

FACHHOCHSCHULE WEDEL

SEMINARARBEIT

in der Fachrichtung

Informatik-Seminar

Computeralgebra

Algebraische Zahlen und Minimalpolynome

Eingereicht von: Koray Seker
sekerkoray@gmx.de

Erarbeitet im: 8. Semester
Abgegeben am: 7. Januar 2008
Betreuer: Prof. Dr. Sebastian Iwanowski
Fachhochschule Wedel
Feldstraße 143
22880 Wedel

Inhaltsverzeichnis

Algebraische Zahlen.....	3
Definition	3
Eigenschaften.....	3
Körpererweiterungen.....	5
Endliche Körpererweiterung.....	7
Algebraische Körpererweiterung.....	8
Minimalpolynome	8
Minimalpolynom von Produkten und Summen algebraischer Zahlen	10
Transzendente Zahlen	12
Eulersche Zahl.....	13
Literaturverzeichnis	16

Algebraische Zahlen

Definition

Eine Zahl heißt *algebraisch*, wenn es zu x ein Polynom $p(x)$ mit rationalen oder ganzzahligen Koeffizienten gibt, wobei mindestens eine von Null verschieden ist, so dass eine Nullstelle dieses Polynoms ist.¹

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x + a_0$$

Bsp. $x^2 - 2$ Nullstelle dazu $\sqrt{2}$, diese wiederum ist algebraisch

Polynome mit rationalen Koeffizienten kann man *normieren*, indem man alle Koeffizienten durch den Koeffizienten a_n dividiert. Nullstellen von normierten Polynomen, deren Koeffizienten ganzzahlig sind, nennt man *ganzalgebraische Zahlen* oder auch *ganze algebraische Zahlen*.

Wenn eine algebraische Zahl reell ist, dann spricht man von reellen algebraischen Zahlen.

Somit sind die algebraischen Zahlen in ganzzahlalgebraische Zahlen und reell-algebraische Zahlen unterteilt.²

Eigenschaften

Betrachten wir eine natürliche Zahl n , hier können wir sagen, dass es nur abzählbar viele Polynome n -ten Grades mit ganzen Koeffizienten gibt, denn man hat für jeden der n Koeffizienten nur abzählbar viele Wahlmöglichkeiten. Also gibt es auch nur abzählbar viele Polynome mit ganzen Koeffizienten. Da jedes dieser abzählbar vielen Polynome endlich viele Nullstellen hat, gibt es nur abzählbar viele algebraische Zahlen.³

Wie erläutert ist Menge der algebraischen Zahlen abzählbar und bildet einen Körper. Der Körper der algebraischen Zahlen ist algebraisch abgeschlossen d.h. jedes Polynom mit algebraischen Koeffizienten besitzt nur algebraische

¹ Vgl.: Bosch: Mathematiklexikon

² Vgl.: www.mpi-inf.mpg.de/

³ Vgl.:

www.mathematik.de/mde/information/landkarte/zahlen/algebraischeundtranszendentezahl

Nullstellen. Dieser Körper wird als ein minimaler abgeschlossener Oberkörper von \mathbb{Q} bezeichnet, und ist somit ein algebraischer Abschluss von \mathbb{Q} .

Dieser Körper hat viele Automorphismen, und jeder davon liefert eine Einbettung in die Komplexen Zahlen \mathbb{C} . Das heißt, es gibt keine Kanonische Einbettung, sondern man hat bei der Zuordnung von algebraischen Zahlen zu komplexen Zahlen gewisse Freiheiten.

So kann man z.B. die Nullstellen des Polynoms $x^2 + 1$ innerhalb des Körpers der algebraischen Zahlen nicht voneinander unterscheiden und

Man hat die Wahl, welcher der beiden man als imaginäre Einheit i bezeichnet. Die andere Nullstelle dieses Polynoms ist dann eindeutig bestimmt und hat den Wert $-i$. Aber auch nach dieser Festlegung hat man für andere Polynome noch Freiheiten, ihre Nullstellen auf komplexe Zahlen abzubilden.

