Transzendenz von e

Nikolai Nowaczyk <mail@nikno.de> http://math.nikno.de/
Lars Wallenborn <lars@wallenborn.net> http://www.wallenborn.net/

07.12.-09.12. 2012

Inhaltsverzeichnis

1 Schlachtplan

Ziel dieses Scripts ist der Beweis des folgenden berühmten Satzes.

1.1 Satz. Die Zahl e ist transzendent.

Dazu werden wir zunächst einige Aussagen annehmen, auf die wir hier aufbauen wollen, siehe Abschnitt 2. In Abschnitt 3 führen wir dann alle noch fehlenden benötigten Grundbegriffe ein. Danach sind wir bereits in der Lage die Aussage dieses Satzes genau zu verstehen. In Abschnitt 4 beweisen wir zunächst einige Hilfsaussagen, bevor dann schließlich in Abschnitt 5 der Beweis von Satz 1.1 geführt wird. Abbildung 1.1 soll die sehr komplexe Beweis-Strategie verdeutlichen. Boxen, die gestichelt umranded sind, entsprechen Aussagen, die wir (ohne Beweis) annehmen werden und Boxen mit einem dickeren Rand sind zentral.

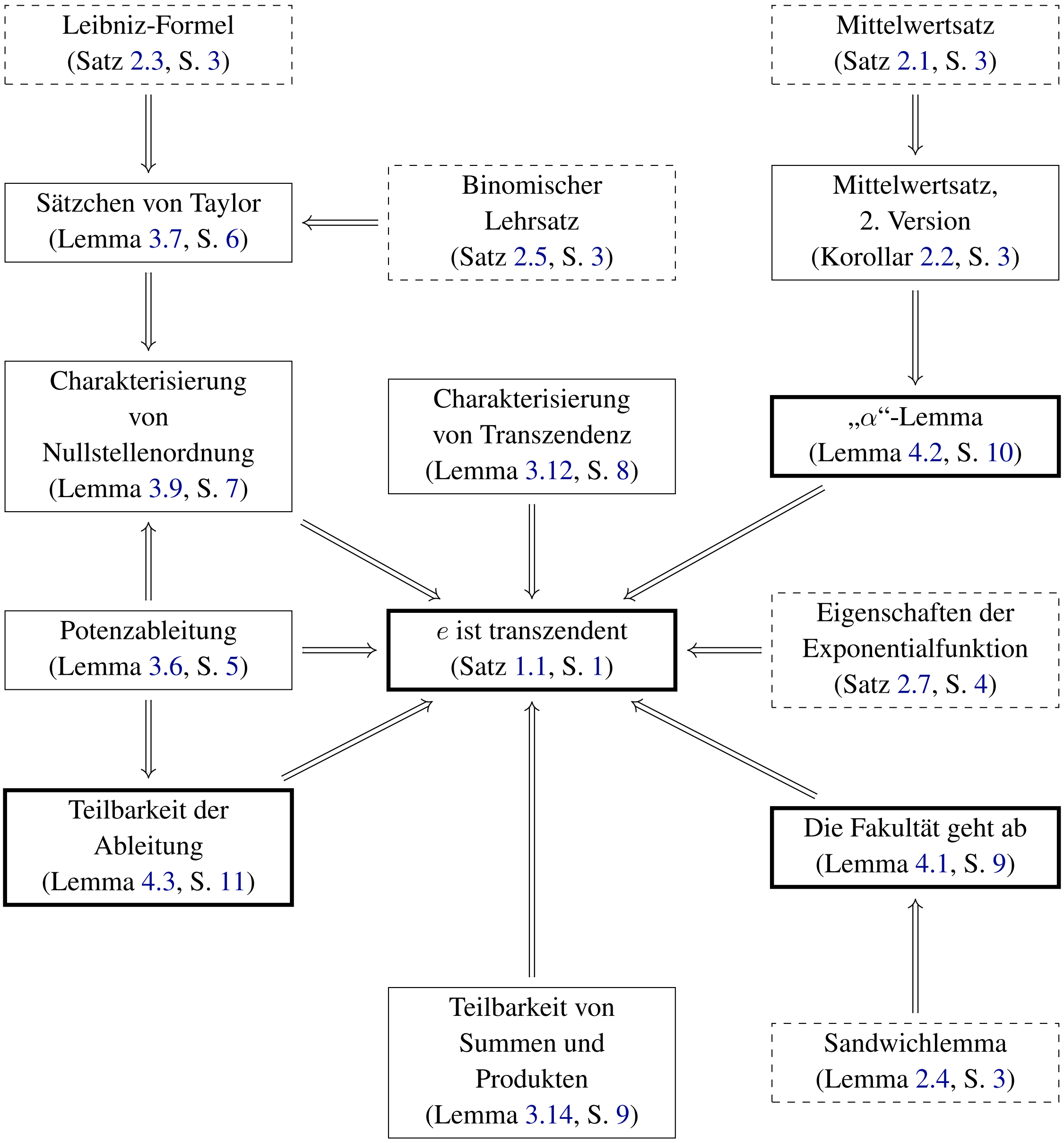

Abbildung 1.1: Beweisstrategie

2 Annahmen

"Faith is eternal."
-HELLFIRE DREADNOUGHT, 40000

2.1 Analytische Grundlagen

2.1 Satz (Mittelwertsatz)**.** Sei $I \subset \mathbb{R}$ ein Interval und $f : I \to \mathbb{R}$ differenzierbar. Seien $a, b \in I$ mit $a < b$. Dann gibt es ein $c \in]a, b[$, sodass

