DR. JOHANNES SPRANG

EINFÜHRUNG IN DIE TRANSZENDENTE ZAHLENTHEORIE

UNIVERSITÄT REGENSBURG

FAKULTÄT FÜR MATHEMATIK - UNIVERSITÄT REGENSBURG

https://homepages.uni-regensburg.de/~spj54141/

First printing, September 2020

Inhaltsverzeichnis

1 Einführung und Grundbegriffe

Bereits in der Schule lernt man die Zahlbereiche

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

kennen. Eine komplexe Zahl heißt *algebraisch*, wenn diese Nullstelle eines Polynoms $0 \neq P \in \mathbb{Q}[X]$ ist. Offensichtlich ist jede rationale Zahl $\alpha \in \mathbb{Q}$, als Nullstelle von $X - \alpha$, insbesondere algebraisch. Wir bezeichnen die Menge der algebraischen Zahlen mit $\overline{\mathbb{Q}}$. Wir erhalten also die Inklusionen

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}.$$

Die *transzendenten* Zahlen sind genau diejenigen Zahlen, die nicht algebraisch sind. In dieser Vorlesung widmen wir uns dem Studium transzendenter Zahlen. Insbesondere werden wir allgemeine Kriterien für Irrationalität und Transzendenz beweisen sowie die Transzendenz wichtiger mathematischer Konstanten zeigen.

1.1 Einleitung

Die transzendente Zahlentheorie birgt viele wunderschöne mathematische Sätze die man bereits mit relativ elementaren Mitteln erklären kann. In dieser Vorlesung möchte ich Sie zu einen Streifzug durch die Geschichte der transzendenten Zahlentheorie einladen. Mein Anliegen war es, die Vorlesung so zu halten, dass diese bereits mit den Mitteln der Vorlesungen „Lineare Algebra I“ und „Analysis I“ verständlich ist. Das heißt keinesfalls, dass die Vorlesung nur auf Studierende des zweiten Semesters beschränkt ist. Ich habe mir Mühe gegeben, den Stoff so auszuwählen, dass die Themen in sich motiviert sind und auch Studierende höheren Semesters ansprechen. So kann man die Fragen nach der Transzendenz von e, π und der Quadratur des Kreises als Teil der „mathematischen Allgemeinbildung“ sehen, auch wenn diese nicht immer im Curriculum Platz finden.

Aus eigener Erfahrung weiß ich, dass man am Anfang des Studiums nur schwer eine Vorstellung von mathematischer Forschung erlangen kann. Die meisten Resultate der aktuellen Forschung liegen so tief,

dass man diese noch nicht in den ersten Semestern verstehen kann[1]. Dennoch hält die transzendente Zahlentheorie ein paar Perlen bereit, deren Beweise zwar relativ elementar sind aber erst in den letzten Jahren entdeckt wurden. Ein Paradebeispiel hierfür ist zum Beispiel Apérys Beweis der Irrationalität der Zahl

$$\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}.$$

Diesem und verwandten Resultaten werden wir uns im letzten Teil der Vorlesung zuwenden und einen Hauch aktueller Forschungsluft schnuppern.

[1] Umso wichtiger ist es, dass Sie am Anfang Ihres Studiums diese Grundlagen festigen. Aus diesem Grund habe ich die Vorlesung bewusst als zwei-stündige Veranstaltung angesetzt

1.2 Überblick

Die Vorlesung gliedert sich grob in drei Teile: [2]

[2] Zu diesem Abschnitt gibt es ein Video:

Diophantische Approximation

Im ersten Teil werden wir uns mit der Frage beschäftigen, wie gut sich reelle und komplexe Zahlen durch rationale Zahlen approximieren lassen. Hierzu beschäftigen wir uns zunächst mit Kettenbrüchen. Die Theorie der Kettenbrüche erlaubt es uns zu jeder reellen Zahl eine Folge von Brüchen zu finden, die die gegebene Zahl bestmöglich approximieren. Als Anwendung werden wir die Schaltjahr-Regeln unseres Kalendersystems mit Hilfe von Kettenbrüchen erklären. Wir werden sehen, dass die Approximierbarkeit einer Zahl viel über deren Struktur preis gibt. In diesem Teil werden wir bereits die erste Klasse von Zahlen kennen lernen, deren Transzendenz wir beweisen können: die Liouville Zahlen. Wir werden zum Beispiel sehen, dass die *Liouville Konstante*

$$\sum_{k=1}^{\infty} 10^{-k!}$$

transzendent ist. In einem Ausblick werden wir sehen, dass sich diese Resultate in einen viel tiefliegenderen Kontext einordnen lassen. Wir werden, ohne Beweis, den Satz von Roth kennen lernen. Dieser Satz ist von zentraler Bedeutung auf dem Gebiet der diophantischen Approximation. Im Jahr 1958 gab es für die Entdeckung dieses Satzes sogar die Fields-Medaille.

Transzendenz mathematischer Konstanten

Im zweiten Teil werden wir die Transzendenz wichtiger mathematischer Konstanten beweisen. Zunächst werden wir den Satz von Hermite

Satz. *e ist transzendent.*

zeigen. Im Anschluss wenden wir uns dem Satz von Lindemann zu:

Satz. *π ist transzendent.*

Als Anwendung werden wir zeigen, dass die Unmöglichkeit der Quadratur des Kreises - ein Problem das auf die Antike zurück geht - zeigen. Diesen Teil schließen wir mit dem Beweis des Satzes von Lindemann-Weierstraß ab:

Satz. *Wenn $0 \neq \alpha$ algebraisch ist, dann ist e^α transzendent.*

Irrationalität von Zeta-Werten

Die Riemannsche Zeta-Funktion

$$\zeta(s) := \sum_{n \geq 1} \frac{1}{n^s}, \quad \text{für}^{[3]} \ \mathrm{Re}(s) > 1$$

ist eine der wichtigsten Funktionen der modernen Zahlentheorie. Bereits Euler kannte eine explizite Formel für die Werte der Riemannschen Zeta-Funktion an den geraden natürlichen Zahlen:

$$\zeta(2n) = -\frac{(2\pi i)^{2n}}{2(2n)!} B_{2n}$$

Hierbei sind B_{2n} gewisse rationale Zahlen, die Bernoulli-Zahlen. Insbesondere sind alle Werte $\zeta(2n)$ nach Lindemann's Satz transzendent. Über die Werte $\zeta(2n+1)$ ist weit weniger bekannt. Ihre Untersuchung ist Gegenstand aktiver mathematischer Forschung. Tatsächlich wurde erst 1979 die Irrationalität von $\zeta(3)$ gezeigt:

Satz (Apéry)**.** $\zeta(3) \notin \mathbb{Q}$

Der australische Mathematiker van der Poorten sagte zu diesem Beweis:

„A proof that Euler missed."

und spielte darauf an, dass bereits Euler alle Methoden kannte, die zum Beweis nötig sind. Siegel wird das Zitat

„Man kann den Beweis nur wie einen Kristall vor sich hertragen."

zugeschrieben. Im dritten Teil werden wir diesen elementaren und eleganten Satz beweisen. Obwohl keine weitere konkrete ungerade Zahl $2n+1$ bekannt ist für die $\zeta(2n+1)$ irrational ist, konnte Rivoal 2001 zeigen, dass es tatsächlich unendlich viele solche Zahlen geben muss. In einer gemeinsamen Arbeit mit Stéphane Fischler und Wadim Zudilin gelang es uns dieses Resultat weiter zu verbessern. In den letzten Vorlesungen werde ich ausgehend von unserem Beweis die Existenz unendlich vieler irrationaler ungerader Zeta-Werte skizzieren.

[3] $\mathrm{Re}(x+iy) := x$ ist der Realteil einer komplexen Zahl.

1.3 Die Entdeckung der Irrationalität

Bevor wir mit dem eigentlichen Inhalt der Vorlesung beginnen, begeben wir uns auf eine kleine Reise in die griechische Antike[4]; genauer ins 6. Jahrhundert vor Christus. Der Zahlbegriff zu jener Zeit war hauptsächlich geprägt von zweierlei Aspekten: Einerseits dem Zählen im Sinne von Mächtigkeiten endlicher Mengen und andererseits dem Messen von Strecken oder Flächeninhalten. Bei letzterem traten (positive) Brüche indirekt auf als Verhältnisse ganzzahliger Längen:

[4] Zu diesem Abschnitt gibt es ein Video:

Definition 1.3.1. Zwei Längen heißen *kommensurabel*, wenn beide ganzzahlige Vielfache einer dritten Länge sind.

Die Gelehrten jener Zeit gingen davon aus, dass je zwei Streckenlängen stets kommensurabel sind. Kurz, der Zahlbegriff jener Zeit wurde beherrscht von den natürlichen Zahlen und deren Verhältnissen, d.h. $\mathbb{Q}_{>0}$.

Der wohl bedeutendste Philosoph und Gelehrte jener Zeit war Pythagoras von Samos. Pythagoras gründete in Süditalien eine religiös-philosophische Bewegung. Das Weltbild der Pythagoräer begründete sich auf den Zahlbegriff. Häufig wird Pythagoras das Zitat

> „Alles ist Zahl!“

zugeschrieben. Wie oben bereits erläutert, waren mit Zahlen die natürlichen Zahlen und deren Verhältnisse gemeint. Umso erstaunlicher scheint es, dass es ausgerechnet ein Pythagoräer war, der dieses Weltbild erschütterte indem er die Existenz irrationaler Zahlen nachwies:

Satz 1.3.2 (Hippasos)**.** *Die Länge der Diagonale in einem Quadrat ist inkommensurabel mit dessen Seitenlängen. Mit anderen Worten:* $\sqrt{2} \notin \mathbb{Q}$.

Beweis. Wir zeigen $\sqrt{2} \notin \mathbb{Q}$ durch Widerspruch. Angenommen $\sqrt{2} \in \mathbb{Q}$, dann gäbe es teilerfremde positive Zahlen $a, b \in \mathbb{Z}$ mit $\sqrt{2} = \frac{a}{b}$. Durch Quadrieren und Umstellen erhalten wir

$$2b^2 = a^2. \tag{1.1}$$

Somit muss a eine gerade Zahl sein[5], sagen wir $a = 2k$ mit $k \in \mathbb{Z}$. Setzen wir dies in (1.1) ein, so erhalten wir

[5] Hier verwenden wir, dass eine natürliche Zahl genau dann gerade ist, wenn ihr Quadrat gerade ist.

$$2b^2 = 4k^2 \Rightarrow b^2 = 2k^2.$$

Somit muss neben a nun auch b gerade sein. Es ergibt sich ein Widerspruch zur Teilerfremdheit von a und b. □

Um das Schicksal von Hippasos von Metapont ranken sich zahlreiche Geschichten und Mythen. Je nach Version der Überlieferung wurde er von den Pythagoräern verfolgt, verstoßen oder gar ertränkt.

Auch über den Grund der Verärgerung gibt es verschiedene Interpretationen. Doch egal, ob die Pythagoräer wegen der Entdeckung selbst, oder wegen der Weitergabe des Wissens an Unwürdige wütend waren, fest steht, dass sie sich der Bedeutung der Entdeckung der Irrationalität durchaus bewusst waren.

In der Lehre der Pythagoräer waren Zahlen eng mit deren Weltbild verknüpft. Doch selbst aus heutiger Sicht wirft die Entdeckung der Irrationalität unmittelbar Fragen auf: Was sind Zahlen eigentlich? Gibt es gewisse Zahlen die natürlicher sind als andere? Existieren Zahlen unabhängig von unserem Geist? Auch wenn wir auf diese Fragen im Folgenden nicht eingehen können, sollten wir sie dennoch im Hinterkopf behalten. Eine von vielen möglichen Antworten hat Leopold Kronecker formuliert:

> „Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk."

Danksagung

An dieser Stelle möchte ich mich ganz herzlich bei Lukas Prader für zahlreiche Verbesserungsvorschläge, Kommentare und Korrekturen bedanken. Seine Bemerkungen und Korrekturvorschläge haben die Qualität des Skripts erheblich verbessert.

1.4 *Konventionen*

In diesem Abschnitt sammeln wir Konventionen, die in diesem Skript verwendet werden:

- Die natürlichen Zahlen enthalten nicht die Null: $\mathbb{N} := \{1, 2, 3, \dots\}$.
- Für die Menge der ganzen Zahlen ≥ 0 schreiben wir $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

1.5 *Ausblick und offene Fragen*

Ich werde am Ende jedes Abschnitts einen kleinen Ausblick auf anschließende Resultate und Fragestellungen geben und ungelöste Probleme diskutieren.

Ein interessanter Aspekt der modernen transzendenten Zahlentheorie mit Anknüpfungen zur algebraischen Geometrie beschäftigt sich mit *Perioden*. Es gibt verschiedene äquivalente Definitionen von Perioden. Eine der elementarsten Definitionen geht auf Kontsevich und Zagier zurück. Eine komplexe Zahl heißt Periode, wenn sich ihr Realteil und ihr Imaginärteil als absolut konvergentes Integral der Form

$$\int_\Delta \frac{P(x_1, \dots, x_n)}{Q(x_1, \dots, x_n)} dx_1 \dots dx_n$$

schreiben lässt. Hierbei sind $P, Q \in \mathbb{Q}[X_1, \ldots, X_n]$ Polynome und $\Delta \subseteq \mathbb{R}^n$ ein Gebiet, das sich durch Polynomungleichungen mit rationalen Koeffizienten beschreiben lässt. Man kann zeigen, dass die Menge $\mathcal{P}$ aller Perioden einen Ring bildet. Perioden enthalten neben den algebraischen Zahlen jede Menge interessante mathematischen Konstanten. So zeigt das Integral

$$\pi = \int_{x^2+y^2<1} dxdy,$$

dass die Kreiszahl π im Ring der Perioden enthalten ist. Perioden treten auf natürliche Weise als Invarianten in der algebraischen Geometrie auf. Umgekehrt kann man häufig Vermutungen aus der transzendenten Zahlentheorie aus tiefliegenden Vermutungen der algebraischen Geometrie ableiten. Diese enge Beziehung untermauert viele sehr teifliegende Vermutungen der transzendenten Zahlentheorie indem es diese Vermutungen in einen größeren Kontext setzt. Der Ring der Perioden erlaubt es die Inklusion vom Anfang dieser Einleitung wie folgt zu ergänzen:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathcal{P} \subseteq \mathbb{C}.$$

Kommen wir zurück zu konkreteren Fragestellungen. In dieser Vorlesung beschäftigen wir uns mit der Frage, wie man beweisen kann, dass eine gegebene Zahl transzendent ist. Wir werden dabei einige Kriterien für Transzendenz kennen lernen und die Transzendenz wichtiger mathematischer Konstanten wie der Eulerschen Zahl e oder der Kreiszahl π nachweisen. Dennoch gibt es eine Vielzahl mathematischer Konstanten für die die Transzendenz zwar vermutet wird aber noch nicht bewiesen ist. In vielen Fällen ist selbst die Frage nach der Irrationalität noch offen. Hier zunächst ein paar Beispiele:

Zahl	Irrationalität	Transzendenz
$e + \pi$	?	?[6]
$e\pi$	?	?
π^e	?	?
$\gamma = \lim_n \left(\sum_{k=1}^n \frac{1}{k} - \ln(n+1) \right)$	?	?
$\zeta(3) = \sum_{n\geq 1} \frac{1}{n^3}$	Apéry	?
$\zeta(2k+1) = \sum_{n\geq 1} \frac{1}{n^{2k+1}}$ für $k \geq 2$	?[7]	?

Tabelle 1.1: Offene Probleme

[6] Es ist bekannt, dass mindestens eine der Zahlen $e + \pi$ und $e\pi$ transzendent ist.

[7] Es ist bekannt, dass unendlich viele der Zahlen $\zeta(2n+1)$ irrational sind.

Wir möchten diesen Abschnitt mit einem Beispiel mit Bezug zum ersten Übungsblatts abschließen: Während die Irrationalität von

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}$$

elementar gezeigt werden kann, ist bereits die Irrationalität verwandter Summen ungemein schwieriger. Für $k \in \mathbb{N}$ definieren wir die k-te

Teilersummenfunktion $\sigma_k(n)\colon \mathbb{N} \to \mathbb{N}$ durch $\sigma_k(n) := \sum_{d|n} d^k$ wobei d die positiven Teiler von n durchläuft[8]. Für $k = 1, 2$ kann man den Irrationalitätsbeweis von e auf die Reihen

$$\sum_{n=0}^{\infty} \frac{\sigma_k(n)}{n!} \tag{1.2}$$

übertragen. Mit etwas mehr Aufwand kann man den Fall $k = 3$ behandeln. Für $k > 3$ ist die Frage nach der Irrationalität der Zahlen (1.2) immer noch offen.

[8] z.B. ist $\sigma_2(6) = 1^2 + 2^2 + 3^2 + 6^2$.

2 Diophantische Approximation

In diesem Abschnitt werden wir uns mit der Approximation reeller Zahlen durch rationale Zahlen beschäftigen. Die Theorie der Kettenbrüche liefert hierbei in gewissem Sinne beste Näherungen durch Brüche. Wir werden sehen, dass die Approximierbarkeit einer reellen Zahl eng mit Fragen nach deren Irrationalität und Transzendenz zusammen hängt.

2.1 Endliche Kettenbrüche

Definition 2.1.1. Für eine ganze Zahl $a_0 \in \mathbb{Z}$ und ein endliches Tupel $(a_1, \dots, a_n) \in \mathbb{N}^n$ natürlicher Zahlen definieren wir

$$[a_0; a_1, \dots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}.$$

Die Zahl $[a_0; a_1, \dots, a_n]$ nennen wir einen *endlichen (regulären)*[1] *Kettenbruch*.

Offensichtlich sind alle endlichen Kettenbrüche rationale Zahlen. In diesem Abschnitt werden wir sehen, dass sich tatsächlich jede rationale Zahl als endlicher Kettenbruch schreiben lässt. Zuvor wiederholen wir noch den euklidischen Algorithmus. Dieser kommt unter anderem zur Bestimmung des größten gemeinsamen Teilers zur Anwendung:[2]

Der Euklidische Algorithmus

Zunächst bemerken wir, dass es zu zwei ganzen Zahlen $x, y \in \mathbb{Z}$ mit $y \neq 0$ eindeutig bestimmte Zahlen $a, r \in \mathbb{Z}$ mit $0 \leq r < |y|$ gibt, so dass[3]

$$x = ay + r$$

gilt. Die Zahl r heißt *Rest* von x bei Division durch y. Der euklidische Algorithmus startet mit zwei ganzen Zahlen $x, y \in \mathbb{Z}$ mit $y \neq 0$ und führt iterativ Divisionen mit Rest aus: Wir setzen $r_0 := x$ und $r_1 := y$.

[1] Allgemeiner betrachtet man nicht-reguläre Kettenbrüche der Form

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{\ddots + \cfrac{b_n}{a_n}}}.$$

Da wir nur reguläre Kettenbrüche betrachten werden verzichten wir in diesem Text auf den Zusatz *regulär*.

[2] Zu diesem Abschnitt gibt es ein Video:

[3] Für $x = 26$ und $y = -3$ gilt z.B. $a = -8$ und $r = 2$.

Für $i \geq 1$ definieren wir induktiv r_{i+1} als den Rest von r_{i-1} bei Division durch r_i, solange r_i nicht Null ist:

$$r_{i-1} = a_{i-1} r_i + r_{i+1} \quad \text{mit } 0 \leq r_{i+1} < |r_i|.$$

Zusammengefasst erhalten wir folgendes Schema, bei welchem in jedem Schritt eine Division mit Rest ausgeführt wird:

$$\begin{aligned}
r_0 &:= x & r_1 &:= y \\
r_0 &= a_0 r_1 + r_2 & &\text{mit } 0 \leq r_2 < |r_1| \\
r_1 &= a_1 r_2 + r_3 & &\text{mit } 0 \leq r_3 < r_2 \\
&\dots \\
r_{n-1} &= a_{n-1} r_n + r_{n+1} & &\text{mit } 0 \leq r_{n+1} < r_n \\
r_n &= a_n r_{n+1} + 0.
\end{aligned}$$

Da der Betrag von r_i in jedem Schritt um mindestens 1 abnimmt, endet der euklidische Algorithmus nach endlich vielen Schritten. Üblicherweise wird der euklidische Algorithmus zur Berechnung des größten gemeinsamen Teilers eingesetzt. Der letzte von Null verschiedene Rest, im obigen Schema also r_{n+1}, ist der ggT der zwei Zahlen x und y.

Algorithmus 1: Euklidischer Algorithmus

```
1: procedure EUKLID(x, y)          ▷ Berechnet den ggT von a und b
2:     r ← Rest von x bei Division durch y
3:     while r ≠ 0 do
4:         x ← y                          ▷ Ersetze x durch y
5:         y ← r                          ▷ Ersetze y durch r
6:         r ← Rest von x bei Division durch y
7:     return y                           ▷ Der ggT ist der Wert von y
```

Wir erläutern den Euklidischen Algorithmus noch einmal an einem Beispiel:

Beispiel 2.1.2. Wir möchten den ggT von 97 und 11 bestimmen:

$$\begin{aligned}
97 &= 8 \cdot 11 + 9 \\
11 &= 1 \cdot 9 + 2 \\
9 &= 4 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Der ggT ist somit 1. Wir bemerken, dass der Euklidische Algorithmus die Kettenbruchentwicklung von $\frac{97}{11}$ gibt, denn: Aus der ersten Gleichung folgt

$$\frac{97}{11} = 8 + \frac{9}{11} = 8 + \frac{1}{\frac{11}{9}}. \tag{2.1}$$

Die zweite Gleichung liefert

$$\frac{11}{9} = 1 + \frac{2}{9} = 1 + \frac{1}{\frac{9}{2}}. \tag{2.2}$$

Setzen wir (2.2) in (2.1) ein, so erhalten wir:

$$\frac{97}{11} = 8 + \frac{1}{1 + \frac{1}{\frac{9}{2}}}. \tag{2.3}$$

Die dritte Gleichung liefert

$$\frac{9}{2} = 4 + \frac{1}{2} \tag{2.4}$$

und einsetzen in (2.3) ergibt die Kettenbruchentwicklung zu $\frac{97}{11}$:

$$\frac{97}{11} = 8 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}} = [8; 1, 4, 2].$$

Wir werden nun sehen, dass sich die obige Rechnung auf beliebige rationale Zahlen übertragen lässt:[4]

[4] Zu diesem Abschnitt gibt es ein Video:

Der Kettenbruch-Algorithmus

Allgemein erlaubt es der Euklidische Algorithmus einer beliebigen rationalen Zahl einen Kettenbruch zu zu ordnen:

Satz 2.1.3. *Jede rationale Zahl lässt sich als endlicher Kettenbruch darstellen.*

Beweis. Sei $x \in \mathbb{Q}$. Wir schreiben $x = \frac{r_0}{r_1}$ mit $r_0 \in \mathbb{Z}, r_1 \in \mathbb{N}$ wobei r_0 und r_1 teilerfremd gewählt sind. Der Euklidische Algorithmus liefert:

$$\begin{aligned}
r_0 &= a_0 r_1 + r_2 && \text{mit } 0 \leq r_2 < r_1 \\
r_1 &= a_1 r_2 + r_3 && \text{mit } 0 \leq r_3 < r_2 \\
&\dots \\
r_{n-1} &= a_{n-1} r_n + r_{n+1} && \text{mit } 0 \leq r_{n+1} < r_n \\
r_n &= a_n r_{n+1} + 0
\end{aligned}$$

Wir bemerken, dass $r_{n+1} = \mathrm{ggT}(r_0, r_1) = 1$ gilt. Die erste Zeile des euklidischen Algorithmus ergibt

$$\frac{r_0}{r_1} = a_0 + \frac{1}{\frac{r_1}{r_2}}.$$

Sukzessives substituieren der Gleichung

$$\frac{r_{i-1}}{r_i} = a_{i-1} + \frac{1}{\frac{r_i}{r_{i+1}}}$$

zeigt nun

$$\frac{r_0}{r_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}} = [a_0; a_1, \dots, a_n].$$

□

Im obigen Beweis haben wir bereits gesehen, dass sich die Kettenbruchentwicklung einer rationalen Zahl $x = \frac{r_0}{r_1}$ durch den euklidischen Algorithmus berechnen lässt:

$$\begin{aligned}
r_0 &= a_0 r_1 + r_2 && \text{mit } 0 \leq r_2 < r_1 \\
r_1 &= a_1 r_2 + r_3 && \text{mit } 0 \leq r_3 < r_2 \\
&\dots \\
r_{n-1} &= a_{n-1} r_n + r_{n+1} && \text{mit } 0 \leq r_{n+1} < r_n \\
r_n &= a_n r_{n+1} + 0.
\end{aligned}$$

Indem wir die i-te Zeile ($r_{i-1} = a_{i-1} r_i + r_{i+1}$) durch r_i teilen und $\alpha_i := \frac{r_i}{r_{i+1}}$ setzen, können wir den obigen Algorithmus umschreiben:

$$\begin{aligned}
\alpha_0 &= a_0 + \alpha_1^{-1} && \text{mit } 0 \leq \alpha_1^{-1} < 1 \\
\alpha_1 &= a_1 + \alpha_2^{-1} && \text{mit } 0 \leq \alpha_2^{-1} < 1 \\
&\dots \\
\alpha_{n-1} &= a_{n-1} + \alpha_n^{-1} && \text{mit } 0 \leq \alpha_n^{-1} < 1 \\
\alpha_n &= a_n + 0.
\end{aligned}$$

Man beachte, dass a_i stets die größte ganze Zahl ist, die kleiner oder gleich α_i ist:

Definition 2.1.4. Die Abrundungsfunktion $\lfloor \cdot \rfloor \colon \mathbb{R} \to \mathbb{Z}$ weist jeder reellen Zahl α die größte ganze Zahl $\lfloor \alpha \rfloor$ zu, welche kleiner oder gleich α ist.[5]

[5] Es gilt z.B. $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$.

Der euklidische Algorithmus zur Bestimmung des endlichen Kettenbruchs einer rationalen Zahl ist also äquivalent zum folgenden Algorithmus:

Algorithmus 2: Kettenbruch Algorithmus

```
1: procedure KETTENBRUCH(α)                    ▷ Berechnet die
   Kettenbruchentwicklung [a_0; a_1, ...] von α
2:     α_0 ← α
3:     a_0 ← ⌊α_0⌋
4:     n ← 0
5:     while α_n ≠ a_n do
6:         α_{n+1} ← (α_n − a_n)^{-1}
7:         a_{n+1} = ⌊α_{n+1}⌋
8:         n ← n + 1
9:     return (a_0, a_1, a_2, ...)
```

Wir erläutern diesen Algorithmus anhand des obigen Beispiels:

Beispiel 2.1.5. Wir betrachten $\alpha = \frac{97}{11}$.

$$\begin{aligned}
\alpha_0 &:= \frac{97}{11}, & a_0 &= \lfloor \alpha_0 \rfloor = \lfloor \frac{97}{11} \rfloor = 8 \\
\alpha_1 &:= (\alpha_0 - a_0)^{-1} = \frac{11}{9}, & a_1 &= \lfloor \alpha_1 \rfloor = \lfloor \frac{11}{9} \rfloor = 1 \\
\alpha_2 &:= (\alpha_1 - a_1)^{-1} = \frac{9}{2}, & a_2 &= \lfloor \alpha_2 \rfloor = \lfloor \frac{9}{2} \rfloor = 4 \\
\alpha_3 &:= (\alpha_2 - a_2)^{-1} = 2, & a_3 &= \lfloor \alpha_3 \rfloor = \lfloor 2 \rfloor = 2
\end{aligned}$$

An dieser Stelle endet der Algorithmus da $\alpha_3 = a_3$ gilt. Wir erhalten $[8; 1, 4, 2]$ als Kettenbruchentwicklung.

Wir haben den Kettenbruch-Algorithmus aus dem euklidischen Algorithmus hergeleitet. Im Gegensatz zum euklidischen Algorithmus macht der Kettenbruch-Algorithmus aber nicht von der Darstellung der Zahl $\alpha = \frac{x}{y}$ Gebrauch. Somit ist es interessant zu versuchen, den Kettenbruch–Algorithmus auf eine irrationale Zahl anzuwenden. Wir führen die ersten Schritte des Kettenbruch-Algorithmus für die irrationale Zahl $\sqrt{2}$ aus:

Beispiel 2.1.6. Wir betrachten $\alpha = \sqrt{2} = 1,41\ldots$:

$$\begin{aligned}
\alpha_0 &:= \sqrt{2}, & a_0 &= \lfloor \alpha_0 \rfloor = \lfloor \sqrt{2} \rfloor = 1 \\
\alpha_1 &:= (\sqrt{2} - 1)^{-1} = \frac{1 + \sqrt{2}}{(1 + \sqrt{2})(1 - \sqrt{2})} = 1 + \sqrt{2}, & a_1 &= \lfloor \alpha_1 \rfloor = \lfloor 1 + \sqrt{2} \rfloor = 2 \\
\alpha_2 &:= (1 + \sqrt{2} - 2)^{-1} = (\sqrt{2} - 1)^{-1} = 1 + \sqrt{2}, & a_2 &= \lfloor \alpha_2 \rfloor = \lfloor 1 + \sqrt{2} \rfloor = 2 \\
\alpha_3 &:= (1 + \sqrt{2} - 2)^{-1} = (\sqrt{2} - 1)^{-1} = 1 + \sqrt{2}, & a_3 &= \lfloor \alpha_3 \rfloor = \lfloor 1 + \sqrt{2} \rfloor = 2 \\
&\ldots
\end{aligned}$$

Da im Kettenbruch-Algorithmus jeder Schritt stets nur vom vorigen abhängt gilt $a_i = 2$ für alle $i \geq 1$. Der Kettenbruch-Algorithmus terminiert nicht und liefert das unendliche Tupe $(1, 2, 2, 2, \ldots)$ für $\sqrt{2}$.

Das vorige Beispiel zeigt, dass der Kettenbruch-Algorithmus zu $\sqrt{2}$ eine unendliche Folge[6] natürlicher Zahlen ausspuckt. Tatsächlich gilt dies für jede irrationale Zahl und liefert unser erstes Irrationalitäts-Kriterium:

Proposition 2.1.7. *Der Kettenbruch-Algorithmus für $\alpha \in \mathbb{R}$ endet genau dann nach endlichen vielen Schritten, wenn α rational ist. In diesem Fall gilt:*

$$\alpha = [a_0; a_1, \dots, a_k]$$

wobei $(a_0, \dots, a_k)$ die durch den Kettenbruch-Algorithmus definierte Folge bezeichnet.

Beweis. Falls der Algorithmus nach endlich vielen Schritten endet, so gilt $\alpha = [a_0; a_1, \dots, a_n]$, also ist α rational. Umgekehrt folgt aus dem Beweis von Satz (2.1.3), dass der Kettenbruch-Algorithmus für eine rationale Zahl nach endlich vielen Schritten terminiert. □

Indem wir Beispiel 2.1.6 mit Proposition 2.1.7 kombinieren, erhalten wir einen neuen Beweis für die Irrationalität von $\sqrt{2}$:

Korollar 2.1.8. *$\sqrt{2}$ ist irrational.*

Definition 2.1.9. Die endliche oder unendliche Folge $(a_i)_{i\geq 0}$ mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \geq 1$, die der Kettenbruch-Algorithmus einer Zahl $\alpha \in \mathbb{R}$ zuweist, heißt *Folge der Teilnenner zu α*. Das i-te Folgenglied a_i heißt i-ter Teilnenner.

Ausblick und offene Fragen:

Wendet man den Kettenbruch-Algorithmus auf π an, so erhält man die Folge der Teilnenner:

$$(3, 7, 15, 1, 292, \dots)$$

Bisher ist noch keine explizite Beschreibung dieser Folge bekannt.[7]

2.2 *Unendliche Kettenbrüche*

Im vorigen Abschnitt hatten wir gesehen, dass der Kettenbruch-Algorithmus jeder reellen Zahl α eine Folge der Teilnenner $(a_i)_{i\geq 0}$ mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \geq 1$ zuordnet. Diese Folge ist genau dann endlich wenn α rational ist. In diesem Fall gilt:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}} =: [a_0; a_1, \dots, a_n].$$

[6] Achtung: Bisher ist $(1, 2, 2, \dots)$ nur eine unendliche Folge natürlicher Zahlen. Da ein unendlicher Bruch

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}$$

zunächst keinen Sinn macht, können wir an dieser Stelle der Folge $(1, 2, 2, \dots)$ noch keinen sinnvollen Wert zuweisen.

[7] Sollte Ihnen im Laufe Ihres Studiums mal eine Zahlenfolge begegnen, deren Bildungsgesetz Sie nicht verstehen, ist es immer einen Versuch Wert diese bei der Online Encyclopedia of Integer Sequences zu suchen. Wenn Sie möchten, können Sie dort einfach mal die ersten Zahlen der Teilnennerfolge zu π eingeben.

Das Ziel dieses Abschnitts ist für irrationale Zahlen α die Konvergenz der Kettenbruchentwicklung zu zeigen. Genauer möchten wir folgende Gleichung zeigen:

$$\alpha = \lim_{n\to\infty}[a_0; a_1, \dots, a_n] =: [a_0, \dots]. \tag{2.5}$$

Hierbei ist $(a_i)_{i\geq 0}$ die Folge der Teilnenner zu $\alpha \in \mathbb{R}\setminus\mathbb{Q}$. Insbesondere, müssen wir die Konvergenz der Folge $([a_0; a_1, \dots, a_n])_{n\geq 0}$ zeigen.

Näherungsbrüche:[8]

[8] Zu diesem Abschnitt gibt es ein Video:

Im Folgenden bezeichne $(a_i)_{i\geq 0}$ entweder eine endliche oder eine unendliche Zahlenfolge mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \geq 1$. Genauer

$$(a_i)_{i\geq 0} \in \begin{cases} \mathbb{Z}\times\mathbb{N}^k & \text{für ein } k \geq 0, \text{ oder} \\ \mathbb{Z}\times\mathbb{N}^{\mathbb{N}}. \end{cases}$$

Man beachte, dass im endlichen Fall nur die Folgenglieder a_i für $0 \leq i \leq k$ definiert sind. Um nicht immer zwischen endlichen und unendlichen Zahlenfolgen unterscheiden zu müssen, fassen wir folgende Konvention:

Konvention 2.2.1. *Wir schreiben $(a_i)_{i\geq 0}$ für eine Folge, die entweder endlich oder unendlich ist. Ist $\mathcal{A}_i$ ein Ausdruck oder eine Aussage über das i-te Folgenglied, so ist im Fall endlicher Folgen $\mathcal{A}_i$ nur für $0 \leq i \leq k$ definiert. Insbesondere treffen wir folgende Konvention für Aussagen $\mathcal{A}_i$ über Folgenglieder:*

$$\text{„Für } i \geq 0 \text{ gilt } \mathcal{A}_i\text{“} := \begin{cases} \text{„Für } 0 \leq i \leq k \text{ gilt } \mathcal{A}_i\text{“}, & \text{falls } (a_i)_{i\geq 0} = (a_0, \dots, a_k) \text{ endlich ist,} \\ \text{„Für } i \geq 0 \text{ gilt } \mathcal{A}_i\text{“}, & \text{falls } (a_i)_{i\geq 0} \text{ unendlich ist.} \end{cases}$$

Definition 2.2.2. Zu $(a_i)_{i\geq 0}$ und $n \geq 0$ definieren wir:

$$A_n := [a_0; a_1, \dots, a_n]$$

Die endliche oder unendliche Folge rationaler Zahlen $(A_i)_{i\geq 0}$ heißt *Folge der Näherungsbrüche* zu $(a_i)_{i\geq 0}$. Falls $(a_i)_{i\geq 0}$ die Folge der Teilnenner zu $\alpha \in \mathbb{R}$ ist, sprechen wir auch von den *Näherungsbrüchen von* α.

Bevor wir fortfahren möchten wir noch ein paar motivierende Worte verlieren. Wir erinnern an das in (2.5) formulierte Ziel dieses Abschnitts: Wir möchten für irrationales α die Gleichung

$$\alpha = \lim_{n\to\infty} A_n$$

zeigen, wenn $(A_i)_{i\geq 0}$ die Folge der Näherungsbrüche zu α ist. Sobald wir dies gezeigt haben ist auch die Bezeichnung *Näherungsbrüche* geklärt, schließlich approximieren die Brüche A_n die Zahl α für wachsendes n immer besser. Falls die Zahl α hingegen rational mit Teilnennern $(a_0, \dots, a_k)$ ist, so gilt[9]

$$\alpha = [a_0; a_1, \dots, a_k] = A_k.$$

[9] das haben wir im letzten Kapitel gesehen, s. Proposition 2.1.7

Also approximieren die Näherungsbrüche die Zahl α im Fall $\alpha \in \mathbb{Q}$ aus trivialen Gründen gut. Aufmerksame Leser*innen werden sich zurecht Fragen, wieso wir uns überhaupt die Mühe machen und endliche Folgen an dieser Stelle mit behandeln, schließlich ist doch nur im Fall unendlicher Folgen eine interessante Konvergenzaussage zu beweisen. Der Grund dafür wird erst im Verlauf der folgenden Kapitel ersichtlich werden. Später möchten wir zu einer gegebenen Zahl $\alpha \in \mathbb{R}$ rationale Approximationen studieren. Hier spielen Näherungsbrüche eine entscheidende Rolle. Es wird sich bezahlt machen, dass wir diese für allgemeine reelle Zahlen definiert haben und nicht nur für irrationale Zahlen.

Um die Folge der Näherungsbrüche zu $(a_i)_{i\geq 0}$ zu studieren definieren wir rekursiv die Folgen $(p_i)_{i\geq -1}$ und $(q_i)_{i\geq -1}$ durch:[10]

$$\begin{aligned} p_{-1} &= 1, \quad p_0 = a_0, \quad p_i = a_i p_{i-1} + p_{i-2} \text{ für } i \geq 1, \\ q_{-1} &= 0, \quad q_0 = 1, \quad q_i = a_i q_{i-1} + q_{i-2} \text{ für } i \geq 1. \end{aligned}$$

[10] Im Sinne der Konvention 2.2.1 sind also $(q_{-1}, \dots, q_k)$ und $(p_{-1}, \dots, p_k)$ endliche Folgen, falls die Folge $(a_i)_{i\geq 0} = (a_0, \dots, a_k)$ endlich ist.

Wie das folgende Lemma zeigt sind diese Folgen eng mit den Näherungsbrüchen verwandt:

Lemma 2.2.3. *Für $\beta \in \mathbb{R}_{>0}$ und $i \geq 1$ gilt:*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\ a_{i-1} + \cfrac{1}{\beta}}} = \frac{p_{i-1}\beta + p_{i-2}}{q_{i-1}\beta + q_{i-2}}.$$

Insbesondere erhalten wir für $\beta = a_i$ den i-ten Näherungsbruch

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

zu unserer gegebenen Folge $(a_i)_{i\geq 0}$.

