1 Zahlen

1.1 Antike — Zahlen und Geometrie

1.1 Bemerkung (Euklidische Geometrie und Konstruktionen)**.** Zahlen nutzt man zum Zählen oder in Form von Längenverhältnissen von Strecken zum Messen. Wir wollen diesen geometrischen Aspekt vorerst näher beleuchten und interessieren uns dafür, wie man Streckenlängen mit Zirkel und Lineal konstruiert und konstruierte Strecken mit einem Zirkel mißt.

Dazu bauen wir die euklidische Geometrie nicht axiomatisch auf, wir beschränken uns darauf zu postulieren was ein ideales Lineal und ein idealer Zirkel ausführen können. Konstruktionen mit Zirkel und Lineal werden uns im weiteren Verlauf der Vorlesung noch mehrmals begegnen.

1.2 Notation. Im Folgenden sei $\mathcal{E}$ die euklidische Ebene (verstanden als Menge von Punkten). Zu zwei Punkten A und B bezeichne $\overline{AB} := \{A, B\}$ die Strecke zwischen A und B, wir schreiben

$$\mathcal{S} := \{\overline{AB} = \{A, B\} \mid A, B \in \mathcal{E}\}$$

für die Menge aller Strecken. Zwei Strecken heißen kongruent (oder gleich lang), falls sie durch eine Kongruenzabbildung der euklidischen Ebene aufeinander abgebildet werden können. Zum Testen der Kongruenz nutzt man einen Zirkel. Wir schreiben $\overline{AB} \simeq \overline{CD}$ dafür, dass zwei Strecken kongruent sind. Kongruenz von Strecken bestimmt eine Äquivalenzrelation auf $\mathcal{S}$, Äquivalenzklassen aus $\mathcal{S}/_{\simeq}$ werden als Streckenlängen bezeichnet.

Postulat (Lineal)**.** Zu zwei verschiedenen Punkten $A, B \in \mathcal{E}$ existiert genau eine Gerade $g = AB$. Diese ist mit dem *Lineal* konstruierbar. Die Menge aller Geraden sei $\mathcal{G}$.

Postulat (Zirkel)**.** Zu zwei verschiedenen Punkten $A, B \in \mathcal{E}$ und einem dritten Punkt M existiert genau ein Kreis $k = K(M, \overline{AB})$ um M mit Radius $\overline{AB}$. Dieser ist mit dem *Zirkel* konstruierbar. Die Menge aller Kreise sei $\mathcal{K}$.

Postulat (Inzidenz)**.** Zu einer konstruierten Geraden $g \in \mathcal{G}$ und einem konstruierten Punkt $A \in \mathcal{E}$ ist stets entscheidbar ob $A \in g$ gilt oder nicht. Ebenso ist entscheidbar, ob für einen konstruierten Kreis $k \in \mathcal{K}$ und einen konstruierten Punkt $A \in \mathcal{E}$ die Beziehung $A \in k$ gilt.

Postulat (Schnittpunkte)**.** Schnittpunkte von schon konstruierten Geraden beziehungsweise Kreisen sind konstruierbar. Dabei ist entscheidbar, ob ein Kreis eine Gerade schneidet.

Postulat (Ordnung)**.** Sei $g \in \mathcal{G}$ Gerade und drei verschiedene Punkten $A, B, C \in g$. Dann ist entscheidbar, welcher der drei Punkte zwischen den beiden anderen liegt.

1.3 Definition. **(i)** Eine Strecke $\overline{AB} \in \mathcal{S}$ heißt durch eine Referenzstrecke $\overline{XY} \in \mathcal{S}$ messbar, falls es Punkte $C_1, \ldots, C_{N-1} \in AB$ zwischen A und B gibt, so dass

$$\overline{AC_1} \simeq \overline{C_iC_{i+1}} \simeq \overline{C_{N-1}B} \simeq \overline{XY}$$

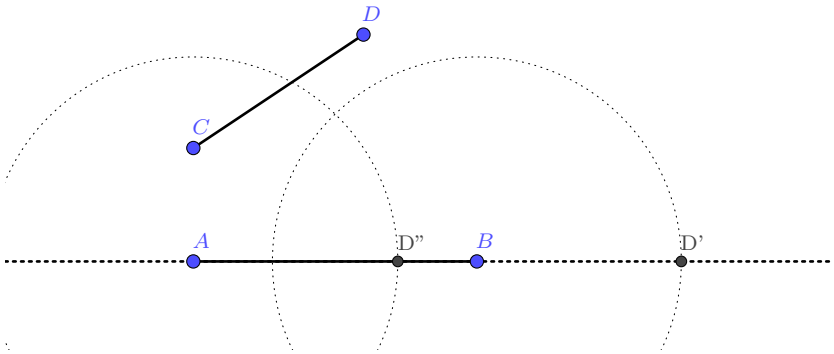
gilt. Wir schreiben dann $[\overline{AB}] = N \times [\overline{XY}]$.

(ii) Strecken, die nicht durch ein gemeinsames Maß messbar sind, heißen inkommensurabel.

1.4 Bemerkung. Im ersten Fall tauchen alle natürlichen Zahlen als Längenverhältnisse auf. Sind zwei Strecken durch ein gemeinsames Maß messbar, so sind ihre Längenverhältnisse rational. In diesem Fall ist das gemeinsame Maß mit Zirkel bestimmbar. Für inkommensurable Strecken bricht die entsprechenden Konstruktion nicht nach endlich vielen Schritten ab.

1.5 Notation. Auf $\mathcal{S}$ kann eine Addition definiert werden. Wir schreiben $\overline{AB} + \overline{CD}$ für die Strecke, die entsteht wenn man auf AB über B hinaus die Strecke $\overline{CD}$ abträgt und damit einen Punkt D' und die neue Strecke $\overline{AD'}$ erhält. Diese Addition ist nicht kommutativ, jedoch wird sie kommutativ in $\mathcal{S}/\simeq$. Übung!

Wir schreiben $\overline{AB} > \overline{CD}$, falls es einen Punkt D'' zwischen A und B mit $\overline{AD''} \simeq \overline{CD}$ gibt. In diesem Fall ist D'' eindeutig bestimmt und wir definieren $\overline{AB} - \overline{CD} := \overline{D''B}$.

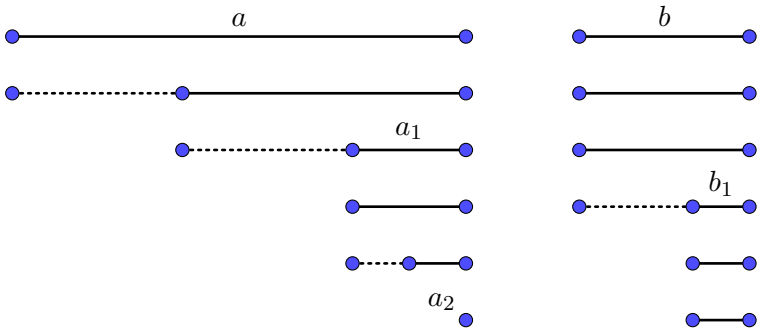


Um die Notation zu vereinfachen, bezeichnen wir Strecken mit Kleinbuchstaben $\boldsymbol{a}, \boldsymbol{b}, \ldots$.

1.6 Algorithmus (Wechselwegnahme, Euklidischer Algorithmus)**.** Gegeben seien zwei Strecken $\boldsymbol{a}_0$ und $\boldsymbol{b}_0$. Führe dann für $j = 0, 1, 2, \ldots$ folgende Schritte aus:

- Gilt $\boldsymbol{a}_j \simeq \boldsymbol{b}_j$, so stoppt der Algorithmus und liefert $\boldsymbol{e} = \boldsymbol{a}_j$ zurück.
- Gilt $\boldsymbol{a}_j > \boldsymbol{b}_j$, so setze $\boldsymbol{a}_{j+1} = \boldsymbol{a}_j - \boldsymbol{b}_j$ und $\boldsymbol{b}_{j+1} = \boldsymbol{b}_j$.
- Gilt $\boldsymbol{b}_j > \boldsymbol{a}_j$, so setze $\boldsymbol{b}_{j+1} = \boldsymbol{b}_j - \boldsymbol{a}_j$ und $\boldsymbol{a}_{j+1} = \boldsymbol{a}_j$.

1.7 Beispiel. Wir betrachten ein einfaches Beispiel und wenden den Algorithmus auf zwei Strecken (der Längen 8 und 3) an. Dabei ergeben sich folgende vier Schritte



und wir erhalten als Resultat die gemeinsame Einheit (mit Länge 1) zurück. Wir notieren uns die Informationen, die der Algorithmus liefert. Es gilt $\boldsymbol{a} > \boldsymbol{b}$. Wir subtrahieren jeweils maximale Vielfache und setzen damit

$$\boldsymbol{a}_1 = \boldsymbol{a} - \boldsymbol{b} - \boldsymbol{b} = \boldsymbol{a} - 2\boldsymbol{b}$$

und

$$\boldsymbol{b}_1 = \boldsymbol{b} - \boldsymbol{a}_1$$

und abschließend $\boldsymbol{a}_2 = \boldsymbol{a}_1 - 2\boldsymbol{b}_1 = 0$. Die jeweils genutzten Vielfachen bezeichnen wir als Teilnenner und notieren uns die Informationen formal als $[2, 1, 2]$. Das Streckenverhältnis ergibt sich zu

$$\boldsymbol{a} : \boldsymbol{b} = [2, 1, 2] = 2 + \frac{1}{1 + \frac{1}{2}} = 2 + \frac{2}{3} = \frac{8}{3},$$

die Begründung für die vorerst formale Rechnung verbleibt als Übungsaufgabe.

