Universität Wien
Fakultät für Informatik
Prof. Wilfried Gansterer, RNDr. CSc. Katerina Schindlerova

Mathematische Grundlagen der Informatik 1

SS 2020

Übungsblatt 2: Gruppen, Ringe, Körper, Permutationen, Hashing

Literatur: Peter Hartmann: Mathematik für Informatiker, Springer, Kapitel 4, 5

Aufgabe 2-1 5P

a) Wir definieren auf der Menge S die Verknüpfung durch

$$a \odot b := a.$$

Überprüfen Sie, ob das Assoziativgesetz erfüllt ist.

b) Es sei $(G, *)$ eine Gruppe und 1 das neutrale Element. Angenommen, die Gleichung $x * y * z = 1$ gilt in der Gruppe G. Folgt daraus, dass $y * z * x = 1$ ist?

Aufgabe 2-2 5P

Es sei $(G, *)$ eine Gruppe. Beweisen Sie die folgenden Kürzungsregeln:

(a) Für alle $x, p, q \in G$ gilt $x * p = x * q$ wenn und nur wenn $p = q$.

(b) Für alle $x, p, q \in G$ gilt $p * x = q * x$ wenn und nur wenn $p = q$.

Aufgabe 2-3 6P

Sei $\mathbb{Z}$ die Menge der ganzen Zahlen. Zeigen Sie, ob die folgende Menge ein Ring oder Körper ist.

- $(G, \oplus, \odot)$, wobei $G = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ und die Verknüpfungen sind wie folgt definiert:
  $(a_1 + b_1\sqrt{2}) \oplus (a_2 + b_2\sqrt{2}) := a_1 + a_2 + (b_1 + b_2)\sqrt{2}$, und $(a_1 + b_1\sqrt{2}) \odot (a_2 + b_2\sqrt{2}) := a_1 a_2 + b_1 b_2\sqrt{2}$.

Aufgabe 2-4 8P

Fügen Sie die folgenden Werte in eine Hashtabelle der Länge 11 mit folgender Hashfunktion $h(x) = min(f(x), g(x))$ und $h_i(x) = h(x + i)$, wobei $f(x) = x \mod 11$ und $g(x) = x^2 \mod 11$.
a) $F = 13, 20, 5, 12, 1, 5$ (in dieser Reihenfolge)
b) F in sortierter Reihenfolge (sort(F) = $1, 5, 5, 12, 13, 20$)

Aufgabe 2-5 8P

Gegeben sind $\pi_1, \pi_2 \in S_6$

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 6 & 1 & 2 \end{pmatrix}, \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 1 & 4 & 5 \end{pmatrix}.$$

(a) Berechnen Sie π_1^{-1}, π_2^{-1}.

(b) Berechnen Sie $\pi_2 \circ \pi_1$.

(c) Finden Sie die Lösungen $x \in S_6$ der Gleichung $\pi_1 \circ x \circ \pi_2 = \pi_2 \circ \pi_1$.

Aufgabe 2-6 10P

Sei $\mathbb{R}$ die Menge der reellen Zahlen. Sei ε ein Symbol, das kein Element von $\mathbb{R}$ repräsentiert. Wir betrachten die Menge $\mathbb{R}[\varepsilon] := \{a + b\varepsilon | a, b \in \mathbb{R}\}$, und definieren darauf die beiden Verknüpfungen $\oplus$ und $\odot$ durch

$$(a + b\varepsilon) \oplus (a' + b'\varepsilon) := (a + a') + (b + b')\varepsilon,$$

$$(a + b\varepsilon) \odot (a' + b'\varepsilon) := (aa') + (ab' + a'b)\varepsilon.$$

Weisen Sie nach, dass $(\mathbb{R}[\varepsilon], \oplus, \odot)$ ein kommutativer Ring mit Einselement ist.

Aufgabe 2-7 10P

Zeigen Sie, dass in $(\mathbb{Z}/5\mathbb{Z}, \oplus, \otimes)$ das Distributivgesetz gilt. Ist $(\mathbb{Z}/5\mathbb{Z}, \oplus, \otimes)$ ein Ring?