(c) Nach (b) konvergiert für jedes positive $x_1 \in \mathbb{R}$ die Folge $(x_n)_{n\geq 1}$ mit

$$x_{n+1} \;:=\; x_n \cdot \frac{x_n^2+9}{3x_n^2+3} \quad \text{für jedes } n \in \mathbb{N}$$

gegen $\sqrt{3}$. Wie kann man jede der beiden von Archimedes angegebenen rationalen Näherungen an $\sqrt{3}$ mit Hilfe einer solchen Folge finden?

16 Periodische Kettenbrüche

(16.1) In diesem Paragraphen werden die Kettenbruchentwicklungen von irrationalen reellen Zahlen, die Nullstellen von quadratischen Polynomen mit rationalen Koeffizienten sind, behandelt. Zuerst wird gezeigt, daß diese Zahlen genau die Zahlen mit periodischer Kettenbruchentwicklung sind. Dann werden die Kettenbruchentwicklungen von Quadratwurzeln aus natürlichen Zahlen genauer untersucht; die dabei erzielten Ergebnisse werden im folgenden Paragraphen benötigt. Zwei der Resultate dieses Paragraphen stammen aus der ersten Publikation von E. Galois (1811 – 1832), die anderen gehen auf P. de Fermat, L. Euler und J. L. Lagrange zurück.

(16.2) Definition: Es sei $a_0 \in \mathbb{Z}$, und es sei $(a_n)_{n\geq 1}$ eine Folge in $\mathbb{N}$. Wenn es ein $k \in \mathbb{N}_0$ und ein $l \in \mathbb{N}$ mit

$$a_{k+l+i} \;=\; a_{k+i} \quad \text{für jedes } i \in \mathbb{N}_0$$

gibt, so nennt man den Kettenbruch $[\,a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots\,]$ periodisch und schreibt

$$[\,a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots\,] \;=\; [\,a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}\,];$$

man nennt $(a_0, a_1, \ldots, a_{k-1})$ eine Vorperiode und $(a_k, a_{k+1}, \ldots, a_{k+l-1})$ eine Periode dieses Kettenbruchs. Der Kettenbruch $[\,a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$ heißt rein-periodisch, wenn es ein $l \in \mathbb{N}$ mit $a_{l+i} = a_i$ für jedes $i \in \mathbb{N}_0$ gibt, also wenn gilt: Es ist

$$[\,a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots\,] \;=\; [\,\overline{a_0, a_1, \ldots, a_{l-1}}\,].$$

(16.3) Bemerkung: Es sei $a_0 \in \mathbb{Z}$, es sei $(a_n)_{n\geq 1}$ eine Folge in $\mathbb{N}$, und es gelte: Der Kettenbruch $[\,a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots\,]$ ist periodisch. Eine Periode $(a_k, a_{k+1}, \ldots, a_{k+l-1})$ dieses Kettenbruchs heißt primitiv, wenn es nicht Zahlen $i, j \in \{k, k+1, \ldots, k+l-1\}$ mit $0 < j-i < l-1$ gibt, für die $(a_i, a_{i+1}, \ldots, a_j)$

ebenfalls eine Periode ist. Alle primitiven Perioden des Kettenbruchs haben dieselbe Länge, und jede Periode entsteht durch Zusammenhängen mehrerer Kopien einer primitiven Periode.

(16.4) Definition: Eine irrationale reelle Zahl α nennt man eine quadratische Irrationalzahl, wenn es ein Polynom $f \in \mathbb{Q}[T]$ vom Grad 2 gibt, das α als Nullstelle besitzt.

(16.5) Satz (L. Euler 1737): *Es sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Wenn der Kettenbruch*

$$\alpha = [a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$$

periodisch ist, so ist α eine quadratische Irrationalzahl.

Beweis: Es gelte: Es gibt ein $k \in \mathbb{N}_0$ und ein $l \in \mathbb{N}$ mit

$$\alpha = [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}].$$

Für

$$\alpha_k := [a_k, a_{k+1}, a_{k+2}, \ldots, a_n, a_{n+1}, \ldots] = [\overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}] \in \mathbb{R} \setminus \mathbb{Q}$$

gilt (vgl. den Beweis in (15.5)): Es ist

$$\alpha = [a_0, a_1, \ldots, a_{k-1}, \alpha_k] = [a_0, a_1, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_{k+l-1}, \alpha_k].$$

Es seien $r_{-2} := 0$, $r_{-1} := 1$, $s_{-2} := 1$, $s_{-1} := 0$ und $r_n := a_n r_{n-1} + r_{n-2}$, $s_n := a_n s_{n-1} + s_{n-2}$ für jedes $n \in \mathbb{N}_0$. Es gilt (vgl. (13.2)(4))

$$\begin{aligned} \frac{\alpha_k r_{k-1} + r_{k-2}}{\alpha_k s_{k-1} + s_{k-2}} &= [a_0, a_1, \ldots, a_{k-1}, \alpha_k] = \alpha = \\ &= [a_0, a_1, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_{k+l-1}, \alpha_k] = \frac{\alpha_k r_{k+l-1} + r_{k+l-2}}{\alpha_k s_{k+l-1} + s_{k+l-2}} \end{aligned}$$

und daher

$$\frac{\alpha s_{k-2} - r_{k-2}}{\alpha s_{k-1} - r_{k-1}} = -\alpha_k = \frac{\alpha s_{k+l-2} - r_{k+l-2}}{\alpha s_{k+l-1} - r_{k+l-1}}.$$

Mit

$$\begin{aligned} a &:= s_{k-2} s_{k+l-1} - s_{k-1} s_{k+l-2} \in \mathbb{Z}, \\ b &:= r_{k-1} s_{k+l-2} + r_{k+l-2} s_{k-1} - r_{k-2} s_{k+l-1} - r_{k+l-1} s_{k-2} \in \mathbb{Z}, \\ c &:= r_{k-2} r_{k+l-1} - r_{k-1} r_{k+l-2} \in \mathbb{Z} \end{aligned}$$

gilt daher

$$a\alpha^2 + b\alpha + c = 0.$$

Angenommen, es gilt $a = 0$, also

$$(*) \qquad s_{k-2}s_{k+l-1} \;=\; s_{k-1}s_{k+l-2}.$$

Es gilt $l \geq 1$, also ist $s_{l-1} \geq s_0 = 1$, und daher ist $k \geq 2$, denn wäre $k = 0$, so wäre wegen $(*)$ $s_{l-1} = s_{-2}s_{l-1} = s_{-1}s_{l-2} = 0$, und wäre $k = 1$, so wäre, wieder wegen $(*)$, $s_{l-1} = s_0 s_{l-1} = s_{-1}s_l = 0$. Nach (15.3)(1) gilt

$$r_{k+l-1}s_{k+l-2} - r_{k+l-2}s_{k+l-1} \;=\; (-1)^{k+l},$$

und daher sind s_{k+l-2} und s_{k+l-1} teilerfremd. Wegen $(*)$ ist s_{k+l-1} ein Teiler von $s_{k-1}s_{k+l-2}$, und wegen $\mathrm{ggT}(s_{k+l-2}, s_{k+l-1}) = 1$ folgt $s_{k+l-1} \mid s_{k-1}$. Aber wegen $k \geq 2$ ist $s_{k+l-1} > s_{k-1} \geq 1$. Damit ist gezeigt, daß $a \neq 0$ gilt.

(16.6) Bemerkung: Es sei α eine irrationale reelle Zahl mit einer periodischen Kettenbruchentwicklung

$$\alpha \;=\; [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}].$$

Der Beweis in (16.5) zeigt, wie man α aus seiner Kettenbruchentwicklung berechnen kann. Man findet dazu mit der im Beweis verwendeten Methode zunächst ein Polynom $f \in \mathbb{Z}[T]$ vom Grad 2, das α als Nullstelle besitzt. Dieses Polynom f hat eine weitere reelle Nullstelle β, und es bleibt noch zu entscheiden, welche der beiden Nullstellen α ist. Dazu kann man ausnützen, daß gilt: Es ist $a_0 < \alpha < a_0 + 1$, $a_1 < \alpha_1 = 1/(\alpha - a_0) < a_1 + 1$ und so fort. In Abschnitt (16.12) wird eine andere Möglichkeit, α aus seiner Kettenbruchentwicklung zu gewinnen, beschrieben.

