DIOPHANTISCHE APPROXIMATION

Teilnehmer:

Franz Arnold	Andreas-Oberschule
Mikolaj Czuchaj	Herder-Oberschule
Alexander Fauck	Heinrich-Hertz-Oberschule
Gabriel Flemming	OSZ KIM
Wiktor Pronobis	Herder-Oberschule
Christian Rekittke	Andreas-Oberschule
Robert Waniek	Heinrich-Hertz-Oberschule

Gruppenleiter:

Jürg Kramer	Humboldt-Universität, Mitglied im DFG-Forschungszentrum „Mathematik für Schlüsseltechnologien“

Die Gruppe beschäftigte sich mit verschiedenen Darstellungsformen reeller Zahlen und der Algebraizität bzw. Transzendenz reeller Zahlen.
Eine Untergruppe untersuchte dazu die Darstellung reeller Zahlen durch Dezimalbrüche, deren Güte zur Approximation reeller Zahlen als auch die Charakterisierung rationaler Zahlen durch abbrechende bzw. periodische Dezimalbrüche.
Eine zweite Untergruppe untersuchte die Darstellung reeller Zahlen durch Kettenbrüche, deren Güte zur Approximation reeller Zahlen als auch die Charakterisierung rationaler bzw. quadratisch-irrationaler Zahlen durch abbrechende bzw. periodische Kettenbrüche.
Eine dritte Untergruppe beschäftigte sich mit den (reellen) algebraischen und transzendenten Zahlen. Es wurde festgestellt, dass es abzählbar unendlich viele algebraische, dagegen aber überabzählbar viele transzendente Zahlen gibt. Mit Hilfe des Satzes von Liouville wurden transzendente Zahlen konstruiert. Als Beispiel eines typischen Transzendenzbeweises wurde die Transzendenz der Eulerschen Zahl $e = 2,71828...$ studiert.

Dokumentation der Arbeitsgruppe "Diophantische Approximation"

1 Dezimalbruchentwicklung

Definition. Die Menge $\mathbb{R}$ der reellen Zahlen ist die Menge aller Punkte auf der Zahlengeraden. Jede reelle Zahl ist durch das Intervallschachtelungsprinzip eindeutig bestimmt.

Satz. Jede reelle Zahl α lässt sich eindeutig in der Form

$$\alpha = [\alpha] + \sum_{i=1}^{\infty} c_i \cdot 10^{-i}$$

darstellen, wobei $c_i \in \{0, 1, \ldots, 9\}$ gilt und ab keinem Index i_0 alle c_i für $i \geq i_0$ gleich 9 sind. Diese Darstellung heißt die *Dezimalbruchentwicklung von* α.

Beweis. Im folgenden können wir ohne Beschränkung der Allgemeinheit annehmen, dass der ganzzahlige Anteil $[\alpha]$ von α verschwindet und somit α mit dem gebrochenen Anteil $\{\alpha\}$ übereinstimmt.
Die c_i ergeben sich nun rekursiv aus

$$\begin{array}{ll} \alpha_1 = \{\alpha\}, & c_1 = [10 \cdot \alpha_1], \\ \alpha_2 = \{10 \cdot \alpha_1\}, & c_2 = [10 \cdot \alpha_2], \\ \vdots & \vdots \\ \alpha_i = \{10 \cdot \alpha_{i-1}\}, & c_i = [10 \cdot \alpha_i], \\ \vdots & \vdots \end{array}$$

