

# Grundbegriffe der Mathematik

Geschrieben von Jan Pöschko

auf Grundlage der Vorlesung im WS 2005/2006 von Ao.Univ.-Prof. Clemens Heuberger

## Inhaltsverzeichnis

<b>1</b>	<b>Aussagenlogik</b>	<b>3</b>
1.1	Verknüpfungen . . . . .	3
1.2	Normalformen . . . . .	5
1.3	Quantoren . . . . .	6
<b>2</b>	<b>Mengen</b>	<b>9</b>
<b>3</b>	<b>Relationen</b>	<b>13</b>
3.1	Äquivalenzrelationen . . . . .	14
3.2	Ordnungsrelationen . . . . .	15
<b>4</b>	<b>Funktionen</b>	<b>19</b>
<b>5</b>	<b>Einführung in algebraische Strukturen</b>	<b>23</b>
5.1	Gruppen . . . . .	23
5.2	Ringe . . . . .	27
5.3	Körper . . . . .	30
<b>6</b>	<b>Aufbau des Zahlensystems</b>	<b>33</b>
6.1	Natürliche Zahlen $\mathbb{N}$ und Vollständige Induktion . . . . .	33
6.2	Ganze Zahlen $\mathbb{Z}$ . . . . .	35
6.3	Rationale Zahlen $\mathbb{Q}$ . . . . .	37
6.4	Reelle Zahlen $\mathbb{R}$ . . . . .	38
6.5	Komplexe Zahlen $\mathbb{C}$ . . . . .	40
<b>7</b>	<b>Elementarste Kombinatorik</b>	<b>45</b>
7.1	Permutationen . . . . .	45
7.2	Binomialkoeffizienten . . . . .	45



# 1 Aussagenlogik

**Definition 1.1.** Eine Aussage ist ein sprachlicher Satz, der seinem Inhalt nach wahr oder falsch ist.

Beispiele.

- „Heute ist Montag, der 3. Oktober 2005“ (wahre Aussage <sup>1</sup>)
- „Es regnet.“ (wahre Aussage)
- „ $x$  ist eine gerade Zahl.“ (keine Aussage)

## 1.1 Verknüpfungen

**Definition 1.2** (Konjunktion, logisches Und). Seien  $p, q$  zwei Aussagen. Dann sei  $p \wedge q$  die Aussage, die genau dann wahr ist, wenn  $p$  und  $q$  beide wahr sind, also:

$p$	$q$	$p \wedge q$
$W$	$W$	$W$
$W$	$F$	$F$
$F$	$W$	$F$
$F$	$F$	$F$

Beispiel.

$p$	„5 ist eine Primzahl.“	.....	wahr
$q$	„5 ist eine ungerade Zahl.“	....	wahr
$p \wedge q$	„5 ist eine ungerade Primzahl.“		wahr

**Definition 1.3** (Disjunktion, logisches Oder). Seien  $p, q$  zwei Aussagen. Dann sei  $p \vee q$  die Aussage, die genau dann wahr ist, wenn  $p$  oder  $q$  (oder beide) wahr sind, also:

$p$	$q$	$p \vee q$
$W$	$W$	$W$
$W$	$F$	$W$
$F$	$W$	$W$
$F$	$F$	$F$

Beispiel.

$p$	„5 ist eine Primzahl.“	.....	wahr
$q$	„2 ist eine ungerade Zahl.“		falsch
$p \vee q$		.....	wahr

**Definition 1.4** (Negation). Sei  $p$  eine Aussage. Dann sei  $\neg p$  die negierte Aussage, also:

$p$	$\neg p$
$W$	$F$
$F$	$W$

**Definition 1.5** (Subjunktion, Wenn-Dann). Seien  $p, q$  zwei Aussagen. Dann sei  $p \rightarrow q$  die Aussage, die genau dann wahr ist, wenn  $q$  aus  $p$  folgt, also:

$p$	$q$	$p \rightarrow q$
$W$	$W$	$W$
$W$	$F$	$F$
$F$	$W$	$W$
$F$	$F$	$W$

Beispiel.

$p$	„Es regnet.“	.....	wahr
$q$	„Die Straße ist nass.“	.....	falsch
$p \vee q$	„Wenn es regnet, dann ist die Straße nass.“		wahr

---

<sup>1</sup>zumindest zum Zeitpunkt der Abhaltung der Vorlesung

**Definition 1.6** (Äquivalenz). Seien  $p, q$  zwei Aussagen. Dann sei  $p \leftrightarrow q$  die Aussage, die genau dann wahr ist,  $p$  und  $q$  äquivalent sind, also:

$p$	$q$	$p \leftrightarrow q$
W	W	W
W	F	F
F	W	F
F	F	W

*Beispiel.*

$p$	„Sie können zur mündlichen Prüfung antreten.“	wahr
$q$	„Sie haben mindestens 50 % der Punkte.“ . . . .	falsch
$p \leftrightarrow q$	„Sie können genau dann zur Prüfung antreten, wenn Sie mindestens 50 % der Punkte haben.“	wahre Aussage

**Satz 1.1** (Rechenregeln für logische Verknüpfungen). Seien  $p, q, r$  Aussagen. Dann gilt:

1.  $\neg(\neg p)$  ist gleichwertig zu  $p$ .
2.  $\neg(p \wedge q)$  ist gleichwertig zu  $\neg p \vee \neg q$ . (Regel von de Morgan)
3.  $\neg(p \vee q)$  ist gleichwertig zu  $\neg p \wedge \neg q$ . (Regel von de Morgan)
4.  $p \rightarrow q$  ist gleichwertig zu  $(\neg q) \rightarrow (\neg p)$ .
5.  $p \wedge (q \vee r)$  ist gleichwertig zu  $(p \wedge q) \vee (p \wedge r)$ .
6.  $p \vee (q \wedge r)$  ist gleichwertig zu  $(p \vee q) \wedge (p \vee r)$ .

*Beweis.*

1. 

$p$	$\neg p$	$\neg(\neg p)$
W	F	W
F	W	F

2. 

$p$	$q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
W	W	W	F	F	F	F
W	F	F	W	F	W	W
F	W	F	W	W	F	W
F	F	F	W	W	W	W

3. 

$p$	$q$	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
W	W	W	F	F	F	F
W	F	W	F	F	W	F
F	W	W	F	W	F	F
F	F	F	W	W	W	W

4. 

$p$	$q$	$p \rightarrow q$	$\neg p$	$\neg q$	$(\neg q) \rightarrow (\neg p)$
W	W	W	F	F	W
W	F	F	F	W	F
F	W	W	W	F	W
F	F	W	W	W	W

5.	$p$	$q$	$r$	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
	W	W	W	W	W	W	W	W
	W	W	F	W	W	W	F	W
	W	F	W	W	W	F	W	W
	W	F	F	F	F	F	F	F
	F	W	W	W	F	F	F	F
	F	W	F	W	F	F	F	F
	F	F	W	W	F	F	F	F
	F	F	F	F	F	F	F	F

6. Entsprechend.

□

*Bemerkung.*

1. Für „ist gleichwertig zu“ schreibt man häufig  $\Leftrightarrow$  oder  $\equiv$  oder  $\sim$ .
2. Bei einer Subjunktion  $p \rightarrow q$  nennt man  $p$  eine „hinreichende Bedingung“ für  $q$  und  $q$  eine „notwendige Bedingung“ für  $p$ .

## 1.2 Normalformen

**Definition 1.7.** *Ein logischer Ausdruck heißt*

- disjunktive Normalform, wenn er die Gestalt

$$D_1 \vee D_2 \vee D_3 \vee \dots \vee D_n$$

hat und jedes der  $D_j$  die Gestalt

$$E_1 \wedge E_2 \wedge E_3 \wedge \dots \wedge E_k$$

hat, wobei die  $E_i$  Aussagen oder verneinte Aussagen sind.

- konjunktive Normalform, wenn er die Gestalt

$$D_1 \wedge D_2 \wedge D_3 \wedge \dots \wedge D_n$$

hat und jedes der  $D_j$  die Gestalt

$$E_1 \vee E_2 \vee E_3 \vee \dots \vee E_k$$

hat, wobei die  $E_i$  Aussagen oder verneinte Aussagen sind.

*Beispiel.*

$$(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$$

ist die disjunktive Normalform von  $p \rightarrow q$  (zu erreichen über die Wahrheitstafel oder Satz 1.1 verbunden mit der Regel  $p \rightarrow q \Leftrightarrow \neg p \vee q$ ).

*Bemerkung.* Die konjunktive Normalform ist über Distributivgesetze usw. oder über de Morgan zu erreichen (betrachte disjunktive Normalform des negierten Ausdrucks und negiere das).

*Beispiel.*

$$p \rightarrow q \Leftrightarrow \neg p \vee q \Leftrightarrow \neg(p \wedge \neg q) \Leftrightarrow (\neg p \vee q)$$

**Satz 1.2** (Beweistechniken). *Seien  $p, q, r$  Aussagen. Dann gilt:*

1.  $p \wedge (p \rightarrow q) \Rightarrow q$  (Abtrennungsregel, direkter Beweis)
2.  $\neg q \wedge (p \rightarrow q) \Rightarrow \neg p$  (indirekter Beweis)
3.  $(p \rightarrow q) \wedge (\neg p \rightarrow q) \Rightarrow q$  (Fallunterscheidung)
4.  $(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow (p \rightarrow r)$  (Verkettung)
5.  $(p \rightarrow q) \wedge (p \rightarrow \neg q) \Rightarrow \neg p$  (Reductio ad Absurdum)

**Definition 1.8** (Prioritäten der logischen Verknüpfungen). *In absteigender Reihenfolge:*

1.  $\neg$
2.  $\wedge, \vee$  (gleichberechtigt, ggf. Klammern)
3.  $\rightarrow$
4.  $\leftrightarrow$

**Definition 1.9.** *Eine Aussage, die immer wahr ist, heißt Tautologie. Eine Aussage, die immer falsch ist, heißt Kontradiktion.*

### 1.3 Quantoren

**Definition 1.10.** *Eine Aussageform ist ein Satz, der eine oder mehrere Variablen enthält und für jeden speziellen Wert dieser Variablen zu einer Aussage wird.*

*Beispiel.*

- $A(x) \dots$  „ $x$  ist eine Quadratzahl“
- $A(16) \dots$  wahre Aussage
- $A(5) \dots$  falsche Aussage

**Definition 1.11** (Allquantor, Existenzquantor). *Sei  $A(x)$  eine Aussageform. Dann spricht für*

- $\forall x : A(x)$  „Für alle  $x$  gilt  $A(x)$ .“
- $\exists x : A(x)$  „Es existiert (mindestens) ein  $x$ , für das  $A(x)$  gilt.“

*Manchmal sieht man auch*

- $\overset{1}{\exists}, \exists!$  für „Es existiert genau ein“.
- $\bigwedge_x$  für den Allquantor bzw.  $\bigvee_x$  für den Existenzquantor.

*Beispiel.* Sei  $A(x, y)$  eine Aussageform (abhängig von zwei Variablen). Dann ist

$$\forall x \exists y : A(x, y)$$

nicht dasselbe wie

$$\exists y \forall x : A(x, y).$$

Seien z.B. die  $x$  Wege, die  $y$  Orte, und  $A(x, y)$  die Aussage, dass der Weg  $x$  nach  $y$  führt. Die erste Aussage heißt dann, dass jeder Weg zu einem Ort führt. Die zweite Aussage bedeutet aber, dass es einen Ort gibt (Rom), zu dem alle Wege führen.

**Satz 1.3** (Negation von Quantoren). *Sei  $A(x)$  eine Aussageform. Dann gilt:*

- $\neg(\forall x : A(x)) \Leftrightarrow \exists x : \neg A(x)$
- $\neg(\exists x : A(x)) \Leftrightarrow \forall x : \neg A(x)$

*Beweis.* durch Händefuchteln. □

*Beispiel.* Eine Funktion  $f : \mathbb{R} \rightarrow \mathbb{R}$  heißt *stetig* in  $x \in \mathbb{R}$ , falls

$$\forall \epsilon > 0 \exists \delta > 0 : |x - y| < \delta \rightarrow |f(x) - f(y)| < \epsilon.$$

Frage: Wann ist  $f$  nicht stetig in  $x \in \mathbb{R}$ ?

$$\exists \epsilon > 0 \forall \delta > 0 : \neg(|x - y| < \delta \rightarrow |f(x) - f(y)| < \epsilon)$$

Schauen wir uns nun die Wahrheitstafel für  $\neg(p \rightarrow q)$  an:

$p$	$q$	$p \rightarrow q$	$\neg(p \rightarrow q)$
W	W	W	F
W	F	F	W
F	W	W	F
F	F	W	F

Das bedeutet, dass  $\neg(p \rightarrow q)$  gleichwertig mit  $p \wedge \neg q$  ist, somit bedeutet *unstetig* in  $x \in \mathbb{R}$ :

$$\exists \epsilon > 0 \forall \delta > 0 : |x - y| < \delta \wedge |f(x) - f(y)| \geq \epsilon$$



## 2 Mengen

Laut Cantor: „Eine Menge ist eine Ansammlung wohlunterschiedener Objekte unseres Denkens oder unserer Anschauung zu einem Ganzen.“

Wir betreiben hier „naive Mengenlehre“ (im Gegensatz zur axiomatischen Mengenlehre).

