RWTH Aachen
WS 2001 / 02
Lineare Algebra I
Prof. Dr. G. Hiß

Mitschrift von Mark Wiesemann
www.mark-wiesemann.de

Stand: 10. Dezember 2007

Hinweise auf evt. Fehler bitte an
post@mark-wiesemann.de

Vorwort

Dieses Skript basiert auf meiner Mitschrift der Vorlesung Lineare Algebra I im WS 2001/02 an der RWTH Aachen (Dozent: Prof. Dr. G. Hiß). Es handelt sich nicht um eine offizielle Veröffentlichung des Lehrstuhls D für Mathematik.

Ich übernehme keine Gewähr für die Fehlerfreiheit und Vollständigkeit des Skripts. Korrekturen können an post@mark-wiesemann.de geschickt werden.

Die in diesem Skript verwendeten Grafiken wurden mir von Jens Liebchen zur Verfügung gestellt.

Mark Wiesemann, 10. Dezember 2007

Fun

Der Lehrstuhl hat nach der ersten Scheinklausur einige lustige Zitate veröffentlicht:

- φ hat offensichtlich eine lineare Beziehung zum Ursprung. Anders gesagt: Abbildung und Ursprung gleichen sich.
- Wir müssen von einem Ring-Gruppen-Homomorphismus sprechen.
- Es gilt: $A + A^t = 0$, da A^t auch als $(-A)^{-1}$ geschrieben werden kann.
- Jeder Ring ist ein Körper.
- linear überflüssig
- Wir sehen, dass die Abbildung nicht linear abhängig ist, also ist sie linear unabhängig.
- $\varphi(v_1) = \varphi(v_2)$, d.h. φ ist nicht injektiv und nicht bijektiv; vielleicht surjektiv.
- … sonst wäre φ injektiv und somit keine lineare Abbildung mehr.
- Da φ linear ist, liegen die Bilder von v_1 und v_2 also auch im Körper K, genauer: im Vektorraum W.
- die Löslichkeit des LGS
- Aufg. 11: Da für $\varphi : V \to W$ keine Abbildungsvorschrift vorliegt, kann φ frei gewählt werden.
- Jeder Wert läuft aufgrund der Def. wieder gegen sich.
- E ist Standardbasis von $\mathbb{Q}^{2\times 2}$.
- Seien $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ und $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ zwei beliebige Matrizen …
- $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ \frac{1}{3} & 0 \end{pmatrix} \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$, da $\frac{1}{3} \notin \mathbb{Q}$.
- Da in $\mathbb{F}_2$ lediglich eine Addition und eine Multiplikation definiert sind, ist ein Vorgehen nach dem Gauß-Algorithmus hier schwierig.

Inhaltsverzeichnis

1 Motivation und Grundlagen

§ 1 Mengen

Definition (Cantor)

Unter einer Menge verstehen wir jede Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

□

Probleme

- Zusammenfassung zu einem Ganzen?
- Führt zu Widersprüchen. □

Russel-Paradoxon

Sei M die Menge aller derjenigen Mengen, die sich nicht selbst als Objekt enthalten.
Frage: Ist M als Objekt in M enthalten?
Lösung: Jede Antwort führt zu einem Widerspruch.
Auflösung der Widersprüche: Axiomatische Mengenlehre (vgl. Logik-Vorlesungen). □

Unser Standpunkt

- Naive Mengenlehre (Cantors Definition, aber vorsichtig verwendet).
- Nur als Sprechweise verwendet. □

Arbeitsbasis

Eine Menge ist gebildet (existiert), wenn feststeht (klar ist), welche Objekte dazugehören.
Die Objekte, die in einer Menge M liegen, heißen ELEMENTE von M. Wir schreiben $x \in M$, falls x Element von M ist.
Sind M und M' Mengen, dann gilt:
$M = M' \Leftrightarrow$ jedes Element von M ist auch Element von M' und umgekehrt.

□

Schreibweisen

- AUFZÄHLUNG

  $\{1,3,17\} = \{3,1,17\} = \{1,3,17,3,1\}$

- BESCHREIBUNG

  $\mathbb{N} :=$ Menge der natürlichen Zahlen $= \{1,2,3,\ldots\}, 0 \notin \mathbb{N}$

  $\mathbb{Z} :=$ Menge der ganzen Zahlen $= \{\ldots,-2,-1,0,1,2,\ldots\}$

  $\mathbb{Q} :=$ Menge der rationalen Zahlen

  $\mathbb{R} :=$ Menge der reellen Zahlen

  ($\rightarrow$ Zahlbereichserweiterungen)

- AUSSONDERN

  M sei eine Menge, ε sei eine Eigenschaft (die ein x aus M hat oder nicht). Dann ist auch $\{x \in M \underbrace{\quad | \quad}_{\text{„für die gilt"}} x \text{ hat die Eigenschaft } \varepsilon\}$ eine Menge.

  Z.B.: $\{x \in \mathbb{Z} \mid x \text{ ist gerade}\} =$ Menge der geraden ganzen Zahlen. $\square$

(1.1) Definition

Seien M, N Mengen.

(a) $N \subseteq M :\Leftrightarrow$ [für alle $x \in N$ gilt: $x \in M$]

N ist TEILMENGE von M.

Es gilt: $M = N \Leftrightarrow [N \subseteq M \wedge M \subseteq N]$.

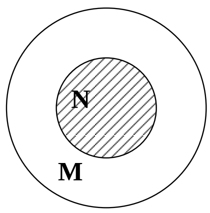

Abbildung 1.1: Teilmenge $N \subseteq M$

(b) $M \cap N := \{x \in M \mid x \in N\} = \{x \in N \mid x \in M\}$

DURCHSCHNITT von M und N

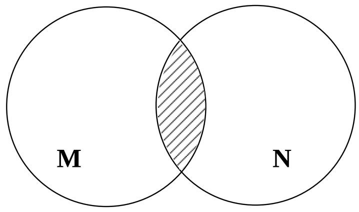

Abbildung 1.2: Durchschnitt $M \cap N$

(c) $M \cup N := \{x \mid x \in M \vee x \in N\}$
VEREINIGUNG von M und N

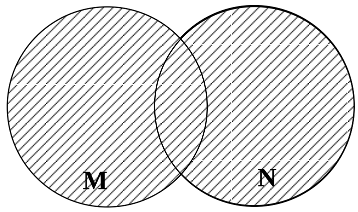

Abbildung 1.3: Vereinigung $M \cup N$

(d) $M \times N := \{(x,y) \mid x \in M \wedge y \in N\}$
KARTESISCHES PRODUKT von M und N
(x,y) ist GEORDNETES PAAR, d.h. $(x,y) = (x',y') \Leftrightarrow [x = x' \wedge y = y']$

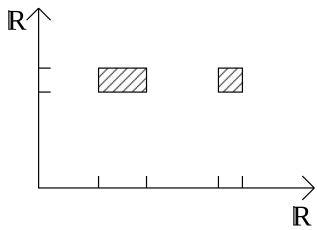

Abbildung 1.4: Kartesisches Produkt $M \times N$

(e) $\mathrm{Pot}(M) := \{X \mid X \subseteq M\}$
POTENZMENGE von M
Z.B. $M = \{1,2\}$: $\mathrm{Pot}(M) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
Allgemein gilt: Hat M n Elemente ($n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$), dann hat $\mathrm{Pot}(M)$ 2^n Elemente.

(f) $\emptyset$: LEERE MENGE (die Menge ohne Elemente)
$\emptyset \in M$ für alle Mengen M. □

Eine Menge M heißt ENDLICH, wenn M nur endlich viele Elemente hat.
Wir schreiben in diesem Fall:
$\mid M \mid :=$ Anzahl der Elemente von M.

Vollständige Induktion

Beweismethode, beruht auf:
(I) Sei $A \subseteq \mathbb{N}$. Dann gilt: Ist $1 \in A$ und ist für jedes Element $n \in A$ auch $n+1 \in A$, dann ist $A = \mathbb{N}$.
Behauptungen der Form „Für alle $n \in \mathbb{N}$ gilt $A(n)$." lassen sich nach folgendem Schema beweisen:
Induktionsanfang:
Zeige: $A(1)$ ist richtig.
Induktionsschritt:
Annahme: $A(n)$ ist richtig.
Zeige unter dieser Annahme: $A(n+1)$ ist richtig.
Dann gilt $A(n)$ für alle $n \in \mathbb{N}$, denn die Menge $A := \{n \in \mathbb{N} \mid A(n) \text{ ist richtig}\}$ erfüllt die Voraussetzungen von (I) und ist somit gleich $\mathbb{N}$. □

Beispiele

(a) Behauptung: Sei $x \in \mathbb{R}, x > -1$. Für alle $n \in \mathbb{N}$ gilt: $(1+x)^n \geq 1 + n \cdot x$.

Beweis: Induktion über n

Induktionsanfang:

$n = 1$: $1 + x \geq 1 + x$ ist richtig.

Induktionsschritt:

$n \to n+1$: Es gelte: $(1+x)^n \geq 1 + n \cdot x$.

$\Rightarrow (1+x)^{n+1} = (1+x) \cdot (1+x)^n \geq (1+x) \cdot (1 + n \cdot x)$.

[Begründung: $(1+x)^n \geq 1 + n \cdot x$ und $1 + x \geq 0$]

$= 1 + x + n \cdot x + n \cdot x^2 \geq 1 + x + n \cdot x$ (weil: $n \cdot x^2 \geq 0$)

$= 1 + (n+1) \cdot x$.

(b) Behauptung: Für alle $n \in \mathbb{N}$ gilt: $\sum\limits_{i=1}^{n} i = \frac{(n+\frac{1}{2})^2}{2}$.

Beweis: Induktion über n

Induktionsschritt:

$n \to n+1$:

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i \right) + n + 1 \underset{\text{Induktionsannahme}}{=} \frac{(n+\frac{1}{2})^2}{2} + n + 1 = \frac{n^2+n+\frac{1}{4}+2n+2}{2} = \frac{n^2+3n+\frac{9}{4}}{2} = \frac{((n+1)+\frac{1}{2})^2}{2}.$$

Fehler: Induktionsanfang fehlt, Formel ist für $n = 1$ falsch! □

§ 2 Abbildungen

(1.2) Definition

Seien M, N Mengen.
Eine ABBILDUNG f von M nach N ist eine VORSCHRIFT, die jedem $x \in M$ genau ein Element $f(x) \in N$ zuordnet. Schreibweise:
$f : M \to N, x \mapsto f(x)$
M heißt DEFINITIONSBEREICH von f, N heißt WERTEBEREICH von f. $x \in M$ heißt ein URBILD von $f(x) \in N$, $f(x) \in N$ heißt das BILD von $x \in M$. □

(1.3) Beispiele

(a) $f : \mathbb{N} \to \mathbb{R}, i \mapsto i^2$

Oft benutzen wir für FOLGEN (d.h. Abbildungen mit Definitionsbereich $\mathbb{N}$) die Schreibweise $a_1, a_2, a_3, \ldots, \underbrace{a_i}_{f(i)}, \ldots$, so dass unsere obige Abbildung geschrieben werden könnte als $1, 4, 9, 16, \ldots$

(b) Die Addition in $\mathbb{Z}$ ist Abbildung.

$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (x, y) \mapsto x + y$

(c) M Menge:

$\mathrm{id}_M : M \to M, x \mapsto x$ heißt die IDENTITÄT auf M. □

(1.4) Definition und Beispiele

Sei M eine Menge (z.B. $M = \mathbb{R}$).

(a) Für $n \in \mathbb{N}$ sei $\underline{n} := \{1, 2, \ldots, n\}$, z.B. $\underline{3} := \{1, 2, 3\}$.

(b) Ein n-TUPEL mit Werten in M ist eine Abbildung $t : \underline{n} \to M$.

Wie bei Folgen verwenden wir für n-Tupel t die Schreibweise $t_1, t_2, \ldots, t_n$, meist mit Klammern $(t_1, t_2, \ldots, t_n)$, wobei wir $t_i := t(i), i = 1, \ldots, n$ gesetzt haben.

Z.B.: $t : \underline{3} \to \mathbb{R}, t(1) = 0, t(2) = \sqrt{3}, t(3) = -\frac{1}{2}$ wird geschrieben als $(0, \sqrt{3}, -\frac{1}{2})$. □

(1.5) Definition

Sei $f : M \to N$ eine Abbildung.

(1) Für $X \subseteq M$ heißt $f(X) := \{f(x) \mid x \in X\} = \{y \in N \mid \text{es existiert ein } x \in X \text{ mit } y = f(x)\}$ das BILD von X.

(2) Für $Y \subseteq N$ heißt $f^{-1}(Y) := \{x \in M \mid f(x) \in Y\}$ das URBILD von Y.
[f^{-1} hat nichts mit der Umkehrabbildung zu tun.]
Die Mengen $f^{-1}(\{y\}) \subseteq M, y \in N$ heißen die FASERN von f.

(3) (a) f heißt SURJEKTIV, falls $f(M) = N$.

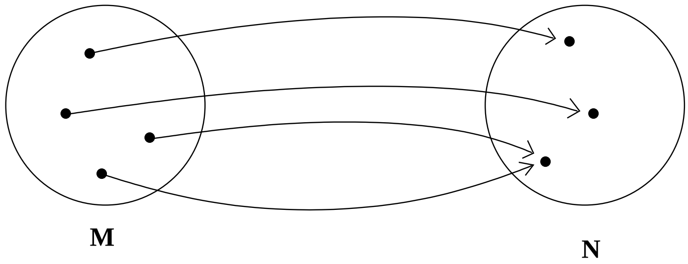

Abbildung 1.5: surjektive Abbildung

(b) f heißt INJEKTIV, falls gilt:
Sind $x, x' \in M$ mit $f(x) = f(x')$, dann ist $x = x'$.

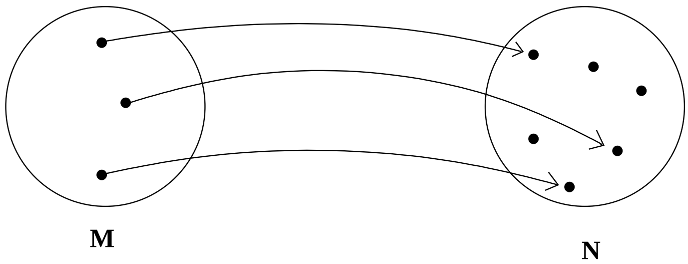

Abbildung 1.6: injektive Abbildung

(c) f heißt BIJEKTIV, falls f injektiv und surjektiv ist.

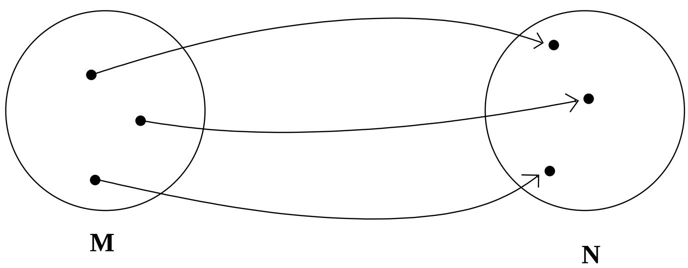

Abbildung 1.7: bijektive Abbildung

□

(1.6) Beispiele

(a) $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist bijektiv.

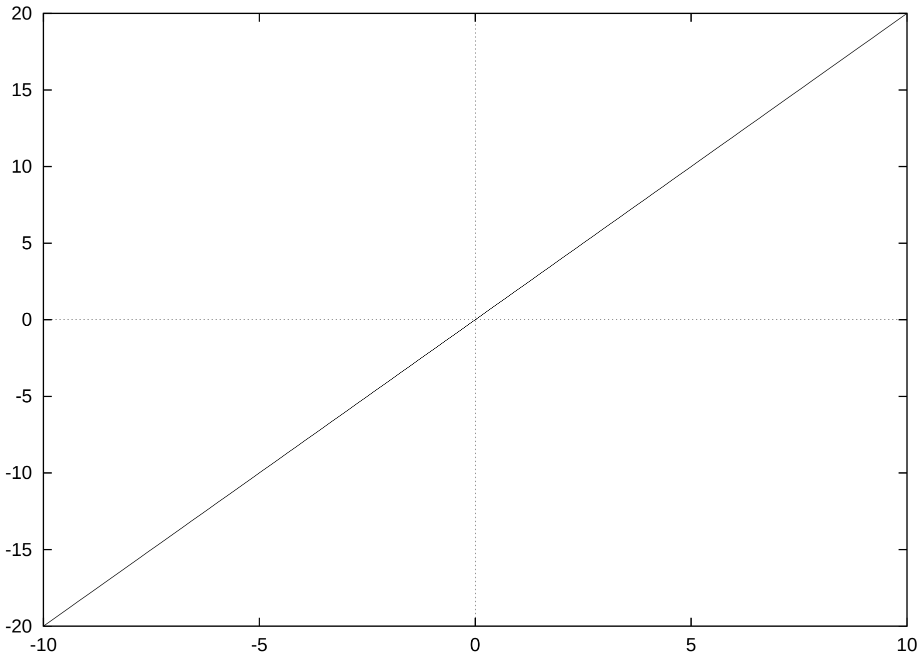

Abbildung 1.8: Abbildung $x \mapsto 2x$

(b) $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ (vgl. Abbildung 1.9) ist weder injektiv noch surjektiv.

f ist nicht injektiv, weil $-\sqrt{y}$ und $\sqrt{y}$ zwei verschiedene Urbilder sind.

f ist nicht surjektiv, weil die Bildmenge ungleich der Wertemenge ist:

$f(\mathbb{R}) = \mathbb{R}_{\geq 0} := \{x \in \mathbb{R} \mid x \geq 0\}$.

$f_1 : \mathbb{R} \to \mathbb{R}_{\geq 0}$ ist daher surjektiv (aber auch nicht injektiv).

Fasern von f_1: $f_1^{-1}(\{y\}) = \{-\sqrt{y}, \sqrt{y}\}, y \in \mathbb{R}_{\geq 0}$.

(c) $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto 2x$ ist injektiv, aber nicht surjektiv, weil z.B. 3 kein Urbild hat.

(d) $f : \mathbb{N} \to \{0, 1\}, x \mapsto$ Rest von x bei Division durch 2

$f^{-1}(\{0\}) = \{x \in \mathbb{N} \mid x \text{ ist gerade}\}$

$f^{-1}(\{1\}) = \{x \in \mathbb{N} \mid x \text{ ist ungerade}\}$

f hat genau zwei Fasern.

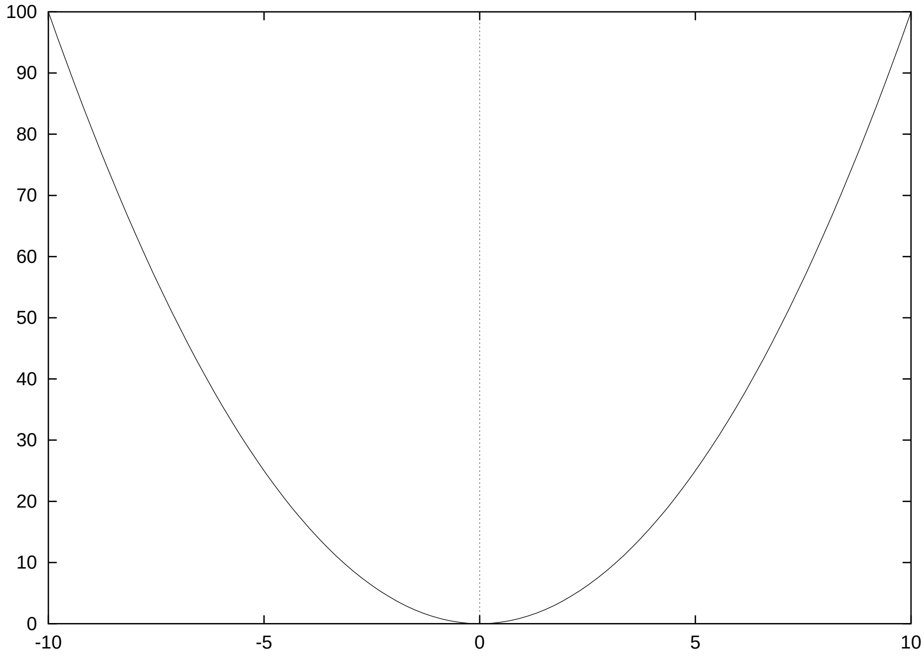

Abbildung 1.9: Abbildung $x \mapsto x^2$

(e) $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (x,y) \mapsto 2x + y$ (vgl. Abbildung 1.10)

Für $a \in \mathbb{R}$ gilt:

$$f^{-1}(\{a\}) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 2x + y = a\} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid \underbrace{y = -2x + a}_{\text{Gerade durch } y=a \text{ mit der Steigung } -2}\}$$

□

(1.7) Definition

Seien $f : M \to N$ und $g : L \to M$ Abbildungen.
Dann heißt die Abbildung $f \circ g : L \to N, x \mapsto f \circ g := f(g(x))$ die KOMPOSITION von f mit g (vgl. Abbildung 1.11). □

(1.8) Bemerkung

Sei $f : M \to N$. Dann gilt:
f bijektiv $\Leftrightarrow$ f besitzt eine UMKEHRABBILDUNG, d.h. es existiert $g : N \to M$ mit $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$.
Ist f bijektiv und g eine Umkehrabbildung von f wie oben, dann ist g durch f eindeutig bestimmt und wird mit f^{-1} bezeichnet. □

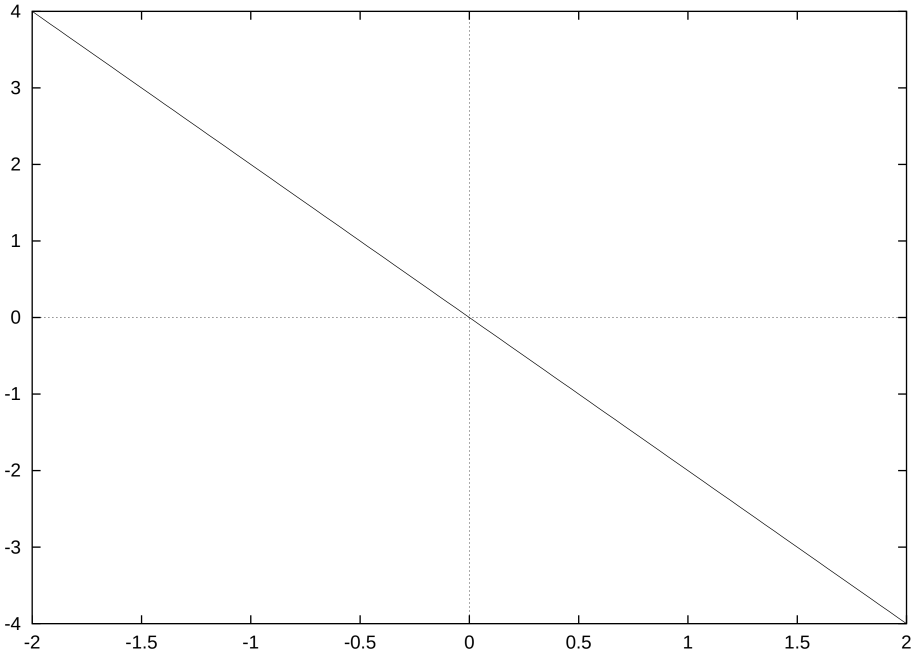

Abbildung 1.10: Abbildungen $f^{-1}(\{0\})$ und $f^{-1}(\{1\})$

$$\begin{tikzcd}
L \arrow[rr, "g"] \arrow[rr, bend left, mapsto, "g(x)"] \arrow[dr, "f\circ g"'] \arrow[dr, bend right, mapsto, "f\circ g(x)"'] & & M \arrow[dl, "f"] \arrow[dl, bend left, mapsto, "f(x)"] \\
& N &
\end{tikzcd}$$

Abbildung 1.11: Komposition von f mit g

Konvention

(1) Zu jeder Menge M existiert *genau eine* Abbildung, die die leere Menge auf M abbildet ($\emptyset \to M$).

(2) Ist $M \neq \emptyset$ eine Menge, dann existiert *keine* Abbildung von M in die leere Menge ($M \to \emptyset$).

[$\emptyset \to M$ ist injektiv; falls $M = \emptyset$, dann auch surjektiv.] $\square$

Ergänzung zu Definition (1.5)(3)

$f : M \to N$

(1) f ist SURJEKTIV, falls zu jedem $y \in N$ ein $x \in M$ existiert mit $f(x) = y$.

(2) f ist INJEKTIV, falls gilt:
Sind $x, x' \in M$ mit $x \neq x'$, dann ist $f(x) \neq f(x')$.

(3) f ist BIJEKTIV, falls f injektiv und surjektiv ist. □

(1.9) Beispiele

(a) $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist bijektiv.
$f^{-1} : \mathbb{R} \to \mathbb{R}, x \mapsto \frac{1}{2}x$ ist die Umkehrabbildung.

(b) $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$ ist bijektiv.
$f^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto \sqrt{x}$ ist die Umkehrabbildung.

□

§ 3 Lineare Gleichungssysteme und Matrizen

(1.10) Definition

Ein lineares Gleichungssystem (über $\mathbb{R}$), kurz LGS, hat die Form:

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

mit $a_{ij}, b_i \in \mathbb{R}, 1 \leq i \leq m, 1 \leq j \leq n$.
Die a_{ij} heißen die KOEFFIZIENTEN des LGS, $x_1, \ldots, x_n$ sind „UNBEKANNTE“.
Gegeben: a_{ij} und b_i.
Gesucht: Alle Lösungen des LGS.
Eine Lösung ist eine „Liste“ $s_1, \ldots, s_n$ mit $s_j \in \mathbb{R}, 1 \leq j \leq n$ (später als Spalte von Zahlen geschrieben), so dass alle m Gleichungen des LGS richtig werden (erfüllt sind), wenn $x_j = s_j$ gesetzt wird $(1 \leq j \leq n)$. □

(1.11) Bemerkung

Die Menge der Lösungen ändert sich nicht, wenn:

(a) zwei Gleichungen vertauscht werden,

(b) das c-fache ($c \in \mathbb{R}$) einer Gleichung zu einer anderen Gleichung addiert wird,

(c) eine Gleichung mit einem $c \in \mathbb{R}, c \neq 0$, multipliziert wird. □

Beweis

(a) Klar.

Seien $s_1, \ldots, s_n \in \mathbb{R}$.

(b) Linke Seiten der beiden Gleichungen nach Einsetzen von $s_1, \ldots, s_n$:

vor der Operation:	nach der Operation:
a_1	a_1
a_2	$a_2 + c \cdot a_1$

Rechte Seiten der bei beiden Gleichungen:

vor der Operation:	nach der Operation:
b_1	b_1
b_2	$b_2 + c \cdot b_1$

Zu zeigen: $a_1 = b_1 \wedge a_2 = b_2 \Leftrightarrow a_1 = b_1 \wedge a_2 + c \cdot a_1 = b_2 + c \cdot b_1$.

„$\Rightarrow$“: $a_1 = b_1 \Rightarrow c \cdot a_1 = c \cdot b_1 \underbrace{\Rightarrow}_{a_2 = b_2} a_2 + c \cdot a_1 = b_2 + c \cdot b_1$

„$\Leftarrow$“: $a_2 + c \cdot a_1 = b_2 + c \cdot b_1 \wedge c \cdot a_1 = c \cdot b_2 \Rightarrow a_2 = b_2$ (Subtraktion von $c \cdot a_1 = c \cdot b_2$)

(c) Linke Seiten:

vor der Operation:	nach der Operation:
a	$c \cdot a$

Rechte Seiten:

vor der Operation:	nach der Operation:
b	$c \cdot b$

Dies ist richtig, weil $c \neq 0$ ist. □

(1.12) Beispiele

(a)

$$\begin{aligned} x_1 + 2x_2 \qquad\quad + \ x_4 &= 1 \\ x_1 + 2x_2 + 2x_3 + 3x_4 &= 5 \\ 2x_1 + 4x_2 \qquad\quad + 3x_4 &= 5 \\ 3x_3 + 2x_4 &= 3 \end{aligned} \tag{$*$}$$

Addiere das (-1)-fache der 1. Gleichung zur 2. Gleichung, addiere das (-2)-fache der 1. Gleichung zur 3. Gleichung:

$$\begin{aligned} x_1 + 2x_2 \qquad + \ x_4 &= 1 \\ 2x_3 + 2x_4 &= 4 \\ x_4 &= 3 \\ 3x_3 + 2x_4 &= 3 \end{aligned}$$

Multipliziere die 2. Gleichung mit $\frac{1}{2}$, addiere das (-3)-fache der 2. Gleichung zur 4. Gleichung:

$$\begin{aligned} x_1 + 2x_2 \quad + \quad x_4 &= 1 \\ x_3 + \quad x_4 &= 2 \\ x_4 &= 3 \\ -x_4 &= -3 \end{aligned}$$

Addiere die 3. Gleichung zur 4. Gleichung, addiere das (-1)-fache der 3. Gleichung zur 2. Gleichung, addiere das (-1)-fache der 3. Gleichung zur 1. Gleichung:

$$\begin{aligned} x_1 + 2x_2 \qquad &= -2 \\ x_3 \quad &= -1 \\ x_4 &= 3 \\ 0 &= 0 \end{aligned} \tag{$**$}$$

Nach Bemerkung (1.11) haben die LGS $(*)$ und $(**)$ die gleichen Lösungen.

$$\begin{aligned} s_1, \ldots, s_4 \text{ ist Lösung von } (**) \Leftrightarrow & s_1 = -2 - 2a \\ & s_2 = a, a \in \mathbb{R} \text{ beliebig} \\ & s_3 = -1 \\ & s_4 = 3 \end{aligned}$$

Insbesondere hat $(*)$ unendliche viele Lösungen.

(b)

$$\begin{aligned} x_1 - \ x_2 &= 1 \\ 2x_1 + 3x_2 &= 0 \end{aligned}$$

Addiere das 2-fache der 1. Gleichung zur 2. Gleichung:

$$\begin{aligned} x_1 - \ x_2 &= 1 \\ 5x_2 &= -2 \end{aligned}$$

$$\begin{aligned} x_1 - x_2 &= 1 \\ x_2 &= -\frac{2}{5} \end{aligned}$$

$$\begin{aligned} x_1 \quad &= \frac{3}{5} \\ x_2 &= -\frac{2}{5} \end{aligned}$$

Es gibt genau eine Lösung: $\frac{3}{5}, -\frac{2}{5}$.

(c)

$$\begin{aligned} x_1 - \;\; x_2 &= 1 \\ -2x_1 + 2x_2 &= 0 \end{aligned}$$

Addiere das 2-fache der 1. Gleichung zur 2. Gleichung:

$$\begin{aligned} x_1 - x_2 &= 1 \\ 0 &= 2 \text{ ↯} \end{aligned}$$

Es gibt keine Lösung. □

Fazit

Ein LGS (mit $m = n$) kann also *unendlich viele*, *genau eine* oder *gar keine* Lösung haben. □

Fragen

(1) Wie sieht man den Koeffizienten eines LGS an, ob es unendlich viele, gar keine oder genau eine Lösung hat?

(2) Mathematisch Präzisierung des Begriffs „Lösung"?

(3) Hat die Menge der Lösungen eine „Struktur"? □

(1.13) **Beispiel** (aus der Elektrotechnik)

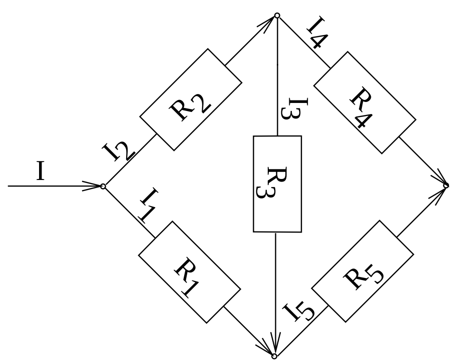

Abbildung 1.12: Netzwerk aus elektrischen Leitern und Widerständen

$I \in \mathbb{R}$: Strom des ein- und ausfließenden, gerichteten Stromes (in A).
$R_j \in \mathbb{R}, 1 \leq j \leq 5$: bekannte Widerstände (in Ω).
$I_j \in \mathbb{R}, 1 \leq j \leq 5$: gesuchte Stromstärken (in A).

KIRCHHOFF'SCHE GESETZE:

(a) Summe der Ströme in jedem Knoten ist 0.

(b) Summe der Spannungen in jeder Schleife ist 0.

$\Longrightarrow$ LGS:

$$\begin{array}{rcrcrcrcrcl}
 & & I_1 & + & I_2 & & & & & & = I \\
 & & & & I_2 & - & I_3 & - & I_4 & & = 0 \\
 & & I_1 & & & + & I_3 & & & - \; I_5 & = 0 \\
 & & & & & & & & I_4 & + \; I_5 & = I \\
 & - & R_1I_1 & + & R_2I_2 & + & R_3I_3 & & & & = 0 \\
 & & & & & - & R_3I_3 & + & R_4I_4 & - \; R_5I_5 & = 0
\end{array}$$

□

(1.14) Definition

Eine Menge K heißt KÖRPER (*field*), wenn zwei Abbildungen definiert sind:
$+: \quad K \times K \to K, (a,b) \mapsto a+b$
$\cdot: \quad K \times K \to K, (a,b) \mapsto a \cdot b$
so dass gilt:

(1) $(a+b)+c = a+(b+c)$ für alle $a,b \in K$.

(2) Es existiert $0 \in K$ mit $a+0 = 0+a = a$ für alle $a \in K$.

(3) Für alle $a \in K$ existiert $-a \in K$ mit $a+(-a) = 0 = -a+a$.

(4) $a+b = b+a$ für alle $a,b \in K$.

(5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a,b,c \in K$.

(6) Es existiert $1 \in K, 1 \neq 0$, mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in K$.

(7) Für alle $a \in K, a \neq 0$, existiert $a^{-1} \in K$ mit $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.

(8) $a \cdot b = b \cdot a$ für alle $a,b \in K$.

(9) $a \cdot (b+c) = a \cdot b + a \cdot c$ und $(a+b) \cdot c = a \cdot c + b \cdot c$ für alle $a,b,c \in K$. □

(1.15) Bemerkung

Sei K ein Körper.

(a) Für $a+(-b), a,b \in K$, schreiben wir $a-b$.

(b) Für $a \cdot b, a,b \in K$, schreiben wir ab. □

(1.16) Beispiele

(a) $\mathbb{R}$ und $\mathbb{Q}$ sind Körper. $\mathbb{Z}$ ist kein Körper.

(b) $\mathbb{Q}(\sqrt{3}) := \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ ist ein Körper (mit $+$ und $\cdot$ aus $\mathbb{R}$), Elemente des Körpers sind z.B. 1 $(1 = 1 + 0\sqrt{3})$, $\frac{13}{11}\sqrt{3}, -17 + \sqrt{3}$. Beweis:

$0, 1 \in \mathbb{R}$ liegen in $\mathbb{Q}(\sqrt{3})$; mit $a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ ist auch $-(a + b\sqrt{3}) = -a - b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$.

$\Rightarrow$ (1.14)(1)-(6),(8),(9) sind erfüllt für $\mathbb{Q}(\sqrt{3})$.

Was ist mit $(a + b\sqrt{3})^{-1}$ für $a + b\sqrt{3} \neq 0$?

$a + b\sqrt{3} \neq 0 \Rightarrow a^2 - 3b^2 \neq 0$ (dies liegt an der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$).

$\Rightarrow \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ und es gilt:

$\frac{1}{a^2-3b^2}(a - b\sqrt{3})(a + b\sqrt{3}) = \frac{1}{a^2-3b^2}(a^2 - 3b^2) = 1.$

Also ist $\mathbb{Q}(\sqrt{3})$ ein Körper. [(1.14)(7) gilt ebenfalls.]

(c) Wir definieren auf der Menge $\{0, 1\}$ eine neue Addition und eine neue Multiplikation (die wir auch mit $+$ und $\cdot$ bezeichnen) mit Hilfe der beiden folgenden Tafeln:

$+$	0	1
0	0	1
1	1	0

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

Dann ist $\{0, 1\}$ zusammen mit diesen neuen Verknüpfungen ein Körper, den wir mit $\mathbb{F}_2$ bezeichnen. ($\mathbb{F}$ steht für „field“, Index 2 für zwei Elemente.) □

(1.17) Definition

Sei K ein Körper, $m, n \in \mathbb{N}$.

(a) Eine $(m \times n)$-Matrix A über K ist ein rechteckiges „Schema“ von $m \cdot n$ Elementen $a_{ij} \in K$ der Form:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} =: (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}.$$

Die $a_{ij} \in K, 1 \leq i \leq m, 1 \leq j \leq n$, heißen die EINTRÄGE (oder KOEFFIZIENTEN) von A.

(b) $K^{m \times n} :=$ Menge der $(m \times n)$-Matrizen über K.

(c) Sei $A = (a_{ij}) \in K^{m \times n}$.

Die $(1 \times n)$-Matrix $z_i := \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}$ heißt die i-te ZEILE (*row*) von A.

Wir schreiben auch: $A = \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{pmatrix}$.

Die $(m \times 1)$-Matrix $s_j := \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ heißt die j-te SPALTE (*column*) von A.

Wir schreiben auch: $A = (s_1, s_2, \ldots, s_n)$. □

(1.18) Beispiel

$$A = \begin{pmatrix} 0 & 1 & -2 & 3 \\ \frac{5}{4} & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in \mathbb{Q}^{3\times 4}$$

Zeilen von A:

$z_1 = \begin{pmatrix} 0 & 1 & -2 & 3 \end{pmatrix}$

$z_2 = \begin{pmatrix} \frac{5}{4} & 1 & 0 & 0 \end{pmatrix}$

$z_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}$

Spalten von A:

$$s_1 = \begin{pmatrix} 0 \\ \frac{5}{4} \\ 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, s_3 = \begin{pmatrix} -2 \\ 0 \\ 3 \end{pmatrix}, s_4 = \begin{pmatrix} 3 \\ 0 \\ 4 \end{pmatrix}$$ □

Bemerkung

Mathematisch präzise Definition von Matrizen über K (K Körper):
Eine $(m \times n)$-Matrix A über K ist eine Abbildung

$$A : \underbrace{m}_{\{1,2,\ldots,m\}\in\mathbb{N}} \times n \to K,\ \underbrace{(i,j)}_{\text{Position}} \mapsto \underbrace{a_{ij}}_{\text{Eintrag der Matrix } A \text{ an der Position } a_{ij}}$$ □

Konventionen

(a) Eine $(1 \times n)$-Matrix oder eine $(n \times 1)$-Matrix über K nennen wir auch n-Tupel (vgl. (1.4)(b)).

(b) $K^n := K^{n\times 1}$ = Menge der SPALTEN-n-TUPEL über K.

$$\mathbb{R}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$$ □

(1.19) Definition

(a) Gegeben sei das LGS über K:

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

mit $a_{ij}, b_i \in K, 1 \leq i \leq m, 1 \leq j \leq n$.

Die Matrix $A = (a_{ij})_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \in K^{m\times n}$ heißt die KOEFFIZIENTEN-MATRIX des LGS.

$b := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m$ heißt RECHTE SEITE des LGS. Ist $b := \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$, dann heißt das LGS HOMOGEN, andernfalls INHOMOGEN.

Die Matrix $(A,b) \in K^{m\times(n+1)}$, d.h. $(A,b) = \begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ a_{21} & \cdots & a_{2n} & b_2 \\ & \vdots & & \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix}$, heißt die ERWEITERTE KOEFFIZIENTEN-MATRIX.

Eine LÖSUNG des LGS ist ein Element $\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \in K^n$ (also ein Spalten-n-Tupel) mit $\sum\limits_{j=1}^{n} a_{ij}s_j = b_i$ für alle $1 \leq i \leq m$.

Die LÖSUNGSMENGE L des LGS ist die Menge aller Lösungen; beachte: $L \subseteq K^n$.

(b) Eine Matrix $(A,b) \in K^{m\times(n+1)}$ mit $A \in K^{m\times n}, b \in K^n$ bestimmt umgekehrt ein LGS, dessen erweiterte Koeffizentenmatrix sie ist. □

(1.20) Beispiele

(a) Das LGS aus (1.13) hat folgende erweiterte Matrix:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & I \\ 0 & 1 & -1 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 1 & I \\ -R_1 & R_2 & R_3 & 0 & 0 & 0 \\ 0 & 0 & -R_3 & R_4 & -R_5 & 0 \end{pmatrix} \in \mathbb{R}^{6\times 6}.$$

(b) Die Lösungsmengen aus (1.12) sind:

$$\text{für (a):}\ L = \left\{ \begin{pmatrix} -2-2a \\ a \\ -1 \\ 3 \end{pmatrix} \mid a \in \mathbb{R} \right\} \subseteq \mathbb{R}^4$$

$$\text{für (b):}\ L = \left\{ \begin{pmatrix} \frac{3}{5} \\ -\frac{2}{5} \end{pmatrix} \right\} \subseteq \mathbb{R}^2$$

$$\text{für (c):}\ L = \emptyset \subseteq \underbrace{\mathbb{R}^2}_{\text{LGS mit 2 Unbekannten}}$$

(c) Betrachte das LGS über $\mathbb{R}$:

$2x_1 + x_2 = 3, m = 1, n = 2$

Definiere dazu eine Abbildung:

$\varphi : \mathbb{R}^2 \to \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto 2x_1 + x_2$

Dann gilt für die Lösungsmenge L:

$$L = \left\{ \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} \mid \underbrace{2s_1 + s_2 = 3}_{\varphi(\binom{x_1}{x_2})} \right\} = \varphi^{-1}(\{3\}), \text{ d.h. } L \text{ ist eine Faser von } \varphi.$$

(d) Allgemein: Sei K ein Körper, $A = (a_{ij}) \in K^{m \times n}$ die Matrix eines LGS mit rechter Seite $b \in K^m$.

Definiere: $\varphi_A : K^n \to K^m, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$ mit $y_i := \sum_{j=1}^{n} a_{ij} x_j, 1 \leq i \leq m.$

Dann ist $L := \varphi_A^{-1}(\{b\})$ die Lösungsmenge des LGS. □

§ 4 Gauß-Algorithmus

Sei K ein Körper, z.B. $\mathbb{R}$ oder $\mathbb{Q}$.

(1.21) Definition

Sei $A \in K^{m \times n}$.
Jede der folgenden drei Umformungen von A heißt ELEMENTARE ZEILENTRANSFORMATION:

(a) $t_{ij}\ (1 \leq i \neq j \leq m)$:

Vertausche die Zeilen i und j.

(b) $a_{ij}(c)$ $(1 \leq i \neq j \leq m, c \in K)$:

Addiere das c-fache von Zeile j zur Zeile i.

