PD. Dr. P.H. Lesky

Universität Stuttgart

Wintersemester 2018/19

Vorlesung Mathematik I für Studierende der Fächer inf, swt, msv

Warnung: Dies ist kein vollständiger Vorlesungsaufschrieb. Dieses Skript ist zur Erleichterung beim Mitschreiben gedacht, Ergänzungen sollen nachgetragen werden.

1 Grundlagen

1.1 Zur Aussagenlogik

1.1 Definition: Eine Aussage ist ein Satz, der entweder wahr oder falsch ist.

1.2 Verknüpfung von Aussagen:

Verknüpfung	in Worten	Definition durch Wahrheitstabelle
$\neg A$	nicht A, Negation von A	

A	$\neg A$
w	
f	

Verknüpfung	in Worten
$A \vee B$	A oder B, logisches Oder
$A \wedge B$	A und B, logisches Und
$A \to B$	wenn A dann B
$A \leftrightarrow B$	A genau dann wenn B

A	B	$A \vee B$	$A \wedge B$	$A \to B$	$A \leftrightarrow B$
w	w				
w	f				
f	w				
f	f				

1.3 Implikation: $A \Rightarrow B$ bedeutet: Die Aussage $A \to B$ ist wahr.
Also: Wenn A wahr ist, dann ist auch B wahr. (Wenn A falsch ist, wird keine Aussage über B gemacht.)

Man sagt: A ist **hinreichende Bedingung** für B,
B ist **notwendige Bedingung** für A.

Z.B. $|x-4| < 1 \quad \Rightarrow \quad x < 5.$

1.4 Äquivalenz: $A \Leftrightarrow B$ bedeutet: Die Aussage $A \leftrightarrow B$ ist wahr.
Also: Entweder sind beide Aussagen wahr oder beide falsch.

Z.B. $(x-1)^2 \le 4 \quad \Leftrightarrow \quad |x-1| \le 2 \quad \Leftrightarrow \quad -2 \le x-1 \le 2 \quad \Leftrightarrow \quad -1 \le x \le 3.$

Z.B. $A \to B \quad \Leftrightarrow \quad \neg B \to \neg A.$

Beweis durch Wahrheitstafel:
(Beweis durch Fallunterscheidung,
Auflistung aller möglichen Fälle)

A	B	$A \to B$	$\neg A$	$\neg B$	$\neg B \to \neg A$
w	w		f	f	
w	f		f	w	
f	w		w	f	
f	f		w	w	

1.5 Wichtige Beweistechniken:

1) Direkter Beweis: Zeige $A \Rightarrow B$, indem aus der Gültigkeit von A durch Umformungen oder Folgerungen auf die Gültigkeit von B geschlossen wird.

2) Kontraposition: Zeige $A \Rightarrow B$ durch Nachweis von $\neg B \Rightarrow \neg A$.

3) Widerspruchsbeweis: Zeige $A \Rightarrow B$ durch Nachweis von $A \wedge \neg B \Rightarrow$ falsche Aussage (markiert durch $\lightning$ oder „Widerspruch“).

2) und 3) werden als **indirekte Beweise** bezeichnet.

Z.B. Beweise $\underbrace{|x-4| < 1}_{A} \quad \Rightarrow \quad \underbrace{x < 5}_{B}$:

1) Direkt: Wir gehen davon aus, dass $|x-4| < 1$ wahr ist.
Fall a) $x \ge 4 \quad \Rightarrow \quad x-4 = |x-4| < 1 \quad \Rightarrow \quad x < 5 \quad \Leftrightarrow \quad B$
Fall b) $x < 4 \quad \Rightarrow \quad x < 5 \quad \Leftrightarrow \quad B$

2) Kontraposition:

$$\neg B \quad \Leftrightarrow \quad x \ge 5 \quad \Rightarrow \quad x-4 \ge 1 \quad \Rightarrow \quad |x-4| = x-4 \ge 1 \quad \Leftrightarrow \quad \neg A.$$

3) Widerspruchsbeweis: Annahme $|x-4| < 1 \wedge x \ge 5$
$\Rightarrow \quad 1 \le x-4 = |x-4| < 1 \quad \Rightarrow \quad 1 < 1 \quad \lightning$

Typisches Beispiel für einen Widerspruchsbeweis: $x^2 = 2 \quad \Rightarrow \quad x \notin \mathbb{Q}$.

Annahme: $x^2 = 2 \wedge x \in \mathbb{Q}$
$\Leftrightarrow \quad x^2 = 2 \wedge x = \frac{p}{q}$, wobei p, q teilerfremd
$\vdots$
$\Rightarrow \quad p, q$ haben den gemeinsamen Teiler 2 $\quad \lightning \quad$ (p, q sind teilerfremd)

1.2 Mengen

1.6 Definition (naiv)***:*** Eine **Menge** ist eine Zusammenfassung von Objekten zu einem Ganzen. Bezeichnung: $m \in M$ bedeutet: Das Objekt m liegt in M (ist in der Menge M enthalten), $m \notin M$ bedeutet: m liegt nicht in M.

Explizit: $M := \{1, 2, 3\}$, $\mathbb{N} = \{1, 2, 3, \ldots\}$.
Durch charakteristische Eigenschaft: $P := \{n \in \mathbb{N} : n \text{ ist Primzahl}\}$
$\emptyset$ (oder $\{\}$): Leere Menge, enthält keine Elemente.

1.7 Gleichheit: $A = B$, falls $x \in A \Leftrightarrow x \in B$.

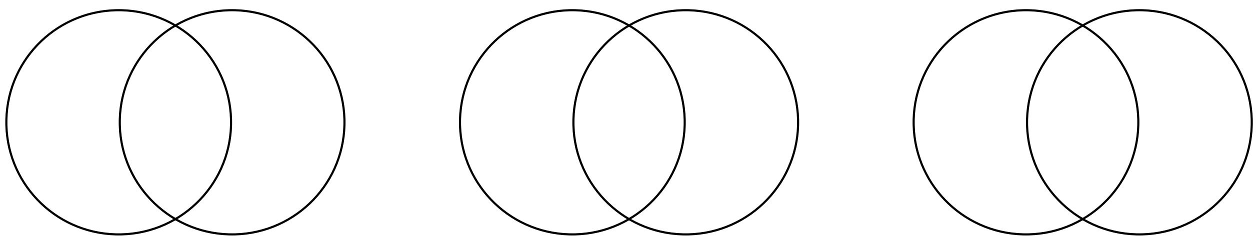
1.8 Teilmenge: $A \subseteq B$, falls: $x \in A \Rightarrow x \in B$.
Für jede Menge A gilt $\emptyset \subseteq A$.

Veranschaulichung im Venn-Diagramm:

1.9 Verknüpfung von Mengen:

$$\begin{aligned} A \cap B &:= \{x : x \in A \wedge x \in B\} \quad \text{(Schnittmenge)} \\ A \cup B &:= \{x : x \in A \vee x \in B\} \quad \text{(Vereinigungsmenge)} \\ A \setminus B &:= \{x : x \in A \wedge x \notin B\} \quad \text{(Differenzmenge)} \end{aligned}$$

Veranschaulichung im **Venn-Diagramm**:



Zwei Mengen heißen **disjunkt**, wenn ihre Schnittmenge leer ist.

1.10 Gesetze von De Morgan: Seien A, B, C Mengen. Dann gelten:

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C), \qquad A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C).$$

1.11 Potenzmenge: $\mathcal{P}(A) := \{B : B \subseteq A\}$

Z.B.: $A = \{1, 2, 3\} \quad \Rightarrow \quad \mathcal{P}(A) =$

Z.B.: $A = \big\{\{1\}, \{2\}\big\} \quad \Rightarrow \quad \mathcal{P}(A) =$

1.12 Kartesisches Produkt: $A \times B \ := \ \{(x,y) : x \in A \wedge y \in B\}$,
(x,y) heißt **geordnetes Paar** (geordnet: Die Reihenfolge ist wichtig)

Z.B.: $\{1,2\} \times \{3,4\} \ =$

Z.B.: $\mathbb{N} \times \mathbb{N} = \{\text{Gitterpunkte}\}$:

Geordnetes Paar definiert durch Mengenlehre: $(x,y) := \{x, \{y\}\}$.
Insbesondere: $(x,y) = (x',y') \ \Leftrightarrow \ x = x' \wedge y = y'$.

1.3 Quantoren

1.13 Definition: Sei M eine Menge, $A(x)$ eine von $x \in M$ abhängige Aussage.

$\forall x \in M : A(x)$
bedeutet: Für alle x aus der Menge M ist die Aussage $A(x)$ wahr.
Z.B.: $\forall n \in \mathbb{N} : n \leq n^2$.

$\exists x \in M : A(x)$
bedeutet: Es gibt (existiert) mindestens ein x in der Menge M, für das die Aussage $A(x)$ wahr ist.
Z.B.: $\exists n \in \mathbb{N} : n - 3 \notin \mathbb{N}$.

$\exists! x \in M : A(x)$
bedeutet: Es gibt genau ein x in der Menge M, für das die Aussage $A(x)$ wahr ist.
Z.B.: $\exists! x \in \mathbb{N} : x + 4 = 6$.

1.14 Negation von Aussagen mit Quantoren:
$\neg\big(\forall x \in M : A(x)\big) \ \Leftrightarrow \ \exists x \in M : \neg A(x)$,
$\neg\big(\exists x \in M : A(x)\big) \ \Leftrightarrow \ \forall x \in M : \neg A(x)$.

Z.B.: Lösbarkeit der Gleichung $x + a = b$ im Raum der ganzen Zahlen:

$$\forall a \in \mathbb{Z} \ \ \forall b \in \mathbb{Z} \ \ \exists x \in \mathbb{Z} : x + a = b$$

Negation:

$$\exists a \in \mathbb{Z} \ \ \exists b \in \mathbb{Z} \ \ \forall x \in \mathbb{Z} : x + a \neq b$$

1.4 Abbildungen

1.15 Definition: Seien A, B Mengen. Eine **Abbildung** f von A nach B ist eine Vorschrift, die jedem $x \in A$ ein eindeutig bestimmtes Element $f(x) \in B$ zuordnet. Manchmal heißt f auch **Funktion**.

Schreibe: $f : A \to B$
oder $f : A \to B : x \mapsto y = f(x)$
oder $f : A \ni x \mapsto y \in B$
oder $f : x \mapsto y = f(x)$.

A heißt **Definitionsbereich** (*engl. domain*) von f, B **Bildbereich** (*engl. codomain*) von f.

Falls $y = f(x)$, heißt y **Bild** von x (*engl. image*), x heißt **Urbild** (*engl. pre-image*) von y.

Die Menge

$$f(A) \ := \ \{f(x) \in B : x \in A\}$$

heißt **Bild von $\boldsymbol{f}$** (*engl. Range*), für $C \subseteq B$ heißt

$$f^{-1}(C) \ := \ \{x \in A : f(x) \in C\}$$

Urbild von $\boldsymbol{C}$.

Z.B.: $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$, $y = 4$, $C = [0, 4]$.
Achtung: $f : \mathbb{R} \to \mathbb{R} : x \mapsto \frac{1}{x}$ ist keine Abbildung.

1.16 Definition: Zwei Abbildungen $f : A \to B$ und $f' : A' \to B'$ heißen **gleich**, falls $A' = A \land \forall x \in A : f(x) = f'(x)$.

1.17 Definition: $f : A \to B$ heißt

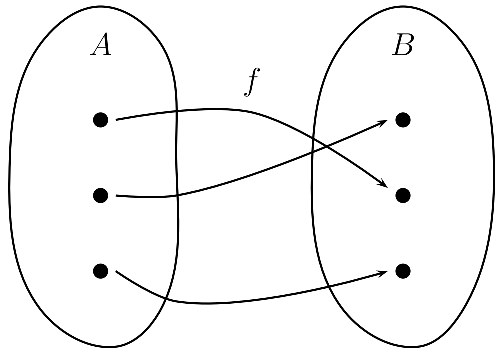
1) **injektiv**, falls für $x, x' \in A$ $\quad f(x) = f(x') \Rightarrow x = x'$
bzw. $\quad x' \neq x \Rightarrow f(x') \neq f(x)$

2) **surjektiv**, falls $f(A) = B$.

3) **bijektiv**, falls f injektiv und surjektiv.

Injektiv bedeutet: In jedem $y \in B$ endet höchstens ein Pfeil
Surjektiv bedeutet: In jedem $y \in B$ endet mindestens ein Pfeil

Bijektiv:



1.18 Definition: Ist $f : A \to B$ bijektiv, so heißt $f^{-1} : B \to A : f(x) \mapsto x$ die **Umkehrabbildung** oder **inverse Abbildung** zu f.

Z.B.:	$f_1 : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$	weder injektiv noch surjektiv	
	$f_2 :]-\infty, 0] \to \mathbb{R} : x \mapsto x^2$	injektiv, nicht surjektiv	
	$f_3 : \mathbb{R} \to [0, \infty[: x \mapsto x^2$	nicht injektiv, aber surjektiv	
	$f_4 :]-\infty, 0] \to [0, \infty[: x \mapsto x^2$	injektiv und surjektiv,	$f_4^{-1} : y \mapsto -\sqrt{y}$

1.19 Definition: Ist $f : A \to B$ und $A_0 \subseteq A$, so heißt $f_0 : A_0 \to B : x \mapsto f_0(x) := f(x)$ die **Einschränkung** von f auf A_0; f heißt **Fortsetzung** von f_0 auf A. Man schreibt $f_0 = f\big|_{A_0}$.

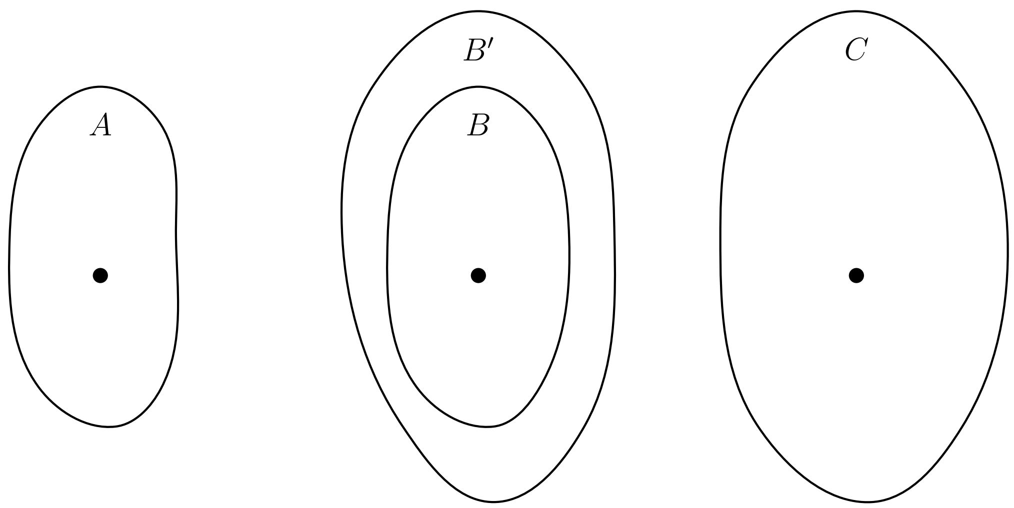
Die Abbildung $\mathrm{id}_A : A \to A : x \mapsto x$ heißt **identische Abbildung**.

Z.B.: Seien f_1, f_2 aus dem vorigen Beispiel. Dann ist f_2 die Einschränkung von f_1 auf $]-\infty, 0]$: $f_2 = f_1\big|_{]-\infty,0]}$. Umgekehrt ist f_1 eine Fortsetzung von f_2 auf $\mathbb{R}$.

1.20 Verknüpfung von Abbildungen: Sei $f : A \to B$, $g : B' \to C$, $B \subseteq B'$. Dann heißt

$$g \circ f : A \to C : x \mapsto (g \circ f)(x) := g(f(x))$$

die **Verknüpfung** oder **Hintereinanderausführung** g nach f.



1.21 Satz: Ist $f : A \to B$ bijektiv, so gilt

$$f \circ f^{-1} = \mathrm{id}_B, \qquad f^{-1} \circ f = \mathrm{id}_A$$

Beweis: **1)** Sei $x \in A$. $\Rightarrow \quad f^{-1}\big(f(x)\big) = x \quad \Rightarrow \quad f^{-1} \circ f = \mathrm{id}_A$.

2) $y \in B \;\Rightarrow\; \exists x \in A : y = f(x)$
$\Rightarrow\; x = f^{-1}(y) \;\Rightarrow\; f\big(f^{-1}(y)\big) = f(x) = y \;\Rightarrow\; f \circ f^{-1} = \mathrm{id}_B$ □

1.22 Abbildungen und Mengenlehre: Sei $f : A \to B$. Dann heißt

$$G := \{(x, f(x)) : x \in A\} \subseteq A \times B$$

der **Graph** von f. Definiere eine Abbildung von A nach B als $G \subseteq A \times B$ mit der Eigenschaft

$$\forall x \in A \;\; \exists! y_x \in B : (x, y_x) \in G.$$

und setze $f(x) := y_x$.

1.5 Relationen

1.23 Definition: Seien A, B Mengen. Eine (zweistellige) **Relation** ist eine Teilmenge $R \subseteq A \times B$. Für $(a, b) \in R$ schreibe aRb: Zwischen a und b besteht die Relation R.

Z.B.: $\leq \;:=\; \{(n, m) \in \mathbb{N} \times \mathbb{N} : n \leq m\}$.
Z.B.: $\mathbb{N}/2\mathbb{N} \;:=\; \{(n, m) \in \mathbb{N} \times \mathbb{N} : |n - m|$ ist durch 2 teilbar$\}$.

Uns interessieren Relationen **auf** A, d.h. $R \subseteq A \times A$.

1.24 Definition: Eine Relation $R \subseteq A \times A$ (d.h. R ist Relation auf A) heißt

1) **reflexiv**, falls $\forall a \in A : (a, a) \in R$.

2) **symmetrisch**, falls $(a, b) \in R \Leftrightarrow (b, a) \in R$.

3) **antisymmetrisch**, falls $(a, b) \in R \;\wedge\; (b, a) \in R \;\Rightarrow\; a = b$.

4) **transitiv**, falls $(a, b) \in R \;\wedge\; (b, c) \in R \;\Rightarrow\; (a, c) \in R$.

1.25 Ordnungsrelation: Ist eine Relation auf A, die reflexiv, antisymmetrisch und transitiv ist. Für $(a, b) \in R$ schreibe $a \leq b$. Es gilt also

$$\begin{aligned} &\forall a \in A : a \leq a \\ &a \leq b \ \wedge b \leq a \ \Rightarrow \ a = b \\ &a \leq b \ \wedge b \leq c \ \Rightarrow \ a \leq c \end{aligned}$$

1.26 Äquivalenzrelation: Ist eine Relation auf A, die reflexiv, symmetrisch und transitiv ist. Für $(a, b) \in R$ schreibe $a \sim b$. Es gilt also

$$\begin{aligned} &\forall a \in A : a \sim a \\ &a \sim b \ \Leftrightarrow \ b \sim a \\ &a \sim b \ \wedge b \sim c \ \Rightarrow \ a \sim c \end{aligned}$$

Z.B.: $\sim \; = \mathbb{N}/2\mathbb{N}$. Dadurch zerfällt $\mathbb{N}$ in zwei Klassen:

$$\begin{array}{ccccccc} \{n \in \mathbb{N} : n \sim 1\} & = & \{1, 3, 5, \ldots\} & = & \{n \in \mathbb{N} : n \sim 3\} & = & \ldots \\ \{n \in \mathbb{N} : n \sim 2\} & = & \{2, 4, 6, \ldots\} & = & \{n \in \mathbb{N} : n \sim 4\} & = & \ldots \end{array}$$

1.27 Äquivalenzrelation ist Klasseneinteilung: Sei $\sim$ eine Äquivalenzrelation auf A. Für $a \in A$ ist

$$[a] \; := \; \{b \in A : b \sim a\}$$

die **Äquivalenzklasse** von a. Für Äquivalenzklassen gelten:

1) $\forall a \in A : a \in [a]$,

2) $[a] \cap [b] \neq \emptyset \ \Rightarrow \ [a] = [b]$.

Das bedeutet: Die Menge

$$\mathcal{A} \; := \; \{[a] : a \in A\} \; \subseteq \; \mathcal{P}(A)$$

besitzt die Eigenschaften

1) $\displaystyle\bigcup_{B \in \mathcal{A}} B \; = \; A$,

2) Sind $B_1, B_2 \in \mathcal{A}$, so gilt entweder $B_1 \cap B_2 = \emptyset$ oder $B_1 = B_2$.

Man nennt $\mathcal{A}$ eine **Klasseneinteilung** von A.

Beweis der Eigenschaften 1) und 2) der Äquivalenzklassen:
Für jedes $a \in A$ gilt $a \sim a \quad \Rightarrow \quad a \in [a]$.
Sei $[a] \cap [b] \neq \emptyset \quad \Rightarrow \quad \exists c \in [a] \cap [b] \quad \Rightarrow \quad a \sim c \sim b \quad \Rightarrow \quad a \sim b \quad \Rightarrow \quad [a] \subseteq [b] \subseteq [a]$.

Umgekehrt: Ist $\mathcal{A}$ eine Klasseneinteilung von A, so definiert

$$R \ := \ \{(a,b) \in A \times A \mid \exists B \in \mathcal{A} : a \in B \ \wedge \ b \in B\}$$

eine Äquivalenzrelation, und die Äquivalenzklassen sind genau die Elemente von $\mathcal{A}$.

Beweis, dass R eine Äquivalenzrelation ist:

Reflexivität: Sei $a \in A$. Wegen $A = \bigcup\limits_{B \in \mathcal{A}} B$ existiert ein $B \in \mathcal{A}$ mit $a \in B \ \Rightarrow \ a\,R\,a$,

Symmetrie: $a\,R\,b \ \Rightarrow \ b\,R\,a$ klar,

Transitivität: $\underbrace{a\,R\,b}_{a,b \in B_1} \wedge \underbrace{b\,R\,c}_{b,c \in B_2} \ \Rightarrow \ B_1 = B_2 \ \Rightarrow \ a, c \in B_1 \ \Rightarrow \ a\,R\,c.$

1.28 Beispiele: **1)** $A = \mathbb{R} \times \mathbb{R}$, $(x,y) \sim (x',y') \ :\Leftrightarrow \ \sqrt{x^2+y^2} = \sqrt{x'^2+y'^2}$
$[(x,y)] =$ Kreis um $(0,0)$ mit Radius $r = \sqrt{x^2+y^2}$.

2) Brüche: Zwei Brüche $\frac{p}{q}, \frac{r}{s}$ sind gleich, wenn $p\,s = r\,q$. Definiere auf $\mathbb{Z} \times \mathbb{N}$ die Relation

$$(p,q) \sim (r,s) \ :\Leftrightarrow \ p\,s = r\,q$$

Ein Bruch ist dann die Äquivalenzklasse $[(p,q)] =: \frac{p}{q}$.

3) Größen von endlichen Mengen: Sei $\mathcal{M} := \{$Mengen M mit endlich vielen Elementen$\}$. Definiere auf $\mathcal{M}$

$$M_1 \sim M_2 \ :\Leftrightarrow \ \exists (f : M_1 \to M_2) : f \text{ ist bijektiv}$$

Die Äquivalenzklassen bestehen aus allen Mengen mit derselben Anzahl von Elementen.

1.6 Die natürlichen Zahlen

1.29 Peano (1889): Die natürlichen Zahlen bilden eine Menge $\mathbb{N}$, auf der eine Abbildung

$$\text{Nachfolger}: \mathbb{N} \to \mathbb{N}$$

erklärt ist mit folgenden Eigenschaften:

($\mathbb{N}$1) $\exists!\, x_0 \in \mathbb{N} : x_0 \notin \text{Nachfolger}(\mathbb{N})$. Bezeichnung $1 := x_0$.
(Es existiert genau eine Zahl, die nicht Nachfolger einer anderen Zahl ist).

($\mathbb{N}$2) Nachfolger ist injektiv
(Nachfolger$(n_1) =$ Nachfolger$(n_2) \ \Rightarrow \ n_1 = n_2$)

($\mathbb{N}$3) (Induktionsaxiom) Ist $M \subseteq \mathbb{N}$ mit den beiden Eigenschaften

- $1 \in M$ und
- $n \in M \;\Rightarrow$ Nachfolger$(n) \in M$,

dann ist $M = \mathbb{N}$.
(Enthält eine Teilmenge $M \subseteq \mathbb{N}$ die 1 und mit jeder Zahl auch ihren Nachfolger, dann ist $M = \mathbb{N}$).

Man schreibt: $2 :=$ Nachfolger(1), $3 :=$ Nachfolger(2), $\ldots$, $n+1 :=$ Nachfolger(n).

Aus diesen Axiomen lassen sich alle bekannten Regeln für die natürlichen Zahlen beweisen, z.B. $m + n = n + m$.

1.30 Vollständige Induktion: Für $n \in \mathbb{N}$ sei $A(n)$ eine Aussage, die von n abhängt, z.B.

$$1 + 2 + \ldots + n \;=\; \frac{n(n+1)}{2},$$

Ziel: Beweise, dass $A(n)$ für alle $n \in \mathbb{N}$ wahr ist.

Verfahren: Beweise

1) $A(1)$ ist wahr (Induktionsanfang),

2) $A(n) \Rightarrow A(n+1)$ für beliebiges $n \in \mathbb{N}$ (Induktionsschritt)
(Falls $A(n)$ wahr („Induktionsannahme“), dann ist $A(n+1)$ wahr („Induktionsbehauptung“).

Induktionsschluss: Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}$.

Beweis: Sei $M := \{n \in \mathbb{N} : A(n) \text{ ist wahr}\} \subseteq \mathbb{N}$. Dann $1 \in M$ und $n \in M \;\Rightarrow\; n+1 \in M$. Also $M = \mathbb{N}$ nach ($\mathbb{N}$3). $\square$

1.31 Beispiele: **1)** $A(n) : 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ (**arithmetische Summe**).

- Induktionsanfang: $A(1):\quad 1 = \frac{1(1+1)}{2}$ ist wahr.
- Induktionsschritt: Falls $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ ($A(n)$ wahr), dann

$$\begin{aligned} 1 + 2 + \ldots + n + n + 1 &= \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2}. \end{aligned}$$

  Also: $A(n+1)$ wahr.

- Induktionsschluss: $\forall n \in \mathbb{N} : 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

2) Sei $q \neq 1$. $A(n)$: $\underbrace{q^0}_{:=1} + q^1 + \ldots + q^n = \frac{1-q^{n+1}}{1-q}$ (**geometrische Summe**).

3) $A(n)$: Ist $M \subseteq \mathbb{N}$ eine Menge mit n Elementen, so besitzt M ein Maximum:

$$k = \max(M) \quad :\Leftrightarrow \quad k \in M \ \wedge \ \forall l \in M : l \leq k.$$

4) Ist M eine Menge mit n Elementen, so besitzt die Potenzmenge $\mathcal{P}(M)$ 2^n Elemente.

1.32 Rekursive Definition: **1)** Fakultät $n!$:

$$\begin{aligned} 0! &:= 1 \\ (n+1)! &:= (n+1)\, n! \text{ für } n \in \mathbb{N}_0. \end{aligned}$$

2) Summen- und Produktzeichen:

$$\sum_{k=1}^{0} a_k := 0, \quad \sum_{k=1}^{n+1} a_k := \sum_{k=1}^{n} a_k + a_{n+1}, \qquad \text{salopp:} \quad \sum_{k=1}^{n} a_k = a_1 + a_2 + \ldots + a_n$$

$$\prod_{k=1}^{0} a_k := 1, \quad \prod_{k=1}^{n+1} a_k := \left(\prod_{k=1}^{n} a_k\right) \cdot a_{n+1}, \qquad \text{salopp:} \quad \prod_{k=1}^{n} a_k = a_1 \cdot a_2 \ldots a_n$$

3) Addition und Multiplikation aus Peano-Axiomen: Für $m \in \mathbb{N}$ setze

$$m + 1 := \text{Nachfolger}(m), \qquad m + (n+1) := \text{Nachfolger}(m+n).$$

Damit ist $m + n$ für alle $m, n \in \mathbb{N}$ definiert.
Analog: $m \cdot 1 := m,\ m \cdot (n+1) := m \cdot n + m$. Damit ist $m \cdot n$ für alle $n, m \in \mathbb{N}$ definiert.
Jetzt können alle Rechengesetze bewiesen werden.

1.33 Binomialkoeffizient:

$$\binom{n}{k} := \frac{n!}{(n-k)! \cdot k!} = \frac{n \cdot (n-1) \cdots (n-k+1)}{1 \cdot 2 \cdots k} \qquad \text{(sprich: „n über k“)}$$

für $n, k \in \mathbb{N}_0,\ k \leq n$. Dann gelten

1) $\binom{n}{k} = \binom{n}{n-k}$

2) $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ für $k \leq n-1$.

3) $\binom{n}{0} = \binom{n}{n} = 1$

4) Pascalsches Dreieck:

$$
\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}
\qquad
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}
$$

1.34 Binomischer Satz: Für beliebige Zahlen a, b und für $n \in \mathbb{N}$ gilt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \ldots + \binom{n}{n} b^n.$$

Z.B.: $(a+b)^4 = a^4 + 4a^3 b + 6a^2 b^2 + 4a b^3 + b^4.$

Beweis: Vollständige Induktion ab $n = 1$:

Induktionsanfang: $\displaystyle\sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b = (a+b)^1$ stimmt.

Induktionsschritt: Induktionsannahme: Die Formel gilt für n.

Induktionsbehauptung: $\displaystyle(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k.$

Beweis der Induktionsbehauptung:

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b) \cdot (a+b)^n \\
&= (a+b) \cdot \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \underbrace{\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}}_{=\sum_{l=1}^{n+1} \binom{n}{l-1} a^{n-(l-1)} b^l} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-(k-1)} b^k \\
&= \underbrace{\binom{n}{0}}_{=\binom{n+1}{0}} a^{n+1} b^0 + \sum_{k=1}^{n} \underbrace{\left(\binom{n}{k} + \binom{n}{k-1}\right)}_{=\binom{n+1}{k}} a^{n+1-k} b^k + \underbrace{\binom{n}{n}}_{\binom{n+1}{n+1}} a^0 b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k
\end{aligned}
$$

Induktionsschluss: Die Formel gilt für alle $n \in \mathbb{N}$.

$\square$

1.35 Von $\mathbb{N}$ zu $\mathbb{Z}$: Idee: $-1 = 1-2 = 2-3 = \ldots = m-(m+1) = \ldots$
Definiere auf $\mathbb{N} \times \mathbb{N}$ die Äquivalenzrelation

$$(m,n) \sim (m',n') \;:\Leftrightarrow\; m+n' = m'+n$$

1) Reflexivität: $(m,n) \sim (m,n)$.

2) Symmetrie: $(m,n) \sim (m',n') \;\Leftrightarrow\; (m',n') \sim (m,n)$

3) Transitivität: $(m,n) \sim (m',n') \;\wedge\; (m',n') \sim (m'',n'') \;\Rightarrow\; (m,n) \sim (m'',n'')$.

Sei $\mathbb{Z} := \{[(m,n)] : m,n \in \mathbb{N}\}$. Setze $0 = [(1,1)],\; n := [(n+1,1)],\; -n := [(1,n+1)]$.
Definiere $[(m,n)] + [(k,l)] := [(m+k, n+l)]$ und zeige, dass die Summe unabhängig von den Repräsentanten der Äquivalenzklassen ist.
$(\mathbb{Z},+)$ erfüllt alle bekannten Gesetze.

1.7 Teilbarkeit

1.36 Definition: Sei $n \in \mathbb{Z}$. Dann heißt $m \in \mathbb{N}$ **Teiler** von n (kurz $m \mid n$), falls

$$\exists k \in \mathbb{Z} : n = k \cdot m;$$

n heißt **teilbar** durch m. Insbesondere: 0 ist durch alle $m \in \mathbb{N}$ teilbar.

$$D(n) \;:=\; \{d \in \mathbb{N} : d \mid n\}$$

ist die Menge der Teiler von n. Für $n,m \in \mathbb{N}$ heißt

$$\mathrm{ggT}(m,n) \;:=\; \max\big(D(m) \cap D(n)\big)$$

der **größte gemeinsame Teiler** von m und n.

Z.B.: $\mathrm{ggT}(30,24)$:

1.37 Satz: Teiler ist Ordnungsrelation auf $\mathbb{N}$.

1.38 Hilfssatz: Seien $n,m,l,k \in \mathbb{Z},\; d \in \mathbb{N}$. Dann gilt

$$d \mid n \;\wedge\; d \mid m \;\Rightarrow\; d \mid (k \cdot n + l \cdot m).$$

Beweis: $d \mid n \;\wedge\; d \mid m \;\Rightarrow\; \exists k_1, k_2 \in \mathbb{Z} : n = k_1 \cdot d \;\wedge\; m = k_2 \cdot d.$
$\Rightarrow\; k \cdot n + l \cdot m = k \cdot k_1 \cdot d + l \cdot k_2 \cdot d = (k \cdot k_1 + l \cdot k_2) \cdot d$
$\Rightarrow d \mid (k \cdot n + l \cdot m).$ □

1.39 Teilen mit Rest: Seien $n, m \in \mathbb{N}$ mit $n > m$. Dann gibt es eindeutig bestimmte Zahlen $q \in \mathbb{N}, r \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$ mit

$$n = q \cdot m + r \quad \wedge \quad r \leq m - 1.$$

Beweis: **1)** $q := \max\{k \in \mathbb{N} : k \cdot m \leq n\},\; r := n - q \cdot m \in \mathbb{N}_0$

$\Rightarrow\; r \geq 0,\; r \leq m - 1,\; n = q \cdot m + r$

$\Rightarrow$ Existenz

2) Sei $q \cdot m + r = q' \cdot m + r'$

$$\Rightarrow \quad \begin{cases} m \cdot (q - q') = r' - r & \text{falls } r' \geq r \\ m \cdot (q' - q) = r - r' & \text{falls } r' < r \end{cases}$$

$$\overset{|r'-r| \leq m-1}{\Rightarrow} \quad q = q' \;\wedge\; r = r'$$

$\Rightarrow$ Eindeutigkeit □

1.40 Teilen mit Rest erhält den ggT: Ist $n = q \cdot m + r$ wie oben, so gilt

$$\mathrm{ggT}(n, m) = \mathrm{ggT}(m, r).$$

Beweis: Wir zeigen: $D(n) \cap D(m) = D(m) \cap D(r)$. Dann $\mathrm{ggT}(n, m) = \mathrm{ggT}(m.r)$.

$$\begin{aligned} \textbf{1)} \quad d \in D(n) \cap D(m) \;&\Rightarrow\; n = k_1 \cdot d \;\wedge\; m = k_2 \cdot d \\ &\Rightarrow\; r = n - q \cdot m = d\,\underbrace{(k_1 - q \cdot k_2)}_{\in \mathbb{Z}} \\ &\Rightarrow\; d \mid r \;\wedge\; d \mid m \\ &\Rightarrow\; d \in D(m) \cap D(r) \end{aligned}$$

$$\textbf{2)} \quad d \in D(m) \cap D(r) \;\overset{1.38}{\Rightarrow}\; d \mid n = q \cdot m + r \;\Rightarrow\; d \in D(n) \cap D(m)$$

□

Z.B.: $30 = 1 \cdot 24 + \underbrace{6}_{r = \mathrm{ggT}(30,24)}$

1.41 Euklidischer Algorithmus: Seien $m, n \in \mathbb{N}$ mit $m > n$. Dann existieren eindeutig bestimmte Zahlen $K \in \mathbb{N}$, $r_1, \dots, r_K, q_1, \dots, q_{K+1} \in \mathbb{N}$ mit

$$\begin{aligned}
m &= q_1 \cdot n + r_1 \quad \text{mit } 0 < r_1 \leq n - 1 \\
n &= q_2 \cdot r_1 + r_2 \quad \text{mit } 0 < r_2 \leq r_1 - 1 \\
r_1 &= q_3 \cdot r_2 + r_3 \quad \dots \\
\vdots & \quad \vdots \\
r_{K-2} &= q_K \cdot r_{K-1} + r_K \quad \dots \\
r_{K-1} &= q_{K+1} \cdot r_K + 0,
\end{aligned}$$

und es gilt $r_K = \mathrm{ggT}(m, n)$.

