Manuskript zur Vorlesung
Ergänzungen zur Elementaren Zahlentheorie

gehalten von

Prof. Dr. D. WOLKE

im Wintersemester 2009/2010

an der

Dieses Manuskript wurde unter LaTeX gesetzt von

Dipl.–Math. S. FEILER

und basiert auf dem von M. GILG geTeXten
Manuskript zur Vorlesung Zahlentheorie II im Wintersemester 2003/04

Inhaltsverzeichnis

Literatur

Zu Kapitel 7 empfiehlt sich das Studium von „*Einführung in die analytische Zahlentheorie*“, J. BRÜDERN, Springer–Verlag (Berlin, Heidelberg, New York — 1995).

Zu Kapitel 8 findet man Literatur in „*Transzendental Number Theory (Second edition)*“, A. BAKER, Cambridge University Press (Cambridge — 1990) und „*Einführung in die Zahlentheorie (Second edition)*“, P. BUNDSCHUH, Springer–Verlag (Berlin — 1992).

Funktionentheoretische Begriffe und Ergebnisse

In Kapitel 7 werden einige Ergebnisse aus der Funktionentheorie verwendet.
Die Beweise können zum Beispiel in „*Funktionentheorie 1*“, E. FREITAG und R. BUSAM, Springer–Verlag (Berlin, Heidelberg, New York — 1993) nachvollzogen werden.

Definition 0.1 (Gebiete, Holomorphie und holomorphe Fortsetzungen)

a) $\mathcal{G} \subseteq \mathbb{C}$ heißt **Gebiet**, falls $\mathcal{G}$ nichtleer, offen und zusammenhängend ist.

b) Sind $\mathcal{G} \subseteq \mathbb{C}$ ein Gebiet, $f : \left\{ \begin{array}{ccc} \mathcal{G} & \to & \mathbb{C} \\ z & \mapsto & f(z) \end{array} \right\}$ und $z_0 \in \mathcal{G}$, so heißt f **in z_0 differenzierbar**, falls $\lim\limits_{\substack{z \to z_0 \\ z \in \mathcal{G}}} \dfrac{f(z) - f(z_0)}{z - z_0}$ existiert.

f heißt **auf $\mathcal{G}$ holomorph (analytisch, regulär)**, falls f für alle $z \in \mathcal{G}$ in z differenzierbar ist.

c) Sind $\mathcal{G} \subseteq \mathbb{C}$ und $\mathcal{H} \subseteq \mathbb{C}$ Gebiete mit $\mathcal{G} \subseteq \mathcal{H}$, sowie $f : \mathcal{G} \to \mathbb{C}$ holomorph auf $\mathcal{G}$ und $g : \mathcal{H} \to \mathbb{C}$, so heißt g **holomorphe (analytische) Fortsetzung von f auf $\mathcal{H}$**, falls g holomorph auf $\mathcal{H}$ ist und $f = g$ auf $\mathcal{G}$ gilt.

Lemma 0.2 (TAYLORentwickung holomorpher Funktionen)
VORAUSSETZUNGEN:
Seien $\mathcal{G} \subseteq \mathbb{C}$ ein Gebiet und $f : \mathcal{G} \to \mathbb{C}$ holomorph auf $\mathcal{G}$.

BEHAUPTUNG: *f ist um jedes $z \in \mathcal{G}$ im größtmöglichen Kreis um z, der ganz in $\mathcal{G}$ liegt* TAYLOR*–entwickelbar.*
Insbesondere ist f auf $\mathcal{G}$ beliebig oft differenzierbar.

SATZ 0.3 (Satz von WEIERSTRASS)
VORAUSSETZUNGEN:
Seien $\mathcal{G} \subseteq \mathbb{C}$ ein Gebiet und $f_n : \mathcal{G} \to \mathbb{C}$ für alle $n \in \mathbb{N}$ holomorph auf $\mathcal{G}$.
$\sum\limits_{n=1}^{\infty} f_n$ konvergiere kompakt auf $\mathcal{G}$ gegen ein $f : \mathcal{G} \to \mathbb{C}$.

BEHAUPTUNG: *Dann ist f holomorph auf $\mathcal{G}$ und $\sum\limits_{n=1}^{\infty} f_n'$ konvergiert kompakt gegen f'.*

Lemma 0.4 (Eindeutigkeit der holomorphen Fortsetzung)
VORAUSSETZUNGEN:
Seien $\mathcal{G} \subseteq \mathbb{C}$ und $\mathcal{H} \subseteq \mathbb{C}$ Gebiete mit $\mathcal{G} \subseteq \mathcal{H}$. Seien $f : \mathcal{G} \to \mathbb{C}$ holomorph auf $\mathcal{G}$ und $h : \mathcal{H} \to \mathbb{C}$ eine holomorphe Fortsetzung von f auf $\mathcal{H}$.

BEHAUPTUNG: *Jede holomorphe Fortsetzung von f auf $\mathcal{H}$ stimmt mit g überein.*
Damit ist die holomorphe Fortsetzung von f auf $\mathcal{H}$ durch f eindeutig bestimmt.

Folgerung 0.5 (Nullstellen)
VORAUSSETZUNGEN:
Seien $\mathcal{G} \subseteq \mathbb{C}$ ein Gebiet und $f : \mathcal{G} \to \mathbb{C}$ mit $f \neq 0$ holomorph auf $\mathcal{G}$.
BEHAUPTUNG: *Dann liegen die Nullstellen von f diskret in $\mathcal{G}$ und haben eine ganzzahlige Ordnung.*

0.6: Wegintegrale
VORAUSSETZUNGEN:
Seien $\mathcal{G} \subseteq \mathbb{C}$ ein Gebiet, $a \in \mathbb{R}$, $b \in \mathbb{R}$ mit $a < b$, $\mathcal{I} := [a; b]$, $\gamma : \left\{ \begin{array}{ccc} \mathcal{I} & \to & \mathcal{G} \\ t & \mapsto & \gamma(t) \end{array} \right\}$ stückweise stetig differenzierbar und $f : \left\{ \begin{array}{ccc} \mathcal{G} & \to & \mathbb{C} \\ z & \mapsto & f(z) \end{array} \right\}$ holomorph auf $\mathcal{G}$.
Für alle $(n, \nu)^T \in \mathbb{N}_0^2$ mit $\nu \leq n$ sei $t_{n,\nu} \in \mathcal{I}$ derart, dass

$$a = t_{n,0}, \qquad b = t_{n,n} \qquad \text{und} \qquad t_{n,\nu} < t_{n,\nu+1}$$

für alle $n \in \mathbb{N}_0$ und alle $\nu \in \mathbb{N}_0$ mit $\nu < n$ gelten.
Für alle $(n, \nu)^T \in \mathbb{N}_0^2$ mit $1 \leq \nu \leq n$ sei $\xi_{n,\nu} \in [t_{n,\nu-1}; t_{n,\nu}]$.
Sei $S_\cdot(f, \gamma, \mathcal{I}) : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & S_n(f, \gamma, \mathcal{I}) := \sum\limits_{\nu=1}^{n} f(\gamma(\xi_{n,\nu})) \cdot (\gamma(t_{n,\nu}) - \gamma(t_{n,\nu-1})) \end{array} \right\}$.
BEHAUPTUNG: *$(\gamma, \mathcal{I})$ definiert einen stückweise glatten Weg in $\mathcal{G}$.*
Die Folge $(S_n(f, \gamma, \mathcal{I}))_{n \in \mathbb{N}}$ konvergiert, falls $\lim\limits_{n \to \infty} \left(\max\limits_{\nu=1}^{n} (t_{n,\nu} - t_{n,\nu-1}) \right) = 0$ ist.
VORAUSSETZUNG: *Es gelte $\lim\limits_{n \to \infty} \left(\max\limits_{\nu=1}^{n} (t_{n,\nu} - t_{n,\nu-1}) \right) = 0$.*
Definition $\int\limits_{(\gamma,\mathcal{I})} f(z)\,\mathrm{d}z := \lim\limits_{n \to \infty} S_n(f, \gamma, \mathcal{I})$ heißt **Wegintegral von f über $(\gamma, \mathcal{I})$**.
BEHAUPTUNG:

$$\text{(i)} \quad \int\limits_{(\gamma,\mathcal{I})} f'(z)\,\mathrm{d}z = f(\gamma(b)) - f(\gamma(a))$$

$$\text{(ii)} \quad \left| \int\limits_{(\gamma,\mathcal{I})} f(z)\,\mathrm{d}z \right| \leq |(\gamma, \mathcal{I})| \cdot \max_{t \in \mathcal{I}} |f(\gamma(t))|$$

Satz 0.7 (Spezialfall des Cauchy'schen Integralsatzes)
Voraussetzungen:
Seien $\mathcal{G} \subseteq \mathbb{C}$ *ein Gebiet und* $f : \left\{ \begin{array}{ccc} \mathcal{G} & \to & \mathbb{C} \\ z & \mapsto & f(z) \end{array} \right\}$ *holomorph auf* $\mathcal{G}$.
Seien $\mathcal{H} \subseteq \mathcal{G}$ *konvex und* $z_0 \in \mathcal{H} \setminus \partial\mathcal{H}$.
Sei $\mathcal{W}$ *ein stückweise glatter Weg in* $\mathcal{G}$, *der* $\partial\mathcal{H}$ *einmal in mathematisch positivem Sinn durchläuft.*
Behauptung: *Es sind*

$$\int_{\mathcal{W}} f(z)\,\mathrm{d}z = 0 \qquad \textit{und} \qquad f(z_0) = \frac{1}{2\pi\mathrm{i}} \cdot \int_{\mathcal{W}} \frac{f(z)}{z - z_0}\,\mathrm{d}z.$$

Kapitel 7: Analytischer Beweis des Primzahlsatzes

Am Beispiel des Primzahlsatzes

$$\pi(x) = \#\{p \in \mathbb{P} |\, p \leq x\} = \frac{x}{\ln x} \cdot (1 + o(1))$$

beziehungsweise

$$\psi(x) = \sum_{n=1}^{\lfloor x \rfloor} \Lambda(n) = \sum_{\substack{(p,k)^T \in \mathbb{P} \times \mathbb{N} \\ p^k \leq x}} \ln(p) = x \cdot (1 + o(1))$$

soll das Grundprinzip der analytischen Zahlentheorie

a) elementar–zahlentheoretisches Problem (hier: asymptotische Formel für ψ)

b) Studium einer erzeugenden Funktion,
(hier der Dirichlet–Reihe $\displaystyle\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ mit $s \in \mathbb{C}$ und $\mathrm{Re}(s) > 1$)

c) Rückschluß von analytischen Eigenschaften der erzeugenden Funktion auf Eigenschaften von ψ

demonstriert werden. Der Schritt c) wird hier mit einem erst vor kurzem gefundenen, besonders elegantem Hilfsmittel, dem Newman'schen Tauber–Satz vollzogen.

Eine Reihe der Gestalt $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ mit $a_n \in \mathbb{C}$ für alle $n \in \mathbb{N}$ und $s \in \mathbb{C}$ wird als Dirichlet–Reihe bezeichnet. Die Wichtigste von allen, auf die sich viele andere zurückführen lassen, ist die Riemann'sche Zeta–Funktion (für reelle s schon von Euler benutzt, für komplexe s 1859 durch Riemann eingeführt).

Bemerkung 7.1 (Holomorphie der RIEMANN'schen ζ–Funktion)
Die Reihe $\sum_{n=1}^{\infty} \frac{1}{n^s}$ stellt eine für $s \in \mathbb{C}$ mit $\operatorname{Re}(s) > 1$ holomorphe Funktion dar.

BEWEIS:
In jeder Halbebene $\{ s \in \mathbb{C} | \operatorname{Re}(s) \geq 1 + \varepsilon \}$ mit $\varepsilon \in \mathbb{R}^+$ ist die Reihe $\sum_{n=1}^{\infty} \frac{1}{n^s}$ wegen

$$\left| \sum_{n=1}^{\infty} \frac{1}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^{1+\varepsilon}}$$

gleichmäßig konvergent.
Nach dem Satz von WEIERSTRASS 0.3 auf Seite 2 stellt sie eine in $\{ s \in \mathbb{C} | \operatorname{Re}(s) > 1 \}$ holomorphe Funktion dar. □

Definition 7.2 (RIEMANN'sche ζ–Funktion)

a) $\mathbb{H} := \{ s \in \mathbb{C} | \operatorname{Re}(s) > 1 \}$ ist die **rechte Halbebene in $\mathbb{C}$**.

b) Für $a : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & a_n \end{array} \right\}$ und $s \in \mathbb{C}$ heißt $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ **DIRICHLET–Reihe zu a an der Stelle s**.

c) $\zeta : \left\{ \begin{array}{ccc} \mathbb{H} & \to & \mathbb{C} \\ s & \mapsto & \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \end{array} \right\}$ heißt **RIEMANN'sche ζ–Funktion**.

