Aufgabe F19T3A4 (12 Punkte)

Sei $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$ der Körper mit elf Elementen.

(a) Zeigen Sie, dass die Restklassenringe $\mathbb{F}_{11}[x]/(x^2+\bar{1})$ und $\mathbb{F}_{11}[x]/(x^2+x+\bar{4})$ jeweils einen Körper (mit 121 Elementen) definieren.

(b) Bestimmen Sie konkret einen Isomorphismus

$$\mathbb{F}_{11}[x]/(x^2+\bar{1}) \to \mathbb{F}_{11}[x]/(x^2+x+\bar{4})$$

durch Angabe des Bildes von $x + (x^2+\bar{1})$.

Lösung:

zu (a) Die Polynome $f = x^2+\bar{1}$ bzw. $g = x^2+x+\bar{4}$ besitzen beide in $\mathbb{F}_{11}$ keine Nullstelle, denn es gilt

$$f(\bar{0}) = \bar{1} \neq \bar{0},\ f(\bar{1}) = \bar{2} \neq \bar{0},\ f(\bar{2}) = \bar{5} \neq \bar{0},\ f(\bar{3}) = \overline{10} \neq \bar{0},\ f(\bar{4}) = \overline{17} = \bar{6} \neq \bar{0},\ f(\bar{5}) = \overline{26} = \bar{3} \neq \bar{0},$$
$$f(\bar{6}) = f(-\bar{5}) = \overline{26} = \bar{3} \neq \bar{0},\ f(\bar{7}) = f(-\bar{4}) = \overline{17} = \bar{6} \neq \bar{0},\ f(\bar{8}) = f(-\bar{3}) = \overline{10} \neq \bar{0},$$
$$f(\bar{9}) = f(-\bar{2}) = \bar{5} \neq \bar{0},\ f(\overline{10}) = f(-\bar{1}) = \bar{2} \neq \bar{0}$$

und

$$g(\bar{0}) = \bar{4} \neq \bar{0},\ g(\bar{1}) = \bar{6} \neq \bar{0},\ g(\bar{2}) = \overline{10} \neq \bar{0},\ g(\bar{3}) = \overline{16} = \bar{5} \neq \bar{0},\ g(\bar{4}) = \overline{24} = \bar{2} \neq \bar{0},\ g(\bar{5}) = \overline{34} = \bar{1} \neq \bar{0},$$
$$g(\bar{6}) = g(-\bar{5}) = \overline{24} = \bar{2} \neq \bar{0},\ g(\bar{7}) = g(-\bar{4}) = \overline{16} = \bar{5} \neq \bar{0},\ g(\bar{8}) = g(-\bar{3}) = \overline{10} \neq \bar{0},$$
$$g(\bar{9}) = g(-\bar{2}) = \bar{6} \neq \bar{0},\ g(\overline{10}) = g(-\bar{1}) = \bar{4} \neq \bar{0}.$$

Wegen $\operatorname{grad}(f) = \operatorname{grad}(g) = 2$ folgt daraus die Irreduzibilität von f und g in $\mathbb{F}_{11}[x]$. Weil $\mathbb{F}_{11}[x]$ als Polynomring über einem Körper ein Hauptidealring ist, folgt daraus, dass (f) und (g) in $\mathbb{F}_{11}[x]$ maximale Ideale sind. Daraus wiederum folgt, dass die Faktorringe $\mathbb{F}_{11}[x]/(f)$ und $\mathbb{F}_{11}[x]/(g)$ Körper sind.

Laut Vorlesung gilt allgemein: Ist K ein Körper und $h \in K[x]$ ein nicht-konstantes Polynom vom Grad $n \in \mathbb{N}$, dann bilden die Polynome vom Grad $< n$ einschließlich des Nullpolynoms ein Repräsentantensystem R von $K[x]/(h)$. (Dies war eine unmittelbare Folgerung aus der Tatsache, dass $K[x]$ ein euklidischer Ring ist und somit jedes Polynom mit Rest durch h geteilt werden kann, wobei jeweils entweder das Nullpolynom oder ein Polynom vom Grad $< n$ übrigbleibt.)

Jedes solche Polynom ist durch seine n Koeffizienten auf eindeutige Weise festgelegt. Ist K zudem endlich, $q = |K|$, dann gibt es für jeden Koeffizienten q Möglichkeiten. Daraus folgt dann $|K[x]/(h)| = |R| = q^n$. Wenden wir dies auf den Körper $\mathbb{F}_{11}$ und die Polynome f und g an, so erhalten wir wegen $\operatorname{grad}(f) = \operatorname{grad}(g) = 2$ die Elementezahl $|\mathbb{F}_{11}[x]/(f)| = 11^2 = 121$ und ebenso $|\mathbb{F}_{11}[x]/(g)| = 11^2 = 121$.