(c) $m_i(c)$ $(1 \leq i \leq m, c \in K, c \neq 0)$:

Multipliziere Zeile i mit c. □

(1.22) Beispiel

$K = \mathbb{Q}, m = 3, n = 4$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 1 \\ -1 & -1 & 5 & 6 \end{pmatrix} \xrightarrow[t_{12}]{} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ -1 & -1 & 5 & 6 \end{pmatrix} \xrightarrow[a_{23}(2)]{}$$

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ -1 & 0 & 13 & 16 \\ -1 & -1 & 5 & 6 \end{pmatrix} \xrightarrow[m_3(-1)]{} \begin{pmatrix} 0 & 0 & 1 & 1 \\ -1 & 0 & 13 & 16 \\ 1 & 1 & -5 & -6 \end{pmatrix}$$ □

(1.23) Bemerkung

Sei $(A,b) \in K^{m \times (n+1)}$ und sei (A',b') aus (A,b) durch eine Folge elementarer Zeilentransformationen entstanden. Dann haben die beiden LGS, deren erweiterte Matrix (A,b) bzw. (A',b') ist (vgl. (1.19)(b)), die gleichen Lösungsmengen.

Beweis

Folgt aus (1.11). □

(1.24) Definition

Eine Matrix (über K) hat ZEILENSTUFENFORM, wenn sie die folgende Gestalt hat:

$$\left(\begin{array}{c|ccccc} & \blacksquare & * & \cdots & \cdots & * \\ & 0 & \blacksquare & * & \cdots & * \\ 0 & \vdots & \vdots & \ddots & \ddots & \vdots \\ & 0 & \cdots & 0 & \blacksquare & * \\ \hline 0 & & & 0 & & \end{array}\right)$$

$\blacksquare$: ein Eintrag $\neq 0$.

$*$: irgendein Eintrag.

Links und unterhalb von $\blacksquare$ stehen nur Nullen. □

(1.25) Bemerkung (Gauß-Algorithmus mit Zeilentransformationen)

Jede Matrix über K kann durch eine endliche Folge elementarer Zeilentransformationen der Form (1.21)(a),(b) in eine Matrix in Zeilenstufenform überführt werden.

Beweis

A habe m Zeilen ($m \in \mathbb{N}$). Wir beweisen die Behauptung durch Induktion über m.
$\underline{m = 1:}$ ✓
$\underline{m-1 \to m:}$ Sei j_1 die Nummer der ersten Spalte von A, in der ein Eintrag $\neq 0$ vorkommt, sagen wir in Zeile i_1.
Durch Vertauschen von Zeilen (Zeile 1 mit Zeile i_1) erhalten wir:

$$\left(\begin{array}{c|c|ccc} & \blacksquare & * & \cdots & * \\ \cline{3-5} & * & & & \\ 0 & \vdots & & B & \\ & * & & & \end{array}\right)$$

Durch „Ausräumen" der Spalte j_1 mit elementaren Zeilentransformationen der Form $a_{i1}(c)$ mit geeigneten $c_i \in K$ erhalten wir:

$$\left(\begin{array}{c|c|ccc} & \blacksquare & * & \cdots & * \\ \cline{3-5} & 0 & & & \\ 0 & \vdots & & C & \\ & 0 & & & \end{array}\right)$$

C hat $(m-1)$ Zeilen.
Weitere Beweisschritte für die übrigen Zeilen analog. □

(1.26) Beispiel

$$A = \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ -1 & 2 & -1 & -3 & -6 \\ 1 & -2 & 5 & 4 & 1 \\ 2 & -4 & 4 & 8 & 5 \end{pmatrix} \in \mathbb{Q}^{4\times 5}$$

$$\begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 2 & 0 & -1 \\ 0 & 0 & -2 & 0 & 1 \end{pmatrix} \qquad (a_{21}(1), a_{31}(-1), a_{41}(-2))$$

$$\begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 1 & -3 \end{pmatrix} \qquad (a_{32}(-1), a_{42}(1))$$

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

(1.27) Algorithmus (Gauß'sches Verfahren zum Lösen eines homogenen LGS)

<u>Gegeben:</u> $A \in K^{m\times n}$, interpretiert als Koeffizienten-Matrix eines homogenen LGS.

<u>Gesucht:</u> Lösungsmenge L
Der Algorithmus besteht aus zwei Schritten:

(a) VORWÄRTSELIMINATION:

Bringe A mit Gauß-Algorithmus (vgl. (1.25)) auf Zeilenstufenform A', etwa:

$$A' = \left(\begin{array}{c|ccccc} & \blacksquare & * & \cdots & \cdots & * \\ & 0 & \blacksquare & * & \cdots & * \\ 0 & \vdots & \vdots & \ddots & \ddots & \vdots \\ & 0 & \cdots & 0 & \blacksquare & * \\ \hline 0 & & & 0 & & \end{array}\right)$$

(b) RÜCKWÄRTSSUBSTITUTION:

Die r Unbekannten an den $\blacksquare$-Spalten heißen ABHÄNGIGE VARIABLEN, die anderen $n-r$ heißen FREIE VARIABLEN.

(1) Bringe die freien Variablen auf die rechte Seite des LGS und ersetze diese der Reihe nach durch $a_1, \ldots, a_{n-r} \in K$ (beliebige Zahlen).

(2) Löse, von unten nach oben, nach den abhängigen Variablen auf. (Nach jedem dieser Schritte steht in der jeweils nächsten zu lösenden Gleichung genau eine abhängige Variable.) $\square$

(1.28) Beispiel (vgl. (1.26))

$$A' = \begin{pmatrix} \boxed{1} & -2 & 3 & 4 & 2 \\ 0 & 0 & \boxed{2} & 1 & -4 \\ 0 & 0 & 0 & \boxed{-1} & 3 \\ 0 & 0 & 0 & 0 & \end{pmatrix} \in \mathbb{Q}^{4\times 5}$$

x_2, x_5 sind freie Variablen.
x_1, x_3, x_4 sind abhängige Variablen.

$$\begin{aligned} x_1 - 2x_2 + 3x_3 + 4x_4 + 2x_5 &= 0 \\ 2x_3 + x_4 - 4x_5 &= 0 \\ -x_4 + 3x_5 &= 0 \end{aligned}$$

(b)(1) $\longrightarrow$

$$\begin{aligned} x_1 + 3x_3 + 4x_4 &= 2a_1 - 2a_2 \\ 2x_3 + x_4 &= 4a_2 \\ -x_4 &= -3a_2 \end{aligned}$$

(b)(2) $\longrightarrow$

$$\begin{aligned}
x_4 &= \phantom{2a_1-{}} 3a_2\\
x_3 &= \phantom{2a_1-{}} \frac{1}{2}a_2\\
x_1 &= 2a_1 - \frac{31}{2}a_2\\
x_2 &= a_1\\
x_5 &= \phantom{2a_1-{}} a_2
\end{aligned}$$

$$L = \left\{ \begin{pmatrix} 2a_1 - \frac{31}{2}a_2 \\ a_1 \\ \frac{1}{2}a_2 \\ 3a_2 \\ a_2 \end{pmatrix} \mid a_1, a_2 \in K \right\}. \qquad \square$$

(1.29) Bemerkung

(a) Ein homogenes LGS hat immer (mindestens) eine Lösung, nämlich $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in K^n$, diese Lösung heißt auch die TRIVALE LÖSUNG.

(b) Hat ein homogenes LGS weniger Gleichungen als Unbekannte ($m < n$), dann hat es eine NICHT-TRIVALE LÖSUNG.

Beweis

(a) ✓

(b) Die Anzahl der abhängigen Variablen (in der Zeilenstufenform des LGS) ist höchstens m, da in jeder Zeile höchstens ein $\blacksquare$ steht.

Anzahl der Unbekannten $= n > m \geq$ Anzahl der abhängigen Variablen.

$\Rightarrow$ Es existieren freie Variablen. $\square$

(1.30) Beispiel

Betrachte die chemische Reaktion $PbN_6 + CrMn_2O_8 \rightarrow Pb_3O_4 + Cr_2O_3 + MnO_2 + NO$.
PbN_6 : Bleiazid (x_1)
$CrMn_2O_8$: Chrompermanganat (x_2)
Pb_3O_4 : Bleioxid (x_3)
Cr_2O_3 : Chromoxid (x_4)
MnO_2 : Manganoxid (x_5)

NO : Stickoxid (x_6).

Gesucht:

Anzahl der Moleküle jeder Sorte, so dass jedes Atom auf beiden Seiten der Reaktion gleich oft vorkommt.

x_i : Anzahl des Moleküls i.

Für jedes der 5 vorkommenden Atome erhalten wir eine Gleichung.

	x_1	x_2	x_3	x_4	x_5	x_6
Pb	1	0	-3	0	0	0
N	6	0	0	0	0	-1
Cr	0	1	0	-2	0	0
Mn	0	2	0	0	-1	0
O	0	8	-4	-3	-2	-1

(Z.B. 1. Gleichung für Pb: $x_1 = 3x_3$ oder $x_1 - 3x_3 = 0$.)

Gauß-Algorithmus:

$$\begin{pmatrix} 1 & 0 & -3 & 0 & 0 & 0 \\ 0 & 0 & 18 & 0 & 0 & -1 \\ 0 & 1 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 4 & -1 & 0 \\ 0 & 0 & -4 & 13 & -2 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & -3 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 & 0 \\ 0 & 0 & -4 & 13 & -2 & -1 \\ 0 & 0 & 0 & 4 & -1 & 0 \\ 0 & 0 & 0 & \frac{117}{2} & -9 & -\frac{11}{2} \end{pmatrix} \longrightarrow$$

$$\begin{pmatrix} 1 & 0 & -3 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 & 0 \\ 0 & 0 & -4 & 13 & -2 & -1 \\ 0 & 0 & 0 & 4 & -1 & 0 \\ 0 & 0 & 0 & 0 & 45 & -44 \end{pmatrix}$$

Lösungsmenge:

$$L = \left\{ \begin{pmatrix} \frac{1}{6}a \\ \frac{22}{45}a \\ \frac{1}{18}a \\ \frac{11}{45}a \\ \frac{44}{45}a \\ a \end{pmatrix} \mid a \in \mathbb{R} \right\}$$

Welche Lösungen sind chemisch sinnvoll?

Alle $x_i \in \mathbb{N}$.

Kleinste solche Lösung für $a = 90$:

$$\begin{pmatrix} 15 \\ 44 \\ 5 \\ 22 \\ 88 \\ 90 \end{pmatrix}, \text{ d.h. } 15 \cdot PbN_6 + 44 \cdot CrMn_2O_8 \to 5 \cdot Pb_3O_4 + 22 \cdot Cr_2O_3 + 88 \cdot MnO_2 + 90 \cdot NO. \qquad \square$$

(1.31) Algorithmus (Gauß'sches Verfahren zum Lösen eines inhomogenen LGS)

Gegeben: $A \in K^{m \times n}$, $b \in K^m$, wobei $(A,b) \in K^{m \times (n+1)}$ als erweiterte Matrix eines inhomogenen LGS interpretiert wird (wobei wir $b \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ voraussetzen).

Gesucht: Lösungsmenge L

Der Algorithmus besteht aus drei Schritten:

(a) VORWÄRTSELIMINATION:

Bringe (A,b) mit Gauß-Algorithmus (vgl. (1.25)) auf Zeilenstufenform (A',b'), etwa:

$$\left(\begin{array}{c|ccccc|c} & \blacksquare & * & \cdots & \cdots & * & b'_1 \\ & 0 & \blacksquare & * & \cdots & * & b'_2 \\ 0 & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ & 0 & \cdots & 0 & \blacksquare & * & b'_r \\ \hline & & & & & & b'_{r+1} \\ 0 & & & 0 & & & \vdots \\ & & & & & & b'_m \end{array}\right)$$

(b) LÖSBARKEITSENTSCHEIDUNG:

Das LGS ist genau dann unlösbar, falls eine der Zahlen $b'_{r+1}, \ldots, b'_m$ ungleich 0 ist (in diesem Fall ist $L = \emptyset$).

Ist z.B. $b'_{r+1} \neq 0$, was wir nach Vertauschen von Zeilen annehmen können, dann liefert die $(r+1)$-te Gleichung den Widerspruch: $0 = 0 \cdot x_1 + 0 \cdot x_2 + \ldots + 0 \cdot x_n = b'_{r+1} \neq 0$ ↯.

(c) RÜCKWÄRTSSUBSTITUTION:

[Nur, falls $b'_{r+1} = b'_{r+2} = \ldots = b'_m = 0$.]

Abhängige und freie Variablen sind wie im homogenen Fall definiert.

(1) Ersetze alle freien Variablen durch 0 und löse nach den abhängigen Variablen auf (von unten nach oben).

$\rightarrow$ Erhalte spezielle Lösung $s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}$.

(2) Bestimmte die Lösungsmenge L_0 des homogenen LGS mit Matrix A'.

Dann gilt: $L = \{s + u \mid u \in L_0\} \subseteq K^n$.

Dabei haben wir zur Abkürzung gesetzt:

$$s+u := \begin{pmatrix} s_1+u_1 \\ s_2+u_2 \\ \vdots \\ s_n+u_n \end{pmatrix} \text{ für } u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} \in K^n. \qquad \square$$

(1.32) Beispiel

$$A = \begin{pmatrix} 1 & -2 & 3 & 4 \\ -1 & 2 & -1 & -3 \\ 1 & -2 & 5 & 4 \\ 2 & 4 & 4 & 8 \end{pmatrix} \in \mathbb{Q}^{4\times 4}, b = \begin{pmatrix} 2 \\ -6 \\ 1 \\ 5 \end{pmatrix} \in \mathbb{Q}^4.$$

$(A,b) \in \mathbb{Q}^{4\times 5}$ ist die Matrix A aus Beispiel (1.26).

$$\Rightarrow \left(\begin{array}{cccc|c} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \qquad (m=4, n=4)$$

$\Rightarrow$ Das LGS ist lösbar.

Freie Variable: x_2. Abhängige Variablen: x_1, x_3, x_4. Spezielle Lösung: $x_2 = 0$.

$$\begin{aligned} x_1 + 3x_3 + 4x_4 &= 2 \\ 2x_3 + x_4 &= -4 \\ -x_4 &= 3 \end{aligned}$$

$$\begin{aligned} \Rightarrow \quad x_4 &= -3 \\ x_3 &= -\frac{1}{2} \\ x_2 &= 0 \\ x_1 &= \frac{31}{2} \end{aligned}$$

$$\Rightarrow s = \begin{pmatrix} \frac{31}{2} \\ 0 \\ -\frac{1}{2} \\ -3 \end{pmatrix} \text{ ist eine spezielle Lösung.}$$

Lösungsmenge des homogenen LGS:

Ersetze x_2 durch $a \in \mathbb{Q}$:

$$\begin{aligned} x_1 + 3x_3 + 4x_4 &= 2a \\ 2x_3 + x_4 &= 0 \\ -x_4 &= 0 \end{aligned}$$

$$\Rightarrow \quad \begin{aligned} x_4 &= 0 \\ x_3 &= 0 \\ x_2 &= a \\ x_1 &= 2a \end{aligned}$$

$$\Rightarrow L_0 = \left\{ \begin{pmatrix} 2a \\ a \\ 0 \\ 0 \end{pmatrix} \mid a \in \mathbb{Q} \right\} \text{ ist eine spezielle Lösung.}$$

$$\Rightarrow L = \left\{ \begin{pmatrix} 2a + \frac{31}{2} \\ a \\ -\frac{1}{2} \\ -3 \end{pmatrix} \mid a \in \mathbb{Q} \right\} \subseteq \mathbb{Q}^4. \qquad \square$$

Einige Fragen

(1) Inwieweit sind die freien bzw. abhängigen Variablen durch das LGS bestimmt?

- Zeilenstufenform, auf die $A \in K^{m \times n}$ transformiert werden kann, ist nicht eindeutig durch A bestimmt.
- Vertauschen von Unbekannten liefert ein äquivalentes LGS, aber andere Menge von freien Variablen.

(2) Ist die Anzahl der freien Variablen eindeutig bestimmt? Wenn ja, warum?

(3) Lösungskriterium (für inhomogene LGS)?

Kriterium für die eindeutige Lösung?

(4) Kurze, kompakte Beschreibung der Lösungsmenge: $L = s + L_0 := \{s + u \mid u \in L_0\}$, L_0 Lösungsmenge des zugehörigen homogenen LGS (vgl. (1.31)(c$_2$)).

$L_0 : u, v \in L_0 \Rightarrow u + v \in L_0$ $\square$

§ 5 Äquivalenzrelationen

Sei M Menge.

(1.33) Definition

(a) Eine RELATION R auf M ist eine Teilmenge $R \subseteq M \times M$.

Schreibweise: $xRy :\Leftrightarrow (x, y) \in R$.

(b) Eine Relation $R \subseteq M \times M$ heißt:

(R) REFLEXIV, falls $(x,x) \in R$ für alle $x \in M$

(S) SYMMETRISCH, falls gilt:
$(x,y) \in R \Rightarrow (y,x) \in R$

(A) ANTISYMMETRISCH, falls gilt:
$(x,y) \in R$ und $(y,x) \in R \Rightarrow x = y$

(T) TRANSITIV, falls gilt:
$(x,y) \in R$ und $(y,z) \in R \Rightarrow (x,z) \in R$

(c) Eine Relation, die (R), (S) und (T) erfüllt, heißt ÄQUIVALENZRELATION.

(d) Eine Relation, die (R), (A) und (T) erfüllt, heißt (HALB-)ORDNUNG. □

(1.34) Beispiele

(a) Aus der Mathematik:

(1) $M = \mathbb{N}, R =$„$<$“ $(x < y :\Leftrightarrow y - x \in \mathbb{N})$
„$<$“ nicht reflexiv, nicht symmetrisch
„$<$“ transitiv

(2) $M = \mathbb{N}, R =$„$\leq$“ $(x \leq y :\Leftrightarrow x < y$ oder $x = y)$
„$\leq$“ ist (R), (A), (T)

(3) $M = \mathrm{Pot}(N)$ für eine Menge N
$R =$ „$\subseteq$“ ist (R), (A) und (T)
(„$\subseteq$“ ist keine TOTAL-ORDNUNG, d.h. nicht alle Elemente aus M sind vergleichbar bzgl. „$\subseteq$“, z.B. $\{1\}, \{2\} \in \mathrm{Pot}(\{1,2\})$, aber $\{1\} \nsubseteq \{2\}$ und $\{2\} \nsubseteq \{1\}$.)

(4) Sei N Menge, $f : M \to N$.
R_f definiert durch $xR_fx' :\Leftrightarrow f(x) = f(x')$ ist Äquivalenzrelation auf M.

(5) „$=$“ ist Äquivalenzrelation auf M (zu $R = \{(x,x) \mid x \in M\}$).

(6) $M = \mathbb{Z}$, „$\equiv_3$“ definiert durch $x \equiv_3 y :\Leftrightarrow 3 \mid x - y$ ist Äquivalenzrelation auf $\mathbb{Z}$.
[(T): $3 \mid x - y$ und $3 \mid y - z \Rightarrow 3 \mid x - y + y - z = x - z$]

(b) Aus dem täglichen Leben:

(1) $M =$ Menge der hier Anwesenden
$xEy :\Leftrightarrow x$ hat die gleichen Eltern (das gleiche Elternpaar) wie y
$xGy :\Leftrightarrow x$ hat das gleiche Geburtsdatum (Tag / Monat) wie y

(2) $M =$ Menge der Stichwörter in einem Lexikon
$xAy :\Leftrightarrow x$ hat den gleichen Anfangsbuchstaben (Großschreibung ignoriert) wie y

(3) $M =$ Menge von farbigen Glasperlen in einer Dose
$xFy :\Leftrightarrow x$ hat die gleiche Farbe wie y

E, G, A, F sind Äquivalenzrelationen. □

(1.35) Definition

Sei R eine Äquivalenzrelation auf M.
Für $x \in M$ heißt $C_x := \{y \in M \mid xRy\}$ eine ÄQUIVALENZKLASSE von R.
$M/R :=$ MENGE DER ÄQUIVALENZKLASSEN von R ($M/R \subseteq \mathrm{Pot}(M)$). □

(1.36) Beispiele

(a) R_f wie in (1.34)(a)(4), $f : M \to N$.

$xR_f x' \Leftrightarrow f(x') = f(x)$

$x \in M : C_x = \{x' \in M \mid f(x') = f(x)\} = \underbrace{f^{-1}(\{f(x)\})}_{\text{Faser}}$

M/R_f : Menge der nicht-leeren Fasern

(b) $R =$ „$=$“, $x \in M : C_x = \{x\}$

$M/R = \{\{x\} \mid x \in M\}$

(c) $M = \mathbb{Z}, R =$ „$\equiv_3$“

$x \equiv_3 y :\Leftrightarrow 3 \mid x - y$

$C_0 = \{y \in \mathbb{Z} \mid 3 \mid y\}$

$C_1 = \{y \in \mathbb{Z} \mid 3 \mid y - 1\} = \{y \in \mathbb{Z} \mid y = 3x + 1 \text{ für ein } x \in \mathbb{Z}\}$

$C_2 = \{y \in \mathbb{Z} \mid y = 3x + 2 \text{ für ein } x \in \mathbb{Z}\}$

Das sind alle Äquivalenzklassen bzgl. „$\equiv_3$“.

(d) M : Menge der Anwesenden

$R = E$ (gleiches Elternpaar)

Äquivalenzklasse: Geschwisterklasse

$R = G$ (gleiches Geburtsdatum)

$C_{\text{Hiß}} = \{a \mid a \text{ hat am 27.7. Geburtstag}\}$

(e) M : Stichwörter in einem Lexikon

$R = A$ (gleicher Anfangsbuchstabe)

$C_x = \{$ Wörter, die mit x oder mit X beginnen $\}$

(f) M : farbige Perlen

Äquivalenzklasse besteht aus einer Menge von Perlen gleicher Farbe. □

(1.37) Definition

Eine PARTITION von M ist eine Menge P von nicht-leeren Teilmengen von M, die TEILE von P, mit:

(a) $M = \bigcup_{C \in P} C$ mit $C = \{x \in M \mid \text{es existiert } C \in P \text{ mit } x \in C\}$

(b) Sind $C_1, C_2 \in P$ mit $C_1 \neq C_2$, dann ist $C_1 \cap C_2 = \emptyset$.

[$P \subseteq \mathrm{Pot}(M)$] □

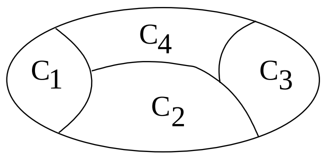

Abbildung 1.13: Partition $P = \{C_1, C_2, C_3, C_4\}$

(1.38) Bemerkung

(a) Sei R eine Äquivalenzrelation auf M. Dann gilt: M/R ist eine Partition von M.

(b) (Umkehrung von (a))

Sei P eine Partition von M. Dann existiert eine Äquivalenzrelation R auf M mit $M/R = P$.

Beweis

(a) Für $x \in M$ ist $x \in C_x$ (weil xRx gilt), also ist $C_x \neq \emptyset$.

Weiter gilt: $M = \bigcup_{x \in M} C_x$.

Seien $x, y \in M$ mit $C_x \cap C_y \neq \emptyset$.

Zu zeigen: $C_x = C_y$.

<u>Beweis:</u>

Sei $z \in C_x \cap C_y$.

$\Rightarrow xRz$ und yRz

$\Rightarrow xRz$ und zRy (wegen Symmetrie)

$\Rightarrow xRy$ (wegen Transitivität)

Sei nun $u \in C_x$ beliebig.

$\Rightarrow xRy$ und yRu (wegen Symmetrie)

$\Rightarrow xRu$ (wegen Transitivität)

$\Rightarrow u \in C_x$

Weil u beliebig war, folgt: $C_y \subseteq C_x$.

Analog: $C_x \subseteq C_y$.

$\Rightarrow C_x = C_y$.

(b) Sei P gegeben. Definiere $R \subseteq M \times M$ wie folgt:

$(x,y) \in R :\Leftrightarrow$ es existiert $C \in P$ mit $x \in C$ und $y \in C$.

Dann ist R eine Äquivalenzrelation auf M:

(R) Sei $x \in M$. Wegen (1.37)(a) existiert $C \in P$ mit $x \in C$. $\Rightarrow (x,x) \in R$.

(S) $(x,y) \in R \Rightarrow (y,x) \in R$

(T) Seien $x,y,z \in M$ mit $(x,y) \in R$ und $(y,x) \in R$.
$\Rightarrow$ Es existieren $C_1, C_2 \in P$ mit $(x \in C_1$ und $y \in C_1)$ und $(y \in C_2$ und $z \in C_2)$.
$y \in C_1 \cap C_2 \underset{(1.37)(b)}{\Rightarrow} C_1 = C_2 \Rightarrow (x,z) \in R$.

Die Äquivalenzklassen von R sind die Teile von P, d.h. $M/R = P$. Dazu zeige ich: Ist $x \in M$ und $C \in P$ mit $x \in C$, dann ist $C = C_1$. Dies ist aber klar. □

(1.39) Beispiele

(a) Sei N Menge und $f : M \to N$ eine Abbildung.

Die zu $R = R_f$ gehörige Partition ist die Menge M/R_f der nicht-leeren Fasern von f (vgl. Abbildung 1.14).

(b) M : Menge der Anwesenden

Die Partition zur Äquivalenzrelation G aus (1.34)(b)(1) ergibt sich aus der Abbildung $M \to \underline{31} \times \underline{12}, x \mapsto$ Geburtsdatum von x.

Die Teile der Partition bestehen aus der Teilmenge von Personen, die am gleichen Tag Geburtstag haben.

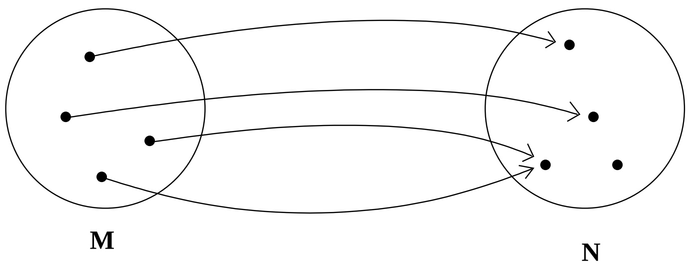

Abbildung 1.14: M/R_f

(c) M : Menge von farbigen Perlen

Die Partition zur Äquivalenzrelation F aus (1.34)(b)(3) ergibt sich auch aus der Abbildung $M \longrightarrow \{\text{Farben}\}, x \mapsto \text{Farbe}(x)$.

Teile der Partition: Menge von Perlen gleicher Farbe. $\square$

(1.40) Definition und Bemerkung

Sei R eine Äquivalenzrelation auf M. Die Abbildung $\pi : M \longrightarrow M/R, x \mapsto C_x$ heißt die zu R zugehörige KANONISCHE (NATÜRLICHE) ABBILDUNG. π ist surjektiv und ihre Fasern sind gerade die Äquivalenzklassen von R. $\square$

(1.41) Bemerkung

Sei N Menge und $f : M \longrightarrow N$ eine Abbildung.
R_f sei die Äquivalenzrelation aus (1.34)(a)(4) und $\pi : M \longrightarrow M/R_f$ die zugehörige kanonische Abbildung (vgl. (1.40)). Dann existiert die injektive Abbildung $\overline{f} : M/R_f \longrightarrow N$ mit $f = \overline{f} \circ \pi$.

$$\begin{tikzcd}
M \arrow[rr, "f"] \arrow[dr, "\pi"'] & & N \\
& M/R_f \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

Abbildung 1.15: Abbildung $\overline{f} : M/R_f \longrightarrow N$ mit $f = \overline{f} \circ \pi$

Beweis

Definiere $\overline{f} : M/R_f \longrightarrow N$ durch $f^{-1}(\{y\}) \mapsto y$ für $y \in f(M)$.
Beachte: $M/R_f = \{f^{-1}(\{y\}) \mid y \in f(M)\}$.

Dann gilt: $f = \overline{f} \circ \pi$:
Sei $x \in M$.
$\pi(x) = C_x = f^{-1}(\{f(x)\}) \Rightarrow \overline{f} \circ \pi(x) = \overline{f}(\pi(x))$, d.h. $f(x) = \overline{f} \circ \pi(x)$ für alle $x \in M$ und damit ist $f = \overline{f} \circ \pi$.
$\overline{f}$ ist injektiv:
Seien $C_x, C_{x'} \in M/R_f$ mit $\overline{f}(C_x) = \overline{f}(C_{x'})$.
$\Rightarrow f(x) = f(x')$, da $C_x = \pi(x), C_{x'} = \pi(x')$
$\Rightarrow C_x = f^{-1}(\{f(x)\}) = f^{-1}(\{f(x')\}) = C_x$. □

(1.42) Beispiel

M : Menge von farbigen Perlen
N : Menge von Farben
$f : M \to N, x \mapsto \text{Farbe}(x)$
Nicht-leere Fasern von f (Äquivalenzklassen von R_f):
Mengen von Perlen gleicher Farbe (Häufchen)
π : Jeder Perle wird ihr Farbhäufchen zugeordnet.
$\overline{f}$: Jedem Häufchen wird „seine" Farbe zugeordnet. □

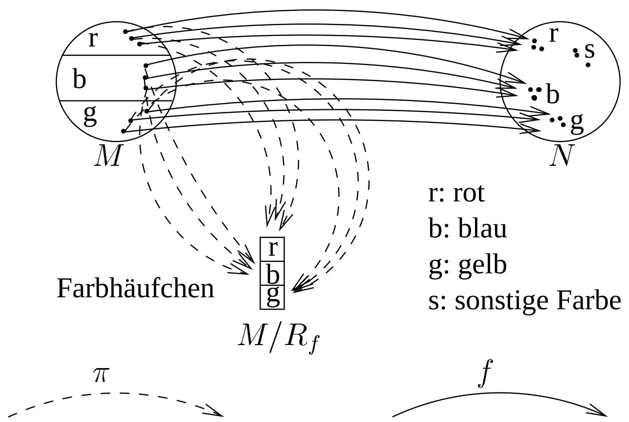

Abbildung 1.16: Perlen-Beispiel

2 Vektorräume und lineare Abbildungen

§ 1 Einige algebraische Strukturen

Eine VERKNÜPFUNG auf einer Menge M ist eine Abbildung $M \times M \to M$ (z.B. $+$, $\cdot$). Eine ALGEBRAISCHE STRUKTUR ist eine Menge M, auf der eine (oder mehrere Verknüpfung(en) definiert ist (sind).

(2.1) Definition

Eine Menge G heißt GRUPPE, wenn eine Verknüpfung $* : G \times G \to G$, $(x,y) \mapsto x * y$ definiert ist, so dass gilt:

(1) $(x * y) * z = x * (y * z)$ für alle $x, y, z \in G$.

(2) Es existiert $e \in G$ mit $e * x = x * e = x$ für alle $x \in G$.

(3) Für alle $x \in G$ existiert $x' \in G$ mit $x * x' = e = x' * x$.

Gilt zusätzlich:

(4) $x * y = y * x$ für alle $x, y \in G$, dann heißt G ABELSCH (KOMMUTATIV). □

(2.2) Bemerkungen

Sei $(G, *)$ eine Gruppe.

(a) Das Element e aus (2.1)(2) heißt *das* NEUTRALE ELEMENT von G (es ist eindeutig bestimmt).

(b) Sei $x \in G$. Das Element x' aus (2.1)(3) ist durch x eindeutig bestimmt. Es heißt *das* INVERSE ELEMENT.

(c) Ist G abelsch, dann schreiben wir oft $+$ für $*$, 0 für e und $-x$ für x' („ADDITIV").

(d) Oft schreiben wir G „MULTIPLIKATIV", d.h. $\cdot$ für $*$ (oder nichts), 1 für e und x^{-1} für x'. □

(2.3) Beispiele

(a) $(\mathbb{Z}, +)$ ist abelsche Gruppe.

(b) Sei K ein Körper. Dann gilt:

- $(K, +)$ ist abelsche Gruppe, die ADDITIVE GRUPPE von K.
- $(K^*, \cdot)$ ist abelsche Gruppe, die MULTIPLIKATIVE GRUPPE von K (hierbei ist $K^* = \{a \in K \mid a \neq 0\}$).

(c) Sei M Menge.

$S_M := \{f : M \to N \mid f \text{ ist bijektiv}\}$

S_M ist Gruppe mit der Verknüpfung „$\circ$":

<u>Klar:</u> $(f \circ g) \circ h = f \circ (g \circ h)$ für alle f, g, $h \in S_M$.

<u>Klar:</u> $f \circ g \in S_M$ für f, $g \in S_M$.

id_M ist das neutrale Elemente bzgl. „$\circ$".

Für $f \in S_M$ ist $f^{-1} \in M$ (hier ist f^{-1} die Umkehrabbildung aus (1.8)) das zu f inverse Element bzgl. „$\circ$".

(d) Spezialfall von (c): Sei $M := \underline{n} = \{1, 2, \dots, n\}$, $S_n := S_{\underline{n}}$ heißt die SYMMETRISCHE GRUPPE auf n Ziffern. Ein Element aus S_n heißt aus PERMUTATION. Für $\pi \in S_n$ schreiben wir oft:
$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$
Es gilt: $\mid S_n \mid = n! = 1 \cdot 2 \cdot 3 \cdots n$. Weiter gilt: S_n abelsch $\Leftrightarrow n \neq 2$.

Beweis

(d) „$\Leftarrow$": $n \leq 2 \Rightarrow \mid S_n \mid \in \{1, 2\} \Rightarrow S_n$ abelsch.

„$\Rightarrow$": Sei $n \geq 3$. Betrachte:

$$\psi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}, \psi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix}$$

$$\psi_1 \circ \psi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}, \psi_2 \circ \psi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{pmatrix}$$

$\Rightarrow \psi_1 \circ \psi_2 \neq \psi_2 \circ \psi_1$ $\square$

(2.4) Definition

Seien G und H Gruppen.
Eine Abbildung $\varphi : G \to H$ heißt (GRUPPEN-)HOMOMORPHISMUS, wenn gilt:
$\varphi(x \underbrace{\cdot}_{\cdot \in G} y) = \varphi(x) \underbrace{\cdot}_{\cdot \in H} \varphi(y)$ für alle $x, y \in G$.
Ein Homomorphismus $\varphi : G \to H$ heißt:

- MONOMORPHISMUS, wenn er *injektiv* ist,
- EPIMORPHISMUS, wenn er *surjektiv* ist,
- ISOMORPHISMUS, wenn er *bijektiv* ist.

G und H heißen ISOMORPH, falls ein Isomorphismus $\varphi : G \to H$ existiert; schreibe $G \cong H$. □

(2.5) Beispiele

(a) $(\mathbb{Z}, +) \to (\mathbb{R}, +), x \mapsto x$ ist ein Monomorphismus.

(b) $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), x \mapsto \exp(x) = e^x$ ist ein Isomorphismus.
[exp ist bijektiv, $e^{x+y} = e^x \cdot e^y, x, y \in \mathbb{R}$] □

(2.6) Definition

Sei $(G, \cdot)$ eine Gruppe, $U \subseteq G$.
U heißt UNTERGRUPPE von G, geschrieben $U \leq G$, falls U bzgl. der Verknüpfung $\cdot$ von G selbst eine Gruppe ist.
<u>Präziser:</u> Falls gilt: $u \cdot v \in U$ für alle $u, v \in U$.
Damit erhalten wir Verknüpfung auf U: $\cdot : U \times V \to U, (u, v) \mapsto u \underbrace{\cdot}_{\cdot \in G} v$.
U soll bzgl. dieser Verknüpfung eine Gruppe sein.

□

(2.7) Beispiele

(a) Für $n \in \mathbb{N}_0$ sei $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$.
Dann ist $n\mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$ $(n\mathbb{Z} \leq (\mathbb{Z}, +))$.
Jede Untergruppe von $(\mathbb{Z}, +)$ ist von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$.
[Konvention: $0\mathbb{Z} = \{0\}, 1\mathbb{Z} = \mathbb{Z}$]

(b) Sei $n \in \mathbb{N}, G = S_n, \{\pi \mid \underline{n} \to \underline{n}, \pi \text{ bijektiv}\}$.
$U = \{\pi \in G \mid \pi(n) = n\} \leq G$.
Es existiert ein Isomorphismus $S_{n-1} \to U$, d.h. $S_{n-1} \cong U$ (falls $n \geq 2$). □

(2.8) Konvention

Sei $(A,+)$ eine abelsche Gruppe, $a \in A$, U, $V \subseteq A$.
Dann schreiben wir:
$a+U := \{a+u \mid u \in U\} \subseteq A$
$U+V := \{u+v \mid u \in U, v \in V\} \subseteq A$
Beispiel:
$A = \mathbb{Z}, 1+7\mathbb{Z} = \{1+7\cdot z \mid z \in \mathbb{Z}\} = \{\dots,-13,-6,1,8,15,\dots\}$ □

(2.9) Beispiele

Sei $n \in \mathbb{N}$.

(a) Division durch n mit Rest:

Zu $x \in \mathbb{Z}$ existieren eindeutig bestimmte $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit $0 \leq r \leq n-1$ und $x = q \cdot n + r$.

Schreibweise: $x \bmod n := r$ (der nicht-negative Rest von x bei Division durch n).

Z.B. $n = 7$:

$21 \bmod 7 = 0, -3 \bmod 7 = 4, 17 \bmod 7 = 3$.

(b) Definition:

Für $x, y \in \mathbb{Z}$ schreiben wir:

$x \equiv y \pmod{n} :\Leftrightarrow x \bmod n = y \bmod n$.

Klar: $\equiv \pmod{n}$ ist Äquivalenzrelation.

Z.B. $n = 7$:

$-3 \equiv 32 \pmod{7}, 8 \equiv 1 \pmod{7}$.

(c) Bemerkung: (vgl. (1.34)(a)(6))

Für $x, y \in \mathbb{Z}$ gilt: $x \equiv y \pmod{n} \Leftrightarrow \underbrace{n \mid x-y}_{n \text{ ist Teiler von } x-y}$.

(d) Bemerkung: (vgl. (1.36)(c))

Sei $x \in \mathbb{Z}$ und C_x die Äquivalenzklasse von x bzgl. $\equiv \pmod{n}$. Dann gilt:

$C_x = x + n\mathbb{Z}$ (vgl. Konvention (2.8))

Beweis:

Sei $y \in \mathbb{Z}$. Dann gilt:

$$\begin{aligned} y \in C_x &\Leftrightarrow x \equiv y \,(\text{mod } n) \text{ (vgl. (b), (1.35))} \\ &\Leftrightarrow n \mid x - y \text{ (vgl. (c))} \\ &\Leftrightarrow \text{es existiert } q \in \mathbb{Z} \text{ mit } x - y = q \cdot n \\ &\Leftrightarrow \text{es existiert } z \in \mathbb{Z} \text{ mit } y = x + n \cdot z \\ &\Leftrightarrow y \in x + n\mathbb{Z} \text{ (vgl. Konvention (2.8))} \end{aligned}$$

(e) Bemerkung:

(1) Sei $x \in \mathbb{Z}$ und $r = x \bmod n$. Dann ist $x + n\mathbb{Z} = r + n\mathbb{Z}$.

(2) $\{\underbrace{n\mathbb{Z}}_{=0+n\mathbb{Z}}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$ ist die Menge der Äquivalenzklassen bzgl. $\equiv (\text{mod } n)$.
Sind $r, r' \in \{0, 1, \ldots, n-1\}, r \neq r'$, dann ist $r + n\mathbb{Z} \neq r' + n\mathbb{Z}$.

Beweis:

(1) Nach Definition von r gilt:
$n \mid x - r \Leftrightarrow x \equiv r \ (\text{mod } n) \underset{(d)}{\Rightarrow} x + n\mathbb{Z} = r + n\mathbb{Z}$.

(f) Schreibweise:

$\overline{x} := x + n\mathbb{Z}$ für $x \in \mathbb{Z}$.

$\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ = Menge der Äquivalenzklassen bzgl. $\equiv (\text{mod } n)$. Diese Äquivalenzklassen heißen auch RESTKLASSEN mod n.

(g) Beispiele:

(1) $n = 2:$
$\overline{0} = 2\mathbb{Z}$: Menge der geraden ganzen Zahlen
$\overline{1} = 1 + 2\mathbb{Z}$: Menge der ungeraden ganzen Zahlen

(2) $n = 7:$
$\overline{0}$: 7-er Reihe
$\overline{1}$: Menge derjenigen ganzen Zahlen, die bei Division durch 7 den Rest 1 haben
$\mathbb{Z}/7\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{6}\}$

(h) Bemerkung:

Für $x, y \in \mathbb{Z}$gilt:

$(x + n\mathbb{Z}) \underbrace{+}_{\text{Konvention (2.8)}} (y + n\mathbb{Z}) = (x + y) + n\mathbb{Z}$.

Beweis:
„$\subseteq$“: Für $z_1, z_2 \in \mathbb{Z}$ ist $(x+nz_1)+(y+nz_2) = (x+y)+n(z_1+z_2) \in (x+y)+n\mathbb{Z}$.
„$\supseteq$“: $(x+y)+n\mathbb{Z} = (x+0z)+(y+nz) \in (x+n\mathbb{Z})+(y+n\mathbb{Z})$.
Mit obiger Schreibweise (d.h. $\overline{x} = x+n\mathbb{Z}$) gilt also: $\overline{x}+\overline{y} = \overline{x+y}$.

(i) Bemerkung:
$\mathbb{Z}/n\mathbb{Z}$ mit der Verknüpfung $+$ aus (2.8) ist abelsche Gruppe mit genau n Elementen.
Die (kanonische) Abbildung $^{-}: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto \overline{x}$ ist ein surjektiver Gruppenhomorphismus.
Beweis:
Nach (h) gilt: $\overline{x}+\overline{y} = \overline{x+y} \in \mathbb{Z}/n\mathbb{Z}$ für $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$, d.h. $+$ ist eine Verknüpfung auf $\mathbb{Z}/n\mathbb{Z}$.
Die Gruppeneigenschaften werden mit Hilfe von (h) aus denjenigen für $\mathbb{Z}$ gefolgert:
Z.B. Assoziativgesetz:
$(\overline{x}+\overline{y})+\overline{z} = \overline{x+y}+\overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x}+\overline{y+z} = \overline{x}+(\overline{y}+\overline{z})$.
$\overline{0}$ ist das neutrale Element, $\overline{(-x)}$ ist das zu $\overline{x}$ inverse Element in $\mathbb{Z}/n\mathbb{Z}$.
$^{-}: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ist Homomorphismus nach (h) und surjektiv.
$(Z/n\mathbb{Z}, +)$ heißt die RESTKLASSENGRUPPE MODULO n.

(j) Rechnen in $\mathbb{Z}/n\mathbb{Z}$:
Z.B. für $n = 7$:
$\overline{6}+\overline{5} = \overline{6+5} = \overline{11} = \overline{4}$ (oder: $\overline{6}+\overline{5} = \overline{-1}+\overline{5} = \overline{4}$)
$\overline{3}-\overline{5} = \overline{3}+(-\overline{5}) = \overline{3}+\overline{-5} = \overline{3-5} = \overline{-2} = \overline{5}$ □

(2.10) (entfällt)

(2.11) Definition

Eine Menge R heißt RING, wenn auf R zwei Verknüpfungen $+: R \times R \to R$ und $\cdot: R \times R \to R$ definiert sind, so dass gilt:

(1) $(R, +)$ ist abelsche Gruppe.

(2) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle $x, y, z \in R$.

(3) Es existiert $1 \in R$ mit $1 \cdot x = x \cdot 1 = x$ für alle $x \in R$.

