Ist die Quadratur des Kreises möglich?

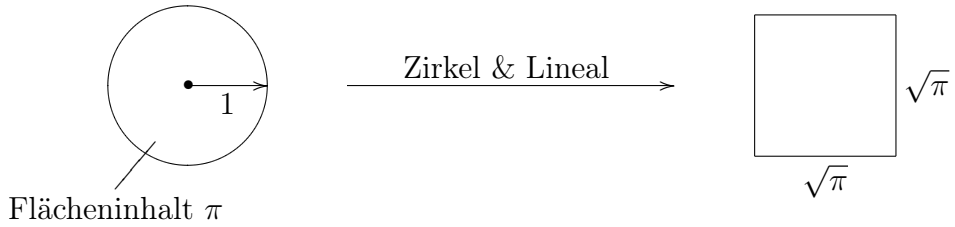
Teilnehmer:

Bodo Graumann	Heinrich-Hertz-Oberschule
Anja Kunkel	Andreas-Oberschule
Daniel Lupp	Herder-Oberschule
Peat Schmolke	Heinrich-Hertz-Oberschule
Dennis Sperlich	Heinrich-Hertz-Oberschule
Sandra Weise	Andreas-Oberschule

Gruppenleiter:

Jürg Kramer	HU Berlin
Anna v. Pippich	HU Berlin

Über 2000 Jahre hat das Problem der Quadratur des Kreises die Mathematiker beschäftigt und vorangetrieben. Schon die alten Griechen stellten sich die Aufgabe, allein mit Hilfe von Zirkel und Lineal aus einem vorgegebenen Kreis ein Quadrat mit demselben Flächeninhalt zu konstruieren:



Wir haben im Zuge unserer Untersuchungen erkannt, dass die Konstruierbarkeit (ebener) geometrischer Objekte mit Zirkel und Lineal mit feineren Eigenschaften der reellen Zahlen zusammenhängt. Deshalb haben bei unserer Arbeit neben geometrischen Aspekten vor allem interessante algebraische bzw. zahlentheoretische Fragestellungen eine prominente Rolle gespielt.

Mit unserem Ansatz haben wir dabei weiterhin das mit der Quadratur verwandte Problem der Würfel-(Volumen)-Verdoppelung betrachtet und bearbeitet.

1 Algebraische und transzendente Zahlen

1.1 Was ist Algebraizität?

Definition 1.1. *Eine reelle Zahl α heißt* algebraisch vom Grad n, *wenn sie Nullstelle eines Polynoms*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

vom Grad $n > 0$ mit ganzzahligen Koeffizienten $a_0, \ldots, a_n$ ist, aber keiner polynomialen Gleichung kleineren Grades dieser Art genügt.

Wir bezeichnen die Menge der algebraischen Zahlen mit $\overline{\mathbb{Q}}$.

Die Menge der algebraischen Zahlen $\overline{\mathbb{Q}}$ enthält alle rationalen Zahlen, denn jede rationale Zahl $r = m/n$ ($m, n \in \mathbb{Z}$; $n > 0$) ist algebraisch vom Grad 1, da sie Nullstelle des Polynoms

$$f(x) = nx - m$$

ist. Daher kann eine algebraische Zahl vom Grad $n > 1$ nicht rational sein.

Satz 1.2. *Die Quadratwurzel $\sqrt{2}$ ist algebraisch vom Grad 2.*

Beweis. Im Folgenden wird die Irrationalität von $\sqrt{2}$ mithilfe der unendlichen Abstiegsmethode bewiesen. Hierzu wird angenommen, dass es sich bei $\sqrt{2}$ um eine rationale Zahl handelt, d.h.

$$\sqrt{2} \in \mathbb{Q} \Rightarrow \exists\, x, y \in \mathbb{Z}_{\neq 0} : \sqrt{2} = \frac{x}{y}.$$

Durch Umstellen ergibt sich

$$\sqrt{2} = \frac{x}{y} \Rightarrow x^2 = 2 \cdot y^2.$$

Da 2 ein Teiler von $2 \cdot y^2$ ist, muss 2 auch Teiler von x^2 sein. Die ganze Zahl x lässt sich eindeutig in Primfaktoren zerlegen. Durch Quadrierung von x kommt jeder Primfaktor in geradzahliger Vielfachheit vor, weshalb insbesondere 2 auch Teiler von x sein muss. Wir haben

$$2|2 \cdot y^2 \Rightarrow 2|x^2 \Rightarrow 2|x.$$

Durch Halbierung von x erhält man durch Umstellen und Einsetzen in die Ursprungsgleichung

$$\exists\, x_1 \in \mathbb{Z}_{\neq 0} :\ x = 2 \cdot x_1 \Rightarrow 2 \cdot x_1^2 = y^2.$$

Die gleiche Methode wird ein weiteres Mal angewendet; wir erhalten

$$2|2 \cdot x_1^2 \Rightarrow 2|y^2 \Rightarrow 2|y \Rightarrow \exists\, y_1 \in \mathbb{Z}_{\neq 0} : \; y = 2 \cdot y_1 \Rightarrow x_1^2 = 2 \cdot y_1^2.$$

Man kann dies unendlich fortsetzen. Wir erhalten immer wieder eine Gleichung der Form $x_j^2 = 2 \cdot y_j^2$ mit $x_j, y_j \in \mathbb{Z}_{\neq 0}$ $(j = 1, 2, \ldots)$. Hier liegt auch der Widerspruch: wir haben gezeigt, dass x_j, y_j immer wieder durch 2 teilbar sind. Bei ganzen, von Null verschiedenen Zahlen kann man diesen Prozess jedoch nicht unendlich fortsetzen, da irgendwann eine Zahl erreicht wird, die nicht mehr durch 2 teilbar ist.

Also ist $\sqrt{2}$ nicht rational. Da sie jedoch Nullstelle des Polynoms $f(x) = x^2 - 2$ ist, wurde sie hiermit als algebraisch vom Grad 2 nachgewiesen. □

Bemerkung. Damit sehen wir also, dass es auch algebraische Zahlen außerhalb von $\mathbb{Q}$ gibt, d.h. $\mathbb{Q}$ ist eine echte Teilmenge von $\overline{\mathbb{Q}}$.

Wir wissen bis jetzt, dass die algebraischen Zahlen im Bereich der reellen Zahlen liegen. Es könnte nun sein, dass alle reellen Zahlen automatisch algebraisch sind. Wir wollen deshalb der Frage nachgehen, ob reelle Zahlen existieren, die nicht algebraisch sind. Diese Zahlen würden wir als transzendente Zahlen bezeichnen.

Definition 1.3. *Die Menge $\mathbb{T}$ der transzendenten Zahlen ist die Komplementärmenge von $\overline{\mathbb{Q}}$ in $\mathbb{R}$.*

1.2 Abzählbarkeit und Überabzählbarkeit

Um herauszufinden, ob die oben genannten transzendenten Zahlen existieren, benötigen wir die Begriffe der Abzählbarkeit und Überabzählbarkeit von Mengen.

Definition 1.4. *Eine Menge, deren Elemente man bijektiv allen natürlichen Zahlen zuordnen kann, bezeichnet man als* abzählbare Menge. *Eine unendliche Menge, die nicht abzählbar ist, bezeichnet man als* überabzählbar.

