Die Quadratur des Kreises

Teilnehmer:

Nils Bohlmann	Andreas-Oberschule, Berlin
Demna Grüning	Andreas-Oberschule, Berlin
Rainer Lang	Heinrich-Hertz-Oberschule, Berlin
Matthias Paulsen	Gymnasium Miesbach
Oliver Schaff	Andreas-Oberschule, Berlin
Karl Schrader	Heinrich-Hertz-Oberschule, Berlin
Vanessa Weigelt	Heinrich-Hertz-Oberschule, Berlin
Philip Wellnitz	Heinrich-Hertz-Oberschule, Berlin

Gruppenleiter:

Barbara Jung	Humboldt-Universität zu Berlin
Jürg Kramer	Humboldt-Universität zu Berlin
	Mitglied im Forschungszentrum MATHEON

Die Quadratur des Kreises ist ein klassisches Problem der Geometrie. Man versteht darunter die Aufgabe, allein mit Hilfe von Zirkel und Lineal aus einem vorgegebenen Kreis ein Quadrat mit demselben Flächeninhalt zu konstruieren.
Wir haben im Zuge unserer Untersuchungen erkannt, dass die Konstruierbarkeit (ebener) geometrischer Objekte mit Zirkel und Lineal mit feineren Eigenschaften der reellen Zahlen zusammenhängt. Deshalb haben bei unserer Arbeit neben geometrischen Aspekten vor allem interessante algebraische bzw. zahlentheoretische Fragestellungen eine prominente Rolle gespielt.

1 Mathematische Grundlagen

1.1 Beweis des Fundamentalsatzes der Algebra

Satz 1.1. *Jedes Polynom der Form* $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ *mit* $n > 0, a_0, ..., a_n \in \mathbb{C}; a_n, a_0 \neq 0$ *besitzt mindestens eine Nullstelle* ζ *in* $\mathbb{C}$.

Beweis. Es gilt, dass eine reelle, stetige Funktion einer oder mehrerer Variablen auf einer abgeschlossenen, beschränkten Menge ein Minimum annimmt.

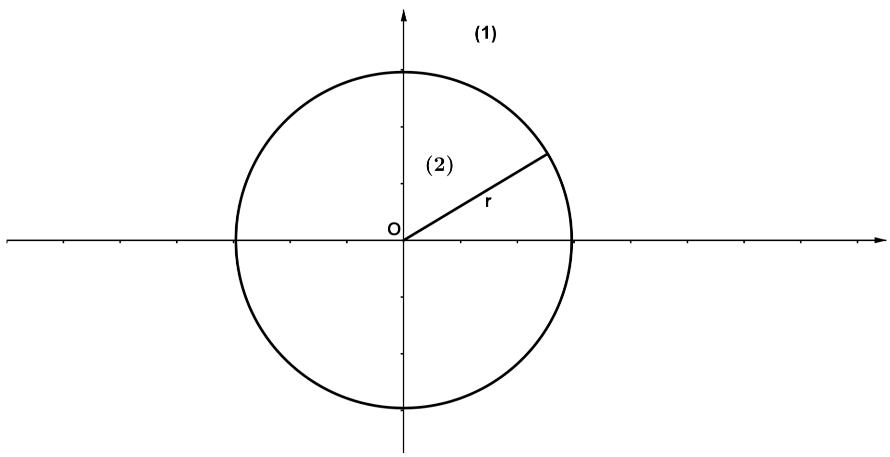


Abbildung 1: Die beiden Bereiche 1 und 2

Wir betrachten die Kreisscheibe, im Folgenden *Bereich 2*, mit einem Radius $r := 1 + |a_{n-1}| + ... + |a_1| + |a_0| \in \mathbb{R}$ um den Koordinatenursprung. Der Rest der Zahlenebene sei mit *Bereich 1* bezeichnet.