Oberhalb der rationalen Zahlen und unterhalb des Körpers der algebraischen Zahlen befinden sich unendlich viele Zwischenkörper, etwa die Menge aller Zahlen der Form $a + b \cdot \sqrt[r]{q}$, wobei a und b rationale Zahlen sind, und q die Quadratwurzel einer rationalen Zahl r ist. Auch der Körper der mit Zirkel und Lineal aus $\{0,1\}$ konstruierbaren Punkte der komplexen Zahlenebene ist ein solcher algebraischer Zwischenkörper.

Im Rahmen der Galoisetheorie werden diese Zwischenkörper untersucht, um so tiefe Einblicke über die Lösbarkeit oder Nicht-Lösbarkeit von Gleichungen zu erhalten. Ein Resultat der Galoisetheorie ist, dass zwar jede komplexe Zahl algebraisch ist, die man aus rationalen Zahlen durch Verwendung der Grundrechenarten $+$, $-$, $*$, $/$ und Ziehen n -ter Wurzeln (n eine natürliche Zahl) erhalten kann (man nennt solche Zahlen „durch Radikale darstellbar“), umgekehrt aber algebraische Zahlen existieren, die man nicht in dieser Weise darstellen kann; alle diese Zahlen sind Nullstellen von Polynomen des Grades ≤ 5 .⁴

Beispiele

Um also eine algebraische Zahl zu finden, bzw. nachzuweisen dass sie algebraisch ist, muss doch „nur“ eine geeignete Funktion

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x + a_0$$

⁴ Vgl.: www.mathepedia.de/Algebraische_Zahlen

gefunden werden, die beim Einsetzen der Zahl den Wert Null liefert.

Wenn wir uns noch mal die oben genannte Definition vor Augen halten können wir also sagen, jede rationale Zahl welche in den reellen Zahlen zu finden ist, ist eine algebraische Zahl!

- Eine rationale Zahl r können wir doch als Bruch $r = m / n$ darstellen, wobei m und n ganze Zahlen sind, dann ist r Nullstelle von

$$n \cdot x - m$$

→ Also algebraisch

- Ebenso ist die n -te Wurzel ($n \in \mathbb{N}$) einer rationalen Zahl algebraisch, denn für $r \in \mathbb{Q}$ erfüllt $\sqrt[n]{r}$ die Gleichung $x^n - r = 0$

Körpererweiterungen

Gegeben sei ein Körper L und ein Teilkörper $K \subset L$. Wir nennen dann L auch einen Erweiterungskörper von K und sagen, dass eine Körpererweiterung L/K gegeben sei.

Für eine Körpererweiterung L/K bezeichne $G(L/K)$ die Gruppe der K -Automorphismen von L , also die Gruppe aller bijektiven K -Automorphismen $\sigma: L \rightarrow L$ mit der Komposition von Abbildungen als Verknüpfung. $|G(L/K)|$ bezeichne die Ordnung von $G(L/K)$, d.h. die Zahl der Elemente dieser Gruppe. Man nennt die Zahl $[L:K]$ den Grad der Körpererweiterung $K \subset L$.⁵

Bemerkung 1

Für eine Körpererweiterung $K \subset L$ gilt: $[L:K]=1 \Leftrightarrow L=K$

⁵ Vgl.: www.math.uni-frankfurt.de/~rehn

Bemerkung 2

Ist $L = K[a]$ eine einfache Erweiterung von K und f das Minimalpolynom von a über K , so ist $|G(L/K)|$ gleich der Zahl der verschiedenen Nullstellen von f in L .

Beispiele

(a) Jede Erweiterung $L:K$ vom Grad 2 ist normal.

Jede solche Erweiterung ist algebraisch. Sei $a \in L \setminus K$ beliebig, und sei f das Minimalpolynom von a . Dann hat f den Grad 2. Da f eine Nullstelle in L hat, hat f beide Nullstellen in L . Das bedeutet: L ist ZFK von f . Nach Satz ist $L:K$ normal.

