Lineare Algebra I (Vogel)

Robin Heinemann

26. Oktober 2017

Inhaltsverzeichnis

1 Einleitung

Übungsblätter/Lösungen: jew. Donnerstag / folgender Donnerstag Abgabe Donnerstag 9:30 50% der Übungsblätter

1.1 Plenarübung

Aufgeteilt

1.2 Moodle

Passwort: vektorraumhomomorphismus

1.3 Klausur

24.02.2017

2 Grundlagen

2.1 Naive Aussagenlogik

naive Logik: wir verwenden die sprachliche Vorstellung ($\neq$ mathematische Logik: eigne Vorlesung) Eine Aussage ist ein feststehender Satz, dem genau einer der Wahrheitswerte „wahr" oder „falsch" zugeordnet werden kann. Aus einfachen Aussagen kann man durch logische Verknüpfungen kompliziertere Aussagen bilden. Angabe der Wahrheitswerts der zusammengesetzten Aussage erfolgt durch Wahrheitstafeln (liefern den Wahrheitswert der zusammengesetzten Aussage, aus dem Wahrheitswert der einzelnen Aussagen). Im folgenden seien A und B Aussagen.

- Negation (NICHT-Verknüpfung)
  - Symbol: $\neg$
  - Wahrheitstafel:

A	$\neg A$
w	f
f	w

  - Beispiel: A: 7 ist eine Primzahl (w) $\neg A$: 7 ist keine Primzahl (f)
- Konjunktion (UND-Verknüpfung)
  - Symbol $\wedge$
  - Wahrheitstafel:

A	B	$A \wedge B$
w	w	w
w	f	f
f	w	f
f	f	f

- Disjunktion (ODER-Verknüpfung)
  - Symbol: $\vee$

- Wahrheitstafel:

A	B	$A \vee B$
w	w	w
w	f	w
f	w	w
f	f	f

- exklusives oder: $(A \vee B) \wedge (\neg(A \wedge B))$

- Beispiel A: 7 ist eine Primzahl (w), B: 5 ist gerade (f)
  - $A \wedge B$ 7 ist eine Primzahl und 5 ist gerade (f)
  - $A \vee B$ 7 ist eine Primzahl oder 5 ist gerade (w)
- Implikation (WENN-DANN-Verknüpfung)
  - Symbol: $\implies$
  - Wahrheitstafel:

A	B	$A \implies B$
w	w	w
w	f	f
f	w	w
f	f	w

  - Sprechweise: A impliziert B, aus A folgt B, A ist eine hinreichende Bedingung für B (ist $A \implies B$ wahr, dann folgt aus A wahr, B ist wahr), B ist eine notwendige Bedingung für A (ist $A \implies B$ wahr, dann kann A nur dann wahr sein, wenn Aussage B wahr ist)
  - Beispiel Es seinen $m, n \in \mathbb{N}$
    - A: m ist gerade
    - B: mn ist gerade
    - Dann gilt $\forall\, m, n \in \mathbb{N}\ A \implies B$ wahr
      Fallunterscheidung:
      - m gerade, n gerade, dann ist A wahr, B wahr, d.h. $A \implies B$ wahr
      - m gerade, n ungerade, dann ist A wahr, B wahr, d.h. $A \implies B$ wahr
      - m ungerade, n gerade, dann ist A falsch, B wahr, d.h. $A \implies B$ wahr
      - m ungerade, n ungerade, dann ist A falsch, B falsch, d.h. $A \implies B$ wahr
- Äquivalenz (GENAU-DANN-WENN-Verknüpfung)
  - Symbol $\iff$
  - Wahrheitstafel:

A	B	$A \iff$ B
w	w	w
w	f	f
f	w	f
f	f	w

  - Sprechweise: A gilt genau dann, wenn B gilt, A ist hinreichend und notwendig für B
    Die Aussagen $A \iff B$ und $(A \implies B) \wedge (B \implies A)$ sind gleichbedeutend:

A	B	$A \iff B$	$A \implies B$	$B \implies A$	$(A \implies B) \wedge (B \implies A)$
w	w	w	w	w	w
w	f	f	f	w	f
f	w	f	w	f	f
f	w	f	w	f	f
f	f	w	w	w	w

– Beispiel: Es sei n eine ganze Zahl
$A:\ n-2>1$
$B:\ n>3$
$\forall n \in \mathbb{N}$ gilt $A \iff B\, C:\ n>0$
$D:\ n^2>0$
Für $n=-1$ ist die Äquivalenz $C \iff$ falsch (C falsch, D wahr)
Für alle ganzen Zahlen n gilt zumindest die Implikation $C \implies D$

2.2 Beweis

Mathematische Sätze, Bemerkungen, Folgerungen, etc. sind meistens in Form wahrer Implikationen formuliert

2.2.1 beweisen

Begründen warum diese Implikation wahr ist
Beweismethoden für diese Implikation $A \implies B$

- direkter Beweis ($A \implies B$)
- Beweis durch Kontraposition ($\neq B \implies \neg A$)
- Widerspruchsbeweis ($\neg(A \wedge \neg B)$)

Diese sind äquivalent zueinander

A	B	$\neg A$	$\neg B$	$A \implies B$	$\neg B \implies \neg A$	$\neg(A \wedge \neg B)$
w	w	f	f	w	w	w
w	f	f	w	f	f	f
f	w	w	f	w	w	w
f	f	w	w	w	w	w

Beispiel m, n natürliche Zahlen

$$A:\ m^2 < n^2$$

$$B:\ m < n$$

Wir wollen zeigen, dass $A \implies B$ für alle natürlichen Zahlen m, n wahr ist

- direkter Beweis:

$$A:\ m^2 < n^2 \implies 0 < n^2 - m^2 \implies 0 < (n-m)\underbrace{(n+m)}_{>0} \implies 0 < n-m \implies m < n$$

- Beweis durch Kontraposition:

$$\neg B:\ m \geq n \implies m^2 \geq nm \wedge mn \geq n^2 \implies m^2 \geq n^2 \implies \neg A$$

- Beweis durch Widerspruch:

  $$A \wedge \neg B \implies m^2 < n^2 \wedge n \le m \implies m^2 < n^2 \wedge mn \le m^2 \wedge n^2 \le mn \implies mn \le m^2 < n^2 \le mn$$

  Widerspruch

2.3 Existenz- und Allquantor

2.3.1 Existenzquantor

$A(x)$ Aussage, die von Variable x abhängt
$\exists x :\ A(x)$ ist gleichbedeutend mit „Es existiert ein x, für das $A(x)$ wahr ist“ (hierbei ist „existiert ein x“ im Sinne von „existiert mindestens ein x“ zu verstehen)
Beispiel:

$$\exists n \in \mathbb{N} :\ n > 5 \quad \text{(w)}$$

$\exists! x :\ A(x)$ ist gleichbedeutend mit „Es existiert genau ein x, für dass $A(x)$ wahr ist“

2.3.2 Allquantor

$\forall\, x :\ A(x)$ ist gleichbedeutend mit „Für alle x ist A(x) wahr“ Beispiel:

$$\forall\, n \in \mathbb{N} : 4n \text{ ist gerade}$$

2.3.3 Negation von Existenz- und Allquantor

$$\neg(\exists x :\ A(x)) \iff \forall\, x :\ \neg A(x)$$

$$\neg(\forall\, x :\ A(x)) \iff \exists x :\ \neg A(x)$$

2.3.4 Spezielle Beweistechniken für Existenz und Allaussagen

- Angabe eines Beispiel, um zu zeigen, dass deine Existenzaussage wahr ist.
  Beispiel:
  $$\exists n \in \mathbb{N} :\ n > 5 \text{ist wahr, denn für } n = 7 \text{ ist die Aussage } n > 5 \text{ wahr}$$
- Angabe eines Gegenbeispiel, um zu zeigen, dass eine Allaussage falsch ist.
  Beispiel:
  $$\forall\, n \in \mathbb{N} :\ n \le 5 \text{ist falsch, dann für } n = 7 \text{ ist die Aussage } n \le 5 \text{ falsch}$$

2.4 Naive Mengenlehre

Mengenbegriff nach Cantor:
Eine Menge ist eine Zusammenfassung von bestimmten, wohl unterschiedenen Objekten unserer Anschauung oder unseres Denkens (die Elemente genannt werden) zu einem Ganzen

2.4.1 Schreibweise

- $x \in M$, falls x ein Element von M ist
- $x \notin M$, falls x kein Element von M ist
- $M = N$, falls M und N die gleichen Elemente besitzen, $M \subseteq N \wedge N \subseteq M$

2.4.2 Angabe von Mengen

- Reihenfolge ist irrelevant ($\{1,2,3\} = \{1,3,2\}$)
- Elemente sind wohlunterschieden $\{1,2,2\} = \{1,2\}$
- Auflisten der Elemente $M = \{a, b, c, \ldots\}$
- Beschreibung der Elemente durch Eigenschaften: $M = \{x \mid E(x)\}$
  (Elemente x, für die E(x) wahr)
  - Beispiel:
  $$\{2,4,6,8\} = \{x \mid x \in \mathbb{N}, x \text{ gerade}, 1 < x < 10\}$$

2.4.3 leere Menge

Die leere Menge $\emptyset$ enthält keine Elemente

Beispiel

$$\{x \mid x \in \mathbb{N}, x < -5\} = \emptyset$$

2.4.4 Zahlenbereiche

Menge der natürlichen Zahlen:
$$\mathbb{N} := \{1,2,3,\ldots\}$$
Menge der natürlichen Zahlen mit Null:
$$\mathbb{N}_0 := \{0,1,2,3,\ldots\}$$
Menge der Ganzen Zahlen:
$$\mathbb{Z} := \{0,1,-1,2,-2\}$$
Menge der rationalen Zahlen:
$$\mathbb{Q} := \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$$
Menge der reellen Zahlen: $\mathbb{R}$

2.4.5 Teilmenge

A, B seien Mengen.
A heißt Teilmenge von B $(A \subseteq B) \overset{\text{Def.}}{\iff} \forall x \in A : x \in B$ A heißt echte Teilmenge von B $(A \subset B) \overset{\text{Def.}}{\iff} A \subseteq B \wedge A \neq B$

Anmerkung Offenbar gilt für Mengen A, B:

$$A = B \iff A \subseteq B \wedge B \subseteq A$$

$\emptyset$ ist Teilmenge jeder Menge

Beispiel

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q}$$

2.4.6 Durchschnitt

$$A \cap B := \{x \mid x \in A \wedge x \in B\}$$

Beispiel

$$A = \{2, 3, 5, 7\}, B = \{3, 4, 6, 7\}, A \cap B = \{3, 7\}$$

2.4.7 Vereinigung

$$A \cup B := \{x \mid x \in A \vee x \in B\}$$

Beispiel

$$A = \{2, 3, 5, 7\}, B = \{3, 4, 6, 7\}, A \cup B = \{2, 3, 4, 5, 6, 7\}$$

2.4.8 Differenz

$$A \setminus B := \{x \mid x \in A \wedge x \notin B\}$$

Im Fall $B \subseteq A$ nennt man $A \setminus B$ auch das Komplement von B in A und schreibt $\complement_A(B) = A \setminus B$

Beispiel

$$A = \{2, 3, 5, 7\}, B = \{3, 4, 6, 7\}, A \setminus B = \{2, 5\}$$

2.4.9 Bemerkung zu Vereinigung und Durchschnitt

A, B seien zwei Mengen. Dann gilt

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

Beweis

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

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

„$\subseteq$“ Sei $x \in A \cap (B \cup C)$. Dann ist $x \in A \wedge x \in B \cup C$

- 1. Fall: $x \in A \wedge x \in B$

$$\implies x \in A \cap B \implies x \in (A \cap B) \cup (A \cap C)$$

- 2. Fall $x \in A \wedge x \in C$

$$\implies x \in A \cap C \implies x \in (A \cap B) \cup (A \cap C)$$

Damit ist „$\subseteq$“ gezeigt. „$\supseteq$“ Sei $x \in (A \cap B) \cup (A \cap C)$

$$\implies x \in A \cap B \vee x \in A \cap C \implies (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \implies x \in A \wedge (x \in B \vee x \in C) \implies x \in A \wedge x \in$$

Damit ist „$\supseteq$“ gezeigt.

2.4.10 Bemerkung zu Äquivalenz von Mengen

Seien A, B Mengen, dann sind äquivalent:

1. $A \cup B = B$
2. $A \subseteq B$

Beweis Wir zeigen 1) $\implies$ 2) und 2) $\implies$ 1.

$1 \implies 2:$ Es gelte $A \cup B = B,$ zu zeigen ist $A \subseteq B$Sei $x \in A \implies x \in A \wedge x \in B \implies x \in A \cup B = B$

$$2 \implies 1: \text{ Es gelte } A \subseteq B, \text{ zu zeigen ist } A \cup B = B$$

„$\subseteq$“: Sei $x \in A \cup B \implies x \in A \vee x \in B \overset{A \subseteq B}{\implies} x \in B$ „$\supseteq$“: $B \subseteq A \cup B$ klar

2.4.11 Kartesisches Produkt

Seien A, B Mengen

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

heißt das kartesische Produkt von A und B. Hierbei ist $(a, b) = (a', b') \overset{\text{Def}}{\iff} a = a' \wedge b = b'$

Beispiel

- $$\{1, 2\} \times \{1, 3, 4\} = \{(1, 1), (1, 3), (1, 4), (2, 1), (2, 3), (2, 4)\}$$
- $$\mathbb{R} \times \mathbb{R} = \{(x, y)| \mid x, y \in \mathbb{R}\} = \mathbb{R}^2$$

2.4.12 Potenzmenge

A sei eine Menge

$$\mathcal{P}(A) := \{M \mid M \subseteq A\}$$

heißt die Potenzmenge von A

Beispiel

$$\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\{1, 2, 3, 4\}\}$$

2.4.13 Kardinalität

M sei eine Menge. Wir setzen

$$|M| := \begin{cases} n & \text{falls } M \text{ eine endliche Menge ist und } n \text{ Elemente enthält} \\ \infty & \text{falls } M \text{ nicht endlich ist} \end{cases}$$

$|M|$ heißt Kardinalität von A

Beispiel

- $|\{7, 11, 16\}| = 3$
- $|\mathbb{N}| = \infty$

2.4.14 Bemerkung zu natürlichen Zahlen

Für die natürlichen Zahlen gilt das Induktionsaxiom Ist $M \subseteq N$ eine Teilmenge, für die gilt:

$$1 \in M \wedge \forall n \in M : n \in M \implies n + 1 \in M$$

dann ist $M = \mathbb{N}$

2.4.15 Prinzip der vollständigen Induktion

Für jedes $n \in \mathbb{N}$ sei eine Aussage $A(n)$ gegeben. Die Aussagen $A(N)$ gelten für alle $n \in \mathbb{N}$, wenn man folgendes zeigen kann:

- (IA) $A(1)$ ist wahr
- (IS) Für jedes $n \in \mathbb{N}$ gilt: $A(n) \implies A(n+1)$

Der Schritt (IA) heißt Induktionsanfang, die Implikation $A(n) \implies A(n+1)$ heißt Induktionsschritt

Beweis Setze $M := \{n \in \mathbb{N} \mid A(n) \text{ ist wahr}\}$ Wegen (IA) ist $1 \in M$, wegen (IS) gilt: $n \in M \implies n + 1 \in M$
Nach Induktionsaxiom folgt $M = \mathbb{N}$, das heißt $A(n)$ ist wahr für alle $n \in \mathbb{N}$

Beispiel Für $n \in \mathbb{N}$ sei $A(n)$ die Aussage: $1 + \ldots + n = \frac{n(n+1)}{2}$ Wir zeigen: $A(n)$ ist wahr für alle $n \in \mathbb{N}$, und zwar durch vollständige Induktion

- (IA) $A(1)$ ist wahr, denn $1 = \frac{1(1+1)}{2}$
- (IS) zu zeigen: $A(n) \implies A(n+1)$
  Es gelte $A(n)$, das heißt $1 + \ldots + n = \frac{n(n+1)}{2}$ ist wahr

$$\implies 1 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \square$$

2.5 Relationen

2.5.1 Definiten

Eine Relation auf M ist eine Teilmenge $R \subseteq M \times M$ Wir schreiben $a \sim b \overset{\text{Def}}{\iff} (a, b) \in R$ („a steht in Relation zu b“)

- anschaulich: eine Relation auf M stellt eine „Beziehung“ zwischen den Elementen von M her.
- Für $a, b \in M$ gilt entweder $a \sim b$ oder $a \not\sim b$, denn: entweder ist $(a, b) \in R$ oder $(a, b) \notin R$

Anmerkung Aufgrund der obigen Notation spricht man in der Regel von Relation „$\sim$“ auf M als von der Relation $R \subseteq M \times M$

Beispiel $M = \{1, 2, 3\}$. Durch $R = \{(1, 1), (1, 2), (3, 3) \subseteq M \times M\}$ ist eine Relation auf M gegeben. Es gilt dann: $1 \sim 1, 1 \sim 2, 3 \sim 3$ (aber zum Beispiel: $1 \not\sim 3, 2 \not\sim 1, 2 \not\sim 2$)

2.5.2 Eigenschaften von Relationen

M Menge, $\sim$ Relation auf M
$\sim$ heißt:

- reflexiv $\overset{\text{Def}}{\iff}$ für alle $a \in M$ gilt $a \sim a$
- symmetrisch $\overset{\text{Def}}{\iff}$ für alle $a, b \in M$ gilt: $a \sim b \implies b \sim a$
- antisymmetrisch $\overset{\text{Def}}{\iff}$ für alle $a, b \in M$ gilt: $a \sim b \wedge b \sim a \implies a = b$
- transitiv $\overset{\text{Def}}{\iff}$ für alle $a, b, c \in M$ gilt: $a \sim b \wedge b \sim v \implies a \sim c$
- total $\overset{\text{Def}}{\iff}$ für alle $a, b \in M$ gilt: $a \sim b \vee b \sim a$

Beispiel Sei M die Menge der Studierenden in der LA1-Vorlesung

1. Für $a, b \in M$ sei $a \sim b \overset{\text{Def}}{\iff} a$ hat den selben Vornamen wie b
   $\sim$ reflexiv, symmetrisch, nicht antisymmetrisch, transitiv, nicht total
2. Für $a, b \in M$ sei $a \sim b \overset{\text{Def}}{\iff}$ Matrikelnummern von a ist kleiner gleich als die Matrikelnummern von b
   $\sim$ ist reflexiv, nicht symmetrisch, antisymmetrisch, transitiv, total
3. Für $a, b \in M$ sei $a \sim b \overset{\text{Def}}{\iff} a$ sitzt auf dem Platz recht von b
   $\sim$ ist nicht reflexiv, nicht symmetrisch, nicht antisymmetrisch, nicht transitiv, nicht total

2.5.3 Halbordnung / Totalordnung

$\sim$ heißt

- Halbordnung auf $M \overset{\text{Def}}{\iff} \sim$ ist reflexiv, antisymmetrisch und transitiv
- Totalordnung auf $M \overset{\text{Def}}{\iff} \sim$ ist eine Halbordnung und $\sim$ ist total

In diesen Fällen sagt man auch: Das Tupel $(M, \sim)$ ist eine halbgeordnete, beziehungsweise totalgeordnete Menge.

Beispiel

1. $\leq$ auf $\mathbb{N}$ ist eine Totalordnung
2. Sei $M = \mathcal{P}(\{1, 2, 3\})$. $\subseteq$ ist auf M eine Halbordnung, aber keine Totalordnung (es ist zum Beispiel weder $\{1\} \subseteq \{3\}$ noch $\{3\} \subseteq \{\}$)

Anmerkung Wegen der Analogie zur $\leq$ auf $\mathbb{N}$ bezeichnen wir Halbordnungen in der Regel mit $\leq$

2.5.4 Größtes / kleinstes Element

$(M, \leq)$ halbgeordnete Menge, $a \in M$
a heißt ein

- größtes Element von $M \overset{\text{Def}}{\iff}$ Für alle $x \in M$ gilt $x \leq a$
- kleinstes Element von $M \overset{\text{Def}}{\iff}$ Für alle $x \in M$ gilt $a \leq x$

Bemerkung $(M, \leq)$ halbgeordnete Menge
Dann gilt: Existiert in M ein größtes (beziehungsweise kleinstes) Element, so ist dieses eindeutig bestimmt

Beweis Es seien $a, b \in M$ größte Elemente von M
$\implies x \leq a$ für alle $x \in M$, also auch $b \leq a$
Außerdem: $x \leq b$ für alle $x \in M$, also auch $a \leq b$
$\xRightarrow{\text{Antisymmetrie}} a = b$
Analog für kleinstes Element

Anmerkung Dies sagt nichts darüber aus, ob ein größtes (beziehungsweise kleinstes) Element in M überhaupt existiert.

Beispiel

1. In $(\mathbb{N}, \leq)$ ist 1 das kleinste Element, ein größtes Element gibt es nicht
2. $(\{\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}\}, \subseteq)$ ist eine halbgeordnete Menge ohne kleinstes beziehungsweise größtes Element

2.5.5 maximales / minimales Element

$(M, \leq)$ halbgeordnete Menge, $a \in M$
a heißt ein

- maximales Element von $M \overset{\text{Def}}{\iff}$ für alle $x \in M$ gilt: $a \leq x \implies a = x$
- minimales Element von $M \overset{\text{Def}}{\iff}$ für alle $x \in M$ gilt: $x \leq a \implies a = x$

Beispiel In $(\{\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}\}, \subseteq)$ sind $\{1,2\}, \{1,3\}, \{2,3\}$ maximale Elemente und $\{1\}, \{2\}, \{3\}$ sind minimale Elemente.

Bemerkung $(M, \leq)$ halbgeordnete Menge, $a \in M$
Dann gilt: Ist a ein größtes (beziehungsweise kleinstes) Element von M, dann ist a ein maximales (beziehungsweise minimales) Element von M.

Beweis Sei a ein größtes Element von M.
zu zeigen ist: Für alle $x \in M$ gilt $a \leq x \implies a = x$ Sei $x \in M$ mit $a \leq x$. Da a größtes Element von M ist, gilt auch $x \leq a$
$\xLeftrightarrow{\text{Antisymmetrie}} a = x$
Analog für kleinstes Element.

2.5.6 Äquivalenzrelation

M Menge, $\sim$ auf M
$\sim$ heißt Äquivalenzrelation $\overset{\text{Def}}{\iff} \sim$ ist reflexiv, symmetrisch und transitiv. In dem Fall sagen wir für $a \sim b$ auch a ist äquivalent zu b. Für $a \in M$ heißt $[a] := \{b \in M \mid b \sim a\}$ heißt die Äquivalenzklasse von a. Elemente aus $[a]$ nennt man Vertreter oder Repräsentanten von a

Beispiel M Menge aller Bürgerinnen und Bürger Deutschlands.
Wir definieren für $a, b \in M$ $a \sim b \overset{\text{Def}}{\iff} a$ und b sind im selben Jahr geboren.
$\sim$ ist ein Äquivalenzrelation.
Jerôme Boateng wurde 1988 geboren.
[Jerôme Boateng] $= \{b \in M \mid b$ ist im selben Jahr geboren wie Jerôme Boateng$\} = \{b \in M \mid b$ wurde 1988 geboren$\}$
Weitere Vertreter von [Jerôme Boateng] sind zum Beispiel Mesut Özil, Mats Hummels. Es ist [Jerôme Boateng] $=$ [Mesut Özil] $=$ [Mats Hummels]. Man sieht in diesem Beispiel: Die Menge M zerfällt komplett in verschiedene Äquivalenzklassen:

- Jeder Bürger / jede Bürgerin Deutschlands ist in genau einer Äquivalenzklasse enthalten
- Jede zwei Äquivalenzklasse sind entweder gleich oder disjunkt (haben leeren Durchschnitt)

Bemerkung M Menge, $\sim$ Äquivalenzrelation auf M
Dann gilt:

1. Jedes Element von M liegt in genau einer Äquivalenzklasse
2. Je zwei Äquivalenzklassen sind entweder gleich oder disjunkt

Man sagt auch: Die Äquivalenzklassen bezüglich „$\sim$“ bilden eine **Partition** von M.

Beweis

1. Sei $a \in M$
   zu zeigen: Es gibt genau eine Äquivalenzklassen, in der a liegt
   a) Es gibt eine Äquivalenzklasse, in der a liegt, denn $a \in [a]$, denn $a \sim a$
   b) Ist $a \in [b]$ und $a \in [c]$, dann ist $[b] = [c]$ (d.h. a liegt in höchstens einer Äquivalenzklasse)
   denn: Seien $b, c \in M$ mit $a \in [b]$ und $a \in [c] \implies a \sim b$ und $a \sim c \xRightarrow{\text{Symmetrie}} b \sim a$ und $a \sim c \xRightarrow{\text{Transitivität}} b \sim c$ Behauptung $[b] = [c]$ denn: „$\subseteq$“ Sei $x \in [b] \implies x \sim b \xRightarrow{Transitivitt}{}^{b\sim c}$ $x \sim c \implies x \in [c]$ denn: „$\supseteq$“ Sei $x \in [c] \implies x \sim c \xRightarrow{Transitivitt}{}^{c\sim b}$ $x \sim b \implies x \in [b]$
2. Sind $b, c \in M$ mit $[b] \cap [c] \neq \emptyset$, dann existiert ein $a \in [b] \cap [c]$, und es folgt wie in 2.:
   $[b] = [c]$ Für $b, c \in M$ gilt also entweder $[b] \cap [c] = \emptyset$ oder $[b] = [c]$ $\square$

Faktormenge M Menge, $\sim$ Äquivalenzrelation auf M $M/\sim := \{[a] | a \in M\}$ (Menge der Äquivalenzklassen) heißt die Faktormenge (Quotientenmenge) von M nach $\sim$

Beispiel

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

Für $a, b, c \in M$ setzen wir $a \sim b \overset{\text{Def.}}{\iff} |x| = |b|$ Das ist eine Äquivalenzrelation auf M Es ist $[1] = \{1, -1\}, [2] = \{2, -2\}, [3] = \{3, -3\}$ Somit: $M/\sim := \{[1], [2], [3]\} = \{\{1, -1\}, \{2, -2\}, \{3, -3\}\}$

Anmerkung Der Übergang zur Äquivalenzklassen soll (für eine jeweils gegebene Relation) irrelevante Informationen abstreifen.

2.6 Abbildungen

naive Definition:
Eine Abbildung f von M nach N ist eine Vorschrift, die jedem $n \in M$ genau ein Element aus N zuordnet, dieses wird mit $f(n)$ bezeichnet. **Notation**:

$$f : M \to N, m \mapsto f(m)$$

Zwei Abbildungen $f, g : M \to N$ sind gleich, wenn gilt $\forall\, n \in M : f(n) = g(n)$ M heißt die Definitionsmenge von f, N heißt die Zielmenge von f

2.6.1 Definition

Eine Abbildung f von M nach N ist ein Tupel (M, N, G_f), wobei G_f eine Teilmenge von $M \times N$ mit der Eigenschaft ist, dass für jedes Element $m \in M$ genau ein Element $n \in N$ mit $(m, n) \in G_f$ existiert. (für dieses Element n schreiben wir auch $f(m)$). G_f heißt der Graph von f.

2.6.2 Beispiel

1. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$
2. $f : \mathbb{R} \to \mathbb{R}^2, x \mapsto (x, x+1)$
3. M Menge, $\mathrm{id}_M : M \to M, m \mapsto m$ heißt Identität (identische Abbildung) auf M
4. I,M Mengen: Eine über I indizierte Familie von Elementen von M ist eine Abbildung:
   $m : I \to M, i \mapsto m(i) =: m_i$. Wir schreiben für die Familie auch kurz $(m_i)_{i\in I}$. I heißt Indexmenge der Familie.
5. Spezialfall von 4.: $I = \mathbb{N}, M = \mathbb{R} :\ \left((m_i)_{i\in\mathbb{N}}\right)$ nennt man auch Folge reeller Zahlen.

2.6.3 Anmerkung über den Begriff der Familie

Über den Begriff der Familie lassen sich diverse Konstruktionen aus der naiven Mengenlehre verallgemeinern. Ist $(M_i)_{i\in I}$ eine Familie von Mengen, dann ist:

$$\cup_{i\in I} M_i := \{x \mid \exists i \in I : x \in M_i\}$$

$$\cap_{i\in I} M_i := \{x \mid \forall\, i \in I : x \in M_i\}$$

$$\prod_{i\in I} M_i := \{(x_i)_{i\in I} \mid \forall\, i \in I : x_i \in M\}$$

2.6.4 Bild

m, N Mengen, $f : M \to n$ Abbildung.
Sind $m \in M, n \in N$ mit $n = f(m)$ dann nennen wir n ein **Bild** von m unter f und wir nennen m ein **Urbild** von n unter f.

Anmerkung In obiger Situation ist das Bild von m unter f eindeutig bestimmt (nach der Definition einer Abbildung) Urbilder sind im allgemeinen nicht eindeutig bestimmt, und im Allgemeinen besitzt nicht jedes Element aus N ein Urbild.

Beispiel $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, dann ist $4 = f(2) = f(-2)$, das heißt 2 und -2 sind Urbilder von 4, das Element -5 hat kein Urbild unter f, denn es existiert kein $x \in \mathbb{R}$ mit $x^2 = -5$

Definition M, N Mengen, $f : M \to N$ Abbildung, $A \subseteq M, B \subseteq N$
$f(A) := \{f(a) \mid a \in A\} \subseteq N$ heißt das Bild von A unter f.
$f^-1(B) := \{m \in M \mid f(m) \in B\} \subseteq M$ heißt das Urbild von B unter f

Beispiel

$$f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$$

$$f(\{1, 2, 3\}) = \{1, 4, 9\}$$
$$f^-1(\{4, -5\}) = \{2, -2\}$$
$$f^-1(\{4\}) = \{2, -2\}$$
$$f^-1(\{-5\}) = \emptyset$$
$$f(\mathbb{R}) = x^2 \mid x \in \mathbb{R} = \{x \in \mathbb{R} \mid x \geq 0\} =: \mathbb{R}_{\geq 0}$$

2.6.5 Restriktion

M, N Mengen, $f : M \to N$ Abbildung, $A \subseteq M$

$$f\mid_A : A \to N, m \mapsto f(m)$$

heißt die Restriktion von f auf A. Ist $B \subseteq N$ mit $f(A) \subseteq B$, dann setzen wir

$$f\mid_A^B : A \to B, m \mapsto f(m)$$

Ist $f(M) \subseteq B$ dann setzen wir:

$$f\mid^B := f\mid_M^B, M \to B, m \mapsto f(m)$$

2.6.6 Komposition

L, M, N Mengen, $f : L \to M, g : M \to N$ Abbildung

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

heißt die Komposition (Hintereinanderausführung) von f und g

Beispiel

$$f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2, g : \mathbb{R} \to \mathbb{R} : x \mapsto x + 1$$
$$\implies g \circ f : \mathbb{R} \to \mathbb{R}, x \mapsto g(f(x)) = g\big(x^2\big) = x^2 + 1$$

Assoziativität L, M, N, P Mengen, $f : L \to M, g : M \to N, h : n \to p$
Dann gilt

$$h \circ (g \circ f) = (h \circ g) \circ f$$

das heißt die Verknüpfung von Abbildungen ist assoziativ.

Beweis Für $x \in List$

$$(h \circ (g \circ f)) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)\square$$

2.6.7 Eigenschaften von Abbildungen

M, N Mengen, $f : M \to N$ Abbildung

Injektivität f heißt injektiv:

$\overset{\text{Def}}{\iff} \forall m_1, m_2 \in M : f(m_1) = f(m_2) \implies m_1 = m_2 \iff \forall m_1, m_2 \in M : m_1 \neq m_2 \implies f(m_1) \neq f(m_2)$

Surjektivität f heißt surjektiv:

$$\overset{\text{Def}}{\iff} \forall n \in M : \exists m \in M : f(m) = n \iff f(M) = N$$

Bijektivität f heißt bijektiv: $\overset{\text{Def}}{\iff}$ f ist injektiv und surjektiv

Beispiel

1. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ ist:
    - nicht injektiv, denn $f(2) = f(-2)$, aber $2 \neq -2$
    - nicht surjektiv, denn es existiert kein $m \in \mathbb{R}$ mit $f(m) = -1$
    - nicht bijektiv
2. $f : \mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto x^2$ ist:
    - injektiv, denn für $m_1, m_2 \in \mathbb{R}_{\geq 0}$ gilt: $f(m_1) = f(m_2) \implies m_1^2 = m_2^2 \xRightarrow{m_1, m_2 > 0} m_1 = m_2$
    - nicht surjektiv, denn es existiere kein $m \in \mathbb{R}_{\geq 0}$ mit $f(m) = -1$
    - nicht bijektiv
3. $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$ ist:
    - injektiv, denn für $m_1, m_2 \in \mathbb{R}_{\geq 0}$ gilt: $f(m_1) = f(m_2) \implies m_1^2 = m_2^2 \xRightarrow{m_1, m_2 > 0} m_1 = m_2$
    - surjektiv, denn für $m \in \mathbb{R}_{\geq 0}$ ist $f(\sqrt{m}) = (\sqrt{m})^2 = m$
    - bijektiv

Bemerkung 4.12 M, N Mengen, $f : M \to N, g : n \to M$ mit $g \circ f = \mathrm{id}_M$ Dann ist f injektiv und g surjektiv.

Beweis

1. f ist injektiv, denn:
   Seien $m_1, m_2 \in M$ mit $f(m_1) = f(m_2) \implies g(f(m_1)) = g(f(m_2)) \implies (g \circ f)(m_1) = (g \circ f)(m_2) \implies \mathrm{id}_m(m_1) = \mathrm{id}_M(m_2) \implies m_1 = m_2$
2. g ist surjektiv, denn:
   Sei $m \in M$ Dann ist $m = \mathrm{id}_M(m) = (g \circ f)(m) = g(f(m))$

Bemerkung Sei $f : M \to N, N, M$ Mengen Dann sind äquivalent:

1. f ist bijektiv
2. Zu jedem $n \in N$ gibt es genau ein $m \in M$ mit $f(m) = n$
3. Es gibt genau eine Abbildung $g : N \to M$ mit $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$

In diesem Fall bezeichnen wir die Abbildung $g : N \to M$ aus 3. mit f^{-1} und nennen f^{-1} die Umkehrabbildung von f. Sie ist gegeben durch

$$f^{-1} : N \to M, n \mapsto \text{ Das eindeutig bestimmte Element } m \in M \text{ mit } f(m) = n$$

Beweis Statt 1. $\iff$ 2. und 2. $\iff$ 3. zeigen 1. $\implies$ 2. $\implies$ 3. $\implies$ 1.

- 1. $\implies$ 2. Sei f bijektiv
  zu zeigen: Ist $n \in N$, dann existiert genau ein $m \in M$ mit $f(m) = n$
  - Existenz folgt aus Surjektivität von f
  - Eindeutigkeit: Seien $m_1, m_2 \in M$ mit $f(m_1) = n, f(m_2) = n \implies f(m_1) = f(m_2) \xRightarrow{finjektiv}$ $m_1 = m_2$
- 2. $\implies$ 3. Zu jedem $n \in M$ existiere genau ein $m \in M$ mit $f(m) = n$
  zu zeigen: Ex existiert genau eine Abbildung $g : N \to M$ mit $f \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$
  - Existenz: Wir definieren $g : N \to M, n \mapsto$ das nach 2. eindeutigbestimmte Element $m \in M$ mit $f(m) = n$
    Dann gilt für $m \in M$:
    $$(g \circ f)(m) = f(f(m)) = m, \text{ das heißt } g \circ f = \mathrm{id}_M$$
    und für $n \in N$ ist $(f \circ g)(n) = f(g(n)) = n$ also $f \circ g = id_N$
  - Eindeutigkeit: Es seinen $g_1, g_2 : N \to M$ mit $g_i \circ f = \mathrm{id}_M, f \circ g_i = \mathrm{id}_N$ für $i = 1, 2$
    $$\implies g_1 = g_1 \circ \mathrm{id}_N = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_M \circ g_2 = g_2$$
- 3. $\implies$ 1. Wegen 3. existiert $g : N \to M$ mit $g \circ f = \mathrm{id}_M, f \circ g = \mathrm{id}_N$
  $$\xRightarrow{[[Bemerkung4.12]]} f \text{ injektiv }, f \text{ surjektiv } \implies f \text{ bijektiv } \implies 1.$$

Anmerkung

- Bitte stets aufpassen, ob mit f^{-1} die Umkehrabbildung (falls existent) oder das Bilden der Urbildmenge gemeint ist.
- Im Beweis von 3. $\implies$ 1. haben wir die Eindeutigkeit von g gar nicht verwendet, das heißt wir haben sogar gezeigt:
  f bijektiv $\iff$ 3.' Es existiert eine Abbildung $g : N \to M$ mit $f \circ g = \mathrm{id}_N$ und $f \circ f = \mathrm{id}_M$ Solch eine Abbildung g ist in diesem Fall automatisch bestimmt.

Beispiel Im Beispiel vorher haben wir gesehen $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$ ist bijektiv. Die Umkehrabbildung ist gegeben durch $f^{-1} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto \sqrt{x}$

Bemerkung M, N Mengen, $f : M \to N$ Dann gilt:

1. f injektiv $\iff$ Es existiert $g : N \to M$ mit $g \circ f = \mathrm{id}_M$
   Beweis:
   - „ $\Longleftarrow$ “ folgt aus 2.6.7
   - „ $\Longrightarrow$ “ Sei f injektiv. Sein x ein beliebiges Element aus M Wir definieren

     $$g : N \to M, n \mapsto \begin{cases} x & n \notin f(M) \\ \text{das eindeutig bestimmte Element } m \in M \text{ mit } f(m) = n & n \in f(M) \end{cases}$$

     Für alle $m \in M$ ist dann $(g \circ f)(m) = g(f(m)) = m$ das heißt $g \circ f = \mathrm{id}_M$
2. f surjektiv $\iff$ Es existiert $g : N \to M$ mit $f \circ g = \mathrm{id}_N$
   Beweis:
   - „ $\Longleftarrow$ “ folgt aus 2.6.7
   - „ $\Longrightarrow$ “ Sei f surjektiv. Für jedes Element $n \in N$ wählen wir ein Element $\tilde{n} \in f^{-1}(\{n\}) \neq \emptyset$ und sehen $g : N \to M, n \mapsto \tilde{n}$. Dann ist $(f \circ g)(n) = f(g(n)) = n$ für alle $n \in N$ und das heißt $f \circ g = \mathrm{id}_N$ □

Anmerkung Das wir stets einen Auswahlprozess wie im Beweis von 2. „ $\Longrightarrow$ “ vornehmen können ist ein Axiom der Mengenlehre (erkennen wir als gültig an, ist jedoch nicht beweisbar), das **Auswahlaxiom**:
Ist I eine Indexmenge und $(A_i)_{i \in I}$ eine Familie von nicht leeren Mengen, dann gibt es eine Abbildung $\gamma : I \to \bigcup_{i \in I} A_i$ mit $\gamma(i) \in A_i$ für alle $i \in I$ (im obigen Beweis ist $I = N, A_n = f^{-1}(\{n\})$ für $n \in N$)

Bemerkung 4.16 L, M, N Mengen, $f : L \to M, g : M \to N$
Dann gilt: g, f beide injektiv (beziehungsweise surjektiv oder bijektiv) $\Longrightarrow$ $g \circ f$ injektiv (beziehungsweise surjektiv oder bijektiv)

Definition 4.17

Bemerkung 4.19 M, N endliche Mengen mit $|M| = |N|, f : M \to N$ Dann sind äquivalent:

1. f ist injektiv
2. f ist surjektiv
3. f ist bijektiv

Beweis

- 1. $\Longrightarrow$ 2. Sei f injektiv $\Longrightarrow$ $|f(M)| = |M| = |N|$ wegen $f(M) \subseteq N$ folgt $f(M) = N$ $\Longrightarrow$ f surjektiv
- 2. $\Longrightarrow$ 3. Sei f surjektiv, das heißt $f(M) = N$
  Annahme: f ist nicht bijektiv $\Longrightarrow$ f nicht injektiv $\Longrightarrow$ $\exists m_1, m_2 \in M : m_1 \neq m_2 \wedge f(M_1) = f(m_2)$ $\Longrightarrow$ $|f(M)| < |M| = |N|$ Widerspruch zu $f(M) = N$
- 3. $\Longrightarrow$ 1. trivial

3 Gruppen, Ringe, Körper

3.1 Gruppe

3.1.1 Verknüpfung

M Menge, Eine Verknüpfung (inverse Verknüpfung) auf M ist ein Abbildung

$$* : M \times M \to M$$

Anstelle von $*(a,b)$ schreiben wir $a * b$

Beispiel

- $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a,b) \mapsto a + b$
- $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a,b) \mapsto a \cdot b$

sind Verknüpfungen

3.1.2 Monoid

Ein Monoid ist ein Tupel $(M, *)$, bestehend aus einer Menge M und einer Verknüpfung $* : M \times M \to M$, welche folgende Bedingungen genügt:

- (M1) Die Verknüpfung ist assoziativ, das heißt
$$\forall\, a, b, c \in M : (a * b) * c = a * (b * c)$$
- (M2) Ex existiert ein neutrales Element e in M, das heißt
$$\exists e \in M : \forall\, a \in M e * a = a = a * e$$

Beispiel

- $(\mathbb{N}_0, +), (\mathbb{Z}, +)$ sind Monoide (neutrales Element: 0)
- $(\mathbb{N}, +)$ ist kein Monoid (ex existiert kein neutrales Element)
- $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot)$ sind Monoide (neutrales Element: 1)

Bemerkung $(M, *)$ Monoid. Dann gibt es in M genau ein neutrales Element.

