Friedrich-Schiller-Universität Jena
Mathematisches Institut
Prof. Dr. David J. Green

14 Transzendenz von e und π

Die Transzendenz von e wurde 1873 von Hermite gezeigt. Auf Hermites Methoden aufbauend zeigte Lindemann 1882, dass π transzendent ist, und bewies damit endgültig die Unmöglichkeit der Quadratur des Kreises. Wir werden beide Ergebnisse von dem folgenden Satz herleiten.

Satz 14.1 *Sei $\alpha \neq 0$ eine ganze algebraische Zahl. Dann sind die Zahlen $\{e^{n\alpha} \mid n \in \mathbb{Z}\}$ linear unabhängig über $\mathbb{Q}$.*

14.1 Wie man Satz 14.1 anwendet

Korollar 14.2 *Für jede algebraische Zahl $\alpha \neq 0$ ist die Zahl e^α transzendent.*

Satz 14.3 (Hermite bzw. Lindemann) *Die Zahl e bzw. π ist transzendent, d.h. nicht algebraisch über $\mathbb{Q}$.*

Beweis von Satz 14.3. Es ist $e = e^1$, und 1 ist eine algebraische Zahl $\neq 0$. Nach Korollar 14.2 ist e transzendent. Wäre π algebraisch, dann wäre auch $i\pi$ eine algebraische Zahl $\neq 0$, denn i ist auf jedem Fall algebraisch. Nach Korollar 14.2 müsste dann $e^{i\pi}$ transzendent sein. Das stimmt aber nicht, denn es ist bekanntlich $e^{i\pi} = -1$. ∎

Um Korollar 14.2 beweisen zu können, benötigen wir zunächt einen Nachtrag zu §10:

Lemma 10.9 *Sei α eine algebraische Zahl. Dann gibt es eine ganze Zahl $n \geq 1$ derart, dass $n\alpha$ eine ganze algebraische Zahl ist.*

Somit ist $\mathbb{A}$, der Körper der algebraischen Zahlen, der Quotientenkörper von $\mathbb{B}$, der Ring der ganzen algebraischen Zahlen.

Beweis. Sei $X^r + \sum_{i=0}^{r-1} a_i X^i$ das Minimalpolynom von α über $\mathbb{Q}$. Dann ist jedes $a_i \in \mathbb{Q}$, also findet man ein $n \geq 1$ derart, dass jedes $b_i := na_i$ in $\mathbb{Z}$ liegt. Sei $\beta = n\alpha$. Dann $\frac{\beta^r}{n^r} + \sum_{i=0}^{r-1} a_i \frac{\beta^i}{n^i} = 0$. Durch Ausmultiplizieren erhält man $\beta^r + \sum_{i=0}^{r-1} n^{r-i-1} b_i \beta^i = 0$, weshalb β ganz ist.

Somit hat jede algebraische Zahl α eine Darstellung der Art $\frac{\beta}{n}$ für eine ganze algebraische Zahl β. Die Aussage über den Quotientenkörper folgt hieraus. ∎

Beweis von Korollar 14.2. Nach Lemma 10.9 ist $\beta := n\alpha$ eine ganze algebraische Zahl, für ein $n \geq 1$. Wäre e^α algebraisch, so wäre auch $e^\beta = (e^\alpha)^n$ algebraisch und hätte deshalb ein Minimalpolynom in $\mathbb{Q}[X]$. Sei m der Grad des Minimalpolynoms. Dann sind $1 = e^{0\beta}, e^\beta, e^{2\beta}, \ldots, e^{m\beta}$ linear abhängig über $\mathbb{Q}$, ein Widerspruch zu Satz 14.1. ∎

14.2 Erste Schritte im Beweis von Satz 14.1

Wir führen einen Widerspruchsbeweis und benutzen Algebra, um eine gewisse Gleichung aufzustellen, nämlich Gleichung (4). Arithmetische Überlegungen zeigen dann, dass die linke Seite eine ganze Zahl $\neq 0$ ist, aber analytische Argumente führen dazu, dass wir die rechte Seite verschwindend klein machen können. Somit haben wir den Widerspruch.