Beweis: Aus Satz 1.39 folgt die Eindeutigkeit der q_j, r_j. Wegen $r_j \leq r_{j-1} - 1 \leq r_{j-2} - 2 \dots$ bricht das Verfahren nach höchstens n Schritten ab.
Aus Satz 1.40 folgt, dass

$$\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r_1) = \mathrm{ggT}(r_1, r_2) = \dots = \mathrm{ggT}(r_{K-1}, r_K) = r_K.$$

$\square$

1.42 Beispiele: **1)** $\mathrm{ggT}(210, 25)$:

2) $\mathrm{ggT}(132, 11)$:

Drei Folgerungen aus dem Euklidischen Algorithmus:

1.43 Hilfssatz: Seien $k, m, n \in \mathbb{N}$. Dann gilt

$$\mathrm{ggT}(km, kn) = k\,\mathrm{ggT}(m, n).$$

Beweis: Multipliziere den euklidischen Algorithmus für m, n mit k:

$$\begin{aligned}
m &= q_1\, n + r_1 \\
n &= q_2\, r_1 + r_2 \\
&\vdots \\
r_{K-1} &= q_{K+1}\, r_K + 0
\end{aligned}
\quad \Rightarrow \quad
\begin{aligned}
km &= q_1\, kn + kr_1 \\
kn &= q_2\, kr_1 + kr_2 \\
&\vdots \\
k\, r_{K-1} &= q_{K+1}\, kr_K + 0
\end{aligned}$$

$\Rightarrow$ $\mathrm{ggT}(km, kn) = kr_K = k\,\mathrm{ggT}(m, n)$.

$\square$

1.44 Folgerung: $k \mid m \;\wedge\; k \mid n \;\Rightarrow\; k \mid \mathrm{ggT}(m,n)$.

Beweis: $m = l_1\,k \;\wedge\; n = l_2\,k \;\Rightarrow\; \mathrm{ggT}(m,n) = \mathrm{ggT}(k\,l_1, k\,l_2) = k\,\mathrm{ggT}(l_1,l_2)$. □

1.45 Satz: Seien $m,n \in \mathbb{N}$ und $M(m,n) := \{mx + ny : x,y \in \mathbb{Z}\}$. Dann besteht $M(m,n)$ genau aus allen Vielfachen von $\mathrm{ggT}(m,n)$:

$$M(m,n) \;=\; \{z\,\mathrm{ggT}(m,n) : z \in \mathbb{Z}\} \;=:\; \mathrm{ggT}(m,n)\cdot\mathbb{Z}.$$

Beweis: **1)** $\mathrm{ggT}(m,n) \mid m \;\wedge\; \mathrm{ggT}(m,n) \mid n \;\Rightarrow\; \mathrm{ggT}(m,n) \mid (mx+ny) \;\Rightarrow\; M(m,n) \subseteq \mathrm{ggT}(m,n)\cdot\mathbb{Z}$.

2) Zeige $\mathrm{ggT}(m,n) \in M(m,n)$. Dann folgt $\mathrm{ggT}(m,n)\cdot\mathbb{Z} \subseteq M(m,n)$.
Für $l_1, l_2 \in \mathbb{Z}$ gilt: $k_1, k_2 \in M(m,n) \;\Rightarrow\; l_1\,k_1 + l_2\,k_2 \in M(m,n)$, denn:

$$\left.\begin{array}{rcl} k_1 &=& m\,x_1 + n\,y_1 \\ k_2 &=& m\,x_2 + n\,y_2 \end{array}\right\} \;\Rightarrow\; l_1\,k_1 + l_2\,k_2 = m(l_1\,x_1 + l_2\,x_2) + n(l_1\,y_1 + l_2\,y_2) \in M(m,n)$$

Betrachte den euklidischen Algorithmus:

$$\begin{array}{rcll} m &=& q_1\,n + r_1 & \Rightarrow\; r_1 = m - q_1\,n \in M(m,n) \\ n &=& q_2\,r_1 + r_2 & \Rightarrow\; r_2 = n - q_2\,r_1 \in M(m,n) \\ &\vdots&& \\ r_{K-2} &=& q_K\,r_{K-1} + r_K & \Rightarrow\; \mathrm{ggT}(m,n) = r_K \in M(m,n) \end{array}$$

□

1.8 Primzahlen

1.46 Definition: $p \in \mathbb{N}$ mit $p \geq 2$ heißt Primzahl, wenn $D(p) = \{1, p\}$. Insbesondere ist 1 keine Primzahl.

1.47 Euklidischer Hilfssatz: Seien $m,n \in \mathbb{N}$, p Primzahl. Dann:

$$p \mid (m \cdot n) \;\Rightarrow\; p \mid m \;\vee\; p \mid n.$$

Beweis: Fall $p \mid m$: okay

Fall $\neg(p \mid m)$: $\;p \mid mn \;\wedge\; p \mid pn \;\Rightarrow\; p \mid \mathrm{ggT}(mn, pn) = n\,\mathrm{ggT}(m,p) = n \;\Rightarrow\; p \mid n$. □

Mit Induktion folgt: p Primzahl $\wedge\; p \mid n_1 \cdots n_k \;\Rightarrow\; \exists j : p \mid n_j$.

1.48 Fundamentalsatz der Arithmetik: Sei $n \in \mathbb{N}, n \geq 2$. Dann lässt sich n als Produkt von Primzahlen darstellen:

$$n = p_1 \cdot p_2 \cdots p_k, \qquad p_1, \ldots, p_k \text{ Primzahlen.}$$

Die Darstellung ist bis auf die Reihenfolge eindeutig.

Beweis: Wir beweisen: Für jedes $n \in \mathbb{N}$ gilt: Jede natürliche Zahl $j \in \{2, \ldots, n\}$ ist als Produkt von Primzahlen darstellbar.

1) Induktionsanfang $n = 2$: $\quad 2 = 2$ okay

2) Induktionsschritt:

$$n+1 = \begin{cases} \text{Primzahl} \;\Rightarrow\; n+1 = n+1, \text{ also Produkt aus der Primzahl } n+1 \\ \text{keine Primzahl: } n+1 = k \cdot l \\ \quad \overset{\text{Ind.Ann}}{\Rightarrow} \; n+1 = \underbrace{p_1 \cdots p_j}_{=k} \cdot \underbrace{\tilde{p}_1 \cdots \tilde{p}_i}_{=l} = \text{ Produkt von Primzahlen} \end{cases}$$

3) Induktionsschluss: Die Aussage gilt für jedes $n \in \mathbb{N}$ mit $n \geq 2$.

Aus der bewiesenen Aussage folgt, dass sich jede Zahl $j \in \mathbb{N}$ mit $j \geq 2$ als Produkt von Primzahlen darstellen lässt. $\square$

1.49 Satz: Es gibt unendlich viele Primzahlen.

Beweis: Annahme: Es gibt nur endlich viele Primzahlen: $P = \{p_1, \ldots, p_n\}$.
Betrachte

$$m := 1 + p_1 \cdot p_2 \cdots p_n \overset{1.48}{=} q_1 \cdots q_k, \quad q_j \text{ Primzahl}$$

Dann folgt $q_1 \notin P$: Andernfalls $q_1 = p_j \;\Rightarrow\; q_1 \mid 1 = q_1 \cdots q_k - p_1 \cdots p_n$ ↯
$\Rightarrow\; q_1$ Primzahl $\wedge\; q_1 \notin P$ ↯ $\square$

1.50 Bemerkung: Primzahlsatz (1896 Hadamard, Vallée Poussin)

$$\pi(n) := \text{Anzahl der Primzahlen} \leq n \quad \Rightarrow \quad \lim_{n \to \infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1.$$

1.9 Kongruenzen

1.51 Definition: Sei $m \in \mathbb{N},\ m \geq 2$. $a, b \in \mathbb{Z}$ heißen **kongruent modulo m** (geschrieben $a \equiv b \pmod{m}$ oder $a \equiv b\ (m)$), wenn $m \mid (a-b)$. D.h. a, b ergeben beim Teilen mit Rest durch m denselben Rest: Ist

$$\begin{aligned} a &= q_1 m + r_1, \quad 0 \leq r_1 \leq m-1 \\ b &= q_2 m + r_2, \quad 0 \leq r_2 \leq m-1 \end{aligned}$$

so sind $a \equiv b \pmod{m}$ und $r_1 = r_2$ äquivalent.

1.52 Satz: Sei $m \in \mathbb{N}$, $m \geq 2$ fest. Dann ist $\equiv\ (m)$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis: **1)** $a \equiv a \pmod{m}$ ist erfüllt,

2) $a \equiv b \pmod{m} \ \Rightarrow\ b \equiv a \pmod{m}$ ist erfüllt,

3) $a \equiv b \pmod{m} \ \wedge\ b \equiv c \pmod{m}$
$\Leftrightarrow\ m \mid (a-b) \ \wedge\ m \mid (b-c)$
$\Rightarrow\ m \mid (a-c) = (a-b) + (b-c)$
$\Rightarrow\ a \equiv c \pmod{m}$. □

1.53 Satz: $+$ und $\cdot$ sind verträglich mit $\equiv\ (m)$, d.h.

$$a \equiv a'\ (m) \ \wedge\ b \equiv b'\ (m) \ \Rightarrow\ a + b \equiv a' + b'\ (m) \ \wedge\ a \cdot b \equiv a' \cdot b'\ (m).$$

1.54 Rechnen mit Äquivalenzklassen: Sei $m \in \mathbb{N}$, $m \geq 2$ fest. Dann besitzt die Äquivalenzrelation $\equiv\ (m)$ genau m Äquivalenzklassen $[0], [1], \ldots, [m-1]$, die **Restklassen modulo m**. Definiere

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &:= \{[0], \ldots, [m-1]\} \\ [a] + [b] &:= [a+b], \qquad [a] \cdot [b] \ := \ [a \cdot b] \end{aligned}$$

Dann gelten:

$$\begin{aligned} [a] + ([b] + [c]) &= ([a] + [b]) + [c] && \text{(Assoziativgesetz)} \\ [a] + [0] &= [a] && \text{(Neutrales Element)} \\ [a] + [-a] &= [0] && \text{(Inverses Element)} \\ [a] + [b] &= [b] + [a] && \text{(Kommutativgesetz)} \end{aligned}$$

D.h. $(Z/m\mathbb{Z}, +)$ bildet eine kommutative (abelsche) Gruppe (siehe später).

Z.B: Multiplikation in $\mathbb{Z}/4\mathbb{Z}$:

$\cdot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Hier ist einiges ungewöhnlich:
$[3] \cdot [3] = [1]$, d.h. $[3] = \frac{[1]}{[3]}$
$[2] \cdot [2] = [0]$, obwohl $[2] \neq [0]$. Man nennt [2] einen Nullteiler.
Die Gleichung $[2] \cdot x = [2]$ hat zwei Lösungen $x = [1]$ und $x = [3]$.
Es gibt keine Zahl $[n]$, so dass $[2] \cdot [n] = [1]$.

1.55 Satz: Sei $m \in \mathbb{N}$, $m \geq 2$ fest. Dann:

1) $[a]$ besitzt ein inverses Element bezüglich $\cdot$ (d.h. eine Restklasse $[b]$ mit $[a] \cdot [b] = [1]$), $\Leftrightarrow$ $\operatorname{ggT}(a, m) = 1$.

2) m ist Primzahl $\Leftrightarrow$ $\forall a \in \{1, \ldots, m-1\}$ $\exists b \in \{1, \ldots, m-1\} : [a] \cdot [b] = [1]$

Beweis: **1)**

$$\begin{aligned}
[a] \cdot [b] = [1] &\Leftrightarrow [ab] = [1] \\
&\Leftrightarrow m \mid (ab - 1) \\
&\Leftrightarrow \exists y \in \mathbb{Z} : \underbrace{my = ab - 1}_{1 = ab - my} \\
&\Leftrightarrow 1 \in \{ax + my : x, y \in \mathbb{Z}\} = \operatorname{ggT}(a, m) \cdot \mathbb{Z} \text{ (vgl. Satz 1.45)} \\
&\Leftrightarrow \operatorname{ggT}(a, m) = 1
\end{aligned}$$

2) "$\Rightarrow$": Aus 1)
"$\Leftarrow$": Zeige: m keine Primzahl $\Rightarrow$ $\exists k \in \mathbb{N} : [k]$ besitzt kein inverses Element.

Sei m keine Primzahl $\Rightarrow$ $\exists k \in D(m) : k \neq 1 \ \wedge \ k \neq m$.
Behauptung: $[k]$ besitzt kein inverses Element.
Für $l \in \mathbb{Z}$ gilt $[k] \cdot [l] = [kl] = \{kl + ym : y \in \mathbb{Z}\}$
Nun gilt: $k \mid (kl + ym)$ $\Rightarrow$ $\forall y \in \mathbb{Z} : kl + ym \neq 1$.
$\Rightarrow$ $1 \notin [kl]$ $\Rightarrow$ $[kl] \neq [1]$.

$\square$

1.10 Darstellung natürlicher Zahlen

Zehnersystem: Stelle alle Zahlen mit den zehn Ziffern $0, 1, \ldots, 9$ dar:

$$\begin{array}{rrrcrl} & 1, & 2, & \ldots & 9 & \\ 10, & 11, & 12, & \ldots & 19 & \text{z.B. } 13 = 1 \cdot 10 + 3 \cdot 1 \\ 20, & 21, & 22, & \ldots & 29 & \\ \vdots & & & & & \\ 100, & 101, & 102, & \ldots & 109 & \text{z.B. } 108 = 1 \cdot 10^2 + 0 \cdot 10^1 + 8 \cdot 10^0 \end{array}$$

Entsprechend geht das auch mit weniger oder mehr Ziffern:

1.56 Definition: Gegeben seien: die **Ziffernbasis** $g \in \mathbb{N},\ g \geq 2$,
die **Ziffern**: Menge mit g Elementen $Z = \{z_0, \ldots, z_{g-1}\}$.

Die Darstellung

$$n \;=\; (a_N a_{N-1} \ldots a_0)_g \;:=\; \sum_{j=0}^{N} a_j g^j,$$

wobei $N \in \mathbb{N},\ a_0, \ldots, a_N \in Z$, heißt ***g*-adische Entwicklung** von $n \in \mathbb{N}$.

Z.B: Zweier-System: $g = 2,\ Z = \{0, 1\}$:
$1011_2 = (1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0)_{10} = (8 + 0 + 2 + 1)_{10} = 11_{10}$.

Z.B: Hexadezimalsystem: $g = 16,\ z = \{0, 1, \ldots, 9, A, B, C, D, E, F\}$:
$D2A_{16} = D\,g^2 + 2\,g^1 + A\,g^0 = (13 \cdot 256 + 2 \cdot 16 + 10 \cdot 1)_{10} = 3370_{10}$.

1.57 Satz: Seien g, Z fest. Jede Zahl $n \in \mathbb{N}$ besitzt eine eindeutige g-adische Darstellung: Es existieren eindeutig bestimmte Zahlen $N \in \mathbb{N}$ und $a_0, \ldots, a_N \in Z$, so dass

$$n = (a_N a_{N-1} \ldots a_0)_g \;\wedge\; a_N \neq z_0.$$

Beweis: Existenz (konstruktiv):

Teilen mit Rest:

$$\begin{array}{rclcrcl} n & = & q_1 \cdot g + r_1 & \Rightarrow & a_0 & = & r_1 \\ q_1 & = & q_2 \cdot g + r_2 & \Rightarrow & a_1 & = & r_2 \\ & \vdots & & & & & \\ q_{N-2} & = & q_{N-1} \cdot g + r_{N-1} & \Rightarrow & a_{N-2} & = & r_{N-1} \\ q_{N-1} & = & q_N \cdot g + r_N & \Rightarrow & a_{N-1} & = & r_N \end{array}$$

Verfahren bricht ab, wenn $0 < q_N < g$. Dann setze noch $a_N := q_N$.

Rückwärts hochgehen:

$$\begin{array}{rclcl} q_{N-1} & = & a_N \cdot g + a_{N-1} & & \\ q_{N-2} & = & q_{N-1} \cdot g + a_{N-2} & = & a_N \cdot g^2 + a_{N-1} \cdot g + a_{N-2} \\ q_{N-3} & = & q_{N-2} \cdot g + a_{N-3} & = & a_N \cdot g^3 + a_{N-1} \cdot g^2 + a_{N-2} \cdot g + a_{N-3} \\ & \vdots & & & \\ n & = & \ldots & = & a_N \cdot g^N + \ldots + a_1 \cdot g + a_0 \end{array}$$

$\square$

Z.B: 2007 im Fünfersystem:
$$\begin{aligned} 2007:5 &= 401 \quad \text{Rest } 2 \Rightarrow a_0 = 2 \\ 401:5 &= 80 \quad \text{Rest } 1 \Rightarrow a_1 = 1 \\ 80:5 &= 16 \quad \text{Rest } 0 \Rightarrow a_2 = 0 \\ 16:5 &= 3 \quad \text{Rest } 1 \Rightarrow a_3 = 1 \end{aligned}$$

Verfahren bricht ab, da $3 < 5$. Also $a_4 = 3$ und $(2007)_{10} = (31012)_5$.

1.11 Mächtigkeit von Mengen

1.58 Definition: Zwei Mengen A, B heißen **gleich groß** oder **gleich mächtig**, falls es eine bijektive Abbildung $f : A \to B$ gibt.

Z.B.: $f : \{1, 2, 3\} \to \{4, 5, 6\} : x \mapsto x + 3$ ist bijektiv

Z.B.: $f :]-\infty, -3] \to [-3, \infty[: x \mapsto -6 - x$ (Spiegelung an -3) ist bijektiv, also sind die Mengen gleich mächtig.

Z.B.: $G := \{2n : n \in \mathbb{N}\}$ und $\mathbb{N}$ sind gleich mächtig, obwohl G echte Teilmenge von $\mathbb{N}$.

Z.B.: $\mathbb{Q}$ ist gleich mächtig wie $\mathbb{N}$.

1.59 Definition: Sei A eine Menge.

1) A heißt **endlich**, falls jede injektive Abbildung $f : A \to A$ auch surjektiv ist. ($\emptyset$ ist automatisch endlich.)

2) A heißt **unendlich**, falls A nicht endlich. D.h. falls es eine injektive Abbildung $f : A \to A$ gibt, die nicht surjektiv ist, oder falls A gleich mächtig ist wie eine echte Teilmenge von A.

3) A heißt **abzählbar unendlich**, falls A gleich mächtig wie $\mathbb{N}$ ist.

4) A heißt **überabzählbar**, falls A unendlich und nicht abzählbar unendlich ist.

Z.B.: $\mathbb{Q}$ ist abzählbar. Später: $\mathbb{R}$ ist überabzählbar.

2 Zahlenkörper

2.1 Mengen und Verknüpfungen

Was ist $+$? Eine Abbildung: $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (a, b) \mapsto a + b$.

2.1 Definition: Sei G Menge. Eine Abbildung $\circ : G \times G \to G : (g, h) \to g \circ h$ heißt **Verknüpfung** auf G.

1) Eine Verknüpfung heißt **assoziativ**, falls

$$\forall g, h, j \in G : g \circ (h \circ j) = (g \circ h) \circ j.$$

2) Eine Verknüpfung heißt **kommutativ**, falls

$$\forall g, h \in G : g \circ h = h \circ g.$$

3) Ein Element $e \in G$ heißt **neutrales Element**, falls

$$\forall g \in G : e \circ g = g = g \circ e.$$

4) Sei $g \in G$. Ein Element $h \in G$ heißt **inverses Element** zu g, falls $g \circ h = e = h \circ g$. Schreibweise: $g^{-1} := h$.

Z.B.: $(\mathbb{N}, +)$.

Z.B.: $(\mathbb{N}, \cdot)$.

Z.B.: $(\mathbb{Z}, +)$.

Z.B.: $(\mathbb{Q}, \cdot)$.

2.2 Definition: Sei $\circ$ eine Verknüpfung auf G.

1) $(G, \circ)$ heißt **Monoid**, falls $\circ$ assoziativ ist und ein neutrales Element existiert.

2) $(G, \circ)$ heißt **Gruppe**, falls $(G, \circ)$ ein Monoid ist und jedes Element von G ein inverses Element besitzt.

3) $(G, \circ)$ heißt **abelsche Gruppe**, falls $(G, \circ)$ eine Gruppe ist und $\circ$ kommutativ ist.

Z.B.: Monoide sind $(\mathbb{N}_0, +)$, $(\mathbb{N}, \cdot)$, $(\mathcal{P}(M), \cap)$.

Z.B.: Abelsche Gruppen sind $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Wichtiges Beispiel: Die **Permutationsgruppe** $(S(M), \circ)$. Sei

$$\begin{aligned} &M \text{ endliche Menge,} \\ &S(M) := \{\pi : M \to M \mid \pi \text{ ist bijektive Abbildung}\}, \\ &\circ : (\pi_1, \pi_2) \mapsto \pi_1 \circ \pi_2 \text{ (Hintereinanderausführung).} \end{aligned}$$

Dann ist $(S(M), \circ)$ eine Gruppe. Falls $\sharp M \geq 3$ ist diese Gruppe nicht kommutativ.

2.3 Satz: In jeder Gruppe gelten:

1) e ist eindeutig.

2) g^{-1} ist eindeutig.

3) $\forall g, h \in G \;\; \exists! x \in G : g \circ x = h$ (nämlich $x = g^{-1} \circ h$).

4) $\forall g \in G : (g^{-1})^{-1} = g$.

5) $\forall g, h \in G : (g \circ h)^{-1} = h^{-1} \circ g^{-1}$.

Beweis: **1)** Seien e, e' zwei Einselemente. Dann: $e = e' \circ e = e'$.

2) Sei $g \circ g^{-1} = e = g^{-1} \circ g$ und $g \circ h = e = h \circ g$.

$$\Rightarrow \quad h = e \circ h = (g^{-1} \circ g) \circ h = g^{-1} \circ (g \circ h) = g^{-1} \circ e = g^{-1}.$$

3) Existenz: $x := g^{-1} \circ h \;\Rightarrow\; g \circ x = g \circ (g^{-1} \circ h) = (g \circ g^{-1}) \circ h = e \circ h = h$.
Eindeutigkeit: $g \circ x = h \;\Rightarrow\; g^{-1} \circ g \circ x = g^{-1} \circ h \;\Rightarrow\; x = g^{-1} \circ h$.

4), **5)** als Übung. $\square$

Schreibweise: Für $g \in G$ und $n \in \mathbb{Z}$ setzt man

$$g^n := \begin{cases} \underbrace{g \circ \ldots \circ g}_{n \text{ Mal}} & \text{für } n \in \mathbb{N}, \\ e & \text{für } n = 0, \\ \underbrace{g^{-1} \circ \ldots \circ g^{-1}}_{-n \text{ Mal}} & \text{für } -n \in \mathbb{N} \end{cases}$$

Dann gilt $g^n \circ g^m = g^{n+m}$ für $n, m \in \mathbb{Z}$.

2.2 Zwei Verknüpfungen

2.4 Definition: Auf der Menge R seien zwei Verknüpfungen $+, \cdot$ definiert.

1) $(R, +, \cdot)$ heißt **Ring**, falls

- **a)** $(R, +)$ ist abelsche Gruppe,
- **b)** $(R, \cdot)$ ist Monoid,
- **c)** Es gelten die **Distributivgesetze**:

$$\forall g, h, j \in R : (g + h) \cdot j = g \cdot j + h \cdot j \ \wedge g \cdot (h + j) = g \cdot h + g \cdot j.$$

- **d)** $0 \neq 1$ ($0 =$ neutrales Element bezüglich $+$ und $1 =$ neutrales Element bezüglich $\cdot$).

2) $(R, +, \cdot)$ heißt **kommutativer Ring**, falls zusätzlich zu 1) $\cdot$ kommutitativ ist.

3) $(R, +, \cdot)$ heißt **Körper** (*englisch: field*), falls zusätzlich zu 1) $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist.

Z.B.: $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring.

Z.B.: $(\mathbb{Q}, +, \cdot)$ ist ein Körper.

Z.B.: p Primzahl. Dann ist $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ein Körper.

Z.B.: m keine Primzahl. Dann ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring.

Z.B.: $R := \{f : \mathbb{Q} \to \mathbb{Q} \text{ Abbildung}\}$
$f + g : x \mapsto f(x) + g(x)$
$f \cdot g : x \mapsto f(x) \cdot g(x)$
Dann ist $(R, +, \cdot)$ ein kommutativer Ring.

2.5 Schreibweisen:

$$\begin{aligned}
-x &:= \text{Inverses bezüglich } + \\
x - y &:= x + (-y) \\
\frac{1}{x} := x^{-1} &:= \text{Inverses bezüglich } \cdot \\
\frac{x}{y} &:= x \cdot y^{-1} \text{ (oder auch } x : y) \\
x^n &:= \underbrace{x \cdot x \cdots x}_{n \text{ mal}}, \qquad x^{-n} := (x^{-1})^n
\end{aligned}$$

2.6 Folgerungen: Sei $(\mathbb{K}, +, \cdot)$ ein Körper. Für $a, b, c, d \in \mathbb{K}$ gelten:

1) $-(-x) = x$

2) $0 \cdot x = x \cdot 0 = 0$

3) $x \cdot y = 0 \ \Rightarrow \ x = 0 \vee y = 0$

4) $(-x) \cdot y = -(x \cdot y)$

5) $(-x) \cdot (-y) = x \cdot y$

6) $\dfrac{1}{\frac{1}{x}} = x$

7) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a \cdot d + b \cdot c}{b \cdot d}$

8) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a \cdot c}{b \cdot d}$

9) $\dfrac{a}{b} : \dfrac{c}{d} = \dfrac{a}{b} \cdot \dfrac{d}{c} = \dfrac{a \cdot d}{b \cdot c}$

2.3 Die reellen Zahlen

2.7 Definition: Die **reellen Zahlen** $(\mathbb{R}, +, \cdot)$ bilden einen Körper mit folgenden Eigenschaften:

(O) $(\mathbb{R}, <)$ ist ein angeordneter Körper,

(A) $(\mathbb{R}, <)$ ist ein archimedischer Körper,

(V) $(\mathbb{R}, |.|)$ ist vollständig.

2.3.1 Die Anordnung in $\mathbb{R}$ und Folgerungen

***2.8 Axiom* (O):** $(\mathbb{R}, <)$ ist ein **angeordneter Körper**, d.h. auf $\mathbb{R}$ ist eine Relation $<$ (kleiner) definiert, so dass:

(O1) $\forall a, b \in \mathbb{R}$: Genau eine der Beziehungen $a < b$, $a = b$, $b < a$ ist wahr.

(O2) $\forall a, b, c \in \mathbb{R} : a < b \ \wedge\ b < c \ \Rightarrow\ a < c$ (Transitivität).

(O3) $\forall a, b, c \in \mathbb{R} : a < b \ \Rightarrow\ a + c < b + c$ (Verträglichkeit mit Addition).

(O4) $\forall a, b, c \in \mathbb{R} : a < b \ \wedge\ 0 < c \ \Rightarrow\ a\,c < b\,c$ (Verträglichkeit mit Multiplikation).

2.9 Bemerkungen: **1)** Für $a < b$ schreibe auch $b > a$ (größer).

2) $a \in \mathbb{R}$ heißt **positiv**, falls $a > 0$. Sei

$$\mathbb{R}^+ := \{a \in \mathbb{R} : a > 0\}, \qquad \mathbb{R}_0^+ := \mathbb{R}^+ \cup \{0\}.$$

3) Definiere

$$\begin{aligned} a \le b \quad &:\Leftrightarrow \quad a < b \ \vee\ a = b, \\ a \ge b \quad &:\Leftrightarrow \quad a > b \ \vee\ a = b; \end{aligned}$$

$\le$ und $\ge$ sind Ordnungsrelationen auf $\mathbb{R}$.

4) Ein Ausdruck der Form $a < b,\ a \le b,\ a > b,\ a \ge b$ heißt **Ungleichung**.

5) Endliche Körper können nicht angeordnet werden (siehe (U6) unten).

2.10 Folgerungen: **(U1)** $a < b \ \Leftrightarrow\ 0 < b - a \ \Leftrightarrow\ b - a > 0$

(U2) $a < b \ \wedge\ x < y \ \Rightarrow\ a + x < b + y$.
Insbesondere: $a < 0 \ \wedge\ x < 0 \ \Rightarrow\ a + x < 0$; $\quad 0 < b \ \wedge\ 0 < y \ \Rightarrow\ 0 < b + y$.

(U3) $a > 0 \Leftrightarrow -a < 0$ und $a < 0 \Leftrightarrow -a > 0$.

(U4) $0 < a < b \wedge 0 < x < y \Rightarrow a\,x < b\,y$.

(U5) $a < 0 \wedge x < y \Rightarrow a\,x > a\,y$.
Insbesondere: $a < 0 \wedge x < 0 \Rightarrow a\,x > 0$; $a < 0 \wedge 0 < y \Rightarrow 0 > a\,y$, d.h. Multiplikation von Ungleichungen mit negativen Zahlen vertauscht $<$ und $>$.

(U6) $a \neq 0 \Rightarrow a^2 > 0$. Insbesondere: $1 = 1^2 > 0$.
In endlichen Körpern gibt es keine Ordnung: $1 > 0 = 1 + 1 + \ldots + 1$.

(U7) $a > 0 \Rightarrow \frac{1}{a} > 0$; $a < 0 \Rightarrow \frac{1}{a} < 0$.

(U8) $0 < a < b \Rightarrow \frac{1}{a} > \frac{1}{b}$.

(U9) $0 < a < b \Rightarrow \frac{b}{a} > 1$.

2.11 Satz (Bernoulli-Ungleichung): Für $x \in \mathbb{R},\ x \geq -1$ und $n \in \mathbb{N}_0$ gilt

$$(1+x)^n \ \geq\ 1 + nx.$$

2.12 Intervalle: Sei $a < b$. Definiere

$$\begin{array}{rcll} [a,b] & := & \{x \in \mathbb{R} : a \leq x \leq b\} & \text{(abgeschlossenes Intervall)} \\ ]a,b[& := & \{x \in \mathbb{R} : a < x < b\} & \text{(offenes Intervall)} \\ [a,b[& := & \{x \in \mathbb{R} : a \leq x < b\} & \text{(rechts halboffenes Intervall)} \\ [a,\infty[& := & \{x \in \mathbb{R} : a \leq x\} & \end{array}$$

analog: $]a,b]$; $]-\infty,b]$; $]-\infty,b[$; $]a,\infty[$; $]-\infty,\infty[= \mathbb{R}$.

2.13 $\mathbb{N}$***,*** $\mathbb{Z}$***,*** $\mathbb{Q}$ ***in*** $\mathbb{R}$***:*** **1)** Identifiziere $\mathbb{N}$ als Teilmenge von $\mathbb{R}$: Definiere $f : \mathbb{N} \to \mathbb{R}$ durch

$$f(1_{\mathbb{N}}) := 1_{\mathbb{R}}, \quad f(n + 1_{\mathbb{N}}) := f(n) + 1_{\mathbb{R}}.$$

Nach dem Induktionsaxiom ist f für alle $n \in \mathbb{N}$ definiert.
Setze $\widetilde{\mathbb{N}} := f(\mathbb{N}) = \{f(n) : n \in \mathbb{N}\}$.

Die Abbildung f ist injektiv: Zeige $n \neq m \Rightarrow f(n) \neq f(m)$:
Sei $n \neq m$. O.B.d.A. $n < m$, also $m = n + k$.
$\Rightarrow f(n) < f(n) + 1_{\mathbb{R}} = f(n + 1_{\mathbb{N}}) < f(n + 2_{\mathbb{N}}) < \ldots < f(n+k) = f(m)$.
$\overset{\text{(O1)}}{\Rightarrow} f(n) \neq f(m)$.

Also: $f : \mathbb{N} \to \widetilde{\mathbb{N}}$ ist bijektiv.
Damit gelten die Peano-Axiome automatisch in $\widetilde{\mathbb{N}}$ mit Nachfolger$(n) = n + 1_{\mathbb{R}}$.
Identifiziere nun $\mathbb{N}$ mit $\widetilde{\mathbb{N}}$, schreibe im Folgenden $\mathbb{N}$ anstelle von $\widetilde{\mathbb{N}}$. (Typisches Mathematisches Vorgehen.)

2) Setze $\mathbb{Z} := \{k \in \mathbb{R} \mid \exists n, m \in \mathbb{N} : k = n - m\}$.

3) Setze $\mathbb{Q} := \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z},\ q \in \mathbb{N} : x = \frac{p}{q}\}$.

Wir übertragen Arithmetik und Ordnung von $\mathbb{R}$ auf diese Teilmengen, soweit das geht.

2.14 Definition: Der **Betrag** oder **Absolutbetrag** von $x \in \mathbb{R}$ ist definiert durch

$$|x| := \begin{cases} x & \text{für } x \geq 0 \\ -x & \text{für } x < 0\ . \end{cases}$$

Insbesondere gelten

$$|x| \ \geq \ x, \quad |x| \ = \ |-x| \ \geq \ -x.$$

2.15 Eigenschaften von |.| : Für $x, y \in \mathbb{R}$ gelten:

(B1) $|x| \geq 0 \quad \wedge \quad (|x| = 0 \ \Leftrightarrow \ x = 0)$

(B2) $|x \cdot y| = |x| \cdot |y|$

(B3) $|x + y| \ \leq \ |x| + |y|$ (**Dreiecksungleichung**, **$\boldsymbol{\Delta}$-Ungleichung**)

Beweis: (B1)
$$\begin{aligned} x > 0 \ &\Rightarrow \ |x| = x > 0 \\ x = 0 \ &\Rightarrow \ |x| = x = 0 \\ x < 0 \ &\Rightarrow \ |x| = -x > 0 \quad \text{(nach (U3))} \end{aligned}$$

(B1) Unterscheide 4 mögliche Fälle $x \geq 0 \ \wedge y \geq 0, \ldots$, getrennt nachrechnen.

(B1)
$$\begin{aligned} x + y \geq 0 \ &\Rightarrow \ |x + y| = x + y \leq |x| + |y| \\ x + y < 0 \ &\Rightarrow \ |x + y| = -(x + y) = (-x) + (-y) \leq |x| + |y| \end{aligned}$$
□

2.16 Definition: Ein Körper $(\mathbb{K}, +, \cdot)$ mit einem Betrag, d.h. einer Funktion $|.| : \mathbb{K} \to \mathbb{R}_0^+$ mit (B1), (B2), (B3) heißt **bewerteter Körper** (z.B. auch $\mathbb{C}$).

2.17 Folgerungen: In jedem bewerteten Körper gelten:

1) $|1| \ = \ |-1| \ = \ 1,$ insbesondere $|-x| \ = \ |x|$.

2) $\left|\dfrac{x}{y}\right| \ = \ \dfrac{|x|}{|y|}$ falls $y \neq 0$.

3) $|x-y| \;\geq\; \big||x|-|y|\big| \quad (\geq\; |x|-|y|),$
$|x+y| \;\geq\; \big||x|-|y|\big|$
(**Δ-Ungleichung nach unten**).

Beweis: **1)** $1 = 1^2 > 0 \;\Rightarrow\; |1| = 1.$
$1 > 0 \;\Rightarrow\; -1 < 0 \;\Rightarrow\; |-1| = -(-1) = 1$
$|-x| = |-(1\cdot x)| = |(-1)\cdot x| = |-1|\cdot|x| = 1\cdot|x| = |x|.$

2) $x = \dfrac{x}{y}\cdot y \;\Rightarrow\; |x| = \left|\dfrac{x}{y}\right|\cdot|y| \;\Rightarrow$ Behauptung.

3) Als Übung

$\square$

2.18 Definition: In einem bewerteten Körper ist der **Abstand** zweier Elemente $x, y \in \mathbb{K}$ definiert durch

$$d(x,y) \;:=\; |x-y|.$$

Die Abstandsfunktion $d : \mathbb{K}\times\mathbb{K} \to \mathbb{R}_0^+$ besitzt die Eigenschaften

(M1) $d(x,y) \;\geq\; 0 \quad\wedge\quad (d(x,y) \;=\; 0 \;\Leftrightarrow\; x = y)$ (**Positivität**, **Definitheit**).

(M2) $d(x,y) \;=\; d(y,x)$ (**Symmetrie**).

