V Kettenbrüche

13 Endliche Kettenbrüche

(13.1) In diesem Kapitel ist von Kettenbrüchen die Rede, genauer von den regelmäßigen Kettenbrüchen. Hier werden zunächst die endlichen Kettenbrüche behandelt, also die Kettenbruchentwicklungen der rationalen Zahlen. Damit wird im nächsten Paragraphen ein Faktorisierungsalgorithmus für natürliche Zahlen begründet, der deutlich mehr leistet als das aus der Schule vertraute Verfahren (vgl. (2.20)). Unendliche Kettenbrüche werden später in diesem Kapitel betrachtet.

(13.2) Es sei $n \in \mathbb{N}_0$, und es seien $a_0, a_1, \ldots, a_n \in \mathbb{R}$ mit $a_i > 0$ für jedes $i \in \{1, 2, \ldots, n\}$.
(1) Man setzt $[a_0] := a_0$ und für jedes $j \in \{1, 2, \ldots, n\}$

$$[a_0, a_1, \ldots, a_{j-1}, a_j] := \left[a_0, a_1, \ldots, a_{j-2}, a_{j-1} + \frac{1}{a_j}\right].$$

Es gilt also

$$[a_0, a_1] = a_0 + \frac{1}{a_1}, \quad [a_0, a_1, a_2] = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}},$$

$$[a_0, a_1, a_2, a_3] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}} \quad \text{und so fort.}$$

Ist $n \geq 1$, so gilt $[a_1, a_2, \ldots, a_n] > 0$ und

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{[a_1, a_2, \ldots, a_n]}.$$

(2) Man definiert rekursiv Zahlen $r_{-2}, r_{-1}, r_0, \ldots, r_n$ und $s_{-2}, s_{-1}, s_0, \ldots, s_n$ durch die folgenden Festsetzungen: Man setzt

$$r_{-2} := 0,\ r_{-1} := 1,\ s_{-2} := 1,\ s_{-1} := 0,$$

$$r_j := a_j r_{j-1} + r_{j-2},\ s_j := a_j s_{j-1} + s_{j-2} \quad \text{für jedes } j \in \{0, 1, \ldots, n\}.$$

Man sieht: Für jedes $j \in \{0,1,\ldots,n\}$ hängen r_j und s_j nur von den Zahlen $a_0, a_1, \ldots, a_j$ und nicht von $a_{j+1}, a_{j+2}, \ldots, a_n$ ab.
(3) Für jedes $j \in \{0,1,\ldots,n\}$ ist $s_j > 0$, denn es gilt $s_0 = 1$ und $s_1 = a_1 > 0$, und ist für ein $j \in \{2,3,\ldots,n\}$ bereits gezeigt, daß $s_0, s_1, \ldots, s_{j-1}$ positiv sind, so folgt $s_j = a_j s_{j-1} + s_{j-2} > 0$.
(4) Für jedes $j \in \{0,1,\ldots,n\}$ gilt

$$[a_0, a_1, \ldots, a_j] = \frac{r_j}{s_j}.$$

Beweis: Es gilt $[a_0] = a_0 = a_0/1 = r_0/s_0$. Es sei $j \in \{1,2,\ldots,n\}$, und es sei bereits bewiesen: Sind $a'_0, a'_1, \ldots, a'_{j-1} \in \mathbb{R}$ mit $a'_1 > 0$, $a'_2 > 0, \ldots, a'_{j-1} > 0$ und sind $r'_{-2}, r'_{-1}, r'_0, \ldots, r'_{j-1}$ und $s'_{-2}, s'_{-1}, s'_0, \ldots, s'_{j-1}$ die dazu gemäß (2) definierten Zahlen, so gilt $[a'_0, a'_1, \ldots, a'_{j-1}] = r'_{j-1}/s'_{j-1}$. Die zu $a'_0 := a_0$, $a'_1 := a_1, \ldots, a'_{j-2} := a_{j-2}$, $a'_{j-1} := a_{j-1} + 1/a_j$ gemäß (2) berechneten Zahlen sind $r'_{-2} = 0 = r_{-2}$, $r'_{-1} = 1 = r_{-1}$, $r'_0 = r_0, \ldots, r'_{j-2} = r_{j-2}$,