$$f(b) - f(a) = f'(c)(b - a).$$

2.2 Korollar (Mittelwertsatz, 2. Version)**.** Sei $I \subset \mathbb{R}$ ein Interval und $f : I \to \mathbb{R}$ differenzierbar. Seien $a, b \in I$ mit $a < b$. Dann gibt es ein $\alpha \in]0, 1[$, sodass

$$f(b) - f(a) = f'(a + \alpha(b - a))(b - a).$$

2.3 Satz (Leibniz-Formel)**.** Seien $f, g : I \subset \mathbb{R} \to \mathbb{R}$ k-mal stetig differenzierbar. Dann gilt

$$\forall x \in I : (fg)^{(k)} = \sum_{i=0}^{k} \binom{k}{i} f^{(i)}(x) g^{(k-i)}(x). \tag{2.1}$$

2.4 Lemma ("Sandwichlemma")**.** Seien $(a_n)_{n\in\mathbb{N}}$, $(c_n)_{n\in\mathbb{N}}$ Folgen mit

$$\lim_{n\to\infty} a_n = x = \lim_{n\to\infty} c_n.$$

Sei $(b_n)_{n\in N}$ eine weitere Zahlenfolge und gelte:

$$\exists N \in \mathbb{N} : \forall n \geq N : a_n \leq b_n \leq c_n.$$

Dann gilt auch

$$\lim_{n\to\infty} b_n = x.$$

2.5 Satz (Binomischer Lehrsatz)**.** Es gilt für alle $x, y \in \mathbb{R}$ und $n \in \mathbb{N}$

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

(Für n=2 folgen so die bekannten "binomischen Formeln").

2.2 Die Exponentialfunktion

Wir erinnern an einige Eigenschaften der Exponentialfunktion, die man evtl. aus der Schule kennt (aber wahrscheinlich nicht so aufgeschrieben).

2.6 Definition (Exponentialfunktion)**.** Die Funktion

$$\begin{aligned} \exp : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \textstyle\sum_{k=0}^{\infty} \frac{x^k}{k!} \end{aligned}$$

heißt *Exponentialfunktion*.

2.7 Satz (Eigenschaften der Exponentialfunktion)**.** Die Funktion $\exp$ erfüllt folgende Eigenschaften.

(i). Es ist die Funktionalgleichung

$$\forall x, y \in \mathbb{R} : \exp(x + y) = \exp(x)\exp(y). \tag{2.2}$$

(ii). $\exp$ ist monoton steigend und sogar bijektiv. Die Umkehrfunktion $\ln := \exp^{-1} : \mathbb{R} \to \mathbb{R}$ heißt *Logarithmus*.

(iii). $\exp$ ist unendlich oft differenzierbar.

2.8 Definition (Eulersche Zahl)**.** Die Zahl

$$e := \exp(1)$$

heißt *Eulersche Zahl*.

2.9 Definition (Potenz)**.** Seien $x, y \in \mathbb{R}$ und $x > 0$ dann definieren wir

$$x^y := \exp(y \ln(x))$$

und nennen einen solchen Ausdruck *Potenz*.

2.10 Bemerkung. In diesem Sinne gilt jetzt

$$e^x = \exp(x \ln(e)) = \exp(x \cdot 1) = \exp(x).$$

Daher führen viele Schulbücher bereits in der Mittelstufe die Exponentialfunktion auch so ein, d.h. sie definieren $\exp(x) = e^x$. Die Autoren dieser Bücher verschweigen in der Regel die Definition der Zahl e, der Logarithmusfunktion $\ln$ und der Potenz x^y für reelle Zahlen. Das liegt daran, dass sie diese Fragen innerhalb ihrer "Theorie" nicht beantworten können.

3 Grundlagen und Problemstellung

"To arms, my brethren! To arms, brave orcs and humans! Twilight falls, and the enemy awaits."
-MALFURION STORMRAGE, 25

3.1 Funktionen und Polynome

3.1 Definition (Funktionenarithmetik)**.** Seien $f, g : \mathbb{R} \to \mathbb{R}$. Dann definieren wir die Funktionen

$$\begin{aligned} f + g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto f(x) + g(x) \end{aligned}$$

und

$$\begin{aligned} fg : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto f(x)g(x). \end{aligned}$$

Durch diese Definitionen erhält man eine Addition und eine Multiplikation auf der Menge aller Funktionen $\mathbb{R} \to \mathbb{R}$. Setzt man insbesondere f gleich einer konstanten $c \in \mathbb{R}$, so erhält man die Funktion

$$\begin{aligned} cg : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto cg(x). \end{aligned}$$

Wir identifizieren häufig die Zahl $c \in \mathbb{R}$ mit der konstanten Funktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto c$. Für eine natürliche Zahl $i \in \mathbb{N}$ ist die Potenz f^i definiert durch

$$f^i := \underbrace{f \cdot \ldots \cdot f}_{i-\text{mal}}.$$

3.2 Definition (Gleichheit von Funktionen)**.** Zwei Funktionen $f, g : \mathbb{R} \to \mathbb{R}$ heißen *gleich*, falls gilt

$$\forall x \in \mathbb{R} : f(x) = g(x).$$

Wir schreiben dann auch einfach $f = g$.

