Kapitel 4

Die rationalen Zahlen

Wir haben gesehen, dass eine Gleichung $a \cdot x = b$ mit $a, b \in \mathbb{Z}$ genau dann eine Lösung $x \in \mathbb{Z}$ besitzt, wenn $a \mid b$. Zum Beispiel hat $2 \cdot x = 1$ keine Lösung $x \in \mathbb{Z}$. Wir wollen nun den Zahlbereich $\mathbb{Z}$ zum Zahlbereich $\mathbb{Q}$ der rationalen Zahlen erweitern, indem wir ein minimales System konstruieren, in dem jede Gleichung $a \cdot x = b$ mit $a, b \in \mathbb{Z}$, $a \neq 0$, eine Lösung hat.

4.1 Konstruktion und Arithmetik

Lemma 4.1. *Auf* $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ *wird durch*

$$(m, n) \sim (j, k) :\iff mk = nj$$

eine Äquivalenzrelation definiert.

Beweis. Übung $\square$

Definition 4.2. Die Menge $\mathbb{Q}$ der rationalen Zahlen ist definiert durch

$$\mathbb{Q} := \big(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\big)/\!\sim\ \equiv \big\{[(m, n)]; (m, n) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\big\},$$

wobei $\sim$ wie in Lemma 4.1 definiert ist.

Wir führen jetzt auf $\mathbb{Z}$ eine Addition $\oplus$ und eine Multiplikation $\odot$ ein durch

$$[(j, k)] \oplus [(m, n)] := [(jn + km, kn)],$$
$$[(j, k)] \odot [(m, n)] := [(jm, kn)].$$

Lemma 4.3. *Die oben eingeführten Verknüpfungen* $\oplus$ *und* $\odot$ *auf* $\mathbb{Q}$ *sind wohldefiniert, d. h. sie sind unabhängig von der Wahl der Repräsentanten.*

Bevor wir die algebraische Struktur von $\mathbb{Q}$ untersuchen, führen wir die notwendigen Begriffe aus der Algebra ein.

Definition 4.4. Ein Tripel $(K, +, \cdot)$ heißt *Körper*, wenn $(K, +, \cdot)$ ein kommutativer, unitärer Ring ist und wenn zu jedem $a \in K$, $a \neq 0$, ein $a^{-1} \in K$ mit $aa^{-1} = 1$ existiert.

$(K;+)$ und $(K \setminus \{0\},\cdot)$ sind also zwei abelsche Gruppen, die durch das Distributivgesetz miteinander verbunden sind.

Satz 4.5. $(\mathbb{Q},\oplus,\odot)$ *ist ein Körper mit Nullelement* $[(0,1)]$ *und die inversen Elemente bezüglich der Addition sind gegeben durch* $-[(m,n)] = [(-m,n)]$. *Das Einselement ist* $[(1,1)]$ *und die inversen Elemente bezüglich der Multiplikation sind* $[(m,n)]^{-1} = [(n,m)]$, $[(m,n)] \neq [(0,1)]$. *Als Körper wird* $\mathbb{Q}$ *von* $\widetilde{\mathbb{Z}} := \big\{[(n,1)]; n \in \mathbb{Z}\big\}$ *erzeugt, d. h. ist* K *ein Körper mit* $\widetilde{\mathbb{Z}} \subset K \subset \mathbb{Q}$, *dann ist* $K = \mathbb{Q}$.

Bemerkung 4.6. Natürlich gelten alle Rechenregeln für Ringe insbesondere für Körper, also auch für $\mathbb{Q}$.

Einbettung von $\mathbb{Z}$ in $\mathbb{Q}$.

Lemma 4.7. *Die Abbildung* $\Phi\colon \mathbb{Z} \to \mathbb{Q}$, $n \mapsto [(n,1)]$ *ist injektiv und erfüllt für alle* $m,n \in \mathbb{Z}$

(i) $\Phi(m+n) = \Phi(m) \oplus \Phi(n)$,

(ii) $\Phi(m \cdot n) = \Phi(m) \odot \Phi(n)$.

Beweis. Übung □

Bemerkung 4.8. a) $\Phi\colon \mathbb{Z} \to \mathbb{Q}$ aus Lemma 4.7 ist ein injektiver Ringhomomorphismus (vgl. Definition 3.4). Wir identifizieren deshalb wieder $\Phi(\mathbb{Z}) = \widetilde{\mathbb{Z}}$ mit $\mathbb{Z}$ und schreiben $\mathbb{Z} \subset \mathbb{Q}$. Damit fassen wir $\mathbb{Z}$ als Teilring (Unterring) von $\mathbb{Q}$ auf. Deshalb verwenden wir im Folgenden auch $+$ und $\cdot$ anstelle von $\oplus$ bzw. $\odot$. Mit der Identifikation $\mathbb{Z} = \widetilde{\mathbb{Z}}$ wird $\mathbb{Q}$ von $\mathbb{Z}$ erzeugt, d. h. $\mathbb{Q}$ ist der kleinste Körper, der $\mathbb{Z}$ enthält.

b) Wie in der „Bruchrechnung“ üblich schreiben wir

$$\frac{m}{n} := [(m,n)] \quad (m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}).$$

Mit dieser Schreibweise hat der Ringhomomorphismus Φ die vertrautere Form

$$\Phi\colon \mathbb{Z} \to \mathbb{Q},\ n \mapsto \frac{n}{1}.$$

c) Die Äquivalenzklassenstruktur von $\mathbb{Q}$ ist bei der Bruchrechnung noch deutlich zu erkennen und wird auch beim täglichen Rechnen immer wieder benutzt. So gilt nach Definition von $\sim$ (vgl. Lemma 4.1)

$$(m,n) \sim (km,kn) \ \text{ bzw. } \ [(m,n)] = [(km,kn)] \quad (k \in \mathbb{Z} \setminus \{0\}).$$

