle = -\operatorname{Re}\langle f(ie_j), f(e_k)\rangle = 0$

Also $\langle f(e_j), f(e_k)\rangle = 0$ für $j \neq k$. $\|f(e_i)\| = 1$ nach Voraussetzung iii, d.h. $(f(e_1), \dots, f(e_n))$ ist ein ON-System in W.

iv $\implies$ i: zu zeigen $\langle f(x), f(y)\rangle = \langle x, y\rangle$ für alle $x, y \in V$. Sei o.B.d.A. $x \neq 0$.

1. Fall: (x, y) ist linear unabhängig. Dann gibt es nach Satz 7.14 eine ON-Basis (e_1, e_2) von $\mathrm{Lin}\{x, y\}$. Sei $x = x_1e_1 + x_2e_2$, $y = y_1e_1 + y_2e_2$. Dann ist $\langle f(x), f(y)\rangle = \langle x_1f(e_1) + x_2f(e_2), y_1f(e_1) + y_2f(e_2)\rangle = x_1\overline{y_1} + x_2\overline{y_2}$, da $\langle f(e_i), f(e_j)\rangle = \delta_{ij}$.
2. Fall: x,y linear abhängig, o.B.d.A. $x \neq 0$, $x = x_1e_1$, $y = y_1e_1$ mit $e_1 = \frac{1}{\|x\|}x$. Weiter wie im 1. Fall.

Sei nun $\dim V < \infty$

iv $\Longrightarrow$ **v:** Nach Folgerung 7.15 gibt es eine ON-Basis von V. Eine solche wird nach iv) auf ein ON-System in W abgebildet.

v) $\Longrightarrow$ **i):** Sei $(e_1, \ldots, e_n)$ eine ON-Basis von V mit $(f(e_1), \ldots, f(e_n))$ ON-System in W. Seien $x, y \in V$. Dann ist nach Fakt 7.13:

$$x = \sum_{i=1}^{n} x_ie_i \text{ mit } x_i = \langle x, e_i\rangle,$$

$$y = \sum_{i=1}^{n} y_ie_i \text{ mit } y_i = \langle y, e_i\rangle,$$

$$\langle f(x), f(y)\rangle = \left\langle \sum_{i=1}^{n} x_if(e_i) \sum_{i=1}^{n} y_if(e_i) \right\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i\overline{y_j}\delta_{ij} = \langle x, y\rangle \,\square$$

Definition 7.19. Sei $A \in \mathbb{C}_{m,n}$. Dann bezeichne $A^* := \left(\overline{A}\right)^\top = \overline{(A^\top)}$ als adjungierte Matrix, wobei $\overline{A}$ die konjugiert komplexe Matrix bezeichnet.

Es gilt offensichtlich:

F 7.20. $\overline{AB} = \overline{A} \cdot \overline{B}$, *also* $(AB)^* = B^*A^*$. *Falls* A *invertierbar ist, folgt (wegen* $E = \overline{E} = E^*$*):*

$$\overline{A}^{-1} = \overline{A^{-1}}, \text{ also } (A^*)^{-1} = \left(A^{-1}\right)^*$$

Für $A \in \mathbb{C}^{n,n}$ *gilt* $\det \overline{A} = \overline{\det A}$*, also wegen* $\det A^\top = \det A$ *folgt* $\det A^* = \overline{\det A}$.

Definition 7.21. $A \in \mathbb{C}^{n,n}$ heißt unitär, falls A regulär und $A^* = A^{-1}$ gilt. Eine reelle unitäre Matrix $A \in \mathbb{R}^{n,n}$ heißt auch orthogonal. $A \in \mathbb{R}^{n,n}$ ist also orthogonal genau dann, wenn $A^\top = A^{-1}$.

Bemerkung. Da für $A, B \in \mathbb{K}^{n,n}$ die Aussagen 1) $AB = E$, 2) $BA = E$, und 3) A regulär und $B = A^{-1}$ äquivalent sind, folgt, dass die Aussagen $AA^* = E$, $A^*A = E$, und A unitär zueinander äquivalent sind (für $A \in \mathbb{C}^{n,n}$) und auch, dass $AA^\top = E$, $A^\top A = E$, und A ist orthogonal zueinander äquivalent sind (für $A \in \mathbb{R}^{n,n}$).

F 7.22. *Für eine Matrix $A \in \mathbb{K}^{n,n}$ sind äquivalent:*

i) A ist orthogonal bzw. unitär.

ii) Die Spaltenvektoren von A bilden eine ON-Basis des $\mathbb{K}^n$.

iii) Die Zeilenvektoren von A bilden eine ON-Basis des $\mathbb{K}^n$.

iv) Die lineare Abbildung $A\colon \mathbb{K}^n \to \mathbb{K}^n$ ist orthogonal bzw. unitär.

Dabei ist mit $\mathbb{K}^n$ jeweils der euklidische bzw unitäre Raum mit dem Standardskalarprodukt gemeint (und Standardbasis).

Beweis. (ii) ist äquivalent zu $A^*A = E$, denn $(a_1, \ldots, a_n)^*(a_1, \ldots, a_n) = (\overline{\langle a_i, a_j \rangle})_{i,j}$, also (i) $\iff$ (ii). Entsprechend ist (iii) äquivalent zu $A^*A = E$, also (i) $\iff$ (iii).
(ii) $\iff$ (iv): Die Spaltenvektoren von A sind die Bilder der Standardbasisvektoren von $\mathbb{K}^n$. Diese ist eine ON-Basis, also folgt die Behauptung aus (v) $\iff$ (i) in Fakt 7.18. □

F 7.23. *Wenn A unitär (oder orthogonal) ist, dann ist $|\det A| = 1$.*

Beweis.

$$A^*A = E \implies 1 = \det AA^* = \det A \det A^* = \det A \overline{\det A} = (\det A)^2$$

□

F 7.24. *Wenn A unitär (oder orthogonal) ist und λ ein Eigenwert von A, dann ist $|\lambda| = 1$.*

Beweis. Sei x Eigenvektor von A zum Eigenwert λ, d.h. $Ax = \lambda x$ mit $x \neq 0$. Dann ist $\langle x, x \rangle = \langle Ax, Ax \rangle = \langle \lambda x, \lambda x \rangle = \lambda\overline{\lambda} \langle x, x \rangle = |\lambda|^2 \langle x, x \rangle$, also wegen $\langle x, x \rangle \neq 0$ folgt $|\lambda| = 1$. □

Definition 7.25.

$U(n) := \{A \in \mathbb{C}^{n,n} \mid A \text{ unitär}\}$ heißt die unitäre Gruppe
$SU(n) := \{A \in U(n) \mid \det A = 1\}$ heißt die spezielle unitäre Gruppe
$O(n) := \{A \in \mathbb{R}^{n,n} \mid A \text{ orthogonal}\}$ heißt die orthogonale Gruppe
$SO(n) := \{A \in O(n) \mid \det A = 1\}$ heißt die spezielle orthogonale Gruppe

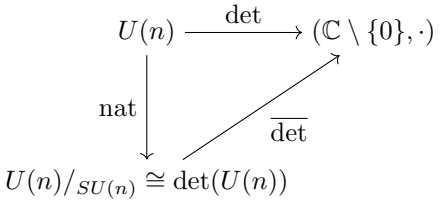
F 7.26. *$U(n)$, $SU(n)$ sind Untergruppen von $GL(n,\mathbb{C})$*
$O(n)$, $SO(n)$ sind Untergruppen von $GL(n,\mathbb{R})$
($GL(n,\mathbb{K})$ ist die Gruppe der invertierbaren Matrizen in $\mathbb{K}^{n,n}$)
$SU(n)$ ist ein Normalteiler von $U(n)$;
$SO(n)$ ist ein Normalteiler von $O(n)$.

Beweis. $U(n)$ bzw. $O(n)$ sind Untergruppen von $GL(n,\mathbb{C})$ bzw. $GL(n,\mathbb{R})$:

$$A^* = A^{-1}, B^* = B^{-1} \implies (AB)^* = B^*A^* = B^{-1}A^{-1} = (AB)^{-1}$$
$$\left(A^{-1}\right)^* = (A^*)^{-1} = \left(A^{-1}\right)^{-1}$$
$$E^* = E = E^{-1}$$

$SU(n) = \ker(\det)$, wobei $\det\colon GL(n,\mathbb{C}) \to (\mathbb{C}\setminus\{0\})$ die Determinantenfunktion ist. det ist ein Gruppenhomomorphismus, denn $\det AB = \det A \det B$, also ist $SU(n)$ ein Normalteiler von $U(n)$.
$SO(n) \subseteq O(n)$ Normalteiler genauso. □

Bemerkung (Aufgabe). Bestimme $U(n)/_{SU(n)}$. Idee: Verwende den Homomorphisatz der Gruppentheorie:



$\overline{\det}$ ist ein injektiver Gruppenhomomorphismus. $SU(n) = \ker(\det)$
Für $n \geq 1$ gilt: $\det(U(n)) = \{z \in \mathbb{C} \mid |z| = 1\}$

$$\det \underbrace{\begin{pmatrix} z & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}}_{\in U(n) \text{ für } |z|=1} = z$$

$O(n)/_{SO(n)} \cong (\{-1,1\},\cdot) \cong \mathbb{Z}_2$

Satz 7.27 (Matrixtheoretische Formulierung von Satz 7.14 (ON-Verfahren nach E. Schmidt))**.** *Sei $A \in \mathbb{K}^{n,n}$ regulär. Dann gibt es eindeutig bestimmte Matrizen S und C, sodass $A = SC$ ist und S unitär ($\mathbb{K} = \mathbb{C}$) bzw. S orthogonal ($\mathbb{K} = \mathbb{R}$) ist und C eine obere Dreiecksmatrix mit positiven (reellen) Elementen auf der Diagonale (d.h. $c_{ii} > 0$ für $i = 1,\ldots,n$).*

Beweis. Wende das ON-Verfahren von E. Schmidt auf die Basis $A = (a_1,\ldots,a_n)$ von $\mathbb{C}^{n,n}$ (bzw. $\mathbb{R}^{n,n}$) an. Dann erhält man eine ON-Basis $S = (e_1,\ldots,e_n)$ und $e_k = \sum_{i=1}^{k} c_{ik}a_k$ mit $c_{kk} > 0$ und $c_{ij} = 0$ für $i > j$. Also $S = AC$, also

$A = SC^{-1}$. Wenn C eine obere Dreiecksmatrix ist mit $c_{ii} > 0 \ \forall i = 1, \ldots, n$, dann ist C^{-1} auch eine obere Dreiecksmatrix mit positiven Elementen auf der Hauptdiagonalen. Eindeutigkeit folgt aus der Eindeutigkeitsaussage im ON-Verfahren. □

F 7.28. *Eine reguläre obere Dreiecksmatrix C lässt sich eindeutig schreiben sowohl als $C = ND$, als auch als $C = D\tilde{N}$, wobei N bzw. $\tilde{N}$ obere Dreiecksmatrizen sind mit $n_{ii} = 1$ für $i = 1, \ldots, n$ und D eine Diagonalmatrix. Ferner ist dann* $D = \begin{pmatrix} c_{11} & & 0 \\ & \ddots & \\ 0 & & c_{nn} \end{pmatrix}$.

Beweis. einfache Übung □

Satz 7.29 (Iwasawa-Zerlegung)**.** *Jede reguläre Matrix $A \in \mathbb{K}^{n,n}$ lässt sich eindeutig darstellen als $A = ND_+S$, wobei N eine obere Dreiecksmatrix mit 1en auf der Diagonale, D_+ eine Diagonalmatrix mit $d_{ii} > 0$ für $i = 1, \ldots, n$ und S eine unitäre bzw. orthogonale Matrix ist.*

Beweis. Wende Satz 7.27 auf A^{-1} an. Man erhält $S = A^{-1}C$, also $A = CS^{-1} = CS^*$ mit S unitäre bzw. orthogonale Matrix und C obere Dreiecksmatrix mit $c_{ii} > 0$, schließlich mit Fakt 7.28 $A = ND_+S^*$ (S unitär $\implies S^* = S^{-1}$ unitär). □

Bemerkung. Analog erhält man Zerlegungen der Form D_+NS, SND_+, SD_+N mit Matrizen S, D_+, N mit den Eigenschaften wie in Satz 7.29.

Definition 7.30 (und Feststellung)**.** Sei $U \subseteq V$ ein linearer Unterraum. Gelte $V = U \oplus U^\perp$. Dann gibt es genau eine lineare Abbildung

$$p_U : V \to V \text{ mit } p_U(x) = x \qquad \forall x \in U$$
$$p_U(x) = 0 \qquad \forall x \in U^\perp$$

Sie heißt orthogonale Projektion auf U. Ferner gilt dann $p_U + p_{U^\perp} = \mathrm{id}_V$.

Beweis. Eindeutigkeit ist klar, da nach Vorraussetzung $V = U + U^\perp$ ($= \mathrm{Lin}(U \cup U^\perp)$) und p_U auf $U \cup U^\perp$ gegeben ist.
Existenz: Wegen $V = U + U^\perp$ und $U \cap U^\perp = 0$ lässt sich jedes x eindeutig schreiben als $x = f(x) + g(x)$ mit $f(x) \in U$, $g(x) \in U^\perp$, f, g lineare Abbildungen (einfaches nachrechnen). □

Sei im Kapitel 7 im weiteren $U \subseteq V$ ein linearer Unterraum mit $V = U + U^\perp$ (also $V = U \oplus U^\perp$)

F 7.31. *Für alle $x \in V$ und alle $u \in U$ sind folgende Aussagen äquivalent:*

i) $u = p_U(x)$

ii) $x - u \in U^\perp$

iii) Für alle $w \in U$ *gilt* $\|x - u\| \leq \|x - w\|$

Beweis.

(i) $\Longrightarrow$ (ii): $x = p_U(x) + p_{U^\perp}(x) = u + p_{U^\perp}(x)$, also $x - u = p_{U^\perp}(x) \in U^\perp$

(ii) $\Longrightarrow$ (i): $p_U(x) = p_U(u + (x-u)) = \underbrace{p_U(u)}_{\in U} + \underbrace{p_U(x-u)}_{\in U^\perp}$

(ii) $\Longrightarrow$ (iii):

$$\begin{aligned}\|x-w\|^2 &= \langle (x-u)+(u-w), (x-u)+(u-w)\rangle \\ &= \|x-u\|^2 + \|u-w\|^2 + 2\,\mathrm{Re}\left\langle \underbrace{x-u}_{\in U^\perp}, \underbrace{u-w}_{\in U}\right\rangle \\ &= \|x-u\|^2 + \|u-w\|^2 \geq \|x-u\|^2\end{aligned}$$

(iii) $\Longrightarrow$ (ii): Wir zeigen $\neg(ii) \implies \neg(iii)$. Aus $\neg(ii)$ folgt, dass es $v \in U$ mit $\langle x-u, v\rangle = \lambda \neq 0$, o.B.d.A. $\|v\| = 1$, gibt. Sei $w = u + \lambda v$. Dann ist $w \in U$ und

$$\begin{aligned}\|x-w\|^2 &= \langle (x-u) - \lambda v, (x-u) - \lambda v\rangle \\ &= \|x-u\|^2 + |\lambda|^2 \|v\|^2 - \lambda \underbrace{\langle v, x-u\rangle}_{=\overline{\lambda}} - \overline{\lambda} \underbrace{\langle x-u, v\rangle}_{=\lambda} \\ &= \|x-u\|^2 - |\lambda|^2 \\ &< \|x-u\|^2\end{aligned}$$

also $\neg(iii)$.

□

F 7.32. *Wenn $(b_1, \ldots, b_m)$ eine ON-Basis von U ist, dann gilt für alle $x \in V$: $p_U(x) = \sum_{i=1}^m \langle x, b_i\rangle\, b_i$.*

Beweis. $\sum_{i=1}^m \langle x, b_i\rangle\, b_i \in U$. Wir zeigen $x - \sum_{i=1}^m \langle x, b_i\rangle\, b_i \in U^\perp$.
Für $j = 1, \ldots, m$ gilt $\langle x - \sum_{i=1}^m \langle x, b_i\rangle\, b_i, b_j\rangle = \langle x, b_j\rangle - \langle x, b_j\rangle = 0$
also $|x - \sum_{i=1}^m \langle x, b_i\rangle\, b_i| \in \{b_1, \ldots, b_m\}^\perp = U^\perp$ □

7.3 Spiegelungen

Definition 7.33 (und Fakt)**.** Sei $U \subseteq V$ linearer Unterraum mit $U + U^\perp = V$. Dann gibt es genau ein lineare Abbildung

$$s_U \colon V \to V \text{ mit } s_U(x) = x \ \forall x \in U$$
$$s_U(x) = -x \ \forall x \in U^\perp$$

Sie heißt Spiegelung von U. Ferner gilt: $s_U = p_U - p_{U^\perp} = 2p_U - \mathrm{id}_V$.

