Mathematik I für Physiker und Geowissenschaftler

C. Devchand

WS 2006/7

Vorlesungsmitschrift von Jonas Hörsch und Kai von Krbek

# Teil I

# Anfangsbeispiele

## 0 Zahlbereiche

1. Die natürlichen Zahlen: $\mathbb{N} = \{0, 1, 2, 3 \dots\}$ ,$\mathbb{N}_0$ auch
2. Die ganzen Zahlen: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
3. Die rationalen Zahlen: $\mathbb{Q}$ =Menge aller Brüche ganzer Zahlen
   $\mathbb{Q} = \{\frac{p}{q} | p \in \mathbb{Z} | q \in \mathbb{N}\}$
4. Die reellen Zahlen $\mathbb{R}$: Zahlen auf der Zahlgeraden
5. Die komplexen Zahlen: $\mathbb{C}$

Inklusionen der Zahlbereiche

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Motivation für die Erweiterung eines Zahlbereiches: im neuen Bereich kann man Gleichungen lösen, die man in bisherigen Zahlbereich nicht lösen könnte.

- $x + a = b \quad a, b \in \mathbb{N}$,
  Nicht für $x \in \mathbb{N}$ lösbar, aber für $x \in \mathbb{Z}$ kann man sie lösen.
- $ax + b = c \quad \forall a, b, c \in \mathbb{Z}$ mit $a \neq 0$,
  nicht mit $x \in \mathbb{Z}$ lösbar, aber in $\mathbb{Q}$ doch.
- $x^2 = a \quad \forall a \in \mathbb{Z}$,
  hat keine Lösung in $\mathbb{Q}$, aber doch in $\mathbb{R}$.
- $x^2 = -1$,
  hat keine Lösung für $x \in \mathbb{R}$, aber in $\mathbb{C}$ lösbar.

# 1 Rechnen mit rationalen Zahlen und Ungleichungen

## 1.1 Approximation von $\sqrt{2}$ mit rationalen Zahlen

Irrationale Zahlen können durch Approximation dargestellt werden, beschrieben am Beispiel von $\sqrt{2}$.

$$1 < \sqrt{2} < 2, \text{ denn } 1^2 < 2 < 2^2$$

Wie kann man besser approximieren?

$$\begin{aligned} \text{Binomische Formel}: \quad & (a+b)(a-b) && = a^2 - b^2 \\ \text{Spezialisieren}: \quad & (\sqrt{2}+1)(\sqrt{2}-1) && = 2-1 = 1 \\ \text{Umformung}: \quad & \sqrt{2} && = \frac{1}{\sqrt{2}+1} + 1 \end{aligned}$$

Wir lesen die rechte Seite als „Wert der Funktion $x \mapsto \frac{1}{1+x} + 1$ an der Stelle $x = \sqrt{2}$“. Dann argumentieren wir, dass das Einsetzen eines Näherungswertes für $\sqrt{2}$ eine bessere Näherung liefert.

### 1.1.1 Ausprobieren:

Setze $x = 1$ ein: $1 + \frac{1}{1+1} = \frac{3}{2} \, (> \sqrt{2}) \quad \rightarrow$ Neue (bessere) obere[1] Grenze.
Setze $x = 2$ ein: $1 + \frac{1}{1+2} = \frac{4}{3} \, (< \sqrt{2}) \quad \rightarrow$ Neue untere Grenze.
$\Rightarrow \frac{4}{3} < \sqrt{2} < \frac{3}{2}$

Wir haben nun $\sqrt{2}$ mit der Fehlerschranke (Approximationsintervall) $\frac{3}{2} - \frac{4}{3} = \frac{1}{6}$ bestimmt.

Wiederholung des Vorganges mit den neuen Werten:

$$1 + \frac{1}{1+\frac{4}{3}} = 1 + \frac{3}{7} = \frac{10}{7} \, (> \sqrt{2})$$
$$1 + \frac{1}{1+\frac{3}{2}} = 1 + \frac{2}{5} = \frac{7}{5} \, (< \sqrt{2})$$

Fehlerschranke: $\frac{10}{7} - \frac{7}{5} = \frac{1}{35}$

Nochmalige Wiederholung: $\frac{24}{17} < \sqrt{2} < \frac{17}{12}$ ; mit der Genauigkeit $\frac{17}{12} - \frac{24}{17} = \frac{1}{204}$