(b) $x^2 - 2$ ist irreduzibel

→daher erweist sich $\mathbb{Q}[x]/(x^2 - 2)$ als Körper

$\mathbb{Q}(\sqrt{2})$ ist eine Körpererweiterung von \mathbb{Q} d.h. zu \mathbb{Q} wird das neue Element $(\sqrt{2})$ adjungiert. $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ ist normal, denn die Erweiterung hat Grad 2.

$\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})$ ist ebenfalls normal, da die Erweiterung den Grad 2 hat.

Aber $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ ist nicht normal. Denn das Polynom $x^4 - 2$ ist irreduzibel

[Über $\mathbb{Q}(\sqrt{2})$ ist $x^4 - 2$ nicht irreduzibel:

$$x^4 - 2 = \frac{\sqrt{2} \cdot (x^2 + \sqrt{2})}{2} \cdot (\sqrt{2}x^2 - 2)$$

Allgemeinen gilt:

Ist $p(x) \in K[x]$ irreduzibel, vom Grad n und ist $K(\alpha) = K[x]/p(x)$, so enthält $K(\alpha)$ als Körper den Vektorraum V über K , welcher von den Potenzen von α erzeugt wird, aber die Gleichung $p(\alpha) = 0$ drückt die lineare Abhängigkeit von $1, \alpha, \dots, \alpha^n$ aus, so dass nur die Potenzen $1, \alpha, \dots, \alpha^{n-1}$ linear unabhängig sind.⁶

Diese einfachen Körpererweiterungen, welche durch Adjunktion eines Elementes α zu K erzeugt werden, haben folgende Form:

$$K(x) := \{c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} \mid c_k \in K, k = 0..n-1\}$$

Beispiel:

$$Q(\sqrt[3]{5}) = a + b\sqrt[3]{5} + c\sqrt[3]{25}$$

Endliche Körpererweiterung⁷

Ein Körper E heißt endliche Körpererweiterung des Körpers E/K vom Grad n , wenn jedes $x \in E$ eine Linearkombination endlich viele Elemente $\alpha_1, \dots, \alpha_n \in E$ mit Koeffizienten in K ist:

$$\sum_{k=1}^n c_k \alpha_k \quad (c_k \in K, k = 1, \dots, n)$$

Satz:

- Jede einfache Körpererweiterung $K(\alpha) = K[x]/p(x)$ ist endlich
- Ist n der Grad des irreduziblen Polynoms, so bilden die Elemente eine Basis von $K(\alpha)$ über K $[K(\alpha):K] = n$

Eine Mehrfache Körpererweiterung $K(\alpha, \beta)$, bei welcher α vom Grad n und β vom Grad m ist, bildet einen $n \cdot m$ dimensionalen Vektorraum über K .

Haben zwei endliche Körpererweiterungen „ K über E über F “ den Grad $[E:K]=n$ und $[F:E]=m$, so ist die Körpererweiterung K über F ebenfalls endlich und hat den Grad $[F:K]=n \cdot m$.

⁶ Vgl.: Koepf: Computeralgebra, 2006, S. 205, S. 212-213

⁷ Vgl.: Koepf: Computeralgebra, 2006, S. 214-215

Algebraische Körpererweiterung⁸

Eine Körpererweiterung E/K heißt algebraisch, wenn jedes Element von E algebraisch über K ist

→ Endliche Körpererweiterung algebraisch

1. Jede endliche Körpererweiterung E/K ist algebraisch und lässt sich durch Adjunktion endlich vieler algebraischer Elemente erzeugen

2. Jede Körpererweiterung E/K , welche durch Adjunktion endlich vieler algebraischer Elemente entsteht, ist endlich

→ Und somit algebraisch

Daraus lässt sich schließen, dass die Summe, Differenz, Produkt und Quotient algebraischer Zahlen wieder algebraisch ist.