Da Bereich 2 abgeschlossen ist und die Funktion $|f|$ dort stetig ist, besitzt $|f|$ auf Bereich 2 ein Minimum ζ_0.

Abschätzungen liefern im Bereich 1 die Ungleichungen $|f(\zeta)| > r \geq |f(\zeta_0)|$.

Daraus folgt: $|f(\zeta_0)| \leq |f(\zeta)|$ für alle $\zeta \in \mathbb{C}$.

Angenommen, $f(\zeta_0) \neq 0$. Über Abschätzungen und Umformungen kann nun eine Zahl α konstruiert werden, bei der $|f(\zeta_0)| > |f(\alpha)|$ gilt. Das ist offensichtlich ein Widerspruch, somit muss eine Nullstelle bei ζ_0 sein. $\square$

1.2 Existenz transzendenter Zahlen

Definition 1.2. *Eine komplexe Zahl* γ *heißt* algebraisch von Grad n*, genau dann, wenn sie Nullstelle eines Polynoms* $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ *mit* ***ganzzahligen*** *Koeffizienten* $a_0, ..., a_n, a_n \neq 0, n > 0$*, ist.*

Wir schreiben im Folgenden für die Menge aller algebraischen Zahlen $\overline{\mathbb{Q}}$.

Definition 1.3. *Eine komplexe Zahl γ heißt* transzendent*, genau dann, wenn sie nicht algebraisch ist.*

Wir schreiben im Folgenden für die Menge aller transzendenten Zahlen $\mathbb{T} = \mathbb{C} \backslash \overline{\mathbb{Q}}$.

Definition 1.4. *Eine Menge M ist* abzählbar*, genau dann, wenn es eine surjektive Abbildung $\mathbb{N}_{\geq 1} \to M$ gibt.*
Surjektiv heißt, dass jedes Element in M getroffen wird.

Definition 1.5. *Eine Menge M ist* überabzählbar*, genau dann, wenn sie nicht abzählbar ist.*

Die Existenz transzendenter Zahlen und somit die Sinnhaftigkeit der Definition 1.3 wird nun über die Mächtigkeiten der Mengen $\overline{\mathbb{Q}}$ und $\mathbb{C}$ gezeigt. Speziell wird gezeigt, dass $\overline{\mathbb{Q}}$ abzählbar unendlich viele Elemente, $\mathbb{C}$ jedoch überabzählbar unendlich viele Elemente enthält, somit also auch $\mathbb{T}$ überabzählbar unendlich viele Elemente enthält.

Satz 1.6. *Die Menge $\overline{\mathbb{Q}}$ ist abzählbar.*

Beweis. Um $\overline{\mathbb{Q}}$ als abzählbar nachzuweisen, genügt es die Menge M_P der Polynome mit ganzzahligen Koeffizienten als abzählbar zu erweisen. Wir betrachten also ein Polynom der Form $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$. Das Polynom ist durch folgende Eigenschaften eindeutig bestimmt:

1. Den Grad $n \in \mathbb{N}$ des Polynoms und
2. die ganzzahligen Koeffizienten $a_0, ..., a_n \in \mathbb{Z}, a_n \neq 0$.

Für jedes $n \in \mathbb{N}$ ist $\mathbb{N} \times \mathbb{Z}^n$ abzählbar, somit ist auch

$$M_P \subset \bigcup_{n \in \mathbb{N}} (\mathbb{N} \times \mathbb{Z}^n)$$

abzählbar. □

Satz 1.7. *Die Menge $\mathbb{C}$ ist überabzählbar.*

Beweis. Angenommen, es existiert eine Nummerierung (z_n) aller reellen Zahlen im Intervall $(0, 1)$.
Wir betrachten die Dezimaldarstellung der z_n:

$$\begin{aligned} z_1 &= 0, \underline{a_{11}} a_{12} a_{13} ... \\ z_2 &= 0, a_{21} \underline{a_{22}} a_{23} ... \\ z_3 &= 0, a_{31} a_{32} \underline{a_{33}} ... \\ z_4 &= ... \end{aligned}$$

