Nachweis von Nichtkonstruierbarkeit

Dipl. Math. Karsten Kremer, Universität Karlsruhe

Problemstellung

In der antiken Geometrie gab es drei klassische Probleme, die sehr lange ungelöst blieben:

Problem 1 (Quadratur des Kreises)**.** *Zu einem gegebenen Kreis konstruiere man ein flächengleiches Quadrat.*

Problem 2 (Verdopplung eines Würfels)**.** *Zu einem gegebenen Würfel konstruiere man die Seitenlänge des Würfels mit doppeltem Volumen.*

Problem 3 (Drittelung eines Winkels)**.** *Zu einem gegebenen Winkel konstruiere man ein Drittel dieses Winkels.*

Selbstverständlich waren für alle Konstruktionen nur Zirkel und Lineal zugelassen. Erst im 19. Jahrhundert konnte gezeigt werden, dass alle drei Probleme unlösbar sind.

Motivation

Wir können uns die Punkte der Ebene als komplexe Zahlen vorstellen. Wir markieren die Punkte 0 und 1 und nennen $\mathfrak{K} \subseteq \mathbb{C}$ die Menge aller aus 0 und 1 in endlich vielen Schritten konstruierbaren Punkte.

Beispiel: Der Kreis um 1 durch 0 schneidet die Gerade durch 1 und 0 in 2. Also gilt auch $2 \in \mathfrak{K}$. Der Kreis um 2 durch 1 schneidet diese Gerade in 3. Also auch $3 \in \mathfrak{K}$. Induktiv zeigt man damit $\mathbb{N} \subset \mathfrak{K}$.

Man kann sich überlegen, dass zu zwei konstruierbaren Zahlen x und y auch $x+y, -x, x \cdot y$ und x^{-1} konstruierbar sind. Die Menge $\mathfrak{K}$ bildet also einen Teilkörper von $\mathbb{C}$. Außerdem enthält $\mathfrak{K}$ den Körper $\mathbb{Q}$, da $\mathbb{Q}$ der kleinste Teilkörper von $\mathbb{C}$ ist.

Körpererweiterungen

Seien $K \subset L$ zwei Körper. Dann nennen wir L eine *Körpererweiterung* von K. Der Körper L kann auch als Vektorraum über dem Körper K aufgefasst werden. Ist dieser Vektorraum endlichdimensional, so nennen wir die Körpererweiterung endlich. In diesem Fall definieren wir den *Grad* der Körpererweiterung L/K durch $[L : K] := \dim_K(L)$.

Satz 4. *Es seien $K \subset L \subset M$ endliche Körpererweiterungen. Dann gilt*

$$[M : K] = [M : L] \cdot [L : K]$$

Zum Beweis wählt man eine Basis B von L über K und eine Basis C von M über L und zeigt, dass dann $\{bc : b \in B, c \in C\}$ eine Basis von M über K ist. Diese Basis hat dann $|B| \cdot |C|$ Elemente. Den ausführlichen Beweis findet man in [Bosch] 3.2, Satz 2. □

Sei L/K wieder eine Körpererweiterung. Zu einem Element $\alpha \in L$ sei $K(\alpha)$ der kleinste Teilkörper von L, der α enthält. Falls es ein Polynom $f \in K[X]\backslash\{0\}$ gibt mit $f(\alpha) = 0$ so heißt α *algebraisch* über K. Ein solches normiertes Polynom f mit minimalem Grad heißt *Minimalpolynom* von α. In diesem Fall gilt:

Satz 5. *Der Grad des Minimalpolynoms von α ist gleich $[K(\alpha) : K]$.*

Zum Beweis überlegt man sich, dass die Menge $\{\alpha^i : i = 0, \ldots, d-1\}$ mit $d = \dim_K(K(\alpha)) = [K(\alpha) : K]$ eine Basis von $K(\alpha)$ bildet. Fügt man zu dieser Basis noch das Element α^d hinzu, so hat man eine linear abhängige Menge über K, es gibt also eine nichttriviale Linearkombination der 0. Diese entspricht einem Polynom f mit Koeffizienten $c_i \in K$, so dass

$$f(\alpha) = \sum_{i=0}^{d} c_i \alpha^i = 0.$$

Der ausführliche Beweis findet sich in [Bosch] 3.2, Satz 6. □

Konstruierbarkeit

Satz 6. *Ist $\alpha \in \mathfrak{K}$, so gibt es ein $k \in \mathbb{N}$ und einen Körper $L \supset \mathbb{Q}$ der α enthält mit $[L : \mathbb{Q}] = 2^k$.*

Beweis: Zunächst konstruieren wir i, dafür ist eine Körpererweierung vom Grad 2 nötig (das Minimalpolynom von i ist $X^2 + 1$). Sei $\alpha \in \mathfrak{K}$, das heißt α ist in endlich vielen Schritten aus 0 und 1 konstruierbar.