Beweis. Wir zeigen die Behauptung durch Induktion nach i:
Für $i = 1$ rechnet man

$$a_0 + \frac{1}{\beta} = \frac{a_0\beta + 1}{\beta} = \frac{p_0\beta + p_{-1}}{q_0\beta + q_{-1}}.$$

Angenommen, die Behauptung wurde bereits für $i \geq 1$ gezeigt. Dann gilt nach Induktionsannahme:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\ a_i + \cfrac{1}{\beta}}} = \frac{p_{i-1}(a_i + \frac{1}{\beta}) + p_{i-2}}{q_{i-1}(a_i + \frac{1}{\beta}) + q_{i-2}}$$

und wir rechnen

$$\frac{p_{i-1}(a_i + \frac{1}{\beta}) + p_{i-2}}{q_{i-1}(a_i + \frac{1}{\beta}) + q_{i-2}} = \frac{p_i + p_{i-1}\frac{1}{\beta}}{q_i + q_{i-1}\frac{1}{\beta}} = \frac{p_i\beta + p_{i-1}}{q_i\beta + q_{i-1}}.$$

Also gilt die Behauptung auch für $i+1$. Dies zeigt die erste Aussage des Lemmas. Die zweite Aussage folgt sofort indem man $\beta = a_i$ in die gezeigte Gleichung einsetzt. □

Im weiteren Verlauf werden wir die folgenden Eigenschaften der Folgen $(p_i)_i$ und $(q_i)_i$ benötigen:

Lemma 2.2.4. *Für alle $i \geq 0$ gelten die folgenden Eigenschaften:*

(a) $(q_i)_{i\geq 1}$ *wächst streng monoton und es gilt $q_i \geq i$.*

(b) $p_{i-1}q_i - p_iq_{i-1} = (-1)^i$. *Insbesondere gilt $ggT(p_i, q_i) = 1$.*

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

(d) $A_{2i} < A_{2(i+1)}$, *also wächst $(A_0, A_2, \dots)$ streng monoton.*

(e) $A_{2i+1} > A_{2i+3}$, *also fällt $(A_1, A_3, \dots)$ streng monoton.*

Beweis. (a) Wir beweisen zunächst die Aussage $q_i \geq i$ induktiv: Es gilt $q_0 = 1 \geq 0$ und $q_1 = a_1q_0 + q_{-1} = a_1 \geq 1$. Falls $q_i \geq i$ für ein $i \geq 1$ bereits gezeigt wurde, so gilt

$$q_{i+1} = q_ia_{i+1} + q_{i-1} \geq q_i + q_{i-1} \geq i + 1.$$

Die strenge Monotonie folgt aus

$$q_{i+1} = a_{i+1}q_i + q_{i-1} > q_i \text{ für } i \geq 1.$$

(b) Für $i = 0$ gilt die Behauptung trivialerweise wegen $p_{-1} = 1, q_0 = 1$ und $p_0 = a_0, q_{-1} = 0$. Wir bemerken zunächst, dass sich die Rekursionsgleichung für $i \geq 1$ elegant als Matrixmultiplikation schreiben lässt:

$$\begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix} = \begin{pmatrix} p_{i-1} & p_{i-2} \\ q_{i-1} & q_{i-2} \end{pmatrix} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$$

Hieraus folgt

$$\begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix} = \prod_{k=0}^{i} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Wenden wir auf beiden Seiten die Determinante an, so erhalten wir:

$$-(p_{i-1}q_i - p_iq_{i-1}) = \prod_{k=0}^{i} \det \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Nun folgt (b) aus der Gleichung

$$\det \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} = -1.$$

(c) Mit Hilfe von (b) folgt dies sofort aus der Rechnung:

$$A_{i+1} - A_i = \frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i} = \frac{p_{i+1}q_i - p_iq_{i+1}}{q_{i+1}q_i} = -\frac{(-1)^{i+1}}{q_{i+1}q_i}.$$

(d) Mit (c) rechnen wir

$$A_{2(i+1)} - A_{2i} = A_{2(i+1)} - A_{2i+1} + A_{2i+1} - A_{2i} = \frac{-1}{q_{2(i+1)}q_{2i+1}} + \frac{1}{q_{2i+1}q_{2i}}.$$

Da $(q_i)_{i\geq 1}$ streng monoton wächst, folgt $\frac{-1}{q_{2(i+1)}q_{2i+1}} + \frac{1}{q_{2i+1}q_{2i}} > 0$.
(e) Wie in (d) rechnen wir

$$A_{2i+1} - A_{2i+3} = \frac{1}{q_{2i+2}q_{2i+1}} - \frac{1}{q_{2i+3}q_{2i+2}}.$$

Da wiederum $(q_i)_{i\geq 1}$ streng monoton wächst, folgt die Ungleichung $\frac{1}{q_{2i+2}q_{2i+1}} - \frac{1}{q_{2i+3}q_{2i+2}} > 0$. □

Konvergenz der Näherungsbrüche[11]

[11] Zu diesem Abschnitt gibt es ein Video:

Der folgende Satz zeigt, dass die Näherungsbrüche einer reellen Zahl α diese tatsächlich gut approximieren.

Satz 2.2.5. *Falls $(a_i)_{i\geq 0}$ die Teilnennerfolge einer reellen Zahl α ist, so gelten für $i \geq 1$ die Abschätzungen:*

$$\frac{1}{q_{i-1}(q_i + q_{i-1})} \leq |\alpha - A_{i-1}| \leq \frac{1}{q_{i-1}q_i} \tag{2.6}$$

und

$$|\alpha - A_i| < |\alpha - A_{i-1}|. \tag{2.7}$$

Beweis. Nach Proposition 2.1.7 liefert der Kettenbruch-Algorithmus Folgen $(\alpha_i)_{i\geq 0}$ und $(a_i)_{i\geq 0}$ mit

$$(\alpha_j - a_j)^{-1} = \alpha_{j+1}, \quad a_{j+1} = \lfloor \alpha_{j+1} \rfloor.$$

Nach Konstruktion des Kettenbruch-Algorithmus gilt für jedes $i \geq 1$:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_{i-1} + \cfrac{1}{\alpha_i}}}.$$

Nun liefert Lemma 2.2.3 gemeinsam mit Lemma 2.2.4 (b) die Gleichung:

$$|\alpha - A_{i-1}| = \left|\frac{p_{i-1}\alpha_i + p_{i-2}}{q_{i-1}\alpha_i + q_{i-2}} - \frac{p_{i-1}}{q_{i-1}}\right| = \left|\frac{(-1)^{i-1}}{q_{i-1}(q_{i-1}\alpha_i + q_{i-2})}\right| \tag{2.8}$$

Für $i \geq 1$ sind die Zahlen $q_{i-1}(q_{i-1}\alpha_i + q_{i-2})$ positiv und wir erhalten

$$|\alpha - A_{i-1}| = \frac{1}{q_{i-1}(q_{i-1}\alpha_i + q_{i-2})}. \tag{2.9}$$

Da a_i die Abrundung von α_i ist, gilt $\alpha_i \geq a_i$ und wir leiten aus (2.9) unter Verwendung der Rekursionsgleichung $q_i = q_{i-1}a_i + q_{i-2}$ die Ungleichung

$$|\alpha - A_{i-1}| \leq \frac{1}{q_{i-1}(q_{i-1}a_i + q_{i-2})} = \frac{1}{q_{i-1}q_i}$$

her. Andererseits gilt auch $\alpha_i < a_i + 1$ und wir erhalten mit der Rekursion $q_i = q_{i-1}a_i + q_{i-2}$ die Abschätzung von unten:

$$|\alpha - A_{i-1}| > \frac{1}{q_{i-1}(q_{i-1}(a_i+1) + q_{i-2})} = \frac{1}{q_{i-1}(q_i + q_{i-1})}. \tag{2.10}$$

Dies zeigt (2.6). Wir können nun (2.7) aus der bereits gezeigten Abschätzung (2.6) und den grundlegenden Eigenschaften der Folgen $(q_i)_{i\geq -1}$ und $(a_i)_{i\geq 0}$ herleiten:

$$|\alpha - A_i| \overset{(2.6)}{\leq} \frac{1}{q_i q_{i+1}} \overset{[12]}{=} \frac{1}{q_i(a_{i+1}q_i + q_{i-1})} \overset{[13]}{\leq} \frac{1}{q_i(q_i + q_{i-1})} \overset{[14]}{\leq} \frac{1}{q_{i-1}(q_i + q_{i-1})} \overset{(2.10)}{<} |\alpha - A_{i-1}| \tag{2.11}$$

Dies zeigt (2.7). □

[12] Hier verwenden wir die Rekursion $q_{i+1} = a_{i+1}q_i + q_{i-1}$.

[13] Es gilt $a_{i+1} \in \mathbb{N}$ und somit $a_{i+1} \geq 1$.

[14] Die Folge $(q_i)_{i\geq 0}$ wächst monoton. Es gilt also $q_{i-1} \leq q_i$. Für $i \geq 1$ wächst sie sogar strikt monoton.

Eine unmittelbare Konsequenz aus dem obigen Satz ist die Konvergenz der Näherungsbrüche:

Korollar 2.2.6. *Die Folge der Näherungsbrüche $(A_n)_{n\geq 0}$ zu einer irrationalen Zahl α konvergiert gegen α.*

Beweis. Es gilt für $i \geq 1$:

$$|\alpha - A_i| \leq \frac{1}{q_i q_{i+1}} \leq \frac{1}{i(i+1)}.$$

Da die rechte Seite für $i \to \infty$ gegen 0 konvergiert, folgt die gewünschte Konvergenz. □

Definition 2.2.7. Für eine reelle Zahl α mit Teilnennerfolge $(a_i)_{i\geq 0}$ definieren wir

$$[a_0; a_1, \dots] := \begin{cases} [a_0; a_1, \dots, a_k] & \text{falls } \alpha = [a_0; a_1, \dots, a_k] \in \mathbb{Q} \\ \lim_{n\to\infty}[a_0; a_1, \dots, a_n] & \text{falls } \alpha \notin \mathbb{Q}. \end{cases}$$

Wir nennen $[a_0; a_1, \dots]$ die Kettenbruchentwicklung zu α.

Wir können also den rationalen und den irrationalen Fall zusammenfassen zu:

Korollar 2.2.8. *Für jedes $\alpha \in \mathbb{R}$ existiert die Kettenbruchentwicklung und es gilt:*

$$[a_0; \dots] = \alpha.$$

Des Weiteren halten wir noch die folgende Abschätzung fest auf die wir später zurückkommen werden:

Korollar 2.2.9 (Dirichletscher Approximationssatz)**.** *Für jede reelle Zahl α und $i \geq 0$ gilt:*

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

Beweis. Falls $i = 0$, so gilt $p_0 = a_0 = \lfloor \alpha \rfloor$ und $q_0 = 1$. In diesem Fall gilt die Aussage trivialerweise:

$$|\alpha - \lfloor \alpha \rfloor| < 1.$$

Wir dürfen also $i > 0$ annehmen. Falls $\alpha = [a_0; a_1, \dots, a_k]$ eine rationale Zahl ist, so gilt $\alpha = A_k$. In diesem Fall ist die Aussage für $i = k$ trivialerweise erfüllt. Wir können also im Fall endlicher Kettenbrüche auch $i < k$ annehmen. Insbesondere dürfen wir annehmen, dass q_{i+1} definiert ist. Wegen $q_i < q_{i+1}$ folgt die Aussage sofort aus der in (2.6) gezeigten Abschätzung

$$\left|\alpha - \frac{p_i}{q_i}\right| = |\alpha - A_i| \leq \frac{1}{q_i q_{i+1}}.$$

□

Da die rationalen Zahlen dicht in den reellen Zahlen liegen, können wir jede reelle Zahl α beliebig gut durch rationale Zahlen approximieren. Je besser wir approximieren möchten, desto größere Nenner werden wir allerdings hinnehmen müssen. Somit macht es Sinn die Güte der Approximation anhand der Größe der Nenner zu messen. In diesem Sinne können wir den Dirichletschen Approximationssatz als ein Gütesiegel für die Näherungsbrüche verstehen. In der nächsten Vorlesung werden wir sehen, dass die Näherungsbrüche die Zahl α tatsächlich bestmöglich approximieren.

Ausblick und offene Fragen:

Für unsere Zwecke reicht es einer gegebenen Zahl α eine Folge $(a_i)_{i \geq 0}$ zuzuordnen, sodass

$$\alpha = [a_0; a_1, \dots].$$

Es ist auf den ersten Blick nicht offensichtlich, ob man auf diese Weise jede Folge $(a_i)_{i\geq 0} \in \mathbb{Z} \times \mathbb{N}^{\mathbb{N}}$ erhält. Tatsächlich werden wir im Übungsbetrieb sehen, dass der Limes

$$\lim_{n\to\infty} [a_0; a_1, ..., a_n]$$

für jede Folge $(a_i)_{i\geq 0} \in \mathbb{Z} \times \mathbb{N}^{\mathbb{N}}$ existiert und dass dieser Grenzwert die Folge $(a_i)_{i\geq 0}$ bereits eindeutig festlegt. Somit wäre gezeigt, dass tatsächlich alle Folgen der Form $(a_i)_{i\geq 0} \in \mathbb{Z} \times \mathbb{N}^{\mathbb{N}}$ als Teilnennerfolgen reeller Zahlen auftreten.

Wir haben bereits gesehen, dass man anhand der Teilnennerfolge einer reellen Zahl ablesen kann, ob diese rational oder irrational ist. Interessanterweise kann man mit relativ wenig Aufwand folgenden Satz zeigen, den wir im Übungsbetrieb genauer betrachten werden:

Satz 2.2.10. *$\alpha \in \mathbb{R}$ ist genau dann algebraisch vom Grad*[15] *2, wenn die Teilnennerfolge von α ab einer gewissen Stelle periodisch wird.*[16]

[15] Der Grad einer algebraischen Zahl α ist die kleinste natürliche Zahl k, sodass ein Polynom $P \in \mathbb{Q}[X]$ vom Grad k existiert mit $P(\alpha) = 0$.

[16] Ein einfaches Beispiel hierfür haben wir bereits gesehen: $\sqrt{2} = [1; 2, 2, \dots]$.

Dies wirft unmittelbar die Frage auf, ob man auch algebraische Zahlen höheren Grads am Bildungsgesetz ihrer Teilnennerfolgen erkennen kann. Bisher ist keine Regelmäßigkeit für algebraische Zahlen höheren Grades bekannt. Viel schlimmer: Es ist für keine einzige algebraische Zahl vom Grad > 2 bekannt ob die Folge $(a_i)_{i\geq 0}$ beschränkt oder unbeschränkt ist.

Obwohl für algebraische Zahlen vom Grad > 2 die Struktur der Kettenbruchentwicklung kompliziert zu sein scheint, gibt es hingegen transzendente Zahlen, deren Kettenbruchentwicklung einem einfachen Bildungsgesetz folgt: Es gilt zum Beispiel

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, \dots].$$

2.3 *Beste rationale Approximation*

Im Folgenden beschäftigen wir uns mit der Frage, wie wir eine gegebene reelle Zahl möglichst gut durch rationale Zahlen approximieren können.

Beste Näherungen erster und zweiter Art[17]

[17] Zu diesem Abschnitt gibt es ein Video:

Da die rationalen Zahlen dicht in $\mathbb{R}$ liegen, finden wir in jeder noch so kleinen Umgebung um α unendlich viele Brüche ganzer Zahlen. Beschränken wir allerdings die Größe des Nenners, so gibt es in jeder Umgebung von α nur endlich viele Brüche. Die Frage, ob es noch bessere Approximationen mit kleinerem Nenner gibt, führt uns zu folgender Definition:

Definition 2.3.1. Zu einer gegebenen reellen Zahl α nennen wir eine rationale Zahl $\frac{a}{b}$ mit teilerfremden $a \in \mathbb{Z}$, $b \in \mathbb{N}$ eine *beste Näherung erster Art* zu α, wenn für alle $c \in \mathbb{Z}, d \in \mathbb{N}$ mit $\frac{c}{d} \neq \frac{a}{b}$ und $d \leq b$ die Abschätzung

$$\left|\alpha - \frac{c}{d}\right| > \left|\alpha - \frac{a}{b}\right|$$

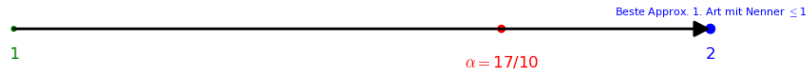
gilt.

Wir möchten diese Definition an einem Beispiel verdeutlichen:

Beispiel 2.3.2. Wir möchten alle besten Näherungen erster Art zu $\alpha = \frac{17}{10}$ finden. Für eine natürliche Zahl N betrachten wir die Menge

$$B_N := \left\{\frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z}, b \in \mathbb{N} \text{ und } b \leq N\right\}$$

aller Brüche mit Nenner $\leq N$ und bestimmen diejenigen Brüche aus B_N, welche minimalen Abstand zu α haben. Wegen $1 \leq \alpha \leq 2$ reicht es die endliche Menge $B_N \cap [1,2]$ zu betrachten.
Für $N = 1$ hat $2 \in B_1 \cap [1,2] = \{\frac{1}{1}, \frac{2}{1}\}$ minimalen Abstand zu α:



Für $N = 2$ hat $\frac{3}{2} \in B_2 \cap [1,2]$ minimalen Abstand zu α:

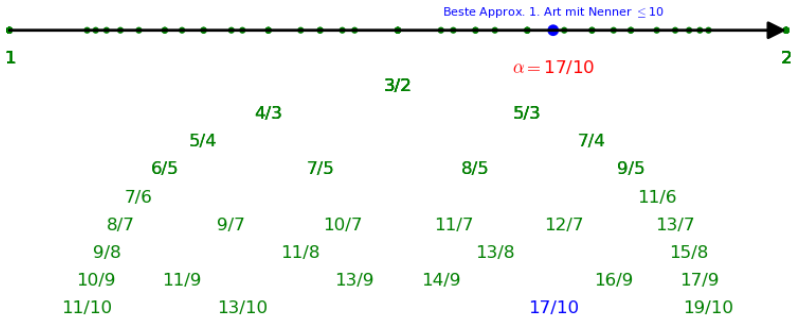
Für $N = 3$ hat $\frac{5}{3} \in B_3 \cap [1,2]$ minimalen Abstand zu α:

Für $N = 7$ hat[18] $\frac{12}{7} \in B_7 \cap [1,2]$ minimalen Abstand zu α:

Für $N = 10$ hat[19] $\frac{17}{10} \in B_{10} \cap [1,2]$ minimalen Abstand zu α:

[18] In den Fällen $N = 4$, $N = 5$ und $N = 6$ wird der minimale Abstand ebenfalls bei $\frac{5}{3}$ angenommen. Erst für $N = 7$ bekommen wir eine bessere Näherung.

[19] In den Fällen $N = 8$ und $N = 9$ wird der minimale Abstand ebenfalls bei $\frac{12}{7}$ angenommen. Erst für $N = 10$ bekommen wir eine bessere Näherung.



Wir können für $N \geq 10$ keine weiteren besten Näherungen erster Art mehr bekommen, da bereits $\alpha = \frac{17}{10}$. Somit haben wir die vollständige Liste

$$\{2, \frac{3}{2}, \frac{5}{3}, \frac{12}{7}, \frac{17}{10}\}$$

aller besten Näherungen erster Art zu $\alpha = \frac{17}{10}$ bestimmt. Es fällt auf, dass diese Liste abgesehen von A_0 alle Näherungsbrüche

$$A_0 = 1, A_1 = 2, A_2 = \frac{5}{3}, A_3 = \frac{17}{10}$$

zu α enthält.

Obiges Beispiel lässt bereits vermuten, dass die Näherungsbrüche A_i zu α für $i \geq 1$ beste Näherungen erster Art zu α sind. Umgekehrt sieht man, dass es beste Näherungen erster Art gibt, die keine Näherungsbrüche sind. Um die Näherungsbrüche unter den besten Näherungen erster Art zu charakterisieren benötigen wir eine Verschärfung des Begriffs „Näherung erster Art“:

Definition 2.3.3. Zu einer gegebenen reellen Zahl α nennen wir eine rationale Zahl $\frac{a}{b}$ mit teilerfremden $a \in \mathbb{Z}$, $b \in \mathbb{N}$ eine *beste Näherung zweiter Art* zu α, wenn für alle $c \in \mathbb{Z}, d \in \mathbb{N}$ mit $\frac{c}{d} \neq \frac{a}{b}$ und $d \leq b$ die Abschätzung

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

gilt.

Bemerkung 2.3.4. Für $d \leq b$ folgt aus

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

bereits die Ungleichung

$$\left|\alpha - \frac{c}{d}\right| = \frac{1}{d}|d\alpha - c| \geq \frac{1}{b}|d\alpha - c| > \frac{1}{b}|b\alpha - a| = \left|\alpha - \frac{a}{b}\right|.$$

Somit ist jede beste Näherung zweiter Art zu α auch eine beste Näherung erster Art zu α. Die Umkehrung gilt nicht, wie wir am folgenden Beispiel sehen:

Beispiel 2.3.5. Wir bestimmen zu $\alpha = \frac{17}{10}$ alle besten Näherungen zweiter Art. Da wir bereits wissen, dass jede beste Näherung zweiter Art auch eine beste Näherung erster Art ist, können wir uns in den folgenden Betrachtungen auf die in Beispiel 2.3.2 bestimmten besten Näherungen erster Art

$$\left\{2, \frac{3}{2}, \frac{5}{3}, \frac{12}{7}, \frac{17}{10}\right\}.$$

beschränken. Wir berechnen für jede beste Näherung erster Art $\frac{a}{b}$ die Zahl $|b\alpha - a|$.

$\frac{a}{b}$	2	$\frac{3}{2}$	$\frac{5}{3}$	$\frac{12}{7}$	$\frac{17}{10}$
$\lvert b\alpha - a\rvert$	0,3	0,4	0,1	0,1	0

Die Näherungen zweiter Art sind nun genau diejenigen Näherungen erster Art für welche der Wert $|b\alpha - a|$ strikt kleiner ist als alle vorherigen Werte von $|b\alpha - a|$ in der obigen Tabelle. Somit sind

$$\{2, \frac{5}{3}, \frac{17}{10}\}$$

alle Näherungen zweiter Art. Es fällt auf, dass dies genau die Menge $\{A_1, A_2, A_3\}$ ist. Wir werden gleich sehen, dass das kein Zufall ist.

Satz 2.3.6. *Jede beste Näherung zweiter Art zu $\alpha \in \mathbb{R}$ ist ein Näherungsbruch von α.*

Beweis. [20] Ist α rational, sagen wir $\alpha = \frac{c}{d}$ mit $d > 0$, und ist $\frac{a}{b}$ mit $b \in \mathbb{N}$ eine beste Näherung zweiter Art für α, dann folgt $b \leq d$. Insbesondere stimmt die Aussage des Satzes, wenn α eine ganze Zahl ist. Wir dürfen im Beweis also annehmen, dass α keine ganze Zahl ist.

Sei nun $\frac{a}{b} \in \mathbb{Q} \setminus \{A_0, A_1, \dots\}$ mit $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Unser Ziel ist es zu zeigen, dass $\frac{a}{b}$ keine beste Näherung zweiter Art zu α sein kann. Je nach relativer Lage von $\frac{a}{b}$ zu α, A_0 und A_1 unterscheiden wir vier Fälle. In jedem der vier Fälle werden wir sehen, dass es einen Näherungsbruch gibt, der eine bessere Näherung zu α ist als $\frac{a}{b}$.

[20] Dieser Beweis ist nicht wesentlich für den weiteren Verlauf der Vorlesung. Der Vollständigkeit halber möchten wir nicht auf ihn verzichten. Sie verpassen nicht viel, wenn Sie diesen Beweis beim ersten Lesen überspringen. OK, Sie verpassen ein paar **wunderschöne**, handgemalte Skizzen ;-).

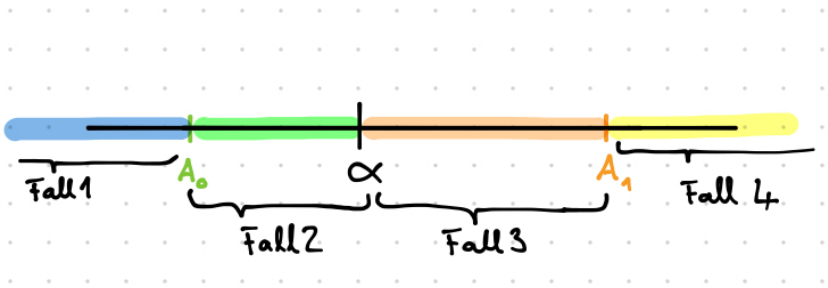


Abbildung 2.1: Skizze

Fall 1: Wir betrachten zunächst den Fall $\frac{a}{b} < A_0$. In diesem Fall gilt

$\frac{a}{b} < A_0 = a_0$. In Anbetracht der Lage[21] der Punkte $\frac{a}{b} < A_0 = a_0 < \alpha$ erhalten wir die Ungleichung

$$\left|\alpha - \frac{a}{b}\right| > |\alpha - a_0|,$$

also insbesondere $|b\alpha - a| = b|\alpha - \frac{a}{b}| > |\alpha - a_0|$. Mit der Wahl $c = a_0$ und $d = 1$ gilt somit $d \leq b$ und $|b\alpha - a| > |\alpha - a_0|$. Dies zeigt, dass $\frac{a}{b}$ im Fall 1 keine beste Näherung zweiter Art sein kann.

Fall 2: Als nächstes betrachten wir den Fall $\frac{a}{b} \in (A_0, \alpha)$. Sei i der größte Index mit $A_{2i} < \frac{a}{b}$, insbesondere gilt also $\frac{a}{b} \neq A_{2i}$. Somit kann der Zähler von

$$\frac{a}{b} - \frac{p_{2i}}{q_{2i}} = \frac{aq_{2i} - bp_{2i}}{bq_{2i}}$$

nicht Null werden, und wir erhalten die Abschätzung

$$\left|\frac{a}{b} - A_{2i}\right| = \left|\frac{a}{b} - \frac{p_{2i}}{q_{2i}}\right| \geq \frac{1}{bq_{2i}}. \tag{2.12}$$

Andererseits erhalten wir unter Verwendung von Lemma 2.2.4 (c) die Ungleichungskette[22]

$$\left|\frac{a}{b} - A_{2i}\right| < |A_{2i+1} - A_{2i}| \leq \frac{1}{q_{2i}q_{2i+1}}. \tag{2.13}$$

Kombinieren wir (2.12) und (2.13), so erhalten wir

$$q_{2i+1} < b.$$

Somit hat A_{2i+1} einen kleineren Nenner als $\frac{a}{b}$. Wir möchten nun zeigen, dass A_{2i+1} die Zahl α besser approximiert als $\frac{a}{b}$. Falls α rational ist und $\alpha = A_{2i+1}$ gilt, ist nichts zu zeigen. Wir dürfen also $\alpha \neq A_{2i+1}$ annehmen. Somit ist A_{2i+2} ebenfalls definiert und wir erhalten[23]

$$\left|\alpha - \frac{a}{b}\right| > \left|A_{2i+2} - \frac{a}{b}\right| \geq \frac{1}{bq_{2i+2}}.$$

Indem wir mit b multiplizieren bekommen wir

$$|b\alpha - a| > \frac{1}{q_{2i+2}}. \tag{2.14}$$

Andererseits folgt aus (2.6) die Ungleichung

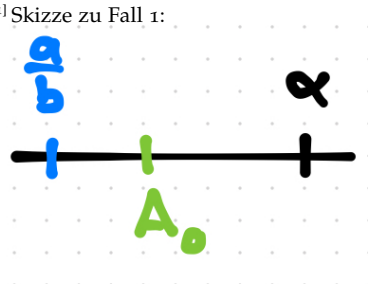
$$|q_{2i+1}\alpha - p_{2i+1}| < \frac{1}{q_{2i+2}}. \tag{2.15}$$

Aus (2.14) und (2.15) folgt nun

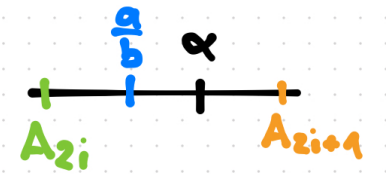
$$|b\alpha - a| > |q_{2i+1}\alpha - p_{2i+1}|.$$

Da wir bereits $q_{2i+1} < b$ gezeigt haben, ist $\frac{a}{b}$ also auch in diesem Fall keine beste Näherung zweiter Art zu α.

[21] Skizze zu Fall 1:

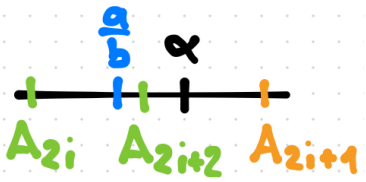


[22] Für die erste Ungleichung in (2.13) beachte man $A_{2i} < \frac{a}{b} < A_{2i+1}$:



Die zweite Ungleichung folgt aus Lemma 2.2.4 (c).

[23] Für die erste Ungleichung beachte man $\frac{a}{b} < A_{2i+2} \leq \alpha$:



Die zweite Ungleichung gilt nach dem gleichen Argument wie in (2.12).

Fall 3:[24] Nun betrachten wir den Fall $\frac{a}{b} \in (\alpha, A_1)$. Sei i der größte Index mit $A_{2i-1} > \frac{a}{b}$. Zunächst folgt aus der Tatsache, dass $\frac{a}{b} \neq A_{2i-1}$ wiederum

$$\left|\frac{a}{b} - A_{2i-1}\right| = \left|\frac{a}{b} - \frac{p_{2i-1}}{q_{2i-1}}\right| \geq \frac{1}{bq_{2i-1}}. \tag{2.16}$$

Andererseits liefert Lemma 2.2.4 (c) in Anbetracht der nebenstehenden Skizze[25] die Ungleichungskette

$$\left|\frac{a}{b} - A_{2i-1}\right| < |A_{2i} - A_{2i-1}| \leq \frac{1}{q_{2i}q_{2i-1}}. \tag{2.17}$$

Kombinieren wir (2.16) und (2.17), so erhalten wir $b > q_{2i}$. Somit ist der Nenner von A_{2i} kleiner als b. Wir möchten nun zeigen, dass A_{2i} eine bessere Approximation für α als $\frac{a}{b}$ ist. Falls $A_{2i} = \alpha$, so ist nichts zu zeigen. Wir dürfen also $A_{2i} \neq \alpha$ annehmen. In diesem Fall ist A_{2i+1} definiert und wir erhalten[26]

$$\left|\alpha - \frac{a}{b}\right| > \left|A_{2i+1} - \frac{a}{b}\right| \geq \frac{1}{bq_{2i+1}}.$$

Indem wir mit b multiplizieren bekommen wir

$$|b\alpha - a| > \frac{1}{q_{2i+1}}. \tag{2.18}$$

Aus (2.6) folgt die Ungleichung

$$|q_{2i}\alpha - p_{2i}| < \frac{1}{q_{2i+1}}. \tag{2.19}$$

Die Ungleichungen (2.18) und (2.19) zusammen liefern

$$|b\alpha - a| > |q_{2i}\alpha - p_{2i}|.$$

Da wir bereits $q_{2i} < b$ gezeigt haben, ist $\frac{a}{b}$ somit auch im Fall 3 keine beste Näherung zweiter Art.

Fall 4:[27] Es verbleibt noch der Fall $\frac{a}{b} > A_1$. Wegen $\alpha \leq A_1 < \frac{a}{b}$ erhalten wir[28]

$$\left|\alpha - \frac{a}{b}\right| \geq \left|A_1 - \frac{a}{b}\right| = \left|\frac{p_1}{q_1} - \frac{a}{b}\right| \geq \frac{1}{bq_1},$$

also

$$|b\alpha - a| \geq \frac{1}{q_1}. \tag{2.20}$$

Andererseits folgt aus (2.6) die Ungleichung

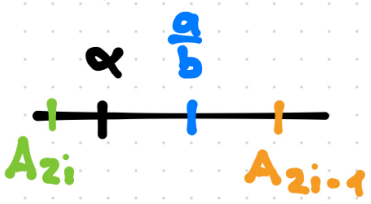
$$|\alpha - A_0| = |q_0\alpha - p_0| \leq \frac{1}{q_1}. \tag{2.21}$$

Aus (2.20) und (2.21) folgt

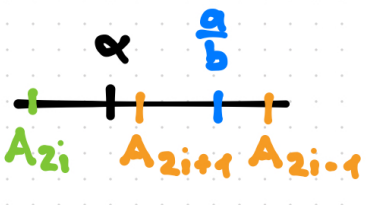
$$|\alpha - A_0| \leq \left|\alpha - \frac{a}{b}\right|.$$

[24] Der Beweis im Fall 3 geht analog zu Fall 2.

[25] Die erste Ungleichung in (2.17) folgt aus $A_{2i} < \frac{a}{b} < A_{2i+1}$:



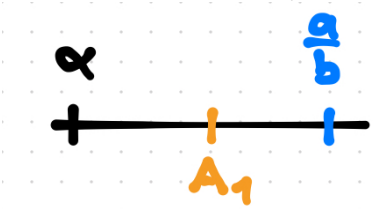
[26] Für die erste Ungleichung beachte man $\alpha \leq A_{2i+1} < \frac{a}{b}$:



Die zweite Ungleichung folgt analog zu (2.12).

[27] Der Beweis von Fall 4 verläuft analog zu Fall 1.

[28] Skizze zu Fall 4: $\alpha \leq A_1 < \frac{a}{b}$:



Wegen $1 \leq b$ erhalten wir auch im letzten der vier Fälle, dass $\frac{a}{b}$ keine beste Näherung zweiter Art zu α ist.

Wir haben somit gezeigt, dass $\frac{a}{b} \in \mathbb{Q} \setminus \{A_0, A_1, \dots\}$ nie eine beste Näherung zweiter Art sein kann. Somit ist jede beste Näherung zweiter Art ein Näherungsbruch. □

Satz 2.3.6 ist aus folgendem Grund interessant. Er erlaubt es uns alle Aussagen, die wir bereits über Näherungsbrüche gezeigt haben, auf beste Näherungen zweiter Art zu übertragen. Des Weiteren gibt er uns ein hinreichendes Kriterium dafür, ob ein gegebener Bruch $\frac{p}{q}$ ein Näherungsbruch zu einer reellen Zahl α ist, ohne dass wir alle Näherungsbrüche von α berechnen müssen. Interessanterweise gilt sogar die Umkehrung des Satzes 2.3.6:

Satz 2.3.7. *Für $i \geq 1$ ist jeder Näherungsbruch A_i einer Zahl α eine beste Näherung zweiter Art für α.*[29]

Beweis. Sei $i \geq 1$ und A_i der i-te Näherungsbruch zu α. Wir möchten zeigen, dass der Näherungsbruch A_i eine beste Näherung zweiter Art zu α ist. Falls $A_i = \alpha$, so ist die Behauptung klar. Somit dürfen wir im folgenden $\alpha \neq A_i$ annehmen[30]. Zunächst betrachten wir für $(a, b) \in \mathbb{Z} \times \{1, 2, \dots, q_i\}$ den Ausdruck $|b\alpha - a|$ und wählen ein Paar $(a, b) \in \mathbb{Z} \times \{1, 2, \dots, q_i\}$ derart, dass

$$|b\alpha - a|$$

minimal wird. Falls es mehrere solche Paare gibt, wählen wir eines mit minimalem b. Aus der Definition von a und b folgt, dass der Bruch $\frac{a}{b}$ eine beste Näherung zweiter Art ist: Angenommen es gäbe ein Paar (c, d) mit $\frac{c}{d} \neq \frac{a}{b}$, $d \leq b$ und $|d\alpha - c| \leq |b\alpha - a|$. Falls $|d\alpha - c| < |b\alpha - a|$ so würde dies der Minimalität von $|b\alpha - a|$ widersprechen. Der Fall $d < b$ und $|d\alpha - c| = |b\alpha - a|$ würde ebenfalls der Minimalität unserer Wahl widersprechen. Gilt hingegen $d = b$ und $|d\alpha - c| = |b\alpha - a|$, so ist notwendigerweise $|b\alpha - a| = \frac{1}{2}$. In diesem Fall erhielten wir allerdings nach Satz 2.2.5 unter Verwendung von $q_i \geq i$ die Ungleichung

$$|q_i\alpha - p_i| \leq \frac{1}{q_{i+1}} \leq \frac{1}{2}.$$

Falls $q_{i+1} > 2$, so gilt also $|q_i\alpha - p_i| < |b\alpha - a|$ im Widerspruch zur Minimalität von (a, b). Es verbleibt der Fall $q_{i+1} = 2$. Da $q_{i+1} \geq i + 1$, erhielten wir $i = 1$. Aus $2 = q_2 > q_1 \geq 1$ würde $q_1 = 1$ folgen. Somit wäre $b = 1$ und wir erhielten $\alpha = a \pm \frac{1}{2}$. Für Zahlen dieser Art sieht man allerdings leicht die Formel $A_1 = a_0 + \frac{1}{2} = \frac{2a_0+1}{2}$, welche $q_1 = 2$ zeigt. Wir erhielten also einen Widerspruch zu $q_1 = 1$. Somit ist also gezeigt, dass $\frac{a}{b}$ eine beste Näherung zweiter Art ist.

Nach Satz 2.3.6 gilt $\frac{a}{b} = A_j$ für ein $j \leq i$. Es bleibt noch zu zeigen, dass $j = i$ gilt. Angenommen es wäre $j < i$ dann erhielten wir unter

[29] Auf die Vorraussetzung $i \geq 1$ können wir nicht verzichten: Zu $\alpha = \frac{17}{10}$ ist $A_0 = 1$ keine beste Näherung zweiter Art, da $|\alpha - 2| < |\alpha - A_0|$. Als kleine Übung können Sie sich gerne überlegen an welcher Stelle der Beweis schiefgeht.

[30] Insbesondere werden wir im folgenden verwenden, dass A_{i+1} existiert.

Verwendung von (2.6), unserer Minimalitätsannahme und nochmals (2.6) die Ungleichungskette

$$\frac{1}{q_{j+1}+q_j} \leq q_j \left|\alpha - A_j\right| = \left|q_j\alpha - p_j\right| < \left|q_i\alpha - p_i\right| \leq \frac{1}{q_{i+1}}.$$

Aufgrund der Monotonie der Folge $(q_i)_{i\geq 1}$ gilt $q_j \leq q_{i-1}$ und $q_{j+1} \leq q_i$, und wir würden aus der obigen Ungleichung

$$q_{i+1} < q_{j+1} + q_j \leq q_i + q_{i-1}$$

erhalten. Andererseits liefert die Rekursionsgleichung $q_{i+1} = q_i a_i + q_{i-1}$ aber die Ungleichung

$$q_{i+1} = q_i a_i + q_{i-1} \geq q_i + q_{i-1}$$

und damit einen Widerspruch. Somit gilt $\frac{a}{b} = A_i$ und A_i ist eine beste Näherung zweiter Art. □

Die Sätze 2.3.6 und 2.3.7 zeigen, dass die Näherungsbrüche im Wesentlichen die besten Näherungen zweiter Art[31] sind. Dies rückt die Näherungsbrüche in ein ganz anderes Licht. Sie sind nicht nur ein Hilfskonstrukt, welches in der Theorie der Kettenbrüche auftritt, sondern spielen eine ausgezeichnete Rolle in der Theorie der rationalen Approximation; schließlich sind sie „beste Näherungen“ in obigem Sinn. Umgekehrt helfen uns Kettenbrüche die rationalen Approximationen einer reellen Zahl besser zu verstehen; schließlich gelten alle bereits gezeigten Eigenschaften der Näherungsbrüche, wie der Dirichletsche Approximationssatz, nun auch für beste Näherungen zweiter Art.