$$r'_{j-1} = \left(a_{j-1} + \frac{1}{a_j}\right) r'_{j-2} + r'_{j-3} = (a_{j-1} r_{j-2} + r_{j-3}) + \frac{r_{j-2}}{a_j} =$$
$$= r_{j-1} + \frac{r_{j-2}}{a_j} = \frac{a_j r_{j-1} + r_{j-2}}{a_j} = \frac{r_j}{a_j},$$

und $s'_{-2} = 1 = s_{-2}$, $s'_{-1} = 0 = s_{-1}$, $s'_0 = s_0, \ldots, s'_{j-2} = s_{j-2}$, $s'_{j-1} = s_j/a_j$. Also gilt auf Grund der Induktionsvoraussetzung

$$[a_0, a_1, \ldots, a_{j-1}, a_j] = \left[a_0, a_1, \ldots, a_{j-1} + \frac{1}{a_j}\right] = [a'_0, a'_1, \ldots, a'_{j-1}] =$$
$$= \frac{r'_{j-1}}{s'_{j-1}} = \frac{r_j/a_j}{s_j/a_j} = \frac{r_j}{s_j}.$$

(5) Für jedes $j \in \{0,1,\ldots,n\}$ definiert man die Matrizen

$$A_j := \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} \in M(2;\mathbb{R}) \quad \text{und} \quad B_j := A_0 A_1 \cdots A_{j-1} A_j \in M(2;\mathbb{R}).$$

Für jedes $j \in \{0,1,\ldots,n\}$ gilt $\det(A_j) = -1$ und daher $\det(B_j) = (-1)^{j+1}$, und es ist

$$B_j = \begin{pmatrix} r_j & r_{j-1} \\ s_j & s_{j-1} \end{pmatrix}.$$

Beweis: Es gilt

$$B_0 = A_0 = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} r_0 & r_{-1} \\ s_0 & s_{-1} \end{pmatrix}.$$

Ist $j \in \{1,2,\dots,n\}$ und ist bereits gezeigt, daß

$$B_{j-1} = \begin{pmatrix} r_{j-1} & r_{j-2} \\ s_{j-1} & s_{j-2} \end{pmatrix}$$

ist, so gilt

$$B_j = B_{j-1} \cdot A_j = \begin{pmatrix} r_{j-1} & r_{j-2} \\ s_{j-1} & s_{j-2} \end{pmatrix} \cdot \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} a_j r_{j-1} + r_{j-2} & r_{j-1} \\ a_j s_{j-1} + s_{j-2} & s_{j-1} \end{pmatrix} = \begin{pmatrix} r_j & r_{j-1} \\ s_j & s_{j-1} \end{pmatrix}.$$

(13.3) Es sei $n \in \mathbb{N}_0$, es seien $a_0 \in \mathbb{Z}$ und $a_1, a_2, \dots, a_n \in \mathbb{N}$, und es seien r_{-2}, r_{-1}, $r_0, \dots, r_n$ und s_{-2}, s_{-1}, $s_0, \dots, s_n$ die gemäß (13.2)(2) zu $a_0, a_1, \dots, a_n$ berechneten Zahlen.
(1) Für jedes $j \in \{0,1,\dots,n\}$ gilt: Es ist $r_j \in \mathbb{Z}$ und $s_j \in \mathbb{N}$, nach (13.2)(5) ist

$$r_j s_{j-1} - r_{j-1} s_j = (-1)^{j+1},$$

und daher gilt $\mathrm{ggT}(r_j, s_j) = 1$.
(2) Es gilt

$$1 = s_0 \leq s_1 = a_1 < s_2 < \cdots < s_n.$$

(3) Für jedes $j \in \{0,1,\dots,n-1\}$ gilt wegen (13.2)(4) und (13.2)(5)

$$[a_0, a_1, \dots, a_j, a_{j+1}] - [a_0, a_1, \dots, a_{j-1}, a_j] =$$
$$= \frac{r_{j+1}}{s_{j+1}} - \frac{r_j}{s_j} = \frac{r_{j+1}s_j - r_j s_{j+1}}{s_j s_{j+1}} = \frac{(-1)^j}{s_j s_{j+1}}.$$

