Mathematik für Informatiker II
Sommersemester 2011

Allgemeines

- Matthias Hein
  hein@cs.uni-saarland.de
  Geb. E1.1, R. 225
  Sprechstunde: Montag, 15.00–17.00 Uhr

- Übungskoordinator:
  Christoph Eisinger
  christoph@math.uni-sb.de
  Geb. E2.4, R. 213

- Informationen zur Vorlesung:

  http://www.ml.uni-saarland.de/MfI2-SS11/MfI2SS11.shtml

- Vorlesungen: Mittwoch und Freitag, jeweils 10–12 Uhr

- Übungen: Vorgesehen sind 11 Gruppen.

  1) Mo 10-12 in SR 016, Geb. E1 3 - Tutor: Peter Rau

  2) Mo 12-14 in SR 014, Geb. E1 3 - Tutor: Marco Holz

  3) Mo 12-14 in SR 016, Geb. E1 3 - Tutor: Peter Rau

  4) Mo 16-18 in SR 014, Geb. E1 3 - Tutor: Patrick Trampert

  5) Mo 16-18 in SR 107, Geb. E1 3 - Tutor: Sebastian Kleer

  6) Mo 16-18 in SR U12, Geb. E1 1 - Tutor: Martina Bruck

  7) Di 8-10 in SR 107, Geb. E1 3 - Tutor: Tanja Dorst

  8) Di 8-10 in SR U12, Geb. E1 1 - Tutor: Julian Steil

  9) Do 8-10 in SR 015, Geb. E1 3 - Tutor: Martina Bruck

  10) Fr 14-16 in SR 016, Geb. E1 3 - Tutor: Sebastian Kleer

  11) Fr 14-16 in SR 107, Geb. E1 3 - Tutor: Patrick Trampert

  Anmeldung über die Internetseite der Vorlesung

von Mittwoch, 13. 04. 2011, 13.00 Uhr
bis Montag, 14. 04. 2011, 18.00 Uhr.

Übungsbeginn: 18. 04. 2011.

Übungsbetrieb

Hausübungen:

- Übungsblätter: freitags auf der Vorlesungswebseite
- Abgabe: 1 Woche später freitags **vor** der Vorlesung in den Kästen der Übungsleiter in E1 3, rechts vor Hörsaal 1.
- Abgabe in Teams bis zu 3 Personen
  - Alle Teammitglieder müssen in derselben Übungsgruppe sein.
  - Die Zusammensetzung des Teams sollte sich im Laufe des Semesters nicht ändern.
- Übungen werden korrigiert und mit Punkten bewertet
- Musterlösungen werden nach Ende der Bearbeitungszeit im Internet bereit gestellt.

Präsenzübungen:

- Präsenz-Übungsaufgaben werden in der Übung bearbeitet und besprochen.
- Die Teilnahme wird stark empfohlen.

Voraussetzungen für die Klausurzulassung:

- 50 % der erreichbaren Übungspunkte aus den Hausübungen
- Bei Nichtteilnahme an einer Präsenzübung (teilweise Anwesenheit zählt nicht) verfallen 50 % der in einer vorausgehenden Hausübung erzielbaren Punkte.

Klausuren

- Hauptklausur: 28. 07. 2011, 9-12
- Wiederholungsklausur: 07. 10. 2011, 9-12

- Bei Teilnahme an beiden Klausuren gilt die bessere Note.
- Probeklausur vorher.
- Erlaubte Hilfsmittel: Ein Din A4 Blatt beidseitig von Hand beschrieben.

Zielgruppe und Inhalt

- Kurs für Studierende der Informatik, Bioinformatik, Medieninformatik oder Wirtschaftsinformatik
- Studierende mit Nebenfach Mathematik besuchen Analysis I und Lineare Algebra I.
- MfI 1: Diskrete Mathematik und eindimensionale Analysis
- MfI 2: Algebraische Strukturen; lineare Algebra
- MfI 3: Stochastik, Numerik, mehrdimensionale Analysis
- MfI 2 setzt MfI 1 nicht notwendig voraus

Literatur

- P. Hartmann: Mathematik für Informatiker. Vieweg, 2003 (30,90 EUR)
  Didaktisch sehr gut, inhaltlich aber nicht immer ausreichend
- M. Wolff, P. Hauck, W. Küchlin: Mathematik für Informatik und Bioinformatik. Springer, 2004 (29,95 EUR)
  für MfI 1–3, sehr umfassend, etwas schwerer zu lesen als das Buch von Hartmann
- M. Wolff: Übungsaufgaben zur Mathematik für Informatiker und Bioinformatiker. Springer, 2006 (19,95 EUR)
  Gute Ergänzung zum Lehrbuch von Wolff/Hauck/Küchlin
- A. Beutelspacher: Lineare Algebra. Vieweg, 2003 (19,90 EUR) – nur für MfI 2
  gut lesbar mit vielen Erklärungen

- H. Anton: Lineare Algebra. Spektrum Akademischer Verlag, 1998 (26,50 EUR) – nur für MfI 2
  recht umfassend, gute Ergänzung, etwas formaler als das Buch von Beutelspacher

Skript

Es ist geplant, ein Skript *im Nachgang* zur Vorlesung online bereit zu stellen.

> **Dies ist keine Fernstudiumsveranstaltung.**
> **Skript und Webseite ersetzen nicht den Vorlesungsbesuch.**
>
> In der Vorlesung und in den Übungen können jederzeit zusätzliche wesentliche Informationen gegeben werden, die nicht online abrufbar sind. Es ist in Ihre Verantwortung gestellt, sich diese Informationen zu verschaffen.

C: Algebraische Strukturen

29 Gruppen

29.1 Bedeutung für die Informatik

- „Mathematik ist die Lehre von den guten Beschreibungen.“ (A. Beutelspacher)
  Die Gruppentheorie arbeitet grundlegende Gemeinsamkeiten hinter vielen Problemen heraus. Ihre Aussagen können dann für all diese Probleme angewandt werden.
- Gruppen sind abstrakte Modelle für Mengen, auf denen eine Verknüpfung (wie Addition oder Multiplikation) definiert ist.

29.2 Definition

Eine **Gruppe** besteht aus einer Menge G und einer Verknüpfung $\bullet$, die je zwei Elementen aus G wieder ein Element aus G zuordnet und für die gilt:

a) *Assoziativgesetz:* $(a \bullet b) \bullet c = a \bullet (b \bullet c) \quad \forall a, b, c \in G.$

b) *Linksneutrales Element:* $\exists e \in G : \quad e \bullet a = a \quad \forall a \in G.$

c) *Linksinverse Elemente:* Zu jedem $a \in G$ existiert ein $b \in G$ mit $b \bullet a = e$. Man schreibt auch $b =: a^{-1}$.

Gilt zusätzlich

d) *Kommutativgesetz:* $a \bullet b = b \bullet a \quad \forall a, b \in G,$

so heißt $(G, \bullet)$ **kommutative Gruppe (abelsche Gruppe)**. (Vergleiche auch 8.2 in MfI 1.)

$|G|$ heißt **Ordnung** der Gruppe. Ist $|G| < \infty$, spricht man von einer **endlichen** Gruppe.

Ein Element e heißt rechtsneutral, wenn

$$a \bullet e = a \quad \forall a \in G.$$

Ein Element heißt neutral, wenn es sowohl linksneutral als auch rechtsneutral ist. Ist ein Element $b \in G$ linksinvers zu $a \in G$ als auch rechtsinvers d.h.

$$b \bullet a = e = a \bullet b,$$

dann nennen wir es inverses Element von a.

Bemerkung: Erfüllt $(G, \bullet)$ lediglich das Assoziativgesetz, so spricht man von einer **Halbgruppe** (englisch *semigroup*). Halbgruppen mit neutralem Element heißen **Monoide**.

29.3 Beispiele

a) Die natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \ldots\}$ bilden mit der Addition als Verknüpfung eine kommutative Halbgruppe $(\mathbb{N}, +)$.

b) Die nichtnegativen ganzen Zahlen $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ mit der Addition bilden ein kommutatives Monoid $(\mathbb{N}_0, +)$ mit 0 als neutralem Element. $(\mathbb{N}_0, +)$ ist keine Gruppe, da zu $a \in \mathbb{N}_0$, $a \neq 0$ kein inverses Element existiert.

c) Ganze Zahlen, rationale Zahlen, reelle Zahlen: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind kommutative Gruppen.

d) $(\mathbb{Z}, \cdot)$ ist ein Monoid (1 ist neutrales Element), jedoch keine Gruppe

e) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ sind kommutative Gruppen.

f) Eine **Abbildung (Funktion)** zwischen zwei Mengen M, N ist eine Vorschrift $f : M \to N$, die jedem Element $x \in M$ ein eindeutiges Element $f(x) \in N$ zuordnet (vgl. MfI 1, 5.2). Die Abbildung f heißt **bijektiv**, falls zu jedem $y \in N$ ein $x \in M$ mit $f(x) = y$ existiert und für $x_1, x_2 \in M$ mit $x_1 \neq x_2$ stets $f(x_1) \neq f(x_2)$ gilt (vgl. MfI 1, 5.6).

   Die Menge aller Abbildungen $g : M \to M$ bildet mit der Komposition (Hintereinanderausführung) $\circ$ als Verknüpfung ein Monoid, mit der identischen Abbildung als neutralem Element. Die Menge aller bijektiven Abbildungen $g : M \to M$ bildet sogar eine Gruppe (i. d. R. nichtkommutativ).

g) Wichtiger Spezialfall von f: $M = \{1, \ldots, n\}$. Die Menge der bijektiven Abbildungen $M \to M$ mit der Komposition $\circ$ bildet die **Permutationsgruppe (symmetrische Gruppe)** $(S_n, \circ) = S_n$.

Beispiel für $n = 3$:

$$\sigma_1 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \sigma_2 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \sigma_3 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\sigma_4 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \sigma_5 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \sigma_6 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Dabei beschreibt z. B. σ_3 die Abbildung

$$1 \mapsto 3$$
$$2 \mapsto 1$$
$$3 \mapsto 2\,.$$

$\sigma_3 \circ \sigma_4$ beschreibt dann (Reihenfolge beachten!)

$$1 \overset{\sigma_4}{\mapsto} 2 \overset{\sigma_3}{\mapsto} 1$$
$$2 \overset{\sigma_4}{\mapsto} 1 \overset{\sigma_3}{\mapsto} 3$$
$$3 \overset{\sigma_4}{\mapsto} 3 \overset{\sigma_3}{\mapsto} 2\,,$$

d. h. $\sigma_3 \circ \sigma_4 = \sigma_5$.

Verknüpfungstafel (oder Gruppentafel):

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_3	σ_1	σ_6	σ_4	σ_5
σ_3	σ_3	σ_1	σ_2	σ_5	σ_6	σ_4
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_6	σ_4	σ_3	σ_1	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

σ_1 ist neutrales Element.

Beachte: S_n ist nicht kommutativ: $\sigma_4 \circ \sigma_6 \neq \sigma_6 \circ \sigma_4$.

29.4 Satz: Eindeutigkeit des neutralen Elements und der inversen Elemente

In jeder Gruppe gibt es nur ein neutrales Element. Jedes Element einer Gruppe hat genau ein inverses Element.

Beweis: Sei e ein neutrales Element. Der Beweis verläuft in 4 Schritten.

a) Ist $ba = e$ (also $b = a^{-1}$), so gilt auch $ab = e$ („linksinverse“ Elemente sind auch „rechtsinvers“):

$$\begin{aligned} ab &= e(ab) \\ &= (b^{-1}b)(ab) \\ &= b^{-1}((ba)b) \qquad \text{(Assoziativität)} \\ &= b^{-1}(eb) \\ &= b^{-1}b = e\ . \end{aligned}$$

b) Für alle $a \in G$ gilt $ae = a$ (das „linksneutrale“ Element e ist auch „rechtsneutral“):

$$\begin{aligned} ae &= a(a^{-1}a) \\ &= (aa^{-1})a \qquad \text{(Assoziativität)} \\ &= ea \qquad \text{(nach (a))} \\ &= a \qquad \text{(Def. (links-) neutrales Element)}\ . \end{aligned}$$

c) Es gibt nur ein neutrales Element.

Sei nämlich e' ein weiteres neutrales Element. Dann folgt

$$e'a = a \qquad \forall a \in G$$

$$\Rightarrow e = e'e \overset{\text{(b)}}{=} ee' = e'\ .$$

d) Zu jedem $a \in G$ gibt es nur ein $a^{-1} \in G$.

Sei nämlich c ein weiteres inverses Element zu a. Dann

$$ca = e \qquad (*)$$

und

$$\begin{aligned} c &= ce \qquad \text{(nach (b))} \\ &= c(aa^{-1}) \qquad \text{(nach (a))} \\ &= (ca)a^{-1} \qquad \text{(Assoziativität)} \\ &= ea^{-1} \qquad \text{(nach (*))} \\ &= a^{-1}\ . \end{aligned}$$

□

Gibt es Gruppen, die selbst wieder Gruppen enthalten?

29.5 Definition: Untergruppe

Eine nichtleere Teilmenge U einer Gruppe $(G, \bullet)$, die mit der Verknüpfung $\bullet$ selbst eine Gruppe ist, heißt **Untergruppe** von G.

29.6 Satz: Untergruppenkriterium

Sei $(G, \bullet)$ eine Gruppe und $U \subset G$ nichtleer. Folgende Aussagen sind äquivalent:

i $(U, \bullet)$ ist eine Untergruppe,

ii für alle $a, b \in U \Rightarrow a \bullet b \in U$ und $a^{-1} \in U$,

iii für alle $a, b \in U \Rightarrow a \bullet b^{-1} \in U$.

Beweis:

$(i) \Rightarrow (ii)$ Da $(U, \bullet)$ eine Gruppe ist, gilt für alle $a, b \in U$, daß auch $a \bullet b \in U$ und für jedes $a \in U$ ist auch das inverse Element $a^{-1} \in U$.

$(ii) \Rightarrow (iii)$ Für alle $b \in U$ ist auch $b^{-1} \in U$. Nach Voraussetzung ist für alle $a, b \in U$ auch $a \bullet b \in U$ und damit auch $a \bullet b^{-1} \in U$.

$(iii) \Rightarrow (i)$ Für alle $a, b \in U$ ist auch $a \bullet b^{-1} \in U$. Damit folgt mit $b = a$, daß $a \bullet a^{-1} = e \in U$ (neutrales Element). Mit $a = e$ folgt für alle $b \in U$ ist auch $e \bullet b^{-1} = b^{-1} \in U$ (inverses Element). Mit $a, b^{-1} \in U$ folgt auch $a \bullet (b^{-1})^{-1} = a \bullet b \in U$. (Verknüpfung ist abgeschlossen). Das Assoziativgesetz überträgt sich aus G.

□

Bemerkung: Ist G eine kommutative Gruppe, so ist auch jede Untegruppe eine kommutative Gruppe.

29.7 Beispiele

a) $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$ sind Untergruppen von $(\mathbb{R}, +)$.

b) $(m\mathbb{Z}, +)$ mit $m\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$ und $m \in \mathbb{N}$ ist Untergruppe von $(\mathbb{Z}, +)$.

c) Ist $(G, \bullet)$ eine Gruppe mit dem neutralen Element e, so sind $(\{e\}, \bullet)$ und $(G, \bullet)$ selbst Untergruppen von $(G, \bullet)$. Da jede Gruppe diese Untergruppen besitzt, werden diese **triviale Untergruppen** genannt.

d) Jede Permutation von $M = \{1, \ldots, n\}$ lässt sich durch eine Sequenz von Vertauschungen je zweier Elemente (**Transpositionen**) darstellen.

   Die Menge aller Permutationen von $M = \{1, \ldots, n\}$ mit einer geraden Anzahl von Transpositionen bildet eine Untergruppe der symmetrischen Gruppe $(S_n, \circ)$, die **alternierende Gruppe** $(A_n, \circ)$.

   Zum Beispiel besteht A_3 aus den Permutationen $\sigma_1, \sigma_2, \sigma_3$ (Bezeichnungen nach 29.3) mit der Verknüpfungstafel

$\circ$	σ_1	σ_2	σ_3
σ_1	σ_1	σ_2	σ_3
σ_2	σ_2	σ_3	σ_1
σ_3	σ_3	σ_1	σ_2

   A_3 ist sogar kommutativ (obwohl S_3 nicht kommutativ ist).

29.8 Zyklenschreibweise für Permutationen

Es sei σ eine Permutation von $M = \{1, \ldots, n\}$. Dann wird jedes Element von M nach spätestens n-maligem Anwenden von σ auf sich selbst abgebildet.

Begründung: Für alle $a \in M$ gilt, daß die Sequenz

$$\big(a, \sigma(a), \sigma(\sigma(a)), \ldots, \sigma^n(a)\big)$$

$n + 1$ Elemente enthält und da $|M| = n$ muß mindestens ein Element in der Sequenz zweimal vorkommen. Das erste Element, daß sich in der Sequenz wiederholt muß a selbst sein, da ansonsten zwei verschiedene Element von σ auf dasselbe Element abgebildet werden würden, was der Injektivität von σ widerspricht.

Beispiel: $n = 4$

a) $\sigma_1 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

$$1 \overset{\sigma_1}{\mapsto} 3 \overset{\sigma_1}{\mapsto} 2 \overset{\sigma_1}{\mapsto} 4 \overset{\sigma_1}{\mapsto} 1$$

b) $\sigma_2 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

$$1 \overset{\sigma_2}{\mapsto} 3 \overset{\sigma_2}{\mapsto} 2 \overset{\sigma_2}{\mapsto} 1$$
$$4 \overset{\sigma_2}{\mapsto} 4$$

c) $\sigma_3 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$$1 \overset{\sigma_3}{\mapsto} 3 \overset{\sigma_3}{\mapsto} 1$$
$$2 \overset{\sigma_3}{\mapsto} 4 \overset{\sigma_3}{\mapsto} 2$$

Dies motiviert die **Zyklenschreibweise**

a) $\sigma_1 = (\ 1\ \ 3\ \ 2\ \ 4\ )$

b) $\sigma_2 = (\ 1\ \ 3\ \ 2\ )$ (der Einerzyklus $(\ 4\ )$ wird weggelassen)

c) $\sigma_3 = (\ 1\ \ 3\ )\ (\ 2\ \ 4\ )$.

Eigenschaften:

- Ein Zyklus $(\ a\ \ b\ \ c\ \ d\ )$ ist invariant unter zyklischer Vertauschung seiner Argumente d.h. $(\ a\ \ b\ \ c\ \ d\ ) = (\ b\ \ c\ \ d\ \ a\ ) = (\ c\ \ d\ \ a\ \ b\ ) = (\ d\ \ a\ \ b\ \ c\ )$.
- Das inverse Element eines Zyklus $(\ a\ \ b\ \ c\ \ d\ )$ ergibt sich durch rückwärts schreiben des Zyklus:

$$(\ a\ \ b\ \ c\ \ d\ )^{-1} = (\ d\ \ c\ \ b\ \ a\ ).$$

- Jede Permutation läßt sich in ein endliches Produkt disjunkter Zyklen zerlegen.
- Jeder Zyklus läßt sich als Verküpfung von Vertauschungen von je zwei Elementen schreiben (Transposition oder 2er-Zyklus).

Fortsetzung der Beispiele:

$\sigma_1 = (\ 1\ \ 3\ \ 2\ \ 4\ ) = (\ 1\ \ 3\ ) \bullet (\ 3\ \ 2\ ) \bullet (\ 2\ \ 4\ )$, (ungerade Permutation)
$\sigma_2 = (\ 1\ \ 3\ \ 2\ ) = (\ 1\ \ 3\ ) \bullet (\ 3\ \ 2\ )$, (gerade Permutation)
$\sigma_3 = (\ 1\ \ 3\ )\ (\ 2\ \ 4\ )$, (gerade Permutation)

- Eine Permutation heißt **gerade**, wenn sie Komposition einer geraden Anzahl von Transpositionen ist. (Die Zerlegung in Transpositionen ist nicht eindeutig aber alle Zerlegungen einer Permutation sind entweder immer gerade oder immer ungerade).

Mit Hilfe von Äquivalenzrelationen kann man eine Menge in Äquivalenzklassen zerlegen (vgl. MfI 1, 4.4–4.6). Gibt es eine ähnliche Zerlegung bei Gruppen?

29.9 Definition

Es sei $(G, \bullet)$ eine Gruppe mit Untergruppe $(U, \bullet)$. Ferner sei $g \in G$. Dann nennen wir

$$gU := \{g \bullet u \mid u \in U\} \quad \textbf{Linksnebenklasse} \text{ von } g,$$
$$Ug := \{u \bullet g \mid u \in U\} \quad \textbf{Rechtsnebenklasse} \text{ von } g.$$

Bemerkung: Häufig betrachtet man nur Linksnebenklassen und nennt diese *Nebenklassen.*

29.10 Satz: Nebenklassenzerlegung einer Gruppe

Es sei $(G, \bullet)$ eine Gruppe, $g, h \in G$ und $(U, \bullet)$ eine Untergruppe. Dann gilt:

a) $g \in U \quad \Rightarrow \quad gU = U$

b) Zwei (Links-) Nebenklassen gU, hU sind entweder gleich oder disjunkt.

c) Jedes $a \in G$ liegt in einer eindeutig bestimmten (Links-) Nebenklasse, d. h. die Nebenklassen von U bilden eine *Partition* von G.

d) Alle (Links-) Nebenklassen bezüglich einer festen Untergruppe U sind gleich mächtig:

$$|gU| = |U| \quad \forall g \in G \, .$$

Bemerkung: Für Rechtsnebenklassen gelten analoge Aussagen.

Beweis:

a) Aus der Abgeschlossenheit von U unter der Gruppenoperation folgt $gU \subset U$. Da auch $g^{-1} \in U$, gilt für jedes $h \in U$, dass

$$g(g^{-1}h) = (gg^{-1})h = h$$

mit $g^{-1}h \in U$, also $U \subset gU$.

b) Angenommen, gU und hU haben ein gemeinsames Element.
Dann folgt: Es gibt $a, b \in U$ mit

$$ga = hb \tag{*}$$

Daraus folgt

$$\begin{aligned} gU &\overset{(a)}{=} g(aU) = (ga)U \overset{(*)}{=} (hb)U \\ &= h(bU) \overset{(a)}{=} hU \, . \end{aligned}$$

c) $a \in G$ liegt in aU, da U das neutrale Element e enthält. Die Eindeutigkeit folgt aus (b).

d) Wir betrachten die Linksnebenklasse gU.

- Zu jedem $a \in gU$ existiert ein $b = b(a) \in U$ mit $gb = a$, wobei für $a_1 \neq a_2$ stets $b(a_1) \neq b(a_2)$ gilt. Also ist $|gU| \leq |U|$.
- Für $a_1, a_2 \in U$ mit $ga_1 = ga_2$ gilt auch $a_1 = a_2$, denn $a_1 = g^{-1}ga_1 = g^{-1}ga_2 = a_2$. Also ist $|gU| \geq |U|$.

Damit folgt $|gU| = |U|$. □

29.11 Beispiele

a) $(5\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$. Wir können $\mathbb{Z}$ in 5 (Links-) Nebenklassen zerlegen:

$$\begin{aligned} 0 + 5\mathbb{Z} &=: [0] \\ 1 + 5\mathbb{Z} &=: [1] \\ 2 + 5\mathbb{Z} &=: [2] \\ 3 + 5\mathbb{Z} &=: [3] \\ 4 + 5\mathbb{Z} &=: [4] \end{aligned}$$

Dies sind gerade die Kongruenzklassen (Restklassen) modulo 5 (vgl. MfI 1, Kap. 7).

b) Die alternierende Gruppe $(A_3, \circ)$ ist eine Untergruppe der symmetrischen Gruppe $(S_3, \circ)$; vgl. 29.3g, 29.7d.

$S_3 = \{\sigma_1, \sigma_2, \ldots, \sigma_6\}$ hat die Linksnebenklassen

$$\begin{aligned} A_3 &= \{\sigma_1, \sigma_2, \sigma_3\} && (= \sigma_1 A_3 = \sigma_2 A_3 = \sigma_3 A_3) \\ \sigma_4 A_3 &= \{\sigma_4, \sigma_5, \sigma_6\} && (= \sigma_5 A_3 = \sigma_6 A_3) \\ \text{denn} \quad & \sigma_4\sigma_1 = \sigma_4\ , && \sigma_5\sigma_1 = \sigma_5\ , && \sigma_6\sigma_1 = \sigma_6\ , \\ & \sigma_4\sigma_2 = \sigma_5\ , && \sigma_5\sigma_2 = \sigma_6\ , && \sigma_6\sigma_2 = \sigma_4\ , \\ & \sigma_4\sigma_3 = \sigma_6\ , && \sigma_5\sigma_3 = \sigma_4\ , && \sigma_6\sigma_3 = \sigma_5\ . \end{aligned}$$

Wie viele Nebenklassen besitzt eine Nebenklassenzerlegung von G bezüglich einer Untergruppe U?

29.12 Definition

Es sei $(U, \bullet)$ eine Untergruppe von $(G, \bullet)$. Dann bezeichnen wir die Menge aller Linksnebenklassen mit G/U (gesprochen: „*G modulo U*“), und $G : U := |G/U|$ nennt man den **Index** von U in G.

29.13 Satz von Lagrange

Es sei $(G, \bullet)$ ene endliche Gruppe mit Untergruppe $(U, \bullet)$. Dann ist die Untergruppenordnung $|U|$ ein Teiler der Gruppenordnung $|G|$, und für die Anzahl der

Linksnebenklassen gilt

$$G : U = \frac{|G|}{|U|} .$$

Beweis: Nach Satz 29.10 sind alle Nebenklassen von G bezüglich U gleich mächtig und bilden eine Partition von G. Also muss $(G : U) \cdot |U| = |G|$ gelten. Daraus folgen die Behauptungen des Satzes. □

29.14 Korollar

Ist die Ordnung von G eine Primzahl, so besitzt G nur die trivialen Untergruppen.

29.15 Beispiele

a) $|S_3| = 6$, $|A_3| = 3$
$S_3/A_3 = \{A_3, \sigma_4 A_3\}$, $S_3 : A_3 = |S_3/A_3| = 2 = \frac{6}{3}$.

b) Eine Gruppe mit 30 Elementen kann nur Untergruppen mit $1, 2, 3, 5, 6, 10, 15$ oder 30 Elementen besitzen.

29.16 Definition: Normalteiler

Eine Untergruppe $(N, \bullet)$ einer Gruppe $(G, \bullet)$, für die Links- und Rechtsnebenklassen identisch sind, d.h.

$$gN = Ng \quad \forall g \in G .$$

heißt **Normalteiler** (oder normale Untergruppe).

Bemerkung: Offensichtlich ist in einer kommutativen Gruppe $(G, \bullet)$ jede Untergruppe ein Normalteiler.

Warum sind Normalteiler wichtig? Ist die Untergruppe ein Normalteiler wird auf der Menge der Nebenklassen eine Gruppenstruktur induziert.

29.17 Satz: Faktorgruppe

Ist eine Untergruppe $(N, \bullet)$ Normalteiler von $(G, \bullet)$ Dann ist die Nebenklassenmenge G/N mit der Verknüpfung $\circ : G/N \times G/N \to G/N$ definiert als

$$(gN) \circ (hN) := (gh)N$$

eine Gruppe $(G/N, \circ)$, die sogenannte **Faktorgruppe** G nach N.

Beweis: Der wesentliche Teil des Beweises ist es zu zeigen, daß die Verknüpfung $\circ$ auf G/N wohldefiniert ist. „wohldefiniert“ heißt, daß die Verküpfung eindeutig definiert ist, d.h. unabhängig von der Wahl der Repräsentaten der Nebenklasse.

Seien $g_1, g_2 \in g_1N$, d.h. $g_1^{-1}g_2 \in N$ und $g_2^{-1}g_1 \in N$ und $h_1, h_2 \in h_1N$, d.h. $h_1^{-1}h_2 \in N$ und $h_2^{-1}h_1 \in N$. Zu zeigen ist, daß

$$(g_1N) \circ (h_1N) = (g_1h_1)N = (g_2h_2)N = (g_2N) \circ (h_2N),$$

d.h. das Ergebnis der Verknüpfung zweier Nebenklassen ist unabhängig von der Wahl des Repräsentanten.

Es gilt:

$$\begin{aligned}
g_2h_2N &= g_2h_2h_2^{-1}h_1N && (h_2^{-1}h_1^{-1} \in N \text{ und } gN = N,\ \forall\, g \in N)\\
&= g_2h_1N && (N \text{ ist Normalteiler})\\
&= g_2Nh_1 && (g_2^{-1}g_1 \in N \text{ und } gN = N,\ \forall\, g \in N)\\
&= g_2g_2^{-1}g_1Nh_1 && (N \text{ ist Normalteiler})\\
&= g_1h_1N
\end{aligned}$$

Die Assoziativität von $\circ$ folgt aus der Assoziativität der Verknüpfung von G. Das neutrale Element von G/N ist N, denn für alle $gN \in G/N$ gilt

$$gN \circ N = gN \circ eN = (ge)N = gN.$$

Das inverse Element von $gN \in G/N$ ist $g^{-1}N$, da

$$gN \circ g^{-1}N = (gg^{-1})N = eN = N.$$

29.18 Beispiel

Die Untergruppe $(5\mathbb{Z}, +)$ (vgl. 29.11a) ist Normalteiler in $(\mathbb{Z}, +)$, da $(\mathbb{Z}, +)$ eine kommutative Gruppe ist. Die Elemente von $\mathbb{Z}_5 := \mathbb{Z}/5\mathbb{Z}$ sind die *Kongruenzklassen* $[0], \ldots, [4]$.

Auf $\mathbb{Z}_5$ wird damit die Gruppenoperation durch

$$(a + 5\mathbb{Z}) + (b + 5\mathbb{Z}) := (a + b) + 5\mathbb{Z}$$

eingeführt, das heißt durch

$$[a] + [b] := [a + b] \ .$$

Dies ist gerade die Addition von Kongruenzklassen modulo 5 (*modulare Addition*, vgl. MfI 1, Kap. 7).

29.19 Definition: Abbildungen zwischen Gruppen

Es seien $(G_1, \circ)$, $(G_2, \bullet)$ Gruppen.

a) Ein **Homomorphismus** von G_1 nach G_2 ist eine Abbildung $f : G_1 \to G_2$ mit

$$\begin{array}{ccccc} f(a \circ b) & = & f(a) \bullet f(b) & & \forall a, b \in G_1 \ . \\ \uparrow & & \uparrow & & \\ \text{Verknüpfung} & & \text{Verknüpfung} & & \\ \text{in } G_1 & & \text{in } G_2 & & \end{array}$$

b) Ein injektiver Homomorphismus heißt **Monomorphismus**.

(Eine Abbildung $f : M \to N$ heißt injektiv, wenn für $x_1, x_2 \in M$, $x_1 \neq x_2$ stets $f(x_1) \neq f(x_2)$ ist, vgl. MfI 1, 5.6.)

c) Ein surjektiver Homomorphismus heißt **Epimorphismus**.

(Eine Abbildung $f : M \to N$ heißt surjektiv, wenn für jedes $y \in N$ ein $x \in M$ existiert mit $f(x) = y$, vgl. MfI 1, 5.6.)

d) Ein bijektiver Homomorphismus heißt **Isomorphismus**. Man schreibt dann $G_1 \cong G_2$.

e) Ein Homomorphismus von G_1 in sich selbst heißt **Endomorphismus**.

f) Ein Isomorphismus von G_1 in sich selbst heißt **Automorphismus**.

29.20 Beispiele

- Sei $\alpha \in \mathbb{R}$. $f : (\mathbb{R}, +) \to (\mathbb{R}, +)$, $x \mapsto \alpha x$. f ist ein Automorphismus. Es gilt für alle $x, y \in \mathbb{R}$,

$$f(x + y) = \alpha(x + y),$$
$$f(x) + f(y) = (\alpha x) + (\alpha y)$$

  Also ist f ein Homomorphismus. Man kann leicht überprüfen, daß f bijektiv ist.

- $f : (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot)$, $x \mapsto e^x$. f ist ein Monomorphismus. Es gilt für alle $x, y \in \mathbb{R}$,

$$f(x + y) = e^{(x+y)},$$
$$f(x) \cdot f(y) = e^x \cdot e^y = e^{(x+y)}$$

  f ist injektiv aber nicht surjektiv.

29.21 Definition: Bild und Kern

Es sei $f : G_1 \to G_2$ ein Homomorphismus der Gruppen G_1, G_2. Dann heißt

$$\mathrm{Im}(f) := \{f(g_1) \mid g_1 \in G_1\}$$

das **Bild** von f.

Sei ferner e_2 das neutrale Element von $(G_2, \bullet)$. Dann bezeichnet man

$$\mathrm{Ker}(f) := \{g_1 \in G_1 \mid f(g_1) = e_2\}$$

als **Kern** von f.

Warum ist der Kern eines Homomorphismus wichtig? Man kann zeigen:

29.22 Satz: Homomorphiesatz für Gruppen

Sei $f : G_1 \to G_2$ ein Homomorphismus der Gruppen G_1 und G_2. Dann ist $\mathrm{Ker}(f)$ Normalteiler von G_1, und die Faktorgruppe $G_1/\mathrm{Ker}(f)$ ist isomorph zum Bild von f:

$$G_1/\mathrm{Ker}(f) \cong \mathrm{Im}(f)\ .$$

Bemerkung: Man kann also eine nicht bijektive Abbildung zwischen Gruppen bijektiv machen, indem man zum Faktorraum übergeht, also Elemente ignoriert, die auf das neutrale Element von G_2 abgebildet werden.

30 Ringe und Körper

30.1 Motivation

- Häufig gibt es auf einer Menge zwei Verknüpfungen: eine „Addition“ und eine „Multiplikation“.
- Beispiele:
  - $(\mathbb{Z}, +, \cdot)$ – hier gibt es sogar noch eine Division mit Rest.
  - $(\mathbb{R}, +, \cdot)$ – hier gibt es auch eine Division.
- Lassen sich diese Konzepte algebraisch abstrahieren?

30.2 Definition: Ring

Eine Menge R mit zwei Verknüpfungen $+, \cdot$ auf R heißt **Ring**, wenn gilt:

a) $(R, +)$ ist eine kommutative Gruppe.

b) $(R, \cdot)$ ist eine Halbgruppe.

c) *Distributivgesetze:*

$$\left.\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (b + c) \cdot a &= (b \cdot a) + (c \cdot a) \end{aligned}\right\} \quad \forall a, b, c \in R$$

Ist $(R, \cdot)$ sogar ein Monoid, so heißt $(R, +, \cdot)$ **Ring mit Einselement**.

Gilt neben (a)–(c) noch

d) *Kommutativgesetz der Multiplikation:*

$$a \cdot b = b \cdot a \qquad \forall a, b \in R\,,$$

so heißt $(R, +, \cdot)$ **kommutativer Ring.**

30.3 Konventionen

In einem Ring $(R, +, \cdot)$ bezeichnet man häufig

- das neutrale Element der Addition als **Nullelement** (0),
- das neutrale Element der Multiplikation (sofern es existiert) als **Einselement** (1),
- das additive Inverse zu a mit $-a$,
- das multiplikative Inverse zu a (sofern es existiert) mit $\frac{1}{a}$.

Um Klammern zu sparen, vereinbart man „Punkt- vor Strichrechnung“.

30.4 Beispiele

a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.

Außerdem kann man ganze Zahlen mittels der $\leq$-Beziehung *vergleichen*. Das ermöglicht die **Division mit Rest** (vgl. MfI 1, 6.2).

Zu jeder Zahl $a \in \mathbb{Z}$ und jeder Zahl $b \in \mathbb{Z}$, $b > 0$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit

$$a = qb + r \ , \qquad 0 \leq r < b \ .$$

Man nennt q den **Quotienten** und r den **Rest** der Division von a durch b. Dabei heißt a **Dividend** und b **Divisor**.

Ist der Rest bei der Division von a durch b gleich 0, so ist a durch b **teilbar** (vgl. MfI 1, 6.3).

b) $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind ebenfalls kommutative Ringe mit Eins. Wir betrachten sie später genauer.

c) Die Menge $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ der Restklassen modulo m (wobei $m \in \mathbb{N}$) bildet mit der modularen Addition (vgl. 29.18 und MfI 1, 7.8ff.)

$$[a] + [b] := [a + b]$$

sowie der Multiplikation („modulare Multiplikation“, vgl. MfI 1, 7.12ff.)

$$[a] \cdot [b] := [a \cdot b] \qquad (*)$$

den **Restklassenring** $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$. Auch er ist kommutativ. Er besitzt das Einselement [1].

Zum Nachweis, dass die Multiplikation $(*)$ auf der Basis der Multiplikation ganzer Zahlen sinnvoll definiert ist, zeigen wir, dass das Ergebnis unabhängig davon ist, welche ganzen Zahlen aus den jeweiligen Kongruenzklassen gewählt werden: Für ganze Zahlen a, b sei $a' = a + q_1 m$ und $b' = b + q_2 m$ mit $q_1, q_2 \in \mathbb{Z}$, d. h. $a, a' \in [a] = a + m\mathbb{Z}$ (bzw. $[a'] = [a]$) und $b, b' \in [b] = b + m\mathbb{Z}$ (bzw. $[b'] = [b]$). Dann ist

$$\begin{aligned} a' \cdot b' &= (a + q_1 m) \cdot (b + q_2 m) \\ &= a \cdot b + (aq_2 + bq_1 + q_1 q_2 m)m \ , \end{aligned}$$

also $a \cdot b, a' \cdot b' \in [a \cdot b] = ab + m\mathbb{Z}$ (bzw. $[a' \cdot b'] = [a \cdot b]$). □

d) Weitere wichtige Beispiele folgen später: für kommutative Ringe (Polynomringe, Kap. 31) und für nichtkommutative Ringe (Matrizen, Kap. 35).

30.5 Satz: Unterringkriterium

Es sei $(R, +, \cdot)$ ein Ring und $S \subset R$. Dann ist $(S, +, \cdot)$ genau dann ein Ring, wenn

a) $(S, +)$ eine Untergruppe von $(R, +)$ ist (vgl. 29.6)

b) $(S, \cdot)$ abgeschlossen ist: $a \cdot b \in S \quad \forall a, b \in S$.

Beweis: analog zu Satz 29.6.

30.6 Beispiel

$(m\mathbb{Z}, +, \cdot)$ $(m \in \mathbb{N})$ ist Unterring von $(\mathbb{Z}, +, \cdot)$, denn

a) $(m\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Z}, +)$ (vgl. 29.7b)

b) $(m\mathbb{Z}, \cdot)$ ist abgeschlossen:
Für $a, b \in m\mathbb{Z}$ existieren $q_1, q_2 \in \mathbb{Z}$ mit $a = q_1 m, b = q_2 m$, also

$$ab = (q_1 m)(q_2 m) = (q_1 q_2 m)m \in m\mathbb{Z} \ .$$

30.7 Definition: Körper

Eine Menge K mit zwei Verknüpfungen $+$ und $\cdot$ auf K heißt **Körper**, wenn gilt:

a) $(K, +, \cdot)$ ist ein kommutativer Ring mit Eins.

b) *Inverse Elemente:* Zu jedem $a \in K$ mit $a \neq 0$ gibt es ein a^{-1} mit $a^{-1}a = 1$.

30.8 Bemerkungen

a) $(K, +, \cdot)$ besteht somit aus den kommutativen Gruppen $(K, +)$ und $(K \setminus \{0\}, \cdot)$, zwischen denen ein Distributivgesetz gilt.

b) Statt $K \setminus \{0\}$ schreibt man auch K^*.

c) Falls $(K^*, \cdot)$ nur eine *nichtkommutative* Gruppe ist, bezeichnet man $(K, +, \cdot)$ als **Schiefkörper** (Beispiel: Quaternionen).

d) Englische Bezeichnung für einen Körper: *field*.

30.9 Beispiele

a) $(\mathbb{Z}, +, \cdot)$ ist *kein* Körper, da zu $a \in \mathbb{Z}^*$ im Allgemeinen kein a^{-1} existiert.

b) $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.

c) $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ ist ein Körper, da $[1] \cdot [1] = [1]$ (selbstinvers). Dieser Körper hat nur die Elemente $[0]$ und $[1]$.

Weitere Beispiele folgen später.