In der Bruchschreibweise bedeutet das

$$\frac{m}{n} = \frac{km}{kn}.$$

Den Übergang von links nach rechts bezeichnet man als *Erweitern* eines Bruchs, die umgekehrte Richtung als *Kürzen*. Erweitern und Kürzen sind also keine Rechenoperationen wie $+$ oder $\cdot$, sondern ein Wechsel des Repräsentanten für ein und dieselbe

Äquivalenzklasse.

d) Auch die Funktion Φ wird beim Bruchrechnen regelmäßig benötigt. Will man z. B. $2 + \frac{2}{3}$ berechnen, so muss man die ganze Zahl 2 erst in einen Bruch „verwandeln“, d. h. man wendet auf $2 \in \mathbb{Z}$ die Funktion Φ an und rechnet dann nach Definition der Addition auf $\mathbb{Q}$

$$\Phi(2) + \frac{2}{3} = \frac{2}{1} + \frac{2}{3} = \frac{2 \cdot 3 + 2 \cdot 1}{1 \cdot 3} = \frac{8}{3}.$$

Ebenso wendet man in der Gleichung

$$\frac{2}{3} + \frac{1}{3} = \frac{3}{3} = \frac{1}{1}$$

auf die rechte Seite die Funktion Φ^{-1} an und erhält das übliche Ergebnis $\frac{2}{3} + \frac{1}{3} = 1$.

Bemerkung 4.9. Es gilt

$$\frac{m}{n} = \frac{m}{1} \cdot \frac{1}{n} = \frac{m}{1} \cdot \left(\frac{n}{1}\right)^{-1} = \Phi(n) \cdot \Phi(m)^{-1} = m \cdot n^{-1} \quad \left(\frac{m}{n} \in \mathbb{Q}\right), \tag{4.1}$$

wobei wir natürlich wieder $\Phi(m)$ und $\Phi(n)$ mit m bzw. n identifiziert haben.

Bei $\frac{m}{n}$ war bisher immer $m \in \mathbb{Z}$, $n \in \mathbb{Z} \setminus \{0\}$. Wir definieren jetzt für beliebige $r, s \in \mathbb{Q}$, $s \neq 0$

$$\frac{r}{s} := rs^{-1}. \tag{4.2}$$

Wegen (4.1) stimmt diese Definition für $r \in \mathbb{Z}$, $s \in \mathbb{Z}\setminus\{0\}$ mit der alten überein. Durch (4.2) sind z. B. Doppelbrüche

$$\frac{\frac{p}{q}}{\frac{r}{s}} = \frac{p}{q} \cdot \left(\frac{r}{s}\right)^{-1} = \frac{p}{q} \cdot \frac{s}{r}$$

für $\frac{p}{q} \in \mathbb{Q}$ und $\frac{r}{s} \in \mathbb{Q} \setminus \{0\}$ definiert.

Auch für die erweiterte Definition (4.2) eines Bruchs gilt

$$\frac{p}{q} = \frac{r}{s} \iff ps = rq \quad (p, q, r, s \in \mathbb{Q}, q \neq 0, s \neq 0),$$

Addition und Multiplikation können nach denselben Regel durchgeführt werden und man darf auch diese Brüche kürzen und erweitern.

In einem Körper kann man die Definition der Potenz (vgl. Definition 3.6) auf ganzzahlige Exponenten erweitern.

Definition 4.10. Für $n \in \mathbb{N}_0$ und $a \in \mathbb{Q}$ sei

$$a^0 := 1,\ a^{n+1} := (a^n)a \quad \text{sowie} \quad a^{-n} := (a^n)^{-1},\ \text{falls } a \neq 0.$$

Folgerung 4.11. *Es gelten die Potenzgesetze für $a, b \in \mathbb{Q} \setminus \{0\}$, $n, m \in \mathbb{Z}$:*

(i) $(a^n) \cdot (a^m) = a^{(n+m)}$,

(ii) $(a^n) \cdot (b^n) = (ab)^n$,

(iii) $(a^n)^m = a^{(nm)}$.

Wir leiten jetzt eine erste Normaldarstellung der rationalen Zahlen her.

Lemma 4.12. *Jedes $a \in \mathbb{Q}$ besitzt eine eindeutige Darstellung*

$$a = \frac{m}{n} = m \cdot n^{-1} \quad \textit{mit} \quad m \in \mathbb{Z},\ n \in \mathbb{N},\ \mathrm{ggT}(m,n) = 1.$$

Beweis. Sei $a = \frac{j}{k}$ mit beliebigen $j, k \in \mathbb{Z}$, $k \neq 0$ und sei $d := \mathrm{ggT}(j,k)$, dann ist $j = xd$, $k = yd$ mit $x, y \in \mathbb{Z}$. Ist $y > 0$ setze $m := x$, $n := y$ und für $y < 0$ setze $m := -x$, $n := -y$. Es folgt

$$\frac{j}{k} = \frac{xd}{yd} = \frac{x}{y} = \frac{m}{n} \tag{4.3}$$

mit $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Sei nun $d' := \mathrm{ggT}(m,n) = \mathrm{ggT}(x,y)$, dann folgt $x = d'x'$, $y = d'y'$ für $x', y' \in \mathbb{Z}$ und $j = x'd'd$, $k = y'd'd$. Damit gilt $(d'd) \mid j$ und $(d'd) \mid k$. Aus $d = \mathrm{ggT}(j,k)$ folgt deshalb $(d'd) \mid d$. Anderseits gilt natürlich $d \mid (d'd)$, d. h. $d'd = d$ bzw. $d' = 1$. Damit sind m und n teilerfremd und (4.3) ist die gesuchte Darstellung.

