Konstruktion mit Zirkel und Lineal

Stephan Ehlen

03. Dezember 2018

Konstruktionen mit Zirkel und Lineal

- Gegeben: $E \subset \mathbb{C} \cong \mathbb{R}^2$ Menge an Punkten in der Ebene.
- Identifiziere $\mathbb{R}^2 \cong \mathbb{C}$.
- **Elementare euklidische Figuren**:
  1. Konstruiere eine Gerade durch zwei verschiedene Punkte (Lineal) in E.
  2. Konstruiere einen Kreis, dessen Mittelpunkt in E liegt und der durch einen weiteren Punkt in E verläuft (Zirkel).
- E_1: Menge der Schnittpunkte elementarer euklidischer Figuren (die man aus $E = E_0$ erhält).
- E_2: Menge der Schnittpunkte elementarer euklidischer Figuren (die man aus E_1 erhält).
- $\hat{E} = \bigcup_{j=0}^{\infty} E_j =$ Menge der aus E konstruierbaren Punkte.
- Ein Punkt $p \in \mathbb{C}$ heißt *aus E (elementar) konstruierbar*, wenn er ein Schnittpunkt elementarer euklidischer Figuren ist (den man *induktiv* nach **endlich** vielen Konstruktionsschritten erhält). D.h.: $p \in \hat{E}$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Klassische Konstruktionsprobleme

Aus der Antike sind folgende klassischen Konstruktionsprobleme überliefert.

1. **Winkeldreiteilung**: Gegeben einen Winkel α, unterteile ihn in 3 gleich große Winkel. Übersetzt: Ist für $E = \{0, 1, \cos(\alpha)\}$ auch $\cos(\alpha/3) \in \hat{E}$?
2. **Das Delische Problem der Würfelverdopplung**: Konstruiere zu einem gegebenen Würfel einen Würfel mit doppeltem Volumen. Äquivalent: $E = \{0, 1\}$; Ist $\sqrt[3]{2} \in \hat{E}$?
3. **Quadratur des Kreises**: Gegeben einen Kreis, konstruiere ein Quadrat mit dem gleichen Flächeninhalt. Äquivalent: $\sqrt{\pi} \in \hat{E}$ für $E = \{0, 1\}$.
4. **Konstruktion eines regelmäßigen n-Ecks**. Äquivalent: Ist für $E = \{0, 1\}$ der Punkt $e^{\frac{2\pi i}{n}} \in \hat{E}$?

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Der Körper der konstruierbaren Zahlen

- Notation: Ist $K \subset L$ eine Körpererweiterung und $A \subset L$ eine Teilmenge, so sei $K(A) \subset L$ der kleinste Teilkörper von L mit $K \subset K(A)$ und $A \subset K(A)$.
- Bei $A = a_1, \ldots, a_n$ schreiben wir auch $K(a_1, \ldots, a_n)$ für $K(A)$.
- Ist $E \subset \mathbb{C}$, so ist die Menge $\hat{E}$ aller aus E konstruierbaren Punkte ein Teilkörper von $\mathbb{C}$, der unter der komplexen Konjugation und Wurzelziehen abgeschlossen ist (siehe Übungen).
- Deshalb ist für $K := \mathbb{Q}(E \cup \bar{E})$ auch $\hat{K} = \hat{E}$ (also man kann E stets durch den Körper K ersetzen).
- Es gilt $\overline{K} = \{\overline{x} \mid x \in K\} = K$.
- Zum Beispiel ist für $E = \{0, 1\}$ der Körper $\mathbb{Q}(E \cup \bar{E}) = \mathbb{Q}$ und $\hat{E} = \hat{\mathbb{Q}}$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Konstruktionen

Proposition 1

Sei $K \subset \mathbb{C}$ ein Teilkörper mit $\overline{K} = K$. Sei $\mathbb{G}(K) =$ Menge der Geraden durch Punkte in K und $\mathbb{K}(K) =$ Menge aller Kreise mit Mittelpunkt in K, die durch einen Punkt in K verlaufen. Dann gilt:

1. *Ist $z \in \mathbb{C}$ Schnittpunkt zweier Geraden in $\mathbb{G}(K)$, so ist $z \in K$*
2. *Ist $z \in \mathbb{C}$ Schnittpunkt zweier Kreise in $\mathbb{K}(K)$ oder eines Kreises in $\mathbb{K}(K)$ und einer Geraden in $\mathbb{G}(K)$, so gibt es ein $w \in \mathbb{C}$ mit*

$$w^2 \in K \text{ und } z \in K(w).$$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis

Schnitt von Geraden:

1. Seien $g_1 = \{z_1 + tz_1' \mid t \in \mathbb{R}\}$ sowie $g_2 = \{z_2 + tz_2' \mid t \in \mathbb{R}\}$ mit $z_1, z_1', z_2, z_2' \in K$ und $z_1', z_2' \neq 0$ und z_2' kein reeles Vielfaches von z_1' (sonst sind die Geraden parallel oder gleich).
2. Dann ist $g_1 \cap g_2$ gegeben durch die Gleichung $z_1 + t_1 z_1' = z_2 + t_2 z_2'$. Äquivalent: Ist $z_i = x_i + iy_i$ sowie $z_i' = x_i' + iy_i'$, so erhält man die beiden Gleichungen $x_1 + t_1 x_1' = x_2 + t_2 x_2'$ und $y_1 + t_1 y_1' = y_2 + t_2 y_2'$. Also:

$$\begin{pmatrix} x_1' & -x_2' \\ y_1' & -y_2' \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \end{pmatrix} = \begin{pmatrix} x_2 - x_1 \\ y_2 - y_1 \end{pmatrix}$$

   Die eindeutig bestimmte Lösung (t_1, t_2) liegt in K^2.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Beweis

Schnitt von Gerade und Kreis:

1. Gerade $g = \{z_1 + tz_1' \mid t \in \mathbb{R}\}$, Kreis $k = \{z \in \mathbb{C} \mid (z-w)\overline{(z-w)} = r^2\}$ (Mittelpunkt w, Radius r^2).
2. Da $k \in \mathbb{K}(K)$ ist, gilt $w \in K$. Außerdem gibt es ein $a \in k \cap K$, so dass $r^2 = (a-w)\overline{(a-w)} \in K = \overline{K}$ ist.
3. Sei nun $z \in k \cap g$. Dann gibt es $t \in \mathbb{R}$ mit $z = z_1 + tz_1'$ und es gilt $(z_1 + tz_1' - w)(\overline{z_1} + t\overline{z_1'} - \overline{w}) = r^2$.
4. Teilen durch $|z_1'|^2 = z_1'\overline{z_1'}$ ergibt

$$\underbrace{1 - \frac{|w|^2}{|z_1'|^2} - r^2}_{=:q} + t\underbrace{\left(\frac{z_1}{z_1'} + \frac{\overline{z_1}}{\overline{z_1'}} - \frac{\overline{w}}{\overline{z_1}} - \frac{w}{z_1}\right)}_{=:p} + t^2 = 0,$$

   wobei $p, q \in K$ sind.
5. Setze $w := t + \frac{p}{2}$. Damit ist $w^2 = t^2 + pt + \frac{p^2}{4} = -q + \frac{p^2}{4} \in K$. Und $z = z_1 + tz_1' = z_1 + (w - \frac{p}{2})z_1' \in K(w)$.

Schnitt von Kreis mit Kreis: so ähnlich, Übung.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Adjunktion von Quadratwurzeln

Definition 1

Sei K ein Körper und L/K eine Körpererweiterung.

1. Wir sagen, dass L aus K durch *Adjunktion einer Quadratwurzel* aus K entsteht, falls es ein $w \in L$ mit $w^2 \in K$ gibt, so dass $L = K(w)$.
2. Wir sagen, dass L durch *sukzessive Adjunktion von Quadratwurzeln* aus K entsteht, falls es eine Folge von Zwischenkörpern $K = L_0 \subset L_1 \subset \ldots \subset L_n = L$ gibt, wobei jeweils L_i aus L_{i-1} durch Adjunktion einer Quadratwurzel entsteht.