30.10 Satz: Eigenschaften von Körpern

In einem Körper $(K, +, \cdot)$ gilt:

a) $a \cdot 0 = 0$ für alle $a \in K$

b) *Nullteilerfreiheit:* Sind $a, b \in K$ mit $a \neq 0$ und $b \neq 0$, so ist auch $a \cdot b \neq 0$. Damit gilt: $a \cdot b = 0$ genau dann, wenn $a = 0$ oder $b = 0$.

Beweis:

a) Da 0 neutrales Element für + ist, gilt

$$\begin{aligned} a \cdot 0 + 0 &= a \cdot 0 \\ &= a \cdot (0 + 0) \\ &= a \cdot 0 + a \cdot 0 \quad \text{(Distributivität)} \end{aligned}$$

Addition von $-a \cdot 0$ auf beiden Seiten ergibt die Behauptung.

b) Es seien $a \neq 0$, $b \neq 0$. Angenommen, es gilt $a \cdot b = 0$. Dann folgt

$$b = (a^{-1}a)b = a^{-1} \underbrace{(ab)}_{0} = a^{-1} \cdot 0 \overset{\text{(a)}}{=} 0$$

im Widerspruch zu $b \neq 0$. □

Bemerkung:

- In Körpern kann man außer Addition und Multiplikation auch Subtraktion und Division definieren.

$$\begin{aligned} a - b &:= a + (-b) \quad \text{für alle } a, b \in K, \\ \frac{a}{b} &:= a \cdot b^{-1}, \quad \text{für alle } a, b \in K \text{ mit } b \neq 0. \end{aligned}$$

- Satz 30.10a impliziert, dass man in Körpern nicht durch 0 dividieren darf: $q := \frac{a}{b}$ bedeutet $a = q \cdot b$. Gilt hierin $b = 0$, so folgt $a = 0$. Für $a = 0$ ist jedoch $a = q \cdot b$ für jedes $q \in K$ erfüllt. Also ist auch der Ausdruck $\frac{0}{0}$ sinnlos.

30.11 Der Körper der komplexen Zahlen

Hier wird nur das Nötigste angegeben – ausführlich werden komplexe Zahlen in MfI 1, Kap. 9 behandelt.

Definition: Es sei $\mathbb{C} := \{(a,b) \mid a,b \in \mathbb{R}\}$, und wir führen auf $\mathbb{C}$ folgende Operationen ein:

a) *Addition:*
$$(a,b) + (c,d) := (a+c, b+d) \quad \forall a,b,c,d \in \mathbb{R}$$

b) *Multiplikation:*
$$(a,b) \cdot (c,d) := (ac - bd, ad + bc) \quad \forall a,b,c,d \in \mathbb{R} \; .$$

Dann ist $(\mathbb{C}, +, \cdot)$ ein Körper mit dem Nullelement $(0,0)$ und dem Einselement $(1,0)$.

Eigenschaften:

a) **Einbettung von R:** Die Teilmenge $\{(a,0) \mid a \in \mathbb{R}\}$ ist bezüglich Addition und Multiplikation abgeschlossen und isomorph dem Körper $(\mathbb{R}, +, \cdot)$. Man identifiziert daher $(a,0)$ mit der reellen Zahl a.

b) **Imaginäre Einheit:** $\mathrm{i} := (0,1)$. Es gilt $\mathrm{i}^2 = -1$.

c) Damit lassen sich komplexe Zahlen darstellen als
$$(a,b) = a + \mathrm{i}b \quad \forall a,b \in \mathbb{R} \; .$$

d) Es sei $z := a + \mathrm{i}b$. Dann heißt a **Realteil**, b **Imaginärteil** von z. Man schreibt
$$a = \mathrm{Re}\, z \; , \qquad\qquad b = \mathrm{Im}\, z \; .$$
$\bar{z} := a - \mathrm{i}b$ heißt **konjugiertes Element** zu z.

e) $|z| := \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$ heißt **Betrag** der komplexen Zahl $z = a + \mathrm{i}b$.

f) $z^{-1} = \frac{\bar{z}}{|z|^2}$ (inverses Element)

g) *Division* mithilfe des komplex Konjugierten:
$$\begin{aligned} \frac{a+\mathrm{i}b}{c+\mathrm{i}d} &= \frac{a+\mathrm{i}b}{c+\mathrm{i}d} \cdot \frac{c-\mathrm{i}d}{c-\mathrm{i}d} \\ &= \frac{(ac+bd) + \mathrm{i}(bc-ad)}{c^2+d^2} \\ &= \frac{ac+bd}{c^2+d^2} + \mathrm{i}\frac{bc-ad}{c^2+d^2} \; . \end{aligned}$$

30.12 Endliche Körper

a) Der Restklassenring $(\mathbb{Z}_m, +, \cdot)$ (vgl. 30.4c) ist ein Körper dann und nur dann, wenn er nullteilerfrei ist. Man kann zeigen, dass dies genau dann der Fall ist, wenn m eine Primzahl ist (vgl. MfI 1, 7.17).

b) Allgemein heißt ein endlicher Körper mit q Elementen **Galoisfeld** (nach Evariste Galois, 1811–1832).

Man kann zeigen: Für $q \in \mathbb{N}$ gibt es ein Galoisfeld genau dann, wenn $q = p^m$ mit einer Primzahl p und einer natürlichen Zahl m. Für jedes solche q ist das zugehörige Galoisfeld bis auf Isomorphie eindeutig bestimmt und wird mit $\mathrm{GF}(q)$ bezeichnet.

Es gilt also für Primzahlen p:

$$\mathrm{GF}(p) = \mathbb{Z}_p \ .$$

31 Polynomringe

31.1 Motivation

Polynome spielen eine wichtige Rolle in vielen Berechnungen, einerseits weil oftmals funktionale Zusammenhänge durch Polynome beschrieben werden, andererseits weil Polynome oft zur Annäherung anderer Funktionen verwendet werden (vgl. Satz von Taylor, MfI 1, Kap. 20).

Polynomringe gehören damit zu den wichtigsten Ringen.

31.2 Definition: Polynomringe

Es sei $(R, +, \cdot)$ ein Ring (z. B. $R = \mathbb{R}$) und $a_0, a_1, \ldots, a_n \in R$. Wir setzen zur Abkürzung

$$x^k := \underbrace{x \cdot x \cdot \ldots \cdot x}_{k \text{ Faktoren}}$$

und verwenden das Summenzeichen analog zur Addition reeller Zahlen auch für die Addition in R.

Dann nennen wir die Abbildung

$$p : R \to R\,, \qquad\qquad x \mapsto \sum_{k=0}^{n} a_k x^k$$

Polynom (über R). $a_0, \ldots, a_n$ heißen **Koeffizienten** von p. Ist $a_n \neq 0$, so heißt n der **Grad** von p, symbolisch $n = \deg(p)$. (Für $p(x) = 0$ definiert man $\deg(p) = -\infty$.)

Beispiel: $p(x) = 5x^3 - 1{,}3x + 6$ ist ein Polynom vom Grad 3 über $\mathbb{R}$.

Die Menge aller Polynome über R nennen wir $R[x]$.

Auf $R[x]$ definieren wir eine Addition und eine Multiplikation „punktweise“ durch

$$\left.\begin{aligned}(p+q)(x) &:= p(x) + q(x)\\ (p \cdot q)(x) &:= p(x) \cdot q(x)\end{aligned}\right\} \quad \forall p, q \in R[x]\,.$$

Dann ist $(R[x], +, \cdot)$ ein Ring, der **Polynomring** über R.

Der Nachweis der Ringeigenschaften ist aufwändig. Man verwendet, dass für

$$p(x) = \sum_{k=0}^{n} a_k x^k \ , \qquad\qquad q(x) = \sum_{k=0}^{n} b_k x^k$$

gilt

$$(p+q)(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$$

$$(p \cdot q)(x) = \sum_{k=0}^{2n} \left(\sum_{\substack{i+j=k \\ 0 \le i,j \le n}} a_i b_j \right) x^k \ .$$

Dabei wurde $n := \max(\deg(p), \deg(q))$ gesetzt (und ggf. die Koeffizienten des Polynoms niedrigeren Grades mit Nullen ergänzt).

31.3 Das Horner-Schema

Häufig müssen Funktionswerte von Polynomen effizient berechnet werden. Eine *naive* Auswertung eines Polynoms

$$p(x) = 5x^7 + 4x^6 - 3x^5 + 4x^4 + 6x^3 - 7x^2 + 4x - 1$$

erfordert 7 Additionen und $7 + 6 + 5 + 4 + 3 + 2 + 1 = 28$ Multiplikationen.

Wesentlich effizienter ist das **Horner-Schema**, das eine geschickte Klammerung ausnutzt:

$$p(x) = ((((((5x + 4)x - 3)x + 4)x + 6)x - 7)x + 4)x - 1 \ .$$

Arbeitet man die Klammern von innen nach außen ab, so benötigt man nur 7 Additionen und 7 Multiplikationen.

Allgemein benötigt man zur naiven Auswertung eines Polynoms n-ten Grades n Additionen und $\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$ Multiplikationen. Das Horner-Schema reduziert den Aufwand auf n Additionen und n Multiplikationen.

In den Abschnitten 31.4–31.13 beschäftigen wir uns ausschließlich mit dem Polynomring $\mathbf{R}[x]$.

31.4 Polynomdivision in $\mathbb{R}[x]$

Im Ring $(\mathbb{Z}, +, \cdot)$ gibt es die Division mit Rest (vgl. 30.4a sowie MfI 1, Kap. 6). Kann man Ähnliches auch im Polynomring $(\mathbb{R}[x], +, \cdot)$ tun? (Achtung: Hier betrachten wir ausschließlich $R = \mathbb{R}$.)

Man kann zeigen:

Satz: Zu $a, b \in \mathbb{R}[x]$ mit $b \neq 0$ gibt es eindeutig bestimmte Polynome $q, r \in \mathbb{R}[x]$ mit

$$a = qb + r \qquad \text{und} \quad \deg(r) < \deg(b) \ .$$

Quotient, Rest, Dividend, Divisor werden definiert wie in 30.4a.

Definition: Ist der Rest der Division von a durch b gleich 0, so ist das Polynom a durch das Polynom b teilbar. (b teilt a, b ist Teiler von a.)

31.5 Praktische Durchführung der Polynomdivision

Analog zur schriftlichen Division natürlicher Zahlen

$$\begin{array}{rl}
 & \rightarrow \text{ 7 geht } 5\times \text{ in } 36 \\
365 & : \ 7 \ = \ 52 \quad \text{Rest} \ \ 1 \\
-\underline{35} & \leftarrow 5 \cdot 7 = 35 \\
15 & \\
-\underline{14} & \\
1 &
\end{array}$$

führt man die Polynomdivision durch:

$$\begin{array}{l}
\qquad \longrightarrow x^4 : x^2 = x^2 \longrightarrow \\
(x^4 + 2x^3 + 3x^2 + 4x + 5) \qquad : (x^2+1) = x^2 + 2x + 2 \quad \text{Rest} \ \ 2x+3 \\
-\underline{(x^4 \qquad + \ x^2)} \ \longleftarrow x^2 \cdot (x^2+1) = x^4 + x^2 \\
\qquad 2x^3 + 2x^2 + 4x \\
\quad -\underline{(2x^3 \qquad + 2x)} \\
\qquad\qquad 2x^2 + 2x + 5 \\
\qquad\quad -\underline{(2x^2 \qquad + 2)} \\
\qquad\qquad\qquad 2x + 3
\end{array}$$

Satz 31.4 hat zwei wichtige Folgerungen.

31.6 Satz: Abspaltung von Nullstellen

Hat $p \in \mathbb{R}[x]$ die **Nullstelle** x_0 (d. h. $p(x_0) = 0$), so ist p durch das Polynom $x - x_0$ ohne Rest teilbar.

Beweis: Nach Satz 31.4 existieren für $p(x)$ und $b(x) = x - x_0$ die Polynome $q(x), r(x)$ mit

$$p(x) = q(x)b(x) + r(x) \ , \quad \deg(r) < \deg(b) \ .$$

In x_0 gilt dann

$$0 = p(x_0) = q(x_0) \cdot \underbrace{b(x_0)}_{=0} + r(x_0) \ . \qquad (*)$$

Wegen $\deg(r) < \deg(b) = 1$ folgt $\deg(r) \leq 0$, also $r(x) = a_0$. Wegen $(*)$ ist $r(x) = r(x_0) = 0$. □

31.7 Satz: Anzahl der Nullstellen

Ein von 0 verschiedenes Polynom $p \in \mathbb{R}[x]$ vom Grad n hat höchstens n Nullstellen.

Beweis: Angenommen, p hat mehr als n Nullstellen. Sukzessives Abspalten der Nullstellen $x_1, x_2, \ldots, x_n$ (aufgrund der Nullteilerfreiheit des Körpers $\mathbb{R}$) ergibt

$$\exists q \in \mathbb{R}[x] : \quad p(x) = (x - x_1)(x - x_2) \cdot \ldots \cdot (x - x_n)q(x)$$

Dabei hat $q(x)$ den Grad 0, sonst wäre $\deg(p) > n$, also ist $q(x) = a_0$.

Es sei nun x_{n+1} eine weitere Nullstelle, d. h.

$$0 = p(x_{n+1}) = (x_{n+1} - x_1)(x_{n+1} - x_2) \cdot \ldots \cdot (x_{n+1} - x_n) \cdot a_0 \ .$$

Aufgrund der Nullteilerfreiheit von $\mathbb{R}$ ist einer der Faktoren $(x_{n+1} - x_1), \ldots, (x_{n+1} - x_n), a_0$ gleich 0. Wegen $p(x) \neq 0$ kann $a_0 = 0$ nicht gelten.

Also stimmt x_{n+1} mit einem der $x_1, \ldots, x_n$ überein. □

Im Ring $(\mathbb{Z}, +, \cdot)$ gibt es die Begriffe der Teilbarkeit und des größten gemeinsamen Teilers (vgl. MfI 1, Kap. 6). Diese lassen sich auch für Polynomringe formulieren.

Teilbarkeit wurde bereits in 31.4 eingeführt.

31.8 Definition: größter gemeinsamer Teiler

Es seien $a, b \in \mathbb{R}[x]$. Ein Polynom $p \in \mathbb{R}[x]$ heißt **gemeinsamer Teiler** von a und b, falls p sowohl a als auch b teilt. p heißt **größter gemeinsamer Teiler** von a und b, falls p außerdem durch jeden gemeinsamen Teiler von a und b teilbar ist (Schreibweise: $p = \mathrm{ggT}(a, b)$).

Für eine effiziente Berechnung des ggT nutzen wir folgende Eigenschaften des ggT aus:

Lemma: Eigenschaften des ggT (vgl. MfI 1, Lemma 6.11 für ganze Zahlen)
Es seien $a, b, q \in \mathbb{R}[x]$. Dann gilt:

a) $d = \mathrm{ggT}(a, b)$ genau dann, wenn $d = \mathrm{ggT}(b, a - qb)$.

b) Ist $a = qb$, so gilt $b = \mathrm{ggT}(a, b)$.

31.9 Euklidischer Algorithmus zur ggT-Bestimmung von Polynomen

(Euklidischer Algorithmus für ganze Zahlen: MfI 1, 6.12)

Für die Polynome $a, b \in \mathbb{R}[x]$ mit $\deg(a) \geq \deg(b)$ setzen wir $r_0 := a$, $r_1 := b$ und führen sukzessive Polynomdivisionen aus:

$$\begin{aligned}
r_0 &= q_0 r_1 + r_2 \ , & \deg(r_2) &< \deg(r_1) \ , \\
r_1 &= q_1 r_2 + r_3 \ , & \deg(r_3) &< \deg(r_2) \ , \\
&\vdots & &\vdots \\
r_{n-2} &= q_{n-2} r_{n-1} + r_n \ , & \deg(r_n) &< \deg(r_{n-1}) \ , \\
r_{n-1} &= q_{n-1} r_n \ . &&
\end{aligned}$$

Dann ist $r_n = \mathrm{ggT}(a, b)$.

Beispiel:

$$a(x) = x^4 + x^3 - x^2 + x + 2$$
$$b(x) = x^3 + 2x^2 + 2x + 1$$

Polynomdivisionen:

$$(x^4 + x^3 - x^2 + x + 2) = (x - 1)(x^3 + 2x^2 + 2x + 1) + (-x^2 + 2x + 3)$$
$$(x^3 + 2x^2 + 2x + 1) = (-x - 4)(-x^2 + 2x + 3) + (13x + 13)$$
$$(-x^2 + 2x + 3) = \left(-\frac{1}{13}\,x + \frac{3}{13}\right)(13x + 13)\ .$$

Also ist $\mathrm{ggT}(a(x), b(x)) = 13x + 13$. (Eindeutig nur bis auf Vielfache: Jedes Polynom $c(13x + 13)$ mit einer Konstanten $c \neq 0$ ist ebenfalls ggT.)

Gibt es in Polynomringen eine Entsprechung zu *Primzahlen* und *Primfaktorenzerlegung* in ganzen Zahlen (vgl. MfI 1, 6.3/6.6)?

31.10 Definition

Es sei K ein Körper. Ein nichtkonstantes Polynom $p \in K[x]$ heißt **reduzibel** über K, falls es Polynome $a, b \in R[x]$ mit $\deg(a) > 0$, $\deg(b) > 0$ (nichtkonstante Polynome) gibt mit $p = a \cdot b$. Andernfalls heißt p **irreduzibel** über K.

31.11 Beispiele

a) $x^2 - 3$ ist irreduzibel $\mathbb{Q}$, aber reduzibel über $\mathbb{R}$:

$$x^2 - 3 = \left(x + \sqrt{3}\right)\left(x - \sqrt{3}\right)\ .$$

b) $x^2 + 1$ ist irreduzibel über $\mathbb{R}$ aber reduzibel über $\mathbb{C}$, da

$$x^2 + 1 = (x - i)(x + i).$$

c) Lineare Polynome $x - a$ mit $a \in K$ sind immer irreduzibel.

31.12 Irreduzible Polynome als „Primfaktoren“ in $\mathbb{R}[x]$

Irreduzible Polynome in $(\mathbb{R}[x], +, \cdot)$ haben ähnliche Eigenschaften wie Primfaktoren in $(\mathbb{Z}, +, \cdot)$. So existiert z. B. eine „Primfaktorzerlegung“:

Jedes nichtkonstante Polynom $p \in \mathbb{R}[x]$ lässt sich als Produkt irreduzibler Polynome aus $\mathbb{R}[x]$ darstellen. Die Darstellung ist bis auf die Reihenfolge der irreduziblen Polynome und bis auf Multiplikation mit konstanten Polynomen eindeutig.

31.13 Beispiel

$p(x) = x^3 - x^2 + x - 1$ hat in $\mathbb{R}[x]$ die folgende Zerlegung in irreduzible Polynome:

$$p(x) = (x^2 + 1)(x - 1)$$

Äquivalent hierzu sind z. B.

$$p(x) = (x - 1)(x^2 + 1) = (4x - 4)\left(\frac{1}{4}\,x^2 + \frac{1}{4}\right) .$$

Generell kann man zeigen, dass es über $\mathbb{R}$ nur zwei Typen irreduzibler Polynome gibt:

a) lineare Polynome,

b) quadratische Polynome $ax^2 + bx + c$ mit $b^2 - 4ac < 0$.

Die Bedingung $b^2 - 4ac < 0$ ist gerade die Bedingung, daß das Polynom $ax^2 + bx + c$ keine Nullstelle in $\mathbb{R}$ hat. Andernfalls wäre mit Satz 31.6 das Polynom reduzibel.

31.14 Polynomringe über allgemeinen Körpern

Das Horner-Schema (31.3) sowie die in den Abschnitten 31.4–31.13 für $\mathbb{R}[x]$ gewonnenen Resultate

- Polynomdivision
- Abspaltung von Nullstellen
- Anzahl der Nullstellen eines Polynoms n-ten Grades
- Teilbarkeit, gemeinsame Teiler, ggT, Euklidischer Algorithmus
- Primfaktorzerlegung

gelten allgemein für jeden Polynomring $K[x]$ über einem Körper K. Die Beweise verlaufen identisch.

31.15 Beispiele

a) Wir betrachten den Polynomring über dem Körper $(\mathbb{Z}_5, +, \cdot)$. Das Polynom

$$p(x) = 4x^2 + 3x - 1$$

hat wegen

$$\begin{aligned}
p([0]) &= [4] \cdot [0]^2 + [3] \cdot [0] - [1] = [4] \\
p([1]) &= [4] \cdot [1]^2 + [3] \cdot [1] - [1] = [1] \\
p([2]) &= [4] \cdot [2]^2 + [3] \cdot [2] - [1] = [1] \\
p([3]) &= [4] \cdot [3]^2 + [3] \cdot [3] - [1] = [4] \\
p([4]) &= [4] \cdot [4]^2 + [3] \cdot [4] - [1] = [0]
\end{aligned}$$

in $\mathbb{Z}_5$ genau eine Nullstelle, nämlich $[4]$.

b) Abspalten der Nullstelle durch Polynomdivision in $(\mathbb{Z}_5, +, \cdot)$:

$$\begin{array}{rl}
([4]x^2 + [3]x - [1]) & : (x - [4]) \quad = [4]x + [4] \\
-(\underline{[4]x^2 - [1]x}\,) & \\
\qquad [4]x - [1] & \\
\qquad -(\underline{[4]x + [4]}) & \\
\qquad\qquad [0] &
\end{array}$$

Also ist

$$[4]x^2 + [3]x - [1] = (x - [4])([4]x + [4]) = [4](x - [4])^2 = [4](x + [1])^2 \quad \text{in } \mathbb{Z}_5.$$

31.16 Anwendung: Fehlerkorrektur in der Datenübertragung

Bei der Übertragung binärer Daten können Bits „umklappen“.

Einfachste Abhilfe zur Fehlererkennung: Einführung von zusätzlichen Prüfbits.

Beispiel: Ein Datenblock von 1 Byte wird übertragen; es wird ein Prüfbit angehängt, das die Summe der Bits modulo 2 angibt:

$$\underbrace{1\ 1\ 0\ 0\ 1\ 1\ 0\ 1}_{\text{Byte (Daten)}}\ \Big|\ \underbrace{1}_{\text{Prüfbit}}$$

Empfängt man beispielsweise 11011101|1, muss ein Fehler aufgetreten sein.

Nachteile:

- Man muss 1/8 mehr Daten übertragen.
- Kein Fehler wird festgestellt, wenn 2 Bits umklappen.

Sicherung mittels Polynomdivision in $\mathbb{Z}_2$: Alternativ kann man wie folgt vorgehen:

1. Interpretiere die Bits eines zu übertragenden Datenblocks als Koeffizienten eines Polynoms $f(x) \in \mathbb{Z}_2[x]$.

   Beispiel: Byte als Datenblock: 11001101
   Polynom: $f(x) = x^7 + x^6 + x^3 + x^2 + 1$

2. Ein festes „Generatorpolynom“ $g(x) \in \mathbb{Z}_2[x]$ mit $\deg(g) = n$ dient als Divisor. Typischerweise ist $\deg(g) \ll \deg f$.

3. Betrachte statt $f(x)$ das Polynom $h(x) = x^n \cdot f(x)$.

   (Das heißt: an die Bitfolge zu $f(x)$ werden n Nullen angehängt.)

   Beispiel ($n = 4$):

$$\overbrace{\underbrace{1\ 1\ 0\ 0\ 1\ 1\ 0\ 1}_{f(x)}\ |\ \underbrace{0\ 0\ 0\ 0}_{\cdot x^n}}^{h(x)}$$

4. Berechne die Polynomdivision $h(x) : g(x)$ in $\mathbb{Z}_2[x]$:

$$h(x) = q(x)g(x) + r(x) \ , \quad \deg(r) < n \ .$$

5. Sende $h(x) - r(x) = q(x)g(x)$. (In $\mathbb{Z}_2[x]$ ist dies auch gleich $h(x) + r(x)$.)

   Wegen $\deg(r) < n$ unterscheiden sich $h(x) - r(x)$ und $h(x)$ höchstens in den letzten n Bits:

$$\overbrace{\underbrace{1\,1\,0\,0\,1\,1\,0\,1}_{f(x)} \mid \underbrace{?\,?\,?\,?}_{r(x)}}^{h(x)-r(x)}$$

   $r(x)$ dient der Fehlererkennung.

6. Der Empfänger erhält das Polynom $p(x)$.

   Tritt bei Division durch $g(x)$ ein Rest auf, so ist $p(x) \neq h(x) - r(x)$, es ist also ein Übertragungsfehler aufgetreten.

Bei geschickter Wahl von $g(x)$

- ist es sehr unwahrscheinlich, dass bei einem Übertragungsfehler die Division $p(x) : g(x)$ ohne Rest aufgeht
- kann man anhand des Divisionsrestes den Fehler lokalisieren und korrigieren.

Konkrete Spezifikation im X.25-Übertragungsprotokoll:

- Datenblock: 4 096 Byte = 32 768 Bit
  $\Rightarrow \deg(f) = 32\,767$.
- Generatorpolynom: $g(x) = x^{16} + x^{12} + x^5 + 1$
  $\Rightarrow \deg(g) = 16$ (2 Byte zur Fehlerkorrektur)

Es werden nur $\frac{2}{4096} \approx 0{,}49$ Promille zusätzliche Daten übertragen. Erkannt werden unter Anderem alle 1-, 2- und 3-Bit-Fehler sowie alle Fehler mit ungerader Anzahl umgeklappter Bits.

Die Algorithmen zur Polynomdivision in $\mathbb{Z}_2[x]$ lassen sich effizient in Soft- und Hardware realisieren.

32 Boolesche Algebren

32.1 Motivation

- Ring- und Körperdefinition beschreiben nicht die einzigen sinnvollen Möglichkeiten, wie zwei Verknüpfungen auf derselben Menge zusammenwirken können.
  - Operationen auf Mengen: Vereinigung $\cup$, Durchschnitt $\cap$, Komplementbildung $\complement$ (vgl. MfI 1, Kap. 1)
  - Operationen auf logischen Ausdrücken: Disjunktion (ODER) $\vee$, Konjunktion (UND) $\wedge$, Negation (NICHT) $\neg$ (vgl. MfI 1, Kap. 2)

  Beide Beispiele folgen ähnlichen Gesetzen.
- Liegt eine gemeinsame algebraische Struktur vor?
- Gibt es weitere wichtige Beispiele hierfür?

32.2 Definition

Eine Menge M bildet mit zwei algebraischen Verknüpfungen $+$ und $\cdot$ sowie einer einstelligen Operation $\neg$ (einer Abbildung von M in M) eine **boolesche Algebra** $(M, +, \cdot, \neg)$, wenn gilt:

a) *Kommutativgesetze:*

$$\left.\begin{array}{c} a+b=b+a \\ a\cdot b=b\cdot a \end{array}\right\} \quad \forall a,b \in M$$

b) *Assoziativgesetze:*

$$\left.\begin{array}{c} (a+b)+c=a+(b+c) \\ (a\cdot b)\cdot c=a\cdot(b\cdot c) \end{array}\right\} \quad \forall a,b,c \in M$$

c) *Distributivgesetze:*

$$\left.\begin{array}{l} a\cdot(b+c)=(a\cdot b)+(a\cdot c) \\ a+(b\cdot c)=(a+b)\cdot(a+c) \end{array}\right\} \quad \forall a,b,c \in M$$

d) *Neutrale Elemente:* Es gibt Elemente $0 \in M$ (Nullelement) und $1 \in M$ (Einselement) mit

$$\left.\begin{aligned} 0 + a &= a \\ 1 \cdot a &= a \end{aligned}\right\} \quad \forall a \in M$$

e) *Komplementäre Elemente:*

$$\left.\begin{aligned} a + (\neg a) &= 1 \\ a \cdot (\neg a) &= 0 \end{aligned}\right\} \quad \forall a \in M$$

Wir nennen $\neg a$ das zu a **komplementäre Element.**

Bemerkung:

- $(M, +)$ und $(M, \cdot)$ sind kommutative Monoide
- Es existiert kein inverses Element ! Das heißt die übliche Argumentation aus $a + b = a + c$ folgt $b = c$ durch Addition des inversen Elements $-a$ funktioniert nicht.

32.3 Beispiel 1: Operationen auf Mengen

Es sei M eine Menge, $\mathcal{P}(M)$ ihre Potenzmenge (also die Menge aller Teilmengen von M) und $\complement$ die Komplementbildung. Dann ist $(\mathcal{P}(M), \cup, \cap, \complement)$ eine boolesche Algebra mit $\emptyset$ als Nullelement und M als Einselement:

a) Vereinigung und Durchschnittsbildung von Mengen sind kommutativ und assoziativ (vgl. MfI 1, 1.6).

b) Vereinigung und Durchschnittsbildung von Mengen erfüllen die Distributivgesetze

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

für alle Mengen A, B, C (vgl. MfI 1, 1.6).

c) Es gilt (beachte: $A \in \mathcal{P}(M)$ bedeutet dasselbe wie $A \subset M$!)

$$\emptyset \cup A = A \qquad \forall A \subset M$$
$$M \cap A = A \qquad \forall A \subset M$$

d) Für $A \subset M$ und $\complement A := \bar{A} := M \setminus A$ gilt

$$A \cup \bar{A} = M$$
$$A \cap \bar{A} = \emptyset \, .$$

32.4 Aussagenlogik

Aussagen: Sätze (in natürlicher oder formalisierter Sprache), denen eindeutig einer der Wahrheitswerte wahr (1) oder falsch (0) zugeordnet werden kann (vgl. MfI 1, 2.3)

ODER-Verknüpfung (Disjunktion): Sind A und B zwei Aussagen, so ist $A \vee B$ (A ODER B) eine Aussage, die genau dann wahr ist, wenn wenigstens eine der Aussagen A und B wahr ist, ansonsten falsch.

UND-Verknüpfung (Konjunktion): Sind A und B zwei Aussagen, so ist $A \wedge B$ (A UND B) eine Aussage, die genau dann wahr ist, wenn sowohl A als auch B wahr ist, ansonsten falsch.

Negation: Ist A eine Aussage, so ist $\neg A$ eine Aussage, die genau dann wahr ist, wenn A falsch ist.

Die Menge aller Aussagen bildet zusammen mit den Operationen $\vee$, $\wedge$ und $\neg$ eine boolesche Algebra. Die logische Konstante falsch stellt darin das Nullelement dar, die Konstante wahr das Einselement.

a) Kommutativität, Assoziativität und Distributivgesetze gelten (vgl. MfI 1, 2.8)

b) Neutrale Elemente:

$$0 \vee A = A \, , \qquad 1 \wedge A = A \qquad \forall A$$

c) Komplementäre Elemente:

$$A \vee \neg A = 1 \qquad \text{(Satz vom ausgeschlossenen Dritten)}$$
$$A \wedge \neg A = 0 \qquad \text{(Satz vom Widerspruch)}$$

(Konvention: $\neg$ hat höhere Priorität als $\vee$ und $\wedge$ / vgl. MfI 1, 2.8)

32.5 Satz: Einige Eigenschaften boolescher Algebren

Es sei $(M, +, \cdot, \neg)$ eine boolesche Algebra. Dann gilt:

a)
$$\left.\begin{aligned} a &= a + a \\ a &= a \cdot a \end{aligned}\right\} \quad \forall a \in M$$

b)
$$\left.\begin{aligned} 1 + a &= 1 \\ 0 \cdot a &= 0 \end{aligned}\right\} \quad \forall a \in M$$

c) Aus $a + b = 1$ und $b \cdot a = 0$ folgt $b = \neg a$ (Eindeutigkeit des Komplements).

d) $\neg(\neg a) = a \quad \forall a \in M$

e) Regeln von de Morgan:
$$\left.\begin{aligned} \neg(a + b) &= (\neg a) \cdot (\neg b) \\ \neg(a \cdot b) &= (\neg a) + (\neg b) \end{aligned}\right\} \quad \forall a, b \in M$$

Beweis: In der Vorlesung wurden alle Eigenschaften bewiesen - hier beweisen wir nur exemplarisch a) und c).

- Es gilt für alle $a \in M$,
$$a \overset{\text{(iv)}}{=} a + 0 \overset{(v)}{=} a + (a \cdot \neg a) \overset{\text{(iii)}}{=} (a + a) \cdot (a + \neg a) \overset{\text{(v)}}{=} (a + a) \cdot 1 \overset{\text{(iv)}}{=} a + a$$
$$a \overset{\text{(iv)}}{=} a \cdot 1 \overset{(v)}{=} a \cdot (a + \neg a) \overset{\text{(iii)}}{=} (a \cdot a) + (a \cdot \neg a) \overset{\text{(v)}}{=} a \cdot a + 0 \overset{\text{(iv)}}{=} a \cdot a$$

- Sei $b \neq \neg a$ mit $a + b = 1$ und $a \cdot b = 0$. Dann gilt
$$b \overset{\text{(iv)}}{=} b \cdot 1 \overset{(v)}{=} b \cdot (a + \neg a) \overset{\text{(iii)}}{=} (b \cdot a) + (b \cdot \neg a) \overset{\text{Annahme}}{=} 0 + (b \cdot \neg a)$$
$$\overset{\text{(v)}}{=} (a \cdot \neg a) + (b \cdot \neg a) \overset{\text{(iii)}}{=} (a + b) \cdot \neg a \overset{\text{Annahme}}{=} \neg a \cdot 1 \overset{\text{(iv)}}{=} \neg a$$

  Dies ist ein Widerspruch zur Annahme $b \neq a$. Damit folgt die Behauptung.

32.6 Satz: Zusammenhang zwischen Boolescher Algebra und Booleschem Ring

1. Sei $(B, \oplus, \odot, \neg, 0, 1)$ eine Boolesche Algebra. Wir definieren

$$x + y := (x \oplus y) \odot \neg(x \odot y),$$
$$x \cdot y := x \odot y.$$

   Dann ist $(B, +, \cdot)$ ein kommutativer Ring mit 1 als Einselement in dem $x^2 = x$ (idempotent) für alle $x \in B$ gilt. Ein solcher Ring heißt **Boolescher Ring**.

2. Sei $(B, +, \cdot)$ ein kommutativer Ring mit Eins in dem $x^2 = x$ für alle $x \in B$ gilt, d.h. $(B, +, \cdot)$ ist ein Boolescher Ring. Wir definieren

$$x \oplus y := x + y + x \cdot y,$$
$$x \odot y := x \cdot y,$$
$$\neg x := 1 + x.$$

   Dann ist $(B, \oplus, \odot, \neg, 0, 1)$ eine Boolesche Algebra.

Man kann sich leicht einen Überblick über alle endlichen booleschen Algebren verschaffen:

32.7 Satz: Endliche boolesche Algebren

a) Jede endliche boolesche Algebra ist isomorph zur booleschen Algebra der Teilmengen einer endlichen Menge.

b) Endliche boolesche Algebren haben immer 2^n Elemente mit einem $n \in \mathbb{N}$.

c) Zwei endliche boolesche Algebren mit der gleichen Anzahl an Elementen sind isomorph.

D: Lineare Algebra

33 Vektorräume

33.1 Motivation

- Im $\mathbb{R}^2$ (Ebene) und $\mathbb{R}^3$ (Raum) kann man Vektoren addieren und mit einem Skalar multiplizieren.
- Ziel: Grundkonzepte algebraisch formalisieren, um sie auch auf andere Situationen anwenden zu können
- Anwendungen z. B. in der Codierungstheorie, Robotik, Computergrafik, Computer Vision

33.2 Definition

Es sei K ein Körper. Ein **K-Vektorraum** ist eine Menge V, auf der eine Verknüpfung $+ : V \times V \to V$ und eine **skalare Multiplikation** $\cdot : K \times V \to V$ definiert sind mit

a) $(V, +)$ ist eine kommutative Gruppe.

b) $\lambda(\mu v) = (\lambda\mu)v \qquad \forall \lambda, \mu \in K,\ \forall v \in V$

c) $1 \cdot v = v \qquad \forall v \in V$

d) $\lambda(v + w) = \lambda v + \lambda w \qquad \forall \lambda \in K,\ \forall v, w \in V$

e) $(\lambda + \mu)v = \lambda v + \mu v \qquad \forall \lambda, \mu \in K,\ \forall v \in V.$

Die Elemente von V heißen **Vektoren,** die Elemente von K heißen **Skalare.** Das neutrale Element der Gruppe $(V, +)$ heißt **Nullvektor** $\vec{0}$. Ist $K = \mathbb{R}$ oder $K = \mathbb{C}$, so sprechen wir von einem **reellen** bzw. **komplexen Vektorraum.**

Bemerkung:

- Es wird keine Unterscheidung in den Bezeichnungen zwischen der + und ·-Operation im Körper K und der Vektorraumaddition und der skalaren Multiplikation gemacht.
- Für Skalare verwenden wir meist kleine griechische Buchstaben wie λ, μ, ν. Vektoren bezeichnen wir mit kleinen lateinischen Buchstaben wie u, v, w. Nur wenn Verwechslungsgefahr besteht, verwenden wir Pfeile, z. B. wenn es erforderlich ist, den Nullvektor $\vec{0} \in V$ von der skalaren Null $0 \in K$ zu unterscheiden.

33.3 Satz: Rechenregeln für Vektorräume

In einem K-Vektorraum V gilt

a) $\lambda \cdot \vec{0} = \vec{0} \quad \forall \lambda \in K$

b) $0 \cdot v = \vec{0} \quad \forall v \in V$

c) $(-1) \cdot v = -v \quad \forall v \in V$

Beweis von (a):

$$\begin{aligned} \lambda \cdot \vec{0} &= \lambda \cdot (\vec{0} + \vec{0}) && \text{(wegen } \vec{0} = \vec{0} + \vec{0}) \\ &= \lambda \cdot \vec{0} + \lambda \cdot \vec{0} && \text{(wegen 33.2e)} \end{aligned}$$

Addition von $-\lambda \cdot \vec{0}$ auf beiden Seiten ergibt die Behauptung. □

33.4 Beispiele

a) Die Menge

$$\mathbb{R}^n = \left\{ \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \;\middle|\; u_1, \ldots, u_n \in \mathbb{R} \right\}$$

ist ein $\mathbb{R}$-Vektorraum für jedes $n \in \mathbb{N}$ mit

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} + \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix}, \qquad \lambda \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} \lambda u_1 \\ \vdots \\ \lambda u_n \end{pmatrix}.$$

b) $\mathbb{C}^n$ ist ein $\mathbb{C}$-Vektorraum für jedes $n \in \mathbb{N}$.

c) Ist K ein Körper, so ist K^n für alle $n \in \mathbb{N}$ ein K-Vektorraum.

d) $\mathbb{R}$ ist ein $\mathbb{Q}$-Vektorraum.

e) Spezialfall von (c): $\mathbb{Z}_2^n$ ist ein Vektorraum über dem Körper $\mathbb{Z}_2$. Er besteht aus allen n-Tupeln von Nullen und Einsen.

   Beispielsweise lassen sich `integer`-Werte in Binärdarstellung als Elemente des Vektorraums $\mathbb{Z}_2^{32}$ interpretieren. (Welche Operation wird dabei durch die Vektorraumaddition realisiert?)

   Die Vektorräume $\mathbb{Z}_2^n$ spielen eine große Rolle in der Codierungstheorie. Lineare Codes verwenden Teilmengen des $\mathbb{Z}_2^n$, bei denen beim Auftreten eines Übertragungsfehlers mit hoher Wahrscheinlichkeit ein Element außerhalb der Teilmenge entsteht (vgl. 31.16).

f) Funktionenräume sind wichtige Vektorräume. Wir bezeichnen die Menge aller Funktionen über einer Menge $\mathcal{X}$ mit $\mathbb{R}^{\mathcal{X}} := \{f : \mathcal{X} \to \mathbb{R}\}$. Wir definieren auf $\mathbb{R}^{\mathcal{X}}$ eine Vektoraddition und eine skalare Multiplikation durch

$$\left.\begin{array}{c}(f+g)(x) := f(x) + g(x) \\ (\lambda \cdot f)(x) := \lambda \cdot f(x)\end{array}\right\} \quad \forall x \in \mathcal{X} \ ,$$

   so ist $(\mathbb{R}^{\mathcal{X}}, +, \cdot)$ ein $\mathbb{R}$-Vektorraum. Der Nullvektor ist dabei durch $f(x) = 0 \ \ \forall x \in \mathcal{X}$ gegebene Funktion.

g) Die Polynome $K[x]$ über einem Körper K bilden einen K-Vektorraum, wenn man als skalare Multiplikation definiert

$$\lambda \cdot \sum_{k=0}^{n} a_k x^k := \sum_{k=0}^{n} (\lambda a_k) x^k \qquad \forall \lambda \in K \ .$$

Zu Gruppen und Ringen haben wir Untergruppen und Unterringe definiert (vgl. 29.6, 30.5). Ähnliches ist auch für Vektorräume möglich.