Um die Eindeutigkeit zu zeigen, betrachten wir zwei Darstellungen $a = \frac{m}{n} = \frac{m'}{n'}$ mit $m, m' \in \mathbb{Z}$, $n, n' \in \mathbb{N}$ und $\mathrm{ggT}(m,n) = \mathrm{ggT}(m',n') = 1$. Wegen $mn' = m'n$ gilt $n \mid mn'$ und wegen $\mathrm{ggT}(m,n) = 1$ erhält man mit Folgerung 3.37 $n \mid n'$. Ebenso zeigt man $n' \mid n$. Es folgt $n = n'$ und damit muss auch $m = m'$ sein. □

Satz 4.13. *Jedes $a \in \mathbb{Q} \setminus \{-1, 0, 1\}$ lässt sich als endliches Produkt von Primzahlpotenzen (mit positiven und negativen Exponenten) darstellen, d. h. es gibt ein $\varepsilon \in \{-1, 1\}$, ein $r \in \mathbb{N}$ sowie $p_0, p_1, \ldots, p_r \in \mathbb{P}$ und $\nu_0, \nu_1, \ldots, \nu_r \in \mathbb{Z} \setminus \{0\}$ mit*

$$a = \varepsilon p_0^{\nu_0} p_1^{\nu_1} \cdots p_r^{\nu_r}.$$

Unter der Zusatzbedingung $p_0 < p_1 < \cdots < p_r$ ist die Darstellung eindeutig.

Beweis. Man hat $a = \frac{j}{k} = j \cdot k^{-1}$ mit $j, k \in \mathbb{Z} \setminus \{0\}$. Die Existenz erhält man aus Folgerung 3.51 und den Potenzgesetzen (Folgerung 4.11).

Zum Beweis der Eindeutigkeit seien zwei Darstellungen von a gegeben

$$a = \varepsilon p_0^{\nu_0} p_1^{\nu_1} \cdots p_r^{\nu_r} = \varepsilon' q_0^{\mu_0} q_1^{\mu_1} \cdots q_s^{\mu_s}$$

mit $\varepsilon, \varepsilon' \in \{-1, 1\}$, $r, s \in \mathbb{N}$ sowie $p_0, \ldots, p_r, q_0, \ldots, q_s \in \mathbb{P}$, $\nu_0, \ldots, \nu_r, \mu_0, \ldots, \mu_s \in \mathbb{Z} \setminus \{0\}$ und $p_0 < p_1 < \cdots < p_r$, $q_0 < q_1 < \cdots < q_s$. Wir setzen

$$m := \varepsilon \prod_{\substack{j=0 \\ \nu_j > 0}}^{r} p_j^{\nu_j}, \quad n := \prod_{\substack{j=0 \\ \nu_j < 0}}^{r} p_j^{-\nu_j}, \qquad m' := \varepsilon' \prod_{\substack{j=0 \\ \mu_j > 0}}^{s} q_j^{\mu_j}, \quad n' := \prod_{\substack{j=0 \\ \mu_j < 0}}^{s} q_j^{-\mu_j}, \tag{4.4}$$

wobei wir leeren Produkten immer den Wert 1 zuweisen. Offensichtlich gilt $m, m' \in \mathbb{Z}$, $n, n' \in \mathbb{N}$ sowie $r = \frac{m}{n} = \frac{m'}{n'}$. Angenommen $d := \mathrm{ggT}(m,n) > 1$, dann besitzt d einen kleinsten Primteiler p. Wegen $p \mid m$ und $p \mid n$ muss p nach Folgerung 3.47b mit einem der p_j aus der Produktdarstellung für m in (4.4) übereinstimmen und ebenso mit einem der p_j in der Darstellung für n. Dies ist ein Widerspruch, da die p_j paarweise verschieden sind. Also gilt $\mathrm{ggT}(m,n) = 1$ und ebenso $\mathrm{ggT}(m',n') = 1$. Nach Lemma 4.12 muss deshalb $m = m'$ und $n = n'$ gelten. Aus der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ (Folgerung 3.51) folgt, dass die beiden Darstellungen für m

$$m = \varepsilon \prod_{\substack{j=0 \\ \nu_j>0}}^{r} p_j^{\nu_j} = \varepsilon' \prod_{\substack{j=10 \\ \mu_j>0}}^{s} q_j^{\mu_j}$$

identisch sind und ebenso sind die Darstellungen für n

$$n = \prod_{\substack{j=0 \\ \nu_j<0}}^{r} p_j^{-\nu_j} = \prod_{\substack{j=0 \\ \mu_j<0}}^{s} q_j^{-\mu_j}$$

identisch. (Das gilt auch im Falle von leeren Produkten.) Damit sind aber auch die beiden Darstellungen für a identisch. □

Satz 4.14. *$\mathbb{Q}$ ist abzählbar unendlich.*

Beweis. Nach Lemma 4.12 gibt es für jedes $a \in \mathbb{Q}$ eindeutig bestimmte $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $\mathrm{ggT}(p,q) = 1$ mit $a = \frac{p}{q}$. Deshalb ist die Abbildung

$$\varphi\colon \mathbb{Q} \to \mathbb{Z} \times \mathbb{N},\ a \mapsto (p,q) \text{ mit } p \in \mathbb{Z},\ q \in \mathbb{N},\ \mathrm{ggT}(p,q) = 1,\ a = \frac{p}{q}$$

injektiv. Nun ist $\mathbb{Z} \times \mathbb{N}$ als kartesisches Produkt zweier abzählbarer Mengen ebenfalls abzählbar (vgl. Satz 2.46b, Folgerung 2.45, Lemma 3.41), d. h. es existiert eine injektive Abbildung $\psi\colon \mathbb{Z} \times \mathbb{N} \to \mathbb{N}_0$. Damit ist $\psi \circ \varphi\colon \mathbb{Q} \to \mathbb{N}_0$ injektiv und $\mathbb{Q}$ ist abzählbar. Wegen $\mathbb{N}_0 \subset \mathbb{Q}$ ist $\mathbb{Q}$ natürlich auch unendlich. □

4.2 Anordnung

Wir definieren jetzt auf $\mathbb{Q}$ eine Kleiner-oder-gleich-Relation $\circledleq$ durch

$$[(j,k)] \circledleq [(m,n)] :\iff jn \le km \quad \text{falls} \quad k,n > 0.$$

Man beachte, dass nach Lemma 4.12 jede rationale Zahl eine Darstellung $\frac{p}{q}$ mit $q > 0$ besitzt.