Als Beispiel einer abzählbaren Menge nennen wir die Menge $\mathbb{Z}$ der ganzen Zahlen:

$$\begin{array}{ccccccc} 0 & -1 & 1 & -2 & \ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 1 & 2 & 3 & 4 & \ldots \end{array}$$

Satz 1.5. *Die Menge der algebraischen Zahlen $\overline{\mathbb{Q}}$ ist abzählbar.*

Beweis. Um die Menge der algebraischen Zahlen als abzählbar nachzuweisen, genügt es, die Menge der Polynome mit ganzzahligen Koeffizienten als abzählbar zu erkennen, da jedes Polynom höchstens endlich viele Nullstellen hat. Für einen fixierten Grad $n > 0$ gibt es nun für jeden der Koeffizienten $a_0, \ldots, a_n$ jeweils abzählbar viele Möglichkeiten:

$$
\begin{array}{lccccccc}
n = 1: & & & a_1 x & + & a_0 \\
 & & & \updownarrow & & \updownarrow \\
 & & & \mathbb{Z} & & \mathbb{Z} \\
 & & & & & \\
n = 2: & a_2 x^2 & + & a_1 x & + & a_0 \\
 & \updownarrow & & \updownarrow & & \updownarrow \\
 & \mathbb{Z} & & \mathbb{Z} & & \mathbb{Z} \\
 & & & & & \\
\ldots & \ldots & & & &
\end{array}
$$

Ein Polynom ersten Grades ist definiert durch seine beiden, in diesem Fall ganzzahligen, Koeffizienten. Also finden wir, dass die Menge der Polynome vom Grad 1 mit ganzzahligen Koeffizienten bijektiv zur Vereinigung der Menge der ganzen Zahlen mit sich, also abzählbar ist. Fährt man so weiter, erkennt man, dass auch die Menge der Polynome n-ten Grades mit ganzzahligen Koeffizienten abzählbar ist. Somit ergibt sich die Menge der Polynome mit ganzzahligen Koeffizienten als abzählbar unendliche Vereinigung abzählbarer Menge. Dies zeigt, dass die fragliche Menge abzählbar ist. Damit ist der Satz bewiesen. □

Satz 1.6. *Die Menge der reellen Zahlen $\mathbb{R}$ ist überabzählbar.*

Beweis. Annahme: Die Menge reeller Zahlen im Intervall $[0, 1]$ ist abzählbar. Unter dieser Annahme lassen sich alle Zahlen im Intervall $[0, 1]$ wie folgt dezimal darstellen:

$$
\begin{aligned}
\alpha_1 &= 0, \alpha_{11}\alpha_{12}\alpha_{13}\ldots\alpha_{1n}\ldots \\
\alpha_2 &= 0, \alpha_{21}\alpha_{22}\alpha_{23}\ldots\alpha_{2n}\ldots \\
\alpha_3 &= 0, \alpha_{31}\alpha_{32}\alpha_{33}\ldots\alpha_{3n}\ldots \\
&\vdots \\
\alpha_n &= 0, \alpha_{n1}\alpha_{n2}\alpha_{n3}\ldots\alpha_{nn}\ldots \\
&\vdots
\end{aligned}
$$

hierbei ist α_{jk} die k-te Dezimalziffer der reellen Zahl α_j. Es ist $\alpha_{jk} \in \{0, 1, 2, \ldots, 9\}$; außerdem bestehen die Dezimalziffern nicht aus lauter Neunen oder Nullen. Wir betrachten nun die reelle Zahl

$$\beta = 0, \beta_1\beta_2\beta_3 \ldots \beta_n \ldots,$$

welche folgendermaßen definiert wird: für β_1 wählen wir eine Ziffer verschieden von α_{11}, für β_2 eine Ziffer verschieden von α_{22}, ..., für β_n eine Ziffer verschieden von α_{nn}, usw. Auch hier wird wieder darauf geachtet, dass nicht nur Neunen oder Nullen erzeugt werden, indem man z.B. nur Einsen und Zweien verwendet. Wir haben also tatsächlich eine neue reelle Zahl gefunden, die in unserer Abzählung noch nicht erfasst war. Damit ist es nicht möglich, die reellen Zahlen abzuzählen; somit ist $\mathbb{R}$ überabzählbar. □

Satz 1.7. *Die Menge $\mathbb{T}$ der transzendenten Zahlen ist nicht leer, ja sogar überabzählbar, d.h. es existieren transzendente Zahlen.*

Beweis. Es besteht die disjunkte Vereinigung

$$\mathbb{R} = \overline{\mathbb{Q}} \,\dot\cup\, \mathbb{T}.$$

Wäre nun $\mathbb{T} = \emptyset$, so hätten wir $\mathbb{R} = \overline{\mathbb{Q}}$. Da nun aber $\overline{\mathbb{Q}}$ abzählbar ist, müsste dann auch $\mathbb{R}$ abzählbar sein, was der eben bewiesenen Überabzählbarkeit von $\mathbb{R}$ widerspricht. Somit ist $\mathbb{T} \neq \emptyset$, also existieren transzendente Zahlen.

Da $\overline{\mathbb{Q}}$ abzählbar ist und $\mathbb{R}$ überabzählbar ist, muss auch $\mathbb{T}$ überabzählbar sein. □

2 Spezielle transzendente Zahlen

2.1 Eine LIOUVILLE'sche Zahl

Im Gegensatz zum Beweis, dass eine Zahl algebraisch ist, wobei man lediglich ein passendes Polynom finden muss, ist es ungleich schwieriger zu zeigen, dass eine Zahl transzendent ist. Schließlich muss man dazu zeigen, dass die gewählte Zahl von **keinem** Polynom mit ganzzahligen Koeffizienten Nullstelle ist. Als günstig bei solchen Beweisen erweist sich der Satz von LIOUVILLE.

Satz 2.1. (Satz von LIOUVILLE). *Es sei α eine reelle algebraische Zahl vom Grad $n > 1$. Dann besteht für alle $p \in \mathbb{Z}$ und hinreichend große $q \in \mathbb{N}$ die Ungleichung*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{n+1}}. \tag{2.1}$$

Diese Abschätzung besagt, dass sich algebraische Zahlen „schlecht" durch rationale Zahlen approximieren lassen.

Beweis. Die reelle algebraische Zahl α sei Nullstelle des Polynoms

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Weiter sei (r_m) eine Folge rationaler Zahlen, die gegen α konvergiert. (Solche rationale Zahlenfolgen müssen existieren, da α reell ist.) Wir nehmen für das folgende an, dass $r_m = \frac{p_m}{q_m}$ mit $p_m \in \mathbb{Z}$, $q_m \in \mathbb{N}$, $q_m \neq 0$ $(m \in \mathbb{N})$ gilt.

