F18-T3-A4

a) Zeigen Sie, dass $R_1 := \mathbb{Q}[X]/(X^4 + 12X - 2)$ ein Integritätsbereich ist.

b) Zeigen Sie, dass $R_2 := \mathbb{Z}[X]/(2, X^2+X+1)$ ein Körper ist. Wie viele Elemente besitzt dieser Körper?

Lösungsvorschlag. Zu a). Das Polynom $P(X) := X^4+12X-2$ ist normiert, insbesondere primitiv und irreduzibel über $\mathbb{Q}$ nach dem Lemma von Gauß und dem Eisensteinkriterium für dir Primzahl 2. Da $\mathbb{Q}[X]$ faktoriell ist, ist P damit schon ein Primelement in $\mathbb{Q}[X]$ und damit $(P(X)) \subset \mathbb{Q}[X]$ ein Primideal, was äquivalent dazu ist, dass $\mathbb{Q}[X]/(P(X))$ ein Integritätsbereich ist.
Bemerkung: Da $\mathbb{Q}[X]$ ein Hauptidealbereich ist, ist (P) damit sogar schon ein maximales Ideal, was äquivalent dazu ist, dass $\mathbb{Q}[X]/(P(X))$ ein Körper ist.
Zu b). Wir behaupten, dass ein kanonischer Isomorphismus von Ringen

$$\pi\colon R_2 = \mathbb{Z}[X]/(2, X^2 + X + 1) \xrightarrow{\simeq} \mathbb{F}_2[X]/(X^2 + X + 1)$$

existiert. Haben wir dies gezeigt, müssen wir nur noch beobachten, dass $P(X) := X^2 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel ist (da $\deg(P) = 2$ und $P(0) = 1 = P(1) \in \mathbb{F}_2$, das heißt P hat keine Nullstelle in $\mathbb{F}_2$), so dass $R_2 = \mathbb{F}_2[X]/(P(X))$ ein Körper ist. Weiter gilt dann

$$|R_2| = |\mathbb{F}_2[X]/(P(X))| = |\mathbb{F}_2|^{\deg(P)} = 4.$$

Um die Existenz eines solchen π zu zeigen, betrachten wir die kanonische Surjektion

$$\begin{aligned}\psi\colon \mathbb{Z}[X] &\xrightarrow{\psi_1} \mathbb{F}_2[X] \xrightarrow{\psi_2} \mathbb{F}_2[X]/(P(X)) \\ f(X) &\longmapsto \overline{f}(X) \longmapsto [\overline{f}(X)]\end{aligned}$$

Wobei hier für ein $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ mit $\overline{f} \in \mathbb{F}_2[X]$ das Polynom $\overline{f} = \sum_{i=0}^n \overline{a_i} X^i \in \mathbb{F}_2[X]$ gemeint ist, welches wir aus f durch Reduktion der Koeffizienten a_i zu $\overline{a_i} = [a_i] \in \mathbb{F}_2$ erhalten. Wir wollen zeigen, dass gilt $\ker\psi = (2, X^2 + X + 1)$, denn dann erhalten wir nach dem Homomorphiesatz den gewünschten Isomorphismus

$$\pi := \overline{\psi}\colon \mathbb{Z}[X]/\ker\psi \xrightarrow{\simeq} \mathbb{F}_2[X]/(P(X)).$$

Für die folgenden Rechnungen nennen wir $Q(X) := X^2 + X + 1 \in \mathbb{Z}[X]$, also $\overline{Q} = P$ in der Notation von oben. Damit erhalten wir

$$\begin{aligned}\ker\psi =& \psi_1^{-1}(\ker\psi_2) = \psi_1^{-1}((P)) \\ =& \{f \in \mathbb{Z}[X] | \psi_1(f) = \overline{f} \in (P)\} \\ =& \{f \in \mathbb{Z}[X] | \exists a \in \mathbb{F}_2[X]\colon \overline{f} = aP\} \\ \overset{\psi_1 \text{ surj.}}{=}& \{f \in \mathbb{Z}[X] | \exists a \in \mathbb{Z}[X]\colon \overline{f} = \overline{(aQ)}\} \\ =& \{f \in \mathbb{Z}[X] | \exists a \in \mathbb{Z}[X]\colon f - aQ \in \ker\psi_1\} \\ =& \{f \in \mathbb{Z}[X] | \exists a, b \in \mathbb{Z}[X]\colon f = b2 + aQ\} = (2, Q).\end{aligned}$$

Kürzere Variante mit Isomorphie- und Korrespondenzsatz: Sei

$$\pi\colon \mathbb{Z}[X] \to \mathbb{F}_2[X] = \mathbb{Z}[X]/(2)$$

die (oben ψ_1 genannte) kanonische Projektion (wir könnten natürlich ebensogut mit $\tilde{\pi}\colon \mathbb{Z}[X] \to \mathbb{Z}[X]/(X^2+X+1)$ beginnen). Ist dann $I \subset \mathbb{F}_2[X]$ ein Ideal (hier also $I = (P)$), dann existiert ein kanonischer Isomorphismus $\mathbb{Z}[X]/\pi^{-1}(I) \simeq \mathbb{F}_2[X]/I$. Wir müssen also nur noch zeigen, dass, mit $P = \overline{Q}$ wie oben, $\pi^{-1}(\overline{Q}) = (Q) + (2) = (Q, 2)$ gilt. Nach dem Korrespondenzsatz für Ideale ist aber $\pi(\bullet)$ eine Bijektion zwischen Idealen in $\mathbb{Z}[X]$, die (2) enthalten und Idealen in $\mathbb{F}_2[X]$, mit Umkehrabbildung $\pi^{-1}(\bullet)$. Aus $\pi((Q)+(2)) = (\pi(Q)) = (P)$ können wir also bereits $\pi^{-1}((P)) = (Q, 2)$ folgern. So haben wir wieder $R_2 = \mathbb{F}_2[X]/(X^2+X+1)$ gezeigt, d.h. R_2 ist ein Körper mit $|\mathbb{F}_2|^{\deg(P)} = 4$ Elementen.