Lemma 4.15. *a) Die Kleiner-oder-gleich-Relation $\circledleq$ auf $\mathbb{Q}$ ist wohldefiniert, d. h. sie ist unabhängig von der Wahl der Repräsentanten.*

b) Durch $\circledleq$ wird eine totale Ordnung im Sinne von Definition 1.61 auf $\mathbb{Q}$ definiert

Beweis. Übung □

Mittels der Bruchschreibweise kann man die Definition von $\circledleq$ wie folgt verstehen

$$\frac{j}{k} \circledleq \frac{m}{n} \iff \frac{jn}{kn} \circledleq \frac{km}{kn} \iff jn \le km.$$

Man macht also die Brüche gleichnamig und vergleicht die Zähler. Dabei müssen die Nenner natürlich positiv sein.

Bemerkung 4.16. Die zu $\circledleq$ gehörende strenge Ordnung $\circledless$ auf $\mathbb{Q}$ erfüllt wie üblich für alle $a, b \in \mathbb{Q}$ genau eine der drei Beziehungen (vgl. Lemma 1.62(iii))

$$a \circledless b, \quad a = b, \quad b \circledless a.$$

Lemma 4.17. *Die Abbildung $\Phi\colon \mathbb{Z} \to \mathbb{Q}$ aus Lemma 4.7 erfüllt außerdem*

(iii) $m \leq n \iff \Phi(m) \circledleq \Phi(n)$,

(iv) $m < n \iff \Phi(m) \circledless \Phi(n)$.

Wir benutzen deshalb auch hier wieder die vereinfachte Schreibweise $\leq$ und $<$ statt $\circledleq$ und $\circledless$.

Da jeder Körper ein Ring ist kann man die Definition eines angeordneten Ringes und einer archimedischen Anordnung (Definition 3.17) unverändert für Körper übernehmen. Man spricht dann natürlich von einem (archimedisch) angeordneten Körper. Lemma 3.18, Folgerung 3.19 und Lemma3.22 gelten natürlich auch in Körpern. Für den Körper $\mathbb{Q}$ gilt nun

Satz 4.18. $(\mathbb{Q}, <)$ *ist ein archimedisch angeordneter Körper.*

Folgerung 4.19. *Zu jedem $x \in \mathbb{Q}$ existiert genau ein $[x] \in \mathbb{Z}$ mit*

$$[x] \leq x < [x] + 1.$$

Beweis. Eindeutigkeit: Seien $j, k \in \mathbb{Z}$ mit $j \leq x < j + 1$ und $k \leq x < k + 1$. Es folgt $0 \leq x - j < 1$, $-1 < k - x \leq 0$ und nach Addition der Ungleichungen $-1 < k - j < 1$, d. h. $|k - j| < 1$, also $k = j$.

Existenz: Sei $x = \frac{m}{n}$ mit $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Nach dem Euklidischen Algorithmus gilt $m = nk + r$ für $k, r \in \mathbb{Z}$ mit $0 \leq r < n$. Es folgt $nk \leq m < nk + n$, was zu $k \leq \frac{m}{n} = x < k + 1$ äquivalent ist. Damit hat $[x] := k \in \mathbb{Z}$ die geforderten Eigenschaften. □

Man nennt $[x]$ das *größte Ganze* von x und $[\,\cdot\,]$ die Gauss-*Klammer*. Anstelle der Gauss-Klammer $[\,\cdot\,]$ benutzt man auch $\lfloor\,\cdot\,\rfloor$ *(Floor function).*

Die Definition des Betrages auf angeordneten Ringen (Definition3.20) gilt natürlich auch für angeordnete Körper, wobei Lemma 3.21 ebenfalls gültig bleibt. Im Falle von $\mathbb{Q}$ ist dabei die Definition des Betrages mit der auf $\mathbb{Z}$ verträglich, in dem Sinne, dass

$$\Phi(|n|) = |\Phi(n)| \qquad (n \in \mathbb{Z})$$

gilt. Hier steht links der Betrag in $\mathbb{Z}$ und rechts der Betrag in $\mathbb{Q}$.

4.3 Die universelle Eigenschaft

Wir erinnern noch einmal an den Begriff des Ringhomomorphismus aus Definition 3.4. Sind $(R, +, \cdot)$, $(S, +, \cdot)$ zwei Ringe, dann heißt eine Abbildung $\varphi\colon R \to S$ ein Ringhomomorphismus, falls

$$\varphi(a + b) = \varphi(a) + \varphi(b),$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Für jeden Ringhomomorphismus gilt außerdem

$$\varphi(0) = 0,$$
$$\varphi(-a) = -\varphi(a).$$

Sind R, S sogar Körper und ist φ nicht der Nullhomomorphismus ist, d. h. $\varphi \neq 0$, dann hat man weiter

$$\varphi(e_R) = e_S,$$
$$\varphi(a^{-1}) = \big(\varphi(a)\big)^{-1},$$

wobei wir in diesem Abschnitt vorübergehend die Einselemente in abstrakten Ringen oder Körpern mit e, e_R oder ähnlich bezeichnen. Definiert man den *Kern* eines Homomorphismus durch

$$\operatorname{Kern}\varphi := \{a \in R; \varphi(a) = 0\},$$

dann ist φ genau dann injektiv, wenn $\operatorname{Kern}\varphi = \{0\}$. Ein bijektiver Homomorphismus heißt *Isomorphismus*. Existiert zwischen zwei Ringen oder Körpern R, S ein Isomorphismus, so heißen die Ringe bzw. Körper *isomorph* (Schreibweise $R \cong S$). Ein Isomorphismus von $R \to R$ heißt *Automorphismus* von R.