[31] Aufmerksame Leser*innen mögen sich nun fragen, ob man auch die besten Näherungen erster Art explizit beschreiben kann. Tatsächlich lassen sich beste Näherungen erster Art durch *Nebennäherungsbrüche* charakterisieren. Da die Näherungen erster Art allerdings eine schwächere Approximationseigenschaft besitzen, als die besten Näherungen zweiter Art, sind erstere für unsere Zwecke weniger interessant.

Anwendung: Schaltjahre[32]

Als Anwendung der besten Näherung zweiter Art möchten wir die Schaltjahrregeln des gregorianischen Kalenders erklären: Das *tropische Jahr* hat ca. 365,2422 Tage. Wir möchten diese Zahl möglichst gut durch rationale Zahlen approximieren. Zunächst berechnen wir die Kettenbruchentwicklung und erhalten

$$365{,}2422... = [365; 4, 7, 1, 3, 4, \dots].$$

Die ersten Näherungsbrüche sind

$$A_0 = 365, \qquad A_1 = 365 + \frac{1}{4}, \qquad A_2 = 365 + \frac{7}{29},$$
$$A_3 = 365 + \frac{8}{33}, \qquad A_4 = 365 + \frac{31}{128}, \qquad A_5 = 365 + \frac{132}{545}.$$

Die Kettenbruchentwicklung legt folgende Regeln für Schalttage nahe:

[32] Zu diesem Abschnitt gibt es ein Video:

A_0 *Das Jahr hat* 365 *Tage und keine Schaltjahre.* Dieses Kalendersystem wurde im Alten Ägypten verwendet und geht mindestens zurück ins 3. Jahrtausend vor Christus. Bereits den Alten Ägyptern war bekannt, dass dieses Kalendersystem zu einer Verschiebung der Jahreszeiten führt.

A_1 *Das Jahr hat* 365 *Tage und alle* 4 *Jahre ein Schaltjahr.* Julius Cäsar führte diesen *Julianischen Kalender* im Jahre 45 v. Chr. ein. Die durchschnittliche Jahreslänge ist ca. 11 Minuten länger als das tropische Jahr.

A_2 *Das Jahr hat* 365 *Tage und in* 29 *Jahren* 7 *Schaltjahre.* Diese Regel erscheint eher unpraktikabel.

A_3 *Das Jahr hat* 365 *Tage und in* 33 *Jahren gibt es* 8 *Schaltjahre.* Auf den ersten Blick erscheint dies auch nicht besonders praktikabel. Beachtet man allerdings

$$\frac{8}{33} = \frac{24}{99} \approx \frac{24}{100} = \frac{1}{4} - \frac{1}{100},$$

so ergibt sich die Regel: *Alle* 4 *Jahre gibt es* 1 *Schaltjahr. Alle* 100 *Jahre entfällt ein Schaltjahr.* Berechnet man den Fehler zum Näherungsbruch

$$\left(\frac{1}{4} - \frac{1}{100}\right) - \frac{8}{33} = \frac{2}{825},$$

so stellt man fest, dass dieser relativ nahe bei $\frac{1}{400}$ liegt. Dies führt auf die Regel: *Das Jahr hat 365 Tage. Alle* 4 *Jahre gibt es ein Schaltjahr. Das Schaltjahr entfällt alle* 100 *Jahre, es sei denn die Jahreszahl ist durch* 400 *teilbar.* Das ist genau der *Gregorianische Kalender*.

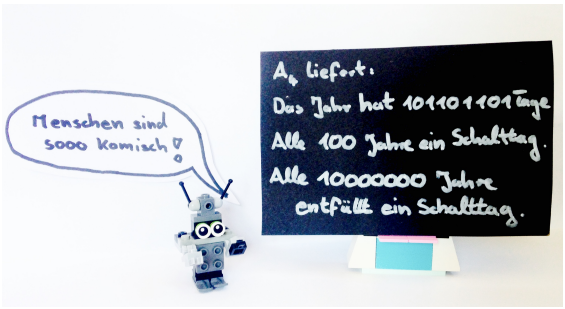


Abbildung 2.2: Der Roboianische Kalender: Einfacher zu merken und viel besser!

Ausblick und offene Fragen

Die besten Näherungen zweiter Art lassen sich auf folgende Art und Weise veranschaulichen. Eine natürliche Zahl q tritt als Nenner einer besten Näherung zweiter Art auf, wenn es kein $d \leq q$ gibt, sodass $d\alpha$ näher an einer ganzen Zahl liegt als $q\alpha$. Dies motiviert die Definition

$$\|x\| := \min_{z \in \mathbb{Z}} |x - z|$$

für den Abstand einer reellen Zahl x zur nächsten ganzen Zahl. Wir haben in dieser Vorlesung gesehen, dass alle Näherungsbrüche A_i mit $i \geq 1$ einer gegebenen Zahl α stets beste Näherungen zweiter Art für α sind. Für Näherungsbrüche $A_i = \frac{p_i}{q_i}$ ist somit $\|q_i\alpha\|$ besonders klein. Der Dirichletsche Approximationssatz gibt eine qualitative Abschätzung

$$\|q_i\alpha\| \leq |q_i\alpha - p_i| = q_i|\alpha - A_i| < \frac{1}{q_i}. \tag{2.22}$$

Mit dieser Vorbemerkung haben wir fast schon die folgende Proposition bewiesen:

Proposition 2.3.8. *Für jede reelle Zahl α gilt*

$$\liminf_{q\to\infty} q \cdot \|q\alpha\|^2 = 0.$$

Beweis. Falls $\alpha = \frac{a}{b}$, so ist die Aussage trivial; schließlich ist $\|q\alpha\| = 0$ für jedes Vielfache q von b. Falls α hingegen irrational ist, ist die Folge $(q_i)_{i\geq 1}$ unendlich. Für q_i gilt nach dem Dirichletschen Approximationssatz die Abschätzung (2.22) und somit

$$q_i\|q_i\alpha\|^2 < \frac{1}{q_i} \to 0 \text{ für } i \to \infty,$$

da die Folge $q_i \geq i$ nach Lemma 2.2.4 (a) gilt. □

Es liegt nun die Frage nahe, ob wir in der obigen Aussage einen der beiden Terme $\|q\alpha\|$ in $\|q\alpha\|^2 = \|q\alpha\| \cdot \|q\alpha\|$ durch $\|q\beta\|$ mit einer beliebigen reellen Zahl β ersetzen können. Überraschenderweise stellt sich diese Frage als ein sehr tiefliegendes Problem heraus:

Vermutung (Littlewood-Conjecture)**.** *Für $\alpha, \beta \in \mathbb{R}$ gilt*

$$\liminf_{q\to\infty} q\|q\alpha\|\|q\beta\| = 0.$$

Im Fall $\alpha = \beta$ folgt diese Vermutung aus der Theorie der Kettenbrüche, siehe Proposition 2.3.8. Sobald eine der Zahlen α oder β rational ist, gilt die Vermutung trivialerweise. Der allgemeine Fall ist allerdings bis heute offen.

2.4 *Der Satz von Liouville*

In diesem Abschnitt möchten wir zeigen, dass reelle Zahlen, die sich sehr gut rational approximieren lassen, irrational oder gar transzendent sind.

Approximation (ir)rationaler Zahlen[33]

[33] Zu diesem Abschnitt gibt es ein Video:

Wir hatten bereits im letzten Abschnitt gesehen, dass die Näherungsbrüche einer gegebenen Zahl α diese bestmöglich approximieren. Wenn die Zahl α irrational ist, so gibt es unendlich viele verschiedene Näherungsbrüche. Zusammen mit dem Dirichletschen Approximationssatz erhalten wir:

Proposition 2.4.1. *Falls $\alpha \in \mathbb{R}$ irrational ist, so besitzt die Ungleichung*

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{1+\epsilon}}$$

für jedes $\epsilon \in (0,1)$ unendlich viele Lösungen $\frac{p}{q} \in \mathbb{Q}$.

Beweis. Nach dem Dirichletschen Approximationssatz gibt uns jeder Näherungsbruch $A_n = \frac{p_n}{q_n}$ eine Lösung der Ungleichung

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2} \leq \frac{1}{q_n^{1+\epsilon}}.$$

□

Tatsächlich gilt sogar die Umkehrung dieser Aussage im folgenden Sinne:

Proposition 2.4.2. *Falls α eine rationale Zahl ist, so besitzt die Ungleichung*

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{1+\epsilon}} \tag{2.23}$$

für jedes $\epsilon > 0$ höchstens endlich viele Lösungen $\frac{p}{q} \in \mathbb{Q}$ mit $p \in \mathbb{Z}, q \in \mathbb{N}$.

Beweis. Wir zeigen zunächst die folgende
Behauptung: Zu α gibt es eine positive Konstante[34] *$c = c(\alpha)$, sodass für alle rationalen Zahlen $\frac{p}{q} \neq \alpha$ mit $ggT(p,q) = 1$ und $q \in \mathbb{N}$ die Ungleichung*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q}$$

erfüllt ist.
Beweis der Behauptung: Sei $\alpha = \frac{a}{b}$ mit teilerfremden $a \in \mathbb{Z}$ und $b \in \mathbb{N}$. Wir setzen $c(\alpha) := \frac{1}{b}$. Dann gilt

$$\left|\alpha - \frac{p}{q}\right| = \frac{|aq - pb|}{bq}.$$

Die linke Seite ist wegen $\frac{a}{b} \neq \frac{p}{q}$ von Null verschieden. Somit ist auch $|aq - pb|$ eine von Null verschiedene ganze Zahl[35], also gilt $|aq - pb| \geq 1$. Wir erhalten

$$\left|\alpha - \frac{p}{q}\right| = \frac{|aq - pb|}{bq} \geq \frac{1}{bq} = \frac{c(\alpha)}{q}.$$

[34] Die Notation $c = c(\alpha)$ bedeutet, dass die Konstante c nur von α abhängt. Insbesondere hängt die Konstante nicht von $\frac{p}{q}$ ab.

[35] Beinahe jeder Satz der transzendenten Zahlentheorie verwendet an irgendeiner Stelle, dass eine von Null verschiedene ganze Zahl Absolutbetrag ≥ 1 hat.

Dies zeigt die Behauptung.

Wir leiten nun die Aussage der Proposition aus der Behauptung ab. Zu $\epsilon > 0$ definieren wir $N := c(\alpha)^{-\frac{1}{\epsilon}}$. Für $\frac{p}{q}$ mit $q > N$ gilt in Anbetracht der obigen Behauptung

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q} = \frac{1}{qN^{\epsilon}} > \frac{1}{q^{1+\epsilon}}.$$

Somit kann es keine Lösung der Ungleichung (2.23) mit $q > N$ geben. Andererseits gilt für jede Lösung $\frac{p}{q}$ von (2.23) mit $1 \leq q \leq N$ bereits

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{1+\epsilon}} \leq 1.$$

Da es in jeder Umgebung von α aber nur endlich viele Brüche mit beschränktem Nenner geben kann, folgt die Aussage der Proposition. □

Eine Lösung $\frac{p}{q}$ der Ungleichung

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{1+\epsilon}}$$

zu einer gegebenen Zahl α liefert stets einen Bruch, der α, gemessen an der Größe des Nenners q von $\frac{p}{q}$, gut approximiert[36]. Die beiden obigen Propositionen zeigen also, dass sich rationale und irrationale Zahlen in ihrer Approximierbarkeit durch rationale Zahlen grundlegend unterscheiden. Während es für irrationale Zahlen also stets unendlich viele Brüche gibt, die die Zahl α in diesem Sinne „gut" approximieren, gibt es für rationale Zahlen nur endlich viele solche „guten" Approximationen.

[36] Tatsächlich werden wir in den Übungen sehen, dass für $\epsilon > 1$ eine Lösung $\frac{p}{q}$ unter einer kleinen Zusatzbedingung an q bereits ein Näherungsbruch ist.

Wir erinnern daran, dass eine Zahl $\alpha \in \mathbb{C}$ *algebraisch* genannt wird, falls es ein von Null verschiedenes Polynom $0 \neq P \in \mathbb{Q}[X]$ gibt mit $P(\alpha) = 0$. Im Folgenden möchten wir Proposition 2.4.2 von rationalen Zahlen auf beliebige algebraische Zahlen verallgemeinern. Angenommen wir haben eine reelle algebraische Zahl α, die sogar Nullstelle eines *ganzzahligen* Polynoms

$$P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$$

ist. Da α eine Nullstelle von P ist, können wir den Linearfaktor $X - \alpha$ abspalten[37]:

$$P = (X - \alpha) \cdot Q \quad \text{mit } Q \in \mathbb{R}[X].$$

[37] Das sieht man zum Beispiel durch Polynomdivision im Ring $\mathbb{R}[X]$.

Sei $\frac{p}{q} \neq \alpha$ ein Bruch mit $q \in \mathbb{N}$ und $P(\frac{p}{q}) \neq 0$. Es folgt $Q(\frac{p}{q}) \neq 0$ und wir erhalten

$$\left|\frac{p}{q} - \alpha\right| = \frac{|P(\frac{p}{q})|}{|Q(\frac{p}{q})|}.$$

Wegen $P(\frac{p}{q}) \neq 0$ und der Gleichung

$$q^n P(\frac{p}{q}) = a_n p^n + a_{n-1} p^{n-1} q + ... + a_0 q^n \in \mathbb{Z}$$

ist $q^n P(\frac{p}{q})$ eine von Null verschiedene ganze Zahl[38] und wir erhalten $|P(\frac{p}{q})| \geq \frac{1}{q^n}$. Dies zeigt

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{1}{q^n |Q(\frac{p}{q})|}. \tag{2.24}$$

Wir werden später sehen, dass wir $\frac{1}{|Q(\frac{p}{q})|}$ explizit durch eine nur von α abhängige Konstante $c(\alpha)$ abschätzen können. Dies wird es uns ermöglichen, ein Analogon von Proposition 2.4.2 für algebraische Zahlen zu beweisen. Motiviert durch diese Rechnung werden wir uns nun der Aufgabe zuwenden zu einer gegebenen algebraischen Zahl α ein *ganzzahliges* Polynom von möglichst kleinem Grad zu finden, welches α als Nullstelle hat.

[38] ... schon wieder...

Das ganzzahlige Minimalpolynom

Im folgenden Unterabschnitt führen wir das ganzzahlige Minimalpolynom einer algebraischen Zahl ein. Ähnlich zum Minimalpolynom eines linearen Endomorphismus können wir das Minimalpolynom einer algebraischen Zahl definieren.

Lemma 2.4.3. *Zu einer algebraischen Zahl $\alpha \in \mathbb{C}$ gibt es genau ein normiertes*[39] *Polynom $P \in \mathbb{Q}[X]$ kleinsten Grades mit $P(\alpha) = 0$. Dieses Polynom wird* Minimalpolynom von α über $\mathbb{Q}$ *genannt und mit* $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$ *bezeichnet. Der* Grad von α *ist der Grad des Minimalpolynoms.*

[39] Ein Polynom $P = a_n X^n + \cdots + a_0$ heißt normiert, wenn für den *Leitkoeffizienten* a_n die Gleichung $a_n = 1$ gilt. Die Normierung macht das Minimalpolynom eindeutig und schließt gleichzeitig das Nullpolynom aus.

Beweis. Da α algebraisch ist, gibt es ein Polynom $a_n X^n + \cdots + a_0 \in \mathbb{Q}[X]$ mit $a_n \neq 0$, welches α als Nullstelle hat. Indem wir durch a_n teilen erhalten wir insbesondere ein normiertes Polynom mit α als Nullstelle. Somit ist die Menge der normierten Polynome mit rationalen Koeffizienten, welche α als Nullstelle haben, nicht leer. Es gibt also normierte Polynome kleinsten Grades mit dieser Eigenschaft. Dies zeigt die Existenz.

Nun zur Eindeutigkeit: Seien P_1 und P_2 zwei normierte Polynome kleinsten Grades mit $P_1(\alpha) = P_2(\alpha) = 0$, so erhalten wir durch Polynomdivision zwei Polynome $Q, R \in \mathbb{Q}[X]$ mit

$$P_1 = QP_2 + R \text{ und } \deg(R) < \deg(P_2).$$

Da P_1 und P_2 vom selben Grad sind, folgt $\deg(Q) = 0$ also $Q \in \mathbb{Q}$. Da außerdem P_1 und P_2 normiert sind, liefert der Vergleich der Leitkoeffizienten $Q = 1$. Setzen wir α in die obige Gleichung ein, so sehen

wir

$$0 = P_1(\alpha) = Q(\alpha)\underbrace{P_2(\alpha)}_{=0} + R(\alpha) = R(\alpha).$$

Wäre $R \neq 0$ so könnten wir R normieren und erhielten ein Polynom kleineren Grades mit Nullstelle α, was im Widerspruch zur Minimalität von P_1 und P_2 stünde. Es gilt also $R = 0$ und daher $P_1 = P_2$. Dies zeigt die Eindeutigkeit. □

Indem wir das Minimalpolynom mit einer geeigneten natürlichen Zahl multiplizieren erhalten wir das ganzzahlige Minimalpolynom:

Definition 2.4.4. Sei $\alpha \in \mathbb{C}$ eine algebraische Zahl mit Minimalpolynom $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$. Sei

$$d := \min\left\{n \in \mathbb{N} : n \cdot \mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[X]\right\}$$

der Hauptnenner der Koeffizienten des Minimalpolynoms. Dann heißt das Polynom

$$\mathrm{MinPol}_{\mathbb{Z}}(\alpha) := d \cdot \mathrm{MinPol}_{\mathbb{Q}}(\alpha)$$

das *ganzzahlige Minimalpolynom von* α.

Beispiel 2.4.5. Wir betrachten die Zahl $\alpha = \frac{i}{2} \in \mathbb{C}$. Es gilt

$$\left(\frac{i}{2}\right)^2 = -\frac{1}{4}.$$

Somit ist α, als Nullstelle des Polynoms $P = X^2 + \frac{1}{4}$, algebraisch. Tatsächlich ist P auch das Minimalpolynom von α über $\mathbb{Q}$: Ein von Null verschiedenes Polynom vom Grad 0 hat keine Nullstellen und ein Polynom vom Grad 1 über $\mathbb{Q}$ hat genau eine Nullstelle und diese liegt in $\mathbb{Q}$. Wegen $\alpha \notin \mathbb{Q}$ kann α also nicht die Nullstelle eines Polynoms ungleich Null vom Grad ≤ 1 sein. Somit gilt $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = X^2 + \frac{1}{4}$. Der Hauptnenner der Koeffizienten von $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$ ist 4. Somit ist das ganzzahlige Minimalpolynom von α gegeben durch

$$\mathrm{MinPol}_{\mathbb{Z}}(\alpha) = 4X^2 + 1.$$

Der Satz von Liouville

Wie bereits oben angedeutet können wir nun Proposition 2.4.2 auf algebraische Zahlen höheren Grades verallgemeinern:

Satz 2.4.6 (Liouville)**.** *Für jedes $\epsilon > 0$ und jede reelle algebraische Zahl α vom Grad n hat die Ungleichung*

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{n+\epsilon}} \tag{2.25}$$

höchstens endlich viele Lösungen $\frac{p}{q} \in \mathbb{Q}$ mit $q \in \mathbb{N}$.

Beweis. Wir zeigen zunächst die folgende[40]
Behauptung: Zu α gibt es eine positive Konstante $c = c(\alpha)$, sodass für alle rationalen Zahlen $\frac{p}{q} \neq \alpha$ mit $ggT(p,q) = 1$ und $q \in \mathbb{N}$ die Ungleichung

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$$

erfüllt ist.
Beweis der Behauptung:
Sei $\frac{p}{q} \neq \alpha$ mit $\mathrm{ggT}(p,q) = 1$, $q \in \mathbb{N}$. Zunächst bemerken wir, dass das Minimalpolynom von α über $\mathbb{Q}$ keine Nullstelle in $\frac{p}{q}$ haben kann. Andernfalls könnten wir durch $X - \frac{p}{q}$ teilen und erhielten ein Polynom echt kleineren Grades mit Nullstelle α. Da sich das ganzzahlige Minimalpolynom

$$P := \mathrm{MinPol}_{\mathbb{Z}}(\alpha) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X].$$

von $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$ nur um einen ganzzahligen Faktor unterscheidet, folgt ebenfalls

$$P(\frac{p}{q}) \neq 0.$$

Wir haben in der Einleitung zu diesem Kapitel in (2.24) bereits die Abschätzung

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{1}{q^n |Q(\frac{p}{q})|} \tag{2.26}$$

gezeigt, wobei das Polynom $Q \in \mathbb{R}[X]$ durch $P = (X - \alpha)Q$ definiert ist. Wir möchten nun den Term $\frac{1}{|Q(\frac{p}{q})|}$ durch eine nur von α abhängige Konstante abschätzen. Wir erinnern für $i \geq 1$ zunächst an die Formel[41]

$$\left(\frac{p}{q} - \alpha\right)\left(\alpha^{i-1} + \alpha^{i-2}\frac{p}{q} + \ldots + \alpha(\frac{p}{q})^{i-2} + (\frac{p}{q})^{i-1}\right) = (\frac{p}{q})^i - \alpha^i.$$

Unter Verwendung dieser Formel und $P(\alpha) = 0$ erhalten wir

$$\begin{aligned} Q(\frac{p}{q}) = \frac{P(\frac{p}{q})}{\frac{p}{q} - \alpha} = \frac{P(\frac{p}{q}) - P(\alpha)}{\frac{p}{q} - \alpha} &= \frac{\sum_{i=1}^n a_i \left((\frac{p}{q})^i - \alpha^i\right)}{\frac{p}{q} - \alpha} \\ &= \sum_{i=1}^n a_i \left(\alpha^{i-1} + \alpha^{i-2}\frac{p}{q} + \cdots + (\frac{p}{q})^{i-1}\right). \end{aligned} \tag{2.27}$$

Wir nehmen nun zunächst an, dass $0 < |\alpha - \frac{p}{q}| < 1$ erfüllt ist. Die Annahme liefert zusammen mit der Dreiecksungleichung die obere Schranke $|\frac{p}{q}| < 1 + |\alpha|$ für den Betrag von $\frac{p}{q}$. Aus (2.27) folgern wir

[40] Man beachte die Analogie zum Beweis von Proposition 2.4.2.

[41] Die Hornersche Regel

$$(x-y)(x^{i-1} + yx^{i-2} + \cdots + y^{i-1}) = x^i - y^i$$

sollte aus der Analysis bekannt sein. Man zeigt diese Gleichung leicht durch Ausmultiplizieren.

unter nochmaliger Verwendung der Dreiecksungleichung

$$\left|Q(\frac{p}{q})\right| = \left|\sum_{i=1}^{n} a_i \left(\alpha^{i-1} + \alpha^{i-2}\frac{p}{q} + \cdots + (\frac{p}{q})^{i-1}\right)\right|$$
$$\leq \sum_{i=1}^{n} |a_i| \sum_{j=0}^{i-1} |\alpha|^j \left|\frac{p}{q}\right|^{i-1-j} \leq \sum_{i=1}^{n} |a_i| \sum_{j=0}^{i-1} |\alpha|^j (1+|\alpha|)^{i-1-j}. \quad (2.28)$$

Wir bemerken, dass die positive Zahl

$$c'(\alpha) := \left(\sum_{i=1}^{n} |a_i| \sum_{j=0}^{i-1} |\alpha|^j (1+|\alpha|)^{i-1-j}\right)^{-1}$$

nur von α und nicht von $\frac{p}{q}$ abhängt[42]. Somit folgt aus (2.26) und (2.28), im Fall $0 < |\alpha - \frac{p}{q}| < 1$, die gewünschte Abschätzung

$$|\alpha - \frac{p}{q}| \geq \frac{c'(\alpha)}{q^n}.$$

Falls hingegen $|\alpha - \frac{p}{q}| \geq 1$ gilt, so können wir $c(\alpha) = 1$ wählen und erhalten

$$\left|\alpha - \frac{p}{q}\right| \geq 1 \geq \frac{1}{q^n}.$$

Indem wir also

$$c(\alpha) = \min(1, c'(\alpha))$$

setzen erhalten wir die Aussage der Behauptung.

Wir leiten nun die Aussage des Satzes aus der Behauptung ab. Wir setzen $N := c(\alpha)^{-\frac{1}{\epsilon}}$. Für $\frac{p}{q}$ mit $q > N$ gilt in Anbetracht der obigen Behauptung

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n} = \frac{1}{q^n N^\epsilon} > \frac{1}{q^{n+\epsilon}}.$$

Somit kann es keine Lösung der Ungleichung (2.25) mit $q > N$ geben. Andererseits gilt für jede Lösung $\frac{p}{q}$ mit $1 \leq q \leq N$ bereits

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{n+\epsilon}} \leq 1.$$

Da es in jeder Umgebung um α aber nur endlich viele Brüche mit beschränktem Nenner geben kann, folgt die Aussage des Satzes. □

Wir halten noch die etwas präzisere Aussage fest, die wir im obigen Beweis gezeigt haben:

Korollar 2.4.7. *Zu jeder reellen algebraischen Zahl α vom Grad n gibt es eine positive Konstante*[43] *$c = c(\alpha)$, sodass für alle rationalen Zahlen $\frac{p}{q} \neq \alpha$ mit $ggT(p,q) = 1$ und $q \in \mathbb{N}$ die Ungleichung*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$$

gilt.

[42] Das Polynom P ist das ganzzahlige Minimalpolynom von α. Somit sind hängen auch die Koeffizienten $a_0, \ldots, a_n$ nur von α ab.

[43] Man beachte, dass die Konstante $c(\alpha)$ im Beweis des Satzes von Liouville zu gegebenem α effektiv berechenbar ist.

Liouville-Zahlen[44]

[44] Zu diesem Abschnitt gibt es ein Video:

Der Satz von Liouville besagt also, dass eine reelle Zahl, die sich „besonders gut“ durch rationale Zahlen approximieren lässt, nicht algebraisch sein kann. Diese Eigenschaft können wir nutzen um erstmals in dieser Vorlesung die Transzendenz konkreter reeller Zahlen zu zeigen:

Definition 2.4.8. Eine reelle Zahl α heißt *Liouville-Zahl*, falls die Ungleichung

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^m}$$

für jede natürliche Zahl $m \in \mathbb{N}$ unendlich viele Lösungen $\frac{p}{q} \in \mathbb{Q}$ besitzt.

Ein unmittelbares Korollar aus dem Satz von Liouville ist die Transzendenz aller Liouville-Zahlen:

Korollar 2.4.9. *Jede Liouville-Zahl ist transzendent.*

Beweis. Nach dem Satz von Liouville kann eine Zahl α für welche die Ungleichung

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{m+1}}$$

unendlich viele Lösungen besitzt nicht algebraisch vom Grad m sein. Da m in der Definition alle natürlichen Zahlen durchläuft, kann eine Liouville-Zahl nicht algebraisch sein. Somit ist sie transzendent. □

Der Satz von Liouville war ein Durchbruch in der Geschichte der transzendenten Zahlentheorie. Tatsächlich waren Liouville-Zahlen die ersten Zahlen, deren Transzendenz nachgewiesen werden konnte.

Beispiel 2.4.10. Die Zahl

$$\alpha = \sum_{i=1}^{\infty} 10^{-i!} = 0,110001000000000000000010\ldots$$

ist eine Liouville-Zahl und somit transzendent: Wir müssen zeigen, dass für jedes m die Ungleichung

$$|\alpha - \frac{p}{q}| < \frac{1}{q^m}$$

unendlich viele Lösungen $\frac{p}{q}$ besitzt. In der Tat erhalten wir für jedes $n \geq m$ eine derartige Lösung indem wir

$$q := 10^{n!} \text{ und } p = \sum_{i=1}^{n} 10^{n!-i!}$$

setzen, denn

$$|\alpha - \frac{p}{q}| = \left|\alpha - \sum_{i=1}^{n} 10^{-i!}\right| < \frac{2}{10^{(n+1)!}} < \frac{1}{q^n} \leq \frac{1}{q^m}.$$

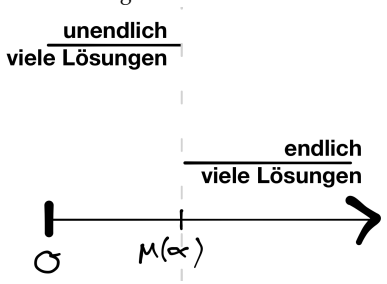
Ausblick und offene Fragen

In diesem Abschnitt haben wir uns mit der Frage beschäftigt für welche Parameter $\mu \in \mathbb{R}_{\geq 0}$ die Ungleichung

$$0 < |\alpha - \frac{p}{q}| \leq \frac{1}{q^\mu}$$

zu einer gegebenen Zahl α endlich viele oder unendlich viele Lösungen $\frac{p}{q} \in \mathbb{Q}$ besitzt. Besitzt diese Ungleichung für ein $\mu_0 \in \mathbb{R}$ höchstens endlich viele Lösungen, so ist klar dass die Ungleichung auch für alle $\mu \geq \mu_0$ höchstens endlich viele Lösungen besitzt. Andererseits besitzt die Ungleichung für $\mu = 0$ trivialerweise unendlich viele Lösungen. Es ist nun eine natürliche Frage, an welcher Stelle die Anzahl der Lösungen von unendlich auf endlich springt. Der Wert der Sprungstelle[45] $\mu(\alpha)$ wird auch *Irrationalitätsmaß* von α genannt. Falls diese Ungleichung für jedes $\mu \in \mathbb{R}$ unendlich viele Lösungen besitzt setzen wir $\mu(\alpha) = \infty$. Der Fall $\mu(\alpha) = \infty$ tritt genau dann ein, wenn α eine Liouville-Zahl ist. In den Übungen werden wir sehen, dass es überabzählbar viele Liouville-Zahlen gibt, dass diese dicht in den reellen Zahlen liegen und sich jede reelle Zahl als Summe zweier Liouville-Zahlen schreiben lässt.

[45] Abbildung zum Irrationalitätsmaß:



Der Satz von Liouville besagt, dass für eine algebraische Zahl α vom Grad n stets die Abschätzung $\mu(\alpha) \leq n$ gilt. Die Frage, ob man diese Schranke für algebraische Zahlen vom Grad n weiter verbessern kann hat eine lange Geschichte: Die erste Verbesserung des Liouvilleschen Satzes geht auf Thue zurück. Er bewies, dass $\mu(\alpha) \leq \frac{1}{2}n + 1$ gilt. Siegel konnte diese Schranke weiter auf $\mu(\alpha) \leq 2\sqrt{n} - 1$ verbessern. Der eigentliche Durchbruch gelang Roth im Jahre 1955. Er konnte unabhängig vom Grad $n \geq 2$ die Gleichung $\mu(\alpha) = 2$ zeigen. Genauer zeigte er:

Satz (Roth, 1955)**.** *Ist α eine algebraische reelle Zahl, so hat die Ungleichung*

$$0 < |\alpha - \frac{p}{q}| \leq \frac{1}{q^{2+\epsilon}},$$

für jedes $\epsilon > 0$ höchstens endlich viele Lösungen $\frac{p}{q} \in \mathbb{Q}$.

Dieses tiefliegende Resultat ist beachtlich und die Verbesserung zu Liouvilles Satz ist immens. Tatsächlich ist dieses Resultat so stark wie nur möglich, da wir ja bereits wissen, dass für $\epsilon = 0$ die obige Ungleichung für irrationale algebraische Zahlen unendlich viele Lösungen besitzt. Die Bedeutung dieses Satzes für die transzendente Zahlentheorie wird auch dadurch ersichtlich, dass Roth für den Beweis dieses Satzes im Jahre 1958 die Fields-Medaille, die höchste Auszeichnung der Mathematik, erhielt.

Doch selbst wenn der Satz von Roth die Frage nach der Approximierbarkeit reeller algebraischer Zahlen auf den ersten Blick abschließend beantwortet, gibt es interessante Verallgemeinerungen (z.B. der Schmidtsche Teilraumsatz) und Anschlussfragen. Wir können nun die Resultate dieses Abschnitts wie folgt zusammenfassen:

$$\mu(\alpha) = \begin{cases} 1 & \text{falls } \alpha \in \mathbb{Q}, \text{ (siehe Proposition 2.4.2)} \\ 2 & \text{falls } \alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}, \text{ (siehe Satz von Roth)} \\ \geq 2 & \text{falls } \alpha \text{ transzendent ist (siehe Proposition 2.4.1),} \\ \infty & \text{falls } \alpha \text{ eine Liouville-Zahl ist (siehe Definition 2.4.8).} \end{cases}$$

In der Übung werden wir sehen, dass das Irrationalitätsmaß für transzendente Zahlen jeden beliebigen Wert zwischen 2 und ∞ annehmen kann. Des Weiteren werden wir einen Zusammenhang zwischen dem Irrationalitätsmaß und der Kettenbruchentwicklung einer reellen Zahl herstellen. Diese Formel wird es uns erlauben, das Irrationalitätsmaß der Eulerschen Zahl e und der Cahen-Konstante C zu berechnen.

Dennoch ist es im Allgemeinen kein einfaches Problem das Irrationalitätsmaß einer transzendenten Zahl α explizit zu bestimmen. Man vermutet zum Beispiel, dass $\mu(\pi) = 2$, aber die stärkste Aussage in diese Richtung ist die Abschätzung $\mu(\pi) \leq 7.10320533$, die im Jahre 2019 von Zeilberger und Zudilin gezeigt wurde.

3 Transzendenz ausgewählter mathematischer Konstanten

Im zweiten Teil der Vorlesung möchten wir die Transzendenz einiger wichtiger mathematischer Konstanten zeigen. Wir behandeln die Sätze von Hermite (Transzendenz von e), Lindemann (Transzendenz von π) und den Satz von Lindemann-Weierstraß. Als Anwendung der Transzendenz von π diskutieren wir die Unmöglichkeit der Quadratur des Kreises.

3.1 Der Satz von Hermite

Ziel der heutigen Vorlesung ist es die Transzendenz von e zu beweisen. Der erste Beweis dieser Aussage gelang Hermite im Jahre 1873. Der Satz von Hermite war einer der Meilensteine der transzendenten Zahlentheorie. Nicht nur, da er die Transzendenz einer der wichtigsten Konstanten der Mathematik zeigt, sondern auch da der Beweis die Grundlage für viele weitere Transzendenzaussagen wie die Sätze von Lindemann oder Lindemann-Weierstrass bildet.

Polynome und Ableitungen[1]

[1] Zu diesem Abschnitt gibt es ein Video:

In den Transzendenzbeweisen für die Zahlen e und π werden Ableitungen von Polynomen eine entscheidende Rolle spielen. Für ein Polynom

$$Q = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$$

definieren wir die *formale Ableitung* $Q' \in \mathbb{C}[X]$ wie folgt:

$$Q' := \sum_{k=1}^{n} k \cdot a_k X^{k-1}.$$

Beispiel 3.1.1. Das Polynom $X^3 + 2X^2 + X - 4 \in \mathbb{C}[X]$ hat die formale Ableitung

$$3X^2 + 4X + 1.$$

Wir bemerken, dass für $Q \in \mathbb{C}[X]$ mit $\deg Q \geq 1$ stets $\deg Q' = \deg Q - 1$ gilt. Der Grad eines komplexen Polynoms verringert sich also beim formalen Ableiten um Eins.

Wir möchten nun den Begriff der formalen Ableitung mit der Ableitung der assoziierten Polynomfunktion[2]

$$\mathbb{C} \to \mathbb{C}, \quad z \mapsto Q(z) := \sum_{k=0}^{n} a_k z^k$$

in Verbindung bringen. Den Begriff der komplexen Differenzierbarkeit einer komplexen Funktion definiert man analog zur Differenzierbarkeit reeller Funktionen wie folgt: Eine komplexe Funktion $f\colon \mathbb{C} \to \mathbb{C}$ heißt *komplex differenzierbar in* $z_0 \in \mathbb{C}$, wenn der Grenzwert (mit $h \in \mathbb{C}$)

$$\lim_{h \to 0} \frac{f(z_0 + h) - f(z_0)}{h}$$

existiert. f heißt *komplex differenzierbar*, falls f an jeder Stelle komplex differenzierbar ist. Für eine komplex differenzierbare Funktion f nennen wir die Funktion $f'\colon \mathbb{C} \to \mathbb{C}$, definiert durch

$$f'(z) := \lim_{h \to 0} \frac{f(z + h) - f(z)}{h},$$

die Ableitung von f. Die Ableitungsregeln im Komplexen sind die selben, wie im Reellen. Es ist nun nicht schwer zu sehen, dass Polynomfunktionen komplex differenzierbar sind, und dass die Polynomfunktion zur formalen Ableitung eines Polynoms Q genau die Ableitung der Polynomfunktion zu Q ist, d.h.

$$\underbrace{(z \mapsto Q(z))'}_{\text{Komplexe Ableitung der Polynomfunktion}} = \underbrace{(z \mapsto Q'(z))}_{\text{Polynomfuktion zur formalen Ableitung } Q' \in \mathbb{C}[X]}.$$

Dies erklärt auch, wieso wir das Polynom Q' „formale Ableitung“ von Q nennen. Da wir nun wissen, dass die formale Ableitung mit der komplexen Ableitung übereinstimmt, werden wir im folgenden das Wort „formale“ weglassen. Wir bezeichnen mit $Q^{(j)}$ die j-te Ableitung von Q, d.h. $Q^{(0)} := Q$ und induktiv $Q^{(j+1)} := (Q^{(j)})'$.

Das folgende Lemma zur Teilbarkeit der Koeffizienten der Ableitungen eines ganzzahligen Polynoms wird in den folgenden Vorlesungen immer wieder eine Rolle spielen.

Lemma 3.1.2. *Für $Q \in \mathbb{Z}[X]$ und $j \in \mathbb{N}$ sind alle Koeffizienten des Polynoms $Q^{(j)}$ durch $j!$ teilbar. Insbesondere ist die Auswertung $Q^{(j)}(k)$ des Polynoms $Q^{(j)}$ an einer ganzen Zahl k durch $j!$ teilbar, d.h.*

$$Q^{(j)}(k) \in j!\mathbb{Z}.$$

[2] Für $z \in \mathbb{C}$ und $Q = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ nennt man $Q(z) := \sum_{k=0}^{n} a_k z^k$ auch die *Auswertung*, oder *Evaluation von Q bei $z \in \mathbb{C}$*.

