Mitschrieb

Proseminar Elementare Zahlentheorie

Emma Bach

2025-11-26

Inhalt

Chapter 1

Kettenbrüche II

1.1 Wiederholung

Definition 1.1.1. Ein regulärer Kettenbruch ist ein Bruch der Form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$$

Proposition 1.1.2. *Es gilt folgende Rekursionsformel:*

$$p_{-2} := 0, p_{-1} := 1, p_i = ap_{i-1} + p_{i-2}$$
$$q_{-2} := 1, p_{-1} := 0, q_i = aq_{i-1} + q_{i-2}$$

Proposition 1.1.3. *Es gilt:*

1. *Für* $i \geq -1$ *gilt* $p_{i-1}q_i - p_i q_{i-1} = (-1)^i$

2. *Für* $i \geq 0$ *gilt*

$$\alpha - \frac{p_i}{q_i} = \frac{(-1)^i}{q_i(q_i\alpha_{i+1} + q_{i-1})}$$

1.2 Neues

Definition 1.2.1. Eine rationale Zahl $\frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$ heißt **beste Näherung** einer reellen Zahl $\alpha \in \mathbb{R}$, falls für alle $c \in \mathbb{Z}$ und $d \in \mathbb{N}_1$ mit $\frac{a}{b} \neq \frac{c}{d}$ und $d \leq b$

$$|d\alpha - c| > |b\alpha - a|$$

gilt.

Das Ziel des Vortrags ist, zu zeigen, dass jede beste Näherung von $\alpha \in \mathbb{R}$ auch ein Näherungsbruch von α ist.

Lemma 1.2.2.

1. *Sei* $\alpha = \frac{p_k}{q_k} \in \mathbb{Q}$*. Dann hat man für alle* $c \in \mathbb{Z}$*,* $a \in \mathbb{N}_1$ *die Ungleichung*

$$|q_k\alpha - p_k| \leq |d\alpha - c|$$

mit Gleichheit für $\frac{c}{d} = \frac{p_k}{q_k}$.

2. *Gilt* $q_k > 1$ *für* $\alpha \in \mathbb{Q}$*, so hat man für alle* $c \in \mathbb{Z}, d \in \mathbb{N}$ *mit* $d < q_k$ *die Ungleichung* $|q_{k-1}\alpha - p_{k-1}| \leq |d\alpha c|$*, mit Gleichheit genau dann, wenn* $(c,d) = (p_{k-1}, q_{k-1})$ *oder* $(c,d) = (p_k - p_{k-1}, q_k - q_{k-1})$ *ist.*

3. *Ist* $\alpha \in \mathbb{Q}, 0 \leq i \leq k-2$ *oder* $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ *und nicht gleichzeitig* $i = 0$ *und* $a_1 = 1$*, dann gilt für alle* $c \in \mathbb{Z}, d \in \mathbb{N}_1$ *mit* $d < q_{i+1}$ *die Ungleichung*

$$|q_i\alpha - p_i| \leq |d\alpha - c|$$

mit Gleichheit genau für $c = p_i, d = q_i$.

Beweis. 1. Da $\alpha \in \mathbb{Q}$ gilt auch $\alpha = \frac{p_k}{q_k}$, also folgt $0 = |q_k\alpha - p_j| \leq |d\alpha - c|$.

2. Betrachte das lineare Gleichungssystem

$$p_i x + p_{i+1} y = c,$$
$$q_i x + q_{i+1} y = d$$

In Matrixschreibweise:

$$\begin{pmatrix} p_i & p_{i+1} \\ q_i & q_{i+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}$$

Dieses Gleichungssystem ist Lösbar, wenn die Determinante nicht Null ist, also $p_i q_{i+1} - q_i p_{i+1} \neq 0$. Dass dies gilt, wurde bereits letzte Woche gezeigt. Insbesondere existieren die Lösungen gemäß der Kramerschen Regel sogar in $\mathbb{Z}$. Es gilt außerdem $x \neq 0$, da sonst $q_{i+1} \mid d$ folgen würde, was unserer Annahme $d \leq q_{i+1}$ widerspricht.

Durch Umstellen des Gleichungssystems folgt

$$x(q_{k-1}\alpha - p_{k-1}) = d\alpha - c.$$

Da $x \in \mathbb{Z} \setminus \{0\}$ folgt $|q_{k-1}\alpha - p_{k-1}| \leq d\alpha - c$.