Minimalpolynome⁹

Sei $\alpha \in E$ algebraisch über K . Dann gibt es genau ein irreduzibles normiertes Polynom $p(x) \in K[x]$, dessen Nullstelle α ist. Dieses Polynom heißt Minimalpolynom der algebraischen Zahl α über K und wird mit $\text{minpol}(\alpha, x)$ bezeichnet. Sein Grad n heißt der Grad der algebraischen Zahl α über K , und wir schreiben $\text{grad}(\alpha) = n$.

*Das **Minimalpolynom** ist dasjenige normierte Polynom kleinsten Grades in $K[x]$ als Nullstelle besitzt.*

In der Computeralgebra interessante algebraische Körpererweiterungen sind etwa:

- $\mathbb{Q}(\sqrt{2})$, denn $\alpha = \sqrt{2}$ ist eine Wurzel von $x^2 - 2$. Da dieses Polynom normiert und irreduzibel ist, gilt sogar $\text{minpol}(\alpha, x) = x^2 - 2$.
 $\sqrt{2}$ ist also algebraisch über \mathbb{Q} vom Grad 2.

⁸ Vgl.: Koepf: Computeralgebra, 2006, S. 223

⁹ Vgl.: Koepf: Computeralgebra, 2006, S. 219-222

- $Q(x, \sqrt[3]{x-1}) = Q(x)(\sqrt[3]{x-1})$ ist eine algebraische Erweiterung von $K=Q(x)$, dem sogenannten Körper der rationalen Funktionen, denn $\sqrt[3]{x-1}$ ist eine Wurzel des Minimalpolynoms $y^3 - x + 1 \in K[y]$.
- $Q[x]/(x^5 + x + 1)$ ist zwar eine algebraische Körpererweiterung von Q ($(x^5 + x + 1)$ ist irreduzibel über Q), eine Wurzel α von $(x^5 + x + 1)$ lässt sich aber nicht mit Hilfe von Radikalen schreiben. Man kann also α nicht genauer spezifizieren, sondern rechnet in $Q(\alpha) = \{a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4; a, b, c, d, e \in Q\}$ mit der zusätzlichen, durch das Minimalpolynom gegebenen Regel $\alpha^5 = -\alpha - 1$.
- Das Minimalpolynom von $i \in \mathbb{R}(i) = \mathbb{C}$ ist $\text{minpol}_{\mathbb{R}}(i, x) = x^2 + 1 \in \mathbb{R}[x]$. Es ist auch $\text{minpol}_{\mathbb{Q}}(i, x) = x^2 + 1$. i ist also algebraisch über \mathbb{Q} und \mathbb{R} jeweils vom Grad 2.
- Sei $K = \mathbb{R}$, $E = \mathbb{C}$ und $\alpha \in \mathbb{C} \setminus \mathbb{R}$ beliebig. Dann ist $\alpha = a + b \cdot i$ mit $b \neq 0$. Wegen $\alpha \in \mathbb{R}$ gibt es kein Minimalpolynom $p(x) \in \mathbb{R}[x]$ vom Grad 1.

Um eine algebraische Zahl zu charakterisieren, ist ihr Minimalpolynom besonders wichtig. Für das oben genannte Beispiel $\alpha = \sqrt{2}$ gilt: $\text{minpol}(\alpha, x) = x^2 - 2$ und $\text{grad}(\alpha) = 2$. Diese Aussage enthält u.a. die Irrationalitätsaussage für $\sqrt{2}$: Wäre $\sqrt{2}$ rational, so hätte das Minimalpolynom den Grad 1.

Weitere nicht triviale Beispiele zum Verständnis:

- Die algebraische Zahl: $\alpha = \sqrt{4}$
 Das dazugehörige Polynom: $p(x) = x^2 - 4 = 0$
 $p(x)$ kann man leicht über \mathbb{Q} faktorisieren $p(x) = x^2 - 4 = (x - 2)(x + 2)$
 Da es nur ein Minimalpolynom geben kann, ist nur eines Der beiden Faktoren das Minimalpolynom für die algebraische Zahl α .
 In diesem Fall ist $\text{minpol}(\alpha, x) = x - 2$, d.h. $\alpha = 2$.