**Notation 2.1.** Sei  $M$  eine Menge.  $x$  heißt Element von  $M$ ,  $x \in M$ , wenn  $x$  in  $M$  enthalten ist.  $x$  heißt kein Element von  $M$ ,  $x \notin M$ , wenn  $x$  nicht in  $M$  enthalten ist.

Mengen können angegeben werden durch

- explizite Aufzählung, z.B.  $M = \{\text{Montag, Dienstag, \dots, Samstag, Sonntag}\}$ ,
- Angabe einer Eigenschaft, z.B.  $\mathbb{Z}_g := \{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z} : x = 2y\}$ .

**Definition 2.2** (Teilmenge). Seien  $M, N$  Mengen.

- $M$  heißt Teilmenge von  $N$ ,  $M \subseteq N$ , falls

$$\forall m \in M : m \in N.$$

- $M$  und  $N$  heißen gleich,  $M = N$ , falls

$$M \subseteq N \wedge N \subseteq M.$$

- $M$  heißt echte Teilmenge von  $N$ ,  $M \subset N$ , falls

$$M \subseteq N \wedge M \neq N.$$

- $M$  heißt Obermenge von  $N$ , falls

$$N \subseteq M.$$

*Bemerkung.* Manchmal sieht man auch  $\subset$  für Teilmenge und  $\subsetneq$  für echte Teilmenge.

**Definition 2.3** (Leere Menge). Die leere Menge  $\emptyset$  wird charakterisiert durch

$$\forall x : x \notin \emptyset.$$

Kann es mehrere leere Mengen geben, z.B.  $\emptyset$  und  $\{\}$ ?

Für jede Menge  $A$  gilt  $\emptyset \subseteq A$ , also gilt (setze  $A = \emptyset$  bzw.  $A = \{\}$ )

$$\emptyset \subseteq \{\} \wedge \{\} \subseteq \emptyset$$

und somit

$$\emptyset = \{\}.$$

**Definition 2.4** (Vereinigung, Durchschnitt, Komplement, Symmetrische Differenz). Seien  $A, B$  Mengen.

1.  $A \cup B = \{x \mid x \in A \vee x \in B\}$
2.  $A \cap B = \{x \mid x \in A \wedge x \in B\}$
3.  $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$
4.  $A \triangle B := A \setminus B \cup B \setminus A$

*Veranschaulichung.* VENN-Diagramm

*Bemerkung.* Falls man im Kontext einer Grundmenge  $X$  ist, so schreibt man für  $X \setminus A$  häufig auch  $\overline{A}$  oder  $A^c$  oder  $\complement A$ .

**Satz 2.1.** Seien  $A, B, C \subseteq X$  Mengen. Dann gilt:

1.  $(A^c)^c = A$
2.  $(A \cup B)^c = A^c \cap B^c$
3.  $(A \cap B)^c = A^c \cup B^c$
4.  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5.  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

*Beweis.* Folgt sofort aus Satz 1.1. □

*Beispiel.* Für eine Primzahl  $p \in \mathbb{P} = \{p \mid p \text{ eine Primzahl}\}$  sei

$$M_p := \{x \in \mathbb{N} \mid \exists a \in \mathbb{N} : a > 1 \text{ und } x = a \cdot p\}$$

die Menge der „echten Vielfachen“ von  $p$ . Dann gilt

$$\bigcup_{p \in \mathbb{P}} M_p = \mathbb{N} \setminus (\mathbb{P} \cup \{1\}).$$

**Definition 2.5.** Sei  $I$  eine Menge und für jedes  $i \in I$  sei  $M_i$  eine Menge. Dann heißt  $(M_i)_{i \in I}$  eine Familie (ein System) von Mengen. Setze

$$\begin{aligned} \bigcup_{i \in I} M_i &:= \{x \mid \exists i \in I : x \in M_i\}, \\ \bigcap_{i \in I} M_i &:= \{x \mid \forall i \in I : x \in M_i\}. \end{aligned}$$

**Korollar 2.6.** Sei  $(M_i)_{i \in I}$  ein Mengensystem. Dann gilt

$$\begin{aligned} \left( \bigcup_{i \in I} M_i \right)^c &= \bigcap_{i \in I} M_i^c, \\ \left( \bigcap_{i \in I} M_i \right)^c &= \bigcup_{i \in I} M_i^c. \end{aligned}$$

*Beweis.*

$$\begin{aligned} \left( \bigcup_{i \in I} M_i \right)^c &= \{x \mid \exists i \in I : x \in M_i\}^c = \{x \mid \neg(\exists i \in I : x \in M_i)\} \\ &= \{x \mid \forall i \in I : x \notin M_i\} = \{x \mid \forall i \in I : x \in M_i^c\} = \bigcap_{i \in I} M_i^c \end{aligned}$$

□

**Definition 2.7** (Kartesisches Produkt). Seien  $A, B$  Mengen. Dann definiere das kartesische Produkt  $A \times B$  als

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

Falls  $A = B$ , so schreibe für  $A \times A$  auch  $A^2$ . Allgemein definiere für  $n \in \mathbb{N}$

$$A^{n+1} := A^n \times A.$$

*Bemerkung.* Streng genommen wäre

$$\mathbb{R}^3 = \{(x_1, x_2), x_3 \mid x_1, x_2, x_3 \in \mathbb{R}\}.$$

*Beispiel.* Seien  $A = \{a, b, c\}$  und  $B = \{1, 2\}$  zwei Mengen. Dann gilt

$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}.$$

**Definition 2.8** (Potenzmenge). *Sei  $X$  eine Menge. Dann heißt*

$$\mathcal{P}(X) = \{M \text{ Menge} \mid M \subseteq X\}$$

*die Potenzmenge von  $X$ .*

*Beispiele.*

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

**Satz 2.2.** *Sei  $M$  eine  $n$ -elementige Menge. Dann hat  $\mathcal{P}(M)$  genau  $2^n$  Elemente.*

*Beweis.* Sei  $M = \{a_1, a_2, \dots, a_n\}$ . Wenn wir eine Teilmenge bestimmen, treffen wir Entscheidungen:

$a_1$  ... ja oder nein? 2 Möglichkeiten

$a_2$  ... ja oder nein? 2 Möglichkeiten

⋮

$a_n$  ... ja oder nein? 2 Möglichkeiten

Insgesamt haben wir also  $2^n$  Möglichkeiten. □

*Frage.* Sei  $M = \{X \text{ Menge} \mid X \notin X\}$  eine Menge. Gilt  $M \in M$ ?

Falls  $M \in M$ , heißt das (laut Definition)  $M \notin M$  (Widerspruch).

Falls  $M \notin M$ , heißt das (laut Definition)  $M \in M$  (ebenfalls Widerspruch).

Dieses Problem heißt *Russelsche Antinomie* (Anfang 20. Jahrhundert) und führte zur Entwicklung der *axiomatischen Mengenlehre* (nach Zermelo-Fraenkel).

*Bemerkung.* Im ZF-System gibt es ein Axiom („Auswahlaxiom“, Axiom of choice), das etwas umstritten ist. Man spricht von ZFC (ZF mit Auswahlaxiom) bzw. ZF (ZF ohne Auswahlaxiom).

**Definition 2.9.** *Zwei Mengen  $A, B$  heißen disjunkt, falls  $A \cap B = \emptyset$ . In diesem Fall nennt man  $A \cup B$  häufig disjunkte Vereinigung und schreibt  $A \uplus B$ .*



### 3 Relationen

*Beispiele.*

1. Sei  $M = \{\text{Personen im Hörsaal}\}$  eine Menge und  $a, b \in M$ . Wir schreiben  $a K b$ , falls  $a$  die Person  $b$  mit Namen kennt.
2. Betrachte  $\mathbb{Z}, a, b \in \mathbb{Z}$ . Es gilt  $a \leq b$  oder  $b \leq a$ .
3. Sei  $X = \{w, x, y, z\}$  und betrachte  $\mathcal{P}(X)$ . Seien  $A, B \in \mathcal{P}(X)$ . Es gilt  $A \subseteq B$  oder  $B \subseteq A$  oder keines von beiden.
4. Seien  $a, b \in \mathbb{Z}$ . Schreibe  $a \equiv b \pmod{5}$ , falls  $a$  und  $b$  denselben Rest bei Division durch 5 lassen.

**Definition 3.1.** Seien  $M, N$  Mengen. Eine Teilmenge  $R$  von  $M \times N$  heißt Relation zwischen  $M$  und  $N$ . Gilt  $M = N$ , so spricht man von einer Relation auf  $M$ . Statt  $(a, b) \in R$  schreibt man meistens  $a R b$ .

**Definition 3.2** (Eigenschaften von Relationen). Sei  $M$  eine Menge und  $R$  eine Relation auf  $M$ .  $R$  heißt

1. reflexiv, falls  $\forall a \in M : a R a$ .

*Beispiele.* 1, 2, 3, 4 sind reflexiv.

*Gegenbeispiel.*  $<$  auf  $\mathbb{Z}$  ist nicht reflexiv.

2. symmetrisch, falls  $\forall a, b \in M : a R b \rightarrow b R a$ .

*Beispiel.* 4

*Gegenbeispiele.* 1, 2, 3

3. transitiv, falls  $\forall a, b, c \in M : a R b \wedge b R c \rightarrow a R c$ .

*Beispiele.* 2, 3, 4

*Gegenbeispiel.* 1

4. Äquivalenzrelation, falls sie reflexiv, symmetrisch und transitiv ist.

*Beispiel.* 4

*Gegenbeispiele.* 1, 2, 3

5. antisymmetrisch, falls  $\forall a, b \in M : a R b \wedge b R a \rightarrow a = b$ .

*Beispiele.* 2, 3

*Gegenbeispiele.* 1, 4

6. Ordnungsrelation (Partialordnung), falls sie reflexiv, transitiv und antisymmetrisch ist.

*Beispiele.* 2, 3

7. konnex, falls  $\forall a, b \in M : a R b \vee b R a$ .

*Beispiel.* 2

*Gegenbeispiele.* 1, 3, 4

8. Totalordnung, falls sie eine konnexe Partialordnung ist.

*Beispiel.* 2

*Gegenbeispiele.* 1, 3, 4

9. asymmetrisch, falls  $\forall a, b \in M : a R b \rightarrow \neg(b R a)$

*Beispiel.*  $<$

*Gegenbeispiele.* 1, 2, 3, 4

Sei  $R$  eine Relation zwischen  $M$  und  $N$ .  $R$  heißt

1. linkstotal, falls  $\forall a \in M \exists b \in N : a R b$ .

*Beispiele.* 1, 2, 3, 4

*Gegenbeispiel.*  $>$  auf  $\mathbb{N}$

2. rechtstotal, falls  $\forall b \in N \exists a \in M : a R b$ .

3. rechtseindeutig, falls  $\forall a \in M \forall b, c \in N : a R b \wedge a R c \rightarrow b = c$ .

*Beispiel.*  $M = N = \mathbb{R}, R = \{(x, x^2) \mid x \in \mathbb{R}\}$

4. linkseindeutig, falls  $\forall a, b \in M \forall c \in N : a R c \wedge b R c \rightarrow a = b$ .

*Beispiel.*  $M = N = \mathbb{R}, R = \{(x, x^3) \mid x \in \mathbb{R}\}$

5. eineindeutig, falls sie linkseindeutig und rechtseindeutig ist.

*Beispiel.*  $M = N = \mathbb{R}, R = \{(x, x^3) \mid x \in \mathbb{R}\}$

**Definition 3.3.** Seien  $M, N$  zwei Mengen. Eine Funktion  $f$  von  $M$  nach  $N$  ist eine linkstotale, rechts-eindeutige Relation zwischen  $M$  und  $N$ , das heißt

$$\forall x \in M \exists! y \in N : (x, y) \in f.$$

*Schreibweise:*

$$\begin{aligned} f : M &\rightarrow N \\ x &\mapsto f(x) \end{aligned}$$

$M$  heißt Definitionsmenge,  $N$  heißt Wertevorrat.