3.3 Definition (Polynom)**.** Es sei

$$\begin{aligned} X : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x \end{aligned}$$

Eine Funktion $f : \mathbb{R} \to \mathbb{R}$ heißt *Polynom*, falls $f = 0$ oder falls es *Koeffizienten* $a_0, \ldots, a_n \in \mathbb{R}$ gibt, sodass

$$f = \sum_{k=0}^{n} a_k X^k, \qquad a_n \neq 0. \tag{3.1}$$

Wir nennen die Zahl n auch den *Grad von* f und setzen $\operatorname{grad} f := n$. Die Funktion $f = 0$ heißt *Nullpolynom*. Wir setzen formal $\operatorname{grad} 0 := -\infty$. Die Menge aller Polynome notieren wir mit $\mathbb{R}[X]$.

3.4 Bemerkung. Der Grund, warum wir die Funktion X einführen ist der, dass wir gerne zwischen der Funktion $X : \mathbb{R} \to \mathbb{R}$ und einer reellen Zahl $x \in \mathbb{R}$ unterscheiden wollen. Per Definition gilt dann für alle $x \in \mathbb{R}$, $X(x) = x$. Gleichung (3.1) ist also als eine Gleichheit zwischen Funktionen $\mathbb{R} \to \mathbb{R}$ zu verstehen. Gemäß Definition 3.2 und der Definition von X ist (3.1) gleichbedeutend mit

$$\forall x \in \mathbb{R} : f(x) = \sum_{k=0}^{n} a_k x^k.$$

3.2 Polynome und ihre Ableitungen

3.5 Bemerkung (Differenzierbarkeit von Polynomen)**.** Es sei festgehalten, dass jedes Polynom $f : \mathbb{R} \to \mathbb{R}$ unendlich oft differenzierbar ist. Für jede k-mal differenzierbare Funktion $f : \mathbb{R} \to \mathbb{R}$ notieren wir mit $f^{(k)} : \mathbb{R} \to \mathbb{R}$ ihre k-te Ableitung. Insbesondere setzen wir $f^{(0)} := f$ als die "nullte"-Ableitung.

3.6 Lemma (Potenzableitungen)**.** Für $n, k \in \mathbb{N}$ gilt, dass

$$(X^n)^{(k)} = \begin{cases} \frac{n!}{(n-k)!} X^{n-k}, & n \geq k, \\ 0, & \text{sonst.} \end{cases} \tag{3.2}$$

Insbesondere gilt für ein Polynom f vom Grad n, dass

$$\forall k > n : f^{(k)} = 0. \tag{3.3}$$

Beweis.

SCHRITT 1 ($n \geq k$): Sei $n \in \mathbb{N}$ beliebig und zunächst $n \geq k$. Wir beweisen die Aussage per Induktion nach k. Dazu stellen wir zuerst fest, dass die Aussage für $k = 0$ erfüllt ist. Sei nun die Aussage für k schon bewiesen. Wir wollen sie nun für $k + 1$ zeigen:

$$\begin{aligned}(X^n)^{(k)} &= \left((X^n)^{(k)}\right)' \overset{\text{I.V.}}{=} \left(\frac{n!}{(n-k)!}X^{n-k}\right)' = \frac{n!}{(n-k)!}\left(X^{n-k}\right)' \\ &= \frac{n!(n-k)}{(n-k)!}X^{n-k-1} = \frac{n!}{(n-(k+1))!}X^{n-(k+1)}.\end{aligned}$$

Damit gilt (3.2) für $n \geq k$.

SCHRITT 2 ($n < k$): Falls nun $n < k$, so gilt $k = n+m$ mit einem $m \geq 1$. Nach dem bisher Bewiesenen folgt damit

$$(X^n)^{(k)} = ((X^n)^{(n)})^{(m)} = \left(\frac{n!}{0!}X^{n-n}\right)^{(m)} = (n!)^{(m)} = 0.$$

SCHRITT 3**:** Nach Voraussetzung ist $f = \sum_{i=0}^n a_i X^i$ und es gilt $k > n$. Damit folgt aus (3.2) jetzt

$$f^{(k)} = \sum_{i=0}^n a_i \underbrace{(X^i)^{(k)}}_{=0} = 0.$$

□

3.7 Lemma (Sätzchen von Taylor)**.** Sei f ein Polynom vom Grad n. Dann gilt

$$\forall x_0 \in \mathbb{R} : f = \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!}(X - x_0)^k$$

Beweis.

SCHRITT 1**:** Per Definition gibt es $a_0, \ldots, a_n \in \mathbb{R}$, sodass

$$f = \sum_{j=0}^n a_j X^j.$$

Wir machen uns zunächst klar, dass es dann auch zu jedem $x_0 \in \mathbb{R}$ Koeffizienten b_j gibt, sodass

$$f = \sum_{j=0}^n b_j (X - x_0)^j.$$

Diese Aussage zeigen wir für jedes Polynom vom Grad $\leq n$ per Induktion nach n. Falls $n = 0$, so gilt sicherlich

$$f = a_0 X^0 = a_0 = a_0(X - x_0)^0,$$

d.h. mit $b_0 := a_0$ gilt die Aussage. Für den Induktionssschritt $n \to n+1$ sei also $f = \sum_{j=0}^{n+1} a_j X^j$. Nach Induktionsvoraussetzung erhalten wir somit b'_j mit

$$\sum_{j=0}^n a_j X^j = \sum_{j=0}^n b'_j (X - x_0)^j.$$

Daraus folgt dann

$$\begin{aligned}
f &= \sum_{j=0}^{n+1} a_j X^j = \sum_{j=0}^{n} a_j X^j + a_{n+1} X^{n+1} \\
&= \sum_{j=0}^{n} b'_j (X - x_0)^j + a_{n+1} (X - x_0 + x_0)^{n+1} \\
&\overset{2.5}{=} \sum_{j=0}^{n} b'_j (X - x_0)^j + a_{n+1} \sum_{j=0}^{n+1} \binom{n+1}{j} (X - x_0)^j x_0^{n+1-k} \\
&= \sum_{j=0}^{n} \underbrace{\left(b'_j + a_{n+1} \binom{n+1}{j} x_0^{n+1-k} \right)}_{=:b_j} (X - x_0)^j + \underbrace{a_{n+1}}_{=:b_{n+1}} (X - x_0)^{n+1}.
\end{aligned}$$

