Z24
−1−

Vorlesung Zahlentheorie I (Algebraische ZT)

WiSe '22/'23, hhu
K. Halupczok

Z24: Kettenbrüche und quadratische Irrationalzahlen

Stichworte: KBE quadr. Irrationalzahlen, periodischer KB, Satz von Euler & Lagrange über periodische KBe, Satz von Galois zu reinperiodischen KBen, KBe von $\sqrt{m}$ und Palindrome

---

24.1. Einleitung: Laut Euler stellt ein periodischer KB eine (reelle) quadratische Irrationalzahl dar, und laut Lagrange gilt auch die Umkehrung. Ein Ergebnis von Galois besagt, dass die reduzierten quadratischen KBe genau zu den reinperiodischen KBen gehören. Damit kann das palindromische Verhalten der KBEn von reellen Zahlen der Form $\sqrt{m}$ erklärt werden.

24.2. Def.: $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ heißt (reelle) quadratische Irrationalzahl, falls α algebraisch vom Grad 2, d.h. α genügt einer quadratischen Glg. $a\alpha^2 + b\alpha + c = 0$ mit $a, b, c \in \mathbb{Z}$, $a > 0$, OE $ggT(a,b,c) = 1$.

24.3. Lemma: In 24.2 sind a, b, c eindeutig bestimmt durch α.
Bew.: Betr. $a_0\alpha^2 + b_0\alpha + c_0 = 0$, $a_0 > 0$ minimal. Haben $a = qa_0 + r$ und $(a - qa_0)\alpha^2 + (b - qb_0)\alpha + (c - qc_0) = 0$, $0 \le r < a_0$. Nun ist $r \neq 0$ unmöglich, also $r = 0$. Dann ist auch $b - qb_0 = 0$ und $c - qc_0 = 0$, ↯ zu $(a,b,c) = 1$ falls $q > 1$. □

24.4. Def.: Setze $D := b^2 - 4ac$ als die Diskriminante von α, d.h. $D = Disc(\alpha)$.
Dann: $\alpha = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{D}$, $D > 0$, $\sqrt{D} \notin \mathbb{Q}$. Haben $\alpha \in \mathbb{Q}(\sqrt{D})$.
Im reellquadratischen ZK $\mathbb{Q}(\sqrt{D})$ bezeichne das Konjugierte von $\xi = x + y\sqrt{D}$ mit $\xi' = x - y\sqrt{D}$. Wissen: $N(\xi) = \xi\xi' = x^2 - Dy^2 \rightsquigarrow \frac{1}{\xi} = \frac{\xi'}{x^2 - y^2 D}$ falls $\xi \neq 0$.

24.5. Def.: Ein Kettenbruch der Form

$$[\overbrace{q_0; q_1, \ldots, q_{m-1},}^{\text{Vorperiode}} \overbrace{q_m, q_{m+1}, \ldots, q_{m+k-1},}^{\text{Periode}} q_m, q_{m+1}, \ldots, q_{m+k-1}, q_m, q_{m+1}, \ldots, q_{m+k-1}, \ldots]$$
$$= [q_0; q_1, \ldots, q_{m-1}, \overline{q_m, q_{m+1}, \ldots, q_{m+k-1}}]$$

bei dem die Folge der Teilnenner ab einer Stelle m periodisch wird, d.h. $\forall n \ge m: q_{n+k} = q_n$, heißt periodischer KB. Die kleinste solche Zahl $k \in \mathbb{N}$ heißt Periodenlänge des KBs, m (minimal) heißt Länge der Vorperiode.

24.6. **Bem.:** Ist α durch einen periodischen KB dargestellt, ist $\alpha \notin \mathbb{Q}$ (da unendl. KB).
Ist m die Länge der Vorperiode und $\hat{\alpha}$ der m-te Rest der KBE von α,
d.h. $\alpha = [q_0; q_1, \dots, q_{m-1}, \hat{\alpha}]$, so gilt $\alpha = \dfrac{c_{m-1}\hat{\alpha} + c_{m-2}}{d_{m-1}\hat{\alpha} + d_{m-2}}$, $c_i, d_i \in \mathbb{Z}$,
vgl. 21.2(iii) (*).

