

# Mathematik für Informatiker I

Andre Johnson

9. Februar 2018



# Inhaltsverzeichnis

<b>1</b>	<b>Mathematische Grundlagen</b>	<b>5</b>
1.1	Aussagen . . . . .	5
1.1.1	Logische Verknüpfungen (Junktoren) . . . . .	5
1.2	Mengen . . . . .	7
1.2.1	Beschreibung von Mengen . . . . .	7
1.3	Existenz- und Allquantoren . . . . .	8
1.4	Mengenoperationen . . . . .	9
<b>2</b>	<b>Relationen &amp; Funktionen</b>	<b>13</b>
2.1	Grundbegriffe zu Relationen . . . . .	13
2.2	Abbildungen und Funktionen . . . . .	14
2.3	Äquivalenzrelationen . . . . .	17
2.4	Ordnungsrelation . . . . .	19
<b>3</b>	<b>Zahlenbereiche</b>	<b>21</b>
3.1	Natürliche Zahlen: Definition . . . . .	21
3.1.1	Notation: Produkt- und Summenschreibweise . . . . .	21
3.2	Vollständige Induktion . . . . .	22
3.3	Rekursive Abbildungen . . . . .	23
3.4	Ganze, rationale und reelle Zahlen . . . . .	24
3.5	Komplexe Zahlen . . . . .	25

<b>4</b>	<b>Folgen und Grenzwerte</b>	<b>27</b>
4.1	Konvergenz . . . . .	27
4.2	Monotone Folgen . . . . .	30
4.3	Uneigentliche Konvergenz . . . . .	30
4.4	Landau-Symbole . . . . .	31
<b>5</b>	<b>Der Ring <math>\mathbb{Z}</math></b>	<b>35</b>
5.1	Gruppen . . . . .	35
5.2	Ringe und Körper . . . . .	37
5.3	Division mit Rest . . . . .	38
5.4	Euklidischer Algorithmus . . . . .	39
5.5	Primfaktorzerlegung (PFZ) . . . . .	41
5.6	Rechnen modulo $n$ . . . . .	43
5.6.1	Addition & Multiplikation modulo $n$ . . . . .	43
5.6.2	Einheiten und Inverse . . . . .	45
<b>6</b>	<b>Gruppentheorie</b>	<b>51</b>
6.1	Untergruppen . . . . .	51
6.2	Gruppenordnungen & Satz von Lagrange . . . . .	53
6.3	Zyklische Gruppen . . . . .	55
<b>7</b>	<b>Lineare Algebra</b>	<b>57</b>
7.1	Vektorräume . . . . .	57
7.2	Unterräume . . . . .	60
7.3	Erzeugendensysteme . . . . .	60
7.4	Lineare Unabhängigkeit . . . . .	61
7.5	Basis und Dimension . . . . .	62
<b>8</b>	<b>Lineare Algebra II: Lineare Abbildungen</b>	<b>65</b>
8.1	Grundlagen und Isomorphismen . . . . .	65
8.2	Kern und Bild, Dimensionsformel . . . . .	67
8.3	Matrizen . . . . .	68
<b>A</b>	<b>Beweise</b>	<b>75</b>
A.1	zu Kapitel 8 Lineare Algebra II: Lineare Abbildungen . . . . .	75

# Kapitel 1

## Mathematische Grundlagen

### 1.1 Aussagen

#### 1.1.1 Logische Verknüpfungen (Junktoren)

##### Definition 1.1

Seien im Folgenden  $A$  und  $B$  Aussagen

- (i) Die *Negation* von  $A$  ist die Aussage “nicht  $A$ ”. Wir verwenden die Schreibweise

$$\neg A \tag{1.1}$$

Wenn  $A$  wahr ist, dann ist  $\neg A$  falsch. Wenn  $A$  falsch ist, dann ist  $\neg A$  wahr.

- (ii) Die Verbindung von  $A$  und  $B$  durch “und” heißt *Konjunktion*. Wir schreiben

$$A \wedge B \tag{1.2}$$

$A \wedge B$  ist wahr, wenn  $A$  und  $B$  wahr sind, sonst falsch.

- (iii) Die Verkettung von  $A$  und  $B$  durch “oder” heißt *Disjunktion* wir schreiben

$$A \vee B \tag{1.3}$$

$A \vee B$  ist falsch, wenn  $A$  und  $B$  beide falsch sind.

- (iv) Die Verkettung von  $A$  und  $B$  zu “wenn  $A$ , dann  $B$ ” heißt *logische Folgerung* oder *Implikation*. Wir schreiben

$$A \Rightarrow B \quad (1.4)$$

$A$  heißt *Voraussetzung*,  $B$  *Behauptung* der Implikation. Die Implikation ist wahr, wenn  $A$  falsch ist oder  $B$  wahr ist, andernfalls ist die falsch.

- (v) Die Verkettung von  $A$  und  $B$  zu “genau dann  $A$ , wenn  $B$ ” heißt *Äquivalenz*. Wir schreiben

$$A \Leftrightarrow B \quad (1.5)$$

Die Äquivalenz ist wahr, wenn  $A$  und  $B$  den selben Wahrheitswert haben.

Wahrheitstafel

$A$	$B$	$\neg A$	$\neg B$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	f	f	w	w	w	w
w	f	f	w	f	w	f	f
f	w	w	f	f	w	w	f
f	f	w	w	f	f	w	w

### Definition 1.2

Ein logischer Ausdruck, der für beliebige Wahrheitswerte der enthaltenen Aussagen immer wahr ist, heißt *Tautologie*.

### Satz 1.3

$A$  und  $B$  seien Aussagen.

Dann sind folgende Aussagen Tautologien:

- a) *De Morgan'sche Regeln*:

$$\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B) \quad (1.6)$$

$$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B) \quad (1.7)$$

b)

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A) \quad (1.8)$$

## 1.2 Mengen

### Schreibeweise:

$x \in M$  steht für die Aussage “ $x$  ist ein *Element* der Menge  $M$ ”

### Definition 1.4: Standardbezeichnungen

$$\mathbb{N} = \{1, 2, 3, 4, \dots\} \text{ natürliche Zahlen} \quad (1.9)$$

$$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\} \text{ natürliche Zahlen mit Null} \quad (1.10)$$

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \text{ ganze Zahlen} \quad (1.11)$$

$$\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\} \text{ rationale Zahlen} \quad (1.12)$$

$$\mathbb{R} \text{ reelle Zahlen} \quad (1.13)$$

$$\emptyset \text{ leere Menge} \quad (1.14)$$

### 1.2.1 Beschreibung von Mengen

#### Beschreibung von Mengen

- Durch *Aufzählen der Elemente*  
Bsp.:

$$M = \{1, 2, 3\} \quad (1.15)$$

$$G = \{2, 4, 6, 8, \dots\} \quad (1.16)$$

- in *beschreibender Form*  
Bsp.:

$$G = \{x : x \in \mathbb{N} \text{ und } x \text{ ist gerade}\} \quad (1.17)$$

$$= \{x \in \mathbb{N} : x \text{ ist gerade}\} \quad (1.18)$$

Allgemeine Form:

$$M = \{x : A(x)\} \quad A \text{ Aussage} \quad (1.19)$$

- in *abgekürzter beschreibender Form*  
Bsp.:

$$G = \{2m : m \in \mathbb{N}\} \quad (1.20)$$

## 1.3 Existenz- und Allquantoren

### Definition 1.5

Sei  $M$  eine nicht-leere Menge, und für jedes  $x \in M$  sei  $A(x)$  eine Aussage.

- (i) Die Aussage “Für Alle  $x \in M$  gilt  $A(x)$ .” bezeichnen wir mit

$$\forall x \in M : A(x) \quad (\forall \text{ Allquantor}) \quad (1.21)$$

- (ii) Die Aussage “Es gibt ein  $x \in M$ , für das  $A(x)$  gilt” bezeichnen wir mit

$$\exists x \in M : A(x) \quad (\exists \text{ Existenzquantor}) \quad (1.22)$$

- (iii) Die Aussage “Es gibt genau ein  $x \in M$ , für das  $A(x)$  gilt” bezeichnen wir mit

$$\exists! x \in M : A(x) \quad (1.23)$$

### Lemma 1.6

Sei  $M$  eine nicht leere Menge und für jedes  $x \in M$  sei  $A(x)$  eine Aussage. Dann gilt:

$$\neg(\forall x \in M : A(x)) \Leftrightarrow (\exists x \in M : A(x)) \quad (1.24)$$



## 1.4 Mengenoperationen

### Definition 1.7

Seien  $X$  und  $Y$  Mengen

- $X$  heißt *Teilmenge* von  $Y$ , falls gilt

$$\forall x \in X : x \in Y \quad (1.25)$$

Wir schreiben dann:

$$X \subseteq Y \quad (1.26)$$

(*Inklusion* von  $X$  in  $Y$ )

- Wenn  $X$  keine Teilmenge von  $Y$  ist, schreiben wir

$$X \not\subseteq Y \quad (1.27)$$

- $X$  heißt Teilmenge von  $Y$  und  $X \neq Y$ : Wir schreiben dann

$$X \subset Y \text{ oder } X \subsetneq Y \quad (1.28)$$

$$(\forall x \in X : x \in Y) \wedge (\exists y \in Y \notin X) \quad (1.29)$$

- *Durchschnitt*

$$X \cap Y := \{z : z \in X \wedge z \in Y\} \quad (1.30)$$

- *Vereinigung*

$$X \cup Y := \{z : z \in X \vee z \in Y\} \quad (1.31)$$

- *Differenzmenge*

$$X \setminus Y := \{z : z \in X \wedge z \notin Y\} \quad (1.32)$$

- Falls  $Y \subseteq X$ , dann heißt  $X \setminus Y$  das *Komplement* von  $Y$  in  $X$
- Wenn  $X \cap Y = \emptyset$ , dann heißen  $X$  und  $Y$  *disjunkt*

**Satz 1.8**

Sei  $M$  eine Menge und  $X, Y, Z$  Teilmengen von  $M$ . Dann gelten

a)

$$M \cap \emptyset = \emptyset \quad (1.33)$$

$$X \cup M = M \quad (1.34)$$

$$X \cup \emptyset = X \quad (1.35)$$

$$X \cap M = M \quad (1.36)$$

b) *Idempotenz*

$$X \cup X = X \quad (1.37)$$

$$X \cap X = X \quad (1.38)$$

c) *Kommutativität*

$$X \cap Y = Y \cap X \quad (1.39)$$

$$x \cup Y = Y \cup X \quad (1.40)$$

d) *Assoziativität*

$$(X \cup Y) \cap Z = X \cap (Y \cup Z) \quad (1.41)$$

$$(X \cap Y) \cup Z = X \cup (Y \cap Z) \quad (1.42)$$

e)

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) \quad (1.43)$$

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \quad (1.44)$$

f)

$$M \setminus (X \cap Y) = (M \setminus X) \cup (M \setminus Y) \quad (1.45)$$

$$M \setminus (X \cup Y) = (M \setminus X) \cap (M \setminus Y) \quad (1.46)$$

Um zu beweisen, dass zwei Mengen  $A$  und  $B$  gleich sind, zeigt man oft  $A \subseteq B$  und  $B \subseteq A$

**Definition 1.9**

Seien  $X, Y$  Mengen.

Das *kartesische Produkt* von  $X$  und  $Y$  ist

$$X \times Y = \{(x, y) : x \in X \wedge y \in Y\} \quad (1.47)$$

$(x, y) \in X \times Y$  heißt *geordnetes Paar*.

Allgemein definiert man für Mengen  $X_1, X_2, \dots, X_n$

$$X_1 \times X_2 \times \dots \times X_n := \{(x_1, x_2, \dots, x_n) : x_i \in X_i \text{ für alle } i \in [1, n]\} \quad (1.48)$$

$(x_1, \dots, x_n) \in X_1 \times \dots \times X_n$  heißt *geordnetes  $n$ -Tupel*



# Kapitel 2

## Relationen & Funktionen

### 2.1 Grundbegriffe zu Relationen

#### Definition 2.1

Seien  $A, B$  Mengen,  $G \subseteq A \times B$

Dann bezeichnet man das Tripel  $(A, B, G)$  als zweistellige/binäre *Relation* zwischen  $A$  und  $B$ .  $G$  heißt *Graph* der Relation.

Wenn  $(a, b) \in G$ , dann sagen wir, dass  $a$  und  $b$  in *Relation zueinander stehen*, oder *reliert* sind. Wir schreiben dann

$$a \sim b \tag{2.1}$$

Falls  $A = B$ , heißt  $(A, A, G)$  *Relation auf  $A$*

Bemerkung: Manchmal wird  $\sim$  oder  $G$  als Relation bezeichnet.

#### Definition 2.2

Sei  $A$  eine Menge,  $(A, A, G)$  Relation auf  $A$ . Die Relation heißt

- *reflexiv*, falls  $a \sim a$  für jedes  $a \in A$
- *symmetrisch*, falls aus  $a \sim b$  stets folgt, dass  $b \sim a$

- *antisymmetrisch*, falls aus  $a \sim b$  und  $b \sim a$  stets folgt, dass,  $a = b$ <sup>1</sup>
- *transitiv*, falls aus  $a \sim b$  und  $b \sim c$  stets folgt, dass,  $a \sim c$

### Definition 2.3

Sei  $(A, B, G)$  eine Relation. Setze

$$G^{-1} := \{(b, a) \in B \times A : (a, b) \in G\} \quad (2.2)$$

$(B, A, G^{-1})$  heißt die zu  $(A, B, G)$  *inverse Funktion*. Falls  $(b, a) \in G^{-1}$ , schreiben wir

$$b \overset{-1}{\sim} a \quad (2.3)$$

## 2.2 Abbildungen und Funktionen

### Definition 2.4

Seien  $X, Y$  Mengen

Eine *Abbildung* (*Funktion* von  $X$  nach  $Y$ ) ist gegeben durch eine *Vorschrift*  $f$ , die jedem Element  $x \in X$  genau ein Element  $y \in Y$  zuordnet. Man schreibt

$$y = f(x) \quad (2.4)$$

Für die gesamte Abbildung schreibt man

$$f : X \rightarrow Y \quad (2.5)$$

Für  $x \in X$  schreiben wir

$$x \mapsto f(x) \quad (2.6)$$

$X$  heißt der *Definitionsbereich* von  $f$

$Y$  heißt der *Ziel-/Wertebereich* von  $f$

Bemerkung: Die *Zuordnung*  $f$  definiert eine Relation  $(X, Y, G)$  durch

$$(x, y) \in G :\Leftrightarrow y = f(x) \quad (2.7)$$

---

<sup>1</sup>antisymmetrisch  $\Leftrightarrow \forall (a, b) \in A \times B : ((a, b) \in G \wedge (b, a) \in G \Rightarrow a = b)$



Abbildung 2.1: Komposition

**Definition 2.5**

Sei  $f : X \rightarrow Y$  Abbildung

- Für  $Z \subseteq X$  definieren wir

$$f(Z) := \{y \in Y : \exists x \in Z : f(x) = y\} \quad (2.8)$$

$$= \{f(x) : x \in Z\} \quad (2.9)$$

$f(Z)$  heißt das *Bild von Z unter f*

$f(X)$  heißt das *Bild von f*

- Für  $M \subseteq Y$  definieren wir

$$f^{-1}(M) := \{x \in X : f(x) \in M\} \quad (2.10)$$

$f^{-1}$  heißt das *Urbild von M unter f*

**Definition 2.6**

Seien  $f : X \rightarrow Y$  und  $g : Y' \rightarrow Z$ , wobei  $Y \subseteq Y'$

Die *Komposition/Verkettung/Hintereinanderausführung*

$$g \circ f : X \rightarrow Z \quad (2.11)$$

ist definiert durch

$$(g \circ f)(x) = g(f(x)) \text{ für alle } x \in X \quad (2.12)$$

**Lemma 2.7**

Die Komposition von Abbildungen ist *assoziativ*, d. h. wenn  $f : X \rightarrow Y, g : Y' \rightarrow Z$  und  $h : Z' \rightarrow W$  Abbildungen sind mit  $Y \subseteq Y'$  und  $Z \subseteq Z'$ , dann gilt

$$h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f \quad (2.13)$$

**Definition 2.8**

Eine Abbildung  $f : X \rightarrow Y$  heißt

- *injektiv*: falls für alle  $a, b \in X$  gilt

$$a \neq b \Rightarrow f(a) \neq f(b) \quad (2.14)$$

- *surjektiv*: falls

$$f(X) = Y \quad (2.15)$$

- *bijektiv*: wenn  $f$  surjektiv und injektiv ist

**Lemma 2.9**

Seien  $X, Y, Z$  Mengen,  $f : X \rightarrow Y, g : Y \rightarrow Z$

- 1) Wenn  $f$  und  $g$  surjektiv sind, dann ist auch  $g \circ f$  surjektiv.
- 2) Wenn  $f$  und  $g$  injektiv sind, dann ist auch  $g \circ f$  injektiv.
- 3) Wenn  $f$  und  $g$  bijektiv sind, dann ist auch  $g \circ f$  bijektiv.

