Aufgabe F16T3A2 (12 Punkte)

Seien $m, n \in \mathbb{N}$ natürliche Zahlen ≥ 1. Man zeige:

(a) $x^m - 1$ ist ein Teiler von $x^n - 1$ in $\mathbb{Q}[x]$ genau dann, wenn m ein Teiler von n ist.

(b) $x^m + 1$ ist ein Teiler von $x^n + 1$ in $\mathbb{Q}[x]$ genau dann, wenn m ein Teiler von n und der Quotient $\frac{n}{m}$ ungerade ist.

(c) Genau dann ist $x^n + 1$ irreduzibel in $\mathbb{Q}[x]$, wenn n eine Potenz von 2 ist.
(*Hinweis:* Für eine Zweierpotenz n ist $(x+1)^n + 1$ ein Eisenstein-Polynom.)

Lösung:

zu (a) Sei $f_m = x^m - 1$, $R_m = \mathbb{Q}[x]/(f_m)$. Für jedes $g \in \mathbb{Q}[x]$ sei $[g]$ jeweils die entsprechende Restklasse in R_m. Es gilt $[x^m] = [x^m - 1] + [1] = [0] + [1] = [1]$ in R_m. Division von n durch m mit Rest liefert ganze Zahlen q, r mit $n = qm + r$ und $0 \leq r < m$. Wir erhalten die Äquivalenz

$$f_m \mid (x^n - 1) \quad \Leftrightarrow \quad [x^n - 1] = [0] \quad \Leftrightarrow \quad [x^n] = [1] \quad \Leftrightarrow \quad [x^{qm+r}] = [1] \quad \Leftrightarrow$$

$$[x^m]^q [x]^r = [1] \quad \Leftrightarrow \quad [1]^q [x]^r = [1] \quad \Leftrightarrow \quad [x^r - 1] = [0] \quad \Leftrightarrow \quad f_m \mid (x^r - 1) \quad \Leftrightarrow \quad r = 0 \quad \Leftrightarrow \quad m \mid n$$

wobei im vorletzten Schritt $\operatorname{grad}(x^r - 1) = r < m = \operatorname{grad}(f_m)$ verwendet wurde.

zu (b) Hier gehen wir auf ähnliche Weise vor. Diesmal sei $f_m = x^m + 1$, $S_m = \mathbb{Q}[x]/(f_m)$, und wieder seien $q, r \in \mathbb{Z}$ so gewählt, dass $n = qm + r$ und $0 \leq r < m$ gilt. In S_m gilt die Gleichung $[x^m] = [x^m + 1] + [-1] = [0] + [-1] = [-1]$. Wir erhalten

$$f_m \mid (x^n + 1) \quad \Leftrightarrow \quad [x^n + 1] = [0] \quad \Leftrightarrow \quad [x^n] = [-1] \quad \Leftrightarrow \quad [x^{qm+r}] = [-1] \quad \Leftrightarrow$$

$$[x^m]^q [x]^r = [-1] \quad \Leftrightarrow \quad [(-1)]^q [x]^r = [-1] \quad \Leftrightarrow \quad (x^m + 1) \mid ((-1)^q x^r + 1).$$

Wegen $r < m$ ist die letzte Relation genau dann erfüllt, wenn $(-1)^q x^r + 1 = 0$ ist, also $r = 0$ und $(-1)^q = -1$ gilt. Dies ist äquivalent dazu, dass m ein Teiler von n und $q = \frac{m}{n}$ ungerade ist.

zu (c) „⇒“ Ist n keine Zweierpotenz, dann besitzt n einen ungeraden Primteiler p. Setzen wir $m = \frac{n}{p}$, dann erfüllen m und n die Voraussetzungen von Teil (b), und es folgt $(x^m + 1) \mid (x^n + 1)$. Wegen $1 \leq m < n$ ist $x^m + 1$ ein echter Teiler von $x^n + 1$ und $x^n + 1$ folglich nicht irreduzibel.

„⇔“ Hier überprüfen wir zunächst den Hinweis aus der Angabe. Ist $n = 2^r$ für ein $r \in \mathbb{N}_0$, dann gilt für das Bild von $f = (x+1)^n + 1$ in $\mathbb{F}_2[x]$ die Gleichung

$$(x + \bar{1})^n + \bar{1} \quad = \quad (x + \bar{1})^{2^r} + \bar{1} \quad = \quad x^{2^r} + \bar{1} + \bar{1} \quad = \quad x^{2^r}.$$

Dies zeigt, dass alle Koeffizienten von f mit Ausnahme des höchsten durch 2 teilbar sind. Allerdings ist der konstante Term von f gleich 2, also nicht durch 4 teilbar, außerdem ist f normiert. Insgesamt sind also die Voraussetzungen des Eisenstein-Kriteriums für $p = 2$ erfüllt.

Nehmen wir nun an, dass $x^n + 1$ in $\mathbb{Q}[x]$ reduzibel ist. Dann gibt es nicht-konstante Polynome $g, h \in \mathbb{Q}[x]$ mit $x^n + 1 = gh$. Ersetzen wir in dieser Gleichung x durch $x + 1$, so erhalten wir $f = (x+1)^n + 1 = \tilde{g}\tilde{h}$ mit den nicht-konstanten Polynomen $\tilde{g}(x) = g(x+1)$ und $\tilde{h}(x) = h(x+1)$. Also ist auch f in diesem Fall reduzibel. Wie wir gerade gesehen haben, kann n in diesem Fall keine Zweierpotenz sein.