1.8 Satz. *Seien $\boldsymbol{a}_0, \boldsymbol{b}_0 \in \mathcal{S}$. Dann sind die folgenden beiden Aussagen äquivalent:*

(i) *Der Algorithmus terminiert für die Startwerte $\boldsymbol{a}_0$ und $\boldsymbol{b}_0$.*

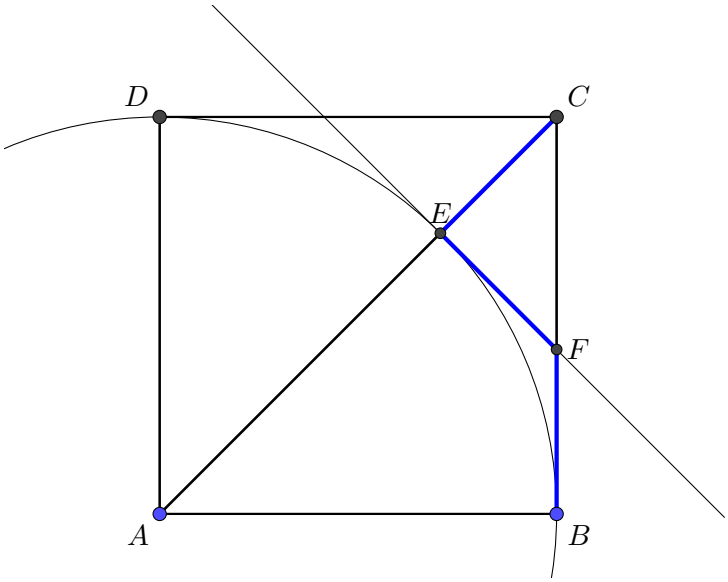
(ii) *Die Strecken $\boldsymbol{a}_0$ und $\boldsymbol{b}_0$ sind durch ein gemeinsames Maß $\boldsymbol{e}$ messbar.*

Beweis. Angenommen der Algorithmus terminiert und liefert nach N Schritten den Rückgabewert $\boldsymbol{e}$. Dann sind $\boldsymbol{a}_N = \boldsymbol{b}_N = \boldsymbol{e}$ durch $\boldsymbol{e}$ messbar. Wir verfolgen den Algorithmus rückwärts. Sind $\boldsymbol{a}_{j+1}$ und $\boldsymbol{b}_{j+1}$ durch $\boldsymbol{e}$ messbar, so ist auch (in Fall 1) $\boldsymbol{b}_j = \boldsymbol{b}_{j+1}$ und $\boldsymbol{a}_j = \boldsymbol{a}_{j+1} + \boldsymbol{b}_j$ durch $\boldsymbol{e}$ messbar beziehungsweise (in Fall 2) $\boldsymbol{a}_j = \boldsymbol{a}_{j+1}$ und $\boldsymbol{b}_j = \boldsymbol{b}_{j+1} + \boldsymbol{a}_j$ durch $\boldsymbol{e}$ messbar. Damit ist aber insbesondere $\boldsymbol{a}_0$ und $\boldsymbol{b}_0$ durch $\boldsymbol{e}$ messbar.

Sind umgekehrt $\boldsymbol{a}_0$ und $\boldsymbol{b}_0$ durch $\boldsymbol{e}$ messbar, so gilt $[\boldsymbol{a}_0] = n \times [\boldsymbol{e}]$ und $[\boldsymbol{b}_0] = m \times [\boldsymbol{e}]$. Nach Konstruktion sind damit auch alle weiteren $\boldsymbol{a}_j$ und $\boldsymbol{b}_j$ durch $\boldsymbol{e}$ messbar. Da sich in jedem Schritt mindestens einer der beiden Faktoren (der jeweils größere) um mindestens Eins verringert, terminiert der Algorithmus nach höchstens $\max(m, n)$ Schritten. □

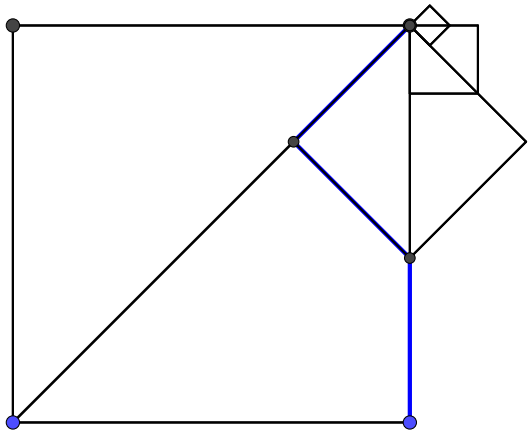
1.9 Satz. *Die Seitenlänge und die Diagonale in einem Quadrat sind inkommensurabel.*

Beweis. Wir zeichnen in einem Quadrat $\square ABCD$ die Diagonale AC und den ihren Schnittpunkt E mit dem Kreis um A durch B. Sei weiter F der Schnittpunkt der Tangente am Kreis in E mit BC.



Dann gilt $\overline{BF} \simeq \overline{EF}$, da die rechtwinkligen Dreiecke $\triangle ABF$ und $\triangle AEF$ in $\overline{EF}$ übereinstimmen und nach Konstruktion $\overline{AB} \simeq \overline{AE}$ gilt und damit kongruent sind. Ebenso gilt $\overline{EF} \simeq \overline{EC}$, da dieses rechtwinklige Dreieck $\angle ECF = \angle EFC = 45°$ erfüllt.

Damit kann aber der Euklidische Algorithmus nicht abbrechen, die Strecken $\overline{AB}$ und $\overline{AC}$ werden nach zwei Schritten zu $\overline{FE}$ und $\overline{FC}$ und wir erhalten eine unendliche Folge kleiner werdender Quadrate in der Konstruktion:



Ablesbar aus der Konstruktion ist die Folge der Teilnenner, formal erhalten wir

$$[1, 2, 2, 2, 2, 2, 2, 2, \ldots].$$

□

1.10 Zusammenfassung.

- Zahlen als Längenverhältnisse sind Eigenschaften geometrischer Figuren, Rechnungen geometrisch konstruierbar
- natürliche Zahlen als Vielfache von Streckenlängen
- rationale Zahlen als Verhältnisse kommensurabler Strecken
- Existenz inkommensurabler Längen entspricht der Existenz irrationaler Zahlen
- Addition, Subtraktion, Multiplikation und Division innerhalb positiver rationaler Zahlen konstruktiv, keine negativen Zahlen

1.2 Axiomatisch - Konstruktiver Aufbau der Zahlensysteme

1.11 Bemerkung. Um Aussagen über Zahlen sauber formulieren und auch beweisen zu können, benötigen wir eine Definition dessen, was Zahlen sind. Die natürlichen Zahlen zusammen mit der Nachfolgerfunktion $\mathfrak{N}$ werden nach Guiseppe Peano durch folgende fünf Axiome charakterisiert.

Axiom. 1 ist eine natürliche Zahl.

Axiom. Jede natürliche Zahl n besitzt einen Nachfolger $\mathfrak{N}(n)$.

Axiom. Sind für natürliche Zahlen m, n ihre Nachfolger gleich (d.h. gilt $\mathfrak{N}(n) = \mathfrak{N}(m)$), so folgt $n = m$.

Axiom. Für alle natürlichen Zahlen n gilt $\mathfrak{N}(n) \neq 1$.

Axiom. Sei $P(n)$ eine Aussageform über natürlichen Zahlen. Gilt dann $P(1)$ und impliziert $P(n)$ stets $P(\mathfrak{N}(n))$, so gilt $P(n)$ für jede natürliche Zahl n.

Die Axiome spiegeln Eigenschaften wider, welche wir für die natürlichen Zahlen kennen. Sie bestimmen auch alle Rechenoperationen auf den natürlichen Zahlen (siehe unten) und erlauben formal aufgeschriebene Beweise. Was sie jedoch nicht erlauben, ist ihre eigene Widerspruchsfreiheit zu beweisen, also zu zeigen, dass mit einer Aussage über natürliche Zahlen nicht auch ihre Negation aus den Axiomen bewiesen werden kann.

1.12 Bemerkung. Im weiteren Verlauf der Vorlesung glauben wir an die Widerspruchsfreiheit der Mengenlehre. Dann kann man ein Modell für die natürlichen Zahlen und (garantiert durch die Axiome der Mengenlehre auch) die Menge der natürlichen Zahlen konstruieren. Das Modell in dieser Form geht auf John von Neumann zurück. Wir setzen dazu

$$\begin{aligned} 1 &:= \{\varnothing\} \\ 2 &:= \{\varnothing, \{\varnothing\}\} = 1 \cup \{1\} \\ 3 &:= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = 2 \cup \{2\} \end{aligned}$$

und definieren allgemein

$$\mathfrak{N}(n) := n \cup \{n\}.$$

Dann sind obige Axiome erfüllt beziehungsweise erfüllbar, wenn wir die so konstruierten Objekte als natürliche Zahlen bezeichnen. Wir nutzen $\mathbb{N}$ als Bezeichnung für die Menge der natürlichen Zahlen, genauer das Unendlichkeitsaxiom der Mengenlehre (nach von Neumann, Paul Bernays und Kurt Gödel) liefert die Existenz einer Menge $\mathcal{U}$ mit

$$\{\varnothing\} \in \mathcal{U} \qquad \text{und} \qquad \forall x \in \mathcal{U} \,:\, x \cup \{x\} \in \mathcal{U}$$

und $\mathbb{N}$ ist der Schnitt über alle Menge $\mathcal{U}$ dieser Form. Im Rahmen der Mengenlehre kann man ausgehend von den natürlichen Zahlen die gebräuchlichen Zahlenbereiche konstruktiv aufbauen.

1.13 Definition (Rechenoperationen auf $\mathbb{N}$)**.** Für festes $n\mathbb{N}$ definiert

$$n + 1 := \mathfrak{N}(n), \qquad n + \mathfrak{N}(m) := \mathfrak{N}(n + m),$$

rekursiv die Addition und entsprechend

$$n \cdot 1 := n, \qquad n \cdot \mathfrak{N}(m) := n \cdot m + n,$$

rekursiv die Multiplikation.

1.14 Satz. ***(i)*** *Für die so definierte Addition $+$ und die Multiplikation $\cdot$ gelten Assoziativ-, Kommutativ- und Distributivgesetz.*

(ii) *Es gelten die Kürzungsregeln*

$$n + m = n' + m \qquad \textit{impliziert} \qquad n = n'$$

und

$$n \cdot m = n' \cdot m \qquad \textit{impliziert} \qquad n = n'$$

für alle natürllichen Zahlen n, n' und m.

1.15 Definition und Satz (Ordnung auf $\mathbb{N}$)**.** Durch

$$m \leq n \quad :\Leftrightarrow \qquad m = n \quad \text{oder} \quad \exists k : m + k = n$$

wird auf $\mathbb{N}$ eine Ordnungsrelation definiert. Diese ist mit Addition und Multiplikation verträglich.

1.16 Definition und Satz (Konstruktion der ganzen Zahlen)**.** **(i)** Auf $\mathbb{N} \times \mathbb{N}$ definiert

$$(m, n) \sim_{\mathbb{Z}} (m', n') \qquad :\Leftrightarrow \qquad m + n' = n + m'$$

eine Äquivalenzrelation.

(ii) Die Âquivalenzklassen dieser Relation heißen ganze Zahlen, $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/_{\sim_{\mathbb{Z}}}$.

(iii) Auf $\mathbb{Z}$ ist durch

$$[(m, n)]_{\sim_{\mathbb{Z}}} + [(m', n')]_{\sim_{\mathbb{Z}}} = [(m + m', n + n')]_{\sim_{\mathbb{Z}}}$$

eine wohldefinierte Addition erklärt. Mit dieser wird $\mathbb{Z}$ zu einer kommutativen Gruppe mit neutralem Element $0 := [(1, 1)]_{\sim_{\mathbb{Z}}}$.

