Die Transzendenz der Zahlen e und π nach Hilbert

Lukas-Fabian Moser, SS 2013

Die Transzendenz von e

Zentral in der Argumentation ist das folgende Lemma, das im Wesentlichen eine Übungsaufgabe in Analysis ist:

Lemma. *Ist $F \in \mathbb{Z}[X]$ ein Polynom, das an der Stelle $s \in \mathbb{N}$ eine k-fache Nullstelle hat, so ist*

$$T := e^s \cdot \int_s^\infty F(x) \cdot e^{-x} \, \mathrm{d}x$$

eine durch $k!$ teilbare ganze Zahl, und es gilt

$$\frac{T}{k!} \equiv \frac{F}{(X-s)^k}\Big|_{X=s} \pmod{k+1}$$

Beweisskizze. Beweise zunächst die Formel

$$\int_0^\infty x^n \cdot e^{-x} \, \mathrm{d}x = n!$$

für jede natürliche Zahl $n \geqslant 0$ (durch Induktion nach n: für $n = 0$ direktes Nachrechnen, für den Induktionsschritt partielle Integration). Der Fall $s = 0$ des Lemmas ergibt sich nun aus dieser Formel durch Ausmultiplizieren, und der allgemeine Fall durch die Substitution $x = x' + s$ im Integranden. $\square$

Nehmen wir nun an, die Zahl e wäre algebraisch über $\mathbb{Q}$. Dann gäbe es also Zahlen $a_0, \ldots, a_n \in \mathbb{Z}$ mit

$$0 = a_0 + a_1 e + a_2 e^2 + \cdots + a_n e^n = \sum_{s=0}^n a_s e^s.$$

und $a_0 \neq 0$. Für ein noch festzulegendes Polynom $F \in \mathbb{Z}[X]$ multiplizieren wir diese Gleichung mit dem Integral

$$\int_0^\infty F(x) \cdot e^{-x} \, \mathrm{d}x$$

und erhalten

$$
\begin{aligned}
0 &= \sum_{s=0}^{n} a_s e^s \int_0^\infty F(x) \cdot e^{-x} \, \mathrm{d}x \\
&= \underbrace{\sum_{s=0}^{n} a_s e^s \int_s^\infty F(x) \cdot e^{-x} \, \mathrm{d}x}_{=:P_1} + \underbrace{\sum_{s=1}^{n} a_s e^s \int_0^s F(x) \cdot e^{-x} \, \mathrm{d}x}_{=:P_2} .
\end{aligned}
$$

Wir zeigen nun, daß für eine geeignete Wahl des Polynoms F diese Beziehung $P_1 + P_2 = 0$ unmöglich ist, indem wir beide Summanden einzeln untersuchen.

Das Lemma sagt: Besitzt F in 0 eine k-fache Nullstelle und in den Stellen $1, 2, \dots, n$ eine $(k+1)$-fache, so ist P_1 durch $k!$ teilbar, und es ist

$$
\frac{P_1}{k!} \equiv a_0 \cdot \frac{F}{X^k}\Big|_{X=0} \pmod{k+1}
$$

Für eine geeignete Wahl von F wird die rechte Seite $\not\equiv 0 \pmod{k+1}$ sein, und das zeigt, daß $\frac{P_1}{k!}$ eine von null verschiedene ganze Zahl ist.

Wie sieht nun eine solche geeignete Wahl aus? Das einfachste Polynom, das die geforderten Nullstelleneigenschaften besitzt, ist

$$
F(X) = X^k \cdot (X-1)^{k+1} \cdot \ldots \cdot (X-n)^{k+1}
$$

(in Abhängigkeit von einer immer noch zu bestimmenden Zahl $k \in \mathbb{N}$). Für diese Wahl ergibt sich dann

$$
\frac{P_1}{k!} \equiv a_0 \cdot \frac{F}{X^k}\Big|_{X=0} = \pm a_0 \cdot (n!)^{k+1} \pmod{k+1}.
$$

Um zu erzwingen, daß die rechte Seite $\not\equiv 0$ ist, genügt es, k als Vielfaches von $a_0 \cdot n!$ zu wählen (denn dann ist sicher kein Primfaktor von $k+1$ in $a_0 \cdot n!$, also auch nicht in $a_0 \cdot (n!)^{k+1}$ enthalten).