**Definition 3.4.** Eine Funktion  $f$  heißt

- surjektiv, wenn sie rechtstotal ist, das heißt

$$\forall y \in N \exists x \in M : f(x) = y.$$

- injektiv, wenn sie linkseindeutig ist, das heißt

$$\forall x_1, x_2 \in M : f(x_1) = f(x_2) \rightarrow x_1 = x_2.$$

- bijektiv, wenn sie injektiv und surjektiv ist.

### 3.1 Äquivalenzrelationen

Zu Beispiel 4: Wir können  $\mathbb{Z}$  in 5 Mengen einteilen:

$$[0] := \{\dots, -10, -5, 0, 5, 10, \dots\} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{5}\}$$

$$[1] := \{\dots, -9, -4, 1, 6, 11, \dots\} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{5}\}$$

$$[2] := \{\dots, -8, -3, 2, 7, 12, \dots\} = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{5}\}$$

$$[3] := \{\dots, -7, -2, 3, 8, 13, \dots\} = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{5}\}$$

$$[4] := \{\dots, -6, -1, 4, 9, 14, \dots\} = \{x \in \mathbb{Z} \mid x \equiv 4 \pmod{5}\}$$

Diese 5 Mengen sind paarweise disjunkt (d.h. je zwei haben keinen Durchschnitt). Die Vereinigung ist ganz  $\mathbb{Z}$ . Man spricht von einer „Klasseneinteilung“.

**Definition 3.5.** Sei  $M$  eine Menge,  $\sim$  eine Äquivalenzrelation auf  $M$ . Dann heißt für  $a \in M$

$$[a]_{\sim} := \{x \in M \mid a \sim x\}$$

die Äquivalenzklasse von  $a$  unter  $\sim$ . Jedes  $x \in [a]_{\sim}$  heißt ein Repräsentant von  $[a]_{\sim}$ .

**Satz 3.1** (Äquivalenzrelationen und Klasseneinteilung). Sei  $\sim$  eine Äquivalenzrelation auf  $M$  und setze  $M/\sim$  als die Menge aller Äquivalenzklassen

$$M/\sim = \{[a]_{\sim} \mid a \in M\}$$

Dann sind alle Äquivalenzklassen nicht leer, paarweise disjunkt, und ihre Vereinigung gleich  $M$ .

*Beweis.*

1. Sei  $[a]_{\sim} \in M/\sim$ .

Es gilt  $a \sim a$  (weil  $\sim$  reflexiv ist), also  $a \in [a]_{\sim}$ , somit  $[a]_{\sim} \neq \emptyset$ .

2. Seien  $[a]_{\sim}, [b]_{\sim}$  zwei Äquivalenzklassen.

Entweder gilt  $[a]_{\sim} \cap [b]_{\sim} = \emptyset$  (dann ist alles in Ordnung) oder es gibt ein  $c \in [a]_{\sim} \cap [b]_{\sim}$ . Dann gilt

$$a \sim c$$

und

$$b \sim c \Rightarrow c \sim b \text{ weil symmetrisch}$$

und somit (weil transitiv)  $a \sim b$  und daher

$$[a]_{\sim} = [b]_{\sim}.$$

3. Da  $[a]_{\sim} \subseteq M$  (lt. Def.) gilt

$$\bigcup_{a \in M} [a]_{\sim} \subseteq M.$$

Da  $\forall a \in M : a \in [a]_{\sim}$  folgt

$$M \subseteq \bigcup_{a \in M} [a]_{\sim}$$

und somit

$$M = \bigcup_{a \in M} [a]_{\sim}.$$

□

## 3.2 Ordnungsrelationen

Zur Erinnerung:  $\leq$  heißt *Partialordnung* auf  $M$ , falls:

1.  $\forall a : a \leq a$  (reflexiv)
2.  $\forall a, b : a \leq b \wedge b \leq a \rightarrow a = b$  (antisymmetrisch)
3.  $\forall a, b, c : a \leq b \wedge b \leq c \rightarrow a \leq c$  (transitiv)

**Definition 3.6.** Sei  $M$  eine Menge,  $\leq$  eine Partialordnung auf  $M$  und  $x \in M$ .

1.  $x$  heißt kleinstes Element von  $M$ , falls

$$\forall a \in M : x \leq a.$$

2.  $x$  heißt größtes Element von  $M$ , falls

$$\forall a \in M : a \leq x.$$

3.  $x$  heißt minimales Element von  $M$ , falls

$$\forall a \in M : a \leq x \rightarrow a = x.$$

4.  $x$  heißt maximales Element von  $M$ , falls

$$\forall a \in M : x \leq a \rightarrow x = a.$$

*Beispiele.*

- Sei  $M = \mathcal{P}(\{a, b, c\})$ . Dann ist  $\emptyset$  sowohl kleinstes Element als auch minimales Element, und  $\{a, b, c\}$  ist größtes Element und maximales Element.
- Sei  $M = \mathcal{P}(\{a, b, c\}) \setminus \{\{a, b, c\}\}$ . Dann ist wieder  $\emptyset$  kleinstes Element und minimales Element. Es gibt allerdings kein größtes Element, dafür aber die drei maximalen Elemente  $\{a, b\}$ ,  $\{a, c\}$ ,  $\{b, c\}$ .

*Veranschaulichung.* Hasse-Diagramm

**Proposition 3.7.** Sei  $M$  eine partialgeordnete Menge. Dann enthält  $M$  höchstens ein kleinstes Element.

*Beweis.* Seien  $x, y$  zwei kleinste Elemente. Da  $x$  kleinstes Element ist, muss  $x \leq y$  gelten. Weil  $y$  kleinstes Element ist, muss umgekehrt  $y \leq x$  gelten. Aufgrund der Antisymmetrie von  $\leq$  gilt daher  $x = y$ . Es kann also nicht mehrere kleinste Elemente geben.  $\square$

*Frage.* Sei  $M$  eine Menge, die nur ein maximales Element enthält. Ist dieses ein größtes Element?

Die Antwort ist Nein! Ein Gegenbeispiel wäre etwa die Menge

$$M = \{\{-1\}, \emptyset, \{0\}, \{0, 1\}, \{0, 1, 2\}, \dots\}.$$

mit der  $\subseteq$ -Relation. Hier ist  $\{-1\}$  das einzige maximale Element, es gibt aber kein größtes Element. (Für eine endliche Menge stimmt die Aussage.)

**Definition 3.8.** Sei  $M$  eine partiell geordnete Menge und  $N \subseteq M$ .

1. Ein Element  $x \in M$  heißt obere Schranke von  $N$ , falls

$$\forall y \in N : y \leq x.$$

2. Falls  $N$  eine obere Schranke besitzt, so heißt  $N$  nach oben beschränkt.

3. Ein Element  $x \in M$  heißt untere Schranke von  $N$ , falls

$$\forall y \in N : x \leq y.$$

4. Falls  $N$  eine untere Schranke besitzt, so heißt  $N$  nach unten beschränkt.

*Beispiel.* Sei  $M = \mathbb{Q}$  und  $N = \{x \in \mathbb{Q} \mid x^2 < 2\}$ . Dann sind z.B. 4, 100, 2005 obere Schranken von  $N$  ( $\sqrt{2}$  wurde disqualifiziert, weil  $\sqrt{2} \notin \mathbb{Q}$ ).  $-2, -4, -1285$  sind untere Schranken von  $N$ .

**Definition 3.9.** Sei  $M$  eine Menge,  $\leq$  eine Partialordnung und  $N \subseteq M$ .

1. Falls die Menge der oberen Schranken von  $N$  ein kleinstes Element besitzt, so heißt dieses das Supremum von  $N$ ; schreibe  $\sup N$ .
2. Falls die Menge der unteren Schranken von  $N$  ein größtes Element besitzt, so heißt dieses das Infimum von  $N$ ; schreibe  $\inf N$ .

*Beispiele.*

- Sei wie vorher  $M = \mathbb{Q}$  und  $N = \{x \in \mathbb{Q} \mid x^2 < 2\}$ . Die Menge der oberen Schranken ist

$$O = \{y \in \mathbb{Q} \mid y > \sqrt{2}\}$$

und enthält kein kleinstes Element. Somit gibt es kein Supremum von  $N$ .

- $M = \mathbb{R}$  und  $N = \{x \in \mathbb{Q} \mid x^2 < 2\}$ . Dann ist  $\sup N = \sqrt{2}$ .

**Satz 3.2** (Lemma von Zorn). Sei  $M$  eine partialgeordnete Menge mit folgender Eigenschaft: Jede Kette  $K \subseteq M$  (d.h.  $\forall a, b \in K : a \leq b \vee b \leq a$ ) besitzt eine obere Schranke in  $M$ . Dann besitzt  $M$  ein maximales Element.

(Leider hier ohne Beweis.)

Das Zorn'sche Lemma ist äquivalent zum Auswahlaxiom und geht im Wesentlichen auf Zermelo zurück.

**Definition 3.10.** Sei  $M$  eine Menge und  $\leq$  eine Totalordnung.  $\leq$  heißt eine Wohlordnung, wenn jede nichtleere Teilmenge  $N \subseteq M$  ein kleinstes Element besitzt.

*Beispiele.*

- $\mathbb{N}$  ist wohlgeordnet.
- $\mathbb{Z}$  ist nicht wohlgeordnet (unter der „gewöhnlichen“  $\leq$ -Relation).
- $\mathbb{Z}$  ist wohlgeordnet unter der neuen Ordnung  $\sqsubseteq$  mit

$$0 \sqsubseteq 1 \sqsubseteq -1 \sqsubseteq 2 \sqsubseteq -2 \sqsubseteq 3 \sqsubseteq -3 \sqsubseteq \dots$$

**Satz 3.3** (Wohlordnungssatz). Sei  $M$  eine Menge. Dann gibt es eine Wohlordnung auf  $M$ .

(Leider hier auch ohne Beweis.)

Der Wohlordnungssatz ist äquivalent zum Lemma von Zorn und zum Auswahlaxiom.



## 4 Funktionen

Zur Erinnerung: Seien  $M, N$  zwei Mengen. Eine Funktion

$$f : M \rightarrow N$$

ordnet jedem Element  $x \in M$  genau ein Element  $y \in N$  zu.

$$y = f(x) \quad \text{oder} \quad x \mapsto y$$

*Beispiele.*

1.  $f : \mathbb{R} \rightarrow \mathbb{R}; x \mapsto x^2$  ist eine Funktion.  
 nicht injektiv:  $2 \neq -2$ , aber  $f(-2) = 4 = f(2)$   
 nicht surjektiv:  $\nexists x \in \mathbb{R} : f(x) = -1$
2.  $f : \mathbb{R} \rightarrow \mathbb{R}; x \mapsto \pm\sqrt{x}$  ist keine Funktion.
3.  $f : \mathbb{R} \rightarrow \mathbb{R}; x \mapsto \frac{1}{x}$  ist keine Funktion (weil für 0 nicht definiert).
4.  $f : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}; x \mapsto \frac{1}{x}$  ist eine Funktion.  
 injektiv  
 nicht surjektiv:  $\nexists x \in \mathbb{R} : f(x) = 0$
5.  $f : [0, \infty) \rightarrow \mathbb{R}; x \mapsto$  Einkommenssteuer, die bezahlen ist, wenn das steuerpflichtige Jahreinkommen  $x$  beträgt (steht im BGBI)  
 ist eine Funktion.
6.  $f : \mathbb{R} \rightarrow \mathbb{R}; x \mapsto \begin{cases} 1 & \text{für } x \in \mathbb{Q} \\ 0 & \text{für } x \notin \mathbb{Q} \end{cases}$  ist eine Funktion.  
 nicht injektiv („irreparabel“)  
 nicht surjektiv

**Definition 4.1.** Sei  $f : M \rightarrow N$ .

1. Für  $A \subseteq M$  definiere

$$f(A) := \{f(x) \mid x \in A\}$$

als das Bild von  $A$  unter  $f$ .

2. Für  $B \subseteq N$  definiere

$$f^{-1}(B) := \{x \in M \mid f(x) \in B\}$$

als das Urbild von  $B$  unter  $f$ .

*Beispiel.* Sei  $f : \mathbb{R} \rightarrow \mathbb{R}; x \mapsto x^2$ .

$$f([0; 2]) = [0; 4]$$

$$f(\mathbb{R}) = [0; \infty) = \{x \in \mathbb{R} \mid x \geq 0\}$$

$$f^{-1}(\{4\}) = \{-2, 2\}$$

$$f^{-1}([0; 4]) = [-2; 2]$$

$$f^{-1}([-3; -1]) = \emptyset$$

*Bemerkung.* Sei  $f : M \rightarrow N$  eine Funktion. Es gilt:

1.  $f$  ist injektiv  $\Leftrightarrow \forall b \in N : f^{-1}(\{b\})$  hat höchstens ein Element.
2.  $f$  ist surjektiv  $\Leftrightarrow \forall b \in N : f^{-1}(\{b\})$  hat mindestens ein Element.
3.  $f$  ist bijektiv  $\Leftrightarrow \forall b \in N : f^{-1}(\{b\})$  hat genau ein Element.