So können wir $\sqrt{2}$ mit einer *beliebigen Genauigkeit* durch rationale Zahlen *approximieren.*

[1] da $\frac{9}{4} > 2$

### 1.1.2 Verallgemeinerung:

Experimentell haben wir so bestimmt[2]:

Obere Grenze $a$ : $\frac{2}{a} < \sqrt{2} < a \leq 2$

Neue obere Schranke: $a \mapsto (\frac{1}{a} + \frac{a}{2})$

$$\frac{1}{a} + \frac{a}{2} > \sqrt{2} \Leftrightarrow (\frac{1}{a} + \frac{a}{2})^2 > 2 \Leftrightarrow \frac{1}{a^2} + 2(\frac{1}{a} \cdot \frac{a}{2}) + \frac{a^2}{4} > 2 \Leftrightarrow \frac{1}{a^2} - 1 + \frac{a^2}{4}$$
$$\Leftrightarrow (\frac{1}{a} - \frac{a}{2})^2 > 0\,; \text{ was stimmt, da alle Quadrate von Zahlen} \neq 0 \text{ positiv sind.}$$

Also haben wir gezeigt:

**Satz 1.1.** *Wenn $\frac{2}{a} < \sqrt{2} < a$ ist, so folgt $\frac{4}{\frac{2}{a}+a} < \sqrt{2} < \frac{1}{a} + \frac{a}{2}$*
*Das Approximationsintervall wird bei jedem Schritt kleiner, aber verschwindet nie. $\rightarrow$ Also folgt $\sqrt{2}$ liegt nicht in $\mathbb{Q}$.*

**Strategie:** Statt $y > x$ zu beweisen, ist es oft einfacher $y - x > 0$ zu beweisen.
Schlußstein der Strategie: Quadrate $\geq 0$.

Aus Satz **??** kann man folgenden **Algorithmus** zur Näherung von $\sqrt{2}$ durch rationale Zahlen ableiten:

Sei $a_1 = 2$ und $a_{n+1} := \frac{1}{a_n} + \frac{a_n}{2}$ für $n \geq 1$,
dann ist $\frac{2}{a_n} < \sqrt{2} < a_n$ (für $a_n$, $n \in \mathbb{N}$) $(\star)$

Für diese Näherung von $\sqrt{2}$ gilt die Fehlerschranke: $a_n - \frac{2}{a_n} \leq \frac{1}{2^{n-1}}$ $(\star\star)$

**Beweis:**

$(\star)$ beweist man durch **vollständige Induktion**:

Dass der Induktionsbeginn mit $n = 1$ stimmt, ist offensichtlich.
Es folgt aus $(\star)$ für $n$ die Aussage $(\star)$ für $n + 1$ – dies ist der Induktionsschritt.

Nun $(\star\star)$:
Sicher ist: $2 - \frac{2}{2} = 1 \leq \frac{1}{2^0}$

Nun folgt der Induktionsschritt:
Von $(\star)$ gilt: $\frac{2}{a_n} < a_n$ oder $\frac{1}{a_n} < \frac{a_n}{2}$
Dies zeigt: $a_{n+1} = \frac{1}{a_n} + \frac{a_n}{2} < a_n$
und damit auch: $\frac{2}{a_n} < \frac{2}{a_{n+1}}$, so dass das neue Intervall jeweils im Vorherigen liegt.

Weiter ist $a_{n+1}$ der Mittelwert der vorherigen Intervallgrenzen. Zusammen folgt, dass sich die Länge des Fehlerintervalles in jedem Schritt mindestens halbiert.

[2] das KANN man sehen, wenn man die gefundenen Werte für die Grenzen vergleicht

**Zentrale Strategie der Analysis: „Konstruktion durch Approximation“**
Zuerst haben wir die Formeln experimentell beobachtet, dann haben wir sie bewiesen.

1. $a_n \mapsto (\frac{1}{a_n} + \frac{a_n}{2}) := a_{n+1}$ ,mit $n \geq 1$, $a_1 := 2$
2. $a_{n+1} := \frac{1}{a_n} + \frac{a_N}{2} > \sqrt{2}$ immer zutrifft $\forall n \in \mathbb{N}$
   $\Leftrightarrow (\frac{1}{a_n} - \frac{a_1}{2})^2 > 0$
   $\frac{2}{a_n} < \sqrt{2} < a_n$ ,$\forall n \in \mathbb{N}$ so dass $a_{n+1} < a_n$

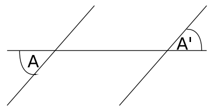
## 1.2 Beweisprinzipien

### 1.2.1 Direkter Beweis

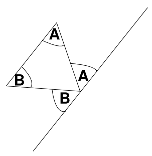
Behauptung A :=„Die Winkelsumme im $\triangle$ beträgt 180°“.