(iv) Für jede Äquivalenzklasse gibt es einen speziellen Vertreter

$$[(m, n)]_{\sim_{\mathbb{Z}}} = \begin{cases} [(1, 1)]_{\sim_{\mathbb{Z}}}, & \text{falls } m = n, \\ [(m', 1)]_{\sim_{\mathbb{Z}}}, & \text{mit } m' + n = m + 1 \text{ falls } m > n, \\ [(1, n')]_{\sim_{\mathbb{Z}}}, & \text{mit } m + n' = n + 1 \text{ falls } n > m. \end{cases}$$

(v) Identifikation $\iota : \mathbb{N} \to \mathbb{Z}$ durch $m := \iota(m) := [(m+1, 1)]_{\sim_{\mathbb{Z}}}$. Es gilt $\iota(m+n) = \iota(m)+\iota(n)$. Weiter vereinbaren wir die Bezeichnung $-n := [(1, n + 1)]_{\sim_{\mathbb{Z}}}$.

(vi) Durch

$$[(m, n)]_{\sim_{\mathbb{Z}}} \leq [(m', n')]_{\sim_{\mathbb{Z}}} \quad :\Leftrightarrow \qquad m + n' \leq m' + n$$

wird auf $\mathbb{Z}$ eine Ordnungsrelation definiert. Diese setzt die Ordnung von $\mathbb{N}$ auf $\mathbb{Z}$ fort und ist wiederum mit den Rechenoperationen (Addition mit ganzen und Multiplikation mit natürlichen Zahlen) verträglich.

(vii) Auf $\mathbb{Z}$ ist durch

$$[(m, n)]_{\sim_{\mathbb{Z}}} \cdot [(m', n')]_{\sim_{\mathbb{Z}}} = [(m \cdot m' + n \cdot n', m \cdot n' + n \cdot m')]_{\sim_{\mathbb{Z}}}$$

eine wohldefinierte Multiplikation definiert. Es gilt $\iota(m \cdot n) = \iota(m) \cdot \iota(n)$. Weiter wird $\mathbb{Z}$ mit dem Einselement $1 = \iota(1)$ zu einem kommutativen Ring.

1.17 Definition und Satz (Konstruktion der rationalen Zahlen)**.** **(i)** Auf $\mathbb{Z} \times \mathbb{N}$ definiert

$$(p, q) \sim_{\mathbb{Q}} (p', q') \qquad :\Leftrightarrow \qquad p \cdot q' = q \cdot p'$$

eine Äquivalenzrelation.

(ii) Die Äquivalenzklassen werden als rationale Zahlen $\mathbb{Q} = (\mathbb{Z} \times \mathbb{N})/_{\sim_{\mathbb{Q}}}$ bezeichnet.

(iii) $\iota : \mathbb{Z} \ni p \mapsto [(p, 1)]_{\sim_{\mathbb{Q}}} \in \mathbb{Q}$ liefert eine Einbettung.

(iv) Wir definieren Rechenoperationen auf $\mathbb{Q}$ durch

$$[(p,q)]_{\sim_{\mathbb{Q}}} + [(p',q')]_{\sim_{\mathbb{Q}}} = [(pq'+qp', qq')]_{\sim_{\mathbb{Q}}}, \qquad [(p,q)]_{\sim_{\mathbb{Q}}} \cdot [(p',q')]_{\sim_{\mathbb{Q}}} = [(pp', qq')]_{\sim_{\mathbb{Q}}}.$$

Diese sind wohldefiniert und mit der Einbettung verträglich. Sie machen $\mathbb{Q}$ zu einem Körper.

(v) Durch

$$[(p,q)]_{\sim_{\mathbb{Q}}} \leq [(p',q')]_{\sim_{\mathbb{Q}}} \quad :\Leftrightarrow \qquad pq' \leq p'q$$

wird auf $\mathbb{Q}$ eine Ordnungsrelation definiert, die $\mathbb{Q}$ zu einem geordneten Körper mit positiven Elementen $(\mathbb{N}\times\mathbb{N})/_{\sim_{\mathbb{Q}}}$ macht.

(vi) Der so entstehende Körper $\mathbb{Q}$ ist archimedisch geordnet, es gilt also

$$\forall r \in \mathbb{Q}\ \exists n \in \mathbb{N}\ :\ r \leq n.$$

1.18 Definition und Satz (Reelle Zahlen)**.** **(i)** Eine Abbildung $a : \mathbb{N} \to \mathbb{Q}$ heißt Folge rationaler Zahlen. Wir schreiben statt $a(n)$ kurz a_n. Zwei Folgen rationaler Zahlen a_n und b_n bilden eine Intervallschachtelung, falls

- für beliebige $m, n \in \mathbb{N}$ stets $a_n < b_m$ gilt;
- für alle $n \in \mathbb{N}$ auch $a_n < a_{n+1}$ und $b_{n+1} < b_n$ gilt;
- und zusätzlich $a_n - b_n \to 0$ gilt, d.h. falls es zu jedem $m \in \mathbb{N}$ ein $n \in \mathbb{N}$ mit $0 < b_n - a_n < \frac{1}{m}$ gibt.

Für eine solche Intervallschachtelung betrachten wir die zugehörigen (rationalen) Intervalle

$$I_n = [a_n, b_n] \cap \mathbb{Q} = \{r \in \mathbb{Q} \mid a_n \leq r \leq b_n\}.$$

(ii) In $\mathbb{Q}$ gibt es Intervallschachtelungen mit $\bigcap I_n = \varnothing$. Dazu betrachte man zum Beispiel

$$a_n = \max\{\frac{p}{q} \mid p \in \mathbb{N},\ q \in \{1,\dots,n\},\ p^2 \leq 2q^2\}$$

und

$$b_n = \min\{\frac{p}{q} \mid p \in \mathbb{N},\ q \in \{1,\dots,n\},\ p^2 \geq 2q^2\},$$

dann gilt $\bigcap I_n = \varnothing$ (da $\sqrt{2} \notin \mathbb{Q}$).

(iii) Die reellen Zahlen $\mathbb{R}$ sind die kleinste geordnete Erweiterung von $\mathbb{Q}$, in der jede Intervallschachtelung I_n nichtleeren Schnitt besitzt. In diesem Fall ist $\bigcap I_n$ stets einelementig.

(iv) Eine Folge a_n heißt Cauchyfolge, falls zu jedem $m \in \mathbb{N}$ ein N_m existiert, so dass für alle $n, n' \geq N_m$ stets $|a_n - a_{n'}| < \frac{1}{m}$ gilt. In $\mathbb{R}$ ist jede Cauchyfolge konvergent. Darüberhinaus folgt aus der Konvergenz aller Cauchyfolgen rationaler Zahlen das Intervallschachtelungsaxiom.

(v) In $\mathbb{R}$ konvergiert jede monotone beschränkte Folge. Umgekehrt folgt aus der Konvergenz jeder monotonen beschränkten Folge das Intervallschachtelungsaxiom.

(vi) Ein Dedekindschnitt von $\mathbb{Q}$ ist eine Zerlegung $\mathbb{Q} = A \cup B$ mit $A, B \neq \varnothing$, $A \cap B = \varnothing$ und $A < B$ (in dem Sinne, dass jedes Element von A kleiner als jedes andere Element aus B ist). Weiter nehmen wir an, dass $\max A$ nicht existiert.

Dedekindschnitte stehen in einer bijektiven Beziehung zu den Elementen von $\mathbb{R}$.

1.3 Der Euklidische Algorithmus

1.19 Definition. **(i)** Für natürliche Zahlen $m, n \in \mathbb{N}$ sagen wir m teilt n, falls es ein $k \in \mathbb{N}$ mit $n = k \cdot m$ gibt.

(ii) Weiter sei zu $m, n \in \mathbb{N}$

$$\mathrm{ggT}(m, n) = \max\{k \in \mathbb{N} \mid k \text{ teilt } m \text{ und } k \text{ teilt } n\}$$

der größte gemeinsame Teiler und

$$\mathrm{kgV}(m, n) = \min\{k \in \mathbb{N} \mid m \text{ teilt } k \text{ und } n \text{ teilt } k\}$$

das kleinste gemeinsame Vielfache.

1.20 Definition und Satz. **(i)** Zu $m, n \in \mathbb{N}$ mit $n \leq m$ gibt es eindeutig bestimmte Zahlen $k \in \mathbb{N}$ und $r \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ mit

$$m = k \cdot n + r, \qquad \text{und} \qquad 0 \leq r < n.$$

(ii) Der ggT zweier Zahlen erfüllt dabei (mit der Zusatzvereinbarung $\mathrm{ggT}(n, 0) = n$)

$$\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r).$$

(iii) Nach endlich vielen Anwendungen der Regel aus **(ii)** entsteht die Situation $\mathrm{ggT}(n, 0)$. Dies entspricht dem Euklidischen Algorithmus.

1.21 Beispiel. **(i)** Es gilt

$$\mathrm{ggT}(288, 60) = \mathrm{ggT}(60, 48) = \mathrm{ggT}(48, 12) = \mathrm{ggT}(12, 0) = 12.$$

(ii) Die Anwendung des Algorithmus ist nicht auf natürliche Zahlen beschränkt. Betrachtet man zum Beispiel Polynome aus $\mathbb{Q}[x]$, also Polynome in einer Variablen mit rationalen Koeffizienten, so ergibt analog die (Polynom-) Division mit Rest zu Polynomen p, q mit $\deg p > \deg q$ eine Zerlegung

$$p(x) = k(x)q(x) + r(x), \qquad \deg r < \deg q$$

und wir können den entsprechenden Algorithmus verwenden, um zum Beispiel

$$\begin{aligned} \mathrm{ggT}(x^3 + 6x^2 + 12x + 16, x^2 + 4x) &= \mathrm{ggT}(2x^2 + 12x + 16, x^2 + 4x) \\ &= \mathrm{ggT}(4x + 16, x^2 + 4x) \\ &= \mathrm{ggT}(4x + 16, 4x^2 + 16x) = x + 4 \end{aligned}$$

zu berechnen. Der größte gemeinsame Teiler ist dabei der gemeinsame Teiler von größtem Grad.

1.4 Kettenbrüche

1.22 Notation. Ein Ausdruck der Form

$$k_1 + \cfrac{1}{k_2 + \cfrac{1}{k_3 + \cfrac{1}{\ddots \cfrac{1}{k_{N-1} + \cfrac{1}{k_N}}}}} = [k_1, k_2, k_3, \ldots, k_{N-1}, k_N]$$

wird als Kettenbruch bezeichnet. Dabei seien für uns vorerst $k_i \in \mathbb{N}$.