(16.7) Es sei d eine natürliche Zahl, die keine Quadratzahl ist.
(1) $K := \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$ ist ein Unterkörper von $\mathbb{R}$ und ein Oberkörper von $\mathbb{Q}$ und mit den Verknüpfungen

$$(\alpha, \beta) \mapsto \alpha + \beta : K \times K \to K \quad \text{und} \quad (x, \alpha) \mapsto x\alpha : \mathbb{Q} \times K \to K$$

ein $\mathbb{Q}$-Vektorraum. Es gilt $\dim_{\mathbb{Q}}(K) = 2$, und $\{1, \sqrt{d}\}$ ist eine $\mathbb{Q}$-Basis von K, d.h. eine Basis des $\mathbb{Q}$-Vektorraums K.
(2) Die Abbildung

$$\sigma_d : K \to K \quad \text{mit} \quad \sigma_d(x + y\sqrt{d}) \;:=\; x - y\sqrt{d} \quad \text{für alle } x, y \in \mathbb{Q}$$

ist ein $\mathbb{Q}$-Automorphismus des Körpers K, d.h. σ_d ist bijektiv, für jedes $x \in \mathbb{Q}$ ist $\sigma_d(x) = x$, und für alle α, $\beta \in K$ gilt $\sigma_d(\alpha + \beta) = \sigma_d(\alpha) + \sigma_d(\beta)$ und $\sigma_d(\alpha\beta) = \sigma_d(\alpha)\sigma_d(\beta)$. σ_d ist der einzige $\mathbb{Q}$-Automorphismus $\neq \mathrm{id}_K$ von K.

Beweis: (a) Es gilt $\mathbb{Q} \subset K$, und für alle x_1, y_1, x_2, $y_2 \in \mathbb{Q}$ gilt

$$\begin{aligned}(x_1 + y_1\sqrt{d}) + (x_2 + y_2\sqrt{d}) &= (x_1 + x_2) + (y_1 + y_2)\sqrt{d} \in K \quad \text{und} \\ (x_1 + y_1\sqrt{d}) \cdot (x_2 + y_2\sqrt{d}) &= (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d} \in K.\end{aligned}$$

Also ist K ein Unterring von $\mathbb{R}$, und $\mathbb{Q}$ ist ein Unterkörper von K. Daß K mit den in $\mathbb{R}$ gegebenen Verknüpfungen $+$ und $\cdot$ ein $\mathbb{Q}$-Vektorraum ist und daß $\{1, \sqrt{d}\}$ darin ein Erzeugendensystem ist, ist klar.
(b) Es seien x, $y \in \mathbb{Q}$ nicht beide Null, und es gelte $x + y\sqrt{d} = 0$. Dann gilt $x \neq 0$ und $y \neq 0$, und es gibt ein $a \in \mathbb{N}$ mit $ax \in \mathbb{Z}$ und $ay \in \mathbb{Z}$. Es ist $(ax)^2 = d(ay)^2$, und somit gilt für jede Primzahl p: Es ist

$$2v_p(ax) = v_p\big((ax)^2\big) = v_p\big(d(ay)^2\big) = v_p(d) + 2v_p(ay),$$

und daher ist $v_p(d)$ gerade. Dies ist aber nicht möglich, da d keine Quadratzahl ist. Also sind 1 und $\sqrt{d}$ im $\mathbb{Q}$-Vektorraum K linear unabhängig, und somit ist $\{1, \sqrt{d}\}$ eine $\mathbb{Q}$-Basis von K.
(c) Für jedes $\alpha \in K \setminus \{0\}$ gilt: Es gibt x, $y \in \mathbb{Q}$ mit $\alpha = x + y\sqrt{d}$, wegen $\alpha \neq 0$ sind x und y nicht beide Null, und daher gilt $x - y\sqrt{d} \neq 0$ und

$$\frac{1}{\alpha} = \frac{1}{x + y\sqrt{d}} = \frac{x - y\sqrt{d}}{(x + y\sqrt{d})(x - y\sqrt{d})} = \frac{x}{x^2 - dy^2} + \frac{-y}{x^2 - dy^2}\sqrt{d} \in K.$$

Also ist K ein Unterkörper von $\mathbb{R}$.
(d) Daß die Abbildung $\sigma_d : K \to K$ ein $\mathbb{Q}$-Automorphismus des Körpers K ist, rechnet man ohne Schwierigkeiten nach. Ist τ ein $\mathbb{Q}$-Automorphismus des Körpers K, so gilt

$$\big(\tau(\sqrt{d})\big)^2 = \tau\big((\sqrt{d})^2\big) = \tau(d) = d,$$

also $\tau(\sqrt{d}) = \sqrt{d}$ oder $\tau(\sqrt{d}) = -\sqrt{d}$, also $\tau = \mathrm{id}_K$ oder $\tau = \sigma_d$.
(3) Der in (1) beschriebene Körper K wird mit $\mathbb{Q}(\sqrt{d})$ bezeichnet; er ist der kleinste Unterkörper des Körpers $\mathbb{R}$, der $\mathbb{Q}$ umfaßt und $\sqrt{d}$ enthält.

(16.8) Bemerkung: Es sei $\alpha \in \mathbb{R}$ eine quadratische Irrationalzahl. Dann gibt es ganze Zahlen a, b, c mit $a \neq 0$ und mit: α ist Nullstelle des Polynoms $f := aT^2 + bT + c$. Wegen $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ist $d := b^2 - 4ac$ eine natürliche Zahl, die keine Quadratzahl ist, und es gilt

$$\alpha = \frac{-b + \sqrt{d}}{2a} \quad \text{oder} \quad \alpha = \frac{-b - \sqrt{d}}{2a}.$$

Im ersten Fall setzt man $v := -b$ und $w := 2a$, und im zweiten Fall setzt man $v := b$ und $w := -2a$. In jedem Fall gilt $v \in \mathbb{Z}$, $w \in \mathbb{Z} \setminus \{0\}$ und

$$\alpha = \frac{v + \sqrt{d}}{w} \quad \text{und} \quad w \,|\, d - v^2.$$

Das Polynom f besitzt noch eine Nullstelle $\beta \neq \alpha$, nämlich

$$\beta = \frac{v - \sqrt{d}}{w} = \sigma_d(\alpha),$$

wobei σ_d der nichttriviale $\mathbb{Q}$-Automorphismus des Körpers $\mathbb{Q}(\sqrt{d})$ ist.

(16.9) Satz (J. L. Lagrange 1770): *Es sei $\alpha \in \mathbb{R}$ eine quadratische Irrationalzahl. Dann ist der Kettenbruch für α periodisch.*

Beweis: Es sei $\alpha = [a_0, a_1, \ldots, a_n, a_{n+1}, \ldots]$ der Kettenbruch für α, und für jedes $n \in \mathbb{N}_0$ sei $\alpha_n := [a_n, a_{n+1}, a_{n+2}, \ldots]$ der n-te vollständige Quotient dieses Kettenbruchs.

