# Lösungen der Übungsaufgaben von Kapitel 1

## zu 1.2

**1.2.1** Für Teilmengen $A, B, C$ einer Menge $M$ beweise man:

1. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
   Zwei Mengen $M, N$ heißen gleich, wenn gilt : $M \subset N \wedge N \subset M$

   (a) Man zeigt zunächst $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$, d.h.
   $x \in (A \cap B) \cup C \Rightarrow x \in (A \cup C) \cap (B \cup C)$

   Sei $x \in (A \cap B) \cup C$, dann gilt :

   $$\begin{aligned} & x \in (A \cap B) \cup C \\ \overset{\text{Definition von } \cup}{\Longrightarrow} \quad & x \in A \cap B \vee x \in C \end{aligned}$$

   Man unterscheidet nun zwei Fälle :

   i. $x \in A \cap B$
      Es gilt :

   $$\begin{aligned} & x \in A \cap B \\ \overset{\text{Definition von } \cap}{\Longrightarrow} \quad & x \in A \wedge x \in B \end{aligned}$$

   Mit $x \in A$ gilt wegen der Definition von $\cup$ auch $x \in A \cup C$, genauso folgt $x \in B \cup C$ aus $x \in B$, damit gilt:

   $$\begin{aligned} & x \in A \wedge x \in B \\ \Longrightarrow \quad & x \in A \cup C \wedge x \in B \cup C \\ \overset{\text{Definition von } \cap}{\Longrightarrow} \quad & x \in (A \cup C) \cap (B \cup C) \end{aligned}$$

   Dies war zu zeigen.

   ii. $x \in C$
       Aus $x \in C$ folgt aufgrund der Definition von $\cup$ sowohl $x \in A \cup C$, als auch $x \in B \cup C$, daher gilt :

   $$\begin{aligned} & x \in C \\ \Longrightarrow \quad & x \in A \cup C \wedge x \in B \cup C \\ \overset{\text{Definition von } \cap}{\Longrightarrow} \quad & x \in (A \cup C) \cap (B \cup C) \end{aligned}$$

   Dies war zu zeigen.

   In beiden Fällen folgt $x \in (A \cup C) \cap (B \cup C)$, daher gilt :
   $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$

(b) Als nächstes zeigt man $(A \cup C) \cap (B \cup C) \subset (A \cap B) \cup C$, d.h.
$x \in (A \cup C) \cap (B \cup C) \Longrightarrow x \in (A \cap B) \cup C$

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

$$\begin{aligned} & x \in (A \cup C) \cap (B \cup C) \\ \overset{\text{Definition von } \cap}{\Longrightarrow} \quad & x \in A \cup C \wedge x \in B \cup C \\ \overset{\text{Definition von } \cup}{\Longrightarrow} \quad & (x \in A \vee x \in C) \wedge (x \in B \vee x \in C) \quad (*) \end{aligned}$$

Man unterscheidet nun zwei Fälle :

i. $x \in C$
$\overset{\text{Definition von } \cup}{\Longrightarrow} \quad x \in (A \cap B) \cup C$
Dies war zu zeigen.

ii. $x \notin C$
$\overset{(*),\text{ Definition von } \cap, \cup}{\Longrightarrow} \quad x \in A \wedge x \in B$
$\overset{\text{Definition von } \cap}{\Longrightarrow} \quad x \in A \cap B$
$\overset{\text{Definition von } \cup}{\Longrightarrow} \quad x \in (A \cap B) \cup C$
Dies war zu zeigen.

In beiden Fällen folgt $x \in (A \cap B) \cup C$, also gilt :
$(A \cup C) \cap (B \cup C) \subset (A \cap B) \cup C$

Es gilt also $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

2. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
Zwei Mengen $M, N$ heißen gleich, wenn gilt : $M \subset N \wedge N \subset M$

(a) Man zeigt zunächst $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$, d.h.
$x \in (A \cap B) \cup C \Rightarrow x \in (A \cup C) \cap (B \cup C)$

Sei $x \in (A \cup B) \cap C$, dann gilt :

$$\begin{aligned} & x \in (A \cup B) \cap C \\ \overset{\text{Definition von } \cap}{\Longrightarrow} \quad & x \in A \cup B \wedge x \in C \\ \overset{\text{Definition von } \cup}{\Longrightarrow} \quad & (x \in A \vee x \in B) \wedge x \in C \end{aligned}$$

$x \in C$ gilt also auf jeden Fall, zusätzlich gilt noch $x \in A$ oder $x \in B$. Wenn $x \in A$ gilt, gilt mit $x \in C$ aber auch $x \in A \cap C$, analog gilt : $x \in B \quad \overset{x \in C}{\Longrightarrow} \quad x \in B \cap C$. Daher folgt :

$$\begin{aligned} & (x \in A \vee x \in B) \wedge x \in C \\ \Longrightarrow \quad & x \in A \cap C \vee x \in B \cap C \\ \overset{\text{Definition von } \cup}{\Longrightarrow} \quad & x \in (A \cap C) \cup (B \cap C) \end{aligned}$$

Dies war zu zeigen. Es gilt : $(A \cup B) \cap C \subset (A \cap C) \cup (B \cap C)$

(b) Als nächstes zeigt man $(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C$, d.h.
$x \in (A \cap C) \cup (B \cap C) \Longrightarrow x \in (A \cup B) \cap C$

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

$$\begin{aligned} & x \in (A \cap C) \cup (B \cap C) \\ \overset{\text{Definition von}}{\underset{\cup}{\Longrightarrow}} \quad & x \in A \cap C \vee x \in B \cap C \end{aligned}$$

Man unterscheidet zwei Fälle :

i. $x \in A \cap C$:
Es gilt :

$$\begin{aligned} & x \in A \cap C \\ \overset{\text{Definition von}}{\underset{\cap}{\Longrightarrow}} \quad & x \in A \wedge x \in C \\ \overset{\text{Definition von}}{\underset{\cup}{\Longrightarrow}} \quad & x \in A \cup B \wedge x \in C \\ \overset{\text{Definition von}}{\underset{\cap}{\Longrightarrow}} \quad & x \in (A \cup B) \cap C \end{aligned}$$

Dies war zu zeigen.

ii. $x \in B \cap C$:
Es gilt :

$$\begin{aligned} & x \in B \cap C \\ \overset{\text{Definition von}}{\underset{\cap}{\Longrightarrow}} \quad & x \in B \wedge x \in C \\ \overset{\text{Definition von}}{\underset{\cup}{\Longrightarrow}} \quad & x \in A \cup B \wedge x \in C \\ \overset{\text{Definition von}}{\underset{\cap}{\Longrightarrow}} \quad & x \in (A \cup B) \cap C \end{aligned}$$

Dies war zu zeigen.

In beiden Fällen gilt : $x \in (A \cup B) \cap C$, damit folgt :
$(A \cap C) \cup (B \cap C) \subset (A \cup B) \cap C$

Es gilt also $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

$A^c$ sei das Komplement von $A$ bzgl. $M$, also $A^c := \{x \in M \mid x \notin A\}$.

1. $(A \cup B)^c = A^c \cap B^c$
Zwei Mengen $M, N$ heißen gleich, wenn gilt : $M \subset N \wedge N \subset M$

(a) Man zeigt zunächst $(A \cup B)^c \subset A^c \cap B^c$, d.h.
$x \in (A \cup B)^c \Rightarrow x \in A^c \cap B^c$

Sei $x \in (A \cup B)^c$, dann gilt :

$$
\begin{aligned}
& x \in (A \cup B)^c \\
\overset{\text{Definition von}}{\underset{}{\overset{c}{\Longrightarrow}}} \quad & x \notin A \cup B \\
\overset{\text{Definition von}}{\overset{\cup}{\Longrightarrow}} \quad & x \notin A \wedge x \notin B \\
\overset{\text{Definition von}}{\overset{c}{\Longrightarrow}} \quad & x \in A^c \wedge x \in B^c \\
\overset{\text{Definition von}}{\overset{\cap}{\Longrightarrow}} \quad & x \in A^c \cap B^c
\end{aligned}
$$

Dies war zu zeigen, also gilt :
$(A \cup B)^c \subset A^c \cap B^c$

(b) Als zweites zeigt man $A^c \cap B^c \subset (A \cup B)^c$, d.h.
$x \in A^c \cap B^c \Rightarrow x \in (A \cup B)^c$

Sei $x \in A^c \cap B^c$, dann gilt :

$$
\begin{aligned}
& x \in A^c \cap B^c \\
\overset{\text{Definition von}}{\overset{\cap}{\Longrightarrow}} \quad & x \in A^c \wedge x \in B^c \\
\overset{\text{Definition von}}{\overset{c}{\Longrightarrow}} \quad & x \notin A \wedge x \notin B \\
\overset{\text{Definition von}}{\overset{\cup}{\Longrightarrow}} \quad & x \notin A \cup B \\
\overset{\text{Definition von}}{\overset{c}{\Longrightarrow}} \quad & x \in (A \cup B)^c
\end{aligned}
$$

Dies war zu zeigen, also gilt :
$A^c \cap B^c \subset (A \cup B)^c$

Es gilt : $(A \cup B)^c = A^c \cap B^c$.

2. $(A \cap B)^c = A^c \cup B^c$
Zwei Mengen $M, N$ heißen gleich, wenn gilt : $M \subset N \wedge N \subset M$

(a) Man zeigt zunächst $(A \cap B)^c \subset A^c \cup B^c$, d.h.
$x \in (A \cap B)^c \Rightarrow x \in A^c \cup B^c$

Sei $x \in (A \cap B)^c$, dann gilt :

$$
\begin{aligned}
& x \in (A \cap B)^c \\
\overset{\text{Definition von}}{\overset{c}{\Longrightarrow}} \quad & x \notin A \cap B \\
\overset{\text{Definition von}}{\overset{\cap}{\Longrightarrow}} \quad & x \notin A \vee x \notin B \\
\overset{\text{Definition von}}{\overset{c}{\Longrightarrow}} \quad & x \in A^c \vee x \in B^c \\
\overset{\text{Definition von}}{\overset{\cup}{\Longrightarrow}} \quad & x \in A^c \cup B^c
\end{aligned}
$$

Dies war zu zeigen, also gilt :
$(A \cap B)^c \subset A^c \cup B^c$

(b) Als zweites zeigt man $A^c \cup B^c \subset (A \cap B)^c$, d.h.
$x \in A^c \cup B^c \Rightarrow x \in (A \cap B)^c$

Sei $x \in A^c \cup B^c$, dann gilt :

$$\begin{aligned} & x \in A^c \cup B^c \\ \overset{\substack{\text{Definition von}\\ \cup}}{\Longrightarrow} \quad & x \in A^c \vee x \in B^c \\ \overset{\substack{\text{Definition von}\\ c}}{\Longrightarrow} \quad & x \notin A \vee x \notin B \\ \overset{\substack{\text{Definition von}\\ \cap}}{\Longrightarrow} \quad & x \notin A \cap B \\ \overset{\substack{\text{Definition von}\\ c}}{\Longrightarrow} \quad & x \in (A \cap B)^c \end{aligned}$$

Dies war zu zeigen, also gilt :
$A^c \cup B^c \subset (A \cap B)^c$

Es gilt : $(A \cap B)^c = A^c \cup B^c$.

**1.2.2** Welche der folgenden Definitionen ist eine zulässige Abbildungsdefinition:

1. $n \mapsto n^5$, auf $\mathbb{N}_{naiv}$:
   Dies ist eine Abbildung, da jedem Element $n$ aus $\mathbb{N}_{naiv}$ eindeutig das Element $n^5$ zugeordnet wird.

2. $n/m \mapsto n/m^2$, auf $\mathbb{Q}_{naiv}$:
   Dies ist keine zulässige Abbildungsdefinition, da nicht jedem Element $n/m \in \mathbb{Q}_{naiv}$ eindeutig ein Element zugeordnet wird.
   Es genügt ein Gegenbeispiel:
   Es gilt $1/2 \mapsto 1/4$ und gleichzeitig $1/2 = 2/4 \mapsto 2/16 = 1/8$. Da aber $1/4 \neq 1/8$ ist, liegt keine eindeutige Zuordnungsvorschrift vor.

3. $(x_1, \ldots, x_m) \mapsto x_m$, auf $\mathbb{K}^m$:
   Dies ist eine zulässige Abbildungsvorschrift.
   Sind $\vec{x} = (x_1, \ldots, x_m)$, $\vec{y} = (y_1, \ldots, y_m) \in \mathbb{K}^m$ zwei gleiche Elemente, dann gilt $x_i = y_i$ für $i = 1, \ldots, m$. Insebsondere gilt dann, dass $x_m = y_m$, was aber genau bedeutet, dass die Bilder von $\vec{x}$ und $\vec{y}$ miteinander übereinstimmen.

## zu 1.3

**1.3.1** Diskutieren Sie die innere Verknüpfung

$$\circ : \ (x,y) \mapsto \frac{x}{y} + \frac{y}{x}$$

auf $\mathbb{R} \setminus \{0\}$: Überprüfen Sie auf

1. Wohldefiniertheit,
2. Assoziativität,
3. Kommutativität,
4. Existenz eines neutralen Elements
5. und Existenz von inversen Elementen.

1. $\circ$ ist wohldefiniert:
   Wegen den Verknüpfungen auf $\mathbb{R}$ gilt mit $x, y \in \mathbb{R} \setminus \{0\}$:
   $$\frac{x}{y} + \frac{y}{x} \ = \frac{x^2 + y^2}{xy}.$$
   Aufgrund der Abgeschlossenheit der bekannten Verknüpfungen auf $\mathbb{R}$ liegt $\frac{x^2+y^2}{xy}$ wieder in $\mathbb{R}$.
   Es bleibt zu zeigen, dass $\frac{x^2+y^2}{xy} \neq 0$ ist: Aufgrund von Satz 1.3.6 ist mit $x, y \neq 0$ auch $xy \neq 0$ und somit auch $(xy)^{-1} \neq 0$; außerdem ist dann auch $x^2, y^2 \neq 0$ und wegen Satz 1.4.3 $x^2 + y^2 \neq 0$. Nochmalige Anwendung von Satz 1.3.6 liefert uns $\frac{x^2+y^2}{xy} \neq 0$.
   Folglich ist diese Verknüpfung wohldefiniert.

2. $\circ$ ist nicht assoziativ:
   Es genügt ein Gegenbeispiel:
   Wähle $x = 1, \ y = 1, \ z = 2$, dann gilt
   $$\begin{aligned}
   (x \circ y) \circ z &= \left(\frac{x}{y} + \frac{y}{x}\right) \circ z \\
   &= \frac{\frac{x}{y} + \frac{y}{x}}{z} + \frac{z}{\frac{x}{y} + \frac{y}{x}} \\
   &= \frac{\frac{1}{1} + \frac{1}{1}}{2} + \frac{2}{\frac{1}{1} + \frac{1}{1}} \\
   &= 2 \\
   x \circ (y \circ z) &= x \circ \left(\frac{y}{z} + \frac{z}{y}\right) \\
   &= \frac{x}{\frac{y}{z} + \frac{z}{y}} + \frac{\frac{y}{z} + \frac{z}{y}}{x} \\
   &= \frac{1}{\frac{1}{2} + \frac{2}{1}} + \frac{\frac{1}{2} + \frac{2}{1}}{1} \\
   &= \frac{29}{10}.
   \end{aligned}$$

Da $2 \neq 29/10$, ist die Verknüpfung nicht assoziativ.

3. $\circ$ ist kommutativ:
Seien $x, y \in \mathbb{R} \setminus \{0\}$. Dann gilt wegen der Kommutativität von ‚+' in $\mathbb{R}$
$$x \circ y = \frac{x}{y} + \frac{y}{x} = \frac{y}{x} + \frac{x}{y} = y \circ x.$$
Dies zeigt die Kommutativität.

4. Es existiert kein neutrales Element:
Es reicht zu zeigen, dass zu $1 \in \mathbb{R} \setminus \{0\}$ kein neurtrales Element existiert. Angenommen $e$ ist neutrales Element, dann müsste $1 \circ e = 1$ gelten. Diese Gleichung führt zu der Gleichung
$$\begin{aligned} \frac{1}{e} + \frac{e}{1} &= 1 \\ \Leftrightarrow 1 + e^2 &= e \\ \Leftrightarrow e^2 - e + 1 &= 0, \end{aligned}$$
welche in $\mathbb{R}$ nicht lösbar ist. (Begründung: Bei der Anwendung der p-q-Formel erhält man eine negative Zahl unter der Wurzel bzw. die Funktion $x \mapsto x^2 - x + 1$ hat auf $\mathbb{R}$ keine Nullstelle.)