Beweis

- Existenz: Es existiert ein neutrales Element: folgt aus Definition eines Monoids
- Eindeutigkeit: Seien $e, \tilde{e} \in M$ neutrale Element
$$\implies e = e * \tilde{e} = \tilde{e}$$

3.1.3 Inverses

$(M, *)$ Monoid mit neutralem Element e, $a \in M$ Ein Element $b \in M$ heißt Inverses zu $a \overset{\text{Def}}{\iff} a * b = e = b * a$

Beispiel

- In $(\mathbb{Z}, +)$ ist -2 ein Inverses zu 2 denn $2 + (-2) = 0 = (-2) + 2$
- In $(\mathbb{N}_0, +)$ existiert kein Inverses zu 2, denn es existiert kein $n \in \mathbb{N}_0$ mit $n + n = 0 = n + 2$
- In $(\mathbb{Z}, \cdot)$ existiert kein Inverses zu 2, denn es existiert kein $n \in \mathbb{Z}$ mit $2 \cdot n = 1 = n \cdot 2$

Bemerkung $(M, *)$ Monoid, $a \in M$ Dann gilt: besitzt a ein Inverses, dann ist dieses eindeutig bestimmt.

Beweis Seinen $b, \tilde{b}$ Inversen zu a, sein $e \in M$ das neutrale Element

$$\implies b = e * b = \left(\tilde{b} * a\right) * b = \tilde{b} * (a * b) = \tilde{b}$$

3.1.4 Gruppe

Eine Gruppe ist ein Tupel $(G, *)$, bestehen aus einer Menge G und einer Verknüpfung $* : G \times G \to G$, sodass gilt:

- (G1) $(G, *)$ ist ein Monoid
- (G2) Jedes Element aus G besitzt ein Inverses

In diesem Fall schreiben wir a' für das nach 3.1.3 eindeutig bestimmte Inverse eines Elements $a \in G$

Beispiel

- $(\mathbb{Z}, +)$ ist eine Gruppe, denn $(\mathbb{Z}, +)$ ist ein Monoid und für $a \in \mathbb{Z}$ ist $-a$ das inverse Element: $a + (-a) = 0 = (-a) + a$
- $(\mathbb{Z}, \cdot)$ ist keine Gruppe, denn das Element $2 \in \mathbb{Z}$ hat kein Inverses (vergleiche 3.1.3).
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine Gruppe denn es ist ein Monoid mit neutralem Element 1 und für jedes Element $a \in \mathbb{Q} \setminus \{0\}$ existiert ein $b \in \mathbb{Q} \setminus \{0\}$ mit $a \cdot b = 1 = b \cdot a$, nämlich $b = \frac{1}{a}$

Bemerkung 5.11 $(G, *)$ Gruppe mit neutralem Element $e, a, b, c \in G$. Dann gilt

1. (Kürzungsregel)
$$a * b = a * c \implies b = c$$
$$a * c = b * c \implies a = b$$
2. $a * b = e \implies b = a'$
3. $(a')' = a$
4. (Regel von Hemd und Jacke) $(a * b)' = b' * a'$

Beweis

1. Sei $a * b = a * c \implies a' * (a * b) = a' * (a * c) \implies (a' * a) * b = (a' * a) * c \implies e * b = e * c \implies b = c$
2. aus 1. $a * b = c = a * a' \implies b = a'$
3. Es ist $a * a' = e = a' * a$, das heißt a ist Inverses zu $a' \implies (a')' = a$
4. Es ist $(a * b) * (b' * a') = a * (b * b') * a' = a * a' = e \implies b' * a' \overset{2.}{\Rightarrow} (a * b)'$

3.1.5 Abelsche Gruppe

$(M, *)$ Monoid / Gruppe heißt kommutativ (abelsch)

$$\overset{\text{Def}}{\iff} \forall\, a, b \in M : a * b = b * a$$

Beispiel Alle bisher betrachteten Beispiele von Monoiden beziehungsweise Gruppen sind abelsch

Bemerkung 5.14 M Menge, Wir setzten $S(M) := \{f : M \to M | f \text{ bijektiv}\}$ Dann ist $(S(M), \circ)$ eine Gruppen, die **symmetrische** Gruppe auf M

Beweis

1. „$\circ$“ ist wohl definiert, das heißt für $f, g \in S(M)$ ist $f \circ g \in S(M)$ folgt aus 2.6.7
2. „$\circ$“ ist assoziativ $f \circ (g \circ h) = (f \circ g) \circ h \,\forall\, f, g \in S(M)$ nach 4.9
3. id_M ist neutral: $\mathrm{id}_M \in S(M)$ und $\mathrm{id}_M \circ f = f = f \circ \mathrm{id}_M \,\forall\, f \in S(M)$
4. Existenz von Inversen: $f \in S(M) \implies f$ bijektiv $\implies$ Es existiert Umkehrabbildung $f^{-1} \in S(M)$ zu f für diese gilt: $f \circ f^{-1} = \mathrm{id}_M = f^{-1} \circ f$ das heißt f^{-1} ist immer zu f bezüglich „$\circ$“

3.1.6 Permutationen

$n \in \mathbb{N}$

$$S_n := S(\{1, \ldots, n\}) = \{\pi\{1, \ldots, n\} \to \{1, \ldots, n\} \mid \pi \text{ ist bijektiv}\}$$

$(S_n, \circ)$ heißt die symmetrische Gruppe auf n Ziffern, Elemente aus S_n heißen Permutationen. Wir schreiben Permutationen $\pi \in S_n$ in der Form:

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix} \tag{1}$$

Beispiel In S_3 ist

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

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

das heißt $(S_3, \circ)$ ist nicht abelsch.

3.1.7 Restklassen

Motivation Im täglichen Leben verwendet man zur Bestimmung von Urzeiten das Rechnen „modulo 24“, zum Beispiel 22Uhr + 7h = 5Uhr. Wir wollen dies mathematisch präzisieren und verallgemeinern

Bemerkung 5.17 $n \in \mathbb{N}$. Dann ist durch

$$a \sim b \overset{\text{Def}}{\iff} \exists\, q \in \mathbb{Z} : a - b = qn$$

eine Äquivalenzrelation auf $\mathbb{Z}$ gegeben. Anstelle von $a \sim b$ schreiben wir auch $a \equiv b(\mod n)$ („n ist kongruent b modulo n") Die Äquivalenzklasse von $a \in \mathbb{Z}$ ist durch

$$\bar{a} := \{b \in \mathbb{Z} \mid b \equiv a(\mod n)\} = a + n\mathbb{Z} := \{a + nq \mid q \in \mathbb{Z}\}$$

gegeben und heißt die Restklasse von a modulo n. Die Menge aller Restklassen modulo n wird $\frac{\mathbb{Z}}{n\mathbb{Z}}$ bezeichnet („$\mathbb{Z}$ modulo $n\mathbb{Z}$") Es ist:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

und die Restklassen $\bar{0}, \dots, \overline{n-1}$ sind paarweise verschieden

Beweis

1. „$\equiv$" ist eine Äquivalenzrelation, denn:
   - „$\equiv$" ist reflexiv: Für $a \in \mathbb{Z}$ ist $a \equiv a(\mod n)$ denn $a - a = 0 = 0n$
   - „$\equiv$" ist symmetrisch: Seien $a, b \in \mathbb{Z}$ mit $a \equiv b(\mod n) \exists q \in \mathbb{Z} : a - b = qn$
     $\implies b - a = (-q)n \implies b \equiv a(\mod n)$
   - „$\equiv$" ist transitiv: Seien $a, b, c \in \mathbb{Z}$ mit $a \equiv b(\mod n), b \equiv c(\mod n)$
     - $\implies \exists q_1, q_2 \in \mathbb{Z}$ mit $a - b = q_1 n, b - c = q_2 n$
     - $\implies a - c = (a - b) + (b - c) = q_1 n + q_2 n = (q_1 + 1_2)n \implies a \equiv c(\mod n)$
2. Die Äquivalenzklasse von $n \in \mathbb{Z}$ ist gegeben durch

$$\begin{aligned} &\{b \in \mathbb{Z} \mid b = a(\mod n)\} \\ &= \{b \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : b - a = qn\} \\ &= \{b \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : b = a + qn\} \\ &= a + n\mathbb{Z} \end{aligned}$$

3.

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

   denn:
   - Ist $a \in \mathbb{Z}$ beliebig, dann liefert Division mit Rest durch n:
     Es gibt $q, r \in \mathbb{Z}$ mit $a = qn + r, 0 \leq r < n$

$$\implies a - r = qn \implies q \equiv r(\mod n) \implies \bar{a} = \bar{r}$$

     Das heißt: Jede Restklasse ist von der Form $\bar{r}$ mit $r \in \{0, \dots, n-1\}$
   - Die Restklassen $\bar{0}, \bar{1}, \dots, \overline{n-1}$ sind paarweise verschieden denn:
     Seien $a, b \in \{0, \dots, n-1\}$ mit $\bar{a} = \bar{b} \implies a \equiv b(\mod n) \implies \exists q \in \mathbb{Z} : a - b = qn \implies |a - b| = |q|n$.
     - Wäre $q \neq 0$, dann $|q| \geq 1$ wegen $q \in \mathbb{Z} \implies |a - b| \geq n$ **Widerspruch** zu $a, b \in \{0, \dots, n-1\}$
       Also: $q = 0$ das heißt $a = b$

Beispiel $n = 3 : a \equiv b(\mod 3) \iff \exists q \in \mathbb{Z} : a - b = 3q$
zum Beispiel: $11 \equiv 5(\mod 3)$, denn $11 - 5 = 6 = 2 \cdot 3$
zum Beispiel: $7 \not\equiv 2(\mod 3)$, denn $7 - 2 = 5$ und es gibt kein $q \in \mathbb{Z}$ mit $5 = 3q$

$$\bar{0} = \{a \in \mathbb{Z} \mid a \equiv 0(\mod 3)\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a = 3q\} = 3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

$$\bar{1} = \{a \in \mathbb{Z} \mid a \equiv 1(\mod 3)\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a - 1 = 3q\} = 1 + 3\mathbb{Z} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$\bar{2} = \{a \in \mathbb{Z} \mid a \equiv 2(\mod 3)\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a - 2 = 3q\} = 2 + 3\mathbb{Z} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

$$\bar{3} = \{a \in \mathbb{Z} \mid a \equiv 3(\mod 3)\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a-3 = 3q\} = \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a = 3(q+1)\}3\mathbb{Z} = \bar{0}$$

$$\bar{4} = \bar{1}, \bar{5} = \bar{2}, \overline{-1} = \bar{2}$$

Bemerkung 5.18 $n \in \mathbb{N}$ wir definieren eine Verknüpfung (Addition) auf $\frac{\mathbb{Z}}{n\mathbb{Z}}$ wie folgt:
Für $\bar{a}, \bar{b} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ setzen wir $\bar{a} + \bar{b} = \overline{a + b}$ Dann gilt $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$ ist eine abelsche Gruppe

Beweis

1. Die Verknüpfung ist wohldefiniert:
   Problem: Die Addition verwendet Vertreter von Restklassen. Es ist zum Beispiel in $\frac{\mathbb{Z}}{n\mathbb{Z}} : \bar{3} + \bar{4} = \overline{3 + 4} = \bar{7} = \bar{2}$, aber man könnte auch Rechnen: $\bar{3} + \bar{4} = \bar{8} + \bar{9} = \overline{8 + 9} = \overline{17} = \bar{2}$
   Wir müssen nachweisen, dass die Wahl der Vertreter keinen Einfluss auf das Ergebnis hat, das heißt die Verknüpfung ist "Vertreter unabhängig":
   Seien $a_1, a_2, b_1, b_2 \in \mathbb{Z}, \overline{a_1} = \overline{a_2}, \overline{b_1} = \overline{b_2}$

$$\implies a_1 \equiv a_2(\mod n), b_1 \equiv b_2(\mod n) \tag{4}$$
$$\implies \exists q_1, q_2 \in \mathbb{Z} : a_1 - a_2 = q_1 n, b_1 - b_2 = q_2 nn, b_1 - b_2 = q_2 n \tag{5}$$
$$\implies (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = q_1 n + q_2 n = (q_1 + q_2)n \tag{6}$$
$$\implies a_1 + b_1 \equiv a_2 + b_2(\mod n) \tag{7}$$
$$\implies \overline{a_1 + b_1} = \overline{a_2 + b_2} \tag{8}$$

2. $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$ ist eine abelsche Gruppe:
   - Assoziativgesetz: Für alle $a, b, c \in \mathbb{Z}$ ist
   $$\left(\bar{a} + \bar{b}\right) + \bar{c} = \overline{a + b} + \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} + \overline{b + c} = \bar{a} + \left(\bar{b} + \bar{c}\right)$$
   - $\bar{0}$ ist neutrales Element, denn $\forall\, a \in \mathbb{Z} : \bar{0} + \bar{a} = \overline{0 + a} = \bar{a} = \bar{a} + \bar{0}$
   - Für $a \in \mathbb{Z}$ ist $\overline{-a}$ das inverse Element zu $\bar{a}$, denn $\bar{a} + \overline{-a} = \overline{a + (-a)} = \bar{0} = \overline{-a} + \bar{a}$
   - Kommutativgesetz: $\forall\, a, b \in \mathbb{Z} : \bar{a} + \bar{b} = \overline{a + b} = \overline{b + a} = \bar{b} + \bar{a}$

Beispiel Wir tragen die Ergebnisse der Verknüpfung „+“ in einer Verknüpfungstafel zusammen: n = 3

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

n = 4

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

3.1.8 Gruppenhomomorphismus

$(G, *), (H, \circledast), \varphi : G \to H$ Abbildung
φ heißt ein Gruppenhomomorphismus $\overset{\text{Def}}{\iff} \forall\, a, b \in G : \varphi(a * b) = \varphi(a) \circledast \varphi(b)$
φ heißt ein Gruppenisomorphismus $\overset{\text{Def}}{\iff}$ φ ist bijektiver Gruppenhomomorphismus

Beispiel

1. $\varphi : \mathbb{Z} \to \mathbb{Z}, a \mapsto 2a$ ist Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}, +)$ denn:
$$\varphi(a + b) = 2(a + b) = 2a + 2b = \varphi(a) + \varphi(b) \,\forall\, a, b \in \mathbb{Z}$$
φ ist aber kein Gruppenisomorphismus, denn φ ist nicht surjektiv $(1 \notin \varphi = \varphi\mathbb{Z})$
2. $n \in \mathbb{N}$. Dann gilt $\varphi : \mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}}, a \mapsto \bar{a}$ ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$, denn
$$\forall\, a, b \in \mathbb{Z} : \varphi(a + b) = \overline{a + b} = \bar{a} + \bar{b} = \varphi(a) + \varphi(b)$$
φ ist kein Gruppenisomorphismus, denn φ ist nicht injektiv ($\varphi(0) = \bar{0} = \bar{n} = \varphi(n)$, aber $0 \neq n$)
3. $\varphi : \mathbb{Z} \to \mathbb{Z}, a \mapsto a + 1$ ist kein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}, +)$, denn
$$\varphi(2 + 6) = \varphi(8) = 9, \text{ aber } \varphi(2) + \varphi(6) = 3 + 7 = 10$$
4. $\exp : \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto \exp x = e^x$ ist ein Gruppenisomorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{R}_{\geq 0}, \cdot)$, denn:
   - $$\exp(a + b) = \exp(a)\exp(b) \,\forall\, a, b \in \mathbb{R}$$
   - exp ist bijektiv (vgl. Ana1 - Vorlesung)

Bemerkung 5.23 $(G, *), (H, \circledast)$ Gruppen mit neutralen Elementen e_G beziehungsweise $e_H, \varphi : G \to H$ Gruppenhomomorphismus. Dann gilt

1. $\varphi(e_G) = e_H$
2. $\forall\, a \in G : \varphi(a') = \varphi(a)'$ (Hierbei ist $'$ das Inverse)
3. Ist φ Gruppenisomorphismus, dann gilt $\varphi^{-1} : H \to G$ ebenfalls Gruppenisomorphismus

$(G, *), (H, \circledast)$ heißen isomorph $\overset{\text{Def}}{\iff}$ Ex existiert ein Gruppenisomorphismus $\phi : G \to H$ Wir schreiben dann $(G, *) \cong (H, \circledast)$

Beweis

1. Es $e_H \circledast \varphi(e_G) = \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) \circledast (e_G) \implies e_H = \varphi(e_G)$
2. Sei $a \in G$ Dann ist $e_H = \varphi(e_G) = \varphi(a * a') = \varphi(a) \circledast (a') \implies \varphi(a') = \varphi(a)'$
3. φ^{-1} ist bijektiv, noch zu zeigen: φ^{-1} ist ein Gruppenhomomorphismus, das heißt
$$\varphi^{-1}(c \circledast d) = \varphi^{-1}(c) * \varphi^{-1}(d) \,\forall\, c, d \in H$$
Seien $c, d \in H$ Weil φ bijektiv: $\exists a, b \in G : \varphi(a) = c, \varphi(b) = d$
$$\implies \varphi^{-1}(c \circledast d) = \varphi^{-1}(\varphi(a) * \varphi(b)) = \varphi^{-1}(\varphi(a * b)) = a * b = \varphi^{-1}(c) * \varphi^{-1}(d) \square$$

3.2 Ring

Ein Ring ist ein Tupel $(R, +, \cdot)$, bestehend aus einer Menge R und 2 Verknüpfungen:

- $+ : R \times R \to R, (a, b) \mapsto a + b$ genannt Addition
- $\cdot : R \times R \to R, (a, b) \mapsto a \cdot b$ genannt Multiplikation

welche den folgenden Bedingungen genügen

- (R1) $(R, +)$ ist eine abelsche Gruppe
- (R2) $(R, \cdot)$ ist ein Monoid
- (R3) Es gelten die Distributivgesetz, das heißt

$$\forall\, a, b, c \in R : a \cdot (a + b) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$$

Ein Ring heißt **kommutativ** $\overset{\text{Def}}{\iff}$ die Multiplikation ist kommutativ, das heißt $\forall\, a, b \in R : a \cdot b = b \cdot a$

3.2.1 Anmerkung

- ohne Klammerung gilt die Konvention „$\cdot$“ vor „$+$“. Das Zeichen „$\cdot$“ wird häufig weggelassen.
- das neutrale Element bezüglich „$+$“ bezeichnen wir mit 0_R (Nullelement), das neutrale Element bezüglich „$\cdot$“ mit 1_R (Einselement). Das zu $a \in R$ bezüglich „$+$“ inverse Element bezeichnen wir mit $-a$, für $a+(-b)$ schreiben wir $a - b$. Existiert zu $a \in R$ ein Inverses bezüglich „$\cdot$“, so bezeichnen wir dieses mit a^{-1}
- Wir schreiben häufig verkürzend „R Ring“ statt „$(R, +, \cdot)$ Ring“
- In der Literatur wird gelegentlich die Forderung der Existenz eines neutralen Elements bezüglich „$\cdot$“ weggelassen, „unser“ Ringbegriff entspricht dort dem Begriff „Ring mit Eins“

3.2.2 Beispiel

1. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring
2. Nullring $(\{0\}, +, \cdot)$ mit $0 + 0 = 0, 0 \cdot 0 = 0$ ist ein kommutativer Ring
   (hier ist Nullelement = Einselement = 0). Wir bezeichnen den Nullring kurz mit 0.

3.2.3 Bemerkung 6.3

R Ring. Dann gilt:

1. $0_R \cdot a = 0_R = a \cdot 0_R \,\forall\, a \in R$
2. $a \cdot (-a) = -ab = (-a) \cdot b \,\forall\, a, b \in R$
3. Ist $R \neq 0$, dann ist $1_R \neq 0_R$

Beweis

1. $0_R + 0_R \cdot a = 0_R \cdot a = (0_R + 0_R) \cdot a = 0_R \cdot a + 0_R \cdot \xrightarrow{\text{„kürzen s. [[Bemerkung 5.11]]“}} 0_R = 0_R \cdot a, a \cdot 0_R = 0_R$ analog

2. $0_R = 0_R \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b \implies$ [[Bemerkung 5.11]] $-ab = (-a) \cdot b, a \cdot (-b) 0 - ab$ analog

3. Beweis durch Kontraposition: Sei $1_R = 0_R$

$$\implies \forall\, a \in R : a = a \cdot 1_R = a \cdot 0_R = 0_R$$

das heißt $R = 0$ □

3.2.4 Bemerkung 6.4

$n \in \mathbb{N}$ Für $\bar{a}, \bar{b} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ setzen wir $\bar{a} + \bar{b} := \overline{a + b}, \bar{a} \cdot \bar{b} := \overline{ab}$, dann ist $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot\right)$ ein kommutativer Ring.
Wenn wir ab jetzt vom Ring $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sprechen, dann meinen wir $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot\right)$ mit den obigen Verknüpfungen

Beweis

1. Multiplikation ist wohldefiniert (das heißt „vertreterunabhängig“, vergleiche 3.1.7)
Sei $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ mit $\overline{a_1} = \overline{a_2}, \overline{b_2} = \overline{b_2}$

$$\implies a_1 \equiv a_2 (\mod n), b_1 \equiv b_2 (\mod n) \tag{9}$$
$$\implies \exists q_1, q_2 \in \mathbb{Z} : a_1 - a_2 = q_1 n, b_1 - b_2 = q_2 n \tag{10}$$
$$\implies a_1 b_2 - a_2 b_2 = a_1 (b_1 - b_2) + b_2 (a_1 - a_2) = a_q q_2 n + b_2 q_1 n = (a_1 q_2 + b_2 q_1) n \tag{11}$$
$$\implies a_1 b_1 \equiv a_2 b_2 (\mod n) \tag{12}$$
$$\implies \overline{a_1 b_1} = \overline{a_2 b_2} \tag{13}$$

2. Multiplikation ist assoziativ, Für $a, b, c \in \mathbb{Z}$ ist

$$\bar{a} \cdot \left(\bar{b} \cdot \bar{c}\right) = \bar{a} \cdot \overline{a \cdot c} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot b} \cdot \bar{c} = \left(\bar{a} \cdot \bar{b}\right) \cdot \bar{c}$$

3. Existenz eines Einselement: $\forall\, a \in \mathbb{Z} : \bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a} = \bar{a} \cdot \bar{1}$

4. Multiplikation ist kommutativ:

$$\forall\, a, b \in \mathbb{Z} : \bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \cdot \bar{a}$$

5. $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$ ist abelsche Gruppe nach 3.1.7

6. Distributivgesetz:

$$\bar{a} \cdot \left(\bar{b} + \bar{c}\right) = \bar{a} \cdot \overline{b + c} \tag{14}$$
$$= \overline{a \cdot (b + c)} \tag{15}$$
$$= \overline{a \cdot b + a \cdot c} \tag{16}$$
$$= \overline{a \cdot b} + \overline{a \cdot c} \qquad = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} \tag{17}$$

$\left(\bar{a} + \bar{b}\right) \cdot \bar{c} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}$ folgt wegen Kommutativität der Multiplikation

Beispiel 6.5 Verknüpfungstafel für $\frac{\mathbb{Z}}{n\mathbb{Z}}$ n = 3:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

n = 4:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

In $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ist $\bar{2} \cdot \bar{2} = \bar{0}$, aber $\bar{2} \neq \bar{0}$.

3.2.5 Integritätsbereich

ist ein kommutativer Ring $(R, +, \cdot)$ mit $R \neq 0$, in dem gilt:

$$\forall\, a, b \in R : a \cdot b = 0_R \implies a = 0_R \vee b = 0_R$$

beziehungsweise äquivalent dazu:

$$a \neq 0_R \wedge b \neq 0_R \implies a \cdot b \neq 0_R$$

Beispiel 6.7

- $\frac{\mathbb{Z}}{3\mathbb{Z}}$ ist ein Integritätsbereich, $\frac{\mathbb{Z}}{4\mathbb{Z}}$ ist kein Integritätsbereich, denn $\bar{2} \cdot \bar{2} = \bar{0}$, aber $\bar{2} \neq \bar{0}$

Bemerkung 6.8 $n \in \mathbb{N}$ Dann sind äquivalent

1. $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ist ein Integritätsbereich
2. n ist eine Primzahl

Beweis $1 \implies 2$ zeigen wir durch Kontraposition, das heißt $\neg 2 \implies \neg 1$
Sei $n \in \mathbb{N}$ keine Primzahl. Falls $n = 1$ dann ist $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}\}$ (Nullring), das heißt $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ist kein Integritätsbereich. Seim im Folgenden $n > 1$ und keine Primzahl.

$$\implies \exists a, b \in \mathbb{N} : 1 \ < a, b < n \wedge n = a \cdot b \tag{18}$$
$$\implies \bar{0} = \bar{n} = \overline{ab} = \bar{a} \cdot \bar{b} \tag{19}$$

und es ist $bara, \bar{b} \neq \bar{0} \implies \frac{\mathbb{Z}}{n\mathbb{Z}}$ kein Integritätsbereich.
$2 \implies 1$: Sein n eine Primzahl $\implies n > 1$, insbesondere $\frac{\mathbb{Z}}{n\mathbb{Z}} \neq 0$. Seien $\bar{a}, \bar{b} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ mit $\bar{a} \cdot \bar{b} = \bar{0}$

$$\implies \exists q \in \mathbb{Z} : ab = qn$$

Da n Primzahl, kommt n n der Primfaktorzerlegung von ab als Primfaktor vor
$\implies n$ kommt in der Primfaktorzerlegung von a oder b als Primfaktor vor

$$\implies n \mid a \vee n \mid b \implies \bar{a} = \bar{0} \vee \bar{b} = \bar{0}$$

3.3 Körper

Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$, in dem gilt $K \neq 0$ und jedes Element $a \in K, a \neq 0$ besitzt ein Inverses in K bezüglich „$\cdot$“, das heißt: $\exists b \in K : a \cdot b = 1_K$. Wir setzen $K^* := K \setminus \{0\}$

3.3.1 Beispiel

1. $(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot)$ sind Körper (mit den üblichen $+, \cdot$)
2. $\frac{\mathbb{Z}}{3\mathbb{Z}}$ ist ein Körper (betrachte Verknüpfungstafel)
3. $\frac{\mathbb{Z}}{4\mathbb{Z}}$ ist ein kein Körper: Das Element $\bar{2}$ besitzt kein Inverses bezüglich „$\cdot$“

3.3.2 Bemerkung 6.11

K Körper, Dann gilt:

1. $0_K \neq 1_K$
2. K ist ein Integritätsbereich
3. $(K^*, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1_K

Beweis

1. folgt aus 3.2.3
2. $K \neq 0$ nach Definition. Seien $a, b \in K$ mit $ab = 0_K$. Falls $a \neq 0_K$ dann

$$b = 1_K \cdot b = \left(a^{-1}a\right) \cdot b = a^{-a}(ab) = a^{-1} \cdot 0_K = 0_K$$

   Insbesondere gilt: $a = 0 \vee b = 0$

3. $K^* \times K^* \to K^*$ ist wohldefiniert nach 2 (aus $a, b \in K^*$ folgt $ab \in K^*$)
   Da $(K, \cdot)$ abelscher Monoid mit neutralem Element 1_K ist auch $(K^*, \cdot)$ abelscher Monoid mit neutralem Element 1_K. Nach 3.3 besitzt jedes Element $a \in K^*$ ein Inverses $b \in K$ mit $ab = 1_K$ Wegen $0_K \neq 1_K$ ist $b \neq 0_K$ (sonst $ab = a \cdot 0_K = 0_K \neq 1_K$), das heißt $b \in K^*$ $\square$

3.3.3 Bemerkung 6.12

R Integritätsbereich, der nur endlich viele Elemente hat. Dann ist R ein Körper.

Beweis R Integritätsbereich $\implies R \neq 0$
Noch zu zeigen: $a \in R \setminus \{0_R\} \implies \exists b \in R : ab = 1_R$ Sei $a \in R \setminus \{0_R\}$. Wir betrachten die Abbildung $\varphi_a : R \to R, x \mapsto ax$

1. Behauptung: φ_a ist injektiv, denn:

   Seien $x, y \in R$ mit

   $$\varphi_a(x) = \varphi_a(y) \implies ax = ay \implies ax + (-(ay)) = 0_R \tag{20}$$

   Mit [[Bemerkung 6.3]] folgt:

   $$\implies ax + a(-a) = -R \implies a(x-y) = 0_R \tag{21}$$

   Aus R Integritätsbereich und $a \neq 0$ folgt:

   $$x - y = 0 \implies x = y \tag{22}$$

2. Da R endlich ist und φ_a injektiv ist, ist φ_a nach 2.6.7 surjektiv

   $$\implies \exists b \in R : \varphi_a(b) = 1_R \implies ab = 1_R$$

3.3.4 Folgerung 6.13

$n \in \mathbb{N}$ Dann sind äquivalent

1. $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ist ein Körper
2. n ist eine Primzahl

Beweis $1 \implies 2$ durch Kontraposition: $\neq 2 \implies \neg 1$
Sei n keine Primzahl $\implies \frac{\mathbb{Z}}{n\mathbb{Z}}$ kein Integritätsbereich $\implies \frac{\mathbb{Z}}{n\mathbb{Z}}$ kein Körper
$2 \implies 1$ Sei n eine Primzahl $\implies \frac{\mathbb{Z}}{n\mathbb{Z}}$ Integritätsbereich, der nur endlich viele Elemente hat $\implies \frac{\mathbb{Z}}{n\mathbb{Z}}$ Körper

Notation p Primzahl. Man nennt $\mathbb{F}_P := \frac{\mathbb{Z}}{p\mathbb{Z}}$ auch den endlichen Körper mit p Elemente

3.3.5 Definition 6.14

R Ring

$$\operatorname{char}(R) := \begin{cases} 0 & \sum_{k=1}^{n} 1_R \neq 0 \,\forall\, n \in \mathbb{N} \\ \min\{n \in \mathbb{N} \mid \sum_{k=1}^{n} 1_R = 0_R\} & \text{sonst} \end{cases}$$

heißt die Charakteristik von R

Beispiel 3.1

1. $\operatorname{char}(\mathbb{Z}) = \operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = 0$
2. $\operatorname{char}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) = n$, denn $\sum_{k=1}^{n} \bar{1} = \bar{n} = \bar{0}$ und $\sum_{k=1}^{m} \bar{1} = \bar{m} \neq \bar{0}$ für $m \in \{1, \ldots, n-1\}$

Bemerkung 3.2 R Integritätsbereich. Dann ist $\mathrm{char}(R) = 0$ oder $\mathrm{char}(R)$ ist eine Primzahl

Beweis Beweis durch Widerspruch. Annahme: $\mathrm{char}(R) \neq 0$ und $\mathrm{char}(R)$ ist keine Primzahl.
Da R Integritätsbereich ist ist $1_R \neq 0_R$ also $\mathrm{char}(R) \neq 1$

$$\begin{aligned}
&\implies \exists a, b \in \mathbb{N}, 1 < a, b < \mathrm{char}(R) : \mathrm{char}(R) = ab \\
&\implies 0_R = \sum_{k=1}^{\mathrm{char}(R)} 1_R = \sum_{k=1}^{a} 1_R \cdot \sum_{k=1}^{b} 1_R \\
&\xRightarrow{R \text{ Integritätsbereich}} \sum_{k=1}^{a} 1_R = 0_R \vee \sum_{k=1}^{b} = 0_R \\
&\implies \mathrm{char}(R) \leq a \vee \mathrm{char}(R) \leq b\text{` zu } a, b < \mathrm{char}(R)
\end{aligned}$$

□

Bemerkung 3.3 K Körper, dann ist $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K)$ ist Primzahl.

Beweis Folgt aus 3.2 und 3.3.2 □

Beispiel 3.4 p Primzahl, dann ist $\mathrm{char}(\mathbb{F}_{\shortmid}) = p$

4 Polynome

Definition 4.1 (7.1 Polynome) K Körper, ein Polynom in der Variablen t über K ist ein Ausdruck der Form

$$f = \sum_{k=0}^{n} a_k t^k$$

mit $n \in \mathbb{N}_0$ (das heißt insbesondere nur endliche Summanden), $a_0, \ldots, a_n \in K$ (fehlende $a = 0$, ebenso setzen wir $a_{k>n} = 0$). Die a_k heißen die Koeffizienten von f

$$\deg(f) := \begin{cases} -\infty & f = 0 \\ \max\{k \in \mathbb{N}_0 \mid a_k \neq 0\} & f \neq 0 \end{cases}$$

heißt Grad von f. für $f \neq 0$ heißt $l(f) := a_{\deg(f)}$ heißt der Leitkoeffizient von f, $l(0) := 0$. f heißt normiert $\overset{\text{Def}}{\iff} l(f) = 1$ Hierbei sind zwei Polynome $f = \sum_{k=0}^{n} a_k t^k, g = \sum_{k=0}^{m} b_m t^k$ gleich ($f = g$) $\overset{\text{Def}}{\iff} \deg(f) = \deg(g) =: r$ und $a_r = b_r, \ldots, a_1 = b_1, a_0 = b_0$

Bemerkung 4.2 Man kann das auch präzise machen (Algebra 1, WS15/16, Blatt 5, Aufgabe 3)

Beispiel 4.3 (7.2)

1. $f = \frac{3}{4}x^2 - 7x + \frac{1}{2} \in \mathbb{Q}[x] \implies \deg(f) = 2, l(f) = \frac{3}{4}$, f ist nicht normiert
2. $f = x^5 - \frac{1}{3}x + \frac{2}{5} \in \mathbb{Q}[x] \implies \deg(f) = 5, l(f) = 1$, f ist normiert

Bemerkung 4.4 (7.3) K Körper, $f, g \in K[t], f = \sum_{k=0}^{n} a_k t^k, g = \sum_{k=0}^{m} b_k t^k$. Wir setzen $r := \max\{m, n\}$ und definieren

$$\begin{aligned}
f + g &= (a_r + b_r)t^r + \ldots + (a_1 + b_1)t + (a_0 + b_0) \\
f \cdot g &= c_{n+m}t^{n+m} + \ldots + c_1 t + c_0, c_k := \sum_{\substack{i,j \in \mathbb{N}_0 \\ i+j=k}} a_i b_j
\end{aligned}$$

Mittels der Verknüpfung $+, \cdot$ wir die Menge aller Polynome über K in der Variablen $t (=: K[t])$ zu einem kommutativen Ring, dem Polynomring über K in der Variablen t

Beweis Man rechnet die Ringaxiome nach □

Bemerkung 4.5 (7.4) K Körper, $f, g \in K[t]$, Dann gilt:

1. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(fg) = \deg(f) + \deg(g)$

(Hierbei setzt man Formel für $n \in \mathbb{N}_0 : -\infty < n, n + (-\infty) = -\infty = (-\infty) + n, (-\infty) + -(\infty) = -\infty$)

Beweis Falls $f = 0$ oder $g = 0$, dann sind 1. und 2. klar. Im Folgenden seien $f, g \neq 0$, etwa $f = \sum_{k=0}^{n} a_k t^k, g = \sum_{k=0}^{m} b_k t^k$ mit $a_n, b_m \neq 0$ (insbesondere $\deg(f) = n, \deg(g) = m$)

1. Wir setzen $k := \max\{m, n\}$

$$\Longrightarrow f + g = (a_k + b_k)t^k + \ldots + (a_1 + b_1)t + (a_0 + b_0)$$
$$\Longrightarrow \deg(f+g) \leq k \qquad \text{(beachte: Es könnte } a_k + b_k = 0 \text{ sein)}$$

2. Es sei $fg = a_n b_m t^{n+m} + \ldots + a_0 b_0$ und es ist $a_n b_m \neq 0$ da K als Körper ein Integritätsbereich ist $\Longrightarrow \deg(fg) = n + m$ □

Folgerung 4.6 (7.5) K Körper, dann ist $K[t]$ ein Integritätsbereich

Beweis $K[t] \neq 0$ klar (zum Beispiel $t \in \approx$) Seien $f, g \in K[t], f, g \neq 0 \implies \deg(f), \deg(g) \geq 0 \implies \deg(fg) = \deg(f) + \deg(g) \geq 0 \implies fg \neq 0$ □

Bemerkung 4.7 $K[t]$ ist kein Körper: Das Polynom $t \in K[t]$ besitzt kein Inverses bezüglich „$\cdot$", denn:
Wäre $f \in K[t]$ invers zu t, dann wäre $ft = 0 \implies \deg(1) = 0 \deg(ft) = \deg(f) + \deg(t) = \deg(f) + 1 \implies \deg(f) = -1$`

Satz 4.8 (7.6 Polynomdivision) K Körper, $f, g \in K[t], g \neq 0$
Dann existieren eindeutig bestimmte Polynome $q, r \in K[t]$, mit $f = qg + r$ und $\deg(r) < \deg(g)$

Beispiel 4.9 (7.7) $f = 3t^3 + 5t + 1, g = t^2 + 1 \in \mathbb{Q}[t]$

$$\left(3t^3 + 5t + 1\right) : \left(t^2 + 1\right) = 3t$$

Also $3t^3 + 5t + 1 = 3^t\left(t^2 + 1\right) + 2t + 1, q = 3t, r = 2t + 1$

Beweis 1. Existenz:
Falls $f = 0$, setzen wir $q := 0, r := 0$ fertig.
Im Folgenden sei $f \neq 0$, das Polynom g sei fixiert. Wir zeigen die Existenz von q, r per Induktion nach $\deg(f) \in \mathbb{N}_0$

- Induktionsanfang: (etwas unkonventionell, geht aber auch): $\deg(f) \in \{0, \ldots, \deg(g) - 1\}$ (das heißt $\deg(f) < \deg(g)$)
  Setze $q := 0, r := g$, dann ist $f = qg + r, \deg(r) = \deg(f) < \deg(g)$.
- Induktionsschritt: Es sei $\deg(f) \geq \deg(g)$ und die Behauptung sei für alle Polynome aus $K[t]$ von Grad < $\deg(f)$ schon gezeigt.
  Wir setzen $n := \deg(f), m := \deg(g)$ und schreiben:

$$f = l(f)t^n + \text{ Terme kleineren Grades}$$

$$g = l(g)t^m + \text{ Terme kleineren Grades}$$

Es ist $f - \frac{l(f)}{l(g)}t^{n-m}g =$

$$l(f)t^n + \text{ Terme kleineren Grades} - \underbrace{\frac{l(f)}{l(g)}t^{n-m}l(g)t^m}_{l(f)t^n} + \text{Terme kleineren Grades}$$

$$\implies \deg\left(f - \frac{l(f)}{l(g)}t^{n-m}\right) < n$$

Nach Induktionsannahme gilt: Es existiert $q_1, r_1 \in K[t]$ mit

$$f - \frac{l(f)}{l(g)}t^{n-m}g = q_1 g + r_1, \text{ mit } \deg r_1 < \deg(g)$$

$$\to f = \left(q_1 + \frac{l(f)}{l(g)}t^{n-1}\right)g + r_1$$

Setze $q := q_1 + \frac{l(f)}{l(g)}t^{n-m}, r := r_1$, dann ist $f = qg + r$ und $\deg(r) < \deg(g)$

2. Eindeutigkeit: Seien $q_1, q_2, r_1, r_2 \in K[T]$ mit $f = q_1 g + r_1 + q_2 g + r_2$ und $\deg(r_1) < \deg(g), \deg(r_2) < \deg(g)$

$$\begin{aligned} &\implies (q_1 - q_2)g = r_2 - r_1 \\ &\implies \deg(g_1 - q_2) + \deg(g) = \deg(r_1 - r_2) \end{aligned}$$

Falls $q_1 \neq q_2$, dann sind beide Seiten der Gleichung in $\mathbb{N}_0$ und es wäre

$$\deg(g) \leq \deg(r_2 - r_1)$$

Nach 4.5 ist $\deg(r_2 - r_1) \leq \max\{\deg(r_2), \deg(-r_1)\} < \deg(g)$` Also $q_1 = q_2$, somit $r_2 - r_1 = \underbrace{q_1 - q_2}_{=0} g = 0$, also $r_1 = r_2$ □

Definition 4.10 (7.8, Nullstelle) $\in K[t], f = a_n t^n + \ldots + a_1 t + a_0, \lambda \in K$
Wir setzen $f(\lambda) := a_n \lambda^n + \ldots + a_1 \lambda + a_0 \in K$ λ heißt Nullstelle von $f \overset{Def.}{\iff} f(\lambda) = 0$

Bemerkung 4.11 (7.9) K Körper, $f \in K[t], \lambda \in K$ Nullstelle von f. Dann gibt es in $K[t]$ ein eindeutig bestimmtes Polynom q mit $f = (t - \lambda)q$. Es ist $\deg(q) = \deg(f) - 1$

Beweis Existenz: Nach 4.8 existiert $q, r \in K[t]$ mit $f = (t - \lambda)q + r$ und $\deg(r) < \underbrace{\deg(t - \lambda)}_{=1}$

$\implies r$ ist konstantes Polynom und es gilt

$$0 = f(\lambda) = \underbrace{(\lambda - \lambda)}_{=0} q + r(\lambda) = r(\lambda) \implies r = 0 \implies f = (t - \lambda)q$$

Eindeutigkeit: aus Eindeutigkeit aus 4.8 □

Folgerung 4.12 K Körper, $f \in K[t], f \neq 0, n := \deg(f)$
Dann besitzt f in K höchstens n Nullstellen.