33.5 Definition: Untervektorraum

Es sei V ein K-Vektorraum und $U \subset V$. Ist U mit den Verknüpfungen von V selbst wieder ein K-Vektorraum, so heißt U **Unterraum** (**Untervektorraum**, **Teilraum**) von V.

33.6 Satz: Unterraumkriterium

Es sei V ein K-Vektorraum und $U \subset V$ nichtleer. Dann ist U genau dann ein Vektorraum (also ein Unterraum von V), wenn gilt

a) $u + v \in U \quad \forall u, v \in U$

b) $\lambda u \in U \quad \forall \lambda \in K \;\; \forall u \in U.$

Das heißt U ist abgeschlossen bezüglich Vektorraumaddition und skalarer Multiplikation.

Beweis:

1. U Unterraum $\Rightarrow$ (a), (b): nach Definition.
2. (a), (b) $\Rightarrow$ U Unterraum:
   - Nach 29.6 ist $(U, +)$ Untergruppe von $(V, +)$, da U abgeschlossen unter $+$ und nach 33.3c zu $u \in U$ auch $-u = (-1) \cdot u \in U$ gilt.
   - Da $(V, +)$ kommutativ, ist auch $(U, +)$ kommutativ.
   - Wegen 33.6b ist $\cdot$ eine Abbildung von $K \times U$ nach U. Die Eigenschaften b–e der Vektorraumdefinition 33.2 übertragen sich von V auf U.

□

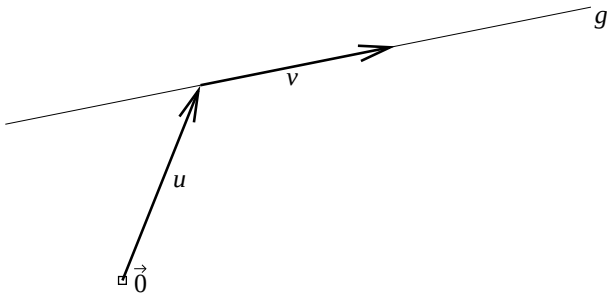
Bemerkung: Der Nullvektor $\vec{0}$ muß in jedem Unterraum enthalten sein, da $0 \cdot u = \vec{0}$, $\forall u \in V$.

33.7 Beispiele

a) Ein K-Vektorraum V hat die trivialen Unterräume $\{0\}$ und V.

b) Lineare Codes sind Unterräume im $\mathbb{Z}_2^n$.

c) Sind Geraden Unterräume des $\mathbb{R}^2$?



Eine Gerade ist gegeben durch

$$\{u + \lambda \cdot v \mid \lambda \in \mathbb{R}\}\ , \quad u, v \in \mathbb{R}^2\ , v \neq 0\ .$$

Ein Unterraum muss stets den Nullvektor enthalten. Damit sind nur Ursprungsgeraden $\{\lambda \cdot v \mid \lambda \in \mathbb{R}\}$, $v \in \mathbb{R}^2$, $v \neq 0$, Unterräume.

d) Verallgemeinerung von (c): In einem K-Vektorraum V bilden die Mengen $\{\lambda v \mid \lambda \in K\}$ Unterräume.

Das letzte Beispiel lässt sich noch weiter verallgemeinern.

33.8 Definition

Es sei V ein K-Vektorraum. Ferner seien $u_1, \ldots, u_n \in V$ und $\lambda_1, \ldots, \lambda_n \in K$. Dann nennt man

$$\sum_{k=1}^{n} \lambda_k u_k$$

eine **Linearkombination** von $u_1, \ldots, u_n$.

Die Menge aller Linearkombinationen bildet das **Erzeugnis** (**Aufspann**, **lineare Hülle**) $\operatorname{span}(u_1, \ldots, u_n)$. Man nennt $\{u_1, \ldots, u_n\}$ das **Erzeugendensystem** von $\operatorname{span}(u_1, \ldots, u_n)$.

Bemerkung: Man definiert $\operatorname{span} \emptyset = \vec{0}$.

33.9 Satz: Erzeugnis als Unterraum

Es sei V ein K-Vektorraum, und es seien $u_1, \ldots, u_n \in V$. Dann bildet $\operatorname{span}(u_1, \ldots, u_n)$ einen Unterraum von V.

Beweis: Wir wenden das Unterraumkriterium an.

a) Es seien $v, w \in \operatorname{span}(u_1, \ldots, u_n)$. Dann existieren $\lambda_1, \ldots, \lambda_n \in K$ und $\mu_1, \ldots, \mu_n \in K$ mit

$$v = \sum_{k=1}^{n} \lambda_k u_k \ , \qquad\qquad w = \sum_{k=1}^{n} \mu_k u_k \ .$$

Daraus folgt

$$\begin{aligned} v + w &= \sum_{k=1}^{n} \lambda_k u_k + \sum_{k=1}^{n} \mu_k u_k \\ &= \sum_{k=1}^{n} (\underbrace{\lambda_k + \mu_k}_{\in K}) u_k \qquad \text{(nach 33.2a, e)} \\ &\in \operatorname{span}(u_1, \ldots, u_n) \ . \end{aligned}$$

b) Es sei $\mu \in K$ und $v \in \operatorname{span}(u_1, \ldots, u_n)$. Dann existieren $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \sum\limits_{k=1}^{n} \lambda_k u_k$. Also gilt

$$\begin{aligned} \mu v &= \mu \sum_{k=1}^{n} \underbrace{\lambda_k u_k}_{\in V} \\ &= \sum_{k=1}^{n} \mu(\lambda_k u_k) \qquad \text{(nach 33.2d)} \\ &= \sum_{k=1}^{n} \underbrace{(\mu \lambda_k)}_{\in K} u_k \qquad \text{(nach 33.2b)} \\ &\in \operatorname{span}(u_1, \ldots, u_n) \ . \end{aligned}$$

□

33.10 Beispiel

Im $\mathbb{R}^3$ bildet jede Ebene durch den Ursprung

$$\{\lambda v + \mu w \mid \lambda, \mu \in \mathbb{R}\} \ , \qquad v, w \in \mathbb{R}^3 \ , \quad v, w \neq \vec{0} \ , \quad v \neq \nu w \ \forall \nu \in \mathbb{R}$$

einen Unterraum.

Wie in $\mathbb{R}^2$ bilden auch in $\mathbb{R}^3$ Geraden durch den Ursprung

$$\{\lambda v \mid \lambda \in \mathbb{R}\}\,, \quad v \in \mathbb{R}^3 \setminus \{0\}$$

Unterräume.

33.11 Lineare Abhängigkeit

Offenbar ist

$$\text{span}\left(\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}\right) = \mathbb{R}^3 = \text{span}\left(\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}\right)\,,$$

d. h. $\begin{pmatrix}1\\1\\0\end{pmatrix}$ lässt sich als Linearkombination von $\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}$ darstellen.

Definition: Ein Vektor u heißt **linear abhängig** von $v_1, \ldots, v_n$, wenn es $\lambda_1, \ldots, \lambda_n$ gibt mit

$$u = \sum_{i=1}^{n} \lambda_i v_i,$$

andernfalls heißt er **linear unabhängig** von $v_1, \ldots, v_n$. Eine Menge von Vektoren $u_1, \ldots, u_n$, bei denen sich keiner der Vektoren als Linearkombination der anderen ausdrücken lässt, heißt **linear unabhängig**, andernfalls **linear abhängig**.

Gibt es ein einfaches Kriterium, anhand dessen man lineare Unabhängigkeit nachweisen kann?

33.12 Satz: Kriterium für lineare Unabhängigkeit

Es sei V ein K-Vektorraum. Die Vektoren $v_1, \ldots, v_n$ sind genau dann linear unabhängig, wenn für jede Linearkombination mit $\sum\limits_{i=1}^{n} \lambda_i v_i = \vec{0}$ gilt

$$\lambda_1 = \ldots = \lambda_n = 0\,.$$

Beweis: „⇐“: Es seien $v_1, \ldots, v_n$ linear abhängig, d. h. es gibt ein v_k mit $v_k = \sum_{\substack{i=1 \\ i \neq k}}^{n} \lambda_i v_i$. Setzt man $\lambda_k := -1$, so folgt $0 = \sum_{i=1}^{n} \lambda_i v_i$.

„⇒“: Angenommen, es gibt eine Linearkombination, in der ein $\lambda_k \neq 0$ existiert und $\sum_{i=1}^{n} \lambda_i v_i = \vec{0}$ gilt. Dann folgt

$$-\lambda_k v_k = \sum_{\substack{i=1 \\ i \neq k}}^{n} \lambda_i v_i$$

$$v_k = \sum_{\substack{i=1 \\ i \neq k}}^{n} \underbrace{\frac{-\lambda_i}{\lambda_k}}_{\in K} v_i \ ,$$

d. h. v_k ist linear abhängig von $\{v_1, \ldots, v_n\} \setminus \{v_k\}$. □

33.13 Einschub: Notation

Eine **Familie** ist eine Funktion ϕ, die jedem Element einer Indexmenge I ein Element einer Menge V zuordnet, $\phi : I \to V, i \mapsto v_i$. Dies wird geschrieben als $(v_i)_{i \in I}$. Eine Familie von Vektoren über einer beliebigen Indexmenge heißt auch ein **System** von Vektoren.

Ist lineare Unabhängigkeit auch bei unendlich vielen Vektoren ein sinnvoller Begriff?

33.14 Definition

Ein unendliches System B von Vektoren heißt **linear unabhängig,** wenn jede endliche Auswahl von Vektoren aus B linear unabhängig ist.

33.15 Beispiel

Betrachte $\mathbb{R}[x]$. Nach 33.4g ist $\mathbb{R}[x]$ ein $\mathbb{R}$-Vektorraum.

Wir zeigen, dass das unendliche System $B = (1, x, x^2, \ldots)$ linear unabhängig in $\mathbb{R}[x]$ ist.

Angenommen, dies trifft nicht zu. Dann gibt es eine endliche Teilmenge $\{x^{m_1}, x^{m_2}, \ldots, x^{m_n}\} \subset B$, die linear abhängig ist. Folglich gibt es eine Linearkombination

$$\sum_{i=1}^{n} \lambda_i x^{m_i} = 0 \qquad (*)$$

mit einem $\lambda \neq 0$.

Auf der linken Seite von $(*)$ steht ein Polynom, das nur endlich viele Nullstellen hat (vgl. Satz 31.7); rechts steht das Nullpolynom mit unendlich vielen Nullstellen – Widerspruch! □

Der Begriff der linearen Unabhängigkeit gestattet uns, ein minimales Erzeugendensystem zu finden.

33.16 Definition

Es sei V ein Vektorraum. Eine Teilmenge $B \subset V$ heißt **Basis** von V, falls gilt:

a) $\operatorname{span}(B) = V$.

b) B ist linear unabhängig.

33.17 Beispiele

a) $\left(\begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix}\right)$ ist eine Basis des $\mathbb{R}^2$, denn

i) Es sei $\begin{pmatrix}x\\y\end{pmatrix} \in \mathbb{R}^2$. Wir suchen λ, μ mit

$$\lambda \begin{pmatrix}2\\3\end{pmatrix} + \mu \begin{pmatrix}3\\4\end{pmatrix} = \begin{pmatrix}x\\y\end{pmatrix} .$$

Das Gleichungssystem

$$2\lambda + 3\mu = x$$

$$3\lambda + 4\mu = y$$

hat die Lösung

$$\lambda = -4x + 3y\ , \qquad \mu = 3x - 2y\ . \qquad (*)$$

Daraus folgt $\mathbb{R}^2 = \operatorname{span}\left\{\begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix}\right\}$.

ii) Es sei

$$\lambda \begin{pmatrix}2\\3\end{pmatrix} + \mu \begin{pmatrix}3\\4\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}\ .$$

Mit $(*)$ folgt $\lambda = -4 \cdot 0 + 3 \cdot 0 = 0$, $\mu = 3 \cdot 0 - 2 \cdot 0 = 0$. Also sind $\begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix}$ linear unabhängig.

b) $\left(\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}, \ldots \begin{pmatrix}0\\0\\0\\\vdots\\1\end{pmatrix}\right)$ ist eine Basis des $\mathbb{R}^n$, die so genannte **Standardbasis.**

c) Es gibt auch Vektorräume mit unendlichen Basen. Beispielsweise ist $(1, x, x^2, \ldots)$ eine unendliche Basis des $\mathbb{R}[x]$:

i) $\{1, x, x^2, \ldots\}$ ist linear unabhängig nach 33.15.

ii) Jedes Polynom aus $\mathbb{R}[x]$ ist als Linearkombination von Elementen aus $\{1, x, x^2, \ldots\}$ darstellbar.

Hat jeder Vektorraum eine Basis? Man kann zeigen:

33.18 Satz: Existenz von Basen

Jeder Vektorraum $V \neq \{\vec{0}\}$ besitzt eine Basis.

Offenbar sind Basen nicht eindeutig: So sind z. B. $\left(\begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix}\right)$ und $\left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$ Basen des $\mathbb{R}^2$. Insbesondere kann man Basisvektoren austauschen:

33.19 Satz: Austauschsatz von Steinitz

Es sei V ein Vektorraum mit einer endlichen Basis $B := (b_1, \ldots, b_n)$. Außerdem sei $v \in V$, $v \neq 0$. Dann existiert ein b_k, für das $(b_1, \ldots, b_{k-1}, v, b_{k+1}, \ldots, b_n)$ eine Basis von V ist.

Beweis: Da B Basis ist, gibt es $\lambda_1, \ldots, \lambda_n$ mit

$$v = \sum_{i=1}^{n} \lambda_i b_i \; . \qquad (*)$$

Da $v \neq 0$, ist dabei mindestens ein $\lambda_i \neq 0$. Ohne Beschränkung der Allgemeingültigkeit sei $\lambda_1 \neq 0$. Wir zeigen, dass dann $(v, b_2, \ldots, b_n)$ eine Basis von V ist.

i) Es gilt $\operatorname{span}(v, b_2, \ldots, b_n) = V$: Es sei nämlich $u \in V$. Da B Basis ist, gibt es $\mu_1, \ldots, \mu_n$ mit

$$u = \sum_{i=1}^{n} \mu_i b_i \; . \qquad (**)$$

Aus $(*)$ und $\lambda_1 \neq 0$ folgt

$$b_1 = \frac{1}{\lambda_1} v - \sum_{i=2}^{n} \frac{\lambda_i}{\lambda_1} b_i \; .$$

Einsetzen in $(**)$ zeigt, dass u als Linearkombination von $v, b_2, \ldots, b_n$ geschrieben werden kann.

ii) Das System $(v, b_2, \ldots, b_n)$ ist linear unabhängig: Es sei nämlich $\mu_1 v + \mu_2 b_2 + \ldots + \mu_n b_n = 0$. Mit $(*)$ erhält man

$$\begin{aligned} 0 &= \mu_1 \sum_{i=1}^{n} \lambda_i b_i + \sum_{i=2}^{n} \mu_i b_i \\ &= \mu_1 \lambda_1 b_1 + \sum_{i=2}^{n} (\mu_1 \lambda_i + \mu_i) b_i \; . \end{aligned}$$

Da $(b_1, \ldots, b_n)$ Basis ist, sind alle Koeffizienten 0:

$$\begin{aligned} \mu_1 \lambda_1 = 0 \quad &\overset{\lambda_1 \neq 0}{\Rightarrow} \quad \mu_1 = 0 \\ \mu_1 \lambda_i + \mu_i = 0 \quad &\overset{\mu_1 = 0}{\Rightarrow} \quad \mu_i = 0 \qquad (i = 2, \ldots, n) \end{aligned}$$

□

Hat ein Vektorraum eine eindeutig bestimmte Anzahl von Basisvektoren?

33.20 Satz: Eindeutigkeit der Anzahl von Basisvektoren

- Hat ein Vektorraum V eine endliche Basis von n Vektoren, so besteht jede Basis von V aus genau n Vektoren.
- Basisergänzungssatz: Ist M eine linear unabhängige Menge von Vektoren in einem Vektorraum V, so gibt es eine linear unabhängige Menge N, so daß $M \cup N$ eine Basis von V ist.

Beweis:

- Es seien $B := (b_1, \ldots, b_n)$ und $C := (c_1, \ldots, c_m)$ Basen von V.

  i) Angenommen, es wäre $n > m$. Per Erweiterung des Satzes 33.19 mittels Induktion kann man zeigen, daß man m der Vektoren von B durch C austauschen kann:

  $$(c_1, \ldots, c_m, b'_{m+1}, \ldots, b'_n) \qquad \text{mit } (b'_{m+1}, \ldots, b'_n) \subset (b_1, \ldots, b_n) \; .$$

  Da C eine Basis ist, sind die nicht ausgetauschten Vektoren $b'_{m+1}, \ldots, b'_n$ aus B als Linearkombinationen von $c_1, \ldots, c_m$ darstellbar. Dies widerspricht der Basiseigenschaft.

  ii) $n < m$ wird analog zum Widerspruch geführt.

- Skizze: Nach Satz 33.18 hat V eine Basis B. Mittels des erweiterten Austauschsatzes von Steinitz tauschen wir M in die bestehende Basis B ein. Die Menge N ergibt sich als $N = B \backslash M$.

□

33.21 Definition: Dimension eines Vektorraums

Ist die Basis B eine endliche Teilmenge von Vektorraums V mit $B = (b_1, \ldots, b_n)$. Dann heißt die Zahl $n =: \dim V$ die **Dimension** von V. Für den Nullraum $\{\vec{0}\}$ definiert man $\dim\{\vec{0}\} := 0$.

33.22 Satz: Basiskriterium

In einem Vektorraum V der Dimension n

- ist jede linear unabhängige Menge von n Vektoren eine Basis.
- bilden n Vektoren, die V erzeugen, stets eine Basis.

Bemerkung:

- In einem n-dimensionalen Vektorraum gibt es keine linear unabhängigen Systeme von mehr als n Vektoren.
- die Basis B ist eine **maximal linear unabhängige** Menge d.h. B ist linear unabhängig und $B \cup \{u\}$ mit $u \in V$ ist linear abhängig.

34 Lineare Abbildungen

34.1 Motivation

- Wir haben wichtige Eigenschaften von Vektorräumen kennen gelernt. Damit ist es sinnvoll zu untersuchen, wie Abbildungen zwischen Vektorräumen aussehen können. Die wichtigsten Abbildungen zwischen Vektorräumen sind lineare Abbildungen.
- Der Basisbegriff bildet ein wichtiges Werkzeug zur Beschreibung linearer Abbildungen.

34.2 Definition

Es seien U, V zwei K-Vektorräume. Eine Abbildung $f : U \to V$ heißt **lineare Abbildung (Vektorraumhomomorphismus),** wenn gilt:

a) $f(u+v) = f(u) + f(v)$ für alle $u, v \in U$

b) $f(\lambda u) = \lambda f(u)$ für alle $\lambda \in K$, $u \in U$.

U und V heißen **isomorph**, wenn es eine bijektive lineare Abbildung $f : U \to V$ gibt. Wir schreiben hierfür $U \simeq V$.

Bemerkung: Die Begriffsbildung ist ähnlich wie bei Gruppen (vgl. 29.19): Ein Vektorraumhomomorphismus überführt die Verknüpfungen in U (Addition, skalare Multiplikation) in die Verknüpfungen in V.

Man fasst oft (a) und (b) in eine Bedingung zusammen:
$f(\lambda u + \mu v) = \lambda f(u) + \mu f(v) \quad \forall \lambda, \mu \in K, \forall u, v \in U$, d. h. Linearkombinationen in U werden in solche in V überführt. Insbesondere folgt per Induktion

$$f\Big(\sum_{i=1}^{n} \lambda_i v_i\Big) = \sum_{i=1}^{n} \lambda_i \, f(v_i).$$

34.3 Beispiele

a) Die Abbildung

$$f:\ \mathbb{R}^3 \to \mathbb{R}^2\ , \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 2x_1 + x_3 \\ -x_2 \end{pmatrix}$$

ist linear, denn

$$\begin{aligned} f\left(\lambda \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \mu \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}\right) &= f\left(\begin{pmatrix} \lambda x_1 + \mu y_1 \\ \lambda x_2 + \mu y_2 \\ \lambda x_3 + \mu y_3 \end{pmatrix}\right) \\ &= \begin{pmatrix} 2(\lambda x_1 + \mu y_1) + (\lambda x_3 + \mu y_3) \\ -(\lambda x_2 + \mu y_2) \end{pmatrix} \\ &= \lambda \begin{pmatrix} 2x_1 + x_3 \\ -x_2 \end{pmatrix} + \mu \begin{pmatrix} 2y_1 + y_3 \\ -y_2 \end{pmatrix} \\ &= \lambda f\left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\right) + \mu f\left(\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}\right) \end{aligned}$$

für alle $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \mathbb{R}^3$ und alle $\lambda, \mu \in \mathbb{R}$.

b) $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x + 1$ ist keine lineare Abbildung, denn $1 = f(0 + 0) \neq f(0) + f(0) = 1 + 1$.

c) $f : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_1 x_2 \end{pmatrix}$ ist ebenfalls nicht linear, da

$$f\left(2 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 4 \end{pmatrix}\ , \quad 2 \cdot f\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = 2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}\ .$$

34.4 Weitere Begriffe

Analog zu 29.19 definiert man auch für Vektorräume **Monomorphismen, Epimorphismen, Isomorphismen, Endomorphismen** und **Automorphismen**.

In Analogie zu 29.21 ist für einen Homomorphismus $f : U \to V$

$$\begin{aligned} \mathrm{Im}(f) &:= \{f(u) \mid u \in U\} && \text{das } \textbf{Bild} \text{ von } f, \\ \mathrm{Ker}(f) &:= \{u \in U \mid f(u) = 0\} && \text{der } \textbf{Kern} \text{ von } f. \end{aligned}$$

34.5 Satz: Eigenschaften linearer Abbildungen

a) Ist $f : U \to V$ ein Isomorphismus, so ist auch die Umkehrabbildung $f^{-1} : V \to U$ linear.

b) Die lineare Abbildung $f : U \to V$ ist genau dann injektiv, wenn $\mathrm{Ker}(f) = \{0\}$ ist.

c) Ist $f : U \to V$ linear, so ist $\mathrm{Ker}(f)$ ein Unterraum von U und $\mathrm{Im}(f)$ ein Unterraum von V.

d) Es gilt $\dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f) = \dim U$ (Dimensionsformel).

34.6 Beispiel

Wir betrachten die lineare Abbildung

$$f : \mathbb{R}^3 \to \mathbb{R}^2 , \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1 - x_3 \\ 0 \end{pmatrix} .$$

$\mathrm{Ker}(f) = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \;\middle|\; x_1 = x_3 \right\}$ ist eine Ebene durch den Ursprung in $\mathbb{R}^3$ (und somit ein zweidimensionaler Unterraum des $\mathbb{R}^3$).

$\mathrm{Im}(f) = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} \in \mathbb{R}^2 \;\middle|\; x \in \mathbb{R} \right\}$ ist eine Gerade durch den Ursprung in $\mathbb{R}^2$ (und somit ein eindimensionaler Unterraum des $\mathbb{R}^2$).

Es ist $\dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f) = 2 + 1 = 3 = \dim(\mathbb{R}^3)$.

Weiteres Beispiel: Abbildung $f : \mathbb{R}^3 \to \mathbb{R}^2$ aus 34.3a. Man überzeugt sich davon, dass $\dim \mathrm{Ker}(f) = 1$, $\dim \mathrm{Im}(f) = 2$.

Welche Rolle spielen Basen bei der Beschreibung linearer Abbildungen? Hierzu betrachten wir zunächst Basisdarstellungen von Vektoren.

34.7 Satz: Eindeutigkeit der Darstellung in einer festen Basis

Es sei $B := (b_1, \ldots, b_n)$ eine Basis des K-Vektorraums V. Dann gibt es zu jedem Vektor $v \in V$ eindeutig bestimmte Elemente $x_1, \ldots, x_n \in K$ mit

$$v = \sum_{i=1}^{n} x_i b_i \ .$$

Diese x_i heißen **Koordinaten** von v bezüglich B. Wir schreiben

$$v = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}_B \ .$$

Beweis: Die Existenz der Darstellung ist klar wegen $V = \mathrm{span}(B)$. Zu zeigen bleibt die Eindeutigkeit. Es sei

$$v = \sum_{i=1}^{n} x_i b_i \quad \text{und} \quad v = \sum_{i=1}^{n} y_i b_i \ .$$

Dann ist

$$\vec{0} = v - v = \sum_{i=1}^{n} (x_i - y_i) b_i \ ,$$

wegen der linearen Unabhängigkeit von B also

$$x_i = y_i \ , \qquad i = 1, \ldots, n \ .$$

□

Selbstverständlich liefern unterschiedliche Basen auch unterschiedliche Koordinatendarstellungen eines Vektors. Wie kann man diese Darstellungen ineinander umrechnen?

34.8 Beispiel: Umrechnung von Koordinatendarstellungen

Im $\mathbb{R}^2$ sei eine Basis $B = (b_1, b_2)$ gegeben. Bezüglich B habe ein Vektor v die Darstellung $v = \begin{pmatrix} x \\ y \end{pmatrix}_B$.

Wir betrachten die neue Basis $C = (c_1, c_2)$ mit $c_1 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}_B$, $c_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}_B$. Wie lautet die Darstellung von v bezüglich C?

Ansatz: $v = \begin{pmatrix} \lambda \\ \mu \end{pmatrix}_C$. Es muss gelten

$$\begin{aligned} \begin{pmatrix} x \\ y \end{pmatrix}_B = v = \begin{pmatrix} \lambda \\ \mu \end{pmatrix}_C &= \lambda c_1 + \mu c_2 \\ &= \lambda \begin{pmatrix} 2 \\ 2 \end{pmatrix}_B + \mu \begin{pmatrix} 1 \\ 2 \end{pmatrix}_B = \begin{pmatrix} 2\lambda + \mu \\ 2\lambda + 2\mu \end{pmatrix}_B . \end{aligned}$$

Die Bestimmungsgleichungen

$$\begin{aligned} 2\lambda + \mu &= x \\ 2\lambda + 2\mu &= y \end{aligned}$$

haben die Lösung

$$\lambda = x - \frac{1}{2}y \, , \qquad\qquad \mu = -x + y \, .$$

Beispielsweise ist

$$\begin{pmatrix} 5 \\ 2 \end{pmatrix}_B = \begin{pmatrix} 5 - \frac{1}{2}2 \\ -5 + 2 \end{pmatrix}_C = \begin{pmatrix} 4 \\ -3 \end{pmatrix}_C .$$

Auf diese Weise kann man allgemein die Koordinatendarstellung von Vektoren bezüglich einer Basis B in eine solche bezüglich einer anderen Basis C umrechnen, wenn nur für die Basisvektoren von C die Darstellungen bezüglich der Basis B bekannt sind.

Basen ermöglichen es, eine lineare Abbildung durch wenige Daten zu beschreiben: Es genügt, zu wissen, was mit den Basisvektoren passiert.

34.9 Satz: Charakterisierung einer linearen Abbildung durch ihre Wirkung auf die Basis

Es seien U, V zwei K-Vektorräume und $B = (b_1, \ldots, b_n)$ eine Basis von U. Außerdem seien $v_1, \ldots, v_n \in V$.

Dann gibt es genau eine lineare Abbildung $f : U \to V$ mit $f(b_i) = v_i$, $i = 1, \ldots, n$.

Beweis: Es sei $u \in U$ und $u = \sum_{i=1}^{n} x_i b_i$. Wir setzen $f(u) = \sum_{i=1}^{n} x_i v_i$.

Man prüft nach:

- f ist eine lineare Abbildung: Für $u = \sum_{i=1}^{n} x_i b_i$ und $w = \sum_{i=1}^{n} y_i b_i$, $\lambda, \mu \in K$ ist

$$\begin{aligned} f(\lambda u + \mu w) &= f\left(\lambda \sum_{i=1}^{n} x_i b_i + \mu \sum_{i=1}^{n} y_i b_i\right) = f\left(\sum_{i=1}^{n} (\lambda x_i + \mu y_i) b_i\right) \\ &= \sum_{i=1}^{n} (\lambda x_i + \mu y_i) v_i = \lambda \sum_{i=1}^{n} x_i v_i + \mu \sum_{i=1}^{n} y_i v_i \\ &= \lambda f(u) + \mu f(w) \; . \end{aligned}$$

- $f(b_i) = v_i$ für $i = 1, \ldots, n$.

Zum Nachweis der Eindeutigkeit nehmen wir an, dass g eine weitere lineare Abbildung mit $g(b_i) = v_i$ für $i = 1, \ldots, n$ ist. Dann folgt

$$\begin{aligned} g(u) = g\left(\sum_{i=1}^{n} x_i b_i\right) &\overset{\text{linear}}{=} \sum_{i=1}^{n} x_i g(b_i) = \sum_{i=1}^{n} x_i v_i \\ = \sum_{i=1}^{n} x_i f(b_i) &\overset{\text{linear}}{=} f\left(\sum_{i=1}^{n} x_i b_i\right) = f(u) \; . \end{aligned}$$

□

Bemerkung:

- Die ausgeführte Konstruktion im Beweis nennt man **lineare Fortsetzung**.

- Eine lineare Abbildung ist vollständig festgelegt durch die Wirkung auf die Basis $B = (b_1, \ldots, b_n)$. Sei $v_i = f(b_i), i = 1, \ldots, n$. Jedes $u \in U$ hat eine eindeutige Koordinatendarstellung $u = \sum_{i=1}^{n} \alpha_i b_i$ mit $\alpha_i \in K$ bezüglich der Basis B. Dann folgt aus der Linearität von f,

$$f(u) \;=\; f\Big(\sum_{i=1}^{n} \alpha_i b_i\Big) \;=\; \sum_{i=1}^{n} \alpha_i \, f(b_i) \;=\; \sum_{i=1}^{n} \alpha_i \, v_i.$$

Eine weitere wichtige Aussage, die mithilfe von Basen bewiesen werden kann, bezieht sich auf isomorphe Vektorräume.

34.10 Satz: Isomorphie endlichdimensionaler Vektorräume

Es seien U, V zwei endlichdimensionale K-Vektorräume. Dann sind U und V genau dann isomorph, wenn sie dieselbe Dimension haben:

$$U \simeq V \quad \Leftrightarrow \quad \dim U = \dim V \; .$$

Bemerkung: Dieser Satz besagt z. B., dass es im Wesentlichen nur einen einzigen n-dimensionalen Vektorraum über $\mathbb{R}$ gibt: den $\mathbb{R}^n$.

Beweisskizze: Man zeigt:

a) "$\Leftarrow$": Eine lineare Abbildung $f : U \to V$, die die Basis von U auf die Basis von V abbildet ist ein Vektorraum-Homomorphismus (per Definition), die injektiv ($\mathrm{Ker}(f) = \{0\}$ da die Basis von V linear unabhängig ist) und surjektiv ($\mathrm{Im}(f) = V$, da der Spann der Basis von V ganz V erzeugt) ist.

b) "$\Rightarrow$": Sei $f : U \to V$ ein Isomorphismus. Da f injektiv ist, gilt $\mathrm{Ker}(f) = \{0\}$. Mit der Dimensionsformel folgt $\dim \mathrm{Im}(f) = \dim U$. Da f surjektiv ist, gilt $\mathrm{Im}(f) = V$ und daher folgt $\dim V = \dim U$. $\square$

35 Matrixschreibweise für lineare Abbildungen

35.1 Motivation

- Wir haben gesehen, dass lineare Abbildungen sich durch ihre Wirkung auf die Basisvektoren ausdrücken lassen.
- Mithilfe von Matrizen können wir dies kompakt aufschreiben und die Hintereinanderausführung linearer Abbildungen elegant berechnen.

35.2 Struktur linearer Abbildungen zwischen endlichdimensionalen Vektorräumen

Es sei K ein Körper (meistens $\mathbb{R}$ oder $\mathbb{C}$). Dann ist

$$f: \quad K^n \to K^m\,, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \vdots \qquad\qquad \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix} \tag{$*$}$$

eine lineare Abbildung: Für $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in K^n$ und $\lambda, \mu \in K$ gilt nämlich

$$\begin{aligned} f(\lambda x + \mu y) &= \begin{pmatrix} a_{11}(\lambda x_1 + \mu y_1) + \ldots + a_{1n}(\lambda x_n + \mu y_n) \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ a_{m1}(\lambda x_1 + \mu y_1) + \ldots + a_{mn}(\lambda x_n + \mu y_n) \end{pmatrix} \\ &= \lambda \begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \vdots \qquad\qquad \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix} + \mu \begin{pmatrix} a_{11}y_1 + \ldots + a_{1n}y_n \\ \vdots \qquad\qquad \vdots \\ a_{m1}y_1 + \ldots + a_{mn}y_n \end{pmatrix} \\ &= \lambda f(x) + \mu f(y)\,. \end{aligned}$$

Umgekehrt besitzt jede lineare Abbildung von K^n nach K^m diese Struktur, da nach 34.9 eine lineare Abbildung von K^n in einen anderen Vektorraum durch die Bilder der Basisvektoren $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in K^n$ eindeutig bestimmt ist. Sind

diese Bilder durch $\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}, \ldots, \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \in K^m$ gegeben, so folgt, dass $(*)$ die entsprechende lineare Abbildung ist.

$$f(x) = \sum_{i=1}^{n} x_i \, f(e_i) = x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}.$$

Diese Struktur gibt Anlass zur nachfolgenden Definition.

35.3 Definition: Matrix

Es sei K ein Körper. Das rechteckige Schema

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

mit $a_{ij} \in K$ für $i = 1, \ldots, m$ und $j = 1, \ldots, n$ heißt $\boldsymbol{m \times n}$**-Matrix** über K. Die Menge aller $m \times n$-Matrizen über K bezeichnen wir mit $K^{m \times n}$.

Die Vektoren $\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}, \ldots, \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}$ heißen **Spaltenvektoren** von A; $(a_{11}, \ldots, a_{1n}), \ldots, (a_{m1}, \ldots, a_{mn})$ heißen **Zeilenvektoren** von A.

Die Matrix A wird auch als (a_{ij}) geschrieben. Dabei bildet i den **Zeilenindex** (bleibt innerhalb jeder Zeile konstant) und j den **Spaltenindex** (innerhalb jeder Spalte konstant).

35.4 Matrizen spezieller Gestalt

a) **Quadratische Matrizen:** Eine $n \times n$-Matrix heißt **quadratisch.** Dagegen heißen $m \times n$-Matrizen mit $m \neq n$ **nichtquadratisch.**

b) **Diagonalmatrizen:** Eine quadratische Matrix $A = (a_{ij})$, bei der $a_{ij} = 0$ für alle (i, j) mit $i \neq j$ gilt (also nur Diagonaleinträge a_{ii} von Null verschieden sein dürfen), heißt Diagonalmatrix.

c) **Dreiecksmatrizen:** Eine quadratische Matrix $A = (a_{ij})$, bei der $a_{ij} = 0$ für alle (i, j) mit $i > j$ gilt (also nur auf der Diagonale und darüber von Null verschiedene Einträge stehen dürfen), heißt **obere Dreiecksmatrix.**

Gilt $a_{ij} = 0$ für alle (i, j) mit $i < j$, so spricht man von einer **unteren Dreiecksmatrix.**

35.5 Matrix-Vektor-Produkt

Ist $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ und $c = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} \in K^m$, so schreiben wir statt

$$\begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \vdots \qquad\qquad\quad \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}$$

jetzt

$$\underbrace{\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}}_{\text{Matrix } A} \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{\text{Vektor } x} = \underbrace{\begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}}_{\text{Vektor } c},$$

also kurz: $A\,x = c$.

Eine solche Schreibweise ist sowohl für lineare Abbildungen nützlich als auch für lineare Gleichungssysteme (spätere Vorlesungen: Kapitel 37, 38). Sie definiert das **Produkt** zwischen einer $m \times n$-Matrix $A = (a_{ij}) \in K^{m\times n}$ und einem Vektor $x \in K^n$ als $Ax = c$ mit $c \in K^m$ und

$$c_i = \sum_{j=1}^{n} a_{ij}x_j \;, \qquad i = 1, \ldots, m \;.$$

Jede lineare Abbildung $f : K^n \to K^m$ kann also geschrieben werden als

$$f(x) = Ax \quad \text{mit } A \in K^{m\times n}.$$

Die Spalten von A sind dabei die Bilder der Basisvektoren.

35.6 Beispiele für lineare Abbildungen in Matrixschreibweise

a) Die lineare Abbildung $f : \mathbb{R}^3 \to \mathbb{R}^2$ mit

$$\begin{pmatrix}1\\0\\0\end{pmatrix} \mapsto \begin{pmatrix}3\\2\end{pmatrix} , \quad \begin{pmatrix}0\\1\\0\end{pmatrix} \mapsto \begin{pmatrix}1\\-4\end{pmatrix} , \quad \begin{pmatrix}0\\0\\1\end{pmatrix} \mapsto \begin{pmatrix}0\\1\end{pmatrix}$$

wird beschrieben durch

$$f(x) = \begin{pmatrix}3 & 1 & 0\\2 & -4 & 1\end{pmatrix} x \quad \forall x \in \mathbb{R}^3 ,$$

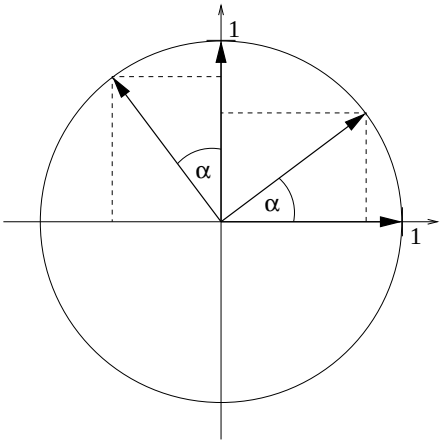
also z. B.

$$x = \begin{pmatrix}2\\3\\1\end{pmatrix} \quad \to \quad f(x) = \begin{pmatrix}3 & 1 & 0\\2 & -4 & 1\end{pmatrix} \begin{pmatrix}2\\3\\1\end{pmatrix} = \begin{pmatrix}3\cdot 2 + 1\cdot 3 + 0\cdot 1\\2\cdot 2 - 4\cdot 3 + 1\cdot 1\end{pmatrix} = \begin{pmatrix}9\\-7\end{pmatrix} .$$

b) **Streckung**

Die Matrix $A = \begin{pmatrix}\lambda & 0\\0 & \lambda\end{pmatrix} \in \mathbb{R}^{2\times 2}$ bildet einen Vektor $\begin{pmatrix}x\\y\end{pmatrix}$ auf $\begin{pmatrix}\lambda & 0\\0 & \lambda\end{pmatrix} \begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}\lambda x\\\lambda y\end{pmatrix} = \lambda \begin{pmatrix}x\\y\end{pmatrix}$ ab.

c) **Drehung in $\mathbb{R}^2$**



$$\begin{pmatrix}1\\0\end{pmatrix} \mapsto \begin{pmatrix}\cos\alpha\\\sin\alpha\end{pmatrix}$$

$$\begin{pmatrix}0\\1\end{pmatrix} \mapsto \begin{pmatrix}-\sin\alpha\\\cos\alpha\end{pmatrix}$$

Die Matrix der Drehung um einen Winkel α lautet demnach

$$A = \begin{pmatrix}\cos\alpha & -\sin\alpha\\\sin\alpha & \cos\alpha\end{pmatrix} .$$

(Drehungen werden dabei gegen den Uhrzeigersinn durchgeführt.)

d) **Spiegelung an der x_1-Achse in $\mathbb{R}^2$**

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

bewirkt offenbar eine Spiegelung an der x_1-Achse.

e) **Drehung in $\mathbb{R}^3$**

$$A = \begin{pmatrix} \cos\alpha & 0 & -\sin\alpha \\ 0 & 1 & 0 \\ \sin\alpha & 0 & \cos\alpha \end{pmatrix}$$

beschreibt eine Drehung in der x_1-x_3-Ebene (entlang der x_2-Achse geschieht nichts).

f) **Translationen**

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$$

sind *keine* linearen Abbildungen.

Welche Verknüpfungen lassen sich mit Matrizen ausführen?