5. Da kein neutrales Element existiert, können nach Definition auch keine inversen Elemente existieren.

**1.3.2** Sei $(K, \oplus, \odot)$ der Restklassenring modulo $p$, also $K = \{0, 1, 2, \ldots, p-1\}$ und $\oplus$ und $\odot$ gegeben durch :
$$x \oplus y (\text{bzw.} x \odot y) = \begin{cases} \text{Rest der bei Teilen von } x + y \\ (\text{bzw. } \; x \cdot y) \text{ durch p bleibt.} \end{cases}$$
Mit der Modulofunktion ($x \bmod y :=$ Rest von $x$ durch $y$) gilt :
$$\begin{aligned} x \oplus y &= (x + y) \bmod p \\ x \odot y &= (x \cdot y) \bmod p \end{aligned}$$
Ohne Beweis darf benutzt werden :
$$\operatorname{ggT}(x, y) = d \Longrightarrow \exists a, b \in \mathbb{Z}_{naiv} : a \cdot x + b \cdot y = d \tag{1}$$
$$\forall a \in \mathbb{Z}_{naiv} : (x + a \cdot p) \bmod p = x \bmod p \tag{2}$$
$$\forall x \in \mathbb{Z}_{naiv} \exists l \in \mathbb{Z}_{naiv} : x \bmod p = x + l \cdot p \tag{3}$$
Aus (2) und (3) folgt :
$$\forall x, y \in \mathbb{Z}_{naiv} : (x \bmod p + y) \bmod p = (x + y) \bmod p \tag{4}$$
$$\forall x, y \in \mathbb{Z}_{naiv} : (x \bmod p \cdot y) \bmod p = (x \cdot y) \bmod p \tag{5}$$

Beweis: Sei $x, y \in \mathbb{Z}_{naiv}$:

$$\begin{aligned}
(x \bmod p + y) \bmod p &\overset{(3)}{=} (x + l \cdot p + y) \bmod p \\
&\overset{(2)}{=} (x + y) \bmod p \\
(x \bmod p \cdot y) \bmod p &\overset{(3)}{=} [(x + l \cdot p) \cdot y] \bmod p \\
&\overset{\text{Distr. in } \mathbb{Z}_{naiv}}{=} (x \cdot y + l \cdot p \cdot y) \bmod p \\
&\overset{(2)}{=} (x \cdot y) \bmod p
\end{aligned}$$

$\oplus$ und $\odot$ sind innere Verknüpfungen in $K$, da $a \bmod p$ für alle $a \in \mathbb{Z}_{naiv}$ in $K$ liegt und somit auch $(x + y) \bmod p$ und $(x \cdot y) \bmod p$.

Um zu überprüfen, ob $(K, \oplus, \odot)$ ein Körper ist, muß man feststellen, ob alle Körperaxiome (A1, A2, A3, M1, M2, M3, D) für $(K, \oplus, \odot)$ gelten :

1. A1 : $\oplus$ ist assoziativ und kommutativ

   - Kommutativität: $x \oplus y = y \oplus x$
     Seien $x, y \in K$ beliebig :
     Es gilt : $x \oplus y = (x + y) \bmod p$
     Wegen der Kommutativität von ‚+' in $\mathbb{N}_{naiv}$ gilt $x + y = y + x$,
     also : $(x + y) \bmod p = (y + x) \bmod p \overset{\text{Definition von } \oplus}{=} y \oplus x$.
     Es gilt also : $x \oplus y = y \oplus x$, d.h. : $\oplus$ ist kommutativ.
   - Assoziativität : $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
     Es gilt $(x, y, z \in K)$ :

   $$\begin{aligned}
   (x \oplus y) \oplus z &\overset{\text{Definition von } \oplus}{=} [(x + y) \bmod p + z] \bmod p \\
   &\overset{(4)}{=} [(x + y) + z] \bmod p \\
   &\overset{\text{Ass. von } +}{=} [x + (y + z)] \bmod p \\
   &\overset{(4)}{=} [x + (y + z) \bmod p] \bmod p \\
   &\overset{\text{Definition von } \oplus}{=} x \oplus (y \oplus z)
   \end{aligned}$$

   $\oplus$ ist assoziativ.

   A1 ist erfüllt.

2. A2 : Es gibt ein neutrales Element ‚0'bzgl. $\oplus$.

   0 ist das neutrale Element bzgl. $\oplus$, was aus der Neutralität von 0 bzgl. ‚+' in $\mathbb{Z}_{naiv}$ folgt $(x \in K)$:

   $$x \oplus 0 = (x + 0) \bmod p = x \bmod p = x$$
   $$0 \oplus x = (0 + x) \bmod p = x \bmod p = x$$

A2 ist erfüllt.

3. A3 : Es gibt zu jedem $x \in K$ ein Inverses bzgl. $\oplus$.

   Das inverse Element zu $x \in K$ ist $(p-x) \bmod p \in K$ da gilt :

   $$\begin{aligned} x \oplus (p-x) \bmod p &= [x + (p-x) \bmod p] \bmod p \\ &\overset{(4)}{=} (x + p - x) \bmod p \\ &= p \bmod p \overset{\text{Def. von mod}}{=} 0 \end{aligned}$$

   A3 ist erfüllt.

4. M1 : $\odot$ ist assoziativ und kommutativ

   - Kommutativität
     Es gilt : $x \odot y = (x \cdot y) \bmod p$
     Wegen der Kommutativität in $\mathbb{N}_{naiv}$ gilt $x \cdot y = y \cdot x$, also:
     $(x \cdot y) \bmod p = (y \cdot x) \bmod p = y \odot x$.
     Es gilt also : $x \odot y = y \odot x$, d.h. : $\odot$ ist kommutativ.
   - Assoziativität : $(x \odot y) \odot z = x \odot (y \odot z)$
     Es gilt $(x, y, z \in K)$ :

     $$\begin{aligned} (x \odot y) \odot z &\overset{\substack{\text{Definition von} \\ \odot}}{=} [(x \cdot y) \bmod p \cdot z] \bmod p \\ &\overset{(5)}{=} [(x \cdot y) \cdot z] \bmod p \\ &\overset{\text{Ass. von } \cdot}{=} [x \cdot (y \cdot z)] \bmod p \\ &\overset{(5)}{=} [x \cdot (y \cdot z) \bmod p] \bmod p \\ &\overset{\substack{\text{Definition von} \\ \odot}}{=} x \odot (y \odot z) \end{aligned}$$

     $\odot$ ist assoziativ.

   M1 ist erfüllt.

5. M2 : Es gibt ein neutrales Element ‚1'bzgl. $\odot$.

   1 ist das neutrale Element bzgl. $\odot$, was aus der Neutralität von 1 bzgl. ‚·' in $\mathbb{Z}_{naiv}$ folgt $(x \in K)$ :

   $$x \odot 1 = (x \cdot 1) \bmod p = x \bmod p = x$$
   $$1 \odot x = (1 \cdot x) \bmod p = x \bmod p = x$$

   M2 ist erfüllt.

6. M3 : Es gibt zu jedem $x \in K \setminus \{0\}$ ein Inverses bzgl. $\odot$.

   Man unterscheidet hier zwei Fälle :

   - $p$ ist eine Primzahl
     Wenn $p$ eine Primzahl ist, dann gilt :

     $$\forall x \in K \setminus \{0\} : ggT(x,p) = 1 \quad \text{sonst wäre p keine Primzahl}$$

     Wegen (1) gibt es dann $a$,$b$ mit :
     $a \cdot x + b \cdot p = 1 \Longrightarrow (a \cdot x + b \cdot p) \bmod p = 1 \quad \stackrel{(2)}{\Longrightarrow}$
     $(a \cdot x) \bmod p = 1$
     Dann ist $a \bmod p \in K$ das Inverse bzgl. $\odot$ zu $x \in K$, da gilt (1) :

     $$\begin{aligned} a \bmod p \odot x \quad & \stackrel{\substack{\text{Definition von} \\ \odot}}{=} \quad (a \bmod p \cdot x) \bmod p \\ & \stackrel{(5)}{=} \quad (a \cdot x) \bmod p = 1 \end{aligned}$$

     Es gibt also, wenn $p$ prim ist, zu jedem $x \in P$ ein Inverses bzgl. $\odot$.

   - $p$ ist keine Primzahl
     Wenn $p$ keine Primzahl ist, gibt es $a, b \in P \setminus \{0\}$ mit $a \cdot b = p$. Für $a$ und $b$ gilt dann wegen der Definition von $\odot$, da $p$ bei Division durch $p$ den Rest 0 läßt : $a \odot b = 0$. a hat dann kein Inverses bzgl. $\odot$, da : Angenommen, es gäbe $a^{-1} \in P \setminus \{0\}$ mit $a \odot a^{-1} = 1$, dann würde gelten:

     $$\begin{aligned} a \odot b &= 0 \\ \Longrightarrow a^{-1} \odot (a \odot b) &= a^{-1} \odot 0 \\ \stackrel{\substack{\text{Ass. von } \odot, \\ \text{Def. von } 0}}{\Longrightarrow} (a^{-1} \odot a) \odot b &= 0 \\ \stackrel{\text{Voraussetzung}}{\Longrightarrow} 1 \odot b &= 0 \\ \stackrel{\text{Def. von } 1}{\Longrightarrow} b &= 0 \end{aligned}$$

     Dies widerspricht aber der Vorraussetzung, dass $b \in P \setminus \{0\}$, also gibt es kein $a^{-1} \in K$ mit $a^{-1} \odot a = 1$, $a$ hat also kein Inverses bzgl. $\odot$, d.h. wenn $p$ keine Primzahl ist, haben nicht alle $x \in P$ ein Inverses bzgl. $\odot$.

   M3 ist nur erfüllt, wenn p eine Primzahl ist.

7. D : Es gilt das Distributivgesetz : $(x \oplus y) \odot z = (x \odot z) \oplus (y \odot z)$

   Es gilt $(x, y, z \in K)$ :

   $$\begin{aligned} (x \oplus y) \odot z \quad & \stackrel{\text{Def. von } \oplus, \odot}{=} \quad [(x+y) \bmod p \cdot z] \bmod p \\ & \stackrel{(5)}{=} \quad [(x+y) \cdot z] \bmod p \end{aligned}$$

$$
\begin{aligned}
&\overset{\text{Dist. in } N_{naiv}}{=} && [(x+y)\cdot(x+z)] \bmod p \\
&\overset{(5)}{=} && [(x+y) \bmod p \cdot (x+y) \bmod p] \bmod p \\
&\overset{\text{Def. von } \oplus, \odot}{=} && (x \odot z) \oplus (y \odot z)
\end{aligned}
$$

D ist erfüllt.

Die Körperaxiome A1, A2, A3, M1, M2 und D sind also stets erfüllt, M3 dagegen nur, wenn $p$ eine Primzahl ist. Des Weiteren gilt $0 \neq 1$. Daher ist $(K, \oplus, \odot)$ nur dann ein Körper, wenn $p$ eine Primzahl ist.

**1.3.3**

1. Diskutiere die innere Verknüpfung

$$(x, y) \mapsto x \circ y := x + 3y$$

auf $\mathbb{R}$ i.e. untersuche sie auf Assoziativität, Kommutativität, Existenz eines neutralen Elementes, Existenz von Inversen.

- Assoziativität:
  $\circ$ ist nicht assoziativ, da für $0, 1 \in \mathbb{R}$ gilt:

$$
\begin{aligned}
(0 \circ 0) \circ 1 &\overset{\text{Def.}}{=} (0 + 3 \cdot 0) \circ 1 \\
&= 0 \circ 1 \\
&\overset{\text{Def.}}{=} 0 + 3 \cdot 1 \\
&= 3
\end{aligned}
$$

$$
\begin{aligned}
0 \circ (0 \circ 1) &\overset{\text{Def.}}{=} 0 \circ (0 + 3 \cdot 1) \\
&= 0 \circ 3 \\
&\overset{\text{Def.}}{=} 0 + 3 \cdot 3 \\
&= 9
\end{aligned}
$$

  also $(0 \circ 0) \circ 1 \neq 0 \circ (0 \circ 1)$, da $3 \neq 9$, damit ist $\circ$ nicht assoziativ.

- Kommutativität:
  $\circ$ ist nicht kommutativ, da für $0, 1 \in \mathbb{R}$ gilt:

$$
\begin{aligned}
0 \circ 1 &\overset{\text{Def.}}{=} 0 + 3 \cdot 1 \\
&= 3
\end{aligned}
$$

$$
\begin{aligned}
1 \circ 0 &\overset{\text{Def.}}{=} 1 + 3 \cdot 0 \\
&= 1
\end{aligned}
$$

  also $0 \circ 1 \neq 1 \circ 0$, da $1 \neq 3$, damit ist $\circ$ nicht kommutativ.

- Existenz eines neutralen Elementes:
  Es gibt in $\mathbb{R}$ kein neutrales Element bzgl. $\circ$, da:
  Angenommen es gäbe $n \in \mathbb{R}$ mit
  $$\forall r \in \mathbb{R} : n \circ r = r \circ n = n$$
  Dann gelte insbesondere auch
  $$n \circ 0 = 0 \Longleftrightarrow n + 3 \cdot 0 = 0 \Longleftrightarrow n = 0$$
  und
  $$n \circ 1 = 1 \Longleftrightarrow n + 3 \cdot 1 = 1 \Longleftrightarrow n = -2$$
  da aber $-2 \neq 0$ ex. in $\mathbb{R}$ kein neutrales Element bzgl. $\circ$.
  Allerdings ist 0 wegen $\forall r \in \mathbb{R} : r \circ 0 = r + 3 \cdot 0 = r$ linksneutral.

- Existenz von Inversen:
  Da in $\mathbb{R}$ bzgl. $\circ$ kein neutrales Element existiert, macht die Betrachtung von Inversen keinen Sinn.

2. Man definiere für $x, y \in \mathbb{R}$
$$\begin{aligned} x \oplus y &:= x + y, \\ x \odot y &:= \frac{x \cdot y}{2} \end{aligned}$$

   Ist dann $(\mathbb{R}, \oplus, \odot)$ ein Körper?

   Um zu überprüfen, ob $(\mathbb{R}, \oplus, \odot)$ ein Körper ist, muss man überprüfen, ob die Körperaxiome von $(\mathbb{R}, \oplus, \odot)$ erfüllt werden.

   (a) A1 : Assoziativität, Kommutativität von $\oplus$

   - Assoziativität:
     z.z.: $\forall x, y, z \in \mathbb{R} : (x \oplus y) \oplus z = x \oplus (y \oplus z)$

     Seien $x, y, z \in \mathbb{R}$ beliebig, dann gilt:
     $$\begin{aligned} (x \oplus y) \oplus z &\overset{\text{Def. von } \oplus}{=} (x + y) + z \\ &\overset{\text{Ass. von } +}{=} x + (y + z) \\ &\overset{\text{Def. von } \oplus}{=} x \oplus (y \oplus z) \end{aligned}$$

     Also ist $\oplus$ assoziativ.

- Kommutativität:
  z.z.: $\forall x, y \in \mathbb{R} : x \oplus y = y \oplus x$

  Seien $x, y \in \mathbb{R}$ beliebig, dann gilt:

$$\begin{aligned} x \oplus y &\overset{\text{Def. von } \oplus}{=} x + y \\ &\overset{\text{Komm. von } +}{=} y + x \\ &\overset{\text{Def. von } \oplus}{=} y \oplus x \end{aligned}$$

  Also ist $\oplus$ kommutativ.

A1 ist erfüllt.

(b) A2 : Existenz eines neutralen Elementes bzgl. $\oplus$
Beh.: 0 ist neutral bzgl. $\oplus$ z.z.: $\forall r \in \mathbb{R} : r \oplus 0 = 0 \oplus r = r$

Sei $r \in \mathbb{R}$ beliebig, dann gilt $r \oplus 0 = r + 0 = r$, da 0 neutral bzgl. ,+' ist. Es gilt aber wegen der Kommutativität von $\oplus$ auch $0 \oplus r = r \oplus 0 = r$. Also hat $\oplus$ ein neutrales Element, nämlich 0.

