Lineare Algebra (Vogel)

Robin Heinemann

December 13, 2016

Contents

1 Einleitung **3**
1.1 Plenarübung . . . 3
1.2 Moodle . . . 3
1.3 Klausur . . . 3

2 Grundlagen **3**
2.1 Naive Aussagenlogik . . . 3
2.2 Beweis . . . 5
2.2.1 beweisen . . . 5
2.2.2 Beweismethoden for diese Implikation $A \implies B$ . . . 5
2.3 Existenz- und Allquantor . . . 6
2.3.1 Existenzquantor . . . 6
2.3.2 Allquantor . . . 6
2.3.3 Negation von Existenz- und Allquantor . . . 7
2.3.4 Spezielle Beweistechniken für Existenz und Allaussagen . . . 7
2.4 Naive Mengenlehre . . . 7
2.4.1 Schreibweise . . . 7
2.4.2 Angabe von Mengen . . . 7
2.4.3 leere Menge . . . 7
2.4.4 Zahlenbereiche . . . 8
2.4.5 Teilmenge . . . 8
2.4.6 Durchschnitt . . . 8
2.4.7 Vereinigung . . . 8
2.4.8 Differenz . . . 9
2.4.9 Bemerkung zu Vereinigung und Durchschnitt . . . 9
2.4.10 Bemerkung zu Äquivalenz von Mengen . . . 9
2.4.11 Kartesisches Produkt . . . 10
2.4.12 Potenzmenge . . . 10
2.4.13 Kardinalität . . . 10
2.4.14 Bemerkung zu natürlichen Zahlen . . . 11

2.4.15 Prinzip der vollständigen Induktion . . . 11
2.5 Relationen . . . 11
2.5.1 Definiten . . . 11
2.5.2 Eigenschaften von Relationen . . . 12
2.5.3 Halbordnung / Totalordnung . . . 12
2.5.4 Größtes / kleinstes Element . . . 13
2.5.5 maximales / minimales Element . . . 13
2.5.6 Äquivalenzrelation . . . 14
2.6 Abbildungen . . . 15
2.6.1 Definition . . . 15
2.6.2 Beispiel . . . 16
2.6.3 Anmerkung über den Begriff der Familie . . . 16
2.6.4 Bild . . . 16
2.6.5 Restriktion . . . 17
2.6.6 Komposition . . . 17
2.6.7 Eigenschaften von Abbildungen . . . 18

3 Gruppen, Ringe, Körper 21
3.1 Gruppe . . . 21
3.1.1 Verknüpfung . . . 21
3.1.2 Monoid . . . 21
3.1.3 Inverses . . . 22
3.1.4 Gruppe . . . 22
3.1.5 Abelsche Gruppe . . . 23
3.1.6 Permutationen . . . 24
3.1.7 Restklassen . . . 24
3.1.8 Gruppenhomomorphismus . . . 27
3.2 Ring . . . 28
3.2.1 Anmerkung . . . 29
3.2.2 Beispiel . . . 29
3.2.3 Bemerkung 6.3 . . . 29
3.2.4 Bemerkung 6.4 . . . 30
3.2.5 Integritätsbereich . . . 31
3.3 Körper . . . 32
3.3.1 Beispiel . . . 32
3.3.2 Bemerkung 6.11 . . . 32
3.3.3 Bemerkung 6.12 . . . 33
3.3.4 Folgerung 6.13 . . . 33
3.3.5 Definition 6.14 . . . 34

4 Polynome 34

5 Vektorräume 39

6 Basis und Dimension **49**

7 Matrizen **56**

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

2.2.2 Beweismethoden for 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:

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

  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:

  $$\forall\, n \in \mathbb{N}:\ n \leq 5 \text{ist falsch, dann für } n = 7 \text{ ist die Aussage } n \leq 5 \text{ falsch}$$

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 $\rfloor_A(B) = A \setminus B$

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

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

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 $x \in A \cup B \implies x \in A \vee x \in B \xRightarrow{A \subseteq B} x \in B$ "$\supseteq$": $B \subseteq A \cup B$ 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:

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

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: $1 \nsim 3, 2 \nsim 1, 2 \nsim 2$)

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 Martrikelnummer 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 $x \leq a$
$\overset{\text{Antisymmetrie}}{\Longleftrightarrow} a = x$
Analog für kleinstes Element.