Um einen Widerspruch zu erhalten, versuchen wir zu zeigen, daß $\frac{P_2}{k!}$ für eine geeignete Wahl von F im Betrag < 1 wird – was wegen $P_2 = -P_1$ nicht sein kann. Dafür hilft ein weiteres Lemma:

Lemma. *Für die obige Wahl von F gibt es (von k unabhängige) Konstanten $C, M \geqslant 0$ mit $|P_2| \leqslant CM^k$.*

Da aber $\lim_{k\to\infty} \frac{M^k}{k!} = 0$ ist, ergibt sich sofort der gewünschte Widerspruch (man muß nur k groß genug und gleichzeitig als Vielfaches von $a_0 \cdot n!$ wählen).

Wir schulden nur noch den

Beweis des Lemmas. Wir schätzen wir die in P_2 aufsummierten Integrale ab: Es ist $F = G^k \cdot H$ mit

$$G = X \cdot (X-1) \cdot \ldots \cdot (X-n) \quad \text{und} \quad H = (X-1) \cdot \ldots \cdot (X-n).$$

Ist nun M das Betragsmaximum von $G(x)$ auf dem Intervall $[0, n]$ und m das Betragsmaximum von $H(x) \cdot e^{-x}$ auf dem gleichen Intervall, so ergibt sich

$$\left| \int_0^s F(x) \cdot e^{-x} \, \mathrm{d}x \right| \leqslant smM^k,$$

und daraus folgt

$$|P_2| = \left| \sum_{s=1}^{n} a_s e^s \int_0^s F(x) \cdot e^{-x} \, \mathrm{d}x \right| \leqslant C \cdot M^k$$

mit

$$C = m \cdot \left(|a_1 e| + 2 \left| a_2 e^2 \right| + \cdots + n \left| a_n e^n \right| \right). \qquad \square$$

Die Transzendenz von π

Hilbert folgert die Transzendenz von π aus dem folgenden allgemeineren Satz:

Satz (Hilbert). *Ist $P \in \mathbb{Z}[X]$ ein Polynom vom Grad n und $s_1, \ldots, s_n \in \mathbb{C}$ seine Nullstellen, so ist*

$$a + e^{s_1} + \cdots + e^{s_n} \neq 0.$$

für alle natürlichen Zahlen $a \geqslant 1$.

Folgerung. *Die Zahl π ist transzendent.*

Beweis. Angenommen, π wäre algebraisch. Dann wäre auch $x_1 := i\pi$ algebraisch, also gäbe es ein Polynom $0 \neq Q \in \mathbb{Z}[X]$ vom Grad m mit $Q(x_1) = 0$. Es seien $x_2, \ldots, x_m$ die übrigen Nullstellen von Q. Wegen $e^{x_1} = -1$ ist dann

$$0 = \prod_{i=1}^{m} (1 + e^{x_i}) = 1 + e^{s_1} + \cdots + e^{s_n},$$

wobei $n = 2^m - 1$ ist und jedes s_i genau die Summe einer gewissen Anzahl der x_i's ist. Die Koeffizienten des Polynoms

$$P := (X - s_1) \cdot \ldots \cdot (X - s_n) \in \mathbb{C}[X]$$

sind symmetrische Ausdrücke in den x_i's und daher nach dem Satz über die symmetrischen Funktionen ganzzahlig, und da die Nullstellen von P nach Konstruktion genau $s_1, \ldots, s_n$ sind, haben wir einen Widerspruch zum Satz von Hilbert erhalten. $\square$

Lemma (Satz über die symmetrischen Funktionen). *Ist $H \in \mathbb{Z}[X]$ ein Polynom vom Grad n, und sind $x_1, \ldots, x_n$ seine Nullstellen, so ist jeder* symmetrische *polynomiale Ausdruck in den x_i eine ganze Zahl.*

Unter einem symmetrischen polynomialen Ausdruck in den x_i verstehen wir dabei einen polynomialen Ausdruck (mit ganzzahligen Koeffizienten) in den $x_1, \dots, x_n$, der sich bei beliebigen Permutationen der Variablen nicht ändert, also beispielsweise

$$
\begin{aligned}
&x_1 + \cdots + x_n \\
&x_1^2 + \cdots + x_n^2 \\
&x_1 x_2 + x_1 x_3 + \cdots + x_i x_j + \cdots + x_{n-1} x_n \\
&x_1 + \cdots + x_n + 2x_1^2 x_2^2 \dots x_n^2
\end{aligned}
$$

Der Beweis des Satzes von Hilbert verläuft ganz ähnlich wie derjenige der Transzendenz von e, nur benötigen wir diesmal auch Integrale entlang Kurven (eigentlich genügen Strecken) in der komplexen Zahlenebene.

