Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, hhu
K. Halupczok

Z20: Kettenbrüche

Stichworte: eukl. Algo = endliche KBE, Teilnenner, k-ter Rest ϱ_k, Näherungsbruch $\frac{c_k}{d_k}$, Rekursionen für NBe, Matrizennotation dafür, Alternieren der NBe, Darstellung eines KBs mit k-tem Rest

---

20.1. Einleitung: Der euklidische Algorithmus lässt sich als Kettenbruchentwicklung (KBE) einer Bruchzahl deuten. Wir definieren auch unendliche Kettenbrüche (formal, und im Falle der Konvergenz identifizieren wir diesen mit dem Grenzwert). Die einhergehenden Bezeichnungen (Näherungsbruch, k-ter Rest, Teilnenner) werden eingeführt und die grundlegenden Rekursionsgleichungen (in gängiger Notation) bewiesen.

20.2. Bekanntlich liefert der euklidische Algorithmus eine effektive Berechnung des ggT's zweier ganzer Zahlen: Seien $a, b \in \mathbb{Z}$, $a \neq 0$.
Führe sukzessive eine Division mit Rest aus wie folgt:

$$\left.\begin{array}{ll} b = q_0 a + r_1 & 0 \le r_1 < b \\ a = q_1 r_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 = q_2 r_2 + r_3 & 0 \le r_3 < r_2 \\ \vdots & \vdots \\ r_{m-2} = q_{m-1} r_{m-1} + r_m & 0 \le r_m < r_{m-1} \end{array}\right\}$$

$$r_{m-1} = q_m r_m$$

(*) Rekursion: $r_{-1} := b$, $r_0 := a$,
$r_{i-1} = q_i r_i + r_{i+1}$, $0 \le r_{i+1} < r_i$ für $0 \le i \le m-1$,
$r_{m-1} = q_m r_m \rightsquigarrow r_{m+1} = 0$

muss abbrechen: $r_{m+1} = 0$, sei $m \in \mathbb{N}_0$ minimal mit $r_{m+1} = 0$
auch, wenn mit absolut kleinstem Rest gerechnet wird!

20.3. Lemma: $r_m = \operatorname{ggT}(a, b) := \max\{d;\ d \mid a \wedge d \mid b\}$.
Haben $r_m = xa + yb$, wo $x, y \in \mathbb{Z}$ aus (*) rekursiv bestimmbar sind.

20.4. Def.: Die Koeffizienten x, y nennt man auch Bézout-Elemente oder Bézout-Koeffizienten.

20.5. Bew.:
- $r_m \mid r_{m-1} \mid r_{m-2} \mid \ldots \mid a \mid b$ und $t \mid a \wedge t \mid b \Rightarrow t \mid r_1 \mid r_2 \mid \ldots \mid r_m$, also $r_m = \operatorname{ggT}(a, b)$.
- Schreibe sukzessive $r_1, r_2, \ldots, r_m$ als $\mathbb{Z}$-Linearkombination von $a, b \rightsquigarrow x, y$. □

20.6. Bem.: Schreibweise (a, b) des $\operatorname{ggT}(a, b)$ erinnert an Ideal $\mathbb{Z}a + \mathbb{Z}b = (a, b)$, haben in Idealschreibweise für $d = \operatorname{ggT}(a, b)$ ja $(d) = (a, b)$.

20.7. Schreiben den eukl. Algo. jetzt anders auf:

$$\frac{b}{a} = q_0 + \frac{r_1}{a}, \qquad q_0 = \left\lfloor \frac{b}{a} \right\rfloor, \qquad 0 \le \frac{r_1}{a} < 1 \quad \overset{r_1 \neq 0}{\rightsquigarrow} \quad \frac{a}{r_1} > 1$$

$$\frac{a}{r_1} = q_1 + \frac{r_2}{r_1}, \qquad q_1 = \left\lfloor \frac{a}{r_1} \right\rfloor, \qquad 0 \le \frac{r_2}{r_1} < 1 \rightsquigarrow \frac{r_1}{r_2} > 1$$

$$\frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2}, \qquad q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor, \qquad 0 < \frac{r_3}{r_2} < 1 \rightsquigarrow \frac{r_2}{r_3} > 1$$

$$\vdots$$

$$\frac{r_{m-2}}{r_{m-1}} = q_{m-1} + \frac{r_m}{r_{m-1}}$$

$$\frac{r_{m-1}}{r_m} = q_m$$

Beachte: $q_1, \dots, q_m \in \mathbb{N}$, und $q_m \ge 2$ im Falle $m \ge 1$ (da $r_{m-1} \gneqq r_m$)

