Lineare Algebra 1

Wintersemester 2011/12

Prof. Dr. Alexander Schmidt

30. Januar 2012

getippt von Viktoria Schubert

Inhaltsverzeichnis

Stichwortverzeichnis

L

M

N

O

P

R

S

T

U

V

W

Z

Bemerkungen

Vorlesungen

Di+Do: 9.20 - 10.50 Uhr Inf 252/gHS

Plenarübung

Für Fragen zur Vorlesung:
Mo 14.00 - 16.00 Inf 227 HS 1 (bis etwa Anfang Dezember)
Di 16.00 - 18.00 Inf 230 gHS

Übungsgruppen

- vorrechnen der Übungsaufgaben, 50% der Punkte zur Klausurzulassung
- Klausur: Samstag, 4.2.2012 10.00-12.00 Uhr
- `https://www.mathe.uni-heidelberg.de/muesli`
- jeden Do gibt es einen Zettel mit 4 Übungsaufgaben
- Abgabe in 2er-Gruppen, Partner innerhalb der gleichen Übungsgruppen
- Zettelkästen im Foyer des Mathematischen Instituts INF 288 bis Do 9.15Uhr
- Aufgaben erhältlich: Anmelden bei `https://elearning.uni-heidelberg.de/`
- Dort: Aufgaben, Informationen, allgemeines Forum, Foren zu den Aufgaben

Fragen

- inhaltlich: Plenarübung
- technisch (allgemein): im Moodle stellen
- technisch (persönlich): Dr Witte, Prof. Schmidt
- Sprechstunde:
  - Inf 109 Di 15.00-16.00 Uhr Witte
  - Inf 223 Do 15.00-16.00 Uhr Schmidt

Literaturempfehlungen

- S. Bosch: Lineare Algebra
- F. Lorenz: Lineare Algebra
- G. Fischer: Lineare Algebra

0 Einführung

Lineare Algebra: Lehre von den Vektorräumen und linearen Abbildungen.

0.1 Zahlen

- $\mathbb{N} = \{1, 2, 3, ...\}$
- $\mathbb{N}_0 = \{0, 1, 2, 3, ..\}$
- $\mathbb{Q} = \left\{ \frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{Z}, \frac{p}{q} \text{ ist gekürzter Bruch} \right\}$, rationaler Zähler in $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}$

kann man addieren und multiplizieren, in $\mathbb{Z}, \mathbb{Q}$ kann man subtrahieren, in $\mathbb{Q}$ kann man dividieren (außer durch 0).
Die Erfordernisse der Analysis führen zur Erweiterung von $\mathbb{Q}$ zu den reellen Zahlen $\mathbb{R}$.
Veranschaulichung reelle Zahl $\widehat{=}$ Punkt auf der Zahlengeraden

0.2 Vektorräume

Nach Festlegung eines Koordinatenkreuzes ($\widehat{=}$ 0-Punkt) auf zwei zueinander senkrechter Geraden "Einheitsvektoren" Bild 1 können wir jedem Punkt der Ebene als Paar reeller Zahlen schreiben.

Abbildung 1 – Einheitsvektoren des $\mathbb{R}^2$

Entsprechend Punkte des Raumes $\widehat{=}$ Tripeln reeller Zahlen
Allgemein: $n \in \mathbb{N}$ Ein n-Tupel $(x_1, ..x_n)$ reeller Zahlen heißt Punkt oder Vektor des n-dimensionalen Raumes. $x_1, ..x_n$ nennt man die Komponenten des Vektors $(x_1, ..x_n)$. Die Gesamtheit dieser n-Tupel wird mit $\mathbb{R}^n$ bezeichnet.
Was kann man mit Vektoren tun?

0.2.1 Vektoraddition

$$(x_1, ..x_n) + (y_1, ..y_n) = (x_1 + y_1, ..., x_n + y_n)$$

0.2.2 Skalarmultiplikation

$\alpha \in \mathbb{R}$ (ein sogenannter Skalar) $x = (x_1, .., x_n) \in \mathbb{R}^n \Rightarrow$

$$\alpha x = (\alpha x_1, ...\alpha x_n)$$

0.2.3 Skalarprodukt

Sei $x = (x_1, ..x_n), y = (y_1, ..y_n)$ dann:

$$\langle x, y \rangle = x_1 y_1 + + x_n y_n \quad n \in \mathbb{R}$$

heißt das (Standard)skalarprodukt von x und y.
Bemerkung: All dies kann man auch mit $\mathbb{Q}$ anstelle von $\mathbb{R}$ machen.
Besonderheit: $n = 3$

0.2.4 Vektorprodukt oder Kreuzprodukt

$x = (x_1, x_2, x_3), y = (y_1, y_2, y_3) \in \mathbb{R}^3$

$$x \times y = (x_2 y_3 - x_3 y_2, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1) \in \mathbb{R}^3$$

0.2.5 Elementare Eigenschaften

Sei $O_{\mathbb{R}^n} = (0, ..., 0) \in \mathbb{R}^n$ dann gilt:

1. $(x + y) + z = x + (y + z)$ für bel. $x, y, z \in \mathbb{R}^n$ (Assoziativität)
2. $0_{\mathbb{R}^n} + x = x$ für alle $x \in \mathbb{R}^n$ (neutrales Element)
3. $x + y = y + x$ für alle $x, y \in \mathbb{R}^n$ (Kommutativität)
4. $\alpha \cdot (\beta \cdot x) = (\alpha \cdot \beta) \cdot x$ für beliebige $\alpha, \beta \in \mathbb{R}, x \in \mathbb{R}^n$
   $\alpha \cdot (\beta \cdot x)$: im $\mathbb{R}^n$, $(\alpha \cdot \beta) \cdot x$ im $\mathbb{R}$ (Verträglichkeit der Multiplikatoren)
5. $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$, $\alpha, \beta \in \mathbb{R}, x \in \mathbb{R}^n$ (erstes Distributivgesetz)
6. $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$,, $\alpha \in \mathbb{R}$, $x, y \in \mathbb{R}^n$ (zweites Distributivgesetz)
7. Wirkung der $0 \in \mathbb{R}$: $0 \cdot x = 0_{\mathbb{R}^n}$ für $x \in \mathbb{R}^n$
8. Wirkung der $1 \in \mathbb{R}$: $1 \cdot x = x$, $x \in \mathbb{R}^n$

Alle diese Eigenschaften folgen komponentenweise aus den bekannten Rechenregeln für $\mathbb{R}$.

0.2.6 Konventionen

- Punkt geht vor Strichrechnung $(\alpha \cdot x) + (\beta \cdot y) = \alpha \cdot x + \beta \cdot y$
- Das Zeichen "+" wird sowohl für die Addition reeller Zahlen als auch für die Addition von Vektoren verwendet.
- Das Zeichen "$\cdot$" wird sowohl für die Multiplikation in $\mathbb{R}$ als auch für die Skalarmultiplikation verwendet. Man lässt den Punkt oft weg. $\alpha \cdot \beta = \alpha\beta$
- Eigenschaft 1 und 4 erlauben es, Ausdrücke wie $x+y+z$ oder $\alpha\beta x$ ohne Klammern zu schreiben
- oft bezeichnet man den $0_{\mathbb{R}^n} \in \mathbb{R}^n$ einfach nur mit 0
- Geometrische Veranschaulichung:

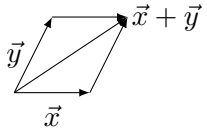


Abbildung 2 – Skalare Multiplikation

- αx = Streckung um den Faktor α:

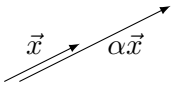


Abbildung 3 – Streckungen

0.3 Eigenschaften des Skalarprodukts

$x = (x_1, ..., x_n), y = (y_1, ..., y_n) \Rightarrow < x, y >= x_1y_2 + ... + x_ny_n$ Für $x, y, z \in \mathbb{R}^n, \alpha \in \mathbb{R}$ gilt:

1. $\langle x + y, z\rangle = \langle x, z\rangle + \langle y, z\rangle$ (Distributivität)
2. $\alpha\langle x, y\rangle = \langle \alpha x, y\rangle$ (Homogenität im ersten Argument)
3. $\langle x, y\rangle = \langle y, x\rangle$ (Symmetrie)
4. $\langle x, x\rangle > 0$ wenn $x \neq 0_{\mathbb{R}^n}$

   1. bis 3. sind offensichtlich

   4. folgt daraus, dass Quadrate nicht negativ sind und $x_1^2 + ... + x_n^2 = 0 \iff x_1 = x_2 = ... = x_n = 0$

Geometrische Veranschaulichung:

Def. 0.1 (Norm von x) $x \in \mathbb{R}^n$

$$\| x \| \stackrel{df}{:=} \sqrt{\langle x, x \rangle}$$

$\| x \|$= *Abstand von x zum Ursprung* 0

Bemerkung: Es gilt $\| \alpha x \| = |\alpha| \cdot \| x \|$

Def. 0.2 (Standardabstand im $\mathbb{R}^n$) $x, y \in \mathbb{R}^n$

$$d(x, y) \stackrel{df}{:=} \| x - y \|$$

Def. 0.3 (Orthogonalität) $x, y \in \mathbb{R}^n$
x und y sind orthogonal ($x \perp y$), wenn

$$\langle x, y \rangle = 0$$

Satz 0.4 (des Pythagoras) *Sind x und y orthogonal zueinander, so gilt:*

$$\| x + y \|^2 = \| x \|^2 + \| y \|^2$$

Beweis:

$$\begin{aligned} \| x + y \|^2 &= \langle x + y \, , \, x + y \rangle \\ &= \langle x, x \rangle + \underbrace{2\langle x, y \rangle}_{=0 \text{ , da orthogonal}} + \langle y, y \rangle \\ &= \| x \|^2 + \| y \|^2 \end{aligned}$$

□

Satz 0.5 (über die Orthogonalprojektion) *Sei $x \in \mathbb{R}^n, x \neq 0$, dann gibt es zu jedem $y \in \mathbb{R}^n$ ein eindeutig bestimmtes $z \in \mathbb{R}^n$ und eine eindeutig bestimmte Zahl $c \in \mathbb{R}$, so dass*

(i) $x \perp z$

(ii) $y = c \cdot x + z$

Beweis (Eindeutigkeit): Falls solche $z \in \mathbb{R}^n, c \in \mathbb{R}$ existieren, so gilt

$$\begin{aligned} \langle y, x \rangle &= \langle cx + z, x \rangle \\ &= \langle cx, x \rangle + \langle z, x \rangle \\ &= c \cdot \| x \|^2 \end{aligned}$$

Wegen $\| x \| \neq 0$ folgt:

$$c = \frac{\langle y, x \rangle}{\| x \|^2}$$

Weiterhin gilt $y = cx + z$, also $z = y - cx$ und somit auch eindeutig bestimmt.

Beweis (Existenz): Eine einfache Rechnung zeigt, dass die oben angegeben c und z die gewünschten Eigenschaften haben:

(i)

$$cx + z = cx + (y - cx) = y$$

□

(ii)

$$\begin{aligned}\langle z, x\rangle &= \langle y - cx, x\rangle \\ &= \langle y, x\rangle - c\langle x, x\rangle \\ &= \langle y, x\rangle - \frac{\langle y, x\rangle}{\| x \|^2}\langle x, x\rangle \\ &= 0\end{aligned}$$

□

0.3.1 Schwarzsche Ungleichung

Für $x, y \in \mathbb{R}^n$ gilt:

$$|\langle x, y\rangle| \leq \| x \| \cdot \| y \|$$

Beweis: Für $x = 0$ sind beide Seiten 0. Sei $x \neq 0$, $c \in \mathbb{R}$, $z \in \mathbb{R}^n$ wie eben, d.h. $y = z + cx$ und $\langle z, x\rangle = 0$. Dann gilt:

$$\begin{aligned}\| y \|^2 &= \langle y, y\rangle \\ \| y \|^2 &= \langle z + cx, z + cx\rangle \\ \| y \|^2 &= c^2 \| x \|^2 + \| z \|^2 \geq c^2 \| x \|^2 = \left(\frac{\langle y, x\rangle}{\| x \|^2}\right)^2 \| x \|^2 = \frac{(\langle y, x\rangle)^2}{\| x \|^2} \\ \| x \| \cdot \| y \| &\geq |\langle x, y\rangle|\end{aligned}$$

0.3.2 Dreiecksungleichung

Für $x, y \in \mathbb{R}^n$ gilt:

$$\| x + y \| \leq \| x \| + \| y \|$$

Beweis:

$$\| x + y \|^2 = \langle x + y, x + y\rangle$$

$$\| x + y \|^2 = \| x \|^2 + 2\langle x, y\rangle + \| y \|^2 \overset{Schwarz.}{\leq} \| x \|^2 + 2 \| x \| \| y \| + \| y \|^2 = (\| x \| + \| y \|)^2$$

Bemerkung: Der Name kommt daher, dass für $x, y, z \in \mathbb{R}^n$ folgt:

$$d(x, z) = \| x - z \| = \| (x - y) + (y - z) \| \leq \| x - y \| + \| y - z \| = d(x, y) + d(y, z)$$

Was ist der Winkel zwischen Vektoren? Beobachtung: Für die Vektoren $x, y \in \mathbb{R}^n$, beide ungleich 0 gilt nach Schwarz:

$$\frac{\langle x, y\rangle}{\| x \| \| y \|} \leq 1$$

Außerdem:

$$-\frac{\langle x, y\rangle}{\| x \| \| y \|} = \frac{\langle x, -y\rangle}{\| x \| \| -y \|} \leq 1$$

Daher gilt:

$$-1 \leq \frac{\langle x, y\rangle}{\| x \| \| y \|} \leq 1$$

Der Kosinus ist eine eineindeutige Funktion im Intervall $[0, \pi]$:

$$\cos [0, \pi] \to [-1, +1]$$

und daher ist die Umkehrfunktion $\cos^{-1} [-1, +1] \to [0, \pi]$ wohldefiniert.

Def. 0.6 (Winkel zwischen Vektoren) *Seien $x, y \in \mathbb{R}^n$ von 0 verschieden, so gilt:*

$$\sphericalangle(x, y) \stackrel{df}{=} \cos^{-1} \left(\frac{\langle x, y \rangle}{\| x \| \cdot \| y \|} \right)$$

Eigenschaften:

$$\sphericalangle(x, y) = \sphericalangle(y, x)$$
$$\sphericalangle(x, x) = 0$$

aus $x \perp y$ folgt $\sphericalangle(x, y) = \frac{\pi}{2}$

Satz 0.7 (Kosinussatz) *Für $x, y \in \mathbb{R}^n \setminus \{0\}$ gilt:*

$$\| x - y \|^2 = \| x \|^2 + \| y \|^2 - 2 \| x \| \cdot \| y \| \cdot \cos (\sphericalangle(x, y))$$

Beweis:

$$\begin{aligned} \| x - y \|^2 &= \langle x - y, x - y \rangle \\ &= \| x \|^2 + \| y \|^2 - 2\langle x, y \rangle \\ &= \| x \|^2 + \| y \|^2 - 2 \| x \| \| y \| \cdot \underbrace{\frac{\langle x, y \rangle}{\| x \| \| y \|}}_{\underbrace{\cos \cos^{-1} \left(\frac{\langle x, y \rangle}{\| x \| \| y \|} \right)}_{\cos(\sphericalangle(x,y))}} \end{aligned}$$

□

0.4 Das Vektorprodukt

für $n = 3$

$$x \times y = (x_2 y_3 - x_3 y_2, x_3 y_1 - x_1 y_3, x_1 y_2 - x_2 y_1)$$

Eigenschaften:

1. Additivität im ersten Argument

$$(x + y) \times z = x \times z + y \times z$$

2. Homogenität im ersten Argument

$$(\alpha x) \times y = \alpha (x \times y)$$

3. Antisymmetrie

$$x \times y = -y \times x$$

Außerdem folgt:

1.' Additivität im zweiten Argument

$$x \times (y + z) = x \times y + x \times z$$

2.' Homogenität im zweiten Argument

$$x \times (\alpha y) = \alpha(x \times y)$$

Weiter:

4. Orthogonalität

$$x \times y \perp x, x \times y \perp y$$

5. Kreuzprodukt gleicher Vektoren

$$x \times x = 0$$

6. Grassmann-Identität

$$\begin{aligned}(x \times y) \times z &= \langle x, z\rangle y - \langle y, z\rangle x \\ &= z \times (y \times x)\end{aligned}$$

7. Jacobi-Identität

$$(x \times y) \times z + (y \times z) \times x + (z \times x) \times y = 0$$

8. Skalarprodukt eines Vektors und einem Kreuzprodukt

$$\langle x \times y, z\rangle = \langle y \times z, x\rangle = \langle z \times x, y\rangle$$

9. Betrag des Kreuzprodukts

$$\| x \times y \|^2 = \| x \|^2 \| y \|^2 \cdot \sin^2(\sphericalangle(x, y))$$

falls $x, y \in \mathbb{R}^3 \setminus \{0\}$

Beweise:

- 4. und 5. rechnet man einfach durch
- 6. Wir zeigen die Grassmann-Identität (nur) in der ersten Komponente, die Rechnung für die zweiter und dritte Komponente sind analog

$$\begin{aligned}((x \times y) \times z)_1 &= (x \times y)_2 z_3 - (x \times y)_3 z_2 \\ &= (x_3 y_1 - x_1 y_3) z_3 - (x_1 y_2 - x_2 y_1) z_2 \\ &= (x_3 z_3 + x_2 z_2) y_1 - (y_2 z_2 + y_3 z_3) x_1 \\ &= (x_1 z_1 + x_2 z_2 + x_3 z_3) y_1 - (y_1 z_1 + y_2 z_2 + y_3 z_3) x_1 \\ &= \langle x, z\rangle y_1 - \langle y, z\rangle x_1\end{aligned}$$

  Das zeigt das erste "="-Zeichen. Das zweite folgt mit 2. und 3.

- Die Jacobi-Identität folgt aus 6. wegen

$$\begin{aligned}(x \times y) \times z + (y \times z) \times x + (z \times x) \times y = &\langle x, z\rangle y - \langle y, z\rangle x + \langle y, x\rangle z \\ &- \langle z, x\rangle y + \langle z, y\rangle x - \langle x, y\rangle z \\ = &\ 0\end{aligned}$$

- Zu 8.:

$$\begin{aligned}\langle x \times y, z\rangle = &\ x_2 y_3 z_1 - x_3 y_2 z_1 + x_3 y_1 z_2 \\ - &\quad x_1 y_3 z_2 + x_1 y_2 z_3 - x_2 y_1 z_3\end{aligned}$$

  Dieser Ausdruck bleibt gleich bei zyklischer Permutation von x, y, z.

- Zu 9.:

$$\begin{aligned}
\| x \times y \|^2 &= \langle x \times y, x \times y \rangle \\
[8. \text{ mit } z = x \times y] \qquad &= \langle y \times (x \times y), x \rangle \\
[3.] \qquad &= -\langle (x \times y) \times y, x \rangle \\
[6.] \qquad &= \langle \langle x, y \rangle y - \langle y, y \rangle x, x \rangle \\
&= \| x \|^2 \| y \|^2 - \langle x, y \rangle^2 \\
&= \| x \|^2 \| y \|^2 \left(1 - \left(\frac{\langle x, y \rangle}{\| x \| \| y \|} \right)^2 \right) \\
&= \| x \|^2 \| y \|^2 \left(1 - \cos^2(\sphericalangle(x, y)) \right) \\
&= \| x \|^2 \| y \|^2 \cdot \sin^2(\sphericalangle(x, y))
\end{aligned}$$

  Geometrische Deutung: $\| x \times y \|$= Volumen des von x und y aufgespannten Parallelogramms. Bezeichnung: $vol(x, y)$. Nach 4. steht $x \times y$ senkrecht auf der Fläche des Parallelogramms. $\Rightarrow$ geometrische Beschreibung des Kreuzprodukts bis auf das Vorzeichen.

0.4.1 Parallelotope

Drei Vektoren $x, y, z \in \mathbb{R}^3$ spannen ein Parallelotop (Spat) auf mit $vol(x, y, z)$.
Schulwissen: $vol(x, y, z) = vol(x, y) \cdot h$, wobei h die Höhe ist. Schreiben wir $z = c \cdot (x \times y) + w$ mit $\langle x \times y, w \rangle = 0$ (Orthogonalprojektion), so gilt:

$$\begin{aligned}
h &= \| c(x \times y) \| \\
h &= |c| \cdot \| x \times y \| \\
h &= \frac{|\langle z, x \times y \rangle|}{\| x \times y \|^2} \| x \times y \| \\
h &= \frac{|\langle z, x \times y \rangle|}{\| x \times y \|}
\end{aligned}$$

Also gilt:

$$\begin{aligned}
vol(x, y, z) &= vol(x, y) \cdot \frac{|\langle z, x \times y \rangle|}{\| x \times y \|} \\
vol(x, y, z) &= |\langle x \times y, z \rangle|
\end{aligned}$$

Def. 0.8 (Spatprodukt) *Das Spatprodukt (=Determinante) dreier Vektoren $x, y, z \in \mathbb{R}^3$ ist die reelle Zahl $\langle x \times y, z \rangle$. ("Volumen mal Vorzeichen")*

Bemerkung: Das Kreuzprodukt im $\mathbb{R}^3$ ist ein Beispiel für eine Operation, die weder kommutativ noch assoziativ ist.
Beispiel:

- $(1, 0, 0) \times (0, 1, 0) = (0, 0, 1)$
- $(0, 1, 0) \times (1, 0, 0) = (0, 0, -1)$
- $((1, 0, 0) \times (1, 0, 0)) \times (0, 1, 0) = (0, 0, 0) \times (0, 1, 0) = (0, 0, 0)$
- $(1, 0, 0) \times ((1, 0, 0) \times (0, 1, 0)) = (1, 0, 0) \times (0, 0, 1) = (0, -1, 0)$

1 Gruppen, Ringe, Körper

1.1 Mengen

Def. 1.1 (Cantor) *Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen*

Bemerkung: Es gibt einen strikten, axiomatischen Zugang zur Mengenlehre.
Schreibweisen für Mengen: $M = \{a, b, c, ...\}$ z.B.

$$\{1, 2, 3\} = \{1, 3, 2\} = \{3, 2, 1\} = \{3, 2, 1, 1\}$$

$a \in M$: a ist ein Element der Menge M
$a \notin M$: a ist kein Element der Menge M
Andere Schreibweise: $M = \{A|B\}$ ist die Menge aller Objekte der Form A, die der Bedingung B genügen. Zum Beispiel: $M = \{x|x \in \mathbb{R}, x \leq 5\}$ oder kürzer $M = \{x \in \mathbb{R}|x \leq 5\}$.

Def. 1.2 (Leere Menge) *Die Leere Menge $\emptyset$ ist die Menge, die kein Element enthält.*

Def. 1.3 (Teilmenge) *Eine Menge N heißt Teilmenge der Menge M ($N \subset M$), wenn M alle Elemente aus N enthält.*

Bsp.:

- $\{1, 2\} \subset \mathbb{N}$
- die leere Menge $\emptyset$ ist Teilmenge jeder Menge

Bemerkung: Anstelle von $N \subset M$ wird auch oft $N \subseteq M$ geschrieben oder auch $N \subseteqq M$. Diese drei Symbole sind gleichwertig. Die Schreibweise $N \subsetneq M$ oder $N \subsetneqq M$ oder $N \subsetneq M$ bedeuten: N ist Teilmenge von M aber nicht gleich M.

Def. 1.4 (Potenzmenge) *Die Menge aller Teilmengen einer Menge M heißt Potenzmenge von M. Schreibweise:*

$$\mathcal{P}(M)$$

Bsp.:

- $M = \{0, 1\} \Rightarrow \mathcal{P}(M) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$
- ist M eine endliche Menge mit n Elementen, so ist $\mathcal{P}(M)$ eine endliche Menge mit 2^n Elementen.

Endlich viele (nicht notwendigerweise endliche) Mengen werden üblicherweise durch Indizes durchnummeriert: $M_1, ..., M_n$. Unendlich viele Mengen werden typischerweise in der Form

$$(M_i)_{i \in I}$$

durchnummeriert wobei I eine Menge ist, die man ihrer Rolle wegen auch Indexmenge nennt. Man sagt $(M_i)_{i \in I}$ sei eine durch I indizierte Familie von Mengen.

Def. 1.5 (Vereinigung, Durchschnitt, Komplement) *Seien K, L Teilmengen einer Menge M und $(M_i)_{i \in I}$ eine Familie von Teilmengen von M. Dann bildet man die folgenden Mengen:*

(i) Vereinigung

$$\bigcup_{i \in I} M_i = \{m \in M| \text{ es gibt } i \in I \text{ mit } m \in M_i\}$$

(ii) Durchschnitt

$$\bigcap_{i \in I} M_i = \{m \in M|m \in M_i \text{ für alle } i \in I\}$$

(iii) Komplement

$$K \backslash L = \{m \in K | m \notin L\}$$

Beispiel: $M = \mathbb{N}$: $\{1,2,3\} \setminus \{3,4,5\} = \{1,2\}$ und $\{1,2\} \setminus \{1,2,3\} = \emptyset$

Def. 1.6 (disjunkte Vereinigung) *Sei $(M_i)_{i \in I}$ eine Familie von Teilmengen einer Menge M. Man sagt M ist die disjunkte Vereinigung der M_i und schreibt*

$$M = \dot{\bigcup_{i \in I}} M_i$$

oder auch

$$M = \dot{\bigsqcup_{i \in I}} M_i$$

wenn $M = \bigcup_{i \in I} M_i$ und $M_i \cap M_j = \emptyset$ für alle $i \neq j$ gilt.

Def. 1.7 (Produktmenge, kartesisches Produkt) *Es seien $M_1, ..., M_n$ Mengen. Die Produktmenge*

$$M_1 \times ... \times M_n$$

besteht aus n-Tupeln $(m_1, ..., m_n)$ mit $m_1 \in M_1, ..., m_n \in M_n$.

- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
- $\mathbb{R} \times \emptyset = \emptyset$

Bem. Def. (1.7) dehnt sich in natürlicher Weise auf eine Familie $(M_i)_{i \in I}$ aus. Schreibweise:

$$\prod_{i \in I} M_i$$

Def. 1.8 (Relation) *Eine Relation R auf einer Menge M ist eine Teilmenge $R \subset M \times M$. Sprechweise: $x, y \in M$ gehen die Relation R ein, wenn $(x, y) \in R$. Schreibweise:*

$$x \sim_R y$$

Bsp.:

1. $M = \mathbb{R}$,$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x < y\}$
2. $M = \mathbb{Z}$, $R = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} | m - n$ ist gerade$\}$
3. $M =$ Menge aller Schüler einer Schule:
   $R = \{(x, y) \in M \times M | x$ und y gehen in die gleiche Klasse $\}$

Def. 1.9 (Äquivalenzrelation) *Sei M eine Menge und R eine Relation auf M. R heißt Äquivalenzrelation (ÄR), wenn die folgenden Bedingungen erfüllt sind:*

Ä1 Reflexivität: $x \sim_R x$ für alle $x \in M$

Ä2 Symmetrie: $x \sim_R y \Rightarrow y \sim_R x$

Ä3 Transitivität: $x \sim_R y$ und $y \sim_R z \Rightarrow x \sim_R z$

Bsp.:

- die Relation in Bsp. 1 ist nicht reflexiv, nicht symmetrisch, aber transitiv

- die Relationen in Bsp. 2 und 3 sind ÄR

Bemerkung: Auf jeder Menge existiert die (nutzlose) ÄR "=", d.h.

$$R = \{(x, y) \in M \times M | x = y\}$$

Def. 1.10 (Äquivalenzklasse) *Sei M eine nichtleere Menge und R eine ÄR auf M. Eine nichtleere Teilmenge $A \subset M$ heißt Äquivalenzklasse, wenn*

- $a, b \in A \Rightarrow a \sim_R b$
- *($a \in A$ und $a \sim_R b$)* $\Rightarrow b \in A$

Lemma 1.11 *Ist R eine ÄR auf M, so gehört jedes $x \in M$ zu genau einer Äquivalenzklasse (ÄK). Insbesondere gilt für die ÄK A, A', dass entweder $A = A'$ oder $A \cap A' = \emptyset$.*

Beweis:

1. Es gibt eine ÄK die x enthält.

   $$A := \{a \in M | x \sim_R a\}$$

   Wegen $x \sim_R x$ (Ä1) gilt $x \in A$, insbesondere gilt $A \neq \emptyset$. Es verbleibt Bedingung (i), (ii) aus Def. 1.10 zu verifizieren

   (i) Seien $a, b \in A$. Dann gilt: $x \sim_R a$, $x \sim_R b$. Aus Ä2 folgt: $a \sim_R x$ und Ä3 liefert $a \sim_R b$

   (ii) Sei $a \in A$ und $a \sim_R b$. Zu zeigen: $b \in A$. Nach Definition gilt:

   $$x \sim_R a \overset{\text{Ä3}}{\Rightarrow} x \sim_R b \Rightarrow b \in A$$

2. Zu zeigen: ($x \in A$ und $x \in A'$) $\Rightarrow A = A'$ wir zeigen $A \subset A'$. Der Nachweis $A' \subset A$ ist dann aus Symmetriegründen der selbe und es gilt:

   $$(A \subset A' \text{und} A' \subset A) \Rightarrow A = A'$$

   Sei nun $a \in A$, dann gilt wegen $x \in A$, dass $a \sim_R x$. Wegen $x \in A'$ folgt $a \in A'$. □

Bemerkung: M zerfällt also in die disjunkte Vereinigung der ÄK bezüglich R.

Def. 1.12 (Menge der Äquivalenzklassen) *Die Menge der ÄK einer Menge M bezüglich einer ÄR R wird mit M/R bezeichnet.*

Beispiele:

- In Beispiel zwei nach Def 1.8 gibt es zwei Äquivalenzklassen
  - $A_{gerade} = \{..., -4, -2, 0, 2, 4, ...\}$
  - $A_{ungerade} = \{..., -3, -1, 1, 3, ...\}$
- In Beispiel drei nach Def 1.8 ist die Menge der ÄK die Menge der Schulklassen der Schule
- Wie man $\mathbb{Z}$ aus $\mathbb{N}$ konstruiert
  Wir betrachten die ÄR $\sim$ auf $\mathbb{N} \times \mathbb{N}$.

  $$(m, n) \sim (m', n') \Longleftrightarrow m + n' = m' + n$$

  Dann gilt $\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim$ Wir Identifizieren die ÄK des Paares (m, n) mit der ganzen Zahl $m - n$.
- Sei $n \in \mathbb{N}$. Wir betrachten die Relation auf $\mathbb{Z}$ $a \sim b \Longleftrightarrow n | (a - b)$ Dies ist eine ÄR, denn

  Ä1 $a - a = 0 \quad n|0$, also $a \sim a$

Ä2 $a \sim b \Rightarrow n|(a-b) \Rightarrow n|(b-a) \Rightarrow b \sim a$

Ä3 $(a \sim b)$ und $(b \sim c) \Rightarrow n|(a-b)$ und $n|(b-c) \Rightarrow n|(a-b)+(b-c) = n|a-c$

Es gibt genau n verschiedene ÄK, die mit $\overline{0}, \overline{1}, ..., \overline{n-1}$ bezeichnet werden. Die Menge der ÄK heißt Menge der *Restklassen modulo n*. Bez: $\mathbb{Z}/n\mathbb{Z}$. Man schreibt $a \equiv b \mod n$, wenn $n|(a-b)$.

Def. 1.13 (Abbildungen) *Eine Abbildung*

$$f : M \to N$$

einer Menge M in eine Menge N ist eine Vorschrift, die jedem Element $m \in M$ genau ein Element $f(m) \in N$ zuordnet.

Beispiel:

- $q : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x^2$
- Ist $M \subset N$ eine Teilmenge, so gibt es die kanonische Inklusionsabbildung

$$i : M \to N$$
$$m \,(\text{aufgefasst als Element von } M) \mapsto m \,(\text{aufgefasst als Element von } N)$$

  - z.B $\{0,1,2\} \to \{0,1,2,3\}$
  - Ist $M = N$, so ist dies die sogenannte Identitätsabbildung

$$id : M \to N \,, m \mapsto m$$

Def. 1.14 (Gleiche Abbildungen) *Zwei Abbildungen $f, g : M \to N$ heißen gleich, wenn $f(m) = g(m) \forall m \in M$*

Beispiel: $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 + 2x + 1$, $g(x) = (x+1)^2$ sind gleich

Def. 1.15 (Urbildmenge, Bild) *Sei $f : M \to N$ eine Mengenabbildung*

(i) Für $n \in N$ heißt die Teilmenge $f^{-1}(n) := \{m \in M | f(m) = n\} \subset M$ die Urbildmenge von n. Die Menge der $n \in N$ mit $f^{-1}(n) \neq \emptyset$ heißt das Bild von f. Bezeichnung: $f(M)$ oder Bild(f) oder im(f) (von Image).