Beweis per Induktion nach n **Induktionsanfang:** $n = 0$ Ein konstantes Polynom $\neq 0$ besitzt keine Nullstellen.
Induktionsschritt: Es sein $n > 0$ und die Aussage sei für alle Polynome von Grad $< n$ schon gezeigt. Falls f keine Nullstelle besitzt, dann fertig. Im Folgenden besitze f eine Nullstelle sei $\lambda \in K$ eine solche, daraus folgt mit 4.11

$$\exists q \in K[t] : f(t-\lambda)q, \deg q = n-1$$

Ist $\varepsilon \neq \lambda$ eine weitere Nullstelle von f dann ist

$$0 = f(\varepsilon) = \underbrace{\varepsilon - \lambda}_{\neq 0} q(\varepsilon)$$

Da K als Körper ein Integritätsbereich ist folgt: $q(\varepsilon) = 0$, das heißt ε ist Nullstelle von q. Nach Induktionsvoraussetzung hat q höchstens $n-1$ Nullstellen $\implies$ f hat höchstens n Nullstellen □

Definition 4.13 (7.11) K Körper, $f \in K[t], f \neq 0, \lambda \in K$

$$\mu(f,\lambda) := \max\{e \in \mathbb{N}_0 \mid \exists\, g \in K[t] : f = (t-\lambda)^e g\}$$

heißt die Vielfachheit der Nullstelle λ von f.

Bemerkung 4.14

- Es ist $\mu(f,\lambda) = 0 \iff f(\lambda) \neq 0 \lambda$ keine Nullstelle von f (denn: $f(\lambda) = 0 \iff \exists\, q \in K[t] : f = (t-\lambda)q \iff \mu(f,\lambda) \neq 0$)
- Die Vielfachheit von λ gibt an, wie oft der Linearfaktor $t-\lambda$ in f vorkommt
- Sind $\lambda_1, \ldots, \lambda_m \in K$ sämtliche verschiedene Nullstellen von f und es ist $e_i := \mu(f,\lambda_i), i = 1,\ldots,m$ dann existiert ein Polynom $g \in K[t]$ mit

  $$f = (t-\lambda_1)^{e_1} \cdot \ldots \cdot (t-\lambda_m)^{e_m} g$$

  und den Eigenschaften, dass g in K kein Nullstelle besitzt und, dass $\deg(g) = \deg(f) - (e_1 + \ldots + e_m)$.
- „bester Fall:“ $\deg(g) = 0$ („f zerfällt in Linearfaktoren“): Dann existiert $a \in K \setminus \{0\}, \lambda_1, \ldots, \lambda_m \in k$ paarweise verschieden, $e_1, \ldots, e_n \in \mathbb{N}$ mit

  $$f = a(t-\lambda_1)^{e_1} \cdot \ldots \cdot (t-\lambda_m)^{e_m}, e_1 + \ldots + e_m = \deg(f)$$

  Alternative Darstellung:

  $$f = a\Big(t - \tilde{\lambda}_1\Big) \cdot \ldots \cdot \Big(t - \tilde{\lambda}_n\Big), n = \deg(f), \tilde{\lambda}_1, \ldots \tilde{\lambda}_n \text{ nicht notwendig verschieden}$$

Satz 4.15 (7.12 Fundamentalsatz der Algebra) Jedes Polynom $f \in \mathbb{C}[t]$ mit $\deg(f) \geq 1$ besitzt eine Nullstelle.

Beweis Zum Beispiel in Vorlesung Funktionentheorie 1, Algebra 1 □

Folgerung 4.16 (7.13) $f \in \mathbb{C}[t], f \neq 0$ Dann zerfällt f in Linearfaktoren.

Beweis **Induktionsanfang:** $n = 0 \implies f$ ist konstantes Polynom, fertig
Induktionsschritt: Sei $n \geq 1$ und die Aussage sei für alle Polynome vom Grad $< n$ bereits bewiesen. Nach Fundamentalsatz der Algebra existiert eine Nullstelle λ von f

$$\overset{4.11}{\implies} \exists\, g \in \mathbb{C}[t] : f = (t-\lambda)g, \deg(g) = n-1$$

Nach Induktionsannahme $\exists\, a \in \mathbb{C}, \lambda_1, \ldots, \lambda_{n-1} \in \mathbb{C}$ (nicht notwendig verschieden)

$$g = a(t-\lambda_1) \cdot \ldots \cdot (t-\lambda_{n-1})$$

Setze $\lambda_n := x \implies f = g(t-\lambda_n) = a(t-\lambda_1) \cdot \ldots \cdot (t-\lambda_{n-1})(t-\lambda_n)$ □

Definition 4.17 (7.14) K Körper, $f \in K[t]$ f induziert eine Abbildung $\tilde{f} : K \to K, \lambda \to f(\lambda)$, $\tilde{f}$ heißt die Polynomfunktion zum Polynom f

Beispiel 4.18 (7.15) Es ist wichtig zwischen dem Polynom $f \in K[t]$ und der dazugehörigen Polynomfunktion $\tilde{f} : K \to K$ zu unterscheiden Sei $f = t^2 + t \in \mathbb{F}_2[t]$. Dann ist $f(\bar{0}) = \bar{0}^2 + \bar{0} = \bar{0}, f(\bar{1}) = \bar{1}^2 + \bar{1} = \bar{0}$ das heißt $\tilde{f} : \mathbb{F}_2 \to \mathbb{F}_2$ ist die Nullabbildung, aber f ist nicht das Nullpolynom

Bemerkung 4.19 (7.16) K Körper mit unendlich vielen Elementen.
Dann ist die Abbildung $\tilde{}: K[t] \to \text{Abb}(K, K) := \{g : K \to K \text{ Abbildung}\}, f \mapsto \tilde{f}$ injektiv, das heißt: Ist K unendlich und sind $f_1, f_2 \in K[t]$, dann gilt $f_1 = f_2 \iff \tilde{f}_1 = \tilde{f}_2$

Beweis Es seien $f_1, f_2 \in K[t]$ mit $\tilde{f}_1 = \tilde{f}_2$ wir setzen $g := f_1 - f_2$
$\implies$ Für alle $a \in K$ ist $g(a) = (f_1 - f_2)(a) = f_1(a) - f_2(a) = \tilde{f}_1(a) - \tilde{f}_2(a) = 0 \xRightarrow{K \text{ unendlich}}$ g hat unendlich viele Nullstellen, mit 4.13 folgt: $g = 0 \implies f_1 = f_2$ □

Bemerkung 4.20
- Lässt man 4.19 die Voraussetzung K hat unendlich viele Elemente weg, wird die Aussage falsch, siehe Beispiel 4.18
- Mit dem Wissen von 4.18 und 4.19 im Hintergrund bezeichnet man die vom Polynom f induzierte Polynomfunktion mit f anstelle von $\tilde{f}$

5 Vektorräume

In diesem Kapitel sei K stets ein Körper

Definition 5.1 (8.1) Ein K-Vektorraum ist ein Tripel $(V, +, \cdot)$ bestehend aus

- einer Menge V
- einer Verknüpfung $+ : V \times V \to V, (v, w) \mapsto v + w$ (Addition)
- und einer äußeren Verknüpfung $\cdot : K \times V \to V, (\lambda, v) \mapsto \lambda \cdot v$ (skalare Multiplikation)

Welche folgende Bedingungen genügen:

1. (V1) $(V, +)$ ist eine abelsche Gruppe
2. (V2) Die skalare Multiplikation ist in folgender Weise mit der anderen Verknüpfung (auf V und K) verträglich:

$\forall\, \lambda, \mu \in K, v, w \in V$

$$\begin{aligned} (\lambda + \mu) \cdot v &= \lambda \cdot v + \mu \cdot v \\ \lambda \cdot (v + w) &= \lambda \cdot v + \lambda \cdot w \\ \lambda \cdot (\mu \cdot w) &= (\lambda \cdot \mu) \cdot v \\ 1 \cdot v &= v \end{aligned}$$

Bemerkung 5.2
- Es ist wichtig, zwischen Addition „+“ und skalarer Multiplikation „·“ auf V und Addition und Multiplikation in K zu unterschieden: In der Gleichung $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ sind die Verknüpfungen wie folgt zu verstehen:

$$\left(\lambda \underset{\text{Addition in } K}{\underset{\downarrow}{+}} \mu\right) \overset{\text{skalare Multiplikation}}{\overset{\uparrow}{\cdot}} v = \lambda \underset{\text{skal. Mult.}}{\underset{\downarrow}{\cdot}} v \overset{\text{Addition in } V}{\overset{\uparrow}{+}} \mu \underset{\text{skal. Mult.}}{\underset{\downarrow}{\cdot}} v$$

- Das neutrale Element bezüglich „+“ auf V bezeichnen wir mit 0_v (Nullvektor), das inverse zu $v \in V$ bezüglich „+“ mit $-v$. Das Zeichen „·“ für die skalare Multiplikation lassen wir ab jetzt meistens weg und schreiben λv statt $\lambda \cdot v$ ($\forall\, \lambda \in K, v \in V$)
- Wir schreiben meist verkürzend „V K-Vektorraum“ (beziehungsweise: „V K-VR“) anstelle von $(V, +, \cdot)$ K-Vektorraum.

Beispiel 5.3 (8.2)

1.
$$K^n := \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in K\}$$
mit
$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n)$$
$$\lambda \cdot (x_1, \dots, x_1) := (\lambda x_1, \dots, \lambda x_n)$$
$$\lambda \in K, (x_1, \dots, x_n), (y_1, \dots, y_n) \in K^n$$
ist ein K-Vektorraum, der so genannte Standardvektorraum über K Die Axiome rechnet man nach, exemplarisch: sind $\lambda, \mu \in K, (x_1, \dots, x_n) \in K^n$, dann ist
$$(\lambda + \mu) \cdot (x - 1, \dots, x_n) = ((\lambda + \mu)x_1, \dots, (\lambda + \mu)x_n)$$
Mit dem Distributivgesetz in K folgt:
$$(\lambda x_1, \dots, \lambda x_n) + (\mu x_1, \dots, \mu x_n) = \lambda(x_1, \dots, x_n) + \mu(x_1, \dots, x_n)$$
Der Nullvektor ist gegeben durch $0_{K^n} = (0, \dots, 0)$, für $x = (x_1, \dots, x_n)$ ist $-x = (-x_1, \dots, -x_n)$
2. $\mathbb{C}$ ist ein $\mathbb{R}$ -VR bezüglich
   - $+$ = übliche Addition auf $\mathbb{C}$
   - skalare Multiplikation $\cdot : \mathbb{R} \times \mathbb{C} \to \mathbb{C}, \lambda(a + \imath b) := \lambda a + \imath \lambda b$
3. $K[t]$ Polynomring über K in der Variablen t wird zum K -VR durch
   - $+$ = Addition von Polynomen
   - skalare Multiplikation, $\cdot : K \times K[t] \to K[t] : \lambda \cdot \sum_{k=0}^{n} a_k t^k := \sum_{k=0}^{n} \lambda a_k t^k$
4. M Menge, $\mathrm{Abb}(M, K) := \{f : M \to K$ Abbildung$\}$ wird zum K -Vektorraum durch die folgende Verknüpfungen:
   - Addition: Zu $f, g \in \mathrm{Abb}(M, K)$ wird $f + g : M \to K$ definiert über
   $$(f + g)(x) := f(x) + g(x), x \in M$$
   - skalare Multiplikation: Zu $\lambda \in K, f \in \mathrm{Abb}(M, K)$ wird $\lambda f : M \to K$ definiert über
   $$(\lambda f)(x) := \lambda f(x), x \in M$$

   („punktweise Addition und skalare Multiplikation“)

Bemerkung 5.4 (8.3) V K -VR. Dann gilt:

1. $0_K \cdot v = 0_V \,\forall\, v \in V$

2. $\lambda \cdot 0_V = 0_V \, \forall \lambda \in K$

3. $\lambda v = 0_V \implies \lambda = 0_K \vee v = 0_V$

4. $(-1_K) \cdot v = -v \, \forall v \in V$

Beweis 1. Sei $v \in V$

$$\implies 0_V + 0_K \cdot v = 0_K \cdot v = (0_K + 0_K) \cdot v = 0_K \cdot v + 0_K \cdot v \implies 0_K \cdot v = 0_V$$

2. Sei $\lambda \in K$

$$\implies \lambda \cdot 0_V + 0_V = \lambda \cdot 0_V = \lambda \cdot (0_V + 0_V) = \lambda \cdot 0_V + \lambda \cdot 0_V \implies \lambda \cdot 0_V = 0_V$$

3. Seien $\lambda \in K, v \in V, \lambda \cdot v = 0$. Falls $\lambda \neq 0_K$:

$$v = 1_K \cdot v = \left(\lambda^{-1}\lambda\right) \cdot v = \lambda^{-1} \cdot \underbrace{(\lambda v)}_{=0_V} = \lambda^{-1} \cdot 0_V = 0_V$$

4. Für $v \in V$ ist

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

□

Definition 5.5 (8.4) V K -VR, $U \subseteq V$
U heißt Untervektorraum (K -Untervektorraum), kurz UVR von $V \overset{\text{Def}}{\iff}$ Die folgenden Bedingungen sind erfüllt

- (U1) $U \neq \emptyset$
- (U2) $v, w \in U \implies v + w \in U$ (das heißt U ist abgeschlossen bezüglich Addition)
- (U3) $v \in U, \lambda \in K \implies \lambda v \in U$ (das heißt U ist abgeschlossen bezüglich skalarer Multiplikation)

Bemerkung 5.6 (8.5) V K -VR, $U \subseteq V$
Dann sind äquivalent

1. U ist ein UVR von V
2. Addition und skalare Multiplikation auf V induzieren durch Einschränkung auf U Verknüpfung $+ : U \times U \to U, \cdot : K \times U \to U$, und bezüglich dieser Verknüpfung ist U ein K -VR

Beweis (1.) $\implies$ (2.): Sei U ein UVR von V

1. Die Verknüpfung $+ : U \times U \to U, \cdot : K \times U \to U$ sind wohldefiniert wegen (U2), (U3)
2. (V1) gilt (das heißt $(U, +)$ ist eine abelsche Gruppe), denn:
   - Assoziativgesetz, Kommutativgesetz bezüglich „+“ gelten, weil sie schon in V gelten.
   - 0_V ist neutral bezüglich „+“ und liegt in U, denn wegen $U \neq \emptyset$ existiert ein $u \in U$, wegen (U3) ist dann auch $\underbrace{0_K \cdot u}_{=0_V} \in U$, also $0_V \in U$
   - $-u$ ist invers zu u und liegt in U, denn: Mit $u \in U$ ist nach (U3) auch $(-1_K) \cdot u$ in U

3. (V2) gilt, da es schon in V gilt

(2.) $\implies$ (1.) Es gelte (2.)

- (U1): $U \neq \emptyset$, denn U ist abelsche Gruppe bezüglich der eingeschränkten Addition
- (U2),(U3): folgt direkt aus der Wohldefiniertheit der Verknüpfung $+ : U \times U \to Z, \cdot : K \times U \to U$ $\square$

Bemerkung 5.7
- der Beweis von (1.) $\implies$ (2.) hat gezeigt: Ist $U \subseteq V$ ein UVR, dann ist $0_V \in U$
- Ab jetzt lassen wir bei 0_V beziehungsweise 0_K meist die Indizes V beziehungsweise K weg und schreiben für beide kurz 0.

Beispiel 5.8 (8.6)

1. $K = \mathbb{R}, V = \mathbb{R}^2$
   Es sei $U = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 - 2x_2 = 0\}$
   - (U1): $(0,0) \in U$ also $U \neq \emptyset$
   - (U2): Es seien $(x_1, x_2) \in U, (y_1, y_2) \in U \implies x_1 - 2x_2 = 0, y_1 - 2y_2 = 0$
     $$\implies (x_1 + y_1) - 2(x_2 + y_2) = 0 \implies (x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \in U$$
   - (U3): Sei $(x_1, x_2) \in U, \lambda \in \mathbb{R} \implies x_1 - 2x_2 = 0 \implies \lambda x_1 - 2\lambda x_2 = 0$
     $$(\lambda x_1, \lambda x_2) = \lambda(x_1, x_2) \in U$$

   Also: U ist ein UVR von $V = \mathbb{R}^2$
2. $K = \mathbb{R}, V = \mathbb{R}$
   Es sei $U = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 - 2x_2 = 1\}$
   Es ist $(0,0) (= 0_V) \notin U \implies U$ ist kein UVR von $V = \mathbb{R}^2$
3. $K = \mathbb{R}, V = \mathbb{R}^{\nvDash}$
   Es sei $U = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 \geq 0 \wedge x_2 \geq 0\}$
   U ist kein UVR von V, denn: $(5,2) \in U$, aber $(-1) \cdot (5,2) = (-5,-2) \notin U$
4. $V = K[t]$
   Es sei $U = \{f \in K[t] \mid \deg f \leq 2\} = \{f \in K[t] \mid \exists\, a_0, a_1, a_2 \in K : f = a_2 t^2 + a_1 t + a_0\}$
   - (U1): $0 \in U$, also $U \neq \emptyset$
   - (U2): Es seien $f, g \in U \implies \deg(f) \leq 2, \deg(g) \leq 2 \implies \deg(f+g) \leq 2 \implies f + g \in U$
   - (U3): Es sei $f \in U, \lambda \in K \implies \deg(f) \leq 2 \implies \deg(\lambda f) \leq 2 \implies \lambda f \in U$

   Also U ist ein UVR von V
5. V K-VR. Dann sind $\{0\}, V$ UVR von V („triviale UVR“), $\{0\}$ heißt Nullvektorraum (Nullraum)

Bemerkung 5.9 (8.7) V K-VR, I Indexmenge, $(U_i)_{i \in I}$ Familie von UVR von V (das heißt für jedes $i \in I$ ist ein UVR U_i von V gegeben) Dann gilt:
$$U := \bigcap_{i \in I} U_i$$
ist ein UVR von V. Mit anderen Worten: der Durchschnitt von UVR von V ist wieder ein UVR von V

Beweis 1. (U1): $U \neq \emptyset$, denn $0 \in U_i \,\forall\, i \in I$, also $0 \in U$

2. (U2): Seien $v, w \in U \implies \forall\, i \in I : v \in U_i, w \in U_i \implies \forall\, i \in I : v + w \in U_i \implies v + w \in U$

3. (U3): Sei $v \in U, \lambda \in K \implies \forall\, i \in I : v \in U_i \implies \forall\, i \in I : \lambda v \in U_i \implies \lambda v \in \bigcap_{i \in I} U_i = U$ □

Beispiel 5.10 (8.8) Die Vereinigung von UVR ist im Allgemeinen kein UVR, zum Beispiel $K = \mathbb{R}, V = \mathbb{R}^2$

- $U_1 = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 = x_2\}$
- $U_2 = \{(x_1, x_2) \in \mathbb{R}^2 \mid 2x_1 = x_2\}$

Aber: $U_1 \cup U_2$ ist kein UVR von $\mathbb{R}^2$, denn

$$(1,1) \in U_1 \subseteq U_1 \cup U_2, (2,4) \in U_2 \subseteq U_1 \cup U_2$$

aber: $(1,1) + (2,4) = (3,5) \notin U_1 \cup U_2$

Definition 5.11 (8.9) V K-VR, $(v_1, \dots, v_r)$ endliche Familie von Vektoren aus V

$$\mathrm{Lin}((v_1, \dots, v_r)) := \{\alpha_1 v_1 + \ldots + \alpha_r v_r \mid \alpha_1, \dots, \alpha_r \in K\}$$

heißt die Lineare Hülle (das Erzeugnis) der Familie $v_1, \dots, v_r$
$v \in V$ heißt Linearkombination von $v_1, \dots, v_r$

$$\overset{\text{Def}}{\iff} v \in \mathrm{Lin}((v_1, \dots, v_r)) \iff \exists\, \alpha_1, \dots \alpha_r \in K : v = \alpha_1 v_1 + \ldots + \alpha_r v_r$$

Bemerkung 5.12 Andere Notation für Lin : $\mathrm{span}(\ldots), < \ldots >$

Beispiel 5.13 (8.10)

1. $V = \mathbb{R}^3, K = \mathbb{R}$
   - $v \in V, v \neq 0 \implies \mathrm{Lin}((v)) = \{\alpha v \mid \alpha \mathbb{R}\}$ = Gerade durch 0 und v
   - $$v, w \in V, v \neq 0 \implies \mathrm{Lin}((v, w)) = \{\alpha_1 v + \alpha_2 w \mid \alpha_1, \alpha_2 \in \mathbb{R}\} = \begin{cases} \text{Gerade durch } 0 & w \in \mathrm{Lin}((v)) \\ \text{Ebene durch } 0, v, w & w \notin \mathrm{Lin}((v)) \end{cases}$$

2. $V = K^n$ als K-VR

$$e_i := \begin{pmatrix} 0, \dots, 0, 1, 0, \dots, 0 \\ \downarrow \\ \text{i-te Stelle} \end{pmatrix}$$

$$\begin{aligned} \mathrm{Lin}((e_1, \dots, e_n)) &= \{\alpha_1 e_1 + \ldots \alpha_n e_n \mid \alpha_1, \dots, \alpha_n \in K\} \\ &= \{(\alpha_1, 0, \dots, 0) + (0, \alpha_2, 0, \dots, 0) + \ldots + (0, \dots, 0, \alpha_n) \mid \alpha_1, \dots, \alpha_n \in K\} \\ &= \{(\alpha_1, \dots, \alpha_n) \mid \alpha_1, \dots, \alpha_n \in K\} \\ &= K^n \end{aligned}$$

Definition 5.14 (8.11) V K-VR, $(v_i)_{i\in I}$ Familie von Vektoren aus V

$$\mathrm{Lin}\big((v_i)_{i\in I}\big) := \{\sum_{i\in I} \alpha_i v_i \mid \alpha_i \in K \,\forall\, i \in I, \alpha_i = 0 \text{ für fast alle } i \in I\}$$

heißt die lineare Hülle (das Erzeugnis) der Familie $(v_i)_{i\in I}$. Hierbei bedeutet „$\alpha_i = 0$ für fast alle $i \in I$": Es gibt nur endlich viele $i \in I$ mit $\alpha_i \neq 0$, das heißt die auftretenden Summen sind endliche Summen. Falls $I = \emptyset$ setzen wir $\mathrm{Lin}\big((v_i)_{i\in\emptyset}\big) := \{0\}$

Bemerkung 5.15 Ein Element $v \in V$ ist genau dann in $\mathrm{Lin}\big((v_i)_{i\in I}\big)$ enthalten, wenn es eine endliche Teilmenge $\{i_1, \dots, i_r\} \subseteq I$ und Elemente $\alpha_{i_1}, \dots, \alpha_{i_r} \in K$ gibt mit

$$v = \alpha_{i_1} v_{i_1} + \ldots + \alpha_{i_r} v_{i_r}$$

Insbesondere ist mit $\mathrm{Lin}\big((v_i)_{i\in I}\big) = \bigcup_{J\subseteq I} \mathrm{Lin}\big((v_i)_{i\in J}\big)$

Beispiel 5.16 (8.12) $V = K[t]$ als K-VR
Es ist

$$\mathrm{Lin}\big((t^n)_{n\in\mathbb{N}_0}\big) = \{\sum_{i\in\mathbb{N}_0} \alpha_i t^i \mid \alpha_i \in K, \alpha_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\} = K[t]$$

Bemerkung 5.17 (8.13) V K-VR, $(v_i)_{i\in I}$ Familie von Vektoren aus V. Dann gilt:

1. $\mathrm{Lin}\big((v_i)_{i\in I}\big)$ ist ein UVR von V
2. Ist $U \subseteq V$ ein UVR mit $v_i \in U \,\forall\, i \in I$, dann ist $\mathrm{Lin}\big((v_i)_{i\in I}\big) \subseteq U$ das heißt $\mathrm{Lin}\big((v_i)_{i\in I}\big)$ ist das bezüglich „$\subseteq$" kleinste Element der Menge derjenigen UVR von V die alle $v_i, i \in I$ enthalten
3. $$\mathrm{Lin}\big((v_i)_{i\in I}\big) = \bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U \,\forall\, i \in I} U$$

Beweis Falls $I = \emptyset$, dann $\mathrm{Lin}\big((v_i)_{i\in I}\big) = \{0\}$, dann 1. klar, und jeder UVR U von V enthält alle $v_i, i \in \emptyset$, und enthält $\{0\} \implies$ 2. Außerdem

$$\bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U \,\forall\, i \in I} U = \bigcap_{U \text{ UVR von } V} U = \{0\} = \mathrm{Lin}\big((v_i)_{i\in\emptyset}\big)$$

es folgt 3.

Im Folgenden sie $I \neq \emptyset$. Wir setzen $W := \mathrm{Lin}\big((v_i)_{i\in I}\big)$

1.
   - (U1): Sei $i \in I$ (Existenz wegen $I \neq \emptyset$). Dann ist $0 \cdot v_i = 0 \in W$, insbesondere $W \neq \emptyset$
   - (U2): Es seinen $v, w \in W$

     $$\implies \exists\, r \in \mathbb{N}, \{i_1, \dots, i_r\} \subseteq I, \alpha_{i_1}, \dots, \alpha_{i_r} \in K, \text{ mit } v = \alpha_{i_1} v_{i_1} + \ldots + \alpha_{i_r} v_{i_r}$$

     sowie

     $$s \in \mathbb{N}, \{j_1, \dots, j_r\} \subseteq I, \beta_{j_1}, \dots, \beta_{j_r} \in K, \text{ mit } w = \beta_{j_1} v_{j_1} + \ldots + \beta_{j_r} v_{j_r}$$
     $$\implies v + w = \alpha_{i_1} v_{i_1} + \ldots + \alpha_{i_r} v_{i_r} + \beta_{j_1} v_{j_1} + \ldots + \beta_{j_s} v_{j_s} \in W$$

   - (U3): Für $\lambda \in K, v \in W$ wie bei (U2) ist

     $$\lambda v = \lambda \alpha_{i_1} v_{i_1} + \ldots + \lambda \alpha_{i_r} v_{i_r} \in W$$

2. Sei $U \subseteq V$ UVR mit $v_i \in U \,\forall\, i \in I$
$\implies$ Jedes Element der Form $\sum_{i \in I} \alpha_i v_i$ mit $\alpha_i \in K \,\forall\, i \in I, \alpha_i = 0$ für fast alle $i \in I$, liegt in U.
$\implies \operatorname{Lin}\big((v_i)_{i \in I}\big) = W \subseteq U$.

3. zu zeigen:
$$\operatorname{Lin}\big((v_i)_{i \in I}\big) = \bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U \,\forall\, i \in I} U$$
„$\subseteq$" Wegen 2. liegt $\operatorname{Lin}\big((v_i)_{i \in I}\big)$ in jedem UVR U von V, der alle $v_i, i \in I$ enthält
$$\implies \operatorname{Lin}\big((v_i)_{i \in I}\big) = \bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U \,\forall\, i \in I} U$$
„$\supseteq$" Nach 1. ist $W = \operatorname{Lin}\big((v_i)_{i \in I}\big)$ ist ein UVR von V mit $v_i \in W \,\forall\, i \in I$, das heißt W ist einer der UVR, über die der obige Durchschnitt gebildet wird
$$\implies \bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U \,\forall\, i \in I} U \subseteq W = \operatorname{Lin}\big((v_i)_{i \in I}\big)$$
□

Notation: Ist $M \subseteq V$, dann setzen wir $\operatorname{Lin}(M) := \operatorname{Lin}\big((m)_{m \in M}\big)$ (= kleinster UVR von V, der alle Elemente aus M enthält) Vorteil der Definition von $\operatorname{Lin}(\ldots)$ für Familien von Vektoren: Bei Familien ist es sinnvoll zu sagen, dass ein Vektor mehrfach vorkommt (im Gegensatz zu Mengen), darüber hinaus haben die Vektoren der Familie $(v_i)_{i \in I}$ im wichtigen Spezialfall $I = \{1, \ldots, n\}$, Familie $(v_1, \ldots, v_n)$ eine natürliche Reihenfolgen. Diese geht verloren, wenn man die Menge $\{v_1, \ldots, v_n\}$ betrachtet (zum Beispiel in $\mathbb{R}^2 : \{e_1, e_2\} = \{e_2, e_1\}$, aber $(e_1, e_2) \neq (e_2, e_1)$)

Definition 5.18 (8.14) V K-VR, $(v_1, \ldots, v_r)$ endliche Familie von Vektoren aus V, $(v_1, \ldots, v_r)$ **linear unabhängig**
$$\overset{\text{Def}}{\iff} \lambda_1, \ldots, \lambda_r \in K, \lambda_1 v_1 + \ldots + \lambda_r v_r = 0 \implies \lambda_1 = \ldots = \lambda_r = 0$$
Mit anderen Worten: Der Nullvektor lässt sich nur auf triviale Weise aus der Familie $(v_1, \ldots, v_r)$ linear kombinieren.
$(v_i)_{i \in I}$ heißt **linear abhängig** $\overset{\text{Def}}{\iff}$ $(v_1, \ldots, v_r)$ ist nicht linear unabhängig
$$\iff \exists\, \lambda_1, \ldots, \lambda_r \in K : (\lambda_1, \ldots, \lambda_r) \neq (0, \ldots, 0) \wedge \lambda_1 v_1 + \ldots + \lambda_r v_r = 0$$
$(v_i)_{i \in I}$ Familie von Vektoren aus V
$(v_i)_{i \in I}$ heißt linear unabhängig $\overset{\text{Def}}{\iff}$ Jede endliche Teilfamilie von $(v_i)_{i \in I}$ ist linear unabhängig, das heißt für jede endliche Teilmenge $J \subseteq I$ ist $(v_i)_{i \in I}$ linear unabhängig.
$(v_i)_{i \in I}$ heißt linear abhängig $\overset{\text{Def}}{\iff}$ $(v_i)_{i \in I}$ ist nicht linear unabhängig
$\iff$ $\exists$ eine endliche Teilfamilie $(v_i)_{i \in J}$ von $(v_i)_{i \in I}$, die linear abhängig ist
$\iff$ Es gibt eine endliche Teilmenge $J = \{i_1, \ldots, i_r\} \subseteq I, \lambda_{i_1}, \ldots, \lambda_{i_r} \in K$ mit
$$(\lambda_{i_1}, \ldots, \lambda_{i_r}) \neq (0, \ldots, 0) \wedge \lambda_{i_1} v_{i_1} + \ldots + \lambda_{i_r} v_{i_r} = 0$$
$M \subseteq V$ heißt linear (un-)abhängig $\iff$ $(m)_{m \in M}$ ist linear (un-)abhängig.

Bemerkung 5.19
- Man sagt häufig statt „$(v_1, \ldots, v_r)$ ist linear (un-)abhängig" auch „die Vektoren $v_1, \ldots, v_r$" sind linear (un-)abhängig.„
- Konvention: () ist linear unabhängig.

Beispiel 5.20 (8.15)

1. $V = K^n$ als K-VR
   Die Familie $(e_1, \ldots, e_n)$ (vgl 8.10) ist linear unabhängig, denn: Sind $\lambda_1, \ldots, \lambda_n \in K$ mit $\lambda_1 e_1 + \ldots + \lambda_n e_n = 0$, dann ist

$$\underbrace{\underbrace{\lambda_1(1,0,\ldots,0)}_{=(\lambda_1,0,\ldots,0)} + \underbrace{\lambda_2(0,1,0,\ldots,0)}_{=(0,\lambda_2,0,\ldots,0)} + \underbrace{\ldots + \lambda_n(0,\ldots,0,1)}_{=(0,\ldots,0,\lambda_n)}}_{=(\lambda_1,\ldots,\lambda_n)} = 0$$

   $\implies \lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$

2. $K = \mathbb{R}, V = \mathbb{R}^2$
   Die Familie $((1,-1),(0,2),(1,2))$ ist linear abhängig, denn:

$$2 \cdot (1,-1) + 3 \cdot (0,2) - 2 \cdot (1,2) = 0$$

   es gibt also eine nicht triviale Linearkombination der Null aus den Vektoren dieser Familie.

3. $V = K[t]$ als K-VR
   Die Familie $(t^n)_{n \in \mathbb{N}_0}$ ist linear unabhängig, denn:
   Sei $J = \{n_1, \ldots, n_r\} \subseteq \mathbb{N}_0$ eine endliche Teilmenge von $\mathbb{N}_0$, und sind $\lambda_{n_1}, \ldots, \lambda_{n_r} \in K$ dann folgt aus

$$\lambda_{n_1} t^{n_1} + \ldots + \lambda_{n_r} t^{n_r} = 0$$

   sofort: $\lambda_{n_1} = \ldots = \lambda_{n_r} = 0$ (vergleiche Definition von „=" von Polynomen) Also: Jede endliche Teilfamilie von $(t^n)_{n \in \mathbb{N}_0}$ ist linear unabhängig, also ist $(t^n)_{n \in \mathbb{N}_0}$ linear unabhängig.

Bemerkung 5.21 (8.16) V K-VR, $(v_i)_{i \in I}$ Familie von Vektoren aus V
Dann sind äquivalent:

1. $(v_i)_{i \in I}$ ist linear unabhängig
2. Jeder Vektor $v \in \operatorname{Lin}\big((v_i)_{i \in I}\big)$ lässt sich in eindeutiger Weise aus Vektoren deren Familie $(v_i)_{i \in I}$ linear kombinieren.

Beweis 1. $\implies$ 2.: Sei $(v_i)_{i \in I}$ linear unabhängig, $v \in \operatorname{Lin}\big((v_i)_{i \in I}\big) \implies \exists$ eine Familie $(\lambda_i)_{i \in I}$ von Elementen aus K mit $\lambda_i = 0$ für fast alle $i \in I$, sodass

$$v = \sum_{i=I} \lambda_i v_i$$

($\implies$ Existenz einer Linearkombination)
Es sei nun $(\mu_i)_{i \in I}$ eine weitere Familie von Elementen aus K mit $\mu_i = 0$ für fast alle $i \in I$ sodass

$$v = \sum_{i=I} \lambda_i v_i = \sum_{i \in I} \mu_i v_i$$

Wir setzen $J := \{i \in I \mid \lambda_i \neq 0\} \cup \{i \in I \mid \mu_i \neq 0\}$. Nach Konstruktion ist J endlich, und es ist

$$\underbrace{\sum_{i \in J} (\lambda_i - \mu_i) v_i}_{=\sum_{i \in I} (\lambda_i - \mu_i) v_i} = 0$$

Da $(v_i)_{i \in I}$ linear unabhängig, ist die endliche Teilfamilie $(v_i)_{i \in J}$ linear unabhängig $\implies \lambda_i - \mu_i = 0 \,\forall\, i \in J \implies \lambda_i = \mu_i \,\forall\, i \in J$ für $i \in J \setminus J$ ist ohnehin $\lambda_i = \mu_i = 0$

$$\implies \lambda_i = \mu_i \,\forall\, i \in I$$

2. $\Longrightarrow$ 1.: Wir setzen voraus, dass sich jeder Vektor $v \in \mathrm{Lin}\big((v_i)_{i\in I}\big)$ eindeutig aus Vektoren der Familie $(v_i)_{i\in I}$ linear kombinieren lässt.
zu zeigen: $(v_i)_{i\in I}$ ist linear unabhängig, das heißt jede endliche Teilfamilie $(v_i)_{i\in I}$ ist linear unabhängig denn: Sei $J \subseteq I$ endlich, und sei $(\lambda_i)_{i\in J}$ eine Familie von Elemente aus K mit
$$\sum_{i\in J} \lambda_i v_i = 0$$
Da auch
$$\sum_{i\in J} 0 \cdot v_i = 0$$
ist, folgt aus der vorausgesetzten Eindeutigkeit der Linearkombination, dass $\lambda_i = 0 \,\forall\, i \in J \Longrightarrow (v_i)_{i\in J}$ ist linear unabhängig □

Bemerkung 5.22 (8.17) Sei V K-Vektorraum, Dann gilt:

1. Ist $v \in V$, dann gilt (v) linear unabhängig $\Longleftrightarrow v \neq 0$
2. Gehört der Nullvektor zu einer Familie, dann ist sie linear abhängig
3. Kommt der gleiche Vektor in einer Familie mehrfach vor so ist sie linear abhängig
4. Ist $r \geq 2$, so gilt: Die Familie $(v_1, \ldots, v_r)$ von Vektoren aus V ist linear abhängig $\Longleftrightarrow \exists\, i \in \{1, \ldots, r\}$: v_i Linearkombination von $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_r$

Beweis 1. „$\Longrightarrow$“ (Durch Kontraposition): Sei $v = 0$. Dann ist $1v = 0$, das heißt (v) ist linear abhängig „$\Longleftarrow$“ (Durch Kontraposition) Sei (v) linear abhängig $\Longrightarrow \exists\, \lambda \in K \setminus \{0\} : \lambda v = 0 \Longrightarrow v = 0$

2. Wegen $1 \cdot 0_v = 0_v$ existiert in diesem Fall eine nicht triviale Linearkombination der Null.
3. Sei $(v_i)_{i\in I}$ eine Familie, sodass $i_1, i_2 \in I$ existiert mit $i_1 \neq i_2$ und $v_{i_1} = v_{i_2} \Longrightarrow 1 \cdot v_{i_1} + (-1) \cdot v_{i_2} = 0 \Longrightarrow (v_i)_{i\in I}$ linear abhängig
4. Sei $r \geq 2$, $(v_1, \ldots, v_r)$ Familie von Vektoren aus V
„$\Longrightarrow$“ Sei $v_1, \ldots, v_r$ linear abhängig $\Longrightarrow \exists\, \lambda_1, \ldots, \lambda_r \in K : (\lambda_1, \ldots, \lambda_r) \neq (0, \ldots, 0) \wedge \lambda_1 v_1 + \ldots \lambda_r v_r = 0$ Insbesondere existiert ein $i \in \{1, \ldots, r\}$, mit $\lambda_i \neq 0$
$$\Longrightarrow v_i = -\frac{\lambda_1}{\lambda_i} v_1 - \ldots - \frac{\lambda_{i-1}}{\lambda_i} v_{i-1} - \frac{\lambda_{i+1}}{\lambda_i} v_{i+1} - \ldots - \frac{\lambda_r}{\lambda_i} v_r$$
” $\Longleftarrow$ ”Sei $i \in \{1, \ldots, r\}$, so dass
$$v_i = \lambda_1 v_1 + \ldots + \lambda_{i-1} v_{i-1} + \lambda_{i+1} v_{i+1} + \ldots + \lambda_r v_r$$
mit geeigneten $\lambda_j \in K$:
$$\Longrightarrow \lambda_1 v_1 + \ldots + \lambda_{i-1} v_{i-1} + (-1) v_i + \lambda i + 1 v_{i+1} + \ldots + \lambda_r v_r = 0$$
$$\Longrightarrow (v_1, \ldots, v_r) \text{ linear abhängig}$$

□

6 Basis und Dimension

In diesem Abschnitt sei V stets ein K-VR

Definition 6.1 (9.1) $(v_i)_{i\in I}$ Familie von Vektoren aus V. $(v_i)_{i\in I}$ heißt **Erzeugendensystem** (ES) von $V \overset{Def}{\Longleftrightarrow}$ $V = \mathrm{Lin}\big((v_i)_{i\in I}\big)$
V heißt **endlich erzeugt** $\overset{\text{Def}}{\Longleftrightarrow}$ V besitzt ein endliches Erzeugendensystem (das heißt es existiert eine endliche Familie $(v_1, \ldots, v_n)$ von Vektoren aus V mit $V = \mathrm{Lin}((v_1, \ldots, v_n)))$
$(v_i)_{i\in I}$ heißt **Basis** von $V \overset{\text{Def}}{\Longleftrightarrow}$ $(v_i)_{i\in I}$ ist linear unabhängiges Erzeugendensystem von V
Ist $\mathcal{B} = (v_1, \ldots, v_n)$ eine endliche Basis von V, dann heißt n die **Länge** von $\mathcal{B}$

Beispiel 6.2 (9.2)

1. Die Familie $(e_1, \ldots, e_n)$ ist eine Basis des K_VR K^n, da $\mathrm{Lin}((e_1, \ldots, e_n)) = K^n$ (vergleiche 8.10.2) und somit $(e_1, \ldots, e_n)$ Erzeugendensystem des K^n, und $(e_1, \ldots, e_n)$ linear unabhängig nach 8.15.1. Die Länge der Basis ist $(e_1, \ldots, e_n)$ ist n. $(e_1, \ldots, e_n)$ heißt die kanonische Basis oder Standardbasis der K^n.