SATZ 7.3 (Fortsetzbarkeit von ζ nach $\{ s \in \mathbb{C} | \operatorname{Re}(s) > 0 \}$)
BEHAUPTUNG: *Die Funktion* $f : \left\{ \begin{array}{ccc} \mathbb{H} & \to & \mathbb{C} \\ s & \mapsto & f(s) := \zeta(s) - \frac{1}{s-1} \end{array} \right\}$ *lässt sich in die Halbebene* $\{ s \in \mathbb{C} | \operatorname{Re}(s) > 0 \}$ *holomorph fortsetzen.*

oder

ζ *ist mit einen Pol erster Ordnung mit Residuum* 1 *an der Stelle* 1 *nach* $\{ s \in \mathbb{C} | \operatorname{Re}(s) > 0 \}$ *meromorph fortsetzbar.*

BEWEIS:
Für alle $N \in \mathbb{N} \setminus \{1\}$ und alle $s \in \mathbb{C}$ mit $\operatorname{Re}(s) > 0$ sieht man mit partieller Summation

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{n^s} &= \frac{N}{N^s} - \int_1^N \lfloor t \rfloor \cdot \frac{\mathrm{d}}{\mathrm{d}t} t^{-s} \, \mathrm{d}t \\ &= N^{1-s} + s \cdot \int_1^N t^{-s} \, \mathrm{d}t - s \cdot \int_1^N \frac{t - \lfloor t \rfloor}{t^{s+1}} \, \mathrm{d}t \\ &= \frac{1}{1-s} \cdot N^{1-s} + 1 + \frac{1}{s-1} - s \cdot \int_1^N \frac{t - \lfloor t \rfloor}{t^{s+1}} \, \mathrm{d}t.\end{aligned}$$

Im Grenzübergang $N \to \infty$ fällt der erste Summand rechts weg und das letzte Integral konvergiert für $\operatorname{Re}(s) > 0$ kompakt gleichmäßig gegen eine holomorphe Funktion I.
Damit folgt für alle $s \in \mathbb{H}$

$$\zeta(s) = \frac{1}{s-1} + (1 - s \cdot I(s)).$$

Durch den Klammerterm ist somit die holomorphe Fortsetzung von f in die Halbebene $\{ s \in \mathbb{C} | \operatorname{Re}(s) > 0 \}$ gefunden. □

Ab jetzt wird mit ζ die meromorphe Fortsetzung der ζ–Funktion nach $\{ s \in \mathbb{C} | \operatorname{Re}(s) > 0 \}$ bezeichnet.

SATZ 7.4 (Produktsatz für DIRICHLET–Reihen)
VORAUSSETZUNGEN:
Seien $f : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & f(n) \end{array} \right\}$ *und* $g : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & g(n) \end{array} \right\}$ *zahlentheoretische Funktionen.*
Sei $h : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & h(n) := (f * g)(n) \end{array} \right\}$ *das Faltprodukt von* f *und* g.
Die Reihen $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ *und* $\sum_{n=1}^{\infty} \frac{g(n)}{n^s}$ *seien für alle* $s \in \mathcal{D}$ *mit* $\mathcal{D} \subseteq \mathbb{C}$ *absolut konvergent.*

BEHAUPTUNG: *Dann ist für alle* $s \in \mathcal{D}$ *auch* $\sum_{n=1}^{\infty} \frac{h(n)}{n^s}$ *absolut konvergent und es gilt*

$$\sum_{n=1}^{\infty} \frac{h(n)}{n^s} = \left(\sum_{n=1}^{\infty} \frac{f(n)}{n^s} \right) \cdot \left(\sum_{n=1}^{\infty} \frac{g(n)}{n^s} \right).$$

BEWEIS:
Für jedes $s \in \mathcal{D}$ kann nach dem Produktsatz für unendliche Reihen wegen der absoluten Konvergenz wie folgt umgeformt werden:

$$\left(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\right) \cdot \left(\sum_{n=1}^{\infty} \frac{g(n)}{n^s}\right) = \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{f(m) \cdot g(n)}{(mn)^s}$$
$$= \sum_{k=1}^{\infty} \frac{1}{k^s} \cdot \sum_{\substack{(m,n)^T \in \mathbb{N}^2 \\ m \cdot n = k}} f(m) \cdot g(n) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}. \qquad \square$$

Beispiele 7.5 (Das Inverse und die logarithmische Ableitung von ζ)

(i) Für alle $s \in \mathbb{H}$ gilt

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

Insbesondere hat ζ in $\mathbb{H}$ keine Nullstelle.

(ii) Für alle $s \in \mathbb{H}$ gilt

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}.$$

Beide Reihen stellen in $\mathbb{H}$ holomorphe Funktionen dar.

BEWEIS:

(i) Inverses der ζ–Funktion

Wegen $|\mu(n)| \leq 1$ für alle $n \in \mathbb{N}$ liefert $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ eine in $\mathbb{H}$ absolut konvergente DIRICHLET–Reihe und holomorphe Funktion.
Mit Satz 7.4 auf der vorherigen Seite erhält man für alle $s \in \mathbb{H}$

$$\zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{k=1}^{\infty} \frac{(\mathbb{1} * \mu)(k)}{k^s} = \sum_{k=1}^{\infty} \frac{\varepsilon(k)}{k^s} = 1.$$

Hätte ζ in $\mathbb{H}$ eine Nullstelle, dann könnte die Identität nur gelten, wenn $\displaystyle\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ dort einen Pol hätte, was aber wegen der Holomorphie ausgeschlossen ist.

(ii) Logarithmische Ableitung von ζ
In $\mathbb{H}$ kann ζ gliedweise differenziert werden.
Wegen $\frac{\mathrm{d}}{\mathrm{d}s}n^{-s} = \frac{\mathrm{d}}{\mathrm{d}s}\mathrm{e}^{-s\cdot\ln(n)} = -\ln(n)\cdot n^{-s}$ ist für alle $s \in \mathbb{H}$

$$\zeta'(s) = -\sum_{n=1}^{\infty}\frac{\ln(n)}{n^s}.$$

Mit Satz 7.4, $\Lambda = \mu * \ln$ und (i) erhält man für alle $s \in \mathbb{H}$

$$\frac{1}{\zeta(s)}\cdot(-\zeta'(s)) = \left(\sum_{m=1}^{\infty}\frac{\mu(m)}{m^s}\right)\cdot\left(\sum_{n=1}^{\infty}\frac{\ln(n)}{n^s}\right) = \sum_{n=1}^{\infty}\frac{\Lambda(k)}{k^s}. \qquad \square$$

Die Bedeutung der ζ–Funktion für die Verteilung der Primzahlen wird auch deutlich durch ihr sogenanntes EULER–Produkt

$$\zeta(s) = \prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}} \qquad \text{für alle } s \in \mathbb{H}.$$

Die Gestalt der Reihe $\displaystyle\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}$ zeigt, dass für das analytische Verhalten der ζ–Funktion, insbesondere die analytische Fortsetzbarkeit nach links, das Nicht–Verschwinden der ζ–Funktion von entscheidender Bedeutung ist.
Schon die Aussage $\zeta(1+\mathrm{i}t) \neq 0$ für alle $t \in \mathbb{R}\setminus\{0\}$ erfordert Einiges an neuen Ideen. Bis heute ist kein einfacher Beweis hierfür bekannt.
Die folgende Methode geht auf DE LA VALLÉE–POUSSIN (1896) zurück.

SATZ 7.6 (Satz von HADAMARD und DE LA VALLÉE–POUSSIN)
BEHAUPTUNG: *Für alle $t \in \mathbb{R}\setminus\{0\}$ ist*

$$\zeta(1+\mathrm{i}t) \neq 0.$$

BEWEIS:

(i) Die zugrundeliegende cos–Identität
Für alle $\alpha \in \mathbb{R}$ gilt

$$3 + 4\cdot\cos(\alpha) + \cos(2\alpha) = 2\cdot(1+\cos(\alpha))^2 \geq 0.$$

(ii) Verbindung zur Logarithmischen Ableitung von ζ
Für alle $\sigma \in \mathbb{R}$ mit $\sigma > 1$ und alle $t \in \mathbb{R} \setminus \{0\}$ sieht man mit (i) und Beispiel 7.5 (ii) auf Seite 7

$$\begin{aligned}
&\operatorname{Re}\left(3 \cdot \frac{\zeta'(\sigma)}{\zeta(\sigma)} + 4 \cdot \frac{\zeta'(\sigma+\mathrm{i}t)}{\zeta(\sigma+\mathrm{i}t)} + \frac{\zeta'(\sigma+2\mathrm{i}t)}{\zeta(\sigma+2\mathrm{i}t)}\right) \\
&\quad = -\operatorname{Re}\left(\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma}} \cdot \left(3 + 4n^{-\mathrm{i}t} + n^{-2\mathrm{i}t}\right)\right) \\
&\quad = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{\sigma}} \cdot (3 + 4 \cdot \cos(-t \cdot \ln(n)) + \cos(-2t \cdot \ln(n))) \qquad \leq 0.
\end{aligned}$$

(iii) Folgerungen aus dem Verschwinden von $\zeta(1+\mathrm{i}t)$
Angenommen, es gebe ein $t \in \mathbb{R} \setminus \{0\}$ und ein $m \in \mathbb{N}$, so dass ζ bei $1+\mathrm{i}t$ mit m–ter Ordnung verschwindet. Sei $\ell \in \mathbb{N}_0$ die Ordnung, mit der ζ bei $1+2\mathrm{i}t$ verschwindet.
Dann gibt es ein $\delta \in \mathbb{R}^+$ und ein auf $(-\delta;\delta)$ differenzierbares $\tilde{h}_1 : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & \tilde{h}_1(x) \end{array} \right\}$ mit

$$\tilde{h}_1(0) \neq 0 \qquad \text{und} \qquad \zeta(\sigma+\mathrm{i}t) = (\sigma-1)^m \cdot \tilde{h}_1(\sigma-1)$$

für alle $\sigma \in \mathbb{R}$ mit $\sigma > 1$.
Damit folgt die Existenz eines $h_1 : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & h_1(x) \end{array} \right\}$ und eines $C_1 \in \mathbb{R}^+$ mit

$$\frac{\zeta'(\sigma+\mathrm{i}t)}{\zeta(\sigma+\mathrm{i}t)} = \frac{m}{\sigma-1} + h_1(\sigma-1)$$

für alle $\sigma \in \mathbb{R}$ mit $\sigma > 1$ und $|h_1(x)| \leq C_1$ für alle $x \in [0;1]$.
Analog sieht man die Existenz eines $h_2 : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & h_2(x) \end{array} \right\}$ und eines $C_2 \in \mathbb{R}^+$ mit

$$\frac{\zeta'(\sigma+2\mathrm{i}t)}{\zeta(\sigma+2\mathrm{i}t)} = \frac{\ell}{\sigma-1} + h_2(\sigma-1)$$

für alle $\sigma \in \mathbb{R}$ mit $\sigma > 1$ und $|h_2(x)| \leq C_2$ für alle $x \in [0;1]$.
Wegen des Pols bei 1 gibt es ein $h_0 : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & h_0(x) \end{array} \right\}$ und ein $C_0 \in \mathbb{R}^+$ mit

$$\frac{\zeta'(\sigma)}{\zeta(\sigma)} = \frac{-1}{\sigma-1} + h_0(\sigma-1)$$

für alle $\sigma \in \mathbb{R}$ mit $\sigma > 1$ und $|h_0(x)| \leq C_0$ für alle $x \in [0;1]$.

(iv) Beweis der Behauptung
Sei $C := C_1 + C_2 + C_0$. (ii) und (iii) liefern für alle $\sigma \in \mathbb{R}$ mit $1 < \sigma \leq 2$

$$0 \geq \operatorname{Re}\left(\frac{-3+4m+\ell}{\sigma-1} + h_1(\sigma-1) + h_2(\sigma-1) + h_0(\sigma-1)\right) \geq \frac{-3+4m+\ell}{\sigma-1} - C.$$

Im Grenzübergang $\sigma \to 1^+$ wird die rechte Seite wegen $m \geq 1$ und $\ell \geq 0$ beliebig groß und insbesondere positiv, was einen Widerspruch bedeutet. $\square$

Folgerung 7.7 (Fortsetzbarkeit von $\frac{\zeta'}{\zeta}$)

BEHAUPTUNG: *Die Funktion* $f : \left\{ \begin{array}{ccc} \mathbb{H} & \to & \mathbb{C} \\ s & \mapsto & f(s) := \dfrac{\zeta'(s)}{\zeta(s)} - \dfrac{1}{s-1} \end{array} \right\}$ *ist holomorph fortsetzbar in ein Gebiet, das die abgeschlossene Halbebene* $\{ s \in \mathbb{C} | \operatorname{Re}(s) \geq 1 \}$ *umfasst.*

BEWEIS:
Der Pol von ζ bei 1 bewirkt einen Pol erster Ordnung mit Residuum -1 von $\frac{\zeta'}{\zeta}$ bei 1.
Also ist f holomorph in eine Umgebung von 1 fortsetzbar.
Die Holomorphie in allen übrigen Punkten der 1–Geraden folgt aus dem Satz von HADAMARD und DE LA VALLÉE–POUSSIN 7.6 auf Seite 8. □

Die Aussage von Folgerung 7.7 wird sich als ausreichend für die Anwendung des NEWMAN'schen TAUBER–Satzes herausstellen.