(M3) $d(x,y) \;\leq\; d(x,z) + d(z,y)$ (**Δ-Ungleichung**).

Diese drei Eigenschaften werden später dazu benützt, abstrakt den Begriff eines Abstandes (Metrik) zu definieren.

Z.B.: $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R},\; d\big((x_1,y_1),(x_2,y_2)\big) \;:=\; \sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$ (euklidischer Abstand).

2.19 Definition: Sei M Menge. Eine **Folge in M** ist eine Abbildung $\mathbb{N} \ni n \mapsto x_n \in M$. Schreibweise: (x_n) oder $(x_n)_{n\in\mathbb{N}}$.

2.20 Konvergenz: Sei $(\mathbb{K}, |.|)$ bewerteter Körper. Die Folge (x_n) in $\mathbb{K}$ heißt **konvergent gegen $\boldsymbol{x}$**, falls

$$\forall \varepsilon > 0 \quad \exists N_\varepsilon \in \mathbb{N} \quad \forall n > N_\varepsilon : |x_n - x| \ < \ \varepsilon.$$

D.h. für jedes noch so kleine $\varepsilon > 0$ ist der Abstand aller x_n zu x kleiner als ε, sobald $n > N_\varepsilon$ gilt. In diesem Fall schreiben wir

$$x \ = \ \lim_{n\to\infty} x_n, \qquad x_n \stackrel{n\to\infty}{\longrightarrow} x, \qquad x_n \to x \text{ für } n \to \infty;$$

x heißt **Grenzwert** oder **Limes** der Folge. Eine Folge (x_n) heißt **konvergent**, falls

$$\exists x \in \mathbb{K} : x = \lim_{n\to\infty} x_n.$$

Ist eine Folge nicht konvergent, so heißt sie **divergent**.

2.21 Eindeutigkeit des Grenzwertes: Sei $(\mathbb{K}, |.|)$ bewerteter Körper. Ist $\lim\limits_{n\to\infty} x_n = x$, so besitzt (x_n) keinen weiteren Grenzwert.

Beweis: Annahme: $x = \lim\limits_{n\to\infty} x_n \ \wedge \ y = \lim\limits_{n\to\infty} x_n \ \wedge \ x \neq y$.

Wähle $\varepsilon := \dfrac{|x-y|}{2}$. Dann: $\exists N_\varepsilon \in \mathbb{N} \quad \forall n > N_\varepsilon : |x_n - x| \ < \ \varepsilon$

$\exists \widetilde{N}_\varepsilon \in \mathbb{N} \quad \forall n > \widetilde{N}_\varepsilon : |x_n - y| \ < \ \varepsilon$

Für $n > \max\{N_\varepsilon, \widetilde{N}_\varepsilon\}$ folgt

$$|x-y| = |x - x_n + x_n - y| \leq |x - x_n| + |x_n - y| = |x - x_n| + |y - x_n| < 2\varepsilon = |x-y| \quad ↯$$

$\square$

2.22 Satz: Sei (x_n) konvergente Folge in $\mathbb{R}$ und $K \in \mathbb{R}$, $N \in \mathbb{N}$. Dann

$$(\forall n \geq N : x_n \leq K) \ \Rightarrow \ \lim_{n\to\infty} x_n \leq K,$$
$$(\forall n \geq N : x_n \geq K) \ \Rightarrow \ \lim_{n\to\infty} x_n \geq K.$$

2.23 Achtung: $x_n := \dfrac{1}{n} > 0$, aber $\underbrace{\lim\limits_{n\to\infty} x_n = 0}_{\text{Beweis später}}.$

2.3.2 Die archimedische Anordnung

2.24 Axiom* (A)*: $(\mathbb{R}, <)$ ist ein **archimedisch geordneter** Körper, d.h. es gilt

$$\forall x \in \mathbb{R} \quad \exists n \in \mathbb{N} : n > x.$$

2.25 Folgerungen: Aus (A) folgt

1) $\forall y \in \mathbb{R} \quad \forall x \in \mathbb{R}^+ \quad \exists n \in \mathbb{N} : n\,x > y$

2) $\forall x \in \mathbb{R}_0^+ \quad \exists! n \in \mathbb{N}_0 : n \leq x < n + 1$
Definiere die **untere Gaußklammer**: $\lfloor x \rfloor := \max\{n \in \mathbb{N}_0 : n \leq x\}$.

3) $\forall \varepsilon > 0 \quad \exists n \in \mathbb{N} : \frac{1}{n} < \varepsilon$

4) $x \in \mathbb{R}_0^+ \ \wedge \ (\forall n \in \mathbb{N} : x < \frac{1}{n}) \ \Rightarrow \ x = 0$

5) $\forall b > 1 \quad \forall x > 0 \quad \exists n \in \mathbb{N} : b^n > x$

6) $\forall b \in \,]0, 1[\quad \forall \varepsilon > 0 \quad \exists n \in \mathbb{N} : b^n < \varepsilon$

2.26 Anwendung auf Folgen: **1)** $\dfrac{1}{n} \to 0.$

2) Sei $|q| < 1$. Dann $q^n \to 0$.

3) Sei $|q| < 1$ und

$$s_n \ := \ \sum_{j=0}^{n} q^j \ = \ 1 + q + q^2 + \ldots + q^n.$$

Dann $s_n \to \dfrac{1}{1-q}$.

4) Die Folge (x_n) mit $x_n = (-1)^n$ ist nicht konvergent (Beweis später).

2.3.3 Die Vollständigkeit

2.27 Verdichtungsprinzip: Sei (x_n) konvergent. Dann gilt:

$$\forall \varepsilon > 0 \quad \exists N_\varepsilon \in \mathbb{N} \quad \forall n, m > N_\varepsilon : |x_n - x_m| \ < \ \varepsilon. \qquad (*)$$

Beweis: Sei $\varepsilon > 0$. Aus $x_n \to x$: $\exists N_\varepsilon \in \mathbb{N} \quad \forall n > N_\varepsilon : |x_n - x| \ < \ \frac{\varepsilon}{2}$.

Für $n, m > N_\varepsilon$ folgt

$$|x_n - x_m| = |x_n - x + x - x_m| \leq |x_n - x| + |x - x_m| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2}.$$

$\square$

2.28 Definition: Eine Folge (x_n) in einem bewerteten Körper heißt **Cauchy-Folge**, falls sie das Verdichtungsprinzip $(*)$ erfüllt.

Also:

$$\begin{aligned} (x_n) \text{ konvergent } &\Rightarrow (x_n) \text{ Cauchy-Folge} \\ (x_n) \text{ keine Cauchy-Folge } &\Rightarrow (x_n) \text{ divergent} \end{aligned}$$

2.29 Dezimalbrüche: Sei $a_0 \in \mathbb{N}_0$, und für $j \in \mathbb{N}$ sei $d_j \in \{0, 1, \ldots, 9\}$. Setze

$$a_n \;:=\; a_0 + \frac{d_1}{10} + \frac{d_2}{100} + \ldots + \frac{d_n}{10^n} \in \mathbb{Q} \subseteq \mathbb{R}.$$

Schreibe zur Abkürzung $a_n = a_0, d_1 d_2 \ldots d_n$. Man nennt die Folge (a_n) einen **Dezimalbruch**.
Behauptung: (a_n) ist eine Cauchy-Folge.

Beweis: Sei $m > n$, also $m = n + k$. Dann gilt

$$\begin{aligned} |a_m - a_n| = a_m - a_n \;&=\; \frac{d_{n+1}}{10^{n+1}} + \ldots + \frac{d_{n+k}}{10^{n+k}} \\ &\le\; \frac{9}{10^{n+1}} + \ldots \frac{9}{10^{n+k}} \\ &=\; \frac{9}{10^{n+1}} \left(1 + \frac{1}{10} + \ldots \frac{1}{10^{k-1}}\right) \\ &=\; \frac{9}{10^{n+1}} \frac{1 - \left(\frac{1}{10}\right)^k}{1 - \frac{1}{10}} \\ &=\; \frac{9}{10^{n+1}} \frac{10}{9} \left(1 - \left(\frac{1}{10}\right)^k\right) \\ &\le\; \frac{1}{10^n} < \varepsilon \text{ für } n > N_\varepsilon, \text{ da } \left(\frac{1}{10}\right)^n \to 0 \end{aligned}$$

□

2.30 Axiom **(V)*:*** $(\mathbb{R}, |.|)$ ist **vollständig**, d.h. in $\mathbb{R}$ konvergiert jede Cauchy-Folge.

Also: In $\mathbb{R}$ gilt $\qquad (x_n) \text{ konvergent} \Leftrightarrow (x_n) \text{ ist Cauchy-Folge}$

2.31 Satz: **1)** Jeder Dezimalbruch konvergiert gegen eine reelle Zahl.

2) Für jede relle Zahl $x \in \mathbb{R}$ existiert ein Dezimalbruch, der gegen x konvergiert.

Meist identifiziert man x mit dem Dezimalbruch, z.B.

$$\sqrt{2} \;=\; 1,41421\ldots$$

Beweis: **1)** folgt aus (V) und 2.29.

2) Sei $x \in \mathbb{R}_0^+$.
Setze $a_0 := \lfloor x \rfloor$. Dann $0 \le x - a_0 < 1$ und $0 \le 10(x - a_0) < 10$.

Setze $d_1 := \lfloor 10(x - a_0) \rfloor \;\Rightarrow \begin{cases} d_1 \in \{0, \ldots, 9\} \\ \text{Für } a_1 := a_0 + \frac{d_1}{10} \text{ gilt } 0 \le x - a_1 < \frac{1}{10} \end{cases}$

Setze $d_2 := \lfloor 100(x - a_1) \rfloor \;\Rightarrow \begin{cases} d_2 \in \{0, \ldots, 9\} \\ \text{Für } a_2 := a_0 + \frac{d_1}{10} + \frac{d_2}{100} \text{ gilt } 0 \le x - a_2 < \frac{1}{100} \end{cases}$

$\vdots$

Dann ist (a_n) Dezimalbruch und $|x - a_n| < \frac{1}{10^n}$, also $a_n \to x$.

Für $x \in \mathbb{R}^-$ führe Verfahren für $-x$ durch. $\square$

Mit diesem Verfahren erhält man zu x einen eindeutigen Dezimalbruch. Alle Dezimalbrüche kommen vor bis auf diejenigen, für die gilt:

$$\exists n_0 \in \mathbb{N} \;\; \forall n \ge n_0 : d_n = 9.$$

Denn sei z.B. $a_n = 3{,}19\ldots9. \;\Rightarrow\; |3{,}2 - a_n| = 10^{-n} \to 0 \;\Rightarrow\; a_n \to 3{,}2.$
Für $x = 3{,}2$ liefert das obige Verfahren aber $x = 3{,}200\ldots$.

2.32 Bemerkung: Entsprechend kann eine g-adische Entwicklung von $x \in \mathbb{R}$ konstruiert werden:

$$x \;=\; (a_N a_{N-1} \ldots a_0, a_{-1}, a_{-2} \ldots)_g \;:=\; \lim_{n\to\infty} \sum_{k=0}^{n} a_{N-k}\, g^{N-k}$$

mit $N \in \mathbb{N},\; a_j \in \{0, 1, \ldots, g-1\}$.

2.33 Satz ($\mathbb{R}$ und $\mathbb{Q}$): **1)** $\mathbb{Q}$ ist abzählbar ($\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{N}$, Cantorsches Diagonalverfahren).

2) $\mathbb{R}$ ist überabzählbar. Insbesondere $\mathbb{Q} \subsetneqq \mathbb{R}$.

3) Für jedes $x \in \mathbb{R}$ existiert eine Folge (q_n) in $\mathbb{Q}$ mit $x = \lim\limits_{n\to\infty} q_n$.
Man sagt: $\mathbb{Q}$ liegt **dicht** in $\mathbb{R}$.

Beweis: **1)** Schon gemacht

2) Zeige: Ist $f : \mathbb{N} \to \mathbb{R}$, so ist f nicht surjektiv.
Sei also eine Abbildung $f : \mathbb{N} \to \mathbb{R}$ gegeben. Definiere $x := 0, d_1\, d_2 \ldots$, wobei

$$d_j \;:=\; \begin{cases} 0 & \text{falls } f(j) = \tilde{a_0}, \tilde{d}_1\, \tilde{d}_2 \ldots \text{ und } \tilde{d}_j \ne 0 \\ 1 & \text{falls } f(j) = \tilde{a_0}, \tilde{d}_1\, \tilde{d}_2 \ldots \text{ und } \tilde{d}_j = 0 \end{cases}$$

$\Rightarrow\; x \in \mathbb{R} \;\wedge\; x \ne f(j)$ für $j \in \mathbb{N}$
$\Rightarrow\; x \in \mathbb{R} \setminus f(\mathbb{N})$.

3) Wähle $(q_n) =$ zu x konstruierter Dezimalbruch. $\square$

Also: Auf dem Zahlenstrahl hat die Menge $\mathbb{Q}$ Lücken. Die Menge der Lücken ist größer als $\mathbb{Q}$.

2.34 Definition: **1)** Eine Folge (a_n) heißt **monoton wachsend / monoton fallend**, falls $a_{n+1} \geq a_n$ / $a_{n+1} \leq a_n$ für $n \in \mathbb{N}$.

2) Seien $(a_n), (b_n)$ Folgen in $\mathbb{R}$. Die Folge von Intervallen $([a_n, b_n])$ heißt **Intervallschachtelung**, falls

- (a_n) monoton wachsend, (b_n) monoton fallend,
- $\forall n \in \mathbb{N} : a_n \leq b_n$,
- $\lim\limits_{n\to\infty} (b_n - a_n) = 0$.

2.35 Satz: Ist $([a_n, b_n])_{n\in\mathbb{N}}$ eine Intervallschachtelung, so konvergieren die Folgen $(a_n), (b_n)$ gegen denselben Grenzwert. Außerdem existiert genau ein $x \in \mathbb{R}$ mit $x \in \bigcap\limits_{n=1}^{\infty} [a_n, b_n]$, nämlich $x = \lim\limits_{n\to\infty} a_n = \lim\limits_{n\to\infty} b_n$.

Beweis: **(i)** (a_n) konvergiert: Sei $\varepsilon > 0$.
$b_n - a_n \to 0 \;\Rightarrow\; \exists N_\varepsilon \in \mathbb{N} \;\; \forall n > N_\varepsilon |b_n - a_n| < \varepsilon$.
Für $m > n > N_\varepsilon$ folgt $|a_m - a_n| = a_m - a_n \leq b_m - a_n \leq b_n - a_n < \varepsilon$
$\Rightarrow\; (a_n)$ ist Cauchy-Folge
$\Rightarrow\; a_n \to a \in \mathbb{R}$.

(ii) $b_n \to a$: Sei $\varepsilon > 0$.

$$\begin{aligned} b_n - a_n \to 0 \;\;&\Rightarrow\;\; \exists N_\varepsilon \in \mathbb{N} \;\; \forall n > N_\varepsilon |b_n - a_n| < \frac{\varepsilon}{2} \\ a_n \to a \;\;&\Rightarrow\;\; \exists \tilde{N}_\varepsilon \in \mathbb{N} \;\; \forall n > \tilde{N}_\varepsilon |a_n - a| < \frac{\varepsilon}{2} \end{aligned}$$

$\Rightarrow\;$ für $n > \max\{N_\varepsilon, \tilde{N}_\varepsilon\} : |b_n - a| = |b_n - a_n + a_n - a| \leq |b_n - a_n| + |a_n - a| < \varepsilon$.

(iii) $a \in [a_n, b_n]$ für alle $n \in \mathbb{N}$: Sei $n \in \mathbb{N}$ fest.

$$\left.\begin{array}{lll} \text{Für } m > n: & a_m \leq b_m \leq b_n & \Rightarrow\; a = \lim_{m\to\infty} a_m \leq b_n \\ \text{Für } m > n: & a_n \leq a_m & \Rightarrow\; a_n \leq \lim_{m\to\infty} a_m = a \end{array}\right\} \;\Rightarrow\; a_n \leq a \leq b_n.$$

(iv) Eindeutigkeit: $y < x \;\Rightarrow\; \exists n \in \mathbb{N} : a_n > y \;\Rightarrow\; y \notin \bigcap_{n\in\mathbb{N}} [a_n, b_n]$
$y > x \;\Rightarrow\; \exists n \in \mathbb{N} : b_n < y \;\Rightarrow\; y \notin \bigcap_{n\in\mathbb{N}} [a_n, b_n]$ $\square$

2.36 Definition: Sei $M \subseteq \mathbb{R}$, $M \neq \emptyset$.

1) $a \in \mathbb{R}$ heißt eine **obere** (**untere**) **Schranke** von M, falls

$$\forall x \in M : x \leq a \quad (x \geq a)$$

2) M heißt **nach oben beschränkt**, falls M eine (und damit unendlich viele) obere Schranke besitzt. Analog: Nach unten beschränkt.
M heißt **beschränkt**, falls M eine obere und eine untere Schranke besitzt.

3) $a \in \mathbb{R}$ heißt **maximales** (**minimales**) Element von M oder **Maximum** (**Minimum**) von M, falls

$$a \in M \ \wedge \ \forall x \in M : x \leq a \quad (x \geq a)$$

Schreibe $a = \max M$ bzw. $a = \min M$.

4) $a \in \mathbb{R}$ heißt **Supremum** von M, falls a kleinste obere Schranke ist:

$$\big(\forall x \in M : x \leq a\big) \ \wedge \ \big((\forall x \in M : x \leq b) \ \Rightarrow \ b \geq a\big).$$

Analog: **Infimum** = größte untere Schranke. Schreibe $a = \sup M$ bzw. $a = \inf M$.

5) Falls M nicht nach oben beschränkt ist, besitzt M kein Supremum. Schreibe dann: $\sup M = \infty$. Genauso $\inf M = -\infty$, falls M nicht nach unten beschränkt.

Z.B.:
$$\begin{aligned} M_1 &= \ ]-\infty, 1] \\ M_2 &= \ ]2, \infty[\\ M_3 &= \ [0, 3[\\ M_4 &= \ \{\tfrac{1}{n} : n \in \mathbb{N}\} \ = \ \{1, \tfrac{1}{2}, \tfrac{1}{3}, \ldots\} \end{aligned}$$

2.37 Satz(Existenz Infimum/Supremum): Jede nach unten (oben) beschränkte Menge $\emptyset \neq M \subseteq \mathbb{R}$ besitzt ein Infimum (Supremum).

Beweis: Intervallschachtelung.

Für Infimum: Wähle a_0 untere Schranke, $b_0 \in M$. Setze $x_1 := \dfrac{a_0 + b_0}{2}$.

Entweder: x_1 ist untere Schranke. Dann $a_1 := x_1, \ b_1 := b_0$.
Oder: x_1 ist keine untere Schranke: $\exists y \in M : a_0 \leq y < x_1$. Dann: $a_1 := a_0, \ b_1 := y$

Setze $x_2 := \dfrac{a_1 + b_1}{2}$.

$\vdots$

Dann ist $[a_n, b_n]$ Intervallschachtelung mit

$$\forall n \in \mathbb{N} : a_n \text{ ist untere Schranke } \wedge\ b_n \in M\ \wedge\ 0 \le b_n - a_n \le \frac{1}{2^n}(b_0 - a_0)$$

$\Rightarrow\ a := \bigcap_{n=1}^{\infty} [a_n, b_n]$ ist Infimum. $\square$

2.38 Hauptsatz über monotone Folgen: Ist (a_n) monoton wachsend und nach oben beschränkt ($a_n \le K$ für $n \in \mathbb{N}$) oder monoton fallend und nach unten beschränkt, so ist (a_n) konvergent.

Beweis: Sei (a_n) monoton wachsend, $a_n \le K$. Setze $a := \sup\{a_n : n \in \mathbb{N}\}$.
Behauptung: $a = \lim_{n\to\infty} a_n$.
Sei $\varepsilon > 0$ fest. $a - \varepsilon$ ist keine obere Schranke.
$\Rightarrow\ \exists N_\varepsilon \in \mathbb{N} : a_{N_\varepsilon} > a - \varepsilon$.

$$\Rightarrow\ \forall n > N_\varepsilon :\ \left.\begin{array}{l} a_n \ge a_{N_\varepsilon} > a - \varepsilon \\ a_n \le a \end{array}\right\} \Rightarrow\ |a - a_n| < \varepsilon.$$

$\square$

2.39 Existenz der Wurzel: Sei $a \in \mathbb{R}^+$ und $x_0 \in \mathbb{R}^+$. Definiere (x_n) rekursiv durch

$$x_{n+1} \ := \ \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) \qquad (n \in \mathbb{N}_0).$$

Dann existiert

$$b \ := \ \lim_{n\to\infty} x_n,$$

und es gilt $b^2 = a$ und $b \ge 0$, d.h. $b =: \sqrt{a}$ (Babylonisches Wurzelziehen, Heron-Verfahren).

Beweis: **1)** $x_n > 0$: Induktionsanfang: $x_0 > 0$

Induktionsschritt: $x_n > 0\ \Rightarrow\ x_{n+1} = \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) > 0$

Induktionsschluss: $x_n > 0$ für alle $n \in \mathbb{N}_0$.

2) $\forall n \in \mathbb{N} : x_n^2 \ge a$:

$$\begin{aligned} x_n^2 - a &= \frac{1}{4}\left(x_{n-1} + \frac{a}{x_{n-1}}\right)^2 - a \\ &= \frac{1}{4}\left(x_{n-1}^2 + 2a + \left(\frac{a}{x_{n-1}}\right)^2 - 4a\right) \\ &= \frac{1}{4}\left(x_{n-1} - \frac{a}{x_{n-1}}\right)^2 \\ &\ge 0 \end{aligned}$$

3) (x_n) ist monoton fallend ab $n = 1$:

$$x_n - x_{n+1} \;=\; x_n - \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) \;=\; \frac{1}{2}\left(x_n - \frac{a}{x_n}\right) \;=\; \frac{1}{2x_n}\left(x_n^2 - a\right) \overset{1),\,2)}{\geq} 0$$

4) Wegen $x_1 \geq x_n > 0$ und der Monotonie konvergiert (x_n).

$$b := \lim_{n\to\infty} x_n \;\geq\; 0.$$

Es gilt $b > 0$: $\quad b^2 \overset{\text{siehe später}}{=} \lim_{n\to\infty} x_n^2 \overset{2)}{\geq} a \;>\; 0.$

5) $b^2 = a$:

$$\begin{aligned} b \;&=\; \lim_{n\to\infty} x_n \;=\; \lim_{n\to\infty} x_{n+1} \;=\; \lim_{n\to\infty} \frac{1}{2}\left(x_n + \frac{a}{x_n}\right) \overset{\text{siehe später}}{=} \frac{1}{2}\left(b + \frac{a}{b}\right) \\ \Rightarrow\;\; 2b \;&=\; b + \frac{a}{b} \\ \Leftrightarrow\;\; b - \frac{a}{b} \;&=\; 0 \\ \Leftrightarrow\;\; b^2 - a \;&=\; 0 \end{aligned}$$

□

2.40 Bemerkungen: **1)** Definiert man den **relativen Fehler** $d_n := \frac{x_n - \sqrt{a}}{x_n}$, dann zeigt eine kurze Rechnung

$$d_{n+1} \;\leq\; d_n^2.$$

Insbesondere verdoppelt sich die Zahl der richtigen Nachkommastellen bei jedem Schritt.

2) Wir wissen: $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

Analog: Sei $k \in \mathbb{N},\; k \geq 2$. Setze

$$x_{n+1} \;:=\; \frac{1}{k}\left((k-1)x_n + \frac{a}{x_n^{k-1}}\right), \quad x_0 > 0.$$

Dann existiert $b := \lim_{n\to\infty} x_n$, und es gilt $b^k = a$ und $b \geq 0$. Schreibe $b =: \sqrt[k]{a}$.

2.41 Die Zahl* e*: Sei $a_n \;:=\; \left(1 + \frac{1}{n}\right)^n$.

Dann ist (a_n) monoton und beschränkt, also konvergent. Der Grenzwert heißt **Eulersche Zahl**:

$$\mathrm{e} \;:=\; \lim_{n\to\infty}\left(1 + \frac{1}{n}\right)^n \;=\; 2,7182818\ldots$$

Man kann zeigen: e ist irrational. Neben π ist e eine der wichtigsten Zahlen in der Mathematik.

Monotonie:

$$\begin{aligned}
\frac{a_n}{a_{n-1}} &= \frac{(1+\frac{1}{n})^n}{(1+\frac{1}{n-1})^{n-1}} \\
&= \frac{(n+1)^n}{n^n} \cdot \frac{(n-1)^{n-1}}{n^{n-1}} \\
&= \frac{(n+1)^n (n-1)^n}{n^{2n}} \cdot \frac{n}{n-1} \\
&= \left(1 - \frac{1}{n^2}\right)^n \cdot \frac{n}{n-1} \\
&\overset{\text{Bernoulli}}{\geq} \left(1 - \frac{n}{n^2}\right) \cdot \frac{n}{n-1} \\
&= \frac{(n^2-n)\cdot n}{n^2 \cdot (n-1)} \\
&= 1
\end{aligned}$$

Also: $a_n \geq a_{n-1}$.

Beschränktheit:

$$\begin{aligned}
a_n &\overset{\text{Binomi}}{=} \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k} \\
&= \sum_{k=0}^{n} \frac{n(n-1)\cdots(n-k+1)}{n \cdot n \cdots n} \cdot \frac{1}{k!}
\end{aligned}$$

$$\begin{aligned}
&\leq \sum_{k=0}^{n} \frac{1}{k!} \\
&= 1 + \sum_{k=1}^{n} \frac{1}{k!} \\
&\overset{k! \geq 2^{k-1}}{\leq} 1 + \sum_{k=1}^{n} \frac{1}{2^{k-1}} \\
&\overset{l=k-1}{=} 1 + \sum_{l=0}^{n-1} \left(\frac{1}{2}\right)^n \\
&= 1 + \frac{1-(\frac{1}{2})^n}{1-\frac{1}{2}} \\
&\leq 1 + \frac{1}{\frac{1}{2}} \\
&= 3
\end{aligned}$$

Hier sieht man: $\mathrm{e} \leq 3$.

2.4 Die komplexen Zahlen

2.42 Überblick:

$3+x=2$ hat keine Lösung in $\mathbb{N}$.	$\mathbb{N}\cup\{-1\}$	$\xrightarrow{\text{Gruppe}}$	$\mathbb{Z}$.
$3\cdot x=1$ hat keine Lösung in $\mathbb{Z}$.	$\mathbb{Z}\cup\{\frac{1}{3}\}$	$\xrightarrow{\text{Körper}}$	$\mathbb{Q}$
$x^2=2$ hat keine Lösung in $\mathbb{Q}$.	$\mathbb{Q}\cup\{\sqrt{2}\}$	$\xrightarrow{\text{vollst. Körper}}$	$\mathbb{R}$
$x^2=-1$ hat keine Lösung in $\mathbb{R}$.	$\mathbb{R}\cup\{\sqrt{-1}\}$	$\xrightarrow{\text{Körper}}$	$\mathbb{C}$

Aber: In $\mathbb{C}$ gibt es keine Ordnung.

Vieles in der Mathematik versteht man leichter in $\mathbb{C}$, z.B. Nullstellen von Polynomen, Matrizen, Potenzreihen, Lösungen von Differentialgleichungen.

2.4.1 Der Körper der komplexen Zahlen

2.43 Idee: Suche Körper $(\mathbb{C},+,\cdot)$ mit $\mathbb{R}\subseteq\mathbb{C}$ und $\sqrt{-1}\;=:\mathrm{i}\in\mathbb{C}$, also $x+\mathrm{i}\,y\in\mathbb{C}$ für $x,y\in\mathbb{R}$, $\mathrm{i}^2=-1$. Falls $(\mathbb{C},+,\cdot)$ Körper, dann

$$\begin{aligned}(x_1+\mathrm{i}\,y_1)+(x_2+\mathrm{i}\,y_2) &= x_1+\mathrm{i}\,y_1+x_2+\mathrm{i}\,y_2\\ &= x_1+x_2+\mathrm{i}\,y_1+\mathrm{i}\,y_2\\ &= (x_1+x_2)+\mathrm{i}\,(y_1+y_2)\end{aligned}$$

und

$$\begin{aligned}(x_1+\mathrm{i}\,y_1)\cdot(x_2+\mathrm{i}\,y_2) &= x_1\,x_2+\mathrm{i}\,y_1\,x_2+x_1\mathrm{i}\,y_2+\mathrm{i}\,y_1\,\mathrm{i}\,y_2\\ &= x_1\,x_2+(\mathrm{i}\cdot\mathrm{i})\,y_1\,y_2+\mathrm{i}\,y_1\,x_2+\mathrm{i}\,x_1\,y_2\\ &= (x_1\,x_2-y_1\,y_2)+\mathrm{i}\,(y_1\,x_2+x_1\,y_2)\end{aligned}$$

Führt das zu einem Körper?

2.44 Satz: $\mathbb{C}:=\mathbb{R}\times\mathbb{R}$ mit den Verknüpfungen

$$\begin{aligned}(x_1,y_1)+(x_2,y_2) &:= (x_1+x_2,y_1+y_2)\\ (x_1,y_1)\cdot(x_2,y_2) &:= (x_1x_2-y_1y_2,x_1y_2+y_1x_2)\end{aligned}$$

ist ein Körper mit

$$\begin{array}{llcll}\text{Nullelement} & 0 & = & (0,0) & \\ \text{Einselement} & 1 & = & (1,0) & \\ & -(x,y) & = & (-x,-y) & \\ & (x,y)^{-1} & = & \left(\dfrac{x}{x^2+y^2}\,,\,\dfrac{-y}{x^2+y^2}\right) & \text{falls } (x,y)\neq(0,0).\end{array}$$

$(\mathbb{C},+,\cdot)$ heißt Körper der **komplexen Zahlen**. In $\mathbb{C}$ kann man also rechnen wie in jedem Körper.

Beweis: Durch Nachrechnen, z.B.

$$(x,y)\cdot\left(\frac{x}{x^2+y^2}\,,\,\frac{-y}{x^2+y^2}\right) \;=\; \left(\frac{x^2}{x^2+y^2}-\frac{-y^2}{x^2+y^2}\,,\,\frac{x\cdot(-y)}{x^2+y^2}+\frac{y\cdot x}{x^2+y^2}\right) \;=\; (1,0)$$

□

2.45 $\mathbb{R}$ ***als Teilmenge von*** $\mathbb{C}$***:*** Die Abbildung $f:\mathbb{R}\to\mathbb{C}:x\mapsto(x,0)$ ist injektiv, und es gilt

$$\begin{aligned} f(x)+f(y) &= (x,0)+(y,0) &= (x+y,0) &= f(x+y)\\ f(x)\cdot f(y) &= (x,0)\cdot(y,0) &= (x\cdot y,0) &= f(x\cdot y)\end{aligned}$$

Es ist egal, ob ich in $\mathbb{R}$ rechne und dann abbilde, oder erst abbilde und dann in $\mathbb{C}$ rechne.
Also: Identifiziere $x\in\mathbb{R}$ mit $(x,0)\in\mathbb{C}$ bzw. $\mathbb{R}=f(\mathbb{R})$. Dann sind die Verknüpfungen $+,\cdot:\mathbb{C}\times\mathbb{C}\to\mathbb{C}$ Fortsetzungen von $+,\cdot:\mathbb{R}\times\mathbb{R}\to\mathbb{R}$. Weiter gilt für $\alpha\in\mathbb{R},\ (x,y)\in\mathbb{C}$

$$\alpha\cdot(x,y) \;=\; (\alpha,0)\cdot(x,y) \;=\; (\alpha x,\alpha y) \;=\; (x,y)\cdot\alpha.$$

2.46 Vereinfachung: Sei $\mathrm{i}:=(0,1)$. Dann gilt

$$\mathrm{i}^2 \;=\; -1 \;\in\mathbb{R}.$$

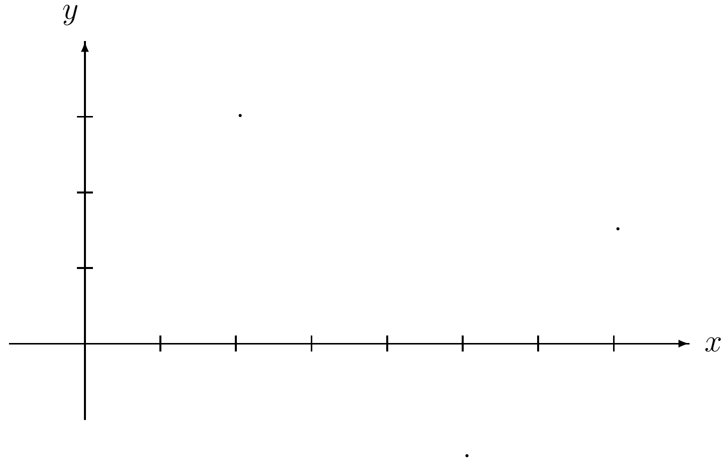
Die komplexe Zahl i heißt **imaginäre Einheit**. Es ist

$$(x,y) \;=\; x(1,0)+y(0,1) \;=\; x+\mathrm{i}\,y \qquad (x,y\in\mathbb{R}).$$

Schreibe statt (x,y) auch $x+\mathrm{i}\,y$ (**Normalform** einer komplexen Zahl), rechne wie in $\mathbb{R}$, beachte $\mathrm{i}^2=-1$.

Z.B.: Berechne $\dfrac{4+3\mathrm{i}}{2-\mathrm{i}}=1+2\mathrm{i}$.

Veranschaulichung in der **Gauß'schen Zahlenebene**.



2.47 Definition: Sei $z = x + \mathrm{i}\, y \in \mathbb{C}$ mit $x, y \in \mathbb{R}$.

1) x heißt **Realteil** von z : $\quad x = \mathrm{Re}\, z$.

2) y heißt **Imaginärteil** von z : $\quad y = \mathrm{Im}\, z$.

3) $\overline{z} := x - \mathrm{i}\, y$ heißt die zu z **konjugierte** Zahl.

2.48 Satz: Für $z, z_1, z_2 \in \mathbb{C}$ gilt:

1) $z \mapsto \overline{z} \;\hat{=}\;$ Spiegelung an reeller Achse in der Gauß'schen Zahlenebene

2) $\overline{\overline{z}} \;=\; z$

3) $z \in \mathbb{R} \quad \Leftrightarrow \quad \overline{z} \;=\; z$

4) $\mathrm{Re}\, z \;=\; \dfrac{z + \overline{z}}{2}, \quad \mathrm{Im}\, z \;=\; \dfrac{z - \overline{z}}{2\mathrm{i}}$

5) $\overline{z_1 + z_2} \;=\; \overline{z}_1 + \overline{z}_2$

6) $\overline{z_1 \cdot z_2} \;=\; \overline{z}_1 \cdot \overline{z}_2, \quad \overline{\left(\dfrac{1}{z}\right)} \;=\; \dfrac{1}{\overline{z}}$

7) $z \;=\; x + \mathrm{i}\, y \;\Rightarrow\; z \cdot \overline{z} \;=\; x^2 + y^2 \;\in \mathbb{R}_0^+$

Z.B.: $z = 3 + 5\mathrm{i} \;\Rightarrow\; z \cdot \overline{z} = 34$.

2.49 Bemerkung: Wegen $\mathrm{i}^2 = -1^2$ kann $\mathbb{C}$ nicht angeordnet werden.

2.50 Definition: Sei $z = x + \mathrm{i}\, y \in \mathbb{C}$. Dann heißt

$$|z| := \sqrt{z \cdot \overline{z}} = \sqrt{x^2 + y^2} \qquad \text{(siehe Satz 2.48)}$$

der **Betrag** von z. (Geometrisch: $|z|$ = Länge von 0 bis z in Gauß'scher Ebene.)

2.51 Hilfssatz: **1)** $|z| = |\overline{z}|$

2) $|\mathrm{Re}\, z| \leq |z|, \quad |\mathrm{Im}\, z| \leq |z|$

3) $z = x \in \mathbb{R} \Rightarrow |z|_{\mathbb{C}} = \sqrt{x^2 + 0} = |x|_{\mathbb{R}}$.
Also: Der Betrag in $\mathbb{C}$ verallgemeinert den Betrag in $\mathbb{R}$.