(c) A3 : Existenz von inversen Elementen bzgl. $\oplus$
Beh.: $-r \in \mathbb{R}$ ist zu $r \in \mathbb{R}$ invers bzgl. $\oplus$
z.z.: $\forall r \in \mathbb{R} : r \oplus (-r) = (-r) \oplus r = 0$

Sei $r \in \mathbb{R}$ beliebig, dann gilt $r \oplus (-r) = r + (-r) = 0$, da $-r$ invers zu $r$ bzgl. $+$ ist. Es gilt aber wegen der Kommutativität von $\oplus$ auch $(-r) \oplus r = r \oplus (-r) = 0$.
Also hat jedes $r \in \mathbb{R}$ ein Inverses bzgl. $\oplus$, nämlich $-r$.

(d) M1 : Assoziativität, Kommutativität von $\odot$

- Assoziativität:
  z.z.: $\forall x, y, z \in \mathbb{R} : (x \odot y) \odot z = x \odot (y \odot z)$

  Seien $x, y, z \in \mathbb{R}$ beliebig, dann gilt:

$$\begin{aligned} (x \odot y) \odot z &\overset{\text{Def. von } \odot}{=} \frac{x \cdot y}{2} \odot z \\ &\overset{\text{Def. von } \odot}{=} \frac{\frac{x \cdot y}{2} \cdot z}{2} \\ &\overset{\text{Ass. von } \cdot}{=} \frac{(x \cdot y) \cdot z}{4} \\ &\overset{\text{Ass. von } \cdot}{=} \frac{x \cdot (y \cdot z)}{4} \end{aligned}$$

$$
\begin{aligned}
&\overset{\text{Ass. von } \cdot}{=} \frac{x \cdot \frac{y \cdot z}{2}}{2} \\
&\overset{\text{Def. von } \odot}{=} x \odot \frac{y \cdot z}{2} \\
&\overset{\text{Def. von } \odot}{=} x \odot (y \odot z)
\end{aligned}
$$

Also ist $\odot$ assoziativ.

- Kommutativität:
  z.z.: $\forall x, y \in \mathbb{R} : x \odot y = y \odot x$

  Seien $x, y \in \mathbb{R}$ beliebig, dann gilt:

$$
\begin{aligned}
x \odot y &\overset{\text{Def. von } \odot}{=} \frac{x \cdot y}{2} \\
&\overset{\text{Komm. von } \cdot}{=} \frac{y \cdot x}{2} \\
&\overset{\text{Def. von } \odot}{=} y \odot x
\end{aligned}
$$

  Also ist $\odot$ kommutativ.

M1 ist erfüllt.

(e) M2 : Existenz eines neutralen Elementes bzgl. $\odot$
Beh.: 2 ist neutral bzgl. $\odot$ z.z.: $\forall r \in \mathbb{R} : r \odot 2 = 2 \odot r = r$

Sei $r \in \mathbb{R}$ beliebig, dann gilt $r \odot 2 = \frac{r \cdot 2}{2} = r \cdot 1 = r$, da 1 neutral bzgl. ‚$\cdot$' ist. Es gilt aber wegen der Kommutativität von $\odot$ auch $2 \odot r = r \odot 2 = r$.
Also hat $\odot$ ein neutrales Element, nämlich 2.

(f) M3 : Existenz von inversen Elementen bzgl. $\odot$
Beh.: $\frac{4}{r} \in \mathbb{R}$ ist zu $r \in \mathbb{R} \setminus \{0\}$ invers bzgl. $\odot$
z.z.: $\forall r \in \mathbb{R} \setminus \{0\} : r \odot \frac{4}{r} = \frac{4}{r} \odot r = 2$

Sei $r \in \mathbb{R}$ beliebig, dann gilt

$$r \odot \frac{4}{r} = \frac{r \cdot \frac{4}{r}}{2} = 2.$$

Es gilt aber wegen der Kommutativität von $\odot$ auch

$$\frac{4}{r} \odot r = r \odot \frac{4}{r} = 2.$$

Also hat jedes $r \in \mathbb{R}$ ein Inverses bzgl. $\odot$, nämlich $\frac{4}{r}$.

(g) D: Distributivgesetz
z.z.: $\forall x, y, z \in \mathbb{R} : (x \oplus y) \odot z = (x \odot z) \oplus (y \odot z)$

Seien $x, y, z \in \mathbb{R}$ beliebig, dann gilt:

$$\begin{aligned}(x \oplus y) \odot z &\overset{\text{Def. von } \odot}{=} \frac{(x \oplus y) \cdot z}{2} \\ &\overset{\text{Def. von } \oplus}{=} \frac{(x + y) \cdot z}{2} \\ &\overset{\text{Distr. von } +, \cdot}{=} \frac{x \cdot z}{2} + \frac{y \cdot z}{2} \\ &\overset{\text{Def. von } \odot}{=} (x \odot z) + (y \odot z) \\ &\overset{\text{Def. von } \oplus}{=} (x \odot z) \oplus (y \odot z)\end{aligned}$$

Also gilt das Distributivgesetz.

Da wegen $2 \neq 0$ das additiv und das multiplikativ Inverse in $(\mathbb{R}, \oplus, \odot)$ nicht übereinstimmen und alle Körperaxiome erfüllt sind, ist $(\mathbb{R}, \oplus, \odot)$ ein Körper.

**1.3.4** Es sei $(K, +, \cdot)$ ein Körper, $y \in K$ und $f : K \to K$ mit $x \mapsto x - y = x + (-y)$ eine Abbildung. Untersuche f auf Invjektivität, Surjektivität und Bijektivität.

1. Injektivität : $f(a) = f(b) \Rightarrow a = b$

   ‘0‘sei das neutrale Element bzgl. ‚+’, $a, b \in K$

$$\begin{aligned} f(a) &= f(b) \\ \overset{\text{Def. von } f}{\Longrightarrow} a + (-y) &= b + (-y) \\ \Longrightarrow (a + (-y)) + y &= (b + (-y)) + y \\ \overset{\text{Ass. von } +}{\Longrightarrow} a + ((-y) + y) &= b + ((-y) + y) \\ \overset{\text{Def. von } -y}{\Longrightarrow} a + 0 &= b + 0 \\ \overset{\text{0 ist neutral}}{\Longrightarrow} a &= b \end{aligned}$$

   $f$ ist also injektiv.

2. Surjektivität: Z.z.: Zu jedem $a \in K$ existiert $b \in K$ mt $f(b) = a$.

   Sei $a \in K$ beliebig, dann setze $b := a + y$. Es gilt :

$$\begin{aligned} f(b) &\overset{\text{Def. von } b}{=} f(a + y) \\ &\overset{\text{Def. von } f}{=} (a + y) + (-y) \end{aligned}$$

$$\begin{aligned}
&\overset{\text{Ass. von }+}{=} && a + [y + (-y)] \\
&\overset{\text{Def. von }-y}{=} && a + 0 \\
&\overset{0\text{ ist neutral}}{=} && a
\end{aligned}$$

$f$ ist also surjektiv.

3. Bijektivität : $f$ ist bijektiv, da $f$ injektiv und surjektiv ist.

## zu 1.4

**1.4.1** Kann der Körper $(K, \oplus, \odot)$ aus Aufgabe 1.3.2 angeordnet werden ?

Nein, denn :
$\bigoplus_{k=1}^{n} 1$ sei für alle $n \in \mathbb{N}$ definiert durch :

$$\bigoplus_{k=1}^{1} 1 = 1$$
$$\bigoplus_{k=1}^{n+1} 1 = \bigoplus_{k=1}^{n} 1 \oplus 1$$

Für $\bigoplus$ gilt offenbar :

$$\bigoplus_{k=1}^{n} 1 = n \bmod p$$

Beweis (durch vollständige Induktion):
Für $n = 1$ gilt nach Definition von $\bigoplus$ : $\bigoplus_{k=1}^{1} 1 = 1 \overset{\text{Def. von mod}}{=} 1 \bmod p$
Wenn nun $\bigoplus_{k=1}^{n} 1 = n \bmod p$ gilt, folgt :

$$\begin{aligned}
\bigoplus_{k=1}^{n+1} 1 &\overset{\text{Def. von } \bigoplus}{=} \bigoplus_{k=1}^{n} 1 \oplus 1 \\
&\overset{\text{Voraussetzung}}{=} n \bmod p \oplus 1 \\
&\overset{\text{Def. von } \oplus}{=} (n \bmod p + 1) \bmod p \\
&\overset{\text{s. Übung 1.3.2}}{=} (n+1) \bmod p
\end{aligned}$$

Angenommen nun, $(K, \oplus, \odot)$ wäre anordbar, dann gälte :

$$\forall n \in \mathbb{N} : \bigoplus_{k=1}^{n} 1 > 0$$

Beweis : Es gilt in angeordneten Körpern stets $1 > 0$ (wegen $1 \neq 0$ (Axiom)) und $\forall x \in K : x^2 > 0 \wedge 1^2 = 1$ also (Def.) auch $\bigoplus_{k=1}^{1} 1 > 0$ und mit $\bigoplus_{k=1}^{n} 1 > 0$ folgt mit $1 > 0$ auch $\bigoplus_{k=1}^{n+1} 1 > 0$ $(\forall a, b \in K : a, b > 0 \Rightarrow a + b > 0)$.
Also gälte auch :

$$\bigoplus_{k=1}^{p-1} 1 = p - 1 \bmod p \overset{\text{Def. von mod}}{=} p - 1 > 0$$

Da $p - 1$ aber wegen $p - 1 \oplus 1 = p \bmod p = 0$ das Inverse zu 1, also $-1$ ist, gelte dann $-1 > 0 \overset{\substack{\text{K geordnet} \\ \text{nach Vor.}}}{\Longrightarrow} 1 < 0$.
$1 < 0$ ist ein Widerspruch zu $1 > 0$, also ist die Voraussetzung falsch, und

$(K, \oplus, \odot)$ kann nicht angeordnet werden.

**1.4.2** Man zeige, dass es auf $\mathbb{R}$ nur einen Positivbereich gibt.
Hinweis : Es darf ausgenutzt werden, dass zu jeder nicht negativen reellen Zahl eine Wurzel in $\mathbb{R}$ existiert.

Zunächst hat $\mathbb{R}$ aufgrund des Axiomensystems von $\mathbb{R}$ ($\mathbb{R}$ ist ein vollständiger, archimedisch angeordneter Körper) einen Positivbereich $P$. Dieser definiert auf $\mathbb{R}$ durch $\forall a, b \in \mathbb{R} : a > b :\Leftrightarrow a - b \in P$ eine Relation $>$. Um zu beweisen, dass dieser Positivbereich der einzige ist, muss man zeigen, dass, wenn $\tilde{P}$ ein beliebiger Positivbereich von $\mathbb{R}$ ist, $P = \tilde{P}$ folgt.
Sei $\tilde{P}$ ein beliebiger Positivbereich in $\mathbb{R}$. Zu zeigen: $P = \tilde{P}$
Zwei Mengen $M, N$ heissen gleich, wenn $M \subset N \wedge N \subset M$.

- ‚$\subset$': Man zeigt zunächst $P \subset \tilde{P}$
  Sei $x \in P$ beliebig. Dann existiert wegen $x \in P \Rightarrow x > 0$ ein $y \in \mathbb{R}$ mit $y^2 = x$. Da aber Quadrate von Zahlen ungleich 0 ($x \neq 0$ gilt, da $0 \notin P$, da kein Positivbereich 0 enthalten kann) in jedem Positivbereich enthalten sind, folgt $y^2 \in \tilde{P}$, da $\tilde{P}$ nach Voraussetzung Positivbereich ist. Und somit wegen $x = y^2$ auch $x \in \tilde{P}$. Dies war zu zeigen.
- ‚$\supset$': Man zeigt nun $\tilde{P} \subset P$
  Sei $x \in \tilde{P}$ beliebig. Angenommen nun $x \notin P$. Dann folgt, da $x \neq 0$ und $P$ ein Positivbereich ist, dass $-x \in P$. Damit gilt aber auch, wie eben bewiesen $-x \in \tilde{P}$, also aufgrund der Positivbereichseigenschaft von $\tilde{P} : x \notin \tilde{P}$. Das widerspricht aber der Voraussetzung $x \in \tilde{P}$, also war die Annahme falsch und es gilt $x \in P$. Dies war aber zu zeigen.

Es gilt also $P = \tilde{P}$ für beliebiges $\tilde{P}$ und somit hat $\mathbb{R}$ nur einen Positivbereich.

**1.4.3** Sei die Menge $K := \mathbb{Q} + \mathbb{Q}\sqrt{2}$ $\big(= \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}\big)$ gegeben.

1. Zeige das $(K, +, \cdot)$ ein Körper ist, wobei ‚+' und ‚$\cdot$' die von $\mathbb{R}$ geerbten Verknüpfungen sind.
2. Es sei „$>$"die übliche Ordnung auf $\mathbb{R}$, und
$$\begin{aligned} \mathcal{P}_1 &:= \{a + b\sqrt{2} \in K \,|\, a + b\sqrt{2} > 0\} \quad \text{und} \\ \mathcal{P}_2 &:= \{a + b\sqrt{2} \in K \,|\, a - b\sqrt{2} > 0\} \end{aligned}$$
   Zeige, dass $\mathcal{P}_1$ und $\mathcal{P}_2$ verschiedene Positivbereiche auf $K$ sind.

Es darf benutzt werden, dass $\sqrt{2}$ irrational ist.

1. Zuerst zeigt man, dass $K \subset \mathbb{R}$.
   Beweis : (z.z. : $x \in K \Rightarrow x \in \mathbb{R}$)
   Sei $x \in K$, dann kann $x$ nach Definition von $K$ als $a + b\sqrt{2}$ mit $a, b \in$

$\mathbb{Q}$ dargestellt werden. Da aber $\mathbb{Q} \subset \mathbb{R}$ und somit auch $a, b \in \mathbb{R}$, aber auch $\sqrt{2} \in \mathbb{R}$, woraus nach den Körpereigenschaften von $\mathbb{R}$ (‚+'und ‚$\cdot$'sind innere Verknüpfungen auf $\mathbb{R}$) $a + b\sqrt{2} \in \mathbb{R}$ folgt. Dies heisst aber $x \in \mathbb{R}$. Dann zeigt man, dass

$$a + b\sqrt{2} = 0 \Longleftrightarrow a = 0 \wedge b = 0 \quad (a, b \in \mathbb{Q}) \tag{6}$$

Beweis :

- ‚$\Rightarrow$': Sei $x = a + b\sqrt{2} = 0 \in K$ gegeben. Man unterscheidet nun zwei Fälle :
  (a) $b = 0$ : Setzt man dies in die Voraussetzung ein, folgt sofort $a = 0$, da $a + 0\sqrt{2} = 0 \Rightarrow a = 0$.
  (b) $b \neq 0$ : Hier folgt

  $$a + b\sqrt{2} = 0 \overset{\mathbb{Q} \text{ ist Körper}}{\Longleftrightarrow} a = -b\sqrt{2} \overset{b \neq 0}{\Longleftrightarrow} -\frac{a}{b} = \sqrt{2}$$

  Da mit $a, b \in \mathbb{Q}$ nach Voraussetzung, da $\mathbb{Q}$ ein Körper ist und so ‚$\cdot$'innere Verknüpfung, auch $-\frac{a}{b} \in \mathbb{Q}$, wäre $\sqrt{2} \in \mathbb{Q}$. Dies ist ein Widerspruch, da $\sqrt{2} \notin \mathbb{Q}$ schon bewiesen wurde. Also gilt $b = 0$ und damit folgt $a = 0$.
- ‚$\Leftarrow$': Aus $a = 0$ und $b = 0$ folgt sofort $x = a + b\sqrt{2} = 0 + 0\sqrt{2} = 0$.

