Andreas Gathmann und Max Mayer Sommersemester 2023

Algebraische Strukturen – Blatt 7

Lösungshinweise

(1) Bestimme alle $x \in \mathbb{Z}$, für die die folgenden Gleichungssysteme erfüllt sind:

(a) $\begin{aligned} x &= 2 \mod 4 \\ x &= 6 \mod 7 \\ x &= 3 \mod 9 \end{aligned}$ (b) $\begin{aligned} x &= 5 \mod 6 \\ 3x &= -1 \mod 14 \end{aligned}$ (c) $x = 1 \mod n$ für alle $n = 2, \dots, 10$

Lösung: (a) Wir verwenden die Bezeichnungen aus Satz 11.22. Für die Zahlen $n_1 = 4$, $n_2 = 7$, $n_3 = 9$ ist $N = n_1 n_2 n_3 = 252$ und $N_1 = \frac{N}{n_1} = 63$, $N_2 = \frac{N}{n_2} = 36$, $N_3 = \frac{N}{n_3} = 28$. Man sieht schnell die Inversen von N_i in $\mathbb{Z}_{n_i}$ für $i = 1, 2, 3$:

$$\begin{aligned} \overline{N_1}^{-1} = \overline{63}^{-1} = \overline{3}^{-1} = \overline{3} \quad &\in \mathbb{Z}_4 \quad \Rightarrow \text{wir setzen } M_1 = 3, \\ \overline{N_2}^{-1} = \overline{36}^{-1} = \overline{1}^{-1} = \overline{1} \quad &\in \mathbb{Z}_7 \quad \Rightarrow \text{wir setzen } M_2 = 1, \\ \overline{N_3}^{-1} = \overline{28}^{-1} = \overline{1}^{-1} = \overline{1} \quad &\in \mathbb{Z}_9 \quad \Rightarrow \text{wir setzen } M_3 = 1. \end{aligned}$$

Eine Lösung des Gleichungssystems ist damit

$$a = 2M_1N_1 + 6M_2N_2 + 3M_3N_3 = 2 \cdot 3 \cdot 63 + 6 \cdot 1 \cdot 36 + 3 \cdot 1 \cdot 28 = 678.$$

Damit sind alle Lösungen die Zahlen $x \in \mathbb{Z}$ mit $\overline{x} = \overline{678} = \overline{174} \in \mathbb{Z}_{252}$, d. h. die Lösungsmenge ist $174 + 252\mathbb{Z}$.

(b) Zunächst ist $\overline{3}$ in $\mathbb{Z}_{14}$ invertierbar mit Inversem $\overline{3}^{-1} = \overline{5}$, und damit ist das gegebene Gleichungssystem äquivalent zu

$$x = 5 \mod 6 \quad \text{und} \quad x = -5 \mod 14.$$

Dies können wir nach dem chinesischen Restsatz äquivalent aufteilen in

$$x = 5 \mod 2 \quad \text{und} \quad x = 5 \mod 3 \quad \text{und} \quad x = -5 \mod 2 \quad \text{und} \quad x = -5 \mod 7,$$

also

$$x = 1 \mod 2 \quad \text{und} \quad x = 2 \mod 3 \quad \text{und} \quad x = 2 \mod 7.$$

Wir rechnen nun wieder wie in Satz 11.22: Für $n_1 = 2$, $n_2 = 3$, $n_3 = 7$ ist $N = n_1 n_2 n_3 = 42$ und $N_1 = \frac{N}{n_1} = 21$, $N_2 = \frac{N}{n_2} = 14$, $N_3 = \frac{N}{n_3} = 6$. Die zugehörigen Inversen sind

$$\begin{aligned} \overline{N_1}^{-1} = \overline{21}^{-1} = \overline{1}^{-1} = \overline{1} \quad &\in \mathbb{Z}_2 \quad \Rightarrow \text{wir setzen } M_1 = 1, \\ \overline{N_2}^{-1} = \overline{14}^{-1} = \overline{2}^{-1} = \overline{2} \quad &\in \mathbb{Z}_3 \quad \Rightarrow \text{wir setzen } M_2 = 2, \\ \overline{N_3}^{-1} = \overline{6}^{-1} = \overline{6}^{-1} = \overline{6} \quad &\in \mathbb{Z}_7 \quad \Rightarrow \text{wir setzen } M_3 = 6. \end{aligned}$$

Damit ist eine Lösung des Gleichungssystems die Zahl

$$a = 1M_1N_1 + 2M_2N_2 + 2M_3N_3 = 21 + 56 + 72 = 149,$$

und die gesamte Lösungsmenge ist $149 + 42\mathbb{Z} = 23 + 42\mathbb{Z}$.