**Definition 4.2.** Seien  $f : M \rightarrow N$  und  $g : N \rightarrow P$ . Dann definiere die Verknüpfung  $f \circ g : M \rightarrow P$  durch

$$(g \circ f)(x) = g(f(x)).$$

*Beispiel.* Seien  $f : \mathbb{R} \rightarrow \mathbb{R}; f(x) = x^2$  und  $g : \mathbb{R} \rightarrow \mathbb{R}; g(x) = x + 6$ . Dann gilt

$$(g \circ f)(x) = g(f(x)) = f(x) + 6 = x^2 + 6$$

$$(f \circ g)(x) = f(g(x)) = f(x + 6) = (x + 6)^2 = x^2 + 12x + 36.$$

*Bemerkung.* Zwei Funktionen  $f : A \rightarrow B$  und  $g : C \rightarrow D$  werden genau dann als gleich betrachtet, wenn

1.  $A = C$ ,
2.  $B = D$ ,
3.  $\forall x \in A : f(x) = g(x)$ .

**Axiom** (Auswahlaxiom). Sei  $(M_\lambda)_{\lambda \in J}$  ein System nichtleerer Mengen. Dann gibt es eine Funktion

$$f : J \rightarrow \bigcup_{\lambda \in J} M_\lambda,$$

sodass

$$\forall \lambda \in J : f(\lambda) \in M_\lambda$$

gilt.

**Definition 4.3.** Sei  $M$  eine Menge. Dann ist die identische Funktion  $\text{id}_M$  auf  $M$  die Funktion

$$\text{id}_M : M \rightarrow M; x \mapsto x.$$

**Satz 4.1** (Charakterisierung von injektiven und surjektiven Funktionen). Sei  $f : M \rightarrow N$ , wobei  $M \neq \emptyset$ .

1.  $f$  ist injektiv  $\Leftrightarrow$  Es gibt eine Funktion  $g : N \rightarrow M$ , sodass

$$g \circ f = \text{id}_M.$$

2.  $f$  ist surjektiv  $\Leftrightarrow$  Es gibt eine Funktion  $g : N \rightarrow M$ , sodass

$$f \circ g = \text{id}_N.$$

3.  $f$  ist bijektiv  $\Leftrightarrow$  Es gibt eine Funktion  $g : N \rightarrow M$ , sodass

$$g \circ f = \text{id}_M \text{ und } f \circ g = \text{id}_N.$$

*Beweis.*

1. „ $\Leftarrow$ “: Seien  $x_1, x_2 \in M$  mit  $f(x_1) = f(x_2)$ . Dann gilt

$$x_1 = \text{id}_M(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = \text{id}_M(x_2) = x_2$$

und somit ist  $f$  injektiv.

„ $\Rightarrow$ “: Es gibt ein  $z \in M$ . Dieses fixieren wir. Sei weiters  $y \in N$ . Falls  $f^{-1}(\{y\}) = \{x\}$  für ein  $x \in M$ , so setze

$$g(y) = x.$$

Falls  $f^{-1}(\{y\}) = \emptyset$ , so setze

$$g(y) = z.$$

(Anders kann  $f^{-1}(\{y\})$  nicht aussehen, da  $f$  injektiv ist.) Nun ist  $g \circ f$  eine Funktion von  $M$  nach  $M$  mit

$$(g \circ f)(x) = g(y) = x = \text{id}_M(x)$$

für alle  $x \in M$ , somit gilt  $g \circ f = \text{id}_M$ .

2. „ $\Leftarrow$ “: Übungsblatt

„ $\Rightarrow$ “: Es muss  $g$  so gewählt werden, dass

$$g(y) \in f^{-1}(\{y\})$$

für alle  $y \in N$ , was auch hinreichend ist. Dieses existiert genau durch das Auswahlaxiom.

□

**Satz 4.2.** Aus dem Wohlordnungssatz folgt das Auswahlaxiom.

*Beweis.* Die Menge

$$M := \bigcup_{\lambda \in J} M_\lambda$$

lässt sich wohlordnen. Dadurch hat für jedes  $\lambda \in J$  die Menge  $M_\lambda$  als Teilmenge von  $M$  ein kleinstes Element  $\min M_\lambda$ . Setze  $f : J \rightarrow M$  mit  $\lambda \mapsto \min M_\lambda$ . Das ist die Auswahlfunktion. □

**Definition 4.4.** Sei  $f : M \rightarrow N$  injektiv. Dann definiere die Umkehrfunktion

$$f^{-1} : f(M) \rightarrow M$$

durch

$$f^{-1}(y) = x, \text{ falls } \underbrace{f^{-1}(\{y\})}_{\text{„Urbild“}} = \{x\}.$$

*Beispiel.* Sei

$$f : [0, \infty) \rightarrow \mathbb{R}; x \mapsto x^2,$$

dann ist die Umkehrfunktion

$$f^{-1} : [0, \infty) \rightarrow [0, \infty); y \mapsto \sqrt{y}.$$

*Bemerkung.* Falls  $f$  bijektiv ist, so ist  $f^{-1}$  genau das  $g$  aus Satz 4.1.

*Bemerkung.* Das Symbol  $f^{-1}$  hat zwei verschiedene Bedeutungen:

- $f^{-1}(B)$  ist für jede *Teilmenge*  $B$  des Wertevorrats definiert und ist wieder eine (möglicherweise leere) *Menge*.
- $f^{-1}(y)$  (die Umkehrfunktion aus Definition 4.4) ist nur für injektive Funktionen und *Elemente*  $y$  aus dem Bild von  $f$  definiert und ist ein *Element* aus der Definitionsmenge.

**Satz 4.3.** Sei  $f : M \rightarrow N$ .

1.  $\forall A, B \subseteq M : f(A \cup B) = f(A) \cup f(B)$
2.  $\forall A, B \subseteq M : f(A \cap B) \subseteq f(A) \cap f(B)$   
(Im Allgemeinen gilt nicht Gleichheit.)
3.  $\forall C, D \subseteq N : f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$
4.  $\forall C, D \subseteq N : f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$

**Definition 4.5** (Einschränkung von Funktionen). Sei  $f : M \rightarrow N$  eine Abbildung (Funktion) und  $A \subseteq M$ . Dann heißt

$$f|_A : A \rightarrow N, x \mapsto f(x)$$

die Einschränkung von  $f$  auf  $A$ .

*Bemerkung.*  $f|_A$  ist im Wesentlichen dasselbe wie  $f$ , nur eben mit „kleinerem“ Definitionsbereich.

## 5 Einführung in algebraische Strukturen

### 5.1 Gruppen

**Definition 5.1.** Sei  $G$  eine Menge und  $\diamond : G \times G \rightarrow G, (a, b) \mapsto a \diamond b$ . Dann heißt  $\diamond$  eine innere Verknüpfung auf  $G$ .

(G1) Falls das Assoziativgesetz

$$\forall a, b, c \in G : a \diamond (b \diamond c) = (a \diamond b) \diamond c$$

gilt, so heißt  $(G, \diamond)$  eine Halbgruppe.

(G2) Falls zusätzlich ein  $e \in G$  existiert, sodass für alle  $a \in G$

$$e \diamond a = a \diamond e = a$$

gilt, so heißt  $(G, \diamond, e)$  ein Monoid.  $e$  heißt das neutrale Element.

(G3) Falls zusätzlich

$$\forall a \in G \exists b \in G : b \diamond a = a \diamond b = e$$

gilt, so heißt  $(G, \diamond, e)$  eine Gruppe.

(G4) Falls zusätzlich das Kommutativgesetz

$$\forall a, b \in G : a \diamond b = b \diamond a$$

gilt, so heißt  $(G, \diamond, e)$  eine kommutative Gruppe (oder abelsche Gruppe).

(Niels Abel war ein norwegischer Mathematiker, 1802–1829.)

Beispiele.

1.  $(\mathbb{Z}, \cdot)$ : assoziativ, 1 ist neutrales Element, (G3) nicht erfüllt, somit (*kommutatives*) Monoid
2.  $(\mathbb{Z}, +)$ : assoziativ, 0 ist neutrales Element,  $-a$  inverses Element von  $a$ , kommutativ, somit *kommutative Gruppe*
3.  $(\mathbb{N}, +)$ : *Halbgruppe* (neutrales Element 0 nicht in  $\mathbb{N}$  enthalten)
4.  $(\mathbb{Q}, +), (\mathbb{R}, +)$ : *kommutative Gruppen*
5.  $(\mathbb{Q}, \cdot)$ : *kommutatives Monoid*, aber

$$\nexists a \in \mathbb{Q} : a \cdot 0 = 0 \cdot a = 1.$$

6.  $(\mathbb{Q} \setminus \{0\}, \cdot)$ : *abelsche Gruppe*. Wir müssen überprüfen, dass

$$\forall a, b \in \mathbb{Q} \setminus \{0\} : a \cdot b \in \mathbb{Q} \setminus \{0\}.$$

7. Sei  $M$  eine Menge und  $H$  die Funktionenmenge

$$H := \{f : M \rightarrow M\}.$$

Betrachte nun  $(H, \circ)$ , wobei  $\circ$  die Hintereinanderausführung von Funktionen bedeutet. Es gilt

$$\forall x \in M : (f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x).$$

Somit ist  $(H, \circ, \text{id}_M)$  ein *Monoid*.

8. Sei  $M$  eine Menge und  $G = \{f : M \rightarrow M \mid f \text{ ist bijektiv}\}$ . Um zu zeigen, dass  $(G, \circ, \text{id}_M)$  eine Gruppe ist, müssen wir zeigen:

$$\forall f, g \text{ bijektiv} : f \circ g \text{ bijektiv}$$

$$\forall f \text{ bijektiv} : g \text{ aus Satz 4.1 ist bijektiv.}$$

9.  $\equiv \pmod{m}$  ist eine Äquivalenzrelation auf  $\mathbb{Z}$ . Wir betrachten die Menge der Äquivalenzklassen („Restklassen“) und bezeichnen sie mit  $\mathbb{Z}_m$  (oder  $\mathbb{Z}/m\mathbb{Z}$ ).

*Beispiel.*

$$[0] = [5] = \dots$$

$$[1] = [6] = \dots$$

$$[2] = [7] = \dots$$

$$[3] = [8] = \dots$$

$$[4] = [9] = \dots$$

Definiere eine Addition auf der Restklasse:

$$[a] + [b] = [a + b]$$

Hier müssen wir allerdings aufpassen!

*Beispiel.*

$$[1] + [4] = [4 + 1] = [5]$$

$$[6] + [9] = [6 + 9] = [15]$$

Wir müssen zeigen, dass die Addition *wohldefiniert* ist.

*Lemma 5.2.* Seien  $a, b, c, d, m$  ganze Zahlen mit

$$a \equiv c \pmod{m}$$

$$b \equiv d \pmod{m}.$$

Dann gilt

$$a + b \equiv c + d \pmod{m}$$

$$a \cdot b \equiv c \cdot d \pmod{m}.$$

*Beweis.*

$$a \equiv c \pmod{m} \Leftrightarrow a - c \text{ ist durch } m \text{ teilbar.}$$

$$b \equiv d \pmod{m} \Leftrightarrow b - d \text{ ist durch } m \text{ teilbar.}$$

Addieren wir diese Ergebnisse, erhalten wir, dass auch  $(a + b) - (c + d)$  durch  $m$  teilbar ist. Das bedeutet

$$a + b \equiv c + d \pmod{m}.$$

Für die Multiplikation gilt

$$a \cdot b - c \cdot d = a \cdot b - c \cdot b + c \cdot b - c \cdot d = \underbrace{(a - c) \cdot b}_{\text{durch } m \text{ teilbar}} + \underbrace{(b - d) \cdot c}_{\text{durch } m \text{ teilbar}} \text{ ist durch } m \text{ teilbar.}$$

Somit gilt

$$a \cdot b \equiv c \cdot d \pmod{m}.$$

□

In unserem Fall bedeutet das:

$$\left. \begin{array}{l} [a] = [c] \Rightarrow a \equiv c \pmod{m} \\ [b] = [d] \Rightarrow b \equiv d \pmod{m} \end{array} \right\} \xrightarrow{\text{Lemma}} a + b \equiv c + d \pmod{m}$$

Somit gilt

$$[a + b] = [c + d]$$

und die Verknüpfung ist wohldefiniert.

Außerdem gilt das *Assoziativgesetz*:

$$[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)] \stackrel{\text{Ass.ges. in } \mathbb{Z}}{=} [(a + b) + c] = ([a] + [b]) + [c]$$

Weiters ist  $[0]$  *neutrales Element* und  $[-a]$  das *inverse Element* zu  $[a]$ .