Es ist oft einfacher, von der Koeffizientenfolge einer Potenz– oder DIRICHLET–Reihe auf die Eigenschaften der Reihe zu schließen, als umgekehrt. Ein kleines Beispiel:

Satz von ABEL
VORAUSSETZUNGEN:
Sei $a : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & a_n \end{array} \right\}$ *eine komplexe Zahlenfolge, für die* $\sum_{n=1}^{\infty} a_n$ *gegen ein* $a \in \mathbb{C} \setminus \{0\}$ *konvergiert.*
Die Potenzreihe $\sum_{n=1}^{\infty} a_n \cdot z^n$ *konvergiere für alle* $z \in \mathbb{C}$ *mit* $|z| < 1$.

BEHAUPTUNG: *Dann ist die Funktion* $A : \left\{ \begin{array}{ccc} (-1;1) & \to & \mathbb{C} \\ t & \mapsto & A(t) := \sum_{n=1}^{\infty} a_n \cdot t^n \end{array} \right\}$ *stetig in den Punkt* $t := 1$ *fortsetzbar und hat dort den Wert* a.

(ohne BEWEIS)

Die Umkehrung (aus der Stetigkeit der Funktion auf die Konvergenz der Reihe zu schließen) ist nur unter Zusatzbedingungen möglich.
Sätze, in denen aus dem Stetigkeits– oder Holomorphieverhalten, insbesondere am Rand des Konvergenzbereichs einer Reihe, auf das Grenzwertverhalten der Koeffizienten geschlossen wird, heißen „TAUBER–Sätze“ (benannt nach Alfred TAUBER, 1866–1942, umgekommen im KZ Theresienstadt).

Der 1980 von Donald J. NEWMAN gefundene TAUBER–Satz kommt mit wenig einschneidenden Bedingungen aus und ist für LAPLACE–Transformierte formuliert.

SATZ 7.8 (NEWMAN'scher TAUBER–Satz)
VORAUSSETZUNG: *Sei* $f : \left\{ \begin{array}{rcl} \mathbb{R}^+ \cup \{0\} & \to & \mathbb{C} \\ x & \mapsto & f(x) \end{array} \right\}$ *beschränkt und für alle* $a \in \mathbb{R}^+ \cup \{0\}$ *auf dem Intervall* $[0; a]$ RIEMANN–*integrierbar.*
BEHAUPTUNG: *Dann stellt die* LAPLACE–*Transformierte von* f

$$F : \left\{ \begin{array}{rcl} \{ w \in \mathbb{C} | \operatorname{Re}(w) > 0 \} & \to & \mathbb{C} \\ z & \mapsto & F(z) := \int\limits_0^\infty f(t) \cdot \mathrm{e}^{-zt} \, \mathrm{d}t \end{array} \right\}$$

eine holomorphe Funktion dar.
Ist F *analytisch fortsetzbar in ein Gebiet, das die imaginäre Achse umfasst,*

$$\textit{so existiert} \qquad \int\limits_0^\infty f(t) \, \mathrm{d}t \qquad \textit{und hat den Wert } F(0) .$$

BEWEIS:

(i) Umformulierung
Für alle $\lambda \in \mathbb{R}^+$ ist

$$F_\lambda : \left\{ \begin{array}{rcl} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & F_\lambda(z) := \int\limits_0^\lambda f(t) \cdot \mathrm{e}^{-zt} \, \mathrm{d}t \end{array} \right\}$$

offenbar eine auf ganz $\mathbb{C}$ holomorphe Funktion. Es reicht zu zeigen, dass

$$\lim_{\lambda \to \infty} F_\lambda(0) = \lim_{\lambda \to \infty} \int\limits_0^\lambda f(t) \, \mathrm{d}t = F(0)$$

ist, bzw., dass es für alle $\delta \in \mathbb{R}^+$ ein $\lambda_0(\delta) \in \mathbb{R}^+$ mit

$$|F_\lambda(0) - F(0)| < \delta$$

für alle $\lambda \in \mathbb{R}^+$ mit $\lambda \geq \lambda_0(\delta)$ gibt.

(ii) Anwenden der CAUCHY'schen Integralformel
Für alle $R \in \mathbb{R}^+$ (später wird in Abhängigkeit von δ ein genügend großes R gewählt werden) gibt es nach der Voraussetzung ein $\eta_R \in \mathbb{R}^+$, so das F holomorph ist auf

$$\{ z \in \mathbb{C} | \operatorname{Re}(z) \geq -\eta_R \text{ und } |\operatorname{Im}(z)| \leq R \} .$$

Für alle $R \in \mathbb{R}^+$ sei $\mathcal{W}_R$ der folgende geschlossene, in mathematisch positivem Sinn durchlaufene Weg:

- Der Halbkreis vom Radius R um 0 in der Halbebene $\{ s \in \mathbb{C} | \operatorname{Re}(s) > 0 \}$ $\left(\mathcal{W}_R^+\right)$.
- Der Rechteckweg von $\mathrm{i}R$ über $(\mathrm{i}R - \eta_R)$ und $(-\mathrm{i}R - \eta_R)$ nach $-\mathrm{i}R$ $\left(\mathcal{W}_R^-\right)$.

Dann bewirkt die CAUCHY'schen Integralformel 0.7 auf Seite 3 für alle $R \in \mathbb{R}^+$ und alle $\lambda \in \mathbb{R}^+$

$$F(0) - F_\lambda(0) = \frac{1}{2\pi\mathrm{i}} \cdot \int\limits_{\mathcal{W}_R} (F(z) - F_\lambda(z)) \cdot \mathrm{e}^{\lambda z} \cdot \left(\frac{1}{z} + \frac{z}{R^2}\right) \mathrm{d}z. \tag{7.1}$$

Die Verwendung dieses Integranden ist als der eigentliche Beweistrick anzusehen. Er erlaubt es, das Integral auf $\mathcal{W}_R$ mit $R \in \mathbb{R}^+$ gut abzuschätzen. Die Standard–Anwendung der CAUCHY'schen Formel mit dem Integranden $\frac{F(z)-F_\lambda(z)}{z}$ würde zu Schwierigkeiten führen.

(iii) Beitrag des Integrals über $\mathcal{W}_R^+$
Nach Voraussetzung gibt es ein $C \in \mathbb{R}^+$ mit

$$|f(t)| \leq C \qquad \text{für alle } t \in \mathbb{R}^+ \cup \{0\}.$$

Für alle $R \in \mathbb{R}^+$, alle $\lambda \in \mathbb{R}^+$ und alle $z \in \mathbb{C}$ mit $x := \operatorname{Re}(z) > 0$, $y := \operatorname{Im}(z)$ und $|z| = R$ sind

$$\frac{1}{z} + \frac{z}{R^2} = \frac{x - \mathrm{i}y}{x^2 + y^2} + \frac{x + \mathrm{i}y}{R^2} = \frac{2x}{R^2}$$

und

$$|F(z) - F_\lambda(z)| = \left| \int\limits_\lambda^\infty f(t) \cdot \mathrm{e}^{-zt}\, \mathrm{d}t \right| \leq C \cdot \int\limits_\lambda^\infty \mathrm{e}^{-xt}\, \mathrm{d}t = \frac{C}{x} \cdot \mathrm{e}^{-\lambda x}.$$

Damit lässt sich der Integrand in (7.1) für alle $R \in \mathbb{R}^+$, alle $\lambda \in \mathbb{R}^+$ und alle $z \in \mathbb{C}$ mit $\operatorname{Re}(z) > 0$ und $|z| = R$ im Betrag abschätzen durch

$$\left| (F(z) - F_\lambda(z)) \cdot \mathrm{e}^{\lambda z} \cdot \left(\frac{1}{z} + \frac{z}{R^2}\right) \right| \leq \frac{C}{\operatorname{Re}(z)} \cdot \mathrm{e}^{-\lambda \cdot \operatorname{Re}(z)} \cdot \mathrm{e}^{\lambda \cdot \operatorname{Re}(z)} \cdot \frac{2 \cdot \operatorname{Re}(z)}{R^2} = \frac{2C}{R^2}.$$

Dies ergibt für alle $R \in \mathbb{R}^+$

$$\left| \frac{1}{2\pi\mathrm{i}} \cdot \int\limits_{\mathcal{W}_R^+} (F(z) - F_\lambda(z)) \cdot \mathrm{e}^{\lambda z} \cdot \left(\frac{1}{z} + \frac{z}{R^2}\right) \mathrm{d}z \right| \leq \frac{C}{R}. \tag{7.2}$$

(iv) Beitrag des Integrals zu F_λ über $\mathcal{W}_R^-$
Da der Integrand in (7.1), wenn man $F(z)$ weglässt, für alle $\lambda \in \mathbb{R}^+$ in $\mathbb{C} \setminus \{0\}$ holomorph ist, kann man unter Berücksichtigung der CAUCHY'schen Integralformel 0.7 bei der Betrachtung des Beitrags des Integrals zu F_λ über $\mathcal{W}_R^-$ für alle $R \in \mathbb{R}^+$ den Weg $\mathcal{W}_R^-$ zu dem

Halbkreis vom Radius R in der Halbebene $\{ s \in \mathbb{C} | \operatorname{Re}(s) < 0 \}$ deformieren, ohne den Wert des Integrals zu verändern.
Wie in (7.2) erhält man für alle $\lambda \in \mathbb{R}$ und alle $z \in \mathbb{C}$ mit $\operatorname{Re}(z) < 0$

$$|F_\lambda(z)| \leq C \cdot \int_0^\lambda \mathrm{e}^{-xt}\,\mathrm{d}t < \frac{C \cdot e^{-\lambda \cdot \operatorname{Re}(z)}}{|\operatorname{Re}(z)|}$$

und damit ergibt sich für alle $R \in \mathbb{R}^+$ und alle $\lambda \in \mathbb{R}^+$

$$\left| \frac{1}{2\pi\mathrm{i}} \cdot \int_{\mathcal{W}_R^-} (-F_\lambda(z)) \cdot \mathrm{e}^{\lambda z} \cdot \left(\frac{1}{z} + \frac{z}{R^2} \right) \mathrm{d}z \right| \leq \frac{C}{R}. \tag{7.3}$$

(v) Beitrag des Integrals zu F über $\mathcal{W}_R^-$
Für alle $R \in \mathbb{R}^+$ sei

$$\mathcal{K}_R := \{ \sigma + \varsigma \mathrm{i}R \in \mathbb{C} | \, \sigma \in [-\eta_R; 0] \text{ und } \varsigma \in \{-1; 1\} \} \cup \{ -\eta_R + \mathrm{i}t \in \mathbb{C} | \, t \in [-R; R] \}.$$

$\mathcal{K}_R$ stimmt für alle $R \in \mathbb{R}^+$ mit der Punktmenge von $\mathcal{W}_R^-$ überein.
Für alle $R \in \mathbb{R}^+$ ist $\mathcal{K}_R$ kompakt und der Integrand in (7.1) ist, wenn man alle Terme, in denen ein „λ“ auftaucht, weglässt, auf $\mathcal{K}_R$ stetig und damit beschränkt.
Also gibt es für alle $R \in \mathbb{R}^+$ ein $B_R \in \mathbb{R}^+$ mit

$$\left| F(z) \cdot \left(\frac{1}{z} + \frac{z}{R^2} \right) \right| \leq B_R$$

für alle $z \in \mathcal{K}_R$.
Für alle $R \in \mathbb{R}^+$ sei $\mathcal{W}_{R,1}^-$ der Weg von $\mathrm{i}R$ nach $(-\eta_R + \mathrm{i}R)$, $\mathcal{W}_{R,2}^-$ der Weg von $(-\eta_R + \mathrm{i}R)$ nach $(-\eta_R - \mathrm{i}R)$ und $\mathcal{W}_{R,3}^-$ der Weg von $(-\eta_R - \mathrm{i}R)$ nach $-\mathrm{i}R$.
Für alle $R \in \mathbb{R}^+$ und alle $\lambda \in \mathbb{R}^+$ gilt daher für das F–Integral über die Vertikale $\mathcal{W}_{R,2}^-$

$$\left| \frac{1}{2\pi\mathrm{i}} \cdot \int_{\mathcal{W}_{R,2}^-} F(z) \cdot \mathrm{e}^{\lambda z} \cdot \left(\frac{1}{z} + \frac{z}{R^2} \right) \mathrm{d}z \right| \leq \frac{RB_R \cdot \mathrm{e}^{-\eta_R \cdot \lambda}}{\pi}. \tag{7.4}$$

Für alle $R \in \mathbb{R}^+$, alle $\lambda \in \mathbb{R}^+$ und alle $j \in \{1; 3\}$ ist das Integral über die Horizontale $\mathcal{W}_{R,j}^-$ beschränkt durch

$$\left| \frac{1}{2\pi\mathrm{i}} \cdot \int_{\mathcal{W}_{R,j}^-} F(z) \cdot \mathrm{e}^{\lambda z} \cdot \left(\frac{1}{z} + \frac{z}{R^2} \right) \mathrm{d}z \right| \leq \frac{B_R}{2\pi} \cdot \int_{-\eta_R}^0 \mathrm{e}^{\lambda x}\,\mathrm{d}x < \frac{B_R}{2\pi\lambda}. \tag{7.5}$$

(vi) Wahl von R und λ_0
Die Zusammenfassung von (7.2), (7.3), (7.4) und (7.5) liefert wegen (7.1) für beliebiges $R \in \mathbb{R}^+$ und beliebiges $\lambda \in \mathbb{R}^+$

$$|F(0) - F_\lambda(0)| < \frac{2C}{R} + B_R \cdot \left(\frac{R \cdot \mathrm{e}^{-\eta_R \cdot \lambda}}{\pi} + \frac{1}{\pi\lambda} \right).$$

Sei $\delta \in \mathbb{R}^+$.
Es werde als erstes $R(\delta) \in \mathbb{R}$ mit

$$R(\delta) > \frac{4C}{\delta}$$

gewählt. Für jetzt festgehaltenes $R(\delta)$ (und damit fixe $\eta_{R(\delta)}$ und $B_{R(\delta)}$) gilt

$$\lim_{\lambda \to \infty} \left(\frac{R(\delta) \cdot \mathrm{e}^{-\eta_{R(\delta)} \cdot \lambda}}{\pi} + \frac{1}{\pi\lambda} \right) = 0.$$

Deshalb gibt es ein $\lambda_0(\delta)$, so dass

$$B_{R(\delta)} \cdot \left(\frac{R(\delta) \cdot \mathrm{e}^{-\eta_{R(\delta)} \cdot \lambda}}{\pi} + \frac{1}{\pi\lambda} \right) \leq \frac{\delta}{2}$$

für alle $\lambda \in \mathbb{R}^+$ mit $\lambda \geq \lambda_0(\delta)$ ist.
Damit ist nach (i) der Beweis geführt. □

Es ist nun nicht mehr weit bis zum Ziel des Kapitels:

Satz 7.9 (Primzahlsatz)
Behauptung: *Es sind*

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1 \qquad \textit{und} \qquad \lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

Die ψ–Aussage wird bewiesen und zum Schluss wird die π–Aussage gefolgert.

