Lineare Algebra I

Mitschrift von Jens Liebchen

WS 2001/2002

Vorwort

Dieses Skript enthält den Inhalt der Vorlesung „Lineare Algebra I" des Wintersemesters 2001/2002 bei Prof. Dr. G. Hiß. Es wurde anhand der vorhandenen Mitschriften von mir in LaTeX gesetzt und erhebt daher keinerlei Anspruch auf Korrektheit und Vollständigkeit. Bei Unstimmigkeiten und evtl. vorhandenen Fehlern bitte ich um eine Email an untenstehende Adresse. Dieses Skript stellt keine offizielle Veröffentlichung des Lehrstuhls D für Mathematik der RWTH Aachen dar.

Letzte Änderung: 23. März 2002

Jens Liebchen
jens@baer.rwth-aachen.de
Download unter http://www.liebchen-online.de/LAI2001

Inhaltsverzeichnis

Kapitel 1

Motivation und Grundlagen

1.1 Mengen

Definition 1.1.1 (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 Paradox:

Sei M die Menge aller derjenigen Mengen, die sich nicht selbst als Objekt enthalten. **Frage**: ist M als Objekt in M enthalten?

Auflösung der Widersprüche

- Axiomatische Mengenlehre (Logik-Vorlesung)
- Naive Mengenlehre (Unser Standpunkt). (Cantors Definition, aber vorsichtig verwendet)

Arbeitsweise

Eine Menge ist gebildet (existiert), wenn feststeht, 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:

$$M = M' \Leftrightarrow \text{Jedes Element von } M \text{ ist Element von } M' \text{ und umgekehrt}$$

Schreibweise für Mengen

- Aufzählung: $\{1,3,17\} = \{3,1,17\} = \{1,3,17,3,1\}$
- Beschreibung:

  $\mathbb{N} :=$ Menge der natürlichen Zahlen $= \{1,2,3,...\}$ $0 \notin \mathbb{N}$
  $\mathbb{Z} :=$ Menge der ganzen Zahlen $= \{..., -2, -1, 0, 1, 2, ...\}$
  $\mathbb{Q} :=$ Menge der rationalen Zahlen
  $\mathbb{R} :=$ Menge der reelen Zahlen

Aussondern:

M sei eine Menge, E eine Eigenschaft (die ein $x \in M$ hat oder nicht). Dann ist auch $\{x \in M |$ x hat Eigenschaft E $\}$ eine Menge.

z.B.: $\{x \in \mathbb{N} |$ x ist gerade $\}$

Definition 1.1.2 *M, N seien Mengen*

a) $N \subseteq M :\Leftrightarrow$ *[für alle $x \in N$ gilt: $x \in M$]*
N ist Teilmenge von M
Es gilt $M = N \Leftrightarrow$ [$N \subseteq M$ und $M \subseteq N$]

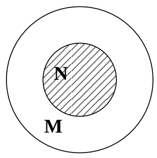

Abbildung 1.1: Teilmenge $N \subseteq M$

b) *Durchschnitt von M und N:* $M \cap N := \{x \in M | x \in N\} = \{x \in N | x \in M\}$

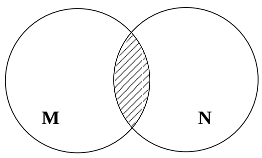

Abbildung 1.2: Durchschnitt $M \cap N$

c) *Vereinigung von M und N:* $M \cup N := \{x | x \in M$ *oder* $x \in N\}$

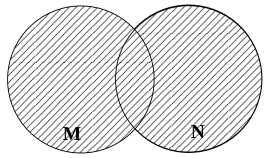

Abbildung 1.3: Vereinigung $M \cup N$

d) *Cartesisches Produkt von M und N:* $M \times N := \{(x,y) | x \in M \text{ und } y \in N\}$
(x,y) *ist geordnetes Paar, d.h.* $(x,y) = (x',y') \Leftrightarrow [x = x' \wedge y = y']$

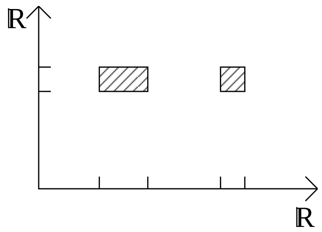

Abbildung 1.4: Cartesisches Produkt $M \times N$

e) *Potenzmenge von M:* $Pot(M) := \{X \mid X \subseteq M\}$

Beispiel: $M = \{1,2\}, Pot(M) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

Allgemein gilt: Hat M n Elemente ($n \in \mathbb{N}_0$)*, dann hat* $Pot(M)$ 2^n *Elemente.*

f) $\emptyset$*: Leere Menge (die Menge ohne Elemente).*
$\emptyset \subseteq M$ *für alle Mengen M.*

Eine Menge M heißt **endlich**, wenn M nur endlich viele Elemente hat. Wir schreiben in diesem Fall

$$|M| := \text{Anzahl der Elemente von M}$$

1.2 Vollständige Induktion

Beweismethode, beruht auf:

(I) Sei $A \subseteq \mathbb{N}$. Dann gilt: Ist $1 \in A$ und ist für jedes $n \in A$ auch $n + 1 \in A$, dann ist $A = \mathbb{N}$.

Behauptungen der Form: „Für alle $n \in \mathbb{N}$ gilt $\mathcal{A}(n)$“ lassen sich nach folgendem Schema beweisen:

Induktionsanfang

Zeige $\mathcal{A}(1)$ ist richtig.

Induktionsschritt

Annahme: $\mathcal{A}(n)$ ist richtig.
Zeige unter dieser Annahme $\mathcal{A}(n+1)$ ist richtig.
Dann gilt $\mathcal{A}(n)$ für alle $n \in \mathbb{N}$, denn die Menge $A := \{n \in \mathbb{N} | \mathcal{A}(n) \text{ ist richtig}\}$ erfüllt die Vorraussetzungen 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: $(1+x)^n \geq 1 + nx$

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

Induktionsschritt
$n \to n+1$: Es gelte $(1+x)^n \geq 1 + nx$

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)(1+x)^n \\
&\underbrace{\geq}_{\left((1+x)^n \geq 1+nx \text{ und } 1+x \geq 0 \right)} (1+x)(1+nx) \\
&= 1 + x + nx + nx^2 \\
&\underbrace{\geq}_{\left(nx^2 \geq 0 \right)} 1 + x + nx \\
&= 1 + (n+1)x
\end{aligned}$$

b)

Der Induktionsanfang ist wichtig!

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

Induktionsschritt: $n \to n+1$

$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{(n+\frac{1}{2})^2}{2} + (n+1) = \frac{n^2+n+\frac{1}{4}+2n+2}{2} = \frac{n^2+3n+\frac{9}{4}}{2} = \frac{((n+1)+\frac{1}{2})^2}{2}$

Bemerkung: Es nicht nötig, bei 1 zu beginnen!

1.3 Abbildungen

Definition 1.3.1 *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: $f\colon \begin{array}{l} M \to N \\ x \mapsto f(x) \end{array}$

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 ein Bild von $x \in M$*

Beispiele

a)

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{R} \\ i &\mapsto i^2 \end{aligned}$$

Oft benutzen wir für Folgen (d.h. Abbildungen mit Definitionsbereich $\mathbb{N}$) die Schreibweise

$$a_1, a_2, ..., \underbrace{a_i}_{f(i)}, ...$$

so dass unsere obige Abbildung geschrieben werden könnte als:

$$1, 4, 9, 16, ...$$

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

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$(x, y) \mapsto x + y$$

c) Sei M Menge,

$$\begin{aligned} id_M : M &\to M \\ x &\mapsto x \end{aligned}$$

heißt die Identität auf M.

Definition 1.3.2 (inkl. Beispiel) *Sei M eine Menge (z.B. $M = \mathbb{R}$)*

a) *Für $n \in \mathbb{N}$ sei $\underline{n} := \{1, 2, ..., n\} \subseteq \mathbb{N}$.*
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 $t_1, t_2, ..., t_n$, meist mit Klammern $(t_1, t_2, ..., t_n)$, wobei wir $t_i := t(i)$, $i = 1, ..., n$ gesetzt haben.)

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

1.3.1 Injektive, surjektive und bijektive Abbildungen

Definition 1.3.3 *Sei $f : M \to N$ Abbildung.*

a) *Für $X \subseteq M$ sei*

$$f(X) := \{\ \underbrace{f(x)}_{Argument}\ | x \in X\} = \{y \in N \mid \exists x \in X \text{ mit } y = f(x)\} \subseteq N$$

*Das Argument heißt **Bild von X**.*

b) *Für $Y \subseteq N$ sei*

$$f^{-1}(Y) := \{y \in M \mid f(y) \in Y\} \subseteq M$$

*das **Urbild von Y**. (f^{-1} hat nichts mit Umkehrfunktion zu tun).*
*Die Mengen $f^{-1}(\{y\}) \subseteq M$, $y \in N$ heißen die **Fasern von f**.*

c) *f heißt **surjektiv**, falls $f(M) = N$ (siehe Abbildung 1.5).*

*f heißt **injektiv**, falls gilt: Sind $x, x' \in M$ mit $f(x) = f(x')$, dann ist $x = x'$ (siehe Abbildung 1.6).*

*f heißt **bijektiv**, falls f injektiv und surjektiv ist (siehe Abbildung 1.7).*

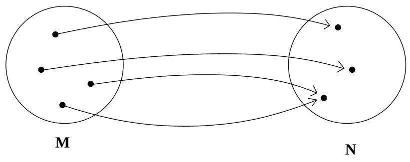

Abbildung 1.5: Surjektive Abbildung

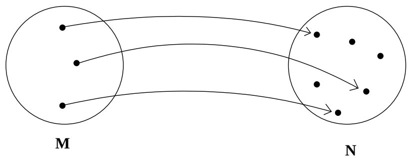

Abbildung 1.6: Injektive Abbildung

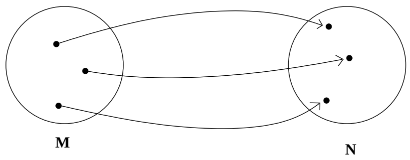

Abbildung 1.7: Bijektive Abbildung

Beispiel

- $f : \mathbb{R} \to \mathbb{R},\ x \mapsto 2x$ (Abbildung 1.8) ist bijektiv

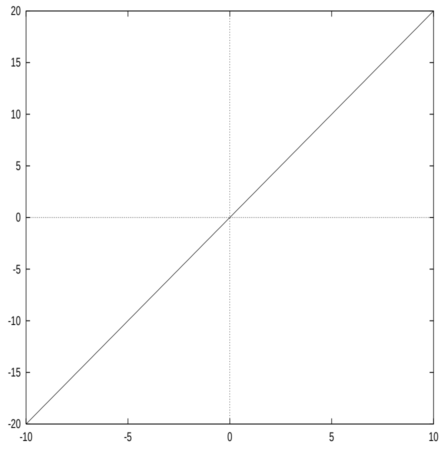

Abbildung 1.8: $f(x) = 2x$

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

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

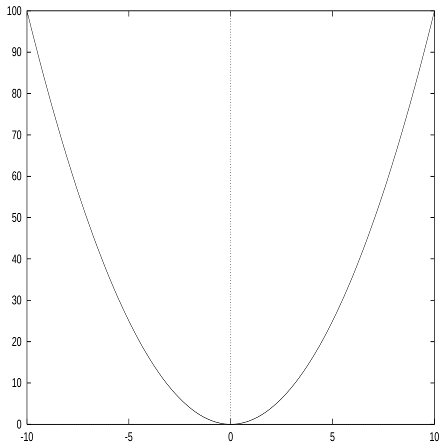

Abbildung 1.9: $f(x) = x^2$

$f_1 : \mathbb{R} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^2$ ist surjektiv aber nicht injektiv.
Fasern von f_1: $f_1^{-1}(\{y\}) = \{-\sqrt{y}, \sqrt{y}\}$, $y \in \mathbb{R}_{\geq 0}$

- $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$ ist injektiv, aber nicht surjektiv.
- $f : \mathbb{N} \to \{0, 1\}$, $x \mapsto$ Rest von x bei Division durch 2
  $f^{-1}(\{0\}) = \{x \in \mathbb{N} \,|\, \text{x ist gerade}\}$
  $f^{-1}(\{1\}) = \{x \in \mathbb{N} \,|\, \text{x ist ungerade}\}$

  f hat genau zwei Fasern.
- $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(x, y) \mapsto 2x + y$

  Für $a \in \mathbb{R}$ gilt:
  $f^{-1}(\{a\}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, 2x + y = a\} = \{(x, y) \,|,\ y = -2x + a\}$
  (Vergleiche Abbildung 1.10)

Definition 1.3.4 *Seien $f : M \to N$ und $g : L \to M$ Abbildungen. Dann heißt die Abbildung*

$$f \circ g \quad L \to N, \quad x \mapsto f \circ g(x) := f(g(x))$$

die ***Komposition von f mit g*** *(siehe Abbildung 1.11).*

Bemerkungen:

Sei $f : M \to N$. Dann gilt: f bijektiv $\Leftrightarrow$ f besitzt eine **Umkehrabbildung**, d.h. es existiert $g : N \to M$ mit $g \circ f = id_M$ und $f \circ g = id_N$.

Ist f bijektiv und g Umkehrabbildung von f wie oben, dann ist g durch f eindeutig bestimmt und wird mit f^{-1} bezeichnet.

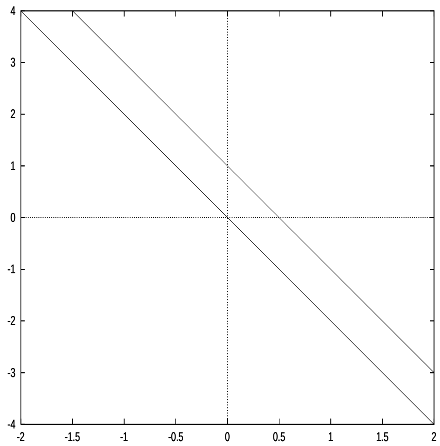

Abbildung 1.10: $f^{-1}(\{0\})$ und $f^{-1}(\{1\})$

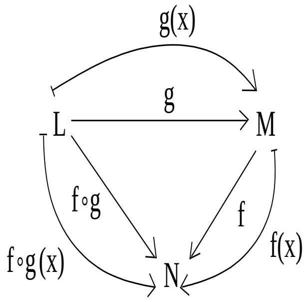

Abbildung 1.11: Kompostion von f mit g

Konventionen

1. Zu jeder Menge M existiert genau eine Abbildung $\emptyset \to M$.
2. Ist $M \neq \emptyset$ eine Menge, dann existiert keine Abbildung $M \to \emptyset$

Beispiele

1.
$$\begin{aligned} f &: \mathbb{R} \to \mathbb{R}, \quad x \mapsto 2x \text{ ist bijektiv.} \\ f^{-1} &: \mathbb{R} \to \mathbb{R}, \quad x \mapsto \frac{1}{2}x \text{ ist die Umkehrabbildung.} \end{aligned}$$

2.
$$\begin{aligned} f &: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \quad x \mapsto x^2 \text{ ist bijektiv.} \\ f^{-1} &: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \quad x \mapsto \sqrt{x} \text{ ist die Umkehrabbildung.} \end{aligned}$$

1.4 Lineare Gleichungssysteme und Matrizen

Definition 1.4.1 *Ein lineares Gleichungssystem (über* $\mathbb{R}$*), kurz LGS, hat die Form*

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

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.* $x_1, ..., x_n$ *sind „Unbekannte“.*

Gegeben: a_{ij}, $b_i \in \mathbb{R}$
Gesucht: Alle Lösungen des LGS.

Eine Lösung ist eine „Liste“ $s_1, s_2, ..., s_n$ mit $s_j \in \mathbb{R}, 1 \leq j \leq n$ (später als Spalte geschrieben), so dass alle m Gleichungen des LGS richtig werden (erfüllt sind), wenn $x_j = s_j$ gesetzt wird.

1.4.1 Bemerkung

Die Menge der Lösungen eines LGS ändert sich nicht, wenn

a) zwei Gleichungen vertauscht werden,

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

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

Beweis:

a) klar.

b) Linke Seiten der beiden Gleichungen nach Einsetzen von $s_1, ..., s_n$:

vor	nach
a_1	a_1
a_2	$a_2 + ca_1$

Rechte Seiten der beiden Gleichungen:

vor	nach
b_1	b_1
b_2	$b_2 + cb_1$

zu zeigen

$$a_1 = b_1 \text{ und } a_2 = b_2 \Leftrightarrow a_1 = b_1 \text{ und } a_2 + ca_1 = b_2 + cb_1$$

Beweis:

„⇒“:
$$\begin{aligned} & a_1 = b_1 \Rightarrow ca_1 = cb_1 \\ \Rightarrow\ & a_2 + ca_1 = b_2 + cb_1 \end{aligned}$$

„⇐“:
$$\begin{aligned} & a_2 + ca_1 = b_2 + cb_1 \text{ und } ca_1 = cb_1 \\ \Rightarrow\ & a_2 = b_2 \text{ (Subtraktion von } ca_1 = cb_1) \end{aligned}$$

c) Linke Seiten:

vor	nach
a	ca

Rechte Seiten:

vor	nach
b	cb

zu zeigen:

$$a = b \Leftrightarrow ca = cb$$

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

1.4.2 Beispiele

a)

$$\left.\begin{array}{rcrcrcrcr} x_1 & + & 2x_2 & & & + & x_4 & = & 1 \\ x_1 & + & 2x_2 & + & 2x_3 & + & 3x_4 & = & 5 \\ 2x_1 & + & 4x_2 & & & + & 3x_4 & = & 5 \\ & & & & 3x_3 & + & 2x_4 & = & 3 \end{array}\right\} (*)$$

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

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

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

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

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.

$$\left.\begin{array}{rcrcrcrcr} x_1 & + & 2x_2 & & & & & = & -2 \\ & & & + & x_3 & & & = & -1 \\ & & & & & & x_4 & = & 3 \\ & & & & & & 0 & = & 0 \end{array}\right\} (**)$$

Nach Bemerkung 1.4.1 haben die LGS (*) und (**) die gleichen Lösungen.

$s_1, ..., s_4$ ist Lösung von (**) $\Leftrightarrow$
$s_1 = -2 - 2a$
$s_2 = a, \quad a \in \mathbb{R}$ beliebig
$s_3 = -1$
$s_4 = 3$

Insbesondere hat (*) unendlich viele Lösungen.

b)

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

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

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

$$x_1 = \frac{3}{5}$$

$$x_2 = -\frac{2}{5}$$

Es gibt genau eine Lösung.

c)

$$\begin{array}{rcrcl} x_1 & - & x_2 & = & 1 \\ -2x_1 & + & 2x_2 & = & 0 \end{array}$$

$$\begin{array}{rcrcl} x_1 & - & x_2 & = & 1 \\ & & 0 & = & 2 \end{array}$$

↯ Widerspruch!
Dieses LGS hat keine Lösung.

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, genau eine oder gar keine Lösung hat?
2. Mathematische Präzisierung des Begriffes „Lösung“.
3. Hat die Menge der Lösungen eine „Struktur“?

Beispiel (Elektrotechnik)

Netzwerk aus Leitern und Widerständen:

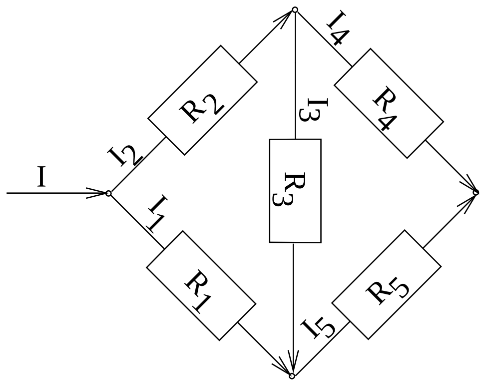

Abbildung 1.12: Netzwerk

I: Stromstärke des ein- (und aus-) fließenden gerichteten Gleichstroms (in A).

R_j, $1 \leq j \leq 5$: Bekannte Widerstände
I_j, $1 \leq j \leq 5$: 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.

$\Rightarrow$ LGS:

$$\left.\begin{array}{ccccccccccc} I_1 & + & I_2 & & & & & & & = & I \\ & & I_2 & - & I_3 & - & I_4 & & & = & 0 \\ I_1 & & & + & I_3 & & & - & I_5 & = & 0 \\ & & & & & & I_4 & + & I_5 & = & I \end{array}\right\} \text{a)}$$

$$\left.\begin{array}{ccccccccccc} -R_1I_1 & + & R_2I_2 & + & R_3I_3 & & & & & = & 0 \\ & & & - & R_3I_3 & + & R_4I_4 & - & R_5I_5 & = & 0 \end{array}\right\} \text{b)}$$

1.4.3 Körper

Definition 1.4.2 *Eine Menge K heißt **Körper** (field), wenn zwei Abbildungen definiert sind:*

$$+ : K \times K \to K,\ (a,b) \mapsto a+b$$

$$\cdot : K \times K \to K,\ (a,b) \mapsto a \cdot b$$

so dass gilt:

1. $(a+b)+c = a+(b+c) \quad \forall a,b,c \in K$
2. $\exists 0 \in K$ *mit* $a+0 = 0+a = a \quad \forall a \in K$
3. $\forall a \in K$ *existiert* $-a \in K$ *mit* $a+(-a) = 0 = (-a)+a$
4. $a+b = b+a \quad \forall a,b \in K$
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a,b,c \in K$
6. *Es existiert* $1 \in K$, $1 \neq 0$, *mit* $1 \cdot a = a \cdot 1 = a \quad \forall a \in K$
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. $a \cdot b = b \cdot a \quad \forall a,b \in K$
9. $a \cdot (b+c) = a \cdot b + a \cdot c$ *und* $(a+b) \cdot c = a \cdot c + b \cdot c \quad \forall a,b,c \in K$

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.

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 $\mathbb{R}$) (z.B. $\underline{1}$, $1 = 1 + 0 \cdot \sqrt{3}$, $\frac{13}{11}\sqrt{3}$, $-17 + \sqrt{3}$)

$0,\ 1 \in \mathbb{R}$ liegen in $\mathbb{Q}(\sqrt{3})$, mit $a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ ist auch $-(a + b\sqrt{3}) = -a + (-b)\sqrt{3} \in \mathbb{Q}(\sqrt{3})$
$\Rightarrow$ (nach Definition 1.4.2): 1. bis 6., 8., 9.

Wie ist es 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 $\mathbb{Z}$.

$$\Rightarrow \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3} \quad \in \mathbb{Q}(\sqrt{3})$$

$$\text{und ergibt:} \qquad \frac{1}{a^2 - 3b^2}\,(a - b\sqrt{3})\,(a + b\sqrt{3}) \;=\; \frac{1}{a^2 - 3b^2} \;=\; 1$$

Also ist $\mathbb{Q}(\sqrt{3})$ ein Körper.

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 $\mathbb{F}_2$ bezeichnen ($\mathbb{F}$ steht für Field, Index 2 für 2 Elemente).

1.4.4 Matrizen

Definition 1.4.3 *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:*

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

Die $a_{ij} \in K$, $1 \le i \le m, 1 \le j \le n$ 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 $z_i := (a_{i1}, a_{i2}, \dots, a_{i,n})$ heißt die i-te Zeile von A (row). Wir schreiben auch

$$A = \begin{pmatrix} z_1 \\ z_2 \\ \dots \\ z_m \end{pmatrix}$$

Die $(m \times 1)$-Matrix

$$s_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \dots \\ a_{mj} \end{pmatrix}$$

heißt die j-te Spalte von A (column). Wir schreiben auch $A = (s_1, s_2, \dots s_n)$

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:

$$\begin{aligned} z_1 &= (0 \quad 1 \quad -2 \quad 3) \\ z_2 &= (\tfrac{5}{4} \quad 1 \quad 0 \quad 0) \\ z_3 &= (1 \quad 2 \quad 3 \quad 4) \end{aligned}$$

Spalten von A:

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

Definition 1.4.4 (Math. präzise Definition einer Matrix über K (K Körper))
Eine $(m \times n)$-Matrix A über K ist eine Abbildung

$$A : \underline{m} \times \underline{n} \to K, \quad \underbrace{(i,j)}_{\text{Position}} \mapsto \underbrace{a_{ij}}_{\text{Eintrag in } A \text{ an Pos } i,j}$$

Konventionen

a) Eine $(1 \times n)$-Matrix oder eine $(n \times 1)$-Matrix über K nennen wir auch **n-Tupel** (vergl. 1.3.2).

b) $K^n := K^{n \times 1}$ Menge der **Spalten-n-Tupel** über K.
$\mathbb{R}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$

Definition 1.4.5 *a) Gegeben sei das LGS über K*

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

$a_{ij},\ b_i \in K(1 \le i \le m,\ 1 \le j \le n)$.

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

$b := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m$ *heißt die **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.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ & & \vdots & & \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

*heißt die **erweiterte (Koeffizienten)-Matrix** des LGS.*

Eine ***Lösung*** *des LGS ist ein Element* $s := \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \in K^n$ *(also ein Spalten-n-Tupel) mit* $\sum\limits_{j=1}^{n} a_{ij}s_j = b_j$ *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* $(A, b) \in K^{m\times(n+1)}$, $b \in K^m$ *bestimmt umgekehrt ein LGS, dessen erweiterte Koeffizientenmatrix sie ist.*

Beispiel

a) Das LGS aus dem Beispiel 1.4.2 hat die 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 dem Beispiel aus der Elektrotechnik im Abschnitt 1.4.2 sind

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

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

$$L = \emptyset \subseteq \mathbb{R}^2 \quad \text{in c)}$$

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

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

Definiere dazu eine Abbildung:

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

Dann gilt für die Lösungsmenge L:

$$L = \left\{ \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} \mid 2s_1 + s_2 = 3 \right\} = \varphi^{-1}(\{3\})$$

d.h. L ist eine Faser von φ.

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

Definiere:

$$\varphi_A : K^n \to K^m, \qquad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$$

mit $y_i := \sum_{j=1}^{n} a_{ij} x_j, \quad 1 \leq i \leq m.$
Dann ist $L := \varphi_A^{-1}(\{b\})$ die Lösungsmenge des LGS.

1.4.5 Der Gauß Algorithmus

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

Definition 1.4.6 *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 c-fache Zeile j zur Zeile i*
c)	$m_i(c)$	$(1 \leq i \leq m),\ c \neq 0)$:	*Multipliziere Zeile i mit c*

Beispiel

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

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 1 \\ -1 & -1 & 5 & 6 \end{pmatrix} \xrightarrow{t_{12}} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ -1 & -1 & 5 & 6 \end{pmatrix}$$

$$\xrightarrow{a_{23(2)}} \begin{pmatrix} 0 & 0 & 1 & 1 \\ -1 & 0 & 13 & 16 \\ -1 & -1 & 5 & 6 \end{pmatrix} \xrightarrow{m_3(-1)} \begin{pmatrix} 0 & 0 & 1 & 1 \\ -1 & 0 & 13 & 16 \\ 1 & 1 & -5 & -6 \end{pmatrix}$$

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 (vergl. Definition 1.4.5 b)) die gleichen Lösungsmengen.

Beweis: Folgt aus Bemerkung 1.4.1.

Definition 1.4.7 *Eine Matrix (über K) hat* ***Zeilenstufenform****, wenn sie die folgende Gestalt hat:*

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

Hierbei bestehen die ersten k Spalten und die letzten l Zeilen aus Nullen.
$\square$ bezeichnet einen Eintrag $\neq 0$.
$*$ bezeichnet einen beliebigen Eintrag.

Links und unterhalb von $\square$ stehen nur Nullen.

Bemerkung (Gauß Algorithmus mit Zeilentransformation)

Jede Matrix über K kann durch eine Folge elementarer Zeilentransformationen der in 1.4.6 a) und b) definierten Form in eine Matrix in Zeilenstufenform überführt werden.

Beweis

A habe m Zeilen ($m \in \mathbb{N}$).
Wir beweisen die Behauptung durch Induktion über m:

$\underline{m=1}$: klar, da A in Zeilenstufenform.
$\underline{m-1 \to m}$: Sei j_1 die Nummer der ersten Spalte von A, in der ein Eintrag $\neq 0$ vorkommt, sagen wir Zeile i_1. Durch Vertauschen von Zeilen (Zeile 1 und Zeile i_1) erhalten wir

$$\begin{pmatrix} 0\cdots 0 & \square & * & \cdots & * \\ 0\cdots 0 & * & * & \cdots & * \\ \vdots \quad \vdots & \vdots & \vdots & & \vdots \\ \underbrace{0\cdots 0}_{j-1} & \underbrace{*}_{j_1} & * & \cdots & * \end{pmatrix}$$

Durch „Ausräumen“ der Spalte j_1 mit elementaren Zeilentransformationen der Form $a_{i1}(c_i)$ mit geigneten $c_i \in K$ erhalten wir

$$\begin{pmatrix} 0\cdots 0 & \square & * & \cdots & * \\ 0\cdots 0 & 0 & * & \cdots & * \\ \vdots \quad \vdots & \vdots & & C & \\ \underbrace{0\cdots 0}_{j-1} & \underbrace{0}_{j_1} & & & \end{pmatrix}$$

C hat $(n-1)$ Zeilen.

Beispiel

$$A \in \mathbb{Q}^{4\times 5} = \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ -1 & 2 & -1 & -3 & -6 \\ 1 & -2 & 5 & 4 & 1 \\ 2 & -4 & 4 & 8 & 5 \end{pmatrix} \xrightarrow{a_{21}(1),\, a_{31}(-1),\, a_{41}(-2)} \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 2 & 0 & -1 \\ 0 & 0 & -2 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{a_{32}(-1),\, a_{42}(1)} \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 1 & -3 \end{pmatrix} \xrightarrow{a_{43}(1)} \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

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

Gegeben: $A \in K^{m\times n}$, interpretiert als Matrix eines homogenen LGS.

Gesucht: Lösungsmenge L

Der Algorithmus besteht aus zwei Schritten:

a) **Vorwärtselimination**: Bringe die Matrix mit dem Gauß-Algorithmus (siehe 1.4.5) auf Zeilenstufenform A', etwa

$$A' = \begin{pmatrix} 0 & \cdots & 0 & \square & * & * & * & * & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \square & * & * & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & 0 & \square & * & * & \cdots & * \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \square & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

wobei die ersten r Zeilen ein $\square$ enthalten, die restlichen $m - r \geq 0$ Zeilen nur Nullen.

b) **Rückwärtssubstitution**: Die r Unbekannten in den $\square$-Spalten nennen wir **abhängige Variablen**, die anderen $(m - r)$ heißen **freie Variablen**.

b1) Bringe die freien Variablen auf die rechte Seite des LGS und ersetze sie der Reihe nach durch $a_1, \cdots, a_{m-r} \in K$ (beliebige Zahlen).

b2) 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.)

Beispiel

(vergl. 1.4.5)

$$A' \in \mathbb{Q}^{4\times 5} = \begin{pmatrix} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ \underbrace{0}_{x_1} & \underbrace{0}_{x_2} & \underbrace{0}_{x_3} & \underbrace{0}_{x_4} & \underbrace{0}_{x_5} \end{pmatrix}$$

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

b1)

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

b2)

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

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

Bemerkung

a) Ein homogenes LGS hat immer eine Lösung, nämlich $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in K^m$. Diese Lösung heißt auch die **triviale Lösung**.

b) Hat ein homogenes LGS weniger Gleichungen als Unbekannte ($m < n$), dann hat es eine **nicht-triviale Lösung**.

Beweis

a) klar.

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

   Anzahl der Unbekannten $= n > m \geq$ Anzahl der abhängigen Variablen.
   $\Rightarrow$ es existiert mindestens eine freie Variable!

Beispiel aus der Chemie

Betrachten wir die chemische Reaktion

$$PbN_6 + CrMnO_8 \longrightarrow Pb_3O_4 + Cr_2O_3 + MnO_2 + NO$$

PbN_6	Bleiazid	x_1
$CrMnO_8$	Chrompermanganat	x_2
Pb_3O_4	Bleioxid	x_3
Cr_2O_3	Chromazid	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: $x_1 = 3x_3 \Leftrightarrow x_1 - 3x_3 = 0$)

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

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

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

Welche Lösungen sind chemisch sinnvoll? Alle $x_i \in \mathbb{N}$. Kleinste solche Lösung ist für $a = 90$:

$$\begin{pmatrix} 15 \\ 44 \\ 5 \\ 22 \\ 88 \\ 90 \end{pmatrix}, \text{ d.h.: } 15*PbN_6+44*CrMn_2O_8 \longrightarrow 5*Pb_3O_4+22*Cr_2O_3+88*MnO_2+90*NO$$

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 $b \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$) vorraussetzen.

Gesucht: Lösungsmenge L

Der Algorithmus besteht aus drei Schritten:

a) **Vorwärtselimination**: Bringe (A, b) mit dem Gauß-Algorithmus (siehe 1.4.5) auf die Form (A', b'), wobei A' Zeilenstufenform hat, etwa

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

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

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

c) **Rückwärtssubstitution**: Nur, falls $b'_{r+1} = b'_{r+2} = \cdots = b'_m = 0$.
Abhängige und freie Variablen werden wie im homogenen Fall definiert.

c1) Ersetze alle freien Variablen durch 0 und löse nach den abhängigen Variablen auf (von unten nach oben).

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

c2) Bestimme die Lösungsmenge L_0 des homogenen LGS mit Matrix A'. Dann gilt $L = \{s + u |\ u \in L_0\} \subseteq K^n$. Dabei haben wir zur Abkürzung gesetzt:

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

Beispiel

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

$(A, b) \in \mathbb{Q}^{4\times 5}$ ist die Matrix aus Beispiel 1.4.5.

$$\longrightarrow \left(\begin{array}{cccc|c} 1 & -2 & 3 & 4 & 2 \\ 0 & 0 & 2 & 1 & -4 \\ 0 & 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$\Rightarrow$ Das LGS ist lösbar!

