Algebra für Informatik (2016S)

11. Übungsblatt

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 $\langle \mathbb{Z}_{102}, \oplus, \ominus, \odot, [0]_{102}, [1]_{102}\rangle$:

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

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 $\cdot$ 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.

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

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

$$W_n = \{0\dots00, 0\dots01, \dots, 1\dots11\}.$$

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 $0_n := 0\dots00$ und $1_n := 1\dots11$ ist.

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