2.5.6 Äquivalenzrelation

M Menge, $\sim$ auf M
$\sim$ heißt Äquivalenzrelation $\overset{\text{Def}}{\Longleftrightarrow}$ $\sim$ 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 $a, b \in M$ $a \sim b \overset{\text{Def}}{\Longleftrightarrow} a$ 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, $id_M : M \to M, m \mapsto m$ 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.: $I = \mathbb{N}, M = \mathbb{R}:$ $((m_i)_{i \in \mathbb{N}})$ 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

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

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 $x \in List$

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

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 $g \circ f = id_M$ Dann ist f injektiv und g surjektiv.

Beweis

1. f ist injektiv, denn:
   Seien $m_1, m_2 \in M$ mit $f(m_1) = f(m_2) \implies g(f(m_1)) = g(f(m_2)) \implies (g \circ f)(m_1) = (g \circ f)(m_2) \implies id_m(m_1) = id_M(m_2) \implies m_1 = m_2$
2. g ist surjektiv, denn:
   Sei $m \in M$ Dann ist $m = id_M(m) = (g \circ f)(m) = g(f(m))$

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 $g \circ f = id_M$ und $f \circ g = id_N$

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 $f \circ f = id_M$ und $f \circ g = id_N$
  - Existenz: Wir definieren $g : N \to M, n \mapsto$ das nach 2. eindeutigbestimmte Element $m \in M$ mit
    Dann gilt für $m \in M$:
    $$(g \circ f)(m) = f(f(m)) = m, \text{ das heißt } g \circ f = id_M$$
    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 $g_i \circ f = id_M, f \circ g_i = id_N$ für $i = 1, 2$
    $$\implies g_1 = g_1 \circ id_N = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = id_M \circ g_2 = g_2$$
- 3. $\implies$ 1. Wegen 3. existiert $g : N \to M$ mit $g \circ f = id_M, f \circ g = id_N$
  $$\xRightarrow{[[Bemerkung 4.12]]} f \text{ injektiv }, f \text{ surjektiv } \implies f \text{ bijektiv } \implies 1.$$

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 $f \circ g = id_N$ und $f \circ f = id_M$ 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 $g \circ f = id_M$
   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 $g \circ f = id_M$
2. f surjektiv $\iff$ Es existiert $g : N \to M$ mit $f \circ g = id_N$
   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 $f \circ g = id_N$ $\square$

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

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

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: $id_M \in S(M)$ und $id_M \circ f = f = f \circ id_M \,\forall\, f \in S(M)$
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: $f \circ f^{-1} = id_M = f^{-1} \circ f$ das heißt f^{-1} ist immer zu f bezüglich "$\circ$"

3.1.6 Permutationen

$n \in \mathbb{N}$

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

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

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

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:

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

und die Restklassen $\bar{0}, \ldots, \overline{n-1}$ 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. $$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

   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 $r \in \{0, \ldots, n-1\}$

   - Die Restklassen $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ sind paarweise verschieden denn:
     Seien $a, b \in \{0, \ldots, n-1\}$ 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 $a, b \in \{0, \ldots, n-1\}$
       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 $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$ 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. $(\frac{\mathbb{Z}}{n\mathbb{Z}})$ ist eine abelsche Gruppe:
   - Assoziativgesetz: Für alle $a, b, c \in \mathbb{Z}$ ist
     $$(\bar{a} + \bar{b}) + \bar{c} = \overline{a+b} + \bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a} + \overline{b+c} = \bar{a} + (\bar{b} + \bar{c})$$
   - $\bar{0}$ 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 $\overset{\text{Def}}{\Longleftrightarrow} \forall\, a,b,c \in G : \varphi(a * b) = \varphi(a) \circledast \varphi(b)$
φ heißt ein Gruppenisomorphismus $\overset{\text{Def}}{\Longleftrightarrow}$ 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 $(\frac{\mathbb{Z}}{n\mathbb{Z}},+)$, 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 $\overset{\text{Def}}{\Longleftrightarrow}$ 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** $\overset{\text{Def}}{\Longleftrightarrow}$ 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 "$+$", "$\cdot$" 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 $R = 0$ $\square$

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 $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot)$ ein kommutativer Ring.