Beweis. Falls j größer als der Grad m des Polynoms Q ist, so ist nichts zu zeigen, da wir in diesem Fall $Q^{(j)} = 0$ haben. Wir können also $j \leq m$ annehmen. Die j-te Ableitung des Polynoms

$$Q = \sum_{k=0}^{m} a_k X^k$$

ist gegeben durch

$$Q^{(j)} = \sum_{k=j}^{m} a_k \frac{k!}{(k-j)!} X^{k-j}.$$

Es bleibt zu zeigen, dass jede der Zahlen $a_k \frac{k!}{(k-j)!}$ durch $j!$ teilbar ist. Dies folgt allerdings aus

$$\frac{1}{j!} a_k \frac{k!}{(k-j)!} = a_k \binom{k}{j} \in \mathbb{Z}.$$

□

Komplexe Wegintegrale

Aus der Vorlesung Analysis I kennen Sie bereits den Riemannschen Integralbegriff einer stetigen Funktion $f\colon \mathbb{R} \to \mathbb{R}$. Wir werden im Folgenden einfache Beispiele komplexer Wegintegrale betrachten. Je nachdem in welchem Semester Sie sich befinden, kennen Sie die Eigenschaften derartiger Integrale bereits aus der Funktionentheorie. Für eine detailliertere Diskussion komplexer Wegintegrale verweisen wir auf das Kapitel „II Integralrechnung im Komplexen“ im Buch[3] „Funktionentheorie“ von Freitag und Busam[4]. Für unsere Zwecke reicht allerdings die folgende ad hoc Definition:

Definition 3.1.3. Für eine stetige Funktion $f\colon \mathbb{C} \to \mathbb{C}$ und $a, b \in \mathbb{C}$ definieren wir[5]

$$\int_a^b f(z)dz := (b-a) \int_0^1 \operatorname{Re}(f(a+(b-a)x))dx + i \cdot (b-a) \int_0^1 \operatorname{Im}(f(a+(b-a)x))dx.$$

Die grundlegenden Eigenschaften des Riemann-Integrals übertragen sich sofort auf das komplexe Wegintegral:

Lemma 3.1.4. *Für $a, b \in \mathbb{C}$ besitzt das komplexe Wegintegral die folgenden Eigenschaften:*

(a) Für stetige Funktionen $f, g\colon \mathbb{C} \to \mathbb{C}$ und $\lambda, \mu \in \mathbb{C}$ gilt

$$\int_a^b (\lambda \cdot f(z) + \mu \cdot g(z))\, dz = \lambda \int_a^b f(z)dz + \mu \int_a^b g(z)dz,$$

d.h. das komplexe Wegintegral ist $\mathbb{C}$-linear.

[3] Eberhard Freitag and Rolf Busam. *Funktionentheorie*. Springer-Verlag, Berlin, 1993. ISBN 3-540-50618-7

[4] Alles was Sie über komplexe Wegintegrale benötigen finden Sie in diesem Skript. Allerdings kann es als Ergänzung nicht schaden einen Blick in das zitierte Kapitel zu werfen. Die relevanten Seiten verlinken wir auf GRIPS.

[5] Ein paar Erläuterungen zu dieser Definition:

- Die Abbildung $\gamma\colon [0,1] \to \mathbb{C}$ mit $\gamma(x) = a + (b-a)x$ parametrisiert die geradlinige Verbindungsstrecke mit Anfangspunkt a und Endpunkt b. Diese Parametrisierung erklärt $a + (b-a)x$ im Argument von f und den Vorfaktor $(b-a)$.
- Die Zerlegung $f = \operatorname{Re} f + i \operatorname{Im} f$ erlaubt es uns die Integration einer komplexwertigen Funktionen f auf die Integrale der reellwertigen Funktionen $\operatorname{Re} f$ und $\operatorname{Im} f$ zurückzuführen.

(b) *Für eine stetige Funktion $f\colon \mathbb{C} \to \mathbb{C}$ und eine positive reelle Zahl C gilt*

$$\left| \int_a^b f(z)dz \right| \leq C|a-b|,$$

falls $|f(a+(b-a)x)| \leq C$ für alle $x \in [0,1]$ erfüllt ist.

(c) *Für komplex differenzierbare Funktionen $f, g\colon \mathbb{C} \to \mathbb{C}$ gilt die Formel der partiellen Integration*

$$\int_a^b f(z)g'(z)dz = [fg]_a^b - \int_a^b f'(z)g(z)dz.$$

Beweis. Die Eigenschaften folgen leicht aus den entsprechenden Eigenschaften des Riemann-Integrals. Wir zeigen exemplarisch die Eigenschaft (b):

$$\begin{aligned}
&\left| \int_a^b f(z)dz \right|^2 \\
&= \left| (b-a) \int_0^1 \operatorname{Re} f(a+(b-a)x)dx + i(b-a) \int_0^1 \operatorname{Im} f(a+(b-a)x)dx \right|^2 \\
&= |b-a|^2 \left[\left(\int_0^1 \operatorname{Re} f(a+(b-a)x)dx \right)^2 + \left(\int_0^1 \operatorname{Im} f(a+(b-a)x)dx \right)^2 \right] \\
&\leq |b-a|^2 \left[\int_0^1 (\operatorname{Re} f(a+(b-a)x))^2 dx + \int_0^1 (\operatorname{Im} f(a+(b-a)x))^2 dx \right] \\
&= |b-a|^2 \int_0^1 |f(a+(b-a)x)|^2 dx \leq |b-a|^2 C^2.
\end{aligned}$$

Hier haben wir im vorletzten Schritt die Cauchy-Schwarz Ungleichung verwendet. Wir erhalten nun (b) indem wir auf beiden Seiten die Wurzel ziehen. □

Wir definieren nun für beliebige Polynome $Q \in \mathbb{C}[X]$ und komplexe Zahlen $\alpha \in \mathbb{C}$ das Integral

$$I(\alpha, Q) := \int_0^\alpha e^{\alpha - z} Q(z)dz.$$

Lemma 3.1.5. *Für ein Polynom $Q \in \mathbb{C}[X]$ vom Grad m gilt die Gleichung*

$$I(\alpha, Q) = e^\alpha \sum_{j=0}^m Q^{(j)}(0) - \sum_{j=0}^m Q^{(j)}(\alpha).$$

Beweis. Partielle Integration liefert die Formel

$$\int_0^\alpha e^{\alpha - z} Q(z)dz = [-e^{\alpha - z} Q(z)]_0^\alpha + \int_0^\alpha e^{\alpha - z} Q^{(1)}(z)dz,$$

also

$$I(\alpha, Q) = e^\alpha Q(0) - Q(\alpha) + I(\alpha, Q^{(1)}). \tag{3.1}$$

Wiederholtes Anwenden der Formel (3.1) zeigt die gewünschte Gleichung. □

Der Satz von Hermite[6]

[6] Zu diesem Abschnitt gibt es ein Video:

Satz 3.1.6 (Hermite, 1873)**.** *Die Zahl e ist transzendent.*

Beweis. Wir bewiesen die Aussage durch Widerspruch. Angenommen e wäre algebraisch, dann gäbe es zu e das ganzzahlige Minimalpolynom

$$\mathrm{MinPol}_{\mathbb{Z}}(e) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X].$$

Somit hätten wir die Gleichung

$$\sum_{k=0}^{n} a_k e^k = 0. \tag{3.2}$$

Wir definieren nun das Hilfspolynom

$$Q := X^{p-1}(X-1)^p \dots (X-n)^p,$$

wobei p eine hinreichend große Primzahl bezeichnet. Im Folgenden möchten wir den Absolutbetrag der Zahl

$$J := \sum_{k=0}^{n} a_k I(k, Q)$$

von oben und unten abschätzen. Wir werden zum Schluss sehen, dass sich die beiden Abschätzungen widersprechen, sobald wir p hinreichend groß wählen. Wir beginnen mit der unteren Abschätzung. Diese ist von algebraischer Natur und verwendet die Annahme, dass e algebraisch ist:

Behauptung 1.: Für eine hinreichend große Primzahl p haben wir die Abschätzung

$$(p-1)! \leq |J|.$$

Beweis der Behauptung 1: Wir möchten zeigen, dass J eine von Null verschiedene, durch $(p-1)!$ teilbare, ganze Zahl ist. Im ersten Schritt zeigen wir, dass J eine ganze durch $(p-1)!$ teilbare Zahl ist. Der Grad des Hilfspolynoms Q ist gegeben durch

$$m := (n+1)p - 1.$$

Wir können mit Lemma 3.1.5 die Zahl J wie folgt ausdrücken:

$$\begin{aligned} J = \sum_{k=0}^{n} a_k I(k, Q) &= \sum_{k=0}^{n} a_k \sum_{j=0}^{m} (e^k Q^{(j)}(0) - Q^{(j)}(k)) \\ &= \sum_{j=0}^{m} Q^{(j)}(0) \sum_{k=0}^{n} a_k e^k - \sum_{j=0}^{m} \sum_{k=0}^{n} a_k Q^{(j)}(k). \end{aligned}$$

Nun bemerken wir, dass nach (3.2) die erste Doppelsumme verschwindet. Wir erhalten also

$$J = -\sum_{j=0}^{m} \sum_{k=0}^{n} a_k Q^{(j)}(k).$$

Da die Polynomfunktion $x \mapsto Q(x)$ bei $x = 1, \dots, n$ Nullstellen der Ordnung p und bei $x = 0$ eine Nullstelle der Ordnung $p-1$ hat, beginnt die obige Summe erst bei $j = p-1$ und für $j = p-1$ kommt der einzige Beitrag vom Index $k = 0$. Dies zeigt die Gleichung

$$J = -a_0 Q^{(p-1)}(0) - \sum_{j=p}^{m} \sum_{k=0}^{n} a_k Q^{(j)}(k).$$

Nach Lemma 3.1.2 gilt also

$$J \in (p-1)!\mathbb{Z}.$$

Wir möchten nun $J \neq 0$ zeigen. Dafür reicht es zu zeigen, dass $J \not\equiv 0 \mod p$ gilt. Nach Lemma 3.1.2 ist $Q^{(j)}(k)$ für $j \geq p$ durch $p!$ teilbar, insbesondere also durch p. Es gilt also

$$J \equiv -a_0 Q^{(p-1)}(0) \mod p.$$

Wir berechnen nun den Term $Q^{(p-1)}(0)$ explizit. Indem wir

$$Q = X^{p-1}(X-1)^p \dots (X-n)^p$$

ausmultiplizieren, sehen wir, dass

$$Q = (-1)^p (-2)^p \dots (-n)^p \cdot X^{p-1} + \textit{ Terme höheren Grades}.$$

Wir erhalten

$$Q^{(p-1)} = (-1)^p (-2)^p \dots (-n)^p \cdot (p-1)! + \textit{ Terme höheren Grades}$$

und somit

$$Q^{(p-1)}(0) = (-1)^{np} n!^p \cdot (p-1)!.$$

Wenn wir $p > \max(|a_0|, n)$ wählen, so kann p weder a_0 noch $n!$ teilen. Außerdem teilt p niemals die Zahl $(p-1)!$. Somit gilt die Kongruenz (oder besser Inkongruenz)

$$J \equiv -a_0 Q^{(p-1)}(0) \equiv -a_0 (-1)^{np} n!^p \cdot (p-1)! \not\equiv 0 \mod p,$$

und es folgt $J \neq 0$. Da J eine von Null verschiedene durch $(p-1)!$ teilbare Zahl ist[7], folgt

[7] Tatarataaaa

$$|J| \geq (p-1)!$$

und wir haben die Behauptung 1 gezeigt.

Behauptung 2: Es gilt

$$|J| \leq A \cdot C^p,$$

wobei A und C zwei nicht von p abhängige positive reelle Zahlen sind.

Beweis von Behauptung 2: Wir zeigen zunächst, dass die Polynomfunktion $x \mapsto |Q(x)|$ für $k \leq n$ auf dem Intervall $[0, k]$ durch $(2n)!^p$ beschränkt ist: Für $x \in [0, 1]$ gilt

$$|Q(x)| \leq \underbrace{|x|^{p-1}}_{\leq 1} \left(\underbrace{|x-1|}_{\leq 1} \dots \underbrace{|x-n|}_{\leq n} \right)^p \leq n!^p \leq (2n)!^p.$$

Für $x \in [1,k]$ gilt hingegen

$$|Q(x)| \leq |x|^{p-1}|x-1|^p \dots |x-n|^p \leq |x|^p|x+1|^p \dots |x+n|^p \leq (2n)!^p.$$

Dies zeigt, dass die Funktion $x \mapsto |Q(x)|$ auf dem Intervall $[0,k]$ durch $(2n)!^p$ beschränkt ist. Die Funktion $x \mapsto Q(x)e^{k-x}$ ist somit auf dem Intervall $[0,k]$ durch $e^k(2n)!^p$ beschränkt. Es folgt

$$|I(k,Q)| \leq \int_0^k |Q(x)|e^{k-x}dx \leq ke^k(2n)!^p \leq ne^n(2n)!^p$$

Wir erhalten

$$|J| \leq \sum_{k=0}^{n} |a_k||I(k,Q)| \leq \sum_{k=1}^{n} |a_k|ne^n(2n)!^p.$$

Indem wir $A := \sum_{k=1}^{n} |a_k|ne^n$ und $C := (2n)!$ setzten, erhalten wir die zweite Behauptung.

Kombinieren wir Behauptung 1 und Behauptung 2, so ergibt sich die Ungleichungskette

$$(p-1)! \leq |J| \leq A \cdot C^p.$$

Da die Fakultät schneller wächst als die Exponentialfunktion, ergibt sich für hinreichend großes p ein Widerspruch. Die Annahme, dass e algebraisch ist, war somit falsch und wir haben die Transzendenz von e gezeigt. □

Ausblick und offene Fragen

Auf weitreichende unbewiesene Vermutungen zu Werten der Exponentialfunktion gehen wir am Ende des zweiten Teils der Vorlesung ein. An dieser Stelle möchten wir nur noch einmal bemerken, dass bisher weder die Irrationalität noch die Transzendenz der Zahlen

$$e + \pi, e \cdot \pi$$

bewiesen wurde. Wir möchten in diesem Ausblick allerdings auf eine erstaunliche Konsequenz des Satzes von Hermite hinweisen. Wir werden zeigen, dass mindestens eine der Zahlen $e + \pi$ und $e \cdot \pi$ transzendent ist. Dafür benötigen wir allerdings folgende Aussage aus der Vorlesung Algebra:

Proposition 3.1.7. *Falls $\alpha \in \mathbb{C}$ Nullstelle eines von Null verschiedenen Polynoms $P \in \overline{\mathbb{Q}}[X]$ ist, so ist α bereits algebraisch.*

Unter Verwendung dieses Resultats ergibt sich die Transzendenz einer der beiden Zahlen $e + \pi$ und $e \cdot \pi$ als unmittelbare Konsequenz des Satzes von Hermite:

Korollar 3.1.8. *Mindestens eine*[8] *der Zahlen $e+\pi$ und $e\cdot\pi$ ist transzendent.*

[8] Natürlich wird vermutet, dass beide Zahlen transzendent sind.

Beweis. Angenommen beide Zahlen $e+\pi$ und $e\cdot\pi$ wären algebraisch. Dann wären auch $b := -(e+\pi)$ und $c := e\cdot\pi$ algebraisch. Wir betrachten nun das Polynom

$$P := (X-e)\cdot(X-\pi).$$

Durch Ausmultiplizieren erhalten wir

$$P = X^2 - (e+\pi)X + e\cdot\pi = X^2 + bX + c.$$

Unsere Annahme würde nun implizieren, dass das Polynom P algebraische Koeffizienten hätte. Allerdings gilt

$$P(e) = (e-e)(e-\pi) = 0.$$

Nach Proposition 3.1.7 wäre e also algebraisch. Wir würden also einen Widerspruch zum Satz von Hermite erhalten. Somit war unsere Annahme, dass beide Zahlen $e+\pi$ und $e\cdot\pi$ algebraisch sind falsch; mindestens eine der Zahlen ist somit transzendent. □

Im Ausblick zu Kapitel 2.4 hatten wir das Irrationalitätsmaß einer reellen Zahl definiert und die noch offenen Vermutung erwähnt, dass $\mu(\pi) = 2$ gilt. In den Übungsaufgaben werden wir sehen, dass für $\alpha,\beta \in \mathbb{R}\setminus\mathbb{Q}$ mit $\mu(\alpha) < \mu(\beta)$ die Zahlen $\alpha\cdot\beta$ und $\alpha+\beta$ irrational sind. Als Anwendung erhalten wir ein weiteres erstaunliches Resultat:

Proposition 3.1.9. *Mindestens eine*[9] *der beiden folgenden Aussagen ist richtig:*

[9] Natürlich wird vermutet, dass beide Aussagen wahr sind.

(a) $\mu(\pi) = 2$,

(b) $e\cdot\pi$ *und* $e+\pi$ *sind irrational.*

Beweis. Wir wissen bereits $\mu(\pi) \geq 2$, da π irrational ist.[10] Falls (a) nicht gilt, so hätten wir $\mu(e) = 2 < \mu(\pi)$. Aus Übungsaufgabe 1 auf Blatt 6 folgt dann die Irrationalität von $e\cdot\pi$ und $e+\pi$. □

[10] Wir verwenden hier auch die Irrationalität von π, diese wird auch auf Blatt 6 gezeigt. In der nächsten Vorlesung zeigen wir dann sogar die Transzendenz von π.

Im Hinblick der obigen Resultate ist es erstaunlich, dass weder die Transzendenz von $e+\pi$ oder $e\cdot\pi$ noch $\mu(\pi) = 2$ bisher bewiesen werden konnte.

3.1.1 *Noch nicht ganz π*

3.1.2 *Immer noch nicht π*

3.1.3 *Fast π*

3.1.4 *Yeah π!!!!!*

Na gut, noch nicht ganz. Aber nächste Woche. Versprochen![11]

[11] 3.1.4... Man bemerke den Geniestreich der Nummerierungskunst ;-)

3.2 *Der Satz von Lindemann*

Im folgenden Abschnitt zeigen wir die Transzendenz von π. Der erste Beweis dieser Aussage gelang Lindemann im Jahre 1882 aufbauend auf Hermites Beweis. Allerdings werden wir für den Beweis der Transzendenz von π ein paar Aussagen aus der Algebra (ohne Beweis) hinnehmen müssen.

Ganze algebraische Zahlen[12]

Die ganzen Zahlen haben uns bisher schon viele gute Dienste erwiesen[13]. Die triviale Tatsache, dass jede von Null verschiedene ganze Zahl mindestens Absolutbetrag Eins hat, haben wir bereits in zahlreichen Beweisen verwendet. Im Folgenden möchten wir den Begriff der „Ganzheit“ auf beliebige algebraische Zahlen verallgemeinern. Wir erinnern (mal wieder), dass eine komplexe Zahl α algebraisch ist, wenn sie Nullstelle eines von Null verschiedenen Polynoms mit rationalen Koeffizienten ist.

[12] Zu diesem Abschnitt gibt es ein Video:

[13] an dieser Stelle ein großes Dankeschön an alle ganzen Zahlen ;-)

Definition 3.2.1. Eine algebraische Zahl α heißt *ganz*, wenn sie Nullstelle eines normierten Polynoms mit ganzzahligen Koeffizienten

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$$

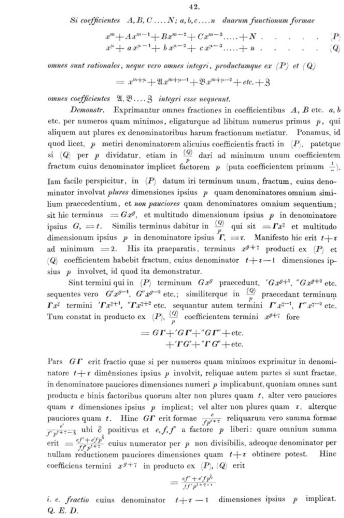
ist.

Wir werden gleich sehen, dass man die ganzen Zahlen bequem an ihrem Minimalpolynom erkennen kann. Dazu benötigen wir folgendes Hilfsresultat aus der Algebra:

Lemma (Lemma von Gauß)**.** *Seien $P, Q \in \mathbb{Q}[X]$ normierte Polynome. Falls das Polynom $P \cdot Q$ ganzzahlige Koeffizienten hat, so haben bereits die Polynome P und Q ganzzahlige Koeffizienten.*

Beweis. Beweis siehe Rand [14]. □

[14] Hier der Originalbeweis:



Jetzt wo die Evaluation vorbei ist, kann ich mir ja unleserliche Beweise in lateinischer Sprache am Rand der Seite erlauben. Und wenn ich schon mal am Austeilen bin: Ja, Herr Fermat, jeder Rand ist groß genug für einen Beweis ;-).
Spaß beiseite, interessierte Leser*Innen finden einen Beweis im Buch „Tutorium Algebra“, Satz 3.11.

F. Modler and M. Kreh. *Tutorium Algebra*. Springer Spektrum, 2018. ISBN 9783662586891

Wir können nun das folgende nützliche Kriterium für Ganzheit beweisen:

Korollar 3.2.2. *Eine algebraische Zahl ist genau dann ganz, wenn ihr Minimalpolynom über $\mathbb{Q}$ ganzzahlige Koeffizienten hat.*

Beweis. Falls das ganzzahlige Minimalpolynom einer algebraischen Zahl α normiert ist, so ist α als Nullstelle eines normierten ganzzahligen Polynoms ganz.

Für die Umkehrung sei α eine ganze algebraische Zahl. Somit ist α die Nullstelle eines normierten ganzzahligen Polynoms

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X].$$

Sei $P := \mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Q}[X]$ das Minimalpolynom über $\mathbb{Q}$. Polynomdivision[15] mit Rest in $\mathbb{Q}[X]$ zeigt, dass das Minimalpolynom P das Polynom $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ in $\mathbb{Q}[X]$ teilt, d.h.

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = P \cdot Q \quad \text{für ein geeignetes } Q \in \mathbb{Q}[X].$$

Nun zeigt das Lemma von Gauß, dass $P = \mathrm{MinPol}_{\mathbb{Q}}(\alpha)$ ganzzahlige Koeffizienten hat.

□

[15] Andernfalls gäbe es ein Polynom $R \neq 0$ mit $\deg R < \deg P$ und

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0 = P \cdot Q + R.$$

Auswerten bei α ergäbe $R(\alpha) = 0$ im Widerspruch zur Minimalität von $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$.

Natürlich wäre unser neuer Ganzheitsbegriff Unsinn, wenn er für rationale Zahlen nicht mit unserem bisherigen Ganzheitsbegriff übereinstimmen würde. Doch wie das folgende Beispiel zeigt, haben wir Glück.

Beispiel 3.2.3. Für eine rationale Zahl $\alpha \in \mathbb{Q}$ ist $X - \alpha$ das Minimalpolynom über $\mathbb{Q}$. Somit ist α genau dann ganz im Sinne der Definition 3.2.1, wenn $\alpha \in \mathbb{Z}$.

Bevor wir fortfahren geben wir noch je ein Beispiel für eine ganze und eine nicht ganze algebraische Zahl zweiten Grades.

Beispiel 3.2.4. Wir haben bereits gesehen, dass das ganzzahlige Minimalpolynom von $\frac{i}{2}$ das Polynom $4X^2 + 1$ ist. Da dieses Polynom nicht normiert ist, also nicht den führenden Koeffizienten 1 hat, ist $\frac{i}{2}$ keine ganze algebraische Zahl. Die Zahl i hat hingegen das ganzzahlige Minimalpolynom $X^2 + 1$ und ist somit ganz.

Wir wissen bereits, dass eine rationale Zahl ganz wird, wenn wir diese mit ihrem Nenner multiplizieren. Das folgende Lemma können wir als eine Verallgemeinerung dieses Sachverhalts auf algebraische Zahlen ansehen.

Lemma 3.2.5. *Falls $\alpha \in \mathbb{C}$ Nullstelle eines ganzzahligen Polynoms*

$$P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X] \tag{3.3}$$

ist, so ist $a_n\alpha$ ganz. Insbesondere lässt sich jede algebraische Zahl als Bruch einer ganzen algebraischen Zahl und einer natürlichen Zahl schreiben.

Beweis. Indem wir (3.3) mit a_n^{n-1} multiplizieren erhalten wir

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_n \cdot a_{n-2}(a_n\alpha)^{n-2} + \cdots + a_n^{n-2}a_1(a_n\alpha) + a_n^{n-1}a_0.$$

Folglich ist $a_n\alpha$ als Nullstelle des normierten ganzzahligen Polynoms

$$X^n + a_{n-1}X^{n-1} + a_n a_{n-2}X^{n-2} + \cdots + a_n^{n-2}a_1 X + a_n^{n-1}a_0 \in \mathbb{Z}[X]$$

ganz. □

Zu guter Letzt benötigen wir noch die Tatsache, dass Summen und Produkte (ganzer) algebraischer Zahlen wieder (ganze) algebraische Zahlen sind:

Lemma 3.2.6. *Für $\alpha, \beta \in \mathbb{C}$ gelten:*

(a) Sind α, β algebraische Zahlen, so sind auch $\alpha \cdot \beta$ und $\alpha + \beta$ algebraische Zahlen. Falls α nicht Null ist, so ist auch $\frac{1}{\alpha}$ algebraisch.[16]

(b) Sind α, β ganze algebraische Zahlen, so sind auch $\alpha \cdot \beta$ und $\alpha + \beta$ ganze algebraische Zahlen.[17]

Beweis. Wir verwenden dieses Resultat ohne Beweis. Die Teilaussage (a) wird in der Vorlesung Algebra gezeigt. Interessierte Leser*innen seien für einen Beweis der Aussage (b) auf Satz 16.8 des Buches *Elementare und Algebraische Zahlentheorie*[18] verwiesen. □

[16] Dies zeigt, dass die Teilmenge $\overline{\mathbb{Q}}$ von $\mathbb{C}$ mit den Verknüpfungen $+$ und $\cdot$ ein *Unterkörper* ist.

[17] Dies zeigt, dass die ganzen algebraischen Zahlen einen Unterring von $\mathbb{C}$ bilden. Diese Tatsache spielt in der algebraischen Zahlentheorie eine wichtige Rolle.

[18] Stefan Müller-Stach and Jens Piontkowski. *Elementare und algebraische Zahlentheorie*. Vieweg + Teubner, Wiesbaden, 2011. ISBN 978-3-8348-1256-8

Ein Hauch von Galoistheorie

Zunächst erinnern wir an den folgenden Satz:

Satz 3.2.7 (Hauptsatz der Algebra)**.** *Jedes Polynom $Q \in \mathbb{C}[X]$ vom Grad $n \geq 1$ zerfällt über $\mathbb{C}$ vollständig in Polynome ersten Grades, d.h.*

$$Q = c(X - \alpha_1) \dots (X - \alpha_n)$$

mit $c, \alpha_1, \dots, \alpha_n \in \mathbb{C}$.

Insbesondere besitzt jedes komplexe Polynom vom Grad $n \geq 1$ genau n Nullstellen, wenn man diese mit Vielfachheit zählt. Nun wissen wir, dass es zu jeder algebraischen Zahl α ein eindeutiges normiertes Polynom in $\mathbb{Q}[X]$ minimalen Grades gibt, das α als Nullstelle hat, nämlich das Minimalpolynom von α. Doch auch die weiteren Nullstellen des Minimalpolynoms spielen in der Algebra eine wichtige Rolle.

Definition 3.2.8. Sei $\alpha \in \mathbb{C}$ eine algebraische Zahl vom Grad n. Die Nullstellen $\alpha_1, \dots, \alpha_n$ des Minimalpolynoms $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$ heißen die *Konjugierten* von α (über $\mathbb{Q}$).

Wir erläutern dies anhand eines Beispiels.

Beispiel 3.2.9. Wir haben bereits gesehen, dass $P = X^2 + \frac{1}{4}$ das Minimalpolynom zu $\frac{i}{2}$ ist. Das Polynom P zerfällt über $\mathbb{C}$ wie folgt

$$X^2 + \frac{1}{4} = \left(X - \frac{i}{2}\right)\left(X + \frac{i}{2}\right).$$

Somit sind $\alpha_1 = \frac{i}{2}$ und $\alpha_2 = -\frac{i}{2}$ die Konjugierten zu $\frac{i}{2}$.

Wir betrachten nun den Polynomring $\mathbb{Q}[X_1, \dots, X_n]$ in n Variablen über $\mathbb{Q}$. Die Elemente dieses Rings sind formale Summen der Form

$$\sum_{(i_1,\dots,i_n)\in\mathbb{N}_0^n} a_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n} \quad \text{mit } a_{i_1,\dots,i_n} \in \mathbb{Q},$$

wobei höchstens endlich viele Koeffizienten $a_{i_1,\dots,i_n}$ von Null verschieden sind.

Definition 3.2.10. Ein Polynom $Q \in \mathbb{Q}[X_1, \dots, X_n]$ heißt *symmetrisches Polynom* in n Variablen, wenn für jede Permutation $\sigma \in S_n$ aus der symmetrischen Gruppe S_n die Gleichung

$$Q(X_1, \dots, X_n) = Q(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

gilt.

Die symmetrischen Polynome sind also genau diejenigen Polynome, die sich nicht ändern wenn wir die Variablen beliebig miteinander vertauschen.

Beispiel 3.2.11. Das Polynom $P = X_1^2 + X_2^2 \in \mathbb{Q}[X_1, X_2]$ ist ein symmetrisches Polynom in 2 Variablen. Allerdings ist das Polynom $Q = X_1^2 + X_2 \in \mathbb{Q}[X_1, X_2]$ kein symmetrisches Polynom in 2 Variablen, da für die Permutation

$$\sigma = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$$

das Polynom

$$Q(X_{\sigma(1)}, X_{\sigma(2)}) = X_2^2 + X_1,$$

nicht mit Q übereinstimmt.

Analog zu Polynomen in einer Variable können wir auch ein Polynom $Q \in \mathbb{Q}[X_1, \dots, X_n]$ in mehreren Variablen an komplexen Zahlen $\alpha_1, \dots, \alpha_n$ auswerten. Die Auswertung des Polynoms

$$Q = \sum_{(i_1,\dots,i_n)\in\mathbb{N}_0^n} a_{i_1,\dots,i_n} X_1^{i_1} \dots X_n^{i_n}, \quad \text{mit } a_{i_1,\dots,i_n} \in \mathbb{Q},$$

bei $\alpha_1, \dots, \alpha_n$ ist definiert als

$$Q(\alpha_1, \dots, \alpha_n) := \sum_{(i_1,\dots,i_n)\in\mathbb{N}_0^n} a_{i_1,\dots,i_n} \alpha_1^{i_1} \dots \alpha_n^{i_n}.$$

Der folgende Satz kann mit Methoden der Galoistheorie[19] bewiesen werden:

Satz 3.2.12. *Ist $P \in \mathbb{Q}[X]$ ein Polynom vom Grad n mit Nullstellen $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ und $Q \in \mathbb{Q}[X_1, \dots, X_n]$ ein symmetrisches Polynom in n Variablen, dann gilt*

$$Q(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}.$$

[19] Für Details zur Galoistheorie möchte ich auf die Vorlesung Algebra verweisen. Falls Sie diese Vorlesung noch nicht gehört haben, finden Sie am Ende dieser Vorlesung einen kleinen Vorgeschmack auf das, was Sie dort erwarten wird. Insbesondere werden wir dort Satz 3.2.12 aus Standardsätzen der Galoistheorie ableiten.

Falls die Zahlen α_i für $1 \leq i \leq n$ zusätzlich ganze algebraische Zahlen sind und Q ganze Zahlen als Koeffizienten hat, so gilt sogar

$$Q(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}.$$

Beweis. Dieser Satz kann mit Methoden der Galoistheorie bewiesen werden. Dies werden wir im Ausblick im Anschluss an Satz 3.2.16 näher erklären. □

Transzendenz von π - Der Satz von Lindemann[20]

Satz 3.2.13 (Lindemann, 1882)**.** *Die Zahl π ist transzendent.*

Beweis. Wir beweisen die Aussage durch Widerspruch. Angenommen π wäre algebraisch. Dann wäre nach Lemma 3.2.6 auch die Zahl $i\pi$ algebraisch[21]. Wir bezeichnen dann mit n den Grad der ganzen algebraischen Zahl $\alpha := i\pi$ und mit $\alpha = \alpha_1, \ldots, \alpha_n$ die Konjugierten zu α. Sei N der führende Koeffizient des ganzzahligen Minimalpolynoms von $\alpha = i\pi$. Die Zahlen $N\alpha_1, \ldots, N\alpha_n$ sind, nach Lemma 3.2.5, ganze algebraische Zahlen. Die Eulersche Formel

$$e^{\alpha} = e^{i\pi} = -1$$

impliziert

$$(1 + e^{\alpha_1}) \cdot (1 + e^{\alpha_2}) \cdots (1 + e^{\alpha_n}) = 0.$$

Multiplizieren wir dieses Produkt aus, so erhalten wir

$$(1 + e^{\alpha_1}) \cdot (1 + e^{\alpha_2}) \cdots (1 + e^{\alpha_n}) = \sum_{(\epsilon_1, \ldots, \epsilon_n) \in \{0,1\}^n} e^{\epsilon_1\alpha_1 + \cdots + \epsilon_n\alpha_n}. \quad (3.4)$$

Wir definieren nun das Polynom

$$P := \prod_{(\epsilon_1, \ldots, \epsilon_n) \in \{0,1\}^n} (X - (\epsilon_1 N\alpha_1 + \cdots + \epsilon_n N\alpha_n))$$

und zeigen zunächst die folgende

Vorüberlegung:[22] *Die Koeffizienten des Polynoms P liegen in $\mathbb{Z}$.*
Beweis der Vorüberlegung: Wir betrachten das Hilfpolynom

$$\widetilde{P} := \prod_{(\epsilon_1, \ldots, \epsilon_n) \in \{0,1\}^n} (X - (\epsilon_1 X_1 + \cdots + \epsilon_n X_n)) \in \mathbb{Q}[X, X_1, \ldots, X_n],$$

und bemerken, dass dieses Polynom P ergibt, wenn wir $N\alpha_1, \ldots, N\alpha_n$ für die Variablen $X_1, \ldots, X_n$ einsetzen, d.h.

$$P = \widetilde{P}(X, N\alpha_1, \ldots, N\alpha_n).$$

Indem wir das Polynom $\tilde{P}$ ausmultiplizieren und die Terme nach Potenzen von X sortieren, erhalten wir

$$\widetilde{P} = \sum_{i=0}^{2^n} A_i X^i \quad \text{für gewisse } A_i \in \mathbb{Z}[X_1, \ldots, X_n].$$

[20] Zu diesem Abschnitt gibt es ein Video:

[21] In diesem konkreten Fall kann man das aber auch ganz direkt sehen: Falls

$$\mathrm{MinPol}_{\mathbb{Q}}(\pi) = X^n + a_{n-1}X^{n-1} + \cdots + a_0,$$

so setzen wir

$$b_i := a_i^2 - 2a_{i-1}a_{i+1} \quad \text{für } 0 \leq i \leq n-1,$$

wobei wir $a_n = 1$ und $a_{-1} = 0$ setzen. Dann ist $i\pi$ eine Nullstelle des Polynoms

$$X^{2n} + b_{n-1}X^{2(n-1)} + \cdots + b_1X^2 + b_0.$$

[22] Wir verwenden hier bewusst die Bezeichnung „Vorüberlegung“statt „Behauptung“, um die Analogie zum Hermiteschen Satz zu unterstreichen. Im Hermiteschen Satz ist die Ganzzahligkeit des betrachteten Hilfspolynoms Q klar. In diesem Beweis benötigen wir hingegen eine kleine „Vorüberlegung“ um die Ganzzahligkiet der Koeffizienten einzusehen.

Insbesondere sehen wir, dass

$$P = \widetilde{P}(X, N\alpha_1, \dots, N\alpha_n) = \sum_{i=0}^{2^n} A_i(N\alpha_1, \dots, N\alpha_n) X^i.$$

Um zu zeigen, dass die Koeffizienten des Polynoms P ganze Zahlen sind, reicht es nach Satz 3.2.12 also zu zeigen, dass für jede Permutation σ in der symmetrischen Gruppe S_n und jedes $0 \leq i \leq 2^n$ die Gleichung

$$A_i(N\alpha_1, \dots, N\alpha_n) = A_i(N\alpha_{\sigma(1)}, \dots, N\alpha_{\sigma(n)})$$

gilt. Allerdings haben wir für jedes $\sigma \in S_n$ die Gleichungskette

$$\begin{aligned}
&\sum_{i=0}^{2^n} A_i(N\alpha_1, \dots, N\alpha_n) X^i \\
&\qquad = \prod_{(\epsilon_1,\dots,\epsilon_n)\in\{0,1\}^n} (X - N(\epsilon_1\alpha_1 + \cdots + \epsilon_n\alpha_n)) \\
&\qquad = \prod_{(\epsilon_1,\dots,\epsilon_n)\in\{0,1\}^n} (X - N(\epsilon_1\alpha_{\sigma(1)} + \cdots + \epsilon_n\alpha_{\sigma(n)})) \\
&\qquad\qquad = \sum_{i=0}^{2^n} A_i(N\alpha_{\sigma(1)}, \dots, N\alpha_{\sigma(n)}) X^i.
\end{aligned}$$

Ein Koeffizientenvergleich beider Seiten zeigt nun

$$A_i(N\alpha_1, \dots, N\alpha_n) = A_i(N\alpha_{\sigma(1)}, \dots, N\alpha_{\sigma(n)})$$

und somit $P \in \mathbb{Z}[X]$. Dies beweist die Vorüberlegung.

Wir schreiben $\beta_1, \dots, \beta_m$ für die von Null verschiedenen Nullstellen von P, d.h.

$$P = X^{2^n - m} \cdot \prod_{i=1}^{m} (X - \beta_i).$$

Da P ganzzahlige Koeffizienten hat gilt auch

$$\prod_{i=1}^{m} (X - \beta_i) \in \mathbb{Z}[X]. \tag{3.5}$$

Für eine hinreichend große Primzahl p betrachten wir nun das Polynom[23]

$$Q := X^{p-1} \prod_{i=1}^{m} (X - \beta_i)^p.$$

Nach (3.5) hat auch dieses Polynom ganzzahlige Koeffizienten. Wir definieren nun

$$J := I\left(\frac{\beta_1}{N}, Q(NX)\right) + \cdots + I\left(\frac{\beta_m}{N}, Q(NX)\right).$$

[23] Wie die Notation Q bereits andeutet, spielt dieses Polynom nun die Rolle des Hilfspolynoms Q im Hermiteschen Beweis. Man beachte die Ähnlichkeit zum Polynom im Hermiteschen Beweis. Auch dieses Polynom hat eine $(p-1)$-fache Nullstelle in Null, während alle anderen Nullstellen mindestens Ordnung p haben.

Von hier an geht der Beweis komplett analog zum Hermiteschen Beweis. Wir teilen den Beweis wieder in zwei Behauptungen. Im ersten Schritt leiten wir aus unserer Annahme, dass π algebraisch ist, eine untere Schranke für J ab. Im zweiten Schritt verwenden wir analytische Methoden um die Linearkombination der Integrale von oben zu beschränken. Wenn wir p groß genug wählen widersprechen sich die beiden Abschätzungen.