Ausgehend von einer Liste (ausdrücklicher/ stillschweigender) Vereinbarungen (Axiome), schreibt man eine Kette von richtigen Aussagen/ Schlußfolgerungen auf, deren letztes Glied die Behauptung A darstellt.

Zum Beweis der Aussage A:
Axiom: Wechselwinkel an Parallelen sind gleich.




Behautpung A ergibt sich beinahe unmittelbar aus dem Axiom.




**Aufgabe:** Formuliere die einzelnen Sätze der Schlussfolgerungskette.

### 1.2.2 Gerüst eines indirekten Beweises der Aussage/Behauptung $A$

1. Außer den vereinbarten Axiomen, nehmen wir zusätzlich an, dass $A$ falsch sei.
2. Eine Kette von erlaubten Schlußfolgerungen (meistens bequeme Umformulierungen) führt zu einer offensichtlich falschen Aussage: z.B.: „$1 = 0$“
3. Aus 2. schließen wir: Negation der Behauptung unmöglich; also gilt die Behauptung

Also: Um eine Behauptung zu beweisen:
Verneine sie $\Rightarrow$ Widerspruch $\Rightarrow$ Verneinung ist falsch, daher stimmt die Behauptung.

**Beispiel.** Behauptung: $\sqrt{2}$ ist irrational.
Annahme: Behauptung sei falsch: $\sqrt{2}$ ist rational.

Dann gibt es zwei ganze Zahlen $Z, N \in \mathbb{Z}$ mit $\sqrt{2} = \frac{Z}{N}$; in bereits in gekürzter Fassung.
Es folgt: $Z^2 = 2N^2 \rightarrow Z$ ist auf jeden Fall gerade: $Z = 2Y$ und folglich ist $N$ ungerade.
Also $4Y^2 = 2N^2$ bzw. $2Y^2 = N^2 \leftarrow N$ gerade $\Rightarrow$ Widerspruch

**Variante:**
$\sqrt{2} = \frac{Z}{N} \Leftrightarrow 2 = \frac{Z^2}{N^2} \Leftrightarrow 2N^2 = Z^2$

**Euklid.** *Jede natürliche Zahl hat eine eindeutige Primfaktorzerlegung.*

Primfaktorzerlegung von $Z, N$ eingesetzt.

$\underbrace{2\underbrace{N \cdot N}_{2}}_{1} = \underbrace{Z \cdot Z}_{2},$

wobei 1 eine ungerade Anzahl von Primfaktoren bedeutet und 2 eine gerade.

## 2 Körperaxiome

Frage: „Nach welchen Regeln rechnet man mit Zahlen?“
„Kann man mit anderen Dingen nach denselben Regeln rechnen?“

Wenn wir betonen wollen, dass wir beim Rechnen garantiert nichts anderes als die aufgeführten Regeln verwenden wollen, dann nennen wir diese Regeln Axiome.

Regeln für das Rechnen mit $\mathbb{Q} \rightarrow$ Nennen wir diese **Körperaxiome**.

**Körperaxiome:** 9 Rechenregeln für die zwei Verknüpfungen:
Addition $(+)$ und Multiplikation $(\cdot)$

Also zwei Abbildungen:
$$\begin{array}{lll} + & : (a,b) & \mapsto & a+b \\ \cdot & : (a,b) & \mapsto & a \cdot b \end{array}$$