Da α Nullstelle von f ist, haben wir

$$\begin{aligned} f(r_m) &= f(r_m) - f(\alpha) \\ &= a_n(r_m^n - \alpha^n) + a_{n-1}(r_m^{n-1} - \alpha^{n-1}) + \ldots + a_2(r_m^2 - \alpha^2) + a_1(r_m - \alpha). \end{aligned}$$

Nach Division durch $(r_m - \alpha)$ ergibt sich daraus

$$\begin{aligned} \frac{f(r_m)}{r_m - \alpha} = &a_n(r_m^{n-1} + r_m^{n-2}\alpha + \ldots + r_m\alpha^{n-2} + \alpha^{n-1}) + \ldots \\ &\ldots + a_3(r_m^2 + r_m\alpha + \alpha^2) + a_2(r_m + \alpha) + a_1. \end{aligned}$$

Da $\lim\limits_{m\to\infty} r_m = \alpha$ gilt, gibt es ein $N \in \mathbb{N}$ mit der Eigenschaft $|r_m - \alpha| < 1$ für alle $m \geq N$. Daraus ergibt sich $|r_m| < |\alpha| + 1$. Somit erhalten wir mit der Dreiecksungleichung für hinreichend große m die Abschätzung

$$\begin{aligned} \left|\frac{f(r_m)}{r_m - \alpha}\right| < &n \cdot |a_n| \cdot (|\alpha| + 1)^{n-1} + \ldots + 3 \cdot |a_3| \cdot (|\alpha| + 1)^2 + \\ &+ 2 \cdot |a_2| \cdot (|\alpha| + 1) + |a_1| =: M. \end{aligned}$$

Da M für ein festes α konstant ist und nicht von m abhängt, können wir $r_m = \frac{p_m}{q_m}$ so erweitern, dass $q_m > M$ gilt. Dies führt zu

$$\left|\frac{f(r_m)}{r_m - \alpha}\right| < q_m \Leftrightarrow |\alpha - r_m| > \frac{|f(r_m)|}{q_m}. \tag{2.2}$$

Nun können die rationalen Zahlen r_m nicht Nullstellen des Polynoms f sein, da andernfalls nach Abspalten des Linearfaktors $(x - r_m)$ von f und geschicktem Erweitern ein Polynom von einem niedrigeren Grad mit ganzzahligen Koeffizienten entsteht, dessen eine Nullstelle α ist, was im Widerspruch zur Voraussetzung steht. Mit anderen Worten gilt also

$$|f(r_m)| = \left|\frac{a_n p_m^n + a_{n-1}p_m^{n-1}q_m + \ldots + a_1 p_m q_m^{n-1} + a_0 q_m^n}{q_m^n}\right| \neq 0. \tag{2.3}$$

Da der Zähler in (2.3) ganzzahlig und ungleich Null ist, muss er betragsmäßig mindestens gleich Eins sein. Unter Verwendung der Abschätzungen (2.2) und (2.3) ergibt sich schließlich

$$\left|\alpha - \frac{p_m}{q_m}\right| > \frac{|f(r_m)|}{q_m} \geq \frac{1}{q_m^n} \cdot \frac{1}{q_m} = \frac{1}{q_m^{n+1}}.$$

Damit ist der Satz von LIOUVILLE vollständig bewiesen. □

Bemerkung. Mit Hilfe des Satzes von LIOUVILLE lassen sich transzendente Zahlen finden indem man annimmt, dass eine vorgegebene reelle Zahl α algebraisch vom Grad $n > 0$ ist und zeigt, dass die Ungleichung (2.1) verletzt ist. Als Beispiel betrachten wir eine LIOUVILLE'sche Zahl, nämlich

$$\alpha_L := \sum_{j=1}^{\infty} 10^{-j!} = 0,\ 110\,001\,000\,000\,000\,000\,000\,001\,000\ldots$$

Wir beweisen nun

Satz 2.2. *Die LIOUVILLE'sche Zahl α_L ist transzendent.*

Beweis. Für $m \in \mathbb{N}$ setzen wir

$$p_m := 10^{m!} \cdot \sum_{j=1}^{m} 10^{-j!}, \quad q_m := 10^{m!}, \quad r_m := \frac{p_m}{q_m}.$$

Damit erhalten wir

$$\alpha_L - r_m = \sum_{j=1}^{\infty} 10^{-j!} - \sum_{j=1}^{m} 10^{-j!} = \sum_{j=m+1}^{\infty} 10^{-j!},$$

und es folgt einerseits

$$\begin{aligned} |\alpha_L - r_m| &= \sum_{j=m+1}^{\infty} 10^{-j!} < 10^{-(m+1)!} \cdot \sum_{j=0}^{\infty} 10^{-j} \\ &= 10^{-(m+1)!} \cdot \frac{1}{1-\frac{1}{10}} = 10^{-(m+1)!} \cdot \frac{10}{9} < 10 \cdot 10^{-(m+1)!}. \end{aligned}$$

Wäre nun α_L algebraisch vom Grad n, beliebig, so würde nach dem Satz von LIOUVILLE für hinreichend große m andererseits gelten

$$|\alpha_L - r_m| > \frac{1}{q_m^{n+1}} = \frac{1}{10^{(n+1)m!}}.$$

Zusammengenommen ergeben sich die äquivalenten Ungleichungen

$$\frac{1}{10^{(n+1)m!}} < \frac{1}{10^{(m+1)!-1}} \Longleftrightarrow (n+1)m! > (m+1)! - 1 \Longleftrightarrow n > m - \frac{1}{m!},$$

was auf die Ungleichung $m < n + 1$ führt. Da n beliebig, aber fest ist, und m beliebig groß gewählt werden kann, erhalten wir einen Widerspruch zur Annahme der Algebraizität von α_L, d.h. α_L ist transzendent. □

Wesentlich populärer als die Transzendenz der LIOUVILLE'schen Zahlen ist die Transzendenz der EULER'schen Zahl e, welche wir im nächsten Abschnitt beweisen wollen.

2.2 Transzendenz von e

Satz 2.3. *Die EULER'sche Zahl e ist transzendent.*

Beweis. 1. Schritt (Beweisstrategie): Wir führen den Beweis indirekt. Im Gegensatz zur Behauptung nehmen wir an, dass e algebraisch vom Grad m ist, d.h. es existieren $a_0, \ldots, a_m \in \mathbb{Z}$ mit $a_0 \neq 0$ und $a_m \neq 0$, so dass

$$a_m e^m + a_{m-1} e^{m-1} + \ldots + a_1 e + a_0 = 0 \tag{2.4}$$

gilt. Wir skizzieren in diesem ersten Schritt, wie wir einen Widerspruch zu dieser Annahme herstellen können. Dazu nehmen wir an, dass es ein Polynom $H \in \mathbb{Q}[x]$ gibt, das die e-Funktion an den Stellen aus (2.4) gut approximiert.

Wir definieren:

$$c := \sum_{j=0}^{m} a_j H(j), \tag{2.5}$$

$H(j)$ statt e^j in (2.4) eingesetzt;

$$\varepsilon_j := H(0)e^j - H(j) \quad (j = 0, \ldots, m), \tag{2.6}$$

die Güte der Approximation an der Stelle j;

$$\sigma := \sum_{j=1}^{m} a_j \varepsilon_j, \tag{2.7}$$

die Gesamtgüte der Approximation H.

Dabei soll gelten:

(i) $H(0) \neq 0$,

(ii) $H(j) \in \mathbb{Z} \quad (j = 0, \ldots, m)$,

(iii) $c \neq 0$,

(iv) $|\sigma| < 1$.