(4) Distributivgesetze:

(1) $x \cdot (y+z) = x \cdot y + x \cdot z$ für alle $x, y, z \in R$.
(2) $(x+y) \cdot z = x \cdot z + y \cdot z$ für alle $x, y, z \in R$.

Gilt zusätzlich:

(5) $x \cdot y = y \cdot x$ für alle $x, y \in R$, dann heißt R KOMMUTATIV. □

(2.12) Beispiele

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

(b) Körper sind kommutative Ringe. □

(2.13) Definition

Sei R ein Ring.

(a) Ein Element $x \in R$ heißt INVERTIERBAR (oder EINHEIT), wenn ein $x' \in R$ existiert mit $x \cdot x' = 1 = x' \cdot x$.

Ist $x \in R$ invertierbar, dann ist x' durch x eindeutig bestimmt und wir schreiben $x^{-1} = x'$.

$R^* :=$ Menge der Einheiten von R.

(b) Sei S ein Ring und $\varphi : R \to S$ eine Abbildung.

φ heißt RINGHOMOMORPHISMUS, wenn gilt:

(1) φ ist Gruppenhomomorphismus: $(R, +) \to (S, +)$.

(2) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ für alle $x, y \in R$ und $\varphi(1) = 1$. □

(2.14) Bemerkung und Beispiele

Sei R ein Ring.

(a) $(R^*, \cdot)$ ist eine Gruppe.

(b) Sei R kommutativ. Dann gilt:

R Körper $\Leftrightarrow R^* = \{x \in R \mid x \neq 0\}$ und $R^* \neq \emptyset$.

(c) $\mathbb{Z}^* = \{1, -1\}$.

Beweis

(a) Zu zeigen ist nur: $x_1, x_2 \in R^*$, dann auch x_1, x_2.

Dies gilt wegen $(x_1 \cdot x_2) \cdot (x_2^{-1} \cdot x_1^{-1}) = 1 = (x_2^{-1} \cdot x_1^{-1}) \cdot (x_1 \cdot x_2)$. □

(2.15) Beispiel (Fortsetzung von (2.9))

Sei $n \in \mathbb{N}$.

(a) Seien $x, x', y, y' \in \mathbb{Z}$ mit $\overline{x} = \overline{x'}$ und $\overline{y} = \overline{y'}$ ($\overline{x} = x + n\mathbb{Z}$), dann gilt: $\overline{x \cdot y} = \overline{x' \cdot y'}$.

Z.B. $n = 7$:

$x = 3, x' = -4, y = 1, y' = 8:$

$x \cdot y = 3, x' \cdot y' = -32 = 7 \cdot (-5) + 3$

(b) Definiere $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ durch $\overline{x} \cdot \overline{y} := \overline{x \cdot y}$.

Wegen (a) ist dies „wohldefiniert“, d.h. hängt nicht ab von der Repräsentanten $x' \in \overline{x}$ bzw. $y' \in \overline{y}$.

Zusammen mit $+$ aus (2.9) ist $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring mit Einselement $\overline{1}$ und $^{-} : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ist ein surjektiver Ringhomomorphismus.

(c) Einheiten in $\mathbb{Z}/n\mathbb{Z}$:

Bemerkung:

Für $x \in \mathbb{Z}$ gilt: $\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow \mathrm{ggT}(x,n) = 1$ (x und n sind teilerfremd).

Beweis:

„$\Rightarrow$“: (indirekt)

Angenommen, es existiert $d \neq 1, d \in \mathbb{N}$ mit $d \mid n$ und $d \mid x$.

$\Rightarrow$ Sei $n = d \cdot b$ für ein $b \in \mathbb{N}$.

$\Rightarrow 0 < b < m$, d.h. $\overline{b} \neq \overline{0}$.

Aus $n \mid b$ folgt: $\overline{x} \cdot \overline{b} = \overline{x \cdot b} = \overline{0}$.

$\overline{x} \in (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow$ es existiert $x' \in \mathbb{Z}$ mit $\overline{x'} \cdot \overline{x} = 1 \Rightarrow \overline{0} = \overline{x'} \cdot \overline{0} = \overline{x'} \cdot \overline{x} \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}$. ↯

„$\Leftarrow$“: Betrachte $l_{\overline{x}} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \overline{y} \mapsto \overline{x} \cdot \overline{y}$.

Zeige: $l_{\overline{x}}$ ist injektiv.

Dazu: Seien $\overline{y_1}$ und $\overline{y_2} \in \mathbb{Z}/n\mathbb{Z}$ mit $\overline{x} \cdot \overline{y_1} = \overline{x} \cdot \overline{y_2}$.

$\Rightarrow x \cdot (y_1 - y_2) \in n\mathbb{Z} \Rightarrow y_1 - y_2 \in n\mathbb{Z}$ (weil $\mathrm{ggT}(x,n) = 1$) $\Rightarrow \overline{y_1} = \overline{y_2}$.

$l_{\overline{x}}$ ist injektiv und $\mathbb{Z}/n\mathbb{Z}$ ist endlich.

$\Rightarrow l_{\overline{x}}$ ist bijektiv und damit surjektiv.

$\Rightarrow$ es existiert $\overline{y} \in \mathbb{Z}$ mit $\overline{x} \cdot \overline{y} = 1$

$\Rightarrow \overline{y} \cdot \overline{x} = 1$, also ist $\overline{y} = (\overline{x})^{-1}$, d.h. $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. □

(2.16) Korollar

Sei $n \geq 2$.
$\mathbb{Z}/n\mathbb{Z}$ ist Körper $\Leftrightarrow n$ ist Primzahl.

Beweis

$\mathbb{Z}/n\mathbb{Z}$ ist Körper.
$\underset{(2.14)(b)}{\Leftrightarrow}$ $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{1}, \ldots, \overline{n-1}\}$
$\underset{(2.15)(c)}{\Leftrightarrow}$ $\mathrm{ggT}(j,n) = 1$ für alle $1 \leq j \leq n-1$
$\Leftrightarrow$ n ist Primzahl. □

Bezeichnung

Sei p eine Primzahl.
$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ bezeichnet den endlichen Körper mit p Elementen. □

Bemerkung (Wie rechnen wir in $\mathbb{Z}/n\mathbb{Z}$?)

$\overline{r} + \overline{s} = \overline{r+s} = \overline{(r+s) \bmod n}$
$\overline{r} \cdot \overline{s} = \overline{r \cdot s} = \overline{(r \cdot s) \bmod n}$
Z.B. $n = 7$:
$\overline{6} \cdot \overline{5} = \overline{30} = \overline{2}$ oder: $\overline{6} \cdot \overline{5} = \overline{(-1) \cdot 5} = \overline{-5} = \overline{2}$
$\overline{6}^{1000000} = \overline{-1}^{1000000} = \overline{1}^{1000000} = \overline{1}$ □

(2.17) Beispiel (RSA-Kryptosystem / Public-Key-Verfahren)

Alice $\xrightarrow[\text{Nachricht}]{\text{geheime}}$ Bob

(1) Einrichten des Kryptosystems:

- Bob wählt (kauft) Primzahlen $p, q, p \neq q$, groß.
- Bob setzt $n := p \cdot g$.
- Bob wählt $a, b \in \mathbb{N}$ mit $1 \leq a, b \leq n-1$ mit $a \cdot b \bmod \varphi(n) = 1$.
  EULERSCHE φ-FUNKTION:
  $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| =$ Anzahl der Zahlen j, $1 \leq j \leq n-1$ mit $\mathrm{ggT}(j,n) = 1$.
  Hier: $\varphi(n) = \varphi(p \cdot q) = (p-1) \cdot (q-1)$.
  Mit anderen Worten:
  $a + \varphi(n)\mathbb{Z}$ und $b + \varphi(n)\mathbb{Z}$ sind zueinander invers in $\mathbb{Z}/n\mathbb{Z}$.
- Bob publiziert n und a.
- Bob behält b für sich.

(2) Verschlüsseln:

- Verschlüsselt werden Zahlen aus $\{0, 1, \ldots, n-1\}$.

- Verschlüsselung:
  $e_{n,a}$:{ 0, 1, ..., n - 1 }$\to${ 0, 1, ..., n - 1 },$x \mapsto x^a \bmod n$
  [Beachte: $\overline{x^a \bmod n} = \overline{x^a} = \overline{x}^a$ in $\mathbb{Z}/n\mathbb{Z}$.]

(3) Entschlüsseln:

- $d_{n,b} : \{0,1,\ldots,n-1\} \to \{0,1,\ldots,n-1\}, y \mapsto y^b \bmod n$
- Es gilt: $d_{n,b}(e_{n,a}(x)) = x$.
  [Denn: $(x^a \bmod n)^b \bmod n = x$.]

Z.B. $p = 3, q = 11$:
[In Anwendungen: p, q ca. 100-stellig.]
$n = p \cdot q = 33, \varphi(n) = (p-1)\cdot(q-1) = 2 \cdot 10 = 20$
$a = 3, b = 7; a \cdot b = 21, 21 \bmod 20 = 1$
Klartext: $x = 13$
Geheimtext: $x^a \bmod 33 = 13^3 \bmod 33$
$13^2 = 169 \equiv 4 (\bmod\ 33)$
$13^3 \equiv 13^2 \cdot 13 \equiv 4 \cdot 13 \equiv 52 \equiv 19 (\bmod\ 33)$
$\Rightarrow 13^3 \bmod 33 = 19$
$19^7 \bmod 33$:
$19 \equiv -14 (\bmod\ 33)$
$14^2 = 196 \equiv -2 (\bmod\ 33)$
$\Rightarrow 19^7 = (-14) \cdot (-2)^3 \equiv 14 \cdot 8 \equiv 112 \equiv 13 (\bmod\ 33)$
$[19^7 = 893871739]$ $\square$

Ab jetzt betrachten wir Matrizen über beliebigen kommutativen Ringen R.
$R^{m\times n}$: Menge der Matrizen $(a_{ij})_{\substack{1\le i\le m\\1\le j\le n}}$ mit $a_{ij} \in R$.

(2.18) Definition (Matrix-Arithmetik)

Sei R kommutativer Ring.

(a) Für $A = (a_{ij}) \in R^{m\times n}$ sei $A^t := (a_{ji})_{\substack{1\le j\le n\\1\le i\le m}} \in R^{n\times m}$.

A^t heißt die TRANSPONIERTE von A.

(b) SKALARE MULTIPLIKATION von A mit r:

Für $A = (a_{ij}) \in R^{m\times n}$ und $r \in R$ sei $r \cdot A := (r \cdot a_{ji})_{\substack{1\le i\le m\\1\le j\le n}} \in R^{m\times m}$.

(c) Für $A = (a_{ij}) \in R^{m\times n}$ und $B = (b_{ij}) \in R^{m\times n}$ sei $A+B := (a_{ij}+b_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in R^{m\times n}$ die SUMME von A und B.

(d) Für $A = (a_{ij}) \in R^{l\times m}$ und $B = (b_{ij}) \in R^{m\times n}$ sei $C := (c_{ij}) \in R^{l\times n}$ definiert durch:

$c_{ij} := \sum\limits_{k=1}^{m} a_{ik}b_{bj}, 1 \le i \le l, 1 \le j \le n.$

$C =: A\cdot B =: AB$ heißt das PRODUKT von A und B.

[AB ist nur definiert, falls die Anzahl der Spalten von A gleich der Anzahl der Zeilen von B ist.] □

(2.19) Beispiele

(a) $A = \begin{pmatrix} 0 & 1 & -2 & 3 \\ \frac{5}{4} & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in \mathbb{Q}^{3\times 4}, B = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \end{pmatrix} \in \mathbb{Q}^{3\times 4}$

(1) $A^t = \begin{pmatrix} 0 & \frac{5}{4} & 1 \\ 1 & 1 & 2 \\ -2 & 0 & 3 \\ 3 & 0 & 4 \end{pmatrix}$

(2) $4A = \begin{pmatrix} 0 & 4 & -8 & 12 \\ 5 & 4 & 0 & 0 \\ 4 & 8 & 12 & 16 \end{pmatrix}$

(3) $A+B = \begin{pmatrix} 0 & 2 & 0 & 6 \\ \frac{21}{4} & 6 & 6 & 7 \\ 9 & 11 & 13 & 15 \end{pmatrix}$

(b) $A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \in \mathbb{Q}^{3\times 4}, B = \begin{pmatrix} 1 & 4 \\ 2 & 3 \\ 3 & 2 \\ 4 & 1 \end{pmatrix} \in \mathbb{Q}^{4\times 2}$

(1) $AB = \begin{pmatrix} 20 & 10 \\ 3 & -3 \\ 3 & 7 \end{pmatrix}$

(2) BA ist nicht definiert

(3) $[(l\times m)\text{-Matrix}]\cdot[(m\times 1)\text{-Matrix}] \to [(l\times 1)\text{-Matrix}]$

A wie oben, $B' = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \Rightarrow A\cdot B' = \begin{pmatrix} 20 \\ 3 \\ 3 \end{pmatrix}$ [$\hat{=}$ 1. Spalte von AB]

(4) $[(1\times m)\text{-Matrix}]\cdot[(m\times n)\text{-Matrix}]\to[(1\times n)\text{-Matrix}]$
$A'=\begin{pmatrix} -1 & 0 & 0 & 1\end{pmatrix}$, B wie oben $\Rightarrow A'\cdot B=\begin{pmatrix} 3 & -3\end{pmatrix}$ [$\hat{=}$ 2. Zeile von AB]

(c) $(1\times m)$-Matrix: $(a_{11},a_{12},\ldots,a_{1m})$

$(m\times 1)$-Matrix: $\begin{pmatrix} b_{11}\\ b_{21}\\ \vdots\\ b_{m1}\end{pmatrix}$

Skalarprodukt: $(a_{11},a_{12},\ldots,a_{1m})\cdot\begin{pmatrix} b_{11}\\ b_{21}\\ \vdots\\ b_{m1}\end{pmatrix}=\sum\limits_{k=1}^{m}a_{1k}b_{k1}\in R^{1\times 1}$.

(d) Sei $A=\begin{pmatrix} z_1\\ \vdots\\ z_l\end{pmatrix}$ mit $z_i\in R^{1\times m}$, d.h. $A\in R^{l\times m}$, $B=(s_1,s_2,\ldots,s_n)$ mit $s_j\in R^m=R^{m\times 1}$, d.h. $B\in R^{m\times n}$ (vgl. (1.17)(c)), dann ist $AB=(z_i\cdot s_j)_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$.

(e) Sei $A=(a_{ij})\in R^{m\times n}, x=\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\in R^{n\times 1}$.

$$\Rightarrow Ax=\begin{pmatrix} \sum\limits_{j=1}^{n}a_{1j}x_j\\ \sum\limits_{j=1}^{n}a_{2j}x_j\\ \vdots\\ \sum\limits_{j=1}^{n}a_{mj}x_j\end{pmatrix}\in R^{m\times 1}$$

Deshalb schreiben wir ab jetzt ein LGS über einem Körper K mit Matrix $A=(a_{ij})\in K^{m\times n}$ und rechter Seite $b=\begin{pmatrix} b_1\\ \vdots\\ b_m\end{pmatrix}\in K^m$ formal als Matrixgleichung $Ax=b$ $(*)$ mit der Spalte $x=\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}$ der Unbekannten. Eine Lösung von $(*)$ ist ein Element $s\in K^n$ mit $As=b$. $\square$

(2.20) Definition

Sei R kommutativer Ring.

(a) $0 \in R^{m\times n}$ bezeichnet die NULLMATRIX, d.h. $0 = (a_{ij}) \in R^{m\times n}$ mit $a_{ij} = 0$ für alle $1 \leq i \leq m, 1 \leq j \leq n$.

(b) Für $n \in \mathbb{N}$ sei $E_n = (\delta_{ij})_{1\leq i,j\leq n} \in R^{n\times n}$ mit $\delta_{ij} = \begin{cases} 1 & \text{, falls } i = j \\ 0 & \text{, sonst} \end{cases}$.

E_n heißt die n-reihige EINHEITSMATRIX.

Beispiele:

(a) (1) $0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in R^{2\times 3}$

(2) $0 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \in R^3$

(b) (1) $E_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in R^{3\times 3}$

(2) $E_1 = \begin{pmatrix} 1 \end{pmatrix} \in R^{1\times 1}$ □

(2.21) Satz

Sei R kommutativer Ring.

(a) Für alle $A, B, C \in R^{m\times n}$ gilt:

(1) $(A+B)+C = A+(B+C)$

(2) $0+A = A = A+0$ $(0 \in R^{m\times n})$

(3) $A+(-1)A = 0 = (-1)A+A$ $(0 \in R^{m\times n})$

(4) $A+B = B+A$

(b) (1) $(AB)C = A(BC)$ für alle $A \in R^{l\times m}, B \in R^{m\times n}, C \in R^{n\times p}$

(2) $E_m A = A = AE_n$ für alle $A \in R^{m\times n}$

(3)
- $(A+B)C = AC+BC$ für alle $A, B \in R^{l\times m}, C \in R^{m\times n}$
- $A(B+C) = AB+AC$ für alle $A \in R^{l\times m}, B, C \in R^{m\times n}$

(4)
- $r(sA) = (rs)A$ für alle $r, s \in R, A \in R^{m\times n}$
- $r(AB) = (rA)B$ für alle $r \in R, A \in R^{l\times m}, B \in R^{m\times n}$

(c) (1) $(A^t)^t = A$ für alle $A \in R^{m\times n}$

(2) $(A+B)^t = A^t + B^t$ für alle $A, B \in R^{m\times n}$

(3) $(AB)^t = B^t A^t$ für alle $A \in R^{l\times m}, B \in R^{m\times n}$

Beweis

(a) Klar.

(b) (1) Beweis später.

(2) Die i-te Zeile von E_m ist $z_i = \begin{pmatrix} 0 & 0 & \cdots & 0 & \underbrace{1}_{\text{Position } i} & 0 & \cdots & 0 \end{pmatrix} \in R^{m\times n}$.

Ist $A = (a_{ij})$, dann ist die j-te Spalte von A gleich $s_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$

Offensichtlich gilt: $z_i \cdot s_j = (a_{ij}) \in R^{m\times n}$.

$\underset{(2.19)(d)}{\Rightarrow}$ $E_m A = A$. Analog: $AE_n = A$.

(3) Sei $A = (a_{ij}), B = (b_{ij}), C = (c_{ij})$.

Sei $D = A + B = (a_{ij} + b_{ij})_{\substack{1\le i\le l \\ 1\le j\le m}}$.

$\Rightarrow$ Der Eintrag an Position (i,j) von $(A+B)C = DC$ ist $\sum_{k=1}^{m} \underbrace{(a_{ik} b_{ik})}_{\text{Eintrag an Pos. } (i,k) \text{ von } D} c_{kj} = \sum_{k=1}^{m} a_{ik} c_{kj} + b_{ik} c_{kj}$ = Eintrag an Position (i,j) von AC + Eintrag an Position (i,j) von BC = Eintrag an Position (i,j) von $AC + BC$.

(2. Aussage analog.)

(4) Selbst überlegen.

(c) (1) Klar.

(2) Klar.

(3) Sei $A = (a_{ij}), B = (b_{ij})$.

$\Rightarrow A^* = (a'_{ij})$ mit $a'_{ij} = a_{ij}, B^* = (b'_{ij})$ mit $b'_{ij} = b_{ij}$

Eintrag an Position (i,j) von $(AB)^*$ = Eintrag an Position (i,j) von $AB = \sum_{k=1}^{m} a_{jk} b_{ki} = \sum_{k=1}^{m} b_{ki} a_{jk} = \sum_{k=1}^{m} b'_{ik} a'_{kj}$ = Eintrag an Position (i,j) von $B^* \cdot A^*$. $\square$

(2.22) Korollar

Sei $n \in \mathbb{N}$, R kommutativer Ring.
$\Rightarrow R^{n\times n}$ ist ein Ring (bzgl. Matrix-Addition und -Multiplikation).
Die neutralen Elemente sind 0 (bzgl. $+$) und E_n (bzgl. $\cdot$). $\square$

(2.23) Definition

Sei R kommutativer Ring, $n \in \mathbb{N}$.
$\mathrm{GL}_n(R) := \{A \in R^{n\times n} \mid A \text{ invertierbar}\} = (R^{n\times n})^*$ (vgl. (2.13)(a)).
$\mathrm{GL}_n(R)$ ist Gruppe, die volle lineare Gruppe über R. $\square$

(2.24) Bemerkung

R, n wie in (2.23). Dann gilt:
$A \in \mathrm{GL}_n(R) \Rightarrow A^* \in \mathrm{GL}_n(R)$ und $(A^*)^{-1} = (A^{-1})^*$.

Beweis

$A^*(A^{-1})^* = (A^{-1}\cdot A^*)^* = (E_n)^* = E_n$ und $(A^{-1})^* = (A \cdot A^{-1})^* = (E_n)^* = E_n \Rightarrow$ Behauptung $\square$

§ 2 Vektorräume

Sei K ein Körper.

(2.25) Definition

Ein K-VEKTORRAUM (Vektorraum über K) ist eine *abelsche Gruppe* $(V,+)$ zusammen mit einer *skalaren Multiplikation* $K \times V \to V$, $(a,v) \mapsto a \cdot v$, so dass gilt:

(V1)	$(a+b)\cdot v = a\cdot v + b \cdot v$	für alle $a,b \in K, v \in V$
(V2)	$a \cdot (v+v') = a\cdot v + a \cdot v'$	für alle $a \in K, v, v' \in V$
(V3)	$a\cdot(b\cdot v) = (a\cdot b)\cdot v$	für alle $a,b \in K, v \in V$
(V4)	$1 \cdot v = v$	für alle $v \in V$

Die Elemente eines K-Vektorraums heißen VEKTOREN. $\square$

(2.26) Bemerkung

Sei V ein K-VR. Dann gilt:

(a) $\underbrace{0}_{0\in(K,+)} \cdot V = \underbrace{0}_{0\in(V,+)}$ für alle $v \in V$ (0: NULLVEKTOR)

(b) $a \cdot \underbrace{0}_{\text{Null-}} = \underbrace{0}_{\text{vektor}}$ für alle $a \in K$

(c) $\underbrace{-v}_{\text{Inverse zu } v \text{ in } (V,+)} = \underbrace{(-1)}_{\text{Inverse zu } 1} \cdot v$ für alle $v \in V$

(d) $(-a) \cdot v = -(a \cdot v)$ für alle $a \in K, v \in V$

(e) Für $a \in K$ und $v \in V$ gilt:
$a \cdot v = 0 \Leftrightarrow a = 0$ oder $v = 0$

Beweis

Ähnlich wie die analogen Aussagen für Körper. □

(2.27) Beispiele

(a) $V = \{0\}$ ist K-VR, der TRIVIALE K-VEKTORRAUM.

(b) $(K,+)$ ist K-VR mit der skalaren Multiplikation $K \times K \to K, (a,b) \mapsto a \cdot b$.

(c) [aus LA] $K^{m \times n}$ ist K-VR (folgt aus (2.21)).

(d) [aus Analysis] $\mathbb{R}^{\mathbb{R}} := \{f \in \mathbb{R} \to \mathbb{R}\}$ ist $\mathbb{R}$-VR.
(Mit der üblichen Summe $f + g$ und den üblichen skalaren Vielfachen $r \cdot f$ von Funktionen.)
$C(\mathbb{R}) := \{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ stetig}\}$ ist $\mathbb{R}$-VR.
$C^\infty(\mathbb{R}) := \{f \in \mathbb{R}^{\mathbb{R}} \mid f \text{ ist beliebig oft differenzierbar}\}$ ist $\mathbb{R}$-VR.

(e) [aus Physik] Wellenfunktion

$$\left\{ \psi : \mathbb{R}^4 \to \mathbb{C} \mid \int_{\mathbb{R}^3} \underbrace{\mid \psi(\vec{x},t) \mid}_{\substack{\text{komplexer} \\ \text{Absolutbetrag}}}^2 d\vec{x} = 1 \right\} \text{ ist } \mathbb{C}\text{-VR.}$$

$\mathbb{C}$: Körper der komplexen Zahlen

$(\vec{x},t) : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ t \end{pmatrix} \in \mathbb{R}^4$

$\vec{x} := \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ Ortskoordinate

t: Zeitkoordinate

$\mathbb{R}^4$: „4“-dim.-Raum-Zeit-Kontinuum ($\mathbb{R}$-VR)

$\psi(\vec{x},t)$: Wellenfunktion eines Teilchens

$\mid \psi(\vec{x},t) \mid$: Wahrscheinlichkeitsdichte

$\int_Q \mid \psi(\vec{x},t) \mid^2 d\vec{x}$ ($q \subseteq \mathbb{R}^3$, Quader): Wahrscheinlichkeit, dass sich das Teilchen zur Zeit t im Quader Q befindet.

(f) [aus Informatik] Suchmaschine speichern (Term-Dokumente-Matrix)

Zeilen $\mathrel{\hat{=}}$ Terme $=$ Suchbegriffe, Spalten $\mathrel{\hat{=}}$ Dokumente (z.B. Web-Seiten)

Eintrag in der Zeile von T_i (Term Nr. i) und der Spalte zu D_j (Dokument Nr. j) $=$ Häufigkeit, mit der T_i in D_j vorkmmt.

Suchanfrage: Folge von Termen $T_{i1}, \dots, T_{in} \Rightarrow$ Suchvektor:

Spalte $s \in \mathbb{R}^m$ (m: Anzahl der zulässigen Terme) mit $s_j = \begin{cases} 1 & , j \in \{i_1, \dots, i_n\} \\ 0 & , \text{ sonst} \end{cases}$.

Gesucht wird nach Spalten der Term-Dokumente-Matrix, die „am Besten“ mit s übereinstimmt. □

(2.28) Definition

Sei V ein K-VR, $W \subseteq V$.
W heißt (K)-Untervektorraum (UVR) von V, geschrieben $W \leq V$, falls gilt:

(1) W ist Untergruppe von $(V, +)$

(2) $a \cdot w \in W$ für alle $a \in K, w \in W$ □

(2.29) Bemerkung

Sei V ein K-VR, $W \subseteq V$. Dann gilt:
$W \leq V \iff$

(UV1) $W \neq \emptyset$
(UV2) $w + w' \in W$ für alle $w, w' \in W$
(W ist abgeschlossen bzgl. $+$)
(UV3) $a \cdot w \in W$ für alle $a \in K, w \in W$
(W ist abgeschlossen bzgl. der skalaren Multiplikation)

Beweis

„$\Rightarrow$“: Klar.
„$\Leftarrow$“: Zu zeigen: W ist Untergruppe von $(V, +)$.
Wegen (UV2) ist $+ : W \times W \to W, (w, w') \mapsto \underbrace{w + w'}_{\text{Addition in } V}$ eine Verknüpfung auf W. Diese ist assoziativ.
Sei $w \in W$ (existiert nach (UV1)).
$\Rightarrow -w = (-1) \cdot w \in W$ ((UV3), (2.26)(c))
$\Rightarrow 0 = -w + w \in W$ (nach (UV2))
$\Rightarrow W$ ist Untergruppe von $(V, +)$. □

(2.30) Beispiele

(a) Sei V ein K-VR.

$\Rightarrow \{0\} \leq V, V \leq V$.

(b) Sei $W := \{(a_1, \ldots, a_n) \in K^{1\times n} \mid \sum\limits_{i=1}^{n} a_i = 0\}$.

$\Rightarrow W \leq K^{1\times n}$ (verwende (2.29)).

(c) $C^\infty(\mathbb{R}) \leq C(\mathbb{R}) \leq \mathbb{R}^{\mathbb{R}}$ (verwende (2.29)).

(d) $V = \mathbb{R}^2$ (EUKLIDISCHE EBENE)

Geraden durch $\binom{0}{0}$ sind UVR von V.

Geraden, die nicht durch $\binom{0}{0}$ gehen, sind keine UVR:

$\binom{0}{0}$ liegt in jedem UVR (trivialer UVR).

Eine Gerade durch $\binom{0}{0}$ hat die Gleichung $y = a \cdot x$ für ein $a \in \mathbb{R}$.

Sie ist also gleich $\{\binom{x}{a\cdot x} \mid x \in \mathbb{R}\} \leq \mathbb{R}^2$.

(e) Sei V K-VR, $W_1, W_2 \leq V$.

$\Rightarrow W_1 + W_2 \leq V (= \{w_1 + w_2 \mid w_i \in W_i\}$, Konvention (2.8)), außerdem gilt: $W_1 \cap W_2 \leq V$. $\square$

(2.31) Definition

Sei V ein K-VR.

(a) Sei $(v_1, \ldots, v_n)$ ein n-Tupel von Vektoren aus V, d.h. $v_i \in V$, $1 \leq i \leq n$.

Eine LINEARKOMBINATION (LK) von $(v_1, \ldots, v_n)$ ist ein Element $v \in V$ der Form $v = \sum\limits_{i=1}^{n} a_i v_i$ mit $a_i \in K$.

(b) Sei $\emptyset \neq M \subseteq V$. Wir setzen:

$< M >:= \{v \in V \mid$ es existieren $v_1, \ldots, v_n \in M$, so dass v eine LK von $(v_1, \ldots, v_n)$ ist$\}$

Menge aller Linearkombinationen von n-Tupeln aus M (n beliebig).

Ist $M = \emptyset$, dann setzen wir $< M >:= \{0\}$ (NULLVEKTORRAUM).

$< M >$ heißt das ERZEUGNIS von M in V. $\square$

(2.32) Satz

Sei V ein K-VR und $M \subseteq V$. Dann gilt:

(a) $< M > \leq V$

(b) Ist $W \leq V$ mit $M \subseteq W$, dann ist $< M > \leq W$.
($< M >$ ist der kleinste UVR von V, der M enthält.)

Beweis

(a) Wir überprüfen (UV1)-(UV3):
O.B.d.A. sei $M \neq 0$ (sonst ist (a) klar).

(UV1) $M \neq 0 \Rightarrow 0 \in < M >$ (als LK von $(v_1), v_1 \in M$)

(UV2) Seien $w, w' \in < M >$, etwa $w = \sum\limits_{i=1}^{m} a_i v_i, w' = \sum\limits_{i=1}^{n} a_i' v_i'$ mit $a_i, a_i' \in K, v_i, v_i' \in M$.

$\Rightarrow w + w' = \sum\limits_{i=1}^{m} a_i v_i + \sum\limits_{i=1}^{n} a_i' v_i'$ ist LK von $(v_1, \ldots, v_m, v_1', \ldots, v_n')$.

(UV3) Sei $w \in < M >, a \in K$.

$w = \sum\limits_{i=1}^{m} a_i v_i$ mit $a_i \in K, v_i \in M$.

$\Rightarrow a \cdot w = \sum\limits_{i=1}^{m} (a \cdot a_i) \cdot v_i$ ist LK von $(v_1, \ldots, v_m)$.

(b) Sei $W \leq V$ mit $M \subseteq W$.
Ist $M = \emptyset$, dann ist $< M > = \{0\} \leq W$. (wahr)
Sei also $M \neq \emptyset$ und $w = \sum\limits_{i=1}^{m} a_i v_i \in < M >$ mit $a_i \in K, v_i \in M$.

$\underset{M \subseteq W}{\Rightarrow} v_i \in W$ für alle $1 \leq i \leq m$.

$\underset{\text{(UV3),(UV2)}}{\Rightarrow} w = \sum\limits_{i=1}^{m} a_i v_i \in W$.

$\Rightarrow < M > \leq W$. □

(2.33) Beispiele

(a) $V = \mathbb{R}^3, v_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix}$

$\Rightarrow v_1 - 2 \cdot v_2 = \begin{pmatrix} 3 \\ 1 \\ -4 \end{pmatrix}$ ist LK von (v_1, v_2) und $v_1 + 2 \cdot v_2 = \begin{pmatrix} 0 \\ -2 \\ 2 \end{pmatrix}$ ist LK von (v_1, v_2).

$$< \{v_1, v_2\} >= \left\{ \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \mid a_i \in \mathbb{R}, \sum_{i=1}^{3} a_i = 0 \right\} \leq \mathbb{R}^3.$$

(b) Sei $A = (a_{ij}) \in K^{m \times n}$ mit Zeilen $z_1, \ldots, z_m \in K^{1 \times n}$ und Spalten $s_1, \ldots, s_n \in K^m$.

Sind $x_1, \ldots, x_n \in K$, dann ist $A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ eine LK von $(s_1, \ldots, s_n)$, nämlich:

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} x_i s_i.$$

Sind $y_1, \ldots, y_m \in K$, dann ist $(y_1, \ldots, y_m) \cdot A$ eine LK von $(z_1, \ldots, z_n)$, nämlich:

$$(y_1, \ldots, y_m) \cdot A = \sum_{i=1}^{m} y_i z_i.$$

$< \{z_1, \ldots, z_m\} > \leq K^{1 \times n}$ heißt der ZEILENRAUM von A.

$< \{s_1, \ldots, s_n\} > \leq K^m$ heißt der SPALTENRAUM von A.

Z.B.: $A = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 2 \\ 3 & 4 & 5 \\ 1 & -2 & 3 \end{pmatrix} \in \mathbb{R}^{4 \times 3}$

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

(2) $(1,1,1,1) \cdot A = 1 \cdot (-1,0,1) + 1 \cdot (0,1,2) + 1 \cdot (3,4,5) + 1 \cdot (1,-2,3) = (3,3,11)$

(c) $K = \mathbb{R}, V = C^\infty(\mathbb{R}), v_1 = \mathrm{id}_\mathbb{R}, v_2 = \sin$.

$< \{v_1, v_2\} >= \{a \cdot \mathrm{id}_\mathbb{R} + b \cdot \sin \mid a, b \in \mathbb{R}\}$

$a \cdot \mathrm{id}_\mathbb{R} + b \cdot \sin : \mathbb{R} \to \mathbb{R}, x \mapsto a \cdot x + b \cdot \sin(x)$ □

(2.34) ! Definition

Seien V, W K-VR, $\varphi : V \to W$.

(1) φ heißt LINEARE ABBILDUNG (K-HOMOMORPHIMUS), falls gilt:

(a) $\varphi(\underbrace{v + v'}_{\text{Addition auf } V}) = \underbrace{\varphi(v) + \varphi(v')}_{\text{Addition auf } W}$ für alle $v, v' \in V$.

(b) $\varphi(a \cdot v) = a \cdot \varphi(v)$ für alle $a \in K, v \in V$.

$\mathrm{Hom}_K(V,W) := \{\psi : V \to W \mid \psi \text{ linear}\}$.

(2) Für $W = V$ und φ linear heißt φ ein ENDOMORPHISMUS.
$\mathrm{End}_K(V) := \mathrm{Hom}_K(V,V)$.

(3) Sei φ linear. Dann heißt φ ein (vgl. (2.4)):

- MONOMORPHISMUS, falls φ *injektiv* ist
- EPIMORPHISMUS, falls φ *surjektiv* ist
- ISOMORPHISMUS, falls φ *bijektiv* ist

V und W heißen ISOMORPH, geschrieben $V \cong W$, falls ein Isomorphismus $\psi : V \to W$ existiert. □

(2.35) Beispiele

(a) $K = \mathbb{R}, V = \mathbb{R}^3, W = \mathbb{R}^2$.

$$\varphi_1 : V \to W, \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} a \\ b \end{pmatrix} \text{ ist linear.}$$

$$\varphi_2 : V \to W, \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} 1+a \\ b \end{pmatrix} \text{ ist nicht linear.}$$

$$\varphi_3 : V \to W, \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} a \\ b^2 \end{pmatrix} \text{ ist nicht linear.}$$

(b) $\varphi : K^{m\times n} \to K^{n\times m}, A \mapsto A^t$ ist ein Isomorphimus.

(c) $K = \mathbb{R}, V = \mathbb{R}^{\mathbb{R}}, r \in \mathbb{R}$.

$\varepsilon_r : V \to \mathbb{R}, f \mapsto f(r)$ ist $\mathbb{R}$-linear (AUSWERTUNGSHOMOMORPHISMUS).

$\varepsilon_r(f+g) : (f+g)(r) = f(r)+g(r) = \varepsilon_r(f)+\varepsilon_r(g)$, $\varepsilon_r(a\cdot f) : (a\cdot f)(r) = a\cdot f(r) = a\cdot\varepsilon_r(f)$ für alle $f,g \in \mathbb{R}^{\mathbb{R}}, a \in \mathbb{R}$.

(d) **!** Sei $A \in K^{m\times n}$.

$\varphi_A : K^n \to K^m, \varphi_A(x) := A\cdot x$ ist linear (vgl. (2.21)).

(e) $K = \mathbb{R}, V = C^\infty(\mathbb{R})$.

$\varphi : V \to W, f \mapsto f'$ (Ableitung) ist linear (Ableitungregel). □

(2.36) Definition

Sei V, W K-VR, $\varphi \in \mathrm{Hom}_K(V,W)$.

(a) $\mathrm{Kern}(\varphi) := \{v \in V \mid \varphi(v) = 0\}$, der KERN von φ.

(b) $\mathrm{Bild}(\varphi) := \{\varphi(v) \mid v \in V\}$, das BILD von φ.

$\mathrm{Kern}(\varphi) \subseteq V, \mathrm{Bild}(\varphi) \subseteq W$. □

(2.37) Bemerkung

(a) $\mathrm{Kern}(\varphi) \leq V$

(b) $\mathrm{Bild}(\varphi) \leq W$

(c) φ injektiv $\Leftrightarrow \mathrm{Kern}(\varphi) = \{0\}$

(d) φ surjektiv $\Leftrightarrow \mathrm{Bild}(\varphi) = W$

(e) Sei $v \in V$ und $w = \varphi(v)$.

$$\Rightarrow \underbrace{\varphi^{-1}(\{w\})}_{\text{eine Faser von } \varphi \text{ zu } w} = \underbrace{v + \mathrm{Kern}(\varphi)}_{\text{Konvention (2.8)}: \{v+v' \mid v' \in \mathrm{Kern}(\varphi)\}}$$

Beweis

(a) (UV1) $\varphi(0) = \varphi(0 \cdot v) = 0 \cdot \varphi(v) = 0 \Rightarrow 0 \in \mathrm{Kern}(\varphi)$.

(UV2) Seien $v, v' \in \mathrm{Kern}(\varphi)$. $\Rightarrow \varphi(v+v') = \varphi(v) + \varphi(v') = 0 + 0 = 0 \Rightarrow v + v' \in \mathrm{Kern}(\varphi)$.

(UV3) Seien $a \in K, v \in \mathrm{Kern}(\varphi)$. $\Rightarrow \varphi(a \cdot v) = a \cdot \varphi(v) = a \cdot 0 = 0 \Rightarrow a \cdot v \in \mathrm{Kern}(\varphi)$.

Aus (2.29) folgt: $\mathrm{Kern}(\varphi) \leq V$.

(b) (UV1) $0 = \varphi(0) \Rightarrow 0 \in \mathrm{Bild}(\varphi)$.

(UV2) Seien $w, w' \in \mathrm{Bild}(\varphi)$, etwa $w = \varphi(v)$ und $w' = \varphi(v')$ für $v, v' \in V$.
$\Rightarrow w + w' = \varphi(v) + \varphi(v') = \varphi(v + v') \Rightarrow w + w' \in \mathrm{Bild}(\varphi)$.

(UV3) Seien $a \in K, w \in \mathrm{Bild}(\varphi)$, etwa $w = \varphi(v)$ für ein $v \in V$.
$\Rightarrow a \cdot w = a \cdot \varphi(v) = \varphi(a \cdot v) \in \mathrm{Bild}(\varphi)$.

Aus (2.29) folgt: $\mathrm{Bild}(\varphi) \leq W$.

(c) „$\Rightarrow$“: Sei $v \in \mathrm{Kern}(\varphi)$. $\Rightarrow \varphi(v) = 0 = \varphi(0) \Rightarrow v = 0$, da φ injektiv.

„$\Leftarrow$“: Sei $\mathrm{Kern}(\varphi) = \{0\}$ und seien $v, v' \in V$ mit $\varphi(v) = \varphi(v')$.

$\Rightarrow 0 = \varphi(v) - \varphi(v') = \varphi(v - v') \Rightarrow v - v' \in \mathrm{Kern}(\varphi) = \{0\} \Rightarrow v = v'$.

(d) Klar.

(e) Zu zeigen: $\varphi^{-1}(\{w\}) = v + \text{Kern}(\varphi)$ (mit $v \in V$).

„$\supseteq$": Sei $u = v + v'$ mit $v' \in \text{Kern}(\varphi)$.

$\Rightarrow \varphi(u) = \varphi(v) + \varphi(v') = w + 0 = w$

$\Rightarrow u \in \varphi^{-1}(\{w\})$.

„$\subseteq$": Sei $u \in \varphi^{-1}(\{w\})$. Zu zeigen: $u = v + v'$ mit einem $v' \in \text{Kern}(\varphi)$.

Setze $v' = u - v$. $\Rightarrow \varphi(v') = \varphi(u - v) = \varphi(u) - \varphi(v) = w - w = 0$

$\Rightarrow v' \in \text{Kern}(\varphi)$, d.h. $u = v + v' \in v + \text{Kern}(\varphi)$. □

(2.38) Beispiele

(a) $K = \mathbb{R}, V = C^\infty(\mathbb{R})$

$\varphi : V \to V, f \mapsto f'$

φ ist surjektiv (Hauptsatz der Infinitesimalrechnung).

$\text{Kern}(\varphi) = \{f \in C^\infty(\mathbb{R}) \mid f \text{ ist konstant}\} \cong \mathbb{R}$.

(b) **!** Sei $A \in K^{m \times n}$, $b \in K^m$. Dann gilt:

(1) $\text{Kern}(\varphi_A) = \{c \in K^n \mid A \cdot c = 0\}$ ist die Lösungsmenge des homogenen LGS $Ax = 0$.

(2) Sei $c \in K^n$ die Lösung des LGS $Ax = b$. Dann ist die Lösungsmenge dieses LGS gleich $c + \text{Kern}(\varphi_A)$ (vgl. (1.31)(c)(2)).

(3) LÖSBARKEITSKRITERIUM: Die folgenden Aussagen sind äquivalent:

(i) $Ax = b$ ist lösbar

(ii) $b \in \text{Bild}(\varphi_A)$

(iii) $b \in$ Spaltenraum von A

(iv) Spaltenraum von A = Spaltenraum von (A, b)

Beweis

(a) s. Analysis

(b) (1) Klar.

(2) Die Lösungsmenge des LGS $Ax = b$ ist:
$\{c' \in K^n \mid \varphi_A(c') = b\} = \varphi_A^{-1}(\{b\}) = c + \text{Kern}(\varphi_A)$ (nach (2.37)(e)).

(3) Seien $s_1, \ldots, s_n \in K^m$ die Spalten von A.
(i) $\Rightarrow$ (ii): Trivial nach Definition von φ_A.
(ii) $\Rightarrow$ (iii): $b \in \text{Bild}(\varphi_A) \Rightarrow$ es existiert $c \in K^n$ mit $Ac = b$.

Sei $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ mit $c_i \in K$. $\underset{(2.33)(\text{b})}{\Rightarrow} A \cdot c = \sum_{i=1}^{n} c_i s_i$, d.h. $b \in$ Spaltenraum von A.