| | | | |
|---|---|---|---|
| AA | Assoziativgesetz der Addition | $a+(b+c)=(a+b)+c$ | $\forall a,b,c \in K$ |
| KA | Kommutativgesetz der Addition | $a+b=b+a$ | $\forall a,b \in K$ |
| NA | Existenz des neutralen Elementes d. Addition | $a+0=a$ | $\forall a \in K$ |
| IA | Es gibt ein inverses Element bzgl. d. Addition | $\forall\, a\, \exists\, b$ , so dass $a+b=0$ | $\forall a,b \in K$ |
| AM | Assoziativgesetz der Multiplikation | $a(b\cdot c)=(a\cdot b)c$ | $\forall a,b,c \in K$ |
| KM | Kommutativgesetz der Multiplikation | $a\cdot b=b\cdot a$ | $\forall a,b \in K$ |
| NM | Existenz d. neutralen Elementes d. Multiplikation | $a\cdot 1=a$ | $\forall a,b \in K$ |
| IM | Es gibt ein inverses Element bzgl. d. Multiplikation | $\forall\, a \neq 0,\ \exists\, b$ , so dass $a\cdot b=1$ | $\forall a,b \in K$ |
| D | Distributibgesetz | $a\cdot(b+c)=(ab)+(bc)$ | $\forall a,b,c \in K$ |

Eine Menge $K$, in der die zwei Verknüpfungen $+$ und $\cdot$ definiert sind, so dass die 9 Körperaxiome gelten, nennt man **Körper**.

Gegenbeispiel: Die Verknüpfung durch Division ist:

- weder assoziativ $(1:2):3=\frac{1}{6}\neq 1:(2:3)$
- noch kommutativ $4:5\neq 5:4$

## 2.1 Beispiele für Körper:

$\mathbb{Q},\mathbb{R},\mathbb{C}$ sind Körper, $\mathbb{Z}$ nicht, da die Multiplikation nicht invertierbar ist.
Mit rationalen Zahlen können wir direkt rechnen. $(\frac{1}{2}+\frac{3}{4})^2=\frac{25}{16}$

Bei zum Beispiel $\pi+\sqrt{7}$ formen wir mit den Regeln um:

$$\begin{aligned}(\pi+\sqrt{7})^2 &= (\pi+\sqrt{7})(\pi+\sqrt{7}) \overset{\text{D}}{=} \pi(\pi+\sqrt{7})+\sqrt{7}(\pi+\sqrt{7})\\ &\overset{\text{D}}{=} \pi^2+\pi\sqrt{7}+\sqrt{7}\pi+7 \overset{\text{KM}}{=} \pi^2+\sqrt{7}\pi+\sqrt{7}\pi+7\\ &\overset{\text{NM}}{=} \pi^2+1\cdot\sqrt{7}\cdot\pi+1\cdot\sqrt{7}\cdot\pi+7\\ &\overset{\text{D}}{=} \pi^2+(1+1)\cdot\sqrt{7}\cdot\pi+7\\ &= \pi+2\sqrt{7}\pi+7\end{aligned}$$

Es gibt eine Fülle von Körpern, die nur endlich viele Elemente enthalten.

### 2.1.1 Beispiele für das Endzifferrechnen

**Beispiel 1.** Rechnen mit Endziffern im Zehnersystem $\{0, 1, 2, 3, \dots, 9\}$

$$3 + 9 = 2 \qquad\qquad 3 \cdot 9 = 7$$

| | | | |
|---|---|---|---|
| Inversion bzgl. | Addition | $a + (10 - a) = 0$ | IA **ok** |
| | Multiplikation | $2 \cdot 5 \neq 1$ | IM **f.** |
| | | 2 hat kein inv. El. | |

Alle anderen Körperaxiome sind erfüllt.

$\Rightarrow$ Menge $\{0, 1, 2, \dots, 9\}$ mit $+, \cdot$ ist kein Körper.

**Beispiel 2.** Rechnen mit Endziffern im Zahlensystem zur Basis 5

| $+$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 0 |
| 1 | 2 | 3 | 4 | 0 | 1 |
| 2 | 3 | 4 | 0 | 1 | 2 |
| 3 | 4 | 0 | 1 | 2 | 3 |
| 4 | 0 | 1 | 2 | 3 | 4 |

| $\cdot$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

- Spiegelsymmetrie an Diagonalen $\Leftrightarrow$ KA, KM **ok**
- $\exists$ neutrales Element $\Rightarrow$ NA, NM **ok**
- Assoziativität gilt (nicht offensichtlich) $\Rightarrow$ AA, AM **ok**
- Inverse Element: Zahl „über 0 bzw. 1“ $\Rightarrow$ IA, IM **ok**

$\Rightarrow$ Alle Körperaxiome erfüllt.

Wir nennen die Menge $\{0, 1, 2, 3, 4\}$ zusammen mit Verknüpfungen $+, \cdot$ der Körper $\mathbb{F}_5$.