Da $H(0) \neq 0$ können wir (2.6) umformen zu

$$e^j = \frac{H(j)}{H(0)} + \frac{\varepsilon_j}{H(0)} \quad (j = 0, \ldots, m);$$

dies verbildlicht nocheinmal gut die Approximation von e^j durch $H(j)/H(0)$ ($j = 0, \ldots, m$). Setzen wir dies in (2.4) ein, so ergibt sich

$$\begin{aligned} 0 = \sum_{j=0}^{m} a_j e^j &= \sum_{j=0}^{m} a_j \left(\frac{H(j)}{H(0)} + \frac{\varepsilon_j}{H(0)} \right) \\ &= \frac{1}{H(0)} \sum_{j=0}^{m} a_j H(j) + \frac{1}{H(0)} \sum_{j=0}^{m} a_j \varepsilon_j \\ &= \frac{c}{H(0)} + \frac{\sigma}{H(0)}. \end{aligned}$$

Nach beidseitiger Multiplikation der letzten Gleichung mit $H(0)$ und Umstellung ergibt sich die Gleichung

$$c = -\sigma, \quad \text{d.h.} \quad |c| = |\sigma|. \tag{2.8}$$

Nun ist aber $c \in \mathbb{Z}$ und $c \neq 0$, d.h. es ist $|c| \geq 1$; auf der anderen Seite gilt $|\sigma| < 1$. Damit kann Gleichung (2.8) nicht bestehen. Dies stellt den gesuchten Widerspruch zur Annahme der Algebraizität von e dar, d.h. die EULER'sche Zahl e muss transzendent sein.

2. Schritt (Definition von H): Wir wählen eine beliebige Primzahl p, die wir im weiteren Verlauf des Beweises präzisieren werden. Weiter definieren wir das Hilfspolynom

$$f(x) := x^{p-1}(x-1)^p(x-2)^p \cdot \ldots \cdot (x-m)^p,$$

welches den Grad $N = p-1+m \cdot p$ hat. Damit bilden wir das weitere Hilfspolynom

$$F(x) := f(x) + f'(x) + \ldots + f^{(N)}(x).$$

Leiten wir dies nocheinmal ab, verschwindet die $(N+1)$-te Ableitung von f also, ergibt sich

$$F'(x) = f'(x) + f''(x) + \ldots + f^{(N)}(x) = F(x) - f(x).$$

Da für die e-Funktion die Beziehung $(e^x)' = e^x$ gilt, sollte unsere Approximation F auf dem interessanten Intervall $[0, m]$ auch eine geringe Differenz zwischen Funktion und Ableitung haben, das heißt f sollte dort „klein“ werden. Zur Abschätzung stellen wir fest, dass

$$|x(x-1) \cdot \ldots \cdot (x-m)| \leq m^{m+1} \quad (x \in [0, m])$$

gilt. Mit $M := m^{m+1}$ ergibt sich somit die Abschätzung

$$\max_{0 \leq x \leq m} |f(x)| \leq M^p.$$

Wir erkennen also, dass das Hilfspolynom f auf dem Intervall $[0,\, m]$ nicht „klein“ ist. Aus diesem Grund betrachten wir anstelle von F das Polynom

$$H(x) := \frac{F(x)}{(p-1)!}.$$

Aufgrund der vorhergehenden Überlegungen besteht die Gleichung

$$H'(x) = H(x) - \frac{f(x)}{(p-1)!};$$

dabei gilt

$$\max_{0\le x\le m} \left| \frac{f(x)}{(p-1)!} \right| \le \frac{M^p}{(p-1)!}.$$

Da nun die Größe $M^p/(p-1)!$ beliebig klein wird, falls die Primzahl p hinreichend groß gewählt wird, erkennen wir, dass das normierte Polynom $H(x)/H(0)$ die Exponentialfunktion e^x auf dem Intervall $[0,\, m]$ gut genug approximiert, wenn p genügend groß gewählt wird.

3. Schritt (H erfüllt Eigenschaft (i)): Wir haben

$$f(x) = \sum_{k=0}^{N} b_k x^k$$

mit $b_0, \ldots, b_N \in \mathbb{Z}$ sowie $b_0, \ldots, b_{p-2} = 0$ und $b_{p-1} = ((-1)^m \cdot m!)^p$. Da nun andererseits für $k = 0, \ldots, N$ die Beziehung $f^{(k)}(0) = b_k \cdot k!$ gilt, finden wir

$$\begin{aligned} F(0) &= f(0) + f'(0) + \ldots + f^{(N-1)}(0) + f^{(N)}(0) \\ &= 0 + \ldots + 0 + ((-1)^m \cdot m!)^p \cdot (p-1)! + b_p \cdot p! + \ldots + b_N \cdot N!\,, \end{aligned}$$

also

$$H(0) = ((-1)^m \cdot m!)^p + b_p \cdot p + \ldots + b_N \cdot \frac{N!}{(p-1)!} \in \mathbb{Z}\,.$$

Wählen wir nun überdies $p > m$, so teilt die Primzahl p den ersten Summanden in obiger Summe nicht, wohl aber alle übrigen. Damit haben wir $H(0) \neq 0$.

4. Schritt (H erfüllt Eigenschaft (ii)): Im vorhergehenden Schritt haben wir insbesondere gezeigt, dass $H(0) \in \mathbb{Z}$ ist; wir haben also noch nachzuweisen, dass die Eigenschaft $H(j) \in \mathbb{Z}$ auch für $j = 1, \ldots, m$ gilt. Dazu schreiben wir

$$f(x) = \sum_{k=0}^{N} c_k (x-j)^k$$

mit $c_0, \ldots, c_N \in \mathbb{Z}$ und beachten, dass $c_0, \ldots, c_{p-1} = 0$ gilt, da in der Definition von $f(x)$ der Faktor $(x-j)$ mit dem Exponenten p auftritt. Aufgrund der für

$k = 0, \ldots, N$ gültigen Beziehung $f^{(k)}(j) = c_k \cdot k!$ berechnen wir

$$\begin{aligned} F(j) &= f(j) + f'(j) + \ldots + f^{(N-1)}(j) + f^{(N)}(j) \\ &= 0 + \ldots + 0 + c_p \cdot p! + \ldots + c_N \cdot N! \,. \end{aligned}$$

Damit ergibt sich für $j = 1, \ldots, m$ wie behauptet

$$H(j) = c_p \cdot p + \ldots + c_N \cdot \frac{N!}{(p-1)!} \in \mathbb{Z},$$

da $N > p-1$ ist. Wir beachten an dieser Stelle, dass die Primzahl p jeweils $H(j)$ $(j = 1, \ldots, m)$ teilt.

5. Schritt (H erfüllt Eigenschaft (iii)): Zunächst stellen wir aufgrund von Eigenschaft (ii) von H fest, dass

$$c = \sum_{j=0}^{m} a_j H(j)$$

ganzzahlig ist. Nun zeigen die Ausführungen zu den Beweisschritten 3 und 4 insbesondere

- $p \nmid H(0)$,
- $p \mid H(j) \quad (j = 1, \ldots, m)$.

