**Aufgabe F14T3A2** (2+5+5+3 Punkte)

Gegeben sei ein Element $c$ aus einem kommutativen Ring $R$. Für $a, b \in R$ definieren wir $a \equiv b \bmod c$ genau dann, wenn es ein $d \in R$ gibt mit $a - b = c \cdot d$.

(a) Zeigen Sie, dass dies eine Äquivalenzrelation auf $R$ definiert.

(b) Es sei nun $R = \mathbb{Z}$. Finden Sie alle Lösungen $y \in \mathbb{Z}$ der Kongruenz

$$51y \equiv 34 \bmod 85.$$

(c) Es sei nun $R = \mathbb{Q}[x]$. Finden Sie alle Lösungen $f \in \mathbb{Q}[x]$ der simultanen Kongruenzen

$$f \equiv 1 \bmod (x^2+1) \qquad \text{und} \qquad f \equiv x \bmod (x^2-1).$$

(d) Es sei wieder $R = \mathbb{Z}$. Ist die Kongruenz $y^2 + 97y \equiv 3 \bmod 101$ lösbar für $y \in \mathbb{Z}$?

*Lösung:*

zu (a) Nach Definition ist eine Relation auf der Menge $R$ genau dann eine Äquivalenzrelation, wenn sie reflexiv, symmetrisch und transitiv ist. Sei $c \in R$ vorgegeben. Wir rechnen die drei Eigenschaften für die Kongruenz modulo $c$ nach.

*Reflexivität:* Für jedes $a \in R$ gilt $a - a = 0 = c \cdot 0$, also ist $a \equiv a \bmod c$.

*Symmetrie:* Seien $a, b \in R$ mit $a \equiv b \bmod c$ vorgegeben. Dann gibt es ein $d \in R$ mit $a - b = c \cdot d$. Es folgt $b - a = c(-d)$. Also gilt $b \equiv a \bmod c$.

*Transitivität:* Seien $a, b, b_1 \in R$ mit $a \equiv b \bmod c$ und $b \equiv b_1 \bmod c$. Dann gibt es Elemente $d, d_1 \in R$ mit $a - b = c \cdot d$ und $b - b_1 = c \cdot d_1$. Es folgt $a - b_1 = (a - b) + (b - b_1) = c \cdot d + c \cdot d_1 = c \cdot (d + d_1)$ und somit $a \equiv b_1 \bmod c$.

zu (b) Für jedes $y \in \mathbb{Z}$ ist $51y \equiv 34 \bmod 85$ äquivalent dazu, dass ein $d \in \mathbb{Z}$ mit $51y - 34 = 85d$ existiert. Dies wiederum ist äquivalent zu $3y - 2 = 5d$ für ein $d \in \mathbb{Z}$, also zu $3y \equiv 2 \bmod 5$. Weil $\bar{2}$ in $\mathbb{Z}/5\mathbb{Z}$ invertierbar ist, ist die Multiplikation der Kongruenz mit der Zahl 2 eine Äquivalenzumformung. Wir erhalten damit $3y \equiv 2 \bmod 5 \Leftrightarrow 6y \equiv 4 \bmod 5 \Leftrightarrow y \equiv 4 \bmod 5$. Die Lösungsmenge $\mathcal{L}$ der ursprünglichen Kongruenz besteht also aus alle $y \in \mathbb{Z}$, die kongruent zu 4 modulo 5 sind, es gilt also $\mathcal{L} = 4 + 5\mathbb{Z}$.

zu (c) Als erstes bemerken wir, dass die Polynome $x^2 + 1$ und $x^2 - 1$ teilerfremd sind. Denn das Polynom $x^2 + 1$ besitzt in $\mathbb{R}$ und somit erst recht in $\mathbb{Q}$ keine Nullstellen und ist somit irreduzibel, und die beiden normierten, irreduziblen Faktoren $x \pm 1$ von $x^2 - 1$ stimmen beide nicht mit $x^2 - 1$ überein. Zunächst bestimmen wir lediglich eine Lösung des angegebenen Kongruenzsystems. Der ersten Schritt besteht darin, Polynome $g, h \in \mathbb{Q}[x]$ mit $g \cdot (x^2+1) + h \cdot (x^2-1) = \mathrm{ggT}(x^2+1, x^2-1) = 1$ zu bestimmen. Dies kann mit dem Euklidischen Algorithmus erledigt werden, hier allerdings sieht man schnell, dass

$$\tfrac{1}{2}(x^2+1) + (-\tfrac{1}{2})(x^2-1) \quad = \quad 1$$

gilt und somit $g = \frac{1}{2}$ und $h = -\frac{1}{2}$ Polynome mit der gewünschten Eigenschaft sind.

