Universität Konstanz
Fachbereich Mathematik und Statistik
Markus Schweighofer

§5.4 Kreisteilungskörper

Proposition 5.4.1. (a) *Sind $a, n \in \mathbb{Z}$, so*

$$\overline{a}^{(n)} \in (\mathbb{Z}/(n))^\times \iff (a,n) = (1).$$

(b) *Ist $n \in \mathbb{N}$, so*

$$(\mathbb{Z}/(n))^\times = \{\overline{a}^{(n)} \mid a \in \{0,\dots,n-1\}, (a,n) = (1)\}.$$

Beweis. (a) Seien $a, n \in \mathbb{Z}$. Ist $\overline{a}^{(n)} \in (\mathbb{Z}/(n))^\times$, so gibt es $s \in \mathbb{Z}$ mit $\overline{sa}^{(n)} = 1$ und daher auch $t \in \mathbb{Z}$ mit $sa + tn = 1$. Ist $(a,n) = (1)$, so gibt es $s, t \in \mathbb{Z}$ mit $sa + tn = 1$ und daher $\overline{s}^{(n)}\overline{a}^{(n)} = 1$. □

Definition 5.4.2. Die Abbildung

$$\varphi\colon \mathbb{N} \to \mathbb{N},\ n \mapsto \#(\mathbb{Z}/(n))^\times$$

heißt die *Eulersche φ-Funktion* [Leonard Euler *1846 †1912].

Proposition 5.4.3. (a) $\forall m, n \in \mathbb{N} : ((m,n) = (1) \implies \varphi(mn) = \varphi(m)\varphi(n))$

(b) $\forall p \in \mathbb{P} : \forall k \in \mathbb{N} : \varphi(p^k) = (p-1)p^{k-1}$

(c) $\forall n \in \mathbb{N} : \varphi(n) = n \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} \left(1 - \frac{1}{p}\right)$

Beweis. **(a)** Sind $m, n \in \mathbb{N}$ mit $(m,n) = (1)$, so gilt nach dem Chinesischen Restsatz 2.8.5

$$\mathbb{Z}/(mn) \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$

und daher [→2.8.7]

$$(\mathbb{Z}/(mn))^\times \cong (\mathbb{Z}/(m))^\times \times (\mathbb{Z}/(n))^\times.$$

(b) Sind $p \in \mathbb{P}$ und $k \in \mathbb{N}$, so

$$\begin{aligned}\varphi(p^k) \overset{5.4.1(b)}{=} \#\{a \in \{0,\dots,p^k-1\} \mid p \nmid a\} &= \#(\{0,\dots,p^k-1\} \setminus \{0,p,\dots,p^k-p\}) \\ &= p^k - p^{k-1} = (p-1)p^{k-1}.\end{aligned}$$

(c) Sei $n \in \mathbb{N}$. Schreibe $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ mit $m \in \mathbb{N}_0$, $p_1, \ldots, p_m \in \mathbb{P}$ paarweise verschieden und $\alpha_1, \ldots, \alpha_m \in \mathbb{N}$. Dann

$$\varphi(n) \overset{(a)}{=} \varphi(p_1^{\alpha_1}) \cdots \varphi(p_m^{\alpha_m}) \overset{(b)}{=} p_1^{\alpha_1 - 1} \cdots p_m^{\alpha_m - 1}(p_1 - 1) \cdots (p_m - 1) =$$
$$= \underbrace{p_1^{\alpha_1} \cdots p_m^{\alpha_m}}_{=n} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

□

Bemerkung 5.4.4. Sei G eine multiplikativ geschriebene geschriebene endliche zyklische Gruppe der Ordnung n. Sei $a \in G$ mit $G = \langle a \rangle$. Dann ist

$$\mathbb{Z}/\langle n \rangle \to G,\ \overline{k} \mapsto a^k \qquad (k \in \mathbb{Z})$$

wohldefiniert und ein Gruppenisomorphismus. Für alle $k \in \mathbb{Z}$ gilt

$$(k, n) = (1) \iff \overline{k} \in (\mathbb{Z}/(n))^\times \iff G = \langle a^k \rangle.$$

Definition 5.4.5. Sei K ein Körper und $\zeta \in K$. Man nennt ζ

- eine *Einheitswurzel* in K, wenn $\exists n \in \mathbb{N} : \zeta^n = 1$,
- eine *n-te Einheitswurzel*, wenn $\zeta^n = 1$ ($n \in \mathbb{N}$) und
- eine *primitive n-te Einheitswurzel* in K, wenn ζ in $K^\times$ die Ordnung n hat ($n \in \mathbb{N}$).

Bemerkung 5.4.6. Sei K ein Körper.

(a) Die Einheitswurzeln in K bilden eine Untergruppe von $K^\times$.