2. Die Familie $(t^n)_{n\in\mathbb{N}_0}$ ist eine Basis der K-VR $K[t]$, denn: $\mathrm{Lin}\big((t^n)_{n\in\mathbb{N}_0}\big) = K[t]$ nach 8.12, $(t^n)_{n\in\mathbb{N}_0}$ ist linear unabhängig nach 8.15.3

3. $((1, -1), (0, 2), (1, 2))$ ist ein Erzeugendensystem des $\mathbb{R}$ -VR $\mathbb{R}^2$, denn für jedes $(x_1, x_2) \in \mathbb{R}^2$ ist $(x_1, x_2) = x_1(1, -1) + \frac{x_1+x_2}{e}(0, 2) \in \mathrm{Lin}((1, -1), (0, 2), (1, 2))$, $((1, -1), (0, 2), (1, 2))$ ist jedoch keine Basis des $\mathbb{R}$, da linear abhängig nach 8.15.2

4. Die leere Familie () ist eine Basis des Nullraums $\{0\}$: vergleiche 8.11 und Annahme nach 8.14

Anmerkung 6.3 Jeder Vektorraum V besitzt ein ES, denn es ist $V = \mathrm{Lin}\big((v)_{v\in V}\big)$
Spannende Frage: Besitzt jeder VR eine Basis?
Wir werden das zunächst für den Fall endlich erzeugter Vektorräume untersuchen

Satz 6.4 (9.3) $V \neq \{0\}, \mathcal{B} = (v_1, \ldots, v_n)$ endliche Familie von Vektoren aus V, dann sind äquivalent:

1. $\mathcal{B}$ ist eine Basis von V, das heißt eine linear unabhängiges ES von V

2. $\mathcal{B}$ ist ein unverkürzbares ES von V, das heißt $\mathcal{B}$ ist ein ES und für jedes $r \in \{1, \ldots, n\}$ ist $(v_1, \ldots, v_{r-1}, v_{r+1}, \ldots, v_n)$ kein ES von V mehr.

3. Zu jedem $v \in V$ gibt es eindeutig bestimmte $\lambda_1, \ldots, \lambda_n \in K$ mit
$$v = \lambda_1 v_1 + \ldots + \lambda_v v_n$$

4. $\mathcal{B}$ ist unverlängerbar linear unabhängig, das heißt $\mathcal{B}$ ist linear unabhängig und für jedes $v \in V$ ist die Familie $(v_1, \ldots, v_n, v)$ linear abhängig

Beweis Wir zeigen 1. $\Longrightarrow$ 2. $\Longrightarrow$ 3. $\Longrightarrow$ 4. $\Longrightarrow$ 1.

1. $\Longrightarrow$ 2.: Sei $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis von $V \Longrightarrow \mathcal{B}$ ist ES von V
Annahme: $\mathcal{B}$ ist verkürzbar, das heißt es gibt ein $r \in \{r, \ldots, n\}$, sodass $(v_1, \ldots, v_{r-1}, v_{r+1}, \ldots, v_n)$ immer noch ein ES von $V \Longrightarrow v_r \in \mathrm{Lin}((v_1, \ldots, v_{r-1}, v_{r+1}, \ldots, v_n))$, das heißt
$$\exists\, \lambda_1, \ldots, \lambda_{r-1}, \lambda_{r+1}, \ldots, \lambda_n \in K : v_r = \lambda_1 v_1 + \ldots + \lambda_{r-1} v_{r-1} + (-1) v_r + \lambda_{r+1} v_{r+1} + \ldots + \lambda_n v_n$$
$\Longrightarrow \mathcal{B}$ linear abhängig ` zu $\mathcal{B}$ Basis von V

2. $\implies$ 1.: Sei $\mathcal{B} = (v_1, \ldots, v_n)$ ein unverkürzbares ES von $V \implies$ Für jedes $v \in V$ existiert $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$ Annahme: Es gibt $v \in V, \lambda_1, \ldots, \lambda_v v_n = \mu_1 v_1 + \ldots \mu_n v_n, i \in \{i, \ldots, n\}$ mit $\lambda_i \notin \mu_i$

$$\implies (\lambda_i - \mu_i)v_i = (\mu_1 - \lambda_1)v_i + \ldots + (\mu_{i-1} - \lambda_{i-1})v_{i-1} + (\mu_{i+1} - \lambda_{i+1})v_{i+1} + \ldots + (\mu_n - \lambda_n)v_n$$
$$\implies v_1 = \frac{\mu_1 - \lambda_1}{\lambda_i - \mu_i}v_1 + \ldots + \frac{\mu_{i-1} - \lambda_{i-1}}{\lambda_i - \mu_i}v_{i-1} + \frac{\mu_{i+1} - \lambda_{i+1}}{\lambda_i - \mu_i}v_{i+1} + \ldots + \frac{\mu_n - \lambda_n}{\lambda_i - \mu_i}v_n$$

$\implies$ Jeder UVR von v_i der $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$ enthält, enthält auch v_i
$\implies \mathrm{Lin}((v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)) = \mathrm{Lin}((v_1, \ldots, v_n)) = v$
$\implies \mathcal{B}$ ist verkürzbar `

3. $\implies$ 4.: Wir setzten 3. voraus, das heißt für jedes $v \in V$ existieren eindeutig bestimmt $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$.
zu zeigen: $\mathcal{B}$ ist unverlängerbar linear unabhängig
denn Insbesondere existiert für jedes $v \in \mathrm{Lin}((v_1, \ldots, v_n))$ eindeutig bestimmt $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \ldots + \lambda_n v_n \implies (v_1, \ldots, v_n)$ linear unabhängig. Ist $v \in V$, dann existiert $\lambda_1, \ldots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \ldots + \lambda_n v_n \implies (v_1, \ldots, v_n, v)$ linear abhängig. Somit: $\mathcal{B}$ unverlängerbar linear unabhängig

4. $\implies$ 1. Sei $\mathcal{B}$ unverlängerbar linear unabhängig zu zeigen: $\mathcal{B}$ ist Basis von V, das heißt es bleibt noch zu zeigen, dass $\mathcal{B}$ ein ES von V ist
Sei $v \in V \implies (v_1, \ldots, v_n, v)$ linear abhängig $\implies \exists\, \lambda_1, \ldots, \lambda_n, \lambda \in K, (\lambda_1, \ldots, \lambda_n, \lambda) \neq (0, \ldots, 0) : \lambda_1 v_1 + \ldots + \lambda_n v_n + \lambda v = 0$ Es ist $\lambda \neq 0$, da sonst $(v_1, \ldots, v_n)$ linear abhängig

$$\implies v = -\frac{\lambda_1}{\lambda}v_1 - \ldots - -\frac{\lambda_n}{\lambda}v_n \in \mathrm{Lin}((v_1, \ldots, v_n))$$

$\implies \mathcal{B}$ ist ES von V □

Folgerung 6.5 (9.4 Basiswahlsatz) Besitzt V ein endliches ES $(v_1, \ldots, v_n)$, dann kann man aus diesem eine Basis auswählen, das heißt es gibt eine Teilmenge $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$, sodass $(v_{i_0}, \ldots, v_{i_r})$ ein Basis von V ist. Insbesondere besitzt jeder endlich erzeuge Vektorraum eine Basis

Beweis Entferne aus dem ES $(v_1, \ldots, v_n)$ nacheinander solange Elemente, bis die resultierende Familie ein unverkürzbares ES und somit nach 8.3 eine Basis von V ist. □

Folgerung 6.6 (9.5) Jeder endlich erzeugte K-VR besitzt eine Basis von endlicher Länge.
Fragen:

- Ist jede Basis von V von endlicher Länge?
- Sind je zwei endliche Basen von V gleicher Länge

Satz 6.7 (9.6 Austauschlemma) V endlich erzeugter K-VR, $\mathcal{B} = (v_1, \ldots, v_r)$ von $V, \lambda_1, \ldots, \lambda_r \in K, w = \lambda_1 v_1 + \ldots + \lambda_r v_r$. Dann gilt: Ist $k \in \{1, \ldots, r\}$ mit $\lambda_k \neq 0$, dann ist

$$\mathcal{B}' = (v_1, \ldots, v_{k-1}, w, v_{k+1}, \ldots, v_r)$$

ebenfalls eine Basis von V, das heißt man kann v_k gegen w austauschen

Beweis Wir können ohne Einschränkung („ohne Beschränkung der Allgemeinheit“) annehmen, dass $k = 1$ ist (können wir durch Umsortieren erreichen). Gegeben ist $w = \lambda_1 v_1 + \ldots + \lambda_r v_r \in V$, mit $\lambda_1 \neq 0$ zu zeigen ist, dass $\mathcal{B}' = (w, v_2, \ldots, v_r)$ ein Basis von V ist.

1. $\mathcal{B}'$ ist ein ES von V
   Sei $v \in V \implies \exists\, \mu_1, \ldots, \mu_r \in K : v = \mu_1 v_1 + \ldots + \mu_r v_r$
   Aus $w = \lambda_1 v_1 + \ldots + \lambda_r v_r$ folgt wegen $\lambda_1 \neq 0$:
   $$v_1 = \frac{1}{\lambda_1} w - \frac{\lambda_2}{\lambda_1} v_2 - \ldots - \frac{\lambda_r}{\lambda_1} v$$
   $$v = \frac{\mu_1}{\lambda_1} w + \left(\mu_2 - \mu_1 \frac{\lambda_2}{\lambda_1}\right) v_2 + \ldots + \left(\mu_r - \mu_1 \frac{\lambda_r}{\lambda_1}\right) v_r \in \mathrm{Lin}((w, v_2, \ldots, v_r))$$

2. $\mathcal{B}'$ ist linear unabhängig, denn:

   Sei $\mu, \mu_2, \ldots, \mu_r \in K$ mit $\mu w + \mu_2 v_2 + \ldots + \mu_r v_r = 0$
   $$\implies \mu(\lambda_1 v_1 + \ldots + \lambda_r v_r) + \mu_2 v_2 + \ldots + \mu_r v_r = 0$$
   $$\implies \mu\lambda_1 v_1 + (\mu\lambda_2 + \mu_2) v_2 + \ldots + (\mu\lambda_r + \mu_r) v_r = 0$$
   $$\implies \mu\lambda_1 = 0 \implies \mu = 0 \implies \mu_2 v_2 + \ldots + \mu_r v_r = 0 \implies \mu_2 = \ldots = \mu_r = 0$$ □

Satz 6.8 (Austauschsatz) V endlich erzeugter K-VR, $(w_1, \ldots, w_n)$ linear unabhängige Familie in V. Dann gilt

1. Ist $\mathcal{B} = (v_1, \ldots, v_r)$ eine Basis von V, dann ist $r \geq n$
2. Es gibt Indizes $i_1, \ldots, i_n \in \{1, \ldots, r\}$ derart, dass man aus der Basis $\mathcal{B} = (v_1, \ldots v_r)$ von V nach Austausch von v_{i_1} gegen w_1, v_{i_2} gegen $w_2, \ldots, v_{i_n}$ gegen w_n wieder eine Basis von V erhält. Nummeriert man $\mathcal{B}$ so um, dass $i_1 = 1, i_2 = 2, \ldots, i_n = n$, bedeutet dies, dass $\mathcal{B}^* := (w_1, \ldots, w_n, w_{n+1}, \ldots, v_r)$ eine Basis von V ist.

Beweis Wir zeigen 1. und 2. zusammen per Induktion nach n
Induktionsanfang: $n = 0$: $(w_1, \ldots, w_n)$ leere Familie
Induktionsschritt: Sei $n \geq 1$, und die Aussage sei für $n - 1$ schon bewiesen. Wegen $(w_1, \ldots, w_a)$ linear unabhängige Familie ist auch $(w_1, \ldots, w_{n-1})$ linear unabhängig $\implies n - 1 \leq r$ und nach Umnummerieren von $\mathcal{B}$ ist auch
$$\widetilde{\mathcal{B}} := (v_1, \ldots, w_{n-1}, v_n, \ldots, v_r)$$
eine Basis von V.

Falls $n - 1 = r$, dann wäre $\widetilde{\mathcal{B}} = (w_1, \ldots, w_{n-1})$ eine Basis von V ` (zu 9.3, denn auch $(w_1, \ldots, w_n)$ linear unabhängig). Also $n - 1 < r$, das heißt $n \leq r$

Da $\widetilde{\mathcal{B}}$ Basis von $V, \exists\, \lambda_1, \ldots, \lambda_r \in K : w_n = \lambda_1 w_1 + \ldots, \lambda_{n-1} w_{n-1} \lambda_n w_n + \ldots + \lambda_r$
Falls $\lambda_n = \ldots = \lambda_r = 0$, dann $(w_1, \ldots, w_n)$ linear abhängig `
Also existiert ein $k \in \{n, \ldots, r\}$ mit $\lambda_k \neq 0$ Nach Umnummerieren von $v_n, \ldots, v_r$ kann man $\lambda_n \neq 0$ erreichen
$$\implies \mathcal{B}^* := (w_1, \ldots, w_{n-1}, w_n, v_{n+1}, \ldots, v_r)$$
ist eine Basis von V (tausche v_n gegen w_n) □

Folgerung 6.9 (9.8) Es gilt:

1. Ist V endlich erzeugt, dann ist jede Basis von V von endlicher Länge und je zwei Basen haben dieselbe Länge
2. Ist V nicht endlich erzeugt, dann existiert für V keine Basis von endlicher Länge

Beweis 1. • V endlich erzeugt $\implies$ es existiert eine endliche Basis $(v_1, \ldots, v_r)$ von V, sei $(w_i)_{i \in I}$ beliebige Basis von V. Falls I unendlich, dann existiert $i_1, \ldots, i_{r+1} \in I$, so dass $\left(w_{i_1} + \ldots + w_{i_{r+1}}\right)$ linear unabhängig $\implies r + 1 \leq r$ `

• Sind $(v_1, \ldots, v_r), (w_1, \ldots, w_k)$ endliche Basen von V, dann folgt nach Austauschsatz $k \leq r$, sowie $r \leq k \implies r = k$

2. Besitzt V eine Basis endlicher Länge, dann ist diese auch ein endliches ES, das heißt V endlich erzeugt `
□

Definition 6.10 (9.9)

$$\dim_k V := \begin{cases} r & \text{falls } V \text{ endlich erzeugt, } r \text{ Länge jeder Basis von } V \\ \infty & \text{falls } V \text{ nicht endlich erzeugt} \end{cases}$$

heißt die Dimension von V über K. Ist $\dim_k V \in \mathbb{N}_0$, dann heißt V endlich dimensional über K.

Anmerkung 6.11 • Der Dimensionsbegriff ist wohldefiniert nach 9.8

Beispiel 6.12 (9.10) 1. $V = K^n$ Die Standardbasis $(e_1, \ldots, e_n)$ von K^n hat Länge von n, das heißt $\dim_k K^n = n$. Insbesondere hat jede Basis von K^n die Länge n

2. In $K[t]$ ist die Familie $(t^n)_{n \in \mathbb{N}_0}$ eine Basis unendlicher Länge. Wäre $K[t]$ endlich dimensional über K, dann wäre jede Basis von $K[t]$ als K-VR von endlicher Länge. Also $\dim_k K[t] = \infty$
3. $\dim_{\mathbb{C}} \mathbb{C} = 1$, aber $\dim_{\mathbb{R}} \mathbb{C} = 2$, (denn: $(1, \imath)$ ist eine Basis von $\mathbb{C}$ also $\mathbb{R}$ -VR)

Anmerkung 6.13 • Ist klar, welcher Körper gemeint ist schreibt man kurz $\dim V$ statt $\dim_K V$.

• Offenbar gilt V endlich erzeugt $\iff$ V endlich dimensional

Folgerung 6.14 (9.11) V endlich dimensionaler K-VR, $U \subseteq V$ UVR von V Dann gilt:

1. U ist endlich dimensional
2. $\dim_k U \leq \dim_K V$
3. Es ist $U = V \iff \dim_k U = \dim_k V$

Beweis 1. Annahme: U ist nicht endlich dimensional
Beweis: per Induktion nach N
Induktionsanfang: $n = 1$: Da $n \neq \{0\}$ wegen $\dim_k U = \infty$ existiert $u_1 \in U \setminus \{0\}, (u_1)$ ist linear unabhängig Induktionsschritt: Sei $n > 1$, die Aussage sei für $n - 1$ bewiesen. $\implies$ ex existiert linear unabhängige Familie $(u_1, \ldots, u_{n-1})$. Falls $(u_1, \ldots, u_{n-1}, u)$ linear abhängig für alle $u \in U$, dann wäre $(u_1, \ldots u_{n-1})$ unverlängerbar linear abhängig und somit nach 9.3 eine Basis von U ` zu U nicht endlich dimensional. Also existiert ein $u_1 \in U$ mit $(u_1, \ldots, u_n)$ linear unabhängig $\implies$ Behauptung Wir setzen $r := \sum_K V$, dann existiert nach 1. eine lineare Familie $(u_1, \ldots, u_{r+1})$ in U. Die Familie $(u_1, \ldots, u_{r+1})$ ist auch eine linear unabhängige Familie in $V \implies r + 1 \leq r$ ` Das heißt U ist endlich

2. Annahme: $n := \dim_k U > \dim V$
   Sei $(u_1, \ldots, u_n)$ Basis von U, das heißt insbesondere ist die Familie $(u_1, \ldots, u_n)$ eine linear unabhängige Familie in $V \implies n \leq \sum_k V$ `

3. „ $\implies$ “ trivial
   „ $\impliedby$ “ Annahme: $U \subsetneq V$
   Sei $(u_1, \ldots, u_r)$ Basis von U. Wegen $U \subsetneq V$ ist $(u_1, \ldots, u_r)$ keine Basis von $V \implies \exists\, v \in V :$ $(u_1, \ldots, u_r, v)$ linear unabhängig. $\implies$ es existiert $v \in V$, sodass $(u_1, \ldots, u_r, v)$ linear unabhängig $\implies r + 1 \leq \dim V = \dim U = r$` □

Satz 6.15 (9.12 Basisergänzungssatz) V endlich dimensionaler K-VR, $(u_1, \ldots, u_n)$ linear unabhängige Familie von V
Dass existiert $u_{n+1}, \ldots, u_r \in V, r = \sum V$, sodass $\mathcal{B} = (u_1, \ldots, u_n, u_{n+1}, \ldots, u_r)$ eine Basis von V ist (das heißt $(u_1, \ldots, u_n)$ kann zu einer Basis ergänzt werden)

Beweis Sei $(v_1, \ldots, v_r)$ eine Basis von V. Aus Austauschsatz folgt: Nach Umnummerierung von $v_1, \ldots, v_r$ ist $(u_1, \ldots, u_n, v_{n+1}, \ldots, v_r)$ eine Basis von B Setze $u_{n+1} := v_{n+1}, \ldots, u_r := v_r$ □

Satz 6.16 (9.13 Zornsches Lemma) Jede induktiv geordnete nicht leere Menge $(M, \leq)$ besitzt ein maximales Element. Hierbei heißt eine halbgeordnete Menge $(m, \leq)$ **induktiv geordnet** $\overset{\text{Def}}{\iff}$ Jede Teilmenge $T \subseteq M$, für die $(T, \leq)$ totalgeordnet ist, besitzt eine obere Schranke in $(M, \leq)$, das heißt $\exists\, S \in M : t \leq S\, \forall\, t \in T$

Anmerkung 6.17 Das Zornsche Lemma ist äquivalent zum Auswahlaxiom

Definition 6.18 (9.14) $(u_j)_{j \in J}$ linear unabhängige Familie in V. Dann kann $(u_j)_{j \in J}$ zu einer Basis von V ergänzt werden, das heißt $\exists\, I : J \subseteq I, (v_i)_{i \in I} : v_j = u_j\, \forall\, j \in J$, sodass $(v_i)_{i \in I}$ eine Basis von V ist. Insbesondere besitzt jeder K-VR eine Basis.

Beweis 1. Wir setzen $A := \{u_j \mid j \in J\}, M := \{X \subseteq V \mid A \subseteq X \wedge X \text{ ist linear unabhängig}\}$

- $(M, \subseteq)$ ist eine halbgeordnete Menge
- $(M \neq \emptyset)$, denn $A \in M$
- $(m, \subseteq)$ ist induktiv geordnet, denn: Sei $T \subseteq M$, sodass $(T, \subseteq)$ totalgeordnet ist.
  zu zeigen: T besitzt eine obere Schranke in M.
  Wir setzen $S := \bigcup\limits_{X \in T} X$, dann ist $X \subseteq S\, \forall\, X \in T$. Noch zu zeigen: $S \in M$, das heißt $A \subseteq S$ und S ist linear unabhängig
  - $A \subseteq S$ klar, denn $A \subseteq X\, \forall\, X \in T$
  - S ist linear unabhängig, das heißt jede endliche Teilfamilie von $(s)_{s \in S}$ ist linear unabhängig:
    Seien $s_1, \ldots, s_n \in S$ paarweise verschieden $\implies \exists\, X_1, \ldots X_n \in T : s_i \in X_i, i = 1, \ldots, n$
    Da $(T, \subseteq)$ totalgeordnet ist existiert ein $i \in \{1, \ldots, n\}$ mit $X_j \subseteq X_i$ für alle $j \in \{1, \ldots, n\} \implies$ $s_1, \ldots, s_n \subseteq X_i \xRightarrow{X_i \in M} (x_1, \ldots, s_n)$ linear unabhängig.

2. Nach 1. können wir das Zornsche Lemma auf $(M, \subseteq)$ anwenden $\implies \exists \max B \in M$
   Behauptung: $(b)_{b \in B}$ ist eine Basis von V mit $A \subseteq B$, denn: Da $(b)_{b \in B}$ linear unabhängig wegen $V \in M$, gilt zu zeigen, dass $\mathrm{Lin}(B) = V$
   „$\subseteq$“ klar
   „$\supseteq$“

Sei $v \in V$. Falls $v \in B$, dann $v \in \mathrm{Lin}(B)$, falls $v = 0$, dann $v \in \mathrm{Lin}(B)$, im Folgenden sei $v \notin B, v \neq 0$

$$\implies A \subseteq B \subsetneq B \cup \{v\}$$

Da B Maximum von $(M, \subseteq)$ ist, ist $B \cup \{v\} \notin M$, das heißt $B \cup \{v\}$ ist linear abhängig

$$\implies \exists n \in \mathbb{N}_0, \lambda_1, \ldots, \lambda_n \in K, \lambda \in K, (\lambda, \lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0), b_1, \ldots, b_n \in B :$$
$$\lambda v + \lambda_1 b_1 + \ldots + \lambda_n b_n = 0$$

Falls $n = 0$

$$\lambda v = 0 \overset{v \neq 0}{\implies} \lambda = 0\text{\`{}}$$

Also $n \geq 1$, Falls $\lambda = 0$

$$(b_1, \ldots, b_n) \text{ linear abhängig\`{}}$$

Also $\lambda \neq 0$, somit:

$$v = -\frac{\lambda_1}{\lambda} v_1 - \ldots - \frac{\lambda_n}{\lambda} b_n \in \mathrm{Lin}((b_1, \ldots, b_n)) \subseteq \mathrm{Lin}(B) \qquad \square$$

Anmerkung 6.19 Der Satz „Jeder VR hat eine Basis“ ist äquivalent zum Auswahlaxiom.

7 Matrizen

In diesem Abschnitt seinen $m, n, r \in \mathbb{N}$
Frage: Gegeben sei ein UVR $U = \mathrm{Lin}((v_1, \ldots, v_m)) \subseteq K^n$ Wie bestimmt man effizient die Basis von U?

Definition 7.1 (10.1) Eine $m \times n$ -Matrix mit Einträgen aus K ist eine Familie $(a_{11}, \ldots, a_{1n}, a_{21}, \ldots, a_{2n}, \ldots, a_{m1}, \ldots, a_{mn}$ von mn Elementen aus K, die wir in der Form

$$(a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \text{ (kurz } (a_{ij}) \text{ wenn } m, n \text{ klar sind)}$$

schreiben. Die Menge aller $m \times n$ Matrizen mit Einträgen aus K bezeichnen wir mit $M(m \times n, K)$. Für $A = (a_{ij})$ wie oben heißen

$$a_i := (1_{i1} \ldots a_{in}), i = 1, \ldots, m$$

Die Zeilen der Matrix A. Im Folgenden fassen wir die Zeilen von A als Elemente von K^n auf: $a_i = (a_{i1}, \ldots, a_{in})$

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \in M(m \times 1, K), j = 1, \ldots, n$$

heißen die Spalten der Matrix A

Bemerkung 7.2 (10.2) Es gilt:

1. $M(m \times n, K)$ ist bezüglich der Verknüpfungen

$$+ : M(m \times n, K) \times M(m \times n, K) \to M(m \times n, K), (a_{ij}) + (b_ij) := (a_{ij} + b_{ij})$$
$$\cdot : K \times M(m \times n, K) \to M(m \times n, K), \lambda \cdot (a_{ij}) := (\lambda a_{ij})$$

ein K_VR. Es ist $\dim_k M(m \times n, K) = m \cdot n$

2. Durch
$$\cdot : M(m \times n, K) \times M(n \times r, K) \to M(m \times r, K)$$
$$(a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} \cdot (b_{jk})_{\substack{1 \le j \le n \\ 1 \le k \le r}} := (c_{ik})_{\substack{1 \le i \le m \\ 1 \le k \le r}}$$
mit
$$c_{ik} := \sum_{j=1}^{n} a_{ij} b_{jk}$$
ist die Multiplikation von Matrizen erklärt. Visualisierung:
$$\begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix} \cdot \begin{pmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{pmatrix} = \begin{pmatrix} c_{ij} \end{pmatrix} \tag{23}$$
Für diese gilt: Sind $A_1, A_2 \in M(m \times n, K), B_1, B_2 \in M(n \times r, K), C \in M(r \times s, K), \lambda \in K$, dann ist
   - $A(B_1 + B_2) = A \cdot B_1 + A \cdot B_2, (A_1 + A_2)B = A_1 B + A_2 B$
   - $A(\lambda B) = (\lambda A)B = \lambda(AB)$
   - $A(BC) = (AB)C$
   - $E_m \cdot A = A \cdot E_n = A$

   Hierbei ist für $l \in \mathbb{N}$
$$E_l := \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in M(l \times l, K)$$
die $l \times l$ -Einheitsmatrix über K

3. $M(n \times n, K)$ ist bezüglich
$$+, \cdot : M(n \times n, K) \times M(n \times n, K) \to M(n \times n, K)$$
(„$+$“ siehe 1., „$\cdot$“ siehe 2.)
ein Ring. (Einselement: E_n). Für $n > 1$ ist dieser Ring **nicht** kommutativ

Beweis Nachrechnen
Zu $\dim M(m \times n, K) = m \cdot n$: Eine Basis von $M(m \times n, K)$ ist durch die Familie der Matrizen $E_{ij}, i = 1, \dots, m, j = 1, \dots, n$ gegeben, wobei E_{ij} diejenige $m \times n$ -Matrix mit Einträgen in K bezeichnen, die in der i-ten Zeile, j-ten Spalte eine Eins und sonst nur Nullen stehen hat.
zu 3.: $M(n \times n, K)$ ist nicht kommutativ für $n > 1$:
$$\left(\begin{array}{cc|c} 1 & 0 & \multirow{2}{*}{0} \\ 0 & 0 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right) \cdot \left(\begin{array}{cc|c} 0 & 1 & \multirow{2}{*}{0} \\ 0 & 0 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right) = \left(\begin{array}{cc|c} 0 & 1 & \multirow{2}{*}{0} \\ 0 & 0 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right)$$
$$\neq \left(\begin{array}{cc|c} 0 & 1 & \multirow{2}{*}{0} \\ 0 & 0 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right) \cdot \left(\begin{array}{cc|c} 1 & 0 & \multirow{2}{*}{0} \\ 0 & 0 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right) = \left(\begin{array}{cc|c} 0 & 0 & \multirow{2}{*}{0} \\ 0 & 0 & \\ \hline \multicolumn{2}{c|}{0} & 0 \end{array}\right)$$
$\square$

Definition 7.3 (10.3) A heißt invertierbar $\overset{\text{Def}}{\iff} \exists\, B \in M(n \times n, K) : AB = BA = E_n$

Bemerkung 7.4 (10.4) Es gilt:

$$GL(n, K) := \{A \in M(n \times n, K) \mid A \text{ ist invertierbar}\}$$

ist bezüglich der Matrizenmultiplikation eine Gruppe, die so genannte allgemeine lineare Gruppe. Das neutrale Element ist E_n, das zu $A \in GL(n, K)$ inverse Element bezeichnen wir mit A^{-1}.

Beweis Wohldefiniertheit von „$\cdot$“ auf $GL(n, K)$
zu zeigen ist: $A_1, A_2 \in GL(n, K) \implies A_1 A_2 \in GL(n, K)$
Dies gilt, denn:

$$\begin{aligned} A_1, A_2 \in GL(n, K) &\implies \exists\, B_1, B_2 \in M(n \times n, K) : A_1 B_1 = B_1 A_1 = E_n, A_2 B_2 = B_2 A_2 = E_N \\ &\implies (A_1 A_2) \cdot (B_2 B_1) = A_1 (A_2 B_2) B_1 = A_1 E_n B_1 = A_1 B_1 = E_n \\ &\quad\ (B_2 B_1) \cdot (A_1 A_2) = B_2 (B_1 A_1) A_2 = B_2 E_n A_2 = B_2 A_2 = E_n \end{aligned}$$

das heißt $A_1 A_2 \in GL(n, K)$

- Assoziativität: Vererbt sich von $M(n \times n, K)$
- neutrales Element: E_n
- Existenz von Inversen: Sei $A \in GL(n, K) \implies \exists\, B \in M(n \times n, K) : AB = BA = E_n$ also ist $B \in GL(n, K)$ und B ist invers zu A bezüglich „$\cdot$“. □

Definition 7.5 (10.5) $A \in M(m \times n, K)$ mit Zeilen $a_1, \ldots, a_m \in K^n$
Unter elementaren Zeilenumformungen von A verstehen wir die folgende Umformungen von A

1. Multiplikation der i-ten Zeile mit $\lambda \in K^* = K \setminus \{0\}$

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ \lambda a_i \\ \vdots \end{pmatrix}$$

2. Addition der j-ten Zeile zur i-ten Zeile, $i \neq j$

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$

3. Addition der λ fachen der j-ten Zeile zur i-ten Zeile, $\lambda \in K^*, i \neq j$

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$

4. Vertauschen der i-ten Zeile mit der j-ten Zeile, $i \neq j$

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix}$$

Anmerkung 7.6

- Typ 3. und 4. kann man durch Kombination von Umformungen vom Typ 1. und 2. erhalten, 3.:

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ \lambda a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ \lambda a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ \lambda a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \tag{24}$$

  Typ 4.:

$$\begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ -a_j \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix} \to \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \tag{25}$$

- Analog zu den elementaren Zeilenumformungen definiert man elementare Spaltenumformungen in nahe liegender Weise

- Elementare Zeilenumformungen erhält man durch Multiplikation von A mit sogenannten **Elementarmatrizen** von links, elementare Spaltenumformungen durch Multiplikation mit Elementarmatrizen von recht.

Definition 7.7 (10.6) $A \in M(m \times n, K)$ mit Zeilen $a_1, \ldots, a_m \in K^n$

$$ZR(A) := \mathrm{Lin}((a_1, \ldots, a_m)) \subseteq K^n$$

heißt Zeilenraum von A.

Beispiel 7.8 (10.7)

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 5 \end{pmatrix} \in M(2, \times 3, \mathbb{Q}) \implies ZR(A) = \mathrm{Lin}((1,2,3),(4,5,6)) \subseteq \mathbb{Q}^2 \tag{26}$$

Bemerkung 7.9 (10.8) $A, B \in M(m \times n, K)$
Dann gilt: Ist B aus A durch eine endliche Folge von elementaren Zeilenumformungen entstanden, dann ist $ZR(B) = ZR(A)$

Beweis Wegen Anmerkung nach 10.5 genügt es, einzelne Zeilenumformungen vom Typ 1. und 2. zu betrachten

1. Typ 1-Umformung:

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}, B = \begin{pmatrix} a_1 \\ \vdots \\ \lambda a_j \\ \vdots \\ a_m \end{pmatrix}, \lambda \in K^*$$

zu zeigen:

$$ZR(A) = \text{Lin}((a_1, \ldots, a_m)) = \text{Lin}((a_1, \ldots, a_{j-1}, \lambda a_j, a_{j+1}, \ldots, a_m)) = ZR(B)$$

Dies gilt, da jeder UVR von K^n, der $a_1, \ldots, a_m$ enthält, auch $a_1, \ldots, a_{j-1}, \lambda a_j, a_{j+1}, \ldots, a_m$ enthält und umgekehrt (Behauptung folgt dann aus 8.13)

2. Typ 2-Umformungen:

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}, B = \begin{pmatrix} a_1 \\ \vdots \\ a_i + a_j \\ \vdots \\ a_m \end{pmatrix}, \lambda \in K^*$$

zu zeigen:

$$ZR(A) = \text{Lin}((a_1, \ldots, a_m)) = \text{Lin}((a_1, \ldots, a_{i-1}, a_i + a_j, a_{i+1}, \ldots, a_m)) = ZR(B)$$

Dies gilt, denn jeder UVR von K^n, der $a_1, \ldots a_m$ enthält auch $a_1, \ldots, a_{i-1}, a_i + a_j, a_{i+1}, \ldots, a_m$ enthält und umgekehrt (Behauptung folgt dann aus 8.13) □

Ziel: Bringe Matrix $A \in M(m \times n, K)$ mit Zeilen $a_1, \ldots, a_m \in K^n$ durch elementare Zeilenumformungen auf „einfache Gestalt", aus oder man eine Basis von $\text{Lin}((a_1, \ldots, a_m)) = ZR(A) = ZR(B)$ ablesen kann.

Definition 7.10 (10.9) $A = (a_{ij}) \in M(m \times n, K)$
A ist in Zeilenstufenform (ZSF) $\overset{\text{Def}}{\iff}$ die folgenden Bedingungen sind erfüllt

- (Z1) Es gibt eine Zahl $r \in \mathbb{N}_0$, mit $0 \leq r \leq m$, so dass in den Zeilen mit Index 1 bis r jeweils nicht nur Nullen stehen und in der Zeile mit den Indizes $r + 1$ bis m stehen nur Nullen.

- (Z2) Setzen wir für i mit $1 \leq i \leq r$

$$j_i := \min\{j \in \{1, \ldots, n\} \mid a_{ij} \neq 0\}$$

dann gilt: $j_1 < j_2 < \ldots < j_r$ (Stufenbedingung), die Elemente $a_{1j_1}, \ldots, a_{1j_r}$ heißen die Pivots von A

Beispiel 7.11 (10.10)

$$A = \begin{pmatrix} 0 & 3 & 1 & 0 & 3 & 4 \\ 0 & 0 & 0 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 6 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in M(4 \times 6, \mathbb{R}) \tag{27}$$

ist in ZSF. Es ist $r = 3, j_1 = 2, j_2 = 4, j_3 = 5$, Pivots: $a_{12} = 3, a_{24} = 2, a_{35} = 6$

Definition 7.12 (10.11) $A \in M(m \times n, K)$
Dann lässt sich A durch endlich viele elementare Zeilenumformungen in eine Matrix B in ZSF umformen:

$$\begin{pmatrix} & b_{1j_1} & * & & & \\ & & b_{1j_2} & * & & \\ & & & \dots & & \\ & & & & b_{1j_r} & * \\ 0 & & & & & \end{pmatrix} \tag{28}$$

Die ersten r Zeilen von B bilden eine Basis von $ZR(A)$.