Zusammengefasst: $$\frac{b}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{m-1} + \cfrac{1}{q_m}}}}$$ "Kettenbruch(entwicklung) von $\frac{b}{a}$"

20.8. Im Bsp.: $$\frac{133}{84} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2}}}}, \quad q_0 = 1,\ q_1 = 1,\ q_2 = 1,\ q_3 = 2,\ q_4 = 2$$

Näherungsbrüche: $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{8}{5}, \frac{19}{12} = \frac{133}{84}$.

numerisch: $1, 2, 1.5, 1.6, 1.58\overline{3}$ $\rightsquigarrow \left| \frac{133}{84} - \frac{3}{2} \right| < \frac{1}{12}$

↑ gute Approximation mit kleinem Nenner

20.9. Anstelle $\alpha = \frac{b}{a}$ sei jetzt $\alpha \in \mathbb{R}$ beliebige reelle Zahl

$\rightsquigarrow$ Schema: $\alpha = \underbrace{\lfloor \alpha \rfloor}_{=: q_0} + \varepsilon$ mit $0 \le \varepsilon < 1$. Falls $\alpha \notin \mathbb{Z}$, ist $\varepsilon \neq 0$, setze $\xi_1 = \frac{1}{\varepsilon} > 1$.

$\rightsquigarrow \alpha = q_0 + \frac{1}{\xi_1}$ mit $\xi_1 > 1$. Falls $\xi_1 \notin \mathbb{Z}$, so.

$\xi_1 = \underbrace{q_1}_{:= \lfloor \xi_1 \rfloor} + \frac{1}{\xi_2}$ mit $\xi_2 > 1$. $\vdots$

$\vdots$

$\xi_k = q_k + \frac{1}{\xi_{k+1}}$, abbrechen, wenn $\xi_n \in \mathbb{Z}$, sonst weiter.

Erhalten so: $$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_k + \cfrac{1}{\xi_{k+1}}}}}$$ in k Schritten.

20.10. Def.: (1) Seien $q_0, q_1, \dots, q_m$ reelle Zahlen (später: ganze Zahlen) mit $q_1, \dots, q_m > 0$.
Unter dem endlichen Kettenbruch $[q_0; q_1, q_2, \dots, q_m]$
verstehen wir sowohl das $(m+1)$-Tupel $(q_0, q_1, \dots, q_m)$ als auch seinen
Wert $$[q_0; q_1, \dots, q_m] := q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \dots + 1/q_m}}.$$

Man nennt $[q_0; q_1, \dots, q_m]$ einen $(m+1)$-gliedrigen Kettenbruch.
Die $q_1, q_2, \dots, q_m$ heißen Teilnenner. (engl. partial quotient/denominator
Die Übersetzung "Teilbrüche" ist irreführend.)

(2) Für $0 \le k \le m$ nennen wir den Kettenbruch $S_k := [q_k; q_{k+1}, \dots, q_m]$ den k-ten Rest des Kettenbruches in (1).
Wir haben so $S_0 = [q_0; q_1, \dots, q_m]$, $S_1 = [q_1; q_2, \dots, q_m], \dots,$ $S_m = [q_m] = q_m$.
Für den Wert des Kettenbruches in (1) gilt $[q_0; q_1, \dots, q_m] = [q_0; q_1, \dots, q_{k-1}, S_k]$ für $0 \le k \le m$.