Wir beweisen nun die Behauptung durch Induktion über die Anzahl n der Konstruktionsschritte: Seien die ersten $n-1$ Zwischenschritte sowie ihre komplex konjugierten bereits konstruiert, $L \supset \mathbb{Q}(i)$ ein Körper mit $[L : \mathbb{Q}] = 2^k$ der alle diese Zwischenschritte enthält. Wir zeigen im folgenden $[L(\alpha) : L] \in \{1, 2\}$. Mit der gleichen Argumentation erhalten wir $[L(\overline{\alpha}) : L] \in \{1, 2\}$ Aus Satz 4 folgt dann $[L(\alpha, \overline{\alpha}) : \mathbb{Q}] = [L(\alpha, \overline{\alpha}) : L] \cdot [L : \mathbb{Q}] \in \{2^k, 2^{k+1}, 2^{k+2}\}$.

Beweisen wir also nun $[L(\alpha) : L] \leq 2$. Wir können α mit einem Schritt aus L konstruieren. Die folgenden Konstruktionsschritte sind möglich: zu sechs bereits konstruierten Punkten $z_1, \ldots, z_6$ konstruiere den Schnittpunkt

(i) der Geraden durch z_1 und z_2 mit der Geraden durch z_3 und z_4,

(ii) der Geraden durch z_1 und z_2 mit dem Kreis um z_3 mit Radius $|z_4 - z_5|$,

(iii) des Kreises um z_1 mit Radius $z_2 - z_3$ mit dem Kreis um z_3 mit Radius $|z_4 - z_5|$.

Wir überlegen uns, dass wegen $\overline{z_i} \in L$ auch $\mathrm{Re}(z_i) = \frac{1}{2}(z_i + \overline{z_i})$ und $\mathrm{Im}(z_i) = \frac{1}{2i}(z_i - \overline{z_i})$ in L enthalten sind. Sei $x := \mathrm{Re}(\alpha)$ und $y := \mathrm{Im}(\alpha)$. Jeder der drei Fälle führt nun zu einem Gleichungssystem über L für x und y.

Im Fall (i) erhält man ein lineares Gleichungssystem für x und y, welches in L lösbar ist. Also gilt in diesem Fall $\alpha = x + yi \in L$, also $L(\alpha) = L$.

Im Fall (ii) erhält man eine quadratische Gleichung über L für x. Es gilt $[L(x) : L] \leq 2$, da das Minimalpolynom von x maximal Grad 2 hat. Man

hat dann $y \in L(x)$ durch die Geradengleichung, also $\alpha \in L(x)$ und daher $L(\alpha) = L(x)$.

Der Fall (iii) lässt sich auf Fall (ii) zurückführen, indem man einen der beiden Kreise mit einer passend gewählten Geraden schneidet.

Details findet man in [Bosch] 6.4, Satz 1, (i) $\Rightarrow$ (ii) □

Korollar 7. *Ist $\alpha \in \mathbb{C}$ konstruierbar (also $\alpha \in \mathfrak{K}$), so ist α algebraisch über $\mathfrak{K}$ und der Grad des Minimalpolynoms von α eine Potenz von 2.*

Beweis: Sei L wie in Satz 6, also $\alpha \in L$. Der Körper $\mathbb{Q}(\alpha)$ ist der kleinste Körper, der α enthält, also $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset L$. Da L endlich-dimensionaler $\mathbb{Q}$-Vektorraum ist, gilt dies auch für $\mathbb{Q}(\alpha)$, also ist α algebraisch über $\mathbb{Q}$.

Weiter gilt $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$ nach Satz 4. Also ist $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ ein Teiler von $[L : \mathbb{Q}]$, und somit ebenfalls eine Potenz von 2. Dies ist nach Satz 5 gleich dem Grad des Minimalpolynoms von α □

Lösung der drei Probleme

Zunächst benötigen wir noch einen letzten Hilfssatz:

Hilfssatz 8. *Sind $\alpha \in \mathbb{C}$ und e^α beide algebraisch über $\mathbb{Q}$, so folgt $\alpha = 0$.*

Der Beweis hierfür ist gar nicht so leicht, man findet ihn im Anhang von [Lang] als Korollar 1. Man setzt $K := \mathbb{Q}(\alpha, e^\alpha)$ und nimmt an, dass $[K : \mathbb{Q}]$ endlich ist. Unter dieser Voraussetzung zeigt man, dass es nur endlich viele Stellen in $\mathbb{C}$ gibt, an denen die Werte der Funktionen $f(z) := z$ und $g(z) := e^z$ beide in K liegen.