Freie Variablen: x_2
Abhängige Variablen: x_1, x_3, x_4

Spezielle Lösung: $x_2 = 0$

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

$\begin{pmatrix} \frac{31}{2} \\ 0 \\ -\frac{1}{2} \\ -3 \end{pmatrix}$ ist eine spezielle Lösung

Lösungsmenge des homogenen LGS:
Ersetze x_2 durch $a \in \mathbb{Q}$

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

$$L_0 = \left\{ \begin{pmatrix} 2a \\ a \\ 0 \\ 0 \end{pmatrix} \mid a \in \mathbb{Q} \right\}$$

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

Einige Fragen:

1. Inwieweit sind die freien bzw. abhängigen Variablen durch ein LGS bestimmt?

   (a) Zeilenstufenform, auf die $A \in K^{m\times n}$ transformiert werden kann, ist nicht eindeutig durch A bestimmt.

   (b) Vertauschen von Unbekannten liefert ein äquivalentes LGS, aber eine andere Menge von Variablen:

   Beispiel:

$$\begin{array}{rcrcrcl} -2x_1 & + & \frac{17}{3}x_2 & + & x_3 & = & 0 \\ \frac{2}{3}x_1 & + & \frac{28}{9}x_2 & - & \frac{1}{3}x_3 & = & 0 \end{array}$$

$$A = \begin{pmatrix} -2 & \frac{17}{3} & 1 \\ \frac{2}{3} & \frac{28}{9} & -\frac{1}{3} \end{pmatrix}$$

   Hierbei steht die erste Spalte für die Koeffizienten von x_1, die zweite für die von x_2 und die dritte für die von x_3.

$$\longrightarrow \begin{pmatrix} -2 & \frac{17}{3} & 1 \\ 0 & 5 & 0 \end{pmatrix}$$

   Somit ist die Variable x_3 frei.

$$\begin{array}{rcrcrcl} x_3 & - & 2x_1 & + & \frac{17}{3}x_2 & = & 0 \\ -\frac{1}{3}x_3 & - & \frac{2}{3}x_3 & + & \frac{28}{9}x_2 & & 0 \end{array}$$

$$A = \begin{pmatrix} 1 & -2 & \frac{17}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{28}{9} \end{pmatrix}$$

   Hierbei steht also die erste Spalte für die Koeffizienten von x_3, die zweite für die von x_1 und die dritte für die von x_2.

$$\longrightarrow \begin{pmatrix} 1 & 2 & \frac{17}{3} \\ 0 & 0 & 5 \end{pmatrix}$$

   Somit ist hier aber x_1 die freie Variable.

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

3. Lösungskriterium (für inhomogene LGS)? Kriterium für <u>eindeutige</u> Lösbarkeit?

4. Kurze, kompakte Beschreibung der Lösungsmenge?
   $L = s + L_0 := \{s + u \mid u \in L_0\}$,
   L_0 Lösungsmenge des zugehörigen homogenen LGS (vergl. 1.4.5)
   $L_0 : u, v \in L_0 \Rightarrow u + v \in L_0$

1.5 Äquivalenzrelationen

M : Menge

Definition 1.5.1 *a) Eine Relation 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 $(x, x) \in R \; \forall x \in M$*
- *(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***

1.5.1 Beispiele

(A) Aus der Mathematik

1. $M = \mathbb{N}$, $\quad R = „<“$
   $(x < y :\Leftrightarrow y - x \in \mathbb{N})$
   $<$ nicht reflexiv, nicht symmetrisch
   $<$ transitiv
2. $M = \mathbb{N}$, $\quad R = „\leq“$
   $(x \leq y :\Leftrightarrow x < y$ oder $x = y)$
   $\leq$ ist (R), (A), (T)
3. $M = Pot(N)$ für eine Menge N
   $R = „\subseteq“$ ist (R), (A), (T) (aber „$\subseteq$“ ist keine Totalordnung, d.h. nicht alle Elemente aus M sind vergleichbar bzgl. „$\subseteq$“, z.B.
   $\{1\}, \{2\} \in Pot(\{1, 2\}$, aber $\{1\} \not\subseteq \{2\}$ und $\{2\} \not\subseteq \{1\})$
4. Sei N Menge: $f : M \to N$
   R_f definiert durch $xR_fx' :\Leftrightarrow f(x) = f(x')$ ist Äquivalenzrelation.
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. Menge der hier Anwesenden:
   $xEy :\Leftrightarrow x$ hat die gleichen Eltern (das gleiche Elternpaar) wie y.
   $xGy :\Leftrightarrow x$ hat den gleichen Geburtstag (Tag und Monat) wie y.
2. M = Menge der Stichwörter $xAy :\Leftrightarrow x$ 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 und F sind Äquivalenzrelationen. Eine Äquivalenzrelation fasst Elemente von M unter einem „Gesichtspunkt“ zusammen.

Definition 1.5.2 *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.
$M/R \subseteq Pot(M)$

1.5.2 Beispiele (vergl. 1.5.1)

a) R_f wie in 1.5.1(A)(4), $f : M \to N$
   $xR_fx' \Leftrightarrow f(x') = f(x)$
   $x \in M : C_x = \{x' \in M \mid f(x) = f(x')\} = f^{-1}(f(x))$
   M/R_f : Menge der nichtleeren Fasern von f.

b) $R =$ „ $=$ “, $\quad x \in M$
   $C_x = \{x\}$
   $M/R = \{\, \{x\} \mid x \in M\}$

c) $M = \mathbb{Z}$, $\quad R =$ „ $\equiv_3$ „
   $x \equiv_3 y :\Leftrightarrow 3 \mid x - y$
   $C_0 = \{y \in \mathbb{Z} \mid 3|y\}$
   $C_1 = \{y \in \mathbb{Z} \mid 3|y-1\} = \{y \in \mathbb{Z} \mid y = 3x + 1 \text{ für ein } x \in \mathbb{Z}\}$
   $C_2 = \{y \in \mathbb{Z} \mid y = 3x + 2 \text{ für ein } x \in \mathbb{Z}\}$
   Das sind alle Äquivalenzklassen bzgl. $\equiv_3$.

d) M: Menge der Anwesenden
   $R = E$ (gleiches Elternpaar)
   Äquivalenzklasse: Geschwisterklasse
   $R = G$ (gleiches Geburtsdatum)
   $C_{\text{Hiß}} = \{a \mid a \text{ hat am 27.07. Geburtstag}\}$

e) M: Stichwörter in einem Lexikon
$R = A$ (gleicher Anfangsbuchstabe)
Äquivalenzklasse: $C_x = \{$Wörter, die mit einem x oder X anfangen$\}$

f) M: farbige Perlen
Äquivalenzklasse besteht aus einer Menge von Perlen gleicher Farbe.

Definition 1.5.3 *Eine* ***Partition*** *von M ist eine Menge P von nicht leeren Teilmengen von M, die Teile von P sind, mit:*

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

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

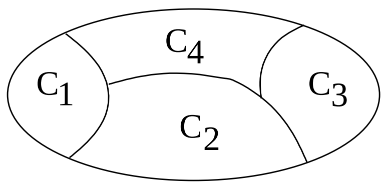

Abbildung 1.13: Partition $P = \{C_1, C_2, C_3, C_4\}$

1.5.3 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), 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: $C_x = C_y$.

Sei $z \in C_x \cap C_y$:
$\Rightarrow xRz$ und yRz
$\Rightarrow xRz$ und zRy wegen (S)
$\Rightarrow xRy$ wegen (T)

Seien nun $u \in C_y$ beliebig:
$\Rightarrow xRy$ und yRu wegen (S)
$\Rightarrow xRu$ wegen (T)
$\Rightarrow u \in C_x$

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 1.5.3(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 $(y,z) \in R$.
$\Rightarrow$ es existiert $C_1, C_2 \in P$ mit ($x \in C_1$ und $y \in C_1$) und ($y \in C_2$ und $z \in C_2$)
$y \in C_1 \cap C_2 \overset{1.5.3(a)}{\Longrightarrow} C_1 = C_2 \Rightarrow (x,z) \in R$

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 $C = C_x$.
Dies ist aber klar.

1.5.4 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.

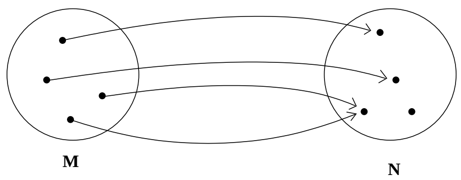

Abbildung 1.14: M/R_f

b) M Menge der Anwesenden.
Die Partition zur Äquivalenzrelation G aus 1.5.1(B)(1) ergibt sich aus der (nicht surjektiven und nicht injektiven) Abbildung:

$$M \to \underbrace{\underline{31}}_{1...31} \times \underbrace{\underline{12}}_{1...12}$$

$$x \mapsto \text{ Geburtsdatum von } x$$

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

c) M: Menge von farbigen Perlen.
Die Partition zur Äquivalenzrelation F aus 1.5.1(B)(3) ergibt sich aus der Abbildung:

$$M \to \{Farben\}$$

$$x \mapsto Farbe(x)$$

Teile der Partition: Menge von Perlen gleicher Farbe.

Definition 1.5.4 (und Bemerkung) *Sei R eine Äquivalenzrelation auf M.*

$$\pi : M \to M/R$$

$$x \mapsto C_x$$

heißt die zu R gehörige ***kanonische (natürliche) Abbildung****.*
π ist surjektiv und ihre Fasern sind gerade die Äquivalenzklassen von R.

1.5.5 Bemerkung

Sei N Menge und $f : M \to N$ eine Abbildung.
R_f sei die Äquivalenzrelation aus Beispiel 1.5.1(A)(4) und $\pi : M \to M/R_f$ die zugehörige kanonische Abbildung (vergl. Def. 1.5.4). Dann existiert eine injektive Abbildung:

$$\bar{f} : M/R_f \to N$$

$$f = \bar{f} \circ \pi$$

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

Beweis

Definiere $\bar{f} : M/R_f \to N$ 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: $f = \bar{f} \circ \pi$.
Sei $x \in M$: $\pi(x) = C_x = f^{-1}(\{f(x)\}) \Rightarrow \bar{f} \circ \pi(x) = \bar{f}(\pi(x)) = f(x)$
d.h. $f(x) = \bar{f} \circ \pi(x)\ \forall x \in M$ und damit ist $f = \bar{f} \circ \pi$

$\bar{f}$ ist injektiv:

Seien C_x, $C_{x'} \in M/R_f$ mit $\bar{f}(C_x) = \bar{f}(C_{x'})$

$$\Rightarrow f(x) = f(x'), \text{ da } C_x = \pi(x),\, C'_x = \pi(x')$$
$$\Rightarrow C_x = f^{-1}(\{f(y)\}) = f^{-1}(\{f(x')\}) = C_x$$

1.5.6 Beispiel

M: farbige Perlen
N: Menge von Farben
$f : M \to N, \qquad x \mapsto Farbe(x)$

Nicht-leere Fasern von f (Äquivalenzklasse von R_f): Menge von Perlen gleicher Farbe (Häufchen).
π: Jede Perle wird ihr Farbhäufchen zugeordnet.
$\bar{f}$: Jedem Häufchen wird „seine“ Farbe zugeordnet.

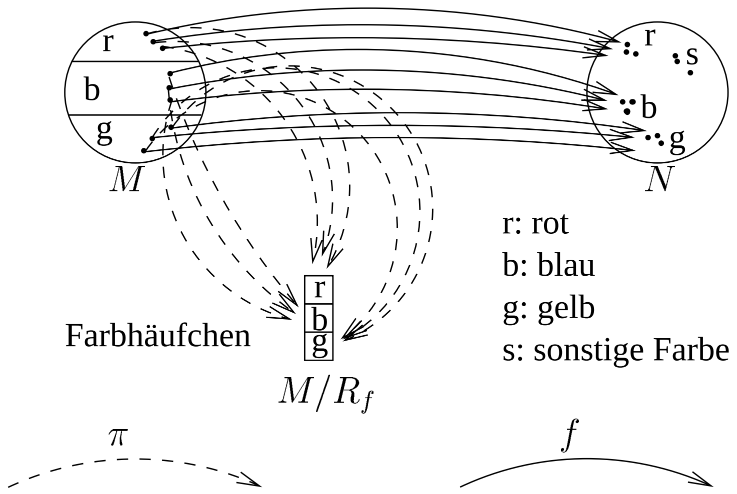

Abbildung 1.15: Beispiel

Kapitel 2

Vektorräume und lineare Abbildungen

2.1 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 (wird/werden).

Definition 2.1.1 *Eine Menge G heißt* ***Gruppe****, wenn eine Verknüpfung $*$*

$$G \times G \to G \qquad (x, y) \mapsto x * y$$

definiert ist, so dass gilt:

1. $(x * y) * z = x * (y * z) \quad \forall x, y, z \in G$

2. *Es existiert $e \in G$ mit $e * x = x * e = x \quad \forall x \in G$*

3. *$\forall x \in G$ existiert $x' \in G$ mit $x * x' = e = x' * x$*

Gilt zusätzlich

4. $x * y = y * x \quad \forall x, y \in G,$

dann heißt G ***abelsch*** *(kommutativ).*

2.1.1 Bemerkung

Sei $(G, *)$ eine Gruppe.

a) Das Element e aus 2.1.1(2) heißt das neutrale Element von G (es ist eindeutig definiert).

b) Sei $x \in G$. Das Element x' aus 2.1.1(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'.

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

2.1.2 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:
$S_M := \{f : M \to M \mid f \text{ ist bijektiv}\}$
S_M ist Gruppe mit der Verknüpfung „$\circ$“:

Klar:
$$f \circ g \in S_M \qquad \forall f, g \in S_M$$
Klar:
$$(f \circ g) \circ h = f \circ (g \circ h) \qquad \forall f, g, h \in S_M$$
id_M ist das neutrale Element bzgl. $\circ$.
Für $f \in S_M$ ist $f^{-1} \in S_M$ (hier ist f^{-1} die Umkehrabbildung aus 1.3.1).

d) Spezialfall von c):
Sei $M := \underline{n} = \{1, ..., n\} \subseteq \mathbb{N} \quad (n \in \mathbb{N})$
$S_n := S_{\underline{n}}$ heißt die symmetrische Gruppe auf n Ziffern.

Eine Element aus S_n heißt **Permutation**.
Für $\pi \in S_n$ schreiben wir oft:
$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}$$
Es gilt: $|S_n| = n! = 1 \cdot 2 \cdot 3 \cdot \ ... \ \cdot n$
Weiter gilt S_n abelsch $\Leftrightarrow n \leq 2$:

„$\Leftarrow$“:
$$n \leq 2 \Rightarrow |S_n| \in \{1, 2\} \Rightarrow S_n \text{ abelsch}$$

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

$$I_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$$

$$I_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$$

$$I_1 \circ I_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}$$

$$I_2 \circ I_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 1 & 2 & 4 & \cdots & n \end{pmatrix}$$

$$\Rightarrow I_1 \circ I_2 \neq I_2 \circ I_1$$

Definition 2.1.2 *Seien G, H Gruppen. Eine Abbildung $\varphi : G \to H$ heißt* ***(Gruppen-) Homomorphismus****, wenn gilt:*

$$\varphi \underbrace{(xy)}_{\text{Verkn. in } G} = \underbrace{\varphi(x)\varphi(y)}_{\text{Verkn. in } H} \qquad \forall x, y \in G$$

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 $f : G \to H$ existiert. Schreibweise: $G \cong H$.*

2.1.3 Beispiele

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

b) $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), \quad x \mapsto exp(x) = e^x$
ist ein Isomorphismus. (exp ist bijektiv und $e^{x+y} = e^x \cdot e^y \; \forall x, y \in \mathbb{R}$)

Definition 2.1.3 *Sei $(G, \cdot)$ eine Gruppe, U heißt* ***Untergruppe*** *von G, geschrieben $U \leq G$, falls U bzgl. der Verknüpfung $\cdot$ von G selbst eine Gruppe ist. (präziser: falls gilt $u \cdot v \in U \; \forall u, v \in U$. Damit erhalten wir eine Verknüpfung auf U*

$$\cdot : U \times U \to U, \quad (u, v) \mapsto \underbrace{u \cdot v}_{\text{Verkn. in } G}$$

U soll bzgl. dieser Verknüpfung eine Gruppe sein.)

2.1.4 Beispiele

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

b) Sei $n \in N$, $G = S_n = \{\pi \mid \underline{n} \to \underline{n},\ \pi \ \mathit{bijektiv}\}$.

$$U = \{\pi \in G \mid \pi(n) = n\} \leq G$$

Es existiert ein Isomorphismus $S_{n-1} \to U$, d.h. $S_{n-1} \cong U$ (falls $n \geq 2$).

2.1.5 Konventionen

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

2.1.6 Beispiele

Sei $n \in N$

a) Division durch n mit Rest: Zu $x \in \mathbb{Z}$ existiert ein eindeutig bestimmtes $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit $0 \leq r \leq n - 1$ und $x = q \cdot n + r$.
<u>Schreibweise</u>: $x \bmod n := r$ (der nicht negative Rest von x bei Division durch n)
[z.B. $n = 7$ $\quad 21 \bmod 7 = 0$
$-3 \bmod 7 = 4$
$17 \bmod 7 = 3$]

b) **Definition 2.1.4** *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. $n = 7$ $\quad -3 \equiv 32 \pmod 7$
$-6 \equiv 1 \pmod 7$ *]*

c) Bemerkung (vergl. 1.5.1(A)(6)): Für $x, y \in \mathbb{Z}$ gilt:

$$x \equiv y \pmod n \Leftrightarrow n \mid x - y$$

d) Bemerkung (vergl. 1.5.2(c)): Sei $x \in \mathbb{Z}$ und C_x die Äquivalenzklasse von x bzgl. $\equiv \pmod n$. Dann gilt $C_x = x + n\mathbb{Z}$ (Konvention 2.1.5).

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

$$\begin{array}{lll} y \in C_x & \Leftrightarrow \ x \equiv y \pmod n & \text{b) und 1.5.2} \\ & \Leftrightarrow \ n \mid x - y & \text{c)} \\ & \Leftrightarrow \ \text{es existiert } q \in \mathbb{Z} \text{ mit } x - y = qn & \\ & \Leftrightarrow \ \text{es existiert } z \in \mathbb{Z} \text{ mit } y = x + nz & \\ & \Leftrightarrow \ y \in x + n\mathbb{Z} & \text{Konventionen 2.1.5} \end{array}$$

e) Bemerkung:

1. Sei $x \in \mathbb{Z}$ und $r = x \bmod n$. Dann ist $x + n\mathbb{Z} = r + n\mathbb{Z}$
2. $\{n\mathbb{Z}, 1+n\mathbb{Z}, ..., (n-1)+n\mathbb{Z}\}$ ist die Menge der Äquivalenzklassen bzgl. $\equiv \pmod n$
   Sind $r, r' \in \{0, ..., n-1\}$, $r \neq r'$, dann ist $r + n\mathbb{Z} \neq r' + n\mathbb{Z}$.

Beweis

1. Nach Definition von r gilt:
   $$n \mid x - r \Rightarrow x \equiv r \pmod n \overset{d)}{\Rightarrow} x + n\mathbb{Z} = r + n\mathbb{Z}$$
2. Wäre $r + n\mathbb{Z} = r' + n\mathbb{Z}$, dann wäre $r \equiv r' \pmod n$, also $n \mid r - r'$. Wegen $0 \leq r,\ r' \leq n - 1$ wäre dann $r = r'$.

f) Schreibweise: $\overline{x} := x + n\mathbb{Z}$ für $x \in \mathbb{Z}$
$\mathbb{Z}/_{n\mathbb{Z}} := \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ = Menge der Äquivalenzklassen bzgl. $\equiv \pmod n$.
Diese Äquivalenzklassen heißen auch **Restklassen** $\pmod n$.

g) Beispiele:

$n = 2$:	$\overline{0} = 2\mathbb{Z}$	Menge der geraden ganzen Zahlen.
	$\overline{1} = 1 + 2\mathbb{Z}$	Menge der ungeraden ganzen Zahlen.
$n = 7$:	$\overline{0}$	7er Reihe
	$\overline{1}$	Menge derjenigen ganzen Zahlen, die bei Division durch 7 den Rest 1 haben.

$\mathbb{Z}/_{7\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{6}\}$

h) Bemerkung: Für $x, y \in \mathbb{Z}$ gilt:

$$(x + n\mathbb{Z}) \underbrace{+}_{2.1.5} (y + n\mathbb{Z}) = (x + y) + n\mathbb{Z}$$

Beispiel: $\overline{0} + \overline{1} = \overline{0 + 1} = \overline{1}$

Beweis:

„ $\subseteq$ “ $\quad (x+nz_1)+(y+nz_2) = (x+y)+n(z_1+z_2) \in (x+y)+n\mathbb{Z} \quad z_1, z_2 \in \mathbb{Z}$

„ $\supseteq$ “ $\quad (x+y)+nz = (x+0\cdot z)+(y+nz) \in (x+n\mathbb{Z})+(y+n\mathbb{Z})$

Mit obiger Schreibweise (d.h. $\overline{x} = x + n\mathbb{Z}$) gilt also: $\overline{x}+\overline{y} = \overline{x+y}$.

i) Bemerkung: $\mathbb{Z}/_{n\mathbb{Z}}$ ist mit der Verknüpfung + aus 2.1.5 abelsche Gruppe mit genau n Elementen. Die Abbildung

$$\overline{}: \mathbb{Z} \to \mathbb{Z}/_{n\mathbb{Z}}, \qquad x \mapsto \overline{x}$$

ist ein surjektiver Gruppenhomomorphismus.

Beweis: Nach Teil h) gilt $\overline{x}+\overline{y} = \overline{x+y}$ für $\overline{x},\overline{y} \in \mathbb{Z}/_{n\mathbb{Z}}$ (d.h. + ist Verknüpfung auf $\mathbb{Z}/_{n\mathbb{Z}}$).

Die Gruppeneingenschaften werden mit Hilfe von h) aus denjenigen für $\mathbb{Z}$ gefolgert:

z.B. A6:

$(\overline{x}+\overline{y})+\overline{z} = \overline{(x+y)}+\overline{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \overline{x}+\overline{(y+z)} = \overline{x}+(\overline{y}+\overline{z})$

$\overline{0}$ ist das neutrale Element.

$\overline{(-x)}$ ist das zu $\overline{x}$ inverse Element in $\mathbb{Z}/_{n\mathbb{Z}}$.

$\overline{}: \mathbb{Z} \to \mathbb{Z}/_{n\mathbb{Z}}$ ist Homomorphismus nach h) und surjektiv.

$(\mathbb{Z}/_{n\mathbb{Z}}, +)$ heißt die **Restklassengruppe modulo n**.

j) Rechnen in $\mathbb{Z}/_{n\mathbb{Z}}$, z.B. $n = 7$:

$$\overline{6}+\overline{5} = \overline{6+5} = \overline{11} = \overline{4} \text{ oder}$$

$$\overline{6}+\overline{5} = \overline{-1}+\overline{5} = \overline{-1+5} = \overline{4}$$

$$\overline{3}-\overline{5} = \overline{3}+(-\overline{5}) = \overline{3}+\overline{(-5)} = \overline{3-5} = \overline{-2} = \overline{5}$$

Definition 2.1.5 *Eine Menge R heißt* ***Ring****, wenn auf R zwei Verknüpfungen*

$$+ : R \times R \to R$$

$$\cdot : R \times R \to R$$

definiert sind, so dass gilt:

1. *$(R, +)$ ist abelsche Gruppe*
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall x, y, z \in R$

3. *Es existiert* $1 \in R$ *mit* $1 \cdot x = x \cdot 1 = x \quad \forall x \in R$

4. *Distributivgesetz:*
   $x \cdot (y + z) = x \cdot y + x \cdot z$ *und* $(x + y) \cdot z = x \cdot z + y \cdot z \quad \forall x, y, z \in R$

Gilt zusätzlich:

5. $x \cdot y = y \cdot x \quad \forall x, y \in R$

dann heißt R ***kommutativ***.

2.1.7 Beispiele

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

b) Körper sind kommutative Ringe.

Definition 2.1.6 *Sei R ein Ring:*

a) Ein Element $x \in R$ *heißt* ***invertierbar*** *oder auch* ***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* $x^{-1} := x'$.

b) Sei S ein Ring und $\varphi : R \to S$ *Abbildung.*
φ heißt ***Ringhomomorphismus***, *wenn gilt:*

1. φ *ist Gruppenhomomorphismus* $(R, +) \to (S, +)$
2. $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \quad \forall x, y \in R$ *und* $\varphi(1) = 1$

2.1.8 Bemerkungen und Beispiele

Sei R ein Ring:

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

b) Sei R kommutativ, dann gilt:

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

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

Beweis zu a): z.z. ist nur:

$$x_1, x_2 \in R^* \Rightarrow x_1 \cdot x_2 \in R^*$$

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

2.1.9 Beispiel (Forsetzung von 2.1.4)

Sei $n \in N$

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

[z.B. $n = 7, \quad x = 3, \quad x' = -4, \quad y = 1, \quad y' = 8$
$x \cdot y = 3 \qquad x' \cdot y' = -32 = 7 \cdot (-5) + 3$]

b) Definiere $\cdot : \mathbb{Z}/_{n\mathbb{Z}} \to \mathbb{Z}/_{n\mathbb{Z}}$ durch $\overline{x} \cdot \overline{y} := \overline{xy}$

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

Zusammen mit $+$ aus 2.1.4 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:

$$\overline{x} \in (\mathbb{Z}/_{n\mathbb{Z}})^* \Leftrightarrow \mathrm{ggT}(x, n) = 1 \quad (x \text{ und } n \text{ sind teilerfremd})$$

<u>Beweis:</u>

„$\Rightarrow$" Indirekter Beweis:
Angenommen, es existiert $d \neq 1,\ d \in \mathbb{N}$ mit $d|n$ und $d|x$.
$\Rightarrow$ Sei $n = d \cdot b$ für ein $b \in \mathbb{N}$
$\Rightarrow 0 < b < n$, d.h. $\overline{b} \neq \overline{0}$
Aus $n|xb$ 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 $\overline{x'} \cdot \overline{x} = \overline{1}$
$\Rightarrow \overline{0} = \overline{x'} \cdot \overline{0} = \overline{x'} \cdot \overline{x} \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}$

„$\Leftarrow$" Betrachte: $\qquad l_{\overline{x}} : \mathbb{Z}/_{n\mathbb{Z}} \to \mathbb{Z}/_{n\mathbb{Z}}, \qquad \overline{y} \mapsto \overline{x} \cdot \overline{y}$
<u>Zeige</u>: $l_{\overline{x}}$ ist injektiv.
<u>Dazu</u>: Seien $\overline{y_1}, \overline{y_2} \in \mathbb{Z}/_{n\mathbb{Z}}$ mit $\overline{x} \cdot \overline{y_1} = \overline{x} \cdot \overline{y_2}$
$\Rightarrow x(y_1 - y_2) \in n\mathbb{Z} \Rightarrow y_1 - y_2 \in n\mathbb{Z}$ (weil $ggT(x, n) = 1$) $\Rightarrow \overline{y_1} = \overline{y_2}$
$l_{\overline{x}}$ ist injektiv und $\mathbb{Z}/_{n\mathbb{Z}}$ ist endlich.
$\Rightarrow l_{\overline{x}}$ ist bijektiv und damit surjektiv.
$\Rightarrow$ Es existiert $\overline{y} \in \mathbb{Z}/_{n\mathbb{Z}}$ und $\overline{x} \cdot \overline{y} = \overline{1}$. $\Rightarrow \overline{y} \cdot \overline{x} = \overline{1}$, also ist $\overline{y} = (\overline{x})^{-1}$, d.h. $\overline{x} \in (\mathbb{Z}/_{n\mathbb{Z}})^*$

d) Wie rechnen wir in $\mathbb{Z}/_{n\mathbb{Z}} = \{\overline{1}, \overline{2}, ..., \overline{n-1}\}$?
$\overline{r} + \overline{s} = \overline{r + s} = \overline{(r + s) \pmod n}$
$\overline{r} \cdot \overline{s} = \overline{r \cdot s} = \overline{(r \cdot s) \pmod n}$
$n = 7$:

$$\overline{6} \cdot \overline{5} = \overline{30} = \overline{2} \text{ oder}$$
$$\overline{6} \cdot \overline{5} = \overline{(-1) \cdot 5} = \overline{-5} = \overline{2}$$
$$\overline{6}^{10000000} = \overline{(-1)}^{10000000} = \overline{1}^{5000000} = \overline{1}$$

2.1.10 Korollar

Sei $n \geq 2$:

$$\mathbb{Z}/_{n\mathbb{Z}} \text{ ist Körper } \Leftrightarrow n \text{ ist Primzahl}$$

Beweis:

$$\begin{aligned} \mathbb{Z}/_{n\mathbb{Z}} \text{ ist Körper } &\overset{2.1.8b)}{\Leftrightarrow} (\mathbb{Z}/_{n\mathbb{Z}})^* = \{\overline{1}, ..., \overline{n-1}\} \\ &\overset{2.1.9c)}{\Leftrightarrow} \operatorname{ggT}(j,n) = 1 \quad 1 \leq j \leq n-1 \\ &\Leftrightarrow \text{n ist Primzahl} \end{aligned}$$

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

2.1.11 Beispiel RSA-Kryptosystem

Public-Key-Kryptosystem, beteiligte Personen: Alice und Bob.

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

1. Einrichten des Kryptosystems
   - Bob wählt (kauft) Primzahlen p, q, $p \neq q$ groß.
   - Bob setzt $n := pq$.
   - Bob wählt $a, b \in \mathbb{N}$ mit $1 \leq a, b \leq n-1$ mit $ab \bmod \varphi(n) = 1$
     [$\varphi(n) = |(\mathbb{Z}/_{n\mathbb{Z}})^*|$ = Anzahl der Zahlen j, $1 \leq j \leq n-1$ mit $ggT(j,n) = 1$ (Eulersche φ-Funktion)]
     Hier: $\varphi(n) = \varphi(p \cdot q) = (p-1)(q-1)$
     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 (z.B. auf seiner Homepage).
   - Bob behält b für sich.
2. Verschlüsseln
   - Verschlüsselt werden Zahlen aus $\{0, 1, ..., n-1\}$

     $$l_{n,a} : \{0, 1, ..., n-1\} \to \{0, 1, ..., n-1\}$$

     $$x \mapsto x^a \bmod n$$

     (Beachte: $\overline{x^a \bmod n} = \overline{x^a} = \overline{x}^a$ in $\mathbb{Z}/_{n\mathbb{Z}}$.)

3. Entschlüsseln

   - $$d_{n,b} : l_{n,a} : \{0,1,...,n-1\} \to \{0,1,...,n-1\}$$
     $$y \mapsto y^b \bmod n$$

     Es gilt: $d_{n,b}(e_{n,a}(x)) = x$, (wegen $(x^a \bmod n)^b \bmod n = x$ (hier ohne Beweis)).

Beispiel

$p = 3$ und $q = 11$ (realitätsfern, in Anwendungen p und q ca. 100-stellig)

$$n = p \cdot q = 33 \qquad \varphi(n) = (p-1)(q-1) = 20$$

$$a = 3 \qquad b = 7 \qquad ab = 21, \qquad 21 \bmod 20 = 1$$

Klartext: 13
Geheimtext:

$$x^a \bmod 33 = 13^3 \bmod 33$$
$$13^2 = 159 \equiv 4 \pmod{33}$$
$$13^3 \equiv 13^2 \cdot 13 \equiv 4 \cdot 13 \equiv 52 \equiv 19 \pmod{33}$$
$$\Rightarrow 13^3 \bmod 33 = 19$$

$$19^7 \bmod 33 :$$
$$19 \equiv -14 \pmod{33}$$
$$14^2 = 196 \equiv (-2) \pmod{33}$$
$$\Rightarrow 19^7 \equiv (-14)(-2)^3 \equiv 14 \cdot 8 \equiv 112 \equiv 13 \pmod{33}$$

$$19^7 = 893871739$$

2.1.12 Matrizen

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

Definition 2.1.7 (Matrix-Arithmetik) *Sei R kommutativer Ring:*

a) Für $A = (a_{ij}) \in R^{m\times n}$ heißt

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

die ***Transponierte von** A.*

b) Für $A = (a_{ij}) \in R^{m\times n}$ und $r \in R$ sei

$$r \cdot A := (ra_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \in R^{m\times n}$$

die ***skalare Multiplikation von** A.*

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:

$$c_{ij} := \sum_{k=1}^{m} a_{ik}b_{kj}, \quad 1 \le i \le l,\ 1 \le j \le n$$

$c =: A\cdot B =: AB$ heißt das ***Produkt von** A **und** B. [AB ist nur definiert, falls die Anzahl von Spalten von A gleich der Anzahl der Zeilen von B ist.]*

2.1.13 Beispiele

a)

$$
\begin{aligned}
A &= \begin{pmatrix} 0 & 1 & -2 & 3 \\ \frac{5}{4} & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 \end{pmatrix} \in \mathbb{Q}^{3\times 4} \\
B &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \end{pmatrix} \in \mathbb{Q}^{3\times 4} \\
A^t &= \begin{pmatrix} 0 & \frac{5}{4} & 1 \\ 1 & 1 & 2 \\ -2 & 0 & 3 \\ 3 & 0 & 4 \end{pmatrix} \\
4A &= \begin{pmatrix} 0 & 4 & -8 & 12 \\ 5 & 4 & 0 & 0 \\ 4 & 8 & 12 & 16 \end{pmatrix} \\
0A &= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\
A+B &= \begin{pmatrix} 0 & 2 & 0 & 6 \\ \frac{21}{4} & 6 & 6 & 7 \\ 9 & 11 & 13 & 15 \end{pmatrix}
\end{aligned}
$$

b)

$$
\begin{aligned}
A &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \in \mathbb{Q}^{3\times 4} \\
B &= \begin{pmatrix} 1 & 4 \\ 2 & 3 \\ 3 & 2 \\ 4 & 1 \end{pmatrix} \in \mathbb{Q}^{4\times 2} \\
A \cdot B &= \begin{pmatrix} 20 & 10 \\ 3 & -3 \\ 3 & 7 \end{pmatrix} \in \mathbb{Q}^{3\times 2} \qquad (BA \text{ ist } \underline{\text{nicht}} \text{ definiert!})
\end{aligned}
$$

$[(l \times m)$-Matrix$] \cdot [(m \times 1)$-Matrix$] \to [(l \times 1)$-Matrix$]$

$$B' = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \qquad \text{1. Spalte von } B$$

$$\Rightarrow A \cdot B' = \begin{pmatrix} 20 \\ 3 \\ 3 \end{pmatrix} \qquad \text{1. Spalte von } A \cdot B$$

$[(1 \times m)$-Matrix$] \cdot [(m \times n)$-Matrix$] \to [(1 \times n)$-Matrix$]$

$$A' = \begin{pmatrix} -1 & 0 & 0 & 1 \end{pmatrix} \qquad \text{2. Zeile von } A$$

$$\Rightarrow A' \cdot B = \begin{pmatrix} 3 & -3 \end{pmatrix} \qquad \text{2. Zeile von } A \cdot B$$

c) $[(1 \times m)$-Matrix$] \cdot [(m \times 1)$-Matrix$] \to [(1 \times 1)$-Matrix$]$

$$(a_{11}, ..., a_{1m}) \cdot \begin{pmatrix} b_{11} \\ \vdots \\ b_{m1} \end{pmatrix} = \left(\sum_{k=1}^{m} a_{1k} b_{k1} \right) \in K^{1 \times 1} \quad \text{„Skalarprodukt“}$$

d) Sei $A = \begin{pmatrix} z_1 \\ \vdots \\ z_l \end{pmatrix}$ mit $z_i \in \mathbb{R}^{1 \times m}$, d.h. $A \in \mathbb{R}^{l \times m}$.