Ebenso gilt das *Kommutativgesetz*:

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

Somit ist  $(\mathbb{Z}_m, +)$  eine *kommutative Gruppe*.

**Satz 5.1.** Sei  $(G, \diamond)$  eine Gruppe und  $a, b \in G$ . Dann gibt es genau ein  $x \in G$  und genau ein  $y \in G$ , sodass

$$a \diamond x = b$$

$$y \diamond a = b.$$

*Beweis.* Sei  $c \diamond a = a \diamond c = e$  (existiert wegen (G3)). Nehmen wir an, es gäbe eine Lösung  $x \in G$  der Gleichung  $a \diamond x = b$ . Dann gilt

$$\begin{aligned} a \diamond x &= b \\ \Rightarrow c \diamond (a \diamond x) &= c \diamond b \\ \Rightarrow (c \diamond a) \diamond x &= c \diamond b \\ \Rightarrow e \diamond x &= c \diamond b \\ \Rightarrow x &= c \diamond b. \end{aligned}$$

Es kann also höchstens eine Lösung geben. Andererseits ist  $a \diamond (c \diamond b) = (a \diamond c) \diamond b = e \diamond b = b$ , also  $x = c \diamond b$  tatsächlich eine Lösung.

Die zweite Aussage über die Gleichung  $y \diamond a = b$  wird analog bewiesen.  $\square$

**Korollar 5.3.** Sei  $(G, \diamond, e)$  eine Gruppe. Dann ist das neutrale Element  $e$  eindeutig bestimmt, d.h.

$$\forall f \in G : (\forall a \in G : f \diamond a = a \diamond f = a) \rightarrow f = e$$

*Beweis.* Die Gleichungen  $x \diamond a = a$  und  $a \diamond x = a$  haben eindeutige Lösungen. Nach Definition ist  $e$  eine Lösung, und damit die einzige.  $\square$

**Korollar 5.4.** Sei  $(G, \diamond, e)$  eine Gruppe und  $a \in G$ . Dann gibt es genau ein Element  $b \in G$  mit  $b \diamond a = e$ .

*Beweis.* Die Gleichung  $x \diamond a = e$  besitzt genau eine Lösung.  $\square$

**Definition 5.5.** Sei  $(G, \diamond, e)$  eine Gruppe und  $a \in G$ . Das eindeutig bestimmte Element  $b$  mit

$$b \diamond a = a \diamond b = e$$

heißt das zu  $a$  inverse Element und wird mit  $a^{-1}$  bezeichnet.

**Definition 5.6.** Sei  $(G, \diamond)$  eine Gruppe und  $H \subseteq G$  nicht leer. Dann heißt  $H$  eine Untergruppe von  $G$ , falls:

1.  $\forall a, b \in H : a \diamond b \in H$
2.  $\forall a \in H : a^{-1} \in H$

*Beispiele.*

- $(\mathbb{Z}, +)$  ist eine Untergruppe von  $(\mathbb{Q}, +)$ .
- Sei  $G = (\mathbb{Z}, +)$  und  $m \in \mathbb{Z}$ . Dann ist

$$H = m\mathbb{Z} := \{m \cdot a \mid a \in \mathbb{Z}\}$$

(die Menge der Vielfachen von  $m$ ) eine Untergruppe von  $(\mathbb{Z}, +)$ .

**Definition 5.7.** Sei  $(G, \diamond, e)$  eine Gruppe. Dann heißen  $\{e\}$  und  $G$  die trivialen Untergruppen von  $G$ .

**Proposition 5.8.** Sei  $H$  eine Untergruppe von  $(G, \diamond, e)$ . Dann ist  $(H, \diamond|_{H \times H}, e)$  ebenfalls eine Gruppe.

*Beweis.*

- $\diamond|_{H \times H} : H \times H \rightarrow H$  ist wahr wegen der Eigenschaft 1 in Definition 5.6.
- Assoziativgesetz: Wir wissen:

$$\forall a, b, c \in G : (a \diamond b) \diamond c = a \diamond (b \diamond c)$$

Diese Eigenschaft wird sozusagen wegen  $H \subseteq G$  „ererb“:

$$\forall a, b, c \in H : (a \diamond b) \diamond c = a \diamond (b \diamond c)$$

- Da  $H \neq \emptyset$  gibt es ein  $a \in H$ . Dann ist wegen der Eigenschaft 2 in Definition 5.6 auch  $a^{-1} \in H$ . Wegen Eigenschaft 1 gilt somit  $e = a \diamond a^{-1} \in H$ . Trivialerweise gilt

$$\forall b \in H : e \diamond b = b \diamond e = e.$$

- Wegen Eigenschaft 2 ub Definition 5.6 gilt für  $a \in H$  auch  $a^{-1} \in H$ , also hat  $a$  ein inverses Element in  $H$ .

□

**Proposition 5.9.** Sei  $(G, \diamond, e)$  eine Gruppe und  $a, b \in G$ . Dann gilt

1.  $(a^{-1})^{-1} = a$ ,
2.  $(a \diamond b)^{-1} = b^{-1} \diamond a^{-1}$ .

*Beweis.*

1. Wir wissen  $a^{-1} \diamond a = a \diamond a^{-1} = e$ .  $a$  „kann alles“, was das Inverse von  $a^{-1}$  können muss. Da  $a^{-1}$  nur ein Inverses hat, folgt

$$a = (a^{-1})^{-1}.$$

2. Es gilt

$$(a \diamond b) \diamond (b^{-1} \diamond a^{-1}) \stackrel{\text{Ass.ges.}}{=} a \diamond (b \diamond b^{-1}) \diamond a^{-1} = (a \diamond e) \diamond a^{-1} = a \diamond a^{-1} = e.$$

Umgekehrt gilt ebenfalls

$$(b^{-1} \diamond a^{-1}) \diamond (a \diamond b) = \dots = e.$$

□

**Notation 5.10.** Die Verknüpfung in abelschen Gruppen schreibt man meist mit  $+$ , das neutrale Element mit  $0$  und das zu  $a$  inverse Element mit  $-a$ . Statt  $b + (-a)$  schreibt man auch  $b - a$ .

Die Rechenregeln sagen:

- $-(-a) = a$
- $-(a + b) = -b - a = -a - b$

**Satz 5.2.** Sei  $(G, \diamond)$  eine Halbgruppe, sodass:

- (1)  $\exists e \in G \forall a \in G : e \diamond a = a$  („linksneutral“)
- (2)  $\forall a \in G \exists b \in G : b \diamond a = e$  („linksinvers“)

Dann ist  $(G, \diamond, e)$  eine Gruppe.

*Beweis.* Seien  $a, b, c \in G$  mit

- (3)  $b \diamond a = e$
- (4)  $c \diamond b = e$

Dann gilt

$$(5) \quad a \diamond b \stackrel{(1)}{=} e \diamond (a \diamond b) \stackrel{(4)}{=} (c \diamond b) \diamond (a \diamond b) \stackrel{\text{Ass.ges.}}{=} c \diamond (b \diamond a) \diamond b \stackrel{(3)}{=} c \diamond (e \diamond b) \stackrel{(1)}{=} c \diamond b \stackrel{(4)}{=} e.$$

Weiters gilt

$$(6) \quad a \diamond e \stackrel{(2)}{=} a \diamond (b \diamond a) \stackrel{\text{Ass.ges.}}{=} (a \diamond b) \diamond a \stackrel{(5)}{=} e \diamond a \stackrel{(1)}{=} a.$$

Also:

$$\begin{aligned} \forall a \in G : e \diamond a &= a \diamond e = a, \\ \forall a \in G \exists b \in G : b \diamond a &= a \diamond b = e. \end{aligned}$$

Somit ist  $(G, \diamond, e)$  eine Gruppe. □

*Bemerkung.* Dieser Satz erleichtert die Überprüfung, ob irgendetwas eine Gruppe ist.

## 5.2 Ringe

**Definition 5.11 (Ring).** Sei  $R$  eine nichtleere Menge, und seien

$$\begin{aligned} + : R \times R &\rightarrow R \\ \cdot : R \times R &\rightarrow R \end{aligned}$$

zwei innere Verknüpfungen. Falls

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

(R2)  $(R, \cdot)$  eine Halbgruppe ist und

(R3)  $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c$  und  $(a + b) \cdot c = a \cdot c + b \cdot c$  (das Distributivgesetz)

gilt, dann heißt  $(R, +, \cdot, 0)$  ein Ring.

Falls weiters

(R4)  $(R, \cdot, 1)$  ist ein Monoid

gilt, so heißt  $(R, +, \cdot, 0, 1)$  ein Ring mit Eins („unitary ring“).

Ein kommutativer Ring ist ein Ring, dessen Multiplikation kommutativ ist, d.h.

(R5)  $\forall a, b \in R : a \cdot b = b \cdot a$ .

Beispiele.

- $(\mathbb{R}, +, \cdot, 0, 1)$  ist ein kommutativer Ring mit 1.
- $(\mathbb{Q}, +, \cdot, 0, 1)$  ist ein kommutativer Ring mit 1.
- $(\mathbb{Z}, +, \cdot, 0, 1)$  ist ein kommutativer Ring mit 1.
- $(\mathbb{Z}_m, +, \cdot, [0], [1])$  ist ein kommutativer Ring mit 1.

**Proposition 5.12** (Rechenregeln für Ringe). Sei  $(R, +, \cdot, 0)$  ein Ring,  $a, b \in R$ . Dann gilt

1.  $0 \cdot a = 0$ ,
2.  $(-a) \cdot b = -(a \cdot b)$ ,
3.  $a \cdot 0 = 0$ ,
4.  $a \cdot (-b) = -(a \cdot b)$ .

Beweis.

1. Es gilt

$$0 \cdot a + 0 \cdot a \stackrel{\text{Distr.ges.}}{=} (0 + 0) \cdot a = 0 \cdot a.$$

Andererseits gilt

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

Laut Satz 5.1 hat die Gleichung  $0 \cdot a + x = 0 \cdot a$  genau eine Lösung. Also muss

$$0 \cdot a = 0$$

gelten.

2. Es gilt

$$(-a) \cdot b + a \cdot b \stackrel{\text{Distr.ges.}}{=} (-a + a) \cdot b = 0 \cdot b \stackrel{1}{=} 0.$$

Da  $a \cdot b$  nur ein Negatives haben kann, ist es  $(-a) \cdot b$ .

3. Analog.
4. Analog.

□

Frage. Sei  $R$  ein kommutativer Ring mit Eins. Gilt

$$\forall a, b \in R : a \cdot b = 0 \rightarrow a = 0 \vee b = 0?$$

Schauen wir  $\mathbb{Z}_4$  an (bei Restklassen schreibt man  $\bar{a}$  statt  $[a]$ ):

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

In diesem Fall gilt also  $\bar{2} \cdot \bar{2} = \bar{0}$ , die Antwort lautet somit Nein.

**Definition 5.13.** Ein Ring  $R$  heißt nullteilerfrei, wenn

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

gilt.