Aus den hervorgehobenen diagonalen Ziffern konstruieren wir eine neue Zahl $x = 0, x_1x_2x_3...$ mit

$$x_i = \begin{cases} 4, & \text{falls } a_{ii} = 5 \\ 5, & \text{falls } a_{ii} \neq 5 \end{cases} .$$

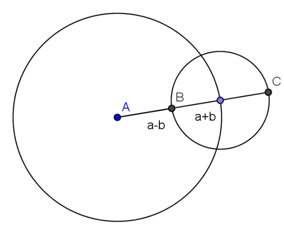
Da sich diese Zahl offenbar von jedem Folgenglied z_i an der i-ten Nachkommastelle unterscheidet, ist sie offenbar keines der z_i, was einen Widerspruch darstellt.

Da das betrachtete Intervall $(0, 1)$ eine Teilmenge der Menge $\mathbb{R}$ aller reellen Zahlen ist, ist $\mathbb{R}$ erst recht überabzählbar. Daraus folgt, dass $\mathbb{C}$ ebenfalls überabzählbar ist. □

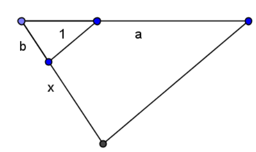
1.3 Erzeugung von Zahlen mittels Konstruktion

Wir stellen uns die Frage, welche Zahlen sich mit Zirkel und Lineal konstruieren lassen. Dazu schauen wir uns zuerst an, welche Rechenoperationen sich ausführen lassen, wenn wir die Strecken a und b bereits aus der gegebenen Einheitsstrecke konstruiert haben.

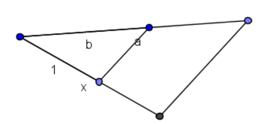
Addition und Subtraktion: Auf einer Gerade werden Kreise abgetragen und so die Längen $a+b$ und $a-b$ konstruiert.



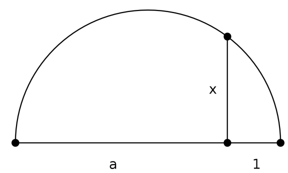
Multiplikation: a,b und das Einheitsmaß werden eingezeichnet und so die Länge $x = a \cdot b$ konstruiert.



Division: a,b und das Einheitsmaß werden eingezeichnet und so die Länge $x = \frac{a}{b}$ konstruiert.



Wurzelziehen: a und das Einheitsmaß werden eingezeichnet, ein Halbkreis gezogen und ein Lot gefällt. Dann gilt $x = \sqrt{a}$.



Korollar 1.8. *In einem x, y-Koordinatensystem mit Einheitsstrecke können nach Vorhergehendem alle Punkte mit rationalen Koordinaten konstruiert werden.*

Korollar 1.9. *Dies bedeutet nun, dass die Zahl $\sqrt{\pi}$ genau dann konstruierbar ist, wenn π konstruierbar ist.*

1.3.1 Schnittpunkte von Geraden oder Kreisen

Durch das Gleichsetzen der Gleichungen für Geraden und Kreise lassen sich die Koordinaten der Schnittpunkte bestimmen. Es stellt sich heraus, dass deren Koordinaten nur durch die Grundrechenarten und Wurzelziehen aus bereits konstruierten Zahlen hervorgehen. Somit handelt es sich bei den Zahlen, die durch Kombination der vorherigen Verfahren konstruiert werden können, um alle mit Zirkel und Lineal konstruierbaren Zahlen.