- $\alpha = \sqrt{4 + 2\sqrt{3}}$ quad. α algebraisch über \mathbb{Q}
 $\alpha^2 = 4 + 2\sqrt{3}$
 $\alpha^2 - 4 = 2\sqrt{3}$ quad.
 $(\alpha^2 - 4)^2 = 12$
 $p(x) = x^4 - 8x^2 + 4 = 0$

$p(x) \rightarrow$ Minimalpolynom?

Nein denn $p(x)$ ist Reduzibel, und somit kein Minimalpolynom

$$p(x) = (x^2 - 2x - 2)(x^2 + 2x - 2)$$

Das Minimalpolynom für $\alpha = \sqrt{4 + 2\sqrt{3}}$ ist in diesem Fall

$$(x^2 - 2x - 2) \rightarrow (\alpha^2 - 2\alpha - 2) = 0$$

Minimalpolynom von Produkten und Summen algebraischer Zahlen

α und β seien zwei algebraische Zahlen über K , mit den Polynomen

$p(x), q(x) \in K[x]$

$\alpha + \beta, \alpha * \beta \rightarrow$ Ergebnis wieder algebraisch über K

Grad des Minimalpolynoms $\leq \text{grad}(\alpha) * \text{grad}(\beta)$

1. Berechne sämtliche Potenzen $(\alpha + \beta)^k, 1 < k \leq m * n$.

Ersetze dabei auftretende Terme mit α^n, β^m gemäß den Minimalpolynomen.

Dies liefert für die k -te Potenz eine rationale Linearkombination des Erzeugendensystems

$$\{\mu_t : 0 \leq t \leq m * n - 1\} = \{\alpha^i * \beta^j : 0 \leq i \leq n - 1, 0 \leq j \leq m - 1\},$$

deren Koeffizient mit $w_{tk} = (w_{0k}, \dots, w_{(z-1)k})$ bezeichnet werden (dabei ist zur Vereinfachung $Z := m * n$). w_{tk} gibt an, mit welchem rationalen Faktor das erzeugende Element μ_t in der k -Potenz von $(\alpha + \beta)$ vertreten ist.

2. Ersetze in der Gleichung

$$X^Z = - \sum_{k=0}^{Z-1} c_k$$

X^k durch die Linearkombination w_{tk} für die entsprechende Potenz $(\alpha + \beta)^k$.
Man erhält ein lineares Gleichungssystem

$$w_{tZ} = - \sum_{k=0}^{Z-1} w_{tk} * c_k$$

Das man in \mathbb{Q} lösen kann. Es liefert als Lösung $((c_0, \dots, c_{Z-1}))$ die Koeffizienten eines Polynoms, das $(\alpha + \beta)$ annulliert. Der Leitkoeffizient c_Z des Polynoms ist aus Normierungsgründen 1.

Bsp.: Was ist das Minimalpolynom von $\sqrt{3} - \sqrt[3]{2}$. Das Minimalpolynom von $\sqrt{3}$ ist 2.Grades, das von $\sqrt[3]{2}$ ist 3.Grades. Also muss man bis zur 6.Potenz ausrechnen.

$$\begin{aligned} (\sqrt{3} - \sqrt[3]{2})^6 &= \sqrt{3}^6 - 6\sqrt{3}^5\sqrt[3]{2} + 15\sqrt{3}^4\sqrt[3]{2}^2 - 20\sqrt{3}^3\sqrt[3]{2}^3 + 15\sqrt{3}^2\sqrt[3]{2}^4 \\ &\quad - 6\sqrt{3}\sqrt[3]{2}^5 + \sqrt[3]{2}^6 \\ &= 27 - 54\sqrt{3}\sqrt[3]{2} + 135\sqrt[3]{4} - 120\sqrt{3} + 90\sqrt[3]{2} - 12\sqrt{3}\sqrt[3]{4} - 4 \\ &= 31 - 120\sqrt{3} + 90\sqrt[3]{2} + 135\sqrt[3]{4} - 54\sqrt{3}\sqrt[3]{2} - 12\sqrt{3}\sqrt[3]{4} \end{aligned}$$