Da für alle i die Ungleichung $0 \leq \alpha_i < 1$, also $0 \leq 10 \cdot \alpha_i < 10$ gilt, haben wir $c_i \in \{0, 1, \ldots, 9\}$. Indem wir noch beachten, dass eine 9-er Periode nicht auftreten kann, erkennen wir, dass die behauptete Darstellung existiert.
Darüber hinaus existiert stets höchstens eine (mithin genau eine) solche Darstellung, denn wäre α auf zwei Arten als Dezimalbruch entwickelbar, so gäbe es zwei Darstellungen

$$\alpha = \sum_{i=1}^{\infty} c_i \cdot 10^{-i} = \sum_{i=1}^{\infty} c_i' \cdot 10^{-i},$$

wobei mindestens für ein i $c_i \neq c_i'$ gilt. Es sei nun $j \geq 1$ der kleinste Index, für den die Ungleichung $c_j \neq c_j'$ erfüllt ist. Damit erhalten wir durch Vergleich

$$\frac{c_j}{10^j} - \frac{c_j'}{10^j} = \frac{c_{j+1}'}{10^{j+1}} + \ldots - \frac{c_{j+1}}{10^{j+1}} - \ldots,$$

d.h. nach Multiplikation mit 10^j

$$c_j - c_j' = 10^j \left(\frac{c_{j+1}' - c_{j+1}}{10^{j+1}} + \frac{c_{j+2}' - c_{j+2}}{10^{j+2}} + \ldots \right) = \sum_{i=1}^{\infty} (c_i' - c_i) \cdot 10^{-i}.$$

Da nun die Differenz zweier verschiedener Elemente c_j, c_j' von $\{0, 1, \ldots, 9\}$ betragsmäßig mindestens 1 beträgt, ergibt sich die Abschätzung

$$\begin{aligned} 1 &\leq |c_j - c_j'| = \left| \sum_{i=1}^{\infty} (c_i' - c_i) \cdot 10^{-i} \right| \\ &\leq \sum_{i=1}^{\infty} |c_i' - c_i| \cdot 10^{-i} \leq 9 \cdot \sum_{i=1}^{\infty} 10^{-i} = 1. \end{aligned}$$

Damit muss in obiger Abschätzung überall das Gleichheitszeichen gelten. Insbesondere erkennt man dabei, dass die Differenzen $(c_i' - c_i)$ für alle i entweder positiv oder negativ sind; nehmen wir an, sie seien positiv. Damit dann die letztere Ungleichung eine Gleichung ist, muss $c_i' - c_i = 9$ gelten, was nur möglich ist, wenn $c_i' = 9$ und $c_i = 0$ ist. Dies ist aber ein Widerspruch. □

Satz. Es sei a/b eine rationale Zahl, wobei wir annehmen, dass die ganzen Zahlen a, b teilerfremd sind. Der Dezimalbruch von a/b bricht genau dann ab, wenn der Nenner b nur die Primteiler 2 und 5 besitzt.

Beweis. Falls b nur die Primteiler 2 und 5 besitzt, so erkennt man durch geeignetes Erweitern des Bruchs a/b sofort, dass der zugehörige Dezimalbruch abbricht.

Falls andererseits der Dezimalbruch zu a/b abbricht, so haben wir

$$\frac{a}{b} = \frac{c}{10^k} \Longleftrightarrow 10^k \cdot a = b \cdot c$$

mit einer geeigneten ganzen Zahl c und einer geeigneten natürlichen Zahl k. Ist nun r ein Primteiler von b, so teilt r das Produkt $b \cdot c$, also auch das Produkt $10^k \cdot a$. Da nun aber a, b teilerfremd sind, muss r den Faktor 10^k teilen, so dass $r = 2$ oder $r = 5$ gilt. □

Falls der Nenner b der rationalen Zahl a/b Primfaktoren besitzt, die verschieden von 2 und 5 sind, so ist die Dezimalbruchentwicklung von a/b periodisch. Zur Vorperiodenlänge bzw. Periodenlänge stellen wir zum Abschluss dieses ersten Abschnitts ohne Beweis folgendes fest.

