Kapitel 2

Die reellen Zahlen

Die reellen Zahlen sind uns anschaulich schon aus der Schule bekannt. Wir wollen im Folgenden die charakteristischen Eigenschaften der reellen Zahlen sammeln, von denen wir dann sehen werden, dass diese die reellen Zahlen (bis auf isomorphe Kopien) eindeutig bestimmen. Dass es die reellen Zahlen (also eine Menge mit den charakteristischen Eigenschaften) unter der Annahme der Gültigkeit der Mengenlehre überhaupt gibt, werden wir später sehen.

2.1 Algebraische Struktur der reellen Zahlen

Zuerst wollen wir uns den Operationen + und ·, also der algebraischen Struktur, zuwenden. Die reellen Zahlen mit diesen Operationen sind ein so genannter Körper:

2.1.1 Definition. Sei K eine nichtleere Menge, und es seien Abbildungen, sogenannte *Verknüpfungen*,

$$+ : K \times K \to K \quad \text{und} \quad \cdot : K \times K \to K\,,$$

welche *Addition* und *Multiplikation* genannt werden, gegeben. Das Tripel $\langle K, +, \cdot \rangle$ heißt Körper, falls es zwei ausgezeichnete Elemente $0, 1 \in K$ gibt, sodass folgende Gesetze, auch *Axiome* genannt, gelten. Wir schreiben dabei $x + y$ für $+(x, y)$ und $x \cdot y$ für $\cdot(x, y)$.

(a1) Die Addition ist assoziativ: $(x + y) + z = x + (y + z)$ für alle $x, y, z \in K$.

(a2) 0 ist ein neutrales Element bezüglich +: $x + 0 = x$ für alle $x \in K$.

(a3) Jedes Element $x \in K$ besitzt ein Inverses $-x \in K$ bezüglich +: $x + (-x) = 0$.

(a4) Die Addition ist kommutativ: $x + y = y + x$ für alle $x, y \in K$.

(m1) Die Multiplikation ist assoziativ: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ für alle $x, y, z \in K$.

(m2) 1 ist ein neutrales Element von $K \setminus \{0\}$ bezüglich ·: $x \cdot 1 = x$ für alle $x \in K \setminus \{0\}$.

(m3) Jedes $x \in K \setminus \{0\}$ besitzt ein Inverses bezüglich ·: $x \cdot x^{-1} = 1$.

(m4) Die Multiplikation ist kommutativ: $x \cdot y = y \cdot x$ für alle $x, y \in K$.

(d) Es gilt das Distributivgesetz: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ für alle $x, y, z \in K$.

2.1.2 Bemerkung (*). Elementarer als der Begriff des Körpers ist jener der Gruppe. Eine nichtleere Menge G versehen mit einer Verknüpfung $* : G \times G \to G$ heißt *Gruppe* (man fasst das in dem Paar $\langle G, * \rangle$ zusammen), falls es ein ausgezeichnetes Element $e \in G$ gibt, sodass

(g1) $*$ assoziativ ist: $(x * y) * z = x * (y * z)$ für alle $x, y \in G$;

(g2) e das neutrale Element ist; $x * e = e * x = x$ für alle $x \in G$;

(g3) es für alle $x \in G$ ein $x^{-1} \in G$ gibt mit $x^{-1} * x = x * x^{-1} = e$.

Eine Gruppe $\langle G, * \rangle$ heißt *abelsch* oder auch *kommutativ*, wenn zusätzlich

(g4) $x * y = y * x$ für alle $x, y \in G$.

Mit diesen Begriffen lässt sich ein Körper K kürzer beschreiben. In der Tat ist eine nichtleere Menge K versehen mit Verknüpfungen $+$ und $\cdot$ genau dann ein Körper, wenn $\langle K, + \rangle$ eine abelsche Gruppe mit neutralem Element 0 ist, wenn $\langle K \setminus \{0\}, \cdot \rangle$ auch eine abelsche Gruppe ist, und wenn das Distributivgesetz für $+$ und $\cdot$ gilt.

2.1.3 Bemerkung. Die jeweiligen neutralen Elemente 0 bzw. 1 sind eindeutig bestimmt[1]. Wäre nämlich etwa $\tilde{0}$ ein weiters neutrales Element bezüglich $+$, so folgte aus $(a2)$ und $(a4)$, dass

$$0 = \tilde{0} + 0 = \tilde{0}\,.$$

Dasselbe gilt für die Inversen $-a$ und a^{-1}. Wäre etwa $\tilde{a}$ ein weiteres additiv Inverses zu a, also $a + \tilde{a} = 0$, so folgte

$$\tilde{a} = \tilde{a} + \underbrace{(a + (-a))}_{=0} = \underbrace{(\tilde{a} + a)}_{=0} + (-a) = 0 + (-a) = -a\,.$$

Somit ist $x \mapsto -x$ eine – wie aus unten stehenden Rechenregeln folgt – bijektive Funktion von K auf sich selbst und $x \mapsto x^{-1}$ eine bijektive Funktion von $K \setminus \{0\}$ auf sich selbst.

2.1.4 Beispiel. Man betrachte die Menge $K = \{\between, \pitchfork\}$. Die Verknüpfungen $+$ und $\cdot$ seien gemäß folgender Verknüpfungstafeln definiert:

$+$	$\between$	$\pitchfork$
$\between$	$\between$	$\pitchfork$
$\pitchfork$	$\pitchfork$	$\between$

$\cdot$	$\between$	$\pitchfork$
$\between$	$\between$	$\between$
$\pitchfork$	$\between$	$\pitchfork$

[1] Die ausgezeichneten Elemente 0 und 1 sind zunächst von den gleich bezeichneten, bekannten ganzen Zahlen zu unterscheiden. Sie haben lediglich ähnliche Eigenschaften. Um zu betonen, dass es sich um das additiv bzw. multiplikativ neutrale Element von K handelt, schreibt man auch 0_K bzw. 1_K.

Man erkennt unschwer, dass die Axiome $(a1)$ – $(a4)$, $(m1)$ – $(m4)$ und (d) für einen Körper erfüllt sind, wobei $\emptyset$ des neutrale 0 Element bezüglich + und $\Cap$ des neutrale Element 1 bezüglich $\cdot$ ist. Es sei noch bemerkt, dass jeder Körper mindestens zwei Elemente hat, und somit der hier vorgestellte Körper kleinstmöglich ist.

Wir werden xy für $x \cdot y$ und, falls $y \neq 0$, für xy^{-1} oft $\frac{x}{y}$ schreiben. Um Klammern zu sparen, wollen wir auch übereinkommen, dass Punkt- vor Strichrechnung kommt, also zB. $xy + xz = (xy) + (xz)$. Schließlich werden wir für $x + (-y)$ bzw. $(-x) + y$ auch $x - y$ bzw. $-x + y$ schreiben.

2.1.5 Lemma. *Für einen Körper $\langle K, +, \cdot \rangle$ gelten folgende Rechenregeln:*

(*i*) *Die Inverse von der Inversen ist die Zahl selbst:*
$-(-x) = x$ *für* $x \in K$ *und* $(x^{-1})^{-1} = x$ *für* $x \in K \setminus \{0\}$.

(*ii*) $-(x + y) = (-x) + (-y)$ *für* $x, y \in K$.

(*iii*) $x \cdot 0 = 0$, *aus* $x, y \neq 0$ *folgt* $x \cdot y \neq 0$, $(xy)^{-1} = x^{-1}y^{-1}$, *sowie* $(-x)^{-1} = -(x^{-1})$.
Insbesondere gilt $(-1)(-1) = 1$.

(*iv*) $x(-y) = -xy$, $(-x)(-y) = xy$, $x(y - z) = xy - xz$.

(*v*) $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$.

Beweis. Exemplarisch wollen wir $x \cdot 0 = 0$ und $-(x + y) = (-x) + (-y)$ nachweisen. Wegen $(a2)$ gilt $0 + 0 = 0$ und mit (d) damit auch $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Addieren wir das nach $(a3)$ existierende additiv Inverse von $x \cdot 0$, so folgt mit Hilfe von $(a1)$, dass

$$0 = x \cdot 0 + (-x \cdot 0) = (x \cdot 0 + x \cdot 0) + (-x \cdot 0) = x \cdot 0 + (x \cdot 0 + (-x \cdot 0)) = x \cdot 0 + 0 = x \cdot 0$$

Wegen dem Kommutativgesetz und Assoziativgesetz gilt

$$\begin{aligned}(x + y) + ((-x) + (-y)) &= ((x + y) + (-x)) + (-y) = ((y + x) + (-x)) + (-y) \\ &= \big(y + (x + (-x))\big) + (-y) = ((y + 0) + (-y)) = y + (-y) = 0\,.\end{aligned}$$

Also ist $(-x) + (-y)$ eine additiv Inverse von $x + y$. Wegen Bemerkung 2.1.3 ist diese additiv Inverse aber eindeutig. Also $(-x) + (-y) = -(x + y)$. ❑

Schließlich wollen wir noch einige Schreibweisen festlegen. Sind A und B Teilmenge unseres Körpers K, so setzen wir

$$-A := \{-a : a \in A\} \quad \text{sowie} \quad A + B := \{a + b : a \in A,\ b \in B\}\,.$$

Insbesondere ist $-A$ das Bild von A unter der Abbildung $- : K \to K$ und $A + B$ das Bild von $A \times B$ ($\subseteq K \times K$) unter der Abbildung $+ : K \times K \to K$. Entsprechend seien A^{-1}, $A - B$, etc. definiert.

2.2 Ordnungsstruktur der reellen Zahlen

Eine weitere wichtige Eigenschaft der reellen Zahlen ist die, dass man je zwei Zahlen x und y der Größe nach vergleichen kann. Dabei ist bekannterweise $x < y$ genau dann, wenn $y - x$ eine positive reelle Zahl ist. Um diesen Sachverhalt mathematisch zu fassen, definieren wir

2.2.1 Definition. Sei $\langle K, +, \cdot \rangle$ ein Körper und sei $P \subseteq K$. Dann heißt K (streng genommen $\langle K, +, \cdot, P \rangle$) ein *angeordneter Körper*, wenn

(p1) $K = P \cup \{0\} \cup (-P)$, wobei $P, -P$ disjunkt sind, also $P \cap (-P) = \emptyset$, und beide 0 nicht enthalten[2];

(p2) $x, y \in P \Rightarrow x + y \in P$;

(p3) $x, y \in P \Rightarrow xy \in P$.

Die Menge P heißt die Menge der *positiven* Zahlen. Für $x, y \in K$ sagen wir, dass

- x kleiner als y ist, in Zeichen $x < y$, wenn $y - x \in P$;
- x größer als y ist, in Zeichen $x > y$, wenn $x - y \in P$;
- x kleiner oder gleich y ist, in Zeichen $x \leq y$, wenn $x < y$ oder $x = y$;
- x größer oder gleich y ist, in Zeichen $x \geq y$, wenn $x > y$ oder $x = y$.

2.2.2 Bemerkung. Man beachte, dass man $\leq$ und $<$ sowie $\geq$ und $>$ als Teilmengen von $K \times K$ betrachten kann, indem man etwa $\leq$ als die Menge aller Paar $(x, y) \in K \times K$, für die $y - x \in P \cup \{0\}$ gilt, ansieht. Also sind $\leq, <, \geq, >$ allesamt Relationen auf K.

2.2.3 Lemma. *In einem angeordneten Körper K gelten für beliebige $a, b, x, y, z \in K$ folgende Regeln:*

(*i*) Reflexivität: $x \leq x$.

(*ii*) Antisymmetrie: $(x \leq y \wedge y \leq x) \Rightarrow x = y$.

(*iii*) Transitivität: $(x \leq y \wedge y \leq z) \Rightarrow x \leq z$.

(*iv*) Totalität: $x \leq y \vee y \leq x$.

(*v*) $(x \leq y \wedge a \leq b) \Rightarrow x + a \leq y + b$.

(*vi*) $x \leq y \Rightarrow -x \geq -y$.

(*vii*) $(z > 0 \wedge x \leq y) \Rightarrow xz \leq yz$ *und* $(z < 0 \wedge x \leq y) \Rightarrow xz \geq yz$.

[2] Um bei einer Vereinigung von Mengen zum Ausdruck zu bringen, dass paarweise disjunkte Mengen vereinigt werden, macht man oft einen Punkt über das Vereinigungszeichen; zB. $K = P \dot\cup \{0\} \dot\cup (-P)$.

(*viii*) $x \neq 0 \Rightarrow x^2 > 0$. *Insbesondere:* $1 > 0$.

(*ix*) $x > 0 \Rightarrow x^{-1} > 0$ *und* $x < 0 \Rightarrow x^{-1} < 0$.

(*x*) $0 < x \leq y \Rightarrow (\frac{x}{y} \leq 1 \leq \frac{y}{x} \wedge x^{-1} \geq y^{-1})$.

(*xi*) $(0 < x \leq y \wedge 0 < a \leq b) \Rightarrow xa \leq yb$.

(*xii*) $x < y \Rightarrow x < \frac{x+y}{2} < y$, *wobei* $2 := 1 + 1$.

Beweis. Wir beweisen exemplarisch (*ii*), (*iii*), (*v*), (*viii*) und (*xii*):

(*ii*) $(x \leq y \wedge y \leq x)$ ist per Definitionem dasselbe, wie $y - x \in P \cup \{0\} \wedge x - y \in P \cup \{0\}$. Also $y - x \in (P \cup \{0\}) \cap (-P \cup \{0\}) = \{0\}$, und damit $x = y$.

(*iii*) $(x \leq y \wedge y \leq z) \Leftrightarrow (y - x \in P \cup \{0\} \wedge z - y \in P \cup \{0\})$. Aus $(p2)$ folgt $z - x = (z - y) + (y - x) \in P \cup \{0\}$, also $x \leq z$.

(*v*) $(x \leq y \wedge a \leq b)$ bedeutet $y - x, b - a \in P \cup \{0\}$. Aus $(p2)$ folgt dann $(y + b) - (x + a) = (y - x) + (b - a) \in P \cup \{0\}$; also $x + a \leq y + b$.

(*viii*) Aus $x \neq 0$ folgt $x \in P \cup -P$. Ist $x \in P$, so folgt wegen $(p3)$, dass $x^2 = xx \in P$ und damit $x^2 > 0$. Ist $x \in -P$, so folgt $-x \in P$ und wieder wegen $(p3)$, dass $x^2 = xx = (-x)(-x) \in P$.

(*xii*) Aus $x < y$ und (*v*) folgt $x + x \leq x + y \leq y + y$, wobei weder links noch rechts ein Gleichheitszeichen stehen kann, da sonst durch Addieren von $-x$ bzw. $-y$ die Gleichung $x = y$ folgen würde; also $x + x < x + y < y + y$. Nun ist wegen des Distributivgesetzes $x + x = x(1 + 1)$ und $y + y = y(1 + 1)$. Da wegen $(p2)$, $1 + 1 \in P$, folgt aus (*vii*), dass $x < \frac{x+y}{2} < y$. ❑

2.2.4 Definition. Eine Menge M versehen mit einer Relation R, also $R \subseteq M \times M$, heißt *Halbordnung* auf M, falls R[3]

- R *reflexiv* ist: xRx für alle $x \in M$;
- R *antisymmetrisch* ist: aus xRy, yRz folgt $x = y$;
- R *transitiv* ist: aus xRy, yRz folgt xRz.

Eine Relation R heißt *total*, wenn für je zwei $x, y \in M$ immer xRy oder yRx.
Totale Halbordnungen nennt man *Totalordnung*.

Die Eigenschaften $(i) - (iii)$ und (iv) besagen also, dass $\leq$ eine Totalordnung ist. Wie jede Totalordnung kann man somit jeden angeordneten Körper als Gerade veranschaulichen, wobei eine Zahl x genau dann links von einer anderen Zahl y liegt, wenn sie kleiner ist:

[3] xRy ist eine andere Schreibweise für $(x, y) \in R$.

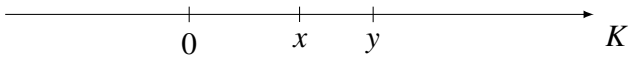

Abbildung 2.1: Zahlengerade

2.2.5 Definition. Sei K eine Menge und $\leq$ eine Totalordnung darauf.

- Sind $x, y \in K$, so sei $\max(x, y)$ das *Maximum* von x und y. Also $\max(x, y) = x$, falls $x \geq y$, und $\max(x, y) = y$ falls $y \geq x$. Entsprechend definiert man das *Minimum* $\min(x, y)$ zweier Zahlen.

- Ist $A \subseteq K$, und gibt es ein $a_0 \in A$, sodass $a \leq a_0$ ($a_0 \leq a$) für alle $a \in A$, so nennt man a_0 das Maximum (Minimum) von A, und schreibt $a_0 = \max A$ ($a_0 = \min A$). Zum Maximum (Minimum) sagt man auch größtes (kleinstes) Element.

- Ist $A \subseteq K$, so heißt A *nach oben beschränkt*, falls es ein $x \in K$ gibt, sodass $A \leq x$, sodass also $a \leq x$ für alle $a \in A$. Jedes $x \in K$ mit $A \leq x$ heißt dabei *obere Schranke* von A. Entsprechend heißt eine Teilmenge A *nach unten beschränkt*, wenn es eine *untere Schranke* in K hat, wenn also $x \leq A$ für ein $x \in K$. Eine nach oben und nach unten beschränkte Teilmenge heißt *beschränkt*.

- Sei $A \subseteq K$ eine nach oben (unten) beschränkte Teilmenge. Hat nun die Menge $\{x \in K : A \leq x\}$ ($\{x \in K : x \leq A\}$) aller oberen (unteren) Schranken von A ein Minimum (Maximum), so heißt dieses *Supremum* (*Infimum*) von A und wird mit $\sup A$ ($\inf A$) bezeichnet.

- Die Tatsache, dass eine Menge $A \subseteq K$ nicht nach oben (nicht unten) beschränkt ist, wollen wir mit der formalen Gleichheit $\sup A = +\infty$ ($\inf A = -\infty$) zum Ausdruck bringen.

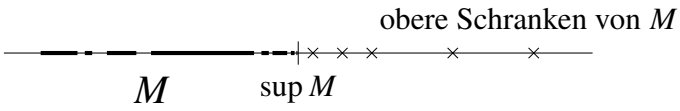

Abbildung 2.2: Supremum der Menge M

2.2.6 Bemerkung. Man sieht leicht, dass jedes Maximum (Minimum) einer Teilmenge auch Supremum (Infimum) dieser Teilmenge ist. Die Umkehrung gilt im Allgemeinen nicht. Es kann auch vorkommen, dass eine beschränkte Teilmenge von K weder ein Supremum, noch ein Infimum hat.

2.2.7 Bemerkung. Wenn das Supremum einer Teilmenge A existiert, so gilt gemäß der Definition $A \leq \sup A$, und $\sup A \leq x$ für alle oberen Schranken x von A. Ist umgekehrt $y \in K$ mit $A \leq y$ und $y \leq x$ für alle oberen Schranken x von A, so folgt aus $A \leq y$, dass y eine obere Schranke von A ist, und aus der zweiten Voraussetzung, dass y das Minimum der oberen Schranken von A ist. Also gilt $y = \sup A$. Entsprechendes lässt sich über das Infimum sagen.

2.2.8 Lemma. *Ist $A \subseteq B \subseteq K$, so gilt*

(*i*) $\{x \in K : A \leq x\} \supseteq \{x \in K : B \leq x\}$ *und* $\{x \in K : x \leq A\} \supseteq \{x \in K : x \leq B\}$.

(*ii*) *Haben A und B ein Maximum (Minimum), so folgt* $\max A \leq \max B$ *(*$\min A \geq \min B$*).*

(*iii*) *Haben A und B ein Supremum (Infimum), so folgt* $\sup A \leq \sup B$ *(*$\inf A \geq \inf B$*).*

Beweis.

(*i*) $t \in \{x \in K : B \leq x\}$ bedingt $b \leq t$ für alle $b \in B$. Wegen $A \subseteq B$ gilt auch $a \leq t$ für alle $a \in A$, und daher $t \in \{x \in K : A \leq x\}$. Die zweite Mengeninklusion beweist man genauso.

(*ii*) Das Maximum von B erfüllt definitionsgemäß $\max B \geq b$ für alle $b \in B$, und damit insbesondere $\max B \geq a$ für alle $a \in A$. Wegen $\max A \in A$ folgt insbesondere $\max B \geq \max A$. Analog zeigt man $\min A \geq \min B$.

(*iii*) Definitionsgemäß gilt $\sup A = \min\{x \in K : A \leq x\}$, $\sup B = \min\{x \in K : B \leq x\}$. Nach (*i*) ist $\{x \in K : B \leq x\} \subseteq \{x \in K : A \leq x\}$, und infolge

$$\sup A = \min\{x \in K : A \leq x\} \leq \min\{x \in K : B \leq x\} = \sup B\,. \qquad \square$$

Ist K ein angeordneter Körper, so gelten für die oben eingeführten Begriffe einfach nachzuprüfende Rechenregeln:

(*i*) Offenbar gilt $x \leq A$ genau dann, wenn $-x \geq -A$. Also ist $A \subseteq K$ genau dann nach oben (unten) beschränkt, wenn $-A$ nach unten (oben) beschränkt ist.

(*ii*) $\min(-A) = -\max A$, $\max(-A) = -\min A$,

(*iii*) $\inf(-A) = -\sup(A)$, $\sup(-A) = -\inf(A)$.

Diese Gleichheiten gelten in dem Sinn, dass die linke Seite des Gleichheitszeichen genau dann existiert, wenn die rechte existiert.

2.2.9 Beispiel. Seien $a, b \in K$. Dann definiert man die Intervalle

$$(a, b) := \{x \in K : a < x < b\},\ \ (a, b] := \{x \in K : a < x \leq b\}\,,$$

und entsprechend

$$[a,b] := \{x \in K : a \le x \le b\},\ \ [a,b) := \{x \in K : a \le x < b\}\,.$$

Außerdem setzt man ($+\infty, -\infty$ sind hier nur formale Ausdrücke)

$$(-\infty,b) := \{x \in K : x < b\},\ \ (-\infty,b] := \{x \in K : x \le b\}\,,$$

$$(a,+\infty) := \{x \in K : a < x\},\ \ [a,+\infty) := \{x \in K : a \le x\}\,.$$

Ist $a < b$, so sind die Mengen $(a,b), [a,b], (a,+\infty)$ z.B. nach unten beschränkt. Nach oben beschränkt sind dagegen nur die ersten beiden. Die Mengen $(a,b), (a,b]$ haben das Supremum b, aber nur für die Menge $(a,b]$ ist b ein Maximum. Um etwa einzusehen, dass $b = \sup(a,b)$, argumentiert man folgendermaßen:
Zunächst ist wegen der Definition von Intervallen $x \le b$ für alle $x \in (a,b)$, also $(a,b) \le b$. Angenommen es gäbe eine obere Schranke y von (a,b) mit $y < b$. Im Falle $y \le a$ wäre $y \le a < \frac{a+b}{2} < b$ (vgl. Lemma 2.2.3, (*xii*)), womit aber y keine obere Schranke sein kann, da $\frac{a+b}{2} \in (a,b)$. Im Falle $a < y$ wäre $a < y < \frac{y+b}{2} < b$, womit wiederum y keine obere Schranke sein kann, da $\frac{y+b}{2} \in (a,b)$. Also ist b tatsächlich die kleinste obere Schranke von (a,b), $\sup(a,b) = b$.

2.2.10 Beispiel. Dem Begriff der rationalen Zahlen vorgreifend seien K die rationalen Zahlen und sei

$$M = \{x \in K : x^2 < 2\}\,.$$

Dann hat diese Menge weder Maximum noch Supremum, obwohl sie nach oben beschränkt ist. Siehe dazu Satz 2.9.5.

Wir wollen noch zwei elementare Funktionen auf einem angeordneten Körper betrachten.

2.2.11 Definition. Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Die Signumfunktion sgn sei jene Funktion von K nach K, sodass für $x \in K$

$$\operatorname{sgn}(x) = \begin{cases} 1\,, & \text{falls } x \in P\,,\\ 0\,, & \text{falls } x = 0\,,\\ -1\,, & \text{falls } x \in -P\,. \end{cases}$$

Die Betragsfunktion $|.| : K \to K$ ist definiert durch

$$|x| = \begin{cases} x\,, & \text{falls } x \in P \cup \{0\}\,,\\ -x\,, & \text{falls } x \in -P\,. \end{cases}$$

2.2.12 Lemma. *Für $x, y \in K$ gilt:*

(*i*) $|x| = \operatorname{sgn}(x)x$.

(*ii*) $|xy| = |x|\,|y|$.

(*iii*) $\max(x,y) = \frac{x+y+|x-y|}{2}$, $\min(x,y) = \frac{x+y-|x-y|}{2}$.

(*iv*) $|x+y| \leq |x| + |y|$.

(*v*) $|x+y| \geq \big||x| - |y|\big|$.