(ii) f heißt *injektiv*, wenn gilt: $m \neq m' \Rightarrow f(m) \neq f(m')$ (Äquivalent: Für jedes $n \in N$ enthält das Urbild f^{-1} höchstens ein Element)

(iii) f heißt *surjektiv*, wenn zu jedem $n \in N$ ein $m \in M$ mit $f(m) = n$ existiert. (Äquivalent: $f^{-1}(n) \neq \emptyset$ für alle $n \in N$

(iv) f heißt *bijektiv*, falls es surjektiv und injektiv ist. (Äquivalent: $f^{-1}(n)$ enthält für jedes $n \in N$ genau ein Element)

Ist $f : M \to N$ bijektiv, so definiert man die Umkehrfunktion $f^{-1} : N \to M$ durch die Regel

$$f^{-1}(n) = \text{DAS Element von } f^{-1}(n)$$

Diese Bezeichnungsdoppelung bringt in der Praxis typischerweise keine Probleme.
Bemerkung: Sei $f : M \to N$ eine Mengenabbildung. Die Eigenschaften injektiv, surjektiv und bijektiv signalisiert man durch Modifikation des Pfeils:

1. injektiv $f : M \hookrightarrow N$
2. surjektiv $f : M \twoheadrightarrow N$
3. bijektiv $f : M \xrightarrow{\sim} N$

Def. 1.16 (kanonische Projektion) *Sei M eine Menge und R eine ÄR auf M, dann ist die kanonische Projektion*

$$p : M \to M/R$$

definiert durch $m \in M$ geht auf die eindeutig bestimmte ÄK $A \in M/R$ mit $m \in A$

Bemerkung: Es gilt: $p^{-1}(A) = A$. Da ÄK per Definition nichtleer sind, ist die kanonische Projektion eine surjektive Mengenabbildung.
Beispiel: Schule, Klasse $12B = \{\text{Albert, Berta,...}\}$. Die kanonische Projektion

$$p : \underbrace{M}_{\text{Menge der Schüler der Schule}} \to \underbrace{M/R}_{\text{Menge der Schulklassen der Schule}}$$

ordnet jedem Schüler seine Klasse zu.

$$\begin{aligned} p^{-1}(12B) &= \text{die Menge der Schüler der Klasse 12B} \\ &= \{\text{Albert, Berta,...}\} \\ &= 12B \end{aligned}$$

Def. 1.17 (Kardinalität) *Sei M eine endliche Menge, dann wird die Anzahl der Elemente von M mit $\sharp M$ oder auch $card(M)$ bezeichnet*[1].

Beispiele:

- $\sharp\emptyset = 0$
- $\sharp\{2, 7, 9\} = 3$

Lemma 1.18 (Kardinalität endlicher Mengen) *Sei $f : M \to N$ eine Abbildung endlicher Mengen, dann gilt:*

(i) ist f injektiv, so gilt: $\sharp M \leq \sharp N$

(ii) ist f surjektiv, so gilt: $\sharp M \geq \sharp N$

(iii) ist f bijektiv, so gilt: $\sharp M = \sharp N$

Lemma 1.19 (Selbstabbildungen) *Sei $f : M \to M$ eine Selbstabbildung einer endlichen Menge M, dann sind die folgenden Aussagen äquivalent:*

(i) f ist injektiv

(ii) f ist surjektiv

(iii) f ist bijektiv

Beweis:

- (i) → (iii): Sei f injektiv, dann gilt für jedes $m \in M$: $\sharp f^{-1}(m) \leq 1$. Nur zerfällt M in die disjunkte Vereinigung der Urbildmengen

  $$M = \dot{\bigcup_{m \in M}} f^{-1}(m)$$

  Daher gilt:

  $$\sharp M = \sum_{m \in M} \sharp f^{-1}(m) \leq \sum_{m \in M} 1 = \sharp M$$

  Daher gilt in der Mitte Gleichheit, also $\sharp f^{-1}(m) = 1$ für alle $m \in M$, d.h. f ist bijektiv.

[1] von Kardinalität, Ordnung

- (ii) $\rightarrow$ (iii) analog, hier haben wir $\sharp f^{-1} \geq 1 \quad \forall m$
- (iii) $\rightarrow$ (i) und (iii) $\rightarrow$ sind trivial $\square$

Die Gesamtheit aller Abbildungen einer Menge M in eine Menge N ist wieder eine Menge und wird mit $Abb(M, N)$ bezeichnet.

Def. 1.20 (Kompositionen) *Seien M, N, K Mengen und $f : M \rightarrow N$, $g : N \rightarrow K$ Abbildungen. Die Abbildungen $g \circ f : M \rightarrow K$, $m \mapsto g(f(m))$ heißt Komposition von f und g.*

Die Komposition kann man als Mengenabbildung auffassen:

$$\begin{aligned} \circ : Abb(M, N) \times Abb(N, K) &\rightarrow Abb(M, K) \\ (f, g) &\mapsto g \circ f \end{aligned}$$

Bemerkung: $Abb(M, N)$ wird auch mit N^M bezeichnet.

Lemma 1.21 (natürliche Bijektion) *Seien I, M Mengen und sei $(M_i)_{i \in I}$ die Familie von (immer gleichen) Mengen $M_i = M$, indiziert durch I. Dann existiert eine natürliche Bijektion*

$$\Phi : M^I \xrightarrow{\sim} \prod_{i \in I} M_i$$

Bemerkung: Die rechte Seite ist die Menge aller Tupel $(m_i)_{i \in I}$, $m_i \in M_i = M$. Die linke Seite ist die Menge der Abbildungen $f : I \rightarrow M$.
Eine solche Abbildung ist dadurch gegeben, dass man jedem $i \in I$ ein $m_i = \underbrace{f(i)}_{\in M}$ zuordnet. Wir definieren Φ durch:

$$f \in M^I \mapsto f(i)_{i \in I} \in \prod_{i \in I} M_i$$

Da die Abbildung f durch ihre Werte $f(i) \in M$, $i \in I$ gegeben ist, ist Φ injektiv. Ist also umgekehrt $(m_i)_{i \in I} \in \prod_{i \in I} M_i$ gebgeben, so ist die Abbildung

$$f : I \rightarrow M, i \mapsto m_i \in M$$

ein Urbild unter Φ. Daher ist Φ auch surjektiv. $\square$

1.2 Gruppen

Def. 1.22 (Verknüpfung) *Eine (binäre) Verknüpfung auf einer Menge M ist eine Abbildung*

$$* : M \times M \rightarrow M, (m, n) \mapsto m * n$$

Def. 1.23 (Gruppe) *Eine Gruppe $(G, *, e)$ ist eine Menge G mit einer Verknüpfung $*$ und einem ausgezeichneten Element $e \in G$, sodass*

G 1 $g * (h * k) = (g * h) * k$ für alle $g, h, k \in G$ (Assoziativität)

G 2 $e * g = g$ für alle $g \in G$ (Existenz eines linksneutralen Elements)

G 3 für alle $g \in G$ existiert ein $h \in G$ mit $h * g = e$ (Existenz eines Linksinversen)

Eine Gruppe G heißt kommutativ oder abelsch, wenn zusätzlich gilt

G 4 $g * h = h * g$ für alle $g, h \in G$

Beispiele:

1. $(\mathbb{Z}, +, 0)$ ist eine abelsche Gruppe
2. $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$,$(\mathbb{C}, +, 0)$ sind abelsche Gruppen

3. $(\mathbb{Q}\setminus\{0\}, \cdot, 1)$ ist abelsche Gruppe

4. $(\mathbb{R} > 0, +, 0)$ ist abelsche Gruppe

5. $(\mathbb{Z}/n\mathbb{Z}, +\overline{0})$ ist eine abelsche Gruppe
   Wie ist die Summe von Restklassen definiert? Vorschrift: Seien $A, B \in \mathbb{Z}/n\mathbb{Z}$

   i Wähle "Vertreter" $a, b \in \mathbb{Z}$ von A, B, d.h. $a \in A, b \in B$

   ii bilde $a + b$ in $\mathbb{Z}$

   iii $A + B \stackrel{df}{=} \overline{a+b}$, d.h. die Restklasse zu der $a + b$ gehört.

   Damit diese Definition widerspruchsfrei ist (Sprich "+" ist wohldefiniert), muss man nachweisen, dass das Ergebnis nicht von der Auswahl von a, b in Schritt 5i abhängt!

6. Die *symmetrische Gruppe* $\mathfrak{S}_n$ (S_n): Sei $n \in \mathbb{N}$:

$$\mathfrak{S}_n \stackrel{df}{=} \text{die Menge aller bijektiven Abbildungen } \pi : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$$

   (so genannte Permutationen)

$$* = \circ \text{ Komposition von Abbildungen}$$
$$e = id_{\{1,2,...,n\}} \text{ die identische Abbildung}$$

   Wir schreiben Permutationen in folgender Form:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \pi(1) & \pi(2) & \pi(3) & ... & \pi(n) \end{pmatrix}$$

   Oben: die natürlichen Zahlen $1, ..., n$ in gewöhnlicher Reihenfolge
   Unten: die natürlichen Zahlen $1, ..., n$ in (eventuell) anderer Reihenfolge
   Umgekehrt definiert ein solches Diagramm eine Permutation - wie viele Permutationen gibt es?

$$\begin{array}{ccc} n & \text{Möglichkeiten für} & 1 \\ n-1 & \text{Möglichkeiten für} & 2 \\ \vdots & & \vdots \\ 1 & \text{Möglichkeit für} & n \end{array}$$

   Daher gilt: $\sharp\mathfrak{S}_n = n(n-1) \cdot ... \cdot 2 \cdot 1 = n!$ (Fakultät) Wir verifizieren G1 bis G3:

   G 1 $g * (h * k) = g \circ (h \circ k) = (g \circ h) \circ k = (g * h) * k$

   G 2 $e * g = id \circ g = g$

   G 3 ist g eine Permutation und h die inverse Abbildung g^{-1}, so gilt:

$$h * g = g^{-1} \circ g = id = e$$

   Für $n \geq 3$ ist $\mathfrak{S}_n$ nicht kommutativ:

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

Satz 1.24 *Sei $(G, *, e)$ eine Gruppe. Dann gilt für alle $g, h, k \in G$:*

1. *aus $g * h = g * k$ folgt $h = k$ (Linkskürzung)*

2. *aus $g * h = k * h$ folgt $g = k$ (Rechtskürzung)*

3. $g * e = e * g = g$ *(das linksneutrale Element ist auch rechtsneutral)*

4. *aus* $g * h = g$ *oder* $h * g = g$ *für ein* $g \in G$ *folgt* $h = e$

5. *für alle* $g \in G$ *gibt es ein eindeutig bestimmtes* $g^{-1} \in G$ *mit* $g^{-1} * g = e = g * g^{-1}$

6. *aus* $h * g = e$ *oder* $g * h = e$ *folgt* $h = g^{-1}$

7. *Es gilt* $(g^{-1})^{-1} = g$

Beweis:

1. Sei $g * h = g * k$. Nach G3 existiert ein $s \in G$ mit $s * g = e$. Daher gilt

$$\left.\begin{array}{r} s * (g * h) \overset{G1}{=} (s * g) * h = e * h \overset{G2}{=} h \\ \text{Analog: } s * (g * k) = (s * g) * k = e * k = k \end{array}\right\} h = k$$

3. $e * g = g$ gilt nach G2. Nach G3 existiert ein $h \in G$ mit $h * g = e$. Daher gilt: $h * (g * e) = (h * g) * e = e * e = e = h * g$. Nach 1. folgt $g * e = g$.

5. Existenz: Sei $h \in G$ mit $h * g = e$ (Existenz nach G3). Dann gilt:
$h * (g * h) = (h * g) * h = e * h = h \overset{3.}{=} h * e$

2. Sei $g * k = h * k$, sei $a \in G$ (nach 5.), sodass $k * s = e$
$\Rightarrow (g * k) * s = g * (k * s) = g * e \overset{3.}{=} g$ Analog: $(h * k) * s = h * (k * s) = h * e = h$. Somit folgt also $g = h$

4. $g * h = g \overset{3.}{=} g * e \overset{1.}{\Rightarrow} h = e$ Analog: $h * g = g = e * g \overset{2.}{\Rightarrow} h = e$

5. Eindeutigkeit: Seien $h, h' \in G$ mit $h * g = e = h' * g$. Mit 2. folgt $h = h'$. $\Rightarrow g^{-1}$ ist eindeutig in G.

6. Seien $h \in G$ mit $g * h = e$. Wegen $g * g^{-1} = e$ folgt mit 1., dass $h = g^{-1}$

7. Aus $g * (g^{-1}) = e$ folgt $g = (g^{-1})^{-1}$

Bemerkung: Sind $g, g' \in G$, so gilt $(g * g')^{-1} = (g')^{-1} * g^{-1}$. Begründung: $\left((g')^{-1} * g^{-1}\right) * (g * g') = (g')^{-1} * e * g' = (g')^{-1} * g' = e$

1.3 Ringe

Def. 1.25 (Ringe) *Ein Ring* $R = (R, +, \cdot, 0_R)$ *ist eine Menge* R *mit zwei Verknüpfungen* $+, \cdot : R \times R \to R$ *und einem ausgezeichneten Element* $0_R \in R$*, sodass*

R1 $(R, +, 0_R)$ *ist eine abelsche Gruppe*

R2 $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in R$

R3 $a \cdot (b + c) = a \cdot b + a \cdot c$ *und* $(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in R$

Ein Ring mit 1 (unitärer Ring) ist ein Tupel $R = (R, +, \cdot, 0_R, 1_R)$ *sodass*

R4 $1_R \cdot a = a = a \cdot 1_R \quad \forall a \in R$

Ein Ring heißt kommutativ, wenn die Multiplikation "·" kommutativ ist, also wenn

R5 $a \cdot b = b \cdot a \quad \forall a, b \in R$

Bemerkung: Das inverse Element von $a \in R$ bezeichnet man mit $-a$.
Beispiele:

1. $(\mathbb{Z}, +\cdot, 0, 1)$ ist ein kommutativer Ring mit 1

2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ analog

3. $\mathbb{Z}/n\mathbb{Z}$ ist ein kommutativer Ring mit 1
   Multiplikationsvorschrift für A, B:

   i Wähle Repräsentanten $a \in A$ und $b \in B$

   ii Bilde $a \cdot b$ in $\mathbb{Z}$

   iii $A \cdot B \stackrel{df}{=}$ Klasse von $a \cdot b$

4. Die Menge der geraden ganzen Zahlen ist ein kommutativer Ring ohne 1

Namensgebung:

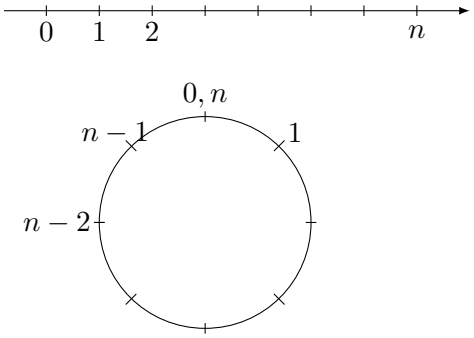


Abbildung 4 – Namensgebung der Ringe

Lemma 1.26 *In einem Ring $R = (R, +, \cdot, 0_R)$ gelten die folgenden Aussagen*

i) $0_R \cdot a = 0_R = a \cdot 0_R$ *für alle* $a \in R$

ii) $a(-b) = -a \cdot b = (-a) \cdot b \quad \forall a, b \in R$

iii) $(-b) = (-1_R) \cdot b \quad \forall b \in R$ *(Falls R unitär ist!)*

Beweis:

i) $0_R \cdot a + 0_R = (0_R + 0_R) \cdot a = 0_R \cdot a + 0_R \cdot a$ Nach kürzen folgt $0_R \cdot a = 0_R$. Analog: $a \cdot 0_R = 0_R$

ii) $0_R = a \cdot 0_R = a(b + (-b)) = ab + a(-b) \Rightarrow$ andere Aussage beweist man analog.

iii) ist R unitär, so setzt man in ii) $a = 1_R$ und erhält iii)

Der Ring $R = \{0\}$ und der einzig möglichen Verknüpfung heißt *Nullring*. Der Nullring ist ein kommutativer Ring mit 1 (Es gilt $0_R = 0 = 1_R$). Dies ist der einzige Ring mit 1, indem $0_R = 1_R$ gilt. Grund: Gilt $0_R = 1_R$, so gilt für jedes $r \in R$: $r = 1_R \cdot r = 0_R \cdot r = 0_R$, dh. $\sharp R = 1$.

Lemma 1.27 *Es sei $R = (R, +, \cdot, 0_R, 1_R)$ ein Ring mit 1 und $R^\times \subset R$ die Menge aller Elemente in R, die sowohl ein Links- als auch ein Rechtsinverses bezüglich der Multiplikation haben, d.h.*

$$R^\times = \{r \in R | \exists s, t \in R : s \cdot r = 1_R = r \cdot t\}$$

Dann ist $R^\times$ die Einheitengruppe von R.

Beweis: Multiplikation führt nicht aus $R^\times$ heraus: Seien $r, r' \in R^\times$ und $s, s', t, t' \in R$ mit $s \cdot r = 1 = r \cdot t$, $s' \cdot r' = 1 = r' \cdot t'$. Dann gilt:

$$(s' \cdot s) \cdot (r \cdot r') = s' \cdot (s \cdot r) \cdot r' = s' \cdot 1 \cdot r' = s' \cdot r' = 1$$
$$(r \cdot r') \cdot (t' \cdot t) = r \cdot (r' \cdot t') \cdot t = r \cdot 1 \cdot t = r \cdot t = 1$$

Daher gilt $r \cdot r' \in R^\times$. Wir weisen jetzt die Gruppenaxiome nach.

G1 folgt aus R2

G2 1_R ist ein neutrales Element und $1_R \in R^\times$

G3 Bleibt zu zeigen: $\forall r \in R^\times$ existiert $r' \in R^\times$ mit $r \cdot r' = 1$:
Nach Definition existiert ein $s \in R$ mit $s \cdot r = 1$ und wir müssen zeigen, dass $s \in R$, s hat offensichtlich ein Rechtsinverses (r), aber r ist auch linksinvers zu s: Wähle $t \in R$ mit $r \cdot t = 1$. Dann gilt $s = s(r \cdot t) = (s \cdot r)t = t \Rightarrow rs = rt = 1$ □

Bemerkungen:

1. Im Beweis haben wir gesehen, dass für $r \in R^\times$ das Links- und Rechtsinverse übereinstimmen. Dies folgt auch aus Def. 1.25 □
2. Angenommen $0_R \in R^\times$, dann existiert $r \in R$ mit $0_R \cdot r = 1_R$ und es folgt $0_R = 0_R \cdot r = 1_R$, d.h. R ist der Nullring.

1.4 Körper

Def. 1.28 (Körper) *Ein Körper ist ein kommutativer Ring mit 1 $K = (K, +, \cdot, 0_K, 1_K)$, in dem gilt $K^\times = K \setminus \{0\}$.*
In Worten: K ist nicht der Nullring (sonst wäre $0_K \in K^\times$) und jedes von 0_K verschiedene Element besitzt ein Inverses bezüglich der Multiplikation.

Beispiele:

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper
2. $\mathbb{Z}$ ist kein Körper $(\mathbb{Z}^\times = \{\pm 1\})$

Lemma 1.29 *In einem Körper K gilt:*

$$a \cdot b = 0_K \Rightarrow (a = 0_K \text{ oder } b = 0_K$$

Beweis: Sei $a \neq 0_K$, dann existiert ein $a^{-1} \in K$ mit $a^{-1} \cdot a = 1_K$. Es folgt $b = 1_K \cdot b = a^{-1}ab = a^{-1}0_K = 0_K$

Lemma 1.30 *Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper*

Beweis: $\mathbb{Z}/p\mathbb{Z}$ ist kommutativer Ring mit 1. Zu zeigen: jede von $\overline{0}$ verschiedene Restklasse hat ein Inverses bezüglich der Multiplikation. Mit anderen Worten: Für $A \in \mathbb{Z}/p\mathbb{Z}$, $A \neq 0_K$ ist die $\overline{1}$ im Bild der Abbildung

$$\cdot A : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \quad B \mapsto A \cdot B$$

Wir zeigen sogar, dass diese Abbildung surjektiv ist. Nach 1.19 genügt zu zeigen, dass die Abbildung injektiv ist.
Angenommen es gäbe $B, C \in \mathbb{Z}/p\mathbb{Z}$ mit $A \cdot B = A \cdot C$. Zu zeigen: $B = C$. Seien $a, b, c \in \mathbb{Z}$ Vertreter von A, B, C. Wegen $A \neq 0_K$ gilt $p \nmid a$. Wegen $A \cdot B = A \cdot C$ gilt: $ab \equiv ac \, mod \, p \Rightarrow p|a(b-c)$. Weil p Primzahl ist und $p \nmid a$, folgt $p|(b-c)$, also $b \equiv c \, mod \, p$. Also $B = C$ Also ist die Abbildung

$$\cdot A : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$

injektiv, also surjektiv und $\overline{1}$ liegt im Bild. □

Bemerkung: Ist $n \in \mathbb{N}$ keine Primzahl, so ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper.
Beweis: Für $n = 1$ ist $\mathbb{Z}/n\mathbb{Z}$ der Nullring. Sei nun $n > 1$ keine Primzahl, dann existieren $a, b \in \mathbb{N}$ miit $1 < a, b < n$ mit $a \cdot b = n$ Für die Restklassen bedeutet dies $\overline{a} \neq 0, \overline{b} \neq 0$ oder $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{u} = \overline{0}$. Nach Lemma 1.30 ist $\mathbb{Z}/n\mathbb{Z}$ kein Körper. □
Wie man in Beispiel $\mathbb{Z}/n\mathbb{Z}$ sieht, kann es in einem Körper passieren, dass

$$1_K + ... + 1_K = 0_K$$

gilt.

Def. 1.31 (Charakteristik eines Körpers) *Sei K ein Körper. Die kleinste natürliche Zahl n mit $\underbrace{1_K + ... + 1_K}_{n-mal} = 0_K$ heißt Charakteristik von K.*
Notation: $char(K)$
Gibt es eine solche Zahl nicht, so setzt man $char\, K = 0$.

Bemerkungen:

1. $char(K) = 0$ oder $char(K) \geq 2$ (wegen $0_K \neq 1_K$)
   Beweis: Sei $char(K) \neq 0$, also $char(K) \geq 2$, wäre n keine Primzahl, so gäbe es $a, b \in \mathbb{N}$, $1 < a, b < n$ mit $a \cdot b = n$

$$\underbrace{(1_K + ... + 1_k)}_{a-mal} \cdot \underbrace{(1_K + ... + 1_k)}_{b-mal} = \underbrace{(1_K + ... + 1_k)}_{n-mal} = 0_K$$

2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ haben die Charakteristik 0

3. $\mathbb{Z}/p\mathbb{Z}$ hat die Charakteristik p

Satz 1.32
Die Charakteristik eines Körpers K ist entweder 0 oder eine Primzahl.

ist $\underbrace{(1_K + ... + 1_k)}_{a-mal}$ oder $\underbrace{(1_K + ... + 1_k)}_{b-mal}$ gleich 0_K im Widerspruch zur Minimalität von n. □

1.5 Homomorphismen

Homophormismen = strukturerhaltende Abbildungen

Def. 1.33 (Homomorphismen) *Seien $(G, *_G, e_G)$ und $(H, *_H, e_H)$ Gruppen. Eine Abbildung $f : G \to H$ heißt Gruppenhomomorphismus, wenn für alle $g, g' \in G$ gilt:*

$$f(g *_G g') = f(g) *_H f(g')$$

Sind $(R, +_R, \cdot_R, 0_R), (S, +_S, \cdot_S, 0_S)$ Ringe, so heißt eine Abbildung $f : R \to S$ Ringhomomorphismus, wenn für alle $a, b \in R$ gilt:

$$f(a +_R b) = f(a) +_S f(b)$$
$$f(a \cdot_R b) = f(a) \cdot_S f(b)$$

Ein Ringhomomorphismus $f : R \to S$ von Ringen mit 1 $(R, +_R, \cdot_R, 0_R, 1_R), (S, +_S, \cdot_S, 0_S, 1_S)$ heißt unitär, wenn zusätzlich $f(1_R) = 1_S$ gilt.
Eine Abbildung zwischen Körpern heißt Körperhomomorphismus, wenn sie ein unitärer Ringhomomorphismus ist.

Def. 1.34 (Monomorphismen, Epimorphismen, Isomorphismen)
Ein Gruppen- (Ring-, Körper-) homomorphismus heißt injektiv (Monomorphismus) bzw. surjektiv (Epimorphismus), wenn er als Mengenabbildung injektiv bzw. surjektiv ist.
Er heißt Gruppen- (Ring-, Körper-) isomorphismus, wenn er bijektiv (also injektiv und surjektiv) ist.

Bemerkung: Die inverse Abbildung f^{-1} zu einem Gruppen- (Ring-, Körper-) isomorphismus ist wieder ein Gruppen- (Ring-, Körper-) isomorphismus.
Zwei Gruppen (Ringe, Körper) heißen isomorph, wenn es einen Isomorphismus zwischen ihnen gibt.

Lemma 1.35 *Sei $f : (G, *_G, e_G) \to (H, *_H, e_H)$ ein Gruppenhomomorphismus. Dann gilt*

(i) $f(e_G) = e_H$

(ii) $f(g^{-1}) = f(g)^{-1}$ für alle $g \in G$

Beweis:

(i) Es gilt $e_G *_G e_G = e_G$ also $f(e_G) *_H f(e_G) = f(e_G *_G e_G) = f(e_G) = f(e_G) *_H e_H$ Kürzen ergibt: $f(e_G) = e_H$. □

(ii) $e_H \overset{(i)}{=} f(e_G) = f(g *_G g^{-1}) = f(g) *_H f(g^{-1})$. Daher gilt $f(g)^{-1} = f(g^{-1})$ □

Beispiel:

- Ist $(G, *_G, e_G)$ eine Gruppe, so ist die Identität $id : G \to G$ ein Gruppenisomorphismus
- Sind $(G, *_G, e_G) \to (H, *_H, e_H)$ Gruppen, so ist der *triviale* Homomorphismus $f : G \to H, f(g) = e_H \, \forall g \in G$ ein Gruppenhomomorphismus. Er ist genau dann injektiv, wenn $G = \{e_G\}$ gilt und genau dann surjektiv, wenn $H = \{e_H\}$ gilt. Sei $n \in \mathbb{N}$. Die Kanonische Projektion $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ist ein surjektiver, unitärer Ringhomomorphismus. Die kanonische Inklusionsabbildung $\mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sind Körperhomomorphismen.
- Die Exponentialabbildung

  $$(\mathbb{R}, +, 0) \to (\mathbb{R}_{>0}, \cdot, 1); \, t \mapsto e^t$$

  ist ein Gruppenisomorphismus.
- Sei $n \in \mathbb{N}$. Die Abbildung

  $$\mathfrak{S}_n \to \mathfrak{S}_{n+1}$$
  $$\begin{pmatrix} 1 & \dots & n \\ \pi(1) & \dots & \pi(n) \end{pmatrix} \mapsto \begin{pmatrix} 1 & \dots & n & n+1 \\ \pi(1) & \dots & \pi(n) & n+1 \end{pmatrix}$$

  ist ein injektiver Gruppenhomomorphismus.

Def. 1.36 *Eine Teilmenge H einer Gruppe $G = (G, *_G, e_G)$ heißt Untergruppe, wenn sie mit der von G ererbten Struktur eine Gruppe ist, das heißt wenn*

(i) $e_G \in H$

(ii) $h, h' \in H \Rightarrow h *_G h' \in H$

(iii) $h \in H \Rightarrow h^{-1} \in H$

Lemma 1.37 *Sei H eine Untergruppe von G, dann ist die Relation*

$$g \sim_H g' \Leftrightarrow g^{-1} * g' \in H$$

eine Äquivalenzrelation auf G.

Beweis:

1. Reflexivität: $g \sim_H g$, weil $g^{-1} * g = e \in H$
2. Symmetrie: $g \sim_H g' \Rightarrow g^{-1} * g' \in H \Rightarrow (g')^{-1} * g = (g^{-1} * g')^{-1} \in H \Rightarrow g' \sim_H g$
3. Transitivität: $g \sim_H g', g' \sim_H g'' \Rightarrow g^{-1} * g'' = (g^{-1} * g') * ((g')^{-1} * g'') \in H \Rightarrow g \sim_H g''$ □

Bemerkung: Die Äquivalenzklasse eines Elements $g \in G$ besteht aus allen $g' \in G$ der Form $g * h$ mit $h \in H$. Die Menge aller Äquivalenzklassen wird mit g/H bezeichnet ("die Linksnebenklassen zu H").

Def. 1.38 (Kern) *Sei $f : G \to H$ ein Gruppenhomomorphismus. Der Kern von f ist die Teilmenge $ker(f) = \{g \in G | f(g) = e_H\}$.*

Lemma 1.39 *Sei $f : G \to H$ ein Gruppenhomomorphismus, dann gilt:*

(i) $ker(f)$ ist eine Untergruppe von G

(ii) $im(f)$ ist eine Untergruppe von H

(iii) f ist injektiv $\Leftrightarrow$ $ker(f) = \{e_G\}$

(iv) f ist surjektiv $\Leftrightarrow$ $im(f) = H$

Beweis:

(i) $f(e_G) = e_H \Rightarrow e_G \in ker(f)$
$g, g' \in ker(f) \Rightarrow f(g * g') = f(g) * f(g') = e_H$ also $g * g' \in ker(f)$. Aus 1.35 (ii) folgt für $g \in ker(f)$, dass $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$ also $g^{-1} \in ker(f)$ ✓

(ii) $f(e_G) = e_H \Rightarrow e_H \in im(f)$
Seien $h, h' \in im(f)$ und $g, g' \in G$ mit $f(g) = h, f(g') = h'$, dann gilt $f(g * g') = f(g) * f(g') = h * h'$ also $h * h' \in im(f)$. Ist $h = f(g) \in im(f)$, so $h^{-1} = f(g)^{-1} = f(g^{-1}) \in im(f)$ ✓

(iii) $\Rightarrow$ Sei f injektiv. Für $g \in ker(f)$ gilt: $f(e_G) = e_H = f(g)$, also $g = e_G$ das heißt $ker(f) = \{e_G\}$
$\Leftarrow$Sei nun $ker(f) \in \{e_G\}$ und $g, g' \in G$ mit $f(g) = f(g^{-1})$, dann gilt: $f(g * (g')^{-1}) = f(g) * f(g')^{-1} = e_H$, also $g * (g')^{-1} \in ker(f) = \{e_G\}$. Es folgt $g * g'$ das heißt f ist injektiv.✓

(iv) trivial. □

Bemerkung: Jeder Gruppenhomomorphismus $f : G \to H$ induziert einen surjektiven Gruppenhomomorphismus $F : G \twoheadrightarrow im(f)$ durch $F(g) := f(g) \in im(f)$.
Notation: Von jetzt an lassen wir das $*$-Zeichen weg und schreiben gh für $g * h$.

Lemma 1.40 *Sei G eine kommutative Gruppe und $H \subset G$ eine Untergruppe.*

(i) die Menge der Linksnebenklassen zu H wird durch die Verknüpfung

$$(gH)(g'H) = (gg')H$$

zu einer kommutativen Gruppe

(ii) Die kanonische Projektion $p : G \to G/H$ ist ein surjektiver Gruppenhomomorphismus und $ker(p) = H$

Bemerkung: G/H heißt die Faktorgruppe[2] von G nach H.
Bew:

(i) Wohldefiniertheit der Verknüpfung, das heißt zu zeigen gilt: $g_1H = g_2H$ und $g_1'H = g_2'H$, so folgt $(g_1g_1')H = (g_2g_2')H$. Wir wissen $g_1^{-1}g_2 \in H$, $(g_1')^{-1}g_2' \in H$, also:

$$\begin{aligned}(g_1 \cdot g_1')^{-1}(g_2 \cdot g_2') &= ((g_1')^{-1}g_1^{-1})(g_2g_2') \\ &= \underbrace{((g_1')^{-1}g_2'}_{\in H}\underbrace{(g_1^{-1}g_2)}_{\in H} \in H\end{aligned}$$

Die Gültigkeit der Gruppenaxiome wird von G *ererbt*, zum Beispiel gilt $e_{G/H} = e_GH$

(ii) Kanonische Projektion ist stets surjektiv. Dass p ein Homomorphismus ist, folgt aus der Definition. Schließlich gilt:

$$\begin{aligned}ker(p) &= \left\{g \in G | p(g) = e_{G/H}\right\} \\ &= \{g \in G | g \sim_H e_G\} \\ &= \left\{g \in G | e_G^{-1}g \in H\right\} \\ &= \{g \in G | g \in H\} \\ &= H\end{aligned}$$

□

[2]auch Quotientengruppe (von engl.: *quotient group*)

Bemerkung: Ist G nicht kommutativ, so ist die Verknüpfung auf G/H nur unter bestimmten Bedingungen wohldefiniert.

Def. 1.41 (Unterring) *Sei $R = (R, +_R, 0_R, \cdot_R)$ ein Ring und $S \subset R$ eine Teilmenge. S heißt Unterring (oder Teilring), wenn S mit den von R ererbten Strukturen ein Ring ist, das heißt*

- *$0_R \in S$ und $(S, +_R, 0_R)$ ist eine Untergruppe von $(R, +_R, 0_R)$ (das heißt mit s_1, $s_2 \in S$ gilt $s_1 + s_2 \in S$ und s mit $s \in S$ liegt $-s \in S$.*
- *mit $s_1, s_2 \in S$ gilt $s_1 \cdot s_2 \in S$. Ist R unitär, so heißt S unitärer Unterring von R, wenn S unitär ist und es gilt $1_S = 1_R$.*

Beispiele:

- $\mathbb{Z}$ ist ein unitärer Unterring in $\mathbb{Q}$
- $2\mathbb{Z} = \{a \in \mathbb{Z} | 2|a\}$ ist ein (nicht unitärer) Unterring in $\mathbb{Z}$
- $\mathbb{R} \times \mathbb{R}$ mit komponentenweiser Addition und Multiplikation ist ein unitärer Ring, $\mathbb{R} \times \{0\} \subset \mathbb{R} \times \mathbb{R}$ ist ein Unterring, ist unitär, aber *kein* unitärer Unterring, weil $1_{\mathbb{R}\times\mathbb{R}} = (1, 1)$, aber $1_{\mathbb{R}\times\{0\}} = (1, 0)$.