35.7 Definition

Es sei K ein Körper.

a) Die **skalare Multiplikation** einer Matrix $A = (a_{ij}) \in K^{m\times n}$ mit einem Skalar $\lambda \in K$ erfolgt komponentenweise:

$$\lambda A := (\lambda a_{ij}) \ .$$

b) Die **Addition** zweier Matrizen $A = (a_{ij}) \in K^{m\times n}, B = (b_{ij}) \in K^{m\times n}$ erfolgt komponentenweise:

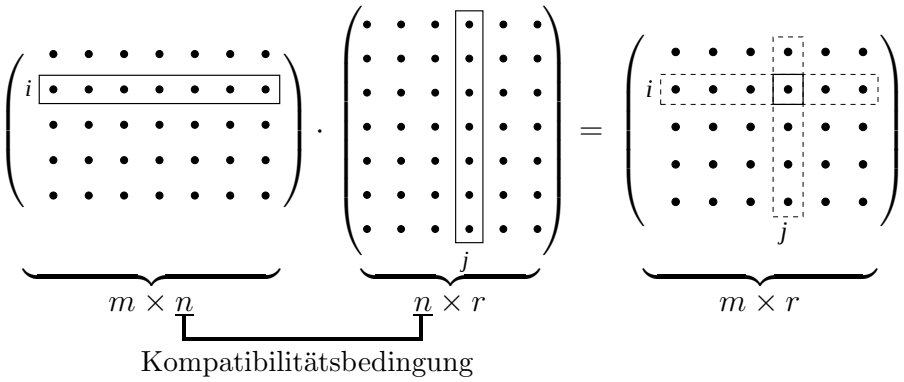
$$A + B = (a_{ij} + b_{ij}) \ .$$

c) Die **Multiplikation** zweier Matrizen $A = (a_{ij}) \in K^{m\times n}, B = (b_{ij}) \in K^{n\times r}$ definiert man als

$$A \cdot B = C \in K^{m\times r} \ ,$$

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \ .$$

Bemerkung: Die Matrixmultiplikation erfolgt also „Zeile mal Spalte“:



Nur zueinander „passende“ Matrizen (Kompatibilitatsbedingung: Spaltenzahl der ersten = Zeilenzahl der zweiten Matrix) können miteinander multipliziert werden.

35.8 Beispiele

(In diesen Beispielen ist stets $K = \mathbb{R}$.)

a) $3 \cdot \begin{pmatrix} 5 & 1 \\ 2 & -4 \end{pmatrix} = \begin{pmatrix} 15 & 3 \\ 6 & -12 \end{pmatrix}$

b) $\begin{pmatrix} 2 & 3 & 1 \\ 4 & -1 & 7 \end{pmatrix} + \begin{pmatrix} 1 & 5 & -8 \\ 0 & 2 & 9 \end{pmatrix} = \begin{pmatrix} 3 & 8 & -7 \\ 4 & 1 & 16 \end{pmatrix}$

c) $\begin{pmatrix} 2 & 3 & 1 \\ 4 & -1 & 7 \end{pmatrix} \cdot \begin{pmatrix} 6 & 4 \\ 1 & 0 \\ 8 & 9 \end{pmatrix} = \begin{pmatrix} 2 \cdot 6 + 3 \cdot 1 + 1 \cdot 8 & 2 \cdot 4 + 3 \cdot 0 + 1 \cdot 9 \\ 4 \cdot 6 - 1 \cdot 1 + 7 \cdot 8 & 4 \cdot 4 - 1 \cdot 0 + 7 \cdot 9 \end{pmatrix} = \begin{pmatrix} 23 & 17 \\ 79 & 79 \end{pmatrix}$.

Welche Rechenregeln ergeben sich aus 35.7?

35.9 Satz: Eigenschaften der Matrixoperationen

Es sei K ein Körper. Dann gilt:

a) $K^{m \times n}$ ist ein Vektorraum:

- $(K^{m\times n}, +)$ ist eine kommutative Gruppe
  - Assoziativgesetz: $(A + B) + C = A + (B + C)$
  - neutrales Element: $0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \in K^{m\times n}$
  - inverses Element zu A ist $-A = (-1)A$
  - Kommutativgesetz: $A + B = B + A$
- $\lambda(\mu A) = (\lambda\mu)A$
- $1 \cdot A = A$
- $\lambda(A + B) = \lambda A + \lambda B$
- $(\lambda + \mu)A = \lambda A + \mu A$

b) $(K^{n\times n}, +, \cdot)$ ist ein Ring mit Eins:

- $(K^{n\times n}, +)$ ist eine kommutative Gruppe
- $(K^{n\times n}, \cdot)$ ist ein Monoid:
  - Assoziativgesetz: $(A \cdot B) \cdot C = A \cdot (B \cdot C)$
  - neutrales Element: $I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} \in K^{n\times n}$
- Distributivgesetze:

$$A \cdot (B + C) = A \cdot B + A \cdot C$$
$$(A + B) \cdot C = A \cdot C + B \cdot C$$

35.10 Bemerkungen

a) Die Matrixmultiplikation ist im Allgemeinen *nicht* kommutativ:

$$\begin{pmatrix} 2 & 1 \\ 7 & -4 \end{pmatrix} \cdot \begin{pmatrix} 5 & 3 \\ 4 & 6 \end{pmatrix} = \begin{pmatrix} 2\cdot 5 + 1\cdot 4 & 2\cdot 3 + 1\cdot 6 \\ 7\cdot 5 - 4\cdot 4 & 7\cdot 3 - 4\cdot 6 \end{pmatrix} = \begin{pmatrix} 14 & 12 \\ 19 & -3 \end{pmatrix}$$
$$\begin{pmatrix} 5 & 3 \\ 4 & 6 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 7 & -4 \end{pmatrix} = \begin{pmatrix} 5\cdot 2 + 3\cdot 7 & 5\cdot 1 - 3\cdot 4 \\ 4\cdot 2 + 6\cdot 7 & 4\cdot 1 - 6\cdot 4 \end{pmatrix} = \begin{pmatrix} 31 & -7 \\ 50 & -20 \end{pmatrix}$$

b) Ebenso besitzt eine $n \times n$-Matrix im Allgemeinen *keine* Inverse bezüglich der Matrixmultiplikation.

c) $(K^{n\times n}, +, \cdot)$ ist nicht nullteilerfrei (d.h. aus $a \cdot b = 0$ folgt **nicht** notwendigerweise $a = 0$ oder $b = 0$):

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

d) $K^{n\times m}$ ist als Vektorraum isomorph zu K^{nm}.

e) Spaltenvektoren aus K^m können als $m \times 1$-Matrizen aufgefasst werden. Vektoraddition und skalare Multiplikation sind Spezialfälle der entsprechenden Matrixoperationen. Das Matrix-Vektor-Produkt ist ein Spezialfall der Matrixmultiplikation.

f) Die Hintereinanderausführung linearer Abbildungen entspricht der Multiplikation ihrer Matrizen:

$$\begin{array}{ccccc} K^r & \xrightarrow{f} & K^n & \xrightarrow{g} & K^m \\ & A \in K^{n\times r} & & B \in K^{m\times n} & \end{array}$$

$g \circ f : K^r \to K^m$ wird durch $B \cdot A \in K^{m\times r}$ repräsentiert.

$$g(f(x)) \;=\; g(Ax) \;= B \cdot (Ax) = BAx.$$

35.11 Inverse Matrizen

Im Allgemeinen hat $A \in K^{n\times n}$ kein multiplikatives Inverses A^{-1}. In vielen Fällen existiert jedoch eine inverse Matrix.

Beispiel: $A = \begin{pmatrix} 5 & 6 \\ 2 & 4 \end{pmatrix}$, $\qquad A^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{3}{4} \\ -\frac{1}{4} & \frac{5}{8} \end{pmatrix}$, denn

$$\begin{pmatrix} 5 & 6 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{3}{4} \\ -\frac{1}{4} & \frac{5}{8} \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 2 & 4 \end{pmatrix} \cdot \frac{1}{8} \begin{pmatrix} 4 & -6 \\ -2 & 5 \end{pmatrix}$$
$$= \frac{1}{8} \begin{pmatrix} 5\cdot 4 - 2\cdot 6 & -5\cdot 6 + 6\cdot 5 \\ 2\cdot 4 - 4\cdot 2 & -2\cdot 6 + 4\cdot 5 \end{pmatrix} = \frac{1}{8} \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Ein Verfahren zur Berechnung der inversen Matrix werden wir in einer späteren Vorlesung kennen lernen.

35.12 Definition

Eine Matrix $A \in K^{n\times n}$ heißt **invertierbar (umkehrbar, regulär),** falls eine Matrix $A^{-1} \in K^{n\times n}$ mit $AA^{-1} = I$ existiert. A^{-1} heißt **inverse Matrix** zu A.

Die Menge der invertierbaren Matrizen aus $K^{n\times n}$ wird mit $\mathrm{GL}(n, K)$ bezeichnet.

Eine nicht invertierbare Matrix wird auch als **singulär** bezeichnet.

35.13 Satz: Gruppeneigenschaft von $\mathrm{GL}(n, K)$

Die Menge $\mathrm{GL}(n, K)$ bildet mit der Matrizenmultiplikation eine multiplikative (nichtkommutative) Gruppe.

35.14 Bemerkungen

a) GL steht für *general linear group.*

b) Sind $A, B \in \mathrm{GL}(n, K)$, so ist $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$, denn

$$A \cdot \underbrace{B \cdot B^{-1}}_{I} \cdot A^{-1} = A \cdot I \cdot A^{-1} = A \cdot A^{-1} = I \ .$$

c) Nichtquadratische Matrizen sind niemals invertierbar. Allerdings kann man u. U. eine so genannte *Pseudoinverse* angeben (spätere Vorlesung).

d) Die Invertierbarkeit einer Matrix entspricht der Bijektivität der zugehörigen linearen Abbildung.

   Nach dem Beweis von Satz 34.10 ist eine lineare Abbildung zwischen endlichdimensionalen Vektorräumen genau dann bijektiv, wenn Basen auf Basen abgebildet werden.

   Daraus folgt: $A \in K^{n\times n}$ ist genau dann invertierbar, wenn die Spaltenvektoren von A eine Basis des K^n bilden.

Bis jetzt wurden alle Matrizen bezüglich der kanonischen Basis dargestellt. Im Folgenden werden wir die allgemeine Darstellung einer Matrix diskutieren und insbesondere das Verhalten bei einem Basiswechsel.

35.15 Matrix einer linearen Abbildung bezüglich gegebener Basen

Es seien U und V Vektorräume über K mit $\dim U = n$ und $\dim V = m$. In U haben wir die Basis $B = (b_1, \ldots, b_n)$ und in V die Basis $C = (c_1, \ldots, c_m)$. Wir betrachten die lineare Abbildung $f : U \to V$. Wie im letzten Kapitel diskutiert wurde, ist eine lineare Abbildung vollständig durch ihre Wirkung auf die Basisvektoren von U festgelegt. Die Matrixdarstellung von f bezüglich der Basen B und C ergibt sich dadurch, daß die Bilder $f(b_i)$, $i = 1 \ldots, n$ der Basis von B bezüglich der Basis von C dargestellt werden:

$$\begin{aligned} f(b_1) &= \sum_{k=1}^{m} a_{k1} c_k \\ \vdots \qquad & \qquad \vdots \\ f(b_n) &= \sum_{k=1}^{m} a_{kn} c_k, \end{aligned}$$

Die Matrix $A_B^C \in K^{n \times m}$ von f bezüglich der Basis B von U und Basis C von V ist dann

$$A_B^C = \Big(\big(f(b_1)\big)_C \ldots \big(f(b_n)\big)_C \Big)_B^C = \left(\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}_C \ldots \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}_C \right)_B^C$$

Das heißt die Matrix A_B^C ist die Koordinatendarstellung der linearen Abbildung f bezüglich B und C. Normalerweise werden die Indizes B und C weggelassen, wenn klar ist mit welchen Basen in U und V gearbeitet wird.

35.16 Verhalten der Matrixdarstellung einer linearen Abbildung bei Basiswechsel

Wir führen in U die Basis $S = (s_1, \ldots, s_n)$ und in V die Basis $T = (t_1, \ldots, t_m)$ ein. Wir möchten nun die Matrix der linearen Abbildung $f : U \to V$ bezüglich S und T finden. Insbesondere ist die Frage wie die Matrix A_S^U mit der Matrix A_B^C zusammenhängt.

Wir interpretieren den Wechsel von der Basis S zur Basis B in U als lineare Abbildung. Da bei einem Basiswechsel sich nur die Darstellung ändert, nicht

aber die Vektoren selbst, ist die dazugehörige lineare Abbildung nicht anderes als die Identität, $I_U : U \to U, u \mapsto u$. Die Matrixdarstellung $(I_U)_S^B$ ergibt sich wie oben diskutiert: die Bilder der Abbildung I_U der Basis S werden bezüglich der Basis B dargestellt:

$$\begin{aligned}(I_U)_S^B &= \Big(\big(I_U(s_1)\big)_B \dots \big(I_U(s_n)\big)_B \Big)_S^B \\ &= \Big((s_1)_B \dots (s_n)_B \Big)_S^B\end{aligned}$$

Analog interpretieren wir den Wechsel von der Basis C zur Basis T als lineare Abbildung $I_V : V \to V, v \mapsto v$. Die Matrixdarstellung $(I_V)_C^T$ ergibt sich dann als

$$(I_V)_C^T = \Big((c_1)_T \dots (c_n)_T \Big)_C^T$$

Wir interpretieren nun die Abbildung f als $f = I_V \circ f \circ I_U$. Die Matrixdarstellung von f bezüglich der Basen S und T ergibt sich dann als die Multiplikation der entsprechenden Matrizen:

$$A_S^T = (I_V)_C^T \, A_B^C \, (I_U)_S^B.$$

Beispiel: Wir betrachten die lineare Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$. Diese hat bezüglich der kanonischen Basis $E = (e_1, e_2)$ mit $e_1 = \begin{pmatrix}1\\0\end{pmatrix}$, $e_2 = \begin{pmatrix}0\\1\end{pmatrix}$ die Matrixdarstellung

$$A_E^E = \begin{pmatrix}1 & 5\\ 3 & 8\end{pmatrix}_E^E.$$

Wir wollen nun die Abbildung f bezüglich der Basis $S = (s_1, s_2)$ gegeben als

$$s_1 = \begin{pmatrix}1\\0\end{pmatrix}_E, \quad s_2 = \begin{pmatrix}1\\-1\end{pmatrix}_E.$$

und der Basis $T = (t_1, t_2)$ gegeben als

$$t_1 = \begin{pmatrix}1\\1\end{pmatrix}_E, \quad t_2 = \begin{pmatrix}0\\3\end{pmatrix}_E.$$

darstellen.

Beim Basiswechsel von S nach E müssen wir die Basis S bezüglich der neuen Basis E darstellen. Da die Vektoren von S bezüglich der kanonischen Basis gegeben sind, erhalten wir

$$(I_{\mathbb{R}^2})_S^E = \Big((s_1)_E \, (s_2)_E \Big)_S^E = \begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}_S^E.$$

Beim zweiten Basiswechsel von E nach T müssen wir die Basis E bezüglich der Basis T darstellen.

$$e_1 \;=\; a_{11}\, t_1 + a_{21}\, t_2, \qquad e_2 \;=\; a_{12}\, t_1 + a_{22}\, t_2.$$

Dies ergibt die linearen Gleichungssysteme

$$\begin{pmatrix}1\\0\end{pmatrix} = a_{11}\begin{pmatrix}1\\1\end{pmatrix} + a_{21}\begin{pmatrix}0\\3\end{pmatrix}, \qquad \begin{pmatrix}0\\1\end{pmatrix} = a_{12}\begin{pmatrix}1\\1\end{pmatrix} + a_{22}\begin{pmatrix}0\\3\end{pmatrix}.$$

Mit Lösung

$$a_{11} = 1,\; a_{21} = -\frac{1}{3}, \qquad a_{12} = 0,\; a_{22} = \frac{1}{3}.$$

Damit erhalten wir

$$(I_{\mathbf{R}^2})_E^T \;=\; \Big((e_1)_T \, (e_2)_T \Big)_E^T \;=\; \begin{pmatrix}1 & -\frac{1}{3}\\ 0 & -\frac{1}{3}\end{pmatrix}_E^T.$$

Die Matrixdarstellung A_S^T von f bezüglich S und T ergibt sich damit als

$$\begin{aligned} A_S^T &= (I_{\mathbf{R}^2})_E^T \, A_E^E \, (I_{\mathbf{R}^2})_S^E \\ &= \begin{pmatrix}1 & -\frac{1}{3}\\ 0 & -\frac{1}{3}\end{pmatrix}_E^T \begin{pmatrix}1 & 5\\ 3 & 8\end{pmatrix}_E^E \begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}_S^E \\ &= \begin{pmatrix}1 & -\frac{1}{3}\\ 0 & -\frac{1}{3}\end{pmatrix}_E^T \begin{pmatrix}1 & -4\\ 3 & -5\end{pmatrix}_S^E \\ &= \begin{pmatrix}1 & -4\\ \frac{2}{3} & -\frac{1}{3}\end{pmatrix}_S^T \end{aligned}$$

Wir berechnen das Bild von $f(s_2)$ mittels der oben berechneten Matrix. Bezüglich der kanonischen Basis haben wir

$$f(s_2) = A_E^E \, (s_2)_E = \begin{pmatrix}1 & 5\\ 3 & 8\end{pmatrix}_E^E \begin{pmatrix}1\\-1\end{pmatrix}_E = \begin{pmatrix}-4\\-5\end{pmatrix}_E,$$

und bezüglich der Basen S und T, bekommen wir

$$f(s_2) = A_S^T \, (s_2)_S = \begin{pmatrix}1 & -4\\ \frac{2}{3} & -\frac{1}{3}\end{pmatrix}_S^T \begin{pmatrix}0\\1\end{pmatrix}_S = \begin{pmatrix}-4\\-\frac{1}{3}\end{pmatrix}_T.$$

Um uns zu überzeugen, daß die berechneten Bilder übereinstimmen, rechnen wir die Darstellung bezüglich T in E um.

$$\begin{pmatrix}-4\\-\frac{1}{3}\end{pmatrix}_T = -4\, t_1 - \frac{1}{3}\, t_2 = -4\begin{pmatrix}1\\1\end{pmatrix}_E - \frac{1}{3}\begin{pmatrix}0\\3\end{pmatrix}_E = \begin{pmatrix}-4\\-5\end{pmatrix}_E.$$

36 Rang einer Matrix

36.1 Motivation

- Interpretiert man eine Matrix als lineare Abbildung, so haben die Spaltenvektoren eine besondere Bedeutung: Nach Def. 35.3 sind sie die Bilder der Basisvektoren.
- Wir wollen die lineare Abhängigkeit/Unabhängigkeit dieser Spaltenvektoren genauer untersuchen. Dies führt unter anderem zu einem wichtigen Kriterium für die Invertierbarkeit von Matrizen.

36.2 Definition

Der **Spaltenrang (Rang)** einer Matrix $A \in K^{m\times n}$ ist die maximale Anzahl linear unabhängiger Spaltenvektoren von A. Man schreibt dafür $\operatorname{rang} A$ (auch rank, rk).

36.3 Satz: Aussagen über den Rang einer Matrix

Es sei $f : K^n \to K^m$ eine lineare Abbildung mit der zugehörigen Matrix $A \in K^{m\times n}$ und den Spaltenvektoren $a_{*1}, \ldots, a_{*n}$. Dann gilt:

a) $\operatorname{Im}(f) = \operatorname{span}(a_{*1}, \ldots, a_{*n})$

b) $\dim \operatorname{Im}(f) = \operatorname{rang} A$

c) $\dim \operatorname{Ker}(f) = n - \operatorname{rang} A$

Beweis:

a) „$\supset$“ ist klar, da $a_{*1}, \ldots, a_{*n}$ die Bilder der Basisvektoren sind.

„$\subset$“: Es ist

$$f(x) = Ax = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \vdots \qquad\qquad \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix} = x_1 a_{*1} + \ldots + x_n a_{*n} \ ,$$

d. h. jedes Element des Bildes ist Linearkombination der Spaltenvektoren.

b) Folgt unmittelbar aus (a).

c) Folgt aus Satz 34.5d. □

36.4 Beispiele

a) Nach 35.14d ist $A \in K^{n\times n}$ genau dann invertierbar, wenn $\operatorname{rang} A = n$ ist.

b) $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ hat den Rang 3: Es ist $a_{*2}, a_{*3} \notin \operatorname{span}(a_{*1})$, $a_{*3} \notin \operatorname{span}(a_{*1}, a_{*2})$.
Man beachte, dass sich aufgrund der speziellen Gestalt von A (obere Dreiecksmatrix) der Rang besonders leicht ablesen lässt.

c) $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 2 & 0 & 2 \end{pmatrix}$ hat den Rang 2: Die Vektoren a_{*1}, a_{*2} sind linear unabhängig, und $a_{*3} = a_{*1} + 2a_{*2}$.

36.5 Definition: transponierte Matrix

Vertauscht man bei einer Matrix $A = (a_{ij}) \in K^{m\times n}$ die Rolle von Zeilen und Spalten, so entsteht die **transponierte Matrix** $A^{\mathrm{T}} = (a_{ji}) \in K^{n\times m}$.

Der Rang von A^{T} gibt die Anzahl der linear unabhängigen Zeilenvektoren von A an. Man nennt ihn daher auch den **Zeilenrang** von A.

36.6 Beispiel

$$A = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 \\ 2 & 0 & 2 & 4 \end{pmatrix} \qquad \Rightarrow \qquad A^{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 1 & 2 & 2 \\ 2 & 1 & 4 \end{pmatrix} =: B$$

rang $A = 2$: a_{*1}, a_{*2} sind linear unabhängig
$a_{*3} = a_{*1} + 2a_{*2}$
$a_{*4} = 2a_{*1} + a_{*2}$

rang $B = 2$: b_{*1}, b_{*2} sind linear unabhängig
$b_{*3} = 2b_{*1}$

In diesem Beispiel stimmen also Spalten- und Zeilenrang überein. Ist dies Zufall?

36.7 Satz: Gleichheit von Spaltenrang und Zeilenrang

Für jede Matrix $A \in K^{m \times n}$ sind Spalten- und Zeilenrang gleich.

Beweis: Es sei die Matrix

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

gegeben. Bezeichnen wir ihren Spaltenrang mit r, so lassen sich die Spaltenvektoren $a_{*1}, \dots, a_{*n}$ als Linearkombinationen von r Basisvektoren

$$b_1 = \begin{pmatrix} b_{11} \\ \vdots \\ b_{1m} \end{pmatrix}, \dots, b_r = \begin{pmatrix} b_{r1} \\ \vdots \\ b_{rm} \end{pmatrix}$$

darstellen:

$$\begin{aligned} a_{*1} &= c_{11}b_1 + \dots + c_{1r}b_r \\ &\vdots \\ a_{*n} &= c_{n1}b_1 + \dots + c_{nr}b_r \end{aligned} \qquad (*)$$

Also haben wir für jedes einzelne Matrixelement von A

$$a_{ij} = c_{j1}b_{1i} + \dots + c_{jr}b_{ri} \; .$$

Für die Elemente eines Zeilenvektors a_{i*} von A haben wir damit

$$\begin{aligned} a_{i1} &= c_{11}b_{1i} + \dots + c_{1r}b_{ri} \\ &\vdots \end{aligned}$$

$$a_{in} = c_{n1}b_{1i} + \ldots + c_{nr}b_{ri}$$

das heißt, der Zeilenvektor lässt sich als Linearkombination der r Zeilenvektoren $c_j := (c_{1j}, \ldots, c_{nj})$, $j = 1, \ldots, r$ darstellen:

$$a_{i*} = b_{1i}c_1 + \ldots + b_{ri}c_r \ .$$

Wir haben also aus den *Koeffizienten* der Linearkombinationen $(*)$ einen Satz von *Erzeugenden* $c_1, \ldots, c_r$ für die Zeilenvektoren von A erhalten, wobei die *Basisvektoren* aus $(*)$ zu *Koeffizienten* geworden sind.

Wegen $\dim \operatorname{span}(c_1, \ldots, c_r) \leq r$ folgt für den Zeilenrang von A, dass $\operatorname{rang} A^{\mathrm{T}} \leq r$, also $\operatorname{rang} A^{\mathrm{T}} \leq \operatorname{rang} A$.

Ganz analog beweist man auch $\operatorname{rang} A \leq \operatorname{rang} A^{\mathrm{T}}$, und die Behauptung folgt. □

36.8 Bemerkungen

a) Man prüft leicht nach, dass $(A \cdot B)^{\mathrm{T}} = B^{\mathrm{T}} \cdot A^{\mathrm{T}}$.

b) Man schreibt (Spalten-) Vektoren gern platzsparend als transponierte Zeilenvektoren, z. B. $\begin{pmatrix} 4 \\ 0 \\ 1 \\ 2 \end{pmatrix} \in \mathbb{R}^4$ als $(4, 0, 1, 2)^{\mathrm{T}}$.

36.9 Folgerung: Links- und Rechtsinversion

Ist eine Matrix $A \in K^{n \times n}$ invertierbar, so gilt für ihre Inverse A^{-1} auch

$$A^{-1}A = I \ .$$

Beweis: A ist invertierbar genau dann, wenn $\operatorname{rang} A = n$. Wegen 36.7 ist dies genau dann der Fall, wenn $\operatorname{rang} A^{\mathrm{T}} = n$. Dies gilt genau dann, wenn auch A^{T} invertierbar ist.

Angenommen, A und A^{T} sind invertierbar mit

$$A^{-1} =: B \ , \qquad\qquad (A^{\mathrm{T}})^{-1} =: C \ ,$$

also

$$AB = I \ , \qquad\qquad A^{\mathrm{T}}C = I \ .$$

Daraus folgt $C^{\mathrm{T}}A = I$ und damit

$$C^{\mathrm{T}} = C^{\mathrm{T}}(AB) = (C^{\mathrm{T}}A)B = B \ .$$

Also gilt auch $BA = I$. □

Bemerkung: Die obige Eigenschaft hätten wir auch direkt daraus folgern können, daß $\mathrm{GL}(n, K)$ eine Gruppe ist und in einer Gruppe Links- und Rechtsinverses übereinstimmen (siehe Abschnitt 29.4).

37 Gauß-Algorithmus und lineare Gleichungssysteme

37.1 Motivation

- Lineare Gleichungssysteme treten in einer Vielzahl von Anwendungen auf und müssen gelöst werden.
- In Abschnitt 35.5 haben wir gesehen, dass Matrizen zur kompakten Notation linearer Gleichungssysteme benutzt werden können:

  Die Gleichheit $Ax = b$ (A Matrix, x, b Vektoren) verkörpert die Gleichungen

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m \ . \end{aligned}$$

- Wir betrachten den Fall $m = n$. Vorausgesetzt, A ist eine invertierbare Matrix (vgl. 35.11–35.14), dann erhalten wir durch Multiplikation mit A^{-1} auf der linken Seite (vgl. auch Satz 36.9) den Vektor x, d. h. inverse Matrizen spielen eine Rolle im Zusammenhang mit der Lösung linearer Gleichungssysteme.

  Aus 36.4a kennen wir den Zusammenhang zwischen Rang und Invertierbarkeit: Eine $n \times n$-Matrix A ist genau dann invertierbar, wenn $\operatorname{rang} A = n$.

Aus diesen Gründen ist es von Interesse, ein Verfahren zur Hand zu haben, das

- den Rang einer Matrix ermittelt
- die Inverse (sofern existent) berechnet

sowie unter geeigneten Voraussetzungen

- lineare Gleichungssysteme löst.

Dies alles leistet der **Gauß-Algorithmus.**

37.2 Idee

In Beispiel 36.4b wurde eine obere Dreiecksmatrix $\left(A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right)$ betrachtet, die auf der Diagonalen nur von 0 verschiedene Einträge hatte. Allgemein hat eine $n \times n$-Matrix mit dieser Eigenschaft stets den Rang n.

Die Idee des Gauß-Algorithmus besteht darin, eine beliebige Matrix in eine solche Dreiecksmatrix (oder eine ähnliche Form) umzuwandeln, und zwar auf eine Weise, die sicher stellt, dass sich der Rang der Matrix dabei nicht ändert.

37.3 Definition: Elementare Zeilenumformungen

Die folgenden Operationen auf Matrizen heißen **elementare Zeilenumformungen:**

a) Vertauschen zweier Zeilen,

b) Addition des λ-fachen ($\lambda \in K$) der Zeile a_{j*} zur Zeile a_{i*},

c) Multiplikation einer Zeile mit einem Skalar $\lambda \neq 0$.

37.4 Satz

Bei elementaren Zeilenumformungen bleibt der Rang einer Matrix stets erhalten.

Beweis:

a) offensichtlich, da $\text{span}(a_{1*}, \ldots, a_{m*})$ bei Vertauschung zweier Zeilenvektoren unverändert bleibt

b) Wir zeigen $\text{span}(a_{1*}, \ldots, a_{i*}, \ldots, a_{m*}) = \text{span}(a_{1*}, \ldots, a_{i*} + \lambda a_{j*}, \ldots, a_{m*})$.
„$\subset$“: Es sei $v \in \text{span}(a_{1*}, \ldots, a_{i*}, \ldots, a_{m*})$, also

$$\begin{aligned} v &= \lambda_1 a_{1*} + \ldots + \lambda_i a_{i*} + \ldots + \lambda_j a_{j*} + \ldots + \lambda_m a_{m*} \\ &= \lambda_1 a_{1*} + \ldots + \lambda_i (a_{i*} + \lambda a_{j*}) + \ldots + (\lambda_j - \lambda\lambda_i) a_{j*} + \ldots + \lambda_m a_{m*} \end{aligned}$$

$$\in \operatorname{span}(a_{1*}, \ldots, a_{i*} + \lambda a_{j*}, \ldots, a_{j*}, \ldots, a_{m*}) \ .$$

„$\supset$“ wird analog gezeigt.

c) Analog zu (b). $\square$

37.5 Gauß-Algorithmus

Gegeben sei eine Matrix $A = (a_{ij}) \in K^{m \times n}$.

- Betrachte a_{11}.
  - Ist $a_{11} \neq 0$, so subtrahiere von jeder Zeile a_{i*}, $i \geq 2$, das $\dfrac{a_{i1}}{a_{11}}$-fache der ersten Zeile. Danach ist a_{11} das einzige von Null verschiedene Element der ersten Spalte.
  - Ist $a_{11} = 0$, aber das erste Element a_{i1} einer anderen Zeile ungleich Null, so vertausche die beiden Zeilen a_{1*} und a_{i*}. Mit der neuen Matrix verfahre wie oben.
  - Sind alle a_{i1}, $i = 1, \ldots, m$, gleich 0, so beachte die erste Spalte nicht weiter und verfahre wie oben mit a_{12} statt a_{11}; sofern auch die 2. Spalte nur Nullen enthält, gehe zur 3. Spalte usf.

  Im Ergebnis dieses 1. Schrittes erhalten wir eine Matrix

$$A' = \left(\begin{array}{c|ccc} a'_{11} & a'_{12} & \ldots & a'_{1n} \\ \hline 0 & a'_{22} & \ldots & a'_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{m2} & \ldots & a'_{mn} \end{array}\right)$$

  (evtl. mit zusätzlichen Nullspalten links).

- Nun wird die erste Zeile und Spalte nicht mehr weiter betrachtet und auf die verbleibende Teilmatrix

$$\begin{pmatrix} a'_{22} & \ldots & a'_{2n} \\ \vdots & & \vdots \\ a'_{m2} & \ldots & a'_{mn} \end{pmatrix}$$

dasselbe Verfahren angewendet. Damit wird A' umgewandelt in

$$A'' = \begin{pmatrix} a'_{11} & a'_{12} & a'_{13} & & a'_{1n} \\ 0 & a''_{22} & a''_{23} & \dots & a''_{2n} \\ 0 & 0 & a''_{33} & \dots & a''_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & a''_{m3} & \dots & a''_{mn} \end{pmatrix}$$

- Danach betrachtet man die wiederum um eine Zeile und (mindestens) eine Spalte verkleinerte Teilmatrix usw., bis die gesamte Matrix auf eine Form A^* wie die folgende gebracht ist:

$$A^* = \begin{pmatrix} a & * & * & * & * & \dots & * \\ 0 & b & * & * & * & \dots & * \\ 0 & 0 & 0 & c & * & \dots & * \\ 0 & 0 & 0 & 0 & d & & * \\ \vdots & \vdots & \vdots & \vdots & & & \\ 0 & 0 & 0 & 0 & \dots & \dots & 0 \end{pmatrix}$$

($*$ steht jeweils für beliebige Werte; $a, b, c, d \neq 0$).

In dieser Matrix heißt der erste von 0 verschiedene Eintrag einer Zeile (a, b, c, d) **Leitkoeffizient.** Im gesamten Bereich unterhalb und links eines

Leitkoeffizienten enthält die Matrix nur Nullen:

$$\left(\begin{array}{ccccccc} a & * & * & * & * & \cdots & * \\ 0 & b & * & * & * & \cdots & * \\ 0 & 0 & 0 & c & * & \cdots & * \\ 0 & 0 & 0 & 0 & d & & * \\ \vdots & \vdots & \vdots & \vdots & & & \\ 0 & 0 & 0 & 0 & \cdots & \cdots & 0 \end{array}\right)$$

Eine solche Matrix heißt **Matrix in Zeilen-Stufen-Form.**

Gauß-Algorithmus als rekursive Funktion (Aufruf: Gauss(1,1)):

Gauss (i,j):
- falls $i = m$ oder $j > n$:
  - Ende
- falls $a_{ij} = 0$:
  - suche $a_{kj} \neq 0$, $k > i$; wenn dies nicht existiert:
    - Gauss $(i,\ j+1)$
    - Ende
  - vertausche Zeile i mit Zeile k
- für alle $k > i$:
  - subtrahiere $\frac{a_{kj}}{a_{ij}} \cdot$ Zeile i von Zeile k $\qquad (*)$
- Gauss $(i+1,\ j+1)$
- Ende.

Das Matrixelement a_{ij}, das in der Zeile $(*)$ als Nenner auftritt, heißt **Pivotelement.**

37.6 Beispiel

$$A = \begin{pmatrix} 0 & 4 & 3 & 1 & 5 \\ 1 & 3 & 2 & 4 & 2 \\ 3 & 1 & 2 & 1 & 0 \\ 2 & 2 & 3 & -2 & 3 \end{pmatrix} \quad \rightarrow \quad \begin{pmatrix} 1 & 3 & 2 & 4 & 2 \\ 0 & 4 & 3 & 1 & 5 \\ 3 & 1 & 2 & 1 & 0 \\ 2 & 2 & 3 & -2 & 3 \end{pmatrix} \begin{matrix} \\ \\ -3\times \\ \end{matrix} \begin{matrix} \\ \\ \\ -2\times \end{matrix}$$

$$A' = \begin{pmatrix} 1 & 3 & 2 & 4 & 2 \\ 0 & 4 & 3 & 1 & 5 \\ 0 & -8 & -4 & -11 & -6 \\ 0 & -4 & -1 & -10 & -1 \end{pmatrix} \begin{matrix} \\ \\ +2\times \\ \end{matrix} \begin{matrix} \\ \\ \\ +1\times \end{matrix}$$

$$A'' = \begin{pmatrix} 1 & 3 & 2 & 4 & 2 \\ 0 & 4 & 3 & 1 & 5 \\ 0 & 0 & 2 & -9 & 4 \\ 0 & 0 & 2 & -9 & 4 \end{pmatrix} \begin{matrix} \\ \\ \\ -1\times \end{matrix}$$

$$A^* = A''' = \begin{pmatrix} 1 & 3 & 2 & 4 & 2 \\ 0 & 4 & 3 & 1 & 5 \\ 0 & 0 & 2 & -9 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

37.7 Satz: Rang einer Matrix in Zeilen-Stufen-Form

Der Rang einer Matrix in Zeilen-Stufen-Form ist gleich der Anzahl ihrer Leitkoeffizienten.

Beweis: Die Anzahl der Leitkoeffizienten sei l.

Jede Zeile, die einen Leitkoeffizienten enthält, ist linear unabhängig von dem System der darunter stehenden Zeilen. Nimmt man also von unten nach oben die linear unabhängigen Zeilen zur Basis hinzu, so folgt, dass

$$\dim \operatorname{span}(a_{1*}, \ldots, a_{m*}) \geq l \ .$$

Andererseits ist auch

$$\dim \operatorname{span}(a_{1*}, \ldots, a_{m*}) \leq l \ ,$$

da es nur l Zeilenvektoren ungleich 0 gibt. □

37.8 Satz: Zeilenumformungen als Matrixmultiplikationen

Jede elementare Zeilenumformung für $m \times n$-Matrizen kann als Multiplikation von links mit einer geeigneten invertierbaren $m \times m$-Matrix ausgedrückt werden:

a) Vertauschung der Zeilen i und j:

$$\begin{pmatrix} 1 & 0 & & \dots & & & 0 \\ 0 & 1 & & \dots & & & 0 \\ & & 1 & & & & \\ & & & 0 \ \dots \ 1 & & & \\ \vdots & & & \vdots \quad\quad \vdots & & & \vdots \\ & & & 1 \ \dots \ 0 & & & \\ & & & & 1 & & \\ & & & & & \ddots & 0 \\ 0 & & & \dots & & 0 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \leftarrow \text{Zeile } i \\ \\ \leftarrow \text{Zeile } j \\ \\ \\ \end{matrix}$$

b) Addition von $\lambda \times$ Zeile j zu Zeile i:

$$\begin{pmatrix} 1 & 0 & & \dots & & & 0 \\ 0 & \ddots & & & & & \\ & & 1 & \dots & \lambda & & \\ \vdots & & & \ddots & \vdots & & \vdots \\ & & & & 1 & & \\ & & & & & \ddots & 0 \\ 0 & & & \dots & & 0 & 1 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow \text{Zeile } i \\ \\ \leftarrow \text{Zeile } j \\ \\ \\ \end{matrix}$$

c) Multiplikation von Zeile i mit $\lambda \neq 0$:

$$\begin{pmatrix} 1 & 0 & & \dots & & & 0 \\ 0 & \ddots & & & & & \\ & & 1 & & & & \\ \vdots & & & \lambda & & & \vdots \\ & & & & 1 & & \\ & & & & & \ddots & 0 \\ 0 & & & \dots & & 0 & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \leftarrow \text{Zeile } i \\ \\ \\ \end{matrix}$$

(ohne Beweis)

37.9 Umformung einer invertierbaren Matrix zur Einheitsmatrix

Es sei A eine invertierbare $n \times n$-Matrix. Wegen $\operatorname{rang} A = n$ hat sie die Zeilen-Stufen-Form

$$A' = \begin{pmatrix} a'_{11} & * & \dots & \dots & * \\ 0 & a'_{22} & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & * \\ 0 & \dots & \dots & 0 & a'_{nn} \end{pmatrix} \qquad \text{mit } a'_{ii} \neq 0,\ i = 1, \dots, n.$$

Multiplikation jeder Zeile a'_{i*} mit $\dfrac{1}{a'_{ii}}$ ergibt eine obere Dreiecksmatrix $A'' = (a''_{ij})$, deren sämtliche Diagonalelemente gleich 1 sind.

Mittels weiterer elementarer Zeilenumformungen wird die Matrix in die Einheitsmatrix umgeformt:

- Subtrahiere für alle $i < n$ das a''_{in}-fache der Zeile n von Zeile i. Danach ist $a''_{nn} = 1$ das einzige Element $\neq 0$ in der letzten Spalte.
- Subtrahiere für alle $i < n - 1$ das $a''_{i,n-1}$-fache der Zeile $n - 1$ von Zeile i

usw.

37.10 Satz: Berechnung der inversen Matrix

Wird eine invertierbare $n \times n$-Matrix A durch elementare Zeilenumformungen in die Einheitsmatrix I umgeformt, so erhält man die Inverse A^{-1}, indem man dieselben Umformungen auf die Einheitsmatrix anwendet.