**Definition 2.10**

Sei  $M$  eine Menge. Die Abbildung

$$\text{id}_X : X \rightarrow X \quad (2.16)$$

$$\text{id}_X(x) : x \mapsto x \text{ für alle } x \in X \quad (2.17)$$

heißt *identische Abbildung*.



**Satz 2.11**

Sei  $f : X \rightarrow Y$  eine Abbildung. Die folgenden Aussagen sind äquivalent:

$$(A) \ f \text{ ist bijektiv} \quad (2.18)$$

$$(B) \ \text{Es gibt eine Abbildung } g : Y \rightarrow X, \text{ so dass } g \circ f = \text{id}_X \text{ und } f \circ g = \text{id}_Y \quad (2.19)$$

Beweis: siehe ??, S. ??

## 2.3 Äquivalenzrelationen

**Definition 2.12**

Sei  $M$  eine nicht-leere Menge.

Eine Relation auf  $M$  heißt *Äquivalenzrelation*, wenn sie reflexiv<sup>2</sup>, symmetrisch<sup>3</sup> und transitiv<sup>4</sup> ist. Für  $x \in M$  nennt man

$$[x]_{\sim} := [x] := \{y \in M : x \sim y\} \quad (2.20)$$

die *Äquivalenzklasse* von  $x$ .

Die Menge aller Äquivalenzklassen bezeichnet man mit  $M/\sim$

**Definition 2.13**

Sei  $M$  eine nicht-leere Menge,  $I$  eine Indexmenge.

Eine *Partition* von  $M$  ist eine Menge

$$\{A_i : A_i \subseteq M, i \in I\} \quad (2.21)$$

von Teilmengen von  $M$ , so dass

(i)

$$A_i \neq \emptyset \text{ für alle } i \in I \quad (2.22)$$

---

<sup>2</sup>reflexiv:  $\forall a \in A : a \sim a$ , d. h.  $(a, a) \in G$

<sup>3</sup>symmetrisch:  $\forall a \in A : \forall b \in A : a \sim b \Rightarrow b \sim a$

<sup>4</sup>transitiv:  $\forall a \in A : \forall b \in A : \forall c \in A : (a \sim b \wedge b \sim c) \Rightarrow a \sim c$

(ii) für  $i, j \in I$  mit  $i \neq j$ ,

$$A_i \cap A_j = \emptyset \quad (2.23)$$

(iii) <sup>5</sup>

$$\bigcup_{i \in I} A_i = M \quad (2.24)$$

### Satz 2.14

Sei  $M$  eine nichtleere Menge

- a) Für jede Äquivalenzklasse auf  $M$  ist  $M / \sim$  eine Partition von  $M$
- b) Ist  $\{A_i \subseteq M : i \in I\}$  eine Partition von  $M$ , dann ist

$$x \sim y :\Leftrightarrow \text{Es gibt ein } i \in I \text{ so dass } x, y \in A_i \quad (2.25)$$

eine Äquivalenzrelation auf  $M$ . Es gilt

$$M / \sim = \{A_i : i \in I\} \quad (2.26)$$

### Definition 2.15

Zwei Mengen  $X, Y$  heißen *gleichmächtig*, wenn es eine bijektive Abbildung  $f : X \rightarrow Y$  gibt.

Eine Menge  $M$  heißt *endlich*, wenn sie gleichmächtig ist zu einer Menge der Form  $\{1, 2, 3, \dots, n\}$  für  $n \in \mathbb{N}$ .  $n \in \mathbb{N}$  heißt *Mächtigkeit* von  $M$ . Wir schreiben

$$|M| = n \quad (2.27)$$

Ist  $M$  nicht endlich, so schreibt man

$$|M| = \infty \quad (2.28)$$

---

<sup>5</sup>Vereinigung aller Mengen  $A_i$  mit  $i \in I$

## 2.4 Ordnungsrelation

### Definition 2.16

- a) Eine *Halbordnung* auf eine Menge  $M$  ist eine reflexive, antisymmetrische<sup>6</sup> und transitive Relation auf  $M$ .
- b) Eine *totale/binäre Ordnung* auf  $M$  ist eine Halbordnung auf  $M$ , so dass für alle  $x, y \in M$  gilt  $x \sim y$  oder  $y \sim x$

**Notation:** Für Halbordnungen schreiben wir für  $x \sim y$  gerne

$$x \preceq y \quad (2.29)$$

**Bemerkung:** Halbordnungen können durch *Hasse-Diagramme* dargestellt werden. Man verbindet  $a$  und  $b$  durch eine Kante, wenn  $a \preceq b$  und es kein drittes Element  $c$  ( $c \neq a, c \neq b$ ) gibt, so dass  $a \preceq c \preceq b$ . Im Hasse-Diagramm steht  $b$  über  $a$ .

Bsp.:  $\{1, 2, 3\}$  mit  $\leq$  Relation:

$$\begin{array}{c} 3 \\ | \\ 2 \\ | \\ 1 \end{array}$$

### Definition 2.17

Sei  $A$  eine halbgeordnete Menge,  $T \subseteq A$  Teilmenge.

- ① Ein Element  $m \in T$  heißt *minimal* in  $T$ , wenn es kein  $t \in T$  mit  $t \neq m$  und  $t \preceq m$ . (entsprechend “*maximal*”)
- ② Wenn  $m \in T$  und  $m \preceq t$  für alle  $t \in T$ , dann heißt  $m$  *Minimum* von  $T$ . (entsprechend “*Maximum*”)
- ③ Wenn  $s \in A$  und  $s \preceq t$  für alle  $t \in T$ , dann heißt  $s$  *untere Schranke* für  $T$  in  $A$ . (entsprechend “*obere Schranke*”)

---

<sup>6</sup>antisymmetrisch:  $\forall (a, b) \in M \times M : a \sim b \wedge b \sim a \Rightarrow a = b$

**Beispiel** Betrachte Menge  $A = \{a, b, c, d, e, f, g\}$  mit Halbordnung gegeben durch Hasse-Diagramm. Betrachte Teilmenge  $T = \{a, b, c\}$

**Bemerkung** Die “größte” untere Schranke  $e$  (d. h.  $e$  ist untere Schranke und für jede untere Schranke  $s$  gilt  $s \preccurlyeq e$ ) heißt *Infimum* von  $T$  in  $A$ .  
Die “kleinste” obere Schranke heißt *Supremum*.

# Kapitel 3

## Zahlenbereiche

### 3.1 Natürliche Zahlen: Definition

#### Definition 3.1: Peano-Axiome

- ① 1 ist eine natürliche Zahl.
- ② Jede natürliche Zahl hat genau einen von 1 verschiedenen Nachfolger  $n^+$ , der eine natürliche Zahl ist (gemeint ist  $n + 1$ ).
- ③ Verschiedene natürliche Zahlen haben verschiedene Nachfolger.
- ④ Ist  $M \subseteq \mathbb{N}$  mit  $1 \in M$  und der Eigenschaft, dass für alle  $n \in M$  auch  $n^+ \in M$  folgt, so gilt  $M = \mathbb{N}$

#### 3.1.1 Notation: Produkt- und Summenschreibweise

Seien  $k, n \in \mathbb{N}$  und  $a_j \in \mathbb{C}$  oder  $\mathbb{R}$ . Wir schreiben:

$$\sum_{j=k}^n a_j := \begin{cases} 0 & \text{falls } n < k \\ a_k & \text{falls } n = k \\ \sum_{j=k}^{n-1} & \text{falls } n > k \end{cases} \quad (3.1)$$

$$\prod_{j=k}^n a_j := \begin{cases} 1 & \text{falls } n < k \\ a_k & \text{falls } n = k \\ \prod_{j=k}^{n-1} & \text{falls } n > k \end{cases} \quad (3.2)$$

## 3.2 Vollständige Induktion

**Idee** Für  $n \in \mathbb{N}$  sei  $A(n)$  eine Aussage über  $n$ . Ist die Aussage  $A(1)$  wahr (“*Induktionsanfang*”) und folgt für jedes  $n \in \mathbb{N}$  die Aussage  $A(n+1)$  (“*Induktionsschritt*”), dann ist  $A(n)$  wahr für alle  $n \in \mathbb{N}$ .

**Beweisskizze** Sei

$$M := \{n \in \mathbb{N} : A(n) \text{ wahr}\} \quad (3.3)$$

Dann

$$1 \in M \text{ (Induktionsanfang)} \quad (3.4)$$

Falls  $n \in M$ , dann gilt

$$(n+1) \in M \text{ (Induktionsschritt)} \quad (3.5)$$

Nach Peano ④  $M = \mathbb{N}$  □

### Lemma 3.2

Für alle  $n \in \mathbb{N}$  gilt

$$1 + \cdots + n := \sum_{j=1}^n j = \frac{n(n+1)}{2} \quad (3.6)$$

**Definition 3.3**

Für  $n \in \mathbb{N}_0$  und  $a \in \mathbb{C}$  setzt man

$$a^n := \prod_{j=1}^n a \quad (3.7)$$

$$\text{Insbesondere: } a^0 = 1 \quad (3.8)$$

Für  $a \neq 0$  und  $n \in \mathbb{Z}$  mit  $n < 0$  setzt man

$$a^n := (a^{-1})^{-n}, a^{-1} = \frac{1}{a} \quad (3.9)$$

**Lemma 3.4**

Sei  $x \in \mathbb{R}, x \neq 1$ . Dann gilt für alle  $n \in \mathbb{N}_0$

$$1 + x + \cdots + x^n = \sum_{j=0}^n x^j = \frac{1 - x^{n+1}}{1 - x} \quad (3.10)$$

**3.3 Rekursive Abbildungen**

**Beispiel:**

$$\sum_{j=n}^n a_j := a_n, \sum_{j=n}^N := \sum_{j=n}^{N-1} a_j + a_N \text{ für } N > n \quad (3.11)$$

$$\prod_{j=n}^n a_j := a_n, \prod_{j=n}^N := \left( \prod_{j=n}^{N-1} a_j \right) \cdot a_N \text{ für } N > n \quad (3.12)$$

**Definition 3.5**

Für  $n \in \mathbb{N}_0$  definieren wir

$$n! := \begin{cases} 1 & \text{falls } n = 0 \\ (n-1)! \cdot n & \text{falls } n \geq 1 \end{cases} \quad (3.13)$$

D. h.:  $n! = 1 \cdot 2 \cdot \dots \cdot n$  für  $n \geq 1$

### Lemma 3.6

Für alle  $n \in \mathbb{N}$  mit  $n \geq 4$  gilt

$$n! > 2^n = \underbrace{2 \cdot 2 \cdot \dots \cdot 2}_{n \text{ Faktoren}} \quad (3.14)$$

### Beispiel: Die Fibonacci-Zahlen

$$F(n), n \in \mathbb{N} \text{ sind rekursiv definiert:} \quad (3.15)$$

$$F(1) := 1, F(2) := 1, F(n+1) := F(n) + F(n-1), n \geq 2 \quad (3.16)$$

$$\text{Also: } F(3) = F(2) + F(1) = 1 + 1 = 2 \quad (3.17)$$

$$F(4) = F(3) + F(2) = 3 \quad (3.18)$$

$$F(5) = 5 \quad (3.19)$$

### Lemma 3.7

Für alle  $n \in \mathbb{N}$  gilt  $F(n) < 2^n$

## 3.4 Ganze, rationale und reelle Zahlen

Wir werden die ganzen Zahlen

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}, \quad (3.20)$$

die rationalen Zahlen

$$\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\} \quad (3.21)$$

und die reellen Zahlen  $\mathbb{R}$  nicht mathematisch sauber einführen, sondern “naiv” verwenden. Es gilt

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \quad (3.22)$$



und wir verwenden die bekannte Totalordnung auf diese Mengen

$$\text{Wichtig: } a \geq b \Leftrightarrow -b \geq -a \quad (3.23)$$

Für rationale Zahlen (“Brüche”)  $\frac{a}{b}$  und  $\frac{c}{d} \in \mathbb{Q}$  definiert man

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \quad (3.24)$$

$$\text{Bsp.: } \frac{2}{3} + \frac{1}{4} = \frac{11}{12} = \frac{8+3}{12} \quad (3.25)$$

und

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d} \quad (3.26)$$

$$\text{Bsp.: } \frac{2}{3} \cdot \frac{1}{4} = \frac{2}{12} = \frac{1}{6} \quad (3.27)$$

Die reellen Zahlen kann man sich vorstellen, als die Menge aller Dezimaldarstellungen. Der Übergang von  $\mathbb{Q}$  zu  $\mathbb{R}$  “füllt” man die “Löcher” im Zahlenstrahl.

## 3.5 Komplexe Zahlen

Wir starten bei  $\mathbb{R}$  und fügen das Element  $i$  dazu mit der Eigenschaft

$$i^2 = -1 \quad (3.28)$$

$i$  heißt auch *imaginäre Zahl*.

