§ 16 Die Konstruierbarkeit des regelmäßigen n–Ecks

In §8. hatten wir uns mit dem Problem der Konstruierbarkeit mit Zirkel und Lineal beschäftigt und dabei eine Lösung für die 3 klassischen Probleme (Verdoppelung des Würfels, Quadratur des Kreises und Dreiteilung eines Winkels) angegeben. Wir greifen jetzt dieses Thema noch einmal auf und wollen insbesondere die Frage stellen, für welche $n \in \mathbb{N}$ das regelmäßige n–Eck mit Zirkel und Lineal konstruierbar ist. Gewisse Teilantworten kennen wir schon (in Aufgabe 1 wird das regelmäßige 5–Eck konstruiert, und die Konstruktion des regelmäßigen 6–Ecks ist auch bekannt). Die Eckpunkte eines regelmäßigen n–Ecks, das dem Einheitskreis einbeschrieben ist, sind in der komplexen Zahlenebene gerade die n–ten Einheitswurzeln. Für $n \in \mathbb{N}$ setzen wir

$$\varepsilon_n \;=\; e^{\frac{2\pi i}{n}} .$$

Dann ist das regelmäßige n–Eck genau dann mit Zirkel und Lineal konstruierbar, wenn

$$\varepsilon_n \in \mathcal{K}(M)$$

gilt, wobei wir im folgenden $M = \{0, 1\}$ voraussetzen.

Wir behandeln zunächst den Fall, daß n eine Primzahl ist.

(16.1) LEMMA: Sei $p \in \mathbb{P}$ und $\varepsilon_p \;=\; e^{\frac{2\pi i}{p}}$. Dann gilt:

a) $\mathrm{grad}_{\mathbb{Q}}(\varepsilon_p) \;=\; p - 1$

b) $\mathbb{Q}(\varepsilon_p) : \mathbb{Q}$ ist eine Galois–Erweiterung mit abelscher (und sogar zyklischer) Galois–Gruppe.

Wir können jetzt beweisen, daß unter bestimmten Voraussetzung auch die Umkehrung in (8.6) gilt.

(16.2) SATZ: Sei $M = \{0, 1\}$. Für die komplexe Zahl $\alpha \in \mathbb{C}$ sei die Körpererweiterung $\mathbb{Q}(\alpha) : \mathbb{Q}$ eine Galois–Erweiterung, deren Galois–Gruppe abelsch ist. Dann sind folgende Aussagen äquivalent:

a) $\alpha \in \mathcal{K}(M)$

b) $\mathrm{grad}_{\mathbb{Q}}(\alpha)$ ist eine Zweier–Potenz .

(16.3) SATZ: Für eine Primzahl $p \geq 3$ sind folgende Aussagen äquivalent:

a) Das regelmäßige p–Eck ist mit Zirkel und Lineal konstruierbar

b) $p - 1$ ist eine Zweierpotenz

c) p ist eine Fermat'sche Primzahl .

(16.4) BEM: Zahlen der Form $F_n = 2^{2^n} + 1$ $(n \in \mathbb{N}_0)$ heißen **Fermat'sche Zahlen**, die Primzahlen unter diesen **Fermat'sche Primzahlen**. Für $n = 0, 1, 2, 3, 4$ ist F_n eine Primzahl. Fermat (1601–1665) vermutete, daß alle F_n Primzahlen sind. Dann zeigte jedoch Euler (1707–1783), daß F_5 keine Primzahl ist $(641|F_n)$. Weitere Fermat'sche Primzahlen sind bisher nicht gefunden worden. Auch ist nicht bekannt, ob es überhaupt unendlich viele Fermat'sche Primzahlen gibt.

n	$F_n = 2^{2^n} + 1$	prim
0	3	ja
1	5	ja
2	17	ja
3	257	ja
4	65 537	ja
5	4 294 967 297	$= 641 \times 6\,700\,417$

Für die 5 bekannten Fermat'schen Primzahlen ist die Konstruktion des regelmäßigen p–Ecks durchgeführt worden:

3–Eck,5–Eck	bereits im Altertum bekannt
17–Eck	Gauß (1796)
257–Eck	Richelot (1832)
65 537–Eck	Hermes (1879–1889)

(16.5) BEM: a) Ist das regelmäßige n–Eck konstruierbar, so ist auch das regelmäßige $(2^k n)$–Eck für jedes $k \in \mathbb{N}$ konstruierbar .

b) Sind das regelmäßige m–Eck und das regelmäßige n–Eck konstruierbar und gilt $\mathrm{ggT}(m, n) = 1$, so ist auch das regelmäßige (mn)–Eck konstruierbar.

c) Mit (16.3) ergibt sich unter Verwendung von a) und b) das folgende Ergebnis: Ist n von der Form $n = 2^k \cdot p_1 \cdot \ldots \cdot p_r$ $(k \geq 0, r \geq 0)$, wobei $p_1, \ldots, p_r$ paarweise verschiedene Fermat'sche Primzahlen sind, so ist das das regelmäßige n–Eck konstruierbar. Im folgenden werden wir sehen, daß auch die Umkehrung gilt.

Sei jetzt $n \in \mathbb{N}$ beliebig. Wir wollen $\boxed{\mathrm{grad}_{\mathbb{Q}}(\varepsilon_n)}$ bestimmen.

Es bezeichne $E_n \subseteq \mathbb{C}$ die Menge der n–ten Einheitswurzeln, d.h. der Nullstellen des Polynoms $T^n - 1 \in \mathbb{Q}[T]$. E_n ist eine Untergruppe von $(\mathbb{C}^\star, \cdot)$ der Ordnung n . $(E_n, \cdot)$ ist eine zyklische Gruppe, was auch aus (4.18) folgt. Ein erzeugendes Element ε von E_n heißt eine **primitive** n**–te Einheitswurzel**. Es gilt dann

$$E_n \;=\; <\varepsilon> \;=\; \{\varepsilon^0, \varepsilon^1, \varepsilon^2, \ldots, \varepsilon^{n-1}\}$$

Z.B. ist $\varepsilon_n = e^{\frac{2\pi i}{n}}$ eine primitive n–te Einheitswurzel. Es gilt

$$\mathrm{ord}(\varepsilon^k) \;=\; n \quad \Longleftrightarrow \quad \mathrm{ggT}(k, n) = 1\,.$$

Bezeichnet E'_n die Menge der primitiven n–ten Einheitswurzeln, so gilt damit

$$|E'_n| \;=\; \varphi(n)\,.$$

$\mathbb{Q}_n \subseteq \mathbb{C}$ bezeichne den Zerfällungskörper des Polynoms $T^n - 1$ über $\mathbb{Q}$. $\mathbb{Q}_n$ heißt der n**–te Kreisteilungskörper**. Es gilt $\mathrm{Null}_{\mathbb{C}}(T^n - 1) = E_n$ und

$$\mathbb{Q}_n \;=\; \mathbb{Q}(E_n) \;=\; \mathbb{Q}(\varepsilon) \quad \forall\, \varepsilon \in E_n'\,.$$

$\mathbb{Q}_n : \mathbb{Q}$ ist eine Galois–Erweiterung als Zerfällungskörper eines separablen Polynoms, und es gilt

$$[\mathbb{Q}_n : \mathbb{Q}] \;=\; \mathrm{grad}_{\mathbb{Q}}(\varepsilon) \quad (\varepsilon \in E_n')\,.$$

Wir müssen jetzt versuchen, das Minimalpolynom von $\varepsilon \in E_n'$ zu bestimmen.

(16.6) BEM: Seien $m, n \in \mathbb{N}$. Dann gilt:

a) $m|n \quad\Longrightarrow\quad E_m \subseteq E_n$ **b)** $E_n \;=\; \bigcup\limits_{m|n} E_m'$ (disjunkte Vereinigung)

c) $\sum\limits_{m|n} \varphi(m) \;=\; n\,.$

(16.7) DEF: Sei $n \in \mathbb{N}$. Dann heißt das Polynom $\quad \Phi_n \;:=\; \prod\limits_{\varepsilon \in E_n'} (T - \varepsilon)$

das n**–te Kreisteilungspolynom**.