Indem wir die Primzahl p gegebenenfalls noch weiter vergrößern, können wir sogar erreichen, dass $p \nmid a_0 H(0)$ gilt. Damit erkennen wir

$$p \nmid (a_0 H(0) + a_1 H(1) + \ldots + a_m H(m)) \Longleftrightarrow p \nmid c.$$

Somit ist c eine ganze Zahl, die nicht durch p teilbar ist, d.h. es gilt $c \neq 0$.

6. Schritt (H erfüllt Eigenschaft (iv)): Für $t \in \mathbb{R}$ besteht die Differentialgleichung

$$\begin{aligned} \frac{d}{dt}\left(F(0) - F(t)e^{-t}\right) &= F(t)e^{-t} - F'(t)e^{-t} \\ &= \left(F(t) - F'(t)\right) e^{-t} \\ &= f(t)e^{-t}. \end{aligned}$$

Nach Anwendung des Hauptsatzes der Differential- und Integralrechnung folgt hieraus für $x \in \mathbb{R}$

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

Nach Division durch $(p-1)!$ ergibt sich an der Stelle $x = j \in \{1, \ldots, m\}$ die Gleichung

$$H(0) - H(j)e^{-j} = \frac{1}{(p-1)!} \int_0^j f(t)e^{-t}\,dt\,.$$

Daraus gewinnen wir die Abschätzung

$$\begin{aligned}\left|H(0) - H(j)e^{-j}\right| &\leq \frac{1}{(p-1)!} \max_{0\leq x\leq m} |f(x)| \int_0^j e^{-t}\,dt \\ &\leq \frac{M^p}{(p-1)!}(1-e^{-j}) \\ &\leq \frac{M^p}{(p-1)!}.\end{aligned}$$

Nach Multiplikation mit e^j finden wir

$$\left|H(0)e^j - H(j)\right| \leq \frac{M^p}{(p-1)!}e^j,$$

also

$$\left|\sum_{j=1}^m a_j\varepsilon_j\right| = \left|\sum_{j=1}^m a_j\left(H(0)e^j - H(j)\right)\right| \leq \frac{M^p}{(p-1)!}\sum_{j=1}^m |a_j|e^j.$$

Da nun die Summe $\sum_{j=1}^m |a_j|e^j$ unabhängig von p ist und die Größe $M^p/(p-1)!$ beliebig klein gemacht werden kann, falls p hinreichend groß gewählt wird, erhalten wir für eine geeignete Wahl der Primzahl p die Abschätzung

$$|\sigma| = \left|\sum_{j=1}^m a_j\varepsilon_j\right| < 1.$$

Damit haben wir schließlich gezeigt, dass das Polynom H auch die Eigenschaft (iv) erfüllt. Somit ist die Existenz des im ersten Schritt postulierten Polynoms H mit den Eigenschaften (i) - (iv) gesichert, womit der dort gegebene Beweis zur Transzendenz von e vollständig wird. □

Beispiel. Anhand einiger Beispiele wollen wir zum Abschluss dieses Kapitels illustrieren, dass sich das im Beweis von Satz 2.3 konstruierte Polynom H sehr gut eignet, um e approximativ zu berechnen. Dazu erinnern wir mit den Bezeichungen von Satz 2.3 daran, dass

$$H(x) = \frac{F(x)}{(p-1)!}$$

gilt und $H(x)/H(0) = F(x)/F(0)$ die Exponentialfunktion e^x auf dem Intervall $[0,\, m]$ „gut“ approximiert. Um die Zahl e selbst approximativ zu erhalten, haben wir dann den Quotienten $F(1)/F(0)$ zu betrachten.

(i) Wir wählen $m = 1$, $p = 3$ und berechnen:

$$\begin{aligned} f(x) &= x^2(x-1)^3, \\ F(x) &= x^5 + 2x^4 + 11x^3 + 32x^2 + 64x + 64, \\ F(0) &= 64,\ F(1) = 174. \end{aligned}$$

Damit erhalten wir

$$\frac{F(1)}{F(0)} = 2,\ 71875,$$

was bereits eine gute Approximation für e darstellt.

(ii) Wir wählen $m = 2$, $p = 5$ und berechnen:

$$\begin{aligned} f(x) &= x^4(x-1)^5(x-2)^5, \\ F(x) &= x^{14} - x^{13} + 87x^{12} + 654x^{11} + \ldots + 29\,141\,344\,128, \\ F(0) &= 29\,141\,344\,128,\ F(1) = 79\,214\,386\,200. \end{aligned}$$

Damit erhalten wir jetzt

$$\frac{F(1)}{F(0)} = 2,\ 718\,281\,828\,458\,561\ldots,$$

was bereits eine Approximation liefert, die bis zur zehnten Nachkommastelle mit e übereinstimmt.

(iii) Für $m = 10$, $p = 19$, berechnen wir die ersten 250 Stellen von e zu:

$F(1) =$

420906890748507029026182096439509299798215521937667860885011769232
032353522691886321308907486213329753198157090736361944906681671395
101366778123779026519746760186889043501028656444923044832427638198
395631853196636139048077335608326831576690811685651555874349110826
758313067698221980479297227106944244125616577422930663331767535191
943131677194116514816608807706206390123771373232848896000000000

$F(0) =$

154842991753770091948200174808926819397648841130421728022277207119
283369343271563100488163885166736855159628368845713254723663081258
630284630066157957241597840085956533824604674642859054318154952386
135537182137438204371859076386530235382636468829174781890527162851
471061173279164730841783625881791600856180971045955566708758727674
171654031394986991246534385152192423883635582566400000000000000

$$\frac{F(1)}{F(0)} =$$

$$2.71828182845904523536028747135266249775724709369995957496696762772407663035354759457138217852516642742746639193200305992181741359662904357290033429526059563073813232862794349076323382988075319525101901157383418793070215408914993488416750924476146066\ldots$$

Bemerkung. Um auf den geometrischen Aspekt zurück zu kommen, ist nun die Transzendenz von π interessant. Der Beweis der diese belegt, verläuft im wesentlich ähnlich zum vorangegangenen Beweis, dass e transzendent ist. Allerdings geht man dabei von allgemeinen algebraischen Zahlen als komplexe Nullstellen von Polynomen mit ganzzahligen Koeffizienten aus und benutzt die Beziehung

$$1 + e^{i\pi} = 0\,.$$

Der Beweis stellt sich dann als ein Spezialfall des LINDEMANN'schen Satzes über Exponentialfunktionen dar und muss im Unterschied zu obigem Beweis im Komplexen geführt werden, wobei mit einem Kurvenintegral unter Verwendung des CAUCHY'schen Integalsatzes gearbeitet wird.

3 Konstruktion mit Zirkel und Lineal

Jede Konstruktion mit Zirkel und Linieal besteht aus einer Aufeinanderfolge von Schritten, deren jeder von einer der folgenden vier Arten ist:

1. Verbinden zweier Punkte durch eine Gerade,
2. Bestimmen des Schnittpunktes zweier Geraden,
3. Schlagen eines Kreises mit gegebenem Radius um einen Punkt,
4. Bestimmen des Schnittpunktes eines Kreises mit einem anderen Kreis oder einer Geraden.