Behauptung 1: Für jede hinreichend große Primzahl p gilt

$$(p-1)! \leq |J|.$$

Beweis der Behauptung 1: Indem wir alle Terme in (3.4) mit Exponenten Null zusammenfassen erhalten wir

$$(2^n - m) + e^{\beta_1/N} + \cdots + e^{\beta_m/N} = 0. \tag{3.6}$$

Nun liefert Lemma 3.1.5, in Anbetracht von $\deg Q = (m+1)p-1$ und $(Q(NX))^{(j)} = N^j Q^{(j)}(NX)$, die Gleichung

$$\begin{aligned} J &= \sum_{j=0}^{(m+1)p-1} N^j Q^{(j)}(0) \sum_{k=1}^{m} e^{\beta_k/N} - \sum_{j=0}^{(m+1)p-1} \sum_{k=1}^{m} N^j Q^{(j)}(\beta_k) \\ &\overset{(3.6)}{=} -(2^n - m) \sum_{j=0}^{(m+1)p-1} N^j Q^{(j)}(0) - \sum_{j=0}^{(m+1)p-1} \sum_{k=1}^{m} N^j Q^{(j)}(\beta_k). \end{aligned}$$

Da Q eine mindestens[24] p-fache Nullstelle in β_k für jedes k und eine $(p-1)$-fache Nullstelle in 0 hat, verschwinden einige Summanden in der obigen Gleichung, und wir erhalten

[24] Es könnte $\beta_i = \beta_j$ für $i \neq j$ gelten.

$$J = -(2^n - m) \sum_{j=p-1}^{(m+1)p-1} N^j Q^{(j)}(0) - \sum_{j=p}^{(m+1)p-1} \sum_{k=1}^{n} N^j Q^{(j)}(\beta_k).$$

Die Zahlen $\beta_1, \ldots, \beta_m$ sind alle von der Form

$$\epsilon_1 N\alpha_1 + \ldots \epsilon_n N\alpha_n,$$

und damit ganzzahlige Linearkombinationen der ganzen algebraischen Zahlen $N\alpha_1, \ldots, N\alpha_n$. Nach Lemma 3.2.6 sind $\beta_1, \ldots, \beta_m$ also selbst ganze algebraische Zahlen. Die Polynome $\frac{1}{j!}Q^{(j)}$ haben nach Lemma 3.1.2 ganzzahlige Koeffizienten. Die Summe

$$\frac{1}{j!} \sum_{k=1}^{m} Q^{(j)}(X_k) \in \mathbb{Z}[X_1, \ldots, X_m]$$

stellt offensichtlich ein symmetrisches Polynom dar. Wir folgern aus Satz 3.2.12, dass

$$\frac{1}{j!} \sum_{k=1}^{m} Q^{(j)}(\beta_k) \in \mathbb{Z}.$$

Für $j \geq p$ erhalten wir also

$$\sum_{k=1}^{m} Q^{(j)}(\beta_k) \in p!\mathbb{Z}.$$

Nach Lemma 3.1.2 gilt für $j \geq p-1$ ebenso

$$Q^{(j)}(0) \in (p-1)!\mathbb{Z}.$$

Wir fassen unsere bisherigen Ergebnisse zu J wie folgt zusammen:

$$J = -(2^n - m) \sum_{j=p-1}^{(m+1)p-1} \underbrace{N^j Q^{(j)}(0)}_{\in (p-1)!\mathbb{Z}} - \sum_{j=p}^{(m+1)p-1} \underbrace{\sum_{k=1}^{m} N^j Q^{(j)}(\beta_k)}_{\in p!\mathbb{Z}}. \quad (3.7)$$

Insbesondere ist J eine durch $(p-1)!$ teilbare ganze Zahl. Wir zeigen nun, dass J ungleich Null ist, indem wir $J \not\equiv 0 \mod p$ zeigen. Da alle Summanden in der zweiten Summe in (3.7) durch p teilbar sind, erhalten wir

$$J \equiv -(2^n - m) N^{p-1} Q^{(p-1)}(0) \mod p.$$

Durch Ausmultiplizieren von $Q = X^{p-1}(X-\beta_1)^p \dots (X-\beta_m)^p$ sehen wir, dass

$$Q^{(p-1)}(0) = (p-1)!(-1)^{mp}(\beta_1 \dots \beta_m)^p \in \mathbb{Z}.$$

Insbesondere zeigt diese Gleichung, dass J für jede hinreichend große Primzahl p nicht durch p teilbar ist. Somit ist J eine von Null verschiedene durch $(p-1)!$ teilbare ganze Zahl und die Behauptung folgt.

Behauptung 2: Es gilt

$$|J| \leq AC^p$$

mit zwei von p unabhängigen positiven reellen Zahlen A und C.
Beweis der Behauptung 2: Wir schätzen zunächst jedes einzelne Integral

$$\left| I\left(\frac{\beta_k}{N}, Q(NX)\right)\right| = \left|\frac{\beta_k}{N}\right| \left| \int_0^1 e^{\beta_k/N(1-x)} Q(\beta_k x) dx \right|$$

mit Hilfe von Lemma 3.1.4 ab. Mit der von p unabhängigen Konstanten[25]

$$C := \max_{x\in[0,1]} |\beta_k||\beta_k x - \beta_1| \dots |\beta_k x - \beta_n|$$

erhalten wir für jedes $x \in [0,1]$ die Abschätzung

$$|\beta_k Q(\beta_k x)| = |x^{p-1}| \left|\beta_k^p (\beta_k x - \beta_1)^p \dots (\beta_k x - \beta_n)^p\right| \leq C^p.$$

Wir können also jedes einzelne der Wegintegrale wie folgt abschätzen

$$\left| I\left(\frac{\beta_k}{N}, Q(NX)\right)\right| \leq \left|\frac{e^{\beta_k/N}}{N}\right| C^p.$$

[25] Das Maximum existiert, da eine stetige Funktion auf einem kompakten Intervall ihr Maximum annimmt.

Somit erhalten wir mit $A := \frac{1}{N}\left|e^{\beta_1/N}\right| + \cdots + \left|e^{\beta_m/N}\right|$ die Abschätzung

$$|J| \leq \left|I\left(\frac{\beta_1}{N}, Q(NX)\right)\right| + \cdots + \left|I\left(\frac{\beta_m}{N}, Q(NX)\right)\right| \leq AC^p.$$

Da die positiven Konstanten A und C nicht von p abhängen, folgt die zweite Behauptung.

Kombinieren wir die beiden obigen Behauptungen, so erhalten wir die Ungleichungskette

$$(p-1)! \leq |J| \leq AC^p.$$

Da $(p-1)!$ für $p \to \infty$ stärker wächst als C^p führt diese Ungleichung für jede hinreichend große Primzahl p zu einem Widerspruch. □

Ausblick und offene Fragen

Wie oben bereits bemerkt, kann man den Satz 3.2.12 mit Methoden der Galoistheorie beweisen. Falls Sie bereits die Vorlesung Algebra gehört haben, dann können Sie diesen Abschnitt getrost überspringen. Ich möchte Ihnen hier einen kleinen Vorgeschmack auf die Themen der Galoistheorie geben.[26] Wir beschränken uns der Einfachheit halber auf den Grundkörper $\mathbb{Q}$ und betrachten nur Teilkörper von $\mathbb{C}$. Es ist nicht schwer zu sehen, dass jeder Teilkörper K von $\mathbb{C}$ bereits die rationalen Zahlen enthält. Zu einem gegebenen Teilkörper $K \subseteq \mathbb{C}$ betrachten wir nun die Menge aller Körperisomorphismen, welche auf $\mathbb{Q}$ die Identität induzieren[27]

$$\mathrm{Gal}(K/\mathbb{Q}) := \left\{\varphi\colon K \xrightarrow{\sim} K : \varphi(\alpha) = \alpha \text{ für alle } \alpha \in \mathbb{Q}\right\}.$$

Körperisomorphismen lassen sich durch Komposition verknüpfen:

$$\varphi, \psi \in \mathrm{Gal}(K/\mathbb{Q}) \Rightarrow \varphi \circ \psi \in \mathrm{Gal}(K/\mathbb{Q}).$$

Die Menge der Körperisomorphismen bildet also zusammen mit der Verknüpfung $\circ$ eine Gruppe mit der Identität als neutralem Element. Die Gruppe $\mathrm{Gal}(K/\mathbb{Q})$ nennen wir *Galoisgruppe* von K über $\mathbb{Q}$.

Beispiel 3.2.14. Die komplexe Konjugation induziert auf $\mathbb{Q}(i)$ einen Körperisomorphismus

$$\sigma\colon \mathbb{Q}(i) \to \mathbb{Q}(i), \quad \alpha \mapsto \overline{\alpha}.$$

Tatsächlich kann man zeigen, dass die Identitätsabbildung und σ die einzigen zwei Körperisomorphismen auf $\mathbb{Q}(i)$ sind. Es gilt also

$$\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \left\{\mathrm{id}_{\mathbb{Q}(i)}, \sigma\right\}.$$

[26] Für den weiteren Verlauf der Vorlesung spielen diese Resultate eher eine untergeordnete Rolle.

[27] Tatsächlich kann man leicht sehen, dass jeder Körperisomorphismus eines Körpers, der $\mathbb{Q}$ enthält, auf $\mathbb{Q}$ die Identität ist. Man kann allerdings die Galoisgruppe auch für beliebige Körpererweiterungen $K \subseteq L$ definieren, dann ist es wirklich notwendig, diese Bedingung zusätzlich zu fordern.

Wir nennen $K \subseteq \mathbb{C}$ algebraisch, wenn jedes $\alpha \in K$ algebraisch ist. Wir nennen eine algebraische Körpererweiterung K von $\mathbb{Q}$ *normal*, wenn K zu jedem $\alpha \in K$ auch bereits alle Konjugierten enthält. Das folgende Lemma zeigt insbesondere, dass jedes Element der Galoisgruppe diese Konjugierten vertauscht. Das Studium dieser Permutationen ist der zentrale Gegenstand der Galoistheorie.

Lemma 3.2.15. *Sei $K \subseteq \mathbb{C}$ eine algebraische Erweiterung und $P \in \mathbb{Q}[X]$ ein Polynom mit Nullstelle $\alpha \in K$. Dann ist auch $\varphi(\alpha)$ für jedes $\varphi \in Gal(K/\mathbb{Q})$ eine Nullstelle von P.*

Beweis. Wir schreiben

$$P = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Q}[X].$$

Es gilt

$$\begin{aligned} P(\varphi(\alpha)) &= a_n \varphi(\alpha)^n + \cdots + a_1 \varphi(\alpha) + a_0 \\ &= \varphi(a_n \alpha^n + \cdots + a_1 \alpha + a_0) = \varphi(0) = 0. \end{aligned}$$

Hier haben wir sowohl verwendet, dass φ ein Körperhomomorphismus ist, als auch die Eigenschaft, dass $\varphi(a) = a$ für $a \in \mathbb{Q}$. □

Im Rahmen der Galoistheorie zeigt man unter anderem das folgende Resultat.

Satz 3.2.16. *Sei K eine normale Erweiterung von $\mathbb{Q}$ und $\alpha \in K$ ein beliebiges Element. Falls $\varphi(\alpha) = \alpha$ für alle $\varphi \in Gal(K/\mathbb{Q})$ gilt, so ist α bereits in $\mathbb{Q}$ enthalten.*

Wir verwenden diesen Satz nun um Satz 3.2.12 zu zeigen:

Beweis. Seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen eines Polynoms $P \in \mathbb{Q}[X]$ und $Q \in \mathbb{Q}[X_1, \ldots, X_n]$ ein symmetrisches Polynom. Wir möchten zeigen, dass dann $Q(\alpha_1, \ldots, \alpha_n)$ rational ist. Nach Satz 3.2.16 reicht es zu zeigen, dass für jedes $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ die Gleichung

$$\varphi(Q(\alpha_1, \ldots, \alpha_n)) = Q(\alpha_1, \ldots, \alpha_n)$$

gilt. Sei also $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ gegeben. Nach Lemma 3.2.15 vertauscht φ die Nullstellen $\alpha_1, \ldots, \alpha_n$ von P. Da φ bijektiv ist und nach Lemma 3.2.15 Nullstellen auf Nullstellen abbildet, gibt[28] es also eine Permutation $\sigma \in S_n$ mit $\varphi(\alpha_i) = \alpha_{\sigma(i)}$. Wir rechnen nun

$$\begin{aligned} \varphi(Q(\alpha_1, \ldots, \alpha_n)) &= \\ &= Q(\varphi(\alpha_1), \ldots, \varphi(\alpha_1)) = Q(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = \\ &= Q(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

[28] Diese Permutation ist im Allgemeinen nicht eindeutig, da $\alpha_i = \alpha_j$ für $i \neq j$ sein könnte. Für uns ist allerdings nur die Existenz wichtig.

Hierbei haben wir in der ersten Gleichung benutzt, dass φ ein Körperhomomorphismus ist, welcher die Identität auf $\mathbb{Q}$ induziert. Die zweite Gleichung folgt aus $\varphi(\alpha_i) = \alpha_{\sigma_i}$, und die dritte Gleichung verwendet die Symmetrie des Polynoms Q. Das zeigt die erste Aussage von Satz 3.2.12. Die zweite Behauptung über die Ganzheit folgt nun leicht: Da Summen und Produkte ganzer algebraischer Zahlen ganz sind, ist $Q(\alpha_1, \ldots, \alpha_n)$ eine ganze algebraische Zahl, falls Q ganzzahlige Koeffizienten hat und $\alpha_1, \ldots, \alpha_n$ ganze algebraische Zahlen sind. Somit liegt $Q(\alpha_1, \ldots, \alpha_n)$ einerseits in $\mathbb{Q}$ und ist andererseits eine ganze algebraische Zahl. Da die Menge der ganzen algebraischen Zahlen in $\mathbb{Q}$ gerade $\mathbb{Z}$ ist, folgt $Q(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$, siehe Beispiel 3.2.3. □

3.3 *Die Quadratur des Kreises*

Wir[29] haben bereits besprochen, dass die Entdeckung der Irrationalität durch Samos von Metapont das mathematische Weltbild der griechischen Antike erschütterte. Nachdem dadurch klar war, dass es mehr Zahlen als nur die ganzen Zahlen und deren Verhältnisse gibt, hofften die Griechen, dass man wenigstens alle Zahlen als Längen geometrischer Konstruktionen mit Zirkel und Lineal erhalten kann. Dies führte auf die drei klassischen Konstruktionsprobleme der antiken Mathematik.

- Die Quadratur des Kreises,
- die Dreiteilung eines gegebenen Winkels,
- die Verdoppelung des Würfels.

Das Problem der Quadratur des Kreises gehört sicherlich zu den populärsten [30] Problemen der Mathematik: Dabei geht es um die Frage, ob man zu einem gegebenen Kreis nur mit Hilfe von Zirkel und Lineal ein Quadrat mit gleichem Flächeninhalt konstruieren kann [31]. Im Jahre 1882 gelang Lindemann mit dem Beweis der Transzendenz von π der Durchbruch. Er konnte die Unmöglichkeit der Quadratur des Kreises zeigen. In der heutigen Vorlesung wollen wir zunächst die Algebraizität aller mit Zirkel und Lineal konstruierbarer Zahlen beweisen. Als Anwendung zeigen wir dann die Unmöglichkeit der Quadratur des Kreises.

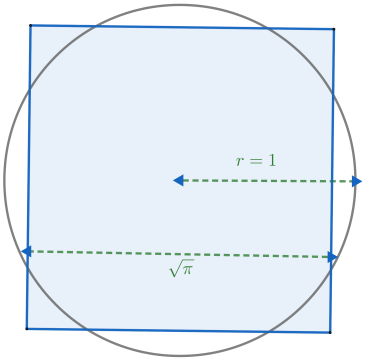
Konstruktionen mit Zirkel und Lineal

Wir präzisieren zunächst, was überhaupt mit einer Konstruktion durch Zirkel und Lineal gemeint ist: Wir starten mit zwei Punkten in der Ebene. Als Modell der Ebene wählen wir im Folgenden $\mathbb{R}^2$ mit dem

[29] Zu diesem Abschnitt gibt es ein Video:

[30] Das Thema der Quadratur des Kreises wurde auch häufig in Kunst und Musik aufgegriffen:

[31] Das Problem ist also äquivalent dazu, zu einer gegebenen Strecke der Länge 1 eine Strecke der Länge $\sqrt{\pi}$ zu konstruieren.



euklidischen Skalarprodukt

$$\langle \cdot, \cdot \rangle \colon \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}, \quad \left\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle := x_1 y_1 + x_2 y_2.$$

Ohne Beschränkung der Allgemeinheit dürfen wir durch Drehung und Skalierung der Ebene annehmen, dass

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ und } \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

die beiden anfangs gegebenen Punkte sind. Ausgehend von diesen beiden Punkten können wir nun iterativ Geraden, Kreise und weitere Punkte konstruieren, wobei wir uns an die folgenden Regeln halten:

- Wir dürfen eine Gerade AB durch zwei bereits konstruierte Punkte A und B legen.
- Wir dürfen einen Kreis $K(A, r)$ um einen bereits konstruierten Punkt A mit Radius r ziehen. Der Radius r des Kreises muss dabei der Abstand zweier bereits konstruierter Punkte sein.
- Ein Punkt gilt als konstruiert, wenn er als Schnittpunkt eines Kreises mit einer Geraden, zweier verschiedener Kreise, oder zweier verschiedener Geraden auftritt.

Eine reelle Zahl α heißt dabei konstruierbar, wenn der Punkt

$$\begin{pmatrix} \alpha \\ 0 \end{pmatrix}$$

konstruierbar ist.[32]

Beispiel 3.3.1. Ausgehend von den Punkten

$$P_0 = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \text{ und } P_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

können wir im ersten Konstruktionsschritt genau drei Konstruktionen ausführen:

- Wir können die Gerade $g = P_0P_1$, also die x-Achse, konstruieren.
- Wir können einen Kreis mit Radius 1 um P_0 ziehen.
- Wir können einen Kreis mit Radius 1 um P_1 ziehen.

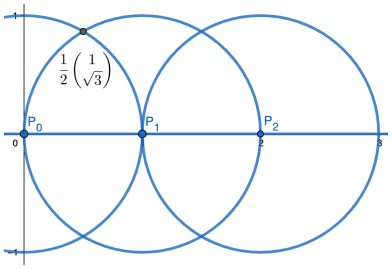
Indem wir den Kreis $K(P_1, 1)$ mit der x-Achse schneiden erhalten[33] wir den „neuen“ Punkt

$$P_2 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

[32] Die klassische euklidische Geometrie kennt keine Koordinatensysteme. Auch die negativen Zahlen traten in der antiken Mathematik eher indirekt auf. Es wäre wohl näher am antiken Mathematikverständnis, eine Zahl als konstruierbar zu bezeichnen, wenn diese als Verhältnis der Längen zweier konstruierbarer Strecken auftritt. Offensichtlich erhält man auf diese Wiese nur positive reelle Zahlen. Allerdings ist der Unterschied nicht wesentlich: Man erhält mit dieser Definition bis auf das Vorzeichen exakt die gleiche Menge an konstruierbaren Zahlen.

Ein Grund auch negative Zahlen zu zulassen ist, dass man dann zeigen kann, dass die Menge der konstruierbaren Zahlen einen Körper bilden. Wir werden dies im Übungsbetrieb sehen.

[33]



Der Schnitt des Kreises $K(P_2, 1)$ mit der x-Achse gibt

$$P_3 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}.$$

Auf diese Art können wir alle ganzen Zahlen konstruieren. Natürlich bekommen wir auch leicht Punkte außerhalb der x-Achse oder Punkte mit nicht nur rationalen Koordinaten. Zum Beispiel liefert $K(P_0, 1) \cap K(P_1, 1)$ die Punkte

$$\frac{1}{2}\begin{pmatrix} 1 \\ \pm\sqrt{3} \end{pmatrix}.$$

Aus der Schule ist bekannt, dass sich Geraden in der Ebene durch lineare Gleichungen beschreiben lassen, und dass Kreise (neben Ellipsen und Hyperbeln) als Nullstellenmengen polynomialer Gleichungen zweiten Grades auftreten. Da konstruierbare Punkte nun gerade die Schnittpunkte dieser geometischen Objekte sind, ist es wenig überraschend, dass die folgende Proposition gilt:

Proposition 3.3.2. *Jede konstruierbare Zahl ist algebraisch.*

Beweis. Für den Rest des Beweises nennen wir einen Punkt $A \in \mathbb{R}^2$ *algebraisch*, wenn dieser algebraische Koordinaten hat, d.h.

$$A \in (\overline{\mathbb{Q}} \cap \mathbb{R})^2.$$

Um die Proposition zu zeigen würde es reichen die Algebraizität aller konstruierbaren Punkte auf der x-Achse zu zeigen. Wir zeigen etwas allgemeiner, dass jeder konstruierbare Punkt algebraisch ist. Da unsere Startpunkte algebraisch sind und alle Punkte durch sukzessives Schneiden bereits konstruierter Kreise und Geraden entstehen, reicht es also die folgende Behauptung zu zeigen:
Behauptung: Es seien

$$A = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, C = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}, D = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix} \in (\overline{\mathbb{Q}} \cap \mathbb{R})^2$$

algebraische Punkte und $r, r' \in \overline{\mathbb{Q}} \cap \mathbb{R}_{>0}$ positive reelle algebraische Zahlen. Dann gilt:

(a) Falls die Geraden $g = AB$ und $h = CD$ verschieden sind, gilt

$$g \cap h \subseteq (\overline{\mathbb{Q}} \cap \mathbb{R})^2.$$

(b) Für die Gerade $g = AB$ und den Kreis $K = K(C, r)$ gilt

$$g \cap K \subseteq (\overline{\mathbb{Q}} \cap \mathbb{R})^2.$$

(c) Falls die Kreise $K = K(A, r)$ und $K' = K(B, r')$ verschieden sind, gilt

$$K \cap K' \subseteq (\overline{\mathbb{Q}} \cap \mathbb{R})^2.$$

Beweis der Behauptung: In jedem der drei Fälle erhalten wir die Koordinaten durch Lösung linearer Gleichungssysteme und polynomieller Gleichungen vom Grad ≤ 2 mit algebraischen Koeffizienten. Daraus folgt dann die Algebraizität der Schnittpunkte, genauer :
(a):[34] Falls die Richtungsvektoren

$$\begin{pmatrix} b_1 - a_1 \\ b_2 - a_2 \end{pmatrix}, \begin{pmatrix} d_1 - c_1 \\ d_2 - c_2 \end{pmatrix} \in \mathbb{R}^2$$

linear abhängig sind, so sind die Geraden g und h parallel und es gibt keinen Schnittpunkt. Andernfalls hat das Gleichungssystem

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} + s \begin{pmatrix} d_1 - c_1 \\ d_2 - c_2 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + t \begin{pmatrix} b_1 - a_1 \\ b_2 - a_2 \end{pmatrix}$$

eine eindeutige Lösung[35] $(s,t) = (s_0, t_0)$ in $(\overline{\mathbb{Q}} \cap \mathbb{R})^2$. Der eindeutige Schnittpunkt der Geraden g und h ist dann gegeben durch

$$S := \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} + s_0 \begin{pmatrix} d_1 - c_1 \\ d_2 - c_2 \end{pmatrix}.$$

Da alle Zahlen c_1, c_2, d_1, d_2, s_0 algebraische reelle Zahlen sind, hat auch S algebraische reelle Koordinaten und (a) folgt.
(b):[36]

Der Kreis $K(C,r)$ lässt sich beschreiben als

$$K(C,r) = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 : (x_1 - c_1)^2 + (x_2 - c_2)^2 = r^2 \right\}$$

und die Gerade $g = AB$ lässt sich parametrisieren durch

$$g = \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + t \begin{pmatrix} b_1 - a_1 \\ b_2 - a_2 \end{pmatrix} : t \in \mathbb{R} \right\}.$$

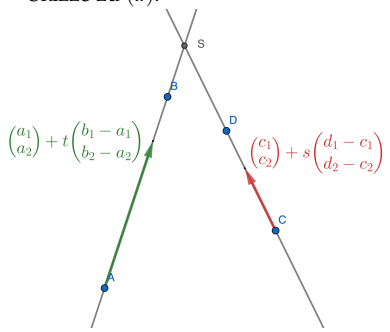
Somit ist die Menge der Schnittpunkte gegeben durch

$$\Bigg\{ \begin{pmatrix} a_1 + t(b_1 - a_1) \\ a_2 + t(b_2 - a_2) \end{pmatrix} : \text{ mit } t \in \mathbb{R}, \\ \text{sodass } (a_1 + t(b_1 - a_1) - c_1)^2 + (a_2 + t(b_2 - a_2) - c_2)^2 = r^2 \Bigg\}. \quad (3.8)$$

Eine reelle Zahl $t \in \mathbb{R}$ erfüllt $(a_1 + t(b_1 - a_1) - c_1)^2 + (a_2 + t(b_2 - a_2) - c_2)^2 = r^2$ genau dann, wenn t Nullstelle des Polynoms

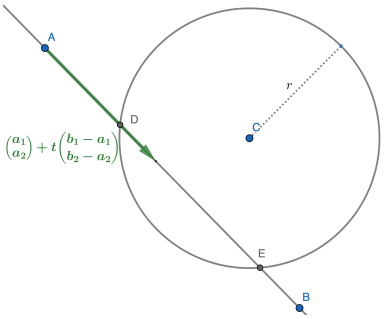
$$((b_1 - a_1)^2 + (b_2 - a_2)^2)X^2 \\ + 2((a_1 - c_1)(b_1 - a_1) + (a_2 - c_2)(b_2 - a_2))X \\ + (a_1 - c_1)^2 + (a_2 - c_2)^2 - r^2$$

[34] Skizze zu (a):



[35] Wir bemerken an dieser Stelle, dass $\overline{\mathbb{Q}} \cap \mathbb{R}$ ein Körper ist, siehe Lemma 3.2.6. Die Eindeutigkeit folgt dann aus der Linearen Algebra.

[36] Skizze zu (b):



ist. Da dieses Polynom algebraische Koeffizienten hat, sind alle Lösungen der Gleichung

$$(a_1 + t(b_1 - a_1) - c_1)^2 + (a_2 + t(b_2 - a_2) - c_2)^2 = r^2$$

algebraisch. Die Formel (3.8) zeigt, dass alle Schnittpunkte in $(\overline{\mathbb{Q}} \cap \mathbb{R})^2$ liegen.

(c):[37] Falls die Schnittmenge leer ist, so ist nichts zu zeigen. Sei also $S = (s_1, s_2) \in K(A, r) \cap K(B, r')$ ein Schnittpunkt. Dann ist $(X_1, X_2) = (s_1, s_2)$ eine Lösung des Gleichungssystems

$$\begin{aligned}(X_1 - a_1)^2 + (X_2 - a_2)^2 - r^2 &= 0\\ (X_1 - b_1)^2 + (X_2 - b_2)^2 - (r')^2 &= 0.\end{aligned}$$

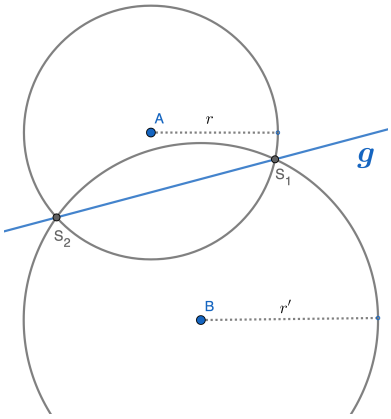
Durch Subtrahieren der beiden Gleichungen sehen wir, dass S auf der Geraden

$$g = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{R}^2 : \right.$$
$$\left. x_1(-2a_1 + 2b_1) + x_2(-2a_2 + 2b_2) + a_1^2 + a_2^2 - r^2 - b_1^2 - b_2^2 + (r')^2 = 0 \right\}$$

liegt. Da diese Geradengleichung algebraische Koeffizienten hat, lässt sich g schreiben als $g = CD$ für geeignete Punkte $C, D \in (\overline{\mathbb{Q}} \cap \mathbb{R})^2$. Somit folgt $S \in g \cap K$. Aus (b) erhalten wir nun $S \in (\overline{\mathbb{Q}} \cap \mathbb{R})^2$ wie gewünscht.

□

[37] Skizze zu (c):



Die Unmöglichkeit der Quadratur des Kreises

Satz 3.3.3. *Die Quadratur des Kreises ist unmöglich.*

Beweis. Angenommen man könnte zu einem gegeben Kreis mit Zirkel und Lineal ein Quadrat konstruieren, welches denselben Flächeninhalt besitzt wie der Kreis. Ohne Einschränkung dürfen wir annehmen, dass der Radius des Kreises 1 ist. Damit wäre die Zahl $\sqrt{\pi}$ als Seitenlänge des Quadrats konstruierbar[38]. Nach Proposition 3.3.2 wäre $\sqrt{\pi}$ algebraisch. Mit $\sqrt{\pi}$ wäre nach Lemma 3.2.6 auch $\sqrt{\pi} \cdot \sqrt{\pi} = \pi$ algebraisch, im Widerspruch zum Satz von Lindemann. □

[38] Hätten wir das Quadrat mit Seitenlänge $\sqrt{\pi}$ konstruiert, dann könnten wir einen Kreis mit Radius $\sqrt{\pi}$ um $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ mit der x-Achse schneiden und erhielten den Punkt

$$\begin{pmatrix} \sqrt{\pi} \\ 0 \end{pmatrix}.$$

Also ist die Lösbarkeit der Quadratur des Kreises wirklich äquivalent zur Konstruierbarkeit von $\sqrt{\pi}$ im Sinne der obigen Definition.

Ausblick

Im Übungsbetrieb werden wir sehen, dass die konstruierbaren Zahlen einen Körper bilden und dass der Grad einer konstruierbaren Zahl stets eine Zweierpotenz ist[39]. Dies hat interessante Konsequenzen und erlaubt es die Unlösbarkeit der beiden anderen klassischen Konstruktionsprobleme der antiken Mathematik zu zeigen.

[39] Der wesentliche Punkt ist hierbei, dass wir in jedem Konstruktionsschritt die Koordinaten des neuen Punkts erhalten, indem wir eine polynomielle Gleichung vom Grad ≤ 2 lösen.

Die *Verdoppelung des Würfels* ist äquivalent zur Konstruierbarkeit von $\sqrt[3]{2}$. Da der Grad von $\sqrt[3]{2}$ allerdings keine Zweierpotenz ist, folgt die Unmöglichkeit der Verdoppelung des Würfels.

Ähnlich verhält es sich bei der *Dreiteilung beliebiger Winkel*. Zum Beispiel wäre die Dreiteilung des Winkels 120 äquivalent zur Konstruierbarkeit des regelmäßigen 9-Ecks. Allerdings werden wir im Übungsbetrieb sehen, dass das regelmäßige 9-Eck nicht konstruierbar ist.

3.4 Der Satz von Lindemann–Weierstraß

Aufbauend auf den Hermiteschen Beweis der Transzendenz von e zeigte Lindemann im Jahre 1882 die Transzendenz von π. Er deutete bereits an, dass sein Beweis stärkere Transzendenzaussagen liefert als nur die Transzendenz von π. Im Jahre 1885 führte Weierstraß diese Ideen näher aus. Dies führte zu dem Beweis des Satzes, der heute gewöhnlich Satz von Lindemann–Weiersrtaß genannt wird.

Separabilität von Polynomen[40]

[40] Zu diesem Abschnitt gibt es ein Video:

In diesem Kapitel möchten wir uns mit der Frage beschäftigen, wie man entscheiden kann, ob ein gegebenes Polynom mehrfache Nullstellen besitzt.

Definition 3.4.1. Ein Polynom $P \in \mathbb{C}[X]$ heißt *separabel*, wenn P in $\mathbb{C}$ keine mehrfachen Nullstellen besitzt.

Wir erinnern daran, dass wir mit P' die (formale) Ableitung eines Polynoms bezeichnen. Das folgenden Kriterium erlaubt es uns zu prüfen, ob ein gegebenes Polynom $P \in \mathbb{C}[X]$ separabel ist.

Lemma 3.4.2. *Ein Polynom $P \in \mathbb{C}[X]$ ist genau dann separabel, wenn P' und P keine gemeinsamen Nullstellen besitzen.*

Beweis. Falls $\alpha \in \mathbb{C}$ eine Nullstelle der Ordnung $k \geq 1$ von P ist, so lässt sich P schreiben als

$$P = (X - \alpha)^k Q$$

für ein geeignetes Polynom $Q \in \mathbb{C}[X]$ mit $Q(\alpha) \neq 0$. Dann gilt

$$P' = k(X - \alpha)^{k-1} Q + (X - \alpha)^k Q'$$

und somit $P'(\alpha) = k(X - \alpha)^{k-1}|_{X=\alpha} \cdot Q(\alpha)$. Diese Zahl ist genau dann Null, wenn $k \geq 2$ ist. □

Wir zeigen nun die Separabilität des Minimalpolynoms über $\mathbb{Q}$.

Korollar 3.4.3. *Das Minimalpolynom einer algebraischen Zahl ist separabel. Insbesondere sind die Konjugierten $\alpha_1, \ldots, \alpha_n$ von α paarweise verschieden.*

Beweis. Sei α eine algebraische Zahl vom Grad n mit Minimalpolynom $P := \mathrm{MinPol}_{\mathbb{Q}}(\alpha)$.

Behauptung: P ist auch das Minimalpolynom aller Konjugierten von α.
Beweis der Behauptung: Seien β eines der Konjugierten von α und

$$Q := \mathrm{MinPol}_{\mathbb{Q}}(\beta).$$

Durch Polynomdivision sehen wir[41]

$$P = Q \cdot \widetilde{Q}.$$

für ein geeignetes Polynom $\widetilde{Q} \in \mathbb{Q}[X]$. Wäre $\deg Q < n$, so hätten wir

$$0 = P(\alpha) = Q(\alpha) \cdot \widetilde{Q}(\alpha)$$

und somit wäre α Nullstelle eines der Polynome Q oder $\widetilde{Q}$. Da beide Polynome kleineren Grad als P haben, wäre das ein Widerspruch. Somit gilt $\deg Q = \deg P$ und da beide Polynome sogar normiert sind folgt $P = Q$. Damit ist die Behauptung gezeigt.

Aus der Behauptung folgt nun, dass P separabel ist. Wäre P nicht separabel, so gäbe es ein Konjugiertes β von α, welches eine mehrfache Nullstelle ist. Nach Lemma 3.4.2 wäre β damit auch Nullstelle des normierten Polynoms $Q := \frac{1}{n}P'$. Da Q echt kleineren Grad als P hat widerspricht dies der oben gezeigten Behauptung, dass P das Minimalpolynom von β über $\mathbb{Q}$ ist. □

[41] Dieses Argument haben wir bereits ein paar Mal gesehen: Polynomdivision von P durch Q mit Rest liefert:

$$P = Q \cdot \widetilde{Q} + R \text{ mit } \deg R < \deg Q.$$

Es folgt

$$R(\beta) = \underbrace{P(\beta)}_{=0} - \underbrace{Q(\beta)}_{=0}\widetilde{Q}(\beta) = 0.$$

Somit ist R ein Polynom mit strikt kleinerem Grad als $Q = \mathrm{MinPol}_{\mathbb{Q}}(\beta)$ und Nullstelle β; es folgt $R = 0$.

Algebraische Unabhängigkeit

Die abelsche Gruppe $(\mathbb{C}, +)$ wird vermöge der Skalarmultiplikation

$$\mathbb{Q} \times \mathbb{C} \to \mathbb{C}, \quad (q, z) \mapsto q \cdot z$$

zu einem $\mathbb{Q}$-Vektorraum. Falls $\alpha_1, \ldots, \alpha_n$ über $\mathbb{Q}$ linear abhängige komplexe Zahlen sind, so gibt es also $a_1, \ldots, a_n \in \mathbb{Q}$, mit $a_i \neq 0$ für mindestens ein $1 \leq i \leq n$, sodass

$$a_1\alpha_1 + \cdots + a_n\alpha_n = 0.$$

Wir können das auch wie folgt formulieren. Es gibt ein von Null verschiedenes lineares Polynom

$$P = a_1X_1 + \cdots + a_nX_n \in \mathbb{Q}[X]$$

mit $P(\alpha_1, \ldots, \alpha_n) = 0$. Lineare Abhängigkeit bedeutet somit eine nichttriviale lineare polynomielle Identität in $\alpha_1, \ldots, \alpha_n$. Der Begriff der algebraischen Abhängigkeit verallgemeinert dies auf beliebige polynomielle Identitäten in n Variablen.

Definition 3.4.4. Die Zahlen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ heißen *algebraisch abhängig* über $\mathbb{Q}$, wenn es ein von Null verschiedenes Polynom $P \in \mathbb{Q}[X_1, \ldots, X_n]$ gibt mit

$$P(\alpha_1, \ldots, \alpha_n) = 0.$$

Andernfalls heißen die Zahlen $\alpha_1, \ldots, \alpha_n$ algebraisch unabhängig. Eine beliebige Teilmenge $S \subseteq \mathbb{C}$ heißt algebraisch unabhängig, wenn jede endliche Folge paarweise verschiedener Zahlen $\alpha_1, \ldots, \alpha_n \in S$ algebraisch unabhängig über $\mathbb{Q}$ ist.

Lemma 3.4.5. *Wenn die Zahlen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ algebraisch unabhängig über $\mathbb{Q}$ sind, so sind sie insbesondere transzendent.*

Beweis. Gäbe es ein von Null verschiedenes Polynom

$$P = a_n X^n + \cdots + a_1 X + a_0$$

mit $P(\alpha_i) = 0$, so wäre

$$Q = a_n X_i^n + \cdots + a_1 X_i + a_0 \in \mathbb{Q}[X_1, \ldots, X_n]$$

ein von Null verschiedenes Polynom in n Variablen mit $Q(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$, im Widerspruch zur algebraischen Unabhängigkeit. □

Ähnlich zum Dimensionsbegriff aus der linearen Algebra definieren wir den Transzendenzgrad:

Definition 3.4.6. Der *Transzendenzgrad* über $\mathbb{Q}$ eines Unterkörpers $K \subseteq \mathbb{C}$ ist die Mächtigkeit einer maximalen über $\mathbb{Q}$ algebraisch unabhängigen Teilmenge.[42]

[42] Ähnlich wie beim Dimensionsbegriff der linearen Algebra zeigt man, dass zwei maximale algebraisch unabhängige Teilmengen die gleiche Kardinalität haben.

Lineare Unabhängigkeit der Werte der Exponentialfunktion

Als Vorarbeit für die allgemeine Version des Satzes von Lindemann-Weierstraß werden wir zunächst das folgende (scheinbar) schwächere Resultat zeigen.

Proposition 3.4.7. *Für paarweise verschiedene algebraische Zahlen $\beta_1, \ldots, \beta_n$ sind die Zahlen $e^{\beta_1}, \ldots, e^{\beta_n}$ linear unabhängig über $\mathbb{Q}$.*

Beweis. Da Teilmengen einer über $\mathbb{Q}$ linear unabhängigen Menge wieder linear unabhängig sind, dürfen wir die Menge $\{\beta_1, \ldots, \beta_n\}$ ohne Einschränkung durch weitere Elemente ergänzen. Wir dürfen also annehmen, dass die Menge

$$\{\beta_1, \ldots, \beta_n\}$$

zu jedem β_i auch alle Konjugierten enthält.

Sei $N \in \mathbb{N}$ eine natürliche Zahl, sodass $N\beta_1, \dots, N\beta_n$ allesamt ganze algebraische Zahlen sind, siehe Lemma 3.2.5. Angenommen die Zahlen $e^{\beta_1}, \dots, e^{\beta_n}$ wären linear abhängig über $\mathbb{Q}$. Dann wäre[43]

$$b_1 e^{\beta_1} + \cdots + b_n e^{\beta_n} = 0 \tag{3.9}$$

mit $b_1, \dots, b_n \in \mathbb{Z}$ und $b_i \neq 0$ für mindestens ein i. Wir bezeichnen mit K die kleinste Körpererweiterung über $\mathbb{Q}$, welche die Zahlen $\beta_1, \dots, \beta_n$ enthält. Wir erinnern daran, dass

$$\mathrm{Gal}(K/\mathbb{Q}) := \left\{ \varphi \colon K \xrightarrow{\sim} K : \varphi(\alpha) = \alpha \text{ für alle } \alpha \in \mathbb{Q} \right\}.$$

Indem wir das folgende Produkt ausmultplizieren und geeignet nach Exponentialtermen sortieren erhalten wir

$$\prod_{\varphi \in \mathrm{Gal}(K/\mathbb{Q})} (b_1 e^{\varphi(\beta_1)} + \cdots + b_n e^{\varphi(\beta_n)}) = \widetilde{b}_1 e^{\widetilde{\beta}_1} + \cdots + \widetilde{b}_m e^{\widetilde{\beta}_m}.$$

eine Linearkombination $\widetilde{b}_1 e^{\widetilde{\beta}_1} + \cdots + \widetilde{b}_m e^{\widetilde{\beta}_m}$ mit den folgenden Eigenschaften:

- $\widetilde{b}_1 \neq 0$ und $\widetilde{b}_k \in \mathbb{Z}$ für $1 \leq k \leq m$.
- Für alle $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ gilt $\widetilde{b}_1 e^{\varphi(\widetilde{\beta}_1)} + \cdots + \widetilde{b}_m e^{\varphi(\widetilde{\beta}_m)} = 0$.
- Die Menge $\{\widetilde{\beta}_1, \dots, \widetilde{\beta}_m\}$ enthält zu jedem Element $\widetilde{\beta}_k$ auch alle Konjugierten.
- Die Zahlen $N \cdot \widetilde{\beta}_k$ für $1 \leq k \leq m$ sind ganze algebraische Zahlen.