### Definition 3.8

Wir definieren die Menge  $\mathbb{C}$  der *komplexen Zahlen*

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\} \quad (3.29)$$

wobei

$$a + bi = a' + b'i : \Leftrightarrow a = a' \wedge b = b' \quad (3.30)$$

Für eine komplexe Zahl  $z = a + bi$  mit  $a, b \in \mathbb{R}$  nennt man

$$a = \operatorname{Re}(z) \text{ den } \textit{Realteil} \text{ und} \quad (3.31)$$

$$b = \operatorname{Im}(z) \text{ den } \textit{Imaginärteil} \quad (3.32)$$

**Bemerkung**  $\operatorname{Re}(z)$  und  $\operatorname{Im}(z)$  sind reelle Zahlen.

**Definition 3.8 (fortgesetzt)**

Für komplexe Zahlen  $a + bi, c + di$  mit  $a, b, c, d \in \mathbb{R}$  definiert man

$$(a + bi) + (c + di) = (a + c) + (b + d)i \quad \text{und} \quad (3.33)$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i \quad (3.34)$$

Addition von komplexen Zahlen entspricht der Addition von Vektoren.

**Definition 3.9**

Für  $z = a + bi \in \mathbb{C}$  mit  $a, b \in \mathbb{R}$  heißt

- $|z| := \sqrt{a^2 + b^2} \in \mathbb{R}$  der *Betrag* von  $z$
- $\bar{z} := a - bi \in \mathbb{C}$  die *konjugent-komplexe Zahl*

**Lemma 3.10**

Seien  $z, w \in \mathbb{C}$ . Dann gilt:

- (i)  $\overline{\bar{z}} = z$
- (ii)  $\overline{z + w} = \bar{z} + \bar{w}$
- (iii)  $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
- (iv)  $|z \cdot w| = |z| \cdot |w|$
- (v)  $|\bar{z}| = |z|$

# Kapitel 4

## Folgen und Grenzwerte

### Definition 4.1

Eine (reelle) *Folge* ist eine Abbildung  $a : \mathbb{N} \rightarrow \mathbb{R}$ . Wir schreiben  $a_n = a(n)$ .  $a_n$  heißen *Glieder* der Folge  $a$ .

### Definition 4.2: Beschränktheit

Eine Folge  $a : \mathbb{N} \rightarrow \mathbb{R}$  heißt *beschränkt*, falls es ein  $L \in \mathbb{R}$  gibt, so dass  $|a_n| \leq L$  für alle  $n \in \mathbb{N}$ . Das heißt

$$\exists L \in \mathbb{R} : \forall n \in \mathbb{N}. |a_n| \leq L \quad (4.1)$$

## 4.1 Konvergenz

### Definition 4.3

Sei  $a : \mathbb{N} \rightarrow \mathbb{R}$  eine Folge, und  $a_* \in \mathbb{R}$ . Die Folge  $a$  konvergiert gegen  $a_*$ , falls gilt

$$\forall \varepsilon > 0 \exists N_0 \in \mathbb{N} \forall n \geq N_0 : |a_n - a_*| < \varepsilon \quad (4.2)$$

Wir schreiben dann  $\lim_{n \rightarrow \infty} a_n = a_*$  oder  $a_n \rightarrow a_*$ .

$a_*$  heißt dann *Grenzwert* der Folge  $a$

$a$  heißt *konvergent*

Falls eine Folge nicht konvergent ist, heißt sie *divergent*

**Bemerkung:**

- Eine Folge, die gegen 0 konvergiert heißt *Nullfolge*
- Eine Folge  $a$  ist genau dann eine Nullfolge, wenn  $|a| : \mathbb{N} \rightarrow \mathbb{R}, |a|_n := |a_n|$  eine Nullfolge ist
- Eine Folge  $a : \mathbb{N} \rightarrow \mathbb{R}$  konvergiert gegen  $a_* \in \mathbb{R}$  genau dann, wenn  $(a - a_*) : \mathbb{N} \rightarrow \mathbb{R}, (a - a_*)_n := a_n - a_*$  eine Nullfolge ist
- Eine Menge der Form  $(-\varepsilon + x, x + \varepsilon), \varepsilon > 0$  heißt (offene) Umgebung von  $x$ . Konvergiert eine Folge  $a$  gegen  $a_*$ , dann liegen in jeder Umgebung von  $a_*$  alle bis auf endlich viele Folgenglieder.

**Satz 4.4**

Sei  $a : \mathbb{N} \rightarrow \mathbb{R}$  eine konvergente Folge. Dann ist der Grenzwert  $a_*$  eindeutig bestimmt.

**Satz 4.5**

Jede konvergente Folge ist beschränkt.

**Satz 4.6**

Seien  $a, b : \mathbb{N} \rightarrow \mathbb{R}$  konvergente Folgen  $\lim_{n \rightarrow \infty} a_n = a_*, \lim_{n \rightarrow \infty} b_n = b_*$ . Dann gilt:

1.  $\lim_{n \rightarrow \infty} (\alpha a_n + \beta b_n) = \alpha a_* + \beta b_*, \alpha, \beta \in \mathbb{R}$
2.  $\lim_{n \rightarrow \infty} (a_n \cdot b_n) = a_* \cdot b_*$
3.  $\lim_{n \rightarrow \infty} |a_n| = |a_*|$

**Satz 4.7: Sandwich-Theorem**

Seien  $a, b, c : \mathbb{N} \rightarrow \mathbb{R}$  Folgen und  $N_0 \in \mathbb{N}$  so dass

$$\lim_{n \rightarrow \infty} a_n = g = \lim_{n \rightarrow \infty} c_n \quad \text{und} \quad (4.3)$$

$$a_n \leq b_n \leq c_n \text{ für alle } n \in \mathbb{N} \quad (4.4)$$

Dann konvergiert auch  $b$  und es gilt  $\lim_{n \rightarrow \infty} b_n = g$

**Bemerkung** Wenn es ein  $N_0 \in \mathbb{N}$  gibt, so dass eine Aussage für für alle  $n \geq N_0$  gilt, dann sagt man, die Aussage gilt für fast alle  $n \in \mathbb{N}$ . (D. h. für alle  $n \in \mathbb{N}$  bis auf endlich viele)

**Korollar 4.8**

Ist  $a : \mathbb{N} \rightarrow \mathbb{R}$  beschränkt und  $b : \mathbb{N} \rightarrow \mathbb{R}$  eine Nullfolge, so gilt  $\lim_{n \rightarrow \infty} (a_n \cdot b_n) = 0$ .

**Lemma 4.9**

Seien  $a, b : \mathbb{N} \rightarrow \mathbb{R}$  konvergente Folgen mit  $a_n \leq b_n$  für fast alle  $n \in \mathbb{N}$ . Dann gilt

$$\lim_{n \rightarrow \infty} a_n \leq \lim_{n \rightarrow \infty} b_n \quad (4.5)$$

**Definition 4.10**

Sei  $f : \mathbb{N} \rightarrow \mathbb{N}$  eine wachsende Funktion:

$$f(1) < f(2) < f(3) < \dots < \quad (4.6)$$

Sei  $a : \mathbb{N} \rightarrow \mathbb{R}$  eine reelle Folge: Dann heißt

$$a_f : \mathbb{N} \rightarrow \mathbb{R}, a_f(n) = a_{f(n)} \quad (4.7)$$

*Teilfolge* von  $a$ .

**Beispiel**

$$f : \mathbb{N} \rightarrow \mathbb{N}, f(n) = 2n \quad (4.8)$$

$$a_f : a_2, a_4, a_6, \dots \quad (4.9)$$

**Bemerkung** Wenn  $a$  konvergiert, dann konvergieren auch alle Teilfolgen gegen den selben Grenzwert.

Eine Folge kann konvergente Teilfolgen haben, ohne selbst zu konvergieren.

(Bsp.:  $a : \mathbb{N} \rightarrow \mathbb{N}, a_n = (-1^n)$ )

## 4.2 Monotone Folgen

### Definition 4.11

Eine Folge  $a : \mathbb{N} \rightarrow \mathbb{R}$  heißt

- *monoton wachsend*, falls  $a_{n+1} \geq a_n$  für alle  $n \in \mathbb{N}$
- *monoton fallend*, falls  $a_{n+1} \leq a_n$  für alle  $n \in \mathbb{N}$
- *monoton*, wenn die monoton wachsend oder monoton fallend ist.

**Beispiel**  $a_n = \frac{1}{n}$  monoton fallend,  $b_n = n$  monoton wachsend

### Satz 4.12 Monotoniekriterien

Sei  $a : \mathbb{N} \rightarrow \mathbb{R}$  eine monotone und beschränkte Folge. Dann konvergiert  $a$ , d. h. es gibt  $a_* \in \mathbb{R}$  so dass  $\lim_{n \rightarrow \infty} a_n = a_*$

## 4.3 Uneigentliche Konvergenz

### Definition 4.13

Eine Folge  $a : \mathbb{N} \rightarrow \mathbb{R}$  heißt *(uneigentlich) konvergent gegen  $\infty$* , wenn gilt

- $a_n > 0$  für fast alle  $n \in \mathbb{N}$

- $\frac{1}{a_n} \rightarrow 0$

Schreibweise:

$$\lim_{n \rightarrow \infty} a_n = \infty \quad (4.10)$$

(uneigentlich) konvergent gegen  $-\infty$ , falls gilt

- $a_n < 0$  für fast alle  $n \in \mathbb{N}$
- $\frac{1}{a_n} \rightarrow 0$

Schreibweise:

$$\lim_{n \rightarrow \infty} a_n = -\infty \quad (4.11)$$

### Beispiel

- $a_n = n$ : uneigentlich konvergent gegen  $\infty$
- $b_n = -n$ : uneigentlich konvergent gegen  $-\infty$
- $c_n = (-1)^n \cdot n$ : nicht uneigentlich konvergent

### Satz 4.14

Sei  $a : \mathbb{N} \rightarrow \mathbb{R}$  monoton und nicht beschränkt. Dann ist  $a$  uneigentlich konvergent.

## 4.4 Landau-Symbole

### Definition 4.15

Sei  $r : \mathbb{N} \rightarrow \mathbb{R}$  Referenzfolge

$$\mathcal{O}(r) := \{a : \mathbb{N} \rightarrow \mathbb{R} : \exists c > 0 \text{ so dass } |a_n| \leq c \cdot |r_n| \text{ für fast alle } n \in \mathbb{N}\} \quad (4.12)$$

$$o(r) := \{a : \mathbb{N} \rightarrow \mathbb{R} : \text{Für jedes } c > 0 \text{ gilt } |a_n| \leq c \cdot |r_n| \text{ für fast alle } n \in \mathbb{N}\} \quad (4.13)$$

$$\Theta(r) := \{a : \mathbb{N} \rightarrow \mathbb{R} : a \in \mathcal{O}(r) \text{ und } r \in \mathcal{O}(a)\} \quad (4.14)$$

**Lemma 4.16**

$$a \in o(r) \implies a \in \mathcal{O}(r) \quad (4.15)$$

Es gilt:

$$\dots \subseteq \mathcal{O}\left(\frac{1}{n^2}\right) \subseteq \mathcal{O}\left(\frac{1}{n}\right) \subseteq \mathcal{O}(1) \subseteq \mathcal{O}(n) \subseteq \mathcal{O}(n^2) \subseteq \dots \quad (4.16)$$

**Satz 4.17**

Sei  $r : \mathbb{N} \rightarrow \mathbb{R} \setminus \{0\}$ . Dann gilt

a)

$$\mathcal{O}(r) = \left\{ a : \mathbb{N} \rightarrow \mathbb{R} : \underbrace{\left| \frac{a}{r} \right|}_{\text{Folge mit Gliedern } \frac{a_n}{r_n}} \text{ beschränkt} \right\} \quad (4.17)$$

b)

$$o(r) = \left\{ a : \mathbb{N} \rightarrow \mathbb{R} : \lim_{n \rightarrow \infty} \left| \frac{a_n}{r_n} \right| = 0 \right\} \quad (4.18)$$

**Satz 4.18 L'Hospital'sche Regel**

Folgen  $a : \mathbb{N} \rightarrow \mathbb{R}$  und  $r : \mathbb{N} \rightarrow \mathbb{R}$  seien gegeben durch differenzierbare Funktionen, d. h.  $a_n = \tilde{a}, r_n = \tilde{r}$  mit diff.baren Funktionen  $\tilde{a}, \tilde{r}$ .

Falls gilt

- $\lim_{n \rightarrow \infty} |r_n| = 0$
- $r'(n) \neq 0$  für fast alle  $n \in \mathbb{N}$



- $\lim_{n \rightarrow \infty} \frac{a'(n)}{r'(n)}$  existiert eigentlich oder uneigentlich

Dann gilt

$$\lim_{n \rightarrow \infty} \frac{a'(n)}{r'(n)} = \lim_{n \rightarrow \infty} \frac{a(n)}{r(n)} \quad (4.19)$$



# Kapitel 5

## Der Ring $\mathbb{Z}$

### 5.1 Gruppen

#### Definition 5.1

Sei  $M$  eine Menge. Eine *Verknüpfung*  $\circ$  auf  $M$  ist eine Abbildung

$$\circ : M \times M \rightarrow M \quad (5.1)$$

Die Verknüpfung heißt *assoziativ*, falls

$$(x \circ y) \circ z = x \circ (y \circ z) \text{ für alle } x, y, z \in M \quad (5.2)$$

Sie heißt *kommutativ*, falls

$$x \circ y = y \circ x \text{ für alle } x, y \in M \quad (5.3)$$

#### Definition 5.2

- a) Eine Menge  $H$  mit einer assoziativen Verknüpfung  $\circ$  heißt *Halbgruppe*  $(H, \circ)$ .
- b) Eine Halbgruppe  $(H, \circ)$  heißt *Monoid*, wenn es ein  $e \in H$  gibt mit

$$e \circ m = m \circ e = m \text{ für alle } m \in H \quad (5.4)$$

Dann heit  $e$  *neutrales Element* des Monoid.

- c) Ein Monoid  $(G, \circ)$  heit *Gruppe*, falls gilt: Zu jedem  $x \in G$  gibt es ein  $x' \in G$  so dass

$$x \circ x' = x' \circ x = e \quad (5.5)$$

Dann heit  $x'$  “zu  $x$  *inverses Element*”.

- d) Eine Gruppe mit kommutativer Verknpfung heit *kommutative* oder *abelsche Gruppe*.

### Beispiele

- “+” ist eine assoziative und kommutative Verknpfung auf  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ .
- $(\mathbb{N}, +)$  ist kein Monoid, da  $0 \notin \mathbb{N}$ .
- $(\mathbb{Z}, +)$  ist abelsche Gruppe, 0 ist neutrales Element.
- “.” ist assoziative Verknpfung auf  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ .
- $(\mathbb{Q}, \times)$  ist Monoid aber keine Gruppe, da 0 kein inverses Element hat.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$  ist abelsche Gruppe.

### Lemma 5.3

Ein Monoid hat genau ein neutrales Element.

