CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL
Institut für Informatik
R. Berghammer

Institut für Informatik

Mathematik für Informatiker A

Wintersemester 2017/18

Lösungsvorschläge zu Serie 12

Präsenzaufgabe 1

Voraussetzung: -

Behauptung: -

Beweis. (a) Setze $(M, *) := (\mathbb{Z}, +)$. Es ist bekannt, dass die Addition sowohl kommutativ, wie auch assoziativ ist. Außerdem ist $(M, 0, *)$ ein Monoid, weil 0 neutral bezüglich der Addition ist.

(b) Setze $(M, *) := \left(\mathbb{N}^{\mathbb{N}}, \circ\right)$. Nach Vorlesung ist $* = \circ$ assoziativ. Allerdings ist es nicht kommutativ, denn für die Funktionen $f, g : \mathbb{N} \to \mathbb{N},\ f(n) = 3n$ und $g(n) = 2 + n$ gilt

$$(g \circ f)(0) = 2 + 3 \cdot 0 = 2 \neq 6 = 3 \cdot (2 + 0) = (f \circ g)(0)\ .$$

Also ist $f * g \neq g * f$ und damit $*$ nicht kommutativ. Ebenfalls nach Vorlesung ist aber $\left(\mathbb{N}^{\mathbb{N}}, \mathrm{id}_{\mathbb{N}}, \circ\right)$ ein Monoid.

(c) Sei $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ f(a, b) := (a + b)^2$. Setze $(M, *) := (\mathbb{N}, f)$. Offensichtlich ist f kommutativ, weil $+$ es ist. Es gilt aber

$$(0 * 1) * 2 = (0 + 1)^2 * 2 = (1 + 2)^2 = 9 \neq 81 = \left(0 + (1 + 2)^2\right)^2 = 0 * (1 * 2)\ .$$

Damit ist $*$ nicht assoziativ.

(d) Setze $(M, *) := (\mathbb{Z}, -)$. Es gilt $0 * 1 = 0 - 1 = -1 \neq 1 = 1 - 0 = 1 * 0$, also ist $-$ nicht kommutativ. Außerdem gilt

$$0 * (1 * 2) = 0 - (1 - 2) = 0 - 1 + 2 = 1 \neq -3 = (0 - 1) - 2 = (0 * 1) * 2\ .$$

Also ist $*$ nicht assoziativ. □

Präsenzaufgabe 2

Voraussetzung: Ein Monoid $(M, e, \cdot)$ heißt angeordnet, falls es kommutativ ist und $x \cdot x = x$ für alle $x \in M$ gilt. Weiter sei eine Relation $\sqsubseteq$ auf der Menge M für alle $x, y \in M$ gegeben durch

$$x \sqsubseteq y \ :\Longleftrightarrow\ x \cdot y = y.$$

Behauptung:

(a) $(\{\,1\,\}, 1, \cdot)$ ist ein Beispiel für ein angeordnetes Monoid und $(\mathbb{N}, 1, \cdot)$ ist ein Beispiel für ein nicht angeordnetes Monoid.

(b) $\sqsubseteq$ ist eine Ordnungsrelation auf M.

(c) Es gelten die zwei Eigenschaften:

$$(1)\ \forall x \in M : e \sqsubseteq x \qquad\qquad (2)\ \forall x, y, z \in M : x \sqsubseteq y \Rightarrow x \cdot z \sqsubseteq y \cdot z$$

Beweis. (a) -

Es sind natürlich noch diverse andere Beispiele denkbar:

Angeordnete Monoide:

$(\{0\}, 0, +)$**,** $(\mathcal{P}(A), \emptyset, \cup)$ **und** $(\mathcal{P}(A), A, \cap)$ **mit beliebiger Menge** A

Nicht angeordnete Monoide:

$(\mathbb{R}, 0, +)$**,** $(\mathbb{Z}, 0, -)$**,** $(\{0, 1\}, 1, \cdot)$**,** $(\mathbb{G}, 0, +)$ **mit** $\mathbb{G} = \{2n \mid n \in \mathbb{N}\}$

(b) *Reflexiv*: Sei $x \in M$. Da $(M, e, \cdot)$ ein angeordnetes Monoid ist, gilt $x \cdot x = x$. Nach Definition von $\sqsubseteq$ folgt $x \sqsubseteq x$.

Antisymmetrisch: Seien $x, y \in M$ mit $x \sqsubseteq y$ und $y \sqsubseteq x$. Nach Definition von $\sqsubseteq$ gelten dann $x \cdot y = y$ und $y \cdot x = x$. $(M, e, \cdot)$ ist als angeordnetes Monoid insbesondere kommutativ. Damit gilt aufgrund der vorherigen Gleichungen $x = y \cdot x = x \cdot y = y$.

