Aufgabe F20T2A2

Zeigen Sie:

(a) Ist $n = dm$ mit ungeradem $m \in \mathbb{N}$, so gilt die Teilbarkeitsrelation $(x^d + 1) \mid (x^n + 1)$.

(b) Das Polynom $x^n + 1$ ist genau dann über $\mathbb{Q}$ irreduzibel, wenn $n = 2^k$ für ein $k \in \mathbb{N}_0$ gilt.

Lösung:

zu (a) Wir zeigen: Für jedes $t \in \mathbb{N}$ ist $\zeta \in \mathbb{C}^\times$ genau dann eine Nullstelle von $x^t + 1$, wenn die Ordnung von ζ in $\mathbb{C}^\times$ zwar ein Teiler von $2t$, aber kein Teiler von t ist. „⇐“ Sei $\mathrm{ord}(\zeta) \mid (2t)$ und $\mathrm{ord}(\zeta) \nmid t$ vorausgesetzt. Wegen $(\zeta^t)^2 = \zeta^{2t} = 1$ ist ζ^t einerseits eine Nullstelle von $x^2 - 1$, also $\zeta^t \in \{\pm 1\}$, andererseits ist $\zeta^t = 1$ ausgeschlossen, da ansonsten $\mathrm{ord}(\zeta) \mid t$ gelten würde. Also gilt $\zeta^t = -1$, und somit ist ζ eine Nullstelle von $x^t + 1$ „⇒“ Sei $\zeta \in \mathbb{C}$ eine Nullstelle von $x^t + 1$. Dann gilt $\zeta^t = -1$ und $\zeta^{2t} = (-1)^2 = 1$, also $\zeta \in \mathbb{C}^\times$ und $\mathrm{ord}(\zeta) \mid 2t$. Würde auch $\mathrm{ord}(\zeta) \mid t$ gelten, dann würde daraus $\zeta^t = 1$ folgen, im Widerspruch zu $\zeta^t = -1$.

Seien nun $d, m, n \in \mathbb{N}$ wie angegeben. Die Polynome x^d+1 und x^n+1 haben wegen $\mathrm{ggT}(x^d+1, dx^{d-1}) = 1$ und $\mathrm{ggT}(x^n + 1, nx^{n-1}) = 1$ nur einfache Nullstellen. Für den Nachweis der Teilbarkeitsrelation genügt es deshalb nachzuweisen, dass jede komplexe Nullstelle von $x^d + 1$ auch eine Nullstelle von $x^n + 1$ ist. Sei also $\zeta \in \mathbb{C}$ eine Nullstelle von $x^d + 1$. Wie im vorherigen Absatz gezeigt, gilt $\zeta \in \mathbb{C}^\times$, $\mathrm{ord}(\zeta) \mid (2d)$ und $\mathrm{ord}(\zeta) \nmid d$. Weil d ein Teiler von n ist, gilt auch $(2d) \mid (2n)$ und damit $\mathrm{ord}(\zeta) \mid (2n)$. Nehmen wir nun an, dass auch $\mathrm{ord}(\zeta) \mid n$ erfüllt ist. Dann ist $\mathrm{ord}(\zeta)$ insgesamt ein Teiler von $\mathrm{ggT}(2d, n) = \mathrm{ggT}(2d, dm) = d$, wobei im letzten Schritt verwendet wurde, dass m ungerade ist. Aber $\mathrm{ord}(\zeta) \mid d$ steht im Widerspruch zu unserer Voraussetzung. Es gilt also $\mathrm{ord}(\zeta) \mid (2n)$ und $\mathrm{ord}(\zeta) \mid n$. Wie oben gezeigt folgt daraus, dass ζ eine Nullstelle von $x^n + 1$ ist.

zu (b) „⇐“ Ist $n = 2^k$ für ein $k \in \mathbb{N}_0$, dann ist $x^n + 1$ das $2n$-te Kreisteilungspolynom und somit laut Vorlesung über $\mathbb{Q}$ irreduzibel. Bezeichnen wir nämlich für jedes $m \in \mathbb{N}$ mit $\Phi_m \in \mathbb{Z}[x]$ das m-te Kreisteilungspolynom, so gilt laut Vorlesung $x^{2n} - 1 = \prod_d \Phi_d$, wobei d die Teiler von $2n = 2^{k+1}$ durchläuft. Die Menge dieser Teiler besteht aus $2n$ und den Teilern von n, so dass die Gleichung in der Form $x^{2n} - 1 = \Phi_{2n} \cdot (x^n - 1)$ geschrieben werden kann. Daraus wiederum folgt

$$\Phi_{2n} \quad = \quad \frac{x^{2n} - 1}{x^n - 1} \quad = \quad x^n + 1.$$

„⇒“ Ist n keine Zweierpotenz, so gibt es eine Zerlegung $n = dm$ mit $d, m \in \mathbb{N}$, wobei $d > 1$ und ungerade ist. Nach Teil (a) wird $x^n + 1$ dann von $x^d + 1$ geteilt, mit $1 < d < n$. Daraus folgt, dass $x^n + 1$ in $\mathbb{Q}[x]$ reduzibel ist.