(c) Das Gleichungssystem ist äquivalent zu der Bedingung, dass $x - 1$ ein Vielfaches von n ist für alle $n = 2, \dots, 10$. Dies bedeutet genau, dass $x - 1$ ein Vielfaches des kleinsten gemeinsamen Vielfachen von $2, \dots, 10$, also von $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$ ist, d. h. die Lösungsmenge ist $1 + 2520\mathbb{Z}$.

(2) Man beweise oder widerlege:

(a) $\mathbb{Z}_{25}^* \cong \mathbb{Z}_5^* \times \mathbb{Z}_5^*$;

(b) $\mathbb{Z}_{15}^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Lösung: (a) Wegen $\mathbb{Z}_{25}^* = \{\overline{k} : \text{ggt}(k,25) = 1\}$ hat

$$\mathbb{Z}_{25}^* = \mathbb{Z}_{25} \backslash \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}\}$$

Ordnung 20. Da $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ Ordnung 4 hat und damit $|\mathbb{Z}_5^* \times \mathbb{Z}_5^*| = 16$ gilt, können die beiden Gruppen also nicht isomorph sein.

(b) Wir behaupten, dass die beiden Gruppen isomorph sind.

Nach dem chinesischen Restsatz gilt $\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*$, wobei die Verknüpfung jeweils die Multiplikation ist. Es genügt also, die Isomorphismen $(\mathbb{Z}_3^*, \cdot) \cong (\mathbb{Z}_2, +)$ und $(\mathbb{Z}_5^*, \cdot) \cong (\mathbb{Z}_4, +)$ zu zeigen. Da weiterhin nach Satz 6.20 jede zyklische Gruppe der Ordnung n isomorph zu $\mathbb{Z}_n$ ist, reicht es damit zu zeigen, dass $\mathbb{Z}_3^*$ und $\mathbb{Z}_5^*$ zyklisch der Ordnung 2 bzw. 4 sind. Dies folgt aber aus

$$\mathbb{Z}_3^* = \{\overline{1}, \overline{2}\} = \left\{\overline{2}^0, \overline{2}^1\right\} \quad \text{und} \quad \mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \left\{\overline{2}^0, \overline{2}^1, \overline{2}^2, \overline{2}^3\right\}.$$

(3) Bestimme die Primfaktorzerlegungen des Polynoms $f = t^3 - t^2 - 2t + 2 \in K[t]$ über den Körpern $K = \mathbb{Q}, \mathbb{R}, \mathbb{Z}_3, \mathbb{Q}[u]/\langle u^2 - 2 \rangle$.

Lösung: Über jedem Körper ist 1 eine Nullstelle von f, und damit zunächst $f = (t-1)(t^2-2)$. Hat nun t^2-2 keine Nullstelle, so kann kein weiterer Linearfaktor mehr abgespalten werden, und $(t-1)(t^2-2)$ ist die Primfaktorzerlegung von f. Hat f dagegen eine Nullstelle $a \in K$, so ist auch $-a$ eine Nullstelle, und wir erhalten die Primfaktorzerlegung $(t-1)(t-a)(t+a)$. Damit gilt:

- Für $K = \mathbb{Q}$ hat t^2-2 keine Nullstelle, die Primfaktorzerlegung ist also $f = (t-1)(t^2-2)$.
- Für $K = \mathbb{R}$ ist die Primfaktorzerlegung $f = (t-1)(t-\sqrt{2})(t+\sqrt{2})$.
- Wegen $\overline{0}^2 - \overline{2} = \overline{1}$, $\overline{1}^2 - \overline{2} = \overline{2}$ und $\overline{2}^2 - \overline{2} = \overline{2}$ hat $t^2 - \overline{2}$ keine Nullstellen in $\mathbb{Z}_3$, und die gesuchte Primfaktorzerlegung ist $f = (t-\overline{1})(t^2-\overline{2})$.
- In $K = \mathbb{Q}[u]/\langle u^2-2\rangle$ gilt natürlich $\overline{u}^2 - \overline{2} = \overline{u^2-2} = \overline{0}$, d. h. $\overline{u}$ ist eine Nullstelle von $t^2 - \overline{2}$. Damit ist $f = (t-\overline{1})(t-\overline{u})(t+\overline{u})$.