Beweis. (*i*) und (*ii*) bzw. (*iii*) folgen ganz leicht, wenn man die Fälle $x > 0, x = 0, x < 0$ bzw. $x \leq y$ und $x > y$ unterscheidet. Wir zeigen (*iv*) und (*v*):
Die (*iv*) ist klar, falls eine der Zahlen x oder y Null ist. Sonst unterscheiden wir folgende zwei Fälle:

$$\rightsquigarrow \operatorname{sgn}(x) = \operatorname{sgn}(y) \neq 0 \Rightarrow |x+y| = |\operatorname{sgn}(x)(|x| + |y|)| = |x| + |y|$$

$$\rightsquigarrow \operatorname{sgn}(x) = -\operatorname{sgn}(y) \neq 0 \Rightarrow |x+y| = |\operatorname{sgn}(x)(|x| - |y|)| = ||x| - |y|| \leq |x| + |y|$$

Letztere Ungleichung gilt wegen

$$|x| - |y| \leq |x| + |y| \quad \text{und} \quad -(|x| - |y|) = |y| - |x| \leq |x| + |y|\,.$$

Aus (*iv*) folgt $|x| = |(x+y)+(-y)| \leq |x+y| + |y|$ und damit $|x| - |y| \leq |x+y|$. Vertauschen der Variablen ergibt $|y| - |x| \leq |x+y|$. Aus diesen beiden Ungleichungen erhalten wir (*v*). ❑

(*iv*) nennt man auch *Dreiecksungleichung* und (*v*) *Dreiecksungleichung nach unten* für $|.|$.

2.3 Die natürlichen Zahlen

Ob es die oben diskutierten angeordneten Körper überhaupt gibt, davon haben wir uns bisher nicht überzeugen können. Um solche Objekte zu konstruieren, wenden wir uns zunächst den natürlichen Zahlen zu.
Die natürlichen Zahlen sind uns als Objekt des Alltages wohlvertraut, aber ihre Existenz als mathematisches Objekt ist keine Trivialität. Trotzdem wollen wir diese voraussetzen. In der Tat folgt sie aus den Axiomen der Mengenlehre.

2.3.1 Definition. Die *natürlichen Zahlen* sind eine Menge $\mathbb{N}$, in der ein Element $1 \in \mathbb{N}$ ausgezeichnet ist,[4] und auf der eine sogenannte *Nachfolgerabbildung* $' : \mathbb{N} \to \mathbb{N}$ definiert ist, sodass gilt:

(S1) $'$ ist injektiv.

(S2) Es gibt kein $n \in \mathbb{N}$ mit $n' = 1$.

(S3) Ist $M \subseteq \mathbb{N}$, $1 \in M$ und $m' \in M$ für alle $m \in M$, so ist $M = \mathbb{N}$.

Für n' wollen wir auch $n+1$ schreiben.

[4] Die Bezeichnung 1 hat zumindest zum gegenwärtigen Zeitpunkt nichts mit der gleichlautenden Bezeichnung für das multiplikative neutrale Element in einem Körper zu tun.

2.3.2 Bemerkung. Wir wollen anmerken, dass wir zunächst weder die Abbildungen $+, \cdot$, die $\mathbb{N} \times \mathbb{N}$ nach $\mathbb{N}$ abbilden, noch die Möglichkeit zwei natürliche Zahlen der Größe nach zu ordnen, zur Verfügung haben. Obige Festlegung, dass $n' = n + 1$, ist nur symbolisch zu verstehen.

Ehe wir uns an die Definition von Addition und Multiplikation machen, wollen wir uns die Möglichkeit schaffen, Ausdrücke, wie nx, x^n, $\sum_{k=1}^{n} c(k)$ für $n \in \mathbb{N}$ zu definieren, wenn z.B. x und $c(k)$ für $k \in \mathbb{N}$ Elemente eines Körpers sind. Alle diese Ausdrücke haben gemein, dass sie Funktionen $n \mapsto \phi(n)$ auf $\mathbb{N}$ sind, wobei $\phi(1)$ bekannt ist und wobei $\phi(n')$ bekannt ist, wenn $\phi(n)$ es ist. Im Falle von $n \mapsto x^n$ ist etwa $x^1 = x$ und $x^{n'} = x^n \cdot x$. Um einzusehen, warum solche Funktionen eindeutig definiert sind, zeigen wir den

2.3.3 Satz (Rekursionssatz)**.** *Sei A eine Menge, $a \in A$, $g : A \to A$ (Rekursionsfunktion). Dann existiert genau eine Abbildung $\phi : \mathbb{N} \to A$ mit $\phi(1) = a$ und $\phi(n') = g(\phi(n))$.*

Beweis. Betrachte alle Teilmengen $H \subseteq \mathbb{N} \times A$ mit den Eigenschaften

(a) $(1, a) \in H$

(b) Ist $(n, b) \in H$, so gilt auch $(n', g(b)) \in H$.

Solche Teilmengen existieren, da z.B. $\mathbb{N} \times A$ die Eigenschaften (a) und (b) hat. Sei D der Durchschnitt aller solchen Teilmengen:

$$D := \bigcap_{H \text{ erfüllt } (a) \text{ und } (b)} H$$

Da $(1, a) \in H$ für alle H, die (a) und (b) erfüllen, ist auch $(1, a) \in D$. Ist $(n, b) \in D$, so gilt $(n, b) \in H$ für alle (a) und (b) erfüllenden H. Nach (b) folgt $(n', g(b)) \in H$ für alle solchen H, und somit $(n', g(b)) \in D$. Also hat D auch die Eigenschaften (a) und (b), und ist damit die kleinste Teilmenge mit diesen Eigenschaften.
Wir behaupten, dass D eine Funktion von $\mathbb{N}$ nach A ist, also, dass es zu jedem $n \in \mathbb{N}$ genau ein $b \in A$ gibt, sodass $(n, b) \in D$; vgl. Definition 1.2.1. Dazu reicht es zu zeigen, dass[5]

$$M = \{n \in \mathbb{N} : \exists!\ b \in A, (n, b) \in D\}$$

mit $\mathbb{N}$ übereinstimmt. Wir prüfen das mit Hilfe von $(S\,3)$ nach.
Zunächst ist $1 \in M$, da einerseits $(1, a) \in D$. Gäbe es andererseits ein weiteres $c \in A, c \neq a$ mit $(1, c) \in D$, so betrachte $D \setminus \{(1, c)\}$. Klarerweise hat $D \setminus \{(1, c)\}$ die Eigenschaft (a). Wegen $(S\,2)$ bleibt auch die Eigenschaft (b) erhalten. Das ist ein Widerspruch dazu, dass D kleinstmöglich ist.
Nun zeigen wir, dass mit n auch n' in M liegt. Für $n \in M$ gibt es genau ein $b \in A$ mit $(n, b) \in D$. Also ist auch $(n', g(b)) \in D$. Wäre noch $(n', c) \in D$ mit $c \neq g(b)$, so kann man wieder $D \setminus \{(n', c)\}$ betrachten. Weil $n' \neq 1$, erfüllt $D \setminus \{(n', c)\}$ Eigenschaft (a).

[5] $\exists!$ steht für: *Es gibt genau ein*

Aus $(k,d) \in D \setminus \{(n',c)\} \subseteq D$ folgt $(k', g(d)) \in D$. Ist $k \neq n$, so folgt wegen $(S\,1)$ daher auch $(k', g(d)) \neq (n', c)$. Ist $n = k$, so muss wegen $n \in M$ die Gleichheit $d = b$ gelten. Es folgt $(k', g(d)) = (n', g(b)) \neq (n', c)$. In jedem Fall gilt also $(k', g(d)) \in D \setminus \{(n', c)\}$, und $D \setminus \{(n', c)\}$ erfüllt auch (b). Das ist wieder ein Widerspruch dazu, dass D kleinstmöglich ist.
Aus $(S\,3)$ folgt $M = \mathbb{N}$. Nach Definition 1.2.1 kann man also D auffassen als Abbildung $\phi : \mathbb{N} \to A$. Die Eigenschaft (a) bedeutet $\phi(1) = a$, und (b) besagt $\phi(n') = g(\phi(n))$.
Wäre $\tilde{\phi}$ eine weitere Funktion mit $\tilde{\phi}(1) = a$ und mit $\tilde{\phi}(n') = g(\tilde{\phi}(n))$, und betrachtet man $\tilde{\phi}$ als Teilmenge $\tilde{D}$ von $\mathbb{N} \times A$, so erfüllt $\tilde{D}$ Eigenschaften $(a), (b)$. Weil wir schon wissen, dass D die kleinste solche Menge ist, folgt $D \subseteq \tilde{D}$. Da aber beide Funktionen sind, muss $D = \tilde{D}$ bzw. $\phi = \tilde{\phi}$. ❑

2.3.4 Beispiel. Satz 2.3.3 rechtfertigt rekursive Definitionen:

(*i*) Zum Beispiel die Funktion $n \mapsto x^n$, wobei x in einem Körper K liegt. Dafür nehmen wir $A = K$, $a = x$ und $g : K \to K,\ y \mapsto yx$. Nach Satz 2.3.3 ist dann x^n für alle $n \in \mathbb{N}$ eindeutig definiert.

(*ii*) Genauso kann man $n \mapsto nx$ definieren.

(*iii*) Um $n \mapsto \prod_{k=1}^{n} c(k)$ zu definieren, wenn $c : \mathbb{N} \to K$ ist, wenden wir Satz 2.3.3 mit $A = \mathbb{N} \times K$, $a = (1, c(1))$ und $g : \mathbb{N} \times K \to \mathbb{N} \times K,\ (n, x) \mapsto (n', x \cdot c(n'))$ an, und definieren $\prod_{k=1}^{n} c(k)$ als die zweite Komponente von $\phi(n)$.

(*iv*) Genauso kann man $n \mapsto \sum_{k=1}^{n} c(k)$, $n \mapsto \max_{k=1,\dots,n} c(k)$ und ähnliche Ausdrücke definieren.

Für $\sum\limits_{k=1}^{n} c(k)$ schreiben wir auch $c(1) + \cdots + c(n)$. Entsprechend setzen wir

$$c(1) \cdot \cdots \cdot c(n) := \prod_{k=1}^{n} c(k) \quad \text{und} \quad \max(c(1), \dots, c(n)) = \max_{k=1,\dots,n} c(k)\,.$$

Als weitere Anwendung des Rekursionssatzes erhalten wir, dass die natürlichen Zahlen im Wesentlichen eindeutig sind.

2.3.5 Korollar. *Seien $\mathbb{N}$ und $\tilde{\mathbb{N}}$ Mengen mit ausgezeichneten Elementen $1 \in \mathbb{N}$ und $\tilde{1} \in \tilde{\mathbb{N}}$ und Abbildungen $' : \mathbb{N} \to \mathbb{N}$, $\tilde{}: \tilde{\mathbb{N}} \to \tilde{\mathbb{N}}$, sodass für beide die Axiome (S1), (S2) und (S3) gelten. Dann gibt es eine eindeutige bijektive Abbildung $\varphi : \mathbb{N} \to \tilde{\mathbb{N}}$ mit $\varphi(1) = \tilde{1}$ und $\widetilde{\varphi(n)} = \varphi(n')$, $n \in \mathbb{N}$.*

Beweis. Wendet man den Rekursionssatz an auf $A = \tilde{\mathbb{N}}$, $a = \tilde{1}$, und $g = \tilde{}$, so folgt, dass genau eine Abbildung $\varphi : \mathbb{N} \to \tilde{\mathbb{N}}$ existiert mit $\varphi(1) = \tilde{1}$ und $\widetilde{\varphi(n)} = \varphi(n')$, $n \in \mathbb{N}$. Durch Vertauschung der Rollen von $\mathbb{N}$ und $\tilde{\mathbb{N}}$ erhält man eine Abbildung $\psi : \tilde{\mathbb{N}} \to \mathbb{N}$ mit $\psi(\tilde{1}) = 1$ und $\psi(x)' = \psi(\tilde{x})$, $x \in \tilde{\mathbb{N}}$.
Betrachte die Abbildung $\Phi = \psi \circ \varphi : \mathbb{N} \to \mathbb{N}$. Es gilt $\Phi(1) = 1$ und

$$\Phi(n)' = \big(\psi(\varphi(n))\big)' = \psi(\widetilde{\varphi(n)}) = (\psi \circ \varphi)(n')\,.$$

Die identische Abbildung $\mathrm{id}_{\mathbb{N}}$ hat dieselben Eigenschaften, also folgt nach der Eindeutigkeitsaussage des Rekursionssatzes $\Phi = \mathrm{id}_{\mathbb{N}}$. Analog zeigt man $\varphi \circ \psi = \mathrm{id}_{\tilde{\mathbb{N}}}$, also ist φ bijektiv und es gilt $\varphi^{-1} = \psi$. ❑

Wenn wir uns den Beweis des Rekursionssatzes nochmals anschauen, so haben wir gezeigt, dass D eine Funktion auf $\mathbb{N}$ ist, es also zu jedem $n \in \mathbb{N}$ genau ein $b \in A$ gibt mit $(n, b) \in D$, indem wir die Menge M aller in diesem Sinne „guten" $n \in \mathbb{N}$ hernehmen und davon zeigen, dass sie die Voraussetzungen von $(S\,3)$ erfüllen. Diese Vorgangsweise kann man auf alle Aussagen $A(n)$ ausdehnen, die für alle natürliche Zahlen n gelten sollen. Das führt zum sogenannten

Prinzip der vollständigen Induktion: Für jedes $n \in \mathbb{N}$ sei $A(n)$ eine Aussage über die natürliche Zahl n. Dabei gelte:

(*i*) *Induktionsanfang*: Die Aussage $A(1)$ ist wahr.

(*ii*) *Induktionsschritt*: Für jedes $n \in \mathbb{N}$ ist wahr, dass aus der Gültigkeit von $A(n)$ die Gültigkeit von $A(n')$ folgt.

Dann ist die Aussage $A(n)$ für jede natürliche Zahl n richtig.

Um das einzusehen, betrachte man die Menge M aller $n \in \mathbb{N}$, für die $A(n)$ richtig ist. Ist nun $A(1)$ richtig, so ist $1 \in M$, und aus $A(n) \Rightarrow A(n')$ sehen wir, dass mit $m \in M$ auch $m' \in M$. Nach Axiom $(S\,3)$ ist $M = \mathbb{N}$. Also ist $A(n)$ für jede natürliche Zahl n richtig.

2.3.6 Beispiel. Als erstes Beispiel für die Anwendung der Methode der vollständigen Induktion, wollen wir zeigen, dass für einen angeordneter Körper $\langle K, +, \cdot, P\rangle$ und $y \in K$ mit $y \geq 0$, also $y \in P \cup \{0\}$, immer $ny \geq 0$ für alle $n \in \mathbb{N}$ gilt. Die zu beweisende Aussage $A(n)$ ist also

$$ny \geq 0 \quad \text{für alle} \quad n \in \mathbb{N}\,.$$

Induktionsanfang: $A(1)$, daher $1y = y \geq 0$, gilt voraussetzungsgemäß.
Induktionsschritt: Gilt $A(n)$, daher $ny \geq 0$, so folgt $n'y = y + ny \geq 0$, da ja

$$(P \cup \{0\}) + (P \cup \{0\}) \subseteq P \cup \{0\}\,.$$

Also gilt $A(n')$, wenn wir $A(n)$ voraussetzen.

Als weitere Anwendung der Beweismethode der vollständigen Induktion bringen wir die später verwendete *Bernoullische Ungleichung*.

2.3.7 Lemma. *Ist $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper, und bezeichnen wir das multiplikative neutrale Element mit 1_K, so folgt für $x \in K,\ x \geq -1_K$, und $n \in \mathbb{N}$, dass*

$$(1_K + x)^n \geq 1_K + nx\,.$$

Beweis. *Induktionsanfang*: Ist $n = 1$, so besagt die Bernoullische Ungleichung $(1_K + x)^n = 1_K + x \geq 1_K + x$, was offenbar stimmt.
Induktionsschritt: Angenommen die Bernoullische Ungleichung sei nun für $n \in \mathbb{N}$ richtig. Dann folgt wegen $1_K + x \geq 0$, dass

$$(1_K + x)^{n'} = (1_K + x)^n(1_K + x) \geq (1_K + nx)(1_K + x) = 1_K + (n')x + nx^2 \geq 1_K + n'x\,.$$

❑

2.3.8 Beispiel. Eine andere unmittelbare Anwendung des Beweisprinzips der vollständigen Induktion ist die Verifikation der offensichtlich für Ausdrücke wie $\sum_{k=1}^{n} c(k)$ geltenden Rechenregeln, etwa des Distributivgesetzes

$$a\sum_{k=1}^{n} c(k) = \sum_{k=1}^{n}(ac(k))\,.$$

Induktionsanfang: Ist $n = 1$, so gilt $a\sum_{k=1}^{1} c(k) = ac(1) = \sum_{k=1}^{1}(ac(k))$.
Induktionsschritt: Angenommen die Rechenregel gilt für n, so rechnen wir:

$$\begin{aligned} a\sum_{k=1}^{n'} c(k) &= a(\left(\sum_{k=1}^{n} c(k)\right) + c(n')) = a\left(\sum_{k=1}^{n} c(k)\right) + ac(n') \\ &= \sum_{k=1}^{n}(ac(k)) + ac(n') = \sum_{k=1}^{n'}(ac(k))\,. \end{aligned}$$

Entsprechend zeigt man auch andere Rechenregeln für solche induktiv definierten Ausdrücke.

Wir kommen nun zur Diskussion der algebraischen Operationen Addition und Multiplikation, sowie der Ordnungsrelation auf $\mathbb{N}$. Ihre Existenz und ihre Eigenschaften müssen wir nun mit mathematischer Strenge aus den Axiomen $(S\,1)$, $(S\,2)$, $(S\,3)$ mittels logischer Schlüsse herleiten. Hauptinstrument dabei wird wieder der Rekursionssatz Satz 2.3.3 sein.

2.3.9 Definition. Wir definieren für jedes $m \in \mathbb{N}$ Abbildungen $+_m : \mathbb{N} \to \mathbb{N}$ und $\cdot_m : \mathbb{N} \to \mathbb{N}$ rekursiv durch

$$\begin{aligned} +_m(1) &:= m' \quad \text{und} \quad +_m(n') := (+_m(n))'\,, \\ \cdot_m(1) &:= m \quad \text{und} \quad \cdot_m(n') := +_m(\cdot_m(n))\,. \end{aligned}$$

Weiters definieren wir Relationen $<$ und $\leq$ auf $\mathbb{N}$ durch

$$\begin{aligned} n < m &:\Leftrightarrow (\exists t \in \mathbb{N} : +_t(n) = m)\,, \\ n \leq m &:\Leftrightarrow (n = m) \text{ oder } (n < m)\,. \end{aligned}$$

Sind $m, n \in \mathbb{N}$, so schreibt man

$$+_m(n) =: m + n,\ \cdot_m(n) =: m \cdot n,$$

und spricht von der *Addition* bzw. *Multiplikation* auf $\mathbb{N}$.

2.3.10 Satz.

⇝ *Für jedes $m \in \mathbb{N}$ sind die Abbildungen $+_m$ und $\cdot_m$ injektiv, wobei $+_m(n) \neq m$ für alle $n \in \mathbb{N}$.*

⇝ *Die Addition im Bereich $\mathbb{N}$ der natürlichen Zahlen erfüllt die Gesetze*

- *Für alle $a, b, c \in \mathbb{N}$ gilt $(a + b) + c = a + (b + c)$. (*Assoziativität*)*
- *Für alle $a, b \in \mathbb{N}$ gilt $a + b = b + a$. (*Kommutativität*)*

sowie die Kürzungsregel

- *Sind $n, m, k \in \mathbb{N}$ und gilt $k + m = k + n$, so folgt $m = n$.*

⇝ *Die Multiplikation ist ebenfalls assoziativ, kommutativ und erfüllt die Kürzungsregel, also folgt aus $k \cdot m = k \cdot n$, dass $m = n$. Zusätzlich gilt noch*

- *Für jedes $a \in \mathbb{N}$ ist $a \cdot 1 = 1 \cdot a = a$. (*Existenz des neutralen Elementes*)*

⇝ *Die Addition hängt mit der Multiplikation zusammen über das* Distributivgesetz

- *Für $a, b, c \in \mathbb{N}$ gilt stets $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.*

⇝ *Die Relation $\leq$ ist eine Totalordnung mit 1 als kleinstes Element, und aus $m < n$ folgt $m \neq n$. Zudem gelten folgende Verträglichkeiten mit den Operationen Plus und Mal:*

- *Sind $a, b, c \in \mathbb{N}$ und gilt $a < b$ $(a \leq b)$, so folgt $a + c < b + c$ $(a + c \leq b + c)$.*
- *Sind $a, b, c \in \mathbb{N}$ und gilt $a < b$ $(a \leq b)$, so folgt $a \cdot c < b \cdot c$ $(a \cdot c \leq b \cdot c)$.*

Weiters gilt

- *Sind $n, m, l \in \mathbb{N}$ mit $n + l < m + l$ $(n + l \leq m + l)$ oder $n \cdot l < m \cdot l$ $(n \cdot l \leq m \cdot l)$, so folgt $n < m$ $(n \leq m)$.*
- *Sind $n, m \in \mathbb{N}$, $n < m$, so gibt es ein eindeutiges $t \in \mathbb{N}$, sodass $m = n + t$. Wir setzen in diesem Falle*
$$m - n := t\,. \tag{2.1}$$
- *Sind $m, n, t \in \mathbb{N}$, $t < n < m$, so folgt $n - t < m - t$.*
- *Sind $l, m, n \in \mathbb{N}$, $n + m < l$, so folgt $n < l - m$ und*
$$l - (m + n) = (l - m) - n\,. \tag{2.2}$$

Beweis.

⇝ Zur Assoziativität von +:

Seien $k, m \in \mathbb{N}$ fest gewählt, wir führen Induktion nach n durch.
Induktionsanfang: $(k + m) + 1 = +_k(m)' = +_k(m') = k + (m + 1)$.
Induktionsschritt: Nach Induktionsvoraussetzung gilt $(k + m) + n = k + (m + n)$. Es folgt

$$\begin{aligned}(k + m) + (n') &= +_{k+m}(n') = +_{k+m}(n)' = ((k + m) + n)' = \\ &= (k + (m + n))' = +_k(m + n)' = +_k((m + n)') \\ &= k + (m + n')\,,\end{aligned}$$

wobei letztere Gleichheit wegen des schon gezeigten Induktionsanfangs folgt.

⇝ Zur Kommutativität von +:

Wir zeigen $\forall m, n \in \mathbb{N} : m + n = n + m$ mittels Induktion nach m.
Induktionsanfang ($m = 1$): Wir zeigen

$$\forall n \in \mathbb{N} : 1 + n = n + 1 \tag{2.3}$$

mittels Induktion nach n. Der Fall $n = 1$ ist klar, denn $1 + 1 = 1 + 1$. Für den Induktionsschritt $n \to n'$ gehen wir aus von der Induktionsvoraussetzung $1 + n = n + 1$. Daraus folgt

$$n' + 1 = n'' = (n + 1)' = (1 + n)' = 1 + n'\,.$$

Induktionsschritt ($m \to m'$): Wir zeigen

$$(\forall n \in \mathbb{N} : m + n = n + m) \Longrightarrow (\forall n \in \mathbb{N} : m' + n = n + m')\,.$$

Dazu führen wir Induktion nach n durch. Betrachte also zuerst den Fall $n = 1$. Nach der bereits bewiesenen Aussage (2.3) mit vertauschten Rollen von m und n gilt $m' + 1 = 1 + m'$.

Der Induktionsschritt $n \to n'$ hat nun als Induktionsvoraussetzung $m' + n = n + m'$ und wir erhalten

$$\begin{aligned}m' + n' &= (m' + n)' = (n + m')' = (n + m)'' \\ &\overset{*}{=} (m + n)'' = (m + n')' \overset{*}{=} (n' + m)' = n' + m'\,.\end{aligned}$$

An den mit $*$ gekennzeichneten Stellen ist die Induktionsvoraussetzung des Induktionsschritts ($m \to m'$) benützt worden.

⇝ Zur Injektivität von $+_m$ und der Tatsache, dass $+_m(n) \neq m$, für alle $n \in \mathbb{N}$:

Für $m = 1$ ist $+_m(n) = n'$. Nach $(S\,1)$ ist $+_1$ injektiv und nach $(S\,2)$ gilt $+_1(n) \neq 1$.

Sei nun $m \in \mathbb{N}$ und $+_m$ injektiv und erfülle $+_m(n) \neq m$ für alle $n \in \mathbb{N}$.

Es folgt $+_{m'}(n) = m' + n = m + (n + 1) = +_m(n')$. Also ist $+_{m'}$ die Zusammensetzung der injektiven Abbildungen $(n \to n')$ und $+_m$ und somit selbst injektiv.

Aus $m + 1 = m' = +_{m'}(n) = (m + n) + 1$ folgt wegen der Injektivität von $+_1$, dass $m = m + n = +_m(n)$ im Widerspruch zur Induktionsvoraussetzung.

Die Kürzungsregel für + folgt sofort aus der Injektivität von $+_k$.

$\rightsquigarrow$ $m < n$ bedeutet $n = m + k$ mit einem $k \in \mathbb{N}$. Aus $m = n$ würde der Widerspruch $m = m + k = +_m(k)$ folgen.