1.23 Satz. *Jede rationale Zahl $x \in \mathbb{Q}$ mit $x > 1$ kann durch einen Kettenbruch für ein $N \in \mathbb{N}$ und mit Teilnennern $k_i \in \mathbb{N}$ dargestellt werden.*

Beweis. Sei $x = \frac{m}{n}$ mit $m > n$. Dann kann der Euklidische Algorithmus zur Bestimmung des $\mathrm{ggT}(m, n)$ tabellarisch wie folgt dargestellt werden:

m	$m_2 = n$	$m_3 = n_2$	$\cdots$	$m_{N-1} = n_{N-2}$	$m_N = n_{N-1}$
n	$n_2 = r_1$	$n_3 = r_2$	$\cdots$	$n_{N-1} = r_{N-2}$	$n_N = r_{N-1}$
k_1	k_2	k_3	$\cdots$	k_{N-1}	k_N
r_1	r_2	r_3	$\cdots$	r_{N-1}	0

Dabei wird in jeder Spalte eine Division mit Rest ausgeführt, die Zahlen in der dritten Zeile entsprechen den Teilnennern. Dies ergibt das Rückwärtseinsetzen. Es gilt

$$\frac{m_N}{n_N} = k_N, \qquad \frac{m_{N-1}}{n_{N-1}} = k_{N-1} + \frac{r_{N-1}}{n_{N-1}} = k_{N-1} + \frac{1}{\frac{m_N}{n_N}} = k_{N-1} + \frac{1}{k_N}$$

und rekursiv folgt die Behauptung. □

Notation. Für einen Kettenbruch $[k_1, \ldots, k_N]$ werden die Anfangskettenbrüche $[k_1, \ldots, k_n]$ für $n = 1, \ldots N$ als Näherungsbrüche bezeichnet. Diese spielen eine Rolle für Approximationseigenschaften rationaler Zahlen. Für das Weitere nutzen wir für sie eine Notation. Es sei

$$\frac{p_n}{q_n} = [k_1, \ldots, k_n].$$

Wir betrachten im Weiteren endliche Kettenbrüche und ebenso Näherungsbrüche für unendliche Folgen (k_i) von Teilnennern gleichzeitig.

1.24 Satz. *Seien k_i die Teilnenner eines Kettenbruchs. Dann gilt für*

$$p_1 = k_1, \qquad q_1 = 1, \qquad p_2 = k_2 k_1 + 1, \qquad q_2 = k_2$$

und die rekursiv definierten Zahlen

$$p_{n+1} = k_{n+1} p_n + p_{n-1}, \qquad q_{n+1} = k_{n+1} q_n + q_{n-1}$$

für $n = 1, 2, \ldots, N$ stets

$$\frac{p_n}{q_n} = [k_1, \ldots, k_n].$$

Beweis. Der Beweis folgt durch Induktion. Wir zeigen die Rekursion jedoch allgemeiner für Teilnenner $k_i \in \mathbb{Q}_{>0}$. Induktionsanfang: Es gilt

$$\frac{p_1}{q_1} = k_1, \qquad \frac{p_2}{q_2} = k_1 + \frac{1}{k_2}.$$

Induktionsschritt: Angenommen, für alle Kettenbrüchen mit n rationalen Teilnennern sind die Darstellungen gezeigt. Dann folgt

$$\begin{aligned}\frac{p_{n+1}}{q_{n+1}} = [k_1, \dots, k_n, k_{n+1}] &= [k_1, \dots, k_n + \frac{1}{k_{n+1}}] \\ &= \frac{(k_n + \frac{1}{k_{n+1}})p_{n-1} + p_{n-2}}{(k_n + \frac{1}{k_{n+1}})q_{n-1} + q_{n-2}} \\ &= \frac{p_n + \frac{1}{k_{n+1}}p_{n-1}}{q_n + \frac{1}{k_{n+1}}q_{n-1}} = \frac{k_{n+1}p_n + p_{n-1}}{k_{n+1}q_n + q_{n-1}},\end{aligned}$$

wobei in der zweiten und dritten Zeile jeweils die Induktionsvoraussetzung genutzt wurde. □

1.25 Folgerung. *In Matrixschreibweise gilt*

$$\begin{pmatrix} p_{n+1} & q_{n+1} \\ p_n & q_n \end{pmatrix} = \begin{pmatrix} k_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix}$$

und damit insbesondere

$$\det \begin{pmatrix} p_n & q_n \\ p_{n-1} & q_{n-1} \end{pmatrix} = (-1)^n.$$

Beweis. Die Rekursionsformel in Matrixschreibweise folgt direkt aus Satz 1.24. Die Determinantenformel ergibt sich daraus per Induktion. Für $n = 2$ gilt

$$\det \begin{pmatrix} p_2 & q_2 \\ p_1 & q_1 \end{pmatrix} = \det \begin{pmatrix} k_2k_1 + 1 & k_2 \\ k_1 & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & k_2 \\ 0 & 1 \end{pmatrix} = 1$$

wobei man im vorletzten Schritt das k_1-fache der zweiten Spalte von der ersten subtrahiert hat. Weiter gilt

$$\det \begin{pmatrix} k_{n+1} & 1 \\ 1 & 0 \end{pmatrix} = -1$$

und der Induktionsschritt ist folgt direkt. □

1.26 Folgerung. *Sei $k_i \in \mathbb{N}$ eine Folge von Teilnennern und bezeichne $p_n/q_n = [k_1, k_2, \dots, k_n]$ die durch Rekursion aus Satz 1.24 bestimmte Folge von Näherungsbrüchen. Dann gilt*

(i) $p_nq_{n-1} - q_np_{n-1} = (-1)^n$*;*

(ii) $\mathrm{ggT}(p_n, q_n) = 1$*, die berechneten Näherungsbrüche sind also stets vollständig gekürzt;*

(iii) *die Folgen der (p_n) und (q_n) sind für $n \geq 2$ streng monoton wachsend;*

(iv) *zwei aufeinanderfolgende Näherungsbrüche besitzen den Abstand*

$$\frac{1}{q_n^2} \leq \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_nq_{n-1}} \leq \frac{1}{q_{n-1}^2};$$

(v) *aufeinanderfolgnde Näherungsbrüche sind geschachtelt*

$$\frac{p_1}{q_1} < \cdots < \frac{p_{2n-1}}{q_{2n-1}} < \frac{p_{2n+1}}{q_{2n+1}} < \cdots < \frac{p_{2n}}{q_{2n}} < \frac{p_{2n-2}}{q_{2n-2}} < \frac{p_2}{q_2};$$

(vi) *im Falle einer unendlichen Folge von Teilnennern bilden die Intervalle* $\mathcal{I}_n = [\frac{p_{2n-1}}{q_{2n-1}}, \frac{p_{2n}}{q_{2n}}]$ *eine Intervallschachtelung und bestimmen damit eindeutig eine reelle Zahl* $x = [k_1, k_2, \ldots]$ *mit*

$$\{x\} = \bigcap_{n\in\mathbb{N}} \mathcal{I}_n.$$

Beweis. **(i)** entspricht der Determinante aus Folgerung 1.25. • **(ii)** ist ℓ ein Teiler von p_n und q_n, so liefert die erste Aussage ℓ teilt 1 und somit folgt $k = 1$. • **(iii)** ergibt sich aus den Rekursionsformeln für alle $n \geq 2$

$$p_{n+1} = k_{n+1}p_n + p_{n-1} \geq p_n + p_{n-1} > p_n, \qquad q_{n+1} = k_{n+1}q_n + q_{n-1} \geq q_n + q_{n-1} > q_n$$

zusammen mit $k_{n+1} \geq 1$ und $p_{n-1} \geq 1$ beziehungsweise $q_{n-1} \geq 1$. • **(iv)** folgt wiederum aus der ersten Aussage zusammen mit der Monotonie der Nenner der Näherungsbrüche. • **(v)** ist nachzurechnen. Dazu nutzen wir

$$\frac{p_{2n-1}}{q_{2n-1}} < \frac{p_{2n-2}}{q_{2n-2}} \quad \Leftrightarrow \quad p_{2n-1}q_{2n-2} < q_{2n-1}p_{2n-2}$$

und die rechte Seite ist nach Aussage (i) genau um 1 größer als die linke. Entsprechend gilt

$$\frac{p_{2n-1}}{q_{2n-1}} < \frac{p_{2n}}{q_{2n}} \quad \Leftrightarrow \quad p_{2n-1}q_{2n} < q_{2n-1}p_{2n}$$

und die rechte Seite ist nach Aussage (i) wiederum um 1 größer als die linke. Da die Abstände aufeinanderfolgender Näherungsbrüche nach (iii) streng monoton fällt folgen alle weiteren angegebenen Ungleichungen. • **(vi)** ergibt sich direkt aus (v). □

1.27 Beispiel. Wir betrachten ein Beispiel. Der Kettenbruch mit den Teilnenner $k_i = 1$, also

$$[1, 1, 1, \ldots]$$

liefert als Rekursion $p_1 = q_1 = q_2 = 1$, $p_2 = 2$ und

$$p_{n+1} = p_n + p_{n-1}, \qquad q_{n+1} = q_n + q_{n-1}.$$

Damit handelt es sich aber bei q_n gerade um die n-te Fibonacci-Zahl F_n und entsprechend gilt $p_n = F_{n+1}$. Als Intervallschachtelung erhalten wir also

$$\mathcal{I}_1 = [1, 2], \qquad \mathcal{I}_2 = [\frac{3}{5}, \frac{2}{3}], \qquad \mathcal{I}_3 = [\frac{8}{5}, \frac{13}{8}], \ldots$$

und die dadurch bestimmte Zahl $\{\tau\} = \bigcap_n \mathcal{I}_n = \lim_{n\to\infty} \frac{F_{n+1}}{F_n}$ erfüllt nach Konstruktion die Gleichung

$$\tau = 1 + \frac{1}{\tau},$$

also die quadratische Gleichung $\tau^2 - \tau - 1 = 0$. Diese besitzt die Lösungsmenge $\{\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\}$, da τ aber in $\mathcal{I}_1$ liegen muss, folgt

$$\tau = \frac{1+\sqrt{5}}{2}.$$

Weiter folgt die Abschätzung

$$\left|\frac{F_{n+1}}{F_n} - \frac{1+\sqrt{5}}{2}\right| \leq \frac{1}{F_n F_{n+1}},$$

die ersten der Abschätzungen sind also

$$\left|\frac{3}{2} - \frac{1+\sqrt{5}}{2}\right| \leq \frac{1}{6}, \qquad \left|\frac{5}{3} - \frac{1+\sqrt{5}}{2}\right| \leq \frac{1}{15}, \qquad \left|\frac{8}{5} - \frac{1+\sqrt{5}}{2}\right| \leq \frac{1}{40}, \qquad \dots .$$

Diese Fehlerabschätzungen sind nicht die bestmöglichen. Es gilt

1.28 Folgerung. *Von zwei aufeinanderfolgenden Näherungsbrüchen p/q einer Kettenbruchsdarstellung für x erfüllt mindestens einer*

$$\left|x - \frac{p}{q}\right| \leq \frac{1}{2q^2}.$$

Beweis. Wir zeigen dies indirekt. Angenommen es gilt

$$\left|x - \frac{p_n}{q_n}\right| \geq \frac{1}{2q_n^2} \qquad \text{und} \qquad \left|x - \frac{p_{n+1}}{q_{n+1}}\right| \geq \frac{1}{2q_{n+1}^2}.$$