Zunächst bemerken wir, daß wir im Beweis annehmen können, daß $P(0) \neq 0$ ist, also alle s_i von Null verschieden sind (indem wir ansonsten P durch die passende Potenz X^e dividieren und die Zahl a durch $a + e$ ersetzen).

Multiplizieren wir nun wieder die widerspruchsweise angenommene Gleichung

$$0 = a + e^{s_1} + \cdots + e^{s_n}$$

mit einem Integral

$$\int_0^\infty F(x) \cdot e^{-x} \, \mathrm{d}x$$

für ein noch zu bestimmendes Polynom $F \in \mathbb{Z}[X]$. Dies ergibt

$$
\begin{aligned}
0 &= a \int_0^\infty F(x) \cdot e^{-x} \, \mathrm{d}x + \sum_{i=1}^n e^{s_i} \int_0^\infty F(x) \cdot e^{-x} \\
&= \underbrace{a \int_0^\infty F(x) \cdot e^{-x}}_{=:P_0} + \underbrace{\sum_{i=1}^n e^{s_i} \int_{s_i}^\infty F(x) \cdot e^{-x} \, \mathrm{d}x}_{=:P_1} + \underbrace{\sum_{i=1}^n e^{s_i} \int_0^{s_i} F(x) \cdot e^{-x} \, \mathrm{d}x}_{=:P_2},
\end{aligned}
$$

wobei jedes der Integrale $\int_{s_i}^\infty$ entlang einer zur reellen Achse parallelen Geraden von s_i bis ins positive Unendliche zu erstrecken ist und die Integrale $\int_0^{s_i}$ jeweils entlang der direkten Verbindungsstrecke von 0 zum Punkt s_i zu verstehen sind.[1] Dabei benutzen wir das folgende Lemma:

Lemma. *Für ein beliebiges Polynom $F \in \mathbb{C}[X]$ und ein festes $s \in \mathbb{C}$ ist*

$$\int_0^\infty F(x) \cdot e^{-x} \, \mathrm{d}x = \int_0^s F(x) \cdot e^{-x} \, \mathrm{d}x + \int_s^\infty F(x) \cdot e^{-x} \, \mathrm{d}x.$$

[1] Die Wahl dieses letzteren Integrationsweges ist eigentlich bedeutungslos, weil das Kurvenintegral über eine holomorphe Funktion nach dem Cauchyschen Integralsatz nur vom Anfangs- und Endpunkt abhängt.

Beweisskizze. Wir schreiben $f(x) := F(x) \cdot e^{-x}$. Nach dem Cauchyschen Integralsatz ist, für jedes (als groß vorzustellende) reelle R,

$$\int_0^R f(x)\,\mathrm{d}x = \int_0^s f(x)\,\mathrm{d}x + \int_s^{s+R} f(x)\,\mathrm{d}x + \int_{s+R}^R f(x)\,\mathrm{d}x.$$

Es genügt nun zu zeigen, daß der letzte Summand im Limes $R \to \infty$ verschwindet, was sich durch eine einfache Abschätzung ergibt. □

Untersuchen wir nun wieder die Summanden P_1 und P_2 einzeln. Die Hauptarbeit steckt im folgenden

Lemma. *Besitzt F in jedem s_i eine k-fache Nullstelle, so ist P_1 eine durch $k!$ teilbare ganze Zahl.*

Beweis. Für die Integrale in der Summe, die P_1 definiert, ergibt jeweils die Substitution $x = x' + s_i$

$$e^{s_i} \int_{s_i}^\infty F(x) \cdot e^{-x}\,\mathrm{d}x = \int_0^\infty F(x + s_i) \cdot e^{-x}\,\mathrm{d}x.$$

Nun ist aber (anders als im Fall des Lemmas im Beweis der Transzendenz von e) $F(X + s_i)$ kein Polynom in $\mathbb{Z}[X]$ mehr, so daß wir seine Gestalt genauer untersuchen müssen. Dazu schreiben wir das Polynom $F(X + \Delta)$ (in zwei Variablen X und Δ) aus als

$$F(X + \Delta) = \sum_{j=0}^d H_j(\Delta) X^j,$$

wobei d der Grad von F ist und H_j ein Polynom in Δ ist, dessen Koeffizienten – das ist der eigentliche Punkt! – **ganzzahlig** sind. Mit dieser Darstellung gilt dann für jede Zahl $s \in \mathbb{C}$:

$$\int_0^\infty F(x+s) \cdot e^{-x}\,\mathrm{d}x = \sum_{j=0}^d \int_0^\infty H_j(s) \cdot x^j \cdot e^{-x}\,\mathrm{d}x = \sum_{j=0}^d H_j(s) \cdot j!$$