(1) Es gibt eine natürliche Zahl d, die keine Quadratzahl ist, und ganze Zahlen v_0 und w_0 mit $w_0 \neq 0$, mit $w_0 \,|\, d - v_0^2$ und mit

$$\alpha_0 = \alpha = \frac{v_0 + \sqrt{d}}{w_0}$$

(vgl. (16.8)). Es seien $(v_n)_{n \geq 0}$ und $(w_n)_{n \geq 0}$ die Folgen in $\mathbb{Q}$ mit

$$v_{n+1} := a_n w_n - v_n \quad \text{und} \quad w_{n+1} := \frac{d - v_{n+1}^2}{w_n} \quad \text{für jedes } n \in \mathbb{N}_0.$$

Für jedes $n \in \mathbb{N}_0$ gilt $v_n \in \mathbb{Z}$, $w_n \in \mathbb{Z}$, $w_n \neq 0$ und $w_n \,|\, d - v_n^2$, wie man durch Induktion beweist: Für $n = 0$ ist nichts zu zeigen, und ist für $n \in \mathbb{N}_0$ bereits gezeigt, daß $v_n \in \mathbb{Z}$, $w_n \in \mathbb{Z}$, $w_n \neq 0$ und $w_n \,|\, d - v_n^2$ gilt, so folgt: $v_{n+1} = a_n w_n - v_n$ und

$$\begin{aligned} w_{n+1} &= \frac{d - v_{n+1}^2}{w_n} = \frac{1}{w_n}\left(d - a_n^2 w_n^2 + 2a_n v_n w_n - v_n^2\right) = \\ &= \frac{d - v_n^2}{w_n} - a_n^2 w_n + 2a_n v_n \end{aligned}$$

sind ganze Zahlen, und weil d keine Quadratzahl ist, gilt $d - v_{n+1}^2 \neq 0$ und daher $w_{n+1} \neq 0$, und wegen $w_n w_{n+1} = d - v_{n+1}^2$ ist schließlich w_{n+1} ein Teiler von $d - v_{n+1}^2$.

(2) Für jedes $n \in \mathbb{N}_0$ ist

$$\alpha_n = \frac{v_n + \sqrt{d}}{w_n}.$$

Auch dies beweist man durch Induktion: Für $n = 0$ ist nichts zu zeigen, und ist für $n \in \mathbb{N}_0$ bereits bewiesen, daß $\alpha_n = (v_n + \sqrt{d})/w_n$ gilt, so folgt

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} = \frac{1}{\dfrac{v_n + \sqrt{d}}{w_n} - a_n} = \frac{w_n}{(v_n + \sqrt{d}) - w_n a_n} =$$

$$= \frac{w_n}{\sqrt{d} - v_{n+1}} = \frac{w_n\,(\sqrt{d} + v_{n+1})}{d - v_{n+1}^2} = \frac{v_{n+1} + \sqrt{d}}{w_{n+1}}.$$

(3) Es sei $(r_n/s_n)_{n \geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs für α, und es sei σ_d der nichttriviale $\mathbb{Q}$-Automorphismus des Körpers $\mathbb{Q}(\sqrt{d})$. Für jedes $n \in \mathbb{N}$ mit $n \geq 2$ gilt

$$\alpha = [\,a_0, a_1, \ldots, a_{n-1}, \alpha_n\,] = \frac{\alpha_n r_{n-1} + r_{n-2}}{\alpha_n s_{n-1} + s_{n-2}}$$

[vgl. (13.2)(4)], also

$$\alpha_n = -\frac{\alpha s_{n-2} - r_{n-2}}{\alpha s_{n-1} - r_{n-1}} = -\frac{s_{n-2}}{s_{n-1}} \cdot \frac{\alpha - r_{n-2}/s_{n-2}}{\alpha - r_{n-1}/s_{n-1}}$$

und daher

$$\sigma_d(\alpha_n) = -\frac{s_{n-2}}{s_{n-1}} \cdot \frac{\sigma_d(\alpha) - r_{n-2}/s_{n-2}}{\sigma_d(\alpha) - r_{n-1}/s_{n-1}}.$$

Die Folge $(r_n/s_n)_{n \geq 0}$ konvergiert gegen α, und wegen $\alpha \notin \mathbb{Q}$ ist $\sigma_d(\alpha) \neq \alpha$. Also konvergiert die Folge

$$\left(\frac{\sigma_d(\alpha) - r_{n-2}/s_{n-2}}{\sigma_d(\alpha) - r_{n-1}/s_{n-1}}\right)_{n \geq 2}$$

gegen 1. Weil s_{n-2}/s_{n-1} für jedes $n \geq 2$ positiv ist, gibt es daher ein $n_0 \in \mathbb{N}$ mit $n_0 \geq 2$ und mit: Für jedes $n \geq n_0$ ist

$$\sigma_d(\alpha_n) = -\frac{s_{n-2}}{s_{n-1}} \cdot \frac{\sigma_d(\alpha) - r_{n-2}/s_{n-2}}{\sigma_d(\alpha) - r_{n-1}/s_{n-1}} < 0.$$

Für jedes $n \geq n_0$ gilt $\alpha_n \geq \lfloor \alpha_n \rfloor = a_n > 0$ und daher

$$\frac{2\sqrt{d}}{w_n} = \frac{v_n + \sqrt{d}}{w_n} - \frac{v_n - \sqrt{d}}{w_n} = \alpha_n - \sigma_d(\alpha_n) > 0,$$

also $w_n > 0$. Für jedes $n \geq n_0 + 1$ gilt daher

$$1 \leq w_n \leq w_{n-1}w_n = d - v_n^2 \leq d$$

und

$$0 \leq v_n^2 < v_n^2 + w_{n-1}w_n = d.$$

Es gibt also nur endlich viele verschiedene Paare (v_n, w_n) mit $n \geq n_0+1$. Somit hat die Menge $\{(v_n, w_n) \mid n \in \mathbb{N}_0\}$ nur endlich viele verschiedene Elemente, und es existieren daher ein $k \in \mathbb{N}$ und ein $l \in \mathbb{N}$ mit $k \geq 2$ und mit $v_k = v_{k+l}$ und $w_k = w_{k+l}$, also mit

$$\alpha_k = \frac{v_k + \sqrt{d}}{w_k} = \frac{v_{k+l} + \sqrt{d}}{w_{k+l}} = \alpha_{k+l}.$$

Hierfür gilt

$$\alpha_k = [a_k, a_{k+1}, \ldots, a_{k+l-1}, \alpha_{k+l}] = [a_k, a_{k+1}, \ldots, a_{k+l-1}, \alpha_k]$$

und

$$\begin{aligned}\alpha &= [a_0, a_1, \ldots, a_{k-1}, \alpha_k] = \\ &= [a_0, a_1, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_{k+l-1}, \alpha_k] = \\ &= [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}].\end{aligned}$$

(16.10) Es sei $\alpha \in \mathbb{R}$ eine quadratische Irrationalzahl. Der Beweis in (16.9) liefert das folgende Verfahren zur Berechnung des periodischen Kettenbruchs für α; es berechnet die kürzeste Vorperiode $(a_0, a_1, \ldots, a_{k-1})$ und die daran anschließende primitive Periode $(a_k, a_{k+1}, \ldots, a_{k+l-1})$ dieses Kettenbruchs:

(PKB1) Man bestimmt $d \in \mathbb{N}$ und $v_0, w_0 \in \mathbb{Z}$ mit $w_0 \neq 0$, mit $w_0 \mid d - v_0^2$ und mit

$$\alpha = \frac{v_0 + \sqrt{d}}{w_0}$$

und setzt $a_0 := \lfloor \alpha \rfloor$ und $n := 1$.

(PKB2) Man setzt

$$v_n := a_{n-1}w_{n-1} - v_{n-1} \quad \text{und} \quad w_n := \frac{d - v_n^2}{w_{n-1}}.$$

Wenn es ein $k \in \{0, 1, \ldots, n-1\}$ mit $v_n = v_k$ und $w_n = w_k$ gibt, so gibt man $(a_0, a_1, \ldots, a_{k-1})$ als Vorperiode und $(a_k, a_{k+1}, \ldots, a_{n-1})$ als Periode aus und bricht ab.

(PKB3) Man setzt

$$a_n \;:=\; \left\lfloor \frac{v_n + \sqrt{d}}{w_n} \right\rfloor \quad \text{und} \quad n \;:=\; n+1$$

und geht zu (PKB2).