2.52 Satz: $(\mathbb{C}, |.|)$ ist ein bewerteter Körper, d.h. es gelten:

(B1) $|z| \geq 0; \qquad |z| = 0 \Leftrightarrow z = 0.$

(B2) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|.$

(B3) $|z_1 + z_2| \leq |z_1| + |z_2|$ (Δ-Ungleichung).

Insbesondere: $\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$, $|z_1 \pm z_2| \geq \big||z_1| - |z_2|\big|$ (vgl. Folgerungen 2.17).

Beweis: **(B1)** $|z| \geq 0$ okay

$$|z| = 0 \Leftrightarrow x^2 + y^2 = 0 \Leftrightarrow x = 0 \wedge y = 0 \Leftrightarrow z = 0$$

(B2) $|z_1\, z_2|^2 = (z_1\, z_2) \cdot \overline{(z_1\, z_2)} = z_1\, z_2\, \overline{z_1}\, \overline{z_2} = z_1\, \overline{z_1}\, z_2\, \overline{z_2} = |z_1|^2\, |z_2|^2$

(B3)
$$\begin{aligned} |z_1 + z_2|^2 &= (z_1 + z_2)\, \overline{(z_1 + z_2)} \\ &= (z_1 + z_2)\, (\overline{z_1} + \overline{z_2}) \\ &= z_1\, \overline{z_1} + z_1\, \overline{z_2} + z_2\, \overline{z_1} + z_2\, \overline{z_2} \\ &= |z_1|^2 + |z_2|^2 + \underbrace{2\mathrm{Re}\, z_1\, \overline{z_2}}_{\leq 2|z_1\, \overline{z_2}| = 2|z_1|\, |\overline{z_2}| = 2|z_1|\, |z_2|} \\ &\leq \big(|z_1| + |z_2|\big)^2 \end{aligned}$$
$\square$

2.4.2 Folgen in $\mathbb{C}$

Definition von Konvergenz: Siehe Definition 2.20

2.53 Hilfssatz Vergleich von Beträgen: Sei $z = x + \mathrm{i}\, y$. Dann gilt

$$|z| \leq |x| + |y| \leq \sqrt{2}\, |z|.$$

D.h., wenn $|z|$ klein ist, sind auch $|x|, |y|$ klein und umgekehrt.

Beweis: (i) $|z|^2 = x^2 + y^2 = |x|^2 + |y|^2 \leq |x|^2 + |y|^2 + 2|x|\, |y| = (|x| + |y|)^2$
$\Rightarrow |z| \leq |x| + |y|.$

(ii) Es gilt $0 \leq (|x| - |y|)^2 = |x|^2 - 2|x|\,|y| + |y|^2 \;\Rightarrow\; 2|x|\,|y| \;\leq\; |x|^2 + |y|^2$.

(iii) $(|x| + |y|)^2 \;=\; |x|^2 + 2|x|\,|y| + |y|^2 \overset{\text{(ii)}}{\leq} 2(|x|^2 + |y|^2) \;=\; 2|z|^2 \;\Rightarrow\; |x| + |y| \;\leq\; \sqrt{2}\,|z|.$ $\square$

2.54 Folgerung: Seien $z_n = x_n + \mathrm{i}\,y_n,\; z = x + \mathrm{i}\,y$. Dann gelten

1) $\lim\limits_{n\to\infty} z_n = z \;\Leftrightarrow\; \lim\limits_{n\to\infty} x_n = x \;\wedge\; \lim\limits_{n\to\infty} y_n = y.$

2) (z_n) ist Cauchy-Folge in $\mathbb{C} \;\Leftrightarrow\; (x_n), (y_n)$ sind Cauchy-Folgen in $\mathbb{R}$.

3) $\mathbb{C}$ ist vollständig.

2.55 Beispiele: **1)** $z_n \;=\; \underbrace{\frac{1}{n}}_{\to 0} + \mathrm{i}\,\underbrace{(2 - \frac{1}{n^2})}_{\to 2} \;\to\; 2\mathrm{i}$

2) $z_n \;=\; \dfrac{1}{n} + \mathrm{i}\,n :$ $\quad (\operatorname{Im} z_n)_{n\in\mathbb{N}}$ ist divergent $\;\Rightarrow\; (z_n)$ ist divergent.

3) $z_n = (-1)^n - \dfrac{\mathrm{i}}{n} :$ $\quad (\operatorname{Re} z_n)_{n\in\mathbb{N}}$ ist divergent $\;\Rightarrow\; (z_n)$ ist divergent.

2.56 Rechenregeln für konvergente Folgen: Seien $(a_n), (b_n)$ konvergente Folgen in $\mathbb{C}$. Dann gelten:

1) $\exists M \in \mathbb{R}^+ \;\; \forall n \in \mathbb{N} : |a_n| \leq M$ $\qquad$ (Eine konvergente Folge ist beschränkt).

2) $(a_n + b_n)$ ist konvergent mit $\lim\limits_{n\to\infty}(a_n + b_n) \;=\; \lim\limits_{n\to\infty} a_n + \lim\limits_{n\to\infty} b_n$.
(endliche Summe und Grenzwert sind vertauschbar)

3) Für $\lambda \in \mathbb{C}$ ist $(\lambda\, a_n)$ konvergent mit $\lim\limits_{n\to\infty} \lambda\, a_n \;=\; \lambda \lim\limits_{n\to\infty} a_n$.

4) $(|a_n|)$ ist konvergent mit $\lim\limits_{n\to\infty} |a_n| \;=\; \left|\lim\limits_{n\to\infty} a_n\right|$.

5) $(a_n\, b_n)$ ist konvergent und $\lim\limits_{n\to\infty} a_n\, b_n \;=\; \left(\lim\limits_{n\to\infty} a_n\right) \cdot \lim\limits_{n\to\infty} b_n$.

6) Sei $\lim\limits_{n\to\infty} a_n \neq 0$. Dann existiert ein $N \in \mathbb{N}$ mit $a_n \neq 0$ für $n > N$. Setze

$$c_n \;:=\; \begin{cases} \dfrac{b_n}{a_n} & \text{für } n \geq N + 1 \\ 0 & \text{für } n \leq N. \end{cases}$$

Dann ist (c_n) konvergent mit $\lim\limits_{n\to\infty} c_n \;=\; \dfrac{\lim\limits_{n\to\infty} b_n}{\lim\limits_{n\to\infty} a_n}$.

7) Sind $(a_n), (b_n)$ Folgen in $\mathbb{R}$ und $N \in \mathbb{N}$, so gelten weiter

a) $(\forall n \geq N : a_n \leq b_n) \;\Rightarrow\; \lim\limits_{n\to\infty} a_n \;\leq\; \lim\limits_{n\to\infty} b_n.$

b) $\lim\limits_{n\to\infty} a_n = \lim\limits_{n\to\infty} b_n \wedge (\forall n \geq N : a_n \leq c_n \leq b_n) \;\Rightarrow\; (c_n)$ konvergent $\wedge \lim\limits_{n\to\infty} c_n = \lim\limits_{n\to\infty} a_n$ (Sandwich-Satz, Prinzip der Polizisten).

Beweis: **Zu 1)** Sei $\varepsilon := 1 \;\Rightarrow\; \exists n_1 \in \mathbb{N} \;\; \forall n > n_1 : |a_n - a| < 1$

$\Rightarrow\; \forall n > n_1 : |a_n| = |a_n - a + a| \leq |a_n - a| + |a| < 1 + |a|$

Wähle

$$M \;:=\; \max\big\{|a_1|, |a_2|, \ldots, |a_{n_1}|, 1 + |a|\big\}.$$

Zu 5) Vorüberlegung:

$$\begin{aligned} |a_n\, b_n - a\, b| &= |a_n\, b_n - a_n\, b + a_n\, b - a\, b| \\ &\leq |a_n\, b_n - a_n\, b| + |a_n\, b - a\, b| \\ &= |a_n|\, |b_n - b| + |b|\, |a_n - a| \end{aligned}$$

Also: Sei $M > 0$ mit $\quad \forall n \in \mathbb{N} : |a_n| \leq M, \quad$ sei $\varepsilon > 0$ fest.

Wähle n_1 mit $\forall n > n_1 : |b_n - b| < \dfrac{\varepsilon}{2M}$

Wähle n_2 mit $\forall n > n_2 : |a_n - a| < \dfrac{\varepsilon}{2|b|}$ (falls $b \neq 0$, sonst n_2 beliebig)

Wähle $n_\varepsilon := \max\{n_1, n_2\}$. Für $n > n_\varepsilon$ gilt

$$|a_n\, b_n - a\, b| \;\leq\; M\, \frac{\varepsilon}{2M} + |b|\, \frac{\varepsilon}{2|b|} \;=\; \varepsilon$$

Zu 7) $a_n \leq c_n \leq b_n \;\Rightarrow\; 0 \leq b_n - c_n \leq b_n - a_n$, also $|b_n - c_n| \leq |b_n - a_n|$

$$\begin{aligned} \Rightarrow\; |c_n - a| &= |c_n - b_n + b_n - a| \\ &\leq |c_n - b_n| + |b_n - a| \\ &\leq |b_n - a_n| + |b_n - a| \\ &\leq |b_n - a| + |a - a_n| + |b_n - a| \\ &\to 0 \end{aligned}$$

□

Z.B.: $a_n \;=\; \dfrac{n^2 + \mathrm{i}\, n^3}{1 + \mathrm{i}\, n^2}$

Z.B.: $a_n \;=\; \dfrac{2^n + \mathrm{i}\, 7^n}{\mathrm{i}\, n - 2 \cdot 7^n}$

Z.B.: $\displaystyle \left(1+\frac{1}{n}\right)^n \;\le\; \sum_{k=0}^{n} \frac{1}{k!} \;\le\; 3$ (vgl. Beweis von 2.41)

$$a_n \;:=\; \left(1+\frac{1}{n}\right)^n \;\to\; \mathrm{e}$$

$\displaystyle b_n \;:=\; \sum_{k=0}^{n} \frac{1}{k!}$ ist monoton wachsend und beschränkt, also in $\mathbb{R}$ konvergent

$$\Rightarrow \quad \mathrm{e} \;\le\; \lim_{n\to\infty} b_n \;\le\; 3.$$

Man kann zeigen: $\displaystyle \sum_{k=0}^{\infty} \frac{1}{k!} \;:=\; \lim_{n\to\infty} b_n \;=\; \mathrm{e}.$

2.4.3 Polardarstellung komplexer Zahlen

2.57 Satz: Für jedes $z \in \mathbb{C} \setminus \{0\}$ existieren eindeutige Zahlen $r \in \mathbb{R}^+$, $\varphi \in [0, 2\pi[$, so dass

$$z \;=\; r(\cos\varphi + \mathrm{i}\sin\varphi). \tag{$*$}$$

Man nennt $(*)$ die **Polardarstellung** von z. Es gilt

$$r = |z|,\; \cos\varphi = \frac{\operatorname{Re} z}{|z|},\; \sin\varphi = \frac{\operatorname{Im} z}{|z|}.$$

Der Winkel φ heißt **Argument** von z: $\quad \varphi = \arg(z)$.

2.58 Tabelle wichtiger Werte:

φ	0	$30°\hat{=}\frac{\pi}{6}$	$45°\hat{=}\frac{\pi}{4}$	$60°\hat{=}\frac{\pi}{3}$	$90°\hat{=}\frac{\pi}{2}$
$\sin\varphi$	$\frac{\sqrt{0}}{2}$	$\frac{\sqrt{1}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{4}}{2}$
$\cos\varphi$	$\frac{\sqrt{4}}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{1}}{2}$	$\frac{\sqrt{0}}{2}$

Z.B.: $z_1 = 1 + \mathrm{i}$, $z_2 = \mathrm{i}$, $z_3 = -1$, $z_4 = -1 - \sqrt{3}\mathrm{i}$.

2.59 Multiplikation: $z_1 = r_1(\cos\varphi_1 + \mathrm{i}\,\sin\varphi_1)$, $\; z_2 = r_2(\cos\varphi_2 + \mathrm{i}\,\sin\varphi_2)$

$$\begin{aligned} \Rightarrow\; z_1\, z_2 \;&=\; r_1\, r_2\big(\cos\varphi_1\, \cos\varphi_2 - \sin\varphi_1\, \sin\varphi_2 + \mathrm{i}\,(\cos\varphi_1\, \sin\varphi_2 + \sin\varphi_1\, \cos\varphi_2)\big) \\ &=\; r_1\, r_2(\cos(\varphi_1+\varphi_2) + \mathrm{i}\, \sin(\varphi_1+\varphi_2)) \end{aligned}$$

wegen der Additionstheoreme

$$\begin{aligned}\cos(\varphi_1+\varphi_2) &= \cos\varphi_1\,\cos\varphi_2-\sin\varphi_1\,\sin\varphi_2,\\ \sin(\varphi_1+\varphi_2) &= \cos\varphi_1\,\sin\varphi_2+\sin\varphi_1\,\cos\varphi_2.\end{aligned}$$

Also: Komplexe Zahlen werden multipliziert, in dem man ihre Beträge multipliziert und die Winkel addiert.

2.60 Vereinfachung: Wir schreiben $\mathrm{e}^{\mathrm{i}\varphi} := \cos\varphi+\mathrm{i}\sin\varphi$ (φ im Bogenmaß). Damit wird die Polardarstellung zu

$$z = r\,\mathrm{e}^{\mathrm{i}\varphi}.$$

Additionstheoreme $\Rightarrow$ $\mathrm{e}^{\mathrm{i}\,\varphi_1}\cdot\mathrm{e}^{\mathrm{i}\,\varphi_2}=\mathrm{e}^{\mathrm{i}(\varphi_1+\varphi_2)}$.
Multiplikation komplexer Zahlen: $r_1\,\mathrm{e}^{\mathrm{i}\varphi_1}\cdot r_2\,\mathrm{e}^{\mathrm{i}\varphi_2}=r_1r_2\,\mathrm{e}^{\mathrm{i}(\varphi_1+\varphi_2)}$.
Wichtig: Für $\varphi\in\mathbb{R}$ gilt $\left|\mathrm{e}^{\mathrm{i}\varphi}\right|=\sqrt{\cos^2\varphi+\sin^2\varphi}=1$.

Z.B.: $(1+\mathrm{i})^n$.

Z.B.: Bestimme alle Lösungen von $z^3=-8$.

2.61 Die n-te Wurzel: Es seien $r\in\,]0,\infty[$ und $\varphi\in[0,\infty[$ gegeben. Die Gleichung

$$z^n = r\,\mathrm{e}^{\mathrm{i}\varphi} = r(\cos\varphi+\mathrm{i}\,\sin\varphi)$$

hat genau n verschiedene Lösungen

$$z_k = r^{1/n}\,\mathrm{e}^{\mathrm{i}\,\frac{\varphi+2k\pi}{n}} = r^{1/n}\left(\cos\frac{\varphi+2k\pi}{n}+\mathrm{i}\,\sin\frac{\varphi+2k\pi}{n}\right),\qquad k=0,1,\ldots,n-1.$$

D.h. die Gleichung $z^n=a$ hat für $a\neq 0$ genau n verschiedene Lösungen.
Spezialfall $n=2$: Für $a\in\mathbb{C}\setminus[0,\infty[$ bezeichnen wir mit $\sqrt{a}$ eine (egal welche) Lösung von $z^2=a$.

Z.B.: $\sqrt{8\mathrm{i}}$ bezeichnet $(2+2\mathrm{i})$ oder $-2-2\mathrm{i}$.

2.62 Quadratische Gleichungen: Die Gleichung $az^2 + bz + c \; = \; 0 \quad (a \neq 0)$ hat die Lösungen

$$z_{1/2} \; = \; \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}\,.$$

Beweis:

$$\begin{aligned}
& a\,z^2 + b\,z + c \;=\; 0 \\
\Leftrightarrow\quad & z^2 + \frac{b}{a}\,z + \frac{c}{a} \;=\; 0 \\
\Leftrightarrow\quad & z^2 + 2\frac{b}{2a}\,z + \left(\frac{b}{2a}\right)^2 \;=\; \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\
\Leftrightarrow\quad & \left(z + \frac{b}{2a}\right)^2 \;=\; \frac{1}{4a^2}\,\left(b^2 - 4ac\right) \\
\Leftrightarrow\quad & z + \frac{b}{2a} \;=\; \pm\frac{1}{2a}\,\sqrt{b^2 - 4ac} \\
\Leftrightarrow\quad & z \;=\; -\frac{b}{2a} \pm \frac{1}{2a}\,\sqrt{b^2 - 4ac}
\end{aligned}$$

□

2.4.4 Polynome

2.63 Definition: **1)** Ein **Polynom** ist eine Funktion

$$P : \mathbb{C} \to \mathbb{C} : z \mapsto \sum_{k=0}^{n} a_k\, z^k \;=\; a_0 + a_1\, z + \ldots + a_n\, z^n$$

mit den **Koeffizienten** $a_k \in \mathbb{C}$. Falls $a_0, a_1, \ldots, a_n \in \mathbb{R}$, heißt das Polynom **reell** (dann betrachtet man auch $P : \mathbb{R} \to \mathbb{R}$). Ist $a_n \neq 0$, so heißt n der **Grad** des Polynoms: $n = \operatorname{Grad} P$. Für das Nullpolynom: $\operatorname{Grad} 0 := -1$.

2) Eine **rationale Funktion** ist eine Funktion $z \mapsto \dfrac{P(z)}{Q(z)}$ mit geeignetem Definitionsbereich, wobei P, Q Polynome sind.

3) Die Menge der komplexen/reellen Polynome: $\mathbb{C}[x]$, $\mathbb{R}[x]$.

2.64 Berechnung: $P(z) = (\ldots((a_n\, z + a_{n-1})\, z + a_{n-2})\, z + \ldots + a_1)\, z + a_0$. Hierfür werden nur n Multiplikationen benötigt statt $\frac{n(n+1)}{2}$ (**Hornerschema**).

Z.B.: $P(z) \;=\; 4z^3 - 3z^2 + 2z - 1 \;=\; \big((4z-3)z + 2\big)z - 1$

Berechnung von $P(2)$:

a_k	4	-3	2	-1
$z = 2$		8	10	24
	4	5	12	23 $= P(2)$

Klar ist: Sind $P_1, P_2 \neq 0$ Polynome, dann ist $P_1 \cdot P_2$ Polynom mit

$$\operatorname{Grad}(P_1 \cdot P_2) \;=\; (\operatorname{Grad} P_1) + \operatorname{Grad} P_2.$$

Philosophie: Rechnen mit Polynomen analog Rechnen mit ganzen Zahlen. Rechnen mit rationalen Funktionen analog Rechnen mit rationalen Zahlen.

2.65 Division mit Rest: Seien P, Q Polynome, $1 \le \operatorname{Grad} Q \le \operatorname{Grad} P$. Dann gibt es eindeutig bestimmte Polynome P_1 und R, so dass

$$P \;=\; Q \cdot P_1 + R \;\wedge\; \operatorname{Grad} R < \operatorname{Grad} Q.$$

Z.B.: $(4z^4 - 14z^3 + 6z^2 \;+ 3z - 5) : (\underbrace{2z^3 + 3z + 1}_{Q}) \;=\; \underbrace{2z - 7}_{P_1} + \dfrac{\overbrace{22z + 2}^{R}}{2z^3 + 3z + 1}$

$$\begin{array}{rrrr}
4z^4 & & +6z^2 & +2z \\
\hline
& -14z^3 & & +\,z-5 \\
& -14z^3 & & -21z-7 \\
\hline
& & & 22z+2
\end{array}$$

2.66 Satz: Sei $P \in \mathbb{C}[x]$, Grad $P \ge 1$, $\lambda \in \mathbb{C}$. Dann gilt:

$$P(\lambda) = 0 \;\Leftrightarrow\; (z - \lambda) \text{ ist Teiler von } P, \text{ d.h. } P(z) = (z - \lambda) P_1(z).$$

Beweis: "$\Leftarrow$" klar.

"$\Rightarrow$": Es gilt $P(z) \;=\; (z - \lambda) P_1(z) + R(z)$, $\quad \operatorname{Grad} R < 1$, also $R =$ konstant.

$0 \;=\; P(\lambda) \;=\; 0 \cdot P_1(\lambda) + R(\lambda) \;\Rightarrow\; R \;=\; 0$ $\square$

2.67 Folgerung: Ein Polynom vom Grad $n \ge 1$ hat höchstens n verschiedene Nullstellen.

Beweis: Annahme: $P(\lambda_j) = 0$, $j = 0, \ldots, n+1$, alle $\lambda_1, \ldots, \lambda_{n+1}$ verschieden.

$\Rightarrow\; P(z) \;=\; (z - \lambda_1) \cdots (z - \lambda_{n+1}) \cdot Q(x) \;=$ Polynom vom Grad $> n$ ↯ $\square$

2.68 Identitätssatz: Sind

$$P(z) \;=\; \sum_{k=0}^{n} a_k z^k, \quad Q(z) \;= \sum_{k=0}^{n} b_k z^k$$

Polynome vom Grad $\le n$, die an mindestens $n+1$ verschiedenen Stellen übereinstimmen, so gilt $P = Q$, d. h. $a_k = b_k$ für $k = 0, 1, \ldots, n$.

Beweis: $P - Q$ hat mindestens $n+1$ Nullstellen und $\operatorname{Grad}(P - Q) \le n \;\Rightarrow\; P - Q = 0.$ $\square$

2.69 Definition: $\lambda \in \mathbb{C}$ heißt **k-fache Nullstelle** von P oder Nullstelle mit **Vielfachheit k**, falls $(z - \lambda)^k$, aber nicht $(z - \lambda)^{k+1}$ Teiler von P ist. D. h. $P(z) = (z - \lambda)^k P_1(z)$ mit $P_1(\lambda) \ne 0$.

2.70 Fundamentalsatz der Algebra (C. F. Gauß 1799): Sei $P \in \mathbb{C}[x]$ Polynom vom Grad $n \geq 1$:

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0 \qquad \text{mit } a_n \neq 0.$$

Dann gelten

1) P hat in $\mathbb{C}$ mindestens eine Nullstelle.

2) Es gibt komplexe Zahlen $\lambda_1, \ldots, \lambda_n$ (nicht notwendig verschieden), so dass

$$P(z) \;=\; a_n(z-\lambda_1)\cdots(z-\lambda_n).$$

Die λ_j sind bis auf Nummerierung eindeutig. Zählt man jede Nullstelle mit ihrer Vielfachheit, so hat P genau $\operatorname{Grad} P$ Nullstellen.

2.71 Hornerschema: Seien $P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0$ und $z_0 \in \mathbb{C}$ gegeben.

a_k	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_0
$z = z_0$		$z_0 a_n$	$z_0 b_{n-1}$	$\ldots$	$z_0 b_1$
	a_n	$a_{n-1} + z_0 a_n$ $=: b_{n-1}$	$a_{n-2} + z_0 b_{n-1}$ $=: b_{n-2}$	$\ldots$	$a_0 + z_0 b_1$ $=: b_0 = P(z_0)$

Dann kann in der letzten Zeile das Ergebnis der Polynomdivision $P(z) : (z - z_0)$ abgelesen werden:

$$P(z) : (z - z_0) \;=\; a_n\, z^{n-1} + b_{n-1}\, z^{n-2} + \ldots + b_2\, z + b_1 + \frac{b_0}{z - z_0}$$

Z.B.: $P(z) \;=\; z^4 - 5z^2 - 2z, \qquad z_0 = -2$

a_k	1	0	-5	-2	0
$z = -2$		-2	4	2	0
	1	-2	-1	0	0

$\Rightarrow\; P(z_0) = 0, \qquad P(z) : (z+2) = z^3 - 2z^2 - z.$

2.72 Reelle Polynome: Ist P reelles Polynom und $\lambda \in \mathbb{C}$ Nullstelle, dann ist auch $\overline{\lambda}$ Nullstelle.

Also: Eine Nullstelle ist entweder reell oder ist $\lambda \in \mathbb{C} \setminus \mathbb{R}$ Nullstelle, dann auch $\overline{\lambda}$.

Fall 1: $\lambda \in \mathbb{R}$: $\qquad P(z) = (z - \lambda)P_1(z) \quad (P_1 \text{ reelles Polynom})$

Fall 2: $\lambda \in \mathbb{C} \setminus \mathbb{R}$:
$$\begin{aligned} P(z) &= (z-\lambda)(z-\overline{\lambda})P_1(z) \\ &= (z^2 - (2\mathrm{Re}\,\lambda)z + |\lambda|^2)P_1(z) \qquad (P_1 \text{ reelles Polynom}) \end{aligned}$$

Aus dem Fundamentalsatz folgt nun: Ein reelles Polynom ist darstellbar als Produkt von linearen und quadratischen reellen Polynomen, wobei die quadratischen Polynome keine reellen Nullstellen besitzen (d.h. sie sind in $\mathbb{R}$ irreduzibel).

Z.B.: $P(z) = z^4 + 4z^3 + 2z^2 + 4z + 1$ hat Nullstelle $z = \mathrm{i}$

$\Rightarrow$ weitere Nullstelle $z = -\mathrm{i}$

$(z - \mathrm{i})(z + \mathrm{i}) = z^2 + 1$

$(z^4 + 4z^3 + 2z^2 + 4z + 1) : (z^2 + 1) = z^2 + 4z + 1$

$z^2 + 4z + 1 = 0 \;\Leftrightarrow\; z_{1/2} = \dfrac{-4 \pm \sqrt{16 - 4}}{2} = -2 \pm \sqrt{3}$

$\Rightarrow\; P(z) = (z^2 + 1) \cdot (z - (-2 + \sqrt{3}))(z - (-2 - \sqrt{3}))$

2.73 Rationale Nullstellen: Sei $P(x) = \sum\limits_{k=0}^{n} a_k\, x^k$ mit $a_0, \ldots, a_n \in \mathbb{Z}$. Ist $x = \dfrac{p}{q}$ Nullstelle von P, wobei $p, q \in \mathbb{Z}$ teilerfremd sind, dann ist p Teiler von a_0 und q Teiler von a_n.

Beweis: $0 \;=\; a_n \left(\dfrac{a}{b}\right)^n + a_{n-1} \left(\dfrac{a}{b}\right)^{n-1} + \ldots + a_0$

$\Leftrightarrow\;\; 0 \;=\; a_n\, a^n + a_{n-1}\, a^{n-1}\, b + \ldots + a_0\, b^n$

$\Leftrightarrow\;\; a_n\, a^n \;=\; -b(\ldots)$

$\Rightarrow\;\; b \mid a_n\, a^n \overset{a,b \text{ teilerfremd}}{\Rightarrow} b \mid a_n$

Genauso: $b^n\, a_0 = -a(\ldots) \;\Rightarrow\; a \mid b^n\, a_0 \;\Rightarrow\; a \mid a_0$ $\square$

Z.B.: $P(x) \;=\; 1 \cdot x^3 - 2x^2 - 6x + 4.$

Wegen $a_n = a_3 = 1$ sind alle rationalen Nullstellen ganze Zahlen.

Wegen $a_0 = 4$ kommen nur $x = \pm 1, \pm 2, \pm 4$ in Frage.

Probieren: $P(-2) = 0$.

Z.B.: $P(x) \;=\; 12x^4 - 4x^3 + 6x^2 + x - 1.$

Teiler von $a_n = a_4 = 12 :\quad 1, 2, 3, 4, 6, 12.$

Teiler von $a_0 = -1 :\quad 1$

$\Rightarrow$ Mögliche rationale Nullstellen $x = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{4}, \pm\frac{1}{6}, \pm\frac{1}{12}$.

Probieren: $P(\frac{1}{3}) = 0$.

3 Lineare Algebra

3.1 Linearität

3.1 Definition: Ein **Vektorraum** oder **linearer Raum** über einem Körper $\mathbb{K}$ (z.B. $\mathbb{K} = \mathbb{R}$, $\mathbb{K} = \mathbb{C}$, $\mathbb{K} = \mathbb{F}_p$) ist eine abelsche (d.h. kommutative) Gruppe $(V, +)$, versehen mit einer **Skalarenmultiplikation** $\cdot : \mathbb{K} \times V \to V : (\lambda, v) \mapsto \lambda \cdot v$, so dass

(S1) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$

(S2) $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$

(S3) $\lambda \cdot (\mu \cdot v) = (\lambda \mu) \cdot v$

(S4) $1 \cdot v = v$

Die Elemente des Vektorraumes heißen **Vektoren**. Das neutrale Element der Gruppe $(V, +)$ heißt auch **Nullvektor** 0.

Beispiele: **1)** $V_1 = \mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} : x_1, \dots, x_n \in \mathbb{R} \right\}$ ist ein Vektorraum über $\mathbb{R}$ mit

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}, \qquad \lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

2) $V_1 = \mathbb{C}^n = \left\{ \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} : z_1, \dots, z_n \in \mathbb{C} \right\}$ ist ein Vektorraum über $\mathbb{C}$ oder über $\mathbb{R}$ mit Definition von $+, \cdot$ wie in 1).

3) Vektorraum der Folgen:

$$V_3 := \{(a_n)_{n \in \mathbb{N}} \mid \forall n \in \mathbb{N} : a_n \in \mathbb{C}\}$$

ist Vektorraum über $\mathbb{C}$ (oder über $\mathbb{R}$) mit

$$(a_n) + (b_n) := (a_n + b_n), \quad \lambda \cdot (a_n) := (\lambda a_n).$$

4) Vektorraum der konvergenten Folgen:

$$V_4 := \mathcal{C} := \{(a_n)_{n \in \mathbb{N}} \mid \forall n \in \mathbb{N} : a_n \in \mathbb{C} \ \wedge \ \exists a \in \mathbb{C} : a_n \to a\}$$

ist Vektorraum über $\mathbb{C}$ (oder über $\mathbb{R}$) mit Definition von $+, \cdot$ wie in 3).

5) $V_5 := \mathcal{F} := \{f : \mathbb{C} \to \mathbb{C}\}$: Vektorraum der komplexen Funktionen mit

$$f + g : x \mapsto f(x) + g(x), \quad \lambda \cdot f : z \mapsto \lambda f(z)$$

6) $V_6 := \mathcal{P} := \{P : \mathbb{C} \to \mathbb{C} \mid P \text{ ist Polynom}\}$ mit $+, \cdot$ wie in 5) ist Vektorraum der Polynome, Untervektorraum von $\mathcal{F}$.

7) $V_7 := \mathcal{P}_n := \{P : \mathbb{C} \to \mathbb{C} \mid P \text{ ist Polynom vom Grad } \leq n\}$ mit $+, \cdot$ wie in 5) ist Untervektorraum von $\mathcal{F}$ und von $\mathcal{P}$.

8) $V_8 := \{f : \mathbb{C} \to \mathbb{C} : z \mapsto \lambda\, z^n \mid \lambda \in \mathbb{C}\}$ ist Untervektorraum von $\mathcal{F}$, $\mathcal{P}$ und von $\mathcal{P}_n$. „Gerade im Raum der Polynome“

9) $(\mathbb{K}, +, \cdot)$ ist ein Vektorraum über $\mathbb{K}$.

3.2 Rechenregeln: Sei $(V, +, \cdot)$ ein Vektorraum. Dann gelten:

1) $\lambda \cdot v = 0 \;\Leftrightarrow\; \lambda = 0 \;\vee\; v = 0$.

2) $(-1) \cdot v \;=\; -v$ (inverses Element zu v).

3) Seien $u, v \in V$ gegeben. Die Gleichung $u + x = v$ besitzt die eindeutige Lösung $x = v + (-u) =: v - u$.

3.3 Definition: Sei $(V, +, \cdot)$ ein Vektorraum über $\mathbb{K}$. Eine Teilmenge $U \subseteq V$ heißt **Untervektorraum** oder **linearer Teilraum** von V, falls $(U, +, \cdot)$ ein Vektorraum über $\mathbb{K}$ ist (hier bezeichnen $+, \cdot$ die Einschränkungen der V-Operationen auf $U \times U$ bzw. $\mathbb{K} \times U$).

3.4 Untervektorraumkriterium: Es seien $(V, +, \cdot)$ ein Vektorraum über $\mathbb{K}$ und $U \subseteq V$. Dann sind äquivalent:

(i) U ist Untervektorraum von V.

(ii) $U \neq \emptyset \;\wedge\; (\forall v, w \in U \;\; \forall \lambda, \mu \in \mathbb{K} : \lambda \cdot v + \mu \cdot w \in U)$.

(iii) $U \neq \emptyset \;\wedge\; (\forall v, w \in U : v + w \in U) \;\wedge\; (\forall v \in U \;\; \forall \lambda \in \mathbb{K} : \lambda \cdot v \in U)$.

Beispiele: **1)** $V = \mathbb{R}^3$:

$$U_1 := \left\{ \begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix} : x_1, x_2 \in \mathbb{R} \right\}$$

$$U_2 := \left\{ \begin{pmatrix} x_1 \\ x_2 \\ 1 \end{pmatrix} : x_1, x_2 \in \mathbb{R} \right\}$$

$$U_3 := \left\{ \begin{pmatrix} x_1 \\ 0 \\ 0 \end{pmatrix} : x_1 \in \mathbb{R} \right\} = \left\{ \lambda \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} : \lambda \in \mathbb{R} \right\}$$

$$U_4 := \left\{ \begin{pmatrix} x_1 \\ 0 \\ 2x_1 \end{pmatrix} : x_1 \in \mathbb{R} \right\} = \left\{ \lambda \cdot \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} : \lambda \in \mathbb{R} \right\}$$

2) $V = \{(a_n)_{n\in\mathbb{N}} \mid \forall n \in \mathbb{N} : a_n \in \mathbb{C}\}$.

$U_1 \ := \ \{(a_n)_{n\in\mathbb{N}} \mid a_n \to 0\}$.

$U_2 \ := \ \{(a_n)_{n\in\mathbb{N}} \mid a_n \to 1\}$.

3) $\mathcal{P}_n$ ist Untervektorraum von $\mathcal{P}$.
Sei $P_j : \mathbb{C} \to \mathbb{C} : z \mapsto z^j \ (j = 0, \ldots, n)$

$$\Rightarrow \ \mathcal{P}_n \ = \ \left\{ \sum_{j=0}^{n} \lambda_j \cdot P_j : \lambda_j \in \mathbb{C} \right\}.$$

3.5 Definition: **1)** Seien $n \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$, $v_1, \ldots, v_n \in V$. Dann heißt

$$v \ := \ \sum_{j=1}^{n} \lambda_j \cdot v_j$$

Linearkombination der Vektoren $v_1, \ldots, v_n$.
Achtung: Eine Linearkombination ist immer eine endliche Summe.

2) Sei $M \subseteq V$. Dann heißt

$$\begin{aligned} \mathrm{LH}(M) \ &:= \ \{\text{Linearkombinationen von Elementen aus } M\} \\ &= \ \left\{ \sum_{j=1}^{n} \lambda_j \cdot v_j : n \in \mathbb{N}, \ \lambda_j \in \mathbb{K}, \ v_j \in M \right\} \end{aligned}$$

die **lineare Hülle** von M. Offensichtlich gelten:

- $\mathrm{LH}(M)$ ist ein Untervektorraum von V.
- $\mathrm{LH}(M)$ ist der kleinste Unterraum von V, der M enthält:

$$M \subseteq W \ \wedge \ W \text{ Unterraum von } V \ \Rightarrow \ \mathrm{LH}(M) \subseteq W.$$

Man sagt: M **spannt** den Untervektorraum $\mathrm{LH}(M)$ auf.

Beispiele: **1)** $V = \mathbb{R}^n$

$$M_1 := \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}$$

$$M_2 := \left\{ \lambda \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} : \lambda \in \mathbb{R} \right\}$$

$$M_3 := \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} \right\}$$

2) $V = \{(a_n) \text{ Folge in } \mathbb{C}\}$, $M := \{e_j \in V \mid j \in \mathbb{N} \ \wedge \ e_j = (0, 0, \ldots, 0, 1, 0, 0, \ldots)\}$
$\uparrow$ j-tes Folgenglied

3) $V = \mathcal{P},\ M := \{P_j : z \mapsto z^j \mid j = 0, 1, 2, \ldots\}$.

3.6 Minimale aufspannende Mengen: Sei $M \subseteq V$ mit $\mathrm{LH}(M) = V$. Dann sind äquivalent:

(i) $\forall m \in M : \mathrm{LH}\big(M \setminus \{m\}\big) \neq V$.