Wenn wir ab jetzt vom Ring $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sprechen, dann meinen wir $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot)$ 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

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

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

6. Distributivgesetz:

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

$(\bar{a} + \bar{b}) \cdot \bar{c} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}$ 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

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

   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

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

heißt die Charakteristik von R

Beispiel 1.

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

Bemerkung 1. 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 $\mathrm{char}(R) \neq 1$

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

□

Bemerkung 2. K Körper, dann ist $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K)$ ist Primzahl.

Beweis. Folgt aus 1 und 3.3.2 □

Beispiel 2. p Primzahl, dann ist $\mathrm{char}(\mathbb{F}_{\shortmid}) = p$

4 Polynome

Definition 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), $a_0, \dots, a_n \in K$ (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 3. Man kann das auch präzise machen (Algebra 1, WS15/16, Blatt 5, Aufgabe 3)

Beispiel 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 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 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 $k := \max\{m, n\}$

$$\begin{aligned} &\implies f + g = (a_k + b_k)t^k + \ldots + (a_1 + b_1)t + (a_0 + b_0) \\ &\implies \deg(f + g) \leq k \qquad \text{(beachte: Ex könnte } a_k + b_k = 0 \text{ sein)} \end{aligned}$$

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 $\implies \deg(fg) = n + m$

□

Folgerung 1 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 6. $K[t]$ 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 $ft = 0 \implies \deg(1) = 0 \deg(ft) = \deg(f) + \deg(t) = \deg(f) + 1 \implies \deg(f) = -1 \lightning$

Satz 1 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 7.7. $f = 3t^3 + 5t + 1, g = t^2 + 1 \in \mathbb{Q}[t]$

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

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

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

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

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

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

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

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

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

□

Definition 2 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 7 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 1 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 1 □

Folgerung 2. 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 **??**

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

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 3 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 8.

- 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:

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

Satz 2 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 3 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

$$\overset{7}{\Rightarrow} \exists\, g \in \mathbb{C}[t] : f = (t-\lambda)g, \deg(g) = n-1$$

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 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 5 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 9 7.16. K Körper mit unendlich vielen Elementen.
Dann ist die Abbildung $\tilde{\ } : K[t] \to \mathrm{Abb}(K, K) := \{g : K \to K \text{ Abbildung}\}, f \mapsto \tilde{f}$ 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 3 folgt: $g = 0 \implies f_1 = f_2$ □

Bemerkung 10.
- Lässt man 9 die Voraussetzung K hat unendlich viele Elemente weg, wird die Aussage falsch, siehe Beispiel 5
- Mit dem Wissen von 5 und 9 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 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:

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

$$(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$$
$$\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$$
$$\lambda \cdot (\mu \cdot w) = (\lambda \cdot \mu) \cdot v$$
$$1 \cdot v = v$$

Bemerkung 11.

- Es ist wichtig, zwischen Addition "+" und skalarer Multiplikation "$\cdot$" 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:

$$\begin{array}{ccccccccc} & & & \text{skalare Multiplikation} & & & \text{Addition in } V & & \\ & & & \uparrow & & & \uparrow & & \\ (\lambda & + & \mu) & \cdot & v = \lambda & \cdot & v + \mu & \cdot & v \\ & \downarrow & & & & \downarrow & & \downarrow & \\ & \text{Addition in } K & & & & \text{skal. Mult.} & & \text{skal. Mult.} & \end{array}$$