## 2.2 Drei Folgerungen aus den Körperaxiomen

1. $x = -(-x)$

   **<u>Beweis:</u>** $-(-x)$ ist das negative Element zu $-x$

$$\begin{aligned} \text{also gilt:}\quad 0 &\overset{\text{IA}}{=} -(-x) + (-x) \\ x &= [-(-x) + (-x)] + x \\ &\overset{\text{AA}}{=} -(-x) + (-x + x) \\ &\overset{\text{IA}}{=} -(-x) + 0 \\ &\overset{\text{NA}}{=} -(-x) \end{aligned}$$

2. $x \cdot 0 = 0$

   Wegen NA ist $0 + 0 = 0$, daher ist

$$x \cdot 0 + x \cdot 0 \overset{\text{D}}{=} x \cdot (0 + 0) = x \cdot 0 \Leftrightarrow x \cdot 0 = 0$$

3. $xy = (-x)(-y)$

   **Beweis:** zunächst $-x = (-1) \cdot x$, denn

$$x + (-1) \cdot x \overset{\text{NM}}{=} 1 \cdot x + (-1) \cdot x \overset{\text{D}}{=} (1 - 1) \cdot x \overset{\text{IA}}{=} 0 \cdot x = 0$$

   Also:

$$(-x) \cdot (-y) \overset{\text{NM}}{=} (-x)(-1)y \overset{\text{KM}}{=} (-(-x)) \cdot y = x \cdot y$$

# 3 Rechnen mit Kongruenzen

Sei $m$ eine beliebige, aber fest gewählte ganze Zahl.

Setze: $\mathbb{Z}m = \{km : k \in \mathbb{Z}\}$ (Menge der ganzen Vielfachen von m)

Für $a, b \in \mathbb{Z}$ gilt offenbar $a - b \in \mathbb{Z}m \Leftrightarrow m$ ein Teiler von $a - b$

Wir sagen dann: $a$ ist **kongruent zu** $b \mod m$

$$\boxed{a \equiv b \pmod{m}}$$

Wenn $m > 0$, so ist $a \equiv b \pmod{m} \Leftrightarrow a$ und $b$ haben bei der Division den selben Rest.
d.h. $a = m \cdot p + r \quad ; \quad b = m \cdot q + r$

## 3.1 Eigenschaften

Die Relation $a \equiv b \pmod{m}$ erfüllt für alle $a, b, c \in \mathbb{Z}$:

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$
   $\Rightarrow a \equiv c \pmod{m}$

## 3.2 Rechenregeln

Seien $a, a', b, b' \in \mathbb{Z}$, mit $a = a' \bmod m$ und $b = b' \bmod m$

Dann ist

1. $a + b = a' + b' \bmod m$
2. $ab = a'b' \bmod m$

**Beweis:** Es gibt $k, l \in \mathbb{Z}$ mit $a - a' = km$ und $b - b' = lm$

Daher: $(a + b) - (a' + b') = (a - a') + (b - b') = km + lm = (k + l)m$ (1.)

Ferner: $ab - a'b' = (a - a')b + a(b - b') = km \cdot b + lm \cdot a = (kb + la)m$ (2.)

Zu $a \in \mathbb{Z}$ setze:

$$[a] := a + \mathbb{Z}m = \{a + km : k \in \mathbb{Z}\} = \{b : a \equiv b \pmod{m}\}$$

**Kongruenzklasse** (bzw. **Restklasse**) von $a$ mod $m$

Es gilt immer $a \in [a]$, insbes. $[a] \neq \phi$

Rechnen mit Kongruenzklassen ist einfacher als Rechnen mit ganzen Zahlen!

**Bsp 1.** Die Uhrzeit: Ziffernblatt der Uhr zeigt 1 bis 12 Stunden: 3 Uhr + 17 Stunden $\rightarrow$ 8 Uhr

Bei der Uhrzeit rechnen wir modulo 12

$[3] = \{\dots, -21, -9, 3, 15, 27, \dots\}$
$[7] = \{\dots, -7, 5, 17, 29, \dots\}$

**Bsp 2.** Winkelmessungen in Grad ist mod 360°

**Bsp 3.** von Datum $\rightarrow$ Rechnung mod 7
http://www.math.uni-bonn.de/people/gw/kalender.html

Die Menge aller Kongruenzklassen nennen wir $\mathbb{Z}$ modulo $m$; schreibe:

$$\mathbb{Z}/m := \{[a] : a \in \mathbb{Z}\}$$

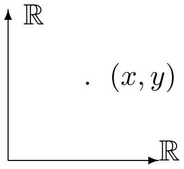
# 4 Gruppen

## 4.1 Definition

Notation: $A$, $B$ beliebige Mengen; das **kartesische[3] Produkt von** $A$ **und** $B$,

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

ist die Menge aller aus je einem Element aus $A$ und aus $B$ gebildeten geordneten Paare $(a, b)$, wobei $a \in A$ , $b \in B$.