24.7. **Satz (Euler):** Ein periodischer KB stellt eine quadratische Irrationalzahl dar.
Bew.: Nach Bem. 24.6 gen. z.z.: $\hat{\alpha}$ ist quadratische Irrationalzahl.
⌜Denn: $D = \mathrm{Disc}(\hat{\alpha}) \underset{24.4}{\Rightarrow} \hat{\alpha} \in \mathbb{Q}(\sqrt{D}) \underset{24.6}{\Rightarrow} \alpha \in \mathbb{Q}(\sqrt{D}) \Rightarrow \alpha = r + s\sqrt{D}$, $r, s \in \mathbb{Q}$.

Dann ist $(\alpha - r)^2 = s^2 D$ eine quadratische Glg. für α, normiert mit rationalen Koeff. $\Rightarrow$ Beh.⌟
Haben:
$\hat{\alpha} = [q_m; q_{m+1}, \dots, q_{m+k-1}, \hat{\alpha}]$ ist reinperiodisch,
also $\hat{\alpha} = \dfrac{\tilde{c}_{k-1}\hat{\alpha} + \tilde{c}_{k-2}}{\tilde{d}_{k-1}\hat{\alpha} + \tilde{d}_{k-2}}$, es folgt $\tilde{d}_{k-1}\hat{\alpha}^2 + (\tilde{d}_{k-2} - \tilde{c}_{k-1})\hat{\alpha} - \tilde{c}_{k-2} = 0$, $\tilde{d}_{k-1} > 0$.
Also ist $\hat{\alpha}$ eine quadratische Irrationalzahl. □

24.8. **Lemma:** Sei α quadr. Irrationalzahl, $D = \mathrm{Disc}(\alpha)$. Dann sind auch alle Reste s_m quadr. Irrationalzahlen mit der gleichen Diskriminante, d.h. $D = \mathrm{Disc}(s_m)$ für alle m.
Bew.: Es genügt, dies für s_1 zu zeigen, für die anderen Reste folgt die Beh. induktiv.
Sei $\alpha = q + \frac{1}{s_1}$ mit $q = q_0$. Mit a, b, c aus Def. 24.2 folgt damit
$a\left(q + \frac{1}{s_1}\right)^2 + b\left(q + \frac{1}{s_1}\right) + c = 0$. Die Multiplikation mit s_1^2 ergibt
$\underbrace{(aq^2 + bq + c)}_{\neq 0,\ \text{da } s_1 \notin \mathbb{Q}} s_1^2 + (b + 2aq)s_1 + a = 0$,
wo $\mathrm{ggT}(aq^2 + bq + c,\ b + 2aq,\ a) = 1$, da $\mathrm{ggT}(a, b, c) = 1$.
Damit ist $\mathrm{Disc}(s_1) = (b + 2aq)^2 - 4a(aq^2 + bq + c) = b^2 - 4ac = D$. □

24.9. **Def.:** Eine quadr. Irrationalzahl α heißt reduziert, wenn (R) $\alpha > 1$ und $-1 < \underset{\text{die Konjugierte von } \alpha}{\alpha'} < 0$.
(Dann ist $-\frac{1}{\alpha'} > 1$.)

24.10. **Bsp.:** Sei $D \in \mathbb{N}$ keine Quadratzahl und $k := \lfloor \sqrt{D} \rfloor$, so dass $1 \le k < \sqrt{D} < k + 1$.
Dann ist $\alpha := k + \sqrt{D}$ reduziert, denn $\alpha > 1$ und $-1 < k - \sqrt{D} < 0$.