Satz. (i) Die Vorperiodenlänge des Dezimalbruchs der rationalen Zahl a/b ist genau dann gleich 0, wenn für den größten gemeinsamen Teiler $\mathrm{ggT}(10, b)$ von 10 und b gilt

$$\mathrm{ggT}(10, b) = 1.$$

(ii) Gilt $\mathrm{ggT}(10, b) = 1$, so ist die Periodenlänge gegeben durch die kleinste natürliche Zahl l mit der Eigenschaft

$$10^l \equiv 1 \bmod b.$$

Beispiel. Dies sei kurz am Beispiel $a/b = 5/7$ erläutert:

l	Restklasse
1	$10^1 \equiv 3 \bmod 7$
2	$10^2 \equiv 2 \bmod 7$
3	$10^3 \equiv 6 \bmod 7$
4	$10^4 \equiv 4 \bmod 7$
5	$10^5 \equiv 5 \bmod 7$
6	$10^6 \equiv 1 \bmod 7$

Daraus folgt, dass die Periodenlänge des Bruches 5/7 gleich 6 ist. In der Tat rechnet man leicht nach

$$\frac{5}{7} = 0, \overline{714285}.$$

2 Kettenbruchentwicklung

2.1 Einführung in die Theorie der Kettenbrüche

Gegeben sei $\alpha \in \mathbb{Q}$. Dann heißt $[a_0; a_1, a_2, ..., a_n]$ Kettenbruchentwicklung von α genau dann, wenn gilt:

$$\begin{array}{ll} \alpha_0 = \alpha\,, & a_0 = [\alpha_0]\,; \\ \alpha_1 = \{\alpha_0\}^{-1}\,, & a_1 = [\alpha_1]\,; \\ \vdots & \vdots \\ \alpha_n = \{\alpha_{n-1}\}^{-1}\,, & a_n = [\alpha_n]\,; \end{array}$$

hierbei ist $[\alpha_i]$ der ganzzahlige Anteil von α_i und $\{\alpha_i\} = \alpha_i - [\alpha_i]$ $(i = 0, \ldots, n)$. Es ergibt sich damit

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

Beispiel.

$$\frac{17}{5} = 3 + \frac{2}{5} = 3 + \frac{1}{\frac{5}{2}} = 3 + \frac{1}{2 + \frac{1}{2}}\,,$$

bzw.

$$\frac{17}{5} = [3; 2, 2]\,.$$

Analog findet man

$$\frac{159}{46} = [3; 2, 5, 4]\,.$$

Verallgemeinert kann man nun auch Kettenbrüche für irrationale Zahlen definieren:
Statt $\alpha \in \mathbb{Q}$ ist nun $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, wodurch alle α_i größer als 1 und irrational sind $(i = 1, 2, \ldots)$. Wir erhalten damit für α den unendlichen Kettenbruch

$$[a_0; a_1, a_2, \ldots, a_i, \ldots].$$

Satz. Der Kettenbruch einer reellen Zahl α bricht genau dann ab, wenn α rational ist.

Beweis. Die Behauptung ergibt sich aus der Beobachtung, dass die Folge der Teilnenner, deren Glieder natürlich sind, streng monoton fällt. □

Aufgrund des vorhergehenden Satzes sind die irrationalen Zahlen dadurch charakterisiert, dass ihre Kettenbrüche nicht abbrechen.

2.2 Konvergenz der unendlichen Kettenbrüche

Sei $[a_0; a_1, \ldots, a_n, (\ldots)]$ ein Kettenbruch (mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$, $i = 1, 2, \ldots$), dessen letztes Glied, sofern er abbricht, a_n lautet.
Dazu seien die beiden ganzzahligen Folgen $(p_i), (q_i)$ rekursiv definiert durch

$$\begin{aligned} p_{-2} &= 0, \quad p_{-1} = 1, \quad p_i = a_i \cdot p_{i-1} + p_{i-2}\,, \\ q_{-2} &= 1, \quad q_{-1} = 0, \quad q_i = a_i \cdot q_{i-1} + q_{i-2}\,. \end{aligned}$$

Bemerkung. Dabei ist $q_0 = 1$ und $q_i \geq q_{i-1} + q_{i-2}$ und somit ist $q_i \geq i$ bzw. q_i unbeschränkt für wachsende i. Der Sinn lässt sich anhand des folgenden Beispiels erahnen:

$$\begin{array}{llll} q_0 = 1, & p_0 = a_0, & \dfrac{p_0}{q_0} = \dfrac{a_0}{1} = [a_0]\,, \\ q_1 = a_1, & p_1 = a_1 \cdot a_0 + 1, & \dfrac{p_1}{q_1} = \dfrac{a_1 \cdot a_0 + 1}{a_1} = a_0 + \dfrac{1}{a_1} = [a_0; a_1]\,, \\ \vdots & \vdots & \vdots \end{array}$$