$(x, y) \in \mathbb{R} \times \mathbb{R}$, kurz $\mathbb{R}^2$
Analog $\mathbb{R}^3$ ist die Menge $\{(x, y, z) : x, y, z \in \mathbb{R}\}$ aller geordneten Tripel.
$\Rightarrow$ allg. $\mathbb{R}^n$ - Menge aller **n-Tupel** $(x_1, x_2, \ldots, x_n)$

Bezeichne für eine beliebige Menge $A$, die Anzahl ihrer Elemente mit $|A|$.

**Definition 4.1.** *Eine* ***Gruppe*** $(G, \Box)$ *ist eine Menge* $G$ *zusammen mit einer Verknüpfung*
*($\Box : G \times G \to G$, bzw. $(g, h) \mapsto g \Box h$), die folgende Eigenschaften hat:*

1. Assoziativgesetz $\forall g, h, k \in G$ gilt:

$$(g \Box h) \Box k = g \Box (h \Box k)$$

2. $\exists e \in G$ (neutrales Element), so dass gilt:

   a) $\forall g \in G$, $e \Box g = g = g \Box e$

   b) $\forall g \in G$, $\exists h \in G$ mit $g \Box h = h \Box g = e$

   - Das **neutrale Element** e ist **eindeutig**
   - Das zu g **inverse Element** h ist auch **eindeutig**, wir können es als $g^{-1}$ schreiben

3. Kommutativgesetz wird **nicht** verlangt (**kann** gelten, muss nicht)

   Falls weiter gilt: $g \Box k = k \Box g \quad \forall g, k \in G$
   nennen wir die Gruppe **kommutativ** oder **abelsch** [4]

[3] nach René Descartes (1596–1650)
[4] nach Niels Henrik Abel (1802-1829)

## 4.2 Beispiele

0. Die zugrunde liegende Menge G muss mindestens das neutrale Element enthalten, sie darf nicht leer sein.

   Menge $\{e\}$ erfüllt die Gruppenaxiome → die **triviale** Gruppe $G = \{e\}$

1. Menge der ganzen Zahlen $\mathbb{Z}$ mit Addition als Verknüpfung: $\square := +$

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$+ : (a, b) \mapsto a + b$$

   Neutrales Element ist die 0.

   Inverses Element zu $g = -g$.

   Diese Gruppe ist **kommutativ**.

2. $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind ebenfalls kommutative Gruppen

   $(\mathbb{N}, +)$ ist **keine** Gruppe (inverses Element fehlt)

## 4.3 Körper

Nun ist eine Beschreibung von Körpern mit neuen Worten möglich:

**Definition 4.2.** *Ein **Körper** ist eine Menge K zusammen mit zwei Verknüpfungen:*

$$\begin{aligned} + : \mathbb{K} \times \mathbb{K} &\to \mathbb{K} \\ (a, b) &\mapsto a + b \end{aligned} \qquad \begin{aligned} \cdot : \mathbb{K} \times \mathbb{K} &\to \mathbb{K} \\ (a, b) &\mapsto a \cdot b \ , \end{aligned}$$

*die folgenden Axiomen genügen:*

**(K1)** $(\mathbb{K}, +)$ *ist eine abelsche (kommutative) Gruppe mit neutralem Element* $0 \in \mathbb{K}$[5]

**(K2)** $(\mathbb{K} - \{0\}, \cdot)$ *ist eine kommutative Gruppe mit neutralem Element* $1 \in \mathbb{K} - \{0\}$[6]

**(K3)** $\forall a, b, c \in \mathbb{K}$ *gelten die Distributivgesetze*

1. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
2. $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

[5] Muss also AA, IA, NA, KA erfüllen.
[6] Muss also AM, IM, NM, KM erfüllen.

## 4.4 Einige Eigenschaften von Funktionen (Abbildungen)

Seien $X, Y$ beliebige Mengen.