<u>(iii) ⇒ (iv):</u> b ist LK von $(s_1, \ldots, s_n) \Rightarrow$ Jede LK von $(s_1, \ldots, s_n)$ (d.h. der Spalten von (A, b)) ist auch LK von $(s_1, \ldots, s_n)$. ⇒ Behauptung.

<u>(iv) ⇒ (i):</u> $b \in$ Spaltenraum von $(A, b) =$ Spaltenraum von A

$\Rightarrow$ es existieren $c_1, \ldots, c_n \in K$ mit $b = \sum_{i=1}^{n} c_i b_i$

$$\underset{(2.33)(\text{b})}{\Rightarrow} A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = b, \text{ d.h. das LGS ist lösbar.}$$ □

§ 3 Basis und Dimension

Sei K ein Körper, V ein K-VR.

(2.39) ! Definition

(a) Ein n-Tupel $(v_1, \ldots, v_n)$ mit $v_i \in V$ heißt LINEAR ABHÄNGIG (l.a.), wenn $a_1, \ldots, a_n \in K$ existieren mit $(a_1, \ldots, a_n) \neq 0 \in K^{1 \times n}$ und $\sum_{i=1}^{n} a_i v_i = 0$.

Andernfalls heißt $(v_1, \ldots, v_n)$ LINEAR UNABHÄNGIG (l.u.).

(b) $M \subseteq V$ heißt LINEAR ABHÄNGIG (l.a.), wenn ein l.a. n-Tupel $(v_1, \ldots, v_n)$ existiert mit $v_i \neq v_j$ für $i \neq j$ und $v_i \in M$, $1 \leq i \leq m$.

Andernfalls heißt M LINEAR UNABHÄNGIG (l.u.).

<u>Konvention:</u> Insbesondere ist $\emptyset \subseteq V$ l.u. □

Schreibweise

$< v_1, \ldots, v_n > := < \{v_1, \ldots, v_n\} > = \sum_{i=1}^{n} a_i v_i$ mit $a_i \in K$. □

(2.40) Bemerkung

Sei $v_1, \ldots, v_n \in V$ und sei $M' \subseteq M \subseteq V$.

(a) (1) $0 \in M \Rightarrow M$ ist l.a.

(2) $M = \{v\}$ mit $v \neq 0 \Rightarrow M$ ist l.u.

(3) M' l.a. $\Rightarrow M$ l.a.

(4) M l.u. $\Rightarrow M'$ l.u.

(b) **!** $(v_1, \ldots, v_n)$ ist l.u. genau dann, wenn gilt:

Sind $a_1, \ldots, a_n \in K$ mit $\sum\limits_{i=1}^{n} a_i v_i = 0$, dann ist $a_1 = a_2 = \ldots = a_n = 0$.

[Der Nullvektor lässt sich also nur auf die triviale Weise aus $v_1, \ldots, v_n$ linear kombinieren.]

(c) Die folgenden Aussagen sind äquivalent:

(1) $(v_1, \ldots, v_n)$ l.a.

(2) Es existiert i_0, $1 \leq i_0 \leq n$ mit $v_{i_0} \in < v_1, \ldots, v_{i_0-1}, v_{i_0+1}, \ldots, v_n >$.

(3) Es existiert i_0, $1 \leq i_0 \leq n$ mit $< v_1, \ldots, v_n > = < v_1, \ldots, v_{i_0-1}, v_{i_0+1}, \ldots, v_n >$.

Beweis

(a) (1) Das 1-Tupel (0) ist l.a.

(2) Folgt aus (2.26)(e).

(3) Enthält M' ein l.a. n-Tupel von paarweise verschiedenen Vektoren, dann auch M.

(4) Ist die Umkehrung von (3).

(b) Ist die Negation von „$(v_1, \ldots, v_n)$ ist l.a.“.

(c) <u>(1) $\Rightarrow$ (2):</u> $(v_1, \ldots, v_n)$ l.a. $\Rightarrow$ es existiert $a_1, \ldots, a_n \in K$ mit $(a_1, \ldots, a_n) \neq 0$ und $\sum\limits_{i=1}^{n} a_i v_i = 0$.

Sei i_0 so, dass $a_{i_0} = 0$ ist.

$$\Rightarrow v_{i_0} = - \sum_{\substack{i=1 \\ i \neq i_0}}^{n} a_{i_0}^{-1} \cdot a_i \cdot v_i \in < v_1, \ldots, v_{i_0-1}, v_{i_0+1}, \ldots, v_n >.$$

<u>(2) $\Rightarrow$ (3):</u> $v_{i_0} \in < v_1, \ldots, v_{i_0-1}, v_{i_0+1}, \ldots, v_n >$, dann gilt:

$< v_1, \ldots, v_n > = < v_1, \ldots, v_{i_0-1}, v_{i_0+1}, \ldots, v_n >$.

<u>(3) $\Rightarrow$ (1):</u> $v_{i_0} \in < v_1, \ldots, v_n > = < v_1, \ldots, v_{i_0-1}, v_{i_0+1}, \ldots, v_n >$

$\Rightarrow$ es existiert $a_1, \ldots, a_{i_0-1}, a_{i_0+1}, \ldots, a_n \in K$ mit $\sum\limits_{\substack{i=1 \\ i \neq i_0}}^{n} a_i v_i = v_{i_0}$, d.h. $\sum\limits_{i=1}^{n} a_i v_i = 0$ mit $a_{i_0} = -1$.

$(a_1, \ldots, a_{i_0-1}, -1, a_{i_0+1}, \ldots, a_n) \neq 0 \Rightarrow (v_1, \ldots, v_n)$ ist l.a. $\square$

(2.41) Definition

$A \in K^{m \times n}$ hat SPALTENSTUFENFORM, wenn A^t Zeilenstufenform hat. $\square$

(2.42) Beispiele

(a) $V = \mathbb{Q}^2$

(1) $\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}\right)$ ist l.u., denn:

Seien $a_1, a_2 \in \mathbb{Q}$ mit $a_1 \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} + a_2 \cdot \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, also:

$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 3 \\ 0 & -2 \end{pmatrix}$ hat Zeilenstufenform.

$\Rightarrow$ Das homogene LGS mit Matrix $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ hat nur die triviale Lösung.

$\Rightarrow a_1 = a_2 = 0$.

(2) $\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 5 \\ 6 \end{pmatrix}\right)$ ist l.a., denn:

$-\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \begin{pmatrix} 3 \\ 4 \end{pmatrix} - \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

(b) **!** Sei $A \in K^{m \times n}$ eine Matrix in Zeilenstufenform und seien $z_1, \dots, z_r$ die von 0 verschiedenen Zeilen von A. Dann ist $(z_1, \dots, z_r)$ l.u.

Analog: Die von 0 verschiedenen Spalten einer Matrix in Spaltenstufenform sind l.u.

Insbesondere: Die Zeilen und Spalten von E_n sind l.u.

Beweis: Sei $z_i = (a_{i1}, \dots, a_{in})$, $1 \leq i \leq r$.

Für $1 \leq i \leq r$ sei a_{i,j_i} der erste von 0 verschiedene Eintrag in z_i. $\Rightarrow j_1 < j_2 < \dots < j_r$.

Seien $a_1, \dots, a_r \in K$ mit $\sum\limits_{i=1}^{r} a_i z_i = 0$.

$\Rightarrow a_1 \cdot a_{1,j_1} = 0$, d.h. $a_{i,j_i} = 0$ für $i = 1$.

$\Rightarrow a_1 = 0$, da $a_{1,j_1} \neq 0$

$\Rightarrow \sum\limits_{i=2}^{r} a_i z_i = 0$

$\Rightarrow a_i = 0$ für alle $2 \leq i \leq r$ (per Induktion)

Die zweite Aussage folgt aus der ersten durch Transponieren.

(c) $V = C^\infty(\mathbb{R})$, $K = \mathbb{R} \Rightarrow (\sin, \cos)$ ist l.u.

Beweis: Seien $a, b \in \mathbb{R}$ mit $a \cdot \sin + b \cdot \cos = 0$.

$\Rightarrow 0 = a \cdot \sin(0) + b \cdot \cos(0) = b$ und $0 = a \cdot \sin(\frac{\pi}{2}) + b \cdot \cos(\frac{\pi}{2}) = a$. $\square$

(2.43) Definition

Sei $M \subseteq V, v_1, \ldots, v_n \in V$.

(a) M heißt ERZEUGENDENSYSTEM von V, wenn $V = < M >$ ist.

(b) V heißt ENDLICH ERZEUGT (e.e.), wenn V ein endliches Erzeugendensystem besitzt.

(c) **!** M heißt BASIS von V, wenn M ein l.u. Erzeugendensystem ist.

$(v_1, \ldots, v_n)$ heißt GEORDNETE BASIS von V, wenn $v_i \neq v_j$ für $i \neq j$ und wenn $\{v_1, \ldots, v_n\}$ eine Basis ist. □

(2.44) Beispiele

(a) $\emptyset$ ist Basis von $\{0\}$. (Konvention)

(b) $V = K^m$. Für $1 \leq i \leq m$ sei $e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow \text{Position } i. \\ \\ \\ \\ \end{array}$

$\Rightarrow (e_1, \ldots, e_m)$ ist geordnete Basis von M, die STANDARDBASIS.

(c) $V = K^{m \times n}$. Für $1 \leq i \leq m$, $1 \leq j \leq n$ sei $E_{i,j} \in K^{m \times n}$ die Matrix mit Eintrag i an Position (i, j) und Nullen sonst, z.B.:

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$\Rightarrow (E_{1,1}, \ldots, E_{1,n}, E_{2,1}, \ldots, E_{2,n}, E_{3,1}, \ldots, E_{m,n})$ ist eine geordnete Basis von $K^{m \times n}$. □

(2.45) ! Satz (Charakterisierung von Basen)

Für $M \subseteq V$ sind folgende Aussagen äquivalent:

(1) M ist Basis von V.

(2) M ist eine maximale l.u. Teilmenge von V.

(D.h.: M ist l.u. und ist $M \subsetneqq M' \subseteq V$, dann ist M' l.a.)

(3) M ist ein minimales Erzeugendensystem von V.

(D.h.: $< M > = V$ und $< M' > \neq V$ für alle $M' \subsetneqq M$.)

Beweis

(1) $\Rightarrow$ (2): M ist l.u., da Basis.
Sei $M' \subseteq V$ mit $M \subsetneq M'$ und sei $v \in M$, $v \notin M'$.
$v \in V = < M > \Rightarrow$ es existieren $v_1, \ldots, v_n \in M$ mit $v_i \neq v_j$ für $i \neq j$ und $v \in < v_1, \ldots, v_n >$.
$\underset{(2.40)(c)}{\Rightarrow} < v_1, \ldots, v_n, v >$ ist l.a.
$\Rightarrow M'$ ist l.a., da $v_1, \ldots, v_n, v$ paarweise verschiedene Elemente von M' sind.
(2) $\Rightarrow$ (3): zu zeigen: (a) $< M >= V$, (b) Ist $M' \subsetneq M$, dann ist $< M' > \neq V$.
zu (a): Sei $v \in V$, $v \notin M$. Setze $M'' := M \cup \{v\}$.
$\Rightarrow M \subsetneq M'' \leq V \Rightarrow M''$ ist l.a.
$\Rightarrow$ es existieren $v_1, \ldots, v_n \in M''$ mit $v_i \neq v_j$ für $i \neq j$ und $(v_1, \ldots, v_n)$ ist l.a.
$\Rightarrow$ es existieren $a_1, \ldots, a_n \in K$ mit $(a_1, \ldots, a_n) \neq 0$ und $\sum\limits_{i=1}^{n} a_i v_i = 0$
$\underset{M \text{ l.u.}}{\Rightarrow} v \in \{v_1, \ldots, v_n\}$, sagen wir $v = v_{i_0}$, und es gilt: $a_{i_0} \neq 0$.
$\Rightarrow v \in < v_1, \ldots, v_{i_0-1}, v_{i_0+1}, \ldots, v_n > \subseteq < M >$.
zu (b): Sei $M' \subsetneq M$. Angenommen: $< M' >= V$.
$\Rightarrow M'$ ist Basis von V (vgl. (2.40)(a)(4))
$\Rightarrow M$ ist l.a. ((1) $\Rightarrow$ (2)) ↯
(3) $\Rightarrow$ (1): zu zeigen: M ist l.u. Angenommen: M ist l.a.
$\Rightarrow$ es existieren $v_1, \ldots, v_n \in M$ mit $v_i \neq v_j$ für $i \neq j$ und $(v_1, \ldots, v_n)$ ist l.a.
$\underset{(2.40)(c)}{\Rightarrow}$ es existiert i_0, $1 \leq i_0 \leq n$ mit $v_{i_0} \in < v_1, \ldots, v_{i_0-1}, v_{i_0+1}, \ldots, v_n >$.
Setze $M' := \{v \in M \mid v \neq v_{i_0}\}$.
$\Rightarrow M' \subsetneq M$ und $< M' >=< M >$. ↯ □

(2.46) Bemerkung

Sei $(v_1, \ldots, v_n)$ eine geordnete Basis von V. Dann gilt:
Zu jedem $v \in V$ existieren eindeutig bestimmte Koeffizienten $a_1, \ldots, a_n \in K$ mit $v = \sum\limits_{i=1}^{n} a_i v_i$.

Beweis

Existenz: Klar wegen $V = < v_1, \ldots, v_n >$.
Eindeutigkeit: Sei $\sum\limits_{i=1}^{n} a_i v_i = v = \sum\limits_{i=1}^{n} a'_i v_i$.
$\Rightarrow 0 = \sum\limits_{i=1}^{n} (a_i - a'_i) \cdot v_i \underset{(v_1, \ldots, v_n) \text{ ist l.u.}}{\Rightarrow} a_i - a'_i = 0$ für alle $1 \leq i \leq n$. □

(2.47) Satz

Sei $(v_1, \ldots, v_m)$ eine geordnete Basis von V und seien $w_1, \ldots, w_n \in V$. Dann gilt:
$n > m \Rightarrow (w_1, \ldots, w_n)$ ist l.a.

Beweis

Für $1 \leq j \leq n$ seien $a_{ij} \in K$, $1 \leq i \leq m$ definiert durch $w_j = \sum\limits_{i=1}^{m} a_{ij} v_i$ (vgl. (2.46)).

Sei $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in K^{m \times n}$.

Sei $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \neq 0$ eine Lösung des homogenen LGS $Ax = 0$ (existiert wegen $n > m$ nach (1.29)).

$$\Rightarrow \sum_{j=1}^{n} c_j w_j = \sum_{j=1}^{n} c_j \cdot \sum_{i=1}^{m} a_{ij} v_i = \sum_{i=1}^{m} \underbrace{\left(\sum_{j=1}^{n} c_j a_{ij} \right)}_{=0 \text{ für alle } i \text{ wegen } A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0} \cdot v_i = 0$$

$\Rightarrow (w_1, \ldots, w_n)$ ist l.u. □

(2.48) ! Satz

Sei V endlich erzeugt. Dann gilt:

(a) V besitzt eine endliche Basis.

(b) Sind M_1, M_2 Basen von V, dann sind M_1 und M_2 endlich und es gilt: $| M_1 | = | M_2 |$.

(c) (BASISERGÄNZUNGSSATZ) Sei $M' \subseteq V$ l.u. Dann existiert Basis M von V mit $M' \subseteq M$.

Beweis

(a) Ist $V = \{0\}$, dann okay.

Sei $V \neq \{0\}$ und $n \in \mathbb{N}$ minimal, so dass $v_1, \ldots, v_n$ existieren mit $V = < v_1, \ldots, v_n >$.

$\Rightarrow \{v_1, \ldots, v_n\}$ ist ein minimales Erzeugendensystem.

$\underset{(2.45)}{\Rightarrow} \{v_1, \ldots, v_n\}$ ist Basis.

(b) Sei $(v_1, \ldots, v_n)$ geordnete Basis von V (existiert nach (a)) und seien $w_1, \ldots, w_m \in M_1$, so dass $(w_1, \ldots, w_m)$ l.u. ist.

$\underset{\text{l.u.}}{\Rightarrow} m \leq n$. Insbesondere ist M_1 endlich und $| M_1 | \leq n$.

$\underset{(2.47)}{\Rightarrow} n \leq | M_1 |$, also $| M_1 | = n$. (Analog für M_2.)

(c) V besitze eine Basis mit genau n Elementen. Sei $M \subseteq V$ mit maximaler Elementanzahl unter allen Mengen $M'' \subseteq V$ mit $M' \subseteq M''$ und M'' ist l.u. (nach (2.47) hat jedes solche M'' maximal n Elemente).

$\Rightarrow M$ ist maximale l.u. Teilmenge von V.

$\underset{(2.45)(2)}{\Rightarrow}$ M ist Basis. □

(2.49) ! Definition

Sei V endlich erzeugt, M eine Basis von V.
$\dim(V) := \dim_K(V) := \mid M \mid$ heißt die DIMENSION von V.
(Anzahl der Elemente einer Basis von V.) □

(2.50) Beispiele

(a) $\dim(K^n) = n$

(b) $\dim(K^{m \times n}) = m \cdot n$

(c) $\left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\} \subseteq \mathbb{Q}^2$ ist Basis von $\mathbb{Q}^2$, denn $\dim_{\mathbb{Q}}(\mathbb{Q}^2) = 2$ und $\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right)$ ist l.u. nach (2.42)(a).

$\Rightarrow \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\}$ ist maximale l.u. Teilmenge. □

Ist V nicht endlich erzeugt, dann setzen wir $\dim_K(V) := \infty$.
Im Folgenden: „endlich erzeugt“ gleichwertig mit „endlich dimensional“.

(2.51) Korollar (zu (2.48))

Sei $\dim_K(V) = n, v_1, \ldots, v_n, v_{n+1} \in V$. Dann gilt:

(a) $(v_1, \ldots, v_n)$ l.u. $\Rightarrow (v_1, \ldots, v_n)$ ist geordnete Basis.

(b) $V = < v_1, \ldots, v_n > \Rightarrow (v_1, \ldots, v_n)$ ist geordnete Basis.

(c) $(v_1, \ldots, v_{n+1})$ l.a.

Beweis

(a) Folgt aus (2.48)(c),(b).

(b) Folgt aus (2.48)(b) und (2.45)(3).

(c) Folgt aus (2.48)(a),(b) und (2.47). □

(2.52) Korollar (zu (2.48))

Seien V und W e.e. K-VR. Dann gilt:
$V \cong W \Leftrightarrow \dim_K(V) = dim_K(W)$.

Beweis

„$\Rightarrow$": Sei $\varphi : V \to W$ ein Isomorphismus und sei $(v_1, \ldots, v_n)$ eine geordnete Basis von V.
$\Rightarrow (\varphi(v_1), \ldots, \varphi(v_n))$ ist geordnete Basis von W.
$\Rightarrow \dim_K(V) = \dim_K(W)$.
„$\Leftarrow$": Sei $(v_1, \ldots, v_n)$ eine geordnete Basis von V. Definiere $\kappa : V \to K^n$ durch:
$v \mapsto \kappa(v) := \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n$, falls $v = \sum\limits_{i=1}^{m} a_i v_i$ (vgl. (2.46)).
Leicht zu sehen: κ ist K-linear und bijektiv, d.h. κ ist ein Isomorphismus. $\Rightarrow V \cong K^n$.
Analog: $W \cong K^n$ (da $\dim_K(W) = \dim_K(V) = n$).
$\Rightarrow V \cong W$. □

Ab jetzt: „Basis" bei e.e. K-VR heißt immer „geordnete Basis".

(2.53) Satz

Sei V e.d. K-VR und $U \subsetneqq V$. Dann gilt:
$\dim_K(U) \leq \dim_K(V)$.

Beweis

Seien $u_1, \ldots, u_m \in U$ mit m maximal, so dass $(u_1, \ldots, u_m)$ l.u. ist (falls $U \neq \{0\}$).
Sei $u \in U$. $\underset{m \text{ max.}}{\Rightarrow}$ $(u_1, \ldots, u_m, u)$ ist l.a.
$\underset{(2.40)(c)}{\Rightarrow}$ $u \in < u_1, \ldots, u_m >$
$\Rightarrow U =< u_1, \ldots, u_m >$, d.h. $(u_1, \ldots, u_m)$ ist Basis von U.
Ist $\dim_K(V) = u$, dann ist $m \leq n$ (nach (2.47)).
Wäre $m = n$, dann wäre $V \underset{(2.51)(a)}{=} < u_1, \ldots, u_m > = u$. ↯ □

(2.54) Beispiel (Version der komplexen Zahlen)

Sei $V = \mathbb{R}^{2\times 2}$, $E := E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in V$, $I := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in V$, $\mathbb{C} =< E, I > \leq V$.
(E, I) l.u. $\Rightarrow (E, I)$ $\mathbb{R}$-Basis von $\mathbb{C}$.
Insbesondere hat jedes $C \in \mathbb{C}$ eine eindeutige Darstellung als $C = x \cdot E + y \cdot I$ mit $x, y \in \mathbb{R}$.

Es ist $I^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -E$.
$\Rightarrow \mathbb{C}$ ist kommutativer Ring mit neutralem Element E bzgl. $\cdot$ (ein Teilring von $\mathbb{R}^{2\times 2}$).
Ist $C = x\cdot E + y\cdot I \neq 0$ (d.h. $x^2+y^2 \neq 0$), dann ist $C \cdot \frac{1}{x^2+y^2} \cdot (x\cdot E + y\cdot I) = E$, d.h. C ist invertierbar.
$\Rightarrow \mathbb{C}$ ist Körper, der Körper der komplexen Zahlen.
$\{x\cdot E \mid x \in \mathbb{R}\}$ ist ein zu $\mathbb{R}$ isomorpher Teilkörper von $\mathbb{C}$. □

(2.55) Definition (elementare Matrizen)

Für $m \in \mathbb{N}$ definieren wir Matrizen aus $K^{m\times n}$:

(1) Für $1 \leq i \leq j \leq m$ sei $T_{i,j}$ die Matrix, die aus E_m durch Vertauschen der Zeilen i und j entsteht.

Z.B. $n = 3$: $T_{1,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

(2) Für $1 \leq i \leq j \leq m$ und $c \in K$ sei $A_{i,j}(c) := E_m + c \cdot E_{i,j}$ (vgl. (2.44)(c)).

(3) Für $0 \neq c \in K$ und $1 \leq i \leq j \leq m$ sei $M_i(c) := E_m + (c-1)\cdot E_{i,j}$. □

(2.56) Bemerkung

Sei $A \in K^{m\times n}$.

(a) $T_{i,j}$, $A_{i,j}(c)$ und $M_i(c) \in K^{m\times n}$ sind invertierbar.

(b) Entsteht A' aus a durch eine elementare Zeilentransformation (vgl. (1.21)) vom Typ (1) $t_{i,j}$ oder (2) $a_{i,j}(c)$ oder (3) $m_i(c)$, dann gilt in den jeweiligen Fällen: (1) $A' = T_{i,j}\cdot A$, (2) $A' = A_{i,j}(c)\cdot A$, (3) $A' = M_i(c)\cdot A$.

(c) Analog werden elementare Spaltentransformationen von A durch Multiplikation von rechts mit elementaren Matrizen aus $K^{n\times m}$ definiert.

(d) Entsteht B aus A durch eine Folge elementarer Zeilen- und Spaltenoperationen, dann existiert $S \in \mathrm{GL}_m(K)$ und $T \in GL_n(K)$ mit $B = S\cdot A\cdot T$.

Beweis

(a) $T_{i,j}^{-1} = T_{i,j}$, $A_{i,j}(c)^{-1} = A_{i,j}(-c)$, $M_i(c)^{-1} = M_i(c^{-1})$

(b) Folgt sofort z.B. aus (2.33)(b).

(c) A'' entstehe aus a durch elementare Spaltentransformationen.

$\Rightarrow A'' = (A')^t$, wobei A' eine Matrix ist, die aus A^t durch eine elementare Zeilentransformation entstanden ist.

$\underset{(b)}{\Rightarrow} A'' = (E \cdot A^t)^t = (A^t)^t \cdot E^t = A \cdot E^t$, wobei E eine elementare Matrix ist. Mit E ist E^t auch elementar.

(d) Nach (b) und (c) ist $B = S_k \cdot S_{k-1} \cdots S_1 \cdot A \cdot T_1 \cdot T_2 \cdots T_l$ mit elementaren Matrizen S_i, T_j, $S_i \in \mathrm{GL}_m(K)$ und $T_j \in \mathrm{GL}_n(K)$. Weil $\mathrm{GL}_m(K)$ und $\mathrm{GL}_n(K)$ Gruppen sind, sind $S := S_k \cdot S_{k-1} \cdot S_1$ und $T := T_1 \cdot T_2 \cdots T_l$ invertierbar und $B = S \cdot A \cdot T$. □

Beispiel

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

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 2 & 3 \\ 0 & 4 & -2 & -4 \\ 3 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 2 & 3 \\ 0 & 4 & -2 & -4 \\ 0 & 4 & -6 & -9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 2 & 3 \\ 2 & 2 & 2 & 2 \\ 3 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 2 & 3 \\ 0 & 4 & -2 & -4 \\ 0 & 4 & -6 & -9 \end{pmatrix}$$

□

(2.57) Bemerkung

Sei $A \in K^{m \times n}$, $S \in \mathrm{GL}_m(K)$, $T \in \mathrm{GL}_n(K)$.

(a) $\varphi_S : K^m \to K^m$, $v \mapsto S \cdot v$ und

$\psi_T : K^{1\times n} \to K^{1\times n}$, $v \mapsto v \cdot T$ sind K-VR-Isomorphismen (also linear und bijektiv).

(b) Zeilenraum von $A =$ Zeilenraum von $S \cdot A$ und Spaltenraum von $A =$ Spaltenraum von $A \cdot T$.

(c) Zeilenraum von $A \cong$ Zeilenraum von $A \cdot T$ und Spaltenraum von $A \cong$ Spaltenraum von $S \cdot A$.

Beweis

(a) φ_S, ψ_T sind K-linear, sie sind bijektiv mit Umkehrabbildung $\varphi_{S^{-1}}$ bzw. $\psi_{T^{-1}}$ (siehe (1.21)).

(b) Zeilenraum von $A =$ Zeilenraum von $S^{-1} \cdot (S \cdot A) \underset{(2.33)(b)}{\subseteq}$ Zeilenraum von $S \cdot A \underset{(2.33)(b)}{\subseteq}$ Zeilenraum von A.

2. Aussage analog durch Transponieren.

(c) Seien $z_1, \ldots, z_m$ die Zeilen von A.

$\underset{(2.33)(\text{b})}{\Rightarrow}$ $z_1 \cdot T = \psi_T(z_1), \ldots, z_m \cdot T = \psi_T(z_m)$ sind die Zeilen von $A \cdot T$.

$\psi_T : K^{1\times n} \to K^{1\times n}$ ist Isomorphimus.

$\Rightarrow \psi_T\,|_U : U \to \psi_T(U),\, u \mapsto \psi_T(u) = u \cdot T$ ist Isomorphismus für alle $U \leq K^{1\times n}$.

$U = < z_1, \ldots, z_m > =$ Zeilenraum von A.

$\Rightarrow \psi_T(U) = < \psi_T(z_1), \ldots, \psi_T(z_m) > =$ Zeilenraum von $A \cdot T$

$\Rightarrow$ Behauptung

2. Ausssage analog. □

(2.58) Definition und Bemerkung

Sei $A \in K^{m\times n}$.

(a) A kann durch elementare Zeilen- und Spaltentransformationen in eine Matrix der Form $\left(\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right) \in K^{m\times n}$ mit $0 \leq r \leq \min\{m,n\}$ übergeführt werden.

(b) Es existieren $S \in \mathrm{GL}_m(K)$ und $T \in GL_n(K)$ und $S \cdot A \cdot T = \left(\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right)$ mit $0 \leq r \leq \min\{m,n\}$.

(c) $\dim_K(\text{Zeilenraum von } A) = \dim_K(\text{Spaltenraum von } A) = r$ mit $0 \leq r \leq \min\{m,n\}$.

(d) $\operatorname{rang}(A) := \dim_K(\text{Zeilenraum von } A)$ heißt *der* RANG von A.

Beweis

(a) Durch elementare Zeilentransformationen folgt Zeilenstufenform wie folgt:

$$\left(\begin{array}{c|cccccccc} & 1 & * & & \cdots & & & & * \\ 0 & 0 & \cdots & 0 & 1 & * & \cdots & & * \\ & & & & \ddots & & & & \\ & 0 & \cdots & & 0 & 1 & * & & * \\ \hline 0 & & & & 0 & & & & \end{array}\right) \xrightarrow[\text{von Zeilen}]{\text{Vertauschen}} \left(\begin{array}{cccccccc} 1 & * & & \cdots & & & & * \\ 0 & 1 & * & & \cdots & & & * \\ & & \ddots & & & & & \\ 0 & \cdots & 0 & 1 & * & \cdots & & * \\ \hline & & & 0 & & & & \end{array}\right) \xrightarrow[\text{von Zeilen}]{\text{Ausräumen}}$$

$$\left(\begin{array}{ccc|c} 1 & & & \\ & \ddots & & 0 \\ & & 1 & \\ \hline & 0 & & 0 \end{array}\right)$$

(b) Folgt aus (a) und (2.56)(a).

(c) Aus (b) und (2.57)(c) folgt:

$\dim_K(\text{Zeilenraum von } A) = \dim_K(\text{Spaltenraum von } S \cdot A) = \dim_K(\text{Zeilenraum von } (S \cdot A) \cdot T) \underset{(2.42)(\text{b})}{=} r \underset{\text{genauso}}{=} \dim_K(\text{Spaltenraum von } A)$. □

(2.59) Bemerkung (Charakterisierung von „Rang")

Sei $A \in K^{m \times n}$. Dann gilt:
$\text{rang}(A) = \text{Maximalzahl l.u. Zeilen von } A = \text{Maximalzahl l.u. Spalten von } A$
[„Maximalzahl l.u. Zeilen von A" heißt: größtes $r \in \mathbb{N}_0$, so dass $z_{i_1}, \ldots, z_{i_r} \in \{z_1, \ldots, z_m\}$ existieren, so dass $(z_{i_1}, \ldots, z_{i_r})$ l.u. ist. Hierbei ist $\{z_1, \ldots, z_m\}$ die Menge der Zeilen von A.]

Beweis

Notation von oben.
$\Rightarrow < z_{i_1}, \ldots, z_{i_r} > = < z_1, \ldots, z_m > = \text{Zeilenraum von } A$
$\Rightarrow r = \dim_K(\text{Zeilenraum von } A) = \text{rang}(A)$
Analog für Spaltenraum. □

(2.60) Beispiel

Sei $A \in K^{m \times n}$.
Bringe A durch elementare Spaltentransformationen auf Spaltenstufenform A' (vgl. (2.41)).

$$A' = \left(\begin{array}{cccc|c} & & 0 & & 0 \\ \hline \square & 0 & \cdots & 0 & \\ * & \square & & & \\ \vdots & & \ddots & & 0 \\ * & \cdots & * & \square & \end{array}\right)$$

Seien $s'_1, \ldots, s'_r$ die von 0 verschiedenen Spalten von A'. Dann gilt:

(a) $\text{rang}(A) = r$

(b) $(s'_1, \ldots, s'_r)$ ist Basis vom Spaltenraum von A.

Beweis

(a) Folgt aus (b).

(b) Spaltenraum von $A \underset{(2.57)(\text{b})}{=}$ Spaltenraum von $A' = < s'_1, \ldots s'_r >$.

Nach (2.42)(b) ist $(s'_1, \ldots s'_r)$ l.u., also eine Basis.

Analoge Aussage gilt für den Zeilenraum. □

(2.61) Beispiel

$V = < \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} > \leq \mathbb{R}^4$. Gesucht: Basis von V.

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

$\Rightarrow \dim_{\mathbb{R}} V = 2$.

$\Rightarrow \left(\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ -2 \\ -3 \end{pmatrix} \right)$ ist Basis von V.

□

(2.62) Satz

Sei V ein m-dimensionaler K-VR mit Basis $(v_1, \ldots, v_m)$. Sei $\kappa : V \to K^m$ der Isomorphismus aus dem Beweis von (2.52) ($\kappa(v) := \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \in K^m$, falls $v = \sum_{i=1}^{m} a_i v_i$).

Seien $w_1, \ldots, w_n \in V$.
Gesucht: Basis von $< w_1, \ldots, w_n > =: W \leq V$.
Methode: Berechne eine Basis $(u_1, \ldots, u_r)$ von $\underbrace{\kappa(W)}_{=<\kappa(w_1),\ldots,\kappa(w_n)>} \leq K^m$.

$\Rightarrow (\kappa^{-1}(u_1), \ldots, \kappa^{-1}(u_r))$ ist Basis von W.

Beweis

$\kappa|_W : W \to \kappa(W)$, $w \mapsto \kappa(w)$ ist ein Isomorphismus, der die Basen überträgt. □

(2.63) ! Beispiel

$V = \mathbb{R}^{3\times 2}$, Basis: $(E_{1,1}, E_{1,2}, E_{2,1}, E_{2,2}, E_{3,1}, E_{3,2})$ (vgl. (2.44)(c)).

$$w_1 = \begin{pmatrix} 1 & 2 \\ 0 & 2 \\ 3 & 2 \end{pmatrix}, w_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \\ 0 & -1 \end{pmatrix}, w_3 = \begin{pmatrix} -1 & 0 \\ -1 & 0 \\ -1 & 0 \end{pmatrix}, w_4 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

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

$$\underset{\kappa^{-1}}{\Rightarrow} \left(\begin{pmatrix} 1 & 2 \\ 0 & 2 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \\ 2 & 3 \end{pmatrix} \right)$$

ist Basis von $W =< w_1, w_2, w_3, w_4 >\leq \mathbb{R}^{3\times 2}$. □

(2.64) Satz

Sei $A \in K^{m\times n}$ und $L_0 \leq K^n$ die Lösungsmenge des homogenen LGS $Ax = 0$. Dann gilt: $\dim_K L_0 = n - \operatorname{rang}(A)$.

Beweis

A' sei aus A durch eine Folge elementarer Zeilentransformationen entstanden und A' hat Zeilenstufenform.
$\Rightarrow L_0$ ist die Lösungsmenge des homogenen LGS $A'x = 0$ (vgl. (1.23)).
Weiter gilt: $\operatorname{rang}(A) \underset{(2.57)(b)}{=} rang(A')$.
$\operatorname{rang}(A') =$ Anzahl der Zeilen von A', die $\neq 0$ sind $=$ Anzahl der abhängigen Variablen.
Aus (1.27) folgt: $\dim_K L_0 \underset{(2.60)}{=}$ Anzahl der freien Variablen $= n - rang(A') = n - rang(A)$ □

(2.65) Satz

Sei $A \in K^{n\times n}$ mit Spalten $s_1, \dots, s_n \in K^n$ und Zeilen $z_1, \dots, z_n \in K^{1\times n}$. Dann sind folgende Aussagen äquivalent:

(a) A invertierbar.

(b) Es existiert $B \in K^{n\times n}$ mit $A \cdot B = E_n$.

(c) Es existiert $C \in K^{n\times n}$ mit $C \cdot A = E_n$.

(d) Das homogene LGS $Ax = 0$ hat nur die triviale Lösung.

(e) Für jedes $b \in K^n$ hat das LGS genau eine Lösung.

(f) $\operatorname{rang}(A) = n$

(g) $(z_1, \dots, z_n)$ l.u.

(h) $(s_1, \dots, s_n)$ l.u.

Beweis

(g) $\Rightarrow$ (f) $\Rightarrow$ (h): Nach (2.59).
(a) $\Rightarrow$ (c): ✓(Definition der Invertierbarkeit)
(c) $\Rightarrow$ (d): Sei $c \in K^n$ mit $Ac = 0$. $\Rightarrow 0 = C \cdot (A \cdot c) = (C \cdot A) \cdot c = E_n \cdot c = c$.
(d) $\Rightarrow$ (f): Der Lösungsraum L_0 des homogenen LGS $Ax = 0$ hat die Dimension 0.
$\underset{(2.64)}{\Rightarrow}$ $\operatorname{rang}(A) = n$.
(f) $\Rightarrow$ (e): $\operatorname{rang}(A) = n \underset{(2.59),(2.47)}{\Rightarrow} \operatorname{rang}(A,b) = n$.
$(A,b) \in K^{n\times(n+1)}$: erweiterte Matrix des LGS $Ax = b$. $\Rightarrow$ Spaltenraum von A = Spaltenraum von (A,b) $\underset{(2.38)(3)}{\Rightarrow}$ Das LGS $Ax = b$ ist lösbar.
Aus (2.38) und $L_0 \underset{(2.64)}{=} \{0\}$ folgt: $Ax = b$ hat genau eine Lösung.
(e) $\Rightarrow$ (h): Seien $e_1, \ldots, e_n \in K^n$ die Spalten von E_n.
Sei $b_i \in K^n$ die Lösung von $Ax = e_i$, $1 \leq i \leq n$, d.h. $A \cdot b_i = e_i$, $1 \leq i \leq n$.
Sei $B = (b_1, \ldots b_n) \in K^{1\times n}$. $\Rightarrow A \cdot B = (A \cdot b_1, \ldots, A \cdot b_n) = (e_1, \ldots e_n) = E_n$.
(b) $\Rightarrow$ (e): $A \cdot B = E_n \Rightarrow B^t \cdot A^t = E_n$
$\Rightarrow \operatorname{rang}(A^t) = n$ (Zeilenraum von E_n = Zeilenraum von $B^t \cdot A^t$ = Zeilenraum von A^t)
$\underbrace{\Longrightarrow}_{\text{nach dem Beweis von (f)} \Rightarrow \text{(e)} \Rightarrow \text{(b)}}$ es existiert $D \in K^{n\times m}$ mit $A^t \cdot D = E_n$
$\Rightarrow B^t = B^t \cdot E_n = B^t \cdot (A^t \cdot D) = (B^t \cdot A^t) \cdot D = E_n \cdot D = D$
$\Rightarrow B^t = D$, d.h. A^t invertierbar.
$\underset{(2.24)}{\Rightarrow}$ A ist invertierbar. □

(2.66) Korollar

Sei $A \in \mathrm{GL}_n(K)$, $b \in K^n$.
Die Lösung von $Ax = b$ (eindeutig lösbar nach (2.65)) ist gegeben durch $A^{-1} \cdot b$.

Beweis

Ist $c \in K^n$ mit $Ac = b$, dann ist $c = E_n \cdot c = (A^{-1} \cdot A) \cdot c = A^{-1} \cdot (A \cdot c) = A^{-1} \cdot b$. □

(2.67) Satz (Antworten auf die Fragen am Ende von Kapitel 1, §4)

Sei $A \in K^{m\times n}$, $L_0 \leq K^n$ die Lösungsmenge von $Ax = 0$.

(1) L_0 ist ein UVR von K^n mit $\dim_K(L_0) = n - \operatorname{rang}(A)$.

(2) Die Anzahl der abhängigen Variablen ist gleich $\operatorname{rang}(A)$.

(3) Sei $b \in K^n$. Dann gilt:

$Ax = b$ ist lösbar $\Leftrightarrow \operatorname{rang}(A) = \operatorname{rang}(A,b)$.

(4) Sei $b \in K^m$ und $c \in K^n$ mit $Ac = b$, d.h. $c \in L :=$ Lösungsmenge des LGS $Ax = b$. Dann gilt: $L = c + L_0$.

(5) Sei $m = n$. Dann sind äquivalent:

(a) Es existiert $b \in K^n$, so dass $Ax = b$ eindeutig lösbar ist.

(b) Für jedes $b \in K^n$ ist $Ax = b$ eindeutig lösbar.

(c) A ist invertierbar. $\square$

(2.68) Bemerkung (Algorithmus zum Invertieren)

Sei $A \in K^{n\times n}$. Dann gilt:
A invertierbar $\Leftrightarrow$ $(A \mid E_n) \in K^{n\times 2n}$ kann durch elementare <u>Zeilen</u>transformationen in $(E_n \mid B)$ übergeführt werden. In diesem Fall ist $B = A^{-1}$.

Beweis

„$\Rightarrow$": Bringe A durch elementare Zeilentransformationen auf Zeilenstufenform A'.
A invertierbar $\underset{(2.65)}{\Rightarrow}$ $n = \operatorname{rang}(A)$ $\underset{(2.65)}{\Rightarrow}$ $n = \operatorname{rang}(A')$

$$\Rightarrow A' = \begin{pmatrix} \square & * & \cdots & * \\ & \square & & * \\ & & \ddots & \\ 0 & & & \square \end{pmatrix} \text{(keine freien Variablen)}$$

„$\Leftarrow$": Nach (2.56) existiert S mit $(E_n \mid B) = S(A \mid E_n) \Rightarrow (SA \mid S) \Rightarrow SA = E_n$ und $S = B$
$\underset{(2.65)}{\Rightarrow}$ A invertierbar und $S = A^{-1}$. $\square$

(2.69) Beispiel

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$$

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \to \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 0 & 1 \end{array}\right) \to$$

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 & 0 \end{array}\right) \to \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 & 0 \end{array}\right) \to$$

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -2 & 1 & 1 & 1 & -1 \end{array}\right) \to \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right) \to$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right) \to \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right)$$

$$\Rightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$ □

§ 4 Matrizen und lineare Abbildungen

Konvention

Objekte	Bezeichnungen	
Matrizen	$A, B, C, \ldots$	(lat. Großbuchstaben)
Vektorräume	$U, V, W, \ldots$	(lat. Großbuchstaben)
lineare Abbildungen	$\alpha, \beta, \ldots, \varphi, \psi, \ldots$	(griech. Kleinbuchstaben)
geordnete Basen	$\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \ldots$	(große Skriptbuchstaben)

□

Grundvoraussetzungen

K sei Körper, K-Vektorräume seien endlich erzeugt, Basen seien geordnet. □

(2.70) Erinnerung und Definition

Sei V K-Vektorraum mit Basis $\mathcal{B} = (v_1, \ldots, v_n)$.
Definiere: $\kappa_{\mathcal{B}} : V \to K^n$ durch

$\kappa_{\mathcal{B}}(v) := \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, falls $v = \sum_{i=1}^{n} a_i v_i$ (vgl. (2.52)).

$\kappa_{\mathcal{B}}(v)$ heißt *der* KOORDINATENVEKTOR VON V BZGL. B.
$\kappa_{\mathcal{B}}$ ist ein Isomorphismus $V \to K^n$. □

(2.71) Beispiele

(a) $V = K^{1\times n}$, $\mathcal{B} = (e_1{}^t, \ldots, e_n{}^t)$, die Standardbasis von V.

$$\Rightarrow \kappa_{\mathcal{B}}((a_1,\ldots,a_n)) = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

(b) $V = \mathbb{R}^2$, $\mathcal{B} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right)$

$$\begin{pmatrix} a \\ b \end{pmatrix} = (a-b)\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 1 \\ 1 \end{pmatrix},\ \kappa_{\mathcal{B}}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a-b \\ b \end{pmatrix}$$ □

(2.72) Definition (Abbildungsmatrix)

V, W seien K-Vektorräume, $\mathcal{B}$ Basis von V, $\mathcal{B} = (v_1,\ldots,v_n)$, $\mathcal{C} = (w_1,\ldots,w_m)$ Basis von W, $\varphi \in \mathrm{Hom}_K(V,W)$.
Definiere $a_{ij} \in K$, $1 \leq i \leq m$, $1 \leq j \leq n$, durch $\varphi(v_j) = \sum\limits_{i=1}^{m} a_{ij} w_i$.
Dann heißt $M^{\mathcal{B}}_{\mathcal{C}}(\varphi) := (a_{ij})_{\substack{1\leq i\leq m \\ 1\leq j\leq n}} \in K^{m\times n}$ die (ABBILDUNGS-)MATRIX von φ bzgl. $\mathcal{B}$ und $\mathcal{C}$.