Transitiv: Seien $x, y, z \in M$ mit $x \sqsubseteq y$ und $y \sqsubseteq z$. Nach Definition von $\sqsubseteq$ gelten dann $x \cdot y = y$ und $y \cdot z = z$. Diese beiden Gleichungen liefern zusammen mit der Assoziativität von $(M, e, \cdot)$ die Gleichungskette

$$x \cdot z = x \cdot (y \cdot z) = (x \cdot y) \cdot z = y \cdot z = z.$$

Nach Definition von $\sqsubseteq$ gilt somit $x \sqsubseteq z$.

Die Relation $\sqsubseteq$ ist also eine Ordnungsrelation auf M.

(c) (1) Sei $x \in M$, dann gilt aufgrund der Linksneutralität von e die Gleichheit $e \cdot x = x$. Nach Definition von $\sqsubseteq$ folgt $e \sqsubseteq x$.

(2) Seien $x, y, z \in M$ und es gelte $x \sqsubseteq y$. Nach Definition von $\sqsubseteq$ gilt dann $x \cdot y = y$. Da $(M, e, \cdot)$ ein angeordnetes Monoid ist, gilt insbesondere $z \cdot z = z$. Es folgt

$$\begin{aligned}
(x \cdot z) \cdot (y \cdot z) &= (z \cdot x) \cdot (y \cdot z) && \text{Kommutativität} \\
&= \big((z \cdot x) \cdot y\big) \cdot z && \text{Assoziativität} \\
&= \big(z \cdot (x \cdot y)\big) \cdot z && \text{Assoziativität} \\
&= (z \cdot y) \cdot z && x \cdot y = y \\
&= (y \cdot z) \cdot z && \text{Kommutativität} \\
&= y \cdot (z \cdot z) && \text{Assoziativität} \\
&= y \cdot z && z \cdot z = z
\end{aligned}$$

und damit $x \cdot z \sqsubseteq y \cdot z$ nach Definition von $\sqsubseteq$.

□

(a) *Beweis. Refl.:* Sei $a \in M$. Dann gilt $a \cdot e = a$, da e neutral bezüglich $\cdot$ ist, also auch $\exists\, c \in M : a \cdot c = a$ und damit $a \sqsubseteq a$.

Antisymm.: Seien $a, b \in M$ und es gelte $a \sqsubseteq b$ und $b \sqsubseteq a$. Dann existieren $x, y \in M$ mit $a \cdot x = b$ und $b \cdot y = a$. Es folgt:

$$a = b \cdot y = (a \cdot x) \cdot y = a \cdot (x \cdot y)\ .$$

Nach Voraussetzung gilt also $a = a \cdot x = b$.

Trans.: Seien $a, b, c \in M$ und es gelte $a \sqsubseteq b$ und $b \sqsubseteq c$. Dann existieren $x, y \in M$ mit $a \cdot x = b$ und $b \cdot y = c$. Setze $z := x \cdot y$. Dann ist $z \in M$ (wegen der Abgeschlossenheit bezüglich $\cdot$) und es gilt:

$$c = b \cdot y = (a \cdot x) \cdot y = a \cdot (x \cdot y) = a \cdot z\ .$$

Also gilt auch $\exists\, r \in M : a \cdot r = c$ und damit auch $a \sqsubseteq c$. □

(b) *Beweis.* (z.z. $e \sqsubseteq m$ für alle $m \in M$)
Sei $m \in M$. Dann gilt $e \cdot m = m$, da e neutral ist. Also gilt $\exists\, c \in M : e \cdot c = m$ und damit $e \sqsubseteq m$. □

Präsenzaufgabe 3

Voraussetzung: Gegeben sei die Menge $M := \{\, 1, 2, 3 \,\}$.
Behauptung: Die Gruppe $(\mathcal{S}(M), \mathsf{id}_M, \circ, ^{-1})$ ist nicht kommutativ.

Beweis. (z.z. es gibt $g, h \in \mathcal{S}(M)$ mit $g \circ h \neq h \circ g$)
Setze $g, h : M \to M$ mit $g(1) = 2$, $g(2) = 1$ und $g(3) = 3$ und $h(1) = 3$, $h(2) = 2$ und $h(3) = 1$.
(z.z. es gibt $x \in M$ mit $(g \circ h)(x) \neq (h \circ g)(x)$)
Setze $x := 1$. Dann gilt:

$$(g \circ h)(x) = g(h(x)) = g(h(1)) = g(3) = 3 \neq 2 = h(2) = h(g(1)) = h(g(x)) = (h \circ g)(x).$$

□