3. Hausaufgabenüberprüfung "Mathematische Strukturen" (Donnerstag, 6. Juli 2017)

Aufgabe 1. Ist die Drehung des $\mathbb{R}^2$ um den Winkel $\pi/4$ mit Drehpunkt $(0,0)$ eine Isometrie, wenn man den $\mathbb{R}^2$ mit der Maximumsmetrik

$$d_{\max}((x_1,x_2),(y_1,y_2)) = \max(|x_1-y_1|,|x_2-y_2|)$$

versieht? Wie lautet die Antwort auf die entsprechende Frage für einen beliebigen Winkel $\varphi \in [0,2\pi)$?

Aufgabe 2. Berechne die Expansion $E(f)$ der linearen Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2$, $(x_1,x_2) \mapsto (x_1+\lambda x_2, x_2)$, mit $\lambda \in \mathbb{R}$. Dabei sei der $\mathbb{R}^2$ mit der Metrik

$$d_1((x_1,x_2),(y_1,y_2)) = |x_1-y_1| + |x_2-y_2|$$

versehen.

Aufgabe 3. Es sei (X,d) ein metrischer Raum mit endlich vielen Elementen. Zeige, daß für jede konvergente Folge $(x_k)_{k\in\mathbb{N}}$ in X gilt: Es gibt eine Zahl $n \in \mathbb{N}$ und ein Element $x_0 \in X$ mit $x_k = x_0$ für alle $k > n$. Folgere hieraus, daß jede Abbildung $f : X \to X$ stetig ist.

Aufgabe 4. Es sei $K = \mathbb{Z}_2$ der Körper mit zwei Elementen.

(a) Wie viele Elemente hat der Matrizenring $R := K^{2\times 2}$? Ist R kommutativ? Besitzt R ein Einselement?

(b) In R betrachten wir die vier Matrizen

$$A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\ B = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},\ C = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix},\ D = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}.$$

Zeige durch explizites Hinschreiben der Verknüpfungstafeln, daß $U := \{A,B,C,D\}$ ein Unterring von R ist. Ist U kommutativ? Besitzt U ein Einselement?

Aufgabe 5. (a) Bestimme 17^{-1} in $\mathbb{Z}_{243}$.

(b) Stelle mit dem Algorithmus von Shanks fest, ob die Gleichung $3^n = 17$ eine Lösung in $\mathbb{Z}_{19}$ besitzt.

Aufgabe 6. Ein Element $x \in R$ eines Rings R heißt idempotent, wenn $x^2 = x$ gilt.

(a) Es sei $R = R_1 \times R_2$ das direkte Produkt zweier Ringe R_1 und R_2. Zeige, daß die idempotenten Elemente von R genau die Paare $x = (x_1,x_2)$ sind, für die x_1 idempotent in R_1 und x_2 idempotent in R_2 ist.

(b) Zeige: Ist $n = p^k$ eine Primzahlpotenz, so hat der Restklassenring $\mathbb{Z}_n$ nur die beiden trivialen idempotenten Elemente 0 und 1.

(c) Finde alle idempotenten Elemente des Restklassenrings $\mathbb{Z}_{400}$. **Hinweis:** $\mathbb{Z}_{400}$ ist isomorph zu $\mathbb{Z}_{16} \times \mathbb{Z}_{25}$. (Warum?)

Lösungen zu den algebraischen Aufgaben

Lösung 4. (a) Für jeden der vier möglichen Einträge einer Matrix in $K^{2\times 2}$ gibt es zwei Möglichkeiten (nämlich 0 und 1); der Ring $K^{2\times 2}$ aller solchen Matrizen hat also $2^4 = 16$ Elemente. Dieser Ring ist nicht kommutativ, denn beispielsweise gilt

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Der Ring $K^{2\times 2}$ besitzt ein Einselement, nämlich die Einheitsmatrix

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

(b) Additions- und Multiplikationstafel sehen folgendermaßen aus.

$+$	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

$\cdot$	A	B	C	D
A	A	A	A	A
B	A	A	B	B
C	A	A	C	C
D	A	A	D	D

Also ist $U := \{A,B,C,D\}$ additiv und multiplikativ abgeschlossen, enthält das Nullelement A und zu jedem Element ein additives Inverses. Dies zeigt, daß U ein Unterring von $K^{2\times 2}$ ist. Da die Multiplikationstafel von U nicht symmetrisch zur Diagonalen ist, ist der Ring U nicht kommutativ. Aus der Multiplikationstafel liest man ferner ab, daß C und D rechtsneutral sind, daß es aber in U kein linksneutrales Element gibt. Insbesondere besitzt U also kein Einselement.

Lösung 5. (a) Wir führen den Euklidischen Algorithmus aus. Sukzessive Divisionen mit Rest liefern die folgenden Gleichungen.

$$\begin{aligned} 243 &= 14\cdot 17 + 5 \\ 17 &= 3\cdot 5 + 2 \\ 5 &= 2\cdot 2 + 1 \end{aligned}$$

Rückwärtseinsetzen ergibt dann

$$\begin{aligned} 1 &= 5 - 2\cdot 2 = 5 - 2\cdot(17 - 3\cdot 5) = 7\cdot 5 - 2\cdot 17 \\ &= 7\cdot(243 - 14\cdot 17) - 2\cdot 17 = 7\cdot 243 - 100\cdot 17. \end{aligned}$$

Modulo 243 gilt also $[1] = [-100]\cdot[17] = [143]\cdot[17]$. In $\mathbb{Z}_{243}^\times$ gilt daher $17^{-1} = 143$.