Eine wichtige Station auf dem Weg nach Gleichung (4) ist Gleichung (2). Um diese Gleichung herzuleiten, werden wir mit linearen Kombinationen von Exponentialen arbeiten. Beispiel: $e^{i\pi} + e^0$ ist eine nichttriviale lineare Kombination von Exponentialen, die aber den Wert Null annimmt. Wir brauchen folgende Tatsache: multiplizieren wir zwei nichttriviale lineare Kombinationen miteinander:

$$\sum_{i=1}^{n} a_i e^{\alpha_i} \cdot \sum_{j=1}^{m} b_j e^{\beta_j} = \sum_{i,j} a_i b_j e^{\alpha_i + \beta_j} ,$$

so ist auch deren Produkt eine nichttriviale lineare Kombination. Um besser Buch führen zu können, arbeiten wir mit der Gruppenalgebra $\mathbb{Q}[\mathbb{C}]$.

Bemerkung Ist R ein kommutativer Ring und G eine Gruppe, so wird der Gruppenring RG manchmal auch mit $R[G]$ bezeichnet. Entsprechend schreibt man dann $r_1[g_1] + \cdots + r_n[g_n]$ für das typische Element, nicht $r_1 g_1 + \cdots + r_n g_n$. Diese Schreibweise wird insbes. dann häufig gewählt, wenn G eine additive Gruppe ist. Multiplikation geht dann so:

$$r_1[g_1] \cdot r_2[g_2] = r_1 r_2[g_1 + g_2] \neq r_1 r_2[g_1] + r_1 r_2[g_2] .$$

Ferner wäre es sonst z.B. im Fall von $\mathbb{Z}[\mathbb{Z}]$ schwer, Koeffizienten von Basiselementen zu unterscheiden: so ist etwa $1[0] \neq 0$.

Beachten Sie, dass die Abbildung $\phi\colon \mathbb{Q}[\mathbb{C}] \to \mathbb{C}$, $\phi\colon \sum_{i=1}^{n} a_i[\alpha_i] \mapsto \sum_{i=1}^{n} a_i e^{\alpha_i}$ ein Homomorphismus von $\mathbb{Q}$-Algebren ist. Wir setzen voraus, dass Satz 14.1 falsch ist. Dies bedeutet, dass es ein $m \geq 1$, ganze Zahlen $n_1 < n_2 < \cdots < n_m$ und Zahlen $q_1, \ldots, q_m \in \mathbb{Q} \setminus \{0\}$ gibt, mit $\sum_{i=1}^{m} q_i e^{n_i \alpha} = 0$, d.h. mit $0 \neq \sum_{i=i}^{m} q_i[n_i\alpha] \in \mathrm{Kern}(\phi)$.

Sei K der Zerfällungskörper des Minimalpolynoms von α über $\mathbb{Q}$. Dann ist $K/\mathbb{Q}$ eine (endliche) Galoiserweiterung. Sei $G = \mathrm{Gal}(K/\mathbb{Q})$ die Galoisgruppe, und schreibe O_K für den Schnitt $K \cap \mathbb{B}$. Das heißt,

$$O_K = \{\beta \in K \mid \beta \text{ ganz über } \mathbb{Z}\} ,$$

ein Unterring von K. Nach Voraussetzung ist $\alpha \in O_K$. Sei $m_\alpha \in \mathbb{Q}[X]$ das Minimalpolynom von α als algebraisches Element über $\mathbb{Q}$. Nach Lemma 10.5 liegt m_α in $\mathbb{Z}[X]$. Nun sei $\sigma \in G$. Dann ist die sog. Galois-Konjugierte $\sigma(\alpha)$ eine Nullstelle von m_α, weshalb $\sigma(\alpha) \in O_K$. Nun setze

$$U = \prod_{\sigma \in G} \sum_{i=1}^{m} q_i[\sigma(n_i\alpha)] . \tag{1}$$

Es ist $U \in \mathbb{Q}[O_K]$, denn jeder Faktor von U liegt dort drin. Es ist auch $U \in \mathrm{Kern}(\phi)$, denn der Faktor für $\sigma = \mathrm{Id}$ im Kern liegt. Ferner ist $U \neq 0$, wegen des folgenden Lemmas, denn $[\sigma(\gamma)] = [\sigma(\delta)]$ genau dann, wenn $\gamma = \delta$.