Def. 1.42 (Unterkörper) *Ein Unterkörper eines Körpers ist ein unitärer Teilring, der selbst Körper ist.*

Beispiel: $\mathbb{Q}$ ist ein Teilkörper von $\mathbb{R}$, $\mathbb{R}$ ist ein Teilkörper von $\mathbb{C}$.

Lemma 1.43 *Ist $f : (R, +_R, 0_R, \cdot_R) \to (S, +_S, 0_S, \cdot_S)$ ein Ringhomomorphismus, so gilt $f(0_R) = 0_S$, $f(-a) = -f(a) \, \forall a \in R$*

Beweis: Der Ringhomomorphismus f induziert einen Homomorphismus der "unterliegenden" Gruppe $f : (R, +_R, 0_R) \to (S, +_S, 0_S)$. Alles folgt aus 1.35. □Bemerkung:

- $ker(f) = \{r \in R | f(r) = 0_S\}$ ist ein Unterring in R, der im Allgemeinen nicht unitär ist, auch wenn R unitär ist
- $im(f)$ ist ein Unterring von S. Sind R und S unitär und f ein unitärer Ringhomomorphismus, so ist $im(f)$ ein unitärer Teilring.

Lemma 1.44 *Sei $f : (R, +_R, 0_R, \cdot_R, 1_R) \to (S, +_S, 0_S, \cdot_S, 1_S)$ ein unitärer Ringhomomorphismus, dann gilt:*

$$f(R^\times) \subset S^\times$$

und die dadurch induziert Abbildung $(R^\times, \cdot_R, 1_R) \to (S^\times, \cdot_S, 1_S)$ ist ein Gruppenhomomorphismus.

Beweis: Sei $r \in R^\times$ und $s \in R$ sei ein (Rechts- wie Links-) Inverses, dann gilt:

$$f(s)f(r) = f(sr) = f(1_R) = 1_S$$
$$f(r)f(s) = f(rs) = f(1_R) = 1_S$$

Also gilt $f(r) \in S^\times$, f ist ein unitärer Ringhomomorphismus $\Rightarrow$ $f : R^\times \to S^\times$ ist Gruppenhomomorphismus.

Satz 1.45 *Seien $K = (K, +_K, 0_K, \cdot_K, 1_K)$ und $L = (L, +_L, 0_L, \cdot_L, 1_L)$ Körper und $f : K \to L$ ein Körperhomomorphismus. Dann gilt:*

(i) f ist injektiv

(ii) $char(K) = char(L)$

(iii) $im(f)$ ist ein Teilkörper von L

Beweis:

(i) Nach 1.39 genügt zu zeigen, $ker(f) = \{0\}$. Sei $a \in ker(f), a \neq 0$, dann existiert ein $a^{-1} \in K$ und es gilt $1_L = f(1_K) = f(aa^{-1}) = f(a) \cdot f(a^{-1}) = 0_L \cdot f(a^{-1}) = 0_L$ ↯Dieser Widerspruch zeigt, dass ein solches a nicht existiert, also gilt $ker(f) = \{0_K\}$

(ii) Aus (i) folgt, $\underbrace{1_k + ... + 1_K}_{n\text{-mal}} = 0_K \Leftrightarrow \underbrace{f(1_K) + ... + f(1_K)}_{n\text{-mal}} = f(0_K) \Leftrightarrow \underbrace{1_L + ... + 1_L}_{n\text{-mal}} = 0_L$ Aus der Definition folgt $char(K) = char(L)$.

(iii) $im(f) \subset L$ ist ein unitärer Teilring. Zu zeigen für $y \in im(f), y \neq 0_L$ so gilt $y^{-1} \in im(f)$. Sei nun $y = f(x)$. Wegen $f(0_K) = 0_L$ gilt $x \neq 0_K$, also $x \in K^\times$. Nach 1.44 ist $f : K^\times \to L^\times$ ein Gruppenhomomorphismus. Nach 1.35 (ii)folgt $f(x^{-1}) = f(x)^{-1} = y^{-1}$ also $y^{-1} \in im(f)$ □

Bemerkung: Die induzierte Abbildung $F : K \to f(K), x \mapsto f(x)$ ist ein Körperisomorphismus und man identifiziert K mit $f(K)$. Sprechweise: Der Körper K ist über f in L eingebettet. Im Allgemeinen kann es mehrere Einbettungen von K nach L geben.
Sind $f : G_1 \to G_2$ und $g : G_2 \to G_3$ Gruppenhomomorphismen, so ist die Verknüpfung $g \circ f : G_1 \to G_3$ auch ein Gruppenhomomorphismus. Gleiches gilt für Ring- und Körperhomomorphismen.
Spezialfall: $G_1 = G_2 = G_3$

Def. 1.46 (Gruppenendomorphismen, Gruppenautomorphismen) *Sei G eine Gruppe. Ein Gruppenhomomorphismus $f : G \to G$ heißt Gruppenendomorphismus. Ist f bijektiv, so heißt f Gruppenautomorphismus, analoge Sprechweise für Ringe und Körper*

Bezeichnung: $End(G)$, $End(R)$, $End(K)$, sowie $Aut(G)$, $Aut(R)$, $Aut(K)$.

Lemma 1.47 *Sei G eine Gruppe (R ein Ring, K ein Körper), dann ist $Aut(G)$ bzw. $Aut(R)$ oder $Aut(K)$ mit der Verknüpfung $Aut(G) \times Aut(G) \to Aut(G)$, $(f, g) \mapsto g \circ f$ eine Gruppe. (Analog $Aut(R), Aut(K)$)*

Beweis:

- Wohldefiniertheit: mit f und g ist $g \circ f$ bijektiv
- Assoziativität: $h \circ (g \circ f) = h \circ g \circ f = (h \circ g) \circ f$
- Neutrales Element: id_G
- Inverses: Mit f ist auch f^{-1} ein Gruppenautomorphismus und $f \circ f^{-1} = id_G$ □

Bemerkung: Ist $R = (R, +_R, 0_R, \cdot_R)$ ein Ring, so muss man zwischen Gruppen $Aut(R, +_R, 0_R, \cdot_R)$ (Ringautomorphismus) und $Aut(R, +_R, 0_R)$ (Gruppenautomorphismus) unterscheiden. Die erstere ist Untergruppe der zweiten.

2 Vektorräume

2.1 Definitionen

Sei R ein unitärer Ring.

Def. 2.1 (Modul) *Ein (unitärer, Links-) Modul*[3] *über R ist eine abelsche Gruppe $(M, +_M, 0_M)$ mit einer Operation $R \times M \to M$, $(a, m) \mapsto a \cdot m$, sodass für alle $a, b \in R$, $v, w \in M$ gilt:*

(M1) $a \cdot (b \cdot v) = (a \cdot b) \cdot v$

(M2) $(a + b) \cdot v = a \cdot v + b \cdot v$

(M3) $a \cdot (v + w) = a \cdot v + a \cdot w$

[3] maskulinum, Plural: Moduln

(M4) $1_R \cdot v = v$

Def. 2.2 (Vektorraum) *Ein Modul über einem Körper K heißt K-Vektorraum.*

Beispiele:

1. $\{0\}$ mit der offensichtlichen und einzig möglichen Operation ist ein K-Vektorraum.
2. $(K, +_K, 0_K)$ mit der Operation $K \times K \to K$, $(a, b) \mapsto a \cdot b$ ist ein K-Vektorraum.
3. $K^n = \underbrace{K \times ... \times K}_{n-mal}$ wird zum K-Vektorraum durch $(v_1, ..., v_n) + (w_1, ..., w_n) = (v_1 + w_1, ..., v_n + w_n)$ und $a(v_1, ..., v_n) = (a \cdot v_1, ..., a \cdot v_n)$.
4. $\mathbb{C}$ ist $\mathbb{R}$-Vektorraum, allgemeiner: Ist L ein Körper und $K \subset L$ ein Teilkörper, so ist L ein K-Vektorraum.
5. Die Menge $C^n(R, R)$ der n-mal stetig differenzierbaren Funktionen von $\mathbb{R}$ nach $\mathbb{R} (0 \leq n \leq \infty)$ ist ein $\mathbb{R}$-Vektorraum durch Addition: $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ und Multiplikation: $(a \cdot f)(x) = a \cdot f(x)$

Von jetzt an sei K ein fixierter Körper, den wir manchmal von der Notation ausschließen.

Lemma 2.3 *Sei V ein K-Vektorraum, dann gilt für alle $v \in V$, $a \in K$:*

(i) $0_K \cdot v = 0_V$

(ii) $(-1_K) \cdot v = -v$

(iii) $a \cdot 0_V = 0_V$

Beweis:

(i) $0_V + 0_K \cdot v = 0_K \cdot v = (0_K + 0_K) \cdot v = 0_K \cdot v + 0_K \cdot v$ Kürzen ergibt (i)

(ii) $0_V = 0_K \cdot v = (1_K + (-1_K))v = v + (-1_K)v$

(iii) $a \cdot 0_V = a \cdot (0_V + 0_V) = a \cdot 0_V + a \cdot 0_V$

Def. 2.4 (K-lineare Abbildungen, K-Vektorraumhomomorphismen)
Seien V, W K-Vektorräume. Ein Gruppenhomomorphismus $f : V \to W$ heißt K-lineare Abbildung oder auch K-Vektorraumhomomorphismus, wenn $f(a \cdot x) = a \cdot f(x)$ für alle $x \in V$ gilt. Eine lineare Abbildung heißt Vektorraummonomorphismus, Vektorraumepimorphismus beziehungsweise Vektorraumisomorphismus, wenn sie injektiv, surjektiv beziehungsweise bijektiv ist.
Die Menge der linearen Abbildungen von V nach W wird mit $Hom_K(V, W)$ bezeichnet.
Weitere Notationen: $End_K(V) = Hom_K(V, V)$, General Linear Group: $GL(V) = Aut_K(V) = \{\varphi \in End_K(V) | \varphi$ ist ISO $\}$

Beispiele linearer Abbildungen:

1. $K^n \to K^1 = K$, $(a_1, ..., a_n) \to a_1$
2. $\mathbb{R}^n \to \mathbb{R}$, $x \mapsto \langle x, y \rangle$ für ein fest gewähltes $y \in \mathbb{R}^n$
3. $K^n \to K^{2n}$, $(a_1, ..., a_n) \mapsto (a_1, ..., a_n, a_1, ..., a_n)$
4. $C^0(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$, $f \mapsto \int_0^1 f(x) \mathrm{d}x$
5. $n \geq 1\, C^n(\mathbb{R}, \mathbb{R}) \to C^{n-1}(\mathbb{R}, \mathbb{R})$, $f \mapsto f' = \frac{\mathrm{d}f}{\mathrm{d}x}$ (Ableitung)

Def. 2.5 (Untervektorraum) *Eine Teilmenge V eine K-Vektorraums W heißt Untervektorraum, wenn sie mit der von W ererbten Struktur ein K-Vektorraum ist, das heißt*

(i) V *ist Untergruppe von* W

(ii) $v \in V \Rightarrow a \cdot v \in V \, \forall a \in K$

Beispiel: $V = \left\{(x, y, z) \in \mathbb{R}^3 | x + y + z = 0\right\}$ ist ein Untervektorraum des $\mathbb{R}^3$.

Lemma 2.6 *Sei* $f : V \to W$ *eine* K*-lineare Abbildung, dann gilt:*

(i) $ker(f) \subset V$ ist ein Untervektorraum

(ii) $im(f) \subset W$ ist ein Untervektorraum

Beweis: $ker(f)$ und $im(f)$ sind Untergruppen nach Lemma 1.39.

(i) Für $v \in ker(f)$ gilt $f(a \cdot v) = a \cdot f(v) = a \cdot 0 = 0$ also $a \cdot v \in ker(f)$ für alle $a \in K$

(ii) Für $w = f(v) \in im(f)$ gilt $a \cdot w = a \cdot f(v) = f(a \cdot v) \in im(f)$ □

2.2 Operationen auf Vektorräumen

1. Seien U, V K-Vektorräume und M eine Menge

   - $Abb(M, V)$ wird zum K-Vektorraum durch $(f_1 + f_2)(m) = f_1(m) + f_2(m)$, $(a \cdot f)(m) = a \cdot f(m)$. Neutrales Element: $e(m) = 0_V \, \forall m \in M$, Nullabbildung Bezeichnung: $0 \in Abb(M, V)$
   - $Hom_K(U, V) \subset Abb(U, V)$ ist ein Untervektorraum, weil f_1 und f_2 linear $\Rightarrow f_1 + f_2$ linear: $a \in K$, f linear $\Rightarrow a \cdot f$ ist linear
   - Spezialfall: $V = K$, $Hom_K(U, K) =: U^*$ heißt der *Dualraum* von U. Seine Elemente heißen *Linearformen* auf U.
   - Ist $f : U \to V$ eine lineare Abbildung, so ist die *duale Abbildung* $f^* : V^* \to U^*$, $\varphi \mapsto \varphi \circ f$ linear.

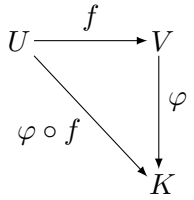


Abbildung 5 – Duale Abbildung

   Die Abbildung $* : Hom_K(U, V) \to Hom_K(V^*, U^*)$, $f \mapsto f^*$ ist linear. Wir haben eine natürliche lineare Abbildung: $U \to (U^*)^*$, $u \mapsto (f \mapsto f(u))$. Dies ist die Auswertungsabbildung.

   - Das kartesische Produkt $U \times V$ wird durch $(u_1, v_1) + (u_2, v_2) = (u_1 + u_2, v_1 + v_2)$ und $a \cdot (u, v) = (a \cdot u, a \cdot v)$ zum K-Vektorraum. Alternative Bezeichnung: $U \oplus V$ (die direkte Summe)

2. Seien $U_1, U_2 \subset V$ Untervektorräume

   - $U_1 \cap U_2$ ist Untervektorraum
   - $U_1 + U_2 := \{u_1 + u_2 | u_1 \in U_1, \, u_2 \in U_2\}$ ist ein Untervektorraum

Lemma 2.7 *Die natürliche Abbildung* $\varphi : U_1 \oplus U_2 \to U_1 + U_2$, $(u_1, u_2) \mapsto u_1 + u_2$ *ist surjektiv und linear. Gilt* $U_1 \cap U_2 = \{0\}$*, so ist* φ *ein Isomorphismus.*

- φ ist linear: Seien $u_1, v_1 \in U_1$, $u_2, v_2 \in U_2$ und $a \in K$:

$$\begin{aligned} \varphi\left((u_1, u_2) + (v_1, v_2)\right) &= \varphi\left((u_1 + v_1, u_2 + v_2)\right) \\ &= u_1 + v_1 + u_2 + v_2 \\ &= (u_1 + u_2) + (v_1 + v_2) \\ &= \varphi((u_1, u_2)) + \varphi((v_1, v_2)) \end{aligned}$$

- Die Surjektivität von φ folgt aus der Definition von $U_1 + U_2$
- Sei $U_1 \cap U_2 = \{0\}$ und $(u_1, u_2) \in ker(\varphi)$, dann gilt $u_1 + u_2 = 0 \Rightarrow u_1 = -u_2$, folglich: $u_1 \in U_2$, $u_2 \in U_1$, also $u_1, u_2 \in U_1 \cap U_2 = \{0\}$. Daher gilt $ker(\varphi) = \{0\}$ und die Injektivität von φ folgt aus 1.39 (ii). □

3. Sei $U \subset V$ ein Untervektorraum. Die Faktorgruppe V/U der Restklassen (= Nebenklassen) $v + U$ von $V \, mod \, U$ wird ein K-Vektorraum durch $a(v + U) = a \cdot v + U$
   - Unabhängigkeit von der Auswahl: Ist $v_1 + U = v_2 + U$, also $v_1 - v_2 \in U$. Folglich $a \cdot v_1 - a \cdot v_2 = a \cdot (v_1 - v_2) \in U$ und daher $a \cdot v_1 + U = a \cdot v_2 + U$

   V/U heißt Faktorvektorraum und die kanonische Projektion $p : V \to V/U$ ist linear.

Satz 2.8 (Universelle Eigenschaft des Faktorraums) *Sei $U \subset V$ ein Untervektorraum und $p : V \to V/U$ die kanonische Projektion. Zu jeder linearen Abbildung $f : V \to W$ mit $U \subset ker(f)$ gibt es eine eindeutig bestimmte lineare Abbildung $\overline{f} : V/U \to W$ mit $f = \overline{f} \circ p$*

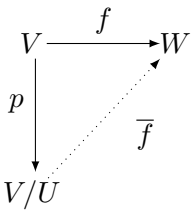


Abbildung 6 – Universaleigenschaft des Faktorraums

Beweis:

- Existenz: Definiere $\overline{f}(v + U) = f(v)$. Wohldefiniertheit: Gilt $v_1 + U = v_2 + U$, so gilt $v_1 - v_2 \in U \subset ker(f)$ Daher: $f(v_1) = f(v_2) + f(v_1 - v_2) = f(v_2) + 0 = f(v_2)$
- Eindeutigkeit: Seien $\overline{f_1}$ und $\overline{f_2}$ zwei solche Abbildungen $v + U \in V/U$ beliebig. Zu zeigen: $\overline{f_1}(v + U) = \overline{f_2}(v + U)$. Wegen $f(v) = \overline{f_1}(p(v)) = \overline{f_1}(v + U)$ und $f(v) = \overline{f_2}(p(v)) = \overline{f_2}(v + U)$ gilt $\overline{f_1}(v + U) = \overline{f_2}(v + U)$ □

Korollar 2.9 *Seien $U \subset V$ Vektorräume und W ein weiterer Vektorraum. Dann gibt es einen natürlichen Isomorphismus von Vektorräumen:*

$$F : \{\varphi \in Hom_K(V, W) | U \subset ker(\varphi)\} \xrightarrow{\sim} Hom_K(V/U, W)$$

Beweis: Die Abbildung F ist durch die Universaleigenschaft des Faktorraums 2.8 gegeben, das heißt $F(\varphi) =: \psi$ ist die eindeutig bestimmte Abbildung mit $\psi(v + U) = \varphi(v) \in W$. Dass F linear ist, folgt direkt aus der Definition. Um zu zeigen, dass F ein Isomorphismus ist, genügt es, eine Umkehrabbilldung anzugeben. Sei $p : V \to V/U$ die kanonische Projektion und für $\psi : V/U \to W$ setze $G(\psi) := \psi \circ p$. Dann gilt $U \in ker(G(\psi))$ und $F \circ G(\psi) = \psi$ und $G \circ F(\varphi) = \varphi$ für alle φ, ψ

Korollar 2.10 *Es gibt einen natürlichen Isomorphismus $(W/im(f))^* = ker(f^* : W^* \to V^*)$*

Beweis: $(W/im(f))^* = Hom_K(W/im(f)) \to K$ und

$$\begin{aligned} ker(f^*) &= \{\varphi : W \to K | f^*(\varphi) = 0\} \\ &= \{\varphi : W \to K | \varphi \circ f = 0\} \\ &= \{\varphi : W \to K | im(f) \subset ker(\varphi)\} \end{aligned}$$

Die Aussage folgt aus 2.9 mit $U = im(f)$ und $W = K$.

Satz 2.11 (Homomorphiesatz für lineare Abbildungen)
Seien V, W Vektorräume und $F : V \to W$ eine lineare Abbildung. Dann gibt es einen natürlichen Vektorraumisomorphismus $f : V/ker(f) \xrightarrow{\sim} im(f)$ mit der Eigenschaft $f = i \circ F \circ p$. Hierbei bezeichnet $p : V \to V/ker(f)$ die kanonische Projektion und $i : im(f) \to W$ die Inklusionsabbildung $V \xrightarrow{p} V/ker(f) \xrightarrow{F}_{\sim} im(f) \xrightarrow{i} W$

Beweis: Nach 2.8 erhalten wir eine lineare Abbildung $\overline{f} : V/ker(f) \to W$ mit $\overline{f}(v + ker(f)) = f(v)$, das heißt $f = \overline{f} \circ p$

- $\overline{f}$ ist injektiv, weil $\overline{f}(v + ker(f)) = 0 \Rightarrow f(v) = 0$ $v \in ker(f) \Rightarrow v + ker(f) = 0 + ker(f)$ ✓
- Das Bild von $\overline{f}$ ist gleich $im(f)$ (klar!)

Daher können wir $\overline{f}$ in der Form $\overline{f} = i \circ F$ mit $F : V/ker(f) \to im(f)$ schreiben. i und $\overline{f}$ sind injektiv, also auch F. Nach Konstruktion ist F surjektiv. Daher ist F ein Isomorphismus und es gilt $f = \overline{f} \circ p = i \circ F \circ p$ □

4. unendliche Familien.
   Seien $(U_i)_{i\in I}$ Untervektorräume in U. Das Kartesische Produkt $\prod_{i\in I} U_i$ wird analog zum Produkt zweier Vektorräume durch komponentenweise Addition und Multiplikation zum Vektorraum.
   Notation: Ist I eine Indexmenge und sind $(a_i)_{i\in I}$ Objekte, die durch I indiziert werden, so sagt man, dass eine Eigenschaft *für fast alle* $i \in I$ erfüllt ist, wenn es eine endliche Teilmenge $J \subset I$ gibt, so dass a_i die Eigenschaft für alle $i \in I\backslash J$ hat. Beispiel:

$$\bigoplus_{i\in I} U_i := \left\{ (u_i)_{i\in I} \in \prod_{i\in I} U_i | u_i = 0 \text{ für fast alle } i \in I \right\}$$

   heißt die *direkte Summe* des Vektorraums U_i und ist ein Untervektorraum im Produkt. Ist I selbst eine endliche Menge, so gilt $\bigoplus_{i\in I} U_i = \prod_{i\in I} U_i$. Ist die Indexmenge I endlich und nicht-leer, nimmt man sich typischerweise eine bijektive Abbildung $I \xrightarrow{\sim} \{1, ..., n\}$ und schreibt $\bigoplus_{i\in I} U_i = \bigoplus_{i=1}^{n} U_i$ und analog für alle anderen Operationen. Konvention: Für Untervektorräume in V:

$$\sum_{i\neq\emptyset} U_i = \{0\}$$
$$\bigcap_{i\neq\emptyset} U_i = V$$

   Sei nun $(U_i)_{i\in I}$ eine Familie von Untervektorräumen eines Vektorraums V, dann haben wir die Untervektorräume

$$\bigcap_{i\in I} U_i = \{u \in U | u \in U_i \text{für alle } i\}$$

   und

$$\sum_{i\in I} U_i = \left\{ \sum_{i\in I} u_i | u_i \in U_i \text{ für alle } i,\ u_i = 0 \text{ für fast alle } i \right\}$$

   Wegen der Bedingung $u_i = 0$ für fast alle i, ist die scheinbar unendliche Summe $\sum_{i\in I} u_i$ nur eine endliche Summe und darum überhaupt erst definiert.

Wir haben gesehen, daß $Hom_K(V, W)$ wieder eine Vektorraumstruktur trägt. Insbesondere ist es eine abelsche Gruppe bzgl. +. Ist $V = W$, so definieren wir auf $Hom_K(V, V) = End_K(V)$ eine Multiplikation durch $\circ$ (Komposition).

Lemma 2.12 *Mit diesen Operationen ist* $(End_K(V), +, \circ, 0, id(V))$ *ein unitärer Ring. Die Abbildung*

$$K \to End_K(V), a \mapsto a \cdot id(V)$$

ist ein unitärer Ringhomomorphismus. Durch die Operation

$$End_K(V) \times V \to V, (f, v) \mapsto f(v)$$

wird V *zu einem (unitären, links)* $End_K(V)$*-Modul .*

Beweis. Wir verifizieren die Ringaxiome für $(End_K(V), +, \circ, 0, id(V))$. Zunächst ist $\circ$ assoziativ. Weiter gilt $g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$ wegen

$$\begin{aligned}(g \circ (f_1 + f_2))(v) &= g((f_1 + f_2)(v)) = g(f_1(v) + f_2(v)) \\ &= g(f_1(v)) + g(f_2(v)) \\ &= g \circ f_1(v) + g \circ f_2(v) = (g \circ f_1 + g \circ f_2)(v)\end{aligned}$$

Analog $(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$. Also ist $End_K(V)$ ein Ring in dem $id(V)$ offenbar ein 1-Element ist. Dass die Abbildung $K \to End_K(V)$, $a \mapsto a \cdot id(V)$, ein Ringhomomorphismus ist, liest man leicht an den Definitionen ab. Die gegebene Operation macht V zu einem $End_K(V)$-Modul weil:

(M1) $g \cdot (f \cdot v) = g(f(v)) = (g \circ f)(v) = (g \cdot f)(v)$

(M2) $(f + g) \cdot v = (f + g)(v) = f(v) + g(v) = f \cdot v + g \cdot v$

(M3) $f \cdot (v + w) = f(v + w) = f(v) + f(w) = f \cdot v + f \cdot w$

(M4) $1_{End_K(V)} \cdot v = (id(V))(v) = v$ □

2.3 Basen

Erinnerung: Eine über eine Indexmenge I indizierte Familie $(m_i)_{i \in I}$ von Elementen einer Menge M ist nichts weiter als eine Abbildung $m : I \to M$ und wir schreiben $m(i) = m_i \in M$ und $m = (m_i)_{i \in I} \in M^I$. Sprechweise: $(m_i)_{i \in I}$ ist ein System von Elementen in M.

Def. 2.13 (endliche Systeme von Skalaren) *Ein System von Skalaren $(\alpha_i)_{i \in I} \in K^I$ heißt endlich, wenn $\alpha_i = 0$ für fast alle i gilt. Die Menge aller endlichen Systeme von Skalaren wird mit $K^{(I)}$ bezeichnet.*

Bemerkung: Sei V ein K-Vektorraum, $(v_i)_{i \in I}$ ein System von Vektoren in V und $(\alpha_i)_{i \in I} \in K^{(I)}$ ein endliches System von Skalaren. Dann gilt $\alpha_i v_i = 0$ für fast alle i, so dass man der Summe $\sum_{i \in I} \alpha_i v_i$ einen Sinn geben kann.

Def. 2.14 *Sei V ein K-Vektorraum, I eine Indexmenge und $v = (v_i)_{i \in I}$ ein System von Vektoren in V . Der Untervektorraum*

$$Lin((v_i)_{i \in I}) = \left\{ \sum_{i \in I} \alpha_i v_i | (\alpha_i)_{i \in I} \in K^{(I)} \right\}$$

heißt die lineare Hülle des Systems $(v_i)_{i \in I}$. Jeder Vektor $v \in Lin((v_i)_{i \in I})$ heißt Linearkombination der v_i. Man nennt $Lin((v_i)_{i \in I})$ auch den von den Vektoren $(v_i)_{i \in I}$ aufgespannten Untervektorraum.

Bemerkung. Setzt man $U_i = Kv_i := \{\alpha v_i | \alpha \in K\}$, so gilt $Lin((v_i)_{i \in I}) = \sum_{i \in I} U_i$.

Def. 2.15 *Sei $(v_i)_{i \in I}$ ein System von Vektoren eines Vektorraums V .*

(i) $(v_i)_{i \in I}$ heißt *Erzeugendensystem* von V , wenn $Lin((v_i)_{i \in I}) = V$ gilt.

(ii) $(v_i)_{i \in I}$ heißt *linear unabhängig*, wenn für jedes endliche System von Skalaren $(\alpha_i)_{i \in I} \in K^{(I)}$ die Implikation $\sum_{i \in I} \alpha_i v_i = 0 \Rightarrow \alpha_i = 0$ für alle $i \in I$ gilt.

(iii) $(v_i)_{i \in I}$ heißt *Basis* von V , wenn es zu jedem Vektor $v \in V$ ein eindeutig bestimmtes endliches System von Skalaren $(\alpha_i)_{i \in I} \in K^{(I)}$ mit $v = \sum_{i \in I} \alpha_i v_i$ gibt.

Lemma 2.16 *Ein System von Vektoren $(v_i)_{i \in I}$ ist genau dann eine Basis von V wenn es ein Erzeugendensystem und linear unabhängig ist.*

Beweis. Sei $(v_i)_{i\in I}$ eine Basis. Da jeder Vektor als Linearkombination der v_i darstellbar ist, gilt $Lin((v_i)_{i\in I}) = V$, d.h. $(v_i)_{i\in I}$ ist ein Erzeugendensystem. Ist nun $(\alpha_i)_{i\in I} \in K^{(I)}$ ein endliches System von Skalaren mit $\sum_{i\in I} \alpha_i v_i = 0$, so gilt wegen $\sum_{i\in I} 0 \cdot v_i = 0$ und der Eindeutigkeit der Darstellung: $\alpha_i = 0$ für alle $i \in I$.
Sei nun $(v_i)_{i\in I}$ ein Erzeugendensystem. Dann ist jeder Vektor Linearkombination der $(v_i)_{i\in I}$. Z.z: ist das System $(v_i)_{i\in I}$ linear unabhängig, so ist die Darstellung jedes Vektors $v \in V$ als Linearkombination der v_i eindeutig.
Seien nun $(\alpha_i), (\beta_i) \in K^{(I)}$ endliche Familien und $\sum \alpha_i v_i = v = \sum \beta_i v_i$. Dann ist die Familie $(\alpha_i - \beta_i)_{i\in I}$ auch endlich und es gilt $\sum_{i\in I}(\alpha_i - \beta_i)v_i = 0 \Rightarrow \alpha_i - \beta_i = 0$ für alle i. Hieraus folgt $\alpha_i = \beta_i$ für alle i. □
Beispiel: Im K^n bilden die Vektoren

$$e_1 = (1, 0, ..., 0),\ e_2 = (0, 1, 0, ..., 0), ..., e_n = (0, ..., 1)$$

eine Basis. Diese heißt die kanonische Basis des K^n . Der Vektor $e_i, (i = 1, ..., n)$, heißt der *i-te Einheitsvektor.*

Lemma 2.17 *Der K-Vektorraum V habe die endliche Basis $(v_1, ..., v_n)$. Dann ist die Abbildung*

$$\varphi : K^n \to V$$
$$(\alpha_1, ..., \alpha_n) \mapsto \sum_{i\in I}^{n} \alpha_i v_i$$

ein Vektorraumisomorphismus.

Beweis. Zunächst ist φ linear.
$v_1, ..., v_n$ linear unabhängig $\Rightarrow ker(\varphi) = 0 \Rightarrow \varphi$ ist injektiv.
$v_1, ..., v_n$ sind Erzeugendensystem $\Rightarrow \varphi$ ist surjektiv. □
Bemerkungen:

- Im Moment wissen wir noch nicht, ob für $n \neq m$ eventuell ein Isomorphismus $K^n \cong K^m$ existieren könnte.
- Aus unseren Konventionen folgt, dass der triviale K-Vektorraum $\{0\}$ die leere Basis hat.
- Jeder Vektorraum V hat ein Erzeugendensystem, z.B. das, welches aus allen Vektoren besteht (wähle $I = V$ und $id : V \to V$).
- Ist $V \neq \{0\}$ und $0 \neq v \in V$, so ist das 1-elementige System (v_1), $v_1 = v$, linear unabhängig ($\alpha_1 v_1 = 0$ und $\alpha_1 \neq 0 \Rightarrow 0 = \alpha_1^{-1}\alpha_1 v_1 = v_1$, Widerspruch).

Def. 2.18 (endlich erzeugte Vektorräume) *Ein Vektorraum V heißt endlich erzeugt, wenn es ein endliches Erzeugendensystem $(v_1, ..., v_n)$ von V gibt.*

Beispiel: K^n ist endlich erzeugt.
Bemerkung. Im Moment wissen wir noch nicht, ob jeder Untervektorraum eines endlich erzeugten Vektorraums wieder endlich erzeugt ist. Später werden wir dies zeigen.

Def. 2.19 (minimales Erzeugendensystem) *Ein Erzeugendensystem $(v_i)_{i\in I}$ eines Vektorraums V heißt minimal, wenn für jede echte Teilmenge $J \subsetneq I$ das System $(v_i)_{i\in J}$ kein Erzeugendensystem ist.*

Beispiel: Das Erzeugendensystem $(e_1, ..., e_n)$ des K^n ist minimal. Lässt man den i-ten Einheitsvektor weg, so kann man nur noch Elemente $(\alpha_1, ..., \alpha_n) \in K^n$ mit $\alpha_i = 0$ als Linearkombination erhalten. Wegen $1 \neq 0$ in K fehlt also z.B. der Vektor $(0, ..., 1, ..., 0)$ (die 1 steht an i-ter Stelle).

Satz 2.20 *Ein Erzeugendensystem ist genau dann minimal, wenn es eine Basis ist.*

Beweis. Sei $(v_i)_{i\in I}$ eine Basis und $J \subsetneq I$ eine echte Teilmenge. Wähle ein $i_0 \in I\backslash J$. Trivialerweise gilt $v_{i0} = 1 \cdot v_{i0}$. Wegen der Eindeutigkeit der Darstellung, lässt sich also v_{i0} nicht als Linearkombination der v_j, $j \in J$, schreiben, und deshalb ist $(v_i)_{i\in J}$ kein Erzeugendensystem. Folglich ist $(v_i)_{i\in I}$ ein minimales Erzeugendensystem.
Sei nun $(v_i)_{i\in I} \in V^I$ ein minimales Erzeugendensystem. Nach 2.17 müssen wir zeigen, dass $(v_i)_{i\in I}$ linear unabhängig ist. Angenommen es gäbe ein von 0 verschiedenes endliches System $(\alpha_i) \in K^{(I)}$ mit $\sum_{i\in I} \alpha_i v_i = 0$. Sei $i_0 \in I$ mit $\alpha_{i0} \neq 0$. Dann gilt

$$-\alpha_{i0} v_{i0} = \sum_{i\in I\backslash\{i0\}} \alpha_i v_i$$

also

$$v_{i0} = \sum_{i\in I\backslash\{i0\}} -\frac{\alpha_i}{\alpha_{i0}} v_i$$

Behauptung: $(v_i)_{i\in I}$ ist auch ein Erzeugendensystem.
Beweis der Behauptung: Sei $v \in V$. Dann existiert eine endliche Familie $\beta_i \in K^{(I)}$ mit $v = \sum_{i\in I} \beta_i v_i$. Nun gilt

$$v = \beta_{i0} v_{i0} + \sum_{i\in I\backslash\{i0\}} \beta_i v_i = \sum_{i\in I\backslash\{i0\}} \left(-\frac{\beta_{i0} \cdot \alpha_i}{\alpha_{i0}} + \beta_i \right) v_i$$

Dies zeigt die Behauptung und wir erhalten einen Widerspruch zur Minimalität des Systems $(v_i)_{i\in I}$.