Beweis. Die lineare Abbildung $\beta_U := 2p_U - \mathrm{id}_V$ erfüllt

$$\beta(x) = \begin{cases} x & \text{für } x \in U \\ -x & \text{für } x \in U^\perp \end{cases}$$

Damit ist die Existenz gezeigt. Die Eindeutigkeit folgt aus $U + U^\perp = V$. □

F 7.34. *Sei* $\dim V = n$, $U \subseteq V$ *ein linearer Unterraum,* B *eine beliebige Basis von* V *mit* $\mathrm{Lin}\{b_1, \ldots, b_m\} = U$, $\mathrm{Lin}\{b_{m+1}, \ldots, b_n\} = U^\perp$. *Dann ist*

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ 0 & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$ *die Matrix von* p_U *bzgl. der Basis* B *und*

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ 0 & & & & \ddots \\ & & & & & -1 \end{pmatrix}$$ *die Matrix von* s_U *bzgl. der Basis* B*;*

8 Affine Unterräume und analytische Geometrie

Sei V ein K-Vektorraum.

Definition 8.1. $U \subseteq V$ heißt ein affiner Unterraum von V, falls $U = \emptyset$ oder es einen linearen Unterraum X_U von V und ein $a \in V$ gibt mit $U = a + X_U = \{a + x \mid x \in X_U\}$.

Beispiel.

1. Die Menge der Lösungen eines linearen Gleichungssystems ist ein affiner Unterraum: $\{x \mid Ax = b\}$.
2. Seien $x, y \in V$. Dann ist $x + \mathrm{Lin}\, x - y =: x + K(x - y)$ ein affiner Unterraum, genannt Verbindungsgerade von x und y.
3. (verallgemeintertes 1.). Sei $f \colon V \to W$ linear (V, W K-Vektorräume),

$b \in W$. Dann ist $f^{-1}(\{b\}) = \{x \in V \mid f(x) = b\}$ ein affiner Unterraum von V.

Beweis. Fall 1: $\{x \in V \mid f(x) = b\} = \emptyset$

Fall 2: Es gibt $x_0 \in V$ mit $f(x_0) = b$. Dann ist $\{x \in V \mid f(x) = b\} = x + \ker f$ □

F 8.2. *Sei $U \subseteq V$. Dann sind äquivalent*

1. *U ist ein affiner Unterraum.*
2. *Für alle $x \in U$ ist $U - x$ ein linearer Unterraum.*
3. *$U = \emptyset$ oder es gibt $x \in U$ mit $U - x$ ist ein linearer Unterraum.*

F 8.3. *Sei m eine Menge von affinen Unterräumen von V. Dann ist $\bigcap m$ ein affinier Unterraum.*

Beweis. Falls $\bigcap m = \emptyset$ klar. Sonst sei $a \in \bigcap m$. Dann ist $(\bigcap m) - a = \bigcap\{ \underbrace{U - a}_{X_U \text{lin. UR}} \mid U \in m\}$ ist ein linearer Unterraum, also ist $\bigcap m$ ein affiner Unterraum. □

Definition 8.4. Sei $M \subseteq V$ eine Teilmenge. Dann heißt $\operatorname{aff} M = \bigcap\{U \mid M \subseteq U, U \text{ affiner UR von V}\}$ die affine Hülle von M (der der von M aufgespannte affine Unterraum).
Das heißt, $\operatorname{aff} M$ ist der kleinste affine Unterraum, der M enthält.

Beispiel. $\operatorname{aff} \emptyset = \emptyset$, $\operatorname{aff}\{x\} = \{x\}$ und $\operatorname{aff}\{x, y\} = x + K(y - x)$ für $x \neq y$.

Von Studenten für Studenten. Wann wackelt ein Tische mit vier Beinen garantiert nicht?
Wenn er auf einem drei-dimensionalen Raum in vierdimensionalen Raum steht. Ein drei-beiniger Tische, der auf einer Geraden steht, wackelt hingegen im Allgemeinen.
Der vier-beinige Tische im fünf-dimensionalen Raum fällt dagegen um.

Definition 8.5. Sei $M \subseteq V$. Eine Linearkombination $\sum_{i=1}^{n} \lambda_i x_i$ mit $\lambda_i \in K$, $x_i \in M$ von Vektoren aus M heißt eine Affinkombination, falls $\sum i = 1^n \lambda_i = 1$.

F 8.6. *Sei $M \subseteq V$, $M \neq \emptyset$, $x_0 \in M$. Dann gilt*

$$\operatorname{aff} M = x_0 + \operatorname{Lin}(M - x_0) = \left\{ \sum_{i=1}^{n} \lambda_i x_i \mid n \in \mathbb{N}, \lambda_i \in K, x_i \in M, \sum_i \lambda_i = 1 \right\},$$

das heißt aff M *ist die Menge aller Affinkombinationen von Elementen von M. Diese Folgerung ist überraschend.*

Beweis. aff $M = x_0 + \operatorname{Lin}(M - x_0)$ ist klar, da $(aff M) - x_0$ der kleinster lineare Unterraum von V ist, der $M - x_0$ enthält.
Sei $\sum_{i=1}^{n} \mu_i(x_i - x_0)$ eine beliebige Linearkombination von Elementen aus $M - x_0$. Dann ist $x_0 + \sum_{i=1}^{n} \mu_i(x_i - x_0) = (1 - \sum_i \mu_i)x_0 + \sum_i \mu_i x_i$ eine Affinkombination von Elementen von M.
Umgekehrt sei $\sum_i \lambda_i x_i$ eine Affinkombination. Dann ist $\sum_i \lambda_i x_i = x_0 + \sum_i \lambda_i (x_i - x_0)$ wegen $\sum_i \lambda_i = 1$. □

Definition 8.7. Sei $U \subseteq V$ ein affiner Unterraum. Dann ist

$$\dim U := \begin{cases} \dim X_U & \text{falls } U \neq \emptyset \\ -1 & \text{falls } U = \emptyset \end{cases}$$

Definition 8.8. Ein affiner Unterraum U von V heißt ein Punkt genau dann, wenn $\dim U = 0$, eine eine Gerade genau dann, wenn $\dim U = 1$, eine Ebene genau dann, wenn $\dim U = 2$ und eine Hyperebene genau dann, wenn ein $x \in V \setminus U$ existiert mit $\operatorname{aff}(U \cup \{x\}) = V$. (Falls $\dim V < \infty$, ist U Hyperebene genau dann, wenn $\dim U = \dim V - 1$).

Von Studenten für Studenten. Ein Ingenieur un ein Mathematiker hören eine Physikvorlesung, in der fünf- bis acht-dimensionale Räume genutzt werden. Der Ingenieur ist frustriert, während der Mathematiker den Vortrag sichtlich genießt- Fragt der Ingenieur den Mathematiker: "Wie stellst du dir das denn vor ?" — "Ganz einfach, ich stelle mir n-dimensionale Räume vor und spezialisiere dann zu $n = 5, 6, 7$ oder 8."

Definition 8.9. $M \subseteq V$ heißt affin unabhängig, falls für alle $x \in M$ gilt, dass $x \notin (M \setminus \{x\})$. $M \subseteq V$ heißt affin abhängig, falls M nicht affin unabhängig ist.
$y \in V$ heißt von M affin abhängig, falls $y \in \operatorname{aff} M$.
$y \in V$ heißt von M affin unabhängig, falls $y \notin \operatorname{aff} M$.

F 8.10. *M ist genau dann affin unabhängig, wenn $M = \emptyset$ oder wenn es $x_0 \in M$ gibt, sodass $(M - x_0) \setminus \{0\}$ linear unabhängig ist.*

Beweis. " $\Longrightarrow$ " Sei M affin unabhängig und $M \neq \emptyset$ und $x_0 \in M$ beliebig. Dann gilt für alle $x \in M$, dass $x \notin \text{aff}(M \setminus \{x\})$, also $x - x_0 \notin \text{aff}(M \setminus \{x\}) - x_0 = \text{aff}((M - x_0) \setminus \{x - x_0\}) = \text{Lin}((M - x_0) \setminus \{x - x_0\})$, also $(M - x_0) \setminus \{0\}$ linear unabhängig.
" $\Longleftarrow$ " Falls $M = \emptyset$ klar. Sonst sei $x_0 \in M$ und $(M - x_0) \setminus \{0\}$ linear unabhängig. Dann ist für alle $x \in M \setminus \{x_0\}$: $x - x_0 \notin \text{Lin}((M - x_0) \setminus \{x - x_0\})$, also $(x \notin \text{aff}(M \setminus \{x\})$ □

F 8.11. *$M \subseteq V$ ist genau dann affin unabhängig, wenn für alle $n \in \mathbb{N}$, $\lambda_i \in K$, $x_1, \dots x_n \in M$ paarweise verschieden gilt: Aus*

$$\sum_{i=1}^{n} \lambda_i x_i = 0 \text{ und } \sum_{i=1}^{n} \lambda_i = 0 \text{ folgt } \lambda_1 = \cdots = \lambda_n = 0$$

Beweis. " $\Longrightarrow$ " Falls $x \in \text{aff}(M \setminus \{0\})$, dann gibt es $\lambda \in K$, $x_1, \dots, x_n, x \in M$ verschieden mit

$$x = \sum_i \lambda_i x_i \text{ und } \sum_i \lambda_i, \text{ also } 0 = (-1)x + \sum_i \lambda_i x_i$$

Also die Summe der Koeffizienten gleich 0. " $\Longleftarrow$ " einfache Übung □

Bemerkung. $M \subseteq V$ ist genau dann affin unabhängi, wenn $\{(1, x) \mid x \in M\} \subseteq K \times V$ linear unabhängig ist.

Beweis.

$$\sum_{i=1}^{n} \lambda_i (1, x) = 0 \iff \sum_{i=1}^{n} \lambda_i = 0 \text{ und } \sum_{i=1}^{n} \lambda_i x_i = 0$$

Weiteres folgt aus der Definition von linear unabhängig und obigem. □

Definition 8.12. Ein Tupel $(x_1, \dots x_n)$ heißt affin unabhängig genau dann, wenn $\{x_1, \dots, x_n\}$ affin unabhängig ist und die x_i paarweise verschieden sind.

Satz 8.13 (Dimensionssatz für affinie Unterräume)**.** *Seien $U_1, U_2 \subseteq V$ nicht-leere endlich-dimensionale affine Unterräume von V. Dann gilt*

1. Fall $U_1 \cap U_2 \neq \emptyset$. Dann gilt

$$\dim(U_1 \vee U_2) = \dim(U_1) + \dim(U_2) - dim(U_1 \cap U_2),$$

wobei $U_1 \vee U_2 = \operatorname{aff}(U_1 \cup U_2) = \sup(U_1, U_2)$.

2. Fall $U_1 \cap U_2 = \emptyset$. *Dann gilt*

$$\dim(U_1 \vee U_2) = \dim U_1 + dim U_2 + 1 - \dim(X_{U_1} \cap X_{U_2}),$$

wobei X_W *der zu* W *gehörige lineare Unterraum ist.*

Beweis. 1. Fall $U_1 \cap U_2 \neq \emptyset$. Sei $x_0 \in U_1 \cap U_2$. Dann ist

$$\begin{aligned}(U_1 \vee U_2) - x_0 &= \operatorname{aff}(U_1 \vee U_2) = \operatorname{Lin}((U_1 - x_0) \cup (U_2 - x_0)) \\ &= (U_1 - x_0) + (U_2 - x_0)\end{aligned}$$

Also

$$\begin{aligned}\dim(U_1 \vee U_2) &= \dim((U_1 - x_0) + (U_2 - x_0)) \\ &= \dim(U_1 - x_0) + \dim(U_2 - x_0) - \dim(\underbrace{(U_1 - x_0) \cap (U_2 - x_0)}_{=(U_1 \cap U_2) - x_0}) \\ &= \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)\end{aligned}$$

2. Fall $U_1 \cap U_2 = \emptyset$. Seien $x_1 \in U_1$ und $x_2 \in U_2$. Dann ist

$$\begin{aligned}(U_1 \vee U_2) - x_1 &= \operatorname{Lin}((U_1 - x_1) \cup (U_2 - x_1)) \\ &= \operatorname{Lin}((U_1 - x_1) \cup \{x_2 - x_1\} \cup (U_2 - x_2)) \\ &= (U_1 - x_1) + (U_2 - x_2) + K(x_2 - x_1) \\ &= X_{U_1} + X_{U_2} + K(x_2 - x_1),\end{aligned}$$

wobei $x_2 - x_1 \notin X_{U_1} + X_{U_2}$, denn sonst gäbe es $u_1 \in U_1$, $u_2 \in U_2$ mit $x_2 - x_1 = (u_1 - x_1) - (u_2 - x_2)$, also $u_1 - u_2 = 0$, also $u_1 = u_2$, was der Annahme $U_1 \cap U_2 = \emptyset$ widerspricht.

Also

$$\begin{aligned}\dim(U_1 \vee U_2) &= \dim((U_1 \vee U_2) - x_1) = \dim(X_{U_1} + X_{U_2} + 1) \\ &\overset{\text{Dim.s.}}{=} \dim(X_{U_1}) + \dim(X_{U_2}) + 1 - \dim(X_{U_1} \cap X_{U_2}) \\ &= \dim U_1 + \dim U_2 + 1 - \dim(X_{U_1} \cap X_{U_2})\end{aligned}$$ □

Definition 8.14. Sei V ein K-Vektorraum und U_1, U_2 nicht leere affine Unterräume. Dann heißen U_1 und U_2 (zueinander) parallel ($\iff$ $U_1 \parallel U_2$), falls $X_{U_1} \subseteq X_{U_2}$ oder $X_{U_2} \subseteq X_{U_1}$.

Bemerkung. $\parallel$ ist eine symmetrische und reflexive Relation, ist aber nicht transitiv, also keine Äquivalenzrelation! Auf der Menge der affinen Unteräumen einer Dimension ist $\parallel$ eine Äquivalenzrelation.

Definition 8.15. Sei V ein K-Vektorraum, $x \in V$. Die Abbildung $t_x \colon V \to V$ mit $t_x(y) = y + x$ heißt die Translation mit Translationsvektor x. Eine Abbildung $f \colon V \to V$ heißt eine Translation, falls es ein $x \in V$ gibt mit $f = t_x$. Eine Translation heißt auch Parallelverschiebung.

F 8.16. *Für $x, y \in V$ gilt $t_{x+y} = t_x \circ t_y = t_y \circ t_x$.*
t_x ist bijektiv und $t_x^{-1} = t_{-x}$. $t_0 = \mathrm{id}$.
t_x bildet affine Unteräume U von V auf affine Unteräume von V ab und es gilt $t_x(U) = U + x$, $\dim(t_x(U)) = \dim U$.

Definition 8.17. Seinen V, W K-Vektorräume. Eine Abbildung $f \colon V \to W$ heißt eine affine Abbildung, falls eine lineare Abbildung $\widehat{f} \colon V \to W$ und $w \in W$ gibt, sodass $f(x) = w + \widehat{f}(x)$ für alle $x \in V$, das heißt $f = t_w \circ \widehat{f}$.

Bemerkung. $w = f(0)$, also w und $\widehat{f}$ sind durch f eindeutig bestimmt, $\widehat{f} = f - f(0) = t_{-f(0)} \circ f$, $f = t_{f(0)} \circ \widehat{f}$.

Definition 8.18. Eine Affinität ist eine bijektive affine Abbildung $f \colon V \to V$.

