Duale Hochschule Baden-Württemberg

Logik und Algebra

8. Übungsblatt

1. Aufgabe: Zeigen Sie mit Hilfe des klassischen Logikkalküls unter Angabe der verwendeten Axiome die Folgerung:

$$\frac{A \to (A \to \bot)}{A \to \bot}$$

2. Aufgabe: Für die Folge (x_n) gilt $x_1 = 0$ und $x_{n+1} = x_n + 2n$ für $n \in \mathbb{N}$. Zeigen Sie mit vollständiger Induktion, dass $x_n = n^2 - n$ gilt.

3. Aufgabe: Für die Menge $M = \mathbb{Z} \cap [-4, 4]$ sei die Relation $x \sim y \;\Leftrightarrow\; (x+1)^2 = (y+1)^2$ definiert. Zeigen Sie, dass $\sim$ auf M eine Äquivalenzrelation darstellt und bestimmen Sie die Äquivalenzklasse $[2]_\sim$. Wie viele Elemente besitzt die Faktormenge $M/_\sim$?

4. Aufgabe: Auf der Menge $M = \{(x_1, x_2) \,|\, x_1, x_2 \in \mathbb{R},\, x_1^2 + x_2^2 < 1\}$ sei die Relation R definiert als

$$(x_1, x_2)\, R\, (y_1, y_2) \;\Leftrightarrow\; x_2 \leq y_2\,.$$

   Beweisen oder widerlegen Sie:

   (a) R ist auf M eine Äquivalenzrelation.

   (b) R ist auf M eine Quasiordnung.

5. Aufgabe: Sei $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ mit $f(x) = x^2$.

   (a) Für welche Teilmengen $B \subseteq \mathbb{Z}_6$ ist $f_B : \mathbb{Z}_6 \to B$ mit $f_B(x) = f(x)$ surjektiv?

   (b) Für welche mögliche Teilmengen $A \subseteq \mathbb{Z}_6$ ist $f_{AB} : A \to B$ für ein B wie zuvor mit $f_{AB}(x) = f(x)$ bijektiv?

6. Aufgabe: Auf $Q = \mathbb{Q}^2 \backslash (0,0)$ sei die Operation $\star : Q \times Q \to Q$ definiert durch

$$(x_1, x_2) \star (y_1, y_2) = (x_1 \cdot y_1 + 2x_2 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1)\,.$$

   (a) Gibt es ein neutrales Element $(e_1, e_2) \in Q$, so dass für alle $(x_1, x_2) \in Q$ gilt: $(x_1, x_2) \star (e_1, e_2) = (x_1, x_2)$?

   (b) Für ein beliebiges $(x_1, x_2) \in Q$ bestimmen Sie $(x_1, x_2) \star (y_1, y_2)$ für

$$(y_1, y_2) = \left(\frac{x_1}{x_1^2 - 2x_2^2}\,,\, \frac{x_2}{2x_2^2 - x_1^2}\right).$$

   In welcher Beziehung stehen (x_1, x_2) und (y_1, y_2) zueinander?

7. Aufgabe: Es sei $G = \langle (25), (2154) \rangle$ in S_5.
   (a) Bestimmen Sie alle Elemente von G.
   (b) Ist $(G, \circ)$ kommutativ?
   (c) Ist $(H, \circ)$ mit $H = \langle (25)(14) \rangle$ eine Untergruppe von G?

8. Aufgabe:
   (a) Bestimmen Sie den $\mathrm{ggT}(62, 39)$ mit dem erweiterten euklidischen Algorithmus.
   (b) Existiert zu 35 eine multiplikative Inverse in $\mathbb{Z}_{62}$? Falls ja, bestimmen Sie diese.

9. Aufgabe: Es sei $p(x) = x^2 + x + 1$ und $q(x) = x^3 + x$.
   (a) Bestimmen Sie das Produkt $p(x) \cdot q(x)$ in $\mathbb{Z}_2[x]$.
   (b) Zeigen Sie, dass $p(x)$ in $\mathbb{Z}_2[x]$ das Polynom $x^6 + 1$ teilt.
   (c) Begründen Sie, warum $p(x)$ ein Generatorpolynom eines zyklischen Codes in $\mathbb{Z}_2[x]/_{x^6+1}$ ist.
   (d) Bestimmen Sie den binären Code von $(1, 0, 1, 0)$ im vom $p(x)$ erzeugten zyklischen Code in $\mathbb{Z}_2[x]/_{x^6+1}$.

10. Aufgabe: Führen Sie das Diffie-Hellman Protokoll in $\mathbb{Z}_{17}$ mit $\alpha = 6$ und den Geheimnissen $a = 2$ von Alice und $b = 3$ von Bob durch. Welche Informationen werden öffentlich kommuniziert und berechnen Sie sowohl für Alice als auch für Bob, auf welchen gemeinsamen geheimen Schlüssel sie sich einigen.

11. Aufgabe: Es sei $n = 7 \cdot 23 = 161$.
    (a) Berechnen Sie den $\mathrm{ggT}(132, 5)$ mit dem erweiterten euklidischen Algorithmus.
    (b) Zeigen Sie, dass $(5, 161)$ ein gültiger öffentlicher Schlüssel im RSA-Verfahren ist, und berechnen Sie den zugehörigen privaten Schlüssel.
    (c) Verschlüsseln Sie die Nachricht $m = 3$ mit dem öffentlichen Schlüssel $(5, 161)$.

12. Aufgabe: Gegeben sei die Boolesche Funktion $f(x_1, x_2, x_3, x_4) = (\overline{x}_3 \wedge \overline{x}_4) \vee (\overline{x}_1 \wedge \overline{x}_2) \vee (x_3 \wedge \overline{x}_4) \vee (x_1 \wedge x_2)$.
    (a) Stellen Sie die konjunktive Normalform der Funktion f auf.
    (b) Bestimmen Sie mit einem KV-Diagramm eine konjunktive Minimalform von f.
    (c) Erstellen Sie aus der konjunktiven Minimalform von f ein Schaltungsdiagramm.
    (d) Erstellen Sie aus der konjunktiven Minimalform von f eine Schaltung mit Logikgattern.