- Das neutrale Element bezüglich "+" auf V bezeichnen wir mit 0_v (Nullvektor), das inverse zu $v \in V$ bezüglich "+" mit $-v$. Das Zeichen "$\cdot$" 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 6 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, $\mathrm{Abb}(M,K) := \{f : M \to K \text{ Abbildung}\}$ 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 12 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 $\lambda \neq 0_K$:
$$v = 1_K \cdot v = (\lambda^{-1}\lambda) \cdot v = \lambda^{-1} \cdot \underbrace{(\lambda v)}_{=0_V} = \lambda^{-1} \cdot 0_V = 0_V$$

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 6 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 13 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 $+ : U \times U \to Z, \cdot : K \times U \to U$

□

Bemerkung 14.
- 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 7 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 $U = \{f \in K[t] \mid \deg f \leq 2\} = \{f \in K[t] \mid \exists\, a_0, a_1, a_2 \in K : f = a_2t^2 + a_1t + a_0\}$
   - (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 15 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 UVRen 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 $v \in U, \lambda \in K \implies \forall\, i \in I : v \in U_i \implies \forall\, i \in I : \lambda v \in U_i \implies \lambda v \in \bigcap_{i \in I} U_i = U$

$\square$

Beispiel 8 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 7 8.9. V K-VR, $(v_1, \ldots, v_r)$ endliche Familie von Vektoren aus V

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

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

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

Bemerkung 16. Andere Notation für Lin : span(…), $< \ldots >$

Beispiel 9 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
   - $$v, w \in V, v \neq 0 \implies \mathrm{Lin}((v,w)) = \{\alpha_1 v + \alpha_2 w \mid \alpha_1, \alpha_2 \in \mathbb{R}\} = \begin{cases} \text{Gerade durch } 0 & w \in \mathrm{Lin}((\\ \text{Ebene durch } 0, v, w & w \notin \mathrm{Lin}((\end{cases}$$
2. $V = K^n$ als K-VR

$$e_i := (0, \ldots, 0, \underset{\substack{\downarrow \\ \text{i-te Stelle}}}{1}, 0, \ldots, 0)$$

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

Definition 8 8.11. V K-VR, $(v_i)_{i\in I}$ Familie von Vektoren aus V

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

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 $\mathrm{Lin}((v_i)_{i\in\emptyset}) := \{0\}$

Bemerkung 17. Ein Element $v \in V$ ist genau dann in $\mathrm{Lin}((v_i)_{i\in I})$ 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 $\mathrm{Lin}((v_i)_{i\in I}) = \bigcup_{J\subseteq I} \mathrm{Lin}((v_i)_{i\in J})$

Beispiel 10 8.12. $V = K[t]$ als K-VR
Es ist

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

Bemerkung 18 8.13. V K-VR, $(v_i)_{i\in I}$ Familie von Vektoren aus V. Dann gilt:

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

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

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

es folgt 3.

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

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 $v, w \in W$

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

sowie

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

- (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 $v_i \in U\, \forall\, i \in I$
$\Longrightarrow$ Jedes Element der Form $\sum\limits_{i \in I} \alpha_i v_i$ mit $\alpha_i \in K\, \forall\, i \in I, \alpha_i = 0$ für fast alle $i \in I$, liegt in U. $\Longrightarrow$ $\mathrm{Lin}((v_i)_{i \in I}) = W \subseteq U$.

3. zu zeigen:
$$\mathrm{Lin}((v_i)_{i \in I}) = \bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U\, \forall\, i \in I} U$$
"$\subseteq$" Wegen 2. liegt $\mathrm{Lin}((v_i)_{i \in I})$ in jedem UVR U von V, der alle $v_i, i \in I$ enthält
$$\Longrightarrow \mathrm{Lin}((v_i)_{i \in I} = \bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U\, \forall\, i \in I} U$$
"$\supseteq$" Nach 1. ist $W = \mathrm{Lin}((v_i)_{i \in I}$ 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
$$\Longrightarrow \bigcap_{U \text{ UVR von } V \text{ mit } v_i \in U\, \forall\, i \in I} U \subseteq W = \mathrm{Lin}((v_i)_{i \in I})$$

