Aufgabe F18T3A4 (12 Punkte)

(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?

Lösung:

zu (a) Nach dem Eisenstein-Kriterium, angewendet auf die Primzahl $p = 2$, ist das Polynom $f = x^4 + 12x - 2$ in $\mathbb{Z}[x]$ irreduzibel (denn es gilt $2 \nmid 1$, $2 \mid 12$, $2 \mid (-2)$ und $4 \nmid (-2)$). Nach dem Gaußschen Lemma ist f damit auch in $\mathbb{Q}[x]$ irreduzibel. Weil $\mathbb{Q}[x]$ als Polynomring über einem Körper ein Hauptidealring ist, folgt aus der Irreduzibilität von f die Maximalität des Hauptideals (f). Daraus wiederum folgt, dass $R_1 = \mathbb{Q}[x]/(x^4 + 12x - 2)$ ein Körper ist. Jeder Körper ist ein Integritätsbereich.

zu (b) Sei $\bar{g} = x^2 + x + \bar{1}$ das Bild des Polynoms $g = x^2 + x + 1 \in \mathbb{Z}[x]$ in $\mathbb{F}_2[x]$. Wegen $\bar{g}(\bar{0}) = \bar{1} \neq \bar{0}$ und $\bar{g}(\bar{1}) = \bar{3} = \bar{1} \neq \bar{0}$ besitzt das Polynom $\bar{g}$ in $\mathbb{F}_2$ keine Nullstelle, ist wegen $\text{grad}(\bar{g}) \leq 2$ also in $\mathbb{F}_2[x]$ irreduzibel. Weil $\mathbb{F}_2$ ein Körper ist, folgt daraus wie in Teil (a), dass es sich beim Faktorring $\bar{R} = \mathbb{F}_2[x]/(\bar{g})$ ebenfalls um einen Körper handelt. Wir zeigen nun, dass R_2 ein Körper ist, indem wir mit dem Homomorphiesatz für Ringe einen Isomorphismus

$$R_2 = \mathbb{Z}[x]/(2, g) \quad \cong \quad \mathbb{F}_2[x]/(\bar{g})$$

von Ringen konstruieren. Dazu betrachten wir die Abbildung $\phi : \mathbb{Z}[x] \to \mathbb{F}_2[x]/(\bar{g})$, $h \mapsto \bar{h} + (\bar{g})$, wobei $\bar{h}$ jeweils das Bild von h in $\mathbb{F}_2[x]$ bezeichnet. Diese Abbildung ist ein Homomorphismus von Ringen. Um dies zu sehen, bemerken wir zunächst, dass ϕ als Komposition von $\mathbb{Z}[x] \to \mathbb{F}_2[x]$, $h \mapsto \bar{h}$ mit dem kanonischen Epimorphismus zu Stande kommt. Es genügt also zu zeigen, dass $h \mapsto \bar{h}$ ein Ringhomomorphismus ist. Nun ist die Reduktionsabbildung $\mathbb{Z} \to \mathbb{F}_2$, $a \mapsto a + 2\mathbb{Z}$ bekanntlich ein Ringhomomorphismus, somit auch die Kompostion $\mathbb{Z} \to \mathbb{F}_2[x]$ der Reduktionsabbildung mit der Inklusionsabbildung $\mathbb{F}_2 \to \mathbb{F}_2[x]$. Die Abbildung $\mathbb{Z}[x] \to \mathbb{F}_2[x]$, $h \mapsto \bar{h}$ ist nun der (auf Grund der universellen Eigenschaft des Polynomrings) eindeutig bestimmte Ringhomomorphismus, der den Homomorphismus $\mathbb{Z} \to \mathbb{F}_2[x]$ auf $\mathbb{Z}[x]$ fortsetzt und x auf x abbildet. (Wahrscheinlich würde es auch akzeptiert, wenn man die Homomorphismus-Eigenschaft von $\mathbb{Z}[x] \to \mathbb{F}_2[x]$, $h \mapsto \bar{h}$ einfach als bekannt voraussetzt. Natürlich kann man die Eigenschaft auch direkt Nachrechnen, was aber bei der Multiplikation etwas aufwändig ist.)

Um den Homomorphiesatz anwenden zu können, müssen wir noch zeigen, dass ϕ surjektiv ist und $\ker(\phi) = (2, g)$ gilt. Zum Nachweis der Surjektivität sei $\bar{h} + (\bar{g}) \in \bar{R}$ vorgegeben, mit $\bar{h} = \sum_{k=0}^{n} \bar{a}_k x^k \in \mathbb{F}_2[x]$ und $n \in \mathbb{N}_0$, $\bar{a}_0, ..., \bar{a}_n \in \mathbb{F}_2$. Für jeden Koeffizieten $\bar{a}_k \in \mathbb{F}_2$ können wir ein Urbild $a_k \in \mathbb{Z}$ wählen. Setzen wir $h = \sum_{k=0}^{n} a_k x^k$, dann ist $h \in \mathbb{Z}[x]$ offenbar ein Element mit $\phi(h) = \bar{h} + (\bar{g})$. Damit ist die Surjektivität nachgewiesen.