□

Vorbemerkung: Seien I, J Mengen, dann kann man die *disjunkte Vereinigung* $I \dot\cup J$ bilden. Die Elemente von $I \dot\cup J$ sind die Elemente von I und die Elemente von J. Sind I und J Teilmengen einer gemeinsamen Obermenge M, so gibt es eine natürliche Surjektion $I \dot\cup J \twoheadrightarrow I \cup J$, die genau dann bijektiv ist, wenn $I \cap J = \emptyset$.
Sind nun $(v_i)_{i\in I}$, $(w_j)_{j\in J}$ zwei Systeme von Vektoren eines Vektorraums V, so bezeichnet man das System

$$(u_K)_{k\in I\dot\cup J} = \begin{Bmatrix} v_k,\ k \in I \\ w_k,\ k \in J \end{Bmatrix}$$

als Vereinigung der Systeme $(v_i)_{i\in I}$ und $(w_j)_{j\in J}$

Def. 2.21 *Ein linear unabhängiges System $(v_i)_{i\in I} \in V^I$ heißt maximal, wenn für jedes $v \in V$ das System $(v_i)_{i\in I\dot\cup\{*\}}$ und $v_i = v_i$ für $i \in I$ und $v_* = v$ nicht linear unabhängig ist.*

Satz 2.22 *Ein linear unabhängiges System ist genau dann Basis, wenn es maximal ist.*

Beweis: Sei $(v_i)_{i\in I}$ eine Basis und $v \in V$ beliebig, dann existiert $(\alpha_i) \in K^{(I)}$ mit $v = \sum \alpha_i v_i$. Also $\sum \alpha_i v_i + (-1)v = 0$, weshalb die Vereinigung von $(v_i)_{i\in I}$ mit dem 1-elementigen System (v) nicht linear unabhängig ist. Sei $(v_i)_{i\in I}$ linear unabhängig. Nach 2.16 genügt zu zeigen, dass (v_i) ein Erzeugendensystem ist. Angenommen nicht, dann existiert $v \in V \backslash Lin((v_i)_{i\in I})$.

Behauptung: Das System $(v_i)_{i\in I\cup\{*\}}$ mit $v_i - v_i$ $i \in I$ und $v_* = v$ ist linear unabhängig.
Bweis der Behauptung: Sei $(\alpha_i)_{i\in I\dot\cup\{*\}}$ eine endliche Familie mit $\sum_{i\in I\cup\{*\}} \alpha_i v_i = 0$, dann gilt $\alpha_* v = -\sum_I \alpha_i v_i$. Da $(v_i)_{i\in I}$ linear unabhängig ist, gilt $\alpha_* \neq 0$. Teilen durch α_* zeigt $v \in Lin((v_i)_{i\in I})$. Widerspruch. Dies zeigt die Behauptung. Wegen des Maximums von $(v_i)_{i\in I}$ erhalten wir einen Widerspruch, also $V = Lin((v_i)_{i\in I})$ □

Satz 2.23 (Basisergänzungssatz) *Sei $(v_i)_{i\in I}$ ein Erzeugendensystem des Vektorraums V und $I' \subset I$ eine Teilmenge, sodass das Sytsem $(v_i)_{i\in I'}$ linear unabhängig ist. Dann gibt es eine Teilmenge $J \subset I$ mit $I' \subset J$, sodass $(v_i)_{i\in J}$ eine Basis ist. Insbesondere besitzt jeder Vektorraum eine Basis und jeder endlich erzeugte Vektorraum besitzt eine endliche Basis.*

Beweis: *Insbesonders* sei $(v_i)_{i\in I}$ ein Erzeugendensystem von V und setze $I' = \emptyset$. So erhält man $J \subset I$ mit $(v_i)_{i\in J}$ Basis. War I endlich, so ist dies auch J.
Beweis des Satzes: Strategie: Vergrößere I' bis I' maximal linear unabhängig, also eine Basis ist. Der Einfachheit halber nehmen wir an, dass I endlich ist[4]. Sei nun $(v_1, ..., v_n)$, $n \geq 0$ ein linear unabhängiges System und $(w_1, ..., w_m)$ ein System, sodass V durch $(v_1, ..., v_n, w_1, ..., w_m)$ erzeugt wird. Wir zeigen, es gibt eine Zahl s, $0 \leq s \leq m$ und Indizes $1 \leq j(1) < j(2) < ... < j(s) \leq m$, sodass $(v_1, ..., v_n, w_{j(1)}, ..., w_{j(s)})$ eine Basis ist. Wie starten mit $(v_1, .., v_n)$:

- nehme w_1 zum System dazu, wenn es dadurch linear abhängig wird, entferne w_1 wieder.
- nehme w_2 hinzu...
- usw.
- nehme w_m hinzu...

Wir erhalten ein System $(w_{j(1)}, ..., w_{j(s)})$ mit den folgenden Eigenschaften:

- $(v_1, ..., v_n, w_{j(1)}, ..., w_{j(s)})$ ist linear unabhängig
- wenn man ein weiteres w_j hinzufügt, wird das System linear abhängig

Nach Umnummerierung von $(w_1, ..., w_m)$ sei dieses System $(v_1, ..., v_n, w_1, ..., w_s)$
Behauptung: dieses linear unabhängige System ist Erzeugendensystem, also eine Basis. Beweis der Behauptung: Sei $s < i \leq m$. Nach Konstruktion ist das S $(v_1, ..., v_n, w_1, ..., w_s, w_i)$ linear abhängig. $\Rightarrow$ Existieren $\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_s$, $\beta_i \in K$ mit $\alpha_1 v_1 + ... + \alpha_n v_n + \beta_1 w_1 + ... + \beta_s w_s + \beta_i w_i = 0$ wobei nicht alle Koffizienten gleich 0 sind. Wäre $\beta_i = 0$, so auch alle anderen α_i , β_i wegen der linearen Unabhängigkeit von $(v_1, ..., v_n, w_1, ...w_s)$. Daher gilt $\beta_i \neq 0$ und $w_i = -\beta_i^{-1}(\alpha_1 v_1 + ... + \alpha_n v_n + \beta_1 w_1, ...\beta_s w_s)$. Ein beliebiges Element $v \in V$ kann nach Voraussetzung als Linearkombination von $(v_1, ..., v_n, w_1, ..., w_m)$ geschrieben werden. Nach Substition der w_i, $i > s$ also auch als Linearkombination von $(v_1, .., v_n, w_1, ..., w_s)$ □
Nach 2.17 und 2.23: Jeder Vektorraum ist isomorph zu K^n für $n \in \mathbb{N}_0$ ist n eindeutig bestimmt.

Satz 2.24 *Sei $(v_1, ..., v_n)$ linear unabhängig und $(w_1, ..., w_m)$ eine Basis von V, dann gilt $n \leq m$. In linear unabhängigen Systemen kommt kein Vektor doppelt vor, also gilt:*

$$\sharp\{v_1, ..., v_n\} = n$$
$$\sharp\{w_1, ..., w_m\} = m$$

Sei $k = \sharp(\{v_1, ..., v_n\} \setminus \{w_1, ..., w_m\})$, dann gilt $0 \leq k \leq n$.

Beweis: per Induktion nach k:

IA $k = 0 \Rightarrow \{v_1, ..., v_n\} \subset \{w_1, ..., w_m\}$ ✓

IV Die Aussage sei für beliebige Systeme $(v_1, ..., v_n)$, $(w_1, ..., w_m)$ mit den obigen Eigenschaften und $\sharp(\{v_1, ..., v_n\} \setminus \{w_1, ..., w_m\}) < k$ bewiesen.

IS Sei nun $(v_1, ..., v_n)$, $(w_1, ..., w_m)$ solche Systeme mit $k = \sharp(\{v_1, ..., v_n\} \setminus \{w_1, ..., w_m\})$. Nach Umnummerierung können wir annehmen

- $\{v_1, ..., v_n\} \cap \{w_1, ..., w_m\} = \emptyset$
- $\{v_1, ..., v_n\} \subset \{w_1, ..., w_m\}$

Wir betrachten nun das linear unabhängig $(v_1, ..., v_{k-1}, v_{k+1}, ...v_n)$.
Nach 2.23 gibt es $w_{j(1)}...w_{j(s)}$, sodass $(v_1, ..., v_{k-1}, v_{k+1}, ..., v_n, w_{j(1)}, ..., w_{j(s)})$ eine Basis ist. Wegen $v_k \notin Lin(v_1, ..., v_{k-1}, v_{k+1}, ..., v_n)$ folgt $s \geq 1$ Die Induktionsvoraussetzung angewendet auf $(v_1, ..., v_{k-1}, v_{k+1}, ..., v_n, w_{j(1)}, ..., w_{j(s)})$ und $(w_j, ..., w_m)$ liefert[5] $n - 1 + s \leq m$ und wegen $s \geq 1$ folgt $n \geq m$. □

[4]Beweis im allgemeinen Fall siehe zum Beispiel: *Greub: Lineare Algebra* oder *Breskorn: Lineare Algebra und analytische Geometrie*
[5]Das geht wegen $\sharp(v_1, ..., v_{k-1}, v_{k+1}, v_n, w_{j(1)}, ..., w_{j(s)}) \setminus (w_j, ..., w_m)$

Korollar 2.25 *Sei V ein Vektorraum, der eine Basis aus n Vektoren hat. Dann gilt:*

(i) mehr als n Vektoren sind stets linear abhängig

(ii) jede Basis besteht aus genau n Vektoren

(iii) jedes Erzeugendensystem besteht aus mindestens n Vektoren

Beweis:

(i) folgt aus 2.24

(ii) Ist $(v_1, ..., v_n)$ eine Basis und $(w_1, ..., w_m)$ eine weitere Basis, so zeigt 2.24: $n \leq m$ und $m \leq n$

(iii) Wäre $(w_1, ..., w_m)$, $m < n$ ein Erzeugendensystem, so gäbe es nach 2.23 eine Basis aus weniger als n Vektoren, was (ii) widerspricht. □

Def. 2.26 (Dimension eines Vektorraums) *Ist V ein endlich erzeugter Vektorraum, so nennt man die Kardinalität einer (jeder) Basis die Dimension von V.*
Bezeichnung: $\dim_K V$ *oder einfach* $\dim V$. *Ist V nich endlich erzeugt, so setzt man* $\dim V = \infty$.

- $V = \{0\} \Leftrightarrow \dim V = 0$
- $\dim K^n = n$, insbesondere gilt $K^n \cong K^m \Rightarrow n = m$, da isomorphe Vektorräume die gleiche Dimension haben
- $\dim C^0(\mathbb{R}, \mathbb{R}) = \infty$
  Begründung: Sei $n \in \mathbb{N}$ beliebig und seien $a_0, ..., a_n \in K$ nicht alle 0, dann ist $a_0 + a_1 x + ... + a_n x^n$ nicht das Nullpolynom und hat nur endlich viele Nullstellen. Das bedeutet, dass die $n+1$-Funktionen $1, x, x^2, ..., x^n$ linear unabhängig sind. Daher gilt $\dim_{\mathbb{R}} C^0(\mathbb{R}, \mathbb{R}) > n \, \forall n \in \mathbb{N} \Rightarrow$ Aussage ✓

Satz 2.27 *Sei V ein endlich erzeugter Vektorraum und $W \subset V$ ein Untervektorraum, so ist W endlich erzeugt und es gilt* $\dim W \leq \dim V$. *Die Gleichheit ist äquivalent zu $W = V$*

Beweis: Sei $n = \dim V$. Wir erhalten eine endliche Basis von W wie folgt:

1. $W = \{0\}$ fertig
2. $W \neq \{0\}$. Wähle $w_1 \in W \setminus \{0\}$- Falls (w_1) Basis ist: fertig. Ansonsten ist (w_1) kein maximal linear unabhängiges System und wir finden $w_2 \in W$ und (w_1, w_2) linear unabhängig. (w_1, w_2) Basis: fertig. Ansonsten: Suche w_3 usw. Dieser Prozess bricht ab, weil mehr als n Vektoren in V, also auch in W stets linear abhängig sind.

Wir erhalten eine Basis $(w_1, ..., w_m)$ von W mit $m \leq n$. Im Fall $m = n$ ist $(w_1, ..., w_m)$ ein maximal linear unabhängiges System von Vektoren in V, also $Lin(\underbrace{w_1, ..., w_n}_{=W}) = V$ Von jetzt an benutzen wir den Begriff *endlichdimensionaler* Vektorraum anstelle von endlich erzeugtem Vektorraum.

Lemma 2.28 *Sei $f : V \to W$ eine lineare Abbildung zwischen endlichdimensionalen Vektorräumen, dann gilt:*

(i) f ist injektiv und $(v_1, ..., v_n)$ linear unabhängig in V, so ist $(f(v_1), .., f(v_n))$ linear unabhängig in W. Insbesondere gilt $\dim V \leq \dim W$ *und Gleichheit gilt genau dann, wenn f ein Isomorphismus ist*

(ii) Ist f surjektiv und $(v_1, ..., v_n)$ ein Erzeugendensystem, so ist $(f(v_1), ..., f(v_n))$ ein Erzeugendensystem von W. Insbesondere gilt $\dim V \geq \dim W$ *und Gleichheit gilt genau dann, wenn f ein Isomorphismus ist.*

Beweis:

(i) Sei $(v_1, ..., v_n)$ linear unabhängig in V, dann gilt

$$\sum_{i=1}^{n} \alpha_i f(v_i) = 0 \Rightarrow f\left(\sum_{i=1}^{n} \alpha_i v_i\right) = 0 \Rightarrow \sum_{i=1}^{n} \alpha_i v_i = 0 \Rightarrow \alpha_i = 0,\ i = 1...n$$

Also $(f(v_1), ..., f(v_n))$ linear unabhängig. Ist nun $(v_1, ..., v_n)$ eine Basis von V, so folgt aus der linearen Unabhängigkeit von $(f(v_1), ..., f(v_n))$: $\underbrace{n}_{\dim V} = \dim W$. Da f injektiv ist, induziert f einen Isomorphismus $F : V \xrightarrow{\sim} im(f)$, $v \mapsto f(v) \in W$ und aus $\dim V = \dim im(f)$ folgt f Isomorphismus $\Leftrightarrow im(f) = W \overset{2.27}{\Longleftrightarrow} \dim im(f) = \dim W \Longleftrightarrow \dim V = \dim W$ ✓

(ii) Sei f surjektiv und $(v_1, ..., v_n)$ ein Erzeugendensystem von V. Sei $w = f(v)$ in W beliebig. Dann existieren $\alpha_1 ... \alpha_n \in K$ mit $v = \sum \alpha_i v_i$. Es folgt $w = f(v) = \sum \alpha_i f(v_i) \Rightarrow (f(v_1), ..., f(v_n))$ ist Erzeugendensystem von W. Wählen wir nun eine Basis $(v_1, ..., v_{\dim V})$ so ist $(f(v_1), ...f(v_{\dim V}))$ ein Erzeugendensystem von W. Also $\dim V \geq \dim W$. Ist f ein Isomorphismus, so gilt $\dim V = \dim W$ Umgekehrt gelte $\dim V = \dim W =: n$
Sei $(w_1, ..., w_n)$ ein Basis von W und $w_i = f(v_i)$, $i = 1...n$. Dann ist $(v_1, ...v_n)$ linear unabhängig[6] und wegen $n = \dim V$ maximal linear unabhängig also eine Basis von V. Ist nun $\sum \alpha_i v_i \in ker(f)$, so folgt $\sum \alpha_i w_i = 0 \Rightarrow \alpha_i = 0 \forall i \Rightarrow ker(f) = \{0\}$ und f ist Isomorphismus. □

Korollar 2.29 *Sei V ein endlichdimensionaler Vektorraum und $f : V \to V$ ein Endomorphismus. Dann sind äquivalent:*

(i) f ist injektiv

(ii) f ist surjektiv

(iii) f ist Isomorphismus

Beweis:

(i) Ist f injektiv, so ist f Isomorphismus nach 2.28(i)

(ii) Ist f surjektiv, so ist f Isomorphismus nach 2.28(ii)

(iii) Die anderen Implikationen sind trivial[7] □

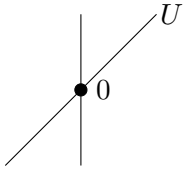
Lemma 2.30 *Sind U, V Vektorräume, so gilt* $\dim(U \oplus V) = \dim U + \dim V$. *Bemerkung: Per Konvention gilt $\infty + n = \infty$, $n + \infty = \infty$ und $\infty + \infty = \infty$.*

Beweis: Gilt $\dim V = \infty$ oder $\dim U = \infty$, so gilt nach 2.27 auch $\dim(U \oplus V) = \infty$. Sind $n = \dim U$ und $m = \dim V$ endlich, $(u_1, ..., u_n)$ eine Basis von U und $(v_1, ..., v_m)$ eine Basis von V, so ist $((u_1, 0), ..., (u_n, 0), (0, v_1), ..., (0, v_m))$ eine Basis von $U \oplus V$. □

Def. 2.31 (Komplement eines Untervektorraums) *Sei V ein Vektorraum und $U \subset V$ ein Untervektorraum. Ein Untervektorraum $U' \subset V$ heißt Komplement zu U, wenn $U \cap U' = \{0\}$ und $U + U' = V$*

Bemerkung: Ist U' ein Komplement zu U, so ist U ein Komplement zu U'.

Im $\mathbb{R}^2$:



Jede andere Gerade durch 0 ist Komplement zu U

Abbildung 7 – Untervektorräume

[6] Grund: $\sum \alpha_i v_i = 0 \Rightarrow \sum \alpha_i f(v_i) = 0 \Rightarrow \alpha_i = 0 \forall i$
[7] nach Definition des Isomorphismus

Satz 2.32 *Sei V ein Vektorraum und $U \subset V$ ein Untervektorraum. Dann existiert ein Komplement zu U.*

Beweis: Sei $(u_i)_{i\in I}$ eine Basis von U. Wir ergänzen diese zu einer Basis $(u_i)_{i\in I\dot\cup J}$ von V. Setze $U' = Lin((u_i)_{i\in J})$. Dann gilt $U \cap U' = \{0\}$, $U + U' = V$ □

Lemma 2.33 *Sei V ein Vektorraum, $U \subset V$ ein Untervektorraum und $U' \subset V$ ein Komplement zu U. Dann ist die natürliche Abbildung $U \oplus U' \to V$, $(u, u') \mapsto u + u'$ ein Isomorphismus. Insbesondere gilt* $\dim V = \dim U + \dim U'$

Beweis: Der Isomorphismus folgt aus 2.7, die Dimensionsformel aus 2.30. □

Satz 2.34 (Dimension des Faktorraums) *Sei V ein endlichdimensionaler Vektorraum und $U \subset V$ ein Untervektorraum, dann ist V/U endlichdimensional und es gilt*

$$\dim V/U = \dim V - \dim U$$

Beweis: Sei U' ein Komplement zu U. Wir betrachten die Kompositionsabbildung

$$\varphi : U' \xrightarrow{i} V \xrightarrow{p} V/U$$

Behauptung: φ ist Isomorphismus. Beweis:

- $ker(\varphi) = ker(p) \cap U' = U \cap U' \Rightarrow \varphi$ ist injektiv
- Sei nun $v + U \in V/U$ beliebig.. Wegen $U + U' = V$ existieren $u \in U$, $u' \in U'$ mit $u + u' = v$, also $u' + U = v + U$. Somit ist u' ein Urbild von $v + U$ unter φ. □

Satz 2.35 (Dimensionsformel für lineare Abbildungen) *Ist $f : V \to W$ eine lineare Abbildung zwischen Vektorräumen, so gilt* $\dim V = \dim ker(f) + \dim im(f)$

Beweis: Nach 2.11 gilt $V/ker(f) \cong im(f)$ (Homomorphiesatz). Die Aussage folgt aus 2.34.

Satz 2.36 *Seien U_1, U_2 Untervektorräume des endlichdimensionalen Vektorraums V, dann gilt:*

$$\dim U_1 + \dim U_2 = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$$

Beweis: Wir betrachten im Beweis von 2.7 die surjektive, lineare Abbildung $p : U_1 \oplus U_2 \to U_1 + U_2$, $(u_1, u_2) \mapsto u_1 + u_2$.
Behauptung: Die Abbildung $i : U_1 \cap U_2 \to ker(\varphi), u \mapsto (u, -u)$ ist ein Isomorphismus. Beweis der Behauptung: Injektivität ist klar. Sei $(u_1, u_2) \in ker(\varphi)$, dann gilt $u_1 = -u_2$ also $u_1, u_2 \in U_1 \cap U_2$. Setze $u = u_1$, dann gilt $i(u) = (u_1, u_2)$, also ist φ surjektiv. ✓
Nach 2.35 gilt nun

$$\dim(U_1 \oplus U_2) = \dim \underbrace{(U_1 \cap U_2)}_{\cong ker(\varphi)} + \dim \underbrace{(U_1 + U_2)}_{im(f)}$$

und nach 2.30 gilt $\dim(U_1 \oplus U_2) = \dim U_1 + \dim U_2$ □

2.4 Basen und lineare Abbildungen

Sei $f : V \to W$ eine lineare Abbildung und $(v_i)_{i\in I}$ eine Basis von V. Wir erhalten das System $(f(v_i))_{i\in I}$ von Vektoren in W.

Satz 2.37 *Zu jedem System $(w_i)_{i\in I}$ von Vektoren in W existiert eine eindeutig bestimmte lineare Abbildung $f : V \to W$ mit $w_i = f(v_i)\,\forall i$.*

Beweis: Jedes $v \in V$ hat eine eindeutig bestimmte endliche Darstellung $v = \sum_{i\in I} \alpha_i v_i$, $\alpha_i = 0$ für fast alle i. Wegen der Eindeutigkeit der Darstellung ist die Abbildung $f : V \to W$, $f(v) = \sum_{i\in I} \alpha_i w_i$ wohldefiniert und hat die gewünschte Eigenschaft. Sind nun f_1, f_2 zwei lineare Abbildungen und $f_1(v_i) = w_i = f_2(v_i)\,\forall i$, so gilt für $v = \sum \alpha_i v_i$: $f_1(v) = \sum \alpha_i f_1(v_i) = \sum \alpha_i w_i = \sum \alpha_i f_2(v_i) = f_2(v)$ also $f_1 = f_2$. □

Korollar 2.38 *Für jeden Vektorraum V ist die kanonische Auswertungsabbildung $\varphi : V \to V^{**}$ injektiv.*

Beweis: Erinnerung: $\varphi(u) \in (V^*)^*$ ist gegeben durch $f \in V^* \mapsto f(u) \in K$. Zu zeigen: $ker(\varphi) = 0$, das heißt aus $f(u) = 0 \, \forall f \in V^*$ folgt $u = 0$. Sei $u \neq 0$. Nach 2.23 (Basisergänzungssatz) existiert eine Basis $(u_i)_{i \in I}$ von V, die u enthält, das heißt $u_{i0} = u$ für ein $i_0 \in I$. Wir definieren (siehe 2.37) eine Linearform $f : V \to W$ durch $f(u_{i0}) = 1$ und $f(u_i) = 0$ für $i \neq i_0$. Dann gilt $f(u) = f(u_{i0}) \neq 0$ □

Satz 2.39 *Ist V endlichdimensional, so gilt* $\dim V = \dim V^*$.

Beweis: Sei $(v_1, ..., v_n)$ eine Basis von V. Seien $v_1^*, ..., v_n^* \in V^*$ definiert durch $v_i^*(v_j) = \delta_{ij}$ mit

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \qquad \text{Kroneckersymbol}$$

Behauptung: $(v_1^*, ..., v_n^*)$ ist eine Basis von V^*.
Beweis der Behauptung: Sei $\alpha_n v_1^* + ... + \alpha_n v_n^*$ der 0-Homomorphismus $V \to K$. Zu zeigen: $\alpha_1 = ... = \alpha_n = 0$. Es gilt $\alpha_1 = \alpha_1 + 0 + ... + 0 = \alpha_1 v_1^*(v_1) + \alpha_2 v_2^*(v_1) + ... + \alpha_n v_n^*(v_1) = (\alpha_1 v_1^* + ... + \alpha_n v_n^*)(v_1) = 0$. Analog: $\alpha_2 = ...\alpha_n = 0 \Rightarrow (v_1^*, ..., v_n^*)$ ist linear unabhängig. Sei $f : V \to K$ beliebig und sei $\alpha_i = f(v_i)$. Dann gilt $f = \alpha_1 v_1^* + ... + \alpha_n v_n^*$, weil beide Seiten Linearformen auf V sind, die die gleichen Bilder auf den Basisvektoren $(v_1, ..., v_n)$ haben. □

Def. 2.40 (duale Basis) *Die ebendefinierte Basis $(v_1^*, ..., v_n^*)$ von V^* heißt die zu $(v_1, ..., v_n)$ duale Basis.*

Korollar 2.41 *Ist V endlichdimensional, so ist die kanonische Auswertungsabbildung $\varphi : V \to V^{**}$ ein Isomorphismus.*

Beweis: Aus 2.38 folgt: φ ist injektiv. Aus 2.39 folgt $\dim V = \dim V^* = \dim V^{**}$. Schließlich folgt aus 2.28(i): φ ist ein Isomorphismus. □
Bemerkung: Für unendlichdimensionale Vektorräume ist 2.41 falsch.

2.5 Der Rangsatz

Def. 2.42 (Rang) *Seien V, W endlichdimensional und $f : V \to W$ linear. Der Rang von f ist definiert durch* $Rg(f) = \dim(im(f))$.

Bemerkungen:

- $f = 0 = Rg(f) = 0$
- f surjektiv $\Leftrightarrow$ $Rg(f) = \dim W$. Im Allgemeinen gilt $0 \leq Rg(f) \leq \min(\dim V, \dim W)$ Nun definiert f die duale Abbildung $f^* : W^* \to V^*$, $\varphi \mapsto \varphi \circ f$. Es gilt:

Satz 2.43 (Rangsatz)

$$Rg(f) = Rg(f^*)$$

Beweis: $Rg(f^*) \overset{df}{=} \dim(im(f)) \overset{2.35}{=} \dim W^* - \dim(ker(f)) \underset{2.29}{\overset{2.10}{=}} \dim W - \dim((W/im(f))^*) \overset{2.39}{=} \dim W - \dim(W/im(f)) \overset{2.35}{=} \dim W + \dim(im(f)) \overset{df}{=} Rg(f)$. □

3 Matrizen und lineare Gleichungssysteme

Im ganzen Kapitel: K ist ein fixierter Körper.
Jeder endlichdimensionale K-Vektorraum ist unkanonisch isomorph zu K^n, $n = \dim V$. Der Isomorphismus hängt von der Auswahl einer Basis ab (Vgl. 2.17).

3.1 Matrizen

Def. 3.1 (Matrix) *Eine $m \times n$-Matrix mit Einträgen in K ist ein Schema*

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

mit $a_{ij} \in K$ für $1 \leq i \leq m$, $1 \leq j \leq n$.
Die Menge der $m \times n$-Matrizen über K wird mit $M_{m,n}(K)$ bezeichnet.

Def. 3.2 *$M_{m,n}(K)$ wird zum K-Vektorraum:*

- $(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$
- $\alpha(a_{ij}) = (\alpha a_{ij}), \alpha \in K$

Üblicherweise identifiziert man K^n mit $M_{n,n}(K)$ durch

$$(a_1, \dots, a_n) \mapsto \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \qquad \textit{(Spaltenvektoren)}$$

Def. 3.3 (Produkt) *Sind $A = (a_{ij})_{1 \leq j \leq n}^{1 \leq i \leq m} \in M_{m,n}(K)$ und $B = (b_{ij})_{1 \leq j \leq k}^{1 \leq i \leq n} \in M_{n,k}(K)$, so heißt die Matrix $C = (c_{ij})_{1 \leq j \leq k}^{1 \leq i \leq m} \in M_{m,k}(K)$ mit $c_{ij} = \sum_{s=1}^{n} a_{is} \cdot b_{sj}$ das Produkt der Matrizen A und B ($C = A \cdot B$).*

Beispiel:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 5 \\ 3 \end{pmatrix}$$

Warnung: Im Allgemeinen ist $B \cdot A$ nicht definiert und selbst wenn $m = n = k$ gilt im Allgemeinen $A \cdot B \neq B \cdot A$.
Identifiziere wie oben K^n mit $M_{n,1}(K)$, so definiert die Multiplikation mit einer festen Matrix $A \in M_{m,n}(K)$ eine Abbildung

$$F_{m,n}(A) : K^n \to K^m$$

Wir erhalten eine Zuordnung $A \mapsto F_{m,n}(A)$, die jeder $m \times n$-Matrix eine Abbildung $K^n \to K^m$ zuordnet.

Satz 3.4 *Die ebendefinierte Zuordnung definiert einen Vektorraumisomorphismus*

$$F_{m,n} : M_{m,n}(K) \to Hom_K(K^n, K^m)$$

Für $A \in M_{m,n}(K)$ und $B \in M_{n,k}(K)$ gilt $F_{m,k}(AB) = F_{m,n}(A) \cdot F_{n,k}(B)$ in $Hom_K(K^k, K^m)$

Beweis:

1. $F_{m,n}(A)$ ist eine lineare Abbildung (nachrechnen)
2. $F_{m,n} : M_{m,n}(K) \to Hom_K(K^n, K^n)$ ist linear (ebenfalls nachrechnen)
3. Beobachtung: Für $1 \leq i \leq n$ gilt

$$F_{m,n}(A)(e_i) = A \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i\text{-te Stelle} = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{m,i} \end{pmatrix}$$

Nun ist $(e_1, ..., e_n)$ eine Basis des K^n und nach 2.37 ist eine lineare Abbildung $\varphi : K^n \to K^n$ eine durch das System $(\varphi(e_1), ..., \varphi(e_n))$ in K^n gegeben und umgekehrt. Daher ist $F_{m,n}$ ein Isomorphismus.
Formel für Multiplikation: Genügt zu zeigen für $i = 1, ..., k$ gilt:
$F_{m,k}(AB)(e_i) = (F_{m,n}(A))(F_{n,k}(B(e_i)))$

(a) Linke Seite: $F_{m,k}(AB)(e_i) = i$-te Spalte von AB:

$$= \begin{pmatrix} a_{11}b_{1i} + a_{12}b_{2i} + ... + a_{1n}b_{ni} \\ \vdots \\ a_{m1}b_{1i} + ... + a_{mn}b_{ni} \end{pmatrix}$$

(b) Rechte Seite: A (i-te Spalte von B) = dasselbe □

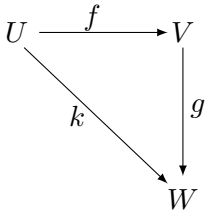
Korollar 3.5 *Das Matrixprodukt ist assoziativ. Für $m = n = k$ erhalten wir einen isomorphen unitären Ring*

$$F_{n,n} : M_{n,n}(K) \xrightarrow{\sim} End_K(K^n)$$

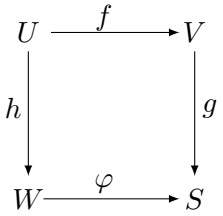
Def. 3.6 (Einheitsmatrix) *Die Matrix $E_n = (\delta_{ij})_{j=1...n}^{i=1...n}$ (also 1en auf der Diagonale und sonst Nullen) heißt die Einheitsmatrix vom Rang n.*

Bemerkungen:

- $F_{n,n,}(E_n) = id_{K^n}$
- eine $n \times n$-Matrix A heißt invertierbar, wenn eine $n \times n$ Matrix B mit $B \cdot A = E_n$ existiert. A ist genau dann invertierbar, wenn $F_{n,n}(A)$ ein Isomorphismus ist.
- die Menge der invertierbaren $n \times n$-Matrizen wird mit $GL_n(K)$ bezeichnet und bildet eine Gruppe unter Matrixmultiplikation, die durch $F_{n,n}$ auf $GL(K^n) = Aut_K(K^n)$ abgebildet wird. Nach 1.24 hat jede inverse Matrix auch ein Rechtsinverses, welches mit dem Linksinversen übereinstimmt
- Wir bezeichnen den zu $F_{n,n}$ inversen Isomorphismus mit $M_{m,n} : Hom_K(K^n, K^n) \xrightarrow{\sim} M_{m,n}(K)$ Für eine lineare Abbildung $f : K^n \to K^n$ heißt $M_{m,n}(f) \in M_{m,n}(K)$ die *Darstellungsmatrix* von f
- Wir nennen ein Diagramm von Vektorräumen und linearen Abbildungen kommutativ, wenn jede Verbindundung zwischen zwei Vektorräumen im Diagramm dieselbe Abbildung repräsentiert. Beispiel:



ist kommutativ, falls $k = g \circ f$



ist kommutativ, falls $g \circ f = \varphi \circ h$

Abbildung 8 – kommutative Diagramme

- Seien V, R endlichdimensionale Vektorräume, $n = \dim V, m = \dim W$ und $\underline{v} = (v_1, ..., v_n)$, $\underline{w} = (w_1, ..., w_m)$ Basen von V und W. Nach 2.17 erhalten wir einen Isomorphismus $\phi_{\underline{v}} : K^n \xrightarrow{\sim} V$, $(\alpha_1, ..., \alpha_n) \mapsto \sum \alpha_i v_i$ und $\psi_{\underline{w}} : K^m \xrightarrow{\sim} W$, $(\beta_1, ..., \beta_m) \mapsto \sum \beta_j w_j$. Für $A \in M_{m,n}(K)$ erhalten wir das kommutative Diagramm

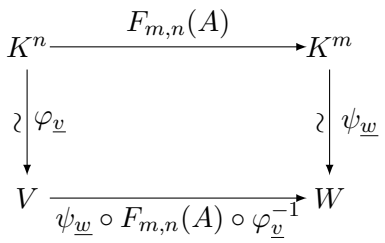


Abbildung 9 – Isomorphismen $\varphi_{\underline{v}}$ und $\psi_{\underline{w}}$

Korollar 3.7 *Wir erhalten einen Isomorphismus von*

$$F_{\underline{w}}^{\underline{v}} : M_{m,n}(K) \to Hom_K(V,W)$$
$$A \mapsto \psi_{\underline{w}} \circ F_{m,n}(A) \circ \varphi_{\underline{v}}^{-1}$$

Den inversen Isomorphismus bezeichnen wir mit

$$M_{\underline{w}}^{\underline{v}} : Hom_K(V,W) \xrightarrow{\sim} M_{m,n}(K)$$

Bezeichnung: $M_{\underline{w}}^{\underline{v}}(f)$ heißt die, die lineare Abbildung f bezüglich der Basen $\underline{v}$ und $\underline{w}$ *darstellende Matrix.*
Alternative Bezeichnung: Darstellungsmatrix, Koordinatenmatrix.
Aus der Definition folgt für eine lineare Abbildung $f : V \to W$ das kommutative Diagramm:

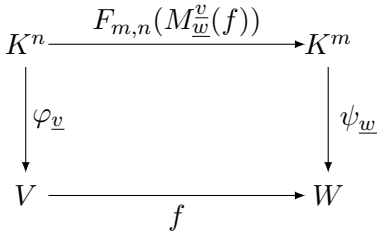


Abbildung 10 – Diagramm $(*)$

Seien nun $\underline{v'} = (v'_1, ..., v'_n)$, $\underline{w'} = (w'_1, ..., w'_m)$ weitere Basen von V und W.