$\rightsquigarrow$ Es gilt $a \cdot 1 = 1 \cdot a = a,\ a \in \mathbb{N}$:

Unmittelbar aus der Definition 2.3.9 folgt $a \cdot 1 = \cdot_a(1) = a$. Die zweite Gleichheit zeigen wir mittels Induktion nach a:
Induktionsanfang $(a = 1)$: $1 \cdot a = 1 \cdot 1 = 1 = a$.
Induktionsschritt $(a \to a')$: Wir nehmen also $1 \cdot a = a$ an und schließen

$$1 \cdot (a') = \cdot_1(a') = +_1(\cdot_1(a)) = +_1(1 \cdot a) = 1 + a = a' .$$

$\rightsquigarrow$ Zur Kommutativität von $\cdot$:

Wir zeigen $\forall m, n \in \mathbb{N} : m \cdot n = n \cdot m$ mittels Induktion nach m.
Induktionsanfang $(m = 1)$: Nach dem letzten Punkt gilt $\forall n \in \mathbb{N} : 1 \cdot n = n = n \cdot 1$.
Induktionsschritt $(m \to m')$: Wir zeigen

$$(\forall n \in \mathbb{N} : m \cdot n = n \cdot m) \Longrightarrow (\forall n \in \mathbb{N} : m' \cdot n = n \cdot m') .$$

Dazu führen wir Induktion nach n durch. Betrachte also zuerst den Fall $n = 1$. Wieder nach dem letzten Punkt gilt $(m') \cdot 1 = m' = 1 \cdot m'$.

Der Induktionsschritt $n \to n'$ hat nun als Induktionsvoraussetzung $m' \cdot n = n \cdot m'$ und wir erhalten

$$\begin{aligned} m' \cdot n' &= m' + (m' \cdot n) = m' + (n \cdot m') = (m + 1) + (n + (n \cdot m)) \\ &= (n + 1) + (m + (n \cdot m)) \overset{*}{=} (n + 1) + (m + (m \cdot n)) \\ &= n' + (m \cdot n') \overset{*}{=} n' + (n' \cdot m) = n' \cdot m' . \end{aligned}$$

An den mit $*$ gekennzeichneten Stellen ist die Induktionsvoraussetzung des Induktionsschritts $(m \to m')$ benützt worden.

$\rightsquigarrow$ Zum Distributivgesetz:

Vollständige Induktion nach a:
Induktionsanfang $(a = 1)$: Da 1 bezüglich $\cdot$ ein neutrales Element ist, folgt

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

Induktionsschritt:

$$\begin{aligned}(b+c)\cdot(a+1) &= (b+c)+((b+c)\cdot a) \overset{*}{=} (b+c)+((b\cdot a)+(c\cdot a))\\ &= (b+(b\cdot a))+(c+(c\cdot a)) = (b\cdot(a+1))+(c\cdot(a+1))\,.\end{aligned}$$

An der mit $*$ gekennzeichneten Stelle ist die Induktionsvoraussetzung eingegangen.

$\rightsquigarrow$ Zur Assoziativität von $\cdot$:

Wir zeigen $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ mittels Induktion nach b.
Induktionsanfang: $a\cdot(1\cdot c) = a\cdot c = (a\cdot 1)\cdot c$.
Induktionsschritt: Nach Induktionsvoraussetzung gilt also $(a\cdot b)\cdot c = a\cdot(b\cdot c)$. Mittels Distributivgesetz folgt

$$\begin{aligned}(a\cdot(b+1))\cdot c &= ((a\cdot b)+(a\cdot 1))\cdot c = ((a\cdot b)\cdot c)+((a\cdot 1)\cdot c)\\ &= (a\cdot(b\cdot c))+(a\cdot(1\cdot c)) = a\cdot((b\cdot c)+(1\cdot c))\\ &= a\cdot((b+1)\cdot c)\,.\end{aligned}$$

$\rightsquigarrow$ Zur Totalität von $\leq$ und zur Tatsache $1\leq n,\ n\in\mathbb{N}$:

Wir wollen zeigen, dass je zwei $n,m\in\mathbb{N}$ bezüglich $\leq$ vergleichbar sind, was wir mittels Induktion nach m beweisen werden.

Für $m = 1$ zeigt man leicht mittels Induktion nach n, dass immer $n = 1$, oder $\exists t\in\mathbb{N},\ n = 1+t$, also immer $1\leq n$.

Gelte die Vergleichbarkeit von m mit allen $n\in\mathbb{N}$. Um sie für m' zu zeigen, machen wir eine Fallunterscheidung: Ist $m = n$, so folgt $n+1 = m'$ also $n\leq m'$.

Aus $n < m$ folgt $m = n+t$ für ein $t\in\mathbb{N}$, und daher $m' = n+(t+1)$, also $n < m'$. Ist $n = m+1$, so folgt $m' = n$.

Ist schließlich $m < n, n\neq m+1$, so gilt $n = m+t$ mit $t\neq 1$. Aus der schon bewiesenen Vergleichbarkeit mit 1 folgt, dass $1 < t$, und somit $t = 1+s,\ s\in\mathbb{N}$. Aus der Assoziativität folgt $n = m'+s$, also $m' < n$.

$\rightsquigarrow$ Die Reflexivität von $\leq$ ist klar.

$\rightsquigarrow$ Zur Transitivität von $<$ und damit von $\leq$:

Sei $k,l,m\in\mathbb{N}$ und $k\leq l,\ l\leq m$. Ist $k = l$ oder $l = m$, so sieht man sofort, dass $k\leq m$.

Im Fall $k < l,\ l < m$ gibt es $i,j\in\mathbb{N}$ mit $k+i = l,\ l+j = m$. Es folgt $k+(i+j) = m$ und daher $k < m$.

$\rightsquigarrow$ Die Antisymmetrie von $\leq$ folgt, da aus $n\leq m$ und $m\leq n$ im Falle $m\neq n$ wegen des vorletzten Punktes und wegen der Transitivität von $<$ folgt $n < n$, was dem vorletzten Punkt widerspricht.

⇝ Zur Verträglichkeit von $<$ mit $+$ und $\cdot$:

Sei $n < m$ und $k \in \mathbb{N}$. Somit ist $n + t = m$ mit $t \in \mathbb{N}$, und es gilt

$$m + k = (n + t) + k = n + (t + k) = n + (k + t) = (n + k) + t\,,$$

sowie

$$m \cdot k = (n + t) \cdot k = (n \cdot k) + (t \cdot k)\,.$$

Also folgt $n + k < m + k$ und $n \cdot k < m \cdot k$.

⇝ Die Injektivität von $\cdot_k$ bzw. – was dasselbe ist – die Kürzungsregel für $\cdot$ folgt nun aus den gezeigten Eigenschaften von $\leq$:

Seien $k, m, n \in \mathbb{N}$ mit $m \neq n$. Wegen der Totalität gilt $m < n$ oder $n < m$, was mit der Verträglichkeit von $<$ mit $\cdot$ bedingt, dass $k \cdot m < k \cdot n$ oder $k \cdot n < k \cdot m$ und somit $k \cdot m \neq k \cdot n$.

⇝ Zum Kürzen in Ungleichungen:

Aus $n + l < m + l$ folgt definitionsgemäß $m + l = (n + l) + k$ für ein $k \in \mathbb{N}$. Gemäß der Kürzungsregel für $+$ folgt $m = n + k$ und somit $n < m$.

Sei nun $n \cdot l < m \cdot l$. Wäre $m \leq n$, so folgte aus dem letzten Punkt der Widerspruch $m \cdot l \leq n \cdot l$. Wegen der Totalität muss $n < m$ gelten.

⇝ Zur Wohldefiniertheit von $m - n$:

Sei also $n < m$. Definitionsgemäß ist $m = n + t$ für ein $t \in \mathbb{N}$. Ist nun $m = n + s$ für eine weitere Zahl $s \in \mathbb{N}$, so folgt aus der Kürzungsregel für $+$ und $n + t = n + s$, dass $s = t$. Also ist $m - n := t$ eindeutig dadurch definiert, dass $n + t = m$.

⇝ Zur Verträglichkeit von $<$ mit $-$:

Ist $t < n < m$, so folgt $n = t + s$ und $m = n + l$ für $s, l \in \mathbb{N}$, und weiters $m = t + (l + s)$. Somit ist $m - t = l + s$ und $n - t = s$, und daher $n - t < m - t$.

⇝ Zu (2.2):

Die Ungleichung $m + n < l$ bedeutet $l = (m + n) + k$ für ein eindeutiges $k \in \mathbb{N}$. Definitionsgemäß ist daher $k = l - (m + n)$. Andererseits gilt wegen $m < m + n < l$ auch $l = m + s,\ s \in \mathbb{N}$.

Wegen der Kürzungsregel für $+$ folgt $s = n + k$, und somit $n < s = l - m$. Außerdem ist $k = s - n = (l - m) - n$. ❑

2.3.11 Bemerkung. Ist $\tilde{\mathbb{N}}$ eine Kopie von $\mathbb{N}$ wie in Korollar 2.3.5, und werden die Operationen $+$ und $\cdot$, sowie $\leq$ auf $\tilde{\mathbb{N}}$ genauso definiert wie auf $\mathbb{N}$, so sieht man leicht, dass die nach Korollar 2.3.5 existierende Abbildung $\varphi : \mathbb{N} \to \tilde{\mathbb{N}}$ mit den Operationen und $<$ (und daher auch mit $\leq$) verträglich ist:

$$\varphi(n + m) = \varphi(n) + \varphi(m),\ \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m),$$

$$n < m \Leftrightarrow \varphi(n) < \varphi(m)\,.$$

Folgende Eigenschaft der natürlichen Zahlen werden wir oft verwenden.

2.3.12 Satz. *Ist $\emptyset \neq T \subseteq \mathbb{N}$, so hat T ein Minimum.*

Beweis. Wir nehmen das Gegenteil an. Sei

$$M = \{n \in \mathbb{N} : \forall m \in T \Rightarrow n < m\}.$$

Zunächst gilt $1 \in M$, da sonst 1 das Minimum von T wäre. Ist $n \in M$, und $m \in T$, so folgt $n < m$. Daraus schließen wir $n + 1 \leq m$. Wäre $n + 1 = m_0$ für ein $m_0 \in T$, so hätte T das Minimum m_0. Wir nehmen aber an, dass es ein solches nicht gibt. Also gilt immer $n + 1 < m,\ m \in T$, bzw. $n + 1 \in M$. Nach $(S\,3)$ folgt $M = \mathbb{N}$. Ist $m \in T \subseteq \mathbb{N}$, so folgt $m \in M$ und daher der Widerspruch $m < m$. ❑

2.3.13 Bemerkung. Diese Eigenschaft der natürlichen Zahlen können wir hernehmen, um folgende *Variante des Prinzips der vollständigen Induktion* zu rechtfertigen.

- Sei $A(n)$, $n \in \mathbb{N}$, eine Aussage über die natürliche Zahl n, und gelte:

  (*i*) Die Aussage $A(1)$ ist wahr.

  (*ii*) Es gelte für jedes $n \in \mathbb{N},\ n > 1$: Ist die Aussage $A(m)$ wahr für alle $m < n$, so ist auch $A(n)$ wahr.

  Dann ist die Aussage $A(n)$ für alle $n \in \mathbb{N}$ wahr. Denn wäre die Menge der $n \in \mathbb{N}$, für die $A(n)$ falsch ist, nicht leer, so hätte sie ein Minimum n. Wegen (*i*) ist aber $n > 1$, wegen (*ii*) ist $A(n)$ wahr, was offensichtlich ein Widerspruch ist.

Ist eine Aussage erst ab einer gewissen Zahl n_0 richtig, so kann man folgende Varianten des Prinzips der vollständigen Induktion anzuwenden versuchen.

- Gelte:

  (*i*) Die Aussage $A(n_0)$ ist wahr.

  (*ii*) Ist $A(n)$ wahr für ein $n \geq n_0$, dann ist $A(n + 1)$ wahr.

  Dann ist die Aussage $A(n)$ für alle $n \geq n_0$ richtig.

- Gelte:

  (*i*) Die Aussage $A(n_0)$ ist wahr.

  (*ii*) Ist $n > n_0$ und ist $A(m)$ wahr für alle m mit $n_0 \leq m < n$, dann ist $A(n)$ wahr.

  Dann ist die Aussage $A(n)$ für alle $n \geq n_0$ richtig.

2.3.14 Beispiel. Mit fast demselben Beweis wie in Lemma 2.3.7, jedoch mit einer Induktion bei 2 startend, zeigt man, dass für $x \geq -1_K$ und $x \neq 0$ sowie $n \geq 2$ sogar

$$(1_K + x)^n > 1_K + nx\,.$$

Induktionsanfang: Ist $n = 2$, so gilt wegen $x^2 > 0$, dass $(1_K + x)^2 = 1_K + 2x + x^2 > 1_K + 2x$.
Induktionsschritt: Angenommen die Ungleichung ist für $n \in \mathbb{N}$ richtig. Dann folgt wegen $1_K + x \geq 0$ und $nx^2 > 0$, dass

$$(1_K + x)^{n'} = (1_K + x)^n(1_K + x) \geq (1_K + nx)(1_K + x) = 1_K + (n')x + nx^2 > 1_K + n'x\,.$$

Klarerweise haben unendliche Teilmengen von $\mathbb{N}$ kein Maximum. Aber wie intuitiv klar ist, hat jede endliche Teilmenge einer total geordneten Menge ein Maximum und ein Minimum. Um das exakt nachzuweisen, benötigen wir die genaue Definition von Endlichkeit.

2.3.15 Definition. Eine nichtleere Menge M heißt *endlich*, wenn es ein $k \in \mathbb{N}$ und eine bijektive Funktion $f : \{n \in \mathbb{N} : n \leq k\} \to M$ gibt. Die Zahl k ist dann die *Mächtigkeit* von M[6]. Man sagt auch, dass M genau k Elemente hat. Die leere Menge nennen wir auch endlich, und ihre Mächtigkeit sei Null.

2.3.16 Bemerkung. Man zeigt elementar durch vollständige Induktion nach der Mächtigkeit der endlichen Menge M, dass alle ihre Teilmengen auch endlich sind.

2.3.17 Lemma. *Jede endliche nichtleere Teilmenge M einer total geordneten Menge $\langle T, \leq\rangle$ hat ein Minimum und ein Maximum, das wir mit* $\min(M)$ *bzw. mit* $\max(M)$ *bezeichnen. Insbesondere gilt diese Aussage für endliche Teilmengen von angeordneten Körpern und von* $\mathbb{N}$.

Beweis. Wir zeigen die Existenz eines Maximums von endlichen Mengen M durch vollständige Induktion nach der Mächtigkeit von M. Die Existenz eines Minimums von endlichen Mengen wird analog bewiesen. Enthält M nur ein Element m, so ist klarerweise m das Maximum von M.
Angenommen alle $\tilde{M} \subseteq T$ mit n Elementen haben ein Maximum. Hat nun $M \subseteq T$ genau $n + 1$ Elemente und ist $m_1 \in M$, so hat $M \setminus \{m_1\}$ genau n Elemente und laut Induktionsvoraussetzung ein Maximum $m_2 \in M \setminus \{m_1\}$. Da $\langle T, \leq\rangle$ eine Totalordnung ist, gilt $m_1 \leq m_2$ oder $m_1 \geq m_2$. Im ersten Fall ist dann m_2 das Maximum von M und im zweiten ist m_1 das Maximum von M. ❑

Eine immer wieder verwendete Tatsache ist im folgenden Lemma vermerkt.

2.3.18 Lemma. *Sei $M \subseteq \mathbb{N}$ nicht endlich. Dann gibt es eine streng monoton wachsende Bijektion ϕ von $\mathbb{N}$ auf M. Für eine solche gilt immer $\phi(n) \geq n$.*

[6] Damit die Mächtigkeit wohldefiniert ist, muss man noch zeigen, dass es im Fall $k_1 \neq k_2$ keine bijektive Funktion von $\{n \in \mathbb{N} : n \leq k_1\}$ auf $\{n \in \mathbb{N} : n \leq k_2\}$ gibt, was sich durch vollständige Induktion bewerkstelligen lässt.

Beweis. Sei $g : M \to M$ definiert durch $g(s) = \min\{m \in M : m > s\}$, und sei $a = \min M$. Man beachte, dass $g(s)$ für alle $s \in M$ definiert ist, da $\{m \in M : m > s\}$ nach Voraussetzung und wegen Bemerkung 2.3.16 niemals leer ist. Nach dem Rekursionssatz gibt es eine eindeutige Abbildung $\phi : \mathbb{N} \to M$ mit $\phi(1) = a = \min M$ und

$$\phi(n+1) = g(\phi(n)) = \min\{m \in M : m > \phi(n)\}\,.$$

Offensichtlich gilt $\phi(n+1) > \phi(n)$. Daraus folgt durch vollständige Induktion, dass $\phi(l) > \phi(k)$, wenn $l > k$. Also ist ϕ streng monoton wachsend und somit auch injektiv. Durch vollständige Induktion schließt man leicht von $\phi(l) > \phi(k)$ auf $\phi(n) \geq n$ für alle $n \in \mathbb{N}$.
Wäre ein $m_1 \in M$ nicht im Bild von ϕ, so ist klarerweise $m_1 > \min M = \phi(1)$. Angenommen $m_1 > \phi(n)$. Dann ist $m_1 \in \{m \in M : m > \phi(n)\}$ und wegen $m_1 \neq \phi(n+1) = \min\{m \in M : m > \phi(n)\}$ muss $m_1 > \phi(n+1)$. Es folgt $\phi(n) < m_1$ für alle $n \in \mathbb{N}$, was aber $\phi(m_1) \geq m_1$ widerspricht. ❑

2.4 Die ganzen Zahlen

Im Bereich der natürlichen Zahlen haben wir zuletzt Operationen + und · definiert. Ist $m < n$, so haben wir auch $n - m \in \mathbb{N}$ definiert. Wir wollen nun aus den natürlichen Zahlen die ganzen Zahlen $\mathbb{Z}$ konstruieren, und die Operationen + und · auf $\mathbb{Z}$ so fortsetzen. Die Menge $\mathbb{Z}$ zu definieren, ist kein Problem.

2.4.1 Definition. Seien $\mathbb{N}_1$ und $\mathbb{N}_2$ zwei disjunkte Kopien der natürlichen Zahlen, und sei 0 ein Element, das in keiner dieser Mengen enthalten ist[7]. Wir definieren

$$\mathbb{Z} := \mathbb{N}_1 \dot\cup \{0\} \dot\cup \mathbb{N}_2\,.$$

Ist $\varphi : \mathbb{N}_1 \to \mathbb{N}_2$ eine bijektive Abbildung wie in Korollar 2.3.5, so definieren wir eine Abbildung $- : \mathbb{Z} \to \mathbb{Z}$

$$-n = \begin{cases} \varphi(n)\,, & \text{falls } n \in \mathbb{N}_1\,, \\ 0\,, & \text{falls } n = 0\,, \\ \varphi^{-1}(n)\,, & \text{falls } n \in \mathbb{N}_2\,. \end{cases}$$

Schreiben wir nun $\mathbb{N}$ für $\mathbb{N}_1$, so gilt

$$\mathbb{Z} = -\mathbb{N} \dot\cup \{0\} \dot\cup \mathbb{N}.$$

Man erkennt unschwer, dass $-$ eine Bijektion ist, die mit sich selber zusammengesetzt die Identität ergibt, also eine *Involution* ist.
Nun definieren wir die Operationen auf $\mathbb{Z}$ in der Art und Weise, wie wir sie der Anschauung nach erwarten.

[7] Man kann z.B. für $\mathbb{N}_j$ einfach die Menge $\mathbb{N} \times \{j\}$ hernehmen, und für 0 das Element $(1, 3)$

2.4.2 Definition. Für $n \in \mathbb{N}$ setzen wir $\operatorname{sgn}(n) := 1$, $\operatorname{sgn}(-n) := -1$, $\operatorname{sgn}(0) = 0$ sowie $|n| := n$, $|-n| := n$ und $|0| := 0$. Weiters sei $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definiert durch[8]

$$p + q := \begin{cases} p + q\,, & \text{falls } p, q \in \mathbb{N}\,, \\ -(|p| + |q|)\,, & \text{falls } -p, -q \in \mathbb{N}\,, \\ p - |q|\,, & \text{falls } p, -q \in \mathbb{N},\ p > -q\,, \\ -(|q| - p)\,, & \text{falls } p, -q \in \mathbb{N},\ p < -q\,, \\ -(|p| - q)\,, & \text{falls } -p, q \in \mathbb{N},\ -p > q\,, \\ q - |p|\,, & \text{falls } -p, q \in \mathbb{N},\ -p < q\,, \\ 0\,, & \text{falls } q = -p\,, \\ p\,, & \text{falls } q = 0\,, \\ q\,, & \text{falls } p = 0\,, \end{cases}$$

und $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ durch[8]

$$p \cdot q := \begin{cases} |p| \cdot |q|\,, & \text{falls } q, p \neq 0,\ \operatorname{sgn}(q) = \operatorname{sgn}(p)\,, \\ -(|p| \cdot |q|)\,, & \text{falls } q, p \neq 0,\ \operatorname{sgn}(q) = -\operatorname{sgn}(p)\,, \\ 0\,, & \text{falls } q = 0 \text{ oder } p = 0\,. \end{cases}$$

Sind $p, q \in \mathbb{Z}$, so schreibt man wie schon zuvor für $p + (-q)$ auch $p - q$.

Offenbar sind $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ und $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ Fortsetzungen der Verknüpfungen $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ und $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ aus Definition 2.3.9. Sind $p, q \in \mathbb{N}$ mit $q < p$, so stimmt dann $p + (-q) = p - q$ mit der Differenz $p - q$ zweier Zahlen aus $\mathbb{N}$ wie in Satz 2.3.10 überein.

2.4.3 Satz. *Für $\langle \mathbb{Z}, +, \cdot \rangle$ gelten folgende Eigenschaften:*

- *Die Addition ist kommutativ und assoziativ,* 0 *ist ein bzgl. + neutrales Element und $-p$ ist das zu $p \in \mathbb{Z}$ bzgl. + inverse Element. Also gelten* $(a1)$-$(a4)$ *von Definition 2.1.1.*
- *Die Multiplikation ist kommutativ und assoziativ, und* 1 *ist ein bzgl. $\cdot$ neutrales Element. Also gelten* $(m1)$,$(m2)$,$(m4)$ *von Definition 2.1.1.*
- *Es gilt das Distributivgesetz.*
- Integritätseigenschaft*: Aus $p \neq 0 \wedge q \neq 0$ folgt $pq \neq 0$.*

Beweis. Seien $p, q \in \mathbb{Z}$. Zunächst folgen $p + q = q + p$ und $p \cdot q = q \cdot p$ unmittelbar aus der Definition und eben der Tatsache, dass diese Operationen auf $\mathbb{N}$ kommutativ sind.

[8] $+$ und $\cdot$ rechts sind hier die Verknüpfungen auf $\mathbb{N}$ wie in Definition 2.3.9. Die Verknüpfung $-$ von zwei Zahlen aus $\mathbb{N}$ – die erste größer als die zweite – ist jene aus Satz 2.3.10, und das $-$ vorne ist die oben definierte Involution $- : \mathbb{Z} \to \mathbb{Z}$.

Ebenfalls unmittelbar aus der Definition sieht man, dass $p + 0 = p$ und $p \cdot 1 = p$. Also ist 0 ein bezüglich + und 1 ein bezüglich $\cdot$ neutrales Element. Genauso elementar verifiziert man $p + (-p) = 0$ und $p \cdot q \neq 0$, wenn p und q beide $\neq 0$.
Es bleibt die Assoziativität und das Distributivgesetz nachzuprüfen. Das ist in der Tat mühsam und durch zahlreiche Fallunterscheidungen zu bewerkstelligen. Wir wollen daher nur $r + (q + p) = (r + q) + p$ im exemplarischen Fall $r, q \in \mathbb{N},\ -p \in \mathbb{N}$ betrachten:
Für $|p| > r + q$ gilt $(r + q) + p = -(|p| - (r + q))$, und nach (2.2) ist dieser Ausdruck gleich $-((|p| - q) - r)$. Wegen $|p| - q > r$ und $|p| > q$ folgt definitionsgemäß $-((|p| - q) - r) = r + (-(|p| - q)) = r + (p + q)$.
Im Falle $|p| = r + q$ gilt einerseits $(r + q) + p = 0$ und andererseits wegen $|p| > q$ und $|p| - q = r$ (siehe (2.1)), dass $r + (q + p) = r + (-(|p| - q)) = 0$.
Sei nun $|p| < r + q$. Dann folgt $(r + q) + p = (r + q) - |p| =: k \in \mathbb{N}$. Also ist k jene Zahl, sodass $|p| + k = r + q$.
Ist $q > |p|$, so gilt andererseits $r + (q + p) = r + (q - |p|)$, und wegen der bekannten Rechenregeln auf $\mathbb{N}$, $|p| + (r + (q - |p|)) = r + q$, also $k = r + (q + p)$.
Wenn $q = |p|$, so folgt $r + (q + p) = r$, und ebenfalls $|p| + r = r + q$, d. h. $k = r + (q + p)$.
Ist schließlich $q < |p|$, so folgt $r+(q+p) = r+(-(|p|-q))$. Da $|p| < r+q$ folgt $r > |p|-q$, und somit $r + (-(|p| - q)) = r - (|p| - q) =: l \in \mathbb{N}$. Das ist also jene Zahl, sodass $(|p| - q) + l = r$. Addiert man hier q und verwendet die Assoziativität von + auf $\mathbb{N}$, so folgt $|p| + l = r + q$, also $l = k$. ❑

2.4.4 Bemerkung (*)**.** Ausgehend vom Begriff der Gruppe wie in Bemerkung 2.1.2 nennt man eine nichtleere Menge R versehen mit zwei Verknüpfungen + und $\cdot$ einen *Ring*, wenn $\langle R, + \rangle$ eine abelsche Gruppe ist, wenn für $\cdot$ das Assoziativgesetz gilt, und wenn für + und $\cdot$ das Distributivgesetz gilt.
Ein Ring heißt *kommutativ*, wenn die Verknüpfung $\cdot$ kommutativ ist. Ein Ring heißt *Ring mit Einselement*, wenn es ein bezüglich $\cdot$ neutrales Element gibt, und ein Ring heißt *Integritätsring* bzw. *Integritätsbereich*, wenn die Integritätseigenschaft, $p \neq 0 \wedge q \neq 0$ impliziert $pq \neq 0$, gilt.
Insbesondere ist $\langle \mathbb{Z}, +, \cdot \rangle$ ein kommutativer Integritätsring mit Einselement.

