# Mathematische Strukturen – Lösungen zu Übungsblatt 5

Hagen Knaf, SS 2016

1. In dieser Aufgabe geht es um das Rechnen modulo $n$, also um den Ring $\mathbb{Z}/n$.

   (a) Zeigen Sie unter Benutzung des Rechnens in $\mathbb{Z}/7$, dass die Polynomgleichung
   $$36x^3 + 56x^2 + 91x + 368 = 0 \tag{1}$$
   keine ganzzahlige Lösung besitzt.
   Lösung: Die Reste der Koeffizienten von Gleichung (1) bei Division durch 7 sind 1, 0, 0 und 4. Ist dann $z \in \mathbb{Z}$ eine Lösung der Polynomgleichung und $z = 7q + r$ die Division von $z$ durch 7 mit Rest $r \in \{0, \ldots, 6\}$, so gilt
   $$7 \mid (r^3 + 0r^2 + 0r + 4),$$
   also
   $$\overline{r}^3 + \overline{4} = \overline{0}$$
   in $\mathbb{Z}/7$.
   Berechnet man die dritten Potenzen in $\mathbb{Z}/7$, so ergibt sich: $\overline{0}^3 = \overline{0}$, $\overline{1}^3 = \overline{1}$, $\overline{2}^3 = \overline{1}$, $\overline{3}^3 = \overline{6}$, $\overline{4}^3 = \overline{1}$, $\overline{5}^3 = \overline{6}$, $\overline{6}^3 = \overline{6}$. Folglich ist $-\overline{4} = \overline{3}$ keine dritte Potenz in $\mathbb{Z}/7$ und die Gleichung $x^3 + \overline{4} = 0$ besitzt keine Lösung in $\mathbb{Z}/7$. Damit kann aber Gleichung (1) keine ganzzahlige Lösung besitzen.

   (b) Beweisen Sie mittels Rechnen modulo 3 die Teilbarkeitsregel ≫Eine Zahl $z \in \mathbb{Z}$ ist durch 3 teilbar genau dann, wenn ihre Quersumme, also die Summe ihrer Ziffern, durch 3 teilbar ist.≪
   Lösung: Für die Teilbarkeit kommt es auf das Vorzeichen nicht an, wir können also $z \geq 0$ annehmen. Es gilt
   $$z = \sum_{k=0}^{e} z_k 10^k,$$
   wobei $z_0, \ldots, z_e$ die Ziffern von $z$ sind. Da $10 = 3 \cdot 3 + 1$ ist, gilt: Die Zahl $z = 3q + r$ besitzt bei Division durch 3 denselben Rest $r$ wie die Zahl $\sum_{k=0}^{e} z_k$, womit die Regel bewiesen ist.

(c) Bestimmen Sie die nilpotenten Elemente von $\mathbb{Z}/2646$.

LÖSUNG: In der Vorlesung wurde gezeigt, dass die nilpotenten Elemente von $\mathbb{Z}/n$ genau diejenigen Elemente $\overline{a}$ sind, für die $a$ und $n$ dieselben Primfaktoren besitzen. Die Primfaktorisierung von 2646 ist

$$2 \cdot 3^3 \cdot 7^2,$$

womit es die nilpotenten Elemente

$$\overline{2 \cdot 3 \cdot 7 \cdot k} \quad = \quad \overline{42k},\ k \in \{0, \ldots 62\}$$

gibt.

(d) Zeigen Sie, dass die nilpotenten Elemente von $Z/n$ bezüglich der Addition eine Gruppe bilden.

BEWEIS: $\overline{a} \in \mathbb{Z}/n$ ist genau dann nilpotent, wenn $a$ und $n$ dieselben Primteiler besitzen.

Es seien nun $\overline{a}, \overline{b} \in \mathbb{Z}/n$ nilpotente Elemente. Dann gilt $\overline{a} + \overline{b} = \overline{c}$, wobei

$$a + b = qn + c.$$

Ist nun $p$ eine Primzahl, die $a$, $b$ und $n$ teilt, so zeigt diese Gleichung, dass auch $c$ durch $p$ teilbar ist. Folglich ist $\overline{c}$ nilpotent.

Weiter gilt $-\overline{a} = \overline{n-a}$. Da $n - a$ durch gemeinsame Primteiler von $a$ und $n$ teilbar ist, ist das additiv Inverse $-\overline{a}$ also nilpotent, womit alles bewiesen ist.

2. In dieser Aufgabe geht es um das Lösen linearer Gleichungssysteme

$$\begin{aligned} a_{11}x + a_{12}y &= b_1 \\ a_{21}x + a_{22}y &= b_2, \end{aligned}$$

wobei die Koeffizienten $a_{ij}$ sowie die rechten Seiten $b_i$ Elemente eines kommutativen Rings $(R, +, \cdot)$ sind.