24.11. Lemma: Zu festem D gibt es nur endlich viele reduzierte quadr. Irrationalzahlen mit Diskriminante D.

Bew.: Sei α reduzierte qu. Irrationalzahl, a, b, c wie in 24.2 gegeben, $D = b^2 - 4ac$.

Dann ist wegen (R) insb. $\alpha' < \alpha$, es folgt $\alpha = \frac{-b+\sqrt{D}}{2a}$, $\alpha' = \frac{-b-\sqrt{D}}{2a}$.

- Da $1 < \alpha$, $-1 < \alpha'$, folgt $0 < \alpha + \alpha' = -\frac{b}{a}$, also ist (da $a \geq 0$) dann $b < 0$.
  Mit $\alpha' < 0$ folgt $-b - \sqrt{D} < 0$, also (1): $-\sqrt{D} < b < 0$.
- Da $1 < \alpha$, folgt $2a < -b + \sqrt{D} \underset{(1)}{\leq} 2\sqrt{D}$, also (2): $0 < a < \sqrt{D}$.
- Aus $D = b^2 - 4ac$ folgt (3) $c = \frac{b^2 - D}{4a}$.

Die Aussagen (1), (2), (3) zeigen: Es gibt nur endl. viele Möglichkeiten für b, a, c. □

24.12. Lemma: Die Reste ς_n einer quadr. Irrationalzahl α sind von einer Stelle n_0 an alle reduziert.

(Nach Lemma 24.8 sind alle ς_n quadr. Irr.zahlen mit der gleichen Diskriminante.)

Bew.: Für bel. $n \in \mathbb{N}$ gilt $\varsigma_n > 1$ und ferner $\alpha = \frac{c_n \varsigma_{n+1} + c_{n-1}}{d_n \varsigma_{n+1} + d_{n-1}}$,
also ist $\varsigma_{n+1} = \frac{d_{n-1}\alpha - c_{n-1}}{-d_n \alpha + c_n}$ und somit

$$\varsigma'_{n+1} = \frac{d_{n-1}\alpha' - c_{n-1}}{-d_n\alpha' + c_n}, \text{ da } \xi \mapsto \xi' \text{ Isom.}$$

Dies zeigt:

$$-\frac{1}{\varsigma'_{n+1}} = \frac{d_n\alpha' - c_n}{d_{n-1}\alpha' - c_{n-1}} \cdot \frac{d_{n-1}}{d_{n-1}} = \frac{d_n d_{n-1}\alpha' - c_n d_{n-1}}{d_{n-1}(d_{n-1}\alpha' - c_{n-1})}.$$

Der Zähler hier ist $= d_n d_{n-1}\alpha' \underbrace{- c_n d_{n-1} + c_{n-1} d_n}_{=(-1)^n} - c_{n-1} d_n$, also ist

$$-\frac{1}{\varsigma'_{n+1}} = \frac{(-1)^n}{d_{n-1}(d_{n-1}\alpha' - c_{n-1})} + \frac{d_n(d_{n-1}\alpha' - c_{n-1})}{d_{n-1}(d_{n-1}\alpha' - c_{n-1})} = \frac{(-1)^n}{d_{n-1}^2(\alpha' - c_{n-1}/d_{n-1})} + \frac{d_n}{d_{n-1}}$$

$$= \frac{1}{d_{n-1}}\left(d_n + \frac{(-1)^n}{d_{n-1}(\alpha' - c_{n-1}/d_{n-1})}\right) = 1 + \frac{1}{d_{n-1}}\Bigg(\underbrace{(d_n - d_{n-1})}_{\geq 1 \text{ für } n \geq 2} + \underbrace{\frac{(-1)^n}{d_{n-1}(\underbrace{\alpha' - c_{n-1}/d_{n-1}}_{\to \alpha \neq \alpha'})}}_{\xrightarrow{n\to\infty} 0}\Bigg)$$

> 1 für fast alle n.

