F18-T1-A1

a) Sei $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ ein normiertes Polynom. Sei $\overline{P}(X) \in \mathbb{F}_3[X]$ das Polynom, das aus $P(X)$ durch Reduktion der Koeffizienten modulo 3 entsteht.

   i) Sei $\overline{P}(X)$ irreduzibel in $\mathbb{F}_3[X]$. Zeigen Sie, dass $P(X)$ 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.

Lösungsvorschlag. Zu a), i). Sei also $\overline{P}(X)$ irreduzibel. Wir wollen zeigen, dass $P(X) \in \mathbb{Z}[X]$ irreduzibel ist. Angenommen, P wäre reduzibel, also $P = Q \cdot R$ für (normierte) $Q, R \in \mathbb{Z}[X]$ mit $\deg(Q), \deg(R) > 0$. Da die Abbildung

$$\pi \colon \mathbb{Z}[X] \longrightarrow \mathbb{F}_3[X], \quad P \mapsto \overline{P}$$

nach Definition ein Ringmorphismus ist, wäre dann aber $\overline{P} = \pi(P) = \pi(Q \cdot R) = \pi(Q) \cdot \pi(R) = \overline{Q} \cdot \overline{R}$, was wegen $\deg(\overline{Q}) = \deg(Q) > 0$ und $\deg(\overline{R}) = \deg(R) > 0$ (aufgrund der Normiertheit von Q, R) ein Widerspruch ist zu der Voraussetzung, dass $\overline{P}$ irreduzibel ist.
Zu a), ii). Beispielsweise ist $P(X) := X^2 + 3 \in \mathbb{Z}[X]$ irreduzibel nach dem Eisensteinkriterium für das Primelement 3 (P ist normiert, insbesondere primitiv), aber

$$\overline{P}(X) = X^2 = X \cdot X \in \mathbb{F}_3[X]$$

ist offensichtlich nicht irreduzibel.
Zu b). Sei $P(X) := X^3 + (3m-1)X + (3n+1) \in \mathbb{Z}[X]$, für $m, n \in \mathbb{Z}$ beliebig. In der Notation von Teil a) ist dann

$$\overline{P}(X) = X^3 - X + 1 \in \mathbb{F}_3[X]$$

und nach Teil a), i) genügt es also, zu zeigen, dass $\overline{P}$ irreduzibel über $\mathbb{F}_3$ ist. Wegen $\deg(\overline{P}) = 3$ genügt es dafür, zu zeigen, dass $\overline{P}$ keine Nullstelle in $\mathbb{F}_3$ besitzt. Dazu berechnen wir $\overline{P}(0) = 1 \in \mathbb{F}_3$, $\overline{P}(1) = 1 \in \mathbb{F}_3$ und $\overline{P}(2) = -1 \in \mathbb{F}_3$.