2.4.5 Bemerkung. Aus der Integritätseigenschaft erhalten wir:

$$m \neq 0, xm = ym \Rightarrow y = x\,,$$

denn aus $xm - ym = (x - y)m = 0$ folgt ja $x - y = 0$.

Wir benötigen noch eine Totalordnung auf $\mathbb{Z}$, welche $\leq$ auf $\mathbb{N}$ erweitert.

2.4.6 Definition. Wir definieren für $p, q \in \mathbb{Z}$

$$q < p :\Leftrightarrow p - q \in \mathbb{N} \quad \text{und} \quad q \leq p :\Leftrightarrow q < p \vee q = p\,. \tag{2.4}$$

Man sieht leicht ein, dass mit $\leq$ eine Totalordnung auf $\mathbb{Z}$ definiert ist, die $\leq$ auf $\mathbb{N}$ erweitert, und die mit den Operationen + und $\cdot$ verträglich ist.

2.4.7 Bemerkung. Wenn man sich an die Definition eines angeordneten Körpers in Definition 2.2.1 erinnert, so haben wir die Existenz einer Teilmenge $P \subseteq K$ verlangt, die $(p1)$ - $(p3)$ erfüllt. Genau diese Situation haben wir hier mit $P = \mathbb{N}$, nur, dass $\mathbb{Z}$ kein Körper, sondern ein Ring ist. Die von uns definierte Totalordnung $\leq$ auf $\mathbb{Z}$ erfüllt auch alle Eigenschaften, die für die entsprechende Totalordnung auf einem angeordneten Körper gelten; vgl. Lemma 2.2.3. Ausgenommen sind nur die Eigenschaften, die sich auf die multiplikativ Inverse beziehen.

2.4.8 Bemerkung. Die ganzen Zahlen sind eindeutig in dem Sinn, dass wenn $\tilde{\mathbb{Z}}$ neben $\mathbb{Z}$ eine weitere Menge versehen mit einer Involution $\tilde{-} : \tilde{\mathbb{Z}} \to \tilde{\mathbb{Z}}$, mit Operationen $\tilde{+}, \tilde{\cdot}$ und einer Relation $\tilde{\leq}$ ist, sodass $\tilde{\mathbb{Z}}$ eine Kopie $\tilde{\mathbb{N}}$ der natürlichen Zahlen enthält, $\tilde{\mathbb{Z}}$ geschrieben werden kann als die disjunkte Vereinigung von $-\tilde{\mathbb{N}}$, $\{0\}$ und $\tilde{\mathbb{N}}$, die Operationen $\tilde{+}$ und $\tilde{\cdot}$ wie in Definition 2.4.2 durch die entsprechenden Operationen auf $\tilde{\mathbb{N}}$ (siehe Bemerkung 2.3.11) definiert sind, und sodass $\tilde{\leq}$ wie in (2.4) definiert ist, es eine eindeutige Bijektion $\phi : \mathbb{Z} \to \tilde{\mathbb{Z}}$ gibt mit

$$\phi(-p) = -\phi(p),\ \phi(1) = \tilde{1},\ \phi(n+1) = \phi(n)\tilde{+}\tilde{1},\ p \in \mathbb{Z}, n \in \mathbb{N}\,.$$

Um das zu zeigen, setzt man einfach die Bijektion φ aus Korollar 2.3.5 zu einer Bijektion ϕ von $\mathbb{Z}$ auf $\tilde{\mathbb{Z}}$ gemäß der Forderung $\phi(-p) = -\phi(p)$ fort. Die erhaltene Bijektion $\mathbb{Z} \to \tilde{\mathbb{Z}}$ ist mit $+, \cdot, -$ und $<$ (und daher auch mit $\leq$) verträglich. Siehe dazu auch Bemerkung 2.3.11.

Wir haben im Abschnitt über die natürlichen Zahlen für eine Zahl x aus einem Körper ihre Potenzen $x^n,\ n \in \mathbb{N}$ definiert (siehe Beispiel 2.3.4). Das wollen wir auf $\mathbb{Z}$ ausdehnen.

2.4.9 Definition. Sei $\langle K, +, \cdot\rangle$ ein Körper. Für eine ganze Zahl p und eine Zahl $x \in K,\ x \neq 0$ definieren wir

$$x^p = \begin{cases} x^p\,, & \text{falls } p \in \mathbb{N}\,, \\ 1\,, & \text{falls } p = 0\,, \\ \frac{1}{x^{-p}}\,, & \text{falls } p \in -\mathbb{N}\,. \end{cases}$$

Für $x \in K \setminus \{0\},\ p, q \in \mathbb{Z}$ gelten die aus der Schule bekannten Rechenregeln:

$$x^p x^q = x^{p+q},\ (x^p)^q = x^{pq},\ x^{-p} = \frac{1}{x^p}\,. \tag{2.5}$$

Den Beweis für diese Rechenregeln führt man mittels vollständige Induktion für $p, q \in \mathbb{N}$, und dann durch Fallunterscheidung für den allgemeinen Fall $p, q \in \mathbb{Z}$.

2.4.10 Lemma. *Ist $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper, so gilt für $n \in \mathbb{N}$ und $x, y \geq 0$, dass $x < y$ genau dann, wenn $x^n < y^n$. Für $x, y > 0$ ist $x < y$ auch zu $x^{-n} > y^{-n}$ äquivalent.*

Beweis. Zunächst zeigt man leicht durch vollständige Induktion und mit Hilfe von $(p3)$, dass aus $0 < t$ immer $0 < t^n$ folgt. Ist $x < y$, so folgt im Falle $x = 0$ daher $x^n = 0 < y^n$. Ist $0 < x < y$, so zeigt man $x^n < y^n$ durch vollständige Induktion:

Für $n = 1$ ist $x^n < y^n$ offensichtlich. Gilt $x^n < y^n$, so folgt aus Lemma 2.2.3 und der rekursiven Definition von x^n (siehe Beispiel 2.3.4)

$$x^{n+1} = x^n \cdot x < y^n \cdot x < y^n \cdot y = y^{n+1} .$$

Ist umgekehrt $x^n < y^n$, so muss $x < y$, da sonst $y \leq x$, und aus dem eben bewiesenem $y^n \leq x^n$ folgte.
Die letzte Behauptung folgt sofort aus $x < y \Leftrightarrow x^{-1} > y^{-1}$ für alle $x, y > 0$. ❑

Also ist $x \mapsto x^n$ eine *streng monoton wachsende Funktion* und somit injektive Funktion von $P \cup \{0\}$ nach $P \cup \{0\}$. Wir werden später sehen, dass diese Funktionen in vollständig angeordneten Körpern auch surjektiv sind. Für $p \in \mathbb{Z}, p < 0$ ist $x \mapsto x^p$ eine *streng monoton fallende Funktion* und somit eine injektive Funktion von P nach P.

2.5 Eine alternative Konstruktion von $\mathbb{Z}^*$

Wir wollen in diesem Abschnitt einen alternativen Zugang zu den ganzen Zahlen vorstellen. Der Vorteil dieser vordergründig aufwendigeren Methode ist, dass die Beweise der Rechengesetze struktureller und kürzer sind.

2.5.1 Definition. Sei $\sim \subseteq (\mathbb{N} \times \mathbb{N})^2$ die Relation

$$(x, n) \sim (y, m) \ :\Leftrightarrow \ x + m = y + n .$$

2.5.2 Lemma. *Die Relation $\sim$ ist eine Äquivalenzrelation.*

Beweis. Die Reflexivität und Symmetrie ist klar. Um zu zeigen, dass $\sim$ transitiv ist, seien $(x, n) \sim (y, m)$ und $(y, m) \sim (z, k)$ gegeben. Dann gilt $x + m = y + n$ und $y + k = z + m$. Es folgt

$$(x + k) + m = (x + m) + k = (y + n) + k = (y + k) + n = (z + m) + n = (z + n) + m ,$$

und wegen der Kürzungsregel in $\mathbb{N}$ daher $x + k = z + n$; also $(x, n) \sim (z, k)$. ❑

2.5.3 Definition. Wir bezeichnen mit $\mathbb{Z}$ die Faktormenge $\mathbb{N} \times \mathbb{N}/_\sim$.

Auf $\mathbb{Z}$ definieren wir algebraische Operationen $+$ und $\cdot$. Die Vorgangsweise dazu ist, zunächst Addition und Multiplikation auf $\mathbb{N} \times \mathbb{N}$ zu definieren, und diese dann auf $\mathbb{Z}$ zu übertragen.

$$+ : \begin{cases} (\mathbb{N} \times \mathbb{N})^2 & \to & \mathbb{N} \times \mathbb{N} , \\ ((x, n), (y, m)) & \mapsto & (x + y, n + m) , \end{cases}$$

$$\cdot : \begin{cases} (\mathbb{N} \times \mathbb{N})^2 & \to & \mathbb{N} \times \mathbb{N} , \\ ((x, n), (y, m)) & \mapsto & (xy + nm, xm + ny) . \end{cases}$$

2.5.4 Lemma. *Die Operationen $+$ und $\cdot$ auf $\mathbb{N} \times \mathbb{N}$ sind kommutativ, assoziativ und es gilt das Distributivgesetz.*

Beweis. Seien $(x,n),(y,m) \in \mathbb{N}\times\mathbb{N}$. Dann ist

$$(x,n)+(y,m) = (x+y,n+m) = (y+x,m+n) = (y,m)+(x,n)\,,$$

$$(x,n)\cdot(y,m) = (xy+nm,xm+ny) = (yx+mn,yn+mx) = (y,m)\cdot(x,n)\,.$$

Sei zusätzlich $(z,k)\in\mathbb{N}\times\mathbb{N}$. Dann gilt

$$\begin{aligned}\big((x,n)+(y,m)\big)+(z,k) &= (x+y,n+m)+(z,k) = \big((x+y)+z,(n+m)+k\big)\\ &= \big(x+(y+z),n+(m+k)\big) = (x,n)+\big((y,m)+(z,k)\big)\,.\end{aligned}$$

Die Gültigkeit der Assoziativität der Multiplikation sowie des Distributivgesetzes rechnet man ähnlich, aber deutlich mühsamer, nach. ❑

Um diese Operationen auf $\mathbb{Z}$ übertragen zu können, benötigen wir die Verträglichkeit mit der Relation $\sim$.

2.5.5 Lemma. *Gilt* $(x,n)\sim(\hat{x},\hat{n})$ *und* $(y,m)\sim(\hat{y},\hat{m})$*, so auch*

$$(x,n)+(y,m)\sim(\hat{x},\hat{n})+(\hat{y},\hat{m}),\ (x,n)\cdot(y,m)\sim(\hat{x},\hat{n})\cdot(\hat{y},\hat{m})\,.$$

Beweis. Seien $(x,n)\sim(\hat{x},\hat{n})$ und $(y,m)\sim(\hat{y},\hat{m})$ gegeben. Dann gilt

$$(x+y)+(\hat{n}+\hat{m}) = (x+\hat{n})+(y+\hat{m}) = (\hat{x}+n)+(\hat{y}+m) = (\hat{x}+\hat{y})+(n+m)\,,$$

und wir sehen, dass $(x,n)+(y,m)\sim(\hat{x},\hat{n})+(\hat{y},\hat{m})$.
Um die Aussage für $\cdot$ zu zeigen, betrachten wir zuerst $(x,n)\sim(\hat{x},\hat{n})$ und ein (y,m). Dann gilt

$$\begin{aligned}(xy+nm)+(\hat{x}m+\hat{n}y) &= (x+\hat{n})y+(\hat{x}+n)m\\ &= (\hat{x}+n)y+(x+\hat{n})m = (\hat{x}y+\hat{n}m)+(xm+ny)\,,\end{aligned}$$

und wir erhalten $(x,n)\cdot(y,m)\sim(\hat{x},\hat{n})\cdot(y,m)$. Wegen der Kommutativität von $\cdot$ folgt auch, dass für (x,n) und $(y,m)\sim(\hat{y},\hat{m})$ stets $(x,n)\cdot(y,m)\sim(x,n)\cdot(\hat{y},\hat{m})$ gilt. Die Aussage für $\cdot$ folgt nun aus der Transitivität von $\sim$ angewandt auf

$$(x,n)\cdot(y,m)\sim(\hat{x},\hat{n})\cdot(y,m)\sim(\hat{x},\hat{n})\cdot(\hat{y},\hat{m})\,.$$ ❑

2.5.6 Definition. Auf $\mathbb{Z}$ seien zwei algebraische Operationen $+$ und $\cdot$ definiert, indem wir für $a,b\in\mathbb{Z}$ Paare $(x,n),(y,m)\in\mathbb{N}\times\mathbb{N}$ so wählen, dass $[(x,n)]_\sim = a$ und $[(y,m)]_\sim = b$, und dann

$$a+b := \big[(x,n)+(y,m)\big]_\sim,\quad a\cdot b := \big[(x,n)\cdot(y,m)\big]_\sim$$

setzen.

Dass die Funktionen $+$ und $\cdot$ tatsächlich wohldefiniert sind, verdanken wir gerade der Verträglichkeitsaussage in Lemma 2.5.5.
Im nächsten Schritt definieren wir die Relation $\le$ auf $\mathbb{Z}$. Dazu sei

$$(x,n)\le(y,m) \ :\Leftrightarrow\ x+m\le y+n,\quad (x,n),(y,m)\in\mathbb{N}\times\mathbb{N}\,.$$

2.5.7 Lemma. *Die Relation $\leq$ auf $\mathbb{N}\times\mathbb{N}$ ist reflexiv, transitiv und total, also $(x,n)\leq(y,m)$ oder $(y,m)\leq(x,n)$ für alle $(x,n),(y,m)\in\mathbb{N}\times\mathbb{N}$. Zudem gilt*

$$(x,n)\leq(y,m) \text{ und } (y,m)\leq(x,n) \iff (x,n)\sim(y,m). \tag{2.6}$$

Außerdem folgt aus $(x,n)\sim(\hat{x},\hat{n})$ und $(y,m)\sim(\hat{y},\hat{m})$, dass

$$(x,n)\leq(y,m) \iff (\hat{x},\hat{n})\leq(\hat{y},\hat{m})\,.$$

Beweis. Die Reflexivität folgt unmittelbar aus der Definition. Sei $(x,n)\leq(y,m)$ und $(y,m)\leq(z,k)$. Dann gilt $x+m\leq y+n$ und $y+k\leq z+m$, und wir erhalten

$$(x+k)+m=(x+m)+k\leq(y+n)+k=(y+k)+n\leq(z+m)+n=(z+n)+m\,.$$

Daraus folgt nun $x+k\leq z+n$, also $(x,n)\leq(z,k)$. Die Totalität folgt aus der Tatsache, dass $\leq$ eine Totalordnung auf $\mathbb{N}$ ist. Da $(x,n)\leq(y,m)$ und $(y,m)\leq(x,n)$ mit $x+m=y+n$ gleichbedeutend ist, folgt (2.6). Die letzte Aussage folgt unmittelbar aus (2.6) und der Transitivität von $\leq$ auf $\mathbb{N}\times\mathbb{N}$. ❑

Wegen der letzte Aussage von Lemma 2.5.7, ist folgende Definition unabhängig von den Repräsentanten der Restklassen a bzw. b. Wir erhalten damit eine Totalordnung auf $\mathbb{Z}$.

2.5.8 Definition. Seien $a,b\in\mathbb{Z}$, $a=[(x,n)]_\sim, b=[(y,m)]_\sim$. Dann schreiben wir $a\leq b$, falls $(x,n)\leq(y,m)$.

2.5.9 Satz. *Die Addition und Multiplikation auf $\mathbb{Z}$ sind kommutativ, assoziativ und es gilt das Distributivgesetz. Das Element $0:=[(1,1)]_\sim$ bzw. $1:=[(2,1)]_\sim$ ist neutrales Element bezüglich $+$ bzw. $\cdot$. Jedes Element besitzt ein additiv Inverses Element. Für $\cdot$ gilt die Kürzungsregel: Ist $a,b,c\in\mathbb{Z}$, $c\neq 0$, und gilt $a\cdot c=b\cdot c$, so folgt $a=b$.*
Die Relation $\leq$ ist eine Totalordnung. Für alle $a,b,c\in\mathbb{Z}$ mit $a\leq b$ gilt $a+c\leq b+c$ und, falls $c\geq 0$, auch $a\cdot c\leq b\cdot c$. Umgekehrt folgt aus $c>0$ und $a\cdot c\leq b\cdot c$, dass $a\leq b$.
Die natürlichen Zahlen $\mathbb{N}$ sind in $\mathbb{Z}$ injektiv eingebettet vermöge der Abbildung

$$\phi:\begin{cases}\mathbb{N} & \to & \mathbb{Z}\,,\\ x & \mapsto & [(x+1,1)]_\sim\,.\end{cases}$$

Diese Einbettung erhält Addition, Multiplikation und Ordnung.

Beweis. Die Gültigkeit von Assoziativität, Kommutativität sowie Distributivität folgt wegen Lemma 2.5.4. Für $a=[(x,n)]_\sim\in\mathbb{Z}$ gilt

$$a+0=[(x,n)]_\sim+[(1,1)]_\sim=[(x+1,n+1)]_\sim=[(x,n)]_\sim=a\,,$$

sowie

$$a\cdot 1=[(x,n)]_\sim\cdot[(2,1)]_\sim=[(2x+n,x+2n)]_\sim=[(x,n)]_\sim=a\,,$$

also ist 0 neutrales Element der Addition und 1 neutrales Element der Multiplikation. Setze $\hat{a}:=[(n,x)]_\sim$, dann gilt

$$a+\hat{a}=[(x,n)]_\sim+[(n,x)]_\sim=[(x+n,n+x)]_\sim=[(1,1)]_\sim=0\,,$$

also hat a ein additives Inverses, nämlich $\hat{a}$.
Wegen Lemma 2.5.7 ist $\leq$ auf $\mathbb{Z}$ eine Totalordnung. Seien $a, b, c \in \mathbb{Z}$, $a = [(x,n)]_\sim, b = [(y,m)]_\sim, c = [(z,k)]_\sim$. Dann gilt

$$\begin{aligned} a + c \leq b + c &\Leftrightarrow (x+z, n+k) \leq (y+z, m+k) \Leftrightarrow x+z+m+k \leq y+z+n+k \\ &\Leftrightarrow x+m \leq y+n \Leftrightarrow a \leq b\,. \end{aligned}$$

Sei nun angenommen, dass $a < b$ und $c \geq 0$, also $x+m < y+n$ und $z \geq k$. Dann gibt es $t \in \mathbb{N}$ mit $y+n = (x+m)+t$. Wegen $z \geq k$ folgt $tz \geq tk$ und daher auch $(y+n)z = (x+m)z + tz \geq (x+m)z + tk$ und schließlich

$$(x+m)k + (y+n)z \geq (x+m)z + tk + (x+m)k = (x+m)z + (y+n)k\,.$$

Also haben wir $(xk+nz)+(yz+mk) \geq (xz+nk)+(yk+mz)$, und das heißt gerade $a \cdot c \leq b \cdot c$.
Sei umgekehrt $a \cdot c \leq b \cdot c$ und $c > 0$, was gemäß obiger Rechnung $(x+m)k + (y+n)z \geq (x+m)z + (y+n)k$ und $z > k$ bedeutet. Angenommen es wäre $a > b$, also $x+m > y+n$. Dann gibt es $t \in \mathbb{N}$ mit $(y+n)+t = x+m$. Damit erhalten wir

$$tk + (y+n)(k+z) \geq tz + (y+n)(z+k)$$

und daraus $tk \geq tz$ und schließlich den Widerspruch $k \geq z$. Also muss $a \leq b$ gelten. Die Kürzungsregel für $\cdot$ folgt aus der gerade bewiesenen Kürzungsregel für $\leq$.
Die Injektivität der Abbildung ϕ gilt, da $(x+1,1) \sim (y+1,1)$ gerade $x+2 = y+2$ bedeutet, und damit $x = y$ folgt. Außerdem gilt

$$\phi(x) + \phi(y) = [((x+1)+(y+1), 1+1)]_\sim = [((x+y)+1, 1)]_\sim = \phi(x+y)\,,$$

$$\begin{aligned} \phi(x) \cdot \phi(y) &= \big[((x+1)(y+1)+1, (x+1)+(y+1))\big]_\sim \\ &= \big[(xy+x+y+1+1, x+y+1+1)\big]_\sim = [(xy+1,1)]_\sim = \phi(xy)\,, \end{aligned}$$

$$\phi(x) \leq \phi(y) \Leftrightarrow (x+1)+1 \leq (y+1)+1 \Leftrightarrow x \leq y\,.$$

Wegen der Injektivität gilt damit auch $\phi(x) < \phi(y) \Leftrightarrow x < y$. ❑

Folgendes Resultat liefert insbesondere, dass die hier konstruierten ganzen Zahlen eine Kopie der eingangs konstruierten ganzen Zahlen sind.

2.5.10 Proposition. *Versteht man die natürlichen Zahlen via ϕ eingebettet in $\mathbb{Z}$ wie in Satz 2.5.9, so gilt*[9]

$$\mathbb{Z} = -\mathbb{N} \dot\cup \{0\} \dot\cup \mathbb{N}\,,$$

wobei

$$p \in \mathbb{N} \Leftrightarrow p > 0 \quad \textit{und} \quad p \in -\mathbb{N} \Leftrightarrow p < 0\,.$$

[9] Der Punkt bedeutet wieder die Vereinigung paarweise disjunkter Mengen.

Definieren wir $\operatorname{sgn}(x) = 0$*, wenn* $x = 0$*,* $\operatorname{sgn}(x) = 1$*, wenn* $x \in \mathbb{N}$*, und* $\operatorname{sgn}(x) = -1$*, wenn* $x \in -\mathbb{N}$*, und setzen* $|p| = \operatorname{sgn}(p)p$*, so gilt für* $p, q \in \mathbb{Z}$

$$p + q = \begin{cases} p + q\,, & \text{falls } p, q \in \mathbb{N}\,, \\ -(|p| + |q|)\,, & \text{falls } -p, -q \in \mathbb{N}\,, \\ p - |q|\,, & \text{falls } p, -q \in \mathbb{N},\ p > -q\,, \\ -(|q| - p)\,, & \text{falls } p, -q \in \mathbb{N},\ p < -q\,, \\ -(|p| - q)\,, & \text{falls } -p, q \in \mathbb{N},\ -p > q\,, \\ q - |p|\,, & \text{falls } -p, q \in \mathbb{N},\ -p < q\,, \\ 0\,, & \text{falls } q = -p\,, \\ p\,, & \text{falls } q = 0\,, \\ q\,, & \text{falls } p = 0\,, \end{cases}$$

und

$$p \cdot q = \begin{cases} |p| \cdot |q|\,, & \text{falls } q, p \neq 0,\ \operatorname{sgn}(q) = \operatorname{sgn}(p)\,, \\ -(|p| \cdot |q|)\,, & \text{falls } q, p \neq 0,\ \operatorname{sgn}(q) = -\operatorname{sgn}(p)\,, \\ 0\,, & \text{falls } q = 0 \text{ oder } p = 0\,, \end{cases}$$

sowie

$$p < q \Leftrightarrow q - p \in \mathbb{N} \quad \text{und} \quad p \leq q \Leftrightarrow (p = q \vee p < q)\,.$$

Beweis. Ist $[(x, n)]_\sim \in \mathbb{Z},\ [(x, n)]_\sim > 0 = [(1, 1)]_\sim$, so gilt $x + 1 > n + 1$. Damit ist $x - n \in \mathbb{N}$, und wegen $(x - n + 1, 1) \sim (x, n)$ folgt $\phi(x - n) = [(x, n)]_\sim$. Umgekehrt ist für $y \in \mathbb{N}$ $\phi(y) = [(y + 1, 1)]_\sim > [(1, 1)]_\sim = 0$.
Ist $[(x, n)]_\sim \in \mathbb{Z},\ [(x, n)]_\sim < 0 = [(1, 1)]_\sim$, so folgt aus den Rechenregeln von Satz 2.5.9 $0 > -[(x, n)]_\sim = [(n, x)]_\sim$. Aus dem schon Bewiesenen folgt $-[(x, n)]_\sim = -\phi(n - x)$, wobei $n - x \in \mathbb{N}$. Umgekehrt ist für $y \in \mathbb{N}$ $-\phi(y) = [(1, y + 1)]_\sim < [(1, 1)]_\sim = 0$. Also kann man $\mathbb{N}$ mit $\{p \in \mathbb{Z} : p > 0\}$ und $-\mathbb{N}$ mit $\{p \in \mathbb{Z} : p < 0\}$ identifizieren.

$$\mathbb{Z} = -\mathbb{N} \dot\cup \{0\} \dot\cup \mathbb{N}$$

folgt nun aus der Tatsache, dass $\leq$ eine Totalordnung ist.
Die restlichen Aussagen folgen aus der Definition von $|.|$, $\operatorname{sgn}(.)$ und der Tatsache, dass $p < q \Leftrightarrow 0 < q - p$, siehe Satz 2.5.9. ❑

2.6 Dividieren mit Rest*

Ausgerüstet mit unserem Grundwissen über die natürlichen und die ganzen Zahlen können wir nun das aus der Schule bekannte *Dividieren mit Rest* mathematisch rechtfertigen.

