



Ein Beweis der Transzendenz der P -adischen Exponentialfunktion.

Von Kurt Mahler in Göttingen.

In dieser Note wird gezeigt, daß die P -adische Exponentialfunktion

$$e^z = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \dots,$$

die bekanntlich für alle durch P bzw. für $P = 2$ durch P^2 teilbaren P -adischen Zahlen existiert, an jeder algebraischen P -adischen Stelle $z \neq 0$ im Existenzgebiet eine transzendente P -adische Zahl darstellt.

Das Beweisverfahren stützt sich auf einige Eigenschaften von e^z , die durch die Sonderheiten des P -adischen Zahlkörpers und seine nichtarchimedische Bewertung bedingt sind. Eine einfache formale Übertragung der klassischen Transzendenzbeweise für die gewöhnliche Exponentialfunktion ist anscheinend nicht möglich, da die P -adische Funktion nur noch eine beschränkt konvergente Reihe hat.

1. Sei ϱ eine feste, m eine über alle Grenzen wachsende natürliche Zahl. Setzt man

$$A_k(z \mid \varrho) = \frac{1}{2\pi i} \int_{C_0}^m \frac{e^{z\beta} d\beta}{\prod_{h=0}^m (\beta + k - h)^e}, \quad R(z \mid \varrho) = \frac{1}{2\pi i} \int_{C_\infty}^m \frac{e^{z\beta} d\beta}{\prod_{h=0}^m (\beta - h)^e},$$

wobei C_0 einen sehr kleinen, C_∞ einen sehr großen Kreis um den Nullpunkt mit positivem Richtungssinn bedeutet, so besteht die Identität

$$\sum_{k=0}^m A_k(z \mid \varrho) e^{kz} = R(z \mid \varrho).$$

Die Ausdrücke $A_k(z \mid \varrho)$ sind Polynome in z vom Grad $\varrho - 1$; man hat für sie die abbrechenden Potenzreihen

$$A_k(z \mid \varrho) = \sum_{l=0}^{\varrho-1} \frac{z^l}{l!} A_k^{(l)}(m)$$

mit den Koeffizienten

$$A_k^{(l)}(m) = \frac{1}{2\pi i} \int_{C_0}^m \frac{\beta^{l-e} d\beta}{\prod_{h=0, h \neq k}^m (\beta + k - h)^e}.$$

Der Charakter dieser Koeffizienten kann auf einfache Weise untersucht werden¹⁾; es zeigt sich, daß die Größen

$$A_k^{(l)}(m) = m!^e D_m^e \frac{(\varrho - 1)!}{l!} A_k^{(l)}(m)$$

¹⁾ Siehe S. 138 meiner Arbeit „Zur Approximation der Exponentialfunktion und des Logarithmus, II“, Journal f. d. r. u. ang. Mathematik 166 (1932).

ganz rational sind und daß gleichmäßig in den Indizes k, l, ϱ für großes m die Ungleichung

$$\left| A_k^{(l)} \binom{m}{\varrho} \right| \leq (3e)^{m\varrho}$$

besteht. Dabei bedeutet

$$D_m = \{1, 2, \dots, m\}$$

das kleinste gemeinschaftliche Vielfache der Zahlen $1, 2, \dots, m$.

Wir führen noch die Abkürzungen

$$F\left(z, w \left| \begin{matrix} m \\ \varrho \end{matrix} \right. \right) = \sum_{k=0}^m \sum_{l=0}^{\varrho-1} A_k^{(l)} \binom{m}{\varrho} z^l w^k,$$

$$r\left(z \left| \begin{matrix} m \\ \varrho \end{matrix} \right. \right) = m!^{\varrho} D_m^{\varrho} (\varrho - 1)! R\left(z \left| \begin{matrix} m \\ \varrho \end{matrix} \right. \right)$$

ein; alsdann besteht die Identität

$$F\left(z, e^z \left| \begin{matrix} m \\ \varrho \end{matrix} \right. \right) = r\left(z \left| \begin{matrix} m \\ \varrho \end{matrix} \right. \right).$$

2. Von jetzt ab gehen wir zum Körper der P -adischen Zahlen K über, wobei P eine feste Primzahl bedeutet. Den P -adischen Wert einer Zahl α aus K bezeichnen wir mit $|\alpha|_P$ zum Unterschied vom gewöhnlichen Absolutbetrag. Eine P -adische Zahl α heiße wie üblich algebraisch, wenn es ein irreduzibles Polynom

$$f(x) = c_0 + c_1 x + \dots + c_n x^n \neq 0$$

mit ganzen rationalen Koeffizienten und mindestens vom ersten Grad gibt, dessen Nullstelle α ist; gibt es kein solches Polynom, so heiße α transzendent.