Allgemein lässt sich beweisen

Satz. Besitzt α den Kettenbruch $[a_0; a_1, \ldots, a_i, \ldots]$, so gilt für den endlichen Kettenbruch $A_i = [a_0; a_1, \ldots, a_i]$ die Beziehung

$$A_i = \frac{p_i}{q_i}.$$

Aus diesem Grund nennen wir den Bruch p_i/q_i den i-ten Näherungsbruch der Zahl α. □

Konvergenzsatz. Besitzt α den unendlichen Kettenbruch $[a_0; a_1, \ldots, a_i, \ldots]$, so gilt für die Näherungsbrüche $A_i = p_i/q_i$

$$A_0 < A_2 < \ldots < \alpha < \ldots < A_3 < A_1\,,$$

und α ist Grenzwert der Folge der Näherungsbrüche.
Beweis. Man zeigt zunächst $p_{i-1}q_i - p_iq_{i-1} = (-1)^i$, woraus

$$A_{i-1} - A_i = \frac{(-1)^i}{q_{i-1}q_i} \tag{1}$$

für $i \geq 1$ folgt. Damit lässt sich weiter zeigen, dass $p_{i-2}q_i - p_iq_{i-2} = (-1)^{i-1}a_i$ bzw. $A_i - A_{i-2} = (-1)^i a_i/(q_{i-2}q_i)$ für $i \geq 2$ folgt. Daraus folgt für gerades $i \geq 2$ die Ungleichung $A_i > A_{i-2}$ bzw. für ungerades $i \geq 3$ die Ungleichung $A_i < A_{i-2}$. Sind jetzt s und t in $\mathbb{N}$ mit $s \leq t$, bzw. $s > t$, so gilt deshalb nach Formel (1)

$$A_{2s} \leq A_{2t} < A_{2t+1} \quad \text{bzw.} \quad A_{2s} < A_{2s+1} < A_{2t+1}.$$

Damit ist die Folge $A_0, A_2, \ldots$ streng monoton wachsend und beschränkt (z.B. durch A_1), bzw. die Folge $A_1, A_3, \ldots$ streng monoton fallend und beschränkt (z.B. durch A_0). Beide Folgen konvergieren somit; seien α', bzw. α'' die entsprechenden Grenzwerte. Damit ergibt sich

$$0 \leq \alpha'' - \alpha' < A_{2s-1} - A_{2s} \overset{(1)}{=} \frac{1}{q_{2s-1}q_{2s}} \leq \frac{1}{(2s-1)2s},$$

da α' das Supremum der Folge $A_0, A_2, \ldots$, bzw. α'' das Infimum der Folge $A_1, A_3, \ldots$ ist, und die Ungleichung $q_i \geq i$ gilt. Der Grenzwert des letzten Ausdrucks ist Null, wenn s gegen unendlich strebt, womit nach dem Grenzwertsatz für die Addition von Folgen $\alpha'' = \alpha' = \alpha$ folgt. □

Corollar. Sei $\alpha \in \mathbb{R}$ und (p_i/q_i) die Folge der Näherungsbrüche. Dann gilt

$$\left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2},$$

d.h. die Approximation durch Kettenbrüche hat im Gegensatz zur dezimalen Approximation eine doppelt so hohe Konvergenzeschwindigkeit.
Beweis. Mit den vorhergehenden Abschätzungen findet man

$$\left|\alpha - \frac{p_i}{q_i}\right| < |A_{i+1} - A_i| = \frac{1}{q_iq_{i+1}} < \frac{1}{q_i^2}.$$