Dann folgt

$$\begin{aligned}\frac{1}{q_n q_{n+1}} &= \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - x + x - \frac{p_{n+1}}{q_{n+1}}\right| \\ &= \left|\frac{p_n}{q_n} - x\right| + \left|x - \frac{p_{n+1}}{q_{n+1}}\right| \\ &\geq \frac{1}{2}\left(\frac{1}{q_n^2} + \frac{1}{q_{n+1}^2}\right)\end{aligned}$$

da $p_n/q_n - x$ und $x - p_{n+1}/q_{n+1}$ beide gleiches Vorzeichen besitzen. Subtrahiert man nun die linke Seite der Gleichung, so folgt

$$0 \geq \left(\frac{1}{q_n} - \frac{1}{q_{n+1}}\right)^2$$

und damit $q_n = q_{n+1}$ im Widerspruch zur strengen Monotonie der Nennerfolge q_n. □

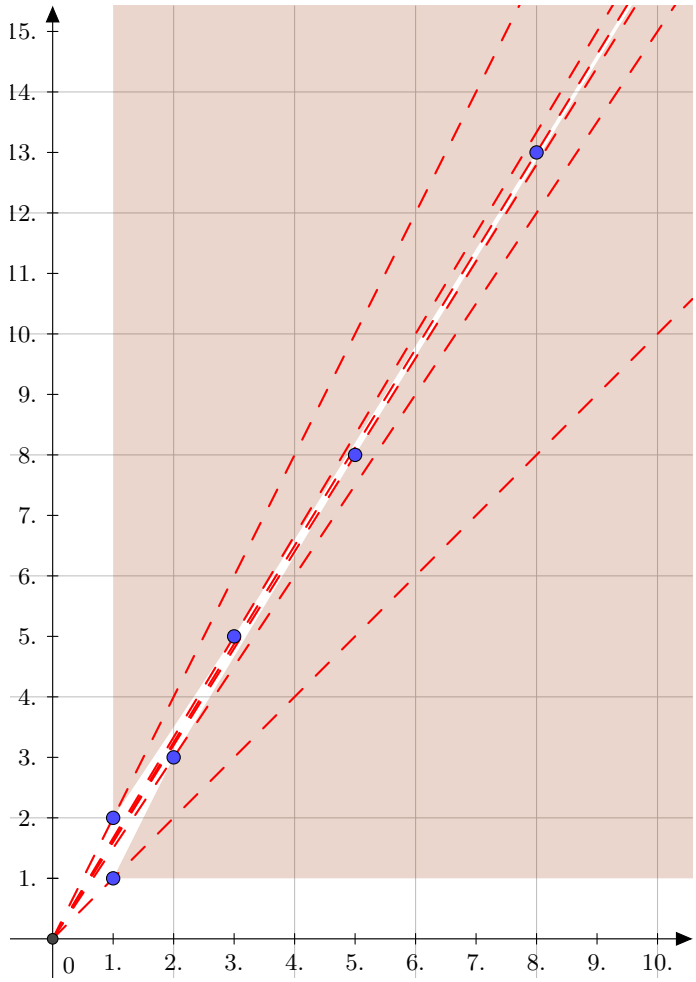
1.29 Satz (Bestapproximationseigenschaft von Kettenbrüchen)**.** *Sei $k_i \in \mathbb{N}$ die Folge von Teilnennern der Kettenbruchsdarstellung einer Zahl $x > 1$ und seien p_n/q_n die zugehörigen Näherungsbrüche. Dann gilt für $n \geq 2$, jedes $p, q \in \mathbb{N}$ mit $1 \leq q \leq q_n$ und $p/q \neq p_n/q_n$*

$$|q_n x - p_n| < |qx - p|$$

sowie

$$\left|x - \frac{p_n}{q_n}\right| > \left|x - \frac{p}{q}\right|.$$

Diese Bestapproximationsaussage kann man sich geometrisch veranschaulichen. Eine Gerade mit irrationalem Anstieg, die also neben dem Ursprung keinen Gitterpunkt mit ganzzahligen Koordinaten trifft, soll durch Geraden mit rationalen Anstiegen approximiert werden. Die unteren / oberen Näherungsbrüche entsprechen nun Gitterpunkten, so dass alle vorherigen Approximationen unterhalb / oberhalb der Geraden durch den Gitterpunkt liegen:



Der Beweis beruht auf zwei Hilfsaussagen, welche wir zuerst zeigen. Es gilt

Hilfsaussage. *Sei* $k'_n := [k_n, k_{n+1}, \ldots]$ *der beim Teilnenner* k_n *startende Rest des Kettenbruchs. Dann gilt*

$$x = \frac{k'_{n+1}p_n + p_{n-1}}{k'_{n+1}q_n + q_{n-1}}, \qquad n \geq 2.$$

Beweis. Wir zeigen dies per Induktion. Es gilt

$$x = k'_1 = k_1 + \frac{1}{k'_2} = k_1 + \frac{1}{k_2 + \frac{1}{k'_3}} = \frac{k_1k_2k'_3 + k_1 + k'_3}{k_2k'_3 + 1} = \frac{k'_3p_2 + p_1}{k'_3q_2 + q_1}$$

unter Ausnutzung von $p_2 = k_2k_1 + 1$, $p_1 = k_1$, $q_2 = k_2$ und $q_1 = 1$. Angenommen, die Aussage

ist schon für ein n gezeigt. Dann folgt

$$x = \frac{k'_{n+1}p_n + p_{n-1}}{k'_{n+1}q_n + q_{n-1}} = \frac{(k_{n+1} + \frac{1}{k'_{n+2}})p_n + p_{n-1}}{(k_{n+1} + \frac{1}{k'_{n+2}})q_n + q_{n-1}}$$
$$= \frac{p_{n+1} + \frac{1}{k'_{n+2}}p_n}{q_{n+1} + \frac{1}{k'_{n+2}}q_n} = \frac{k'_{n+2}p_{n+1} + p_n}{k'_{n+2}q_{n+1} + q_n}$$

unter Ausnutzung der Rekursionsformeln aus Satz 1.24. Nach dem Induktionsprinzip folgt die Behauptung für alle $n \geq 2$. □

Hilfsaussage. *Mit $q'_n = k'_n q_{n-1} + q_{n-2}$ gilt weiterhin für alle $n \geq 3$:*

(i) *(q'_n) ist streng monoton wachsend;*

(ii) *und für alle $n \geq 2$*

$$x - \frac{p_n}{q_n} = \frac{(-1)^{n+1}}{q_n q'_{n+1}}.$$

Insbesondere ist stets

$$\left|x - \frac{p_n}{q_n}\right| < \left|x - \frac{p_{n-1}}{q_{n-1}}\right|, \qquad |q_n x - p_n| < |q_{n-1}x - p_{n-1}|.$$

Beweis. **(i)** folgt aus $k_n < k'_n = k_n + \frac{1}{k'_{n+1}} < k_n + 1$ und den daraus folgenden Abschätzungen

$$q_n = k_n q_{n-1} + q_{n-2} < q'_n < (k_n + 1)q_{n-1} + q_{n-2} = q_n + q_{n-1} \leq k_{n+1}q_n + q_{n-1} = q_{n+1}$$

zusammen mit der Monotonie der Folge (q_n). • **(ii)** Es gilt

$$x - \frac{p_n}{q_n} = \frac{k'_{n+1}p_n + p_{n-1}}{k'_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_n(k'_{n+1}p_n + p_{n-1}) - p_n(k'_{n+1}q_n + q_{n-1})}{q'_{n+1}q_n}$$
$$= \frac{q_n p_{n-1} - p_n q_{n-1}}{q'_{n+1}q_n} = \frac{(-1)^{n+1}}{q_n q'_{n+1}}$$

unter Ausnutzung der ersten Hilfsaussage und der Folgerung 1.25. • Damit ergeben sich beide Ungleichungen: Einerseits gilt

$$\left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n q'_{n+1}} < \frac{1}{q_{n-1}q'_n} = \left|x - \frac{p_{n-1}}{q_{n-1}}\right|,$$

da $q_{n-1}q'_n < q_{n-1}q_{n+1} < q_n q_{n+1} < q_n q'_{n+1}$ mit der Einschließung aus **(i)**. Andererseits gilt

$$|q_n x - p_n| = \frac{1}{q'_{n+1}} < \frac{1}{q'_n} = |q_{n-1}x - p_{n-1}|$$

als Konsequenz der Monotonie der Folge q'_n. □

Beweis zu Satz 1.29. Die erste Ungleichung impliziert die zweite, da damit wegen $p \leq q_n$

$$\left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n}|q_n x - p_n| > \frac{1}{q}|qx - p| = \left|x - \frac{p}{q}\right|$$

gilt. Es genügt also die erste der Ungleichungen zu beweisen.

Wir unterscheiden drei Fälle. Sei dazu $n \geq 2$.

Fall 1: $q = q_n$. In diesem Fall gilt $q'_{n+1} > q_n \geq 2$ und damit

$$|q_n x - p_n| = \frac{1}{q'_{n+1}} < \frac{1}{2}$$

und damit wegen $q = q_n$, $p \neq p_n$, ebenso

$$|qx - p| = |qx - p_n + p_n - p| \geq |p_n - p| - |qx - p_n| \geq 1 - \frac{1}{2} = \frac{1}{2}.$$

Fall 2: $q_{n-1} < q < q_n$. Wir bestimmen zuerst Zahlen μ und ν mit

$$p = \mu p_n + \nu p_{n-1}, \qquad q = \mu q_n + \nu q_{n-1}.$$

Multipliziert man die erste Gleichung mit q_n und die zweite mit p_n, so folgt nach Subtraktion

$$pq_n - qp_n = \nu(q_n p_{n-1} - p_n q_{n-1}) = -\nu(-1)^n$$

und entsprechend bei Multiplikationen mit q_{n-1} beziehungsweise p_{n-1}

$$pq_{n-1} - qp_{n-1} = \mu(p_n q_{n-1} - q_n p_{n-1}) = \mu(-1)^n.$$

Damit sind μ und ν bestimmt, beide ganzzahlig, von Null verschieden und aufgrund von $q_{n-1} < \mu q_n + \nu q_{n-1} < q_n$ besitzen beide unterschiedliches Vorzeichen. Damit folgt

$$\begin{aligned} |qx - p| &= |(\mu q_n + \nu q_{n-1})x - (\mu p_n + \nu p_{n-1})| = |\mu(q_n x - p_n) + \nu(q_{n-1}x - p_{n-1})| \\ &= |\mu|\,|q_n x - p_n| + |\nu|\,|q_{n-1}x - p_{n-1}| \geq |\nu|\,|q_{n-1}x - p_{n-1}| \\ &\geq |q_{n-1}x - p_{n-1}| > |q_n x - p_n| \end{aligned}$$

wobei nun genutzt wurde, dass $\mu(q_n x - p_n)$ und $\nu(q_{n-1}x - p_{n-1})$ gleiches Vorzeichen besitzen, $|\nu| \geq 1$ gilt und nach der zweiten Hilfsaussage $|q_n x - p_n|$ streng monoton fällt.