Def. 3.8 *Sind $\underline{v}$ und $\underline{v'}$ zwei Basen desselben Vektorraums V, so heißt die Matrix*

$$T = M_{\underline{v'}}^{\underline{v}}(id_V)$$

die Transformationsmatrix von $\underline{v}$ nach $\underline{v'}$.

Lemma 3.9 *T ist invertierbar, T^{-1} ist die Transformation von $\underline{v'}$ nach $\underline{v}$.*

Beweis: Das Diagramm setzt sich aus zwei kommutativen Diagrammen zusammen.

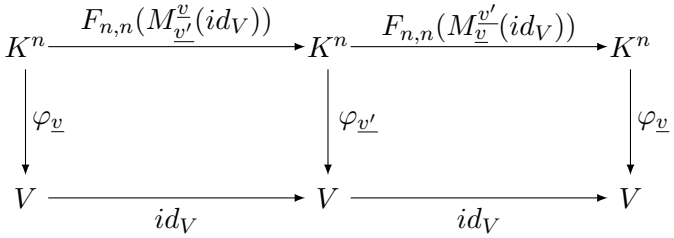


Abbildung 11 – Transformationsmatrizen

Daher gilt: $id_V \circ id_V \circ \varphi_{\underline{v}} = \varphi_{\underline{v}} \circ F_{n,n}(M_{\underline{v}}^{\underline{v'}}(id_V)) \circ F_{n,n} M_{\underline{v'}}^{\underline{v'}}(id_V))$. Wegen $id_{K^n} = F_{n,n}(E_n)$ und weil $F_{n,n}$ nach 3.5 ein Isomorphismus ist, folgt $E_n = M_{\underline{v}}^{\underline{v'}}(id_V)) \cdot M_{\underline{v'}}^{\underline{v}}(id_V))$ □
Aus Abbildung 10 folgt:

Lemma 3.10 *Ist $M_{\underline{w}}^{\underline{v}}(f) = (a_{ij}) \in M_{m,n}(K)$, so gilt für $j = 1, ..., n$:*

$$f(v_j) = a_{1j}w_1 + ... + a_{mx}w_m$$

Beweis: In der j-ten Spalte von $M_{\underline{w}}^{\underline{v}}(f)) = (a_{ij})$ steht das Bild des j-ten Basisvektors, also $F_{n,n}(M_{\underline{w}}^{\underline{v}}(f))(e_j) \in K^m$. Nun gilt $\varphi_{\underline{v}}(e_j) = v_j$ und die Kommutativität von 10 zeigt

$$f(v_j) = \psi_{\underline{w}}\left(F_{m,n}\left(M_{\underline{w}}^{\underline{v}}(f)\right)(e_j)\right) = \psi_{\underline{w}}\left(\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}\right) = a_{1j}w_1 + ... + a_{mj}w_m$$

Lemma 3.11
Seien U, V, W endlichdimensionale Vektorräume und $\underline{u}(u_1, ..., u_n)$, $\underline{v}(v_1, ..., v_m)$, $\underline{w}(w_1, ..., w_k)$ Basen von U, V und W. Desweiteren seien $f : U \to V$, $g : V \to W$ lineare Abbildungen. Dann gilt:

$$M_{\underline{w}}^{\underline{v}}(g) \cdot M_{\underline{v}}^{\underline{u}}(f) = M_{\underline{w}}^{\underline{u}}(g \circ f)$$

Beweis: Sei $M_{\underline{w}}^{\underline{u}}(g \circ f) = (c_{ij})$, dann gilt $g(f(u_j)) = c_{1j}w_1 + ... + c_{k,j}w_k$. Setzt man $M_{\underline{v}}^{\underline{u}}(f) = (b_{ij})$ und $M_{\underline{w}}^{\underline{v}}(g) = (a_{ij})$, so gilt:
$f(u_j) = b_{1k}v_1 + ... + b_{mj}v_m$ und $g(v_i) = a_{1i}w_1 + ... + a_{ki}w_k$. Zusammen ergibt sich $g(f(u_j)) = g(b_{1j}v_1 + ... + b_{mj}v_m) = b_{1j}g(v_1) + ... + b_{mj}g(v_m) = b_{1j}a_{11}w_1 + ... + b_{1j}a_{n1}w_k + b_{2j}a_{12}w_1 + ...$
Koeffizientenvergleich von $g(f(u_j))$ bei w_i für $i = 1, ...k$, $j = 1, ..., n$:

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + ... + a_{im}b_{mj}$$

□

Satz 3.12 (Basiswechselsatz) *Seien V, W endlichdimensionale Vektorräume und $f : V \to W$ eine lineare Abbildung. Seien $\underline{v} = (v_1, ..., v_n)$ und $\underline{v'} = (v'_1, ..., v'_n)$ zwei Basen von V und $T_1 \in M_{n,n}(K)$ die Transformationsmatrix. Seien des weiteren $\underline{w} = (w_1, ..., w_m)$ und $\underline{w'} = (w_1{}', ..., w'_m)$ zwei Basen von W und T_2 die Transformationsmatrix.*
Dann gilt:

$$M_{\underline{w'}}^{\underline{v'}}(f) = T_2 M_{\underline{w}}^{\underline{v}} \cdot T_1^{-1}$$

Beweis: Wende 3.11 auf die Abbildung $V \xrightarrow{id_V} V \xrightarrow{f} W \xrightarrow{id_V} W$ und die Basen $\underline{v'}, \underline{v}, \underline{w}, \underline{w'}$ an und erhalten unter Beachtung von $T_1^{-1} = M_{\underline{v}}^{\underline{v'}}(id_V)$ 3.9
$T_2 \cdot M_{\underline{w}}^{\underline{v}} \cdot T_1^{-1} = M_{\underline{w}}^{\underline{v}}(id_W) \cdot M_{\underline{w}}^{\underline{v}}(f) M_{\underline{v}}^{\underline{v'}}(id_V) = M_{\underline{w'}}^{\underline{v}}(f) \cdot M_{\underline{v}}^{\underline{v'}} = M_{\underline{w'}}^{\underline{v'}}(f)$ □

3.2 Ränge von Matrizen

Def. 3.13 (Zeilen und Spaltenränge) *Sei $A \in M_{m,n}(K)$. Der Zeilen- (bzw. Spalten)rang von A ist die Dimension des durch die Zeilen (bzw. Spalten) von A in K^n (bzw. in K^m) aufgespannten Untervektorraums.*
Bezeichnung: $Z\,\mathrm{Rg}(A)$, $S\,\mathrm{Rg}(A)$
n Vektoren im K^m spannen einen Vektorraum der Dimension höchstens $\min(n, m)$ auf:

$$0 \leq Z\,\mathrm{Rg}(A), S\,\mathrm{Rg}(A) \leq \min(n, m)$$

Satz 3.14

$$Z\,\mathrm{Rg}(A) = S\,\mathrm{Rg}(A)$$

Beweis in 3.17

Lemma 3.15 *(i)* $S\,\mathrm{Rg}(A) = \mathrm{Rg}(F_{m,n}(A))$

(ii) Seien V, W endlichdimensionale Vektorräume, $n = \dim V$, $m = \dim W$ und $\underline{v}, \underline{w}$ Basen. Sei $f : V \to W$ linear. Dann gilt $\mathrm{Rg}(f) = S\,\mathrm{Rg}(M_{\underline{w}}^{\underline{v}}(f))$

Beweis:

(i) die Spalten von A sind die Bilder der Basisvektoren $e_1, ..., e_n$ unter $F_{m,n}(A)$. Diese Bilder spannen $im(F_{m,n}(A))$ auf. Dies zeigt (i).

(ii) Aus dem kommutativen Diagramm

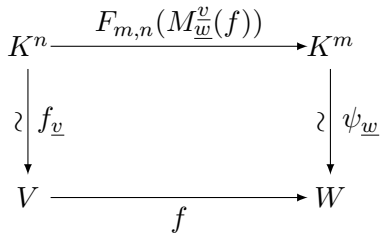


Abbildung 12 – Kommutatives Diagramm

folgt, dass die Einschränkung von $\psi_{\underline{w}}$ auf den Untervektorraum $im(F_{m,n}(M^{\underline{v}}_{\underline{w}}(f))$ ein Isomorphismus $im(F_{m,n}(M^{\underline{v}}_{\underline{w}}(f)) \xrightarrow{\sim} im(f)$ induziert. Insbesondere gilt also

$$\mathrm{Rg}(f) = \mathrm{Rg}(F_{m,n}(M^{\underline{v}}_{\underline{w}}(f)) \overset{(i)}{=} S\,\mathrm{Rg}(M^{\underline{v}}_{\underline{w}}(f))$$

□

Def. 3.16 (transponierte Matrix) *Zu $A = (a_{ij}) \in M_{m,n}(K)$ definiert man die transponierte Matrix*

$$A^t = (a_{ji}) \in M_{n,m}(K)$$

Beispiel:

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

$$\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^t = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Bemerkung: Notation oft ${}^tA$
Offenbar gilt: $Z\,\mathrm{Rg}(A) = S\,\mathrm{Rg}(A^t)$ Für $A \in M_{m,n}(K), B \in M_{n,k}(K)$ gilt $(AB)^t = B^tA^t \in M_{k,m}(K)$
Erinnerung: V, $\underline{v} = (v_1, ..., v_n)$, $V^* = Hom_K(V, K)$ $\underline{v}^*_1 = (v_1^*, ..., v_n^*)$ $v_i^*(v_j) = \delta_{ij}$, $f : V \to W \xrightarrow{induziert} f^* : W^* \to V^*$, $\varphi \mapsto \varphi \circ f$ Für $V \xrightarrow{f} W \xrightarrow{g} U$ gilt: $(g \circ f)^* = f^* \circ g^*$

Lemma 3.17 *Seien V, W endlichdimensionale Vektorräume mit Basen $\underline{v}, \underline{w}, f : V \to W$ linear. Dann gilt:*

$$M^{\underline{w}^*}_{\underline{v}^*}(f^*) = M^{\underline{v}}_{\underline{w}} \in M_{n.m}(K)$$

Beweis: Sei $M^{\underline{v}}_{\underline{w}}(f) = (a_{ij}) \in M_{m,n}(K)$, das heißt für $i = 1, ..., n$ gilt: $f(v_i)) = a_{1v}w_1 + ... + a_{mi}w_m$. Die Spalten auf der rechten Seite sind die Koeffizienten (in $(v_1^*, ..., v_n^*)$) der Bilder der Basisvektoren $w_1^*, ..., w_m^*$ unter f^*. Um Gleichheit zu zeigen, ist also für jedes $1 \le j \le m$ zu zeigen, dass $f^*(w_j^*) = a_{j1}v_1^* + ... + a_{jn}v_n^*$ Beide Seiten sind Linearformen auf V, das heißt Elemente in $V^* = Hom_K(V, K)$. Daher genügt zu zeigen, für alle i: $1 \le i \le n$ gilt: $f^*(w_j^*)(v_i) = (a_{j1}v_1^* + ... + a_{jn}v_n^*)(v_i) = a_{ji}$ Nun ist $f^*(w_j^*)$ die Komposition $V \xrightarrow{f} W \xrightarrow{w_j^*} K$. Daraus folgt: $f^*(w_j^*)(v_i) = w_j^*(f(v_i)) = w_j^*(a_{1i}w_1 + ... + a_{mi}w_m) = a_{ji}$ □
Beweis von 3.14:
Wir betrachten die Abbildung $f = F_{m,n}(A) \cdot K^n \to K^m$. Nach 3.17 wird $f^* : (K^m)^* \to (K^n)^*$ bezüglich der zu den kanonischen Basen dualen Basen $(e_1^*, ..., e_m^*)$ von $(K^m)^*$ und $(e_1^*, ..., e_n^*)$ von $(K^n)^*$ durch die (transponierte) Matrix A^t dargestellt. Nach 2.43 und 3.15 zeigen daher $S\,\mathrm{Rg}(A) = \mathrm{Rg}(f) = \mathrm{Rg}(f^*) = S\,\mathrm{Rg}(A^t) = Z\,\mathrm{Rg}(A)$ □

Satz 3.18 *Für $A \in M_{n,n}(K)$ sind äquivalent.*

(i) *A ist invertierbar, das heißt $A \in GL_n(K)$*

(ii) *Die Zeilen von A bilden eine Basis des K^n*

(iii) *Die Spalten von A bilden eine Basis des K^n*

(iv) $\mathrm{Rg}(A) = n$

Von jetzt an schreiben wir $\mathrm{Rg}(A)$ *für* $Z\,\mathrm{Rg}(A) = S\,\mathrm{Rg}(A)$

Beweis: (ii) $\Leftrightarrow$ (iii) $\Leftrightarrow$ folgt aus dem Rangsatz. Schließlich gilt A invertierbar $\Leftrightarrow$ $F_{n,n}(A)$ ist bijektiv $\overset{2.29}{\Longleftrightarrow}$ $F_{n,n}(A)$ surjektiv $\Leftrightarrow$ $\mathrm{Rg}(A) = n$.

Korollar 3.19 *$A \in M_{m,n}(K)$, $T \in GL_n(K)$, $S \in GL_m(K)$, so gilt*

$$\mathrm{Rg}(A) = \mathrm{Rg}(S \cdot A \cdot T)$$

Beweis: Sei $f = F_{m,n}(A) : K^n \to K^m$. Sei $w_1, ..., w_m$ die durch die Spalten von S^{-1} gegebene Basis des K^m und $v_1, ..., v_n$ die durch Spalten von T gegebene Basis des K^n. Dann ist S die Transformationsmatrix $(e_1, ..., e_m)$ zu $(w_1, ..., w_m)$ im K^m und T^{-1} die Transformationsmatrix von $(e_1, ..., e_n)$ nach $(v_1, ..., w_n)$ im K^n. Nach 3.12:

$$M_{\underline{w}}^{\underline{v}}(f) = S \cdot A \cdot \left(T^{-1}\right)^{-1} = S \cdot A \cdot T$$

und daher nach 3.15 $\mathrm{Rg}(A) = \mathrm{Rg}(f) = \mathrm{Rg}(S \cdot A \cdot T)$ □

Korollar 3.20 *Sei $A \in M_{m,n}(K)$, $r = \mathrm{Rg}(A)$. Dann gibt es eine invertierbare $r \times r$-Untermatrix von A, das heißt Indizes $1 \le i \le .. \le i_r \le m$, sodass die $\widetilde{A}(a_{ij})$, $i \in \{i_1, ..., i_r\}, j \in \{j_1, ..., j_r\}$ invertierbar ist. Umgekehrt folgt aus der Existenz einer Invertierbaren $s \times s$-Untermatrix, dass $s \le r = \mathrm{Rg}(A)$*

Beweis: Wähle r Zeilen aus, dass diese einen r-dimensionalen Untervektorraum im K^n aufspannen. Streiche die anderen Zeilen. Die erhaltene Matrix hat den Rang r. Dann wähle r linear unabhängige Spalten aus und erhalte eine $r \times r$-Matrix vom Rang r.
Umgekehrt: Ist A^t eine invertierbare $s \times s$-Untermatrix von A, so sind die Spalten von A' linear unabhängig, also auch die s-vielen Spalten von A, die A' treffen $\Rightarrow r \ge s$. □

Satz 3.21 *Sei $f : V \to W$ linear, $n = \dim V$, $m = \dim W$, $r = \mathrm{Rg}(f)$, dann existieren Basen $\underline{v}$, $\underline{w}$ von V und W, sodass*

$$M_{\underline{w}}^{\underline{v}} = \underbrace{\begin{pmatrix} \overbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}^{r} & \\ & \end{pmatrix}}_{n} \Bigg\} r$$

Beweis: Sei $U \subset V$ ein Komplement zu $ker(f)$ (siehe 2.32). Wähle eine Basis $(v_1, ..., v_n)$ von V, sodass $Lin(v_1, ..., v_r) = U$, $Lin(v_{r+1}, ..., v_n) = ker(f)$. Es gilt $r = \dim f(v) = \dim V - \dim ker(f)$, also $\dim ker(f) = n - r$. Die eingeschränkte Abbildung $f/U : V \to W$ ist injektiv wegen $U \cap ker(f) = 0$. Setze $w_i = f(v_i)$ für $i = 1, ..., r$ und wähle $w_{r+1}, ..., w_m$ so, dass $w_1, ..., w_m$ Basis von W ist.

Korollar 3.22 *Sei $A \in M_{m,n}(K)$ und $r = \mathrm{Rg}(A)$, dann existiert $S \in GL_m(K)$, $T \in GL_n(K)$ mit*

$$S \cdot A \cdot T = \begin{pmatrix} \overbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}^{r} & \\ & \end{pmatrix}$$

Beweis: Wende 3.21 auf $F_{m,n}(A) : K^n \to K^m$ und den Basiswechselsatz 3.12. □

4 Lineare Gleichungssysteme

4.1 Gauß-Elimination

Aufgabe der Gauß-Elimination: $v_1, ..., v_m \in K^n$ seien gegeben.
Ziel: Berechne eine Basis von $Lin(v_1, ..., v_m)$

Def. 4.1 (lineare Äquivalenz) *Zwei Tupel $(v_1, ..., v_m)$, $(w_1, ..., w_m)$ von Vektoren im K^n heißen linear äquivalent, wenn $Lin(v_1, ..., v_m) = Lin(w_1, ..., w_m)$.*
Man setzt $\mathrm{Rg}(v_1, .., v_m) = \dim(Lin(v_1, ..., v_m))$.
Die folgenden Operationen heißen Zeilenumformungen (Tupel $\mapsto$ lin. äquivalentes Tupel):

(i) Multiplikation von v_i mit $\lambda \neq 0$, $\lambda \in K$

(ii) Ersetze v_i durch $v_i + \lambda v_j$, $j \neq i$, $\lambda \in K$

(iii) Vertauschen der v_i

(iv) Streichen von v_i, wenn $v_i = 0$

Bemerkung: Schreibt man $v_1, ..., v_m$ in der Form

$$\begin{aligned} v_1 &= (a_{11}, ..., a_{1n}) \\ &\vdots \\ v_m &= (a_{m1}, ..., a_{mn}) \end{aligned}$$

So bewirken die Operationen $(i), (ii), (iii)$ auf der Matrix $A = (a_{ij})$ das folgende:

(i) Multiplikation mit der $m \times m$-Matrix $E_i(\lambda)$, die gegeben ist durch

$$E_i(\lambda)_{k,l} = \left.\begin{cases} 0 & k \neq 0 \\ 1 & k = l \neq i \\ \lambda & k = l = i \end{cases}\right| = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \leftarrow i\text{-te Stelle}$$

(ii) Multiplikation von Links mit der $m \times m$-Matrix

$$E_{ij}(\lambda)_{k,l} = \left.\begin{cases} 1 & k = l \\ \lambda & (k = 1 \text{ und } l = j) \\ 0 & \text{sonst} \end{cases}\right| = \begin{pmatrix} 1 & & \\ & \ddots & \\ \lambda & & 1 \end{pmatrix} \quad \text{mit } \lambda \text{ an Stelle } ij$$

(iii) Multiplikation von Links mit P_{ij}:

$$(P_{ij})_{k,l} = \begin{cases} 1 & (k,l) = (i,j) \text{ oder } (j,i) \\ 1 & i \neq k = l \neq j \\ 0 & \text{sonst} \end{cases}$$

Vertausche $i - k$ und $j - k$ Zeile in E_m:

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

Def. 4.2 (Zeilenstufenform) *Eine $m \times n$-Matrix A hat Zeilenstufenform, wenn es Zahlen $0 \leq r \leq m$, $1 \leq j_1 < ... < j_r < n$ gibt, sodass*

(1) $a_{ij} = 0$ *falls* $i > r$ *oder falls* $i \leq r$ *und* $j < j_i$

(2) $a_{ij_i} = 1$ *für alle* $1 \leq i \leq r$

A hat strenge Zeilenstufenform, wenn zusätzlich gilt:

(3) $a_{ij_k} = 0$ *für alle* $1 \leq k \leq r$, $k \neq i$

$$\left(\begin{array}{cccccccccccccccc}
 & & & j_1 & & & & j_2 & & & & & & j_r & & & \\
0 & ... & 0 & 1 & * & ... & * & 0 & * & ... & * & ... & * & 0 & * & ... & * \\
 & & & & & & & 1 & * & ... & * & ... & * & 0 & * & ... & * \\
 & & & & & & & & & & & & & 0 & & & \\
 & & & & & & & & & & & & & \vdots & & & \\
 & & & & & & & & & & & & & 0 & & & \\
 & & & & & & & & & & & & & 1 & * & ... & *
\end{array}\right) \Big\} r$$

Satz 4.3 (Gauß-Elimination) *Durch Zeilenumformungen $(i), (ii), (iii)$ kann man jede $m \times n$-Matrix in strenge Zeilenstufenform bringen.*

Beweis: Die j-te Spalte sei die erste, die nicht nur aus Nullen besteht: $j_1 = j$

(a) Heraufbringen: Ein Zeilentausch (iii) bringt $a_{1j} \neq 0$

(b) Normieren: Anwenden von (i) bewirkt $a_{1j} = 1$

(c) Ausräumen: Durch Ersetzen von v_i durch $v_i - a_{ij}v_1$ erhält die Matrix bis zur j-ten Spalte die gewünschte Form

Nun betrachte die Matrix ohne die 1. Zeile und wähle j_2. Mache Schritt $1, 2, 3$ und beachte, dass sich in Schritt 3 der wesentliche Teil der ursprünglichen 1. Zeile nicht ändert. □

Beispiel: Sei $char(K) \neq 2$:

$$\begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 3 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & 6 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Satz 4.4 *Der von den Vektoren $v_1, ..., v_m$ im K^n erzeugte Untervektorraum ist durch die strenge Stufe eindeutig bestimmt und umgekehrt. Das heißt: Gilt $Lin(v_1, ..., v_n) = Lin(w_1, ...w_k)$, so unterscheiden sich die strengen Zeilenstufenformen nur um 0-Zeilen unterhalb der Stufe.*

Beweis: Sei $U = Lin(v_1, ...v_m)$ und $r = \dim U$, dann ist $U = Lin(v'_1, ...v'_m)$, wobei $v'_1, ...v'_m$ die ersten r Zeilen der assoziierten Matrix in Zeilenstufenform sind. Seien nun $(v_1, ...v_m)$ und $(w_1, ..., w_k)$ mit $Lin(v_1, ...v_m) = Lin(w_1, ...w_k)$ und $A \in M_{m,n}(K)$ und $B \in M_{k,n}(K)$ die assoziierten Matrizen in strenger Zeilenstufenform. Wegen $\mathrm{Rg}(A) = \dim U = \mathrm{Rg}(B)$ sind bei A und B die i-ten Zeilen für $i > r = \dim U$ alle null. Betrachten wir für $1 \leq j \leq r$ die Projektion $p_j : K^n \to K^j$, $(a_1, ..., a_n) \mapsto (a_1, ..., a_j)$, so sind die Stufen bei A wie bei B gerade die j mit $\dim p_j(U) > \dim p_{j-1}(U)$. Also haben die Stufen von A und B die gleiche geometrische Form. Seien nun $a_1 = (a_{11}, ..., a_{1n}), ..., a_r = (a_{r1}, ..., a_{rn})$ und $b_1 = (b_{11}, ..., b_{1n}), ...b_r = (b_{r1}, ..., b_{rn})$ die ersten r Zeilen von A beziehungsweise B. Dann sind $(a_1, ..., a_r)$, $(b_1, ..., b_r)$ beide Basen von U.
Schreiben wir nun $a_j = \sum_{i=1}^{r} \lambda_{ij} b_i$ so ist (weil die j_i-Spalte von B genau eine 1 bei (i, j_i) hat)

$\lambda_{ij} = a_{jj_i}$. Da A strenge Zeilenstufenform hat, also $a_{jj_i} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$ folgt $\lambda_{ij} = 0$ für $i \neq j$ und $\lambda_{ij} = 1$ für $i = j$ und damit $a_j = b_j$, $j = (1, ..., r)$ $\square$

Berechnen der inversen Matrix: Ist $A \in GL_n(K)$, das heißt $A \in M_{n,n}(K)$ invertierbar, so ist die strenge Zeilenstufenform die Einheitsmatrix $E_n \rightsquigarrow$ Methode zur Berechnung von A^{-1}: Führe die gleichen Operationen die A auf strenge Zeilenstufenform (also auf E_n) bringen auch auf E_n an. Das Ergebnis ist A^{-1}.
Begündung: Jede der Operationen $(i), (ii), (iii)$ entspricht der Linksinversen mit eine Matrix. Ist M das (von rechts nach links gebildete) Produkt dieser M, so gilt $M \cdot A = E_n$.
Beispiel: Suche Inverses, wenn $char(K) \neq 2$:

$$\left(\begin{array}{ccc} 2 & 0 & -1 \\ -1 & -1 & 2 \\ 0 & 1 & -1 \end{array}\right) \left| \begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \xrightarrow{1} \left(\begin{array}{ccc} 1 & 0 & -\frac{1}{2} \\ -1 & -1 & 2 \\ 0 & 1 & -1 \end{array}\right) \left| \begin{array}{ccc} \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \xrightarrow{2} \left(\begin{array}{ccc} 1 & 0 & -\frac{1}{2} \\ 0 & -1 & \frac{3}{2} \\ 0 & 1 & -1 \end{array}\right) \left| \begin{array}{ccc} \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \xrightarrow{3}$$
$$\left(\begin{array}{ccc} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & -\frac{3}{2} \\ 0 & 1 & -1 \end{array}\right) \left| \begin{array}{ccc} \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & -1 & 0 \\ 0 & 0 & 1 \end{array}\right) \xrightarrow{4} \left(\begin{array}{ccc} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & -\frac{3}{2} \\ 0 & 0 & \frac{1}{2} \end{array}\right) \left| \begin{array}{ccc} \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & -1 & 0 \\ \frac{1}{2} & 1 & 1 \end{array}\right) \xrightarrow{5}$$
$$\left(\begin{array}{ccc} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & -\frac{3}{2} \\ 0 & 0 & 1 \end{array}\right) \left| \begin{array}{ccc} \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & -1 & 0 \\ 1 & 2 & 2 \end{array}\right) \xrightarrow{6} \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \left| \begin{array}{ccc} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 2 & 2 \end{array}\right)$$

1. Erste Zeile mit $\frac{1}{2}$ multiplizieren
2. Erste Zeile zur zweiten addieren
3. Zweite Zeile mit -1 multiplizieren
4. Zweite Zeile von dritter Zeile subtrahieren
5. Dritte Zeile mit 2 multiplizieren
6. $\frac{1}{2}$ mal die dritte Zeile zur ersten Zeile addieren, das $\frac{3}{2}$-fache der dritten Zeile zur zweiten addieren

Also folgt:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & -1 \\ -1 & -1 & 2 \\ 0 & 1 & -1 \end{pmatrix} = E_3$$

Und dies gilt auch in $char(K) = 2$ (ausrechnen). In $char(K) = 2$ hätte aber auch folgende Rechnung zum Ziel geführt:

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

Also folgt:

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

Bemerkung:

$$\begin{pmatrix}1&1&1\\1&0&1\\1&0&0\end{pmatrix} = \begin{pmatrix}1&1&1\\1&2&3\\1&2&2\end{pmatrix} \quad \text{in } char(K) = 2$$

Berechnen der dualen Basis: Element des Dualraums $(K^n)^*$ sind Linearform auf K^n. Die kanonische Basis des $(K^n)^*$ ist durch die zur kanonischen Basis $(e_1, ..., e_n)$ des K^n duale Basis $(e_1^*, ..., e_n^*)$ gegeben. Wir unterscheiden von Elementen des K^n als Spaltenvektoren (das heißt $(n \times 1)$-Matrizen). Jeder Zeilenvektor (das heißt eine $(1 \times n)$-Matrix) $(a_1, ..., a_n)$ definiert man mit Hilfe der Matrixmultiplikation $M_{1,n}(K) \times M_{n,1}(K) \to M_{1,1}(K) = K$ durch

$$\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix} \mapsto \begin{pmatrix}a_1 & \cdots & a_n\end{pmatrix} \begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix} = a_1x_1 + ... + a_nx_n \in K \text{ das heißt ein Element in } (K^n)^*$$

Es gilt

$$\begin{pmatrix}1 & ... & 0\end{pmatrix} = e_1^*, ..., \begin{pmatrix}0 & ... & 1\end{pmatrix} = e_n^*$$

Daher lässt sich die Linearform $\varphi = a_1e_1^* + ... + a_ne_n^*$ durch den Zeilenvektor $(a_1, ...a_n)$ darstellen, mit anderen Worten: wir können den Vektorraum $(K^n)^*$ mit dem Vektorraum der Zeilen der Länge n identifizieren. Sei nun $(v_1, ..., v_n)$ eine Basis des K^n und $(v_1^*, ..., v_n^*)$ die duale Basis des $(K^n)^*$ (die durch $v_i^*(v_j) = \delta_{ij}$ bestimmt ist). Die Zeilenvektorform der dualen Basis berechnet man wie folgt: Bilde die Matrix A, deren i-te Spalte $= v_i$ ist, dann ist die i-te Zeile von A^{-1} v_i^*.
Begründung: v_i^* ist durch $v_i^*(v_j) = \delta_{ij}$ charakterisiert, das heißt für den als Zeile geschriebenen Vektor v_i^* gilt $v_i^* \cdot v_j = \delta_{ij}$. Bildet man die Matrix B mit den v_i^* als Zeilen, so gilt $B \cdot A = E_n$, also $B = A^{-1}$.
Basisergänzung: Seien $(v_1, ..., v_k)$ linear unabhängige Vektoren im K^n und $(w_1, ..., w_n)$ ein Erzeugendensystem. Wir suchen Indizes $1 \leq j(1) \leq j(s) \leq n$, $s = n - k$, sodass $(v_1, , ..., v_k, w_{j(1)}, ..., w_{j(s)})$ eine Basis des K^n ist (Existenz: 2.23). Bilde A mit Zeilen $v_1, ..., v_k, w_1, ...w_m$. Bringe A auf strenge Zeilenstufenform. Hierbei muss eventuell noch mehrere Male Schrit 1 (also Zeilentausch) durchgeführt werden. Wir nehmen hier stets zum Tauschen die Zeile, die möglichst weit oben steht. Dann gilt: Unter den ersten n Zeilen sind $s = n - k$ Stück, die ursprünglich zu einem Zeilenvektor $w_j(i)$ gehörten mit $i = 1...s$. Dies liefert die gesuchten $j(i)$.

Lineares Komplement
Gegeben: $U = Lin(v_1, ...v_m) \subset K^n$ Gesucht: $U' \subset K^n$ mit $U \cap U' = \{0\}$ und $U + U' = K^n$ sowie eine Basis von U'.
Methode: Forme die Matrix mit Zeilen $v_1...v_m$ in strenge Zeilenstufenform um. Die von 0 verschiedenen Zeilen sind eine Basis von U. Die Vektoren e_j, wobei j *kein* Stufenindex ist, sind Basis eines Untervektorraums U' mit $U \cap U' = \{0\}$, $U + U' = K^n$.

Notatiosnvereinfachung: Wir identifizieren $A \in M_{m,n}(K)$ direkt mit der assoziierten linearen Abbildung $K^n \to K^m$ und umgekehrt.