3. In diesem Fall ist $c = \lambda p_i$ und $d = \lambda q_i$ $\lambda \in \mathbb{N}_{\geq 2}$, da $q_i\alpha - p_i \neq 0$ und $|q_i\alpha - p_i| < \lambda |q_i\alpha - p_i| = |d\alpha - c|$.

Sei nun also (c,d) von allen $(\lambda p_i, \lambda q_i)$ verschieden. Dann gilt für die Lösung des LGS $xy < 0$, denn $y = 0$ führt zu $\frac{p_i}{q_i} = \frac{c}{d}$ und $xy > 0$ ist im Widerspruch zu $0 < d < q_{i+1}$ und der Gleichheit in 1).

Nach Wiederholung haben $q_i\alpha - p_i$ und $q_{i+1}\alpha - p_{i+1}$ unterschiedliche Vorzeichen. Da $0 \leq i \leq k-2$ sind auch beide Ungleich 0.

Insgesamt folgt, dass $x(q_i\alpha - p_i)$ und $y(q_{i+1}\alpha - p_{i+1})$ gleiches Vorzeichen haben. Dementsprechend gilt Gleichheit in der folgenden Dreiecksungleichung:

$$\begin{aligned} |d\alpha - c| &= |x(q_i\alpha - p_i) + y(q_{i+1}\alpha - p_{i+1})| \\ &= |x||x(q_i\alpha - p_i)| + |y||(q_{i+1}\alpha - p_{i+1})| \\ &> |q_i\alpha - p_i| \end{aligned}$$

□

Satz 1.2.3. *Jede beste Näherung wird als Näherungsbruch angenommen.*

Beweis. Sei $\frac{a}{b}$ eine beste Näherung, aber $\frac{a}{b} \neq \frac{q_i}{p_i}$ für alle i.

Fall 1: Sei $\alpha \in \mathbb{Q}$ und $q_k \leq b$. Wähle $c = p_n, d = q_n$. Dann gilt $\frac{c}{d} \neq \frac{a}{b}$, $d \leq b$ und nach Lemma 1 folgt

$$0 = |q_k\alpha - p_k| = |d\alpha - c| < |b\alpha - c|,$$

also war $\frac{a}{b}$ keine beste Näherung.

Fall 2: Sei $\alpha \in \mathbb{Q}$ mit $q_k > b$ oder $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Fixiere i, sodass $q_i \leq b \leq q_{i+1}$. Man erhält $i < k$ und

$$1 < q_{i+1} = a_i q_i + q_{i-1},$$

also $i \geq 1$ oder $a_i > 1$. Nach Lemma 2 und Lemma 3 und $b < q_{i+1}$ gilt

$$|q_i\alpha - p_i| \leq |b\alpha - a|$$

Die Wahl von $c = p_i$ und $d = q_i$ liefert dann wieder $\frac{c}{d} \neq \frac{a}{b}$, $d \leq b$, und

$$|d\alpha - c| < |b\alpha - c|,$$

also war $\frac{a}{b}$ wieder keine beste Näherung.

□

Satz 1.2.4. *Sei $\alpha \in \mathbb{R}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$ und*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

dann ist $\frac{p}{q}$ eine beste Näherung von α, und somit insbesondere ein Näherungsbruch.

Beweis. Angenommen, $\frac{p}{q}$ wäre keine beste Näherung. Dann gibt es $c \in \mathbb{Z}$, $d \in \mathbb{N}$ mit $d \leq q$ und $\frac{p}{q} \neq \frac{c}{d}$, sodass

$$|d\alpha - c| \leq |q\alpha - c|$$

Nach Vorraussetzung gilt

$$|q\alpha - p| < \frac{1}{2q},$$

also auch

$$|d\alpha - c| < \frac{1}{2q}.$$

Nun gilt

$$\begin{aligned} \frac{1}{qb} &\leq \frac{p}{q} - \frac{c}{d} \\ &\leq \left|\alpha - \frac{p}{q}\right| + \left|\alpha - \frac{c}{d}\right| \\ &\leq \frac{1}{2q^2} + \frac{1}{2qd} \end{aligned}$$

Es folgt $\frac{1}{qd} < \frac{q+d}{2q^2 d}$, also $2q < d + q$, also $q < d$, was ein Widerspruch zur Annahme ist. □

Satz 1.2.5. *Sei $\alpha \in \mathbb{R}$. Angenommen, der 0-te Näherungsbrüchen von α hat nicht die Form $[0, 2]$, $[a_0, 1, a_2, \ldots, a_k]$, oder $[a_0, 1, a_2, \ldots]$. Dann ist jeder Näherungsbruch von α eine beste Näherung.*

Beweis. Wir müssen zeigen, dass für $\frac{p_i}{q_i}$ ($i \geq 1$ in den Ausnahmefällen) für alle $c \in \mathbb{Z}$, $d \in \mathbb{N}$ mit $\frac{c}{d} \neq \frac{p}{q}$ der Satz gilt.