Fall 3: $q \leq q_{n-1}$. Dann existiert ein $1 \leq m < n$ mit $q_{m-1} < q \leq q_m$ oder es gilt $q = q_1$. Damit folgt aber

$$|qx - p| > |q_m x - p_m| > |q_{m+1}x - p_{m+1}| > \cdots > |q_n x - p_n|$$

wobei im ersten Schritt die Resultate aus Fall 1 und Fall 2 genutzt wurden, in den weiteren Schritten entsprechend die zweite Hilfsaussage. □

1.30 Beispiel. Die Zahl $\sqrt{2}$ besitzt wegen

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + \sqrt{2} - 1}$$

die Kettenbruchsentwicklung

$$\sqrt{2} = [1, 2, 2, 2, \ldots].$$

Wir bestimmen die Folge der Näherungsbrüche. Dazu nutzen wir folgende Tabelle

k_n	1	2	2	2	2	2	2	2	2
p_n	1	3	7	17	41	99	239	$\cdots$	$\cdots$
q_n	1	2	5	12	29	70	169	408	$\cdots$

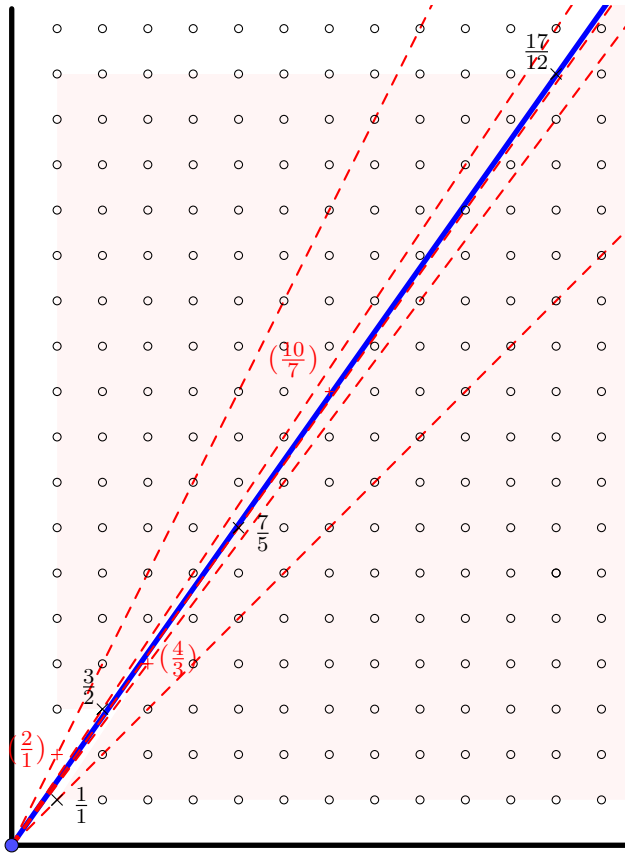
zum bestimmen der Rekursion aus Satz 1.24. Es ergeben sich die Näherungsbrüche

$$1, \quad 1+\frac{1}{2}=\frac{3}{2}, \quad 1+\frac{1}{2+\frac{1}{2}}=\frac{7}{5}, \quad 1+\frac{1}{2+\frac{1}{2+\frac{1}{2}}}=\frac{17}{12}, \quad \frac{41}{29}, \quad \frac{239}{169}, \quad \dots$$

Schreibt man Näherungsbrüche alternativ als $[1,2,\dots,2]=[1,2,\dots,1,1]$, so ergeben sich weitere Näherungen

$$1+\frac{1}{1}=2, \quad 1+\frac{1}{2+\frac{1}{1}}=\frac{4}{3}, \quad 1+\frac{1}{2+\frac{1}{2+\frac{1}{1}}}=\frac{10}{7},$$

welche nicht in der Aussage des Theorems auftreten, die aber ebenso beste Approximationen in dem angegebenen Sinne sind. Die ersten Näherungsbrüche sind in folgendem Bild markiert:



Die Näherungen werden jeweils besser, es gilt also

$$\sqrt{2}-1>\frac{3}{2}-\sqrt{2}>\sqrt{2}-\frac{7}{5}>\frac{17}{12}-\sqrt{2}>\sqrt{2}-\frac{41}{29}>\frac{99}{70}-\sqrt{2}>\sqrt{2}-\frac{239}{169}>\cdots$$

und wir können den Fehler mit den Nennern abschätzen, so gilt

$$\begin{aligned} 0 < \sqrt{2} - \frac{41}{29} &< \frac{1}{29 \cdot 70} = \frac{1}{2030}, \\ 0 < \frac{99}{70} - \sqrt{2} &< \frac{1}{70 \cdot 169} = \frac{1}{11380}, \\ 0 < \sqrt{2} - \frac{239}{169} &< \frac{1}{169 \cdot 408} = \frac{1}{68950} \end{aligned}$$

Die Bestapproximationsaussagen sind ebenso bemerkenswert. So gilt für den letzten angegebenen Näherungsbruch

$$\forall q \in \{1, 2, \ldots, 168\}\ \forall p \in \mathbb{N}: \qquad \sqrt{2} - \frac{239}{169} < \left| \sqrt{2} - \frac{p}{q} \right|.$$

Jede andere rationale Zahl mit kleineren Nennern liegt weiter weg von der zu approximierenden Irrationalzahl!

1.31 Zusammenfassung. **(i)** Jede rationale Zahl $x \in \mathbb{Q}$, $x > 1$, besitzt zwei endliche Kettenbruchsdarstellungen

$$x = [k_1, k_2, \ldots, k_N] = [k_1, k_2, \ldots, k_N - 1, 1]$$

mit Teilnennern $k_i \in \mathbb{N}$ und $k_N \geq 2$. Zum Beispiel gilt $2 = [2] = [1, 1]$.

Umgekehrt entspricht jeder endlichen Kettenbruchsdarstellung eine rationale Zahl $x > 1$.

(ii) Irrationale Zahlen $x \in \mathbb{R} \setminus \mathbb{Q}$, $x > 1$, besitzen eindeutig bestimmte unendliche Kettenbruchsdarstellungen

$$x = [k_1, k_2, k_3, \ldots]$$

mit Teilnennern $k_i \in \mathbb{N}$ (die man entsprechend mit dem Wechselwegnahmeverfahren zur Zahl 1 als Vergleich erhält). Umgekehrt entspricht jedem solchen unendlichen Kettenbruch eine Irrationalzahl. Es besteht also eine Bijektion

$$\{x \in \mathbb{R} \setminus \mathbb{Q} \mid x > 1\} \longleftrightarrow \{(k_n)_{n \in \mathbb{N}} \mid k_n \in \mathbb{N}\} = \mathbb{N}^{\mathbb{N}}.$$

Insbesondere ist damit $\mathbb{R} \setminus \mathbb{Q}$ überabzählbar.

(iii) Näherungsbrüche zu Kettenbrüchen liefern beste rationale Näherungen mit kleinen Nennern. Das kann man einerseits nutzen, Näherungsbrüche zu bestimmen, andererseits sind bekannte rationale Näherungen von Irrationalzahlen oft von dieser Form. Dies gilt zum Beispiel für die Approximationen

$$\frac{22}{7} \qquad \text{und} \qquad \frac{355}{113}$$

der Kreiszahl π. Die erste Näherung ist mindestens seit Archimedes bekannt, die zweite geht auf Zu Chongzhi[1] zurück.

[1] Zu Chongzhi lebte von 429 – 500 und hielt mit dem Näherungsbruch für ca. 800 Jahre den Rekord der genauesten Bestimmung von π.

1.5 Irrationalzahlen und transzendente Zahlen

1.32 Bemerkung. Durch periodische Kettenbrüche dargestellte Zahlen

$$x = [k_1, k_2, \ldots, k_M, k_1, k_2, \ldots, k_M, \ldots] = [\overline{k_1, k_2, \ldots, k_M}]$$

lösen quadratische Gleichungen mit ganzzahligen Koeffizienten. Dies ist recht einfach einzusehen, es gilt

$$x = k_1 + \cfrac{1}{k_2 + \cfrac{1}{\ddots + \cfrac{1}{k_M + \cfrac{1}{x}}}} = \frac{xp_M + p_{M-1}}{xq_M + q_{M-1}}$$

unter Ausnutzung der Darstellung aus Hilfsaussage 1 zum Beweis von Satz 1.29. Also gilt

$$x^2 q_M + x(q_{M-1} - p_M) - p_{M-1} = 0.$$

Es gilt sogar nahezu die Umkehrung dieser Aussage. Lösungen quadratischer Gleichungen mit ganzen Koeffizienten besitzen periodisch endende Kettenbruchsentwicklungen. Das besagt:

1.33 Satz (Lagrange)**.** *Die folgenden beiden Aussagen sind äquivalent.*

(i) $x \in \mathbb{R} \setminus \mathbb{Q}$ *erfüllt*

$$Ax^2 + Bx + C = 0$$

mit ganzen Zahlen $A, B, C \in \mathbb{Z}$*.*

(ii) *Es gilt für geeignete* N *und* M

$$x = [k_1, \ldots, k_{N-1}, \overline{k_N, \ldots, k_{N+M-1}}]$$

mit $k_1 \in \mathbb{Z}$ *und* $k_i \in \mathbb{N}$ *für* $i \geq 1$*.*

Reelle Zahlen, welche die erste der Aussagen erfüllen bezeichnet man auch als quadratische Irrationalzahlen.

Der Beweis benötigt die folgende Hilfsaussage.