Also ex. n_0 mit $-\frac{1}{\varsigma'_{n+1}} > 1$ für alle $n \geq n_0$. Zusammen mit $\varsigma_{n+1} > 1$ ist somit ς_{n+1} reduziert für alle $n \geq n_0$. □

24.13 Satz (Lagrange): Jede quadr. Irrationalzahl $\alpha \in \mathbb{R}$ hat periodische KBE.
(Umkehrung des Satzes 24.7 von Euler)

Bew.: Nach Lemma 24.12 ex. n_0 so, dass S_n reduziert für jedes $n \geq n_0$.
Nach Lemma 24.8 haben alle S_n die gleiche Diskriminante D wie α.
Nach Lemma 24.11 gibt es aber nur endl. viele reduzierte quadr. Irr.zahlen mit Diskriminante D. Folglich ex. $n_2 > n_1 \geq n_0$ mit $S_{n_2} = S_{n_1}$.
Sei $n_2 = n_1 + k$ mit $k \in \mathbb{N}$. Dann ist $[q_{n_1+k}; q_{n_1+k+1}, \ldots] = S_{n_1+k} = S_{n_1} = [q_{n_1}; q_{n_1+1}, \ldots]$.
Nach Eind. des KBE folgt $q_{m+k} = q_m$ für alle $m \geq n_0$, d.h. die KBE ist periodisch. □

24.14 Satz (Galois): Eine quadr. Irrationalzahl α ist genau dann reduziert, wenn α eine rein-periodische KBE hat (d.h. periodisch ohne Vorperiode ist).
Bew.: „$\Leftarrow$": Sei $\alpha = [\overline{q_0; q_1, \ldots, q_{\ell-1}}]$. Dann ist $\alpha = S_\ell = S_{2\ell} = S_{3\ell} = \ldots$
Aber S_n ist nach Lemma 24.12 für fast alle n reduziert, also ist α selbst reduziert.
„$\Rightarrow$": 1) Haben: α reduziert $\Rightarrow$ alle S_n reduziert.
⌈Gen. z.z.: S_1 reduziert. Nach Vor. ist $\alpha > 1$, $-1 < \alpha' < 0$.
Es ist $\alpha = q + \frac{1}{S_1}$ mit $q \in \mathbb{N}$ (wegen $\alpha > 1$) und $S_1 > 1$.
Dann ist $-\frac{1}{S_1} = q - \alpha$, also $-\frac{1}{S_1'} = q - \alpha' > q \geq 1$. ⌋

2.) Sei α eine reduzierte quadr. Irrationalzahl. Alle S_m sind also reduziert und haben dieselbe Diskriminante wie α nach Lemma 24.8. Nach Lemma 24.11 gibt es aber nur endl. viele solcher quadratischen Irrationalzahlen.
Also ex. $m \in \mathbb{N}_0$, $k \in \mathbb{N}$ mit $S_m = S_{m+k}$. Sei m minimal gewählt.
z.z.: $m = 0$ (dann $\alpha = S_k$, die KBE ist dann rein-periodisch).
Ann.: $m > 0$, $(m-1 \geq 0)$ und $[q_m; q_{m+1}, \ldots] = [q_{m+k}; q_{m+k+1}, \ldots]$
Die Eind. der KBE zeigt $q_{n+k} = q_n$ für alle $n \geq m$.

① Haben $\varsigma'_{m-1} = q_{m-1} + \frac{1}{\varsigma'_m} \Rightarrow \underbrace{\lfloor \varsigma'_{m-1} \rfloor}_{=-1} = q_{m-1} + \lfloor \frac{1}{\varsigma'_m} \rfloor$.

② Haben $\varsigma'_{m+k-1} = q_{m+k-1} + \underbrace{\frac{1}{\varsigma'_{m+k}}}_{=\frac{1}{\varsigma'_m}} \Rightarrow \overbrace{\lfloor \varsigma'_{m+k-1} \rfloor}^{\sim} = q_{m+k-1} + \lfloor \frac{1}{\varsigma'_m} \rfloor$.