Beispiel:

$$
\begin{array}{cc}
A & I \\
\begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{matrix} \\ -2\times \\ \\ \end{matrix} \\
\begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -4 & 0 & 1 \end{pmatrix} \begin{matrix} \\ +1\times \\ \\ \end{matrix} \\
\begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & -1 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -6 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \times(-1) \\ \times(-1) \end{matrix} \\
\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 2 & -1 & 0 \\ 6 & -1 & -1 \end{pmatrix} \begin{matrix} \\ -1\times \\ \end{matrix} \begin{matrix} \\ \\ -2\times \end{matrix} \\
\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{pmatrix} \\
I & A^{-1}
\end{array}
$$

Probe:

$$
\begin{pmatrix} -11 & 2 & 2 \\ -4 & 0 & 1 \\ 6 & -1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 3 \\ 4 & 1 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .
$$

Beweis des Satzes: Es seien $D_1, \ldots, D_k$ die Matrizen, die gemäß Satz 37.8 die elementaren Zeilenumformungen darstellen, durch die A in I übergeht. Dann ist

$$I = D_k D_{k-1} \ldots D_1 A = (D_k D_{k-1} \ldots D_1) A$$

und somit

$$A^{-1} = D_k D_{k-1} \ldots D_1 = D_k D_{k-1} \ldots D_1 I \ .$$

□

Bemerkung: Eine alternative Sichtweise auf die obige Berechnung ist, daß wir simultan die linearen Gleichungssysteme für die Spalten von A^{-1} lösen (siehe nächster Abschnitt). Denn es gilt für die i-te Spalte a_i^{-1} der inversen Matrix A^{-1} von A, $Aa_i^{-1} = e_i$, wobei e_i die i-te Spalte der Einheitsmatrix ist bzw. der i-te Basisvektor der Standardbasis im K^n.

Wie kann man den Gauß-Algorithmus zum Lösen linearer Gleichungssysteme verwenden?

37.11 Lineare Gleichungssysteme

Ein lineares Gleichungssystem mit m Gleichungen und n Unbekannten hat die Form

$$Ax = b$$

mit $A \in K^{m \times n}$, $x \in K^n$, $b \in K^m$.

Falls $b \neq 0$, spricht man von einem **inhomogenen** Gleichungssystem. $Ax = 0$ heißt zugehöriges **homogenes** Gleichungssystem.

Die Matrix $(A, b) \in K^{m \times (n+1)}$, d. h. A mit rechts angefügter Spalte b, heißt **erweiterte Matrix** des Systems.

Interpretiert man A als lineare Abbildung, so sind Lösungen des Systems $Ax = b$ gerade die Vektoren, die durch A auf b abgebildet werden.

37.12 Satz: Lösungsverhalten linearer Gleichungssysteme

a) Die Lösungsmenge von $Ax = 0$ ist $\operatorname{Ker} A$ und daher ein Unterraum von K^n.

b) Die folgenden Aussagen sind äquivalent:

   i) $Ax = b$ hat mindestens eine Lösung.

   ii) $b \in \operatorname{Im} A$.

   iii) $\operatorname{rang} A = \operatorname{rang}(A, b)$.

c) Ist w eine Lösung von $Ax = b$, so ist die vollständige Lösungsmenge gleich $w + \operatorname{Ker} A := \{w + x \mid x \in \operatorname{Ker} A\}$.

Beweis:

a) Klar nach Definition von $\operatorname{Ker} A$.

b) (i)⇒(ii): Existiert eine Lösung w, so gilt $Aw = b$, d. h. $b \in \operatorname{Im} A$.

(ii)⇒(iii): Ist $b \in \operatorname{Im} A$, so ist b Linearkombination der Spalten von A. Damit ist $\operatorname{rang}(A, b) = \operatorname{rang} A$.

(iii)⇒(i): Ist $\operatorname{rang}(A, b) = \operatorname{rang} A$, so ist b Linearkombination der Spalten von A d.h. das lineare Gleichungssystem $Ax = b$ hat mindestens eine Lösung.

„⊃“: Es sei v eine weitere Lösung von $Ax = b$. Dann gilt

$$A(v - w) = Av - Aw = b - b = 0 \,,$$

d. h. $v - w \in \operatorname{Ker} A$ und folglich $v \in w + \operatorname{Ker} A$. Also liegt die Lösungsmenge von $Ax = b$ in $w + \operatorname{Ker} A$. □

37.13 Bemerkungen

a) Ist $\operatorname{rang}(A, b) > \operatorname{rang} A$, so hat $Ax = b$ keine Lösung.

b) Jedes homogene System hat mindestens eine Lösung: 0.

c) Zur Lösung des inhomogenen Systems benötigt man

- die vollständige Lösung des homogenen Systems,
- eine spezielle Lösung des inhomogenen Systems.

d) Aus (b) und (c) folgt: Besitzt ein inhomogenes System $A\,x = b$ eine Lösung, so ist diese eindeutig, wenn $\operatorname{Ker} A = \{0\}$ ist.

Um mithilfe des Gauß-Algorithmus das Lösungsverhalten von $Ax = b$ zu studieren, bezeichnen wir mit $\operatorname{Lös}(A, b)$ die Lösungsmenge von $Ax = b$. Wir benötigen zunächst zwei Hilfsaussagen.

37.14 Lemma: Invarianz der Lösungsmenge unter Matrixmultiplikation mit invertierbarer Matrix

Ist $B \in \operatorname{GL}(m, K)$ und $A \in K^{m \times n}$, $b \in K^m$, so gilt

$$\operatorname{Lös}(A, b) = \operatorname{Lös}(BA, Bb) \,.$$

Beweis: Ist $x \in \text{Lös}(A, b)$, so gilt $Ax = b$. Damit ist auch $BAx = Bb$, also $x \in \text{Lös}(BA, Bb)$.

Ist umgekehrt $x \in \text{Lös}(BA, Bb)$, so gilt $BAx = Bb$. Da $B \in \text{GL}(m, K)$, existiert ein $B^{-1} \in \text{GL}(m, K)$ nach Satz 35.13. Damit folgt $B^{-1}BAx = B^{-1}Bb$ und somit $Ax = b$, d. h. $x \in \text{Lös}(A, b)$. □

37.15 Satz: Invarianz der Lösungsmenge unter elementaren Zeilenumformungen

Ist die erweiterte Systemmatrix (A', b) aus (A, b) durch elementare Zeilenumformungen entstanden (mit anderen Worten, es wurden die gleichen Zeilenumformungen an A und b vorgenommen), so gilt

$$\text{Lös}(A', b') = \text{Lös}(A, b) \ .$$

Beweisidee: Elementare Zeilenumformungen entsprechen nach 37.8 der Multiplikation mit invertierbaren Matrizen $D_k, D_{k-1}, \ldots, D_1$. □

.

Nun können wir zum eigentlichen Ziel kommen.

37.16 Gauß-Algorithmus zum Lösen linearer Gleichungssysteme

Zur Lösung von $Ax = b$ geht man in vier Schritten vor.

i) Schritt 1: Bringe die Matrix (A, b) in Gauß-Jordan-Form (A', b').

   Die **Gauß-Jordan-Form** ist eine spezielle Zeilen-Stufen-Form, bei der alle Leitkoeffizienten gleich 1 sind und oberhalb der Leitkoeffizienten nur Nullen stehen.

   Enthält in der Gauß-Jordan-Form (A', b') die Spalte b' einen Leitkoeffizienten, so ist $\text{rang}(A', b') > \text{rang}\, A'$, und das System hat keine Lösung (Ende

des Algorithmus). Andernfalls ist $\operatorname{rang}(A', b') = \operatorname{rang} A'$ (Algorithmus fortsetzen).

Beispiel: ($K = \mathbb{R}$)

$(A', b') = \left(\begin{array}{cccccc|c} 1 & 0 & 3 & 0 & 0 & 2 & 2 \\ 0 & 1 & 2 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 1 & 0 & 5 & 6 \\ 0 & 0 & 0 & 0 & 1 & 4 & 0 \end{array}\right)$ ist in Gauß-Jordan-Form. Man liest ab: $\operatorname{rang} A' = 4$, $\operatorname{rang}(A', b') = 4$. Es existieren also Lösungen, wir müssen weitermachen.

ii) Schritt 2: Finde die Lösungsmenge U des homogenen Gleichungssystems $A'x = 0$.

Wähle hierzu die Unbekannten, die zu den Spalten ohne Leitkoeffizienten gehören, als freie Parameter.

Beispiel: Im obigen Beispiel setzen wir $x_3 =: \lambda$, $x_6 =: \mu$. Dann hat das homogene System die Lösungsmenge

$$\begin{aligned} x_1 &= -3\lambda - 2\mu \\ x_2 &= -2\lambda - \mu \\ x_3 &= \lambda \\ x_4 &= -5\mu \\ x_5 &= -4\mu \\ x_6 &= \mu \end{aligned}$$

oder als Vektorgleichung

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} = \begin{pmatrix} -3\lambda - 2\mu \\ -2\lambda - \mu \\ \lambda \\ -5\mu \\ -4\mu \\ \mu \end{pmatrix} = \lambda \begin{pmatrix} -3 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} -2 \\ -1 \\ 0 \\ -5 \\ -4 \\ 1 \end{pmatrix},$$

d. h.

$$U = \operatorname{span}\left(\begin{pmatrix} -3 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ -1 \\ 0 \\ -5 \\ -4 \\ 1 \end{pmatrix} \right).$$

iii) Schritt 3: Suche eine spezielle Lösung des inhomogenen Gleichungssystems $A'x = b'$.

Setze hierzu die Unbekannten, die zu den Spalten ohne Leitkoeffizienten gehören, gleich 0 (möglich, da dies freie Parameter sind).

Beispiel: Mit $x_3 = 0$ und $x_6 = 0$ erlaubt die Gauß-Jordan-Form im obigen Beispiel die direkte Bestimmung von

$$x_1 = 2\,, \quad x_2 = 4\,, \quad x_4 = 6\,, \quad x_5 = 0\,,$$

also $w = \begin{pmatrix} 2 \\ 4 \\ 0 \\ 6 \\ 0 \\ 0 \end{pmatrix}$.

iv) Schritt 4: Die Lösungsmenge von $Ax = b$ ist dann $w + U$.

Beispiel:

$$\mathrm{Lös}(A,b) = \left\{ \begin{pmatrix} 2 \\ 4 \\ 0 \\ 6 \\ 0 \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} -3 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} -2 \\ -1 \\ 0 \\ -5 \\ -4 \\ 1 \end{pmatrix} \;\middle|\; \lambda, \mu \in \mathbb{R} \right\}$$

37.17 Geometrische Interpretation linearer Gleichungssysteme

Es sei $A \in K^{m \times n}$, $x \in K^n$, $b \in K^m$. Wir wissen: $\mathrm{Lös}(A,0) = \mathrm{Ker}\, A$ ist Unterraum des K^n. (Jedoch ist $\mathrm{Lös}(A,b)$ im Allgemeinen kein Unterraum!)

Für die Dimension von $\mathrm{Lös}(A,0)$ gilt

$$\underbrace{\dim \mathrm{Ker}\, A}_{\dim \mathrm{Lös}(A,0)} + \underbrace{\dim \mathrm{Im}\, A}_{\mathrm{rang}\, A} = \underbrace{\dim K^n}_{n}\,,$$

also

$$\dim \mathrm{Lös}(A,0) = n - \mathrm{rang}\, A\,.$$

Beispiel: $A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{R}^{3\times 3}$, $b = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

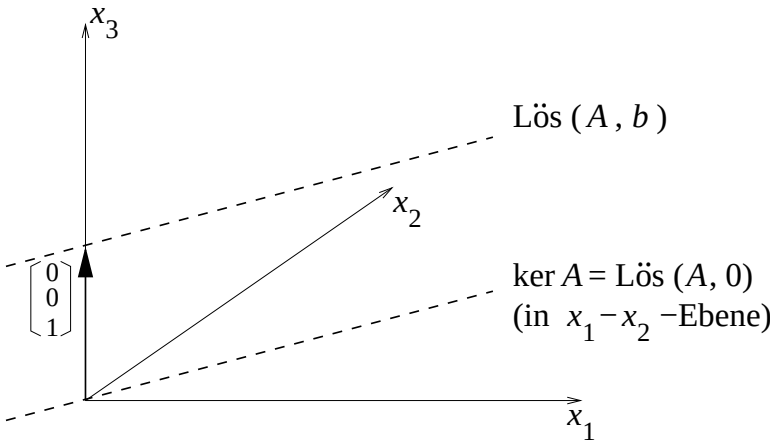
$n = 3$, $\operatorname{rang} A = 2 \Rightarrow \dim \text{Lös}(A, 0) = 1$.

$$\text{Lös}(A, 0) = \left\{ \begin{pmatrix} \lambda \\ \lambda \\ 0 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\} \qquad \text{Ursprungsgerade}$$

Spezielle Lösung des inhomogenen Systems: $w = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

Allgemeine Lösung:

$$\text{Lös}(A, b) = \left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + \lambda \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\} \qquad \text{Gerade}$$

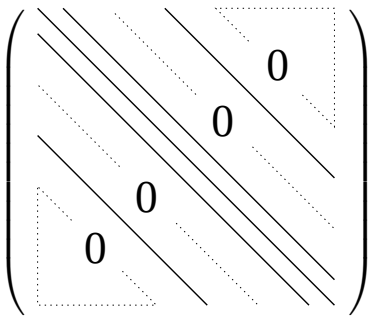


38 Iterative Verfahren für lineare Gleichungssysteme

38.1 Motivation

- Viele praktische Probleme führen auf sehr große lineare Gleichungssysteme, bei denen die Systemmatrix **dünn besetzt** ist, d. h. nur wenige von Null verschiedene Einträge aufweist.

  Beispiel: Pentadiagonalmatrix bei der Berechnung von 2-D-Diffusionsfiltern in der Bildverarbeitung

- Aus Speicherplatzgründen will man oft nur die von 0 verschiedenen Elemente abspeichern.

  Beispiel: Ein Grauwertbild mit 512×512 Pixeln führt zu $512^2 = 262\,144$ Gleichungen mit ebenso vielen Unbekannten. Bei 4 Byte je Eintrag (Datentyp `float`) und vollem Abspeichern benötigt die Pentadiagonalmatrix $4 \cdot 512^4$ Byte ≈ 275 GB, bei effizientem Abspeichern nur $5 \cdot 4 \cdot 512^2$ Byte $\approx$ 5,2 MB!

- Direkte Verfahren wie der Gauß-Algorithmus können die Nullen auffüllen (fill in) und so zu einem enormen Speicherplatzbedarf führen.

  Zudem ist ihr Rechenaufwand oft zu hoch: $\mathrm{O}(n^3)$ Operationen für ein $n \times n$-Gleichungssystem.

- Daher verwendet man oft iterative Näherungsverfahren, die kaum zusätzlichen Speicherplatz benötigen und nach wenigen Schritten eine brauchbare Approximation liefern.

38.2 Grundstruktur klassischer iterativer Verfahren

Gegeben: $A \in \mathbb{R}^{n \times n}, b \in \mathbb{R}^n$

Gesucht: $x \in \mathbb{R}^n$ mit $A\,x = b$

Falls $A = S - T$ mit einer einfach zu invertierenden Matrix S ist (z. B. Diagonalmatrix, Dreiecksmatrix), so kann man $A\,x = b$ umformen in

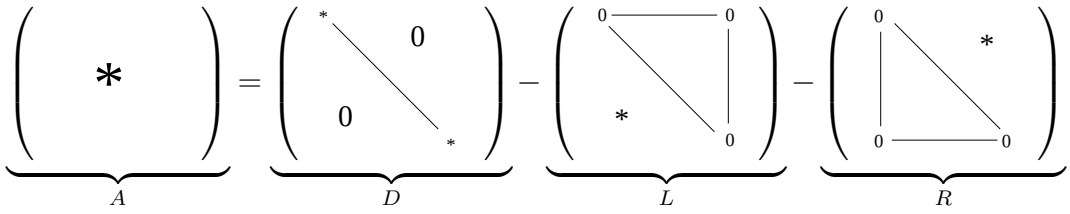
$$S\,x = T\,x + b$$

und mit einem Startvektor $x^{(0)} \in \mathbb{R}^n$ die Fixpunktiteration

$$S\,x^{(k+1)} = T\,x^{(k)} + b\,, \quad k = 0, 1, 2, \ldots$$

anwenden.

Wir wollen nun drei verschiedene Aufspaltungen $A = S - T$ untersuchen. Dazu sei $A = D - L - R$ eine Aufspaltung von A in eine Diagonalmatrix D, eine strikte untere Dreiecksmatrix (also eine untere Dreiecksmatrix, die auf der Diagonale nur Nullen hat) und eine strikte obere Dreiecksmatrix R.



Bemerkung: In Bezug auf die Komponenten von $A = (a_{ij})$ gilt

$$D_{ij} = \begin{cases} a_{ii}, & i = j \\ 0 & \text{sonst} \end{cases}, \quad L_{ij} = \begin{cases} -a_{ij}, & i > j, \\ 0 & \text{sonst} \end{cases}, \quad R_{ij} = \begin{cases} -a_{ij}, & j < i, \\ 0 & \text{sonst} \end{cases}.$$

38.3 Das Jacobi-Verfahren (Gesamtschrittverfahren)

Hier wählt man $S := D$ und $T := L + R$. In jeder Iteration wird also nur das Diagonalsystem

$$D\,x^{(k+1)} = (L + R)\,x^{(k)} + b$$

nach $x^{(k+1)}$ aufgelöst, d. h. es wird nur durch die Diagonalelemente dividiert:

$$x^{(k+1)} = D^{-1}\Big((L + R)\,x^{(k)} + b\Big)$$

oder explizit:

$$x_i^{(k+1)} = \frac{1}{a_{ii}} \left(-\sum_{\substack{j=1 \\ j \neq i}}^{n} a_{ij} x_j^{(k)} + b_i \right), \quad i = 1, \ldots, n$$

38.4 Beispiel

$A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ führt auf das Diagonalsystem

$$2x_1^{(k+1)} = x_2^{(k)} + 3$$
$$2x_2^{(k+1)} = x_1^{(k)} + 4 \, .$$

Bei vierstelliger Genauigkeit und Startvektor $x^{(0)} = (0,0)^{\mathrm{T}}$ erhält man

k	$x_1^{(k)}$	$x_2^{(k)}$
0	0	0
1	1,5	2
2	2,5	2,75
3	2,875	3,25
4	3,125	3,438
5	3,219	3,563
6	3,282	3,610
7	3,305	3,641
8	3,321	3,653
9	3,327	3,661
10	3,331	3,664
11	3,332	3,666
12	3,333	3,666

Die exakte Lösung ist $x_1 = 3\,\frac{1}{3}$, $x_2 = 3\,\frac{2}{3}$.

Bemerkung: Vorteil des Jacobi-Verfahrens ist, da die Berechnung von $x_i^{(k+1)}$ und $x_j^{(k+1)}$ für $i \neq j$ unabhängig sind. Damit ist die Parallelisierung der Berechnung sehr einfach. Nachteil ist typischerweise eine geringere Konvergenzgeschwindigkeit gegenüber den folgenden Verfahren.

38.5 Das Gauß-Seidel-Verfahren (Einzelschrittverfahren)

Hier setzt man $S := D - L$, $T := R$.

In jeder Iteration wird daher das Dreieckssystem

$$(D - L)\, x^{(k+1)} = R\, x^{(k)} + b$$

in Komponenten, für $i = 1, \ldots, n$,

$$a_{ii} x_i^{(k+1)} + \sum_{j=1}^{i-1} a_{ij} x_j^{(k+1)} = - \sum_{j=i+1}^{n} a_{ij} x_j^k + b_i,$$

durch einfache Rückwärtssubstitution gelöst:

$$x_i^{(k+1)} = \frac{1}{a_{ii}} \left(- \sum_{j=1}^{i-1} a_{ij} x_j^{(k+1)} - \sum_{j=i+1}^{n} a_{ij} x_j^{(k)} + b_i \right) \, , \quad i = 1, \ldots, n \, ,$$

d. h. die neuen Werte $x_j^{(k+1)}$, $j = 1, \ldots, i-1$ werden für die Berechnung des i-ten Elements $x_i^{(k+1)}$ verwendet.

38.6 Beispiel

$A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$, $x^{(0)} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ergibt

$$x_1^{(k+1)} = \frac{1}{2}(x_2^{(k)} + 3)$$
$$x_2^{(k+1)} = \frac{1}{2}(x_1^{(k+1)} + 4)$$

k	$x_1^{(k)}$	$x_2^{(k)}$
0	0	0
1	1,5	2,75
2	2,875	3,438
3	3,219	3,609

k	$x_1^{(k)}$	$x_2^{(k)}$
4	3,305	3,652
5	3,326	3,663
6	3,332	3,666
7	3,333	3,666

Bemerkung: Vorteil ist die etwa doppelt so schnelle Konvergenz gegenüber dem Jacobi-Verfahren. Nachteil ist, daß eine direkte Parallelisierung aufgrund der Abhängigkeit von $x_i^{(k+1)}$ von $x_j^{(k+1)}$, $j = 1, \ldots, i-1$ nicht möglich ist.

38.7 SOR-Verfahren (Successive Overrelaxation)

Sei $\omega \in \mathbb{R}$. Setze: $S := \frac{1}{\omega}D - L$ und $T := \left(\frac{1}{\omega} - 1\right)D + R$.

Bemerkung:

- Gauss-Seidel Verfahren ist Spezialfall für $\omega = 1$.
- Man kann zeigen, daß für $\omega \notin (0, 2)$ man nie Konvergenz hat.

In jeder Iteration wird das Dreieckssystem

$$(\frac{1}{\omega}D - L)\, x^{(k+1)} = \left(\frac{1}{\omega} - 1\right)Dx^{(k)} + R\, x^{(k)} + b$$

in Komponenten, für $i = 1, \ldots, n$,

$$\frac{1}{\omega} a_{ii} x_i^{(k+1)} + \sum_{j=1}^{i-1} a_{ij} x_j^{(k+1)} = \Big(\frac{1}{\omega} - 1\Big) a_{ii} x_i^{(k)} - \sum_{j=i+1}^{n} a_{ij} x_j^{(k)} + b_i,$$

durch Rückwärtssubstitution gelöst:

$$\begin{aligned} x_i^{(k+1)} &= \frac{\omega}{a_{ii}} \left(- \sum_{j=1}^{i-1} a_{ij} x_j^{(k+1)} - \sum_{j=i+1}^{n} a_{ij} x_j^{(k)} + b_i + \Big(\frac{1}{\omega} - 1\Big) a_{ii} x_i^{(k)} \right) \\ &= x_i^k + \omega \Big[\frac{1}{a_{ii}} \Big(- \sum_{j=1}^{i-1} a_{ij} x_j^{(k+1)} - \sum_{j=i+1}^{n} a_{ij} x_j^{(k)} + b_i \Big) - x_i^{(k)} \Big] \\ &= x_i^k + \omega \Big[\tilde{x}_i^{(k+1)} - x_i^{(k)} \Big], \quad i = 1, \ldots, n \, , \end{aligned}$$

wobei $\tilde{x}_i^{(k+1)}$ dem Ergebnis des Gauss-Seidel Verfahrens aus der Menge

$$(x_1^{(k+1)}, \ldots, x_{i-1}^{(k+1)}, x_i^{(k)}, \ldots, x_n^{(k)})$$

entspricht. Da typischerweise $1 < \omega < 2$ als Parameter verwendet wird, entspricht daher der Iterationsschritt einer Extrapolation des Iterationsschritt des Gauss-Seidel-Verfahrens d.h. man geht etwas weiter in die Richtung, die vom Gauss-Seidel-Verfahren vorgegeben wird.

Für große Gleichungssysteme kann damit die Iterationsanzahl für ein geeignetes ω oft um eine Zehnerpotenz gesenkt werden.

38.8 Konvergenzresultate

a) Die Jacobi-, Gauß-Seidel- und SOR-Verfahren können als Fixpunktiterationen interpretiert werden. Ihre Konvergenz kann unter anderem mittels des Banach'schen Fixpunktsatzes (vgl. MfI 1, 22.2) untersucht werden; danach liegt Konvergenz vor, wenn die lineare Abbildung $f : \mathbb{R}^n \to \mathbb{R}^n, \; x \mapsto S^{-1}Tx$ kontrahierend ist d.h. es existiert $L \in \mathbb{R}$ mit $L < 1$, so daß für alle $x, y \in \mathbb{R}^n$,

$$\|f(x) - f(y)\| \; \leq \; L \, \|x - y\| \, .$$

(Der Begriff der Norm $\|x\|$ eines Vektors x wird in Kapitel 40 und 41 eingeführt).
Die Abbildung f ist nicht in allen Fällen kontrahierend.

b) Für wichtige Spezialfälle existieren jedoch Konvergenzaussagen, z. B.:

- Ist die Systemmatrix $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ streng **diagonaldominant,** d. h. für jedes i gilt

$$|a_{ii}| > \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{ij}| \ ,$$

  so konvergieren das Jacobi- und das Gauß-Seidel-Verfahren.

- Allgemein kann man Konvergenz zeigen, wenn die spektrale Norm (siehe Kapitel **??**) von $S^{-1}T$ kleiner 1 ist.

38.9 Effizienz

a) Die vorgestellten Verfahren sind die einfachsten, allerdings nicht die effizientesten iterativen Verfahren zum Lösen linearer Gleichungssysteme.

b) Effizientere, aber kompliziertere Verfahren:

   - PCG-Verfahren (PCG = preconditioned conjugate gradients)
   - Mehrgitterverfahren (Multigrid)

   Vgl. dazu numerische Spezialliteratur.

c) Hocheffiziente Ansätze wie etwa die Mehrgitterverfahren verwenden oft das Gauß-Seidel-Verfahren als Grundbaustein. Mit ihnen ist es z. T. möglich, lineare Gleichungssysteme in *optimaler* Komplexität (d. h. $O(n)$) zu lösen.

39 Determinanten

39.1 Motivation

- Wir stellen uns das Ziel, wesentliche Information über
  - die Invertierbarkeit einer $n \times n$-Matrix
  - das Lösungsverhalten zugehöriger linearer Gleichungssysteme

  möglichst kompakt auszudrücken: durch eine einzelne Zahl.
- Wir definieren also eine K-wertige Funktion auf Matrizen $A \in K^{n \times n}$.
- Determinanten haben auch eine geometrische Bedeutung: Volumenbestimmung eines Parallelepipeds

39.2 Definition

Eine **Multilinearform** (oder k-Form) ist eine Abbildung

$$F : K^n \times K^n \times \ldots \times K^n \to K, \quad (v_1, \ldots, v_k) \mapsto F(v_1, \ldots, v_k),$$

die linear in jedem Argument ist, d.h. für alle $c_1, \ldots, c_m \in K$ und $u_1, \ldots, u_m \in K^n$ gilt

$$F(\ldots, \sum_{k=1}^{m} c_k u_k, \ldots) \;=\; \sum_{k=1}^{m} c_k F(\ldots, u_k, \ldots).$$

Eine Multilinearform F heißt alternierend, genau dann wenn F null ist, wenn zwei Argumente gleich sind, d.h. $F(\ldots, a_i, \ldots, a_i, \ldots) = 0$.

Bemerkung:

- Multilinear bedeutet linear in jedem Argument.
- Im folgenden betrachten wir immer n-Formen, d.h. die Anzahl der Argumente der Multilinearform ist gleich der Dimension von K^n.
- Wenn nur die Körper $\mathbb{R}$ oder $\mathbb{C}$ betrachtet werden, werden alternierende Multilinearformen oft über den Vorzeichenwechsel bei Vertauschung von Argumenten definiert. Während aus der obigen definierenden Eigenschaft

der alternierenden Multilinearform immer der Vorzeichenwechsel bei Vertauschung der Argumente folgt (siehe folgender Satz), gilt die Umkehrung im Allgemeinen nicht. Denn für einen Vektorraum über einem allgemeinen Körper folgt für $u \in K^n$ aus $u = -u$ **nicht** zwingend $u = 0$. Denn für $K = \mathbb{Z}_2$ gilt $1 + 1 = 0$ (1 ist zu sich selbst-invers d.h. $-1 = 1$) und daher folgt aus $1 = -1$ nicht $1 = 0$!

39.3 Satz (Eigenschaften von alternierenden Multilinearformen)

Sei F eine alternierende Multilinearform, dann gilt

1. $F(\ldots, u, \ldots, v, \ldots) = -F(\ldots, u, \ldots, v, \ldots)$ für alle $u, v \in K^n$
   (Vorzeichenwechsel bei Vertauschung von Argumenten),
2. $F(u_1, \ldots, u_n) = 0$, falls $u_1, \ldots, u_n \in K^n$ linear abhängig sind.

Beweis:

1. Nach Definition gilt für eine alternierende Multilinearform:

   $$F(\ldots, u + v, \ldots, u + v, \ldots) = 0.$$

   Unter Ausnützung der Linearität in beiden Argumenten erhalten wir,

   $$\begin{aligned} 0 =& F(\ldots, u + v, \ldots, u + v, \ldots) = F(\ldots, u, \ldots, u + v, \ldots) + F(\ldots, v, \ldots, u + v, \ldots) \\ =& F(\ldots, u, \ldots, u, \ldots) + F(\ldots, u, \ldots, v, \ldots) \\ & + F(\ldots, v, \ldots, u, \ldots) + F(\ldots, v, \ldots, v, \ldots) \\ =& F(\ldots, u, \ldots, v, \ldots) + F(\ldots, v, \ldots, u, \ldots), \end{aligned}$$

   wobei ausgenützt wurde, daß der Wert einer alternierenden Multilinearform null ist, wenn zwei Argumente gleich sind. Damit folgt mit der Eindeutigkeit des inversen Elements bezüglich der Vektoraddition $F(\ldots, u, \ldots, v, \ldots) = -F(\ldots, u, \ldots, v, \ldots)$.

2. Da $u_1, \ldots, u_n \in K^n$ linear abhängig sind, kann einer der Vektoren als Linearkombination der anderen geschrieben werden. ObdA nehmen wir an, daß $c_1, \ldots, c_n \in K$ existieren, so daß $u_n = \sum_{k=1}^{n-1} c_k u_k$. Unter Ausnützung der

Linearität im n-ten Argument erhalten wir für den Wert der Multilinearform,

$$F(u_1,\ldots,u_{n-1},u_n) = F\Big(u_1,\ldots,u_{n-1},\sum_{k=1}^{n-1} c_k u_k\Big) = \sum_{k=1}^{n-1} c_k\, F(u_1,\ldots,u_{n-1},u_k).$$

Die Terme, $F(u_1,\ldots,u_{n-1},u_k)$, $k=1,\ldots,n$ sind alle null, da immer zwei Argumente gleich sind. Damit folgt die Aussage.

39.4 Definition

Eine **Determinantenform** ist eine alternierende Multilinearform F mit $F(e_1,\ldots,e_n)=1$, wobei $(e_1,\ldots,e_n)$ die kanonische Standardbasis im K^n ist.

39.5 Satz (Eindeutigkeitssatz für alternierende Multilinearformen)

Es sei $F: K^n \times \ldots \times K^n \to K$ eine alternierende Multilinearform.

1. Gilt $F(e_1,\ldots,e_n)=0$, so ist $F\equiv 0$.
2. Stimmen zwei alternierende Multilinearformen auf der kanonischen Basis überein, so sind sie gleich. Insbesondere gibt es genau eine Determinantenform auf K^n.

Beweis:

1. Wir zeigen die Aussage für $n=3$. Der allgemeine Beweis folgt direkt. Sei $u,v,w \in K^n$ mit Basisdarstellung bzgl der kanonischen Basis $u=\sum_{i=1}^3 u_i e_i$, $v=\sum_{j=1}^3 v_j e_j$ und $w=\sum_{k=1}^3 w_k e_k$. Wegen der Multi-linearität von F folgt,

$$\begin{aligned} F(u,v,w) &= F\Big(\sum_{i=1}^3 u_i e_i, \sum_{j=1}^3 v_j e_j, \sum_{k=1}^3 w_k e_k\Big) \\ &= \sum_{i=1}^3 u_i\, F\Big(e_i, \sum_{j=1}^3 v_j e_j, \sum_{k=1}^3 w_k e_k\Big) \end{aligned}$$

$$= \sum_{i=1}^{3} \sum_{j=1}^{3} u_i \, v_j \; F\Big(e_i, e_j, \sum_{k=1}^{3} w_k e_k\Big)$$
$$= \sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} u_i \, v_j \, w_k \; F\Big(e_i, e_j, e_k\Big)$$

Nach Definition gilt $F(e_i, e_j, e_k) = 0$ wenn $i = j$ oder $i = k$ oder $j = k$ d.h. $F(e_i, e_j, e_k)$ kann nur dann ungleich null sein, wenn $i \neq j \neq k \neq i$ d.h. im Fall $n = 3$ wenn das Tripel (i, j, k) eine Permutation von $(1, 2, 3)$ ist. Nun gilt aber Vorzeichenwechsel bei Vertauschung von Argumenten, d.h.

$$F(e_1, e_2, e_3) = -F(e_1, e_3, e_2) = F(e_3, e_1, e_2) = -F(e_3, e_2, e_1)$$
$$= F(e_2, e_3, e_1) = -F(e_2, e_1, e_3)$$

Das bedeutet, daß die alternierende Multilinearform F vollständig durch den Wert $F(e_1, e_2, e_3)$ bestimmt ist. Insbesondere ist F genau dann null, wenn $F(e_1, e_2, e_3) = 0$ ist.

2. Folgt direkt aus dem ersten Teil. Denn sind F, G zwei alternierende Multlinearformen mit $F(e_1, e_2, e_3) = G(e_1, e_2, e_3)$, dann gilt für die Differenz $H = F - G$, $H(e_1, e_2, e_3) = 0$, und mit dem ersten Teil des Satzes folgt $H = 0$ und damit $F = G$. Daraus ergibt sich direkt die Eindeutigkeit der Determinantenform. Die Existenz einer Determinantenform ergibt sich über die obige multi-lineare Fortsetzung.

Bemerkung:

- Im obigen Beweis zeigen wir implizit, daß eine Multilinearform genauso wie eine lineare Abbildung vollständig über die Wirkung auf die Basisvektoren bestimmt ist, oder formal korrekt über die Wirkung auf alle n-Tupel von Basisvektoren.
- Die Eigenschaft "alternierend" ist eine starke Einschränkung einer Multilinearform F - der Wert $F(e_1, e_2, e_3)$ bestimmt die gesamte alternierende Multilinearform.

39.6 Definition

Seien $(a_1, \ldots, a_n)$ die Spaltenvektoren einer Matrix $A \in K^{n \times n}$ und sei det die Determinantenform. Die Determinante $\det A$ der Matrix A ist definiert als

$$\det A := \det(a_1, \ldots, a_n).$$

Bemerkung:

- Die Determinante einer Matrix A wird auch mit $|A|$ bezeichnet.
- Nach Definition gilt: $\det I = \det(e_1, \ldots, e_n) = 1$
- Die Determinate einer 2×2-Matrix A ist gegeben als

$$\det A = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

  Dies ergibt sich direkt aus den Eigenschaften der alternierenden Multilinearform und $\det I = 1$:

$$\begin{aligned} \det A = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= a \det \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} + c \det \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix} \\ &= ab \det \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + ad \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + cb \det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + cd \det \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= ad \det(e_1, e_2) + cb \det(e_2, e_1) = ad - bc \end{aligned}$$

- Die Determinante einer $n \times n$-Matrix kann man rekursiv auf 2×2-Matrizen zurückführen. Das ergibt sich aus dem Laplaceschen Entwicklungssatz. Die Determinante einer 1×1-Matrix $a \in K$ ist $\det a = a$.
- Die Determinante einer Matrix $A \in K^{n \times n}$ mit $\operatorname{rang} A < n$ ist null nach Satz 39.3.

39.7 Definition

Es sei $A = (a_{ij}) \in K^{n \times n}$. Die aus einer $n \times n$-Determinante $D = \det A$ durch Streichung der i-ten Zeile und j-ten Spalte entstehende $(n-1) \times (n-1)$-Determinante D_{ij} nennen wir **Unterdeterminante** von D. Der Ausdruck $A_{ij} := (-1)^{i+j} D_{ij}$ heißt **algebraisches Komplement** des Elements a_{ij} in der Determinante D.

39.8 Beispiel

$$A = \begin{pmatrix} 3 & 9 & 1 \\ 2 & 5 & \boxed{4} \\ -2 & 8 & 7 \end{pmatrix}, \qquad D_{23} = \begin{vmatrix} 3 & 9 \\ -2 & 8 \end{vmatrix} = 3 \cdot 8 - (-2) \cdot 9 = 42$$
$$A_{23} = (-1)^{2+3} \cdot D_{23} = -42 \, .$$

Damit können wir $n \times n$-Determinanten rekursiv berechnen.

39.9 Satz: Laplace'scher Entwicklungssatz

Der Wert einer $n \times n$-Determinante ergibt sich, indem die Elemente einer beliebigen Zeile (oder Spalte) mit ihren algebraischen Komplementen multipliziert und die so entstandenen Produkte addiert werden.

Die **Entwicklung nach der i-ten Zeile** lautet also

$$\det A = \sum_{j=1}^{n} a_{ij} A_{ij} \, .$$

Entwickelt man nach der j-ten Spalte, so erhält man

$$\det A = \sum_{i=1}^{n} a_{ij} A_{ij} \, .$$

39.10 Beispiel

a) Entwicklung einer 3×3-Determinante nach der 2. Zeile:

$$\begin{vmatrix} 3 & 9 & 1 \\ 2 & 5 & 4 \\ -2 & 8 & 7 \end{vmatrix} = -2 \cdot \begin{vmatrix} 9 & 1 \\ 8 & 7 \end{vmatrix} + 5 \cdot \begin{vmatrix} 3 & 1 \\ -2 & 7 \end{vmatrix} - 4 \cdot \begin{vmatrix} 3 & 9 \\ -2 & 8 \end{vmatrix}$$
$$= -2 \cdot (63 - 8) + 5 \cdot (21 + 2) - 4 \cdot (24 + 18)$$
$$= -2 \cdot 55 + 5 \cdot 23 - 4 \cdot 42 = -163 \, .$$

b) Entwicklung nach der 3. Spalte:

$$\begin{vmatrix} 3 & 9 & 1 \\ 2 & 5 & 4 \\ -2 & 8 & 7 \end{vmatrix} = 1 \cdot \begin{vmatrix} 2 & 5 \\ -2 & 8 \end{vmatrix} - 4 \cdot \begin{vmatrix} 3 & 9 \\ -2 & 8 \end{vmatrix} + 7 \cdot \begin{vmatrix} 3 & 9 \\ 2 & 5 \end{vmatrix}$$

$$= 1 \cdot (16 + 10) - 4 \cdot (24 + 18) + 7 \cdot (15 - 18)$$
$$= 1 \cdot 26 - 4 \cdot 42 + 7 \cdot (-3) = -163 \, .$$

Wie rechnet man mit Determinanten?

39.11 Rechenregeln für Determinanten

a) Transposition verändert den Wert einer Determinante nicht:

$$\det A^{\mathrm{T}} = \det A \, .$$

(Folgt aus dem Laplace'schen Entwicklungssatz, indem man die Entwicklung nach Zeilen und Spalten vertauscht.)

b) Aus Satz 39.3 folgt: Sind Spaltenvektoren oder Zeilenvektoren linear abhängig, so ist die Determinante 0:

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = 0 \, .$$

c) Addiert man zu einer Zeile/Spalte das Vielfache einer anderen Zeile/Spalte, so bleibt die Determinante gleich:

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \begin{matrix} \\ \circlearrowright -1\times \\ \\ \end{matrix} \begin{matrix} \\ \\ \circlearrowright -1\times \end{matrix} = \begin{vmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \\ 6 & 6 & 6 \end{vmatrix}$$

d) Vertauscht man zwei Zeilen/zwei Spalten, so ändert die Determinante ihr Vorzeichen:

$$\begin{vmatrix} 3 & 9 & 1 \\ -2 & 8 & 7 \\ 2 & 5 & 4 \end{vmatrix} = - \begin{vmatrix} 3 & 9 & 1 \\ 2 & 5 & 4 \\ -2 & 8 & 7 \end{vmatrix} \, .$$

e) Die Determinante einer Dreiecksmatrix ist das Produkt der Diagonalelemente:

$$\begin{vmatrix} 3 & 0 & 9 \\ 0 & -7 & 4 \\ 0 & 0 & 2 \end{vmatrix} = 3 \cdot (-7) \cdot 2 = -42 \, .$$

(Folgt durch rekursives Anwenden des Laplace'schen Entwicklungssatzes.)