Beweis 1. A lässt sich wie behauptet auf ZSF bringen:
Falls $A = 0$, dann ist A bereits in ZSF (mit r = 0), also im Folgenden sei $A \neq 0$

a) Bestimme minimalen Index $j_1 \in \{1, \dots, n\}$, so dass es ein $i_1 \in \{1, \dots, m\}$ gibt mit $a_{i_1 j_1} \neq 0$ („Wie weit links in der Matrix A befinden sich Einträge $\neq 0$?“)
Wähle solch ein i_1 aus.

b) Vertausche i_1 -te Zeile mit erster Zeile, erhalte ersten Pivot:

$$\tilde{a}_{1,j_1} := a_{i_1,j_1} \neq 0 A_1 := \begin{pmatrix} 0 & \dots & 0 & \tilde{a}_{1,j_1} & * & \dots & * \\ & & & * & & & \\ & \mathbf{0} & & \vdots & & * & \\ & & & * & & & \end{pmatrix} \tag{29}$$

c) Durch Umformungen vom Typ 3. können alle Einträge der j_1 -ten Spalte unterhalb der ersten Zeile zu Null gemacht werden, erhalte:

$$\begin{pmatrix} 0 & \dots & 0 & \tilde{a}_{1,j_1} & * & \dots & * \\ & & & 0 & & & \\ & \mathbf{0} & & \vdots & & A_2 & \\ & & & 0 & & & \end{pmatrix} \tag{30}$$

d) Wende das Verfahren 1. - 3. auf A_2 an. Die dafür benötigten elementaren Zeilenumformungen von A_2 kann man auf die Zeilen 2 bis m von $\tilde{A}_1$ ausdehnen, ohne dass sich in den Spalten 1 bis j_1 von $\tilde{A}_1$ etwas ändert, denn dort stehen Nullen. Erhalte auf diese Weise $\tilde{A}_2$ beziehungsweise A_3. Iteriere dieses Verfahren. Das Verfahren bricht ab, weil die Folge der Spaltenzahlen der Matrizen A_k streng monoton fallend in $\mathbb{N}$ ist, oder irgendwann eine Matrix $A_k = 0$ entsteht.
$\implies$ erhalte ZSF. Die ersten r Zeilen $b_1, \dots, b_r$ von B bilden eine Basis von $ZR(A)$, denn Es ist $ZR(A) = ZR(B) = \mathrm{Lin}((b_1, \dots, b_r))$
noch zu zeigen: $(b_1, \dots, b_r)$ ist linear unabhängig.
Es seien $\lambda_1, \dots, \lambda_r \in K$ mit $\lambda_1 b_1 + \dots + \lambda_r b_r = 0$. In der j_1 -ten Komponente von $\lambda_1 b_1 + \dots + \lambda_r b_r$ steht $\lambda_1 b_{1j_1}$ = 0. Wegen $b_{1j_1} = 0$ folgt λ_1 = 0. In der j_2 -ten Komponente von $\lambda_1 v_1 + \dots + \lambda_r b_r = \lambda_2 b_2 + \dots + \lambda_r b_r$ steht $\lambda_2 b_{2j_2} = 0$ Wegen $b_{2j_2} \neq 0$ folgt $\lambda_2 = 0$. Durch Iterieren dieses Arguments erhalten wir $\lambda_1 = \dots = \lambda_r = 0$ □

Algorithmus 7.13 (10.12) Eingabe: $W = \mathrm{Lin}((v_1, \dots, v_m)) \subseteq K^n$
Ausgabe: Eine Basis $(w_1, \dots, w_r)$ von W
Durchführung:

1. Bilde aus den Zeilenvektoren $v_1, \dots, v_m$ die Matrix $A \in M(m \times n, K)$
2. Bringe die Matrix A durch elementare Zeilenumformung auf ZSF B
3. Die Familie $(w_1, \dots, w_r)$ der ersten r Zeilenvektoren von B ist ein Basis von W

Beispiel 7.14 (10.13) $W = \mathrm{Lin}((0,0,3,-1),(0,1,2,0),(0,3,0,2)) \subseteq \mathbb{R}^4$

$$A = \begin{pmatrix} 0 & 0 & 3 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 3 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & -6 & 2 \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{31}$$

$\Longrightarrow$ $((0,1,2,0),(0,0,3,-1))$ ist eine Basis von W insbesondere ist $\dim_W = 2$

Definition 7.15 (10.14 transponierte Matrix) $A = (a_{ij}) \in M(m \times n, K)$

$$A^t := \begin{pmatrix} a_{11} & & a_{m1} \\ \vdots & \dots & \vdots \\ a_{1n} & & a_{mn} \end{pmatrix} \in M(n \times m, K)$$

heißt die zu A transponierte Matrix (Transponierte von A).

Beispiel 7.16 (10.15)

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in M(2 \times 3, \mathbb{R}) \implies A^t = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \in M(3 \times 2, \mathbb{R})$$

Bemerkung 7.17 (10.16) $A, A_2, A_2 \in M(m \times n, K), B \in M(n \times r, K), \lambda K$ dann gilt:

1. $(A_1 + A_2)^t = A_1^t + A_2^t$
2. $(\lambda A)^t = \lambda A^t$
3. $\left(A^t\right)^t = A$
4. $(AB)^t = B^t A^t$

Beweis 1. trivial

2. trivial
3. trivial
4. Nach 3. gezeigt: $AB = \left(B^t A^t\right)^t \implies (AB)^t = \left(\left(B^t A^t\right)^t\right)^t = B^t A^t$. Sei $A = (a_{ij})_{\substack{1 \leq 1 \leq m \\ 1 \leq j \leq n}}, B = (b_{ij})_{\substack{1 \leq 1 \leq n \\ 1 \leq j \leq r}}$
   $\Longrightarrow$ Eintrag an Position (i,k) von AB ist gegeben durch

   $$\sum_{1 \leq j \leq n} a_{ij} b_{jk}$$

   Eintrag an Position (i,k) in $\left(B^t A^t\right)^t$ = Eintrag an Position (r,i) von $B^t A^t$. Dieser ist gegeben durch:

   $$\sum_{i \leq j \leq n} b'_{kj} a'_{ji} = \sum_{1 \leq j \leq n} b_{jk} a_{ij} = \sum_{1 \leq j \leq m} a_{ij} b_{jk}$$

   wobei:

- b'_{kj} = Eintrag an Position (k, j) von $B^t = b_{jk}$
- a'_{ji} = Eintrag an Position (j, i) von $A^t = a_{ij}$

Somit $AB = \left(B^t A^t\right)^t$ □

Definition 7.18 (10.17) $A \in M(m \times n, K)$

- Zeilenrang$(A) := \dim_k \mathrm{ZR}(A)$ heißt der **Zeilenrang** von A
- $\mathrm{SR}(A) := \mathrm{ZR}\left(A^t\right) \subseteq k^m$ heißt der **Spaltenraum** von A
- Spaltenrang$(A) := \dim_k \mathrm{SR}(A)$ heißt der **Spaltenrang** von A

Beispiel 7.19 (10.18) Wir betrachten die Matrix A aus Beispiel 10.13

$$A = \begin{pmatrix} 0 & 0 & 3 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix} \in M(3 \times 4, \mathbb{R}), \dim \mathrm{ZR}(A) = 2$$

$$A^t = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 3 \\ 3 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix} \in M(4 \times 3, \mathbb{R}) \implies \mathrm{SR}(A) := \mathrm{Lin}((0,0,0),(0,1,3),(3,2,0),(-1,0,2))$$

Wir bestimmen eine Basis von $\mathrm{SR}(A)$:

$$A^t = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 3 \\ 3 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix} \to \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 3 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 2 & 6 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$\implies$ $((-1,0,2),(0,1,3))$ ist eine Basis von $\mathrm{SR}(A)$ $\implies$ Spaltenrang(A) = 2. In diesem Beispiel ist also Zeilenrang(A) = Spaltenrang(A).

Anmerkung 7.20 Wir werden später zeigen: Für jedes $A \in M(m \times n, K)$ ist Zeilenrang(A) = Spaltenrang(A).

8 Summen von Untervektorräumen

In diesem Abschnitt sei V stets ein K -VR

Definition 8.1 (11.1) $U_1, \ldots, U_r \subseteq V$ UVR.

$$U_1 + \ldots + U_r := \{u_1 + \ldots + u_r \mid u_1 \in U_1, \ldots, u_r \in U_r\} \subseteq V$$

heißt die Summe von $U_1, \ldots, U_r$. Für $U_1 + \ldots + U_r$ schreiben wir auch

$$\sum_{i=1}^{r} U_i$$

Bemerkung 8.2 (11,2) $U_1, \ldots, U_r \subseteq V$ UVR. Dann gilt:

1. $U_1 + \ldots + U_r = \mathrm{Lin}(U_1 \cup \ldots \cup U_r)$ das heißt $U_1 + \ldots + U_r$ ist der kleinste UVR von V, der alle Elemente aus $U_1, \ldots, U_r$ enthält.

2. Sind $U_1, \ldots, U_r$ endlichdimensional, dann ist auch $U_1 + \ldots + U_r$ endlichdimensional, und es ist

$$\dim(U_1 + \ldots + U_r) \leq \sim (U_1) + \ldots + \dim(U_r)$$

Beweis 1. „$\subseteq$" Sei $v \in U_1 + \ldots + U_r$

$$\implies \exists\, u_1 \in U_1, \ldots, u_r \in U_r : v = u_1 + \ldots + u_r$$

somit $v \in \mathrm{Lin}(U_1 \cup \ldots \cup U_r)$
„$\supseteq$" Sei $v \in \mathrm{Lin}(U_1 \cup \ldots \cup U_r)$

$$\implies \exists\, w_1, \ldots, w_s \in U_1 \cup \ldots \cup U_r, \lambda_1, \ldots, \lambda_s \in K : v = \lambda_1 w_1 + \ldots + \lambda_s w_s$$

Wegen $w_i \in U_1 \cup \ldots \cup U_r$:

$$\exists\, j_i \in \{1, \ldots, r\} : w_i \in U_{j_i}$$

somit

$$v_i := \lambda w_1 \in U_{j_i} \implies v = v_1 + \ldots + v_s \in U_1 + \ldots + U_r$$

2. Ist $\left(u_1^{(i)}, \ldots, u_{s_i}\right)^{(i)}$ eine Basis von U_i, dann ist

$$\left(u_1^{(1)}, \ldots u_{s_1}^{(1)}, \ldots, u_1^{(r)}, \ldots, u_{s_r}^{(r)}\right)$$

ein ES von $U_1 + \ldots + U_r \implies \dim(U_1 + \ldots + U_r) \leq s_1 + \ldots + s_r = \dim(U_1) + \ldots + \dim(U_r)$ □

Beispiel 8.3 (11.3) 1. $K = \mathbb{R}, V = \mathbb{R}^2, U_1 = \mathrm{Lin}((1, -1)), U_2 = \mathrm{Lin}((1, 1))$

$$\implies U_1 + U_2 = \mathrm{Lin}((1, -1), (1, 1)) = \mathbb{R}^2$$

2. $K = \mathbb{R}, V = \mathbb{R}^3, U_1 = \mathrm{Lin}((e_1, e_2)) =$ („$x_1 - x_2$ -Ebene"), $U_2 = \mathrm{Lin}((e_2, e_3))$ („$x_2 - x_3$ -Ebene")

$$\implies U_1 + U_2 \ni e_1, e_2, e_3 \implies U_1 + U_2 = \mathbb{R}^3 \implies \dim(U_1 + U_2) = 3 < \dim(U_1) + \sim (U_2) = 4$$

Satz 8.4 (11.4) $U_1, U_2 \subseteq V$ endlichdimensionale UVR. Dann gilt:

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

Beweis 1. Sei $(v_1, \ldots, v_m)$ eine Basis von $U_1 \cap U_2$

$$\implies \exists\, u_1, \ldots, u_k \in U_1 : \mathcal{B}_1 := (v_1, \ldots, v_m, u_1, \ldots, u_k) \text{ Basis von } U_1$$

und es gibt $u'_1, \ldots, u'_l$ sodass

$$\mathcal{B}_2 := \left(v_1, \ldots, v_m, u'_1, \ldots u'_l\right) \text{ Basis von } U_2$$

2. Behauptung: $\mathcal{B} := (v_1, \ldots, v_m, u_1, \ldots, u_k, u'_1, \ldots u'_l)$ ist Basis von $U_1 + U_2$ Beweis:
   - $\mathcal{B}$ ist ES von $U_1 + U_2$

- $\mathcal{B}$ ist linear unabhängig, denn: Sei

$$\underbrace{\lambda_1 v_1 + \ldots + \lambda_m v_m + \mu_1 u_1 + \ldots \mu_k u_k}_{=:v \in U_1} + \mu_1' u_1' + \ldots + \mu_l' u_l' = 0$$
$$\implies v = -\mu_1' u_1' - \ldots - \mu_l' u_l' \in U_1 \cap U_2 = \operatorname{Lin}((v_1, \ldots, v_m))$$

  Eindeutigkeit der Darstellung in $\mathcal{B}_1$

$$\implies \mu_1 = \ldots = \mu_k = 0$$
$$\implies \lambda_1 v_1 + \ldots + \lambda_m v_m + \mu_1' u_1' + \ldots + \mu_l' u_l' = 0$$

  Wegen $\mathcal{B}_2$ Basis von U_2

$$\implies \lambda_1 = \ldots = \lambda_m = \mu_1' = \ldots = \mu_l' = 0$$

3. Aus Aussage 1. und 2. folgt: $\dim(U_1 \cap U_2) = m, \dim U_1 = m + k, \dim U_2 = m + l, \dim(U_1 + U_2) = m + k + l = m + k + l$

$$\implies \dim(U_1 + U_2) = \dim(U_1) + \dim(U_2) - \dim(U_1 \cap U_2) \qquad \square$$

Definition 8.5 (11.5 Direkte Summe) $U_1, \ldots, U_r \subseteq V$ UVR. V heißt die direkte Summe von $U_1, \ldots, U_r \overset{\text{Def}}{\iff}$:

$$V = U_1 + \ldots + U_r \wedge U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j = \{0\}$$

Notation: $V = U_1 \oplus \ldots \oplus U_r$

Anmerkung 8.6

- Spezialfall: $r = 2$:

$$V = U_1 \oplus U_2 \iff V = U_1 + U_2 \wedge U_1 \cap U_2 = \{0\}$$

  In diesem Fall ist $\dim(V) = \dim(U_1) + \dim(U_2)$

- Ist $r \geq 3$, dann genügt es nicht für $V = U_1 \oplus \ldots \oplus U_r$ zu fordern, dass

$$V = U_1 + \ldots + U_r \wedge U_i \cap U_j = \{0\} \, \forall \, i \neq j$$

  zum Beispiel:

$$K = \mathbb{R}, V = \mathbb{R}^2, U_1 = \operatorname{Lin}((e_1)), U_2 = \operatorname{Lin}((e_2)), U_3 = \operatorname{Lin}((1,1))$$

  Dann ist $V = U_1 + U_2 + U_3$ und $U_i \cap U_j = \{0\} \, \forall \, i \neq j$, aber

$$U_1 \cap \left(\underbrace{U_2 + U_3}_{=\mathbb{R}^{\not\vDash}} \right) = U_1 \neq \{0\}$$

  das heißt die Summe ist nicht direkt.

Beispiel 8.7 (11.6) (vergleiche Beispiel 11.3)

1. $K = \mathbb{R}, V = \mathbb{R}^2, U_1 = \operatorname{Lin}((1,1)), U_2 = \operatorname{Lin}((1,-1)) \implies V = U_1 \oplus U_2$

2. $K=\mathbb{R}, V=\mathbb{R}^3, U_1=\operatorname{Lin}((e_1,e_2)), U_2=\operatorname{Lin}((e_2,e_3)) \implies V=U_1+U_2$, aber die Summe ist nicht direkt, denn $e_2\in U_1\cap U_2$

Bemerkung 8.8 (11.7) $U_1,\dots,U_r\subseteq V$. Dann sind äquivalent

1. $V=U_1\oplus\ldots\oplus U_r$
2. Für jedes $v\in V$ existieren eindeutig bestimmte $u_i\in U_i, i=1,\dots,r$ mit $v=u_1+\ldots u_r$

Beweis 1. $\implies$ 2. Sei $V=U_1\oplus\ldots\oplus U_r, v\in V$

$$\implies V=U_1+\ldots+U_r \implies \exists\, u_i\in U_i, i=1,\ldots r: v=u_1+\ldots+u_r$$

Eindeutigkeit: Seien $\tilde u_i\in U_i, i=1,\dots,r$ mit $v=u_1+\ldots+u_r=\tilde u_1+\tilde u_r$

$$\implies \underbrace{u_1-\tilde u_1}_{\in U_1}=\underbrace{(\tilde u_2-u_2)}_{\in U_2}+\ldots+\underbrace{(\tilde u_r-u_r)}_{\in U_r}\in U_1\cap\sum_{i=2}^r U_i=\{0\}$$
$$\implies u_1=\tilde u_1 \implies u_1+\ldots+u_r=\tilde u_2+\ldots+\tilde u_r$$

Induktiv folgt durch Wiederholung dieses Arguments: $u_2=\tilde u_2,\dots,u_r=\tilde u_r$

2. $\implies$ 1. Aus 2. folgt sofort: $V=U_1+\ldots+U_r$
Annahme:

$$\exists\, i\in\{1,\dots,r\}: U_i\cap\sum_{\substack{j=1\\ j\neq i}}^r U_j\neq\{0\}$$

$\implies \exists\, u_k\in U_k, k=1,\dots,r, u_1\neq 0$ und

$$u_i=u_1+\ldots+u_{i-1}+u_{i+1}+\ldots+u_r`$$

Widerspruch zur Eindeutigkeit der Darstellung. □

Satz 8.9 (11.8) V endlichdimensionaler K -VR, $U_1,\dots,U_r\subseteq V$ UVR. Dann sind äquivalent

1. $V=U_1\oplus\ldots\oplus U_r$
2. Für alle Basen $\mathcal{B}_i=\left(v_1^{(i)},\dots,v_{s_i}^{(i)}\right)$ von $U_i, i=1,\dots,r$ ist

$$\mathcal{B}:=\left(v_1^{(i)},\dots,v_{s_1}^{(1)},\dots,v_1^{(r)},\dots,v_{s_r}^{(r)}\right)$$

eine Basis von V

3. Es gibt Basen $\mathcal{B}_i=\left(v_1^{(i)},\dots,v_{s_i}^{(i)}\right)$ von $U_i, i=1,\dots,r$ sodass

$$\mathcal{B}:=\left(v_1^{(1)},\dots,v_{s_1}^{(1)},\dots,v_1^{(r)},\dots,v_{s_r}^{(r)}\right)$$

eine Basis von V ist.

4. $V=U_1+\ldots+U_r$ und $\dim V=\dim U_1+\ldots+\dim U_r$

Beweis (1.) $\implies$ (2.)
Es sei

$$V = U_1 \oplus \ldots \oplus U_r, \mathcal{B}_i = \left(v_1^{(i)}, \ldots, v_{s_i}^{(i)}\right), i = 1, \ldots, r \text{ Basis von } U_i$$

$$\mathcal{B} := \left(v_1^{(i)}, \ldots, v_{s_1}^{(1)}, \ldots, v_1^{(r)}, \ldots, v_{s_r}^{(r)}\right)$$

1. Wegen $V = U_1 + \ldots + U_r$ ist $\mathcal{B}$ ES von V
2. $\mathcal{B}$ ist linear unabhängig, denn: Sei

$$\underbrace{\mu_1^{(1)}, v_1^{(1)} + \ldots + \mu_{s_1}^{(1)} v_{s_1}^{(1)}}_{=:u_1} + \ldots + \underbrace{\mu_1^{(r)} v_1^{(r)} + \ldots + \mu_{s_r}^{(r)} v_{s_r}^{(r)} = 0}_{=:u_r}$$

also $U_1 + \ldots + u_r = 0$. Falls $u_1 = \ldots = u_r = 0$, dann folgt wegen $\mathcal{B}_i$ linear unabhängig, dass

$$\mu_1^{(i)} = \ldots = \mu_{s_i}^{(i)} = 0 \,\forall\, i \in \{1, \ldots, r\}$$

Falls ein $i \in \{1, \ldots, r\}$ existiert mit $u_i \neq 0$, dann

$$u_i = -u_1 - \ldots - u_{i-1} - u_{i+1} - \ldots - u_r \in U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j = \{0\}`$$

(2.) $\implies$ (3.) klar
(3.) $\implies$ (4.) klar
(4.) $\implies$ (2.) Es gelte 4., das heißt $V = U_1 + \ldots + U_r$ und $\dim(V) = \dim(U_1) + \ldots + \dim(U_r)$. Es seien $B_i = \left(v_1^{(i)}, \ldots, v_{s_i}^{(i)}\right), i = 1, \ldots, r$ Basen von $U_i, \mathcal{B} := \left(v_1^{(1)}, \ldots, v_{s1}^{(1)}, \ldots, v_1^{(r)}, v_{sr}^{(r)}\right)$. $\implies$ $\mathcal{B}$ ist Erzeugendensystem von $U_1 + \ldots + U_r = V$, $\mathcal{B}$ besteht aus $s_1 + \ldots + s_r = \dim(U_1) + \ldots + \dim(U_r) = \dim V$ Vektoren $\implies$ $\mathcal{B}$ ist Basis von V.
(2.) $\implies$ (1.) Es gelte 2., das heißt für alle Basen $\mathcal{B}_i = \left(v_1^{(i)}, \ldots, v_{s_i}^{(i)}\right), i = 1, \ldots, r$ von U_i ist $\mathcal{B} := \left(v_1^{(1)}, \ldots, v_{s1}^{(1)}, \ldots, v_1^{(r)}, v_{sr}^{(r)}\right)$ eine Basis von V.
zu zeigen: $V = U_1 \oplus \ldots \oplus U_r$.
klar: $V = U_1 + \ldots U_r$
Sei $i \in \{1, \ldots, r\}, v \in U_1 \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j$. $\implies$ $\exists\, \mu_1^{(k)} \in K, k = 1, \ldots, r, = 1, l = 1, \ldots, s_k$:

$$\underset{\substack{\downarrow \\ v \in U_i}}{v} = \mu_1^{(i)} v_1^{(i)} + \ldots + \mu_{s_i}^{(i)} v_{s_i}^{(i)} = \sum_{\substack{j=1 \\ j \neq i}}^{r} \left(\mu_1^{(j)} v_1^{(j)} + \ldots + \mu_{s_i}^{(j)} v_{s_i}^{(j)}\right)$$

Wegen $\mathcal{B}$ Basis folgt $\mu_l^{(k)} = 0 \,\forall\, k = 1, \ldots, r, l = 1, \ldots, s_k$, also $v = 0$. Somit

$$U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j = \{0\}$$

also $V = U_1 \oplus \ldots \oplus U_r$ $\square$

Satz 8.10 (11.9 Existenz des Komplement) $U \subseteq V$ UVR. Dann $\exists$ ein UVR $W \subseteq V$ mit $V = U \oplus W$. W heißt ein Komplement zu U in V.

Beweis Sei $(U_j)_{j\in J}$ eine Basis von U. Daraus folgt mit dem Basisergänzungssatz: Es existiert eine Menge $I \subseteq J$, Basis $(v_i)_{i\in i}$ von V mit $v_j = u_j \,\forall\, j \in J$ insbesondere $U = \operatorname{Lin}\big((v_i)_{i\in J}\big)$. Setze $V := \operatorname{Lin}\Big((v_i)_{i\in I\setminus J}\Big) \implies U + W = V$.
Behauptung: $U \cap W = \{0\}$, denn Sei $v \in U \cap W \implies \exists\, j_1, \ldots j_r \in J, i_1, \ldots, i_s \in I \setminus J, \lambda_{j_1}, \ldots, \lambda_{j_r}, \lambda_{i_1}, \ldots, \lambda_{i_s} \in K$:

$$\begin{aligned} v &= \lambda_{j_1} v_{j_1} + \ldots + \lambda_{j_r} v_{j_r} = \lambda i_1 v_{i_1} + \ldots + \lambda_{i_s} v_{i_s}. \\ &\implies \lambda_{j_1} v_{j_1} + \ldots + \lambda_{j_r} v_{j_r} - \lambda_{i_1} v_{i_1} - \ldots - \lambda_{i_s} v_{i_s} = 0 \\ &\implies v = 0 \end{aligned}$$

□

Anmerkung 8.11 W wie in 11.9 ist im allgemeinen nicht eindeutig bestimmt. Zum Beispiel:

$$K = \mathbb{R}, V = \mathbb{R}^2, U = \operatorname{Lin}((e_1)) \implies V = U \oplus \operatorname{Lin}((e_2)) = U \oplus \operatorname{Lin}((1,1))$$

9 Lineare Abbildungen

In diesem Kapitel sei K stets ein Körper, U, V, W stets ein K -VR.

Definition 9.1 (12.1 Lineare Abbildung) $f : V \to W$ Abbildung. f heißt K -lineare Abbildung (Homomorphismus von K-VR, kurz lineare Abbildung) $\overset{\text{Def.}}{\Longleftrightarrow}$ Die folgende Bedingungen sind erfüllt:

- (L1) $f(u + v) = f(u) + f(v) \,\forall\, u, v \in V$
- (L1) $f(\lambda v) = \lambda f(v) \,\forall\, u, v \in V \,\forall\, w \in V, \lambda \in K$

Beispiel 9.2 (12.2) 1. $A = (a_{i,j}) \in M(m \times n, K)$. Wir schreiben die Elemente von K^n als Spaltenvektoren und betrachten die Abbildung:

$$\tilde{A} : K^n \to K^m, x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto Ax$$

Es gilt für $u, v \in K^n, \lambda \in K$:

$$\begin{aligned} \tilde{A}(u + v) = A(u + v) = Au + Av = \tilde{A}(u) + \tilde{A}(v) \\ \tilde{A}(\lambda v) = A(\lambda v) = \lambda(Av) = \lambda \tilde{A}(v) \end{aligned}$$

Wegen $\tilde{A}(e_i) = Ae_i = \begin{pmatrix} a_{i1} \\ \vdots \\ a_{in} \end{pmatrix}$ stehen in den Spalten von A genau die Bilder der kanonischen Basisvektoren $e_1, \ldots e_n$ von K^n unter $\tilde{A}$. Sind $A \in M(m \times n, K), B \in M(n \times r, K), x \in K^r$, dann ist

$$\widetilde{AB}(x) = (AB)(x) = A(B(x)) = A\tilde{B}(x) = \tilde{A}\Big(\tilde{B}(x)\Big) = \Big(\tilde{A}\tilde{B}\Big)(x)$$

das heißt die Verknüpfung von $\tilde{A}, \tilde{B}$ entspricht der Multiplikation der Matrizen $A, B : \tilde{A} \cdot \tilde{B} = \widetilde{AB}$

2. Wir betrachten die Abbildung

$$f : \mathbb{R}^2 \to \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ -x_2 \end{pmatrix}$$

Diese ist linear nach 1., beschreibt Spiegelung an der x_1 -Achse.

3. Sei $V = \{f : (0,1) \to \mathbb{R} \mid f \text{ ist differenzierbar}\}$ (ist ein $\mathbb{R}$ -VR)

$$' : V \to \{g : (0,1) \to \mathbb{R} \text{ Abb}\}, f \mapsto f'$$

ist eine lineare Abbildung, denn es gilt für $f, g \in V, \lambda \in \mathbb{R}$:

$$(f+g)' = f' + g'$$
$$(\lambda f)' = \lambda f'$$

Bemerkung 9.3 (12.3) $f : V \to W$ lineare Abbildung. Dann gilt:

1. $f(0) = 0$
2. $f(\lambda_1 v_1 + \ldots + \lambda_n v_n) = \lambda_1 f(v_1) + \ldots + \lambda_n f(v_n) \,\forall\, v_1, \ldots v_n \in V, \lambda_1, \ldots \lambda_n \in K$
3. $V' \subseteq V$ UVR $\implies f(V') \subseteq W$ ist UVR
4. $W' \subseteq W$ UVR $\implies f^1(W') \subseteq V$ ist UVR
5. $(v_i)_{i \in I}$ linear abhängige Familie in $V \implies (f(v_i))_{i \in I}$ linear abhängige Familie in W
6. $V' = \operatorname{Lin}\big((v_i)_{i\in I}\big) \implies f(V') = \operatorname{Lin}\big((f(v_i))_{i \in I}\big)$
7. W endlich dimensional $\implies f(V)$ endlich dimensionaler UVR von W mit $\dim f(V) \leq\sim W$

Beweis 1. $f(0) * f(0+0) = f(0) + f(0) \implies f(0) = 0$

2. $f(\lambda_1 v_1 + \ldots + \lambda_n v_n) = f(\lambda_1 v_1) + \ldots + f(\lambda_n v_n) = \lambda_1 f(v_1) + \ldots \lambda_n f(v_n)$
3. Sei $V' \subseteq V$ UVR.
   Behauptung: $F(V') \subseteq W$ ist UVR denn:
   - (U1): $0 \in V' \implies f(0) \in f(V')$
   - (U2): Seien $w_1, w_2 \in f(V') \implies \exists\, v_1, v_2 \in V' : w_1 = f(v_1), v_2 = f(v_2)$

   $$\implies w_1 + w_2 = f(v_1) + f(v_2) = f\left(\underbrace{v_1 + v_2}_{\in V'}\right) \in f\big(V'\big)$$

   - (U3): Sei $\lambda \in K, w \in f(V') \implies \exists\, v \in V' : w = f(v)$

   $$\implies \lambda w = \lambda f(v) = f\left(\underbrace{\lambda v}_{\in V'} \in f\big(V'\big)\right)$$

4. Sei $W' \subseteq W$ UVR.
   Behauptung: $f^{-1}(w') \subseteq V$ ist UVR, denn
   - (U1): $f(0) = 0 \in W' \implies 0 \in f^{-1}(W')$
   - (U2): Seien $v_1, v_2 \in f^{-1}(w')$:

   $$\implies f(v_1), f(v_2) \in W' \implies f(v_1 + v_2) = f(v_1) + f(v_2) \in W' \implies v_1 + v_2 \in f^{-1}\big(W'\big)$$

   - (U3): Sei $\lambda \in K, v \in f^{-1}(W')$:

   $$\implies f(v) \in W' \implies f(\lambda v) = \lambda f(v) \in W' \implies \lambda v \in f^{-1}\big(W'\big)$$

5. Sei $(v_i)_{i\in I}$ linear abhängig

$$\begin{aligned}&\implies \exists\, r\in\mathbb{N}, i_1,\dots,i_r\in I, \lambda_{i_1},\lambda_{i_r}\in K : (\lambda_{i_1},\dots,\lambda_{i_r})\neq(0,\dots,0)\wedge \lambda_{i_1}v_{i_1}+\ldots+\lambda_{i_r}v_{i_r}=0\\ &\implies 0=f(0)=f(\lambda_{i_1}v_{i_1}+\ldots+\lambda_{i_r}v_{i_r})=\lambda_{i_1}f(v_{i_1})+\ldots+\lambda_{i_1}f(v_{i_1})\\ &\implies (f(v_i))_{i\in I} \text{ linear abhängig}\end{aligned}$$

6. zu zeigen: $V'=\mathrm{Lin}\big((v_i)_{i\in I}\big) \implies f(V')=\mathrm{Lin}\big((f(v_i))_{i\in I}\big)$
„$\subseteq$“ Sei $w\in f(V') \implies \exists\, v\in V' : w=f(v)$. wegen V' = $\mathrm{Lin}\big((v_i)_{i\in I}\big)$:

$$\begin{aligned}&\exists\, i_1,\dots,i_r\in I, \lambda_{i_1},\dots,\lambda_{i_r}\in K : v=\lambda_{i_1}v_{i_1}+\ldots+\lambda_{i_r}v_{i_r}\\ &\implies f(v)=\lambda_{i_1}f(v_{i_1})+\ldots+\lambda_{i_r}f(v_{i_r})\in\mathrm{Lin}\big((f(v_i))_{i\in I}\big)\end{aligned}$$

„$\supseteq$“ Sei $w\in\mathrm{Lin}\big((f(v_i))_{i\in I}\big) \implies \exists\, i_1,\dots,i_r\in I, \lambda_{i_1},\dots,\lambda_{i_r}\in K$ mit

$$w=\lambda_{i_1}f(v_{i_1})+\ldots+\lambda_{i_r}f(v_{i_r})=f(\lambda_{i_1}v_{i_1}+\ldots+\lambda_{i_r}v_{i_r})\in f\big(V'\big)$$

7. $f(V)$ ist UVR von W nach 3. Rest aus Eigenschaften von dim. □

Bemerkung 9.4 (12.4 Verknüpfung von Linearen Abbildungen) $f:V\to W, g:U\to V$ lineare Abbildungen. Dann ist $f\circ g:U\to W$ ebenfalls eine lineare Abbildung.

Beweis

(L1): Seien $u_1,u_2\in U$

$$\begin{aligned}\implies (f\circ g)(u_1+u_2)&=f(g(u_1+u_2))=f(g(u_1)+g(u_2))\\ &=f(g(u_1))+f(g(u_2))=(f\circ g)(u_1)+(f\circ g)(u_2)\end{aligned}$$

(L2:) Seien $u\in U, \lambda\in K$

$$\begin{aligned}\implies (f\circ g)(\lambda u)&=f(g(\lambda u))=f(\lambda g(u))\\ &=\lambda f(g(u))=\lambda(f\circ g)(u)\end{aligned}$$ □

Definition 9.5 (12.5)

$$\mathrm{Hom}_K(V,W):=\{f:V\to W \mid f \text{ ist } K\text{ -linear}\}$$

Eine K -lineare Abbildung $f:V\to V$ heißt ein **Endomorphismus** von V.

$$\mathrm{End}_K(V):=\{f:V\to V\mid f \text{ ist Endomorphismus}\}=\mathrm{Hom}_K(V,V)$$

Bemerkung 9.6 (12.6) Es gilt:

1. $\mathrm{Hom}_K(V,W)$ ist bezüglich
   - $+:\mathrm{Hom}_K(V,W)\times\mathrm{Hom}_K(V,W)\to\mathrm{Hom}_K(V,W), (f,g)\mapsto f+g$
     mit $(f+g)(v):=f(v)+g(v)$ für $v\in V$
   - $\cdot : D\times\mathrm{Hom}_K(V,W)\to\mathrm{Hom}_k(V,W), (\lambda,f)\mapsto\lambda f$
     mit $(\lambda f)(c):=\lambda f(v)$ für $v\in V$

   ein K-Vektorraum. Nullvektor ist die Nullabbildung. $0:V\to W$ mit $0(v)=0$

2. $\mathrm{End}_k(V)$ ist bezüglich
   - $+ : \mathrm{End}_K(V) \times \mathrm{End}_K(V) \to \mathrm{End}_K(V), (f,g) \mapsto f+g$
   - $\circ : \mathrm{End}_K(V) \times \mathrm{End}_K(V) \to \mathrm{End}_K(V), (f,g) \mapsto f \circ g$

   ein Ring, Einselement ist id_V

Beweis Nachrechnen. □

Definition 9.7 (12.7) Eine bijektive K -lineare Abbildung $f : V \to W$ heißt ein **Isomorphismus** von V nach W. Eine bijektive K -lineare Abbildung $f : V \to V$ heißt **Automorphismus** von V.

$$\mathrm{Iso}_K(V,W) := \{f : V \to W \mid f \text{ ist ein Isomorphismus}\}$$
$$\mathrm{Aut}_K(V) := \{f : V \to V \mid f \text{ ist ein Automorphismus}\} = \mathrm{Iso}_K(V,V)$$

Bemerkung 9.8 (12.8) $f : V \to W$ lineare Abbildung. Dann gilt: Ist f ein Isomorphismus, dann ist auch $f^{-1} : W \to V$ ein Isomorphismus. Existiert zwischen V und W ein Isomorphismus, dann nennen wir V, W isomorph. (Notation: $V \cong W$)

Beweis analog zu 5.23c. □

Definition 9.9 (12.9) $f : V \to W$ lineare Abbildung.
$\mathrm{im}\, f := f(V)$ heißt das Bild von f
$\ker f := f^{-1}(0) = \{v \in V \mid f(v) = 0\}$ heißt der Kern von f

Bemerkung 9.10 (12.10) $f : V \to W$ lineare Abbildung. Dann gilt:

1. $\mathrm{im}\, f \subseteq W \wedge \ker f \subseteq V$ sind UVR
2. f surjektiv $\iff \mathrm{im}\, f = W$
3. f injektiv $\iff \ker f = \{0\}$
4. f injektiv $\wedge (v_i)_{i\in I}$ linear unabhängige Familie in $V \implies \left((f(v_i))_{i\in I}\right)$ ist linear unabhängig

Beweis 1. folgt aus 12.3 3.,4.

2. klar
3. „ $\implies$ “ sei f injektiv zu zeigen: $\ker f = \{0\}$
   - „$\subseteq$“ Sei $a \in \ker f \implies f(a) = 0 = f(0) \implies a = 0$
   - „$\supseteq$“ $f(0) = 0 \implies 0 \in \ker f$

   „ $\impliedby$ “ Sei $\ker f = \{0\}$ zu zeigen: f ist injektiv. Seien $v_1, v_2 \in V, f(v_1) = f(v_2) \implies f(v_1 - v_2) = f(v_1) - f(v_2) = 0 \implies v_1 - v_2 \in \ker f = \{0\} \implies v_1 - v_2 = 0 \implies v_1 = v_2$
4. Sei f injektiv, $(v_i)_{i\in I}$ linear unabhängige Familie in V zu zeigen: $\left((f(v_i))_{i\in I}\right)$ linear unabhängig. Seien $i_1, \ldots, i_r \in I, \lambda_{i_1}, \ldots, \lambda_{i_r} \in K, \lambda_{i_1} f(v_{i_1}) + \ldots + \lambda_{i_r} f(v_{i_r}) = 0$

$$\implies f\left(\underbrace{\lambda_{i_1} v_{i_1} + \ldots + \lambda_{i_r} v_{i_r}}_{\in \ker f = \{0\} \text{ wegen } f \text{ injektiv}}\right) = 0 \implies \lambda_{i_1} v_{i_1} + \ldots + \lambda_{i_r} v_{i_r} = 0$$
$$\implies \lambda_{i_1} = \ldots = \lambda_{i_r} = 0$$
□

Definition 9.11 (12.11) $f : V \to W$ lineare Abbildung.

$$\operatorname{Rang}(f) := \dim(\operatorname{im} f)$$

heißt der Rang von f

Definition 9.12 (12.12) $A \in M(m \times n, K)$. Wir betrachten die zu A gehörende lineare Abbildung $\tilde{A} : K^n \to K^m, x \mapsto Ax$. Wegen $K^n = \operatorname{Lin}((e_1, \dots, e_n))$ aus 12.3 5.:

$$\operatorname{im} \tilde{A} = \operatorname{Lin}\Big(\Big(\tilde{A}(e_1), \dots, \tilde{A}(e_n)\Big)\Big)$$

Nach 12.2 1. sind $\tilde{A}(e_1), \dots, \tilde{A}(e_n)$ genau die Spalten von A, das heißt:

$$\operatorname{Rang}\Big(\tilde{A}\Big) = \dim\Big(\operatorname{im} \tilde{A}\Big) = \dim SR(A) = \text{ Spaltenrang}(A)$$

Wir setzen $\operatorname{Rang}(A) := \operatorname{Rang}\Big(\tilde{A}\Big) = \text{ Spaltenrang}(A)$

Satz 9.13 (Dimensionsformel für lineare Abbildungen) V endlichdimensionaler K -Vektorraum, $f : V \to W$ lineare Abbildung. $(v_1, \dots, v_k)$ Basis von $\ker f$, $(w_1, \dots, w_r)$ Basis von $\operatorname{im} f$ (beachte $\operatorname{im} f$ endlichdimensional wegen 12.3 5.). Für $i = 1, \dots r$ sei $u_i \in V$ mit $f(u_i) = w_i$. Dann ist

$$\mathcal{A} := (u_1, \dots, u_r, v_1, \dots v_k)$$

eine Basis von V. Insbesondere ist $\dim V = \dim(\ker f) + \dim(\operatorname{im} f)$

Beweis 1. $\mathcal{A}$ ist ein ES von V:

Sei $v \in V$

$$\implies f(v) \in \operatorname{im} f \implies \exists\, \mu_1, \dots, \mu_r \in K : f(v) = \mu_1 w_1 + \ldots + \mu_r w_r$$

Setze $u := \mu_1 u_1 + \ldots + \mu_r u_r$, dann ist

$$\begin{aligned}
f(u) &= \mu_1 f(u_1) + \ldots + \mu_r f(u_r) = \mu_1 w_1 + \ldots + \mu_r w_r = f(v)\\
&\implies f(u - v) = 0 \implies u - v \in \ker f\\
&\exists\, \lambda_1 + \ldots + \lambda_k \in K : u - v = \lambda_1 v_1 + \ldots + \lambda_k v_k\\
&\implies v = -\lambda_1 v_1 - \ldots - \lambda_k v_k + \mu_1 u_1 + \ldots + \mu_r u_r \in \operatorname{Lin}((v_1, \dots, v_k, u_1, \dots, u_r))
\end{aligned}$$

2. $\mathcal{A}$ ist linear unabhängig:

Seien $\mu_1, \dots, \mu_r, \lambda_1, \dots, \lambda_k \in K$ mit

$$\begin{aligned}
&\mu_1 u_1 + \ldots + \mu_r u_r + \lambda_1 v_1 + \ldots + \lambda_k v_k = 0\\
&\implies \mu_1 f(u_1) + \ldots + \mu_r f(u_r) + \lambda_1 f(v_1) + \ldots + \lambda_k f(v_k) = 0\\
&\implies \mu_1 w_1 + \ldots + \mu_r w_r = 0 \implies \mu_1 = \ldots = \mu_r = 0\\
&\implies \lambda_1 v_1 + \ldots + \lambda_k v_k = 0 \implies \lambda_1 = \ldots = \lambda_k = 0
\end{aligned}$$

$\implies \mathcal{A}$ ist linear unabhängig. □

Folgerung 9.14 (12.14) V, W endlichdimensionale K-Vektorräume. Dann sind äquivalent

1. $V \cong W$
2. $\dim V = \dim W$

Beweis 1. $\implies$ 2. Sei $V \cong W$, das heißt $\exists\, f : V \to W : f$ isomorph. Sei $(v_1, \ldots, v_r)$ eine Basis von V. Wegen f injektiv folgt aus 12.10: $(f(v_1), \ldots, f(v_r))$ linear unabhängig. Wegen f surjektiv ist $W = f(V) = \mathrm{Lin}((f(v_1), \ldots, f(v_r))) \implies (f(v_1), \ldots, f(v_r))$ ist eine Basis von W. $\implies \dim W = r = \dim V$.