(ii) Für jede endliche Teilmenge $\{m_1, \ldots, m_n\} \subseteq M$ gilt

$$\forall \lambda_1, \ldots \lambda_n \in \mathbb{K} : \left(\sum_{j=1}^{n} \lambda_j \cdot m_j = 0 \ \Rightarrow \ \lambda_1 = \ldots = \lambda_n = 0 \right).$$

(iii) Ist $v = \sum\limits_{j=1}^{n} \lambda_j \cdot m_j$ mit $m_1, \ldots, m_n \in M$, so sind die Koeffizienten (Koordinaten) $\lambda_1, \ldots, \lambda_n$ eindeutig.

3.7 Definition: Seien V, W Vektorräume über $\mathbb{K}$. Eine Abbildung $L : V \to W$ heißt **linear** oder **Vektorraum-Homomorphismus**, falls

(i) $\big(\forall u, v \in V : L(u + v) = L(u) + L(v)\big) \ \wedge \ \big(\forall u \in V \ \ \forall \lambda \in \mathbb{K} : L(\lambda \cdot v) = \lambda \cdot L(v)\big)$

oder äquivalent

(ii) $\forall u, v \in V \ \ \forall \lambda, \mu \in \mathbb{K} : L(\lambda \cdot u + \mu \cdot v) = \lambda \cdot L(u) + \mu \cdot L(v)$.

Beispiele: **1)** $L : \mathbb{R}^3 \to \mathbb{R} : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto x_1$.

2) $L : \mathbb{R}^2 \to \mathbb{R}^2 : \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} a_1\, x_1 + a_2 x_2 \\ b_1\, x_1 + b_2\, x_2 \end{pmatrix}$.

3) $L : \mathcal{F} \to \mathbb{C} : f \mapsto f(1)$.

4) $L : \mathcal{P} \to \mathcal{P} : P \mapsto P'$.

5) $V = \mathcal{C} = \{(a_n) \text{ Folge in } \mathbb{C} \mid (a_n) \text{ konvergent}\}$, $L : \mathcal{C} \to \mathbb{C} : (a_n) \mapsto \lim\limits_{n \to \infty} a_n$.

3.8 Satz: Seien U, V, W Vektorräume über $\mathbb{K}$. Sind $K : U \to V$ und $L : V \to W$ linear, dann ist auch $L \circ K : U \to W$ linear.

3.9 Definition: Sei $L : V \to W$ linear. Dann heißt

$$\mathrm{Bild}\,(L) \;:=\; \{L(x) : x \in V\}$$

das **Bild** von L und das Urbild der Menge $\{0\} \subseteq W$

$$\mathrm{Kern}\,(L) \;:=\; \{x \in V : L(x) = 0\} \;=\; L^{-1}(\{0\})$$

der **Kern** von L.

Beispiele: 1) $L : \mathbb{R}^2 \mapsto \mathbb{R}^2 : \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ 0 \end{pmatrix}$.

2) $L : \mathcal{F} \to \mathbb{C} : f \mapsto f(1)$.

3) $L : \mathcal{P}_n \to \mathcal{P}_n : P \mapsto P'$.

4) $L : \mathcal{C} \to \mathbb{C} : (a_n) \mapsto \lim\limits_{n\to\infty} a_n$.

3.10 Eigenschaften linearer Abbildungen: Sei $L : V \to W$. Dann gelten:

1) $L(0) = 0$.

2) Bild (L) ist ein Untervektorraum von W.

3) Kern (L) ist ein Untervektorraum von V.

4) Ist zusätzlich L bijektiv, so ist $L^{-1} : W \to V$ linear.

3.11 Definition: Sei $L : V \to W$ linear und bijektiv. Dann heißt L **Isomorphismus**, die Vektorräume V und W heißen **isomorph**. Man kann dann V und W identifizieren, sie sind nur verschiedene Realisierungen desselben Vektorraumes.

Beispiele: 1) $L : \mathbb{C}^{n+1} \to \mathcal{P}_n : \begin{pmatrix} a_1 \\ \vdots \\ a_{n+1} \end{pmatrix} \mapsto \big(P : z \mapsto a_1 + a_2\, z + \ldots + a_{n+1}\, z^n\big)$.

2) $L : \mathcal{P} \to \{\text{abbrechende Folgen}\}$:

$$\big(P : z \mapsto a_0 + a_1\, z + \ldots + a_n\, z^n\big) \mapsto (a_0, a_1, \ldots, a_n, 0, 0, \ldots).$$

Anwendung: In einem endlichen Körper $\mathbb{K}$ mit n Elementen gibt es nur n^n verschiedene Abbildungen $f : \mathbb{K} \to \mathbb{K}$. Der Raum der Polynome soll aber unendlich viele Elemente enthalten. Deshalb definiert man den Vektorraum der Polynome $\mathcal{P}$ nicht als Raum von Abbildungen sondern durch

$$\mathcal{P} \;:=\; \{\text{abbrechende Folgen in } \mathbb{K}\}.$$

Im Fall von $\mathbb{K} = \mathbb{R}$ ist diese Definition äquivalent zu unserer ursprünglichen Definition.

3.12 Kern und Injektivität: Für $L : V \to W$ linear sind äquivalent:

(i) $\mathrm{Kern}\,(L) = \{0\}$.

(ii) L ist injektiv.

Beweis: **(i) $\Rightarrow$ (ii):**
$$\begin{aligned} Lu = Lv \quad &\Leftrightarrow \quad Lu - Lv = 0 \\ &\Leftrightarrow \quad L(u-v) = 0 \\ &\Leftrightarrow \quad u - v \in \mathrm{Kern}\,(L) \\ &\Leftrightarrow \quad u - v = 0 \end{aligned}$$

(ii) $\Rightarrow$ (i): $L(0) = 0 \ \wedge \ L$ injektiv $\ \Rightarrow\ L^{-1}(\{0\}) = \{0\}$. $\square$

3.2 Lineare Gleichungssysteme - Vorläufiges

3.13 Definition: Seien $m, n \in \mathbb{N}$ und $a_{jk}, b_j \in \mathbb{K}$ für $j = 1, \ldots, m,\ k = 1, \ldots, n$ gegeben. Das System

$$\left.\begin{array}{lllllll} a_{11}x_1 & + & a_{12}x_2 & + \ \ldots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & \ldots & & + & a_{2n}x_n & = & b_2 \\ \vdots & & & & & & & \\ a_{m1}x_1 & + & \ldots & & + & a_{mn}x_n & = & b_m \end{array}\right\} \qquad (*)$$

für die n Unbekannten $x_1, \ldots, x_n \in \mathbb{K}$ heißt **lineares Gleichungssystem** (**LGS**). Falls die rechte Seite verschwindet (d.h. $b_1 = \ldots = b_m = 0$) heißt das LGS **homogen**, sonst **inhomogen**. Ist $(*)$ inhomogen, so heißt das LGS mit denselben Koeffizienten a_{jk}, aber $b_1 = \ldots = b_m = 0$, das **zugehörige homogene** LGS.

Kürzere Schreibweise für $(*)$:

$$\sum_{k=1}^{n} a_{jk}\, x_k \ = \ b_j, \quad j = 1, \ldots, m$$

Praktische Schreibweise für kleinere LGS:

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ \vdots & & & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & b_m \end{array}\right)$$

3.14 Bemerkung: Die Abbildung

$$L : \mathbb{K}^n \to \mathbb{K}^n : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \sum_{k=1}^n a_{1k}\, x_k \\ \vdots \\ \sum_{k=1}^n a_{mk}\, x_k \end{pmatrix}$$

ist linear.

Also: $(*)$ lösen bedeutet: $L^{-1}\left(\left\{\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}\right\}\right)$ bestimmen.

3.15 Das Gauß-Verfahren: **1)** Vertausche die Zeilen, so dass keine Zeile weiter links beginnt als die erste Zeile:

$$\forall j \geq 2 : \min\{k : a_{jk} \neq 0\} \geq \min\{k : a_{1k} \neq 0\}.$$

2) Durch Addition von Vielfachen der 1. Zeile zu den anderen Zeilen erreiche „führende Nullen“ ab der 2. Zeile:

$$\forall j \geq 2 : \min\{k : a_{jk} \neq 0\} \geq \min\{k : a_{1k} \neq 0\} + 1.$$

3) Vergiss die erste Zeile, betrachte die zweite Zeile als erste und wiederhole den Vorgang.

Abbruchbedingung: Führe das Gauß-Verfahren so lange durch, bis das LGS **Zeilenstufenform** hat, d.h. dass jede Zeile entweder vom linken Rand her mehr Nullkoeffizienten als die vorhergehende Zeile hat oder links vom Gleichheitszeichen aus lauter Nullen besteht:

$$\begin{array}{ccccccccccccc}
a_{11}\,x_1 & + & a_{12}\,x_2 & + & \dots & & & & & + & a_{1n}\,x_n & = & b_1 \\
0\,x_1 & + & a_{22}\,x_2 & + & \dots & & & & & + & a_{2n}\,x_n & = & b_2 \\
0\,x_1 & + & 0\,x_2 & + & a_{33}\,x_3 & + & \dots & & & + & a_{3n}\,x_n & = & b_3 \\
 & & & & & \ddots & & & & & & & \\
0\,x_1 & + & \dots & & & & a_{lk}\,x_k & + & \dots & + & a_{ln}\,x_n & = & b_l \qquad (k \geq l) \\
 & & & & & & & & & & 0 & = & b_{l+1} \\
 & & & & & & & & & & & \vdots & \\
 & & & & & & & & & & 0 & = & b_m
\end{array}$$

Klar ist: Falls $b_{l+1} \neq 0$ oder $b_{l+2} \neq 0$ $\dots$ oder $b_m \neq 0$, dann gibt es keine Lösung. Pech! Andernfalls kann man das LGS „von unten nach oben“ auflösen.

3.16 Begründung: Ist $(x_1, \dots, x_n)$ Lösung von $(*)$, dann auch von dem umgeformten System nach einem Gauß-Schritt (Wir haben ja nur Gleichungen addiert).
Ist $(x_1, \dots, x_n)$ Lösung des umgeformten Systems, dann können wir die ursprünglichen Gleichungen durch Gauß-Umformungen rekonstruieren.
Also: Ein Gauß-Schritt ändert die Lösungsgesamtheit nicht.

3.17 Folgerung: Ein homogenes LGS besitzt immer die Lösung $x_1 = \dots = x_n = 0$. Im Fall $m \leq n-1$ (weniger Zeilen als Variablen) besitzt ein homogenes LGS immer nichttriviale Lösungen.

3.3 Basis und Dimension

3.18 Definition: Sei $(V, +, \cdot)$ ein Vektorraum über $\mathbb{K}$.

1) Eine Teilmenge $M \subseteq V$ heißt **linear unabhängig**, falls folgende äquivalente Bedingungen erfüllt sind:

(i) Für jede endliche Teilmenge $\{m_1, \ldots, m_n\} \subseteq M$ gilt

$$\forall \lambda_1, \ldots \lambda_n \in \mathbb{K} : \left(\sum_{j=1}^{n} \lambda_j \cdot m_j = 0 \;\Rightarrow\; \lambda_1 = \ldots = \lambda_n = 0 \right).$$

(ii) Ist $v = \sum\limits_{j=1}^{n} \lambda_j \cdot m_j$ mit $m_1, \ldots, m_n \in M$, so sind die Koeffizienten $\lambda_1, \ldots, \lambda_n$ eindeutig.

(iii) $\forall m \in M : \mathrm{LH}\big(M \setminus \{m\}\big) \neq \mathrm{LH}(M)$.

Falls M nicht linear unabhängig ist, heißt M **linear abhängig**.

2) Eine Teilmenge $B \subseteq V$ heißt **Basis**, falls B linear unabhängig ist und $\mathrm{LH}(B) = V$. Insbesondere besitzt dann jeder Vektor $v \in V$ eine eindeutige Darstellung

$$v \;=\; \sum_{j=1}^{n} \lambda_j \cdot b_j \qquad \text{mit } n \in \mathbb{N},\ \lambda_j \in \mathbb{K},\ b_j \in B.$$

Die Koeffizienten $\lambda_1, \ldots, \lambda_n$ heißen **Koordinaten** von v bezüglich B. Wir schreiben

$$v \;=\; \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}_B$$

Beispiele: **1)** $V = \mathbb{K}^n$, $e_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \ldots e_n := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$.

$B := \{e_1, \ldots, e_n\}$ ist die kanonische Basis von $\mathbb{K}^n$.

2) $V = \mathbb{K}^n$, $a_1, \ldots a_n \in \mathbb{K}^n \setminus \{0\}$, so dass a_j für $j > k$ mehr Nullen „von oben her“ hat als a_k. Dann ist $\{a_1, \ldots, a_n\}$ Basis von $\mathbb{K}^n$.

3) $V = \{(a_n) \text{ Folge in } \mathbb{C}\}$, $e_j = (0, 0, \ldots, 0, 1, 0, 0, \ldots)$
$\uparrow$ j-tes Folgenglied

$M = \{e_1, e_2, \ldots\}$ ist linear unabhängig, aber keine Basis.

4) Seien $P_j : \mathbb{C} \to \mathbb{C} : z \mapsto z^j$, $j \in \mathbb{N}_0$.
$\{P_0, \ldots, P_n\}$ ist Basis von $\mathcal{P}_n$,
$\{P_0, P_1, \ldots\}$ ist Basis von $\mathcal{P}$.

5) $V = \mathcal{F} = \{f : \mathbb{R} \to \mathbb{R} \text{ Abbildung}\}$.
$M := \{x \mapsto \mathrm{e}^{ax} \mid a \in \mathbb{R}\}$ ist linear unabhängig, aber keine Basis.

3.19 Die Idee von Descartes: Sei $\{v_1, \ldots, v_n\} \subseteq V$. Definiere

$$T : \mathbb{K}^n \to V : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{j=1}^{n} x_j \cdot v_j$$

Falls T umkehrbar: Jeder Vektor $v \in V$ besitzt Koordinaten $x_1, \ldots, x_n$. Mit Koordinaten kann man rechnen.

3.20 Satz: **1)** T ist linear

2) Äquivalent sind: **(i)** LH $\{v_1, \ldots, v_n\} = V$.
(ii) T ist surjektiv.

3) Äquivalent sind: **(i)** $\{v_1, \ldots, v_n\}$ ist linear unabhängig.
(ii) T ist injektiv.

4) Äquivalent sind: **(i)** $\{v_1, \ldots, v_n\}$ ist Basis von V.
(ii) T ist bijektiv.

3.21 Folgerung: Sei V Vektorraum über $\mathbb{K}$ mit einer endlichen Basis B und $n := \sharp B$. Dann ist V isomorph zu $\mathbb{K}^n$.

3.22 Satz: Der Vektorraum V besitze eine Basis mit n Elementen. Dann gelten:

1) Jede Menge mit mehr als n Elementen ist linear abhängig.

2) Jede Basis hat genau n Elemente.

Beweis: **1)** Sei $B = \{b_1, \ldots, b_n\}$ die Basis. Dann ist $T : \mathbb{K}^n \to V$ Isomorphismus. Seien nun $w_1, \ldots, w_{n+1} \in V$. Zu zeigen:

$$\begin{aligned} & \lambda_1 \cdot w_1 + \ldots + \lambda_{n+1} \cdot w_{n+1} = 0 \text{ hat nichttriviale Lösungen} \\ \Leftrightarrow\ & T^{-1}(\lambda_1 \cdot w_1 + \ldots + \lambda_{n+1} \cdot w_{n+1}) = 0 \text{ hat nichttriviale Lösungen} \\ \Leftrightarrow\ & \lambda_1 \cdot T^{-1}(w_1) + \ldots + \lambda_{n+1} \cdot T^{-1}(w_{n+1}) = 0 \text{ hat nichttriviale Lösungen} \\ \Leftrightarrow\ & \text{wahr,} \end{aligned}$$

da hier ein homogenes LGS mit $n + 1$ Unbekannten und n Zeilen vorliegt.

2) Seien B, B' Basen von V.

$$\left.\begin{array}{l} 1) \;\Rightarrow\; \sharp B' \leq \sharp B \quad \text{(da } B' \text{ linear unabhängig)} \\ 1) \;\Rightarrow\; \sharp B \leq \sharp B' \quad \text{(da } B \text{ linear unabhängig)} \end{array}\right\} \quad \Rightarrow \quad \sharp B' = \sharp B.$$

□

3.23 Definition: Besitzt V eine endliche Basis B, so heißt $\sharp B$ die **Dimension** von V :

$$\dim V := \sharp B.$$

Besitzt V keine endliche Basis, so heißt V **unendlichdimensional**.

Beispiele: **1)** $\dim(\mathbb{K}^n) = n$,

2) $\mathbb{C}^n$ als Vektorraum über $\mathbb{R}$: $\dim(\mathbb{C}^n) = 2n$,

3) $V = \mathrm{LH}\left\{ \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\} \Rightarrow \dim(V) = 2$,

4) $\dim(\mathcal{P}_n) = n + 1$,

5) $\mathcal{P}$ ist unendlichdimensional.

3.24 Folgerung: Falls $\dim V = n$ und $\{v_1, \ldots, v_n\} \subseteq V$ linear unabhängig, ist $\{v_1, \ldots, v_n\}$ eine Basis.

3.25 Basisergänzungssatz: Sei V endlichdimensional, $m \in \mathbb{N}$, $m < n := \dim V$ und $\{v_1, \ldots, v_m\} \subseteq V$ linear unabhängig. Dann existieren Vektoren $v_{m+1}, \ldots, v_n \in V$, so dass $\{v_1, \ldots, v_n\}$ eine Basis von V ist.

Beweis: Sei $\{b_1, \ldots, b_n\}$ Basis von V.

$$v_1 = \sum_{j=1}^{n} \lambda_j \cdot b_j \;\wedge\; v_1 \neq 0 \;\Rightarrow\; \exists \lambda_{j_1} \neq 0.$$

Dann kann b_{j_1} durch v_1 ersetzt werden, d.h.

$$\big(\{b_1, \ldots, b_n\} \setminus \{b_{j_1}\}\big) \cup \{v_1\} \text{ ist Basis von } V.$$

Genauso folgt, dass es ein b_{j_2} gibt, das durch v_2 ersetzt werden kann, und die enstehende Menge ist immer noch Basis von V.

So fortfahrend erhalten wir

$$\big(\{b_1, \ldots, b_n\}\big) \setminus \{b_{j_1}, \ldots, b_{j_m}\} \cup \{v_1, \ldots, v_m\}$$

als gewünschte Basis von V.

□

3.26 Bemerkung: Man kann beweisen: Jeder Vektorraum besitzt eine Basis.

3.27 Dimensionsformel: Sei $L : V \to W$ linear, $\dim V < \infty$. Dann gilt

$$\dim V \;=\; \dim \operatorname{Kern}(L) + \dim \operatorname{Bild}(L)$$

(wobei $\dim\big(\{0\}\big) := 0$).

Beweis: Sei $k := \dim \operatorname{Kern}(L),\; n := \dim(V)$.

Fall $k = n$**:** $\Rightarrow\; V = \operatorname{Kern}(L) \;\wedge\; \operatorname{Bild}(L) = \{0\} \;\Rightarrow\; n = 0 + n$ stimmt.

Fall $1 \le k \le n-1$**:** Sei $\{b_1, \ldots b_k\}$ Basis von $\operatorname{Kern}(L)$.
Ergänze zu einer Basis $\{b_1, \ldots, b_n\}$ von V

$$\Rightarrow\; \operatorname{Bild}(L) = L(V) = L\big(\mathrm{LH}\{b_1, \ldots, b_n\}\big) = \mathrm{LH}\{Lb_1, \ldots, Lb_n\} = \mathrm{LH}\{Lb_{k+1}, \ldots, Lb_n\}.$$

Behauptung: $\{Lb_{k+1}, \ldots, Lb_n\}$ ist linear unabhängig.
Dann: $n = k + (n-k)$ stimmt.

$$\begin{aligned} 0 \;&=\; \lambda_{k+1} \cdot Lb_{k+1} + \ldots + \lambda_n \cdot Lb_n \;=\; L(\lambda_{k+1} \cdot b_{k+1} + \ldots + \lambda_n \cdot b_n) \\ &\Rightarrow\; \lambda_{k+1} \cdot b_{k+1} + \ldots + \lambda_n \cdot b_n \in \operatorname{Kern}(L) \\ &\Rightarrow\; \lambda_{k+1} \cdot b_{k+1} + \ldots + \lambda_n \cdot b_n = \lambda_1 \cdot b_1 + \ldots + \lambda_k \cdot b_k \\ &\Rightarrow\; \lambda_{k+1} = \ldots = \lambda_n = 0. \end{aligned}$$

Fall $k = 0$**:** Sei $\{b_1, \ldots, b_n\}$ Basis von V. Behauptung: $\{Lb_1, \ldots, Lb_n\}$ ist linear unabhängig.
Dann: $n = 0 + n$ stimmt.

$$\begin{aligned} 0 \;&=\; \lambda_1 \cdot Lb_1 + \ldots + \lambda_n \cdot Lb_n \;=\; L(\lambda_1 \cdot b_1 + \ldots + \lambda_n \cdot b_n) \\ &\Rightarrow\; \lambda_1 \cdot b_1 + \ldots + \lambda_n \cdot b_n \in \operatorname{Kern}(L) = \{0\} \\ &\Rightarrow\; \lambda_1 \cdot b_1 + \ldots + \lambda_n \cdot b_n = 0 \\ &\Rightarrow\; \lambda_1 = \ldots = \lambda_n = 0. \end{aligned}$$

$\square$

Beispiele: **1)** $L : \mathbb{R}^4 \to \mathbb{R}^2 : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \mapsto \begin{pmatrix} x_2 \\ 0 \end{pmatrix}$ ist linear.

$$\begin{aligned} \operatorname{Kern}(L) \;&=\; \left\{ \begin{pmatrix} x_1 \\ 0 \\ x_3 \\ x_4 \end{pmatrix} : x_1, x_3, x_4 \in \mathbb{R} \right\} &&\Rightarrow\; \dim(\operatorname{Kern}(L)) = 3 \\ \operatorname{Bild}(L) \;&=\; \left\{ \begin{pmatrix} x_2 \\ 0 \end{pmatrix} : x_2 \in \mathbb{R} \right\} &&\Rightarrow\; \dim(\operatorname{Bild}(L)) = 1 \\ 3 + 1 \;&=\; 4 \;=\; \dim(\mathbb{R}^4) \end{aligned}$$

2) $L : \mathcal{P}_n \to \mathcal{P} : P \mapsto P'$:

$$\left.\begin{array}{rcl} \dim(\mathrm{Kern}\,(L)) & = & 1 \\ \dim(\mathcal{P}_n) & = & n+1 \end{array}\right\} \Rightarrow \ \dim(\mathrm{Bild}\,(L)) \ = \ n+1-1 \ = \ n$$

3.28 Definition: Sei $L : V \to W$ linear. Dann heißt $\mathrm{Rang}(L) := \dim\big(\mathrm{Bild}\,(L)\big)$ der **Rang** der Abbildung L.

3.4 Lineare Abbildungen und Matrizen

3.29 Erinnerung: Seien V, W Vektorräume über $\mathbb{K}$.

1) $L : V \to W$ heißt linear, falls

$$\forall u, v \in V \ \ \forall \lambda, \mu \in \mathbb{K} : L(\lambda \cdot u + \mu \cdot v) = \lambda \cdot Lu + \mu \cdot Lv.$$

2) Der Kern von L: $\mathrm{Kern}\,(L) := \{v \in V : Lv = 0\} = L^{-1}(\{0\}$ ist ein Untervektorraum von V.

3) Das Bild $\mathrm{Bild}\,(L) := \{Lv : v \in V\}$ ist ein Untervektorraum von W.

3.30 Lineare Abbildung und Basis: Sei $\{b_1, \ldots, b_n\}$ Basis von V, $\{w_1, \ldots, w_n\} \subseteq W$. Dann existiert genau eine lineare Abbildung $L : V \to W$ mit

$$L(b_1) = w_1, \ \ldots, \ L(b_n) = w_n.$$

Beweis: **1)** Annahme: $L : V \to W$ ist eine lineare Abbildung mit $L(b_j) = w_j, \ j = 1, \ldots, n$.

$$\begin{aligned} \text{Sei } v \in V \quad \Rightarrow \quad & v = \sum_{j=1}^{n} \lambda_j \cdot b_j, \ \lambda_j \text{ eindeutig} \\ \Rightarrow \quad & L(v) \ = \ \sum_{j=1}^{n} \lambda_j \cdot L(b_j) \ = \ \sum_{j=1}^{n} \lambda_j \cdot w_j \ \Rightarrow \ L(v) \text{ ist eindeutig} \end{aligned}$$

$\Rightarrow$ Eindeutigkeit von L.

2) Definiere $L : V \to W : \sum_{j=1}^{n} \lambda_j \cdot b_j \mapsto \sum_{j=1}^{n} \lambda_j \cdot w_j$ Dann ist L linear (durch Nachrechnen)

$\Rightarrow$ Existenz von L.

$\square$

Beispiele: **1)** $V = \mathbb{K}^n,\ b_j = e_j$ (kanonische Basis)

$$\Rightarrow\ L : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{j=1}^{n} x_j \cdot w_j$$

2) $L : \mathbb{R}^2 \to \mathbb{R}^3$ definiert durch $L\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix},\ L\begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix}$

$$\Rightarrow\ L\begin{pmatrix} x \\ y \end{pmatrix} = L\left(x \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = x \cdot \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix} + y \cdot \begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 2x - y \\ 2x - y \end{pmatrix}$$

3.31 Satz: **1)** Äquivalent sind: **(i)** LH $\big(\{w_1, \ldots, w_n\}\big) = W$.
(ii) L ist surjektiv.

2) Äquivalent sind: **(i)** $\{w_1, \ldots, w_n\}$ ist linear unabhängig.
(ii) L ist injektiv.

3) Äquivalent sind: **(i)** $\{w_1, \ldots, w_n\}$ ist Basis von W.
(ii) L ist bijektiv.

Beweis: Siehe 3.20 □

3.32 Folgerung: Seien $B = \{b_1, \ldots, b_n\}, C = \{c_1, \ldots, c_m\}$ Basen von V bzw. W, und

$$w_k \ = \ \sum_{j=1}^{m} \alpha_{jk} \cdot c_j \qquad (k = 1, \ldots, n)$$

die eindeutigen Darstellungen von $w_1, \ldots, w_n$ bezüglich der Basis C. Dann ist die in 3.30 gegebene Abbildung eindeutig bestimmt durch Angabe der α_{jk}. Vereinbarung: Schreibe die α_{jk} in Matrixform:

$$M \ = \ M_L^{C,B} \ = \ \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{pmatrix} \ = \ (\alpha_{jk}) \ = \ (\alpha_{jk})_{\substack{j = 1, \ldots, m \\ k = 1, \ldots, n}} .$$

3.33 Definition: $M = M_L^{C,B}$ heißt die $\boldsymbol{m \times n}$ **- Matrix** der linearen Abbildung L bezüglich der Basen B und C. Es gelten:

1) Zeilenzahl = dim W (Bildraum),

2) Spaltenzahl = dim V (Urbildraum),

3) in den Spalten stehen die Koordinaten bezüglich C der Bilder der Basisvektoren:

$$M_L^{C,B} = \begin{pmatrix} \cdot & \alpha_{12} & \cdots & \cdots \\ \cdot & \alpha_{22} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ \cdot & \alpha_{m2} & \cdots & \cdots \end{pmatrix} \Rightarrow L(b_2) = \alpha_{12} \cdot c_1 + \ldots + \alpha_{m2} \cdot c_m =: \begin{pmatrix} \alpha_{12} \\ \alpha_{22} \\ \vdots \\ \alpha_{m2} \end{pmatrix}_C$$

Beispiele: **1)** $L : \mathbb{R}^2 \to \mathbb{R}^2 : \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}$

$$B = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} = C \Rightarrow M_L^{C,B} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Aber:

$$C' = \left\{ \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix} \right\} \Rightarrow M_L^{C',B} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}$$

2) Zu $\mathbb{0} : V \to W : v \mapsto 0$ gehört immer die Nullmatrix

$$M_{\mathbb{0}}^{C,B} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} =: \mathbb{0}$$

3) Zu $\mathrm{Id}_V : V \to V : x \mapsto x$ gehört bezüglich **einer** Basis B die Einheitsmatrix:

$$M_{\mathrm{Id}_V}^{B,B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} =: E_n \ (n = \text{Anzahl Spalten/Zeilen})$$

Aber: $M_{\mathrm{Id}_V}^{C,B}$ sieht anders aus, wenn $C \neq B$ (Transformationsmatrizen).

4) Sei $L : V \to W$ bijektiv, $B = \{b_1, \ldots, b_n\}$ Basis von V, $C := \{Lb_1, \ldots, Lb_n\}$ (nach 3.31 ist C Basis von W).

$$\Rightarrow M_L^{C,B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} = E_n$$

Diese Matrix sagt über die Abbildung nicht viel aus.

5) $V = \mathbb{R}^3,\ B = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}, W = \mathbb{R}^2,\ C = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}.$

$$M_L^{C,B} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \Rightarrow \left\{ \begin{array}{lcl} L\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} & = & \begin{pmatrix} 1 \\ 4 \end{pmatrix} \\ L\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} & = & \begin{pmatrix} 2 \\ 5 \end{pmatrix} \\ L\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} & = & \begin{pmatrix} 3 \\ 6 \end{pmatrix} \end{array} \right.$$

$$\Rightarrow L\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = L\left(x_1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + x_3 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} 1x_1 + 2x_2 + 3x_3 \\ 4x_1 + 5x_2 + 6x_3 \end{pmatrix}$$

3.34 Das Bild eines Vektors: Sei $L : V \to W$ gegeben durch $M_L^{C,B} = (\alpha_{jk})$, und sei $B = \{b_1, \ldots, b_n\}$, $C = \{c_1, \ldots, c_m\}$.
Für $v \in V$ gilt $v = \sum_{k=1}^{n} v_k \cdot b_k$ und

$$\begin{aligned} Lv &= \sum_{k=1}^{n} v_k \cdot L(b_k) \\ &= \sum_{k=1}^{n} v_k \cdot \left(\sum_{j=1}^{m} \alpha_{jk} \cdot c_j \right) \\ &= \sum_{j=1}^{m} \underbrace{\left(\sum_{k=1}^{n} \alpha_{jk}\, v_k \right)}_{= \text{Koordinaten von } Lv \text{ bezüglich C}} \cdot c_j \end{aligned}$$

Also $L : v \mapsto Lv$

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}_B \mapsto \begin{pmatrix} \sum_{k=1}^{n} \alpha_{1k}\, v_k \\ \vdots \\ \sum_{k=1}^{n} \alpha_{mk}\, v_k \end{pmatrix}_C =: \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \vdots & & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}_B$$

D.h.: 1. Koordinate des Bildvektors = 1. Zeile der Matrix „Mal“ Vektor

$\vdots$

m-te Koordinate des Bildvektors = m-te Zeile der Matrix „Mal“ Vektor

3.35 Satz: Seien $B = \{b_1, \ldots, b_n\}, C = \{c_1, \ldots, c_m\}$ Basen von V bzw. W und $M_L^{C,B}$ die Matrix der Abbildung $L : V \to W$. Dann berechnen sich die Koordinaten von Lv bezüglich der Basis C aus den Koordinaten von v bezüglich B durch

$$\big(Lv\big)_C = \begin{pmatrix} (Lv)_1 \\ \vdots \\ (Lv)_m \end{pmatrix}_C = \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \ldots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}_B = M_L^{C,B}\, v_B$$

3.36 Satz: Sei $L : V \to W$ linear, B Basis von V, C Basis von W und $M_L^{C,B} = (a_{jk})$ mit den Spaltenvektoren

$$a_k := \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{mk} \end{pmatrix}_C \qquad (k = 1, \ldots, m).$$

Dann gelten

$$\begin{aligned} \text{Bild}\,(L) &= \text{LH}\{a_1, \ldots, a_n\}, \\ \text{Rang}\,(L) &= \dim\Big(\text{LH}\{a_1, \ldots, a_n\}\Big). \end{aligned}$$

3.37 Satz: Sei $L : V \to W$ linear, $\dim(V) = n,\ \dim(W) = m$. Dann existieren Basen B, C von V bzw. W so, dass

$$M_L^{C,B} \;=\; \begin{array}{c}
\left(\begin{array}{ccccccc}
1 & 0 & 0 & \dots & & & 0 \\
0 & 1 & 0 & \dots & & & 0 \\
\vdots & \ddots & \ddots & \ddots & & & \vdots \\
0 & \dots & 0 & 1 & 0 & \dots & 0 \\
0 & \dots & & & & \dots & 0 \\
\vdots & & & & & & \vdots \\
0 & \dots & & & & \dots & 0
\end{array}\right)
\begin{array}{l}
\\ \\ \\
\leftarrow k\text{-te Zeile} \\
\left.\begin{array}{l} \\ \\ \\ \end{array}\right\} m-k \text{ Nullzeilen}
\end{array}
\\
\begin{array}{cc}
\uparrow & \underbrace{\hphantom{0 \quad \dots \quad 0}}_{n-k \text{ Nullspalten}} \\
k\text{-te Spalte} &
\end{array}
\end{array}$$

und es gelten

$$\begin{array}{rcl}
\operatorname{Rang}(L) & = & \text{Anzahl der Spalten ungleich Null} \;=\; k \\
\dim \operatorname{Kern}(L) & = & \text{Anzahl der Nullspalten} \;=\; n-k \;=\; \dim V - k
\end{array}$$

3.38 Verknüpfung linearer Abbildungen: Seien U, V, W Vektorräume mit endlichen Basen B_U, B_V, B_W und

$K : U \to V$ linear mit Matrix $\quad M_K^{B_V, B_U} = (\beta_{jk})_{\substack{j=1,\dots,m \\ k=1,\dots,n}}$

$L : V \to W$ linear mit Matrix $\quad M_L^{B_W, B_V} = (\alpha_{ij})_{\substack{i=1,\dots,l \\ j=1,\dots,m}}$

Dann ist die Matrix von $L \circ K$ gegeben durch

$$(\gamma_{ik})_{\substack{i=1,\dots,l \\ k=1,\dots,n}} \;=\; M_{L\circ K}^{B_W, B_U} \;=:\; M_L^{B_W, B_V} \cdot M_K^{B_V, B_U} \;=\; (\alpha_{ij}) \cdot (\beta_{jk})$$

wobei das **Matrizenprodukt** definiert ist durch

$$\gamma_{ik} \;:=\; \sum_{j=1}^{m} \alpha_{ij}\, \beta_{jk}$$

($\gamma_{ik} = i$-te Zeile der Matrix (α_{ij}) „Mal“ k-te Spalte der Matrix (β_{jk})).

Beweis: $B_u = \{a_1, \dots, a_n\},\ B_V = \{b_1, \dots, b_m\},\ B_W = \{c_1, \dots, c_l\}$

$$\begin{aligned}
\Rightarrow\ (L \circ K)(a_k) &= L\big(K(a_k)\big) \\
&= L\left(\sum_{j=1}^{m} \beta_{jk} \cdot b_j\right) \\
&= \sum_{j=1}^{m} \beta_{jk} \cdot L(b_j) \\
&= \sum_{j=1}^{m} \beta_{jk} \cdot \left(\sum_{i=1}^{l} \alpha_{ij} \cdot c_i\right) \\
&= \sum_{i=1}^{l} \underbrace{\left(\sum_{j=1}^{m} \alpha_{ij}\, \beta_{jk}\right)}_{=\gamma_{ik}} \cdot c_i
\end{aligned}$$

□

3.39 Definition: Die Matrix $C = (\gamma)_{ik}$ heißt **Matrizenprodukt** von A und B: $\quad C = A \cdot B$. Das Matrizenprodukt $A \cdot B$ kann nur gebildet werden, wenn Spaltenzahl von A = Zeilenzahl von B.

Beispiele: **1)** $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$

2) $\begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 2 & -2 \\ 2 & -1 & 0 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 \\ 0 & -1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -5 \\ 0 & 1 \\ -1 & -3 \end{pmatrix}.$

3) $\begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 2 & -2 \\ 2 & -1 & 0 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}.$

4) $\begin{pmatrix} 1 & 2 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = (1).$

5) $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 2 & -1 & 1 \\ 1 & 2 & -1 & 1 \end{pmatrix}$

(manchmal auch "dyadisches Produkt"). Insbesondere $A \cdot B \neq B \cdot A$ (vergleiche mit dem vorigen Beispiel).