Beweis:

(i) Integraldarstellung der Logarithmischen Ableitung von ζ
Für alle $s \in \mathbb{H}$ und alle $N \in \mathbb{N}$ folgt mit partieller Summation

$$\sum_{n=1}^{N} \frac{\Lambda(n)}{n^s} = \frac{\psi(N)}{N^s} + s \cdot \int_1^N \frac{\psi(u)}{u^{s+1}} \, \mathrm{d}u.$$

Für alle $s \in \mathbb{H}$ und alle $N \in \mathbb{N}$ folgt durch die Substitution $t = \ln(u)$

$$\sum_{n=1}^{N} \frac{\Lambda(n)}{n^s} = \frac{\psi(N)}{N^s} + s \cdot \int_0^{\ln(N)} \frac{\psi(\mathrm{e}^t)}{\mathrm{e}^{t \cdot (s+1)}} \cdot \mathrm{e}^t \, \mathrm{d}t.$$

Im Grenzübergang $N \to \infty$ geht für alle $s \in \mathbb{H}$ wegen $\psi(N) = O(N)$ (siehe den Satz von Чебышёв[†] — Satz 6.3 im Manuskript zur Vorlesung Elementaren Zahlentheorie aus dem Sommersemester 2009) und $\operatorname{Re}(s) > 1$ der Term $\frac{\psi(N)}{N^s}$ gegen Null, $\sum_{n \le N} \frac{\Lambda(n)}{n^s}$ wird nach Beispiel 7.5 (ii) auf Seite 7 zu $-\frac{\zeta'(s)}{\zeta(s)}$ und das Integral konvergiert.
Damit folgt für alle $s \in \mathbb{H}$

$$-\frac{\zeta'(s)}{\zeta(s)} \cdot \frac{1}{s} = \int_0^\infty \frac{\psi(\mathrm{e}^t)}{\mathrm{e}^t} \cdot \mathrm{e}^{-t\cdot(s-1)}\,\mathrm{d}t$$

und mit $z = s - 1$, folgt hieraus für alle $z \in \mathbb{C}$ mit $\operatorname{Re}(z) > 0$

$$-\frac{1}{z+1} \cdot \frac{\zeta'(z+1)}{\zeta(z+1)} = \int_0^\infty \frac{\psi(\mathrm{e}^t)}{\mathrm{e}^t} \cdot \mathrm{e}^{-tz}\,\mathrm{d}t.$$

(ii) Integraldarstellung von ζ
In ähnlicher Weise sieht man für alle $z \in \mathbb{C}$ mit $\operatorname{Re}(z) > 0$

$$\frac{1}{z+1} \cdot \zeta(z+1) = \int_0^\infty \frac{\lfloor \mathrm{e}^t \rfloor}{\mathrm{e}^t} \cdot \mathrm{e}^{-tz}\,\mathrm{d}t.$$

(iii) Anwendung des Newman'schen Tauber–Satzes 7.8
Nach Satz 7.3 auf Seite 5 und Folgerung 7.7 auf Seite 10 ist

$$F : \left\{ \begin{array}{rcl} \{ s \in \mathbb{C} | \operatorname{Re}(s) > 0 \} & \to & \mathbb{C} \\ z & \mapsto & F(z) := \frac{1}{z+1} \cdot \left(-\frac{\zeta'(z+1)}{\zeta(z+1)} - \zeta(z+1) \right) \end{array} \right\}$$

holomorph auf ein Gebiet fortsetzbar, das $\{ s \in \mathbb{C} | \operatorname{Re}(s) \ge 0 \}$ umfasst.
Wegen $\psi(\mathrm{e}^t) = O(\mathrm{e}^t)$ für alle $t \in \mathbb{R}^+ \cup \{0\}$ ist $\left\{ \begin{array}{rcl} \mathbb{R}^+ \cup \{0\} & \to & \mathbb{R} \\ t & \mapsto & \frac{\psi(\mathrm{e}^t) - \lfloor \mathrm{e}^t \rfloor}{\mathrm{e}^t} \end{array} \right\}$ beschränkt (und offenbar auf jedem Intervall Riemann–integrierbar).
Es kann der Newman'sche Tauber–Satz 7.8 auf Seite 11 angewandt werden:

$$\int_0^\infty \frac{\psi(\mathrm{e}^t) - \lfloor \mathrm{e}^t \rfloor}{\mathrm{e}^t}\,\mathrm{d}t \qquad \text{konvergiert.}$$

Ersetzt man $\lfloor \mathrm{e}^t \rfloor$ durch $\mathrm{e}^t - (\mathrm{e}^t - \lfloor \mathrm{e}^t \rfloor)$ und berücksichtigt die Konvergenz von $\int_0^\infty \frac{\mathrm{e}^t - \lfloor \mathrm{e}^t \rfloor}{\mathrm{e}^t}\,\mathrm{d}t$, so folgt, dass

$$\int_0^\infty \left(\frac{\psi(\mathrm{e}^t)}{\mathrm{e}^t} - 1 \right) \mathrm{d}t \qquad \text{konvergiert.} \tag{7.6}$$

[†]sprich: Chebyshev

(iv) Beweis der ψ–Aussage

Aus (7.6) folgt $\lim\limits_{t\to\infty}\dfrac{\psi\left(\mathrm{e}^t\right)}{\mathrm{e}^t}=1$:
Es werde zum Beispiel

$$\limsup_{t\to\infty}\frac{\psi\left(\mathrm{e}^t\right)}{\mathrm{e}^t}>1 \qquad \text{angenommen.}$$

Dies bedeutet, dass es eine gegen ∞ divergierende Folge $t:\ \left\{\begin{array}{ccc}\mathbb{N}&\to&\mathbb{R}\\ n&\mapsto&t_n\end{array}\right\}$ und ein $\delta\in\mathbb{R}^+$ mit

$$\psi\left(\mathrm{e}^{t_n}\right)\geq \mathrm{e}^{t_n}\cdot(1+\delta) \qquad \text{für alle } n\in\mathbb{N}$$

gibt. Für alle $c\in\mathbb{R}^+$ folgt daraus für jedes $n\in\mathbb{N}$

$$\int\limits_{t_n}^{t_n+c}\left(\frac{\psi\left(\mathrm{e}^t\right)}{\mathrm{e}^t}-1\right)\mathrm{d}t\geq\int\limits_{t_n}^{t_n+c}\left(\frac{\mathrm{e}^{t_n}\cdot(1+\delta)}{\mathrm{e}^{t_n+c}}-1\right)\mathrm{d}t=c\left(\frac{1+\delta}{\mathrm{e}^c}-1\right).$$

Wählt man $c_\delta\in\mathbb{R}^+$ mit $c_\delta\leq\ln\left(1+\frac{\delta}{2+\delta}\right)$, so folgt für alle $n\in\mathbb{N}$

$$\int\limits_{t_n}^{t_n+c_\delta}\left(\frac{\psi\left(\mathrm{e}^t\right)}{\mathrm{e}^t}-1\right)\mathrm{d}t\geq\frac{\delta c_\delta}{2}.$$

Wegen der Konvergenz des Integrals in (7.6) müsste $\lim\limits_{n\to\infty}\int\limits_{t_n}^{t_n+c_\delta}\left(\dfrac{\psi\left(\mathrm{e}^t\right)}{\mathrm{e}^t}-1\right)\mathrm{d}t=0$ gelten.

Ähnlich argumentiert man bei der Annahme $\liminf\limits_{t\to\infty}\dfrac{\psi\left(\mathrm{e}^t\right)}{\mathrm{e}^t}<1$.

Damit ist der Primzahlsatz in der ψ–Version gezeigt.

(v) Übergang von ψ zu π

Seien $\mathcal{D}:=\{w\in\mathbb{R}|\,w\geq1\}$ und $x\in\mathbb{R}$ mit $x\geq1$. Wegen

$$0\leq\sum_{\substack{(p,k)^T\in\mathbb{P}\times\mathbb{N}\\ k\geq2\text{ und }p^k\leq x}}\ln(p)=\sum_{\substack{p=2\\ p\in\mathbb{P}}}^{\lfloor\sqrt{x}\rfloor}\ln(p)\cdot\sum_{k=2}^{\lfloor\frac{\ln(x)}{\ln(p)}\rfloor}1\leq\sum_{\substack{p=2\\ p\in\mathbb{P}}}^{\lfloor\sqrt{x}\rfloor}\ln(p)\cdot\frac{\ln(x)}{\ln(p)}\leq\sqrt{x}\cdot\ln(x)=o(x)$$

gilt für $\vartheta:\ \left\{\begin{array}{ccc}\mathcal{D}&\to&\mathbb{R}\\ y&\mapsto&\vartheta(y):=\displaystyle\sum_{\substack{p=2\\ p\in\mathbb{P}}}^{\lfloor y\rfloor}\ln(p)\end{array}\right\}$

$$\vartheta(x)=\psi(x)-\sum_{\substack{(p,k)^T\in\mathbb{P}\times\mathbb{N}\\ k\geq2\text{ und }p^k\leq x}}\ln(p)=x+o(x)$$

nach dem oben Bewiesenen.
Es gibt also eine Funktion $\eta: \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ y & \mapsto & \eta(y) \end{array} \right\}$ mit $\lim\limits_{y\to\infty} \eta(y) = 0$ und

$$\vartheta(x) = x + \eta(x) \cdot x. \tag{7.7}$$

$\pi(x) = \sum\limits_{\substack{p=2 \\ p\in\mathbb{P}}}^{\lfloor x \rfloor} \ln(p) \cdot \dfrac{1}{\ln(p)}$ kann daraus durch partielle Summation bestimmt werden.

Seien

$$f: \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{R} \\ n & \mapsto & f(n) := \begin{cases} \ln(n), & \text{für } n \in \mathbb{P} \\ 0, & \text{sonst} \end{cases} \end{array} \right\}, \; F: \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ t & \mapsto & F(t) := \sum\limits_{n=1}^{\lfloor t \rfloor} f(n) \end{array} \right\}$$

und

$$g: \left\{ \begin{array}{ccc} \mathcal{D} & \to & \mathbb{R} \\ t & \mapsto & g(t) := \left\{ \begin{array}{l} \dfrac{1}{\ln(t)}, \quad \text{falls } t > 2 \text{ ist} \\ \text{irgendwie stetig differenzierbar bis } t = 1 \text{ fortgesetzt} \end{array} \right. \end{array} \right\}$$

Für alle $t \in \mathcal{D}$ ist

$$F(t) = \vartheta(t) = \begin{cases} 0, & \text{falls } 1 \le t < 2 \text{ ist,} \\ t + t \cdot \eta(t) & \text{falls } t \ge 2 \text{ ist.} \end{cases}$$

Mit partieller Summation erhält man

$$\pi(x) = \frac{\vartheta(x)}{\ln(x)} + \int_2^x \vartheta(t) \cdot \frac{1}{t \cdot \ln^2(t)} \, \mathrm{d}t. \tag{7.8}$$

Im Integral kann für alle $t \in \mathbb{R}$ grob durch $|\vartheta(t)| \le Ct$ mit einem $C \in \mathbb{R}^+$ abgeschätzt werden. Man erhält für das Integral die Betragsschranke

$$\left| \int_2^x \frac{\vartheta(t)}{t \cdot \ln^2(t)} \, \mathrm{d}t \right| \le C \cdot \int_2^x \frac{1}{\ln^2(t)} \, \mathrm{d}t \le C \left(\int_2^{\sqrt{x}} \frac{1}{\ln^2(2)} \, \mathrm{d}t + \int_{\sqrt{x}}^x \frac{1}{\ln^2(\sqrt{x})} \, \mathrm{d}t \right) = O\left(\frac{x}{\ln^2(x)} \right).$$

Mit (7.7) und (7.8) ergibt das

$$\pi(x) = \frac{x}{\ln(x)} + \eta(x) \cdot \frac{x}{\ln(x)} + O\left(\frac{x}{\ln^2(x)} \right) = \frac{x}{\ln(x)} + o\left(\frac{x}{\ln(x)} \right)$$

wie behauptet. □

Kapitel 8: Algebraische und transzendente Zahlen

Definition 8.1 (Algebraische Zahlen)

a) Für einen kommutativen, Nullteiler–freien Ring $\mathcal{R}$ mit Einselement und $n \in \mathbb{N}$ bezeichne $\mathcal{R}[x_1, \ldots, x_n]$ den **Ring der Polynome über $\mathcal{R}$ in n Unbestimmten** $x_1, \ldots, x_n$.

b) Ein Polynom $f : \left\{ \begin{array}{ccc} \mathcal{R} & \to & \mathcal{R} \\ x & \mapsto & f(x) := \sum_{\ell=0}^{n} a_\ell \cdot x^\ell \end{array} \right\}$ mit $n \in \mathbb{N}$ mit $a_\ell \in \mathcal{R}$ für alle $\ell \in \mathbb{N}_0$ mit $\ell \leq n$ und $a_n \neq 0$ heißt **normiert**, wenn der Leitkoeffizient $a_n = 1$ ist.

c) $\alpha \in \mathbb{C}$ heißt **algebraisch(e Zahl)**, wenn es ein Polynom $f \in \mathbb{Q}[x] \setminus \{0\}$ gibt, das an der Stelle α verschwindet.