Wir betrachten nun für eine hinreichend große Primzahl p die Zahl

$$I := \sum_{k=1}^{m} \widetilde{b}_k I(\widetilde{\beta}_k, Q)$$

mit

$$Q := N^{mp} (X - \widetilde{\beta}_1)^{p-1} \prod_{i=2}^{m} (X - \widetilde{\beta}_i)^p \in K[X].$$

Wir werden im Folgenden sehen, dass die Zahl I zwar eine ganze algebraische Zahl im Körper K ist, im Allgemeinen wird diese allerdings nicht notwendigerweise schon in $\mathbb{Z}$ liegen. Deswegen benötigen wir die folgende Konstruktion. Wir setzen $J := \prod_{\varphi \in \mathrm{Gal}(K/\mathbb{Q})} \varphi(I)$. Wie bereits in den Beweisen von Hermite und Lindemann möchten wir nun eine untere und eine obere Schranke für $|J|$ herleiten.[44] Die untere Schranke ist wieder algebraischer Natur, während die obere Schranke durch analytische Abschätzung der beteiligten Integrale gezeigt wird.

Behauptung 1: Die Zahl I liegt in K, deshalb ist

$$J := \prod_{\varphi \in Gal(K/\mathbb{Q})} \varphi(I)$$

[43] Zunächst finden wir $b_1, \dots, b_n \in \mathbb{Q}$ mit $b_i \neq 0$ für mindestens ein i und

$$b_1 e^{\beta_1} + \cdots + b_n e^{\beta_n} = 0.$$

Nach Multiplikation mit dem Hauptnenner der rationalen Zahlen $b_1, \dots, b_n$ können wir allerdings annehmen, dass die Zahlen $b_1, \dots, b_n$ ganzzahlig sind.

[44] Die Beweise der Behauptungen sind wieder ähnlich zu den jeweiligen Beweisen in den Sätzen von Hermite und Lindemann, nur etwas technischer. Es reicht vollkommen, wenn Sie die Beweise nur überfliegen.

wohldefiniert. Wenn wir die Primzahl p hinreichen groß wählen, so gilt $|J| \geq (p-1)!$.

Beweis der Behauptung 1: Wir überlegen uns zunächst, dass I in K liegt. Unter Verwendung von Lemma 3.1.5 und in Anbetracht der Gleichung (3.9) erhalten wir

$$I = -\sum_{k=1}^{m} \sum_{j=0}^{mp-1} \widetilde{b}_k Q^{(j)}(\widetilde{\beta}_k).$$

Da die Nullstelle $\widetilde{\beta}_1$ von Q die Ordnung $p-1$ hat und alle anderen Nullstellen die Ordnung p haben, sind einige Summanden in der obigen Summe Null und wir erhalten

$$I = -\widetilde{b}_1 Q^{(p-1)}(\widetilde{\beta}_1) - \sum_{k=1}^{m} \sum_{j=p}^{mp-1} \widetilde{b}_k Q^{(j)}(\widetilde{\beta}_k). \tag{3.10}$$

Da alle Zahlen $\widetilde{\beta}_k$ in K liegen und Q Koeffizienten in K hat folgt $I \in K$. Insbesondere macht es Sinn einen Körperautomorphismus $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ auf I an zu wenden. Wir zeigen nun, dass J eine durch $(p-1)!$ teilbare von Null verschiedene ganze Zahl ist. Wir betrachten zunächst die Zahl I. Wir werden gleich sehen, dass diese Zahl das $(p-1)!$-fache einer ganzen algebraischen Zahl aus dem Körper K ist. Wir bezeichnen im Folgenden die Menge der ganzen Zahlen in K mit $\mathcal{O}_K$. Da ganze algebraische Zahlen abgeschlossen unter Addition und Multiplikation sind, siehe Lemma 3.2.6, ist $\mathcal{O}_K$ sogar ein Unterring des Körpers K.

Wir möchten nun zeigen, dass $Q^{(j)}(\widetilde{\beta}_k)$ für $j \geq 0$ und $1 \leq k \leq m$ das $j!$-fache einer ganzen algebraischen Zahl ist, d.h.

$$Q^{(j)}(\widetilde{\beta}_k) \in j!\mathcal{O}_K.$$

Wir können Q auch schreiben als

$$Q = P(NX)$$

mit

$$P = N(X - N\widetilde{\beta}_1)^{p-1} \prod_{i=2}^{m} (X - N\widetilde{\beta}_i)^p.$$

Wir erinnern, dass die Zahlen $N\widetilde{\beta}_1, \ldots, N\widetilde{\beta}_m$, und somit auch die Koeffizienten des Polynoms P, ganze algebraische Zahlen sind. Da die j-fache Ableitung jedes Monoms durch $j!$ teilbar ist, folgern wir wie im Beweis des Lemmas 3.1.2, dass

$$Q^{(j)}(\widetilde{\beta}_k) = N^j P^{(j)}(N\widetilde{\beta}_k) \in j!\mathcal{O}_K. \tag{3.11}$$

Indem wir die Gleichungen (3.10) und (3.11) kombinieren, sehen wir, dass I das $(p-1)!$ fache einer ganzen algebraischen Zahl $\alpha \in \mathcal{O}_K$ ist, d.h.

$$I = (p-1)! \cdot \alpha.$$

Aus Lemma 3.2.15 folgt, dass mit I auch $\varphi(I)$ für jedes $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ wieder ganz ist. Wir erhalten also, dass auch J das $(p-1)!$-fache einer ganzen algebraischen Zahl ist. Andererseits gilt für jedes $\psi \in \mathrm{Gal}(K/\mathbb{Q})$ die Gleichung

$$\psi(J) = \psi\left(\prod_{\varphi\in\mathrm{Gal}(K/\mathbb{Q})} \varphi(I)\right) = \prod_{\varphi\in\mathrm{Gal}(K/\mathbb{Q})} (\psi\circ\varphi)(I) = \prod_{\varphi\in\mathrm{Gal}(K/\mathbb{Q})} \varphi(I) = J,$$

und wir folgern aus Satz 3.2.16, dass J rational ist, d.h. $J \in \mathbb{Q}$. Insgesamt ist J eine durch $(p-1)!$ teilbare ganze algebraische Zahl in $\mathbb{Q}$ und wir erhalten $J \in (p-1)!\mathbb{Z}$.

Die Gleichungen (3.10) und (3.11) zeigen[45]

$$I \equiv -\widetilde{b}_1 Q^{(p-1)}(\widetilde{\beta}_1) \mod p\mathcal{O}_K.$$

[45] Die Notation $a \equiv b \mod p\mathcal{O}_K$ heißt, dass die Differenz $a-b$ das p fache einer ganzen algebraischen Zahl aus p ist.

Dies erlaubt es uns nun J modulo p zu berechnen:

$$J = \prod_{\varphi\in\mathrm{Gal}(K/\mathbb{Q})} \varphi(I) \equiv \prod_{\varphi\in\mathrm{Gal}(K/\mathbb{Q})} \varphi(-\widetilde{b}_1 Q^{(p-1)}(\widetilde{\beta}_1))$$
$$\equiv \prod_{\varphi} \varphi\left((-\widetilde{b}_1(p-1)!N^p)\cdot\prod_{j=2}^{m}(N\widetilde{\beta}_1 - N\widetilde{\beta}_j)^p\right) \mod p\mathcal{O}_K. \quad (3.12)$$

Die von Null verschiedene Zahl

$$K := \prod_{\varphi} \varphi\left(\prod_{j=2}^{m}(N\widetilde{\beta}_1 - N\widetilde{\beta}_j)\right)$$

ist einerseits als Produkt ganzer algebraischer Zahlen ganz, andererseits liegt sie nach Satz 3.2.16 in $\mathbb{Q}$. Es folgt also $K \in \mathbb{Z}$. Nach (3.12) erhalten wir die folgende Kongruenz in $\mathbb{Z}$

$$J \equiv (-\widetilde{b}_1(p-1)!N^p)^{|\mathrm{Gal}(K/\mathbb{Q})|}K^p.$$

Für jede Primzahl p, die keine der Zahlen K, $\widetilde{b}_1$ und N teilt, gilt $J \neq 0 \mod p$. Für hinreichend großes p ist J also nicht durch p teilbar und somit $J \neq 0$. Als durch $(p-1)!$ teilbare von Null verschiedene ganze Zahl hat J mindestens Absolutbetrag $(p-1)!$.

Behauptung 2: Es gilt

$$|J| \leq AC^p$$

mit zwei von p unabhängigen positiven reellen Zahlen A und C.

Beweis der Behauptung 2: Für $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ erhalten wir unter Verwendung von Lemma 3.1.5 die Gleichung[46]

$$\varphi(I) = \varphi\left(-\sum_{k=1}^{m}\sum_{j=0}^{mp-1}\widetilde{b}_k Q^{(j)}(\widetilde{\beta}_k)\right) = \sum_{k=1}^{m}\widetilde{b}_k I(\varphi(\widetilde{\beta}_k), Q^{(\varphi)}),$$

[46] In der zweiten Gleichung verwenden wir neben Lemma 3.1.5 zusätzlich, dass

$$\widetilde{b}_1 e^{\varphi(\widetilde{\beta}_1)} + \cdots + \widetilde{b}_m e^{\varphi(\widetilde{\beta}_m)} = 0.$$

Diese Stelle ist der Grund, wieso wir nicht mit der ursprünglichen Linearkombination

$$b_1 e^{\beta_1} + \cdots + b_1 e^{\beta_1}$$

arbeiten, sondern diese durch die Linearkombination

$$\widetilde{b}_1 e^{\varphi(\widetilde{\beta}_1)} + \cdots + \widetilde{b}_m e^{\varphi(\widetilde{\beta}_m)}$$

ersetzen.

wobei

$$Q^{(\varphi)} := N^{mp}(X - \varphi(\widetilde{\beta}_1))^{p-1} \prod_{i=2}^{m} (X - \varphi(\widetilde{\beta}_i))^p.$$

Nun können wir wie in den Sätzen von Hermite und Lindemann jedes einzelne Integral für $\varphi \in \mathrm{Gal}(K/\mathbb{Q})$ und $1 \leq k \leq n$ mit positiven Konstanten $A_{k,\varphi}$ und $C_{k,\varphi}$ wie folgt abschätzen:

$$|\varphi(I(\beta_k, Q))| \leq A_{k,\varphi} C_{k,\varphi}^p,$$

wobei die Konstanten $A_{k,\varphi}$ und $C_{k,\varphi}$ nur von k und $\widetilde{\beta}_1, \ldots, \widetilde{\beta}_m$ abhängen. Indem wir

$$C = \prod_{\varphi \in \mathrm{Gal}(K/\mathbb{Q})} \max_{1 \leq k \leq m} |C_{k,\varphi}| \text{ und } A = \prod_{\varphi \in \mathrm{Gal}(K/\mathbb{Q})} \sum_{k=1}^{m} |\widetilde{b}_k| |A_{k,\varphi}|$$

setzen, erhalten wir die Behauptung.

Für hinreichend großes p ergeben die Behauptungen 1 und 2 den Widerspruch

$$(p-1)! \leq |J| \leq AC^p.$$

□

Der Satz von Lindemann–Weierstraß[47]

[47] Zu diesem Abschnitt gibt es ein Video:

Im vorigen Abschnitt haben wir die lineare Unabhängigkeit von

$$e^{\beta_1}, \ldots, e^{\beta_n}$$

über $\mathbb{Q}$ gezeigt. Daraus folgern wir nun den Satz von Lindemann–Weierstraß:

Satz 3.4.8 (Lindemann–Weierstraß)**.** *Falls $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ algebraische Zahlen sind, die linear unabhängig über $\mathbb{Q}$ sind, so sind $e^{\alpha_1}, \ldots, e^{\alpha_n}$ algebraisch unabhängig über $\mathbb{Q}$.*

Beweis. Seien $\alpha_1, \ldots, \alpha_n$ komplexe algebraische Zahlen, sodass $e^{\alpha_1}, \ldots, e^{\alpha_n}$ algebraisch abhängig über $\mathbb{Q}$ sind. Unser Ziel ist es zu zeigen, dass die Zahlen $\alpha_1, \ldots, \alpha_n$ dann linear abhängig über $\mathbb{Q}$ sind. Da $e^{\alpha_1}, \ldots, e^{\alpha_n}$ algebraisch abhängig sind, gibt es ein von Null verschiedenes Polynom

$$Q = \sum_{(i_1,\ldots,i_n) \in \mathbb{N}_0^n} a_{i_1,\ldots,i_n} X^{i_1} \ldots X^{i_n}$$

mit $Q(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0$. Wegen der Multplikativität der Exponentialfunktion können wir diese Gleichung auch schreiben als:

$$\sum_{(i_1,\ldots,i_n) \in \mathbb{N}_0^n} a_{i_1,\ldots,i_n} e^{i_1\alpha_1 + \cdots + i_n\alpha_n} = 0.$$

Aus Proposition 3.4.7 folgt, dass nicht alle Exponenten $i_1\alpha_1 + \cdots + i_n\alpha_n$ verschieden sein können. Es gibt also $(i_1, \ldots, i_n) \neq (j_1, \ldots, j_n) \in \mathbb{N}_0^n$ mit

$$i_1\alpha_1 + \cdots + i_n\alpha_n = j_1\alpha_1 + \cdots + j_n\alpha_n.$$

Nun folgt aus der Gleichung

$$(i_1 - j_1)\alpha_1 + \cdots + (i_n - j_n)\alpha_n = 0$$

die lineare Abhängigkeit der Zahlen $\alpha_1, \ldots, \alpha_n$ über $\mathbb{Q}$. □

Korollar 3.4.9 (Hermite–Lindemann)**.** *Für $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$ ist e^α stets transzendent.*

Beweis. Das ist der Spezialfall $n = 1$ in Satz 3.4.8. □

Korollar 3.4.10. *Für $\alpha \in \overline{\mathbb{Q}} \setminus \{0, 1\}$ ist $\log \alpha$ transzendent.*

Beweis. Das ist die Negation der Aussage des vorigen Korollars. □

Wir erhalten auch die Sätze von Lindemann und Hermite als Spezialfälle:

Korollar 3.4.11 (Hermite)**.** *e ist transzendent.*

Beweis. Setze $\alpha = 1$ in Korollar 3.4.9. □

Korollar 3.4.12 (Lindemann)**.** *π ist transzendent.*

Beweis. Wäre π algebraisch, so auch $i\pi$. Wegen

$$e^{i\pi} = -1$$

erhielten wir einen Widerspruch zu Korollar 3.4.9. □

Ausblick und offene Fragen

Der Satz von Lindemann-Weierstraß liefert uns sehr starke Transzendenzaussagen über die Werte der Exponentialfunktion. Dennoch gibt es noch viel zu erforschen. Wir möchten zum Abschluss dieses Kapitels auf die Vermutung von Schanuel eingehen. Für komplexe Zahlen $\alpha_1, \ldots, \alpha_n$ bezeichnen wir mit $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ den kleinsten Teilkörper von $\mathbb{C}$, welcher $\alpha_1, \ldots, \alpha_n$ enthält.

Vermutung (Schanuel)**.** *Für komplexe Zahlen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, die linear unabhängig über $\mathbb{Q}$ sind, ist der Transzendenzgrad des Körpers*

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$$

mindestens n.

Die Vermutung von Schanuel besagt also, dass es in dem Körper

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$$

mindestens n algebraisch unabhängige Elemente gibt. Somit impliziert der Satz von Lindemann-Weierstraß diese Vermutung, falls $\alpha_1, \ldots, \alpha_n$ algebraische komplexe Zahlen sind. Auch der Spezialfall $n = 1$ folgt aus dem Satz von Lindemann–Weierstraß. Eine weitere Konsequenz der Vermutung von Schanuel, für $\alpha_1 = 1, \alpha_2 = i\pi$, wäre die algebraische Unabhängigkeit von e und π. Insbesondere würde daraus die Transzendenz der Zahlen $e + \pi$ und $e \cdot \pi$ folgen: Wäre $e + \pi$ bzw. $e \cdot \pi$ algebraisch, so wären

$$Q_1 = X_1 + X_2 - (e + \pi) \text{ bzw. } Q_2 = X_1 X_2 - e \cdot \pi$$

von Null verschiedene Polynome mit algebraischen Koeffizienten und $Q_1(e, \pi) = 0$ bzw. $Q_2(e, \pi) = 0$.Das stünde im Widerspruch zur algebraischen Unabhängigkeit von e und π.

Zum Schluß möchten wir auch noch den Satz von Gelfond–Schneider erwähnen:

Satz (Gelfond–Schneider)**.** *Für algebraische Zahlen α, β mit $\alpha \neq 0, 1$ und $\beta \notin \mathbb{Q}$ ist α^β transzendent.*

Indem man im Satz von Gelfond–Schneider die Zahlen

$$\alpha = e^{i\pi} = -1 \text{ und } \beta = -i\sqrt{163}$$

wählt, erhält man die Transzendenz der Ramanujan-Konstante

$$e^{\pi\sqrt{163}}.$$

Auf den ersten Blick sieht diese Zahl unscheinbar aus, allerdings liegt diese Zahl erstaunlich nahe an einer ganzen Zahl:

$$e^{\pi\sqrt{163}} = 262537412640768743,99999999999250072597...$$

Dass dies mehr als nur ein kurioser Zufall ist, werden wir in den Übungen genauer beleuchten.

r

4 Zeta-Werte

Die Riemannsche Zeta-Funktion ist eine der bedeutendsten Funktionen der Zahlentheorie. In diesem Abschnitt werden wir uns mit der Frage nach den Werten der Riemannschen Zeta-Funktion an den natürlichen Zahlen beschäftigen.

4.1 Die Eulersche Formel

Die Ursprünge des Studiums spezieller Werte der Riemannschen Zeta-Funktion geht zurück ins 17-te Jahrhundert. Im Jahre 1644 warf der italienische Mathematiker Pietro Mengoli die Frage nach dem Wert der Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n^2}$$

auf. Anfangs beschäftigten sich hauptsächlich Mathematiker der Stadt Basel mit der Lösung dieses Problems, worauf dieses unter dem Namen *Baseler Problem* bekannt wurde. Der Durchbruch gelang schließlich Leonhard Euler im Jahre 1735. Er zeigte nicht nur die Formel

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6},$$

sondern konnte auch die Werte der Reihen

$$\sum_{n=1}^{\infty} \frac{1}{n^{2k}}$$

für alle natürlichen Zahlen k explizit angeben. In diesem Abschnitt werden wir diese Eulerschen Formeln beweisen.

Die Riemannsche Zeta-Funktion[1]

Die *Riemannsche Zeta-Funktion* ist für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ wie folgt definiert:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Der Vollständigkeit halber halten wir die absolute Konvergenz der definierenden Reihe fest.

[1] Zu diesem Abschnitt gibt es ein Video:

Lemma 4.1.1. *Für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ konvergiert die Reihe*

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

absolut.

Beweis. Für $n \in \mathbb{N}$ und $s \in \mathbb{C}$ gilt[2]

$$|n^{-s}| = |n^{-\mathrm{Re}(s)}| \cdot \underbrace{|n^{-i\,\mathrm{Im}(s)}|}_{=1} = n^{-\mathrm{Re}(s)}.$$

Daher reicht es die Aussage für $s \in \mathbb{R}$ zu zeigen. Für $s \in \mathbb{R}_{>1}$ ist die Funktion

$$[1, \infty) \to \mathbb{R}, \quad x \mapsto x^{-s}$$

streng monoton fallend. Somit folgt die Konvergenz, nach dem Integral-Kriterium, aus der Konvergenz des Integrals

$$\int_1^{\infty} x^{-s} dx = \frac{1}{s-1}.$$

□

[2] Für reelle Zahlen x und y mit $x > 0$ gilt stets

$$|x^{iy}| = |e^{iy \log x}| = |\cos(y \log x) + i \sin(y \log x)| = 1.$$

Analytische Funktionen

Sei $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ und $f \colon U \to \mathbb{K}$ eine stetige Funktion auf einer offenen Teilmenge $U \subseteq \mathbb{K}$. Wir nennen f *analytisch in* $x_0 \in U$, wenn es eine Potenzreihe

$$\sum_{n=0}^{\infty} a_n (x - x_0)^n \tag{4.1}$$

gibt, die auf einer Umgebung von x_0 punktweise gegen $f(x)$ konvergiert. Eine Potenzreihe (4.1), welche f lokal bei x_0 darstellt, heißt Potenzreihenentwicklung von f bei x_0. Wir nennen f *analytisch*, wenn f in jedem Punkt aus U analytisch ist. Im Folgenden erinnern wir an die grundlegenden Eigenschaften analytischer Funktionen aus der Analysis:

Proposition 4.1.2 (Eindeutigkeit der Potenzreihenentwicklung)**.** *Ist*

$$f \colon U \to \mathbb{K}$$

analytisch in x_0 mit einer Potenzreihenentwicklung

$$f(x) = \sum_{n=0}^{\infty} a_n (x - x_0)^n, \tag{4.2}$$

so ist (4.2) die Taylor-Entwicklung der Funktion f in x_0. Insbesondere zeigt dies, dass die Potenzreihenentwicklung (4.2) eindeutig ist und dass die Koeffizienten dieser Potenzreihenentwicklung durch die Formel

$$a_n = \frac{f^{(n)}(x_0)}{n!}$$

gegeben sind.

Beweis. Siehe Vorlesung Analysis, oder §14.2 in Königsberger[3], „Analysis I". □

[3] K. Königsberger. *Analysis. 1.* Springer-Lehrbuch. [Springer Textbook]. Springer-Verlag, Berlin, 1995. ISBN 3-540-52006-6

Proposition 4.1.3. *Sind $f, g\colon U \to \mathbb{K}$ analytisch in x_0 mit*

$$f(x) = \sum_{n=0}^{\infty} a_n (x - x_0)^n, \quad g(x) = \sum_{n=0}^{\infty} b_n (x - x_0)^n,$$

so ist auch $f \cdot g$ analytisch[4] *mit Potenzreihenentwicklung*

$$(f \cdot g)(x) = \sum_{n=0}^{\infty} c_n (x - x_0)^n$$

und $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Falls f keine Nullstelle auf U besitzt, so ist auch $\frac{1}{f}$ analytisch in x_0.

[4] Da auch Summen und Differenzen analytischer Funktionen offensichtlich analytisch sind, folgt hieraus, dass die analytischen Funktionen auf U einen Ring bilden.

Beweis. Beweis siehe Vorlesung Analysis, oder §14.2 in Königsberger[5], „Analysis I". □

[5] K. Königsberger. *Analysis. 1.* Springer-Lehrbuch. [Springer Textbook]. Springer-Verlag, Berlin, 1995. ISBN 3-540-52006-6

Bernoulli-Zahlen

Die Bernoulli-Zahlen spielen eine entscheidende Rolle in der Eulerschen Formel für die Werte der Riemannschen Zeta-Funktion an den geraden natürlichen Zahlen. Wir definieren die Bernoulli-Zahlen mithilfe der Taylor-Entwicklung der Funktion $\frac{x}{e^x - 1}$.

Definition 4.1.4. Die Bernoulli-Zahlen $(B_n)_{n \geq 0}$ sind definiert als die Taylor-Koeffizienten[6] der Funktion

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} \tag{4.3}$$

an der Stelle $x = 0$.[7]

[6] Die Funktion $\frac{x}{e^x-1}\colon \mathbb{R} \to \mathbb{R}$ ist als Kehrwert der analytischen Funktion $\frac{e^x-1}{x}$ analytisch, siehe Proposition 4.1.3.

[7] Eine Potenzreihe der Form

$$f = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$$

wird häufig eine exponentiell erzeugende Funktion der Folge $(a_n)_{n \geq 0}$ genannt.

Proposition 4.1.5. *Die Bernoulli-Zahlen erfüllen die Gleichungen $B_0 = 1$ und für $n > 1$*

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0.$$

Beweis. Indem wir die Gleichung (4.3) mit $e^x - 1$ multiplizieren, erhalten wir

$$\begin{aligned} x = (e^x - 1) \sum_{i=0}^{\infty} B_i \frac{x^i}{i!} &= \left(\sum_{j=0}^{\infty} \frac{x^{j+1}}{(j+1)!} \right) \left(\sum_{i=0}^{\infty} B_i \frac{x^i}{i!} \right) \\ &= x \left(\sum_{j=0}^{\infty} \frac{x^j}{(j+1)!} \right) \left(\sum_{i=0}^{\infty} B_i \frac{x^i}{i!} \right). \end{aligned} \tag{4.4}$$

Die rechte Seite der Gleichung (4.4) ist nach Proposition 4.1.3 analytisch in $x = 0$ mit Reihenentwicklung

$$x = x \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{(n+1-k)!} \frac{B_k}{k!} x^n = \sum_{n=1}^{\infty} \sum_{k=0}^{n-1} \binom{n}{k} B_k \frac{x^n}{n!}. \tag{4.5}$$

Durch Koeffizientenvergleich[8] in (4.5) erhalten wir für $n = 1$

$$B_0 = 1$$

und für $n > 1$

$$0 = \sum_{k=0}^{n-1} \binom{n}{k} B_k.$$

□

[8] In (4.5) steht auf der linken und rechten Seite jeweils eine Potenzreihenentwicklungen der analytischen Funktion $x \mapsto x$. Nach Proposition 4.1.2 sind die Koeffizienten beider Potenzreihenentwicklungen gleich.

Proposition 4.1.5 liefert also die Gleichungen:

$$\begin{aligned}
1 &= B_0 \\
0 &= B_0 + 2B_1 \\
0 &= B_0 + 3B_1 + 3B_2 \\
0 &= B_0 + 4B_1 + 6B_2 + 4B_3 \\
0 &= B_0 + 5B_1 + 10B_2 + 10B_3 + 5B_4 \\
&\vdots
\end{aligned}$$

Diese Gleichungen erlauben es uns, die Bernoulli-Zahlen rekursiv zu berechnen:

$$\begin{aligned}
B_0 &= 1 \\
B_1 &= -\frac{1}{2} B_0 = -\frac{1}{2} \\
B_2 &= -\frac{1}{3}(B_0 + 3B_1) = \frac{1}{6} \\
B_3 &= -\frac{1}{4}(B_0 + 4B_1 + 6B_2) = 0 \\
B_4 &= -\frac{1}{5}(B_0 + 5B_1 + 10B_2 + 10B_3) = -\frac{1}{30} \\
&\vdots
\end{aligned}$$

Insbesondere folgt daraus die Rationalität der Bernoulli-Zahlen:

Korollar 4.1.6. *Alle Bernoulli-Zahlen sind rational.*

Beweis. Das folgt unmittelbar aus $B_0 = 1$ und der Rekursionsgleichung

$$B_n = -\frac{1}{n+1} \sum_{k=0}^{n-1} B_k \binom{n+1}{k}.$$

□

Wir bemerken noch, dass bis auf B_1 alle ungeraden Bernoulli-Zahlen verschwinden[9]:

Proposition 4.1.7. $B_{2n+1} = 0$ *für* $n \geq 1$.

[9] Tatsächlich sind alle übrigen Bernoulli-Zahlen ungleich Null, wie wir aus der Positivität der geraden Zeta-Werte gleich sehen werden.

Beweis. Wegen

$$\frac{x}{e^x-1} = B_0 + B_1 x + B_2 \frac{x^2}{2!} + \dots$$

ist die Behauptung äquivalent dazu, dass

$$x \mapsto \frac{x}{e^x-1} - B_1 x$$

eine gerade Funktion ist. Allerdings haben wir

$$\begin{aligned}\frac{x}{e^x-1} - B_1 x &= \frac{x}{e^x-1} + \frac{x}{2} \\ &= \frac{2x + x(e^x-1)}{2(e^x-1)} \\ &= \frac{x(e^x+1)}{2(e^x-1)}\end{aligned}$$

und somit nach Erweiterung des letzten Bruchs mit $e^{-x/2}$

$$\frac{x}{e^x-1} - B_1 x = \frac{x}{2}\frac{e^{x/2}+e^{-x/2}}{e^{x/2}-e^{-x/2}}. \tag{4.6}$$

Die folgende direkte Rechnung zeigt schließlich, dass $g(x) := \frac{x}{e^x-1} - B_1 x$ eine gerade Funktion ist:

$$g(-x) = \frac{-x}{2}\frac{e^{-x/2}+e^{x/2}}{e^{-x/2}-e^{x/2}} = \frac{x}{2}\frac{e^{x/2}+e^{-x/2}}{e^{x/2}-e^{-x/2}} = g(x).$$

Somit ist die Behauptung $B_{2n+1} = 0$ für $n \geq 1$ gezeigt. □

Die Rechnungen im Beweis der Proposition 4.1.7 zeigen die folgende Formel für die Taylor-Entwicklung bei $x = 0$ des Kotangens[10]:

$$\cot x = \frac{\cos x}{\sin x} = i\frac{e^{ix}+e^{-ix}}{e^{ix}-e^{-ix}}$$

Korollar 4.1.8. *Die Funktion $x \mapsto x\cot x$, definiert auf $(-\pi,\pi)$, besitzt an der Stelle $x = 0$ die Taylor-Entwicklung*[11]

$$x\cot x = \sum_{n=0}^{\infty} (-4)^n B_{2n} \frac{x^{2n}}{(2n)!}.$$

Beweis. In (4.6) haben wir für die Funktion $g(x) := \frac{x}{e^x-1} - B_1 x$ die Formel

$$g(x) = \frac{x}{2}\frac{e^{x/2}+e^{-x/2}}{e^{x/2}-e^{-x/2}}$$

gezeigt. Daher gilt für $x \in (-\pi/2, \pi/2)$ die Gleichung

$$x\cot x = ix\frac{e^{ix}+e^{-ix}}{e^{ix}-e^{-ix}} = g(2ix).$$

[10] Wir erinnern an dieser Stelle an die Definition von Sinus und Kosinus für komplexe Argumente:

$$\sin(x) := \frac{e^{ix}-e^{-ix}}{2i}, \quad \cos(x) := \frac{e^{ix}+e^{-ix}}{2}.$$

[11] Die Funktion $x \mapsto \frac{\sin x}{x}$ hat in $(-\pi,\pi)$ keine Nullstellen und ist in $x = 0$ analytisch. Somit ist

$$x \mapsto x\cot x = \cos x \cdot \left(\frac{\sin x}{x}\right)^{-1}$$

eine wohldefinierte stetige Funktion auf $(-\pi,\pi)$. Nach Proposition 4.1.3 ist $x \mapsto x\cot x$ analytisch in $x = 0$.

Andererseits besitzt die analytische Funktion g an der Stelle $x = 0$ die Potenzreihenentwicklung

$$g(x) := \frac{x}{e^x - 1} - B_1 x = \sum_{n=0}^{\infty} B_{2n} \frac{x^{2n}}{(2n)!}.$$

Somit erhalten wir für $x \mapsto g(2ix)$ die Potenzreihenentwicklung bei $x = 0$

$$g(2ix) = \sum_{n=0}^{\infty} B_{2n} \frac{(2ix)^{2n}}{(2n)!} = \sum_{n=0}^{\infty} (-4)^n B_{2n} \frac{x^{2n}}{(2n)!}.$$

Wir haben insgesamt also die Potenzreihenentwicklung

$$x \cot x = \sum_{n=0}^{\infty} (-4)^n B_{2n} \frac{x^{2n}}{(2n)!}$$

an der Stelle $x = 0$ gefunden. Nach Proposition 4.1.2 ist diese Reihe notwendigerweise die Taylor-Entwicklung. □

Die Eulersche Formel[12]

[12] Zu diesem Abschnitt gibt es ein Video:

Wir möchten nun die auf Euler zurückgehende Formel für $\zeta(2k)$ mit $k \in \mathbb{N}$ beweisen. Dafür benötigen wir noch die „Partialbruchentwicklung des Kotangens".

Proposition 4.1.9. *Für $x \in (-\pi, \pi)$ gilt*

$$x \cot x = 1 - 2 \sum_{k=1}^{\infty} \frac{x^2}{k^2\pi^2 - x^2}.$$

Beweis. Wir zeigen diese Reihenentwicklung auf Übungsblatt 11. □

Satz 4.1.10 (Euler, 1735)**.** *Für $n \geq 1$ gilt die Formel*[13]

$$\zeta(2n) = -\frac{(2\pi i)^{2n}}{2 \cdot (2n)!} B_{2n}.$$

Beweis. Für $x \in (-\pi, \pi)$ starten wir mit der Partialbruchentwicklung des Kotangens

$$x \cot x = 1 - 2 \sum_{k=1}^{\infty} \frac{x^2}{k^2\pi^2 - x^2}.$$

Nun entwickeln wir jeden Summanden mit Hilfe der geometrischen Reihe,

$$\frac{x^2}{k^2\pi^2 - x^2} = \left(\frac{x}{k\pi}\right)^2 \frac{1}{1 - \left(\frac{x}{k\pi}\right)^2} = \sum_{n=1}^{\infty} \left(\frac{x}{k\pi}\right)^{2n},$$

und erhalten[14]

[13] Selbstverständlich könnte man diese Formel auch in der Form

$$\zeta(2n) = (-1)^{n-1} \frac{(2\pi)^{2n}}{2(2n)!} B_{2n}$$

schreiben. Man *könnte*, **sollte** man aber nicht. Sie erinnern sich sicherlich noch an den Merkspruch

> „Trenne nie $2\pi i$, denn es tut ihm weh."

aus Ihrer Grundschulzeit ;-). Nein, Spaß beiseite, aber tatsächlich zeigt die Eulersche Formel einen einfachen Spezialfall einer tiefliegenden Vermutung der arithmetischen Geometrie – der Deligne Vermutung. Im Falle der Riemannschen Zeta-Funktion besagt diese Vermutung im Wesentlichen, dass $\zeta(2n)$ ein rationales Vielfaches der Periode $(2\pi i)^{2n}$ ist.

[14] Wir dürfen hier im zweiten Schritt wegen absoluter Konvergenz die Reihenfolge der Summation vertauschen.

$$x\cot x = 1 - 2\sum_{k=1}^{\infty}\sum_{n=1}^{\infty}\left(\frac{x}{k\pi}\right)^{2n}$$
$$= 1 - 2\sum_{n=1}^{\infty}\underbrace{\sum_{k=1}^{\infty}\frac{1}{k^{2n}}}_{=\zeta(2n)}\frac{x^{2n}}{\pi^{2n}} = 1 - 2\sum_{n=1}^{\infty}\frac{\zeta(2n)}{\pi^{2n}}x^{2n}. \quad (4.7)$$

Andererseits haben wir in Korollar 4.1.8 die Taylorentwicklung des Kotangens mit den Bernoulli-Zahlen in Verbindung gebracht

$$x\cot x = \sum_{n=0}^{\infty}(-4)^n B_{2n}\frac{x^{2n}}{(2n)!}. \quad (4.8)$$

Durch Koeffizientenvergleich[15] der beiden Reihen (4.7) und (4.8) erhalten wir für jede natürliche Zahl n die Gleichung

$$-2\frac{1}{\pi^{2n}}\zeta(2n) = (-4)^n B_{2n}\frac{1}{(2n)!}.$$

Umstellen dieser Gleichung liefert nun wie gewünscht

$$\zeta(2n) = -\frac{(2\pi i)^{2n}}{2\cdot(2n)!}B_{2n}.$$

□

[15] Wieder haben wir zwei Potenzreihenentwicklungen an der Stelle $x = 0$ einer analytischen Funktion. Aus Proposition 4.1.2 folgt, dass die Koeffizienten der Potenzreihen übereinstimmen.

Damit wir nicht vergessen, dass wir uns hier in einem Skript zur transzendenten Zahlentheorie befinden, bemerken wir an dieser Stelle, dass die Eulersche Formel zusammen mit Lindemanns Beweis die Transzendenz aller Werte der Riemannschen Zeta-Funktion an geraden natürlichen Zahlen zeigt:

Korollar 4.1.11. *Für $n \geq 1$ ist $\zeta(2n)$ transzendent.*

Beweis. Wegen

$$\zeta(2n) = \sum_{k=1}^{\infty}\frac{1}{k^{2n}}$$

ist $\zeta(2n)$ eine strikt positive reelle Zahl und somit nicht Null. Aus der Transzendenz von π folgt die Transzendenz von π^{2n} und damit auch die Transzendenz aller von Null verschiedener rationaler Vielfachen von π^{2n}. □

Ausblick und offene Fragen

In diesem Abschnitt haben wir nur die nötigsten Eigenschaften der Riemannschen Zeta-Funktion eingeführt. Es ist nicht schwer zu zeigen, dass die Riemannsche Zeta-Funktion für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ eine Produktentwicklung[16]

$$\zeta(s) = \prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}} = \prod_{p\in\mathbb{P}}\left(1 + p^{-s} + p^{-2s} + \dots\right)$$

[16] Für Details verweisen wir auf Übungsblatt 12.

besitzt. Wenn wir an dieser Stelle mal kurz die Frage nach der Konvergenz ausblenden, dann folgt diese Produktentwicklung indem wir die rechte Seite ausmultiplizieren und beachten, dass sich jede natürliche Zahl n eindeutig in der Form

$$n = \prod_{p \in \mathbb{P}} p^{\alpha_p}$$

mit $\alpha_p \in \mathbb{N}_0$ und $\alpha_p = 0$ für fast alle $p \in \mathbb{P}$ schreiben lässt. Im Wesentlichen encodiert die Produktdarstellung also die eindeutige Primfaktorzerlegung der ganzen Zahlen. Die Tatsache, dass die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

für $s \to 1$ divergiert, zeigt gemeinsam mit der Produktformel, dass es unendlich viele Primzahlen gibt: Gäbe es nur endlich viele Primzahlen, so würde der Grenzwert

$$\lim_{s \to 1} \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p}}$$

für $s \to 1$ existieren, denn es ist ein endliches Produkt. Tatsächlich gibt es einen viel tieferen Zusammenhang zwischen der Verteilung der Primzahlen und der Riemannschen Zeta-Funktion. Dazu müssen wir allerdings etwas ausholen: Wir haben die Riemannsche Zeta-Funktion bisher nur für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ definiert. Allerdings lässt sich zeigen, dass sich die Riemannsche Zeta-Funktion auf eindeutige Weise zu einer komplex differenzierbaren Funktion

$$\zeta \colon \mathbb{C} \setminus \{1\} \to \mathbb{C}$$

fortsetzen lässt. Man kann zeigen, dass die Riemannsche Zeta-Funktion auf der Halbebene

$$\{s \in \mathbb{C} : \mathrm{Re}(s) \geq 1\}$$

keine Nullstellen besitzt. Diese Tatsache liefert nun erstaunliche Aussagen über die Verteilung der Primzahlen:[17]

[17] Obwohl wir den Primzahlsatz in dieser Vorlesung nicht beweisen werden, wird er uns im Laufe dieses Skripts noch einmal begegnen.