$$(\sqrt{3} - \sqrt[3]{2})^5 = -60 + 9\sqrt{3} - 45\sqrt[3]{2} - 2\sqrt[3]{4} + 15\sqrt{3}\sqrt[3]{2} + 30\sqrt{3}\sqrt[3]{4}$$

$$(\sqrt{3} - \sqrt[3]{2})^4 = 9 - 8\sqrt{3} + 2\sqrt[3]{2} + 18\sqrt[3]{4} - 12\sqrt{3}\sqrt[3]{2}$$

$$(\sqrt{3} - \sqrt[3]{2})^3 = -2 + 3\sqrt{3} - 9\sqrt[3]{2} + 3\sqrt{3}\sqrt[3]{2}$$

$$(\sqrt{3} - \sqrt[3]{2})^2 = 3 + \sqrt[3]{4} - 2\sqrt{3}\sqrt[3]{2}$$

$$(\sqrt{3} - \sqrt[3]{2})^1 = \sqrt{3} - \sqrt[3]{2}$$

$$(\sqrt{3} - \sqrt[3]{2})^0 = 1$$

Dies tragen wir folgendermaßen in ein 6 x 6 System ein:

60	-9	2	-3	0	-1	a	31
-9	8	-3	0	-1	0	b	-120
45	-2	9	0	1	0	* c	= 90
2	-18	0	-1	0	0	d	135
-15	12	0	2	0	0	e	-54
-30	0	-3	0	0	0	f	-12

Dieses System wird gelöst durch

$$\begin{aligned} a &= 0 \\ b &= -9 \\ c &= 4 \\ d &= 27 \\ e &= 36 \\ f &= -23 \end{aligned}$$

so dass wir

$$r(x) = x^6 - 9x^4 + 4x^3 + 27x^2 + 36x - 23$$

als Minimalpolynom von $\sqrt{3} - \sqrt[3]{2}$ gefunden haben.

Transzendente Zahlen

Eine reelle Zahl, die nicht algebraisch ist, heißt transzendent. D.h. eine transzendente Zahl ist eine Zahl, die nicht Nullstelle eines Polynoms mit ganzzahligen Koeffizienten ist. Durch ein Abzählbarkeitsargument, welcher bereits oben beschrieben wurde, kann man einsehen, dass es transzendente Zahlen geben muss.

Viel, viel schwieriger ist der Nachweis, dass eine konkrete Zahl z transzendent (also nicht algebraisch) ist:

Keine Funktion der Form

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x + a_0$$

darf beim Einsetzen von z Null ergeben (wie kompliziert sie auch sein mag).

Damit dürfte klar sein, dass es äußerst schwierig ist, überhaupt transzendente Zahlen zu finden. Es waren denn auch zu Recht gefeierte Ergebnisse, als die Transzendenz einiger „berühmter“ Zahlen gefunden wurde: Die Eulersche Zahl e ist transzendent (Hermite, 1873), ebenso die Kreiszahl π (Lindemann, 1882).