zu (b) Nehmen wir an, $\bar{\phi} : \mathbb{F}_{11}[x]/(f) \to \mathbb{F}_{11}[x]/(g)$ ist ein Isomorphismus. Weil die Polynome der Form $ax+b$ mit $a, b \in \mathbb{F}_{11}$ ein Repräsentantensystem von $\mathbb{F}_{11}[x]/(g)$ bilden (siehe Teil (a)), gibt es insbesondere $a, b \in \mathbb{F}_{11}$ mit $\bar{\phi}(x + (f)) = ax + b + (g)$. Definieren wir nun die Ring R, S durch $R = \mathbb{F}_{11}[x]/(f)$ und $S = \mathbb{F}_{11}[x]/(g)$, so gilt die Äquivalenz

$$\bar{\phi}(0_R) = 0_S \quad \Leftrightarrow \quad \bar{\phi}(\bar{0} + (f)) = \bar{0} + (g) \quad \Leftrightarrow \quad \bar{\phi}(x^2 + \bar{1} + (f)) = (g) \quad \Leftrightarrow$$

$$\bar{\phi}(x + (f))^2 + \bar{\phi}(\bar{1} + (f)) = (g) \quad \Leftrightarrow \quad (ax + b + (g))^2 + (\bar{1} + (g)) = (g) \quad \Leftrightarrow$$

$$(ax + b)^2 + \bar{1} + (g) = (g) \quad \Leftrightarrow \quad a^2x^2 + \bar{2}abx + b^2 + \bar{1} + (g) = (g) \quad \Leftrightarrow$$

$$a^2(-x - \bar{4}) + \bar{2}abx + b^2 + \bar{1} + (g) = (g) \quad \Leftrightarrow$$

$$(-a^2 + \bar{2}ab)x + (-\bar{4}a^2 + b^2 + \bar{1}) + (g) = \bar{0} \cdot x + \bar{0} + (g) \quad \Leftrightarrow$$

$$a(-a + \bar{2}b) = \bar{0} \text{ und } -\bar{4}a^2 + b^2 + \bar{1} = \bar{0}$$

wobei im fünften Schritt verwendet wurde, dass aus $x^2 + x + \bar{4} + (g) = (g)$ im Faktorring die Gleichung $x^2 + (g) = -x - \bar{4} + (g)$ folgt. Im letzten Schritt wurde verwendet, dass die Polynome der Form $ax + b$ mit $a, b \in \mathbb{F}_{11}$ ein Repräsentantensystem von $\mathbb{F}_{11}[x]/(g)$ bilden und somit jedes Elemente in $\mathbb{F}_{11}[x]/(g)$ eine *eindeutige* Darstellung der Form $ax + b + (g)$ besitzt.

Setzen wir $a = \bar{2}b$, dann wird die Gleichung $-\bar{4}a^2 + b^2 + \bar{1} = \bar{0}$ zu $-\bar{4}(\bar{2}b)^2 + b^2 + \bar{1} = \bar{0} \Leftrightarrow -\overline{16}b^2 + b^2 + \bar{1} = \bar{0} \Leftrightarrow \bar{4}b^2 = \bar{1}$, und dies ist wegen $\bar{4}^{-1} = \bar{3}$ äquivalent zu $b^2 = \bar{3}$. Diese Gleichung wiederum wird durch $\bar{b} = 5$ gelöst. Also ist $(\bar{a}, \bar{b}) = (\overline{10}, \bar{5})$ eine Lösung des Gleichungssystems $a(-a+\bar{2}b) = \bar{0}, -\bar{4}a^2+b^2+\bar{1} = \bar{0}$. Auf Grund der obigen Äquivalenz ist durch $\phi(x) = \overline{10}x + \bar{5} + (g)$ also ein Homomorphismus $\phi : \mathbb{F}_5[x] \to \mathbb{F}_5[x]/(g)$ mit $\phi(x^2 + \bar{1}) = (g)$ definiert.

Wir zeigen nun mit dem Homomorphiesatz, dass ϕ tatsächlich einen Isomorphismus $\bar{\phi} : \mathbb{F}_{11}[x]/(f) \to \mathbb{F}_{11}[x]/(g)$ induziert. Weil $\mathbb{F}_{11}[x]$ ein Hauptidealring und $\ker(\phi)$ ein Ideal in $\mathbb{F}_{11}[x]$ ist, gibt es ein normiertes Polynom $h \in \mathbb{F}_{11}[x]$ mit $\ker(\phi) = (h)$. Wegen $x^2 + \bar{1} \in \ker(\phi)$ gilt $x^2 + \bar{1} \in (h)$, also ist h ein Teiler von $x^2 + \bar{1}$. Weil $x^2 + \bar{1}$ irreduzibel ist, muss $h = x^2 + \bar{1}$ gelten oder h eine Einheit sein. Im Fall $h \in \mathbb{F}_{11}[x]^\times$ wäre aber $\ker(\phi) = (h) = \mathbb{F}_{11}[x]$ und insbesondere $\bar{1} \in \ker(\phi)$. Aber das ist nicht der Fall, denn wegen $\bar{1} \notin (g)$ ist $\phi(\bar{1}) = \bar{1} + (g) \neq (g)$. Also bleibt $\ker(\phi) = (x^2 + \bar{1})$ als einzige Möglichkeit.

Der Homomorphiesatz induziert damit einen Isomorphismus $\bar{\phi}$ von $\mathbb{F}_{11}[x]/(f)$ auf den Teilring $\mathrm{im}(\phi)$ von $\mathbb{F}_{11}[x]/(g)$. Weil die Ringe $\mathbb{F}_{11}[x]/(f)$ und $\mathbb{F}_{11}[x]/(g)$ aber beide 121 Elemente haben, muss $\mathrm{im}(\phi)$ mit $\mathbb{F}_{11}[x]/(g)$ übereinstimmen. Also ist $\bar{\phi}$ ein Isomorphismus zwischen $\mathbb{F}_{11}[x]/(f)$ und $\mathbb{F}_{11}[x]/(g)$, und nach Definition des induzierten Isomorphismus gilt

$$\bar{\phi}(x + (f)) \quad = \quad \phi(x) \quad = \quad \overline{10}x + \bar{5} + (g).$$