Eine **Abbildung** (oder Funktion) von $X$ nach $Y$ ist eine Vorschrift $f$, die für jedes Element $x \in X$ ein bestimmtes Element $y =: f(x) \in Y$ als **Bildelement** (oder Funktionswert) festlegt.

Wir schreiben $\begin{array}{rcl} f : X & \to & Y \\ x & \mapsto & f(x) \end{array}$

Die Menge $X =: Dom(f)$ heißt **Defintionsbereich** (domain) von $f$. $Y$ ist der **Zielbereich** (range) von $f$.

Die Menge der tatsächlich angenommenen Werte

$$Im(f) := \{y \in Y : \exists x \in X : y = f(x)\}$$

heißt Bild oder **Bildmenge** (Image) oder **Wertebereich** von $f$.

**Definition 4.3.**

1. *Eine Abbildung $f : X \to Y$ heißt **surjektiv**, falls es zu jedem $y \in Y$ ein $x \in X$ mit $f(x) = y$ gibt, also wenn $f(X) = Y$.*

   *Jedes Element der Zielmenge $Y$ ist erreicht.*

2. *Die Abbildung $f : X \to Y$ heißt **injektiv** (eineindeutig), wenn sie verschiedene Elemente in $X$ auf verschiedene Elemente in $Y$ abbildet,*
   *d.h. wenn aus $f(x_1) = f(x_2)$ folgt: $x_1 = x_2$.*

   *In anderen Worten: Ist $x_1 \neq x_2$, so muss auch $f(x_1) \neq f(x_2)$ sein [7].*

3. *Eine Abbildung, die sowohl surjektiv als auch injektiv ist, heißt **bijektiv**.*

Eine Menge $X$ heißt **abzählbar**, wenn eine bijektive Abbildung $f : \mathbb{N} - \{0\} \to X$ existiert.

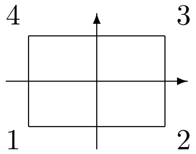
**Bsp.** Betrachten wir eine abzählbare Menge $X$ mit endlicher Zahl $n$ an Elementen.

Jedem Objekt in $X$ können wir eine Zahl aus $\{1, 2, \ldots, n\}$ zuordnen, so dass jeder Zahl ein Element zugeordnet wird.

Anschaulicher können wir dann $X = \{1, 2, \ldots, n\}$ setzen. Eine bijektive Abbildung $f : X \to X$ ist einfach eine neue Zuordnung, bzw. Umordnung der Zahlen.

[7] Übrigens ein Beispiel für die Kontraposition. (s. S. **??**)

## 4.5 Beispiel einer Symmetriegruppe




$X = \{$Ecken eines Rechtecks mit ungleichen Seiten$\}$
Man ordnet den Ecken $\{1, 2, 3, 4\}$ zu $\rightarrow$ die Menge ist abzählbar.

bijektive Abbildungen:

$$
\begin{aligned}
e &: (1,2,3,4) \rightarrow (1,2,3,4) && \text{neutrale Abbildung} \\
f &: (1,2,3,4) \rightarrow (4,3,2,1) && \text{Spiegelung an der x-Achse} \\
g &: (1,2,3,4) \rightarrow (2,1,4,3) && \text{Spiegelung an der y-Achse} \\
h &: (1,2,3,4) \rightarrow (3,4,1,2) && \text{Drehung um } 180^\circ X
\end{aligned}
$$

**Definition 4.4.** *$f : X \rightarrow Y$ und $g : Y \rightarrow Z$ sind zwei Abbildungen. Die* ***Komposition*** *(Verkettung) $g \circ f$ von $g$ mit $f$ ist definiert als:*

$$g \circ f : X \rightarrow Z$$

$$
\begin{tikzcd}
X \arrow[r, "f"] \arrow[rr, bend right, "g\circ f"'] & Y \arrow[r, "g"] & Z
\end{tikzcd}
$$

$$g \circ f(\underbrace{x}_{\in X}) := g(\underbrace{f(x)}_{\in Y})$$

$$
\begin{tikzcd}
(1,2,3,4) \arrow[r, "f"] \arrow[rr, bend right, "g\circ f=h"'] & (4,3,2,1) \arrow[r, "g"] & (3,4,1,2)
\end{tikzcd}
$$

$$
\begin{tikzcd}
(1,2,3,4) \arrow[r, "g"] \arrow[rr, bend right, "g\circ f=h=f\circ g"'] & (2,1,4,3) \arrow[r, "f"] & (3,1,4,2)
\end{tikzcd}
$$

**Aufgabe:** Menge der obigen Abbildungen $\{e, f, g, h\}$ bilden eine kommutative Gruppe. (**Beweis als Übung**)

## 4.6 Beispiel einer nicht-kommutativen (nicht-abelschen) Gruppe

Permutation[8] von Zahlen 1 bis 3.