**Beweis** Angenommen  $e$  und  $f$  sind neutrale Elemente.  $e = e \circ f = f$  □

### Lemma 5.4

Ist  $(G, \circ)$  eine Gruppe und  $x \in G$ . Dann gibt es genau ein inverses Element  $y \in G$  zu  $x$ .

**Beweis** Seien  $y, z \in G$  inverse Elemente zu  $x$ . Dann gilt  
 $y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z$  □

**Lemma 5.5**

Sei  $(G, \circ)$  eine Gruppe,  $x, y \in G$ . Seien  $x'$  das inverse Element zu  $x$ , und  $y'$  das inverse Element zu  $y$ . Dann ist  $(x \circ y)' := y' \circ x'$  das inverse Element zu  $x \circ y$ .

**Beweis**  $(x \circ y) \circ (y' \circ x') = (x \circ (y \circ y')) \circ x' = (x \circ e) \circ x' = x \circ x' = e \quad \square$

## 5.2 Ringe und Körper

**Definition 5.6**

Sei  $R$  eine Menge mit zwei Verknüpfungen

$\oplus$  *Addition*

$\otimes$  *Multiplikation*

so dass gilt

- 1)  $(R, \oplus)$  ist abelsche Gruppe mit neutralem Element  $0 \in R$
- 2)  $(R, \otimes)$  ist Halbgruppe:
- 3) *Distributivität:*

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z) \text{ und} \quad (5.6)$$

$$(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x) \text{ für alle } x, y, z \in R \quad (5.7)$$

Dann ist  $(R, \oplus, \otimes)$  ein *Ring*.

- $(R, \oplus, \otimes)$  heißt *Ring mit Eins*, falls  $(R, \otimes)$  ein Monoid ist, dessen neutrales Element  $1 \in R$  ungleich dem neutralen Element  $0$  der Addition ist.
- Der Ring  $(R, \oplus, \otimes)$  heißt *kommutativ*, falls  $\otimes$  kommutativ ist.
- Ein kommutativer Ring mit Eins  $(R, \oplus, \otimes)$  heißt *Körper*, wenn jedes Element  $x \neq 0$  ein multiplikatives Inverses hat.

**Beispiele**

- $(\mathbb{Z}, +, \cdot)$  kommutativer Ring mit Eins
- $(2\mathbb{Z}, +, \cdot)$  kommutativer Ring ohne Eins
- $(\mathbb{R}, +, \cdot)$  Körper
- $(\mathbb{Q}, +, \cdot)$  Körper

- Auf  $M = \{0, 1\}$  definiere
 

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

 Körper

**Lemma 5.7**

Sei  $(R, \oplus, \otimes)$  ein Ring, 0 das neutrale Element bzgl. der Addition. Dann gilt

$$0 \otimes x = x \otimes 0 = 0 \text{ für alle } x \in R \quad (5.8)$$

**5.3 Division mit Rest****Lemma 5.8**

Sei  $a \in \mathbb{Z}$  und  $m \in \mathbb{N}$ .

Dann gibt es eindeutig bestimmte Zahlen  $q \in \mathbb{Z}$  und  $r \in \{0, \dots, m-1\}$  so dass  $a = q \cdot m + r$ .

**Definition 5.9**

Mit den Bezeichnungen von Lemma 5.8 heißt  $r$  der *Rest von  $a$  bei Division mit  $m$* . Schreibweisen:

$$r = a \overset{a \% m}{\text{mod}} m \quad (5.9)$$

$$q = a \underset{a / m}{\text{div}} m = \left\lfloor \frac{a}{m} \right\rfloor \quad (5.10)$$

**Korollar 5.10**

Für  $a \in \mathbb{Z}$  und  $n, m \in \mathbb{N}$  gilt

$$(a \operatorname{div} n) \operatorname{div} m = a \operatorname{div}(n \cdot m) \quad (5.11)$$

**Definition 5.11**

Seien  $a, b \in \mathbb{Z}$ .

- 1)  $a$  *teilt*  $b$ , wenn es ein  $z \in \mathbb{Z}$  gibt mit  $b = a \cdot z$ . Schreibweise:  $a \mid b$   
 $b$  heißt *Vielfaches* von  $a$
- 2) Eine Zahl  $d$  heißt *größter gemeinsamer Teiler* (ggT) von  $a$  und  $b$ , falls gilt
  - $d \mid a$  und  $d \mid b$
  - falls  $z \in \mathbb{Z}$  so dass  $z \mid a$  und  $z \mid b$ , dann gilt  $z \mid d$ .

Schreibweise:

$$d = \operatorname{ggT}(a, b) \quad (5.12)$$

Wir definieren:

$$\operatorname{ggT}(0, 0) := 0 \quad (5.13)$$

- 3) Falls  $\operatorname{ggT}(a, b) = 1$ , dann heißen  $a$  und  $b$  *teilerfremd*.

**Beispiel**  $\operatorname{ggT}(27, 12) = 3; \operatorname{ggT}(5, 20) = 5$

## 5.4 Euklidischer Algorithmus

Ziel: Finde  $\operatorname{ggT}(a, b)$

Eingabe:  $a, b \in \mathbb{N}$  mit  $a \leq b$

Ausgabe:  $d \in \mathbb{N}$

- 1) Finde  $q \in \mathbb{N}$  und  $r \in \{0, \dots, a-1\}$  mit  $b = q \cdot a + r$
- 2) Falls  $r = 0$ , dann  $d := a$  und STOP
- 3) Falls  $r \neq 0$  rufe Algorithmus rekursiv auf mit  $b := a$  und  $a := r$

### Beispiel

$$a = 7, b = 143 \quad (5.14)$$

$$\rightarrow 143 = 20 \cdot 7 + 3 \quad (5.15)$$

$$\quad \quad \quad \underbrace{7 = 2 \cdot 3 + 1} \quad (5.16)$$

$$\quad \quad \quad \underbrace{3 = 3 \cdot 1 + 0} \quad (5.17)$$

$$\rightarrow d = 1 = \underbrace{\text{ggT}(7, 143)} \quad (5.18)$$

Es gibt  $x, y \in \mathbb{Z}$  so dass  $d = x \cdot a + y \cdot b$

### Satz 5.12

Seien  $a, b \in \mathbb{N}$  mit  $a \leq b$ .

Dann terminiert der Euklidische Algorithmus.

Für die Ausgabezahl  $d \in \mathbb{N}$  gilt:

$$\textcircled{1} \quad d = \text{ggT}(a, b)$$

$$\textcircled{2} \quad \text{Es gibt } x, y \in \mathbb{Z} \text{ mit } d = x \cdot a + y \cdot b$$

### Korollar 5.13 Lemma von Bezout

Sind  $a, b \in \mathbb{Z}$ , dann gibt es  $x, y \in \mathbb{Z}$  mit

$$\text{ggT}(a, b) = x \cdot a + y \cdot b \quad (5.19)$$

### Korollar 5.14

Zwei ganze Zahlen  $a, b \in \mathbb{Z}$  sind teilerfremd (d. h.  $\text{ggT}(a, b) = 1$ ) genau dann, wenn es ganze Zahlen gibt mit

$$1 = x \cdot a + y \cdot b \quad (5.20)$$



**Lemma 5.15**

Seien  $a, b \in \mathbb{Z}$  mit  $\text{ggT}(a, b) = 1$ . Dann gibt es  $m \in \mathbb{Z}$  so dass

$$a \mid (m \cdot b - 1) \quad (5.21)$$

## 5.5 Primfaktorzerlegung (PFZ)

**Lemma 5.16**

Seien  $a, b, c \in \mathbb{N}$ . Falls  $\text{ggT}(a, c) = 1$  und  $a \mid (b \cdot c)$ , dann  $a \mid b$ .

**Definition 5.17**

Eine natürliche Zahl  $n \geq 2$  heißt *Primzahl*, wenn sie “nur von 1 und sich selbst geteilt wird”. Präzise Def.:

$$\forall m \in \mathbb{N} : (m \mid n \implies m \in \{1, n\}) \quad (5.22)$$

**Satz 5.18 Hauptsatz der Arithmetik**

1) Jede natürliche Zahl  $n \geq 2$  lässt sich als Produkt von Primzahlen schreiben:

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_r; p_1, \dots, p_r \text{ Primzahlen} \quad (5.23)$$

2) Die PFZ von  $n$  ist eindeutig im folgenden Sinne

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_r; p_i \text{ prim} \quad (5.24)$$

$$n = q_1 \cdot q_2 \cdot q_3 \cdot \dots \cdot q_s; q_j \text{ prim} \quad (5.25)$$

Falls

$$p_1 \leq p_2 \leq p_3 \leq \dots \leq p_r \text{ und} \quad (5.26)$$

$$q_1 \leq q_2 \leq q_3 \leq \dots \leq q_s \quad (5.27)$$

dann

$$r = s \text{ und} \quad (5.28)$$

$$p_i = q_j \quad (5.29)$$

**Satz 5.18a**

Es gibt unendlich viele Primzahlen.

**Beweis** durch Widerspruch

Angenommen, es gibt nur endlich viele Primzahlen  $p_1, p_2, \dots, p_r; r \in \mathbb{N}$ . Betrachte

$$n := p_1 \cdot p_2 \cdot \dots \cdot p_r + 1 \quad (5.30)$$

Nach Satz 5.18 (S. 41) hat  $n$  eine PFZ. Aber keine der Primzahlen  $p_1, \dots, p_r$  teilt  $n$ .  $\nexists \square$

**Bemerkung** Aus der PFZ einer natürlichen Zahl  $n$  kann man alle natürlichen Teiler ( $\neq 1$ ) von  $n$  durch Produkte der Primfaktoren erhalten.

**Beispiel**

$$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3 \quad (5.31)$$

Natürliche Teiler von 24: 1, 2, 3, 4, 6, 8, 12, 24

**Definition 5.19**

Falls  $a, b \in \mathbb{Z} \setminus \{0\}$ , dann ist das *kleinste gemeinsame Vielfache* (kgV) von  $a$  und  $b$ , die kleinste natürliche Zahl, die sowohl Vielfaches von  $a$ , als auch  $b$  ist. Wir schreiben:

$$\text{kgV}(a, b) := \min\{n \in \mathbb{N} : a \mid n \text{ und } b \mid n\} \quad (5.32)$$

Falls  $a = 0$  oder  $b = 0$ ,

$$\text{kgV}(a, b) := 0 \quad (5.33)$$

**Beispiel**  $a = 125, b = 265$ ; PFZ:  $a = 5 \cdot 5 \cdot 5 = 5^3, b = 5 \cdot 3$   
 $\text{ggT}(125, 265) = 5$ ;  $\text{kgV}(125, 265) = 5^3 \cdot 53 = 6625 = \frac{125 \cdot 265}{\text{ggT}(125, 265)}$

**Lemma 5.20**

Seien  $a, b \in \mathbb{N}$  mit  $a, b \geq 2$

Die erweiterten PFZ seien

$$\left. \begin{aligned} a &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r} \\ b &= p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_r^{\beta_r} \end{aligned} \right\} \begin{array}{l} \text{mit } p_1, \dots, p_r \text{ prim und} \\ \alpha_i, \beta_i \in \mathbb{N}_0 \text{ f\"ur } i = 1, \dots, r \end{array} \quad (5.34)$$

Dann gilt

$$\textcircled{1} \quad \text{ggT}(a, b) = \prod_{i=1}^r p_i^{\min\{\alpha_i, \beta_i\}} \quad (5.35)$$

$$\textcircled{2} \quad \text{kgV}(a, b) = \prod_{i=1}^r p_i^{\max\{\alpha_i, \beta_i\}} \quad (5.36)$$

$$\textcircled{3} \quad a \cdot b = \text{ggT}(a, b) \cdot \text{kgV}(a, b) \quad (5.37)$$

**Bemerkung** ggT und kgV kann man auch für mehr als zwei Zahlen definieren, aber

$$\text{ggT}(a, b, c) \cdot \text{kgV}(a, b, c) \neq a \cdot b \cdot c \text{ für manche } a, b, c \in \mathbb{N} \quad (5.38)$$

## 5.6 Rechnen modulo $n$

### 5.6.1 Addition & Multiplikation modulo $n$

**Definition 5.21**

Für  $n \in \mathbb{N}$  und  $x, y \in \mathbb{Z}$  schreiben wir

$$x \equiv y \pmod{n} \quad (5.39)$$

falls gilt

$$n \mid (x - y) \quad (5.40)$$

Wir sagen dann, dass  $x$  und  $y$  *kongruent modulo  $n$*  sind.

**Vorsicht** Nicht verwechseln mit  $x = y \bmod n \in \{0, \dots, n-1\}$

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

$$x \sim y :\Leftrightarrow x \equiv y \pmod{n} \quad (5.41)$$

definiert eine Äquivalenzrelation auf  $\mathbb{Z}$ .

**Beispiele:**  $6 \equiv 12 \pmod{6}$ ,  $6 \equiv 0 \pmod{6}$ ,  $15 \equiv 21 \pmod{6}$

Wir betrachten die Äquivalenzklassen

$$[x] = \{y \in \mathbb{Z} : y \equiv x \pmod{n}\} \quad (5.42)$$

$$= \{y \in \mathbb{Z} : n \mid (y - x)\} \quad (5.43)$$

$$\mathbb{Z}/\sim = \{[0], [1], \dots, [n-1]\} \quad (5.44)$$

ist eine Partition von  $\mathbb{Z}$  (Satz 2.14, S. 18). Schreibweise:  $\mathbb{Z}/\sim =: \mathbb{Z}_n$

### Definition 5.22

Für  $[x], [y] \in \mathbb{Z}_n$  definieren wir

$$[x] + [y] := [x + y] \quad (5.45)$$

$$[x] \cdot [y] := [x \cdot y] \quad (5.46)$$

### Satz 5.23

1. Die Verknüpfungen  $+$  und  $\cdot$  in  $\mathbb{Z}_n$  sind wohldefiniert, d. h. unabhängig vom Repräsentanten.
2.  $(\mathbb{Z}_n, +, \cdot)$  ist ein kommutativer Ring.

**Beispiele**  $n = 2, \mathbb{Z}_2 = \{ \underbrace{[0]}_{\text{gerade Zahlen}}, \underbrace{[1]}_{\text{ungerade Zahlen}} \}$

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

·	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

$n = 3, \mathbb{Z}_3 = \{[0], [1], [2]\}$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$n = 4, \mathbb{Z}_4 = \{[0], [1], [2], [3]\}$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Beobachtung bei Multiplikation: In den Zeilen der Klassen, die teilerfremd zu  $n$  sind, kommen alle Äquivalenzklassen vor (z. B. die Zeilen  $[1]$  und  $[3]$  bei  $n = 4$ ).

5.6.2 Einheiten und Inverse

Definition 5.24

Sei  $(R, +, \cdot)$  ein Ring mit Eins. Ein Element heißt *Einheit* oder *invertierbar*, falls es  $y \in R$  gibt, mit

$$x \cdot y = y \cdot x = \underbrace{1}_{\text{Eins-Element}} \tag{5.47}$$

Schreibweise:

$$R^* := \{x \in R : x \text{ ist Einheit}\} \tag{5.48}$$

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

In einem Körper  $(K, +, \cdot)$  gilt

$$K^* = K \setminus \{0\} \quad (5.49)$$

**Lemma 5.25**

Sei  $(R, +, \cdot)$  Ring mit Eins. Dann ist  $(R^*, \cdot)$  eine Gruppe. D. h.