(3) Eine rekursive Def. des Wertes in (1) ist auch möglich:
$[q_0] := q_0$, $[q_0; q_1] = q_0 + \frac{1}{q_1}$, und für $m \ge 1$: $[q_0; q_1, \dots, q_m] = [q_0; S_1] = q_0 + \frac{1}{S_1}$
(wo $S_1 > 0$ per Rekursion). Oder auch: $[q_0; q_1, \dots, q_m] = [q_0; q_1, \dots, q_{m-1}, S_{m-1}]$
$= [q_0; q_1, \dots, q_{m-2}, q_{m-1} + \frac{1}{q_m}]$ (ist m-gliedrig).

20.11. **Def.:** (1) Geg. sei die Folge $(q_n)_{n \in \mathbb{N}}$ reeller Zahlen mit $q_k > 0$ für $k \ge 1$.
Unter dem (unendlichen) Kettenbruch $[q_0; q_1, q_2, \dots]$ verstehen wir die Folge der $[q_0; q_1, q_2, \dots, q_n]$, $n = 0, 1, 2, \dots$ Falls diese Folge konvergiert, bezeichnen wir auch deren Grenzwert mit $[q_0; q_1, q_2, \dots]$.
(2) Der (unendliche) Kettenbruch $S_k = [q_k; q_{k+1}, \dots]$, $k = 0, 1, 2, \dots$ heißt der k-te Rest des Kettenbruches in (1).
Formal gilt: $[q_0; q_1, q_2, \dots] = [q_0; q_1, \dots, q_{k-1}, S_k]$.
Wir zeigen dies für die Werte der Kettenbrüche im Falle der Konvergenz später.
Abkürzungen: KB = Kettenbruch, KBE = Kettenbruchentwicklung.

20.12. **Def.:** Jedem endlichen KB $[q_0; q_1, \dots, q_k]$ ordnen wir rekursiv ein Paar $(c, d) \in \mathbb{R} \times \mathbb{R}_{>0}$ zu mit $[q_0; q_1, \dots, q_k] = \frac{c}{d}$ gemäß der Rekursion:
$k = 0$: $\binom{c}{d} = \binom{q_0}{1}$ $\quad \to$ ok: $[q_0] = q_0 = \frac{c}{d}$ ✓
$k \ge 1$: $\binom{c}{d} = \binom{q_0 c' + d'}{c'} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \binom{c'}{d'}$, wo (c', d') zu KB $S_1 = [q_1; q_2, \dots, q_k]$ gehöre. $\quad \to$ ok: $[q_0; q_1, \dots, q_k] = q_0 + \frac{1}{S_1} = q_0 + \frac{d'}{c'} = \frac{q_0 c' + d'}{c'} = \frac{c}{d}$ ✓
(Bem.: wegen $S_1 > 0, d' > 0$ ist $c' > 0$.)

20.13 **Def.:** Sei $[q_0; q_1, q_2, \ldots]$ ein endlicher oder unendlicher KB.
Das dem k-ten Abschnitt $[q_0; q_1, q_2, \ldots, q_k]$, $k \geq 0$, als 20.12 zugeordnete Paar $\binom{c_k}{d_k}$ heißt k-ter Näherungsbruch des KBes. Auch $\frac{c_k}{d_k}$ heißt k-ter Näherungsbruch. Ist der KB endlich, etwa $= [q_0; q_1, \ldots, q_m]$, so ist der m-te Näherungsbruch $\frac{c_m}{d_m}$ gleich dem Wert dieses KBes.
Aus formalen Gründen setzen wir $\binom{c_{-1}}{d_{-1}} = \binom{1}{0}$, $\binom{c_{-2}}{d_{-2}} = \binom{0}{1}$.
Abkürzung: NB = Näherungsbruch (engl. convergent. Die Übersetzung "Konvergente" ist eher irreführend).

20.14 **Lemma** (Rekursionsformeln für NBe): Bezeichnungen wie eben, setze
$c_{-2} = 0,\quad c_{-1} = 1,\quad c_0 = q_0;$
$d_{-2} = 1,\quad d_{-1} = 0,\quad d_0 = 1.$ Dann: $c_k = q_k c_{k-1} + c_{k-2}$, $d_k = q_k d_{k-1} + d_{k-2}$, $k = 0, 1, 2, \ldots$ ($k \leq m$ bei endl. KB)
In Matrizenform: $\binom{c_k}{d_k} = \underbrace{\begin{pmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{pmatrix}}_{=: M_k} \binom{q_k}{1}$ $\oplus$.