3.40 Matrizen und lineare Abbildungen: Zu einer $m \times n$-Matrix

$$M = (a_{jk})_{\substack{j=1,\dots,m\\k=1,\dots,n}} \quad \text{mit Spaltenvektoren } a_k = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix} \in \mathbb{K}^m$$

definieren wir die lineare Abbildung

$$L_M : \mathbb{K}^n \to \mathbb{K}^m : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{k=1}^{n} x_k \cdot a_k = M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Dann gilt $M_{L_M}^{E',E} = M$, wenn E, E' die kanonischen Basen von $\mathbb{K}^n$ bzw. $\mathbb{K}^m$ bezeichnen. Die Abbildung

$$\Phi : M \mapsto L_M \text{ mit Umkehrabbildung } \Phi^{-1} : L \mapsto M_L^{E',E}$$

ist eine bijektive Abbildung von der Menge aller $m \times n$-Matrizen auf die Menge aller linearen Abbildungen $L : \mathbb{K}^n \to \mathbb{K}^m$

Sei nun M eine $m \times n$-Matrix und K eine $l \times m$-Matrix. Dann: $\Phi(M) : \mathbb{R}^n \to \mathbb{R}^m$, $\Phi(K) : \mathbb{R}^m \to \mathbb{R}^l$, und

$$\begin{array}{ccccl} (K, & M) & \longmapsto & K \cdot M & \text{Matrizenmultiplikation} \\ \updownarrow & \updownarrow & & \updownarrow & \\ (\Phi(K), & \Phi(M)) & \longmapsto & \Phi(K) \circ \Phi(M) & \text{Hintereinanderausführung} \end{array}$$

Also: $\Phi(K \cdot M) = \Phi(K) \circ \Phi(M)$.
So wurde die Matrizenmultiplikation definiert!

3.41 Umkehrabbildungen: **1)** Sei $L : V \to V$ linear und invertierbar, B eine Basis von V mit n Elementen. Dann gilt

$$M_L^{B,B} \cdot M_{L^{-1}}^{B,B} = M_{L^{-1}}^{B,B} \cdot M_L^{B,B} = M_{\mathrm{Id}}^{B,B} = E_n := \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

Die $n \times n$-Matrix E_n heißt **Einheitsmatrix**.

2) Sei M eine $n \times n$-Matrix (über $\mathbb{K}$). Falls eine $n \times n$-Matrix M^{-1} existiert mit $M \cdot M^{-1} = E_n$, so gilt auch $M^{-1} \cdot M = E_n$. Außerdem ist die Matrix M^{-1} eindeutig, d.h. die Matrizengleichung

$$M \cdot X = E_n$$

besitzt genau eine Lösung $X = M^{-1}$.

3.42 Definition: Eine $n \times n$-Matrix M über $\mathbb{K}$ heißt **invertierbar**, falls eine $n \times n$-Matrix M^{-1} existiert mit $M \cdot M^{-1} = E_n$. Dann gilt auch $M^{-1} \cdot M = E_n$, und die Matrix M^{-1} heißt **inverse Matrix** zu M.

3.43 Folgerung: Es sei $L : V \to V$ linear mit Matrix $M = M_L^{B,B}$. Dann sind äquivalent:

(i) L ist invertierbar (d.h. bijektiv).

(ii) M ist invertierbar.

Beweis: (i) $\Rightarrow\ M_{L^{-1}}^{B,B} = M^{-1}\ \Rightarrow$ (ii)

(ii) $\Rightarrow$ Setze $K : V \to V : x \mapsto K(x)$ mit $\big(K(x)\big)_B := M^{-1}\, x_B$.
Dann: $M_K^{B,B} = M^{-1}$ und $M_{L\circ K}^{B,B} = M_L^{B,B} \cdot M_K^{B,B} = M \cdot M^{-1} = E = M_{\mathrm{Id}_V}^{B,B}$
$\Rightarrow\ L \circ K = \mathrm{Id}_V$, also $K = L^{-1}$
$\Rightarrow$ (i)

$\square$

3.44 Satz: Die Menge

$$\big\{L : \mathbb{K}^n \to \mathbb{K}^n \;\big|\; L \text{ ist linear und bijektiv}\big\}$$

mit der Hintereinanderausführung $\circ$ als Verknüpfung bildet eine Gruppe, die **lineare Gruppe $\mathbf{GL}_n(\mathbb{K})$**.

3.45 Folgerung: Sind A, B invertierbare Matrizen, dann ist auch $A \cdot B$ invertierbar und es gilt

$$(A \cdot B)^{-1} \;=\; B^{-1} \cdot A^{-1}.$$

3.46 Folgerung: Die Menge

$$\big\{M \;\big|\; M \text{ ist invertierbare } n \times n\text{-Matrix über } \mathbb{K}\big\}$$

mit der Matrizenmultiplikation als Verknüpfung bildet eine Gruppe. Sie wird ebenfalls als **lineare Gruppe $\mathbf{GL}_n(\mathbb{K})$** bezeichnet.

3.5 Lineare Gleichungssysteme II

3.47 Matrizen und lineare Abbildungen: Zu einer $m \times n$-Matrix

$$M = (a_{jk})_{\substack{j=1,\dots,m\\ k=1,\dots,n}} \qquad \text{mit den Spaltenvektoren} \quad a_k = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix} \in \mathbb{K}^m$$

definieren wir die lineare Abbildung

$$L_M : \mathbb{K}^n \to \mathbb{K}^m : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{k=1}^{n} x_k \cdot a_k = M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Dann gilt $M_{L_M}^{E',E} = M$, wenn E, E' die kanonischen Basen von $\mathbb{K}^n$ bzw. $\mathbb{K}^m$ bezeichnen.

Damit definiert

$$M \ \mapsto \ L_M \qquad \text{mit Umkehrabbildung} \qquad L \ \mapsto M_L^{E',E}$$

eine bijektive Abbildung von der Menge aller $m \times n$-Matrizen auf die Menge aller linearen Abbildungen $L : \mathbb{K}^n \to \mathbb{K}^m$.

3.48 LGS und Matrizen: Sei ein LGS

$$\left.\begin{array}{lllllll} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & \dots & & & + & a_{2n}x_n & = & b_2 \\ \vdots & & & & & & & & \\ a_{m1}x_1 & + & \dots & & & + & a_{mn}x_n & = & b_m \end{array}\right\} \qquad (*)$$

mit der **Koeffizientenmatrix**

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

gegeben. Dann ist $x_1, \dots, x_n$ genau dann Lösung von $(*)$, wenn der Vektor $x := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ Lösung von

$$L_M\, x \ = \ b \ := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \qquad (**)$$

ist, oder anders geschrieben:

$$M\, x \ = \ b \qquad (***)$$

3.49 Folgerung: Das LGS $L\, x = b$ ist genau dann lösbar, wenn $b \in \mathrm{Bild}\,(L)$.

3.50 Lösungsstruktur: Sei $L : \mathbb{K}^n \to \mathbb{K}^m$ und das inhomogene LGS $L\, x = b$ gegeben. Ist x_0 eine Lösung, dann sind alle Lösungen gegeben durch

$$x \ = \ x_0 + \mathrm{Kern}\,(L) \ := \ \{x_0 + y : y \in \mathrm{Kern}\,(L)\} \ = \ \{x_0 + y : Ly = 0\}.$$

Man nennt x_0 **partikuläre Lösung**, obwohl x_0 nur irgendeine Lösung bezeichnet (falls es mehrerere Lösungen gibt).

3.51 Folgerung: Sei $L : \mathbb{K}^n \to \mathbb{K}^n$ und das LGS $L\,x = b$ gegeben. Dann sind äquivalent:

(i) Das LGS besitzt für jeden Vektor $b \in \mathbb{K}^n$ genau eine Lösung.

(ii) $\operatorname{Kern}(L) = \{0\}$

(iii) $\operatorname{Rang}(L) = n$

Beweis: (i) $\Rightarrow$ $\operatorname{Kern}(L) = \{0\}$ $\Leftrightarrow$ (ii)

(ii) $\Leftrightarrow$ (iii): Dimensionsformel $n = \dim(\operatorname{Kern}(L)) + \underbrace{\dim(\operatorname{Bild}(L))}_{=\operatorname{Rang}(L)}$

(ii) $\Rightarrow$ (i): (ii) $\Rightarrow$ (iii) $\Rightarrow$ $\operatorname{Bild}(L) = \mathbb{K}^n$ $\Rightarrow$ $b \in \operatorname{Bild}(L) \Rightarrow$ mindestens eine Lösung existiert.
(ii) $\Rightarrow$ Lösung ist eindeutig
$\Rightarrow$ (i) $\square$

3.52 Definition: Sei $M = (a_{jk})$ eine $m \times n$-Matrix mit den Spaltenvektoren $a_k = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix}$ $(k = 1, \ldots, n)$. Der **Rang** von M ist definiert durch

$$\operatorname{Rang}(M) \;:=\; \operatorname{Rang}(L_M) \;=\; \dim(\operatorname{Bild}(L_M)) \;=\; \dim \operatorname{LH}\big(\{a_1, \ldots, a_n\}\big).$$

3.53 Folgerung: Eine $n \times n$-Matrix M ist genau dann invertierbar, wenn $\operatorname{Rang}(M) = n$.

Beweis: M invertierbar

$$\begin{aligned} &\Leftrightarrow\; L_M \text{ bijektiv} \\ &\Leftrightarrow\; \begin{cases} \operatorname{Bild}(L_M) = \mathbb{K}^n & (L_M \text{ surjektiv}) \\ \operatorname{Kern}(L_M) = \{0\} & (\Leftrightarrow\; L_M \text{ injektiv}) \end{cases} \\ &\Leftrightarrow\; \dim(\operatorname{Bild}(L_M)) = n \\ &\Leftrightarrow\; \operatorname{Rang}(L_M) = n \end{aligned}$$

$\square$

3.54 Satz: Sei das LGS $A\,x = b$ gegeben, $A' := (A\,b)$ die **erweiterte Koeffizientenmatrix**. Dann sind äquivalent:

(i) $A\,x = b$ besitzt mindestens eine Lösung.

(ii) $\operatorname{Rang}(A) = \operatorname{Rang}(A')$.

Beweis: (i) $\Leftrightarrow\ b \in \mathrm{LH}\{a_1, \dots, a_n\}$

$\Leftrightarrow\ \mathrm{LH}\{a_1, \dots, a_n\} = \mathrm{LH}\{a_1, \dots, a_n, b\}$

$\Leftrightarrow\ \mathrm{Rang}(A) = \mathrm{Rang}(A')$ □

3.55 Berechnung inverser Matrizen: Sei M eine $n \times n$-Matrix. Schreibe $\big(M \big| E_n\big)$. Wende Gaußalgorithmus an, bis links vom Trennstrich die Einheitsmatrix steht. Dann steht rechts die inverse Matrix:

$$\big(M \big| E_n\big) \Leftrightarrow \dots \Leftrightarrow \big(E_n \big| M^{-1}\big).$$

3.6 Basiswechsel

3.56 Definition: Sei V ein Vektorraum mit Basen B, B'. Dann heißt

$$S \ := \ M_{\mathrm{Id}_V}^{B',B}$$

die **Basiswechselmatrix** von B auf B'.

3.57 Eigenschaften: **1)** Ist $B = \{b_1, \dots, b_n\}$ und $B' = \{c_1, \dots, c_n\}$ und

$$v \ = \ \sum_{j=1}^{n} x_j \cdot b_j \ = \ \sum_{j=1}^{n} y_j \cdot c_j,$$

so können die Koordinaten $x_1, \dots, x_n$ und $y_1, \dots, y_n$ folgendermaßen umgerechnet werden:

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}_{B'} = M_{\mathrm{Id}_V}^{B',B} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}_{B} \quad \text{bzw.} \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}_{B} = M_{\mathrm{Id}_V}^{B,B'} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}_{B'}$$

2) S ist invertierbar: $S^{-1} = M_{\mathrm{Id}_V}^{B,B'}$.

3) Ist $L : V \to V$ linear, dann ist

$$M_L^{B',B'} \ = \ M_{\mathrm{Id}_V}^{B',B} \cdot M_L^{B,B} \cdot M_{\mathrm{Id}_V}^{B,B'}$$

4) Allgemeiner: Seien $L : U \to V$, B, B' Basen von U, C, C' Basen von V, $M := M_L^{C,B}$, $R := M_{\mathrm{Id}_U}^{B',B}$, $S := M_{\mathrm{Id}_V}^{C',C}$. Dann gelten

$$\begin{aligned} M_L^{C',B} &= M_{\mathrm{Id}_V}^{C',C} \cdot M_L^{C,B} &&= S \cdot M \\ M_L^{C,B'} &= M_L^{C,B} \cdot M_{\mathrm{Id}_U}^{B,B'} &&= M \cdot R^{-1} \\ M_L^{C',B'} &= M_{\mathrm{Id}_V}^{C',C} \cdot M_L^{C,B} \cdot M_{\mathrm{Id}_U}^{B,B'} &&= S \cdot M \cdot R^{-1} \end{aligned}$$

3.58 Definition: **1)** Zwei $m \times n$-Matrizen A, B heißen **äquivalent**, wenn es invertierbare Matrizen S $(m \times m)$ und R $(n \times n)$ gibt mit

$$B \;=\; S \cdot A \cdot R^{-1} \qquad \text{(vgl. oben } M_L^{C',B'} = S \cdot M \cdot R^{-1}\text{)}.$$

D.h. A und B beschreiben bezüglich geeigneter Basen dieselbe Abbildung.
Insbesondere: $\operatorname{Rang}(A) = \operatorname{Rang}(B)$.

2) Zwei $n \times n$-Matrizen A, B heißen **ähnlich**, wenn es eine invertierbare $n \times n$-Matrix S gibt mit

$$B \;=\; S \cdot A \cdot S^{-1}\,.$$

3.59 Satz: Es sei M eine $m \times n$-Matrix. Die Anwendung des Gauß-Algorithmus (Vertauschen von Zeilen und Addition des Vielfachen einer Zeile zu einer anderen Zeile) ändert den Rang von M nicht. Insbesondere gilt

$$\begin{aligned} \operatorname{Rang}(M) \;&=\; \text{maximale Anzahl linear unabhängiger Spalten} \\ &=\; \text{maximale Anzahl linear unabhängiger Zeilen} \end{aligned}$$

Beweis: **1)** Vertauschung zweier Zeilen, z.B. 1. und 2. Zeile:

$$M' = \begin{pmatrix} 0 & 1 & 0 & \dots & & 0 \\ 1 & 0 & 0 & \dots & & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & 0 & \ddots & & \vdots \\ & & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \cdot M \cdot E_n$$

$\Rightarrow$ M', M sind äquivalent, haben denselben Rang.

2) Addition $\lambda \cdot$ (1. Zeile) zur 2. Zeile:

$$M' = \begin{pmatrix} 1 & 0 & \dots & & 0 \\ \lambda & 1 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \vdots & \\ \vdots & \vdots & & & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \cdot M \cdot E_n$$

$\Rightarrow$ M', M sind äquivalent, haben denselben Rang.

3) Forme M mit Gaußschritten um zu Zeilenstufenmatrix M'

$$\Rightarrow \operatorname{Rang}(M) = \operatorname{Rang}(M') = \text{ Anzahl der nicht-Null Zeilen in } M'$$

Gauß-Schritte ändern nicht die maximale Anzahl der linear unabhängigen Zeilen. $\square$

3.7 Länge von Vektoren

3.60 Definition: Seien $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ und V ein $\mathbb{K}$-Vektorraum. Eine Abbildung $\|.\| : V \to \mathbb{R} : x \mapsto \|x\|$ heißt **Norm**, falls für $x, y \in V$ und $\lambda \in \mathbb{K}$ gilt:

(N1) $\|x\| \geq 0 \quad \wedge \quad (\|x\| = 0 \Leftrightarrow x = 0)$ (**Positivität**)

(N2) $\|\lambda \cdot x\| \;=\; |\lambda|\,\|x\|$ (**Homogenität**)

(N3) $\|x + y\| \;\leq\; \|x\| + \|y\|$ (**$\boldsymbol{\Delta}$-Ungleichung**)

(vgl. Eigenschaften des Betrages in Satz 2.15).

3.61 Definition: Ist $\|.\|$ eine Norm auf V, so heißt $B_1(0) \;:=\; \{x \in V : \|x\| \leq 1\}$ **Einheitskugel**. Ist $\|x\| = 1$, so heißt x **Einheitsvektor**.

3.62 Definition: Sei V Vektorraum über $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ mit Norm $\|.\|$. Dann heißt

$$d(x, y) \;:=\; \|x - y\| \qquad \text{für } x, y \in V$$

der **Abstand** von x zu y. Der Abstand besitzt folgende Eigenschaften:

(M1) $d(x, y) \;\geq\; 0$ sowie $d(x, y) \;=\; 0 \;\Leftrightarrow\; x = y$ (**Positivität**, **Definitheit**).

(M2) $d(x, y) \;=\; d(y, x)$ (**Symmetrie**).

(M3) $d(x, y) \;\leq\; d(x, z) + d(z, y)$ (**$\boldsymbol{\Delta}$-Ungleichung**).

(vgl. Abstand in Körpern, Definition 2.18).

3.8 Winkel im Vektorraum

3.63 Definition: Sei V Vektorraum über $\mathbb{R}$ oder $\mathbb{C}$. Eine Abbildung

$$V \times V \to \mathbb{K} : (x, y) \mapsto \langle x, y \rangle$$

heißt **Skalarprodukt** (*engl. inner product*) auf V, falls

(SP1) $\langle x, x \rangle \geq 0 \quad \wedge \quad (\langle x, x \rangle = 0 \Leftrightarrow x = 0)$

(SP2) $\langle y, x \rangle = \overline{\langle x, y \rangle}$

(SP3) $\langle \lambda \cdot x + \mu \cdot y, z \rangle = \lambda \langle x, z \rangle + \mu \langle y, z \rangle$

Ein Vektorraum mit Skalarprodukt $(V, \langle ., . \rangle)$ heißt auch **euklidischer** $(\mathbb{K} = \mathbb{R})$ oder **unitärer** $(\mathbb{K} = \mathbb{C})$ Vektorraum.

Beispiele: **1)** Standard-Skalarprodukt im $\mathbb{R}^n$:

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = \sum_{j=1}^{n} x_j \, y_j .$$

2) Standard-Skalarprodukt im $\mathbb{C}^n$:

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = \sum_{j=1}^{n} x_j \, \overline{y_j} .$$

3) Im $\mathbb{R}^n$ ist auch

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle^{\sim} = \left\langle \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle = \sum_{j=1}^{n} \lambda_j \, x_j \, y_j$$

ein Skalarprodukt, falls $\lambda_1, \ldots, \lambda_n > 0$.

3.64 Eigenschaften: **1)** Für festes $y \in V$ ist die Abbildung

$$x \mapsto \langle x, y \rangle$$

linear nach (SP3).

2) Nach (SP2) und (SP3)

$$\langle x, \lambda \cdot y + \mu \cdot z \rangle \;=\; \overline{\lambda} \, \langle x, y \rangle + \overline{\mu} \, \langle x, z \rangle \, .$$

3) $\big(\forall y \in V : \langle x, y \rangle = 0\big) \;\Rightarrow\; x = 0$ (Setze $y := x$, siehe (SP1)).

3.65 Satz (Cauchy-Schwarz-Bunjakowski Ungleichung (CSB)): Für $x, y \in V$ gilt

$$|\, \langle x, y \rangle \,| \;\leq\; \sqrt{\langle x, x \rangle} \cdot \sqrt{\langle y, y \rangle}.$$

Beweis: Fall $y = 0 : \Rightarrow\; 0 \leq 0$ stimmt.

Fall $y \neq 0$: Setze $\lambda := -\dfrac{\langle x, y \rangle}{\langle y, y \rangle}$.

$$\begin{aligned}
\text{(SP1)} \;\Rightarrow\; 0 \;&\leq\; \langle y, y \rangle \, \langle x + \lambda y, x + \lambda y \rangle \\
&=\; \langle y, y \rangle \big(\langle x, x \rangle + \lambda \, \langle y, x \rangle + \overline{\lambda} \, \langle x, y \rangle + |\lambda|^2 \, \langle y, y \rangle \big) \\
&=\; \langle y, y \rangle \, \langle x, x \rangle - |\, \langle x, y \rangle \,|^2 - |\, \langle x, y \rangle \,|^2 + |\, \langle x, y \rangle \,|^2 \\
&=\; \langle y, y \rangle \, \langle x, x \rangle - |\, \langle x, y \rangle \,|^2 \\
\Rightarrow\; |\, \langle x, y \rangle \,|^2 &\leq \langle y, y \rangle \, \langle x, x \rangle
\end{aligned}$$

$\square$

3.66 Satz: Ist $(V, \langle .,. \rangle)$ ein Vektorraum mit Skalarprodukt, so definiert

$$\|x\|_2 \;:=\; \sqrt{\langle x, x\rangle}$$

eine Norm auf V. Die Cauchy-Schwarz-Bunjakowski-Ungleichung wird zu

$$|\langle x, y\rangle| \;\leq\; \|x\|_2 \cdot \|y\|_2.$$

Beweis: **(N1)** $\|x\|_2 \geq 0$ stimmt, $\|x\|_2 = 0 \;\Leftrightarrow\; \langle x, x\rangle = 0 \;\Leftrightarrow\; x = 0$.

(N2) $\|\lambda \cdot x\|_2 = \sqrt{\langle \lambda \cdot x, \lambda \cdot x\rangle} = \sqrt{|\lambda|^2 \langle x, x\rangle} = |\lambda|\, \|x\|_2$.

(N3)
$$\begin{aligned} \|x+y\|_2^2 &= \langle x+y, x+y\rangle \;=\; \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle \\ &= \|x\|_2^2 + \|y\|_2^2 + 2\mathrm{Re}\,\langle x, y\rangle \\ &\leq \|x\|_2^2 + \|y\|_2^2 + 2|\langle x, y\rangle| \\ &\leq \|x\|_2^2 + \|y\|_2^2 + 2\|x\|_2\,\|y\|_2 \\ &= \big(\|x\|_2 + \|y\|_2\big)^2 \end{aligned}$$

□

3.9 Orthogonalität

3.67 Definition: Sei V ein Vektorraum mit Skalarprodukt $\langle .,. \rangle$.

1) $x, y \in V$ heißen **orthogonal** ($x \perp y$), falls $\langle x, y\rangle = 0$.

2) Eine Familie $(v_i)_{i \in I} \subseteq V$ mit $v_i \neq 0$ für $i \in I$ heißt **Orthogonalsystem**, falls $v_i \perp v_j$ für $i \neq j$, und **Orthonormalsystem** (ONS), falls

$$\langle v_i, v_j\rangle \;=\; \delta_{ij} \;=\; \begin{cases} 0 & \text{für } i \neq j \\ 1 & \text{für } i = j. \end{cases}$$

Ist ein ONS gleichzeitig Basis, so heißt es **Orthonormalbasis** (ONB).

3.68 Satz des Pythagoras: Sei $x \perp y$. Dann gilt

$$\|x+y\|_2^2 \;=\; \|x\|_2^2 + \|y\|_2^2\,.$$

3.69 Satz: Ist $(v_i)_{i \in I}$ ein Orthogonalsystem, so ist $\{v_i : i \in I\}$ linear unabhängig.

Beweis: Sei $J \subseteq I$, J endlich und $\sum_{j\in J} \lambda_j \cdot v_j = 0$. Für $k \in J$ folgt

$$0 = \left\langle \sum_{j\in J} \lambda_j \cdot v_j, v_k \right\rangle = \sum_{j\in J} \lambda_j \underbrace{\langle v_j, v_k\rangle}_{=0 \text{ für } j\neq k} = \lambda_k \, \|v_k\|_2^2 \;\Rightarrow\; \lambda_k = 0.$$

□

3.70 Satz: Sei $(V, \langle .,. \rangle)$ Vektorraum mit Skalarprodukt, $\{v_1, v_2, \ldots\} \subseteq V$ endliche oder abzählbare linear unabhängige Menge. Dann gibt es ein ONS $\{e_1, e_2, \ldots\}$ mit der Eigenschaft

$$\forall k \in \mathbb{N} \text{ mit } k \leq \ \sharp\{v_1, v_2, \ldots\} : \mathrm{LH}\{v_1, \ldots, v_k\} = \mathrm{LH}\{e_1, \ldots, e_k\}$$

Insbesondere gilt: Ist $\dim V < \infty$, so besitzt V eine ONB, und jedes ONS lässt sich zu einer ONB ergänzen.

Beweis: Verwende das **Gram-Schmidtsche Orthogonalisierungsverfahren**:

Schritt 1: $e_1 := \dfrac{1}{\|v_1\|_2} \cdot v_1$

Schritt 2: $f_2 := v_2 - \langle v_2, e_1\rangle \cdot e_1 \neq 0$, da $v_2 \notin \mathrm{LH}\{v_1\} = \mathrm{LH}\{e_1\}$

Es gilt $f_2 \perp e_1 : \langle f_2, e_1\rangle = \langle v_2, e_1\rangle - \langle v_2, e_1\rangle \underbrace{\langle e_1, e_1\rangle}_{=1} = 0$

Setze $e_2 := \dfrac{1}{\|f_2\|_2} \cdot f_2 \;\Rightarrow\; \begin{cases} \{e_1, e_2\} \text{ ist ONS} \\ \mathrm{LH}(\{e_1, e_2\} = \mathrm{LH}(\{v_1, v_2\} \end{cases}$

$\vdots$

Schritt k: Sei $\{e_1, \ldots, e_{k-1}\}$ bereits konstruiert.

Dann gilt $v_k \notin \mathrm{LH}\{v_1, \ldots, v_{k-1}\} = \mathrm{LH}\{e_1, \ldots, e_{k-1}\}$

$\Rightarrow \; f_k := v_k - \sum_{j=1}^{k-1} \langle v_k, e_j\rangle \cdot e_j \neq 0$

Es gilt $f_k \perp e_j$ für $j = 1, \ldots, k-1$:

$$\langle f_k, e_j\rangle = \langle v_k, e_j\rangle - \sum_{i=1}^{k-1} \langle v_k, e_i\rangle \underbrace{\langle e_i, e_j\rangle}_{=\delta_{ij}} = \langle v_k, e_j\rangle - \langle v_k, e_j\rangle = 0.$$

Setze $e_k := \dfrac{1}{\|f_k\|_2} \cdot f_k \;\Rightarrow\; \begin{cases} \{e_1, \ldots, e_k\} \text{ ist ONS} \\ \mathrm{LH}(\{e_1, \ldots, e_k\} = \mathrm{LH}(\{v_1, \ldots, v_k\} \end{cases}$

□

3.71 Entwicklung nach Orthonormalbasen: Sei $B = \{e_1, \ldots, e_n\}$ ONB von V.

1) Für alle $v \in V$ gilt

$$v \;=\; \sum_{j=1}^{n} \langle v, e_j \rangle \cdot e_j,$$

d.h. $\langle v, e_1 \rangle, \ldots, \langle v, e_n \rangle$ sind die Koordinaten von v bezüglich $\{e_1, \ldots, e_n\}$.

2) Ist $u = \sum_{j=1}^{n} \lambda_j \cdot e_j,\; v = \sum_{j=1}^{n} \mu_j \cdot e_j$, so gilt

$$\langle u, v \rangle \;=\; \sum_{j=1}^{n} \lambda_j \, \overline{\mu}_j \;=\; \left\langle \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}, \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} \right\rangle_{\mathbb{K}^n} \;=\; \big\langle (u)_B, (v)_B \big\rangle_{\mathbb{K}^n}.$$

Insbesondere gilt

$$\|u\|_2^2 \;=\; \langle u, u \rangle \;=\; \sum_{j=1}^{n} |\lambda_j|^2 \;=\; \sum_{j=1}^{n} \big|\, \langle u, e_j \rangle \,\big|^2$$

(**Parsevalsche Gleichung**).

Beweis: **1)** B Basis $\Rightarrow\; v = \sum_{j=1}^{n} \lambda_j \cdot e_j$.

$$\Rightarrow \text{ für } k = 1, \ldots, n: \; \langle v, e_k \rangle = \sum_{j=1}^{n} \lambda_j \langle e_j, e_k \rangle = \lambda_k.$$

2) $$\langle u, v \rangle \;=\; \left\langle \sum_{j=1}^{n} \lambda_j \cdot e_j, \sum_{k=1}^{n} \mu_k \cdot e_k \right\rangle \;=\; \sum_{j=1}^{n} \sum_{k=1}^{n} \lambda_j \overline{\mu_k} \langle e_j, e_k \rangle \;=\; \sum_{j=1}^{n} \lambda_j \overline{\mu_j}$$

□

3.72 Folgerung: Der Isomorphismus

$$L : \mathbb{K}^n \to V : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{j=1}^{n} x_j \cdot e_j$$

erhält das Skalarprodukt:

$$\langle x, y \rangle_{\mathbb{K}^n} \;=\; \langle L\,x, L\,y \rangle_V\,,$$

und damit auch die Norm. $\mathbb{K}^n$ und V können als identisch angesehen werden.

Beispiele: **1)** $V = \mathbb{R}^2$, $B = \{e_1, e_2\} = \left\{ \begin{pmatrix} \cos\varphi \\ \sin\varphi \end{pmatrix}, \begin{pmatrix} -\sin\varphi \\ \cos\varphi \end{pmatrix} \right\}$ mit festem $\varphi \in \mathbb{R}$.

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}_E \quad \Rightarrow \quad x = \begin{pmatrix} x_1 \cos\varphi + x_2 \sin\varphi \\ -x_1 \sin\varphi + x_2 \cos\varphi \end{pmatrix}_B$$

2) $V = C([0, 2\pi]) := \{f : [0, 2\pi] \to \mathbb{C} \mid f \text{ ist stetig}\}$.

$$\begin{aligned} \langle f, g \rangle &:= \int_0^{2\pi} f(x)\,\overline{g(x)}\,\mathrm{d}x \quad \text{ist Skalarprodukt} \\ \|f\|_2 &:= \left(\int_0^{2\pi} |f(x)|^2\,\mathrm{d}x\right)^{1/2} \quad \text{zugehörige Norm} \end{aligned}$$

Setze

$$\begin{aligned} e_0 :&\quad x \mapsto \frac{1}{\sqrt{2\pi}} \\ e_{2n-1} :&\quad x \mapsto \frac{1}{\sqrt{\pi}} \sin(nx) \\ e_{2n} :&\quad x \mapsto \frac{1}{\sqrt{\pi}} \cos(nx) \end{aligned}$$

Nachrechnen: $\{e_0, e_1, \ldots\}$ ist ONS. Für $f \in \mathrm{LH}\{e_0, e_1, \ldots\}$ gilt

$$f = \sum_n \langle f, e_n \rangle \cdot e_n = b_0 + \sum_{n=1}^{\infty} a_n \sin(nx) + \sum_{n=1}^{\infty} b_n \cos(nx)$$

$$\begin{aligned} b_0 &= \frac{1}{2\pi} \int_0^{2\pi} f(x)\,\mathrm{d}x \\ b_n &= \frac{1}{\pi} \int_0^{2\pi} f(x) \cos(nx)\,\mathrm{d}x \\ a_n &= \frac{1}{\pi} \int_0^{2\pi} f(x) \sin(nx)\,\mathrm{d}x \end{aligned}$$

Lässt man auch „unendliche Summen“ zu, so kann man praktisch jede Funktion f so entwickeln: Theorie der Fourierreihen.

3.73 Satz: Seien V ein Vektorraum mit Skalarprodukt, U ein endlichdimensionaler Unterraum, $\{e_1, \ldots, e_k\}$ ONB von U und $x \in V$ fest. Für $y \in U$ sind äquivalent

(i) $y = \displaystyle\sum_{j=1}^{k} \langle x, e_j \rangle \cdot e_j$

(ii) $x = y + z$ mit $z \perp U$ (d.h. $\forall \tilde{y} \in U : z \perp \tilde{y}$)

(iii) $\forall \tilde{y} \in U : \|x - y\|_2 \leq \|x - \tilde{y}\|_2$.

D.h.: y ist das Element von U, das zu x den kleinsten Abstand hat.

Beweis: **(i) $\Rightarrow$ (ii):** Sei $z := x - y$ und $\widetilde{y} \in U,\ \widetilde{y} = \sum_{j=1}^{k} \lambda_j \cdot e_j$.

$$\begin{aligned} \Rightarrow\ \langle z, \widetilde{y} \rangle &= \langle x - y, \widetilde{y} \rangle = \langle x, \widetilde{y} \rangle - \langle y, \widetilde{y} \rangle \\ &= \sum_{j=1}^{k} \overline{\lambda_j} \langle x, e_j \rangle - \sum_{j=1}^{k} \langle x, e_j \rangle \sum_{l=1}^{k} \langle e_j, \lambda_l \cdot e_l \rangle \\ &= \sum_{j=1}^{k} \overline{\lambda_j} \langle x, e_j \rangle - \sum_{j=1}^{k} \langle x, e_j \rangle \overline{\lambda_j} \cdot 1 \\ &= 0 \end{aligned}$$

(ii) $\Rightarrow$ (iii): Sei $z := x - y \perp U,\ \widetilde{y} \in U$.

$$\begin{aligned} \Rightarrow\ \|x - \widetilde{y}\|_2^2 &= \|\underbrace{x - y}_{\perp U} + \underbrace{y - \widetilde{y}}_{\in U}\|_2^2 \\ &= \|x - y\|_2^2 + \|y - \widetilde{y}\|_2^2 \\ &\geq \|x - y\|_2^2 \end{aligned}$$

(iii) $\Rightarrow$ (i): Fall $x \in U$: Dann $y = x = \sum_{j=1}^{k} \langle x, e_j \rangle \cdot e_j$

Fall $x \notin U$: Sei $\{e_1, \ldots, e_k, e_{k+1}\}$ ONB von $\mathrm{LH}\{e_1, \ldots, e_k, x\}$. Es gilt

$$x = \sum_{j=1}^{k+1} \langle x, e_j \rangle \cdot e_j, \quad y = \sum_{j=1}^{k+1} \lambda_j \cdot e_j \text{ mit } \lambda_{k+1} = 0.$$

$$\begin{aligned} \Rightarrow\ \|x - y\|_2^2 &= \left\| \sum_{j=1}^{k+1} (\langle x, e_j \rangle - \lambda_j) \cdot e_j \right\|_2^2 \\ &= \sum_{j=1}^{k+1} \big| \langle x, e_j \rangle - \lambda_j \big|^2 \\ &= \text{Minimum, falls } \lambda_j = \langle x, e_j \rangle \text{ für } 1 \leq j \leq k \end{aligned}$$

$\square$

3.74 Bemerkung: Aus dem Satz: Für $x \in V\ \exists!\, y \in U : \|x - y\|_2$ ist minimal. Es gilt

$$y = \sum_{j=1}^{k} \langle x, e_j \rangle \cdot e_j.$$

Die Abbildung $P : V \to U : x \mapsto \sum_{j=1}^{k} \langle x, e_j \rangle \cdot e_j$ ist linear und heißt **orthogonale Projektion** von V auf U.

3.10 Die adjungierte Matrix

3.75 Definition: Sei

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

eine $m \times n$-Matrix. Dann heißt die $n \times m$-Matrix

$$A^* := \begin{pmatrix} \overline{a_{11}} & \dots & \overline{a_{m1}} \\ \vdots & & \vdots \\ \overline{a_{1n}} & \dots & \overline{a_{mn}} \end{pmatrix}$$

die **adjungierte Matrix** zu A und die $n \times m$-Matrix

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

die **transponierter Matrix** von A. Im Fall $\mathbb{K} = \mathbb{R}$ gilt $A^* = A^T$.

3.76 Definition: Eine $n \times n$-Matrix A heißt

1) **selbstadjungiert**, falls $A^* = A$,

2) **symmetrisch**, falls $A^T = A$,

3) **unitär**, falls $A^* = A^{-1}$. Im Fall $\mathbb{K} = \mathbb{R}$ heißt A dann auch **orthogonal** $(A^T = A^{-1})$.

3.77 Satz: Seien B, C zwei ONB's von V. Dann ist $M_{\text{Id}}^{C,B}$ unitär, d.h. die inverse Matrix ist besonders einfach zu berechnen: $M_{\text{Id}}^{B,C} = \left(M_{\text{Id}}^{C,B}\right)^*$.

