Aufgabe F14T1A3 (5+7 Punkte)

Es seien K ein Körper und $K[x]$ der Polynomring über K. Es seien weiter m, n nichtnegative ganze Zahlen. Zeigen Sie:

(a) Ist $m > 0$, dann ist $x^r - 1$ der Rest bei Division von $x^n - 1$ durch $x^m - 1$, wobei r der Rest bei Division von n durch m ist.

(b) Sei $g = \mathrm{ggT}(m, n)$. Dann ist $x^g - 1$ ein größter gemeinsamer Teiler von $x^n - 1$ und $x^m - 1$ in $K[x]$.

Lösung:

zu (a) Nach Voraussetzung gibt es ein $q \in \mathbb{Z}$ mit $n = qm + r$, und es ist $0 \leq r < m$. Sei nun $f \in K[x]$ das Polynom, das man bei Division von $x^n - 1$ durch $x^m - 1$ als Rest erhält. Dann gibt es also ein Polynom $g \in K[x]$ mit $x^n - 1 = g(x^m - 1) + f$, außerdem ist $\mathrm{grad}(f) < \mathrm{grad}(x^m - 1) = m$. Zu zeigen ist nun, dass $f = x^r - 1$ gilt. Die entscheidende Idee besteht darin, diese Gleichung im Restklassenring $R = K[x]/(h)$ zu betrachten, mit $h = x^m - 1$.

Nach Definition von R sind zwei Elemente $f_1 + (h)$ und $f_2 + (h)$ aus R genau dann gleich, wenn die Differenz $f_1 - f_2$ der Polynome $f_1, f_2 \in K[x]$ ein Vielfaches von h ist. Deshalb gilt zum Beispiel $x^m + (h) = 1 + (h)$, was nach Definition der Multiplikation in R auch in der Form $(x + (h))^m = 1 + (h)$ geschrieben werden kann. Auf Grund der Gleichung $x^n - 1 = gh + f$ gilt auch $(x + (h))^n - (1 + (h)) = f + (h)$. Insgesamt erhalten wir

$$\begin{aligned} f + (h) &= (x + (h))^n - (1 + (h)) = (x + (h))^{mq+r} - (1 + (h)) = \\ ((x + (h))^m)^q (x + h)^r - (1 + (h)) &= (1 + (h))^q (x + (h))^r - (1 + (h)) = \\ (x + (h))^r - (1 + (h)) &= (x^r - 1) + (h). \end{aligned}$$

Die Gleichung zeigt, dass die Differenz $f - (x^r - 1)$ durch h teilbar ist, außerdem ist sie vom Grad $< m = \mathrm{grad}(h)$. Daraus folgt $f - (x^r - 1) = 0$ und $f = x^r - 1$.

zu (b) Nach Definition des größten gemeinsamen Teilers müssen wir die folgenden beiden Aussagen verifizieren.

(i) Das Polynom $x^g - 1$ ist ein Teiler von $x^n - 1$ und $x^m - 1$.

(ii) Ist $f \in K[x]$ ein gemeinsamer Teiler von $x^n - 1$ und $x^m - 1$, dann ist f auch ein Teiler von $x^g - 1$.

zu (i) Weil g ein Teiler von m und n ist, gibt es $p, q \in \mathbb{Z}$ mit $m = pg$ und $n = qg$. Sei $R = K[x]/(h)$ mit $h = x^g - 1$. Dann gilt $(x + (h))^g = x^g + (h) = 1 + (h)$. Wir erhalten

$$x^m + (h) = (x + (h))^m = ((x + (h))^g)^p = (1 + (h))^p = 1 + (h)$$

und ebenso $x^n + (h) = (x + (h))^n = ((x + (h))^g)^q = (1 + (h))^q = 1 + (h)$. Die erste Gleichung zeigt, dass h ein Teiler von $x^m - 1$ ist, die zweite entsprechend die Teilbarkeit von $x^n - 1$ durch h.

zu (ii) Hier rechnen wir im Restklassenring $S = K[x]/(f)$. Nach Voraussetzung ist f ein Teiler von $x^n - 1$ und $x^m - 1$. Daraus folgen die beiden Gleichungen $(x + (f))^m = x^m + (f) = 1 + (f)$ und $(x + (f))^n = x^n + (f) = 1 + (f)$ im Ring S. Nach dem Lemma von Bézout gibt es $p, q \in \mathbb{Z}$ mit $pm + qn = g$. Damit erhalten wir

$$\begin{aligned} x^g + (f) &= (x + (f))^g = (x + (f))^{pm+qn} = ((x + (f))^m)^p((x + (f))^n)^q \\ &= (1 + (f))^p(1 + (f))^q = 1 + (f). \end{aligned}$$

Diese Gleichung im Restklassenring S zeigt, dass f in $K[x]$ ein Teiler von $x^g - 1$ ist.