Dies beweist die Behauptung □

Satz. Unter der Voraussetzung, dass der Kettenbruch nicht auf 1 endet, (was stets möglich ist, da man diese 1 mit dem vorletzten Glied des Kettenbruchs zusammenfassen kann,) ist die Kettenbruchentwicklung für jede reelle Zahl α eindeutig.
Beweis. Der Beweis für diese Aussage erfolgt induktiv über die Annahme, dass es zwei verschiedene Darstellungen gibt. Dabei wird nachgewiesen, dass $a_i = a'_i$ gilt, wenn bereits $a_0, \ldots, a_{i-1}$ und $a'_0, \ldots, a'_{i-1}$ gleich sind. Außerdem wird, unter Ausnutzung der Voraussetzung (das letzte Glied ist nicht 1), gezeigt, dass die beiden Kettenbrüche gleichlang sind. □

2.3 Periodische Kettenbrüche (Sätze von Euler und Lagrange)

Im folgenden beschäftigen wir uns mit Kettenbrüchen, die in ihrer Entwicklung eine Periode aufweisen, also der Form $[a_0; a_1, \ldots, \overline{a_{l+1}, \ldots, a_{l+h}}]$ sind. Z.B. ist die Kettenbruchentwicklung von $\sqrt{2}$ wie folgt zu gewinnen:

$$\begin{aligned}(\sqrt{2}-1)(\sqrt{2}+1) = 1 \quad &\Rightarrow \quad \sqrt{2}-1 = \frac{1}{\sqrt{2}+1} \\ &\Rightarrow \quad \sqrt{2} = 1 + \frac{1}{2+\frac{1}{1+\sqrt{2}}}\,.\end{aligned}$$

Durch sukzessive Weiterführung obiger Rechnung ergibt sich schließlich

$$\sqrt{2} = [1; 2, 2, 2, \ldots]\,.$$

Das lässt sich verallgemeinern zum

Satz von Euler. Jeder unendliche, periodische Kettenbruch definiert eine reell-quadratische Irrationalzahl, d.h. eine algebraische Zahl vom Grad zwei (s. Abschnitt 3). □

Andererseits lässt sich auch die Umkehrung dieses Satzes beweisen, nämlich

Satz von Lagrange. Jede reell-quadratische Irrationalzahl hat einen unendlichen, periodischen Kettenbruch.

Beweisskizze. Der Beweis hierfür nutzt aus, dass eine bestimmte, unendliche Folge von ganzzahligen Koeffizienten eines quadratischen Polynoms beschränkt ist und sich somit ein Teil der Glieder der Folge unendlich oft wiederholt, also periodisch ist. Damit ist auch der Kettenbruch periodisch. □

3 Algebraizität und Transzendenz

3.1 Abzählbarkeit

Definition. Eine Menge M ist *abzählbar unendlich* genau dann, wenn eine bijektive Abbildung $f : M \longrightarrow \mathbb{N}$ existiert.

Satz. Eine abzählbar unendliche Vereinigung von abzählbar unendlichen Mengen ist abzählbar unendlich.

Beweis. Wir ordnen die abzählbar unendlich vielen abzählbar unendlichen Mengen $A_1, A_2, A_3, \ldots$ folgendermaßen an:

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, a_{13}, \ldots\}, \\ A_2 &= \{a_{21}, a_{22}, a_{23}, \ldots\}, \\ A_3 &= \{a_{31}, a_{32}, a_{33}, \ldots\}, \\ &\vdots \end{aligned}$$

Nun kann man mittels Diagonalverfahren jedem Element in obiger Darstellung folgendermaßen eine Nummer zuordnen:

$$\begin{aligned} a_{11} &\mapsto n_1, \\ a_{12} &\mapsto n_2, \\ a_{21} &\mapsto n_3, \\ a_{31} &\mapsto n_4, \\ a_{22} &\mapsto n_5, \\ a_{13} &\mapsto n_6, \\ &\vdots \end{aligned}$$

Damit erkennt man die Vereinigung der abzählbar unendlichen Mengen $A_1, A_2, A_3, \ldots$ als gleichmächtig zur abzählbar unendlichen Menge

$$V = \{n_1, n_2, n_3, n_4, n_5, n_6, \ldots\}.$$

□

3.2 Überabzählbarkeit

Definition. Eine Menge M ist *überabzählbar unendlich* genau dann, wenn M nicht abzählbar unendlich ist.