□

Notation: Ist $M \subseteq V$, dann setzen wir $\mathrm{Lin}(M) := \mathrm{Lin}((m)_{m \in M})$ (= kleinster UVR von V, der alle Elemente aus M enthält) Vorteil der Definition von $\mathrm{Lin}(\ldots)$ 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 9 8.14. V K-VR, $(v_1, \ldots, v_r)$ endliche Familie von Vektoren aus V, $(v_1, \ldots, v_r)$ **linear unabhängig**

$$\overset{\text{Def}}{\Longleftrightarrow} \lambda_1, \ldots, \lambda_r \in K, \lambda_1 v_1 + \ldots + \lambda_r v_r = 0 \Longrightarrow \lambda_1 = \ldots = \lambda_r = 0$$

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 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 11 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 20 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 $v \in \mathrm{Lin}((v_i)_{i\in I})$ 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, $v \in \mathrm{Lin}((v_i)_{i\in I}) \implies \exists$ 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. $\implies$ 1.: Wir setzen voraus, dass sich jeder Vektor $v \in \mathrm{Lin}((v_i)_{i\in I})$ 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

$$\sum_{i\in J} 0 \cdot i = 0$$

ist, folgt aus der vorausgesetzten Eindeutigkeit der Linearkombination, dass $\lambda_i = 0 \,\forall\, i \in J \implies (v_i)_{i\in J}$ ist linear unabhängig

□

Bemerkung 21 8.17. Sei V K-Vektorraum, Dann gilt:

1. Ist $v \in V$, dann gilt (v) linear unabhängig $\iff v \neq 0$
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 $\iff \exists\, i \in \{1, \ldots, r\} : v_i$ Linearkombination von $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_r$

Beweis.

1. " $\implies$ " (Durch Kontraposition): Sei $v = 0$. Dann ist $1v = 0$, das heißt (v) ist linear abhängig " $\impliedby$ " (Durch Kontraposition) Sei (v) linear abhängig $\implies \exists\, \lambda \in K \setminus \{0\} : \lambda v = 0 \implies v = 0$
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 $v_{i_1} = v_{i_2} \implies 1 \cdot v_{i_1} + (-1) \cdot v_{i_2} = 0 \implies (v_i)_{i \in I}$ linear abhängig
4. Sei $r \geq 2, (v_1, \ldots, v_r)$ Familie von Vektoren aus V
" $\implies$ " Sei $v_1, \ldots, v_r$ linear abhängig $\implies \exists\, \lambda_1, \ldots, \lambda_r \in K : (\lambda_1, \ldots, \lambda_r) \neq (0, \ldots, 0) \wedge \lambda_1 v_1 + \ldots \lambda_r v_r = 0$ Insbesondere existiert ein $i \in \{1, \ldots, r\}$, mit $\lambda_i \neq 0$
$$\implies v_i = -\frac{\lambda_1}{\lambda_i} v_1 - \ldots - \frac{\lambda_{i-1}}{\lambda_i} v_{i-1} - \frac{\lambda_{i+1}}{\lambda_i} v_{i+1} - \ldots - \frac{\lambda_r}{\lambda_i} v_r$$
" $\impliedby$ " 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 $\lambda_j \in K$:
$$\implies \lambda_1 v_1 + \ldots + \lambda_{i-1} v_{i-1} + (-1) v_i + \lambda i + 1 v_{i+1} + \ldots + \lambda_r v_r = 0$$
$$\implies (v_1, \ldots, v_r) \text{ linear abhängig}$$