2.6.1 Satz. *Sind* $m \in \mathbb{N},\ n \in \mathbb{Z}$*, so gibt es eindeutige Zahlen* $l \in \mathbb{Z}$ *und* $r \in \{0, \ldots, m - 1\}$[10]*, sodass* $n = ml + r$*. Dabei ist* $n \geq 0$ *genau dann, wenn* $l \geq 0$*.*

[10] $\{0, \ldots, m - 1\}$ steht für $\{k \in \mathbb{N} \cup \{0\} : 0 \leq k < m\}$.

Beweis. Sei zunächst $n \in \mathbb{N} \cup \{0\}$ beliebig. Da die Menge aller $l \in \mathbb{N} \cup \{0\}$ mit $m \cdot l + m > n$ nicht leer ist – n ist sicher in dieser Menge, hat sie ein Minimum; Variante von Satz 2.3.12. Ist $l = 0$, so muss $n \in \{0, \dots, m-1\}$, und ist $l > 0$, so folgt wegen der Minimalität $ml = m(l-1) + m \leq n < ml + m$. Also muss immer $n = ml + r$ für ein $l \in \mathbb{N} \cup \{0\}$ und ein $r \in \{0, \dots, m-1\}$ gelten.
Falls auch $n = m\hat{l} + \hat{r}$ für $\hat{l} \in \mathbb{N} \cup \{0\}$ und $\hat{r} \in \{0, \dots, m-1\}$, so folgt $m\hat{l} + m > n$ und wegen der Minimalitätseigenschaft von l auch $\hat{l} \geq l$. Andererseits gilt $m\hat{l} \leq n$, weshalb nicht $\hat{l} > l$ sein kann, da sonst $n \geq m\hat{l} = ml + m(\hat{l} - l) \geq ml + m$. Somit gibt es eindeutige $l \in \mathbb{N} \cup \{0\}$ und $r \in \{0, \dots, m-1\}$, sodass $n = ml + r$.
Für $n < 0$ ist $-n - 1 \geq 0$. Somit gibt es eindeutige $s \in \mathbb{N} \cup \{0\},\ t \in \{0, \dots, m-1\}$, sodass $-n - 1 = sm + t = (s+1)m + (t-m)$, und daher sodass $-n = (s+1)m + (t - m + 1)$, bzw. $n = -(s+1)m + (-t + m - 1)$. Setzen wir $l = -(s+1)$ und $r = -t + m - 1$, so sehen wir, dass $n = ml + r$ für ein eindeutiges $l < 0$ und ein eindeutiges $r \in \{0, \dots, m-1\}$. ❑

2.6.2 Bemerkung. Die geraden (ungeraden) Zahlen sind genau die ganzen Zahlen der Form $2k$ ($2k+1$) für ein $k \in \mathbb{Z}$. Aus Satz 2.6.1 folgt insbesondere, dass jede gegebene ganze Zahl gerade oder ungerade ist, wobei aus der Eindeutigkeitsaussage in Satz 2.6.1 folgt, dass sie nicht gleichzeitig gerade und ungerade sein kann; also $\mathbb{Z} = 2\mathbb{Z} \dot\cup (2\mathbb{Z} + 1)$. Entsprechendes gilt, wenn man 2 durch eine andere natürliche Zahl m ersetzt:

$$\mathbb{Z} = m\mathbb{Z} \dot\cup (m\mathbb{Z} + 1) \dot\cup \dots \dot\cup (m\mathbb{Z} + m - 1)\,.$$

2.6.3 Definition. Eine Zahl $q \in \mathbb{N}$ *teilt* eine Zahl $p \in \mathbb{N}$, falls es ein $m \in \mathbb{N}$ gibt, sodass $mq = p$, wofür wir $q|p$ schreiben. In dem Fall setzen wir $p : q := m$[11]. Teilt q die Zahl p nicht, so schreiben wir $q \nmid p$.
Eine Zahl $p \in \mathbb{N} \setminus \{1\}$ heißt *Primzahl*, wenn p nur von 1 und p geteilt wird. Die Menge aller Primzahlen sei $\mathbb{P}$.

2.6.4 Fakta.

1. Falls $q|p$, so folgt aus $mq = p$ und $1 \leq m$, dass $q \leq p$, wobei $q = p$ genau dann, wenn $m = 1$.

2. Um zu sehen, ob eine Zahl p eine Primzahl ist, genügt es somit zu überprüfen, ob $q \nmid p$ für alle $q \in \mathbb{N},\ 1 < q < p$.

3. Man sieht sofort, dass $2, 3, 5, \dots$ Primzahlen sind.

4. Ist $n \in \mathbb{N} \setminus \{1\}$ und $M = \{r \in \mathbb{N} \setminus \{1\} : r|n\}$, so ist M nicht leer, da zumindest $n \in M$. Gilt $M = \{n\}$, so ist n definitionsgemäß eine Primzahl. Anderenfalls sei m das kleinste Element von M und k so, dass $km = n$. Nun ist m eine Primzahl, da sonst $m = pq$ mit $1 < p, q < m$, und weiter $p(qk) = n$. Es wäre $p \in M$ im Widerspruch zur Minimalität von m.

   Insbesondere wird jede Zahl in $\mathbb{N} \setminus \{1\}$ von einer Primzahl geteilt.

[11] Da wir in $\mathbb{Z}$ kürzen dürfen, ist $p : q$ eindeutig definiert.

2.6.5 Lemma. *Seien $a, b \in \mathbb{N}$ und $p \in \mathbb{P}$. Gilt $p|(ab)$, so muss $p|a$ oder $p|b$.*

Beweis. Sei $T \subseteq \mathbb{P}$ die Menge aller Primzahlen, sodass die Aussage für gewisse $a, b \in \mathbb{N}$ falsch ist. Wir bringen die Annahme $T \neq \emptyset$ auf einen Widerspruch.
Sei also $T \neq \emptyset$ und p die kleinste Zahl in T; vgl. siehe Satz 2.3.12. Somit gibt es $a, b \in \mathbb{N}$ mit $p \nmid a \wedge p \nmid b$, aber $p|(ab)$, bzw. $pn = ab$ für ein $n \in \mathbb{N}$. Daher ist die Menge

$$S = \{n \in \mathbb{N} : \exists a, b \in \mathbb{N} : p \nmid a \wedge p \nmid b \wedge pn = ab\},$$

aller solchen n nicht leer und hat somit ein Minimum s. Seien $c, d \in \mathbb{N}$, sodass $p \nmid c$, $p \nmid d$ und $ps = cd$. Aus den ersten beiden Tatsachen folgt $c, d \neq p,\ c, d \neq 1$, und daraus zusammen mit der Tatsache, dass p eine Primzahl ist, folgt $s > 1$.
Nun muss $c < p$ sein, da sonst $c - p \in \mathbb{N}$ und damit $p(s - d) = (c - p)d$, was $s - d \in \mathbb{N}$ implizieren und somit der Minimalität von s widersprechen würde. Genauso gilt $d < p$.
Daraus schließen wir wegen $ps = cd$ auf $s < p$. Gemäß Fakta 2.6.4 gibt es eine Primzahl $p' \leq s < p$, sodass $p'|s$, also $s = p's'$ für ein $s' \in \mathbb{N},\ s' < s$. Somit folgt $p'(ps') = cd$, also $p'|(cd)$. Wegen der Minimalität von p muss $p'|c$ oder $p'|d$. Ohne Beschränkung der Allgemeinheit sei $c = c'p',\ c' \in \mathbb{N}$, womit

$$p'(ps') = p'(c'd) \text{ und daraus } ps' = c'd$$

folgt, was ebenfalls der Minimalität von s widerspricht. ❑

2.6.6 Satz. *Ist $n \in \mathbb{N} \setminus \{1\}$, so gibt es eindeutige Primzahlen $p_1, \ldots, p_m \in \mathbb{P}$ und Exponenten $e_1, \ldots, e_m \in \mathbb{N}$, sodass*

$$n = p_1^{e_1} \cdot \ldots p_m^{e_m}. \tag{2.7}$$

Diese Zerlegung heißt Primfaktorzerlegung.

Beweis. Wir zeigen zuerst die Existenz einer solchen Zerlegung. Für $n = 2$ ist diese klar. Angenommen für ein $n > 2$ gibt es zu allen $k < n,\ k \geq 2$ eine solche Zerlegung. Nach Fakta 2.6.4 gibt es eine Primzahl $p \leq n$ mit $p|n$. Ist $n = p$, so haben wir unsere Zerlegung. Ist $p < n$, so folgt $n = (n : p)p$, wobei nach Voraussetzung $n : p\ (< n)$ eine solche Zerlegung hat. Somit hat auch n eine solche Zerlegung. Nach einer Variante des Prinzips der vollständigen Induktion gibt es eine Primfaktorzerlegung für alle $n \in \mathbb{N} \setminus \{1\}$.
Die Eindeutigkeit ist für $n = 2$ wieder klar, da alle Produkte der Form (2.7) einen Wert > 2 ergeben, außer für $m = 1$ und $e_1 = 1, p_1 = 2$.
Angenommen mit einem $n > 2$ ist die Primfaktorzerlegung eindeutig für alle $k < n,\ k \geq 2$, und angenommen

$$q_1^{f_1} \cdot \ldots q_l^{f_l} = n = p_1^{e_1} \cdot \ldots p_m^{e_m},$$

mit $l, m \in \mathbb{N}$ und $e_1, \ldots, e_m, f_1, \ldots, f_l \in \mathbb{N}$ sowie $p_1, \ldots, p_m, q_1, \ldots, q_l \in \mathbb{P}$. Insbesondere gilt $q_1|p_1^{e_1} \cdot \ldots p_m^{e_m}$. Nach Lemma 2.6.5 muss $q_1|p_j$ und daher $q_1 = p_j$ für ein $j \in \{1, \ldots, m\}$. Durch Umnummerierung können wir $q_1 = p_1$ annehmen. Es folgt

$$q_1^{f_1 - 1} \cdot \ldots q_l^{f_l} = n : q_1 = p_1^{e_1 - 1} \cdot \ldots p_m^{e_m}.$$

Ist $n : q_1 = 1$, so muss $n = p_1 = q_1$ und $l = 1 = m, e_1 = 1 = f_1$. Sonst folgt wegen $1 < n : q_1 < n$ aus unserer Annahme, dass auch $l = m$ und $e_j = f_j$ sowie $p_j = q_j$, $j = 1, \ldots, l$. ❑

2.7 Der Körper $\mathbb{Q}$

Oben haben wir $\langle \mathbb{Z}, +, \cdot \rangle$ konstruiert. Diesen werden wir nun zu einem angeordneten Körper, dem Körper der rationalen Zahlen erweitern, und damit sehen, dass es zumindest einen angeordneten Körper gibt.
Der Grundgedanke der folgenden Konstruktion entspringt der Tatsache, dass in einem Körper $\frac{p_1}{q_1} = \frac{p_2}{q_2}$ genau dann gilt, wenn $p_1 q_2 = p_2 q_1$.

2.7.1 Definition. Sei $\sim \subseteq (\mathbb{Z} \times \mathbb{N})^2$ die Relation

$$(x, n) \sim (y, m) \;:\Leftrightarrow\; xm = yn\,.$$

2.7.2 Lemma. *Die Relation $\sim$ ist eine Äquivalenzrelation.*

Beweis. Die Reflexivität und Symmetrie sind offensichtlich. Sei nun $(x, n) \sim (y, m)$ und $(y, m) \sim (z, k)$. Es gilt also $xm = yn$ und $yk = zm$. Wir erhalten

$$(xk)m = (xm)k = (yn)k = (yk)n = (zm)n = (zn)m\,,$$

und da in $\langle \mathbb{Z}, +, \cdot \rangle$ die Kürzungsregel (siehe Bemerkung 2.4.5) gilt, folgt daraus $xk = zn$, also $(x, n) \sim (z, k)$. ❑

2.7.3 Definition. Wir bezeichnen mit $\mathbb{Q}$ die Menge $\mathbb{Z} \times \mathbb{N}/_\sim$ aller Äquivalenzklassen. $\mathbb{Q}$ heißt der Körper der *rationalen Zahlen*.

Wir wollen $\mathbb{Q}$ mit den algebraischen Operationen $+$ und $\cdot$ versehen. Dazu definieren wir zunächst Addition und Multiplikation auf $\mathbb{Z} \times \mathbb{N}$, und übertragen diese dann durch Faktorisieren auf $\mathbb{Q}$:

$$+ : \begin{cases} (\mathbb{Z} \times \mathbb{N})^2 & \to & \mathbb{Z} \times \mathbb{N}\,, \\ ((x, n), (y, m)) & \mapsto & (xm + yn, nm)\,, \end{cases}$$

$$\cdot : \begin{cases} (\mathbb{Z} \times \mathbb{N})^2 & \to & \mathbb{Z} \times \mathbb{N}\,, \\ ((x, n), (y, m)) & \mapsto & (xy, nm)\,. \end{cases}$$

Die Motivation für unsere Definition ergibt sich aus den Regeln der Bruchrechnung.

$$\frac{x}{n} + \frac{y}{m} = \frac{xm}{nm} + \frac{yn}{mn} = \frac{xm + yn}{nm}, \quad \frac{x}{n} \cdot \frac{y}{m} = \frac{xy}{nm}\,.$$

2.7.4 Lemma. *Für die Verknüpfungen $+, \cdot$ gilt das Kommutativ- und das Assoziativgesetz.*

Beweis. Die Gesetze gelten, da man sie leicht auf die Gültigkeit dieser Gesetze auf $\mathbb{Z}$ zurückführt. Zum Beispiel gilt das Assoziativgesetz wegen

$$\begin{aligned}((x, n) + (y, m)) + (z, k) &= (xm + yn, nm) + (z, k) = ((xm + yn)k + z(nm), (nm)k) \\ &= (x(mk) + (yk + zm)n, n(mk)) = (x, n) + ((y, m) + (z, k))\,.\end{aligned}$$

❑

Um $\mathbb{Q}$ anordnen zu können, definieren wir noch

$$\operatorname{sgn} : \begin{cases} (\mathbb{Z}\times\mathbb{N}) & \to & \mathbb{Z}\,, \\ (x,n) & \mapsto & \operatorname{sgn}(x)\,. \end{cases}$$

2.7.5 Lemma. *Sind* $(x,n) \sim (\hat{x},\hat{n})$ *und* $(y,m) \sim (\hat{y},\hat{m})$*, so folgt* $\operatorname{sgn}((x,n)) = \operatorname{sgn}((\hat{x},\hat{n}))$ *und*

$$(x,n)+(y,m) \sim (\hat{x},\hat{n})+(\hat{y},\hat{m}),\quad (x,n)\cdot(y,m) \sim (\hat{x},\hat{n})\cdot(\hat{y},\hat{m})\,.$$

Beweis. Seien $(x,n) \sim (\hat{x},\hat{n})$ und (y,m) gegeben. Zunächst folgt aus $x\hat{n} = \hat{x}n$ und $n,\hat{n} \in \mathbb{N}$, dass $\operatorname{sgn}((x,n)) = \operatorname{sgn}(x) = \operatorname{sgn}(\hat{x}) = \operatorname{sgn}((\hat{x},\hat{n}))$. Weiters gilt

$$\begin{aligned}(xm+yn)\hat{n}m &= xm\hat{n}m + yn\hat{n}m \\ &= \underbrace{(x\hat{n}-\hat{x}n)}_{=0}mm + \hat{x}nmm + yn\hat{n}m = (\hat{x}m+y\hat{n})nm\,,\end{aligned}$$

also $(x,n)+(y,m) \sim (\hat{x},\hat{n})+(y,m)$. Wegen der Kommutativität folgt daraus mit vertauschter Notation, dass für $(\hat{x},\hat{n})$ und $(y,m) \sim (\hat{y},\hat{m})$ stets auch $(\hat{x},\hat{n})+(y,m) \sim (\hat{x},\hat{n})+(\hat{y},\hat{m})$. Wegen der Transitivität folgt

$$(x,n)+(y,m) \sim (\hat{x},\hat{n})+(\hat{y},\hat{m})\,.$$

Bei der Multiplikation geht man analog vor. Seien $(x,n) \sim (\hat{x},\hat{n})$ und (y,m) gegeben. Dann gilt

$$xy\hat{n}m = \underbrace{(x\hat{n}-\hat{x}n)}_{=0}ym + \hat{x}nym = \hat{x}ynm\,,$$

also $(x,n)\cdot(y,m) \sim (\hat{x},\hat{n})\cdot(y,m)$. Wegen der Kommutativität folgt daraus mit vertauschter Notation, dass für $(\hat{x},\hat{n})$ und $(y,m) \sim (\hat{y},\hat{m})$ stets auch $(\hat{x},\hat{n})\cdot(y,m) \sim (\hat{x},\hat{n})\cdot(\hat{y},\hat{m})$. Wegen der Transitivität folgt schließlich

$$(x,n)\cdot(y,m) \sim (\hat{x},\hat{n})\cdot(\hat{y},\hat{m})\,. \qquad \text{❑}$$

2.7.6 Definition. Auf $\mathbb{Q}$ seien zwei algebraische Operationen $+$ und $\cdot$ dadurch definiert, dass wir für $a,b \in \mathbb{Q}$ Paare $(x,n),(y,m) \in \mathbb{Z}\times\mathbb{N}$ mit $[(x,n)]_\sim = a$ und $[(y,m)]_\sim = b$ wählen, und $\operatorname{sgn}(a) := \operatorname{sgn}((x,n))$ sowie

$$a+b := \big[(x,n)+(y,m)\big]_\sim\,,\quad a\cdot b := \big[(x,n)\cdot(y,m)\big]_\sim$$

setzen.

Wegen Lemma 2.7.5 hängen $\operatorname{sgn}(a)$, $a+b$ und $a\cdot b$ nicht von den gewählten Repräsentanten (x,n) bzw. (y,m) ab.

2.7.7 Satz. *Setzt man* $P = \{a \in \mathbb{Q} : \operatorname{sgn}(a) = 1\}$*, so ist* $\langle \mathbb{Q},+,\cdot,P\rangle$ *ist ein angeordneter Körper.*

- *Dabei ist* $[(0,1)]_\sim$ *das neutrale Element bzgl.* $+$*,*

- $[(1,1)]_\sim$ *das neutrale Element bezüglich* $\cdot$.
- *Zu* $[(x,n)]_\sim \in \mathbb{Q}$ *ist* $[(-x,n)]_\sim$ *das additiv Inverse, und*
- *zu* $[(x,n)]_\sim \in \mathbb{Q} \setminus \{0\}$ *ist* $[(\operatorname{sgn}(x)n, |x|)]_\sim$ *das multiplikativ Inverse.*
- *Außerdem gilt*
$$[(x,n)]_\sim \leq [(y,m)]_\sim \Leftrightarrow xm \leq ny\,. \tag{2.8}$$
- *Die ganzen Zahlen* $\mathbb{Z}$ *sind in* $\mathbb{Q}$ *eingebettet durch*
$$\phi : \begin{cases} \mathbb{Z} & \to & \mathbb{Q}\,, \\ x & \mapsto & [(x,1)]_\sim\,. \end{cases}$$
Diese Einbettung erhält Addition, Multiplikation und Ordnung.
- *Schließlich hat* $\mathbb{Q}$ *die Eigenschaft, dass die Teilmenge* $\phi(\mathbb{N})$ *von* $\mathbb{Q}$ *keine obere Schranke hat.*

Beweis. Die Gültigkeit der Rechenregeln wie Kommutativität und Assoziativität ergibt sich aus den entsprechenden Regeln für + und $\cdot$ auf $\mathbb{Z} \times \mathbb{N}$. Das Distributivgesetz gilt, da für $[(x,n)]_\sim, [(y,m)]_\sim, [(z,k)]_\sim \in \mathbb{Q}$

$$\begin{aligned}([(x,n)]_\sim + [(y,m)]_\sim) \cdot [(z,k)]_\sim &= [(xm+yn, mn)]_\sim \cdot [(z,k)]_\sim = [((xm+yn)z, kmn)]_\sim \\ &= [(xzkm + yzkn, (km)(kn))]_\sim \\ &= [(x,n)]_\sim \cdot [(z,k)]_\sim + [(y,m)]_\sim \cdot [(z,k)]_\sim\,.\end{aligned}$$

Für $a = [(x,n)]_\sim \in \mathbb{Q}$ gilt

$$a + [(0,1)]_\sim = [(x+0, n\cdot 1)]_\sim = a,\ a \cdot [(1,1)]_\sim = [(x\cdot 1, n\cdot 1)]_\sim = a\,.$$

Weiters hat man für $b := [(-x,n)]_\sim$

$$a + b = [(xn - xn, nn)]_\sim = [(0,nn)]_\sim = [(0,1)]_\sim = 0\,.$$

Sei nun $a \neq 0$, also $(x,n) \not\sim (0,1)$ oder äquivalent $x \neq 0$. Mit $c := [(\operatorname{sgn}(x)n, |x|)]_\sim$ folgt $ac = [(\operatorname{sgn}(x)xn, n|x|)]_\sim = [(1,1)]_\sim$.
Wegen $\operatorname{sgn}([(-x,n)]_\sim) = \operatorname{sgn}(-x) = -\operatorname{sgn}([(x,n)]_\sim)$ und, weil $\operatorname{sgn}([(x,n)]_\sim) = 0$ genau dann, wenn $[(x,n)]_\sim = [(0,1)]_\sim$, gilt für jedes $a \in \mathbb{Q}$

$$\begin{aligned} a \in P &\Leftrightarrow \operatorname{sgn}(a) = 1\,, \\ a \in \{0\} &\Leftrightarrow \operatorname{sgn}(a) = 0\,, \\ a \in -P &\Leftrightarrow \operatorname{sgn}(a) = -1\,, \end{aligned}$$

womit $\mathbb{Q} = P \dot\cup \{0\} \dot\cup -P$.

Aus $\operatorname{sgn}([(x,n)]_\sim + [(y,m)]_\sim) = \operatorname{sgn}(xm+yn)$ und $\operatorname{sgn}([(x,n)]_\sim \cdot [(y,m)]_\sim) = \operatorname{sgn}(xy)$ erhalten wir, dass $a, b \in P$ die Tatsache $a + b, a \cdot b \in P$ nach sich zieht. Somit ist $\langle \mathbb{Q}, +, \cdot, P\rangle$ ein angeordneter Körper, und wir haben damit eine Totalordnung $\leq$ auf $\mathbb{Q}$. (2.8) folgt aus

$$[(y,m)]_\sim - [(x,n)]_\sim = [(yn - xm, mn)]_\sim \in \{0\} \cup P \Leftrightarrow \operatorname{sgn}(yn - xm) \geq 0 \Leftrightarrow xm \leq yn\,.$$

Betrachte nun die Abbildung $\phi : \mathbb{Z} \to \mathbb{Q}$. Diese ist injektiv, denn $(x,1) \sim (y,1)$ gilt genau dann, wenn $x = y$. Dass ϕ die algebraischen Operationen erhält, rechnet man leicht nach. Die Verträglichkeit mit der Ordnung gilt, da wegen (2.8)

$$x \leq y \Leftrightarrow x \cdot 1 \leq y \cdot 1 \Leftrightarrow [(x,1)]_\sim \leq [(y,1)]_\sim \Leftrightarrow \phi(x) \leq \phi(y)\,.$$

Wegen der Injektivität gilt damit auch $x < y$ genau dann, wenn $\phi(x) < \phi(y)$.
Angenommen $[(x,n)]_\sim$ ist eine obere Schranke von $\phi(\mathbb{N})$, also $mn \leq x$ für alle $m \in \mathbb{N}$. Das ist aber offensichtlich falsch, wenn $x \leq 1$ und man zum Beispiel $m = 2$ setzt. Ist $x > 1$, so erhält man mit $m = x^2$ den Widerspruch $x \leq xn \leq 1$. ❑

Wir werden im Folgenden für die rationale Zahl $[(x,n)]_\sim$ stets das Symbol $\frac{x}{n}$ schreiben. Dieses Symbol drückt tatsächlich die Division von x durch n aus, denn man hat

$$[(x,1)]_\sim = [(x,n)]_\sim \cdot [(n,1)]_\sim\,.$$

Wir sehen insbesondere, dass jede rationale Zahl der Quotient von zwei ganzen Zahlen ist. Nun wollen wir zeigen, dass jeder angeordnete Körper die rationalen Zahlen, und damit insbesondere auch die ganzen Zahlen, enthält.