$B = (s_1, ..., s_n)$ mit $s_i \in R^m = R^{m \times 1}$, d.h. $B \in R^{m \times n}$, dann ist
$A \cdot B = (z_i \cdot s_j)_{\substack{1 \le i \le l \\ 1 \le j \le n}}$

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

$$A \cdot x = \begin{pmatrix} \sum\limits_{j=1}^{n} a_{1j} x_j \\ \vdots \\ \sum\limits_{j=1}^{n} a_{mj} x_j \end{pmatrix}$$

Deshalb schreiben wir ab jetzt ein LGS über einen Körper K mit Matrix $A = (a_{ij}) \in K^{m \times n}$ und rechter Seite $b = \begin{pmatrix} b_1 \\ \cdots \\ b_n \end{pmatrix} \in K^m$ formal als Matrixgleichung

$$A \cdot x = b$$

mit der Spalte $x := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ der Unbekannten $s \in K^n$ mit $A \cdot s = b$.

Definition 2.1.8 *Sei R ein kommutativer Ring*

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

b) *Für* $n \in \mathbb{N}$ *sei* $E_n = (\delta_{ij})_{1\leq i,j\leq n} \in R^{n\times n}$*mit*

$$\delta_{i,j} := \begin{cases} 1, \textit{ falls } i = j \\ 0, \textit{ sonst} \end{cases}$$

E_n *heißt die n-reihige* ***Einheitsmatrix***.

2.1.14 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. $0 + A = A = A + 0 \qquad (0 \in R^{m\times n})$
3. $A + (-1)A = 0 = (-1)A + A$
4. $A + B = B + A$

b)
1. $(A \cdot B) \cdot C = A \cdot (B \cdot C) \quad \forall A \in R^{l\times m},\ B \in R^{m\times n},\ C \in R^{n\times p}$
2. $E_m A = A = A E_n \quad \forall A \in R^{m\times n}$
3. $(A + B)C = AC + BC \quad \forall A, B \in R^{l\times m},\ C \in R^{m\times n}$ und
   $A(B + C) = AB + AC \quad \forall A \in R^{l\times m},\ B, C \in R^{m\times n}$
4. $r(sA) = (rs)A \quad \forall r, s \in R,\ A \in R^{m\times n}$ und
   $r(AB) = (rA)B = A(rB) \quad \forall r \in R,\ A \in R^{l\times m},\ B \in R^{m\times n}$

c)
1. $(A^t)^t = A \quad \forall A \in R^{m\times n}$
2. $(A + B)^t = A^t + B^t \quad \forall A, B \in R^{m\times n}$
3. $(AB)^t = B^t \cdot A^t \quad \forall A \in R^{l\times m},\ B \in R^{m\times n}$

Beweis

a) Klar.

b) 1. Beweis später.

2. Die i-te Zeile von E_m ist

$$z_i = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \in R^{1\times m}$$

Ist $A = (a_{ij})$, dann ist die j-te Spalte von A:

$$s_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

Offensichtlich gilt:

$$z_i \cdot s_j = (a_{ij}) \in R^{1\times 1} \Rightarrow E_m \cdot A = A$$

Analog: $A \cdot E_m = A$

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

$$\begin{aligned} & \sum_{k=1}^{m} (a_{ik} + b_{ik})c_{kj} \\ = & \sum_{k=1}^{m} (a_{ik}c_{kj} + b_{ik}c_{kj}) \\ = & \sum_{k=1}^{m} (a_{ik}c_{kj}) + \sum_{k_1}^{m} (b_{ik}c_{kj}) \end{aligned}$$

Einträge an Position (i,j) von $A \cdot C+$
Einträge an Position (i,j) von $B \cdot C =$
Einträge an Position (i,j) von $A \cdot C + B \cdot C$

2. Aussage analog.

4. Selbst überlegen.

c) 1. Klar.

2. Klar.

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

$$\Rightarrow A^t = (a'_{ij}) \text{ mit } a'_{ij} = a_{ji}$$

$$\text{und } B^t = (b'_{ij}) \text{ mit } b'_{ij} = b_{ji}$$

$$\text{Eintrag an Position } (i, j) \text{ von } (A \cdot B)^t =$$

$$\text{Eintrag an Position } (j, i) \text{ von } A \cdot B =$$

$$\sum_{k=1}^{m} a_{jk} b_{ki} \underbrace{=}_{R \text{ kommutativ}} \sum_{k=1}^{m} b_{ki} a_{jk} = \sum_{k=1}^{m} b'_{ik} a'_{kj} =$$

$$\text{Eintrag an Position } (i, j) \text{ von } B^t \cdot A^t.$$

2.1.15 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. $\cdot$).

Definition 2.1.9 *Sei R kommutativer Ring, $n \in \mathbb{N}$.*

$$GL_n(R) := \{A \in R^{n \times n} \mid A \text{ invertierbar } \} = (R^{n \times n})^* \qquad \textit{(vergl. 2.1.6)}$$

$GL_n(R)$ ist Gruppe, die ***volle lineare Gruppe über R****.*

2.1.16 Bemerkung

Sei R kommutativer Ring, $n \in \mathbb{N}$, dann gilt:

$$A \in GL_n(R) \Rightarrow A^t \in GL_n(R) \text{ und } (A^t)^{-1} = (A^{-1})^t$$

Beweis

$$A^t \cdot (A^{-1})^t = (A^{-1} \cdot A)^t = (E_n)^t = E_n$$

und

$$(A^{-1})^t \cdot A^t = (A \cdot A^{-1})^t = (E_n)^t = E_n$$

$$\Rightarrow \text{Behauptung}$$

2.2 Vektorräume

Definition 2.2.1 *Sei K ein Körper. Ein* ***(K-) Vektorraum*** *(**Vektorraum über K**) ist eine abelsche Gruppe $(V,+)$ zusammen mit einer* ***skalaren Multiplikation***

$$K \times V \to V, \qquad (a,v) \mapsto av$$

so dass gilt:

(V1) $(a+b)v = av + bv \qquad \forall a,b \in K,\ v \in V$

(V2) $a(v+v') = av + av' \qquad \forall a \in K,\ v,v' \in V$

(V3) $a(bv) = (ab)v \qquad \forall a,b \in K,\ v \in V$

(V4) $1v = v \qquad \forall v \in V$

Die Elemente eines K-VR heißen ***Vektoren****.*

2.2.1 Bemerkung

Sei V ein K-Vektorraum, dann gilt:

a) $\underbrace{0}_{0\in(K,+)} \cdot v = \underbrace{0}_{0\in(V,+)\ (\textbf{Nullvektor})} \qquad \forall v \in V$

b) $a \cdot 0 = 0 \qquad \forall a \in K$

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

d) $(-a)v = -(av) \qquad \forall a \in K,\ v \in V$

e) Für $a \in K$ und $v \in V$ gilt:

$$av = 0 \Leftrightarrow a = 0 \vee v = 0$$

Beweis

Ähnlich wie die analoge Aussage für Körper.

2.2.2 Beispiele

a) $V = \{0\}$ ist ein K-VR, der triviale K-VR.

b) $(K,+)$ ist K-VR mit der skalaren Multiplikation

$$K \times K \to K, \qquad (a,b) \mapsto ab$$

c) (aus LA:) $K^{m\times n}$ ist K-VR (folgt aus 2.1.14).

d) (aus Analysis:) $\mathbb{R}^{\mathbb{R}} := \{f : \mathbb{R} \to \mathbb{R}\}$ ist $\mathbb{R}$-VR (mit der üblichen Summe $f+g$ und den skalarem 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

$$\left\{\psi : \mathbb{R}^4 \to \mathbb{C} \mid \int\limits_{\mathbb{R}^3} |\psi(\vec{x},t)|^2 \, d\vec{x} = 1\right\} \text{ ist } \mathbb{C}\text{-VR.}$$

$\mathbb{C}$:	Körper der komplexen Zahlen
$(\vec{x},t) \in \mathbb{R}^4$:	
$\vec{x} \in \mathbb{R}^3$:	Ortsvektor
t:	Zeitkoordinate
$\vert\vert$:	komplexer Absolutbetrag
$\mathbb{R}^4$:	4-dimensionales Raum-Zeit-Kontinuum ($\mathbb{R}$-VR)
$\psi(\vec{x},t)$:	Wellenfunktion eines Teilchens
$\vert\psi(\vec{x},t)\vert^2$:	Wahrscheinlichkeitsdichte
$\int\limits_Q \vert\psi(\vec{x},t)\vert^2 \, d\vec{x}$:	Wahrscheinlichkeit, Teilchen zur Zeit t im Quader $Q \in \mathbb{R}^3$

f) (aus Informatik:) Suchmaschine speichert Term-Dokumente-Matrizen:
Zeilen $\widehat{=}$ Terme = Suchbegriff
Spalten $\widehat{=}$ Dokumente
Eintrag in der Zeile zu T_i (Term Nr. i) und der Spalte D_j (Dokument Nr. j) = Häufigkeit, mit der T_i in D_j vorkommt.

Suchanfrage: Folge aus Termen:
$T_{i1}, ..., T_{in} \rightsquigarrow$ Suchvektor
Spalte $s \in R^m$ (m: Anzahl der zulässigen Terme) mit

$$s_j = \begin{cases} 1, & j \in \{i_1, ..., i_n\} \\ 0, & \text{sonst} \end{cases}$$

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

Definition 2.2.2 *Sei V ein K-VR, $W \subseteq V$. W heißt (K-)**Unterverktorraum** (UVR) von V, geschrieben $W \leq V$ falls gilt:*

1. *W ist Untergruppe von $(V,+)$*
2. *$aw \in W \qquad \forall a \in K,\ w \in W$*

2.2.3 Bemerkung

Sei V ein K-VR, $W \subseteq V$, dann gilt:

$$W \leq V \Leftrightarrow$$

(UV1) $W \neq \emptyset$

(UV2) $w + w' \in W \qquad \forall w, w' \in W$ (W ist abgeschlossen bzgl. $+$)

(UV3) $aw \in W \qquad \forall a \in K, w \in W$ (W ist abgeschlossen bzgl. der skalaren Multiplikation)

Beweis

„$\Rightarrow$" Klar.

„$\Leftarrow$" Zu zeigen: W ist Untergruppe von $(V, +)$.
Wegen (UV2) ist

$$+ : W \times W \to W \qquad (w, w') \mapsto w + w'$$

eine Verknüpfung auf W. Diese ist assoziativ.
Sei $w \in W$ (ex. nach (UV1))
$\Rightarrow -w = (-1)w \in W$ ((UV3) + 2.2.1)
$\Rightarrow 0 = -w + w \in W$ (UV2)
$\Rightarrow W$ ist Untergruppe von $(V, +)$.

2.2.4 Beispiele

a) Sei V ein K-VR $\Rightarrow \{0\} \leq V,\ V \leq V$

b) Sei $W := \{(a_1, ..., a_n) \in K^{1\times n} \mid \sum\limits_{i=1}^{n} a_i = 0\}$
$\Rightarrow W \leq K^{1\times n} \qquad$ (verwende 2.2.3)

c) $C^\infty(\mathbb{R}) \leq C(\mathbb{R}) \leq \mathbb{R}^\mathbb{R} \qquad$ (verwende 2.2.3)

d) $V = \mathbb{R}^2$
Geraden durch $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ sind UVR von V. Geraden, die nicht durch $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ gehen, sind keine UVR, weil $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ in jedem UVR liegt. Eine Gerade durch $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ hat die Gleichung $y = ax$ für ein $a \in \mathbb{R}$, ist also gleich

$$\{\begin{pmatrix} x \\ ax \end{pmatrix} \mid x \in \mathbb{R}\}$$

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

$$\Rightarrow W_1 + W_2 \leq V \quad (= \{w_1 + w_2 \mid w_i \in W_i\}) \qquad \text{(verwende 2.2.3)}$$

Definition 2.2.3 *Sei V ein K-VR.*

*a) Sei $(v_1, ..., v_n)$ ein n-Tupel von Vektoren aus V (d.h. $v_i \in V$, $1 \leq i \leq n$). Eine **Linearkombination** (LK) **von** $(v_1, ..., v_n)$ ist ein Element $v \in V$ der Form:*

$$v = \sum_{i=1}^{n} a_i v_i \qquad \text{mit } a_i \in K$$

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

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

Menge aller Linearkombinationen von n-Tupeln aus M (n beliebig).
Ist $M = \emptyset$, dann setzen wir $<M> := \{0\}$.
*$<M>$ heißt das **Erzeugnis von M in V**.*

2.2.5 Satz

Sei V ein K-VR, $M \subseteq V$, 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) bis (UV3), o.B.d.A. sei $M \neq \emptyset$ (sonst ist a) klar).

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

(UV2) Seien $w, w' \in <M>$, etwa

$$w = \sum_{i=1}^{m} a_i v_i, \qquad w' = \sum_{i=1}^{n} a'_i v'_i$$

mit $a_i, a'_i \in K$, $v_i, v'_i \in M$.

$$\Rightarrow w + w' = \sum_{i=1}^{m} a_i v_i + \sum_{i=1}^{n} a'_i v'_i \text{ ist LK von } (v_1, ..., v_m, v'_1, ..., v'_n)$$

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

$$w = \sum_{i=1}^{m} a_i v_i, \qquad \text{mit } a_i \in K, v_i \in M$$

$$\Rightarrow aw = \sum_{i=1}^{m} (aa_i) v_i \text{ ist LK von } (v_1, ..., v_m)$$

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

$$\underbrace{\Rightarrow}_{M \subseteq W} v_i \in W \qquad \forall 1 \leq i \leq m$$

$$\underbrace{\Rightarrow}_{(UV3),(UV2)} \quad w = \sum_{i=1}^{m} (a_i) v_i \in W \Rightarrow <M> \leq W$$

2.2.6 Beispiele

a) $V = \mathbb{R}^3$

$$v_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix} \Rightarrow v_1 - 2 \cdot v_2 = \begin{pmatrix} 3 \\ 1 \\ -4 \end{pmatrix}$$

oder

$$v_1 + v_2 = \begin{pmatrix} 0 \\ -2 \\ 2 \end{pmatrix} \text{ ist LK von } (v_1, v_2)$$

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

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

Sind $x_1, ..., x_n \in K$, dann ist

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

eine LK von $(s_1, ..., s_n)$, nämlich

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

Sind $y_1, ..., y_m \in K$, dann ist $(y_1, ..., y_m) \cdot A$ eine LK von $(z_1, ..., z_m)$, nämlich

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

$<\{z_1, ..., z_m\}> \leq K^{1\times n}$ heißt der **Zeilenraum von A**.
$<\{s_1, ..., s_n\}> \leq K^{m}$ heißt der **Spaltenraum von A**.

z.B.:

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

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

$$\begin{pmatrix} 1, & 1, & 1, & 1 \end{pmatrix} \cdot A =$$
$$1 \cdot \begin{pmatrix} -1, & 0, & 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0, & 1, & 2 \end{pmatrix} + 1 \cdot \begin{pmatrix} 3, & 4, & 4 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1, & -2, & 3 \end{pmatrix} =$$
$$\begin{pmatrix} 3, & 3, & 11 \end{pmatrix}$$

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

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

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

Definition 2.2.4 *Seien V, W K-VR* $\qquad \varphi : V \to W$

1. *φ heißt **lineare Abbildung** (K-Homomorphismus) falls gilt:*

   a) $\varphi(v + v') = \varphi(v) + \varphi(v') \qquad \forall v, v' \in V$

b) $\varphi(a \cdot v) = a \cdot \varphi(v) \qquad \forall a \in K, v \in V$

$$Hom_K(V,W) := \{\psi : V \to W \mid \psi \text{ linear}\}$$

2. *Für $W = V$ und φ linear, heißt φ ein* ***Endomorphismus***
   $End_K(V) := Hom_K(V,V)$.

3. *Sei φ linear, dann heißt φ ein*
   Monomorphismus*, wenn φ injektiv ist,*
   Epimorphismus*, wenn φ surjektiv ist,*
   Isomorphismus*, wenn φ bijektiv ist.*
   (vergl. 2.1.2)
   V und W heißen ***isomorph****, geschrieben $V \cong W$, falls ein Isomorphismus $\psi : V \to W$ existiert.*

2.2.7 Beispiele

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

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

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

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

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

c) $K = \mathbb{R}, \qquad V = \mathbb{R}^{\mathbb{R}}, \quad r \in \mathbb{R}$
   $\epsilon_r : V \to \mathbb{R}, \qquad f \mapsto f(x)$
   $\epsilon(f+g) = (f+g)(r) = f(r) + g(r) = \epsilon(f) + \epsilon(g) \quad \forall f,g \in \mathbb{R}^{\mathbb{R}}$
   $\epsilon(af) = (af)(r) = a \cdot f(r) = a \cdot \epsilon(f) \qquad \forall f,g \in \mathbb{R}^{\mathbb{R}},\ a \in \mathbb{R}$

d) Sei $A \in K^{m\times n}$.
   $\varphi_A : K^n \to K^m, \qquad \varphi_A(x) := A \cdot x$ ist linear (vergl. 2.1.14)

e) $K = \mathbb{R}, \qquad V = C^\infty(\mathbb{R})$.
   $\varphi : V \to V, \qquad f \mapsto f'$ (Ableitung) ist linear (Ableitungsregel)

Definition 2.2.5 *Seien V, W K-VR, $\varphi \in Hom_k(V,W)$*

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

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

$$\textit{Kern } \varphi \subseteq V, \qquad \textit{Bild } \varphi \subseteq W$$

2.2.8 Bemerkung

Seien V, W K-VR, $\varphi \in \mathrm{Hom}_k(V, W)$, dann gilt:

a) Kern $\varphi \leq V$

b) Bild $\varphi \leq W$

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

d) φ surjektiv $\Leftrightarrow$ Bild $\varphi = W$

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

$$\Rightarrow \underbrace{\varphi^{-1}(\{w\})}_{\text{Fasern von } \varphi \text{ zu } w} = \underbrace{v + \text{Kern } \varphi}_{\text{Konv. 2.1.5: } \{v+v' \mid v' \in \text{Kern } \varphi\}}$$

Beweis

a) (UV1) $\varphi(0) = \varphi(0v) = 0\varphi(v) = 0 \Rightarrow 0 \in$ Kern φ

(UV2) Seien $v, v' \in$ Kern $\varphi \Rightarrow$
$\varphi(v + v') = \varphi(v) + \varphi(v') = 0 + 0 = 0 \Rightarrow v + v' \in$ Kern φ

(UV3) Seien $a \in K$, $v \in$ Kern $\varphi \Rightarrow$
$\varphi(a \cdot v) = a \cdot \varphi(v) = a \cdot v = 0 \Rightarrow av \in$ Kern φ.
Aus 2.2.1 folgt: Kern $\varphi \leq V$.

b) (UV1) $0 = \varphi(0) \Rightarrow 0 \in$ Bild φ

(UV2) Seien $w, w' \in$ Bild φ, etwa $w = \varphi(v)$, $w' = \varphi(v')$ für $v, v' \in V$
$\Rightarrow w + w' = \varphi(v) + \varphi(v') = \varphi(v + v') \Rightarrow w + w' \in$ Bild φ

(UV3) Seien $a \in \mathbb{R}$, $w \in$ Bild φ, etwa $w = \varphi(v)$ für ein $v \in V$
$\Rightarrow aw = a \cdot \varphi(v) = \varphi(a \cdot v) \in$ Bild φ
Aus 2.2.1 folgt: Bild $\varphi \leq W$

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

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

d) Klar.

e) $v \in V, \qquad v \overset{\varphi}{\mapsto} w, \qquad v' \overset{\varphi}{\mapsto} w$
zu zeigen: $\varphi^{-1}(\{w\}) = v +$ Kern φ.

„$\supseteq$" Sei $u = v + v'$ mit $v' \in$ Kern φ
$\Rightarrow \varphi(u) = \varphi(v) + \varphi(v') = w + 0 = w \Rightarrow u \in \varphi^{-1}(\{w\})$

„$\subseteq$" Sei $u \in \varphi^{-1}(\{w\})$, zu zeigen: $u = v + v'$ mit einem $v' \in$ Kern φ.
Setze $v' := u - v = \varphi(u - v) = \varphi(u) - \varphi(v) = w - w = 0$
$\Rightarrow v' \in$Kern φ, d.h. $u = v + v' \in v +$ Kern φ

2.2.9 Beispiele

a) $K = \mathbb{R}, \qquad V = C^\infty(\mathbb{R}), \qquad \varphi : V \to V, \qquad f \mapsto f'$ f ist surjektiv (Hauptsatz der Infinitesimalrechnung)
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) Kern $\varphi_A = \{c \in K^n \mid Ac = 0\}$ ist <u>die</u> Lösungsmenge des homogenen LGS $Ax = 0$.
2) Sei $c \in K^n$ eine Lösung des LGS $Ax = b$. Dann ist die Lösungsmenge dieses LGS gleich $c+$Kern φ_A
3) (Lösbarkeitskriterium): Die folgenden Aussagen sind äquivalent:
   i) $Ax = b$ ist lösbar
   ii) $b \in$ Bild φ_A
   iii) $b \in$ Spaltenraum von A
   iv) Spaltenraum von A = Spaltenraum von (A, b)

Beweis

a) Analysis.

b) 1) Klar.
2) Die Lösungsmenge des LGS $Ax = b$ ist

$$\{c' \in K^n \mid \varphi_A(c') = b\} = c + \text{Kern } \varphi_A \qquad \text{(nach 2.2.8 e))}$$

3) Seien $s_1, ..., s_n \in K^m$ die Spalten von A

$i) \Rightarrow ii)$ Trivial nach Definition von φ_A

ii) $\Rightarrow$ *iii)* $b \in$ Bild $\varphi_A \Rightarrow \exists c \in K^n$ mit $Ac = b$. Sei $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ mit $c_i \in K$

$$\underbrace{\Rightarrow}_{2.2.6 \text{ b)}} \quad Ac = \sum_{i=1}^{n} c_i s_i, \text{ d.h. } b \in \text{ Spaltenraum von } A$$

iii) $\Rightarrow$ *iv)* b ist LK von $(s_1, ..., s_n) \Rightarrow$ Jede LK von $(s_1, ..., s_n, b)$ (d.h. der Spalten von (A, b)) ist auch LK von $(s_1, ..., s_n) \Rightarrow$ Behauptung.

iv) $\Rightarrow$ *i)* $b \in$ Spaltenraum von $(A, b) =$ Spaltenraum von A
$\Rightarrow$ es existiert $c_1, ..., c_n \in K$ mit

$$b = \sum_{i=1}^{n} c_i s_i$$

$$\underbrace{\Rightarrow}_{2.2.6 \text{ b)}} \quad A = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = b, \text{ d.h. das LGS ist lösbar.}$$

2.3 Basis und Dimension

Sei K ein Körper, V ein K-VR.

Definition 2.3.1 *a) Ein n-Tupel $(v_1, ..., v_n)$ mit $v_i \in V$ heißt **linear abhängig** (l.a.), wenn $a_1, ..., a_n \in K$ existiert mit $(a_1, ..., a_n) \neq 0 \in K^{1 \times n}$ und $\sum_{i=1}^{n} a_i v_i = 0$. Andernfalls heißt $(v_1, ..., v_n)$ **linear unabhängig** (l.u.).*

*b) $M \subseteq V$ heißt **linear abhängig** (l.a.), wenn ein l.a. n-Tupel $(v_1, ..., v_n)$ existiert mit $v_i \neq v_j$ für $i \neq j$ und $v_i \in M \quad 1 \leq i \leq n$*
Andernfalls heißt M linear unabhängig (l.u.). Insbesondere ist $\emptyset \subseteq V$ l.u..

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

2.3.1 Bemerkung

Seien $v_1, ..., v_n \in V$ und seien $M' \subseteq M \subseteq V$

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. $\Rightarrow M$ ist l.a.

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

b) $(v_1, ..., v_n)$ ist l.u. genau dann, wenn gilt:
Sind $a_i, ..., a_n \in K$ mit $\sum\limits_{i=1}^{n} a_i v_i = 0$, dann ist $a_1 = a_2 = \cdots = a_n = 0$ (Der Nullvektor lässt sich nur auf die triviale Weise aus $v_1, ..., v_n$ linear kombinieren).

c) Die folgenden Aussagen sind äquivalent:

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

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

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

Beweis

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

(2) Folgt aus 2.2.1 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 „$(v_1, ..., v_n)$ ist l.a.“.

c) $\underline{(1) \Rightarrow (2)}$:

$(v_1, ..., v_n)$ l.a. $\Rightarrow$ Es existiert $a_1, ..., a_n \in K$ mit $(a_1, ..., a_n) \neq 0$ und $\sum\limits_{i=1}^{n} a_i v_i = 0$.

Sei i_0 so, dass $a_{i_0} \neq 0$ ist $\Rightarrow v_{i_0} = -\sum\limits_{\substack{i=1 \\ i \neq i_0}}^{n} a_{i_0}^{-1} a_i v_i \in <v_1, ..., v_{i_0-1}, v_{i_0+1}, ..., v_n>$

$\underline{(2) \Rightarrow (3)}$:
Ist $v_{i_0} \in <v_1, ..., v_n> = <v_1, ..., v_{i_0-1}, v_{i_0+1}, ..., v_n>$, dann ist
$<v_1, ..., v_n> = <v_1, ..., v_{i_0-1}, v_{i_0+1}, ..., v_n>$

$\underline{(3) \Rightarrow (1)}$:
$v_{i_0} \in <v_1, ..., v_n> = <v_1, ..., v_{i_0-1}, v_{i_0+1}, ..., v_n>$
$\Rightarrow$ es ex. $a_1, ..., a_{i_0-1}, a_{i_0+1}, ..., a_n \in K$
mit $\sum\limits_{\substack{i=1 \\ i \neq i_0}}^{n} a_i v_i = v_{i_0}$, d.h. $\sum\limits_{i=0}^{n} a_i v_i = 0$ mit $a_{i_0} = -1$
$(a_1, ..., a_{i_0-1}, -1, a_{i_0+1}, ..., a_n) \neq 0 \Rightarrow (v_1, ..., v_n)$ ist l.a.

Definition 2.3.2 *$A \in K^{m \times n}$ hat* ***Spaltenstufenform****, wenn A^t Zeilenstufenform hat.*

2.3.2 Beispiele

a) $V = \mathbb{Q}^2$ $\quad \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\}$ ist l.u. Seien $a_1, a_2 \in \mathbb{Q}$ mit

$$a_1 \begin{pmatrix} 1 \\ 2 \end{pmatrix} + a_2 \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\text{also: } \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

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

$\Rightarrow$ Das homogene LGS mit Matrix $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ hat nur die triviale Lösung $a_1 = a_2 = 0$.

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

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

b) Sei $A \in K^{m \times n}$ eine Matrix in Zeilenstufenform, und seien $z_1, ..., z_r$ die von 0 verschiedenen Zeilen von A, dann ist $(z_1, ..., z_r)$ l.u..
Analog: Die von 0 verschiedenen Spalten einer Matrix in Spaltenstufenform sind l.u..
Insbesondere sind die Zeilen und Spalten von E_n l.u..

Beweis

Für $1 \leq i \leq r$ sei $(a_{i,1}, \ldots, a_{i,n}) = z_i$, wobei a_{i,j_i} der erste von 0 verschiedene Eintrag in z_i sei:

$$A = \begin{pmatrix} z_1 \\ \vdots \\ z_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & a_{1,j_1} & \ldots & a_{1,j_r} & \ldots & a_{1,n} \\ \vdots & 0 & \ddots & & & \vdots \\ 0 & \ldots & 0 & a_{r,j_r} & \ldots & a_{r,n} \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \\ \vdots & \ldots & \ldots & \ldots & \ldots & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & 0 \end{pmatrix}.$$

Da A in Zeilenstufenform ist, gilt $j_1 < j_2 < \ldots < j_r$.
Seien nun $a_1, \ldots, a_r \in K$ beliebig mit $\sum_{i=1}^r a_i z_i = 0$. Da $a_{i,j_1} = 0$ für $i > 1$, muß $a_1 a_{1,j_1} = 0$ gelten. Da $a_{1,j_1} \neq 0$ nach Konstruktion von j_1, ist $a_1 = 0$.

Somit erhalten wir $\sum_{i=2}^{r} a_i z_i = 0$, und durch Induktion ergibt sich $a_i = 0$ auch für $2 \leq i \leq r$.
Die 2. Aussage folgt aus der 1. durch Transponieren.

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

Beweis

Seien $a, b \in \mathbb{R}$ mit $a \cdot \sin + b \cdot \cos = 0$
$\Rightarrow \quad 0 = a \cdot \sin(0) + b \cdot \cos(0) = b$ und
$\qquad 0 = a \cdot \sin(\frac{\pi}{2}) + b \cos(\frac{\pi}{2}) = a$

Definition 2.3.3 *Sei $M \subseteq V$, $\qquad v_1, ..., v_n \in V$*

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

2.3.3 Beispiele

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

b) $V = K^m$, $\qquad$ für $1 \leq i \leq m$ sei $e_i := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ $\qquad$ (1 an i-ter Position)

$\Rightarrow (e_1, ..., e_m)$ ist geordnete Basis von K^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 1 an Position (i, j) und Null sonst:

z.B. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$
$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

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

2.3.4 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 $M \subsetneq M' \subset V$, dann ist M' l.a.).

3) M ist ein minimales Erzeugendensystem von V (d.h. $<M> = V$ und $<M'> \neq V$ für alle $M' \subsetneq M$).

Beweis

1) $\Rightarrow$ 2): M ist l.u., da Basis.
$v \in V = <M> \Rightarrow$ es existiert $v_1, ..., v_n \in M$ mit $v_i \neq v_j$ für $i \neq j$ und $v \in <v_1, ..., v_n>$
$\Rightarrow$ $(v_1, ..., v_n, v)$ ist l.a. $\Rightarrow$ M' ist l.a., da $v_1, ..., v_n, v$ paarweise verschiedene Elemente aus M'.

2) $\Rightarrow$ 3): z.z.

a) $<M> = V$

b) Ist $M' \subsetneq M$, dann ist $<M'> \neq V$.

zu a) Sei $v \in V$, $v \notin M$.
Setze $M'' := M \cup \{v\}$
$\Rightarrow M \subsetneq M'' \subseteq V$
$\Rightarrow M''$ ist l.a.
$\Rightarrow$ es existiert $v_1, ..., v_n \in M''$ mit $v_i \neq v_j$ für $i \neq j$ und $(v_1, ..., v_n)$ ist l.a.
$\Rightarrow$ es existiert $a_1, ..., a_n \in K$ mit $(a_1, ..., a_n) \neq 0$ und $\sum\limits_{i=1}^{n} a_i v_i = 0$
$\overset{M \text{ l.a.}}{\Longrightarrow}$ $v \in \{v_1, ..., v_n\}$, sagen wir $v = v_{i_0}$, und es gibt $a_{i_0} \neq 0$.
$\Rightarrow v \in <v_1, ..., v_{i_0-1}, v_{i_0+1}, ..., v_n> \subseteq <M>$

zu b) Sei $M' \subsetneq M$. Angenommen M' ist Basis von V (2.3.1 a) (4))
$\Rightarrow M$ ist la (1) $\Rightarrow$ 2)) Widerspruch!

3) $\Rightarrow$ 1) z.z. M ist l.u. Angenommen: M ist l.a., es existiert $v_1, ..., v_n \in M$ mit $v_i \neq v_j$ für $i \neq j$ und $(v_1, ..., v_n)$ ist l.a. $\Rightarrow \exists i_0,\ 1 \leq i_0 \leq n$ mit $v_{i_0} \in <v_1, ..., v_{i_0-1}, v_{i_0+1}, ..., v_n>$
Setze $M' := \{v \in M \mid v \neq v_{i_0}\}$
$\Rightarrow M' \subsetneq M$ und $<M'> = <M>$ Widerspruch!
Damit sind alle Teile bewiesen!