- $R^* \times R^* \rightarrow R^* \Leftrightarrow R^* \cdot R^* \in R^*$
- Assoziativität
- Eins-Element (neutrales Element bzgl.  $\cdot$ )
- inverses Element

**Beispiel**

- $\mathbb{Z}_2^* = \{[1]\}$ , denn  $[1] \cdot [1] = [1 \cdot 1] = [1]$
- $\mathbb{Z}_3^* = \{[1], [2]\}$ , denn  $[2] \cdot [2] = [4] = [1]$
- $\mathbb{Z}_4^* = \{[1], [3]\}$ , denn  $[3] \cdot [3] = [9] = [1]$

**Satz 5.26**

Sei  $n \in \mathbb{N}$ . Dann gilt  $\mathbb{Z}_n^* = \{[a] : \text{ggT}(a, n) = 1\}$

**Beispiel**

- $\mathbb{Z}_7^* = \{[1], [2], [3], [4], [5], [6]\}$
- $\mathbb{Z}_{16}^* = \{[1], [3], [5], [7], [9], [11], [13], [15]\}$

**Bemerkung** Für  $p$  prim ist in  $\mathbb{Z}_p$  jedes Element außer  $[0]$  eine Einheit.

**Satz 5.27**

Für jede Primzahl  $p$  ist  $(\mathbb{Z}_p, +, \cdot)$  ein Körper.

**Lemma 5.28**

Sei  $(G, \cdot)$  eine Gruppe. Seien  $a, b \in G$ . Dann hat die Gleichung  $a \cdot x = b$  genau eine Lösung  $x \in G$ .

**Beispiel** Betrachte  $\mathbb{Z}_5, a = [2], b = [3]$ . Suche Lösungen von  $[2] \cdot \underbrace{x}_{\in \mathbb{Z}_5} = [3]$ . Durch Ausprobieren ergibt sich,  $x = [4]$  ist eindeutige Lösung.

**Korollar 5.29**

Sei  $n \geq 2, n \in \mathbb{N}$ . Dann gilt für  $[a] \in \mathbb{Z}_n^*$

$$\mathbb{Z}_n^* + \{[a] \cdot [x] : [x] \in \mathbb{Z}_n^*\} \quad (5.50)$$

**Satz 5.30 Kleiner Satz von Fermat**

Sei  $p$  Primzahl. Sei  $a \in \mathbb{Z}$  mit  $\text{ggT}(a, p) = 1$ . Dann gilt

$$a^{p-1} \equiv 1 \pmod{p} \quad (5.51)$$

**Beispiel**  $p = 5$

$$2^{p-1} = 2^4 = 16 \equiv 1 \pmod{5} \quad (5.52)$$

$$3^{p-1} = 3^4 = 81 \equiv 1 \pmod{5} \quad (5.53)$$

$$4^{p-1} = 4^4 = 256 \equiv 1 \pmod{5} \quad (5.54)$$

**Definition 5.31**

Die Funktion

$$\varphi : \mathbb{N} \rightarrow \mathbb{N} \quad (5.55)$$

$$\varphi(n) := |\{k \in \{1, \dots, n\} : \text{ggT}(k, n) = 1\}| \quad (5.56)$$

heißt *Eulersche  $\varphi$ -Funktion*.

**Bemerkung**  $\varphi(n)$  gibt die Anzahl der Einheiten in  $\mathbb{Z}_n$  an.  
Für  $p$  Primzahl:  $\varphi(p) = p - 1$

**Beispiel**  $\varphi(1) = 1$     $\varphi(3) = 2$     $\varphi(5) = 4$     $\varphi(7) = 6$   
 $\varphi(2) = 1$     $\varphi(4) = 2$     $\varphi(6) = 2$     $\varphi(8) = 4$

### Lemma 5.32

Sei  $p \geq 2$  Primzahl,  $k \in \mathbb{N}$ . Dann gilt

$$\varphi(p^k) = p^{k-1} \cdot (p - 1) \quad (5.57)$$

**Beispiele**  $\varphi(2^3) = 2^2 \cdot (2 - 1) = 4 \cdot 1 = 4$   
 $\varphi(9) = \varphi(3^2) = 3^1 \cdot (3 - 1) = 3 \cdot 2 = 6$

### Lemma 5.33

Seien  $a, b \in \mathbb{N}$  mit  $\text{ggT}(a, b) = 1$ . Dann gilt

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \quad (5.58)$$

### Satz 5.34 Satz von Euler-Fermat

Seien  $n \in \mathbb{N}$  und  $a \in \mathbb{Z}$  mit  $\text{ggT}(a, n) = 1$ . Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad (5.59)$$

### Korollar 5.35

Seien  $p, q$  prim,  $p \neq q$ ,  $n = p \cdot q$ . Dann gilt für alle  $a < n$  und  $k \in \mathbb{N}$

$$a^{k \cdot \varphi(n) + 1} \equiv a \pmod{n} \quad (5.60)$$



## RSA-Verschlüsselung

Es gibt:

$n \in \mathbb{N}$	öffentliche Zahl (groß!)
$e \in \mathbb{N}$	öffentlicher Schlüssel
$d \in \mathbb{Z}$	privater Schlüssel
$m < n$	Nachricht in Klartext
$c \in \mathbb{N}$	verschlüsselte Nachricht

**Ablauf:**

### Empfänger B

1. B wählt große Primzahlen  $p \neq q$  und setzt  $n := p \cdot q$
2. B wählt  $e$  mit  $\text{ggT}(e, \varphi(n)) = 1$
3. B berechnet  $d$  so dass  $d \cdot e \equiv 1 \pmod{\varphi(n)}$
4. B veröffentlicht  $n$  und  $e$

### Sender A

5. A verschlüsselt Nachricht  $m < n - 1$  durch  $c := m^e \bmod n$

### Empfänger B

6. B entschlüsselt  $m = c^d \bmod n$



# Kapitel 6

## Gruppentheorie

### 6.1 Untergruppen

#### Definition 6.1

Sei  $(G, \otimes)$  eine Gruppe<sup>1</sup> mit neutralem Element  $e$ , und  $H \subseteq G$ . Dann heißt  $(H, \otimes)$  *Untergruppe* von  $G$ , falls gilt:

- $e \in H$
- $x, y \in H \rightarrow x \otimes y \in H$
- $x \in H \implies x^{-1} \in H$

---

<sup>1</sup>  $(G, \otimes)$  heißt Gruppe, wenn:

- $G$  Menge
- $\otimes : G \times G \rightarrow G$  assoziative Verknüpfung
- Es gibt  $e \in G : e \otimes g = g \otimes e = g$  für alle  $g \in G$
- Zu jedem  $g \in G$  gibt es  $g^{-1} \in G : g \otimes g^{-1} = g^{-1} \otimes g = e$

**Lemma 6.2**

Eine Untergruppe ist selbst eine Gruppe.

**Beispiele**

- $(\mathbb{Z}, +)$  ist Untergruppe von  $(\mathbb{R}, +)$
- $(2\mathbb{Z}, +)$  ist Untergruppe von  $(\mathbb{Z}, +)$
- $(\mathbb{Q} \setminus \{0\}, \cdot)$  und  $(\{-1, 1\}, \cdot)$  sind Untergruppen von  $(\mathbb{R} \setminus \{0\}, \cdot)$

**Notation** Sei  $(G, \otimes)$  eine Gruppe mit neutralem Element  $e$ . Seien  $x \in G, n \in \mathbb{N}_0$ .

$$\text{Dann } x^n := \begin{cases} e & \text{für } n = 0 \\ x \otimes x^{n-1} = x^{n-1} \otimes x & \text{für } n \in \mathbb{N} \end{cases} \quad (6.1)$$

$$x^{-n} := (\underbrace{x^{-1}}_{\text{inv. Elem. zu } x})^n \quad (6.2)$$

**Bemerkung** Für  $q, r \in \mathbb{Z}$  gilt

$$x^{q+r} = x^q \otimes x^r = x^r \otimes x^q \quad (6.3)$$

**Definition 6.3**

Sei  $(G, \otimes)$  eine Gruppe,  $H \subseteq G$ . Dann heißt die kleinste Untergruppe  $(\tilde{H}, \otimes)$  von  $G$ , so dass  $H \subseteq \tilde{H}$ , die *von  $H$  erzeugte Untergruppe*.

**Beispiele**

- Betrachte Gruppe  $(\mathbb{Z}, +)$  und  $H = \{3\}$ . Dann ist die von  $H$  erzeugte Untergruppe  $(3\mathbb{Z}, +)$ .
- Betrachte  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $H = \{2\}$ . Dann ist die von  $H$  erzeugte Untergruppe  $(2^{\mathbb{Z}}, \cdot)$
- $(\mathbb{Z}_5, +)$ ,  $H_1 = \{[1]\}$ , von  $H_1$  erzeugte Untergruppe  $(\mathbb{Z}_5, +)$   
 $H_2 = \{[2]\}$  von  $H_2$  erzeugte Untergruppe  $(\mathbb{Z}_5, +)$

**Lemma 6.4**

Sei  $(G, \otimes)$  Gruppe und  $g \in G$ . Dann ist  $\langle g \rangle := \{g^z : z \in \mathbb{Z}\}$  die von  $\{g\}$  erzeugte Halbgruppe.

**Lemma 6.5**

Sei  $(G, \otimes)$  eine endliche Gruppe, d. h.  $|G| < \infty$ , mit neutralem Element  $e$ . Sei  $g \in G$ . Setze  $k := |\langle g \rangle| \in \mathbb{N}$ . Dann gilt

$$g^k = e \text{ und} \quad (6.4)$$

$$\langle g \rangle = \{g^0, g^1, g^2, \dots, g^{k-1}\} \quad (6.5)$$

**Beispiel**  $(\mathbb{Z}_5, +), [2] \in \mathbb{Z}_5$ . Dann

$$\langle [2] \rangle \stackrel{\text{Lemma 6.4, S. 53}}{=} \{[2]^n : n \in \mathbb{Z}\} \quad (6.6)$$

$$\begin{array}{lll} \text{Es gilt} & \begin{array}{l} [2]^0 = [0] \\ [2]^1 = [2] \\ [2]^2 = [2 + 2] = [4] \end{array} & \begin{array}{l} [2]^3 = [2 + 2 + 2] = [6] = [1] \\ [2]^4 = [8] = [3] \end{array} \end{array} \implies \langle [2] \rangle = \mathbb{Z}_5$$

Also  $k := |\langle [2] \rangle| = 5$ ,

$$[2]^5 = [2 + 2 + 2 + 2 + 2] = [10] = [0] = e,$$

$$\langle [2] \rangle = \mathbb{Z}_5 = \{[2]^0, [2]^1, [2]^2, [2]^3, [2]^4\}$$

## 6.2 Gruppenordnungen & Satz von Lagrange

**Definition 6.6**

Sei  $(G, \otimes)$  eine Gruppe.

a) Die *Ordnung* von  $G$  ist

- unendlich, falls  $G$  unendlich viele Elemente enthält.
- die Kardinalität von  $G$ , falls  $G$  endlich viele Elemente enthält.

- b) Die *Ordnung eines Elements*  $g \in G$  ist die Ordnung der von  $\{g\}$  erzeugten Untergruppe  $\langle g \rangle$ .

Schreibweise:

$$\text{ord}(g) := |\langle g \rangle| \quad (6.7)$$

**Beispiel** Betrachte<sup>2</sup>  $(\mathbb{Z}_5^*, \cdot)$ . Es gilt  $\mathbb{Z}_5^* = \{[1], [2], [3], [4]\}$ . Ordnung der Elemente:  
 $\langle [1] \rangle = \{[1]\} \implies \text{ord}([1]) = 1$   
 $\langle [2] \rangle = \{[2], [1], [4], [3]\} \implies \text{ord}([2]) = 4$   
 $\langle [3] \rangle = \{[1], [3], [4], [2]\} \implies \text{ord}([3]) = 4$   
 $\langle [4] \rangle = \{[1], [4]\} \implies \text{ord}([4]) = 2$

### Satz 6.7 Satz von Lagrange

Sei  $(G, \otimes)$  eine endliche Gruppe. Ist  $(H, \otimes)$ ,  $H \subseteq G$  eine Untergruppe von  $G$ , so teilt die Ordnung von  $H$  die Ordnung von  $G$ .

### Definition 6.8

Sei  $(G, \otimes)$  eine abelsche Gruppe,  $(H, \otimes)$  Untergruppe. Dann heißt

$$[G : H] := \frac{|G|}{|H|} \quad (6.8)$$

der *Index* von  $H$  in  $G$ .

### Korollar 6.9

Sei  $(G, \otimes)$  eine endliche Gruppe mit neutralem Element  $e$ , und sei  $g \in G$ . Dann ist die Ordnung von  $g$  ein Teiler der Gruppenordnung  $|G|$  und es gilt

$$g^{|G|} = e \quad (6.9)$$

---

<sup>2</sup> $R^* := \{x \in R : x \text{ ist Einheit}\}$  (Def. 5.24, S. 45)  
 $x \in R$  heißt Einheit oder invertierbar, falls  $\exists y \in R : x \otimes y = 1$  ( $1 := \text{Eins-Element}$ )

## 6.3 Zyklische Gruppen

### Definition 6.10

Eine Gruppe  $(G, \otimes)$  heißt *zyklisch*, wenn es ein  $g \in G$  gibt, so dass  $G = \langle g \rangle$ .

### Beispiele

- $(\mathbb{Z}, +)$  ist zyklisch mit Erzeuger 1
- $(\{-1, +1\}, \cdot)$  ist zyklisch mit Erzeuger  $-1$
- $(\mathbb{Z}_{37}, +)$  ist zyklisch mit Erzeuger  $[1]$

### Lemma 6.11 Konsequenzen aus Lemma 6.5 (S. 53)

Sei  $(G, \otimes)$  eine Gruppe mit neutralem Element  $e$ , und sei  $g \in G$  von endlicher Ordnung. Dann

a) Für  $x, y \in \mathbb{Z}$  gilt:

$$g^x = g^y \iff \text{ord}(g) \mid (x - y) \quad (6.10)$$

b)

$$\text{ord}(g) = \min \{n \in \mathbb{N} : g^n = e\} \quad (6.11)$$

c) Für  $z \in \mathbb{Z}$  gilt:

$$g^z = e \iff \text{ord}(g) \mid z \quad (6.12)$$

d) Für  $k \in \mathbb{N}$  gilt:

$$\text{ord}(g^k) = \frac{\text{ord}(g)}{\text{ggT}(k, \text{ord}(g))} \quad (6.13)$$

**Korollar 6.12**

Sei  $(G, \otimes)$  zyklische Gruppe von Ordnung  $n$ ,  $G = \langle g \rangle$

$$G = \langle g^k \rangle \iff \text{ggT}(k, \underbrace{\text{ord}(g)}_n) = 1 \quad (6.14)$$

Insbesondere gibt es  $\varphi(n)$  Erzeuger.