(16.11) Satz (E. Galois 1829): *Es seien a, b, $c \in \mathbb{Z}$, und es gelte: Es ist $a \neq 0$, und $d := b^2 - 4ac$ ist eine natürliche Zahl, die keine Quadratzahl ist; es seien α, $\beta \in \mathbb{R}$ die beiden Nullstellen des Polynoms $aT^2 + bT + c \in \mathbb{Z}[T]$. Es gilt: Der Kettenbruch für α ist dann und nur dann rein-periodisch, wenn $\alpha > 1$ und $-1 < \beta < 0$ gilt.*

Beweis: Es sei $\alpha = [\,a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots\,]$ der Kettenbruch für α.
(1) Es gelte: Der Kettenbruch für α ist rein-periodisch. Es gibt dann ein $l \in \mathbb{N}$ mit

$$\alpha \;=\; [\,\overline{a_0, a_1, \ldots, a_{l-1}}\,].$$

(a) Für jedes $n \in \mathbb{N}$ ist $a_n \in \mathbb{N}$, und wegen $a_0 = a_l$ ist auch $a_0 \in \mathbb{N}$. Wegen $\alpha \geq \lfloor \alpha \rfloor = a_0 \geq 1$ und $\alpha \notin \mathbb{Q}$ gilt $\alpha > 1$.
(b) Es sei $(r_n/s_n)_{n \geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs für α. Es gilt $r_0 = a_0 \geq 1 =: r_{-1}$, und für jedes $n \in \mathbb{N}$ gilt $r_n > r_{n-1}$, denn es ist $r_1 = a_1 r_0 + r_1 > a_1 r_0 \geq r_0$, und ist für eine natürliche Zahl n bereits gezeigt, daß $r_n > r_{n-1} > \cdots > r_0$ gilt, so folgt $r_{n+1} = a_{n+1} r_n + r_{n-1} > a_{n+1} r_n \geq r_n$. Es gilt $s_0 = 1 > 0 =: s_1$, und für jedes $n \in \mathbb{N}$ ist $s_n \geq s_{n-1}$ (vgl. (13.3)(2)).
(c) Es sei σ_d der nichttriviale $\mathbb{Q}$-Automorphismus des Körpers $\mathbb{Q}(\sqrt{d})$. Es gilt

$$\alpha \;=\; [\,\overline{a_0, a_1, \ldots, a_{l-1}}\,] \;=\; [\,a_0, a_1, \ldots, a_{l-1}, \alpha\,] \;=\; \frac{\alpha r_{l-1} + r_{l-2}}{\alpha s_{l-1} + s_{l-2}}$$

und daher

$$\beta \;=\; \sigma_d(\alpha) \;=\; \sigma_d\Big(\frac{\alpha r_{l-1} + r_{l-2}}{\alpha s_{l-1} + s_{l-2}}\Big) \;=\; \frac{\sigma_d(\alpha) r_{l-1} + r_{l-2}}{\sigma_d(\alpha) s_{l-1} + s_{l-2}} \;=\; \frac{\beta r_{l-1} + r_{l-2}}{\beta s_{l-1} + s_{l-2}}.$$

Also sind α und β Nullstellen der Polynomfunktion

$$g : \mathbb{R} \to \mathbb{R} \quad \text{mit} \quad g(t) \;:=\; s_{l-1} t^2 + (s_{l-2} - r_{l-1})\, t - r_{l-2} \quad \text{für jedes } t \in \mathbb{R}.$$

Aus (b) folgt, daß

$$g(-1) \;=\; (s_{l-1} - s_{l-2}) + (r_{l-1} - r_{l-2}) \;>\; 0 \quad \text{und} \quad g(0) \;=\; -r_{l-2} \;<\; 0$$

gilt, und daher liegt nach dem Zwischenwertsatz im Intervall $]-1, 0[$ eine Nullstelle von f. Da g außer α und β keine Nullstellen besitzt und $\alpha > 1$ ist, gilt somit $-1 < \beta < 0$.

(2) Es gelte $\alpha > 1$ und $-1 < \beta < 0$. Es ist $a_0 = \lfloor \alpha \rfloor \geq 1$, und daher ist $a_n \in \mathbb{N}$ für jedes $n \in \mathbb{N}_0$. Für jedes $n \in \mathbb{N}_0$ sei $\alpha_n := [\,a_n, a_{n+1}, a_{n+2}, \dots\,]$ der n-te vollständige Quotient des Kettenbruchs für α.
(a) Für jedes $n \in \mathbb{N}_0$ ist $-1 < \sigma_d(\alpha_n) < 0$. Denn nach Voraussetzung gilt $-1 < \sigma_d(\alpha_0) = \sigma_d(\alpha) = \beta < 0$, und ist für ein $n \in \mathbb{N}_0$ bereits gezeigt, daß $-1 < \sigma_d(\alpha_n) < 0$ gilt, so gilt wegen $\alpha_n = a_n + 1/\alpha_{n+1}$

$$\frac{1}{\sigma_d(\alpha_{n+1})} \;=\; \sigma_d\Big(\frac{1}{\alpha_{n+1}}\Big) \;=\; \sigma_d(\alpha_n - a_n) \;=\; \sigma_d(\alpha_n) - a_n \;<\; -\,a_n \;\leq\; -1$$

und daher $-1 < \sigma_d(\alpha_{n+1}) < 0$.
(b) Für jedes $n \in \mathbb{N}_0$ gilt nach (a)

$$a_n \;<\; -\frac{1}{\sigma_d(\alpha_{n+1})} \;=\; a_n - \sigma_d(\alpha_n) \;<\; a_n + 1,$$

also

$$a_n \;=\; \Big\lfloor -\frac{1}{\sigma_d(\alpha_{n+1})} \Big\rfloor .$$

Nach (16.9) ist der Kettenbruch für α periodisch, also gibt es ein $k \in \mathbb{N}_0$ und ein $l \in \mathbb{N}$ mit

$$\alpha \;=\; [\,a_0, a_1, \dots, a_{k-1}, \overline{a_k, a_{k+1}, \dots, a_{k+l-1}}\,].$$

Ist dabei $k = 0$, so gilt

$$\alpha \;=\; [\,\overline{a_0, a_1, \dots, a_{l-1}}\,],$$

und der Kettenbruch für α ist somit rein-periodisch. Ist $k > 0$, so gilt

$$\alpha_{k+l} \;=\; [\,a_{k+l}, a_{k+l+1}, a_{k+l+2}, \dots\,] \;=\; [\,a_k, a_{k+1}, a_{k+2}, \dots\,] \;=\; \alpha_k,$$

also $\sigma_d(\alpha_{k+l}) = \sigma_d(\alpha_k)$ und daher

$$a_{k+l-1} \;=\; \Big\lfloor -\frac{1}{\sigma_d(\alpha_{k+l})} \Big\rfloor \;=\; \Big\lfloor -\frac{1}{\sigma_d(\alpha_k)} \Big\rfloor \;=\; a_{k-1}$$

und

$$\alpha_{k+l-1} \;=\; a_{k+l-1} + \frac{1}{\alpha_{k+l}} \;=\; a_{k-1} + \frac{1}{\alpha_k} \;=\; \alpha_{k-1},$$

und die Fortsetzung des Verfahrens liefert $\alpha_{k+l-2} = \alpha_{k-2}, \dots, \alpha_l = \alpha_0 = \alpha$, also schließlich

$$\alpha \;=\; [\,a_0, a_1, \dots, a_{l-1}, \alpha_l\,] \;=\; [\,a_0, a_1, \dots, a_{l-1}, \alpha\,] \;=\; [\,\overline{a_0, a_1, \dots, a_{l-1}}\,].$$

(16.12) Bemerkung: Es sei α eine irrationale reelle Zahl mit einer periodischen Kettenbruchentwicklung

$$\alpha = [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}].$$

Das folgende Verfahren erlaubt es, α aus seiner Kettenbruchentwicklung zu berechnen [vgl. dazu auch (16.6)]:

(a) Es sei $\alpha_k := [\overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}]$, und es sei $(r'_n/s'_n)_{n\geq 0}$ die Folge der Näherungsbrüche dieses Kettenbruchs; es seien $r'_{-1} := 1$ und $s'_{-1} := 0$. Wegen

$$\alpha_k = [a_k, a_{k+1}, \ldots, a_{k+l-1}, \alpha_k] = \frac{\alpha_k r'_{l-1} + r'_{l-2}}{\alpha_k s'_{l-1} + s'_{l-2}}$$

ist α_k eine Nullstelle des quadratischen Polynoms

$$f := s'_{l-1} T^2 + (s'_{l-2} - r'_{l-1}) T - r'_{l-2} \in \mathbb{Z}[T].$$

Da der Kettenbruch für α_k rein-periodisch ist, gilt nach (16.11): Es ist $\alpha_k > 1$, wogegen die zweite Nullstelle von f negativ ist. Damit kann man α_k aus f berechnen.