Durch Umstellen dieser Gleichung erhält man

$$(-\tfrac{1}{2})(x^2-1) \quad = \quad 1 + (-\tfrac{1}{2})(x^2+1).$$

Sie zeigt, dass das Polynom $u = (-\frac{1}{2})(x^2-1)$ die Kongruenzen $u \equiv 1 \bmod (x^2+1)$ und $v \equiv 0 \bmod (x^2-1)$ erfüllt. Ebenso zeigt die umgestellte Gleichung $\frac{1}{2}(x^2+1) = 1 + \frac{1}{2}(x^2-1)$, dass $v = \frac{1}{2}(x^2+1)$ eine Lösung des Systems $v \equiv 0 \bmod (x^2+1)$ und $v \equiv 1 \bmod (x^2-1)$ liefert. Setzen wir nun $w = 1 \cdot u + x \cdot v = \frac{1}{2}x^3 - \frac{1}{2}x^2 + \frac{1}{2}x + \frac{1}{2}$, dann erhalten wir eine Lösung des Systems $w \equiv 1 \bmod (x^2+1)$ und $w \equiv x \bmod (x^2-1)$.

Nun zeigen wir, dass die Lösungsmenge $\mathcal{L}$ des Kongruenzsystems durch $\mathcal{L} = w + (x^2-1)(x^2+1)\mathbb{Q}[x] = w + (x^4-1)$ gegeben ist. Ist $f$ ein Element der Menge rechts, dann gibt es ein $g \in \mathbb{Q}[x]$ mit $f = w + g \cdot (x^4-1)$. Es folgt $f \equiv w \equiv 1 \bmod (x^2+1)$ und $f \equiv w \equiv x \bmod (x^2-1)$, also $f \in \mathcal{L}$. Setzen wir nun umgekehrt $f \in \mathcal{L}$ voraus. Dann gilt $f \equiv 1 \bmod (x^2+1)$ und $f \equiv x \bmod (x^2-1)$. Weil $x^2+1$ und $x^2-1$ teilerfremd sind, ist der Ringhomomorphismus

$$\phi : \mathbb{Q}[x]/(x^4-1) \longrightarrow \mathbb{Q}[x]/(x^2+1) \times \mathbb{Q}[x]/(x^2-1)$$

gegeben durch

$$g + (x^4-1) \mapsto (g + (x^2+1), g + (x^2-1))$$

nach dem Chinesischen Restsatz wohldefiniert und injektiv. Weil die Elemente $f + (x^4-1)$ und $w + (x^4-1)$ beides Urbild von $(1 + (x^2+1), x + (x^2-1))$ sind, muss $f + (x^4-1) = w + (x^4-1)$ gelten. Somit ist $f - w$ ein Vielfaches von $x^4-1$, es gilt also $f \in w + (x^4-1)\mathbb{Q}[x]$.

zu (d) Die Zahl 101 ist eine Primzahl. Somit ist die Kongruenz $y^2 + 97y \equiv 3 \bmod 101$ ist genau dann lösbar, wenn die Gleichung $y^2 + \overline{97}y = \bar{3}$ im Körper $\mathbb{F}_{101}$ eine Lösung besitzt. Nun gilt für alle $y \in \mathbb{F}_{101}$ die Äquivalenz

$$y^2 + \overline{97}y = \bar{3} \quad \Leftrightarrow \quad y^2 - \bar{4}y = \bar{3} \quad \Leftrightarrow \quad y^2 - \bar{4}y = \bar{3} \quad \Leftrightarrow \quad y^2 - \bar{4}y + \bar{4} = \bar{7} \quad \Leftrightarrow \quad (y - \bar{2})^2 = \bar{7}.$$

Die Umformung zeigt, dass die Ursprungsgleichung über $\mathbb{F}_{101}$ genau dann lösbar ist, wenn $\bar{7}$ in $\mathbb{F}_{101}$ ein Quadrat, die Zahl 7 also modulo 101 ein quadratischer Rest ist. Ob dies der Fall ist, lässt sich durch Berechnung des Legendre-Symbols mit Hilfe des Quadratischen Reziprozitätsgesetzes herausfinden. Es gilt

$$\left(\frac{7}{101}\right) \quad = \quad \left(\frac{101}{7}\right) \quad = \quad \left(\frac{3}{7}\right) \quad = \quad -\left(\frac{7}{3}\right) \quad = \quad -\left(\frac{1}{3}\right) \quad = \quad -1.$$

Das Legendre-Symbol zeigt an, dass 7 *kein* quadratischer Rest modulo 101 ist. Also ist besitzt die angegebene Kongruenz keine Lösung in $\mathbb{Z}$.