# Kapitel 7

## Lineare Algebra

### 7.1 Vektorräume

#### Definition 7.1

Sei  $(K, +, \cdot)$  ein Körper<sup>1</sup>.

Ein  $K$ -Vektorraum ist ein Tripel  $(V, \oplus, \otimes)$ , wobei  $V$  eine Menge ist,

$$\oplus : V \times V \rightarrow V, (v, w) \mapsto v \oplus w \quad (7.1)$$

$$\otimes : K \times V \rightarrow V, (s, v) \mapsto s \otimes v \quad (7.2)$$

$$\text{für } v, w \in V, s \in K \quad (7.3)$$

so dass gilt

1.  $(V, \oplus)$  ist kommutative Gruppe. Schreibweise:  
Neutrales Element ist  $\mathbf{0} \in V$  (“Nullvektor”)  
Inverses Element zu  $v \in V$  ist  $-v \in V$

---

<sup>1</sup>Körper  $(K, +, \cdot)$ , d. h.

- kommutativer Ring mit Eins, bei dem jedes Element  $x \neq o$  ein multiplikatives Inverses hat.
- Nullelement  $0 \in K$  als neutrales Element bzgl.  $+$
- Einselement  $1 \in K$  als neutrales Element bzgl.  $\cdot$

2.

$$\underbrace{1}_{\text{Eins-Element in } K} \otimes v = v \text{ für alle } v \in V \quad (7.4)$$

3.

$$(s \cdot t) \otimes v = s \otimes (t \otimes v) \text{ für alle } s, t \in K, v \in V \quad (7.5)$$

4.

$$(s + t) \otimes v = (s \otimes v) \oplus (t \otimes v) \text{ für alle } s, t \in K, v \in V \quad (7.6)$$

5.

$$s \otimes (v \oplus w) = (s \otimes v) \oplus (s \otimes w) \text{ für alle } s \in K, v, w \in V \quad (7.7)$$

Elemente in  $V$  heißen *Vektoren*.

### Beispiele

a) Für  $n \in \mathbb{N}$  ist  $K^n$  ein Vektorraum (VR) mit

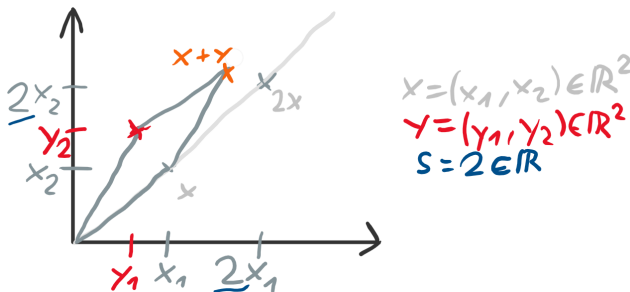
$$(x_1, \dots, x_n) \oplus (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n) \quad (7.8)$$

$$s \otimes (x_1, \dots, x_n) = (s \cdot x_1, \dots, s \cdot x_n) \quad (7.9)$$

$$\text{für } x_1, \dots, x_n, y_1, \dots, y_n \in K, s \in K \quad (7.10)$$

Spezialfälle,  $(K, +, \cdot)$  ist  $K$ -VR

- $K = \mathbb{R}, V = \mathbb{R}^2$



b)  $(\mathbb{C}, +, \cdot)$  ist  $\mathbb{C}$ -VR,  $\mathbb{R}$ -VR,  $\mathbb{Q}$ -VR.

c) Sei  $M \neq \emptyset$  eine Menge,  $(K, +, \cdot)$  ein Körper. Sei  $V := \{f : M \rightarrow K\}$ . Betrachte

$$(f \oplus g)(x) := f(x) + g(x) \quad (7.11)$$

$$(s \otimes f)(x) := s \cdot (f(x)) \quad (7.12)$$

$$\text{für } f, g \in V, x \in M, s \in K \quad (7.13)$$

Dann ist  $(V, \oplus, \otimes)$  ein  $K$ -VR.

### Lemma 7.2 Rechenregeln

Sei  $(K, +, \cdot)$  ein Körper,  $(V, \oplus, \otimes)$  ein  $K$ -Vektorraum (VR). Dann gilt

a)

$$0 \cdot v = \mathbf{0} \text{ für alle } v \in V \quad (7.14)$$

b)

$$s \cdot \mathbf{0} = \mathbf{0} \text{ für alle } s \in K \quad (7.15)$$

c) Für alle  $s \in K$  und  $v \in V$  gilt

$$s \otimes v = \mathbf{0} \iff s = \mathbf{0} \wedge v = \mathbf{0} \quad (7.16)$$

d) Für alle  $s \in K$  und  $v \in V$  gilt

$$\left( \underbrace{-s}_{\substack{\text{inv. Elem.} \\ \text{zu } s \text{ in } K \\ \text{(bzgl. } +)}} \right) \otimes v = \underbrace{-(s \otimes v)}_{\substack{\text{inv. Elem.} \\ \text{bzgl. } \oplus \text{ zu} \\ (s \otimes v)}} \quad (7.17)$$

## 7.2 Unterräume

### Definition 7.3

Sei  $(K, +, \cdot)$  Körper,  $(V, \oplus, \otimes)$  ein  $K$ -VR. Dann heißt  $U \subseteq V$  *Unter(vektor)raum* oder *Teilraum* von  $V$ , falls gilt

1.  $U \neq \emptyset$
2.  $v, w \in U \implies v \oplus w \in U$
3.  $s \in K, v \in U \implies s \otimes v \in U$

**Bemerkung** Ist  $U \subseteq V$  ein Untervektorraum (UVR) dann ist  $(U, \oplus, \otimes)$  ein  $K$ -VR.

### Beispiele

- a)  $V, \{\mathbf{0}\}$  sind UVR.
- b) Sei  $v \in V \setminus \{\mathbf{0}\}$ . Dann ist  $\{v\}$  kein UVR, denn  $0 \otimes v = \mathbf{0} \notin \{v\}$ .
- c) Für  $v \in V$  ist

$$\langle v \rangle := \{s \otimes v : s \in K\} \quad (7.18)$$

ein UVR.

## 7.3 Erzeugendensysteme

### Definition 7.4

- a) Sei  $(V, \oplus, \otimes)$  ein  $K$ -VR,  $v_1, \dots, v_n \in V$ . Dann heißt  $V \in V$  *Linearkombination* von  $v_1, \dots, v_n$ , falls es  $s_1, \dots, s_n$  gibt mit

$$v = (s_1 \otimes v_1) \oplus (s_2 \otimes v_2) \oplus \dots \oplus (s_n \otimes v_n) \quad (7.19)$$

b) Ist  $M \subseteq V$  mit  $M \neq \emptyset$ , so definieren wir das *Erzeugnis* von  $M$  als

$$\langle M \rangle := \{v \in V : v \text{ ist Linearkombination von endlich vielen Vektoren von } M\} \quad (7.20)$$

$$=: \text{span}(M) \quad (7.21)$$

Wir definieren:

$$\langle \emptyset \rangle := \{\mathbf{0}\} \quad (7.22)$$

**Bemerkung** Der  $K$ -VR  $(K, +, \cdot)$  hat nur die Untervektorräume  $K$  und  $\underbrace{\{0\}}_{=0}$ .

### Lemma 7.5

Sei  $(V, \oplus, \otimes)$  ein  $K$ -VR,  $M \subseteq V$  beliebige Teilmenge. Dann ist  $\langle M \rangle$  ein UVR von  $V$ .

## 7.4 Lineare Unabhängigkeit

### Definition 7.6

Sei  $(V, \oplus, \otimes)$  ein  $K$ -VR.

a) Vektoren  $v_1, \dots, v_n$  heißen *linear unabhängig*, falls folgendes gilt:

$$(s_1 \otimes v_1) \oplus \dots \oplus (s_n \otimes v_n) = \mathbf{0} \text{ mit } s_1, \dots, s_n \in K \implies s_1 = \dots = s_n = 0 \quad (7.23)$$

Andernfalls heißen  $v_1, \dots, v_n$  *linear abhängig*.

b) Eine Teilmenge  $M \subseteq V$ ,  $M \neq \emptyset$  heißt *linear unabhängig*, falls je endlich viele paarweise verschiedene Vektoren aus  $M$  linear unabhängig sind. Wir definieren  $\emptyset$  als linear unabhängig. Ist  $M \subseteq V$  nicht linear unabhängig, so heißt  $M$  *linear abhängig*.

**Bemerkung**

- Jede Menge, die eine linear abhängige Teilmenge enthält ist linear abhängig.
- Jede Teilmenge einer linear unabhängigen Menge ist linear unabhängig.

**Satz 7.7**

Sei  $(V, \oplus, \otimes)$  ein  $K$ -VR,  $M \subseteq V$ ,  $M \neq \emptyset$ ,  $M \neq \{0\}$ . Folgende Aussagen sind äquivalent:

1.  $M$  ist linear abhängig.
2. Jeder Vektor  $w \in \langle M \rangle$  kann **eindeutig** geschrieben werden als Linearkombination von Vektoren aus  $M$ , bis auf die Reihenfolge der Summanden, d. h.

$$\text{für } v_1, \dots, v_n \in M, s_1, \dots, s_n, t_1, \dots, t_n \in K \quad (7.24)$$

$$\text{mit } w = (s_1 \otimes v_1) \oplus \dots \oplus (s_n \otimes v_n) = (t_1 \otimes v_1) \oplus \dots \oplus (t_n \otimes v_n) \quad (7.25)$$

$$\text{gilt } s_1 = t_1, \dots, s_n = t_n \quad (7.26)$$

3. Für alle  $v \in M$  gilt

$$v \notin \langle M \setminus \{v\} \rangle \quad (7.27)$$

4. Für alle  $v \in M$  gilt

$$\langle M \setminus \{v\} \rangle \neq \langle M \rangle \quad (7.28)$$

## 7.5 Basis und Dimension

**Definition 7.8**

Sei  $V, \oplus, \otimes$   $K$ -VR,  $M \subseteq V$ .

- a)  $M$  heißt *Erzeugendensystem* von  $V$ , falls

$$\langle M \rangle = V \quad (7.29)$$

- b)  $M$  heißt *Basis* von  $V$ , falls  $V$  ein linear unabhängiges Erzeugendensystem ist.

- c)  $V$  heißt *endlich erzeugt*, falls  $V$  ein endliches Erzeugendensystem besitzt.

**Beispiel**  $\mathbb{R}^3$  als  $\mathbb{R}$ -VR.

$\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$  ist Erzeugendensystem von  $\mathbb{R}^3$ , denn für beliebiges  $(x, y, z) \in \mathbb{R}^3$  gilt

$$(x, y, z) = (x \otimes (1, 0, 0)) \oplus (y \otimes (0, 1, 0)) \oplus (z \otimes (0, 0, 1)) \quad (7.30)$$

sogar Basis, da linear unabhängig. Insbesondere ist  $\mathbb{R}^3$  endlich erzeugt.

**Bemerkung** Jeder VR  $(K, \oplus, \otimes)$  hat ein Erzeugendensystem, z. B.  $V$  selbst.

**Frage** Hat jeder endlich erzeugte VR ein Basis?

**Beispiel**  $\mathbb{R}^3$  als  $\mathbb{R}$ -VR.

$$\varepsilon = \{(1, 0, 0), (0, 0, 0), (0, 1, 0), (3, 4, 0), (0, 0, 1)\} \text{ ist Erzeugendensystem von } \mathbb{R}^3 \quad (7.31)$$

Bastele Basis  $B \subseteq \varepsilon$  von  $\mathbb{R}^3$ : Gehe Vektoren der Reihe nach durch:

$$\begin{aligned} (1, 0, 0) &\in B, \text{ denn } (1, 0, 0) \notin \langle \emptyset \rangle = \{\mathbf{0}\} = \{(0, 0, 0)\} \\ (0, 0, 0) &\notin B, \text{ denn } (0, 0, 0) \in \langle \{(1, 0, 0)\} \rangle \\ (0, 1, 0) &\in B, \text{ denn } (0, 1, 0) \notin \langle \{(1, 0, 0)\} \rangle \\ (3, 4, 0) &\notin B, \text{ denn } (3, 4, 0) \in \langle \{(1, 0, 0), (0, 1, 0)\} \rangle \\ (0, 0, 1) &\in B, \text{ denn } (0, 0, 1) \notin \langle \{(1, 0, 0), (0, 1, 0)\} \rangle \\ &\rightarrow B = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\} \end{aligned}$$

Es gilt  $B \subseteq \varepsilon$  und  $B$  Basis von  $\mathbb{R}^3$ . Andere Basis  $B' = \{(3, 4, 0), (1, 0, 0), (0, 0, 1)\}$ .

### Satz 7.9

Jeder endlich erzeugte VR besitzt eine Basis.

### Beweis

$$\varepsilon = \{v_1, \dots, v_n\} \subseteq V \text{ Erzeugendensystem für } V \quad (7.32)$$

Bastele  $B$  wie folgt:

1. Falls  $v_1 \notin \langle \emptyset \rangle = \{\mathbf{0}\}$ , dann  $v_1 \in B$ .  
 Falls  $v_1 \in \langle \emptyset \rangle = \{\mathbf{0}\}$ , dann  $v_1 \notin B$ .
2. Für  $i = 2, \dots, n$ :  
 Falls  $v_i \in \langle \{v_1, \dots, v_{i-1}\} \cap B \rangle$ , dann  $v_i \notin B$ , andernfalls  $v_i \in B$ .

### Satz 7.10

Sei  $(V, \oplus, \otimes)$  ein endlich erzeugter VR. Dann haben je zwei Basen die gleiche Anzahl an Elementen.

**Beweis** siehe A.1, Seite 75

### Definition 7.11

Sei  $(V, \oplus, \otimes)$  endlich erzeugter VR. Dann heißt  $V$  *n-dimensional*,  $n \in \mathbb{N}_0$ , falls es ein Basis mit  $n$  Elementen gibt.  $n$  heißt die *Dimension* von  $V$ .



# Kapitel 8

## Lineare Algebra II: Lineare Abbildungen

### 8.1 Grundlagen und Isomorphismen

#### Definition 8.1

a) Seien  $V, W$   $K$ -VR. Eine Abbildung

$$f : V \rightarrow W \tag{8.1}$$

heißt *linear* oder *Homomorphismus*, falls gilt

$$f(x \oplus y) = f(x) \oplus f(y) \tag{8.2}$$

$$f(s \otimes x) = s \otimes f(x) \tag{8.3}$$

$$\text{für alle } x, y \in V, s \in K \tag{8.4}$$

Wir setzen

$$L(V, W) := \{f : V \rightarrow W : f \text{ ist linear}\} \tag{8.5}$$

b) Eine bijektive lineare Abbildung heißt *Isomorphismus*. Falls es einen Isomorphismus zwischen  $V$  und  $W$  gibt, so heißen  $V$  und  $W$  *isomorph*.