Insbesondere kann man mit dem Gauß-Algorithmus die Matrix auf Dreiecksgestalt bringen (unter Beachtung von (d)) und kann dann ihre Determinante bequem berechnen. Für große n ist dies wesentlich effizienter als der Laplace'sche Entwicklungssatz.

f) Für $A, B \in K^{n\times n}$ gilt

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

g) *Folgerung:* Falls A invertierbar, so $1 = \det(I) = \det(A \cdot A^{-1}) = \det A \cdot \det(A^{-1})$, also

$$\det(A^{-1}) = \frac{1}{\det A} \ .$$

h) *Vorsicht:* Für $A \in K^{n\times n}$ und $\lambda \in K$ gilt

$$\det(\lambda A) = \lambda^n \det A$$

(und nicht etwa $\cdots = \lambda \det A$, denn det ist linear *in jeder Zeile*).

Wozu sind Determinanten nützlich?

39.12 Bedeutung der Determinanten

a) Mit Determinanten kann man prüfen, ob eine Matrix $A \in K^{n\times n}$ invertierbar ist:

$$A \in K^{n\times n} \text{ ist invertierbar} \quad \Leftrightarrow \quad \det A \neq 0$$

(vgl. Satz 39.3).

b) Man kann mit ihrer Hilfe lineare Gleichungssysteme lösen (für numerische Rechnungen ist dieses Verfahren allerdings zu ineffizient!):

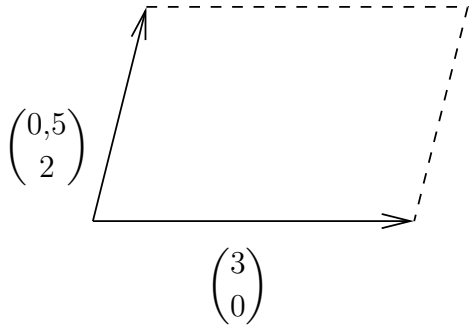
> **Cramersche Regel:** Ist $A = (a_{*1}, \ldots, a_{*n}) \in \mathrm{GL}(n, K)$ und $b \in K^n$, so lässt sich die Lösung des linearen Gleichungssystems $A\,x = b$ angeben durch
>
> $$x_k = \frac{\det(a_{*1}, \ldots, a_{*(k-1)}, \boldsymbol{b}, a_{*(k+1)}, \ldots, a_{*n})}{\det A}\,, \quad k = 1, \ldots, n\,.$$

Beispiel: Für das System $\begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -2 \\ 6 \end{pmatrix}$ erhält man

$$x_1 = \frac{\begin{vmatrix} -2 & 5 \\ 6 & 4 \end{vmatrix}}{\begin{vmatrix} 2 & 5 \\ 1 & 4 \end{vmatrix}} = \frac{-8-30}{8-5} = -\frac{38}{3}$$

$$x_2 = \frac{\begin{vmatrix} 2 & -2 \\ 1 & 6 \end{vmatrix}}{\begin{vmatrix} 2 & 5 \\ 1 & 4 \end{vmatrix}} = \frac{12+2}{3} = \frac{14}{3}\,.$$

c) $|\det A|$ ist das Volumen des durch die Spaltenvektoren von A aufgespannten Parallelepipeds:



$$\left|\det \begin{pmatrix}3 & 0{,}5\\0 & 2\end{pmatrix}\right| = |3 \cdot 2 - 0 \cdot 0{,}5| = |6| \quad \text{Parallelogrammfläche}$$

40 Euklidische Vektorräume, Skalarprodukt

40.1 Motivation

Im $\mathbb{R}^2$ und $\mathbb{R}^3$ kann das Skalarprodukt zweier Vektoren gebildet werden. Mit seiner Hilfe lassen sich Längen von Vektoren bestimmen sowie feststellen, ob Vektoren senkrecht (orthogonal) zueinander sind; allgemein können auch Winkel zwischen Vektoren berechnet werden.

Ziel: Wir wollen dieses Konzept auf andere Vektorräume über $\mathbb{R}$ ausdehnen und auch in diesen ein Skalarprodukt bereit stellen, Orthogonalität definieren, Längen und Winkel bestimmen.

40.2 Definition: euklidischer Raum

Es seien $u = (u_1, \ldots, u_n)^{\mathrm{T}}$ und $v = (v_1, \ldots, v_n)^{\mathrm{T}}$ Vektoren im $\mathbb{R}^n$.

Das **euklidische Produkt (euklidische Skalarprodukt)** $u \cdot v$ wird definiert durch

$$u \cdot v := \sum_{i=1}^{n} u_i v_i \ .$$

Den Vektorraum $\mathbb{R}^n$ versehen mit dem euklidischen Produkt bezeichnet man als ***n*-dimensionalen euklidischen Raum.**

40.3 Beispiel

Es sei $u = \begin{pmatrix} -1 \\ 3 \\ 5 \\ 7 \end{pmatrix}$, $v = \begin{pmatrix} 5 \\ -4 \\ 7 \\ 0 \end{pmatrix}$. Dann ist

$$u \cdot v = (-1) \cdot 5 + 3 \cdot (-4) + 5 \cdot 7 + 7 \cdot 0 = 18 \ .$$

40.4 Satz: Eigenschaften des euklidischen Produkts

Es seien $u, v, w \in \mathbb{R}^n$ und $\alpha \in \mathbb{R}$. Dann gilt:

a) $u \cdot v = v \cdot u$ **(Kommutativität)**

b) $(u + v) \cdot w = u \cdot w + v \cdot w$ **(Additivität** oder **Distributivität)**

c) $(\alpha u) \cdot v = \alpha(u \cdot v)$ **(Homogenität)**

d) $v \cdot v \geq 0$
$v \cdot v = 0$ genau dann, wenn $v = 0$ **(positive Definitheit)**.

Bemerkungen:

- Die Kommutativität des Skalarproduktes bezeichnet man auch als **Symmetrie.**
- Distributivität und Homogenität ergeben zusammen

$$(\alpha u + \beta v) \cdot w = \alpha(u \cdot w) + \beta(v \cdot w)$$

sowie mit der Symmetrie

$$u \cdot (\alpha v + \beta w) = \alpha(u \cdot v) + \beta(u \cdot w)$$

für alle $u, v, w \in \mathbb{R}^n$ und $\alpha, \beta \in \mathbb{R}$. Diese Eigenschaften fasst man unter dem Begriff **Bilinearität** zusammen.

Beweis: (a) und (c) folgen unmittelbar aus der Definition.

Zu (b): Es gilt

$$\begin{aligned}(u + v) \cdot w &= (u_1 + v_1, \ldots, u_n + v_n)^{\mathrm{T}} \cdot (w_1, \ldots, w_n)^{\mathrm{T}} \\ &= \sum_{i=1}^{n} (u_i + v_i) w_i \\ &= \sum_{i=1}^{n} u_i w_i + \sum_{i=1}^{n} v_i w_i \\ &= u \cdot w + v \cdot w \; .\end{aligned}$$

Zu (d): Es gilt $v \cdot v = v_1^2 + v_2^2 + \ldots + v_n^2 \geq 0$.

Gleichheit gilt genau dann, wenn $v_1 = v_2 = \ldots = v_n = 0$, d. h. wenn $v = 0$. □

Bemerkung: Ein Skalarprodukt ist eine symmetrische, positiv definite Bilinearform (eine Bilinearform ist eine Multilinearform mit zwei Argumenten). Wie im vorigen Kapitel gezeigt ist eine Multilinearform vollständig durch die Wirkung auf alle Tupel von Basisvektoren festgelegt. Sei $F : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ eine symmetrische Bilinearform d.h. $F(u, v) = F(v, u)$, $\forall u, v \in \mathbb{R}^n$, dann gilt für $u, v \in \mathbb{R}^n$,

$$F(u, v) = F\big(\sum_{i=1}^{n} u_i e_i, \sum_{j=1}^{n} v_j e_j\big) = \sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j F(e_i, e_j)$$

Die Bilinearform des euklidischen Skalarprodukts erhalten wir also durch die Wahl

$$F(e_i, e_j) = \begin{cases} 1, & \text{wenn } i = j, \\ 0, & \text{sonst.} \end{cases}$$

40.5 Definition: euklidische Norm

Es sei $u = (u_1, \ldots, u_n)^{\mathrm{T}} \in \mathbb{R}^n$ ein Vektor. Die **euklidische Norm** von u ist definiert durch

$$|u| := \sqrt{u \cdot u} = \sqrt{u_1^2 + \ldots + u_n^2}\,.$$

Der **euklidische Abstand** zweier Vektoren $u = (u_1, \ldots, u_n)^{\mathrm{T}}$ und $v = (v_1, \ldots, v_n)^{\mathrm{T}}$ ist definiert durch

$$d(u, v) := |u - v| = \sqrt{(u_1 - v_1)^2 + \ldots + (u_n - v_n)^2}\,.$$

Auch die Bezeichnung **euklidische Metrik** wird verwendet.

Bemerkung: Die euklidische Norm misst die *Länge* eines Vektors.

40.6 Beispiel

Für $u = \begin{pmatrix} 1 \\ 3 \\ -2 \\ 7 \end{pmatrix}$ und $v = \begin{pmatrix} 0 \\ 7 \\ 2 \\ 2 \end{pmatrix}$ ist

$$\begin{aligned} |u| &= \sqrt{1+9+4+49} = \sqrt{63} = 3\sqrt{7} \\ d(u,v) &= \sqrt{(1-0)^2+(3-7)^2+(-2-2)^2+(7-2)^2} \\ &= \sqrt{1+16+16+25} = \sqrt{58}\ . \end{aligned}$$

40.7 Satz: Cauchy-Schwarz'sche Ungleichung im $\mathbb{R}^n$

Für $u, v \in \mathbb{R}^n$ gilt stets

$$|u \cdot v| \leq |u| \cdot |v|\ .$$

Beweis: in der nächsten Vorlesung (in allgemeinerer Form)

40.8 Satz: Eigenschaften der euklidischen Norm

Es seien $u, v \in \mathbb{R}^n$ und $\alpha \in \mathbb{R}$. Dann gilt:

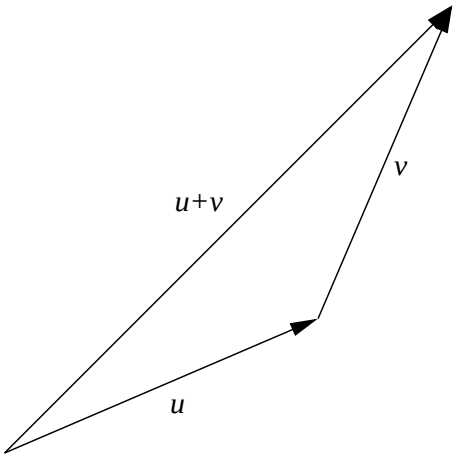
a) $|u| \geq 0$

b) $|u| = 0 \quad \Rightarrow \quad u = 0$

c) $|\alpha u| = |\alpha| \ \ |u|$

d) $|u+v| \leq |u| + |v|$ **(Dreiecksungleichung)**

Bedeutung der Dreiecksungleichung: Die Summe der Längen zweier Dreiecksseiten ist nie kleiner als die Länge der dritten Dreiecksseite.



Beweis: Die ersten beiden Eigenschaften ergeben sich direkt aus der Definition der euklidischen Norm und der positiven Definitheit des euklidischen Produktes.

Zu (c): Nach Definition der euklidischen Norm ist

$$\begin{aligned} |\alpha u| &= \sqrt{(\alpha u_1)^2 + \ldots + (\alpha u_n)^2} \\ &= \sqrt{\alpha^2 (u_1^2 + \ldots + u_n^2)} \\ &= \sqrt{\alpha^2}\ \sqrt{u_1^2 + \ldots + u_n^2} \\ &= |\alpha|\ \ |u| \end{aligned}$$

Zu (d): Es ist

$$\begin{aligned} |u+v|^2 &= (u+v)\cdot(u+v) && \text{(nach Def.)} \\ &= u^2 + u\cdot v + v\cdot u + v^2 && \text{(Distributivität)} \\ &= |u|^2 + 2u\cdot v + |v|^2 \\ &\leq |u|^2 + 2\,|u|\ \ |v| + |v|^2 && \text{(Cauchy-Schwarz)} \\ &= (|u| + |v|)^2\ . \end{aligned}$$

Wegen der Monotonie der Quadratwurzelfunktion (man beachte, dass beide Seiten der Ungleichung nichtnegativ sind) folgt

$$|u+v| \leq |u| + |v|\ .$$

□

40.9 Satz: Eigenschaften des euklidischen Abstandes

Es seien $u, v, w \in \mathbb{R}^n$. Dann gilt:

a) $d(u, v) \geq 0$

b) $d(u, v) = 0 \quad \Leftrightarrow \quad u = v$

c) $d(u, v) = d(v, u)$

d) $d(u, v) \leq d(u, w) + d(w, v)$

Beweis: Alle Eigenschaften ergeben sich als direkte Folgerungen aus Satz 40.8. □

40.10 Definition: Orthogonale Vektoren

Zwei Vektoren $u, v \in \mathbb{R}^n$ heißen **orthogonal,** falls $u \cdot v = 0$.

Beispiel: Es sei $u = \begin{pmatrix} -2 \\ 3 \\ 1 \\ 4 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}$. Dann gilt

$$u \cdot v = -2 + 6 + 0 - 4 = 0 \ ,$$

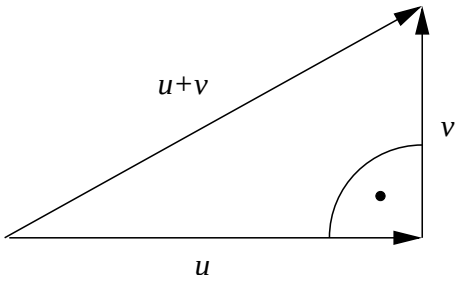
u und v sind also orthogonal.

Bemerkung: „orthogonal“ = „zueinander senkrecht“

40.11 Satz von Pythagoras im $\mathbb{R}^n$

Sind $u, v \in \mathbb{R}^n$ orthogonal, so gilt

$$|u + v|^2 = |u|^2 + |v|^2 \ .$$



Hypotenusenquadrat =
Summe der Kathetenquadrate

Beweis: Es gilt

$$|u + v|^2 = (u + v) \cdot (u + v) = |u|^2 + 2\underbrace{u \cdot v}_{\substack{=0 \\ \text{wegen Orthogonalität}}} + |v|^2$$

□

Beispiel: $u = \begin{pmatrix} -2 \\ 3 \\ 1 \\ 4 \end{pmatrix}$ und $v = \begin{pmatrix} 1 \\ 2 \\ 0 \\ -1 \end{pmatrix}$ sind orthogonal.

$$\begin{aligned} |u|^2 &= 4 + 9 + 1 + 16 = 30 \\ |v|^2 &= 1 + 4 + 0 + 1 = 6 \\ u + v &= (-1, 5, 1, 3)^{\mathrm{T}} \\ |u + v|^2 &= 1 + 25 + 1 + 9 = 36 \\ &= |u|^2 + |v|^2 \ . \end{aligned}$$

40.12 Interpretation des euklidischen Produktes als Matrixmultiplikation

Es seien $u, v \in \mathbb{R}^n$. Dann kann man das euklidische Produkt $u \cdot v$ als Multiplikation der $1 \times n$-Matrix u^{T} mit der $n \times 1$-Matrix v auffassen:

$$u \cdot v = u^{\mathrm{T}} v \ .$$

(Zur Erinnerung: Vektoren im $\mathbb{R}^n$ sind für uns stets Spaltenvektoren.)

Beispiel: Für $u = \begin{pmatrix} 1 \\ -3 \\ 7 \\ 4 \end{pmatrix}$, $v = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 9 \end{pmatrix}$ gilt

$$u^{\mathrm{T}} v = (1, -3, 7, 4) \begin{pmatrix} 0 \\ 2 \\ 1 \\ 9 \end{pmatrix} = 0 - 6 + 7 + 36 = 37 \ .$$

41 Funktionalanalytische Verallgemeinerungen

41.1 Motivation

- Die Begriffe des euklidischen Produktes, der Norm und des Abstandes sollen abstrahiert werden, um sie auch auf andere Räume übertragen zu können.
- Dies ist auch für Anwendungen wichtig: Zum Beispiel ist in Signal- und Bildverarbeitung die Fouriertransformation von großer Bedeutung. Sie beruht auf den in diesem Abschnitt besprochenen Konzepten.

41.2 Definition: inneres Produkt

Es sei V ein reeller Vektorraum. Eine Funktion

$$\langle \cdot\,, \cdot \rangle : V \times V \to \mathbb{R}$$

heißt **inneres Produkt (Skalarprodukt),** wenn für alle $u, v, w \in V$ und $\alpha \in \mathbb{R}$ gilt:

(a)	$\langle u, v\rangle = \langle v, u\rangle$	**(Symmetrie)**
(b)	$\langle u + v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$	**(Additivität)**
(c)	$\langle \alpha u, v\rangle = \alpha\langle u, v\rangle$	**(Homogenität)**
(d)	$\langle v, v\rangle \geq 0$	**(Nichtnegativität)**
	$\langle v, v\rangle = 0 \quad \Rightarrow \quad v = 0$	**(positive Definitheit)**

Ist dies der Fall, so heißt $(V, \langle \cdot\,, \cdot \rangle)$ **Skalarproduktraum** oder auch Prä-Hilbert-Raum.

Bemerkungen:

1. Wenn jede Cauchy-Folge aus Elementen von V (siehe MfI 1, 10.11) gegen ein Element von V konvergiert, so heißt der Raum V *vollständig.* Ein vollständiger Prä-Hilbert-Raum heißt **Hilbertraum.** Eine Folge x_n in einem metrischen Raum $(\mathcal{X}, d)$ heißt Cauchy-Folge wenn für alle $\epsilon > 0$ $\exists N \in \mathbb{N}$, so daß für alle $n, m \geq N$ gilt $d(x_n, d_m) < \epsilon$. Wie für den euklidischen Raum induziert auch ein allgemeines Skalarprodukt eine Metrik d auf V.
2. Jeder endlichdimensionale Skalarproduktraum ist vollständig und daher ein Hilbertraum.

3. Der Anlass für unsere Beschränkung auf reelle Vektorräume liegt in dem Gebrauch der Ordnungsrelation $\geq$ für die Definition der Nichtnegativität. Eine solche Ordnungsrelation existiert nicht für endliche Körper oder die komplexen Zahlen. Trotzdem ist es möglich auch über dem Körper der komplexen Zahlen ein Skalarprodukt zu definieren indem per Konstruktion gilt, $\langle v, v\rangle \in \mathbb{R}$, $\forall v \in \mathbb{C}^n$.

4. Wie im euklidischen Raum ist das Skalarprodukt über $\mathbb{R}$ eine symmetrische, positiv definite Bilinearform. Ein Skalarprodukt über $\mathbb{C}$ erfüllt statt der Symmetrie die Eigenschaft,

$$\langle u, v\rangle = \overline{\langle v, u\rangle}, \quad \text{(hermitesch)}.$$

und ist linear im ersten Argument und anti-linear im zweiten Argument, d.h. $\langle u, \lambda\, v\rangle = \overline{\lambda}\, \langle u, v\rangle$, $\forall u, v \in \mathbb{C}^n$, $\lambda \in \mathbb{C}$ (es wird auch mit der umgekehrten Definition gearbeitet). Die Eigenschaft der Nichtnegativität und der positiven Definitheit sind wie über $\mathbb{R}$. Eine solche Funktion $\mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ wird hermitesche, positiv definite Sesquilinearform genannt.

41.3 Beispiele

a) **Euklidische Räume**

Der n-dimensionale euklidische Raum ist ein Skalarproduktraum. Nach Satz 40.4 sind alle Eigenschaften von Definition 41.2 erfüllt.

b) **Gewichtete euklidische Räume**

Für Vektoren $u = (u_1, u_2)^{\mathrm{T}}$ und $v = (v_1, v_2)^{\mathrm{T}}$ in $\mathbb{R}^2$ wird durch

$$\langle u, v\rangle := 3u_1v_1 + 5u_2v_2$$

ein Skalarprodukt definiert.

Beweis: *Symmetrie:* Für alle $u, v \in \mathbb{R}^2$ gilt

$$\langle u, v\rangle = 3u_1v_1 + 5u_2v_2 = \langle v, u\rangle\ .$$

Additivität: Für alle $u, v, w \in \mathbb{R}^2$ gilt

$$\begin{aligned}\langle u + v, w\rangle &= 3(u_1 + v_1)w_1 + 5(u_2 + v_2)w_2\\ &= (3u_1w_1 + 5u_2w_2) + (3v_1w_1 + 5v_2w_2)\\ &= \langle u, w\rangle + \langle v, w\rangle\ .\end{aligned}$$

Homogenität: Für $u, v \in \mathbb{R}^2$, $\alpha \in \mathbb{R}$ gilt

$$\langle \alpha u, v \rangle = 3\alpha u_1 v_1 + 5\alpha u_2 v_2 = \alpha \langle u, v \rangle \ .$$

Nichtnegativität: Für alle $v \in \mathbb{R}^2$ ist

$$\langle v, v \rangle = 3 \underbrace{v_1^2}_{\geq 0} + 5 \underbrace{v_2^2}_{\geq 0} \geq 0 \ .$$

Dabei gilt $\langle v, v \rangle = 0$ genau dann, wenn $v_1 = v_2 = 0$ *(Nichtdegeneriertheit).* □

c) **Polynomräume**

Für beliebige Polynome

$$p := \sum_{k=0}^{n} a_k x^k \ , \qquad\qquad q := \sum_{k=0}^{n} b_k x^k$$

vom Grad $\leq n$ definieren wir

$$\langle p, q \rangle := \sum_{k=0}^{n} a_k b_k \ .$$

Mit diesem Skalarprodukt wird der reelle Vektorraum der Polynome vom Grad kleiner oder gleich n zu einem Skalarproduktraum.

d) **Funktionenraum $C[a, b]$**

Es sei $C[a, b]$ der Vektorraum der auf $[a, b]$ stetigen Funktionen $f : [a, b] \to \mathbb{R}$. Für alle $f, g \in C[a, b]$ wird mittels

$$\langle f, g \rangle := \int_a^b f(x) g(x) \, \mathrm{d}x$$

ein Skalarprodukt definiert, mit dem $C[a, b]$ zum Skalarproduktraum wird.

Lässt sich auch die euklidische Norm verallgemeinern?

41.4 Definition: Norm

Es sei V ein reeller Vektorraum.

Eine Abbildung $\|\cdot\| : V \to \mathbb{R}$ heißt **Norm** auf V, wenn für alle $u, v \in V$, $\alpha \in \mathbb{R}$ gilt

a) $\|v\| \geq 0$

b) $\|v\| = 0 \quad \Rightarrow \quad v = 0$

c) $\|\alpha v\| = |\alpha| \, \|v\|$

d) $\|u + v\| \leq \|u\| + \|v\|$ **(Dreiecksungleichung).**

In diesem Fall heißt $(V, \|\cdot\|)$ **normierter Raum.**

Bemerkung: Ein vollständiger normierter Raum heißt **Banachraum** (vgl. Bemerkung zu Def. 41.2 zum Begriff Vollständigkeit).

41.5 Satz: Cauchy-Schwarz'sche Ungleichung in Skalarprodukträumen

Es sei $(V, \langle\cdot\,,\cdot\rangle)$ ein Skalarproduktraum. Dann gilt

$$\langle u, v\rangle^2 \leq \langle u, u\rangle \cdot \langle v, v\rangle$$

für beliebige $u, v \in V$.

Beweis: Falls $u = 0$ ist, so sind beide Seiten gleich 0, und die Ungleichung gilt.

Es sei also $u \neq 0$. Dann gilt für alle $x \in \mathbb{R}$ und $v \in V$

$$\begin{aligned} 0 &\leq \langle ux + v, ux + v\rangle \\ &= \langle ux, ux\rangle + \langle ux, v\rangle + \langle v, ux\rangle + \langle v, v\rangle \\ &= \underbrace{\langle u, u\rangle}_{=:a} x^2 + \underbrace{2\langle u, v\rangle}_{=:b} x + \underbrace{\langle v, v\rangle}_{=:c} . \end{aligned}$$

Die Parabel $ax^2 + bx + c$ besitzt also höchstens eine reelle Nullstelle. Für ihre Diskriminante gilt daher

$$0 \geq b^2 - 4ac = 4\langle u, v\rangle^2 - 4\langle u, u\rangle\langle v, v\rangle \ .$$

Daraus folgt die Behauptung. □

41.6 Satz: Induzierte Norm von Skalarprodukträumen

Jeder Skalarproduktraum $(V, \langle \cdot\,, \cdot \rangle)$ wird mit

$$\|v\| := \sqrt{\langle v, v\rangle}$$

zum normierten Raum.

Beweis: Die Eigenschaften (a), (b) folgen unmittelbar aus Def. 41.2(d).

Zu (c): Es gilt

$$\begin{aligned}
\|\alpha v\| &= \sqrt{\langle \alpha v, \alpha v\rangle} && \text{(nach Def.)} \\
&= \sqrt{\alpha\langle v, \alpha v\rangle} && \text{(Homogenität)} \\
&= \sqrt{\alpha\langle \alpha v, v\rangle} && \text{(Symmetrie)} \\
&= \sqrt{\alpha^2\langle v, v\rangle} && \text{(Homogenität)} \\
&= |\alpha|\ \|v\| && \text{(Def.)}
\end{aligned}$$

Zu (d): Es ist

$$\begin{aligned}
\|u + v\|^2 &= \langle u + v, u + v\rangle && \text{(Def.)} \\
&= \langle u, u\rangle + \langle u, v\rangle \\
&\quad + \langle v, u\rangle + \langle v, v\rangle && \text{(Additivität, Symmetrie)} \\
&= \|u\|^2 + 2\langle u, v\rangle + \|v\|^2 && \text{(Symmetrie, Def.)} \\
&\leq \|u\|^2 + 2\,\|u\|\ \|v\| + \|v\|^2 && \text{(Cauchy-Schwarz)} \\
&= (\|u\| + \|v\|)^2 \ .
\end{aligned}$$

□

41.7 Beispiele

a) **Norm einer stetigen Funktion**

$C[a,b]$ wird mit

$$\|f\| := \left(\int_a^b (f(x))^2 \, \mathrm{d}x \right)^{1/2} \qquad \text{für alle } f \in C[a,b]$$

zum normierten Raum.

Beispielsweise hat $f(x) = 1/x$ im Intervall $[1,2]$ die Norm

$$\|f\| = \sqrt{\int_1^2 \frac{1}{x^2} \, \mathrm{d}x} = \sqrt{\left[-\frac{1}{x} \right]_1^2} = \sqrt{-\frac{1}{2} + 1} = \sqrt{\frac{1}{2}} = \frac{\sqrt{2}}{2} \, .$$

b) **Gewichtete euklidische Norm**

Der Raum $\mathbb{R}^2$ mit dem Skalarprodukt, das durch

$$\langle u, v \rangle := \frac{1}{9} u_1 v_1 + \frac{1}{4} u_2 v_2$$

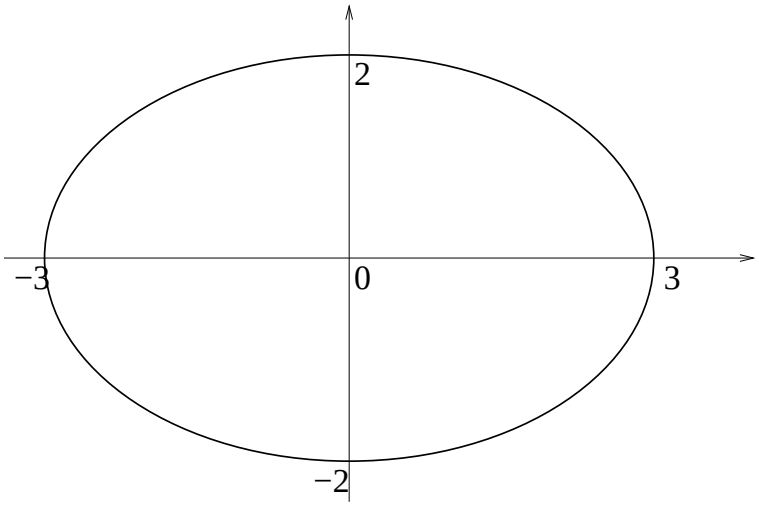
für alle $u = (u_1, u_2)^{\mathrm{T}}, v = (v_1, v_2)^{\mathrm{T}} \in \mathbb{R}^2$ definiert ist, hat die induzierte Norm

$$\|u\| := \sqrt{\frac{u_1^2}{9} + \frac{u_2^2}{4}} \, .$$

Der Einheitskreis bezüglich dieser Norm (das heißt die Menge aller $u \in \mathbb{R}^2$ mit $\|u\| = 1$) ist gegeben durch

$$\frac{u_1^2}{9} + \frac{u_2^2}{4} = 1 \, .$$

Dies ist eine Ellipsengleichung vom Typ $\dfrac{u_1^2}{a^2} + \dfrac{u_2^2}{b^2} = 1$ mit den Halbachsen $a = 3$ und $b = 2$:



Einheitskreise in solchen Normen sind also nicht immer „rund“.

c) l_p-Norm auf $\mathbb{R}^n$. Sei $u = (u_1, \ldots, u_n)^T \in \mathbb{R}^n$. Dann wird für $p \geq 1$ durch

$$\|u\|_p := \Big(\sum_{i=1}^{n} |u_i|^p \Big)^{\frac{1}{p}},$$

eine Norm definiert. Insbesondere gilt $\|u\|_\infty = \max_{i=1,\ldots,n} |u_i|$. Beweis: Übungsaufgabe.

Kann man auch den Begriff des euklidischen Abstands verallgemeinern?

41.8 Definition: Metrik

Es sei V ein Vektorraum über $\mathbb{R}$. Eine Abbildung $d : V \times V \to \mathbb{R}$ heißt **Metrik,** falls für alle $u, v, w \in V$ die folgenden Bedingungen erfüllt sind:

a) $d(u, v) \geq 0$

b) $d(u, v) = 0 \quad \Leftrightarrow \quad u = v$

c) $d(u, v) = d(v, u)$

d) $d(u, v) \leq d(u, w) + d(w, v)$

In diesem Falle heißt (V, d) **metrischer Raum.**

Bemerkung:

- Die obige Einschränkung auf Vektorräume ist nicht erforderlich, da für keine der Eigenschaften der Metrik d die Vektorraumstruktur verwendet wird. Jede Menge $\mathcal{X}$ mit einer Funktion $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ mit den obigen Eigenschaften heißt daher metrischer Raum $(\mathcal{X}, d)$.
- Für vollständige metrische Räume gibt es keinen speziellen Namen.

41.9 Satz: Induzierte Metrik eines normierten Raumes

Jeder normierte Raum $(V, \|\cdot\|)$ ist mit der Metrik

$$d(u, v) := \|u - v\| \quad \text{für alle } u, v \in V$$

ein metrischer Raum.

Beweis: Folgt direkt durch Vergleich der Definitionen 41.4 und 41.8. □

41.10 Beispiel: Metrik auf $C[a, b]$

Für $f, g \in C[a, b]$ wird durch

$$d(f, g) := \left(\int_a^b (f(x) - g(x))^2 \, \mathrm{d}x \right)^{1/2}$$

eine Metrik erklärt.

Beispielsweise haben $f(x) = 5x$ und $g(x) = 2x - 1$ in der so definierten Metrik über dem Intervall $[0, 1]$ den Abstand

$$\begin{aligned} d(f, g) &= \left(\int_0^1 (3x + 1)^2 \, \mathrm{d}x \right)^{1/2} \\ &= \left(\int_0^1 (9x^2 + 6x + 1) \, \mathrm{d}x \right)^{1/2} \end{aligned}$$

$$= \left(\left[3x^3 + 3x^2 + x \right]_0^1 \right)^{1/2}$$
$$= \sqrt{7} \, .$$

42 Orthogonalität

42.1 Motivation

Im euklidischen Raum ist das euklidische Produkt zweier Vektoren $u, v \in \mathbb{R}^n$ gleich 0, wenn die Vektoren orthogonal zueinander sind. Für beliebige Vektoren lässt sich sogar der Winkel zwischen ihnen mittels des euklidischen Produktes bestimmen.

Wir wollen die Begriffe der Orthogonalität und des Winkels in allgemeinen Prä-Hilbert-Räumen formulieren.

Dies führt zu Darstellungen in Orthogonalbasen, die wichtige Anwendungen in der Informatik haben, z. B. in der geometrischen Datenverarbeitung, in der Bildverarbeitung und im Information Retrieval.

42.2 Definition: Orthogonalität

Es sei $(V, \langle \cdot\,, \cdot \rangle)$ ein Prä-Hilbert-Raum über $\mathbb{R}$. Wir nennen zwei Vektoren $u, v \in V$ orthogonal genau dann, wenn $\langle u, v \rangle = 0$ gilt.

42.3 Beispiel

Wir betrachten $C[-1, 1]$ mit dem Skalarprodukt

$$\langle u, v \rangle := \int_{-1}^{1} u(x)v(x)\,\mathrm{d}x \ .$$

Für $u(x) := x$ und $v(x) := x^2$ erhalten wir

$$\langle u, v \rangle = \int_{-1}^{1} x^3\,\mathrm{d}x = \left[\frac{1}{4}x^4\right]_{-1}^{1} = \frac{1}{4} - \frac{1}{4} = 0 \ .$$

Die Funktionen $u(x) = x$ und $v(x) = x^2$ sind also orthogonal in $C[-1, 1]$.

Satz 40.11 kann unmittelbar auf Skalarprodukträume verallgemeinert werden.

42.4 Satz des Pythagoras in Skalarprodukträumen

Es sei $(V, \langle \cdot, \cdot \rangle)$ ein Skalarproduktraum über $\mathbb{R}$ mit der induzierten Norm $\| \cdot \|$. Sind $u, v \in V$ orthogonale Vektoren, so gilt

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2 \ .$$

Beweis: Es gilt

$$\|u + v\|^2 = \langle u + v, u + v \rangle = \langle u, u \rangle + 2 \underbrace{\langle u, v \rangle}_{=0} + \langle v, v \rangle = \|u\|^2 + \|v\|^2 \ .$$

□

42.5 Beispiel

Nach Beispiel 42.3 sind $u(x) = x$ und $v(x) = x^2$ in $C[-1, 1]$ orthogonal. Wir berechnen

$$\begin{aligned}
\|u + v\|^2 &= \int_{-1}^{1} (x + x^2)^2 \, \mathrm{d}x = \int_{-1}^{1} (x^2 + 2x^3 + x^4) \, \mathrm{d}x \\
&= \left[\frac{1}{3}x^3 + \frac{1}{2}x^4 + \frac{1}{5}x^5 \right]_{-1}^{1} \\
&= \left(\frac{1}{3} + \frac{1}{2} + \frac{1}{5} \right) - \left(-\frac{1}{3} + \frac{1}{2} - \frac{1}{5} \right) = \frac{2}{3} + \frac{2}{5} = \frac{16}{5} \\
\|u\|^2 &= \int_{-1}^{1} x^2 \, \mathrm{d}x = \left[\frac{1}{3}x^3 \right]_{-1}^{1} = \frac{2}{3} \\
\|v\|^2 &= \int_{-1}^{1} x^4 \, \mathrm{d}x = \left[\frac{1}{5}x^5 \right]_{-1}^{1} = \frac{2}{5} \ .
\end{aligned}$$

Wie erwartet gilt also $\|u + v\|^2 = \|u\|^2 + \|v\|^2$.

42.6 Satz und Definition: Winkel zwischen Vektoren

Es sei $(V, \langle \cdot\,, \cdot \rangle)$ ein Skalarproduktraum über $\mathbb{R}$ mit der induzierten Norm $\| \cdot \|$. Für zwei Vektoren $u, v \in V \setminus \{0\}$ gibt es dann stets eine eindeutig bestimmte Zahl $\vartheta \in [0, \pi]$ mit

$$\cos \vartheta = \frac{\langle u, v \rangle}{\|u\| \, \|v\|} \, .$$

Wir bezeichnen ϑ als den **Winkel** zwischen u und v.

Beweis zum Satz:

1. Nach der Cauchy-Schwarz'schen Ungleichung (Satz 41.5) ist stets

$$\left| \frac{\langle u, v \rangle}{\|u\| \, \|v\|} \right| \leq 1 \, ,$$

   der Quotient liegt also tatsächlich im Wertebereich der Kosinusfunktion.

2. Die Kosinusfunktion eingeschränkt auf das Intervall $[0, \pi]$ ist eine bijektive Abbildung von $[0, \pi]$ auf $[-1, 1]$. Das sichert die Eindeutigkeit von ϑ im angegebenen Intervall. □

Bemerkung: Für orthogonale Vektoren $u, v \in V \setminus \{0\}$ findet man $\cos \vartheta = 0$, also $\vartheta = \frac{\pi}{2}$ ($\widehat{=}\, 90°$).

42.7 Beispiele

a) **Euklidischer Raum $\mathbb{R}^4$:**
Für die Vektoren $u = (4, 3, 1, -2)^{\mathrm{T}}$ und $v = (-2, 1, 2, 3)^{\mathrm{T}}$ findet man

$$\begin{aligned} \langle u, v \rangle &= -8 + 3 + 2 - 6 = -9 \\ |u| &= \sqrt{16 + 9 + 1 + 4} = \sqrt{30} \\ |v| &= \sqrt{4 + 1 + 4 + 9} = \sqrt{18} \\ \Rightarrow \quad \cos \vartheta &= \frac{u \cdot v}{|u| \, |v|} = \frac{-9}{\sqrt{30}\sqrt{18}} \approx -0{,}3873 \\ \Rightarrow \quad \vartheta &\approx 1{,}968 \quad (\widehat{=}\, 112{,}8°) \, . \end{aligned}$$

b) **Funktionenraum $C[-1,1]$** mit Skalarprodukt wie in 42.3:
Für die Funktionen $u(x) = x$ und $v(x) = x^3$ findet man

$$\langle u, v\rangle = \int_{-1}^{1} x^4 \,\mathrm{d}x = \left[\frac{1}{5}x^5\right]_{-1}^{1} = \frac{2}{5}$$

$$\|u\| = \sqrt{\int_{-1}^{1} x^2 \,\mathrm{d}x} = \sqrt{\left[\frac{1}{3}x^3\right]_{-1}^{1}} = \sqrt{\frac{2}{3}}$$

$$\|v\| = \sqrt{\int_{-1}^{1} x^6 \,\mathrm{d}x} = \sqrt{\left[\frac{1}{7}x^7\right]_{-1}^{1}} = \sqrt{\frac{2}{7}}$$

$$\Rightarrow \quad \cos\vartheta = \frac{2/5}{\sqrt{2/3}\sqrt{2/7}} = \frac{\sqrt{21}}{5} \approx 0{,}9165$$

$$\Rightarrow \quad \vartheta \approx 0{,}4115 \quad (\widehat{=}\, 23{,}6^\circ)\,.$$

Oftmals ist es in Skalarprodukträumen sinnvoll, Basen zu wählen, deren Elemente paarweise orthogonal sind. Dies ergibt sich vor allem aus der Einfachheit der Koeffizientenbestimmung im Gegensatz zu einer allgemeinen Basis.

Beispielsweise besteht im euklidischen Raum $\mathbb{R}^3$ die Standardbasis

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

aus drei paarweise orthogonalen Vektoren, die außerdem sämtlich die Norm 1 haben.

42.8 Definition: Orthogonalbasis

In einem Skalarproduktraum heißt eine Menge von Vektoren **orthogonale Menge**, wenn ihre Elemente paarweise orthogonal sind. Haben die Elemente einer orthogonalen Menge außerdem die (induzierte) Norm 1, so spricht man von einer **orthonormalen Menge.**

Ist eine Basis eines Skalarproduktraumes eine orthogonale [orthonormale] Menge, so heißt sie **Orthogonalbasis (OB) [Orthonormalbasis (ONB)].**

42.9 Beispiel

Die Vektoren $u_1 := (0,1,0)^{\mathrm{T}}$, $u_2 := (1,0,1)^{\mathrm{T}}$, $u_3 := (1,0,-1)^{\mathrm{T}}$ bilden eine orthogonale Menge im euklidischen Raum $\mathbb{R}^3$, denn es gilt $u_1 \cdot u_2 = u_1 \cdot u_3 = u_2 \cdot u_3 = 0$.

Sie bilden jedoch keine orthonormale Menge: Zwar ist $|u_1| = 1$, aber $|u_2| = |u_3| = \sqrt{2}$.