Aus (1) folgt aber, dass sich jede Zahl $x \in K$ auf genau eine Art als $a+b\sqrt{2}$ mit $a, b \in \mathbb{Q}$ darstellen lässt. Denn : Sei $x \in K$ dargestellt als : $x = a+b\sqrt{2}$ und $x = \tilde{a} + \tilde{b}\sqrt{2}$. Das ist aufgrund der Definition von $K$ stets möglich Dann folgt :

$$\begin{aligned}
&& x &= x \\
&\overset{\text{Voraussetzung}}{\Longleftrightarrow} & a + b\sqrt{2} &= \tilde{a} + \tilde{b}\sqrt{2} \\
&\overset{\mathbb{R} \text{ ist ein Körper}}{\Longleftrightarrow} & -\tilde{a} + a + b\sqrt{2} - \tilde{b}\sqrt{2} &= 0 \\
&\overset{\substack{\text{Ass., Komm.in} \\ \mathbb{R}}}{\Longleftrightarrow} & (a - \tilde{a}) + (b - \tilde{b}) &= 0 \\
&\overset{(1)}{\Longleftrightarrow} & a - \tilde{a} = 0 &\wedge \; b - \tilde{b} = 0 \\
&& \Longleftrightarrow a = \tilde{a} &\wedge \; b = \tilde{b}
\end{aligned}$$

D.h. (2) : Jede Zahl $x \in K$ lässt sich auf genau eine Art als $x = a + b\sqrt{2}, \quad a, b \in \mathbb{Q}$ darstellen.
Um zu zeigen, dass $(K, +, \cdot)$ ein Körper ist, muss man überprüfen, ob die Körperaxiome für $K$ erfüllt sind. Zunächst hat man zu zeigen, dass die von $\mathbb{R}$ geerbten Verknüpfungen ‚+' und ‚$\cdot$' innere Verknüpfungen auf $K$ sind.
zu Zeigen : $\forall x_1, x_2 \in K : x_1 + x_2 \in K \wedge x_1 \cdot x_2 \in K$.
Seien nun $x_1, x_2 \in K$ bel. gegeben. Dann lassen sich $x_1$ und $x_2$ wegen (2) eindeutig darstellen durch :

$$\begin{aligned} x_1 &= a_1 + b_1\sqrt{2} \quad a_1, b_1 \in \mathbb{Q} \\ x_2 &= a_2 + b_2\sqrt{2} \quad a_2, b_2 \in \mathbb{Q} \end{aligned}$$

Damit folgt für $x_1 + x_2$:

$$x_1 + x_2 = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})$$

$$\begin{aligned} &\overset{\text{Komm.,Ass. in } \mathbb{R}}{=} (a_1 + a_2) + b_1\sqrt{2} + b_2\sqrt{2} \\ &\overset{\text{Distr. in } \mathbb{R}}{=} (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \end{aligned}$$

Da aufgrund der Körpereigenschaften von $\mathbb{Q}$ (‚+'ist innere Verknüpfung) mit $a_1, a_2$ auch $a_1 + a_2 \in \mathbb{Q}$ und mit $b_1, b_2$ auch $b_1 + b_2 \in \mathbb{Q}$ liegt, ist $x_1 + x_2$ nach der Definition von $K$ Element von $K$.
Für $x_1 \cdot x_2$ folgt :

$$\begin{aligned} x_1 \cdot x_2 &= (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) \\ &\overset{\text{Distr. in } \mathbb{R}}{=} a_1 \cdot a_2 + a_1 \cdot b_2\sqrt{2} + a_2 \cdot b_1\sqrt{2} + b_1\sqrt{2} \cdot b_2\sqrt{2} \\ &\overset{\text{Ass.,Komm. in } \mathbb{R}}{=} a_1 \cdot a_2 + b_1\sqrt{2} \cdot b_2\sqrt{2} + a_2 \cdot b_1\sqrt{2} + a_1 \cdot b_2\sqrt{2} \\ &\overset{\text{Distr. in } \mathbb{R},\ \sqrt{2}^2 = 2}{=} (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \end{aligned}$$

Auch hier folgt aus den Eigenschaften von ‚+'und ‚·'als innere Verknüpfungen auf $\mathbb{Q}$, dass $a_1a_2+2b_1b_2 \in \mathbb{Q}$ und $a_1b_2+a_2b_1 \in \mathbb{Q}$ und somit $x_1 \cdot x_2 \in K$. Dies war aber zu zeigen.
Jetzt kann man die Gültigkeit der Körperaxiome für $(K, +, \cdot)$ überprüfen :

(a) A1 : Kommutativität und Assoziativität von ‚+'.
‚+'ist kommutativ und assoziativ, da es vom Körper $(\mathbb{R}, +, \cdot)$ geerbt wurde und somit auf $\mathbb{R}$ kommutativ und assoziativ ist, also erst recht auf $K \subset \mathbb{R}$.

(b) A2 : Es gibt ein neutrales Element bzgl. ‚+'
Da ‚+'in $\mathbb{R}$ das neutrale Element 0 hat, hat es dies wegen $K \subset \mathbb{R}$ und $0 \in K$, da $0 = 0 + 0\sqrt{2}$ auch in $K$.

(c) A3 : Jedes Element $x \in K$ hat ein Inverses bzgl. ‚+'
In $\mathbb{R}$ hat jedes $x \in K \subset \mathbb{R}$ ein Inverses bzgl. ‚+', nämlich $-x$, es bleibt noch zu zeigen, dass

$$\forall x \in K : -x \in K$$

Beweis :
Sei $x \in K$ bel. Dann kann $x$ eindeutig als $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$ dargestellt werden. Für $-x$ gilt damit $-x = -a - b\sqrt{2} \overset{\mathbb{R}\text{ Körper}}{=} -a+(-b)\sqrt{2}$. Da aber $\mathbb{Q}$ ein Körper ist, liegen mit $a, b$ auch $-a, -b \in \mathbb{Q}$ und somit ist nach Definition von $K$, $-x \in K$ und das Inverse zu $x$.

(d) M1 : Kommutativität und Assoziativität von ‚·'.
‚·'ist kommutativ und assoziativ, da es vom Körper $(\mathbb{R}, +, \cdot)$ geerbt wurde und somit auf $\mathbb{R}$ kommutativ und assoziativ ist, also erst recht auf $K \subset \mathbb{R}$.

(e) M2 : Es gibt ein neutrales Element bzgl. ‚·'.
Da ‚·'in $\mathbb{R}$ das neutrale Element 1 hat, hat es dies wegen $K \subset \mathbb{R}$ und $1 \in K$, da $1 = 1 + 0\sqrt{2}$ auch in $K$.

(f) M3 : Zu jedem $x \in K \neq 0$ gibt es ein Inverses bzgl. ‚$\cdot$'.
In $\mathbb{R}$ hat jedes $x \neq 0 \in K \subset \mathbb{R}$ ein Inverses bzgl. ‚$\cdot$', nämlich $x^{-1}$, es bleibt noch zu zeigen, dass

$$\forall x \in K : x^{-1} \in K$$

Beweis: Sei $x \in K \setminus \{0\}$ bel. gegeben, dann gilt für $x$ wg. (2) : $x = a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$ und (1) : $a \neq 0 \vee b \neq 0$. Mit $a \neq 0 \vee b \neq 0$ ist aber auch $a - b\sqrt{2} \neq 0$. Nun ist :

$$\begin{aligned} x^{-1} &\overset{\text{Def.}}{=} \frac{1}{x} \\ &\overset{(2)}{=} \frac{1}{a + b\sqrt{2}} \\ &\overset{a - b\sqrt{2} \neq 0}{=} \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \\ &\overset{\mathbb{R} \text{ ist Körper}}{=} \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &\overset{\text{Ass.,Distr. in } \mathbb{R}}{=} \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \end{aligned}$$

Aus den Eigenschaften von ‚+'und ‚$\cdot$'in $\mathbb{Q}$ folgt : $a^2 - 2b^2 \in \mathbb{Q}$ und $-b \in Q$, da $a, b \in \mathbb{Q}$ und somit gilt $x^{-1} \in K$. Also hat jedes $x \in K$ ein Inverses bzgl. ‚$\cdot$'.

(g) D : Es gilt das Distributivgesetz
Da das Distributvgesetz in $\mathbb{R}$ für ‚+'und ‚$\cdot$'gilt, und ‚+'und ‚$\cdot$'innere Verknüpfungen auf $K \subset \mathbb{R}$ sind, gilt es auch in K.

Alle Axiome sind erfüllt und es gilt $0 \neq 1$ wie in $\mathbb{R} \Rightarrow (K, +, \cdot)$ ist ein Körper.

2. Zunächst zeigt man, dass $\mathcal{P}_1$ und $\mathcal{P}_2$ wohldefiniert sind :
Wie oben (2) bewiesen, gibt es für jedes $x \in K$ genau eine Möglichkeit, es in der Form $x = a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$ darzustellen, d.h. mit $x$ sind auch $a$ und $b$ eindeutig bestimmt, und man kann eindeutig für jedes $x \in K$ entscheiden, ob $a + b\sqrt{2} > 0$ und $a - b\sqrt{2} > 0$ gelten. Man kann also für jedes $x \in K$, da das gerade die Eigenschaften sind, die die Teilmengen $\mathcal{P}_1 \subset K$ und $\mathcal{P}_2 \subset K$ definieren, eindeutig feststellen, ob $x \in \mathcal{P}_1$ oder $x \notin \mathcal{P}_1$, bzw. $x \in \mathcal{P}_2$ oder $x \notin \mathcal{P}_2$. Also sind $\mathcal{P}_1$ und $\mathcal{P}_2$ wohldefiniert.

Als nächstes hat man zu zeigen, dass $\mathcal{P}_1$ und $\mathcal{P}_2$ Positivbereiche sind, d.h. dass sie die für Positivbereiche geforderten Axiome erfüllen (‚>'sei die natürlich Ordnung in $\mathbb{R}$) :

Sei $(K, +, \cdot)$ ein Körper. $P \subset K$ heisst Positivbereich, wenn gilt :

P1 : $\forall x \in K \setminus \{0\} : (x \in P \vee -x \in P) \wedge \neg(x \in P \wedge -x \in P)$
P2 : $\forall a, b \in P : a + b \in P$
P3 : $\forall a, b \in P : a \cdot b \in P$

- Man zeigt zunächst, dass $\mathcal{P}_1$ ein Positivbereich in $K$ ist.

  (a) P1
  Sei $x \in K \setminus \{0\}$ dargestellt als $x = a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$.
  $x \in \mathcal{P}_1$ gilt laut Definition von $\mathcal{P}_1$ genau dann, wenn in $\mathbb{R}$ $a + b\sqrt{2} = x > 0$ gilt. Da $\mathbb{R}$ ein geordneter Körper ist, gilt stets $x > 0$ oder $-x > 0$, aber nie beides zugleich. Somit gilt auch stets $x \in \mathcal{P}_1$ oder $x \notin \mathcal{P}_1$, aber nie beides zugleich.

  (b) P2
  Seien $x, y \in \mathcal{P}_1$ beliebig. $x \in \mathcal{P}_1$ bedeutet aber (s. P1) gerade $x > 0$, wobei „$>$“die natürliche Ordnung in $\mathbb{R}$ ist. Genauso gilt mit $y \in \mathcal{P}_1$ auch $y > 0$. Aufgrund der Ordnung in $\mathbb{R}$ folgt aus $x > 0$ und $y > 0$ aber auch $x + y > 0$. Da $x + y \in K$ gilt, und $x + y > 0$ folgt, dass $x + y \in \mathcal{P}_1$ aus der Definition von $\mathcal{P}_1$ ($\mathcal{P}_1$ enthält gerade die Elemente aus $K$, für die $x = a + b\sqrt{2} > 0$ ist).

  (c) P3
  Seien $x, y \in \mathcal{P}_1$ beliebig. Analog wie oben (P2) gilt $x > 0 \wedge y > 0 \Rightarrow x \cdot y > 0$ und da $K$ bzgl. ‚$\cdot$‘abgeschlossen ist, folgt $x \cdot y \in \mathcal{P}_1$.

  Da alle Axiome von $\mathcal{P}_1$ erfüllt werden, ist $\mathcal{P}_1$ Positivbereich in $K$.

- Jetzt zeigt man, dass $\mathcal{P}_2$ ein Positivbereich in $K$ ist.

  (a) P1
  Sei $x \in K \setminus \{0\}$ eindeutig dargestellt als $x = a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$.
  $x \in \mathcal{P}_2$ gilt, wenn $a - b\sqrt{2} > 0$ ist, wenn dies gilt, ist aber $-x = -a - b\sqrt{2}$ wegen $a - b\sqrt{2} > 0 \Rightarrow -a + b\sqrt{2} = -a - (-b)\sqrt{2} < 0$.
  $-x \notin \mathcal{P}_2$. Gilt aber $x \notin \mathcal{P}_2$, so folgt $a - b\sqrt{2} < 0$ ($a - b\sqrt{2} = 0$ ist wegen $x \neq 0$ unmöglich, da (1) $x \neq 0 \Longrightarrow a \neq 0 \vee b \neq 0 \overset{\text{a}}{\Longrightarrow} -b\sqrt{2} \neq 0$). Damit gilt aber $-a - (-b)\sqrt{2} > 0$ und somit $-x \in \mathcal{P}_2$. Somit gilt für $x$ stets $x \in \mathcal{P}_2$ oder $-x \in \mathcal{P}_2$ aber nie beides zugleich.

  (b) P2
  Seien $x = a + b\sqrt{2} \in \mathcal{P}_2$ und $y = c + d\sqrt{2} \in \mathcal{P}_2$ gegeben. $x + y = (a + c) + (b + d)\sqrt{2} \in K$ kann als $x + y = e + f\sqrt{2}$ mit $e := a + c$ und $f := b + d$ geschrieben werden. ($a, b, c, d, e, f \in \mathbb{Q}$).
  Es gilt : $a - b\sqrt{2} > 0$ und $c - d\sqrt{2} > 0$, da $x, y \in \mathcal{P}_2$.
  Zu zeigen $x + y \in \mathcal{P}_2 \Leftrightarrow e - f\sqrt{2} > 0$.
  Da $\mathbb{R}$ ein geordneter Körper ist, folgt aus $a - b\sqrt{2} > 0$ und $c - d\sqrt{2} > 0$, dass $a - b\sqrt{2} + c - d\sqrt{2} > 0$ gilt. Wegen der Körpereigenschaften von $\mathbb{R}$ ist dies gleichbedeutend mit :$(a + c) - (b + d)\sqrt{2} > 0$, was mit den Definitionen von $e$ und $f$ gerade $e - f\sqrt{2} > 0$ ergibt, dies war aber zu zeigen. Also gilt: $x + y \in \mathcal{P}_2$.

  (c) P3
  Seien $x = a + b\sqrt{2} \in \mathcal{P}_2$ und $y = c + d\sqrt{2} \in \mathcal{P}_2$ gegeben. $x \cdot y = (ac + 2bd) + (ad + bc)\sqrt{2} \in K$ kann als $x \cdot y = e + f\sqrt{2}$ mit $e := ac + 2bd$ und $f := ad + bc$ geschrieben werden ($a, b, c, d, e, f \in \mathbb{Q}$).
  Es gilt : $a - b\sqrt{2} > 0$ und $c - d\sqrt{2} > 0$
  zu zeigen : $x \cdot y \in \mathcal{P}_2 \Leftrightarrow e - f\sqrt{2} > 0$

$$\begin{aligned}
& a-b\sqrt{2}>0 \quad \wedge \quad c-d\sqrt{2}>0 \\
\overset{\text{Ordnung in } \mathbb{R}}{\Longrightarrow} \quad & (a-b\sqrt{2})(c-d\sqrt{2}) > 0 \\
\overset{\text{Distr. in } \mathbb{R}}{\Longrightarrow} \quad & ac-bc\sqrt{2}-ad\sqrt{2}+bd\sqrt{2}\sqrt{2} > 0 \\
\overset{\substack{\text{Komm. in } \mathbb{R},\\ \sqrt{2}^2=2}}{\Longrightarrow} \quad & ac+2bd-bc\sqrt{2}-ad\sqrt{2} > 0 \\
\overset{\text{Ass., Distr. in } \mathbb{R}}{\Longrightarrow} \quad & (ac+2bd)-(bc+ad)\sqrt{2} > 0 \\
\overset{\text{Def. von } e,f}{\Longrightarrow} \quad & e-f\sqrt{2} > 0
\end{aligned}$$

Dies war zu zeigen, also gilt : $x \cdot y \in \mathcal{P}_2$.

Da alle Axiome von $\mathcal{P}_2$ erfüllt werden, ist $\mathcal{P}_2$ ein Positivbereich.