$\square$

6 Basis und Dimension

In diesem Abschnitt sei V stets ein K-VR

Definition 10 9.1. $(v_i)_{i \in I}$ Familie von Vektoren aus V. $(v_i)_{iI}$ heißt **Erzeugendensystem** (ES) von $V \overset{Def}{\iff} V = \mathrm{Lin}((v_i)_{i \in I})$
V heißt **endlich erzeugt** $\overset{\text{Def}}{\iff}$ 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 $V \overset{\text{Def}}{\iff} (v_i)_{i \in I}$ 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 12 9.2. 1. Die Familie $(e_1, \dots, e_n)$ ist eine Basis des K_{VR} K^n, da $\mathrm{Lin}((e_1, \dots, e_n)) = K^n$ (vergleiche 8.10.2) und somit $(e_1, \dots, e_n)$ Erzeugendensystem des K^n, und $(e_1, \dots, e_n)$ linear unabhängig nach 8.15.1. Die Länge der Basis ist $(e_1, \dots, e_n)$ ist n. $(e_1, \dots, e_n)$ 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: $\mathrm{Lin}((t^n)_{n \in \mathbb{N}_0}) = K[t]$ 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 1. Jeder Vektorraum V besitzt ein ES, denn es ist $V = \mathrm{Lin}((v)_{v \in V})$
Spannende Frage: Besitzt jeder VR eine Basis?
Wir werden das zunächst für den Fall endlich erzeugter Vektorräume untersuchen

Satz 3 9.3. *$V \neq \{0\}, \mathcal{B} = (v_1, \dots, v_n)$ 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 $r \in \{1, \dots, n\}$ ist $(v_1, \dots, v_{r-1}, v_{r+1}, \dots, v_n)$ kein ES von V mehr.*

3. *Zu jedem $v \in V$ gibt es eindeutig bestimmte $\lambda_1, \dots, \lambda_n \in K$ 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 $(v_1, \dots, v_n, v)$ linear abhängig*

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

1. $\implies$ 2.: Sei $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von $V \implies \mathcal{B}$ ist ES von V
Annahme: $\mathcal{B}$ ist verkürzbar, das heißt es gibt ein $r \in \{r, \dots, n\}$, sodass $(v_1, \dots, v_{r-1}, v_{r+1}, \dots, v_n)$ immer noch ein ES von $V \implies v_r \in \mathrm{Lin}((v_1, \dots, v_{r-1}, v_{r+1}, \dots, v_n))$, das heißt

$$\exists\, \lambda_1, \dots, \lambda_{r-1}, \lambda_{r+1}, \dots, \lambda_n \in K : v_r = \lambda_1 v_1 + \ldots + \lambda_{r-1} v_{r-1} + (-1) v_r + \lambda_{r+1} v_{r+1} + \ldots + \lambda_n v_n$$

$\implies \mathcal{B}$ linear abhängig $\lightning$ zu $\mathcal{B}$ Basis von V

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

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

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

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

3. $\implies$ 4.: Wir setzte 3. vor raus, das heißt für jedes $v \in V$ existieren eindeutig bestimmt $\lambda_1, \dots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \dots + \lambda_n v_n$.
zu zeigen: $\mathcal{B}$ ist unverlängerbar linear unabhängig
denn Insbesondere existiert für jedes $v \in \mathrm{Lin}((v_1, \dots, v_n))$ eindeutig bestimmt $\lambda_1, \dots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \dots + \lambda_n v_n \implies (v_1, \dots, v_n)$ linear unabhängig. Ist $v \in V$, dann existiert $\lambda_1, \dots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \dots + \lambda_n v_n \implies (v_1, \dots, v_n, v)$ 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 $v \in V \implies (v_1, \dots, v_n, v)$ linear abhängig $\implies \exists\, \lambda_1, \dots, \lambda_n, \lambda \in K, (\lambda_1, \dots, \lambda_n, \lambda) \neq (0, \dots, 0) : \lambda_1 v_1 + \dots + \lambda_n v_n + \lambda v = 0$ Es ist $\lambda \neq 0$, da sonst $(v_1, \dots, v_n)$ linear abhängig

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

$\implies \mathcal{B}$ ist ES von V

□

Folgerung 4 9.4 Basiswahlsatz. Besitzt V ein endliches ES $(v_1, \dots, v_n)$, dann kann man aus diesem eine Basis auswählen, das heißt es gibt eine Teilmenge $\{i_1, \dots, i_r\} \subseteq \{1, \dots, n\}$, sodass $(v_{i_0}, \dots, v_{i_r})$ ein Basis von V ist. Insbesondere besitzt jeder endlich erzeuge Vektorraum eine Basis