Um eine orthonormale Menge $\{v_1, v_2, v_3\}$ zu erhalten, muss man durch die euklidischen Normen dividieren:

$$v_1 := \frac{u_1}{|u_1|} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \ , \qquad v_2 := \frac{u_2}{|u_2|} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \end{pmatrix} \ , \qquad v_3 := \frac{u_2}{|u_2|} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ -1/\sqrt{2} \end{pmatrix}$$

42.10 Satz: Koordinatendarstellung in einer Orthonormalbasis

Es sei $S := \{v_1, \ldots, v_n\}$ eine Orthonormalbasis eines endlichdimensionalen Skalarproduktraums $(V, \langle \cdot\,, \cdot \rangle)$ über $\mathbb{R}$. Dann gilt für jeden Vektor $u \in V$

$$u = \langle u, v_1 \rangle \, v_1 + \ldots + \langle u, v_n \rangle \, v_n \ .$$

Beweis: Da S Basis ist, gibt es $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ mit $u = \sum_{i=1}^{n} \alpha_i v_i$. Daraus folgt für jedes $k = 1, \ldots, n$

$$\langle u, v_k \rangle = \left\langle \sum_{i=1}^{n} \alpha_i v_i, v_k \right\rangle = \sum_{i=1}^{n} \alpha_i \, \langle v_i, v_k \rangle \ .$$

Wegen $\langle v_i, v_k \rangle = \begin{cases} 0 & \text{falls } i \neq k \\ 1 & \text{falls } i = k \end{cases}$ folgt daraus

$$\langle u, v_k \rangle = \alpha_k \quad \text{für } k = 1, \ldots, n.$$

□

42.11 Beispiel

Die Vektoren $v_1 := (0,1,0)^{\mathrm{T}}$, $v_2 = (-\frac{4}{5},0,\frac{3}{5})^{\mathrm{T}}$, $v_3 = (\frac{3}{5},0,-\frac{4}{5})^{\mathrm{T}}$ bilden eine Orthonormalbasis des euklidischen Raumes $\mathbb{R}^3$.

Um $u = (1,2,7)^{\mathrm{T}}$ als Linearkombination von v_1, v_2, v_3 zu schreiben, berechnet man

$$\begin{aligned} u \cdot v_1 &= 2 \\ u \cdot v_2 &= -\frac{4}{5} + 7 \cdot \frac{3}{5} = \frac{17}{5} \\ u \cdot v_3 &= \frac{3}{5} + 7 \cdot \frac{4}{5} = \frac{31}{5} \end{aligned}$$

und erhält damit

$$\begin{pmatrix} 1 \\ 2 \\ 7 \end{pmatrix} = 2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \frac{17}{5} \begin{pmatrix} -\frac{4}{5} \\ 0 \\ \frac{3}{5} \end{pmatrix} + \frac{31}{5} \begin{pmatrix} \frac{3}{5} \\ 0 \\ \frac{4}{5} \end{pmatrix} .$$

42.12 Satz: Koordinatendarstellung in einer Orthogonalbasis

Es sei $S := \{v_1, \ldots, v_n\}$ eine Orthogonalbasis eines endlichdimensionalen Skalarproduktraumes $(V, \langle \cdot, \cdot \rangle)$ über $\mathbb{R}$. Dann gilt für jeden Vektor $u \in V$

$$u = \frac{\langle u, v_1 \rangle}{\|v_1\|^2} v_1 + \ldots + \frac{\langle u, v_n \rangle}{\|v_n\|^2} v_n \, .$$

Beweis: Aus der Orthogonalbasis S erhält man durch Normierung (d. h. indem alle Basisvektoren durch ihre jeweiligen Normen dividiert werden) die Orthonormalbasis

$$S' = \left\{ \frac{v_1}{\|v_1\|}, \ldots, \frac{v_n}{\|v_n\|} \right\} .$$

Nach Satz 42.10 gilt dann

$$\begin{aligned} u &= \left\langle u, \frac{v_1}{\|v_1\|} \right\rangle \frac{v_1}{\|v_1\|} + \ldots + \left\langle u, \frac{v_n}{\|v_n\|} \right\rangle \frac{v_n}{\|v_n\|} \\ &= \frac{\langle u, v_1 \rangle}{\|v_1\|^2} v_1 + \ldots + \frac{\langle u, v_n \rangle}{\|v_n\|^2} v_n \, . \end{aligned}$$

□

Bemerkung: Unter Zusatzvoraussetzungen gelten ähnliche Aussagen auch in unendlichdimensionalen Skalarprodukträumen.

Um die Basiseigenschaft einer Menge von Vektoren in einem Skalarproduktraum nachzuweisen, muss unter anderem ihre lineare Unabhängigkeit untersucht werden. Beim Nachweis der Eigenschaft als Orthogonal- oder Orthonormalbasis vereinfacht sich dieser Schritt durch den folgenden Satz.

42.13 Satz: Lineare Unabhängigkeit orthogonaler Mengen

Eine orthogonale Menge $S := \{v_1, \ldots, v_n\}$ aus von 0 verschiedenen Elementen eines Skalarproduktraumes ist linear unabhängig.

Beweis: Zum Nachweis der linearen Unabhängigkeit müssen wir zeigen, dass aus $\sum_{i=1}^{n} \alpha_i v_i = 0$ stets $\alpha_i = 0$ für $i = 1, \ldots, n$ folgt.

Wir nehmen also an, dass $\sum_{i=1}^{n} \alpha_i v_i = 0$ gilt. Dann ergibt sich für jedes v_k, $k = 1, \ldots, n$

$$0 = \left\langle \sum_{i=1}^{n} \alpha_i v_i, v_k \right\rangle = \sum_{i=1}^{n} \alpha_i \langle v_i, v_k \rangle = \alpha_k \|v_k\|^2 \ ,$$

da $\langle v_i, v_k \rangle = 0$ für $i \neq k$ gilt. Wegen $v_k \neq 0$ und daher $\|v_k\| \neq 0$ folgt $\alpha_k = 0$ für jedes k. □

42.14 Beispiele

a) Aus Beispiel 42.9 wissen wir, dass

$$\left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \end{pmatrix}, \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ -1/\sqrt{2} \end{pmatrix} \right\}$$

eine orthonormale Menge im euklidischen Raum $\mathbb{R}^3$ ist. Nach Satz 42.13 ist sie linear unabhängig. Da die Menge aus drei Vektoren besteht und $\mathbb{R}^3$ die Dimension 3 besitzt, liegt eine Orthonormalbasis vor.

b) Im Raum $C[-1,1]$ aus Beispiel 42.3 (mit dem dort angegebenen Skalarprodukt) betrachten wir den Unterraum aller quadratischen Polynome

$$\{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\} .$$

Die Polynome

$$p_1 := 1 , \qquad p_2 := x , \qquad p_3 := x^2 - \frac{1}{3}$$

bilden darin eine Orthogonalbasis: Zunächst gilt

$$\begin{aligned}
\langle p_1, p_2 \rangle &= \int_{-1}^{1} x \, \mathrm{d}x = \left[\frac{1}{2} x^2 \right]_{-1}^{1} = 0 \\
\langle p_1, p_3 \rangle &= \int_{-1}^{1} \left(x^2 - \frac{1}{3} \right) \mathrm{d}x = \left[\frac{1}{3} x^3 - \frac{1}{3} x \right]_{-1}^{1} = 0 - 0 = 0 \\
\langle p_2, p_3 \rangle &= \underbrace{\langle x, x^2 \rangle}_{=0 \ (42.3)} - \frac{1}{3} \underbrace{\langle x, 1 \rangle}_{= \langle p_2, p_1 \rangle = 0} = 0 ,
\end{aligned}$$

die drei Funktionen sind also paarweise orthogonal. Nach Satz 42.13 sind sie linear unabhängig, und da der Raum der quadratischen Polynome die Dimension 3 besitzt, wird er von $\{p_1, p_2, p_3\}$ auch erzeugt.

Um Satz 42.12 anwenden zu können, berechnen wir noch

$$\begin{aligned}
\|p_1\|^2 = \langle p_1, p_1 \rangle &= \int_{-1}^{1} 1 \, \mathrm{d}x = 2 \\
\|p_2\|^2 = \langle p_2, p_2 \rangle &= \int_{-1}^{1} x^2 \, \mathrm{d}x = \left[\frac{1}{3} x^3 \right]_{-1}^{1} = \frac{2}{3} \\
\|p_3\|^2 = \langle p_3, p_3 \rangle &= \int_{-1}^{1} \left(x^4 - \frac{2}{3} x^2 + \frac{1}{9} \right) \mathrm{d}x = \left[\frac{1}{5} x^5 - \frac{2}{9} x^3 + \frac{1}{9} x \right]_{-1}^{1} = \frac{8}{45} .
\end{aligned}$$

Ist nun beispielsweise $q = x^2 + 2x + 1$ gegeben, so berechnen wir

$$\langle q, p_1 \rangle = \int_{-1}^{1} (x^2 + 2x + 1) \, \mathrm{d}x = \left[\frac{1}{3} x^3 + x^2 + x \right]_{-1}^{1} = \frac{8}{3}$$

$$\langle q, p_2 \rangle = \int_{-1}^{1} (x^3 + 2x^2 + x)\,\mathrm{d}x = \left[\frac{1}{4}x^4 + \frac{2}{3}x^3 + \frac{1}{2}x^2\right]_{-1}^{1} = \frac{4}{3}$$

$$\begin{aligned}\langle q, p_3 \rangle &= \int_{-1}^{1} \left(x^4 + 2x^3 + \frac{2}{3}x^2 - \frac{2}{3}x - \frac{1}{3}\right)\,\mathrm{d}x \\ &= \left[\frac{1}{5}x^5 + \frac{1}{2}x^4 + \frac{2}{9}x^3 - \frac{1}{3}x^2 - \frac{1}{3}x\right]_{-1}^{1} = \frac{8}{45}\ .\end{aligned}$$

Einsetzen in die Gleichung aus Satz 42.12 ergibt die Darstellung

$$\begin{aligned}q &= \frac{8/3}{2}p_1 + \frac{4/3}{2/3}p_2 + \frac{8/45}{8/45}p_3 \\ &= \frac{4}{3}p_1 + 2p_2 + p_3\ .\end{aligned}$$

Die orthogonale Projektion auf einen Unterraum ist eine eminent wichtige Operation in Skalarprodutkräumen.

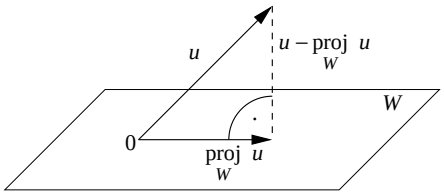
42.15 Satz: Orthogonale Projektion auf Unterräume

Es sei $(V, \langle \cdot\,, \cdot \rangle)$ ein Skalarproduktraum. Weiter sei $u \in V$, und W sei ein endlichdimensionaler Unterraum von V mit der Orthogonalbasis $(v_1, \ldots, v_n)$.

Dann beschreibt

$$\operatorname*{proj}_W u := \sum_{i=1}^{n} \frac{\langle u, v_i \rangle}{\|v_i\|^2} v_i$$

eine **orthogonale Projektion** von u auf W, d. h. es gilt $\operatorname*{proj}_W u \in W$ und $\left\langle u - \operatorname*{proj}_W u, w \right\rangle = 0$ für alle $w \in W$.



Bemerkung: Ist $(v_1, \ldots, v_n)$ eine Orthonormalbasis, gilt

$$\operatorname*{proj}_W u = \sum_{i=1}^{n} \langle u, v_i \rangle \, v_i \ .$$

Beweis: Wir beweisen den Satz für eine ONB $(v_1, \ldots, v_n)$ von W.

- $\operatorname{proj}_W u \in W$ da $(v_1, \ldots, v_n)$ Basis von W.
- Da sowohl $\operatorname*{proj}_W u$ als auch w in W liegen, können wir sie in der ONB von W darstellen,

$$\left\langle u - \operatorname*{proj}_W u, w \right\rangle = \left\langle u - \sum_{i=1}^{n} \langle u, v_i \rangle \, v_i, \sum_{j=1}^{n} \langle w, v_j \rangle \, v_j \right\rangle$$

$$= \sum_{j=1}^{n} \langle w, v_j \rangle \langle u, v_j \rangle - \sum_{i=1}^{n} \sum_{j=1}^{n} \langle u, v_i \rangle \langle w, v_j \rangle \langle v_i, v_j \rangle$$
$$= \sum_{j=1}^{n} \langle w, v_j \rangle \langle u, v_j \rangle - \sum_{i=1}^{n} \sum_{j=1}^{n} \langle u, v_i \rangle \langle w, v_i \rangle = 0,$$

wobei in der zweiten Gleichung die Linearität des Skalarprodukts in beiden Argumenten ausgenützt haben und in der dritten Gleichung die ONB-Eigenenschaft der Basis $(v_1, \ldots, v_n)$, d.h. $\langle v_i, v_j \rangle = 0$ wenn $i \neq j$ und $\langle v_i, v_i \rangle = 1$.

Ist die Orthogonalprojektion eindeutig?

42.16 Definition: orthogonales Komplement

Es sei W ein Unterraum eines Skalarproduktraums $(V, \langle \cdot, \cdot \rangle)$. Dann wird

$$W^\perp := \{v \in V \mid \langle v, w \rangle = 0 \ \ \forall w \in W\}$$

als **orthogonales Komplement** von W bezeichnet.

42.17 Satz: Projektionssatz

Es sei W ein endlichdimensionaler Unterraum eines Skalarproduktraums $(V, \langle \cdot, \cdot \rangle)$. Dann besitzt jedes $v \in V$ eine *eindeutige* Darstellung

$$v = w_1 + w_2$$

mit $w_1 \in W$ und $w_2 \in W^\perp$.

Beweis: Die Existenz einer solchen Zerlegung folgt aus den Eigenschaften der orthogonalen Projektion: $v = \underbrace{v - \operatorname{proj}_W v}_{\in W^\perp} + \underbrace{\operatorname{proj}_W v}_{\in W}$

Es seien $w_1, w_1' \in W$ und $w_2, w_2' \in W^\perp$ mit

$$w_1 + w_2 = w_1' + w_2' = v \ .$$

Daraus folgt $w_1 - w_1' = w_2' - w_2$. Da Unterräume abgeschlossen bezüglich der Vektorraumoperationen sind, folgt $w_1 - w_1' \in W$. Wir erhalten

$$\|w_2' - w_2\|^2 = \langle w_2' - w_2, w_2' - w_2 \rangle = \left\langle \underbrace{w_2' - w_2}_{\in W^\perp}, \underbrace{w_1 - w_1'}_{\in W} \right\rangle = 0,$$

nach der Definition des orthogonalen Komplements. Damit gilt $w_2' - w_2 = w_1 - w_1' = 0$, also $w_2 = w_2'$ und $w_1 = w_1'$. □

Die Hauptanwendung der orthogonalen Projektion ergibt sich aus dem folgenden Approximationssatz.

42.18 Satz: Approximationssatz

Es sei $(V, \langle \cdot\,, \cdot \rangle)$ ein Skalarproduktraum mit der induzierten Norm $\|\cdot\|$ und W ein endlichdimensionaler Unterraum. Zu jedem $v \in V$ ist dann $\underset{W}{\operatorname{proj}} v$ die beste Approximation von v in W, d. h.

$$\left\| v - \underset{W}{\operatorname{proj}} v \right\| < \|v - w\| \quad \text{für alle } w \in W \text{ mit } w \neq \underset{W}{\operatorname{proj}} v.$$

Beweis: Es gilt

$$\begin{aligned} \|v - w\|^2 &= \|\underbrace{v - \underset{W}{\operatorname{proj}} v}_{\in W^\perp} + \underbrace{\underset{W}{\operatorname{proj}} w - w}_{\in W}\|^2 \\ &= \left\| v - \underset{W}{\operatorname{proj}} v \right\|^2 + \left\| \underset{W}{\operatorname{proj}} w - w \right\|^2 \quad \text{(Satz des Pythagoras)} \\ &\geq \left\| v - \underset{W}{\operatorname{proj}} v \right\|^2 . \end{aligned}$$

Gleichheit gilt genau dann, wenn $w = \underset{W}{\operatorname{proj}} v$. □

42.19 Beispiel

Wir betrachten $V = C\left[0, \frac{\pi}{2}\right]$ mit dem Skalarprodukt

$$\langle u, v\rangle := \int_0^{\pi/2} u(x)v(x)\,\mathrm{d}x\ .$$

Wir wollen die Gerade bestimmen, die die Funktion $u(x) = \sin x$ im Intervall $\left[0, \frac{\pi}{2}\right]$ bestmöglich (bezüglich der induzierten Norm) approximiert.

Dazu sei $W := \operatorname{span}\{1, x\}$ der Unterraum aller Geraden ($v_1 = 1$, $v_2 = x$).

Wir suchen $\underset{W}{\operatorname{proj}}\, u = \lambda_1 v_1 + \lambda_2 v_2$ mit

$$0 = \langle u - \lambda_1 v_1 - \lambda_2 v_2, v_k\rangle \quad \text{für } k = 1, 2.$$

In unserem Fall haben wir

$$\begin{aligned} 0 &= \langle \sin x - \lambda_1 - \lambda_2 x, 1\rangle \\ 0 &= \langle \sin x - \lambda_1 - \lambda_2 x, x\rangle\ , \end{aligned}$$

woraus sich das folgende lineare Gleichungssystem für die Unbekannten λ_1 und λ_2 ergibt:

$$\begin{aligned} \langle 1, 1\rangle\,\lambda_1 + \langle x, 1\rangle\,\lambda_2 &= \langle \sin x, 1\rangle \\ \langle 1, x\rangle\,\lambda_1 + \langle x, x\rangle\,\lambda_2 &= \langle \sin x, x\rangle\ . \end{aligned}$$

Mit

$$\begin{aligned} \langle 1, 1\rangle &= \int_0^{\pi/2} \mathrm{d}x = \frac{\pi}{2} \\ \langle x, 1\rangle = \langle 1, x\rangle &= \int_0^{\pi/2} x\,\mathrm{d}x = \frac{\pi^2}{8} \\ \langle x, x\rangle &= \int_0^{\pi/2} x^2\,\mathrm{d}x = \left[\frac{1}{3}x^3\right]_0^{\pi/2} = \frac{\pi^3}{24} \\ \langle \sin x, 1\rangle &= \int_0^{\pi/2} \sin x\,\mathrm{d}x = [-\cos x]_0^{\pi/2} = 0 - (-1) = 1 \end{aligned}$$

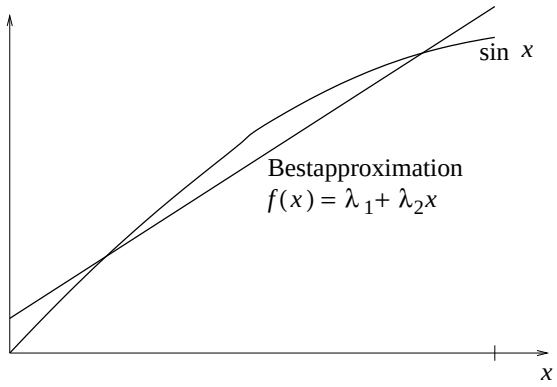
$$\langle \sin x, x \rangle = \int_0^{\pi/2} x \sin x \, \mathrm{d}x = [-x \cos x]_0^{\pi/2} + \int_0^{\pi/2} \cos x \, \mathrm{d}x$$
$$= -\frac{\pi}{2} \cdot 0 + 0 \cdot 1 + [\sin x]_0^{\pi/2} = 1$$

lautet dieses System

$$\begin{pmatrix} \pi/2 & \pi^2/8 \\ \pi^2/8 & \pi^3/24 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} .$$

Es besitzt die Lösung

$$\lambda_1 = 8 \cdot \frac{\pi - 3}{\pi^2} \approx 0{,}11 , \quad \lambda_2 = 24 \cdot \frac{4 - \pi}{\pi^3} \approx 0{,}66 .$$



Nach Satz 42.13 sind orthogonale Mengen linear unabhängig. Kann man umgekehrt aus einer linear unabhängigen Menge eine orthogonale Menge konstruieren ?

42.20 Orthogonalisierungsalgorithmus von Gram und Schmidt

Gegeben:

- Skalarproduktraum $(V, \langle \cdot , \cdot \rangle)$
- Basis $\{u_1, \ldots, u_n\}$ für V

Gesucht: Orthonormalbasis $\{v_1, \ldots, v_n\}$ von V

Schritt 1: $v_1 := \frac{u_1}{\|u_1\|}$,

Schritt k:

- Definiere $W_{k-1} = \text{span}(v_1, \ldots, v_{k-1}) = \text{span}(u_1, \ldots, u_{k-1})$.
- $$v_k' = u_k - \underset{W_{k-1}}{\text{proj}}\, u_k = u_k - \sum_{i=1}^{k-1} \langle u_k, v_i \rangle\, v_i.$$
  $$v_k = \frac{v_k}{\|v_k\|}.$$

  Wir bemerken, daß v_k eine Linearkombination von $v_1, \ldots, v_{k-1}$ und u_k ist. Darauf folgt per Induktion, daß $\text{span}(v_1, \ldots, v_{k-1}) = \text{span}(u_1, \ldots, u_{k-1})$. Es gilt $v_k' \in W_{k-1}^{\perp}$ mit den Eigenschaften der orthogonalen Projektion und damit $\langle v_k', v_i \rangle = 0$ für $i = 1, \ldots, k-1$. und $v_k' \neq 0$, da ansonsten u_k eine Linearkombination von $u_1, \ldots, u_{k-1}$ wäre, was der linearen Unabhängigkeit von $(u_1, \ldots, u_n)$ widerspricht. Zusätzlich gilt $\|v_k\| = 1$.

In der Praxis verwendet man die obige Form des Gram-Schmidt Verfahrens nicht, da sich für großes n Rundungsfehler anhäufen und dazu füren, daß die Basisvektoren nicht mehr orthogonal sind.

Das Gram-Schmidt-Orthogonalisierungsverfahren liefert einen konstruktiven Beweis des folgenden Satzes.

42.21 Satz: Existenz einer Orthogonalbasis

Jeder endlichdimensionale Skalarproduktraum besitzt eine Orthogonalbasis.

Bemerkung: Eine Orthonormalbasis erhält man durch Normierung.

42.22 Beispiel

Wir wollen aus

$$u_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad u_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad u_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

mittels des Gram-Schmidt-Algorithmus eine Orthogonalbasis des euklidischen Raums $\mathbb{R}^3$ konstruieren. Anschließend soll eine Orthonormalbasis konstruiert werden.

$$
\begin{aligned}
v_1 &= u_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \\
v_2 &= u_2 - \frac{\langle u_2, v_1 \rangle}{\|v_1\|^2} v_1 \\
&= \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} - \frac{2}{3} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -2/3 \\ 1/3 \\ 1/3 \end{pmatrix} \\
v_3 &= u_3 - \frac{\langle u_3, v_1 \rangle}{\|v_1\|^2} v_1 - \frac{\langle u_3, v_2 \rangle}{\|v_2\|^2} v_2 \\
&= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - \frac{1}{3} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - \frac{1/3}{2/3} \begin{pmatrix} -2/3 \\ 1/3 \\ 1/3 \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1/3 \\ 1/3 \\ 1/3 \end{pmatrix} - \begin{pmatrix} -1/3 \\ 1/6 \\ 1/6 \end{pmatrix} = \begin{pmatrix} 0 \\ -1/2 \\ 1/2 \end{pmatrix} .
\end{aligned}
$$

$\{v_1, v_2, v_3\}$ ist die gesuchte Orthogonalbasis des $\mathbb{R}^3$.

Die entsprechende Orthonormalbasis $\{w_1, w_2, w_3\}$ lautet

$$
\begin{aligned}
w_1 &= \frac{v_1}{\|v_1\|} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \\
w_2 &= \frac{v_2}{\|v_2\|} = \frac{1}{\sqrt{6}/3} \begin{pmatrix} -2/3 \\ 1/3 \\ 1/3 \end{pmatrix} = \frac{1}{\sqrt{6}} \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix} \\
w_3 &= \frac{v_3}{\|v_3\|} = \frac{1}{1/\sqrt{2}} \begin{pmatrix} 0 \\ -1/2 \\ 1/2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} .
\end{aligned}
$$

43 Fourierreihen

43.1 Motivation

Ähnlich wie eine Taylorreihe (vgl. MfI 1, Kap. 20) eine Funktion durch ein Polynom approximiert, wollen wir eine Funktion durch ein trigonometrisches Polynom annähern.

Hierzu verwenden wir den Approximationssatz 42.18.

43.2 Fourierbasis

Gegeben sei der Vektorraum $V = C[0, 2\pi]$ mit dem Skalarprodukt

$$\langle u, v\rangle := \int_0^{2\pi} u(x)v(x)\,\mathrm{d}x$$

und der induzierten Norm $\|u\| := \sqrt{\langle u, u\rangle}$.

Wir betrachten den endlichdimensionalen Unterraum

$$W := \operatorname{span}\{1, \cos x, \cos(2x), \ldots, \cos(nx), \sin x, \sin(2x), \ldots, \sin(nx)\}\ .$$

Die Elemente von W nennen wir **trigonometrische Polynome vom Grad $\leq n$.**

Satz: Das System

$$\{1, \cos x, \cos(2x), \ldots, \cos(nx), \sin x, \sin(2x), \ldots, \sin(nx)\}$$

ist eine Orthogonalbasis von W.

Beweis: Nach Definition erzeugt das angegebene System W; zu zeigen ist daher die Orthogonalität (aus der die lineare Unabhängigkeit folgt).

Es gilt für $l, m > 0$

$$\langle 1, \cos(mx)\rangle = \int_0^{2\pi} \cos(mx)\,\mathrm{d}x = 0$$

$$\langle 1, \sin(mx)\rangle = \int_0^{2\pi} \sin(mx)\,\mathrm{d}x = 0$$

$$\begin{aligned}
\langle \sin(lx), \cos(mx)\rangle &= \int_0^{2\pi} \sin(lx)\cos(mx)\,\mathrm{d}x \\
&= \frac{1}{2}\int_0^{2\pi} \sin((l+m)x)\,\mathrm{d}x + \frac{1}{2}\int_0^{2\pi} \sin((l-m)x)\,\mathrm{d}x \\
&= \left[\frac{1}{2(l+m)}\cos((m+n)x)\right]_0^{2\pi} + \begin{cases} \int_0^{2\pi} 0\,\mathrm{d}x\,, & l = m\,, \\ \left[\frac{1}{2(l-m)}\cos((l-m)x)\right]_0^{2\pi}\,, & l \neq m \end{cases} \\
&= 0
\end{aligned}$$

$$\begin{aligned}
\langle \cos(lx), \cos(mx)\rangle &= \int_0^{2\pi} \cos(lx)\cos(mx)\,\mathrm{d}x \\
&= \frac{1}{2}\int_0^{2\pi} \cos((l+m)x)\,\mathrm{d}x + \frac{1}{2}\int_0^{2\pi} \cos((l-m)x)\,\mathrm{d}x \\
&= \left[\frac{1}{2(l+m)}\sin((l+m)x)\right]_0^{2\pi} + \begin{cases} \frac{1}{2}\int_0^{2\pi} 1\,\mathrm{d}x\,, & l = m\,, \\ \left[\frac{1}{2(l-m)}\sin((l-m)x)\right]_0^{2\pi}\,, & l \neq m \end{cases} \\
&= \begin{cases} \pi\,, & l = m\,, \\ 0\,, & l \neq m \end{cases}
\end{aligned}$$

$$\begin{aligned}
\langle \sin(lx), \sin(mx)\rangle &= \int_0^{2\pi} \sin(lx)\sin(mx)\,\mathrm{d}x \\
&= -\frac{1}{2}\int_0^{2\pi} \cos((l+m)x)\,\mathrm{d}x + \frac{1}{2}\int_0^{2\pi} \cos((l-m)x)\,\mathrm{d}x
\end{aligned}$$

$$= -\left[\frac{1}{2(l+m)}\sin((l+m)x)\right]_0^{2\pi} + \begin{cases} \frac{1}{2}\int_0^{2\pi} 1\,\mathrm{d}x\ , & l = m\ , \\ \left[\frac{1}{2(l-m)}\sin((l-m)x)\right]_0^{2\pi}\ , & l \neq m \end{cases}$$

$$= \begin{cases} \pi\ , & l = m\ , \\ 0\ , & l \neq m\ . \end{cases}$$

□

Berechnet man noch

$$\langle 1, 1\rangle = \int_0^{2\pi} 1\,\mathrm{d}x = 2\pi\ ,$$

so kennt man auch schon die Nenner für die Anwendung von Satz 42.15 (im Orthogonalbasis-Fall).

43.3 Fourierkoeffizienten

Vektorräume V und $W \subset V$ wie oben; zur Abkürzung setzen wir

$$\begin{aligned} v_0 &:= 1\ , & v_1 &:= \cos x\ , & v_2 &:= \cos(2x)\ , & \ldots \quad v_n &:= \cos(nx)\ , \\ v_{n+1} &:= \sin x\ , & v_{n+1} &:= \sin(2x)\ , & \ldots \quad v_{2n} &:= \sin(nx)\ . \end{aligned}$$

Problemstellung: Es sei eine Funktion $u \in V$ gegeben. Gesucht sind die Koeffizienten

$$a_0, a_1, \ldots, a_n, b_1, \ldots, b_n,$$

für die das trigonometrische Polynom

$$f(x) = \frac{a_0}{2} + \sum_{k=1}^{n} (a_k \cos(kx) + b_k \sin(kx))$$

die beste Approximation an $u(x)$ bezüglich der induzierten Norm $\|\cdot\|$ ist („Approximation im quadratischen Mittel“).

Diese Koeffizienten heißen **Fourierkoeffizienten.**

Lösung: Nach Satz 42.18 ist die Approximation im quadratischen Mittel durch die Orthogonalprojektion

$$f = \operatorname*{proj}_W u$$

gegeben.

Mit der Orthogonalbasis für W nach Satz 43.2 haben wir

$$\begin{aligned} f = \operatorname*{proj}_W u &= \sum_{k=0}^{2n} \frac{\langle u, v_k \rangle}{\|v_k\|^2} \\ &= \frac{1}{2\pi} \langle u, 1 \rangle + \sum_{k=1}^{n} \frac{1}{\pi} \left(\langle u, \cos(kx) \rangle \cos(kx) + \langle u, \sin(kx) \rangle \sin(kx) \right) \end{aligned}$$

und damit

$$\begin{aligned} a_0 &= \frac{1}{\pi} \langle u, 1 \rangle && = \frac{1}{\pi} \int_0^{2\pi} u(x) \, \mathrm{d}x \, , \\ a_k &= \frac{1}{\pi} \langle u, \cos(kx) \rangle && = \frac{1}{\pi} \int_0^{2\pi} u(x) \cos(kx) \, \mathrm{d}x \, , \\ b_k &= \frac{1}{\pi} \langle u, \sin(kx) \rangle && = \frac{1}{\pi} \int_0^{2\pi} u(x) \sin(kx) \, \mathrm{d}x \, , \qquad k = 1, \ldots, n \, . \end{aligned}$$

43.4 Beispiel

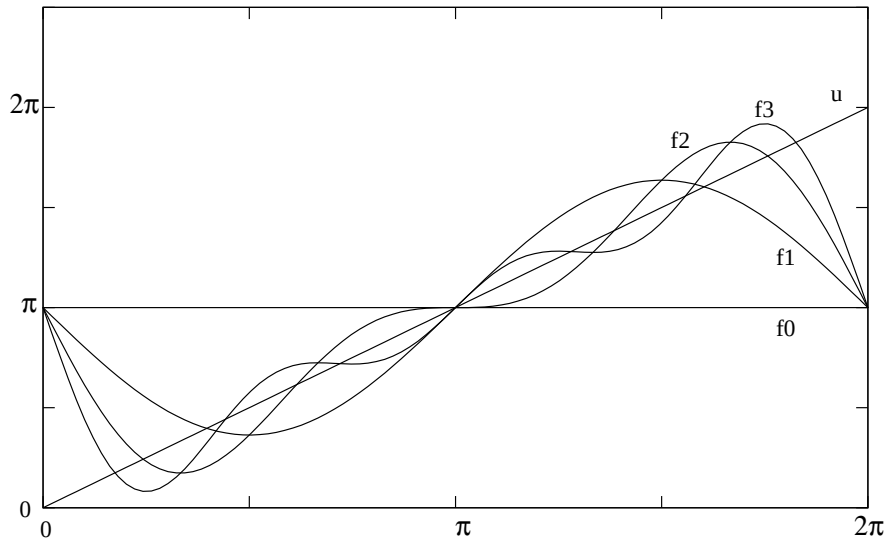
Die Funktion $u(x) = x$ soll auf $[0, 2\pi]$ im quadratischen Mittel durch ein trigonometrisches Polynom vom Grad $\leq n$ approximiert werden.

$$\begin{aligned} a_0 &= \frac{1}{\pi} \int_0^{2\pi} x \, \mathrm{d}x = \frac{1}{\pi} \left[\frac{x^2}{x} \right]_0^{2\pi} = 2\pi \\ a_k &= \frac{1}{\pi} \int_0^{2\pi} x \cos(kx) \, \mathrm{d}x \\ &= \frac{1}{\pi} \Bigg(\underbrace{\left[\frac{x}{k} \sin(kx) \right]_0^{2\pi}}_{=0} - \int_0^{2\pi} \frac{1}{k} \sin(kx) \, \mathrm{d}x \Bigg) \\ &= \frac{1}{\pi} \left[\frac{1}{k^2} \cos(kx) \right]_0^{2\pi} = 0 \quad (k \geq 1) \end{aligned}$$

$$
\begin{aligned}
b_k &= \frac{1}{\pi} \int_0^{2\pi} x \sin(kx)\,\mathrm{d}x \\
&= \frac{1}{\pi} \left(\left[-\frac{x}{k} \cos(kx) \right]_0^{2\pi} + \int_0^{2\pi} \frac{1}{k} \cos(kx)\,\mathrm{d}x \right) \\
&= -\frac{1}{\pi} \cdot \frac{2\pi}{k} + \frac{1}{\pi} \left[\frac{1}{k^2} \sin(kx) \right]_0^{2\pi} \\
&= -\frac{2}{k} \quad (k \geq 1)
\end{aligned}
$$

Das trigonometrische Approximationspolynom lautet also

$$
f_n(x) = \pi - 2 \left(\sin x + \frac{\sin(2x)}{2} + \frac{\sin(3x)}{3} + \ldots + \frac{\sin(nx)}{n} \right) .
$$



43.5 Definition: Fourierreihe

Lässt man den Grad des trigonometrischen Approximationspolynoms gegen ∞ streben, so entsteht die Reihe

$$f(x) = \frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos(kx) + b_k \sin(kx))$$

mit

$$a_k = \frac{1}{\pi} \int_0^{2\pi} u(x) \cos(kx)\, \mathrm{d}x\ , \qquad k = 0, 1, \ldots,$$

$$b_k = \frac{1}{\pi} \int_0^{2\pi} u(x) \sin(kx)\, \mathrm{d}x\ , \qquad k = 1, 2, \ldots$$

Sie heißt **Fourierreihe** von u.

Bemerkung: Falls u differenzierbar ist und $u(0) = u(2\pi), u'(0) = u'(2\pi)$ gilt, so kann man zeigen, dass die Fourierreihe punktweise gegen u konvergiert. (Das heißt, es gibt für jede Stelle $x \in [0, 2\pi]$ und jede Fehlerschranke $\varepsilon > 0$ ein $n_0(x, \varepsilon)$ derart, dass $|u(x) - f_n(x)| < \varepsilon$ für $n > n_0(x, \varepsilon)$ gilt.)

Besitzt u Sprungstellen, so zeigen die Fourierpolynome an den Sprungstellen ausgeprägtes Über- und Unterschwingen (*Gibbs-Phänomen*).

43.6 Praktische Bedeutung

- Fourierreihen sind unentbehrlich in der Signalverarbeitung.
- Die Fourierkoeffizienten eines Signals geben die Anteile der einzelnen Frequenzen an:

  a_k, b_k mit kleinem k entsprechen niedrigen Frequenzen
  a_k, b_k mit großem k entsprechen hohen Frequenzen

- *Filterentwurf* durch Spezifikation im Frequenzbereich:

  1. **Tiefpassfilter:**

- dämpfen hohe Frequenzen
- zur Elimination von Rauschen (das i. A. hochfrequent ist)

2. **Hochpassfilter:**

   - dämpfen tiefe Frequenzen (wie Brumm- oder Rumpelgeräusche)

3. **Bandpassfilter:**

   - lassen nur vorgegebenen Frequenzbereich passieren (z. B. mittlere Frequenzen zur Sprachübertragung)

- Ähnliche Rolle in der Bildverarbeitung:
  - Grauwertbilder sind 2D-Signale
  - Niedrige Frequenzen entsprechen großräumigen Bildstrukturen
  - Hohe Frequenzen verkörpern kleinskalige Details
- Signale und Bilder liegen meist diskret (abgetastet, „gesampelt“) vor. Dann verwendet man eine *diskrete Fouriertransformation,* die Integrale durch Summen ersetzt.
- Es existieren sehr schnelle Algorithmen zur diskreten Fouriertransformation, die ein Signal mit N Werten mit einer Komplexität von $\mathrm{O}(N \log N)$ in seine Frequenzanteile zerlegen (*fast Fourier transform (FFT)*)

43.7 Aktuelle Weiterentwicklung: Wavelets

- Verwenden Basisfunktionen, die nicht nur in der Frequenz, sondern auch im Ort lokalisiert sind.
- Derzeit effizienteste Verfahren zur Signal- und Bildkompression (in JPEG2000- und neuen MPEG-Standards): Viele der Waveletkoeffizienten sind sehr klein und können weggelassen werden, ohne dass es auffällt.
- Hocheffiziente Algorithmen mit $\mathrm{O}(N)$-Komplexität.

44 Orthogonale Matrizen

44.1 Motivation

Im euklidischen Raum $\mathbb{R}^n$ haben wir gesehen, dass Orthonormalbasen zu besonders einfachen und schönen Beschreibungen führen.

Wir wollen das Konzept der Orthonormalität auf Matrizen erweitern. Dies führt auf die wichtige Klasse von orthogonalen Matrizen, die eine Reihe nützlicher Eigenschaften aufweisen. Unter Anderem lassen sich mit ihnen Drehungen und Spiegelungen beschreiben.

44.2 Definition: Orthogonale Matrizen

Besitzt eine Matrix $Q \in \mathbb{R}^{n\times n}$ orthonormale Spaltenvektoren $q_{*1}, \ldots, q_{*n}$, so wird sie als **orthogonale Matrix** bezeichnet.

Man definiert ferner

$$\mathrm{O}(n) := \{Q \in \mathbb{R}^{n\times n} \mid Q \text{ orthogonal}\} .$$

Bemerkungen:
1. Eine präzisere Bezeichnung wäre „orthonormale Matrix“ – hat sich aber nicht durchgesetzt.

2. Die Spaltenvektoren einer orthogonalen Matrix bilden eine Orthonormal*basis* des euklidischen Raumes $\mathbb{R}^n$.

Im Beweis verwenden wir die zwei folgenden Resulate:

44.3 Lemma

Sei $A \in \mathbb{R}^{n\times m}$ und $u \in \mathbb{R}^n, v \in \mathbb{R}^m$. Dann gilt

$$\langle u, Av\rangle = \left\langle A^T u, v\right\rangle ,$$

wobei $\langle\cdot,\cdot\rangle$ das euklidische Skalarprodukt ist.

Beweis: Mit $A = (a_{ij})$ ergibt sich das Matrix-Vektor-Produkt Av in Komponenten: $(Av)_i = \sum_{j=1}^{m} a_{ij} v_j$. Damit ergibt sich das euklidische Skalarprodukt als:

$$\langle u, Av \rangle = \sum_{i=1}^{n} u_i (Av)_i = \sum_{i=1}^{n} \sum_{j=1}^{m} u_i a_{ij} v_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ji}^T u_i v_j = \sum_{j=1}^{n} (A^T u)_j v_j = \left\langle A^T u, v \right\rangle .$$

44.4 Lemma: Polarisierungsgleichung

Sei $(V, \langle \cdot, \cdot \rangle)$ ein reeller Skalarproduktraum. Dann gilt für alle $u, v \in V$,

$$\langle u, v \rangle = \frac{1}{4} \Big[\, \|u + v\|^2 - \|u - v\|^2 \, \Big]$$

Beweis: Übungsaufgabe.