(b) Es sei $(r_n/s_n)_{n\geq 0}$ die Folge der Näherungsbrüche des Kettenbruchs für α, und es seien $r_{-2} := 0$, $r_{-1} := 1$ und $s_{-2} := 1$, $s_{-1} := 0$. Es gilt

$$\alpha = [a_0, a_1, \ldots, a_{k-1}, \alpha_k] = \frac{\alpha_k r_{k-1} + r_{k-2}}{\alpha_k s_{k-1} + s_{k-2}},$$

und damit kann man α aus α_k berechnen.

(16.13) Satz (E. Galois 1829): *Es seien a, b, $c \in \mathbb{Z}$, und es gelte: Es ist $a \neq 0$, und $d := b^2 - 4ac$ ist eine natürliche Zahl, die keine Quadratzahl ist; es seien α, $\beta \in \mathbb{R}$ die beiden Nullstellen des Polynoms $aT^2 + bT + c \in \mathbb{Z}[T]$, es gelte $\alpha > 1$ und $-1 < \beta < 0$, und es sei*

$$\alpha = [\overline{a_0, a_1, \ldots, a_{l-2}, a_{l-1}}]$$

die nach (16.11) *rein-periodische Kettenbruchentwicklung von α. Dann gilt*

$$-\frac{1}{\beta} = [\overline{a_{l-1}, a_{l-2}, \ldots, a_1, a_0}].$$

Beweis: Es sei σ_d der nichttriviale $\mathbb{Q}$-Automorphismus des Körpers $\mathbb{Q}(\sqrt{d})$, und für jedes $n \in \mathbb{N}_0$ sei $\alpha_n = [a_n, a_{n+1}, a_{n+2}, \ldots]$ der n-te vollständige Quotient des Kettenbruchs für α. Für jedes $n \in \mathbb{N}_0$ gilt: Es ist $a_n = \lfloor \alpha_n \rfloor$

und $\alpha_{n+1} = 1/(\alpha_n - a_n)$, und wie im Beweis von (16.11) folgt $a_n \in \mathbb{N}$ und $-1 < \sigma_d(\alpha_n) < 0$. Den Kettenbruch

$$-\frac{1}{\beta} = [c_0, c_1, \dots, c_n, c_{n+1}, \dots]$$

erhält man so: Man setzt $\gamma_0 := -1/\beta$, $c_0 := \lfloor \gamma_0 \rfloor$ und für jedes $n \in \mathbb{N}_0$

$$\gamma_{n+1} := \frac{1}{\gamma_n - c_n} \quad \text{und} \quad c_{n+1} := \lfloor \gamma_{n+1} \rfloor .$$

(a) Für jedes $j \in \{0, 1, \dots, l-1\}$ gilt

$$\gamma_j = -\frac{1}{\sigma_d(\alpha_{l-j})} \quad \text{und} \quad c_j = a_{l-j-1}.$$

Dies beweist man durch Induktion: Es gilt

$$\alpha = \alpha_0 = \alpha_l = \frac{1}{\alpha_{l-1} - a_{l-1}}$$

und daher

$$\gamma_0 = -\frac{1}{\beta} = -\frac{1}{\sigma_d(\alpha)} = -\sigma_d(\alpha_{l-1} - a_{l-1}) = -\sigma_d(\alpha_{l-1}) + a_{l-1},$$

und wegen $-1 < \sigma(\alpha_{l-1}) < 0$ folgt: Es ist $c_0 = \lfloor \gamma_0 \rfloor = a_{l-1}$. Es sei $j \in \{0, 1, \dots, l-2\}$, und es sei bereits bewiesen, daß $\gamma_j = -1/\sigma_d(\alpha_{l-j})$ und $c_j = a_{l-j-1}$ gilt. Wegen

$$\alpha_{l-j} = \frac{1}{\alpha_{l-j-1} - a_{l-j-1}}$$

gilt

$$\sigma_d(\alpha_{l-j}) = \frac{1}{\sigma_d(\alpha_{l-j-1} - a_{l-j-1})} = \frac{1}{\sigma_d(\alpha_{l-j-1}) - a_{l-j-1}}$$

und daher

$$\gamma_{j+1} = \frac{1}{\gamma_j - c_j} = \frac{1}{-\dfrac{1}{\sigma_d(\alpha_{l-j})} - a_{l-j-1}} = -\frac{1}{\sigma_d(\alpha_{l-j-1})},$$

und wegen

$$\alpha_{l-j-1} = \frac{1}{\alpha_{l-j-2} - a_{l-j-2}}$$

folgt

$$\gamma_{j+1} = -\frac{1}{\sigma_d(\alpha_{l-j-1})} = -\sigma_d(\alpha_{l-j-2} - a_{l-j-2}) = -\sigma_d(\alpha_{l-j-2}) + a_{l-j-2}.$$

Wegen $-1 < \sigma_d(\alpha_{l-j-2}) < 0$ folgt: Es ist $c_{j+1} = \lfloor \gamma_{j+1} \rfloor = a_{l-j-2}$.
(b) Nach (a) gilt

$$-\frac{1}{\beta} = \gamma = [c_0, c_1, \ldots, c_{l-2}, c_{l-1}, \gamma_l] = [a_{l-1}, a_{l-2}, \ldots, a_1, a_0, \gamma_l],$$

und es ist

$$\gamma_l = \frac{1}{\gamma_{l-1} - c_{l-1}} = \frac{1}{-\dfrac{1}{\sigma_d(\alpha_1)} - a_0} = \frac{1}{-\sigma_d(\alpha_0) + a_0 - a_0} =$$

$$= -\frac{1}{\sigma_d(\alpha_0)} = -\frac{1}{\sigma_d(\alpha)} = -\frac{1}{\beta},$$

und daher gilt

$$-\frac{1}{\beta} = \left[a_{l-1}, a_{l-2}, \ldots, a_1, a_0, -\frac{1}{\beta}\right] = [\overline{a_{l-1}, a_{l-2}, \ldots, a_1, a_0}].$$

(16.14) Satz: *Es sei d eine natürliche Zahl, die keine Quadratzahl ist. Es sei*

$$\sqrt{d} = [a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$$

der Kettenbruch für $\sqrt{d}$, und es sei l die Länge einer primitiven Periode dieses Kettenbruchs. Es gilt: Der Kettenbruch ist nicht periodisch, (a_0) ist Vorperiode, $(a_1, a_2, \ldots, a_l)$ ist primitive Periode, es ist $a_l = 2a_0$, und für jedes $j \in \{1, 2, \ldots, l-1\}$ ist $a_j = a_{l-j}$. Der Kettenbruch hat also die folgende Gestalt: Ist l gerade, so ist

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{l/2-2}, a_{l/2-1}, a_{l/2}, a_{l/2-1}, a_{l/2-2} \ldots, a_2, a_1, 2a_0}],$$

und ist l ungerade, so ist

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{(l-1)/2-1}, a_{(l-1)/2}, a_{(l-1)/2}, a_{(l-1)/2-1}, \ldots, a_2, a_1, 2a_0}].$$

