Algebra für Informatik (2016S)

11. Übungsblatt, mit Lösungen

für den 13. Juni 2016

1. Beweisen Sie, dass in einem kommutativen Ring $\langle R, +, -, \cdot, 0, 1\rangle$ die binomische Formel gilt. Das heißt, zeigen Sie mittels vollständiger Induktion nach n, dass für alle $a, b \in R$ und alle $n \in \mathbb{N}$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

gilt. Dabei bezeichnet mx für $m \in \mathbb{N}$ und $x \in R$ das Element $\sum_{k=1}^{m} x \in R$.
Hinweis: Sie können dabei ohne Beweis verwenden, dass einerseits der Binomialkoeffizient $\binom{n}{k} \in \mathbb{N}$ für $n, k \in \mathbb{N}$

$$\binom{n}{0} = \binom{n}{n} = 1 \quad \text{und} \quad \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

erfüllt sowie andererseits, dass $nx + mx = (n+m)x$ für $n, m \in \mathbb{N}$ und $x \in R$ gilt.

2. Zeigen Sie, dass ein kommutativer Ring, in dem $0 = 1$ gilt, kein Körper sein kann. Füllen Sie dazu die Lücken in folgendem Beweistext:
Für jedes $x \in R$ gilt $x \cdot 1 =$ _____ und $x \cdot 0 =$ _____. Wegen $0 = 1$ gilt außerdem $x \cdot 1 =$ _____. Insgesamt folgt also $x =$ _____. Daher ist jedes Element des Rings gleich _____ und es gilt $|R| =$ _____. Wäre der Ring auch ein Körper, dann müsste aber _____ gelten.

3. Füllen Sie die Lücken in folgenden Beweistexten:

   (a) Zeigen Sie, dass das Produkt zweier Elemente in einem Körper genau dann gleich 0 ist, wenn mindestens einer der beiden Faktoren gleich 0 ist.
   Seien x und y Elemente des Körpers. Falls $x = 0$ oder $y = 0$, dann ist $x \cdot y =$ _____. Ist umgekehrt $x \cdot y = 0$ und nehmen wir $y \neq 0$ an, dann gibt es im Körper ein z, sodass _____. Mit diesem z ist einerseits $x \cdot (y \cdot z) =$ _____ und andererseits gilt $(x \cdot y) \cdot z =$ _____. Daraus folgt $x =$ _____. Insgesamt folgt also aus $x \cdot y = 0$ entweder _____ oder $y \neq 0$ und _____. In beiden Fällen ist mindestens einer _____ x und y _____.

   (b) Schließen Sie daraus, dass $\langle \mathbb{Z}_4, \oplus, \ominus, \odot, [0]_4, [1]_4\rangle$ kein Körper sein kann.
   In $\langle \mathbb{Z}_4, \oplus, \ominus, \odot, [0]_4, [1]_4\rangle$ können wir $x =$ _____ und $y =$ _____ wählen, sodass $x \cdot y =$ _____ und _____ sowie _____. Wegen _____ ist in einem Körper das Produkt _____ nur dann _____ wenn mindestens _____.

4. Berechnen Sie alle Lösungen der folgenden Gleichung in $\langle \mathbb{Z}_{102}, \oplus, \ominus, \odot, [0]_{102}, [1]_{102}\rangle$:

$$[63]_{102} \cdot x = [39]_{102}$$

Lösung:
Mit $x = [z]_{102}$ ist $[63]_{102} \cdot x = [63z]_{102}$. Daher ist $[63]_{102} \cdot x = [39]_{102}$ äquivalent zu $[63z]_{102} = [39]_{102}$ bzw. $63z = 39 \pmod{102}$. Mit dem erweiterten Euklidischen Algorithmus berechnet man $63 \cdot 13 + 102 \cdot (-8) = 3$, daher ist $z_0 = 13 \cdot \frac{39}{3}$ eine Lösung von $63z = 39 \pmod{102}$. Nach Satz 6.16

sind dann alle Lösungen durch $z = z_0 + \frac{102}{3}k$ mit $k \in \mathbb{Z}$ gegeben. Die ursprüngliche Gleichung $[63]_{102} \cdot x = [39]_{102}$ hat also die Lösungen $[169 + 34k]_{102}$, $k \in \mathbb{Z}$. Mit $k \in \{-4, -3, -2\}$ erhält man also die drei Lösungen $x = [33]_{102}$, $x = [67]_{102}$ und $x = [101]_{102}$. □

5. Auf der Menge

$$C := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{R}^{2\times 2} \;\middle|\; a, b \in \mathbb{R} \right\}$$

seien die binären Operationen + und · durch die übliche Addition und Multiplikation von Matrizen definiert sowie die unäre Operation − durch komponentenweises Minus. Weisen Sie nach, dass $\langle C, +, -, \cdot, 0_{2\times 2}, E_2 \rangle$ ein kommutativer Ring ist, wobei $0_{2\times 2}$ die Nullmatrix und E_2 die Einheitsmatrix ist.
Hinweis: Vergessen Sie nicht nachzuprüfen, dass mit $x, y \in C$ auch $x + y$, $x \cdot y$ und $-x$ in C liegen.