Beispiele.  $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$

**Lemma 5.14.** Sei  $p$  eine Primzahl. Dann ist  $\mathbb{Z}_p$  ein nullteilerfreier Ring.

Beweis. Wir nehmen

$$\exists \bar{a}, \bar{b} \in \mathbb{Z}_p : \bar{a} \cdot \bar{b} = \bar{0} \wedge \bar{a} \neq \bar{0} \wedge \bar{b} \neq \bar{0}$$

an. Das heißt, dass  $a \cdot p$  ein Vielfaches von  $p$  ist, aber weder  $a$  noch  $b$  ein Vielfaches von  $p$  sind. Das ist mit dem uns in der Schule eingetrichterten Verständnis von Primzahlen nicht verträglich. (Widerspruch) □

**Definition 5.15.** Sei  $R$  ein kommutativer Ring mit Eins und  $\leq$  eine Totalordnung.  $(R, \leq)$  heißt geordneter Ring, falls:

$$(OR1) \forall a, b, c \in R : a \leq b \rightarrow a + c \leq b + c,$$

$$(OR2) \forall a, b \in R : 0 \leq a \wedge 0 \leq b \rightarrow 0 \leq a \cdot b,$$

$$(OR3) 0 \leq 1.$$

Beispiele.  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

**Proposition 5.16** (Rechenregeln für geordnete Ringe). Sei  $(R, \leq)$  ein geordneter Ring und seien  $a, b, c, d, p, n, n' \in R$  mit  $p \geq 0$  und  $n, n' \leq 0$ . Dann gilt:

$$1. a \leq b \Leftrightarrow b - a \geq 0,$$

$$2. a \geq 0 \Leftrightarrow -a \leq 0,$$

$$3. a \leq b \wedge c \leq d \Rightarrow a + c \leq b + d,$$

$$4. n \cdot p \leq 0,$$

$$5. n \cdot n' \geq 0,$$

$$6. a \leq b \Rightarrow p \cdot a \leq p \cdot b,$$

$$7. a \leq b \Rightarrow n \cdot a \geq n \cdot b,$$

$$8. a^2 = a \cdot a \geq 0.$$

*Beweis.*

1. Addiere  $(+a)$  bzw.  $(-a)$  und benutze (OR1).

2. Wie 1.

3.

$$\left. \begin{array}{l} a \leq b \Rightarrow a + c \leq b + c \\ c \leq d \Rightarrow b + c \leq b + d \end{array} \right\} \text{Transitivität} \Rightarrow a + c \leq b + d$$

4.

$$n \leq 0 \stackrel{2}{\Rightarrow} (-n) \geq 0 \stackrel{\text{(OR2)}}{\Rightarrow} (-n) \cdot p \geq 0 \stackrel{\text{Proposition 5.12}}{\Rightarrow} -(n \cdot p) \geq 0 \stackrel{2}{\Rightarrow} n \cdot p \leq 0$$

□

### 5.3 Körper

**Definition 5.17.** Sei  $(K, +, \cdot)$  ein kommutativer Ring mit Eins mit mindestens zwei Elementen.  $K$  heißt ein Körper (engl. „field“), falls

$$\forall a \in K \setminus \{0\} : \exists a^{-1} \in K : a \cdot a^{-1} = 1.$$

**Proposition 5.18.** Sei  $K$  ein Körper. Dann ist  $K$  ein nullteilerfreier Ring.

*Beweis.* Wir nehmen an, dass

$$\exists a, b \in K \ a \cdot b = 0 \wedge a \neq 0 \wedge b \neq 0$$

gilt. Multipliziere nun die Gleichung  $a \cdot b = 0$  mit  $a^{-1}$  (existiert wegen  $a \neq 0$ ) und erhalte somit

$$b = a^{-1} \cdot 0 = 0.$$

(Widerspruch)

□

**Lemma 5.19.** Sei  $M$  eine endliche Menge und  $f : M \rightarrow M$  injektiv. Dann ist  $f$  bijektiv.

*Beweis.* Es gilt

$$f(M) \subseteq M.$$

Weiters hat  $f(M)$  gleich viele Elemente wie  $M$ , da für jedes  $x \in M$  ein  $f(x) \in f(M)$  „verbraucht“ wird. Daraus folgt

$$f(M) = M$$

und somit ist  $f$  surjektiv.

□

**Satz 5.3.** Sei  $R$  ein endlicher, nullteilerfreier, kommutativer Ring mit mindestens zwei Elementen. Dann ist  $R$  ein Körper.

*Beweis.* Für  $a \in R \setminus \{0\}$  definiere  $f_a : R \rightarrow R; x \mapsto a \cdot x$ .

Behauptung:  $f_a$  ist injektiv.

Seien  $x, y \in R$  mit  $f_a(x) = f_a(y)$ , also  $a \cdot x = a \cdot y$ , und somit

$$0 = a \cdot x - a \cdot y = a \cdot (x - y) \xrightarrow{a \neq 0} x - y = 0,$$

also  $x = y$ .

Laut Lemma 5.19 ist  $f_a$  bijektiv, da  $R$  ja endlich ist.

Aufgrund der Surjektivität von  $f_a$  gibt es ein  $e_a \in R$  mit

$$e_a \cdot a = f_a(e_a) = a.$$

Jedes  $a \in R \setminus \{0\}$  hat also sein „privates“ neutrales Element.

Sei  $b \in R$  beliebig und  $a \in R \setminus \{0\}$  fest.

Da  $f_a$  surjektiv ist, gibt es ein  $y \in R$  mit  $b = f_a(y) = a \cdot y$ . Es gilt

$$e_a \cdot b = (e_a \cdot a) \cdot y = a \cdot y = b.$$

$e_a$  ist also neutrales Element bzgl. der Multiplikation, nenne es 1.

Für  $a \in R \setminus \{0\}$  gibt es (wegen der Surjektivität von  $f_a$ ) ein  $x \in R$  mit  $1 = f_a(x) = a \cdot x$ , also gibt es ein Inverses bzgl. der Multiplikation.  $\square$

*Bemerkung.* Hätten wir vorausgesetzt, dass  $R$  ein Einselement besitzt, hätten wir uns den Mittelteil des Beweises sparen können.

**Korollar 5.20.** Sei  $p$  eine Primzahl. Dann ist  $\mathbb{Z}_p$  ein Körper.

*Beweis.*  $\mathbb{Z}_p$  ist endlich und nullteilerfrei und enthält  $p$  Elemente.  $\square$

**Definition 5.21.** Definiere:

1. Ein Ring mit Eins und multiplikativem Inversem für alle von 0 verschiedenen Elemente (also ein Körper ohne Kommutativität) heißt Schiefkörper (engl. „division ring“: ein Ring, in dem man dividieren kann).
2. Aus sprachlichen Gründen heißt eine Unterstruktur eines Körpers ein Teilkörper.



## 6 Aufbau des Zahlensystems

### 6.1 Natürliche Zahlen $\mathbb{N}$ und Vollständige Induktion

Was sind die natürlichen Zahlen?

- 1, 2, 3, 4, 5, 6, ...
- I, II, III, IV, V, VI, ...
- Eins, zwei drei, vier, fünf, sechs, ...

**Definition 6.1** (Peano-Axiome). Eine Menge  $\mathbb{N}$  mit einer Abbildung  $S : \mathbb{N} \rightarrow \mathbb{N}$  heißt Menge der natürlichen Zahlen, wenn

1. Es gibt ein  $1 \in \mathbb{N}$ .
2.  $S$  ist injektiv.
3.  $\nexists x \in \mathbb{N} : S(x) = 1$
4.  $\forall A \subseteq \mathbb{N} : (1 \in A \wedge (\forall x \in A : S(x) \in A)) \rightarrow A = \mathbb{N}$  (Prinzip der vollständigen Induktion)

gilt.

(Die Bedingungen 1 bis 3 würde  $\mathbb{R}^+$  auch erfüllen!)

**Notation 6.2.**

$$2 := S(1)$$

$$3 := S(2)$$

$$4 := S(3)$$

⋮

*Bemerkung.*

- Das Prinzip der vollständigen Induktion sagt:

$$\left. \begin{array}{l} 1 \in A \\ \forall x \in A : S(x) \in A \end{array} \right\} \Rightarrow 1 \in A, 2 \in A, 3 \in A, \dots \Rightarrow A = \mathbb{N}$$

- Man könnte auch mit 0 starten. Hier bezeichnen wir eine so entstandene Menge mit  $\mathbb{N}_0$ .

*Beispiel.* Behauptung:  $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$  für alle  $n \in \mathbb{N}$ .

Beweis durch vollständige Induktion nach  $n$ :

Sei  $A := \{n \in \mathbb{N} \mid 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}\}$ .

Induktionsbasis:

$$1 = 1$$

$$\frac{1 \cdot (1+1)}{2} = 1$$

Somit gilt  $1 \in A$ .

Induktionsschritt: Sei  $n \in A$ . Dann gilt

$$(1 + 2 + \dots + n) + (n+1) \stackrel{n \in A}{=} \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2}$$

und somit auch  $(n+1) \in A$ .

Nach dem Prinzip der vollständigen Induktion gilt somit  $A = \mathbb{N}$ . Die Behauptung ist daher bewiesen.

**Definition 6.3** (Addition). *Wir definieren eine Abbildung  $+$  :  $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  durch*

1.  $\forall a \in \mathbb{N} : a + 1 := S(a)$ ,
2.  $\forall a, b \in \mathbb{N} : a + S(b) := S(a + b)$ .

*Bemerkung.* Sei  $a \in \mathbb{N}$ . Die Menge

$$A(a) = \{b \in \mathbb{N} \mid a + b \text{ ist definiert}\}$$

ist dadurch (und durch vollständige Induktion) gleich  $\mathbb{N}$ .

**Proposition 6.4.**  $(\mathbb{N}, +)$  ist eine Halbgruppe.

*Beweis.* Seien  $a, b \in \mathbb{N}$  und setze

$$A_{a,b} := \{c \in \mathbb{N} \mid (a + b) + c = a + (b + c)\}$$

Induktionsbasis: Setze  $c = 1$ , somit

$$(a + b) + 1 \stackrel{\text{Def. 1}}{=} S(a + b) \stackrel{\text{Def. 2}}{=} a + S(b) \stackrel{\text{Def. 1}}{=} a + (b + 1),$$

also  $1 \in A_{a,b}$ .

Induktionsschritt: Sei  $c \in A_{a,b}$ . Dann gilt

$$(a + b) + S(c) \stackrel{\text{Def. 2}}{=} S((a + b) + c) \stackrel{c \in A_{a,b}}{=} S(a + (b + c)) \stackrel{\text{Def. 2}}{=} a + S(b + c) \stackrel{\text{Def. 2}}{=} a + (b + S(c)),$$

also  $S(c) \in A_{a,b}$  und nach dem Prinzip der vollständigen Induktion  $A_{a,b} = \mathbb{N}$ . □

**Proposition 6.5.**  $(\mathbb{N}, +)$  ist kommutativ.

**Definition 6.6** (Multiplikation). *Die Abbildung  $\cdot$  :  $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  wird definiert durch*

1.  $a \cdot 1 := a$ ,
2.  $a \cdot S(b) := a \cdot b + a$ .

**Proposition 6.7.** *Es gelten Assoziativgesetz, Kommutativgesetz und Distributivgesetz.*

**Definition 6.8** (Ordnungsrelation). *Definiere die Relation  $\leq$   $\subseteq \mathbb{N} \times \mathbb{N}$  durch*

$$a \leq b \Leftrightarrow a = b \vee \exists c \in \mathbb{N} : b = a + c.$$

**Proposition 6.9.** *Die Relation  $\leq$  ist eine Totalordnung und „verträglich“ mit Addition und Multiplikation.*

**Definition 6.10.** *Sei  $X$  eine Menge. Eine Folge aus  $X$ /in  $X$ /mit Werten in  $X$  ist eine Abbildung*

$$f : \mathbb{N} \rightarrow X.$$

*Statt  $f(n)$  schreibt man meist  $f_n$ .*

*Beispiel.*  $f_n = \sqrt{n}$  ist eine Folge in  $\mathbb{R}$ .

**Definition 6.11** (Summen- und Produktzeichen). *Definiere:*

1. Sei  $(G, +)$  eine abelsche Gruppe und  $a_n$  eine Folge in  $G$ . Dann setze

$$\sum_{k=1}^n a_k := a_1 + a_2 + \cdots + a_n.$$

Die leere Summe wird als 0 definiert, also z.B.

$$\sum_{k=1}^0 a_k = 0.$$

2. Sei  $(G, \cdot)$  eine Gruppe und  $a_n$  eine Folge in  $G$ . Setze

$$\prod_{k=1}^n a_k := a_1 \cdot a_2 \cdot \cdots \cdot a_n.$$

Das leere Produkt wird als 1 definiert.

*Beispiel.*

$$\sum_{k=1}^n k = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

$$\sum_{k=1}^n 1 = \underbrace{1 + 1 + \cdots + 1}_n = n$$

*Bemerkung.*

$$\sum_{k=1}^n a_k = \sum_{l=1}^n a_l = \sum_{k=0}^{n-1} a_{k+1} = \sum_{k=0}^{n-1} a_{n-k}$$

Man schreibt auch

$$\sum_{1 \leq k \leq n} a_k = \sum_{1 \leq n-l \leq n} a_{n-l} = \sum_{0 \leq l \leq n-1} a_{n-l}$$

Bei einer vollständigen Induktion ist es nützlich, die Summe aufzuspalten:

$$\sum_{k=1}^{n+1} a_k = \left( \sum_{k=1}^n a_k \right) + a_{n+1}$$

*Bemerkung.* Die von Neumannschen natürlichen Zahlen sind ein Modell für die natürlichen Zahlen der Form

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots$$

also mit der Nachfolgerfunktion  $S : \mathbb{N} \rightarrow \mathbb{N}; A \mapsto A \cup \{A\}$ .