Satz 4.1.12. *[Primzahlsatz] Für $x \in \mathbb{R}$ schreiben wir*

$$\pi(x) := |\{p \in \mathbb{P} : p \leq x\}|$$

für die Anzahl der Primzahlen $\leq x$. Dann gilt

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Beweis. Wir werden den Primzahlsatz hier aus Zeitgründen nicht beweisen können[18]. Interessierte Leser*innen verweisen wir auf Kapitel 7 §3 im Buch „Einführung in die Zahlentheorie“ von P. Bundschuh[19]. □

[18] Allerdings werden wir im Übungsbetrieb untere und obere Schranken für $\frac{\pi(x)}{\frac{x}{\log x}}$ herleiten.

[19] P. Bundschuh. *Einführung in die Zahlentheorie*. Springer-Lehrbuch. [Springer Textbook]. Springer-Verlag, Berlin, second edition, 1992. ISBN 3-540-55178-6

Der Primzahlsatz besagt also, dass es asymptotisch etwa $\frac{x}{\log x}$ viele Primzahlen $\leq x$ gibt. Nun fiel Riemann auf, dass man eine starke Verbesserung des Primzahlsatzes erhalten würde, wenn man eine stärkere Aussage über die nullstellenfreien Regionen der Riemannschen Zeta-Funktion zeigen könnte. Dies führte ihn auf die berühmte

Vermutung (Riemannsche Vermutung)**.** *Alle Nullstellen der Riemannschen Zeta-Funktion auf dem* kritischen Streifen

$$\{s \in \mathbb{C} : 0 < \mathrm{Re}(s) < 1\}$$

befinden sich auf der Geraden $\{s \in \mathbb{C} : \mathrm{Re}(s) = \frac{1}{2}\}$.

Wir möchten noch kurz erklären, wie der kritische Streifen zu seinem Namen kommt: Man kann zeigen, dass die Riemannsche Zeta-Funktion eine wunderschöne Symmetrie besitzt. Die Riemannsche Zeta-Funktion erfüllt für alle $s \in \mathbb{C} \setminus \{1\}$ die Funktionalgleichung

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right) \cdot \zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s),$$

mit der Gamma-Funktion $\Gamma(s) := \int_0^\infty t^{s-1}e^{-t}dt$. Diese Funktionalgleichung setzt die Werte der Riemannschen Zeta-Funktion für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ mit den Werten $\mathrm{Re}(s) < 0$ in Beziehung. Da wir wissen, dass es keine Nullstellen mit $\mathrm{Re}(s) \geq 1$ gibt, kennen wir dank der Funktionalgleichung auch alle Nullstellen mit $\mathrm{Re}(s) \leq 0$. Der einzige Streifen, auf dem wir die Nullstellen nicht verstehen ist somit der Streifen $0 < \mathrm{Re}(s) < 1$. Dies erklärt die Bezeichnung *kritischer Streifen*.

Zuletzt möchte ich noch kurz auf die Werte der Riemannschen Zeta-Funktion an den negativen ganzen Zahlen eingehen. Dank der Funktionalgleichung folgern wir aus dem Eulerschen Satz[20]

$$\zeta(1-n) = -\frac{B_n}{n}.$$

[20] Details dazu werden wir auf dem Übungsblatt 11 sehen.

Bitte nehmen Sie sich ein paar Sekunden Zeit um über diese Formel zu staunen:

- Im Gegensatz zur Eulerschen Formel gilt diese Formel für *alle* negativen ganzen Zahlen.
- Der Grund, wieso uns die Funktionalgleichung dennoch nur etwas über die geraden positiven Zahlen sagt, ist, dass die Vorfaktoren der Funktionalgleichung an den geraden negativen Werten einen Pol haben.
- Die Formel an den negativen Werten ist viel einfacher!
- Wir haben den Definitionsbereich der Riemannsche Zeta-Funktion durch einen komplizierten analytischen Fortsetzungsprozess von

$\{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$ auf die punktierte komplexe Ebene $\mathbb{C} \setminus \{1\}$ erweitert. Auf den ersten Blick würde man nun beim Auswerten der Riemannschen Zeta-Funktion an den negativen ganzen Zahlen *jeden* Wert erwarten, aber sicherlich keinen rationalen. Umso erstaunlicher ist es, dass sogar alle Werte an negativen ganzen Zahlen rational sind.[21]

[21] Ein noch größeres Wunder ist, dass diese Zahlen auch noch schöne Kongruenzen erfüllen, wenn man sie modulo Primzahlpotenzen betrachtet. Und ein noch noch noch viel größeres Wunder ist, dass die negativen Zeta-Werte tiefliegende arithmetische Informationen enthalten. Die Tatsache, dass der Ring

$$\mathbb{Z}[X]/(X^{690} + X^{659} + \cdots + X^2 + X + 1)$$

kein Hauptidealring ist, lässt sich in gewisser Weise durch $\zeta(-11) = \frac{691}{32760}$ erklären. Aber das würde an dieser Stelle viel zu weit führen.

4.2 *A proof that Euler missed*

Die Eulersche Formel

$$\zeta(2n) = -\frac{(2\pi i)^{2n}}{2 \cdot (2n)!} B_{2n}.$$

wirft unmittelbar die Frage nach den Werten der Riemannschen Zeta-Funktion an den ungeraden natürlichen Zahlen auf. Diese Frage ist ungemein schwieriger. Zwar geht man davon aus, dass jede der Zahlen

$$\zeta(3), \zeta(5), \ldots$$

transzendent ist, aber bisher konnte die Transzendenz für keine einzige der Zahlen

$$\zeta(2n+1) \quad \text{für } n \geq 1$$

nachgewiesen werden. Apérys Beweis der Irrationalität von $\zeta(3)$ im Jahre 1979 war eine mathematische Sensation. So wird zum Besipiel dem berühmten Mathematiker Carl Ludwig Siegel das folgende Zitat zu Apérys Beweis zugeschrieben:

„Man kann diesen Beweis nur wie einen Kristall vor sich her tragen."

Noch erstaunlicher ist, dass Apérys Beweis ziemlich elementar ist. Das folgende Zitat des Mathematikers van der Poorten bringt das schön auf den Punkt:

„A proof that Euler missed..."

Bis heute ist $\zeta(3)$ die einzige der Zahlen

$$\zeta(2n+1) \quad \text{für } n \geq 1$$

für welche die Irrationalität bewiesen wurde. In dieser Vorlesung möchten wir uns mit einem Beweis des Satzes von Apéry beschäftigen, der auf Frits Beukers zurück geht.

Abschätzung für kgV$(1, \ldots, n)$

In den folgenden Irrationalitätsbeweisen werden die Zahlen

$$d_n := \mathrm{kgV}(1, \ldots, n)$$

eine wesentliche Rolle spielen. Insbesondere benötigen wir eine Aussage über das Wachstum der Zahlenfolge $(d_n)_{n\geq 1}$. Die folgende Abschätzung kann man aus dem Primzahlsatz, Satz 4.1.12, folgern.

Proposition 4.2.1. *Für alle hinreichend großen natürlichen Zahlen n gilt*[22]

$$d_n \leq 3^n.$$

Beweis. Siehe Aufgabe 2 auf Blatt 11. □

[22] Tatsächlich kann man sogar zeigen, dass

$$\lim_{n\to\infty} \frac{d_n}{e^n} = 1$$

gilt.

Der Satz von Apéry[23]

[23] Zu diesem Abschnitt gibt es ein Video:

Die Idee des Satzes von Apéry ist leicht erklärt. Wir konstruieren zwei Folgen $(A_n)_{n\geq 0}$ und $(B_n)_{n\geq 0}$ ganzer Zahlen mit der Eigenschaft[24]

$$0 < |A_n + B_n\zeta(3)| \to 0 \text{ für } n \to \infty.$$

Wäre $\zeta(3) = \frac{a}{b}$ eine rationale Zahl, so wäre

$$(|bA_n + aB_n|)_{n\geq 0}$$

eine von Null verschiedene Folge ganzer Zahlen, die gegen Null konvergiert – ein Widerspruch.

[24] Wir können die folgende Gleichung auch wie folgt interpretieren: Die Folge $(\frac{A_n}{B_n})$ rationaler Zahlen approximieren $\zeta(3)$ sehr gut. Die Idee Irrationalität oder Transzendenz reeller Zahlen durch rationale Approximationen zu zeigen kennen wir bereits aus den ersten Kapiteln der Vorlesung.

Für die Konstruktion der Zahlenfolgen $(A_n)_{n\geq 0}$ und $(B_n)_{n\geq 0}$ benötigen wir das folgende Lemma:

Proposition 4.2.2. *Für $r, s \in \mathbb{N}_0$ betrachten wir das Integral*

$$I_{r,s} := \int_0^1 \int_0^1 -\frac{\log(xy)}{1-xy} x^r y^s dxdy.$$

(a) Für $r > s$ gilt[25]

$$d_r^3 \cdot I_{r,s} \in \mathbb{Z}.$$

Hierbei erinnern wir an die Definition $d_r = kgV(1, \ldots, r)$.

(b) Für $r = s$ haben wir

$$I_{r,r} = 2\left(\zeta(3) - \sum_{k=1}^{r} \frac{1}{k^3}\right).$$

Insbesondere gilt $d_r^3 I_{r,r} \in \mathbb{Z} + \zeta(3)\mathbb{Z}$.

[25] Wir bemerken an dieser Stelle, dass $I_{r,s} = I_{s,r}$ somit können wir zur Berechnung von $I_{r,s}$ ohne Einschränkung stets $r \geq s$ annehmen.

Beweis. Durch partielle Integration sehen wir für $k \geq 0$, dass

$$\begin{aligned}\int_0^1 \log(x)x^{r+k}dx &= \lim_{\epsilon\to 0}\int_\epsilon^1 \log(x)x^{r+k}dx \qquad (4.9)\\ &= \frac{1}{r+k+1}\lim_{\epsilon\to 0}\left([x^{r+k+1}\log(x)]_\epsilon^1 - \int_\epsilon^1 \frac{1}{x}\cdot x^{r+k+1}dx\right)\\ &= \frac{-1}{(r+k+1)^2}.\end{aligned}$$

Unter Verwendung der Gleichungskette (4.9) und der geometrischen Reihe erhalten wir nun

$$\begin{aligned} I_{r,s} &= \int_0^1 \int_0^1 -\frac{\log(xy)}{1-xy} x^r y^s dx dy \\ &= -\int_0^1 \left(\sum_{k=0}^{\infty} \int_0^1 \log(xy) x^{r+k} y^{s+k} dx \right) dy \\ &= -\int_0^1 \left(\sum_{k=0}^{\infty} \log(y) y^{s+k} \int_0^1 x^{r+k} dx \right) dy + y^{s+k} \int_0^1 \log(x) x^{r+k} dx \\ &= -\sum_{k=0}^{\infty} \int_0^1 \left(\frac{y^{s+k} \log y}{r+k+1} - \frac{y^{s+k}}{(r+k+1)^2} \right) dy. \end{aligned}$$

Indem wir nun (4.9) auf das erste der beiden Integrale anwenden, erhalten wir

$$I_{r,s} = \sum_{k=0}^{\infty} \left(\frac{1}{(r+k+1)(s+k+1)^2} + \frac{1}{(r+k+1)^2(s+k+1)} \right). \quad (4.10)$$

a) Für $r > s$ können wir die Terme auf der rechte Seite von (4.10) wie folgt umformen

$$\begin{aligned} &\frac{1}{(r+k+1)(s+k+1)^2} + \frac{1}{(r+k+1)^2(s+k+1)} \\ &= \frac{1}{(r+k+1)(s+k+1)} \left(\frac{1}{s+k+1} + \frac{1}{r+k+1} \right) \\ &= \frac{1}{r-s} \frac{(r+k+1)-(s+k+1)}{(r+k+1)(s+k+1)} \left(\frac{1}{s+k+1} + \frac{1}{r+k+1} \right) \\ &= \frac{1}{r-s} \left(\frac{1}{s+k+1} - \frac{1}{r+k+1} \right) \left(\frac{1}{s+k+1} + \frac{1}{r+k+1} \right) \\ &= \frac{1}{r-s} \left(\frac{1}{(s+k+1)^2} - \frac{1}{(r+k+1)^2} \right). \end{aligned}$$

Setzen wir dies in Gleichung (4.10) ein, so erhalten wir

$$I_{r,s} = \sum_{k=0}^{\infty} \frac{1}{r-s} \left(\frac{1}{(s+k+1)^2} - \frac{1}{(r+k+1)^2} \right) = \frac{1}{r-s} \sum_{k=1}^{r-s} \frac{1}{(s+k)^2}.$$

Für $1 \leq k \leq r-s$ ist $s+k$ in der Menge $\{1, \dots, r\}$ enthalten. Somit ist $\mathrm{kgV}(1, \dots, r)$ ein Vielfaches von $s+k$, also

$$d_r^2 \frac{1}{(s+k)^2} \in \mathbb{Z}.$$

Da auch $1 \leq r-s \leq r$ gilt, erhalten wir ebenfalls

$$d_r \frac{1}{r-s} \in \mathbb{Z}.$$

Insgesamt also

$$d_r^3 I_{r,s} = \frac{d_r}{r-s} \sum_{k=1}^{r-s} \frac{d_r^2}{(s+k)^2} \in \mathbb{Z}.$$

(b) Für $r = s$ können wir (4.10) schreiben als

$$I_{r,r} = 2\sum_{k=0}^{\infty}\left(\frac{1}{(r+k+1)^3}\right) = 2\left(\sum_{k=1}^{\infty}\frac{1}{k^3} - \sum_{k=1}^{r}\frac{1}{k^3}\right) = 2\left(\zeta(3) - \sum_{k=1}^{r}\frac{1}{k^3}\right).$$

Da k^3 stets ein Teiler von d_r^3 ist, folgt auch die Behauptung über die Ganzzahligkeit der Linearkombination. □

Für $n \in \mathbb{N}$ definieren wir das Polynom $Q_n := X^n(1-X)^n$ und setzen

$$P_n := \frac{1}{n!}Q_n^{(n)}.$$

Wir bemerken, dass P_n ein Polynom vom Grad n ist. Nach Lemma 3.1.2 hat dieses Polynom ganzzahlige Koeffizienten.

Korollar 4.2.3. *Es existieren Folgen ganzer Zahlen $(A_n)_{n\in\mathbb{N}}$ und $(B_n)_{n\in\mathbb{N}}$ mit der Eigenschaft*

$$d_n^3\int_0^1\int_0^1 -\frac{\log(xy)}{1-xy}P_n(x)P_n(y)dxdx = A_n + B_n\zeta(3).$$

Beweis. Wir definieren die ganzen Zahlen $a_{r,s}$ für $0 \le r, s \le n$ indem wir das Polynom $P_n(X)P_n(Y) \in \mathbb{Z}[X,Y]$ ausmutliplizieren:

$$P_n(X)P_n(Y) = \sum_{r=0}^{n}\sum_{s=0}^{n}a_{r,s}X^rY^s.$$

Wir definieren nun

$$B_n := d_n^3 \cdot 2 \cdot (a_{0,0} + a_{1,1} + \cdots + a_{n,n})$$

und

$$A_n := d_n^3\left(\sum_{0\le s<r\le n} 2a_{r,s}I_{r,s}\right) - 2\sum_{r=1}^{n}a_{r,r}\sum_{k=1}^{r}\frac{d_n^3}{k^3}.$$

Wir bemerken, dass A_n und B_n ganze Zahlen sind. Aus Proposition 4.2.2 folgt:

$$d_n^3\int_0^1\int_0^1 -\frac{\log(xy)}{1-xy}P_n(x)P_n(y)dxdx = A_n + B_n\zeta(3).$$

□

Wir können nun die Irrationalität von $\zeta(3)$ beweisen:

Satz 4.2.4 (Apéry)**.** *Die Zahl $\zeta(3)$ ist irrational.*

Beweis. Wir haben bereits für jedes $n \in \mathbb{N}$ ganze Zahlen A_n und B_n mit der Eigenschaft

$$d_n^3 \int_0^1 \int_0^1 -\frac{\log(xy)}{1-xy} P_n(x)P_n(y)dxdx = A_n + B_n\zeta(3)$$

konstuiert. Wir möchten nun zeigen, dass

$$0 < |A_n + B_n\zeta(3)| \to 0 \text{ mit } n \to \infty$$

gilt. Um das Integral abzuschätzen, ist folgende Umformung nützlich:

Behauptung: Es gilt

$$\int_0^1 \int_0^1 -\frac{\log(xy)}{1-xy} P_n(x)P_n(y)dxdy = \int_0^1 \int_0^1 \int_0^1 \frac{Q_n(u)Q_n(v)Q_n(w)}{(1-(1-uv)w)^{n+1}}$$

mit $Q_n(x) = x^n(1-x)^n$.
Beweis der Behauptung: Wir erinnern zunächst an

$$P_n = \frac{1}{n!}Q_n^{(n)}.$$

Da Q_n jeweils eine Nullstelle der Ordnung n bei 0 und 1 hat gilt

$$Q_n^{(k)}(0) = Q_n^{(k)}(1) = 0$$

für $0 \leq k \leq n-1$. Wir bemerken zunächst für $x, y \in [0,1]$ die Integralformel[26]

$$\int_0^1 \frac{P_n(x)P_n(y)}{1-(1-xy)z}dz = -\frac{\log(xy)}{1-xy}P_n(x)P_n(y)$$

[26] Man bemerke, dass $-\frac{\log(1-\alpha z)}{\alpha}$ eine Stammfunktion für $\frac{1}{1-\alpha z}$ ist und setze $\alpha = 1-xy$.

Unter Verwendung dieser Formel erhalten wir durch wiederholte partielle Integration bezüglich der Variablen x, dass

$$\begin{aligned}
&\int_0^1 \int_0^1 -\frac{\log(xy)}{1-xy} P_n(x)P_n(y)dxdy \\
&= \int_0^1 \int_0^1 \int_0^1 \frac{P_n(x)P_n(y)}{1-(1-xy)z}dxdydz \\
&= \frac{1}{n!}\int_0^1 \int_0^1 \int_0^1 P_n(y)\frac{Q_n^{(n)}(x)}{1-(1-xy)z}dxdydz \\
&= \frac{1}{n!}\int_0^1 \int_0^1 \int_0^1 P_n(y)yz\frac{Q_n^{(n-1)}(x)}{(1-(1-xy)z)^2}dxdydz \\
&= \frac{1}{n!}\int_0^1 \int_0^1 \int_0^1 P_n(y)2(yz)^2\frac{Q_n^{(n-2)}(x)}{(1-(1-xy)z)^3}dxdydz \\
&= \dots \\
&= \frac{1}{n!}\int_0^1 \int_0^1 \int_0^1 P_n(y)n!(yz)^n\frac{Q_n(x)}{(1-(1-xy)z)^{n+1}}dxdydz \\
&= \int_0^1 \int_0^1 \int_0^1 P_n(y)(yz)^n\frac{Q_n(x)}{(1-(1-xy)z)^{n+1}}dxdydz.
\end{aligned}$$

Für jedes $x, y \in [0,1]$ definiert die Abbildung

$$z \mapsto \frac{1-z}{1-(1-xy)z}$$

einen selbstinversen Diffeomorphismus[27] $[0,1] \xrightarrow{\sim} [0,1]$. Entsprechend führt die Variablensubstitution

[27] Ein Diffeomorphismus ist eine stetig differenzierbare bijektive Abbildung, deren Inverses wieder stetig differnzierbar ist.

$$\begin{aligned} x &:= u \\ y &:= v \\ z &:= \frac{1-w}{1-(1-uv)w}. \end{aligned}$$

im Integranden der obigen Formel zu

$$\begin{aligned} &P_n(y)(yz)^n \frac{Q_n(x)}{(1-(1-xy)z)^{n+1}} \\ &\quad = P_n(v)v^n \left(\frac{1-w}{(1-(1-uv)w)}\right)^n \frac{u^n(1-u)^n}{\left(1-\left(\frac{(1-uv)(1-w)}{1-(1-uv)w}\right)\right)^{n+1}} \\ &\quad = P_n(v)(1-u)^n(1-w)^n \frac{(1-(1-uv)w)}{uv}. \end{aligned}$$

Die obige Variablensubstitution ergibt somit

$$\begin{aligned} &\int_0^1 \int_0^1 -\frac{\log(xy)}{1-xy} P_n(x)P_n(y)dxdy \\ &= \int_0^1 \int_0^1 \int_0^1 P_n(v)(1-u)^n(1-w)^n \frac{(1-(1-uv)w)}{uv} \frac{uv}{(1-(1-uv)w)^2} dudvdw \\ &= \int_0^1 \int_0^1 \int_0^1 (1-u)^n(1-w)^n \frac{P_n(v)}{(1-(1-uv)w)} dudvdw, \end{aligned}$$

wobei der Term $\frac{uv}{(1-(1-uv)w)^2}$ aus der Transformationsformel kommt. Abermalige n-fache partielle Integration bezüglich v führt schließlich zur gewünschten Formel:

$$\begin{aligned} &\int_0^1 \int_0^1 \int_0^1 (1-u)^n(1-w)^n \frac{P_n(v)}{(1-(1-uv)w)} dudvdw \\ &= \int_0^1 \int_0^1 \int_0^1 (uvw)^n(1-u)^n(1-w)^n(1-v)^n \frac{1}{(1-(1-uv)w)^{n+1}} dudvdw \\ &= \int_0^1 \int_0^1 \int_0^1 Q_n(u)Q_n(v)Q_n(w) \frac{1}{(1-(1-uv)w)^{n+1}} dudvdw. \end{aligned}$$

Dies zeigt die Behauptung.

Wir möchten nun eine Abschätzung für das Integral

$$\int_0^1 \int_0^1 \int_0^1 \frac{Q_n(u)Q_n(v)Q_n(w)}{(1-(1-uv)w)^{n+1}} dudvdw \tag{4.11}$$

zeigen. Da der Integrand auf dem Inneren des Würfels $[0,1]^3$ strikt positiv ist, gilt

$$0 < \int_0^1 \int_0^1 \int_0^1 \frac{Q_n(u)Q_n(v)Q_n(w)}{(1-(1-uv)w)^{n+1}}.$$

Andererseits zeigt eine einfache Kurvendiskusion die Abschätzung

$$\frac{u(1-u)v(1-v)w(1-w)}{1-(1-uv)w} \leq (\sqrt{2}-1)^4 \text{ für } 0 \leq u,v,w \leq 1.$$

Wir erhalten für das Integral (4.11) also die obere Schranke

$$\begin{aligned}\int_0^1 \int_0^1 \int_0^1 &\frac{Q_n(u)Q_n(v)Q_n(w)}{(1-(1-uv)w)^{n+1}} dudvdw \\ &\leq (\sqrt{2}-1)^{4n} \int_0^1 \int_0^1 \int_0^1 \frac{1}{(1-(1-uv)w)} dudvdw \\ &= (\sqrt{2}-1)^{4n} \int_0^1 \int_0^1 -\frac{\log(uv)}{1-uv} dudv = (\sqrt{2}-1)^{4n} 2\zeta(3).\end{aligned}$$

Mit Korollar 4.2.3 und der obigen Behauptung erhalten wir somit

$$0 < |A_n + B_n\zeta(3)| \leq d_n^3(\sqrt{2}-1)^{4n}2\zeta(3).$$

Aus Proposition 4.2.1 folgt wegen $3^3 \cdot (\sqrt{2}-1)^4 \approx 0{,}79 < 1$ nun, dass die rechte Seite für $n \to \infty$ gegen 0 konvergiert. Wäre $\zeta(3) = \frac{a}{b}$ rational, so wäre

$$0 < |bA_n + B_n a| \to 0 \text{ für } n \to \infty$$

eine von Null verschiedene gegen Null konvergente Folge ganzer Zahlen – ein Widerspruch. □

Ausblick und offene Fragen

Die Perioden-Vermutung von Grothendieck, eine tiefliegende offene Vermutung der algebraischen Geometrie, impliziert, dass die Zahlen

$$2\pi i, \zeta(3), \zeta(5), \ldots, \zeta(2n+1), \ldots$$

algebraisch unabhängig über $\mathbb{Q}$ sind. Tatsächlich ist bisher für keine konkrete ungerade natürliche Zahl $2n+1 > 3$, die Irrationalität von $\zeta(2n+1)$ gezeigt. Erstaunlicherweise konnte Wadim Zudilin beweisen, dass mindestens eine der Zahlen

$$\zeta(5), \zeta(7), \zeta(9), \zeta(11)$$

irrational sein muss. An dieser Stelle möchten wir auch erwähnen, dass die Irrationalität der Catalanschen Konstante

$$G = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^2}$$

bisher noch unbewiesen ist.

4.3 *Irrationalität unendlich vieler ungerader Zeta-Werte*

Wir haben bereits eine geschlossene Formel für $\zeta(2n)$ bewiesen, die auf Euler zurückgeht. Die Frage nach der Natur der ungeraden Werte $\zeta(2n+1)$ der Riemannschen Zeta-Funktion ist ungemein schwerer.

Der Satz von Apéry zeigt, dass $\zeta(3)$ irrational ist. Tatsächlich ist $\zeta(3)$ der einzige explizite Wert der Riemannschen Zeta-Funktion an einer ungeraden natürlichen Zahl, dessen Irrationalität wir beweisen können. Umso verblüffender ist es, dass wir dennoch beweisen können, dass es unendlich viele irrationale Zeta-Werte gibt. Dieses Resultat wurde erstmals von Rivoal und Ball-Rivoal im Jahre 2001 gezeigt.

Satz (Rivoal, Ball–Rivoal, 2001)**.** *Für jedes $\epsilon > 0$ gibt es eine Zahl $s_0 \in \mathbb{N}$ mit der folgenden Eigenschaft: Für alle ungeraden Zahlen $s \in \mathbb{N}$, $s \geq s_0$ gilt*

$$\dim_{\mathbb{Q}}(\mathbb{Q} + \zeta(3)\mathbb{Q} + \zeta(5)\mathbb{Q} + \cdots + \zeta(s)\mathbb{Q}) \geq \frac{(1-\epsilon)\log s}{1+\log 2}.$$

Insbesondere sind mindestens $\frac{(1-\epsilon)\log s}{1+\log 2}$ der Zahlen

$$\zeta(3), \zeta(5), \ldots, \zeta(s)$$

irrational.

Insbesondere zeigt dieser Satz, dass es unendlich viele irrationale Zeta-Werte gibt. Allerdings wächst die untere Schranke für die Mindestanzahl an ungeraden Zeta-Werten $\frac{(1-\epsilon)\log s}{1+\log 2}$ sehr schwach. In einer gemeinsamen Arbeit mit Stéphane Fischler und Wadim Zudilin konnten wir diese untere Grenze wesentlich verschärfen:

Satz (Fischler-S.-Zudilin, 2018)**.** *Für jedes $\epsilon > 0$ gibt es eine Zahl $s_0 \in \mathbb{N}$ mit der folgenden Eigenschaft: Für alle ungeraden Zahlen $s \in \mathbb{N}$, $s \geq s_0$ sind mindestens*

$$2^{(1-\epsilon)\frac{\log s}{\log\log s}}$$

der Zahlen

$$\zeta(3), \zeta(5), \ldots, \zeta(s)$$

irrational.

Aufbauend auf den Ideen aus dieser Veröffentlichung konnten neulich Li Lai und Pin Yu die untere Schranke weiter verbessern:

Satz (Lai-Yu, 2019)**.** *Für jedes $\epsilon > 0$ gibt es eine Zahl $s_0 \in \mathbb{N}$ mit der folgenden Eigenschaft: Für alle ungeraden Zahlen $s \in \mathbb{N}$, $s \geq s_0$ sind mindestens*

$$(c_0 - \epsilon)\sqrt{\frac{s}{\log s}}, \quad c_0 \approx 1,1925\ldots$$

der Zahlen

$$\zeta(3), \zeta(5), \ldots, \zeta(s)$$

irrational.

Das Ziel der letzten beiden Vorlesungen ist es einen elementaren Beweis für die Existenz unendlich vieler irrationaler Zeta-Werte der Form $\zeta(2n+1)$ zu präsentieren.

4.3.1 Die Hurwitzsche Zeta-Funktion

Für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ und $\alpha \in \mathbb{R}_{>0}$ betrachten wir die folgende Verallgemeinerung der Riemannschen Zeta-Funktion:

$$\zeta(s,\alpha) := \sum_{n=0}^{\infty} \frac{1}{(n+\alpha)^s}.$$

Die Funktion $\zeta(s,\alpha)$ wird *Hurwitzsche Zeta-Funktion* genannt. Man bemerke, dass $\zeta(s,1) = \zeta(s)$. Die absolute Konvergenz weist man wie im Falle der Riemannschen Zeta-Funktion nach. Die folgende Gleichung wird im Laufe des Beweises eine wichtige Rolle spielen:

Lemma 4.3.1. *Für $d \in \mathbb{N}$ und $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$ gilt, dass*

$$\sum_{j=1}^{d} \zeta\left(s, \frac{j}{d}\right) = d^s \zeta(s).$$

Beweis. Das folgt sofort aus der folgenden Rechnung:

$$\begin{aligned}\sum_{j=1}^{d} \zeta\left(s, \frac{j}{d}\right) &= \sum_{j=1}^{d} \sum_{n=0}^{\infty} \frac{1}{(n+j/d)^s} \\ &= \sum_{j=1}^{d} \sum_{n=0}^{\infty} \frac{d^s}{(dn+j)^s} = d^s \sum_{m=1}^{\infty} \frac{1}{m^s} = d^s \zeta(s).\end{aligned}$$

Hierbei haben wir im vorletzten Schritt verwendet, dass $dn+j$ für $n \in \mathbb{N}_0$ und $j \in \{1,\dots,d\}$ alle natürlichen Zahlen genau einmal durchläuft. □

4.3.2 Überblick über den Beweis

In der heutigen Vorlesung möchten wir die Struktur des Beweises erklären. Als Input benötigen wir dazu die folgende Proposition über die Konstruktion von Linearformen in Hurwitzschen Zeta-Werten und deren Eigenschaften. Für natürliche Zahlen s und D betrachten wir die Folge rationaler Funktionen $(R_n)_{n\in\mathbb{N}}$, die durch

$$R_n := D^{3Dn} n!^{s+1-3D} \frac{\prod_{j=0}^{3Dn}(X-n+j/D)}{\prod_{j=0}^{n}(X+j)^{s+1}} \tag{4.12}$$

definiert ist.

Proposition 4.3.2 (Linearformen in Hurwitzschen Zeta-Werten)**.** *Angenommen s ist ungerade, D ist gerade und es gilt die Ungleichung $s \geq 3D$, dann gelten für die in (4.12) definierten rationalen Funktionen die folgenden Eigenschaften:*

(a) Für $n \in \mathbb{N}$ und jedes $j \in \{1, \dots, D\}$ konvergiert die Reihe

$$r_{n,j} := \sum_{m=1}^{\infty} R_n(m + j/D)$$

absolut und es gilt

$$r_{n,j} = \rho_{0,j} + \rho_3 \zeta(3, j/D) + \rho_5 \zeta(5, j/D) + \cdots + \rho_s \zeta(s, j/D)$$

mit geeigneten rationalen Zahlen $\rho_{0,j}$ und ρ_i. Für $3 \leq i \leq s$ hängen die rationalen Zahlen ρ_i nicht von j ab[28].

[28] Selbstverständlich hängen die Koeffizienten $\rho_{0,j}$ und ρ_i auch von n, D und s ab. Der Leserlichkeit halber, unterdrücken wir diese Abhängigkeiten in der Notation.

(b) Für $n \in \mathbb{N}$ und $1 \leq i \leq s$ gilt

$$d_n^{s+1-i} \rho_i \in \mathbb{Z} \quad \textit{und} \quad d_{n+1}^{s+1} \rho_{0,j} \in \mathbb{Z}.$$

Hier erinnern wir an $d_n = kgV(1, \dots, n)$.

(c) Für $j, j' \in \{1, \dots, D\}$ gilt

$$0 < \lim_{n \to \infty} |r_{n,j}|^{1/n} < 3^{-(s+1)} \quad \textit{und} \quad \lim_{n \to \infty} \frac{r_{n,j}}{r_{n,j'}} = 1.$$

Beweis. Wir werden die Beweise der Aussagen dieser Proposition im nächsten Abschnitt skizzieren. □

Wir werden nun unter Voraussetzung der obigen Behauptungen die Existenz unendlich vieler irrationaler Zeta-Werte zeigen. Der Beweis basiert auf dem folgenden einfachen Irrationalitätskriterium:

Lemma 4.3.3. *Seien $\alpha_1, \dots, \alpha_N$ reelle Zahlen und $(l_n)_{n \in \mathbb{N}}$ eine Folge von Null verschiedener Linearkombinationen*

$$l_n = a_1^{(n)} \alpha_1 + \cdots + a_N^{(n)} \alpha_N \in \mathbb{R}_{\neq 0}$$

mit ganzzahligen Koeffizienten $a_1^{(n)}, \dots, a_N^{(n)} \in \mathbb{Z}$. Falls

$$\lim_{n \to \infty} l_n = 0,$$

dann ist mindestens eine der Zahlen $\alpha_1, \dots, \alpha_N$ irrational.

Beweis. Angenommen alle Zahlen $\alpha_1, \dots, \alpha_N$ wären rational, dann gäbe es ein $M \in \mathbb{N}$ mit $M\alpha_i \in \mathbb{Z}$ für $i = 1, \dots, N$. Somit wäre

$$(Ml_n)_{n \in \mathbb{N}} = (a_1^{(n)} M\alpha_1 + \cdots + a_N^{(n)} M\alpha_N)_{n \in \mathbb{N}}$$

eine Folge von Null verschiedener ganzer Zahlen, die gegen Null konvergiert - ein Widerspruch. □

Satz 4.3.4. *Unendlich viele der Zahlen*

$$\zeta(3), \zeta(5), \dots, \zeta(2n+1), \dots$$

sind irrational.