(a) Es sei $R = \mathbb{Z}/13$. Bestimmen Sie die Lösungen des obigen Gleichungssystems für die Koeffizienten

$$a_{11} = \overline{7}, a_{12} = \overline{2}, a_{21} = \overline{9}, a_{22} = \overline{6}$$

sowie die rechten Seiten

$$b_1 = \overline{3}, b_2 = \overline{5}.$$

Lösung: Das Gleichungssystem lautet

$$\begin{array}{rcl} \overline{7}x + \overline{2}y & = & \overline{3} \\ \overline{9}x + \overline{6}y & = & \overline{5}. \end{array}$$

Subtraktion der 2. Gleichung vom $\overline{3}$-fachen der 1. Gleichung liefert:

$$\overline{12}x = \overline{4}.$$

Es gilt $\overline{12}^{-1} = 12$, da $12 \cdot 12 = 11 \cdot 13 + 1$. Folglich ist $x = \overline{12} \cdot \overline{4} = \overline{9}$. Einsetzen in die 1. Gleichung liefert

$$\overline{2}y = \overline{3} - \overline{7} \cdot \overline{9} = \overline{3} + \overline{7} \cdot \overline{4} = \overline{5}.$$

Es ist $\overline{2}^{-1} = \overline{7}$, da $2 \cdot 7 = 13 + 1$. Also ist $y = \overline{7} \cdot \overline{5} = \overline{9}$.

(b) Es sei $R = \mathbb{Z}/12$. Lösen Sie das obige Gleichungssystem mit den Koeffizienten und rechten Seiten aus Aufgabe (a) jetzt natürlich aufgefasst als Elemente von $\mathbb{Z}/12$.

Lösung: Das Gleichungssystem besitzt in diesem Fall *keine* Lösung, denn die 2. Gleichung lautet leicht umgeformt:

$$\overline{3} \cdot (\overline{3}x + \overline{2}y) = \overline{5}.$$

Da 5 und 12 teilerfremd sind, ist $\overline{5}$ eine Einheit in $\mathbb{Z}/12$ also inbesondere kein Nullteiler. Andererseits ist $\overline{3} \cdot \overline{4} = \overline{0}$, das Element $\overline{3}$ ist also ein Nullteiler. Dann ist auch jedes von $\overline{0}$ verschiedene Vielfache von $\overline{3}$ ein Nullteiler. Folglich müsste $\overline{5}$ ein Nullteiler sein, was nicht stimmt.

(c) Es sei $R = \mathbb{Z}$. Zeigen Sie, dass für die Koeffizienten $a_{ij}$ des obigen Gleichungssystems folgende Aussage gilt: Genau dann besitzt das Gleichungssystem für *jede* Vorgabe der rechten Seiten $b_i$ eine eindeutige *ganzzahlige* Lösung, wenn die Bedingung

$$a_{11}a_{22} - a_{21}a_{12} \in \{-1, 1\}$$

gilt.

Beweis: Man betrachtet die Matrix $A := (a_{ij}) \in \mathbb{Z}^{2\times 2}$ der Koeffizienten des obigen linearen Gleichungssystem. Die Größe $a_{11}a_{22} - a_{21}a_{12}$ ist gerade die Determinante von $A$. Setzt man $z = (x, y)^t$ und $b = (b_1, b_2)^t$, so kann man das Gleichungsystem in der Form $Az = b$ schreiben.

$\Leftarrow$: Da nach Voraussetzung die Determinante von $A$ ungleich 0 ist, ist $A$ invertierbar. Die Inverse ist

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix},$$

also nach Voraussetzung über $\det(A)$ eine Matrix mit ganzzahligen Koeffizienten. Dann ist aber auch die eindeutige Lösung $z = A^{-1}b$ des linearen Gleichungssystems ganzzahlig.

$\Rightarrow$: Nach Voraussetzung muss es zu den rechten Seiten $(1,0)^t$ und $(0,1)^t$ eindeutige Lösungen von $Az = b$ geben. Wie aus der linearen Algebra bekannt, muss dann der Rang von $A$ gleich 2 sein, $A$ ist also invertierbar. (Für diesen Schluss wird die Ganzzahligkeit der Lösungen nicht benötigt.)

Die Lösungen zu $Az = (1,0)^t$ und $Az = (0,1)^t$ sind gerade die Spalten der Matrix $A^{-1}$. Betrachtet man die Formel für die Inverse, so müssen also alle Koeffizienten der Matrix $A$ durch $\det(A)$ teilbar sein, um die Ganzzahligkeit der Lösungen zu gewährleisten:

$$A = \begin{pmatrix} \det(A)b_{11} & \det(A)b_{12} \\ \det(A)b_{21} & \det(A)b_{22} \end{pmatrix}$$

für gewisse ganze Zahlen $b_{ij}$. Es folgt:

$$\det(A) = \det(A)^2(b_{11}b_{22} - b_{12}b_{21}),$$

wobei der zweite Faktor auf der rechten Seite eine ganze Zahl ist. Teilen durch $\det(A)$ liefert die Behauptung.

3. Es seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe. Betrachten Sie die Menge

$$R \times S := \{(r,s) : r \in R,\ s \in S\}$$

versehen mit den inneren Verknüpfungen

$$(r,s) + (r',s') := (r +_R r', s +_S s')$$

und

$$(r,s) \cdot (r',s') := (r \cdot_R r', s \cdot_S s').$$

Zeigen Sie, dass $(R \times S, +, \cdot)$ ein Ring ist.