2 Beweis der Algebraizität konstruierbarer Zahlen

2.1 Definition konstruierbarer Zahlen

Wir definieren den Körper $\mathbb{K}_{1,k} := \{a + b\sqrt{k} | a, b \in \mathbb{Q}\}$ für ein festes $k \in \mathbb{Q}$.
Die Koordinaten unserer bisher konstruierbaren Zahlen lassen sich in einen solchen Körper einordnen. Wir können nun mehr als nur Zahlen aus $\mathbb{K}_{1,k}$ konstruieren. Mithilfe dieser Zahlen können wir neue Geraden- und Kreisgleichungen erschaffen und anschließend wieder neue Koordinaten.
Wir erzeugen so neue Körper $\mathbb{K}_{n,k_n} = \{a_{n-1} + b_{n-1}\sqrt{k_{n-1}} | a_{n-1}, b_{n-1} \in \mathbb{K}_{n-1,k_{n-1}}\}$
Da durch das erneute Wurzelziehen nach jedem neuen Körper neue irrationale Zahlen hinzukommen, ergibt sich die Beziehung:

$$\mathbb{Q} = \mathbb{K}_{0,k_0} \subset \mathbb{K}_{1,k_1} \subset \mathbb{K}_{2,k_2} \subset \ldots \subset \mathbb{K}_{n,k_n} \subset \ldots .$$

Intuitiv lassen sich nun die konstruierbaren Zahlen definieren:

Definition 2.1. *Eine Zahl α heißt* konstruierbar *genau dann, wenn gilt:*

$$\exists n \in \mathbb{N}, \exists q \in \mathbb{Q} : \alpha \in \mathbb{K}_{n,q}.$$

2.1.1 Algebraizität konstruierbarer Zahlen

Zunächst beweisen wir folgenden Hilfssatz:

Lemma 2.2. *Sei $x_k \in \mathbb{K}_k$ eine konstruierbare Zahl. Dann genügt x_k einer Gleichung vom Grad 2^l mit Koeffizienten aus $\mathbb{K}_{k-l}$, wobei $0 < l \leq k$ ist.*

Beweis. Mithilfe vollständiger Induktion über $l \in \mathbb{N}$.
Induktionsanfang ($l = 1$): Sei $x_k = a_{k-1} + b_{k-1}\sqrt{m_{k-1}} \in \mathbb{K}_k$ mit $a_{k-1}, b_{k-1}, m_{k-1} \in \mathbb{K}_{k-1}$ gegeben. Wegen

$$x_k = a_{k-1} + b_{k-1}\sqrt{m_{k-1}} \Leftrightarrow (x_k - a_{k-1})^2 = b_{k-1}^2 m_{k-1}$$

ist ersichtlich, dass x_k Nullstelle eines Polynoms 2^1-ten Grades ist mit Koeffizienten aus $\mathbb{K}_{k-1}$
Induktionsschritt:
x_k sei Nullstelle des Polynoms $f(x) = a_L x^L + a_{L-1}x^{L-1} + ... + a_1 x + a_0$ vom Grad $L := 2^l$ mit $a_j \in \mathbb{K}_{k-l}$ für alle $j = 0, 1, ..., L$.
Wir schreiben für ein festes $w \in \mathbb{K}_{k-l-1}$:

$$a_j := b_j + c_j\sqrt{w} \text{ mit } b_j, c_j \in \mathbb{K}_{k-l-1}$$

So gilt:

$$f(x) = (b_L x^L + b_{L-1}x^{L-1} + ... + b_1 x + b_0) + \sqrt{w} \cdot (c_L x^L + c_{L-1}x^{L-1} + ... + c_1 x + c_0)$$

Wenn wir x_k einsetzen ($f(x_k) = 0$) und die entstehende Gleichung quadrieren, erhalten wir:
$(b_L x_k^L + b_{L-1}x_k^{L-1} + ... + b_1 x_k^1 + b_0)^2 = w \cdot (c_L x_k^L + c_{L-1}x_k^{L-1} + ... + c_1 x_k^1 + c_0)^2$
Wie schon im Induktionsanfang ist hier ersichtlich, dass x_k Nullstelle eines Polynoms vom Grad $2 \cdot L = 2^{l+1}$ mit Koeffizienten aus $\mathbb{K}_{k-l-1} = \mathbb{K}_{k-(l+1)}$. Damit ist der Induktionsschritt bewiesen. □