Ist $\mathcal{R}$ ein Körper, dann kann jedes $f \in \mathcal{R}[x]$ mit nicht–verschwindendem Leitkoeffizienten normiert werden.

Folgerung 8.2 (Existenz und Eindeutigkeit des Minimalpolynoms)
Voraussetzung: *Sei $\alpha \in \mathbb{C}$ algebraisch.*

Behauptung: *Dann existiert ein eindeutig bestimmtes, über $\mathbb{Q}$ irreduzibles und normiertes Polynom $p \in \mathbb{Q}[x] \setminus \{0\}$, das an der Stelle α verschwindet.*

Beweis:

(i) Existenz
Es gibt ein Polynom $f \in \mathbb{Q}[x] \setminus \{0\}$, das α als Nullstelle hat. Ist f irreduzibel über $\mathbb{Q}$, so ist das gesuchte Polynom bereits gefunden.
Ist f nicht irreduzibel über $\mathbb{Q}$, so zerfällt es wegen der Nullteilerfreiheit von $\mathbb{Q}$ in zwei Polynome, von denen eines wiederum an der Stelle α verschwindet.
So arbeitet man sich weiter vor, bis man über $\mathbb{Q}$ irreduzibles Polynom gefunden hat, das α als Nullstelle hat. Da $\mathbb{Q}$ ein Körper ist, kann dieses normiert werden.

(ii) Eindeutigkeit
Sei $p \in \mathbb{Q}[x] \setminus \{0\}$ ein normiertes Polynom minimalen Grades, das an der Stelle α verschwindet. p ist damit über $\mathbb{Q}$ irreduzibel.
Sei $q \in \mathbb{Q}[x] \setminus \{0\}$ ein normiertes und über $\mathbb{Q}$ irrduzibles Polynom, das an der Stelle α verschwindet.
Da $\mathbb{Q}$ Körper ist, kann in $\mathbb{Q}[x]$ Polynomdivision durchgeführt werden und es gibt Polynome $a \in \mathbb{Q}[x]$ und $r \in \mathbb{Q}[x]$ mit

$$q = ap + r \qquad \text{und} \qquad \deg(r) < \deg(p).$$

Wegen $q = ap+r$ und des Veschwindens von p und q an der Stelle α ist α also auch Nullstelle von r. Wäre r nicht das Nullpolynom, hätte man einen Widerspruch zur Minimalität des Grades von p.
Also gilt $q = ap$ und wegen Irreduzibilität und Normiertheit von p und q bleibt nur $p = q$. □

Definition 8.3 (Minimalpolynom und ganz–algebraische Zahlen)

a) Für ein algebraisches $\alpha \in \mathbb{C}$ heißt das über $\mathbb{Q}$ irreduzible und normierte Polynom, das an der Stelle α verschwindet, **Minimalpolynom von $\boldsymbol{\alpha}$**.

b) $\alpha \in \mathbb{C}$ heißt **algebraisch vom Grad $\boldsymbol{n}$**, wenn das Minimalpolynom von α Grad $n \in \mathbb{N}$ hat.

c) Die algebraische Zahl $\alpha \in \mathbb{C}$ heißt **ganz–algebraisch**, wenn das Minimalpolynom in $\mathbb{Z}[x]$ liegt.

Beispiele für ganz–algebraische Zahlen:

- Die $\alpha \in \mathbb{Z}$ sind genau die ganz–algebraischen Zahlen vom Grad 1.
- $\sqrt{2}$ ist ganz–algebraisch vom Grad 2.

Folgerung 8.4
BEHAUPTUNG: *Ist $\alpha \in \mathbb{C}$ algebraisch, so existiert ein $d \in \mathbb{N}$, so dass $d\alpha$ ganz–algebraisch ist.*

BEWEIS:
Seien $\alpha \in \mathbb{C}$ algebraisch, $n \in \mathbb{N}$ und $a_\ell \in \mathbb{Q}$ für alle $\ell \in \mathbb{N}_0$ mit $\ell < n$ derart, dass $p : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & p(x) := x^n + \sum_{\ell=0}^{n-1} a_\ell \cdot x^\ell \end{array} \right\}$ das Minimalpolynom von α ist.
Man wähle als $d \in \mathbb{N}$ das kgV der Nenner der Zahlen a_ℓ mit $\ell \in \mathbb{N}$ und $\ell < n$.
Dann ist

$$d^n \cdot p(\alpha) = (d\alpha)^n + da_{n-1} \cdot (d\alpha)^{n-1} + \ldots + d^{n-1}a_1 \cdot (d\alpha) + d^n a_0.$$

Die Koeffizienten von $q : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & q(x) := x^n + \sum_{\ell=0}^{n-1} d^\ell a_\ell \cdot x^\ell \end{array} \right\}$ liegen in $\mathbb{Z}$. Mit p ist auch q irreduzibel, denn wegen $q(dx) = d^n \cdot p(x)$ für alle $x \in \mathbb{C}$ ergäbe eine Zerlegung von q auch eine von p. □

Definition 8.5 (Konjugierte von algebraischen Zahlen)

a) Zerfällt das Minimalpolynom $p : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & p(x) \end{array} \right\}$ eines algebraischen $\alpha \in \mathbb{C}$ für alle $x \in \mathbb{C}$ wie folgt

$$p(x) = \left(x - \alpha^{(1)}\right) \cdot \ldots \cdot \left(x - \alpha^{(n)}\right)$$

mit $n := \deg(p)$, $\alpha^{(1)} := \alpha$ und $\alpha^{(\ell)} \in \mathbb{C}$ für alle $\ell \in \mathbb{N}$ mit $2 \leq \ell \leq n$, so heißen $\alpha^{(2)}, \ldots, \alpha^{(n)}$ die **Konjugierten von α**.

b) $\mathbb{A} := \{\alpha \in \mathbb{C} | \, \alpha \text{ algebraisch}\}$ ist die **Menge der algebraischen Zahlen**.

c) Alle $\beta \in \mathbb{C} \setminus \mathbb{A}$ heißen **transzendent(e Zahl)**.

Folgerung 8.6
BEHAUPTUNG: *Die Konjugierten eines $\alpha \in \mathbb{A}$ sind paarweise verschieden und verschieden zu α.*

BEWEIS:
Wie in $\mathbb{Z}$ kann in $\mathbb{Q}[x]$ ein ggT definiert und mit dem EUKLIDischen Algorithmus berechnet werden: Zu $f \in \mathbb{Q}[x]$ und $g \in \mathbb{Q}[x]$ gibt es ein $h \in \mathbb{Q}[x]$, das f und g teilt und das von jedem $t \in \mathbb{Q}[x]$, das f und g teilt, geteilt wird.
In normierter Form ist $\mathrm{ggT}(f, g)$ eindeutig bestimmt.

Angenommen, $\alpha \in \mathbb{C}$ sei mehrfache Nullstelle eines Minimalpolynoms p einer algebraischen Zahl $\tilde{\alpha} \in \mathbb{A}$. Dann ist α Nullstelle von $p' \in \mathbb{Q}[x]$. Klar ist $\deg(p') = \deg(p) - 1 < \deg(p)$. Wie in $\mathbb{Z}$ sieht man, dass für den $\mathrm{ggT}(f, g)$ zweier Polynome $f \in \mathbb{Q}[x]$ und $g \in \mathbb{Q}[x]$ eine Darstellung

$$\mathrm{ggT}(f, g) = qf + rg \qquad \text{mit } q \in \mathbb{Q}[x] \text{ und } r \in \mathbb{Q}[x]$$

existiert. Hieraus folgt, dass α Nullstelle von $\mathrm{ggT}(p', p)$ ist. Da $\mathrm{ggT}(p', p)$ ein Polynom ungleich dem Nullpolynom von kleinerem Grad als p ist, bedeutet dies einen Widerspruch. □

Bemerkung 8.7
Die Menge aller algebraischen Zahlen $\mathbb{A}$ versehen mit der gewöhnlichen Addition und Multiplikation ist ein Körper.
Es ist $\mathbb{Q} \subseteq \mathbb{A} \subseteq \mathbb{C}$, aber es gilt $\mathbb{Q} \neq \mathbb{A} \neq \mathbb{C}$.

BEWEIS:
Die Körpereigenschaft wird sich mit Hilfe des Hauptsatzes über symmetrische Polynome 8.13 auf Seite 27 ergeben, die zweite Aussage folgt unmittelbar aus $\sqrt{2} \in \mathbb{A} \setminus \mathbb{Q}$ und der Existenz transzendenter Zahlen 8.8 auf der nächsten Seite. □

Die einfachste Methode, die Existenz transzendenter Zahlen zu zeigen, geht auf Georg Cantor (1845–1918) zurück. Sie liefert keine konkrete transzendente Zahl.

Satz 8.8 (Satz von Cantor)
Behauptung: *Die Menge* $\mathbb{A}$ *der algebraischen Zahlen ist abzählbar.*
Es gibt transzendente Zahlen.

Beweis:
Da jedes $\alpha \in \mathbb{A}$ Nullstelle eines $f \in \mathbb{Z}[x] \setminus \{0\}$ ist, reicht es, solche Polynome zu betrachten.
Für $f : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & f(x) := \sum_{\ell=0}^{n} a_\ell \cdot x^\ell \end{array} \right\}$ mit $n \in \mathbb{N}$, $a_\ell \in \mathbb{Z}$ für alle $\ell \in \mathbb{N}_0$ mit $\ell < n$ und $a_n \in \mathbb{Z} \setminus \{0\}$ sei

$$N(f) := n + \sum_{\ell=0}^{n} |a_\ell|.$$

Zu jedem $M \in \mathbb{N}$ gibt es nur endlich viele $g \in \mathbb{Z}[x] \setminus \{0\}$ mit $N(g) = M$.
Also gibt es für alle $M \in \mathbb{N}$ nur endlich viele $\alpha \in \mathbb{C}$, für die ein $g \in \mathbb{Z}[x] \setminus \{0\}$ mit $g(\alpha) = 0$ und $N(g) = M$ existiert. Auf die Weise kann $\mathbb{A}$ abgezählt werden.
Wegen der Überabzählbarkeit von $\mathbb{C}$ ist $\mathbb{C} \setminus \mathbb{A}$ nicht leer. □

Der chronologisch erste Beweis für die Existenz transzendenter Zahlen stammt von Liouville (1844) und beruht auf der Beobachtung, dass algebraische Zahlen sich nicht extrem gut durch rationale Zahlen approxomieren lassen.