SCHRITT 2**:** In einem zweiten Schritt überlegen wir uns, dass aus

$$f = \sum_{k=0}^{n} a_k (X - x_0)^k$$

automatisch folgt, dass $a_k = \frac{f^{(k)}(x_0)}{k!}$. Denn es gilt für alle $0 \leq k \leq n$

$$\begin{aligned}
f^{(k)}(x_0) &= \sum_{j=0}^{n} a_j \left((X - x_0)^j \right)^{(k)} (x_0) \\
&= \sum_{j=0}^{k-1} a_j \left((X - x_0)^j \right)^{(k)} (x_0) + a_k \left((X - x_0)^k \right)^{(k)} (x_0) + \sum_{j=k+1}^{n} a_j \left((X - x_0)^j \right)^{(k)} (x_0) \\
&\overset{3.6}{=} a_k k!.
\end{aligned}$$

□

3.3 Nullstellen und Transzendenz

3.8 Definition (Ordnung einer Nullstelle)**.** Es sei f ein Polynom und $x_0 \in \mathbb{R}$. Dann heißt x_0 *Nullstelle von f der Ordnung m*, falls es ein Polynom g gibt, mit $g(x_0) \neq 0$ und

$$\forall x \in \mathbb{R} : f(x) = (x - x_0)^m g(x).$$

Ein $x_0 \in \mathbb{R}$ heißt *Nullstelle von f*, wenn es Nullstelle irgendeiner Ordnung ist.

3.9 Lemma (Charakterisierung von Nullstellenordnung)**.** Sei f ein Polynom und $x_0 \in \mathbb{R}$. Dann ist x_0 eine Nullstelle der Ordnung m von f genau dann, wenn gilt:

$$\forall\, k \in \{\, 0, \ldots, m-1 \,\} : \; f^{(k)}(x_0) = 0, \qquad\qquad f^{(m)}(x_0) \neq 0.$$

Beweis.

„$\Longrightarrow$“: Sei $f = (x - x_0)^m g$ mit $g(x_0) \neq 0$. Das Polynom $h(x) := (x - x_0)^m$ hat nach Lemma 3.6 die Eigenschaft, dass

$$\forall\, 0 \leq k \leq m-1 : \; h^{(k)}(x_0) = \left(\tfrac{m!}{(m-k)!} (x - x_0)^{m-k} \right) (x_0) = 0.$$

Daraus folgt für alle $0 \leq k \leq m-1$

$$f^{(k)}(x_0) = (gh)^{(k)}(x_0) \overset{(2.1)}{=} \sum_{i=0}^{k} \binom{k}{i} h^{(i)}(x_0) g^{(k-i)}(x_0) = 0. \tag{3.4}$$

Ebenfalls nach Lemma 3.6 gilt $h^{(m)} = m!$. Da $g(x_0) \neq 0$ nach Voraussetzung folgt:

$$f^{(m)}(x_0) \overset{(2.1)}{=} \sum_{k=0}^{m} \binom{m}{k} h^{(k)}(x_0) g^{m-k}(x_0) \overset{(3.4)}{=} g^{(0)}(x_0) = g(x_0) \neq 0.$$

„$\Longleftarrow$“: Das Polynom f hat irgendeinen Grad d und kann somit gemäß Lemma 3.7 geschrieben werden als

$$f(x) = \sum_{i=0}^{d} a_i (x-x_0)^i, \qquad a_i = \frac{f^{(i)}(x_0)}{i!}.$$

Nun gilt nach Voraussetzung, dass $a_i = 0$ für alle $0 \leq i \leq m-1$. Also

$$f(x) = \sum_{i=m}^{d} a_i (x-x_0)^i = \sum_{i=0}^{d-m} a_{i+m} (x-x_0)^{i+m} = (x-x_0)^m \underbrace{\sum_{i=0}^{d-m} a_{i+m} (x-x_0)^i}_{=:g},$$

wobei

$$g(x_0) = a_{0+m} = a_m = \frac{f^{(m)}(x_0)}{m!} \neq 0.$$

□

3.10 Definition (transzendent)**.** Eine Zahl $x \in \mathbb{R}$ heißt *algebraisch*, falls es ein rationales Polynom $f \in \mathbb{Q}[X]$ gibt, sodass $f(x) = 0$. Eine Zahl $x \in \mathbb{R}$ heißt *transzendent*, falls sie nicht algebraisch ist, d.h. wenn es also kein rationales Polynom f gibt, sodass $f(x) = 0$.

3.11 Definition (rational, ganzzahlig)**.** Ein Polynom $f = \sum_{k=0}^{n} a_k X^k$ heißt *rational*, falls für alle $0 \leq k \leq n$ gilt $a_k \in \mathbb{Q}$. Ein Polynom heißt *ganzzahlig* , falls für alle $0 \leq k \leq n$ gilt $a_k \in \mathbb{Z}$. Die Menge dieser Polynome notieren wir entsprechend mit $\mathbb{Q}[X]$ bzw. $\mathbb{Z}[X]$.