Wegen $\phi(2) = \bar{2} + (\bar{g}) = \bar{0} + (\bar{g}) = 0_{\bar{R}}$ und $\phi(g) = \bar{g} + (\bar{g}) = \bar{0} + (\bar{g}) = 0_{\bar{R}}$ gilt $2, g \in \ker(\phi)$ und somit $(2, g) \subseteq \ker(\phi)$, da $\ker(\phi)$ ein Ideal des Rings $\mathbb{Z}[x]$ ist. Zum Nachweis von $\ker(\phi) \subseteq (2, g)$ sei $h \in \ker(\phi)$ vorgegeben. Wegen $\bar{h} + (\bar{g}) = \phi(h) = 0_{\bar{R}} = \bar{0} + (\bar{g})$ gilt $\bar{h} \in (\bar{g})$. Es gibt also ein Polynom $\bar{u} \in \mathbb{F}_2[x]$ mit $\bar{h} = \bar{u}\bar{g}$. Sei $u \in \mathbb{Z}[x]$ ein Urbild von $\bar{u}$. Wegen $\bar{h} - \bar{u}\bar{g} = \bar{0}$ sind sämtliche Koeffizienten von $h - ug$ modulo 2 gleich Null. Daraus folgt, dass ein $v \in \mathbb{Z}[x]$ mit $h - ug = 2v$ existiert. Daraus wiederum folgt $h = 2v + ug \in (2, g)$, und der Nachweis von $\ker(\phi) = (2, g)$ ist abgeschlossen. Der Homomorphiesatz von Ringen liefert nun den gewünschten Isomorphismus und damit die Körpereigenschaft des Rings $R_2 = \mathbb{Z}[x]/(2, g)$.

Auf Grund des Isomorphismus gilt auch $|R_2| = |\bar{R}|$; es genügt also, die Mächtigkeit von $\bar{R} = \mathbb{F}_2[x]/(\bar{g})$ zu bestimmen. Dazu weisen wir nach, dass $S = \{\bar{a}x + \bar{b} \mid \bar{a}, \bar{b} \in \mathbb{F}_2\}$ ein Repräsentantensystem von $\bar{R}$ gegeben ist. Zu zeigen ist, dass jede Nebenklasse $\bar{h} + (\bar{g})$ von $\bar{R}$ mit $\bar{h} \in \mathbb{F}_2[x]$ genau ein Element aus S enthält. Für vorgegebenes $\bar{h}$ erhalten wir durch Division mit Rest Polynome $\bar{q}, \bar{r} \in \mathbb{F}_2[x]$ mit $\bar{h} = \bar{q}\bar{g} + \bar{r}$, wobei $\bar{r} = 0$ oder $\text{grad}(\bar{r}) < \text{grad}(\bar{g}) = 2$ gilt. Dies zeigt, dass $\bar{r}$ in S enthalten ist. Außerdem gilt $\bar{h} + (\bar{g}) = \bar{q}\bar{g} + \bar{r} + (\bar{g}) = \bar{r} + (\bar{g})$ und somit $\bar{r} \in \bar{h} + (\bar{g})$. Nehmen wir an, dass $\bar{r}_1$ ein weiteres Element in $\bar{h} + (\bar{g})$ ist. Aus $\bar{r}_1 + (\bar{g}) = \bar{r} + (\bar{g})$ folgt dann $\bar{r}_1 - \bar{r} \in (\bar{g})$, also ist $\bar{g}$ ein Teiler von $\bar{r}_1 - \bar{r}$. Wegen $\bar{r}, \bar{r}_1 \in S$ gilt entweder $\bar{r}_1 - \bar{r} = \bar{0}$ oder $\text{grad}(\bar{r}_1 - \bar{r}) < 2$; letzteres ist aber wegen $\bar{g} \mid (\bar{r}_1 - \bar{r})$ ausgeschlossen. Also gilt $\bar{r} = \bar{r}_1$, was zeigt, dass $\bar{h} + (\bar{g})$ nur ein Element aus S enthält.

Es gilt $|S| = 2 \cdot 2 = 4$, denn jedes Element in S hat die Form $\bar{a}x + \bar{b}$ mit $\bar{a}, \bar{b} \in \mathbb{F}_2$, und für $\bar{a}$ und $\bar{b}$ gibt es jeweils zwei Möglichkeiten. Weil S ein Repräsentantensystem von $\bar{R}$ ist, folgt $|\bar{R}| = |S| = 4$.