2.3.5 Bemerkung

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

Beweis

Existenz: Klar, wegen $v = <v_1, ..., v_n>$
Eindeutigkeit: Sei $\sum_{i=1}^{n} a_i v_i = v = \sum_{i=1}^{n} a'_i v_i \Rightarrow 0 = \sum_{i=1}^{n} (a_i - a'_i) v_i$

$$\underbrace{\Rightarrow}_{(v_1,...,v_n) \text{ ist l.u.}} \quad a_i - a'_i = 0 \quad \forall\, 1 \leq i \leq n$$

2.3.6 Satz

Sei $(v_1, ..., v_m)$ eine geordnete Basis von V und seien $w_1, ..., w_n \in V$. Dann gilt:

$$n > m \Rightarrow (w_1, ..., w_n) \text{ ist l.a.}$$

Beweis

Für $1 \leq j \leq n$ seien $a_{ij} \in K,\ 1 \leq i \leq m$ definiert durch

$$w_j = \sum_{i=1}^{m} a_{ij} v_i \qquad \text{(siehe 2.3.5)}$$

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 $n > m$)

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

$\Rightarrow (w_1, .., w_n)$ ist l.a.

2.3.7 Satz

Sei V endlich erzeugt, dann gilt:

a) V besitzt eine endliche Basis

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

c) (Basisergänzungssatz) Sei $M' \subset V$ l.u., dann existiert Basis M von V mit $M' \subset M$.

Beweis

a) $V = \{0\}$, dann o.k.
Sei $V \neq \{0\}$ und $n \in \mathbb{N}$ minimal, so dass $v_1, ..., v_n$ existiert mit $V = <v_1, ..., v_n>$.
$\Rightarrow \{v_1, ..., v_n\}$ ist ein minimales Erzeugendensystem $\overset{2.3.4}{\Rightarrow} \{v_1, ..., v_n\}$ ist Basis

b) Sei $(v_1, ..., v_n)$ geordnete Basis von V (existiert nach a)), und seien $w_1, ..., w_m \in M_1$, so dass $(w_1, ..., w_m)$ l.u. ist. $\overset{2.3.6}{\Longrightarrow} m \leq n$.
Insbesondere ist M_1 endlich und $|M_1| \leq n$
$\overset{2.3.6}{\Longrightarrow} n \leq |M_1|$ also $|M_1| = n$
Analog für M_2.

c) V besitzt 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 2.3.6 hat jedes solche M'' maximal n Elemente).
$\Rightarrow M$ ist maximale l.u. Teilmenge von $V \overset{2.3.4\ 2)}{\Longrightarrow} M$ ist Basis von V.

Definition 2.3.4 *Sei V endlich erzeugt, M eine Basis von V.*

$$\dim V := \dim_K V := |M|$$

*heißt die **Dimension** von V. (Anzahl der Elemente einer Basis von V)*

2.3.8 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 eine Basis von $\mathbb{Q}^2$, dann $\dim \mathbb{Q}^2 = 2$ und
$\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right)$ ist l.u. nach 2.3.2 a)

$\Rightarrow \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\}$ ist maximale l.u. Teilmenge von Q^2.
Ist V nicht endlich erzeugt, dann setzen wir $\dim_K V := \infty$.
Im Folgenden sei „endlich erzeugt“ gleichwertig „endlich-dimensional“.

2.3.9 Korollar (zu 2.3.7)

Sei $\dim_K V = n, \quad v_1, ..., v_n, v_{n+1} \in V$, dann gilt:

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

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

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

Beweis

a) Folgt aus 2.3.7 c) und b)

b) Folgt aus 2.3.7 b) und 2.3.4 3)

c) Folgt aus 2.3.7 a) und b) und aus 2.3.6

2.3.10 Korollar (zu 2.3.7)

Seien V und W endlich erzeugte 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 $(v_1, ..., v_n)$ eine geordnete Basis von V

$$\Rightarrow (\varphi(v_1), ..., \varphi(v_n)) \text{ ist geordnete Basis von W} \Rightarrow \dim_K V = \dim_K W$$

„$\Leftarrow$“ Sei $(v_1, ..., v_n)$ geordnete Basis von V. Definiere $\kappa : V \to K^n$ durch

$$v \mapsto \kappa(v) := \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n, \text{ falls } v = \sum_{i=1}^{n} a_i v_i \text{ (vergl. 2.3.5).}$$

Leicht selbst zu sehen: κ ist K-linear und bijektiv, d.h. κ ist 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 heißt „Basis“ bei e. e. K-VR immer „geordnete Basis“.

2.3.11 Satz

Sei V endlich dimensionaler K-VR, $U \lneq V$, dann gilt:

$$\dim_K U < \dim_K V$$

Beweis

Seien $u_1, ..., u_m \in U$ mit m maximal, so dass $(u_1, ..., u_m)$ l.u. ist (falls $U \neq \{0\}$).

$$\text{Sei } u \in U \overset{m \text{ max.}}{\Longrightarrow} (u_1, ..., u_m, u) \text{ ist l.a.} \overset{2.3.1 \text{ c)}}{\Longrightarrow} u \in <u_1, ..., u_m>$$

$$\Rightarrow U = <u_1, ..., u_m> \quad \text{d.h. } (u_1, ..., u_m) \text{ ist Basis von U}$$

Ist $\dim_K V = n$, dann ist $m \leq n$ nach 2.3.6.
Wäre $m = n$, dann wäre $V \overset{2.3.9 \text{ a)}}{=} <u_1, ..., u_m> = U$

2.3.12 Beispiel (Version der komplexen Zahlen)

Sei $V = \mathbb{R}^{2\times 2}$, $\qquad E := E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in V, \qquad I := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in V$
$\mathbb{C} := <E, I> \leq V$
(E, I) l.u. $\qquad (aE + bI = 0 \Rightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = 0 \Rightarrow a = b = 0$
$\Rightarrow E, I$ $\mathbb{R}$-Basis von $\mathbb{C}$
Insbesondere hat jedes $C \in \mathbb{C}$ eine eindeutige Darstellung als $C = xE + yI$ 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 $C = xE + yI \neq 0$ (d.h. $x^2 + y^2 \neq 0$), dann ist $C \cdot \frac{1}{x^2+y^2}(xE - yI) = E$, d.h. C ist invertierbar.
$\Rightarrow \mathbb{C}$ ist Körper, der Körper der komplexen Zahlen.
$\{xE \mid x \in \mathbb{R}\} \subseteq \mathbb{C}$ ist ein zu $\mathbb{R}$ isomorpher Teilkörper von $\mathbb{C}$.

Definition 2.3.5 (elementare Matrizen) *Für $n \in \mathbb{N}$ definieren wir Matrizen aus $K^{m\times n}$:*

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

Zeilen i und j entsteht.

$$T_{i,j} = \begin{pmatrix} 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 0 & & & 1 & & & \\ & & & & 1 & & & & & \\ & & & & & \ddots & & & & \\ & & & 1 & & & 0 & & & \\ & & & & & & & 1 & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & 1 \end{pmatrix}$$

(2) Für $1 \leq i \neq j \leq m$ und $c \in K$ sei $A_{i,j}(c) := E_m + cE_{i,j}$ (vergl. 2.3.3 c))

$$A_{i,j}(c) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 1 & & c & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

(c steht in der i-ten Zeile und j-ten Spalte)

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

$$M_i(c) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & c & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

(c steht in der i-ten Zeile)

2.3.13 Bemerkung

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

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

b) Entsteht A' aus A durch eine elementare Zeilentransformation (vergl. 1.4.6) vom Typ:

(1) $t_{i,j}$ oder

(2) $a_{i,j}(c)$ oder

(3) $m_i(c)$

dann gilt in den jeweiligen Fällen:

(1) $A' = T_{i,j}A$

(2) $A' = A_{i,j}(c)A$

(3) $A' = M_i(c)A$

c) Analog werden elementare Spaltenraumtransformationen von A duch 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 $S \in GL_m(K)$ und $T \in GL_n(K)$ mit $B = SAT$.

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 2.2.4 b).

c) A'' entstehe aus A durch eine elementare Spaltentransformation.
$\Rightarrow A'' = (EA^t)^t$ wobei A durch eine elementare Zeilentransformation entstanden ist.

$$\Rightarrow A'' = (EA^t)^t = (A^t)^t E^t = AE^t$$

d) Nach b) und c) ist

$$B = S_k S_{k-1} \dots S_1 A T_1 T_2 \dots T_l$$

mit elementaren Matrizen S_i, T, j, $S_i \in GL_M(K)$, $T_j \in GL_n(K)$.
Weil $GL_m(K)$, $GL_n(K)$ Gruppen sind, sind $S := S_k S_{k-1} \dots S_1$ und $T := T_1 T_2 \dots T_l$ invertierbar und $B = SAT$

2.3.14 Beispiel

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

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

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

2.3.15 Bemerkung

Sei $A \in K^{m\times n}$, $S \in GL_m(K)$, $T \in GL_n(K)$

a) $\varphi_S : K^m \to K^m, \qquad v \mapsto Sv$, und
$\psi_T : K^{1\times n} \to K^{1\times n}, \qquad v \mapsto vT$
sind $K-VR$ Isomorphismen.

b) Zeilenraum von $A =$ Zeilenraum von SA und
Spaltenraum von $A =$ Spaltenraum von AT

c) Zeilenraum von $A \cong$ Zeilenraum von AT und
Spaltenraum von $A \cong$ Spaltenraum von SA

Beweis

a) φ_S, ψ_T sind K-linear. Sie sind bijektiv mit den Umkehrabbildungen $\varphi_{S^{-1}}$ bzw. $\psi_{T^{-1}}$ (siehe 1.4.1).

b) Zeilenraum von $A =$ Zeilenraum von $S^{-1}(SA)$
$\underbrace{\subseteq}_{2.2.6\text{ b)}}$ Zeilenraum von $S \cdot A$ $\underbrace{\subseteq}_{2.2.6\text{ b)}}$ Zeilenraum von A

2. Aussage analog duch Transponieren.

c) Seien $z_1, \ldots, z_m$ die Zeilen von A
$\overset{2.2.6\text{ b)}}{\Longrightarrow} z_1T = \psi_T(z_1), \ldots, z_MT = \psi_T(z_m)$ sind die Zeilen von AT
$\psi_T : K^{1\times n} \to K^{1\times n}$ ist Isomorphismus
$\Rightarrow \psi_T|_U : U \to \psi_T(U), \qquad u \mapsto \psi_T(u) = uT$ ist Isomorphismus $\forall U \leq K^{1\times m}$
$U = <z_1, \ldots, z_m>$ =Zeilenraum von A
$\Rightarrow \psi_T(U) = <\psi_T(z_1), \ldots, \psi_T(z_m)> =$ Zeilenraum von AT
$\Rightarrow$ Behauptung.

2. Aussage analog

Definition 2.3.6 (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 $0 \leq r \leq \min\{m,n\}$ *überführt werden.*

b) Es existiert $S \in GL_m(K)$, $T \in GL_n(K)$ *mit*

$$SAT = \left(\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right) \quad \textit{mit } 0 \leq r \leq \min\{m,n\}$$

.

c) $\dim_K$ *(Zeilenraum von A)* $= \dim_K$ *(Spaltenraum von A)* $= r$ *mit* r *wie in a) oder b).*

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

Beweis

a) Durch elementare Zeilentransformationen $\longrightarrow$ Zeilenstufenform wie folgt:

$$\left(\begin{array}{ccc|cccccccc}
0 & \cdots & 0 & 1 & * & * & * & * & * & \cdots & * \\
0 & \cdots & 0 & 0 & 0 & 1 & * & * & * & \cdots & * \\
0 & \cdots & 0 & 0 & 0 & 0 & 1 & * & * & \cdots & * \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & * \\ \hline
0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0
\end{array}\right)$$

wobei die ersten r Zeilen nicht nur aus Nullen bestehen.

$$\xrightarrow{\text{Vertauschen von Spalten}}$$

$$\left(\begin{array}{ccccccccccc}
1 & * & * & * & * & * & * & * & * & \cdots & * \\
0 & 1 & * & * & * & * & * & * & * & \cdots & * \\
0 & 0 & 0 & 0 & 1 & * & * & * & * & \cdots & * \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & * \\ \hline
0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0
\end{array}\right)$$

$$\xrightarrow{\text{Ausräumen von Spalten}} \left(\begin{array}{ccc|c} 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right)$$

b) Folgt aus a) und 2.3.13 a)

c) Aus b) und 2.3.15 c) folgt:
$\dim_K$ (Zeilenraum von A) $=$
$\dim_K$ (Zeilenraum von SA) $=$
$\dim_K$ (Zeilenraum von $(SA)T$) $=$
$\dim_K$ (Spaltenraum von A)

$\dim_K$ (Zeilenraum von A) heißt auch **Zeilenrang**.
$\dim_K$ (Spaltenraum von A) heißt auch **Spaltenrang**.

Nach 2.3.6 c) gilt: Spaltenrang = Zeilenrang.

2.3.16 Charakterisierung von „Rang“

Sei $A \in K^{m\times n}$, dann gilt: rang A = Maximalzahl l.u. Zeilen von A = Maximalzahl l.u. Spalten von A

(„Maximalzahl l.u. Zeilen von A“ heißt größtes $r \in \mathbb{N}_0$, so dass $z_{i1}, \ldots, z_{ir} \in \{z_1, ..., z_m\}$ existieren, so dass $(z_{i1}, \ldots, z_{ir})$ l.u. ist. Hierbei ist $\{z_1, ..., z_m\}$ die Menge der Zeilen von A.)

Beweis

Notation wie oben.
$\overset{2.3.1}{\Longrightarrow} <z_{i1}, \ldots, z_{ir}> = <z_1, \ldots, z_m>$ = Zeilenraum von A
$\Rightarrow r = \dim_K$ (Zeilenraum von A) = rang A

Analog für Spaltenraum.

2.3.17 Bemerkung

Sei $A \in K^{m\times n}$. Bringe A durch elementare Spaltentransformationen auf Spaltenstufenform A' (vgl. 2.3.2). Seien $s'_1, ..., s'_r$ die von 0 verschiedenen Spalten von A'. Dann gilt:

a) rang $A = r$

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

Beweis

a) folgt aus b)

b) Spaltenraum von A $\overset{2.3.15\text{ b)}}{=}$ Spaltenraum von $A' = <s'_1, ..., s'_r>$
Nach 2.3.2 b) ist $(s'_1, ..., s'_r)$ l.u., also eine Basis.
Analoges gilt für den Zeilenraum.

2.3.18 Beispiel

$V = <\begin{pmatrix}1 & 1 & 1 & 1\end{pmatrix}, \begin{pmatrix}4 & 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}> \subseteq \mathbb{R}^4$

Gesucht: Basis von V.

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

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

2.3.19 Bemerkung

Verallgemeinerung: Sei V m-dimensionaler K-VR mit Basis $(v_1, ..., v_m)$.
Sei $\kappa : V \to K^m$ der Isomorphismus aus 2.3.10. Seien $w_1, ..., w_n \in V$

Gesucht: Basis von $<w_1, ..., w_n> =: W \leq V$

Methode: Berechne Basis $(u_1, ..., u_r)$ von $\kappa(W) = <\kappa(w_1), ..., \kappa(w_n)> \leq K^m$
$\Rightarrow (\kappa^{-1}(u_1), ..., \kappa^{-1}(u_r))$ ist Basis von W.

Beweis

$\kappa|_W : W \to \kappa(W), \qquad w \mapsto \kappa(w)$
ist ein Isomorphismus, der die Basen überträgt.

2.3.20 Beispiel

$V = \mathbb{R}^{3\times 2}, \qquad$ Basis: $(E_{1,1}, E_{1,2}, E_{2,1}, E_{2,2}, E_{3,1}, E_{3,2})$ (vgl. 2.3.3 c))

$$w_1 = \begin{pmatrix}1 & 2\\0 & 2\\3 & 2\end{pmatrix}, \quad w_2 = \begin{pmatrix}0 & 1\\-1 & 0\\0 & -1\end{pmatrix}, \quad w_3 = \begin{pmatrix}-1 & 0\\-1 & 0\\-1 & 0\end{pmatrix}, \quad w_4 = \begin{pmatrix}0 & 1\\0 & 0\\0 & 0\end{pmatrix}$$

$$\left[\begin{pmatrix}1&2\\0&2\\3&2\end{pmatrix} = 1\cdot E_{1,1} + 2\cdot E_{1,2} + 0\cdot E_{2,1} + 2\cdot E_{2,2} + 3\cdot E_{3,1} + 2\cdot E_{3,3}\right]$$

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

$$\Rightarrow \left(\begin{pmatrix}1&2\\0&2\\3&2\end{pmatrix}, \begin{pmatrix}0&1\\0&0\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\-1&0\\0&-1\end{pmatrix}, \begin{pmatrix}0&0\\0&2\\2&3\end{pmatrix}\right) \text{ ist Basis von } W = <w_1, w_2, w_3, w_4> \leq \mathbb{R}^{3\times 2}$$

2.3.21 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' habe Zeilenstufenform.
$\Rightarrow L_0$ ist die Lösungsmenge des homogenen LGS $A'x = 0$ (1.4.1)
Weiter gilt:
$\operatorname{rang} A \overset{2.3.15\text{ b)}}{=} \operatorname{rang} A' \overset{2.3.17}{=}$ Anzahl der Zeilen von A' die $\neq 0$ sind
$=$ Anzahl der abhängigen Variablen.
Aus 1.4.5 folgt:
$\dim_K L_0 =$ Anzahl der freien Variablen $= n - \operatorname{rang} A' = n - \operatorname{rang} A$

2.3.22 Satz

Sei $A \in K^{n\times n}$ mit Spalten $s_1, ..., s_n \in K^n$ und Zeilen $z_1, ..., z_n \in K^{1\times n}$. Dann sind folgende Aussagen äquivalent:

(a) A invertierbar

(b) Es existiert $B \in K^{n\times n}$ mit $AB = E_n$

(c) Es existiert $C \in K^{n\times n}$ mit $CA = E_n$

(d) Das homogene LGS $Ax = 0$ hat nur die triviale Lösung.

(e) Für jedes $b \in K^n$ hat das LGS $Ax = b$ genau eine Lösung.

(f) rang $A = n$

(g) $(z_1, ..., z_n)$ ist l.u.

(h) $(s_1, ..., s_n)$ ist l.u.

Beweis

$(g) \Leftrightarrow (f) \Leftrightarrow (h)$ nach 2.3.16
$\underline{(a) \Rightarrow (c)}$: Definition der Invertierbarkeit
$\underline{(c) \Rightarrow (d)}$: Sei $c \in K^n$ mit $Ac = 0 \Rightarrow 0 = C(Ac) = (CA)c = E_n c = c$
$\underline{(d) \Rightarrow (f)}$: Der Lösungsraum L_0 des homogenen LGS $Ax = 0$ hat die Dimension $0 \overset{2.3.21}{\Rightarrow}$ rang $A = n$
$\underline{(f) \Rightarrow (e)}$: rang $A = n \overset{2.3.16,\ 2.3.6}{\Longrightarrow}$ 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)
$\overset{2.2.9\ (3)}{\Longrightarrow}$ Das LGS $Ax = b$ ist lösbar.
Aus 2.2.9 und $L_0 \overset{2.3.21}{=} \{0\}$ folgt: $Ax = b$ hat genau eine Lösung.
$\underline{(e) \Rightarrow (b)}$: Seien $e_1, ..., e_n \in K^n$ 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 $B = (b_1, ..., b_n) \in K^{n \times n} \Rightarrow AB = (Ab_1, ..., Ab_n) = (e_1, ..., e_n) = E_n$
$\underline{(b) \Rightarrow (a)}$: $AB = E_n \Rightarrow B^t A^t = E_n$ $(E_n^t = E_n)$
$\Rightarrow$ rang $A^t = n$ (Zeilenraum von E_n) = Zeilenraum von $B^t A^t \leq$ Zeilenraum von A^t
$\overset{\text{nach Beweis } (f)\Rightarrow(e)\Rightarrow(b)}{\Longrightarrow} \exists D \in K^{n \times n}$ mit $A^t \cdot D = E_n$
$\Rightarrow B^t = B^t \cdot E_n = B^t(A^t D) = (B^t A^t)D = E_n D = D$
$\Rightarrow B^t = D$, d.h. A^t ist invertierbar.
$\overset{2.1.16}{\Longrightarrow}$ A ist invertierbar.

2.3.23 Korollar

Sei $A \in GL_n(K),\ b \in K^n$..
Die Lösung von $Ax = b$ (eindeutig nach 2.3.22) ist gegeben durch $A^{-1} \cdot b$.

Beweis

Ist $c \in K^n$ mit $Ac = b$, dann ist $c = E_n c = (A^{-1}A)c = A^{-1}(Ac) = A^{-1}b$.

2.3.24 Satz

Sei $A \in K^{m \times n},\ L_0 \leq K^n$ die Lösungsmenge von $Ax = 0$. Dann gilt:

(1) L_0 ist UVR von K^n mit $\dim_K L_0 = n -$ rang A.

(2) Die Anzahl der abhängigen Variablen ist gleich: $\operatorname{rang} A$.

(3) Sei $b \in K^n$, dann gilt: $Ax = b$ 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.

Beweis

Aus vorstehenden Resultaten zusammensetzen.
zu (5) : $(b) \Rightarrow (a) \overset{2.3.22}{\Longrightarrow} (c) \Rightarrow (b)$

2.3.25 Bemerkung (Algorithmus zum Invertieren)

Sei $A \in K^{n\times n}$, dann gilt:
A invertierbar $\Leftrightarrow (A|E_n) \in K^{n\times 2n}$ kann durch elementare Zeilentransformationen in $(E_n|B)$ überführt werden. In diesem Fall ist $B = A^{-1}$.

Beweis

„$\Rightarrow$“: Bringe A durch elementare Zeilentransformationen auf Zeilenstufenform A'.
A invertierbar $\overset{2.3.22}{\Longrightarrow} n = \operatorname{rang} A \overset{2.3.15}{\Longrightarrow} n = \operatorname{rang} A'$

$$\Rightarrow \begin{pmatrix} \square & * & * & \cdots & * \\ 0 & \square & * & \cdots & * \\ 0 & 0 & \square & \cdots & * \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \square \end{pmatrix} \text{ Keine freien Variablen.}$$

Räume nun (von hinten her) die Spalten aus.

„$\Leftarrow$“: Nach 2.3.13 existiert S mit $(E_n|B) = S(A|E_n) = (SA|S)$
$\Rightarrow SA = E_n$ und $S = B$
$\overset{2.3.22}{\Longrightarrow} A$ invertierbar und $S = A^{-1}$

2.3.26 Beispiel

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$$

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 0 & 1 \end{array}\right) \longrightarrow$$

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & -1 & -1 & 1 & 0 & 0 \end{array}\right) \longrightarrow$$

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -2 & -1 & 1 & 1 & -1 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right) \longrightarrow$$

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right) \longrightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & -1 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right)$$

$$\Rightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}^{-1} = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{array}\right)$$

2.4 Matrizen und lineare Abbildungen

2.4.1 Konventionen

Objekte:	Bezeichnungen:	
Matrizen	A,B,C,...	lateinische Großbuchstaben
Vektorräume	U,V,W,...	lateinische Großbuchstaben
lineare Abbildungen	$\alpha, \beta, ..., \varphi, \psi$	kleine griechische Buchstaben
geordnete Basen	$\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, ...$	Skript Buchstaben

Grundvorraussetzungen: K Körper, K-VR seien endlich erzeugt (e. e.), Basen geordnet.

2.4.2 Erinnerung und Definition

Sei V K-VR mit Basis $\mathcal{B} = (v_1, ..., v_n)$.

Definiere $\kappa_B : V \to K^n$ durch $\kappa_{\mathcal{B}}(v) := \begin{pmatrix} a_1 \\ \cdots \\ a_n \end{pmatrix}$, falls $v = \sum_{i=1}^{n} a_i v_i$ (vergl. 2.3.10).

$\kappa_{\mathcal{B}}(v)$ heißt der **Koordinatenvektor von v bzgl. $\mathcal{B}$**.

$\kappa_{\mathcal{B}}(v)$ ist ein Isomorphismus $V \to K^n$.

2.4.3 Beispiele

a) $V = K^{1\times n}$, $\mathcal{B} = (e_1^t, ..., e_n^t)$ die Standardbasis von V.

$$\Rightarrow \kappa_{\mathcal{B}}((a_1, ..., a_n)) = \begin{pmatrix} a_1 \\ \cdots \\ a_n \end{pmatrix}$$

b) $V = \mathbb{R}^2$, $\mathcal{B} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right)$

$$\begin{pmatrix} a \\ b \end{pmatrix} = (a-b) \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\kappa_{\mathcal{B}} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a-b \\ b \end{pmatrix}$$

Definition 2.4.1 (Abbildungsmatrix) *V, W K-VR, $\mathcal{B}$ Basis von V, $\mathcal{B} = (v_1, ..., v_n)$, $\mathcal{C} = (w_1, ..., w_m)$ Basis von W, $\varphi \in Hom_K(V, W)$*

Definiere $a_{ij} \in K$, $1 \le i \le m$, $1 \le j \le n$, durch

$$\varphi(v_j) = \sum_{i=1}^{m} a_{ij} w_i$$

Dann heißt $M_{\mathcal{C}}^{\mathcal{B}}(\varphi) := a_{ij}{}_{\substack{1\le i\le m \\ 1\le j\le n}} \in K^{m\times n}$ die Abbildungsmatrix von φ bzgl. $\mathcal{B}$ und $\mathcal{C}$.

2.4.4 Beispiele

a) $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} a+b \\ a-b \end{pmatrix}$

$\mathcal{B} = \mathcal{C} = (e_1, e_2)$ Standardbasis

$\varphi(e_1) = \varphi(\begin{pmatrix} 1 \\ 0 \end{pmatrix}) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1 \cdot e_1 + 1 \cdot e_2$

$\varphi(e_2) = \varphi(\begin{pmatrix} 0 \\ 1 \end{pmatrix}) = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = 1 \cdot e_1 - 1 \cdot e_2$

$\Rightarrow M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

b) $\varphi : K^{3\times 2} \to K^{2\times 3},\ A \mapsto A^t$
$\mathcal{B} = (E_{11}, E_{12}, E_{21}, E_{22}, E_{31}, E_{32})$
$\mathcal{C} = (E_{11}, E_{12}, E_{13}, E_{21}, E_{22}, E_{23})$

$$\Rightarrow M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

c) Sei $A \in K^{m\times n}$.
$\varphi = \varphi_A : K^n \to K^m,\ v \mapsto Av$
$\mathcal{B} = (e_1, ..., e_n), \qquad \mathcal{C} = (e_1, ..., e_m)$ Standardbasen
$\varphi(e_j) = Ae_j = j$-te Spalte von $A\ \forall\ 1 \leq j \leq n$
$\Rightarrow M_{\mathcal{C}}^{\mathcal{B}}(\varphi_A) = A$

d) In $C^\infty(\mathbb{R})$ seien p_i, $i \in \mathbb{N}_0$, definiert durch:

$$p_0 : \mathbb{R} \to \mathbb{R}, \qquad x \mapsto 1$$

$$p_i : \mathbb{R} \to \mathbb{R}, \qquad x \mapsto x^i,\ i \in \mathbb{N}$$

Sei $V = <p_0, ..., p_n> \leq C^\infty(\mathbb{R})$.
$(p_0, ..., p_n)$ ist l.u.:
Seien $a_0, ..., a_n \in \mathbb{R}$ mit $\sum\limits_{i=1}^{n} a_i p_i :\ x \mapsto \sum\limits_{i=1}^{n} a_i x^i = 0$
$\Rightarrow a_0 = a_1 = \ldots = a_n = 0$ (denn Polynom $\neq 0$ hat nur endlich viele Nullstellen)
$\Rightarrow \mathcal{B} = (p_0, ..., p_n)$ Basis von V.
Sei $\varphi : V \to V, \qquad f \mapsto f'$ (Ableitung).

$$\varphi(p_i) = \begin{cases} 0 \text{ für } i = 0 \\ ip_{i-1} \text{ für } i > 0 \end{cases}$$

$$\Rightarrow M_{\mathcal{B}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & n \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \in \mathbb{R}^{(n+1)\times(n+1)}$$

2.4.5 Satz

V, W seien K-VR, $\dim_K V = n$, $\dim_K W = m$, $\mathcal{B}, \mathcal{C}$ seien Basen von V bzw. W. Dann gilt für $\varphi \in \mathrm{Hom}_K(V, W)$:

a) $\kappa_{\mathcal{C}}(\varphi(v)) = M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \cdot \kappa_{\mathcal{B}}(v) \qquad \forall v \in V$

b) Sei $A = M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ und $\varphi_A : K^n \to K^m, \quad v \mapsto Av$, dann gilt:

$$\text{Kern } \varphi = \kappa_{\mathcal{B}}^{-1}(\text{Kern } \varphi_A)$$

$$\text{Bild } \varphi = \kappa_{\mathcal{C}}^{-1}(\text{Bild } \varphi_A)$$

c) $\dim_K V = \dim_K(\text{Kern } \varphi) + \dim_K(\text{Bild } \varphi)$

Beweis

a) $M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = (a_{ij})_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$, d.h. $\varphi(v_j) = \sum\limits_{i=1}^{m} a_{ij} w_i$ Sei $v \in V$, etwa $v = \sum\limits_{j=1}^{n} c_j v_j$,

$$\kappa_{\mathcal{B}}(v) = \begin{pmatrix} c_1 \\ \cdots \\ c_n \end{pmatrix}$$

$$\Rightarrow \varphi(v) = \sum_{j=1}^{n} c_j \varphi(v_j) = \sum_{j=1}^{n} c_j (\sum_{i=1}^{m} a_{ij} w_i) = \sum_{j=1}^{n} (\sum_{i=1}^{m} c_j a_{ij}) w_i = \sum_{j=1}^{n} (\sum_{i=1}^{m} a_{ij} c_j) w_i$$

$$\Rightarrow \kappa_{\mathcal{C}}(\varphi(v)) = \begin{pmatrix} \sum\limits_{j=1}^{n} a_{1j} c_j \\ \cdots \\ \sum\limits_{j=1}^{n} a_{mj} c_j \end{pmatrix} = A \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = A \cdot \kappa_{\mathcal{B}}(v)$$

b) $v \in \text{Kern } \varphi \Leftrightarrow \varphi(v) = 0 \overset{\kappa_{\mathcal{C}} \text{ Isom.}}{\Leftrightarrow} \kappa_{\mathcal{C}}(\varphi(v)) = 0$
$\overset{\text{a)}}{\Leftrightarrow} A \cdot \kappa_{\mathcal{B}}(v) = 0 \Leftrightarrow \kappa_{\mathcal{B}}(v) \in \text{Kern } \varphi_A$
$\overset{\kappa_{\mathcal{B}} \text{ Isom.}}{\Leftrightarrow} v \in \kappa_{\mathcal{B}}^{-1}(\text{Kern } \varphi_A)$

$w \in \text{Bild } \varphi \Leftrightarrow$ es gibt $v \in V : w = \varphi(v)$
$\Leftrightarrow$ es gibt $v \in V : \kappa_{\mathcal{C}}(w) = \kappa_{\mathcal{C}}(\varphi(v))$
$\overset{\text{a)}}{\Leftrightarrow}$ 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) $\dim \text{Kern } \varphi_A = \dim L_0$, da L_0 die Lösungsmenge von $Ax = 0$ ist.
Bild φ_A = Spaltenraum von A
$\Rightarrow \dim(\text{Bild } \varphi_A) = \text{rang}(A)$
$\Rightarrow n - \dim(\text{Bild } \varphi_A) = \dim \text{Kern } \varphi_A \qquad$ (siehe 2.3.21)

2.4.6 Beispiel

(vergl. 2.4.4 a))
$V := \langle p_0, ..., p_n \rangle \leq \mathbb{R}^{\mathbb{R}}, \mathcal{B} = (p_0, ..., p_n)$ mit $p_i : \mathbb{R} \to \mathbb{R},\ x \mapsto x^i$

Sei $\varphi : V \to V$, $\quad f \mapsto f'$ (Ableitung)
Sei $f : \mathbb{R} \to \mathbb{R}$, $\quad x \mapsto \sum\limits_{i=0}^{n} a_i x^i,\ f = \sum\limits_{i=0}^{n} a_i p_i$

$\kappa_{\mathcal{B}}(f) = \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix}$

$$M_{\mathcal{B}}^{\mathcal{B}}(\varphi) \cdot \kappa_{\mathcal{B}}(f) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & n \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ 2a_2 \\ \vdots \\ na_{n-1} \\ 0 \end{pmatrix}$$

$\Rightarrow \varphi(f) = f' = \sum\limits_{i=0}^{n-1} (i+1) a_{i+1} p_i, \qquad x \mapsto \sum\limits_{i=0}^{n-1} (i+1) a_{i+1} x^i$

2.4.7 Satz

Seien U, V, W K-VR 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 $\mathcal{A} = (u_1, ..., u_n)$, $\mathcal{B} = (v_1, ..., v_m)$ und $\mathcal{C} = (w_1, ..., w_l)$. 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:

$$\begin{aligned}
\psi \circ \varphi(u_k) &= \psi(\varphi(u_k)) = \psi(\sum_{j=1}^{m} b_{jk} v_j) \\
&= \sum_{j=1}^{m} b_{jk} \psi(v_j) \\
&= \sum_{j=1}^{m} b_{jk} (\sum_{i=1}^{l} a_{ij} w_i) \\
&= \sum_{j=1}^{m} \sum_{i=1}^{l} (a_{ij} b_{jk}) w_i \; 1 \leq k \leq n \\
\Rightarrow c_{ik} &= \sum_{j=1}^{m} a_{ij} b_{jk}, \; 1 \leq i \leq l, \; 1 \leq k \leq n
\end{aligned}$$

2.4.8 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 2.4.7 und 2.4.4 c).