Seien z und w zwei algebraische P -adische Zahlen. Dann gibt es einen kleinsten algebraischen Körper über dem Körper R der rationalen Zahlen, in dem gleichzeitig z und w liegen. Er heiße $R(s)$, sei vom Grad n über R und werde etwa durch die ganze algebraische P -adische Zahl s erzeugt. In s lassen sich z und w ausdrücken in der Gestalt

$$z = \frac{a_0 + a_1 s + \dots + a_{n-1} s^{n-1}}{a_n},$$

$$w = \frac{b_0 + b_1 s + \dots + b_{n-1} s^{n-1}}{b_n},$$

wobei $a_n \neq 0$ und $b_n \neq 0$ und die Zahlen $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_n$ ganz rational sind. Sei zur Abkürzung

$$a = \max(|a_0|, |a_1|, \dots, |a_n|), \quad b = \max(|b_0|, |b_1|, \dots, |b_n|).$$

Offenbar läßt sich die ganze P -adische Zahl

$$G\left(s \left| \begin{matrix} m \\ \varrho \end{matrix} \right. \right) = a_n^{m\varrho-1} b_n^m F\left(z, w \left| \begin{matrix} m \\ \varrho \end{matrix} \right. \right)$$

als ein Polynom in s mit ganzen rationalen Koeffizienten vom Grad

$$(n-1)(m+\varrho-1)$$

darstellen. Wird bei festem ϱ der Index m genügend groß gewählt, so ist nach 1 aber

$$\left| A_k^{(l)} \binom{m}{\varrho} \right| \leq (3e)^{m\varrho}$$

und $A_k^{(l)} \binom{m}{\varrho}$ ganz rational. Offenbar erhält man die Majorante

$$G\left(s \left| \begin{matrix} m \\ \varrho \end{matrix} \right. \right) \ll (3e)^{m\varrho} a^{m\varrho-1} b^m \sum_{k=0}^m \sum_{l=0}^{\varrho-1} (1+s+\dots+s^{n-1})^{k+l}.$$

Jetzt ist

ist folglich eine von Null verschiedene ganze rationale Zahl; man erhält für sie leicht die obere Schranke

$$|D| \leq (2n-1)! g^{n-1} ((3e)^{m_0} a^{e-1} b^m (n+1)^{m+e-1} (2g)^{(n-1)(m+e-2)})^n.$$

Jetzt gibt es aber nach bekannten Sätzen über Elimination zwei Polynome $\gamma(x)$ und $H(x)$ mit ganzen rationalen Koeffizienten, so daß identisch

$$\gamma(x)g(x) + H(x)H^*\left(x \middle| \begin{matrix} m \\ \varrho \end{matrix}\right) = D$$

ist, folglich für $x = s$

$$H^*\left(s \middle| \begin{matrix} m \\ \varrho \end{matrix}\right) = \frac{D}{H(s)}.$$

Auf der rechten Seite ist der Zähler eine nichtverschwindende ganze rationale Zahl, so daß

$|D|_P \geq |D|^{-1} \geq ((2n-1)! g^{n-1})^{-1} ((3e)^{m_0} a^{e-1} b^m (n+1)^{m+e-1} (2g)^{(n-1)(m+e-2)})^{-n}$ ist. Im Nenner steht ein Polynom in der ganzen P -adischen Zahl s mit ganzen rationalen Koeffizienten; da der Nenner nicht Null sein kann, ist also

$$\left| \frac{1}{H(s)} \right|_P \geq 1.$$

Damit sind wir zu folgender Abschätzung gekommen:

$$\begin{aligned} \left| G\left(s \middle| \begin{matrix} m \\ \varrho \end{matrix}\right) \right|_P &= \left| H^*\left(s \middle| \begin{matrix} m \\ \varrho \end{matrix}\right) \right|_P \\ &\geq ((2n-1)! g^{n-1})^{-1} ((3e)^{m_0} a^{e-1} b^m (n+1)^{m+e-1} (2g)^{(n-1)(m+e-2)})^{-n}. \end{aligned}$$

Die rechte Seite kann noch auf eine etwas bequemere Gestalt gebracht werden. Offenbar ist für jede genügend große feste natürliche Zahl ϱ und für über alle Grenzen wachsende natürliche Zahlen m

$$(2n-1)! g^{n-1} a^{(e-1)n} b^{mn} (n+1)^{(m+e-1)n} (2g)^{(n-1)(m+e-2)n} \leq \left(\frac{4}{3}\right)^{mn_0}.$$

Es folgt daraus

Hilfssatz 1: Wird $\varrho \geq \varrho_0(z, w)$ und $m \geq m_0(z, w, \varrho)$ angenommen, so verschwindet entweder $G\left(s \middle| \begin{matrix} m \\ \varrho \end{matrix}\right)$ oder ist eine von Null verschiedene ganze P -adische Zahl mit

$$\left| G\left(s \middle| \begin{matrix} m \\ \varrho \end{matrix}\right) \right|_P \geq (4e)^{-mn_0}.$$