(b) Ist $n \in \mathbb{N}$, so bilden die n-ten Einheitswurzeln in K eine zyklische Untergruppe von $K^\times$, deren Ordnung n teilt ($X^n - 1$ hat nur endlich viele Nullstellen, aber endliche Untergruppen von $K^\times$ sind zyklisch [→ 4.4.19] und nach Lagrange teilt die Ordnung eines Erzeugers n).

Beispiel 5.4.7. Sei $n \in \mathbb{N}$. Die n-ten Einheitswurzeln in $\mathbb{C}$ sind

$$e^{\frac{2k\pi i}{n}} \qquad (k \in \{0, \ldots, n-1\}).$$

Ist $k \in \mathbb{Z}$, so ist $e^{\frac{2k\pi i}{n}}$ eine primitive n-te Einheitswurzel in $\mathbb{C}$ genau dann, wenn

$$(k, n) = (1).$$

Proposition 5.4.8. *Sei K ein Körper, $p := \operatorname{char} K \in \{0\} \cup \mathbb{P}$ und $n \in \mathbb{N}$. Dann sind folgende Aussagen äquivalent:*

(a) *K besitzt eine primitive n-te Einheitswurzel.*

(b) *K besitzt n n-te Einheitswurzeln.*

(c) $p \nmid n$ *und* $X^n - 1$ *zerfällt in* $K[X]$.

Beweis. (a) $\Longrightarrow$ (b) trivial

(b) $\Longrightarrow$ (a) klar mit 5.4.6(b).

Setzt man $f := X^n - 1$, so $f' = nX^{n-1}$ und daher

$$f \text{ separabel} \iff f' \neq 0 \iff n \neq 0 \text{ in } K \iff p \nmid n.$$

Hieraus folgt (b) $\Longleftrightarrow$ (c). □

Proposition 5.4.9. *Sei R ein faktorieller Ring und K sein Quotientenkörper. Dann liegt jeder normierte Teiler in $K[X]$ eines normierten Polynoms aus $R[X]$ schon in $R[X]$.*

Beweis. Sei $f \in R[X$ normiert und seien $g, h \in K[X]$ mit $f = gh$ und g normiert. Zu zeigen ist $g \in R[X]$. Betrachte für jedes $p \in \mathbb{P}_R$ [→ 2.4.1] die p-Bewertung v_p auf K [→ 2.5.3] und ihre Gauß-Fortsetzung w_p auf $K(X)$ [→ 2.5.7]. Es ist h natürlich auch normiert und damit $w_p(h) \leq 0$ für alle $p \in \mathbb{P}_R$. Es folgt

$$0 = w_p(f) = w_p(gh) \overset{2.5.1}{=} w_p(g) + w_p(h) \leq w_p(g)$$

für alle $p \in \mathbb{P}_R$ und damit $g \in R[X]$. □

Definition und Proposition 5.4.10. Sei $n \in \mathbb{N}$. Dann heißt

$$\Phi_n := \prod_{\substack{\xi \text{ primitive } n\text{-te} \\ \text{Einheitswurzel in } \mathbb{C}}} (X - \zeta) = \prod_{\substack{k=0 \\ (k,n)=(1)}}^{n-1} \left(X - e^{\frac{2k\pi i}{n}} \right) \in \mathbb{Z}[X]$$

das *n-te Kreisteilungspolynom* und sein Zerfällungskörper [→ 4.3.4] über $\mathbb{Q}$ der n-te *Kreisteilungskörper*.

Beweis. Zu zeigen ist $\Phi_n \in \mathbb{Z}[X]$. Da Φ_n in $\mathbb{Q}[X]$ offensichtlich ein normierter Teiler von $X^n - 1 \in \mathbb{Z}[X]$ ist, reicht es nach 5.4.9 $\Phi_n \in \mathbb{Q}[X]$ zu zeigen. Da $\overline{\mathbb{Q}}|\mathbb{Q}$ galoissch ist, reicht es nach 5.1.4(c) zu zeigen, dass für alle $\varphi \in \mathrm{Aut}(\overline{\mathbb{Q}}|\mathbb{Q})$ für den Ringhomomorphismus [→ 2.2.7]

$$\widetilde{\varphi}\colon \overline{\mathbb{Q}}[X] \to \overline{\mathbb{Q}}[X], \begin{array}{l} a \mapsto \varphi(a) \quad (a \in \overline{\mathbb{Q}}) \\ X \mapsto X \end{array}$$

gilt $\widetilde{\varphi}(\Phi_n) = \Phi_n$. Dies folgt aber daraus, dass jedes solche φ die primitiven n-ten Einheitswurzeln in $\overline{\mathbb{Q}}$ permutiert. □

Bemerkung 5.4.11. Sei $n \in \mathbb{N}$ und ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Dann ist $\mathbb{Q}(\zeta)$ der Zerfällungskörper von $X^n - 1$ und damit auch der n-te Kreisteilungskörper.