Sei nun $R = \mathbb{Z}$ und S eine beliebiger Ring mit Einselement e, dann ist

$$\varphi\colon \mathbb{Z} \to S,\ n \mapsto ne$$

ein Ringhomomorphismus. Dabei ist (vgl. Definition 3.17)

$$ne := \begin{cases} 0,\ n = 0, \\ \underbrace{e + e + \cdots + e}_{n-mal},\ n \in \mathbb{N}, \\ -(\underbrace{e + e + \cdots + e}_{|n|-mal}),\ n \in -\mathbb{N}. \end{cases}$$

In diesem Abschnitt wollen wir nun zeigen, dass der Körper $\mathbb{Q}$ unter allen denkbaren Körpern eine gewisse Sonderstellung einnimmt. Dazu fassen wir $\mathbb{Z}$ natürlich als Unterring von $\mathbb{Q}$ auf.

Lemma 4.20. *Für jeden Körper K und jeden injektiven Ringhomomorphismus $f : \mathbb{Z} \to K$, existiert ein Ringhomomorphismus*

$$F\colon \mathbb{Q} \to K \quad \textit{mit} \quad F|_{\mathbb{Z}} = f.$$

Dieses F ist eindeutig bestimmt und injektiv.

Beweis. Da f injektiv ist, haben wir $f(n) \neq 0$ für alle $n \in \mathbb{Z} \setminus \{0\}$. Weiter gilt $f(1) = f(1 \cdot 1) = f(1)f(1)$ und nach Multiplikation mit $\big(f(1)\big)^{-1}$ folgt $f(1) = e$.

Wir zeigen jetzt zunächst: Ist $\frac{m}{n} = \frac{m'}{n'}$ für $m, m' \in \mathbb{Z}$, $n, n' \in \mathbb{Z} \setminus \{0\}$, dann ist

$$f(m)\big(f(n)\big)^{-1} = f(m')\big(f(n')\big)^{-1}. \tag{4.5}$$

Wegen $mn' = nm'$ folgt dies aber sofort aus

$$\begin{aligned} f(mn') = f(nm') &\iff f(m)f(n') = f(n)f(m') \\ &\iff f(m)\big(f(n)\big)^{-1} = f(m')\big(f(n')\big)^{-1}. \end{aligned}$$

Existenz von F: Wir definieren nun

$$F\colon \mathbb{Q} \to K,\ a = \frac{m}{n} \mapsto f(m)\big(f(n)\big)^{-1}$$

Wegen (4.5) ist diese Definition unabhängig von der Wahl des Repräsentanten für a, d. h. F ist wohldefiniert. F ist ein Homomorphismus, denn

$$\begin{aligned} F\Big(\frac{m}{n} + \frac{r}{s}\Big) &= F\Big(\frac{ms+nr}{ns}\Big) \\ &= f(ms+nr)\big(f(ns)\big)^{-1} \\ &= \Big(f(m)f(s) + f(n)f(r)\Big)\big(f(n)\big)^{-1}\big(f(s)\big)^{-1} \\ &= f(m)\big(f(n)\big)^{-1} + f(r)\big(f(s)\big)^{-1} \\ &= F\Big(\frac{m}{n}\Big) + F\Big(\frac{r}{s}\Big) \quad \Big(\frac{m}{n}, \frac{r}{s} \in \mathbb{Q}\Big) \end{aligned}$$

und ebenso gilt

$$F\Big(\frac{m}{n} \cdot \frac{r}{s}\Big) = F\Big(\frac{m}{n}\Big)F\Big(\frac{r}{s}\Big) \quad \Big(\frac{m}{n}, \frac{r}{s} \in \mathbb{Q}\Big).$$

Schließlich erfüllt F wie gefordert für $a = \frac{m}{1} \in \mathbb{Z}$

$$F(a) = F\Big(\frac{m}{1}\Big) = f(m)\big(f(1)\big)^{-1} = f(m)e^{-1} = f(m),$$

womit die Existenz gezeigt ist.

Eindeutigkeit von F: Sei $G\colon \mathbb{Q} \to K$ ein weiterer Homomorphismus mit $G|_{\mathbb{Z}} = f$. Wegen $G(k) = f(k) = F(k)$ für alle $k \in \mathbb{Z}$ folgt für beliebiges $a = \frac{m}{n} \in \mathbb{Q}$

$$\begin{aligned} F(a) &= F(mn^{-1}) = F(m)F(n^{-1}) = F(m)\big(F(n)\big)^{-1} \\ &= G(m)\big(G(n)\big)^{-1} = G(m)G(n^{-1}) = G(mn^{-1}) = G(a). \end{aligned}$$

Damit ist auch die Eindeutigkeit von G gezeigt.