Da der Hilfssatz nun für alle l, $0 < l \leq k$, und somit auch für $l = k$ gilt, genügt jede konstruierbare Zahl x_k einem Polynom mit rationalen Koeffizienten, wodurch folgende Schlussfolgerung gilt:

Korollar 2.3. *Jede konstruierbare Zahl ist algebraisch.*

Weiterhin gilt nun auch:

Korollar 2.4. *Dies bedeutet nun, dass die Zahl π höchstens dann konstruierbar ist, wenn sie algebraisch ist.*

3 Beweis der Transzendenz von e

Satz 3.1. *Die Zahl e ist transzendent.*

3.1 Beweisstrategie

Wir treffen die indirekte Annahme, dass e algebraisch vom Grad m ist.
Somit gilt:

$$\exists a_0, ..., a_m \in \mathbb{Z}, a_0 \neq 0, a_m \neq 0 : a_m e^m + a_{m-1} e^{m-1} + ... + a_1 e + a_0 = 0.$$

Um dies zu einem Widerspruch zu führen, konstruieren wir ein Hilfspolynom $H \in \mathbb{Q}[x]$ mit folgenden Eigenschaften:

(i) $H(0) \neq 0$,

(ii) $H(j) \in \mathbb{Z} \quad (j = 0, ..., m)$,

(iii) $\sum\limits_{j=0}^{m} a_j H(j) \neq 0$,

(iv) $\left| \sum\limits_{j=1}^{m} a_j \left(H(0) e^j - H(j) \right) \right| < 1$.

Zur Konstruktion des Widerspruches definieren wir nun folgende Größen:

$$c := \sum_{j=0}^{m} a_j H(j) \in \mathbb{Z} \setminus \{0\} \Rightarrow |c| \geq 1, \tag{1}$$

$$\varepsilon_j := H(0) e^j - H(j) \quad (j = 0, ..., m), \tag{2}$$

$$\sigma := \sum_{j=1}^{m} a_j \varepsilon_j. \tag{3}$$

Aus Eigenschaft (ii) folgern wir, dass $c \in \mathbb{Z}$ und aus (iii), dass $c \neq 0$ gilt.
Mit (i) lässt sich (2) nach e^j umstellen, sodass gilt:

$$e^j = \frac{H(j)}{H(0)} + \frac{\varepsilon_j}{H(0)}.$$

Dies lässt sich als Approximation von e^j $(j = 0, ..., m)$ durch die Werte des Polynoms $\frac{H(j)}{H(0)}$ interpretieren, da wir zeigen werden, dass $\frac{\varepsilon_j}{H(0)}$ sehr klein wird.
Außerdem bemerken wir, dass nach Eigenschaft (iv) die Ungleichung $|\sigma| < 1$ besteht.

Mit e als Nullstelle des Polynoms muss gelten:

$$\begin{aligned}0 &= \sum_{j=0}^{m} a_j e^j \\ &= \sum_{j=0}^{m} a_j \left(\frac{H(j)}{H(0)} + \frac{\varepsilon_j}{H(0)} \right) \\ &= \frac{1}{H(0)} \sum_{j=0}^{m} a_j H(j) + \frac{1}{H(0)} \sum_{j=0}^{m} a_j \varepsilon_j \\ &= \frac{c}{H(0)} + \frac{\sigma}{H(0)}.\end{aligned}$$

Mit $H(0) \neq 0$ erhält man:

$$|c| = |\sigma|.$$

Da $|c| > 1$ und $|\sigma| < 1$, kann diese Gleichung nicht gelten. Somit wird der Annahme der Algebraizität von e widersprochen, weshalb e transzendent ist.

