Die Konstruierbarkeit des regelmäßigen Fünfecks

Lukas-Fabian Moser, SS 2013

Satz (Hauptsatz über Konstruierbarkeit)**.** *Eine komplexe Zahl $a \in \mathbb{C}$ ist genau dann mit Zirkel und Lineal konstruierbar (ausgehend von der Punktmenge $\{0, 1\}$), wenn es eine Körperkette*

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

gibt mit $a \in K_n$ und $[K_i : K_{i-1}] \leqslant 2$ für alle i.

Das regelmäßige Fünfeck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die Zahl $\zeta := \zeta_5 := e^{2\pi i/5}$ konstruierbar ist. *Daß* beides der Fall ist, ist im Prinzip seit der Antike bekannt (eine Konstruktionsvorschrift für das regelmäßige Fünfeck findet sich schon in Euklids Elementen). Wir wollen aber die prinzipielle Möglichkeit einer Konstruktion *algebraisch* nachweisen.

Lemma. *Es gilt $\zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} = -1$.*

Beweis. Als fünfte Einheitswurzel ist ζ eine Nullstelle des Polynoms

$$X^5 - 1 = (X - 1) \cdot (X^4 + X^3 + X^2 + X^1 + 1),$$

und da $\zeta \neq 1$ ist, muß ζ deswegen eine Nullstelle des zweiten Faktors

$$X^4 + X^3 + X^2 + X^1 + 1$$

sein. (Man bezeichnet dieses Polynom auch als Φ_5 und nennt es das *Fünfte Kreisteilungspolynom*; die Beziehung $\Phi_n = X^{n-1} + X^{n-2} + \cdots + X + 1$ gilt stets, wenn n eine Primzahl ist.) Also ist $\zeta^4 + \zeta^3 + \zeta^2 + \zeta = -1$, und wegen $\zeta^5 = 1$, also $\zeta^{-n} = \zeta^{5-n}$, folgt daraus die Behauptung. □

Satz. *Die Zahl $\zeta = \zeta_5$ (und mit ihr das regelmäßige Fünfeck) ist mit Zirkel und Lineal konstruierbar.*

Beweis. Wir schreiben $\alpha := \zeta + \zeta^{-1}$ und zeigen, daß in der Körperkette

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta)$$

beide Erweiterungen den Grad $\leqslant 2$ haben (in Wirklichkeit ist der Grad sogar jeweils genau 2).

i) Zur Berechnung von $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)]$ bemerken wir, daß $\zeta \cdot \alpha = \zeta^2 + 1$ ist; also ist ζ eine Nullstelle des Polynoms $X^2 - \alpha X + 1 \in \mathbb{Q}(\alpha)[X]$, so daß $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] \leqslant 2$ folgt.

ii) Zur Berechnung von $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ betrachten wir das Polynom F vom Grad 2, dessen Nullstellen α und $\beta := \zeta^2 + \zeta^{-2}$ sind; es gilt also

$$F = (X - \alpha) \cdot (X - \beta) = X^2 - (\alpha + \beta)X + \alpha \cdot \beta.$$

Unser obiges Lemma besagt $\alpha + \beta = -1$, und eine direkte Rechnung ergibt

$$\alpha \cdot \beta = (\zeta + \zeta^{-1}) \cdot (\zeta^2 + \zeta^{-2}) = \zeta^3 + \zeta + \zeta^{-1} + \zeta^{-3} = \alpha + \beta = -1.$$

Damit $F = X^2 + X - 1$, insbesondere liegt F in $\mathbb{Q}[X]$, und wegen $F(\alpha) = 0$ folgt daraus $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leqslant 2$. □

Die Wahl der Körperkette und des Polynoms F fallen hier ein wenig unmotiviert vom Himmel, und die Berechnung von $\alpha \cdot \beta = -1$ gleicht beinahe einem Wunder. All dies findet seine systematische Erklärung erst mit Hilfe der Galoistheorie (durch Untersuchung der Galoisschen Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\zeta)$); der siebzehnjährige Carl Friedrich Gauß erkannte jedoch ohne sie, nur „durch angestrengtes Nachdenken", das Bildungsgesetz dieser und ähnlicher Körpertürme und konnte damit beweisen:

Satz (Gauß)**.** *Für die Zahl $\zeta := \zeta_{17} := e^{2\pi i/17}$ ist*

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta) \subset \mathbb{Q}(\gamma) \subset \mathbb{Q}(\zeta)$$

mit

$$\begin{aligned}
\alpha &:= \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \zeta^4 + \zeta^{-4} + \zeta^8 + \zeta^{-8} \\
\beta &:= \zeta + \zeta^{-1} + \zeta^4 + \zeta^{-4} \\
\gamma &:= \zeta + \zeta^{-1}
\end{aligned}$$

eine Körperkette, deren Erweiterungen alle den Grad $\leqslant 2$ haben. Insbesondere ist das regelmäßige Siebzehneck mit Zirkel und Lineal konstruierbar.

Eine genaue Erklärung der Wahl von α, β, γ würde hier zu weit führen. Wir beschränken uns auf den sachdienlichen Hinweis, daß

$$\left\{\pm\overline{1}, \pm\overline{2}, \pm\overline{4}, \pm\overline{8}\right\}, \left\{\pm\overline{1}, \pm\overline{4}\right\}, \left\{\pm\overline{1}\right\}$$

jeweils Untergruppen der Einheitengruppe des Körpers $\mathbb{Z}/17\mathbb{Z}$ sind – *de facto* die einzigen nichttrivialen Untergruppen dieser zyklischen Gruppe der Ordnung 16.