□

(2.73) Beispiel

(a) $\varphi : \mathbb{Q} \to \mathbb{R}^2$, $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} a+b \\ a-b \end{pmatrix}$.

$\mathcal{B} = \mathcal{C} = (e_1, e_2)$ Standardbasis.

$$\varphi(e_1) = \varphi\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1\cdot e_1 + 1\cdot e_2$$

$$\varphi(e_2) = \varphi\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1\cdot e_1 - 1\cdot e_2$$

(b) $\varphi : K^{3\times 2} \to K^{2\times 3}$, $A \mapsto A^t$

$\mathcal{B} = (E_{11}, E_{12}, E_{21}, E_{22}, E_{31}, E_{32})$

$\mathcal{C} = (E_{11}, E_{12}, E_{13}, E_{21}, E_{22}, E_{23})$

$$\Rightarrow M^{\mathcal{B}}_{\mathcal{C}}(\varphi) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(c) Sei $A \in K^{m\times n}$.

$\varphi = \varphi_A : K^n \to K^m$, $v \mapsto A\cdot v$

$\mathcal{B} = (e_1, \ldots, e_n)$, $\mathcal{C} = (e_1, \ldots, e_m)$ Standardbasen

$\varphi(e_j) = A \cdot e_j = j$-te Spalte von A für alle $1 \leq j \leq m$

$\Rightarrow M_{\mathcal{C}}^{\mathcal{B}}(\varphi_A) = A$

(d) In $C^\infty(\mathbb{R})$ seien φ_i, $i \in \mathbb{N}_0$, definiert durch:

$p_0 : \mathbb{R} \to \mathbb{R}, x \mapsto 1$

$p_i : \mathbb{R} \to \mathbb{R}, x \mapsto x^i$, $i \in \mathbb{N}$

Sei $V =< p_0, \ldots, p_n > \leq C^\infty(\mathbb{R})$.

$(p_0, \ldots, p_n)$ ist linear unabhängig:

Seien $a_0, \ldots, a_n \in \mathbb{R}$ mit $\sum\limits_{i=0}^{n} a_i p_i : x \mapsto \sum\limits_{i=0}^{n} a_i x^i$

$\Rightarrow a_0 = a_1 = \ldots = a_n = 0$ (denn: Polynom $\neq 0$ hat nur endlich viele Nullstellen)

$\Rightarrow \mathcal{B} = (p_0, \ldots, p_n)$ Basis von V.

Sei $\varphi : V \to V$, $f \mapsto f'$ (Ableitung).

$$\varphi(p_i) = \begin{cases} 0 & \text{für } i = 0 \\ i \cdot p_{i-1} & \text{für } i > 0 \end{cases}$$

$$\Rightarrow M_{\mathcal{B}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 2 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & n \\ 0 & 0 & 0 & \ldots & 0 \end{pmatrix} \in \mathbb{R}^{(n+1)\times(n+1)}$$ □

(2.74) Satz

V, W seien K-Vektorräume, $\dim_K V = n$, $\dim_K W = m$, $\mathcal{B}$, $\mathcal{C}$ seien Basen von V bzw. W. Dann gilt für $\varphi \in \mathrm{Hom}_K(V,W)$:

(a) $\kappa_{\mathcal{C}}(\varphi(v)) = M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \cdot \kappa_{\mathcal{B}}(v)$ für alle $v \in V$

(b) Sei $A \in M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ und $\varphi_A : K^n \to K^m, v \mapsto A \cdot v$. Dann gilt:

- $\mathrm{Kern}(\varphi) = {\kappa_{\mathcal{B}}}^{-1}(\mathrm{Kern}(\varphi_A))$
- $\mathrm{Bild}(\varphi) = {\kappa_{\mathcal{C}}}^{-1}(\mathrm{Bild}(\varphi_A))$

(c) $\dim_K V = \dim_K(Kern(\varphi)) + \dim_K(Bild(\varphi))$

Beweis

(a) $M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$, d.h. $\varphi(v_j) = \sum_{i=1}^{n} a_{ij}w_i$.

Sei $v \in V$, etwa $v = \sum_{j=1}^{n} c_j v_j$. $\kappa_{\mathcal{B}}(v) = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$.

$\Rightarrow \varphi(v) = \sum_{j=1}^{n} c_j \cdot \varphi(v_j) = \sum_{j=1}^{n} c_j(\sum_{i=1}^{m} a_{ij}w_i) = \sum_{i=1}^{m}(\sum_{j=1}^{n} c_j a_{ij})w_i = \sum_{i=1}^{m}(\sum_{j=1}^{n} a_{ij}c_j)w_i$

$$\Rightarrow \kappa_{\mathcal{C}}(\varphi(v)) = \begin{pmatrix} \sum_{j=1}^{n} a_{ij}c_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj}c_j \end{pmatrix} = A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A \cdot \kappa_{\mathcal{B}}(v).$$

(b) $v \in \text{Kern}(\varphi) \Leftrightarrow \varphi(v) = 0$

($\kappa_{\mathcal{C}}$ Isomorphismus) $\Leftrightarrow \kappa_{\mathcal{C}}(\varphi(v)) = 0 \underset{(a)}{\Leftrightarrow} A \cdot \kappa_{\mathcal{B}}(v) = 0 \Leftrightarrow \kappa_{\mathcal{B}}(v) \in \text{Kern}(\varphi_A)$

($\kappa_{\mathcal{B}}$ Isomorphismus) $\Leftrightarrow v \in {\kappa_{\mathcal{B}}}^{-1}(\text{Kern}(\varphi_A))$

$w \in \text{Bild}(\varphi) \Leftrightarrow$ es gibt $v \in V : w = \varphi(v) \Leftrightarrow$ es gibt $v \in V : A \cdot \kappa_{\mathcal{C}}(w) = \kappa_{\mathcal{C}}(\varphi(v)) \underset{(a)}{\Leftrightarrow}$ es gibt $v \in V : A \cdot \kappa_{\mathcal{B}}(v) = \kappa_{\mathcal{C}}(w) \Leftrightarrow \kappa_{\mathcal{C}}(w) \in \text{Bild}(\varphi_A) \Leftrightarrow w \in {\kappa_{\mathcal{C}}}^{-1}(\text{Bild}(\varphi_A))$.

(c) $\dim(\text{Kern}(\varphi_A)) = \dim(L_0)$, wobei L_0 die Lösungsmenge von $Ax = 0$ ist.

$\text{Bild}(\varphi_A) =$ Spaltenraum von A

$\Rightarrow \dim(\text{Bild}(\varphi_A)) = \text{rang}\, A$

$\Rightarrow$ n-$\dim(\mathit{Bild}(\varphi_A)) = \dim(\text{Kern}(\varphi_A))$ (vgl. (2.64))

$\underset{(b)}{\Rightarrow}$ Behauptung, da $\kappa_{\mathcal{B}}$ und $\kappa_{\mathcal{C}}$ Isomorphismen sind. □

(2.75) Beispiel (vgl. (2.73)(d))

$V := < p_0, \ldots, p_n > \le \mathbb{R}^{\mathbb{R}}$ mit $p_i : \mathbb{R} \to \mathbb{R}, x \mapsto x^i$; $\mathcal{B} = < p_0, \ldots, p_n >$.
Sei $\varphi : V \to V$, $f \mapsto f'$ (Ableitung).

Sei $f : \mathbb{R} \to \mathbb{R}, x \mapsto \sum_{i=0}^{n} a_i x^i$, $f = \sum_{i=0}^{n} a_i p_i \kappa_{\mathcal{B}}(f) = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$.

$$M_{\mathcal{B}}^{\mathcal{B}}(\varphi)\cdot\kappa_{\mathcal{B}}(f)=\begin{pmatrix}0&1&0&\dots&0\\0&0&2&\dots&0\\0&0&0&\dots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\dots&n\\0&0&0&\dots&0\end{pmatrix}\begin{pmatrix}a_o\\\vdots\\a_n\end{pmatrix}=\begin{pmatrix}a_1\\2\cdot a_2\\\vdots\\n\cdot a_n\\0\end{pmatrix}$$

$\Rightarrow \varphi(f)=f'=\sum\limits_{i=0}^{n-1}(i+1)a_{i+1}\cdot p_i,\ x\mapsto\sum\limits_{i=0}^{n-1}(i+1)a_{i+1}\cdot x^i$ □

(2.76) Satz

Seien U, V, W K-Vektorräume mit Basen $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ und sei $\varphi\in\mathrm{Hom}_K(U,V)$, $\psi\in\mathrm{Hom}_K(V,W)$. Dann gilt:
$M_{\mathcal{C}}^{\mathcal{A}}(\psi\circ\varphi)=M_{\mathcal{C}}^{\mathcal{B}}(\psi)M_{\mathcal{B}}^{\mathcal{A}}(\varphi)$.

Beweis

Seien $\mathcal{A}=(u_1,\dots,u_n)$, $\mathcal{B}=(v_1,\dots,v_m)$, $\mathcal{C}=(w_1,\dots,w_l)$. Dann gilt:

$M_{\mathcal{C}}^{\mathcal{B}}(\psi)=(a_{ij})_{\substack{1\le i\le l\\1\le j\le m}}$ mit $\psi(v_j)=\sum\limits_{i=1}^{l}a_{ij}w_i,\ 1\le j\le m$

$M_{\mathcal{B}}^{\mathcal{A}}(\varphi)=(b_{jk})_{\substack{1\le j\le m\\1\le k\le n}}$ mit $\varphi(u_k)=\sum\limits_{j=1}^{m}b_{jk}v_j,\ 1\le k\le n$

$M_{\mathcal{C}}^{\mathcal{A}}(\psi\circ\varphi)=(c_{ik})_{\substack{1\le i\le l\\1\le k\le n}}$ mit $\psi\circ\varphi(u_k)=\sum\limits_{i=1}^{l}c_{ik}w_i,\ 1\le k\le n$

Andererseits:

$\psi\circ\varphi(u_k)=\psi(\varphi(u_k))=\psi\left(\sum\limits_{j=1}^{m}b_{jk}v_j\right)=\sum\limits_{j=1}^{m}b_{jk}\psi(v_j)=\sum\limits_{j=1}^{m}b_{jk}\left(\sum\limits_{i=1}^{l}a_{ij}w_i\right)$

$=\sum\limits_{i=1}^{l}\left(\sum\limits_{j=1}^{m}a_{ij}b_{jk}\right)w_i,\ 1\le k\le n.$

$\Rightarrow c_{ik}=\sum\limits_{j=1}^{l}a_{ij}b_{jk},\ 1\le i\le l,\ 1\le j\le k.$ □

(2.77) Korollar

Seien $A\in K^{l\times m}$, $B\in K^{m\times n}$ und $C\in K^{n\times p}$. Dann gilt:
$(AB)C=A(BC)$.

Beweis

Folgt aus $(\varphi_A\circ\varphi_B)\circ\varphi_C=\varphi_A\circ(\varphi_B\circ\varphi_C)$ mit (2.76) und (2.73)(c). □

(2.78) Bemerkung

Seien V, W n-dimensionale K-Vektorräume mit Basen $\mathcal{B}$ bzw. $\mathcal{C}$ und sei $\varphi \in \mathrm{Hom}_K(V,W)$. Dann gilt:
φ Isomorphismus $\Leftrightarrow M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ invertierbar.
In diesem Fall: $M_{\mathcal{C}}^{\mathcal{B}}(\varphi)^{-1} = M_{\mathcal{B}}^{\mathcal{C}}(\varphi^{-1})$.

Beweis

Sei $A = M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \in K^{m\times n}$. Dann gilt:
φ Isomorphismus $\overset{(2.74)(c)}{\underset{\dim V=\dim W}{\Longleftrightarrow}}$ φ injektiv $\underset{(2.37)(c)}{\Longleftrightarrow}$ $\mathrm{Kern}(\varphi) = \{0\}$ $\underset{(2.74)(b)}{\Longleftrightarrow}$ $\mathrm{Kern}(\varphi_A) = \{0\}$
$\overset{(2.38)(b)}{\underset{(2.64)}{\Longleftrightarrow}}$ $\mathrm{rang}\,A = n$ $\underset{(2.65)}{\Longleftrightarrow}$ A ist invertierbar.
Ist φ bijektiv, dann gilt:
$M_{\mathcal{B}}^{\mathcal{C}}(\varphi^{-1})M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = M_{\mathcal{B}}^{\mathcal{B}}(\varphi^{-1}\circ\varphi) = M_{\mathcal{B}}^{\mathcal{B}}(\mathrm{id}_V) = E_n$
$\underset{(2.65)}{\Longrightarrow}$ A ist invertierbar und $A^{-1} = M_{\mathcal{B}}^{\mathcal{C}}(\varphi^{-1})$. □

(2.79) Bezeichnungen

Seien V und W endlich dimensionale K-Vektorräume mit Basen $\mathcal{B} = (v_1,\dots,v_n)$ und $\mathcal{B}' = (v_1',\dots,v_n')$ von V bzw. $\mathcal{C} = (w_1,\dots,w_m)$ und $\mathcal{C}' = (w_1',\dots,w_m')$ von W. Sei $\varphi \in \mathrm{Hom}_K(V,W)$. □

Frage

Wie hängen $M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ und $M_{\mathcal{C}'}^{\mathcal{B}'}(\varphi)$ zusammen? □

(2.80) Definition

Bezeichnungen wie in (2.79). Dann heißt $M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V) \in K^{n\times n}$ BASISWECHSELMATRIX.
[Die Spalten von $M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$ sind die Koeffizientenvektoren der v_j', $1 \le j \le n$, bzgl. $\mathcal{B}$.] □

(2.81) Bemerkung

Bezeichnungen wie in (2.79). Dann gilt:

(a) $M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$ ist invertierbar und $M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)^{-1} = M_{\mathcal{B}'}^{\mathcal{B}}(\mathrm{id}_V)$.

(b) Ist $T \in \mathrm{GL}_n(K)$, dann existiert Basis B'' von V mit $M_{\mathcal{B}}^{\mathcal{B}''}(\mathrm{id}_V) = T$.

Beweis

(a) Folgt aus (2.78).

(b) Sei $T = (t_{ij})_{1\leq i,j\leq n}$.

Für $1 \leq j \leq n$ sei $v''_j := \sum\limits_{i=1}^{n} t_{ij} v_j$.

Sei $B'' := (v''_1, \ldots, v''_n)$. Dann gilt:

B'' ist Basis von V, da T invertierbar ist.

Klar: $M_{\mathcal{B}}^{\mathcal{B}''}(\mathrm{id}_V) = T$. □

(2.82) ! Satz (Basiswechselsatz)

Bezeichnungen wie in (2.79). Dann gilt:
$M_{\mathcal{C}'}^{\mathcal{B}'}(\varphi) = M_{\mathcal{C}'}^{\mathcal{C}}(\mathrm{id}_W) M_{\mathcal{C}}^{\mathcal{B}}(\varphi) M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V) = M_{\mathcal{C}}^{\mathcal{C}'}(\mathrm{id}_W)^{-1} M_{\mathcal{C}}^{\mathcal{B}}(\varphi) M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$.

Beweis

Betrachte das Diagramm von Abbildungen:

$$\begin{tikzcd}
\mathcal{B}\ V \arrow[r, "\varphi"] & W\ \mathcal{C} \arrow[d, bend left, "id_W"] \\
\mathcal{B}'\ V \arrow[u, bend left, "id_V"] \arrow[r, "\varphi"] & W\ \mathcal{C}'
\end{tikzcd}$$

Abbildung 2.1: Basiswechselsatz

Aus $\varphi = \mathrm{id}_W \circ \varphi \circ \mathrm{id}_V$ folgt die Behauptung mit (2.76) und (2.81)(a). □

(2.83) Korollar (Basiswechselsatz für Endomorphismen)

Sei V K-Vektorraum mit Basen $\mathcal{B}$ und $\mathcal{B}'$ und sei $\varphi \in \mathrm{End}_K(V) = \mathrm{Hom}_K(V,V)$.
Setze $A := M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$, $A' := M_{\mathcal{B}'}^{\mathcal{B}'}(\varphi)$, $T := M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$. Dann gilt:
$A' = T^{-1}AT$.

Beweis

Folgt aus (2.82). □

(2.84) Beispiel

$V = W = \mathbb{R}^2$

$\varphi = \varphi_A$ mit $A = \begin{pmatrix} -\frac{3}{5} & \frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix}$, d.h. $\varphi = \left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = A \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{5}\begin{pmatrix} -3a+4b \\ 4a+3b \end{pmatrix}$.

Gesucht: Einfachere Beschreibung von φ.

$B = (e_1, e_2)$ mit $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

$B' = (v'_1, v'_2)$ mit $v'_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, $v'_2 = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$.

B und B' sind Basen von V.

$\Rightarrow T := M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V) = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$

$T^{-1} = \frac{1}{5} \cdot \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$

$\Rightarrow \frac{1}{5} \cdot T^{-1}AT = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} -\frac{3}{5} & \frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} = \frac{1}{5} \cdot \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$

$= \frac{1}{5} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$\Rightarrow \varphi(v'_1) = v'_1$, $\varphi(v'_2) = -v'_2$, d.h. φ ist die Spiegelung an der Geraden durch $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

$\square$

3 Determinanten

Die DETERMINANTE ist eine Abbildung

$$\det : K^{n\times n} \to K$$

mit „schönen“ Eigenschaften, z.B.:

- $\det(A) \neq 0 \Leftrightarrow A$ invertierbar
- $\det(A\cdot B) = \det(A)\cdot\det(B)$

Zur Einführung der Determinante benötigen wir einige Aussagen über S_n.

§ 1 Das Signum einer Permutation

Sei $n \in \mathbb{N}$.

Erinnerung (vgl. (2.3))

$S_n = \{\pi : \underline{n} \to \underline{n} \mid \pi \text{ ist bijektiv}\}$, $\underline{n} = \{1,\dots,n\}$
Elemente aus S_n heißen PERMUTATIONEN.
S_n ist Gruppe mit „$\circ$“ als Verknüpfung, die SYMMETRISCHE GRUPPE auf n Ziffern.
$\mid S_n \mid = n!$

Schreibweise: $n \in S_n$: $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$

Z.B. für $n = 5$: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$.

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

□

(3.1) Definition

Sei $n \geq 2$: $\tau \in S_n$ heißt TRANSPOSITION (Vertauschung), wenn gilt: es existiert $k \neq l \in \underline{n}$ mit $\tau(k) = l$, $\tau(l) = k$ und $\tau(i) = i$ für alle $i \neq k, l$.
τ vertauscht die Ziffern k und l.
Wir schreiben $(k\ l)$ für τ. □

Z.B. für $n = 5$: $(2\ \ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

(3.2) Bemerkung

Ist $\tau \in S_n$ eine Transposition, dann ist $\tau \neq 1$ $(= \mathrm{id}_{\underline{n}})$ und $\tau^2 = 1$. □

(3.3) Satz

(a) Sei $\tau \in S_n$ Transposition.

$\Rightarrow$ τ ist Produkt einer ungeraden Anzahl von Transpositionen benachbarter Ziffern (d.h. von der Form $(i\ \ i+1)$).

(b) Sei $\pi \in S_n$, $\pi \neq 1$.

$\Rightarrow$ π ist Produkt von Transpositionen benachbarter Ziffern.

Beweis

(a) Sei $\tau = (k\ \ l)$ mit $1 \leq k < l \leq n$. Induktion über $l - k$:

$\underline{l - k = 1}$ ✓

$\underline{l - k > 1}$: $(k\ \ l) = \overset{\tau_3}{(l-1\ \ l)}\overset{\tau_2}{(k\ \ l-1)}\overset{\tau_1}{(l-1\ \ l)}$

$$\begin{array}{ccccccc} l-1 & \xrightarrow{\tau_1} & l & \xrightarrow{\tau_2} & l & \xrightarrow{\tau_3} & l-1 \\ l & \xrightarrow{\tau_1} & l-1 & \xrightarrow{\tau_2} & k & \xrightarrow{\tau_3} & k \\ k & \xrightarrow{\tau_1} & k & \xrightarrow{\tau_2} & l-1 & \xrightarrow{\tau_3} & l \end{array}$$

$(k\ \ l-1)$ erfüllt die Behauptung nach Induktion

$\Rightarrow$ $(k\ \ l)$ erfüllt die Behauptung nach Induktion.

(b) Wegen (a) genügt es zu zeigen:

π ist Produkt von Transpositionen $(*)$.

Beweise $(*)$ durch Induktion über n:

$\underline{n = 2}$: $(1\ \ 2) = (1\ \ 2)$, $1 = (1\ \ 2)(1\ \ 2)$ ✓

$\underline{n \to n+1}$: Sei $\pi \in S_{n+1}$.

1. Fall:

$\pi(n+1) = n+1$.

Definiere $\pi' \in S_n$ durch $\pi'(i) = \pi(i)$ für $1 \leq i \leq n$.

$\underset{\text{Induktion}}{\Rightarrow}$ π' ist Produkt von Transpositionen aus S_n.

$\Rightarrow \pi$ ist Produkt der entsprechenden Transpositionen aus S_{n+1}.

2. Fall:

$\pi(k) = n+1$ für ein k mit $1 \leq k \leq n$.

Sei $\pi' := \pi \cdot (k \;\; n+1) \in S_{n+1}$.

$\Rightarrow \pi'(n+1) = n+1$

$\underset{\text{1. Fall}}{\Rightarrow}$ π' ist Produkt von Transpositionen

$\Rightarrow \pi = \pi' \, (k \;\; n+1)$ ist Produkt von Transpositionen. □

Die Darstellung von $\pi \in S_n$ als Produkt von Transpositionen ist i.A. nicht eindeutig.
Z.B.: $(1 \;\; 2)\,(2 \;\; 3) = (4 \;\; 5)\,(1 \;\; 2)\,(2 \;\; 3)\,(4 \;\; 5)$ in S_5.

(3.4) Definition

Sei $\pi \in S_n$.

(a) Ein Paar (i, j), $1 \leq i < j \leq n$ heißt FEHLSTANDSPAAR (FSP), wenn gilt: $\pi(i) > \pi(j)$.

(b) $\operatorname{sgn}(\pi) := (-1)^{|\{\text{FSP von } \pi\}|} \in \mathbb{Z}$ heißt das SIGNUM VON π. □

(3.5) Beispiele

(a) $\pi = 1$ hat keine FSPs. $\Rightarrow \operatorname{sgn}(\underbrace{1}_{\in S_n}) = \underbrace{1}_{\in \mathbb{Z}}$.

(b) $\tau(i \;\; i+1)$ (mit $i < n$) hat genau ein FSP, nämlich $(i, i+1)$.

$\Rightarrow \operatorname{sgn}(\tau) = -1$ □

(3.6) ! Satz

Seien $\pi, \sigma \in S_n$. Dann gilt:
$\operatorname{sgn}(\pi \;\; \sigma) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\sigma)$
(Mit anderen Worten: $\operatorname{sgn} : S_n \to \{1, -1\} = \mathbb{Z}^*$ ist ein Gruppenhomorphismus.)

Beweis

<u>1. Fall:</u>
$n \geq 2$ und $\sigma = (i \;\; i+1)$ $(i < n)$ ist Transposition benachbarter Ziffern.
$\underset{(3.5)(b)}{\Rightarrow} \operatorname{sgn}(\sigma) = -1$

$$\pi \cdot \sigma = \pi \cdot (i \;\; i+1) = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & i+2 & \dots & n \\ \pi(1) & \dots & \pi(i-1) & \pi(i+1) & \pi(i) & \pi(i+2) & \dots & \pi(n) \end{pmatrix}$$

Es gilt:

(a) $(k,i), k < i$, FSP von $\pi \Leftrightarrow (k,i+1)$ ist FSP von $\pi \cdot \sigma$

(b) $(i,k), k > i+1$, FSP von $\pi \Leftrightarrow (i+1,k)$ ist FSP von $\pi \cdot \sigma$

(c)(d) Analog zu (a)(b) für $i+1$ statt i.

(e) $(i,i+1)$ ist FSP von $\pi \Leftrightarrow (i,i+1)$ ist kein FSP von $\pi \cdot \sigma$

$\underset{(a)-(e)}{\Rightarrow} |\, \{\text{FSP von } \pi\} \,| = |\, \{\text{FSP von } \pi \cdot \sigma\} \,| \pm 1$
$\Rightarrow \operatorname{sgn}(\pi \;\; \sigma) = -\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\sigma)$
<u>2. Fall:</u>
Schreibe $\sigma = \tau_1 \cdots \tau_l$, wobei τ_i für $1 \leq i \leq l$ Transposition benachbarter Ziffern ist (nach (3.3)(b)).
Induktion über l:
<u>$l = 1$</u> : ✓(1. Fall)
<u>$l-1 \to l$</u> : Setze $\sigma' = \tau_1 \cdots \tau_i$

$$\begin{aligned} \Rightarrow \operatorname{sgn}(\pi \;\; \sigma) &= \operatorname{sgn}((\pi \;\; \sigma')\, \tau_l) \\ &= \operatorname{sgn}\left(\pi \;\; \sigma'\right) \cdot \operatorname{sgn}(\tau_l) \text{ (1. Fall)} \\ &= \operatorname{sgn}(\pi) \operatorname{sgn}(\sigma') \operatorname{sgn}(\tau_l) \text{ (Induktion)} \\ &= \operatorname{sgn}(\pi) \operatorname{sgn}\left(\sigma' \;\; \tau_l\right) \text{ (1. Fall)} \\ &= \operatorname{sgn}(\pi) \operatorname{sgn}(\sigma) \end{aligned}$$

□

(3.7) Korollar

Sei $\tau \in S_n$ Transposition.
$\Rightarrow \operatorname{sgn}(\tau) = -1$.

Beweis

Folgt mit (3.3)(a), (3.5)(b), (3.6). □

§ 2 Determinanten

R kommutativer Ring (z.B. $\mathbb{Z}$ oder R Körper), $n \in \mathbb{N}$, $A \in R^{n\times n}$ fassen wir als n-Tupel der Spalten $s_1, \ldots, s_n$ von A auf, d.h. wir schreiben $A = (s_1, \ldots, s_n)$ mit $s_i \in R^n$.

(3.8) Definition

Eine Abbildung $D : R^{n\times n} \to R$ heißt DETERMINANTE, wenn gilt:

(1) D ist *multi-linear*, d.h.

$$\begin{aligned} D(s_1, \ldots, s_{j-1}, a\cdot s_j + b\cdot s'_j, s_{j+1}, \ldots, s_n) = {} & a\cdot D(s_1, \ldots, s_{j-1}, s_j, s_{j+1}, \ldots, s_n) \\ & + b\cdot D(s_1, \ldots, s_{j-1}, s'_j, s_{j+1}, \ldots, s_n) \end{aligned}$$

für alle $1 \le j \le n$ und für alle $a, b \in R$, $s_1, \ldots, s_n, s'_j \in R^n$.

(2) D ist *alternierend*, d.h.

$D(s_1, \ldots, s_n) = 0$, falls $s_i = s_j$ für zwei $i \neq j$.

(3) D ist *normiert*, d.h.

$D(e_1, \ldots, e_n) = 1$ mit $E_n = (e_1, \ldots, e_n)$. □

(3.9) Beispiele

(a) $n = 1$:

$D : R^{1\times 1} \to R$, $(a) \mapsto a$ ist Determinante.

(b) $n = 2$:

$D : R^{2\times 2} \to R$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$ ist Determinante. □

(3.10) Lemma

Sei $D : R^{n\times n} \to R$ eine Determinante und sei $\pi \in S_n$. Dann gilt für alle $s_1, \ldots, s_n \in R^n$:

$$D(s_{\pi(1)}, s_{\pi(2)}, \ldots, s_{\pi(n)}) = \operatorname{sgn}(\pi) \cdot D(s_1, \ldots, s_n)$$

Insbesondere ist $D(s_{\pi(1)}, s_{\pi(2)}, \ldots, s_{\pi(n)}) = -D(s_1, \ldots, s_n)$, falls π Transposition ist.

Beweis

$\pi = 1$: ✓
Sei $\pi = \tau_1 \cdots \tau_n$ mit Transposition τ_i, $1 \leq i \leq l$.
Induktion über l:
$\underline{l=1}: \pi = \tau_1 = (i \;\; j)$ mit $1 \leq i < j \leq n$.

$$\begin{aligned}
0 &\underset{(3.8)(2)}{=} D(s_1, \ldots, \underbrace{s_i + s_j}_{i}, \ldots, \underbrace{s_i + s_j}_{j}, \ldots, s_n) \\
&\underset{(3.8)(1)}{=} D(s_1, \ldots, s_i, \ldots, s_j, \ldots, s_n) + \underbrace{D(s_1, \ldots, s_i, \ldots, s_i, \ldots, s_n)}_{=0} \\
&+ \underbrace{D(s_1, \ldots, s_j, \ldots, s_i, \ldots, s_n)}_{=D(s_{\pi(1)}, \ldots, s_{\pi(i)}, \ldots, s_{\pi(j)}, \ldots, s_{\pi(n)})} + \underbrace{D(s_1, \ldots, s_j, \ldots, s_j, \ldots, s_n)}_{=0}
\end{aligned}$$

$\Rightarrow D(s_{\pi(1)}, \ldots, s_{\pi(n)}) = -D(s_1, \ldots, s_n)$
$\underline{l > 1}: l-1 \mapsto l$
Sei $\pi' = \tau_2 \cdots \tau_l$, d.h. $\pi = \tau_1 \cdot \pi'$.

$$\begin{aligned}
D(s_{\pi(1)}, \ldots, s_{\pi(n)}) &= D(s_{\tau_1 \pi'(1)}, \ldots, s_{\tau_n \pi'(n)}) \\
&= D(s_{\tau_1(\pi'(1))}, \ldots, s_{\tau_n(\pi'(n))}) \\
&\underset{\text{Fall } l=1}{=} -D(s_{\pi'(1)}, \ldots, s_{\pi'(n)}) \\
&\underset{\text{Induktion}}{=} -\operatorname{sgn}(\pi') \cdot D(s_1, \ldots, s_n) \\
&= \operatorname{sgn}(\tau_1 \cdot \pi') \cdot D(s_1, \ldots, s_n)
\end{aligned}$$

□

(3.11) **Satz** (Existenz und Eindeutigkeit der Determinante)

(a) Es existiert genau eine Determinante $D : R^{n \times n} \to R$.

Ist $A = (a_{ij}) \in R^{n \times n}$, also $s_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \in R^n$, dann ist

$$D(s_1, \ldots, s_n) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot a_{\pi(1),1} \cdot a_{\pi(2),2} \cdots a_{\pi(n),n} \qquad (*)$$

($n!$ Summanden, jeder davon mit n Faktoren ($\times$ Vorzeichen).)

(b) Sei $r \in R$ und $D_r : R^{n \times n} \to R$ eine Abbildung, die (3.8)(1),(2) erfüllt und $D_r(e_1, \ldots, e_n) = r$.
$\Rightarrow D_r = r \cdot D$ mit D wie in $(*)$.

Beweis

(b) Wir zeigen zuerst (b). Mit $r = 1$ folgt daraus die Eindeutigkeit in (a).

$$\begin{aligned} D(s_1,\dots,s_n) &= D_r\left(\sum_{i_1=1}^{n} a_{i_1,1} e_{i_1}, s_2,\dots,s_n\right) \\ &\underset{(3.8)(1)}{=} \sum_{i_1=1}^{n} a_{i_1,1}\cdot D_r\left(e_{i_1}, s_2,\dots,s_n\right) \\ &= \sum_{i_1=1}^{n} a_{i_1,1}\cdot D_r\left(e_{i_1}, \sum_{i_2=1}^{n} a_{i_2,2} e_{i_2}, s_3,\dots,s_n\right) \\ &= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n} a_{i_1,1} a_{i_2,2}\cdot D_r\left(e_{i_1}, e_{i_2}, s_3,\dots,s_n\right) \\ &= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_n=1}^{n} a_{i_1,1} a_{i_2,2}\cdots a_{i_n,n}\cdot D_r\left(e_{i_1}, e_{i_2},\dots,e_{i_n}\right) \qquad (**) \end{aligned}$$

$D_r(e_{i_1},\dots,e_{i_n}) \neq 0$ nur, falls $\{i_1,\dots,i_n\} = \{1,\dots,n\}$, d.h. falls $\begin{pmatrix} 1 & 2 & \cdots & n \\ \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} =: \pi \in S_n$ ist.

In diesem Fall ist $D_r(e_{i_1},\dots,e_{i_n}) = D_r(e_{\pi(1)},\dots,e_{\pi(n)}) = \operatorname{sgn}(\pi)\cdot D_r(e_1,\dots,e_n) = \operatorname{sgn}(\pi)\cdot r$.

Zu jedem $\pi \in S_n$ existiert genau ein Summand $a_{\pi(1),1}\cdots a_{\pi(n),n}\cdot D_r(e_{\pi(1)},\dots,e_{\pi(n)})$ in $(**)$.

$$\begin{aligned} \Rightarrow D_r(s_1,\dots,s_n) &= \sum_{\pi\in S_n} a_{\pi(1),1}\cdots a_{\pi(n),n}\cdot D_r(e_{\pi(1)},\dots,e_{\pi(n)}) \\ &= \sum_{\pi\in S_n} a_{\pi(1),1}\cdots a_{\pi(n),n}\cdot \operatorname{sgn}(\pi)\cdot r \end{aligned}$$

(a) <u>Existenz</u>: Sei $D : R^{n\times n} \to R$ die durch $(*)$ definierte Abbildung.

Zu zeigen: D ist Determinante.

<u>(3.8)(1)</u>: Übung.

<u>(3.8)(2)</u>: Beweis für den Fall $i = 1$, $j = 2$, d.h. $s_1 = s_2$. Der allgemeine Fall geht analog.

Sei $\tau = (1\ \ 2) \in S_n$.

Es gilt für $\pi \in S_n : \pi(1) > \pi(2) \Leftrightarrow \pi\tau(1) < \pi\tau(2)$.

Damit ist die Abbildung

$$\{\pi \in S_n \mid \pi(1) > \pi(2)\} \to \{\pi \in S_n \mid \pi(1) < \pi(2)\}, \quad \pi \mapsto \pi\cdot\tau$$

eine Bijektion.

$$\begin{aligned}D(s_1,\dots,s_n) &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\cdot a_{\pi(1),1}\cdots a_{\pi(n),n}\\ &= \underbrace{\sum_{\pi\in A_2} \operatorname{sgn}(\pi)\cdot a_{\pi(1),1}\cdots a_{\pi(n),n}}_{D_2} + \underbrace{\sum_{\pi\in A_1} \operatorname{sgn}(\pi)\cdot a_{\pi(1),1}\cdots a_{\pi(n),n}}_{D_1}\end{aligned}$$

$$\begin{aligned}D_1 &= \sum_{\pi\in A_1} \operatorname{sgn}(\pi)\cdot \underbrace{a_{\pi(1),2}\cdot a_{\pi(2),1}}_{\text{weil } s_1=s_2}\cdot a_{\pi(3),3}\cdots a_{\pi(n),n}\\ &= \sum_{\pi\in A_1} \operatorname{sgn}(\pi)\cdot a_{\pi(2),1}\cdot a_{\pi(1),2}\cdot a_{\pi(3),3}\cdots a_{\pi(n),n}\\ &= \sum_{\pi\in A_1} \operatorname{sgn}(\pi)\cdot a_{\pi\tau(1),1}\cdot a_{\pi\tau(2),2}\cdot a_{\pi\tau(3),3}\cdots a_{\pi\tau(n),n}\\ &= \sum_{\pi\in A_1} \operatorname{sgn}(\pi\tau)\cdot a_{\pi\tau(1),1}\cdot a_{\pi\tau(2),2}\cdot a_{\pi\tau(3),3}\cdots a_{\pi\tau(n),n}\\ &= -\sum_{\pi\in A_2} \operatorname{sgn}(\pi)\cdot a_{\pi(1),1}\cdots a_{\pi(n),n}\\ &= -D_2\end{aligned}$$

(3.8)(3): Klar. □

(3.12) Schreibweisen

Sei $A=(a_{ij})\in R^{n\times n}$.
Wir schreiben $\det(A)$ für die nach (3.11) eindeutig bestimmte Determinante von A und auch $|A| := \det(A)$ oder auch $\begin{vmatrix} a_{11} & \cdots & a_{1n}\\ \vdots & & \vdots\\ a_{n1} & \cdots & a_{nn}\end{vmatrix} := \det(A)$. □

(3.13) Beispiele

(a) $n=2$:

S_2 :

π	$\begin{pmatrix}1&2\\1&2\end{pmatrix}$	$\begin{pmatrix}1&2\\2&1\end{pmatrix}$
$\operatorname{sgn}(\pi)$	1	-1

$$\begin{vmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{vmatrix} = a_{11}a_{22}-a_{21}a_{12}$$

(b) $n = 3$:

S_3 :

π	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
sgn(π)	1	-1	-1	-1

π	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
sgn(π)	1	1

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

□

Regel von Sarrus (für (3×3)-Matrizen)

Schreibe die ersten Spalten neben die Matrix, bilde Produkte entlang der Linien, nehme die Vorzeichen nach folgendem Schema:

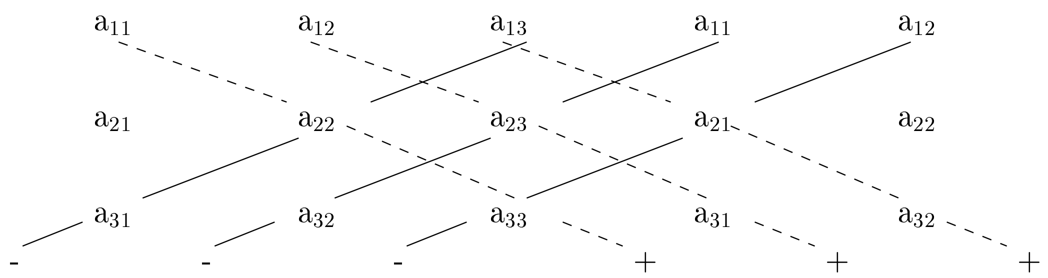

Abbildung 3.1: Regel von Sarrus

Beispiel:

$$\begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ -1 & 0 & 5 \end{vmatrix} = \begin{matrix} 1 & 2 & 3 & 1 & 2 \\ 0 & 1 & 2 & 0 & 1 \\ -1 & 0 & 5 & -1 & 0 \end{matrix} = 5 - 4 + 3 = 4$$

□

§ 3 Rechenregeln und Anwendungen für Determinanten

R kommutativer Ring, $n \in \mathbb{N}$.

(3.14) Bemerkung

Die Abbildung $S_n \to S_n$, $\pi \mapsto \pi^{-1}$ ist bijektiv; für $\pi \in S_n$ gilt:
$\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$

Beweis

Für $\pi \in S_n$ ist $(\pi^{-1})^{-1} = \pi$.
$\Rightarrow$ Abbildung ist bijektiv.
$1 = \operatorname{sgn}(1) = \operatorname{sgn}(\pi \cdot \pi^{-1}) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\pi^{-1})$
$\Rightarrow \operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$, da $\in \{1, -1\}$. □

(3.15) Satz

Sei $A \in R^{n\times n}$.
$\Rightarrow \det(A^t) = \det(A)$.

Beweis

Sei $A = (a_{ij})_{1\leq i,j\leq n}$.
$\Rightarrow A^t = (a_{ij})_{1\leq i,j\leq n}$ mit $a'_{ij} = a_{ij}$.

$$\begin{aligned}
\Rightarrow \det(A^t) &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \cdot a'_{\pi(1),1} \cdots a'_{\pi(n),n} \\
&= \sum_{\pi\in S_n} \underbrace{\operatorname{sgn}(\pi)}_{(3.14)} \cdot \underbrace{a_{1,\pi(1)} \cdots a_{n,\pi(n)}}_{=\text{, da gleiche Faktoren } (*)} \\
&= \sum_{\pi\in S_n} \overbrace{\operatorname{sgn}(\pi^{-1})} \cdot \overbrace{a_{\pi^{-1}(1),1} \cdots a_{\pi^{-1}(n),n}}
\end{aligned}$$

$(*)$ $a_{k,l}$ kommt als Faktor im Produkt $a_{1,\pi(1)} \cdots a_{n,\pi(n)}$ vor $\Leftrightarrow l = \pi(k) \Leftrightarrow \pi^{-1}(l) = k \Leftrightarrow a_{k,l}$ kommt als Faktor im Produkt $a_{\pi^{-1}(1),1} \cdots a_{\pi^{-1}(n),n}$ vor. □

(3.16) Schreibweise

Sei $A = (a_{ij}) \in R^{n\times n}$, sei $n \geq 2$ und seien $i, j \in \underline{n}$. Dann schreiben wir:
$A_{ij} := (a_{k,l})_{\substack{1\leq k\leq n, k\neq i \\ 1\leq l\leq n, l\neq j}} \in R^{(n-1)\times(n-1)}$.
A_{ij} entsteht aus A durch Streichen der i-ten Zeile und der j-ten Spalte. □

(3.17) Lemma

Sei $A = (s_1, \ldots, s_n) \in R^{n\times n}$ (also $s_i \in R^n$) und seien $i, j \in \underline{n}$ $(n \geq 2)$.

$$\Rightarrow \det(\underbrace{s_1,\dots,s_{j-1},e_i,s_{j+1},\dots,s_n}_{\substack{\text{Entsteht aus } A \text{ durch Ersetzen der}\\ j\text{-ten Spalte } s_j \text{ durch die } i\text{-te Spalte}\\ e_i \text{ der Einheitsmatrix.}}}) = (-1)^{i+j}\cdot\det(A_{ij}).$$

Beweis

$(s_1,\dots,s_{j-1},e_i,s_{j+1},\dots,s_n)$ kann durch $n-j$ Spaltentranspositionen und $n-i$ Zeilentranspositionen in die Matrix $B = \left(\begin{array}{c|c} A_{ij} & \begin{matrix}0\\ \vdots\\ 0\end{matrix} \\ \hline * \cdots * & 1\end{array}\right)$ übergeführt werden.

$$\underset{(3.10)}{\Rightarrow} \det(s_1,\dots,s_{j-1},e_i,s_{j+1},\dots,s_n) = (-1)^{n-j+n-i}\cdot\det(B) = (-1)^{i+j}\cdot\det(B).$$

Sei $B = (b_{kl})_{1\le k,l\le n}$.
Für $\pi \in S_n$ ist $b_{\pi(n),n} = 0$, außer für $\pi(n) = n$.
Für $\pi \in S_n$ ist $b_{n,n} = 1$.

$$\begin{aligned}\Rightarrow \det(B) &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\cdot b_{\pi(1),1}\cdots b_{\pi(n-1),n-1}\cdot b_{\pi(n),n}\\ &= \sum_{\substack{\pi\in S_n\\ \pi(n)=n}} \operatorname{sgn}(\pi)\cdot b_{\pi(1),1}\cdots b_{\pi(n-1),n-1}\\ &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\cdot b_{\pi(1),1}\cdots b_{\pi(n-1),n-1}\\ &= \det(A_{ij})\end{aligned}$$

□

(3.18) Satz (Laplace-Entwicklung)

Sei $A = (a_{ij}) \in R^{n\times n}$. Dann gilt:

(a) Entwicklung nach der j-ten Spalte $(1 \le j \le n)$:

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j}\cdot a_{ij}\cdot\det(A_{ij})$$

(b) Entwicklung nach der i-ten Zeile $(1 \le i \le n)$:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j}\cdot a_{ij}\cdot\det(A_{ij})$$

Beweis

(b) Folgt aus (a) durch Transponieren.