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

Folgerung 5 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 4 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 $\lambda_1 \neq 0$:

$$v_1 = \frac{1}{\lambda_1} w - \frac{\lambda_2}{\lambda_1} v_2 - \ldots - \frac{\lambda_r}{\lambda_1} v$$

$$v = \frac{\mu_1}{\lambda_1} w + (\mu_2 - \mu_1 \frac{\lambda_2}{\lambda_1}) v_2 + \ldots + (\mu_r - \mu_1 \frac{\lambda_r}{\lambda_1}) v_r \in \mathrm{Lin}((w, v_2, \ldots, v_r))$$

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 5 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, …, 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

$(w_1, \dots, w_a)$ linear unabhängige Familie ist auch $(w_1, \dots, w_{n-1})$ linear unabhängig $\implies$ $n-1 \leq r$ und nach Umnummerieren von $\mathcal{B}$ ist auch

$$\tilde{\mathcal{B}} := (v_1, \dots, w_{n-1}, v_n, \dots, v_r)$$

eine Basis von V.

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

Da $\tilde{\mathcal{B}}$ Basis von $V, \exists\, \lambda_1, \dots, \lambda_r \in K : w_n = \lambda_1 w_1 + \dots, \lambda_{n-1} w_{n-1} \lambda_n w_n + \dots + \lambda_r$
Falls $\lambda_n = \dots = \lambda_r = 0$, dann $(w_1, \dots, w_n)$ linear abhängig $\lightning$
Also existiert ein $k \in \{n, \dots, r\}$ mit $\lambda_k \neq 0$ Nach umnummerieren von $v_n, \dots, v_r$ kann man $\lambda_n \neq 0$ erreichen

$$\implies \mathcal{B}^* := (w_1, \dots, w_{n-1}, w_n, v_{n+1}, \dots, v_r)$$

ist eine Basis von V (tausche v_n gegen w_n) □

Folgerung 6 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 $\implies$ ex existiert eine endliche Basis $(v_1, \dots, v_r)$ von V, sei $(w_i)_{i \in I}$ beliebige Basis von V. Falls I unendlich, dann existiert $i_1, \dots, i_{r+1} \in I$, so dass $(w_{i_1} + \dots + w_{i_{r+1}})$ linear unabhängig $\implies$ $r+1 \leq r \lightning$
   • Sind $(v_1, \dots, v_r), (w_1, \dots, w_k)$ 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 $\lightning$

□

Definition 11 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 2. • Der Dimensionsbegriff ist wohldefiniert nach 9.8

Beispiel 13 9.10. 1. $V = K^n$ Die Standardbasis $(e_1, \dots, e_n)$ 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 3.

- 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 7 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 $\lightning$ 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 $V \implies r+1 \leq r$ $\lightning$ 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 $V \implies n \leq \sum_k V$ $\lightning$
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 $\implies r+1 \leq \dim V = \dim U = r$ $\lightning$

$\square$

Satz 6 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 $u_{n+1} := v_{n+1}, \ldots, u_r := v_r$ $\square$

Satz 7 9.13 Zorsches Lemma. *Jede induktiv geordnete nicht leere Menge* $(M, \leq)$ *besitzt ein maximales Element. Hierbei heißt eine halbgeordnete Menge* $(m, \leq)$ ***induktiv geordnet*** $\overset{Def}{\iff}$ *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 4. Das Zornsche Lemma ist äquivalent zum Auswahlaxiom

Definition 12 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 $A := \{uj \mid j \in J\}, M := \{X \subseteq V \mid A \subseteq X \wedge X \text{ ist linear unabhängig}\}$

- $(M, \subseteq)$ 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 $S := \bigcup_{X\in T} X$, 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 $j \in \{1, \ldots, n\} \implies s_1, \ldots, s_n \subseteq X_i \overset{X_i \in M}{\Longrightarrow} (x_1, \ldots, s_n)$ 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 $n = 0$

$$\lambda v = 0 \overset{v \neq 0}{\Longrightarrow} \lambda = 0 \lightning$$

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

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

Also $\lambda \neq 0$, somit:

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

$\square$

Anmerkung 5. 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 $U = \operatorname{Lin}((v_1, \ldots, v_m)) \subseteq K^n$ Wie bestimmt man effizient die Basis von U?