Lemma 14.4 *Sei R ein Integritätsbereich. Dann ist auch der Gruppenring $R[\mathbb{C}]$ ein Integritätsbereich.*

Jetzt werden wir sehen, dass U außerdem invariant unter der Operation von G ist. Sei $\sigma \in G$ und sei $x = \sum_{\gamma \in K} q_\gamma[\gamma]$ ein Element aus der $\mathbb{Q}$-Algebra $\mathbb{Q}[K]$, also $q_\gamma \in \mathbb{Q}$ ist $\neq 0$ für nur endlich viele γ. Wir definieren eine Operation $(\sigma, x) \mapsto \sigma * x$ von G auf $\mathbb{Q}[K]$ durch

$$\sigma * \sum_{\gamma \in K} q_\gamma[\gamma] = \sum_{\gamma \in K} q_\gamma[\sigma(\gamma)]\,.$$

Beachten Sie, dass $x \mapsto \sigma * x$ ein $\mathbb{Q}$-Algebrenautomorphismus von $\mathbb{Q}[K]$ ist, für jedes $\sigma \in G$; das heißt, $\sigma * (x + y) = \sigma * x + \sigma * y$, $\sigma * (xy) = (\sigma * x)(\sigma * y), \sigma * (qx) = q(\sigma * x)$ für $q \in \mathbb{Q}$, und $\sigma^{-1} * (\sigma * x) = x$.

Auch U liegt in der $\mathbb{Q}$-Algebra $\mathbb{Q}[K]$, denn jeder Faktor in (1) liegt in $\mathbb{Q}[K]$. Wir zeigen jetzt, dass $\sigma * U = U$ ist, für jedes $\sigma \in G$. Es gilt nämlich $\{\sigma\tau \mid \tau \in G\} = \{\tau \mid \tau \in G\}$. Also

$$\sigma * U = \prod_{\tau \in G} \sum_{i=1}^{m} q_i[\sigma\tau(n_i\alpha)] = \prod_{\tau \in G} \sum_{i=1}^{m} q_i[\tau(n_i\alpha)] = U\,.$$

Zusammenfassend liegt $0 \neq U = \sum_{\gamma \in K} q_\gamma[\gamma]$ in $\mathrm{Kern}(\phi) \cap \mathbb{Q}[O_K]$, und es ist $\sigma * U = U$ für jedes $\sigma \in G$. Wir zeigen jetzt, dass es ein $V = \sum_{\gamma \in G} \nu_\gamma[\gamma]$ gibt, die diese Eigenschaften von U teilt, und zusatzlich $\nu_0 \neq 0$ erfüllt. Nur im Falle $q_0 = 0$ ist etwas zu zeigen. Sei $\beta \in K$ derart, dass $q_\beta \neq 0$. Da $U \in \mathbb{Q}[O_K]$ ist, muss auch β ganz sein. Sei $W = \sum_{\tau \in G}[-\tau(\beta)]$. Dann $0 \neq W \in \mathbb{Q}[O_K]$, und $\sigma * W = W$ für alle $\sigma \in G$. Setze $V = UW$. Dann $0 \neq V \in \mathbb{Q}[O_K] \cap \mathrm{Kern}(\phi)$, und $\sigma * V = V$ für jedes $\sigma \in G$. Der Koefficient von $[0]$ in $U[-\tau(\beta)]$ ist $q_{\tau(\beta)}$, also ist $\sum_{\tau \in G} q_{\tau(\beta)}$ der Koeffizient ν_0 von $[0]$ in V. Wegen $\sigma * U = U$ folgt $q_{\tau(\beta)} = q_\beta$, d.h. $\nu_0 = |G| q_\beta \neq 0$.

Indem wir jetzt V mit einer geeigneten ganzen Zahl multiplizieren, können wir die Nenner der ν_γ wegmachen. Somit haben wir gezeigt:

Lemma 14.5 *Sei $\alpha \neq 0$ eine ganze algebraische Zahl. Sei K der Zerfällungskörper des Minimalpolynoms von α über $\mathbb{Q}$, und sei $G = \mathrm{Gal}(K/\mathbb{Q})$.*

Ist e^α algebraisch über $\mathbb{Q}$, so gibt es ein $0 \neq k \in \mathbb{Z}$, ein $n \geq 1$, ganze Zahlen $a_1, \ldots, a_n$ und paarweis verschiedene Elemente $\beta_1, \ldots, \beta_n \in O_K \setminus \{0\}$ derart, dass

$$k + \sum_{i=1}^{n} a_i e^{\beta_i} = 0\,, \tag{2}$$

und für jedes $\sigma \in G$ und für jedes i gilt: $\sigma(\beta_i)$ ist ein β_j, und es ist $a_i = a_j$.