(b) Sei $A = (s_1, \ldots, s_n)$, $s_i \in R^n$.

$$
\begin{aligned}
\Rightarrow \det(A) &= \det(s_1, \ldots, s_{j-1}, \sum_{i=1}^{n} a_{ij} e_i, s_{j+1}, \ldots, s_n) \\
&\underset{(3.8)(1)}{=} \sum_{i=1}^{n} a_{ij} \cdot \det(s_1, \ldots, s_{j-1}, e_i, s_{j+1}, \ldots, s_n) \\
&\underset{(3.17)}{=} \sum_{i=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det(A_{ij})
\end{aligned}
$$

□

(3.19) Beispiel

$$
\begin{aligned}
\begin{vmatrix} 1 & 2 & 3 & 4 \\ -1 & -1 & 0 & 1 \\ 4 & 0 & 3 & -1 \\ 2 & 0 & -1 & 1 \end{vmatrix} &= -2 \cdot \begin{vmatrix} -1 & 0 & 1 \\ 4 & 3 & -1 \\ 2 & -1 & 1 \end{vmatrix} + (-1) \cdot \begin{vmatrix} 1 & 3 & 4 \\ 4 & 3 & -1 \\ 2 & -1 & 1 \end{vmatrix} \\
&= -2 \cdot \left((-1) \cdot \begin{vmatrix} 3 & -1 \\ -1 & 1 \end{vmatrix} + 1 \cdot \begin{vmatrix} 4 & 3 \\ 2 & -1 \end{vmatrix} \right) \\
&+ (-1) \cdot \left(1 \cdot \begin{vmatrix} 3 & -1 \\ -1 & 1 \end{vmatrix} - 3 \cdot \begin{vmatrix} 4 & -1 \\ 2 & 1 \end{vmatrix} + 4 \cdot \begin{vmatrix} 4 & 3 \\ 2 & -1 \end{vmatrix} \right) \\
&= \begin{vmatrix} 3 & -1 \\ -1 & 1 \end{vmatrix} - 6 \cdot \begin{vmatrix} 4 & 3 \\ 2 & -1 \end{vmatrix} + 3 \cdot \begin{vmatrix} 4 & -1 \\ 2 & 1 \end{vmatrix} \\
&= 2 - 60 + 18 \\
&= 80
\end{aligned}
$$

□

(3.20) Korollar

Sei $A \in R^{n \times n}$ eine obere Dreiecksmatrix, d.h.:

$$
A = \begin{pmatrix} a_{11} & & & * \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{pmatrix}.
$$

Dann ist $\det(A) = \prod_{i=1}^{n} a_{ii}$.

Beweis

Induktion über n:
$\underline{n=1}$: ✓
$\underline{n-1 \to n}$: Entwickle $\det(A)$ gemäß (3.18)(a) nach der ersten Spalte:

$$\det(A) = a_{11} \cdot \begin{vmatrix} a_{22} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{vmatrix} \underset{\text{Induktion}}{=} a_{11} \cdot \prod_{i=2}^{n} a_{ii}.$$

□

(3.21) Satz (Kästchensatz für Determinanten)

Seien $A_i \in R^{n \times n}$, $1 \leq i \leq m$. Dann gilt:

$$\det \begin{pmatrix} \boxed{A_1} & & & * \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_m} \end{pmatrix} = \prod_{i=1}^{m} \det(A_i).$$

Beweis

Per Induktion können wir $m = 2$ annehmen, d.h. wir betrachten $\det \left(\begin{array}{c|c} A & * \\ \hline 0 & B \end{array} \right)$ mit $A \in R^{n \times n}$, $B \in R^{l \times l}$.
Induktion über n:

$\underline{n=1}$: Behauptung folgt aus (3.18)(a): $\left(\begin{array}{c|ccc} \square & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array} \right)$.

$\underline{n>1}$: Sei $C = \left(\begin{array}{c|c} A & * \\ \hline 0 & B \end{array} \right)$.

$\Rightarrow C_{i1} = \left(\begin{array}{c|c} A_{i1} & * \\ \hline 0 & B \end{array} \right)$, $1 \leq i \leq n$.

$$\begin{aligned} \underset{(3.18)(\mathrm{a})}{\Rightarrow} \det(C) &= \sum_{i=1}^{n+l} (-1)^{i+1} \cdot \underbrace{c_{i1}}_{=0 \text{ für } i>n} \cdot \det(C_{i1}) \\ &= \sum_{i=1}^{n} (-1)^{i+1} \cdot a_{i1} \cdot \det \left(\begin{array}{c|c} A_{i1} & * \\ \hline 0 & B \end{array} \right) \\ &\underset{\text{Induktion}}{=} \sum_{i=1}^{n} (-1)^{i+1} \cdot a_{i1} \cdot \det(B) \\ &\underset{(3.18)(\mathrm{a})}{=} \det(A) \cdot \det(B) \end{aligned}$$

□

(3.22) Satz (Multiplikationssatz für Determinanten)

Sei $A, B \in R^{n\times n}$. Dann gilt:
$\det(A \cdot B) = \det(A) \cdot \det(B)$.

Beweis

Sei $a = \det(A) \in R$.
Betrachte $D_a : R^{n\times n} \to R$, $C \mapsto \det(A \cdot C)$.
Sei $C = (s_1, \ldots, s_n) \in R^{n\times n}$, d.h. $s_i \in R^n$.
$\Rightarrow A \cdot C = (A \cdot s_1, \ldots, A \cdot s_n)$
$\Rightarrow D_a$ erfüllt die Bedingungen aus (3.8)(1),(2) und es gilt: $D_a(E_n) = \det(A) = a$.
$\underset{(3.11)(\mathrm{b})}{\Rightarrow} D_a = a \cdot \det$
$\Rightarrow \det(A \cdot B) = a \cdot \det(B) = \det(A) \cdot \det(B)$. □

(3.23) Korollar

Seien $A, T \in R^{n\times n}$, T invertierbar. Dann gilt:

(a) $\det(T), \det(T^{-1}) \in R^*$ und $\det(T^{-1}) = \det(T)^{-1}$.

(b) $\det(T^{-1} \cdot A \cdot T) = \det(A)$.

Beweis

(b) Folgt aus (a) und (3.22).

(a) $1 = \det(E_n) = \det(T^{-1} \cdot T) = \det(T^{-1}) \cdot \det(T)$
$\Rightarrow \det(T), \det(T^{-1})$ sind invertierbar (in R) und $\det(T^{-1}) = \det(T)^{-1}$. □

(3.24) Definition

Sei $A \in R^{n\times n}$.
$\tilde{A} := \left((-1)^{i+j} \cdot \det(A_{ji})\right)_{1\le i,j\le n} \in R^{n\times n}$ heißt die zu A KOMPLEMENTÄRE MATRIX (oder ADJUNKTE MATRIX).
$\left[A_{ji}\right.$ ist in (3.16) definiert; beachte die vertauschten Indizes.$\left.\right]$
□

(3.25) Beispiel

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tilde{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
$A \cdot \tilde{A} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \det(A) \cdot E_2$. □

(3.26) Satz

Sei $A \in R^{n \times n}$. Dann gilt:
$A \cdot \tilde{A} = \det(A) \cdot E_n = \tilde{A} \cdot A$.

Beweis

Nur für $A \cdot \tilde{A}$. Der Beweis für $\tilde{A} \cdot A$ geht analog.
Sei $A = (a_{ij}), \tilde{A} = (\tilde{a}_{ij}), A \cdot \tilde{A} = (c_{ij})$.
$c_{ij} = \sum\limits_{k=1}^{n} a_{ik} \cdot \tilde{a}_{kj} = \sum\limits_{k=1}^{n} a_{ik} \cdot (-1)^{k+j} \cdot \det(A_{jk})$.
<u>1. Fall:</u> $i = j$:
$\Rightarrow c_{ii} = \sum\limits_{k=1}^{n} a_{ik} \cdot (-1)^{k+i} \cdot \det(A_{ik}) \underset{(3.18)(b)}{=} \det(A)$.
<u>2. Fall:</u> $i \neq j$:
Sei $A' = (a'_{kl})$ die Matrix, die aus A entsteht, indem die j-te Zeile durch die i-te ersetzt wird.
$\Rightarrow \det(A') = 0$ ((3.8)(2) + (3.15))
Aus (3.18)(b) (Entwicklung nach der j-ten Zeile) folgt:

$$\begin{aligned} 0 = \det(A') &= \sum_{k=1}^{n} (-1)^{j+k} \cdot a'_{jk} \cdot \det(A'_{jk}) \\ &= \sum_{k=1}^{n} (-1)^{j+k} \cdot a_{ik} \cdot \det(A_{jk}) \\ &= c_{ij} \end{aligned}$$

□

(3.27) Korollar

Sei $A \in R^{n \times n}$. Dann gilt:

(a) A invertierbar $\Leftrightarrow \det(A)$ invertierbar.

(b) Ist R ein Körper, dann gilt:

A invertierbar $\Leftrightarrow \det(A) \neq 0$.

Beweis

(b) Folgt aus (a).

(a) „$\Rightarrow$“: (3.23)(a)

„$\Leftarrow$“: Aus (3.26) folgt: $A \cdot (\det(A)^{-1} \cdot \tilde{A}) = E_n = (\det(A)^{-1} \cdot \tilde{A}) \cdot A$. □

(3.28) Satz (Cramersche Regel)

Sei K ein Körper, $A = (a_{ij}) \in K^{n \times n}$ mit $\det(A) \neq 0$.
Nach (3.27)(b) ist A invertierbar.
Sei $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in K^n$.

Nach (2.67)(5) hat das LGS $Ax = b$ genau eine Lösung $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$. Hierfür gilt:

$$c_j = \frac{1}{\det(A)} \cdot \begin{vmatrix} a_{11} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2,j-1} & b_2 & a_{2,j+1} & \cdots & a_{2n} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{nn} \end{vmatrix}$$

(Ersetze j-te Spalte von A durch b.)

Beweis

Seien $s_1, \dots, s_n$ die Spalten von A.
Es ist $b = A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \sum\limits_{i=1}^{n} c_i \cdot s_i$.

$$\underset{(3.8)(1)}{\Rightarrow} \det(s_1, \dots, s_{j-1}, b, s_{j+1}, \dots, s_n) = \sum_{i=1}^{n} c_i \cdot \underbrace{\det(s_1, \dots, s_{j-1}, s_i, s_{j+1}, \dots, s_n)}_{=0,\text{ außer für } i=j} = c_j \cdot \det(A). \qquad \square$$

4 Eigenwerte und Eigenvektoren

§ 1 Der Polynomring

Sei K ein Körper.
$\sum_{i=0}^{n} a_i X^i$: „formale" Linearkombination, X: Unbestimmte.

(4.1) Definition

(a) Ein K-VR V heißt K-ALGEBRA, falls eine Verknüpfung $\cdot : V \times V \to V$ definiert ist, so dass gilt:

(1) $(V, +, \cdot)$ ist ein Ring.

(2) $a \cdot (v \cdot v') = (a \cdot v) \cdot v' = v \cdot (a \cdot v')$ für alle $a \in K$, v, $v' \in V$.

(b) Seien V, W K-Algebren.

Ein Homo-(Epi-, Mono-, Iso-)morphismus $\varphi : V \to W$ heißt K-ALGEBREN-HOMO-(EPI-, MONO-, ISO-)MORPHISMUS, falls gilt:

$\varphi(\underbrace{1}_{1 \in V}) = \underbrace{1}_{1 \in W}$, $\varphi(v \underbrace{\cdot}_{\cdot \in V} v') = \varphi(v) \underbrace{\cdot}_{\cdot \in W} \varphi(v')$ für alle v, $v' \in V$. □

(4.2) Beispiel

$K^{n \times n}$ ist K-Algebra (mit Matrixmultiplikation). □

(4.3) Definition

Ein Paar (P, X) heißt POLYNOMRING *in der Unbestimmten X über K*, falls gilt:

(a) P ist K-Algebra.

(b) $\{1 =: X^0, X = X^1, X^2 = X \cdot X, X^3, \ldots\}$ ist K-Basis von P und unendlich. □

(4.4) Bemerkung

Sei (P,X) Polynomring über K.

(a) Jedes $f \in P$ besitzt eine eindeutige Darstellung als Linearkombination

$$f = \sum_{i=0}^{n} a_i X^i \text{ mit } a_i \in K, a_n \neq 0 \tag{*}$$

(b) Seien $f = \sum_{i=0}^{m} a_i X^i$, $g = \sum_{i=0}^{n} b_i X^i \in P$, dann ist

$$f \cdot g = \sum_{k=0}^{m+n} c_k X^k \text{ mit } c_k = \sum_{l=0}^{k} a_l b_{k-l}$$

Beweis

(a) Folgt aus (4.3)(b).

(b) Distributivgesetz in einem Ring, zusammen mit (4.1)(a)(2). □

(4.5) Bemerkung

Bis auf K-Algebren-Isomorphismus existiert genau ein Polynomring über K in der Unbestimmten X. Dieser wird mit $K[X]$ bezeichnet.

Beweis

(1) Existenz (vgl. Aufgabe 6, Übungsblatt 7):

$K^{(\mathbb{N}_0)} := \{f : \mathbb{N}_0 \to K \mid f(i) = 0 \text{ für fast alle } i \in \mathbb{N}_0\}$

$([f(0), f(1), \ldots, f(n)]$, falls $f(i) = 0$ für alle $i > n)$

$K^{(\mathbb{N}_0)}$ ist K-VR, $* : K^{(\mathbb{N}_0)} \to K^{(\mathbb{N}_0)}$ sei definiert durch $f * g := \sum_{l=0}^{k} f(l) g(k-l)$, $k \in \mathbb{N}_0$.

$X := [0, 1, 0, \ldots] \in K^{(\mathbb{N}_0)}$.

$\Rightarrow \left(K^{(\mathbb{N}_0)}, X\right)$ ist Polynomring.

(2) Seien (P,X), (Q,Y) Polynomringe über K.

$\varphi : P \to Q$, $\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} a_i Y^i$ ist ein K-Algebren-Isomorphismus. □

(4.6) Definition

Sei $f = \sum_{i=0}^{m} a_i X^i \in K[X]$, $f \neq 0$, $a_m \neq 0$.
$\deg(f) := m$ heißt der GRAD von f.
a_m, a_0 heißen HÖCHSTER bzw. KONSTANTER KOEFFIZIENT von f.
f heißt NORMIERT, falls $a_m = 1$.
f heißt KONSTANT, falls $f = a_0 \cdot 1$, d.h. falls $\deg(f) = 0$.
f heißt LINEAR, falls $\deg(f) = 1$. □

Konvention

Das Nullpolynom ist auch konstant.
$f = 0$ hat keinen Grad. □

(4.7) Bemerkung

Seien $0 \neq f, g \in K[X]$.

(a) $f + g \neq 0 \Rightarrow \deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
$\deg(f) \neq \deg(g) \Rightarrow deg(f+g) = \max\{\deg(f), \deg(g)\}$

(b) $\deg(f \cdot g) = \deg(f) + \deg(g)$. Insbesondere ist $f \cdot g \neq 0$.

Beweis

(a) Klar.

(b) Seien a_m bzw. b_n die höchsten Koeffizienten von f bzw. g, dann ist $a_m b_m$ der höchste Koeffizient von $f \cdot g$. □

Wir betrachten K als Teilmenge von $K[X]$, indem wir $a \in K$ als konstantes Polynom $a \cdot 1 \in K[X]$ auffassen.

(4.8) Bemerkung

$K[X]^* = K^* = \{a \in K \mid a \neq 0\}$

Beweis

Sei $f = K[X]^*$, d.h. es existiert $g \in K[X]$ mit $f \cdot g = 1$.
$\underset{(4.7)(b)}{\Rightarrow} 0 = \deg(f \cdot g) = \deg(f) + \deg(g)$
$\Rightarrow \deg(f) = 0$, d.h. $f \in K^*$. □

(4.9) **Satz** (Division mit Rest in $K[X]$)

Seien $f, g \in K[X], g \neq 0$.
Dann existieren eindeutig bestimmte $q, r \in K[X]$ mit $f = q \cdot g + r$ und $r = 0$ oder $\deg(r) < \deg(g)$.

Beweis (algorithmisch)

Existenz: $f = 0$. Setze $q = r = 0$.
Seien a_m bzw. b_n die höchsten Koeffizienten von f bzw. g.
Ist $m < n$, setze $q = 0$, $r = f$.
Ist $m \geq n$, setze $f_1 := f - \frac{a_m}{b_n} \cdot X^{m-n} \cdot g$.
$\Rightarrow f_1 = 0$ oder $\deg(f_1) < m$.
$\underset{\text{Induktion}}{\Rightarrow}$ es existieren $q_1, r \in K[X]$ mit $f_1 = q_1 \cdot g + r$ und $r = 0$ oder $\deg(r) < \deg(g)$.
$\Rightarrow q := q_1 + \frac{a_m}{b_n} \cdot X^{m-n}$ und r erfüllen das Gewünschte.
Eindeutigkeit: Sei $q \cdot g + r = f = q' \cdot g + r'$ mit $q, r, q', r' \in K[X]$ und $r, r' = 0$ oder $\deg(r) < \deg(q)$, $\deg(r') < \deg(q')$.
$\Rightarrow (q - q') \cdot g = r' - r$
Angenommen: $q \neq q'$ (d.h. $q - q' \neq 0$).
$\Rightarrow r - r' \neq 0$ und es gilt:
$\deg(q - q') + deg(g) = deg((q - q') \cdot g) = \det(r - r') < \deg(g)$ ↯
$\Rightarrow q - q' = 0$, $r - r' = 0$. □

(4.10) Definition

Seien $f, g \in K[X]$.

(a) g TEILT f, geschrieben $g \mid f$, falls $h \in K[X]$ existiert mit $f = g \cdot h$.

(b) Seien $f, g \neq 0$.

f, g heißen TEILERFREMD, falls gilt:

Ist $h \in K[X]$ mit $h \mid f$ und $h \mid g$, dann ist $h \in K$.

(c) f heißt IRREDUZIBEL, falls gilt:

$f \neq 0$, $\deg(f) \geq 1$ und ist $f = g \cdot h$ mit $g, h \in K[X]$, dann ist $\deg(g) = 0$ oder $\deg(h) = 0$. □

(4.11) ! Satz

Seien $0 \neq f, g \in K[X]$. Dann gilt:
f, g teilerfremd $\Leftrightarrow$ es existieren $h, k \in K[X]$ mit $1 = f \cdot h + g \cdot k$

Beweis

„$\Leftarrow$": Sei $d \in K[X]$ mit $d \mid f$ und $d \mid g \Rightarrow d \mid f \cdot h + g \cdot k = 1$, d.h. $d \in K$ (vgl. (4.7))
„$\Rightarrow$": Sei $I := \{f \cdot h + g \cdot k \mid h,k \in K[X]\}$ und sei $0 \neq d \in I$ von minimalem Grad.
Behauptung: $d \mid y$ für alle $y \in I$.
Beweis: Sei $y \in I$.
Nach (4.9) existieren $q,r \in K[X]$ mit $y = q \cdot d + r$ und $r = 0$ oder $\deg(r) < \deg(d)$.
$y,d \in I \Rightarrow q \cdot d, y - q \cdot d = r \in I \Rightarrow r = 0$ (nach Wahl von d)
$\Rightarrow$ Behauptung
$f,g \in I \underset{\text{Behauptung}}{\Rightarrow} d \mid f$ und $d \mid g \underset{(4.10)(b)}{\Rightarrow} d \in K, d \neq 0$
$\Rightarrow 1 = d^{-1} \cdot d \in I$ $\square$

(4.12) Korollar

Sei $p \in K[X]$ irreduzibel, $f, g \in K[X]$ mit $p \mid f \cdot g$.
$\Rightarrow p \mid f$ oder $p \mid g$.

Beweis

Angenommen: $p \nmid f$.
$\Rightarrow p, f$ teilerfremd. ((4.10)(b), (4.10)(c))
$\underset{(4.11)}{\Rightarrow}$ es existieren $h,k \in K[X]$ mit $1 = f \cdot h + p \cdot k$
$\Rightarrow g = g \cdot 1 = (f \cdot g) \cdot h + p \cdot (g \cdot k)$
$\Rightarrow p \mid (f \cdot g) \cdot h,\ p \mid p(g \cdot k) \Rightarrow p \mid g$. $\square$

$\rightsquigarrow$ Eindeutige „Primfaktorzerlegung" in $K[X]$

(4.13) ! Satz

Sei $0 \neq f \in K[X]$, $\deg(f) \neq 0$ mit höchstem Koeffizienten $a \in K$.
Dann existieren irreduzible, normierte $p_1, \dots, p_t \in K[X]$ mit $f = a \cdot p_1 \cdots p_t$.
Die $p_1, \dots, p_t$ sind eindeutig (bis auf Reihenfolge) durch f bestimmt.

Beweis

Existenz: Induktion über $\deg(f)$.
f irreduzibel $\Rightarrow a^{-1} \cdot f$ irreduzibel, normiert ✓
f nicht irreduzibel $\Rightarrow$ es existieren $g,h \in K[X]$ mit $f = g \cdot h$ und $\deg(g), \deg(h) < \deg(f)$.
Fertig mit Induktion.
Eindeutigkeit: zu zeigen:
Behauptung: Seien $p_1, \dots, p_t, q_1, \dots q_s \in K[X]$ irreduzibel, normiert mit $p_1 \cdots p_t = q_1 \cdots q_s$.
$\Rightarrow s = t$ und es existiert $\pi \in S_t$ mit $q_i = p_{\pi(i)}$, $1 \leq i \leq t$.
Beweis:

$p_1 \cdots p_t = q_1 \cdots q_s \Rightarrow p_1 \mid q_1 \cdot (q_2 \cdots q_s)$
$\underset{\text{(4.12) und Induktion über } s}{\Rightarrow}$ es existiert j, $1 \le j \le s$ mit $p_1 \mid q_j$.
$\Rightarrow p_1 = q_j$ (da p_1, q_j irreduzibel, normiert)
$\Rightarrow p_1 \cdot (p_2 \cdots p_t - q_1 \cdots q_{j-1} \cdot q_{j+1} \cdots q_s) = 0$
$\underset{\text{(4.7)(b)}}{\Rightarrow} p_2 \cdots p_t = q_1 \cdots q_{j-1} \cdot q_{j+1} \cdots q_s$
$\Rightarrow$ Behauptung (Induktion über s) $\square$

(4.14) Bemerkung und Definition

Sei V K-Algebra, $v \in V$.
Dann existiert genau ein K-Algebren-Homomorphismus $\tau_v : K[X] \to V$ mit $\tau_v(X) = v$.
τ heißt EINSETZUNGSHOMOMORPHISMUS.
Für $f \in K[X]$ schreiben wir $f(x) := \tau_v(f)$.

Beweis

Eindeutigkeit: Ist $\tau_v : K[X] \to V$ ein K-Algebren-Homomorphismus mit $\tau_v(X) = v$, dann gilt für $f = \sum\limits_{i=0}^{n} a_i X^i \in K[X]$:

$$\tau_v(f) \underset{\tau_v\ K\text{-linear}}{=} \sum_{i=0}^{n} a_i \cdot \underbrace{\tau_v(X^i)}_{=\tau_v(X)^i} = \sum_{i=0}^{n} a_i v^i.$$

Beachte: $v^0 = \tau_v(\underbrace{X^0}_{1 \in K[X]}) = \tau_v(1) = 1 \in V$.

Existenz: Für $f = \sum\limits_{i=0}^{m} a_i X^i \in K[X]$ definiere $\tau_v(f) = \sum\limits_{i=0}^{m} a_i v^i$ (mit $v^0 := 1 \in V$).
$\Rightarrow \tau_v \in \mathrm{Hom}_K(K[X], V)$ und $\tau_v(f \cdot g) = \tau(f) \cdot \tau(g)$. $\square$

(4.15) Beispiele

$f = \sum\limits_{i=0}^{m} a_i X^i$

(a) $V = K$ ($\cong K^{1\times 1}$), $a \in K$.

$$f(a) = \sum_{i=0}^{m} a_i a^i \in K \quad (a^0 = 1 \in K).$$

(b) $V = K^{n\times n}$, $a \in K^{n\times n}$.

$$f(A) = \sum_{i=0}^{m} a_i A^i \in K^{n\times n} \quad (A^0 = E_n \in K)$$

$[f = X^2 + X + 1 \Rightarrow f(A) = A^2 + A + E_n]$ $\square$

(4.16) Definition

Sei $f \in K[X]$, $a \in K$.
a NULLSTELLE, falls $f(a) = 0$. □

(4.17) Bemerkung

Sei $f \in K[X]$, $a \in K$ Nullstelle von f.
$\Rightarrow$ es existiert $q \in K[X]$ mit $f = (X - a) \cdot q$.

Beweis

Es existieren $q, r \in K[X]$ mit $f = (X - a) \cdot q + r$ und $r = 0$ oder $\deg(r) < \deg(X - a) = 1$.
$\Rightarrow r \in K$
$\Rightarrow 0 = f(a) = (a - a) \cdot q(a) + r(a) = 0 \cdot q(a) + r$. □

(4.18) Definition und Bemerkung

Sei $0 \neq f \in K[X]$, $a \in K$ Nullstelle von f.
$\Rightarrow$ es existiert ein eindeutig bestimmtes $m \in \mathbb{N}$ und es existiert $g \in K[X]$ mit $f = (X - a)^m \cdot g$ und $g(a) \neq 0$.
m heißt die VIELFACHHEIT *von a als Nullstelle von f.*

Beweis

Existenz und Eindeutigkeit folgen aus (4.13) und (4.17), denn $X - a$ ist irreduzibel. □

(4.19) Definition

K heißt ALGEBRAISCH ABGESCHLOSSEN, falls jedes $f \in K[X]$, $f \notin K$, eine Nullstelle in K hat. □

(4.20) Satz

$\mathbb{C}$ ist algebraisch abgeschlossen (hier ohne Beweis; FUNDAMENTALSATZ DER ALGEBRA). □

(4.21) Bemerkung

Sei K alg. abg. und $f \in K[X]$ irreduzibel, normiert.
$\Rightarrow f = X - a$ für ein $a \in K$.

Beweis

f irreduzibel $\Rightarrow \deg(f) \geq 1$
$\underset{(4.19)}{\Rightarrow}$ es existiert $a \in K$ mit $f(a) = 0$
$\underset{(4.17)}{\Rightarrow} X - a \mid f \underset{f \text{ irreduzibel, normiert}}{\Rightarrow} f = X - a.$ □

§ 2 Eigenwerte und Eigenvektoren

K Körper, V e.d. K-VR, $\mathrm{End}_K(V)$ $[\mathrm{End}_K(V) = \mathrm{Hom}_K(V,V)]$

(4.22) ! Definition

Sei $\varphi \in \mathrm{End}_K(V)$, $A \in K^{n \times n}$.

(1) $a \in K$ heißt EIGENWERT (EW) von φ (bzw. A), falls ein $0 \neq v \in V$ (bzw. $0 \neq v \in K^n$) existiert mit $\varphi(v) = a \cdot v$ (bzw. $A \cdot v = a \cdot v$).

[Erinnerung: $\varphi_A : K^n \to K^n, v \mapsto A \cdot v$]

(2) $0 \neq v \in V$ (bzw. $0 \neq v \in K^n$) heißt EIGENVEKTOR (EV) von φ (bzw. A) zum Eigenwert $a \in K$, falls $\varphi(v) = a \cdot v$ (bzw. $A \cdot v = a \cdot v$) ist.

(3) Für $a \in K$ sei

$$V(a,\varphi) := \{v \in V \mid \varphi(v) = a \cdot v\} = \{v \in V \mid (a \cdot \mathrm{id}_V - \varphi)(v) = 0\} = \mathrm{Kern}(a \cdot \mathrm{id}_V - \varphi)$$

bzw.

$$V(a,A) := \{v \in K^n \mid A \cdot v = a \cdot v\} = V(a, \varphi_A).$$

Ist $V(a,\varphi) \neq \{0\}$ (bzw. $V(a,A) \neq \{0\}$), dann heißt $V(a,\varphi)$ (bzw. $V(a,A)$) der EIGENRAUM von φ (bzw. A) zum Eigenwert a. □

(4.23) Bemerkung

Bezeichnungen wie in (4.22).

(a) $a \in K$ EW von $\varphi \Leftrightarrow V(a,\varphi) \neq \{0\}$.

(b) $V(a,\varphi) \neq \{0\} \Rightarrow$ jedes $0 \neq v \in V(a,\varphi)$ ist EV von φ zum EW a.

(c) $V(0,\varphi) = \mathrm{Kern}(\varphi)$

0 ist EW von $\varphi \Leftrightarrow \mathrm{Kern}(\varphi) \neq \{0\} \Leftrightarrow \varphi$ nicht injektiv $\underset{V \text{ e.d.}}{\Leftrightarrow} \varphi$ nicht bijektiv. □

Schreibweise

Sei $\mathcal{B}$ (geordnete) Basis von V, $\varphi \in \mathrm{End}_K(V)$.
$M_{\mathcal{B}}(\varphi) := M_{\mathcal{B}}^{\mathcal{B}}(\varphi) \in K^{n \times n}$. □

(4.24) Beispiele

(a) $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$, $\varphi_A : \mathbb{R}^2 \to \mathbb{R}^2$.

$\varphi_A(e_1) = e_2$, $\varphi_A(e_2) = e_1$

φ_A: Spiegelung an $< e_1 + e_2 >$.

φ_A hat die EW 1 und -1.

$\varphi_A(e_1 + e_2) = e_1 + e_2$, d.h. $e_1 + e_2 \in V(1, A)$.

$\varphi_A(e_1 - e_2) = -(e_1 - e_2)$, d.h. $e_1 - e_2 \in V(-1, A)$.

$(e_1 - e_2, e_1 + e_2)$ ist l.u.

$\Rightarrow \mathcal{B}' = (e_1 - e_2, e_1 + e_2)$ ist Basis von $\mathbb{R}^2$.

$M_{\mathcal{B}'}(\varphi_A) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

$V(1, A) =< e_1 + e_2 >$, $V(-1, A) =< e_1 - e_2 >$.

(b) Sei $\dim_K(V) = n \geq 2$, $\varphi \in \mathrm{End}_K(V)$. Es gelte $1 + 1 \neq 0$ in K. φ heißt SPIEGELUNG, falls gilt:

1, -1 sind EW von φ und $\dim_K(V(1, \varphi)) = n - 1$.

Sei $0 \neq v_1 \in V(-1, \varphi)$, d.h. $\varphi(v_1) = -v_1$ und sei $(v_2, \ldots, v_n)$ eine Basis von $V(1, \varphi)$.

$\Rightarrow v_1 \notin < v_2, \ldots, v_n >= V(1, \varphi)$, d.h. $\mathcal{B} := (v_1, v_2, \ldots, v_n)$ ist Basis von V. Es gilt:

$$M_{\mathcal{B}}(\varphi) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Wir sagen auch: φ ist Spiegelung an $V(1, \varphi)$. □

(4.25) Definition

$A = (a_{ij}) \in K^{n \times n}$ heißt DIAGONALMATRIX, falls $a_{ij} = 0$ für alle $i \neq j$.

$$A = \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix}.$$ □

(4.26) Definition

Sei $\varphi \in \mathrm{End}_K(V)$, $A \in K^{n\times n}$.

(a) φ heißt DIAGONALISIERBAR, falls Basis $\mathcal{B}$ von V existiert, so dass $M_{\mathcal{B}}(\varphi)$ eine Diagonalmatrix ist.

(b) A heißt DIAGONALISIERBAR, falls $T \in \mathrm{GL}_n(K)$ existiert, so dass $T^{-1}\cdot A\cdot T$ eine Diagonalmatrix ist. □

(4.27) Bemerkung

Bezeichnungen wie in (4.26).

(a) φ diagonalisierbar $\Leftrightarrow V$ besitzt Basis aus EV von φ.

(b) A diagonalisierbar $\Leftrightarrow \varphi_A$ diagonalisierbar.

Beweis

(a) „$\Rightarrow$": Sei $\mathcal{B} = (v_1,\dots,v_n)$ Basis von φ mit $M_{\mathcal{B}}(\varphi) = \begin{pmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n \end{pmatrix}$.

$\underset{(2.72)}{\Rightarrow}$ $\varphi(v_j) = a_j \cdot v_j$, $1 \le j \le n$, d.h. v_j ist EV von φ mit EW a_j.

„$\Leftarrow$": Genauso mit (2.72).

(b) Sei $\mathcal{B} = (e_1,\dots,e_n)$ die Standardbasis von K^n.

$\Rightarrow M_{\mathcal{B}}(\varphi_A) = A$ (nach (2.73)(c)).

Ist $\mathcal{B}'$ eine andere Basis von K^n und $T := M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$ die Basiswechselmatrix, dann gilt:

$M_{\mathcal{B}'}(\varphi_A) = T^{-1}\cdot A\cdot T$ (vgl. (2.83))

$\Rightarrow$ Behauptung □

(4.28) Definition

$A, B \in K^{n\times n}$ heißen ÄHNLICH, falls $T \in \mathrm{GL}_n(K)$ existiert mit $B = T^{-1}\cdot A\cdot T$. □

Nach (2.83): ähnliche Matrizen beschreiben den gleichen Endomorphismus, nur bzgl. verschiedener Basen.
$A \in K^{n\times n}$ diagonalisierbar $\Leftrightarrow A$ ähnlich zu einer Diagonalmatrix.

(4.29) Satz

Sei $\varphi \in \mathrm{End}_K(V)$, $\dim_K(V) = n$.

(a) Seien $a_1, \ldots, a_m \in K$ EW von φ mit $a_i \neq a_j$ für $i \neq j$. Seien $v_j \in V$ EV von φ zum EW a_j, $1 \leq j \leq m$. $\Rightarrow (v_1, \ldots, v_m)$ l.u.

(b) Besitzt φ n paarweise verschiedene EW, dann ist φ diagonalisierbar.

Beweis

(b) Folgt aus (a) mit (4.27)(a).

(a) Induktion über m:

$\underline{m = 1}$: Klar, da $v_1 \neq 0$.

$\underline{m > 1, m-1 \mapsto m}$: Seien $b_j \in K$, $1 \leq j \leq m$ mit $\sum_{j=1}^{m} b_j \cdot v_j = 0$. Es gilt:

$$\begin{aligned}
0 &= (\varphi - a_m \cdot \mathrm{id}_V)(0) \\
&= (\varphi - a_m \cdot \mathrm{id}_V)\left(\sum_{j=1}^{m} b_j \cdot v_j\right) \\
&= \sum_{j=1}^{m} b_j \cdot (\varphi - a_m \cdot id_V)(v_j) \\
&= \sum_{j=1}^{m} b_j \cdot (\varphi(v_j) - a_m \cdot v_j) \\
&= \sum_{j=1}^{m-1} b_j \cdot (a_j - a_m) \cdot v_j
\end{aligned}$$

$\underset{\text{Induktion}}{\Rightarrow} b_j \cdot (a_j - a_m) = 0$ für $1 \leq j \leq m-1$.

$a_j - a_m \neq 0$ für $1 \leq j \leq m-1$

$\Rightarrow b_j = 0$ für $1 \leq j \leq m-1$

$\Rightarrow b_m \cdot v_m = 0$

$\Rightarrow b_m = 0$, da $v_m \neq 0$ □

(4.30) Beispiel

$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ ist nicht diagonalisierbar.

Beweis

Angenommen, A wäre diagonalisierbar.
Sei $T \in \mathrm{GL}_2(\mathbb{R})$ mit $T^{-1} \cdot A \cdot T = B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.
$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow \begin{pmatrix} a^2 & 0 \\ 0 & b^2 \end{pmatrix} = B^2$
$= T^{-1} \cdot A \cdot T \cdot T^{-1} \cdot A \cdot T = T^{-1} \cdot A^2 \cdot T = T^{-1} \cdot \underbrace{(-1) \cdot E_2}_{=A^2} \cdot T = (-1) \cdot T^{-1} \cdot T = -E_2$

$\Rightarrow a^2 = b^2 = -1$ ↯ □

Sei $A \in K^{n \times n}$, $0 \in K$.
a EW von $A \Leftrightarrow$ es existiert $0 \neq v \in K^n$ mit $A \cdot v = a \cdot v \Leftrightarrow$ es existiert $0 \neq v \in K^n$ mit $(a \cdot E_n - A) \cdot v = 0 \underset{(2.65)(\mathrm{d})}{\Leftrightarrow} a \cdot E_n - A$ nicht invertierbar $\underset{(3.27)(\mathrm{b})}{\Leftrightarrow} \det(a \cdot E_n - A) = 0$.

§ 3 Das charakteristische Polynom

Sei K ein Körper.

(4.31) Definition und Bemerkung

(a) Sei $A \in K^{n \times n}$.

(1) $X \cdot E_n - A \in K[X]^{n \times n}$ heißt die CHARAKTERISTISCHE MATRIX von A.

(2) $\chi_A := \det(X \cdot E_n - A) \in K[X]$ heißt das CHARAKTERISTISCHE POLYNOM von A.

(3) Sei $T \in \mathrm{GL}_n(K)$. Dann gilt:
$\chi_{T^{-1} \cdot A \cdot T} = \chi_A$.

(b) Sei V ein n-dim. K-VR, $\varphi \in \mathrm{End}_K(V)$, B Basis von V, $A := M_B(\varphi) \in K^{n \times n}$.
Dann heißt $\chi_\varphi := \chi_A$ das CHARAKTERISTISCHE POLYNOM von φ.
Dies ist unabhängig von der gewählten Basis.

Beweis

(a) (3)

$$\begin{aligned} \chi_{T^{-1} \cdot A \cdot T} &= \det(X \cdot E_n - T^{-1} \cdot A \cdot T) \\ &= \det(T^{-1} \cdot (X \cdot E_n - A) \cdot T) \quad (\text{da } T^{-1} \cdot X \cdot E_n \cdot T = X \cdot E_n) \\ &\underset{(3.23)}{=} \det(X \cdot E_n - A) = \chi_A \end{aligned}$$

(b) Die Unabhängigkeit von χ_φ von B folgt aus (a)(3) und (2.83). □

Ziel

$A \in K^{n\times n}$, $a \in K$. Dann:
a EW von $A \Leftrightarrow \chi_A(a) = 0$. □

(4.32) Beispiele

(a) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$.

$$X \cdot E_2 - A = \begin{pmatrix} X & -1 \\ 1 & X \end{pmatrix},\ \chi_A = \begin{vmatrix} X & -1 \\ 1 & X \end{vmatrix} = X^2 + 1.$$

(b) $A = \begin{pmatrix} a_{11} & & & * \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{pmatrix}$ obere Dreiecksmatrix.

$$\underset{(3.20)}{\Rightarrow} \chi_A = \prod_{i=1}^{n} (X - a_{ii}).$$ □

Erinnerung

R kommutativer Ring, $A = (a_{ij}) \in R^{n\times n}$.
$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot a_{\pi(1),1} \cdot a_{\pi(2),2} \cdots a_{\pi(n),n}$. □

(4.33) Bemerkung

Seien R, S Ringe, $\varphi : R \to S$ Ringhomomorphismus $[\varphi(1) = 1, \varphi(r + r') = \varphi(r) + \varphi(r'), \varphi(r \cdot r') = \varphi(r) \cdot \varphi(r')]$.
$A = (a_{ij}) \in R^{n\times n}$, $\varphi(A) := (\varphi(a_{ij})) \in S^{n\times n}$.
Dann ist $\det(\varphi(A)) = \varphi(\det(A))$.

Beweis

$$\begin{aligned}
\det(\varphi(A)) &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot \varphi(a_{\pi(1),1}) \cdots \varphi(a_{\pi(n),n}) \\
&= \varphi\left(\sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot a_{\pi(1),1} \cdots a_{\pi(n),n} \right) \\
&= \varphi(\det(A)).
\end{aligned}$$

$\square$

(4.34) Korollar

Sei $A \in K^{n\times n}$, $a \in K$. Dann gilt:
$\underbrace{\chi_A(a)}_{\in K} = \det(\underbrace{a \cdot E_n - A}_{\in K^{n\times n}})$.

Beweis

Betrachte den Einsetzungshomomorphismus:
$\tau_A : K[X] \to K$, $f \mapsto \tau_A(f) = f(a)$ (vgl. (4.14))
$\chi_A(a) = \tau_a(\chi_A) = \tau(\det(X \cdot E_n - A)) \underset{(4.33)}{=} \det(\tau_a(X \cdot E_n - A)) = \det(a \cdot E_n - A)$. $\square$

(4.35) Satz

Sei $A \in K^{n\times n}$, V n-dim. K-VR, $\varphi \in \mathrm{End}_K(V)$, $a \in K$. Dann gilt:
a EW von A (bzw. von φ) $\Leftrightarrow \chi_A(a) = 0$ (bzw. $\chi_\varphi(a) = 0$).

Beweis

a EW von $A \Leftrightarrow$ es existiert $0 \neq v \in K^n$ mit $A \cdot v = a \cdot v \Leftrightarrow$ es existiert $0 \neq v \in K^n$ mit $(a \cdot E_n - A) \cdot v = 0 \underset{(2.65)(d)}{\Leftrightarrow} a \cdot E_n - A$ nicht invertierbar $\underset{(3.27)(b)}{\Leftrightarrow} \det(a \cdot E_n - A) = 0 \underset{(4.34)}{\Leftrightarrow} \chi_A(a) = 0$.
Sei B Basis von V, $v \in V$. Dann gilt:
$\varphi(v) = a \cdot v \Leftrightarrow M_B(\varphi) \cdot \kappa_B(v) = a \cdot \kappa_B(v)$ und $v \neq 0 \Leftrightarrow \kappa_B(v) \neq 0$ [κ_B Isomorphismus]
Also: a EW von $\varphi \Leftrightarrow a$ EW von $M_B(\varphi) \Leftrightarrow \underbrace{\chi_{M_B(\varphi)}}_{=\chi_A}(a) = 0$. $\square$

Sei $A \in K^{n\times n}$, $a \in K$.
$\Rightarrow V(a,A) = \{v \in V \mid A \cdot v = a \cdot v\}$ ist die Lösungsmenge des homogenen LGS $(a \cdot E_n - A) \cdot x = 0$.