4.2 Lineare Gleichungen

Ein *lineares Gleichungssystem* ist ein System von linearen Gleichungen:

$$\begin{aligned} a_{11}x_1 + ... + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + ... + a_{mn}x_n &= b_m \end{aligned} \qquad (*)$$

mit $a_{ij}, b_k \in K$.
$(*)$ heißt *homogen*, wenn alle b_i Null sind, ansonsten *inhomogen*. Ist $(*)$ inhomogen, so nennt man das System $(**)$ mit den gleichen a_{ij} und rechts überall Nullen das *zugehörige homogene System*.
Wir schreiben $(*)$ in der Form $A \cdot x = b$ mit $A = (a_{ij})$, $x = (x_1, ..., x_n)^t$ $b = (b_1, ..., b_m)^t$.

Satz 4.5 *Die Menge der Lösungen $x \in K^n$ des homogenen Systems $A \cdot x = 0$ ist ein Untervektorraum des K^n der Dimension $n - \mathrm{Rg}(A)$.*

Beweis: Die Lösungsmenge ist $ker(A)$. Die Aussage über die Dimension folgt aus 2.35 sowie aus $\mathrm{Rg}(A) = \dim(im(A))$ □

Korollar 4.6 *Die folgenden Aussagen sind äquivalent:*

(i) $\mathrm{Rg}(A) = n$

(ii) *A ist invertierbar*

(iii) *$A \cdot x = 0$ hat genau die triviale Lösung $(0, ..., 0) \in K^n$*

Def. 4.7 *Eine Teilmenge eines Vektorraums V heißt affiner Teilraum, wenn es $v \in V$ und einen Untervektorraum $U \subset V$ gibt, sodass $A = v + U = \{v + u | u \in U\}$ gilt.*

Bemerkung: Mit anderen Worten: Ein affiner Teilraum ist ein Element in V/U, wobei $U \subset V$ ein Untervektorraum ist.

Lemma 4.8 *Ist $A \subset V$ ein affiner Teilraum, so existiert genau ein Untervektorraum $U \subset V$ mit $A = v + U$ für ein $v \in V$.*

Beweis: Ein solcher Untervektorraum existiert nach Definition. Sei $A = v_0 + U_0 = v_1 + U_1$, dann gilt: $U_0 = \{a - a' | a, a' \in A\} = U_1$. □

Def. 4.9 *Ist $A \subset V$ ein affiner Teilraum, so setzt man $\dim A := \dim U$, wobei U der nach 4.8 eindeutig bestimmte Untervektorraum $U \subset V$ mit $A = v + U$ ist.*

Satz 4.10 *Sei $A \cdot x = b$ $(*)$ und $A \cdot x = 0$ $(**)$. Für das System $(*)$ gibt es genau zwei Möglichkeiten:*

(i) *$b \notin im(A)$ und Lösungsmenge ist leer*

(ii) *$b \in im(A)$, dann ist die Lösungsmenge L ein affiner Teilraum des K^n der Dimension $n - \mathrm{Rg}(A)$. Ist $v_0 \in L$ eine Lösung von $(*)$, so gilt $L = v_0 + U$, wobei U der Lösungsraum des zugehörigen homogenen Systems $A \cdot x = 0$ ist.*

Beweis: Nach Definition gilt $b \notin im(A) \iff L = \emptyset$. Ist $b \in im(A)$, so gilt es eine Lösung $v_0 \in K^n$ mit $A \cdot v_0 = b$ zu finden. Für $u \in U$ gilt $A(v_0 + u) = A \cdot v_0 + A \cdot u = b + 0 = b$ also $v + U \subset L$. Umgekehrt sei $v \in L$, das heißt $A \cdot v = b$, dann gilt für $u = v - v_0$: $A \cdot u = A(v - v_0) = A \cdot v - A \cdot v_0 = b - b = 0$ also $u \in U$ und $v = v_0 + u \Rightarrow L = v_0 + U$. Schließlich gilt $\dim L = \dim U = n - \mathrm{Rg}(A)$ □

Korollar 4.11 *Das inhomogenene System $(*)$ hat genau dann eine Lösung, wenn $\mathrm{Rg}(A) = \mathrm{Rg}(A|b)$ gilt. Hierbei ist $(A|b)$ die $m \times (n+1)$-Matrix, die durch Anfügen von B als $(n+1)$-te Spalte entsteht.*

Beweis: $\mathrm{Rg}(A) = \mathrm{Rg}(A|b) \iff b \in Lin(\text{Spalten von } A) \iff b \in im(A)$ □

4.3 Explizite Lösungen linearer Gleichungssystem

Betrachte $Ax = 0\,(*)$. Zeilenumformungen $(i), (ii), (iii)$ ändern nicht den Lösungsraum $ker(A)$, zum Beispel weil diese Umformunegn der Multiplikation von Links mit invertierbaren Matrizen entsprechen $\rightsquigarrow$ erhalten Verfahren.

1. Bringe A auf strenge Zeilenstufenform
2. Sei nun S die strenge Zeilenstufenform von A:

$$S = \begin{pmatrix}
 & & & j_1 & & & & j_2 & & & & & & j_r & & & \\
0 & \dots & 0 & 1 & * & \dots & * & 0 & * & \dots & * & \dots & * & 0 & * & \dots & * \\
 & & & & & & & 1 & * & \dots & * & \dots & * & 0 & * & \dots & * \\
 & & & & & & & & & & & & & 0 & & & \\
 & & & & & & & & & & & & & \vdots & & & \\
 & & & & & & & & & & & & & 0 & & & \\
 & & & & & & & & & & & & & 1 & * & \dots & *
\end{pmatrix}$$

Die von $j_1, ..., j_r$ verschiedenen Indizes in $\{1, ...n\}$ seien $k_1 < ... < k_{n-r}$ das heißt $\{j_1, ..., j_r, k_1, ...k_{n-r}\}$. Dann gilt $Sx = 0 \iff (x_{j_1}...x_{j_r})^t = -B(x_{k_1}...x_{k_{n-r}})^t$, wobei B aus den ersten r Zeilen von S entsteht, indem man die Spalten des Index j_i, $i = 1, ...r$ weglässt (also $B \in M_{r,u-r}(K)$). Folglich kann man $x_{k_1}, ..., x_{k_{n-r}}$ frei wählen und $x_{j_1}...x_{j_r}$ ergeben sich eindeutig. Setzt man nun den i-ten Standardbasisvektor in K^{n-r} ein, erhält man links die i-te Spalte von $-B$ und einen i-ten Basisvektor $(x_1, ..., x_n)$ des Lösungsraums durch $(x_{k_1}, ..., x_{k_{n-r}}) = e_i$, $(x_{j_1}...x_{j_r}) = -i$-te Spalte von B.
Beispiel: $char(K) \neq 2$:

$$\begin{aligned} 2x_1 + 4x_2 + 2x_3 + 6x_4 &= 0 \\ 3x_1 + 6x_2 + 3x_3 + 9x_4 &= 0 \\ 4x_1 + 8x_2 + 5x_3 + 9x_4 &= 0 \end{aligned}$$

$$A = \begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \xrightarrow{Bsp\,nach 4.3} S = \begin{pmatrix} 1 & 2 & 0 & 6 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Also ist $j_1 = 1$, $j_2 = 3 \Rightarrow k_1 = 2$, $k_2 = 4$, für B folgt:

$$B = \begin{pmatrix} 2 & 6 \\ 0 & -3 \end{pmatrix} \Rightarrow -B = \begin{pmatrix} -2 & -6 \\ 0 & 3 \end{pmatrix}$$

Somit ist die Basis des zweidimensionalen Lösungsraums:

$$(-2, 1, 0, 0) \quad (-6, 0, 3, 1)$$

Nun betrachten wir das inhomogene System $Ax = b\,(*)$. Die Zeilenumformungen $(i), (ii)(iii)$ auf der Matrix $(A|b)$ kommen auf $(S|s)$ als strenge Zeilenstufenform. Sei $r = \mathrm{Rg}(A) = \mathrm{Rg}(S)$. Wegen $\mathrm{Rg}(A|b) = \mathrm{Rg}(S|s)$ ist die Existenz von Lösungen nach 4.11 äquivalent zu $s_{r+1} = ... = s_n = 0$. Ist dies erfüllt, setzte $x_j = 0$ für $j \notin (j_1, ..., j_r)$ und $(x_{j_1}, ..., x_{j_r}) = (s_1, ..., s_r)$ um eine spezielle Lösung zu erhalten. Alle anderen Lösungen erhält man durch Addition von Lösungen des zugehörigen homogenen Systems.

$$\begin{aligned} 2x_1 + 4x_2 + 2x_3 + 6x_4 &= 4 \\ 3x_1 + 6x_2 + 3x_3 + 9x_4 &= 6 \\ 4x_1 + 8x_2 + 5x_3 + 9x_4 &= 9 \end{aligned}$$

$$(A|b) = \begin{pmatrix} 2 & 4 & 2 & 6 & 4 \\ 3 & 6 & 3 & 9 & 6 \\ 4 & 8 & 5 & 9 & 9 \end{pmatrix} \xrightarrow{Bsp\,nach 4.3} S = \begin{pmatrix} 1 & 2 & 0 & 6 & 1 \\ 0 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Stufenindizes: $j_1 = 1, j_2 = 3$ Spezielle Lösung: $(1, 0, 1, 0)$. Also folgt:

$$L = \left\{(1 - 2x_2 - 6x_4, x_2, 1 + 3x_4, x_4) \in K^4 | x_2, x_4 \in K\right\}$$

5 Determinanten und Eigenwerte

Def. 5.1 (Polynome) *Ein Polynom mit Koeffizienten in einem Körper K ist ein Ausdruck*

$$f = f(x) = a_0 + a_1 x + ... + a_n x^n, \quad a_j \in K$$

Das Zeichen x heißt Unbestimmte oder Variable des Polynoms. Die Menge der Polynome mit Koeffizienten in K wird mit $K[x]$ bezeichnet.

Bemerkung:

1. Ein Polynom ist ein formaler Ausdruck, das heißt nichts weiter als die Familie seiner Koeffizienten $a_0, a_1, ..., a_n$, das heißt eine Abbildung $f : \mathbb{N}_0 \to K$, $f(i) = 0$ für fast alle i.

2. Jedes Polynom $f(x) = a_0 + ... + a_n x^n \in K[x]$ induziert eine Abbildung $K \to K$, $\alpha \mapsto f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n$. Im Allgemeinen ist f durch diese Abbildung nicht allgemein bestimmt, zum Beispiel induzieren Polynome $x, x^2 \in \mathbb{Z}/2\mathbb{Z}[x]$ die gleiche Abbildung: $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ (nämlich die Identität).

$K[x]$ wird zum kommutativen unitären Ring

$$f = \sum_{i \in \mathbb{N}_0} a_i x^i \quad g = \sum_{i \in \mathbb{N}_0} b_i x^i$$

$$\Rightarrow f + g = \sum_{i \in \mathbb{N}_0} (a_i + b_i) x^i \quad f \cdot g = \sum_{s \in \mathbb{N}_0} \left(\sum_{i \in 0}^{s} a_i x^i \right) x^s$$

Wir haben eine natürliche Inklusion $K \hookrightarrow K[x]$ die $\alpha \in K$ das konstante Polynom α (das heißt $a_0 = \alpha_i$, $\alpha_i = 0$ für $i \geq 1$ zuordnet).

Def. 5.2 (Grad eines Polynoms, Normierung) *Ist $f = a_0 + ... + a_n x^n$ und $a_n \neq 0$, so heißt n der Grad von f $\deg(f)$ und a_n der Leitkoeffizient.*
Notation: $a_n = e(f)$. Gilt $a_n = 1$, so nennt man f normiert. Konvention: $\deg(0) = -\infty$, $e(0) = 0$.

Lemma 5.3 *Es gilt:*

(i) $\deg(f \cdot g)) = \deg(f) \cdot \deg(g)$

(ii) $\deg(f + g) \leq \max(\deg(f), \deg(g))$ *und wenn* $\deg(f) \neq \deg(g)$, *so gilt* $\deg(f + g) = \max(\deg(f), \deg(g))$

(iii) $e(f \cdot g) = e(f) \cdot e(g)$

Beweis: direkt aus der Definition, wobei man verwendet, dass K nullteilerfrei ist, das heißt es gilt $a \cdot b = 0 \Rightarrow (a = 0$ oder $b = 0)$

Korollar 5.4 *Der Ring $K[x]$ ist nullteilerfrei, das heißt aus $f \cdot g = 0$ folgt $f = 0$ oder $g = 0$.*

Beweis: dies folgt aus $e(f \cdot g) = e(f) \cdot e(g)$ und der Nullteilerfreiheit von K.

Satz 5.5 (Division mit Rest) *Seien $f, g \in K[x], g \neq 0$, dann existieren eindeutig bestimmte Polynome $q, r \in K[x]$ mit $f = q \cdot g + r$, $\deg(r) < \deg(g)$. Das Polynom r heißt Rest der Division von f durch g.*

Beweis:

- Eindeutigkeit: Sei $f = q_1 g + r_1 = q_2 g + r_2$. Dann gilt $(q_1 - q_2)g = r_2 - r_1$. Wegen $\deg(r_2 - r_1) < \deg g$ folgt $q_1 - q_2 = 0$ also auch $r_2 - r_1$
- Existenz: Per Induktion nach $\deg(f)$: Ist $\deg(f) < \deg(g)$, so setze $q = 0$, $f = r$. Sonst sei $f = ax^{n+k} +$ niedere Potenzen, $g = bx^n +$ niedere Potenzen, $n, k \geq 0$, $a, b \neq 0$. Dann gilt:

  $$\deg\left(f - \frac{a}{b} x^k g\right) < \deg(f)$$

  Nach Induktionsannahme gibt es q_1, q_2 mit $f - \frac{a}{b} x^k g = q_1 g + r_1$, $\deg(r_1) < \deg(g)$ Wir erhalten die Darstellung

  $$f = \left(q_1 + \frac{a}{b} x^k\right) g + r_1$$

□

Beispiel:

$$
\begin{array}{llllll|l}
x^5 & +3x^4 & -4x^3 & +0x^2 & +0x & +2 & : (x^2+1) \quad = \quad x^3+3x^2-5x-3 \\
x^5 & & x^3 & & & & \\
\hline
 & 3x^4 & -5x^3 & +0x^2 & +0x & +2 & \\
 & 3x^4 & & +2x^2 & & & \\
\hline
 & & -5x^3 & -3x^2 & +0x & +2 & \\
 & & -5x^3 & & -5x & & \\
\hline
 & & & -3x^2 & +5x & +2 & \\
 & & & -3x^2 & & -3 & \\
\hline
 & & & & 5x & +2 & \text{Rest}
\end{array}
$$

Def. 5.6 (Wurzel, Nullstelle) *Ein $\alpha \in K$ heißt Nullstelle oder Wurzel von $f \in K[x]$ wenn $f(\alpha) = 0$.*

Korollar 5.7 *Ist $\alpha \in K$ eine Wurzel von $f \in K[x]$, so existiert $g \in K[x]$ mit $f = g(x - \alpha)$.*

Beweis: Ist $f = 0$ setze $g = 0$, falls $f \neq 0$, so sei $f = g(x-\alpha) + r$ mit $\deg(r) \leq 0$ also r konstant. Einsetzen von $\alpha : 0 = f(\alpha) = g(\alpha)(\alpha - \alpha) + r(\alpha)$, also $r = 0$ □

Korollar 5.8 *Ein Polynom $f \neq 0$ vom Grad n hat höchstens n Wurzeln in K.*

Beweis: Sei $f(\alpha) = 0 : f = g(x-\alpha)$, $\deg(g) = n-1$. Ist nun $\beta \neq \alpha$ eine weitere Wurzel, so gilt $0 = f(\beta) = g(\beta)(\beta - \alpha) \Rightarrow g(\beta) = 0$. Vollständige Induktion nach Grad. □

5.1 Euklidischer Algorithmus

Seien $f_1, f_2 \in K[x] \setminus \{0\}$. Der euklidische Algorithmus ist eine Folge von Divisionen mit Rest:

$$
\begin{aligned}
f_1 &= q_1 \cdot f_2 + f_3 \quad \deg(f_3) < \deg(f_2) \\
f_2 &= q_2 \cdot f_3 + f_4 \quad \deg(f_3) < \deg(f_4) \\
&\vdots \\
f_{n-1} &= q_{n-1} \cdot f_n + 0 \quad \text{weil die Grade abnehmen}
\end{aligned}
$$

Def. 5.9 *f teilt g (Notation $f|g$), wenn $g = f \cdot h$ für ein $h \in K[x]$.*

Satz 5.10 *Seien $f_1, f_2 \in K[x] \setminus \{0\}$ und $d = f_n$ wie im euklidischen Algorithmus. Dann gilt:*

(i) $d|f_1$, $d|f_2$

(ii) *Aus $g|f_1$ und $g|f_2$ folgt $g|d$*

(iii) *Es gilt $p, q \in K[x]$ mit $pf_1 + qf_2 = d$*

(i) "Aufwärts" $d|f_n \Rightarrow d|f_{n-1}$ $f_{n-2} = q_{n-2}f_{n-1} + f_n \Rightarrow d|f_{n-2}, ..., d|f_2, d|f_1$ ✓

(ii) "Abwärts" $g|f_1$, $g|f_2 \Rightarrow g|f_3 \Rightarrow g|f_n = d$

(iii) "Absteigend" sieht man, dass jedes f_k eine Darstellung der Form $f_k = p_k f_1 + q_k f_2$ hat □

Def. 5.11 *$d \in K[x]$ mit (i) und (ii) aus 5.10 heißt ein größter gemeinsamer Teiler von f und g.*

Satz 5.12 *Sind $f_1, f_2 \in K[x] \setminus \{0\}$, so existiert ein größer gemeinsamer Teiler. Dieser ist bis auf einen konstanten Faktor $\neq 0$ eindeutig bestimmt.*

Beweis: Existenz folgt aus 5.10. Sind d_1, d_2 beide größe gemeinsame Teiler, so gilt $d_1|d_2$, $d_2|d_1$ also $\deg(d_1) \leq \deg(d_2) \leq \deg(d_1)$ also folgt $\deg(d_1) = \deg(d_2)$ und aus $d_1|d_2$ folgt $d_2 = d_1 \cdot \alpha$, $\alpha \in K \setminus \{0\}$.
Bemerkung: Unter den größen gemeinsamen Teilern existiert genau eine normierte Potenz. Diesen nennt man *den* größten gemeinsamen Teiler. Notation: $\mathrm{ggT}(f_1, f_2)$

Korollar 5.13 *Haben $f, g \in K[x] \setminus \{0\}$ nur konstant gemeinsame Teiler, so existieren Polynome p, q mit $p \cdot f + q \cdot g = 1$*

Beweis: $\mathrm{ggT}(f, g) = 1$ □

Def. 5.14 *$f \in K[x]$, $\deg(f) \geq 1$ heißt irreduzibel, wenn gilt: $f = g \cdot h \Rightarrow g$ konstant oder h konstant. Ansonsten heißt f reduzibel.*

Beispiele:

- Jedes Polynom $ax + b$, $a \neq 0$ ist irreduzibel
- $x^2 + 2x + 1 = (x + 1)^2$ ist reduzibel
- $x^2 + 1$ ist irreduzibel in $\mathbb{Q}[x], \mathbb{R}[x]$, aber reduzibel in $\mathbb{C}[x]$

Lemma 5.15 *f ist irreduzibel, $f|gh \Rightarrow f|g$ oder $f|h$.*

Beweis: f ist irreduzibel, also sind $a, a \cdot f$ mit $a \in K[x]$ die einzigen Teiler von f. Gilt nun $f \nmid g$, so folgt $\mathrm{ggT}(f, g) = 1$. Daher existieren $p, q \in K[x]$ mit $p \cdot f + q \cdot g = 1 \Rightarrow p \cdot f \cdot h + q \cdot g \cdot h = h \Rightarrow f|h$□

Satz 5.16 *Jedes $f \in K[x] \setminus \{0\}$ besitzt eine, bis auf die Reihenfolge der Faktoren eindeutig bestimmte Primfaktorzerlegung*

$$f = a \cdot p_1 + ... + p_r, \quad a = e(f),\ e(p_i) = 1,\ i = 1, ..., k$$

mit irreduziblen, normierten Faktoren p_i.

Beweis:
Existenz: per Induktion nach $\deg(f)$. Ist f irreduzibel, so $f = e(f)(e(f)^{-1}f)$ und $e(f)^{-1}f$ ist irreduzibel und normiert. Sei f reduzibel, $\deg(f) = n$, $f = g \cdot h$ mit $\deg(g), \deg(h) < n$ und die Induktionsvoraussetzung für g, h liefert eine Darstellung für f.
Eindeutigkeit: $a = e(f)$ ist eindeutig. Angenommen es gilt $p_1...p_k = q_1...q_l$ mit irreduziblen normierten Polynomen $p_1, ..., p_k, q_1, ..., q_l$. Aus 5.10 folgt $p_k|q_i$ für ein $1 \leq i \leq l$. Da q_i irreduzibel ist, folgt $p_k = q_i$. Nach Umnummerierung sei $i = l \Rightarrow p_k(p_1...p_{k-1}, -q_1...q_{l-1}) = 0$. Nach 5.4 folgt $p_1...p_{k-1} = q_1...q_{l-1}$ usw. □

5.2 Determinanten

Def. 5.17 (Multilinearformen) *Sei V ein K-Vektorraum. Eine Multilinearform (n-Form) ist eine Abbildung*

$$\alpha : \underbrace{V \times ... \times V}_{n\ mal} \to K$$

die in jeder Variable (das heißt bei Festhalten der $n-1$ anderen) linear ist. α heißt alternierend, wenn $\alpha(v_1, ..., v_n) = 0$ für jedes n-Tupel $(v_1, ..., v_n)$ mit $v_i = v_j$ für irgendwelche $i \neq j$ gilt.
Alternierende n-Formen bilden in natürlicher Weise einen K-Vektorraum, der mit $\mathrm{Alt}^n(V)$ bezeichnet wird.
Spezialfall: $n = 1$: $\mathrm{Alt}^1(V) = V^*$

Bemerkung: $\alpha \in \mathrm{Alt}^n V : \alpha(v_1, ..., v_i, v_j ... v_n) = -\alpha(v_1 ..., v_j, v_i, ... v_n)$
Beweis: $0 = \alpha(v_1, ..., v_i + v_j, ..., v_i + v_j, ..., v_n) = \alpha(v_1, ..., v_i, ..., v_i, ..., v_n) + \alpha(v_1, ..., v_j, ..., v_i, ..., v_n) + \alpha(v_1, ..., v_i, ..., v_j, ..., v_n) + \alpha(v_1, ..., v_j, ..., v_j, ..., v_n)$

Satz 5.18 *Eine alternierende n-Form ist*

(i) homogen, das heißt $\alpha(v_1, ..., \lambda v_i, ..., v_n) = \lambda\alpha(v_1, ..., v_i, ..., v_n)$ *für alle* $\lambda \in K$, $v_1 ..., v_n \in V$, $j = 1...n$

(ii) scherungsinvariant, das heißt $\alpha(v_1, ..., v_{j-1}, v_j + \lambda v_i, v_{j+1}, ..., v_n) = \alpha(v_1, ..., v_n)$

Beweis:

(i) folgt aus Multilinearität

(ii) $\alpha(v_1, ..., v_j + \lambda v_i, ...v_n) = \alpha(v_1, ..., v_j, ..., v_n) + \alpha(v_1, ..., \lambda v_i, ..., v_n)$ und $\alpha(v_1, ..., \lambda v_i, ..., v_i, ..., v_n) = \lambda\alpha(v_1, ..., v_i, ..., v_i, ..., v_n) = 0$ □

Lemma 5.19 *Ist* $\alpha : V^n \to K$ *eine homogene und scherungsinvariante n-Form und* $(v_1, ..., v_n)$ *linear abhängig, so gilt* $\alpha(v_1, ...v_n) = 0$

Beweis: Sei zum Beispiel $v_1 = \lambda_2 v_2 + ... + \lambda_n v_n$, dann gilt: $\alpha(v_1, ..., v_n) = \alpha(v_1 - \lambda_2 v_2 - ... - + \lambda_n v_n, v_2, ..., v_n) = \alpha(0, v_2, ..., v_n) = 0\alpha(0, v_2, ..., v_n) = 0$ □

Satz 5.20 *Sei* $\dim_K V = n$, *dann ist jede homogene und scherungsinvariante Abbildung* $V^n \to K$ *eine alternierende n-Form.*

Beweis: Sei $\alpha : V^n \to K$ homogen und scherungsinvariant, dann gilt $\alpha(v_1, ..., v_n) = 0$ falls $(v_1, ..., v_n)$ linear abhängig sind 5.19. α ist n-Form, wegen Homogenität genügt zu zeigen:

$$\alpha(v_1, ..., v_i + v_i', ...v_n) = \alpha(v_1, ..., v_i, ..., v_n) + \alpha(v_1, ..., v_i', ..., v_n)$$

- Fall 1: $(v_1, ..., v_{i-1}, v_{i+1}, ..., v_n)$ linear abhängig $\Rightarrow$ beide Seiten $= 0$ ✓
- Fall 2: Sonst ergänze zu Basis $(v_1, ...v_{i-1}, w, v_{i+1}, ..., v_n)$. Dann ist $v_i = a + \lambda \cdot w$, $v_i' = a' + \lambda' w$ mit $\lambda, \lambda' \in K$ und $a, a' \in Lin(v_1, ..., v_{i-1}, v_{i+1}, ..., v_n)$ Scherungsinvarianz: $\alpha(v_1, ..., v_i, ..., v_n) = \alpha(v_1, ..., \lambda w, ..., v_n) = \lambda\alpha(v_1, ..., w, ..., v_n) = \alpha(v_1, ..., v_i', ..., v_n) = \alpha(v_1, ..., \lambda' w, ...v_n) = \lambda'\alpha(v_1, ..., w, ...v_n)$ Analog: $\alpha(v_1, ..., v_i + v_i', ..., v_n) = (\lambda + \lambda')\alpha(v_1, ..., w, ...v_n)$ □

Scherungsinvarianz und Homogenität sind geometrische Forderungen an ein Volumen:

1. Streckt man v_1 um λ in eine Richtung, so multipliziert sich das Volumen mit λ:

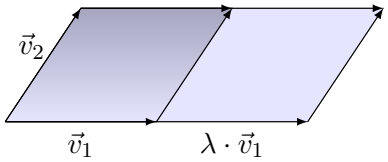


Abbildung 13 – Parallelogramme: Homogenität

2. Die beiden eingezeichneten Parallelogramme haben gleiche Flächen:

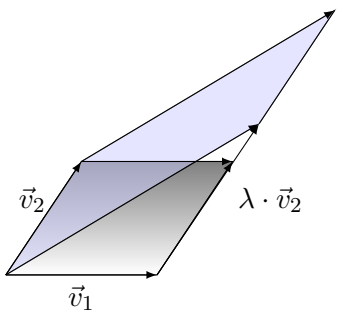


Abbildung 14 – Parallelogramme: Scherungsinvarianz

Definition: Eine alternierende n-Form $\alpha : V^n \to K$, $\alpha \neq 0$ auf einem n-dimensionalen K-Vektorraum V heißt Volumenform.

Satz 5.21 *Sei $n = \dim V$ und $(v_1, ..., v_n)$ eine Basis. Dann ist die lineare Abbildung $\mathrm{Alt}^n V \to K$, $\alpha \mapsto \alpha(v_1, ..., v_n)$ ein K-Vektorraumismorphismus. Insbesondere gibt es zu jedem $\lambda \in K$ genau eine alternierende n-Form α auf V mit $\alpha(v_1, .., v_n) = \lambda$ und es gilt $\dim \mathrm{Alt}^n V = 1$*

Beweis: Dies folgt mittels des Isomorphismus $K^n \xrightarrow{\sim} V$, $(\lambda_1, ..., \lambda_n) \mapsto \sum \lambda_i v_i$ aus dem nächsten Satz.

Satz 5.22 *Es existiert genau eine alternierende n-Form auf dem K^n*

$$\det : (K^n)^n \to K$$

mit $\det(e_1, ..., e_n) = 1$. Sie heißt Determinante.

Beweis: Wir fassen Vektoren $v_1, ..., v_n$ als Zeilen einer Matrix auf. Damit sind Existenz und Eindeutigkeit einer Funktion $\det : M_{n,n}(K) \to K$ zu zeigen und

(i) det ist multilinear in den Zeilen

(ii) sind zwei Zeilen gleich, so gilt $\det(A) = 0$

(iii) $\det(E_n) = 1$

Nach 5.18 und 5.20 sind (i) und (ii) zusammen äquivalent zu

(i)' det bleibt invariant unter der Zeilenumformung $v_i \mapsto v_i + \lambda + v_j$, $i \neq j$

(ii)' bei der Zeilenumformung $v_i \mapsto \lambda v_i$ multipliziert sich det mit λ

Beweis:
Eindeutigkeit: Sei det eine solche Funktion. Ist $(v_1, ..., v_n)$ linear abhängig, so gilt $\det(v_1, ..., v_n) = 0$ nach 5.19. Ansonsten kann man die Matrix mit den Zeilen $v_1, ..., v_n$ durch Zeilenumformungen vom Typ (i)' und (ii)' auf E_n transformieren. Wegen (iii) gilt $\det(E_n) = 1$ und rückwärts ist $\det(v_1, ..., v_n)$ eindeutig bestimmt.
Existenz: Für $n = 1$ setze $\det((a)) = a$. Sei $n \geq 2$ und $\det M_{n-1,n-1}(K) \to K$ bereits konstruiert. Sei $A \in M_{n,n}(K)$. Für $1 \leq i, j \leq n$ sei $A_{ij} \in M_{n-1,n-1}(K)$ die Matrix, die durch das Streichen der i-ten Zeile und j-ten Spalte aus A entsteht. Sei nun j, $1 \leq j \leq n$ beliebig, aber fest gewählt. Wir definieren $\det : M_{n,n}(K) \to K$ induktiv durch *Entwicklung nach der j-ten Spalte*:

$$\det A \overset{df}{=} \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij})$$

Zu zeigen: die so definierte Funktion erfüllt (i) - (iii).

$$\begin{aligned} \det(E_n) &= \sum_{i=1}^{n} (-1)^{i+j} \delta_{ij} \det((E_n)_{ij}) \\ &= \delta_{jj} \det(E_{n-1}) \\ &= 1 \end{aligned}$$

(i) folgt direkt aus der Definition. Bleibt (ii). Sei $v_s = v_k$ für $s \neq k$. Da det das Vorzeichen wechselt, wenn man zwei Zeilen vertauscht, erhalten wir:

$$\det(A_{sj}) = (-1)^{s+k} \det(A_{kj})$$

woraus wegen $a_{sj} = a_{kj}$ folgt:

$$0 = (-1)^{s+j} a_{sj} \det(A_{sj}) + (-1)^{k+j} a_{kj} \det(A_{kj})$$

Für $i \neq s$, $i \neq k$ hat A_{ij} zwei gleiche Zeilen, das heißt $\det(A_{ij}) = 0$ für $i \notin \{s, k\}$. Zusammen:

$$\begin{aligned}\det(A) &= \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij} \\ &= (-1)^{s+j} a_{sj} \det(A_{sj}) + (-1)^{k+j} a_{kj} \det(A_{kj})\end{aligned}$$

□

Man schreibt die Determinante auch in der Form

$$\det A = |A| = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

In kleinen Dimensionen:

n=1: $\det(a) = a$

n=2: $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - cb$

n=3: Entwicklung nach der ersten Spalte:

$$\begin{aligned}\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} &= a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21} \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31} \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \\ &= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ &\quad - a_{11}a_{32}a_{23} - a_{21}a_{12}a_{33} - a_{31}a_{22}a_{13}\end{aligned}$$

5.3 Eigenschaften der Determinante

Satz 5.23 *Eine Funktion $\alpha : M_{n,n}(K) \to K$, die (in den Zeilen) homogen und scherungsinvariant ist, ist von der Form*

$$\alpha = c \cdot \det \quad \textit{für } c \in K$$

Beweis: Nach 5.20 ist α eine alternierende n-Form. Nach 5.21 gilt $\dim \mathrm{Alt}^n K^n = 1$ und $0 \neq \det \in \mathrm{Alt}^n(K^n)$. Erinnerung:

$$E_j(\lambda) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \quad \lambda\text{an Stelle } (j,j)$$

$$E_{ij}(\lambda) = \begin{pmatrix} 1 & & \\ & \ddots & \\ \lambda & & 1 \end{pmatrix} \quad \lambda \text{ an Stelle } (i,j),\ i \neq j$$

Setze $E = E_n$. Es gilt $\alpha : M_{n,n}(K) \to K$:

- homogen $\Leftrightarrow$ $\alpha(E_j(\lambda) \cdot A) = \lambda \cdot \alpha(A)$
- scherungsinvarianz $\Leftrightarrow$ $\alpha(E_{ij}(\lambda) \cdot A) = \alpha(A)$

Korollar 5.24 *Es gilt:*

$$\begin{aligned}\det(E_j(\lambda)) &= \lambda \\ \det(E_{ij}(\lambda)) &= 1\end{aligned}$$

Beweis:
$\det(E_j(\lambda)) = \det(E_j(\lambda) \cdot E) = \lambda \cdot \det(E) = \lambda$
$\det(E_{ij}(\lambda)) = \det(E_{ij} \cdot E) = \det(E) = 1$

Satz 5.25

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

Beweis: Für festes B betrachten wir $\alpha = M_{n,n}(K) \to K$, $A \mapsto |A \cdot B|$. Es gilt:
$\alpha(E_j(\lambda) \cdot A) = |E_j(\lambda) \cdot AB| = \lambda |A \cdot B| = \lambda \cdot \alpha(A)$
$\rightsquigarrow$ α ist homogen
$\alpha(E_{ij}(\lambda) \cdot A) = |E_{ij}(\lambda) AB| = |AB| = \alpha(A)$
$\rightsquigarrow$ α ist scherungsinvariant
Nach 5.23 gilt $\alpha(A) = c \cdot |A|$ für alle A und festes $c \in K$. Setzt man $A = E$, so erhält man $c = |B|$.□

Satz 5.26 *Für die Determinante gilt:*

$$|A| = |A^t|$$

Beweis: Betrachte $\alpha : M_{n,n}(K) \to K$, $A \mapsto \det(A^t)$, dann gilt

$$\begin{aligned}
\alpha(E_j(\lambda)A) &= |(E_j(\lambda) \cdot A)^t| = |A^t \cdot E_j(\lambda)^t| = |A^t E_j(\lambda)| = |A^t| \cdot \lambda = \lambda \cdot \alpha(A) \\
\alpha(E_{ij}(\lambda)A) &= |E_{ij}(\lambda)A| = |A^t E_{ij}(\lambda)^t| = |A^t E_{ji}(\lambda)| = |A| = \alpha(A) \\
\alpha(E) &= \alpha(E^t) = |E| = 1
\end{aligned}$$

Also $\alpha = \det$

Korollar 5.27 (Entwicklung nach der i-ten Zeile)

$$|A| = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} |A_{ij}|$$

Beweis: Man entwickle $|A^t|$ nach der i-ten Spalte und verwende 5.26. □

Def. 5.28 (Adjunkte) *Die Matrix $\widetilde{A} = (\widetilde{a}_{ij})$ mit*

$$\widetilde{a}_{ij} = (-1)^{i+j} |A_{ji}|$$

heißt die Adjunkte zu A.