Beweis: Wegen $-1/\sigma_d(\sqrt{d}) = 1/\sqrt{d} > 0$ ist der Kettenbruch für $\sqrt{d}$ nicht rein-periodisch (vgl. (16.11)). Es ist $a_0 = \lfloor \sqrt{d} \rfloor \in \mathbb{N}$, und

$$\alpha := \frac{1}{\sqrt{d} - a_0} = \frac{a_0 + \sqrt{d}}{d - a_0^2} \in \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$$

ist eine Nullstelle des Polynoms

$$f := (d - a_0^2)\,T^2 - 2a_0\,T - 1 \ \in\ \mathbb{Z}[T].$$

Es gilt $\alpha > 1$, und für

$$\beta := \sigma_d(\alpha) = \frac{a_0 - \sqrt{d}}{d - a_0^2} = -\frac{1}{a_0 + \sqrt{d}}$$

gilt $f = (d - a_0^2)(T - \alpha)(T - \beta)$ und $-1 < \beta < 0$. Nach (16.11) gibt es ein $l \in \mathbb{N}$ und $a_1, a_2, \ldots, a_l \in \mathbb{N}$ mit

$$\alpha = [\,\overline{a_1, a_2, \ldots, a_l}\,],$$

und damit gilt

$$\sqrt{d} = a_0 + \frac{1}{\alpha} = a_0 + \frac{1}{[\,\overline{a_1, a_2, \ldots, a_l}\,]} = [\,a_0, \overline{a_1, a_2, \ldots, a_l}\,].$$

Es gilt einerseits

$$a_0 + \sqrt{d} = 2a_0 + \frac{1}{\alpha} = [\,2a_0, \overline{a_1, a_2, \ldots, a_{l-1}, a_l}\,]$$

und andererseits

$$a_0 + \sqrt{d} = -\frac{1}{\beta} \overset{(16.13)}{=} [\,\overline{a_l, a_{l-1}, \ldots, a_2, a_1}\,],$$

und daher gilt wegen (15.4): Es ist $a_l = 2a_0$, und für jedes $j \in \{1, 2, \ldots, l-1\}$ ist $a_{l-j} = a_j$.

(16.15) Es sei d eine natürliche Zahl, die keine Quadratzahl ist. Es sei

$$\sqrt{d} = [\,a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots\,]$$

der Kettenbruch für $\sqrt{d}$, für jedes $n \in \mathbb{N}$ seien $\alpha_n := [\,a_n, a_{n+1}, a_{n+2}, \ldots\,]$ der n-te vollständige Quotient und r_n/s_n der n-te Näherungsbruch dieses Kettenbruchs, und es seien $r_{-1} := 1$ und $s_{-1} := 0$. Es seien $(v_n)_{n \geq 0}$ und $(w_n)_{n \geq 0}$ die Folgen in $\mathbb{Q}$ mit $v_0 := 0$ und $w_0 := 1$ und mit

$$v_{n+1} := a_n w_n - v_n \quad \text{und} \quad w_{n+1} := \frac{d - v_{n+1}^2}{w_n} \quad \text{für jedes } n \in \mathbb{N}_0.$$

In diesem Abschnitt werden einige Eigenschaften dieser Folgen zusammengestellt.

(1) Im Beweis in (16.9) wurde gezeigt: Für jedes $n \in \mathbb{N}_0$ gilt $v_n \in \mathbb{Z}$, $w_n \in \mathbb{Z}$, $w_n \neq 0$, $w_n \mid d - v_n^2$ und

$$\alpha_n = \frac{v_n + \sqrt{d}}{w_n}.$$

(2) Für jedes $n \in \mathbb{N}$ gilt

$$1 \leq w_{n-1} < 2\sqrt{d} \quad \text{und} \quad 1 \leq v_n < \sqrt{d}.$$

Dies beweist man durch Induktion nach n: Es ist $w_0 = 1 < 2\sqrt{d}$, und wegen $v_1 = a_0 w_0 - v_0 = a_0 = \lfloor\sqrt{d}\rfloor$ gilt $1 \leq v_1 < \sqrt{d}$. Es sei n eine natürliche Zahl, für die bereits bewiesen ist, daß $1 \leq w_{n-1} < 2\sqrt{d}$ und $1 \leq v_n < \sqrt{d}$ gilt. Dann ist $v_n + \sqrt{d} > \sqrt{d} > 0$, und wegen $\alpha_n \geq \lfloor\alpha_n\rfloor = a_n \geq 1$ und $\alpha_n \notin \mathbb{Q}$ gilt

$$\frac{v_n + \sqrt{d}}{w_n} = \alpha_n > 1,$$

und daraus folgt $0 < w_n < v_n + \sqrt{d} < 2\sqrt{d}$. Wegen $w_n \in \mathbb{Z}$ gilt daher $w_n \geq 1$. Wegen $w_n > 0$ und $\alpha_{n+1} \geq \lfloor\alpha_{n+1}\rfloor = a_{n+1} > 0$ gilt

$$\begin{aligned}\sqrt{d} - v_{n+1} &= \frac{(\sqrt{d} - v_{n+1})(\sqrt{d} + v_{n+1})}{\sqrt{d} + v_{n+1}} = \frac{d - v_{n+1}^2}{\sqrt{d} + v_{n+1}} = \\ &= \frac{d - v_{n+1}^2}{w_{n+1}} \cdot \frac{w_{n+1}}{v_{n+1} + \sqrt{d}} = w_n \cdot \frac{1}{\alpha_{n+1}} > 0,\end{aligned}$$

und daher ist $v_{n+1} < \sqrt{d}$.

Angenommen, es ist $v_{n+1} \leq 0$. Wegen $a_n \geq 1$ und $w_n \geq 1$ gilt dann

$$w_n \leq a_n w_n = v_n + (a_n w_n - v_n) = v_n + v_{n+1} \leq v_n < \sqrt{d}$$

und daher

$$\begin{aligned}\alpha_n - a_n &= \frac{v_n + \sqrt{d}}{w_n} - a_n = \frac{1}{w_n}\big(\sqrt{d} - (a_n w_n - v_n)\big) = \\ &= \frac{\sqrt{d} - v_{n+1}}{w_n} \geq \frac{\sqrt{d}}{w_n} > 1,\end{aligned}$$

im Widerspruch dazu, daß $\alpha_n - a_n = \alpha_n - \lfloor\alpha_n\rfloor < 1$ gilt. Also ist $v_{n+1} > 0$, und wegen $v_{n+1} \in \mathbb{Z}$ folgt $v_{n+1} \geq 1$.

(3) Nach (2) gilt

$$\#(\{\alpha_n \mid n \in \mathbb{N}\}) = \#(\{(v_n, w_n) \mid n \in \mathbb{N}\}) < 2d,$$

und daher hat eine primitive Periode des Kettenbruchs für $\sqrt{d}$ höchstens die Länge $2d-1$.
(4) Für jedes $n \in \mathbb{N}$ gilt

$$1 \leq a_n < \alpha_n = \frac{v_n + \sqrt{d}}{w_n} \leq v_n + \sqrt{d} < 2\sqrt{d}.$$