(4.36) Beispiele

(a) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ hat keine EW in $\mathbb{R}$, denn $\chi_A = X^2 + 1$.

Über $\mathbb{C}$ hat A die EW $\sqrt{1}$ und $\sqrt{-1}$.

(b) Ähnliche Matrizen haben die gleichen EW.

(Nach (4.31)(a)(3) haben sie das gleiche charakteristische Polynom.)

[B, A ähnlich $\Leftrightarrow$ es existiert $T \in \mathrm{GL}_n(K)$: $B = T^{-1} \cdot A \cdot T$]

(c) Sei A ähnlich zu Dreiecksmatrix $\begin{pmatrix} a_{11} & & & * \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{pmatrix} \underset{(?)(b)}{\overset{(4.31)(a)(3)}{\Rightarrow}} \chi_A = \prod_{i=1}^{n}(X - a_{ii})$

$\underset{(4.35)}{\Rightarrow} a_{11}, \dots, a_{nn}$ sind die EW von A.

χ_A zerfällt in ein Produkt von Linearfaktoren.

(d) $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in K^{2\times 2}$ ist nicht diagonalisierbar.

Angenommen, es existiert $T \in \mathrm{GL}_2(K)$ mit $T^{-1} \cdot A \cdot T = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

$\underset{(c)}{\Rightarrow} \chi_{T^{-1}\cdot A \cdot T} = (X-a)\cdot(X-b)$ und $\chi_A = (X-1)\cdot(X-1)$.

Aus $\chi_A = \chi_{T^{-1}\cdot A\cdot T}$ (vgl. (4.31)(a)(3)) folgt:

$a = b = 1$, d.h. $T^{-1}\cdot A \cdot T = E_2 \Rightarrow A = T^{-1}\cdot E_2 \cdot T = E_2$. ↯ □

(4.37) Definition

Sei R komm. Ring, $A = (a_{ij}) \in R^{n\times n}$.
$\mathrm{Sp}(A) = \sum_{i=1}^{n} a_{ii} \in R$ heißt die SPUR von A. □

(4.38) Bemerkung

Sei R komm. Ring, $A, B \in R^{n\times n}$, $T \in \mathrm{GL}_n(R)$. Dann gilt:

(a) $\mathrm{Sp}(A\cdot B) = \mathrm{Sp}(B \cdot A)$

(b) $\mathrm{Sp}(T^{-1}\cdot A \cdot T) = \mathrm{Sp}(A)$

Beweis

(a) Sei $A = (a_{ij})$, $B = (b_{ij})$.

Die i-ten Diagonaleinträge von $A\cdot B$ bzw. $B\cdot A$ sind:

$\sum_{k=1}^{n} a_{ik}\cdot b_{ki}$ bzw. $\sum_{k=1}^{n} b_{ik}\cdot a_{ki}$

$\Rightarrow \mathrm{Sp}(A\cdot B) = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}\cdot b_{ki} = \sum_{k=1}^{n}\sum_{i=1}^{n} b_{ki}\cdot a_{ik} = \mathrm{Sp}(B\cdot A)$

(b) $\mathrm{Sp}(T^{-1}\cdot(A\cdot T)) = \mathrm{Sp}((A\cdot T)\cdot T^{-1}) = \mathrm{Sp}(A)$. □

(4.39) Bemerkung

Sei $A \in K^{n \times n}$. Dann gilt:
$\chi_A = X^n - \mathrm{Sp}(A) \cdot X^{n-1} + c_{n-2} \cdot X^{n-2} + \ldots + c_1 \cdot X + (-1)^n \cdot \det(A)$
mit geeigneten $c_1, \ldots, c_{n-2} \in K$.

Beweis

Sei $E_n = (\delta_{ij})_{1 \le i,j \le n}$ (Kronecker-Delta) und sei $A = (a_{ij})$. Dann gilt:
$\chi_A = \det(X \cdot E_n - A) = \sum_{\pi \in S_n} \mathrm{sgn}(\pi) \cdot \underbrace{(X \cdot \delta_{\pi(1),1} - a_{\pi(1),1}) \cdots (X \cdot \delta_{\pi(n),n} - a_{\pi(n),n})}_{f_{A,\pi}}$
$f_{A,\pi}$: Produkt von n Faktoren p, $p \in K[X]$ mit $p = 0$ oder $\deg(p) \le 1$.
$\underline{\pi \in S_n, \pi \neq \mathrm{id}:}$
$\Rightarrow$ für mindestens zwei i's ist $\pi(i) \neq i$.
$\Rightarrow f_{A,\pi} = 0$ oder $\deg(f_{A,\pi}) \le n-2$.
$\underline{\pi = \mathrm{id}:}$
$f_{A,\pi} = \prod_{i=1}^{n} (X - a_{ii}) = X^n - \mathrm{Sp}(A) \cdot X^{n-1} + g$ mit $g = 0$ oder $\deg(g) \le n-2$.
Sei c_0 der konstante Koeffizient von χ_A.
$c_0 = \chi_A(0) \underset{(?)}{=} \det(0 \cdot E_n - A) = \det(-A) = (-1)^n \cdot \det(A)$. □

(4.40) Korollar

Sei $A \in K^{n \times n}$ (bzw. $\varphi \in \mathrm{End}_K(V)$) für einen n-dim. K-VR V.
Dann hat A (bzw. φ) höchstens n EW (inkl. Vielfachheiten). □

(4.41) Definition

Sei $f = X^n + a_{n-1} \cdot X^{n-1} + \ldots + a_1 \cdot X + a_0 \in K[X]$ normiert.

Dann heißt $C(f) := \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & \cdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$ die Begleitmatrix von f.

$\underline{n = 1:}$ $f = X + a_0$ und $C(f) = (-a_0) \in K^{1 \times 1}$. □

(4.42) Bemerkung

Sei $f = X^n + a_{n-1} \cdot X^{n-1} + \ldots + a_1 \cdot X + a_0 \in K[X]$.
Dann ist $\chi_{C(f)} = f$.

Beweis

$$X \cdot E_n - C(f) = \begin{pmatrix} X & 0 & 0 & \cdots & 0 & a_0 \\ -1 & X & 0 & \cdots & 0 & a_1 \\ 0 & -1 & X & \cdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & X & a_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & X + a_{n-1} \end{pmatrix} =: A \in K[X]^{n \times n}.$$

Sei $A = (a_{ij})$.
Wir entwickeln $\det(A)$ nach der letzten Spalte (vgl. (3.18)(a)):
$\chi_{C(f)} = \det(A) = \sum_{i=1}^{n} (-1)^{i+n} \cdot a_{in} \cdot \det(A_{in})$

$$A_{1n} = \begin{pmatrix} -1 & X & & & 0 \\ & -1 & X & & \\ & & \ddots & \ddots & \\ 0 & & & -1 & X \end{pmatrix} \Rightarrow \det(A_{1n}) = (-1)^{n-1}$$

$$A_{in} = \left(\begin{array}{cccc|cccc} X & & & 0 & & & & \\ -1 & X & & & & 0 & & \\ & \ddots & \ddots & & & & & \\ 0 & & -1 & X & & & & \\ \hline & & & & -1 & X & & 0 \\ & & & & & \ddots & \ddots & \\ & 0 & & & & & -1 & X \\ & & & & 0 & & & -1 \end{array}\right) \text{ für } 2 \leq i \leq n.$$

$\Rightarrow \det(A_{in}) = X^{i-1} \cdot (-1)^{n-i}$ für $2 \leq i \leq n$.
$a_{in} = a_{i-1}$ für $1 \leq i \leq n-1$.
$a_{nn} = X + a_{n-1}$.
$\Rightarrow \chi_{C(f)} = \det(A)$
$= (-1)^{1+n} \cdot a_0 \cdot (-1)^{n-1} + \sum_{i=2}^{n-2} (-1)^{i+n} \cdot a_{i-1} \cdot X^{i-1} \cdot (-1)^{n-i} + (-1)^{2n} \cdot (X + a_{n-1}) \cdot X^{n-1} \cdot (-1)^0$
$= a_0 + a_1 \cdot X + \ldots + a_{n-2} \cdot X^{n-2} + (X + a_{n-1}) \cdot X^{n-1} = f.$ □

§ 4 Das Minimalpolynom

Sei K Körper, V n-dim. K-VR, $\varphi \in \mathrm{End}_K(V)$.

(4.43) Definition

(a) $U \leq V$ heißt φ-INVARIANT, falls $\varphi(U) \leq U$ ist.

(b) Sei $U \leq V$ φ-invariant.

Dann sei $\varphi_U : U \to U, u \mapsto \varphi(u)$ mit $u \in U$.

$\varphi_U \in \mathrm{End}_K(V)$ ist die EINSCHRÄNKUNG von φ auf U. □

(4.44) Bemerkung

Sei $U \leq V$ φ-invariant.

(a) Sei $\mathcal{C} = (v_1, \dots, v_m)$ die Basis von U.
Ergänze $\mathcal{C}$ zu einer Basis $\mathcal{B} = (v_1, \dots, v_m, v_{m+1}, \dots, v_n)$ von V. Dann gilt:
$M_{\mathcal{B}}(\varphi) = \left(\begin{array}{c|c} M_{\mathcal{C}}(\varphi_U) & C \\ \hline 0 & D \end{array}\right)$ für geeignete Matrizen C und D.

(b) $\chi_{\varphi_U} \mid \chi_\varphi$

Beweis

(a) Für $1 \leq j \leq m$ ist $\varphi(v_j) = \varphi_U(v_j) \in U$.
Behauptung folgt aus der Definition von $M_{\mathcal{B}}(\varphi)$.

(b) $X \cdot E_n - M_{\mathcal{B}}(\varphi) = \left(\begin{array}{c|c} X \cdot E_m - M_{\mathcal{C}}(\varphi_U) & -C \\ \hline 0 & X \cdot E_{n-m} - D \end{array}\right)$
$\underset{(3.21)}{\Rightarrow} \chi_\varphi = \det(X \cdot E_n - M_{\mathcal{B}}(\varphi)) = \det(X \cdot E_m - M_{\mathcal{C}}(\varphi_U)) - \det(X \cdot E_{n-m} - D) = \chi_{\varphi_U} \cdot f$ für ein $f \in K[X]$. □

(4.45) Beispiel

Sei $v_1 \in V$ EV von φ zum EW $a \in K$.
$\Rightarrow U := < v_1 >$ ist φ-invariant.

Ist $(v_1, \dots, v_n)$ Basis von V, dann ist $M_{\mathcal{B}}(\varphi) = \left(\begin{array}{c|ccc} a & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & D & \\ 0 & & & \end{array}\right)$ für ein $D \in K^{(n-1)\times(n-1)}$. □

Erinnerung

A ähnlich zu $\begin{pmatrix} a_{11} & & & * \\ & a_{22} & & \\ & & \ddots & \\ 0 & & & a_{nn} \end{pmatrix} \Rightarrow \chi_A = \prod_{i=1}^{n} X - a_{ii}$. □

Umkehrung von (4.36)(c):

(4.46) Satz

Sei $A \in K^{n\times n}$ mit $\chi_A = \prod_{i=1}^{n}(X-a_i)$, d.h. das charakteristische Polynom von A zerfällt in Linearfaktoren.
$\Rightarrow A$ ist ähnlich zu einer oberen Dreiecksmatrix.

Beweis

Induktion über n:
$\underline{n=1}$: Klar.
$\underline{n>1, n-1\mapsto n}$: Sei $v_1 \in K^n$ EV von A zum EW a_1 (existiert nach (4.35)).
$\mathcal{B} = (v_1,\dots,v_n)$ Basis von K^n.

$$\Rightarrow M_{\mathcal{B}}(\varphi_A) = \left(\begin{array}{c|ccc} a_1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & D & \\ 0 & & & \end{array}\right) \text{ mit } D \in K^{(n-1)\times(n-1)}.$$

$M_{\mathcal{B}}(\varphi_A)$ ähnlich zu A (vgl. (2.83)).
$\Rightarrow \chi_A \underset{(4.31)}{=} \chi_{M_{\mathcal{B}}(\varphi_A)} \underset{(3.21)}{=} (X-a_1)\cdot\chi_D$.

$\underset{(4.13)}{\Rightarrow} \chi_D = \prod_{i=2}^{n}(X-a_i)$

$\underset{\text{Induktion}}{\Rightarrow}$ Es existiert $S \in \mathrm{GL}_{n-1}(K)$, so dass $S^{-1}\cdot D\cdot S$ eine obere Dreicksmatrix ist.

$$\text{Setze } T := \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & S & \\ 0 & & & \end{array}\right) \in K^{n\times n}.$$

$\Rightarrow \det(T) = \det(S) \neq 0$, d.h. $T \in \mathrm{GL}_n(K)$.

$$\text{Weiter gilt: } T^{-1}\cdot M_{\mathcal{B}}(\varphi_A)\cdot T = \left(\begin{array}{c|ccc} a_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & S^{-1}\cdot D\cdot S & \\ 0 & & & \end{array}\right) \text{ ist eine obere Dreiecksmatrix.} \qquad \square$$

Für $K=\mathbb{C}$: Jede $(n\times n)$-Matrix ist ähnlich zu einer oberen Dreicksmatrix.

(4.47) Bemerkung

(a) $\mathrm{End}_K(V)$ ist K-VR mit

$$+ : \mathrm{End}_K(V)\times\mathrm{End}_K(V) \to \mathrm{End}_K(V), (\varphi+\psi)(v) := \varphi(v)+\psi(v) \text{ mit } \varphi,\psi \in \mathrm{End}_K(V), v \in V$$

und

$$\cdot : K \times \mathrm{End}_K(V) \to \mathrm{End}_K(V), (a \cdot \varphi)(v) := a \cdot \varphi(v) \text{ mit } a \in K, \varphi \in \mathrm{End}_K(V), v \in V$$

(b) $\mathrm{End}_K(V)$ wird K-Algebra mit (a) und $\cdot : \mathrm{End}_K(V) \times \mathrm{End}_K(V) \to \mathrm{End}_K(V), (\varphi, \psi) \mapsto \varphi \circ \psi$.

(c) Ist $\mathcal{B}$ eine Basis von V, dann ist $M_{\mathcal{B}} : \mathrm{End}_K(V) \to K^{n \times n}, \varphi \mapsto M_{\mathcal{B}}(\varphi)$ ein K-Algebren-Isomorphismus.

Beweis

Formales Rechnen. □

(4.48) Bemerkung

Sei $0 \neq v \in V$.
Die Folge $(v, \varphi(v), \underbrace{\varphi^2(v)}_{\varphi \cdot \psi = \varphi \circ \psi} = \varphi(\varphi(v)), \ldots, \varphi^n(v))$ ist l.a.
Sei m minimal, $m \in \mathbb{N}$, so dass $(v, \varphi(v), \ldots, \varphi^{m-1}(v))$ l.u., aber $(v, \varphi(v), \ldots, \varphi^{m-1}(v), \varphi^m(v))$ l.a. ist mit $\varphi^0 = \mathrm{id}$.
$\Rightarrow$ Es existieren $a_0, \ldots, a_{m-1} \in K$ mit $\varphi^m(v) = \sum\limits_{i=0}^{m-1} a_i \varphi^i(v)$.
$\Rightarrow U := < v, \varphi(v), \ldots, \varphi^{m-1}(v) >$ ist m-dim. φ-invarianter UR von V.
Sei $\mathcal{C} = (v, \varphi(v), \ldots, \varphi^{m-1}(v))$ und $f = X^m - \sum\limits_{i=0}^{m-1} a_i X^i \in K[X]$.

$$\text{Dann ist } M_{\mathcal{C}}(\varphi_U) = \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & \cdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & a_{m-2} \\ 0 & 0 & \cdots & 0 & 1 & a_{m-1} \end{pmatrix} = C(f).$$

$\underset{(4.43)}{\Rightarrow} \chi_{\varphi_U} = \chi_{C(f)} = f$

$f(\varphi) = \varphi^m - \sum\limits_{i=0}^{m-1} a_i \varphi^i \in \mathrm{End}_K(V)$

$f(\varphi)(v) = \varphi^m(v) - \sum\limits_{i=0}^{m-1} a_i \varphi^i(v) = 0.$ □

(4.49) Satz (Cayley-Hamilton)

Sei $\varphi \in \mathrm{End}_K(V)$ bzw. $A \in K^{n \times n}$. Dann gilt:
$\chi_\varphi(\varphi) = 0$ bzw. $\chi_A(A) = 0$.

Beweis

Aussage für A folgt aus der für φ mit (4.47)(c).
Zu zeigen: $\chi_\varphi(\varphi) = 0 \in \mathrm{End}_K(V)$, d.h. $\chi_\varphi(\varphi)(v) = 0$ für alle $v \in V$.
$v = 0$: ✓
Sei also $v \neq 0$ und $U =< v, \varphi(v), \ldots, \varphi^{m-1}(v) >$ wie in (4.48).
Nach (4.44)(c) existiert $f \in K[X]$ mit $\chi_\varphi = \chi_{\varphi_U} \cdot f = f \cdot \chi_{\varphi_U}$.
$\Rightarrow \chi_\varphi(\varphi) = (f \cdot \chi_{\varphi_U})(\varphi) = \underbrace{f(\varphi)}_{\in \mathrm{End}_K(V)} \circ \underbrace{\chi_{\varphi_U}(\varphi)}_{\in \mathrm{End}_K(V)}$
$\Rightarrow \chi_\varphi(\varphi)(v) = [f(\varphi) \circ \chi_{\varphi_U}(\varphi)](v) = f(\varphi)(\underbrace{\chi_{\varphi_U}(\varphi)(v)}_{=0 \text{ nach } (4.48)}) = 0.$ □

(4.50) Beispiel

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in Q^{2\times 2}, X \cdot E_2 - A = \begin{pmatrix} X-1 & -2 \\ -3 & X-4 \end{pmatrix}$
$\chi_A = (X-1)\cdot(X-4) - 6 = X^2 - 5\cdot X - 2$
$\chi_A(A) = A^2 - 5 \cdot A - 2 \cdot E_2$
$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}, A^2 - 5 \cdot A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2 \cdot E_2.$ □

(4.51) ! Bemerkung und Definition

Sei $A \in K^{n\times n}, \varphi \in \mathrm{End}_K(V)$, wobei V n-dim. K-VR sei.

(a) Es existiert $\mu_A \in K[X], \deg(\mu_A) \geq 1$ (bzw. $\mu_\varphi \in K[X], \deg(\mu_\varphi) \geq 1$).

(1) μ_A (bzw. μ_φ) ist normiert

(2) $\mu_A(A) = 0$ (bzw. $\mu_\varphi(\varphi) = 0$)

(3) $\mu_A \mid f$ (bzw. $\mu_\varphi \mid f$) für alle $f \in K[X]$ mit $f(A) = 0$ (bzw. $f(\varphi) = 0$)

Durch (1) - (3) ist μ_A (bzw. μ_φ) eindeutig festgelegt. Es heißt das MINIMALPOLYNOM von A (bzw. φ).

(b) Ist $\mathcal{B}$ eine Basis von V, dann ist $\mu_\varphi = \mu_{M_{\mathcal{B}}(\varphi)}$.

(c) Ist $B \in K^{n\times n}$ ähnlich zu A, dann ist $\mu_A = \mu_B$.

Beweis

(a) Nur für A. Der Beweis für φ geht analog.

Sei $I = \{f \in K[X] \mid f(A) = 0\}$.

$\chi_A \in I$ nach (4.49) $\Rightarrow I \neq \{0\}$

Sei $0 \neq \mu \in I$ von minimalem Grad und sei $a \in K$ der höchste Koeffizient von μ.

Setze $\mu_A := a^{-1} \cdot \mu$.

$\Rightarrow \deg(\mu_A) = \deg(\mu), \mu_A$ normiert, d.h. (1), und $\mu_A(A) = 0$, d.h. (2).

Sei $f \in I$. $\Rightarrow$ Es existieren $q, r \in K[X]$ mit $f = q \cdot \mu_A + r$ und $r = 0$ oder $\deg(r) < \deg(\mu_A)$.

Es gilt: $r(A) = f(A) - (q \cdot \mu_A)(A) = f(A) - q(A) \cdot \mu_A(A) = 0$.

$\Rightarrow r = 0$ nach Wahl von μ.

Eindeutigkeit: Seien $\mu_1, \mu_2 \in K[X]$ mit (1) - (3).

$\Rightarrow \mu_1 \mid \mu_2$ und $\mu_2 \mid \mu_1$

$\Rightarrow \mu_1 = \mu_2$, da beide normiert sind.

(b) Folgt aus (a) mit (4.47)(c).

(c) Folgt aus (b) und (2.83), oder auch durch direktes Rechnen mit (a). $[B = T^{-1} \cdot A \cdot T]$. $\square$

(4.52) Beispiele

(a) Sei $A = \begin{pmatrix} \boxed{\begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{matrix}} & & 0 \\ & \boxed{1} & \\ 0 & & \boxed{\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}} \end{pmatrix} \in K^{6 \times 6}$.

$\chi_A = X^2 \cdot (X-1)^4, \mu_A = X \cdot (X-1)^3$.

(b) Sei $a \in K$ und $A = \begin{pmatrix} a & 1 & & & 0 \\ & a & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & a \end{pmatrix} \in K^{n \times n}$.

$\Rightarrow \chi_A = \mu_A = (X-a)^n$.

(c) Sei $f \in K[X], f \notin K, f$ normiert.

$\Rightarrow \chi_{C(f)} = \mu_{C(f)} = f$.

(d) Sei $A = \begin{pmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n \end{pmatrix}$ eine Diagonalmatrix und sei $\{a_1, \ldots, a_n\} = \{b_1, \ldots, b_m\}$ mit $b_i \neq b_j$ für $i \neq j$.

$\Rightarrow \mu_A = \prod_{i=1}^{m} (X - b_i).$

Beweis

(a) $\mu_A \mid \chi_A \Rightarrow X^r \cdot (X-1)^s$ mit $0 \leq r \leq 2$ und $0 \leq s \leq 4$.

$A^i \neq 0$ für alle $i \geq 1, (A - E_6)^i \neq 0$ für alle $i \geq 1$.

$\Rightarrow X \cdot (X-1) \mid \mu_A$

$A \cdot (A - E_6)^3 = 0, A \cdot (A - E_6)^2 \neq 0.$

(b) $\chi_A = (X - A)^n$

$$A - a \cdot E_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \cdots & \cdots & 0 \\ \vdots & & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

$$(A - a \cdot E_n)^i = \begin{pmatrix} 0 & \cdots & 0 & 0 & 1 & & 0 \\ & & & & \ddots & \ddots & \\ & & 0 & & & \ddots & 1 \\ & & & & & & 0 \\ 0 & & & \cdots & & & 0 \end{pmatrix}$$

(c) Übung.

(d) Der i-te Diagonaleintrag von $\prod_{j=1}^{m} (A - b_j \cdot E_n)$ ist $\underbrace{\prod_{j=1}^{m} (a_i - b_j)}_{=0 \text{ wegen } a_i \in \{b_1, \ldots, b_m\}}$.

Für keinen echten Teiler ρ von $\prod_{i=1}^{m} (X - b_i)$ ist $\rho(A) = 0$. □

(4.53) Lemma

Sei $0 \neq f \in K[X]$ mit $f(\varphi) = 0$.
Seien $g, h \in K[X]$ teilerfremd mit $f = g \cdot h$.
Setze $U := \mathrm{Kern}(g(\varphi)), W := \mathrm{Kern}(h(\varphi))$.
Dann sind U und W φ-invariant und es gilt: $V = U \oplus W$, d.h. $V = U + W$ und $U \cap W = \{0\}$.

Beweis

Sei $u \in U$, d.h. $g(\varphi)(u) = 0$.
$\Rightarrow g(\varphi)(\varphi(u)) = g(\varphi) \circ \varphi(u) = \varphi \circ g(\varphi)(u) = \varphi(g(\varphi)(u)) = \varphi(0) = 0$.
$\Rightarrow \varphi(u) \in \mathrm{Kern}(g(\varphi)) = U$, d.h. U φ-invariant.
Analog: W φ-invariant.
Seien $g_1, h_1 \in K[X]$ mit $1 = g_1 \cdot g + h_1 \cdot h$ (vgl. (4.11)).
φ einsetzen $\Rightarrow \mathrm{id} = \underbrace{(g_1 \cdot g)(\varphi)}_{g_1(\varphi)\circ g(\varphi)} + (h1 \cdot h)(\varphi)$
$\Rightarrow v = (g_1 \cdot g)(\varphi)(v) + (h_1 \cdot h)(\varphi)(v)$ für alle $v \in V$.
<u>Zeige:</u> $(g_1 \cdot g)(\varphi)(v) \in \underbrace{W}_{=\mathrm{Kern}(h(\varphi))}, (h_1 \cdot h)(\varphi)(v) \in U$.
$h(\varphi)[(g_1 \cdot g)(\varphi)(v)] = [h(\varphi) \circ (g_1 \cdot g)(\varphi)](v) = (h \cdot g_1 \cdot g)(\varphi)(v) = (g_1 \cdot f)(\varphi)(v)$
$= [g_1(\varphi) \circ f(\varphi)](v) = g_1(\varphi)(\underbrace{f(\varphi)(v)}_{=0}) = 0$.
Also: $(g_1 \cdot g)(\varphi)(v) \in W$.
Analog: $(h_1 \cdot h)(\varphi)(v) \in U$.
$\Rightarrow V = U + W$.
Sei $v \in U \cap W$.
$\Rightarrow v = [g_1(\varphi) \circ g(\varphi)](v) + [h_1(\varphi) \circ h(\varphi)](v) = g_1(\varphi)(\underbrace{g(\varphi)(v)}_{=0,\text{ da } v \in U}) + h_1(\varphi)(\underbrace{h(\varphi)(v)}_{=0,\text{ da } v \in W}) = 0$
$\Rightarrow U \cap W = \{0\}$. □

(4.54) Satz

Sei $A \in K^{n \times n}$. Dann gilt:
A diagonalisierbar $\Leftrightarrow \mu_A$ zerfällt in ein Produkt von paarweise verschiedenen Linearfaktoren.

Beweis

<u>„$\Rightarrow$“:</u> Folgt aus (4.51)(a) und (4.52)(d).
<u>„$\Leftarrow$“:</u> Sei $\mu_A = \prod_{j=1}^{m} (X - b_j)$ mit $b_i \neq b_j$ für $i \neq j$.
Betrachte $\varphi_A : K^n \to K^n$, setze $f := \mu_A, g := X - b_1, h := \prod_{j=2}^{m} (X - b_j)$.
$\Rightarrow g, h$ teilerfremd (o.B.d.A: $n > 1$)
$\Rightarrow K^n = U \oplus W$ mit $U = \mathrm{Kern}(g(\varphi_A)), W = \mathrm{Kern}(h(\varphi_A))$.
$\mathrm{Kern}(g(\varphi_A)) = \mathrm{Kern}(\varphi_A - b_1 \cdot \mathrm{id}) = V(b_1, A)$.
Sei $(u_1, \ldots, u_m)$ Basis von U und $(w_1, \ldots, w_l)$ Basis von W.
$\underset{\text{Aufg. 6, Blatt 8}}{\Rightarrow} (u_1, \ldots, u_m, w_1, \ldots, w_l) =: \mathcal{B}$ ist Basis von $V = K^n$.

Weil U, W φ-invariant sind, ist $M_{\mathcal{B}}(\varphi) = \left(\begin{array}{ccc|c} b_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & b_1 & \\ \hline & 0 & & D \end{array}\right)$.

Es gilt: $\mu_A(D) = 0. \Rightarrow \mu_D \mid \mu_A$.
$\Rightarrow \mu_D$ zerfällt in ein Produkt von verschiedenen Linearfaktoren.
$\underset{\text{Induktion}}{\Rightarrow}$ D ist diagonalisierbar.
$\Rightarrow A$ ist diagonalisierbar. (Argument wie im Beweis von (4.46).) $\square$

5 Euklidische und Unitäre Räume

Zusätzliche Struktur für reele oder komplexe Vektorräume, *Skalarprodukt*.
$\rightsquigarrow$ Längen, Winkel.

Voraussetzungen

$K = \mathbb{R}$ oder $\mathbb{C}$
$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}, i \in \mathbb{C}$ mit $i^2 = -1$.
$(1, i)$ l.u. über $\mathbb{R}$ (vgl. Beispiel (2.54)); $\mathbb{R} \subseteq \mathbb{C}$.
$^- : \mathbb{C} \to \mathbb{C}$, $a + ib \mapsto a - ib$ (KOMPLEXE KONJUGATION)
$^-$ ist ein Körperautomorphismus, d.h. ein bijektiver Ringhomomorphismus, $\mathbb{R} = \{c \in \mathbb{C} \mid \overline{c} = c\}$.
$\mid c \mid := \sqrt{c \cdot \overline{c}} \in \mathbb{R}_{\geq 0}$ heißt (komplexer) ABSOLUTBETRAG von $\mathbb{C}$. $(c \cdot \overline{c} \in \mathbb{R}_{\geq 0})$
$A = (a_{ij}) \in \mathbb{C}^{n \times n}, \overline{A} := (\overline{a}_{ij})$

$\square$

§ 1 Skalarprodukte

Sei $K = \mathbb{R}$ oder $\mathbb{C}$ und sei V K-VR (nicht notwendig e.e.).

(5.1) Definition und Bemerkung

(a) Eine Abbildung $\beta : V \times V \to K$ heißt BILINEARFORM (im Fall $K = \mathbb{R}$) bzw. SESQUILINEARFORM (im Fall $K = \mathbb{C}$), falls gilt:

(1) $\beta(v_1 + v_2, w) = \beta(v_1, w) + \beta(v_2, w)$ und
$\beta(av, w) = a \cdot \beta(v, w)$ für alle $v, v_1, v_2, w \in V, a \in K$.

(2) $\beta(v, w_1 + w_2) = \beta(v, w_1) + \beta(v, w_2)$ und
$\beta(v, aw) = \overline{a} \cdot \beta(v, w)$ für alle $v, w, w_1, w_2 \in V, a \in K$.
(Beachte: Für $K = \mathbb{R}$ ist $\overline{a} = a$.)

(b) Sei β Bilinearform (bzw. Sesquilinearform) auf K.

β heißt SYMMETRISCH (bzw. HERMITE'SCH), falls gilt:

$\beta(v, w) = \beta(w, v)$ für alle $v, w \in V$ (bzw. $\beta(v, w) = \overline{\beta(w, v)}$ für alle $v, w \in V$).

$(*)$ Ist β hermite'sch (also $K = \mathbb{C}$), dann ist $\beta(v,v) \in \mathbb{R}$ für alle $v \in V$.

Sei β symmetrisch (bzw. hermite'sch).
Dann heißt β ein SKALARPRODUKT auf V, falls β POSITIV DEFINIT ist, d.h. falls gilt:
$\beta(v,v) > 0$ für alle $v \in V, v \neq 0$.

Beweis

(b) $(*)$ $\beta(v,v) = \overline{\beta(v,v)}$, da β hermite'sch.
$\Rightarrow \beta(v,v) \in \mathbb{R}$. □

(5.2) Beispiele

(1) $V = K^n$ ($\mathbb{R}^n$ oder $\mathbb{C}^n$)

$<,>: V \times V \to K, < \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} > := \sum_{j=1}^{n} a_j \overline{b_j} \in K$ ist ein Skalarprodukt auf V, das STANDARD-SKALARPRODUKT.

(2) Sei $V := \{f : [0,1] \to \mathbb{R} \mid f \text{ stetig}\}$. V ist $\mathbb{R}$-VR. Für $f, g \in V$ sei $(f,g) := \int_0^1 f(t)g(t)dt \in \mathbb{R}$.

$(,)$ ist ein Skalarprodukt. □

(5.3) Satz (Cauchy-Schwarz'sche Ungleichung)

Sei $(,)$ ein Skalarprodukt auf V.
Dann gilt für alle $v_1, v_2 \in V$:

$$\mid (v_1,v_2) \mid^2 \leq (v_1,v_1) \cdot (v_2,v_2) \text{ sowie}$$
$$\mid (v_1,v_2) \mid^2 = (v_1,v_1) \cdot (v_2,v_2) \Leftrightarrow v_1, v_2 \text{ l.a.}$$

Beweis

Ist $v_2 = 0$, dann sind beide Aussagen klar.
Sei also $v_2 \neq 0$ und $a := -\frac{(v_1,v_2)}{(v_2,v_2)} \in K$.

$$\begin{aligned} \Rightarrow 0 \leq (v_1 + av_2, v_1 + av_2) &= (v_1,v_1) + a \cdot (v_2,v_1) + \overline{a} \cdot (v_1,v_2) + a \cdot \overline{a} \cdot (v_2,v_2) \\ &= (v_1,v_1) - \frac{\mid (v_1,v_2) \mid^2}{(v_2,v_2)} - \frac{\mid (v_1,v_2) \mid^2}{(v_2,v_2)} + \frac{\mid (v_1,v_2) \mid^2}{(v_2,v_2)} \\ &= (v_1,v_1) - \frac{\mid (v_1,v_2) \mid^2}{(v_2,v_2)} \Rightarrow \text{ 1. Behauptung.} \end{aligned}$$

Es gelte: $|(v_1,v_2)|^2 = (v_1,v_1)\cdot(v_2,v_2)$.
$\Rightarrow (v_1+av_2, v_1+av_2) = 0$
$\Rightarrow v_1+av_2 = 0$, d.h. v_1,v_2 sind l.a.
Sind v_1,v_2 l.a., dann ist $v_1 = bv_2$ für ein $b \in K$ (weil $v_2 \neq 0$).
$\Rightarrow |(v_1,v_2)|^2 = |b\cdot(v_2,v_2)|^2 = |b|^2 \cdot |(v_2,v_2)|^2 = b\cdot\overline{b}\cdot(v_2,v_2)\cdot\underbrace{(v_2,v_2)}_{\in\mathbb{R}} = (v_1,v_1)\cdot(v_2,v_2)$. □

(5.4) Beispiele

(1) Seien $a_j, b_j \in \mathbb{C}, 1 \leq j \leq n$.

$$\Rightarrow \left|\sum_{j=1}^n a_j\overline{b_j}\right|^2 \leq \left(\sum_{j=1}^n |a_j|^2\right)\left(\sum_{j=1}^n |b_j|^2\right)$$

Mit Gleichheit genau dann, wenn $\underbrace{\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}}_{v_1}$ und $\underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}}_{v_2}$ l.a. sind.

(2) Für alle stetigen Funktionen $f,g : [0,1] \to \mathbb{R}$ gilt:

$$\left|\int_0^1 f(t)g(t)dt\right|^2 \leq \left(\int_0^1 |f(t)|^2\, dt\right)\left(\int_0^1 |g(t)|^2\, dt\right).$$ □

(5.5) Definition und Bemerkung

Sei V e.d. und β eine Bilinearform (bzw. eine Sesquilinearform) auf V.
Sei $\mathcal{B}$ eine Basis von V, $\mathcal{B} = (v_1,\dots,v_n)$.

(a) Dann heißt $G_{\mathcal{B}}(\beta) := \big(\beta(v_i,v_j)\big)_{1\leq i,j\leq n} \in K^{n\times n}$ die GRAM-MATRIX von β bzgl. $\mathcal{B}$.

(b) Sei $A := G_{\mathcal{B}}(\beta)$. Dann gilt für alle $v,w \in V$:
$\beta(v,w) = \kappa_{\mathcal{B}}(v)^t \cdot A \cdot \overline{\kappa_{\mathcal{B}}(w)}$.
β symmetrisch $\Leftrightarrow A$ SYMMETRISCH, d.h. $A = A^t$.
β hermite'sch $\Leftrightarrow A$ HERMITE'SCH, d.h. $A = \overline{A}^t$.

Beweis

(b) Sei $\kappa_{\mathcal{B}}(v) = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, d.h. $v = \sum_{j=1}^n a_jv_j$, $\kappa_{\mathcal{B}}(w) = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

$$\Rightarrow \beta(v,w) = \beta\left(\sum_{j=1}^n a_jv_j, \sum_{k=1}^n a_kv_k\right) = \sum_{j=1}^n\sum_{k=1}^n a_j\cdot\overline{b_k}\cdot\beta(v_j,v_k)$$

$$(a_1,\dots,a_n)\cdot A\cdot\begin{pmatrix}\overline{b_1}\\ \dots\\ \overline{b_n}\end{pmatrix}=(a_1,\dots,a_n)\cdot\begin{pmatrix}\sum\limits_{k=1}^{n}\beta(v_1,v_k)\cdot\overline{b_k}\\ \vdots\\ \sum\limits_{k=1}^{n}\beta(v_n,v_k)\cdot\overline{b_k}\end{pmatrix}=\sum_{j=1}^{n}\sum_{k=1}^{n}a_j\cdot\beta(v_j,v_k)\cdot\overline{b_k}$$

$$\begin{aligned}\beta \text{ symmetrisch} &\Rightarrow \beta(v_j,v_k)=\beta(v_k,v_j) \text{ für alle } j,k\\ &\Rightarrow A=A^t\end{aligned}$$

$$\begin{aligned}A=A^t\Rightarrow\beta(v,w)&=\kappa_{\mathcal{B}}(v)^t\cdot A\cdot\kappa_{\mathcal{B}}(w)\\ &=\kappa_{\mathcal{B}}(v)^t\cdot A^t\cdot(\kappa_{\mathcal{B}}(w)^t)^t\\ &=(\kappa_{\mathcal{B}}(w)^t\cdot A\cdot\kappa_{\mathcal{B}}(v))^t\\ &=\kappa_{\mathcal{B}}(w)^t\cdot A\cdot\kappa_{\mathcal{B}}(v)\\ &=\beta(w,v)\end{aligned}$$

Aussage für hermite'sch analog. □

Bemerkung

Ist in (5.5) $V=K^n$ und $\mathcal{B}$ die Standardbasis, dann gilt:
$\boxed{\beta(v,w)=v^t\cdot A\cdot\overline{w}}$ für alle $v,w\in K^n$.

□

(5.6) Bemerkung

Sei $A\in K^{n\times n}$.

(a) $\beta_A:K^n\times K^n\to K,\beta_A(v,w):=v^t\cdot A\cdot\overline{w},v,w\in K^n$ ist Bilinearform (bzw. Sesquilinearform) auf K^n.

(b) β_A symmetrisch $\Leftrightarrow$ A symmetrisch ($K=\mathbb{R}$)

β_A hermite'sch $\Leftrightarrow$ A hermite'sch ($K=\mathbb{C}$)

Beweis

(a) Klar.

(b) Folgt aus (5.5)(b), denn $A=G_{\mathcal{B}}(\beta_A)$, wenn $\mathcal{B}$ die Standardbasis von K^n ist.

Beachte: $e_i^t\cdot A\cdot a_j=a_{ij}$. □

(5.7) Definition

(a) $A \in \mathbb{R}^{n \times n}$ heißt POSITIV DEFINIT, wenn $A = A^t$ ist und $v^t \cdot A \cdot v > 0$ für alle $0 \neq v \in \mathbb{R}^n$.

(b) $A \in \mathbb{C}^{n \times n}$ heißt POSITIV DEFINIT, wenn $A = \overline{A}^t$ ist und $v^t \cdot A \cdot \overline{v} > 0$ für alle $0 \neq v \in \mathbb{C}^n$. □

Erinnerung

V n-dim. K-VR, $\mathcal{B} = (v_1, \ldots, v_n), \mathcal{B}' = (v'_1, \ldots, v'_n)$ Basen von V.
$T := M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$ Basiswechselmatrix, definiert durch $T := (t_{ij}) \in K^{n \times n}$ mit $v'_j = \sum\limits_{i=1}^{n} t_{ij} v_i$. □

(5.8) Satz

Sei V n-dim. K-VR und β eine Bilinearform (bzw. eine Sesquilinearform) auf V. Seien $\mathcal{B} = (v_1, \ldots, v_n)$ und $\mathcal{B}' = (v'_1, \ldots, v'_n)$ Basen von V und $T = M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$ die Basiswechselmatrix.
Setze $A := G_{\mathcal{B}}(\beta)$ und $A' := G_{\mathcal{B}'}(\beta)$. Dann gilt:
$A' = T^t \cdot A \cdot \overline{T}$ (vgl. (2.83)).

Beweis

Sei $T = (t_{ij})$, d.h. $v'_j = \sum\limits_{i=1}^{n} t_{ij} v_i$.
Beachte: $A = \left(\beta(v_i, v_j)\right), A' = \left(\beta(v'_i, v'_j)\right)$.

$$\beta(v'_i, v'_j) = \beta\left(\sum_{k=1}^{n} t_{ki} v_k, \sum_{l=1}^{n} t_{lj} v_l\right) = \underbrace{\sum_{k=1}^{n} \sum_{l=1}^{n} t_{ki} \cdot \overline{t_{lj}} \cdot \beta(v_k, v_l)}_{(i,j)\text{-Eintrag von } T^t A \cdot \overline{T}} \qquad \square$$

§ 2 Längen, Winkel, Orthogonalität

Sei $K = \mathbb{R}$ oder $\mathbb{C}$, sei V K-VR mit Skalarprodukt $(\,,\,)$.

(5.9) Definition

(a) Im Fall $K = \mathbb{R}$ [bzw. $K = \mathbb{C}$] heißt $(V, (\,,\,))$ EUKLIDISCHER [bzw. UNITÄRER] RAUM.

Die Abbildung $|| \; ||: V \to \mathbb{R}, v \mapsto \sqrt{(v,v)} \in \mathbb{R}_{\geq 0}$ heißt die EUKLIDISCHE [bzw. UNITÄRE] NORM auf V.

(b) $(\mathbb{R}^n, <,>)$ [bzw. $(\mathbb{C}^n, <,>)$] heißt der n-DIM. EUKLIDISCHE [bzw. UNITÄRE] RAUM $\mathbb{R}^n$ [bzw. $\mathbb{C}^n$]. □

(5.10) Beispiel

Im n-dim. euklidischen Raum $\mathbb{R}^n$ ist $|| \, v \, ||$ die „Länge“ des Ortsvektors v.

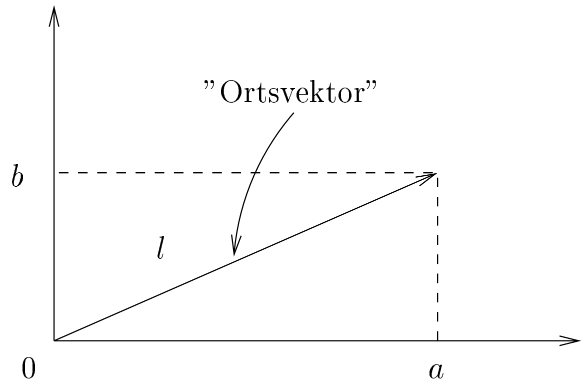

Abbildung 5.1: Ortsvektor

Länge von $\overrightarrow{0v}$ (nach Pythagoras):

$l^2 = a^2 + b^2 \Rightarrow l = \sqrt{a^2 + b^2} = \sqrt{< \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} a \\ b \end{pmatrix} >} = \sqrt{< v, v >}.$

Allgemein: $v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$.