(b) Mit $m := [\sqrt{18}] + 1 = 5$ erhalten wir in $\mathbb{Z}_{19}^\times$ die Gleichung $\gamma = 3^{-5} = (3^{-1})^5 = (-6)^5 = 14$ (denn in $\mathbb{Z}_{19}$ haben wir zunächst $-6\cdot 3 = -18 = 1$, also $3^{-1} = -6$, und dann $(-6)^5 = -36\cdot 36\cdot 6 = -(-2)(-2)\cdot 6 = -24 = 14$).

Nach dem Algorithmus von Shanks berechnen wir also zunächst

r	0	1	2	3	4
3^r	1	3	9	8	5

und dann

k	0	1	2	3 $\cdots$
$17 \cdot 14^k$	17	10	7	3 $\cdots$

Für $r = 1$ und $k = 3$ tritt Übereinstimmung auf; wir haben also $\log_3 17 = km + r = 3 \cdot 5 + 1 = 16$. (Zur Probe kann man natürlich nachprüfen, daß tatsächlich $3^{16} = 17$ in $\mathbb{Z}_{19}^\times$ gilt.)

Lösung 6. (a) Weil die Verknüpfungen in einem direkten Produkt von Ringen einfach die komponentenweise durchgeführten Verknüpfungen in den einzelnen Faktoren sind, gelten für $x = (x_1, x_2)$ die Äquivalenzen

$$x^2 = x \;\Leftrightarrow\; (x_1^2, x_2^2) = (x_1, x_2) \;\Leftrightarrow\; x_1^2 = x_1 \text{ und } x_2^2 = x_2.$$

Also ist $x = (x_1, x_2)$ genau dann idempotent in $R_1 \times R_2$, wenn x_1 idempotent in R_1 und x_2 idempotent in R_2 ist.

(b) Es sei $[x]$ die Restklasse von $x \in \mathbb{Z}$ modulo $n = p^k$. Ist $[x]$ idempotent, so gilt $[0] = [x]^2 - [x] = [x^2 - x]$, so daß $x^2 - x = x(x-1)$ durch p^k teilbar ist. Nun können die beiden Zahlen x und $x-1$ (die sich ja nur um 1 unterscheiden) nicht beide durch p teilbar sein; also ist entweder x durch p^k teilbar (so daß $[x] = [0]$ gilt), oder aber $x - 1$ ist durch p^k teilbar (so daß $[x - 1] = [0]$ bzw. $[x] = [1]$ gilt). Also kann es außer $[0]$ und $[1]$ in $\mathbb{Z}_n$ keine idempotenten Elemente geben. Daß $[0]$ und $[1]$ tatsächlich idempotente Elemente sind, ist klar.

(c) Wegen $400 = 2^4 \cdot 5^2 = 16 \cdot 25$ und der Teilerfremdheit von 16 und 25 ist die Abbildung $\varphi : \mathbb{Z}_{400} \to \mathbb{Z}_{16} \times \mathbb{Z}_{25}$ mit

$$\varphi([x]_{400}) \;:=\; ([x]_{16}, [x]_{25})$$

ein wohldefinierter Ringisomorphismus. Nach Teil (a) und Teil (b) gibt es in $\mathbb{Z}_{16} \times \mathbb{Z}_{25}$ genau vier idempotente Elemente, nämlich $(0,0)$, $(1,0)$, $(0,1)$ und $(1,1)$ (wobei wir etwas schlampig x statt $[x]$ schreiben). Die idempotenten Elemente von $\mathbb{Z}_{400}$ sind also die Elemente $\varphi^{-1}(0,0) = 0$, $\varphi^{-1}(1,0) =: u$, $\varphi^{-1}(0,1) =: v$ und $\varphi^{-1}(1,1) = 1$. Dabei ist u bestimmt durch die Kongruenzen $u \equiv 1$ modulo 16 und $u \equiv 0$ modulo 25 mit der Lösung $u \equiv 225$ modulo 400. Ferner ist v bestimmt durch die Kongruenzen $v \equiv 0$ modulo 16 und $v \equiv 1$ modulo 25, die die Lösung $v \equiv 176$ modulo 400 haben. In $\mathbb{Z}_{400}$ gibt es also die vier idempotenten Elemente

$$0, \quad 1, \quad 176, \quad 225.$$

Bemerkungen. (a) Die Lösungen u und v der simultanen Kongruenzen

$$(1) \qquad \begin{aligned} u &\equiv 1 \text{ modulo } 16 \\ u &\equiv 0 \text{ modulo } 25 \end{aligned}$$

und

$$(2) \qquad \begin{aligned} v &\equiv 0 \text{ modulo } 16 \\ v &\equiv 1 \text{ modulo } 25 \end{aligned}$$

kann man mittels einfachem Durchprobieren aller Möglichkeiten finden (und so war die Aufgabe gedacht).

(b) Man kann aber auch systematisch vorgehen. Zur Lösung von (1) schreiben wir $u = 16k + 1$ und haben dann $16k \equiv -1$ modulo 25. Wegen $16^{-1} = 11$ modulo 25 muktiplizieren wir mit 11 durch und erhalten $k \equiv -11 \equiv 14$ modulo 25, also $k = 25\ell + 14$ und damit

$$u \;=\; 16k + 1 \;=\; 400\ell + 225.$$

Zur Lösung von (2) schreiben wir analog $v = 16k$ und haben dann $16k \equiv 1$ modulo 25. Durchmultiplizieren mit 11 liefert $k \equiv 11$ modulo 25, also $k = 25\ell + 11$ und damit

$$v \;=\; 16k \;=\; 400\ell + 176.$$

(c) Ist die Kongruenz (1) gelöst, so kann man sich die Lösung der Kongruenz (2) sparen. Mit e ist nämlich immer auch $1 - e$ idempotent. Das idempotente Element $u = 225$ von $\mathbb{Z}_{400}$ liefert also das weitere idempotente Element $1 - u = -224 = 176$.