Injektivität von F: Dazu wählen wir ein beliebiges $a = \frac{m}{n} \in \mathbb{Q} \setminus \{0\}$. Wegen $m \neq 0$ folgt sofort

$$F(a) = F\Big(\frac{m}{n}\Big) = f(m)\big(f(n)\big)^{-1} \neq 0,$$

da $f(m) \neq 0$, $f(n) \neq 0$ und K nullteilerfrei ist. $\square$

Als eine einfache Folgerung formulieren wir zunächst

Folgerung 4.21. *Ist $F\colon \mathbb{Q} \to \mathbb{Q}$ ein Ringhomomorphismus mit $F(n) = n$ für $n \in \mathbb{Z}$, dann ist $F = \mathrm{Id}_{\mathbb{Q}}$.*

Beweis. Wir benutzen Lemma 4.20 mit $K = \mathbb{Q}$ und dem injektiven Ringhomomorphismus $f\colon \mathbb{Z} \to \mathbb{Q}$, $n \mapsto n$. Für die Ringhomomorphismen $F\colon \mathbb{Q} \to \mathbb{Q}$ und $\mathrm{Id}_Q\colon \mathbb{Q} \to \mathbb{Q}$ gilt nun $F(n) = \mathrm{Id}_{\mathbb{Q}}(n) = n$ für $n \in \mathbb{Z}$ und damit folgt die Behauptung aus der Eindeutigkeit der Fortsetzung in Lemma 4.20. □

Da der Homomorphismus f in Lemma 4.20 injektiv ist, ist $f(\mathbb{Z})$ ein zu $\mathbb{Z}$ isomorpher Teilring von K. Ebenso ist $F(\mathbb{Q})$ ein zu $\mathbb{Q}$ isomorpher Teilkörper von K. Lemma 4.20 sagt nun aus, dass jeder Körper, der einen zu $\mathbb{Z}$ isomorphen Teilring besitzt auch einen zu $\mathbb{Q}$ isomorphen Teilkörper besitzt. Identifiziert man wie üblich isomorphe Strukturen, dann kann man vereinfacht sagen, dass jeder Körper der $\mathbb{Z}$ enthält, auch $\mathbb{Q}$ enthält.

Wir wollen nun zeigen, dass $\mathbb{Q}$ der einzige Körper mit dieser Eigenschaft ist. Dazu ersetzen wir $\mathbb{Q}$ durch einen beliebigen Körper K_0. Die Aussage von Lemma 4.20 geht dann über in

$$(4.6)\quad \left\{\begin{array}{l}\text{Für jeden Körper } K \text{ und jeden injektiven Ringhomomorphismus } f\colon \mathbb{Z} \to K \\ \text{exitiert ein Ringhomomorphismus} \\ \qquad\qquad F\colon K_0 \to K \text{ mit } F(ne_0) = f(n) \quad (n \in \mathbb{Z}).\end{array}\right.$$

Damit können wir die angekündigten Sonderstellung von $\mathbb{Q}$ wie folgt formulieren.

Satz 4.22 (Satz von der universellen Eigenschaft)**.** *Sei K_0 ein Körper mit der Eigenschaft* (4.6)*, dann ist K_0 isomorph zu $\mathbb{Q}$.*

In Verbindung mit Lemma 4.20 haben wir damit

$$K_0 \text{ erfüllt (4.6)} \iff K_0 \text{ isomorph zu } \mathbb{Q}$$

und wenn wir wie üblich isomorphe Körper identifizieren, dann können wir sogar sagen

$$K_0 = \mathbb{Q} \text{ ist der einzigen Körper, der (4.6) erfüllt.}$$

Beweis von Satz 4.22. Wählt man in (4.6) $K = \mathbb{Q}$ und als injektiven Ringhomomorphismus $f\colon \mathbb{Z} \to \mathbb{Q}$, $n \mapsto n$, die Inklusion, so existiert nach Voraussetzung ein Ringhomomorphismus

$$F\colon K_0 \to \mathbb{Q} \text{ mit } F(ne_0) = f(n) = n \quad (n \in \mathbb{Z}).$$

Wir wollen zeigen, dass F bijektiv ist.

Injektivität: Wegen $F(e_0) = 1$ gilt für beliebiges $a \in K_0$

$$1 = F(e_0) = F(aa^{-1}) = F(a)F(a^{-1}).$$

Es folgt $F(a) \neq 0$ und damit $\mathrm{Kern}\, F = \{0\}$, d. h. F ist injektiv.

Surjektivität: Dazu betrachten wir den Ringhomomorphismus $g\colon \mathbb{Z} \to K_0$, $n \mapsto ne_0$. Die Funktion g ist injektiv, denn aus $me_0 = ne_0$ folgt

$$m = F(me_0) = F(ne_0) = n.$$

Nach Lemma 4.20 existiert ein Ringhomomorphismus

$$G : \mathbb{Q} \to K_0 \text{ mit } G(n) = ne_0 \quad (n \in \mathbb{Z}).$$

Also ist $F \circ G \colon \mathbb{Q} \to \mathbb{Q}$ ein Ringhomomorphismus mit $F \circ G(n) = n$ für alle $n \in \mathbb{Z}$ und nach Folgerung 4.21 folgt $F \circ G = \mathrm{Id}_{\mathbb{Q}}$. Mit Lemma 1.39a folgt nun, dass F surjektiv ist.

Damit haben wir gezeigt, dass der Homomorphismus $F \colon K_0 \to \mathbb{Q}$ sogar ein Isomorphismus ist und somit sind K_0 und $\mathbb{Q}$ isomorph. □

Wir kommen nun zur Charakterisierung von $\mathbb{Q}$ als Primkörper.

Folgerung 4.23. *Sei K ein Körper, so dass die Abbildung*

$$\mathbb{Z} \to K,\ n \mapsto ne,$$

injektiv ist. Dann ist der Primkörper P von K

$$P := \bigcap_{k \,\text{Teilkörper von}\, K} k$$

isomorph zu $\mathbb{Q}$.