(5) Für jedes $n \in \mathbb{N}_0$ gilt $w_{n+2} = w_n + a_{n+1}(v_{n+1} - v_{n+2})$.
Beweis: Für jedes $n \in \mathbb{N}_0$ gilt $w_n w_{n+1} = d - v_{n+1}^2$ und $w_{n+1}w_{n+2} = d - v_{n+2}^2$ und daher

$$\begin{aligned} w_{n+1}(w_{n+2} - w_n) &= -v_{n+2}^2 + v_{n+1}^2 = (v_{n+1} + v_{n+2})(v_{n+1} - v_{n+2}) = \\ &= a_{n+1}w_{n+1}(v_{n+1} - v_{n+2}), \end{aligned}$$

und es ist $w_{n+1} \neq 0$.
(6) Für jedes $n \in \mathbb{N}_0$ gilt

$$v_{n+1}r_n + w_{n+1}r_{n-1} = ds_n \quad \text{und} \quad v_{n+1}s_n + w_{n+1}s_{n-1} = r_n$$

und

$$r_n^2 - ds_n^2 = (-1)^{n+1}w_{n+1}.$$

Beweis: Es sei $n \in \mathbb{N}_0$. Es gilt $\alpha_{n+1} = (v_{n+1} + \sqrt{d})/w_{n+1}$ und

$$\begin{aligned} \sqrt{d} &= [\,a_0, a_1, \ldots, a_n, \alpha_{n+1}\,] = \frac{\alpha_{n+1}r_n + r_{n-1}}{\alpha_{n+1}s_n + s_{n-1}} = \\ &= \frac{(v_{n+1} + \sqrt{d})\,r_n + w_{n+1}r_{n-1}}{(v_{n+1} + \sqrt{d})\,s_n + w_{n+1}s_{n-1}} \end{aligned}$$

und daher

$$\begin{aligned} (v_{n+1}r_n + w_{n+1}r_{n-1}) + r_n\sqrt{d} &= \big((v_{n+1} + \sqrt{d})s_n + w_{n+1}s_{n-1}\big)\sqrt{d} = \\ &= ds_n + (v_{n+1}s_n + w_{n+1}s_{n-1})\sqrt{d}. \end{aligned}$$

Da $\{1, \sqrt{d}\}$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{d})$ ist, folgt daraus

$$v_{n+1}r_n + w_{n+1}r_{n-1} = ds_n \quad \text{und} \quad v_{n+1}s_n + w_{n+1}s_{n-1} = r_n.$$

Hieraus folgt schließlich wegen (13.3)(1)

$$\begin{aligned} r_n^2 - ds_n^2 &= (v_{n+1}s_n + w_{n+1}s_{n-1})\,r_n - (v_{n+1}r_n - w_{n+1}r_{n-1})\,s_n = \\ &= (r_n s_{n-1} - r_{n-1}s_n)\,w_{n+1} = (-1)^{n+1}w_{n+1}. \end{aligned}$$

(7) Nach (16.14) gilt: Es gibt ein $l \in \mathbb{N}$ mit

$$\sqrt{d} \;=\; [\,a_0, \overline{a_1, a_2, \ldots, a_{l-1}, a_l}\,],$$

es ist $a_l = 2a_0$, und es ist $a_j = a_{l-j}$ für jedes $j \in \{1, 2, \ldots, l-1\}$. Für jedes $j \in \{0, 1, \ldots, l-1\}$ gilt

$$\alpha_{l-j} \;=\; \frac{v_{j+1} + \sqrt{d}}{w_j}$$

und daher

$$v_{l-j} \;=\; v_{j+1} \quad \text{und} \quad w_{l-j} \;=\; w_j.$$

Beweis: Es gilt $\alpha_{l+1} = [\,a_{l+1}, a_{l+2}, a_{l+3}, \ldots\,] = [\,a_1, a_2, a_3, \ldots\,] = \alpha_1$, und wegen $w_0 = 1$ und $v_1 = a_0 w_0 + v_0 = a_0$ folgt

$$\alpha_l \;=\; a_l + \frac{1}{\alpha_{l+1}} \;=\; 2a_0 + \frac{1}{\alpha_1} \;=\; a_0 + \alpha_0 \;=\; a_0 + \sqrt{d} \;=\; \frac{v_1 + \sqrt{d}}{w_0}.$$

Ist $j \in \{1, 2, \ldots, l-1\}$ und ist bereits gezeigt, daß

$$\alpha_{l-j+1} \;=\; \frac{v_j + \sqrt{d}}{w_{j-1}}$$

ist, so gilt

$$\begin{aligned} \alpha_{l-j} \;&=\; a_{l-j} + \frac{1}{\alpha_{l-j+1}} \;=\; a_{l-j} + \frac{w_{j-1}}{v_j + \sqrt{d}} \;=\; a_j + \frac{w_{j-1}}{v_j^2 - d}(v_j - \sqrt{d}) \;= \\ &=\; a_j - \frac{v_j - \sqrt{d}}{w_j} \;=\; \frac{(a_j w_j - v_j) + \sqrt{d}}{w_j} \;=\; \frac{v_{j+1} + \sqrt{d}}{w_j}. \end{aligned}$$

(8) Für jedes $n \in \mathbb{N}_0$ gilt $w_n \in \mathbb{N}$ und daher

$$\begin{aligned} \left\lfloor \frac{v_n + \lfloor\sqrt{d}\rfloor}{w_n} \right\rfloor \;&\le\; \frac{v_n + \sqrt{d}}{w_n} \;=\; \frac{v_n + \lfloor\sqrt{d}\rfloor}{w_n} + \frac{\sqrt{d} - \lfloor\sqrt{d}\rfloor}{w_n} \;< \\ &<\; \left\lfloor \frac{v_n + \lfloor\sqrt{d}\rfloor}{w_n} \right\rfloor + \frac{w_n - 1}{w_n} + \frac{1}{w_n} \;=\; \left\lfloor \frac{v_n + \lfloor\sqrt{d}\rfloor}{w_n} \right\rfloor + 1, \end{aligned}$$

also

$$\left\lfloor \frac{v_n + \sqrt{d}}{w_n} \right\rfloor \;=\; \left\lfloor \frac{v_n + \lfloor\sqrt{d}\rfloor}{w_n} \right\rfloor.$$

(16.16) Bemerkung: Es sei d eine natürliche Zahl, die keine Quadratzahl ist. (1) Der Satz in (16.14) liefert, zusammen mit (16.15)(8), das folgende Verfahren zur Berechnung des Kettenbruchs

$$\sqrt{d} = [a_0, a_1, a_2, \dots, a_n, a_{n+1}, \dots];$$

es berechnet die Vorperiode (a_0) und die mit a_1 beginnende primitive Periode $(a_1, a_2, \dots, a_l)$ dieses Kettenbruchs:

(QW1) Man setzt

$$m := \lfloor\sqrt{d}\rfloor, \quad a_0 := m, \quad l := 1$$

und

$$v_1 := a_0, \quad w_1 := d - a_0^2, \quad v := v_1, \quad w := w_1.$$

(QW2) Man setzt

$$a_l := \left\lfloor \frac{v+m}{w} \right\rfloor, \quad v := a_l w - v \quad \text{und} \quad w := \frac{d-v^2}{w}.$$

Gilt $v = v_1$ und $w = w_1$, so gibt man die Vorperiode (a_0) und die Periode $(a_1, a_2, \dots, a_l)$ aus und bricht ab.

(QW3) Man setzt $l := l + 1$ und geht zu (QW2).

(2) Das in (1) beschriebene Verfahren zur Berechnung des Kettenbruchs für $\sqrt{d}$ nützt von der von Satz (16.14) gelieferten Information nur aus, daß mit a_1 eine Periode beginnt. Ein anderes Verfahren, das die gesamte von Satz (16.14) gelieferte Information ausnützt, wird in (16.18) behandelt.