(13.4) Bemerkung: Es sei $n \in \mathbb{N}$, es seien $a_0 \in \mathbb{Z}$ und $a_1, a_2, \dots, a_n \in \mathbb{N}$, und es gelte $a_n \geq 2$.
(1) Es gilt

$$a_0 < [a_0, a_1, \dots, a_n] < a_0 + 1;$$

insbesondere ist $[a_0, a_1, \dots, a_n] \notin \mathbb{Z}$.
(2) Für jedes $j \in \{0,1,\dots,n\}$ ist

$$a_j = \lfloor [a_j, a_{j+1}, \dots, a_n] \rfloor.$$

Beweis: (1) Im Fall $n = 1$ gilt $a_0 < [a_0, a_1] = a_0 + 1/a_1 \leq a_0 + 1/2 < a_0 + 1$. Es gelte $n \geq 2$, und es sei bereits bewiesen: Sind $a_0' \in \mathbb{Z}$ und $a_1', a_2', \dots, a_{n-1}' \in \mathbb{N}$

und ist $a'_{n-1} \geq 2$, so gilt $a'_0 < [a'_0, a'_1, \ldots, a'_{n-1}] < a'_0 + 1$. Dann gilt nach Induktionsvoraussetzung $a_1 < [a_1, a_2, \ldots, a_n] < a_1 + 1$ und daher

$$a_0 < a_0 + \frac{1}{a_1 + 1} < a_0 + \frac{1}{[a_1, a_2, \ldots, a_n]} = [a_0, a_1, \ldots, a_n] = \\ < a_0 + \frac{1}{a_1} \leq a_0 + 1.$$

(2) Es gilt $[a_n] = a_n$ und daher $\lfloor [a_n] \rfloor = a_n$. Für jedes $j \in \{0, 1, \ldots, n-1\}$ gilt nach (1) $a_j < [a_j, a_{j+1}, \ldots, a_n] < a_j + 1$, also $\lfloor [a_j, a_{j+1}, \ldots, a_n] \rfloor = a_j$.

(13.5) Satz: *Es seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Dann gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte Zahlen $a_0 \in \mathbb{Z}$ und $a_1, a_2, \ldots, a_n \in \mathbb{N}$ mit $a_n \geq 2$, falls $n \geq 1$ ist, und mit*

$$\frac{a}{b} = [a_0, a_1, \ldots, a_n].$$

Beweis: (1) Zum Beweis der Existenz – und zur Berechnung – kann man die folgende Variante des Euklidischen Algorithmus verwenden: Zu a und zu $b_0 := b$ gibt ein $n \in \mathbb{N}_0$ und Zahlen $a_0 \in \mathbb{Z}$ und $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbb{N}$ mit

$$\begin{array}{lllll} a & = a_0 b_0 + b_1 & \text{und} & b_1 < b_0, \\ b_0 & = a_1 b_1 + b_2 & \text{und} & b_2 < b_1, \\ & \vdots & & \vdots \quad \vdots \\ b_{n-2} & = a_{n-1} b_{n-1} + b_n & \text{und} & b_n < b_{n-1}, \\ b_{n-1} & = a_n b_n. & & \end{array}$$

Es ist $b_n = \mathrm{ggT}(a, b)$. Ist $n \geq 1$, so gilt $a_n \geq 1$ und $b_n < b_{n-1} = a_n b_n$, und daher ist $a_n \geq 2$. Mit den so berechneten Zahlen $a_0, a_1, \ldots, a_n$ gilt

$$\frac{a}{b} = [a_0, a_1, \ldots, a_n].$$

Beweis: Ist $n = 0$, so gilt $a/b = a_0 = [a_0]$; ist $n = 1$, so ist

$$a/b = a_0 + \frac{1}{b/b_1} = \left[a_0, \frac{b_0}{b_1}\right].$$

Es sei $n \geq 2$, es sei $j \in \{0, 1, \ldots, n-2\}$, und es sei bereits gezeigt, daß $a/b = [a_0, a_1, \ldots, a_j, b_j/b_{j+1}]$ gilt. Wegen

$$\frac{b_j}{b_{j+1}} = a_{j+1} + \frac{1}{b_{j+1}/b_{j+2}}$$

gilt dann

$$\frac{a}{b} = \left[a_0, a_1, \ldots, a_j, a_{j+1} + \frac{1}{b_{j+1}/b_{j+2}}\right] = \left[a_0, a_1, \ldots, a_j, a_{j+1}, \frac{b_{j+1}}{b_{j+2}}\right].$$

Für jedes $j \in \{0, 1, \ldots, n-1\}$ gilt also

$$\frac{a}{b} = \left[a_0, a_1, \ldots, a_j, \frac{b_j}{b_{j+1}}\right],$$

und daher ist insbesondere

$$\frac{a}{b} = \left[a_0, a_1, \ldots, a_{n-1}, \frac{b_{n-1}}{b_n}\right] = [a_0, a_1, \ldots, a_{n-1}, a_n].$$