3.12 Lemma (Charakterisierung von Transzendenz)**.** Eine Zahl $x \in \mathbb{R}$ ist transzendent genau dann, wenn x nicht Nullstelle eines ganzzahligen Polynoms ist.

Beweis. Sei $x \in \mathbb{R}$. Wir zeigen, dass x genau dann Nullstelle eines rationalen Polynoms ist, wenn x Nullstelle eines ganzzahligen Polynoms ist.

„$\Longrightarrow$“: Sei x Nullstelle des rationalen Polynoms $f = \sum_{k=0}^{n} a_k X^k$. Da alle $a_k \in \mathbb{Q}$ kann man diese als gekürzte Brüche $a_k = \frac{p_k}{q_k}$ schreiben. Sei $b := q_0 \ldots q_n$ das Produkt der Nenner. Dann gilt sicherlich, dass $ba_k \in \mathbb{Z}$ und es folgt

$$0 = b \cdot 0 = bf(x) = \sum_{k=0}^{n} ba_k x^k$$

und somit ist x Nullstelle des ganzzahligen Polynoms $\sum_{k=0}^{n} ba_k X^k$.

„$\Longleftarrow$“: Da $\mathbb{Z} \subset \mathbb{Q}$, ist ein ganzzahliges Polynom insbesondere auch ein rationales Polynom.

□

3.4 Teilbarkeit

3.13 Definition (Teilbarkeit)**.** Seien $x, y \in \mathbb{Z}$. Dann sagen wir, dass die Zahl x die Zahl y *teilt*, falls es ein $k \in \mathbb{Z}$ gibt, sodass $y = kx$. Wir notieren dann $x \mid y$. In Zeichen

$$x \mid y :\Longleftrightarrow \exists k \in \mathbb{Z} : y = kx.$$

Falls x nicht y teilt, dann schreiben wir $x \nmid y$.

3.14 Lemma (Teilbarkeit von Summen und Produkten)**.** Seien $a, b, c \in \mathbb{Z}$.

(i). Gilt $a \mid b$ und $a \mid c$, dann folgt $a \mid b + c$.

(ii). Gilt $a \nmid b$ und $a \mid c$, dann folgt $a \nmid b + c$.

(iii). Gilt $a \mid b$, dann folgt $a \mid bc$.

(iv). Ist p eine Primzahl und gilt $p \nmid b$ und $p \nmid c$, dann gilt $p \nmid bc$.

Beweis.

(i). Per Definition gibt es $k, n \in \mathbb{Z}$, sodass $b = ka$ und $c = na$. Also gilt $b + c = ka + na = a(k + n)$ und somit $a \mid b + c$.

(ii). Angenommen $a \mid b + c$. Dann gibt es ein $n \in \mathbb{Z}$, sodass $b + c = na$. Nach Voraussetzung gilt $a \mid c$, d.h. es existiert $k \in \mathbb{Z}$, sodass $c = ka$. Dann folgt

$$na = b + c = b + ka \Longrightarrow b = na - ka = (n - k)a \Longrightarrow a \mid b.$$

Widerspruch!

(iii). Es gibt also $n \in \mathbb{Z}$ mit $b = na$. Also ist $bc = nac$ und somit gilt $a \mid bc$.

(iv). Es folgt, dass p weder in der Primfaktorzerlegung von b noch in der Primfaktorzerlegung von c vorkommt. Also kommt es auch nicht in der Primfaktorzerlegung von bc vor.

□

4 Lemmata

"You think you know pain, Nephalem?"
AZMODAN, LORD OF SIN, 1285

4.1 Lemma (Die Fakultät geht ab)**.** Es gilt für jedes $c \in \mathbb{R}_{\geq 0}$

$$\lim_{n\to\infty} \frac{c^n}{n!} = 0.$$

Beweis. Sei $\bar{c} := \lceil c \rceil$, d.h. $\bar{c}$ erhält man, indem man c auf die nächste natürliche Zahl aufrundet. Für alle $n \geq \bar{c}$ gilt

$$0 \leq \frac{c^n}{n!} \leq \frac{\bar{c}^n}{n!} = \underbrace{\frac{\bar{c}}{1} \cdot \frac{\bar{c}}{2} \cdot \ldots \cdot \frac{\bar{c}}{\bar{c}}}_{=:K} \cdot \underbrace{\frac{\bar{c}}{(\bar{c}+1)} \cdot \frac{\bar{c}}{\bar{c}+2} \cdots \frac{\bar{c}}{n-1}}_{\leq 1} \cdot \frac{\bar{c}}{n} \leq K \frac{\bar{c}}{n}$$

Da die Konstante K nicht von n abhängt, folgt nach dem "Sandwichlemma", siehe Lemma 2.4,

$$0 \leq \lim_{n\to\infty} \frac{c^n}{n!} \leq \lim_{n\to\infty} K \frac{\bar{c}}{n} = 0$$

und somit die Behauptung. □

4.2 Lemma („α"-Lemma)**.** Angenommen es gibt ein ganzzahliges Polynom $\varphi = \sum_{k=0}^{n} c_k X^k$ mit $\varphi(e) = 0$. Sei f ein Polynom und $F := \sum_{i=0}^{\infty} f^{(i)}$. Dann gibt es $\alpha_1, \dots, \alpha_n \in]0,1[$, sodass

$$\sum_{k=0}^{n} c_k F(k) = \sum_{k=1}^{n} c_k \beta_k, \qquad \beta_k := -k e^{k(1-\alpha_k)} f(k\alpha_k). \tag{4.1}$$