Satz. Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar unendlich.

Beweis. Beweis durch Widerspruch. Wir treffen die Annahme: Das offene Intervall $I =]0, 1[$ ist abzählbar unendlich. Dann kann man alle Elemente $x \in I$ folgendermaßen untereinander anordnen:

$$\begin{aligned} x_1 &= 0, a_1 b_1 c_1 \ldots, \\ x_2 &= 0, a_2 b_2 c_2 \ldots, \\ x_3 &= 0, a_3 b_3 c_3 \ldots, \\ &\vdots \\ x_n &= 0, a_n b_n c_n \ldots, \\ &\vdots \end{aligned}$$

Man konstruiere nun eine reelle Zahl $\alpha \in I$ mit $\alpha = 0, a'_1 b'_2 c'_3 \ldots$, wobei

$$a'_1 \neq a_1, b'_2 \neq b_2, c'_3 \neq c_3, \ldots, z'_n \neq z_n, \ldots$$

Da $\alpha \in I$ ist, müsste α in der obigen Aufzählung vorkommen, d.h. es müsste $\alpha = x_n$ für einen geeigneten Index n gelten. Dann müsste aber an der n-ten Stelle von α die Ziffer z_n stehen; im Gegensatz dazu steht aber an der n-ten Stelle z'_n. Damit kann also α in der obigen Aufzählung nicht vorkommen. Dies ist ein Widerspruch zu unserer Annahme. □

3.3 Algebraizität

Definition. Eine reelle Zahl $\alpha \in \mathbb{R}$ heißt *(reell) algebraisch vom Grad n*, wenn sie Nullstelle eines Polynoms

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

vom Grad n mit ganzzahligen Koeffizienten ist, aber es kein solches Polynom kleineren Grades gibt, das α zur Nullstelle hat.
Wir bezeichnen mit $\mathbb{A}$ die Menge der reell algebraischen Zahlen.

Satz. Die Menge der algebraischen Zahlen $\mathbb{A}$ ist abzählbar unendlich.
Beweis. Zunächst ordnen wir jedem Polynom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

die sogenannte Höhe $h(f)$ zu, welche durch

$$h(f) = |a_0| + |a_1| + \ldots + |a_{n-1}| + |a_n| + n \in \mathbb{N}$$

definiert ist. Da es nur endlich viele Möglichkeiten gibt, eine natürliche Zahl als Summe natürlicher Zahlen darzustellen, gibt es zu einer gegebenen Höhe nur eine endliche Anzahl von Polynomen in $\mathbb{Z}[x]$ und somit nur eine endliche Anzahl algebraischer Zahlen, deren Polynome die gleiche Höhe besitzen.
Indem wir nun die Höhe alle natürlichen Zahlen durchlaufen lassen, erkennen wir die Menge $\mathbb{A}$ der algebraischen Zahlen als abzählbar unendliche Vereinigung endlicher Mengen, welche nach dem Abschnitt 3.1 abzählbar unendlich sein muss. □

3.4 Transzendenz

Definition. Eine reelle Zahl $\alpha \in \mathbb{R}$ heißt *(reell) transzendent*, wenn sie nicht algebraisch ist.
Wir bezeichnen mit $\mathbb{T}$ die Menge der reell transzendenten Zahlen.