Satz 8.9 (Satz von Liouville)
Behauptung:

(i) *Ist* $\alpha \in \mathbb{A}$ *algebraisch vom Grad* $n \in \mathbb{N} \setminus \{1\}$*, so existiert ein* $C_\alpha \in \mathbb{R}^+$*, so dass für alle* $b \in \mathbb{Z}$ *und alle* $k \in \mathbb{N}$ *mit* $(b, k) = 1$ *gilt*

$$\left| \alpha - \frac{b}{k} \right| > \frac{C_\alpha}{k^n}.$$

(ii) *Existieren für* $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ *zu jedem* $\varepsilon \in \mathbb{R}^+$ *und jedem* $n \in \mathbb{N} \setminus \{1\}$ *ein* $b_{\varepsilon,n} \in \mathbb{Z}$ *und ein* $k_{\varepsilon,n} \in \mathbb{N}$ *mit* $(b_{\varepsilon,n}, k_{\varepsilon,n}) = 1$ *und*

$$\left| \alpha - \frac{b_{\varepsilon,n}}{k_{\varepsilon,n}} \right| \leq \frac{\varepsilon}{k_{\varepsilon,n}^n},$$

dann ist α *transzendent.*

BEWEIS:
Seien $\alpha \in \mathbb{A}$ und $f : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & f(x) \end{array} \right\} \in \mathbb{Z}[x] \setminus \{0\}$ ein über $\mathbb{Q}$ irreduzibles Polynom mit

$$\deg(f) \geq 2 \qquad \text{und} \qquad f(\alpha) = 0.$$

Für alle $b \in \mathbb{Z}$ und alle $k \in \mathbb{N}$ mit $\left|\alpha - \frac{b}{k}\right| \geq 1$ ist insbesondere $\left|\alpha - \frac{b}{k}\right| \geq \frac{1}{k^n}$.
Es reicht also, ein $b \in \mathbb{Z}$ und ein $k \in \mathbb{N}$ mit $0 < \left|\alpha - \frac{b}{k}\right| < 1$ zu betrachten.
Nach dem Mittelwertsatz der Differentialrechnung existiert ein $t \in (0;1)$ mit dem für $\xi := \alpha + t \cdot \left(\frac{b}{k} - \alpha\right)$ gilt:

$$-f\left(\tfrac{b}{k}\right) = f(\alpha) - f\left(\tfrac{b}{k}\right) = \left(\alpha - \tfrac{b}{k}\right) \cdot f'(\xi) \tag{8.1}$$

Wegen $|\alpha - \xi| < \left|\alpha - \frac{b}{k}\right| < 1$ ist

$$|f'(\xi)| \leq D_\alpha := \max_{\substack{z \in \mathbb{C} \\ |\alpha - z| \leq 1}} |f'(z)|. \tag{8.2}$$

Da $\deg(f) \geq 2$ und f irreduzibel über $\mathbb{Q}$ sind, hat f nur irrationale Nullstellen.
Wegen $f \in \mathbb{Z}[x]$ ist deshalb $f\left(\frac{b}{k}\right) \cdot k^n \in \mathbb{Z} \setminus \{0\}$.
Damit folgt $\left|f\left(\frac{b}{k}\right)\right| \geq \frac{1}{k^n}$ und mit (8.1) und (8.2) ergibt sich

$$\left|\alpha - \frac{b}{k}\right| \cdot D_\alpha \geq \left|\alpha - \frac{b}{k}\right| \cdot |f'(\xi)| = \left|f\left(\frac{b}{k}\right)\right| \geq \frac{1}{k^n}.$$

Mit $C_\alpha := \min\left\{1; \frac{1}{D_\alpha}\right\}$ folgt Behauptung (i).
Behauptung (ii) folgt direkt aus Behauptung (i). □

Bemerkungen

(i) Rasch konvergente Reihen
Reelle $\alpha \in \mathbb{R}$, die durch sehr rasch konvergente Reihen dargestellt werden, erweisen sich nach dem Satz von LIOUVILLE 8.9 auf der vorherigen Seite als transzendent.
Zum Beispiel ist

$$\alpha := \sum_{n=1}^{\infty} \frac{1}{2^{n!}}$$

transzendent. Definiert man nämlich für alle $N \in \mathbb{N}$ zunächst $k_N := 2^{N!}$ und dann zu 2 teilerfremde $b_N \in \mathbb{Z}$ mit

$$\alpha_N := \sum_{n=1}^{N} \frac{1}{2^{n!}} = \frac{b_N}{k_N},$$

so gilt für alle $N \in \mathbb{N}$

$$|\alpha - \alpha_N| = \sum_{n=N+1}^{\infty} \frac{1}{2^{n!}} < \frac{1}{2^{(N+1)!}} \cdot 2 = \frac{2^{1-N!}}{k_N^N}.$$

Wegen $\lim\limits_{N \to \infty} 2^{1-N!} = 0$, ist die Bedingung in (ii) von Satz 8.9 erfüllt.

Da für e und π rasch konvergente Reihen bekannt sind und insbesondere für π immer noch neue gefunden werden, könnte man hoffen, dass die Transzendenz von e und π nach LIOUVILLE gezeigt werden kann. Dies ist nicht der Fall (für π: Kurt MAHLER, 1952).

(ii) Mächtigkeit der LIOUVILLE–Zahlen
Zahlen, die nach Satz 8.9 (ii) transzendent sind, werden **LIOUVILLE–Zahlen** genannt. Man überlegt sich leicht, dass sie eine überabzählbare Teilmenge von $\mathbb{R}$ vom (LEBESGUE–) Maß Null bilden. Nach dem Satz von CANTOR 8.8 auf Seite 21 erfasst man auf diese Weise nur einen geringen Teil aller reellen, transzendenten Zahlen.

(iii) Verschärfungen von Satz 8.9
Der Approximationssatz von LIOUVILLE wurde mehrfach verschärft. Einen Schlusspunkt der Entwicklung bildete der Satz von ROTH (1955).

Satz von ROTH
VORAUSSETZUNGEN:
Seien $n \in \mathbb{N} \setminus \{1;2\}$ und $\alpha \in \mathbb{A}$ algebraisch vom Grad n.
BEHAUPTUNG: *Dann existieren zu jedem $\delta \in \mathbb{R}^+$ und jedem $C \in \mathbb{R}^+$ nur endlich viele $(b,k)^T \in \mathbb{Z} \times \mathbb{N}$ mit $(b,k) = 1$ und*

$$\left| \alpha - \frac{b}{k} \right| \leq \frac{C}{k^{2+\delta}}.$$

Zu der Frage nach einer effektiven Abschätzung für die Anzahl der $(b,k)^T \in \mathbb{Z} \times \mathbb{N}$ und der Größe der Nenner gibt es bislang nur Teilergebnisse.

Einen der Höhepunkte der Zahlentheorie im 19. Jahrhundert stellt Charles HERMITEs (1822–1901) Beweis der Transzendenz von e aus dem Jahr 1873 dar.

Zunächst wird ein Hilfssatz benötigt, der auch bei π nützlich sein wird.

Lemma 8.10
VORAUSSETZUNGEN:
Seien $n \in \mathbb{N}$, $a_\ell \in \mathbb{Z}$ für alle $\ell \in \mathbb{N}_0$ mit $\ell \leq n$,

$$f: \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & f(z) := \sum_{\ell=0}^{n} a_\ell \cdot z^\ell \end{array} \right\} \quad \text{und} \quad F: \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & F(z) := \sum_{\nu=0}^{n} f^{(\nu)}(z) \end{array} \right\}.$$

BEHAUPTUNG: *Dann gilt für alle $z \in \mathbb{C}$*

$$|F(0) \cdot \mathrm{e}^z - F(z)| \leq \mathrm{e}^{|z|} \cdot \sum_{\ell=0}^{n} |a_\ell| \cdot |z|^\ell.$$

BEWEIS:
Nach Definition ist für alle $z \in \mathbb{C}$

$$F(z) = \sum_{\nu=0}^{n} \sum_{\ell=\nu}^{n} a_\ell \cdot \frac{\ell!}{(\ell-\nu)!} \cdot z^{\ell-\nu} = \sum_{\ell=0}^{n} a_\ell \cdot \sum_{\nu=0}^{\ell} \frac{\ell!}{(\ell-\nu)!} \cdot z^{\ell-\nu} = \sum_{\ell=0}^{n} a_\ell \cdot \sum_{\nu=0}^{\ell} \frac{\ell!}{\nu!} \cdot z^{\nu}.$$

Damit folgt insbesondere

$$F(0) = \sum_{\ell=0}^{n} a_\ell \cdot \ell!.$$

Daraus ergibt sich für alle $z \in \mathbb{C}$

$$\begin{aligned}
|F(0) \cdot \mathrm{e}^z - F(z)| &= \left| \sum_{\ell=0}^{n} a_\ell \cdot \sum_{\nu=0}^{\infty} \frac{\ell!}{\nu!} \cdot z^\nu - \sum_{\ell=0}^{n} a_\ell \cdot \sum_{\nu=0}^{\ell} \frac{\ell!}{\nu!} \cdot z^\nu \right| \\
&= \left| \sum_{\ell=0}^{n} a_\ell \cdot \sum_{\nu=\ell+1}^{\infty} \frac{\ell!}{\nu!} \cdot z^\nu \right| \\
&\leq \sum_{\ell=0}^{n} |a_\ell| \cdot \sum_{\nu=\ell+1}^{\infty} \frac{|z|^\nu}{(\nu-\ell)!} \\
&= \sum_{\ell=0}^{n} |a_\ell| \cdot |z|^\ell \cdot \sum_{j=1}^{\infty} \frac{|z|^j}{j!} \\
&< \mathrm{e}^{|z|} \cdot \sum_{\ell=0}^{n} |a_\ell| \cdot |z|^\ell.
\end{aligned}$$

□

SATZ 8.11 (Satz von HERMITE)
BEHAUPTUNG: *Die Zahl* $\mathrm{e} = 2,71828\ldots$ *ist transzendent.*

Die Grundidee des Beweises (und diese tritt in der Transzendenztheorie immer wieder auf) ist, unter Annahme der Algebraizität einen Ausdruck zu definieren, der analytisch nach oben und zahlentheoretisch nach unten abgeschätzt werden kann. Einen solchen Ausdruck zu finden, erfordert ein hohes Maß an Intuition.

BEWEIS:

(i) „Minimalpolynom von e“
Angenommen, e sei algebraisch und habe das Minimalpolynom

$$g: \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & g(x) := \displaystyle\sum_{j=0}^{m} \frac{b_j}{b_m} \cdot x^j \end{array} \right\}$$

mit $m \in \mathbb{N}$, $b_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}_0$ mit $j < m$ und $b_m \in \mathbb{N}$.

(ii) Das Polynom f_p mit $p \in \mathbb{P}$
Für alle $p \in \mathbb{P}$ (später wird ein hinreichend großes gewählt) setze man

$$f_p : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & f_p(x) := x^{p-1} \cdot \prod_{j=1}^{m} (j-x)^p \end{array} \right\} \in \mathbb{Z}[x].$$

Seien $n_p := (m+1) \cdot p - 1$ und $a_{p,p-1} := (m!)^p$ für alle $p \in \mathbb{P}$
Dann gibt es für alle $p \in \mathbb{P}$ und alle $\ell \in \mathbb{N}_0$ mit $p \le \ell \le n_p$ ein $a_{p,\ell} \in \mathbb{Z}$, so dass für alle $p \in \mathbb{P}$ und alle $x \in \mathbb{C}$

$$f_p(x) = a_{p,p-1} \cdot x^{p-1} + \ldots + a_{p,n_p} \cdot x^{n_p} \tag{8.3}$$

gilt. Da für alle $p \in \mathbb{P}$ die Zahlen $1, \ldots, m$ jeweils p–fache Nullstellen von f_p sind, kann f_p für alle $j \in \mathbb{N}$ mit $j \le m$ auch als

$$f_p(x) = a_{p,j,p} \cdot (x-j)^p + \ldots + a_{p,j,n_p} (x-j)^{n_p} \tag{8.4}$$

mit $a_{p,j,\ell} \in \mathbb{Z}$ für alle $\ell \in \mathbb{N}$ mit $p \le \ell \le n_p$ und $x \in \mathbb{C}$ geschrieben werden.