Beweis.
SCHRITT 1 (F verstehen): Die Definition $F := \sum_{i=0}^{\infty} f^{(i)}$ bedarf einer Erklärung: Falls $f = 0$, so bedeutet diese Gleichung, dass auch $F = 0$. Ansonsten hat f irgendeinen endlich Grad r, d.h. $r = \operatorname{grad} f$. Dann gilt aber gemäß eq. (3.3)

$$\forall i \geq r+1 : f^{(i)} = 0.$$

Daher ist F in Wirklichkeit eine endliche Summe, d.h. es gilt

$$\forall x \in \mathbb{R} : F(x) = \sum_{i=0}^{r} f^{(i)}(x).$$

Insbesondere ist F ebenfalls ein Polynom. Für die Ableitung von F erhalten wir

$$F' = \sum_{i=0}^{r} f^{(i+1)} = \underbrace{f^{(r+1)}}_{=0} + \sum_{i=1}^{r} f^{(i)} = F - f. \tag{4.2}$$

SCHRITT 2 (Hilfsfunktion g einführen): Wir definieren nun die Hilfsfunktion

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto e^{-x} F(x). \end{aligned}$$

Deren Ableitung lässt sich mit der Produktregel bestimmen. Es gilt für alle $x \in \mathbb{R}$

$$\begin{aligned} g'(x) &= -e^{-x} F(x) + e^{-x} F'(x) \\ &\overset{(4.2)}{=} -e^{-x} F(x) + e^{-x}(F(x) - f(x)) \\ &= -e^{-x} f(x). \end{aligned} \tag{4.3}$$

SCHRITT 3 (Mittelwertsatz auf g anwenden): Sei nun $1 \leq k \leq n$ beliebig, aber fest gewählt. Nach dem Mittelwertsatz, Korollar 2.2, angewandt auf das Interval $[0,k]$ erhalten wir ein $\alpha_k \in]0,1[$, sodass

$$g(k) - g(0) = g'(0 + \alpha_k(k-0))(k-0) = g'(\alpha_k k)k.$$

Setzt man in diese Gleichung die Definition von g bzw. den Ausdruck (4.3) für g' ein, so erhält man

$$\begin{aligned} &\Longrightarrow e^{-k} F(k) - e^0 F(0) = -e^{-\alpha_k k} f(\alpha_k k) k \\ &\Longrightarrow e^{-k} F(k) - F(0) = -k e^{-\alpha_k k} f(\alpha_k k) \\ &\Longrightarrow F(k) - e^k F(0) = -k e^{k - \alpha_k k} f(\alpha_k k) = \beta_k, \end{aligned}$$

wobei die β_k in Gleichung (4.1) definiert wurden. Wir haben also erreicht, dass

$$\forall 1 \leq k \leq n : \beta_k = F(k) - e^k F(0). \tag{4.4}$$

SCHRITT 4 (Beziehung zwischen β_k und c_k herstellen): Wir erinnern uns, dass die $\varphi = \sum_{k=0}^n c_k X^k$. Damit erhält man aus (4.4)

$$c_k\beta_k = c_k F(k) - c_k e^k F(0).$$

Wenn wir das jetzt von 1 bis n aufsummieren, erhalten wir

$$\sum_{k=1}^n c_k F(k) - c_k e^k F(0) = \sum_{k=1}^n c_k\beta_k \tag{4.5}$$

Nach Voraussetzung ist $\varphi(e) = 0$, was nichts andereres bedeutet als

$$0 = \varphi(e) = \sum_{k=0}^n c_k e^k \Longrightarrow \sum_{k=1}^n c_k e^k = -c_0. \tag{4.6}$$

Damit kann man (4.5) umformen zu

$$\sum_{k=1}^n c_k\beta_k = \sum_{k=1}^n c_k F(k) - F(0)\sum_{k=1}^n c_k e^k \overset{(4.6)}{=} \sum_{k=1}^n c_k F(k) + c_0 F(0) = \sum_{k=0}^n c_k F(k).$$

Und das war zu zeigen.

□

4.3 Lemma (Teilbarkeit der Ableitung)**.** Sei $g \in \mathbb{Z}[X]$, also ein Polynom mit ganzzahligen Koeffizienten, $p \in \mathbb{N}_{>0}$ und $i \in \mathbb{N}_{\geq p}$. Dann gilt für $f := \frac{g}{(p-1)!}$ und alle $i \geq p$, dass die Koeffizienten von $f^{(i)}$ ganzzahlig und sogar durch p teilbar sind.

Beweis.
SCHRITT 1 ($g = X^n$,$i = p$): Wir zeigen die Aussage zuerst für $g = X^n$ mit $n \in \mathbb{N}$ und $i = p$. Es gilt

$$f^{(p)} = \left(\frac{X^n}{(p-1)!}\right)^{(p)} \overset{3.6}{=} \frac{n!}{(p-1)!(n-p)!}X^{n-p} = p\frac{n!}{p!(n-p)!}X^{n-p} = p\binom{n}{p}X^{n-p} \in \mathbb{Z}[X]$$

SCHRITT 2 ($i = p$): Die Aussage für ein allgemeines Polynom g folgt nun wegen der Linearität der Ableitung: Sei g von Grad $d \in \mathbb{N}$ mit Koeffizienten a_k (für $k = 0, \ldots, d$): $g(X) = \sum_{k=0}^d a_k X^k$. Dann gilt:

$$f^{(p)} = \left(\frac{g}{(p-1)!}\right)^{(p)} = \left(\frac{\sum_{k=0}^d a_k X^k}{(p-1)!}\right)^{(p)} = \sum_{k=0}^d a_k\left(\frac{X^k}{(p-1)!}\right)^{(p)} = \sum_{k=0}^d p\binom{k}{p}a_k X^{k-p}.$$

Also ist Aussage für die p-te Ableitung erfüllt.