Dabei wird von einer gegebenen Einheitsstrecke ausgegangen.

3.1 Mögliche Konstruktionen von Rechenoperationen

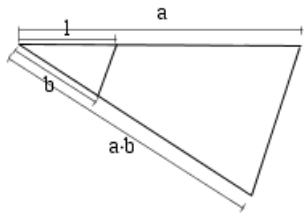
Sind zwei Strecken a und b bereits konstruiert, so können wir $a + b$, $a - b$, $a \cdot b$ und a/b mit Zirkel und Lineal konstruieren.

Bei der *Addition* werden auf einer Geraden nacheinander Kreise mit den Längen a bzw. b abgetragen, so dass die Streckenlänge $a+b$ auf der Geraden abgetragen ist.

Bei der *Subtraktion* wird dementsprechend die zweite Streckenlänge in Richtung des Ausgangspunktes abgetragen.

Für die *Multiplikation* wird als Hilfsmittel der Strahlensatz verwendet. Es werden auf einer Geraden von einem Ausgangspunkt 0 die Strecken 1 und a abgetragen. Auf einer Hilfsgeraden, welche die Gerade im Punkt 0 unter einem positiven Winkel schneidet, wird von 0 aus die Strecke b abgetragen. Es wird eine Gerade durch 1 und b gelegt; die Parallele zu dieser durch a schneidet die Hilfsgerade im Abstand $x = ab$ vom Nullpunkt, denn es gilt

$$\frac{x}{b} = \frac{a}{1} \quad \Leftrightarrow \quad x = ab.$$



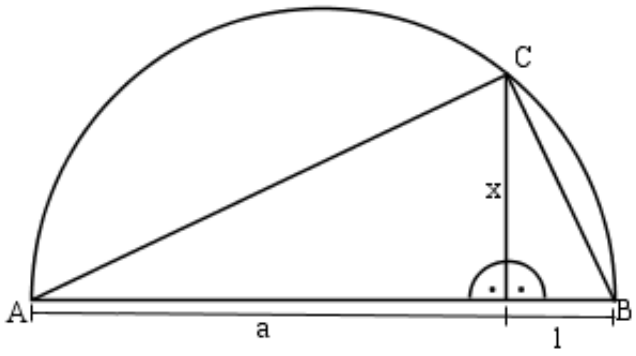
Bei der *Division* wird in ähnlicher Weise verfahren. Auf einer Geraden wird die Strecke a vom Nullpunkt aus abgetragen. Auf der Hilfsgeraden, welche die Gerade im Punkt 0 unter beliebigem Winkel schneidet, werden vom Nullpunkt aus die Strecken 1 und a abgetragen. Es wird eine Gerade durch b und a gelegt; die Parallele zu dieser durch 1 schneidet die ursprüngliche Gerade im Abstand $x = a/b$ vom Nullpunkt, denn es gilt

$$\frac{x}{1} = \frac{a}{b} \quad \Leftrightarrow \quad x = \frac{a}{b}.$$

Neben den vier Grundrechenoperation ist es außerdem möglich, die *Quadratwurzel* von a zu konstruieren. Dazu werden auf einer Geraden nacheinander a und 1 abgetragen, über $a + 1$ wird ein Halbkreis mit Radius $r = \frac{a+1}{2}$ konstruiert. Über dem Punkt a wird lotrecht eine Gerade konstruiert, der Schnittpunkt C dieser Geraden mit dem Halbkreis bildet nach dem Satz des THALES mit 0 und B ein rechtwinkliges Dreieck. Nach dem Höhensatz des EUKLID gilt

$$x^2 = 1 \cdot a \Leftrightarrow x = \sqrt{a},$$

wobei x die Höhe unter C bezeichnet.



3.2 Konstruierbare Zahlen

Ausgehend von einem x,y-Koordinatensystem mit Einheitsstrecke lässt sich nach dem vorhergehenden der Körper $\mathbb{Q}$ der rationalen Zahlen und daher alle rationalen Punkte der x,y-Ebene, d.h. alle Punkte, deren Koordinaten beide rational sind, konstruieren.

3.2.1 Schnittpunkt zweier Geraden

Wir schneiden nun zwei nicht parallele Geraden, welche durch die Gleichungen

$$\begin{aligned} 0 &= ax + by + c && (a, b, c \in \mathbb{Q}), \\ 0 &= dx + ey + f && (d, e, f \in \mathbb{Q}) \end{aligned}$$

beschrieben sind; beachte $ae - bd \neq 0$.

Durch Auflösen der ersten Gleichung nach y (o.B.d.A: $b \neq 0$) und Einsetzen in die zweite ergibt sich

$$\begin{aligned} 0 &= dx + e\left(-\frac{a}{b}x - \frac{c}{b}\right) + f \\ \Leftrightarrow 0 &= x\left(d - \frac{ae}{b}\right) - \left(\frac{ce}{b} - f\right) \\ \Leftrightarrow 0 &= x\left(\frac{bd - ae}{b}\right) - \left(\frac{ce - bf}{b}\right) \\ \Leftrightarrow x &= \frac{ce - bf}{bd - ae} \in \mathbb{Q}\,. \end{aligned}$$

Entsprechend erkennt man, dass auch y rational ist. Das Schneiden zweier Geraden liefert also einen Punkt mit rationalen Koordinaten.

3.2.2 Schnittpunkt von Gerade und Kreis

Wir schneiden nun eine Gerade und einen Kreis, welche durch die Gleichungen

$$\begin{aligned} 0 &= ax + by + c && (a, b, c \in \mathbb{Q}), \\ 0 &= x^2 + y^2 + 2\alpha x + 2\beta y + \gamma && (\alpha, \beta, \gamma \in \mathbb{Q}) \end{aligned}$$

beschrieben sind; o.B.d.A. können wir $b \neq 0$ annehmen.

Indem wir die Geradengleichung nach y umstellen und in die Kreisgleichung eingesetzen, erhalten wir

$$\begin{aligned} & 0 = x^2 + \left(-\frac{a}{b}x - \frac{c}{b}\right)^2 + 2\alpha x + 2\beta\left(-\frac{a}{b}x - \frac{c}{b}\right) + \gamma \\ \Leftrightarrow\ & 0 = x^2 + \frac{a^2}{b^2}x^2 + \frac{2ac}{b^2}x + \frac{c^2}{b^2} + 2\alpha x - \frac{2\beta a}{b}x - \frac{2\beta c}{b} + \gamma \\ \Leftrightarrow\ & 0 = \left(1 + \frac{a^2}{b^2}\right)x^2 + \left(\frac{2ac}{b^2} + 2\alpha - \frac{2\beta a}{b}\right)x + \left(\frac{c^2}{b^2} - \frac{2\beta c}{b} + \gamma\right) \\ \Leftrightarrow\ & 0 = (a^2 + b^2)x^2 + (2ac + 2\alpha b^2 - 2\beta ab)x + (c^2 - 2\beta cb + \gamma b^2). \end{aligned}$$

Um die Gleichung zu vereinfachen, führen wir die neuen Koeffizienten A, B und C ein:

$$A := a^2 + b^2 \ \in \mathbb{Q}_{\neq 0} \quad B := 2ac + 2\alpha b^2 - 2\beta ab \ \in \mathbb{Q} \quad C := c^2 - 2\beta cb + \gamma b^2 \ \in \mathbb{Q}\,.$$

Somit erhält man die quadratische Gleichung:

$$Ax^2 + Bx + C = 0$$

mit den beiden Lösungen

$$x_{1,2} = -\frac{B}{2A} \pm \sqrt{\frac{B^2}{4A^2} - \frac{C}{A}}.$$

Beim Schneiden von einem Kreis mit einer Geraden enstehen also entweder Schnittpunkte mit rationalen Koordinaten oder Koordinaten, die quadratische Irrationalitäten, d.h. Quadratwurzeln rationaler Zahlen, sind.