Wäre nun $\alpha \neq 0$, so wäre $z := m\alpha \in K$ und $e^{m\alpha} \in K$ für alle $m \in \mathbb{Z}$. Dies ist ein Widerspruch dazu, dass es nur endlich viele solcher z gibt. □

Korollar 9. *π ist nicht algebraisch (über $\mathbb{Q}$).*

Beweis: $e^{2\pi i} = 1$ ist algebraisch, daher kann $\alpha := 2\pi i$ wegen Hilfssatz 8 nicht algebraisch sein. Da $2i$ algebraisch ist, kann π nicht algebraisch sein. □

Mit Hilfe von Korollar 7 können wir nun zeigen, dass die anfangs vorgestellten Probleme alle unlösbar sind:

Satz 10 (Quadratur des Kreises)**.** *Zu einem gegebenen Kreis kann man kein flächengleiches Quadrat konstruieren.*

Beweis: Wir nennen den Mittelpunkt des Kreises 0 und einen Punkt auf dem Rand 1. Damit haben wir unseren Kreis in die komplexe Ebene eingebettet. Der Flächeninhalt des zu konstruierenden Quadrats ist π, seine Seitenlänge ist $\sqrt{\pi}$. Falls man dieses Quadrat konstruieren könnte, so wäre also $\sqrt{\pi}$ konstruierbar.

Allerdings ist $\sqrt{\pi}$ nicht algebraisch, da π nach Korollar 9 nicht algebraisch ist. Also ist $\sqrt{\pi}$ nach Korollar 7 nicht konstruierbar. □

Satz 11 (Verdopplung eines Würfels)**.** *Zu einem gegebenen Würfel kann man die Seitenlänge des Würfels mit doppeltem Volumen nicht konstruieren.*

Beweis: Der Würfel habe die Seitenlänge 1. Die Seitenlänge des verdoppelten Würfels ist $\sqrt[3]{2}$. Das Minimalpolynom hierfür ist $f(X) = X^3 - 2$ (man sieht sofort, dass $\sqrt[3]{2} \notin \mathbb{Q}$ die einzige reelle Nullstelle von f ist, daher gibt es keinen Teiler von f in $\mathbb{Q}[X]$). Der Grad von f ist 3, also keine Potenz von 2. Also ist $\sqrt[3]{2}$ nach Korollar 7 nicht konstruierbar. □

Satz 12 (Drittelung eines Winkels)**.** *Es gibt keine Methode um ein Drittel eines beliebigen Winkels zu konstruieren.*

Beweis: Der Winkel $60° = \frac{2\pi}{6}$ ist aus 0 und 1 konstruierbar: $\zeta_6 := e^{2\pi i/6}$ ist der Schnittpunkt der Mittelsenkrechten von 0 und 1 mit dem Einheitskreis. Der Winkel zwischen der Ursprungsgeraden durch ζ_6 und der reellen Achse ist genau 60°. Könnten wir ein Drittel dieses Winkels mit Zirkel und Lineal konstruieren, so könnten wir auch dessen Schnittpunkt $\zeta_{18} := e^{2\pi i/18}$ mit dem Einheitskreis konstruieren. Das Minimalpolynom von ζ_{18} ist $\Phi_{18}(X) = X^6 - X^3 + 1$, dieses hat den Grad $\varphi(18) = 6$. Also ist ζ_{18} nach Korollar 7 nicht konstruierbar. □

Verallgemeinerung

Man kann sich nun allgemeiner fragen, welche Winkel konstruierbar sind, und welche nicht. Man stellt fest, dass dafür nur rationale Teiler des Vollkreises in Frage kommen (da sonst der Schnittpunkt des Winkels mit dem Einheitskreis nicht algebraisch ist).

Für $n \in \mathbb{N}$ sei $\zeta_n := e^{2\pi i/n}$. Der Winkel zwischen der Ursprungsgeraden durch ζ_n und der reellen Achse ist dann genau $\frac{1}{n} \cdot 360°$. Sei Φ_n das Minimalpolynom vom ζ_n (das sogenannte n-te Kreisteilungspolynom). Den Grad dieses Polynoms berechnet die Eulersche φ-Funktion

$$\varphi(n) = \left|\mathbb{Z}/n\mathbb{Z}^\times\right| = \#\left\{a \in \mathbb{N} : 0 \leq a < n \text{ und } \operatorname{ggT}(a,n) = 1\right\}$$

(siehe dazu auch [Bosch] 4.5, Satz 12). Falls $\varphi(n)$ keine Zweierpotenz ist, so ist ζ_n nach Korollar 7 nicht konstruierbar.

Durch Verwendung der Galois-Theorie lassen sich übrigens auch die Umkehrungen von Satz 6 und Korollar 7 zeigen ([Bosch] 6.4, Satz 1). Damit folgt: falls $\varphi(n)$ eine Zweierpotenz ist, dann ist ζ_n konstruierbar. Insbesondere kann man damit beweisen, dass ein regelmäßiges 17-Eck konstruierbar ist, denn $\varphi(17) = 16 = 2^5$. Die Konstruktion selbst ist jedoch sehr kompliziert. Ebenso kann man zeigen, dass ein regelmäßiges 65537-Eck konstruierbar ist ($65537 = 2^{16} + 1$ ist prim, also $\varphi(65537) = 2^{16}$). Diese Konstruktion ist dann aber wirklich nur noch theoretischer Natur...

Literatur

[Bosch] Siegfried Bosch: Algebra, 4. Auflage, Springer (2001)

[Lang] Serge Lang: Algebra, Addison-Wesley (1965)