Man hat jetzt noch zu zeigen, dass $\mathcal{P}_1$ und $\mathcal{P}_2$ voneinander verschieden sind. Dazu reicht es, ein $x \in K$ zu finden, für das $x \in P_1$ und $x \notin \mathcal{P}_2$ gilt. Wir setzen $x := \sqrt{2}$. Offenbar gilt $x = 0 + 1\sqrt{2} \in K$. Wegen $0 + 1\sqrt{2} = \sqrt{2} > 0$ ist $x \in \mathcal{P}_1$, aber wegen $0 - 1\sqrt{2} \not> 0$ gilt $x \notin \mathcal{P}_2$. Also sind $\mathcal{P}_1$ und $\mathcal{P}_2$ verschiedene Positivbereiche auf $K$.

**1.4.4** Für $a, b, c, d \in \mathbb{R}$ mt $b, d > 0$ zeige :

$$\frac{a}{b} < \frac{c}{d} \Longrightarrow \frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$$

1. Man zeigt zunächst $\frac{a}{b} < \frac{c}{d} \Longrightarrow \frac{a}{b} < \frac{a+c}{b+d}$
   Es sei $a, c \in \mathbb{R}, b, d \in \mathbb{R}^+$, $\frac{a}{b} < \frac{c}{d}$, dann gilt :

$$\begin{aligned}
& \frac{a}{b} < \frac{c}{d} \\
\overset{b,d>0}{\Longleftrightarrow} \quad & ad < bc \\
\overset{\text{Monotoniegesetz}}{\Longleftrightarrow} \quad & ad+ab < bc+ab \\
\overset{\text{Distributiv}}{\Longleftrightarrow} \quad & a(b+d) < b(a+c) \\
\overset{b,b+d>0}{\Longleftrightarrow} \quad & \frac{a}{b} < \frac{a+c}{b+d}
\end{aligned}$$

2. Man zeigt nun $\frac{a}{b} < \frac{c}{d} \Longrightarrow \frac{a+c}{b+d} < \frac{c}{d}$
   Es sei $a, c \in \mathbb{R}, b, d \in \mathbb{R}^+$, $\frac{a}{b} < \frac{c}{d}$, dann gilt :

$$\begin{aligned}
& \frac{a}{b} < \frac{c}{d} \\
\overset{b,d>0}{\Longleftrightarrow} \quad & ad < bc \\
\overset{\text{Monotoniegesetz}}{\Longleftrightarrow} \quad & ad+cd < bc+cd \\
\overset{\text{Distributiv}}{\Longleftrightarrow} \quad & d(a+c) < c(b+d) \\
\overset{d,b+d>0}{\Longleftrightarrow} \quad & \frac{a+c}{b+d} < \frac{c}{d}
\end{aligned}$$

## zu 1.5

**1.5.1** Beweise folgende Summenformeln :

1. $$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

   Induktionsanfang : Die Formel gilt für $n = 1$ wegen
   $$\sum_{k=1}^{1} k^2 = 1^2 = 1 = \frac{1}{6} \cdot 1 \cdot (1+1) \cdot (2+1)$$
   Induktionsvoraussetzung : Die Formel gelte für ein festes $n$, i.e. es gelte :
   $$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$
   Induktionsschluss : Dann gilt sie auch für $n+1$ :
   zu zeigen : $\sum_{k=1}^{n+1} k^2 = \frac{1}{6}(n+1)(n+2)(2n+3)$
   $$\begin{aligned}\sum_{k=1}^{n+1} k^2 &= \sum_{k=1}^{n} k^2 + (n+1)^2 \\ &\overset{\text{Voraussetzung}}{=} \frac{1}{6}n(n+1)(2n+1) + (n+1)^2 \\ &= \frac{1}{6}(2n^3+3n^2+n) + \frac{1}{6}(6n^2+12n+6) \\ &= \frac{1}{6}(2n^3+9n^2+13n+6) \\ &= \frac{1}{6}(n+1)(2n^2+7n+6) \\ &= \frac{1}{6}(n+1)(n+2)(2n+3)\end{aligned}$$
   Aufgrund des Induktionsprinzips gilt die Formel für alle $n \in \mathbb{N}$.

2. $$\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2$$

   Induktionsanfang : Die Formel gilt für $n = 1$ wegen
   $$\sum_{k=1}^{1} k^3 = 1^3 = 1 = \frac{1}{4} \cdot 1^2 \cdot 2^2$$
   Induktionsvoraussetzung : Die Formel gelte für ein festes $n$, i.e. es gelte :
   $$\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2$$
   Induktionsschluss : Dann gilt sie auch für $n+1$ :
   zu zeigen : $\sum_{k=1}^{n+1} k^3 = \frac{1}{4}(n+1)^2(n+2)^2$

$$\begin{aligned}
\sum_{k=1}^{n+1} k^3 &= \sum_{k=1}^{n} k^3 + (n+1)^3 \\
&\overset{\text{Voraussetzung}}{=} \frac{1}{4}n^2(n+1)^2 + (n+1)^3 \\
&= \frac{1}{4}(n^4 + 2n^3 + n^2) + \frac{1}{4}(4n^3 + 12n^2 + 12n + 4) \\
&= \frac{1}{4}(n^4 + 6n^3 + 13n^2 + 12n + 4) \\
&= \frac{1}{4}(n+1)(n^3 + 5n^2 + 8n + 4) \\
&= \frac{1}{4}(n+1)^2(n^2 + 4n + 4) = \frac{1}{4}(n+1)^2(n+2)^2
\end{aligned}$$

Aufgrund des Induktionsprinzips gilt die Formel für alle $n \in \mathbb{N}$.

**1.5.2** Finde und beweise eine Formel für die Zeilensummen im „Dreieck der ungeraden Zahlen “:

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 3 & & 5 & & & \\
 & & 7 & & 9 & & 11 & & \\
 & 13 & & 15 & & 17 & & 19 & \\
21 & \cdots & & & & & & &
\end{array}$$

Es gilt :

$$\begin{aligned}
1 = 1 &= 1^3 \\
3 + 5 = 8 &= 2^3 \\
7 + 9 + 11 = 27 &= 3^3 \\
&\vdots
\end{aligned}$$

Vermutung : Die Summe der $n$-ten Zeile des Dreiecks beträgt für alle $n \in \mathbb{N}$ gerade $s(n) = n^3$.
Beweis :

1. Zuerst zeigt man: Für alle $i \in \mathbb{N}$ ist $2i - 1$ die $i$-te ungerade Zahl.
   Beweis:
   Induktionsanfang:
   Für $i = 1$ gilt : $2 \cdot 1 - 1 = 1$ ist die 1 ungerade Zahl.
   Induktionsvoraussetzung:
   Für ein $i \in \mathbb{N}$ gelte :
   $2i - 1$ ist die $i$-te ungerade Zahl.
   Induktionsschluss:
   Es folgt : $2(i + 1) - 1 = (2i - 1) + 2$, also nach Voraussetzung, die Zahl, die um 2 größer ist, als die $i$-te Ungerade, also die $(i + 1)$-te. q.e.d.

2. Als nächstes zeigt man :
   Für alle $n \in \mathbb{N}$ ist die Summe der ersten $n$ ungerade Zahlen $n^2$, also :
$$\sum_{k=1}^{n} 2k - 1 = n^2$$
   Beweis :
   Induktionsanfang :
   Für n = 1 gilt :
$$\sum_{k=1}^{1} 2k - 1 = 2 \cdot 1 - 1 = 1 = 1^2$$
   Induktionsvoraussetzung :
   Für ein $n \in \mathbb{N}$ sei :
$$\sum_{k=1}^{n} 2k - 1 = n^2$$
   Induktionsschluss :
   zu zeigen : $\sum_{k=1}^{n+1} 2k - 1 = (n+1)^2$
$$\begin{aligned} \sum_{k=1}^{n+1} 2k - 1 &= \sum_{k=1}^{n} 2k - 1 + 2(n+1) - 1 \\ \stackrel{\text{Voraussetzung}}{=} n^2 + 2n + 1 &= (n+1)^2 \end{aligned}$$

3. Des Weiteren gilt : Da in der $k$-ten Zeile $k$ Zahlen stehen, stehen in den ersten $n$-Zeilen zusammen
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \qquad \text{(s. Buch)}$$
   Also ist die letzte Zahl der $k$-ten Zeile die $\frac{n(n+1)}{2}$-te ungerade Zahl.

Die Summe der ersten Zeile ist s(1) = 1 (Dies ist klar). Die Summe der $n$-ten Zeile ist für $n > 1$ offensichtlich die Summe der ersten $n$ Zeilen minus die Summe der ersten $n - 1$ Zeilen.
Die Summe $S(n)$ der ersten $n$ Zeilen ist aber die Summe der ersten $\frac{n(n+1)}{2}$ ungeraden Zahlen, also:
$$S(n) = \sum_{k=1}^{\frac{n(n+1)}{2}} 2k - 1 = \left[\frac{n(n+1)}{2}\right]^2 = \frac{1}{4} n^2 (n+1)^2.$$
Die Summe $S(n-1)$ ist also:
$$S(n-1) = \frac{1}{4}(n-1)^2 n^2.$$
Die Differenz ist $(n > 1)$:
$$s(n) = S(n) - S(n-1) = \frac{1}{4}(n^4 + 2n^3 + n^2 - n^4 + 2n^3 - n^2) = \frac{1}{4} \cdot 4n^3 = n^3 \text{ für alle } n > 1.$$
Wegen $s(1) = 1 = 1^3$ gilt $s(n) = n^3$ für alle $n \in \mathbb{N}$.

**1.5.3** Beweise mit vollständiger Induktion :

1. Für $q \in \mathbb{R} \setminus \{1\}$ und $N \in \mathbb{N}$ gilt
$$\sum_{n=0}^{N} q^n = \frac{1 - q^{N+1}}{1 - q}.$$
2. Für alle reellen Zahlen $x$ mit $0 \leq x \leq 1$ und alle natürlichen Zahlen $n$ gilt :
$$(1 + x)^n \leq 1 + (2^n - 1)x$$

1.
- Induktionsanfang :
  Für $N = 1$ gilt:
$$\begin{aligned} \sum_{n=0}^{1} q^n &\overset{\text{Def. von } \Sigma}{=} q^0 + q^1 \\ &\overset{\text{Def. von } q^0, q^1}{=} 1 + q \end{aligned}$$
$$\begin{aligned} \frac{1 - q^{1+1}}{1 - q} &= \frac{1 - q^2}{1 - q} \\ &\overset{\text{binom. Formel}}{=} \frac{(1 - q)(1 + q)}{1 - q} \\ &\overset{1 - q \neq 0}{=} 1 + q \end{aligned}$$
  Das ist offensichtlich gleich.
- Induktionsvoraussetzung :
  Für ein $N \in \mathbb{N}$ gelte :
$$\sum_{n=0}^{N} q^n = \frac{1 - q^{N+1}}{1 - q}.$$
- Induktionsschluss :
  zu zeigen : Dann gilt auch :
$$\sum_{n=0}^{N+1} q^n = \frac{1 - q^{N+2}}{1 - q}.$$
  Es gilt :
$$\begin{aligned} \sum_{n=0}^{N+1} q^n &\overset{\text{Def. von } \Sigma}{=} \sum_{n=0}^{N} q^n + q^{N+1} \\ &\overset{\text{Voraussetzung}}{=} \frac{1 - q^{N+1}}{1 - q} + q^{N+1} \\ &\overset{1 - q \neq 0}{=} \frac{1 - q^{N+1}}{1 - q} + \frac{q^{N+1} - q^{N+2}}{1 - q} \\ &= \frac{1 - q^{N+2}}{1 - q} \end{aligned}$$

2. • Induktionsanfang:
Für $n = 1$ gilt:

$$(1+x)^1 \overset{\text{Def.}}{=} 1+x \leq 1+x = 1+(2^1-1)x \quad \text{wahr}$$

• Induktionsvoraussetzung:
Für ein $n \in \mathbb{N}$ gelte :

$$(1+x)^n \leq 1+(2^n-1)x$$

• Induktionsschluss:
zu zeigen, dann gilt auch :

$$(1+x)^{n+1} \leq 1+(2^{n+1}-1)x$$

Es gilt :

$$(1+x)^{n+1} \overset{\text{Def.}}{=} (1+x)^n \cdot (1+x)$$

Aus der Voraussetzung folgt mit $(1+x) > 0$ wegen $x \geq 0$

$$\begin{aligned}
(1+x)^n \cdot (1+x) &\leq [1+(2^n-1)x] \cdot (1+x) \\
&\overset{\text{Distributivgesetz}}{=} (1+x)+(1+x)(2^n-1)x \\
&\overset{x \leq 1}{\leq} 1+x+2\cdot(2^n-1)x \\
&\overset{\text{Distributivität}}{=} 1+x+2^{n+1}x-2x \\
&\overset{\text{Ass., Komm.}}{=} 1+2^{n+1}x-x \\
&\overset{\text{Distr.}}{=} 1+(2^{n+1}-1)x
\end{aligned}$$

Dies war zu zeigen.

**1.5.4** Auf einer einsamen Insel gibt es $n \in \mathbb{N}$ Städte, und zwischen je zwei Städten genau eine Einbahnstraße. Zeige, dass es möglich ist, jede Stadt einmal zu besuchen, ohne gegen die Verkehrsregeln zu verstoßen.

Man zeigt dies durch vollständige Induktion :

• Induktionsanfang:
Für $n = 1$ gibt es nur eine Stadt und keine Straße. Diese Stadt ist Start und Ziel der Reise, die alle Städte besucht.
Für $n = 2$ gibt es die zwei Städte $S_1$ und $S_2$ wenn die Einbahnstraße in $S_1$ beginnt, ist $S_1 \to S_2$ die gesuchte Reise, ansonsten $S_2 \to S_1$.

• Induktionsvoraussetzung:
Für ein $n \in \mathbb{N}$ gelte : Es ist möglich $n$ Städte, die jeweils mit Einbahnstraßen verbunden sind, alle hintereinander zu besuchen.

- Induktionsschluss:
  zu zeigen : Es ist auch mit $n+1$ Städten möglich :
  Seien die $n+1$ Städte mit $S_1, S_2, S_3, S_4, \ldots, S_{n+1}$ bezeichnet, und zwar in der Art, dass die Reise, die nach Induktionsvoraussetzung in $(S_1, S_2, \ldots S_n)$ existiert, die Städte in der Reihenfolge ihrer Nummerierung besucht, also $S_1 \to S_2 \to \ldots \to S_n$ die Reise ist.
  Betrachte nun die Straße, die $S_1$ und $S_{n+1}$ verbindet. Wenn sie von $S_{n+1}$ in Richtung $S_1$ läuft (im Folgenden mit $S_{n+1} \to S_1$ abgekürzt) , ist eine Reise gefunden, die alle Städte besucht, nämlich $S_{n+1} \to S_1 \to S_2 \to \ldots \to S_n$.
  Wenn aber $S_1 \to S_{n+1}$, dann betrachte die Straße zwischen $S_n$ und $S_{n+1}$. Wenn $S_n \leftarrow S_{n+1}$, ist man fertig, da dann $S_1 \to S_2 \to \ldots \to S_n \to S_{n+1}$ alle Städte besucht.
  Wenn aber $S_{n+1} \to S_n$, dann muss es, da $S_{n+1} \to S_n$ aber $S_{n+1} \leftarrow S_1$ eine Stadt $S_i$ mit $(1 \leq i < n)$ geben, so dass $S_i \to S_{n+1}$ und $S_{n+1} \to S_{i+1}$, da ansonsten wegen $S_1 \to S_{n+1}$ und aus $S_i \to S_{n+1}$ folgt stets $S_{i+1} \to S_{n+1}$ für alle $1 \leq i < n$ auch $S_n \to S_{n+1}$ folgen würde (Induktionsprinzip) und dies der Voraussetzung $S_n \leftarrow S_{n+1}$ widerspricht.
  Dann ist aber $S_1 \to \ldots \to S_i \to S_{n+1} \to S_{i+1} \to \ldots \to S_n$ die gesuchte Reise.

Es ist also stets möglich alle Städte zu besuchen.

**1.5.5** Zeigen Sie durch vollständige Induktion, dass die Zahl $n^3 - 4n$ für alle $n \in \mathbb{N}$ mit $n \geq 2$ durch 3 teilbar ist.