**Notation** ( $\ker$  = kernel = Kern,  $\text{Im}$  = Image = Bild)

$$\text{für } f : V \rightarrow W \text{ linear} \quad (8.6)$$

$$\ker(f) = \text{Kern}(f) = f^{-1}(\{\mathbf{0}_W\}) = \{v \in V : f(v) = \mathbf{0}_W\} \subseteq V \quad (8.7)$$

$$\text{Im}(f) = \{w \in W : \text{es gibt ein } v \in V : f(v) = w\} \subseteq W \quad (8.8)$$

### Lemma 8.2

Seien  $U, V, W$   $K$ -VR.

Sind  $f : U \rightarrow V$  und  $g : V \rightarrow W$  linear, dann ist auch  $g \circ f : U \rightarrow W$  linear.

### Satz 8.3

Seien  $V, W$   $K$ -VR,  $\{b_1 \dots b_n\}$  Basis von  $V$ ,  $\{w_1, \dots, w_n\} \subseteq W$ . Dann gibt es genau eine lineare Abbildung  $f : V \rightarrow W$  mit  $f(b : i) = w_i$  für alle  $i \in \{1, \dots, n\}$

### Satz 8.4

Seien  $U, V, W$   $K$ -VR.

- Ist  $f : U \rightarrow V$  ein Isomorphismus<sup>1</sup> (Iso), dann ist  $f^{-1} : U \rightarrow V$  auch ein Iso.
- Sind  $f : U \rightarrow V$  und  $g : V \rightarrow W$  Iso, dann ist auch  $g \circ f : U \rightarrow W$  ein Iso.
- Auf der Menge aller  $K$ -VR ist durch

$$U \cong V : \Longleftrightarrow U \text{ und } V \text{ sind isomorph} \quad (8.9)$$

eine Äquivalenzrelation gegeben.

### Satz 8.5

Seien  $U, V$   $K$ -VR mit  $\dim U = \dim V \in \mathbb{N}_0$ . Dann sind  $U$  und  $V$  isomorph.

---

<sup>1</sup>Isomorphismus = bijektive lineare Abbildung

## 8.2 Kern und Bild, Dimensionsformel

### Definition 8.6

Seien  $U, V$   $K$ -VR,  $f : U \rightarrow V$  linear. Dann ist

$$\ker(f) = \text{Kern}(f) = \{u \in U : f(u) = \mathbf{0}_V\} \quad (8.10)$$

$$\text{Im}(f) = \text{Bild}(f) = f(U) \quad (8.11)$$

$$= \{v \in V : \text{es gibt ein } u \in U \text{ mit } f(u) = v\} \quad (8.12)$$

$$= \{f(u) : u \in U\} \quad (8.13)$$

**Bemerkung**  $\ker(f)$  ist UVR von  $U$ .  $\text{Im}(f)$  ist UVR von  $V$ .

### Satz 8.7

Seien  $U, V$   $K$ -VR,  $f : U \rightarrow V$  linear.

1. Es gilt:

$$f \text{ ist injektiv} \iff \ker(f) = \{\mathbf{0}_U\} \quad (8.14)$$

2. Es gilt (nach Definition von Surjektivität):

$$f \text{ ist surjektiv} \iff \text{Im}(f) = V \quad (8.15)$$

3. Falls  $U = \langle \{u_1, \dots, u_n\} \rangle$  endlich erzeugt ist, dann ist

$$\text{Im}(f) = \langle \{f(u_1), \dots, f(u_n)\} \rangle \quad (8.16)$$

### Lemma 8.8

Sei  $V$  ein endlich erzeugter  $K$ -VR,  $V \neq \{\mathbf{0}\}$ ,  $B = \{b_1, \dots, b_n\} \subseteq V$ . Folgende Aussagen sind äquivalent:

1.  $B$  ist Basis von  $V$ .

2.  $B$  ist ein linear unabhängiges Erzeugendensystem für  $V$ .
3.  $B$  ist linear unabhängig und  $|B| = \dim(V)$ .
4.  $B$  ist linear unabhängig und  $B \cup \{v\}$  ist linear abhängig für alle  $v \in V \setminus B$ .
5.  $B$  ist ein Erzeugendensystem für  $V$ , und  $B \setminus \{b_i\}$  ist kein Erzeugendensystem für alle  $b_i \in B$ .
6. Jedes  $v \in V$  ist eine eindeutige Darstellung der Form

$$v = (s_1 \otimes b_1) \oplus \dots \oplus (s_n \otimes b_n) \text{ mit } s_1, \dots, s_n \in K \quad (8.17)$$

7. Ist  $A = \{a_1, \dots, a_k\} \subseteq V$  linear unabhängig, dann  $k \leq n$ , und es gibt  $(n - k)$  Elemente in  $B$  so dass  $A$  und diese Elemente  $b_{i_1}, \dots, b_{i_{n-k}}$  eine Basis von  $V$  bilden.

### Satz 8.9

Seien  $U, V$   $K$ -VR,  $\dim(U) = n \in \mathbb{N}_0$ . Sei  $f : U \rightarrow V$  linear. Dann gilt

$$\dim(U) = \dim(\ker(f)) + \dim(\operatorname{Im}(f)) \quad (8.18)$$

### Korollar 8.10

Seien  $U, V$   $K$ -VR mit  $\dim(U) = \dim(V) \in \mathbb{N}_0$ ,  $f : U \rightarrow V$  linear. Dann gilt

$$f \text{ injektiv} \iff f \text{ surjektiv} \iff f \text{ bijektiv} \quad (8.19)$$

## 8.3 Matrizen

### Idee

$U, V$   $K$ -VR,  $f : U \rightarrow V$  linear,  $U$  endlich erzeugt.

$f$  ist eindeutig bestimmt durch die Bilder einer Basis von  $U$ .

$B = \{b_1, \dots, b_n\}$  Basis von  $U$

$$[f(b_1) \quad \dots \quad f(b_n)] \quad (8.20)$$

**Notation**

Von jetzt an schreiben wir Vektoren von  $K^n$  "vertikal", also

$$K^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} : x_i \in K, i = 1, \dots, n \right\} \text{ mit} \quad (8.21)$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \quad (8.22)$$

$$s \otimes \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} s \cdot x_1 \\ \vdots \\ s \cdot x_n \end{pmatrix}, \text{ für } x_1, \dots, x_n, y_1, \dots, y_n, s \in K \quad (8.23)$$

**Definition 8.11**

Sei  $(K, +, \cdot)$  ein Körper,  $m, n \in \mathbb{N}$ . Eine  $(m \times n)$ -Matrix mit Einträgen aus  $K$  ist ein rechteckiges Schema

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \quad (8.24)$$

aus  $m$  Zeilen und  $n$  Spalten mit Einträgen  $a_{ij} \in K, 1 \leq i \leq m, 1 \leq j \leq n$ .

$i \in \{1, \dots, m\}$  ist Zeilenindex,  $j \in \{1, \dots, n\}$  ist Spaltenindex.

Schreibweise:  $(a_{ij})$  oder  $(a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$

Die Menge aller  $(m \times n)$ -Matrizen mit Einträgen aus  $K$  bezeichnen wir mit  $K^{(m \times n)}$ .

**Bemerkung** Wir identifizieren  $K^n \triangleq K^{n \times 1}$

**Definition 8.12**

Seien  $U, V$  zwei  $K$ -VR,  $B = \{b_1, \dots, b_n\} \subseteq U$  Basis von  $U$ ,  $P = \{p_1, \dots, p_m\} \subseteq V$  Basis von  $V$ . Sei  $f : U \rightarrow V$  linear. Für  $j = 1, \dots, n$

$$f(b_j) = (a_{1j} \otimes p_1) \oplus \dots \oplus (a_{mj} \otimes p_m) \quad (8.25)$$

$$\text{mit } a_{ij} \in K \text{ für alle } i \in \{1, \dots, m\}, j \in \{1, \dots, n\} \quad (8.26)$$

Dann heißt  $(a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$  die *Darstellungsmatrix* von  $f$  bezüglich der Basen  $B$  und  $P$ .

**Bemerkung** “In der Darstellungsmatrix stehen in den Spalten die Basen der Basisvektoren.”

**Beispiele** Sei  $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3, f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = \begin{pmatrix} x+y \\ -y \\ x-y \end{pmatrix}$

- Betrachte Standardbasen  $B = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^2$ ,

$$P = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^3$$

Dann

$$f\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = 1 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \oplus 0 \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \oplus 1 \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad (8.27)$$

$$f\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = 1 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \oplus (-1) \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \oplus 0 \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad (8.28)$$

$$\rightarrow \text{Darstellungsmatrix } \begin{bmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{bmatrix} \in \mathbb{R}^{3 \times 2} \quad (8.29)$$

- Betrachte  $B = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} \subset \mathbb{R}^2, P = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^3$

Es gilt

$$f\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} = 2 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \oplus (-1) \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \oplus 0 \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad (8.30)$$

$$f\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = 0 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \oplus 1 \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \oplus 2 \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad (8.31)$$

$$\rightarrow \text{Darstellungsmatrix} \begin{bmatrix} 2 & 0 \\ -1 & 1 \\ 0 & 2 \end{bmatrix} \in \mathbb{R}^{3 \times 2} \quad (8.32)$$

- Betrachte  $B = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^2, P = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\} \subset \mathbb{R}^3$

Es gilt

$$f\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = 1 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \oplus (-1) \otimes \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \oplus 1 \otimes \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad (8.33)$$

$$f\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} = 2 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \oplus 0 \otimes \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \oplus (-1) \otimes \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad (8.34)$$

$$\rightarrow \text{Darstellungsmatrix} \begin{bmatrix} 1 & 2 \\ -1 & 0 \\ 0 & -1 \end{bmatrix} \in \mathbb{R}^{3 \times 2} \quad (8.35)$$

**Beobachtung** Sei  $f : K^n \rightarrow K^m$  linear mit Darstellungsmatrix  $A = (a_{ij})$   $\begin{smallmatrix} 1 \leq i \leq m \\ 1 \leq j \leq n \end{smallmatrix}$

bzgl. Standardbasen. Dann gilt für  $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$

$$f(x) = f \left( x_1 \otimes \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \oplus \dots \oplus x_n \otimes \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right) \quad (8.36)$$

$$\stackrel{f \text{ linear}}{=} x_1 \cdot f \left( \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right) \oplus \dots \oplus x_n \otimes f \left( \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right) \quad (8.37)$$

$$= x_1 \otimes \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} \oplus \dots \oplus x_n \otimes \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \quad (8.38)$$

### Definition 8.13

Wir definieren für  $(a_{ij}) = A \in K^{m \times n}$  und  $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x \in K^n$

$$A \cdot x = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11} \cdot x_1 + \cdots + a_{1n} \cdot x_n \\ \vdots \\ a_{m1} \cdot x_1 + \cdots + a_{mn} \cdot x_n \end{bmatrix} \quad (8.39)$$

### Satz 8.14

a) Sei  $B \in K^{m \times n}$ . Dann ist die Abbildung  $g : K^n \rightarrow K^m, g(x) := B \cdot x$  linear.



- b) Sei  $f : K^n \rightarrow K^m$  linear. Dann gibt es eine Matrix  $A \in K^{m \times n}$  so dass  $f(x) = A \cdot x$  für alle  $x \in K^n$ .

**Definition 8.15**

- a) Für  $A \in K^{m \times n}$ ,  $B \in K^{l \times m}$  definieren wir  $BA \in K^{k \times n}$  als

$$(B \cdot A)_{rs} = \sum_{i=1}^m b_{ri} \cdot a_{is}, r \in \{1, \dots, l\}, s \in \{1, \dots, n\} \quad (8.40)$$

*“Zeile mal Spalte”*

- b) Für  $A, A' \in K^{m \times n}$  definieren wir  $A + A' \in K^{m \times n}$  als

$$(A + A')_{ij} = a_{ij} + a'_{ij} \quad (8.41)$$

**Bemerkung**

Falls	$A$	Darstellungsmatrix zu	$f : K^n \rightarrow K^m$
	$A'$	Darstellungsmatrix zu	$f' : K^n \rightarrow K^m$
	$B$	Darstellungsmatrix zu	$g : K^m \rightarrow K'$
dann	$(A + A')$	Darstellungsmatrix zu	$f + f' : K^n \rightarrow K^m$
	$B \times A$	Darstellungsmatrix zu	$g \circ f : K^n \rightarrow K'$



# Anhang A

## Beweise

### A.1 zu Kapitel 8 Lineare Algebra II: Lineare Abbildungen

#### Beweis Satz 7.10

**Satz 7.10** (7.5, Seite 64)

Sei  $(V, \oplus, \otimes)$  ein endlich erzeugter VR. Dann haben je zwei Basen die gleiche Anzahl an Elementen.

Idee des Beweises: “Basisaustausch”.

**Beispiel**  $\mathbb{R}^2$  als  $\mathbb{R}$ -VR,  $B = \{(1, 0), (0, 1)\}$  Basis.

Betrachte  $A = \{(1, 1), (5, 3), (3, 5)\}$ . Beobachtung:  $A \not\subseteq \langle \{(1, 0)\} \rangle$

Wir haben z. B.

$$\underbrace{(1, 1)}_{\in A} = (1, 0) \oplus (0, 1) \tag{A.1}$$

$$\implies (0, 1) = (1, 1) \oplus [(-1) \otimes (0, 1)] \tag{A.2}$$

$$\implies \{(1, 1), (0, 1)\} \text{ ist Erzeugendensystem von } \mathbb{R}^2 \tag{A.3}$$

Nächster Schritt: Es gilt

$$(5, 3) = (5 \otimes (1, 1)) \oplus ((-2) \otimes (0, 1)) \implies (0, 1) \in \langle \{(5, 3), (1, 1)\} \rangle \quad (\text{A.4})$$

$$\implies \{(5, 3), (1, 1)\} \text{ ist Erzeugendensystem von } \mathbb{R}^2 \quad (\text{A.5})$$

$$\implies (3, 5) \in \langle \{(5, 3), (1, 1)\} \rangle \implies A \text{ ist linear abhängig} \quad (\text{A.6})$$

**Beweis** des Satzes: Wir zeigen: Falls  $\{b_1, \dots, b_n\}, n \in \mathbb{N}_0$  ein Erzeugendensystem von  $V$  ist und  $A = \{a_1, \dots, a_{n+1}\}, |A| = n + 1$ , dann ist  $A$  linear abhängig, also insbesondere keine Basis.

Vollständige Induktion nach  $n$ :

I. A.:  $n = 0$

$$V = \langle \emptyset \rangle = \{\mathbf{0}\} \implies A = \{\mathbf{0}\} \text{ (einzige Teilmenge von } V \text{ mit einem Element)} \quad (\text{A.7})$$

$$\implies A \text{ linear abhängig} \quad (\text{A.8})$$

I. V.: Falls  $\tilde{V} \subseteq V$  von  $k$  Vektoren aus  $V$  erzeugt wird mit  $k \leq n \in \mathbb{N}_0$  beliebig, aber fest, dann ist je  $(k + 1)$  Vektoren aus  $\tilde{V}$  linear abhängig.