(2) Es seien $r, s \in \mathbb{N}_0$, es seien $x_0, y_0 \in \mathbb{Z}$ und $x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s \in \mathbb{N}$, und es gelte $[x_0, x_1, \ldots, x_r] = [y_0, y_1, \ldots, y_s]$, sowie $x_r \geq 2$, falls $r \geq 1$ ist, und $y_s \geq 2$, falls $s \geq 1$ ist. Dann gilt $r = s$ und $x_j = y_j$ für jedes $j \in \{0, 1, \ldots, r\}$.

Beweis: Man braucht nur den Fall $r \leq s$ zu betrachten. Ist $r = 0$, so ist auch $s = 0$ [denn nach (13.4)(1) wäre sonst $x_0 = [x_0] = [y_0, y_1, \ldots, y_s] \notin \mathbb{Z}$], und es folgt $x_0 = [x_0] = [y_0] = y_0$. Ist $r \geq 1$, so gilt nach (13.4)(2)

$$x_0 = \lfloor [x_0, x_1, \ldots, x_r] \rfloor = \lfloor [y_0, y_1, \ldots, y_s] \rfloor = y_0,$$

wegen

$$x_0 + \frac{1}{[x_1, x_2, \ldots, x_r]} = [x_0, x_1, \ldots, x_r] = \\ = [y_0, y_1, \ldots, y_s] = y_0 + \frac{1}{[y_1, y_2, \ldots, y_s]}$$

folgt $[x_1, x_2, \ldots, x_r] = [y_1, y_2, \ldots, y_s]$, und Induktion liefert dann $r - 1 = s - 1$ und $x_j = y_j$ für jedes $j \in \{1, 2, \ldots, r\}$.

(13.6) Bemerkung: Es seien $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Nach (13.5) gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_0$ und eindeutig bestimmte Zahlen $a_0 \in \mathbb{Z}, a_1, \ldots, a_n \in \mathbb{N}$ mit $a_n \geq 2$, falls $n \geq 1$ ist, und mit

$$(*) \quad \frac{a}{b} = [a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

(1) Man nennt (∗) die Kettenbruchentwicklung von a/b oder den Kettenbruch für a/b, genauer den endlichen regelmäßigen Kettenbruch für a/b. Die Zahlen $a_0, a_1, \ldots, a_n$ heißen die Teilnenner dieses Kettenbruchs. Der Existenzbeweis in (13.5) zeigt, wie man diese Teilnenner mit Hilfe der im Euklidischen Algorithmus durchzuführenden Rechnung ermitteln kann. Die gemäß (13.2)(2) zu dem Kettenbruch (∗) berechneten rationalen Zahlen

$$\frac{r_0}{s_0}, \frac{r_1}{s_1}, \ldots, \frac{r_n}{s_n}$$

heißen die Näherungsbrüche, ihre Zähler die Näherungszähler und ihre Nenner die Näherungsnenner dieses Kettenbruchs.
Nach (13.2)(4) und nach (13.3)(1) gilt

$$\frac{r_n}{s_n} = [a_0, a_1, \ldots, a_n] = \frac{a}{b} \quad \text{und} \quad \operatorname{ggT}(r_n, s_n) = 1.$$

(2) Für jedes $j \in \{0, 1, \ldots, n-1\}$ gilt nach (13.3)(3): Es ist

$$\frac{r_{j+1}}{s_{j+1}} - \frac{r_j}{s_j} = \frac{(-1)^j}{s_j s_{j+1}} \quad \text{und}$$

$$\frac{a}{b} - \frac{r_j}{s_j} = \frac{r_n}{s_n} - \frac{r_j}{s_j} = \sum_{i=j}^{n-1} \left(\frac{r_{i+1}}{s_{i+1}} - \frac{r_i}{s_i} \right) = \sum_{i=j}^{n-1} \frac{(-1)^i}{s_i s_{i+1}} =$$

$$= (-1)^j \left(\frac{1}{s_j s_{j+1}} + \frac{-1}{s_{j+1} s_{j+2}} + \cdots + \frac{(-1)^{n-j-1}}{s_{n-1} s_n} \right).$$