2.7.8 Proposition. *Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Dann gibt es eine eindeutige Abbildung $\phi : \mathbb{Q} \to K$, die nicht identisch gleich 0_K ist, und welche mit der Addition und Multiplikation verträglich ist. Diese Abbildung ist dann injektiv und auch mit $-$ sowie mit den Ordnungen $<$ (und daher auch $\leq$) verträglich.*

Beweis.

⇝ Für $n \in \mathbb{N}$ und $x \in K$ haben wir im Abschnitt über die natürlichen Zahlen eine Funktion $n \mapsto nx$ von $\mathbb{N}$ nach K rekursiv durch $1x = x$ und $(n')x = nx + x$ definiert; siehe Beispiel 2.3.4. Nun nehmen wir für $x \in K$ das multiplikativ neutrale Element 1_K von K, und bezeichnen mit $\phi : \mathbb{N} \to K$ die entsprechende Funktion $n \mapsto n1_K$, welche offensichtlicherweise $\phi(1) = 1_K$ und $\phi(n+1) = \phi(n) + 1_K$ erfüllt.

Mit vollständiger Induktion nach m zeigt man leicht, dass $\phi(n+m) = \phi(n) + \phi(m)$ und $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$ für alle $n, m \in \mathbb{N}$.

Wegen $1_K \in P$ (siehe Lemma 2.2.3) sieht man ebenfalls mit vollständiger Induktion, dass $\phi(n) \in P$ für alle $n \in \mathbb{N}$. Insbesondere gilt immer $\phi(n) \neq 0_K$.

⇝ Nun setzen wir ϕ auf $\mathbb{Z}$ dadurch fort, dass wir $\phi(0) = 0_K$ und $\phi(-n) = -\phi(n)$, $n \in \mathbb{N}$ setzen. Man beweist durch Fallunterscheidungen mit der in Definition 2.4.2

angegebenen Form von + und · auf $\mathbb{Z}$ auf elementare Art und Weise, dass diese Fortsetzung die Addition und Multiplikation erhält.

Wegen ($p, q \in \mathbb{Z}$)

$$p < q \Leftrightarrow q - p \in \mathbb{N} \Leftrightarrow \phi(q-p) = \phi(q) - \phi(p) \in P \Leftrightarrow \phi(p) < \phi(q)$$

ist ϕ auch mit der Ordnung verträglich.

⇝ Da ganz $\mathbb{Q}$ von den Quotienten $\frac{x}{n}$ mit $x \in \mathbb{Z}$, $n \in \mathbb{N}$, ausgeschöpft wird, lässt sich ϕ durch die Vorschrift

$$\phi\left(\frac{x}{n}\right) := \frac{\phi(x)}{\phi(n)}$$

zu einer Abbildung von $\mathbb{Q}$ nach K fortsetzen. Man beachte hier, dass aus $\frac{x}{n} = \frac{\hat{x}}{\hat{n}}$ folgt, dass $x\hat{n} = \hat{x}n$ und daher $\phi(x)\phi(\hat{n}) = \phi(\hat{x})\phi(n)$ bzw. $\frac{\phi(x)}{\phi(n)} = \frac{\phi(\hat{x})}{\phi(\hat{n})}$. Also ist diese Abbildung wohldefiniert.

Diese Fortsetzung erhält ebenfalls die Addition und Multiplikation, denn für $\frac{x}{n}, \frac{y}{m} \in \mathbb{Q}$ gilt

$$\begin{aligned}\phi\left(\frac{x}{n} + \frac{y}{m}\right) &= \phi\left(\frac{xm+yn}{nm}\right) = \frac{\phi(xm+yn)}{\phi(nm)} \\ &= \frac{\phi(x)\phi(m) + \phi(y)\phi(n)}{\phi(n)\phi(m)} = \frac{\phi(x)}{\phi(n)} + \frac{\phi(y)}{\phi(m)} = \phi\left(\frac{x}{n}\right) + \phi\left(\frac{y}{m}\right),\end{aligned}$$

$$\begin{aligned}\phi\left(\frac{x}{n} \cdot \frac{y}{m}\right) &= \phi\left(\frac{xy}{nm}\right) = \frac{\phi(xy)}{\phi(nm)} \\ &= \frac{\phi(x)\phi(y)}{\phi(n)\phi(m)} = \frac{\phi(x)}{\phi(n)} \cdot \frac{\phi(y)}{\phi(m)} = \phi\left(\frac{x}{n}\right) \cdot \phi\left(\frac{y}{m}\right).\end{aligned}$$

Sie erhält auch die Ordnung, denn es gilt

$$\frac{x}{n} < \frac{y}{m} \Leftrightarrow xm < yn \Leftrightarrow \phi(x)\phi(m) < \phi(y)\phi(n) \Leftrightarrow \frac{\phi(x)}{\phi(n)} < \frac{\phi(y)}{\phi(m)}.$$

Es folgt insbesondere, dass ϕ injektiv ist.

⇝ Um die Eindeutigkeit von ϕ nachzuweisen, sei ψ eine weitere mit Addition und Multiplikation verträgliche Abbildung, sodass $\psi(x) \neq 0$ für zumindest ein $x \in \mathbb{Q}$. Aus $\psi(x)\psi(1) = \psi(x1) = \psi(x)$ folgt $\psi(1) = 1_K$, und aus $\psi(0)+\psi(0) = \psi(0+0) = \psi(0)$ folgt $\psi(0) = 0_K$.

Durch vollständige Induktion zeigt man, dass $\psi(n) = \phi(n)$ für $n \in \mathbb{N}$. Aus $\psi(-n) + \psi(n) = \psi(0) = 0_K = \phi(-n) + \phi(n)$ folgt $\psi(p) = \phi(p)$, $p \in \mathbb{Z}$. Schließlich folgt aus $\psi(\frac{p}{n})\psi(n) = \psi(p) = \phi(p) = \phi(\frac{p}{n})\phi(n)$, dass $\psi = \phi$. ❑

Das letzte Resultat zeigt uns, dass die rationalen Zahlen in einem gewissen Sinn der kleinste angeordnete Körper ist.
Wenn wir im Folgenden von den natürlichen (ganzen, rationalen) Zahlen als Teilmenge eines angeordneten Körpers sprechen, so wollen wir darunter die gemäß Proposition 2.7.8 existierende isomorphe Kopie $\phi(\mathbb{N}) = \{n1_k : n \in \mathbb{N}\}$, $\phi(\mathbb{Z})$, bzw. $\phi(\mathbb{Q})$ verstehen und nicht mehr z.B. zwischen n und $n \cdot 1_K$ unterscheiden.

2.7.9 Bemerkung (*)**.** Die am Beginn vom Beweis von Proposition 2.7.8 konstruierte Einbettung ϕ der natürlichen Zahlen in einen angeordneten Körper lässt sich auch auf beliebigen Körpern K durchführen.
Dabei kann es passieren, dass $\phi(n) = 0_K$ für ein $n \in \mathbb{N}$. Das kleinste derartige n ist dann eine Primzahl und heißt die *Charakteristik* des Körpers K.
Ist hingegen immer $\phi(n) \neq 0_K$, so sagt man, dass K von Charakteristik Null ist. Insbesondere sind angeordnete Körper von Charakteristik Null. Man sieht leicht ein, dass dann ϕ injektiv ist, und man denselben Beweis wie den von Proposition 2.7.8 hernehmen kann, um zu zeigen, dass sich $\mathbb{Q}$ injektiv in jeden Körper der Charakteristik Null einbetten lässt.

2.7.10 Bemerkung (*)**.** Die angegebene Art und Weise, aus $\mathbb{Z}$ die rationalen Zahlen zu konstruieren, lässt sich auf beliebige kommutative Integritätsringe R ausdehnen; vgl. Bemerkung 2.4.4. Dazu betrachtet man $R \times (R \setminus \{0\})$ und die Äquivalenzrelation $\sim$ mit $(x, a) \sim (y, b) \Leftrightarrow xb = ya$ darauf.
Die in diesem Abschnitt gebrachten Ergebnisse (samt Beweise) gelten sinngemäß auch in dieser allgemeineren Situation, wobei man hier i.A. keine sgn-Funktion hat, und wobei das multiplikativ Inverse zu $[(x, n)]_\sim$ genau $[(n, x)]_\sim$ ist. $(R \times (R \setminus \{0\}))/_\sim$ ist dann ein Körper (*Quotientenkörper* von R), aber i.A. kein angeordneter Körper.
Wendet man diese Konstruktion auf $\mathbb{Z}$ an, so erhält man wieder $\mathbb{Q}$.

2.8 Archimedisch angeordnete Körper

2.8.1 Definition. Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Dann heißt K *archimedisch angeordnet*, wenn $\mathbb{N}$ als Teilmenge von K nicht nach oben beschränkt ist.

In Satz 2.7.7 haben wir gesehen, dass die rationalen Zahlen archimedisch angeordnet sind. Wir werden auch sehen, dass die reellen Zahlen archimedisch angeordnet sind.

2.8.2 Beispiel. Die Eigenschaft, dass $\langle K, +, \cdot, P\rangle$ ein archimedisch angeordneter Körper ist, ermöglicht es uns das Infimum von Mengen wie

$$M = \left\{\frac{1}{n} : n \in \mathbb{N}\right\}$$

zu berechnen. Der Vermutung nach gilt $\inf M = 0$.
Um das zu beweisen, sei zunächst bemerkt, dass 0 offensichtlich eine untere Schranke von M ist. Wäre $\epsilon > 0$ eine weitere untere Schranke von M, also $0 < \epsilon < \frac{1}{n}$ für alle $n \in \mathbb{N}$, so folgte $n < \frac{1}{\epsilon}$, was aber der Eigenschaft von K, archimedisch angeordnet zu sein, widerspricht.

In archimedisch angeordneten Körpern gilt der folgende für die später zu entwickelnde Konvergenztheorie wichtige

2.8.3 Satz. *Sei $\langle K, +, \cdot, P\rangle$ ein archimedisch angeordneter Körper. Sind $x, y \in K$, $x < y$, dann existiert ein $p \in \mathbb{Q}$ mit $x < p < y$* [12].

Beweis. Seien zunächst $x, y \in K$ mit $0 \leq x < y$ gegeben. Dann ist $y - x > 0$ und damit auch $\frac{1}{y-x} > 0$. Da K archimedisch angeordnet ist, gibt es ein $n \in \mathbb{N}$ mit $n > \frac{1}{y-x}$ und daher $n(y - x) > 1$.
Nach Satz 2.3.12 hat $\{k \in \mathbb{N} : k > nx\}$ ein Minimum, und somit gibt es eine kleinste natürliche Zahl $m \in \mathbb{N}$, sodass $m > nx$. Ist $m > 1$, so folgt aus der Wahl von m, dass $m - 1 \leq nx$. Ist $m = 1$, so folgt gemäß unserer Voraussetzung $m - 1 = 0 \leq nx$. Also gilt immer $m - 1 \leq nx < m$. Kombiniert man diese Ungleichung mit $n(y - x) > 1$, so folgt

$$nx < m \leq nx + 1 < ny\,,$$

und damit $x < \frac{m}{n} < y$.
Ist schließlich $x < 0$, so können wir ein $k \in \mathbb{N}$ wählen mit $k \geq |x|$, da $\mathbb{N}$ ja nicht nach oben beschränkt ist. Es folgt $0 \leq x + k < y + k$, und nach dem eben Bewiesenen $x + k < \frac{m}{n} < y + k$. Nun ist $\frac{m}{n} - k$ eine rationale Zahl mit $x < \frac{m}{n} - k < y$. ❑

2.8.4 Bemerkung. Da man obigen Satz induktiv immer wieder anwenden kann, liegen zwischen zwei verschiedenen Zahlen sogar unendlich viele rationale Zahlen.
Ist $\mathbb{Q} \subsetneq K$, so kann man mit einer linearen Transformation sogar zeigen, dass es eine nicht rationale Zahl zwischen 0 und 1 gibt, und weiters unter Verwendung von Satz 2.8.3, dass es zwischen zwei Zahlen von K auch eine nicht rationale Zahl gibt.

2.9 Das Vollständigkeitsaxiom

Wie wir später sehen werden, ist die Vollständigkeit die Eigenschaft der reellen Zahlen, die sie unverwechselbar von anderen angeordneten Körpern unterscheidet.

2.9.1 Definition. Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Dann heißt K *vollständig angeordnet*, wenn jede nach oben beschränkte Teilmenge von K ein Supremum hat. Diese Eigenschaft wollen wir (s) nennen.

Wie schon im vorhergehenden Abschnitt erwähnt, gilt

2.9.2 Lemma. *Ist $\langle K, +, \cdot, P\rangle$ ein vollständig angeordneter Körper, so ist er archimedisch angeordnet.*

Beweis. Wäre nämlich $\mathbb{N}$ nach oben beschränkt, so existierte wegen (s)

$$\eta = \sup \mathbb{N}.$$

Sei n beliebig in $\mathbb{N}$. Mit n gehört aber auch $n+1$ zu $\mathbb{N}$. Also gilt $n+1 \leq \eta$, und somit $n \leq \eta - 1$. Daher ist $\eta - 1$ eine obere Schranke von $\mathbb{N}$, was den Widerspruch $\eta - 1 \geq \sup \mathbb{N} = \eta$ nach sich zieht. ❑

[12] Diese Aussage nennt man auch die *Dichteeigenschaft* von $\mathbb{Q}$ in K.

Fundamental ist folgender Satz, dessen Beweis wir später – am Ende dieses Abschnittes bzw. im Kapitel 4 – bringen werden.

2.9.3 Satz. *Es gibt einen vollständig angeordneten Körper $\langle L, +, \cdot, L^+\rangle$.*
Ist $\langle K, +, \cdot, P\rangle$ ein weiterer vollständig angeordneter Körper, so gibt es einen eindeutigen Isomorphismus $\phi : L \to K$, also eine Bijektion, sodass ϕ mit den Operationen verträglich ist und sodass $\phi(L^+) = P$.

Wenn wir ab jetzt von den reellen Zahlen sprechen, dann sei immer ein vollständig angeordneter Körper $\langle L, +, \cdot, L^+\rangle$ gemeint. Wir schreiben im Folgenden immer $\langle \mathbb{R}, +, \cdot, \mathbb{R}^+\rangle$ dafür. Wegen Satz 2.9.3 ist $\langle \mathbb{R}, +, \cdot, \mathbb{R}^+\rangle$ bis auf Kopien eindeutig. Es sei aber bemerkt, dass diese Eindeutigkeit für die restlichen Aussagen dieses Kapitels und auch für Kapitel 3 unerheblich sind – diese also in jedem vollständig angeordneten Körper gelten.

2.9.4 Bemerkung. Zusammenfassend sei nochmals betont, dass die reellen Zahlen $\mathbb{R}$ einen vollständig angeordneter Körper bilden, der die Körperaxiome $(a1)$-$(a4)$, $(m1)$-$(m4)$, (d), die Axiome eines angeordneten Körpers $(p1)$-$(p3)$ und das Vollständigkeitsaxiom (s) erfüllt.
Alle bisher gezeigten Rechenregeln und Eigenschaften von $\mathbb{R}$ lassen sich alle aus diesen Axiomen herleiten, bzw. haben wir hergeleitet. Auch die im Folgenden aufgebaute Analysis setzt nur auf diese Axiome auf.

Die Vollständigkeit von $\mathbb{R}$ garantiert zum Beispiel, dass es n-te Wurzeln von nichtnegativen Zahlen gibt.

2.9.5 Satz. *Sei $x \in \mathbb{R}$, $x \geq 0$, und $n \in \mathbb{N}$. Dann existiert genau eine Zahl $y \in \mathbb{R}$, $y \geq 0$, sodass $y^n = x$.*

Beweis. Im Fall $n = 1$ ist die Aussage trivial. Sei also $n \geq 2$. Die Eindeutigkeit von y folgt unmittelbar aus Lemma 2.4.10, da aus $0 \leq y_1 < y_2$ immer $y_1^n < y_2^n$ folgt. Somit können nicht beide der Gleichung $y^n = x$ genügen.
Zur Existenz: Ist $x = 0$, so ist klarerweise $y^n = x$ für $y = 0$. Im Fall $x > 0$ sei

$$E := \{t \in \mathbb{R} : \ t > 0, t^n < x\}.$$

Diese Menge ist nicht leer, denn für $s = \frac{x}{1+x}$ gilt $0 < s < \min(x, 1)$ und daher $s^n < s < x$; also $s \in E$. Für $\tau := 1 + x$ gilt $\tau > 1$ und daher $\tau^n > \tau > x$. Aus $t \geq \tau$ folgt dann $t^n \geq \tau^n > x$ und damit $t \notin E$. Also muss τ eine obere Schranke von E sein.
Da $\mathbb{R}$ vollständig angeordnet ist, existiert $y := \sup E$. Wegen $0 < \frac{x}{1+x} \in E$ gilt $y > 0$. Wir zeigen im Folgenden, dass $y^n = x$, und zwar indem wir die beiden anderen Möglichkeiten $y^n < x$ und $y^n > x$ ausschließen. Dazu benötigen wir, dass die für beliebige Elemente $a, b \in \mathbb{R}$ geltende und mit vollständiger Induktion nach n zu beweisende Gleichung

$$b^n - a^n = (b - a)(b^{n-1} + b^{n-2}a + \ldots + ba^{n-2} + a^{n-1}) . \tag{2.9}$$

Für $0 < a < b$ erhalten wir daraus die Abschätzung

$$b^n - a^n < (b - a)nb^{n-1} . \tag{2.10}$$

Angenommen $y^n < x$, so gibt es gemäß Satz 2.8.3 ein $\epsilon \in \mathbb{Q}$ mit

$$0 < \epsilon < \min\left(\frac{x - y^n}{n(y+1)^{n-1}}, 1\right).$$

Für $a = y$ und $b = y + \epsilon$ folgt aus (2.10)

$$(y+\epsilon)^n - y^n < \epsilon n(y+\epsilon)^{n-1} < \epsilon n(y+1)^{n-1} < x - y^n.$$

Also gilt $(y+\epsilon)^n < x$ und daher $y + \epsilon \in E$ im Widerspruch zu $y = \sup E$.
Wäre andererseits $y^n > x$, so gilt für

$$\delta := \frac{y^n - x}{n y^{n-1}}$$

$0 < \delta < \frac{y}{n} < y$. Wir wollen zeigen, dass $y - \delta$ eine obere Schranke von E ist. Wäre dem nicht so, dann gilt $t > y - \delta$ für ein $t \in E$. Aus (2.10) folgt aber mit $b = y, a = (y - \delta)$

$$y^n - t^n < y^n - (y-\delta)^n < \delta n y^{n-1} = y^n - x.$$

Also $t^n > x$, und daher der Widerspruch $t \notin E$. Die Tatsache, dass $y - \delta$ eine obere Schranke von E ist, widerspricht aber $y = \sup E$. ❑

2.9.6 Definition. Die nach obigem Satz eindeutig bestimmte Zahl $y \geq 0$, die n-te *Wurzel* von x, schreibt man auch als $\sqrt[n]{x}$ oder $x^{\frac{1}{n}}$.

2.9.7 Bemerkung. Man betrachte die Funktion

$$\begin{cases} \mathbb{R}^+ \cup \{0\} & \to & \mathbb{R}^+ \cup \{0\}, \\ y & \mapsto & y^n. \end{cases}$$

Gemäß Lemma 2.4.10 ist diese Funktion streng monoton wachsend und daher injektiv. Zu gegebenem x ist $y = \sqrt[n]{x}$ jene Zahl, sodass $y^n = x$. Also ist $y \mapsto y^n$ auch surjektiv als Funktion von $\mathbb{R}^+ \cup \{0\}$ nach $\mathbb{R}^+ \cup \{0\}$. Sie ist also bijektiv und ihre Umkehrfunktion ist genau $x \mapsto \sqrt[n]{x}$. Wegen Lemma 2.4.10 ist auch $x \mapsto \sqrt[n]{x}$ streng monoton wachsend.

2.9.8 Bemerkung. Mit Hilfe der Existenz von Wurzeln sehen wir auch, dass $\mathbb{R}$ nicht nur aus rationalen Zahlen bestehen kann, also $\mathbb{Q} \subsetneq \mathbb{R}$ gilt. Wäre nämlich

$$\sqrt{2} = \frac{p}{q} \in \mathbb{Q}, \tag{2.11}$$

so kann man p, q teilerfremd wählen. Also gibt es kein $k \in \mathbb{N} \setminus \{1\}$, welches p und q teilt[13]. Insbesondere ist nur höchstens eine der Zahlen p oder q gerade. Ausquadrieren und mit q^2 Multiplizieren in (2.11) ergibt $2q^2 = p^2$. Da eine Zahl genau dann gerade ist, wenn ihr Quadrat es ist, folgt, dass p gerade und damit q ungerade ist; siehe Satz 2.6.6. Schreibt man $p = 2m$, so folgt $2q^2 = 4m^2$, und damit $q^2 = 2m^2$. Wir erhalten daraus den Widerspruch, dass auch q gerade sein müsste.

[13] Eine ganze Zahl $k \neq 0$ teilt eine ganze Zahl n, wenn es ein $m \in \mathbb{Z}$ gibt, sodass $km = n$.

2.9.9 Definition. Ist $x > 0$ und ist $r \in \mathbb{Q}$ dargestellt in der Form $r = \frac{p}{q}$ mit $p \in \mathbb{Z},\ q \in \mathbb{N}$, so definieren wir

$$x^r := \left(\sqrt[q]{x}\right)^p .$$

Da die Darstellung einer rationalen Zahl als Bruch nicht eindeutig ist, müssen wir nachweisen, dass die Definition von x^r nicht von der Wahl von p, q abhängt. Dazu brauchen wir

2.9.10 Lemma. *Sind $x > 0, z > 0$ und $p \in \mathbb{Z},\ q \in \mathbb{N}$, so gilt $\sqrt[q]{\frac{1}{x}} = \frac{1}{\sqrt[q]{x}}$, $\sqrt[q]{xz} = \sqrt[q]{x}\sqrt[q]{z}$ sowie*

$$(\sqrt[q]{x})^p = \sqrt[q]{x^p}. \tag{2.12}$$

Beweis. $\sqrt[q]{\frac{1}{x}} = \frac{1}{\sqrt[q]{x}}$ folgt aus $(\frac{1}{\sqrt[q]{x}})^q = \frac{1}{(\sqrt[q]{x})^q} = \frac{1}{x}$ und der Tatsache, dass nach Satz 2.9.5 $\sqrt[q]{\frac{1}{x}}$ die eindeutige Lösung y von $y^q = \frac{1}{x}$ ist.
Wegen $(\sqrt[q]{x}\sqrt[q]{z})^q = (\sqrt[q]{x})^q(\sqrt[q]{z})^q = xz$ muss $\sqrt[q]{x}\sqrt[q]{z}$ mit $\sqrt[q]{xz}$ übereinstimmen.
Ist $p = 0$, so ist (2.12) trivialerweise richtig, da ja $\sqrt[q]{1} = 1$. Sonst folgt (2.12) aus $((\sqrt[q]{x})^p)^q = ((\sqrt[q]{x})^q)^p = x^p$ (siehe (2.5)) und aus der Tatsache, dass nach Satz 2.9.5 $\sqrt[q]{x^p}$ die eindeutige Lösung y von $y^q = x^p$ ist. ❑

Ist jetzt $r = \frac{p}{q} = \frac{m}{n}$, so folgt wegen $pn = qm$

$$(\sqrt[q]{x^p})^n = \sqrt[q]{x^{pn}} = \sqrt[q]{x^{qm}} = (\sqrt[q]{x^q})^m = x^m.$$

Zieht man links und rechts die n-te Wurzel, so gilt wegen (2.12)

$$\sqrt[q]{x^p} = \sqrt[n]{x^m},$$

und damit ist x^r wohldefiniert. Außerdem gelten die (mit einer Beweisführung ähnlich wie der von Lemma 2.9.10 zu zeigenden) Rechenregeln ($r, s \in \mathbb{Q},\ x > 0$)

$$x^{r+s} = x^r x^s,\ (x^r)^s = x^{rs},\ x^{-r} = \frac{1}{x^r}.$$

2.9.11 Lemma (Lemma vom iterierten Supremum)**.** *Seien M, N zwei nichtleere Mengen und $f : M \times N \to \mathbb{R}$, sodass $\{f(m,n) : (m,n) \in M \times N\}$ nach oben beschränkt ist. Man nennt eine solche Funktion nach oben beschränkt. Dann gilt*

$$\begin{aligned}\sup\{\, f(m,n) : (m,n) \in M \times N \,\} &= \sup\{\, \sup\{f(m,n) : m \in M\} : n \in N \,\} \\ &= \sup\{\, \sup\{f(m,n) : n \in N\} : m \in M \,\}.\end{aligned}$$

Sind umgekehrt alle Mengen $\{f(m,n) : m \in M\},\ n \in N$, nach oben beschränkt genauso wie $\{\sup\{f(m,n) : m \in M\} : n \in N\}$, bzw. gilt entsprechendes mit M und N vertauscht, so ist auch $\{f(m,n) : (m,n) \in M \times N\}$ nach oben beschränkt, womit obige Gleichung wieder gilt. [14]
Eine entsprechende Aussage gilt fürs Infimum.