3.2.3 Schnittpunkt zweier Kreise

Wir schneiden nun zwei Kreise, welche durch die Gleichungen

$$\begin{aligned} 0 &= x^2 + y^2 + 2\alpha x + 2\beta y + \gamma && (\alpha, \beta, \gamma \in \mathbb{Q}), \\ 0 &= x^2 + y^2 + 2\alpha' x + 2\beta' y + \gamma' && (\alpha', \beta', \gamma' \in \mathbb{Q}) \end{aligned}$$

beschrieben sind; o.B.d.A. können wir $\alpha \neq \alpha'$ annehmen.

Durch Differenzbildung der beiden Gleichungen erhält man nach x aufgelöst

$$\begin{aligned} 0 &= 2(\alpha - \alpha')x + 2(\beta - \beta')y + (\gamma - \gamma') \\ \Leftrightarrow x &= \frac{2(\beta' - \beta)y + (\gamma' - \gamma)}{2(\alpha - \alpha')} \\ \Leftrightarrow x &= \frac{\beta' - \beta}{\alpha - \alpha'}y + \frac{\gamma' - \gamma}{2(\alpha - \alpha')}. \end{aligned}$$

Zur Vereinfachung führen wir die Koeffizienten A und B ein:

$$A := \frac{\beta' - \beta}{\alpha - \alpha'} \in \mathbb{Q}, \quad B := \frac{\gamma' - \gamma}{2(\alpha - \alpha')} \in \mathbb{Q}.$$

Damit gilt $x = Ay + B$; nach Einsetzen in die erste Kreisgleichung erhält man

$$\begin{aligned} 0 &= (Ay + B)^2 + y^2 + 2\alpha(Ay + B) + 2\beta y + \gamma \\ \Leftrightarrow 0 &= A^2y^2 + 2ABy + B^2 + y^2 + 2\alpha Ay + 2\alpha B + 2\beta y + \gamma \\ \Leftrightarrow 0 &= (A^2 + 1)y^2 + (2AB + 2\alpha A + 2\beta)y + (B^2 + 2\alpha B + \gamma). \end{aligned}$$

Mit den neuen Koeffizienten

$$M := A^2 + 1 \in \mathbb{Q}, \quad N := 2AB + 2\alpha A + 2\beta \in \mathbb{Q}, \quad P := b^2 - 2\alpha B + \gamma \in \mathbb{Q}$$

ergibt sich folgende quadratische Gleichung:

$$My^2 + Ny + P = 0$$

Mit den beiden Lösungen

$$y_{1,2} = -\frac{N}{2M} \pm \sqrt{\frac{N^2}{4M^2} - \frac{P}{M}}.$$

Beim Schneiden von zweier Kreise enstehen also wiederum entweder Schnittpunkte mit rationalen Koordinaten oder Koordinaten, die quadratische Irrationalitäten, d.h. Quadratwurzeln rationaler Zahlen, sind.

3.2.4 Zusammenfassung

Sowohl beim Schneiden einer Geraden mit einem Kreis als auch beim Schneiden zweier Kreise entstehen entweder Schnittpunkte mit rationalen x,y- Koordinaten oder x,y-Koordinaten, die quadratische Irrationalitäten, d.h. Quadratwurzeln rationaler Zahlen, sind. Zusammengefasst sind die Koordianten also jeweils von der Form

$$a + b\sqrt{k} \quad (a, b, k \in \mathbb{Q}).$$

Wir betrachten somit die Menge $\mathbb{K}_1 := \{a+b\sqrt{k} |\, a, b \in \mathbb{Q}\}$. Wir beachten, das $\mathbb{K}_1$ ein Körper ist, da $\mathbb{K}_1$ bezüglich der vier Grundrechenoperationen abgeschlossen ist (es seinen $a, b, c, d, k \in \mathbb{K}_0 := \mathbb{Q}$):

$$\begin{aligned}
(a + b\sqrt{k}) + (c + d\sqrt{k}) &= (a + c) + (b + d)\sqrt{k},\\
(a + b\sqrt{k}) - (c + d\sqrt{k}) &= (a - c) + (b - d)\sqrt{k},\\
(a + b\sqrt{k})(c + d\sqrt{k}) &= (ac + bdk) + (ad + bc)\sqrt{k},\\
\frac{a + b\sqrt{k}}{c + d\sqrt{k}} &= \frac{a + b\sqrt{k}}{c + d\sqrt{k}} \cdot \frac{c - d\sqrt{k}}{c - d\sqrt{k}}\\
&= \frac{ac - bdk}{c^2 - d^2k} + \frac{bc - ad}{c^2 - d^2k}\sqrt{k}.
\end{aligned}$$

Dieser Prozess kann nun iteriert werden: Ausgehend von den Zahlen aus $\mathbb{K}_1$ können wir für ein festes $k_1 \in \mathbb{K}_1$ die Menge

$$\mathbb{K}_2 = \{a_1 + b_1\sqrt{k_1} \mid a_1, b_1 \in \mathbb{K}_1\}$$

betrachten. Indem wir so fortfahren, erhalten wir nach n Schritten mit einem festen $k_{n-1} \in \mathbb{K}_{n-1}$ den Körper

$$\mathbb{K}_n = \{a_{n-1} + b_{n-1}\sqrt{k_{n-1}} \mid a_{n-1}, b_{n_1} \in \mathbb{K}_{n-1}\}.$$

Insgesamt entsteht der Körperturm

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots \subset \mathbb{K}_n \subset \ldots$$

Zusammenfassend erhalten wir den

Satz 3.1. *Konstruierbare Zahlen sind solche und nur solche, die durch eine derartige Folge von Erweiterungskörpern „erreicht“ werden können, d.h. die zu einem Körper $\mathbb{K}_n$ der oben beschriebenen Art gehören.*

3.3 Algebraizität konstruierbarer Zahlen

Wir wollen zeigen, dass jede konstruierbare Zahl algebraisch ist. Dazu beweisen wir zunächst induktiv das folgende

Lemma 3.2. *Sei $x_k \in \mathbb{K}_k$ eine konstruierbare Zahl. Dann genügt x_k einer Gleichung vom Grade 2^l mit Koeffizienten aus $\mathbb{K}_{k-l}$, wobei $0 < l \leq k$ ist.*

Beweis. Wir führen eine Induktion über $l \in \mathbb{N}$.