F 8.19. *Seien $g \colon V \to W$, $f \colon W \to V$ affine Abbildungen. Dann gilt*

1. *$f \circ g$ ist eine affine Abbildung mit $f \circ g = \widehat{f} \circ g + f(0)$ und $\widehat{(f \circ g)} = f \circ g - (f \circ g)(0) = \widehat{f} \circ \widehat{g}$.*
2. *Falls f bijektiv ist, ist f^{-1} eine affine Abbildung mit $f^{-1} = \widehat{f^{-1}} - \widehat{f^{-1}}(f(0))$*

Beweis.

$$\begin{aligned}(f \circ g)(0) &= \widehat{f}(g(0)) = \widehat{f}(g(0)) + f(0)\\ \widehat{(f \circ g)}(x) &= (f \circ g)(x) - (f \circ g)(0) = \widehat{f}(g(x)) + f(0) - (f \circ g)(0)\\ &= \widehat{f}(\widehat{g}(x) + g(0)) + f(0) - (f \circ g)(0)\\ &= \widehat{f}(\widehat{g}(x)) + (\widehat{f} \circ g)(0) + f(0) - (f \circ g)(0) = (\widehat{f} \circ \widehat{g})(x)\end{aligned}$$

Sei nun f bijektiv, dann

$$f^{-1}(x) = \widehat{f^{-1}}(x) - f^{-1}(f(0)), \text{ denn}$$
$x = f^{-1}(f(x)) = \widehat{f^{-1}}(f(0)) = \widehat{f^{-1}}(\widehat{f}(x) + f(0)) - \widehat{f^{-1}}(f(0))$, denn $\widehat{f^{-1}}$ ist linear. □

Definition 8.20.

$$\begin{aligned} A(V) &:= \{f\colon V \to V \mid f \text{ affine bijektive Abbildung}\} \\ &:= \{f\colon V \to V \mid f \text{ Affinität}\}, \end{aligned}$$

die affine Gruppe, ist eine Untergruppe der Gruppe der bijektiven Abbildungen $V \to V$.
$GL(V) \subset A(V)$ ist eine Untergruppe von $A(V)$.
$T(V)$, die Gruppe der Translationen, ist eine Normalteiler (und Untergruppe) von $A(V)$.
Offensichtlich ist $(T(V), \circ) \cong (V, +)$.
$\widehat{\ }\colon A(V) \to GL(V)$ mit $f \mapsto \widehat{f}$ ist ein Gruppenhomomorphismus, da $\widehat{fg} = \widehat{f}\widehat{g}$. $\ker(\widehat{\ }) = T(V)$, daher ist $T(V)$ ein Normalteiler.

F 8.21. *Affine Abbildungen bewahren Affinkombinationen, d.h. sei $f\colon V \to W$ eine affine Abbildung und $v_1, \dots v_n \in V$, $\lambda_i \in K$ mit $\sum_i \lambda_i = 1$. Dann gilt $f(\sum_i \lambda_i v_1) = \sum_i \lambda_i f(v_i)$.*

Beweis. Lineare Abbildungen bewahren Linearkombination, also reicht es die Behauptung für Translationen zu zeigen. Sei $x \in V$. Dann

$$t_x\left(\sum_i \lambda_i v_i\right) = \sum_i \lambda_i v_i + 1 \cdot x = \sum_i \lambda_i v_i + \sum_i \lambda_i x = \sum_i \lambda_i (v_i + x) \sum_i \lambda_i t_x(v_i)$$

□

Definition 8.22. Punkte $P_1, P_2, \dots$ heißen kollinear, falls $\dim \operatorname{aff}\{P_1, \dots\} = 1$, d. h. $P_1, P_2, \dots$ auf einer Geraden liegen.
Sie heißen koplanar, falls $\dim \operatorname{aff}\{P_1, P_2, \dots\} \leq 2$.

Definition 8.23. Seien p_1, p_2, p_3, kollinear mit $p_1 \neq p_3$. Dann gibt es ein eindeutig bestimmtes $\lambda \in K$ mit $p_1 - p_2 = \lambda(p_1 - p_3)$, denn $p_2 = \lambda p_3 + (1-\lambda)p_1$. λ heißt dann das Teilverhältnis von p_1, p_2, p_3, geschrieben $\lambda = \mathrm{TV}(p_1, p_2, p_3)$.

Aus Fakt 8.21 folgt, dass affine Abbildungen des Teilverhältnis bewahren.

8.1 Abstände: Euklidische Analytische Geometrie

Betrachte einen euklidischen Vektorraum V ($\mathbb{R}$-Vektorraum mit Skalarprodukt $\langle\ ,\ \rangle$).

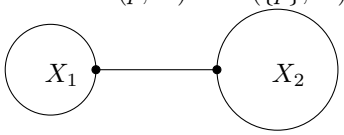
Definition 8.24. Eine Bewegung ist eine bijektive Abbildung $f\colon V \to V$ mit $f(v) = \widehat{f}(v) + t$ (wobei $\widehat{f}$ eine othogonale (bijektive) Abbildung ist und $t \in V$), also $\widehat{f}(v) = f(v) - f(0)$ zugehörige orthogonale Abbildung.

Betrachte den $\mathbb{R}^n$ mit dem Standardskalarprodukt $\langle\ ,\ \rangle$. Die Bewegungen sind die Abbildung $f\colon \mathbb{R}^n \to \mathbb{R}^n$ mit $f(x) = Ax + t$, wobei A eine orthogonale $n \times n$ - Matrix ist, d.h. $A^T = A^{-1}$ $(A \in \mathbb{R}^n)$.

Definition 8.25. Seien $X_1, X_2 \in V$ nichtleere Teilmenge. Dann definiert man den Abstand zwischen X_1 und X_2 durch

$$\mathrm{d}(X_1, X_2) := \inf\{\mathrm{d}(x_1, x_2) \mid x_1 \in X_1, x_2 \in X_2\}$$
$$\mathrm{d}(x_1, x_2) = \|x_1 - x_2\| = \sqrt{\langle x_1 - x_2, x_1 - x_2\rangle}$$

Wir schreiben $\mathrm{d}(p, X)$ für $\mathrm{d}(\{p\}, X)$, wenn $p \in V$. Für affine Unterräume



$(\neq \emptyset)$
Für $p_1 + U_1$ und $p_2 + U_2$ (U_i lineare Unterräume) ergibt sich

$$\mathrm{d}(p_1 + U_1, p_2 + U_2) = \mathrm{d}(p_2 + p_1, U_1 + U_2),$$

Beweis.

$$\{(p_2 + u_2) - (p_1 + u_1) \mid u_1 \in U_1, u_2 \in U_2\}$$
$$= \{p_2 - p_1 - (u_1 - u_2) \mid u_1 \in U_1, u_2 \in U_2\} = \{(p_2 - p_1) - u \mid u \in U_1 + U_2\},$$

also stimmt das Infimum der Norm der Element der beiden Mengen überein. □

Seien U_1, U_2 lineare Unterräume und $p_1 + U_1$ und $p_2 + U_2$ affine Unterräume. Dann ist $\mathrm{d}(p_1 + U_1, p_2 + U_2) = \mathrm{d}(p_2 - p_1, U_1 + U_2)$. Damit wird die Frage nach dem Abstand von affinen Unteräumen zurückgeführt auf den Frage nach dem Abstand von einem Punkt und einem linearen Unterraum.

F 8.26. *Sei $U \subseteq V$ ein linearer Unterraum und $x \in V$. Dann gilt*

$$\mathrm{d}(x, U) = \|x - p_U(x)\| = (\|x\|^2 + \|p_U(x)\|^2)^{\frac{1}{2}} = \left(\|x\|^2 - \sum_{k=1,\dots,m} \langle b_k, x\rangle^2\right)^{\frac{1}{2}}$$

für jede ON-Basis $(b_1, \dots, b_m$ von U.

Beweis. Schreibe $x = u + v$ mit $u \in U$, $v \in U^\perp$, also $u = p_U(x)$, also

$\|x\|^2 = \langle u + v, u + v\rangle = \|u\|^2 + \|v\|^2$, also

$$\mathrm{d}(x, U) \overset{7.31}{=} \|x - p_U(x)\| = (\|x\|^2 - \|p_U(x)\|^2)^{\frac{1}{2}} \overset{7.32}{=} \left(\|x\|^2 - \sum_{k=1,\dots,m} \langle x, b_k\rangle^2\right)^{\frac{1}{2}}$$

□

Definition 8.27. Zwei affine Unterräume $A_1 = p_1 + U_1$ und $A_2 = p_2 + U_2$ mit U_1, U_2 lineare Unterräume heißen windschief, falls $A_1 \cap A_2 = \emptyset$ und $U_1 \cap U_2 = \{0\}$. Dann gilt

$$\mathrm{d}(A_1, A_2) = \mathrm{d}(p_2 - p_1, U_1 + U_2 \overset{8.1}{=} \|(p_2 - p_1) - p_{U_1+U_2}(p_2 - p_1)\| .$$

Nach F. 8.1 ist $u = p_{U_1+U_2}(p_2 - p_1)$ der eindeutig bestimmt Vektor $u \in U_1 + U_2$, für den $\mathrm{d}(p_2 - p_1, u) = d(p_2 - p_1, U_1 + U_2)$ angenommen wird. Wenn A_1, A_2 windschief sind ($\implies$ $U_1 \cap U_2 = \emptyset$), dann lässt such u eindeutig zerlegen als $u = u_1 + u_2$ mit $u_1 \in U$ und $u_2 \in U$. Dann sind $p_1 + u_1 \in A_1$ und $p_2 - u_2 \in A_2$ das eindeutig bestimmte Punktepaar in A_1 bzw. A_2 mit kleinstem Abstand, denn

$$(p_2 - u_2) - (p_1 + u_1) = (p_2 - p_1) - (U_1 + u_2) = (p_2 - p_1) - u$$

Definition 8.28. $\mathrm{aff}\{p_1 + u_1, p_2 - u_2\}$ heißt des Gemeinlot von A_1 und A_2. Diese Gerade trifft A_1 und A_2 und ist ortogonal zu U_1 und U_2, denn $(p_2 - u_2) - (p_1 + u_1) = (p_2 - p_1) - u \in (U_1 + U_2)^\perp$.

Definition 8.29. Die Punkte $p_1 + u_1 \in A_1$ und $p_2 - u_2 \in A_2$ heißen die Fußpunkte des Gemeinlots.

F 8.30. *Hyperebenen des $\mathbb{R}^n$ mit Standardskalarprodukt bezüglich Standardbasis können durch eine (nicht-triviale) Gleichung dargestellt werden:*

$$H = \{x \in \mathbb{R}^n \mid \langle x, u\rangle = b\} \text{ mit } u \neq 0, b \in \mathbb{R}.$$

$$\text{Beachte: } u^\perp x = \begin{pmatrix} u_1 & \dots u_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_i x_i u_i = \langle x, u\rangle = \langle u, x\rangle$$

Man kann umformen: $\langle x, u\rangle = b \iff \langle x, \lambda u\rangle = \lambda b$, also kann man u normieren. Falls $b \neq 0$ multipliziere mit $\frac{b}{|b|}$. Man erhält die Hesse'sche Normalform:

$$H = \{x \in \mathbb{R}^n \mid \langle x, u\rangle = b\} \text{ mit } \|u\| = 1, b \geq 0$$

- *Dabei sind u und b eindeutig durch H bestimmt, falls $b \neq 0$.*
- *Falls $b = 0$ gibt es zwei Möglichkeiten: u und $-u$.*
- *u heißt der Einheitsnormalenvektor von H.*
- *b ist der Abstand zwischen O und H.*

- *bu ist der Lotfußpunkt von O auf H.*
- *Der zu H gehörige lineare Unterraum ist $\{x \in \mathbb{R}^n \mid \langle x, u\rangle = 0\}$.*

Definition 8.31. Die orthogonale Projektion auf einen affinen Unterraum $A = a+U$ (U linearer Unterraum) ist durch $p_A(x) = a+p_U(x-a)$ gegeben. Es gilt, dass $p_A(x)$ der nächstgelegenste Punkt von x in A ist.

Definition 8.32. Sei $A = a+U$ ein affiner Unterraum, U der zugehörige lineare Unterraum. Die Spiegelung an A ist $s_A(x = p_A(x)+(p_A(x)-x) = 2p_A(x) - x = 2a + 2p_U(x-a) - x$, also $s_A = 2p_A - \mathrm{id}$.
Dann gilt $s|_A = \mathrm{id}$ und für $w \in A$, $v \in U^\perp$: $s_A(w+v) = w - v$. (Nachrechnen!)

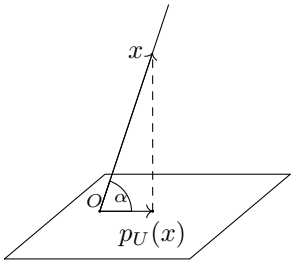
8.2 Winkel

Definition 8.33. Der Winkel zwischen zwei Strahlen (Halbgeraden) $s + \mathbb{R}_{\geq 0}u$ und $x + \mathbb{R}_{\geq 0}v$ mit $u, v \neq 0$ ist definiert als

$$\alpha = \arccos\left(\frac{\langle u, v\rangle}{\|u\| \cdot \|v\|}\right)$$

Definition 8.34. Der Winkel zwischen einer Geraden $\mathbb{R}x$ ($x \neq 0$) eine einem linearen Unterraum $U \neq \{0\}$ ist

$$\alpha = \arccos\left(\frac{\|p_u(x)\|}{\|x\|}\right)$$



Definition 8.35. Der Winkel α zwischen einer Hyperebene $H = \{x \in \mathbb{R}^n \mid \langle x, u\rangle =\}$ mit $u \neq 0$ (also $H = \{u\}^\perp$) und einem linearen Unterraum

$U \neq 0$:

$$\beta = \arccos\left(\frac{\|p_U(u)\|}{\|u\|}\right)$$
$$\alpha = \frac{\pi}{2} - \beta = 90° - \beta$$

Von Studenten für Studenten (sinngemäß zitiert von Prof. Brehm). Stellen Sie sich vor, sie sich im 7-dimensionalen Raum und wollen dien Winkel zwischen einem drei-dimensionalen Raum und einer Hyperebene erklären.

Definition 8.36. Der Winkel zwischen zwei affinen Unterräumen A_1 und A_2 it definiert als der Winkel zwischen den zugehörigen linearen Unterräumen. Dabei muss einer der beiden Unterräume eine Gerade oder eine Hyperebene sein und der andere muss eine Dimension von 1 bis $n-1$ haben.

8.3 Das Kreuzprodukt

Definition 8.37 (Das vektorielle Produkt in $\mathbb{R}^3$)**.** Betrachte $\mathbb{R}^3$ mit Standardskalarprodukt und Standardbasis e_1, e_2, e_3. $a, b \in \mathbb{R}^3$. Dann definiere

$$\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3, a \times b := \sum_{i=1}^{3} \det(a, b, e_i) e_i$$
$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix}$$

$a \times b$ heißt das vektorielle Produkt oder Kreuzprodukt von a und b.
Konvention: $\times$ bindet stärker als $+$.
Verallgemeinerung (Diskussion in den Übungen): $f : \mathbb{R}^n \times \cdots \times \mathbb{R}^n \to \mathbb{R}^n$ mit

$$f(a_1, \ldots, a_{n-1}) := \sum_{i=1}^{n} \det(a_1, \ldots, a_{n-1}, e_i) \cdot e_i$$

Satz 8.38. *(I)* $a \times b = -b \times a$ *(alternierend oder schiefsymetrisch)*

(II) (bilinear)

$$(a + b) \times c = a \times c + b \times c$$
$$a \times (b + c) = a \times b + a \times c$$
$$(\lambda a) \times b = \lambda(a \times b)$$
$$a \times (\lambda b) = \lambda(a \times b)$$

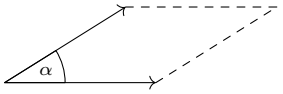
(III) $\langle a \times b, c\rangle = \det(a,b,c)$ *„Skalarprodukt“(Volumen des von a, b, c aufgespannten Spates mit Vorzeichen).*

(IV) $a \times b \in \{a,b\}^\perp$ *($a \times b$ steht senkrecht auf a und b)*

(V) $\|a \times b\|^2 = \|a\|^2 \|b\|^2 - \langle a,b\rangle$ *Geometrisch:*

$$\|a \times b\|^2 = \|a\|^2 \|b\|^2 - (\|a\| \|b\| \cos \sphericalangle(a,b))^2 = \|a\|^2 \|b\|^2 \sin^2 \sphericalangle(a,b)$$
$$\implies \|a \times b\| = \|a\| \|b\| |\sin \sphericalangle(a,b)|$$

Damit ist $\|a \times b\|$ gleich dem Flächeninhalt des von a und b aufgespannten Parallegramms.



(VI) a, b *linear unabhängig* $\iff a \times b = 0$.