2.4.9 Bemerkung

Seien V, W n-dimensionale K-VR mit Basen $\mathcal{B}$ bzw. $\mathcal{C}$ und sei $\varphi \in \operatorname{Hom}_K(V, W)$. Dann gilt:

$$\varphi \text{ Isomorphismus} \Leftrightarrow M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \text{ invertierbar}$$

In diesem Fall gilt: $M_{\mathcal{C}}^{\mathcal{B}}(\varphi)^{-1} = M_{\mathcal{B}}^{\mathcal{C}}(\varphi^{-1})$

Beweis

Sei $A = M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \in K^{n \times n}$, dann gilt:

$$\begin{aligned}
\varphi \text{ Isomorphismus} &\overset{2.4.5 \text{ c) und } \dim V = \dim W}{\Leftrightarrow} \varphi \text{ injektiv} \\
&\overset{2.2.8 \text{ c)}}{\Leftrightarrow} \text{Kern } \varphi = \{0\} \\
&\overset{2.4.5 \text{ b)}}{\Leftrightarrow} \text{Kern } \varphi_A = \{0\} \\
&\overset{2.2.9 \text{ b) und } 2.3.21}{\Leftrightarrow} \text{rang } A = n \\
&\overset{2.3.22}{\Leftrightarrow} A \text{ invertierbar}
\end{aligned}$$

Ist φ bijektiv, dann gilt:

$$M_{\mathcal{B}}^{\mathcal{C}}(\varphi^{-1})M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = M_{\mathcal{B}}^{\mathcal{B}}(\varphi^{-1} \circ \varphi) = M_{\mathcal{B}}^{\mathcal{B}}(id_V) = E_n.$$

$\overset{2.3.22}{\Rightarrow}$ A ist invertierbar und $A^{-1} = M_{\mathcal{B}}^{\mathcal{B}}(\varphi^{-1})$.

2.4.10 Bezeichnungen

Seien V, W endliche dimensionale K-VR mit Basen $\mathcal{B} = (v_1, ..., v_n)$ und $\mathcal{B}' = (v_1', ..., v_n')$ von V bzw.$\mathcal{C} = (w_1, ..., w_m)$ und $\mathcal{C}' = (w_1', ..., w_m')$ 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?

Definition 2.4.2 *Bezeichnungen wie in 2.4.10, dann heißt:*

$$M_{\mathcal{B}}^{\mathcal{B}'}(id_V) \in K^{n\times n} \quad \textit{\textbf{Basiswechselmatrix}}$$

Die Spalten von $M_{\mathcal{B}}^{\mathcal{B}'}(id_V)$ sind die Koeffizientenvektoren der v_j', $1 \leq j \leq n$, bzgl. $\mathcal{B}$.

2.4.11 Bemerkung

Bezeichnungen wie in 2.4.10. Dann gilt:

a) $M_{\mathcal{B}}^{\mathcal{B}'}(id_V)$ ist invertierbar und $M_{\mathcal{B}}^{\mathcal{B}'}(id_V)^{-1} = M_{\mathcal{B}'}^{\mathcal{B}}(id_V)$

b) Ist $T \in GL_n(K)$, dann existiert eine Basis $\mathcal{B}''$ von V mit $M_{\mathcal{B}}^{\mathcal{B}''}(id_V) = T$

Beweis

a) Folgt aus 2.4.9.

b) Sei $T = (t_{ij})_{1\leq i,j\leq n}$.
Für $1 \leq j \leq n$ sei $v_j'' := \sum_{i=1}^{n} t_{ij}v_j$.
Sei $\mathcal{B}'' := (v_1'', ..., v_n'')$, dann gilt: $\mathcal{B}''$ ist Basis von V, da T invertierbar.
Klar: $M_{\mathcal{B}}^{\mathcal{B}''}(id_V) = T$.

2.4.12 Basiswechselsatz

Bezeichnungen wie in 2.4.10, dann gilt:

$$\begin{aligned} M_{\mathcal{C}'}^{\mathcal{B}'}(\varphi) &= M_{\mathcal{C}'}^{\mathcal{C}}(id_W)M_{\mathcal{C}}^{\mathcal{B}}(\varphi)M_{\mathcal{B}}^{\mathcal{B}'}(id_V) \\ &= M_{\mathcal{C}}^{\mathcal{C}'}(id_W)^{-1}M_{\mathcal{C}}^{\mathcal{B}}(\varphi)M_{\mathcal{B}}^{\mathcal{B}'}(id_V) \end{aligned}$$

$$\begin{tikzcd} \overset{\mathcal{B}}{V} \arrow[r, bend left, "\varphi"] & \overset{\mathcal{C}}{W} \arrow[d, bend left, "id_W"] \\ \underset{\mathcal{B}'}{V} \arrow[u, bend left, "id_V"] \arrow[r, bend left, "\varphi"] & \underset{\mathcal{C}'}{W} \end{tikzcd}$$

Abbildung 2.1: Basiswechselsatz

Beweis

Betrachte das Abbildungsdiagramm 2.1: Aus $\varphi = id_W \circ \varphi \circ id_V$ folgt die Behauptung mit 2.4.7 und 2.4.11 a).

2.4.13 Korollar (Basiswechselsatz für Endomorphismen)

Sei V K-VR mit Basen $\mathcal{B}$ und $\mathcal{B}'$ und sei $\varphi \in \mathrm{End}_K(V) = \mathrm{Hom}_K(V,V)$
Setze $A := M^{\mathcal{B}}_{\mathcal{B}}(\varphi)$, $A' := M^{\mathcal{B}'}_{\mathcal{B}'}(\varphi)$, $T = M^{\mathcal{B}'}_{\mathcal{B}}(id_V)$, dann gilt:

$$A' = T^{-1}AT$$

Beweis

Siehe 2.4.12.

2.4.14 Beispiel

$V = W = \mathbb{R}^2 \qquad \varphi = \varphi_A$ mit $A = \begin{pmatrix} -\frac{3}{5} & \frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix}$

d.h. $\varphi(\begin{pmatrix} a \\ b \end{pmatrix}) = A \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{5}\begin{pmatrix} -3a+4b \\ 4a+3b \end{pmatrix}$, $a, b \in \mathbb{R}$

<u>Gesucht</u>: Einfachere Beschreibung von φ.

$\mathcal{B} = (e_1, e_2)$ mit $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$\mathcal{B}' = (v_1', v_2')$ mit $v_1' = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, $v_2' = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$

$\mathcal{B}$ und $\mathcal{B}'$ sind Basen von V.
$\Rightarrow T := M^{\mathcal{B}'}_{\mathcal{B}}(id_V) = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$

$T^{-1} = \frac{1}{5}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$

$$\begin{aligned} \Rightarrow T^{-1}AT &= \frac{1}{5}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} -\frac{3}{5} & \frac{4}{5} \\ \frac{4}{5} & \frac{3}{5} \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \\ &= \frac{1}{5}\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

$\Rightarrow \varphi(v_1') = v_1',\ \varphi(v_2') = -v_2'$, d.h. φ ist die Spiegelung an der Geraden durch $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

Kapitel 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 (vergl. 2.1.2).

3.1 Das Signum einer Permutation

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

Definition 3.1.1 *Sei $n \geq 2$. $\pi \in S_n$ heißt* ***Transposition*** *(Vertauschung), wenn gilt:*

$$\exists k \neq l \in \underline{n} \textit{ mit } \tau(k) = l,\ \tau(l) = k \textit{ und } \tau(i) = i\ \forall i \neq k, l$$

τ vertauscht also die Ziffern k und l.
Wir schreiben $(k\ \ l)$ für τ, z.B. für $n = 5$:

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

3.1.1 Bemerkung

Ist $\tau \in S_n$ Transposition, dann ist $\tau \neq 1 (= id_{\underline{n}})$ und $\tau^2 = 1$.

3.1.2 Satz

a) Sei $\tau \in S_n$ Transposition $\Rightarrow \tau$ ist Produkt einer ungeraden Anzahl von Tranpositionen benachbarter Ziffern (d.h. von der Form $(i \;\; i+1)$)

b) Sei $\pi \in S_n,\ \pi \neq 1 \Rightarrow \pi$ ist Produkt von Transpositionen benachbarter Ziffern.

Beweis

a) Sei $\tau = (k \;\; l)$ mit $1 \leq k < l \leq n$.
Induktion über $l-k$:
$\underline{l-k=1}$: gilt.
$\underline{l-k>1}$: $(k \;\; l) = (l-1 \;\; l)(k \;\; l-1)(l-1 \;\; l)$
$(k \;\; l-1)$ erfüllt die Behauptung nach Induktion.
$(k \;\; l)$ erfüllt die Behauptung.

b) Wegen a) genügt es zu zeigen: π ist Produkt von Transpositionen (*). Beweis von (*) durch Induktion über n:
$\underline{n=2}$ $\quad (1 \;\; 2) = (1 \;\; 2),\ 1 = (1 \;\; 2)(1 \;\; 2)$
$\underline{n \to n+1}$: Sei $\pi \in S_{n+1}$
<u>1. Fall</u>: $\pi(n+1) = n+1$
Definiere $\pi' \in S_n$ durch $\pi'(i) = \pi(i)$ für $1 \leq i \leq n$.
$\overset{\text{Induktion}}{\Longrightarrow} \pi'$ ist Produkt von Transpositionen aus S_n.
$\Rightarrow \pi$ ist Produkt der entsprechenden Transpositionen aus S_{n+1}.
<u>2. Fall</u>: $\pi(k) = n+1$ für ein k mit $1 \leq k \leq n$
Sei $\pi' := \pi \cdot (k \;\; n+1) \in S_{n+1}$
$\Rightarrow \pi'(n+1) = n+1$
$\overset{\text{1. Fall}}{\Rightarrow} \pi = \pi'(k \;\; n+1)$ ist Produkt von Transpositionen.
Die Darstellung von $\pi \in S_n$ als Produkt von Transpostionen ist i.A. <u>nicht eindeutig</u>.

$$(1 \;\; 2)(2 \;\; 3) = (4 \;\; 5)(1 \;\; 2)(2 \;\; 3)(4 \;\; 5) \text{ in } S_5$$

Definition 3.1.2 *Sei $\pi \in S_n$*

a) Ein Paar $(i,j),\ 1 \leq i < j \leq n$ heißt ***<u>Fehlstandspaar</u>*** *(FSP), wenn gilt: $\pi(i) > \pi(j)$.*

b) $\operatorname{sgn}(\pi) := (-1)^{|\{FSP\ von\ \pi\}|} \in \mathbb{Z}$ heißt das ***<u>Signum von π</u>****.*

3.1.3 Beispiele

a) $\pi = 1$ hat keine FSP's $\Rightarrow \operatorname{sgn}(1) = 1$

b) $\tau(i \;\; i+1)$ (mit $i < n$) hat genau ein FSP, nämlich $(i, i+1) \Rightarrow \operatorname{sgn}(\tau) = -1$

3.1.4 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 Gruppenhomomorphismus)

Beweis

1. Fall: $n \leq 2$ und $\sigma = (1 \;\; i+1)$
$(i \;\; i+1)$ ist Transposition benachbarter Ziffern. $\overset{3.1.3b)}{\Longrightarrow} \operatorname{sgn}(\sigma) = -1$
$\pi\sigma = \pi \cdot (i \;\; i+1) = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & i+2 & \cdots & n \\ \pi(1) & \cdots & \pi(i-1) & \pi(i+1) & \pi(i) & \pi(i+2) & \cdots & \pi(n) \end{pmatrix}$
Es gilt:

a) $(k, i),\; k > i$ FSP von $\pi \Leftrightarrow (k, i+1)$ ist FSP von $\pi\sigma$

b) $(i, k),\; k > i+1$ FSP von $\pi \Leftrightarrow (i+1, k)$ ist FSP von $\pi\sigma$

c) Analog zu a), b) für $i+1$ statt i.

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 $\pi\sigma$.

$\overset{a)-e)}{\Longrightarrow} |\{\text{FSP von } \pi\}| = |\{\text{FSP von } \pi\sigma\}| \pm 1 \Rightarrow \operatorname{sgn}(\pi\sigma) = -\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$

2. Fall: Schreibe $\sigma = \tau_1 \cdots \tau_l$, wobei τ_i für $1 \leq i \leq l$ Transposition benachbarter Ziffer ist (nach 3.1.2 b)).
Induktion über l:
$l = 1$: Gilt nach 1. Fall.
$l-1 \to l$: Setze $\sigma' := \tau_1 \cdots \tau_{l-1}$

$$\begin{aligned} \Rightarrow \operatorname{sgn}(\pi\sigma) &= \operatorname{sgn}((\pi\sigma')\tau_l) \\ &= \operatorname{sgn}(\pi\sigma')\operatorname{sgn}(\tau_l) && \text{(1. Fall)} \\ &= \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma')\operatorname{sgn}(\tau_l) && \text{(Induktion)} \\ &= \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma'\tau_l) && \text{(1. Fall)} \\ &= \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma) \end{aligned}$$

3.1.5 Korollar

Sei $\tau \in S_n$ Transposition $\Rightarrow \operatorname{sgn}(\tau) = -1$.

Beweis

3.1.2a), 3.1.3b), 3.1.4

3.2 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 $s_1, ..., s_n$ von A auf, d.h. wir schreiben $A = (s_1, ..., s_n)$ mit $s_i \in R^n$)

Definition 3.2.1 *Eine Abbildung $D : R^{n\times n} \to R$ heißt* ***<u>Determinante</u>****, wenn gilt:*

1.) D ist ***<u>multi-linear</u>****, d.h. $D(s_1, ..., s_{j-1}, as_j + bs'_j, s_{j+1}, ..., s_n) =$
$aD(s_1, ..., s_{j-1}, s_j, s_{j+1}, ..., s_n) + bD(s_1, ..., s_{j-1}, s'_j, s_{j+1}, ..., s_n)$
für alle $1 \le j \le n$ und für alle $a, b \in R$, $s_1, ..., s_n, s'_j \in R^n$.*

2.) D ist ***<u>alternierend</u>****, d.h. $D(s_1, ..., s_n) = 0$, falls $s_i = s_j$ für zwei $i \neq j$.*

3.) D ist ***<u>normiert</u>****, d.h. $D(e_1, ..., e_n) = 1$ mit $E_n = (e_1, ..., e_n)$.*

3.2.1 Beispiel

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

3.2.2 Lemma

Sei $D : R^{n\times n} \to R$ eine Determinante und sei $\pi \in S_n$. Dann gilt für alle $s_1, ..., s_n \in R^n$: $D(s_{\pi(1)}, s_{\pi(2)}, ..., s_{\pi(n)}) = \mathrm{sgn}(\pi) D(s_1, ..., s_n)$.
Insbesondere ist $D(s_{\pi(1)}, ..., s_{\pi(n)}) = -D(s_1, ..., s_n)$ falls π Transposition ist.

Beweis

$\pi = 1$ klar.

Sei $\pi = \tau_1 \cdots \tau_l$ mit Transpositionen τ_i, $1 \le i \le l$

Induktion über l:

<u>$l = 1$</u>: $\pi = \tau_1 = (i\ \ j)$ mit $1 \le i < j \le n$

$$
\begin{aligned}
0 &\overset{3.2.1\ 2.)}{=} D(s_1, ..., \underbrace{s_i + s_j}_{i}, ..., \underbrace{s_i + s_j}_{j}, ..., s_n) \\
&\overset{3.2.1\ 1.)}{=} D(s_1, ..., s_i, ..., s_j, ..., s_n) + \underbrace{D(s_1, ..., s_i, ..., s_i, ..., s_n)}_{0} \\
&+ \underbrace{D(s_1, ..., s_j, ..., s_i, ..., s_n)}_{D(s_{\pi(1)}, ..., s_{\pi(i)}, ..., s_{\pi(j)}, ..., s_{\pi(n)})} + \underbrace{D(s_1, ..., s_j, ..., s_j, ..., s_n)}_{0}
\end{aligned}
$$

$\Rightarrow D(s_{\pi(1)}, ..., s_{\pi(i)}, ..., s_{\pi(j)}, ..., s_{\pi(n)}) = -D(s_1, ..., s_n)$
$\underline{l > 1}$, $l - 1 \mapsto l$
Sei $\pi' = \tau_2 \cdots \tau_l$, d.h. $\pi = \tau_1 \cdot \pi'$

$$
\begin{aligned}
& D(s_{\tau_1(\pi'(1))}, ..., s_{\tau_1(\pi'(n))}) \\
\overset{\text{Fall } n=1}{=} & -D(s_{\pi'(1)}, ..., s_{\pi'(n)}) \\
\overset{\text{Induktion}}{=} & -\operatorname{sgn}(\pi') D(s_1, ..., s_n) \\
= \ & \operatorname{sgn}(\tau_1 \pi') \cdot D(s_1, ..., s_n)
\end{aligned}
$$

3.2.3 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

$$D(s_1, ..., s_n) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \cdots a_{\pi(n),n} \qquad (*)$$

(n! Summanden, jeder davon mit n Faktoren (mal Vorzeichen))

b) Sei $r \in R$ und $D_r : R^{n \times n} \to R$ eine Abbildung, die 3.2.1 1.) und 2.) erfüllt und $D_r(e_1, ..., e_n) = r \Rightarrow D_r = r \cdot D$ mit D wie in (*).

Beweis

Wir zeigen zuerst b):
Mit $r = 1$ folgt die Eindeutigkeit in a).

$$\begin{aligned}
D_r(s_1, ..., s_n) &= D_r(\sum_{i_1=1}^{n} a_{i_1,1} e_{i_1}, s_2, ..., s_n) \\
&= \sum_{i_1=1}^{n} a_{i_1,1} D_r(e_{i_1}, s_2, ..., s_n) \\
&= \sum_{i_1=1}^{n} a_{i_1,1}, D_r(e_{i_1}, \sum_{i_2=1}^{n} a_{i_2,2} e_{i_2}, s_3, ..., s_n) \\
&= \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} a_{i_1,1} a_{i_2,2} D_r(e_{i_1}, e_{i_2}, s_3, ..., s_n) \\
&= ... \\
&= \sum_{i_1=1}^{n} \sum_{i_2=1}^{n} ... \sum_{i_n=1}^{n} a_{i_1,1} a_{i_2,2} ... a_{i_n,n} D_r(e_{i_1}, e_{i_2}, ..., e_{i_n}) \qquad (**)
\end{aligned}$$

$D_r(e_{i_1}, ..., e_{i_n}) \neq 0$ nur falls $\{i_1, ..., i_n\} = \{1, ..., n\}$, d.h. falls $\begin{pmatrix} 1 & 2 & ... & n \\ \imath_1 & \imath_2 & ... & i_n \end{pmatrix} := \pi \in S_n$ ist.

In diesem Fall ist $D_r(e_{i_1}, ..., e_n) = D_r(e_{\pi(1)}, ..., e_{\pi(n)}) = \mathrm{sgn}(\pi)(e_1, ..., e_n) = \mathrm{sgn}(\pi) \cdot r$
Zu jedem $\pi \in S_n$ existiert genau ein Summand $a_{\pi(1),1} \cdots a_{\pi(n),n} D_r(e_{\pi(1)}, ..., e_{\pi(n)})$ in (**):
$\Rightarrow D_r(s_1, ..., s_n) = \sum\limits_{\pi \in S_n} a_{\pi(1),1} \cdots a_{\pi(n),n} D_r(e_{\pi(1)}, ..., e_{\pi(n)})$
$= \sum\limits_{\pi \in S_n} a_{\pi(1),1} \cdots a_{\pi(n),n} \cdot \mathrm{sgn}(\pi) \cdot r$

a) Existenz: Sei $D : R^{n \times n} \to R$, die durch (*) definierte Abbildung. Zu zeigen: D ist Determinante.
3.2.1 1.): Übung.
3.2.1 2.): Beweis für den Fall $i = 1$, $j = 2$, d.h. $s_1 = s_2$.
Der allgemeine Fall gilt analog. Sei $\tau = (1\ \ 2) \in S_n$
Es gilt: $\pi \in S_n : \quad \pi(1) > \pi(2) \Leftrightarrow \pi\tau(1) < \pi\tau(2)$
Damit ist die Abbildung

$$\{\pi \in S_n \mid \pi(1) > \pi(2)\} \to \{\pi \in S_n \mid \pi(1) < \pi(2)\}, \qquad \pi \mapsto \pi \cdot \tau$$

eine Bijektion.

$$\begin{aligned}
D(s_1, s_2, ..., s_n) &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n} \\
&= \underbrace{\sum_{\pi \in A_2} \operatorname{sgn}(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n}}_{D_2} + \underbrace{\sum_{\pi \in A_1} \operatorname{sgn}(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n}}_{D_1} \\
D_1 &= \sum_{\pi \in A_1} \operatorname{sgn}(\pi) \underbrace{a_{\pi(1),2} a_{\pi(2),1}}_{\text{weil } s_1 = s_2} a_{\pi(3),3} \cdots a_{\pi(n),n} \\
&= \sum_{\pi \in A_1} \operatorname{sgn}(\pi) a_{\pi(1),1} a_{\pi(2),2} \cdots a_{\pi(n),n} \\
&= \sum_{\pi \in A_1} - \operatorname{sgn}(\pi\tau) a_{\pi(1),1} a_{\pi(2),2} \cdots a_{\pi(n),n} \\
&= - \sum_{\pi \in A_1} a_{\pi(1),1} a_{\pi(2),2} \cdots a_{\pi(n),n} \\
&= -D_2
\end{aligned}$$

3.2.1 3.): Klar.

3.2.4 Schreibweise

Sei $A = (a_{ij}) \in R^{n \times n}$. Wir schreiben $\det(A)$ für die nach 3.2.3 eindeutig bestimmte Determinate von A und auch $|A| := \det(A)$, oder auch

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \det(A)$$

3.2.5 Beispiele

a) $n = 2,\ S_2:$

$\pi:$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$
$\operatorname{sgn}(\pi):$	1	-1

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}$$

b) $n = 3,\ S_3$:

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

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

3.2.6 Regel von Sarrus (für (3×3)-Matrizen)

Schreibe die ersten beiden Spalten neben die Matrix, bilde Produkte anhand der Linien, nehme die Vorzeichen nach unterem Schema (Abbildung 3.1):

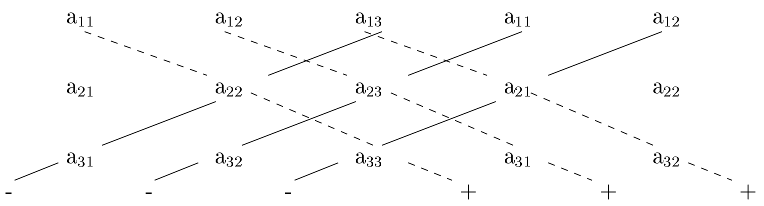

Abbildung 3.1: Sarrus-Regel

$$\begin{vmatrix}1&2&3\\0&1&2\\-1&0&5\end{vmatrix} = -(-3)-0-0+5+(-4)+0=4$$

3.3 Rechenregeln und Anwendungen für Determinanten

R kommutativer Ring, $n\in\mathbb{N}$

3.3.1 Bemerkung

Die Abbildung

$$S_n\to S_n,\qquad \pi\mapsto\pi^{-1}$$

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
$1 = \mathrm{sgn}(1) = \mathrm{sgn}(\pi \cdot \pi^{-1}) = \mathrm{sgn}(\pi) \cdot \mathrm{sgn}(\pi^{-1})$
$\Rightarrow \mathrm{sgn}(\pi) = \mathrm{sgn}(\pi^{-1})$, da $\in \{1, -1\}$

3.3.2 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 $a'_{ij} = a_{ji}$

$$\begin{aligned} \Rightarrow \det(A') &= \sum_{\pi\in S_n} \mathrm{sgn}(\pi)\, \underbrace{a'_{\pi(1),1}\cdots a'_{\pi(n),n}}_{(*)} \\ &= \sum_{\pi^{-1}\in S_n} \mathrm{sgn}(\pi^{-1})\, \underbrace{a'_{\pi^{-1}(1),1}\cdots a'_{\pi^{-1}(n),n}}_{(*)} \\ &\overset{3.3.1}{=} \det(A) \end{aligned}$$

(*): Gleiche Faktoren: $a_{k,l}$ kommt als Faktor in $a_{\pi(1),1}\cdots a_{\pi(n),n}$ vor
$\Leftrightarrow l = \pi(k)$
$\Leftrightarrow \pi^{-1}(l) = k$
$\Leftrightarrow a_{k,l}$ kommt als Faktor in $a_{\pi^{-1}(1),1}\cdots a_{\pi^{-1}(n),n}$ vor.

3.3.3 Schreibweise

Sei $A = (a_{ij}) \in R^{n\times n},\ n \geq 2$ 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} ensteht aus A durch Streichen der i-ten Zeile und der j-ten Spalte.

3.3.4 Lemma

Sei $A = (s_1, ..., s_n) \in R^{n\times n}$ (also $s_i \in R^n$), und seien $i, j \in \underline{n}$ $(n \geq 2)$.

$$\det(\underbrace{s_1, ..., s_{j-1}, e_i, s_{j+1}, ..., s_n}_{(*)}) = (-1)^{i+j}\det(A_{ij})$$

(*) entsteht aus A durch Ersetzen der j-ten Spalte s_j durch die i-te Spalte e_i von E_n.

Beweis

$(s_1, ..., s_{j-1}, e_i, s_{j+1}, ..., s_n)$ kann durch $n-j$ Spaltentransformationen und $n-i$ Zeilentransformationen in die Matrix

$$B = \begin{pmatrix} & & & 0 \\ & A_{ij} & & \vdots \\ & & & 0 \\ * & \cdots & * & 1 \end{pmatrix}$$

übergeführt werden.

$$\overset{3.2.2}{\Longrightarrow} \det(s_1, ..., s_{j-1}, e_i, s_{j+1}, ..., s_n) = (-1)^{n-j+n-i} \det(B) = (-1)^{i+j} \det(B)$$

Sei $B = (b_{kl})_{1 \le k,l \le n}$. Für $\pi \in S_n$ ist $b_{\pi(n),n} = 0$ außer für $\pi(n) = n$.

$$b_{n,n} = 1$$

$$\begin{aligned} \Rightarrow \det(B) &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) b_{\pi(1),1} \cdots b_{\pi(n-1),n-1} b_{\pi(n),n} \\ &= \sum_{\substack{\pi \in S_n \\ \pi(n)=n}} \operatorname{sgn}(\pi) b_{\pi(1),1} \cdots b_{\pi(n-1),n-1} \\ &= \sum_{\pi \in S_{n-1}} \operatorname{sgn}(\pi) b_{\pi(1),1} \cdots b_{\pi(n-1),n-1} \\ &= \det(A_{ij}) \end{aligned}$$

3.3.5 Satz (Laplace Entwicklung)

Sei $A = (a_{ij}) \in R^{n \times n}$, dann gilt:

a) Entwicklung nach der j-ten Spalte ($1 \le j \le n$):

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij})$$

b) Entwicklung nach der i-ten Zeile ($1 \le i \le n$):

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij})$$

Beweis

b) Folgt aus a) durch Transponieren.

a) Sei $A = (s_1, ..., s_n), \qquad s_i \in R^n$

$$\begin{aligned}
\Rightarrow \det(A) &= \det(s_1, ..., s_{j-1}, \sum_{i=1}^{n} a_{ij} e_i, s_{j+1}, ..., s_n) \\
&= \sum_{i=1}^{n} a_{ij} \det(s_1, ..., s_{j-1}, e_i, s_{j+1}, ..., s_n) \\
&\overset{3.3.4}{=} \sum_{i=1}^{n} a_ij (-1)^{i+j} \det(A_{ij})
\end{aligned}$$

3.3.6 Beispiel

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ -1 & -1 & 0 & 1 \\ 4 & 0 & 3 & -1 \\ 2 & 0 & -1 & 1 \end{vmatrix} = -2 \begin{vmatrix} -1 & 0 & 1 \\ 4 & 3 & -1 \\ 2 & -1 & 1 \end{vmatrix} + (-1) \begin{vmatrix} 1 & 3 & 4 \\ 4 & 3 & -1 \\ 2 & -1 & 1 \end{vmatrix}$$

$$= -2 \left((-1 \begin{vmatrix} 3 & -1 \\ -1 & 1 \end{vmatrix} + 1 \begin{vmatrix} 4 & 3 \\ 2 & -1 \end{vmatrix} \right) + (-1) \left(1 \begin{vmatrix} 3 & -1 \\ -1 & 1 \end{vmatrix} - 3 \begin{vmatrix} 4 & -1 \\ 2 & 1 \end{vmatrix} + 4 \begin{vmatrix} 4 & 3 \\ 2 & -1 \end{vmatrix} \right)$$

$$= \begin{vmatrix} 3 & -1 \\ -1 & 1 \end{vmatrix} - 6 \begin{vmatrix} 4 & 3 \\ 2 & -1 \end{vmatrix} + 3 \begin{vmatrix} 4 & -1 \\ 2 & 1 \end{vmatrix}$$

$= 2 + 60 + 18 = 80$

3.3.7 Korollar

Sei $A = R^{n \times n}$ eine **obere Dreiecksmatrix**, d.h.

$$A = \begin{pmatrix} a_{11} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$$

Dann ist $\det(A) = \prod_{i=1}^{n} a_{ii}$.

Beweis

Induktion:

$n = 1$: gilt.

$\underline{n-1 \mapsto n}$: Entwickle $\det(A)$ gemäß 3.3.5 a) nach der 1. Spalte:

$$\det(A) = a_{11} \begin{vmatrix} a_{22} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{vmatrix} \overset{\text{Induktion}}{=} a_{11} \prod_{i=2}^{n} a_{ii}$$

3.3.8 Satz (Kästchensatz für Determinanten)

Seien $A_i \in R^{n_i \times n_i}$, $1 \leq i \leq n$, dann gilt:

$$\det \begin{pmatrix} A_1 & & & * \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_m \end{pmatrix} = \prod_{i=1}^{m} \det(A_i)$$

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 3.3.5 a). $\left(\begin{array}{c|ccc} \square & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right)$

$\underline{n > 1}$: Sei $C = \left(\begin{array}{c|c} A & * \\ \hline 0 & B \end{array}\right) \Rightarrow C_{i1} = \left(\begin{array}{c|c} A_{i1} & * \\ \hline 0 & B \end{array}\right)$, $1 \leq i \leq n$

$$\begin{aligned} \overset{3.3.5\text{ a)}}{\Longrightarrow} \det(C) &= \sum_{i=1}^{n+l} (-1)^{i+1} \underbrace{c_{i1}}_{=0 \text{ für } i>n} \det(c_{ij}) \\ &= \sum_{i=1}^{n} (-1)^{i+1} a_{i1} \det(\left(\begin{array}{c|c} A_{i1} & * \\ \hline 0 & B \end{array}\right) \\ &\overset{\text{Induktion}}{=} \sum_{i=1}^{n} (-1)^{i+1} a_{i1} \det(A_{i1}) \det(B) \\ &\overset{3.3.5\text{ a)}}{=} \det(A) \cdot \det(B) \end{aligned}$$

3.3.9 Satz (Multiplikationssatz für Determinanten)

Sei $A, B \in R^{n\times n}$, dann gilt:

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

Beweis

Sei $a = \det(A) \in R$
Betrachte $D_a : R^{n\times n} \to R,\ C \mapsto \det(A \cdot C)$
Sei $C = (s_1, ..., s_n) \in R^{n\times n}$, d.h. $s_i \in R^n$

$$\begin{array}{cl} \Rightarrow & AC = (As_1, ..., As_n) \\ \Rightarrow & D_a \text{ erfüllt die Bedingungen aus 3.2.1 1), 2) und es gilt: } D_a(E_n) = \det(A) = a \\ \overset{3.2.3\text{ b)}}{\Longrightarrow} & D_a = a \cdot \det \\ \Rightarrow & \det(A \cdot B) = a \cdot \det(B) = \det(A) \cdot \det(B) \end{array}$$

3.3.10 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) $\det(T^{-1}AT) = \det(A)$

Beweis

b) folgt aus a) und 3.3.9.

a)

$$\begin{aligned} 1 &= \det(E_n) \\ &= \det(T^{-1} \cdot T) \\ &= \det(T^{-1}) \det(T) \end{aligned}$$

$\Rightarrow \det(T),\ \det(T^{-1})$ sind invertierbar (in R) und $\det(T^{-1}) = \det(T)^{-1}$.

Definition 3.3.1 *Sei $A \in R^{n\times n}$*

$$\tilde{A} := \left((-1)^{i+j} \det(A_{ji})\right)_{1\le i,j\le n} \in R^{n\times n}$$

heißt die zu A ***komplementäre Matrix*** *(oder* ***Adjunkte*** *von A).*
(A_{ji} ist wie in 3.3.3 definiert; Beachte die vertauschten Indizes.)

3.3.11 Beispiel

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \tilde{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$A \cdot \tilde{A} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = \det(A) \cdot E_2$

3.3.12 Satz

Sei $A \in R^{n \times n}$. Dann gilt:

$$A\tilde{A} = \det(A) \cdot E_n = \tilde{A}A$$

Beweis

Nur für $A \cdot \tilde{A}$. Der Beweis für $\tilde{A} \cdot A$ geht analog. Sei $A = (A_{ij}),\ \tilde{A} = (\tilde{a}_{ij}),\ A\tilde{A} = (c_{ij})$

$$c_{ij} = \sum_{k=1}^{n} A_{ik}\tilde{a}_{kj} = \sum_{k=1}^{n} a_{ik}(-1)^{k+j}\det(A_{jk})$$

<u>1. Fall</u>: $i = j$

$\Rightarrow c_{ii} = \sum\limits_{k=1}^{n} a_{ik}(-1)^{k+j}\det(A_{jk}) \overset{3.3.5\text{ b)}}{=} \det(A)$

<u>2. Fall</u>: $i \neq j$

Sei $A' = (a'_{kl})$ die Matrix, die aus A ensteht, indem man die j-te Zeile durch die i-te ersetzt wird.