Lösung:
Seien $x = \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \in C$ und $y = \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} \in C$, dann gilt

$$x + y = \begin{pmatrix} a_1 + a_2 & -(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{pmatrix} \in C, \quad x \cdot y = \begin{pmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ a_1b_2 + a_2b_1 & a_1a_2 - b_1b_2 \end{pmatrix} \in C$$

und

$$-x = \begin{pmatrix} -a_1 & -(-b_1) \\ -b_1 & -a_1 \end{pmatrix} \in C.$$

Die meisten Eigenschaften von Definition 7.1 folgen direkt aus allgemeinen Eigenschaften des Rechnens mit Matrizen (z.B. Satz 2.8 und Satz 2.10). Einzig Eigenschaft (6), also die Kommutativität der Multiplikation, ist speziell nachzuprüfen:

$$x \cdot y = \begin{pmatrix} a_1a_2 - b_1b_2 & -a_1b_2 - a_2b_1 \\ b_1a_2 + a_1b_2 & -b_1b_2 + a_1a_2 \end{pmatrix} = \begin{pmatrix} a_2a_1 - b_2b_1 & -a_2b_1 - b_2a_1 \\ b_2a_1 + a_2b_1 & -b_2b_1 + a_2a_1 \end{pmatrix} = \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} \cdot \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix}$$

□

6. Handelt es sich beim Ring $\langle C, +, -, \cdot, 0_{2\times 2}, E_2 \rangle$ aus der vorigen Aufgabe um einen Körper?

Lösung:
Wegen $0_{2\times 2} \neq E_2$ gilt $|C| \geq 2$. Weiters gilt für $(a_1, b_1) \neq (0, 0)$ mit $a_2 := \frac{a_1}{a_1^2 + b_1^2}$ und $b_2 := -\frac{b_1}{a_1^2 + b_1^2}$

$$x \cdot y = \begin{pmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{pmatrix} = E_2.$$

Also ist dieser Ring tatsächlich auch ein Körper. □

7. Für $n \in \mathbb{N}$ sei W_n die Menge aller Wörter mit n Bit:

$$W_n = \{0 \ldots 00, 0 \ldots 01, \ldots, 1 \ldots 11\}.$$

Auf W_n seien die binäre Operation $\oplus$ als bitweises XOR (ausschließendes Oder) und die binäre Operation $\odot$ als bitweises AND (Konjunktion) definiert. Weiters sei die unäre Operation $\ominus$ durch $\ominus x := x$ definiert. Weisen Sie nach, dass dann $\langle W_n, \oplus, \ominus, \odot, 0_n, 1_n \rangle$ ein kommutativer Ring ist, wobei $0_n := 0 \ldots 00$ und $1_n := 1 \ldots 11$ ist.

Lösung:
Da alle Operationen bitweise definiert sind genügt es den Fall $n = 1$ zu betrachten. Die Eigenschaften von Definition 7.1 lassen sich unter Ausnutzung der Eigenschaften der logischen Operationen einfach nachrechnen. Alternativ lässt sich auch beobachten, dass die Operationen auf W_1 die selben sind wie im Ring $\langle \mathbb{Z}_2, \oplus, \ominus, \odot, [0]_2, [1]_2 \rangle$, wobei die Wörter 0 und 1 den Elementen $[0]_2$ bzw. $[1]_2$ entsprechen, folglich ist $\langle W_1, \oplus, \ominus, \odot, 0, 1 \rangle$ ebenfalls ein kommutativer Ring. □

8. Bestimmen sie alle Lösungen der Gleichung $x^2 = -1$ in den folgenden Ringen, wobei − die unäre Operation und 1 das Einselement des jeweiligen Rings sein sollen.

(a) $\langle \mathbb{Z}_3, \oplus, \ominus, \odot, [0]_3, [1]_3 \rangle$

(b) $\langle \mathbb{Z}_5, \oplus, \ominus, \odot, [0]_5, [1]_5 \rangle$

(c) $\langle C, +, -, \cdot, 0_{2\times 2}, E_2 \rangle$ aus Aufgabe 5

(d) $\langle W_n, \oplus, \ominus, \odot, 0_n, 1_n \rangle$ aus Aufgabe 7

Lösung:

(a) Durchprobieren aller Elemente $x \in \mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ zeigt, dass keine Lösung von $x^2 = [2]_3 = -[1]_3$ existiert.

(b) Durchprobieren aller Elemente $x \in \mathbb{Z}_5$ führt auf die Lösungen $x = [2]_5$ und $x = [3]_5$ von $x^2 = [4]_5 = -[1]_5$.

(c) Es ist $x^2 = \begin{pmatrix} a^2 - b^2 & -2ab \\ 2ab & a^2 - b^2 \end{pmatrix}$ für $x = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Um $x^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -E_2$ zu erfüllen muss also $ab = 0$ und $a^2 - b^2 = -1$ gelten, woraus $a = 0$ und $b = \pm 1$ folgt.

(d) Für alle Wörter $x \in W_n$ gilt $x^2 = x \odot x = x$. Um $x^2 = 1_n = \ominus 1_n$ zu erfüllen muss also $x = 1_n$ gelten.

□