(VII) $\det(a,b,a \times b) = \|a \times b\|^2 \geqslant 0$. *Geometrisch: $(a,b,a \times b)$ ist positiv orientiert (falls a, b linear unabhängig) („3-Fingerregel der rechten Hand“)*

(VIII) a, b *linear abhängig* $\Leftrightarrow a \times b = 0$

(IX) $a \times (b \times c) = \langle a,c\rangle b - \langle a,b\rangle c$ *(Grassman-Identität)*

(X) $a \times (b \times c) + b \times (c \times a) + c \times (a \times b) = 0$ *(Jacobi-Identität)*

(XI) $\langle a \times b, c \times d\rangle = \langle a,c\rangle \langle b,d\rangle - \langle b,c\rangle \langle a,d\rangle$ *(Lagrange-Identität)*

Beweis. Für alle a, b, c, $d \in \mathbb{R}^3$, $\lambda \in \mathbb{R}^3$ gilt:

I, II klar nach Def. (Rechenregeln für det)

III $\left\langle a \times b, \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} \right\rangle = c_1 \det(a,b,e_1) + c_2 \det(a,b,e_2) + c_3 \det(a,b,e_3) = \det(a,b,c)$

IV $\langle a \times b, a\rangle = \det(a,b,a) = 0$, $\langle a \times b, b\rangle = \det(a,b,b) = 0$

V ist ein Spezialfall von XI für $a = c$, $b = d$.

Geometrisch interpretiert, betrachte $c \in \{a,b\}^\perp$ mit $\|c\| = 1$, $\det(a,b,c) > 0$. $\det(a,b,c)$ = Volumen des Spates = Flächeninhalt des von a, b aufgespannten Parallelogrammes, da Höhe $= \|c\| = 1$.

$\alpha = \sphericalangle(a,b)$, also $\|a \times b\| = \|a\|\|b\| |\sin \alpha|$ ist der Flächeninhalt des von a, b aufgespannten Parallelogrammes.

VII $\det(a,b,a \times b) = \langle a \times b, a \times b\rangle = \|a \times b\|^2$

VIII a, b linear abhängig $\Rightarrow a \times b = 0$ klar (nach Def.)

Seien a, b linear unabhängig, wähle dazu linear unabhängig Vektor c. Dann ist $\langle a \times b, c\rangle = \det(a,b,c) \neq 0$, also $a \times b \neq 0$.

IX Nachrechnen!! (Übung)

X folgt aus IX:

$$\begin{aligned} a \times (b \times c) + b \times (c \times a) + c \times (a \times b) \\ = \langle a, c\rangle\, b - \langle a, b\rangle\, c + \langle b, a\rangle\, c - \langle b, c\rangle\, a + \langle c, b\rangle\, a - \langle c, a\rangle\, b = 0 \end{aligned}$$

XI

$$\begin{aligned} \langle a \times b, c \times d\rangle &\overset{\text{IV}}{=} \det(a, b, c \times d) = \det(b, c \times d, a) \overset{\text{III}}{=} \langle bx(c \times d), a\rangle \\ &\overset{\text{IX}}{=} \langle \langle b, d\rangle\, c - \langle b, c\rangle\, d, a\rangle = \langle b, d\rangle \langle c, a\rangle - \langle b, c\rangle \langle d, a\rangle \end{aligned}$$

□

Beispiel. (Anwendung)

- Bestimmung eines Normalenvektors zu a, b
- Ergänzung zu ON-Basis. Falls (a, b) ein ON-System in $\mathbb{R}^3$ ist, dann ist $(a, b, a \times b)$ eine ON-Basis des $\mathbb{R}^3$.
- Wechsel der Darstellung einer Ebene in $\mathbb{R}^3$ von $a + \mathbb{R}b + \mathbb{R}c$ mit b, c linear unabhängig. $b \times c$ ist ein Normalenvektor zu b, c. Daher $a + \mathbb{R}b + \mathbb{R}c = \{v \mid \langle v, b \times c\rangle = \langle a, b \times c\rangle\} = \{v \mid \det(v - a, b, c) = 0\}$

8.4 Kategorisierung von Isometrien im $\mathbb{R}^2$ und $\mathbb{R}^3$

Sei V ein euklidischer Vektoraum ($\dim V = \infty$ ist zugelassen)

Definition 8.39. Eine Abbildung $f\colon V \to V$ heißt eine Isometrie, falls

$$\|f(x) - f(y)\| = \|x - y\| \text{ für alle } x, y \in V,$$

d.h. Abstände werden bewahrt.

Satz 8.40. *Sei $g\colon V \to V$ eine Isometrie. Dann ist $f\colon V \to V$ mit $f(x) := g(x) - g(0)$ eine orthogonale Abbildung (also insbesondere eine lineare Abbildung) (also g eine affine Abbildung, was wir nicht vorausgesetzt hatten).*

Beweis. Sei g eine Isometrie. Sei $f\colon V \to V$ definiert durch $f(x) := g(x) - g(0)$. Dann folgt

$$\begin{aligned} \|f(x)\| &= \|g(x) - g(0)\| = \|x - 0\| = \|x\| \\ \implies \|f(x_1) - f(x_2)\|^2 &= \|f(x_1)\|^2 + \|f(x)\|^2 - 2\langle f(x_1), f(x_2)\rangle \\ &= \|x_1\|^2 + \|x_2\|^2 - 2\langle f(x_1), f(x_2)\rangle \\ = \|g(x_1) - g(x_2)\|^2 &\overset{g \text{ Isometrie}}{=} \|x_1 - x_2\|^2 = \|x_1\|^2 + \|x_2\|^2 - 2\langle x_1, x_2\rangle \end{aligned}$$

Also bewahrt f das Skalarprodukt.
f ist linear:

$$\begin{aligned}\|f(x_1+x_2)-f(x_1)-f(x_2)\|^2 &= \|f(x_1+x_2)\|^2 - 2\langle f(x_2)\rangle - 2\langle f(x_1), f(x_2)\rangle + \\ &\quad \|f(x_1)\|^2 + \|f(x_2)\|^2 \\ = \|x_1+x_2\|^2 - 2\langle x_1+x_2, x_1\rangle - 2\langle x_1+x_2, x_2\rangle - 2\langle x_1, x_2\rangle + \|x_1\|^2 + \|x_2\|^2 \\ &= \|(x_1+x_2)-x_1-x_2\|^2 = 0 \\ \|f(\lambda x)-\lambda f(x)\|^2 &= \|f(\lambda x)\|^2 - 2\lambda\langle f(\lambda x), f(x)\rangle + \lambda^2\|f(x)\|^2 \\ &= \|\lambda x\|^2 - 2\lambda\langle \lambda x, x\rangle + \lambda^2\|x\|^2 = 0\end{aligned}$$

Also f ist linear. f bewahrt das Skalarprodukt, also ist f eine orthogonale Abbildung. □

F 8.41. *Sei $g\colon V \to V$ eine affine Abbildung, $\dim V < \infty$ und $f = g - t$, $t = g(0)$ die zugehörige lineare Abbildung. Falls 1 keine Eigenwert von f ist, hat g genau einen Fixpunkt x_0 und lässt sich schreiben als $g(x) = f(x - x_0) + x_0$.*

Beweis.

$$g(x_0) = x_0 \iff f(x_0) - t = x_0 \iff (\mathrm{id} - f)x_0 = t \iff x_0 = (\mathrm{id} - f)^{-1}(t)$$

Beachte, dass $\mathrm{id} - f$ bijektiv ist, da 1 kein Eigenwert von f ist und $\dim V < \infty$.
Also

$$f(x - x_0) + x_0 = f(x) + (\mathrm{id} - f)(x_0) = f(x) + t = g(x)$$

□

8.5 Klassifikation der Isometrien in $\mathbb{R}^2$ und $\mathbb{R}^3$

Sei $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ eine orthogonale Abbildung und A die Matrix zu f bzgl. der Standartbasis. Dann ist $\left(\begin{pmatrix}a_{11}\\a_{12}\end{pmatrix}, \begin{pmatrix}a_{21}\\a_{22}\end{pmatrix}\right)$ eine ON-Basis des $\mathbb{R}^2$.
$a_{11}^2 + a_{12}^2 = 1$. Dann gibt es $\varphi \in [0, 2\pi)$ mit $a_{11} = \cos(\varphi)$ und $a_{12} = \sin(\varphi)$.
Damit ist entweder:

1. $\begin{pmatrix}a_{21}\\a_{22}\end{pmatrix} = \begin{pmatrix}-\sin(\varphi)\\\cos(\varphi)\end{pmatrix}$, falls $\det A = 1$ (Drehung um den Winkel φ)
2. oder $\begin{pmatrix}a_{21}\\a_{22}\end{pmatrix} = \begin{pmatrix}\sin(\varphi)\\-\cos(\varphi)\end{pmatrix}$, falls $\det A = -1$ (Spiegelung an einer Geraden)

1.Fall: $\det A = 1$ Spezialfälle:

$$A = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = E \ (\varphi = 0), \text{ EW } 1, \text{ 2-dim. Eigenraum}$$

$$A = \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix} = -E \ (\varphi = \pi), \text{ EW } -1, \text{ 2-dim. Eigenraum}$$

$\det \begin{pmatrix} \cos(\varphi) - \lambda & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) - \lambda \end{pmatrix} = \lambda^2 - 2\lambda\cos(\varphi) + 1$
Nullstellen: $\cos(\varphi) \pm \sqrt{\cos^2(\varphi) - 1} = \cos(\varphi) \pm i\sin(\varphi)$

2.Fall: $\det A = -1$.
$\det \begin{pmatrix} \cos(\varphi) - \lambda & \sin(\varphi) \\ \sin(\varphi) & -\cos(\varphi) - \lambda \end{pmatrix} = \lambda^2 - 1$
also EW 1 und -1.

Nun zum affinen Fall:

1.Fall: Falls die zugehörige Matrix $\neq E$, ist 1 kein EW, also ist es eine Drehung um den Punkt x_0 (mit x_0 wie in F8.41)
Falls die zugehörige Matrix $= E$, dann ist es eine Translation $g(x) = x + t$

2.Fall: Sei $\det A = -1$. Seien u EV zum EW 1 und v EV zum EW -1. $\langle u, v\rangle = 0$, da A orthogonale Matrix.

Zerlege t in die Komponenten t_1 im Eigenraum zum EW 1, $U :=$ ER zum EW 1 $t_1 = t - t_1 \in U^\perp$, also $t_1 = \frac{\langle t,u\rangle}{\|u\|^2} \cdot u$, $t_2 = \frac{\langle t,v\rangle}{\|v\|^2} \cdot v$, $(t = t_1 + t_2)$. Dann ist die Abbildung $g_1(x) = Ax + t_2$ eine Spiegelung an der Geraden $G = \frac{t_2}{2} + \mathbb{R}u$, also $g(x) = g_1(x) + t_1 = Ax + t$ die Komposition aus einer Spiegelung an G und einer Translation t_1 in Richtung der Geraden.

Eine solche Abbildung heißt Gleitspiegelung (oder Schubspiegelung) an einer Geraden G mit Translation t_1 (falls $t_1 \neq 0$, sonst normale Spiegelung)

8.5.1 Klassifikation der Isometrien in $\mathbb{R}^2$

8.5.2 Isometrien des $\mathbb{R}^3$

Zunächst betrachte $A \in O(3)$ orthogonale 3×3-Matrix. Das charakteristische Polynom von A ist vom Grad 3, hat also mindestens eine reelle Nullstelle; ferner haben alle komplexen Nullstellen Betrag 1.
Falls das charakteristische Polynom über $\mathbb{R}$ in Linearfaktoren zerfällt, hat A eine ON-Basis aus Eigenvektoren und ist bzg. dieser Basis von der Form

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ Identität oder $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ Spiegelung an einer Ebene oder
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ Sp. an Gerade oder $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ Punktspiegelung

Anderenfalls hat A einen reellen EW +1 oder -1 und das charakteristische Polynom konjugiert komplexe Nullstellen $\cos(\varphi) \pm i\sin(\varphi)$ mit $\varphi \neq 0, \pi$. Sei b_1 ein EV zum EW +1 oder -1 mit $\|b_1\| = 1$.
Ergänze zu einer ON-Basis (b_1, b_2, b_3). Dann ist die Matrix bzgl. dieser Basis von der Form $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\varphi) & -\sin(\varphi) \\ 0 & \sin(\varphi) & \cos(\varphi) \end{pmatrix}$ oder $\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\varphi) & -\sin(\varphi) \\ 0 & \sin(\varphi) & \cos(\varphi) \end{pmatrix}$.
Im ersten Fall ist dies eine Drehung um die Gerade $\mathbb{R}b_1$ um den Winkel φ.
Im zweiten Fall ist dies eine Drehspiegelung mit Drehspiegelachse $\mathbb{R}b_1$ und Drehspiegelebene $\mathbb{R}b_2 + \mathbb{R}b_3$ um den Winkel φ, d.h. die Komposition aus einer Drehung um eine Gerade g und eine anschließende Spiegelung an einer Ebene $\perp g$.

9 Adjungierte und normale Abbildungen

Wenn nicht anders angegeben, seien in diesem Kapitel V, W euklidische bzw. unitäre Räume mit Skalarprodukt $\langle \cdot, \cdot \rangle$.

Definition 9.1. Sei $f\colon V \to W$ linear. Eine lineare Abbildung $f^*\colon W \to V$ heißt eine zu f adjungierte Abbildung, falls für alle $x \in V$, $y \in W$ gilt:

$$\langle f(x), y \rangle_W = \langle x, f^*(y) \rangle_V$$

F 9.2. *Falls eine adjungierte Abbildung zu f existiert, dann ist sie eindeutig bestimmt.*

Beweis. Sei f' auch eine zu f adjungierte Abbildung, dann gilt für alle $x \in V$, $y \in W$:

$$\langle x, f^*(y) - f'(y) \rangle = \langle x, f^*(y) \rangle - \langle x, f'(y) \rangle = \langle f(x), y \rangle - \langle f(x), y \rangle = 0$$

also $f^*(y) = f'(y)$, also da $y \in W$ bel. folgt $f^* = f'$. □

F 9.3. *Wenn $\dim V < \infty$, dann existiert zu jeder linearen Abbildung $f\colon V \to W$ die adjungierte Abbildung f^*, wenn $(e_1, \ldots, e_n)$ eine ON-Basis von V ist, dann gilt:*

$$f^*(y) = \sum_{i=1}^{n} \langle y, f(e_1) \rangle \cdot e_i$$

Beweis. Es gibt eine ON-Basis $(e_1, \ldots, e_n)$ von V. Für alle $x \in V$ gilt:

$$x = \sum_{i=1}^{n} \langle x, e_1 \rangle \cdot e_i$$

Definiere $f^*(y) := \sum_{i=1}^{n} \langle y, f(e_1) \rangle \cdot e_i$. Dann ist f^* eine lineare Abbildung (da $\langle \cdot, \cdot \rangle$ in erster komponente linear ist).
Für alle $x \in V$, $y \in W$ gilt:

$$\begin{aligned} \langle f(x), y \rangle &= \sum_{i=1}^{n} \langle x, e_1 \rangle \langle f(e_1), y \rangle \overset{*}{=} \sum_{i=1}^{n} \langle x, \langle y, f(e_i) \rangle \cdot e_i \rangle \\ &= \left\langle x, \sum_{i=1}^{n} \langle y, f(e_i) \rangle e_i \right\rangle = \langle x, f^*(y) \rangle \end{aligned}$$

* beachte $a \langle x, e_i \rangle = \langle x, \overline{a} e_i \rangle$ und $\langle f(e_i), y \rangle = \langle y, f(e_i) \rangle$,
also ist die oben definierte Abbildung f^* wirklich die zu f adjungierte Abbildung. □

Definition 9.4. Sei $A = (a_{ij})_{i,j}$ eine Matrix ($K \in \mathbb{R}, \mathbb{C}$). Dann bezeichne $\overline{A} := \left(\overline{A}\right)^T = \overline{A^T}$ heißt die zu A adjungierte Matrix.