44.5 Satz: Eigenschaften orthogonaler Matrizen

Die folgenden Aussagen sind für Matrizen $Q \in \mathbb{R}^{n \times n}$ äquivalent:

a) $Q \in \mathrm{O}(n)$.

b) Q ist invertierbar, und es ist

$$Q^{-1} = Q^{\mathrm{T}} \, .$$

c) Multiplikation von Vektoren mit Q erhält das euklidische Produkt zwischen Vektoren:

$$(Qu) \cdot (Qv) = u \cdot v \qquad \text{für alle } u, v \in \mathbb{R}^n.$$

d) Multiplikation von Vektoren mit Q erhält die euklidische Norm:

$$|Qv| = |v| \qquad \text{für alle } v \in \mathbb{R}^n.$$

Man nennt daher Q auch **Isometrie** (längenerhaltende Abbildung).

Beweis:

- (a)⇒(b): Da die Spaltenvektoren einer orthogonalen Matrix $Q \in \mathbb{R}^{n\times n}$ ein Orthonormalsystem bilden, sind sie nach Satz 42.13 auch linear unabhängig. Damit hat Q den Rang n, ist also invertierbar.

  Es sei $A = (a_{ij}) = Q^{\mathrm{T}}Q$. Dann gilt:

  $$a_{ij} = \sum_{k=1}^{n} q_{ki}q_{kj} = q_{*i} \cdot q_{*j} = \begin{cases} 1\,, & i = j\,, \\ 0\,, & \text{sonst.} \end{cases}$$

  Also ist $Q^{\mathrm{T}}Q = I$.

  Wegen der Invertierbarkeit von Q und 36.9 ist damit $Q^{\mathrm{T}} = Q^{-1}$.

- (b)⇒(c): Für alle $u, v \in \mathbb{R}^n$ gilt für das euklidische Skalarprodukt $\langle\cdot,\cdot\rangle$,

  $$\langle Qu, Qv\rangle = \left\langle u, \underbrace{Q^T Q}_{=I} v \right\rangle = \langle u, v\rangle\,.$$

- (c)⇒(d): Für alle $u \in \mathbb{R}^n$ gilt,

  $$\|Qu\|^2 = \langle Qu, Qu\rangle = \langle u, u\rangle = \|u\|^2\,.$$

- (d)⇒(a): Der i-te Spaltenvektor q_i der Matrix Q ist gegeben durch $q_i = Qe_i$, wobei e_i der i-te kanonische Basisvektor ist. Mittels der Polarisierungsgleichung aus Lemma 44.4 erhalten wir,

  $$\begin{aligned} \langle q_i, q_j\rangle = \langle Qe_i, Qe_j\rangle &= \frac{1}{4}\Big[\, \|Q(e_i + e_j)\|^2 - \|Q(e_i - e_j)\|^2 \,\Big] \\ &= \frac{1}{4}\Big[\, \|e_i + e_j\|^2 - \|e_i - e_j\|^2 \,\Big] = \begin{cases} 1, & \text{wenn } i = j, \\ 0, & \text{sonst.} \end{cases} \end{aligned}$$

  Daher sind die Spaltenvektoren $(q_1, \ldots, q_n)$ der Matrix Q orthonormal und damit ist Q eine orthogonale Matrix.

□

Bemerkung: Ist $Q \in \mathbb{R}^{n\times n}$ eine orthogonale Matrix, dann ist auch die transponierte Matrix Q^T orthogonal, denn es gilt für alle $u, v \in \mathbb{R}^n$,

$$\left\langle Q^T u, Q^T v\right\rangle = \left\langle u, QQ^T v\right\rangle = \langle u, v\rangle\,.$$

44.6 Beispiele

a) Rotationen können durch orthogonale Matrizen beschrieben werden:

$$Q = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

beschreibt eine Drehung um den Winkel α, vgl. 35.6(e).

$$Q^{\mathrm{T}} = Q^{-1} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$$

entspricht der Drehung um $-\alpha$.

Es gilt

$$\det Q = \cos^2\alpha + \sin^2\alpha = 1 \ .$$

b) Es gibt auch orthogonale Matrizen, die keine Drehungen beschreiben, z. B.

$$Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ .$$

Q vertauscht die x- und y-Komponente

$$Q \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} v_2 \\ v_1 \end{pmatrix}$$

und stellt damit eine *Spiegelung* an der Winkelhalbierenden des 1. Quadranten dar.

Hier gilt

$$\det Q = 0 - 1 = -1 \ .$$

Kann die Determinante orthogonaler Matrizen andere Werte als ± 1 annehmen? Nein!

44.7 Satz: Determinante orthogonaler Matrizen

Für jedes $Q \in \mathrm{O}(n)$ gilt $|\det Q| = 1$.

Beweis: Aus $QQ^{\mathrm{T}} = I$ folgt

$$1 = \det I = \det(QQ^{\mathrm{T}}) = \det Q \cdot \det Q^{\mathrm{T}} = (\det Q)^2 \ .$$

□

Orthogonale Matrizen Q mit $\det Q = 1$ werden noch einmal besonders ausgezeichnet.

44.8 Definition

Man definiert

$$\mathrm{SO}(n) := \mathrm{O}^{+}(n) := \{Q \in \mathrm{O}(n) \mid \det Q = 1\} \ .$$

44.9 Satz: Gruppeneigenschaft von O(n) und SO(n)

$\mathrm{O}(n)$ und $\mathrm{SO}(n)$ sind Untergruppen der allgemeinen linearen Gruppe $\mathrm{GL}(n, \mathbb{R})$ (vgl. 35.12).

Man nennt $\mathrm{O}(n)$ die **orthogonale Gruppe** und $\mathrm{SO}(n)$ die **spezielle orthogonale Gruppe.**

Beweis: Übungsaufgabe

Bemerkung: Eine Matrix aus $\mathrm{O}(n)$ beschreibt eine *orthogonale Transformation* des euklidischen Raumes $\mathbb{R}^n$, d. i. eine „starre“ Transformation des $\mathbb{R}^n$, die den Ursprung 0 fest lässt.

Matrizen aus $\mathrm{SO}(n)$ entsprechen dabei *orientierungserhaltenden* Transformationen. (Diese lassen in $\mathbb{R}^2$ z. B. den Umlaufsinn unverändert, in $\mathbb{R}^3$ die „Händigkeit“ eines Tripels von Vektoren oder den Drehsinn einer Schraube, einer Spirale etc. Entsprechende Konzepte von Orientierung lassen sich auch in höheren Dimensionen einführen.) Es handelt sich um „echte Bewegungen“, die eine stetige Überführung des Anfangs- in den Endzustand ermöglichen. Das sind beliebige Drehungen um 0 im $\mathbb{R}^n$.

Eine Matrix aus $\mathrm{O}^-(n) := \mathrm{O}(n) \setminus \mathrm{SO}(n)$ verkörpert hingegen stets eine *orientierungsumkehrende* Transformation, d. h. eine Drehung verknüpft mit einer Spiegelung. (Nur im $\mathbb{R}^2$ reicht eine Spiegelung alleine aus.)

Wo treten orthogonale Matrizen noch auf? Der Wechsel zwischen Orthogonalbasen ist besonders einfach, da er durch eine orthogonale Matrix erzeugt wird.

44.10 Wechsel zwischen Orthonormalbasen

Seien $B = (u_1, \ldots, u_n)$ und $C = (v_1, \ldots, v_n)$ zwei Orthonormalbasen des $\mathbb{R}^n$. In der Übergangs-Matrix $(I)_B^C = (s_{ij})$, die die Koordinatendarstellung bezüglich der Basis B in die Koordinatendarstellung bezüglich der Basis C überführt, stehen als Spaltenvektoren die Bilder Basisvektoren von C bezüglich der Basis C d.h. für $i = 1, \ldots, n$

$$u_i = \sum_{j=1}^{n} s_{ji} v_j.$$

Die Koeffizienten s_{ij} erhalten wir für eine ONB besonders einfach, denn

$$s_{ji} = \langle v_j, u_i \rangle .$$

Die Vektoren der ONB B und C sind orthonormal und daher,

$$\left.\begin{array}{ll} 1, & \text{wenn } i = j, \\ 0, & \text{sonst.} \end{array}\right\} = \langle u_i, u_j \rangle = \left\langle \sum_{k=1}^{n} s_{ki} v_k, \sum_{l=1}^{n} s_{lj} v_l \right\rangle$$
$$= \sum_{k=1}^{n} \sum_{l=1}^{n} s_{ki} s_{lj} \ \langle v_k, v_l \rangle$$
$$= \sum_{k=1}^{n} s_{ki} s_{kj}$$

und daher sind die Spaltenvektoren $s_{\cdot i}$ und $s_{\cdot j}$ der Matrix $(I)_B^C$ orthonormal und daher ist $(I)_B^C$ eine orthogonale Matrix.

Die Umkehrtransformation $(I)_C^B$ ist die inverse Matrix und daher in diesem Fall einfach gegeben durch $(I)_C^B = \left((I)_B^C\right)^T$.

Bemerkungen:
1. Umgekehrt beschreibt bei gegebener Orthonormalbasis $\{v_1, \ldots, v_n\}$ jede orthogonale Matrix Q den Wechsel zu einer anderen Orthonormalbasis $\{w_1, \ldots, w_n\}$.

2. Drehungen oder allgemeiner Orthogonaltransformationen der Vektoren im $\mathbb{R}^n$ in einer festen Basis und Basiswechsel stehen in einem engen Zusammenhang:

Eine Drehung/Transformation der Basis um eine Matrix Q unter Beibehaltung der Vektoren entspricht einer Drehung/Transformation der Vektoren um $Q^{-1} = Q^{\mathrm{T}}$ unter Beibehaltung der Basis.

Beispielsweise dreht in $\mathbb{R}^2$ die Matrix

$$R = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

die Vektoren bezüglich einer festen Basis um α, vgl. 35.6(e), 44.6(a).

Für eine Drehung der Basis um α erhält man dagegen Folgendes: Wählen wir für die erste Basis die Standardbasisvektoren $v_1 = (1,0)^{\mathrm{T}}$, $v_2 = (0,1)^{\mathrm{T}}$, so lauten die Vektoren der gedrehten Basis $w_1 = (\cos\alpha, \sin\alpha)^{\mathrm{T}}$, $w_2 = (-\sin\alpha, \cos\alpha)$, und es ergibt sich

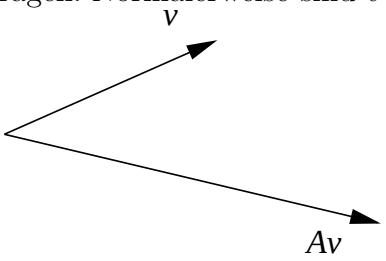
$$\begin{aligned} Q &= \begin{pmatrix} - & w_1^{\mathrm{T}} & - \\ - & w_2^{\mathrm{T}} & - \end{pmatrix} \begin{pmatrix} | & | \\ v_1 & v_2 \\ | & | \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = R^{-1} \,. \end{aligned}$$

45 Eigenwerte und Eigenvektoren

45.1 Motivation

- Eigenvektor- bzw. Eigenwertprobleme sind wichtig in vielen Gebieten wie Physik, Elektrotechnik, Maschinenbau, Statik, Biologie, Informatik, Wirtschaftswissenschaften. Eigenvektoren/Eigenwerte beschreiben oft besondere Zustände von Systemen.

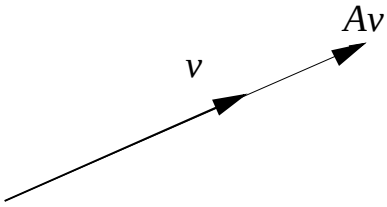
- Ist $v \in \mathbb{R}^n$ ein Vektor und $A \in \mathbb{R}^{n \times n}$ eine quadratische Matrix, so liegen die Vektoren v und Av beide in $\mathbb{R}^n$. Man kann daher sinnvoll nach ihrer gegenseitigen Lage fragen. Normalerweise sind v und Av nicht parallel.



  Gibt es ausgezeichnete Richtungen v, für die Av ein skalares Vielfaches von v ist, also

$$A\,v = \lambda v$$

  gilt?



- *Beispiel zur Anwendung:* Schwingungsfähige Systeme besitzen bevorzugte Frequenzen – Resonanzfrequenzen – , die durch Eigenvektoren beschrieben werden können (vgl. Fourierbasen/Fourierreihen, Kap 43).

  – Erwünscht: Musikinstrumente

  – Unerwünscht: Eigenschwingungen von Bauwerken.
    Hier können so genannte „Resonanzkatastrophen“ bis zur Zerstörung führen: Die Brücke von Angers soll 1850 durch den Gleichschritt darüber marschierender Soldaten zum Einsturz gebracht worden sein. Die Hängebrücke über die Tacoma Narrows stürzte 1940 ein, nachdem sie durch den Wind zu immer stärkeren Schwingungen angeregt wurde.

45.2 Definition: Eigenwert, Eigenvektor

Es sei $A \in K^{n\times n}$. Dann heißt ein von 0 verschiedener Vektor $v \in K^n$ **Eigenvektor** von A, wenn es ein $\lambda \in K$ gibt mit

$$A\,v = \lambda v\ .$$

Der Skalar λ heißt dann **Eigenwert** von A.

Bemerkung: Wir werden nur auf $K = \mathbb{R}$ und $K = \mathbb{C}$ näher eingehen.

45.3 Beispiel

Der Vektor $v = \begin{pmatrix}1\\2\end{pmatrix} \in \mathbb{R}^2$ ist ein Eigenvektor von $A = \begin{pmatrix}3 & 0\\8 & -1\end{pmatrix}$, denn

$$A\,v = \begin{pmatrix}3 & 0\\8 & -1\end{pmatrix}\begin{pmatrix}1\\2\end{pmatrix} = \begin{pmatrix}3\\6\end{pmatrix} = 3v\ .$$

Der zugehörige Eigenwert ist 3.

Wie kann man Eigenwerte und Eigenvektoren bestimmen?

45.4 Bestimmung von Eigenwerten

Es sei $A \in K^{n\times n}$. Aus der Bedingung $A\,v = \lambda v$ folgt $(A - \lambda I)v = 0$.

Der Nullvektor ist in der Eigenvektordefinition ausgeschlossen, da $A0 = 0$ stets gilt. Wir suchen also nichttriviale Lösungen von

$$(A - \lambda I)v = 0\ .$$

Dies ist ein homogenes lineares Gleichungssystem, es besitzt also nichttriviale Lösungen genau dann, wenn $\operatorname{rang}(A - \lambda I) < n$ ist, also genau dann, wenn

$$\det(A - \lambda I) = 0\ .$$

Dies ist ein Polynom n-ten Grades in λ (das **charakteristische Polynom** von A). Seine Nullstellen sind die gesuchten Eigenwerte.

45.5 Beispiel

a) Für $A = \begin{pmatrix} 2 & 1 \\ 6 & 1 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ erhalten wir

$$\begin{aligned} 0 = \det(A - \lambda I) &= \begin{vmatrix} 2-\lambda & 1 \\ 6 & 1-\lambda \end{vmatrix} \\ &= (2-\lambda)(1-\lambda) - 6 = \lambda^2 - 3\lambda - 4 \end{aligned}$$

und damit

$$\begin{aligned} \lambda_{1,2} &= \frac{3 \pm \sqrt{9+16}}{2} = \frac{3 \pm 5}{2} \\ \lambda_1 &= 4\,, \qquad \lambda_2 = -1\,. \end{aligned}$$

b) Für $A = \begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ ergibt sich

$$\begin{aligned} 0 = \det(A - \lambda I) &= \begin{vmatrix} 3-\lambda & 4 \\ -4 & 3-\lambda \end{vmatrix} \\ &= (3-\lambda)^2 - 4 \cdot (-4) = \lambda^2 - 6\lambda + 25\,. \end{aligned}$$

Da die Diskriminante $\frac{(-6)^2}{4} - 25 < 0$ ist, hat diese quadratische Gleichung für λ keine reellen Lösungen. Es gibt also keine Eigenwerte.

Das ist plausibel: A ist gleich dem Fünffachen einer Rotationsmatrix (zum Winkel $\alpha = -\arcsin\frac{4}{5} \approx 0{,}927 \mathrel{\widehat{=}} 53{,}1°$). Da alle Vektoren gedreht werden, gibt es keine Eigenvektoren, daher auch keine Eigenwerte.

c) Betrachten wir dieselbe Matrix $A = \begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix}$ als Matrix aus $\mathbb{C}^{2\times 2}$, so finden wir für die charakteristische Gleichung die beiden komplexen Lösungen

$$\lambda_{1,2} = 3 \pm \sqrt{-16} = 3 \pm 4\mathrm{i}\,.$$

Es gibt also zwei konjugiert komplexe Eigenwerte.

45.6 Bemerkungen

a) Wie das letzte Beispiel zeigt, kann das charakteristische Polynom selbst dann komplexe Nullstellen besitzen, wenn A nur reelle Einträge hat. Es ist oft sinnvoll, auch die komplexen Eigenwerte mit zu betrachten.

b) Sucht man Eigenwerte einer $n \times n$-Matrix A als Nullstellen des charakteristischen Polynoms, so kann dies für $n \geq 3$ schon recht schwierig werden; für $n \geq 5$ ist es im Allgemeinen nicht mehr möglich, die Lösungen auf analytischem Wege zu finden. Dann werden numerische Approximationen benötigt (ebenfalls nicht ganz einfach, vgl. späteres Kapitel).

c) Im Falle $K = \mathbb{C}$ kann man zeigen, dass $\det A$ das Produkt der Eigenwerte ist. Allgemein ist A genau dann invertierbar, wenn 0 kein Eigenwert von A ist.

Trotz der genannten Einschränkungen ist das charakteristische Polynom in Spezialfällen sehr nützlich, etwa bei Dreiecksmatrizen (vgl. 35.4(c)).

45.7 Satz: Eigenwerte von Dreiecksmatrizen

Ist $A \in K^{n \times n}$ eine obere oder untere Dreiecksmatrix, so sind die Eigenwerte durch die Diagonaleinträge gegeben.

Beweis: Die Determinante einer Dreiecksmatrix ist das Produkt ihrer Diagonaleinträge. Ist $A = (a_{ij})$, so erhält man daraus für die Matrix $A - \lambda I$

$$\det(A - \lambda I) = (a_{11} - \lambda) \cdot \ldots \cdot (a_{nn} - \lambda) \ ,$$

woraus unmittelbar folgt, dass die Eigenwerte durch

$$\lambda_1 = a_{11} \ , \quad \ldots , \quad \lambda_n = a_{nn}$$

gegeben sind. □

45.8 Beispiel

Die Eigenwerte von $A = \begin{pmatrix} 3 & 0 \\ 8 & -1 \end{pmatrix}$ sind $\lambda_1 = 3$ und $\lambda_2 = -1$ (vgl. Beispiel 45.3).

45.9 Bestimmung der Eigenvektoren

Angenommen, der Eigenwert λ der Matrix $A \in K^{n\times n}$ sei bereits bekannt. Dann sind die zugehörigen Eigenvektoren nichttriviale Lösungen von

$$(A - \lambda I)v = 0\ . \qquad (*)$$

Eigenvektoren sind daher *nicht* eindeutig bestimmt:

Mit v ist stets auch jedes αv, $\alpha \in K$, Eigenvektor.

Der Lösungsraum von $(*)$ heißt **Eigenraum** von A zum Eigenwert λ. Man sucht daher Basisvektoren im Eigenraum und gibt diese als Eigenvektoren an.

45.10 Beispiel

Man bestimme die Basen der Eigenräume von $A = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 2 & 1 \\ 1 & 0 & 3 \end{pmatrix}$.

Eigenwerte: Wegen $\det(A - \lambda I) = (\lambda - 1)(\lambda - 2)^2$ sind $\lambda_1 = 2$ und $\lambda_2 = 1$ die Eigenwerte von A.

- Der Eigenraum zum $\lambda_1 = 2$ ist der Lösungsraum von

$$\begin{pmatrix} -2 & 0 & -2 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}\ .$$

  Dies sind drei linear abhängige Gleichungen mit der Lösungsmenge

$$\left\{ \begin{pmatrix} s \\ t \\ -s \end{pmatrix} \;\middle|\; s, t \in \mathbb{R} \right\}\ .$$

  Eine Basis dieses Eigenraums ist daher z. B.

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

- Der Eigenraum zu $\lambda_2 = 1$ ist die Lösungsmenge von

$$\begin{pmatrix} -1 & 0 & -2 \\ 1 & 1 & 1 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} .$$

  Die erste und dritte Gleichung sind linear abhängig. Addition der Gleichungen 1 und 2 ergibt $x_2 - x_3 = 0$. Setzt man $x_2 := s$, so folgt $x_3 = s$ und über Gleichung 3 schließlich $x_1 = -2s$.

  Damit ergibt sich der eindimensionale Eigenraum

$$\left\{ \begin{pmatrix} -2s \\ s \\ s \end{pmatrix} \;\middle|\; s \in \mathbb{R} \right\} ,$$

  der z. B. von dem Basisvektor $\begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}$ aufgespannt wird.

Die Wirkung einer Matrix $A \in \mathbb{R}^{n \times n}$ auf ihre Eigenvektoren ist besonders einfach zu überblicken. Falls es gelingt, eine Basis des $\mathbb{R}^n$ anzugeben, die nur aus Eigenvektoren von A besteht, so kann man die Wirkung von A auf alle Vektoren in $\mathbb{R}^n$ auf diesen einfachen Fall zurückführen. Deshalb interessieren wir uns jetzt für die Frage: Unter welchen Bedingungen kann man zu einer Matrix $A \in \mathbb{R}^{n \times n}$ eine Basis des $\mathbb{R}^n$ angeben, die aus Eigenvektoren von A besteht?

45.11 Definition: Diagonalisierbare Matrizen

Eine Matrix $A \in \mathbb{R}^{n \times n}$ heißt **diagonalisierbar,** wenn es eine invertierbare Matrix P gibt, mit der $P^{-1}AP$ eine Diagonalmatrix ist.

45.12 Satz: Diagonalisierbarkeit und Basis aus Eigenvektoren

Eine Matrix $A \in \mathbb{R}^{n \times n}$ ist genau dann diagonalisierbar, wenn sie n linear unabhängige Eigenvektoren besitzt.

Beweisidee: Ist $P^{-1}AP = D$ Diagonalmatrix, so folgt $AP = PD$, und man überlegt sich, dass dann der i-te Spaltenvektor von P Eigenvektor von A ist, mit dem i-ten Diagonaleintrag von D als Eigenwert.

Umgekehrt kann man aus n gegebenen linear unabhängigen Eigenvektoren von A eine Matrix P aufbauen, die A diagonalisiert. □

45.13 Beispiel:

Aus Beispiel 45.10 kennen wir die Eigenwerte und Eigenvektoren der Matrix

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

Aus den drei linear unabhängigen Eigenvektoren erhalten wir die Matrix

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

und berechnen

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

Andererseits können wir aus den Eigenwerten die Diagonalmatrix $D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ bilden und prüfen nach, dass

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

gilt. Also ist tatsächlich

$$P^{-1}AP = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 0 & -2 \\ 1 & 2 & 1 \\ 1 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

eine Diagonalisierung von A.

45.14 Paarweise verschiedene Eigenwerte

Man kann insbesondere zeigen: Sind $\lambda_1, \ldots, \lambda_k$ paarweise verschiedene Eigenwerte von A und $v_1, \ldots, v_k$ Eigenvektoren zu diesen Eigenwerten, so ist $\{v_1, \ldots, v_k\}$ linear unabhängig. Das führt zu dem folgenden Satz.

Satz: Ist $A \in \mathbb{R}^{n \times n}$ eine Matrix mit n paarweise verschiedenen Eigenwerten, so ist A diagonalisierbar.

Bemerkung: Eine (über $\mathbb{R}$ und auch über $\mathbb{C}$) nicht diagonalisierbare Matrix ist z. B. $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

45.15 Satz: Eigenwerte von Potenzen einer Matrix

Es sei $A \in K^{n \times n}$, $k \in \mathbb{N}$, und λ sei Eigenwert von A zum Eigenvektor v. Dann ist λ^k Eigenwert von A^k zum Eigenvektor v.

Ist A invertierbar, so gilt diese Aussage sogar für beliebige ganze Zahlen k, wobei $A^{-k} = (A^{-1})^k$.

Beweis: Für $k > 0$ gilt

$$\begin{aligned} A^k v &= A^{k-1}(A\,v) = A^{k-1}(\lambda v) = \lambda\, A^{k-1} v \\ &= \lambda\, A^{k-2}(A\,v) = \lambda^2 A^{k-2} v = \ldots = \lambda^k v\ . \end{aligned}$$

Für $k = 0$ ist $A^0 = I$. $\lambda^0 = 1$ ist offenbar Eigenwert der Einheitsmatrix für jeden Eigenvektor $v \in K^n$.

Ist A invertierbar, so gilt für den Eigenvektor v von A mit zugehörigem Eigenwert $\lambda \neq 0$

$$v = A^{-1}(A\,v) = A^{-1}(\lambda v) = \lambda(A^{-1} v)$$

und daher $A^{-1} v = \lambda^{-1} v$. Analog zum Fall $k \geq 1$ schließt man auf beliebige negative k. □

45.16 Beispiel

A^7 mit $A = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 2 & 1 \\ 1 & 0 & 3 \end{pmatrix}$ aus Beispiel 45.10 hat die Eigenwerte $\lambda_1 = 2^7 = 128$ und $\lambda_2 = 1^7 = 1$.

46 Eigenwerte und Eigenvektoren symmetrischer Matrizen

46.1 Motivation

- Symmetrische Matrizen ($a_{ij} = a_{ji}$ für alle i, j) kommen in der Praxis besonders häufig vor. Gibt es für sie spezielle Aussagen über Eigenwerte und Eigenvektoren?
- Wir hatten den Zusammenhang zwischen Diagonalisierbarkeit und linear unabhängigen Eigenvektoren kennengelernt. Spielt hier die Symmetrie von Matrizen eine besondere Rolle?

46.2 Satz: Eigenwerte und Eigenvektoren symmetrischer Matrizen

Für eine symmetrische Matrix $A \in \mathbb{R}^{n\times n}$ gilt:

a) A hat nur reelle Eigenwerte.

b) Eigenvektoren zu verschiedenen Eigenwerten sind orthogonal.

Beweis: zu (a): Wir erinnern daran, dass für eine komplexe Zahl $z = x + \mathrm{i}y$ ihr Produkt mit der konjugiert komplexen Zahl $\bar{z} = x - \mathrm{i}y$ reell ist: $z\,\bar{z} = |z|^2 = x^2 + y^2 \in \mathbb{R}$.

Die komplexe Konjugation von Vektoren und Matrizen wird komponentenweise definiert.

Dann ist

$$\begin{aligned}\bar{\lambda}\bar{v}^{\mathrm{T}}v &= \overline{(\lambda v)}^{\mathrm{T}}v = \overline{(Av)}^{\mathrm{T}}v \\ &= \bar{v}^{\mathrm{T}}\bar{A}^{\mathrm{T}}v = \bar{v}^{\mathrm{T}}Av \qquad \text{(da } A \text{ reell und symmetrisch)} \\ &= \bar{v}^{\mathrm{T}}(\lambda v) = \lambda\bar{v}^{\mathrm{T}}v\ .\end{aligned}$$

Da $\bar{v}^{\mathrm{T}}v$ reell und ungleich 0 ist, folgt $\bar{\lambda} = \lambda$, also $\lambda \in \mathbb{R}$.

zu (b): Es seien v_1, v_2 Eigenvektoren von A zu verschiedenen Eigenwerten λ_1, λ_2. Dann gilt

$$\begin{aligned}\lambda_1 v_1^{\mathrm{T}} v_2 &= (Av_1)^{\mathrm{T}} v_2 = v_1^{\mathrm{T}} A^{\mathrm{T}} v_2 \\ &= v_1^{\mathrm{T}} (Av_2) \qquad (A \text{ symmetrisch}) \\ &= \lambda_2 v_1^{\mathrm{T}} v_2\end{aligned}$$

und damit

$$0 = \underbrace{(\lambda_1 - \lambda_2)}_{\neq 0} v_1^{\mathrm{T}} v_2 \, .$$

Folglich sind v_1 und v_2 orthogonal. □

46.3 Beispiel

Wir betrachten die symmetrische Matrix $A = \begin{pmatrix} 4 & 12 \\ 12 & 11 \end{pmatrix}$. Wegen

$$0 = \det(A - \lambda I) = \begin{vmatrix} 4-\lambda & 12 \\ 12 & 11-\lambda \end{vmatrix} = \lambda^2 - 15\lambda - 100$$

besitzt A die beiden reellen Eigenwerte $\lambda_1 = 20$ und $\lambda_2 = -5$.

Eigenvektor zu $\lambda_1 = 20$*:*

$$\begin{pmatrix} -16 & 12 \\ 12 & -9 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0$$

hat die Lösungen $x_1 = 3s, x_2 = 4s$, $s \in \mathbb{R}$.

Also ist $v_1 = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ ein Eigenvektor zu λ_1.

Eigenvektor zu $\lambda_2 = -5$*:*

$$\begin{pmatrix} 9 & 12 \\ 12 & 16 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0$$

hat die Lösungen $x_1 = 4s, x_2 = -3s$, $s \in \mathbb{R}$.

Also ist $v_2 = \begin{pmatrix} 4 \\ -3 \end{pmatrix}$ ein Eigenvektor zu λ_2.

Wegen $v_1 \cdot v_2 = 3 \cdot 4 - 4 \cdot 3$ sind die Eigenvektoren orthogonal.

Bemerkung: Es gilt auch: Ist λ ein Eigenwert der Vielfachheit k, so hat λ auch einen k-dimensionalen Eigenraum.

Diese Eigenschaft und die Eigenschaften aus Satz 46.2 stellen insgesamt sicher, dass $\mathbb{R}^n$ eine Basis aus Eigenvektoren von A besitzt. Es handelt sich sogar um eine Orthogonalbasis.

Da sich aus einer Orthogonalbasis eine Orthonormalbasis herstellen lässt, ist eine symmetrische Matrix nicht nur stets diagonalisierbar, sondern die Diagonalisierung ist sogar stets durch eine orthogonale Matrix möglich.

46.4 Satz: Hauptachsentransformation, Spektraldarstellung

Es sei $A \in \mathbb{R}^{n\times n}$ symmetrisch. Dann ist

$$A = Q\Lambda Q^{\mathrm{T}}$$

eine Diagonalisierung von A, wobei

$$\Lambda = \operatorname{diag}(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & \lambda_n \end{pmatrix}$$

die Diagonalmatrix aus den (reellen) Eigenwerten von A ist und Q eine orthogonale Matrix ist, deren Spaltenvektoren orthonormale Eigenvektoren von A sind.

Beweis: Da A symmetrisch ist, gibt es eine Basis von $\mathbb{R}^n$ aus orthonormalen Eigenvektoren von A. Nach Satz 45.12 kann daraus eine Diagonalisierung von A konstruiert werden:

$$D = P^{-1}AP\ ,$$

wobei die invertierbare Matrix P aus den Eigenvektoren von A gebildet wird und D die Diagonalmatrix der zugehörigen Eigenwerte ist, also $D = \Lambda$. Wegen der Orthonormalität der Eigenvektoren ist $P = Q$ dann eine orthogonale Matrix, und es folgt

$$A = Q\Lambda Q^{-1}\ ,$$

also wegen $Q^{-1} = Q^{\mathrm{T}}$ die behauptete Darstellung. □

Bemerkungen: 1. Die Diagonalisierung durch eine orthogonale Matrix bedeutet, die durch die Matrix A beschriebene Abbildung von Vektoren in einem neuen Koordinatensystem zu beschreiben (orthogonale Matrix – Wechsel des Orthonormalsystems!).

$$Au = Q\Lambda Q^{-1}u$$

u	Vektor in Standardbasis
$Q^{-1}u$	Vektor in neuer Basis aus orthonormalen Eigenvektoren von A
$\Lambda Q^{-1}u$	Abbildung darauf angewendet, Vektor noch immer in Eigenvektorbasis ausgedrückt
$Q\Lambda Q^{-1}u$	Rücktransformiert in Standardbasis

Die Basisvektoren der neuen Basis sind die orthonormalen Eigenvektoren von A. In dieser neuen Basis ist die Gestalt der Abbildung besonders einfach, da sie hier durch die Diagonalmatrix Λ gegeben ist. Deswegen nennt man die Basisvektorrichtungen auch Hauptachsenrichtungen von A.

Geometrisch bedeutet dies, dass unabhängig voneinander in jeder Hauptachsenrichtung eine Streckung mit dem jeweiligen Eigenwert als Streckungsfaktor erfolgt (einschließlich Richtungsumkehr für negative Eigenwerte).

2. A lässt sich auch schreiben als

$$A = \lambda_1 v_1 v_1^{\mathrm{T}} + \ldots + \lambda_n v_n v_n^{\mathrm{T}} \; .$$

In dieser Darstellung erkennt man sofort, dass λ_k die Eigenwerte und v_k die zugehörigen Eigenvektoren sind, denn

$$Av_k = \sum_{i=1}^{n} \lambda_i v_i \underbrace{v_i^{\mathrm{T}} v_k}_{=0 \text{ für } i \neq k} = \lambda_k v_k \; .$$

46.5 Beispiel

Wir wollen $A = \begin{pmatrix} 4 & 12 \\ 12 & 11 \end{pmatrix}$ diagonalisieren. Wir benutzen die Eigenwerte und Eigenvektoren aus Beispiel 46.3, normieren letztere aber zu $w_1 = \begin{pmatrix} 3/5 \\ 4/5 \end{pmatrix}, w_2 = \begin{pmatrix} 4/5 \\ -3/5 \end{pmatrix}$.

Damit finden wir die orthogonale Matrix

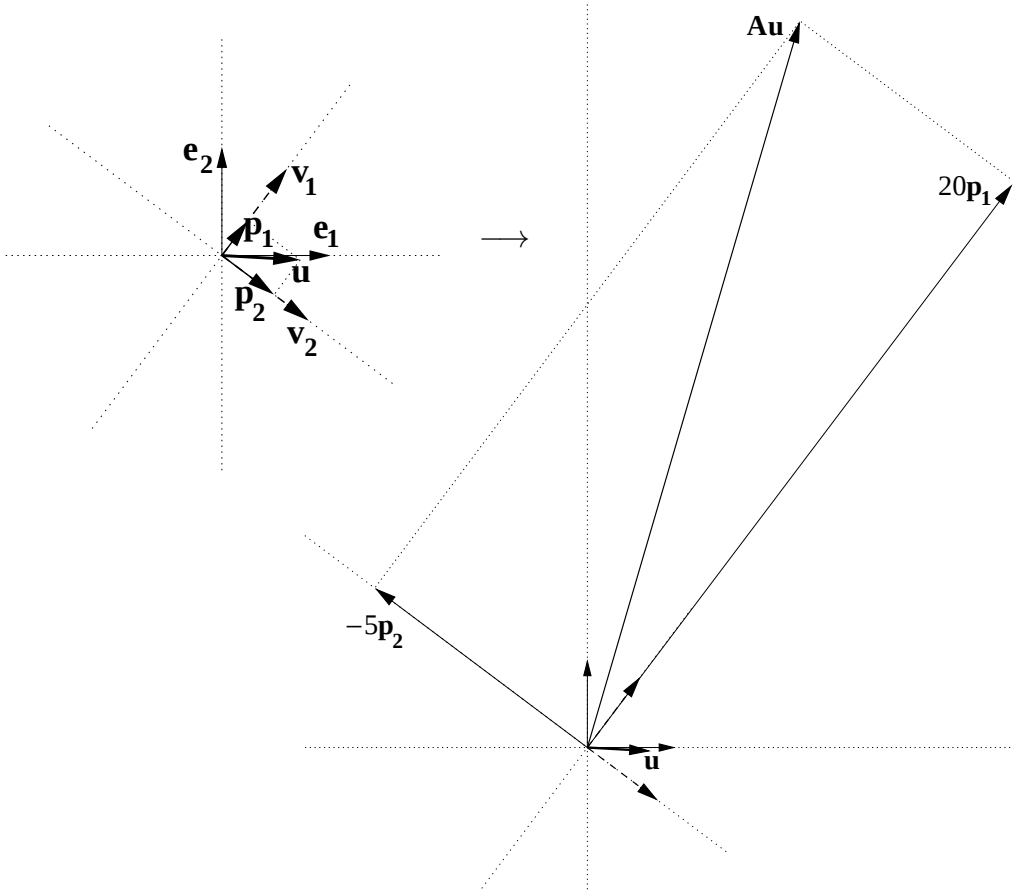
$$Q = \begin{pmatrix} 3/5 & 4/5 \\ 4/5 & -3/5 \end{pmatrix}$$

und berechnen

$$\begin{aligned} Q^{\mathrm{T}} A Q &= \frac{1}{25} \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix} \begin{pmatrix} 4 & 12 \\ 12 & 11 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix} \\ &= \frac{1}{25} \begin{pmatrix} 60 & 80 \\ -20 & 15 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix} = \frac{1}{25} \begin{pmatrix} 500 & 0 \\ 0 & -125 \end{pmatrix} \\ &= \begin{pmatrix} 20 & 0 \\ 0 & -5 \end{pmatrix} \\ &= \operatorname{diag}(\lambda_1, \lambda_2) \ , \end{aligned}$$

wie zu erwarten war.

Anwendung auf einen Vektor u:



u	gegebener Vektor
e_1, e_2	Standardbasisvektoren $e_1 = (1,0)^{\mathrm{T}}, e_2 = (0,1)^{\mathrm{T}}$
v_1, v_2	orthonormale Basisvektoren von A
p_1, p_2	Projektionen von u auf Hauptachsenrichtungen (entsprechen Darstellung von u bezüglich der Basis $\{v_1, v_2\}$)
$20p_1, -5p_2$	Ergebnis der Anwendung der Diagonalmatrix
Au	resultierender Vektor

46.6 Anwendung von Funktionen auf symmetrische Matrizen

Satz 45.15 über die Eigenwerte von Potenzen einer Matrix motiviert die folgenden Überlegungen:

- Ist $p(x) = a_m x^m + \ldots + a_1 x + a_0$ ein Polynom m-ten Grades, so kann man dieses direkt auf $n \times n$-Matrizen anwenden:

  $$p(A) = a_m A^m + \ldots + a_1 A + a_0 I \ .$$

  Aus Satz 45.15 folgt, dass alle A^k, $k = 0, \ldots, m$, dieselben Eigenvektoren wie A besitzen und die zugehörigen Eigenwerte die entsprechenden Potenzen der Eigenwerte von A sind.

  Ist damit λ ein Eigenwert zum Eigenvektor v von A, so gilt auch

  $$p(A)v = p(\lambda)v \ .$$

- Ist dabei A eine symmetrische Matrix, so kann sie dargestellt werden als

  $$A = \lambda_1 v_1 v_1^{\mathrm{T}} + \ldots + \lambda_n v_n v_n^{\mathrm{T}} \ ;$$

  entsprechend gilt auch

  $$p(A) = p(\lambda_1) v_1 v_1^{\mathrm{T}} + \ldots + p(\lambda_n) v_n v_n^{\mathrm{T}} \ .$$

- Über Potenzreihen (vgl. MfI 1) überträgt sich dieses Vorgehen auf beliebige analytische Funktionen $f : \mathbb{R} \to \mathbb{R}$ (also solche, die durch Potenzreihen darstellbar sind). Man hat dann allgemein

  $$f(A) = f(\lambda_1) v_1 v_1^{\mathrm{T}} + \ldots + f(\lambda_n) v_n v_n^{\mathrm{T}}$$

  für eine solche Funktion f.

- Sofern die Funktion auch für komplexe Argumente definiert ist, kann eine entsprechende Verallgemeinerung sogar für nichtsymmetrische diagonalisierbare Matrizen angegeben werden (wird hier nicht weiter behandelt).

Beispiel: Für

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

haben wir

$$\exp(A) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \mathrm{e}^a & 0 \\ 0 & \mathrm{e}^{-a} \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \frac{\mathrm{e}^a + \mathrm{e}^{-a}}{2} & \frac{-\mathrm{e}^a + \mathrm{e}^{-a}}{2} \\ \frac{-\mathrm{e}^a + \mathrm{e}^{-a}}{2} & \frac{\mathrm{e}^a + \mathrm{e}^{-a}}{2} \end{pmatrix} \ .$$