Satz 5.4.12. *Sei $n \in \mathbb{N}$.*

(a) *Φ_n ist irreduzibel in $\mathbb{Q}[X]$.*

(b) *Der n-te Kreisteilungskörper ist galoissch über $\mathbb{Q}$ mit Galoisgruppe $G \cong (\mathbb{Z}/(n))^\times$. Für jede primitive n-te Einheitswurzel ζ in $\mathbb{C}$ ist*

$$G \to (\mathbb{Z}/(n))^\times,\ \varphi \mapsto \overline{k} \text{ falls } k \in \mathbb{Z} \text{ mit } \varphi(\zeta) = \zeta^k$$

ein Gruppenisomorphismus.

Beweis. Sei ζ eine primitive n-te Einheitswurzel in $\mathbb{C}$. Dann ist natürlich $f := \operatorname{irr}_{\mathbb{Q}}(\zeta)$ ein Teiler von Φ_n in $\mathbb{Q}[X]$. Wir zeigen $f = \Phi_n$, womit auch (a) gezeigt ist. Mit 5.4.4 reicht es hierfür zu zeigen, dass für jede primitive n-te Einheitswurzel z in $\mathbb{C}$ und alle $p \in \mathbb{P}$ mit $p \nmid n$ gilt

$$f(z) = 0 \implies f(z^p) = 0.$$

Sei hierzu $z \in \mathbb{C}$ und $p \in \mathbb{P}$ mit $f(z) = 0$ und $f(z^p) \neq 0$. Zu zeigen: $p \mid n$. Schreibe $X^n - 1 = fg$ mit $g \in \mathbb{Q}[X]$. Nach 5.4.9 gilt $f, g \in \mathbb{Z}[X]$. Wegen $f(z^p) \neq 0$ und $(fg)(z^p) = 0$ folgt $g(z^p) = 0$, das heißt z ist Nullstelle von $g(X^p)$. Wegen $f = \operatorname{irr}_{\mathbb{Q}}(z)$ gibt es $h \in \mathbb{Q}[X]$ mit $g(X^p) = fh$. Wieder mit 5.4.9 erhält man $h \in \mathbb{Z}[X]$. Wir reduzieren nun die Koeffizienten modulo p, das heißt wir wenden den Ringhomomorphismus $\psi\colon \mathbb{Z}[X] \to \mathbb{F}_p[X],\ X \mapsto X$ an und benutzen den Frobeniushomomorphismus $\Phi_{\mathbb{F}_p[X]}\colon \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ [$\to$ 4.4.3], um $X^n - 1 = \psi(f)\psi(g)$ und $\psi(g)^p = \psi(g(X^p)) = \psi(fh) = \psi(f)\psi(h)$ zu erhalten. Wegen $\psi(f) \mid (\psi(g))^p$ ist $X^n - 1$ nicht separabel über $\mathbb{F}_p$. Wegen $(X^n - 1)' = nX^{n-1} \in \mathbb{F}_p[X]$ gilt dann aber $n = 0$ in $\mathbb{F}_p[X]$, das heißt $p \mid n$ wie gewünscht.

(b) Als Zerfällungskörper von $X^n - 1$ über $\mathbb{Q}$ ist der n-te Kreisteilungskörper $\mathbb{Q}(\zeta)$ galoissch über $\mathbb{Q}$. Wendet man 5.4.4 auf die Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$ an, so sieht man, dass die Abbildung wohldefiniert ist. Sie ist auch injektiv und wegen

$$\#G \overset{\text{Galoistheorie}}{=} [\mathbb{Q}(\zeta) : \mathbb{Q}] \overset{4.1.10}{=} \deg \operatorname{irr}_{\mathbb{Q}}(\zeta) \overset{\text{(a)}}{=} \deg(\Phi_n) = \varphi(n)$$

daher auch surjektiv. □

Bemerkung 5.4.13. Die für alle $n \in \mathbb{N}$ gültige Formel

$$X^n - 1 = \prod_{\substack{\zeta \in \mathbb{C} \\ \zeta^n = 1}} (X - \zeta) = \prod_{\substack{d \in \mathbb{N} \\ d \mid n}} \prod_{\substack{\zeta \text{ primitive} \\ d\text{-te Einheitswurzel}}} (X - \zeta) = \prod_{\substack{d \in \mathbb{N} \\ d \mid n}} \Phi_d$$

liefert ein rekursives Berechnungsverfahren für Φ_n. Zum Beispiel gilt

$$\Phi_{12} = \frac{X^{12} - 1}{\Phi_1\Phi_2\Phi_3\Phi_4\Phi_6} = \frac{X^{12} - 1}{(X^6 - 1)\Phi_4} = \frac{X^6 + 1}{\Phi_4}$$

und $\Phi_4 = \frac{X^4 - 1}{\Phi_1\Phi_2} = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1$. Also $\Phi_{12} = \frac{X^6 + 1}{X^2 + 1} = X^4 - X^2 + 1$.