Offensichtlich gelten folgende Rechenregeln.

$$\begin{aligned}
(A^*)^* &= A \\
(A+B)^* &= A^* + B^* \\
(\lambda A)^* &= \overline{\lambda} A^* \\
(AB)^* &= B^* A^* \\
\det A^* &= \overline{\det A} \qquad \text{(für } A \text{ quadratische Matrix)}
\end{aligned}$$

F 9.5. *Seien V, W endlich-dimensional und $f\colon V \to W$ eine lineare Abbildung. Wenn A die Matrix von f bezüglich ON-Basis von V und W ist, dann ist A^* die Matrix von f^* (bzgl. derselben Basen).*

Beweis. Seien $(e_1, \ldots, e_n)$, $(c_1, \ldots, c_m)$ ON-Basen von V bzw W. Für $A = (a_{ij})_{i,j}$ gilt $f(e_i) = \sum_{j=1}^{m} a_{ji} c_j$. Da $(c_1, \ldots, c_m)$ eine ON-Basis ist, ist $a_{ji} = \langle f(e_i), c_j \rangle$.
Sei $B = (b_{ij})_{i,j}$ die Matrix zu f^* bzgl. $(c_1, \ldots, c_m)$ und $(e_1, \ldots, e_m)$.
$f^*(c_j) = \sum_i b_{ij} e_i$, also $b_{ij} = \langle f^*(c_j), e_i \rangle$, dann:

$$b_{ij} = \langle f^*(c_j), e_i \rangle = \overline{\langle e_i, f^*(c_j) \rangle} = \overline{\langle f(e_i), c_j \rangle} = \overline{a_{ji}} \qquad \square$$

F 9.6. *Sei $f\colon V \to W$ eine lineare Abbildung, für die die adjungierte Abbildung $f^*\colon W \to V$ existiert.*

1. *Dann existiert die zu f^* adjungierte Abbildung $(f^*)^*\colon V \to W$ und es gilt $f^{**} = f$. Ferner gilt:*

$$\begin{aligned}
\ker f^* &= (f(V))^{\perp} & & f \text{ surjektiv} \implies f^* \text{ injektiv} \\
\ker f &= (f^*(W))^{\perp} & & f^* \text{ surjektiv} \implies f \text{ injektiv}
\end{aligned}$$

2. $$\begin{aligned}
f^* \text{ injektiv und } \operatorname{Rang} f < \infty &\implies f \text{ surjektiv} \\
f \text{ injektiv und } \operatorname{Rang} f^* < \infty &\implies f^* \text{ surjektiv}
\end{aligned}$$

3. *Falls* $\dim V < \infty$ *und* $\dim W < \infty$, *dann gilt* $\operatorname{Rang} f^* = \operatorname{Rang} f$.

4. Falls die zu $g\colon W \to X$ adjungierte Abbildung g^* existiert, dann existiert die adjungierte Abbildung zu $g \circ f$ und es gilt $f^* \circ g^* = (g \circ f)^* = (g \circ f)^*$

Beweis. 1. Für alle $x \in V$, $y \in W$ gilt:

$$\langle f^*(y), x\rangle = \overline{\langle x, f^*(y)\rangle} = \overline{\langle f(x), y\rangle} = \langle y, f(x)\rangle\,, \text{ also ist } f^{**} = f$$

$$\text{Sei } y \in \ker f^* \iff f^*(y) = 0 \iff \langle f(x), y\rangle = \langle x, f^*(y)\rangle = 0 \text{ für alle } x \in V$$

$$\iff y \in f(V)^\perp$$

$$f \text{ surjektiv} \implies \ker f^* = (f(V))^\perp = 0 \iff f^* \text{ injektiv}$$

2. Falls $\dim f(V) < \infty$ und f^* injektiv, dann ist

$$f(V) = (f(V)^\perp)^\perp = (\ker f^*)^\perp = \{0\}^\perp = W$$

Damit ist f surjektiv.

3. Mit 1. und dem Dimensionssatz gilt

$$\operatorname{Rang} f^* = \dim W - \dim \ker f^* = \dim W - \dim f(V)^\perp = \dim f(V) = \operatorname{Rang} f$$

4. Für alle $x \in V$, $y \in W$:

$$\langle (g \circ f)(x), y\rangle = \langle f(x), g^*(x)\rangle = \langle x, (f^* \circ g^*)(y)\rangle$$

Also existiert $(g \circ f)^* = f^* \circ g^*$.

Der Rest folgt durch Vertauschen von f und f^*. □

Definition 9.7. Ein Endomorphismus $f\colon V \to V$ heißt normal, falls der zu ihm adjungierte Endomorphismus f^* existiert und wenn $f \circ f^* = f^* \circ f$ gilt.
Entsprechend heißt eine Matrix $A \in \mathbb{C}^{n,n}$ normal, falls $AA^* = A^*A$.

F 9.8. *$f \in \operatorname{End}(V)$ ist genau dann normal, wenn f^* existiert und für alle $x, y \in V$ gilt: $\langle f(x), f(y)\rangle = \langle f^*(x), f^*(y)\rangle$*

Beweis. Aus $f \circ f^* = f^* \circ f$ folgt

$$\langle f(x), f(y)\rangle = \langle x, (f^* \circ f)(y)\rangle = \langle x, (f \circ f^*)(y)\rangle = \langle f^*(x), f^*(y)\rangle$$

Umkehrung gelte $\langle f(x), f(y)\rangle = \langle f^*(x), f^*(y)\rangle$. Dann folgt

$$\langle (f \circ f^*)(x), y\rangle = \langle f^*(x), f^*(y)\rangle = \langle f(x), f(y)\rangle = \langle f^* f(x), y\rangle$$

Da dies bei festem x für alle $y \in V$ gilt, folgt $(f \circ f^*)(x) = (f^* \circ f)(x)$. Dies gilt für alle $x \in V$, also $f \circ f^* = f^* \circ f$ □

F 9.9. *Für einen normalen Endomorphismus $f\colon V \to V$ gilt* $\ker f = \ker f^*$

Beweis. Nach Fakt 9.8 gilt für $x \in V$:

$\|f(x)\|^2 = \langle f(x), f(x)\rangle = \langle f^*(x), f^*(x)\rangle = \|f^*(x)\|^2$ also $f(x) = 0 \iff f^*(x) = 0$.

□

F 9.10. *Sei $f\colon V \to V$ ein normaler Endomorphismus. Dann haben f und f^* dieselben Eigenvektoren. Falls a ein Eigenvektor von f zum Eigenwert λ, dann ist a ein Eigenvektor von f^* zum Eigenwert $\overline{\lambda}$.*

Beweis. Nach Fakt 9.8 ist

$$\begin{aligned}\langle f(a) - \lambda a, f(a) - \lambda a\rangle &= \langle f(a), f(a)\rangle - \lambda\langle a, f(a)\rangle - \overline{\lambda}\langle f(a), a\rangle + \lambda\overline{\lambda}\langle a, a\rangle \\ &= \langle f^*(a), f^*(a)\rangle - \lambda\langle f^*(a), a\rangle - \overline{\lambda}\langle a, f^*(a)\rangle + \lambda\overline{\lambda}\langle a, a\rangle \\ &= \left\langle f^*(a) - \overline{\lambda}a, f^*(a) - \overline{\lambda}a\right\rangle\end{aligned}$$

Also gilt

$$f(a) = \lambda a \iff f^*(a) = \overline{\lambda}a$$

□

Satz 9.11 (Normalform für normale Abbildungen)**.** *Sei V ein unitärer Raum mit* $\dim V < \infty$*, sei $f \in \mathrm{End}(V)$. Dann sind äquivalent:*

1. *f ist normal.*
2. *Es gibt eine ON-Basis von V, die aus Eigenvektoren von f besteht.*
3. *Es gibt eine ON-Bais von V, bzgl. der die f gehörige Matrix eine Diagonalmatrix ist.*

Beweis. **1. $\Longrightarrow$ 2.: (Vollständige Induktion über n)** Sei f normal. Da V ein $\mathbb{C}$-Vektorraum ist, gibt es mindestens einen Eigenwert λ_1 von f mit Eigenvektor e_1 und $\|e_1\| = 1$.

Für $n = 1$ gilt Behauptung.

Gelte die Behauptung für die Dimension $n - 1 \geq 1$.

Sei $U := \{e_1\}^\perp$. Wegen Fakt 7.8 gilt $\dim U = n - 1$.

Für $x \in U$ gilt $\langle f(x), e_1\rangle = \langle x, f^*(e_1)\rangle = \left\langle x, \overline{\lambda}e_1\right\rangle = \lambda\langle x, e_1\rangle = 0$, da $x \in U \perp e_1$.

Also ist $f(x) \in U$ und somit $f(U) \subseteq U$. Also ist die Einschränkung $f|_U : U \to U$ ein normaler Endomorphismus eines unitären $(n-1)$ dimensionalen Vektorraum, also nach Induktionsannahme eine ON-Basis $\{e_1, \ldots, e_n\}$ aus Eigenvektoren von $f|_U$. Also ist $\{e_1, \ldots, e_n\}$ eine ON-Basis aus Eigenvektoren von f.

2. $\Longrightarrow$ **3.** klar

3. $\Longrightarrow$ **1.** Sei $D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ die zu f gehörige Matrix gehörige Matrix bezüglich einer ON-Basis $(e_1, \ldots, e_n)$. Dann ist nach Fakt 9.5 D^* die zu f gehörige Matrix bezüglich derselben Basis. Dann

$$DD^* = \begin{pmatrix} \lambda_1\overline{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \lambda_n\overline{\lambda_n} \end{pmatrix} = \begin{pmatrix} \overline{\lambda_1}\lambda_1 & & 0 \\ & \ddots & \\ 0 & & \overline{\lambda_n}\lambda_n \end{pmatrix} = D^*D$$

□

F 9.12 (Normalform für normale Matrizen)**.** *(Matizentheoretische Formulierung von 9.11) Sei $A \in \mathbb{C}^{n,n}$. Dann gibt es eine Matrix $S \in U(n)$ (d.h. $S^* = S^{-1}$), sodass $D = S^{-1}AS = S^*AS$ eine Diagonalmatrix ist.*

Beweis. Sei S die ON-Basis aus Eigenvektoren von A, also $S \in U(n)$, d.h. $S^* = S^{-1}$. Ferner für $S = (s_1, \ldots, s_n)$ ist

$$As_j = \lambda_j s_j \ (j = 1, \ldots, n) \iff AS = S \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} = SD,$$

also $S^{-1}AS = D$ □

Definition 9.13. $f \in \mathrm{End}(V)$ heißt selbstadjungiert, wenn die adjungierte Abbildung f^* existiert und $f = f^*$ gilt.

F 9.14. *$f \in \mathrm{End}(V)$ ist selbstadjungiert, falls für alle $x, y \in V$ gilt $\langle f(x), y\rangle = \langle x, f(y)\rangle$*

Beweis. klar nach Definition □

Definition 9.15. $A \in \mathbb{C}^{n,n}$ heißt eine Hermitesche Matrix, falls $A^* = A$ gilt.
In $\mathbb{R}^{n,n}$ bedeutet Hermitesch symmetrisch.

F 9.16. *Falls $\dim V < \infty$ und $B = \{e_1, \ldots, e_n\}$ eine ON-Basis ist, dann ist ein Endomorphismus $f : V \to V$ genau dann selbstadjungiert, wenn die zugehörige Matrix A bzgl. B Hermitisch (bzw symmetrisch, falls $\mathbb{K} := \mathbb{R}$)*

Beweis. klar. □

F 9.17. *Sei* $\dim V < \infty$ *und* V *ein unitärer Raum und* $f \in \mathrm{End}(V)$*. Dann sind äquivalent*

1. *f ist selbstadjungiert.*
2. *f ist normal und alle Eigenwerte von f sind reell.*

Beweis. **1.** $\Rightarrow$ **2.** f ist selbstadjungiert. Dann

$$f = f^* \implies f \circ f^* = f^2 = f^* \circ f \implies f \text{ ist normal.}$$

Sei a ein Eigenvektor von f zum Eigenwert λ. Dann ist a ein Eigenvektor von $f = f^*$ zum Eigenwert $\overline{\lambda}$ (Fakt 9.10). Also ist $\lambda = \overline{\lambda} \implies \lambda \in \mathbb{R}$.

2. $\Rightarrow$ **1.** Nach Satz 9.11 gibt es (wegen f normal) eine ON-Basis bzgl. der die zu f gehörige Matrix eine Diagonalmatrix $D = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$ ist. Alle Eigenwerte $a_{jj} \in \mathbb{R} \implies D = \overline{D} = D^*$, also $f = f^*$.

□

F 9.18. *Sei* $A \in \mathbb{R}^{n,n} \subseteq \mathbb{C}^{n,n}$*. Dann gilt für A als Matrix in $\mathbb{C}^{n,n}$ aufgefasst:*
Falls $x \in \mathbb{C}^n$ ein Eigenvektor von A zum Eigenwert $c \in \mathbb{C}$ ist, dann ist $\overline{x}$ ein Eigenvektor von A zum Eigenwert $\overline{c} \in \mathbb{C}$, wobei $\overline{x} = \overline{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}} = \begin{pmatrix} \overline{x_1} \\ \vdots \\ \overline{x_n} \end{pmatrix}$.
Falls A normal und $x \in \mathbb{C} \setminus \mathbb{R}$ ein Eigenvektor von A zum Eigenwert $c \in \mathbb{C}$, dann ist $\langle x, \overline{x} \rangle = 0$ ($\langle \cdot, \cdot \rangle$ Standardskalarprodukt in $\mathbb{C}$)

Beweis. $Ax = cx \implies A\overline{x} = \overline{A}\overline{x} = (\overline{Ax}) = \overline{cx}$. Also ist $\overline{x}$ eine Eigenvektor zum Eigenwert $\overline{c}$. Falls $A \in \mathbb{R}^{n,n}$ normal ist, dann ist $A^*A = A^TA = AA^T = AA^*$, also A auch als Matrix in $\mathbb{C}^{n,n}$ normal. Sei $x \in \mathbb{C}$ ein Eigenvektor zum Eigenwert $c \in \mathbb{C}$. Dann $\overline{c}\,\langle \overline{x}, x \rangle = \langle \overline{cx}, x \rangle = \langle \overline{Ax}, x \rangle = \langle A\overline{x}, x \rangle = \langle \overline{x}, A^*x \rangle \overset{9.10}{=} c\,\langle \overline{x}, x \rangle$, also wegen $\overline{c} \neq c$ ($c \neq \mathbb{R}$) folgt $0 = \langle x, \overline{x} \rangle = \overline{\langle \overline{x}, x \rangle}$. □

Satz 9.19 (Normalform für über $\mathbb{C}$ diagonalisierbare reelle Matrizen)**.** *Sei $A \in \mathbb{R}^{n,n}$ und A als Element von $\mathbb{C}^{n,n}$ diagonalisierbar. Dann gibt es eine Matrix $S \in \mathrm{GL}(n, \mathbb{R})$ für welche $S^{-1}AS$ die folgende Gestalt hat:*

$$\begin{pmatrix} d_1 & & & & & \mathbf{0} \\ & \ddots & & & & \\ & & d_k & & & \\ & & & \square_1 & & \\ & & & & \ddots & \\ \mathbf{0} & & & & & \square_m \end{pmatrix} \quad \text{wobei } \square_\mu = \begin{pmatrix} a_\mu & b_\mu \\ -b_\mu & a_\mu \end{pmatrix} \text{ für } \mu = 1, \ldots, m$$

mit $b_\mu \neq 0$, $k + 2m = n$. Dabei sind $d_1, \ldots, d_k$ die reellen Eigenwerte von A und $a_\mu \pm ib_\mu$ die komplexen Eigenwerte von A.