Beweis. Wir wechseln die Bezeichnung und schreiben V als $k[0] + \sum_{i=1}^{n} a_i[\beta_i]$. Gleichung (2) entspricht $V \in \mathrm{Kern}(\phi)$. Die $\sigma(\beta_i)$-Bedingung entspricht $\sigma * V = V$. Wegen $V \in \mathbb{Q}[O_K]$ sind die β_i ganz. ∎

Beweis von Lemma 14.4. Die Eins ist $1[0] \neq 0$. Betrachten wir folgende Totalordnung auf $\mathbb{C}$: $x + iy \leq a + ib$ genau dann, wenn entweder $x < a$ gilt oder $x = a$ und $y \leq b$ gelten: dies ist die sogenannte lexikographische Ordnung. Beachten Sie, dass für $z_1, z_2, w, w_1, w_2 \in \mathbb{C}$ es ist $z_1 \leq z_2$ genau dann, wenn $z_1 + w \leq z_2 + w$; und aus $z_1 \leq w_1$ und $z_2 \leq w_2$ folgt $z_1 + z_2 \leq w_1 + w_2$. Somit verträgt sich die Ordnung mit der Addition.

Ist $0 \neq f \in R[\mathbb{C}]$, so hat f einen führenden Term $r[z]$, d.h. es ist $r \in R \setminus \{0\}$ und

$$f = r[z] + (\text{Terme } s[w] \text{ mit } w < z)\,.$$

Sind f_1, f_2 zwei Elemente aus $R[\mathbb{C}]$ mit führenden Term $r_1[z_1]$ bzw. $r_2[z_2]$, so ist $r_1 r_2[z_1 + z_2]$ der führende Term von $f_1 f_2$, und es ist insbesondere $f_1 f_2 \neq 0$. ∎

14.3 Konstruktion der Funktion F

In diesem Unterabschnitt leiten wir die Gleichung (4) her. Sei $\theta \in \mathbb{Q}[X]$ das Produkt (ohne wiederholte Faktoren) der Minimalpolynome der Zahlen β_i aus Lemma 14.5. Da die β_i ganz sind, ist $\theta(X)$ ein normiertes Polynom in $\mathbb{Z}[X]$. Da jedes $\sigma(\beta_i)$ ein β_j ist, ist jede Nullstelle von $\theta(X)$ ein β_j, und auch umgekehrt. Somit stimmt der Grad von $\theta(X)$ mit der Zahl n aus Gleichung (2) überein.

Beispiel Die Gleichung (2) könnte so lauten:

$$e^i + e^{-i} - 2e^{\sqrt[3]{2}} - 2e^{\omega\sqrt[3]{2}} - 2e^{\bar{\omega}\sqrt[3]{2}} + 7 = 0\,.$$

In diesem Fall wäre $\theta(X) = (X^2+1)(X^3-2)$.

Jetzt wählen wir eine Primzahl p und setzen

$$\begin{aligned} f(X) &= \frac{X^{p-1}\theta(X)^p}{(p-1)!} \in \mathbb{Q}[X] \\ F(X) &= f(X) + f'(X) + f''(X) + \cdots + f^{(np+p-1)}(X) \in \mathbb{Q}[X]\,. \end{aligned}$$

Beachten Sie, dass $f(X)$ vom Grad $np+p-1$ ist, weshalb $f^{(np+p)}(X) = 0$. Hieraus und aus der Definition von F folgt es, dass

$$\frac{d}{dx}\left(e^{-x}F(x)\right) = -e^{-x}f(x)\,.$$

Nach dem Hauptsatz ist also

$$e^{-x}F(x) - F(0) = -\int_0^x e^{-y}f(y)dy\,.$$

Durch die Substitution $y = \lambda x$ erhalten wir

$$F(x) - e^x F(0) = -x\int_0^1 e^{(1-\lambda)x}f(\lambda x)d\lambda\,. \tag{3}$$

Jetzt kombinieren wir die Gleichungen (2) und (3). Es ist

$$\sum_{i=1}^n a_i F(\beta_i) - F(0)\sum_{i=1}^n a_i e^{\beta_i} = -\sum_{i=1}^n a_i\beta_i \int_0^1 e^{(1-\lambda\beta_i)}f(\lambda\beta_i)d\lambda\,,$$

weshalb

$$\sum_{i=1}^n a_i F(\beta_i) + kF(0) = -\sum_{i=1}^n a_i\beta_i \int_0^1 e^{(1-\lambda\beta_i)}f(\lambda\beta_i)d\lambda\,. \tag{4}$$