Beweis: Für $V = \mathbb{C}^n$ und $C = E =$ kanonische Basis. Sei $B = \{b_1, \dots, b_n\}$.

$$M_{\text{Id}}^{E,B} = \begin{pmatrix} (b_1)_1 & \dots & (b_n)_1 \\ \vdots & & \vdots \\ \underbrace{(b_1)_n}_{\substack{\text{Koord.}\\ \text{von } b_1\\ \text{bzgl. } E}} & & \underbrace{(b_n)_n}_{\substack{\text{Koord.}\\ \text{von } b_n\\ \text{bzgl. } E}} \end{pmatrix} = \big((b_1)_E, \dots, (b_n)_E\big)$$

$$\begin{aligned}
\Rightarrow \left(M_{\mathrm{Id}}^{E,B}\right)^* \cdot M_{\mathrm{Id}}^{E,B} &= \begin{pmatrix} (b_1)_E^* \\ \vdots \\ (b_n)_E^* \end{pmatrix} \cdot \begin{pmatrix} (b_1)_E & \dots & (b_n)_E \end{pmatrix} \\
&= \begin{pmatrix} \langle b_1, b_1\rangle & \langle b_1, b_2\rangle & \dots & \langle b_1, b_n\rangle \\ \langle b_2, b_1\rangle & & & \\ \vdots & & & \\ \langle b_n, b_1\rangle & \dots & \dots & \langle b_n, b_n\rangle \end{pmatrix} \\
&= E \quad \text{(Einheitsmatrix)}
\end{aligned}$$

□

3.78 Satz: Seien $\langle .\,,.\rangle_{\mathbb{K}^n}$, $\langle .\,,.\rangle_{\mathbb{K}^m}$ die Standard-Skalarprodukte in $\mathbb{K}^n$ bzw. $\mathbb{K}^m$, und sei A eine $m \times n$-Matrix. Für $x \in \mathbb{K}^n$, $y \in \mathbb{K}^m$ gilt

$$\langle A\,x, y\rangle_{\mathbb{K}^m} \;=\; \langle x, A^*\,y\rangle_{\mathbb{K}^n}\,.$$

Beweis: j-te Koordinate von Ax: $(Ax)_j = \sum_{k=1}^{n} a_{jk}\,x_k$

$$\Rightarrow \langle Ax, y\rangle_{\mathbb{K}^m} \;=\; \sum_{j=1}^{m}\left(\sum_{k=1}^{n} a_{jk}\,x_k\right)\overline{y_j}.$$

Genauso

$$\begin{aligned}
\langle x, A^*\,y\rangle_{\mathbb{K}^n} &= \sum_{k=1}^{n} x_k\overline{(A^*\,y)_k} \\
&= \sum_{k=1}^{n} x_k\overline{\left(\sum_{j=1}^{m}\overline{a_{jk}}\,y_j\right)} \\
&= \sum_{j=1}^{m}\sum_{k=1}^{n}\overline{\overline{a_{jk}}}\,x_k\,\overline{y_j} \\
&= \langle A\,x, y\rangle_{\mathbb{K}^m}
\end{aligned}$$

□

3.79 Folgerungen: **1)** Ist A selbstadjungierte $n \times n$-Matrix, so gilt für $x, y \in \mathbb{K}^n$:

$$\langle A\,x, y\rangle \;=\; \langle x, A\,y\rangle\,.$$

2) Ist A unitär, so gilt für $x, y \in \mathbb{K}^n$

$$\langle A\,x, A\,y\rangle \;=\; \langle x, y\rangle\,.$$

Insbesondere gilt $\|Ax\|_2 = \sqrt{\langle A\,x, A\,x\rangle} = \|x\|_2$. Eine unitäre Matrix erhält Längen und Winkel.

3.11 Die adjungierte Abbildung

3.80 Satz und Definition: Sei $L : V \to W$. Dann existiert genau eine lineare Abbildung $L^* : W \to V$, so dass

$$\forall v \in V \ \ \forall w \in W : \langle L\, v, w \rangle_W = \langle v, L^*\, w \rangle_V \, .$$

L^* heißt die **adjungierte Abbildung** zu L.
Ist $B = \{b_1, \ldots, b_n\}$ ONB von V und $C = \{c_1, \ldots, c_m\}$ ONB von W, so gilt

$$M_{L^*}^{B,C} \ = \ \left(M_L^{C,B} \right)^*,$$

d.h. zur adjungierten Abbildung gehört die adjungierte Matrix.

Beweis: **Existenz:** Sei $(Lv)_C = M_L^{C,B}(v)_B$. Offensichtlich ist $M_L^{C,B}$ eine $m \times n$-Matrix und $\left(M_L^{C,B}\right)^*$ eine $n \times m$-Matrix. Definiere

$$L^* : W \to V : (L^*w)_B := \left(M_L^{C,B} \right)^* (w)_C.$$

Dann gilt $M_{L^*}^{B,C} = \left(M_L^{C,B}\right)^*$ und

$$\begin{aligned}
\langle v, L^*w \rangle &= \langle (v)_B, (L^*w)_B \rangle_{\mathbb{K}^n} \\
&= \left\langle (v)_B, \left(M_L^{C,B} \right)^* (w)_C \right\rangle_{\mathbb{K}^n} \\
&= \left\langle M_L^{C,B} (v)_B, (w)_C \right\rangle_{\mathbb{K}^m} \\
&= \langle (Lv)_C, (w)_C \rangle_{\mathbb{K}^m} \\
&= \langle Lv, w \rangle_W
\end{aligned}$$

Eindeutigkeit: Sei $K : W \to V$ mit $\langle Lv, w \rangle = \langle v, Kw \rangle_V$

$$\begin{aligned}
&\Rightarrow \ \langle Kw - L^*w, v \rangle \ = \ \langle w, Lv \rangle - \langle w, Lv \rangle \ = \ 0 \quad \forall v \in V \\
&\Rightarrow \ Kw - L^*w = 0.
\end{aligned}$$

□

3.81 Eigenschaften der Adjungierten: Es sei $L : V \to W$, $K : W \to U$. Dann gelten

1) $(L^*)^* = L$.

2) $(K \circ L)^* = L^* \circ K^*$ (Reihenfolge dreht sich um!).

3) $\operatorname{Kern}(L) = (\operatorname{Bild}(L^*))^\perp := \left\{ x \in W : \langle x, y \rangle = 0 \ \forall y \in \operatorname{Bild}(L^*) \right\}$.

4) Falls $L : V \to V$, gilt $\operatorname{Rang}(L) = \operatorname{Rang}(L^*)$.

Beweis: **1)** Für $x \in V,\ y \in W$ gilt

$$\langle x, (L^*)^* y\rangle \;=\; \langle L^* x, y\rangle \;=\; \langle x, Ly\rangle \;\Rightarrow\; (L^*)^* y = Ly.$$

2) $\langle (K \circ L)x, y\rangle \;=\; \langle K(L(x)), y\rangle \;=\; \langle Lx, K^* y\rangle \;=\; \langle x, L^*(K^* y)\rangle \;=\; \langle x, L^* \circ K^* y\rangle.$

3)
$$\begin{aligned} x \in \text{Kern}\,(L) \;&\Leftrightarrow\; Lx = 0 \\ &\Leftrightarrow\; \forall y \in W : \langle Lx, y\rangle = 0 \\ &\Leftrightarrow\; \forall y \in W : \langle x, L^* y\rangle = 0 \\ &\Leftrightarrow\; x \in (\text{Bild}\,(L^*))^\perp \end{aligned}$$

4) Dimensionsformel: $\dim V = \dim\ \text{Kern}\,(L) + \dim\ \text{Bild}\,(L)$.

$$\begin{aligned} \Rightarrow \text{Rang}\,(L) \;&=\; \dim\ \text{Bild}\,(L) \;=\; \dim(V) - \dim\ \text{Kern}\,(L) \\ &=\; \dim(V) - \dim\big(\text{Bild}\,(L^*)^\perp\big) \\ &=\; \dim(V) - \big(\dim(V) - \dim\ \text{Bild}\,(L^*)\big) \\ &=\; \dim\ \text{Bild}\,(L^*) \;=\; \text{Rang}\,(L^*). \end{aligned}$$

□

3.82 Definition: Eine Abbildung $L : V \to V$ heißt

1) **normal**, falls $L \circ L^* = L^* \circ L$.

2) **unitär**, falls $L^* = L^{-1}$. Ist L unitär und gilt $\mathbb{K} = \mathbb{R}$, so heißt L auch **orthogonal**.

3) **selbstadjungiert**, falls $L^* = L$. Ist L selbstadjungiert und gilt $\mathbb{K} = \mathbb{R}$, so heißt L auch **symmetrisch**.

3.83 Eigenschaften unitärer Abbildungen: Für $L : V \to V$ linear sind äquivalent:

(i) L ist unitär.

(ii) $\forall u, v \in V : \langle L\,u, L\,v\rangle = \langle u, v\rangle$. Insbesondere ist L längen- und winkelerhaltend.

(iii) L ist **isometrisch**, d.h $\forall u \in V : \|L\,u\|_2 = \|u\|_2$.

(iv) L transformiert ONBen in ONBen.

(v) Es existiert eine ONB B, so dass die Spalten von $M_L^{B,B}$ eine ONB bilden.

(vi) Für jede ONB B bilden die Spalten von $M_L^{B,B}$ eine ONB.

3.12 Determinanten

3.84 Definition: Seien $x, y \in \mathbb{R}^2$. Die **orientierte Fläche** des von x, y aufgespannten Parallelogramms ist definiert durch

$$F(x,y) \;:=\; x_1\, y_2 - x_2\, y_1 \;=\; \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$$

3.85 Folgerung: Die orientierte Fläche besitzt folgende Eigenschaften:

1) $F(x,y) = 0 \;\Leftrightarrow\; \{x, y\}$ ist linear abhängig.

2) $F(e_1, e_2) = 1$.

3) $F(\lambda \cdot x, y) = \lambda\, F(x,y)$, $F(x, \lambda \cdot y) = \lambda\, F(x,y)$, $F(\lambda \cdot x, \lambda \cdot y) = \lambda^2\, F(x,y)$.

4) $F(x+z, y) = F(x,y) + F(z,y)$, $F(x, y+z) = F(x,y) + F(x,z)$.

5) $F(y,x) = -F(x,y)$.

3.86 Definition: Seien $x, y, z \in \mathbb{R}^3$. Dann heißt

$$\begin{aligned} V(x,y,z) \;&:=\; x_1\, y_2\, z_3 + y_1\, z_2\, x_3 + z_1\, x_2\, y_3 - z_1\, y_2\, x_3 - x_1\, z_z\, y_3 - y_1\, x_2\, z_3 \\ &=\; \left|\begin{array}{ccc|cc} x_1 & y_1 & z_1 & x_1 & y_1 \\ x_2 & y_2 & z_2 & x_2 & y_2 \\ x_3 & y_3 & z_3 & x_3 & y_3 \end{array}\right. \end{aligned}$$

das **orientierte Volumen** des von x, y, z aufgespannten Parallelepipeds.

3.87 Definition: Es sei $M_{n,n}(\mathbb{K})$ die Menge der $n \times n$-Matrizen mit Elementen in $\mathbb{K}$. Eine Abbildung $\det : M_{n,n}(\mathbb{K}) \to \mathbb{K} : A \mapsto \det(A) =: |A|$ heißt **Determinante**, falls sie folgende Eigenschaften besitzt: Ist

$$A \;=\; \begin{pmatrix} a_1 & \ldots & a_n \end{pmatrix} \qquad \text{mit Spaltenvektoren } a_j \in \mathbb{K}^n,$$

so gelten:

(D1) $\det(E_n) = 1$.

(D2) Für jedes $k \in \{1, \ldots, n\}$ gilt:

$$\begin{aligned}&\det\big(a_1 \ldots a_{k-1}\ (\alpha \cdot a_k + \beta \cdot b)\ a_{k+1} \ldots a_n\big) = \\ &= \alpha \det(a_1 \ldots a_{k-1}\ a_k\ a_{k+1} \ldots a_n\big) + \beta \det(a_1 \ldots a_{k-1}\ b\ a_{k+1} \ldots a_n\big).\end{aligned}$$

D.h. die Abbildung det ist in jedem Argument linear.

(D3) Für alle Paare (k, j) mit $k \neq j$ gilt:

$$\det(a_1 \ldots a_k \ldots a_j \ldots a_n\big) = (-1) \det(a_1 \ldots a_j \ldots a_k \ldots a_n\big),$$

d.h. Vertauschung zweier Spalten ändert das Vorzeichen.

3.88 Bemerkung: Man kann beweisen, dass es genau eine Determinante $\det : M_{n,n}(\mathbb{K}) \to \mathbb{K}$ mit diesen Eigenschaften gibt.

3.89 Satz: Es sei A eine $n \times n$-Matrix. Für die Determinante gelten:

1) Verschwindet eine Spalte: $a_k = 0$ für ein k, so gilt $\det(A) = 0$.

2) Enthält A zwei gleiche Spalten: $a_k = a_j$ für ein Paar (k, j) mit $k \neq j$, so gilt $\det(A) = 0$.

3) $\det \begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & a_{nn} \end{pmatrix} = a_{11}\, a_{22} \cdots a_{nn}.$

4) Addition des Vielfachen einer Spalte zu einer anderen ändert nicht den Wert der Determinante.

3.90 Satz: Es sei $A = (a_1 \ldots a_n)$ eine $n \times n$-Matrix mit den Spaltenvektoren a_j. Dann gilt:

$$\{a_1, \ldots, a_n\} \text{ ist linear abhängig } \Leftrightarrow \det(A) = 0.$$

Oder anders ausgedrückt: Es gilt

$$\operatorname{Rang}(A) < n \;\Leftrightarrow\; \det(A) = 0 \quad \text{bzw.} \quad \operatorname{Rang}(A) = n \;\Leftrightarrow\; \det(A) \neq 0.$$

Beweis: „$\Rightarrow$": Es sei $\lambda_1 \cdot a_1 + \ldots + \lambda_n \cdot a_n = 0$. OBdA $\lambda_1 \neq 0 \;\Rightarrow\; a_1 + \frac{\lambda_2}{\lambda_1} \cdot a_2 + \ldots + \frac{\lambda_n}{\lambda_1} \cdot a_n = 0$

$$\Rightarrow\; \det(A) = \det\left(\underbrace{\left(a_1 + \frac{\lambda_2}{\lambda_1} \cdot a_2 + \ldots + \frac{\lambda_n}{\lambda_1} \cdot a_n\right)}_{=0} \; a_2 \; \ldots \; a_n \right) = 0$$

„$\Leftarrow$": Kontraposition: Zeige $\{a_1, \ldots, a_n\}$ linear unabhängig $\Rightarrow\; \det(A) = 0$.

Sei $\{a_1, \ldots, a_n\}$ linear unabhängig

$$\begin{aligned}
\Rightarrow \quad e_1 &= \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \lambda_1 \cdot a_1 + \ldots + \lambda_n \cdot a_n \quad \text{wobei } \exists k_1 : \lambda_{k_1} \neq 0 \\
\Rightarrow \quad \frac{1}{\lambda_{k_1}} \cdot e_1 &= \frac{\lambda_1}{\lambda_{k_1}} \cdot a_1 + \ldots + a_{k_1} + \ldots + \frac{\lambda_n}{\lambda_{k_1}} \cdot a_n \\
\Rightarrow \quad \det(A) &= \det\left(a_1 \; \ldots \; a_{k_1-1} \; \left(\frac{\lambda_1}{\lambda_{k_1}} \cdot a_1 + \ldots + a_{k_1} + \ldots + \frac{\lambda_n}{\lambda_{k_1}} \cdot a_n \right) \; a_{k_1+1} \; \ldots \; a_n \right) \\
&= \pm \frac{1}{\lambda_{k_1}} \det\left(e_1 \; a_1 \; a_{k_1-1} \; a_{k_1+1} \; \ldots \; a_n\right) \\
&\;\vdots \\
&= \pm \frac{1}{\lambda_{k_1}} \cdot \frac{1}{\lambda_{k_2}} \cdots \frac{1}{\lambda_{k_n}} \det(e_1 \; \ldots \; e_n) \\
&\neq 0
\end{aligned}$$

$\square$

3.91 Lineare Gleichungssysteme: Es sei A eine $n \times n$-Matrix. Dann gelten:

1) Das LGS $A\,x = 0$ besitzt nichttriviale Lösungen genau dann, wenn $\det(A) = 0$.

2) Das LGS $A\,x = b$ ist für jedes $b \in \mathbb{K}^n$ eindeutig lösbar genau dann, wenn $\det(A) \neq 0$.

Beweis: **1)** $\det(A) = 0 \;\Leftrightarrow\; \operatorname{Rang}(A) < n \;\Leftrightarrow\;$ LGS $Ax = 0$ besitzt mehr als eine Lösung.

2) $\det(A) \neq 0 \;\Leftrightarrow\; \operatorname{Rang}(A) = n \;\Leftrightarrow\;$ LGS $Ax = b$ ist für jedes $b \in \mathbb{K}^n$ eindeutig lösbar. $\square$

3.92 Rechenregeln: **1)** $\det(A \cdot B) = \big(\det(A)\big)\det(B)$.

2) Falls A invertierbar ist: $\det(A^{-1}) = \dfrac{1}{\det(A)}$.

3) $\det(A^T) = \det(A)$.
Insbesondere: Addition des Vielfachen einer Spalte zu einer anderen ändert nicht den Wert der Determinante.

3.93 Laplace-Entwicklung: Für $A = (\alpha_{ij}) \in M_{n,n}$ setze

$$A_{ij} \;:=\; \begin{pmatrix} & \alpha_{1j} & \\ \alpha_{i1} & & \alpha_{in} \\ & \alpha_{nj} & \end{pmatrix} \;\in\; M_{n-1,n-1}$$

(Streichen der i-ten Zeile und j-ten Spalte in A).

Für jedes $i \in \{1, \ldots, n\}$ gilt

$$\det A \;=\; \sum_{j=1}^{n} (-1)^{i+j} \alpha_{ij} \, \det A_{ij}$$

(Entwicklung nach i-ter Zeile), und für jedes $j \in \{1, \ldots, n\}$ gilt

$$\det A \;=\; \sum_{i=1}^{n} (-1)^{i+j} \alpha_{ij} \, \det A_{ij}$$

(Entwicklung nach j-ter Spalte).

3.94 Geometrische Bedeutung: **1)** Für $v_1, \ldots, v_n \in \mathbb{R}^n$ ist

$$V(v_1, \ldots, v_n) \;:=\; \det \begin{pmatrix} v_1 & \ldots & v_n \end{pmatrix}$$

das orientierte Volumen des von den Vektoren $v_1, \ldots, v_n$ aufgespannten Parallelepipeds.

2) Sei A eine reelle $n \times n$-Matrix. Betrachte $L : \mathbb{R}^n \to \mathbb{R}^n : x \mapsto A\,x$. Sind $v_1, \ldots, v_n \in \mathbb{R}^n$, so gilt

$$V(L\,v_1, \ldots, L\,v_n) \;=\; \det(A)\, V(v_1, \ldots, v_n),$$

d.h. $\det(A)$ gibt an, wie sich das Volumen unter der Abbildung L verändert.

3.95 Definition: Sei $L : V \to V$ linear und B Basis von V. Dann ist die **Determinante** von L definiert durch

$$|L| \;:=\; \det(L) \;:=\; \left| M_L^{B,B} \right|.$$

3.96 Bemerkung: Sind B, B' Basen von V und ist $L : V \to V$ linear, so gilt

$$\left| M_L^{B,B} \right| \;=\; \left| M_L^{B',B'} \right|.$$

Beweis: Sei $M_{\mathrm{Id}}^{B',B}$ die Basiswechselmatrix. Dann gilt:

$$\begin{aligned} \left| M_L^{B',B'} \right| &= \left| M_{\mathrm{Id}}^{B',B} \cdot M_L^{B,B} \cdot M_{\mathrm{Id}}^{B,B'} \right| \\ &= \underbrace{\left| M_{\mathrm{Id}}^{B',B} \right|}_{=\left(M_{\mathrm{Id}}^{B,B'}\right)^{-1}} \cdot \left| M_L^{B,B} \right| \cdot \left| M_{\mathrm{Id}}^{B,B'} \right| \\ &= \frac{1}{\left| M_{\mathrm{Id}}^{B,B'} \right|} \cdot \left| M_L^{B,B} \right| \cdot \left| M_{\mathrm{Id}}^{B,B'} \right| \end{aligned}$$

$\square$

3.13 Diagonalisierung

3.97 Definition: Sei $L : V \to V$ linear.

1) $\lambda \in \mathbb{K}$ heißt **Eigenwert** (EW) von L, falls ein $v \in V$ mit $v \neq 0$ existiert, so dass $L\,v = \lambda{\cdot}v$. Der Vektor v heißt dann **Eigenvektor** (EV) zum Eigenwert λ (*englisch: eigenvalue, eigenvector*).

2) Die Menge $\sigma(L) := \big\{\lambda \in \mathbb{K} : \lambda \text{ ist EW von } L\big\}$ heißt **Spektrum** von L.

3.98 Satz: Sei $L : V \to V$ linear, $B = \{b_1, \ldots, b_n\}$ Basis von V. Äquivalent sind:

(i) B besteht nur aus Eigenvektoren.

(ii) Die Matrix $M_L^{B,B}$ hat **Diagonalgestalt**, d.h.

$$M_L^{B,B} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Sind (i) und (ii) erfüllt, so ist b_j Eigenvektor zum Eigenwert λ_j: $L(b_j) = \lambda_j \cdot b_j$, und es gilt

$$\begin{aligned} M_{L^k}^{B,B} &= \begin{pmatrix} \lambda_1^k & & 0 \\ & \ddots & \\ 0 & & \lambda_n^k \end{pmatrix} \\ M_{L^{-1}}^{B,B} &= \begin{pmatrix} \lambda_1^{-1} & & 0 \\ & \ddots & \\ 0 & & \lambda_n^{-1} \end{pmatrix} \quad \text{(falls } L \text{ invertierbar)} \\ \det(L) &= \lambda_1 \cdots \lambda_n \end{aligned}$$

Beweis: (i) $\Leftrightarrow$ $\forall j = 1, \ldots, n\ \exists \lambda_j \in \mathbb{K} : Lb_j = \lambda_j \cdot b_j \ \Leftrightarrow\ M_L^{B,B} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ $\square$

3.99 Definition: L heißt **diagonalisierbar**, falls es eine Basis von V aus Eigenvektoren von L gibt.

3.100 Satz: Es sei $L : V \to V$ linear. Dann sind für $\lambda \in \mathbb{K}$ äquivalent:

(i) λ ist Eigenwert von L,

(ii) $\det(L - \lambda \cdot \mathrm{Id}) = 0$.

Beweis: Sei B Basis von V. Dann:

$$\begin{aligned}
\text{(i)} \quad &\Leftrightarrow \quad \exists v \in V \setminus \{0\} : Lv = \lambda \cdot v \\
&\Leftrightarrow \quad \exists v \in V \setminus \{0\} : M_L^{B,B}(v)_B = \lambda \cdot (v)_B \\
&\Leftrightarrow \quad \text{Das LGS } \left(M_L^{B,B} - \lambda \cdot E\right)(v)_B = 0 \text{ hat nichttriviale Lösungen} \\
&\Leftrightarrow \quad \det\left(M_L^{B,B} - \lambda \cdot E\right) = 0 \\
&\Leftrightarrow \quad \det(L - \lambda \cdot \mathrm{Id}) = 0
\end{aligned}$$

□

3.101 Satz und Definition: Sei $L : V \to V$ linear, $\dim(V) = n$.

1) $p_L : \mathbb{K} \ni \lambda \mapsto p_L(\lambda) := \det(L - \lambda \cdot \mathrm{Id})$ ist Polynom n-ten Grades in λ. p_L heißt **charakteristisches Polynom** von L.

2) Ist $A = M_L^{B,B}$ bezüglich einer Basis B von V, so ist

$$p_L(\lambda) \;=\; \det(A - \lambda \cdot E)$$

und hängt nicht von B ab.

3) Es gilt $p_L(\lambda) = (-1)^n \lambda^n + (-1)^{n-1}(\alpha_{11} + \ldots + \alpha_{nn})\lambda^{n-1} + \ldots + \det A$.
Die Summe der Diagonalelemente von A hängt also nicht von der Basis B ab und heißt **Spur** von L (oder auch Spur von A).
Schreibweise: $\mathrm{Sp}(L)$ oder $\mathrm{tr}(L)$ (trace) bzw. $\mathrm{Sp}(A)$ oder $\mathrm{tr}(A)$.

3.102 Folgerung: Für eine lineare Abbildung $L : V \to V$ gelten:

1) $\lambda \in \mathbb{K}$ ist Eigenwert von $L \quad \Leftrightarrow \quad p_L(\lambda) = 0$.

2) Falls $\mathbb{K} = \mathbb{C}$ besitzt L mindestens einen Eigenwert.

3) L hat höchstens n verschiedene Eigenwerte.

3.103 Definition: Sei λ Eigenwert von L. Dann heißt

$n_g(\lambda) := \dim\{v \in V : L\,v = \lambda \cdot v\}$ die **geometrische Vielfachheit** von λ.
$n_a(\lambda) :=$ Ordnung der Nullstelle λ von p_L die **algebraische Vielfachheit** von λ.

3.104 Satz: Sei λ Eigenwert von L. Dann gilt $n_g(\lambda) \leq n_a(\lambda)$.

Beweis: Wir bezeichnen den Eigenwert mit λ_0. Sei $\{b_1, \ldots, b_k\}$ eine Basis des Eigenraumes $\{v \in V : Lv = \lambda_0 \cdot v\}$ (also $k = n_g(\lambda_0)$). Ergänze zu einer Basis $B = \{b_1, \ldots, b_n\}$ von V.

$$\Rightarrow \; M_L^{B,B} \;=\; \begin{pmatrix} \lambda_0 & 0 & \ldots & 0 & * \\ 0 & \lambda_0 & \ddots & \vdots & \\ \vdots & \ddots & \ddots & 0 & \\ 0 & \ldots & 0 & \lambda_0 & * \\ 0 & \ldots & 0 & 0 & \\ \vdots & & \vdots & \vdots & A \\ 0 & \ldots & 0 & 0 & \end{pmatrix}$$

$$\begin{aligned} \Rightarrow \; p_L(\lambda) &= \det(M_L^{B,B} - \lambda \cdot E) \;=\; \det \begin{pmatrix} \lambda_0 - \lambda & & 0 & * \\ & \ddots & & \\ 0 & & \lambda_0 - \lambda & * \\ 0 & \ldots & 0 & A - \lambda \cdot E \end{pmatrix} \\ &= (\lambda_0 - \lambda)^k \det(A - \lambda \cdot E) \end{aligned}$$

$\Rightarrow$ $\lambda = \lambda_0$ ist mindestens k-fache Nullstelle von p_l, also $n_a(\lambda_0) \geq k = n_g(\lambda_0)$. □

3.105 Satz: Sind $\lambda_1, \ldots, \lambda_k \in \mathbb{K}$ paarweise verschiedene Eigenwerte von L mit Eigenvektoren $v_1, \ldots, v_k$, so ist $\{v_1, \ldots, v_k\}$ linear unabhängig (Eigenvektoren zu verschiedenen Eigenwerten sind linear unabhängig).

Beweis: Induktion nach k:

Induktionsanfang $k = 1$: $\{v_1\}$ ist linear unabhängig, da $v_1 \neq 0$.

Induktionsschritt: Sei $\alpha_1 \cdot v_1 + \ldots + \alpha_{k+1} \cdot v_k = 0$.

$$\begin{aligned} \Rightarrow \; 0 &= (L - \lambda_{k+1} \cdot \mathrm{Id})(\alpha_1 \cdot v_1 + \ldots + \alpha_{k+1} \cdot v_k) \\ &= \alpha_1(\lambda_1 - \lambda_{k+1}) \cdot v_1 + \ldots + \alpha_k(\lambda_k - \lambda_{k+1}) \cdot v_k + 0 \\ \Rightarrow \; & \alpha_1 = \ldots = \alpha_k = 0 \\ \Rightarrow \; & \alpha_{k+1} = 0 \end{aligned}$$

□

3.106 Hauptsatz: Für eine lineare Abbildung $L : V \to V$ sind äquivalent

(i) L ist diagonalisierbar.

(ii) p_L zerfällt über $\mathbb{K}$ in Linearfaktoren (hat also n nicht notwendig verschiedene Nullstellen = Eigenwerte in $\mathbb{K}$):

$$p(\lambda) \;=\; (\lambda - \lambda_1)(\lambda - \lambda_2) \cdots (\lambda - \lambda_n),$$

und für jede Nullstelle gilt geometrische = algebraische Vielfachheit.

Beweis: Sei $n := \dim V$.

(i) $\Rightarrow$ (ii):

$$\begin{aligned}
\text{(i)} \quad &\Leftrightarrow \quad V \text{ besitzt Basis aus EVen } B = \{b_1, \ldots, b_n\} \\
&\Leftrightarrow \quad M_L^{B,B} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \\
&\Rightarrow \quad p_L(\lambda) = \det(M_L^{B,B} - \lambda \cdot E) = (\lambda_1 - \lambda) \cdots (\lambda_n - \lambda)
\end{aligned}$$

Da zu jedem λ_j ein Eigenvektor b_j aus der Basis gehört, gilt $n_g(\lambda_j) \geq n_a(\lambda_j)$. Mit Satz 3.104 folgt $n_g(\lambda_j) = n_a(\lambda_j)$.

(ii) $\Rightarrow$ (i):

Seien $\lambda_1, \ldots, \lambda_k$ die paarweise verschiedenen Nullstellen von p_L. Da das Polynom in Linearfaktoren zerfällt, gilt

$$\sum_{j=1}^{k} n_a(\lambda_j) = n.$$

Wegen der Bedingung $n_a(\lambda_j) = n_g(\lambda_j)$ folgt

$$\sum_{j=1}^{k} n_g(\lambda_j) = n.$$

Sind $B_1, \ldots, B_k$ Basen der Eigenräume zu $\lambda_1, \ldots, \lambda_k$, so folgt aus Satz 3.105, dass $B := B_1 \cup \ldots \cup B_k$ linear unabhängig ist. Wegen

$$\sharp B = \sum_{j=1}^{k} n_g(\lambda_j) = n = \dim V$$

ist B dann eine Basis von V.

$\square$

3.14 Sesquilineare Abbildungen

3.107 Definition: Sei V ein Vektorraum über $\mathbb{K}$. Eine Abbildung $b : V \times V \to \mathbb{K}$ mit

$$\begin{aligned}
b(\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2, w) &= \lambda_1\, b(v_1, w) + \lambda_2\, b(v_2, w), \\
b(w, v) &= \overline{b(v, w)} \\
\Big(\text{Dann gilt auch } b(v, \lambda_1 \cdot w_1 + \lambda_2 \cdot w_2) &= \overline{\lambda_1}\, b(v, w_1) + \overline{\lambda_2}\, b(v, w_2) \\
\text{und } b(v, 0) &= 0 = b(0, w)\Big)
\end{aligned}$$

heißt **Sesquilinearform** auf V. Falls $\mathbb{K} = \mathbb{R}$, heißt b auch **Bilinearform**.

3.108 Satz: Sei V Vektorraum mit Skalarprodukt, $E = \{e_1, \ldots, e_n\}$ Orthonormalbasis von V, b eine Sesquilinearform auf V. Dann existiert eine selbstadjungierte Matrix $M_b^E \in M_{n,n}(\mathbb{K})$, so dass

$$b(v,w) \;=\; \left\langle M_b^E\,(v)_E, (w)_E \right\rangle_{\mathbb{K}^n} .$$

Falls $\mathbb{K} = \mathbb{R}$, ist M_b^E symmetrisch.

Beweis: Sei $M_b^E := (\alpha_{jk})$ mit $\alpha_{jk} := b(e_k, e_j)$.

$$\Rightarrow\; \alpha_{kj} = b(e_j, e_k) = \overline{b(e_k, e_j)} = \overline{\alpha_{jk}}, \quad \text{also } \left(M_b^E\right)^* = M_b^E$$

Außerdem:

$$\begin{aligned}
b(v,w) &= b\left(\sum_{j=1}^n \underbrace{\langle v, e_j\rangle}_{=v_k} \cdot e_j, \sum_{k=1}^n \underbrace{\langle w, e_k\rangle}_{=w_k \text{ (k-te Koordinate von $(w)_E$)}} \cdot e_k\right) \\
&= \sum_{j=1}^n \sum_{k=1}^n v_j \overline{w_k}\, b(e_j, e_k) \\
&= \sum_{k=1}^n \left(\sum_{j=1}^n \alpha_{kj}\, v_j\right) \overline{w_k} \\
&= \left\langle M_b^E (v)_E, (w)_E \right\rangle_{\mathbb{K}^n}
\end{aligned}$$

□

3.109 Bemerkung: Durch $b \mapsto M_b^E$ wird eine bijektive Abbildung von der Menge aller Sesquilinearformen auf V auf die Menge aller selbstadjungierten $n \times n$-Matrizen in $\mathbb{K}$ definiert. Dies entspricht dem Vorgehen bei linearen Abbildungen: Durch $L \mapsto M_L^{B',B}$ wird eine bijektive Abbildung von der Menge alle linearen Abbildungen $L : V \to W$ auf die Menge aller $m \times n$-Matrizen definiert.

3.110 Satz: Zusätzlich zum letzten Satz sei E' eine weitere Orthonormalbasis von V und $S := M_{\mathrm{Id}}^{E,E'}$ die Basiswechselmatrix von E' zu E. Dann gilt

$$M_b^{E'} \;=\; S^* \cdot M_b^E \cdot S \;=\; S^{-1} \cdot M_b^E \cdot S\,.$$

Beweis:

$$\begin{aligned}
b(v,w) &= \left\langle M_b^E (v)_E, (w)_E \right\rangle \\
&= \left\langle M_b^E \cdot M_{\mathrm{Id}}^{E,E'} (v)_{E'}, M_{\mathrm{Id}}^{E,E'} (w)_{E'} \right\rangle \\
&= \left\langle S^* \cdot M_b^E \cdot S (v)_{E'}, (w)_{E'} \right\rangle,
\end{aligned}$$

und $S^* = S^{-1}$, da S unitär ist.

□

3.111 Definition: Sei b eine Sesquilinearform auf V.

1) Die Abbildung

$$q : V \to \mathbb{K} : v \mapsto b(v,v)$$

heißt die zu b gehörige **quadratische Form**.

2) Eine quadratische Form heißt **positiv semidefinit**, falls

$$\forall v \in V : q(v) \;\geq\; 0$$

b heißt **positiv semidefinit**, falls die zugehörige quadratische Form positiv semidefinit ist.
Eine selbstadjungierte $n \times n$-Matrix A heißt **positiv semidefinit**, falls

$$\forall x \in \mathbb{K}^n : \langle A\,x, x\rangle_{\mathbb{K}^n} \;\geq 0.$$

3) Eine Sesquilinearform bzw. die zugehörige quadratische Form heißt **positiv definit**, falls

$$\forall v \in V \setminus \{0\} : b(v,v) \;=\; q(v) \;>\; 0.$$

Eine selbstadjungierte $n \times n$-Matrix A heißt **positiv definit**, falls

$$\forall x \in \mathbb{K}^n \setminus \{0\} : \langle A\,x, x\rangle_{\mathbb{K}^n} \;> 0.$$

Bemerkung: Jede positiv definite Sesquilinearform definiert ein Skalarprodukt.

3.112 Satz: Es sei M eine selbstadjungierte $n \times n$-Matrix in $\mathbb{K}$, und die zugehörige Abbildung $L_M : x \mapsto M\,x$ besitze eine Orthonormalbasis E aus Eigenvektoren.

1) Äquivalent sind: **(i)** M ist positiv semidefinit,
(ii) Für alle Eigenwerte λ von L_M gilt $\lambda \geq 0$.

2) Äquivalent sind: **(i)** M ist positiv definit,
(ii) Für alle Eigenwerte λ von L_M gilt $\lambda > 0$.