Beispiel:

$$\begin{aligned}
A = \begin{pmatrix} 3 & 5 \\ 1 & 3 \end{pmatrix} \Rightarrow \widetilde{A} &= \begin{pmatrix} 3 & -5 \\ -1 & 3 \end{pmatrix} \\
\widetilde{A} \cdot A = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = A \cdot \widetilde{A} &= \begin{pmatrix} |A| & 0 \\ 0 & |A| \end{pmatrix}
\end{aligned}$$

Satz 5.29 (Erste Cramersche Regel)

$$\widetilde{A} \cdot A = A \cdot \widetilde{A} = |A| \cdot E$$

Beweis: Sei $(B)_{ij}$ die Koeffizienten der Matrix B an der Stelle (ij). Es gilt:

$$\begin{aligned}
(A \cdot \widetilde{A})_{ii} &= \sum_j a_{ij} \widetilde{a}_{ji} \\
&= \sum_j a_{ij} (-1)^{i+j} |A_{ij}| \\
&= |A|
\end{aligned}$$

Für $i \neq j$ ist

$$(A \cdot \widetilde{A})_{ij} = \sum_k (-1)^{j+k} a_{ik} |A_{jk}|$$

Rechts steht die Entwicklung nach der j-ten Zeile der Matrix, die man erhält, wenn man in A die j-te durch die $i$te Zeile ersetzt, das heißt 0.
Der Beweis von $\widetilde{A} \cdot A = |A| \cdot E$ geht analog mit Spaltenentwicklung. □

Korollar 5.30

$$A \in M_{n,n,}(K) \text{ } \textit{invertierbar} \Leftrightarrow |A| \neq 0$$

Beweis: "⇒" A invertierbar ⇒ $1 = |E| = |A \cdot A^{-1}| = |A| \cdot |A^{-1}|$ also $|A| \neq 0$.
"⇐" Ist $|A| \neq 0$, so gilt $|A|^{-1} \cdot \widetilde{A} \cdot A = E$, also ist A invertierbar. □

Korollar 5.31 det *induziert einen surjektiven Gruppenhomomorphismus:*

$$\det : GL_n(K) \to K^\times$$

Beweis: $A \in GL_n(K) \Rightarrow \det(A) \in K^\times$ nach 5.30. Die Homomorphieeigenschaft folgt aus 5.25. Surjektivität folgt aus $|E_j(\lambda)| = \lambda$.

Def. 5.32 (Spezielle Lineare Gruppe) *Die Gruppe*

$$SL_n(K) = ker(\det : GL_n(K) \to K^\times)$$

heißt Spezielle Lineare Gruppe[8]*.*

Satz 5.33 *Es sei $R \subset K$ ein unitärer Unterring und A eine $n \times n$-Matrix mit Koeffizienten in R. Es sei $A \in GL_n(K)$. Die Matrix A^{-1} hat genau dann Koeffizienten in R, wenn $|A| \in R^\times$.*

Beweis: Entwicklung nach Spalten zeigt induktiv, dass $|A| \in R$. Hat A^{-1} Koeffizienten in R, so gilt $|A^{-1}| \cdot |A| = 1 \Rightarrow |A| \in R^\times$. Die Koeffizienten von $\widetilde{A}$ sind Wechselsummen von Determinanten von Untermatrizen und daher in R. Gilt $|A| \in R^\times$, so hat auch $A^{-1} = |A|^{-1}\widetilde{A}$ Koeffizienten in R. □

Korollar 5.34 *Sei A eine $n \times n$-Matrix mit Koeffizienten in $\mathbb{Z}$. Es existieren genau dann A^{-1} mit Koeffizienten in $\mathbb{Z}$, wenn $|A| = \pm 1$.*

Beweis: Es gilt $\mathbb{Z}^\times = \{\pm 1\}$.

Satz 5.35 (Zweite Cramersche Regel) *Das lineare Gleichungssystem $A \cdot x = b$, $A \in GL_n(K)$, $b \in K^n$ hat die Lösung*

$$x = |A|^{-1} \cdot \widetilde{A} \cdot b$$

Für die i-te Komponente x_i von x gilt:

$$x_i = |A|^{-1} \sum_j (-1)^{i+j} |A_{ij}| \cdot b_j = \frac{|(A, i, b)|}{|A|}$$

Hierbei ist (A, i, b) die Matrix, die aus A entsteht, wenn man die i-te Spalte durch b ersetzt.

Beweis: $A^{-1} = |A|^{-1} \cdot \widetilde{A}$.
Praktische Regeln für det*:*

- $B \in M_{n,n}(K)$ und $k \in \mathbb{N}$ so gilt:

$$\begin{vmatrix} E_k & 0 \\ A & B \end{vmatrix} = |B|$$

  Entwicklung nach der 1. Zeile und Induktion nach k

[8] Dies ist die Gruppe aller $n \times n$-Matrizen mit det = 1 = neutrales Element von $K^\times$ und nicht det = 0.

- Analog für $A \in M_{s,s}(K)$:

$$\begin{vmatrix} A & 0 \\ B & E_k \end{vmatrix} = |A| = \begin{vmatrix} E_k & B \\ 0 & A \end{vmatrix}$$
$$\begin{vmatrix} 0 & A \\ E_k & B \end{vmatrix} = (-1)^s \cdot |A| = \begin{vmatrix} B & A \\ E_k & 0 \end{vmatrix}$$

- Sind A und C quadratisch:

$$\begin{vmatrix} A & 0 \\ B & C \end{vmatrix} = \begin{vmatrix} A & 0 \\ B & E \end{vmatrix} \cdot \begin{vmatrix} E & 0 \\ 0 & C \end{vmatrix} = |A| \cdot |C|$$

  und durch transponieren erhalten wir:

$$\begin{vmatrix} A & B \\ 0 & C \end{vmatrix} = |A| \cdot |C|$$

- Induktiv erhält man:

$$\begin{vmatrix} \lambda_1 & & 0 \\ & \ddots & \\ * & & \lambda_n \end{vmatrix} = \lambda_1 \cdot ... \cdot \lambda_n = \begin{vmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{vmatrix}$$

Def. 5.36 (Orientierungserhaltende Matrizen)
Die Elemente der Gruppe $GL_n^+(\mathbb{R}) = \left\{A \in GL_n(\mathbb{R}) \middle| |A| > 0\right\}$ *heißen orientierungserhaltend.*

Lemma 5.37 *Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum und B die Menge der Basen von V. Die Relation $\underline{v} \sim \underline{w} \Leftrightarrow M_{\underline{w}}^{\underline{v}}(id_V) \in GL_n^+(\mathbb{R})$ ist eine Äquivalenzrelation auf B. Es existieren genau zwei Äquivalenzklasse. .*

Beweis: Da sich die Transformationsmatrizen (und damit auch deren Determinanten) multiplizieren lassen, ist $\sim$ eine Äquivalenzrelation. Sei nun $\underline{v}$ eine fixierte Basis, dann gilt $\underline{w} \not\sim \underline{v}$ und $\underline{w'} \not\sim \underline{v}$ $\Rightarrow$ $\underline{w} \sim \underline{w'}$. Also gibt es höchstens zwei Äquivalenzklassen. Da det surjektiv ist, kommen negative det vor, also gilt $GL_n^+(\mathbb{R}) \subsetneq GL_n(\mathbb{R})$ und daher existieren genau zwei Klassen. □

Def. 5.38 (Orientierung, orientierte Basis)
Die Auswahl einer Äquivalenzklasse bezüglich $\sim$ heißt Orientierung des n-dimensionalen reellen Vektorraums V. Jedes Element dieser Äquivalenzklasse heißt dann orientierte Basis.

Bemerkung: Der $\mathbb{R}^n$ wird durch die Äquivalenzklasse der Standardbasis orientiert (kanonische Orientierung des $\mathbb{R}^n$).. Eine Basis $(v_1, ..., v_n)$ des $\mathbb{R}^n$ ist somit genau dann orientiert, wenn $\det(v_1, ..., v_n) > 0$.
Beispiel: Sei (x, y) linear unabhängig in $\mathbb{R}^3$, dann ist $z := x \times y \neq 0$ und es gilt $\det(x, y, z) = \langle x \times y, z\rangle = \langle z, z\rangle = |z|^2 > 0$ nach Kapitel 0. Also ist $(x, y, x \times y)$ eine orientierte Basis des $\mathbb{R}^3$.

5.4 Leibniz-Formel

Erinnerung: $\mathfrak{S}_n = Aut(\{1, ..., n\})$ mit Elementen *Permutationen*

$$\pi = \begin{pmatrix} 1 & 2 & ... & n \\ \pi(1) & \pi(2) & ... & \pi(n) \end{pmatrix}$$

Def. 5.39 (Transposition) *Ein $\sigma \in \mathfrak{S}_n$ heißt Transposition, wenn es zwei Zahlen vertauscht und alle anderen festhält. Schreibweise: $\sigma = (i\, j)$ vertauscht i und j, $(i \neq j)$ und hält alle anderen Zahlen fest.*

Lemma 5.40 *Die Transpositionen erzeugen $\mathfrak{S}_n$, das heißt jedes Element in $\mathfrak{S}_n$ kann (auf nicht notwendigerweise endliche Weise) als Produkt von Transpositionen erzeugt werden.*

Beweis:
$n = 1$: die Aussage ist formal. $n = 2$: die Aussage ist trivial. Sei $n > 2$ Induktion über n. Betrachte

$$\mathfrak{S}_{n-1} \to \mathfrak{S}$$
$$\pi \mapsto \begin{pmatrix} 1 & 2 & ... & n-1 & n \\ \pi(1) & \pi(2) & ... & \pi(n-1) & n \end{pmatrix}$$

Sei nun $\sigma \in \mathfrak{S}_n$ beliebig. Gilt $\sigma(n) = n$, $1 \leq m \leq n-1$, so ist $(m\,n)\sigma \in \mathfrak{S}_{n-1}$ also Produkt von Transpositionen. $(m\,n)\sigma) = t_1...t_r$ also $\sigma = (n\,m)t_1...t_r$

Lemma 5.41 *Die Abbildung*

$$\operatorname{sgn} : \mathfrak{S}_n \to \{\pm 1\}, \quad \sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{i-j}{\sigma(i) - \sigma(j)}$$

ist ein Gruppenhomomorphismus.

Beweis: Im Zähler und Nenner von

$$\prod_{1 \leq i < j \leq n} \frac{i-j}{\sigma(i) - \sigma(j)}$$

kommen bis auf Reihenfolge und Vorzeichen die gleichen Faktoren vor, also ist $\operatorname{sgn}(\sigma) \in \{\pm 1\}$. Für $\sigma, \tau \in \mathfrak{S}_n$ und $1 \leq i < j \leq n$, $\tau(i) > \tau(j)$ gilt:

$$\frac{\tau(i) - \tau(j)}{\sigma\tau(i) - \sigma\tau(j)} = \frac{\tau(j) - \tau(i)}{\sigma\tau(j) - \sigma\tau(i)}$$

also gilt

$$\prod_{1 \leq i < j \leq n} \frac{\tau(i) - \tau(j)}{\sigma\tau(i) - \sigma\tau(j)} = \prod_{1 \leq i < j \leq n} \frac{i-j}{\sigma(i) - \sigma(j)}$$

$\Rightarrow$

$$\begin{aligned} \operatorname{sgn}(\sigma\tau) &= \prod_{1 \leq i < j \leq n} \frac{i-j}{\sigma\tau(i) - \sigma\tau(j)} \\ &= \prod_{1 \leq i < j \leq n} \frac{\tau(i) - \tau(j)}{\sigma\tau(i) - \sigma\tau(j)} \cdot \prod_{1 \leq i < j \leq n} \frac{i-j}{\tau(i) - \tau(j)} \\ &= \prod_{1 \leq i < j \leq n} \frac{i-j}{\sigma(i) - \sigma(j)} \cdot \prod_{1 \leq i < j \leq n} \frac{i-j}{\tau(i) - \tau(j)} \\ &= \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) \end{aligned}$$

Def. 5.42 (Vorzeichen, Signum) *Die Zahl* $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ *heißt Vorzeichen oder Signum der Permutation* σ*.*

Lemma 5.43
Für $t = (i\,j) \in \sigma_n$ *gilt* $\operatorname{sgn}(t) = -1$

Beweis: Sei $t = (i, j) \in \mathfrak{S}_n$, ohne Einschränkung $i < j$ Vorzeichen von $\frac{\alpha - \beta}{t(\alpha) - t(\beta)}$ für $1 \leq \alpha < \beta \leq n$

$\{\alpha, \beta\} \cap \{i, j\} = \emptyset$	$+$	
$\alpha = i < \beta \leq j$	$-$ $(j-i)$-mal	
$\alpha = i < j < \beta$	$+$	
$\alpha < i < j = \beta$	$+$	Es folgt $\operatorname{sgn}(t) = (-1)^{2j-2i-1} = (-1)$.
$i < \alpha < j = \beta$	$-$ $(j-i-1)$-mal	
$i < j = \alpha < \beta$	$+$	
$\alpha < \beta = i < j$	$+$	

Satz 5.44 *Ist $\sigma = t_1 ... t_r$ eine Darstellung von σ also Produkt von Transpositionen, so gilt* $\operatorname{sgn}(r) = (-1)^r$. *Insbesondere ist $r \mod$ unabhängig von der Wahl der Darstellung.*

Beweis: $\operatorname{sgn}(\sigma) = \sigma(t_1) ... \operatorname{sgn}(t_r) = (-1)^r$. □
Anwendung: Schiebespiel:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

Abbildung 15 – Das Schiebespiel: Originalzustand und gewünschter Zustand

Frage: Kommt man vom linken Zustand zum Rechten durch Verschieben des leeren Feldes?
Antwort: Nein. Begründung: Wir bezeichnen das leere Feld mit 16. Jeder Zustand des Spiels entspricht einem Element σ_{16}. Jeder einzelnde Zug entspricht einer Transposition.

+	-	+	-
-	+	-	+
+	-	+	-
-	+	-	+

Abbildung 16 – Das Schiebespiel: Bezeichnung der Felder

Das Schema aus Abbildung 16 zeigt, dass ein Zustand σ mit Loch unten rechts nur nach einer geraden Anzahl von Zügen erreicht wird, das heißt $\operatorname{sgn}\sigma = +1$. Wegen $\operatorname{sgn}(1\,2) = -1$ kann dieser Zustand nicht erreicht werden.

Def. 5.45 (Alternierende Gruppe) *Die Untergruppe $\mathfrak{A}_n$ mit*

$$\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n | \operatorname{sgn}(\sigma) = +1\}$$

heißt die alternierende Gruppe (über n Elemente)

Bem: $\mathfrak{A}_n = ker(\operatorname{sgn}(\sigma_n) \to \{\pm 1\})$ und für $n \geq 2$ ist sgn surjektiv. $\Rightarrow n \geq 2 : \sharp\mathfrak{A}_n = \frac{1}{2}\sharp\mathfrak{S}_n = \frac{n!}{2}$. Nun sei K ein Körper. Wir betrachten die Abbildung

$$\varphi : \sigma_n \to GL_n(K),\ \varphi(\sigma)(e_i) = e_{\sigma(i)}$$

das heißt

$$\varphi(\sigma) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}$$

Seien $\sigma, \tau \in \mathfrak{S}_n$ und $x \in K^n$. Setzt man $y = \varphi(\tau)(x)$, so gilt $y_i = x_{\tau^{-1}(i)}$, $i = 1, ..., n$ und somit $\varphi(\sigma) \circ \varphi(\tau)(x_i) = (\varphi(\sigma)(y))_i = x_{\tau^{-1}(i)} = x_{(\sigma\tau)^{-1}(i)} = \varphi(\sigma\tau)(x)_i$. Dies zeigt $\varphi(\sigma) \circ \varphi(\sigma\tau)(x)\, \forall x$ also $\varphi(\sigma) \circ \varphi(\tau) = \varphi(\sigma\tau)$, daher ist φ ein (injektiver) Gruppenhomomorphismus.

Def. 5.46 (Permutationsmatrizen) *Matrizen der Form $\varphi(\sigma)$, $\sigma \in \mathfrak{S}_n$ heißen Permutationsmatrizen. Ist $t = (i\,j)$, so gilt $\varphi(t) = P_{ij}$ das heißt die Matrix, die aus E_n durch Vertauschen der i-ten und j-ten Zeile entsteht und daher* $\det(\varphi(t)) = \det P_{ij} = -1_K$.

Korollar 5.47 *Ist $\sigma \in \mathfrak{S}_n$ Produkt von r Transpositionen, so gilt* $\det(\varphi(\sigma)) = (-1_k)^r = \operatorname{sgn}(\sigma)$. *Hier fassen wir* $\operatorname{sgn}(\sigma) \in \{\pm 1\}$ *als Element von K auf.*

Satz 5.48 (Leibniz-Formel) *Für $A = (a_{ij}) \in M_{n,n}(K)$:*

$$|A| = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} ... a_{n,\sigma(n)}$$

Beweis:

$$|A| = \det\left(\sum_j a_{1j}e_j, ..., \sum_j a_{nj}e_j\right)$$

Multlineares Ausrechnen:

$$|A| = \sum_{J=(j_1,...,j_n)} a_{1j_1}...a_{nj_n}\det(e_{j_1}...e_{j_n})$$

Ist $\begin{pmatrix} 1 & ... & n \\ j_1 & ... & j_n \end{pmatrix}$ keine Permutation, so ist $\det(e_{j_1}...e_{j_n}) = 0$ (ein Vektor ist doppelt). Ist $\sigma = \begin{pmatrix} 1 & ... & n \\ j_1 & ... & j_n \end{pmatrix}$ eine Permutation, so gilt $\det(e_{j_1}...e_{j_n}) = \operatorname{sgn}(\sigma)$. nach 5.47.

Korollar 5.49 *Für $K = \mathbb{R}$ ist* $\det : \mathbb{R}^{n^2} = M_{n,n}(\mathbb{R}) \to \mathbb{R}$ *beliebig oft stetig differenzierbar.*

Ist R ein kommutativer unitäter Ring, der Teilring eines Körper K ist, so kann man det einer quadratischen Matrix mit Einträgen in R definieren, indem man die Einträge als Elemente von K auffasst. Wegen der Leibniz-Formel ist det wieder in R und von Auswahl von K unabhängig.
Beispiel: $R = K[t]$, K Körper. Wir betrachten die Äquivalenzrelation auf $K[t] \times (K[t] \setminus \{0\}$ durch $(f_1, g_1) \sim (f_2, g_2) \Leftrightarrow f_1g_2 = f_2g_1$.
Übungsaufgabe: Verifiziere Ä1- Ä3. Die Äquivalenzklassen des Paares $(f, g), g \neq 0$ wird mit $\frac{f}{g}$ bezeichnet. Die Äquivalenzklassen heißen rationale Funktionen. Rechnen wie mit gewohnten Brüchen:

$$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 \cdot f_2}{g_1 \cdot g_2}, \frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1g_2 + f_2g_1}{g_1g_2}$$

Die Menge der rationalen Funktionen wird mit $K(t)$ bezeichnet, $K(t)$ ist ein kommutativer Ring mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1}$. Es gilt $\frac{f}{g} \neq \frac{0}{1}$ genau dann, wenn $f \neq 0$ ist. Daher hat $\frac{f}{g}$ das Inverse $\frac{g}{f}$, weshalb $K(t)$ ein Körper ist. Die Zuordnung $K[t] \to K(t)$, $f \mapsto \frac{f}{1}$ ist ein injektiver Ringhomomorphismus.

Def. 5.50 *Sei R ein kommutativer unitärer Ring und $A \in M_{n,n}(R)$, so definiert man* $\det(A) \in R$ *über die Leibniz-Formel. Man kann dann zeigen:*

1. det *kann über Zeilen- oder Spaltenentwicklung berechnet werden*
2. $\det(AB) = \det(BA)$, $A \cdot \widetilde{A} = \widetilde{A} \cdot A = \det(A) \cdot E$
3. *A ist genau dann invertierbar, wenn* $\det(A) \in R^\times$*, dann gilt* $A^{-1} = \det(A)^{-1} \cdot \widetilde{A}$
4. *Ist $f : R \to S$ ein Ringhomomorphismus, so gilt für $f(A) \in M_{n,n}(S)$:* $\det(f(A)) = f(\det(A))$

5.5 Das Charakteristische Polynom

Sei $A \in M_{n,n}(K)$.

Def. 5.51 (Spur) *Die Spur von $A = (a_{ij})$ ist definiert durch*

$$sp(A) = \sum_{i=1}^{n} a_{ii}$$

Lemma 5.52 *Es gilt:*

$$sp(AB) = sp(BA)$$

Beweis:

$$(AB)_{ii} = \sum_j a_{ij} b_{ji}$$
$$(BA)_{ii} = \sum_i b_{ji} a_{ij}$$
$$sp(AB) = \sum_{i,j} a_{ij} b_{ji} = sp(BA)$$

□

Korollar 5.53 *Für $T \in GL_n(K)$ gilt*

$$\det(T \cdot A \cdot T^{-1}) = \det A$$
$$sp(T \cdot A \cdot T^{-1}) = sp(A)$$

Beweis:
$\det(T \cdot A \cdot T^{-1}) = \det(T \cdot T^{-1} \cdot A) = \det(A)$
$sp(T \cdot A \cdot T^{-1}) = sp(T \cdot T^{-1} \cdot A) = sp(A)$ □

Def. 5.54 (Charakteristisches Polynom) *Sei $A \in M_{n,n}(K)$. Das Polynom $\chi_A(t) = \det(tE - A) \in K[t]$ heißt das charakeristische Polynom der Matrix A.*

Lemma 5.55 *χ_A ist normiert vom Grad n*

$$\chi_A(t) = t^n + c_{n-1}t^{n-1} + ... + c_0$$

und es gilt $c_0 = \chi_A(0) = (-1)^n|A|$ und $c_{n-1} = -sp(A)$.

Beweis: Die Leibniz-Formel zeigt, dass χ_A die Form $\chi_A(t) = (t-a_{11})...(t-a_{nn}+Polynom\,vom\,Grad \leq n-2$ hat. Daher ist χ_A normiert vom Grad n und $c_{n-1} = -a_{11} - a_{22} - ... - a_{nn}$ Schließlich gilt $c_0 = \chi_A(0) = |0 \cdot E - A| = |-A| = (-1)^n|A|$ □

Lemma 5.56 *Ist $T \in GL_n(K)$ so gilt*

$$\chi_{TAT^{-1}}(t) = \chi_A(t)$$

Beweis:

$$\chi_{TAT^{-1}} = |tE - TAT^{-1}| = |T(tE - A)T^{-1}| = |T| \cdot |tE - A| \cdot |T^{-1}|$$
$$= \chi_A(t)$$

□

Unsere Regeln zur Determinantenberechnung wenden sich nun hier an und wir erhalten:
Drehmatrix:

$$A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \Rightarrow tE - A = \begin{pmatrix} t-\lambda_1 & & -* \\ & \ddots & \\ 0 & & t-\lambda_n \end{pmatrix}$$
$$\Rightarrow \chi_A(t) = (t-\lambda_1)(t-\lambda_2)...(t-\lambda_n)$$

Blockmatrix:

$$A = \begin{pmatrix} B & * \\ 0 & C \end{pmatrix} \quad oder \quad A = \begin{pmatrix} B & 0 \\ * & C \end{pmatrix}$$
$$\Rightarrow \chi_A(t) = \chi_B(t) \cdot \chi_C(t)$$

Sei nun $f = c_0 + c_1 t + ... + c_r t^r \in K[t]$ ein Polynom. Wir können $A \in M_{m,m}(K)$ in f einsetzen durch die Regel

$$f(A) = c_0 E + c_1 A + c_2 A^2 + ... + c_r A^r \in M_{m,m}(K)$$

Bemerkung: Man sieht leicht für $f, g \in K[t]$ und $A \in M_{m,m}(K)$:

$$f(A) \cdot g(A) = (fg)(A) = (gf)(A) = g(A) \cdot f(A)$$

das heißt, die Matrizen $f(A)$ und $g(A)$ kommutieren.

Satz 5.57 (Cayley-Hamilton)

$$\chi_A(A) = 0$$

mit der 0 *als Nullelement der* $n \times n$*-Matrizen.*

Beweis: Sei D die Adjunkte zu $tE - A$, also

$$D(tE - A) = \det(tE - A) \cdot E = \chi_A(t)E \qquad (*)$$

In der Definition der Adjunkte treten Determinanten von $(n-1) \times (n-1)$-Untermatrizen auf, also sind die Einträge von D Polynome vom Grad $\leq n - 1$.

$$D = \sum_{i=0}^{n-1} D_i t^i \quad D_i \in M_{n,n}(K)$$

Des weiteren sei $\chi_A(t) = \sum_{i=0}^{n} a_i t^i$; $a_i \in K$. Ein Koeffizientenvergleich in $(*)$ liefert: $D_{i-1} - D_i A = a_i \cdot E$ wobei wir $D_{-1} = 0$, $D_n = 0$ ergänzen. Es folgt

$$\begin{aligned}\chi_A(t) = \sum_{i=0}^{n} a_i A^i &= \sum_{i=0}^{n} (D_{i-1} - D_i A) A^i \\ &= -D_0 A + D_0 A - D_1 A^2 + D_1 A^2 - ... + D_{n-1} A^n - D_n A^{n+1} \\ &= 0\end{aligned}$$

□

5.6 Endomorphismen

Sei $f : V \to W$ eine lineare Abbildung. Wir haben gelernt 3.21, dass sich f bei Wahl geeigneter Basen $(v_1, ..., v_n)$, $(w_1, ..., w_n)$ von V und W durch die Matrix

$$\begin{pmatrix} & \overbrace{\quad}^{r} & \\ r \left\{ \right. & \begin{matrix} 1 & & \\ & 1 & \\ & & 1 \end{matrix} & \\ & & \end{pmatrix}$$

darstellen lässt. $(r = rg(f))$.
Sei nun V ein n-dimensionaler K-Vektorraum und $\alpha : V \to V$ ein Endomorphismus, das heißt $\alpha \in End(V)$. Sei A die Darstellungsmatrix von α bezüglich einer Basis $(v_1, ..., v_n)$. Bezüglich einer anderen Basis $(v_1', ..., v_n')$ wird α durch die Matrix TAT^{-1} dargestellt, wobei $T \in GL_n(K)$ die Transformationsmatrix ist. Nach 5.56 hängt das charakeristische Polynom nicht von der Wahl der Basis ab und wir erhalten, dass folgende Objekte wohldefiniert sind:

Def. 5.58

$$\chi_\alpha(t) = \chi_A(t)$$
$$sp(\alpha) = sp(A)$$
$$\det \alpha = \det A$$

wobei A die Darstellungsmatrix von α bezüglich irgendeiner Basis ist.

Def. 5.59 (Eigenräume, Eigenwerte, Eigenvektoren) *Sei $\alpha \in End(V)$. Ein $\lambda \in K$ heißt Eigenwert von α, wenn es einen Vektor $v \in V$ gibt mit $v \neq 0$ und $\alpha(v) = \lambda v$. Ist λ ein Eigenwert von α, so heißt der Unterraum $v_\lambda = ker(\lambda \cdot id - \alpha)$ der Eigenraum zu α und seine Elemente $\neq 0$ das heißt $v \neq 0$ mit $\alpha(v) = \lambda v$ heißen Eigenvektoren zum Eigenwert λ.*

Bemerkung: Ideal wäre es, wenn man V in die direkte Summe von Eigenräumen zerlegen könnte. Dann hätte α bezüglich einer anderen Basis von V Diagonalgestalt. Leider geht das nicht immer. Beispiel:

$$\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in GL_n(\mathbb{R})$$

entspricht der Drehung um $\frac{\pi}{2}$ in der Ebene und hat keinen Eigenwert.

Satz 5.60 *Die Eigenwerte von α sind genau Nullstellen von $\chi_A(t)$*

Beweis: Es sei α bezüglich irgendeiner Basis durch die Matrix A dargestellt. Dann gilt:

$$\begin{aligned} &\lambda \, Eigenwert \, von \, \alpha \Leftrightarrow \exists v \neq 0 : \alpha(v) = \lambda v \\ \Leftrightarrow \exists v \neq 0 : (\lambda \cdot id_v - \alpha)(v) = 0 &\Leftrightarrow ker(\lambda \cdot id_V - \alpha) \neq 0 \\ &\Leftrightarrow \det(\lambda E - A) = 0 \Leftrightarrow \chi_A(\lambda) = 0 \end{aligned}$$

□

Bemerkung: Damit sehen wir auch algebraisch, dass $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ keine Eigenwerte hat, da $\chi_A(t) = t^2 + 1$ keine reellen Nullstellen hat. Aber $\pm i$ sind komplexe Nullstellen, das heißt als komplexe Matrix besitzt A zwei Eigenwerte.
Sei nun $f = c_0 + c_1 + ... + c_r t^r \in K[t]$, V ein n-dimensionaler Vektorraum und $\alpha \in End(V)$. Da $End(V)$ ein unitärer Ring mit K als Unterring ist, kann man Endomorphismen in f einsetzen und erhält wieder Endomorphismen.
Explizit:

$$f(\alpha) = c_0 \cdot id_V + c_1\alpha + c_2\alpha \circ \alpha + c_3\alpha \circ \alpha \circ \alpha + ... + c_r \underbrace{\alpha \circ ... \circ \alpha}_{r-mal}$$

Bemerkung: Man sieht leicht für $f, g \in K[t]$ und $\alpha \in End(V)$, dass $f(\alpha) \cdot g(\alpha) = (f \cdot g)(\alpha) = (g \cdot f)(\alpha) = g(\alpha) \cdot f(\alpha)$ das heißt, dass die Endomorphismen $f(\alpha)$ und $g(\alpha)$ kommutieren.

Satz 5.61 (Cayley-Hamilton für Endomorphismen)

$$\chi_A(\alpha) = 0$$

für alle $\alpha \in End_K(V)$

Beweis: Sei α bezüglich einer Basis durch die Matrix A dargestellt, dann wird für $f \in K[t]$ $f(\alpha)$ durch $f(A)$ dargestellt. Insbesondere wird $\chi_A(\alpha)$ durch $\chi_A(A) = 0$ (nach 5.57, Cayley-Hamilton für Matrizen) dargestellt. □

5.7 Zerlegung in Eigenräume

Sei V ein n-dimensionaler K-Vektorraum und $\alpha \in End_K(V)$.

Def. 5.62 (Diagonalgestalt) *Man sagt eine Matrix $A = (a_{ij})$ habe Diagonalgestalt falls $a_{ij} = 0$ wenn $i \neq j$. Der Endomorphismus α von V heißt diagonalisierbar, falls es eine Basis $(v_1, ..., v_n)$ von V gibt, bezüglich der die Darstellungsmatrix von α Diagonalgestalt hat.*
Schreibweise: $A = diag(a_{11}, ..., a_{nn})$

Lemma 5.63 *Der Endomorphismus α ist genau dann diagonalisierbar, wenn es eine Basis $(v_1, ..., v_n)$ von V bestehend aus den Eigenvektoren zu α gibt.*

Beweis: Es ist $diag(\lambda_1, ..., \lambda_n)$ genau dann Darstellungsmatrix von α bezüglich eines Basis $(v_1, ..., v_n)$, wenn $\alpha(v_i) = \lambda_i v_i$ gilt. □
Bemerkung: Ist α diagonalisierbar, also die Darstellungsmatrix von α bezüglich $(v_1, ..., v_n)$ von Diagonalgestalt $diag(\lambda_1, ..., \lambda_n)$ so gilt

$$\chi_A(t) = |diag(t - \lambda_1, ..., t - \lambda_n)| = \prod_{i=1}^{n}(t - \lambda_i)$$

das heißt $\chi_\alpha(t)$ zerfällt in Linearfaktoren.