3.2 Definition des Hilfspolynoms H

Wir wählen eine Primzahl $p \in \mathbb{P}$ beliebig. Nun definieren wir einige Hilfspolynome:

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

mit Grad $N = p - 1 + m \cdot p$. Basierend darauf definieren wir

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

Betrachten wir die Ableitung

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

so erkennen wir, dass das Polynom mit seiner Ableitung auf $[0, m]$ fast übereinstimmen würde, falls f ausreichend klein wäre.
Dies wollen wir nun durch eine Abschätzung überprüfen. Dazu stellen wir fest:

$$x \in [0, m] \Longrightarrow |x(x-1) \cdot ... \cdot (x-m)| \leq m^{m+1}.$$

Mit $M := m^{m+1}$ ergibt sich:

$$\max_{0 \leq x \leq m} |f(x)| \leq M^p.$$

Man erkennt, dass f auf $[0, m]$ nicht klein ist. Somit müssen wir ein neues Polynom definieren:

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

Aus den für F nachgewiesenen Eigenschaften können wir für H ableiten:

$$H'(x) = H(x) - \frac{f(x)}{(p-1)!},$$

und auch

$$\max_{0 \leq x \leq m} \left| \frac{f(x)}{(p-1)!} \right| \leq \frac{M^p}{(p-1)!}.$$

Wählen wir p hinreichend groß, wird $\frac{f(x)}{(p-1)!}$ beliebig klein. Somit approximiert $\frac{H(x)}{H(0)}$ nach Gleichung (2) die Exponentialfunktion für große p gut.

Es kann weiterhin einfach gezeigt werden, dass H die geforderten Eigenschaften (i)–(iv) erfüllt. □

Beispiel 3.2. *Mit* $\frac{H(x)}{H(0)}$ *als Approximation erhalten wir* e*, wenn wir* $x := 1$ *setzen. Man erhält:*

$$\frac{H(1)}{H(0)} = \frac{F(1)}{(p-1)!} \cdot \frac{(p-1)!}{F(0)} = \frac{F(1)}{F(0)}.$$

Für das Beispiel wählen wir nun $m = 2$ *und* $p = 5$*.*

$$\begin{aligned}
f(x) &= x^4(x-1)^5(x-2)^5, \\
F(x) &= x^{14} - x^{13} + 84x^{12} + 654x^{11} + ... + 29\,141\,344\,128, \\
F(0) &= 29\,141\,344\,128, \quad F(1) = 79\,214\,386\,200, \\
\frac{F(1)}{F(0)} &= 2,718281828458561...
\end{aligned}$$

Diese Näherung ist bereits auf zehn Nachkommastellen korrekt. Es zeigt sich, dass das beschriebene Verfahren sinnvoll ist, um eine Näherung für e *zu erhalten.*

4 Beweis der Transzendenz von π

Satz 4.1. *Die Zahl* π *ist transzendent.*

Beweis. Sei $\mathbb{N}$ die Menge der positiven ganzen Zahlen.

Angenommen, π wäre algebraisch. Dann wäre auch $i\pi$ algebraisch, d. h. es gibt ein Polynom Q mit ganzzahligen Koeffizienten und einer Nullstelle bei $i\pi$. Seien

$\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ alle Nullstellen dieses Polynoms. Bekanntlich gilt $1 + e^{\mathrm{i}\pi} = 0$ und somit

$$\begin{aligned} & (1+e^{\alpha_1})(1+e^{\alpha_2}) \cdots (1+e^{\alpha_n}) = 0 \\ \iff \quad & 1 + e^{\alpha_1} + \cdots + e^{\alpha_n} + e^{\alpha_1+\alpha_2} + \cdots + e^{\alpha_1+\cdots+\alpha_n} = 0 \,. \end{aligned}$$

Die in den Exponenten auftretenden Summen, die nicht 0 sind, werden mit $\beta_1, \ldots, \beta_N$ bezeichnet. Damit ist

$$a_0 + e^{\beta_1} + \cdots + e^{\beta_N} = 0 \quad \text{mit } a_0 \in \mathbb{N},\ \beta_k \in \mathbb{C} \setminus \{0\} \text{ für } 1 \leq k \leq N \,. \tag{4}$$