Beispiel 2

1. $L = \mathbb{Q}(\sqrt{2})$ entsteht aus $\mathbb{Q}$ durch Adjunktion einer Quadratwurzel.
2. $L = \mathbb{Q}(e^{\frac{2\pi i}{3}})$ ensteht aus $\mathbb{Q}$ durch Adjunktion einer Quadratwurzel, denn $e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{1}{2} i\sqrt{3}$, also $L = \mathbb{Q}(\sqrt{-3})$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Adjunktion von Quadratwurzeln

Beispiel 3

$L = \mathbb{Q}(e^{\frac{2\pi i}{5}})$ ensteht aus $\mathbb{Q}$ durch sukzessive Adjunktion von Quadratwurzeln. Die 5. Einheitswurzeln (außer der 1 und damit auch $w = e^{\frac{2\pi i}{5}}$) erfüllen die Gleichung $w^4 + w^3 + w^2 + w + 1 = 0$. Teile durch w^2:

$$(w^2 + w^{-2}) + (w + w^{-1}) + 1 = 0.$$

Mit $(w + w^{-1})^2 = w^2 + 2 + w^{-2}$ erfüllt $z = w + w^{-1}$ die quadratische Gleichung

$$z^2 + z - 1 = 0.$$

Die Lösungen dieser Gleichung sind $z = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$. Sei $K_1 := \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(z)$. Ausgehend hiervon erfüllt w die quadratische Gleichung

$$w^2 - zw + 1 = 0,$$

denn $zw = w^2 + 1$. D.h. $w = \frac{z}{2} \pm \frac{\sqrt{z^2-4}}{2}$. Somit ist $\mathbb{Q} \subset K_1 \subset L = K_1(w) = K_1(w')$, wobei $w'^2 = z^2 - 4 \in K_1$.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät

Ein notwendiges und hinreichendes Kriterium

Proposition 2

Sei $K \subset \mathbb{C}$ ein Teilkörper mit $\overline{K} = K$ und sei $z \in \mathbb{C}$. Die folgenden beiden Aussagen sind äquivalent.

(i) *Der Punkt z ist aus K mit Zirkel und Lineal konstruierbar.*

(ii) *Die Körpererweiterung $K(z)/K$ ensteht aus K durch sukzessive Adjunktion von Quadratwurzeln.*

Beweis.

(i) $\Rightarrow$ (ii): Sei z zunächst in einem einzigen Konstuktionsschritt konstruierbar. Dann ist entweder $z \in K$ oder es existiert nach Proposition 1 ein w, so das $z \in K(w)$ ist und $w^2 \in K$ ist.
Betrachte $K' = K(w, \overline{w}) = K(w)(\overline{w})$. Da $w^2 \in K$, ist $\overline{w}^2 = \overline{w^2} \in \overline{K} = K \subset K(w)$, also geht K' aus K durch sukzessive Adjunktion von Quadratwurzeln hervor und $\overline{K'} = K'$. Die Behauptung folgt per Induktion nach der Anzahl der Konstruktionsschritte. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Ein notwendiges und hinreichendes Kriterium

Proposition 3

Sei $K \subset \mathbb{C}$ ein Teilkörper mit $\overline{K} = K$ und sei $z \in \mathbb{C}$. Die folgenden beiden Aussagen sind äquivalent.

1. *Der Punkt z ist aus K mit Zirkel und Lineal konstruierbar.*
2. *Die Körpererweiterung $K(z)/K$ ensteht aus K durch sukzessive Adjunktion von Quadratwurzeln.*

Beweis.

(ii) $\Rightarrow$ (i): Sei $K = K_0 \subset \dots K_n = K(z)$ eine Kette von Körpererweiterungen, die jeweils durch Adjunktion einer Quadratwurzel entstehen: $K_i = K_{i-1}(w_i)$ mit $w_i^2 \in K_{i-1}$.
Da man mit Zirkel und Lineal Wurzeln ziehen kann, sind alle $w_i \in \hat{K}$ und damit ist auch $K(z) = K_{n-1}(w_n) \subset \hat{K}$. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Ein notwendiges Kriterium

Proposition 4

Sei L/K eine Körpererweiterung, die durch sukzessive Adjunktion von Quadratwurzeln entsteht. Dann ist der Grad $[L : K] = 2^n$ eine Potenz von 2 für ein $n \in \mathbb{N}_0$.
Insbesondere: ist $z \in \mathbb{C}$ aus K durch Zirkel und Lineal konstruierbar, so ist $[K(z) : K] = 2^n$ für ein $n \in \mathbb{N}_0$.