I. S.: Sei  $\tilde{V} = \langle \{b_1, \dots, b_{n+1}\} \rangle, A = \{a_1, \dots, a_{n+2}\}, |A| = n + 2$

Angenommen  $A$  ist linear unabhängig.

Zwei Möglichkeiten:

1.  $\underbrace{A}_{2 \text{ Vektoren}} \subseteq \langle \{b_2, \dots, b_{n+1}\} \rangle \implies \text{nach I. V. ist } A \text{ linear unabhängig. } \zeta$

2. Es gibt ein  $a \in A$ , o. E.<sup>1</sup>  $a_1$  (umnummerieren möglich), so dass

$$a_1 \in \langle \{b_2, \dots, b_{n+1}\} \rangle \quad (\text{A.9})$$

---

<sup>1</sup>ohne Einschränkung

$\implies$  Jede Linearkombination  $a_1 = (s_1 \otimes b_1) \oplus \dots \oplus (s_{n+1} \otimes b_{n+1})$ ,  $s_i \in K$   
erfüllt  $s_1 \neq 0$

$$\implies b_1 = s_1^{-1} \cdot a_1 - s_1^{-1} \cdot [(s_2 \otimes b_2) \oplus \dots \oplus (s_{n+1} \otimes b_{n+1})] \implies \{a_1, b_2, \dots, b_{n+1}\} \quad (\text{A.10})$$

Falls  $\underbrace{\{a_2, \dots, a_{n+1}\}}_{n+1 \text{ Vektoren}} \subseteq \underbrace{\{\cancel{a_1}, b_3, \dots, b_{n+1}\}}_{\substack{n-1 \\ \cancel{\text{Vektoren}}}}$ , dann sind  $a_2, \dots, a_{n+2}$  linear abhän-

gig.  $\nrightarrow$

Ähnlich wie oben: o. E.

$$\{a_1, a_2, b_3, \dots, b_{n+1}\} \text{ Erzeugendensystem} \quad (\text{A.11})$$

Rest: Übungsblatt

# Index

- Abbildung, 14
  - bijektiv, 16
  - Definitionsbereich, 14
  - identische Abbildung/Identität, 16
  - injektiv, 16
  - surjektiv, 16
  - Verknüpfungen, 35
  - Vorschrift, 14
  - Ziel-/Wertebereich, 14
- abelsche/kommutative Gruppe (Verknüpfungen), 36
- Addition (Verknüpfungen), 37
- Allquantor, 8
- antisymmetrisch (Relation), 14
- Assoziativität
  - Komposition, 16
  - Mengen, 10
  - Verknüpfungen, 35
- Aufzählen der Elemente (Beschreibung von Mengen), 7
- Basis (Vektorräume), 62
- Behauptung (Implikation), 6
- Beschreibung von Mengen, 7
  - abgekürzte beschreibende Form, 8
  - Aufzählen der Elemente, 7
  - beschreibende Form, 7
- Beschränktheit (Folgen), 27
- Betrag (komplexe Zahlen), 26
- bijektiv (Abbildung), 16
- Bild
  - von Funktion  $f$ , 15
  - von Menge  $Z$  unter Funktion  $f$ , 15
  - lineare Abbildungen, 66, 67
- Bild Im (lineare Abbildungen), 66, 67
- binäre/totale Ordnung (Mengen), 19
- Darstellungsmatrix (Matrizen), 70
- De Morgan'sche Regeln (Tautologie), 6
- Definitionsbereich (Abbildung), 14
- die Aussage gilt für fast alle  $n \in \mathbb{N}$  (Folgen), 29
- Differenzmenge (Mengen), 9
- Dimension (Vektorräume), 64
- disjunkt (Mengen), 9
- Disjunktion, 5
- Distributivität (Verknüpfungen), 37
- divergent (Folgen), 28
- Division mit Rest, 38
- Durchschnitt (Mengen), 9
- Einheit (Ring mit Eins, Verknüpfungen),

- 45
- Element, 7
- endlich (Mengen), 18
- endlich erzeugt (Vektorräume), 62
- Erzeugendensystem (Vektorräume), 62
- Erzeugnis (Vektorräume), 61
- Euklidischer Algorithmus, 39
- Eulersche  $\varphi$ -Funktion, 48
- Existenzquantor, 8
  
- Fakultät, 23
- Kleiner Satz von Fermat, 47
- Fibonacci-Zahlen, 24
- Folgen, 27
  - Beschränktheit, 27
  - die Aussage gilt für fast alle  $n \in \mathbb{N}$ , 29
  - divergent, 28
  - Divergenz, 28
  - Glieder, 27
  - Grenzwert, 27
  - konvergent, 28
  - konvergent gegen  $\pm\infty$ , 30
  - Konvergenz, 27
  - L'Hospital'sche Regel, 32
  - monoton, 30
  - monoton fallend, 30
  - monoton wachsend, 30
  - Monotonie, 30
  - Nullfolge, 28
  - Teilfolge, 29
  - Umgebung von  $x$ , 28
  - (uneigentlich) konvergent gegen  $\pm\infty$ , 30
- Funktion, 14
  
- ganze Zahlen, 7
- geordnetes  $n$ -Tupel (Mengen), 11
- geordnetes Paar (Mengen), 11
- ggT, *siehe* größter gemeinsamer Teiler, 39
- gleichmächtig (Mengen), 18
- Glieder (Folgen), 27
- Graph, 13
- Grenzwert (Folgen), 27
- Gruppe (Verknüpfungen), 36
- Gruppen
  - Index, 54
  - Ordnung, 53
  - Ordnung eines Elements, 54
  - Untergruppen, 51
  - von  $H$  erzeugte Untergruppe, 52
  - zyklisch, 55
- größter gemeinsamer Teiler (ggT), 39
  
- Halbgruppe (Verknüpfungen), 35
- Halbordnung (Mengen), 19
  - Hasse-Diagramm, 19
  - Infimum, 20
  - maximal, 19
  - Maximum, 19
  - minimal, 19
  - Minimum, 19
  - obere Schranke, 19
  - Supremum, 20
  - untere Schranke, 19
- Hauptsatz der Arithmetik, 41
- Hintereinanderausführung/Komposition/Verkettung, 15
- Homomorphismus (lineare Abbildungen), 65

- $i$  (komplexe Zahlen), 25
- Idempotenz (Mengen), 10
- identische Abbildung/Identität, 16
- Im, *siehe* Bild (lineare Abbildungen), 66, 67
- imaginäre Zahl (komplexe Zahlen), 25
- Imaginärteil (komplexe Zahlen), 26
- Implikation, 6
  - Behauptung, 6
  - Voraussetzung, 6
- Index (Gruppen), 54
- Induktion, 22
  - Induktionsanfang, 22
  - Induktionsschritt, 22
- Induktionsanfang (Induktion), 22
- Induktionsschritt (Induktion), 22
- Infimum (Halbordnung), 20
- injektiv (Abbildung), 16
- Inklusion (Mengen), 9
- inverse Funktion, 14
- inverses Element (Verknüpfungen), 36
- invertierbar (Ring mit Eins, Verknüpfungen), 45
- isomorph (lineare Abbildungen), 65
- Isomorphismus (lineare Abbildungen), 65
- Junktoren, 5
- $K$ -Vektorraum (Vektorräume), 57
- kartesische Produkt (Mengen), 11
- ker, *siehe* Kern (lineare Abbildungen), 66, 67
- Kern ker (lineare Abbildungen), 66, 67
- kgV, *siehe* kleinstes gemeinsames Vielfaches, 42
- Kleiner Satz von Fermat, 47
- kleinstes gemeinsames Vielfaches (kgV), 42
- Komposition/Verkettung/Hintereinanderausführung, 15
- kommutative/abelsche Gruppe (Verknüpfungen), 36
- Kommutativität
  - Mengen, 10
  - Ring (Verknüpfungen), 37
  - Verknüpfungen, 35
- Komplement (Mengen), 9
- komplexe Zahlen, 25
  - Addition, 26
  - Betrag, 26
  - $i$ , 25
  - imaginäre Zahl, 25
  - Imaginärteil, 26
  - konjugent-komplexe Zahl, 26
  - Multiplikation, 26
  - Realteil, 26
- kongruent modulo  $n$ , 43
- Kongruenz modulo  $n$ , 43
  - $\mathbb{Z}_n$ , 44
- konjugent-komplexe Zahl (komplexe Zahlen), 26
- Konjunktion, 5
- konvergent (Folgen), 28
- konvergent gegen  $\pm\infty$  (Folgen), 30
- Konvergenz (Folgen), 27
- Körper (Verknüpfungen), 37
- L'Hospital'sche Regel (Folgen), 32
- leere Menge, 7
- linear abhängig (Vektorräume), 61



- linear unabhängig (Vektorräume), 61
- lineare Abbildungen, 65
  - Bild  $\text{Im}$ , 66, 67
  - Homomorphismus, 65
  - isomorph, 65
  - Isomorphismus, 65
  - Kern  $\text{ker}$ , 66, 67
- lineare Abbildungen (Bild), 66, 67
- Linearkombination (Vektorräume), 60
- logische Folgerung, 6
- $(m \times n)$ -Matrix mit Einträgen aus  $K$  (Matrizen), 69
- Matrizen
  - Darstellungsmatrix, 70
  - $(m \times n)$ -Matrix mit Einträgen aus  $K$ , 69
- maximal (Halbordnung), 19
- Maximum (Halbordnung), 19
- Mengen, 7
  - Assoziativität, 10
  - Differenzmenge, 9
  - disjunkt, 9
  - Durchschnitt, 9
  - endlich, 18
  - geordnetes  $n$ -Tupel, 11
  - geordnetes Paar, 11
  - gleichmächtig, 18
  - Halbordnung, 19
    - Hasse-Daigramm, 19
    - Infimum, 20
    - maximal, 19
    - Maximum, 19
    - minimal, 19
    - Minimum, 19
    - obere Schranke, 19
    - Supremum, 20
    - untere Schranke, 19
  - Idempotenz, 10
  - Inklusion, 9
  - kartesische Produkt, 11
  - Kommutativität, 10
  - Komplement, 9
  - Mächtigkeit, 18
  - Partition, 17
  - totale/binäre Ordnung, 19
  - Verknüpfungen, 35
  - Vereinigung, 9
- minimal (Halbordnung), 19
- Minimum (Halbordnung), 19
- Monoid (Verknüpfungen), 35
- monoton (Folgen), 30
- monoton fallend (Folgen), 30
- monoton wachsend (Folgen), 30
- Monotonie (Folgen), 30
- Multiplikation (Verknüpfungen), 37
- Mächtigkeit (Mengen), 18
- $n$ -dimensional (Vektorräume), 64
- natürliche Zahlen, 7, 21
  - mit Null, 7
- Negation, 5
- neutrales Element (Verknüpfungen), 36
- Nullfolge (Folgen), 28
- Nullvektor (Vektorräume), 57
- obere Schranke (Halbordnung), 19
- ord, *siehe* Ordnung (Gruppen), 54
- Ordnung (Gruppen), 53
- Ordnung eines Elements (Gruppen), 54

- Partition (Mengen), 17
- PFZ, *siehe* Primfaktorzerlegung, 41
- Potenz, 23
- Primfaktorzerlegung, 41
- Primzahl, 41
- Produkt, rekursiv, 23
- Produktschreibweise, 21
- Quantoren
  - Allquantor, 8
  - Existenzquantor, 8
- rationale Zahlen, 7
- Realteil (komplexe Zahlen), 26
- reelle Zahlen, 7
- reflexiv (Relation), 13
- Relation, 13
  - antisymmetrisch, 14
  - reflexiv, 13
  - Relation auf Menge  $A$ , 13
  - reliert sein/in Relation zueinander stehen, 13
  - symmetrisch, 13
  - transitiv, 14
- Rest bei Division, 38
- Ring (Verknüpfungen), 37
- Ring mit Eins (Verknüpfungen), 37
- Ring mit Eins (Verknüpfungen)
  - Einheit, 45
  - invertierbar, 45
- RSA-Verschlüsselung, 49
- Summe, rekursiv, 23
- Summenschreibweise, 21
- Supremum (Halbordnung), 20
- surjektiv (Abbildung), 16
- symmetrisch (Relation), 13
- Tautologie, 6
  - De Morgan'sche Regeln, 6
- teilerfremd, 39
- Teilfolge (Folgen), 29
- Teilmenge, 9
- Teilraum (Vektorräume), 60
- teilt, 39
- totale/binäre Ordnung (Mengen), 19
- transitiv (Relation), 14
- Tupel, 11
- Umgebung von  $x$  (Folgen), 28
  - (uneigentlich) konvergent gegen  $\pm\infty$  (Folgen), 30
- Unter(vektor)raum (Vektorräume), 60
- untere Schranke (Halbordnung), 19
- Untergruppen (Gruppen), 51
  - von  $H$  erzeugte Untergruppe, 52
- Urbild von Menge  $M$  unter Funktion  $f$ , 15
- UVR, *siehe* Unter(vektor)raum, 60
- Vektoren (Vektorräume), 58
- Vektorräume
  - Basis, 62
  - Dimension, 64
  - endlich erzeugt, 62
  - Erzeugendensystem, 62
  - Erzeugnis, 61
  - $K$ -Vektorraum, 57
  - linear abhängig, 61
  - linear unabhängig, 61

- lineare Abbildungen, 65
- Linearkombination, 60
- $n$ -dimensional, 64
- Nullvektor, 57
- Teilraum, 60
- Unter(vektor)raum, 60
- Vektoren, 58
- Verkettung/Komposition/Hintereinander-  
ausführung, 15
- Verknüpfungen, 35
  - abelsche/kommutative Gruppe, 36
  - Addition, 37
  - Assoziativität, 35
  - Distributivität, 37
  - Gruppe, 36
  - Halbgruppe, 35
  - inverses Element, 36
  - kommutative/abelsche Gruppe, 36
  - Kommutativität, 35
  - Kommutativität (Ring), 37
  - Körper, 37
  - Monoid, 35
  - Multiplikation, 37
  - neutrales Element, 36
  - Ring, 37
    - Kommutativität, 37
  - Ring mit Eins, 37
- Vereinigung (Mengen), 9
- Verknüpfungen
  - Ring mit Eins
    - Einheit, 45
  - invertierbar, 45
- Vielfaches, 39
- Vollständige Induktion, 22
- von  $H$  erzeugte Untergruppe (Gruppen),  
52
- Voraussetzung (Implikation), 6
- Vorschrift (Abbildung), 14
- VR, *siehe* Vektorräume, 57
- Werte-/Zielberich (Abbildung), 14
- Ziel-/Wertebereich (Abbildung), 14
- $\mathbb{Z}_n$  (Kongruenz modulo  $n$ ), 44
- Zuordnung, 14
- zyklisch (Gruppen), 55
- Äquivalenz, 6
- Äquivalenzklasse, 17
- Äquivalenzrelation, 17