Definition 13 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

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

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 22 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 $\mathrm{K_{VR}}$. 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., ”·” 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 $E_{ij}, i = 1, \ldots, m, j = 1, \ldots, n$ 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 $n > 1$:

$$\left(\begin{array}{c|c} \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right) \cdot \left(\begin{array}{c|c} \begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right) = \left(\begin{array}{c|c} \begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right)$$
$$\neq \left(\begin{array}{c|c} \begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right) \cdot \left(\begin{array}{c|c} \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right) = \left(\begin{array}{c|c} \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right)$$

□

Definition 14 **10.3.** A heißt invertierbar $\overset{\text{Def}}{\iff} \exists\, B \in M(n \times n, K) : AB = BA = E_n$

Bemerkung 23 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:

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

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 15 10.5. $A \in M(m \times n, K)$ mit Zeilen $a_1, \dots, a_m \in K^n$
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 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 16 10.6. $A \in M(m \times n, K)$ mit Zeilen $a_1, \dots, a_m \in K^n$

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

heißt Zeilenraum von A.

Beispiel 14 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 24 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:

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

Dies gilt, da jeder UVR von K^n, der $a_1, \dots, a_m$ enthält, auch $a_1, \dots, a_{j-1}, \lambda a_j, a_{j+1}, \dots, a_m$ 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:

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

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 $\mathrm{Lin}((a_1, \ldots, a_m)) = ZR(A) = ZR(B)$ ablesen kann.

Definition 17 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 15 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 18 10.11. $A \in M(m \times n, K)$
Dann lässt sich A durch endlich viele elementare Zeilenstufenumformungen in eine Matrix B in ZSF umformen:

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

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 $j_1 \in \{1, \ldots, n\}$, so dass es ein $i_1 \in \{1, \ldots, m\}$ 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:

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

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

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

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 string monoton fallend in $\mathbb{N}$ ist, oder irgendwann eine Matrix $A_k = 0$ entsteht.
$\Longrightarrow$ erhalte ZSF. Die ersten r Zeilen $b_1, \ldots, b_r$ von B bilden eine Basis von $ZR(A)$, denn Es ist $ZR(A) = ZR(B) = \mathrm{Lin}((b_1, \ldots, b_r))$
noch zu zeigen: $(b_1, \ldots, b_r)$ ist linear unabhängig.
Es seien $\lambda_1, \ldots, \lambda_r \in K$ mit $\lambda_1 b_1 + \ldots + \lambda_r b_r = 0$. In der j_1-ten Komponente von $\lambda_1 b_1 + \ldots + \lambda_r b_r$ steht $\lambda_1 b_{1j_1} = 0$. Wegen $b_{1j_1} = 0$ folgt $\lambda_1 = 0$. In der j_2-ten Komponente von $\lambda_1 v_1 + \ldots + \lambda_r b_r = \lambda_2 b_2 + \ldots + \lambda_r b_r$ steht $\lambda_2 b_{2j_2} = 0$ Wegen $b_{2j_2} \neq 0$ folgt $\lambda_2 = 0$. Durch Iterieren dieses Arguments erhalten wir $\lambda_1 = \ldots = \lambda_r = 0$

□

Algorithmus 1 10.12. Eingabe: $W = \mathrm{Lin}((v_1, \ldots, v_m)) \subseteq K^n$
Ausgabe: Eine Basis $(w_1, \ldots, w_r)$ 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 16 10.13. $W = \mathrm{Lin}((0,0,3,-1),(0,1,2,0),(0,3,0,2)) \subseteq \mathbb{R}^4$

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

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