(iii) Die grundlegende Identität
Für alle $p \in \mathbb{P}$ seien $F_p : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & F_p(x) := \sum_{\ell=0}^{n_p} f_p^{(\ell)}(x) \end{array} \right\}$
und $G_p : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & G_p(x) := F_p(0) \cdot \mathrm{e}^x - F_p(x) \end{array} \right\}$.
Nach Annahme (i) ist für alle $p \in \mathbb{P}$

$$0 = F_p(0) \cdot g(\mathrm{e}) \cdot b_m = \sum_{j=0}^{m} b_\ell \cdot F_p(0) \cdot \mathrm{e}^j = \sum_{j=0}^{m} b_\ell \cdot F_p(j) + \sum_{j=0}^{m} b_\ell \cdot G_p(j).$$

Damit folgt also für alle $p \in \mathbb{P}$

$$\Sigma_p := \sum_{j=0}^{m} b_\ell \cdot F_p(j) = -\sum_{j=0}^{m} b_\ell \cdot G_p(j). \tag{8.5}$$

(iv) Zahlentheoretische Abschätzung von Σ_p nach unten
Für alle $p \in \mathbb{P}$ gibt es nach Definition von F_p, (8.3) und (8.4) ein $a_p \in \mathbb{Z}$ mit

$$\begin{aligned} &\sum_{j=0}^{m} b_j \cdot F_p(j) \\ &= b_0 \cdot \sum_{\ell=0}^{n_p} f^{(\ell)}(0) + \sum_{j=1}^{m} b_j \cdot \sum_{\ell=0}^{n_p} f^{(\ell)}(j) \\ &= b_0 \cdot \left((m!)^p \cdot (p-1)! + a_{p,p} \cdot p! + \ldots + a_{p,n_p} \cdot n_p! \right) + \sum_{j=1}^{m} b_j \cdot \left(a_{p,j,p} \cdot p! + \ldots + a_{p,j,n_p} \cdot n_p! \right) \\ &= b_0 \cdot (m!)^p \cdot (p-1)! + a_p \cdot p!. \end{aligned}$$

Für alle $p \in \mathbb{P}$ mit $p > \max\{m; |b_0|\}$ ist $b_0 \cdot (m!)^p$ nicht durch p teilbar und damit ist die rechte Seite eine durch $(p-1)!$, aber nicht durch p teilbare Zahl, insbesondere also nicht 0. Für alle $p \in \mathbb{P}$ mit $p > \max\{m; |b_0|\}$ folgt mit (8.5)

$$|\Sigma_p| = \left| \sum_{j=0}^{m} b_j \cdot F_p(j) \right| \geq (p-1)!. \tag{8.6}$$

(v) Analytische Abschätzung von Σ_p nach oben
Für alle $p \in \mathbb{P}$ werde Lemma 8.10 auf Seite 23 auf f_p angewandt:

$$\left| \sum_{j=0}^{m} b_j \cdot G_p(j) \right| \leq \sum_{j=0}^{m} |b_j| \cdot \mathrm{e}^j \cdot \sum_{\ell=p-1}^{n_p} |a_{p,\ell}| \cdot j^\ell.$$

Die innere Summe lässt sich nach (8.3) für alle $p \in \mathbb{P}$ und alle $j \in \mathbb{N}_0$ mit $j \leq m$ abschätzen durch

$$\sum_{\ell=p-1}^{n_p} |a_{p,\ell}| \cdot j^\ell \leq j^{p-1} \cdot \sum_{\nu=1}^{m} (\nu + j)^p \leq \left(2m^2\right)^p.$$

Mit $C_g := \sum_{j=0}^{m} |b_j| \cdot \mathrm{e}^j$ und $D_m := 2m^2$ folgt mit (8.5) für alle $p \in \mathbb{P}$

$$|\Sigma_p| = \left| \sum_{j=0}^{m} b_j \cdot G_p(j) \right| \leq C_g \cdot D_m^p. \tag{8.7}$$

(vi) Der Widerspruch
Für alle $p \in \mathbb{P}$ mit $p > \max\{m; |b_0|\}$ liefern (8.6) und (8.7)

$$(p-1)! \leq |\Sigma_p| \leq C_g \cdot D_m^p.$$

Für hinreichend großes $p \in \mathbb{P}$ sind diese beiden Ungleichungen nicht miteinander verträglich, da ein $N_0 \in \mathbb{N}$ existiert, so dass für alle $N \in \mathbb{N}$ mit $N \geq N_0$

$$(N-1)! \geq \left(\frac{N}{3}\right)^{\frac{N}{2}} > C_g \cdot D_m^N$$

gilt. Die Annahme in (i) war also falsch und e ist transzendent. □

Im Beweis zu π wird mehrfach mit dem aus der Algebra bekannten Satz über symmetrische Polynome argumentiert. Der Vollständigkeit halber soll dieser hier kurz dargestellt werden.

Definition 8.12 (Symmetrische Polynome)

a) Ein Polynom $f: \left\{ \begin{array}{rcl} \mathcal{R}^n & \to & \mathcal{R} \\ (x_1,\ldots,x_n)^T & \mapsto & f(x_1,\ldots,x_n) \end{array} \right\} \in \mathcal{R}[x_1,\ldots,x_n]$ mit $n \in \mathbb{N}$ Variablen über einem Ring $\mathcal{R}$ heißt **symmetrisch**, wenn für jede n–Permutation $\sigma: \left\{ \begin{array}{rcl} \{m \in \mathbb{N} | \, m \leq n\} & \to & \mathbb{N} \\ \ell & \mapsto & \sigma(\ell) \end{array} \right\} \in \mathcal{S}_n$ und alle $(x_1,\ldots,x_n)^T \in \mathcal{R}^n$ gilt:

$$f\left(x_{\sigma(1)},\ldots,x_{\sigma(n)}\right) = f(x_1,\ldots,x_n).$$

b) Die speziellen symmetrischen Polynome in $n \in \mathbb{N}$ Variablen über einem Ring $\mathcal{R}$

$$\sigma_1: \left\{ \begin{array}{rcl} \mathcal{R}^n & \to & \mathcal{R} \\ (x_1,\ldots,x_n)^T & \mapsto & \sigma_1(x_1,\ldots,x_n) := \displaystyle\sum_{\substack{\ell_1 \in \mathbb{N}^1 \\ 1 \leq \ell_1 \leq n}} x_{\ell_1} \end{array} \right\}$$

$$\sigma_2: \left\{ \begin{array}{rcl} \mathcal{R}^n & \to & \mathcal{R} \\ (x_1,\ldots,x_n)^T & \mapsto & \sigma_2(x_1,\ldots,x_n) := \displaystyle\sum_{\substack{(\ell_1,\ell_2)^T \in \mathbb{N}^2 \\ 1 \leq \ell_1 < \ell_2 \leq n}} x_{\ell_1} \cdot x_{\ell_2} \end{array} \right\}$$

$$\vdots$$

$$\sigma_n: \left\{ \begin{array}{rcl} \mathcal{R}^n & \to & \mathcal{R} \\ (x_1,\ldots,x_n)^T & \mapsto & \sigma_n(x_1,\ldots,x_n) := x_1 \cdot \ldots \cdot x_n \end{array} \right\}.$$

(für alle $\ell \in \mathbb{N}$ mit $\ell \leq n$ ist σ_ℓ die Summe aller Produkte aus ℓ verschiedenen Unbestimmten) heißen **die elementarsymmetrischen Funktionen über $\mathcal{R}$ in n Variablen**.

Beispiele
Sei $\mathcal{R}$ ein Ring.

- $f: \left\{ \begin{array}{rcl} \mathcal{R}^3 & \to & \mathcal{R} \\ (x_1,x_2,x_3)^T & \mapsto & f(x_1,x_2,x_3) := x_1^3x_2 + x_1^3x_3 + x_1x_2^3 + x_1x_3^3 + x_2^3x_3 + x_2x_3^3 \end{array} \right\}$ ist symmetrisch.
- $g: \left\{ \begin{array}{rcl} \mathcal{R}^3 & \to & \mathcal{R} \\ (x_1,x_2)^T & \mapsto & g(x_1,x_2) := x_1^2x_2 + 2x_1x_2^2 \end{array} \right\}$ ist nicht symmetrisch, da $g(x_1,x_2)$ für $(x_1,x_2)^T \in \mathcal{R}^2$ nicht notwendig mit $g(x_2,x_1) = x_1x_2^2 + 2x_1^2x_2$ übereinstimmt.

Satz 8.13 (Hauptsatz über symmetrische Polynome)
Voraussetzungen:
Seien $\mathcal{R}$ ein Ring und $n \in \mathbb{N}$.

Behauptung: *Jedes symmetrische Polynom über $\mathcal{R}$ in n Unbekannten lässt sich als Polynom mit Koeffizienten in $\mathcal{R}$ in den elementarsymmetrischen Funktionen über $\mathcal{R}$ in n Variablen schreiben.*

BEWEIS:

(i) Anordnung der Exponententupel
Sei $f \in \mathcal{R}[x_1, \ldots, x_n]$ symmetrisch.
f ist Summe von Termen der Form $a \cdot x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ mit $a \in \mathcal{R}$ und $\alpha_\ell \in \mathbb{N}_0$ für alle $\ell \in \mathbb{N}$ mit $\ell \leq n$.
Die Exponenten–n–Tupel $(\alpha_1, \ldots, \alpha_n)$ werden wie folgt (lexikografisch) angeordnet.
$(\alpha_1, \ldots, \alpha_n) \succ (\beta_1, \ldots, \beta_n)$ für $(\alpha_1, \ldots, \alpha_n) \neq (\beta_1, \ldots, \beta_n)$, wenn

- $\alpha_1 + \ldots + \alpha_n > \beta_1 + \ldots + \beta_n$ ist oder wenn
- $\alpha_1 + \ldots + \alpha_n = \beta_1 + \ldots + \beta_n$ ist und es ein $\ell \in \mathbb{N}$ mit $1 \leq \ell \leq n$, sowie $\alpha_1 = \beta_1, \ldots, \alpha_{\ell-1} = \beta_{\ell-1}$ und $\alpha_\ell > \beta_\ell$ gibt.

(ii) Induktives Abspalten der Terme mit dem größten Exponententupel
Im symmetrischen f seien die Terme lexikographisch (gemäß $\succ$) angeordnet. Für den ersten Term $a \cdot x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ gilt $\alpha_1 \geq \ldots \geq \alpha_n$, denn in f tritt auch jeder andere Term auf, der durch Umordnen der α_ℓ mit $\ell \in \mathbb{N}$ und $\ell \leq n$ entsteht. Man bilde

$$f_1 := f - a \cdot \sigma_1^{\alpha_1 - \alpha_2} \cdot \sigma_2^{\alpha_2 - \alpha_3} \cdot \ldots \cdot \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \cdot \sigma_n^{\alpha_n}.$$

f_1 ist symmetrisch. Der erste Term des σ–Ausdrucks ist

$$a \cdot x_1^{\alpha_1 - \alpha_2} \cdot (x_1 x_2)^{\alpha_2 - \alpha_3} \cdot \ldots \cdot (x_1 \ldots x_n)^{\alpha_n} = a \cdot x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}.$$

f_1 besteht also nur aus Termen, deren Exponententupel $(\alpha_1, \ldots, \alpha_n)$ bezüglich $\succ$ nachfolgen. Es gibt nur endlich viele n–Tupel $(\beta_1, \ldots, \beta_n)$ nach $(\alpha_1, \ldots, \alpha_n)$.
Es reichen also endlich viele der obigen Schritte, so dass die Differenz schließlich das Nullpolynom ist. □

Beispiel
Seien $\mathcal{R}$ ein Ring mit $2 \in \mathcal{R}$ und $f: \left\{ \begin{array}{rcl} \mathcal{R}^2 & \to & \mathcal{R} \\ (x_1, x_2)^T & \mapsto & f(x_1, x_2) := x_1^3 \cdot x_2 + x_1 \cdot x_2^3 \end{array} \right\}$.
Dann gilt für alle $(x_1, x_2)^T \in \mathcal{R}^2$

$$\begin{aligned} f(x_1, x_2) - 1 \cdot \sigma_1^{3-1}(x_1, x_2) \cdot \sigma_2(x_1, x_2) &= x_1^3 \cdot x_2 + x_1 \cdot x_2^3 - (x_1 + x_2)^2 \cdot (x_1 x_2) \\ &= -2x_1^2 \cdot x_2^2 \\ &= -2 \cdot \sigma_2^2(x_1, x_2). \end{aligned}$$

Also gilt

$$f = \sigma_1^2 \sigma_2 - 2\sigma_2^2.$$

Die praktische Durchführung ist im Allgemeinen recht mühsam.

Sind zum Beispiel $f : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & f(x) \end{array} \right\} \in \mathbb{Z}[x]$ normiert mit $n := \deg(f) \in \mathbb{N}$ und $\alpha := (\alpha_1, \ldots, \alpha_n)^T \in \mathbb{C}^n$ mit $f(\alpha_j) = 0$ für alle $j \in \mathbb{N}$ mit $j \leq n$, dann folgt für alle $x \in \mathbb{C}$

$$f(x) = x^n - \sigma_1(\alpha) \cdot x^{n-1} + \sigma_2(\alpha) \cdot x^{n-2} \mp \ldots + (-1)^n \cdot \sigma_n(\alpha).$$

Das heißt, die Werte der elementarsymmetrischen Funktionen an den Nullstellen von f liegen in $\mathbb{Z}$ (ebenso mit $\mathbb{Q}$ statt $\mathbb{Z}$).

Nach diesem Prinzip wird der Beweis geführt, dass mit $\alpha \in \mathbb{A}$ und $\beta \in \mathbb{A}$ auch $\alpha + \beta \in \mathbb{A}$ und $\alpha \cdot \beta \in \mathbb{A}$ sind.
Der Beweis werde für $\alpha + \beta$ ausgeführt.
Seien $\alpha \in \mathbb{A}$ algebraisch vom Grad $m \in \mathbb{N}$ und $\beta \in \mathbb{A}$ algebraisch vom Grad $n \in \mathbb{N}$.
Seien $\alpha^{(1)} := \alpha$ und $\alpha^{(2)} \in \mathbb{A}, \ldots, \alpha^{(m)} \in \mathbb{A}$ die Konjugierten zu α.
Seien $\beta^{(1)} := \beta$ und $\beta^{(2)} \in \mathbb{A}, \ldots, \beta^{(n)} \in \mathbb{A}$ die Konjugierten zu β.
Man bilde $a := \left(\alpha^{(1)}, \ldots, \alpha^{(m)}\right)^T$, $b := \left(\beta^{(1)}, \ldots, \beta^{(m)}\right)^T$ und

$$h : \left\{ \begin{array}{ccc} \mathbb{C} \times \mathbb{C}^m \times \mathbb{C}^n & \to & \mathbb{C} \\ (x, y, z)^T & \mapsto & h(x, y, z) := \displaystyle\prod_{j=1}^{m} \prod_{\ell=1}^{n} (x - (y_j + z_\ell)) \end{array} \right\}.$$

h kann als Polynom aus $\mathbb{Z}[x, y_1, \ldots, y_m][z_1, \ldots, z_n]$ (in den Variablen $z_1 \ldots, z_n$ mit Koeffizienten aus $\mathbb{Z}[x, y_1, \ldots, y_n]$) aufgefasst werden. h ist als solches symmetrisch in $z_1, \ldots, z_n$. Da die elementarsymmetrischen Funktionen von $z_1, \ldots, z_n$, an der Stelle b Werte aus $\mathbb{Q}$ liefern, ist also

$$h(\cdot, \cdot, b) \in \mathbb{Q}[x, y_1, \ldots, y_m]$$

und symmetrisch in $y_1, \ldots, y_m$. Die gleiche Schlussweise mit den elementarsymmetrischen Funktionen in $y_1, \ldots, y_n$ zeigt, dass $h(\cdot, a, b)$ Koeffizienten in $\mathbb{Q}$ hat.
$\alpha^{(1)} + \beta^{(1)} = \alpha + \beta$ ist als Nullstelle von $h(\cdot, a, b)$ somit algebraisch.