Satz 5.64 *Es seien $\lambda_1, ..., \lambda_m$ paarweise verschiedene Eigenwerte von α und $v_1, ..., v_m$ Eigenvektoren zu $\lambda_1, ..., \lambda_n$, dann ist das System $(v_1, ..., v_m)$ linear unabhängig.*

Beweis: Nach Voraussetzung gilt

$$(\alpha - \lambda_i id_V)(v_j) = (\lambda_j - \lambda_i)v_j$$

Setzt man für $i = 1...m$

$$\beta_i = (\alpha - \lambda_1 id_V) \circ (\alpha - \lambda_2 id_V) \circ ... \circ (\alpha - \lambda_{i-1} id_V) \circ (\alpha - \lambda_{i+1} id_V) \circ (\alpha - \lambda_m id_V)$$

so folgt

$$\beta_i(v_j) = \left(\prod_{k \neq i}(\lambda_j - \lambda_k)\right) v_j = \begin{cases} 0 & i \neq j \\ (Skalar \neq 0) \cdot v & i = j \end{cases}$$

Gilt nun $\alpha_1, ..., \alpha_m \in K$, $\alpha_1 v_1 + ... + \alpha_m v_m = 0$, so gilt nach Anwenden von $\beta_i : \alpha(Skalar \neq 0)v_i = 0$ $\Rightarrow \alpha_i = 0 \Rightarrow (v_1, ..., v_m)$ ist linear unabhängig. □

Satz 5.65 *Sei V ein n-dimensionaler Vektorraum und $\alpha \in End_K(V)$. Zerfällt das charakeristische Polynom von α in paarweise verschiedene Linearfaktoren, das heißt*

$$\chi_\alpha(t) = (t - \lambda_1)...(t - \lambda_n)$$

mit $\lambda_i \neq \lambda_j$ für $i \neq j$, dann gibt es eine Basis von V aus Eigenvektoren von α. Insbesondere wird α bezüglich dieser Basis durch eine Diagonalmatrix dargestellt.

Beweis: In diesem Fall sind $\lambda_1, ..., \lambda_n$ paarweise verschiedene Eigenwere von α. Sind $v_1, ..., v_n$ assoziative Eigenvektoren, so ist nach 5.64 $(v_1, ..., v_n)$ ein linear unabhängiges System und wegen $n = dim(V)$ eine Basis. □

Wie macht man das explizit?

Betrachte den Endomorphismus α des $\mathbb{R}^2$, der bezüglich der kanonischen Basis durch $A = \begin{pmatrix} 1 & -2 \\ 1 & 4 \end{pmatrix}$ dargestellt wird. Dann ist das charakeristische Polynom:

$$\chi_A(t) = \det \begin{pmatrix} t-1 & 2 \\ -1 & t-4 \end{pmatrix} = t^2 - 5t + 6 = (t-2)(t-3)$$

Suche Eigenvektoren, betrachte dazu das homogene Lineare Gleichungssystem für $\lambda = 2$:

$$(2E - A)x = 0$$
$$\begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0$$

Nichttriviale Lösung: $\begin{pmatrix} 2 \\ -1 \end{pmatrix}$ ist Eigenvektor zum Eigenwert $\lambda = 2$.

Probe:

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

Für $\lambda = 3$: Lösung: $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$ ist Eigenvektor zum Eigenwert 3.

Probe:

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

Also hat α bezüglich der Basis $\begin{pmatrix} 2 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix}$ die Darstellungsmatrix $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$.

Testrechnung: Der Basiswechsel von $\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$ zu $\left(\begin{pmatrix} 2 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right)$ ist durch die Transformationsmatrix $T = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}^{-1}$ gegeben. $\Rightarrow T = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ Wenden wir den Basiswechselsatz an, so müssten wir erhalten $TAT^{-1} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. Probe:

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

5.8 Trigonalisierbarkeit

Def. 5.66 (Trigonalisierbarkeit) *Sei V ein K-Vektorraum und $\alpha \in End_K(V)$, dann heißt α trigonalisierbar, wenn es eine Basis von V gibt, bezüglich derer α durch die obere Dreiecksmatrix, das heißt Matrix der Form*

$$\begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix}$$

dargestellt wird.

Satz 5.67 *α ist genau dann trigonalisierbar, wenn $\chi_\alpha(t)$ vollständig in Linearfaktoren zerfällt.*

Beweis: Ist α bezüglich einer Basis durch $A = \begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix}$ gegeben, so gilt

$$\chi_A(t) = \det(tE - A) = (t - \lambda_1)...(t - \lambda_n)$$

Die andere Richtung beweisen wir per Induktion nach n. Falls $n = 1$: klar. Sei $\chi_\alpha(t) = (t-\lambda_1)...(t-\lambda_n)$ und sei v_1 ein Eigenvektor zum Eigenwert λ_1. Ergänze v_1 zu einer Basis $(v_1, ..., v_n)$ von V. Bezüglich dieser Basis hat α die Gestalt

$$\begin{pmatrix} \lambda_1 & * \\ 0 & A' \end{pmatrix}$$

mit einer $(n-1) \times (n-1)$-Matrix A'. Sei $V' = Lin(v_2, ..., v_n)$, dann gilt $V = Kv_1 \oplus V'$. Außerdem gilt $\chi_A(t) = (t - \lambda_1)\chi_{A'}(t)$. Wegen der Eindeutigkeit der Primpolynomzerlegung gitl

$$\chi_{A'}(t) = (t - \lambda_2)...(t - \lambda_n)$$

Sei α' der Endomorphismus auf V', der durch A' bezüglich $(v_2, ..., v_n)$ dargestellt wird. Nach Induktionsvoraussetzung gibt es eine Basis $(v_2', ..., v_n')$ von V', bezüglich derer α' durch eine obere Dreiecksmatrix B' dargestellt wird. Dann wird α bezüglich der Basis $(v_1, v_2', ..., v_n')$ durch

$$\begin{pmatrix} \lambda_1 & * \\ 0 & B' \end{pmatrix}$$

dargestellt. Dies ist eine obere Dreiecksmatrix, also ist α trigonalisierbar. □

Korollar 5.68 *Über $K = \mathbb{C}$ ist jeder Endomorphismus trigonalisierbar.*

Beweis: Hauptsatz der Algebra: Über $\mathbb{C}$ zerfällt jedes Polynom in Linearfaktoren. □
Sei nun K wieder allgemein und λ ein Eigenwert von $\alpha \in End_K(V)$

Def. 5.69 (Algebraische und geometrische Vielfachheit) *(i) Die algebraische Vielfachheit $\mu_{alg}(\lambda)$ ist die Vielfachheit von λ als Nullstelle von $\chi_A(t)$, das heißt die Potenz von $(t - \lambda)$ in der Primfaktorzerlegung von $\chi_A(t)$*

(ii) Die geometrische Vielfachheit $\mu_{geo}(\lambda)$ ist gleich $dim(V_\lambda)$

Satz 5.70 *Es gilt:*

$$1 \leq \mu_{geo}(\lambda) \leq \mu_{alg}(\lambda)$$

Beweis: Sei $r = \mu_{geo}(\lambda)$ und $v_1, ...v_r$ eine Basis von V_λ. Ergänze zu $(v_1, ..., v_r, v_{r+1}, ..., v_n)$; so wird α durch eine Matrix der Form

$$A = \begin{pmatrix} \lambda E_r & * \\ 0 & A' \end{pmatrix}$$

dargestellt. Also gilt $\chi_\alpha(t) = (t - \alpha)^r \chi_{A'}(t)$. Dies impliziert $\mu_{alg} > r$ □

Satz 5.71 *Für einen Endomorphismus α auf dem n-dimensionalen Vektorraum V gilt:*

$$\alpha \, diag \Leftrightarrow \sum_{\lambda \, EW \, von \, \alpha} \mu_{geo}(\lambda) = n$$

Beweis: Ist α bezüglich einer Basis durch $A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ gegeben, so gilt $\chi_\alpha(t) = \det(tE - A) = (t - \lambda_1) \cdot ... \cdot (t - \lambda_n)$. Die andere Richtung beweisen wir durch Induktion nach n. $n = 1$ ist klar. Sei $\chi_\alpha(t) = (t - \lambda_1) \cdot ... \cdot (t - \lambda_n)$ und sei v_1 ein Eigenvektor zum Eigenwert λ_1. Ergänze v_1 zu einer Basis $(v_1, ..., v_n)$ von V. Bezüglich dieser Basis hat α die Gestalt $\begin{pmatrix} \lambda_1 & * \\ 0 & A' \end{pmatrix} = A$ mit $(n-1) \times (n-1) = \mu A'$. Sei $V' = Lin(v_2, ..., v_n)$, dann gilt $V = Kv_1 \oplus V'$. Außerdem $\chi_A(t) = (t - \lambda_n)\chi_{A'}(t)$. Wegen der Eindeutigkeit der Primpolynomzerlegung gilt

$$\chi_{A'}(t) = (t - \lambda_1) \cdot ... \cdot (t - \lambda_n)$$

Sei α' der Endomorphismus auf V', der durch A' bezüglich $(v_2, ..., v_n)$ dargestellt wird. Nach Induktionsvoraussetzung gilt, dass es eine Basis $(v_2', ..., v_n')$ von V' gibt, bezüglich der α' durch eine obere Dreiecksmatrix B' dargestellt wird. Dann wird α bezüglich der Basis $(v_1, v_2', ..., v_n')$ durch $\begin{pmatrix} \lambda_1 & * \\ 0 & B \end{pmatrix}$ dargestellt. Dies ist eine obere Dreiecksmatrix, also ist α trigonalisierbar. □

$$\alpha\, trigonalisierbar \Leftrightarrow \sum_{\lambda\, EW} \mu_{alg}(\lambda) = n$$

Beweis: Es seien $\lambda_1, ..., \lambda_r$ die verschiedenen Eigenwerte von α. Gilt

$$\sum_{i=1}^{r} \mu_{alg}(\lambda_i) = n = \deg(\chi_\alpha)$$

so folgt $\chi_\alpha(t) = (t-\lambda_1)^{\mu_{alg}(\lambda_1)} \cdot ... \cdot (t-\lambda_r)^{\mu_{alg}(\lambda_r)}$, nach 5.67 ist α trigonalisierbar. Ist umgekehrt α trigonalisierbar, so zerfällt nach 5.67 χ_α in Linearfaktoren und es folgt $\sum_\lambda \mu_{alg}(\lambda) = n$.
Ist α diagonalisierbar, so zerfällt V in die direkte Summe der Eigenräume und $n = \dim V = \sum_{\lambda\, EW} \mu_{geo}(\lambda)$. Gelte umgekehrt die Formel. Betrachte den Homomorphismus

$$\phi : \bigoplus_{i=1}^{r} V_{\lambda_i} \to V$$
$$(v_1, ..., v_r) \mapsto \sum_{i=1}^{r} V_i$$

Wir zeigen ϕ ist ein Isomorphismus. Nach Vorraussetzung genügt zu zeigen, dass ϕ injektiv ist. Dies folgt aus 5.64. □

6 Bilinearformen

Wir betrachten 2-Formen auf V

$$\gamma : V \times V \to K$$

das heißt γ ist in jedem Argument linear.

6.1 Bilinearformen

Def. 6.1 (Fundamentalmatrix) *Sei V ein endlichdimensionaler Vektorraum mit Basis $(v_1, ..., v_n)$ und $\gamma : V \times V \to K$ eine Bilinearformen. Die Matrix $G = (g_{ij}) = (\gamma_(v_i, v_j))$ heißt die Fundamentalmatrix von γ bezüglich dieser Basis. Da γ bilinear ist, gilt für Vektoren $v = \sum a_i v_i$, $w = \sum b_i v_i$:*

$$\begin{aligned} \gamma(v, w) &= \gamma\left(\sum a_i v_i, \sum b_i v_i\right) \\ &= (a_1, ..., a_n) G \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ &= a^t G b \in K \end{aligned} \qquad (*)$$

weshalb γ durch G eindeutig bestimmt ist. Umgekehrt ist jedes $G \in M_{n,n}(K)$ mit Hilfe von $*$ eine Bilinearform $\gamma : V \times V \to K$ mit Fundamentalmatrix G.

Die Menge aller Bilinearformen wird zum Vektorraum $Bil(V)$ durch

$$(\alpha\gamma_1 + \beta\gamma_2)(v, w) = \alpha\gamma_1(v, w) + \beta\gamma_2(v, w)$$

Sind G_1, G_2 Fundamentalmatrizen zu γ_1, γ_2, so ist $\alpha G_1 + \beta G_2$ die Fundamentalmatrix zu $\alpha\gamma_1 + \beta\gamma_2$. Wir erhalten

Lemma 6.2 *Sei V ein n-dimensionaler K-Vektorraum und $(v_1, ..., v_n)$ eine Basis, dann gibt es einen Isomorphismus von Vektorräumen*

$$\begin{aligned} fv_1, ..., v_n : Bil(V) &\to M_{n,n}(K) \\ \gamma &\mapsto G \end{aligned}$$

Sei $(w_1, ..., w_n)$ eine weitere Basis und $S = M^{w_1,...,w_n}_{v_1,...,v_n}(id_V)$ die Transformationsmatrix. Dann ist die Fundamentalmatrix von γ bezüglich $(w_1, ..., w_n)$ gegeben durch

$$\begin{aligned} G' = (g'_{ij}) &= (\gamma(w_i, w_j)) \\ &= \left(\gamma \left(\sum_{k=1}^{n} s_{ki} v_k, \sum_{l=1}^{n} s_{lj} v_l \right) \right)_{ij} \\ &= \left(\sum_{k=1}^{n} \sum_{l=1}^{n} s_{ki} g_{kl} s_{lj} \right)_{ij} \\ &= S^t G S \end{aligned}$$

Lemma 6.3 *Ist $S = M^{\underline{w}}_{\underline{v}}(id_V)$, so gilt:*

$$\varphi_{w_1,...,w_n}(\gamma) = S^t \varphi_{v_1,...,v_m}(\gamma) S$$

Bemerkung: Bei $G \to S^t G S$ gilt $\det(S^t G S) = det(S)^2 det(G)$, das heißt die Determinante der Fundamentalmatrix ist *nicht* basisunabhängig. Sei $\gamma : V \times V \to K$ Bilinearform. Die assoziierte Abbildung $\Gamma : V \to V^*$, $\Gamma(v)(w) := \gamma(v, w)$ ist linear (einfache Rechnung). Umgekehrt definiert jede lineare Abbildung $\Gamma : V \to V^*$ eine Bilinearform γ durch $\gamma(v, w) := \Gamma(v)(w)$.

Def. 6.4 (Ausgeartet) *γ heißt nicht ausgeartet, wenn $\Gamma : V \to V^*$ ein Isomorphismus ist. Wegen $\dim V = \dim V^*$ 2.39 ist Γ genau dann ein Isomorphismus, wenn es injektiv ist. Also ist γ genau dann nicht ausgeartet, wenn gilt:*

$$\gamma(v, w) = 0 \, \forall w \in V \Rightarrow v = 0$$

Lemma 6.5 *Sei $({}_v1, ..., v_n)$ eine Basis und $G = \varphi_{v_1,...,v_n}(\gamma) \in M_{n,n}(K)$ die Fundamentalmatrix von γ bezüglich $(v_1, ..., v_n)$. Dann sind äquivalent:*

(i) γ ist nicht ausgeartet

(ii) G ist invertierbar

Beweis: Sei $(v_1^*, ..., v_n^*)$ die zu $(v_1, ..., v_n)$ duale Basis von V^* , das heißt$v_i^*(v_j) = \delta_{ij}$. Behauptung: $\Gamma(v_i) = \gamma(v_i, v_1)v_1^* + ... + \gamma(v_i, v_n)v_n$. Grund: per Definition gilt: $\Gamma(v_i)(v_j) = \gamma(v_i, v_j) = (\gamma(v_i, v_1)v_1^* + ... + \gamma(v_i, v_n)v_n^*)\,(v_j)$. Also stimmen die beiden Linearfaktoren dieser Basis überein und sind somit gleich. $\Rightarrow M^{\underline{v}}_{\underline{v^*}}(\Gamma) = (\gamma(v_j, v_i))_{ij} = G^t$

$$\begin{aligned} \gamma \text{ nicht ausgeartet} &\overset{df}{\iff} \Gamma \text{ ist Isomorphismus} \\ &\iff G^t \text{ist invertierbar} \\ &\iff G \text{ist invertierbar} \end{aligned}$$

□

Korollar 6.6 *Ist γ nicht ausgeartet, so gilt:*

$$\gamma(v, w)) = 0 \, \forall v \Rightarrow w = 0$$

Beweis: Sei G die Fundamentalmatrix von γ bezüglich $(v_1, ..., v_n)$. Wir betrachten die Bilinearform $\gamma : V \times V \to K$, $\gamma'(v, w) := \gamma(w, v)$. Dann hat γ die Fundamentalmatrix G^t . Nach Voraussetzung ist γ nicht ausgeartet. Daher ist G invertierbar, also auch G^t , das heißt γ' ist nicht ausgeartet.

$$\gamma(v, w) = 0 \, \forall v \Rightarrow \gamma'(w, v) = 0 \, \forall v \Rightarrow w = 0$$

□

Def. 6.7 (Symmetrische und antisymmetrische Bilinearformen) *γ heißt*

$$\begin{aligned} \textit{symmetrisch} &\Leftrightarrow \gamma(v_1, v_2) = \gamma(v_2, v_1) \quad \forall v_1, v_2 \in V \\ \textit{antisymmetrisch} &\Leftrightarrow \gamma(v_1, v_2) = -\gamma(v_2, v_1) \quad \forall v_1, v_2 \in V \end{aligned}$$

Bemerkung: Aus Definition 5.17: γ alternierend $\Rightarrow$ γ antisymmetrisch: Im Fall $char(K) = 2$ gilt auch die Umkehrung wegen

$$\gamma(v, v) = -\gamma(v, v) \Rightarrow 2\gamma(v, v) = 0 \xrightarrow{\frac{1}{2} \in K} \gamma(v, v) = 0$$

Im Fall $char(K) = 2$ gilt $-1_K = 1_K$, also hier symmetrisch = antisymmetrisch. Die Form $\gamma : K^3 \times K^3 \to K$, $\gamma(x, y) = x^t y = x_1y_1 + x_2y_2 + x_3y_3$ ist im Fall $char(K) = 2$ antisymmetrisch, aber nicht alternierend.

Lemma 6.8 *Sei $\gamma : V \times V \to K$ eine Bilinearform und $(v_1, ..., v_n)$ eine Basis. Sei $G = \varphi_{v_1,...,v_n}(\gamma)$ die Fundamentalmatrix, so gilt:*

(i) γ symmetrisch $\Leftrightarrow$ G ist symmetrische Matrix (das heißt $G^t = G$)

(ii) γ antisymmetrisch $\Leftrightarrow$ G ist antisymmetrische Matrix (das heißt $G^t = -G$)

6.2 Quadratische Räume

Sei $char(K) \neq 2$

Def. 6.9 (Quadratischer Raum, Orthonormalbasis) *Ein n-dimensionaler K-Vektorraum V zusammen mit einer symmetrischen Bilinearform γ heißt quadratischer Raum der Dimension n über K. Eine Basis $(v_1, ..., v_n)$ von V heißt Orthogonalbasis, wenn $\gamma(v_i, v_j) = 0$ für $i = j$ gilt.*

Bemerkung:

1. $(v_1, ..., v_n)$ ist Orthogonalbasis, wenn die Fundamentalmatrix $G = \gamma(v_i, v_j)$ eine Diagonalmatrix ist.

2. Der Kürze halber schreiben wir von jetzt an $\gamma(v, w) = \langle v, w \rangle$

Theorem 6.10 *Sei (V, γ) ein quadratischer Raum. Dann gibt es eine Orthogonalbasis.*

Beweis: Induktion über $n = \dim V$. Der Fall $n = 1$ ist trivial. Sei $n \geq 2$. Gilt $\langle n, n \rangle = 0$ für alle $v \in V$, so gilt $0 = \langle v + w, v + w \rangle = 2\langle v, w \rangle$ und wegen $char(K) \neq 2$ist γ identisch 0. In diesem Fall ist jede Basis orthogonal. Ansonsten existiert ein $v_1 \in V$ mit $\langle v_1, v_1 \rangle = a_1 \neq 0$. Sei$H = \{w \in V | \langle v_1, w \rangle = 0\}$. Dann gilt $H = (ker\Gamma(v_1) : V \to K)$, also $\dim H \in \{n, n-1\}$ nach Dimensionsformel. Wegen $v_1 \in H$ gilt $\dim H = n - 1$ und $V \stackrel{\sim}{=} Kv_1 \oplus H$. Nun ist $(H, \gamma|_{H \times H})$ ein quadratischer Raum der Dimension $n-1$. Nach Induktionsvoraussetzung existiert Orthogonalbasis $(v_2, ..., v_n)$ von H. Dann ist $(v_1, ..., v_n)$ eine Orthogonalbasis von V wegen $\langle v_i, vj \rangle = 0$ für $i = j$. □

Korollar 6.11 *Sei $char(K) = 2$, $A \in M_{n,n}(K)$ symmetrisch. Dann existiert $S \in GL_n(K)$, sodass S^tAS Diagonalform hat.*

Beweis: Bezüglich der Standardbasis des K^n definiert A eine symmetrische Bilinearform. Bezüglich einer Orthogonalbasis des K^n hat diese Diagonalform. Der Basiswechsel von der Standardbasis zur Orthogonalbasis überführt A in S^tAS für ein $S \in GL_n(K)$) und S^tAS hat Diagonalform.

Def. 6.12 (Homomorphismus quadratischer Räume) *Es seien (H_1, γ_1), (H_2, γ_2) quadratische Räume. Ein Homomorphismus quadratischer Räume $f : (H_1, \gamma_1) \to (H_2, \gamma_2)$ ist ein Vektorraumhomomorphismus $f : H_1 \to H_2$, sodass $\gamma_2(f(v, w)) = \gamma_1(v, w) \forall v, w \in H_1$.*

Def. 6.13 (Orthogonale direkte Summe) *Sind $(V_1, \gamma_1), (V_2, \gamma_2)$ quadratische Räume, so heißt (V, γ) mit $V = V_1 \oplus V2$ und $\gamma((v_1, v_2), (w_1, w_2)) = \gamma_1(v1, w1) + \gamma_2(v2, w2)$ die orthogonale direkte Summe von $(V_1, \gamma_1), (V_2, \gamma_2)$.*
Bezeichnung: $(V, \gamma) = (V_1, \gamma_1)\widehat{\oplus}(V_2, \gamma_2)$ oder einfach $V = V_1\widehat{\oplus}V_2$.

Lemma 6.14 *Seien U_1, U_2 Untervektorräume des quadratischen Raumes (V, γ). Dann ist der induzierte Homomorphismus*

$$f : (U_1, \gamma|_{U_1})\widehat{\oplus}(U_2, \gamma|_{U_2}) \to (V, \gamma), \quad f(u_1, u_2) = u_1 + u_2$$

genau dann ein Homomorphismus quadratischer Räume, wenn $\gamma(u_1, u_2) = 0$ für alle $u_1 \in U_1, u_2 \in U_2$. Ist dies der Fall und ist f überdies ein Isomorphismus ($\Leftrightarrow U_1 \cap U_2 = \{0\}$ und $U_1 + U_2 = V$, vergleiche 2.7) so sagt man, V sei die orthogonale direkte Summe seiner Untervektorräume U_1, U_2 und schreibt $V = U_1\widehat{\oplus}U_2$.

Beweis: Sei h die Bilinearform auf $(U_1, \gamma|_{U_1})\widehat{\oplus}(U_2, \gamma|U_2)$ siehe 6.13. Für $u_1, u_1' \in U_1$, $u_2, u_2' \in U_2$ gilt:

$$h\left((u_1, u_2), (u_1', u_2')\right) = \gamma(u_1, u_1') + \gamma(u_2, u_2')$$

Es ist f genau dann ein Homomorphismus quadratischer Räume, wenn für beliebige $u_1, u_1' \in U_1$, $u_2, u_2' \in U_2$ gilt:

$$\begin{aligned} h\left((u_1, u_2), (u_1', u_2')\right) &= \gamma\left(f(u_1, u_2'), f(u_1, u_2')\right) \\ &= \gamma(u_1 + u_2, u_1' + u_2') \end{aligned}$$

also $\gamma(u_1, u_1') + \gamma(u_2, u_2') = \gamma(u_1, u_1') + \gamma(u_1, u_2') + \gamma(u_2, u_1') + \gamma(u_2, u_2')$ gilt, das heißt $0 = \gamma(u_1, u_2') + \gamma(u_2, u_1')$. Dies ist äquivalent zu $\gamma(u_1, u_2) = 0 \forall u_1 \in U_1$, $u_2 \in U_2$. □

Satz 6.15 *Sei (V, γ) ein quadratischer Raum über $\mathbb{C}$. Dann existiert eine Orthogonalbasis $(v_1, ..., v_n)$ von V, sodass $\lambda_i = \gamma(v_i, v_i) \in \{0, 1\}$.*
Die Zahlen $r_0 =$ Anzahl der $\lambda_i = 0$ und $r =$ Anzahl der $\lambda_i = 1$ sind unabhängig von der Wahl der Orthogonalbasis.

Beweis: Sei $(\widetilde{v}_1, ..., \widetilde{v}_n)$ eine Orthogonalbasis. Setze

$$v_i \begin{cases} \widetilde{v}_i & falls\, \widetilde{\lambda}_i = \gamma(\widetilde{v}_i, \widetilde{v}_i) = 0 \\ \frac{1}{\sqrt{\lambda_i}} \cdot \widetilde{v}_i & falls\, \widetilde{\lambda}_i = \gamma(\widetilde{v}_i, \widetilde{v}_i) \neq 0 \end{cases}$$

Dann ist $(v_1, ..., v_n)$ eine Orthogonalbasis mit $\lambda_1 = \langle v_i, v_i \rangle \in \{0, 1\}$. Für die Fundamentalmatrix $G = diag(\lambda_1, ..., \lambda_n)$ gilt nun $r = Rg(G)$, $r_0 = n - r$. Bezüglich einer anderen Orthogonalbasis hat γ die Fundamentalmatrix T^tGT für ein $T \in GL_n(\mathbb{C})$ und es gilt $Rg(T^tGT) = Rg(G)$. Daher sind r_0, r unabhängig von der Auswahl der Orthogonalbasis.

Korollar 6.16 *Sei G eine symmetrische komplexe $n \times n$-Matrix. Dann existiert $T \in GL_n(\mathbb{C})$ mit*

$$T^tGT = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

Die Zahl $r = Rg(G)$ ist unabhängig von der Wahl von T.

Satz 6.17 *Sei (V, γ) ein quadratischer Raum über R. Dann existiert eine Orthogonalbasis $(v_1, ..., v_n)$, sodass $\lambda_i = \gamma(vi, vi) \in \{0, \pm 1\}$.*
Die Zahlen $r_0 =$ Anzahl der $\lambda_i = 0$, $r_+ =$ Anzahl der $\lambda_i = +1$ und $r_- =$ Anzahl der $\lambda_i = -1$ sind unabhängig von der Wahl der Basis.

Beweis: Sei eine Orthogonalbasis. Setze

$$v_i \begin{cases} \widetilde{v}_i & falls\, \widetilde{\lambda}_i = \gamma(\widetilde{v}_i, \widetilde{v}_i) = 0 \\ \frac{1}{\sqrt{\lambda_i}} \cdot \widetilde{v}_i & falls\, \widetilde{\lambda}_i = \gamma(\widetilde{v}_i, \widetilde{v}_i) \neq 0 \end{cases}$$

Wir erhalten die gewünschte Orthogonalbasis mit Fundamentalmatrix $A = diag(\lambda_1, ..., \lambda_n)$ und $\lambda_i \in \{0, \pm 1\}$. Wie im Komplexen erhalten wir, dass $r_+ + r_- = Rg(A)$ und $r_0 = n - Rg(A)$ unabhängig von der Wahl der Orthogonalbasis sind. Daher genügt es zu zeigen, dass r_+ unabhängig von der Wahl ist. Sei V_+ der Untervektorraum in V, erzeugt von den v_i mit $\lambda_i = +1$. Analog V_-, V_0. Dann gilt $V = V_+ \widehat{\oplus} V_- \widehat{\oplus} V_0$. Setze

$$a = \max(\dim(W) | W \subset V, \gamma(w, w) > 0 \, \forall 0 = w \in W)$$

Zunächst hat V_+ diese Eigenschaft, also $a \geq r_+$. Wäre $a > r_+$, so existiert $W \subset V$ wie oben und $\dim(W) > r_+$. Es folgt $\dim(W) + \dim(V_-) + \dim(V_0) > n$. Die Dimensionsformel liefert $W \cap (V_- \oplus V_0) \neq \{0\} \Rightarrow$ es existiert $0 = w \in W$ mit $\gamma(w, w) > 0$ und $\gamma(w, w) \leq 0$. ↯
$\Rightarrow a = r_+$, also r_+ unabhängig von der Wahl der Orthogonalbasis. □

Korollar 6.18 (Sylvesterscher Trägheitssatz) *Sei $G \in M_{n,n}(\mathbb{R})$ symmetrisch. Dann existiert $T \in GL_n(\mathbb{R})$, sodass*

$$T^t G T = \begin{pmatrix} E_{r_+} & 0 & 0 \\ 0 & -E_{r_-} & 0 \\ 0 & 0 & O_{r_+} \end{pmatrix}$$

r_+, r_-, r_0 sind unabhängig von der Wahl von T.

6.3 Euklidische Vektorräume

Def. 6.19 (Definitheit, Semidefinitheit) *Eine symmetrische Bilinearform $\gamma : V \times V \to \mathbb{R}$ auf einem endlich dimensionalen $\mathbb{R}$-Vektorraum heißt positiv definit (beziehungsweise positiv semidefinit), wenn $\gamma(v, v) > 0$ (beziehungsweise $\gamma(v, v) \geq 0$) für alle $v \in V \setminus \{0\}$ gilt. Analog definiert man negativ definit und negativ semidefinit.*

Beispiel: $\mathbb{R}^n$ mit Standardskalarprodukt $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$ ist positiv definit wegen $\langle x, x \rangle = x_1^2 + ... + x_n^2$

Def. 6.20 (Euklidischer Raum, Norm, Isometrie, Orthogonalbasis) *Ein euklidischer Raum ist ein endlich dimensionaler $\mathbb{R}$-Vektorraum V mit einer positiv definiten symmetrischen Bilinearform. Für ein $v \in V$ nennt man*

$$\| v \| = \sqrt{\langle v, v \rangle}$$

die Norm von v. Zwei euklidische Vektorräume V, W heißen isometrisch, wenn es einen Vektorraumisomorphismus $\varphi : V \xrightarrow{\sim} V$ gibt mit

$$\langle \varphi(v_1), \varphi(v_w) \rangle_W = \langle v_1, v_2 \rangle_V$$

für alle $v_1, v_2 \in V$. Eine Basis $(e_1, ..., e_n)$ eines euklidischen Vektorraumes heißt Orthonormalbasis, wenn

$$\langle e_i, e_j \rangle = \delta_{ij}$$

Theorem 6.21 *Jeder euklidische Vektorraum besitzt eine Orthonormalbasis.*

Beweis: Sei $(v_1, ..., v_n)$ eine Orthogonalbasis und G die Fundamentalmatrix von γ bezüglich $(v_1, ..., v_n)$. Auf der Diagonalen stehen Werte $\langle v_i, v_i \rangle > 0$. Setze $e_i = \frac{1}{\sqrt{\langle v_i, v_i \rangle}} \cdot v_i$. □

Korollar 6.22 *Eine positiv definite symmetrische Bilinearform ist nicht ausgeartet. Es existiert eine Basis bezüglich derer sie durch die Einheitsmatrix dargestellt wird.*

Korollar 6.23 *Ein euklidischer Vektorraum (V,γ) mit $\dim_{\mathbb{R}} V = n$ ist isometrische zum $\mathbb{R}^n$ mit dem Standardskalarprodukt.*

Beweis: Sei $(v_1,...,v_n)$ eine Orthonormalbasis des Vektorraumes V . Dann ist die Abbildung $\varphi : (\mathbb{R}^n, \langle\cdot,\cdot\rangle_{Std}) \to (V,\gamma)$, $e_i \mapsto v_i$ eine Isometrie.

Korollar 6.24 *Sei (V,γ) ein euklidischer Vektorraum. Dann gelten:*

(i) Dreiecksungleichung $\| x+y \| \leq \| x \| + \| y \|$

(ii) Schwarzsche Ungleichung $|\langle x,y\rangle| \leq \| x \| \cdot \| y \|$

Beweis: (i) und (ii) gelten im R^n (siehe Kapitel 0). □

Korollar 6.25 (Satz des Pythagoras) *Sind x und y orthogonal, das heißt $\langle x,y\rangle = 0$, so gilt*

$$\| x+y \|^2 = \| x \|^2 + \| y \|^2$$

Def. 6.26 (Orthogonales Komplement) *Sei V ein euklidischer Vektorraum und $U \subset V$ ein Untervektorraum. Dann heißt*

$$U^{\perp} = \{v \in V | \langle v,u\rangle = 0 \, \forall u \in U\}$$

das orthogonale Komplement zu U.

Satz 6.27 *Es gilt:*

$$V = U \widehat{\oplus} U^{\perp}$$

Beweis: Für $u \in U \cap U^{\perp}$ gilt $\langle u,u\rangle = 0$, also $u = 0 \Rightarrow U \cap U^{\perp} = \{0\}$. Zu zeigen: $U + U^{\perp} = V$.
Sei $(u_1,...,u_m)$ eine Orthonormalbasis von U . Für $v \in V$ sei $v' = v - \sum_{i=1}^{m} \langle v,u_i\rangle u_i$. Dann gilt:

$$\langle v', u_i\rangle = \langle v,u_i\rangle - \langle v,u_i\rangle = 0 \quad \text{für } i = 1,...,m$$

also $v \in U^{\perp}$. Daher gilt $V = U \oplus U^{\perp}$. Schließlich gilt $\langle u,v\rangle = 0$ für alle $u \in U$, $v \in U^{\perp}$, weshalb die Summe orthogonal ist (siehe 6.14).

Def. 6.28 (Orthogonalprojektion) *Die Projektion*

$$V \xrightarrow{\sim} U \widehat{\oplus} U^{\perp} \xrightarrow{P_1} U$$

heißt die Orthogonalprojektion von V auf U.