3. Von jetzt ab nehmen wir an, daß ϱ die Gestalt

$$\varrho = P^r + 1$$

hat, wobei r eine ganze rationale nichtnegative Zahl bedeutet. Ist dann

$$\varphi = \varphi(P^r + 1),$$

so besteht nach dem kleinen Fermatschen Satz die Kongruenz

$$P^\varphi \equiv 1(\varrho).$$

Setzt man

$$m + 1 = \frac{P^{r+\mu\varphi} + 1}{P^r + 1},$$

wobei auch μ eine nichtnegative ganze rationale Zahl bedeutet, so ist offenbar die Zahl

$$(m+1)\varrho - 1 = P^{r+\mu\varphi}$$

eine reine Potenz von P .

Es soll eine obere Schranke für den P -adischen Wert der Zahl

$$\Re\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix}\right) = a_n^{e-1} b_n^m r\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix}\right) = m!^e D_m^e (\varrho - 1)! a_n^{e-1} b_n^m R\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix}\right)$$

abgeleitet werden; dabei wollen wir aber annehmen, daß z nicht verschwindet und die Ungleichung

$$0 < |z|_P = P^{-f} \leq P^{-3}$$

erfüllt.

Nach **1** ist

$$R\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix} \right) = \frac{1}{2\pi i} \int_{C_\infty} \frac{e^{z\delta} d\delta}{\prod_{h=0}^m (\delta - h)^{\varrho}}$$

Entwickelt man den Integranden in der Umgebung des unendlich fernen Punktes in eine Laurentreihe und wendet alsdann den Residuensatz an, indem man C_∞ auf den Punkt $\delta = \omega$ zusammenzieht, so erhält man die Potenzreihe

$$R\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix} \right) = \frac{z^{(m+1)\varrho-1}}{((m+1)\varrho-1)!} \left(1 + \frac{c_1 z}{(m+1)\varrho} + \frac{c_2 z^2}{((m+1)\varrho)((m+1)\varrho+1)} + \frac{c_3 z^3}{((m+1)\varrho)((m+1)\varrho+1)((m+1)\varrho+2)} + \dots \right),$$

wobei c_1, c_2, c_3, \dots gewisse ganze rationale Zahlen bedeuten. Hieraus folgt

$$\Re\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix} \right) = m!^{\varrho} D_m^{\varrho} (\varrho - 1)! a_n^{\varrho-1} b_n^m \frac{z^{(m+1)\varrho-1}}{((m+1)\varrho-1)!} r\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix} \right)$$

mit der Abkürzung

$$r\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix} \right) = 1 + \frac{c_1 z}{(m+1)\varrho} + \frac{c_2 z^2}{((m+1)\varrho)((m+1)\varrho+1)} + \dots$$

Nach bekannten Sätzen ist für jede nichtnegative ganze rationale Zahl h

$$|h!|_P = P^{-\left(\left[\frac{h}{P}\right] + \left[\frac{h}{P^2}\right] + \dots\right)}$$

Wegen

$$(m+1)\varrho - 1 = P^{r+\mu\varphi}$$

folgt hieraus erstens die Gleichung

$$|((m+1)\varrho - 1)!|_P = P^{-(P^{r+\mu\varphi-1} + P^{r+\mu\varphi-2} + \dots + 1)} = P^{-\frac{P^{r+\mu\varphi} - 1}{P-1}} = P^{-\frac{(m+1)\varrho - 2}{P-1}}$$

Zweitens ist für jede nichtnegative ganze rationale Zahl h

$$\begin{aligned} |((m+1)\varrho + h - 1)!|_P &= P^{-\left(\left[\frac{(m+1)\varrho+h-1}{P}\right] + \left[\frac{(m+1)\varrho+h-1}{P^2}\right] + \dots\right)} \\ &\geq P^{-\left(\frac{(m+1)\varrho+h-1}{P} + \frac{(m+1)\varrho+h-1}{P^2} + \dots\right)} = P^{-\frac{(m+1)\varrho+h-1}{P-1}} \end{aligned}$$

und daher für $h \geq 1$ wegen $P \geq 2$

$$\begin{aligned} &\left| \frac{c_h z^h}{((m+1)\varrho)((m+1)\varrho+1) \dots ((m+1)\varrho+h-1)} \right|_P \\ &\leq P^{-\frac{(m+1)\varrho+h-1}{P-1} - \frac{(m+1)\varrho-2}{P-1} - hf} \leq P^{h+1-3h} = P^{-2h+1} \leq P^{-h} < 1. \end{aligned}$$