Beweis. Das charakteristische Polynom $\chi_A = \det(XE - A)$ zerfällt über $\mathbb{C}$ in Linearfaktoren. Da A eine reelle Matrix ist, ist $\det(XE - A)$ ein Polynom mit reellen Koeffizienten und die nichtreellen Nullstellen treten in Paaren konjugiert komplexer Nullstellen auf. Wir können also die Nullstellen (mit Berücksichtigung der Vielfachheit) sortieren als $d_1, \ldots, d_k, a_1 + ib_1, a_1 - ib_1, \ldots, a_m + ib_m, a_m - ib_m$, wobei $k + 2m = n$ und die d_μ, a_μ, b_μ reell sind und $b_\mu \neq 0$. Da A über $\mathbb{C}$ diagonalisierbar ist, gibt es eine Basis von Eigenvektoren und die geometrische und algebraische Vielfachheit stimmen überein. Falls $u_1, \ldots, u_r$ eine Basis von Eigenvektoren von A zu einem nicht reellen Eigenwert $a + ib$ von A ist, dann sind (nach Fakt 9.18) $\overline{u_1}, \ldots, \overline{u_r}$ Eigenvektoren von A zum Eigenwert $a - ib$. Sie bilden sogar eine Basis des Eigenraumes zum Eigenwert $a - ib$. Da A über $\mathbb{C}$ diagonalisierbar ist, ist $\mathbb{C}^n$ die direkte Summe der Eigenräume. Wir erhalten eine Basis der Form $s_1, \ldots, s_k, t_1, \overline{t_1}, \ldots, t_m, \overline{t_m}$ mit $s_v \in V$ zu $t_m \in V$ Eigenvektoren zu $a_\mu + ib_\mu$, $\overline{t_\mu} \in V$ Eigenvektoren zu $a_\mu - ib_\mu$. (Beachte: μ als Index der Eigenwerte läuft über einen anderen Bereich als als Index der Basisvektoren!) Definiere nun $u_\mu := \frac{1}{2}(t_\mu + \overline{t_\mu}) = \mathrm{Re}(t_\mu)$, $v_\mu = \frac{1}{2i}(t_\mu - \overline{t_\mu}) = \mathrm{Im}(t_\mu)$. $S := (s_1, \ldots, s_k, u_1, v_1, u_2, v_2, \ldots, u_m, v_m)$ eine Basis von $\mathbb{C}^n$ (Erzeugendensystem klar, lineare Unabhängigkeit ebenfalls klar).

$$\text{Nun ist } S^{-1}AS = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_k & & & \\ & & & \boxed{\begin{matrix} a_1 & b_1 \\ -b & a_1 \end{matrix}} & & \\ & & & & \ddots & \end{pmatrix}, \text{ denn}$$

$$\begin{aligned} Au_\mu &= \frac{1}{2}(At_\mu + A\overline{t_\mu}) = \frac{1}{2}(a_\mu + ib_\mu)t_\mu + \frac{1}{2}(a_\mu - ib_\mu)\overline{t_\mu} \\ &= \frac{1}{2}a_\mu(t_\mu + \overline{t_\mu}) + \frac{i}{2}b_\mu(t_\mu - \overline{t_\mu}) = a_\mu u_\mu - b_\mu v_\mu \\ Av_\mu &= \frac{1}{2i}(At_\mu - A\overline{t_\mu}) = \frac{1}{2i}(a_\mu + ib_\mu)t_\mu - \frac{1}{2i}(a_\mu - ib_\mu)\overline{t_\mu} \\ &= \frac{1}{2}b_\mu(t_\mu + \overline{t_\mu}) + \frac{1}{2i}a_\mu(t_\mu - \overline{t_\mu}) = b_\mu u_\mu + a_\mu v_\mu \qquad \square \end{aligned}$$

Satz 9.20 (Normalform normaler Endomorphismen auf euklidischem Vektorraum)**.** *Sei V ein euklidischer Vektorraum mit* $\dim = n < \infty$. *Sei* $f \in \mathrm{End}(V)$

(a) Dann sind äquivalent:

- *f ist normal.*
- *Es gibt eine ON-Basis von V bezüglich der die zu f gehörige*

Matrix die folgende Gestalt (Normalform) hat:

$$\begin{pmatrix} d_1 & & & & & & \mathbf{0} \\ & \ddots & & & & & \\ & & d_k & & & & \\ & & & \square_1 & & & \\ & & & & \ddots & & \\ \mathbf{0} & & & & & & \square_m \end{pmatrix} \tag{1}$$

wobei $\square_\mu = \begin{pmatrix} a_\mu & b_\mu \\ -b\mu & a_\mu \end{pmatrix}$, $b_\mu \neq 0$, $\mu = 1, \ldots, m, k + 2m = n$

(b) In der Matrix gemäß 1 sind $d_1, \ldots, d_k$ die Eigenwerte von f, $a_\mu \pm ib_\mu$ die nichtreellen Nullstellen des charakteristischen Polynoms $\chi_f = \det(X \operatorname{id} - f)$

Beweis. Sei A die Matrix zu f bezüglich einer beliebigen ON-Basis von V. A ist als normale (reelle) Matrix nach Fakt 9.11 über $\mathbb{C}$ diagonalisierbar bezüglich einer ON-Basis über $\mathbb{C}$ und von der Form $s_1, \ldots, s_k, t_1, \overline{t_1}, \ldots, t_m, \overline{t_m}$. Wie im Beweis von Satz 9.19 ist nun ($\left\|t_\mu + \overline{t_\mu}\right\| = \sqrt{2}$ (da $\langle t_\mu, \overline{t_\mu} \rangle = 0$, $\|t_\mu\| = \left\|\overline{t_\mu}\right\| = 1$). Sei nun

$$u_\mu = \frac{1}{\sqrt{2}}(t_\mu + \overline{t_\mu}), \quad v_\mu = \frac{1}{\sqrt{2}i}(t_\mu - \overline{t_\mu})$$

Dann ist $\|u_\mu\| = \|v_\mu\| = 1$

$$\langle u_\mu, v_\mu \rangle = \frac{i}{2} \left\langle t_\mu + \overline{t_\mu}, t_\mu - \overline{t_\mu} \right\rangle = \frac{i}{2}(\underbrace{\|t_\mu\|^2}_{=1} - \underbrace{\left\|\overline{t_\mu}\right\|^2}_{=1}) = 0$$

$S = (s_1, \ldots, s_k, u_1, v_1, \ldots, u_m, v_m)$ ist gesuchte ON Basis bezüglich der die zu f gehörige Matrix die Form (1) hat.
Der zweite Teil ist klar, denn

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a^2 + b^2 & 0 \\ 0 & a^2 + b^2 \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

$\implies AA^T = A^T A \implies f$ normal (Basis ist ON-Basis). □

Geometrische Interpretation der $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ - Kästchen:
Falls $a^2 + b^2 = 1$, dann gibt es genau ein $\alpha \in (-\pi, \pi]$ mit $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{smallmatrix}\right)$, also Drehung um α.
Falls $b \neq 0$ ist $\alpha \neq 0, \pi$. Durch Basistransformation $(e_1, e_2) \mapsto (e_1, -e_2)$ wird $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ in $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ überführt, also α in $-\alpha$.
Allgemein ist $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ eine Drehstreckung mit Streckungsfaktor $\sqrt{a^2 + b^2}$ und Drehwinkel $\alpha = \arccos a$ (falls $b \geq 0$), $\alpha = -\arccos a$ (falls $b \leq 0$).
Abbildung in $\mathbb{C}$: $z = (x + iy) \mapsto (a + ib)(x + iy) = ax - by + i(bx + ay)$, $a + ib = re^{i\alpha}$, $r = \sqrt{a^2 + b^2}$.
Sei f ein normaler Endomorphismus des $\mathbb{R}^n$. Dann lässt sich der $\mathbb{R}^n$ als direkte Summe paarweise orthogonaler 1- und 2-dimensionale Unterräume zerlegen, auf denen f jeweils als Streckung (Faktor $d_j \in \mathbb{R}$) auf der 1-dimensionalen Unterräumen und als Drehstreckung auf den 2-dimensionalen Unterräumen operiert.

F 9.21 (Spezialfall Normalform für orthogonale Abbildungen)**.** *Sei A eine orthogonale Matrix. Alle komplexen Nullstellen des charakteristischen Polynoms haben Betrag 1, also die reellen Eigenwerte $d_1, \ldots, d_k \in \{1, -1\}$, den Paaren nicht reeller konjugiert komplexer Nullstellen entspricht eine Drehmatrix.*

Satz 9.22. *Sei $f \in \mathrm{End}(V)$, $\dim V = n < \infty$, V unitärer oder euklidischer Vektorraum. Dann sind äquivalent:*

(i) f ist selbstadjungiert (d.h. $f = f^*$)

(ii) Es gibt eine ON-Basis von V aus Eigenvektoren von f zu reellen Eigenwerten.

(iii) Es gibt eine ON-Basis von V bzgl. der f durch eine reelle Diagonalmatrix dargestellt wird.

(iv) Es gibt eine ON-Basis von V bzgl der f durch eine Hermitesche (bzw. symmetrische (falls $\mathbb{K} = \mathbb{R}$)) Matrix A dargestellt wird (d.h. $A = A^*$)

(v) Bezüglich jeder ON-Basis von V wird f durch eine Hermitesche Matrix dargestellt.

(vi) f ist normal und das charakteristische Polynom von f hat nur reelle Nullstellen.

Beweis. Folgende Implikationen sind offensichtlich (mit 9.5 Matrix zu f^* ist A^* bezüglich einer ON-Basis) ii $\Longrightarrow$ iii $\Longrightarrow$ iv $\Longrightarrow$ i $\Longrightarrow$ v $\Longrightarrow$ iv
„i $\Longleftrightarrow$ vi“: Sei A die Matrix von f bzgl. einer ON-Basis. Dann ist A^* die Matrix von f^* Nach 9.17 gilt i $\Longleftrightarrow$ vi für A, also für f.
„i $\Longrightarrow$ ii“: Für $\mathbb{K} := \mathbb{R}$ nach 9.20 (und wegen i $\Longrightarrow$ iv hat χ_f nur reelle Nullstellen). Für $\mathbb{K} := \mathbb{C}$ nach 9.11 (und wegen i $\Longrightarrow$ iv hat χ_f nur reelle Nullstellen) □

Definition 9.23. $f \in \mathrm{End}(V)$ heißt anti-selbstadjungiert, falls $f = -f^*$
Eine Matrix $A \in \mathbb{C}^{n,n}$ heißt schief-Hermitesch, falls $A = -A^*$ bzw. schief-symmetrisch, falls $A \in \mathbb{R}^{n,n}$ und $A^T = -A$

F 9.24. *Falls $\dim V = n < \infty$, dann ist f anti-selbstadjungiert genau dann, wenn für die zugehörige Matrix bzgl. einer ON-Basis gilt $A^* = -A$, d.h. für $\mathbb{K} := \mathbb{C}$ schief-Hermitesch, für $\mathbb{K} = \mathbb{R}$ schief-symmetrisch.*

Beweis. Klar mit 9.5. □

F 9.25. *Falls* $\dim V = n < \infty$*, dann gilt* f *ist genau dann anti-selbstadjungiert, wenn* f *normal ist und alle Nullstellen des charkteristischen Polynoms* χ_f *in* $i\mathbb{R}$ *sind (rein imaginär).*

Beweis. Klar mit Satz 9.24 bzw. Satz 9.11. □

F 9.26. *Normalform für* $\mathbb{K} = \mathbb{R}$*: Falls* $f \in \mathrm{End}(V)$ *anti-selbst-adjungiert ist, dann gibt es eine ON-Basis von* V *bezüglich der die Matrix die Gestalt*

$$A = \begin{pmatrix} 0 & & & & & \mathbf{0} \\ & \ddots & & & & \\ & & 0 & & & \\ & & & \square_1 & & \\ & & & & \ddots & \\ \mathbf{0} & & & & & \square_m \end{pmatrix} \quad \textit{mit} \quad \square_\mu = \begin{pmatrix} 0 & b_\mu \\ -b_\mu & 0 \end{pmatrix},\ b_\mu \neq 0$$

Folgerung: Falls $f \in \mathrm{End}(V)$*,* $\mathbb{K} = \mathbb{R}$ *anti-selbstadjungiert ist, dann ist* $\mathrm{Rang}\, f$ *gerade* $(= 2m)$*, insbesondere ist für* n *ungerade* f *nicht regulär.*

Satz 9.27. *Jede Isometrie des* $\mathbb{R}$ *lässt sich das Komostion von höchstens* $(n+1)$ *Spiegelungen an Hyperebenen schreiben.*

Beweis. Übung □

Satz 9.28. *Jede Isometrie des* $\mathbb{R}^n$ *lässt sich Komposition von zwei Spiegelungen an affinen Unterräumen schreiben.*

9.1 Eigenschaften normaler Matrizen

Die Menge der orthogonalen Matrizen ist kein linearer $\mathbb{R}-$Unterraum von $\mathrm{End}(V)$. Gegenbeispiel:

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

Die Summanden sind normal, aber die Summe ist nicht normal.
Schließe daraus, was du willst:

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

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

Die symmetrische Matrizen sind keine Untergruppe von $GL(V)$ unter Multiplikation (Komposition). Gegenbeispiel:

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

Folgere daraus, was du willst:

$$\begin{pmatrix}-2 & 1\\ 0 & -2\end{pmatrix}\begin{pmatrix}-2 & 0\\ 1 & -2\end{pmatrix} = \begin{pmatrix}5 & -2\\ -2 & 4\end{pmatrix} \neq \begin{pmatrix}4 & -2\\ -2 & 5\end{pmatrix} = \begin{pmatrix}-2 & 0\\ 1 & -2\end{pmatrix}\begin{pmatrix}-2 & 1\\ 0 & -2\end{pmatrix}$$

Die schiefsymmetrischen Matrizen sind keine Untergruppe von $GL(V)$ unter Multiplikation (Komposition). Gegenbeispiel:

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

Selbstadjungierte und anti-selbstadjungierte Matrizen sind jeweils lineare $\mathbb{R}$-Unterräume von $\mathrm{End}(V)$, denn

$$\begin{aligned}&(f+g)^* = f^* + g^*, \text{ also } f^* = f \wedge g^* = g\\ \Longrightarrow\ &(f+g)^* = f+g \text{ und } f^* = -f \wedge g^* = -g \implies (f+g)^* = -f-g\end{aligned}$$

Für $\lambda \in \mathbb{R}$ ist $(\lambda f)^* = \overline{\lambda} f^* = \lambda f^*$, also bilden die selbstadjungierten bzw. die anti-selbstadjungierten Endomorphismen einen linearen $\mathbb{R}$-Unterraum.
Für $f \neq 0$, $\mathbb{K} = \mathbb{C}$, $\lambda \in \mathbb{R}$ ist λf nicht selbstadjungiert: $(\lambda f)^* = \overline{\lambda} f^* = \lambda f = \frac{\overline{\lambda}}{\lambda}(\lambda f)$, aber $\frac{\overline{\lambda}}{\lambda} \neq 1$

9.2 Normale Endomorphismen des $\mathbb{R}^2$

1. Fall 2 reelle Eigenwerte a, b, Normalform $\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}$: Streckung in zwei zueinander ortogonalen Richtungen mit Streckungsfaktor a, b.

2. Fall Ein Paar konjugiert komplexer Eigenwerte $a + ib = re^{\mp i\alpha}$ (der komplexen Erweiterungen) reelle Normalform $\begin{pmatrix}a & b\\ -b & a\end{pmatrix}$: Drehstreckung mit Streckungsfaktor $\sqrt{a^2+b^2} = r$ und Winkel α bzw. $-\alpha$

weitere Betrachtungen siehe Tabelle.

10 Bilinearformen

Definition 10.1. Seien V, WK-Vektorräume. Eine Abbildung $\beta\colon V \times W \to K$ heißt eine Bilinearform, falls β linear in beiden Komponenten ist, das heißt

$$\begin{aligned}\beta(x_1 + \lambda x_2, y) &= \beta(x_1, y) + \lambda\beta(x_2, y)\\ \beta(x, \lambda y_1 + y_2) &= \lambda\beta(x, y_1) + \beta(x, y_2)\end{aligned}$$

für alle $x_1, x_2, x \in V$, $y_1, y_2, y \in W$, $\lambda \in K$

Definition 10.2. β heißt eine Bilinearform auf V, falls $V = W$.
β heißt symmetrisch, falls $V = W$ und $\beta(x,y) = \beta(y,x)$ für alle $x, y \in V$.
β heißt nicht ausgeartet (auch nicht degeneriert), falls

$(\forall y \in W : \beta(x,y) = 0 \implies x = 0)$ und $(\forall x \in W : \beta(x,y) = 0 \implies y = 0)$

Definition 10.3. Die Menge der Bilinearformen $\beta \colon V \times W \to K$ wird mit $\mathrm{Bil}(V,W)$ bezeichnet. Dies ist in offensichtlicher Weise ein K-Vektorraum (Unterraum von $K^{V \times W}$).

Definition 10.4. Seien V, W K-Vektorräume mit $\dim V = n < \infty$ und $\dim W = m < \infty$. $\beta \colon V \times W \to K$ sei eine Bilinearform. Seien $C = (v_1, \dots v_n)$ bzw. $D = (w_1, \dots w_m)$ Basen von V bzw. W. Dann heißt die $(n \times m)$ - Matrix $B := (\beta(v_i, w_i))_{i,j}$ die (Struktur-)Matrix der Bilinearform β bezüglich der Basen C und D. Falls $V = W$, $C = D$ heißt B die (Struktur-)Matrix von β bezüglich C.

F 10.5. *Seien c_C bzw. c_D die Koordinatenabbildung für die Basen C bzw. D und sei B die Strukturmatrix von β bezüglich C und D. Dann gilt:*

$$\beta(x,y) = c_C(x)^T B c_D(y) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}^T B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

wobei $c_C(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $c_D(y) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ *mit* $x = \sum_{i=1}^n x_i v_1$, $y = \sum_{i=1}^m y_i w_i$
Also insbesondere für die Standardbasen von $V = K^n$, $W = K^m$ ist $\beta(x,y) = x^T B y$.
Umgekehrt ist für jede *$(n \times m)$-Matrix B die Abbildung $\beta(x,y) = x^T B y$ $(x \in K^n,\ y \in K^m)$ eine Bilinearform $\beta \colon K^n \times K^m \to K$.*

Beweis. Die erste Gleichung gilt, da β eine Bilinearform ist:

$$\beta\left(\sum_{i=1}^n x_i v_1, \sum_{i=1}^m y_i w_i\right) = \sum_{i=1}^n \sum_{j=1}^m x_i y_i \beta(v_i, w_j) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}^T B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \quad \square$$

F 10.6. *Sei* $\dim V = n < \infty$, $\dim W = m < \infty$, *C, D Basen von V, bzw. W, B bezeichne die Matrix von β bzgl. C und D.*

a) Die Abbildung $\mathrm{Bil}(V,W) \to K^{n,m} \cong K^{n\cdot m}, \beta \mapsto B$ *ist eine lineare Abbildung.*

b) Ferner gilt: β ist nicht-ausgeartet genau dann, wenn $\operatorname{Rang} B = m = n$

c) Falls $V = W$ und $C = D$, dann ist β ist genau dann symmetrisch, wenn B symmetrisch ist.