20.15 **Bem.:** Die Rekursionen zeigen $d_k > 0$ für $k \geq 0$. (Und $d_k \geq d_{k-1}$, $c_k \geq c_{k-1}$ für $q_i \geq 1$.)

20.16 **Bew.:** Setzen $M_i := \begin{pmatrix} c_{i-1} & c_{i-2} \\ d_{i-1} & d_{i-2} \end{pmatrix}$ für $i = 0, 1, 2, \ldots$, also $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $M_1 = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}$.
Es gilt $\binom{c_0}{d_0} = \binom{q_0}{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \binom{q_0}{1}$, also ist $\oplus$ richtig für $k = 0$.
Weiter: habe $[q_1; q_2, \ldots, q_m]$ die NBe $\binom{c_i'}{d_i'}$ mit $-2 \leq i \leq m-1$, $m \geq 1$.
Dann ist per Def. 20.12: $\binom{c_i}{d_i} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \binom{c'_{i-1}}{d'_{i-1}} = M_1 \binom{c'_{i-1}}{d'_{i-1}}$ für $i \geq -1$.
Induktionsschritt: Sei $k \geq 1$ und Beh. wahr für $k-1$. Dann gilt für $[q_1; q_2, \ldots, q_m]$ nach Ind.vor. mit $m = k$: $\binom{c'_{k-1}}{d'_{k-1}} = \begin{pmatrix} c'_{k-2} & c'_{k-3} \\ d'_{k-2} & d'_{k-3} \end{pmatrix} \binom{q_k}{1}$. Wollen Rekursion für $[q_0; q_1, \ldots, q_m]$ zeigen. Aus $\binom{c_k}{d_k} = M_1 \binom{c'_{k-1}}{d'_{k-1}}$ folgt

$$\binom{c_k}{d_k} = M_1 \binom{c'_{k-1}}{d'_{k-1}} = M_1 \begin{pmatrix} c'_{k-2} & c'_{k-3} \\ d'_{k-2} & d'_{k-3} \end{pmatrix} \binom{q_k}{1} = \left(M_1 \binom{c'_{k-2}}{d'_{k-2}}, M_1 \binom{c'_{k-3}}{d'_{k-3}} \right) \cdot \binom{q_k}{1} = \begin{pmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{pmatrix} \binom{q_k}{1}$$

$\hookrightarrow \oplus$ ✓ □

20.17 **Bsp.:** KBE für $[1; 1, 1, 2, 2]$:

k			0	1	2	3	$4 = m$
q_k			1	1	1	2	2
c	0	1	1	2	3	8	19
d	1	0	1	1	2	5	12
$\frac{c}{d}$			$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{2}$	$\frac{8}{5}$	$\frac{19}{12}$

$\frac{19}{12} = [1; 1, 1, 2, 2]$.

Zelle = vorletzte Zelle + letzter Zelle mal q-Wert drüber = Rekursionen

20.18 Lemma: Mit obigen Bezeichnungen gilt: (i) $M_{k+1} = M_k \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$, $k=0,1,2,\dots$,

(ii) $M_{k+1} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$, $k=0,1,2,\dots$

(iii) $d_k c_{k-1} - c_k d_{k-1} = (-1)^k$ für $k \ge -1$

(iv) $\frac{c_{k-1}}{d_{k-1}} - \frac{c_k}{d_k} = \frac{(-1)^k}{d_k d_{k-1}}$ für $k \ge 1$ $[d_{-1} = 0]$

(v) $d_k c_{k-2} - c_k d_{k-2} = (-1)^{k-1} q_k$ für $k \ge 0$

(vi) $\frac{c_{k-2}}{d_{k-2}} - \frac{c_k}{d_k} = \frac{(-1)^{k-1} q_k}{d_k d_{k-2}}$ für $k \ge 0$, aber $k \ne 1$ da $d_{-1} = 0$.