Es folgt $q_{m-1} = q_{m+k-1}$
und aus ①, ② auch $\varsigma'_{m-1} = \varsigma'_{m+k-1}$, so dass $\varsigma_{m-1} = \varsigma_{m+k-1} = \varsigma_{(m-1)+k}$
folgt im ↯ zur Minimalität von m. □

24.15 **Bem.:** Ist α reduzierte qu. Irr.zahl, also $\alpha = [\overline{q_0, q_1, \dots, q_{k-1}}]$ reinperiodisch, so gilt $-\frac{1}{\alpha'} = [\overline{q_{k-1}, \dots, q_1, q_0}]$, d.h. der gespiegelte KB.

Bew.: Aufgrund der Periodizität gilt
$$\varsigma_0' = q_0 + \frac{1}{\varsigma_1'},\ \varsigma_1' = q_1 + \frac{1}{\varsigma_2'},\ \dots,\ \varsigma_{k-1}' = q_{k-1} + \frac{1}{\varsigma_0'},$$
also ist $\underbrace{-\frac{1}{\varsigma_0'}}_{=-\frac{1}{\alpha'}} = q_{k-1} - \varsigma'_{k-1}$, $-\frac{1}{\varsigma'_{k-1}} = q_{k-2} - \varsigma'_{k-2}, \dots, -\frac{1}{\varsigma_1'} = q_0 - \varsigma_0'$,
woraus die behauptete KBE für $-1/\alpha'$ folgt. □

24.16 **Satz:** Ist $m \in \mathbb{N}$ keine Quadratzahl, gilt $\sqrt{m} = [\lfloor\sqrt{m}\rfloor; \overline{\underbrace{q_1, q_2, q_3, \dots, q_3, q_2, q_1}, 2\lfloor\sqrt{m}\rfloor}]$.
Palindrom, d.h. von vorwärts und rückwärts gleich

Bem.: Bsp.: $\sqrt{109} = [10; \overline{2, 3, 1, 2, 4, 1, 6, 6, 1, 4, 2, 1, 3, 2, 20}]$.
(Man kann auch die Umkehrung zeigen: eine KBE dieser Form hat als Wert $\sqrt{m}$ mit $m \in \mathbb{N}, m > 1$.)

Bew.: Haben $-1 < \lfloor\sqrt{m}\rfloor - \sqrt{m} < 0$ und $1 < \lfloor\sqrt{m}\rfloor + \sqrt{m}$, also ist $\lfloor\sqrt{m}\rfloor + \sqrt{m}$ reduziert, also nach Satz 24.14 von Galois rein-periodisch. Also ist $\lfloor\sqrt{m}\rfloor + \sqrt{m} = [\overline{2\lfloor\sqrt{m}\rfloor; q_1, \dots, q_{k-1}}]$
$= [2\lfloor\sqrt{m}\rfloor; \overline{q_1, \dots, q_{k-1}, 2\lfloor\sqrt{m}\rfloor}]$ (*). Weiter ist $\frac{1}{\sqrt{m} - \lfloor\sqrt{m}\rfloor} = \frac{-1}{-\sqrt{m} + \lfloor\sqrt{m}\rfloor} = [\overline{q_{k-1}, \dots, q_1, 2\lfloor\sqrt{m}\rfloor}]$
nach Bem. 24.15. Also ist $\sqrt{m} = [\lfloor\sqrt{m}\rfloor, \frac{1}{\sqrt{m} - \lfloor\sqrt{m}\rfloor}] = [\lfloor\sqrt{m}\rfloor, \overline{q_{k-1}, \dots, q_1, 2\lfloor\sqrt{m}\rfloor}]$.
Zusammen mit (*) zeigt dies die Beh. □