**I.A.** $n = 2$: $2^3 - 4 \cdot 2 = 8 - 8 = 0$ ist durch 3 teilbar.

**I.V.** Für ein $n \in \mathbb{N}$ ist $n^3 - 4n$ durch 3 teilbar, d.h. es existiert ein $a \in \mathbb{N}$, so dass gilt:

$$3a = n^3 - 4n$$

**I.S.** $n \to n+1$:

$$\begin{aligned}
(n+1)^3 - 4(n+1) &= n^3 + 3n^2 + 3n - 4n - 3 \\
&= n^3 - 4n + 3n^2 + 3n - 3 \\
&= (n^3 - 4n) + 3(n^2 + n - 1) \\
&\overset{\text{I.V.}}{=} 3a + 3(n^2 + n - 1) \\
&\overset{\text{Distr.-Gesetz}}{=} 3\underbrace{(a + n^2 + n - 1)}_{=:m \in \mathbb{N}} \\
&= 3m
\end{aligned}$$

Also ist $(n+1)^3 - 4(n+1)$ durch 3 teilbar. q.e.d.

**1.5.6** Zeigen Sie durch vollständige Induktion, dass für alle $n \in \mathbb{N}$

$$\sum_{k=1}^{2n} (-1)^k k = n$$

gilt.

**I.A.** $n = 1$: $\sum_{k=1}^{2}(-1)^k k = -1 + 2 = 1 = n$.

**I.V.** $\sum_{k=1}^{2n}(-1)^k k = n$ gilt für ein $n \in \mathbb{N}$.

**I.S.** $n \to n + 1$

$$\begin{aligned}
\sum_{k=1}^{2(n+1)} (-1)^k k \quad &= \quad \sum_{k=1}^{2n}(-1)^k k + (-1)^{2n+1}(2n+1) + \\
&\quad\quad +(-1)^{2n+2}(2n+2) \\
&\overset{\text{I.V.}}{=} \quad n - 2n - 1 + 2n + 2 \\
&= \quad n + 1
\end{aligned}$$

**1.5.7** Beweisen Sie die binomische Formel:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Dabei ist der so genannte Binomialkoeffizient $\binom{n}{k}$ für $k > 0$ durch den Quotienten $n \cdot (n-1) \cdots (n-k+1)/k!$ erklärt, und $\binom{n}{0} := 1$.

**I.A.** $n = 0$ $(a+b)^0 = 1 = \binom{0}{0} a^0 b^0 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{n-k}$.

**I.V.** $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ gilt für ein $n \in \mathbb{N}$.

**I.S.** $n \to n + 1$

$$\begin{aligned}
(a+b)^{n+1} \quad &= \quad (a+b)^n (a+b) \\
&\overset{\text{I.V.}}{=} \quad \left( \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right) (a+b) \\
&= \quad \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k}
\end{aligned}$$

Man mache eine Indexverschiebung im ersten Summanden und verwende $\binom{n}{n+1} = 0$ für den zweiten:

$$= \quad \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k}$$

Nun addiere man den Summanden $\binom{n}{-1} x^{n+1} y^0 = 0$ beim ersten Summanden:

$$= \quad \sum_{k=0}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k}$$

Man verwende jetzt noch

die Tatsache, dass $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$$

## zu 1.6

**1.6.1** Zeigen Sie, dass $\mathbb{Q}$ der kleinste Körper ist, der in $\mathbb{R}$ enthalten ist. (Genauer: Ist $K \subset \mathbb{R}$ bezüglich der üblichen Operationen ein Körper, so gilt $\mathbb{Q} \subset K$.)

Es wird konstruktiv gezeigt, dass jede rationale Zahl $\frac{n}{m}$ (mit $n \in \mathbb{Z}, m \in \mathbb{N}$) in jedem beliebigen Körper, der in $\mathbb{R}$ enhalten ist, liegt.

Sei also $K \subset \mathbb{R}$ ein Körper (mit den von $\mathbb{R}$ geerbten Verknüpfungen), dann gilt:

- $1 \in K \Rightarrow \forall\, n \in \mathbb{N}: \ n \in K$ (Aufgrund der Verknüpfung ‚+' in $\mathbb{R}$
- $\forall\, z \in \mathbb{Z}: \ z \in K$ (wegen $n \in K \Rightarrow \ -n \in K$)
- $\forall\, z \in \mathbb{Z} \setminus \{0\}: \ z^{-1} = \frac{1}{z} \in K$ (wegen $z \in K \setminus \{0\} \Rightarrow z^{-1} \in K$)
- Somit auch $\frac{n}{m} \in K \ \forall\, n \in \mathbb{Z}, m \in \mathbb{N}$ (weil $n \in K, \frac{1}{m} \in K \Rightarrow \frac{n}{m} \in K$)
- Somit gilt: $\mathbb{Q} \subset K$.

Da $\mathbb{Q}$ ein Körper ist, ist somit $\mathbb{Q}$ der kleinste Körper in $\mathbb{R}$.

**1.6.2** Ist $\mathbb{Z}$ wohlgeordnet?

Behauptung: $\mathbb{Z}$ ist nicht wohlgeordnet.

Zu zeigen ist, dass eine nicht leere Teilmenge $T$ von $\mathbb{Z}$ existiert, die kein kleinstes Element besitzt:
Wähle $T = \mathbb{Z}$. Dann gilt für jedes $z \in \mathbb{Z}$ (bzw. aus $T$):

- $z - 1 \in \mathbb{Z}$
- $z - 1 < z$

Angenommen also es würde ein minimales Element $m$ in $T$ existieren, dann wäre $m - 1 \in T$ und echt kleiner als $m$, was im Widerspruch dazu steht, dass $m$ das kleinste Element in $T$ sein sollte.
Also kann $T$ kein kleinstes Element besitzen.

## zu 1.7

**1.7.1** Zeige : Zwischen je zwei rationalen Zahlen, liegt eine irrationale.
Es darf verwendet werden, das es irrationale Zahlen gibt.

Man zeigt zunächst (Hilfssatz) : Ist $k \in \mathbb{R}$ irrational, ist auch $a \cdot k + b$ $(a, b \in \mathbb{Q} \setminus \{0\})$ irrational.
Beweis : Angenommen, $a \cdot k + b$ wäre rational, so wäre auch $k = [(a \cdot k + b) - b] \cdot a^{-1}$ aufgrund der Körpereigenschaften von $\mathbb{Q}$ eine rationale Zahl. Dies ist ein Widerspruch zur Voraussetzung $k \notin \mathbb{Q}$.

Seien nun $q_1, q_2 \in \mathbb{Q}$ mit $q_1 < q_2$ gegeben. Wähle eine irrationale Zahl $k \in \mathbb{R} > 0$. Diese existiert, da irrationale Zahlen nach Voraussetzung existieren, und da mit $r$ nach Hilfssatz auch $-r = -1r$ irrational ist und stets eine der beiden Zahlen $r$ und $-r$ positiv ist ($r \neq 0$, da 0 rational). Aufgrund der Gültigkeit des Archimedes-Axioms in $\mathbb{R}$ gibt es ein $n_0 \in \mathbb{N}$ mit $n_0 > k$. Dann setze $s = \frac{k \cdot (q_2 - q_1)}{n_0} + q_1$ und $s$ ist die gesuchte irrationale Zahl zwischen $q_1$ und $q_2$.
Beweis:

- s ist irrational
  Nach Voraussetzung ist $k$ irrational. Dann folgt aus dem Hilfssatz mit $a = \frac{q_2 - q_1}{n_0} \in \mathbb{Q}$ und $b = q_1 \in \mathbb{Q}$ die Irrationalität von s.

- Es gilt $q_1 < s$, da

$$
\begin{array}{rcccl}
 & 0 & \overset{\text{Voraussetzung}}{<} & k & \\
\overset{q_2 - q_1 > 0}{\Longrightarrow} & 0 & < & k \cdot (q_2 - q_1) & \\
\overset{n_0 > 0}{\Longrightarrow} & 0 & < & \dfrac{k \cdot (q_2 - q_1)}{n_0} & \\
\overset{\text{Monotonie}}{\Longrightarrow} & q_1 & < & \dfrac{k \cdot (q_2 - q_1)}{n_0} + q_1 & \overset{\text{Def.}}{=} s
\end{array}
$$

- Es gilt $s < q_2$, da

$$
\begin{array}{rcccl}
 & & k & \overset{\text{Voraussetzung}}{<} & n_0 \\
 & \overset{\frac{1}{n_0} > 0}{\Longrightarrow} & \dfrac{k}{n_0} & < & 1 \\
 & \overset{q_2 - q_1 > 0}{\Longrightarrow} & \dfrac{k \cdot (q_2 - q_1)}{n_0} & < & q_2 - q_1 \\
\overset{\text{Monotonie}}{\Longrightarrow} \dfrac{k \cdot (q_2 - q_1)}{n_0} + q_1 & \overset{\text{Def.}}{=} & s & < & q_2
\end{array}
$$

## zu 1.8

**1.8.1** Schnittzahlen Dedekindscher Schnitte sind eindeutig bestimmt.
Sei $(A, B)$ ein Dedekindscher Schnitt und angenommen $w, z$ seien Schnittzahlen mit $w \neq z$.
D.h. es gilt:

$a \leq w \leq b$ für alle $a \in A,\ b \in B$

$a \leq z \leq b$ für alle $a \in A,\ b \in B$

Sei o.B.d.A. $w < z$. Seien $a \in A$, $b \in B$ und man betrachte $\frac{w+z}{2}$:

$$\begin{aligned} a \leq w < \frac{w+z}{2} &\Rightarrow \frac{w+z}{2} \in B \\ \frac{w+z}{2} < z \leq b\ &\Rightarrow \frac{w+z}{2} \in A \end{aligned}$$

Also ist $\frac{w+z}{2}$ ein Element von $A \cap B$. Das ist jedoch ein Widerspruch zur Voraussetzung, dass $A \cap B = \emptyset$. Somit kann ein Dedekindscher Schnitt keine zwei verschiedenen Schnittzahlen besitzen.

**1.8.2** Sei $(A, B)$ ein Dedekindscher Schnitt in $\mathbb{R}$. Dann gibt es ein $x_0$, so dass entweder

$$A = \{x|x < x_0\},\ B = \{x|x \geq x_0\}$$

oder

$$A = \{x|x \leq x_0\},\ B = \{x|x > x_0\}$$

gilt.

In $\mathbb{R}$ hat jeder Dedekindsche Schnitt eine Schnittzahl (Definition von $\mathbb{R}$:1.8.2). Hat $(A, B)$ die Schnittzahl $s$, so gilt entweder $s \in A$ oder $s \in B$, da $A \cap B = \emptyset$. Da nach Definition der Schnittzahl immer $a \leq s \leq b$ für alle $a \in A, b \in B$ gilt, gilt im Fall $s \in A$

$$A = \{x|x \leq s\},\ B = \{x|x > s\}$$

und im Fall $s \in B$

$$A = \{x|x < s\},\ B = \{x|x \geq s\}.$$

Mit $s = x_0$ ist dann alles gezeigt.

## zu 1.9

### 1.9.1

$$\begin{aligned}\frac{1+i}{7-i}\frac{7+i}{7+i} &= \frac{6+8i}{50}\\ &= \frac{6}{50}+\frac{8}{50}i\\ \frac{i^3}{7-i}\frac{7+i}{7+i} &= \frac{1-7i}{50}\\ &= \frac{1}{50}-\frac{7}{50}i\end{aligned}$$

$i^{19032003}$: Da $i^4$ wieder 1 ergibt muss man nur noch 19032003 durch 4 teilen und den Rest betrachten. Der Rest ist 3 und somit ist $i^3 = -i$ das Ergebnis.

Die Lösung von $\sum\limits_{n=1}^{50212345123\,02} i^n$ ist etwas länger:

$z = \sum\limits_{n=1}^{5021234512302} i^n$

Zunächst gilt für alle $n \in \mathbb{N}$ offenbar :

$$\begin{array}{lclclcr} i^{4n} & \overset{\text{Pot.gesetz}}{=} & (i^4)^n & \overset{i^2=-1}{=} & ((-1)^2)^n = 1^n & = & 1\\ i^{4n+1} & \overset{\text{Pot.gesetz}}{=} & & & i\cdot i^{4n} = i\cdot 1 & = & i\\ i^{4n+2} & \overset{\text{Pot.gesetz}}{=} & & & i^2\cdot i^{4n} = i^2\cdot 1 & = & -1\\ i^{4n+3} & \overset{\text{Pot.gesetz}}{=} & & & i^3\cdot i^{4n} = i^3\cdot 1 & = & -i\end{array}$$

Desweiteren gilt :

$$\forall n \in \mathbb{N} : \sum_{k=1}^{4n} i^k = 0$$

Beweis durch vollstänige Induktion :

- Induktionsanfang : zu zeigen : $\sum\limits_{k=1}^{4} i^k = 0$
  Es gilt für $n = 1$ :

$$\begin{aligned}\sum_{k=1}^{4} i^k &\overset{\text{Def. von }\Sigma}{=} i^1+i^2+i^3+i^4\\ &\overset{i^2=-1}{=} i-1-i+1\\ &\overset{\text{Kommutativität}}{=} 1-1+i-i=0\end{aligned}$$

- Induktionsvoraussetzung :
  Für $n \in N$ gelte :

$$\sum_{k=1}^{4n} i^k = 0$$

- Induktionsschluss :
  zu zeigen :
$$\sum_{k=1}^{4(n+1)} i^k = 0$$
  Es gilt :
$$\begin{aligned}
\sum_{k=1}^{4(n+1)} i^k &= \sum_{k=1}^{4n+4} i^k \\
&\overset{\text{Def. von } \Sigma}{=} \sum_{k=1}^{4n} i^k + i^{4n+1} + i^{4n+2} + i^{4n+3} + i^{4n+4} \\
&\overset{\text{Induktionsvoraussetzung}}{=} 0 + i^{4n+1} + i^{4n+2} + i^{4n+3} + i^{4(n+1)} \\
&\overset{\text{siehe oben}}{=} i - 1 - i + 1 = 0
\end{aligned}$$

Damit folgt für $z$ :
$$\begin{aligned}
z &= \sum_{n=1}^{5021234512302} i^n \\
&\overset{\text{Def. von } \Sigma}{=} \sum_{n=1}^{5021234512300} i^n + i^{5021234512301} + i^{5021234512302} \\
&= \sum_{n=1}^{4\cdot 1255308628075} i^n + i^{4\cdot 1255308628075+1} + i^{4\cdot 1255308628075+2} \\
&\overset{\text{siehe oben}}{=} 0 + i - 1 = \underline{\underline{-1+i}}
\end{aligned}$$

### 1.9.2 $z = \left(\frac{1+i}{\sqrt{2}}\right)^{21}$

Es gilt :
$$\begin{aligned}
z = \left(\frac{1+i}{\sqrt{2}}\right)^{21} &\overset{\text{Pot.gesetz}}{=} \left(\frac{1+i}{\sqrt{2}}\right)^{20} \cdot \left(\frac{1+i}{\sqrt{2}}\right) \\
&\overset{\text{Pot.gesetz}}{=} \left[\left(\frac{1+i}{\sqrt{2}}\right)^{2}\right]^{10} \cdot \left(\frac{1+i}{\sqrt{2}}\right) \\
&= \left(\frac{1+2i-1}{2}\right)^{10} \cdot \left(\frac{1+i}{\sqrt{2}}\right) \\
&= i^{10} \cdot \left(\frac{1+i}{\sqrt{2}}\right) \\
&\overset{\text{siehe oben}}{=} -1 \cdot \left(\frac{1+i}{\sqrt{2}}\right) \\
&= -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} i = -\frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{2} i
\end{aligned}$$

**1.9.3** Zeichne die folgenden Mengen in der Gaußschen Zahlenebene :

1. $\mathcal{M}_a := \{z \in \mathbb{C} \mid |z-1| = |z+1|\}$
   Wenn man $z \in \mathbb{C}$ als $a + bi$ schreibt, kann man aus der $\mathcal{M}_a$ definierenden Eigenschaft Bedingungen für $a, b$ herleiten, die die $z \in \mathcal{M}_a$ erfüllen müssen, da die Darstellung von $z = a + bi$ eindeutig ist.
   Es sei $z = a + bi \in \mathbb{C}$ beliebig, dann gilt :