Beweis. a, c klar, b: nachrechnen (sehr einfach) □

Beispiel. Das Standardskalarprodukt $\langle\cdot,\cdot\rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ hat bezüglich der Standardbasis die Einheitsmatrix E als Strukturmatrix, denn $\langle e_i, e_j\rangle = \delta_{ij}$. Sei V ein endlich-dimensionaler euklidischer Raum mit Standardskalarprodukt $\langle\cdot,\cdot\rangle$ und C eine Orthonormalbasis von V, dann ist die Strukturmatrix von $\langle\cdot,\cdot\rangle$ bezüglich C die Einheitsmatrix.
Achtung! Das Skalarprodukt in unitären Räumen ($K = \mathbb{C}$) ist *keine* Bilinearform, denn $\langle x, iy\rangle = -i\langle x, y\rangle \neq i\langle x, y\rangle$, falls $\langle x, y\rangle \neq 0$.

Satz 10.7. *Sei B die Matrix einer Bilinearform $\beta\colon V \times W \to K$ bezüglich der Basen $C = (v_1, \ldots, v_n)$ von V, $D = (w_1, \ldots, w_m)$ von W. Seien Basen $C' = (v'_1, \ldots, v'_n)$ von V, $D' = (w'_1, \ldots, w'_m)$ von W und sei B' die Matrix von β bezüglich C' und D' und seien S die Übergangsmatrix von C nach C', T die Übergangsmatrix von D nach D'. Dann gilt $B' = S^T BT$. Insbesondere für $V = W$, $C = D$, $C' = D'$, also $S = T$: $B' = S^T BS$*

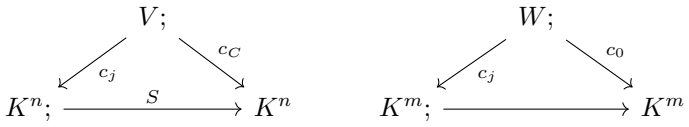


Abbildung 1: Diagramm 10 zu Satz 10.7

Beweis. Also mit dem Diagramm 10

$$\begin{aligned}\beta(x,y) &= (c_C(x))^T B(c_D(y)) = (Sc_{C'}(x))^T B(Tc_{D'}(y))\\ &= (c_{C'}(x))^T \underbrace{(S^T BT)}_{=B'} c_{D'}(y)\end{aligned}$$ □

Definition 10.8. Zwei Matrizen B, $B' \in K^{n,n}$ heißen kongruent, geschrieben $B \simeq B'$, falls es ein $S \in \mathrm{GL}(n,K)$ gibt mit $B' = S^T BS$.

F 10.9. *$\simeq$ ist eine Äquivalenzrelation auf $K^{n,n}$.*

Beweis. Beweis: klar (einfaches nachrechnen) □

Definition 10.10. Wenn $\beta\colon V \times W \to K$ eine Bilinearform ist, dann bezeichne $\beta^T\colon W \times V \to K$ die durch $\beta^T(y,x) := \beta(x,y)$ definierte Bilinearform.

F 10.11. *Wenn B die Matrix von β bzgl. Basen C von V, D von W ist, dann ist B^T die Matrix von β^T bzgl. Basen D von W und C von V.*

Beweis. klar □

Satz 10.12 (Existenz einer Orthogonalbasis für symmetrische Bilinearformen)**.** *Sei $B \in K^{n,n}$ symmetrisch und* $\operatorname{char}(K) \neq 2$*. Dann gibt es eine invertierbare Matrix S, sodass S^TBS eine Diagonalmatrix ist, d.h. jede symmetrische Matrix ist kongruent zu einer Diagonalmatrix (falls* $\operatorname{char}(K) \neq 2$*).*

Beweis. algorithmisch/ rekursiv, ähnlich dem Gaußalgorithmus
Sei $B_0 := B$. Sei $B_\nu = S_\nu^T B S_\nu = (a_{ij})_{i,j}$ eine Matrix in welcher in mindestens ν Zeilen (und Spalten wegen $B_\nu^T = B_\nu$) alle Elemente außerhalb der Diagonalen gleich 0 sind.

1. Fall Es gibt eine Zeile, sagen wir die k-te Zeile $(a_{k1}, \ldots, a_{kk}, \ldots, a_{kn})$ in welcher $a_{kk} \neq 0$ und (mindestens) eine weiteres $a_{ki} \neq 0$ ist. Dann definiere

$$B_{\nu+1} := T^T B_\nu T = (S_\nu T)^T B \underbrace{S_\nu T}_{:=S_{\nu+1}} = (\tilde{a}_{ij})_{i,j}$$

T is gegeben durch

$$t_{kj} := -\frac{a_{kj}}{a_{kk}} \text{ für } j \neq k, \qquad t_{kk} := 1, \qquad t_{ij} = \delta_{ij} \text{ für } i \neq k$$

$$T^T B_\nu T = T^T \cdot \begin{pmatrix} & \vdots & & & \\ & \vdots & & & \\ \ldots & a_{kk} & \ldots & a_{kj} & \ldots \\ & \vdots & & & \\ & a_{jk} & & & \end{pmatrix} \begin{pmatrix} 1 & & & & \mathbf{0} \\ & \ddots & & & \\ 1 & \ldots & \underbrace{t_{kk}}_{=1} & \ldots & -\frac{a_{kj}}{a_{kk}} \\ & & & \ddots & \\ \mathbf{0} & & & & 1 \end{pmatrix}$$

Seien $B_\nu T = (\widehat{a}_{ij})_{i,j}$, $T^T B_\nu T = (\tilde{a}_{ij})_{ij}$

$$\widehat{a}_{ij} = a_{ij} + t_{kj} \cdot a_{ik} = a_{ij} - \frac{a_{ik}a_{kj}}{a_{kk}} \qquad \text{für } i \neq k, j \neq k$$

$$\widehat{a}_{ik} = a_{ik} \qquad \text{für } i \neq k$$

$$\widehat{a}_{ki} = a_{ki} + t_{ki} \cdot a_{kk} = 0 \qquad \text{für } i \neq k$$

$$\widehat{a}_{kk} = a_{kk}$$

$$\tilde{a}_{ij} = \widehat{a}_{ij} + t_{ki} \cdot \widehat{a}_{kj} = a_{ij} - \frac{a_{ik}a_{jk}}{a_{kk}} - 0$$

$$= a_{ji} - \frac{a_{jk}a_{ik}}{a_{kk}} = \tilde{a}_{ji} \qquad \text{für } i \neq k, j \neq k$$

$$\tilde{a}_{ik} = \widehat{a}_{ik} + t_{ki}\widehat{a}_{kk} = a_{ik} - \frac{a_{ki}a_{kk}}{a_{kk}} = 0 \qquad \text{für } i \neq k$$

$$\tilde{a}_{ki} = \widehat{a}_{ki} = 0 = a_{ik} \qquad \text{für } i \neq k$$

$$\tilde{a}_{kk} = \widehat{a}_{kk} = a_{kk}$$

Insbesondere ist $B_{\nu+1}$ auch symmetrisch und es bleiben alle Zeilen, die kein Element $\neq 0$ außerhalb der Diagonalen hatten, erhalten. Mit der k-ten Zeile haben wir nun eine weitere Zeile erhalten, in der alle Elemente außerhalb der Diagonalen gleich 0 sind.

2. Fall Der 1. Fall trifft nicht zu, d.h. in jeder Zeile von B_ν sind alle Elemente außerhalb der Diagonalen gleich 0 oder das Diagonalelement gleich 0. Falls es kein a_{ij} gibt mit $i \neq j$ und $a_{ij} \neq 0$, dann ist B_ν eine Diagonalmatrix und $S = S_\nu$ die gesuchte Matrix.

Sei nun $a_{ij} \neq 0$ und $a_{ii} = a_{jj} = 0$. Dann sei $(\tilde{a}_{ij})_{i,j} = \tilde{B}_\nu = U^T B_\nu U$ mit $U := Q_{ij}^{(1)}$ (Elementarmatrix)

Erstes U addiert die j-te Zeile zur i-ten Zeile.

Zweites U addiert die j-te Spalte zur i-ten Spalte.

$$U = (u_{kl})_{k,l} \text{ mit } a_{kl} = \begin{cases} 1 & \text{falls } k = l \text{ oder } k = i, l = j \\ 0 & \text{sonst} \end{cases}$$

Also $\tilde{a}_{kl} = a_{kl}$ für $k \neq i$ und $l \neq i$ und $\tilde{a}_{ik} = a_{ik} + a_{jk} = \tilde{a}_{ki}$ für $k \neq i$ und $\tilde{a}_{ii} = a_{ij} + a_{ji} = 2a_{ij} \neq 0$, da $a_{ij} \neq 0$ (nach Vorausetzung) und $2 \neq 0$, da $\text{char}(K) \neq 2$ nach Voraussetzung. Insbesondere bleiben alle Zeilen, die kein Element $\neq 0$ außerhalb der Diagonale hatten, erhalten. Damit ist der 1. Fall anwendbar auf die i-te Zeile von $\tilde{B}_\nu$. Mit der dort definierten Matrix (angewendet auf $\tilde{B}_\nu$) ergibt sich

$$B_{\nu+1} = T^T \tilde{B}_\nu T = T^T U^T B_\nu U T = (S_\nu U T)^T B (\underbrace{S_\nu U T}_{= S_{\nu+1}}) \qquad \square$$

In der Vorlesung wurde ein Beispiel parallel vorgerechnet. Dieses ist hier nicht dabei. Wenn du Lust hast, es aufzuschreiben, fühle dich herzlich dazu eingeladen!

F 10.13. *Sei V ein K-Vektorraum mit* $\dim V < \infty$, $\mathrm{char}(K) \neq 2$, *β eine symmetrische Bilinearform auf V. Dann existiert eine Basis C von V sodass die Matrix B von β bzgl. C eine Diagonalmatrix ist.*

Definition 10.14. Bezeichne $[a_1, \ldots, a_n] := \begin{pmatrix} a_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & a_n \end{pmatrix}$

Wir wissen, dass für $B \in K^{n,n}$ mit $B = B^T$ gilt: Falls $\mathrm{char}(K) \neq 2$, dann gibt es $a_1, \ldots, a_n$ mit $B \simeq [a_1, \ldots, a_n]$
Frage: Wann gilt: $[a_1, \ldots, a_n] \simeq [b_1, \ldots, b_n]$?

F 10.15. *Für $t_1, \ldots, t_n \in K \backslash \{0\}$ gilt $[a_1, \ldots, a_n] \simeq [a_1 t_1^2, \ldots, a_n t_n^2]$*

Beweis. $\begin{pmatrix} a_1 t_1^2 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & a_n t_n^2 \end{pmatrix} = \begin{pmatrix} t_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & t_n \end{pmatrix} \begin{pmatrix} a_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & a_n \end{pmatrix} \begin{pmatrix} t_1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & t_n \end{pmatrix}$ □

Satz 10.16. $B \simeq C \Rightarrow \mathrm{Rang}\, B = \mathrm{Rang}\, C$

Beweis. $B \simeq C \overset{Def.}{\Longrightarrow} \exists S$ invertierbar: $C = S^T B S$ wegen S invertierbar ist $\mathrm{Rang}\, B = \mathrm{Rang}\, C$. □

F 10.17. *(Kürzungssatz von Witt): Seien $1 \leq k \leq n$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in K$, $\mathrm{char}\, K \neq 2$ Dann gilt: Aus $[a_1, \ldots, a_k, a_{k+1}, \ldots, a_n] \simeq [b_1, \ldots, b_k, b_{k+1}, \ldots, b_n]$ und $[a_1, \ldots, a_k] \simeq [b_1, \ldots, b_k]$ folgt $[a_{k+1}, \ldots, a_n] \simeq [b_{k+1}, \ldots, b_n]$*

Beweis. wird weggelassen (vgl. z.B. F. Lorenz, Lineare Algebra II) □

F 10.18. *Sei K ein Körper mit* $\mathrm{char}(K) \neq 2$, *in dem die Gleichung $x^2 = a$ für alle $a \in K$ eine Lösung hat (also z.B.: $K := \mathbb{C}$)*

(i) Dann gilt für jede symmetrische *Matrix $B \in K^{n,n}$, dass $B \simeq [\underbrace{1, \ldots, 1}_{\mathrm{Rang}\, B}, \underbrace{0, \ldots, 0}_{n - \mathrm{Rang}\, B}]$*

(ii) Für alle symmetrischen Matrizen $B, C \in K^{n,n}$ gilt $B \simeq C \Leftrightarrow \mathrm{Rang}\, B = \mathrm{Rang}\, C$

Beweis. (i) Nach Satz 10.12 ist $B \simeq [a_1, \dots, a_n]$, o.B.d.A $a_1, \dots, a_k \neq 0$, $a_{k+1} = \cdots = a_n = 0$, $k = \operatorname{Rang} B$ (nach 10.16). Nach Vorausetzung gibt es $t_i \in K$ mit $t_i^2 = \frac{1}{a_i}$ für $i = 1, \dots k$ Nach 10.15 ist $[a_1, \dots, a_n] \simeq [a_1 t_1^2, \dots, a_k t_k^2, 0, \dots, 0] = [\underbrace{1, \dots, 1}_{\operatorname{Rang} B}, 0, \dots, 0]$ $(S = [t_1, \dots, t_k, 1, \dots, 1])$.

(ii) „⇒“10.16
„⇐“nach a)

□

Satz 10.19 (Trägheitssatz von Sylvester)**.** *Seien B, $C \in \mathbb{R}^{n,n}$ symmetrische Matrizen, Dann gilt: $B \simeq C$ is äquivalent dazu, dass B und C dieselbe Anzahl n_+ von positiven Eigenwerten und n_- von negativen Eigenwerten haben (jeweils unter Berücksichtigung der Vielfachheiten).*
Insbesondere gilt:

$$B \simeq [\underbrace{1, \dots, 1}_{n_+}, \underbrace{-1, \dots, -1}_{n_-}, \underbrace{0, \dots, 0}_{n_0}]$$

mit $n_+ + n_- + n_0 = n$ und $n_+ + n_- = \operatorname{Rang} B$

Beweis. „⇐“Sei $B \in \mathbb{R}^{n,n}$ symmetrisch. Nach Fakt 9.12 gibt es $S \in O(n)$ sodass $S^T B S = S^{-1} B S$ eine Diagonalmatrix $[d_1, \dots, d_n]$ ist. Dabei sind die d_i die Eigenwerte von B. O.B.d.A. seien $d_1, \dots d_{n_+} > 0$, $d_{n_+ + 1}, \dots, d_{n_+ + n_-} < 0$, die übrigen $d_i = 0$. Damit ist

$$\begin{aligned} B \simeq [d_1, \dots, d_n] \simeq \Bigg[& d_1 \cdot \left(\frac{1}{\sqrt{d_1}}, \right), \dots, d_{n_+} \cdot \left(\frac{1}{\sqrt{d_{n_+}}} \right), \\ & d_{n_+ + 1} \cdot \left(\frac{1}{\sqrt{|d_{n_+ + 1}|}} \right), \dots, d_m \cdot \left(\frac{1}{\sqrt{|d_m|}} \right) \Bigg] \\ = [\underbrace{1, \dots, 1}_{n_+}, & \underbrace{-1, \dots, -1}_{n_-}, \underbrace{0, \dots, 0}_{n_0}] \end{aligned}$$

(mit $m = n_+ + n_-$)
„⇒“: Wegen „⇐“und Fakt 10.16 reicht es zu zeigen

$$[\underbrace{1, \dots, 1}_{n_+}, \underbrace{-1, \dots, -1}_{n_-}, \underbrace{0, \dots, 0}_{n_0},] \simeq [\underbrace{1, \dots, 1}_{\tilde{n}_+}, \underbrace{-1, \dots, -1}_{\tilde{n}_-}, \underbrace{0, \dots, 0}_{n_0}] \implies n_+ = \tilde{n}_+$$

(und $n_- = \tilde{n}_-$ folgt dann, da dann $n_- = n - n_+ - n_- = 0$).
O.B.d.A. $n_+ \geq \tilde{n}_+$. Angenommen $n_+ > \tilde{n}_+$, dann folgt nach Satz 10.17:

$$\tilde{A} = [\underbrace{1, \dots, 1}_{n_+}] \simeq [\underbrace{1, \dots, 1}_{\tilde{n}_+}, \underbrace{-1, \dots, -1}_{n_+ - \tilde{n}_+}] = \tilde{B}$$

Die linke Seite ist positiv definit, d.h. $x^T \tilde{A} x = x^T x > 0$ für alle $x \neq 0$, aber die rechte Seite nicht. Beispielsweise gilt $\begin{pmatrix} 0 & \dots & 0 & 1 \end{pmatrix} \tilde{B} \begin{pmatrix} 0 & \dots & 0 & 1 \end{pmatrix}^T = -1$. Dies ist ein Widerspruch zu $\tilde{A} \simeq \tilde{B}$ □

F 10.20. *Für jede symmetrische Bilinearform β auf einem $\mathbb{R}$-Vektorraum mit $\dim V = n < \infty$ gibt es eindeutig bestimmte Zahlen n_+, n_-, n_0 mit $n_+ + n_- + n_0 = n$, sodass es eine Basis von V gibt, sodass die Matrix von β bzgl. dieser Basis die Form $[\underbrace{1,\dots,1}_{n_+},\underbrace{-1,\dots,-1}_{n_-},\underbrace{0,\dots,0}_{n_0}]$ hat.*

Beweis. Klar mit Fakt 10.20. □

Definition 10.21. Sei β eine symmetrische Bilinearform auf einem $\mathbb{R}$-Vektorraum V mit $\dim V < \infty$.