Hilfsaussage. *Sei für* $x, y \in \mathbb{R}$ *die Relation* $x \sim y$ *durch*

$$x \sim y \qquad :\Leftrightarrow \qquad \exists a, b, c, d \in \mathbb{Z} : \quad ad - bc \in \{-1, 1\} \quad \textit{und} \quad x = \frac{ay + b}{cy + d}$$

definiert. Dann gilt

(i) $\sim$ *ist Äquivalenzrelation auf* $\mathbb{R}$*;*

(ii) $x \in \mathbb{Q}$ *genau dann, wenn* $x \sim 0$*;*

(iii) $x \sim y$ *für* $x = [k_1, k_2, \ldots]$ *und* $y = [k_2, k_3, \ldots]$*;*

(iv) $x \sim y$ *genau dann, wenn die Kettenbruchsentwicklungen von* x *und* y *bis auf endlich viele Teilnenner übereinstimmen.*

Beweis. **(i)** ist nachzurechnen. Es gilt stets $x \sim x$, da wir $a = d = 1$ und $b = c = 0$ wählen können. Gilt $x \sim y$ und $y \sim z$, so finden wir insbesondere ganze Zahlen $a, b, c, d, \tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in \mathbb{Z}$ mit $ad - bc \in \{\pm 1\}$ und $\tilde{a}\tilde{d} - \tilde{b}\tilde{c} \in \{\pm 1\}$ sowie

$$x = \frac{ay+b}{cy+d} =: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet y, \qquad y = \frac{\tilde{a}z+\tilde{b}}{\tilde{c}z+\tilde{d}} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \bullet z$$

und durch Einsetzen sieht man

$$x = \frac{(a\tilde{a}+b\tilde{c})z + (a\tilde{b}+b\tilde{d})}{(c\tilde{a}+d\tilde{c})z + (c\tilde{b}+d\tilde{d})} = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \right] \bullet z.$$

Die auftretende Matrixmultiplikation garantiert, dass wiederum die Determinante der Matrix ± 1 ist und es folgt $x\tilde{z}$. Damit ergibt sich ebenso die Symmetrie, aus $x \sim y$ ergibt sich

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet y \qquad \text{und damit} \qquad y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \bullet x,$$

also $y \sim x$. • **(ii)** Aus $x \sim 0$ folgt offenbar direkt $x \in \mathbb{Q}$. Ist umgekehrt $x \in \mathbb{Q}$, so gilt $x = b/d$ mit $\mathrm{ggT}(b, d) = 1$. Insbesondere liefert der Euklidische Algorithmus damit Zahlen $a, c \in \mathbb{Z}$ mit $ad - bc = \mathrm{ggT}(b, d) = 1$ und es folgt $x \sim 0$. • **(iii)** folgt direkt aus

$$x = k_1 + \frac{1}{y} = \frac{k_1 y + 1}{y}$$

und damit der Wahl $a = k_1, b = 1, c = 1, d = 0$. • **(iv)** wenn die Kettenbruchsentwicklungen bis auf endlich viele Teilnenner übereinstimmen, so folgt aus **(iii)** die Äquivalenz. Für die Umkehrung verweisen wir auf die Literatur.[2]

□

Beweis von Satz 1.33. ***(ii)** impliziert **(i)**:* Die Zahl $y = [\overline{k_N, \ldots, k_{N+M-1}}]$ ist quadratische Irrationalzahl, es gibt also Koeffizienten $A, B, C \in \mathbb{Z}$, $A \neq 0$, mit $Ay^2 + By + C = 0$. Weiter gibt es aufgrund von $x \sim y$ Zahlen $a, b, c, d \in \mathbb{Z}$ mit $ad - bc \in \{-1, 1\}$ und

$$y = \frac{ax+b}{cx+d}$$

und damit

$$A\left(\frac{ax+b}{cx+d}\right)^2 + B\frac{ax+b}{cx+d} + C = 0.$$

Dies ist nach Ausmultiplizieren aber gerade eine quadratische Gleichung mit ganzzahligen Koeffizienten. • ***(i)** impliziert **(ii)**:* Angenommen, x ist quadratische Irrationalzahl mit Kettenbruchsentwicklung $x = [k_1, k_2, \ldots]$ und Näherungsbrüchen $p_n/q_n = [k_1, \ldots, k_n]$. Dann gilt

$$x = \frac{k'_n p_{n-1} + p_{n-2}}{k'_n q_{n-1} + q_{n-2}}$$

mit $k'_{n+1} = [k_{n+1}, k_{n+2}, \ldots]$. Eingesetzt in die quadratische Gleichung liefert dies

$$0 = Ax^2 + Bx + C = A\left(\frac{k'_n p_{n-1} + p_{n-2}}{k'_n q_{n-1} + q_{n-2}}\right)^2 + B\left(\frac{k'_n p_{n-1} + p_{n-2}}{k'_n q_{n-1} + q_{n-2}}\right) + C$$

[2] Siehe zum Beispiel: G.H. Hardy, E.M. Wright, *Zahlentheorie*, Kapitel 10.11.

und damit nach Ausmultiplizieren

$$A(k'_n p_{n-1} + p_{n-2})^2 + B(k'_n p_{n-1} + p_{n-2})(k'_n q_{n-1} + q_{n-2}) + C(k'_n q_{n-1} + q_{n-2})^2 = 0.$$

Dies ist eine quadratische Gleichung für k'_n,

$$A_n (k'_n)^2 + B_n k'_n + C_n = 0$$

mit Koeffizienten

$$\begin{aligned} A_n &= A p_{n-1}^2 + B p_{n-1} q_{n-1} + C q_{n-1}^2 \in \mathbb{Z} \\ B_n &= 2A p_{n-1} p_{n-2} + B(p_{n-1} q_{n-2} + p_{n-2} q_{n-1}) + 2C q_{n-1} q_{n-2} \in \mathbb{Z} \\ C_n &= A p_{n-2}^2 + B p_{n-2} q_{n-2} + C q_{n-2}^2 = A_{n-1} \in \mathbb{Z} \end{aligned}$$

und nach kurzer Rechnung

$$B_n^2 - 4A_n C_n = (B^2 - 4AC)(p_{n-1} q_{n-2} - p_{n-2} q_{n-1})^2 = B^2 - 4C.$$

Aus der Fehlerabschätzung der Approximationseigenschaft folgt $p_{n-1} = q_{n-1} x + \frac{(-1)^{n-1}}{q'_n}$ und damit nach Einsetzen in die Koeffizientenformel

$$\begin{aligned} A_n &= A x^2 q_{n-1}^2 + 2Ax \frac{(-1)^{n-1}}{q'_n} q_{n-1} + A \frac{1}{(q'_n)^2} + B x q_{n-1}^2 + B \frac{(-1)^{n-1}}{q'_n} q_{n-1} + C q_{n-1}^2 \\ &= 2Ax \frac{(-1)^{n-1}}{q'_n} q_{n-1} + A \frac{1}{(q'_n)^2} + B \frac{(-1)^{n-1}}{q'_n} q_{n-1} \end{aligned}$$

und Anwenden der Ausgangsgleichung für x. Dadurch Ergeben sich Abschätzungen für die Koeffizienten A_n, B_n und C_n durch x und A, B, C in Form von

$$|A_n| \le |2Ax| + |A| + |B|, \qquad |C_n| = |A_{n-1}| \le |2Ax| + |A| + |B|,$$

und

$$|B_n|^2 \le |B^2 - 4AC| + |4A_n C_n| \le |B^2 - 4AC| + 4(|2Ax| + |A| + |B|)^2.$$

Also sind die ganzzahligen Koeffizienten der quadratischen Gleichungen für k'_n gleichmäßig in n beschränkt. Damit gibt es aber nur endlich viele solche Gleichungen und die Menge

$$\{k'_n \mid n \in \mathbb{N}\}$$

ist endlich. Also muss es Zahlen N und M geben mit $k'_N = k'_{N+M}$ und die geforderte Darstellung mit periodischer Teilnennerfolge ist gezeigt. □

1.34 Definition. Wir sagen eine Zahl $x \in \mathbb{R}$ ist zur Ordnung $m \in \mathbb{N}$ approximierbar, falls es eine Zahl $K > 0$ derart gibt, dass unendlich viele Zahlen $p \in \mathbb{Z}$, $q \in \mathbb{N}$ mit $\mathrm{ggT}(p, q) = 1$ und

$$\left| x - \frac{p}{q} \right| < \frac{K}{q^m}$$

existieren. Ist eine Zahl zur Ordnung $m \in \mathbb{N}$ approximierbar aber nicht zur Ordnung $m + 1$, so bezeichnet m die Approximationsordnung der Zahl x. Eine zu jeder Ordnung approximierbare Zahl habe die Approximationsordnung ∞.

1.35 Beispiel. **(i)** Eine Zahl besitzt genau dann die Approximationsordnung 1, wenn sie rational ist.

(ii) Jede irrationale Zahl ist zur Ordnung 2 approximierbar.

(iii) Quadratische Irrationalzahlen besitzen die Approximationsordnung 2.

(iv) Es gibt Zahlen mit Approximationsordnung 2 die keine quadratischen Irrationalzahlen sind.

Beweis. **(i)** Sei $x = a/b$ mit $\mathrm{ggT}(a,b) = 1$. Dann existieren (Euklidischer Algorithmus) unendlich viele Lösungen p, q zu

$$qa - pb = \mathrm{ggT}(a,b) = 1.$$

Diese sind teilerfremd und es gilt

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{1}{bq}.$$

Damit folgt Approximierbarkeit zu erster Ordnung mit der Wahl $K = 1/b$. Angenommen, für $p/q \neq a/b$ und $m \geq 2$ gilt

$$\frac{K}{q^m} \geq \left|\frac{bp - aq}{qb}\right| \geq 1qb,$$

so folgt $Kb \geq q^{m-1}$ und es kann nur endlich viele derartige q geben. Approximierbarkeit höherer Ordnung gilt also nicht. • **(ii)** folgt direkt aus den nicht abbrechenden Kettenbruchsentwicklungen, für Näherungsbrüche gilt

$$\left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n q'_{n+1}} \leq \frac{1}{q_n^2}$$

und davon gibt es unendlich viele. • **(iii)** und **(iv)** Quadratische Irrationalzahlen haben periodisch endende Kettenbrüche. Sei allgemeiner $x = [k_1, k_2, \ldots]$ mit $\{k_n \mid n \in \mathbb{N}\}$ endlich. Dann gilt mit $M = \max_n k_n$ und für alle $q > q_2$ aufgrund der Bestapproximationseigenschaft mit $q_n < q \leq q_{n+1}$

$$\begin{aligned}\left|x - \frac{p}{q}\right| \geq \left|x - \frac{p_{n+1}}{q_{n+1}}\right| = \frac{1}{q_{n+1}q'_{n+2}} &> \frac{1}{(M+2)q_{n+1}^2} \\ &> \frac{1}{(M+2)(M+1)^2 q_n^2} > \frac{1}{(M+2)(M+1)^2 q^2}\end{aligned}$$

wegen $q'_{n+2} = k'_{n+2}q_{n+1} + q_n < (k_{n+2}+1)q_{n+1} + q_{n+1} < (M+2)q_{n+1}$ und $q_{n+1} < (M+1)q_n$. Wäre nun x zur Ordnung 3 approximierbar, so gäbe es unendlich viele p, q mit

$$\frac{K}{q^3} \geq \left|x - \frac{p}{q}\right| \geq \frac{1}{(M+2)(M+1)^2 q^2}.$$

Das kann aber nicht sein, da dies nur endlich viele q erfüllen. □

1.36 Definition. Eine Zahl $x \in \mathbb{R}$ heißt algebraisch der Ordnung $\leq m$, falls es ein Polynom $P(X) \in \mathbb{Z}[X]$ mit ganzzahligen Koeffizienten und vom Grad m mit $P(x) = 0$ gibt. Sie heißt algebraisch der Ordnung m, falls sie darüberhinaus nicht algebraisch der Ordnung $\leq m-1$ ist.