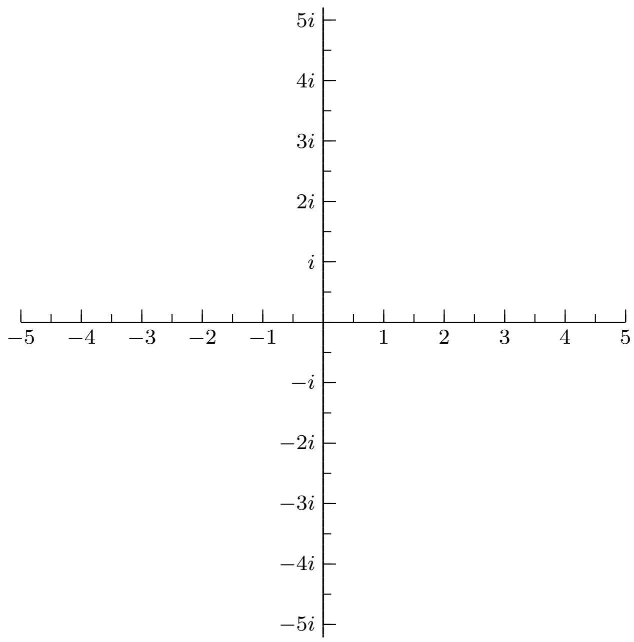
$$\begin{aligned} |z-1| &= |z+1| \\ \overset{\text{Komm, Ass.}}{\iff} |(a-1)+bi| &= |(a+1)+bi| \\ \overset{\text{Def. von }||}{\iff} \sqrt{(a-1)^2+b^2} &= \sqrt{(a+1)^2+b^2} \end{aligned}$$

Zwei Wurzeln sind dann gleich, wenn ihre Radikanden gleich sind.

$$\begin{aligned} \sqrt{(a-1)^2+b^2} &= \sqrt{(a+1)^2+b^2} \\ \iff (a-1)^2+b^2 &= (a+1)^2+b^2 \\ \overset{\text{Distr.}}{\iff} a^2-2a+1+b^2 &= a^2+2a+1+b^2 \\ \iff -2a &= 2a \\ \iff 4a &= 0 \\ \iff a &= 0 \end{aligned}$$

In $\mathcal{M}_a$ liegen also alle $z \in \mathbb{C}$, deren Realteil 0 ist. Das sind aber alle $z$, die die Form $bi$ mit $b \in \mathbb{R}$ haben, also alle $z$ auf der Imaginärachse :

Darstellung von $\mathcal{M}_a$



2. $\mathcal{M}_b := \{z \in \mathbb{C} \mid 1 \leq |z-i| \leq 2\}$
   Die $z \in \mathcal{M}_b$ müssen also zwei Eigenschaften haben, nämlich $|z-i| \geq 1$ und $|z-i| \leq 2$. Man prüft zunächst, welche $z \in \mathbb{C}$ die erste Bedingung erfüllen, indem man sie wie oben umformt, und tut dann gleiches für die zweite.

   - Es sei $z = a + bi \in \mathbb{C}$ bel., dann gilt :

   $$\begin{aligned} |z-i| &\geq 1 \\ \iff |a+bi-i| &\geq 1 \\ \overset{\text{Distr., Ass.}}{\iff} |a+(b-1)i| &\geq 1 \\ \overset{\text{Def. von } ||}{\iff} \sqrt{a^2+(b-1)^2} &\geq 1 \end{aligned}$$

   Die Wurzel kann nur größer als 1 sein, wenn ihr Radikand größer als 1 ist, da $\forall x \in \mathbb{R} : 0 \leq x \leq 1 \iff 0 \leq x^2 \leq 1$ und die Wurzel auf $\mathbb{R}_0^+$ gerade die Umkehrabbildung von $x^2$ ist.

   $$\begin{aligned} \sqrt{a^2+(b-1)^2} &\geq 1 \\ \iff a^2+(b-1)^2 &\geq 1 \\ \iff a^2+(b-1)^2 &\geq 1^2 \end{aligned}$$

   $a^2 + (b-1)^2 = 1^2$ ist gerade die Gleichung eines Kreises mit dem Radius 1 um den Punkt der Gaußschen Zahlenebene, an dem $a = 0$ und $b = 1$ ist, also um $i$. Die Bedingung wird von allen Punkten erfüllt, die auf oder außerhalb dieses Kreises liegen.

   - Es sei $z = a + bi \in \mathbb{C}$ bel., dann gilt :

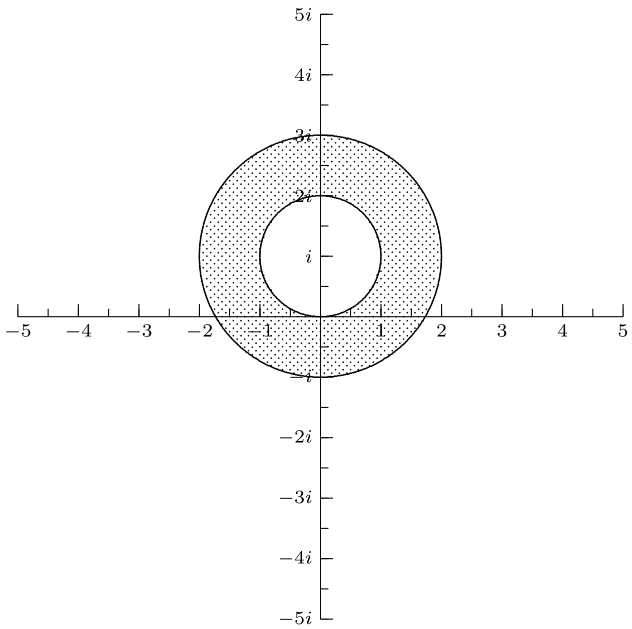
   $$\begin{aligned} |z-i| &\leq 2 \\ \iff |a+bi-i| &\leq 2 \\ \overset{\text{Distr., Ass.}}{\iff} |a+(b-1)i| &\leq 2 \\ \overset{\text{Def. von } ||}{\iff} \sqrt{a^2+(b-1)^2} &\leq 2 \end{aligned}$$

   Die Wurzel kann nur kleiner als 2 sein, wenn ihr Radikand kleiner als 4 ist, da $\forall x \in \mathbb{R} : 0 \leq x \leq 2 \iff 0 \leq x^2 \leq 4$ und die Wurzel auf $\mathbb{R}_0^+$ gerade die Umkehrabbildung von $x^2$ ist.

   $$\begin{aligned} \sqrt{a^2+(b-1)^2} &\leq 4 \\ \iff a^2+(b-1)^2 &\leq 4 \\ \iff a^2+(b-1)^2 &\leq 2^2 \end{aligned}$$

   $a^2 + (b-1)^2 = 2^2$ ist gerade die Gleichung eines Kreises mit dem Radius 2 um den Punkt der Gaußschen Zahlenebene, an dem $a = 0$ und $b = 1$ ist, also um $i$. Die Bedingung wird von allen Punkten erfüllt, die auf oder innerhalb dieses Kreises liegen.

Darstellung von $\mathcal{M}_b$



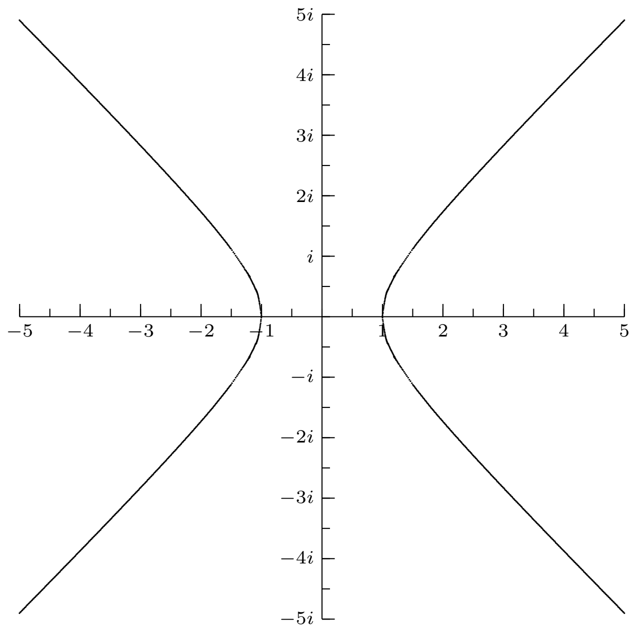

Insgesamt ergibt sich für $\mathcal{M}_b$ die Darstellung als Schnitt der beiden eben beschriebenen Flächen $\mathcal{M}_b$ kann also durch den Kreisring um $i$ mit dem inneren Radius 1 und dem äußeren Radius 2 dargestellt werden.

3. $\mathcal{M}_c := \{z \in \mathbb{C} \mid \mathrm{Re}(z^2) = 1\}$
   Zunächst überlegt man wieder, wie man die Eigenschaft $\mathrm{Re}(z^2) = 1$ als Eigenschaft für $a$ und $b$ schreiben kann, um diese dann als Darstellung einer Kurve in der Gaußschen Zahlenebene zu deuten.
   Sei $z = a + bi \in \mathbb{C}$ beliebig, dann gilt :

$$
\begin{aligned}
\mathrm{Re}(z^2) &= 1 \\
\Longleftrightarrow \mathrm{Re}\big((a+bi)^2\big) &= 1 \\
\overset{\text{Distributivität}}{\Longleftrightarrow} \mathrm{Re}\big(a^2 + 2abi - b^2\big) &= 1 \\
\overset{\text{Kommutativität}}{\Longleftrightarrow} \mathrm{Re}\big((a^2 - b^2) + 2abi\big) &= 1 \\
\overset{\text{Def. von Re()}}{\Longleftrightarrow} a^2 - b^2 &= 1 \\
\overset{1^2=1}{\Longleftrightarrow} a^2 - b^2 &= 1^2
\end{aligned}
$$

Dies ist aber gerade die Gleichung der Einheitshyperbel in der Gaußschen Zahlenebene, $\mathcal{M}_c$ enthält also alle komplexen Zahlen, die durch Punkte auf der Einheitshyperbel repräsentiert werden.

Darstellung von $\mathcal{M}_c$

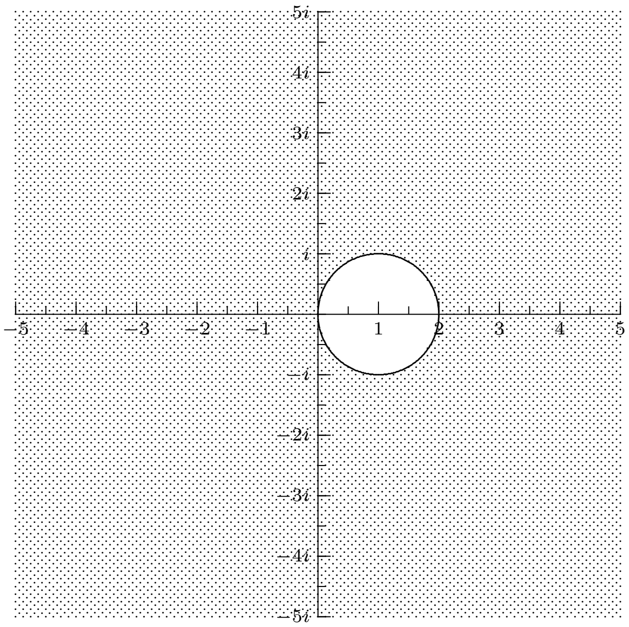



4. $\mathcal{M}_d := \{z \in \mathbb{C} \setminus \{0\} \mid \mathrm{Re}\big(\frac{1}{z}\big) < \frac{1}{2}\}$
   Wie bisher verschafft man sich auch hier eine äquivalente Beziehung zwischen $a$ und $b$.
   Sei $z = a + bi \in \mathbb{C} \setminus \{0\}$, dann gilt :

$$
\begin{aligned}
\mathrm{Re}\left(\frac{1}{z}\right) &< \frac{1}{2} \\
\Longleftrightarrow \mathrm{Re}\left(\frac{1}{a+bi}\right) &< \frac{1}{2} \\
\overset{\text{Erw. mit } \overline{z}}{\Longleftrightarrow} \quad \mathrm{Re}\left(\frac{a-bi}{(a+bi)(a-bi)}\right) &< \frac{1}{2} \\
\overset{\substack{\text{Distr., Ass.,}\\ \text{Komm.}}}{\Longleftrightarrow} \quad \mathrm{Re}\left(\frac{a-bi}{a^2+b^2}\right) &< \frac{1}{2} \\
\overset{\text{Distributivität}}{\Longleftrightarrow} \quad \mathrm{Re}\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i\right) &< \frac{1}{2} \\
\overset{\text{Def. von Re()}}{\Longleftrightarrow} \quad \frac{a}{a^2+b^2} &< \frac{1}{2} \\
\overset{a^2+b^2>0}{\Longleftrightarrow} \quad 2a &< a^2 + b^2 \\
\overset{\text{Monotoniegesetz}}{\Longleftrightarrow} 0 &< a^2 - 2a + b^2 \\
\overset{\text{Monotoniegesetz}}{\Longleftrightarrow} 1 &< a^2 - 2a + 1 + b^2 \\
\overset{\text{Distributivität}}{\Longleftrightarrow} \quad (a-1)^2 + b^2 &> 1^2
\end{aligned}
$$

Zunächst betrachtet man einmal $(a-1)^2 + b^2 = 1^2$, dies ist die Gleichung des um 1 in Richtung der reellen Achse verschobenen Einheitskreises in der Gaußschen Zahlenebene. $(a-1)^2 + b^2 > 1$ gilt also für alle Punkte die „außerhalb"dieses Kreises liegen, gehören zu $\mathcal{M}_d$ alle $z \in \mathbb{C} \setminus \{0\}$, die durch außerhalb dieses Kreises liegende Punkte repräsentiert werden.

Darstellung von $\mathcal{M}_d$




**1.9.4** Beweise das Parallelogrammgesetz für zwei komplexe Zahlen $w$ und $z$ :

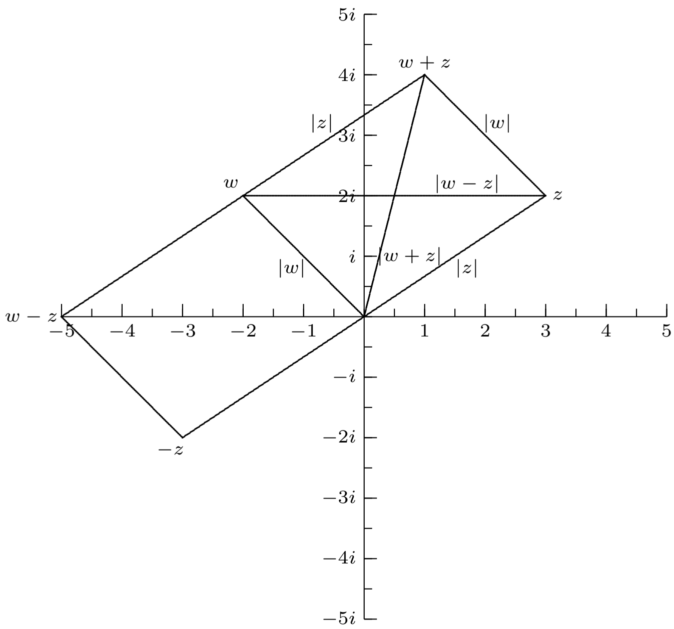
$$|w+z|^2 + |w-z|^2 = 2\left(|w|^2 + |z|^2\right).$$

Offensichtlich gilt mit $\forall z \in \mathbb{C} : |z| = \sqrt{z\overline{z}}$ auch $\forall z \in \mathbb{C} : |z|^2 = z\overline{z}$
Damit gilt : Seien $z, w \in \mathbb{C}$ beliebig :

$$\begin{aligned}
|w+z|^2 + |w-z|^2 &\overset{\text{Def. von } |\cdot|}{=} (w+z)(\overline{w+z}) + (w-z)(\overline{w-z}) \\
&\overset{\text{Konj. ist Isom.}}{=} (w+z)(\overline{w}+\overline{z}) + (w-z)(\overline{w}-\overline{z}) \\
&\overset{\text{Distributivität}}{=} w\overline{w} + \overline{z}w + z\overline{w} + z\overline{z} + w\overline{w} - \overline{z}w - z\overline{w} + z\overline{z} \\
&\overset{\text{Komm., Ass.}}{=} w\overline{w} + w\overline{w} + z\overline{z} + z\overline{z} \\
&\overset{\text{Distributivität}}{=} 2\left(w\overline{w} + z\overline{z}\right) \\
&\overset{z\overline{z} = |z|^2}{=} 2\left(|w|^2 + |z|^2\right)
\end{aligned}$$

Um die geometrische Bedeutung dieses Gesetzes zu veranschaulichen, zeichnet man $z, w, z+w, z-w$ in die Gaußsche Zahlenebene ein, dann bedeutet dieses Gesetz :

Darstellung der Parallelogrammregel




Wie man sieht hat das Parallelogramm mit den Ecken $(0, z, w + z, w)$ die Seitenlängen $|z|$ und $|w|$ und die Diagonalenlängen $|w+z|$ und $|w-z|$. Als geometrische Deutung für das Gesetz ergibt sich :

> Die Summe der Flächeninhalte der Quadrate über den Diagonalen eines Parallelogramms ist gleich der Summe der Flächeninhalte der Quadrate über dessen Seiten.