Man kann zeigen, dass $\beta_1, \ldots, \beta_N$ die Nullstellen eines Polynoms

$$P(z) = b_0 + b_1 z + \cdots + b_N z^N = 0 \quad \text{mit } b_0, b_N \neq 0,\ b_k \in \mathbb{Z} \text{ für } 1 \leq k \leq N$$

sind, weil selbiges mit dem Polynom Q für $\alpha_1, \ldots, \alpha_n$ gilt.

Wir wollen nun $e^{\beta_1}, \ldots, e^{\beta_N}$ approximieren durch

$$e^{\beta_k} = \frac{M_k + \varepsilon_k}{M} \quad \text{mit } M \in \mathbb{Z},\ M_k, \varepsilon_k \in \mathbb{C} \text{ für } 1 \leq k \leq N \,. \tag{5}$$

Dann ist nach (4)

$$(a_0 M + M_1 + \cdots + M_N) + (\varepsilon_1 + \cdots + \varepsilon_N) = 0 \,. \tag{6}$$

Gelingt es, M sowie die M_k und ε_k derart zu wählen, dass der linke Summand von (6) eine ganze Zahl $\neq 0$ ist und der Betrag des rechten Summanden < 1 ist, erhalten wir offenbar den erwünschten Widerspruch.

Wir setzen nun für eine Primzahl p

$$M := \int_0^\infty \frac{e^{-z} z^{p-1}}{(p-1)!} \cdot P(z)^p \cdot b_N^{(N-1)p-1} \, \mathrm{d}z \,.$$

Schreibt man den Integranden als

$$\frac{e^{-z} z^{p-1}}{(p-1)!} \cdot (c_0 + c_1 z + \cdots + c_m z^m) \quad \text{mit } c_k \in \mathbb{Z},\ m \in \mathbb{N} \,,$$

so erhalten wir gemäß der Γ-Funktion

$$M = c_0 + c_1 p + \cdots + c_m \frac{(p-1+m)!}{(p-1)!} \in \mathbb{Z} \,. \tag{7}$$

Es ist $c_0 = b_0^p b_N^{(N-1)p-1}$. Wählen wir also $p > |b_0|$ und $p > |b_N|$, ist c_0 nicht durch p teilbar. Deshalb ist nach (7) insgesamt M nicht durch p teilbar. Zusätzlich können wir $p > |a_0|$ einrichten, damit p auch $a_0 M$ nicht teilt.

Wir setzen ferner für $1 \leq k \leq N$

$$\varepsilon_k := e^{\beta_k} \int\limits_0^{\beta_k} \frac{e^{-z} z^{p-1}}{(p-1)!} \cdot P(z)^p \cdot b_N^{(N-1)p-1} \,\mathrm{d}z$$

$$\text{und} \quad M_k := e^{\beta_k} \int\limits_{\beta_k}^{\infty} \frac{e^{-z} z^{p-1}}{(p-1)!} \cdot P(z)^p \cdot b_N^{(N-1)p-1} \,\mathrm{d}z \,,$$

wodurch (5) erfüllt ist.

Bezeichnet G das Maximum des Ausdrucks

$$\left| z P(z) b_N^{N-1} \right| \,,$$

wobei z auf der Strecke zwischen 0 und einem beliebigen β_k liegt, dann gilt

$$|\varepsilon_k| \leq C \cdot \frac{G^{p-1}}{(p-1)!}$$

mit einer von p unabhängigen Konstanten C. Folglich ist

$$\lim_{p \to \infty} |\varepsilon_k| = 0 \,.$$

Insbesondere kann p so groß gewählt werden, dass $|\varepsilon_1 + \cdots + \varepsilon_N| < 1$ erfüllt ist.

