Universität Konstanz
Fachbereich Mathematik und Statistik
Markus Schweighofer

§5.5 Konstruktionen mit Zirkel und Lineal

Satz 5.5.1. *Sei K ein vollkommener Körper und $a \in \overline{K}$. Dann sind äquivalent:*

(a) *Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \dots, F_n$ von $\overline{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \dots, n\}$.*

(b) *Es gibt einen Zwischenkörper L von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist.*

(c) *Für den Zerfällungskörper L des Minimalpolynoms von a über K ist $[L : K]$ eine Zweierpotenz.*

Beweis. (a) $\Longrightarrow$ (c) Gelte (a). Dann gibt es $n \in \mathbb{N}_0$ und $a_1, \dots, a_n \in \overline{K}$ mit $a_n = a$ und

$$[K(a_1, \dots, a_k) : K(a_1, \dots, a_{k-1})] \leq 2$$

für alle $k \in \{1, \dots, n\}$. Wähle $\varphi_1, \dots, \varphi_m \in \mathrm{Aut}(\overline{K}|K)$ derart, dass $\varphi_1(a), \dots, \varphi_m(a)$ die verschiedenen K-Konjugierten von a sind, wobei $\varphi_1 = \mathrm{id}_{\overline{K}}$ sei. Dann ist nach 4.3.11 $L := K(\varphi_1(a), \dots, \varphi_m(a))$ der Zerfällungskörper von $\mathrm{irr}_K(a)$ über K. Nach der Gradformel reicht es zu zeigen, dass

$$[K(a_1, \dots, a_n, \varphi_2(a_1), \dots, \varphi_2(a_n), \quad . \quad . \quad . \quad , \varphi_m(a_1), \dots, \varphi_m(a_n)) : K]$$

eine Zweierpotenz ist, was mit der Gradformel durch sukzessives Adjungieren folgt.

(c) $\Longrightarrow$ (b) trivial

(b) $\Longrightarrow$ (a) Sei L ein Zwischenkörper von $\overline{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist. Nach Galois 5.2.2 gilt für die Galoisgruppe $G := \mathrm{Aut}(L|K)$, dass $\#G = [L : K]$ eine Zweierpotenz ist. Also ist G eine 2-Gruppe und nach 3.3.10 daher auflösbar. Nach 3.3.12 und dem Satz von Lagrange 1.3.19 gibt es $n \in \mathbb{N}_0$ und Untergruppen $H_0, \dots, H_n$ von G mit $G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = \{1\}$ und $[H_{k-1} : H_k] = 2$ für alle $k \in \{1, \dots, n\}$. Setzt man $F_k := L^{H_k}$ für $k \in \{0, \dots, n\}$, so folgt mit Galois 5.2.2 $K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \dots, n\}$. □

Notation 5.5.2. Sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$. Mit $\bigstar M$ bezeichnen wir den in Aufgabe 43 auf Blatt 12 eingeführten Körper aller aus M mit *Zirkel und Lineal konstruierbaren* Punkte. Weiter sei $M^* := \{a^* \mid a \in M\}$.

Satz 5.5.3. *Sei $\{0, 1\} \subseteq M \subseteq \mathbb{C}$ und $a \in \mathbb{C}$. Dann sind äquivalent:*

(a) $a \in \bigstar M$

(b) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper $F_0, \ldots, F_n$ von $\mathbb{C}|\mathbb{Q}(M \cup M^*)$ mit $\mathbb{Q}(M \cup M^*) = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \ldots, n\}$.

Beweis. Aufgabe 49(b) auf Blatt 14. □

Satz 5.5.4. *Für $a \in \mathbb{C}$ sind äquivalent:*

(a) *a ist aus $\{0, 1\}$ mit Zirkel und Lineal konstruierbar.*

(b) *Für den Zerfällungskörper L des Minimalpolynoms von a über $\mathbb{Q}$ ist $[L : \mathbb{Q}]$ eine Zweierpotenz.*

Beweis. 5.5.1 und 5.5.3 □

Definition 5.5.5. Zahlen der Form $2^{2^n} + 1$ ($n \in \mathbb{N}_0$) nennt man *Fermatzahlen*. Fermatzahlen, die Primzahlen sind, nennt man *Fermatsche Primzahlen* [Pierre de Fermat *1607 †1665].

Bemerkung 5.5.6. Die einzigen bekannten Fermatschen Primzahlen sind 3, 5, 17, 257 und 65537. Man weiß nicht, ob es noch andere oder sogar unendlich viele gibt, obwohl Fermat noch glaubte, jede Fermatzahl sei prim.

Lemma 5.5.7. *Jede Primzahl der Form $2^n + 1$ ($n \in \mathbb{N}$) ist eine Fermatsche Primzahl.*

Beweis. Sei $n \in \mathbb{N}$ und $2^n + 1 \in \mathbb{P}$. Um zu zeigen, dass n eine Zweierpotenz ist, seien $r, s \in \mathbb{N}$ mit $n = rs$ und s ungerade. Zu zeigen: $s = 1$. Dann $2^n + 1 = 2^{rs} + 1 \equiv_{(2^r+1)} (-1)^s + 1 = 0$ und $(2^r + 1) \mid (2^n + 1)$ in $\mathbb{Z}$. Wegen $2^n + 1 \in \mathbb{P}$ folgt $r = n$, also $s = 1$. □

Satz 5.5.8. [Pierre Laurent Wantzel *1814 † 1848] *Sei $n \in \mathbb{N}$. Dann sind äquivalent:*

(a) *$e^{\frac{2\pi i}{n}}$ ist aus $\{0, 1\}$ mit Zirkel und Lineal konstruierbar, das heißt „das regelmäßige n-Eck ist mit Zirkel und Linear konstruierbar".*

(b) *Es gibt $k, m \in \mathbb{N}_0$ und verschiedene Fermatsche Primzahlen $p_1, \ldots, p_m$ mit $n = 2^k p_1 \cdots p_m$.*

Beweis. Nach 5.4.12(a) gilt $\mathrm{irr}_{\mathbb{Q}}(e^{\frac{2\pi i}{n}}) = \Phi_n$. Der Zerfällungskörper von Φ_n über $\mathbb{Q}$ hat nach 5.4.12(b) den Grad $\varphi(n)$ über $\mathbb{Q}$, womit gemäß 5.5.4 die Bedingung (a) dazu äquivalent ist, dass $\varphi(n)$ eine Zweierpotenz ist. Nach 5.4.3(a)(b) ist dies dazu äquivalent, dass n ein Produkt von einer Zweierpotenz und von paarweise verschiedenen ungeraden Primzahlen ist, die jeweils eine Zweipotenz ergeben, wenn man sie um eins vermindert. Nach Lemma 5.5.7 ist dies zu (b) äquivalent. □

Bemerkung 5.5.9. Johann Gustav Hermes [*1846 †1912] hat über zehn Jahre seines Lebens mit der expliziten Konstruktion des regelmäßigen 65537-Ecks verbracht.