14.4 Die linke Seite der Gleichung (4)

Jedes β_i ist eine p-fache Nullstelle von f. Somit ist $f^{(r)}(\beta_i) = 0$ für $r \le p-1$; und für $r \ge p$ ist $f^{(r)}(\beta_i)$ eine durch p teilbare ganze algebraische Zahl[1] in K. Somit ist $\sum_{i=1}^n a_i F(\beta_i)$ eine

[1] Das heißt, $f^{(r)}(\beta_i) = p\gamma$ für eine ganze algebraische Zahl γ.

durch p teilbare ganze algebraische Zahl in K. Ferner ist $\sigma(\sum_{i=1}^n a_i F(\beta_i)) = \sum_{i=1}^n a_i F(\beta_i)$ für jedes $\sigma \in G = \mathrm{Gal}(K(\mathbb{Q}))$, denn σ permutiert die β_i mit dem gleichen Wert von a_i. Das heißt, $\sum_{i=1}^n a_i F(\beta_i)$ liegt in $\mathbb{Z}$ und ist durch p teilbar.

Wir wollen zeigen, dass die linke Seite der Gleichung (4) eine ganze Zahl $\neq 0$ ist. Hierfür reicht es nach den obigen Überlegungen zu zeigen, dass $kF(0)$ eine nicht durch p teilbare ganze Zahl ist. Nun, $f^{(r)}(0)$ ist 0 für $r < p-1$, und für $r \geq p-1$ ist es eine ganze Zahl. Diese Zahl ist durch p teilbar für $r \geq p$, dagegen ist $f^{(p-1)}(0) = \theta(0)^p$.

Somit ist die linke Seite der Gleichung eine ganze Zahl, die kongruent $k\theta(0)^p$ modulo p ist. Da θ ein Produkt von minimalen Polynomen von Zahlen $\neq 0$ ist, ist $\theta(0) \neq 0$; da die β_i alle ganz sind, ist $\theta(0) \in \mathbb{Z}$. Wählen wir jetzt $p > \max\{|k|, |\theta(0)|\}$, so ist $k\theta(0)^p$ nicht durch p teilbar. Wir haben gezeigt:

Lemma 14.6 *Die linke Seite der Gleichung* (4) *ist eine ganze Zahl. Für p groß genug ist diese Zahl ungleich Null.* ∎

14.5 Die rechte Seite der Gleichung (4)

Sei $m(i) = \sup\{|\theta(\lambda\beta_i)| \mid \lambda \in [0,1]\}$. Für $\lambda \in [0,1]$ gilt dann $|f(\lambda\beta_i)| \leq \frac{|\beta_i|^{p-1} m(i)^p}{(p-1)!}$, weshalb $\left|a_i\beta_i \int_0^1 e^{(1-\lambda\beta_i)} f(\lambda\beta_i) d\lambda\right| \leq |a_i| \frac{|\beta_i m(i)|^p}{(p-1)!} \left|\int_0^1 e^{(1-\lambda)\beta_i} d\lambda\right|$. Dieses strebt gegen Null für $p \to \infty$, denn $\frac{a^n}{(n-1)!} \to 0$ für $n \to \infty$. Somit strebt die rechte Seite der Gleichung (4) gegen Null für $p \to \infty$.

Beweis von Satz 14.1 (Zusammenfassung). Wir setzten eine lineare Abhängigkeit voraus, und folgerten in Gleichung (2), dass es eine Galois-invariante lineare Abhängigkeit mit ganzzähligen Koeffizienten und einem nicht verschwindenden konstanten Term geben müsste. Danach wählten wir eine Primzahl p, konstruierten die Funktionen f and F, and leiteten Gleichung (4) her. Eigenschaften von ganzen Zahlen bedeuteten einerseits, dass die linke Seite dieser Gleichung eine ganze Zahl $\neq 0$ sein muss; anderseits führt eine einfache Abschätzung dazu, dass die rechte Seite gegen Null strebt für $p \to \infty$. Dies ist aber ein Widerspruch. ∎

Bemerkung Quellen: Die zweite Hälfte des Beweises folgt dem Beweis der Transzendenz von π in §6 von I. Stewart, *Galois Theory*. Die erste Hälfte ist ein Spezialfall des Beweises des Satzes von Lindemann–Weierstraß in N. Jacobson, *Basic Algebra I*.