In der Potenzreihe

$$r\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix} \right) = 1 + \frac{c_1 z}{(m+1)\varrho} + \frac{c_2 z^2}{((m+1)\varrho)((m+1)\varrho+1)} + \dots$$

streben also die Summanden gegen Null; alle von ihnen außer dem ersten haben einen P-adischen Wert kleiner als eins. Daraus folgt

$$\left| r\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix} \right) \right|_P = 1 \quad \text{und} \quad \left| \Re\left(z \middle| \begin{matrix} m \\ \varrho \end{matrix} \right) \right|_P = \left| m!^{\varrho} D_m^{\varrho} (\varrho - 1)! a_n^{\varrho-1} b_n^m \frac{z^{(m+1)\varrho-1}}{((m+1)\varrho-1)!} \right|_P \neq 0,$$

wegen

$$0 < |D_m^q(q-1)! a_n^{q-1} b_n^q|_P \leq 1,$$

also

$$0 < \left| \Re \left(z \left| \begin{matrix} m \\ q \end{matrix} \right|_P \right) \right| \leq \left| \frac{m!^q}{((m+1)q-1)!} z^{(m+1)q-1} \right|_P.$$

Wendet man noch einmal die Formel für den P -adischen Wert der Fakultäten an, so erhält man

$$|m!|_P = P^{-\left(\left[\frac{m}{P}\right] + \left[\frac{m}{P^2}\right] + \dots\right)} \leq P^{-\left(\frac{m}{P-1} - \frac{\log m}{\log P} - 1\right)},$$

also

$$\left| \frac{m!^q}{((m+1)q-1)!} \right|_P \leq P^{\frac{(m+1)q-2}{P-1} - q\left(\frac{m}{P-1} - \frac{\log m}{\log P} - 1\right)} = P^{\frac{q-2}{P-1} + q\frac{\log m}{\log P} + q}$$

und damit schließlich die Abschätzung

$$0 < \left| \Re \left(z \left| \begin{matrix} m \\ q \end{matrix} \right|_P \right) \right| \leq P^{\frac{q-2}{P-1} + q\frac{\log m}{\log P} + q} P^{-((m+1)q-1)f}.$$

Ihr entnimmt man bei festem q für genügend großes m den

Hilfssatz 2: Sind die beiden natürlichen Zahlen q und m von der speziellen Gestalt

$$q = P^r + 1, \quad m + 1 = \frac{P^{r+\mu q} + 1}{P^r + 1}$$

und ist $q \geq q_1(z)$, $m \geq m_1(z, q)$, $|z|_P = P^{-f}$ mit $f \geq 3$, so ist

$$0 < \left| \Re \left(z \left| \begin{matrix} m \\ q \end{matrix} \right|_P \right) \right| \leq P^{-\frac{mqf}{2}} = |z|_P^{\frac{mq}{2}}.$$

4. Lehrsatz: Ist ζ eine P -adische Zahl mit

$$0 < |\zeta|_P < \frac{1}{2} \quad \text{für } P = 2, \quad 0 < |\zeta|_P < 1 \quad \text{für } P \geq 3,$$

so ist höchstens eine der beiden Zahlen ζ und e^ζ algebraisch.

Beweis: Es genügt offenbar zu zeigen, daß für eine beliebige natürliche Zahl n die beiden Zahlen ζ und e^ζ nicht gleichzeitig in einem algebraischen Zahlkörper n -ten Grades liegen können.

Wir bestimmen eine natürliche Zahl λ , so daß

$$P^{-\lambda} < (4e)^{-2n}$$

ist, und setzen

$$z = P^\lambda \zeta.$$

Liegen dann ζ und e^ζ in einem algebraischen Zahlkörper n -ten Grades, so offenbar auch z und $e^z = w$. Jetzt besteht die Identität

$$G\left(s \left| \begin{matrix} m \\ q \end{matrix} \right|_P\right) = \Re\left(z \left| \begin{matrix} m \\ q \end{matrix} \right|_P\right),$$

wo s zu z und w nach 2 bestimmt ist. Auf der rechten Seite ist nach Hilfssatz 2 für unendlich viele Paare q, m beliebig großer natürlicher Zahlen

$$0 < \left| \Re \left(z \left| \begin{matrix} m \\ q \end{matrix} \right|_P \right) \right| \leq |z|_P^{\frac{mq}{2}} < P^{-\frac{mq\lambda}{2}} < (4e)^{-mqn}.$$

Die linke Seite kann für diese Paare also auch nicht verschwinden; nach Hilfssatz 1 ist daher

$$\left| G\left(s \left| \begin{matrix} m \\ q \end{matrix} \right|_P\right) \right| \geq (4e)^{-mqn},$$

und damit sind wir zu dem gewünschten Widerspruch gelangt.