Bew.: (i) ✓

(ii): $M_k \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{pmatrix} \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c_k & c_{k-1} \\ d_k & d_{k-1} \end{pmatrix} = M_{k+1}$, $k=0,1,\dots$, $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightsquigarrow$ (ii) ✓

(iii): $c_k d_{k-1} - c_{k-1} d_k = \det(M_{k+1}) = \underbrace{\det\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}}_{=-1} \cdots \underbrace{\det\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}}_{=-1} = (-1)^{k+1}$, $k \ge 0 \rightsquigarrow$ (iii) ✓

(iv): aus (iii) ✓, (vi): aus (v) ✓,

(v): $-(d_k c_{k-2} - c_k d_{k-2}) = \begin{vmatrix} c_k & c_{k-2} \\ d_k & d_{k-2} \end{vmatrix} \overset{2014}{=} \begin{vmatrix} q_k c_{k-1} + c_{k-2} & c_{k-2} \\ q_k d_{k-1} + d_{k-2} & d_{k-2} \end{vmatrix} = \begin{vmatrix} q_k c_{k-1} & c_{k-2} \\ q_k d_{k-1} & d_{k-2} \end{vmatrix}$

$= q_k \begin{vmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{vmatrix} = q_k \det(M_k) \underset{\text{vgl. (iii)}}{=} q_k (-1)^k = -q_k (-1)^{k-1}$. □

20.19 Lemma: (i) $\left(\frac{c_{2m}}{d_{2m}}\right)_{m \ge 0}$ ist streng monoton wachsend

(ii) $\left(\frac{c_{2m+1}}{d_{2m+1}}\right)_{m \ge 0}$ ist streng monoton fallend

(iii) $\frac{c_{2m}}{d_{2m}} < \frac{c_{2n+1}}{d_{2n+1}}$ für alle $m \ge 0$, $n \ge 0$.

Bew.: (i), (ii): aus 2018 (vi) (beachte $q_k > 0$ für $k \ge 1$, $d_k > 0$ für $k \ge 0$).

(iii): Beh. wahr für $m = n \ge 0$ nach 2018 (iv). Für $m \le n$ ist $\frac{c_{2m}}{d_{2m}} \underset{(i)}{\le} \frac{c_{2n}}{d_{2n}} \overset{m=n ✓}{<} \frac{c_{2n+1}}{d_{2n+1}}$,

für $m \ge n$ ist $\frac{c_{2n+1}}{d_{2n+1}} \underset{(ii)}{\ge} \frac{c_{2m+1}}{d_{2m+1}} \overset{m=n ✓}{>} \frac{c_{2m}}{d_{2m}}$. □

20.20 Lemma: (i) $[q_0; q_1, \dots, q_n] = \frac{s_k c_{k-1} + c_{k-2}}{s_k d_{k-1} + d_{k-2}}$ für $1 \le k \le n$ (Nenner > 0 da $s_k > 0$, $d_{k-1} > 0$, $d_{k-2} \ge 0$)

(ii) $[q_k; q_{k-1}, \dots, q_1] = \frac{d_k}{d_{k-1}}$ für $k \ge 1$.

Bew.: (i): $[q_0; q_1, \dots, q_n] = [q_0; q_1, \dots, q_{k-1}, s_k] \overset{2014}{=} \frac{s_k c_{k-1} + c_{k-2}}{s_k d_{k-1} + d_{k-2}}$

(ii): $\begin{pmatrix} c'_{k-1} & c'_{k-2} \\ d'_{k-1} & d'_{k-2} \end{pmatrix} = M'_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} = \left(\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \right)^T$

$\overset{2018 (ii)}{=} \left(\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} M_{k+1} \right)^T = \left(\begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} c_k & c_{k-1} \\ d_k & d_{k-1} \end{pmatrix} \right)^T = \begin{pmatrix} d_k & d_{k-1} \\ * & * \end{pmatrix}^T = \begin{pmatrix} d_k & * \\ d_{k-1} & * \end{pmatrix}$,

also ist $[q_k; q_{k-1}, \dots, q_1] = \frac{c'_{k-1}}{d'_{k-1}} = \frac{d_k}{d_{k-1}}$. □