Korollar 1

Jede aus K konstruierbare Zahl ist algebraisch über K.

Beweis.

Dies folgt aus Satz 4.4 im Skript, der besagt, dass endliche Körpererweiterungen algebraisch sind. □

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Quadratur des Kreises

- Problem: Gegeben einen Kreis, konstruiere ein Quadrat mit dem gleichen Flächeninhalt.
- Äquivalent: $\sqrt{\pi} \in \hat{\mathbb{Q}}$?
- Da π transzendent über $\mathbb{Q}$ ist (von Lindemann, 1882), ist auch $\sqrt{\pi}$ transzendent über $\mathbb{Q}$.
- Somit ist $\sqrt{\pi}$ nicht konstruierbar.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Das Problem der Würfelverdopplung

- Problem: Konstruiere zu einem gegebenen Würfel einen Würfel mit doppeltem Volumen.
- Äquivalent: Ist $\sqrt[3]{2} \in \hat{\mathbb{Q}}$?
- Antwort: **Nein!**.
- Denn: der Grad $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ ist keine Potenz von 2.
- Beweis: Das Polynon $X^3 - 2$ is irreduzibel nach Eisenstein-Kriterium für $p = 2$.
- Damit ist es das Minimalpolynom von $\sqrt[3]{2}$ und $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Winkeldreiteilung

- Problem: Gegeben einen Winkel α, unterteile ihn in 3 gleich große Winkel.
- Übersetzt: Ist für $K = \mathbb{Q}(e^{i\alpha})$ der Punkt $e^{i\alpha/3} \in \hat{K}$?
- Antwort: Es kommt auf α an.
- Zum Beispiel: $\alpha = \frac{\pi}{3}$. Frage: Ist $z = e^{i\pi/9} \in \hat{K}$ für $K = \mathbb{Q}(e^{i\pi/3})$.
- Der Punkt z ist Nullstelle des Polynoms $X^9 - 1$.
- Dieses faktorisiert in $\mathbb{Z}[X]$ als $\left(X^6 + X^3 + 1\right)\left(X^2 + X + 1\right)(X - 1)$.
- $e^{\pm i\pi/3}$ ist schon Nullstelle von $X^2 + X + 1$. Es ist also $[K : \mathbb{Q}] = 2$
- Der andere Faktor $f(X) = X^6 + X^3 + 1$ ist irreduzibel nach Eisenstein ($p = 3$) angewandt auf
  $f(X+1) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$.
- Damit ist der Grad $[K(z) : \mathbb{Q}] = 6$.
- Und somit $[K(z) : K] = 3$ nach Gradsatz.
- In diesem Falle ist die Winkeldreiteilung also nicht möglich.

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln

Konstruktion eines regelmäßigen n-Ecks

- Äquivalent: Ist der Punkt $e^{\frac{2\pi i}{n}} \in \hat{\mathbb{Q}}$?
- Antwort: Das kommt auf n an.
- Beispiel: $n = 5$. Wir haben eben gesehen, dass die Konstruktion möglich ist, denn $\mathbb{Q}(e^{\frac{2\pi i}{5}})$ ensteht aus $\mathbb{Q}$ durch sukzessive Adjunktion von Quadratwurzeln.
- Allgemeiner: Ist p eine Primzahl, so ist der Grad $[\mathbb{Q}(e^{\frac{2\pi i}{p}}) : \mathbb{Q}] = p - 1$ (das Minimalpolynom ist $X^{p-1} + X^{p-2} + \ldots + X + 1$).
- Also: ist $p - 1$ keine Potenz von 2, so ist das regelmässige n-Eck nicht konstruierbar.
- Beispiel: Für $n = 7$ ist dies nicht möglich.
- Später (Galoistheorie): Dies ist auch ein hinreichendes Kriterium!

Stephan Ehlen
Mathematisches Institut
Mathematisch-Naturwissenschaftliche Fakultät
Universität zu Köln