Wegen $s_0 \leq s_1 < s_2 < \cdots < s_n$ folgt daraus: Es ist

$$\left| \frac{a}{b} - \frac{r_j}{s_j} \right| \leq \frac{1}{s_j s_{j+1}} \quad \text{für jedes } j \in \{0, 1, \ldots, n-1\}.$$

(13.7) Beispiel: Für $a = 225$ und $b = 157$ erhält man, wenn man wie im Beweis von (13.5) rechnet:

$$225 = 1 \cdot 157 + 68,\ 157 = 2 \cdot 68 + 21,\ 68 = 3 \cdot 21 + 5,\ 21 = 4 \cdot 5 + 1,\ 5 = 5 \cdot 1.$$

Also gilt

$$\frac{225}{157} = [1, 2, 3, 4, 5].$$

Die Näherungsbrüche dieses Kettenbruchs sind

$$\frac{1}{1}, \frac{3}{2}, \frac{10}{7}, \frac{43}{30}, \frac{225}{157}.$$

(13.8) Bemerkung: Das klassische Werk über Kettenbrüche ist das Buch [77] von O. Perron (1880 – 1975). Eine neuere Darstellung der Zahlentheorie der Kettenbrüche ist das Buch [92] von A. M. Rockett und P. Szüsz.

(13.9) Aufgaben:

Aufgabe 1: Man schreibe eine MuPAD-Funktion, die zu einer rationalen Zahl q mit Hilfe der im Beweis von (13.5) verwendeten Methode den Kettenbruch für die Zahl q berechnet.

Aufgabe 2: (a) Man schreibe eine MuPAD-Funktion, die zu einer Liste aus einer ganzen Zahl a_0, aus natürlichen Zahlen $a_1, \ldots, a_{n-1}$ und aus einer natürlichen Zahl $a_n \geq 2$ die Liste der Näherungsbrüche des Kettenbruchs $[a_0, a_1, \ldots, a_n]$ berechnet. Man richte diese Funktion so ein, daß sie bei Aufruf mit einem zweiten Argument $k \in \{0, 1, \ldots, n\}$ nur den k-ten Näherungsbruch dieses Kettenbruchs ausgibt.

(b) Man schreibe eine MuPAD-Funktion, die zu einer Liste aus einer ganzen Zahl a_0, aus natürlichen Zahlen $a_1, \ldots, a_{n-1}$ und aus einer natürlichen Zahl $a_n \geq 2$ nur den Wert des Kettenbruchs $[a_0, a_1, \ldots, a_n]$ berechnet.

14 Der Algorithmus von R. S. Lehman

(14.1) In diesem Paragraphen wird ein Faktorisierungsalgorithmus für natürliche Zahlen vorgestellt, der mehr leistet als das in (2.20) beschriebene naive Verfahren; zu seiner Begründung werden die im letzten Paragraphen behandelten Kettenbruchentwicklungen von rationalen Zahlen verwendet.

(14.2) Es seien a, $b \in \mathbb{N}$, und es gelte $b < a$ und $b \nmid a$.
(1) Es sei $a/b = [a_0, a_1, \ldots, a_n]$ die Kettenbruchentwicklung von a/b. Wegen $b < a$ ist $a_0 = \lfloor a/b \rfloor \in \mathbb{N}$, und wegen $b \nmid a$ gilt $n \geq 1$ und daher $a_n \geq 2$. Es gilt

$$\frac{b}{a} = 0 + \frac{1}{a/b} = \left\lfloor \frac{b}{a} \right\rfloor + \frac{1}{[a_0, a_1, \ldots, a_n]} = [0, a_0, a_1, \ldots, a_n].$$

Wegen $a_0, a_1, \ldots, a_n \in \mathbb{N}$ und wegen $a_n \geq 2$ ist dies der Kettenbruch für b/a.
(2) Es seien $r_0/s_0, r_1/s_1, \ldots, r_n/s_n$ die $n+1$ Näherungsbrüche des Kettenbruchs $a/b = [a_0, a_1, \ldots, a_n]$. Für jedes $j \in \{0, 1, \ldots, n\}$ gilt

$$\frac{r_j}{s_j} = [a_0, a_1, \ldots, a_j]$$

und

$$[0, a_0, a_1, \ldots, a_j] = 0 + \frac{1}{[a_0, a_1, \ldots, a_j]} = \frac{1}{r_j/s_j} = \frac{s_j}{r_j},$$