Fall 1: Sei $\alpha \in \mathbb{Q}, i = k$. Dann gilt der Satz nach Lemma 1.

Fall 2: Sei $\alpha \in \mathbb{Q}, i = k - 1$. Dann gilt nach Vorraussetzung $d \leq q_i = q_{k-1}$, also gilt nach Lemma 2 $|q_{k-1}\alpha.p_{k-1}| \leq |d\alpha - c|$.

Da nicht $k = 1$, $\alpha_k = 2$ gilt, folgt $q_k > 2q_{k-1}$. Es kann also keine Gleichheit eintreten, da $(c, d) \neq (p_{k-1}, q_{k-1})$ und $(c, d) \neq (p_k - p_{k-1}, q_k - q_{k-1})$, da $d \leq q_{k-1} < q_k - q_{k-1}$.

Fall 3: Sei $\alpha \in \mathbb{Q}$, $0 \leq i \leq k - 2$ oder $\alpha \in \mathbb{R} \setminus Q$ nach Vorraussetzung ist $d \leq q_i \leq q_{i+1}$ und nach Ausnahmen ist nicht gleichzeitig $i = 0$ und $a_1 = 1$. Also folgt $|q_i\alpha - p_i| < |d\alpha - c|$, da $c \neq p_i$, $\alpha \neq q_i$.

□

Chapter 2

Das Louville-Kriterium für Transzendente Zahlen

Definition 2.0.1. Eine komplexe Zahl $\alpha \in \mathbb{C}$ heißt **algebraisch**, wenn ein $f \in \mathbb{Z}[X]$ mit $f \neq 0$ existiert, sodass $f(\alpha) = 0$.

Definition 2.0.2. Eine komplexe Zahl $\alpha \in \mathbb{C}$ heißt **transzendent**, wenn sie nicht algebraisch ist.

Definition 2.0.3. Eine algebraische Zahl α hat **Grad** n, wenn kein Polynom vom Grad $< n$ existiert, welches α als Nullstelle hat.

Satz 2.0.4. *Transzendente Zahlen existieren.*

> *Beweis.* Die Menge der komplexen Zahlen ist überabzählbar. Die Menge $\mathbb{Z}[]X$ist in Bijektion mit der Menge der Tupel beliebig vieler ganzer Zahlen, also abzählbar. Jedes Polynom hat nur endlich viele Nullstellen. Somit muss es komplexe Zahlen geben, die keine Nullstellen eines Polynoms aus $\mathbb{Z}[X]$ sind. □

Definition 2.0.5. Sei α eine reelle Zahl. Wir sagen, α ist **approximierbar zur Ordnung** m, wenn eine Konstante K existiert, sodass unendlich viele $\frac{p}{q} \in \mathbb{Q}$ existieren, sodass:

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

Satz 2.0.6. **Satz von Louville:** *Ist α eine algebraische Zahl vom Grad $n > 1$, so existiert eine Konstante $c > 0$, sodass für alle $\frac{p}{q} \in \mathbb{Q}$:*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}$$

also ist α zu keiner höheren Ordnung als n approximierbar.

Beweis. Sei $\alpha \in \mathbb{C}$ algebraisch. So existiert ein Polynom $f \in \mathbb{Z}[x] \setminus \{0\}$, welches α als Nullstelle hat. Sei

$$f = a_0 x^n + a_1 x^{n-1} + \dots a_n$$

Wir betrachten f nun auf dem Intervall $(\alpha - 1, \alpha + 1)$. □

Korollar 2.0.7. *Ist α zu beliebig hoher Ordnung m approximierbar, so ist α nicht algebraisch, also transzendent.*

Anmerkung 2.0.8. Die Umkehrung gilt nicht - viele transzendente Zahlen sind nicht beliebig hoch approximierbar. Insbesondere sind e und π nicht zu beliebig hoher Ordnung approximierbar.