Beweis. P ist ein Körper mit $P \supset \{ne; n \in \mathbb{Z}\}$. Nach Voraussetzung ist die Abbildung $f : \mathbb{Z} \to P, n \mapsto ne$ ein injektiver Ringhomomorphismus und nach Lemma 4.20 existiert genau ein injektiver Ringhomomorphismus

$$F \colon \mathbb{Q} \to P \quad \text{mit} \quad F(n) = f(n) = ne \quad (n \in \mathbb{Z}).$$

Damit ist $F(\mathbb{Q})$ ein zu $\mathbb{Q}$ isomorpher Teilkörper von P. Andererseit ist nach Definition P ein Teilkörper von $F(\mathbb{Q})$ und es folgt $P = F(\mathbb{Q})$. □

4.4 Konvergenz

Im Hinblick auf die Konstruktion von $\mathbb{R}$ im nächsten Kapitel beschäftigen wir und jetzt noch mit Folgen und deren Konvergenz. Es sei noch einmal an die Definition einer Folge als Abbildung von $\mathbb{N}_0$ oder $\mathbb{N}$ in eine Menge X erinnert (vgl. Abschnitt 1.4). Im Folgenden ist X immer ein angeordneter Körper K.

Definition 4.24. Sei $a = (a_n)_{n \in \mathbb{N}_0}$ eine Folge in einem angeordneten Körper$(K, <)$.

a) a heißt *konvergent mit Grenzwert* oder *Limes* $\alpha \in K$, wenn es zu jedem $\varepsilon \in K, \varepsilon > 0$, ein $N \in \mathbb{N}_0$ gibt mit $|a_n - \alpha| < \varepsilon$ für alle $n \geq N$. Man schreibt dann $\lim_{n \to \infty} a_n = \alpha$. Eine Folge $(a_n)_{n \in \mathbb{N}_0}$ mit $\lim_{n \to \infty} a_n = 0$ heißt *Nullfolge*.

b) a heißt CAUCHY-*Folge*, wenn es zu jedem $\varepsilon \in K$, $\varepsilon > 0$, ein $N \in \mathbb{N}_0$ gibt mit $|a_n - a_m| < \varepsilon$ für alle $n, m \geq N$.

c) Man nennt a *beschränkt*, wenn es ein $\beta \in K$ gibt mit $|a_n| \leq \beta$ für alle $n \in \mathbb{N}_0$.

d) Die Folge a heißt *monoton wachsend* (bzw. *monoton fallend*), wenn $a_n \leq a_{n+1}$ (bzw. $a_n \geq a_{n+1}$) für alle $n \in \mathbb{N}_0$ gilt.

Wie in der reellen Analysis beweist man das folgend Lemma.

Lemma 4.25. *Für Folgen $a = (a_n)_{n \in \mathbb{N}_0}$, $b = (b_n)_{n \in \mathbb{N}_0}$ in einem angeordneten Körper $(K, <)$ gilt:*

a) *Wenn a konvergent ist, so ist der Grenzwert eindeutig bestimmt.*

b) *Wenn a konvergent ist, so ist a eine* Cauchy-*Folge.*

c) *Wenn a eine* Cauchy-*Folge ist, so ist a beschränkt.*

d) *a besitzt eine monotone Teilfolge.*

e) *Sind a, b* Cauchy-*Folgen, so sind auch $a + b = (a_n + b_n)_{n\in\mathbb{N}_0}$ und $ab = (a_n b_n)_{n\in\mathbb{N}_0}$* Cauchy-*Folgen.*

f) *Ist a eine* Cauchy-*Folge, b einen Nullfolge, so ist ab eine Nullfolge.*

g) *Ist a eine* Cauchy-*Folge und ist $a_n = b_n$ für fast alle $n \in \mathbb{N}_0$ (alle bis auf endlich viele), dann ist b eine* Cauchy-*Folge.*

h) *Ist a konvergent und ist $a_n = b_n$ für fast alle $n \in \mathbb{N}_0$, dann ist b konvergent mit $\lim_{n\to\infty} b_n = \lim_{n\to\infty} a_n$.*

Die Grenzwertsätze über die Summe, das Produkt und den Quotienten konvergenter Folgen beweist man ebenfalls wie in der reellen Analysis.

Satz 4.26. *Sind $a = (a_n)_{n\in\mathbb{N}_0}$, $b = (b_n)_{n\in\mathbb{N}_0}$ konvergente Folgen in einem angeordneten Körper $(K, <)$ mit Grenzwerten α bzw. β und ist $\gamma \in K$, dann gilt:*

a) *$(\gamma a_n)_{n\in\mathbb{N}_0}$ ist konvergent zum Grenzwert γa.*

b) *$(a_n + b_n)_{n\in\mathbb{N}_0}$ ist konvergent zum Grenzwert $\alpha + \beta$.*

c) *$(a_n b_n)_{n\in\mathbb{N}_0}$ ist konvergent zum Grenzwert $\alpha\beta$.*

d) *Ist $\alpha \neq 0$, so ist $a_n \neq 0$ für fast alle $n \in \mathbb{N}_0$ und die Folge $(c_n)_{n\in\mathbb{N}_0}$ mit*

$$c_n := \begin{cases} a_n^{-1}, & \text{falls } a_n \neq 0, \\ 0, & \text{falls } a_n = 0 \end{cases}$$

konvergiert gegen α^{-1}.

Als Nächstes betrachten wir einige spezielle Folgen in $(\mathbb{Q}, <)$.