$\Rightarrow \det(A') = 0 \qquad$ (3.2.1 a) und 3.3.2)

Aus 3.3.5 b) (Entwicklung nach der j-ten Zeile) folgt:

$$\begin{aligned} 0 &= \det(A') \\ &= \sum_{k=1}^{n} (-1)^{j+k} a'_{jk}\det(A'_{jk}) \\ &= \sum_{k=1}^{n} (-1)^{j+k} a_{jk}\det(A_{jk}) \\ &= c_{ij} \end{aligned}$$

3.3.13 Korollar

Sei $A \in R^{n \times n}$. Dann gilt:

a) A invertierbar $\Leftrightarrow \det(A)$ invertierbar

b) Ist R Körper, dann gilt:

$$A \text{ invertierbar } \Leftrightarrow \det(A) \neq 0$$

Beweis

b) folgt aus a)

a) „$\Rightarrow$“ 3.3.10 a)
„$\Leftarrow$“ Aus 3.3.12 folgt: $A(\det(A)^{-1}\tilde{A}) = E_n = (\det(A)^{-1}\tilde{A}) \cdot A$

3.3.14 Satz (Cramersche Regel)

Sei K ein Körper, $A = (a_{ij}) \in K^{n\times n}$ mit $\det(A) \neq 0$. Nach 3.3.13 b) ist A invertierbar.

Sei $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in K^n$

Nach 2.3.24 5.) hat das LGS $Ax = b$ genau eine Lösung $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$. Hierfür gilt:

$$c_j = \frac{1}{\det(A)} \begin{vmatrix} a_{1,1} & \cdots & a_{1,j-1} & b_1 & a_{1,j+1} & \cdots & a_{1,n} \\ a_{2,1} & \cdots & a_{2,j-1} & b_2 & a_{2,j+1} & \cdots & a_{2,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j-1} & b_n & a_{n,j+1} & \cdots & a_{nin} \end{vmatrix}$$

(Ersetze j-te Spalte von A durch b)

Beweis

Seien $s_1, ..., s_n$ die Spalten von A. Es ist

$$b = A \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \sum_{i=1}^{n} c_i s_i$$

$$\begin{aligned} &\overset{3.2.1\ 1)}{\Longrightarrow} && \det(s_1, ..., s_{j-1}, b, s_{j+1}, ..., s_n) \\ &= && \sum_{i=1}^{n} c_i \underbrace{\det(s_1, ..., s_{j-1}, s_i, s_j + 1, ..., s_n)}_{=0 \text{ außer für } i=j} \\ &= && c_j \det(A) \end{aligned}$$

Kapitel 4

Eigenwerte und Eigenvektoren

4.1 Polynomring

K Körper
$\sum\limits_{i=0}^{m} a_i X^i$ „formale" Potenzreihe, X : Unbestimmte

Definition 4.1.1 *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.) $a(v \cdot v') = (av) \cdot v' = v \cdot (av') \qquad \forall a \in K,\ v, v' \in V$

b) Seien V, W K-Algebra. Ein Homo- (Epi-, Mono-, Iso-) morphismus

$$\varphi : V \to W$$

heißt K-Algebra-Homo- (Epi-, Mono-, Iso-) morphismus, falls gilt:

$$\varphi(1) = 1,\ \varphi(v \cdot v') = \varphi(v) \cdot \varphi(v') \qquad \forall v, v' \in V$$

4.1.1 Beispiel

$K^{n \times n}$ ist K-Algebra (mit Matrixmultiplikation).

Definition 4.1.2 *Ein Paar (P, X) heißt* ***Polynomring*** *in der Unbestimmten X über K, falls gilt:*

a) P ist K-Algebra.

b) $\{1 =: X^0, X = X^1, X^2 = X \cdot X, X^3, ...\}$ ist K-Basis von P und unendlich.

4.1.2 Bemerkung

Sei (P, X) Polynomring über K.

a) Jedes $f \in P$ besitzt eine eindeutige Darstellung als LK

$$f = \sum_{i=0}^{n} a_i X^i \text{ mit } a_i \in K, a_n \neq 0$$

b) Seien $f = \sum\limits_{i=0}^{m} a_i X^i,\ g = \sum\limits_{i=0}^{n} b_i X^i \in P$,

dann ist $f \cdot g = \sum\limits_{k=0}^{m+n} c_k X^k$ mit $c_k = \sum\limits_{l=0}^{k} a_l b_{k-l}$.

Beweis

a) Folgt aus 4.1.2 b).

b) Distributivgesetz in einem Ring, zusammen mit 4.1.1 a) 2.).

4.1.3 Bemerkung

Bis auf K-Algebra-Isomorphismus existiert genau ein Polynomring über K in der Unbestimmten X. Dieser wird mit $K[X]$ bezeichnet.

4.1.4 Beweis

1.) Existenz (vergl. Aufg. 6 Blatt 7)

$$K^{(\mathbb{N}_0)} := \{f : \mathbb{N}_0 \to K \mid f(i) = 0 \text{ für fast alle } i \in \mathbb{N}_0\}$$

$$([f(0), f(1), ..., f(n)] \text{ falls } f(i) = 0\ \forall i > n)$$

$K^{(\mathbb{N}_0)}$ ist K-VR.

$$* : K^{(\mathbb{N}_0)} \times K^{(\mathbb{N}_0)} \to K^{(\mathbb{N}_0)}$$

sei definiert durch:

$$f * g(k) := \sum_{l=0}^{k} f(l) g(k-l),\ k \in \mathbb{N}_0$$

$X := [0, 1, 0, ...] \in K^{(\mathbb{N}_0)} \Rightarrow (K^{(\mathbb{N}_0)}, X)$ 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-Algebrenisomorphismus.

Definition 4.1.3 *Sei* $f = \sum\limits_{i=0}^{m} a_i X^i \in K[X],\ f \neq 0,\ a_m \neq 0.$

$$\deg(f) := m \textit{ heißt der } \underline{\boldsymbol{Grad\ von\ f}}$$

a_m, a_0 *heißen höchster bzw. konstanter Koeffizient von* f.
f ***normiert***, *falls* $a_m = 1$
f ***konstant***, *falls* $f = a_0 \cdot 1$, *d.h.* $\deg(f) = 0$
f ***linear***, *falls* $\deg(f) = 1$
Konvention: Das Nullpolynom heißt auch konstant! $f = 0$ *hat keinen Grad.*

4.1.5 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 gilt: $fg \neq 0$

Beweis

a) Klar.

b) Seien a_m bzw. b_n die höchste Koeffizienten von f bzw. g, dann ist $a_m b_n$ 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.

4.1.6 Bemerkung

$K[X]^* = K^* = \{a \in K \mid a \neq 0\}$

Beweis

Sei $f \in K[X]^*$, d.h. es existiert $g \in K[X]$ mit $f \cdot g = 1$
$\overset{4.1.5\ b)}{\Longrightarrow} 0 = \deg(f \cdot g) = \deg(f) + \deg(g) \Rightarrow \deg(f) = 0$, d.h. $f \in K^*$.

4.1.7 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

$$f = q \cdot g + r$$

mit $r = 0$ oder $\deg(r) < \deg(g)$.

Beweis (algorithmisch)

<u>Existenz</u>:
$f = 0$: 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 $f_1 := f - \frac{a_m}{b_n} X^{m-n} g$
$\Rightarrow f_1 = 0$ oder $\deg(f_1) < m$
$\overset{\text{Induktion}}{\Longrightarrow}$ es existieren $q_1, r \in K[X]$ mit $f_1 = q_1 \cdot g + r$ und $r = 0$ oder $\deg(r) < \deg(g)$
$\Rightarrow q := q_1 + \frac{a_m}{b_n} X^{m-n}$ und r erfüllen das Gewünschte.

<u>Eindeutigkeit</u>:
Sei $qg + r = f = q' \cdot g + r'$ mit $q, q', r, r \in K[X]$ und $r, r' = 0$ oder $\deg(r) < \deg(g), \deg(r') < \deg(g')$.
$\Rightarrow (q - q') \cdot g = r' - r$
Angenommen $q \neq q'$ (d.h. $q - q' \neq 0$):
$\Rightarrow r - r' \neq 0$ und es gilt:
$\deg(q - q') + \deg(g) = \deg((q - q')g) = \deg(r - r') < \deg(g)$
Widerspruch! $\Rightarrow q - q' = 0,\ r - r' = 0$

Definition 4.1.4 *Seien $f, g \in K[X]$.*

*a) g **<u>teilt</u>** f, geschrieben $g|f$ falls $h \in K[X]$ existiert mit $f = g \cdot h$.*

*b) Seien $f, g \neq 0$. f, g heißen **<u>teilerfremd</u>**, falls gilt: Ist $h \in K[X]$ mit $h|f$ und $h|g$, dann ist $h \in K$.*

*c) f heißt **<u>irreduzibel</u>**, falls gilt $f \neq 0$, $\deg(f) \geq 1$ und ist $f = gh$ mit $g, h \in K[X]$, dann ist $\deg(g) = 0$ oder $\deg(h) = 0$.*

4.1.8 Satz

Seien $0 \neq f, g \in K[X]$. Dann gilt:

$$f, g \text{ teilerfremd} \Leftrightarrow \text{ es ex. } h, k \in K[X] \text{ mit } 1 = f \cdot h + g \cdot k$$

Beweis

„$\Leftarrow$“ Sei $d \in K[X]$ mit $d|f$ und $d|g$
$\Rightarrow d|fh + gk = 1$, d.h. $d \in K$ (4.1.5)

„$\Rightarrow$“ Sei $I := \{fh + gk \mid h, k \in K[X]\}$ und sei $0 \neq d \in I$ von minimalen Grad ($I \neq \{0\}$).
Behauptung: $d|y \; \forall y \in I$
Beweis: Sei $y \in I$. Nach 4.1.7 existieren $q, r \in K[X]$ mit $y = q \cdot d + r$ mit $r = 0$ oder $\deg(r) < \deg(d)$
$y, d \in I \Rightarrow y - q \cdot d = r \in I \Rightarrow d|y$ (nach Wahl von d) $\Rightarrow r = 0$
$f, g \in I \overset{\text{Beh.}}{\Longrightarrow} d|f$ und $d|g$
$\overset{\text{4.1.4 b)}}{\Longrightarrow} d \in K\backslash\{0\} \Rightarrow 1 = d^{-1} \cdot d \in I$

4.1.9 Korollar

Sei $p \in K[X]$ irreduzibel $f, g \in K[X]$ mit $p|fg \Rightarrow p|f$ oder $p|g$

Beweis

Angenommen $p \not| f$
$\Rightarrow p, f$ teilerfremd (4.1.4 b), 4.1.4 c))
$\overset{4.1.8}{\Longrightarrow}$ es existieren $h, k \in K[X]$ mit $1 = fh + pk$
$\Rightarrow g = g \cdot 1 = (fg)h + p(gk)$

$$p|(fg)h, \; p|p(gk) \Rightarrow p|g$$

$\rightsquigarrow$ Eindeutige „Primfaktorzerlegung“ in $K[X]$.

4.1.10 Satz

Sei $0 \neq f \in K[X]$, $\deg(f) \neq 0$ mit höchstem Koeffizienten $a \in K$. Dann existieren irreduzible, normierte $p_1, ..., p_t \in K[X]$ mit $f = a \cdot p_1 \cdots p_t$.
Die $p_1, ..., p_t$ sind eindeutig (bis auf die Reihenfolge) durch f bestimmt.

Beweis

Existenz: Induktion über $\deg(f)$.
f irreduzibel $\Leftrightarrow a^{-1}f$ 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 $p_1, ..., p_t$ und $q_1, ..., q_s \in K[X]$ irreduzibel, normiert mit

$p_1 \cdots p_t = q_1 \cdots q_s$
$\Rightarrow s = t$ und es existiert $\pi \in S_t$ mit

$$q_i = p_{\pi(i)} \qquad 1 \leq i \leq t$$

<u>Beweis</u>: $p_1 \cdots p_t = q_1 \cdots q_s \Rightarrow p_1 | q_1(q_2 \cdots q_s)$
$\overset{\text{4.1.9 und Induktion über } s}{\Longrightarrow} \exists j, 1 \leq j \leq s$ mit $p_1 | q_j$
$\Rightarrow p_1 = q_j$ (da p_1, q_j irreduzibel normiert)
$\Rightarrow p_1 \cdot (p_2 \cdots p_t - q_1 \cdots q_{j-1} \cdot q_{j+1} \cdots q_s) = 0$
$\overset{\text{4.1.5 b)}}{\Longrightarrow} p_2 \cdots p_t = q_1 \cdots q_{j-1} \cdot q_{j+1} \cdots q_s$
$\Rightarrow$ Behauptung (Induktion über s)

4.1.11 Bemerkung und Definition

Sei V K-Algebra, $v \in V$, dann existiert genau ein K-Algebren-Homomorphismus

$$\tau_v : K[X] \to V \text{ mit } \tau_v(X) = v$$

τ_v heißt <u>**Einsetzungshomomorphismus**</u>.
Für $f \in K[X]$ schreiben wir $f(v) := \tau_v(f)$.

Beweis

<u>Eindeutigkeit</u>: Ist $\tau_v : K[X] \to V$ ein K-Algebren-Homomorphismus mit $\tau_v(X) = v$, dann gilt für $f = \sum\limits_{i=0}^{m} a_i X^i \in K[X]$:

$$\tau_v(f) \overset{\tau_v\ K\text{-linear}}{=} \sum_{i=0}^{m} a_i \underbrace{\tau_v(X^i)}_{\tau_v(X)^i} = \sum_{i=0}^{m} a_i v^i$$

<u>Beachte</u>: $v^0 = \tau_v(X^0) = \tau_v(1) = 1 \in V$.
$X^0 = 1 \in K[X]$ per Konvention

<u>Existenz</u>: Für $f = \sum\limits_{i=0}^{m} a_i X^i \in K[X]$ definiere

$$\tau_v(f) := \sum_{i=0}^{m} a_i v^i \qquad (\text{mit } v^0 := 1 \in V)$$

$\Rightarrow \tau_v \in Hom_K(K[X], V)$ und $\tau_v(f \cdot g) = \tau_v(f) \cdot \tau_v(g)$

4.1.12 Beispiel

$f = \sum_{i=0}^{m} a_i X^i$

a) $V = K \quad (\cong K^{1\times 1}),\ a \in K$
$f(a) = \sum_{i=0}^{m} a_i a^i \qquad (a^0 = 1 \in K)$

b) $V = K^{n\times n},\ A \in K^{n\times n}$
$f(A) = \sum_{i=0}^{m} a_i A^i \in K^{n\times n} \qquad (A^0 = E_n)$
$f = x^2 + x + 1 \Rightarrow f(A) = A^2 + A + E_n$

Definition 4.1.5 *Sei $f \in K[X]$, $a \in K$. a heißt* **Nullstelle von** f, *falls $f(a) = 0$.*

4.1.13 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 $\deg(r) < \deg(X - a) = 1$
$\Rightarrow r \in K \Rightarrow 0 = f(a) = (a - a)q(a) + r(a) = 0 \cdot q(a) + r$

4.1.14 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 $g \in K[X]$ mit $f = (X - a)^m g$ und $g(a) \neq 0$.
m heißt die **Vielfachheit von a als Nullstelle**.

Beweis

Existenz und Eindeutigkeit folgen aus 4.1.10 und 4.1.13, denn $X - a$ ist irreduzibel.

Definition 4.1.6 *K heißt* **algebraisch abgeschlossen**, *falls jedes $f \in K[X]$, $f \notin K$, eine Nullstelle in K hat.*

4.1.15 Satz

$\mathbb{C}$ ist algebraisch abgeschlossen (hier ohne Beweis; **Fundamentalsatz der Algebra**).

4.1.16 Bemerkung

Sei K algebraisch abgeschlossen, und $f \in K[X]$ irreduzibel, normiert
$\Rightarrow f = X - a$ für ein $a \in K$

Beweis

f irreduzibel $\Rightarrow \deg(f) \geq 1 \overset{\text{Def. 4.1.6}}{\Longrightarrow}$ es existiert $a \in K$ mit $f(a) = 0$
$\overset{4.1.13}{\Longrightarrow} X - a | f \overset{f \text{ irred., norm.}}{\Longrightarrow} f = X - a$

4.2 Eigenwerte und Vektoren

K Körper, V e.d. K-VR. ($End_K(V) = Hom_K(V, V)$)

Definition 4.2.1 *Sei $\varphi \in End_K(V)$, $A \in K^{n \times n}$.*

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*

$$\varphi(v) = av \text{ (bzw. } Av = av\text{)}.$$

[Erinnerung: $\varphi_A : K^n \to K^n,\ v \mapsto Av$]

2.) $0 \neq v \in V$ (bzw. $0 \neq v \in K^n$) heißt ***Eigenvektor (EV) von φ (bzw. von A) zum Eigenwert $a \in K$****, falls*

$$\varphi(v) = av \text{ (bzw. } Av = av\text{)}$$

ist.

3.) Für $a \in K$ sei

$$\begin{aligned} V(a, \varphi) &:= \{v \in V \mid \varphi(v) = av\} \\ &= \{v \in V \mid (a \cdot id_V - \varphi)(v) = 0\} \\ &= Kern(a \cdot id_V - \varphi) \\ V(a, A) &:= \{v \in K^n \mid Av = av\} \\ &= V(a, \varphi_A) \end{aligned}$$

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. von A) zum Eigenwert a****.*

4.2.1 Bemerkung

Bezeichnungen wie in Definition 4.2.1.

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) $V(0,\varphi) = Kern(\varphi)$

$$\begin{aligned} 0 \text{ ist EW von } \varphi &\Leftrightarrow Kern(\varphi) \neq \{0\} \\ &\Leftrightarrow \varphi \text{ ist nicht injektiv} \\ &\overset{V \text{ e.d.}}{\Leftrightarrow} \varphi \text{ ist nicht bijektiv} \end{aligned}$$

<u>Schreibweise</u>: Sei $\mathcal{B}$ (geordnete) Basis von V, $\varphi \in End_K(V)$.

$$M_{\mathcal{B}}(\varphi) := M_{\mathcal{B}}^{\mathcal{B}}(\varphi) \in K^{n\times n}$$

4.2.2 Beispiele

a) $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{R}^2,\ \varphi_A : \mathbb{R}^2 \to \mathbb{R}^2,\ \varphi_A(e_1) = e_2,\ \varphi_A(e_2) = e_1$
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. $e_1 - e_2 \in V(-1, A)$

$$(e_1 - e_2, e_1 + e_2) \text{ ist l.u.}$$

$\Rightarrow \mathcal{B}' = (e_1 - e_2, e_1 + e_2)$ ist Basis von $\mathbb{R}^2$

$$M_{\mathcal{B}'}(\varphi_A) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$V(1, A) = <e_1 + e_2>$ $\qquad V(-1, A) = <e_1 - e_2>$

b) Sei $\dim_K(V) \geq 2,\ \varphi \in End_K(V)$. Es gelte $1 + 1 \neq 0$ in K.
φ heißt <u>**Spiegelung**</u>, 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 $(v_2, ..., v_n)$ eine Basis von $V(1,\varphi)$

$\Rightarrow v_1 \notin <v_2, ..., v_n> = V(1, \varphi)$, d.h. $\mathcal{B} := (v_1, v_2, ..., v_n)$ ist Basis von V.
Es gilt:

$$M_{\mathcal{B}}(\varphi) = \begin{pmatrix} -1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

Wir sagen auch: φ ist **Spiegelung an $V(1, \varphi)$**.

Definition 4.2.2 *$A = (a_{ij}) \in K^{n \times n}$ heißt **Diagonalmatrix**, falls*

$$a_{ij} = 0 \ \forall i \neq j \qquad A = \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix}.$$

Definition 4.2.3 *Sei $\varphi \in End_K(V)$, $A \in K^{n \times n}$.*

*a) φ heißt **diagonalisierbar**, falls eine Basis $\mathcal{B}$ von V existiert, so dass $M_{\mathcal{B}}(\varphi)$ eine Diagonalmatrix ist.*

b) A heißt diagonalisierbar, falls $T \in GL_n(K)$ existiert mit $T^{-1}AT$ eine Diagonalmatrix ist.

4.2.3 Bemerkung

Bezeichnung wie in Definition 4.2.3.

a) φ diagonalisierbar $\Leftrightarrow$ V besitzt Basis aus EV von φ

b) A diagonalisierbar $\Leftrightarrow$ φ_A diagonalisierbar

Beweis

a) „$\Rightarrow$“ Sei $\mathcal{B} := (v_1, ..., v_n)$ Basis von φ, mit $M_{\mathcal{B}}(\varphi) = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$.

$\overset{\text{Def. 2.4.4}}{\Longrightarrow} \varphi(v_j) = a_j v_j$, $1 \leq j \leq n$, d.h. v_j ist EV von φ mit EW a_j

„$\Leftarrow$“ genau so mit Def. 2.4.1

b) Sei $\mathcal{B} = (e_1, ..., e_n)$ die Stardardbasis von K^n.
$\Rightarrow M_{\mathcal{B}}(\varphi_A) = A$ (nach 2.4.4 c))
Ist $\mathcal{B}'$ eine andere Basis von K^n und $T := M_{\mathcal{B}}^{\mathcal{B}'}(id_V)$ die Basiswechselmatrix, dann ist $M_{\mathcal{B}'}(\varphi_A) = T^{-1}AT$ (vgl. 2.4.13)
$\Rightarrow$ Behauptung

Definition 4.2.4 *$A, B \in K^{n\times n}$ heißen* ***ähnlich****, falls*

$$T \in GL_n(K) \text{ existiert mit } B = T^{-1}AT$$

Nach 2.4.13: Ähnliche Matrixzen beschreiben den gleichen Endomorphismus, nur bzgl. verschiedener Basen.
$A \in K^{n\times n}$ diagonalisierbar $\Leftrightarrow$ A ähnlich einer Diagonalmatrix

4.2.4 Satz

Sei $\varphi \in End_K(V)$, $\dim_K(V) = n$.

a) Seien $a_1, ..., a_m \in K$ EW von φ mit $a_i \neq a_j$ für $i \neq j$. Sei $v_j \in V$ EV von φ zum EW a_j, $1 \leq j \leq m$
$\Rightarrow (v_1, ..., v_m)$ l.u.

b) Besitzt φ n paarweise verschiedene EW, dann ist φ diagonalisierbar.

Beweis

b) folgt aus a) mit 4.2.3

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 $\sum\limits_{j=1}^{m} b_j v_j = 0$
Es gilt:

$$\begin{aligned}
0 &= (\varphi - a_m \cdot id_V)(0) \\
&= (\varphi - a_m \cdot id_V)(\sum_{j=1}^{m} b_j v_j) \\
&= \sum_{j=1}^{m} b_j(\varphi - a_m id_V)(v_j) \\
&= \sum_{j=1}^{m} b_j(\varphi(v_j) - a_m \cdot v_j) \\
&= \sum_{j=1}^{m-1} b_j(a_j - a_m)v_j \\
&\overset{\text{Induktion}}{\Longrightarrow} b_j(a_j - a_m) = 0 \text{ für } 1 \leq j \leq m-1 \\
&\Rightarrow a_j - a_m \neq 0 \text{ für } 1 \leq j \leq m-1 \\
&\Rightarrow b_j = 0 \text{ für } 1 \leq j \leq m-1 \\
&\Rightarrow b_m v_m = 0 \Rightarrow b_m = 0
\end{aligned}$$

4.2.5 Beispiel

a) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ ist nicht diagonalisierbar.

<u>Beweis</u>: Annahme, A wäre diagonalisierbar.
Sei $T \in GL_2(\mathbb{R})$ mit $T^{-1}AT = B = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$
$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow \begin{pmatrix} a^2 & 0 \\ 0 & b^2 \end{pmatrix} = B^2 = T^{-1}ATT^{-1}AT$
$= T^{-1}A^2T = T^{-1}(-1)E_2T = (-1)T^{-1}T = -E_2$
$\Rightarrow a^2 = b^2 = -1$ Widerspruch!

b) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbb{C}^{2\times 2}$ ist nicht diagonalisierbar. (Beweis später)

c) Sei $A \in K^{n\times n}$, $a \in K$

$$\begin{aligned} a \text{ EW von A} \quad &\Leftrightarrow \quad \text{es ex. } 0 \neq v \in K^n \text{ mit } Av = av \\ &\Leftrightarrow \quad \text{es ex. } 0 \neq v \in K^n \text{ mit } (aE_n - A)v = 0 \\ &\overset{2.3.22\text{ d)}}{\Leftrightarrow} \quad aE_n - A \text{ nicht invertierbar} \\ &\overset{3.3.13\text{ b)}}{\Leftrightarrow} \quad \det(aE_n - A) = 0 \end{aligned}$$

4.3 Das Charakteristische Polynom

K Körper

4.3.1 Definition und Bemerkung

a) Sei $A \in K^{n\times n}$

1.) $XE_n - A \in K[X]^{n\times n}$ heißt die <u>**charakteristische Matrix von A**</u>.

2.) $\chi_A := \det(XE_n - A) \in K[X]$ heißt das <u>**charakteristische Polynom von A**</u>.

3.) Sei $T \in GL_n(K)$. Dann gilt:

$$\chi_{T^{-1}AT} = \chi_A$$

Sei V ein n-dimensionaler K-VR, $\varphi \in End_K(V)$, $\mathcal{B}$ Basis von V, $A := M_{\mathcal{B}}(\varphi) \in K^{n\times n}$. Dann heißt $\chi_\varphi := \chi_A$ das <u>**charakteristische Polynom**</u> von φ. Dies ist unabhängig von der gewählten Basis $\mathcal{B}$.

Beweis

a) 3.)

$$\begin{aligned}\chi_{T^{-1}AT} &= \det(XE_n - T^{-1}AT)\\ &= \det((T^{-1}XE_n - A)T) \qquad (\text{da } T^{-1}XE_nT = XE_n)\\ &\overset{3.3.10}{=} \det(XE_n - A) = \chi\end{aligned}$$

a) Die Unabhängigkeit von χ_φ von $\mathcal{B}$ folgt aus a) 3.) und 2.4.13.

4.3.2 Beispiele

a) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$

$XE_2 - A = \begin{pmatrix} x & -1 \\ 1 & x \end{pmatrix} \qquad \chi_A = \begin{vmatrix} X & -1 \\ 1 & X \end{vmatrix} = x^2 + 1$

b) $A = \begin{pmatrix} a_{11} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$ obere Dreiecksmatrix

$$\overset{3.3.7}{\Longrightarrow} \chi_A = \prod_{i=1}^{n} X - a_{ii}$$

4.3.3 Bemerkung

[Erinnerung: R kommutativer Ring, $A = (a_{ij}) \in \mathbb{R}^{n\times n}$

$$\det(A) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n}]$$

Seien R, S Ringe, $\varphi : R \to S$ Ringhomomorphismus
$A = (a_{ij}) \in R^{n\times n}$, $\varphi(A) := (\varphi(a_{ij})) \in S^{n\times n}$
Dann ist $\det(\varphi(A)) = \varphi(\det(A))$

Beweis

$$\begin{aligned}\det(\varphi(A)) &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi)\varphi(a_{\pi(1),1}) \cdots \varphi(a_{\pi(n),n})\\ &= \varphi(\sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{\pi(1),1} \cdots a_{\pi(n),n})\\ &= \varphi(\det(A))\end{aligned}$$

4.3.4 Korollar

Sei $A \in K^{n\times n}$, $a \in K$. Dann gilt:

$$\underbrace{\chi_A(a)}_{\in K} = \det(\underbrace{aE_n - A}_{\in K^{n\times n}})$$

Beweis

Betrachte den Einsetzunghomomorphismus

$$\tau_a : K[X] \to K, \qquad f \mapsto \tau_a(f) = f(a) \qquad \text{(vergl. 4.1.11)}$$

$$\begin{aligned} \chi_A(a) &= \tau_a(\chi_a) \\ &= \tau_a(\det(XE_n - A)) \\ &\overset{4.3.3}{=} \det(aE_n - A) \end{aligned}$$

4.3.5 Satz

Sei $A \in K^{n\times n}$, V n-dimensionaler K-VR, $\varphi \in End_K(V)$, $a \in K$, dann gilt:

$$a \text{ EW von } A \text{ (bzw. von } \chi_\varphi) \;\Leftrightarrow \chi_A(a) = 0 \text{ (bzw. } \chi_\varphi(a) = 0)$$

Beweis

$$\begin{aligned} a \text{ EW von } A \quad &\Leftrightarrow \quad \text{es ex. } 0 \neq v \in K^n \text{ mit } Av = av \\ &\Leftrightarrow \quad \text{es ex. } 0 \neq v \in K^n \text{ mit } (aE_n - A)v = 0 \\ &\overset{2.3.22\text{ a)}}{\Leftrightarrow} \quad aE_n - A \text{ nicht invertierbar} \\ &\overset{3.3.13\text{ b)}}{\Leftrightarrow} \quad \det(aE_n - A) = 0 \\ &\overset{4.3.4}{\Leftrightarrow} \quad \chi_a(a) = 0 \end{aligned}$$

Sei $\mathcal{B}$ Basis von V, $v \in V$. Dann gilt:
$\varphi(v) = av \Leftrightarrow M_\mathcal{B}(\varphi)\kappa_\mathcal{B}(v) = a \cdot \kappa_\mathcal{B}(v)$, und
$v \neq 0 \Leftrightarrow \kappa_\mathcal{B} \neq 0$ [$\kappa_\mathcal{B}$ ist Isomorphismus]
Also: a EW von $\varphi \Leftrightarrow a$ EW von $M_\mathcal{B}(\varphi) \Leftrightarrow \underbrace{\chi_{M_\mathcal{B}(\varphi)}}_{\chi_\varphi}(a) = 0$

4.3.6 Bemerkung

Sei $A \in K^{n\times n},\ a \in K$.
$\Rightarrow V(a,A) = \{v \in V \mid Av = av\}$ ist die Lösungsmenge des homogenen LGS $(aE_n - A)x = 0$.

4.3.7 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 Eigenwerte $\sqrt{-1},\ -\sqrt{-1}$.

b) Ähnliche Matrizen haben die gleichen EW. (Nach 4.3.1 3.) haben sie das gleiche charakteristische Polynom.)

c) Sei A ähnlich zu Dreiecksmatrix

$$\begin{pmatrix} a_{11} & & * \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} \overset{4.3.1\ 3.)}{\Longrightarrow} \chi_A = \prod_{i=1}^{n} X - a_{ii}$$

$\overset{4.3.5}{\Longrightarrow} a_{11}, ..., a_{nn}$ 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 ex. $T \in GL_2(K)$ mit

$$T^{-1}AT = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \Rightarrow \chi_{T^{-1}AT} = (X-a)(X-b)$$

$$\chi_A = (X-1)(X-1)$$

Aus $\chi_A = \chi_{T^{-1}AT}$ aus 4.3.1 3.) folgt $a = b = 1$, d.h.

$$T^{-1}AT = E_n \Rightarrow A = TE_2T^{-1} = E_2 \qquad \lightning$$

Definition 4.3.1 *Sei R kommutativer 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.*

4.3.8 Bemerkung

Sei R kommutativer Ring $A, B \in R^{n\times n},\ T \in GL_n(R)$. Dann gilt:

a) $\mathrm{Sp}(A \cdot B) = \mathrm{Sp}(B \cdot A)$

b) $\mathrm{Sp}(T^{-1}AT) = \mathrm{Sp}(A)$

Beweis

a) Sei $A = (a_{ij}),\ B = (b_{ij})$ Die i-ten Diagonaleinträge von AB bzw. BA sind $\sum\limits_{k=1}^{n} a_{ik}b_{ki}$ bzw. $\sum\limits_{k=1}^{n} b_{ik}a_{ki}$.

$$\begin{aligned}\Rightarrow \mathrm{Sp}(AB) &= \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}b_{ki} \\ &= \sum_{i=1}^{n}\sum_{k=1}^{n} b_{ki}a_{ik} \\ &= \mathrm{Sp}(B \cdot A)\end{aligned}$$

b) $\mathrm{Sp}(T^{-1}(AT)) = \mathrm{Sp}((AT)T^{-1}) = \mathrm{Sp}(A)$

4.3.9 Bemerkung

Sei $A \in K^{n\times n}$, dann gilt:

$$\chi_A = X^n - \mathrm{Sp}(A)X^{n-1} + c_{n-2}X^{n-2} + ... + c_1X + (-1)^n \det(A)$$

mit geeigneten $c_1, ..., c_{n-2} \in K$.

Beweis

Sei $E_n(\delta_{ij})_{1\leq i,j\leq n}$ und sei $A = (a_{ij})$. Dann gilt:

$$\begin{aligned}\chi_A &= \det(XE_n - A) \\ &= \sum_{\pi\in S_n} \mathrm{sgn}(\pi) \quad \underbrace{(X\delta_{\pi(1),1} - a_{\pi(1),1}) \cdots (X\delta_{\pi(n),n} - a_{\pi(n),n})}_{f_{A,\pi}\ \text{Produkt von } n \text{ Faktoren, } p \in K[X] \text{ mit } p=0 \text{ oder } \deg(p)\leq 1}\end{aligned}$$

$\underline{\pi \in S_n,\ \pi \neq id}$:
$\Rightarrow$ für mindestens 2 $i's$ mit $\pi(i) \neq i$
$\Rightarrow f_A, \pi = 0$ oder $\deg(f_{A,\pi}) \leq n - 2$

$\underline{\pi = id}$:
$f_{A,\pi} = \sum\limits_{i=1}^{n} (X - a_{ii})$
$X^n - \mathrm{Sp}(A)X^{n-1} + g$ mit $g = 0$ oder $\deg(g) \leq n-2$
Sei c_0 der konstante Koeffizient von χ_A

$$c_0 = \chi_A(0) = \det(0E_n - A) = (-1)^n \det(A)$$

4.3.10 Korollar

Sie $A \in K^{n\times n}$, bzw. $\varphi \in End_K(V)$, für einen n-dimensionaler K-VR V. Dann hat A (bzw. φ) höchstens n EW (inkl. Vielfachheit).