β heißt	falls $\forall x \in V \setminus \{0\}$	das heißt
positiv definit	$\beta(x,x) > 0$	$n_- = n_0 = 0$, $n_+ = n$
positiv semidefinit	$\beta(x,x) \geq 0$	$n_- = 0$
negativ definit	$\beta(x,x) < 0$	$n_- = n$, $n_+ = n_0 = n$
negativ semidefinit	$\beta(x,x) \leq 0$	$n_+ = n$
indefinit	$\exists y \in V : \beta(y,y) > 0$ und $\exists z \in V : \beta(z,z) < 0$	$n_- = n$, $n_+ = n_0 = n$
nicht ausgeartet/ nicht degeneriert		$n_0 = 0$

Bemerkung. Es gilt: β negativ definit $\Leftrightarrow -\beta$ positiv definit.
Es gilt: β negativ semidefinit $\Leftrightarrow -\beta$ positiv semidefinit.
Es gilt: β indefinit $\Leftrightarrow -\beta$ indefinit
$n_+ - n_-$ heißt auch die Signatur von β.
n_+ heißt auch Index von β.
Das alles ist nicht ganz einheitlich in der Literatur.

Satz 10.22 (Determinantenkriterium für positive Definitheit)**.** *Sei $B \in \mathbb{R}^{n,n}$ symmetrisch, $B = (b_{ij})_{i,j}$. Bezeichne für $1 \leq k \leq n$*

$$d_k := \det \begin{pmatrix} b_{11} & \dots & b_{1k} \\ \vdots & & \vdots \\ b_{k1} & \dots & b_{kk} \end{pmatrix}$$

1. *B ist genau dann positiv definit, wenn $d_k > 0$ für alle $k = 1,\dots,n$ gilt.*
2. *Falls nicht $d = 0$ für alle $k = 1,\dots,n$, dann ist n_- gleich der Anzahl der Vorzeichenwechsel in der Folge $(1, d_1, d_2, \dots, d_n)$*

Beweis durch vollständige Induktion nach n wird weggelassen.

Definition 10.23. Seien $\beta\colon V\times V\to K$, $\beta'\colon V'\times V'\to K$ Bilinearformen auf V bzw. V'.
Eine lineare Abbildung $f\colon V\to V'$ heißt eine (lineare) Isometrie von (V,β) auf (V',β') falls für alle $x,y\in V$ gilt $\beta'(f(x),f(y))=\beta(x,y)$.
Falls eine Isometrie von (V,β) auf (V',β') existiert, dann heißen (V,β) und (V',β') isometrisch, geschrieben $(V,\beta)\simeq(V',\beta')$

Satz 10.24. *Seien V und V' k-Vektorräume. mit $\dim V=V'=n<\infty$. β bzw. β' Bilinearformen auf V bzw V', sei $f\colon V\to V$ eine bijektive lineare Abbildung. Seien B, B', S die Matrizen zu β, β', f bzgl. (derselben) Basen auf V bzw. auf V'. Dann ist f eine Isometrie genau dann, wenn $B=S^TB'S$ gilt.*
Also insbesondere für $V=V'$, dieselbe Basis auf V und V':

$$(V,\beta)\simeq(V,\beta')\Leftrightarrow\beta\simeq\beta'$$

Beweis. Für alle $x,y\in V$ gilt (mit $\tilde a$, $\tilde y$ zugehörige Koordinatenvektoren bzgl. der gegebenen Basen)

$$\beta(x,y)=\beta'(f(x),f(y))\Leftrightarrow\tilde x^TB\tilde y=(S\tilde x)^TB'(S\tilde y)=\tilde x^T(S^TB'S)\tilde y$$

also ist f Isometrie von (V,β) auf (V',β') äquivalent zu $B=S^TB'S$. □

Definition 10.25. Sei $\beta\colon V\times V\to K$ eine Bilinearform.
Die Menge der linearen Isometrien auf (V,β) bildet bzgl. $\circ$ eine Gruppe $O(V,\beta)$. Sie heißt die orthogonale Gruppe von (V,β). Für $\dim V=n<\infty$ ist $SO(V,\beta):=\{f\in O(V,\beta)\mid\det f=1\}$ eine Untergruppe. Sie heißt die spezielle orthogonale Gruppe von (V,β).
Matrizentheoretische Beschreibung und Bezeichnung:

$$O(K^n,B)=\{S\in K^{n,n}\mid S\text{ invertierbar, }S^TBS=B\},$$

wobei die Matrix B als Matrix der Biliearform $(x,y)\mapsto x^TBy$ (bezüglich der Standardbasis des K^n) aufgefasst wird.

$O(n,m):=\{S\in\mathbb{R}^{n+m,n+m}\mid S\text{ invertierbar, }S^TBS=B\}$,
wobei $B:=[1,\dots,1,-1,\dots,-1],SO(n,m):=\{S\in O(n,m)\mid\det S=1\}$

$\det\colon\mathrm{GL}(V)\to K\setminus\{0\}$ ist ein Gruppenhomorphismus von $(\mathrm{GL}(V),\cdot)$ nach $(K\setminus\{0\},\cdot)$. Also ist $SO(V,\beta)$ ein Normalteiler von $O(V,\beta)$ (Kern eines Gruppenhomorphismus det),

Bemerkung. Die $SO(3,1)$ ist wichtig in der Relativitätstheorie, die $O(n,1)$ ist wichtig in der nichteuklidischen Geometrie.

Satz 10.26. *Sei* $\dim V = \dim W = n < \infty$. *Sei* $\beta\colon V \times W \to K$ *eine nichtausgeartete Bilinearform,* $\gamma\colon V \times W \to K$ *eine beliebige Bilinearform. Dann gibt es genau eine lineare Abbildung* $f\colon V \to V$ *mit* $\gamma(x,y) = \beta(f(x),y)$ *für alle* $x \in V$, $y \in W$ *und genau eine lineare Abbildung* $g\colon W \to W$ *mit* $\gamma(x,y) = \beta(x,g(y))$ *für alle* $x \in V$, $y \in W$.

Beweis. Wähle Basen D bzw. D' von V bzw. W. Seien B, C die Matrizen von β bzw. γ bezüglich D bzw. D'. Seien $x \in V$, $y \in W$ und $\tilde{x}$, $\tilde{y}$ die zugehörigen Koordinatenvektoren bezüglich D bzw. D'. Dann gilt $\operatorname{Rang} B = n$ (wegen β nichtausgeartet) und $\beta(x,y) = \tilde{x}^T B\tilde{y}$. Für eine lineare Abbildung $f\colon V \to V$ mit Matrix A bzgl. D gilt

$$\tilde{x}^T C\tilde{y} = \gamma(x,y) = \beta(f(x),y) = (A\tilde{x})^T B\tilde{y} = \tilde{x}^T(A^T B)\tilde{y} \quad \text{für alle } \tilde{x},\tilde{y} \in K^n$$

genau dann, wenn $C = A^T B$, also $A^T = CB^{-1}$, also $A = (CB^{-1})^T$ gilt. Damit ist die eindeutige Existenz von f gezeigt. Für g genauso (vertausche die Rollen von V und W). □

10.1 Der Dualraum

Definition 10.27. Sei V ein K-Vektorraum. $V^* := \{f\colon V \to K \mid f\text{linear}\}$ heißt der Dualraum von V. $\langle\cdot,\cdot\rangle : V^* \times V \to K$ mit $\langle f,x\rangle := f(x)$ für $f \in V^*$, $x \in V$ ist eine nichtausgeartete Bilinearform.

Beweis. $\langle\cdot,\cdot\rangle$ Bilinearform ist klar. Nicht ausgeartet: $\langle f,x\rangle = 0$ für alle $x \in V$ $\Rightarrow f = 0$ ist klar.
Sei $x \neq 0$. Dann kann man $\{x\}$ zu einer Basis B von V ergänzen (mit dem Auswahlaxiom, falls $\dim V = \infty$) und definiere $f\colon V \to K$ durch $f(x) = 1$ und $f(b) = 0$ für $b \in B\backslash\{x\}$ und durch eindeutige Fortsetzung zu einer linearen Abbildung. Dann ist $\langle f,x\rangle = f(x) = 1 \neq 0$, also $x \neq 0 \Rightarrow \exists f \in V^*\colon \langle f,x\rangle \neq 0$ □

F 10.28. *Falls* $\dim V = n < \infty$ *ist, dann gilt* $\dim V^* = \dim V$. *Falls* $B = (b_1,\ldots,b_n)$ *eine Basis von* V *ist, dann ist* $\tilde{B} := (\tilde{b}_1,\ldots,\tilde{b}_n)$ *eine Basis von* V^*, *wobei* $\tilde{b}_i$ *definiert ist durch* $\left\langle \tilde{b}_i, \tilde{b}_j \right\rangle := \delta_{ij} = \tilde{b}_i(b_j)$. $\tilde{B}$ *heißt die Dualform von* B. *Also hat die Bilinearform* $\langle\cdot, cdot\rangle : V^* \times V \to K$ *bzgl.* $\tilde{B}$ *und* B *die Einheitsmatrix als Strukturmatrix.*

Beweis. Klar. □

F 10.29. *Die Abbildung* $i\colon V \to V^{**} := (V^*)^*$ *mit* $i(x)(f) := f(x)$ *heißt die natürliche Einbettung.*
$i(x)$ *ist eine lineare Abbildung* $V^* \to K$, *also* $i(x) \in V^{**}$.
$i\colon V \to V^{**}$ *ist linear.*
i *ist injektiv:* $x \in \ker(i) \Rightarrow \langle f,x\rangle = f(x) = i(x)(f) = 0$ *für alle* $f \in V^* \Rightarrow$

$x = 0$, da $\langle \cdot, \cdot \rangle$ nicht ausgeartet.

F 10.30. *Falls* $\dim V < \infty$, *dann ist* $i \colon V \to V^{**}$ *ein Isomorphismus*

Beweis. $\dim V = \dim V^* = dim(V^*)^*$. Mit i injektiv folgt die Behauptung. □

Beispiel. Für $V = K^n$ mit der Standardbasis $(e_1, e_2, \ldots, e_n)$ ist $V^* = K^{1,n}$ der Raum der Zeilenvektoren aufgefasst als lineare Abbildung und $(e_1^T, \ldots, e_n^T)$ die Dualbasis zu $(e_1, \ldots, e_n)$.

Beispiel. Sei $V = K^{(\mathbb{N})}$. Dann ist $V^* \cong K^{\mathbb{N}}$, $(e_i)_{i \in \mathbb{N}}$ ist eine Basis in einem Vektorraum. W (hier $W := K$) ist zu V^* isomorph zum Raum aller Abbildungen $\mathbb{N} \to \mathbb{R}$, also zu $K^{\mathbb{N}}$. Es gilt $K^{(\mathbb{N})} \ncong K^{\mathbb{N}}$ ($K^{\mathbb{N}}$ hat keine abzählbare Basis).

Beispiel. Sei $V = C^0[0,1]$ der Raum der stetigen Abbildungen $f \colon [0,1] \to \mathbb{R}$ Dann ist $\int_0^1 \in V^*$, wobei $\int_0^1 \colon V \to \mathbb{R}$ definiert ist durch $f \mapsto \int_0^1 f(t)\mathrm{d}t \in \mathbb{R}$

Definition 10.31. Sei $f \colon V \to W$ eine lineare Abbildung, dann ist $f^* \colon W^* \to V^*$ durch $f^*(g) = g \circ f$ für alle für alle $g \in W^*$ definiert. Offensichtlich ist $f^*(g) \in V^*$ und f^* linear. f^* heißt die zu f duale Abbildung.

F 10.32. *Falls* $\dim V < \infty$, $\dim W < \infty$ *und* A *die Matrix die linearen Abbildung* $f \colon V \to W$ *bzgl. der (geordneten) Basen* B *von* V' *und* C *von* W, *dann ist* A^T *die Matrix von* f^* *bzgl. der Dualbasen* $\tilde{C}$ *und* $\tilde{B}$

Beweis. Seien $B = (b_1, \ldots, b_n)$, $C = (c_1, \ldots, c_m)$ Basen von V bzw. W. $\tilde{B} = (\tilde{b_1}, \ldots, \tilde{b_n})$, $\tilde{C} = (\tilde{c_1}, \ldots, \tilde{c_m})$ die Dualbasen, $A = (a_{ij})_{i,j}$ die Matrix von f bezüglich B und C. Dann gilt

$$f(b_j) = \sum_{i=1}^{m} a_{ij} c_i, \text{ also } f^*(\tilde{c}_i(b_j)) = \tilde{c}_i \left(\sum_{k=1}^{m} a_{kj} c_k \right) \overset{(*)}{=} a_{ij} \tilde{b}_j(b_j)$$

$$(*) \text{ wegen } \tilde{c}_i(c_k) = \delta_{ik}, \tilde{b}_i(b_j) = \delta_{ij}$$

$$\text{also } f^*(\tilde{c}_i) = \sum_{j=1}^{n} a_{ij} \tilde{b_j}$$

also ist die Matrix von f^* gleich $(a_{ji})_{i,j} = A^T$ □

Sei $\beta\colon V \times W \to K$ eine Bilinearform. Dann können wir die Abbildung $\beta_1\colon V \to W^*, x \mapsto \beta(x, \cdot)$ mit $\beta(x, \cdot)(y) := \beta(x, y)$ betrachten.
$\beta(x, \_) \in W^*$ klar und β_1 linear ist klar.
Bezeichne $\mathrm{Bil}(V, W)$ den Vektorraum aller Bilinearformen $\beta\colon V \times W \to K$ und $\mathrm{Hom}(V, W^*)$ den Vektorraum aller linearen Abbildungen $f\colon V \to W$.

F 10.33. *Die Abbildung* $\mathrm{Bil}(V, W) \to \mathrm{Hom}(V, W^*)$, $\beta \mapsto \beta_1$ *ist eine bijektive lineare Abbildung.*

Beweis. Dass $\beta_1 \in \mathrm{Hom}(V, W^*)$ hatten wir schon gezeigt, dass $\beta \mapsto \beta_1$ eine lineare Abildung ist ist auch klar.
Die Umkehrabildung ist $\mathrm{Hom}(V, W^*) \mapsto \mathrm{Bil}(V, W)$, $h \mapsto \beta_1$ mit $\beta_h(x, y) := h(x)(y) = \langle h(x), y\rangle$. Es ist klar, dass die so definierte Abbildung β_h eine Bilinearform ist und rechnet sofort nach, dass die Umkehrabildung ist. □

$\mathrm{Bil}(V, W)$ und $\mathrm{Hom}(V, W^*)$ sind also in natürlicher Weise isomorph (das heißt, der Isomorphismus hängt nicht der der Wahl einer Basis ab).