Aufgabe H18T3A5 (12 Punkte)

(a) Sei $\mathbb{Z}$ der Ring der ganzen Zahlen. Zeigen Sie, dass der Ring $\mathbb{Z}[i]/(2)$ (wobei $i^2 = -1$) genau vier Elemente hat.

(b) Sei R ein kommutativer Ring mit 1. Sei weiter $t \in R$. Zeigen Sie, dass jedes Element im Quotientenring $R[x]/(tx-1)$ kongruent zu einem Element der Form ax^n modulo $tx-1$ ist, wobei $a \in R$ und $n \geq 1$ eine natürliche Zahl ist.

(c) Für einen kommutativen Ring R mit 1 wollen wir mit $\operatorname{Spec}(R)$ die Menge der Primideale von R bezeichnen. Sei $\phi : R \to S$ ein Ringhomomorphismus in einen weiteren kommutativen Ring mit 1. Geben Sie einen Beweis dafür an, dass

$$\phi^{-1} : \operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R) \quad , \quad \mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p})$$

eine wohldefinierte Abbildung ist.

Lösung:

zu (a) Wir zeigen, dass $S = \{0, 1, i, 1+i\}$ ein Repräsentantensystem von $\mathbb{Z}[i]/(2)$ ist. Daraus folgt dann $|\mathbb{Z}[i]/(2)| = |S| = 4$. Sei $\alpha \in \mathbb{Z}[i]$ vorgegeben, $\alpha = a + bi$ mit $a, b \in \mathbb{Z}$. Zu zeigen ist, dass die Nebenklasse $\alpha + (2)$ genau ein Element aus S enthält. Weil jede ganze Zahl entweder gerade oder ungerade ist, gibt es eindeutig bestimmte $c_0, d_0 \in \{0, 1\}$ mit $a \equiv c_0 \bmod 2$ und $b \equiv d_0 \bmod 2$. Für jedes Element $c + di \in S$ mit $c, d \in \{0, 1\}$ gilt nun die Äquivalenz

$$\begin{aligned} & c + di \in \alpha + (2) \quad \Leftrightarrow \quad c + di \in a + bi + (2) \quad \Leftrightarrow \quad \exists\, k, \ell \in \mathbb{Z} : c + di = a + bi + 2(k + \ell i) \\ \Leftrightarrow \quad & \exists\, k, \ell \in \mathbb{Z} : c + di = (a + 2k) + (b + 2\ell)i \quad \Leftrightarrow \quad \exists\, k, \ell \in \mathbb{Z} : (c = a + 2k) \ \wedge \ (d = b + 2\ell) \\ & \Leftrightarrow \quad (c \equiv a \bmod 2) \ \wedge \ (d \equiv b \bmod 2) \quad \Leftrightarrow \quad (c = c_0) \ \wedge \ (d = d_0). \end{aligned}$$

Damit ist gezeigt, dass $\alpha + (2)$ tatsächlich genau ein Element aus S enthält, nämlich das Element $c_0 + d_0 i$.

zu (b) Wir zeigen zunächst durch vollständige Induktion über $n \in \mathbb{N}_0$, dass im Faktorring $R[x]/(tx-1)$ jeweils die Gleichung $1 + (tx-1) = t^n x^n + (tx-1)$ gilt. Für $n = 0$ folgt dies direkt aus der Gleichung $t^0 x^0 = 1$. Sei nun $n \in \mathbb{N}_0$, und setzen wir die Gleichung $1 + (tx-1) = t^n x^n + (tx-1)$ voraus. Wegen $tx - 1 \in (tx-1)$ gilt $tx - 1 + (tx-1) = 0 + (tx-1)$ und damit $tx + (tx-1) = 1 + (tx-1)$. Es folgt

$$\begin{aligned} t^{n+1}x^{n+1} + (tx-1) \quad &= \quad tx \cdot t^n x^n + (tx-1) \quad = \quad (tx + (tx-1)) \cdot (t^n x^n + (tx-1)) \quad = \\ (1 + (tx-1))(t^n x^n + (tx-1)) \quad &= \quad t^n x^n + (tx-1) \quad = \quad 1 + (tx-1) \quad , \end{aligned}$$

wobei im letzten Schritt die Induktionsvoraussetzung angewendet wurde.

Sei nun $f + (tx-1)$ ein beliebiges Element in $R[x]/(tx-1)$, mit $f \in R[x]$. Dann gibt es ein $n \in \mathbb{N}$ und $a_0, ..., a_n \in R$ mit $f = \sum_{k=0}^{n} a_k x^k$. Wir erhalten

$$
\begin{aligned}
f + (tx-1) \quad &= \quad \sum_{k=0}^{n} a_k t^k + (tx-1) \quad = \quad \sum_{k=0}^{n} (a_k + (tx-1))(x^k + (tx-1)) \quad = \\
&\sum_{k=0}^{n} (a_k + (tx-1))(x^k + (tx-1))(1 + (tx-1)) \quad = \\
&\sum_{k=0}^{n} (a_k + (tx-1))(x^k + (tx-1))(t^{n-k}x^{n-k} + (tx-1)) \quad = \\
&\sum_{k=0}^{n} (a_k t^{n-k} x^n + (tx-1)) \quad = \quad \left(\sum_{k=0}^{n} a_k t^{n-k} \right) x^n + (tx-1).
\end{aligned}
$$

Setzen wir also $a = \sum_{k=0}^{n} a_k t^{n-k}$, dann ist die Gleichung $f + (tx-1) = ax^n + (tx-1)$ erfüllt. Es gilt also in $R[x]$ die Kongruenz $f \equiv ax^n \mod (tx-1)$.

zu (c) Sei $\mathfrak{p}$ ein Primideal in S. Zu zeigen ist, dass die Urbildmenge $\phi^{-1}(\mathfrak{p})$ unter dem Ringhomomorphismus ϕ ein Primideal in R ist. Zunächst bemerken wir, dass $1_R \notin \phi^{-1}(\mathfrak{p})$ gilt. Denn andernfalls wäre $1_S = \phi(1_R) \in \mathfrak{p}$, im Widerspruch zur Voraussetzung, dass $\mathfrak{p}$ in S ein Primideal ist. Seien nun $a, b \in R$ mit $ab \in \phi^{-1}(\mathfrak{p})$ vorgegeben. Zu zeigen ist, dass a oder b in $\phi^{-1}(\mathfrak{p})$ liegt. Aus $ab \in \phi^{-1}(\mathfrak{p})$ folgt $\phi(a)\phi(b) = \phi(ab) \in \mathfrak{p}$. Weil $\mathfrak{p}$ ein Primideal in S ist, gilt damit $\phi(a) \in \mathfrak{p}$ oder $\phi(b) \in \mathfrak{p}$. Daraus wiederum folgt $a \in \phi^{-1}(\mathfrak{p})$ oder $b \in \phi^{-1}(\mathfrak{p})$.