(16.8) BEM: **a)** $\Phi_n \in \mathbb{Q}_n[T]$ ist ein normiertes Polynom. Später sehen wir, daß die Koeffizienten von Φ_n sogar in $\mathbb{Z}$ liegen. Jede primitive n–te Einheitswurzel ist eine Nullstelle von Φ_n, und es gilt

$$\mathrm{grad}(\Phi_n) \;=\; |E_n'| \;=\; \varphi(n)\,.$$

b) Ist $\varepsilon \in E_n'$, so gilt

$$\Phi_n \;=\; \prod_{\substack{k = 1 \ldots n \\ \mathrm{ggT}(k,n) = 1}} (T - \varepsilon^k)$$

(16.9) LEMMA: $\quad T^n - 1 \;=\; \prod\limits_{m|n} \Phi_m\,.$

(16.9) liefert eine Methode zur sukzessiven Bestimmung der Kreisteilungspolynome.

(16.10) BEISPIELE:

n	Φ_n
1	$\Phi_1 = T - 1$
2	$T^2 - 1 = \Phi_1\Phi_2 = (T-1)\Phi_2 \quad\Longrightarrow\quad \Phi_2 = T + 1$
3	$T^3 - 1 = \Phi_1\Phi_3 = (T-1)\Phi_3 \quad\Longrightarrow\quad \Phi_3 = T^2 + T + 1$
4	$T^4 - 1 = \Phi_1\Phi_2\Phi_4 = (T-1)(T+1)\Phi_4 \quad\Longrightarrow\quad \Phi_4 = T^2 + 1$
$p \in \mathbb{P}$	$T^p - 1 = \Phi_1\Phi_p = (T-1)\Phi_p \quad\Longrightarrow\quad \Phi_p = T^{p-1} + T^{p-2} + \ldots + T + 1$

In all diesen Fällen ist Φ_n sogar ein Polynom mit ganzzahligen Koeffizienten, das außerdem irreduzibel über $\mathbb{Q}$ ist (Φ_p ist für $p \in \mathbb{P}$ nach (5.7) irreduzibel über $\mathbb{Q}$). Dieses Ergebnis läßt sich allgemein beweisen.

(16.11) LEMMA: Für $n \in \mathbb{N}$ gilt:

a) $\Phi_n \in \mathbb{Z}[T]$

b) Φ_n ist irreduzibel über $\mathbb{Q}$

c) Φ_n ist Minimalpolynom einer jeden primitiven n–ten Einheitswurzel über $\mathbb{Q}$.

(16.12) SATZ: Sei $n \in \mathbb{N}$. Dann gilt

a) $\mathbb{Q}_n : \mathbb{Q}$ ist eine Galois–Erweiterung

b) $[\,\mathbb{Q}_n : \mathbb{Q}\,] = \varphi(n)$

c) $\mathrm{Gal}(\mathbb{Q}_n : \mathbb{Q}) \cong (\mathbb{Z}_n^\star, \cdot)$ (Einheitengruppe des Ringes $\mathbb{Z}_n$).

Dieser Satz enthält (16.1) als Spezialfall.

(16.13) KOROLLAR: $\mathrm{grad}_{\mathbb{Q}}(\varepsilon_n) = \varphi(n)$.

(16.14) SATZ: Für $n \in \mathbb{N}, n \geq 3$ sind folgende Aussagen äquivalent:

a) Das regelmäßige n–Eck ist mit Zirkel und Lineal konstruierbar

b) $\varphi(n)$ ist eine Zweierpotenz.

(16.15) KOROLLAR: Sei $n \in \mathbb{N}, n \geq 3$. Genau dann ist das regelmäßige n–Eck mit Zirkel und Lineal konstruierbar, wenn n die folgende Gestalt hat:

$$n = 2^k \cdot p_1 \cdot \ldots p_r \quad (k \geq 0, r \geq 0),$$

wobei $p_1, \ldots, p_r$ paarweise verschiedene Fermat'sche Primzahlen sind.