Beweis. Angenommen, es gäbe nur endlich viele irrationale Zeta-Werte an ungeraden natürlichen Zahlen, sagen wir

$$\zeta(i_1), \dots, \zeta(i_m)$$

mit $3 = i_1 < \cdots < i_m$. Wir setzen $i_0 := 1$ und wählen eine gerade Zahl D mit genau $m+1$ Teilern, zum Beispiel $D = 2^m$. Seien $\delta_0, \dots, \delta_m$ die Teiler von D. Proposition 4.3.2 (a) liefert uns für eine hinreichend große Zahl ungerade natürliche Zahl s jedes $j \in \{1, \dots, D\}$ Folgen von Linearformen in Hurwitzschen Zeta-Werten

$$r_{n,j} = \rho_{0,j} + \sum_{\substack{3 \le i \le s \\ i \text{ ungerade}}} \rho_i \zeta(i, j/D).$$

Für jede Zahl $0 \le r \le m$ setzen wir

$$l_{n,r} := d_{n+1}^{s+1} \sum_{j=1}^{\delta_r} r_{n,jD/\delta_r}.$$

Man beachte, dass hierbei jede der Zahlen jD/δ_r eine ganze Zahl aus der Menge $\{1, \dots, D\}$ ist, da δ_r ein Teiler von D ist. Somit ist $r_{n,jD/\delta_r}$ wohldefiniert. In Anbetracht von Lemma 4.3.1 erhalten wir

$$\begin{aligned} l_{n,r} &:= d_{n+1}^{s+1} \left(\sum_{j=1}^{\delta_r} \rho_{0,jD/\delta_r} + \sum_{j=1}^{\delta_r} \sum_{\substack{3 \le i \le s \\ i \text{ ungerade}}} \rho_i \zeta(i, j/\delta_r) \right) \\ &= d_{n+1}^{s+1} \left(\sum_{j=1}^{\delta_r} \rho_{0,jD/\delta_r} + \sum_{\substack{3 \le i \le s \\ i \text{ ungerade}}} \rho_i \delta_r^i \zeta(i) \right). \end{aligned}$$

Aus Proposition 4.3.2 (b) folgern wir die Ganzzahligkeit der Koeffizienten dieser Linearformen:

$$l_{n,r} \in \mathbb{Z} + \zeta(3)\mathbb{Z} + \zeta(5)\mathbb{Z} + \cdots + \zeta(s)\mathbb{Z}.$$

Andererseits können wir auch die Konvergenzgeschwindigkeit der Folge $(l_{n,r})_{n \in \mathbb{N}}$ gut kontrollieren. Aus Proposition 4.3.2 (c) folgern wir

$$\lim_{n \to \infty} \frac{l_{n,r}}{d_{n+1}^{s+1} r_{n,1}} = \lim_{n \to \infty} \sum_{j=1}^{\delta_r} \frac{r_{n,jD/\delta_r}}{r_{n,1}} = \delta_r.$$

Indem wir Proposition 4.2.1 beachten und nochmals Proposition 4.3.2 (c) anwenden, erhalten wir

$$0 < \lim_{n \to \infty} |l_{n,r}|^{1/n} = \lim_{n \to \infty} |\delta_r r_{n,1} d_{n+1}^{s+1}|^{1/n} < \left(\frac{3}{4}\right)^{-(s+1)}.$$

Somit konvergiert die Folge $(l_{n,r})_{n\in\mathbb{N}}$ für $n \to \infty$ gegen Null und alle bis auf endliche viele Folgenglieder sind ungleich Null. Da die Koeffizienten der Linearkombination ganzzahlig sind, könnten wir Lemma 4.3.3 anwenden, um die Irrationalität einer der Zahlen

$$\zeta(3), \zeta(5), \ldots, \zeta(s)$$

zu zeigen. Wir hätten damit allerdings nichts gewonnen, da wir ja bereits wissen, dass $\zeta(3)$ irrational ist. Nun kommt der entscheidende Trick: Wir haben nicht nur *eine* Folge von Linearkombinationen konstruiert, sondern für *jeden* Teiler δ_r von D eine solche Folge:

$$\begin{aligned}
l_{n,0} &= d_{n+1}^{s+1} \left(\sum_{j=1}^{\delta_0} \rho_{0,jD/\delta_0} + \rho_3 \delta_0^3 \zeta(3) + \rho_5 \delta_0^5 \zeta(5) + \cdots + \rho_s \delta_0^s \zeta(s) \right) \\
l_{n,1} &= d_{n+1}^{s+1} \left(\sum_{j=1}^{\delta_1} \rho_{0,jD/\delta_1} + \rho_3 \delta_1^3 \zeta(3) + \rho_5 \delta_1^5 \zeta(5) + \cdots + \rho_s \delta_1^s \zeta(s) \right) \\
&\cdots\cdots \\
l_{n,m} &= d_{n+1}^{s+1} \left(\sum_{j=1}^{\delta_m} \rho_{0,jD/\delta_m} + \rho_3 \delta_m^3 \zeta(3) + \rho_5 \delta_m^5 \zeta(5) + \cdots + \rho_s \delta_m^s \zeta(s) \right).
\end{aligned}$$

Die Koeffizienten der Zeta-Werte in diesen Linearkombinationen sind sich sehr ähnlich. Tatsächlich unterscheiden sie sich nur um gewisse Potenzen der Form δ_r^i. Indem wir nun geschickt Linearkombinationen der obigen Linearformen bilden und beachten, dass die Matrix

$$\Delta = \begin{pmatrix} \delta_0^{i_0} & \delta_0^{i_1} & \ldots & \delta_0^{i_m} \\ \delta_1^{i_0} & \delta_1^{i_1} & \ldots & \delta_1^{i_m} \\ \vdots & & \ddots & \\ \delta_m^{i_0} & \delta_m^{i_1} & \ldots & \delta_m^{i_m} \end{pmatrix} \in M_{m+1,m+1}(\mathbb{Q})$$

invertierbar ist[29], können wir die Zeta-Werte

[29] Siehe Übungsblatt 13.

$$\zeta(i_1), \ldots, \zeta(i_m)$$

aus den Linearformen eliminieren. Wir erläutern das nun genauer: Da Δ invertierbar ist, existieren ganze Zahlen $(w_r)_{r=0,\ldots,m}$ mit der Eigenschaft, dass

$$\sum_{r=0}^{m} w_r \delta_r^{i_j} = 0 \text{ für jedes } j \in \{1, \ldots, m\} \quad \text{und} \quad \sum_{r=0}^{m} w_r \delta_r^{i_0} \neq 0. \tag{4.13}$$

Wir definieren nun

$$l_n := \sum_{r=0}^{m} w_r l_{n,r}$$

und können l_n als Linearkombination von Zeta-Werten schreiben:

$$l_n = \sum_{r=0}^{m} w_r \sum_{j=1}^{\delta_r} d_{n+1}^{s+1} \rho_{0,jD/\delta_r} + \sum_{\substack{3\le i\le s \\ i \text{ ungerade}}} d_{n+1}^{s+1} \rho_i \underbrace{\left(\sum_{r=0}^{m} w_r \delta_r^i \right)}_{=0 \text{ für } i\in\{i_1,\ldots,i_m\}} \zeta(i).$$

Per Konstruktion, siehe (4.13), verschwinden für $i \in \{i_1, \dots, i_m\}$ die Koeffizienten

$$d_{n+1}^{s+1} \rho_i \sum_{r=0}^{m} w_r \delta_r^i$$

vor $\zeta(i)$. Wir erhalten also

$$l_n \in \mathbb{Z} + \sum_{\substack{3 \le i \le s \text{ ungerade} \\ i \notin \{i_1, \dots, i_m\}}} \zeta(i)\mathbb{Z}.$$

Andererseits gilt

$$C := \lim_{n\to\infty} \frac{l_n}{r_{n,1}} = \lim_{n\to\infty} \frac{\sum_{r=0}^{m} w_r l_{n,r}}{d_{n+1}^{s+1} r_{n,1}} = \lim_{n\to\infty} \sum_{r=0}^{m} w_r \delta_r \neq 0.$$

Somit sind alle bis auf endlich viele Terme der Folge l_n ungleich Null und es gilt

$$\lim_{n\to\infty} |l_n|^{1/n} = \lim_{n\to\infty} |C \cdot d_{n+1}^{s+1} \cdot r_{n,1}|^{1/n} < 1.$$

Nach Lemma 4.3.3 ist mindestens eine der Zahlen

$$\zeta(i) \text{ für } i \text{ ungerade und } i \notin \{i_1, \dots, i_m\}$$

irrational. Dies widerspricht allerdings der Annahme, dass

$$\zeta(i_1), \dots, \zeta(i_m)$$

bereits alle irrationalen ungeraden Zeta-Werte sind. Somit muss es unendlich viele irrationale Zeta-Werte der Form $\zeta(2n+1)$ geben. □

Ausblick und offene Fragen

Die Riemannsche Zeta-Funktion ist das einfachste Beispiel einer L-Funktion. L-Funktionen zu verschiedenen mathematischen Objekten spielen eine entscheidende Rolle in der Zahlentheorie und enthalten tiefliegende arithmetische Informationen. Eine relativ einfache Klasse von L-Funktionen sind die Dirichletschen L-Funktionen. Ein *Dirichlet-Charakter* ist ein Gruppenhomomorphismus

$$\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Wir können einen Dirichlet-Charakter zu einer Funktion auf $\mathbb{Z}$ fortsetzen, indem wir für $n \in \mathbb{Z}$ definieren

$$\chi(n) := \begin{cases} \chi(n \bmod N) & \text{falls } \operatorname{ggT}(n, N) = 1 \\ 0 & \text{sonst.} \end{cases}$$

Wir nennen den Dirichlet-Charakter *gerade*, falls $\chi(-1) = 1$, andernfalls nennen wir ihn *ungerade*. Die *Dirichletsche L-Funktion* zu einem Dirichlet-Charakter χ ist definiert als

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \text{für } s \in \mathbb{C} \text{ mit } \operatorname{Re}(s) > 1.$$

Man kann sich nun fragen, was man über die Werte der Dirichletschen L-Funktionen an den natürlichen Zahlen aussagen kann. Tatsächlich kann man zeigen, dass für einen geraden Dirichlet-Charakter die Werte

$$\frac{L(\chi,2n)}{\pi^{2n}}$$

algebraisch sind, während für einen ungeraden Dirichlet-Charakter die Werte

$$\frac{L(\chi,2n+1)}{\pi^{2n+1}}$$

algebraisch sind. Über die verbleibenden Werte der Dirichletschen L-Funktionen ist so gut wie nichts bekannt. Ähnlich zur Riemannschen Zeta-Funktion kann man zwar zeigen, dass es unter den verbleibenden Werten stets unendlich viele irrationale geben muss, aber über konkrete Werte weiß man quasi gar nichts. Die Frage nach der Irrationalität der Catalanschen Konstante können wir nun umformulieren zur Frage nach der Irrationalität des L-Werts

$$L(\chi_4,2)$$

mit

$$\chi_4 \colon (\mathbb{Z}/4\mathbb{Z})^\times = \{1,3\} \to \mathbb{C}^\times$$

und

$$\chi(1) = 1, \quad \chi(3) = -1.$$

4.4 *Linearformen in Hurwitzschen Zeta-Werten*

In der letzten Vorlesung haben wir, unter der Annahme gewisser Behauptungen über Linearformen in Hurwitzschen Zeta-Werten, bewiesen, dass unendlich viele der Zeta-Werte

$$\zeta(3), \zeta(5), \ldots, \zeta(2n+1), \ldots$$

irrational sind. Der Beweis basiert auf Linearformen in Hurwitzschen Zeta-Werten und deren analytischen und arithmetischen Eigenschaften. In der heutigen Vorlesung möchten wir die Konstruktion dieser Linearformen erklären und die Beweise der analytischen und arithmetischen Eigenschaften skizzieren.

Partialbruchentwicklung rationaler Funktionen[30]

In Proposition 4.3.2 (a) haben wir behauptet, dass Reihen der Form

$$r_{n,j} := \sum_{m=1}^{\infty} R_n(m + j/D)$$

Linearformen in Hurwitzschen Zeta-Werten liefern. Um dies zu beweisen, werden wir die Partialbruchentwicklung rationaler Funktionen[31] benötigen:

[30] Zu diesem Abschnitt gibt es ein Video:

[31] Eine rationale Funktion ist ein Quotient zweier Polynome.

Satz 4.4.1 (Partialbruchentwicklung). *Seien $\alpha_1, \dots, \alpha_m$ paarweise verschiedene Elemente eines Körpers $K \subseteq \mathbb{C}$ und $i_1, \dots, i_m$ natürliche Zahlen. Sei $Q := (X - \alpha_1)^{i_1} \dots (X - \alpha_m)^{i_m}$ und $P \in K[X]$ mit $\deg P < \deg Q$. Dann gibt es eindeutig bestimmte Elemente $a_{k,i} \in K$ mit $1 \le k \le m$ und $1 \le i \le i_k$, sodass*

$$\frac{P}{Q} = \sum_{k=1}^{m} \sum_{i=1}^{i_k} \frac{a_{k,i}}{(X - \alpha_k)^i}.$$

Die Koeffizienten $a_{k,i}$ lassen sich berechnen durch

$$a_{k,i} = \frac{1}{(i_k - i)!} \left(\frac{\partial}{\partial X}\right)^{i_k - i} \left((X - \alpha_k)^{i_k} \frac{P}{Q}\right)\Bigg|_{X=\alpha_k}. \tag{4.14}$$

Beweis. Siehe Übungsblatt 13, Aufgabe 3. □

Das folgende Resultat wird nützlich sein, um die arithmetischen Eigenschaften der Linearformen, siehe Proposition 4.3.2 (b), zu studieren:

Lemma 4.4.2. *Seien n, m natürliche Zahlen und $k_1, \dots, k_m$ paarweise verschiedene Elemente aus der Menge $\{0, \dots, n\}$ sowie $i_1, \dots, i_m \in \mathbb{N}$. Wir betrachten nun die Partialbruchentwicklung*

$$\frac{1}{\prod_{j=1}^{m} (X + k_j)^{i_j}} = \sum_{j=1}^{m} \sum_{i=1}^{i_j} \frac{b_{j,i}}{(X + k_j)^i}.$$

Dann gilt für die Koeffizienten der Partialbruchentwicklung, dass

$$d_n^{(\sum_{\alpha=1}^{m} i_\alpha) - i} b_{j,i} \in \mathbb{Z},$$

wobei wir an $d_n = kgV(1, \dots, n)$ erinnern.

Beweis. Für $m = 1$ ist die Behauptung trivialerweise erfüllt, wir dürfen also ohne Einschränkung $m \ge 2$ annehmen. Aufgrund der Symmetrie reicht es außerdem die Formel für $j = 1$ zu zeigen. Nach (4.14) berechnet sich der Koeffizient $b_{1,i}$ wie folgt unter Verwendung der Leibniz-Regel[32]

[32] Wir verwenden hier die allgemeine Leibniz-Formel für die n-fache Ableitung eines m-fachen Produkts $u_1 \cdots u_m$:

$$\frac{1}{n!}(u_1 \cdots u_m)^{(n)} = \sum_{n_1 + \dots + n_m = n} \frac{1}{n_1! \cdots n_m!} u_1^{(n_1)} \cdots u_m^{(n_m)}.$$

Diese Formel kann man induktiv aus der Produktregel für Ableitungen folgern.

$$\begin{aligned} b_{1,i} &= \frac{1}{(i_1-i)!}\left(\frac{\partial}{\partial X}\right)^{i_1-i}\left((X+k_1)^{i_1}\frac{1}{\prod_{\alpha=1}^{m}(X+k_\alpha)^{i_\alpha}}\right)\Bigg|_{X=-k_1} \\ &= \frac{1}{(i_1-i)!}\left(\frac{\partial}{\partial X}\right)^{i_1-i}\left(\prod_{\alpha=2}^{m}(X+k_\alpha)^{-i_\alpha}\right)\Bigg|_{X=-k_1} \\ &= \sum_{\substack{l_2,\dots,l_m\geq 0\\ l_2+\cdots+l_m=i_1-i}}\prod_{\alpha=2}^{m}\frac{1}{l_\alpha!}\left(\frac{\partial}{\partial X}\right)^{l_\alpha}(X+k_\alpha)^{-i_\alpha}\Bigg|_{X=-k_1} \\ &= \sum_{\substack{l_2,\dots,l_m\geq 0\\ l_2+\cdots+l_m=i_1-i}}\prod_{\alpha=2}^{m}(-1)^{l_\alpha}\binom{i_\alpha+l_\alpha-1}{l_\alpha}(k_\alpha-k_1)^{-i_\alpha-l_\alpha}. \end{aligned}$$

Wir bemerken, dass $\frac{d_n}{k_\alpha-k_1}\in\mathbb{Z}$. Wegen

$$\sum_{\alpha=2}^{m}(i_\alpha+l_\alpha)=i_1-i+\sum_{\alpha=2}^{m}i_\alpha=\left(\sum_{\alpha=1}^{m}i_\alpha\right)-i$$

folgt die Behauptung. □

Die Stirlingsche Formel

Die Stirlingsche Formel beschäftigt sich mit dem asymptotischen Wachstum der Folge $(n!)_{n\in\mathbb{N}}$. Wir werden etwas allgemeiner das Wachstum der Gamma-Funktion $\Gamma\colon\mathbb{R}_{>0}\to\mathbb{R}$,

$$\Gamma(x):=\int_0^\infty t^{x-1}e^{-t}dt,\quad x>0$$

für $x\to\infty$ studieren. Wir haben bereits auf Übungsblatt 11 mit Hilfe von partieller Integration die Formel

$$\Gamma(x+1)=x\Gamma(x)$$

gezeigt und daraus $\Gamma(n)=(n-1)!$ für $n\in\mathbb{N}$ gefolgert. Dies gibt den Bezug zu Fakultäten. Wir nennen zwei Funktionen $f,g\colon\mathbb{R}_{>0}\to\mathbb{R}$ asymptotisch äquivalent und schreiben $f\sim g$ für $x\to\infty$, falls

$$\lim_{x\to\infty}\frac{f(x)}{g(x)}=1.$$

Die folgende Proposition studiert das asymptotische Wachstum der Gamma-Funktion:

Proposition 4.4.3 (Stirlingsche Formel, schwache Version)**.** *Für alle $x>0$ gilt*

$$x^{x-1}e^{1-x}\leq\Gamma(x)\leq x^xe^{1-x}.$$

Insbesondere haben wir[33]

$$\Gamma(x)^{1/x}\sim\frac{x}{e}\quad \textit{für } x\to\infty.$$

[33] Man kann diese Aussage stark verbessern. Mit etwas mehr Aufwand kann man zum Beispiel

$$\Gamma(x)\sim\sqrt{\frac{2\pi}{x}}\left(\frac{x}{e}\right)^x\quad\text{für } x\to\infty$$

zeigen. Aber auch diese stärkere Aussage lässt sich noch weiter verbessern.

Beweis. Wir definieren $\psi(x) := \frac{\partial}{\partial x} \log \Gamma(x) = \frac{\Gamma'(x)}{\Gamma(x)}$ und zeigen zunächst die folgende Behauptung:
Behauptung: Für alle $x > 0$ gilt

$$\log x - \frac{1}{x} \leq \psi(x) \leq \log x. \tag{4.15}$$

Beweis der Behauptung: Aus $\Gamma(x+1) = x\Gamma(x)$ folgt einerseits durch Logarithmieren

$$\log \Gamma(x+1) - \log \Gamma(x) = \log x. \tag{4.16}$$

und durch Ableiten

$$\psi(x+1) = \psi(x) + \frac{1}{x}.$$

Nach dem Zwischenwertsatz folgt aus (4.16) die Existenz eines Elements $\xi \in (x, x+1)$ mit

$$\log \Gamma(x+1) - \log \Gamma(x) = \psi(\xi).$$

Da ψ wachsend ist, gilt

$$\psi(x) \leq \psi(\xi) = \log(x) \leq \psi(x+1) = \psi(x) + \frac{1}{x}$$

und die Behauptung ist bewiesen.

Indem wir (4.15) von 1 bis x integrieren und

$$\int_1^x \psi(t)dt = \log \Gamma(x)$$

beachten, erhalten wir

$$(x-1)\log x - x + 1 \leq \log \Gamma(x) \leq x \log x - x + 1.$$

Die Aussage der Proposition folgt hieraus durch anwenden der Exponentialfunktion. □

Wenn wir uns in Proposition 4.4.3 auf Werte der Gamma-Funktion an natürlichen Zahlen beschränken, erhalten wir:

Korollar 4.4.4. *Es gilt* [34]

$$\sqrt[n]{n!} \sim \frac{n}{e} \quad \text{für } n \to \infty.$$

[34] Streng genommen haben wir nur $u \sim v$ bisher nur für Funktionen $u, v \colon \mathbb{R}_{>0} \to \mathbb{R}$ definiert. Für Folgen $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ definieren wir analog $a_n \sim b_n$ für $n \to \infty$, falls

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 1.$$

Linearformen in Hurwitzschen Zeta-Werten und ihre Eigenschaften

Das Ziel des folgenden Abschnitts ist es den Beweis der Proposition 4.3.2 zu skizzieren. Wir erinnern zunächst an die Definition der rationalen Funktionen R_n für natürliche Zahlen n, D und s, siehe (4.12):

$$R_n := D^{3Dn} n!^{s+1-3D} \frac{\prod_{j=0}^{3Dn}(X - n + j/D)}{\prod_{j=0}^{n}(X+j)^{s+1}}.$$

Im Folgenden werden wir stets annehmen, dass D gerade und s ungerade ist und $s \geq 3D$ gilt. Die Annahme $s \geq 3D$ impliziert, dass der Grad des Zählers von R_n kleiner ist als der Grad des Nenners. Des Weiteren bemerken wir, dass jede der Zahlen $j = 0, -1, \ldots, -n$ eine einfache Nullstelle des Produkts im Zähler ist. Somit besitzt R_n nur Pole der Ordnung s in $j = 0, -1, \ldots, -n$. Nach Satz 4.4.1 hat R_n somit eine eindeutige Partialbruchentwicklung der Form

$$R_n = \sum_{k=0}^{n} \sum_{i=1}^{s} \frac{a_{k,i}}{(X+k)^i}. \tag{4.17}$$

Als erstes werden wir Teilaussage (a) aus Proposition 4.3.2 beweisen. Genauer zeigen wir die folgende etwas präzisere Aussage, welche Proposition 4.3.2 (a) impliziert.

Lemma 4.4.5. *Für $n \in \mathbb{N}$ und jedes $j \in \{1, \ldots, D\}$ konvergiert die Reihe*

$$r_{n,j} := \sum_{m=1}^{\infty} R_n(m + j/D)$$

absolut und es gilt

$$r_{n,j} = \rho_{0,j} + \sum_{\substack{3 \leq i \leq s \\ i \text{ ungerade}}} \rho_i \zeta(i, j/D).$$

Hierbei sind die Koeffizienten ρ_i für $3 \leq i \leq s$ gegeben durch

$$\rho_i := \sum_{k=0}^{n} a_{k,i}.$$

Der nullte Koeffizient lässt sich für $j \in \{1, \ldots, D\}$ durch die Formel

$$\rho_{0,j} = -\sum_{k=0}^{n} \sum_{l=0}^{k} \sum_{i=1}^{s} \frac{a_{k,i}}{(l + j/D)^i}$$

beschreiben.[35]

[35] Wir weisen nochmal explizit darauf hin, dass die Koeffizienten ρ_i für $3 \leq i \leq s$ nicht von j abhängen.

Beweis. Zunächst bemerken wir, dass $R_n(X + j/D)$ keine Pole in den natürlichen Zahlen besitzt. Für k hinreichend groß gilt $R_n(k + j/D) > 0$, somit folgt aus Übungsaufgabe 2 auf Blatt 13 die absolute Konvergenz der Reihe $r_{n,j}$.

Nun zeigen wir, dass sich $r_{n,j}$ als Linearkombination von Hurwitzschen Zeta-Werten schreiben lässt. Unter Verwendung der Partialbruchentwicklung

$$R_n = \sum_{k=0}^{n} \sum_{i=1}^{s} \frac{a_{k,i}}{(X+k)^i},$$

erhalten wir:

$$\begin{aligned}\sum_{m=1}^{\infty} R_n\Big(m+\frac{j}{D}\Big) &= \sum_{m=1}^{\infty}\sum_{i=1}^{s}\sum_{k=0}^{n}\frac{a_{k,i}}{(m+k+\frac{j}{D})^i}\\ &= \sum_{i=1}^{s}\sum_{k=0}^{n} a_{k,i}\sum_{m=1}^{\infty}\frac{1}{(m+k+\frac{j}{D})^i}\\ &= \sum_{i=1}^{s}\sum_{k=0}^{n} a_{k,i}\Big(\zeta\Big(i,\frac{j}{D}\Big)-\sum_{\ell=0}^{k}\frac{1}{(\ell+\frac{j}{D})^i}\Big).\end{aligned}$$

Mit Blick auf die Partialbruchentwicklung von R_n sehen wir nun, dass

$$\sum_{k=0}^{n} a_{k,1} = \lim_{x\to\infty} xR_n(x) = 0,$$

und der Term $\zeta(i, j/D)$ für $i = 1$ verschwindet in der obigen Formel[36]. Wir erhalten

$$r_{n,j} := \sum_{m=1}^{\infty} R_n\Big(m+\frac{j}{D}\Big) = \rho_{0,j} + \sum_{2\le i\le s}\rho_i\zeta(i, j/D)$$

mit

$$\rho_i = \sum_{k=0}^{n} a_{k,i}$$

für $3 \le i \le s$, und

$$\rho_{0,j} = -\sum_{k=0}^{n}\sum_{l=0}^{k}\sum_{i=0}^{s}\frac{a_{k,i}}{(l+j/D)^i}.$$

Es verbleibt nur noch das Verschwinden der Koeffizienten ρ_i für gerade Indizes i zu zeigen: Wir erinnern daran, dass wir am Anfang des Kapitels die Zahlen D und s so gewählt haben, dass s ungerade und D gerade ist. Eine direkte Rechnung zeigt nun

$$R_n(-X-n) = -R_n(X).$$

Indem wir in dieser Gleichung auf beiden Seiten die Partialbruchentwicklung von R_n anwenden, sehen wir

$$\begin{aligned}-\sum_{k=0}^{n}\sum_{i=1}^{s}\frac{a_{k,i}}{(X+k)^i} &= -R_n(X)\\ &= R_n(-X-n) = \sum_{k=0}^{n}\sum_{i=1}^{s}\frac{a_{k,i}}{(-X-n+k)^i}\\ &= \sum_{k=0}^{n}\sum_{i=1}^{s}\frac{a_{n-k,i}(-1)^i}{(X+k)^i}.\end{aligned}$$

Da die Partialbruchentwicklung einer rationalen Funktion eindeutig ist, folgt

$$a_{k,i} = -a_{n-k,i}(-1)^i.$$

[36] Vielleicht haben Sie gemerkt, dass ich an dieser Stelle gemogelt habe, denn für $s = 1$ hat die Funktion $s \mapsto \zeta(s, j/D)$ einen Pol. Man kann das obige Argument präzise machen, wenn man die obige Rechnung zunächst für die Reihe

$$\sum_{m=1}^{\infty} R_n\Big(m+\frac{j}{D}\Big)z^m$$

mit $|z| < 1$ durchführt und dann z gegen 1 laufen lässt.

Setzen wir diese Gleichung in die definierende Gleichung der Koeffizienten ρ_i ein, so erhalten wir für gerade Indizes i:

$$\rho_i = \sum_{k=0}^{n} a_{k,i} = \sum_{k=0}^{n} -a_{n-k,i} = -\rho_i.$$

Hieraus folgt, dass ρ_i für gerade Indizes verschwindet, und die Aussage der Proposition ist gezeigt. □

Im nächsten Schritt studieren wir die arithmetischen Eigenschaften der Koeffizienten der in Lemma 4.4.5 konstruierten Linearformen $r_{n,j}$. Das folgende Lemma beweist die Aussage (b) in Proposition 4.3.2.

Lemma 4.4.6. *Für $n \in \mathbb{N}$ und $1 \le i \le s$ gilt*

$$d_n^{s+1-i}\rho_i \in \mathbb{Z} \tag{4.18}$$

und

$$d_{n+1}^{s+1}\rho_{0,j} \in \mathbb{Z}. \tag{4.19}$$

Beweis. Für jede Zahl $\alpha \in \frac{1}{D}\mathbb{Z}$ definieren wir

$$F_\alpha := D^n \, \frac{\prod_{j=1}^{n}(X+\alpha+\frac{j}{D})}{\prod_{j=0}^{n}(X+j)}$$

und betrachten die zugehörige Partialbruchentwicklung

$$F_\alpha = \sum_{k=0}^{n} \frac{A_{\alpha,k}}{X+k}.$$

In Anbetracht von (4.14) können wir die Koeffizienten $A_{\alpha,k}$ explizit berechnen und erhalten

$$\begin{aligned}(-1)^k A_{\alpha,k} &= \binom{n}{k} \frac{\prod_{j=1}^{n}(D(\alpha-k)+j)}{n!} \\ &= \begin{cases} \binom{n}{k}\binom{D(\alpha-k)+n}{n} & \text{if } \alpha-k \ge 0, \\ 0 & \text{if } \frac{-n}{D} \le \alpha-k < 0, \\ (-1)^n\binom{n}{k}\binom{D(k-\alpha)-1}{n} & \text{if } \alpha-k < \frac{-n}{D}. \end{cases}\end{aligned}$$

Die Partialbruchentwicklung der rationalen Funktion

$$G := \frac{n!}{\prod_{j=0}^{n}(X+j)}$$

ist gegeben durch

$$G = \sum_{k=0}^{n} \frac{(-1)^k\binom{n}{k}}{X+k}$$

und hat deshalb ebenfalls ganzzahlige Koeffizienten. Wir betrachten nun die Partialbruchentwicklung der rationalen Funktion

$$G^{s+1-3D}\prod_{\ell=0}^{3D-1} F_{-n+\frac{\ell n}{D}} = \sum_{k=0}^{n}\sum_{i=1}^{s}\frac{b_{k,i}}{(X+k)^i}.$$

Indem wir dieses Produkt ausmultiplizieren, die Formeln für die Partialbruchentwicklungen von F_α und G anwenden, und Lemma 4.4.2 verwenden, sehen wir

$$d_n^{s+1-i} b_{k,i} \in \mathbb{Z}.$$

Indem wir R_n als

$$R_n(t) = (X-n)\, G^{s+1-3D} \prod_{\ell=0}^{3D-1} F_{-n+\frac{\ell n}{D}}. \tag{4.20}$$

schreiben und die Formel

$$\frac{X-n}{X+k} = 1 - \frac{k+n}{X+k}$$

beachten, erhalten wir

$$d_n^{s+1-i} a_{k,i} \in \mathbb{Z}.$$

Nun folgt die (4.18) aus

$$d_n^{s+1-i} \rho_i = \sum_{k=0}^{n} d_n^{s+1-i} a_{k,i}.$$

Der Beweis der Ganzzahligkeitsaussage (4.19) ist ähnlich, wir verweisen auf Lemma 2 in Fischler–S.–Zudilin[37]. □

[37] S. Fischler, J. Sprang, and W. Zudilin. Many odd zeta values are irrational. *Compositio Mathematica*, 155(5):938–952, 2019. DOI: 10.1112/S0010437X1900722X

Letztendlich betrachten wir die Asymptotik der Folgen $r_{n,j}$:

Lemma 4.4.7. *Für jede hinreichend große ungerade ganze Zahl s und $j, j' \in \{1, \dots, D\}$ gilt*

$$0 < \lim_{n\to\infty} |r_{n,j}|^{1/n} < 3^{-(s+1)} \quad \textit{und} \quad \lim_{n\to\infty} \frac{r_{n,j}}{r_{n,j'}} = 1.$$

Beweis. Wir bemerken zunächst, dass die Summanden $R_n(m + j/D)$ für $1 \le m < n$ in der Reihe

$$r_{n,j} = \sum_{m=1}^{\infty} R_n(m + j/D)$$

verschwinden, da dies Nullstellen von R_n sind. Für $j \in \{1, \dots, D\}$ und $k \ge 0$, definieren wir

$$c_{k,j} := R_n\Big(n + k + \frac{j}{D}\Big) = D^{3Dn}\, n!^{s+1-3D}\, \frac{\prod_{\ell=0}^{3Dn}(k + \frac{j+\ell}{D})}{\prod_{\ell=0}^{n}(n+k+\ell+\frac{j}{D})^{s+1}},$$

sodass sich

$$r_{n,j} = \sum_{m=1}^{\infty} R_n\Big(m + \frac{j}{D}\Big) = \sum_{k=0}^{\infty} c_{k,j}$$

als Reihe strikt positiver Terme schreiben lässt. Als nächstes betrachten wir die Quotienten

$$\frac{c_{k+1,j}}{c_{k,j}} = \Bigg(\prod_{\ell=1}^{D} \frac{k+3n+\frac{j+\ell}{D}}{k+\frac{j+\ell-1}{D}}\Bigg)\Bigg(\frac{k+n+\frac{j}{D}}{k+2n+1+\frac{j}{D}}\Bigg)^{s+1}. \tag{4.21}$$

Für eine positive reelle Zahl x setzen wir $k = \lfloor xn \rfloor$. Dann konvergiert der Quotient $\frac{c_{k+1,j}}{c_{k,j}}$ für $n \to \infty$ und jedes j gegen $f(x)$, wobei

$$f(x) = \Big(\frac{x+3}{x}\Big)^D \Big(\frac{x+1}{x+2}\Big)^{s+1}.$$

Wir betrachten nun die logarithmische Ableitung von f und erhalten

$$\frac{f'(x)}{f(x)} = \frac{D}{x+3} - \frac{D}{x} + \frac{s+1}{x+1} - \frac{s+1}{x+2} = \frac{ax^2+bx+c}{x(x+1)(x+2)(x+3)},$$

mit $a = s+1-3D > 0$ und $c = -6D < 0$. Somit hat die Ableitung $f'(x)$ genau eine Nullstelle x_1 in den positiven reellen Zahlen. Dies zeigt, dass die Funktion $f(x)$ auf dem Intervall $(0, x_1]$ fällt und auf $[x_1, +\infty)$ wächst. Wegen $\lim_{x\to 0^+} f(x) = +\infty$ und $\lim_{x\to+\infty} f(x) = 1$ folgern wir, dass es eine eindeutige positive reelle Zahl x_0 gibt mit $f(x_0) = 1$. Bevor wir fortfahren möchten wir erklären, was die obige Rechnung für die Folge $\frac{c_{k+1,j}}{c_{k,j}}$ für hinreichend großes n und $k = \lfloor xn \rfloor$ bedeutet. Falls n hinreichend groß ist, wird der Quotient $\frac{c_{k+1,j}}{c_{k,j}}$ gut durch den Wert $f(x)$ beschrieben. Die Existenz einer eindeutigen reellen Zahl x_0 mit $f(x_0) = 1$ bedeutet dann, dass für $k = \lfloor x_0 n \rfloor$ die Werte $c_{k+1,j}$ und $c_{k,j}$ etwa gleich groß sind.

Im ersten Schritt zeigt man für $\epsilon > 0$ und jede hinreichend große Zahl n die Ungleichungskette

$$(1-\epsilon) r_{n,j} \le \sum_{(x_0-\epsilon)n \le k \le (x_0+\epsilon)n} c_{k,j} \le r_{n,j}. \tag{4.22}$$

Der Beweis dieser Ungleichungskette ist elementar, aber länglich. Wir verweisen auf Lemma 3 in Fischler–S.–Zudilin[38]. Die Ungleichung (4.22) zeigt, dass fast alle Beiträge der Reihe $r_{n,j}$ von wenigen Summanden rund um den Index $x_0 n$ kommen. Insbesondere folgt

[38] S. Fischler, J. Sprang, and W. Zudilin. Many odd zeta values are irrational. *Compositio Mathematica*, 155(5):938–952, 2019. DOI: 10.1112/S0010437X1900722X

$$\lim_{n\to\infty} (r_{n,j})^{1/n} = \lim_{n\to\infty} (c_{k_0(n),j})^{1/n}$$

mit $k_0(n) := \lfloor x_0 n \rfloor$. Im Folgenden reicht es also die Asymptotik der Folge $(c_{k_0(n),j}^{1/n})_{n\in\mathbb{N}}$ genauer zu betrachten. Wir beginnen zunächst für beliebiges k mit einer Umformung des Folgenglieds $c_{k,j}$:

$$\begin{aligned} c_{k,j} &= D^{-1} n!^{s+1-3D} \frac{\prod_{l=0}^{3Dn} (Dk+l+j)}{\prod_{l=0}^{n} (n+k+l+j/D)^{s+1}} \\ &= D^{-1} n!^{s+1-3D} \frac{(3Dn+Dk+j)!}{(Dk+j-1)!} \frac{\Gamma(n+k+j/D)^{s+1}}{\Gamma(2n+k+1+j/D)^{s+1}}. \end{aligned} \tag{4.23}$$

Wir möchten diese Rechnung nun für $k = k_0(n)$ verwenden um $\lim_{n\to\infty} c_{k_0(n),j}^{1/n}$ zu berechnen. Für $x \in \mathbb{R}$ gilt

$$\Gamma(x) \le \Gamma(x+j/D) \le \Gamma(x+1),$$

und somit unter Verwendung der Stirlingschen Formel

$$\sqrt[n]{\Gamma(n+k_0(n)+j/D)} \sim \sqrt[n]{(n+k_0(n))!} \sim \left(\frac{n+k_0(n)}{e}\right)^{1+x_0},$$

für $n \to \infty$. Ähnlich berechnen wir

$$\frac{1}{\sqrt[n]{\Gamma(2n+k_0(n)+1+j/D)}} \sim \left(\frac{e}{2n+k_0(n)}\right)^{2+x_0}$$

sowie

$$\sqrt[n]{(3Dn+Dk_0(n)+j)!} \sim \left(\frac{3Dn+Dk_0(n)}{e}\right)^{3D+Dx_0}$$

und

$$\sqrt[n]{(Dk_0(n)+j-1)!} \sim \left(\frac{Dk_0(n)}{e}\right)^{Dx_0},$$

für $n \to \infty$. Setzen wir nun alles in (4.23) ein, so erhalten wir

$$\begin{aligned} c_{k_0(n),j}^{1/n} &\sim \left(\frac{n}{e}\right)^{s+1-3D} \left(\frac{3Dn+Dk_0(n)}{e}\right)^{3D+Dx_0} \left(\frac{e}{Dk_0(n)}\right)^{Dx_0} \\ &\quad \times \left(\frac{n+k_0(n)}{e}\right)^{(s+1)(x_0+1)} \left(\frac{e}{2n+k_0(n)}\right)^{(s+1)(x_0+2)} \\ &\sim \frac{((x_0+3)D)^{(x_0+3)D}}{(x_0D)^{x_0D}} \frac{(x_0+1)^{(s+1)(x_0+1)}}{(x_0+2)^{(s+1)(x_0+2)}} \\ &= g(x_0)f(x_0)^{x_0} = g(x_0), \end{aligned} \tag{4.24}$$

mit

$$f(x) = \left(\frac{x+3}{x}\right)^D \left(\frac{x+1}{x+2}\right)^{s+1} \quad \text{und} \quad g(x) = D^{3D}\frac{(x+3)^{3D}(x+1)^{s+1}}{(x+2)^{2(s+1)}}.$$

Die Ungleichung $g(x_0) < 3^{-(s+1)}$ zeigt man durch eine direkte Rechnung, für Details verweisen wir auf Lemma 3 in Fischler–S.–Zudilin[39]. Wir möchten diese Ungleichung wenigstens heuristisch erklären: Mit Hilfe der Kurvendiskussion der Funktion f am Anfang des Beweises sieht man leicht, dass x_0 beliebig klein wird, wenn wir s hinreichend groß wählen. Setzen wir nun einen hinreichend kleinen Wert x_0 in g ein, so erhalten wir einen Wert der Größenordnung

$$g(x_0) \approx g(0) = (3D)^{3D}\frac{1}{2^{2(s+1)}}.$$

Für festes D und hinreichend großes s können wir also $g(0)$ durch $4^{-(s+1)}$ abschätzen. Indem man dieses heuristische Argument präzise macht, erhält man einen Beweis für $g(x_0) < 3^{-(s+1)}$.

Mit ähnlichen Argumenten wie oben lässt sich der Grenzwert

$$\lim_{n\to\infty} \frac{r_{n,j}}{r_{n,j'}} = 1$$

[39] S. Fischler, J. Sprang, and W. Zudilin. Many odd zeta values are irrational. *Compositio Mathematica*, 155(5):938–952, 2019. DOI: 10.1112/S0010437X1900722X

zeigen. Für Details verweisen wir auf Lemma 3 in Fischler–S.–Zudilin[40]. □

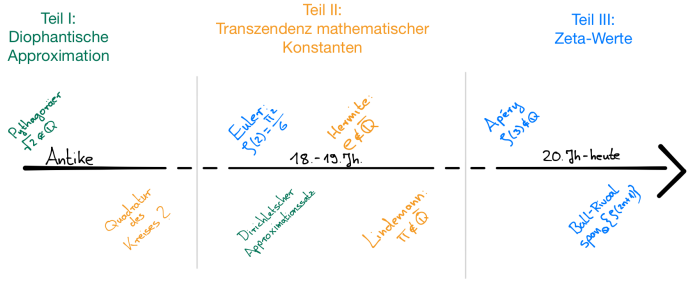
Indem wir die Resultate dieses Abschnitts zusammenfassen erhalten wir einen Beweis für Proposition 4.3.2.

Beweis von Proposition 4.3.2. (a) folgt aus Lemma 4.4.5. Lemma 4.4.6 zeigt (b) und die Aussage von (c) wurde in Lemma 4.4.7 bewiesen. □

Dies schließt den Beweis des Satzes 4.3.4 und damit das letzte Kapitel dieser Vorlesung ab.

Rückblick und Ausblick[41]

Vielen herzlichen Dank, dass Sie sich auf diesen Streifzug durch die Transzendente Zahlentheorie eingelassen haben. Ich hoffe Ihnen hat die Vorlesung genauso viel Spaß gemacht wie mir! Wir haben die-



se Vorlesung mit der Geschichte der Entdeckung der Irrationalität aus dem 5. Jahrhundert vor Christus begonnen und sind im letzten Kapitel der Vorlesung bei Themen der aktuellen Forschung angelangt. Natürlich konnten wir in dieser Vorlesung nur einen Bruchteil der Themen der Transzendenten Zahlentheorie anschneiden. Falls nun Ihr Interesse an transzendenten Zahlen geweckt ist, kann ich Ihnen nur wärmstens das Seminar „Transzendente Zahlen und Modulformen“, welches Lukas Prader im Wintersemester 2020/2021 betreuen wird, empfehlen[42]. Bei dieser Gelegenheit möchte ich nochmal Lukas für alle Unterstützung rund um diese Vorlesung und vor allem beim Übungsbetrieb danken. Ohne ihn wäre diese Vorlesung sicherlich nicht so geworden, wie sie es ist.

[40] S. Fischler, J. Sprang, and W. Zudilin. Many odd zeta values are irrational. *Compositio Mathematica*, 155(5):938–952, 2019. DOI: 10.1112/S0010437X1900722X

[41] Zu diesem Abschnitt gibt es ein Video:

[42] Sie finden die Seminarbeschreibung hier.

Literaturverzeichnis

P. Bundschuh. *Einführung in die Zahlentheorie*. Springer-Lehrbuch. [Springer Textbook]. Springer-Verlag, Berlin, second edition, 1992. ISBN 3-540-55178-6.

S. Fischler, J. Sprang, and W. Zudilin. Many odd zeta values are irrational. *Compositio Mathematica*, 155(5):938–952, 2019. DOI: 10.1112/S0010437X1900722X.

Eberhard Freitag and Rolf Busam. *Funktionentheorie*. Springer-Verlag, Berlin, 1993. ISBN 3-540-50618-7.

K. Königsberger. *Analysis. 1*. Springer-Lehrbuch. [Springer Textbook]. Springer-Verlag, Berlin, 1995. ISBN 3-540-52006-6.

F. Modler and M. Kreh. *Tutorium Algebra*. Springer Spektrum, 2018. ISBN 9783662586891.

Stefan Müller-Stach and Jens Piontkowski. *Elementare und algebraische Zahlentheorie*. Vieweg + Teubner, Wiesbaden, 2011. ISBN 978-3-8348-1256-8.