Satz 4.27. *a)* *$\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ ist eine Nullfolge in $\mathbb{Q}$.*

b) *Für $n \in \mathbb{N}_0$, $x \in \mathbb{Q}$, $x \neq 1$, gilt*

$$\sum_{j=0}^{n} x^j = \frac{x^{n+1} - 1}{x - 1}.$$

c) *Für $x \in \mathbb{Q}$, $|x| < 1$, ist $(x^n)_{n\in\mathbb{N}_0}$ eine Nullfolge und*

$$\lim_{n\to\infty} \sum_{j=0}^{n} x^j = \frac{1}{1 - x}.$$

d) *Für $x \in \mathbb{Q}$, $|x| > 1$, ist $(x^n)_{n\in\mathbb{N}_0}$ nicht beschränkt.*

e) *Ist $a = (a_n)_{n\in\mathbb{N}_0}$ eine* CAUCHY*-Folge in $\mathbb{Q}$, aber keine Nullfolge, dann existieren $\delta \in \mathbb{Q}$, $\delta > 0$ und ein $N \in \mathbb{N}_0$ mit $|a_n| > \delta$ für alle $n \geq N$.*

f) *Seien $a = (a_n)_{n\in\mathbb{N}_0}$, $b = (b_n)_{n\in\mathbb{N}_0}$* CAUCHY*-Folgen in $\mathbb{Q}$ mit $a \neq b$, dann existierte ein $\delta \in \mathbb{Q}$, $\delta > 0$ und ein $N \in \mathbb{N}_0$ mit*

$$a_n + \delta < b_n \quad (n \geq N) \quad \textit{oder} \quad b_n + \delta < a_n \quad (n \geq N).$$

Beweis. a) Sei $\varepsilon \in \mathbb{Q}$, $\varepsilon > 0$. Da $\mathbb{Q}$ archimedisch angeordnet ist, existiert ein $N \in \mathbb{N}_0$ mit $N > \varepsilon^{-1}$. Es gilt deshalb $n \geq N > \varepsilon^{-1}$ für alle $n \geq N$ und nach Lemma 3.18 (vi) wie gefordert $|\frac{1}{n}| = \frac{1}{n} < \varepsilon$ für alle $n \geq N$.

f) Setze $c := a - b$, also $c_n := a_n - b_n$ für alle $n \in \mathbb{N}_0$. Dann ist c eine CAUCHY-Folge in $\mathbb{Q}$, aber keine Nullfolge. Nach Teil e) existiert deshalb ein $\delta \in \mathbb{Q}$, $\delta > 0$ und ein $N_1 \in \mathbb{N}_0$ mit $|c_n| > \delta$ für alle $n \geq N_1$. Weiter existiert zu diesem δ ein $N_2 \in \mathbb{N}_0$ mit $|c_m - c_n| < \delta$ für alle $m, n \geq \mathbb{N}_2$.

Sei nun $N := \max\{N_1, N_2\}$. Wegen $|c_n| > \delta$ für alle $n \geq N$ gilt für jedes derartige n entweder $c_n > \delta$ oder $-c_n > \delta$. wegen der CAUCHY-Eigenschaft muss dann aber sogar

$$c_n > \delta \quad (n \geq N) \quad \text{oder} \quad -c_n > \delta \quad (n \geq N) \tag{4.7}$$

gelten. Denn angenommen es existieren ein $n_0, n_1 \geq N$ mit $c_{n_0} > \delta$ und $-c_{n_1}n > \delta$, dann erhält man wegen

$$\delta > |c_{n_0} - c_{n_1}| = c_{n_0} - c_{n_1} > 2\delta$$

einen Widerspruch. Wegen $c_n = a_n - b_n$ erhält man aus (4.7) die Behauptung. □

Wichtig ist die folgende Definition aus der Algebra.

Definition 4.28. a) Eine Teilmenge I eines Ringes $(R, +, \cdot)$ heißt (zweiseitiges) *Ideal* in R, wenn

(i) $(I, +)$ Untergruppe von $(R, +)$ ist,

(ii) für alle $x \in I$ und $a \in R$ gilt $xa \in I$ und $ax \in I$.

b) Ein Ideal I in einem Ring R heißt *maximales Ideal*, wenn $I \neq R$ und für jedes Ideal J in R mit $I \subset J$ folgt $I = J$ oder $J = R$.

Bemerkung 4.29. Jedes Ideal in einem Ring R ist ein Teilring von R.

Satz 4.30. *Ist I ein Ideal in einem Ring R, so ist die Quotientenmenge $R/I := \{a + I; a \in R\}$ mit den Verknüpfungen*

$$(a + I) + (b + I) := (a + b) + I, \qquad (a + I) \cdot (b + I) := (a \cdot b) + I$$

wieder ein Ring mit Nullemement $0 + I = I$. Insbesondere sind die Verknüpfungen $+$ und $\cdot$ auf R/I wohldefiniert.

Beweis. Übung. Beim Beweis wird ganz wesentlich benutzt, dass I ein Ideal ist. Für einen beliebigen Teilring J von R anstelle von I sind dir Verknüpfungen im Allgemeinen nicht wohldefiniert. □

Als Vorbereitung auf die Konstruktion von $\mathbb{R}$ im nächsten Kapitel formulieren wir nun

Satz 4.31. *Die Menge $\mathfrak{C}$ aller rationalen* Cauchy-*Folgen ist mit den Verknüpfungen*

$$a + b = (a_n + b_n)_{n\in\mathbb{N}_0} \quad ab = (a_n b_n)_{n\in\mathbb{N}_0} \qquad (a, b \in \mathfrak{C})$$

ein kommutativer Ring mit Nullelement $0 := (0)_{n\in\mathbb{N}_0}$ und Einselement $1 := (1)_{n\in\mathbb{N}_0}$. Die Menge $\mathfrak{C}_0$ aller rationalen Nullfolgen ist ein Ideal in $\mathfrak{C}$.

Beweis. Die Ringeigenschaften von $\mathfrak{C}$ folgen im Wesentlichen aus Lemma 4.25e und die Idealeigenschaften von $\mathfrak{C}_0$ aus Lemma 4.25f. □