Aufgabe F18T1A1 (12 Punkte)

(a) Sei $p = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Z}[x]$ ein normiertes Polynom. Sei $\bar{p} \in \mathbb{F}_3[x]$ das Polynom, das aus p durch Reduktion der Koeffizienten modulo 3 entsteht.

(i) Sei $\bar{p}$ irreduzibel in $\mathbb{F}_3[x]$. Zeigen Sie, dass p irreduzibel in $\mathbb{Z}[x]$ ist.

(ii) Zeigen Sie anhand eines Beispiels, dass die Umkehrung der Aussage in (i) falsch ist.

(b) Zeigen Sie, dass das Polynom $x^3 + (3m-1)x + (3n+1)$ für alle $m, n \in \mathbb{Z}$ irreduzibel in $\mathbb{Z}[x]$ ist.

Lösung:

zu (a)(i) Wäre p in $\mathbb{Z}[x]$ nicht irreduzibel, dann wäre p entweder im Ring $\mathbb{Z}[x]$ eine Einheit, oder es gäbe eine Zerlegung $p = fg$ von p in Nicht-Einheiten $f, g \in \mathbb{Z}[x]$. Im ersten Fall würde $p \in \{\pm 1\}$ und damit $\bar{p} \in \{\pm\bar{1}\}$ folgen, denn weil $\mathbb{Z}$ ein Integritätsbereich ist, gilt $\mathbb{Z}[x]^\times = \mathbb{Z}^\times$, und bekanntlich ist $\mathbb{Z}^\times = \{\pm 1\}$ die Einheitengruppe von $\mathbb{Z}$. Aber $\bar{p} \in \{\pm\bar{1}\}$ würde bedeuten, dass $\bar{p}$ in $\mathbb{F}_3[x]$ eine Einheit ist, im Widerspruch zur Irreduzibilität von $\bar{p}$.

Betrachten wir nun den zweiten Fall $p = fg$. In diesem Fall würde $\bar{p} = \bar{f}\bar{g}$ folgen. Weil $\bar{p}$ in $\mathbb{F}_3[x]$ irreduzibel ist, muss $\bar{f}$ oder $\bar{g}$ in $\mathbb{F}_3[x]$ eine Einheit sein, o.B.d.A. sei dies $\bar{f}$. Seien $c, d \in \mathbb{Z}$ die Leitkoeffizienten von f, g. Weil p normiert ist, gilt $cd = 1$ und somit $c \in \{\pm 1\}$. Für das Bild $\bar{c} \in \mathbb{F}_3$ von c folgt daraus $\bar{c} \neq \bar{0}$. Damit muss $\mathrm{grad}(\bar{f}) = \mathrm{grad}(f)$ gelten. Weil $\bar{f}$ in $\mathbb{F}_3[x]$ eine Einheit ist, folgt $\mathrm{grad}(f) = \mathrm{grad}(\bar{f}) = 0$. Aber damit gilt $f = c \in \{\pm 1\}$. Das Element f ist also eine Einheit in $\mathbb{Z}[x]$, im Widerspruch zur Annahme.

zu (a)(ii) Das Polynom $p = x^2 + x + 1$ ist laut Vorlesung als drittes Kreisteilungspolynom irreduzibel in $\mathbb{Z}[x]$. Aber das Bild $\bar{p} = x^2 + x + \bar{1}$ ist in $\mathbb{F}_3[x]$ reduzibel. Denn $\bar{1}$ ist eine Nullstelle von $\bar{p}$ in $\mathbb{F}_3$, es gibt also ein Polynom $\bar{h} \in \mathbb{F}_3[x]$ vom Grad 1, so dass $\bar{p} = (x - \bar{1})\bar{h}$ gilt.

zu (b) Sei $p = x^3 + (3m-1)x + (3n+1) \in \mathbb{Z}[x]$ mit $m, n \in \mathbb{Z}$. Wegen $3m - 1 \equiv -1 \bmod 3$ und $3n + 1 \equiv 1 \bmod 3$ ist $\bar{p} = x^3 - x + \bar{1}$ das Bild von p in $\mathbb{F}_3[x]$. Das Polynom $\bar{p}$ ist in $\mathbb{F}_3[x]$ irreduzibel, denn es gilt $\mathrm{grad}(\bar{p}) \leq 3$, und $\bar{p}$ besitzt in $\mathbb{F}_3[x]$ keine Nullstelle wegen $\bar{p}(\bar{0}) = \bar{1} \neq \bar{0}$, $\bar{p}(\bar{1}) = \bar{1} \neq \bar{0}$ und $\bar{p}(\bar{2}) = \bar{7} = \bar{1} \neq \bar{0}$. Mit Teil (a)(i) folgt daraus die Irreduzibilität von p in $\mathbb{Z}[x]$.