Aufgabe H19T2A1 (12 Punkte)

(a) Seien $k, \ell \in \mathbb{N}_0$ mit $k < \ell$. Betrachte die Polynome $x^{2^k} + 1$ und $x^{2^\ell} - 1$ aus $\mathbb{Q}[x]$. Man zeige, dass $x^{2^k} + 1$ ein Teiler von $x^{2^\ell} - 1$ ist.

(b) Für $m \in \mathbb{N}$ setze $n = 2^{2^m} + 1$. Man beweise, dass $2^{n-1} \equiv 1 \bmod n$ gilt.

Lösung:

zu (a) Sei $R_k = \mathbb{Q}[x]/(x^{2^k} + 1)$ und $\alpha = x + (x^{2^k} + 1) \in R_k$. Wegen $x^{2^k} \equiv -1 \bmod (x^{2^k} + 1)$ gilt $\alpha^{2^k} \equiv -1_{R_k}$ im Faktorring R_k. Daraus folgt

$$\alpha^{2^\ell} \quad = \quad (\alpha^{2^k})^{2^{\ell-k}} \quad = \quad (-1_{R_k})^{2^{\ell-k}} \quad = \quad ((-1_{R_k})^2)^{2^{\ell-k-1}} \quad = \quad 1_{R_k}^{2^{\ell-k-1}} \quad = \quad 1_{R_k}.$$

Daraus wiederum folgt $x^{2^\ell} \equiv 1 \bmod (x^{2^k} + 1)$. Dies zeigt, dass $x^{2^k} + 1$ in $\mathbb{Q}[x]$ ein Teiler von $x^{2^\ell} - 1$ ist.

zu (b) Es gilt $m < 2^m$, denn durch Anwendung der Bernoullischen Ungleichung $(1 + x)^k \geq 1 + kx$ (die für alle $k \in \mathbb{N}$ und alle $x \in \mathbb{R}$ mit $x \geq -1$ gültig ist) auf $x = 1$ und $k = m$ erhält man $2^m \geq 1 + m > m$. (Dies kann man natürlich auch ohne die Bernoullische Ungleichung, durch vollständige Induktion über m, beweisen.) Definieren wir $f_k = x^{2^k} + 1$ und $g_k = x^{2^k} - 1$ für alle $k \in \mathbb{N}_0$, dann ist nach Teil (a) das Polynom f_m somit ein Teiler von g_{2^m} in $\mathbb{Q}[x]$. Weil f_m und g_{2^m} in $\mathbb{Z}[x]$ liegen und f_m darüber hinaus normiert und damit primitv ist, teilt f_m das Polynom g_{2^m} sogar in $\mathbb{Z}[x]$.

Es gibt also ein $h \in \mathbb{Z}[x]$, so dass $g^{2^m} = hf_m$ gilt. Nun ist $f_m(2) = 2^{2^m} + 1 = n$ und $g_{2^m}(2) = 2^{2^{2^m}} - 1 = 2^{(2^{2^m}+1)-1} - 1 = 2^{n-1} - 1$. Wegen $g_{2^m}(2) = h(2)f_m(2)$ und $h(2) \in \mathbb{Z}$ ist $f_m(2) = n$ im Ring $\mathbb{Z}$ ein Teiler von $g_{2^m}(2) = 2^{n-1} - 1$. Aus $n \mid (2^{n-1} - 1)$ folgt $2^{n-1} \equiv 1 \bmod n$.