[14] Also gilt obige Gleichung auch für nicht notwendigerweise nach oben beschränkte Funktionen, wenn man auch den Wert $+\infty$ zulässt.

Beweis. Wir setzen $s = \sup\{f(m,n) : (m,n) \in M \times N\}$ und für festes $q \in N$ auch $s_q = \sup\{f(m,q) : m \in M\}$. Aus $\{f(m,q) : m \in M\} \subseteq \{f(m,n) : (m,n) \in M \times N\}$ folgt dann $s_q \leq s$ für jedes $q \in N$; also auch $\sup\{s_q : q \in N\} \leq s$.
Umgekehrt folgt für festes $(m,n) \in M \times N$, dass $f(m,n) \in \{f(m,q) : m \in M\}$, wenn nur $q = n$. Für dieses q ist $f(m,n) \leq s_q$; also gilt auch $f(m,n) \leq \sup\{s_q : q \in N\}$. Da $(m,n) \in M \times N$ beliebig war, folgt schließlich $s \leq \sup\{s_q : q \in N\}$. ❑

2.10 Dedekindsche Schnitte*

Am Ende dieses Abschnitts werden wir beweisen, dass vollständig angeordnete Körper tatsächlich existieren, und dass alle solche immer Kopien von einander sind. Eine andere Art und Weise, das zu tun, findet sich in Kapitel 4.
Um diese anspruchsvolle Konstruktion zu motivieren, denken wir uns eine Gerade gemeinsam mit einer Einheitsstrecke gezeichnet. Auf dieser Geraden denken wir uns die rationalen Zahlen durch fortgesetztes unterteilen der Einheitsstrecke aufgetragen. Obwohl es anschaulich beliebig nahe an jedem Punkt eine rationale Zahl gibt, gibt es gemäß Bemerkung 2.9.8 Punkte, welche nicht rational sind.
Unsere Konstruktion beruht auf der folgenden Bemerkung, die Richard Dedekind gemacht hat: Zerfallen alle Punkte der Geraden in zwei Klassen von der Art, dass jeder Punkt der ersten Klasse links von jedem Punkt der zweiten Klasse liegt, so existiert ein und nur ein Punkt, welcher diese Einteilung aller Punkte in zwei Klassen, diese Zerschneidung der Geraden in zwei Stücke, hervorbringt.
Man kann also einen Punkt P der Geraden identifizieren mit der Menge aller Punkte, die links von ihm liegen. Da man nun aber mit den rationalen Punkten beliebig nahe an den Punkt P herankommt, genügt es, alle rationalen Punkte, die links von P liegen, zu kennen, um P selbst eindeutig zu rekonstruieren.

2.10.1 Satz. *Es gibt einen vollständig angeordneten Körper. Dieser ist bis auf Isomorphie eindeutig bestimmt.*

Beweis. Der Beweis dieses Satzes ist relativ lang und wird in mehreren Schritten geführt, von denen wir auch nicht alle im Detail ausführen werden.

Schritt 1: Eine Teilmenge α von $\mathbb{Q}$ heißt ein *Dedekindscher Schnitt*, wenn sie die folgenden drei Eigenschaften besitzt:

- (I) $\alpha \neq \emptyset$, $\alpha \neq \mathbb{Q}$.
- (II) Aus $p \in \alpha$ folgt $(-\infty, p] \subseteq \alpha$.
- (III) Ist $p \in \alpha$, so existiert ein $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, sodass $p + \epsilon \in \alpha$.

Die Menge aller Dedekindschen Schnitte bezeichnen wir mit K.

Dieser Begriff modelliert die Anschauung der Menge aller rationalen Punkte, die „links von dem Punkt der Geraden liegen“.

Die Eigenschaft (*III*) besagt, dass α kein größtes Element hat. Aus der Eigenschaft (*II*) erhält man unmittelbar die folgenden beiden Aussagen.

(*i*) Ist $p \in \alpha$ und $q \notin \alpha$, dann ist $p < q$.

(*ii*) Ist $r \notin \alpha$ und $s > r$, so ist $s \notin \alpha$.

Schritt 2: Wir definieren eine Relation $\leq$ auf K durch

$$\alpha \leq \beta \ :\Leftrightarrow \ \alpha \subseteq \beta,\ \alpha, \beta \in K\,,$$

Diese Relation ist offenbar eine Halbordnung. Wir zeigen, dass sie sogar eine Totalordnung ist. Seien $\alpha, \beta \in K$ und sei angenommen, dass $\alpha \not\leq \beta$, also $\alpha \not\subseteq \beta$. Dann existiert $p \in \alpha$ mit $p \notin \beta$. Somit folgt aus $q > p$, dass $q \notin \beta$, und aus $q < p$, dass $q \in \alpha$. Ist also $q \in \beta$, so muss $q < p$ sein und daher zu α gehören. Infolge gilt $\beta \leq \alpha$.

Für $\alpha \subsetneq \beta$ schreiben wir auch $\alpha < \beta$.

Schritt 3: In diesem Schritt zeigen wir, dass K mit der Ordnung $\leq$ die Supremumseigenschaft besitzt. Sei $A \subseteq K$ eine nichtleere und nach oben beschränkte Teilmenge von K, und setze

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

Wir zeigen, dass $\gamma \in K$. Da A nichtleer ist, existiert ein $\alpha_0 \in A$. Nun ist α_0 nichtleer und $\alpha_0 \subseteq \gamma$, also gilt auch $\gamma \neq \emptyset$. Da A nach oben beschränkt ist, existiert $\beta \in K$ mit $\alpha \subseteq \beta$ für alle $\alpha \in A$, was $\gamma \subseteq \beta$ nach sich zieht. Wegen $\beta \neq \mathbb{Q}$ ist auch $\gamma \neq \mathbb{Q}$. Also erfüllt γ die Eigenschaft (*I*). Ist $p \in \gamma$, so existiert $\alpha \in A$ mit $p \in \alpha$. Also folgt $(-\infty, p] \subseteq \alpha \subseteq \gamma$. Weiters existiert ein rationales $\epsilon > 0$ mit $r + \epsilon \in \alpha \subseteq \gamma$. Wir sehen also, dass γ die Eigenschaften (*II*) und (*III*) hat.

Es bleibt $\gamma = \sup A$ zu zeigen. Offenbar gilt $\alpha \leq \gamma$ für alle $\alpha \in A$. Ist $\beta \in K$ mit $\beta \geq \alpha$ bzw. $\beta \supseteq \alpha$ für alle $\alpha \in A$, so folgt $\beta \supseteq \gamma$. Also ist γ tatsächlich die kleinste obere Schranke von A.

Schritt 4: Wir definieren eine Addition auf K. Für $\alpha, \beta \in K$ setze

$$\alpha + \beta := \{r + s :\ r \in \alpha, s \in \beta\}\,.$$

Weiters setze $0^* := \{p \in \mathbb{Q} :\ p < 0\}$.

Als erstes zeigen wir, dass $\alpha + \beta \in K$. Da $\alpha \neq \emptyset$ und $\beta \neq \emptyset$, folgt auch $\alpha + \beta \neq \emptyset$. Wähle $r' \notin \alpha$ und $s' \notin \beta$, dann ist $r' > r$, $r \in \alpha$, und $s' > s$, $s \in \beta$. Also erhalten wir $r' + s' > r + s$, $r \in \alpha$, $s \in \beta$. Damit kann $r' + s'$ nicht zu $\alpha + \beta$ gehören. Wir sehen, dass $\alpha + \beta$ die Eigenschaft (*I*) besitzt. Sei nun $p \in \alpha + \beta$ gegeben, und schreibe $p = r + s$ mit gewissen $r \in \alpha$, $s \in \beta$. Für $q < p$ folgt $q - s < r$ und daher $q - s \in \alpha$. Also $q = (q - s) + s \in \alpha + \beta$, und wir sehen, dass (*II*) gilt. Zu $p = r + s \in \alpha + \beta$ wähle ein rationales $\epsilon > 0$ mit $r + \epsilon \in \alpha$, dann folgt $r + s + \epsilon \in \alpha + \beta$, also gilt auch (*III*).

Die Addition ist kommutativ, denn

$$\alpha + \beta = \{r + s : \ r \in \alpha, s \in \beta\} = \{s + r : \ r \in \alpha, s \in \beta\} = \beta + \alpha \, .$$

Sie ist assoziativ, denn

$$\begin{aligned} \alpha + (\beta + \gamma) &= \{r + u : \ r \in \alpha, u \in (\beta + \gamma)\} \\ &= \{r + (s + t) : \ r \in \alpha, s \in \beta, t \in \gamma\} \\ &= \{(r + s) + t : \ r \in \alpha, s \in \beta, t \in \gamma\} \\ &= \{v + t : \ v \in (\alpha + \beta), t \in \gamma\} = (\alpha + \beta) + \gamma \, . \end{aligned}$$

Nun identifizieren wir 0^* als das neutrale Element bezüglich der Addition: Ist $r \in \alpha$ und $s \in 0^*$, so folgt $r + s < r$, also $r + s \in \alpha$. D.h. $\alpha + 0^* \leq \alpha$.

Sei umgekehrt $p \in \alpha$, und wähle ein rationales $\epsilon > 0$ mit $p + \epsilon \in \alpha$. Dann gilt $p = p + \epsilon + (-\epsilon) \in \alpha + 0^*$.

Es bleibt zu zeigen, dass jedes Element von K ein additives Inverses besitzt. Sei also $\alpha \in K$ gegeben. Setze

$$\beta := \{p \in \mathbb{Q} : \ \exists \, \epsilon > 0 : p + \epsilon \notin -\alpha\} \, .$$

Als erstes zeigen wir, dass $\beta \in K$. Sei $s \notin \alpha$ und setze $p := -s - 1$, dann ist $p + 1 = -s \notin -\alpha$, also $p \in \beta$ und damit $\beta \neq \emptyset$. Aus $q \in \alpha$ folgt $-q \notin \beta$, da sonst $q - \epsilon \notin \alpha$, und somit $q \notin \alpha$; also $\beta \neq \mathbb{Q}$. Damit gilt (I). Sei nun $p \in \beta$ gegeben. Wähle $\epsilon > 0$, sodass $-p - \epsilon \notin \alpha$. Ist $q < p$, so gilt $-q - \epsilon > -p - \epsilon$ und daher $-q - \epsilon \notin \alpha$. Es folgt $q \in \beta$, und somit gilt (II). $t := p + \frac{\epsilon}{2}$ erfüllt $t > p$ und $-t - \frac{\epsilon}{2} = -p - \epsilon \notin \alpha$, wodurch $t \in \beta$. Also gilt (III).

Ist $r \in \alpha$ und $s \in \beta$, so ist $-s \notin \alpha$ und daher $r < -s$. Daher ist $r + s < 0$, bzw, $r + s \in 0^*$. Wir sehen, dass $\alpha + \beta \leq 0^*$.

Umgekehrt sei $v \in 0^*$. Setze $w := -\frac{v}{2} > 0$. Sei $q \notin \alpha$. Da $\mathbb{Q}$ archimedisch angeordnet ist, gibt es ein $n_1 \in \mathbb{N}$ mit $n_1 w > q$ und daher mit $n_1 w \notin \alpha$. Zu $q \in \alpha$ gibt es auch ein $n_2 \in \mathbb{N}$ mit $n_2 w > -q$ und daher mit $-n_2 w \in \alpha$.

Es existiert also ein $n \in \mathbb{Z}$ mit $nw \in \alpha$ und $(n + 1)w \notin \alpha$. Setze $p := -(n + 2)w$. Dann ist $p \in \beta$, denn $-p - w \notin \alpha$. Wir haben also

$$v = nw + p \in \alpha + \beta \, .$$

Schritt 5: Die Addition ist mit der Ordnung verträglich. Ist nämlich $\alpha \leq \beta$, also $\alpha \subseteq \beta$, und ist $\gamma \in K$, so folgt $\alpha + \gamma \subseteq \beta + \gamma$. Addieren von $-\gamma$ zeigt, dass in der Tat $\alpha \leq \beta \Leftrightarrow \alpha + \gamma \leq \beta + \gamma$.

Daraus folgt unmittelbar $\alpha < \beta \Leftrightarrow \beta - \alpha \in P := \{\gamma \in K : \gamma > 0\}$, und die Tatsache, dass mit $\alpha, \beta \in P$ auch $\alpha + \beta > \alpha + 0^* > 0^*$ und somit $\alpha + \beta \in P$.

Schritt 6: Wir definieren eine Multiplikation auf K. Seien zunächst $\alpha, \beta > 0$. Dann setze

$$\alpha \cdot \beta := \{p \in \mathbb{Q} : \exists r \in \alpha, s \in \beta, r, s > 0 : p \leq rs\}.$$

Man zeigt genauso wie in Schritt 4, dass $\alpha \cdot \beta$ tatsächlich ein Element von K ist, dass die Multiplikation kommutativ und assoziativ ist, und dass das Distributivgesetz gilt.

Weiters definieren wir

$$1^* := \{p \in \mathbb{Q} : p < 1\}.$$

Wieder sieht man analog wie in den vorherigen Beweisschritten, dass 1^* neutrales Element bezüglich der Multiplikation ist, und dass jedes Element $\alpha > 0$ ein multiplikatives Inverses

$$\beta := \{p \in \mathbb{Q} : \exists \epsilon > 0 : p + \epsilon \notin \{\frac{1}{q} : q \in \alpha, q > 0\}\}$$

besitzt.

Um nun die Multiplikation auch für Elemente $\alpha < 0$ zu definieren, setze

$$\alpha \cdot \beta := \begin{cases} (-\alpha) \cdot (-\beta), & \text{falls } \alpha < 0^* \text{ und } \beta < 0^*, \\ (-\alpha) \cdot \beta, & \text{falls } \alpha < 0^* \text{ und } \beta > 0^*, \\ \alpha \cdot (-\beta), & \text{falls } \alpha > 0^* \text{ und } \beta < 0^*, \\ 0^*, & \text{falls } \alpha = 0^* \text{ oder } \beta = 0^*. \end{cases}$$

Der Beweis der Rechengesetze folgt aus den bereits bekannten Regeln für die Multiplikation von positiven Zahlen durch Fallunterscheidungen.

Um $\alpha, \beta \in P \Rightarrow \alpha \cdot \beta \in P$ einzusehen, wähle man $a \in \alpha \setminus 0^*,\ b \in \beta \setminus 0^*$. Also $a, b \geq 0$. Wegen (III) können wir sogar $a, b > 0$ annehmen. Es folgt $a \cdot b \in \alpha \cdot \beta \setminus 0^*$ und somit $\alpha, \beta \in P$.

Wir haben also bewiesen, dass $\langle K, +, \cdot, P\rangle$ ein vollständig angeordneter Körper ist.

Schritt 7: Wie jeder angeordnete Körper enthält K eine Kopie von $\mathbb{Q}$, daher eine mit den Operationen und mit $\leq$ Verträgliche Injektion $\phi : \mathbb{Q} \to K$; vgl. Proposition 2.7.8. Aus $\phi(1) = 1^*$ folgt mit vollständiger Induktion $\phi(n) = \{p \in \mathbb{Q} : p < n\}$.

Außerdem zeigt man, dass für $r, s \in \mathbb{Q}$ und $\alpha_r = \{p \in \mathbb{Q} : p < r\},\ \alpha_s = \{p \in \mathbb{Q} : p < s\}$

$$\alpha_r + \alpha_s = \{p \in \mathbb{Q} : p < r + s\},\ \ -\alpha_r = \{p \in \mathbb{Q} : p < -r\},$$

$$\alpha_r \cdot \alpha_s = \{p \in \mathbb{Q} : p < rs\},\ \ \alpha_r^{-1} = \{p \in \mathbb{Q} : p < \frac{1}{r}\}.$$

Für $r > 0$ sieht man z.B. letztere Tatsache folgendermaßen:

$$\begin{aligned} \alpha_r^{-1} &= \{p \in \mathbb{Q} : \exists \epsilon > 0 : p + \epsilon \notin \{\frac{1}{q} : q \in \mathbb{Q}, 0 < q < r\}\} \\ &= \{p \in \mathbb{Q} : \exists \epsilon > 0 : p + \epsilon \leq \frac{1}{r}\} = \{p \in \mathbb{Q} : p < \frac{1}{r}\}. \end{aligned}$$

Aus $\phi(\frac{x}{n}) = \operatorname{sgn}(x)\frac{\phi(|x|)}{\phi(n)}$ für $x \in \mathbb{Z},\ n \in \mathbb{N}$, folgt somit $\phi(r) = \alpha_r,\ r \in \mathbb{Q}$.

Schritt 8: Wir zeigen, dass jeder vollständig angeordnete Körper L isomorph zu dem oben konstruierten Körper K ist. Beachte, dass L und K als angeordnete Körper den Körper der rationalen Zahlen enthalten. Definiere

$$\omega : \begin{cases} L & \to & K\,, \\ x & \mapsto & \{p \in \mathbb{Q} : \ p < x\}\,, \end{cases} \quad , \quad \psi : \begin{cases} K & \to & L\,, \\ \alpha & \mapsto & \sup \alpha\,. \end{cases}$$

Die Abbildung ω ist wohldefiniert, denn $\{p \in \mathbb{Q} : \ p < x\}$ ist, wie man unmittelbar überprüft, ein Dedekindscher Schnitt. Auch ψ ist wohldefiniert, denn α ist eine nichtleere und beschränkte Teilmenge von $\mathbb{Q} \subseteq L$ und besitzt daher in L ein Supremum.

Außerdem sind diese beiden Abbildungen streng monoton wachsend, und für $p \in \mathbb{Q}$ gilt $\omega(p) = \alpha_p$ und $\psi(\alpha_p) = \sup \alpha_p = p$.

Aus dem noch zu zeigenden Lemma 2.10.2 folgt, dass ω und ψ mit den Operationen verträglich sind. Wendet man Lemma 2.10.2 nun auch auf $\omega \circ \psi$ und $\psi \circ \omega$ an, so folgt aus der Eindeutigkeitsaussage, dass $\omega \circ \psi = \mathrm{id}_K$ und $\psi \circ \omega = \mathrm{id}_L$. Also sind ω und ψ zueinander inverse Bijektionen, welche mit Addition, Multiplikation und Ordnung verträglich sind. Daher sind L und K als angeordnete Körper isomorph. Mit derselben Argumentation zeigt man auch, dass der von uns angegebene Isomorphismus eindeutig ist. ❑

2.10.2 Lemma. *Seien K_1 und K_2 zwei vollständig angeordnete Körper, und bezeichne $\mathbb{Q}_1$ bzw. $\mathbb{Q}_2$ die gemäß Proposition 2.7.8 existierende Kopie von $\mathbb{Q}$, welche in K_1 bzw. K_2 enthalten ist. Seien $\phi_j : \mathbb{Q} \to K_j$, $j = 1, 2$, die entsprechenden Einbettungen.*
Ist $\omega : K_1 \to K_2$ streng monoton wachsend und so, dass $\omega(\phi_1(p)) = \phi_2(p)$ für alle $p \in \mathbb{Q}$, dann ist ω mit $+$ und $\cdot$ verträglich.
Schließlich muss jede weitere streng monoton wachsende Abbildung $\tilde{\omega} : K_1 \to K_2$ mit $\tilde{\omega}(\phi_1(p)) = \phi_2(p)$, $p \in \mathbb{Q}$ schon mit ω übereinstimmen.

Beweis. Zunächst beweisen wir die letzte Aussage. Angenommen es gäbe ein $x \in K_1$, sodass $\omega(x) \neq \tilde{\omega}(x)$. Ohne Beschränkung der Allgemeinheit sei $\omega(x) < \tilde{\omega}(x)$. Nach Satz 2.8.3 gibt es ein $p \in \mathbb{Q}$ mit $\omega(x) < \phi_2(p) < \tilde{\omega}(x)$.
Nun muss $x < \phi_1(p)$, da widrigenfalls $\phi_1(p) \leq x$ und daher $\omega(\phi_1(p)) = \phi_2(p) \leq \omega(x)$. Andererseits muss aber $\phi_1(p) < x$, da sonst $x \leq \phi_1(p)$ und daher $\tilde{\omega}(x) \leq \phi_2(p) = \tilde{\omega}(\phi_1(p))$. Beides kann aber nicht gleichzeitig gelten. Somit muss $\omega = \tilde{\omega}$.
Zur Verträglichkeit mit $+$ halte man zunächst ein $p \in \mathbb{Q}$ fest, und betrachte

$$\omega_p : \begin{cases} K_1 & \to & K_2\,, \\ x & \mapsto & \omega(x + \phi_1(p)) - \phi_2(p)\,. \end{cases}$$

Wegen den Eigenschaften von ϕ_1, ϕ_2 aus Proposition 2.7.8 folgt $\omega_p(\phi_1(q)) = \omega(\phi_1(q + p)) - \phi_2(p) = \phi_2(q)$ für alle $q \in \mathbb{Q}$. Außerdem ist ω_p offensichtlicherweise streng monoton wachsend.
Nach obiger Eindeutigkeitsaussage folgt $\omega = \omega_p$ bzw. $\omega(x + \phi_1(p)) = \omega(x) + \phi_2(p) = \omega(x) + \omega(\phi_1(p))$ für alle $x \in K_1$ und wegen der Beliebigkeit von p auch für alle $p \in \mathbb{Q}$.

Nun betrachte man für ein festes $y \in K_1$ die Abbildung $\omega_y(x) = \omega(x+y) - \omega(y)$. Wegen dem eben gezeigten erfüllt diese $\omega_y(\phi_1(q)) = \phi_2(q),\ q \in \mathbb{Q}$, und sie ist ebenfalls streng monoton wachsend. Also folgt $\omega_y = \omega$, bzw. $\omega(x+y) = \omega(x) + \omega(y),\ x, y \in K_1$.
Indem man zunächst $x \mapsto \frac{\omega(x\cdot\phi_1(p))}{\phi_1(p)}$ für festes $p \in \mathbb{Q} \setminus \{0\}$ und dann $x \mapsto \frac{\omega(x\cdot y)}{\omega(y)}$ für festes $y \in K_1 \setminus \{0\}$ betrachtet, folgt wie oben auch die Verträglichkeit mit $\cdot$. ❑

2.11 Die komplexen Zahlen

Betrachtet man die quadratische Gleichung $x^2 + 1 = 0$ und sucht die Lösungen davon, indem man formal rechnet, so erhält man $x_{1,2} = \pm\sqrt{-1}$, also eigentlich kein Ergebnis. Das stimmt mit der Tatsache überein, dass die Gleichung $x^2 + 1 = 0$ keine reellen Lösungen hat. Aus vielen Gründen wäre es trotzdem wünschenswert, mit Wurzeln aus negativen Zahlen rechnen zu können. Insbesondere hätte $x^2 + 1 = 0$ zwei Lösungen.
Wir formalisieren nun das Konzept der Wurzel aus einer negativen Zahl.

2.11.1 Definition. Die Menge der *komplexen Zahlen* $\mathbb{C}$ wird definiert als die Menge der Paare reeller Zahlen, $\mathbb{C} := \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Wir schreiben eine komplexe Zahl $(a, b) \in \mathbb{C}$ meist als $a + ib$ an, wobei i ein formales Symbol, die sogenannte *imaginäre Einheit*, ist. Für $z = a + ib \in \mathbb{C}$ heißt $a =: \operatorname{Re} z$ der *Realteil* und $b =: \operatorname{Im}$ der *Imaginärteil* von z. Sind $a + ib$ und $c + id$ zwei komplexe Zahlen, so definieren wir eine Addition und eine Multiplikation, indem wir

$$(a + ib) + (c + id) := (a + c) + i(b + d)\,, \tag{2.13}$$

$$(a + ib) \cdot (c + id) := (ac - bd) + i(bc + ad)\,. \tag{2.14}$$

setzen. Ist $a + ib \in \mathbb{C}$ mit $b = 0$, so schreibt man auch a anstatt $a + i0$, und ist $a = 0$, so schreibt man ib anstatt $0 + ib$. Für $0 + i1 \in \mathbb{C}$ schreibt man kurz i und für $0 + i0$ auch 0.

Wir wollen die triviale, aber nützliche Tatsache herausstellen, dass zwei komplexe Zahlen genau dann übereinstimmen, wenn ihre Realteile und ihre Imaginärteile übereinstimmen. Die imaginäre Einheit modelliert den Ausdruck $\sqrt{-1}$. Tatsächlich gilt gemäß (2.14), dass $i^2 = -1$ sowie $(-i)^2 = -1$.

2.11.2 Satz. *Die komplexen Zahlen $\langle \mathbb{C}, +, \cdot \rangle$ sind ein Körper, wobei $0 + i0$ das neutrale Element bezüglich $+$, $1 + i0$ das neutrale Element bezüglich $\cdot$, $(-a) + i(-b)$ die additiv Inverse zu $a + ib$, und*

$$\frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2} \tag{2.15}$$

die multiplikativ Inverse zu $a + ib \neq 0 + i0$ ist.