Definition 4.3.2 *Sei $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in K[X]$ normiert. Dann gilt:*

$$C(f) := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

die ***Begleitmatrix von*** $\underline{f}$.

$\underline{n=1}$: $\quad f = X + a_0 \quad C(f) = (-a_0) \in K^{1\times 1}$

4.3.11 Bemerkung

Sei $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in K[X]$. Dann ist $\chi_{C(f)} = f$.

Beweis

$$XE_n - C(f) = \begin{pmatrix} X & 0 & 0 & \cdots & 0 & a_0 \\ -1 & X & 0 & \cdots & 0 & a_1 \\ 0 & -1 & X & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & -1 & X & X + a_{n-1} \end{pmatrix} =: A \in K[X]^{n\times n}$$

Sei $A = (a_{ij})$. Wir entwickeln $\det(A)$ nach der letzten Spalte 3.3.5a):

$$\chi_{C(f)} = \det(A) = \sum_{i=1}^{n} (-1)^{i+n} a_{in} \det(A_{in})$$

$$A_{1n} = \begin{pmatrix} -1 & X & & 0 \\ & \ddots & \ddots & \\ & & -1 & X \\ 0 & & & -1 \end{pmatrix} \Rightarrow \det(A_{1n}) = (-1)^{n-1}$$

$$A_{in} = \left(\begin{array}{cccc|cccc} -1 & X & & 0 & & & & \\ & \ddots & \ddots & & & & 0 & \\ & & -1 & X & & & & \\ 0 & & & -1 & & & & \\ \hline & & & & -1 & X & & 0 \\ & & & & & \ddots & \ddots & \\ & 0 & & & & & -1 & X \\ & & & & 0 & & & -1 \end{array}\right) \qquad \text{für } 2 \leq i \leq n$$

$\Rightarrow \det(A_{in}) = X^{i-1}(-1)^{n-i}$ für $2 \leq i \leq n$
$a_{in} = a_{i-1}$ für $1 \leq i \leq n-1$
$a_{nn} = X + a_{n-1}$

$$\begin{aligned} \Rightarrow \chi_{C(f)} &= \det(A) \\ &= (-1)^{1+n} a_0 (-1)^{n-1} \\ &\quad + \sum_{i=2}^{n-i} (-1)^{i+n} a_{i-1} X^{i-1} (-1)^{n-1} + (-1)^{2n}(X + a_{n-1}) X^{n-1} (-1)^0 \\ &= a_0 + a_1 X + ... + a_{n-2} X^{n-2} + (X + a_{n-1}) X^{n-1} \\ &= f \end{aligned}$$

4.4 Das Minimalpolynom

K Körper, V n-dim. K-VR, $\varphi \in End_K(V)$

Definition 4.4.1 *a) $U \leq V$ heißt **φ- invariant**, falls $\varphi(U) \leq U$ ist.*

*b) Sei $U \leq V$, $u \mapsto \varphi(u)$, $u \in U$. $\varphi_U \in End_K(U)$ ist die **Einschränkung von φ auf U**.*

4.4.1 Bemerkung

Sei $U \leq V$, φ invariant.

a) Sei $\mathcal{C} = (v_1, ..., v_m)$ Basis von U. Ergänze $\mathcal{C}$ zu einer Basis $\mathcal{B} = (v_1, ..., v_m, v_{m+1}, ..., v_n)$ 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 C und D.

b) $\chi_{\varphi_U} | \chi_\varphi$

Beweis

a) Für $1 \leq j \leq m$ ist $\varphi(v_j) = \varphi_U(v_j) \in U$. Die Behauptung folgt aus der Definition von $M_{\mathcal{B}}(\varphi)$.

b) $XE_n - M_{\mathcal{B}}(\varphi) = \left(\begin{array}{c|c} XE_m - M_{\mathcal{C}}(\varphi_U) & -C \\ \hline 0 & XE_{n-m} - D \end{array}\right)$

$$\begin{aligned} \overset{3.3.8}{\Longrightarrow} \chi_\varphi &= \det(XE_n - M_{\mathcal{B}}(\varphi)) \\ &= \det(XE_m - M_{\mathcal{C}}(\varphi_U)) \cdot \det(XE_{n-m} - D) \\ &= \chi_{\varphi_U} \cdot f \qquad \text{für ein } f \in K[X] \end{aligned}$$

4.4.2 Beispiel

Sei $v_1 \in V$ EV von φ zum EW $a \in K$.
$\Rightarrow U := <v_1>$ ist φ-invariant.
ist $(v_1, ..., v_n)$ Basis von V, dann ist

$$M_{\mathcal{B}}(\varphi) = \left(\begin{array}{c|ccc} a & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & D & \\ 0 & & & \end{array}\right) \quad \text{für ein } D \in K^{(n-1)\times(n-1)}$$

4.4.3 Satz (Umkehrung von 4.3.6 c))

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 (ex. nach 4.3.5 a)). $\mathcal{B} = (v_1, .., v_n)$ Basis von K^n.

$$\Rightarrow M_{\mathcal{B}}(\varphi_A) = \left(\begin{array}{c|ccc} a & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & D & \\ 0 & & & \end{array}\right) \text{ mit } D \in K^{(n-1)\times(n-1)}$$

$M_{\mathcal{B}}(\varphi_A)$ ähnlich zu A (vergl. 2.4.13)

$$\Rightarrow \chi_A \overset{4.3.1}{=} \chi_{M_{\mathcal{B}}(\varphi_A)} \overset{3.3.8}{=} (X - a_1)\chi_D \overset{4.1.10}{\Rightarrow} \chi_D = \prod_{i=2}^{n} (X - a_i)$$

$\overset{\text{Ind.}}{\Longrightarrow}$ Es ex. $S \in GL_{n-1}(K)$, so dass $S^{-1}DS$ eine obere Dreiecksmatrix ist.

$$\text{Setze } T := \left(\begin{array}{c|ccc} 1 & 0 & \cdots & o \\ \hline 0 & & & \\ \vdots & & S & \\ 0 & & & \end{array}\right) \in K^{n \times n}$$

$\Rightarrow \det(T) = \det(S) \neq 0$, d.h. $T \in GL_n(K)$. Weiter gilt:

$$T^{-1}M_{\mathcal{B}}(\varphi_A)T = \left(\begin{array}{c|ccc} a_1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & S^{-1}DS & \\ 0 & & & \end{array}\right)$$

ist eine obere Dreiecksmatrix.

4.4.4 Bemerkung

a) $End_K(V)$ ist K-VR mit

$$\begin{array}{ll} + : & End_K(V) \times End_K(V) \to End_K(V) \\ & (\varphi + \psi)(v) := \varphi(v) + \psi(v) \qquad \varphi, \psi \in End_K(v),\ v \in V \\ \cdot : & K \times End_K(V) \to End_K(V) \\ & (a\varphi)(v) := a\varphi(v) \qquad \varphi \in End_K(v),\ v \in V \end{array}$$

b) $End_K(V)$ ist K-Algebra mit a) und

$$\begin{array}{ll} \cdot : & End_K(V) \times End_K(V) \to End_K(V) \\ & (\varphi, \psi) \mapsto \varphi \circ \psi \end{array}$$

c) Ist $\mathcal{B}$ eine Basis von V, dann ist
$M_{\mathcal{B}} : End_K(V) \to K^{n \times n},\ \varphi \mapsto M_{\mathcal{B}}(\varphi)$
ein K-Algebra-Isomorphismus.

Beweis

Formales Rechnen.

4.4.5 Bemerkung

Sei $0 \neq v \in V$. Die Folge $v(, \varphi(v), \varphi^2(v) = \varphi(\varphi(v)), ..., \varphi^n(v))$ ist l.a. .
Sei $m \in \mathbb{N}$ minimal, so dass

$$(v, \varphi(v), ..., \varphi^{m-1}(v)) \text{ l.u. aber}$$

$$(v, \varphi(v), ..., \varphi^{m-1}(v), \varphi^m(v)) \text{ l.a. ist } (\varphi^0 := id).$$

$\Rightarrow$ Es existieren $a_0, ..., a_{m-1} \in K$ mit $\varphi^m(v) = \sum\limits_{i=0}^{m-1} a_i \varphi^i(v)$.
$\Rightarrow U := <v, \varphi(v), ..., \varphi^{m-1}(v)>$ ist m-dimensionaler $\varphi-$invarianter UR von V.

Sei $\mathcal{C} = (v, \varphi(v), ..., \varphi^{m-1}(v))$ und $f = X^m - \sum\limits_{i=0}^{m-1} a_i X^i \in K[X]$. Dann ist

$$M_{\mathcal{C}}(\varphi_U) = \begin{pmatrix} 0 & 0 & & & a_0 \\ 1 & 0 & & & a_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 & a_{m-2} \\ 0 & 0 & & 1 & a_{m-1} \end{pmatrix} = C(f)$$

$\overset{4.4.1}{\Longrightarrow} \chi_{\varphi_U} = \chi_{C(f)} = f$
$f(\varphi) = \varphi^m - \sum\limits_{i=0}^{m-1} a_i \varphi^i \in End_K(V)$
$f(\varphi)(v) = \varphi^m(v) - \sum\limits_{i=0}^{m-1} a_i \varphi^i(v) = 0$

4.4.6 Satz (Cayley-Hamilton)

Sei $\varphi \in End_K(V)$ bzw. $A \in K^{n \times n}$. Dann gilt:

$$\chi_\varphi(\varphi) = 0 \text{ bzw. } \chi_A(A) = 0$$

Beweis

Aussage für A folgt aus der für φ mit 4.4.4 c).

zu zeigen: $\chi_\varphi(\varphi) = 0 \in End_K(V)$, d.h. $\chi_\varphi(\varphi)(v) = 0 \ \forall v \in V$
$\underline{v = 0}$: klar.
Sei also $v \neq 0$ und $U = <v, \varphi(v), ..., \varphi^{m-1}(v)>$ wie in 4.4.5. Nach 4.4.1 c) ex. $f \in K[X]$ mit

$$\chi_\varphi = \chi_{\varphi_U} \cdot f = f \cdot \chi_{\varphi_U}$$

$$\begin{aligned}
\Rightarrow \chi_\varphi(\varphi) &= (f \cdot \chi_{\varphi_U}(\varphi)) \\
&= \underbrace{f(\varphi}_{\in End_K(V)} \circ \underbrace{\chi_{\varphi_U}(\varphi)}_{\in End_K(V)}) \\
\Rightarrow \chi_\varphi(\varphi)(v) &= [f(\varphi) \circ \chi_{\varphi_U}(\varphi)](v) \\
&= f(\varphi)(\underbrace{\chi_{\varphi_U}(\varphi(v))}_{=0 \text{ nach } 4.4.5}) = 0
\end{aligned}$$

4.4.7 Beispiel

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in K^{2\times 2}, \qquad XE_2 - A = \begin{pmatrix} X-1 & -2 \\ -3 & X-4 \end{pmatrix}$

$\chi_A = (X-1)(X-4) - 6 = X^2 - 5X - 2$

$\chi_A(A) = A^2 - 5A - 2E_2$

$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$

$A^2 - 5A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2E_2$

$A(A - 5E_2) = 2E_2 \Rightarrow A^{-1} = \frac{1}{2}(A - 5E_2)$

4.4.8 Bemerkung und Definition

Sei $A \in K^{n\times n}$, $\varphi \in End_K(V)$, wobei V n-dimensionaler K-VR sei.

a) Es ex. $\mu_A \in K[X]$, $\deg(\mu_A) \geq 1$ (bzw. $\mu_\varphi \in K[X]$, $\deg(\mu_\varphi) \geq 1$, mit

1.) μ_A (bzw. μ_φ) ist normiert

2.) $\mu_A(A) = 0$ (bzw. $\mu_\varphi(\varphi) = 0$)

3.) $\mu_A | f$ (bzw. $\mu_\varphi | f$) $\forall f \in K[X]$ 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. von 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 4.4.6 $\Rightarrow I \neq \{0\}$
Sei $0 \neq \mu \in I$ von minimalem Grad und sei $a \in K$ der höchste Koeffizient von μ. Setzte $\mu_A := a^{-1}\mu$.
$\Rightarrow \deg(\mu_A) = \deg(\mu)$, μ_A normiert, d.h. 1.) und $\mu_A(A) = 0$, d.h. 2.)
Sei $f \in I \Rightarrow$ es ex. $q, r \in K[X]$ mit $f = q \cdot \mu_A + r$ und $r = 0$ oder $\deg(r) < \deg(\mu_A)$ Es gilt:

$$\begin{aligned} r(A) &= f(A) - (q \cdot \mu_A)(A) \\ &= f(A) - q(A) \cdot \mu_A(A) = 0 \end{aligned}$$

$\Rightarrow r = 0$ nach Wahl von μ.

Eindeutigkeit: Seien $\mu_1,\ \mu_2 \in K[X]$ mit 1.) - 3.)
$\Rightarrow \mu_1 | \mu_2$ und $\mu_2 | \mu_1$
$\Rightarrow \mu_1 = \mu_2$, da beide normiert sind.

b) Folgt aus a) und 4.4.4 c).

c) Folgt aus b) und 2.4.13, oder auch durch direktes Rechnen mit a).

4.4.9 Beispiele

a) Sei $A = \begin{pmatrix} 1 & 1 & 0 & & & 0 \\ 0 & 1 & 1 & & & \\ 0 & 0 & 1 & & & \\ & & & 1 & & \\ & & & & 0 & 0 \\ 0 & & & & 0 & 0 \end{pmatrix} \in K^{6\times 6}$

$\chi_A = X^2(X-1)^4,\ \mu_A = X(X-1)^3$

b) Sei $a \in K$ und

$$A = \begin{pmatrix} a & 1 & & 0 \\ & \ddots & \ddots & \\ & & & 1 \\ & & & a \end{pmatrix} \in K^{n\times n}$$

$\Rightarrow \chi_A = \mu_A = (X-a)^n$

c) Sei $f \in K[X],\ f \in K,\ f$ normiert.
$\Rightarrow \chi_{C(f)} = \mu_{C(f)} = f$

d) Sei $A = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$ eine Diagonalmatrix.
Sei $\{a_1, ..., a_n\} = \{b_1, ..., b_m\}$ mit $b_i \neq b_j$ für $i \neq j$.
$\Rightarrow \mu_A = \prod_{i=1}^{m} (X - b_i)$

Beweis

a) $\mu_A | \chi_A \Rightarrow \mu_A = X^r (X-1)^s$ mit $0 \leq r \leq 2$ und $0 \leq s \leq 4$
$A^i \neq 0 \ \forall i \geq 1$
$(A - E_6)^i \neq 0 \ \forall i \geq 1$
$\Rightarrow X(X-1) | \mu_A$
$A(A - E_6)^3 = 0, \ A(A - E_6)^2 \neq 0$

b) $\chi_A = (X - a)^n$

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

c) Übung.

d) Der i-te Diagonaleintrag von $\prod_{j=1}^{m} (A - b_j E_n)$ ist $\underbrace{\prod_{j=1}^{n} (a_i b_j)}_{=0 \text{ wegen } a_i \in \{b_1, ..., b_m\}}$

Füre keinen echten Teiler ρ von $\prod_{j=1}^{m} (X - b_j)$ ist $\rho(A) = 0$.

4.4.10 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 $U := \text{Kern}(g(\varphi))$, $W := \text{Kern}(h(\varphi))$.
Dann sind U und W φ-invariant und es gilt:

$$V = U \oplus W, \text{ d.h. } V = U + W \text{ und } U \cap W = \{0\}$$

Beweis

Sei $u \in U$, d.h. $g(\varphi)(u) = 0$
$\Rightarrow g(\varphi)(\varphi(u)) = g(\varphi) \circ \varphi(u) = \varphi \circ g(\varphi)(u)) = \varphi(g(\varphi(u) = \varphi(0) = 0$
$\Rightarrow \varphi(u) \in \text{Kern}(g(\varphi) = U$ d.h. U φ-invariant.

Analog: W φ-invariant.

Seien $g_1, h_1 \in K[X]$ mit $1 = q_1 g + h_1 h$ 4.1.8
φ einsetzen $\Rightarrow id = \underbrace{(g_1 g)(\varphi)}_{g_1(\varphi)\circ g(\varphi)} + (h_1 h)(\varphi) \in End_K(V)$
$\Rightarrow v = (g_1 g)(\varphi)(v) + (h_1 h)(\varphi)(v)\ \forall v \in V$
Zeige: $(g_1 g)(\varphi)(v) \in \underbrace{W}_{=\text{Kern}(h(\varphi))}$, $(h_1 h)(\varphi)(v) \in U$

$$\begin{aligned} h(\varphi[(g_1 g)(\varphi)(v)] &= [h(\varphi) \circ (g_1 g)(\varphi)](v) \\ &= (hg_1 g)(\varphi)(v) \\ &= (hg_1 g)(\varphi)(v) \\ &= (g_1 f)(\varphi)(v) \\ &= [g_1(\varphi) \circ f(\varphi)](v) \\ &= g_1(\varphi)(\underbrace{f(\varphi)(v)}_{=0}) = 0 \end{aligned}$$

Also: $(g_1 g)(\varphi)(v) \in W$
Analog: $(h_1 h)(\varphi)(v) \in V$

$$\Rightarrow V = U + W$$

Sei $v \in U \cap W$.

$$\begin{aligned} \Rightarrow v &= [g_1(\varphi) \circ g(\varphi)](v) + [h_1(\varphi) \circ h(\varphi)](v) \\ &= g_1(\varphi)(\underbrace{g(\varphi)(v)}_{0,\text{ da } v\in U}) + h_1(\varphi)(\underbrace{h(\varphi)(v)}_{=0,\text{ da } v\in W}) = 0 \end{aligned}$$

$$\Rightarrow U \cap W = \{0\}$$

4.4.11 Satz

Sei $A \in K^{n\times n}$. Dann gilt:
A diagonalisierbar $\Leftrightarrow$ μ_A zerfällt in ein Produkt von paarweise verschiedenen Linearfaktoren

Beweis

„$\Rightarrow$“: 4.4.8 c), 4.4.9 d)

„$\Leftarrow$“: Sei $\mu_A = \prod_{j=1}^{m} (X - b_j)$ mit $b_1 \neq b_j$ für $i \neq j$.

Betrachte $\varphi_A : K^n \to K^n$, setze $f := \mu_A,\ g := X - b_1,\ b = \prod_{j=2}^{m} (X - b_j)$

$\Rightarrow g, h$ teilerfremd (o.B.d.A.: $n > 1$)
$\Rightarrow K^n = U \oplus W$ mit $U = \text{Kern}(g(\varphi_A)),\ W = \text{Kern}(h(\varphi_A))$
$\text{Kern}(g(\varphi_A)) = \text{Kern}(\varphi_A - b_A \cdot id)$
Sei $(u_1, ..., u_m)$ Basis von U, $(w_1, ..., w_l)$ Basis von W.

$$\Rightarrow (u_1, ..., u_m, w_1, ..., w_l) =: \mathcal{B} \text{ ist Basis von } V$$

Weil U, W φ_A-invariant sind, ist

$$M_{\mathcal{B}}(\varphi_A) = \left(\begin{array}{ccc|c} b_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & b_1 & \\ \hline & & & \\ & 0 & & \\ & & & \end{array}\right)$$

Es gilt: $\mu_A(D) = 0 \Rightarrow \mu_D | \mu_A$
$\Rightarrow \mu_D$ zerfällt in Produkt von paarweise verschiedenen Linearfaktoren.
$\overset{\text{Ind.}}{\Longrightarrow} D$ ist diagonalisierbar.
$\Rightarrow A$ ist diagonalisierbar (Argument wie in Beweis von 4.4.3)

Kapitel 5

Euklidische und Unitäre Räume

Zusätzliche Struktur für reele oder komplexe Vektorräume, **Skalarprodukt** $\rightsquigarrow$ Längen, Winkel.

$K = \mathbb{R}$ oder $\mathbb{C}$

$\mathbb{C} = \{a + ib \mid a + b \in \mathbb{R}\}$, $i \in \mathbb{C}$ mit $i^2 = -1$
$(1, i)$ l.a. über $\mathbb{R}$ (vgl. 2.3.10)
$\mathbb{R} \subseteq \mathbb{C}$

$^- : \mathbb{C} \to \mathbb{C}$, $a+ib \mapsto a-ib$ heißt **komplexe Konjugation**. $^-$ ist ein Körperautomorphismus, d.h. ein bijektiver Ringhomomorphismus.
$|c| := \sqrt{c\overline{c}} \in \mathbb{R}_{\geq 0}$ heißt (**komplexer**) **Absolutbetrag** .
$A = (a_{ij}) \in \mathbb{C}^{n \times n}$, $\overline{A} = (\overline{a}_{ij})$

5.1 Skalarprodukt

$K = \mathbb{R}$ oder $\mathbb{C}$, V K-VR (nicht notwendig endlich erzeugt).

5.1.1 Definition und Bemerkung

a) Eine Abbildung $\beta : V \times V \to K$ heißt **Bilinearform** (im Fall $K = \mathbb{R}$) bzw. **Sesqui-Linearform** (im Fall $K = \mathbb{C}$), falls gilt

   1.) $\beta(v_1 + v_2, w) = \beta(v_1, w) + \beta(v_2, w)$ und
   $\beta(av, w) = a\beta(v, w) \qquad \forall\ v, v_1, v_2, w \in V,\ a \in K$

   2.) $\beta(v, w_1 + w_2) = \beta(v, w_1) + \beta(v, w_2)$ und
   $\beta(v, aw) = \overline{a}\beta(v, w) \qquad \forall\ v, w_1, w_2 \in V,\ a \in K$

b) Sei β Bilinearform (bzw. Sesqui-Linearform) auf V. β heißt **symmetrisch** (bzw. **hermite'sch**), falls gilt:

$$\beta(v, w) = \beta(w, v) \qquad \forall\ v, w \in V$$

$$\beta(v,w) = \overline{\beta(w,v)} \qquad \forall\ v,w \in V$$

(*) Ist β hermite'sch (also $K = \mathbb{C}$), dann ist $\beta(v,v) \in \mathbb{R}\ \forall\ v \in V$
Sei β symmetrisch (bzw. hermite'sch). Dann heißt β ein **Skalarprodukt auf V**, falls β **positiv definit** ist, d.h. falls gilt:

$$\beta(v,v) > 0\ \forall v \in V,\ v \neq 0$$

Beweis

Von b) (*):

$$\beta(v,v) = \underbrace{\overline{\beta(v,v)}}_{v \text{ und } v \text{ vertauscht}}, \text{ da } \beta \text{ hermite'sch} \Rightarrow \beta(v,v) \in \mathbb{R}$$

5.1.2 Beispiele

$V = K^n$ ($\mathbb{R}^n$ oder $\mathbb{C}^n$)

1.) $<\ ,\ > : V \times V \to K, \qquad <\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}> := \sum\limits_{j=1}^{n} a_j \overline{b_j} \in K$

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 $(f,g) := \int\limits_0^1 f(t)g(t)dt \in \mathbb{R}$
$(\ ,\ )$ ist ein Skalarprodukt auf V.

5.1.3 Satz (Cauchy-Schwarz'sche Ungleichung)

Sei $(\ ,\ )$ ein Skalarprodukt auf V, dann gilt für alle $v_1, v_2 \in V$:

$$\begin{aligned} |(v_1,v_2)|^2 &\leq (v_1,v_1)(v_2,v_2), \text{ sowie} \\ |(v_1,v_2)|^2 &= (v_1,v_1)(v_2,v_2) \Leftrightarrow v_1, v_2 \text{ sind l.a.} \end{aligned}$$

Beweis

Ist $v_2 = 0$, dann sind beide Aussagen klar. Sei also $v_2 \neq 0$ und $a := -\frac{(v_1,v_2)}{(v_2,v_2)} \in K$:

$$\begin{aligned}
\Rightarrow 0 \quad &\leq \quad (v_1 + a_v 2, v_1 + av_2) \\
&= \quad (v_1, v_1) + a(v_2, v_1) + \overline{a}(v_1, v_2) + a\overline{a}(v_2, v_2) \\
&= \quad (v_1, v_1) - \frac{|(v_1, v_2)|^2}{(v_2, v_2)} - \frac{|(v_1, v_2)|^2}{(v_2, v_2)} + \frac{|(v_1, v_2)|^2}{(v_2, v_2)} \\
&= \quad (v_1, v_1) - \frac{|(v_1, v_2)|^2}{(v_2, v_2)} \\
&\Rightarrow \quad \text{1. Behauptung}
\end{aligned}$$

Es gelte: $|(v_1, v_2)|^2 = (v_1, v_1)(v_2, v_2)$.

$$\begin{aligned}
&\Rightarrow \quad (v_1 + av_2, v_1 + av_2) = 0 \\
&\Rightarrow \quad v_1 + av_2 = 0, \text{ d.h. } v_1, v_2 \text{ sind l.a.}
\end{aligned}$$

Seien v_1, v_2 l.a., dann ist $v_1 = bv_2$ für ein $b \in K$ (weil $v_2 \neq 0$).

$$\begin{aligned}
\Rightarrow |(v_1, v_2)|^2 \quad &= \quad v|(v_2, v_2)|^2 \\
&= \quad |b|^2 |(v_2, v_2)|^2 \\
&= \quad b\overline{b}(v_2, v_2)(v_2, v_2) \\
&= \quad (v_1, v_1)(v_2, v_2)
\end{aligned}$$

5.1.4 Beispiele

1.) Seien $a_j, b_j \in \mathbb{C}, \ 1 \leq j \leq n$

$$\Rightarrow |\sum_{j=1}^{n} a_j \overline{b_j}|^2 \leq \left(\sum_{j=1}^{n} |a_j|^2 \right) \left(\sum_{j=1}^{n} |b_j|^2 \right)$$

mit Gleichheit genau dann, wenn $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ und $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ l.a. sind.

2.) Für alle stetigen Funktionen $f, g : [0, 1] \to \mathbb{R}$ gilt:

$$|\int_0^1 f(t)g(t)dt|^2 \leq \left(\int_0^1 |f(t)|^2 dt \right) \left(\int_0^1 |g(t)|^2 dt \right)$$

5.1.5 Definition und Bemerkung

Sei V e.d. und β eine Bilinearform (bzw. eine Sesqui-Linearform) auf V. Sei $\mathcal{B}$ eine Basis von V, $\mathcal{B} = (v_1, ..., v_n)$.

a) Dann heißt

$$G_{\mathcal{B}}(\beta) := (\beta(v_i, v_j))_{1 \le i,j \le n} \in K^{n \times n}$$

die **Gram-Matrix von β bzgl. $\mathcal{B}$**.

b) Sei $A := G_{\mathcal{B}}(\beta)$. Dann gilt für alle $v, w \in V$

- $\beta(v, w) = \kappa_{\mathcal{B}}(v)^t A \overline{\kappa_{\mathcal{B}}(w)}$
- 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. $v = \sum_{j=1}^{n} a_j v_j$, $\kappa_{\mathcal{B}}(w) = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$.

$$\begin{aligned}
\Rightarrow \beta(v, w) &= \beta\Big(\sum_{j=1}^{n} a_j v_j, \sum_{k=1}^{n} b_k v_k\Big) \\
&= \sum_{j=1}^{n} \sum_{k=1}^{n} a_j \overline{b_k} \beta(v_j, v_k) \\
&= (a_1, ..., a_n) A \begin{pmatrix} \overline{b_1} \\ \vdots \\ \overline{b_n} \end{pmatrix} \\
&= (a_1, ..., a_n) \cdot \begin{pmatrix} \sum_{k=1}^{n} \beta(v_1, v_k) \overline{b_k} \\ \vdots \\ \sum_{k=1}^{n} \beta(v_n, v_k) \overline{b_k} \end{pmatrix} \\
&= \sum_{j=1}^{n} \sum_{k=1}^{n} a_j \beta(v_j, v_k) \overline{b_k}
\end{aligned}$$

$$\begin{aligned}
\beta \text{ symmetrisch} \quad &\Rightarrow \quad \beta(v_j, v_k) = \beta(v_k, v_j) \forall j, k \\
&\Rightarrow \quad A = A^t
\end{aligned}$$

$$\begin{aligned} A = A^t \Rightarrow \beta(v,w) &= \kappa_{\mathcal{B}}(v)^t A \kappa_{\mathcal{B}}(w) \\ &= \kappa_{\mathcal{B}}(v)^t A^t (\kappa_{\mathcal{B}}(w)^t)^t \\ &= (\kappa_{\mathcal{B}}(w)^t A (\kappa_{\mathcal{B}}(v))^t \\ &= \kappa_{\mathcal{B}}(w)^t A (\kappa_{\mathcal{B}}(v)) \\ &= \beta(w,v) \end{aligned}$$

Aussage hermite'sch analog.

Ist in 5.1.5 $V = K^n$ und $\mathcal{B}$ die Standardbasis, dann gilt:

$$\beta(v,w) = v^t A \overline{w} \quad \forall\ v,w \in K^n$$

5.1.6 Bemerkung

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

a) $\beta_A : K^n \times K^n \to K$
$\beta_A(v,w) := v^t A\overline{w}, \qquad v,w \in K^n$
ist Bilinearform (bzw. Sesqui-Linearform) auf K^n.

b) β_A ist symmetrisch $\Leftrightarrow$ A symmetrisch $(K = \mathbb{R})$
β_A ist hermite'sch $\Leftrightarrow$ A hermite'sch $(K = \mathbb{C})$

Beweis

a) Klar.

b) Folgt aus 5.1.5 b), denn $A = G_{\mathcal{B}}(\beta_A)$, wenn $\mathcal{B}$ die Standardbasis von K^n ist. (Beachte: $e^t A e_j = a_{ij}$)

Definition 5.1.1 *a) $A \in \mathbb{R}^{n\times n}$ heißt* ***positiv definit****, wenn $A = A^t$ ist und $v^t A v > 0 \qquad \forall\ 0 \neq v \in \mathbb{R}^n$.*

b) $A \in \mathbb{C}^{n\times n}$ heißt ***positiv definit****, wenn $A = \overline{A}^t$ ist und $v^t A \overline{v} > 0 \qquad \forall\ 0 \neq v \in \mathbb{C}^n$.*

Erinnerung: V n-dim. K-VR, $\mathcal{B} = (v_1, ..., v_n)$, $\mathcal{B}' = (v_1', ..., v_n')$ Basis von V. $T := M_{\mathcal{B}}^{\mathcal{B}'}(id_V)$ Basiswechselmatrix, definiert durch $T = (t_{ij}) \in K^{n\times n}$ mit $v_j = \sum\limits_{i=1}^{n} t_{ij} v_i$.

5.1.7 Satz

Sei V n-dim. K-VR und β eine Bilinearform (bzw. Sesqui-Linearform) auf V. Seien $\mathcal{B} = (v_1, ..., v_n)$ und $\mathcal{B}' = (v_1', ..., v_n')$ Basen von V und $T = M_B^{B'}(id_V)$ die Basiswechselmatrix.

Setze $A := G_{\mathcal{B}}(\beta)$ und $A' := G_{\mathcal{B}'}(\beta)$. Dann gilt: $A' = T^t A \overline{T}$ (vgl. 2.4.13).

Beweis

Sei $T = (t_{ij})$, d.h. $v'_j = \sum\limits_{i=1}^{n} t_{ij} v_i$.
Beachte: $A = (\beta(v_i, v_j))$, $A' = (\beta(v'_i, v'_j))$

$$\begin{aligned}\beta(v_i, v_j) &= \beta\left(\sum_{k=1}^{n} t_{ki} v_k,\ \sum_{l=1}^{n} t_{lj} v_l\right) \\ &= \underbrace{\sum_{k=1}^{n}\sum_{l=1}^{n} t_{ki}\overline{t_{lj}}\beta(v_k, v_l)}_{(i,j)\text{-Eintrag von } T^t A\overline{T}}\end{aligned}$$

5.2 Länge, Winkel, Orthogonalität

$K = \mathbb{R}, \mathbb{C}$ $\quad$ V K-VR mit Skalarprodukt (,)

Definition 5.2.1 *a) Im Fall $K = \mathbb{R}$ (bzw. $K = \mathbb{C}$) heißt $(V, (\ ,\ ))$* ***euklidischer*** *(bzw.* ***unitärer****)* ***Raum****.*
Die Abbildung $||.|| : V \to \mathbb{R}$, $\quad v \mapsto \sqrt{(v,v)} \in \mathbb{R}_{\geq 0}$ 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. $\mathbb{C}^n$).*

5.2.1 Beispiel

Im n-dim. euklischen Raum $\mathbb{R}^n$ ist $||v||$ die „Länge“ des Ortsvektors $\vec{v}$.