Satz. Es gibt überabzählbar unendliche viele transzendente Zahlen, d.h. die Menge $\mathbb{T}$ ist insbesondere nicht leer.
Beweis. Da $\mathbb{R}$ nach 3.2 überabzählbar unendlich ist und die Menge $\mathbb{A}$ der algebraischen Zahlen Teilmenge von $\mathbb{R}$ und nach Abschnitt 3.4 abzählbar ist, muss das Komplement $\mathbb{R} \setminus \mathbb{A}$ dieser beiden Mengen eine überabzählbar unendliche Menge sein. Diese Menge ist aber nichts anderes als die Menge $\mathbb{T}$ der transzendenten Zahlen. □

Satz von Liouville. Sei $z \in \mathbb{A}$ vom Grad $n > 1$. Dann gilt für alle $p \in \mathbb{Z}$

und hinreichend großen $q \in \mathbb{N}$:

$$\left| z - \frac{p}{q} \right| > \frac{1}{q^{n+1}} \, .$$

Wir verzichten hier auf den Beweis. Vielmehr weisen wir darauf hin, dass, wenn eine reelle Zahl $z \in \mathbb{R}$ das Liouvillesche Kriterium nicht erfüllt, diese Zahl transzendent sein muss.
Auf diese Art lässt sich beispielsweise zeigen, dass die sogenannte Liouvillesche Zahl

$$z = \sum_{i=1}^{\infty} 10^{-i!} = 0,110001000000000000000000100\ldots$$

transzendent ist.

3.5 Transzendenz von e

Satz. Die Eulersche Zahl $e = 2,71828\ldots$ ist transzendent.
Strategie zum Beweis. Indirekter Beweis.
An dem Beweis der Transzendenz der Eulerschen Zahl e wird im Wesentlichen die Strategie für Transzendenzbeweise dargelegt. Derartige Beweise werden immer indirekt geführt.
Beweisidee: Wir nehmen an, dass e eine algebraische Zahl ist; e ist dann Nullstelle eines Polynoms, d.h. es gilt

$$\sum_{k=0}^{m} a_k \cdot e^k = 0$$

mit $a_k \in \mathbb{Z}, a_0, a_m \neq 0$ für $k \in \{0, 1, ..., m\}$. Im Laufe des Beweises wird diese Annahme zu einem Widerspruch geführt. Zu diesem Zwecke konstruieren wir uns ein Hilfspolynom $H(x) \in \mathbb{Z}[x]$, das e^k approximiert und die folgenden weiteren Eigenschaften erfüllt:

I:

$$H(0) \neq 0.$$

Diese Eigenschaft wird benötigt, um Quotienten mit $H(0)$ im Nenner bilden zu können.

II:

$$\sum_{k=0}^{m} a_k \cdot \frac{H(k)}{H(0)} \neq 0.$$

Hiermit wird eine qualitative Aussage der Güte der Approximation getroffen, d.h. unser Hilfspolynom approximiert e^k nicht so gut, dass $H(k)/H(0)$ Nullstelle des Polynoms ist.

III:

$$\left| \sum_{k=0}^{m} a_k \cdot \left(e^k - \frac{H(k)}{H(0)} \right) \right| < \left| \frac{1}{H(0)} \right|.$$

Mit der dritten Voraussetzung wird eine quantitative Aussage über die Approximation getroffen, d.h. das Polynom nähert sich dem Wert e^k so gut an, dass die Summe der Produkte aus a_k und $e^k - H(k)/H(0)$ im Betrag kleiner ist als der Betrag von $1/H(0)$.

Eine Funktion mit diesen Eigenschaften existiert tatsächlich und wird im nächsten Abschnitt nachgewiesen.

Nachdem wir unser Hilfspolynom konstruiert haben, gilt es nun, den Widerspruch zu finden, um die Transzendenz von e zu beweisen. Dazu betrachten wir

$$\sum_{k=0}^{m} a_k \cdot e^k = \sum_{k=0}^{m} a_k \cdot \frac{H(k)}{H(0)} + \sum_{k=0}^{m} a_k \cdot \left(e^k - \frac{H(k)}{H(0)} \right).$$

Wegen der Annahme $\sum_{k=0}^{m} a_k \cdot e^k = 0$ und nach äquivalenter Umformung (Multiplikation mit $H(0)$) erhalten wir weiter

$$0 = \sum_{k=0}^{m} a_k \cdot H(k) + \sum_{k=0}^{m} a_k \cdot \left(e^k \cdot H(0) - H(k) \right).$$

Nach Eigenschaft II von H und wegen der Ganzzahligkeit der Koeffizienten von H gilt einerseits

$$\sum_{k=0}^{m} a_k \cdot H(k) \in \mathbb{Z}_{\neq 0};$$

andererseits muss aber nach Eigenschaft III

$$\sum_{k=0}^{m} a_k \cdot \left(e^k \cdot H(0) - H(k) \right) \in]-1, 1[$$

gelten. Eine ganze Zahl ungleich 0 und eine reelle Zahl im offenen Intervall $]-1,1[$ können sich nun aber nicht zu 0 addieren. Dies ist der gesuchte Widerspruch!