Die Beweise sind allerdings nur sehr schwer nachzuvollziehen. Im Laufe der Zeit gab es aber immer wieder Vereinfachungen dieser Beweise. Einen sehr "eleganten" Beweis veröffentlichte der berühmte Mathematiker David Hilbert im Jahre 1893 welchen ich hier einmal aufführen möchte:

Eulersche Zahl¹⁰

Von fundamentaler Bedeutung ist der für alle $k \in \mathbb{N}$ geltenden Sachverhalt

$$(1) \int_0^{\infty} x^k e^{-x} dx = k!$$

Beim Beweis für e geht man folgendermaßen vor: Man nimmt an, dass e algebraisch ist, also einer Gleichung

$$a + a_1 e + a_2 e^2 + \dots + a_n e^n = 0 \quad (2)$$

mit ganzen Koeffizienten genügt. Man betrachtet nun das Integral

$$\int_0^{\infty} z^k [(z-1)(z-2)\dots(z-n)]^{k+1} e^{-z} dz$$

dessen Integrand das Produkt der Funktionen

$$[z(z-1)(z-2)\dots(z-n)]^k \text{ und}$$

$(z-1)(z-2)\dots(z-n)e^{-z}$ ist. Dieses Integral multipliziert man nun mit der linken Seite der Gleichung (2) und bekommt folgenden Ausdruck:

$$a \int_0^{\infty} + a_1 e \int_0^{\infty} + \dots + a_n e^n \int_0^{\infty}$$

¹⁰ Hilbert: Über die Transzendenz der Zahlen e und π . Mathematische Annalen 43, S. 216-219

Diesen Ausdruck kann man aufspalten in $P_1 + P_2$ mit

$$P_1 = a \int_0^\infty + a_1 e \int_1^\infty + \dots + a_n e^n \int_n^\infty$$

$$P_2 = a_1 e \int_0^1 + a_2 e^2 \int_0^2 + \dots + a_n e^n \int_0^n$$

Ziel ist es nun zu zeigen, dass $\frac{P_1}{k!} + \frac{P_2}{k!}$ ungleich Null ist. Dazu weist man

nach, dass $\frac{P_1}{k!}$ eine ganze von Null verschiedene Zahl und $\left| \frac{P_2}{k!} \right|$ kleiner als 1 ist.

Um zu zeigen, dass $\frac{P_1}{k!}$ eine ganze von Null verschiedene Zahl ist, zeigt man

mit (1), dass das Integral \int_0^∞ eine ganze, durch $k!$ teilbare Zahl ist und die übrigen Integrale \int_i^∞ , $i = 1, \dots, n$ sogar mindestens durch $(k+1)!$ teilbar sind. Nach wenigen Schritten wählt man schließlich k so, dass $k+1$ eine Primzahl ist, die größer als n und a ist und erhält die gewünschte Forderung für $\frac{P_1}{k!}$.

Um zu zeigen, dass $\frac{P_2}{k!} < 1$ ist, stellt man fest, dass die Funktionen

$$z(z-1)(z-2)\dots(z-n) \text{ und } (z-1)(z-2)\dots(z-n)e^{-z}$$

als stetige Funktionen auf dem Intervall $[0, n]$ durch G bzw. H beschränkt sind. Dann lassen sich die einzelnen Integrale in P_2 sehr gut abschätzen und man kommt zu der Ungleichung:

$$\frac{P_2}{k!} \leq \frac{t \cdot G^k}{k!}.$$

Da $\lim_{k \rightarrow \infty} \frac{G^k \cdot t}{k!} = 0$, existiert ein genügend großes k sowie ein davon

abhängiges $\frac{P_2}{k!}$, für welche gilt:

$$\left| \frac{P_2}{k!} \right| \leq \frac{G^k \cdot t}{k!} < 1$$

Da es unendlich viele Primzahlen gibt, existiert ein k , für das sowohl $\frac{P_1}{k!} \neq 0$

als auch $\left| \frac{P_2}{k!} \right| < 1$ gilt.

Literaturverzeichnis

Wolfram Koepf: Computeralgebra, Springer 2006, ISBN 3-540-29894-0

Bosch: Mathematiklexikon, Oldenburg 1999

www.mpi-inf.mpg.de/

www.mathematik.de/mde/information/landkarte/zahlen/algebraischeundtranszendentezahl

www.mathepedia.de/Algebraische_Zahlen

www.math.uni-frankfurt.de/~rehn

Hilbert: Über die Transzendenz der Zahlen e und π . Mathematische Annalen