Hat nun F in s eine k-fache Nullstelle, so ist $F(X + s)$ durch X^k teilbar; das bedeutet, daß $H_0, \dots, H_{k-1}$ in s verschwinden, und dann wird der letzte Ausdruck zu $k! \cdot H(s)$, wobei $H := H_k + (k+1)H_{k+1} + \dots + \frac{d!}{k!} H_d \in \mathbb{Z}[\Delta]$ ein ganzzahliges Polynom ist.

Wenn also das Polynom F so gewählt ist, daß es in $s_1, \dots, s_n$ jeweils eine k-fache Nullstelle besitzt, so folgt

$$\sum_{i=1}^n e^{s_i} \int_{s_i}^\infty F(x) \cdot e^{-x}\,\mathrm{d}x = k! \cdot \sum_{i=1}^n H(s_i).$$

Nun kommt der Clou: Die Summe $\sum_{i=1}^n H(s_i)$ ist ein symmetrischer Ausdruck in den s_i mit ganzzahligen Koeffizienten, also nach dem Satz über symmetrische Funktionen eine *ganze Zahl*, und wir sind fertig.[2] □

Hat außerdem F in 0 eine k-fache Nullstelle, so ist P_0 eine durch $k!$ teilbare ganze Zahl, und zwar gilt

$$\frac{P_0}{k!} \equiv a \cdot \frac{F}{X^k}\bigg|_{X=0} \pmod{k+1}.$$

[2] Hilbert argumentiert hier stattdessen mit der Ganzabgeschlossenheit von $\mathbb{Z}$ und muß deswegen etwas mehr arbeiten.

Wir möchten, modulo $k+1$ rechnend, den Summanden P_1 vernachlässigen können und wählen deshalb F so, daß es in 0 eine k-fache, in jedem s_i aber sogar eine $(k+1)$-fache Nullstelle hat. Die einfachste Wahl dafür ist also

$$F := X^k \cdot P^{k+1}.$$

Für diese Wahl gilt dann

$$\frac{P_0 + P_1}{k!} \equiv a \cdot P(0)^{k+1} \pmod{k+1}.$$

Von dieser Stelle ab verläuft der Beweis genau wie bei der Transzendenz von e: Daß die rechte Seite der letzten Gleichung $\not\equiv 0$ wird, können wir wieder dadurch erzwingen, daß wir k als Vielfaches der von Null verschiedenen ganzen Zahl $a \cdot P(0)$ wählen. Damit ist dann $\frac{P_0+P_1}{k!}$ eine nichtverschwindende ganze Zahl.

Lemma. *Für die obige Wahl von F gibt es (von k unabhängige) Konstanten $C, M \geqslant 0$ mit $|P_2| \leqslant CM^k$.*

Da aber $\lim_{k\to\infty} \frac{M^k}{k!} = 0$ ist, ergibt sich sofort der gewünschte Widerspruch (man muß nur k groß genug und gleichzeitig als Vielfaches von $a_0 \cdot n!$ wählen). Wir schulden nur noch den

Beweis des Lemmas. Wir schätzen wieder die in P_2 aufsummierten Integrale ab: Wegen $F = X^k \cdot P^{k+1} = P \cdot (X \cdot P)^k$ betrachten wir das Betragsmaximum M von $X \cdot P$ über alle Verbindungsstrecken von 0 zu jedem der Punkte s_i sowie das Betragsmaximum von $x \cdot e^{-x}$ auf der gleichen Punktmenge. Dann ergibt sich

$$\left| \int_0^{s_i} F(x) \cdot e^{-x} \,\mathrm{d}x \right| \leqslant |s_i| \, mM^k,$$

woraus folgt

$$|P_2| = \left| \sum_{i=1}^{n} e^{s_i} \int_0^{s_i} F(x) \cdot e^{-x} \,\mathrm{d}x \right| \leqslant C \cdot M^k$$

mit

$$C = m \cdot (|e^{s_1} s_1| + \cdots + |e^{s_n} s_n|).$$ □