## zu 1.10

**1.10.1** Zeige, dass $\mathbb{Q} + \mathbb{Q}\sqrt{2}$ (vgl. Aufgabe 1.4.3) abzählbar ist.

Wir wissen, dass $\mathbb{Q}$ abzählbar ist, betrachte nun die Abbildung

$$\begin{array}{rcl} f : \mathbb{Q} & \to & \mathbb{Q}\sqrt{2} \\ q & \mapsto & q\sqrt{2} \end{array}$$

Diese Abbildung $f$ ist bijektiv, da:

- $f$ ist injektiv
  z.z.: $\forall x, y \in \mathbb{Q} : f(x) = f(y) \Longrightarrow x = y$

  Seien also $x, y \in \mathbb{Q}$ mit $f(x) = f(y)$ geg., dann gilt:

  $$f(x) = f(y) \Longleftrightarrow x\sqrt{2} = y\sqrt{2} \Longleftrightarrow x = y$$

  Also ist $f$ injektiv.

- $f$ ist surjektiv
  z.z.: $\forall r \in \mathbb{Q}\sqrt{2}\, \exists q \in \mathbb{Q} : f(q) = r$

  Sei also $r \in \mathbb{Q}\sqrt{2}$ beliebig, $r$ hat nach Def. von $\mathbb{Q}\sqrt{2}$ die Form $r = t\sqrt{2}$ mit $t \in \mathbb{Q}$ passend, dann gilt $f(t) = t\sqrt{2} = r$.
  Also ist $f$ surjektiv.

Da es eine Bijektion zwischen $\mathbb{Q}\sqrt{2}$ und einer abzählbaren Menge gibt, ist auch $\mathbb{Q}\sqrt{2}$ abzählbar.
$\mathbb{Q}$ ist abzählbar, i.e. es gibt eine bijektive Abbildung $g : \mathbb{N} \to \mathbb{Q}$, dann gilt : $\mathbb{Q} = \{g(1), g(2), \ldots\}$, $\mathbb{Q}\sqrt{2}$ ist abzählbar, i.e. es gibt eine bijektive Abbildung $h : \mathbb{N} \to \mathbb{Q}$, dann gilt : $\mathbb{Q}\sqrt{2} = \{h(1), h(2), \ldots\}$.
Man kann nun (Cantorsches Diagonalverfahren) die Menge $\mathbb{Q}+\sqrt{2}$ in folgendem Schema anordnen:

$$\begin{array}{ccccccccc}
f(1)+g(1) & \to & f(2)+g(1) & & f(3)+g(1) & \to & f(4)+g(1) & & \ldots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
f(1)+g(2) & & f(2)+g(2) & & f(3)+g(2) & & f(4)+g(2) & & \ldots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
f(1)+g(3) & & f(2)+g(3) & & f(3)+g(3) & & f(4)+g(3) & & \ldots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
f(1)+g(4) & & f(2)+g(4) & & f(3)+g(4) & & f(4)+g(4) & & \ldots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\vdots & & \vdots & & \vdots & & \vdots & & \ddots
\end{array}$$

Die eingezeichneten Pfeile definieren eine Abbildung $\phi : \mathbb{N} \to \mathbb{Q} + \mathbb{Q}\sqrt{2}$ mit $\phi(n) :=$ das als $n$-tes erreichte Element.

Diese Abbildung ist bijektiv, da jedes Element aus $\mathbb{Q}+\mathbb{Q}\sqrt{2}$ in der Liste vertreten ist, also jedes erreicht wird, also ist $\phi$ surjektiv, andererseits ist aber jedes Element von $\mathbb{Q}+\mathbb{Q}\sqrt{2}$ eindeutig als $f(n)+g(m)$ mit $n, m \in \mathbb{N}$ passend, darstellbar (siehe Übung 1.4.3), also ist jedes Element nur einmal in der Liste vertreten, damit ist $\phi$ injektiv.
$\phi$ ist also eine bijektive Abbildung von $\mathbb{N}$ nach $\mathbb{Q}+\mathbb{Q}\sqrt{2}$, daher ist $\mathbb{Q}+\mathbb{Q}\sqrt{2}$ abzählbar.

**1.10.2** Beweise:

1. Die Menge aller endlichen Teilmengen von $\mathbb{N}$ ist abzählbar.

   Zu zeigen: Es gibt eine bijektive Abbildung von $\mathbb{N}$ in die Menge aller endlichen Teilmengen von $\mathbb{N}$.
   Man kann die endlichen Teilmengen von $\mathbb{N}$ im folgenden quadratischen Schema anordnen (Diagonalverfahren) :

$$\begin{array}{cccccccc}
\emptyset & \{1\} & \{2\} & \{3\} & \{4\} & \{5\} & \{6\} & \cdots \\
\{1,2\} & \{1,3\} & \{2,3\} & \{1,4\} & \{2,4\} & \{3,4\} & \{1,5\} & \cdots \\
\{1,2,3\} & \{1,2,4\} & \{1,3,4\} & \{2,3,4\} & \{1,2,5\} & \{1,3,5\} & \{1,4,5\} & \cdots \\
\{1,2,3,4\} & \{1,2,3,5\} & \{1,2,4,5\} & \{1,3,4,5\} & \{2,3,4,5\} & \cdots & & \\
\{1,2,3,4,5\} & \{1,2,3,4,6\} & \{1,2,3,5,6\} & \cdots & & & & \\
\{1,2,3,4,5,6\} & \{1,2,3,4,5,7\} & \cdots & & & & & \\
\vdots & \vdots & & & & & &
\end{array}$$

   In jeder Zeile sind dabei die Teilmengen von $\mathbb{N}$ lexikographisch geordnet. Jetzt kann man indem man durch dieses Quadrat „wandert", eine bijektive Abbildung zwischen der aufgeschriebenen Menge und $\mathbb{N}$ bestimmen :
   $n \mapsto$ die auf dem Weg als $n$-tes erreichte Menge.

$$\begin{array}{cccccccccccccc}
\emptyset & & \{1\} & \rightarrow & \{2\} & & \{3\} & \rightarrow & \{4\} & & \{5\} & \rightarrow & \{6\} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
\{1,2\} & & \{1,3\} & & \{2,3\} & & \{1,4\} & & \{2,4\} & & \{3,4\} & & \{1,5\} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \\
\{1,2,3\} & & \{1,2,4\} & & \{1,3,4\} & & \{2,3,4\} & & \{1,2,5\} & & \{1,3,5\} & & \{1,4,5\} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
\{1,2,3,4\} & & \{1,2,3,5\} & & \{1,2,4,5\} & & \{1,3,4,5\} & & \{2,3,4,5\} & & \cdots & & & \\
 & \swarrow & & \nearrow & & \swarrow & & & & & & & & \\
\{1,2,3,4,5\} & & \{1,2,3,4,6\} & & \{1,2,3,5,6\} & & \cdots & & & & & & & \\
\downarrow & \nearrow & & \swarrow & & & & & & & & & & \\
\{1,2,3,4,5,6\} & & \{1,2,3,4,5,7\} & & \cdots & & & & & & & & & \\
\vdots & & \vdots & & & & & & & & & & &
\end{array}$$

   Durch dieses Durchlaufen des quadratischen Schemas der endlichen Teilmengen von $\mathbb{N}$ wird folgende Abbildung bestimmt :

$$\begin{aligned}
f : \mathbb{N} &\rightarrow \{C \subset \mathbb{N} \mid C \,\text{endlich}\} \\
1 &\mapsto \emptyset
\end{aligned}$$

$$\begin{array}{ccc} 2 & \mapsto & \{1,2\} \\ 3 & \mapsto & \{1\} \\ 4 & \mapsto & \{2\} \\ 5 & \mapsto & \{1,3\} \\ & \vdots & \end{array}$$

Diese Abbildung ist injektiv, da im Schema jede Menge nur einmal aufgeführt ist und nur einmal erreicht wird, und sie ist surjektiv, da alle endlichen Teilmengen von $\mathbb{N}$ im Schema aufgeführt sind und beim diagonalen durchlaufen alle erreicht werden, es also zu jeder Menge ein $n \in \mathbb{N}$ gibt, das auf sie abgebildet wird.
Die Abbildung ist damit bijektiv und $\{C \subset \mathbb{N} \,|\, C \,\text{endlich}\}$ ist abzählbar, da es zwischen ihr und $\mathbb{N}$ eine Bijektion gibt.

2. Die Menge aller Teilmengen von $\mathbb{N}$ ist überabzählbar.

Zu zeigen: Es gibt keine bijektive Abbildung von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$, das ist die Menge aller Teilmengen von $\mathbb{N}$.
Da jede bijektive Abbildung auch surjektiv ist, reicht es zu zeigen: Es gibt keine surjektive Abbildung von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$.
Man zeigt dies durch einen Widerspruchsbeweis :
Angenommen es existierte $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ mit $f$ surjektiv.
Dann betrachte man die Menge $M := \{x \in \mathbb{N} \,|\, x \notin f(x)\}$. Offensichtlich gilt, da $M$ nur natürliche Zahlen enthält : $M \subset \mathbb{N}$, also $M \in \mathcal{P}(\mathbb{N})$.
Also gibt es, da $f$ surjektiv ist, nach Definition der Surjektivität ein $m \in \mathbb{N}$ mit $f(m) = M$.
Es kann nun aber weder $m \in M$ noch $m \notin M$ gelten, obwohl $M$ wohldefiniert ist, da :
Sei $m \in M$, dann gilt :

$$m \in M \quad \stackrel{f(m)=M}{\Longrightarrow} \quad m \in f(m) \quad \stackrel{\text{Def. von } M}{\Longrightarrow} \quad m \notin M$$

Dies ist ein Widerspruch. Also kann $m \in M$ nicht gelten.
Sei nun $m \notin M$, dann gilt :

$$m \notin M \quad \stackrel{f(m)=M}{\Longrightarrow} \quad m \notin f(m) \quad \stackrel{\text{Def. von } M}{\Longrightarrow} \quad m \in M$$

Auch dies ist ein Widerspruch. Es gilt also weder $m \in M$ noch $m \notin M$.
Da $M$ aber eine wohldefinierte Teilmenge von $\mathbb{N}$ und $m \in \mathbb{N}$ ist, muss entweder $m \in M$ oder $m \notin M$ gelten.
Da sich ein Widerspruch ergibt, war die Voraussetzung, dass eine surjektive Abbildung von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$ existiert falsch.

Also ist $\mathcal{P}(\mathbb{N})$ überabzählbar.

## zu 1.11

**1.11.1** Zu einer komplexen Zahl $z = a + bi$ definiert man ihre konjugierte $\overline{z}$ gemäß $\overline{z} := a - bi$. Zeige, dass die Konjugation, also die Abbildung

$$f : \mathbb{C} \to \mathbb{C},\ z \mapsto \overline{z}$$

ein Körperisomorphismus auf $\mathbb{C}$ ist.

Um zu zeigen dass die Konjugation, also die Abbildung $f$, ein Körperisomorphismus auf $\mathbb{C}$ ist, hat man zu zeigen, dass $f$ alle Bedingungen erfüllt, die ein Körperisomorphismus erfüllen muss, nämlich :

1. $f$ ist bijektiv
2. $\forall z_1, z_2 \in \mathbb{C} : \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
3. $\forall z_1, z_2 \in \mathbb{C} : \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

1. Eine Abbildung $f$ heisst bijektiv, wenn sie sowohl injektiv als auch surjektiv ist.
   - Injektvität : $f$ inj. $\Longleftrightarrow (f(z_1) = f(z_2) \Longrightarrow z_1 = z_2)$
     Es seien $z_1 = a + bi \in \mathbb{C}, z_2 = c + di \in \mathbb{C}$ mit $\overline{z_1} = \overline{z_2}$ gegeben. Zu zeigen $z_1 = z_2$

     $$\begin{aligned} \overline{z_1} &= \overline{z_2} \\ \Longleftrightarrow \overline{a+bi} &= \overline{c+di} \\ \overset{\text{Def. von } \overline{z}}{\Longleftrightarrow} a - bi &= c - di \\ \overset{\text{Def. von } =}{\Longleftrightarrow} a = c &\wedge -b = -d \\ \Longleftrightarrow a = c &\wedge b = d \\ \overset{\text{Def. von } =}{\Longleftrightarrow} a + bi &= c + di \\ \Longleftrightarrow z_1 &= z_2 \end{aligned}$$

     Die Konjugation ist also injektiv.
   - Surjektivität : $f$ surj. $\Longleftrightarrow \forall z_2 \in \mathbb{C}\, \exists z_1 \in \mathbb{C} : f(z_1) = z_2$
     Es sei $z_2 = a + bi \in \mathbb{C}$ bel. gegeben. Dann setze $z_1 = a - bi$. Damit gilt:

     $$\begin{aligned} f(z_1) &= f(a - bi) \\ &\overset{\text{Def. von } f}{=} \overline{a - bi} \\ &\overset{\text{Def. von } \overline{z}}{=} a + bi \\ &= z_2 \end{aligned}$$

     Die Konjugation ist also surjektiv.

Da die Konjugation injektiv und surjektiv ist, ist sie auch bijektiv.

2. Es seien $z_1 = a + bi, z_2 = c + di \in \mathbb{C}$ bel. zu zeigen : $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$

$$\begin{aligned}
\overline{z_1 + z_2} &= \overline{(a+bi)+(c+di)} \\
&\overset{\substack{\text{Komm., Ass.,}\\ \text{Dist.}}}{=} \overline{(a+c)+(b+d)i} \\
&\overset{\text{Def. von } \overline{z}}{=} (a+c)-(b+d)i \\
&\overset{\substack{\text{Komm., Ass.,}\\ \text{Dist.}}}{=} (a-bi)+(c-di) \\
&\overset{\text{Def. von } \overline{z}}{=} \overline{a+bi}+\overline{c+di} \\
&= \overline{z_1}+\overline{z_2}
\end{aligned}$$

Die Konjugation ist also verknüpfungstreu bzgl. ‚+'.

3. Es seien $z_1 = a + bi, z_2 = c + di \in \mathbb{C}$ bel.
Zu zeigen: $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

$$\begin{aligned}
\overline{z_1 \cdot z_2} &= \overline{(a+bi)(c+di)} \\
&\overset{\text{Distributivität}}{=} \overline{ac+bci+adi-bd} \\
&\overset{\substack{\text{Ass., Komm.,}\\ \text{Dist.}}}{=} \overline{(ac-bd)+(ad+bc)i} \\
&\overset{\text{Def. von } \overline{z}}{=} (ac-bd)-(ad+bc)i \\
&\overset{\substack{\text{Ass., Komm.,}\\ \text{Dist.}}}{=} ac-bci-adi-bd \\
&\overset{-1=i^2}{=} ac-bci-adi+bdi^2 \\
&\overset{\text{Distributivität}}{=} (a-bi)c-(a-bi)di \\
&\overset{\text{Distributivität}}{=} (a-bi)(c-di) \\
&\overset{\text{Def. von } \overline{z}}{=} (\overline{a+bi})\cdot(\overline{c+di}) \\
&= \overline{z_1}\cdot\overline{z_2}
\end{aligned}$$

Die Konjugation ist also verknüpfungstreu bzgl. ‚·'.

Da die Konjugation eine bijektive Abbildung von $\mathbb{C}$ nach $\mathbb{C}$ ist, die verknüpfungstreu bzgl. ‚+'und ‚·'ist, ist sie ein Körperisomorphismus auf $\mathbb{C}$.