SCHRITT 3**:** Daraus folgt die Aussage auch für $i \in \mathbb{N}_{\geq p}$. Denn beim Ableiten bleiben die Teilbarkeit und Ganzzahligkeit der Koeffizienten durch p erhalten.

□

5 Beweis der Transzendenz

"And I thought cigars tasted bad!"
DUKE NUKEM, 1996

Dieser Beweis orientiert sich an einem Post im Blog von Prof. Dave Richeson, siehe [1]. Wie dort nachzulesen stammt die Idee zu diesem Beweis von Charles Hermite aus dem Jahre 1873. Der Beweis wurde 1893 von Adolf Hurwicz vereinfacht.

5.1 Satz. Die Zahl e ist transzendent.

Beweis.

SCHRITT 1 (Strategie): Unsere gundsätzliche Strategie ist ein Widerspruchsbeweis. Es sei also angenommen, dass e nicht transzendent ist. Dann ist e Nullstelle eines rationalen Polynoms. Nach Lemma 3.12 gibt es dann auch ein ganzzahliges Polynom $\varphi = \sum_{k=0}^{n} c_k X^k$ vom Grad $n > 0$, sodass $\varphi(e) = 0$. Sei außerdem p eine beliebige Primzahl, sodass $p \geq \max(c_0, n)$. (Eine solche kann man stets finden, da die Menge der Primzahlen unbeschränkt ist.)

SCHRITT 2 (Hilfspolynom formulieren): Damit definieren wir das Hilfspolynom

$$f := \frac{X^{p-1}}{(p-1)!} \prod_{k=1}^{n} (k - X)^p. \tag{5.1}$$

Wenn man diese Formel ausmultipliziert sieht man, dass f auch wirklich ein Polynom ist, und zwar vom Grad $r := p(n+1) - 1$. Nach Lemma 4.2 gibt es dann $\alpha_1, \ldots, \alpha_n \in]0, 1[$, sodass für die dort definierte Funktion $F = \sum_{i=0}^{\infty} f^{(i)}$ (bezüglich des in (5.1) definierten f) gilt:

$$\sum_{k=0}^{n} c_k F(k) = \sum_{k=1}^{n} c_k \beta_k, \qquad \beta_k = -k e^{k(1-\alpha_k)} f(k\alpha_k). \tag{5.2}$$

SCHRITT 3 ($p \nmid z$): Wir behaupten, dass daraus folgt

$$z := \sum_{k=0}^{n} c_k F(k) \in \mathbb{Z} \setminus \{0\}, \qquad p \nmid z, \tag{5.3}$$

d.h. wir behaupten, dass nicht nur $z \neq 0$, sondern dass sogar z nicht durch p teilbar ist.

SCHRITT 3.1 ($p \mid f^{(i)}(k)$): Wendet man Lemma 4.3 auf das Polynom $g := X^{p-1} \prod_{k=1}^{n} (k - X)^p$ an, so erhält man, dass für alle $i \geq p$ das Polynom $f^{(i)}$ ganzzahlig ist und alle Koeffizienten sogar durch p teilbar sind. Insbesondere gilt also

$$\forall i \geq p : \forall k \in \mathbb{Z} : p \mid f^{(i)}(k). \tag{5.4}$$

SCHRITT 3.2 ($p \mid F(k), 1 \leq k \leq n$): Aus der Definition von f sieht man, dass jedes $1 \leq k \leq n$ eine Nullstelle der Ordnung p von f ist. Aus Lemma 3.9 folgt damit also

$$\forall\, 0 \leq i \leq p-1 : \forall\, 1 \leq k \leq n : f^{(i)}(k) = 0. \tag{5.5}$$

Damit gilt also

$$\forall 1 \leq k \leq n : F(k) = \sum_{i=0}^{\infty} f^{(i)}(k) \overset{(5.5)}{=} \sum_{i=p}^{r} f^{(i)}(k). \tag{5.6}$$

Da gemäß (5.4) alle $f^{(i)}(k)$ durch p teilbar sind, ist auch $F(k)$ durch p teilbar, siehe Lemma 3.14. Wir haben also gezeigt:

$$\forall 1 \leq k \leq n : p \mid F(k). \tag{5.7}$$

SCHRITT 3.3 ($p \nmid F(0)$): Wir betrachten nun andererseits den Fall $k = 0$. Nach Definition von f ist $k = 0$ eine Nullstelle von f der Ordnung $p - 1$. Also gilt (erneut unter Verwendung von Lemma 3.9) insbesondere

$$F(0) = \sum_{i=0}^{r} f^{(i)}(0) = \sum_{i=p-1}^{r} f^{(i)}(0).$$

Aus Lemma 4.3 folgt wie gesagt, dass $f^{(p)}(0), \ldots, f^{(r)}(0)$ durch p teilbar ist. Wir wollen zeigen, dass jedoch $f^{(p-1)}(0)$ nicht durch p teilbar ist. Gemäß Lemma 3.14 ist dann auch $F(0)$ nicht durch p teilbar und wir sind fertig (mit diesem Teilschritt). Um nun also $p \nmid f^{(p-1)}(0)$ zu zeigen, gehen wir wie folgt vor: Würde man in der Definition (5.1) von f alle Produkte ausmultiplizieren, so würde man eine Darstellung von f der Form

$$f = \sum_{k=p-1}^{r} a_k X^k, \qquad a_{p-1} = \frac{(n!)^p}{(p-1)!}$$

erhalten. Daraus folgt

$$f^{(p-1)}(0) \overset{(3.2)}{=} \tfrac{(p-1)!}{0!} a_{p-1} = (n!)^p.$$

Nach Voraussetzung ist $p > n$ und somit teilt p nicht $(n!)^p = f^{(p-1)}(0)$. Und das wollten wir hier zeigen.