Beweis. Wir müssen die Körperaxiome aus Definition 2.1.1 nachweisen. Die Kommutativität von $+$ und $\cdot$, daher Axiome $(a4)$, $(m4)$, folgt unmittelbar aus der Definition in (2.13)

und (2.14). Genauso schnell überzeugt man sich von der Gültigkeit der Assoziativität von +, also von Axiom ($a1$). Wegen

$$\begin{aligned}((a+ib)\cdot(c+id))\cdot(x+iy) &= ((ac-bd)+i(bc+ad))\cdot(x+iy)\\ &= (acx-bdx-bcy-ady)+i(bcx+adx+acy-bdy)\\ &= (a+ib)\cdot((cx-dy)+i(cy+dx))\\ &= (a+ib)\cdot((c+id)\cdot(x+iy))\end{aligned}$$

gilt ($m1$). Ganz leicht sieht man, dass $0+i0$ das additiv neutrale Element von $\mathbb{C}$ ist, und dass $(-a)+i(-b)$ das zu $a+ib$ additiv inverse Element ist. Also sind ($a2$) und ($a3$) erfüllt. Genauso elementar sieht man, dass $1+i0$ das multiplikativ neutrale Element ist, und dass die in (2.15) angegebene komplexe Zahl das zu $a+ib$ multiplikativ inverse Element ist, womit ($m2$) und ($m3$) erfüllt sind. Schließlich gilt (d), da in $\mathbb{R}$ das Distributivgesetz gilt und da

$$\begin{aligned}(x+iy)\cdot((a+ib)+(c+id)) &= (x+iy)\cdot((a+c)+i(b+d))\\ &= (xa+xc-yb-yd)+i(xb+xd+ya+yc)\\ &= ((xa-yb)+i(xb+ya))+((xc-yd)+i(xd+yc))\\ &= (x+iy)\cdot(a+ib)+(x+iy)\cdot(c+id).\end{aligned}$$

❑

Die reellen Zahlen sind in $\mathbb{C}$ eingebettet vermöge der Abbildung $a\mapsto a+i\cdot 0$. Offenbar ist diese Einbettung ein Körperhomomorphismus, also verträglich mit den Verknüpfungen $+,\cdot$. Insbesondere sehen wir, dass $\mathbb{C}$ ein $\mathbb{R}$-Vektorraum ist. Die dafür nötigen Rechengesetze gelten, da sie einfach Spezialfälle der Rechenregeln des Körpers $\mathbb{C}$ sind. Eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum lässt sich leicht angeben, nämlich $\{1,i\}$. Denn es lässt sich ja jede komplexe Zahl in eindeutiger Weise als Linearkombination $a\cdot 1+b\cdot i$ mit den reellen Koeffizienten a,b anschreiben. Wir sehen also, dass die Dimension von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum zwei ist.
Graphisch lassen sich die Zahlen aus $\mathbb{C}$ als Punkte in der Ebene veranschaulichen, man spricht auch von der *Gaußschen Zahlenebene*. Dabei ist

$$|z| := \sqrt{a^2+b^2}\ \ (\geq 0) \tag{2.16}$$

die Länge des Vektors von $(0,0)$ nach (a,b). Wir nennen $|z|$ auch den *Betrag* von z.
Der Betrag auf den komplexen Zahlen wird gleich wie die Betragsfunktion auf einem angeordneten Körper bezeichnet. Es gelten nämlich vergleichbare Regeln ($z,w\in\mathbb{C}$):

(i) $|\operatorname{Re} z|\leq|z|,\ |\operatorname{Im} z|\leq|z|$

(ii) $|zw|=|z||w|$.

(iii) $|z+w|\leq|z|+|w|$.

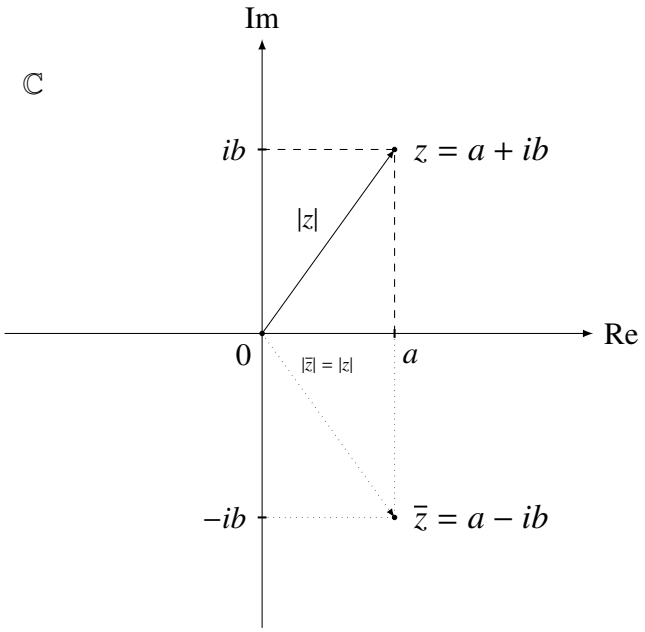

Abbildung 2.3: Zahlenebene

(*iv*) $|z + w| \geq \big||z| - |w|\big|$.

(*i*) und (*ii*) lassen sich dabei elementar nachprüfen. Die Dreiecksungleichung folgt durch Ausquadrieren, und die Dreiecksungleichung nach unten beweist man genauso, wie bei den angeordneten Körpern (siehe Lemma 2.2.12).
Eine weitere Begriffsbildung im Zusammenhang mit den komplexen Zahlen ist die der *konjugiert komplexen* Zahl $\bar{z}$ zu einer komplexen Zahl $z = a + ib$:

$$\bar{z} := a - ib\,.$$

Offenbar gilt $|\bar{z}| = |z|$, $|z|^2 = z\bar{z}$, und $z^{-1} = \frac{\bar{z}}{|z|^2}$ wenn $z \neq 0$. Der Übergang von z zu seiner konjugierten $\bar{z}$ entspricht bei der graphischen Veranschaulichung der komplexen Zahlen genau dem Spiegeln an der reellen Achse.

2.12 Übungsaufgaben

2.1 Sei $K = \{0, 1, 2\}$. Man definiere + und · so, dass $(K, +, \cdot)$ ein Körper wird. Lässt sich dieser Körper anordnen? Begründung!

2.2 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Man zeige ($x, y, a, b \in K$):

$x \leq y \vee y \leq x$,

$x \neq 0 \Rightarrow x^2 > 0$,

$(z > 0 \wedge x \leq y) \Rightarrow xz \leq yz$,

$(z < 0 \wedge x \leq y) \Rightarrow xz \geq yz$.

2.3 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Man zeige $(x, y, z \in K)$:

$0 < x \leq y \Rightarrow (\frac{x}{y} \leq 1 \leq \frac{y}{x} \wedge x^{-1} \geq y^{-1})$.

Außerdem beweise man $-\frac{2}{3} > -\frac{3}{4}$, wobei $2 := 1_K + 1_K, 3 := 1_K + 1_K + 1_K, 4 := 1_K + 1_K + 1_K + 1_K$.

2.4 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Zeigen Sie, dass $[-3, 1] + (-1, 1)$ ein Intervall ist! Welches? Entsprechend verfahre man mit $[2, 5] + [-2, -1]$!

2.5 Sei $\langle K, +, \cdot\rangle$ ein Körper, und seien $p, q \in K$. Man betrachte die Funktion $f(x) = x^2 + px + q$ von K nach K.

Man zeige, dass wenn x_1 eine Nullstelle ist, dann auch $x_2 := -p - x_1$ eine Nullstelle ist, dass dann $f(x) = (x - x_1)(x - x_2)$, und dass es dann keine weitere Nullstellen von f gibt. Also hat f höchstens zwei Nullstellen. Dabei heißt x_0 eine Nullstelle von f, wenn $f(x_0) = 0$.

Hinweis: Ist x_1 eine feste Nullstelle und $x \in K$, so gilt $f(x) = f(x) - f(x_1)$. Man berechne die rechte Seite unter zu Hilfenahme von $x^2 - x_1^2 = (x - x_1)(x + x_1)$.

2.6 Sei $\langle K, +, \cdot\rangle$ ein Körper, sodass $2 := 1_K + 1_K \neq 0$ und damit $4 := 1_K + 1_K + 1_K + 1_K = 2 \cdot 2 \neq 0$, und seien $p, q \in K$. Man betrachte die Funktion $f(x) = x^2 + px + q$ von K nach K. Man zeige, dass f genau dann eine Nullstelle hat, falls es ein $y \in K$ gibt, sodass $y^2 = \frac{p^2}{4} - q$. In diesem Falle zeige man, dass dann $-\frac{p}{2} + y$ und $-\frac{p}{2} - y$ genau die Lösungen von $f(x) = 0$ sind.

Hinweis: Quadratische Ergänzung.

2.7 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Um die Lösungsmenge einer Ungleichung z.B. der Form

$$|2 - x| \geq 4\,,$$

zu erhalten ($2 := 1_K + 1_K$, $4 := 2 + 2$) geht man folgendermaßen vor: Betrachte zuerst den Fall $x < 2$. Dann schreibt sich unsere Ungleichung als $2 - x \geq 4$, was zu $x \leq -2$ äquivalent ist. Also ist unsere Lösungsmenge in diesem Fall $\{x \in K : x < 2\} \cap \{x \in K : x \leq -2\} = \{x \in K : x \leq -2\}$.

Ist $x \geq 2$, so schreibt sich unsere Ungleichung als $x - 2 \geq 4$, und somit $x \geq 6 := 4 + 2$. Unsere Lösungsmenge ist in diesem Fall $\{x \in K : x \geq 2\} \cap \{x \in K : x \geq 6\} = \{x \in K : x \geq 6\}$.

Die Lösungsmenge insgesamt ist somit $\{x \in K : x \leq -2\} \cup \{x \in K : x \geq 6\} = (-\infty, -2] \cup [6, +\infty)$.

Man bestimme auf analoge Weise die Menge aller $x \in K,\ x \neq 1$, sodass

$$\frac{4x}{|1 - x|} \leq 2\,.$$

2.8 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Man bestimme die Menge aller $x \in K$, sodass

$$4|x| + |5 - 2x| \leq 8.$$

2.9 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Man zeige: Die Abbildung $\phi : x \mapsto \frac{x}{1_K+|x|}$ ist eine bijektive Abbildung von K auf $(-1_K, 1_K) = \{x \in K : -1_K < x < 1_K\}$. Man gebe auch die Inverse $\phi^{-1} : (-1_K, 1_K) \to K$ von ϕ an.

Weiters zeige man, dass ϕ streng monoton steigend ist: $x < y \Rightarrow \phi(x) < \phi(y)$.

2.10 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Man bestimme Minimum, Maximum, Infimum und Supremum (falls existent) der Menge

$$\left(-1_K, \frac{1_K}{2 \cdot 1_K}\right] \cup \left\{1_K + \frac{1_K}{n \cdot 1_K} : n \in \mathbb{N}\right\} \cup (2 \cdot 1_K, 3 \cdot 1_K] .$$

Begründen Sie ihre Antwort in mathematisch stichhaltiger Art und Weise!

2.11 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Man bestimme Minimum, Maximum, Infimum und Supremum (falls existent) der Menge

$$\bigcup_{0<x<y<1_K} \{t \in K : \frac{1_K}{y} < t < \frac{1_K}{x}\} .$$

Begründen Sie ihre Antwort in mathematisch stichhaltiger Art und Weise!

2.12 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper. Sei $M \subseteq K$ so, dass $\inf M$ existiert, und $s \in K$.

Man zeige: Es gilt $s < \inf M$ genau dann, wenn es ein $t \in K$ gibt, sodass $s < t \leq m$ für alle $m \in M$. Weiters zeige man: $s \leq \inf M \Leftrightarrow s \leq m,\ \forall m \in M$.

2.13 Man zeige: Ist $M \subseteq K$, so existiert $\sup M$ genau dann, wenn $\inf(-M)$ existiert. In diesem Falle gilt $-\sup M = \inf(-M)$.

2.14 Sei $\langle K, +, \cdot, P\rangle$ ein angeordneter Körper.

Sei $M \subseteq K$ nach oben beschränkt, und bezeichne O die Menge aller oberen Schranken. Man zeige, dass $O \cap M = \emptyset$ oder $O \cap M = \{z\}$, und dass die zweite Möglichkeit genau dann eintritt, wenn M ein Maximum hat.

2.15 Man stelle eine Formel für ($n \in \mathbb{N}$)

$$p(n) := 1^2 + 2^2 + 3^2 + \cdots + n^2$$

auf, und beweise diese mittels vollständiger Induktion.

Hinweis: Setzen Sie unbestimmt $p(n) = an^3 + bn^2 + cn + d$ an, und ermitteln Sie die unbekannten Koeffizienten durch Einsetzen von $n = 1$, $n = 2$, usw. .

2.16 Man stelle eine Formel für ($n \in \mathbb{N}$)

$$p(n) := \sum_{k=1}^{n} (2k-1)^2 = 1^2 + 3^2 + \cdots + (2n-1)^2$$

auf, und beweise diese mittels vollständiger Induktion.

Hinweis: Setzen Sie unbestimmt $p(n) = an^3 + bn^2 + cn + d$ an, und ermitteln Sie die unbekannten Koeffizienten durch Einsetzen von $n = 1$, $n = 2$, usw. .

2.17 Zeige mittels vollständiger Induktion, dass für $n \in \mathbb{N},\ n \geq 2$,

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

2.18 Zeige mittels vollständiger Induktion, dass für $n \in \mathbb{N}$,

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

2.19 Zeige mittels vollständiger Induktion, dass für $n \in \mathbb{N},\ n \geq 2$,

$$\prod_{k=1}^{n} \left(1 + \frac{1}{n+k}\right) = 2 - \frac{1}{n+1}\,.$$

2.20 Zeige mittels vollständiger Induktion, dass für $n \in \mathbb{N},\ n \geq 2$,

$$\prod_{k=2}^{n} \left(1 - \frac{2}{k(k+1)}\right) = \frac{1}{3}(1 + \frac{2}{n})\,.$$

2.21 Zeige mittels vollständiger Induktion:

(a) $2^n > n$ für $n \in \mathbb{N}$ und $2^n > n^2$ für $n \in \mathbb{N}, n \geq 5$.

(b) Für ein beliebiges $x \geq 2$ aus einem angeordneten Körper, folgere man $x^n > n$ für $n \in \mathbb{N}$ und $x^n > n^2$ für alle $n \in \mathbb{N}, n \geq 5$.

2.22 Zeige mittels vollständiger Induktion: Für beliebige Elemente a, b aus einem Körper und $n \in \mathbb{N}$ gilt

$$b^{n+1} - a^{n+1} = (b-a) \sum_{j=0}^{n} a^j b^{n-j}\,.$$

Leite daraus für $x \neq 1$ die Formel

$$\sum_{k=0}^{n} x^k = \frac{1 - x^{n+1}}{1 - x}, \quad n \in \mathbb{N}\,.$$

her.

2.23 Die Zahlen $a_n \in \mathbb{N}$ ($n \in \mathbb{N}$) sind rekursiv definiert durch

$$a_1 = 1,\ a_{n+1} = a_1 + a_2 + \ldots + a_n\,.$$

Zeige, dass $a_n = 2^{n-2}$ für $n \geq 3$.

Anmerkung: Die Existenz dieser Zahlen a_n folgt aus dem Rekursionssatz, wenn für A die Menge $\cup_{k\in\mathbb{N}} \mathbb{N}^k$, also die Menge aller endlichen geordneten Tupel, für a das Element $1 \in \mathbb{N} \subseteq A$ gewählt, und g durch $g((b_1, \ldots, b_k)) := (b_1, \ldots, b_k, \sum_{j=1}^{k} b_j)$ definiert wird. Die gesuchten Zahlen a_n sind dann genau die letzten Einträge von $\phi(n)$.

2.24 Eine Zahl $p \in \mathbb{N},\ p > 1$, heißt Primzahl, wenn aus $m \cdot n = p$ für $m, n \in \mathbb{N}$ folgt, dass $n = 1$ oder $m = 1$.

Sei $A(n),\ n \in \mathbb{N},\ n \geq 2$, die Aussage:

Es gibt endlich viele (nicht notwendigerweise verschiedene) Primzahlen $p_1, \ldots, p_m$, sodass

$$n = \prod_{j=1}^{m} p_j \,.$$

Beweise diese Aussage mit Hilfe einer im Skriptum angegebenen Variante der vollständigen Induktion.

2.25 Für $n \in \mathbb{N}$ und $k \in \{0, \ldots, n\}$, sei der *Binomialkoeffizient* $\binom{n}{k}$ durch $\binom{n}{0} = 1$ und durch

$$\binom{n}{k} = \frac{n}{1} \cdot \frac{n-1}{2} \cdot \ldots \cdot \frac{n-k+1}{k} = \frac{n!}{k!(n-k)!} \quad \text{für } n \geq k \geq 1$$

definiert, wobei $n!$ durch $0! = 1,\ 1! = 1$ und $(n+1)! = n!(n+1)$ induktiv definiert ist. Zeige, dass für $n \geq k \geq 1$

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Weiters beweise den Binomischen Lehrsatz mittels vollständiger Induktion:

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

wobei a, b Elemente aus einem beliebigen Körper sind.

Anmerkung: Ist $k \in \mathbb{Z} \setminus \{0, \ldots, n\}$, so definiere $\binom{n}{k} := 0$. Dann gilt die Gleichung $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ für alle $n \in \mathbb{N},\ k \in \mathbb{Z}$.

2.26 Sei $p, q \in \mathbb{Z}$ mit $p \leq q$. Zeige, dass $\{r \in \mathbb{Z} : p \leq r \leq q\}$ eine endliche Teilmenge von $\mathbb{Z}$ ist. Dabei ist die Definition 2.3.15 zu verwenden.

2.27 Beweisen Sie, dass für ein endliches M das $k \in \mathbb{N}$, sodass es ein bijektives $f : M \to \{n \in \mathbb{N} : n \leq k\}$ gibt, eindeutig ist; vgl. Definition 2.3.15.

Hinweis: Zeigen Sie zuerst, dass es reicht zu zeigen, dass es für natürliche $k_1 > k_2$ keine injektive Funktion g von $\{n \in \mathbb{N} : n \leq k_1\}$ nach $\{n \in \mathbb{N} : n \leq k_2\}$ gibt. Beweisen Sie letzteres mit vollständiger Induktion nach k_1.

2.28 Beweisen Sie, dass Teilmengen T endlicher Mengen M wieder endlich sind; vgl. Bemerkung 2.3.16.

Hinweis: Vollständige Induktion nach dem $k \in \mathbb{N}$, sodass es ein bijektives $f : M \to \{n \in \mathbb{N} : n \leq k\}$ gibt.

2.29 Sei $\langle K, +, \cdot \rangle$ ein Körper, und sei $x \in K \setminus \{0\},\ p, q \in \mathbb{Z}$. Zeige mittels vollständiger Induktion für natürliche p, q und/oder mittels Fallunterscheidungen im allgemeinen Fall: $x^{-p} = \frac{1}{x^p},\ x^p x^q = x^{p+q},\ (x^p)^q = x^{pq}$.

2.30 Zeigen Sie, dass für $m < n,\ m, n \in \mathbb{N}$ und $k = 2, \ldots, n$, folgende Ungleichungskette gilt:

$$\frac{1}{m^k}\binom{m}{k} < \frac{1}{n^k}\binom{n}{k} \leq \frac{1}{k!} \leq \frac{1}{2^{k-1}}\,,$$

wobei $\binom{m}{k} := 0$, falls $m < k$.

Weiters beweise man, dass für $k \geq 2,\ k \in \mathbb{N}$,

$$\frac{\binom{2k}{k}}{2^{2k}} = \frac{1 \cdot 3 \ldots (2k-1)}{2 \cdot 4 \ldots (2k)}\,.$$

2.31 Sei $\langle K, +, \cdot, P\rangle$ ein archimedisch angeordneter Körper. Dieser enthält bekanntlich $\mathbb{Q}$ – genauer, eine Kopie der rationalen Zahlen. Ist nun $\mathbb{Q} \subsetneq K$, so zeige man, dass es sogar ein $\eta \in K \setminus \mathbb{Q}$ gibt mit $0 < \eta < 1$.

Weiters zeige man, dass zwischen je zwei $x < y$ aus K ein nicht rationales ξ mit $x < \xi < y$ gibt.

Hinweis: Zeigen Sie die letzte Behauptung zunächst für $x, y \in \mathbb{Q}$.

2.32 Sei $\langle K, +, \cdot, P\rangle$ ein archimedisch angeordneter Körper. Man bestimme das Supremum und Infimum der Menge

$$M = \left\{(-1)^n + \frac{2}{n} : n \in \mathbb{N}\right\}\,.$$

2.33 Sei $\langle K, +, \cdot, P\rangle$ ein archimedisch angeordneter Körper. Man bestimme die Menge aller oberen Schranken und die Menge aller unteren Schranken der Teilmenge

$$M := \{(-1)^n - \frac{(-1)^n}{n} : n \in \mathbb{N}\} \cup [\frac{1}{2}, 1) \subseteq K\,.$$

Hat diese Menge ein Infimum bzw. ein Supremum in K? Falls ja, dann bestimme man diese und überprüfe, ob diese auch Minimum bzw. Maximum von M sind!

2.34 Sei $p(x) = a_k x^k + \cdots + a_0$ ein Polynom mit reellen Koeffizienten a_j, sodass $a_k > 0$. Zeigen Sie, dass es ein $N \in \mathbb{N}$ gibt, sodass $p(n) > 0$ für alle $n \geq N,\ n \in \mathbb{N}$.

Hinweis: Zeigen Sie, dass man $a_k = 1$ annehmen kann, und dass wenn $n > k \max(|a_{k-1}|, \ldots, |a_0|)$ auch $p(n) > 0$ gilt.

2.35 Zeigen Sie für eine Teilmenge M von $\mathbb{R}$ und $x \in \mathbb{R}$, dass $\inf(\{x\} + M) = x + \inf M$ in dem Sinne, dass die linke Seite genau dann existiert, wenn die rechte es tut!

Unter der Annahme, dass $\emptyset \neq M_1, M_2 \subseteq \mathbb{R}$ nach unten beschränkt sind, zeigen Sie weiters, dass $\inf(M_1 + M_2) = \inf M_1 + \inf M_2$

2.36 Betrachte die quadratische Ungleichung ($p, q \in \mathbb{R}$)

$$x^2 + px + q \geq 0\,.$$

Man beweise, dass die Menge aller $x \in \mathbb{R}$, für die diese Ungleichung stimmt, mit $\mathbb{R}$ übereinstimmt, wenn $x^2 + px + q$ keine Nullstellen in $\mathbb{R}$ hat, und sonst gleich $(-\infty, x_1] \cup [x_2, +\infty)$ ist, wobei

$x_1 = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q},\ x_2 = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q}.$

Wie schauen die Lösungsmengen für die Ungleichungen $x^2 + px + q > 0$, $x^2 + px + q \leq 0$, $x^2 + px + q < 0$ aus?

Hinweis: Man beachte $x^2 + px + q = (x + \frac{p}{2})^2 + q - \frac{p^2}{4}$ und verwende die Tatsache, dass $x \mapsto x^2$ die Menge $\mathbb{R}^+ \cup \{0\}$ bijektiv auf $\mathbb{R}^+ \cup \{0\}$ abbildet.

2.37 Man bestimme die Menge aller $x \in \mathbb{R}$, sodass $6|x| + (1 - 3x)^2 \leq 37$.

2.38 Man rechne nach,

(*i*) dass $1 + i0$ das multiplikativ neutrale Element von $\mathbb{C}$ ist.

(*ii*) dass für $z \in \mathbb{C} \setminus \{0\}$ tatsächlich $w := \frac{\bar{z}}{|z|^2}$ das multiplikativ Inverse Element zu z ist, dass also $wz = 1 + 0i$ gilt.

(*iii*) dass $|zw| = |z||w|$, $|z + w| \leq |z| + |w|$ für $z, w \in \mathbb{C}$.

2.39 Man berechne: $\frac{3+i9}{-2-i3}$, $(-1 + i2)^{-2}$, $(1 + i)^2$, $\sum_{j=0}^{17} i^j$.

2.40 Sei $z = a + ib \in \mathbb{C}$. Man zeige mit den Mitteln der Vorlesung (also ohne Polarkoordinaten), dass z Quadratwurzeln hat, dass es also ein $w \in \mathbb{C}$ gibt, sodass $w^2 = z$. Wie viele Lösungen gibt es? Man berechne damit alle Quadratwurzeln von i und von $3 - i2$.

Hinweis: Man setze $w = c + id$ unbestimmt an und löse die gewünschte Gleichung.

2.41 Man betrachte die Intervalle $I_n := \left(-\frac{1}{n}, \frac{1}{n}\right) \subseteq \mathbb{R}$ und bestimme $\cap_{n\in\mathbb{N}} I_n$.

Weiters sei $B_n := \{z \in \mathbb{C} : \mathrm{Re}(z) + \mathrm{Im}(z) \in I_n\}$. Man bestimme $B = \cap_{n\in\mathbb{N}} B_n$ und skizziere die Lage von B und B_n in der Zahlenebene.