Wir schreiben für $f : (1, 2, 3, 4) \rightarrow (f(1), f(2), f(3), f(4))$

$$
\text{kürzer:} f = \left(\begin{array}{cccc}
1 & 2 & 3 & 4 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
f(1) & f(2) & f(3) & f(4)
\end{array}\right)
$$

[8]**Def.:** Umordnung im Sinne einer bijektiven Abbildung

So findet man für alle Permutationen:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

**Komposition der Abbildungen:**

klar[9]:

$$e \circ a = a, \qquad e \circ b = b, \qquad \text{usw.}$$
$$a \circ e = a, \qquad b \circ e = b, \qquad \text{usw.}$$

aber:

$$a \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = d$$
$$b \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f$$

also $a \circ b \neq b \circ a \leftrightarrow$ nicht kommutativ

**Inverse?**

$a$ vertauscht $1, 2$ also $a^2 = e \Rightarrow a = a^{-1}$. Analog für $b$ und $c$.

Was passiert für $d$ und $f$? Was sind $d^{-1}, f^{-1}$?

$$d^{-1} = d^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f$$
$$f^{-1} = f^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = d$$

**Aufgabe:** Die Permutationen von Zahlen bilden eine Gruppe (Übung).

[9] Das neutrale Element bildet per Definition auf sich selbst ab.

# 5 Kurzer Ausflug in die Logik

Seien $A, B$ Aussagen.

Mathematische Sachverhalte können oft in Form einer **Implikation**

$$A \Rightarrow B \quad \text{oder „}A\text{ hat }B\text{ zur Folge“}$$

ausgedrückt werden.

**Interpretation:** Vielleicht trifft $A$ zu, vielleicht auch nicht.
Es gilt nur: Falls $A$ zutrifft, trifft auch $B$ zu. $B$ kann aber wahr sein und gleichzeitig $A$ falsch, d.h. die **Umkehrung** $B \Rightarrow A$ ist mitnichten bewiesen.

Logisch äquivalent zur Implikation $A \Rightarrow B$ ist deren Kontraposition: Wenn $B$ nicht zutrifft, dann trifft auch sicher $A$ nicht zu ($\neg B \Rightarrow \neg A$).

Äquivalenz: Falls $A \Rightarrow B$ und $B \Rightarrow A$, dann schreiben wir

$$A \Leftrightarrow B \quad \text{oder „}A\text{ gilt genau dann, wenn }B\text{ gilt“}$$

Also, Kontraposition $\neg B \Rightarrow \neg A \quad \Leftrightarrow \quad A \Rightarrow B$.

Für einige immer wieder gebrauchte Aussagen führen wir abgekürzte Schreibweisen mittels Symbole ein. Wir benötigen dazu die sogenannten Quantoren, die Zeichen $\forall$, $\exists$, $\exists!$, $\nexists$.

| Symbol | Bedeutung |
|---|---|
| $\forall$ | für alle |
| $\exists$ | es gibt |
| $\exists!$ | es gibt genau ein |
| $\nexists$ | es gibt kein |
| $a \in M$ | $a$ ist ein Element der Menge $M$ |
| $a \ni M$ | $a$ ist kein Element der Menge $M$ |
| $\emptyset$ | leere menge (Menge ohne Elemente) |
| $\{x \in M \| A(x)\}$ | Menge der $x \in M$, für die die Aussage A(x) gilt |
| $\forall x \in M \quad A(x)$ | für alle $x \in M$ gilt die Aussage A(x) |
| $\exists x \in M \quad A(x)$ | es gibt ein $x \in M$ mit der Aussage A(x) |
| $A \wedge B$ | $A$ und $B$ |
| $A \vee B$ | $A$ oder $B$ |
| $\neg A$ | nicht $A$; Verneinung der Aussage $A$ |

Die Symbole $\wedge, \vee, \neg$ werden wir recht selten benutzen.