## 6.2 Ganze Zahlen $\mathbb{Z}$

**Definition 6.12.** Auf der Menge  $\mathbb{N} \times \mathbb{N}$  definiere die Relation  $\sim$  durch

$$(a, b) \sim (c, d) :\Leftrightarrow a + d = c + b.$$

**Lemma 6.13.**  $\sim$  ist eine Äquivalenzrelation.

*Beweis.*

- $(a, b) \sim (a, b) \Leftrightarrow a + b = a + b$ , somit ist  $\sim$  reflexiv.
- $(a, b) \sim (c, d) \Leftrightarrow a + d = c + b \Leftrightarrow c + b = a + d \Leftrightarrow (c, d) \sim (a, b)$ , somit ist  $\sim$  symmetrisch.
- Es gilt

$$(a, b) \sim (c, d) \wedge (c, d) \sim (e, f) \Leftrightarrow a + d = c + b \wedge c + f = e + d$$

Daraus folgt durch Addition von  $f$ :

$$(a + f) + d = (a + d) + f = (c + b) + f = (c + f) + b = (e + d) + b = (e + b) + d,$$

also  $a + f = e + b$  und somit  $(a, b) \sim (e, f)$ , womit  $\sim$  transitiv ist. □

**Definition 6.14.** Die Menge  $(\mathbb{N} \times \mathbb{N})/\sim$  wird als die Menge der ganzen Zahlen  $\mathbb{Z}$  bezeichnet, und zwar mit den Operationen:

$$[(a, b)] + [(c, d)] := [(a + c, b + d)]$$

$$[(a, b)] \cdot [(c, d)] := [(ac + bd, bc + ad)]$$

$$[(a, b)] \geq [(c, d)] :\Leftrightarrow a + d \geq b + c$$

*Bemerkung.* Diese Definitionen werden durch die Interpretation von  $[(a, b)]$  als  $a - b$  motiviert.

**Satz 6.1.** Obige Definitionen von  $+$ ,  $\cdot$ ,  $\geq$  sind wohldefiniert und  $(\mathbb{Z}, +, \cdot, \geq)$  ist ein geordneter Ring.

*Beweisskizze.* Wir zeigen die Wohldefiniertheit der Addition:

Falls  $[(a_1, b_1)] = [(a_2, b_2)]$  und  $[(c_1, d_1)] = [(c_2, d_2)]$ , so gilt lt. Definition

$$a_1 + b_2 = a_2 + b_1$$

$$c_1 + d_2 = c_2 + d_1$$

---


$$a_1 + c_1 + b_2 + d_2 = a_2 + c_2 + b_1 + d_1$$

und somit

$$[(a_1 + c_1, b_1 + d_1)] = [(a_2 + c_2, b_2 + d_2)].$$

Es bleibt noch zu zeigen:

- Wohldefiniertheit von  $\cdot$ ,
- Wohldefiniertheit von  $\geq$ ,
- Assoziativgesetz bzgl.  $+$ ,
- $[(1, 1)]$  ist neutrales Element bzgl.  $+$ ,
- $[(b, a)]$  ist additives Inverses von  $[a, b]$ ,
- Kommutativgesetz bzgl.  $+$ ,
- Assoziativgesetz bzgl.  $\cdot$ ,
- Kommutativgesetz bzgl.  $\cdot$ ,
- $[(2, 1)]$  ist neutrales Element bzgl.  $\cdot$ ,
- Distributivgesetz,
- $\geq$  ist reflexiv, transitiv und antisymmetrisch,
- $a \geq b \Rightarrow a + c \geq b + c$ ,
- $a \geq 0 \wedge b \geq 0 \Rightarrow a \cdot b \geq 0$ .

### 6.3 Rationale Zahlen $\mathbb{Q}$

Motivation: Gleichung  $a \cdot x = b$  in  $\mathbb{Z}$  nicht immer lösbar.

**Definition 6.15.** Auf  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  definiere die Relation  $\sim$  durch

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

Das ist eine Äquivalenzrelation (ähnlich Lemma 6.13).

Die Menge der Äquivalenzklassen  $(\mathbb{Z} \times \mathbb{Z} \setminus \{0\}) / \sim$  heißt die Menge der rationalen Zahlen  $\mathbb{Q}$ . Die Äquivalenzklasse von  $(a, b)$  schreibe als  $\frac{a}{b}$ . Weiters setze

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &:= \frac{ad + cb}{bd}, \\ \frac{a}{b} \cdot \frac{c}{d} &:= \frac{a \cdot c}{b \cdot d}. \end{aligned}$$

Falls  $b > 0, d > 0$ , setze

$$\frac{a}{b} \geq \frac{c}{d} := \Leftrightarrow a \cdot d \geq b \cdot c.$$

(Falls nicht, wähle anderen Repräsentanten.)

**Satz 6.2.** Die Operationen  $+, \cdot, \geq$  sind wohldefiniert und  $\mathbb{Q}$  ist ein geordneter Körper.

*Beweisskizze.* Wir zeigen die Wohldefiniertheit der Addition:

$$\begin{aligned} \frac{a_1}{b_1} = \frac{a_2}{b_2} &\Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1 \\ \frac{c_1}{d_1} = \frac{c_2}{d_2} &\Leftrightarrow c_1 \cdot d_2 = c_2 \cdot d_1 \end{aligned}$$

Das bedeutet (multipliziere diese Gleichungen mit  $d_1 d_2$  bzw.  $b_1 b_2$  und addiere sie):

$$\begin{aligned} a_1 b_2 \cdot d_1 d_2 + c_1 d_2 \cdot b_1 b_2 &= b_1 a_2 \cdot d_1 d_2 + c_2 d_1 \cdot b_1 b_2 \\ \Leftrightarrow (a_1 d_1 + c_1 b_1) \cdot b_2 d_2 &= b_1 d_1 \cdot (a_2 d_2 + c_2 b_2) \\ \Leftrightarrow \frac{a_1 d_1 + c_1 b_1}{b_1 d_1} &= \frac{a_2 d_2 + c_2 b_2}{b_2 d_2} \end{aligned}$$

Es bleibt u.a. noch entsprechend zu Satz 6.1 zu zeigen:

- $\frac{0}{1}$  ist neutrales Element bzgl.  $+$ ,
- $\frac{-a}{b}$  ist additives Inverses von  $\frac{a}{b}$ ,
- $\frac{1}{1}$  ist neutrales Element bzgl.  $\cdot$ ,
- $\frac{b}{a}$  ist multiplikatives Inverses von  $\frac{a}{b}$ .

Die Abbildung  $\iota : \mathbb{Z} \rightarrow \mathbb{Q}; a \mapsto \frac{a}{1}$  („Jota“) ist injektiv und erfüllt

$$\begin{aligned} \iota(a + b) &= \iota(a) + \iota(b) \\ \iota(a \cdot b) &= \iota(a) \cdot \iota(b) \\ a \leq b &\Leftrightarrow \iota(a) \leq \iota(b) \end{aligned}$$

Man identifiziert  $\mathbb{Z}$  mit  $\iota(\mathbb{Z})$  (also z.B.  $2 = \frac{2}{1}$ ), somit gilt

$$\mathbb{Z} \subseteq \mathbb{Q}.$$

## 6.4 Reelle Zahlen $\mathbb{R}$

Wunsch: Jede beschränkte Menge soll Supremum und Infimum besitzen.

Nebenbei: Löse Gleichung  $x^a = b$  für  $a \in \mathbb{Z}, b \in \mathbb{Q}, b > 0$ .

**Definition 6.16.** Eine Teilmenge  $\alpha \subset \mathbb{Q}$  heißt Dedekindscher Schnitt, falls

1.  $\alpha \neq \emptyset \wedge \alpha \neq \mathbb{Q}$ ,
2.  $\forall r, s \in \mathbb{Q} : r \in \alpha \wedge r < s \rightarrow s \in \alpha$ ,
3.  $\alpha$  hat kein kleinstes Element, d.h.

$$\forall r \in \alpha \exists s < r : s \in \alpha.$$

Beispiele.

1. Sei  $q \in \mathbb{Q}$ . Dann ist

$$\bar{q} := \{r \in \mathbb{Q} \mid r > q\}$$

ein Dedekindscher Schnitt.

2.  $M = \{x \in \mathbb{Q} \mid x > 0 \wedge x^2 > 2\}$

**Definition 6.17.**

$$\mathbb{R} := \{\alpha \subseteq \mathbb{Q} \mid \alpha \text{ ist Dedekindscher Schnitt}\}$$

**Definition 6.18.** Seien  $\alpha, \beta \in \mathbb{R}$ . Dann setze

$$\alpha \leq \beta := \beta \subseteq \alpha.$$

**Proposition 6.19.**  $\leq$  ist eine Totalordnung auf  $\mathbb{R}$ .

*Beweis.* Dass  $\leq$  eine Partialordnung ist, folgt sofort aus den mengentheoretischen Eigenschaften von  $\subseteq$ .

Seien  $\alpha, \beta \in \mathbb{R}$  mit  $\alpha \not\subseteq \beta$ .

O.B.d.A. („Ohne Beschränkung der Allgemeinheit“) nehmen wir an, dass  $\alpha \setminus \beta \neq \emptyset$ . Es gibt also ein  $r \in \alpha$  mit  $r \notin \beta$ . Sei  $s \in \beta$ . Dann wissen wir

$$s > r \Rightarrow s \in \alpha \Rightarrow \beta \subseteq \alpha \Rightarrow \alpha \leq \beta.$$

□

**Proposition 6.20.** Sei  $A \subseteq \mathbb{R}$  nach unten beschränkt und nicht leer. Dann besitzt  $A$  ein Infimum in  $\mathbb{R}$ .

*Beweis.* Es gibt ein  $\beta \in \mathbb{R}$ , sodass

$$\forall \alpha \in A : \beta \leq \alpha.$$

Das bedeutet per Definition  $\alpha \subseteq \beta$ . Setze nun

$$\gamma := \bigcup_{\alpha \in A} \alpha.$$

Es folgt für alle  $\alpha \in A$ :

$$\alpha \subseteq \beta \Rightarrow \gamma \subseteq \beta \Rightarrow \gamma \geq \beta \text{ für jede untere Schranke } \beta$$

Andererseits gilt für alle  $\alpha \in A$ :

$$\gamma \supseteq \alpha \stackrel{\text{Def.}}{\iff} \gamma \leq \alpha$$

Das heißt, dass  $\gamma$  eine untere Schranke für  $A$  ist.

Wenn wir zeigen, dass  $\gamma \in \mathbb{R}$ , so ist  $\gamma$  größte untere Schranke von  $A$ , also ist  $\gamma$  ein Infimum.

1. Wir wissen

$$\emptyset \neq \alpha \subseteq \gamma \subseteq \beta \subsetneq \mathbb{Q}.$$

2. Falls  $r \in \gamma, r < s$ , so ist  $r \in \alpha$  für ein passendes  $\alpha \in A$ , somit

$$s \in \alpha \subseteq \gamma.$$

3. Sei  $r \in \gamma$ . Dann gilt

$$\exists \alpha : r \in \alpha \Rightarrow \exists s < r : s \in \alpha \Rightarrow \exists s < r : s \in \gamma.$$

□

**Definition 6.21.** Seien  $\alpha, \beta \in \mathbb{R}$ . Definiere

$$\begin{aligned} \alpha + \beta &:= \{a + b \mid a \in \alpha \wedge b \in \beta\}, \\ 0 &:= \{q \in \mathbb{Q} \mid q > 0\}. \end{aligned}$$

Für  $\alpha, \beta \geq 0$  definiere

$$\alpha \cdot \beta := \{a \cdot b \mid a \in \alpha \wedge b \in \beta\}.$$

**Satz 6.3.**  $(\mathbb{R}, +, \cdot)$  ist ein geordneter Körper. Jede beschränkte Teilmenge von  $\mathbb{R}$  besitzt ein Infimum und ein Supremum.

Weiters definiere die Abbildung  $\iota : \mathbb{Q} \rightarrow \mathbb{R}; \iota(q) = \{r \in \mathbb{Q} \mid r > q\}$ . Dann ist  $\iota$  injektiv und es gilt

$$\begin{aligned} \iota(a + b) &= \iota(a) + \iota(b) \\ \iota(a \cdot b) &= \iota(a) \cdot \iota(b) \\ a \leq b &\Leftrightarrow \iota(a) \leq \iota(b) \end{aligned}$$

*Beweis.* mühsam. □

*Bemerkung.* Man identifiziert  $\mathbb{Q}$  mit  $\iota(\mathbb{Q})$ , sodass

$$\mathbb{Q} \subseteq \mathbb{R}.$$

**Satz 6.4.**  $\mathbb{Q}$  liegt dicht in  $\mathbb{R}$ , d.h. zwischen je zwei reellen (nichtrationalen) Zahlen liegt eine rationale Zahl.

*Beweis.* Seien  $\alpha, \beta \in \mathbb{R}, \alpha \neq \beta$ , o.B.d.A.  $\alpha < \beta \Leftrightarrow \beta \subsetneq \alpha$ . Es gibt daher eine rationale Zahl  $r \in \alpha \setminus \beta$ . Da  $r$  nicht das kleinste Element von  $\alpha$  ist, folgt

$$\alpha < r < \beta.$$

□

**Definition 6.22.** Sei  $x \in \mathbb{R}$ . Dann definiere

$$|x| := \begin{cases} x & \text{für } x \geq 0 \\ -x & \text{für } x < 0 \end{cases}$$

als den (Absolut-)Betrag von  $x$ .

