H18-T3-A5

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. Seit 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

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

eine wohldefinierte Abbildung ist.

Lösungsvorschlag. Zu a). Sei $R = \mathbb{Z}[i]/(2)$. Für $a + bi \in \mathbb{Z}[i]$ findet man $a', b' \in \{0, 1\}$, sodass $[a + bi] = [a' + b'i]$. Es ist also $R = \{[0], [1], [i], [1 + i]\}$. Um zu zeigen, dass diese vier Elemente paarweise verschieden sind, verwenden wir:

$$[x] = [y] \text{ für } [x], [y] \in R \Leftrightarrow x - y \in (2) \Leftrightarrow 2 \mid_{\mathbb{Z}[i]} (x - y)$$

Man rechnet leicht nach (z.B. mit Hilfe der Norm), dass 2 in $\mathbb{Z}[i]$ kein Teiler von $x - y$ für $x, y \in \{0, 1, i, 1 + i\}$ ist. Folglich hat R genau vier Elemente.
Zu b). Sei $f(X) = c_nX^n + \ldots + c_1X + c_0 \in R[X]$. In $R[X]/(tX - 1)$ gilt $[tX] = [1]$ und wir berechnen damit:

$$\begin{aligned}
[f(x)] &= [c_nX^n + c_{n-1}X^{n-1} \cdot 1 + \ldots + c_1X \cdot 1^{n-1} + c_0 \cdot 1^n] \\
&= [c_nX^n] + [c_{n-1}X^{n-1}] \cdot [1] + \ldots + [c_1X] \cdot [1]^{n-1} + c_0 \cdot [1]^n \\
&= [c_nX^n] + [c_{n-1}X^{n-1}] \cdot [tX] + \ldots + [c_1X] \cdot [tX]^{n-1} + c_0 \cdot [tX]^n \\
&= [c_nX^n + c_{n-1}tX^n + \ldots + c_1t^{n-1}X^n + t^nX^n] \\
&= [(c_n + c_{n-1}t + \ldots + c_1t^{n-1} + t^n)X^n]
\end{aligned}$$

Setze also $a := c_n + c_{n-1}t + \ldots + c_1t^{n-1} + t^n \in R$, dann ist $[f(x)] = [aX^n]$ wie gefordert.
Zu c). Für die Wohldefiniertheit ist lediglich zu zeigen, dass für ein Primideal $\mathfrak{p} \subset S$ das Urbild $\phi^{-1}(\mathfrak{p}) \subset R$ wieder ein Primideal ist.
$\phi^{-1}(\mathfrak{p})$ ist eine additive Untergruppe von R, denn $\mathfrak{p}$ ist eine additive Untergruppe von S und Urbilder von Gruppen unter Gruppenhomomorphismen sind bekanntlich Untergruppen (ϕ ist als Ringhomomorphismus insbesondere ein Gruppenhomomorphismus der additiven Gruppen) .
Für beliebige $r \in R$, $a \in \phi^{-1}(\mathfrak{p})$ ist $ra \in \phi^{-1}(\mathfrak{p})$ zu zeigen. Wegen $a \in \phi^{-1}(\mathfrak{p})$ ist $\phi(a) \in \mathfrak{p}$ und da $\mathfrak{p}$ ein Ideal ist, ist $\phi(r)\phi(a) \in \mathfrak{p}$, also $\phi(ra) \in \mathfrak{p}$ und damit $ra \in \phi^{-1}(\mathfrak{p})$.
Es bleibt nur noch die Primidealeigenschaft zu zeigen: sei $ab \in \phi^{-1}(\mathfrak{p})$, dann ist $\phi(ab) \in \mathfrak{p}$, bzw. $\phi(a)\phi(b) \in \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, ist $\phi(a) \in \mathfrak{p}$ oder $\phi(a) \in \mathfrak{p}$ und damit folgt sofort, dass $a \in \phi^{-1}(\mathfrak{p})$ oder $b \in \phi^{-1}(\mathfrak{p})$.