Genauso verfährt man mit $\alpha \cdot \beta$.
Dass mit $\gamma \in \mathbb{A} \setminus \{0\}$ auch $\frac{1}{\gamma}$ algebraisch ist, sieht man unmittelbar.
Es dauerte nahezu zehn Jahre nach HERMITEs Beweis der Transzendenz von e, bis Carl Louis Ferdinand VON LINDEMANN (1852–1939) 1882 in Freiburg die Argumentation auf π übertragen konnte. Der Beweis der Transzendenz von π ist insofern bedeutsam, als damit die Frage nach der Quadratur des Kreises negativ beantwortet wird. Denn könnte man in endlich vielen Schritten mit Zirkel und Lineal aus dem Radius eines Kreises die Seitenlänge eines flächengleichen Quadrats konstruieren, müsste π algebraisch sein.

SATZ 8.14 (Satz von LINDEMANN)
BEHAUPTUNG: *Die Zahl π ist transzendent.*

Beweis:

(i) Folgerungen aus „$\pi \in \mathbb{A}$“
Es werde $\pi \in \mathbb{A}$ angenommen. Dann ist nach Bemerkung 8.7 auf Seite 20 auch $\mathrm{i}\pi \in \mathbb{A}$. Nach Folgerung 8.4 auf Seite 19 existiert ein $d \in \mathbb{N}$, so dass $d\mathrm{i}\pi$ ganz–algebraisch ist. Seien nun $m \in \mathbb{N}$ und $b_j \in \mathbb{Z}$ für alle $j \in \mathbb{N}_0$ mit $j < m$, so dass

$$g : \left\{ \begin{array}{ccl} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & g(x) := x^m + \sum\limits_{j=0}^{m-1} b_j \cdot x^j \end{array} \right\} \in \mathbb{Z}[x] \setminus \{0\}$$

ein Polynom mit Nullstelle $d\mathrm{i}\pi$ ist.
Seien $\alpha^{(1)} := \mathrm{i}\pi$ und $\alpha^{(j)} \in \mathbb{C}$ für alle $j \in \mathbb{N}$ mit $2 \leq j \leq m$ derart, dass für alle $x \in \mathbb{C}$

$$g(x) = \prod_{j=1}^{m} \left(x - d\alpha^{(j)}\right) \tag{8.8}$$

gilt. Wegen $0 = 1 + \mathrm{e}^{\mathrm{i}\pi} = \mathrm{e}^0 + \mathrm{e}^{\alpha^{(1)}}$ gilt

$$R := \prod_{j=1}^{m} \left(\mathrm{e}^0 + \mathrm{e}^{\alpha^{(j)}}\right) = 0. \tag{8.9}$$

(ii) Definition der β_ν
Das Produkt R werde ausmultipliziert und als

$$R = (2^m - k) + e^{\beta_1} + \ldots + e^{\beta_k}$$

geschrieben. Dabei sind

$$k := \# \left\{ \sum_{j=1}^{m} \delta_j \alpha^{(j)} \in \mathbb{C} \setminus \{0\} \,\middle|\, \delta_j \in \{0;1\} \text{ für alle } j \in \mathbb{N} \text{ mit } j \leq m \right\}$$

die Anzahl der nicht–verschwindenden Summen aus (8.10) und die β_ν mit $\nu \in \mathbb{N}$ und $\nu \leq k$ sind gerade die nicht–verschwindenden (nicht notwendig verschiedenen) unter den Zahlen

$$\delta_1 \alpha^{(1)} + \ldots + \delta_m \alpha^{(m)} \qquad \text{mit } \delta_j \in \{0;1\} \text{ für alle } j \in \mathbb{N} \text{ mit } j \leq m. \tag{8.10}$$

(iii) Definition von f_p mit $p \in \mathbb{P}$
Für alle $p \in \mathbb{P}$ (später wird ein hinreichend großes gewählt) werde

$$f_p : \left\{ \begin{array}{ccl} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & f_p(x) := (dx)^{p-1} \cdot \prod\limits_{\nu=1}^{k} (dx - d\beta_\nu)^p \end{array} \right\}$$

gesetzt.

Definiert man $n_p := (k+1) \cdot p - 1$ für alle $p \in \mathbb{P}$, so gibt es für alle $p \in \mathbb{P}$ und alle $\ell \in \mathbb{N}$ mit $p - 1 \leq \ell \leq n_p$ ein $a_{p,\ell} \in \mathbb{Z}$ mit

$$f_p(x) = a_{p,p-1} \cdot x^{p-1} + \ldots + a_{p,n_p} \cdot x^{n_p}. \tag{8.11}$$

Zum Beweis für die Ganzzahligkeit der Koeffizienten bedenke man, dass die $a_{p,\ell}$ mit $\ell \in \mathbb{N}$ und $p - 1 \leq \ell \leq n_p$ für alle $p \in \mathbb{P}$ symmetrisch in $d\beta_1, \ldots, d\beta_k$ (genauer: in Unbestimmten, die man an die Stellen der $d\beta_\nu$ mit $\nu \in \mathbb{N}$ und $\nu \leq k$ setzt) sind.
Die elementarsymmetrischen Funktionen in $d\beta_1, \ldots, d\beta_k$ sind gleich den elementarsymmetrischen Funktionen in den d–Fachen der 2^m Summen aus (8.10), denn setzt man zum Beispiel in $\sigma_h(x_1, \ldots, x_r)$ gerade $x_1 = \ldots = x_\varrho = 0$, so bleiben die elementarsymmetrischen Funktionen in $x_{\varrho+1}, \ldots x_r$.
Die elementarsymmetrischen Funktionen in den Summen aus (8.10) sind symmetrisch in $d\alpha^{(1)}, \ldots, d\alpha^{(m)}$. Die elementarsymmetrischen Funktionen hiervon sind wegen (8.8) aus $\mathbb{Z}$. Mehrfache Anwendung des Hauptsatzes über symmetrische Polynome 8.13 auf Seite 27 ergibt $f \in \mathbb{Z}[x]$.

(iv) Definition der $\gamma_{p,\nu,\ell}$
Für alle $p \in \mathbb{P}$, alle $\nu \in \mathbb{N}$ mit $\nu \leq k$ und alle $\ell \in \mathbb{N}$ mit $p \leq \ell \leq n_p$ gibt es ein $\gamma_{p,\nu,\ell} \in \mathbb{C}$, so dass für alle $x \in \mathbb{C}$ und alle $\nu \in \mathbb{N}$ mit $\nu \leq k$

$$f_p(x) = \gamma_{p,\nu,p} \cdot (x - \beta_\nu)^p + \ldots + \gamma_{p,\nu,n_p} (x - \beta_\nu)^{n_p} \tag{8.12}$$

geschrieben werden kann. Für alle $p \in \mathbb{P}$ und alle $\ell \in \mathbb{N}$ mit $p \leq \ell \leq n_p$ ist

$$c_{p,\ell} := \sum_{\nu=1}^{k} \gamma_{p,\nu,\ell} \in \mathbb{Z}, \tag{8.13}$$

denn die Summe lässt sich darstellen als

$$\frac{1}{\ell!} \cdot \sum_{\nu=1}^{k} f_p^{(\ell)}(\beta_\nu), \qquad \text{da } f_p^{(\ell)}(\beta_\nu) = \ell! \cdot \gamma_{p,\nu,\ell} \text{ ist.}$$

Nach Definition von f_p ist dies für alle $p \in \mathbb{P}$ ein in $d\beta_1, \ldots, d\beta_k$ symmetrisches Polynom mit Koeffizienten in $\mathbb{Z}$.

(v) Die grundlegende Identität
Für alle $p \in \mathbb{P}$ seien $F_p : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & F_p(x) := \sum\limits_{\ell=0}^{n_p} f_p^{(\ell)}(x) \end{array} \right\}$
und $G_p : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ x & \mapsto & G_p(x) := F_p(0) \cdot \mathrm{e}^x - F_p(x) \end{array} \right\}$.
Ähnlich wie im Beweis zu Satz 8.11 und mit (8.9) ergibt sich für alle $p \in \mathbb{P}$

$$\begin{aligned} 0 = F_p(0) \cdot R &= F_p(0) \cdot \left(2^m - k + \sum_{\nu=1}^{k} e^{\beta_\nu} \right) \\ &= (2^m - k) \cdot F_p(0) + \sum_{\nu=1}^{k} F_p(\beta_\nu) + \sum_{\nu=1}^{k} G_p(\beta_\nu) \end{aligned} \tag{8.14}$$

(vi) Zahlentheoretische Abschätzung
Nach (8.11) ist für alle $p \in \mathbb{P}$

$$F_p(0) = (p-1)! \cdot \left(a_{p,p-1} + p \cdot a_{p,p} + \ldots + \frac{n_p!}{(p-1)!} \cdot a_n \right).$$

Für alle $p \in \mathbb{P}$ mit $p > \max\left\{ d; \prod_{\nu=1}^{k} |\beta_\nu| \right\}$ ist $|a_{p,p-1}| = d^{p-1} \cdot \prod_{\nu=1}^{k} |d\beta_\nu|^p$ nicht durch p teilbar.
Für alle $p \in \mathbb{P}$ mit $p > \max\left\{ 2^m - k; d; \prod_{\nu=1}^{k} |\beta_\nu| \right\}$ ist also

$$(2^m - k) \cdot F_p(0) \text{ durch } (p-1)!, \text{ aber nicht durch } p \text{ teilbar.}$$

Aus (8.12) und (8.13) folgt für alle $p \in \mathbb{P}$ die Existenz eines $a_p \in \mathbb{Z}$ mit

$$\sum_{\nu=1}^{k} F_p(\beta_\nu) = \sum_{\nu=1}^{k} \sum_{\ell=0}^{n_p} f_p^{(\ell)}(\beta_\nu) = \sum_{\nu=1}^{k} \sum_{\ell=p}^{n_p} \ell! \cdot \gamma_{p,\nu,\ell} = \sum_{\ell=p}^{n_p} \ell! \cdot c_{p,\ell} = p! \cdot \sum_{\ell=p}^{n_p} \frac{\ell!}{p!} \cdot c_{p,\ell} = p! \cdot a_p.$$

Die Zusammenfassung zeigt, dass $(2^m - k) \cdot F_p(0) + \sum_{\nu=1}^{k} F_p(\beta_\nu)$ für alle $p \in \mathbb{P}$ mit $p > \max\left\{ 2^m - k; d; \prod_{\nu=1}^{k} |\beta_\nu| \right\}$ eine ganze, durch $(p-1)!$, aber nicht durch p teilbare (und damit nicht–verschwindende) Zahl ist, also

$$\left| (2^m - k) \cdot F_p(0) + \sum_{\nu=1}^{k} F_p(\beta_\nu) \right| \geq (p-1)! \tag{8.15}$$

gilt.

(vii) Analytische Abschätzung
Bei der umgekehrten Abschätzung mit Lemma 8.10 auf Seite 23 kann man wieder relativ großzügig vorgehen.
Es gibt nur von g und d abhängige $C_{g,d} \in \mathbb{R}^+$ und $D_{g,d} \in \mathbb{R}^+$, so dass für alle $p \in \mathbb{P}$

$$\begin{aligned}
\left| \sum_{\nu=1}^{k} G_p(\beta_\nu) \right| &\leq \sum_{\nu=1}^{k} \mathrm{e}^{|\beta_\nu|} \cdot \sum_{\ell=p-1}^{n_p} |a_{p,\ell}| \cdot |\beta_\nu|^\ell \\
&\leq \sum_{\nu=1}^{k} \mathrm{e}^{|\beta_\nu|} \cdot (d\,|\beta_\nu|)^{p-1} \cdot \left(\prod_{\ell=1}^{k} (d\,|\beta_\nu| + d\,|\beta_\ell|) \right)^p \\
&\leq C_{g,d} \cdot D_{g,d}^p
\end{aligned}$$

ist!
Das stärkere Wachstum von $(N-1)!$ gegenüber $C_{g,d} \cdot D_{g,d}^N$ für $N \in \mathbb{N}$ führt unter Verwendung von (8.14) bei hinreichend großem $p \in \mathbb{P}$ auf einen Widerspruch zu (8.15).

Also war die Annahme, π sei algebraisch, falsch. □