

§5.4 Konstruktionen mit Zirkel und Lineal

Notation 5.4.1. Ist K ein Körper und $a \in K$, so bezeichne \sqrt{a} stets eines der höchstens zwei Elemente $b \in \bar{K}$ mit $b^2 = a$ (ist $a \in \mathbb{R}_{\geq 0}$, so sei wie üblich $\sqrt{a} \geq 0$). Man beachte, dass \sqrt{a} bis auf das Vorzeichen eindeutig bestimmt ist. Insbesondere ist $K(\sqrt{a})$ der Zerfällungskörper von $X^2 - a$ über K .

Proposition 5.4.2. Sei $L|K$ eine Körpererweiterung mit $\text{char } K \neq 2$. Dann

$$[L : K] \leq 2 \iff \exists a \in K : L = K(\sqrt{a}).$$

Beweis. Aufgabe 3(a) auf Blatt 12. □

Proposition 5.4.3. Sei K ein vollkommener Körper und $a \in \bar{K}$. Dann sind äquivalent:

- (a) Es gibt $n \in \mathbb{N}_0$ und Zwischenkörper F_0, \dots, F_n von $\bar{K}|K$ mit $K = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n$, $a \in F_n$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \dots, n\}$.
- (b) Es gibt einen Zwischenkörper L von $\bar{K}|K$ 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) \implies (c) Gelte (a). Dann gibt es $n \in \mathbb{N}_0$ und $a_1, \dots, a_n \in \bar{K}$ 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 $\varphi_1, \dots, \varphi_m \in \text{Aut}(\bar{K}|K)$ derart, dass $\varphi_1(a), \dots, \varphi_m(a)$ die verschiedenen K -Konjugierten von a sind, wobei $\varphi_1 = \text{id}_{\bar{K}}$ sei. Dann ist nach 4.3.11 $L := K(\varphi_1(a), \dots, \varphi_m(a))$ der Zerfällungskörper von $\text{irr}_K(a)$ über K . Nach der Gradformel reicht es zu zeigen, dass

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

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

(c) \implies (b) trivial

(b) \implies (a) Sei L ein Zwischenkörper von $\bar{K}|K$ mit $L|K$ galoissch und $a \in L$ derart, dass $[L : K]$ eine Zweierpotenz ist. Nach Galois 5.2.2 gilt für die Galoisgruppe $G := \text{Aut}(L|K)$, 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 $G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_n = \{1\}$ 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 $K = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = L$ und $[F_k : F_{k-1}] = 2$ für $k \in \{1, \dots, n\}$. □

Notation 5.4.4. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$. Mit $\star M$ bezeichnen wir den in Aufgabe 3 auf Blatt 11 eingeführten Körper aller aus M mit Zirkel und Lineal konstruierbaren Punkte. Weiter sei $M^* := \{a^* \mid a \in M\}$.

Satz 5.4.5. Sei $\{0,1\} \subseteq M \subseteq \mathbb{C}$ und $a \in \mathbb{C}$. Dann sind äquivalent:

(a) $a \in \star M$

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

Beweis. Aufgabe 3(b) auf Blatt 12. □

Bemerkung 5.4.6. Mit Hilfe von 5.4.3 und 5.4.5 werden wir in der Zahlentheorie zeigen, dass die regelmässigen p -Ecke mit $p \in \{3, 5, 17, 257, 65537\}$ mit Zirkel und Lineal konstruierbar sind. Man vermutet, dass dies die einzigen konstruierbaren regelmäßigen p -Ecke mit $p \in \mathbb{P}$ sind. Johann Gustav Hermes [*1846 †1912] hat zehn Jahre seines Lebens nur mit der expliziten Konstruktion des regelmäßigen 65537-Ecks verbracht.