Schließlich betrachten wir die Summe der M_k, von der wir zeigen wollen, dass sie eine durch p teilbare ganze Zahl ist:

$$\sum_{k=1}^{N} M_k = \sum_{k=1}^{N} \left(e^{\beta_k} \int\limits_{\beta_k}^{\infty} \frac{e^{-z} z^{p-1}}{(p-1)!} \cdot P(z)^p \cdot b_N^{(N-1)p-1} \,\mathrm{d}z \right) .$$

Wir substituieren $z - \beta_k$ durch ζ:

$$= \sum_{k=1}^{N} \left(\int\limits_0^{\infty} \frac{e^{-\zeta} (\zeta + \beta_k)^{p-1}}{(p-1)!} \cdot P(\zeta + \beta_k)^p \cdot b_N^{(N-1)p-1} \,\mathrm{d}\zeta \right)$$

$$= \int\limits_0^{\infty} \frac{e^{-\zeta}}{(p-1)!} \sum_{k=1}^{N} \left((\zeta + \beta_k)^{p-1} \cdot P(\zeta + \beta_k)^p \cdot b_N^{(N-1)p-1} \right) \mathrm{d}\zeta.$$

Mit $P(z) = b_N(z-\beta_1)\cdots(z-\beta_N)$ ergibt sich weiter

$$= \int\limits_0^\infty \frac{e^{-\zeta}}{(p-1)!} \sum_{k=1}^{N} \Big((\zeta+\beta_k)^{p-1}(\zeta+\beta_k-\beta_1)^p \cdots \zeta^p \cdots (\zeta+\beta_k-\beta_N) b_N^{Np-1} \Big) \,\mathrm{d}\zeta$$

$$= \int\limits_0^\infty \frac{e^{-\zeta}\zeta^p}{(p-1)!} \sum_{k=1}^{N} \Big((b_N\zeta + b_N\beta_k)^{p-1}(b_N\zeta + b_N\beta_k - b_N\beta_1)^p \cdot \ldots$$

$$\ldots \cdot (b_N\zeta + b_N\beta_k - b_N\beta_{k-1})^p (b_N\zeta + b_N\beta_k - b_N\beta_{k+1})^p \cdot \ldots$$

$$\ldots \cdot (b_N\zeta + b_N\beta_k - b_N\beta_N)^p \Big) \,\mathrm{d}\zeta$$

$$= \int\limits_0^\infty \frac{e^{-\zeta}\zeta^p}{(p-1)!} \left(t_0 + t_1\zeta + \cdots + t_{Np-1}\zeta^{Np-1}\right) \mathrm{d}\zeta.$$

Dabei sind die Koeffizienten t_k symmetrische Polynome in $b_N\beta_1$ bis $b_N\beta_N$. Weil diese die Lösungen der Gleichung

$$b_0 + b_1\frac{z}{b_N} + \cdots + b_N\left(\frac{z}{b_N}\right)^N = 0 \iff b_0 b_N^{N-1} + \cdots + z^N = 0$$

sind, d. h. die Nullstellen eines normierten Polynoms mit ganzen Koeffizienten sind, handelt es sich bei den elementarsymmetrischen Polynomen in $b_N\beta_1$ bis $b_N\beta_N$ und somit auch bei den t_k um ganze Zahlen. Folglich ist

$$\sum_{k=1}^{N} M_k = t_0 p + t_1 p(p+1) + \cdots + t_{Np-1}\frac{(Np-1)!}{(p-1)!}$$

eine durch p teilbare ganze Zahl. Deshalb ist $a_0M + M_1 + \cdots + M_N$ nicht durch p teilbar und daher betragsmäßig mindestens 1, was im Widerspruch zur Gleichung (6) steht. Die Annahme, π wäre algebraisch, ist deswegen falsch. $\square$

Korollar 4.2. *Die Quadratur des Kreises allein mit Zirkel und Lineal ist unmöglich.*