*Bemerkung.* Rechenregeln für reelle Absolutbeträge folgen aus den Rechenregeln für den komplexen Absolutbetrag, siehe nächster Abschnitt.

## 6.5 Komplexe Zahlen $\mathbb{C}$

Motivation: Die Gleichung  $x^2 = -1$  soll lösbar werden.

**Definition 6.23.** Auf  $\mathbb{R} \times \mathbb{R} =: \mathbb{C}$  definiere

$$(a, b) + (c, d) := (a + c, b + d)$$

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc)$$

**Satz 6.5.**  $(\mathbb{C}, +, \cdot)$  ist ein Körper.

*Beweis.*

- $+, \cdot$  sind alle  $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$ .
- Addition assoziativ
- Addition kommutativ
- Neutrales Element bzgl. Addition:  $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$ , daher ist  $(0, 0)$  neutrales Element bzgl.  $+$ .
- Inverses Element bzgl. Addition:  $(a, b) + (-a, -b) = (0, 0)$ , also ist  $(-a, -b)$  das Negative von  $(a, b)$ .
- Multiplikation assoziativ:

$$\begin{aligned} ((a, b) \cdot (b, c)) \cdot (e, f) &= (ac - bd, ad + bc) \cdot (e, f) = (ace - bde - adf - bcf, acf - bdf + ade + bce) \\ &= (a, b) \cdot ((b, c) \cdot (e, f)) \end{aligned}$$

- Multiplikation kommutativ: durch Hinsehen
  - Neutrales Element bzgl. Multiplikation:
- $$(a, b) \cdot (1, 0) = (a, b)$$
- Inverses Element bzgl. Multiplikation („name & conquer“):

$$(a, b) \cdot (x, y) = (1, 0)$$

$$(ax - by, bx + ay) = (1, 0)$$

Aufspalten in die beiden Komponenten ergibt:

$$\begin{array}{rcl} ax - by = 1 & | \cdot a \\ bx + ay = 0 & | \cdot b \\ \hline a^2x + b^2x = a \end{array}$$

Daraus folgt

$$x = \frac{a}{a^2 + b^2} \text{ bzw. } y = \frac{-b}{a^2 + b^2}.$$

Es gilt  $x, y \in \mathbb{R} \Leftrightarrow a^2 + b^2 \neq 0 \Leftrightarrow (a, b) \neq (0, 0)$ . Für  $(a, b) = (0, 0)$  brauchen wir allerdings eh kein inverses Element.

(Wir sollten jetzt eine Probe machen.)

- Distributivgesetz:

$$\begin{aligned} ((a, b) + (c, d)) \cdot (e, f) &= (a + c, b + d) \cdot (e, f) = (ae + ce - bf - df, af + cf + be + de) \\ &= (a, b) \cdot (e, f) + (c, d) \cdot (e, f) \end{aligned}$$

□

**Proposition 6.24.**  $\iota : \mathbb{R} \rightarrow \mathbb{C}, a \mapsto (a, 0)$  ist eine injektive Abbildung mit

$$\begin{aligned} \iota(a + b) &= \iota(a) + \iota(b), \\ \iota(a \cdot b) &= \iota(a) \cdot \iota(b) \end{aligned}$$

( $\iota$  ist ein Körperhomomorphismus.)

*Beweis.* durch Händefuchteln.

□

**Definition 6.25.** Definiere

$$i := (0, 1).$$

*Bemerkungen.*

1.  $i^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = \iota(-1)$

2. Wir identifizieren  $x \in \mathbb{R}$  mit  $\iota(x) = (x, 0) \in \mathbb{C}$ , daraus folgt

$$\mathbb{R} \subseteq \mathbb{C}.$$

3.

$$(a, b) = (a, 0) + (0, b) = \underbrace{(a, 0)}_a + \underbrace{(b, 0)}_b \cdot \underbrace{(0, 1)}_i = a + bi$$

4.

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi) \cdot (c + di) &= ac + bdi^2 + (bc + ad)i^2 = (ac - bd) + (bc + ad)i \end{aligned}$$

**Definition 6.26.** Sei  $z = a + bi \in \mathbb{C} (a, b \in \mathbb{R})$ . Dann setze

$$\operatorname{Re}(z) := a$$

als den Realteil von  $z$  und

$$\operatorname{Im}(z) := b$$

als den Imaginärteil von  $z$ .

Die zu  $z$  konjugiert komplexe Zahl ist

$$\bar{z} := a - bi.$$

Weiters ist der Betrag von  $z$  gleich

$$|z| := \sqrt{a^2 + b^2}.$$

*Bemerkung.* Da  $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$  (mit speziellen Rechenoperationen), entspricht  $a + bi$  dem Punkt  $(a, b) \in \mathbb{R}^2$ . Somit ist  $|z|$  der euklidische Abstand vom Ursprung (Satz von Pythagoras).

**Satz 6.6** (Rechenregeln für komplexe Zahlen). *Seien  $z, w \in \mathbb{C}$ . Dann gilt:*

1.  $\overline{z + w} = \bar{z} + \bar{w}$
2.  $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
3.  $\overline{\left(\frac{1}{z}\right)} = \frac{1}{\bar{z}}$
4.  $-(\bar{z}) = \overline{-z}$
5.  $|z| = \sqrt{z \cdot \bar{z}}$
6.  $|z \cdot w| = |z| \cdot |w|$
7.  $\left|\frac{1}{z}\right| = \frac{1}{|z|}$
8.  $|-z| = |z|$
9.  $|z + w| \leq |z| + |w|$
10.  $||z| - |w|| \leq |z + w|$
11.  $2 \cdot \operatorname{Re}(z) = z + \bar{z}$
12.  $2i \cdot \operatorname{Im}(z) = z - \bar{z}$
13.  $-|z| \leq \operatorname{Re}(z) \leq |z|$
14.  $-|z| \leq \operatorname{Im}(z) \leq |z|$
15.  $z \in \mathbb{R} \Leftrightarrow z = \bar{z}$
16.  $\overline{(\bar{z})} = z$
17.  $|z| \geq 0$  und  $|z| = 0 \Leftrightarrow z = 0$

*Beweis.*

1.  $\overline{z + w} = (a + c) - (b + d)i = \bar{z} + \bar{w}$
- 2.
3.  $\frac{1}{z} = \frac{\bar{z}}{z \cdot \bar{z}} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i = \dots$
4. leicht
5.  $z \cdot \bar{z} = (a + bi)(a - bi) = a^2 + b^2$ , somit  $\sqrt{z \cdot \bar{z}} = |z|$
6.  $|z \cdot w| = \sqrt{(z \cdot w) \cdot (\bar{z} \cdot \bar{w})} = \sqrt{z \cdot \bar{z} \cdot w \cdot \bar{w}} = \sqrt{z \cdot \bar{z}} \cdot \sqrt{w \cdot \bar{w}} = |z| \cdot |w|$
7. leicht
8. leicht

9.

$$\begin{aligned}
0 &\leq (bc - ad)^2 \\
2abcd &\leq b^2c^2 + a^2d^2 \\
a^2c^2 + 2abcd + b^2d^2 &\leq a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 \\
4(ac + bd)^2 &\leq 4(a^2 + b^2)(c^2 + d^2) \\
2ac + 2bd &\leq 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\
(a + c)^2 + (b + d)^2 &\leq a^2 + b^2 + 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2} + c^2 + d^2 \\
\sqrt{(a + c)^2 + (b + d)^2} &\leq \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2} \\
|z + w| &\leq |z| + |w|
\end{aligned}$$

10.

$$|z| = |(z + w) + (-w)| \stackrel{9}{\leq} |z + w| + |-w| \stackrel{8}{=} |z + w| + |w|$$

Andererseits gilt:

$$|w| = |(w + z) + (-z)| \leq |w + z| + |-z| \Rightarrow -|z + w| \leq |z| - |w|$$

Wir wissen also

$$-|z + w| \leq |z| - |w| \leq |z + w|$$

und somit

$$||z| - |w|| \leq |z + w|.$$

□



## 7 Elementarste Kombinatorik

**Definition 7.1.** Sei  $M$  eine endliche Menge. Mit  $|M|$  oder  $\#M$  wird die Anzahl der Elemente (auch Mächtigkeit bzw. Kardinalität) von  $M$  bezeichnet.

**Lemma 7.2.** Seien  $M, N$  zwei endliche Mengen und  $f : M \rightarrow N$  bijektiv. Dann gilt  $|M| = |N|$ .

*Beweis.* durch Händefucheln. □

**Definition 7.3.** Seien  $M, N$  zwei (nicht notwendigerweise endliche) Mengen.  $M$  und  $N$  heißen gleichmächtig ( $|M| = |N|$ ), wenn es eine Bijektion  $f : M \rightarrow N$  gibt.

**Definition 7.4.** Eine Menge  $M$  heißt abzählbar unendlich, wenn sie gleichmächtig zu  $\mathbb{N}$  ist.

**Proposition 7.5.** Seien  $A, B$  endliche Mengen,  $n \in \mathbb{N}$ . Dann gilt:

1.  $|A \times B| = |A| \cdot |B|$
2.  $|A^n| = |A|^n$
3.  $|\mathcal{P}(A)| = 2^{|A|}$

### 7.1 Permutationen

**Definition 7.6.** Sei  $M$  eine endliche Menge. Eine bijektive Abbildung von  $M$  nach  $M$  heißt Permutation. Die Menge der Permutationen der Menge  $\{1, \dots, n\}$  heißt die symmetrische Gruppe der Ordnung  $n$ ,  $S_n$ .

**Satz 7.1.** Sei  $n \in \mathbb{N}$ . Dann gilt

$$|S_n| = n! := n \cdot (n-1) \cdot \dots \cdot 1.$$

*Beweis.*

Für Element 1 gibt es $n$ Möglichkeiten.	}	$\Rightarrow n \cdot (n-1) \cdot \dots \cdot 1$ Möglichkeiten.
Für Element 2 gibt es $n-1$ Möglichkeiten.		
$\vdots$		
Für Element $n$ gibt es 1 Möglichkeit.		

□

**Definition 7.7.** Sei  $n \in \mathbb{N}_0$ . Definiere die Fakultät von  $n$  als

$$n! := \prod_{k=1}^n k.$$

*Bemerkung.*  $0! = 1$  (leeres Produkt).

### 7.2 Binomialkoeffizienten

**Definition 7.8.** Für  $\alpha \in \mathbb{C}$  und ein  $k \in \mathbb{N}_0$  definiere

$$\binom{\alpha}{k} := \frac{\alpha \cdot (\alpha-1) \cdot \dots \cdot (\alpha-k+1)}{k!}$$

als „Binomialkoeffizient“ oder „ $n$  über  $k$ “ (engl. „ $n$  choose  $k$ “).

**Lemma 7.9.** Für  $n, k \in \mathbb{N}_0$  gilt

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

**Satz 7.2.** Seien  $n, k \in \mathbb{N}_0$ . Die Anzahl der  $k$ -elementigen Teilmengen einer  $n$ -elementigen Menge ist  $\binom{n}{k}$ .

*Beweis.*

1. Element:  $n$  Möglichkeiten
2. Element:  $n - 1$  Möglichkeiten
- $\vdots$
- $k$ . Element:  $n - k + 1$  Möglichkeiten

Wir müssen durch die Anzahl der Permutationen von  $k$  Elementen dividieren, weil wir jede Teilmenge in allen ihren Permutationen gezählt haben.  $\square$

**Lemma 7.10.** Für Binomialkoeffizienten gilt:

1.  $\binom{n}{k} = 0$ , falls  $k > n$ .
2.  $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

*Beweis.*

1. klar
2. Um eine  $k$ -elementige Teilmenge einer  $n$ -elementigen Menge auszuwählen, können wir Element 1 auswählen (brauchen noch  $\binom{n-1}{k-1}$ ) oder Element 1 verbieten (brauchen noch  $\binom{n-1}{k}$ ). (oder: Nachrechnen)

*Veranschaulichung.* Pascalsches Dreieck

$\square$

**Satz 7.3** (Binomischer Lehrsatz). Sei  $R$  ein kommutativer Ring,  $x, y \in R, n \in \mathbb{N}_0$ . Dann gilt

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k \cdot y^{n-k}.$$

*Beweis.* Es gilt

$$(x + y)^n = (x + y) \cdot (x + y) \cdot \dots \cdot (x + y).$$

Um  $x^k \cdot y^{n-k}$  zu erhalten, gibt es  $\binom{n}{k}$  Möglichkeiten,  $k$  Klammern ein  $x$  zu entreißen. (oder: Induktionsbeweis über die Rekursion aus Lemma 7.10)  $\square$

*Beispiele.*

$$(x + y)^2 = x^2 + 2xy + y^2$$

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$