$< v, v > = \sum\limits_{j=1}^{n} a_j^2, || \, v \, || = \sqrt{< v, v >} = \sqrt{\sum\limits_{j=1}^{n} a_j^2}.$ $\square$

(5.11) Bemerkung (Eigenschaften der Norm)

(1) $|| \; ||$ ist NORM auf V, d.h.:

(a) $|| \, v \, || \geq 0$ für alle $v \in V$ und $|| \, v \, || = 0 \Leftrightarrow v = 0$.

(b) $|| \, a \cdot v \, || = | \, a \, | \cdot || \, v \, ||$ für alle $v \in V, a \in K$.

(c) $|| \, v_1 + v_2 \, || \leq || \, v_1 \, || + || \, v_2 \, ||$ für alle $v_1, v_2 \in V$ (DREICKECKSUNGLEICHUNG).

(2) POLARISATIONSFORMELN:

(a) Für $K = \mathbb{R}$ gilt:
$(v, w) = \frac{1}{2} \cdot \left(|| \, v + w \, ||^2 - || \, v \, ||^2 - || \, w \, ||^2 \right)$ für alle $v, w \in V$.

(b) Für $K = \mathbb{C}$ gilt:
$(v, w) = \frac{1}{4} \cdot \left(|| \, v + w \, ||^2 - || \, v - w \, ||^2 + i \cdot || \, v + i \cdot w \, ||^2 - i \cdot || \, v - i \cdot w \, ||^2 \right)$ für alle $v, w \in V$.

(3) Für $0 \neq v, 0 \neq w \in W$ gilt:

$$\frac{(v,w)}{||\, v \,|| \cdot ||\, w \,||} \leq 1$$

Beweis

(1) (a) Klar mit (5.1)(b).

(b) $||\, a \cdot v \,|| = \sqrt{(a \cdot v, a \cdot v)} = \sqrt{a \cdot \overline{a} \cdot (v,v)} = \sqrt{a \cdot \overline{a}} \cdot \sqrt{(v,v)} = |\, a \,| \cdot ||\, v \,||$.

(c) (5.3) besagt: $|\,(v_1,v_2)\,|^2 \leq (v_1,v_1) \cdot (v_2,v_2)$.
$\Rightarrow |\,(v_1,v_2)\,| \leq ||\, v_1 \,|| \cdot ||\, v_2 \,||$.
Damit gilt:

$$\begin{aligned}
||\, v_1 + v_2 \,||^2 &= |\,(v_1+v_2, v_1+v_2)\,| \\
&= |\,(v_1,v_1) + (v_1,v_2) + (v_2,v_1) + (v_2,v_2)\,| \\
&\leq |\,(v_1,v_1)\,| + |\,(v_1,v_2)\,| + |\,(v_2,v_1)\,| + |\,(v_2,v_2)\,| \quad \text{(Dreiecksungleichung)} \\
&= ||\, v_1 \,||^2 + ||\, v_1 \,|| \cdot ||\, v_2 \,|| + ||\, v_2 \,|| \cdot ||\, v_1 \,|| + ||\, v_2 \,||^2 \\
&= (||\, v_1 \,|| + ||\, v_2 \,||)^2
\end{aligned}$$

(2) Übungsaufgabe auf Blatt 14.

(3) Folgt aus (5.3) (wie im Beginn des Beweises zu (1)(c)). □

(5.12) Definition und Bemerkung

(a) $v \in V$ heißt NORMIERT, falls $||\, v \,|| = 1$.

(b) Ist $0 \neq v \in V$, dann ist $\frac{v}{||v||}$ normiert.

Beweis

(b)

$$\left|\left| \frac{v}{||\, v \,||} \right|\right| \underset{(5.11)(1)(b)}{=} \left| \frac{1}{||\, v \,||} \right| \cdot ||\, v \,|| = \frac{||\, v \,||}{||\, v \,||} = 1$$ □

Bemerkung

Benutze (5.11)(3), um für euklidische Räume „WINKEL“ zu definieren.
V euklidisch, $v, w \in V$, $v, w \neq 0$.
$\underset{(5.11)(3)}{\Rightarrow} -1 \leq \frac{(v,w)}{||v|| \cdot ||w||} \leq 1$

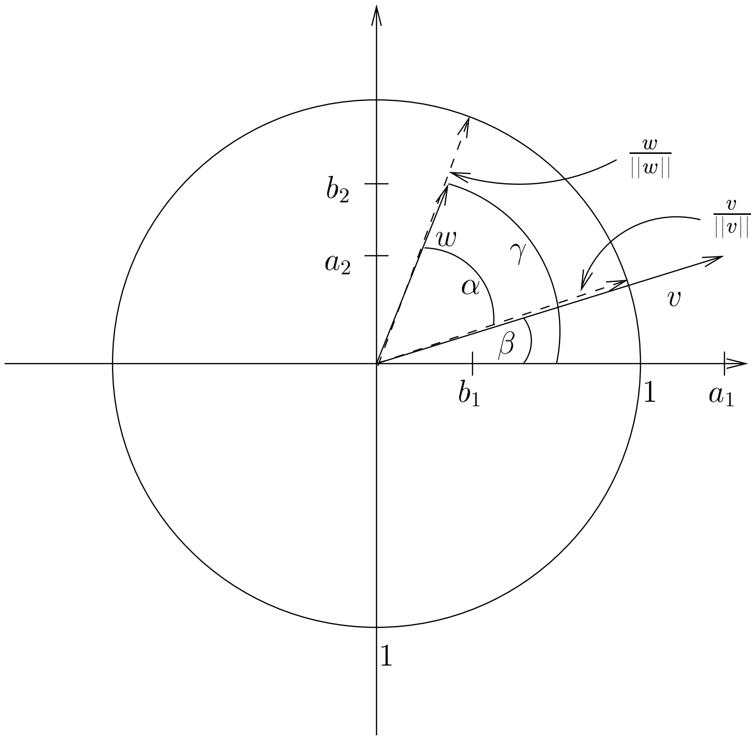

Abbildung 5.2: Winkelberechnung

$\Rightarrow$ Es existiert genau ein $\alpha \in \mathbb{R}, 0 \leq \alpha \leq \underbrace{\pi}_{\text{Kreiszahl}}$, mit $\cos\alpha = \frac{(v,w)}{||v|| \cdot ||w||} = \left(\frac{v}{||v||}, \frac{w}{||w||}\right)$.

$\frac{v}{||v||} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \frac{w}{||w||} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, \gamma = \alpha + \beta, \alpha = \gamma - \beta$

$\cos\alpha = \cos(\gamma - \beta) = \cos\gamma \cdot \cos\beta + \sin\gamma \cdot \sin\beta$

$\cos\beta = a_1, \sin\beta = a_2, \cos\gamma = b_1, \sin\gamma = b_2$

$\Rightarrow \cos\alpha = b_1 \cdot a_1 + b_2 \cdot a_2 = < \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} > = < \frac{v}{||v||}, \frac{w}{||w||} >$. □

(5.13) Definition

Sei V ein euklidischer Vektorraum.
Für $0 \neq v, w \in V$ sei $\alpha \in \mathbb{R}$, $0 \leq \alpha \leq \pi$, definiert durch $\cos\alpha = \frac{(v,w)}{||v|| \cdot ||w||}$.
α heißt WINKEL zwischen v und w.
v, w heißen ORTHOGONAL $:\Leftrightarrow \alpha = \frac{\pi}{2} \Leftrightarrow \cos\alpha = 0 \Leftrightarrow (v, w) = 0$. □

(5.14) Bemerkungen

Bezeichnungen wie in (5.13). Dann gilt:

$$\begin{aligned} v, w \text{ l.a. } &\underset{(5.3)}{\Leftrightarrow} |\,(v,w)\,|^2 = (v,v)\cdot(w,w) \\ &\Leftrightarrow |\,(v,w)\,| = ||\,v\,|| \cdot ||\,w\,|| \\ &\Leftrightarrow \cos\alpha \in \{1,-1\} \\ &\Leftrightarrow \alpha = 0 \text{ oder } \alpha = \pi, \end{aligned}$$

wobei α den Winkel zwischen v und w bezeichnet.
Sind v und w normiert, dann gilt:

$$\begin{aligned} \alpha = 0 &\Leftrightarrow v = w \\ \alpha = \pi &\Leftrightarrow v = -w \end{aligned}$$

□

(5.15) Beispiel (vgl. (2.27)(f): Suchmaschinen)

Term-Dokumente-Matrix M

- *Zeilen:* Terme (m)
- *Spalten:* Dokumente (n)
- *Einträge:* Häufigkeit eines Terms ($\rightarrow$ Zeile) in einem Dokument ($\rightarrow$ Spalten)
- *Suchanfrage:* $(0,1)$-Vektor $\in \mathbb{R}^m$ (s)
- *Gesucht:* Die Dokumente, zu denen s am Besten passt.
- *Möglichkeit:* Euklidische Norm auf $\mathbb{R}^m$ als Maß für die „Gleichheit" von s mit Spalten von M.

  Seien $d_1, \ldots, d_n$ die Spalten von m; normiere zu $c_1 = \frac{d_1}{||d_1||}, \ldots, c_n = \frac{d_n}{||d_n||}$ (Preprocessing).

  Berechne $< \frac{s}{||s||}, c_j >$ für $1 \leq j \leq n$ und gib diejenigen Dokumente aus, für die dieses Skalarprodukt größer als eine vorgegebene Schranke ist.
- *Intuition:* $< \frac{s}{||s||}, c_j > \geq 0$ für alle j, da alle Einträge der Vektoren ≥ 0.

  $< \frac{s}{||s||}, c_j > = 1 \Leftrightarrow \frac{s}{||s||} = c_j$

  $< \frac{s}{||s||}, c_j > \geq 0 \Leftrightarrow$ kein Übereinstimmung zwischen s und c_j.

□

(5.16) Satz (Schmidt'sches Orthogonalisierungsverfahren)

Seien $v_1, \ldots, v_n \in V$ l.u. und sei $0 \leq m \leq n$ mit $(v_i, v_j) = \delta_{ij}$ (Kronecker-Delta) für $1 \leq i, j \leq m$ (keine Bedingung für $m = 0$).

Dann existieren $w_1, \ldots, w_n \in V$ mit $w_j = v_j$ für $1 \leq j \leq m$ und $w_l = \sum\limits_{j=1}^{l} a_{lj} v_l$ mit geeigneten $a_{lj} \in K, a_{ll} \neq 0$ und $(w_j, w_k) = \delta_{jk}$ für $1 \leq j, k \leq n$.

Beweis (algorithmisch)

Induktion über $n - m$:
$\underline{n - m = 0}$: ✓
$\underline{n - m > 0}$: Ist w_{m+1} wie gewünscht konstruiert, dann gilt: $< v_1, \ldots, v_m, v_{m+1} >$
$=< \underbrace{w_1}_{=v_1}, \ldots, \underbrace{w_m}_{=v_m}, w_{m+1} >$, denn $v_{m+1} \in < w_1, \ldots, w_m, w_{m+1} >$, weil $a_{m+1,m+1} \neq 0$.
$\Rightarrow < v_1, \ldots, v_m, w_{m+1}, v_{m+2}, \ldots, v_n > = < v_1, \ldots, v_m, v_{m+1}, v_{m+2}, \ldots, v_n >$
$\Rightarrow < v_1, \ldots, v_m, w_{m+1}, v_{m+2}, \ldots, v_n >$ ist l.u.
Es genügt also, die Behauptung für $n = m + 1$ zu beweisen.
Sei $u := v_{m+1} - \sum\limits_{j=1}^{m} (v_{m+1}, v_j) v_j$
$\Rightarrow u \neq 0$, da $(v_1, \ldots, v_{m+1})$ l.u.
Es gilt für $1 \leq k \leq n$:

$$(u, v_k) = (v_{m+1}, v_k) - \sum_{j=1}^{m} (v_{m+1}, v_j) \cdot \underbrace{(v_j, v_k)}_{= \begin{cases} 0 & , j \neq k \\ 1 & , j = k \end{cases}} = (v_{m+1}, v_k) - (v_{m+1}, v_k) = 0.$$

$\Rightarrow w_{m+1} := \frac{u}{||u||}$ erfüllt das Gewünschte (vgl. Abbildung 5.3). □

(5.17) Beispiel

$V = \mathbb{R}^3, <,>, n = 3, m = 0.$

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, v_3 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$$

$$w_1 = \frac{v_1}{||v_1||} = \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ \frac{2}{3} \end{pmatrix}$$

$$u := v_2 - < v_2, w_1 > w_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} - 1 \cdot \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ \frac{2}{3} \end{pmatrix} = \begin{pmatrix} \frac{2}{3} \\ -\frac{2}{3} \\ \frac{1}{3} \end{pmatrix}$$

$$< u, u > = 1 \Rightarrow u = w_2 = \begin{pmatrix} \frac{2}{3} \\ -\frac{2}{3} \\ \frac{1}{3} \end{pmatrix}$$

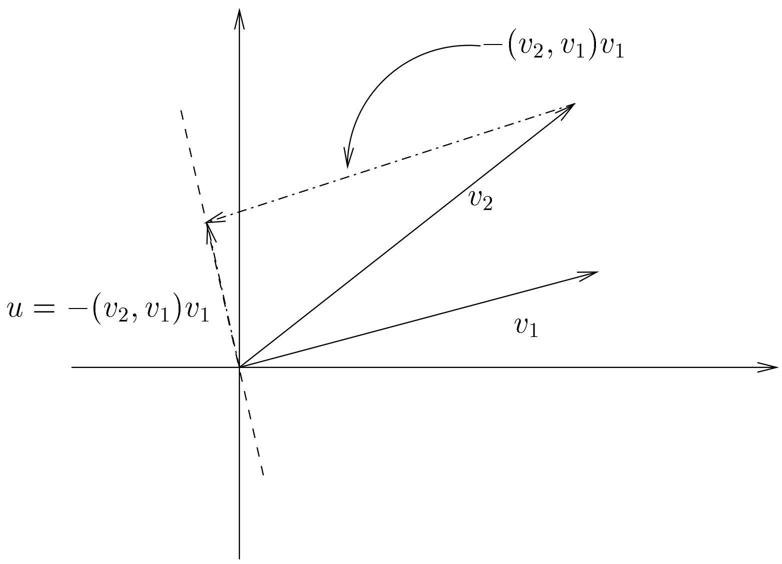

Abbildung 5.3: Orthogonalisierbarkeit

$$u := v_3 - < v_3, w_1 > w_1 - < v_3, w_2 > w_2 = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} - 0 \cdot w_1 - 1 \cdot \begin{pmatrix} \frac{2}{3} \\ -\frac{2}{3} \\ \frac{1}{3} \end{pmatrix} = \begin{pmatrix} -\frac{2}{3} \\ -\frac{1}{3} \\ \frac{2}{3} \end{pmatrix}$$

$$< u, u >= 1 \Rightarrow w_3 = \begin{pmatrix} -\frac{2}{3} \\ -\frac{1}{3} \\ \frac{2}{3} \end{pmatrix}$$ □

(5.18) Definition

(a) Sei V e.d. Eine Basis $(v_1, \ldots, v_n)$ von V heißt ORTHONORMALBASIS (ONB) von V, falls gilt:

$(v_i, v_j) = \delta_{ij}, 1 \leq i, j \leq n$

(b) Sei $U \leq V$.

$U^\perp := \{v \in V \mid (u, v) = 0$ für alle $u \in U\}$ heißt der ORTHONORMALRAUM zu U. □

(5.19) Korollar

Sei $\dim_K(V) = n$.

(a) V besitzt ONB.

(b) Ist $A \in K^{n \times n}$ positiv definit, dann existiert $S \in \mathrm{GL}_n(K)$ mit $A = S^t \cdot \overline{S}$.

(c) Ist $U \leq V$, dann ist $V = U \oplus U^\perp$ (d.h. $V = U + U^\perp$ und $U \cap U^\perp = \{0\}$).

Insbesondere ist $\dim(V) = \dim(U) + \dim(U^\perp)$.

Beweis

(a) Folgt aus (5.16) für $m = 0$.

(b) Sei $\mathcal{B}$ die Standardbasis von K^n und $\mathcal{B}'$ eine ONB bzgl. des Skalarprodukts β_A ($\beta_A(v,w) = v^t \cdot A \cdot \overline{w}$ ist Skalarprodukt nach (5.6) und (5.7)).

Nach (5.8) existiert $T \in \mathrm{GL}_n(K)$ mit $E_n = G_{\mathcal{B}'}(\beta_A) = T^t \cdot G_{\mathcal{B}}(\beta_A) \cdot \overline{T} = T^t \cdot A \cdot \overline{T}$.

$S := T^{-1}$ leistet das Gewünschte.

(c) $(\,,\,)\,|_{U \times U}$ ist Skalarprodukt auf U.

Sei $(v_1, \ldots, v_m)$ eine ONB von U, ergänze zu ONB $(v_1, \ldots, v_m, v_{m+1}, \ldots, v_n)$ von V (nach (5.16)).

Sei $W := < v_{m+1}, \ldots, v_n > \Rightarrow V = U \oplus W$.

Zu zeigen: $W = U^\perp$.

Klar: $W \subseteq U^\perp$. ✓

Sei umgekehrt $v \in U^\perp$, $v = \sum\limits_{j=1}^{n} a_j v_j$.

$\Rightarrow 0 = (v, v_k) = \sum\limits_{j=1}^{n} a_j (v_j, v_k) = a_k$ für alle $1 \leq k \leq m$.

$\Rightarrow v \in W$.

Also gilt: $W = U^\perp$ und beide Behauptungen folgen. □

(5.20) Definition

(a) $\varphi \in \mathrm{End}_K(V)$ heißt ORTHOGONAL, falls $K = \mathbb{R}$ ist (bzw. UNITÄR, falls $K = \mathbb{C}$ ist) und es gilt:

$(\varphi(v), \varphi(w)) = (v, w)$ für alle $v, w \in V$.

(b) $A \in \mathbb{R}^{n \times n}$ heißt ORTHOGONAL, falls $A^t \cdot A = E_n$ ist.

$A \in \mathbb{C}^{n \times n}$ heißt UNITÄR, falls $A^t \cdot \overline{A} = E_n$ ist.

$O(n) := \{A \in \mathbb{R}^{n \times n} \mid A \text{ orthogonal}\}$ ORTHOGONALE GRUPPE.

$U(n) := \{A \in \mathbb{C}^{n \times n} \mid A \text{ unitär}\}$ UNITÄRE GRUPPE. □

(5.21) Bemerkung

(a) Sei V n-dim. und $\mathcal{B}$ eine ONB von V.

Sei $\varphi \in \mathrm{End}_K(V)$ und $A = M_{\mathcal{B}}(\varphi)$. Dann gilt:

A orthogonal (bzw. unitär) $\Leftrightarrow$ φ orthogonal (bzw. unitär).

(b) Sei $A \in K^{n\times n}$. Dann gilt:

A orthogonal (bzw. unitär) $\Leftrightarrow$ Spalten von A bilden eine ONB von K^n bzgl. $<,>$.

(c) $O(n) \leq \mathrm{GL}_n(\mathbb{R}), U(n) \leq \mathrm{GL}_n(\mathbb{C})$.

Beweis

(a) Weil $\mathcal{B}$ eine ONB ist, ist $G_{\mathcal{B}}((,)) = E_n$, also gilt:

$(v,w) = \kappa_{\mathcal{B}}(v)^t \cdot \overline{\kappa_{\mathcal{B}}(w)}$ für alle $v,w \in V$ (vgl. (5.5)(b)).

Andererseits ist $\kappa_{\mathcal{B}}(\varphi(v)) = A\cdot\kappa_{\mathcal{B}}(v)$ (vgl. (2.74)).

$\Rightarrow (\varphi(v),\varphi(w)) = \kappa_{\mathcal{B}}(\varphi(v))^t \cdot \overline{\kappa_{\mathcal{B}}(\varphi(w))} = (A\cdot\kappa_{\mathcal{B}}(v))^t \cdot \overline{(A\cdot\kappa_{\mathcal{B}}(w))} = \kappa_{\mathcal{B}}(v)^t \cdot A^t \cdot \overline{A} \cdot \kappa_{\mathcal{B}}(w)$.

Mit $v,w \in V$ durchlaufen $\kappa_{\mathcal{B}}(v), \kappa_{\mathcal{B}}(w)$ ganz K^n.

$\Rightarrow$ Behauptung.

(b) Matrixmultiplikation.

(c) Klar ist: $O(n) \subseteq \mathrm{GL}_n(\mathbb{R}), U(n) \subseteq \mathrm{GL}_n(\mathbb{C})$ (vgl. (2.65)).

$A,B \in U(n) : (A\cdot B)^t \cdot \overline{(A\cdot B)} = B^t \cdot (A^t \cdot \overline{A}) \cdot \overline{B} = B^t \cdot E_n \cdot \overline{B} = E_n$

$\Rightarrow A\cdot B \in U(n)$.

$(A^{-1})^t \cdot \overline{(A^{-1})} = (A^t)^{-1} \cdot (\overline{A})^{-1} \underbrace{=}_{A^t=A^{-1} \text{ vertauscht mit } \overline{A}} (\overline{A}\cdot A^t)^{-1} = (A^t \cdot \overline{A})^{-1} = \overline{E_n} = E_n$. □

(5.22) Definition

Sei $A \in \mathbb{C}^{n\times n}$.
$A^+ := \overline{A}^t$ heißt die zu A ADJUNGIERTE MATRIX. □

Zusammenfassung

(a) $A \in \mathbb{C}^{n\times n}$:

A hermite'sch $\Leftrightarrow A^+ = A$ (vgl. (5.5)(b))

A unitär $\Leftrightarrow A$ invertierbar und $A^{-1} = A^+$

(b) $A \in \mathbb{R}^{n \times n}$:

A *symmetrisch* $\Leftrightarrow A^t = A$ (vgl. (5.5)(b))

A *orthogonal* $\Leftrightarrow A$ invertierbar und $A^{-1} = A^t$ □

(5.23) Definition

$\varphi \in \mathrm{End}_K(V)$ heißt SELBSTADJUNGIERT, falls gilt:
$(\varphi(v), w) = (v, \varphi(w))$ für alle $v, w \in V$. □

Analog zu (5.21) gilt:

(5.24) Bemerkung

Sei V n-dimensional und $\mathcal{B}$ eine ONB von V. Sei $\varphi \in \mathrm{End}_K(V), A := M_{\mathcal{B}}(\varphi)$. Dann gilt:
φ selbstadjungiert $\Leftrightarrow \overline{A}^t = A$.

Beweis

Für $v, w \in V$ gilt:
$(\varphi(v), w) = \kappa_{\mathcal{B}}(\varphi(v))^t \cdot \overline{\kappa_{\mathcal{B}}(w)} = \kappa_{\mathcal{B}}(v)^t \cdot A^t \cdot \overline{\kappa_{\mathcal{B}}(w)}$ und
$(v, \varphi(w)) = \kappa_{\mathcal{B}}(v)^t \cdot \overline{\kappa_{\mathcal{B}}(\varphi(w))} = \kappa_{\mathcal{B}}(v)^t \cdot \overline{A} \cdot \overline{\kappa_{\mathcal{B}}(w)}$.
Also: φ selbstadjungiert $\Leftrightarrow A^t = \overline{A} \Leftrightarrow \overline{A}^t = A$. □

§ 3 Der Spektralsatz

Sei $K = \mathbb{R}$ oder $\mathbb{C}$, sei $(V, (\,,\,))$ ein n-dim. eukl. oder unitärer Raum.

(5.25) Lemma

Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch.
Dann existiert $a \in \mathbb{R}$ mit $\chi_A(a) = 0$.
(A besitzt [mind.] einen reelen EW.)

Beweis

$\chi_A \in \mathbb{R}[X] \subseteq \mathbb{C}$.
Sei $a \in \mathbb{C}$ mit $\chi_A(a) = 0$ ($\mathbb{C}$ ist alg. abg.).
Sei $0 \neq v \in \mathbb{C}^n$ mit $A \cdot v = a \cdot v$ (v EV zum EW a).
$\Rightarrow a \cdot (v^t \cdot \overline{v}) = (a \cdot v)^t \cdot \overline{v} = (A \cdot v)^t \cdot \overline{v} = v^t \cdot A^t \cdot \overline{v} = v^t \cdot A \cdot \overline{v} = v^t \cdot \overline{A} \cdot \overline{v} = v^t \cdot \overline{A \cdot v} = v^t \cdot \overline{a \cdot v} = v^t \cdot \overline{a} \cdot \overline{v} = \overline{a} \cdot (v^t \cdot \overline{v})$.

Weil $v \neq 0$, ist auch $\underbrace{v^t \cdot \overline{v}}_{<v,v>} \neq 0$.

$\Rightarrow a = \overline{a}$. □

(5.26) Satz (Spektralsatz)

Sei $\varphi \in \mathrm{End}_K(V)$ selbstadjungiert. Sei $A \in K^{n \times n}$ mit $\overline{A}^t = A$ (d.h. A symmetrisch oder hermite'sch).

(a) Es existiert ONB von V, die aus EV von φ besteht.

(b) $K = \mathbb{R}$:

Es existiert $S \in O(n)$, so dass $S^t \cdot A \cdot S$ eine Diagonalmatrix ist, deren Diagonaleinträge die EW von A sind.

(c) $K = \mathbb{C}$:

Es existiert $S \in U(n)$, so dass $S^+ \cdot A \cdot S$ eine Diagonalmatrix ist, deren Diagonaleinträge die EW von A sind.

Beweis

(a) Induktion über n:

$\underline{n = 1:}$ ✓

$\underline{n > 1:}$ Sei $\mathcal{B}$ ONB von V, $A = M_{\mathcal{B}}(\varphi)$.

$K = \mathbb{R} \underset{(5.24)}{\Rightarrow} A^t = A \underset{(5.25)}{\Rightarrow}$ es existiert $a_1 \in \mathbb{R}$: $\chi_\varphi(a_1) = 0$.

$K = \mathbb{C} \underset{\mathbb{C}\text{ alg. abg.}}{\Rightarrow}$ es existiert $a_1 \in \mathbb{C}$: $\chi_\varphi(a_1) = 0$.

Sei $v_1 \in V$ EV von φ zum EW a_1, $|| v_1 || = 1$.

Setze $W = < v_1 >^\perp$.

Behauptung: W ist φ-invariant.

Beweis: Sei $w \in W$.

$\Rightarrow (v_1, \varphi(w)) = (\varphi(v_1), w) = (a_1 \cdot v_1, w) = a_1 \cdot (v_1, w) = 0$, da $w \in < v_1 >^\perp$

$\Rightarrow \varphi(w) \in < v_1 >^\perp = W$

$\Rightarrow$ Behauptung.

$(,)\,|_{W,W}$ ist Skalarprodukt, φ_W selbstadjungiert.

$\underset{\text{Induktion}}{\Rightarrow}$ W besitzt ONB $(v_2, \ldots, v_n)$ aus EV von φ_W

$\Rightarrow (v_1, \ldots, v_n)$ ist ONB aus EV von φ.

(b)(c) Betrachte $V = K^n$, $<,>$, $\mathcal{B}$ Standardbasis.

$\varphi = \varphi_A : K^n \to K^n, v \mapsto A \cdot v, A = M_{\mathcal{B}}(\varphi_A)$.

$\underset{(5.24)}{\Rightarrow}$ φ_A selbstadjungiert.

Sei $\mathcal{B}' = (v'_1, \dots, v'_n)$ eine ONB aus EV von $\varphi_A, \varphi_A(v'_j) = a_j \cdot v'_j, 1 \le j \le n$.

Sei $S = M_{\mathcal{B}}^{\mathcal{B}'}(\mathrm{id}_V)$ die Basiswechselmatrix.

$$\Rightarrow \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} = M_{\mathcal{B}'}(\varphi) \underset{(2.83)}{=} S^{-1} \cdot M_{\mathcal{B}}(\varphi) \cdot S = S^-1 \cdot A \cdot S.$$

Die Spalten von S sind die v'_j, sie bilden also eine ONB von V.

$\underset{(5.21)(b)}{\Rightarrow}$ $S^{-1} = \overline{S}^t$. □

(5.27) Korollar

Sei $A \in K^{n \times n}$. Dann gilt:
$\overline{A}^t = A$ (d.h. A symmetrisch oder hermite'sch)
$\Rightarrow A$ diagonalisierbar. □

(5.28) Beispiel

Sei $K = \mathbb{R}$.
Eine QUADRATISCHE GLEICHUNG über $\mathbb{R}$ ist eine Gleichung

$$Q : \sum_{j=1}^{n} \sum_{k=1}^{n} a_{jk} \cdot x_j \cdot x_k + \sum_{j=1}^{n} b_j \cdot x_j + a = 0.$$

Hierbei ist $A = (a_{jk}) \in \mathbb{R}^{n \times n}, b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, a \in \mathbb{R}$.

$x_1, \dots, x_n$ sind die UNBEKANNTEN der Gleichung.

Eine LÖSUNG von Q ist ein Element $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in \mathbb{C}^n$ mit $c^t \cdot A \cdot c + b^t \cdot c + a = 0$.

$Q(\mathbb{C})$ = Menge der Lösungen von Q.
$Q(\mathbb{C})$ heißt QUADRIK.
$Q(\mathbb{R}) := Q(\mathbb{C}) \cap \mathbb{R}^n$: reele Punkte von $Q(\mathbb{C})$.
<u>Geometrische Beschreibung von $Q(\mathbb{R})$:</u>
Spezialfall: $A = A^t, b = 0$.
$Q : x^t \cdot A \cdot x + a = 0, x \in \mathbb{C}$.

Nach (5.26)(b) existiert $S \in O(n)$ mit $S^{-1} \cdot A \cdot S = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$.

Mit $c' := S \cdot c$ für $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in \mathbb{R}^n$ gilt damit:

$(c')^t \cdot A \cdot c' + a = 0 \Leftrightarrow c^t \cdot (S^t \cdot A \cdot S) \cdot c + a = 0 \Leftrightarrow \left(\sum_{j=1}^{n} a_j c_j^2 \right) + a = 0.$

Mit $Q' : \left(\sum_{j=1}^{n} a_j x_j^2 \right) + a = 0$ haben wir: $Q(\mathbb{R}) = S \cdot Q'(\mathbb{R})$.

Koordinatentransformation: $x' := S \cdot x, x \in \mathbb{R}^n$, bildet $e_1, \ldots, e_n$ (Standardbasis von $\mathbb{R}^n$) ab auf die ONB $e_1', \ldots, e_n'$ mit $e_j' = S \cdot e_j$ (Spalte j von S).
$< e_1 >, \ldots, < e_n >$ heißt ein System von Hauptachsen für Q.
Satz (5.26)(b) heißt auch Satz von der Hauptachsentransformation. □

Beispiel

Sei $A = \begin{pmatrix} 5 & 2 \\ 2 & 8 \end{pmatrix}$.
$Q : x^t \cdot A \cdot x - 36 = 0$
$S = \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \in O(2)$
$S^{-1} = S^t = \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$
$S^t \cdot A \cdot S = \begin{pmatrix} 9 & 0 \\ 0 & 4 \end{pmatrix}$
$Q' : 9x_1^2 + 4x_2^2 = 36$ (Ellipse)
$x' := S \cdot x, x \in \mathbb{R}^2, e_1' = S \cdot e_1 = \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix}, e_2' = \frac{1}{\sqrt{5}} \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ □

§ 4 Orthogonale Endomorphismen

Sei $K = \mathbb{R}$, sei $(V, (\,,\,))$ ein n-dim. euklidischer Raum.

(5.29) Bemerkung

Sei $A \in 0(2)$.
Dann existiert $\alpha \in \mathbb{R}, 0 \leq \alpha < 2\pi$ mit:

(1) $A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ oder

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

Im Fall (1) ist $\varphi_A : \mathbb{R}^2 \to \mathbb{R}^2$ eine Drehung um den Winkel α und $\chi_A = X^2 - 2\cdot\cos\alpha\cdot X + 1$.
Im Fall (2) ist φ_A eine Spiegelung an der Geraden durch $\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} \cos\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} \end{pmatrix}$ und A ist ähnlich zu $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ (vgl. (4.24)).

Beweis

Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

$$\underset{A\in O(2)}{\Longrightarrow} \begin{matrix} a^2+c^2=1 \\ b^2+d^2=1 \\ a\cdot b+c\cdot d=0 \end{matrix} \quad \text{und} \quad \begin{matrix} a^2+b^2=1 \\ c^2+d^2=1 \end{matrix} \quad [A^t\cdot A = E_2 = A\cdot A^t]$$

$\Rightarrow$ Existenz von α wie behauptet.

(1) $\varphi_A(e_1) = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \varphi_A(e_2) = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$

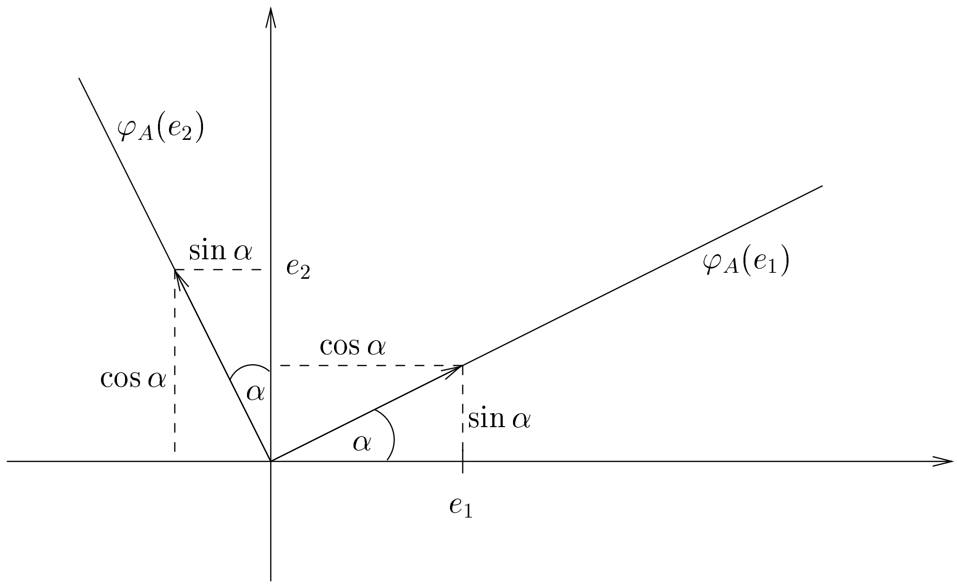

Abbildung 5.4: $\varphi_A(e_1)$ und $\varphi_A(e_2)$

Berechnung von χ_A selbst.

(2) $\varphi_A(e_1) = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \varphi_A(e_2) = \begin{pmatrix} \sin\alpha \\ -\cos\alpha \end{pmatrix}$

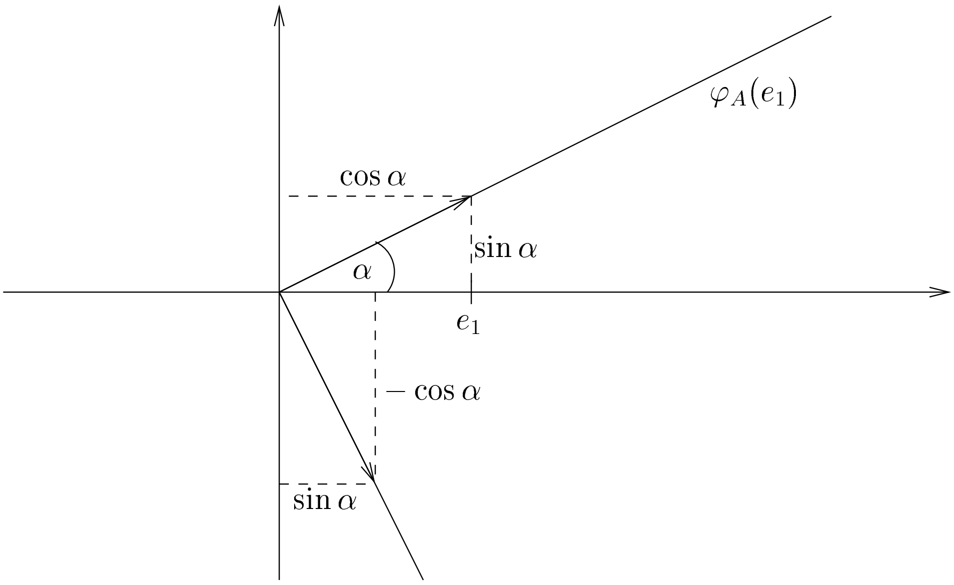

Abbildung 5.5: $\varphi_A(e_1)$ und $\varphi_A(e_2)$

$$\chi_A = \begin{vmatrix} X-\cos\alpha & -\sin\alpha \\ -\sin\alpha & X+\cos\alpha \end{vmatrix} = X^2-\cos^2\alpha-\sin^2\alpha = X^2-1 = (X-1)\cdot(X+1).$$

Behauptung folgt aus (4.29)(b) und (4.24). □

(5.30) Bemerkung

Sei $f \in \mathbb{R}[X]$ irreduzibel.
$\Rightarrow \deg(f) \leq 2.$

Beweis

Ist f linear, dann okay.
Sei also $\deg(f) \geq 2, f = \sum\limits_{j=0}^{m} a_j X^j, a_m = 1$ (o.B.d.A.), $m \geq 2$.
Sei $z \in \mathbb{C}$ Nullstelle von f, d.h. $0 = \sum\limits_{j=0}^{m} a_j z^j$.
$\Rightarrow 0 = \overline{0} = \sum\limits_{j=0}^{m} \overline{a_j} \cdot \overline{z}^j = \sum\limits_{j=0}^{m} a_j \cdot \overline{z}^j$, d.h. $\overline{z}$ ist auch Nullstelle von f.
$z = \overline{z}$, sonst wäre $z \in \mathbb{R}$ eine reele Nullstelle von f und $X - z \mid f$ in $\mathbb{R}[X]$.
$\Rightarrow X - z \neq X - \overline{z}$ und $(X-z)\cdot(X-\overline{z}) \mid f$ in $\mathbb{C}[X]$
$(X-z)\cdot(X-\overline{z}) = X^2 - (z+\overline{z})\cdot X + z\cdot\overline{z} \in \mathbb{R}[X]$
Fassen wir $(X-z)\cdot(X-\overline{z})$ für jede Nullstelle z von f zusammen, dann erhalten wir eine Faktorisierung von f in $\in \mathbb{R}[X]$ in Faktoren vom Grad z.

$\Rightarrow$ Behauptung. □

(5.31) Bemerkung

Sei $\varphi \in \mathrm{End}_{\mathbb{R}}(V)$ orthogonal.

(a) Ist $W \leq V$ φ-invariant, dann ist auch $W^\perp$ φ-invariant und es gilt: $V = W \oplus W^\perp$.

(b) Es existiert $W \leq V$ φ-invariant mit $\dim_{\mathbb{R}}(W) \leq 2$.

Beweis

(a) Sei $\mathcal{B}$ eine ONB von V und $A = M_{\mathcal{B}}(\varphi)$.

$\underset{(5.21)(a)}{\Rightarrow}$ A orthogonal $\underset{(5.21)(c)}{\Rightarrow}$ A invertierbar und A^{-1} ist auch orthogonal

$\underset{(5.21)(a)}{\Rightarrow}$ φ^{-1} ist orthogonal und $\varphi(W) = W, \varphi^{-1}(W) = W$.

Sei nun $w \in W, u \in W^\perp$.

$\Rightarrow (u, \varphi(u)) = \left(\varphi^{-1}(w), \varphi^{-1}(\varphi(u))\right) = \left(\varphi^{-1}(w), u\right) = 0$, da $u \in W^\perp$ und $\varphi^{-1}(w) \in W$.

$\Rightarrow \varphi(u) \in W^\perp$, d.h. $W^\perp$ ist φ-invariant.

Die 2. Behauptung ist gerade (5.19)(c).

(b) Sei $\chi_\varphi = f_1 \cdots f_r$ mit $f_i \in \mathbb{R}[X]$ normiert und irreduzibel.

Ist f_j linear für ein $j \leq r$, dann hat φ einen EV, also auch einen 1-dim. φ-invarianten Unterraum.

Sei also $\deg(f_j) = 2$ für $1 \leq j \leq r$.

Sei $0 \neq w \in V$.

$\underset{(4.49)}{\Rightarrow}$ $0 = \chi_\varphi(\varphi)(w) = (f_1(\varphi) \circ \cdots \circ f_r(\varphi))(w)$.

$\Rightarrow$ Es existiert $1 \leq j \leq r$ mit

$v := \underbrace{\left(f_{j+1}(\varphi) \circ \cdots \circ f_r(\varphi)\right)}_{\text{Konvention: } \mathrm{id}_V \text{, falls } j=r}(w) \neq 0$ und $f_j(\varphi) \circ \left(f_{j+1}(\varphi) \circ \cdots \circ f_r(\varphi)\right)(w) = 0$.

$\Rightarrow v \neq 0, f_j(\varphi)(v) = 0$.

$\Rightarrow < v, \varphi(v) >$ ist φ-invariant. □

(5.32) ! Satz

Sei $\varphi \in \mathrm{End}_{\mathbb{R}}(V)$ orthogonal.
Dann existiert ONB $\mathcal{B}$ von V mit

$$M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_k} \end{pmatrix}$$

mit $A_j = (1) \in \mathbb{R}^{1\times 1}$ oder $A_j = (-1) \in \mathbb{R}^{1\times 1}$ oder $A_j = \begin{pmatrix} \cos\alpha_j & -\sin\alpha_j \\ \sin\alpha_j & \cos\alpha_j \end{pmatrix} \in \mathbb{R}^{2\times 2}$ für ein $\alpha_j \in \mathbb{R}$ mit $0 \leq \alpha_j \leq 2\pi$.

Beweis

Sei $0 \neq W \leq V$ φ-invariant mit $\dim_{\mathbb{R}}(W) \leq 2$.
$\underset{(5.31)}{\Rightarrow}$ $V = W \oplus W^{\perp}$ und $W^{\perp}$ ist φ-invariant.
Seien $\mathcal{B}_1 = (v_1, \ldots, v_j)$ (mit $j = 1, 2$) bzw. $\mathcal{B}_2 = (v_{j+1}, \ldots, v_n)$ ONB's von W bzw. $W^{\perp}$.
$\Rightarrow \mathcal{B} = (v_1, \ldots, v_n)$ ist ONB von V und
$M_{\mathcal{B}}(\varphi) = \left(\begin{array}{c|c} M_{\mathcal{B}_1}(\varphi_W) & 0 \\ \hline 0 & M_{\mathcal{B}_2}(\varphi_{W^{\perp}}) \end{array}\right)$.
Nach Induktion über n genügt es also, die Behauptung für $n \leq 2$ zu beweisen.
$\underline{n = 1}$: ✓
$\underline{n = 2}$: Verwende (5.29).
Im Fall (2) ist $\mathcal{B}_1 = \left(\begin{pmatrix} \cos\frac{\alpha+\pi}{2} \\ \sin\frac{\alpha+\pi}{2} \end{pmatrix}, \begin{pmatrix} \cos\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} \end{pmatrix} \right)$ die gesuchte ONB. □

— ENDE —

Abbildungsverzeichnis

Index