1.37 Satz (Liouville)**.** *Sei $x \in \mathbb{R}$ algebraisch der Ordnung m. Dann ist die Approximationsordnung von x höchstens m.*

Beweis. Sei $P(X) = a_m X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ ein Polynom mit $P(x) = 0$ und minimalem Grad und mit $a_m \neq 0$. Dann ist x einfache Nullstelle, da sonst ebenso $P'(x) = 0$ gelten würde (und dies ein Polynom vom Grad $m-1$ mit ganzzahligen Koeffizienten ist).

Da P' stetig auf $\mathbb{R}$ ist, gibt es damit ein $\delta > 0$ mit $P'(y) \neq 0$ für alle $y \in (x-\delta, x+\delta)$. Ist nun $p/q \in (x-\delta, x+\delta)$ rational, so folgt

$$0 \neq P\left(\frac{p}{q}\right) = \frac{a_m p^m + a_{m-1}p^{m-1}q + \cdots + a_1 pq^{m-1} + a_0 q^m}{q^m}, \qquad \left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^m},$$

und damit auf Grund des Zwischenwertsatzes

$$P\left(\frac{p}{q}\right) = P\left(\frac{p}{q}\right) - P(x) = \left(\frac{p}{q} - x\right) P'(y)$$

für ein y zwischen x und p/q und somit

$$\left|x - \frac{p}{q}\right| \geq \frac{|P(\frac{p}{q})|}{\min_{y\in(x-\delta,x+\delta)} |P'(y)|} \geq \frac{1}{q^m} \frac{1}{\min_{y\in(x-\delta,x+\delta)} |P'(y)|}.$$

Das schliesst aber Approximierbarkeit höherer Ordnung als m aus. □

1.38 Beispiel. Die durch den Kettenbruch

$$x = [10, 10^{2!}, 10^{3!}, \ldots, 10^{k!}, \ldots]$$

dargestellte Zahl ist transzendent.

Beweis. Dazu genügt es Approximierbarkeit zu jeder Ordnung zu zeigen. Wir betrachten die Näherungsbrüche p_n/q_n der Kettenbruchsentwicklung und wenden darauf die Fehlerabschätzung an. Dies liefert wegen $q'_{n+1} = k'_{n+1}q_n + q_{n-1} > k_{n+1}q_n + q_{n-1} > k_{n+1}$, $q_n > 1$ für alle $n \geq 2$

$$\left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n q'_{n+1}} < \frac{1}{k_{n+1}} = \frac{1}{10^{(n+1)!}}.$$

Umgekehrt gilt für q_n wegen $q_1 < k_1 + 1$ und $\frac{q_{n+1}}{q_n} < k_{n+1} + \frac{q_{n-1}}{q_n} < k_{n+1} + 1$ die Abschätzung

$$q_n < \prod_{j=1}^{n}(10^{j!} + 1) < 10^{1!+2!+\cdots+n!} \prod_{j=1}^{n}\left(1 + \frac{1}{10^{j!}}\right) < 10^n 10^{1!+2!+\cdots+n!} < 10^{2(n!)} = (10^{n!})^2$$

und damit folgt

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{10^{(n+1)!}} = \frac{1}{(10^{n!})^{n+1}} < \frac{1}{(10^{n!})^n} < \frac{1}{q_n^{n/2}} < \frac{1}{q_n^{N/2}}$$

für alle $n \geq N$ und beliebiges N. Das ist aber gerade Approximierbarkeit zur Ordnung $\lfloor N/2 \rfloor$ und Transzendenz von x folgt. □

1.6 Die Eulersche Zahl e

1.39 Definition und Satz. **(i)** Die Reihe

$$\sum_{k=0}^{\infty} \frac{1}{k!}$$

konvergiert.

(ii) Der Grenzwert

$$\lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n$$

existiert.

(iii) Beide Grenzwerte stimmen überein und werden als Eulersche Zahl e bezeichnet.

Beweis. **(i)** folgt durch Nachrechnen, die Folge der Partialsummen $s_n = \sum_{k=0}^{n} 1/k!$ ist monoton wachsend und aufgrund von $k! \geq 2^{k-1}$ für $k \geq 1$ durch

$$s_n = 1 + \sum_{k=1}^{n} \frac{1}{k!} < 1 + \sum_{k=1}^{n} \frac{1}{2^{k-1}} = 1 + \frac{1-\frac{1}{2^n}}{1-\frac{1}{2}} = 1 + 2\left(1-\frac{1}{2^n}\right) \leq 3$$

beschränkt. Insbesondere ist damit die Folge der Partialsummen konvergent und der Grenzwert kleiner gleich 3. • **(ii)** ist ebenso monoton wachsend und beschränkt. Dabei folgt Monotonie aus

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

unter Ausnutzung der Bernoullischen Ungleichung in Form von

$$\frac{(n^2-1)^n}{n^{2n}} = \left(1-\frac{1}{n^2}\right)^n \geq 1 - \frac{n}{n^2} = 1 - \frac{1}{n}.$$

Für Beschränktheit nutzen wir einen Vergleich zu obigen Partialsummen, es gilt

$$\left(1+\frac{1}{n}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k} = \sum_{k=0}^{n} \frac{1}{k!} \frac{n\cdot(n-1)\cdots(n-k+1)}{n\cdot n\cdots n} \leq \sum_{k=0}^{n} \frac{1}{k!} = s_n \leq 3.$$

(iii) Wir wissen mit der gerade gezeigten Abschätzung schon, dass

$$\lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n \leq \sum_{k=0}^{\infty} \frac{1}{k!}$$

gilt. Für die umgekehrte Ungleichung fixieren wir m und nutzen

$$\left(1+\frac{1}{n}\right)^n \geq \sum_{k=0}^{m} \binom{n}{k} \frac{1}{n^k} = \sum_{k=0}^{m} \frac{1}{k!} \frac{n\cdot(n-1)\cdots(n-k+1)}{n\cdot n\cdots n},$$

so dass nach Grenzwertbildung für $n \to \infty$ (bei festem m) jetzt

$$\lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n \geq \sum_{k=0}^{m} \frac{1}{k!} = s_m$$

und damit die umgekehrte Ungleichung folgt. □

Die Eulersche Zahl e ist die erste 'interessante' Zahl, für welche Transzendenz bewiesen wurde. Der Vollständigkeit halber geben wir einen Beweis. Er nutzt Mittel der Analysis und insbesondere, dass die Funktion

$$\mathrm{e}^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

sich selbst als Ableitung besitzt.

1.40 Satz (Hermite)**.** *Die Zahl* e *ist transzendent.*

Beweis. Angenommen, e ist algebraisch. Dann gibt es Zahlen $a_0, \ldots, a_m \in \mathbb{Z}$ mit

$$a_0 + a_1\mathrm{e} + a_2\mathrm{e}^2 + \cdots + a_m\mathrm{e}^m = 0.$$

Sei weiter $p > \max(m, |a_0|)$ eine Primzahl. Dann betrachten wir das Polynom

$$P(x) = x^{p-1}(x-1)^p(x-2)^p \cdots (x-m)^p = \sum_{k=p-1}^{(n+1)p-1} b_k x^k.$$

Nach Konstruktion gilt dafür

- für $j = 1, \ldots, p-1$ und $\ell = 1, \ldots, m$ stets $P^{(j)}(\ell) = 0$;
- für $j = 1, \ldots, p-2$ weiterhin $P^{(j)}(0) = 0$;
- $P^{(p-1)}(0) = (p-1)!(-1)^{mp}(m!)^p$ ist durch $(p-1)!$ teilbar, aber nicht durch $p!$;
- für $j \geq p$ und $\ell = 0, 1, \ldots, m$ ist $P^{(j)}(\ell)$ durch $p!$ teilbar.

Setzt man nun

$$I(x) = \int_0^x \mathrm{e}^{x-t} P(t)\mathrm{d}t,$$

so folgt durch partielle Integration

$$\begin{aligned} I(x) &= -P(t)\mathrm{e}^{x-t}\Big|_{t=0}^{x} + \int_0^x \mathrm{e}^{x-t}P'(t)\mathrm{d}t = \mathrm{e}^x P(0) - P(x) + \int_0^x \mathrm{e}^{x-t}P'(t)\mathrm{d}t \\ &= \mathrm{e}^x P(0) - P(x) + \mathrm{e}^x P'(0) - P'(x) + \int_0^x \mathrm{e}^{x-t}P''(t)\mathrm{d}t \\ &\vdots \\ &= \sum_{j=0}^{(m+1)p-1} \left(\mathrm{e}^x P^{(j)}(0) - P^{(j)}(x)\right). \end{aligned}$$

Sei nun

$$K = \sum_{\ell=0}^{m} a_\ell I(\ell) = \sum_{\ell=0}^{m} \sum_{j=0}^{(m+1)p-1} a_\ell \left(\mathrm{e}^\ell P^{(j)}(0) - P^{(j)}(\ell)\right) = -\sum_{\ell=0}^{m} \sum_{j=p-1}^{(m+1)p-1} a_\ell P^{(j)}(\ell) \in \mathbb{Z}.$$

Dann ist K durch $(p-1)!$ teilbar (weil jeder Summand es ist), aber nicht durch $p!$ (weil genau einer der Summanden nicht durch $p!$ teilbar ist). Also gilt $|K| \geq (p-1)!$.

Andererseits gilt mit

$$P^\sharp(x) = \sum_{k=p-1}^{(m+1)p-1} |b_k| x^k,$$

also dem Polynom welches aus P durch ersetzen aller Koeffizienten durch ihren Betrag entsteht,

$$|P(t)| \le P^\sharp(|t|) \le P^\sharp(|x|), \qquad |t| \le |x|,$$

und damit

$$|I(x)| \le \int_0^x \mathrm{e}^{x-t} P^\sharp(t) \mathrm{d}t \le P^\sharp(x) x \mathrm{e}^x, \qquad x \ge 0.$$

Da weiterhin $(PQ)^\sharp(|x|) \le P^\sharp(|x|) Q^\sharp(|x|)$ gilt, folgt

$$P^\sharp(\ell) \le \ell^{p-1} (\ell+1)^p (\ell+2)^p \cdots (\ell+m)^p$$

und somit

$$|K| \le \sum_{\ell=0}^{m} |a_\ell| |I(\ell)| \le \sum_{\ell=0}^{m} |a_\ell| \ell \mathrm{e}^\ell (\ell+m)^{(m+1)p-1} \le \left(\frac{1}{m} \sum_{\ell=0}^{m} |a_\ell| \ell \mathrm{e}^\ell \right) \left((2m)^{m+1} \right)^p,$$

also eine Abschätzung der Form $|K| \le CM^p$. Beide Abschätzungen $(p-1)! \le |K| \le CM^p$ können zusammen aber nur für endlich viele p erfüllt sein. Widerspruch. Damit ist e transzendent. □