2. $\implies$ 1. Sei $\dim V = \dim W =: r$. Sei $(v_1, \ldots, v_r)$ Basis von V, $(w_1, \ldots, w_r)$ Basis von W. Wir definieren $f : V \to W, \lambda_1 v_1 + \ldots + \lambda_r v_r \mapsto \lambda_1 w_1 + \ldots + \lambda_r w_r$
   - f wohldefiniert, da $(v_1, \ldots, v_r)$ Basis von V ist
   - f ist linear, denn: Seien $u, v \in V$, etwa $u = \lambda_1 u_1 + \ldots + \lambda_r u_r, v = \mu_1 v_1 + \ldots + \mu_r v_r$ $\implies f(u+v) = f((\lambda_1+\mu_1)v_1 + \ldots + (\lambda_r+\mu_r)v_r) = (\lambda_1+\mu_1)w_1 + \ldots + (\lambda_r+\mu_r)w_r = \lambda_1 w_r + \ldots + \lambda_r w_r + \mu_1 w_1 + \ldots + \mu_r w_r = f(u) + f(v)$ Für $\lambda \in K$ ist $f(\lambda v) = f(\lambda\mu_1 v_1 + \ldots + \lambda\mu_r v_r) = \lambda\mu_1 w_1 + \ldots + \lambda\mu_r w_r = \lambda f(v)$
   - Es ist $\mathrm{im}\, f = \mathrm{Lin}((w_1, \ldots, w_r)) = W$, das heißt f ist surjektiv
   - f ist injektiv, denn $\dim V = \dim(\ker f) + \underbrace{\dim(\mathrm{im}\, f)}_{=\dim W = \dim V} \implies \dim(\ker f) = 0 \implies \ker f = \{0\}$, das heißt f injektiv. □

Folgerung 9.15 (12.15) $n, m \in \mathbb{N}$. Dann gilt: $K^n \cong K^m \iff n = m$.

Folgerung 9.16 (12.16) V endlich dimensionaler K-Vektorraum. Dann gilt:

$$\exists\, n \in \mathbb{N}_0 : V \cong K^n$$

Beweis Setze $n := \dim V$ □

Folgerung 9.17 (12.17) V, W endlich dimensionale K-Vektorraum mit $\dim V = \dim W$, $f : V \to W$ lineare Abbildung. Dann sind äquivalent:

1. f injektiv
2. f surjektiv
3. f bijektiv

Beweis 1. $\implies$ 2. Sei f injektiv $\implies \ker f = \{0\}$, also $\dim(\ker f) = 0$. Wegen $\dim V = \underbrace{\dim(\ker f)}_{=0} + \dim(\mathrm{im}\, f) = \dim(\mathrm{im}\, f) = \dim V = \dim W \implies \mathrm{im}\, f = W$, das heißt f surjektiv.

2. $\implies$ 3. Sei f surjektiv $\implies \dim(\ker f) = \dim(V) - \dim\left(\underbrace{\mathrm{im}\, f}_{=W}\right) = \dim V - \dim W = 0 \implies \ker f = \{0\} \implies f$ injektiv $\implies f$ bijektiv

3. $\implies$ 1. klar □

10 Faktorräume und der Homomorphiesatz

In diesem Abschnitt seien V, W stets K-Vektorräume.

Definition 10.1 (13.1) $A \subseteq V$. A heißt ein affiner Unterraum von $V \overset{\text{Def}}{\iff}$ Es gibt ein $a \in V$ und einen UVR $U \subseteq V$, sodass

$$A = a + U := \{a + u \mid u \in U\}$$

ist, oder $A = \emptyset$

Anmerkung 10.2
- affine Unterräume von V entstehen (mit Ausnahme von $\emptyset$) durch „Parallelverschiebung" von UVR von V.
- ist $A = a + U$ mit $a \notin U$, dann $0 \notin a + U$, das heißt A ist in diesem Fall kein UVR von V

Definition 10.3 (13.2) $a \in V, U \subseteq V$ UVR, $A = a + U$. Dann gilt:

1. Für jedes $b \in A$ ist $A = b + U$
2. Ist $\tilde{A} \in V, \tilde{U} \subseteq V$ UVR mit $\tilde{a} + \tilde{U} = a + U$, dann ist $U = \tilde{U}$ und $a - \tilde{a} \in U$.

Mit anderen Worten: Zu einem affinen Unterraum $A = a+U$ ist der UVR U eindeutig bestimmt, der „Aufhängepunkt" a kann beliebig in A gewählt werden. Wir setzen $\dim A := \dim U, \dim \emptyset := -1$

Beweis
1. Sei $b \in A = a + U \implies \exists\, u \in U : b = a + u$ zu zeigen: $a + U = b + U$
   „$\subseteq$" Sei $v \in a + U \implies \exists\, t \in U : v = a + t = \underbrace{b - u}_{=a} + t = b + \left(\underbrace{t - u}_{\in U}\right) \in b + U$.
   „$\supseteq$" Sei $v \in b + U \implies \exists\, t \in U : v = b + t = a + \left(\underbrace{u + t}_{\in U}\right) \in a + U$
2. Behauptung $U = \{b_1 - b_2 \mid b_1, b_2 \in a + U\}$ denn:
   „$\subseteq$" Sei $u \in U$. Setze $b_1 := a + u \in a + U, b_2 := a + 0 \in a + U$, dann $b_1 - b_2 = a + u - (a + 0) = 0$
   „$\supseteq$" Seien $b_1, b_2 \in a + U \implies \exists\, u_1, u_2 \in U : b_1 = a + u_1, b_2 = a + u_2 \implies b_1 - b_2 = (a + u_1) - (a + u_2) = u_1 - u_2 \in U$
   Analog: $\tilde{U} = \{b_1 - b_2 \mid b_1, b_2 \in \tilde{a} + \tilde{U}\}$
   Somit: $U = \{b_1 - b_2 \mid b_1, b_2 \in a + U\} = \{b_1 - b_2 \mid b_1, b_2 \in \tilde{a} + \tilde{U}\} = \tilde{U} \implies a + U = \tilde{a} + U \implies a \in a + U = \tilde{a} + U \implies \exists\, u \in U : a = \tilde{a} + u \implies a - \tilde{a} = u \in U$ ☐

Beispiel 10.4 (13.3)
- UVR U im $\mathbb{R}$ -Vektorraum $\mathbb{R}^2$:
  - $\dim U = 0 : \{0\}$
  - $\dim U = 1 : \mathrm{Lin}((v)), v \neq 0$ (Ursprungsgeraden)
  - $\dim U = 2 : \mathbb{R}^2$
- affine UR A in $\mathbb{R}^2$:
  - $\dim A = -1 : \emptyset$
  - $\dim A = 0 : \{a\}, a \in \mathbb{R}^2$ (Punkte)
  - $\dim A = 1 : a + \mathrm{Lin}((v)), a, v \in R^2, v \neq 0$ (Geraden)
  - $\dim A = 2 : \mathbb{R}^2$

Definition 10.5 (13.4) $f : V \to W$ lineare Abbildung, $w \in W$

$$f^{-1}(\{w\}) = \{v \in V \mid f(v) = w\}$$

heißt die Faser von f über w

Bemerkung 10.6
- Ist $A \in M(m \times n, K)$, so erhalten wir eine lineare Abbildung $\tilde{A} : K^n \to K^m, x \mapsto Ax$. Für $b \in K^m$ ist $\tilde{A}^{-1}(b) = x \in K^n \mid \tilde{A}(x) = b = \{x \in K^n \mid Ax = b\}$ genau die Lösungsmenge des lineare Gleichungssystems $Ax = b$
- Durch $v_1 \sim v_2 \overset{\text{Def}}{\iff} f(v_1) = f(v_2)$ ist eine Äquivalenzrelation auf V erklärt, die Äquivalenzklasse von $v \in V$ ist gegeben durch $\{u \in V \mid f(u) = f(v)\} = f^{-1}(f(v))$. Somit sind die nichtleeren Fasern von A genau die Äquivalenzklassen bezüglich „$\sim$“. Insbesondere ist V die Vereinigung der Fasern von f, je zwei Fasern von f sind gleich oder disjunkt.

Satz 10.7 (13.5) $f : V \to W$ lineare Abbildung, $w \in W$. Dann gilt:

$$f^{-1}(\{w\}) = \begin{cases} u + \ker f & \text{falls } w \in \operatorname{im} f \text{ (hierbei } u \in f^{-1}(\{w\})) \\ \emptyset & \text{falls } w \notin \operatorname{im} f \end{cases}$$

Somit ist die Faser von f über w ein affiner UR von V mit

$$\dim f^{-1}(\{w\}) = \begin{cases} \dim \ker f = \dim V - \dim \operatorname{im} f & \text{falls } w \in \operatorname{im} f \\ -1 & \text{falls } w \notin \operatorname{im} f \end{cases}$$

Insbesondere haben alle nichtleeren Fasern von f dieselbe Dimension.

Beweis Falls $w \notin \operatorname{im} f$, dann $f^{-1}(\{w\}) = \emptyset$. Im Folgenden sei $w \in \operatorname{im} f$. zu zeigen: $f^{-1}(\{w\}) = u + \ker f$ „$\subseteq$“ Sei $v \in f^{-1}(\{w\}) \implies f(v) = w = f(u) \implies f(v) - f(u) = 0 \implies f(v-u) = 0 \implies v - u \in \ker f \implies v \in u + \ker f$. „$\supseteq$“ Sei $v \in u + \ker f \implies \exists t \in \ker f : v = u + t \implies f(v) = f(u+t) = f(u) + \underbrace{f(t)}_{=0} = f(u) \implies v \in f^{-1}(\{w\})$. Es ist $\dim(u + \ker f) = \dim(\ker f) = \dim V - \dim \operatorname{im} f$ □

Beispiel 10.8 (13.6) $K = \mathbb{R}, V = \mathbb{R}^2$. Wir betrachten die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$,

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \end{pmatrix}$$

f ist linear und es ist $\operatorname{im} f = \operatorname{Lin}((e_1))$, $\ker f = \operatorname{Lin}((e_2))$ und für $w = \lambda e_1 = \begin{pmatrix} \lambda \\ 0 \end{pmatrix} \in \operatorname{im} f$ ist $f^{-1}(\{w\}) = f^{-1}\left(\begin{pmatrix} \lambda \\ 0 \end{pmatrix}\right) = \begin{pmatrix} \lambda \\ 5 \end{pmatrix} + \ker f = \begin{pmatrix} \lambda \\ 5 \end{pmatrix} + \operatorname{Lin}((e_2))$

Ziel: Wir haben gesehen, dass der Kern einer linearen Abbildung $f : V \to W$ ein UVR von V ist und dass für jedes $w \in W$ die Faser von f über w ein affiner UR von V ist. Wir wollen nun zu einem gegebenen UVR $U \subseteq V$ einen UR W und eine lineare Abbildung $f : V \to W$ konstruieren, sodass $U = \ker f$ ist (beziehungsweise dass ein gegebener affiner UR von V eine Faser von f ist)

Bemerkung 10.9 (13.7) $U \subseteq V$ UVR. Dann ist durch $a \sim_U b \overset{\text{Def}}{\iff} a - b \in U$ eine Äquivalenzrelation auf V gegeben. Anstelle von $s \sim_U b$ schreiben wir auch $a \equiv b(\mod U)$ („a kongruent b modulo U“). Die Äquivalenzklasse von $a \in V$ ist gegeben durch

$$\bar{a} := a + U$$

und heißt die **Restklasse** von a modulo U. Die Menge aller Äquivalenzklassen modulo U bezeichnen wir mit $\frac{V}{U}$.

Beweis 1. „≡“ ist eine Äquivalenzrelation:

- „≡“ ist reflexiv: Für $a \in V$ ist $a \equiv a(\mod U)$, denn $a - a = 0 \in U$
- „≡“ ist symmetrisch: Seien $a, b \in V$ mit $a \equiv b(\mod U)$, dann $a - b \in U \implies b - a = -(a - b) \in U \implies b \equiv a(\mod U)$
- „≡“ ist transitiv: Seien $a, b \in V$ mit $a \equiv b(\mod U), b \equiv (\mod U) \implies a - b \in U, b - c \in U \implies a - c = (a - b) + (b - c) \in U \implies a \equiv c(\mod U)$

2. Die Äquivalenzklasse von $a \in V$ ist gegeben durch

$$\begin{aligned}\bar{a} &= \{b \in V \mid b \equiv a(\mod U)\} = \{b \in V \mid b - a \in U\} \\ &= \{b \in V \mid \exists\, u \in U : b - a = u\} \\ &= \{b \in V \mid \exists\, u \in U : b = a + u\} = a + U\end{aligned}$$

□

Satz 10.10 (13.8) $U \subseteq V$ UVR. Wir definieren auf V/U Verknüpfungen

- $+ : V/U \times V/U \to V/U, \bar{a} + \bar{b} := \overline{a + b}$
- $\cdot : K \times V/U \to V/U, \lambda \cdot \bar{a} := \overline{\lambda a}$

Dann gilt:

1. V/U wird mit der obigen Addition und skalaren Multiplikation zu einem K-Vektorraum, dem **Faktorvektorraum** (**Faktorraum**, **Quotientenvektorraum**) von V/U. Der Nullvektor in V/U ist $\bar{0} = 0 + u = u$
2. Die Abbildung
$$\pi : V \to V/U, a \mapsto \bar{a}$$
ist die surjektiv lineare Abbildung mit $\ker \pi = U$
3. Ist V endlichdimensional, dann ist $\dim_K V/U = \dim_K V - \dim_K U$

Beweis 1. a) „+“„
$cdot$“ wohldefiniert:
„+“ wohldefiniert: Seien $a_1, a_2, b_1, b_2 \in V, \bar{a}_1 = \bar{a}_2, \bar{b}_1 = \bar{b}_2 \implies a_1 \equiv a_1(\mod u), b_1 \equiv b_2(\mod u) \implies a_1 - a_2 \in U, b_1 - b_2 \in U \implies (a_1 + b_1 - (a_2 + b_2)) = \left(\underbrace{a_1 - a_2}_{\in U}\right) + \left(\underbrace{b_1 - b_2}_{\in U}\right) \in U \implies a_1 + b_2 \equiv a_2 + b_2(\mod u) \implies \overline{a_1 + b_1} = \overline{a_2 + b_2}$
„·“ wohldefiniert: Seien $\lambda \in K, a_1, a_2 \in V, \bar{a}_1 = \bar{a}_2 \implies a_1 - a_2 \in U \implies \lambda a_1 - \lambda a_2 = \lambda\left(\underbrace{a_1 - a_2}_{\in U}\right) \in U \implies \lambda a_1 \equiv \lambda a_2(\mod U) \implies \overline{\lambda a_1} = \overline{\lambda a_2}$

b) Vekorraumaxiome gelten: nachrechnen.
Nullvektor: $\forall\, a \in V : \bar{a} + \bar{0} = \overline{a + 0} = \bar{a} = \bar{0} + \bar{a}, \bar{0} = 0 + U$

2.
- π ist linear: Seien $a_1, a_2 \in V, \lambda \in K$, dann $\pi(a_1 + a_2) = \overline{a_1 + a_2} = \bar{a}_1 + \bar{a}_2 = \pi(a_1) + \pi(a_2), \pi(\lambda a_1) = \overline{\lambda a_1} = \lambda \bar{a}_1 = \lambda \pi(a_1)$
- π ist surjektiv: $\operatorname{im} \pi = \pi(V) = \{\bar{a} \mid a \in V\} = V/U$

- $\ker \pi = U$, denn: Sei $a \in V$. Dann gilt:

$$\dim_K V = \dim_K(\ker \pi) + \dim_K(\operatorname{im} \pi) = \dim_K U + \dim_K V/U \implies \text{Behauptung} \quad \square$$

Folgerung 10.11 (13.9) $U \subseteq V$. Dann sind äquivalent:

1. U ist UVR von V
2. Es gibt einen K-Vektorraum W und eine lineare Abbildung $F : V \to W$ mit $\ker f = U$. Ist V endlichdimensional, dann kann in diesem Fall W auch endlichdimensional mit $\dim W \leq \dim V$ gewählt werden.

Beweis 1. $\implies$ 2. Setze $W := V/U, v := \pi, V \to V/U, a \mapsto \bar{a}$, Behauptung folgt aus 12.8. (Zusatzaussage folgt aus 13.8: $\dim_K V/U \leq \dim_K V$)

2. $\implies$ 1. $\ker f$ ist UVR von V nach 12.10 $\square$

Folgerung 10.12 (13.10) $A \subseteq V$. Dann sind äquivalent:

1. A ist ein affiner Unterraum von V
2. Es gibt einen K-Vektorraum W, eine lineare Abbildung $f : V \to W$ und ein $w \in W$ mit $A = f^{-1}(\{w\})$. ist V endlichdimensional, dann kann in diesem Fall auch W endlichdimensional, mit $\dim W \leq \dim V$ gewählt werden.

Beweis 1. $\implies$ 2. Sei A affiner Unterraum von V. Falls $A = \emptyset$, setze $W := K, f : V \to K, v \mapsto 0$ (ist linear), $w := 1 \implies f^{-1}(\{w\}) = \emptyset = A$. Im Folgenden sei $A \neq \emptyset$. Dann $\exists\, a \in V, U \subseteq V$ UVR mit $A = a + U$. Setze $W := V/U, f := \pi V \to V/U, v \mapsto \bar{v}, w := \bar{a} = a + U \implies f^{-1}(\{\bar{a}\}) = \{b \in V \mid f(v) = \bar{a}\} = \{b \in B \mid \bar{b} = \bar{a}\} = \bar{a} = a + U = A$ (Zusatzaussage folgt aus 13.8)

2. $\implies$ 1. $f^{-1}(\{w\})$ ist ein affiner Unterraum. $\square$

Bemerkung 10.13 Philosophie hinter 13.9 / 13.10: UVR = Kerne von lineare Abbildungen, affine Unterräume = Fasern von linearen Abbildungen.

Satz 10.14 (13.11 Homomorphiesatz) $f : V \to W$ lineare Abbildung. Dann induziert f einen Isomorphismus

$$\bar{f} : V/\ker f \to \operatorname{im} f, \bar{v} \mapsto f(v)$$

das heißt: $V/\ker f \cong \operatorname{im} f$

Beweis 1. $\bar{f}$ wohldefiniert: Seien $v_1, v_2 \in V$ mit $\bar{v}_1 = \bar{v}_2 \implies v_1 \equiv v_2 (\mod \ker f) \implies v_1 - v_2 \in \ker \implies f(v_1 - v_2) = 0 \implies f(v_1) = f(v_2) f$

   - Für $v \in V$ ist $f(v) \in \operatorname{im} f$.

2. $\bar{f}$ ist linear: Seien $\bar{v}_1, \bar{v}_2 \in V/\ker f \implies \bar{f}(\bar{v}_1 + \bar{v}_2) = \bar{f}(\overline{v_1 + v_2}) = f(v_1 + v_2) = f(v_1) + f(v_2) = \bar{f}(\bar{v}_1) + \bar{f}(\bar{v}_2)$ Sei $\lambda \in K, \bar{v} \in V/\ker f \implies \bar{f}(\lambda \bar{v}) = \bar{f}(\overline{\lambda v}) = f(\lambda v) = \lambda f(v) = \lambda \bar{f}(\bar{v})$.
3. $\bar{f}$ ist injektiv, das heißt $\ker \bar{f} = \{0\}$. Sei $\bar{v} \in \ker \bar{f} \implies \bar{f}(\bar{v}) = 0 \implies f(v) = 0 \implies v \in \ker f \implies \bar{v} = v + \ker f = \ker f = \bar{0}$
4. $\bar{f}$ ist surjektiv, dann $\operatorname{im} \bar{f} = \{\bar{f}(\bar{v}) \mid \bar{v} \in V/\ker f\} = \{f(v) \mid v \in V\} = \operatorname{im} f$ $\square$

Folgerung 10.15 (13.12) $f : V \to W$ lineare Abbildung. Dann lässt sich f schreiben als

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

wobei $\pi : V \to V/\ker f, v \mapsto \bar{v}, \bar{f}$: Abbildung aus 1311, $i : \operatorname{im} f \to W, w \mapsto w$ Man sagt auch: das Diagramm

$$\begin{tikzcd} V \arrow[r, "f"'] \arrow[d, "\pi"'] & W \\ V/\ker f \arrow[r, "\bar{f}"'] & \operatorname{im} f \arrow[u, "i"] \end{tikzcd}$$

kommutiert. Hierbei ist π surjektiv, $\bar{f}$ ein Isomorphismus, i ist surjektiv.

Beweis Für $v \in V$ ist $\left(i \circ \bar{f} \circ \pi\right)(v) = \left(i \circ \bar{f}\right)(\bar{v}) = i(f(v)) = f(v)$ □

Bemerkung 10.16 Für einen UVR $U \subseteq V$ nennt man die Abbildung $\pi : V \to V/U, v \mapsto \bar{v}$ die kanonische Projektion von V nach V/U

11 Lineare Gleichungssysteme

In diesem Abschnitt seien stets $m, n \in \mathbb{N}, A = (a_{ij}) \in M(m \times n, K), b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ im K^m Ziel: bestimme alle $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ mit $Ax = b$, das heißt löse das lineare Gleichungssystem $Ax = b$. explizit

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

Die Matrix A induziert eine lineare Abbildung $\tilde{A} : K^n \to K^m, x \mapsto Ax$, das heißt: Bestimmung der Lösungsmenge von $Ax = b$ korrespondiert zur Bestimmung der Faser $\tilde{A}^{-1}(b)$

Definition 11.1 (14.1) Das Lineare Gleichungssystem $Ax = b$

- **homogen** $\overset{\text{Def}}{\iff} b = 0$
- **inhomogen** $\overset{\text{Def}}{\iff} b \neq 0$

Das LGS $Ax = 0$ heißt das zu $Ax = b$ gehörige homogene LGS. A heißt die **Koeffizientenmatrix** des LGS $Ax = b$. $\text{Lös}(A, b) := \{x \in K^n \mid Ax = b = \tilde{A}^{-1}(\{b\})\}$ heißt der Lösungsraum des LGS $Ax = b$. Insbesondere ist $\text{Lös}(A, 0) = \ker \tilde{A}$.

Satz 11.2 (14.2) Es gilt:

1. $\text{Lös}(A, 0) \subseteq K^n$ ist ein UVR der Dimension $u - \text{Rang}(A)$.
2. $\text{Lös}(A, b) \subseteq K^n$ ist ein affiner Unterraum von K^n. Ist $\text{Lös}(A, b) \neq \emptyset$ dann hat dieser die Dimension $n - \text{Rang}(A)$
3. Ist $\text{Lös}(A, b) \neq \emptyset$ und $v \in \text{Lös}(A, b)$, dann ist $\text{Lös}(A, b) = v + \text{Lös}(A, 0)$

Beweis 1. Es ist $\text{Lös}(A, 0) = \ker \tilde{A}$, $\ker \tilde{A}$ ist ein UVR von K^n mit $\dim\left(\ker \tilde{A}\right) = \dim(K^n) - \dim\left(\text{im } \tilde{A}\right) = n - \text{Rang}\left(\tilde{A}\right) = n - \text{Rang}(A)$

2. Es ist $\text{Lös}(A, b) = \tilde{A}^{-1}(\{b\})$, dies ist nach 13.5 ein affiner UR von K^n. Falls $\text{Lös}(A, b) \neq \emptyset$, dann ist $b \in \text{im } \tilde{A}$ und $\dim \text{Lös}(A, b) = \dim(\{b\}) = \dim \ker \tilde{A} = u - \text{Rang } A$

3. Falls $\text{Lös}(A, b) \neq \emptyset, v \in \text{Lös}(A, b)$, dann

$$\text{Lös}(A, b) = \tilde{A}^{-1}(\{b\}) = v + \ker \tilde{A} = v + \text{Lös}(A, 0)$$ □

Anmerkung 11.3 • $\text{Lös}(A, 0)$ enthält immer die triviale Lösung 0, nichttriviale Lösung von $Ax = 0$ gibt es wegen 1. genau dann, wenn $\text{Rang } A < n$

Definition 11.4 (14.3)

$$A \mid b := \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{pmatrix} \subseteq M(m \times (n+1), K)$$

heißt die erweiterte Koeffizientenmatrix des LGS $Ax = b$.

Satz 11.5 (14.4) Es sind äquivalent:

1. $\text{Lös}(A, b) \neq \emptyset$, das heißt LGS $Ax = b$ besitzt eine Lösung
2. $\text{Rang}(A) = \text{Rang}(A \mid b)$

Beweis 1. Es ist $\text{im } \tilde{A} = \tilde{A}(K^n) = \tilde{A}(\text{Lin}(e_1, \dots, e_n)) = \text{Lin}\left(\tilde{A}(e_1), \dots, \tilde{A}(e_n)\right) = \text{Lin}(Ae_1, \dots, Ae_n)$ und es ist $\text{im } \widetilde{A \mid b} = \widetilde{A \mid b}(K^{n+1}) = \widetilde{A \mid b}(\text{Lin}(e_1, \dots, e_{n+1})) = \text{Lin}\left(\widetilde{A \mid b}(e_1), \dots, \widetilde{A \mid b}(e_n), \widetilde{A \mid b}(e_{n+1})\right) = \text{Lin}((A \mid b)e_1, \dots, (A \mid b)e_n, (A \mid b)e_{n+1}) = \text{Lin}(Ae_1, \dots, Ae_n, b)$ insbesondere $\text{im } \tilde{A} \subseteq \text{im } \widetilde{A \mid b}$

2. Also $\text{Lös}(A, b) \neq \emptyset \iff b \in \text{im } \tilde{A} \iff \widetilde{A \mid b} \iff \dim \text{im } \tilde{A} = \dim \text{im } \widetilde{A \mid b} \iff \text{Rang } \tilde{A} = \text{Rang } \widetilde{A \mid b} \iff \text{Rang } A = \text{Rang } A \mid b$ □

Folgerung 11.6 (14.5) Es sind äquivalent:

1. Das LGS $Ax = b$ besitzt genau eine Lösung
2. $\text{Rang}(A) = \text{Rang}(A \mid b) = n$

Beweis 1. $\implies$ 2. Das LGS $Ax = b$ besitze genau eine Lösung. Aus der Existenz einer Lösung folgt nach 14.4: $\text{Rang } A = \text{Rang}(A \mid b)$ aus der Eindeutigkeit folgt $\dim \text{Lös}(A, b) = 0$, also nach 14.2:

$$0 = \dim \text{Lös}(A, b) = n - \text{Rang}(A)$$

also $\text{Rang}(A) = n$

2. $\implies$ 1. Sei $\mathrm{Rang}(A) = \mathrm{Rang}(A \mid b) = n \implies$ $\text{Lös}(A,b) \neq \emptyset$ nach 14.2 ist $\dim \text{Lös}(A,b) = n - \mathrm{Rang}(A) = 0$, das heißt die Lösung ist eindeutig bestimmt. □

Ziel: Algorithmus zur Bestimmung von Lös(A, b)

Definition 11.7 (14.6) A ist in **strenger Zeilenstufenform** (SZSF) $\overset{\text{Def}}{\iff}$ A ist in ZSF mit Pivotspalten bei $j_1, \ldots, j_r$ und es gilt:

- (SZ1) $a_{1j_1} = \ldots = a_{rj_r} = 1$
- (SZ2) $a_{ij_k} = 0 \,\forall\, k \in \{1, \ldots, r\}, i \in \{1, \ldots, k-1\}$

Satz 11.8 (14.7) A lässt sich durch elementare Zeilenumformung auf SZSF bringen.

Beweis Bringe A auf ZSF B nach Satz 10.11. Multipliziere die i-te Zeile für $i = 1, \ldots r$ mit $\frac{1}{b_{ij_i}}$ und annulliere dann die Einträge der j_k -ten Spalte oberhalb des Pivotelements durch Subtraktion geeigneter Vielfacher der k -ten Zeile. □

Beispiel 11.9 (14.8)

$$A = \begin{pmatrix} 0 & 0 & 3 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix} \in M(3 \times 4, \mathbb{R}) \to \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & -\frac{1}{3} \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 0 & \frac{2}{3} \\ 0 & 0 & 1 & -\frac{1}{3} \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{32}$$

Anmerkung 11.10 Die strenge ZSF von A ist eindeutig bestimmt (vergleiche Blatt 11 ZA 5)

Bemerkung 11.11 (14.9) $C \in M(m \times n, K), d \in K^m$ ist $C \mid d$ durch eine Folge elementarer Zeilenumformungen aus $A \mid b$ entstanden, dann ist Lös$(C, d) =$ Lös(A, b)

Beweis Wegen Anmerkung nach 10.5 genügt es, einzelne Zeilenumformungen von Typ 1. beziehungsweise 2. zu betrachten

1. Typ 1-Umformungen

$$A \mid b = \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & & & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{pmatrix} \quad C \mid d = \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & & & \vdots \\ \lambda a_{j1} & \ldots & \lambda a_{jn} & \lambda b_j \\ \vdots & & & \vdots a_{m1} & \ldots & a_{mn} & b_m \end{pmatrix}$$

mit $\lambda \in K^x$. Es ist $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \text{Lös}(A, b) \iff$

$$a_{11}x_1 + \ldots + a_{1n}x_n = b_1$$

$$\vdots a_{m1}x_1 + \ldots + a_{mn}x_n \qquad = b_m$$

$\iff$

$$a_{11}x_1 + \ldots + a_{1n}x_n = b_1$$

$$\vdots \lambda a_{j1}x_1 + \ldots + a_{jn}x_n \qquad = b_j$$

$$\vdots a_{m1}x_1 + \ldots + a_{mn}x_n \qquad = b_m$$

$\iff$

$$x \in \text{Lös}(C, d)$$

2. Typ 2-Umformung: analog ☐

Algorithmus 11.12 (14.10 Gauß-Algorithmus zur Lösung homogener LGS) **Eingabe**: $A \in M(m \times n, K)$
Ausgabe: eine Basis von Lös$(A, 0)$
Durchführung:

1. Bringe die Matrix A durch elementare Zeilenumformung auf SZSF S:

$$S = \begin{pmatrix} 1 & * & 0 & & & 0 \\ & & 1 & * & \vdots & * \\ & & & & 0 & \\ & & & & 1 & \\ & & & & & \end{pmatrix} \tag{33}$$

Mit den Spalten $j_1, \ldots, j_r$ als die Spalten der Pivot-Elemente, $r =$ Zeilenrang (A)

2. Sei $B \in M(r \times (n - r), K)$, die aus S durch Streichen der Spalten mit den Indizes $j_1, \ldots, j_r$ und der Zeilen mit den Indizes $r + 1, \ldots, m$ entsteht. Seinen $k_1 < k_2 < \ldots < k_{n-r}$ mit $\{1, \ldots, n\} = \{j_1, \ldots, j_r, k_1, \ldots, k_{n-1}\}$

3. Eine Basis von Lös$(A, 0)$ ist gegeben durch $(w_1, \ldots, w_{n-r})$, wobei

$$w_i = \begin{pmatrix} w_{i_1} \\ \vdots \\ w_{i_n} \end{pmatrix} \in K^n$$

für $i = 1, \ldots, n - r$ wie folgt gegeben ist:

$$\begin{pmatrix} w_{ij_1} \\ \vdots \\ w_{ij_r} \end{pmatrix} = \text{ i-te Spalte von B, } \begin{pmatrix} w_{ik_1} \\ \vdots \\ w_{ik_{n-r}} \end{pmatrix} = e^i \in k^n - r$$

Beweis Nach 14.9 ist Lös$(A, 0) =$ Lös$(B, 0)$. Es ist $x \in$ Lös$(S, 0) \iff Sx = 0 \iff$

$$0 = \begin{pmatrix} x_{j_1} \\ x_{j_2} \\ \vdots \\ x_{j_r} \end{pmatrix} + B \begin{pmatrix} x_{k_{n1}} \\ \vdots \\ x_{k_{n-r}} \end{pmatrix} \iff - \begin{pmatrix} x_{j_1} \\ x_{j_2} \\ \vdots \\ x_{j_r} \end{pmatrix} = B \begin{pmatrix} x_{k_1} \\ \vdots \\ x_{k_{n-r}} \end{pmatrix}$$

das heißt nach beliebiger Vorgabe von $x_{k_1}, \ldots, x_{k_{n-r}}$ ergeben sich $x_{j_1}, \ldots, x_{j_r}$ eindeutig. Setzen wir

$$\begin{pmatrix} x_{k_1} \\ \vdots \\ x_{k_{n-r}} \end{pmatrix} = e_i \in K^{n-r}$$

für $i = 1, \ldots, n-r$, dann ist

$$\begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_r} \end{pmatrix}$$

die i-te Spalte von $-B$. Das heißt auf diese Weise erhalten wir $w_1, \ldots, w_{n-1}$. $(w_1, \ldots, w_{n-r})$ ist nach Konstruktion ein ES von $\text{Lös}(A, 0) = \text{Lös}(S, 0)$ wegen

$$K^{n-r} = \text{Lin}((e_1, \ldots, e_{n-r}))$$

$(w_1, \ldots, w_{n-r})$ ist linear unabhängig, denn: Seinen $\lambda_1, \ldots, \lambda_{n-r} \in K$ mit

$$\lambda_1 w_1 + \ldots + \lambda_{n-r} w_{n-r} = 0$$

Für $i = 1, \ldots, n-r$ lautet Eintrag in k_1 -ter Zeile:

$$\lambda_1 \underbrace{w_{1k_i}}_{=0} + \ldots + \lambda_{i-1} \underbrace{w_{i-1,k_i}}_{=0} + \lambda_i \underbrace{w_{i,k_i}}_{=1} + \lambda_{i+1} \underbrace{w_{i+1,k_i}}_{=0} + \ldots + \lambda_{n-r} \underbrace{w_{n-r,k_i}}_{=0} = 0$$

$$\implies \lambda_i \cdot i = 0 \implies \lambda_i = 0, i = 1, \ldots, n-r$$ □

Folgerung 11.13 (14.11) Es gilt: Zeilenrang(A) = Spaltenrang(A) = $\text{Rang}(A)$

Beweis In 14.10 haben wir gezeigt: $\dim \text{Lös}(A, 0) = n-$ Zeilenrang(A), nach 14.2 ist $\dim \text{Lös}(A, 0) = n - \text{Rang}(A) = n-$ Spaltenrang(A) $\implies$ Zeilenrang(A) = Spaltenrang (A) □

Beispiel 11.14 (14.12) Sei

$$A = \begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \in M(3 \times 4, \mathbb{R})$$

gesucht ist eine Basis von $\text{Lös}(A, 0) \subseteq \mathbb{R}^4$

$$A \to \begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & 6 \\ 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{34}$$

Insbesondere ist $\text{Rang}(A) = 2, \dim \text{Lös}(A, 0) = 4 - \text{Rang}(A) = 2$. Es ist $j_1 = 1, j_2 = 3$. Wegen $\{1, 2, 3, 4\} = \{j_1, j_2, k_1, k_2\}$ und $k_1 < k_2$ ist $k_1 = 2, k_2 = 4$. Es ist

$$B = \begin{pmatrix} 2 & 6 \\ 0 & -3 \end{pmatrix}, -B = \begin{pmatrix} -2 & -6 \\ 0 & 3 \end{pmatrix} \tag{35}$$

Eine Basis von $\text{Lös}(A, 0)$ ist gegeben durch (w_1, w_2) mit

$$w_1 = \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, w_2 = \begin{pmatrix} -6 \\ 0 \\ 3 \\ 1 \end{pmatrix}$$

Algorithmus 11.15 (14.13 Gauß-Algorithmus zur Lösung inhomogener LGS) **Eingabe**: $A \in M(m \times n, K), b \in K^m, b \neq 0$
Ausgabe: Lös(A, b)
Durchführung:

1. Bringe die Matrix $A \mid b$ durch elementare Zeilenumformung auf SZSF $S \mid s$
$$S = \begin{pmatrix} 1 & * & 0 & & & 0 & & s_1 \\ & & 1 & * & \vdots & * & \vdots & \\ & & & & 0 & & & \\ & & & & 1 & & s_r & \\ & & & & & & 0 & \end{pmatrix} \in M(m \times (n+1), K), r = \mathrm{Rang}(A \mid b) \tag{36}$$
2. Falls $j_r = n + 1$, dann ist Lös$(A, b) = \emptyset$
3. Falls $j_r < n + 1$, dann ist eine spezielle Lösung von $Ax = b$ gegeben durch
$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in K^n$$
wobei
$$v_{j_1}; \because; v_{j_r} = \vdots s_1; \because; s_r, i \in \{1, \dots, n\} \setminus \{j_1, \dots, j_r\} \implies v_i = 0$$
Es ist Lös$(A, b) = v +$ Lös$(A, 0)$, wobei Lös$(A, 0)$ mittels 14.10 bestimmt.

Beweis Wegen $S \mid s \in M(m \times (n+1), K)$ ist $j_r \leq n + 1$. Falls $j_r = n + 1$, dann ist $\mathrm{Rang}(A \mid b) =$ Spaltenrang$(A \mid b) =$ Zeilenrang$(A \mid b) =$ Zeilenrang$(S \mid s) =$ Spaltenrang$(S \mid s) >$ Spaltenrang$(S) = \mathrm{Rang}(A) \implies$ Lös$(A, b) = \emptyset$. Falls $j_r < n + 1$, dann ist v aus Schritt 3 eine spezielle Lösung von $Sx = s$, also auch von $Ax = b$ wegen 14.9. Somit ist Lös$(A, b) = v +$ Lös$(A, 0)$ nach 14.2. $\square$

Beispiel 11.16 (14.14) Wir betrachten das LGS $Ax = b$ mit
$$A = \begin{pmatrix} 2 & 4 & 2 & 6 \\ 3 & 6 & 3 & 9 \\ 4 & 8 & 5 & 9 \end{pmatrix} \in M(3 \times 4, \mathbb{R}), b = \begin{pmatrix} 4 \\ 6 \\ 9 \end{pmatrix} \in \mathbb{R}^3$$

$$A \mid b \to \begin{pmatrix} 2 & 4 & 2 & 6 & 4 \\ 3 & 6 & 3 & 9 & 6 \\ 4 & 8 & 5 & 9 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 3 & 6 & 3 & 9 & 6 \\ 4 & 8 & 5 & 9 & 9 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -3 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 3 & 2 \\ 0 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & 6 \\ 0 & 0 & 1 & - \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{37}$$

Es ist $\mathrm{Rang}(A \mid b) = \mathrm{Rang}(A) = 2$, insbesondere ist Lös$(A, b) \neq \emptyset$, dim Lös$(A, b) = 4 - \mathrm{Rang}(A) = 2$. Es ist $j_1 = 1, j_2 = 3$. Eine spezielle Lösung von $Ax = b$ ist nach 14.13 gegeben durch
$$v = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Nach Beispiel 14.12 ist
$$\text{Lös}(A, b) = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mathrm{Lin}\left(\begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -6 \\ 0 \\ 3 \\ 1 \end{pmatrix} \right) = \{ \begin{pmatrix} 1 - 2\lambda - 6\mu \\ \lambda \\ 1 + 3\mu \\ \mu \end{pmatrix} \mid \lambda, \mu \in \mathbb{R}\}$$

12 Lineare Abbildungen und Matrizen

In diesem Abschnitt seien V, W endlichdimensionale K-VR.