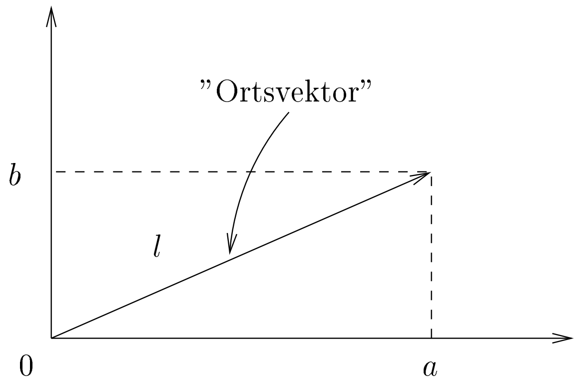

Abbildung 5.1: Ortsvektor

Länge $\overrightarrow{0v}$ (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: $<v,v> = \sum_{j=1}^{n} {a_j}^2,\ ||v|| = \sqrt{<v,v>} = \sqrt{\sum_{i=1}^{n} a_j^2}$

5.2.2 Bemerkung (Eigenschaften von $||\ ||$)

1.) $||\ ||$ ist **<u>Norm auf V</u>**, d.h.

a) $||v|| \geq 0 \quad \forall\ v \in V$ und
$||v|| = 0 \Leftrightarrow v = 0$

b) $||av|| = |a| \cdot ||v|| \quad \forall v \in V, a \in K$

c) $||v_1 + v_2|| \leq ||v_1|| + ||v_2|| \quad \forall v_1, v_2 \in V$ (Dreiecksungleichung)

2.) Polarisationsformeln:

a) Für $K = \mathbb{R}$ gilt:

$$(v,w) = \frac{1}{2}(||v+w||^2 - ||v||^2 - ||w||^2) \quad \forall\ v,w \in V$$

b) Für $K = \mathbb{C}$ gilt:

$$(v,w) = \frac{1}{4}(||v+w||^2 - ||v-w||^2 + i||v+iw||^2 - i||v-iw||^2) \quad \forall\ v,w \in V$$

3.) Für $0 \neq v,\ 0 \neq w \in V$ gilt:

$$\left| \frac{(v,w)}{||v|| \cdot ||w||} \right| \leq 1$$

Beweis

1.) a) Klar, mit 5.1.1 b).

b)

$$\begin{aligned} ||av|| &= \sqrt{(av,av)} \\ &= \sqrt{a\overline{a}(v,v)} \\ &= \sqrt{a\overline{a}}\sqrt{(v,v)} \\ &= |a|\ ||v|| \end{aligned}$$

c) Nach 5.1.3 gilt:

$$\begin{aligned}
||v_1 + v_2||^2 &= |(v_1 + v_2, v_1 + v_2)| \\
&= |(v_1, v_1) + (v_1, v_2) + (v_2, v_1) + (v_2, v_2)| \\
&\leq |(v_1, v_1)| + |(v_1, v_2)| + |(v_2, v_1)| + |(v_2, v_2)| \\
&\leq ||v_1||^2 + ||v_1|| \; ||v_2|| + ||v_2|| \; ||v_1|| + ||v_2||^2 \\
&= (||v_1|| + ||v_2||)^2
\end{aligned}$$

2.) Übung, Blatt 14.

3.) Folgt aus 5.1.3, wie in Beginn des Beweises zu 1) c).

5.2.3 Zwischenbemerkung

Wir benutzen 5.2.2 3), um „Winkel " für euklidische Räume zu defnieieren.
V euklidisch, $v, w \in V$, $v, w \neq 0$

$$\overset{5.2.2\ 3.)}{\Longrightarrow} -1 \leq \frac{(v,w)}{||v|| \; ||w||} \leq 1$$

$\Rightarrow$ es existiert genau ein $\alpha \in \mathbb{R}$, $0 \leq \alpha \leq \pi$ mit

$$\cos(\alpha) = \frac{(v,w)}{||v|| \; ||w||} = \left(\frac{v}{||v||}, \frac{w}{||w||} \right)$$

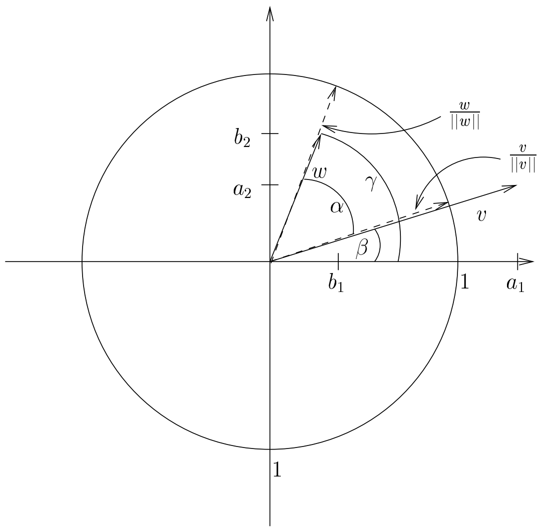

Abbildung 5.2: Winkelberechnung

$\frac{v}{||v||} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \qquad \frac{w}{||w||} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$
$\gamma = \alpha + \beta, \qquad \alpha = \gamma - \beta$
$\cos(\alpha) = \cos(\gamma - \beta) = \cos(\gamma)\cos(\beta) + \sin(\gamma)\sin(\beta)$
$\cos(\beta) = a_1,\ \sin(\beta) = a_2,\ \cos(\gamma) = b_1,\ \sin(\gamma) = b_2$

$$\Rightarrow \cos(\alpha) = b_1 a_1 + b_2 a_2 = <\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}> = <\frac{v}{||v||}, \frac{w}{||w||}>$$

Definition 5.2.2 *Sei V ein euklidischer VR. 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 der **Winkel zwischen v und w**.*

$$v, w \text{ heißen } \underline{\textbf{orthogonal}} \Leftrightarrow \alpha = \frac{\pi}{2} \Leftrightarrow \cos(\alpha) = 0 \Leftrightarrow (v, w) = 0$$

5.2.4 Bemerkung

Bezeichnungen wie in 5.2.2, dann gilt:

$$\begin{array}{rcl} v, w \text{ l.a.} & \stackrel{5.1.3}{\Longrightarrow} & |(v, w)|^2 = (v, v) \cdot (w, w) \\ & \Leftrightarrow & |(v, w)| = \pm ||v|| \cdot ||w|| \\ & \Leftrightarrow & cos(\alpha) \in \{1, -1\} \\ & \Leftrightarrow & \alpha = 0 \text{ oder } \alpha = \pi \\ & & \text{wobei } \alpha \text{ den Winkel zwischen } v \text{ und } w \text{ bezeichnet} \end{array}$$

Sind v und w normiert, dann gilt:

$$\alpha = 0 \Leftrightarrow v = w$$

$$\alpha = \pi \Leftrightarrow v = -w$$

5.2.5 Beispiel (vgl. 2.2.2 f), Suchmaschinen)

Term-Dokumente-Matrizen M
Zeilen: Terme m
Spalten: Dokumente n
Einträge: Häufigkeit eines Termes
Suchanfrage: $(0, 1)$-Vektor $\in \mathbb{R}^n$, s
Gesucht: Die Dokumente, zu denen s am besten passt.

Möglichkeit: Euklidische Norm auf $\mathbb{R}^n$ als Maß für die „Gleichheit" von s mit Spalten von M.
Seien $d_1, ..., d_n$ die Spalten von M; normiere zu $c_1 = \frac{d_1}{||d_1||}, ..., c_n = \frac{d_n}{||d_n||}$.
Prepocessing: Berechne $<\frac{s}{||s||}, c_j>$ für $1 \leq j \leq n$ und gebe diejenigen Dokumente aus, für die dieses Skalarprodukt größer als eine vorgegebene Schranke ist.
Intuition: $<\frac{s}{||s||}, c_j> \geq 0 \; \forall j$, da alle Einträge der Vektoren ≥ 0.
$<\frac{s}{||s||}, c_j> = 1 \Leftrightarrow \frac{s}{||s||} = c_j$
$<\frac{s}{||s||}, c_j> = 0 \Leftrightarrow$ keine Übereinstimmung zwischen s und d_j

5.2.6 Satz (Schmidt'sches Orthogonalisierungsverfahren)

Seien $v_1, ..., v_n \in V$ l.u. und sei $0 \leq m \leq n$ mit $(v_i, v_j) = \delta_{i,j}$ (Kronecker Delta) für $1 \leq i, j \leq m$ (Keine Bedingung für $m = 0$).
Dann existieren $w_1, ..., w_n \in V$ 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 $(w_j, w_k) = \delta_{j,k}$ für $1 \leq j, k \leq n$.

Beweis

Induktion über $n - m$
$n - m = 0$: Klar.
$n - m > 0$: Ist w_{m+1} wie gewünscht konstruiert, dann gilt:

$$<v_1, ..., v_m, v_{m+1}> = <\underbrace{w_1}_{=v_1}, ..., \underbrace{w_m}_{=v_m}, w_{m+1}>$$

denn $v_{m+1} \in <w_1, ..., w_m, w_{m+1}>$, weil $a_{m+1,m+1} \neq 0$.

$$\Rightarrow <v_1, ..., v_m, w_{m+1}, v_{m+2}, ..., v_n> = <v_1, ..., v_m, v_{m+1}, v_{m+1}, ..., v_n>$$

$$\Rightarrow (v_1, ..., v_m, v_{m+1}, v_{m+2}, ..., v_n) \text{ ist l.u.}$$

Es genügt also die Behauptung für $n = m + 1$ zu beweisen. Sei

$$u := v_{m+1} - \sum_{j=1}^{m} (v_{m+1}, v_j) v_j$$

$\Rightarrow u \neq 0$, da $(v_1, ..., v_{m+1})$ l.u.
Es gilt für $1 \leq k \leq m$:

$$(u, v_k) = (v_{m+1}, v_k) - \sum_{j=1}^{m} (v_{m+1}, k_j) \underbrace{(v_j, v_k)}_{=\begin{cases} 0, & j \neq k \\ 1, & j = k \end{cases}}$$

$$= (v_{m+1}, v_k) - (v_{m+1}, v_k) = 0$$

$\Rightarrow w_{m+1} := \frac{u}{||u||}$ erfüllt das Gewünschte.

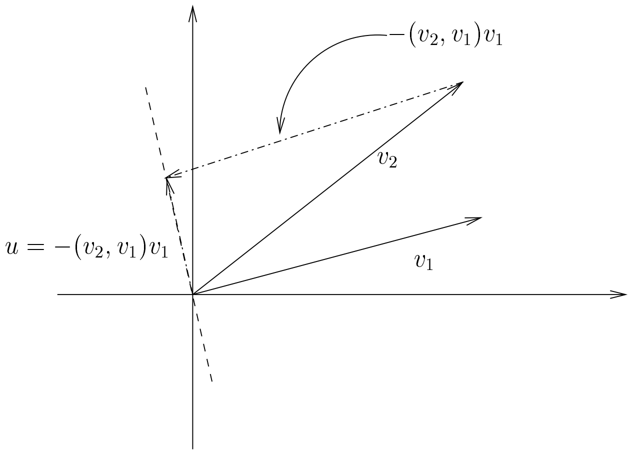

Abbildung 5.3: Orthogonalisierbarkeit

5.2.7 Beispiel

$V = \mathbb{R}^3,\ <\ ,\ >,\ n = 3,\ m = 0$

$v_1 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, \qquad v_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \qquad v_3 \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$

$w_1 = \frac{v_1}{||v_1||} = \frac{1}{3} \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}$

$u = v_2 - <v_2, w_1>\ w_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} - 1 \cdot \frac{1}{3} \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}$

$<u, u> = 1 \Rrightarrow u = w_2 = \frac{1}{3} \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}$

$$\begin{aligned} u &:= v_3 - <v_3, w_1>\ w_1 - <v_3, w_2>\ w_2 \\ &= \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} + 0 w_1 - 1 \cdot \frac{1}{3} \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} \\ &= \frac{1}{3} \begin{pmatrix} -2 \\ -1 \\ 2 \end{pmatrix} \end{aligned}$$

$<u,u> = 1 \Rightarrow w_3 = \frac{1}{3}\begin{pmatrix}-2\\-1\\2\end{pmatrix}$

Definition 5.2.3 *a) Sei V e.d.. Eine Basis $v_1, ..., v_n)$ von V heißt* ***Orthonormalbasis (ONB) von*** *V, falls gilt*

$$(v, v_j) = \delta_{ij} \quad 1 \le i, j \le n$$

b) $U^\perp := \{v \in V \mid (u, v) = 0 \ \forall\ u \in U\}$ heißt der ***Orthogonalraum zu*** *U.*

5.2.8 Korollar

Sei $\dim_K(V) = n$.

a) V besitzt ONB.

b) Ist $a \in K^{n\times n}$ positiv definit, dann ex. $S \in GL_n(K)$ mit $A = S^t\overline{S}$.

c) Ist $U \le V$, 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 5.2.6 für $m = 0$.

b) Sei $\mathcal{B}$ die Standardbasis von K^n und $\mathcal{B}'$ eine ONB bzgl. des Skalarproduktes β_A ($\beta_A(v, w) = v^tA\overline{w}$ ist Skalarprodukt nach 5.1.6 und 5.1.1). Nach 5.1.7 existiert $T \in GL_n(K)$ mit $E_n = G_{\mathcal{B}'}(\beta_A) = T^tG_{\mathcal{B}}(\beta_A)\overline{T} = T^tA\overline{T}$.
$S := T^{-1}$ besitzt das Gewünschte.

c) $(\ , \ )|_{U\times U}$ ist Skalarprodukt auf U. Sei $(v_1, ..., v_m)$ eine ONB von U. Ergänze zu ONB $(v_1, ..., v_m, v_{m+1}, ..., v_n)$ von V nach 5.2.6.
Sei $W := <v_{m+1}, ..., v_n> \Rightarrow U \oplus W = V$
Zu zeigen: $W = U^\perp$
Klar: $W \subseteq U^\perp$ Sei umgekehrt $v \in U^\perp$, $v = \sum\limits_{j=1}^{n} a_jv_j$
$0 = (v, v_k) = \sum\limits_{j=1}^{n} a_j(v_j, v_k) = a_k \ \forall\ 1 \le k \le m$
$\Rightarrow v \in W$
Also gilt $W = U^\perp$ und beide Behauptungen folgen.

Definition 5.2.4 *a) $\varphi \in End_K(V)$ heißt* ***orthogonal****, falls $K = \mathbb{R}$ ist (bzw.* ***unitär****, falls $K = \mathbb{C}$ ist) und es gilt:*

$$(\varphi(v), \varphi(w)) = (v, w) \ \forall v, w \in V$$

b) $A \in \mathbb{R}^{n\times n}$ *heißt* ***orthogonal***, *falls* $A^tA = E_n$.
$A \in \mathbb{C}^{n\times n}$ *heißt* ***unitär***, *falls* $A^t\overline{A} = E_n$.
$O(n) := \{A \in \mathbb{R}^{n\times n} \mid A \text{ orthogonal}\}$ *heißt* ***orthogonale Gruppe***.
$U(n) := \{A \in \mathbb{C}^{n\times n} \mid U \text{ unitär}\}$ *heißt* ***unitäre Gruppe***.

5.2.9 Bemerkung

a) Sei V n-dimensional und $\mathcal{B}$ ein ONB von V. Sei $\varphi \in End_K(V)$ 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 ONB von K^n bzgl. $<,>$.

c) $O(n) \leq GL_n(\mathbb{R}),\ U(n) \leq GL_n(\mathbb{C})$

Beweis

a) Weil $\mathcal{B}$ eine ONB ist, ist $G_{\mathcal{B}}(\ (\ ,\ )\ ) = E_n$, also gilt:

$$(v,w) = \kappa_{\mathcal{B}}(v)^t\overline{\kappa_{\mathcal{B}}(w)} \qquad \forall v,w \in W\ \ (5.1.5\text{ b}))$$

Andererseits ist $\kappa_{\mathcal{B}}(\varphi(v)) = A \cdot \kappa_{\mathcal{B}}(v) \qquad (2.4.5)$

$$\begin{aligned}\Rightarrow (\varphi(v),\varphi(w)) &= \kappa_{\mathcal{B}}(\varphi(v))^t\overline{\kappa_{\mathcal{B}}(\varphi(w))}\\ &= (A\kappa_{\mathcal{B}}(v))^t\overline{(A\cdot\kappa_{\mathcal{B}}(w))}\\ &= \kappa_{\mathcal{B}}(v)^t\cdot A^t\overline{A}\cdot\kappa(w)\end{aligned}$$

Mit $v,w \in V$ durchlaufen $\kappa_{\mathcal{B}}(v), \kappa_{\mathcal{B}}(w)$ ganz K^n $\Rightarrow$ Behauptung

b) Matrixmultiplikation.

c) Klar ist: $O(n) \leq GL_n(\mathbb{R}),\ U(n) \leq GL_n(\mathbb{C})\quad (2.3.22)$

$$\begin{aligned}A,B \in U(n):\ (AB)^t\overline{(AB)} &= B^t(A^t\overline{A})\overline{B}\\ &= B^tE_n\overline{B}\\ &= E_n\\ &\Rightarrow AB \in U(n)\end{aligned}$$

$$\begin{aligned}(A^{-1})^t\overline{(A^{-1})} &= (A^t)^{-1}(\overline{A})^{-1}\\ &= (\overline{A}\cdot A^t)^{-1}\\ &\overset{A^t=\overline{A}^{-1}}{=} (A^t\overline{A})^{-1}\\ &= \overline{E_n} = E_n\end{aligned}$$

Definition 5.2.5 *Sei $A \in \mathbb{C}^{n\times n}$. $A^t := \overline{A}^t$ heißt die zu A __**adjungierte**__ Matrix.*

Definition 5.2.6 *$\varphi \in End_K(V)$ heißt __**selbstadjungiert**__ falls gilt:*

$$(\varphi(v), w) = (v, \varphi(w)) \qquad \forall v, w \in V$$

5.2.10 Bemerkung

Analog zu 5.2.9 gilt: Sei V n-dimensional und $\mathcal{B}$ eine ONB von V. Sei $\varphi \in End_K(V)$, $A := M_{\mathcal{B}}(\varphi)$. Dann gilt:

$$\varphi \text{ selbstadjungiert} \Leftrightarrow \overline{A} = A$$

Beweis

Für $v, w \in V$ gilt:

$$(\varphi(v), w) = \kappa_{\mathcal{B}}(\varphi(v))^t\overline{\kappa_{\mathcal{B}}(w)} = \kappa_{\mathcal{B}}(v)^t A^t \overline{\kappa_{\mathcal{B}}(w)}$$

und

$$(v, \varphi(w)) = \kappa_{\mathcal{B}}(v)^t\overline{\kappa_{\mathcal{B}}\varphi(w)} = \kappa_{\mathcal{B}}(v)^t\overline{A}^t\ \overline{\kappa_{\mathcal{B}}(w)}$$

Also: φ selbstadjungiert $\Leftrightarrow A^t = \overline{A} \Leftrightarrow \overline{A}^t = A$

5.3 Spektralsatz

$K = \mathbb{R},\ \mathbb{C},\ (V,\ (\ ,\ ))$ ein n-dimensionaler euklidischer oder unitärer Raum.

5.3.1 Lemma

Sei $A \in \mathbb{R}^{n\times n}$ symmetrisch. Dann existiert ein $a \in \mathbb{R}$ mit $\chi_A(a) = 0$. (A besitzt einen reellen Eigenwert).

Beweis

$\chi_A \in \mathbb{R}[X] \subseteq \mathbb{C}[X]$
Sei $a \in \mathbb{C}$ mit $\chi_A(a) = 0$ ($\mathbb{C}$ ist algebraisch abgeschlossen).
Sei $0 \neq v \in \mathbb{C}^n$ mit $Av = av$ (v EV zum EW a).

$$\begin{aligned} \Rightarrow a(v^t\overline{v}) &= (av)^t\overline{v} \\ &= (Av)^t\overline{v} \\ &= v^tA^t\overline{v} \\ &= v^tA\overline{v} \\ &= v^t\overline{A}\overline{v} \\ &= v^t\overline{(Av)} \\ &= v^t\overline{av} \\ &= v^t\overline{av} \\ &= \overline{a}(v^t\overline{v}) \end{aligned}$$

Weil $v \neq 0$, ist auch $\underbrace{v^t\overline{v}}_{\langle v,v\rangle} \neq 0 \Rightarrow a = \overline{a}$

5.3.2 Satz (Spektralsatz)

Sei $\varphi \in End_K(V)$ selbstadjungiert. Sei $A \in K^{n\times n}$ und $\overline{A}^t = A$ (d.h. A symmetrisch oder hermite'sch).

a) Es ex. ONB von V, die aus EV von φ besteht.

b) (Satz von der Hauptachsentransformation:) $K = \mathbb{R}$: Es existiert $S \in O(n)$, so dass S^tAS eine Diagonalmatrix ist, deren Diagonaleinträge die EW von A sind.

c) $K = \mathbb{C}$: Es ex. $S \in U(n)$, so dass S^tAS eine Diagonalmatrix ist, deren Diagonaleinträge die EW von A sind.

Beweis

a) Induktion über n:
 $\underline{n=1}$: $\surd$
 $\underline{n>1}$: Sei $\mathcal{B}$ ONB von V, $A = M_{\mathcal{B}}(\varphi)$
 $K = \mathbb{R} \overset{5.2.10}{\Longrightarrow} A^t = \overline{A} \overset{5.3.1}{\Rightarrow}$ es existiert $a_1 \in \mathbb{R} : \chi_\varphi(a_1) = 0$
 $K = \mathbb{C} \overset{\mathbb{C}\text{ alg. abg.}}{\Longrightarrow}$ 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 $W = < v_1 >^{\perp}$

Beh.: w ist φ-invariant.

Bew.:

$$\begin{aligned} \text{Sei } w \in W \Rightarrow (v, 1, \varphi(w)) &= (\varphi(v_1), w) \\ &= (a_1 v_1, w) \\ &= a_1(v_1, w) = 0, \text{ da } w \in < v_1 >^{\perp} \\ &\Rightarrow \varphi(w) \in < v_1 >^{\perp} = w \end{aligned}$$

$(\, , \,)|_{W \times W}$ ist Skalarprodukt, φ_W selbstadjungiert
$\Rightarrow W$ besitzt ONB $(v_2, ..., v_n)$ aus EV von φ_W
$\Rightarrow (v_1, ..., v_n)$ ist ONB aus EV von φ.

b) c) Betrachte $V = K^n$, $< \, , \, >$, $\mathcal{B}$ Standardbasis.
$\varphi = \varphi_A : K^n \to K^n, \; v \mapsto Av, \; A = M_{\mathcal{B}}(\varphi_A)$
$\overset{5.2.10}{\Longrightarrow} \varphi_A$ selbstadjungiert
Sei $\mathcal{B}' = (v_1', ..., v_n')$ ONB aus EV von φ_A.
$\varphi_A(v_j') = a_j v_j', \; 1 \leq j \leq n$
Sei $S = M_{\mathcal{B}}^{\mathcal{B}'}(id_v)$ die Basiswechselmatrix.

$$\Rightarrow \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \overset{2.4.13}{=} M_{\mathcal{B}'}(\varphi_A) = S^{-1} M_{\mathcal{B}}(\varphi_A) S = S^{-1} A S$$

Die Spalten von S sind die v_j', bilden also eine ONB von V

$$\overset{5.2.9 \text{ b)}}{\Longrightarrow} S^{-1} = \overline{S}^t$$

5.3.3 Korollar

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

$\overline{A}^t = A$ (d.h. A symmetrisch oder hermite'sch) $\Rightarrow$ ist diagonalisierbar

5.3.4 Beispiel

Sei $K = \mathbb{R}$. Eine quadratische Gleichung über $\mathbb{R}$ ist eine Gleichung

$$Q : \sum_{j=1}^{n} \sum_{k=1}^{n} a_{jk} x_j x_k + \sum_{j=1}^{n} b_j x_j + a = 0$$

Hierbei ist $A = (a_{jk}) \in \mathbb{R}^{n \times n},\ b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{R}^n,\ a \in \mathbb{R}.$

$x_1, ..., x_n$ 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 $c^t A c + b^t c + a = 0.$

$Q(\mathbb{C}) :=$ Menge der Lösungen von Q

$Q(\mathbb{C})$ heißt **Quadrik**.

$Q(\mathbb{R}) := Q(\mathbb{C}) \cap \mathbb{R}^n$: reelle Funktion von $Q(\mathbb{C})$.

Geometrische Beschreibung von $Q(\mathbb{R})$

Spezialfall: $A = A^t,\ b = 0$

$Q : x^t A x + a = 0,\ x \in \mathbb{C}^n$

Nach 5.3.2 b) existiert $S \in O_n(\mathbb{R})$ sind

$$S^{-1}AS := S^tAS = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

Mit $c' := Sc$ für $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in \mathbb{R}^n$ gilt damit:

$$\begin{aligned} & (c')^t A c' + a = 0 \\ \Leftrightarrow\ & c^t(S^tAS)c + a = 0 \\ \Leftrightarrow\ & \left(\sum_{j=1}^{n} a_j c_j^2\right) + a = 0 \end{aligned}$$

Mit $Q' = \sum\limits_{j=1}^{n} a_j c_j^2 + a = 0$ haben wir $Q(\mathbb{R}) = S \cdot Q'(\mathbb{R})$. Koordinatentransformation

$$x' := Sx,\ x \in \mathbb{R}^n$$

bildet $e_1, ..., e_n$ (Standardbasis von $\mathbb{R}^n$ ab auf die ONB $e'_1, ..., e'_n$ mit $e'_j = Se_j$ (Spalte j von S).

$<e'_1>$, ..., $<e'_n>$ heiß ein **System von Hauptachsen für Q**.

(vergl. Satz 5.3.2 b)).

5.4 Orthogonale Endomorphismen

$K = \mathbb{R}$ $\quad (V,\ (,))$ n-dimensionaler euklidischer Raum

5.4.1 Bemerkung

Sei $A \in O(2)$. Dann existiert $\alpha \in \mathbb{R} \quad 0 \leq \alpha \leq 2\pi$ mit:

$$(1) \qquad A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

oder

$$(2) \qquad A = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$$

Im Fall (1) ist $\varphi_A : \mathbb{R}^2 \to \mathbb{R}^2$ eine Drehung um den Winkel α und $\chi_A = X^2 - 2 \cdot \cos\alpha X + 1$.

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 zur $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ (vgl. 4.2.2).

Beweis

Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \overset{A \in O(2)}{\Longrightarrow}$

$$\begin{aligned} a^2 + c^2 &= 1 & & a^2 + b^2 = 1 \\ b^2 + d^2 &= 1 & \text{und} \quad & c^2 + d^2 = 1 \\ ab + cd &= 0 & & \end{aligned}$$

$\Rightarrow$ Einsetzen von α wie behauptet.

(1) $\varphi_A(e_1) = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \ \varphi_A(e_2) = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$

Auf die Berechnung von χ_A wird hier verzichtet.

(2) $\varphi_A(e_1) = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \ \varphi_A(e_2) = \begin{pmatrix} \sin\alpha \\ -\cos\alpha \end{pmatrix}$

$$\begin{aligned} \chi_A = \begin{vmatrix} X - \cos\alpha & -\sin\alpha \\ -\sin\alpha & X + \cos\alpha \end{vmatrix} &= X^2 - \cos^2 X - \sin^2\alpha \\ &= X^2 - 1 = (X-1)(X+1) \end{aligned}$$

Die Behauptung folgt aus 4.2.4 b) und 4.2.2.

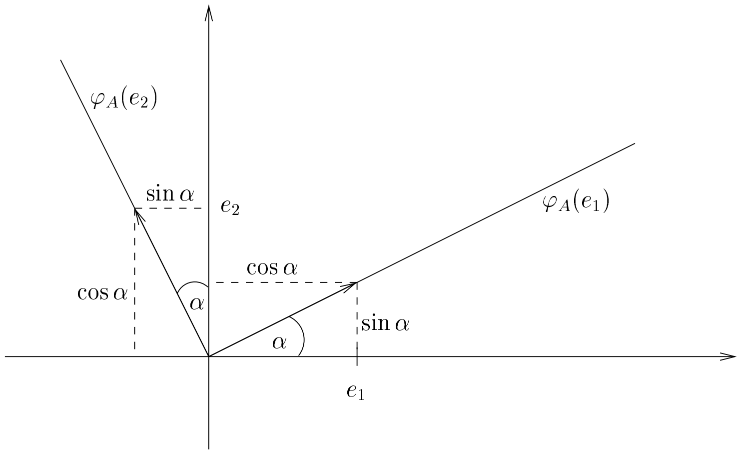

Abbildung 5.4: zu 5.4.1 (1)

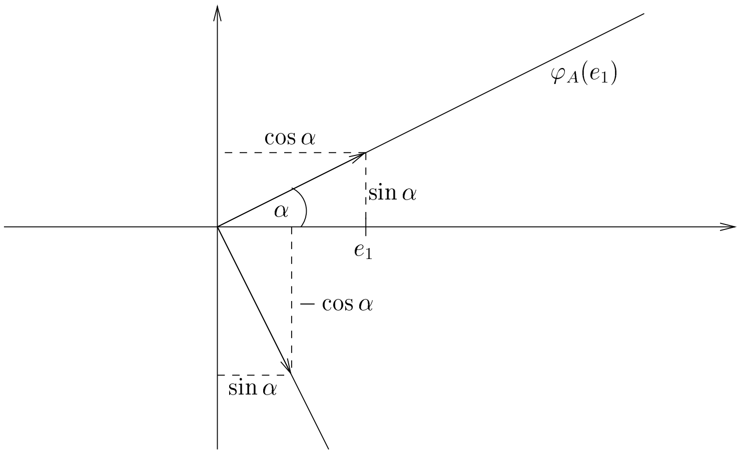

Abbildung 5.5: zu 5.4.1 (2)

5.4.2 Bemerkung

Sei $f \in \mathbb{R}[X]$ irreduzibel $\Rightarrow \deg(f) \leq 2$

Beweis

Ist f linear, dann o.k.

Sei also $\deg(f) \geq 2$, $\quad f = \sum\limits_{j=1}^{m} a_j X^j \quad a_m \neq 0 \quad m \geq 2$

Sei $z \in \mathbb{C}$ Nullstelle von f, d.h. $0 = \sum\limits_{j=0}^{m} a_j z^j$

$$\Rightarrow 0 = \overline{0} = \sum_{j=0}^{m} \overline{a_j z^j} \sum_{j=0}^{m} a_j \overline{z}^j$$

d.h. $\overline{z}$ ist auch Nullstelle von f.
$z \neq \overline{z}$, sonst wäre $z \in \mathbb{R}$ eine reelle Nullstelle von f und $X - z | f \in \mathbb{R}[X]$.

$$\Rightarrow X - z \neq X - \overline{z} \text{ und } (X - z)(X - \overline{z}) | f \in \mathbb{C}[X]$$

$$(X - z)(X - \overline{z}) = X^2 - (z + \overline{z})X + z\overline{z} \in \mathbb{R}[X]$$

Fassen wir $(X - z)(X - \overline{z})$ für jede Nullstelle z von f zusammen, erhalten wir eine Faktorisierung von f in Faktoren vom Grad 2 $\Rightarrow$ Behauptung in $\mathbb{R}[X]$.

5.4.3 Bemerkung

Sei $\varphi \in End_{\mathbb{R}}(V)$ orthogonal.

a) Ist $W \leq V$ φ-invariant, dann ist auch $W^{\perp}\varphi$-invariant und es gilt: $V = W \oplus W^{\perp}$

b) Es existiert $W \leq V\varphi$-invariant mit $\dim_{\mathbb{R}} W \leq 2$

Beweis

a) Sei $\mathcal{B}$ eine ONB von V und $A = M_{\mathcal{B}}(\varphi)$
$\overset{5.2.9\text{ a)}}{\Longrightarrow}$ A orthogonal $\overset{5.2.9\text{ c)}}{\Longrightarrow}$ A invertierbar und A^{-1} ist orthogonal
$\overset{5.2.9}{\Longrightarrow}$ φ^{-1} ist orthogonal und $\varphi(W) = W,\ \varphi{-}1(W) = W$
Sein nun $w \in W,\ u \in W^{\perp}$

$$\Rightarrow (w, \varphi(u) = (\varphi^{-1}(w), \varphi^{-1}(\varphi(u))) = (\varphi^{-1}(w), u) = 0,$$

da $u \in W^{\perp}$ und $\varphi^{-1}(w) \in W$

$$\Rightarrow \varphi(u) \in W^{\perp}, \text{ d.h. } W^{\perp} \text{ ist } \varphi\text{-invariant}$$

Die zweite Behauptung ist gerade 5.2.8 b).

b) Sei $\chi_f = f_1 \cdots f_r$ mit $f_i \in \mathbb{R}[X]$ normiert, irreduzibel.
Ist f_j linear für ein $j \leq r$, dann hat φ einen EV, also einen 1-dim. φ-invarianter UR.
Sei also $\deg(f_j) = 2\ \forall\ 1 \leq j \leq r$
Sei $0 \neq w \in V \overset{4.4.6}{\Longrightarrow} 0 = \chi_{\varphi}(\varphi)(w) = (f_2(\varphi) \circ ... \circ f_r(\varphi))(w)$
$\Rightarrow$ es ex. $1 \leq j \leq r$ mit

$$\underbrace{(f_{j+1}(\varphi) \circ ... \circ f_r(\varphi))}_{\text{Konvention: } id_V \text{, falls } j = r}(w) \neq 0$$

$f_j(\varphi) \circ (f_{j+1}(\varphi) \circ ... \circ f_r(\varphi))(w) = 0$
$\Rightarrow v \neq 0,\ f_j(\varphi)(v) = 0$
$\Rightarrow <v, \varphi(v)>$ ist φ-invariant

5.4.4 Satz

Sei $\varphi \in End_{\mathbb{R}}(V)$ orthogonal. Dann existiert ONB $\mathcal{B}$ von V mit

$$M_{\mathcal{B}}(\varphi) = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_k \end{pmatrix}$$

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 α_j mit $0 < \alpha_j < 2\pi$

Beweis

Sei $0 \neq W \leq V$ φ-invariant mit $\dim_{\mathbb{R}}(W) \leq 2$
$\overset{??}{\Longrightarrow} V = W \oplus W^{\perp}$ und $W^{\perp}$ ist φ-invariant.
Seien $\mathcal{B}_1 = (v_1, ..., v_j)$ (mit $j = 1, 2$) bzw. $\mathcal{B}_2 = (v_{j+1}, ..., v_n)$ ONB's von W bzw. $W^{\perp}$
$\Rightarrow \mathcal{B} = (v_1, ..., v_n)$ 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.
$n = 1 : \surd$
$n = 2$: Verwende 5.4.1.
Im Fall (2) ist

$$\mathcal{B}_2 = \left(\begin{pmatrix} \cos\frac{\alpha+\pi}{2} \\ \sin\frac{\alpha+\pi}{2} \end{pmatrix}, \begin{pmatrix} \cos\frac{\pi}{2} \\ \sin\frac{\pi}{2} \end{pmatrix} \right)$$

die gesuchte Matrix.

Index