Für Transzendenzbeweise wird also immer angenommen, die fragliche Zahl sei algebraisch, und es wird versucht, eine approximierende Funktion zu konstruieren, um letzten Endes obigen Widerspruch zu finden.

Konstruktion des Hilfspolynoms H.

Ziel: Approximation von e^k $(k = 0, ..., m)$ durch $H(x)$

Vorüberlegung:

$$g(x) = a \cdot e^x \Leftrightarrow g'(x) = g(x) \ \ (a \in \mathbb{R}),$$

$$g(x) = e^x \Leftrightarrow g'(x) = g(x) \ \wedge \ g(0) = 1.$$

Definition des Hilfspolynoms f:

$$f(x) := x^{p-1} \cdot (x-1)^p \cdot (x-2)^p \cdot ... \cdot (x-m)^p,$$

dabei hat das Polynom f den Grad $N := mp+p-1$; p ist eine große Primzahl.

Definition des Hilfspolynoms F:

$$F(x) := f(x) + f'(x) + ... + f^{(N)}(x).$$

Wegen $f^{(N+1)}(x) = 0$ erhalten wir $F'(x) = F(x) - f(x)$. $F(x)$ ist deshalb zur Approximation von e^x geeignet, wenn $f(x)$ auf dem Intervall $[0, m]$ betragsmäßig "klein" ist, d.h.:

$$F'(x) \approx F(x).$$

Abschätzung von $f(x)$ auf dem Intervall $[0, m]$: Für alle $x \in [0, m]$ gilt:

$$|x \cdot (x-1) \cdot (x-2) \cdot ... \cdot (x-m)|^p \leq \left(m^{m+1}\right)^p,$$

also

$$\max_{0 \leq x \leq m} |f(x)| \leq \left(m^{m+1}\right)^p.$$

Somit erhalten wir die Ungleichungen

$$0 \leq \frac{\max_{0\leq x\leq m} |f(x)|}{(p-1)!} \leq \frac{(m^{m+1})^p}{(p-1)!},$$

also

$$0 \leq \lim_{p\to\infty} \frac{(m^{m+1})^p}{(p-1)!} = 0.$$

Da beide Grenzwerte existieren und gleich sind, muss auch der Grenzwert

$$\lim_{p\to\infty} \frac{\max_{0\leq x\leq m} |f(x)|}{(p-1)!}$$

existieren und gleich Null sein. Folglich gilt für $x \in [0, m]$:

$$\lim_{p\to\infty} \frac{f(x)}{(p-1)!} = 0.$$

Wenn man die Gleichung $F'(x) = F(x) - f(x)$ durch $(p-1)!$ dividiert, so erhält man folgende Approximation:

$$\frac{F'(x)}{(p-1)!} \approx \frac{F(x)}{(p-1)!}.$$

Man bildet die gesuchte Hilfsfunktion in der Form

$$H(x) := \frac{F(x)}{(p-1)!},$$

und es lässt sich daher folgern

$$\frac{H(x)}{H(0)} \approx e^x.$$

Literatur

[1] *P. Bundschuh:* Einführung in die Zahlentheorie. Springer-Verlag, 1996.

[2] *F. Klein:* Elementarmathematik vom höheren Standpunkt aus I. Springer-Verlag, 1933.

[3] *J. Kramer:* Vorlesungsnotizen, 2000.

[4] *H. Schied:* Zahlentheorie. Spektrum Akademischer Verlag, 2003.