Satz 12.1 (15.1) $v_1, \dots, v_r \in V, w_1, \dots, w_r \in W$. dann gilt:

1. Ist $(v_1, \dots, v_r)$ linear unabhängig, dann gibt es eine lineare Abbildung $f : V \to W$ mit $f(v_i) = w_i$ für $i = 1, \dots, r$
2. Ist $(v_1, \dots, v_r)$ eine Basis von V, dann gibt es genau ein lineare Abbildung $f : V \to W$ mit $f(v_i) = w_i$ für $i = 1, \dots, r$. Diese Abbildung hat die folgenden Eigenschaften
   - $\operatorname{im} f = \operatorname{Lin}((w_1, \dots, w_r))$, insbesondere f surjektiv $\iff (w_1, \dots, w_r)$ ES von W
   - f injektiv $\iff (w_1, \dots, w_r)$ linear unabhängig
   - f Isomorphismus $\iff (w_1, \dots, w_r)$ Basis von W

Beweis (2):

1. Existenz: Für $v \in V$ existieren eindeutig bestimmte $\lambda_1, \dots, \lambda_r \in K$ mit $v = \lambda_1 v_1 + \ldots + \lambda_r v_r$. Wir setzen $f : V \to W, v \mapsto \lambda w_1 + \ldots + \lambda_r w_r$, dann ist insbesondere $f(v_i) = w_i$ f+r $i = 1, \dots, r$. Behauptung: f linear, denn Seien $u, v \in U$ mit $u = \lambda_1 v_1 + \ldots + \lambda_r v_r, v = \mu_1 v_1 + \ldots + \mu_r v_r$

   $$\implies f(u+v) = f((\lambda_1 + \mu_1)v_1 + \ldots + (\lambda_r + \mu_r)v_r) = (\lambda_1 + \mu_1)w_1 + \ldots + (\lambda_r + \mu_r)w_r = f(u) + f(v)$$

   Ist $\lambda \in K, v \in V$ wie oben, dann ist

   $$f(\lambda v) = f(\lambda\mu_1 v_1 + \ldots + \lambda\mu_r v_r) = \lambda\mu_1 w_1 + \ldots + \lambda\mu_r w_r = \lambda f(v)$$

2. Eindeutigkeit: Sei $f : V \to W$ eine weitere lineare Abbildung $g(v_i) = w_i$ für $i = 1, \dots, r \implies$ Für $v \in V$ mit $v = \lambda_1 v_1 + \ldots + \lambda_r v_r$ ist dann

   $$g(v) = \lambda_1 g(v_1) + \ldots + \lambda_r g(v_r) = \lambda w_1 + \ldots + \lambda_r w_r = f(v) \implies f = g$$

3. Eigenschaften von f:
   - $\operatorname{im} f = \operatorname{Lin}((f(v_1), \dots, f(v_r))) = \operatorname{Lin}((w_1, \dots, w_r))$
   - f injektiv $\iff (w_1, \dots, w_r)$ linear unabhängig, denn:
     „$\implies$" (durch Kontraposition) Sei $(w_1, \dots, w_r)$ linear abhängig $\implies \exists\, \mu_1, \dots, \mu_r \in K$ mit

     $(\mu_1, \dots, \mu_r) \neq (0, \dots, 0)$ und $\mu_1 w_1 + \ldots + \mu_r w_r = 0 \implies f\left(\underbrace{\mu_1 v_1 + \ldots + \mu_r v_r}_{\neq 0}\right) = 0 \implies$

     f nicht injektiv
     „$\impliedby$" Sei $w_1, \dots, w_r$ linear unabhängig. Sei $v \in V$ mit $f(v) = 0, v = \lambda_1 v_1 + \ldots + \lambda_r v_r \implies$ $f(v) = \lambda_1 w_1 + \ldots + \lambda_r w_r = 0 \implies \lambda_1 = \ldots = \lambda_r = 0 \implies v = 0$

(1):
Sei $(v_1, \dots, v_r)$ linear unabhängig $\implies (v_1, \dots, v_r)$ kann zu Basis $(v_1, \dots, v_r, v_{r+1}, \dots, v_n)$ von V ergänzt werden. Wir wählen $w_{r+1}, \dots, w_n \in W$ beliebig. Dann existiert nach 2. eine lineare Abbildung $f : V \to W$ mit $f(v_i) = w_i$ für $i = 1, \dots, n$, insbesondere ist $f(v_i) = w_i$ für $i = 1, \dots, r$ $\square$

Folgerung 12.2 (15.2) $\mathcal{B} = (v_1, \ldots, v_2)$ Basis von V. Dann gibt es genau einen Isomorphismus

$$\Phi_{\mathcal{B}} : K^n \to V$$

von K-VR mit $\Phi_{\mathcal{B}}(e_i) = v_i$ für $i = 1, \ldots, n$. $\Phi_{\mathcal{B}}$ heißt das durch $\mathcal{B}$ bestimmte **Koordinatensystem** von V. Ist $v = \lambda_1 v_1 + \ldots + \lambda_n v_n \in V$, dann nennt man $\Phi_{\mathcal{B}}^{-1} = \lambda_1 e_1, \ldots, \lambda_n e_n = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in K^n$ die **Koordinaten** von v bezüglich $\mathcal{B}$

Beweis Wende 15.1.2 auf die Basen $(e_1, \ldots, e_n)$ von K^n und $(v_1, \ldots, v_n)$ von V an. □

Satz 12.3 (15.3) $\mathcal{A} = (v_1, \ldots, v_n)$ Basis von $V, \mathcal{B} = (w_1, \ldots, w_m)$ Basis von W. Dann gilt:

1. Für jede lineare Abbildung $f : V \to W$ gibt es genau eine Matrix $A = (a_{ij}) \in M(m \times n, K)$, sodass

$$f(v_j) = \sum_{j=1}^{m} a_{ij} w_i, j = 1, \ldots, n$$

   $M_{\mathcal{B}}^{\mathcal{A}}(f) := A$ heißt die **Darstellungsmatrix** von f bezüglich der Basen $\mathcal{B}$ und $\mathcal{B}$. In der j-ten Spalte von $M_{\mathcal{B}}^{\mathcal{A}}(f)$ stehen die Koordinaten von $f(v_j)$ bezüglich der Basis von $\mathcal{B}$ von W (für $j = 1, \ldots, n$)

2. Die aus 1. erhaltene Abbildung

$$M_{\mathcal{B}}^{\mathcal{A}} : \mathrm{Hom}_K(V, W) \to M(m \times n, K), f \mapsto M_{\mathcal{B}}^{\mathcal{A}}(f)$$

   ist ein Isomorphismus von K-VR. Insbesondere ist im Fall $V = W, \mathcal{A} = \mathcal{B}$ die Abbildung

$$M_{\mathcal{B}} : \mathrm{End}_K(V) \to M(n \times m, K), f \mapsto M_{\mathcal{B}}(f) := M_{\mathcal{B}}^{\mathcal{B}}(f)$$

   ein Isomorphismus von K-Vektorraum.

Beweis 1. klar, weil $\mathcal{B} = (w_1, \ldots, w_m)$ Basis von W ist.

2. $M_{\mathcal{B}}^{\mathcal{A}}$ ist linear, denn:
   Sind $f, g \in \mathrm{Hom}_K(V, W), \lambda \in K$ mit $M_{\mathcal{B}}^{\mathcal{A}}(f) = (a_{ij}), M_{\mathcal{B}}^{\mathcal{A}}(g) = (b_{ij})$, dann ist

$$(f+g)(v_j) = f(v_j) + g(v_j) = \sum_{i=1}^{m} a_{ij} w_i + \sum_{i=1}^{m} b_{ij} w_i = \sum_{i=1}^{m} (a_{ij} + b_{ij}) w_i, j = 1, \ldots, n w_i, j = 1, \ldots, n$$

   das heißt $M_{\mathcal{B}}^{\mathcal{A}}(f+g) = M_{\mathcal{B}}^{\mathcal{A}}(f) + M_{\mathcal{B}}^{\mathcal{A}}(g)$

$$(\lambda f)(v_j) = \lambda f(v_j) = \lambda \sum_{i=1}^{m} a_{ij} w_i = \sum_{i=1}^{m} (\lambda a_{ij}) w_i, j = 1, \ldots, n$$

   also $M_{\mathcal{B}}^{\mathcal{A}}(\lambda f) = \lambda M_{\mathcal{B}}^{\mathcal{A}}(f)$
   $M_{\mathcal{B}}^{\mathcal{A}}$ ist bijektiv, denn:
   Ist $A = (a_{ij}) \in M(m \times n, K)$, dann existiert nach 15.1.2 genau ein $f \in \mathrm{Hom}_K(V, W)$ mit

$$f(v_j) = \sum_{i=1}^{m} a_{ij} w_i, j = 1, \ldots, n$$

□

Folgerung 12.4 (15.4) Die Abbildung

$$M^{(e_1,\dots,e_n)}_{(e_1,\dots,e_m)} : \operatorname{Hom}_K(K^n, K^m) \to M(m \times n, K)$$

ist ein Isomorphismus von K-VR mit Umkehrabbildung:

$$\sim: M(m \times n, K) \to \operatorname{Hom}_K(K^n, K^m), A \mapsto \tilde{A}$$

Insbesondere ist $\sim$ ebenfalls ein Isomorphismus.

Beweis $M^{(e_1,\dots,e_n)}_{(e_1,\dots,e_m)}$ ist ein Isomorphismus nach 15.3, und für $A \in M(m \times n, K)$ ist $M^{(e_1,\dots,e_n)}_{(e_1,\dots,e_m)}\left(\tilde{A}\right) = A$, da $\tilde{A}(e_j) = Ae_j =$ j-te Spalte von A für $j = 1, \dots, n$ □

Beispiel 12.5 (15.5) $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in M(2 \times 2, \mathbb{R})$. Es ist $M^{(e_1,\dots,e_n)}_{(e_1,\dots,e_m)}\left(\tilde{A}\right) = A$. Es sei $\mathcal{A} = \left(\begin{pmatrix} -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)$, $\mathcal{B} = \left(\begin{pmatrix} 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right)$. Was ist $M^{\mathcal{A}}_{\mathcal{B}}\left(\tilde{A}\right)$?

$$\begin{aligned}
\tilde{A}\left(\begin{pmatrix} -1 \\ 1 \end{pmatrix}\right) &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix} = -\begin{pmatrix} 2 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \end{pmatrix} \\
\tilde{A}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix} = 5\begin{pmatrix} 2 \\ -1 \end{pmatrix} - 7\begin{pmatrix} 1 \\ -1 \end{pmatrix} \\
\implies M^{\mathcal{A}}_{\mathcal{B}}\left(\tilde{A}\right) &= \begin{pmatrix} -1 & 5 \\ 1 & -7 \end{pmatrix}
\end{aligned}$$

Wir haben einen Basiswechsel durchgeführt. Wie das systematisch geht, sehen wir im nächsten Abschnitt.

Folgerung 12.6 (15.6) $A \in M(n \times n, K)$. Dann sind äquivalent:

1. $A \in GL(n, K)$
2. Es gibt ein $B \in M(n \times n, K)$ mit $AB = E_n = BA$
3. Es gibt ein $B \in M(n \times n, K)$ mit $AB = E_n$
4. Es gibt ein $B \in M(n \times n, K)$ mit $BA = E_n$
5. $\tilde{A} : K^n \to K^n$ ist ein Isomorphismus
6. $\operatorname{Rang}(A) = n$

Beweis (1) $\iff$ (2) Definition.
(5) $\iff$ (6) $\tilde{A}$ Isomorphismus $\iff$ $\tilde{A}$ surjektiv $\iff$ $\dim \operatorname{im} \tilde{A} = n$ $\iff$ $\operatorname{Rang} \tilde{A} = n$ $\iff$ $\operatorname{Rang}(A) = n$
(2) $\implies$ (3), (2) $\implies$ (4) trivial
(3) $\implies$ (5) Sei $B \in M(n \times n, K)$ mit $AB = E_n$ $\implies$ $\tilde{A} \circ \tilde{B} = \widetilde{AB} = \tilde{E}_n = \operatorname{id}_{K^n}$ $\implies$ $\tilde{A}$ surjektiv $\implies$ $\tilde{A}$ Isomorphismus
(4) $\implies$ (5) analog
(5) $\implies$ (2) Sei $\tilde{A}$ Isomorphismus $\implies$ $\exists g \in \operatorname{End}_K(K^n) : \tilde{A} \circ g = \operatorname{id}_{K^n} = g \circ \tilde{A}$. Nach 15.4 $\exists B \in M(n \times n, K)$ mit $g = \tilde{B}$, insbesondere $\tilde{A} \circ \tilde{B} = \operatorname{id}_{K^n} = \tilde{B} \circ \tilde{A}$, also $\tilde{A} \circ \tilde{B} = \tilde{E}_n = \tilde{B} \circ \tilde{A}$ $\implies$ $\tilde{E}_n = \widetilde{AB} = \widetilde{BA}$ $\implies$ $E_n = AB = BA$ □

Folgerung 12.7 (15.7) Es gilt:

$$\dim_K \mathrm{Hom}_K(V, W) = \dim_K(V) \cdot \dim_K(W)$$

Beweis Nach Wahl von Basen $\mathcal{A} = (v_1, \dots, v_n)$ von $V, \mathcal{B} = (w_1, \dots, w_n)$ von W erhalten wir nach 15.2 einen Isomorphismus

$$M_{\mathcal{B}}^{\mathcal{A}} : \mathrm{Hom}_K(V, W) \to M(m \times n, K)$$

also ist $\dim_K \mathrm{Hom}_K(V, W) = \dim_K M(m \times n, K) = m \times n = \dim_K W \cdot \dim_K V$ □

Folgerung 12.8 (15.8) $U \subseteq K^n$. Dann sind äquivalent:

1. U ist UVR von K^n
2. Es gibt ein $m \in \mathbb{N}$ und ein $A \in M(m \times n, K)$, sodass $U = \text{Lös}(A, 0)$

Beweis 1. $\implies$ 2. nach 13.9 existiert ein endlichdimensionaler K-VR und eine lineare Abbildung $f : K^n \to W$ mit $\ker f = U$. Sei $m = \dim W$, dass existiert ein Isomorphismus $g : W \to K^m$. Wir setzen

$$\phi := g \circ f : K^n \to K^m$$

Es ist $\ker \phi = \ker f$, denn: Für $v \in K^n$ ist $f(v) = 0 \iff g(f(v)) = g(0) = 0 \iff \phi(v) = 0$, also $\ker \phi = U$. Nach 15.4 existiert $A \in M(m \times n, K)$ mit $\phi = \tilde{A} \implies U = \ker \phi = \ker \tilde{A} = \text{Lös}(A, 0)$

2. $\implies$ 1. aus Satz 14.2 □

Folgerung 12.9 (15.9) $U \subseteq K^n$. Dann sind äquivalent:

1. U ist affiner UR von K^n
2. Es gibt $m \in \mathbb{N}, A \in M(m \times n, K), b \in K^m$, sodass $U = \text{Lös}(A, b)$

Beweis 1. $\implies$ 2. Nach 13.10 Existiert ein endlichdimensionaler K-VR, $W, w \in W$ und eine lineare Abbildung $K^n \to W$ mit $U = f^{-1}(\{w\})$. Sei $m = \dim W$, dass Existiert ein Isomorphismus $g : W \to K^m$. Wir setzten $\phi := g \circ g : K^n \to K^m$. Es ist $f^{-1}(\{w\}) = \phi^{-1}(\{b\})$, wobei $b := g(w)$, denn für $v \in K^n$ ist

$$f(v) = w \iff g(f(v)) = g(w) = b \iff \phi(v) = b$$

Nach 15.4 existiert ein $A \in M(m \times n, K)$ mit $\phi = \tilde{A} \implies U = \phi^{-1}(\{b\}) = \tilde{A}^{-1}(\{b\}) = \text{Lös}(A, b)$

2. $\implies$ 1. aus Satz 14.2 □

Anmerkung 12.10 Philosophie hinter 15.8/15.9: affine UR von K^n = Lösungsräume von LGS (in n Variablen) über K, UVR von K^n = Lösungsräume homogener GLS (in n Variablen) über K

Frage: $f : V \to W$ lineare Abbildung, Wie einfach kann man $M_{\mathcal{B}}^{\mathcal{A}}(f)$ durch geeignete Wahl von $\mathcal{A}, \mathcal{B}$ bekommen?

Bemerkung 12.11 (15.19) $f : V \to W$ lineare Abbildung. Dann gibt es Basen $\mathcal{A}$ von V, $\mathcal{B}$ von W mit

$$M_{\mathcal{B}}^{\mathcal{A}}(f) = \begin{pmatrix} E_r & \\ & 0 \end{pmatrix}, r = \text{Rang } f$$

Beweis Sei $\mathcal{B} := (w_1, \dots, w_r)$ Basis von $\operatorname{im} f$. Sind $u_1 \in f^{-1}(\{w_1\}), \dots, u_r \in f^{-1}(\{w_r\})$ und ist $(v_1, \dots, v_k)$ eine Basis von $\ker f$, dann ist nach 12.13

$$\mathcal{A} := (u_1, \dots, u_r, v_1, \dots, v_k)$$

eine Basis von V. Nach Konstruktion ist $f(u_1) = w_1, \dots, f(u_r) = w_r, f(v_1) = 0, \dots, f(v_k) = 0$, also ist

$$M_{\mathcal{B}}^{\mathcal{A}}(f) = \begin{pmatrix} E_r & \\ & 0 \end{pmatrix}$$

□

Anmerkung 12.12 Das Problem für $f \in End_K(V)$ eine Basis $\mathcal{B}$ zu finden, sodass $M_{\mathcal{B}}(f) = M_{\mathcal{B}}^{\mathcal{B}}(f)$ möglichst einfach ist, ist wesentlich schwieriger zu lösen ($\to$ Jordansche Normalform, LA2)

13 Basiswechsel

In diesem Abschnitt seien V, W endlich dimensionale K-VR.
Ziel: $f : V \to W$ lineare Abbildung, $\mathcal{A}, \mathcal{A}'$ Basen von $V, \mathcal{B}, \mathcal{B}'$ Basen von W. Wie hängen $M^{\mathcal{A}}_{\mathcal{B}}(f)$ und $M^{\mathcal{A}}_{\mathcal{B}}(f)$ zusammen?

Bemerkung 13.1 (16.1) $f : V \to W$ lineare Abbildung, $\mathcal{A}$ Basis von V, $\mathcal{B}$ Basis von W. Dann gilt: Das Diagramm

$$\begin{tikzcd}
K^n \arrow[r, "\widetilde{M^{\mathcal{A}}_{\mathcal{B}}(f)}"'] \arrow[d, "\Phi_{\mathcal{A}}"'] & V \arrow[d, "f"'] \\
K^m \arrow[r, "\Phi_{\mathcal{B}}"'] & W
\end{tikzcd}$$

ist kommutativ, das heißt $\Phi_{\mathcal{B}} \circ M^{\mathcal{A}}_{\mathcal{B}} = f \circ \Phi_{\mathcal{A}}$ (Hierbei sind $\Phi_{\mathcal{A}}$, $\Phi_{\mathcal{B}}$ Koordinatensysteme von V bezüglich $\mathcal{A}$ beziehungsweise von W bezüglich $\mathcal{B}$) Insbesondere ist $\widetilde{M^{\mathcal{A}}_{\mathcal{B}}(f)} = \Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{A}}$

Beweis Es gilt zu zeigen, dass die Abbildung $\Phi_{\mathcal{B}} \circ \widetilde{M^{\mathcal{A}}_{\mathcal{B}}(f)} : K^n \to W$ und $f \circ \Phi_{\mathcal{A}} : K^n \to W$ auf der kanonischen Basis $(e_1, \dots, e_n)$ von K^n übereinstimmen. Sei $A = (a_{ij}) = M^{\mathcal{A}}_{\mathcal{B}}(f)$, $\mathcal{A} = (v_1, \dots, v_n), \mathcal{B} = (w_1, \dots, w_m)$

$$\implies (\Phi_{\mathcal{B}}) \circ \widetilde{M^{\mathcal{A}}_{\mathcal{B}}(f)}(e_j) = \Phi_{\mathcal{B}}\Big(\tilde{A}(e_j)\Big) = \Phi_{\mathcal{B}}(Ae_j) = \Phi_{\mathcal{B}}\left(\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}\right) = a_{1j}w_1 + \ldots + a_{mj}w_m$$

$$(f \circ \Phi_{\mathcal{A}})(e_j) = f(\Phi_{\mathcal{A}}(e_j)) = f(v_j) = a_{ij}w_1 + \ldots + a_{mj}w_m \qquad \square$$

Bemerkung 13.2 (16.2) $\mathcal{A}, \mathcal{A}'$ Basen von $V, n = \dim(V)$

$$T^{\mathcal{A}}_{\mathcal{A}'} := M^{\mathcal{A}}_{\mathcal{A}'}(\mathrm{id}_V) \in M(n \times n, K)$$

heißt die **Transformationsmatrix** des Basiswechsels von $\mathcal{A}$ nach $\mathcal{A}'$. Es gilt:

1. $T^{\mathcal{A}}_{\mathcal{A}'} \in GL(n, K)$
2. $\widetilde{T^{\mathcal{A}}_{\mathcal{A}'}} = \Phi^{-1}_{\mathcal{A}'} \circ \Phi_{\mathcal{A}}$
3. $T^{\mathcal{A}}_{\mathcal{A}'} = \left(T^{\mathcal{A}'}_{\mathcal{A}}\right)^{-1}$

Beweis (2) nach 16.1 ist das Diagramm

$$\begin{tikzcd}
K^n \arrow[r, "\widetilde{T^{\mathcal{A}}_{\mathcal{A}'}} = \widetilde{M^{\mathcal{A}}_{\mathcal{A}'}(f)}"'] \arrow[d, "\Phi_{\mathcal{A}}"'] & V \arrow[d, "\mathrm{id}_V"] \\
K^n \arrow[r, "\Phi_{\mathcal{A}'}"'] & V
\end{tikzcd}$$

kommutativ $\implies$

$$\Phi_{\mathcal{A}'} \circ T^{\mathcal{A}}_{\mathcal{A}'} = \mathrm{id}_V \circ \Phi_{\mathcal{A}} = \Phi_{\mathcal{A}} \implies \widetilde{T^{\mathcal{A}}_{\mathcal{A}'}} = \Phi^{-1}_{\mathcal{A}'} \circ \Phi_{\mathcal{A}}$$

(1) Da $\Phi_{\mathcal{A}'}, \Phi_{\mathcal{A}}$ Isomorphismen, ist auch $\widetilde{T^{\mathcal{A}}_{\mathcal{A}'}} = \Phi^{-1}_{\mathcal{A}'} \circ \Phi_{\mathcal{A}}$ ein Isomorphismus, nach 15.6 folgt $T^{\mathcal{A}}_{\mathcal{A}'} \in GL(n, K)$

(3) Nach (2) ist $T^{\mathcal{A}}_{\mathcal{A}'} \cdot T^{\mathcal{A}'}_{\mathcal{A}} = \tilde{T}^{\mathcal{A}}_{\mathcal{A}'} \circ \tilde{T}^{\mathcal{A}'}_{\mathcal{A}} = \Phi^{-1}_{\mathcal{A}'} \circ \Phi_{\mathcal{A}} \circ \Phi^{-1}_{\mathcal{A}} \circ \Phi_{\mathcal{A}'} = \Phi^{-1}_{\mathcal{A}'} \circ id_{K^n} \circ \Phi_{\mathcal{A}'} = \mathrm{id}_{K^n} = \tilde{E}_n$

$$\implies T^{\mathcal{A}}_{\mathcal{A}'} \cdot T^{\mathcal{A}'}_{\mathcal{A}} = E_n \implies T^{\mathcal{A}}_{\mathcal{A}'} = \left(T^{\mathcal{A}'}_{\mathcal{A}}\right)^{-1}$$

□

Beispiel 13.3 (16.3) $K = \mathbb{R}, V = \mathbb{R}^2, \mathcal{A} = \left(\begin{pmatrix}-1\\1\end{pmatrix}; \begin{pmatrix}1\\1\end{pmatrix}\right), \mathcal{A}\left(\begin{pmatrix}2\\-1\end{pmatrix}; \begin{pmatrix}1\\-1\end{pmatrix}\right)$. Gesucht ist $T^{\mathcal{A}}_{\mathcal{B}} = M^{\mathcal{A}}_{\mathcal{B}}(\mathrm{id}_{\mathbb{R}^2})$ Es ist

$$\begin{pmatrix}-1\\1\end{pmatrix} = 0\begin{pmatrix}2\\-1\end{pmatrix} + (-1)\begin{pmatrix}1\\-1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix} = 2\begin{pmatrix}2\\-1\end{pmatrix} + (-3)\begin{pmatrix}1\\-1\end{pmatrix}$$

also:

$$T^{\mathcal{A}}_{\mathcal{B}} = \begin{pmatrix}0 & 2\\-1 & -3\end{pmatrix}$$

Satz 13.4 (16.4) U, V, W endlichdimensionale K-VR mit Basen $\mathcal{A}, \mathcal{B}, \mathcal{C}, g : U \to V, f : V \to W$ lineare Abbildungen. Dann gilt:

$$M^{\mathcal{A}}_{\mathcal{C}}(f \circ g) = M^{\mathcal{B}}_{\mathcal{C}}(f) \cdot M^{\mathcal{A}}_{\mathcal{B}}(g)$$

Beweis Wir setzen $r := \dim U, m := \dim V, n := \dim W, A := M^{\mathcal{B}}_{\mathcal{C}}(f), B := M^{\mathcal{A}}_{\mathcal{B}}(g)$ Wir erhalten das Diagramm

$$\begin{tikzcd}
K^r \arrow[rrr, "\Phi_{\mathcal{A}}"] \arrow[dd, "\widetilde{AB}"'] \arrow[dr, "\tilde{B}"'] & & & U \arrow[dl, "g"'] \arrow[dd, "f \circ g"] \\
& K^m \arrow[r, "\Phi_{\mathcal{B}}"] \arrow[dl, "\tilde{A}"'] & V \arrow[dr, "f"] & \\
K^n \arrow[rrr, "\Phi_{\mathcal{C}}"'] & & & W
\end{tikzcd}$$

Die Trapeze sind kommutativ nach 16.1, das linke Dreieck nach 12.2, das rechte Dreieck trivialerweise. Damit kommutiert auch das äußere Rechteck, das heißt

$$\Phi_{\mathcal{C}} \circ \widetilde{AB} = f \circ g \circ \Phi_{\mathcal{A}}$$

$$\implies \widetilde{AB} = \Phi^{-1}_{\mathcal{C}} \circ (f \circ g) \circ \Phi_{\mathcal{A}} = \widetilde{M^{\mathcal{A}}_{\mathcal{C}}(f \circ g)} \implies M^{\mathcal{B}(f)}_{\mathcal{C}} \cdot M^{\mathcal{A}}_{\mathcal{B}} = AB = M^{\mathcal{A}}_{\mathcal{C}}(f \circ g)$$

□

Folgerung 13.5 (16.5) $\mathcal{A}, \mathcal{B}, \mathcal{C}$ Basen von V. Dann gilt:

1. $T^{\mathcal{A}}_{\mathcal{C}} = T^{\mathcal{B}}_{\mathcal{C}} \cdot T^{\mathcal{A}}_{\mathcal{B}}$
2. $M_{\mathcal{B}} : \mathrm{End}_K(v) \to M(n \times n, K), f \mapsto M_{\mathcal{B}}(f) = M^{\mathcal{B}}_{\mathcal{B}}(f)$ ist ein Isomorphismus von Ringen, das heißt $M_{\mathcal{B}}$ ist bijektiv,

$$M_{\mathcal{B}}(f + g) = M_{\mathcal{B}}(f) + M_{\mathcal{B}}(g), M_{\mathcal{B}}(f \circ g) = M_{\mathcal{B}}(f)M_{\mathcal{B}}(g), M_{\mathcal{B}}(\mathrm{id}_V) = E_n \,\forall\, f, g \in \mathrm{End}_K(v)$$

Beweis 1. aus 16.4 für $U = V = W, f = g = \mathrm{id}_V$

2. Nach 15.3.2 ist $M_{\mathcal{B}}$ ein Isomorphismus von K-VR, es ist $M_{\mathcal{B}}(\mathrm{id}_V) = E_n$ nach 16.4

$$M_{\mathcal{B}}(f \circ g) = M_{\mathcal{B}}(f) M_{\mathcal{B}}(g)$$

□

Satz 13.6 (Transformationsformel) $f : V \to W$ lineare Abbildung, $\mathcal{A}, \mathcal{A}'$ Basen von $V, \mathcal{B}, \mathcal{B}'$ Basen von W. Dann gilt:

$$M_{\mathcal{B}'}^{\mathcal{A}'}(f) = T_{\mathcal{B}'}^{\mathcal{B}} M_{\mathcal{B}}^{\mathcal{A}}(f) T_{\mathcal{A}}^{\mathcal{A}'}$$

Setzen wir $A := M_{\mathcal{B}}^{\mathcal{A}}(f), B := M_{\mathcal{B}'}^{\mathcal{A}'}(f), S := T_{\mathcal{B}'}^{\mathcal{B}}, T := T_{\mathcal{A}'}^{\mathcal{A}}$, dann gilt also

$$B = SAT^{-1}$$

Beweis Wir betrachten das Diagramm

$$\begin{tikzcd}
K^n \arrow[rrr, "\widetilde{M_{\mathcal{B}}^{\mathcal{A}}(f)}"] \arrow[dr, "\Phi_{\mathcal{A}}"] \arrow[dd, "\widetilde{T_{\mathcal{A}'}^{\mathcal{A}}}"'] & & & K^m \arrow[dl, "\Phi_{\mathcal{B}}"'] \arrow[dd, "\widetilde{T_{\mathcal{B}'}^{\mathcal{B}}}"] \\
& V \arrow[r, "f"] & W & \\
K^n \arrow[ur, "\Phi_{\mathcal{A}'}"'] \arrow[rrr, "\widetilde{M_{\mathcal{B}'}^{\mathcal{A}'}(f)}"'] & & & K^m \arrow[ul, "\Phi_{\mathcal{B}'}"]
\end{tikzcd}$$

Die Trapeze sind kommutativ nach 16.1, die Dreiecke nach 16.2.2 $\Longrightarrow$ Das äußere Rechteck kommutiert, das heißt

$$\widetilde{M_{\mathcal{B}'}^{\mathcal{A}'}(f)} \circ \widetilde{T_{\mathcal{A}'}^{\mathcal{A}}} = \widetilde{T_{\mathcal{B}'}^{\mathcal{B}}} \circ \widetilde{M_{\mathcal{B}}^{\mathcal{A}}(f)}$$

$$\Longrightarrow \widetilde{M_{\mathcal{B}'}^{\mathcal{A}'}(f) \cdot T_{\mathcal{A}'}^{\mathcal{A}}} = \widetilde{T_{\mathcal{B}'}^{\mathcal{B}} \cdot M_{\mathcal{B}}^{\mathcal{A}}(f)} \Longrightarrow M_{\mathcal{B}'}^{\mathcal{A}'}(f) \cdot T_{\mathcal{A}'}^{\mathcal{A}} = T_{\mathcal{B}'}^{\mathcal{B}} M_{\mathcal{B}}^{\mathcal{A}}(f)$$

$$\Longrightarrow M_{\mathcal{B}'}^{\mathcal{A}'}(f) = T_{\mathcal{B}'}^{\mathcal{B}} M_{\mathcal{B}}^{\mathcal{A}}(f) \left(T_{\mathcal{A}'}^{\mathcal{A}}\right)^{-1}$$

□

Beispiel 13.7 (16.7) Sei

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in M(2 \times 2, \mathbb{R}), \mathcal{A} = \left(\begin{pmatrix} -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right), \mathcal{B} = \left(\begin{pmatrix} 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right)$$

Gesucht ist $M_{\mathcal{B}}^{\mathcal{A}}\left(\tilde{A}\right)$ Nach 16.6 ist

$$M_{\mathcal{B}}^{\mathcal{A}}\left(\tilde{A}\right) = T_{\mathcal{B}}^{(e_1,e_2)} \underbrace{M_{(e_1,e_2)}^{(e_1,e_2)}\left(\tilde{A}\right)}_{=A} T_{(e_1,e_2)}^{\mathcal{A}} = T_{\mathcal{B}}^{(e_1,e_2)} A T_{(e_1,e_2)}^{\mathcal{A}} = \left(T_{(e_1,e_2)}^{\mathcal{B}}\right) A T_{(e_1,e_2)}^{\mathcal{A}}$$

Es ist

$$T_{(e_1,e_2)}^{\mathcal{A}} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, T_{(e_1,e_2)}^{\mathcal{B}} = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}$$

$$\Longrightarrow M_{\mathcal{B}}^{\mathcal{A}}\left(\tilde{A}\right) = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = \ldots = \begin{pmatrix} -1 & 5 \\ 1 & -7 \end{pmatrix}$$

Folgerung 13.8 (16.8) $\mathcal{A}, \mathcal{B}$ Basen von V, $f \in \mathrm{End}_K(V)$. Dann gilt:

$$M_{\mathcal{B}}(f) = T^{\mathcal{A}}_{\mathcal{B}} M_{\mathcal{A}}(f) T^{\mathcal{B}}_{\mathcal{A}}$$

Setzen wir $A := M_{\mathcal{A}}(f), B := M_{\mathcal{B}}(f) = S := T^{\mathcal{A}}_{\mathcal{B}}$ dann gilt also

$$B = SAS^{-1}$$

Definition 13.9 (16.9) $A, B \in M(m \times n, K)$. A, B heißen äquivalent $(A \sim B) \overset{\text{Def}}{\iff} \exists\, S \in GL(m, K), T \in GL(n, K)$:

$$B = SAT^{-1}$$

Bemerkung 13.10 (16.10) Äquivalenz von Matrizen ist eine Äquivalenzrelation auf $M(m \times n, K)$

Beweis leicht nach zurechnen. □

Bemerkung 13.11 (16.11) $A, B \in M(m \times n, K)$, $\mathcal{A}$ Basis von K^n, $\mathcal{B}$ Basis von K^m, $f : K^n \to K^m$ lineare Abbildung mit $M^{\mathcal{A}}_{\mathcal{B}}(f) = A$ (Existenz nach 15.3.2). Dann sind äquivalent:

1. $A \sim B$, das heißt $\exists\, S \in GL(m, K), T \in GL(n, K) : B = SAT^{-1}$
2. Es existieren Basen $\mathcal{A}'$ von K^n, $\mathcal{B}'$ von Km mit $M^{\mathcal{A}'}_{\mathcal{B}'}(f) = B$ (das heißt A, B beschreiben bezüglich geeigneter Paare von Basen dieselbe lineare Abbildung)
3. $\mathrm{Rang}\, A = \mathrm{Rang}\, B$

Insbesondere ist jede Matrix aus $M(m \times n, K)$ vom Rang r äquivalent zu

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

Beweis 1. $\implies$ 2. Sei $A \sim B \implies \exists\, S \in GL(m, K), T \in GL(n, K) : B = SAT^{-1}$. Sei $\mathcal{A} = (v_1, \ldots, v_n), T^{-1} = (a_{ij})$. Wir setzen für $j = 1, \ldots, n$:

$$v'_j := a_{1j} v_1 + \ldots + a_{nj} v_n, \mathcal{A}' := \big(v'_1, \ldots, v'_n\big)$$

Insbesondere ist

$$v'_j = \Phi_{\mathcal{A}}\left(\begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}\right) = \Phi_{\mathcal{A}}\big(T^{-1} e_j\big) = \left(\Phi_{\mathcal{A}} \circ \widetilde{T^{-1}}\right)(e_j)$$

Wegen $T^{-1} \in GL(n, K)$ ist $\widetilde{T^{-1}}$ nach 15.6 ein Isomorphismus, $\Phi_{\mathcal{A}}$ ist ein Isomorphismus, das heißt $\Phi_{\mathcal{A}} \circ \widetilde{T^{-1}}$ ein Isomorphismus $\implies$ $\mathcal{A}'$ Basis von K^n. Nach Konstruktion ist $T^{-1} = T^{\mathcal{A}'}_{\mathcal{A}}$

$$\implies B = SAT^{-1} = T^{\mathcal{B}}_{\mathcal{B}'} M^{\mathcal{A}}_{\mathcal{B}}(f) T^{\mathcal{A}'}_{\mathcal{A}} = M^{\mathcal{A}'}_{\mathcal{B}'}(f)$$

2. $\implies$ 3. Es gelte 2. Es ist

$$\begin{aligned} \mathrm{Rang}\, A = \mathrm{Rang}\, \tilde{A} = \mathrm{Rang}\, \widetilde{M^{\mathcal{A}}_{\mathcal{B}}(f)} &= \mathrm{Rang}\big(\Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{A}}\big) = \dim \mathrm{im}\big(\Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{A}}\big) \\ &= \dim\big(\Phi_{\mathcal{B}}^{-1} \circ f\big)(K^n) = \dim f(K^n) = \dim \mathrm{im}\, f = \mathrm{Rang}\, f \end{aligned}$$

Analog:

$$\mathrm{Rang}(B) = \mathrm{Rang}(f) \implies \mathrm{Rang}(A) = \mathrm{Rang}(B)$$

3. $\implies$ 1. Sei $\operatorname{Rang} A = \operatorname{Rang} B = r$. Nach 15.10 existieren Basen $\mathcal{A}$ von K^n, $\mathcal{B}$ von K^m mit

$$M_{\mathcal{B}}^{\mathcal{A}}\left(\tilde{A}\right) = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, \operatorname{Rang} \tilde{A} = \operatorname{Rang} A = r$$

$$\implies \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = M_{\mathcal{B}}^{\mathcal{A}}\left(\tilde{A}\right) = \underbrace{T_{\mathcal{B}}^{(e_1,\dots,e_m)}}_{\in GL(m,K)} \underbrace{M_{(e_1,\dots,e_m)}^{e_1,\dots,e_n}\left(\tilde{A}\right)}_{A} \underbrace{T_{(e_1,\dots,e_n)}^{\mathcal{A}}}_{\in GL(n,K)}$$

$$\implies \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \sim A$$

Analog:

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \sim B \implies A \sim B$$

□

Definition 13.12 (16.12) $A, B \in M(n \times n, K)$. A, B heißen **ähnlich** $\overset{\text{Def}}{\iff}$

$$\exists\, S \in GL(n,K) : B = SAS^{-1}$$

(Notation: $A \approx B$)

Bemerkung 13.13 (16.13) Ähnlichkeit von Matrizen ist eine Äquivalenzrelation.

Beweis Übung. □

Bemerkung 13.14 (16.14) $A, B \in M(n \times n, K)$, $\mathcal{A}$ Basis von K^n, $f : K^n \to K^n$ lineare Abbildung mit $M_{\mathcal{A}}(f) = A$. Dann sind äquivalent:

1. $A \approx B$
2. Es existiert eine Basis $\mathcal{B}$ von K^n mit $M_{\mathcal{B}}(f)$ (das heißt A, B beschrieben bezügliche geeigneter Basen denselben Endomorphismus)

Beweis 1. $\implies$ 2. analog zu 16.11 1. $\implies$ 2.