SCHRITT 3.4 (Ergebnis): Unter massiver Verwendung von Lemma 3.14 argumentieren wir jetzt wie folgt: $F(0)$ ist nicht durch p teilbar. Da $p > c_0$, ist c_0 nicht durch p teilbar. Also gilt $p \nmid c_0 F(0)$. Da $p \mid F(k)$ für $1 \le k \le n$, folgt $p \mid c_k F(k)$ und somit $\sum_{k=1}^{n} c_k F(k)$. Folglich gilt $p \nmid z$. Insbesondere ist $z \neq 0$.

SCHRITT 4: Wir möchten nun zeigen, dass andererseits

$$\left| \sum_{k=1}^{n} c_k \beta_k \right| < 1. \tag{5.8}$$

SCHRITT 4.1 (Abschätzung für β_k): Aus (5.2) wissen wir, dass für $1 \le k \le n$ gilt:

$$\beta_k = -k e^{k(1-\alpha_k)} f(k\alpha_k).$$

Mit der Definition von f in (5.1) liefert dies

$$\beta_k = -e^{k(1-\alpha_k)} \frac{k\,(k\alpha_k)^{p-1}}{(p-1)!} \prod_{k=1}^{n} (k - k\alpha_k)^p. \tag{5.9}$$

Aufgrund der Monotie der Exponentialfunktion (Satz 2.7) und der Tatsache, dass $0 < \alpha_k < 1$ und $k \le n$ folgt, dass

$$e^{k(1-\alpha_k)} \le e^n \tag{5.10}$$

und

$$k\,(k\alpha_k)^{p-1} \le k k^{p-1} = k^p \le n^p. \tag{5.11}$$

Außerdem gilt für alle $1 \leq k \leq n$

$$\begin{array}{rrcl} & \alpha_k & > & 0 \\ \Leftrightarrow & -\alpha_k & < & 0 \\ \Leftrightarrow & -k\alpha_k & < & 0 \\ \Leftrightarrow & k - k\alpha_k & < & k, \end{array}$$

was zu

$$\prod_{k=1}^{n} (k - k\alpha_k)^p < \prod_{k=1}^{n} k^p = \left(\prod_{k=1}^{n} k \right)^p = (n!)^p \,. \tag{5.12}$$

führt. Setzt man (5.10), (5.11) und (5.12) in (5.9) ein, so erhält man

$$|\beta_k| \leq \frac{e^n n^p \, (n!)^p}{(p-1)!}. \tag{5.13}$$

SCHRITT 4.2 (Asymptotik ausnutzen): Nach Lemma 4.1 gilt

$$\lim_{p\to\infty} |\beta_k| \overset{(5.13)}{\leq} \lim_{p\to\infty} \frac{e^n \, (n \cdot n!)^p}{(p-1)!} = e^n \lim_{p\to\infty} \frac{(n \cdot n!)^p}{(p-1)!} \overset{4.1}{=} 0.$$

Also gibt es insbesondere eine Primzahl p sodass für alle $1 \leq k \leq n$ gilt, dass $|c_k \beta_k| < \frac{1}{n}$. Damit rechnen wir:

$$\left| \sum_{k=1}^{n} c_k \beta_k \right| \leq \sum_{k=1}^{n} |c_k \beta_k| < 1.$$

SCHRITT 5 (Schlussargument): Wir wissen aus (5.2), dass die Gleichheit

$$z = \sum_{k=0}^{n} c_k F(k) = \sum_{k=1}^{n} c_k \beta_k$$

besteht. Wir haben soeben (5.8) gezeigt, d.h. $|z| < 1$. Vorher haben wir aber (5.3) gezeigt, dass z ganzzahlig ist. Daraus folgt aber $z = 0$. Das steht im Widerspruch zu $z \neq 0$, was wir ebenfalls in (5.3) gezeigt haben.

□

Index

Symbolverzeichnis

e	Eulersche Zahl, page 4
$f^{(0)}$	$f^{(0)} = f$, page 5
$f^{(k)}$	k-te Ableitung von f, page 5
$\operatorname{grad} f$	der Grad von f, page 5
$\mathbb{Q}[X]$	Menge aller rationalen Polynome, page 8
$\mathbb{R}[X]$	Menge aller reellen Polynome, page 5
X	die Identität auf $\mathbb{R}$, page 5
x^y	x hoch y, page 4
$x \nmid y$	x teilt nicht y, page 9
$x \mid y$	x teilt y, page 9
$\mathbb{Z}[X]$	Menge aller ganzzahligen Polynome, page 8

Abbildungsverzeichnis

Literatur

[1] Dave Richeson. The transcendence of e. http://divisbyzero.com/2010/09/28/the-transcendence-of-e/, 2010.