(4) (a) Zeige, dass $\mathbb{Z}[\mathrm{i}]$ mit der Funktion $\delta(z) := |z|^2$ ein euklidischer Ring (und damit ein Hauptidealring) ist.

(b) Zerlege die Zahl 15 im Ring $\mathbb{Z}[\mathrm{i}]$ in Primfaktoren.

Lösung: (a) Wir müssen die Existenz einer Division mit Rest zeigen. Es seien dazu $x, y \in \mathbb{Z}[\mathrm{i}]$ mit $y \neq 0$ gegeben. Dann können wir $\frac{x}{y}$ in $\mathbb{C}$ bestimmen und erhalten so

$$\frac{x}{y} = c + d\,\mathrm{i} \quad \text{für gewisse } c, d \in \mathbb{R}.$$

Da eine reelle Zahl höchstens den Abstand $\frac{1}{2}$ von der nächstgelegenen ganzen Zahl hat, können wir dazu $a, b \in \mathbb{Z}$ finden mit $|c-a| \leq \frac{1}{2}$ und $|d-b| \leq \frac{1}{2}$. Wir setzen nun

$$q := a + b\,\mathrm{i} \in \mathbb{Z}[\mathrm{i}] \quad \text{und} \quad r := x - qy \in \mathbb{Z}[\mathrm{i}].$$

Dann ist $x = qy + r$ die gewünschte Division mit Rest, denn es gilt

$$\begin{aligned} |r|^2 &= |y|^2 \cdot \left|\frac{x}{y} - q\right|^2 = |y|^2 \cdot |(c-a) + (d-b)\,\mathrm{i}|^2 = |y|^2 \cdot ((c-a)^2 + (d-b)^2) \leq |y|^2 \cdot \left(\frac{1}{4} + \frac{1}{4}\right) \\ &< |y|^2, \end{aligned}$$

also $\delta(r) < \delta(y)$.

(b) Wir sehen zunächst, dass

$$15 = 3 \cdot 5 = 3 \cdot (2+\mathrm{i}) \cdot (2-\mathrm{i}),$$

und behaupten, dass $3 \cdot (2+\mathrm{i}) \cdot (2-\mathrm{i})$ eine Primfaktorzerlegung von 15 in $\mathbb{Z}[\mathrm{i}]$ ist.

Da $\mathbb{Z}[\mathrm{i}]$ nach Aufgabe 4 ein Hauptidealring ist, ist jedes irreduzible Element prim, und damit genügt es zu zeigen, dass die obigen drei Faktoren irreduzibel sind.

- Ist $3 = (a+b\,\mathrm{i})(c+d\,\mathrm{i})$, so bedeutet dies für die Betragsquadrate $9 = (a^2+b^2)(c^2+d^2)$, und damit muss $a^2+b^2, c^2+d^2 \in \{1,3,9\}$ gelten. Dabei hat $a^2+b^2 = 3$ bzw. $c^2+d^2 = 3$ keine Lösung in ganzen Zahlen, also ist $a^2+b^2 = 1$ oder $c^2+d^2 = 1$. Ist aber ohne Einschränkung $a^2+b^2 = 1$, so ist $a+b\,\mathrm{i} \in \{\pm 1, \pm \mathrm{i}\}$ eine Einheit in $\mathbb{Z}[\mathrm{i}]$. Also ist 3 irreduzibel.
- Die Rechnung für $2 \pm \mathrm{i}$ ist analog: Aus $2+\mathrm{i} = (a+b\,\mathrm{i})(c+d\,\mathrm{i})$ folgt $5 = (a^2+b^2)(c^2+d^2)$, ohne Einschränkung also $a^2+b^2 = 1$ und damit wieder $a+b\,\mathrm{i} \in \{\pm 1, \pm \mathrm{i}\}$.