Induktionsanfang ($l = 1$): Sei $x_k = a_{k-1} + b_{k-1}\sqrt{k_{k-1}} \in \mathbb{K}_k$ mit $a_{k-1}, b_{k-1}, k_{k-1} \in \mathbb{K}_{k-1}$ gegeben. Wegen

$$\begin{aligned} x_k = a_{k-1} + b_{k-1}\sqrt{k_{k-1}} &\Leftrightarrow x_k - a_{k-1} = b_{k-1}\sqrt{k_{k-1}} \\ &\Leftrightarrow (x_k - a_{k-1})^2 = b_{k-1}^2 k_{k-1} \end{aligned}$$

erkennt man, dass x_k Nullstelle des Polynoms $f(x) = x^2 - b_{k-1}^2 k_{k-1}$ ist. Da $f(x)$ ein Polynom vom Grad 2^1 mit Koeffizienten aus $\mathbb{K}_{k-1}$ ist, ist der Induktionsanfang bewiesen.

Induktionsschritt: Wir nehmen an, dass $x_k \in \mathbb{K}_k$ Nullstelle eines Polynoms

$$f(x) = \alpha_L x^L + \alpha_{L-1} x^{L-1} + \ldots + \alpha_1 x + \alpha_0$$

vom Grad $L := 2^l$ ist mit Koeffizienten aus $\mathbb{K}_{k-l}$ ist, d.h. es ist $\alpha_j \in K_{k-l}$ für alle $j = 0, 1, \ldots, L$. Wir schreiben

$$\alpha_j := a_j + b_j\sqrt{w}$$

mit $a_j, b_j \in \mathbb{K}_{k-l-1}$ und einem festen $w \in \mathbb{K}_{k-l-1}$. Damit gilt

$$f(x) = (a_L x^L + a_{L-1} x^{L-1} + \ldots + a_1 x + a_0) + \sqrt{w} \cdot (b_L x^L + b_{L-1} x^{L-1} + \ldots + b_1 x + b_0).$$

Wir setzen x_k in das Polynom ein und erhalten unter Beachtung von $f(x_k) = 0$ die Gleichheit

$$-(a_L x_k^L + a_{L-1} x_k^{L-1} + \ldots + a_1 x_k + a_0) = \sqrt{w} \cdot (b_L x_k^L + b_{L-1} x_k^{L-1} + \ldots + b_1 x_k + b_0)$$

und nach Quadrieren

$$(a_L x_k^L + a_{L-1} x_k^{L-1} + \ldots + a_1 x_k + a_0)^2 = w \cdot (b_L x_k^L + b_{L-1} x_k^{L-1} + \ldots + b_1 x_k + b_0)^2.$$

Diese Gleichung zeigt, dass x_k Nullstelle eines Polynoms vom Grad $2 \cdot L = 2^{l+1}$ mit Koeffizienten aus $\mathbb{K}_{k-l-1}$ ist. Damit ist der Induktionsschritt bewiesen. □

Mit Hilfe des obigen Lemmas ergibt sich sofort der folgende

Satz 3.3. *Jede konstruierbare Zahl ist algebraisch.*

4 Konstruktionsprobleme

4.1 Die Würfelverdopplung

Wir zeigen nun die Unmöglichkeit der Würfelverdopplung, d.h. ausgehend von einem gegebenen Würfel von Volumen eins die Unmöglichkeit der Konstruktion eines Würfels mit doppeltem Volumen. Zur Konstruktion eines Würfels mit Volumen zwei ist die Konstruktion der $\sqrt[3]{2}$ nötig.
Wir nehmen an, dass $x = \sqrt[3]{2}$ konstruierbar ist und deshalb in einem Körper $\mathbb{K}_k$ liegt. Wir nehmen weiter an, dass K_k minimal ist, d.h. K_k der kleinste Körper in der Inklusionskette von Körpern ist, der x enthält. Wir schreiben

$$x = p + q\sqrt{w} \quad (p, q, w \in \mathbb{K}_{k-1}; \sqrt{w} \notin \mathbb{K}_{k-1}).$$

Da x zum Körper K_k gehört, liegt auch $x^3 - 2$ im Körper K_k und lässt sich folgendermaßen darstellen:

$$x^3 - 2 = a + b\sqrt{w} \quad (a, b \in \mathbb{K}_{k-1}).$$

Durch Einsetzen von x erhält man:

$$\begin{aligned} & a + b\sqrt{w} = (p + q\sqrt{w})^3 - 2 \\ & \Rightarrow a + b\sqrt{w} = (p^3 + 3pq^2w - 2) + \sqrt{w}(3p^2q + q^3w) \\ & \Rightarrow a = p^3 + 3pq^2w - 2 \wedge b = 3p^2q + q^3w. \end{aligned}$$

Da $x^3 - 2 = 0$ gilt, ist auch $a + b\sqrt{w} = 0$. Wir unterscheiden nun zwei Fälle.

1.Fall: $b \neq 0 \Rightarrow \sqrt{w} = -\frac{a}{b} \in \mathbb{K}_{k-1}$.
Dies ist aber ein Widerspruch zur Minimalität von K_k, da aus $\sqrt{w} \in \mathbb{K}_{k-1}$ bereits $x \in \mathbb{K}_{k-1}$ folgt.

2.Fall: $b = 0 \Rightarrow a = 0$.

Ziel ist es jetzt eine weitere Lösung zu konstruieren, die ungleich x ist. Dann hätte man zwei Lösungen für $x^3 - 2$ und damit einen Widerspruch. Wir setzen $y = p - q\sqrt{w} \in \mathbb{K}_k$.
Setzt man y nun in die Formeln für a und b ein, so erhält man

$$y^3 - 2 = a - b\sqrt{w}.$$

Da a und b gleich 0 sind, ergibt sich

$$y^3 - 2 = 0.$$

Damit ist y wirklich Lösung und wir müssen nur noch zeigen, dass $x \neq y$ ist. Um das zu zeigen, betrachten wir die Differenz von x und y. Es gilt

$$x - y = 2q\sqrt{w}.$$

1.Fall: q=0. Man setze q in die Formel für x ein:

$\Rightarrow x = p$

$\Rightarrow x \in K_{k-1}$

$\Rightarrow$ Widerspruch, da x im kleinsten Körper K_k liegen soll.

2.Fall: $q \neq 0$.

$\Rightarrow x - y \neq 0$

$\Rightarrow x \neq y$.

Wir haben also bewiesen, dass $0 = x^3 - 2$ zwei verschiedene reelle Lösungen hat und so einen Widerspruch erzeugt. Die Würfelverdopplung ist mit Zirkel und Lineal nicht möglich.

4.2 Die Quadratur des Kreises

Wir zeigen nun, dass es unmöglich ist, nur mit Zirkel und Lineal aus einem gegebenen Kreis ein Quadrat mit gleichem Flächeninhalt zu konstruieren. Angenommen, der Kreis besitzt (ohne Beschränkung der Allgemeinheit) den Radius $r = 1$. Dann ist der Flächeninhalt des Kreises π. Eine Seite des flächengleichen Quadrates müsste also von der Länge $\sqrt{\pi}$ sein. Da $\sqrt{\pi}$ jedoch wie π nicht algebraisch ist, ist $\sqrt{\pi}$ nicht konstruierbar. Somit ist das Problem der Quadratur des Kreises nicht lösbar.