Beweis: Sei E' die ONB aus EVen, $S := M_{\mathrm{Id}}^{E,E'}$.

$$\begin{aligned}
\Rightarrow \underbrace{S^*}_{=S^{-1}} \cdot M \cdot S &= M_{\mathrm{Id}}^{E',E} \cdot M_{L_M}^{E,E} \cdot M_{\mathrm{Id}}^{E,E'} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \\
\Rightarrow q(x) &= \langle Mx, x\rangle \\
&= \langle S^* \cdot M \cdot S(x)_{E'}, (x)_{E'}\rangle \\
&= \lambda_1 (x_1')^2 + \ldots \lambda_n (x_n')^2.
\end{aligned}$$

$\square$

3.15 Diagonalisierung mit Orthonormalbasen

3.113 Satz: Sei V Vektorraum mit Skalarprodukt. Ist $L : V \to V$ normal (d.h. $L^* \circ L = L \circ L^*$), so gilt:

$$v \text{ ist Eigenvektor von } L \text{ zum Eigenwert } \lambda \;\Rightarrow\; v \text{ ist Eigenvektor von } L^* \text{ zum Eigenwert } \overline{\lambda}$$

Beweis:
$$\begin{aligned} \left\| \left(L^* - \overline{\lambda} \cdot \mathrm{Id}\right) v \right\|_2^2 &= \left\langle \left(L^* - \overline{\lambda} \cdot \mathrm{Id}\right) v, \left(L^* - \overline{\lambda} \cdot \mathrm{Id}\right) v \right\rangle \\ &= \underbrace{\left\langle L^* v, L^* v \right\rangle}_{=\langle Lv, Lv \rangle} - \underbrace{\left\langle L^* v, \overline{\lambda} \cdot v \right\rangle}_{=\langle \lambda v, Lv \rangle} - \underbrace{\left\langle \overline{\lambda} \cdot v, L^* v \right\rangle}_{=\langle Lv, \lambda \cdot v \rangle} + \underbrace{\left\langle \overline{\lambda} \cdot v, \overline{\lambda} \cdot v \right\rangle}_{=\langle \lambda \cdot v, \lambda \cdot v \rangle} \\ &= \left\langle (L - \lambda \cdot \mathrm{Id})\, v, (L - \lambda \cdot \mathrm{Id})\, v \right\rangle \\ &= 0 \end{aligned}$$

□

3.114 Charakterisierung normaler Abbildungen: Sei V Vektorraum über $\mathbb{C}$ mit Skalarprodukt. Für eine lineare Abbildung $L : V \to V$ sind äquivalent:

(i) L besitzt eine ONB aus Eigenvektoren.

(ii) $L^* \circ L = L \circ L^*$ (d.h. L ist normal).

3.115 Folgerung: Ist L normal, dann gelten:

1) Eigenvektoren zu verschiedenen Eigenwerten sind orthogonal.

2) L ist diagonalisierbar

Beweis: **(i) ⇒ (ii):** Sei B die ONB aus EVen.

$$\begin{aligned} \text{(i)} \;\Rightarrow\; M_L^{B,B} &= \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}, \quad M_{L^*}^{B,B} = \begin{pmatrix} \overline{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \overline{\lambda_n} \end{pmatrix} \\ \Rightarrow\; M_{L \circ L^*}^{B,B} &= M_L^{B,B} \circ M_{L^*}^{B,B} = M_{L^*}^{B,B} \circ M_L^{B,B} \circ = M_{L^* \circ L}^{B,B} \\ \Rightarrow\; L \circ L^* &= L^* \circ L \end{aligned}$$

(ii) ⇒ (i): Vollständige Induktion nach $n = \dim V$:

Induktionsanfang $n = 1$: Klar, jede lineare Abbildung besitzt eine ONB $\{b_1\}$ aus EVen.

Induktionsschritt: Sei $\dim V = n + 1$. Da $\mathbb{K} = \mathbb{C}$, besitzt p_L mindestens eine Nullstelle $\lambda_1 \;\Rightarrow\; \lambda_1$ ist EW. Sei v_1 EV zu λ_1.
Betrachte $W := \{v_1\}^\perp = \{v \in V : \langle v, v_1 \rangle = 0\}$. W ist Unterraum von V mit $\dim W = n$.

(α) Es gilt $L(W) \subseteq W$:

$$w \in M \;\Rightarrow\; \langle Lw, v_1 \rangle = \langle w, L^* v_1 \rangle = \left\langle w, \overline{\lambda_1} v_1 \right\rangle = 0 \;\Rightarrow\; Lw \in W.$$

(β) Es gilt $L^*(W) \subseteq W$: Beweis genauso.

Betrachte nun $\widetilde{L} := L\big|_W : W \to W$. Dann gilt $\widetilde{L}^* = L^*\big|_W$.

$$\Rightarrow\; \widetilde{L}^* \circ \widetilde{L} = L^*\big|_W \circ L\big|_W = L\big|_W \circ L^*\big|_W = \widetilde{L} \circ \widetilde{L}^*.$$

Also ist $\widetilde{L}$ normal.

Induktionsvoraussetzung: Es existiert eine ONB $\{e_1, \ldots, e_n\}$ von W aus EVen von $\widetilde{L}$

$$\Rightarrow\; \{e_1, \ldots, e_n, \frac{v_1}{\|v_1\|}\} \text{ ist ONB aus EVen von } L.$$

$\square$

3.116 Charakterisierung unitärer Abbildungen: Sei V Vektorraum über $\mathbb{C}$ und $L : V \to V$ linear. Dann sind äquivalent:

(i) L ist unitär,

(ii) L ist normal und $\sigma(L) \subseteq \{\lambda \in \mathbb{C} : |\lambda| = 1\}$.

Insbesondere ist jede unitäre Abbildung über $\mathbb{C}$ diagonalisierbar, und alle Eigenwerte liegen auf dem komplexen Kreis um 0 mit Radius 1.

Beweis: **(i) $\Rightarrow$ (ii):** $L^* = L^{-1} \;\Rightarrow\; L$ ist normal, also diagonalisierbar mit ONB.

Sei B ONB aus EVen $\Rightarrow\; M_L^{B,B} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$, $M_{L^*}^{B,B} = \begin{pmatrix} \overline{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \overline{\lambda_n} \end{pmatrix}$.

$$L \circ L^* = \mathrm{Id} \;\Rightarrow\; \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \cdot \begin{pmatrix} \overline{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \overline{\lambda_n} \end{pmatrix} = \mathrm{E}.$$

$\Rightarrow\; |\lambda_1|^2 = \ldots = |\lambda_n|^2 = 1.$

(ii) $\Rightarrow$ (i): L ist normal, also diagonalisierbar mit ONB. Sei B ONB aus EVen

$$\Rightarrow\; M_L^{B,B} \cdot M_{L^*}^{B,B} = \begin{pmatrix} |\lambda_1|^2 & & 0 \\ & \ddots & \\ 0 & & |\lambda_n|^2 \end{pmatrix} = \mathrm{E} = M_{\mathrm{Id}}^{B,B}.$$

$\square$

3.117 Satz und Definition: **1)** Die unitäre Gruppe

$$U(n) \ := \ \{L : \mathbb{C}^n \to \mathbb{C}^n \mid L \text{ ist unitär}\}$$

ist eine **Untergruppe** der linearen Gruppe $(\mathrm{GL}_n(\mathbb{C}), \circ)$, d.h. dass $U(n) \subseteq \mathrm{GL}_n(\mathbb{C})$ gilt und $(U(n), \circ)$ eine Gruppe ist.

2) Die lineare Gruppe $\mathrm{GL}_n(\mathbb{R})$ enthält folgende Untergruppen:

- Die orthogonale Gruppe $\mathrm{O}(n) \ := \ \{L : \mathbb{R}^n \to \mathbb{R}^n \mid L \text{ ist orthogonal}\}$,
- Die spezielle orthogonale Gruppe $\mathrm{SO}(n) \ := \ \{L \in \mathrm{O}(n) \mid \det(L) = 1\}$.

Beweis: Zur Erinnerung: $(\mathrm{GL}_n(\mathbb{K}), \circ) = \{L : \mathbb{K}^n \to \mathbb{K}^n \mid L \text{ bijektiv}\}$, $(\mathrm{GL}_n(\mathbb{K}), \circ)$ ist eine nicht abelsche Gruppe.

1) Sei $U : \mathbb{C}^n \to \mathbb{C}^n$ unitär.

$$\Rightarrow \ |\det(U)| = \left|\prod_{j=1}^{n} \lambda_j\right| = 1 \neq 0 \ \Rightarrow \ U \text{ ist bijektiv.}$$

Also: $U(n) \subseteq \mathrm{GL}(\mathbb{K})$.

Seien U, V unitär.

$$\Rightarrow \begin{cases} U \circ V \text{unitär:} & (U \circ V)^* = V^* \circ U^* = V^{-1} \circ U^{-1} = (U \circ V)^{-1} \\ U^{-1} \text{ unitär:} & (U^{-1})^* = (U^*)^* = U = U^{-1})^{-1} \end{cases}$$

(Insbesondere $\mathrm{Id} = U \circ U^{-1} \in U(n)$)
Damit ist $U(n)$ Untergruppe von $(\mathrm{GL}_n(\mathbb{K}), \circ)$.

2) Wie in 1) folgt, dass $O(n)$ Untergruppe von $(\mathrm{GL}_n(\mathbb{K}), \circ)$ ist.
Es gilt: $U \in O(n) \ \Rightarrow \ \det U = \pm 1$.

Seien $U, V \in SO(n) \ \Rightarrow \begin{cases} U \circ V \in SO(n) : \det(U \circ V) = (\det U) \cdot \det V = 1 \\ U^{-1} \in SO(n) : \det(U^{-1}) = \dfrac{1}{\det U} = 1 \end{cases}$

$\square$

3.118 Charakterisierung selbstadjungierter Abbildungen: Sei V Vektorraum über $\mathbb{C}$ mit Skalarprodukt und $L : V \to V$ linear. Dann sind äquivalent:

(i) L ist selbstadjungiert,

(ii) L ist normal und $\sigma(L) \subseteq \mathbb{R}$,

(iii) $\forall v \in V : \langle L\,v, v\rangle \in \mathbb{R}$.

Beweis: **(i) $\Rightarrow$ (ii):** $L^* = L \;\Rightarrow\; L$ ist normal.

Sei B ONB aus EVen. Dann:

$$M_L^{B,B} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \overset{L=L^*}{=} M_{L^*}^{B,B} = \begin{pmatrix} \overline{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \overline{\lambda_n} \end{pmatrix}$$

$\Rightarrow\; \forall j \in \{1, \ldots, n\} : \lambda_j \in \mathbb{R}$.

(ii) $\Rightarrow$ (iii): Sei B ONB aus EVen.

$$\Rightarrow\; \langle Lv, v\rangle = \left\langle M_L^{B,B}(v)_B, (v)_B \right\rangle = \lambda_1^2|v_1|^2 + \ldots + \lambda_n|v_n|^2 \in \mathbb{R}.$$

(iii) $\Rightarrow$ (i): $\langle Lv, v\rangle = \langle v, Lv\rangle = \langle L^*v, v\rangle$.

$$\Rightarrow\; \forall v \in V : \langle (L - L^*)v, v\rangle = 0.$$

Nun gilt: $L - L^*$ ist normal (Nachrechnen!)

Sei B ONB aus EVen von $L - L^*$, $B = \{b_1, \ldots, b_n\}$.

$$\Rightarrow\; 0 = \langle (L - L^*)b_j, b_j\rangle = \lambda_j \|b_j\|^2 \;\Rightarrow\; \lambda_j = 0$$

$\Rightarrow\; L = L^*$, L ist selbstadjungiert. □

3.119 Folgerung: Im Satz 3.112 ist die Voraussetzung „L_M besitze eine Orthonormalbasis aus Eigenvektoren“ automatisch erfüllt, da M als selbstadjungiert vorausgesetzt wird.

3.120 Charakterisierung symmetrischer Abbildungen: Sei $L : \mathbb{R}^n \to \mathbb{R}^n : x \mapsto A\,x$. Dann sind äquivalent:

(i) A bzw. L ist symmetrisch,

(ii) L besitzt eine Orthonormalbasis aus Eigenvektoren.

Insbesondere zerfällt das charakteristische Polynom p_L in reelle Linearfaktoren, und für jeden Eigenwert λ von L gilt: $n_a(\lambda) = n_g(\lambda)$.

Beweisskizze:

(ii) $\Rightarrow$ (i): Sei B ONB aus EVen

$$\Rightarrow \quad S = M_{\mathrm{Id}}^{B,E} \text{ ist orthogonal,} \quad S \cdot A \cdot S^{-1} = D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

$$\Rightarrow \quad A^T = (S^{-1} \cdot D \cdot S)^T = (S^T \cdot D \cdot S)^T = S^T \cdot D \cdot (S^T)^T = S^T \cdot D \cdot S = A.$$

(i) $\Rightarrow$ (ii): Idee: Betrachte $\widetilde{L} : \mathbb{C}^n \to \mathbb{C}^n : x \mapsto Ax$.

$\widetilde{L}$ ist selbstadjungiert $\Rightarrow \begin{cases} \widetilde{B} \text{ ONB aus EVen existiert} \\ \text{Alle Eigenwerte sind reell} \end{cases}$

Ist nun $Ab_j = \lambda_j b_j$, so folgt für $c_j := \operatorname{Re} b_j = \frac{1}{2}(b_j + \overline{b_j}) \in \mathbb{R}^n$ und $\widetilde{c_j} := \operatorname{Im} b_j = \frac{1}{2}(b_j - \overline{b_j}) \in \mathbb{R}^n$:

$$Ac_j = \lambda_j \cdot c_j \ \wedge \ A\widetilde{c_j} = \lambda_j \cdot \widetilde{c_j}.$$

3.121 Anwendung auf quadratische Formen: Auf $\mathbb{R}^n$ sei die quadratische Form

$$q(x) \ := \ \langle A\,x, x\rangle$$

mit beliebiger quadratischer Matrix $A \in M_{n,n}(\mathbb{R})$ gegeben. Dann ist $(A + A^T)$ symmetrisch, und q ist die zur Bilinearform

$$b(x,y) \ = \ \left\langle \frac{1}{2}(A + A^T)x, y \right\rangle$$

gehörende quadratische Form. Sei nun $B = \{b_1, \ldots, b_n\}$ eine Orthonormalbasis aus Eigenvektoren: $\frac{1}{2}(A + A^T)\, b_j = \lambda_j\, b_j$. Dann gilt

$$q(x) \ = \ \lambda_1\, \widetilde{x}_1^2 + \ldots + \lambda_n\, \widetilde{x}_n^2 \qquad \text{mit } \widetilde{x} = (x)_B.$$

3.16 Die Jordansche Normalform

3.122 Definition: Für $\lambda_0 \in \mathbb{K}$ und $k \in \mathbb{N}$ heißt die $k \times k$-Matrix

$$J_{\lambda_0}^{(k)} \ := \ \begin{pmatrix} \lambda_0 & 1 & 0 & \ldots & 0 \\ 0 & \lambda_0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ 0 & \ldots & & 0 & \lambda_0 \end{pmatrix} \ \in \ M_{k,k}(\mathbb{K})$$

Jordan-Matrix oder **Jordan-Block**.

3.123 Satz: Für eine Jordan-Matrix $J_{\lambda_0}^{(k)}$ gelten:

1) $\lambda = \lambda_0$ ist einziger Eigenwert von $J_{\lambda_0}^{(k)}$,

2) $n_a(\lambda_0) = k$ und $n_g(\lambda_0) = 1$. Insbesondere ist $J_{\lambda_0}^{(k)}$ nicht diagonalisierbar für $k \geq 2$.

3) $\left(J_{\lambda_0}^{(k)} - \lambda_0 \cdot E\right)^k = 0$, d.h. die Matrix $J_{\lambda_0}^{(k)} - \lambda_0 \cdot E$ bzw. die zugehörige lineare Abbildung ist **nilpotent**.

Beweis: **1)** Es gilt $\det(J_{\lambda_0}^{(k)} - \lambda \cdot E) = (\lambda_0 - \lambda)^k$.

2) Folgt aus

$$\big(J_{\lambda_0}^{(k)} - \lambda_0 \cdot \mathrm{Id}\big)v \;=\; 0 \quad\Leftrightarrow\quad \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ 0 & \dots & & 0 & 0 \end{pmatrix} v \;=\; 0 \quad\Leftrightarrow\quad v \;=\; \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

3) Die Anwendung von $\big(J_{\lambda_0}^{(k)} - \lambda_0 \cdot \mathrm{Id}\big)$ auf einen Vektor v verschiebt alle Koordinateneinträge um eine Stelle nach oben und setzt die letzte Koordinate auf 0. Da der Vektor genau k Koordinaten hat, sind nach k Anwendungen alle Koordinaten 0, also $\big(J_{\lambda_0}^{(k)} - \lambda_0 \cdot \mathrm{Id}\big)^k v = 0$.

□

3.124 Satz: Es sei $k \geq 2$ und $L : \mathbb{K}^k \to \mathbb{K}^k$ eine lineare Abbildung, die nur einen Eigenwert λ_0 besitzt, und für die gilt: $n_a(\lambda_0) = k$, $n_g(\lambda_0) = 1$. Für eine Basis B von $\mathbb{K}^k$ sind äquivalent:

(i) $M_L^{B,B} = J_{\lambda_0}^{(k)}$,

(ii) Die Basis $B = \{b_1, \dots, b_k\}$ besteht aus einer **Vektorkette** zum Eigenwert λ_0 von L, d.h. es gilt

$$\begin{aligned} (L - \lambda_0 \cdot \mathrm{Id})\, b_1 &= 0 \quad (b_1 \text{ ist Eigenvektor}), \\ (L - \lambda_0 \cdot \mathrm{Id})\, b_{j+1} &= b_j \quad \text{für } j = 1, 2, \dots, k-1. \end{aligned}$$

Das bedeutet, man kommt von einem Element der Vektorkette zum vorherigen durch Anwendung der Abbildung $L - \lambda_0 \cdot \mathrm{Id}$.

Beweis: **(i) ⇒ (ii):** Durch Nachrechnen, z.B.

$$L\, b_2 \;=\; J_{\lambda_0}^{(k)} \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_B \;=\; \begin{pmatrix} 1 \\ \lambda_0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_B \;=\; b_1 + \lambda_0 \cdot b_2$$

(ii) ⇒ (i):

$$L\,b_1 \;=\; \lambda_0 \cdot b_1 \;\;\Rightarrow\;\; M_L^{B,B} \;=\; \begin{pmatrix} \lambda_0 & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \dots & * \end{pmatrix}$$

$$L\,b_2 \;=\; \lambda_0 \cdot b_2 + b_1 \;\;\Rightarrow\;\; M_L^{B,B} \;=\; \begin{pmatrix} \lambda_0 & 1 & * & \dots & * \\ 0 & \lambda_0 & * & \dots & * \\ 0 & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & * & \dots & * \end{pmatrix}$$

usw. □

3.125 Jordansche Normalform: Sei $L : V \to V$ linear. Falls p_L über $\mathbb{K}$ in Linearfaktoren zerfällt:

$$p_L(\lambda) \;=\; (\lambda_1 - \lambda)^{n_1} \cdots (\lambda_k - \lambda)^{n_k},$$

so gibt es eine Basis B von V, so dass

$$M_L^{B,B} \;=\; \begin{pmatrix} \boxed{J_1} & & & 0 \\ & \boxed{J_2} & & \\ & & \ddots & \\ 0 & & & \boxed{J_r} \end{pmatrix},$$

wobei $J_i = J_{\lambda_i}^{(k_i)}$ Jordan-Blöcke sind. L ist genau dann diagonalisierbar, wenn alle Jordan-Blöcke 1-dimensional sind.
Vorsicht: Es kann mehrere Jordan-Blöcke zu einem Eigenwert geben. Sind z.B. $J_1, \dots, J_l$ alle Jordan-Blöcke zum Eigenwert λ_1, so gilt $k_1 + \dots + k_l = n_a(\lambda_1)$ und $n_g(\lambda_1) = l$.

Ergänzung: Beweis des Satzes 3.125

3.126 Grundvoraussetzung: Für den Beweis von Satz 3.125 sei im folgenden vorausgesetzt:

- $L : V \to V$ ist linear, und es gilt $\dim(V) = n$.
- Für das charakteristische Polynom von L gilt

  $$p_L(\lambda) \;=\; (\lambda_1 - \lambda)^{n_1} \cdots (\lambda_k - \lambda)^{n_k},$$

  wobei die Eigenwerte $\lambda_1, \dots, \lambda_k$ paarweise verschieden sind. D.h. die algebraische Vielfachheit von λ_j ist $n_a(\lambda_j) = n_j$. Insbesondere gilt $n_1 + \dots + n_k = n$.

- Wir betrachten die Untervektorräume

$$V_j := \text{Kern}\left((L - \lambda_j \cdot \text{Id})^{n_j}\right) \quad \text{mit Basis} \quad B_j \qquad (j = 1, \ldots, k).$$

Zunächst sei B_j ganz allgemein eine Basis von V_j, später werden diese Basen speziell gewählt.

3.127 Satz: **1)** Für jedes $j \in \{1, \ldots, k\}$ ist V_j **invariant** unter L, d.h. es gilt

$$L(V_j) \subseteq V_j.$$

2) Für $i \neq j$ ist die Abbildung $(L - \lambda_i \cdot \text{Id})\big|_{V_j} : V_j \to V_j$ bijektiv.

Beweis: **1)** Sei j fest. Für $v \in V_j$ gilt $(L - \lambda_j \cdot \text{Id})^{n_j} v = 0$. Daraus folgt

$$(L - \lambda_j \cdot \text{Id})^{n_j}(Lv) = L(L - \lambda_j \cdot \text{Id})^{n_j} v = 0,$$

also $Lv \in V_j$.

2) Zunächst erhalten wir aus 1), dass für $v \in V_j$ auch $(L - \lambda_i \cdot \text{Id})v = L\,v - \lambda_i \cdot v \in V_j$.
Sei $v \in \text{Kern}\left((L - \lambda_i \cdot \text{Id})\big|_{V_j}\right)$. Das bedeutet einerseits $v \in V_j$, also $(L - \lambda_j \cdot \text{Id})^{n_j} v = 0$, und andererseits $L\,v = \lambda_i \cdot v$, also $(L - \lambda_j \cdot \text{Id})^{n_j} v = (\lambda_i - \lambda_j)^{n_j} \cdot v$. Wegen $\lambda_i - \lambda_j \neq 0$ folgt $v = 0$. Also gilt $\text{Kern}\left((L - \lambda_i \cdot \text{Id})\big|_{V_j}\right) = \{0\}$, und daraus folgt die Bijektivität. $\square$

3.128 Satz: $B := \bigcup_{j=1}^{k} B_j$ ist linear unabhängig (B_j = Basis von V_j, vgl. 3.126). Insbesondere gilt

$$\sum_{j=1}^{k} \dim(V_j) \leq \dim(V) = n.$$

Beweis: Wir bezeichnen die Elemente von B_j mit $b_1^{(j)}, \ldots, b_{d_j}^{(j)}$, wobei $d_j := \dim(V_j)$. Wir zeigen, wie aus

$$0 = \sum_{j=1}^{k} \sum_{l=1}^{d_j} c_{jl} \cdot b_l^{(j)}$$

$c_{1\,1} = c_{1\,2} = \ldots = c_{1\,d_1} = 0$ folgt. Genauso folgt dann $c_{j\,l} = 0$ für alle j, l, also die lineare Unabhängigkeit von B.

Wegen $(L - \lambda_j \cdot \text{Id})^{n_j}\, b_l^{(j)} = 0$ gilt

$$0 = \left(\prod_{j=2}^{k} (L - \lambda_j \cdot \text{Id})^{n_j}\right) \left(\sum_{j=1}^{k} \sum_{l=1}^{n_j} c_{jl} \cdot b_l^{(j)}\right) = \sum_{l=1}^{n_1} c_{1l} \cdot \left(\prod_{j=2}^{k} (L - \lambda_j \cdot \text{Id})^{n_j}\right) b_l^{(1)}$$

Für $j \neq 1$ ist die Abbildung $(L - \lambda_j \cdot \mathrm{Id})\Big|_{V_1} : V_1 \to V_1$ bijektiv. Das bedeutet, dass linear unabhängige Mengen auf linear unabhängige Mengen abgebildet werden. Somit ist die Menge

$$\left\{ \prod_{j=2}^{k} (L - \lambda_j \cdot \mathrm{Id})^{n_j}\, b_l^{(1)} : l = 1, \ldots, d_1 \right\}$$

linear unabhängig, und es folgt $c_{1\,1} = c_{1\,2} = \ldots = c_{1\,d_1} = 0$. □

3.129 Satz: Es gilt $\dim(V_j) = n_j$ für $j = 1, \ldots, k$.

Beweis: Es genügt, $\dim(V_j) \geq n_j$ zu beweisen. Mit $\dim(V_1) + \ldots + \dim(V_k) \leq n_1 + \ldots n_k$ (letzter Satz) folgt dann die Behauptung.

Wir führen den Beweis für $j = 1$. Dazu sei $\tilde{B}$ eine Basis von V, die durch Ergänzung von B_1 entstanden ist. Da V_1 invariant unter L ist, folgt

$$M_L^{\tilde{B},\tilde{B}} = \begin{pmatrix} A_1 & * \\ 0 & A \end{pmatrix},$$

mit einer $d_1 \times d_1$-Matrix A_1 und einer $(n - d_1) \times (n - d_1)$-Matrix A ($d_1 = \dim(V_1)$).

Aus dem Entwicklungssatz folgt

$$p_L(\lambda) = \det(L - \lambda \cdot \mathrm{Id}) = \big(\det(A_1 - \lambda \cdot E_{d_1})\big) \cdot \det(A - \lambda \cdot E_{n-d_1})$$

($E_l = l \times l$-Einheitsmatrix). Falls λ_1 keine Nullstelle von $\det(A - \lambda \cdot E_{n-d_1})$ ist, muss $(\lambda_1 - \lambda)^{n_1}$ Teiler von $\det(A_1 - \lambda \cdot E_{d_1})$ sein und somit $d_1 \geq n_1$ gelten.

Annahme: λ_1 ist Nullstelle von $\det(A - \lambda \cdot E_{n-d_1})$. Dann besitzt A einen Eigenvektor zum Eigenwert λ_1. Hieraus folgt, dass L einen Eigenvektor zum Eigenwert λ_1 besitzt, der nicht in V_1 (von B_1 aufgespannt) liegt. Dies ist ein Widerspruch zu $V_1 = \mathrm{Kern}\big((L - \lambda_1 \cdot \mathrm{Id})^{n_1}\big)$. □

3.130 Satz: $B := \bigcup_{j=1}^{k} B_j$ ist Basis von V, und es gilt

$$M_L^{B,B} = \begin{pmatrix} A_1 & 0 & \ldots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & A_k \end{pmatrix},$$

wobei für $j = 1, \ldots, k$ die Matrix A_j eine $n_j \times n_j$-Matrix ist.

Beweis: Nach dem letzten Satz spannt B einen Raum der Dimension $n_1 + \ldots + n_k = n = \dim(V)$ auf, ist also Basis von V.

Die Gestalt der Matrix $M_L^{B,B}$ folgt aus der Tatsache, dass die von den Basen B_j aufgespannten Räume V_j unter L invariant sind. $\square$

Mit dem nächsten Satz bzw. der Verallgemeinerung für B_j folgt dann die Behauptung von Satz 3.125.

3.131 Satz: Die Basis B_1 von V_1 kann so gewählt werden, dass sie als Vereinigung von Vektorketten dargestellt werden kann, d.h. es gibt Vektorketten $K_1, \ldots, K_m$, so dass $B_1 = K_1 \cup K_2 \cup \ldots \cup K_m$. Für diese Wahl von B_1 hat die Matrix A_1 im letzten Satz die Form

$$A_1 = \begin{pmatrix} \boxed{J_1} & & & 0 \\ & \boxed{J_2} & & \\ & & \ddots & \\ 0 & & & \boxed{J_m} \end{pmatrix},$$

wobei $J_i = J_{\lambda_1}^{(k_i)}$ Jordan-Blöcke zum Eigenwert λ_1 mit $k_i = \sharp K_i$ sind $(i = 1, \ldots, m)$.

Zum Beweis reicht es, eine Basis von V_1 zu konstruieren, die nur aus Vektorketten zum Eigenwert λ_1 von L besteht. Zu jeder Vektorkette (die auch nur aus einem Vektor bestehen kann, das ist dann ein Eigenvektor) gehört dann in A ein Jordan-Block (vgl. 3.124). Wir untersuchen zunächst die lineare Unabhängigkeit von Vektorketten.

3.132 Satz: E seien l Vektorketten $K_1 = \{v_1^{(1)}, \ldots\}, \ \ldots, \ K_l = \{v_1^{(l)}, \ldots\}$ zum Eigenwert λ_1 von L gegeben. Dann sind äquivalent:

(i) $K_1 \cup \ldots \cup K_l$ ist linear unabhängig.

(ii) $\{v_1^{(1)}, \ldots, v_1^{(l)}\}$ ist linear unabhängig (d.h. die Menge aus allen ersten Vektoren der Vektorketten).

Beweis: (i) $\Rightarrow$ (ii): Folgt direkt aus $\{v_1^{(1)}, \ldots, v_1^{(l)}\} \subseteq K_1 \cup \ldots \cup K_l$.

(ii) $\Rightarrow$ (i): Wir beweisen folgende einfachere Fassung: Es seien $K_1 = \{v_1, \ldots, v_i\}$ und $K_2 = \{w_1, \ldots, w_j\}$ zwei Vektorketten zum Eigenwert λ_1. Ist $\{v_1, w_1\}$ linear unabhängig, dann auch $K_1 \cup K_2$. Der allgemeine Beweis geht genauso.

Sei

$$0 = \sum_{l=1}^{i} c_l \cdot v_l + \sum_{l=1}^{j} d_l \cdot w_l.$$

Annahme: Mindestens einer der Koeffizienten c_l, d_l ist von Null verschieden. Dann ist

$$M \;:=\; \max\{l : c_l \neq 0 \;\vee\; d_l \neq 0\} \;\geq\; 1.$$

Da alle c_l, d_l mit $l \geq 0$ verschwinden, folgt aus der Definition von Vektorketten

$$\begin{aligned} 0 &= (L - \lambda_1 \cdot \mathrm{Id})^{M-1} \left(\sum_{l=1}^{M} c_l \cdot v_l + \sum_{l=1}^{M} d_l \cdot w_l \right) \\ &= c_M \cdot v_1 + d_M \cdot w_1 \end{aligned}$$

und aus der linearen Unabhängigkeit von $\{v_1, w_1\}$ schließlich $c_M = d_M = 0$ im Widerspruch zur Definition von M. Also müssen alle Koeffizienten c_l, d_l verschwinden. $\square$

Beweis: (von Satz 3.131, konstruktiv, kann so programmiert werden)

Wir ändern die Basis B_1 von V_1 sukzessive ab, bis sie nur noch aus Vektorketten besteht. Dazu betrachten wir für jedes Element $v \in B_1$ die zugehörige Vektorkette

$$\begin{aligned} K(v) \;:=\; &\left\{ (L - \lambda_1 \cdot \mathrm{Id})^l \, v, (L - \lambda_1 \cdot \mathrm{Id})^{l-1} \, v, \ldots, v \right\} \\ &\text{mit } (L - \lambda_1 \cdot \mathrm{Id})^l \, v \neq 0 \;\wedge\; (L - \lambda_1 \cdot \mathrm{Id})^{l+1} \, v = 0. \end{aligned}$$

Aus der Definition von V_1 folgt $l \leq n_1 - 1$.

Schritt 1: Wir setzen

$$L(B_1) \;:=\; \max\{\sharp K(v) : v \in B_1\} \quad \text{(maximale Kettenlänge)},$$

Wir stellen fest, wie viele der Vektorketten maximaler Länge benötigt werden:

$$d(B_1) \;:=\; \dim \mathrm{LH} \left\{ (L - \lambda_1 \cdot \mathrm{Id})^{L(B_1)-1} \, v : v \in B_1 \right\}.$$

Nun seien $v_1, \ldots, v_{d(B_1)} \in B_1$ so ausgewählt, dass gilt:

$$\begin{aligned} &\left\{ (L - \lambda_1 \cdot \mathrm{Id})^{L(B_1)-1} \, v_l : l = 1, \ldots, d(B_1) \right\} \\ &\qquad \text{ist eine Basis von } \mathrm{LH}\left\{ (L - \lambda_1 \cdot \mathrm{Id})^{L(B_1)-1} \, v : v \in B_1 \right\}. \end{aligned}$$

Nun reduzieren wir die Länge der anderen Ketten maximaler Länge. Dazu wird jedes $v \in B_1 \setminus \{v_1, \ldots, v_{d(B_1)}\}$, das eine Kette $K(v)$ mit maximaler Länge erzeugt ($\sharp K(v) = L(B_1)$), ersetzt durch

$$\tilde{v} \;:=\; v - \sum_{j=1}^{d_1} c_j \cdot v_j, \quad \text{so dass } (L - \lambda_1 \cdot \mathrm{Id})^{L(B_1)-1} \, \tilde{v} = 0.$$

Dadurch entsteht eine Basis $\tilde{B}_1$, in der nur die Ketten $K(v_1), \ldots, K(v_{d(B_1)})$ die Länge $\sharp K(v) = L(B_1)$ haben. Für alle anderen Ketten gilt $\sharp K(v) < L(B_1)$.

Nun verwenden wir den letzten Satz. Aus der Definition der Vektoren $v_1, \ldots, v_{d(B_1)}$ folgt, dass die Menge $K(v_1) \cup \ldots \cup K(v_{d(B_1)})$ linear unabhängig ist. Nun tauschen wir diese Vektoren mit ebenso vielen passend gewählten Vektoren aus der Basis $\tilde{B}_1$ aus (Basisaustauschsatz). Dann haben wir eine Basis $B_1^{(1)}$ von V_1 mit

$$K(v_1) \cup \ldots \cup K(v_{d(B_1)}) \;\subseteq\; B_1^{(1)}.$$

Schritt 2: Falls $C_1 := B_1^{(1)} \setminus \big(K(v_1) \cup \ldots \cup K(v_{d(B_1)}\big) \neq 0$, führen wir dieselbe Prozedur für diese Menge durch: Wir bestimmen $L(C_1)$ und wählen $d(C_1)$ Vektoren aus C_1 aus, so dass gilt:

$$\big\{(L - \lambda_1 \cdot \mathrm{Id})^{L(C_1)-1}\, v_l : l = d(B_1)+1, \ldots, d(B_1)+d(C_1)\big\}$$
$$\text{ist eine Basis von } \mathrm{LH}\big\{(L - \lambda_1 \cdot \mathrm{Id})^{L(C_1)-1}\, v : v \in C_1\big\}.$$

Entsprechend der obigen Vorgehensweise entsteht eine Basis $B_1^{(2)}$, so dass

$$K(v_1) \cup \ldots \cup K(v_{d(B_1)+d(B_2)}) \;\subseteq\; B_1^{(2)}.$$

Dieses Verfahren kann so lange fortgesetzt werden, bis die entstandene Basis $B_1^{(l)}$ nur noch aus Vektorketten (eventuell der Länge 1, dann enthält die Vektorkette nur einen Eigenvektor und keine anderen Vektoren) besteht. □

3.133 Bemerkungen: **1)** Aus dem letzten Beweis folgt, dass $V_1 = \mathrm{Kern}\,\big((L - \lambda_1 \cdot \mathrm{Id})^{L(B_1)}\big)$ gilt, wobei $L(B_1) \leq n_1$.

2) Sei p_L das charakteristische Polynom von L. Man kann nun in die Variable auch lineare Abbildungen (oder Matrizen) einsetzen, da Potenzen und Linearkombinationen von linearen Abbildungen definiert sind. Dann ist z.B. $p_L(L)$ wieder eine lineare Abbildung. Aus der Jordanschen Normalform von L folgt, dass

$$p_L(L) \;:=\; (L - \lambda_1 \cdot \mathrm{Id})^{n_1} \cdots (L - \lambda_k \cdot \mathrm{Id})^{n_k} \;=\; \mathbb{0}.$$

Diese Gleichung heißt **Gleichung von Cayley-Hamilton**. Mit der vorigen Bemerkung folgt sogar

$$(L - \lambda_1 \cdot \mathrm{Id})^{L(B_1)} \cdots (L - \lambda_k \cdot \mathrm{Id})^{L(B_k)} \;=\; \mathbb{0}.$$

Inhaltsverzeichnis

Stichwortverzeichnis