(16.17) Satz: *Es sei d eine natürliche Zahl, die keine Quadratzahl ist, es sei*

$$\sqrt{d} = [a_0, a_1, a_2, \dots, a_n, a_{n+1}, \dots] = [a_0, \overline{a_1, a_2, \dots, a_{l-1}, a_l}]$$

der Kettenbruch für $\sqrt{d}$, wobei $(a_1, a_2, \dots, a_{l-1}, a_l)$ die mit a_1 beginnende primitive Periode dieses Kettenbruchs ist, und es seien $(v_n)_{n\geq 0}$ und $(w_n)_{n\geq 0}$ die Folgen in $\mathbb{Z}$ mit $v_0 = 0$, $w_0 = 1$ und mit

$$v_{n+1} = a_n w_n - v_n \quad \text{und} \quad w_{n+1} = \frac{d - v_{n+1}^2}{w_n} \quad \text{für jedes } n \in \mathbb{N}_0.$$

(1) *Ist l gerade, so gilt*

$$\begin{aligned} v_{l/2} &= v_{l/2+1}, \\ v_j &\neq v_{j+1} \quad \text{für jedes } j \in \{0, 1, \dots, l-1\} \setminus \{l/2\}, \\ w_j &\neq w_{j+1} \quad \text{für jedes } j \in \{0, 1, \dots, l-1\}. \end{aligned}$$

(2) *Ist l ungerade, so gilt*

$$\begin{array}{lll} v_j & \neq v_{j+1} & \textit{für jedes } j \in \{0, 1, \ldots, l-1\}, \\ w_{(l-1)/2} & = w_{(l-1)/2+1}, & \\ w_j & \neq w_{j+1} & \textit{für jedes } j \in \{0, 1, \ldots, l-1\} \setminus \{(l-1)/2\}. \end{array}$$

Beweis: Für jedes $n \in \mathbb{N}_0$ sei α_n der n-te vollständige Quotient des Kettenbruchs für $\sqrt{d}$. Da dieser Kettenbruch nicht rein-periodisch und $(a_1, a_2, \ldots, a_l)$ eine primitive Periode ist, sind die Zahlen $\alpha_0, \alpha_1, \ldots, \alpha_l$ paarweise verschieden.
(a) Aus (16.15)(7) folgt: Ist l gerade, so ist $v_{l/2} = v_{l-l/2} = v_{l/2+1}$, und ist l ungerade, so ist $w_{(l-1)/2} = w_{l-(l+1)/2} = w_{(l+1)/2}$.
(b) Es gelte: Es gibt ein $j \in \{0, 1, \ldots, l-1\}$ mit $v_j = v_{j+1}$. Dann gilt

$$\alpha_{l-j} \stackrel{(16.15)(7)}{=} \frac{v_{j+1} + \sqrt{d}}{w_j} = \frac{v_j + \sqrt{d}}{w_j} = \alpha_j,$$

und weil $\alpha_0, \alpha_1, \ldots, \alpha_l$ paarweise verschieden sind, folgt $l - j = j$. Also ist l gerade, und es gilt $j = l/2$.
(c) Es gelte: Es gibt ein $j \in \{0, 1, \ldots, l-1\}$ mit $w_j = w_{j+1}$. Dann gilt

$$\alpha_{l-j} \stackrel{(16.15)(7)}{=} \frac{v_{j+1} + \sqrt{d}}{w_j} = \frac{v_{j+1} + \sqrt{d}}{w_{j+1}} = \alpha_{j+1},$$

und weil $\alpha_0, \alpha_1, \ldots, \alpha_l$ paarweise verschieden sind, folgt $l - j = j + 1$. Also ist l ungerade, und es gilt $j = (l-1)/2$.

(16.18) Bemerkung: Es sei d eine natürliche Zahl, die keine Quadratzahl ist. Die Sätze in (16.14) und (16.17) liefern das folgende Verfahren zur Berechnung des Kettenbruchs

$$\sqrt{d} = [a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots];$$

es berechnet die Vorperiode (a_0) und die mit a_1 beginnende primitive Periode $(a_1, a_2, \ldots, a_l)$ dieses Kettenbruchs und nützt dabei die gesamte Information aus, die der Satz in (16.14) über den Kettenbruch für $\sqrt{d}$ liefert:
(QWplus1) Man setzt $v := 0$, $w := 1$, $m := \lfloor \sqrt{d} \rfloor$, $a_0 := m$ und $i := 0$.
(QWplus2) Man setzt $V := a_i w - v$. Wenn $v = V$ ist, so gibt man die Vorperiode (a_0) und die Periode

$$(a_1, a_2, \ldots, a_{i-1}, a_i, a_{i-1}, \ldots, a_2, a_1, 2a_0)$$

aus und bricht ab.

(QWplus3) Man setzt

$$W := \frac{d - V^2}{w}.$$

Wenn $W = w$ ist, so gibt man die Vorperiode (a_0) und die Periode

$$(a_1, a_2, \ldots, a_{i-1}, a_i, a_i, a_{i-1}, \ldots, a_2, a_1, 2a_0)$$

aus und bricht ab.
(QWplus4) Man setzt

$$i := i + 1, \quad a_i := \left\lfloor \frac{V + m}{W} \right\rfloor, \quad v := V \quad \text{und} \quad w := W$$

und geht zu (QWplus2).

(16.19) Bemerkung: Ist $d \in \mathbb{N}$ keine Quadratzahl, so gilt nach (16.15)(3) für die Länge $l(d)$ einer primitiven Periode des Kettenbruchs für $\sqrt{d}$: Es ist $l(d) \leq 2d - 1$. Man kann mehr beweisen (vgl. Cohn [21]): Es gilt

$$l(d) \leq \frac{7}{2\pi^2} \sqrt{d} \cdot \log d + O(\sqrt{d}).$$

(16.20) Aufgaben:

Aufgabe 1: Man schreibe eine MuPAD-Funktion, die zu einer ganzen Zahl a_0 und natürlichen Zahlen $a_1, a_2, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_{k+l-1}$ die reelle Zahl

$$\alpha = [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}]$$

berechnet (vgl. dazu (16.12)). Dabei ist zuzulassen, daß $k = 0$ ist.

Aufgabe 2: Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl d, die keine Quadratzahl ist, und zu rationalen Zahlen x und y nach dem in (16.10) angegebenem Verfahren die periodische Kettenbruchentwicklung der Zahl $x + y\sqrt{d}$ berechnet.

Aufgabe 3: (a) Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl d, die keine Quadratzahl ist, nach dem in (16.15) beschriebenen Verfahren QW den Kettenbruch

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{l-1}, a_l}]$$

berechnet.

(b) Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl d, die keine Quadratzahl ist, nach dem in (16.18) beschriebenen Verfahren QWplus den Kettenbruch

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{l-1}, a_l}]$$

berechnet.

(c) Man vergleiche die Funktionen aus (a) und (b).

Aufgabe 4: Man schreibe eine MuPAD-Funktion, die zu einer natürlichen Zahl d, die keine Quadratzahl ist, nach dem in (16.18) beschriebenen Verfahren QWplus die Länge einer primitiven Periode des Kettenbruchs

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{l-1}, a_l}]$$

berechnet, ohne die Periode wirklich auszurechnen.

17 Die Pellschen Gleichungen

(17.1) In diesem Paragraphen wird eine spezielle Klasse von Diophantischen Gleichungen behandelt. Eine Diophantische Gleichung ist – im einfachsten Fall – eine Gleichung der Form

$$f(X_1, X_2, \ldots, X_n) = 0,$$

wobei f ein Polynom in $n \geq 2$ Unbestimmten $X_1, X_2, \ldots, X_n$ über dem Ring $\mathbb{Z}$ ist und wobei nach den Lösungen $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ gefragt wird. Der griechische Mathematiker Diophantos (um 250 n. Chr. Geb.) hat sich mit der Untersuchung solcher "unbestimmter Gleichungen" beschäftigt, er interessierte sich aber mehr für ihre Lösungen $(x_1, x_2, \ldots, x_n) \in \mathbb{Q}^n$. Trotzdem sind Gleichungen der angegebenen Form, bei denen man sich für die ganzzahligen Lösungen interessiert, nach ihm benannt.

Im Jahr 1621 veröffentlichte C. G. Bachet de Méziriac (1581 – 1638) den griechischen Text der Schriften von Diophantos, zusammen mit einer Übersetzung ins Lateinische und einem ausführlichen Kommentar, und zwischen diesem Jahr und 1636 beschaffte sich P. de Fermat ein Exemplar, wohl das, in das er seine berühmte Vermutung notierte. Mit Fermats Beschäftigung mit diesem Buch beginnt nach der Meinung von A. Weil (vgl. [112]) die moderne Zahlentheorie. Fermat befaßte sich dabei auch mit Diophantischen Gleichungen der Gestalt

$$(*) \qquad X^2 - dY^2 = 1,$$

in denen d eine natürliche Zahl ist, die keine Quadratzahl ist, und fand wohl ein Verfahren, Lösungen solcher Gleichungen zu berechnen. Auch die englischen