2. $\implies$ 1. Es gelte 2. Nach 16.8 existiert ein $S \in GL(n,K)$ mit $B = M_{\mathcal{B}}(f) = SAS^{-1} \implies A \simeq B$. □

Anmerkung 13.15 Einen möglichst einfachen Vertreter der Ähnlichkeitsklassen von A zu finden, ist eine schwierige Aufgabe (→ LA2, Jordansche Normalform)

14 Determinanten

In diesem Abschnitt sei $n \in \mathbb{N}$
Ziel: Ordne jeder Matrix aus $M(n \times n, K)$ ein Element aus K zu, dass genau dann $= 0$ ist, wenn die Matrix nicht invertierbar ist. Die Zuordnung soll mehreren Bedingungen genügen.

Definition 14.1 (17.1) Eine Abbildung $\det : M(n \times n, K) \to K, A \mapsto \det A$ heißt **Determinante** $\overset{\text{Def}}{\iff}$ Die folgenden Bedingungen sind erfüllt:

- (D1) det ist **linear in jeder Zeile**, das heißt ist
$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in M(n \times n, K)$$
mit Zeilen $a_1, \ldots, a_n$, dann gilt für jedes $i \in \{1, \ldots, n\}$:
  - (D1a) Ist $a_i = a_i' + a_i''$, dann ist
$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_i' \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_i'' \\ \vdots \\ a_n \end{pmatrix}$$
  - (D1b) Ist $a_i = \lambda a_i'$ mit $\lambda \in K$, dann ist
$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} = \lambda \det \begin{pmatrix} a_1 \\ \vdots \\ a_i' \\ \vdots \\ a_n \end{pmatrix}$$
- (D2) det ist **alternierend**, das heißt: Hat $A \in M(n \times n, K)$ zwei gleiche Zeilen, dann ist $\det A = 0$
- (D3) det ist **normiert**, das heißt $\det E_n = 1$

Weitere Schreibweise: Für $A = (a_{ij})$ schreiben wir auch
$$\begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \\ a_{n1} & \ldots & a_{nn} \end{vmatrix} := \det \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$$

Anmerkung 14.2 Wir müssen erst noch zeigen, dass es Determinanten überhaupt gibt.

- geometrische Motivation für (D1)-(D3) für den Fall $K = \mathbb{R}$: ist $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in M(n \times n, \mathbb{R})$, dann spannen die Vektoren $a_1, \ldots, a_n$ ein „Parallelotop im $\mathbb{R}$ auf ($n = 2$: Parallogramm).
D1-D3 sind sinnvolle Forderungen für ein Volumen im $\mathbb{R}^n$:
  - D2: Volumen ist Null, wenn $i \neq j$ mit $a_i = a_j$ existiert.
  - D3: Volumen des „Einheitspolytops“ ist 1
  - D1b: Volumen ist „homogen“
  - D1 + D2 implizieren (siehe Satz 17.2): Für $\lambda \in \mathbb{R}, i \neq j$ ist
$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_1 + \lambda a_j \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$
(„Scherungsinvarianz“)

Satz 14.3 (17.2) $\det : M(n \times n, K) \to K$ sei einen Determinante,

$$A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, B \in M(n \times n, K)$$

Dann gilt:

- (D4) $\det(\lambda A) = \lambda^n \det(A)$
- (D5) Ist eine Zeile von A gleich Null, dann ist $\det A = 0$
- (D6)
$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} = -\det(A)$$
das heißt bei Zeilenumformungen vom Typ 4 wird das Ergebnis mit -1 multipliziert.
- (D7)
$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_n \end{pmatrix} = \det A$$
für $i \neq j, \lambda \in K$, das heißt $\det$ ist invariant unter Zeilenumformungen vom Typ 3
- (D8) Ist A eine obere Dreiecksmatrix, das heißt
$$A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$
dann ist $\det A = \lambda_1 \cdot \cdots \cdot \ldots \cdot \cdots \lambda_n$ Analog für untere Dreiecksmatrizen.
- (D9) Ist $n \geq 2$ und A von der Gestalt
$$A = \begin{pmatrix} A_1 & C \\ 0 & A_2 \end{pmatrix}$$
mit $A_1 \in M(r \times r, K), A_2 \in M(s \times s, K), r + s = n$, dann ist $\det A = \det(A_1) \cdots \det(A_2)$.
- (D10) $\det A = 0 \iff \text{Rang } A < 0$ (das heißt $\det A \neq 0 \iff A \in GL(n, K)$)
- (D11) $\det(AB) = \det(A)\det(B)$. Insbesondere ist $\det\left(A^{-1}\right) = \det(A)^{-1}$

Beweis (D4)

$$\det(\lambda A) = \det \begin{pmatrix} \lambda a_1 \\ \vdots \\ \lambda a_n \end{pmatrix} = \lambda \det \begin{pmatrix} a_1 \\ \lambda a_2 \\ \vdots \\ \lambda a_n \end{pmatrix} = \ldots = \lambda^n \det \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \lambda^n \det(A)$$

(D5) Sei etwa $a_1 = 0 = 0_k \cdots 0$. Es ist

$$\det \begin{pmatrix} a_1 \\ \vdots \\ 0 \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ 0_K \cdot 0 \\ \vdots 0 \end{pmatrix} = 0_K \det \begin{pmatrix} a_1 \\ \vdots \\ 0 \\ \vdots \\ a_n \end{pmatrix} = 0$$

(D6)

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_i + a_j \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_i + a_j \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} \\ \\ a_i + \\ \\ a_1 + \\ \\ \end{pmatrix}$$

(D7)

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} + \lambda \det \begin{pmatrix} a_1 \\ \vdots \\ a_j \\ \vdots \\ a_j \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ a_n \end{pmatrix}$$

(D8) A sei von der Form

$$\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

1. Fall: $\lambda_i \neq 0 \,\forall\, i \in \{1, \ldots, n\}$. Durch Zeilenumformungen von Typ 3 kann man A auf die Form

   $$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

   bringen

   $$\implies \det(A) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \lambda_1 \cdot \ldots \cdot \lambda_n \det \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = \lambda_1 \cdot \ldots \cdot \lambda_n$$

2. Fall: $\exists\, i \in \{1,\dots,n\} : \lambda_i = 0$. Wir setzen $j := \max\{i \in \{1,\dots,n\} \mid \lambda_i = 0\}$, dann ist

$$\begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & * & & \\ & & \lambda_{j-1} & & & & \\ & & & 0 & & & \\ & & & & \lambda_{j+1} & & \\ & & & & & \ddots & \\ & & & & & & \lambda_n \end{pmatrix}$$

wobei $\lambda_{j+1},\dots,\lambda_n \neq 0$. Insbesondere kann man die j-te Zeile durch Zeilenumformung vom Typ 3 zu einer Nullzeile machen. $\implies \det A = 0 = \lambda_1 \cdot \ldots \cdot \lambda_n$

(D9) Sei

$$A = \begin{pmatrix} A_1 & c \\ 0 & A_2 \end{pmatrix}, A_1 \in M(r \times r, K), A_2 \in M(s \times s, K), r + s = n$$

Bringe A_1 durch elementare Zeilenumformungen an A vom Typ 3, 4 auf obere Dreiecksgestalt (das geht!)

$$A \to \begin{pmatrix} B_1 & C' \\ 0 & A_2 \end{pmatrix}$$

Wurden dabei k Zeilenvertauschungen gemacht, dann ist nach D6

$$\det(B_1) = (-1)^k \det\bigl(A^1\bigr)$$

Überführe A_2 durch Zeilenumformungen vom Typ 3, 4 auf obere Dreiecksgestalt

$$A \to \begin{pmatrix} B_1 & C' \\ 0 & B_2 \end{pmatrix} =: B$$

Es ist $\det(B_2) = (-1)^l \det(A_2)$, wenn dabei l Zeilenvertauschungen gemacht wurden. B_1, B_2, B sind obere Dreiecksmatrizen

$$\implies \det(B) = \det(B_1)\det(B_2) = (-1)^{k+l}\det(A_1)\det(A_2)$$

B kann man aus A durch Zeilenumformungen vom Typ 3, 4 mit $k + l$ Zeilenumformungen erhalten

$$\implies \det(B) = (-1)^{k+l}\det(A) \implies \det(A) = \det(A_1)\det(A_2)$$

(D10) Wir bringen A durch Zeilenumformungen vom Typ 3,4 auf obere Dreiecksgestalt

$$A \to \begin{pmatrix} \lambda_1 & & x \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} =: B \implies \det(A) = \pm\det(B)$$

Außerdem $\mathrm{ZR}(A) = ZR(B)$ und somit

$$\operatorname{Rang} A = \operatorname{Rang} B$$

. Es ist

$$\operatorname{Rang} A = n \iff \operatorname{Rang} B = n \iff \lambda_1 \cdot \ldots \cdot \lambda_n \neq 0 \iff \det(B) \neq 0 \iff \det(A) \neq 0$$

(D11)

1. Fall:

$$\operatorname{Rang} A < n \implies \dim\left(\operatorname{im} \tilde{A}\right) < n \implies \dim\left(\operatorname{im}\left(\tilde{A} \circ \tilde{B}\right)\right) < n \implies \operatorname{Rang}(AB) < n \implies \det(AB) = 0 = \mathrm{c}$$

2. Fall: Rang $A = n$, das heißt $A \in GL(n, K)$
   a) Überlegung: A lässt sich schreiben als Produkt von Elementarmatrizen vom Typ $D_i(\lambda), E_{ij}(1)$, etwa $A = C_1 \cdot \ldots \cdot C_s$, wobei $C_1, \ldots, C_s$ Elementarmatrizen obigen Types

$$\implies AB = C_1 \cdot \ldots \cdot C_s B$$

   b) Nach 1. gilt zu zeigen: Ist

$$B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in M(n \times n, K)$$

und ist C eine Elementarmatrix vom Typ $D_i(\lambda)$ beziehungsweise $E_{ij}(1)$, dann ist

$$\det(CB) = \det(C)\det(B)$$

(Dann ist nämlich

$$\det(AB) = \det(C_1(C_2 \cdot \ldots \cdot C_s B)) = \det(C_1)\det(C_2 \cdot \ldots \cdot C_s B) = \ldots = \det(C_1) \cdot \ldots \cdot \det(C_s)\det(B) = \det(\mathrm{C}$$

   a) Fall:

$$C = D_i(\lambda) = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \implies \det(CB) = \det \begin{pmatrix} b_1 \\ \vdots \\ \lambda b_i \\ \vdots \\ b_n \end{pmatrix} = \lambda \det(B)$$

   und es ist $\det(C) = \lambda$, somit $\det(CB) = \det(C)\det(B)$

   b) Fall:

$$C = \begin{pmatrix} 1 & & \\ & \ddots & 1 \\ 0 & & 1 \end{pmatrix}, \det(C) = 1$$

   Es ist

$$CB = \begin{pmatrix} b_1 \\ \vdots \\ b_i + b_j \\ \vdots \\ b_j \\ \vdots \\ b_n \end{pmatrix}$$

   das heißt

$$\det(CB) = \det(B) = \det(C)\det(B)$$

   Insbesondere für $A \in GL(n, K)$ gilt:

$$1 = \det(E_n) = \det\left(AA^{-1}\right) = \det(A)\det\left(A^{-1}\right) \implies \det\left(A^{-1}\right) = (\det(A))^{-1} \qquad \square$$

Anmerkung 14.4 Wir müssen immer noch zeigen, dass es überhaupt Abbildungen $\det : M(n \times n, K) \to K$ gibt, die D1-D3 erfüllen. Wir werden dies tun, indem wir eine explizite Formel angeben (Leibniz-Formel)

Definition 14.5 (17.3) $\sigma \in S_n$

$$\operatorname{sgn}(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - 1}$$

heißt das **Sigma** von σ. σ heißt **gerade** $\overset{\text{Defn.}}{\Longleftrightarrow} \operatorname{sgn}(\sigma) = 1$, σ heißt **ungerade** $\overset{\text{Def.}}{\Longleftrightarrow} \operatorname{sgn}(\sigma) = -1$

$$(i, j) \in \{1, \dots, n\} \times \{1, \dots, n\}, i < j, \sigma(i) > \sigma(j)$$

heißt ein **Fehlstand** von σ

Bemerkung 14.6 (17.4) Es gilt:

1. $\operatorname{sgn} : S_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus von $(S_n, \circ)$ nach $(\{\pm\}, \cdot)$, das heißt
$$\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau) \, \forall \, \sigma, \tau \in S_n$$
2. $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma) \, \forall \, \sigma \in S_n$
3. Es ist
$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{wenn } \sigma \text{ eine gerade Anzahl von Fehlständen hat} \\ -1 & \text{wenn } \sigma \text{ eine ungerade Anzahl von Fehlständen hat} \end{cases} = (-1)^k, k \text{ Anzahl der Fehlstände von } \sigma$$

Beweis 1. und 3. nachrechnen

2. $1 = \operatorname{sgn}(\mathrm{id}) = \operatorname{sgn}(\sigma \circ \sigma^{-1}) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\sigma^{-1}) \implies \operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$ □

Definition 14.7 (17.5) $\tau \in S_n$ heißt **Transposition** $\overset{\text{Def.}}{\Longleftrightarrow}$ Es existiert $a, b \in \{1, \dots, n\}, a \in b$ mit $\tau(a) = b, \tau(b) = a$ und $\tau(c) = c \, \forall \, c \in \{1, \dots, n\} \setminus \{a, b\}$

Bemerkung 14.8 (17.6) $n \geq 2$. Dann gilt

1. Für jedes $\sigma \in S_n$ existieren Transpositionen $\tau_1, \dots, \tau_k \in S_k$ mit $\sigma = \tau_1 \circ \dots \circ \tau_k$, das heißt für jedes Element aus S_n kann (auf nicht notwendig eindeutige Weise!) als Produkt von Transpositionen geschrieben werden.
2. Ist $\tau \in S_n$ eine Transposition, dann existiert ein $\sigma \in S_n$ mit $\tau = \sigma \delta \sigma^{-1}$ wobei
$$\delta = \begin{pmatrix} 1 & 2 & 4 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}$$

Beweis 1. per Induktion nach n:
Induktionsanfang:

$$p = 2, S_2 = \{\mathrm{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$$

$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ ist eine Transposition,

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Induktionsschritt: Die Aussage sei für $n - 1$ bewiesen. Wir betrachten die Abbildung

$$\phi : S_{n-1} \to S_n, \pi \mapsto \begin{pmatrix} 1 & \dots & n-1 & n \\ \pi(1) & & \pi(n-1) & n \end{pmatrix}$$

ϕ ist ein injektiver Gruppenhomomorphismus.

a) Fall:

$$\sigma \in S_n \text{ mit } \sigma(n) = n \implies \exists\, \pi \in S_{n-1} : \sigma = \phi(\pi)$$

Nach Induktionsannahme existieren Transpositionen $\tau_1, \ldots, \tau_k \in S_{n-1}$ mit $\pi = \tau_1 \circ \ldots \circ \tau_k$

$$\implies \sigma = \phi(\pi) = \phi(\tau_1) \circ \ldots \circ \phi(\tau_k)$$

$\phi(\tau_1), \ldots, \phi(\tau_k)$ sind wieder Transpositionen $\implies$ Behauptung

b) $\sigma \in S_n$ mit $\sigma(n) = m$ mit $1 \leq m \leq n-1$. Wir setzen

$$\varepsilon := \begin{pmatrix} 1 & \ldots & m & \ldots & n \\ 1 & \ldots & n & \ldots & m \end{pmatrix}, \tilde{\sigma} := \varepsilon \circ \sigma$$

$$\implies \tilde{\sigma}(n) = \varepsilon(\sigma(n)) = \varepsilon(m) = n$$

$\implies$ Es existieren Transpositionen $\tilde{\tau}_1, \ldots, \tilde{\tau}_k \in S_n$ mit

$$\tilde{\sigma} = \tilde{\tau}_1 \circ \ldots \circ \tilde{\tau}_m \implies \sigma = \varepsilon \circ \tilde{\tau} = \varepsilon \circ \tilde{\tau}_1 \circ \ldots \circ \tilde{\tau}_k$$

$\implies$ Behauptung

2. Sei

$$\tau = \begin{pmatrix} 1 & \ldots & k & \ldots & l & \ldots & n \\ 1 & \ldots & l & \ldots & k & \ldots & n \end{pmatrix}$$

Wir setzen

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ k & l & * & \ldots & * \end{pmatrix}$$

$$\begin{aligned} \left(\sigma \circ \delta \circ \sigma^{-1}\right)(k) &= (\sigma \circ \delta)(1) = \sigma(2) = l \\ \left(\sigma \circ \delta \circ \sigma^{-1}\right)(l) &= (\sigma \circ \delta)(2) = \sigma(1) = k \end{aligned}$$

für $i \notin \{k, l\}$ ist $\left(\sigma \circ \delta \circ \sigma^{-1}\right)(i) = (\sigma)\left(\sigma^{-1}(i)\right) = \sigma\left(\sigma^{-1}(i)\right) = i \implies \sigma \circ \delta \circ \sigma^{-1} = \tau$ □

Folgerung 14.9 (Folgerung 17.7) $n \geq 2$. Dann gilt:

1. Ist $\tau \in S_n$ eine Transposition, dann ist $\operatorname{sgn}(\tau) = -1$
2. Ist $\sigma \in S_n, \sigma = \tau_1 \circ \ldots \circ \tau_k$ mit Transpositionen $\tau_1, \ldots, \tau_k \in S_n$, dann ist $\operatorname{sgn}(\sigma) = (-1)^k$

Beweis 1. Nach 17.6.2 existiert ein $\sigma \in S_n$ mit

$$\tau = \sigma \circ \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix} \circ \sigma^{-1}$$

$$\implies \operatorname{sgn} \tau = \operatorname{sgn}(\sigma) \operatorname{sgn}\left(\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix}\right) \operatorname{sgn}\left(\sigma^{-1}\right) = \operatorname{sgn}\left(\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix}\right)$$

Die Transponierte

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix}$$

hat genau einen Fehlstand, nämlich $(1, 2)$, also $\operatorname{sgn}(\tau) = -1$

2. $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1 \circ \ldots \circ \tau_k) = \operatorname{sgn}(\tau_1) \cdot \ldots \cdot \operatorname{sgn}(\tau_k) = (-1)^k$ □

Folgerung 14.10 (17.8) $\det : M(n \times n, K) \to K$ sei eine Determinante, $\sigma \in S_n$. Dann gilt

$$\det\left(\begin{pmatrix} e_{sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}\right) = \operatorname{sgn}(\sigma)$$

Beweis Nach 17.6 existieren Transpositionen $\tau_1, \ldots, \tau_k \in S_n$ mit $\sigma = \tau_1 \circ \ldots \circ \tau_k$. Wir erhalten folgende Sequenz von k Zeilenvertauschungen:

$$E_n = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} \to \begin{pmatrix} e_{\tau_k(1)} \\ \vdots \\ e_{\tau_k(n)} \end{pmatrix} \to \begin{pmatrix} e_{\tau_{k-1} \circ \tau_k(1)} \\ \vdots \\ e_{\tau_{k-1} \circ \tau_k(n)} \end{pmatrix} \to \ldots \to \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}$$

$$\implies \det\left(e_{\sigma(1)}, \ddots, e_{\sigma(n)}\right) = (-1)^k \det(E_n) = (-1)^k = \operatorname{sgn}(\sigma)$$ □

Definition 14.11 (17.9) $A_n := \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}$ ist eine Gruppe bezüglich „$\circ$“, die sogenannte **alternierende Gruppe**

Beweis Übung □

Beispiel 14.12 (17.10) Es ist

$$S_3 = \{\mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$$

Es ist

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

das heißt

$$\operatorname{sgn}\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right) = (-1)^2 = 1$$

Vergleiche Definition sgn:

$$\operatorname{sgn}\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right) = \prod_{1 \leq i < j \leq 3} \frac{\sigma(j) - \sigma(i)}{j - i} = \frac{3-2}{2-1}\frac{1-2}{3-1}\frac{1-3}{3-2} = 1$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \implies \operatorname{sgn}\left(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right) = 1$$

$$\implies A_3 = \{\mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$$

Bemerkung 14.13 (17.11) $n \geq 2, \pi \in S_n \setminus A_n$. Dann gilt:

1. $S_n = S_n \cup A_n\pi, A_n \cap A_n\pi = \emptyset$. Hierbei ist $A_n\pi\{\sigma \circ \pi \mid \sigma \in A_n\}$. Also:

$$S_n = A_n \dot{\cup} A_n\pi$$

2. $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$

Beweis 1. „$\supseteq$“ trivial
„$\subseteq$“ Sei $\sigma \in S_n$

a) Fall: $\operatorname{sgn}(\sigma) = 1 \implies \sigma \in A_n \subseteq S_n \cup A_n\pi$

b) Fall: $\operatorname{sgn}(\sigma) = -1 \implies \operatorname{sgn}\big(\sigma \circ \pi^{-1}\big) = \operatorname{sgn}(\sigma)\operatorname{sgn}\big(\pi^{-1}\big) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\pi) = (-1)(-1) = 1 \implies \sigma \circ \pi^{-1} \in A_n \implies \sigma = \underbrace{\big(\sigma \circ \pi^{-1}\big)}_{\in A_n} \circ \pi \in A_n\pi \subseteq A_n \cup A_n\pi$

Annahme: $A_n \cap A_n\pi \neq \emptyset \implies \exists\, \sigma \in A_n \cap A_n\pi \implies \operatorname{sgn}(\sigma) = 1$ und es existiert $\varepsilon \in A_n$ mit

$$\sigma = \varepsilon \circ \pi \implies \operatorname{sgn}(\sigma) = \operatorname{sgn}(\varepsilon)\operatorname{sgn}(\pi) = 1(-1) = -1`$$

2. Die Abbildung $A_n \to A_n\pi, \sigma \mapsto \sigma \circ \pi$ ist
   - surjektiv nach Definition
   - injektiv, denn: $\sigma_1 \circ \pi = \sigma_2 \circ \pi \implies \sigma_1 = \sigma_2$

$$\implies |A_n| = |A_n\pi|$$

Wegen $S_n = A_n \dot\cup A_n\pi$ folgt $|A_n| = |A_n\pi| = \frac{1}{2}|S_n| = \frac{1}{2}n!$ □

Satz 14.14 (17.12) Es gibt genau eine Determinante

$$\det : M(n \times n, K) \to K$$

Diese ist durch

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}, A = (a_{ij}) \in M(n \times n, K)$$

Beispiel 14.15 (17.13) 1. $n = 2$

$$\det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \sum_{\sigma \in S_2} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} = \operatorname{sgn}(\mathrm{id}) a_{11}a_{22} + \operatorname{sgn}\left(\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right) a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}$$

2. $n = 3$: Erinnerung (vergleiche 17.10)

$$S_3 = \{\underbrace{\mathrm{id}}_{1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}_{1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}_{1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}}_{-1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{-1}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}_{-1}\}$$

$$\implies \det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$$

$$\begin{array}{|ccc|cc} + & + & + & & \\ a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \\ - & - & - & & \end{array}$$

Achtung: Die Sarussche Regel gilt nicht für $n \geq 4$. Die Leibnizformel für $n = 4$ hat $4! = 24$ Terme.

Beweis 1. Eindeutigkeit: Sei $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ mit Zeilenvektoren $a_1, \ldots, a_n \in K^n$ Für $i = 1, \ldots, n$ schrieben wir $a_i = a_{i1}e_1 + \ldots + a_{in}e_n$ (e_i als Zeilenvektoren)

$$\implies \det(A) = \det \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_{11}e_1 + \ldots + a_{1n}e_n \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \sum_{i_1=1}^{n} a_{1i} \det \begin{pmatrix} e_{i1} \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

$$= \sum_{i_1=1}^{n} a_{1i_1} \sum_{i_2=1}^{n} a_{2i_2} \det \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ a_3 \\ \vdots \\ a_n \end{pmatrix} = \ldots = \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} a_{1i_1} \cdot \ldots \cdot a_{ni_n} \det \begin{pmatrix} e_{i_1} \\ \vdots \\ e_{i_n} \end{pmatrix}$$

Falls $\{i_1, \ldots, i_n\} \subsetneq \{1, \ldots, n\}$, dann gilt nach D2:

$$\det \begin{pmatrix} e_{i_1} \\ \vdots \\ e_{i_n} \end{pmatrix} = 0$$

Falls $\{i_1, \ldots, i_n\} = \{1, \ldots, n\}$, dann existiert ein $\sigma \in S_n$ mit $\sigma(k) = i_k$ für $k = 1, \ldots, n$, und es ist

$$\det \begin{pmatrix} e_{i_1} \\ \vdots \\ e_{1_n} \end{pmatrix} = \det \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix} = \operatorname{sgn}(\sigma)$$

und jedes $\sigma \in S_n$ kommt in obiger Summe genau einmal vor

$$\implies \det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}$$

2. Existenz: Wir definieren $\det : M(n \times n, K) \to K$ durch die Leibnizformel und müssen D1-D3 nachrechnen. D1a:

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_i' + a_i'' \\ \vdots \\ a_n \end{pmatrix} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot \left(a'_{i\sigma(i)} + a''_{i\sigma(i)}\right) \cdot \ldots \cdot a_{n\sigma(n)}$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a'_{i\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} + \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a''_{i\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)}$$

$$= \det \begin{pmatrix} a_1 \\ \vdots \\ a_i' \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_i'' \\ \vdots \\ a_n \end{pmatrix}$$

D1b: analog

D2: Sei $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in M(n \times n, K)$ mit $a_k = a_l$ ohne Einschränkung $k < l$. Sei

$$\tau = \begin{pmatrix} 1 & \dots & k & \dots & l & \dots & n \\ 1 & \dots & l & \dots & k & \dots & n \end{pmatrix} \in S_n \setminus A_n$$

dann ist $S_n = A_n \dot\cup A_n \tau$ nach 17.11. Ist $\sigma \in A_n$, dann ist $\operatorname{sgn}(\sigma) = 1, \operatorname{sgn}(\sigma \circ \tau) = -1$

$$\begin{aligned} \implies \det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} &= \sum_{\sigma \in A_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} + \sum_{sigma \in A_n} \operatorname{sgn}(\sigma \circ \tau) a_{1,\sigma\circ\tau(1)} \cdot \\ &= \sum_{\sigma \in A_n} a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} - \sum_{\sigma \in A_n} a_{1,\sigma\circ\tau(1)} \cdot \ldots \cdot a_{n\sigma\circ\tau(n)} \end{aligned}$$

Es ist

$$\begin{aligned} & a_{1,\sigma\tau(1)} \cdot \ldots \cdot a_{k,\sigma\tau(k)} \cdot \ldots \cdot a_{l,\sigma\tau(l)} \cdot \ldots \cdot a_{n,\sigma\tau(n)} \\ =& a_{1,\sigma(1)} \cdot \ldots \cdot a_{k,\sigma(l)} \cdot \ldots \cdot a_{l,\sigma(k)} \cdot \ldots \cdot a_{n,\sigma\tau(n)} \\ =& a_{1,\sigma(1)} \cdot \ldots \cdot a_{l,\sigma(l)} \cdot \ldots \cdot a_{k,\sigma(k)} \cdot \ldots \cdot a_{n,\sigma\tau(n)} \\ =& a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma\tau(n)} \\ & \implies \det(A) = 0 \end{aligned}$$

D3: Sei

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \text{ (Kronecker-Symbol, dann ist } E_n = (\delta_{ij}))$$

und

$$\delta_{1,\sigma(1)} \cdot \ldots \cdot \delta_{n,\sigma(n)} = \begin{cases} 0 & \sigma \neq id \\ 1 & \sigma = \mathrm{id} \end{cases} \implies \det(E_n) = \det((\delta_{ij})) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \delta_{1\sigma(1)} \cdot \ldots \cdot \delta_{n\sigma(n)} = 1$$

□

Satz 14.16 (17.14) $A \in M(n \times n, K)$. Dann gilt:

$$\det(A^T) = \det(A)$$

Beweis Sei $A = (a_{ij})$

$$\implies \det(A^T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \cdot \ldots \cdot a_{\sigma(n)n} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) A_{1\sigma^{-1}(1)} \cdot \ldots \cdot a_{n\sigma^{-1}(n)}$$

Die Abbildung $\psi : S_n \to S_n, \sigma \mapsto \sigma^{-1}$ ist bijektiv wegen $\psi \circ \psi = \mathrm{id}_{S_n}$.

$$\implies \det(A^T) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} = \det(A)$$

□

Algorithmus 14.17 (17.15) **Eingabe**: $A \in M(n \times n, K)$
Ausgabe: $\det(A)$
Durchführung:

1. Bringe A durch elementare Zeilen- und Spaltenumformungen vom Typ 3, 4 auf obere Dreiecksgestalt
$$B = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$
2. Ist k die Zahl der benötigten Vertauschungen von Zeilen und Spalten, dann ist
$$\det(A) = (-1)^k \lambda_1 \cdot \ldots \cdot \lambda_n$$

Beweis folgt aus 17.2, 17.12, 17.14. □

Definition 14.18 (17.16) $A = (a_{ij}) \in M(n \times n, K)$

$$A_{ij} := \begin{pmatrix} a_{1,1} & \ldots & a_{1,j-1} & 0 & a_{1,j+1} & \ldots & a_{1,n} \\ \vdots & & & \vdots & & & \\ a_{i-1,1} & \ldots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \ldots & a_{i-1,n} \\ 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ a_{i+1,1} & \ldots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \ldots & a_{i+1,n} \\ \vdots & & & \vdots & & & \\ a_{n,1} & \ldots & a_{n,j-1} & 0 & a_{n,j+1} & \ldots & a_{n,n} \end{pmatrix}$$
$$a_{ij}^{\#} := \det(A_{ji}) \in K$$
$$A^{\#} := \left(a_{ij}^{\#}\right) \in M(n \times n, K) = (\det(A_{ij}))^T$$

$A^{\#}$ heißt die zu A komplementäre Matrix:

$$A'_{ij} := \begin{pmatrix} a_{1,1} & \ldots & a_{1,j-1} & a_{1,j+1} & \ldots & a_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \ldots & a_{i-1,j-1} & a_{i-1,j+1} & \ldots & a_{1-1,n} \\ a_{i+1,1} & \ldots & a_{i+1,j-1} & a_{i+1,j+1} & \ldots & a_{1+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,j-1} & a_{n,j+1} & \ldots & a_{n,n} \end{pmatrix} \in M((n-1) \times (n-1), K)$$

Beispiel 14.19 (17.17)

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$
$$A_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, A_{12} = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, A_{21} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, A_{22} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$A^{\#} = \begin{pmatrix} 4 & -3 \\ -2 & 1 \end{pmatrix}^T = \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$$

Bemerkung 14.20 (17.18) $A \in M(n \times n, K), i, j \in \{1, \ldots, n\}$. Dann gilt:
$$\det(A_{ij}) = (-i)^{i+j} \det\left(A'_{ij}\right)$$

Beweis Durch $i-1$ Vertauschungen benachbarter Zeilen und $j-1$ Vertauschungen benachbarter Spalten kann man A_{ij} auf die Form

$$\begin{pmatrix} 1 & 0 \\ & 0 & A_{ij} \end{pmatrix}$$

bringen $\Longrightarrow$

$$\det(A_{ij}) = (-1)^{i-1+j-1} \det\bigl(A'_{ij}\bigr) = (-1)^{i+j} \det A'_{ij}$$ □

Bemerkung 14.21 (17.19) $A = \bigl(a^1, \dots, a^n\bigr) \in M(n \times n, K)$ mit Spaltenvektoren $a^1, \dots, a^n$,

$$e^i := \begin{vmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{vmatrix}$$

Dann gilt:

$$\det(A_{ij}) = \det\bigl(\bigl(a^1, \dots, a^{j-1}, e^i, a^{j+1}, \dots, a^n\bigr)\bigr)$$

Beweis Führe $\bigl(a^i, \dots, a^{j-1}, e^i, a^{j+1}, \dots, a^n\bigr)$ durch Addition von geeigneten Vielfachen der j-ten Spalte in A_{ij} über („i-te Zeile ausräumen“) $\overset{D7}{\Longrightarrow}$ Behauptung □

Satz 14.22 (17.20) $A \in M(n \times n, K)$. Dann gilt:

$$A \cdot A^{\#} = \det(A) \cdot E_n = A^{\#} \cdot A$$

Beweis Sei $A = \bigl(a^i, \dots, a^n\bigr) = (a_{ij})$. Es ist $A^{\#}A = (b_{ik})$ mit

$$b_{ij} = \sum_{j=1}^{n} a^{\#}_{ij} a_{ik} = \sum_{j=1}^{n} a_{jk} \det(A_{ji}) = \sum_{j=1}^{n} a_{jk} \det\bigl(\bigl(a^1, \dots, a^{i-1}, e^j, a^{i+1}, \dots, a^n\bigr)\bigr)$$

$$= \det\left(\left(a^1, \dots, a^{i-1}, \underbrace{\sum_{j=1}^{n} a_{jk} e^j}_{a^k}, a^{i+1}, \dots, a^n\right)\right) = \delta_{ij} \det(A)$$

$$\Longrightarrow A^{\#} \cdot A = \det(A) E_n$$

Analog: $A \cdot A^{\#} = \det(A) E_n$. □

Satz 14.23 (17.21 Entwicklungssatz von Laplace) $n \geq 2, A \in M(n \times n, K)$. Dann gilt: Für jede $i \in \{1, \dots, n\}$ ist

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det\bigl(A'_{ij}\bigr) \text{ (Entwicklung nach der i-ten Zeile)}$$

und für jedes $j \in \{1, \dots, n\}$ ist

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det\bigl(A'_{ij}\bigr) \text{ (Entwicklung nach der j-ten Spalte)}$$

Beweis Nach 17.20 ist $A \cdot A^{\#} = \det(A) = E_n$, insbesondere ist für jedes $i \in \{1, \ldots, n\}$:

$$\det(A) = \sum_{j=1}^{n} a_{ij} a_{ij}^{\#} = \sum_{j=1}^{n} a_{ij} \det(A_{ij}) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det\big(A'_{ij}\big)$$

Analog für Entwicklung nach j-ten Spalte über $A^{\#} \cdot A = \det(A) E_n$ □

Beispiel 14.24 (17.22)

$$\det \begin{pmatrix} -2 & 2 & 3 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} = (-1)^{1+2} \cdot 2 \cdot \det \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} + (-1)^{2+2} \cdot 2 \cdot \det \begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix} + (-1)^{3+2} \cdot 0 \cdot \det \begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix}$$
$$= 0 + \det \begin{pmatrix} -2 & 3 \\ -1 & 1 \end{pmatrix} + 0 = (-2)1 - 4(-1) = 1$$

Anmerkung 14.25
- Versuche, nach Zeilen beziehungsweise Spalten mit möglichst vielen Nullen zu entwickeln.
- Vorzeichenverteilung durch $(-1)^{i+j}$:

$$\begin{pmatrix} + & - & + & \\ - & + & & \\ + & & \ddots & \end{pmatrix}$$

Satz 14.26 (17.23) $A \in GL(n, K)$. Dann gilt:

$$A^{-1} = \frac{1}{\det(A)} A^{\#} = \frac{1}{\det(A)} B^T$$

wobei

$$B = (\det(A_{ij})) = \Big((-1)^{i+j} \det A'_{ij}\Big)$$

Beweis folgt aus 17.20 □

Beispiel 14.27 (17.24) Sei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, K)$$

$$\implies A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}^T = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Satz 14.28 (17.25 Cramersche Regel) $A = \big(a^1, \ldots, a^n\big) \in GL(n, K), b \in K^n, x \in \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$ Sei die eindeutig bestimmte Lösung des LGS $Ax = b$ (es ist $x = A^{-1}b$) Dann: für jedes $i \in \{1, \ldots, n\}$ ist

$$x_1 = \frac{\det\big(a^1, \ldots, a^{i-1}, b, a^{i+1}, \ldots, a^n\big)}{\det(A)}$$

Beweis Es ist $x = A^{-1}b$, und $A^{-1} = (d_{ij})$ mit $d_{ij} = \frac{1}{\det(A)} a_{ij}^{\#}$, also

$$\mathrm{d}_{ij} = \frac{1}{\det(A)} \det(A_{ji}) = \frac{\det\big(a^1, \ldots, a^{i-1}, e^j, a^{i+1}, \ldots, a^n\big)}{\det(A)}$$

$$\implies x_i = \sum_{j=1}^{n} d_{ij} b_j = \sum_{j=1}^{n} b_j \frac{\det\left(a^1, \dots, a^{i-1}, e^j, a^{i+1}, \dots, a^n\right)}{\det(A)}$$
$$= \frac{\det\left(a^1, \dots, a^{i-1}, \sum_{j=1}^{n} b_j e^j, a^{i+1}, \dots, a^n\right)}{\det(A)} = \frac{\det\left(a^1, \dots, a^{i-1}, b, a^{i+1}, \dots, a^n\right)}{\det(A)} \qquad \square$$

Beispiel 14.29 (17.26) Wir betrachten das reelle 3×3 LGS

$$\underbrace{\begin{pmatrix} -2 & 2 & 3 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}}_{=:b}$$

Nach Beispiel 17.22 ist $\det(A) = 1$

$$\implies x_1 = \det \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = 1 \det \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = -3$$
$$x_2 = \det \begin{pmatrix} -2 & 2 & 3 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} = 1(-1) \det \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} + 1 \cdot 1 \det \begin{pmatrix} -2 & 1 \\ -1 & 2 \end{pmatrix} = 5 + (-3) = 2$$
$$x_3 = \det \begin{pmatrix} -2 & 2 & 3 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} = 1(-1) \det \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = -3$$

Anmerkung 14.30 In der Praxis findet die Cramersche Regel wegen d er vielen zu berechnenden Determinanten kaum Anwendung.

Definition 14.31 (17.27) V endlichdimensionaler K-VR, $f \in \mathrm{End}_K(V)$. Wir wählen eine Basis $\mathcal{B}$ von V und setzen

$$\det(f) := \det(M_{\mathcal{B}}(f))$$

Dann gilt:

1. $\det(f)$ ist wohldefiniert.
2. f ist ein Isomorphismus $\iff \det(f) \neq 0$

Beweis 1. Sei $\mathcal{A}$ eine weitere Basis von V, $S := T_{\mathcal{A}}^{\mathcal{B}}$

$$\implies M_{\mathcal{A}}(f) = S M_{\mathcal{B}}(f) S^{-1} \implies \det(M_{\mathcal{A}}(f)) = \det\left(M_{\mathcal{B}}(f) S^{-1}\right) = \det(S) \det(M_{\mathcal{B}}(f)) \det\left(S^{-1}\right)$$
$$= \det(S) \det\left(S^{-1}\right) \det(M_{\mathcal{B}}(f)) = \det(M_{\mathcal{B}}(f))$$

2. f Isomorphismus

$$\iff \Phi_{\mathcal{B}}^{-1} \circ f \circ \Phi_{\mathcal{B}} = \widetilde{M_{\mathcal{B}}(f)} \text{ Isomorphismus}$$
$$\iff M_{\mathcal{B}}(f) \in GL(n, K)$$
$$\iff \det(M_{\mathcal{B}}(f)) \neq 0$$
$$\iff \det(f) \neq 0 \qquad \square$$

Anmerkung 14.32 Ist R ein kommutativer Ring, dann kann man (in Analogie zu $M(n \times n, K)$ für einen Körper K) den Ring $M(n \times n, R)$ der $n \times n$ -Matrizen mit Einträgen in R betrachten. Im Beweis von 17.12 wird nicht dividiert. Somit: Definiert man

$$\det : M(n \times n, R) \to R, \det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot A_{n\sigma(n)}, A = (a_{ij})$$

dann sind D1-D3 (für R statt K) erfüllt. (und man kann zeigen: D4 - D9, D11 sind erfüllt, $\det(A) = \det\left(A^T\right)$, $A \cdot A^{\#} = A^{\#} \cdot A = \det(A) E_n$, Entwicklungssatz von Laplace)