Musterlösung Serie 2

MODELLE FORMALER THEORIEN

---

8. Sei R ein 2-stelliges Relationssymbol, sei $\mathscr{L} = \{R\}$ und seien σ_1, σ_2, σ_3 die folgenden drei $\mathscr{L}$-Sätze:

$$\sigma_1 \equiv \forall x(Rxx), \quad \sigma_2 \equiv \forall x\forall y(Rxy \to Ryx), \quad \sigma_3 \equiv \forall x\forall y\forall z\big((Rxy \wedge Ryz) \to Rxz\big).$$

Konstruiere drei Modelle $\mathbf{M}_1$, $\mathbf{M}_2$, $\mathbf{M}_3$ mit Bereich $\{a, b, c\}$ sodass gilt:

(a) $\mathbf{M}_1 \models \neg\sigma_1 \wedge \sigma_2 \wedge \sigma_3$

(b) $\mathbf{M}_2 \models \sigma_1 \wedge \neg\sigma_2 \wedge \sigma_3$

(c) $\mathbf{M}_3 \models \sigma_1 \wedge \sigma_2 \wedge \neg\sigma_3$

Lösung: Sei $B := \{a, b, c\}$ der Bereich der Modelle $\mathbf{M}_1$, $\mathbf{M}_2$, $\mathbf{M}_3$ und gelte:

$$R^{\mathbf{M}_1} = \varnothing, \qquad R^{\mathbf{M}_2} = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle, \langle a, b\rangle\}, \qquad R^{\mathbf{M}_3} = B^2 \backslash \{\langle a, c\rangle, \langle c, a\rangle\}$$

Dann kann man schnell nachprüfen, dass alle Bedingungen erfüllt sind.

9. Definiere auf $\mathbb{N}$ eine binäre Relation "$\prec$" sodass gilt:

$$(\mathbb{N}, \prec) \models \mathsf{DLO}$$

Lösung: Für $n \in \mathbb{N}$ sei $k_n := \min\{k \in \mathbb{N} : n + 1 < 2^k\}$. Definiere

$$\begin{array}{rccc} \eta: & \mathbb{N} & \to & \mathbb{Q} \\ & n & \mapsto & \frac{2n - 2^{k_n} + 3}{2^{k_n}} \end{array}$$

und

$$n \prec m \iff \eta(n) < \eta(m)$$

wobei "$<$" die natürliche Ordnung auf $\mathbb{Q}$ ist. Wir zeigen zuerst, dass

$$\eta(\mathbb{N}) = \{\tfrac{2m+1}{2^k} \mid m, k \in \mathbb{N} \wedge 2m + 1 < 2^k\} :$$

$\subset$ Sei $n \in \mathbb{N}$ beliebig, dann gilt per Definition von k_n, dass $2^{k_n - 1} \leqslant n + 1 < 2^{k_n}$. Setzten wir nun $m := n + 1 - 2^{k_n - 1}$ und $k := k_n$, dann gilt offenbar $m \in \mathbb{N}$ und $2n - 2^{k_n} + 3 = 2m + 1$. Es bleibt also zu zeigen, dass $2n - 2^{k_n} + 3 < 2^{k_n}$. Aus $n + 1 < 2^{k_n}$ folgt $2(n + 1) - 2^{k_n} < 2^{k_n}$. Da 2 beide Seiten teilt, ist die Differenz der beiden Terme sicher mindestens 2 und deshlab gilt auch $2(n + 1) - 2^{k_n} + 1 < 2^{k_n}$.

$\supset$ Seien $m, k \in \mathbb{N}$ mit $2m+1 < 2^k$. Wir möchten ein $n \in \mathbb{N}$ finden mit $\eta(n) = \frac{2m+1}{2^k}$ mit $k = k_n$. Setze $n := m + 2^{k-1} - 1$ (da $k \geqslant 1$, wegen $2m+1 < 2^k$, ist $n \in \mathbb{N}$). Dann gilt

$$\eta(n) = \frac{2(m + 2^{k-1} - 1) - 2^k + 3}{k} = \frac{2m+1}{2^k},$$

wenn $k_n = k$. Es bleibt also zu zeigen, dass die letzte Gleichheit erfüllt ist und dies folgt aus

$$2^{k-1} \leqslant m + 2^{k-1} = n + 1 = m + 2^{k-1} \overset{2m+1<2^k}{<} 2^{k-1} + 2^{k-1} - \tfrac{1}{2} < 2^k.$$

Wir zeigen nun, dass "$<$" alle Axiome einer dichten linearen Ordnung erfüllt:

- DLO_0 ist erfüllt, da "$<$" in $\mathbb{Q}$ ebenfalls nicht reflexiv ist.
- DLO_1 ist erfüllt, da "$<$" in $\mathbb{Q}$ ebenfalls transitiv ist.
- DLO_2 ist erfüllt da "$<$" in $\mathbb{Q}$ eine dichte lineare Ordnung ist.
- Man sieht schnell, dass $\eta(\mathbb{N})$ und "$<$" eine dichte lineare Ordnung definiert. Deshalb ist DLO_3 erfüllt.
- Auch gibt es in $\eta(\mathbb{N})$ bezüglich "$<$" kein grösstes und kleinstes Element und deshalb ist auch DLO_4 wahr.

10. Für positive ganze Zahlen n sei $[n] := \{1, 2, \ldots, n\}$, sei S_n die Menge aller Bijektionen $f : [n] \to [n]$ und für Funktionen $f, g \in S_n$ sei $f \circ g(a) := f\big(g(a)\big)$ (für $a \in [n]$). Weiter sei $\iota : [n] \to [n]$ die Identität, d.h. $\iota(a) = a$ für alle $a \in [a]$.

Zeige, dass für $n \geqslant 3$, $\big(S_n, \iota, \circ\big)$ eine nicht-kommutative Gruppe ist.

Lösung: Wir müssen nachweisen, dass die Gruppenaxiome erfüllt sind:

- Wir wissen bereits, dass die Verknüpfung von Funktionen assoziativ ist. Also gilt dies auch für alle Elemente in S_n.
- Auch wissen wir, dass die Identitätsabbildung ι, (links-)neutral ist, wie dies auch allgemein der Fall ist bei Funktionen.
- Da die Funktionen in S_n bijektiv sind, können wir zu jeder Funktion $f \in S_n$ eine (links-)inverse Funktion $f^{-1} \in S_n$ konstruieren.

Somit ist $\big(S_n, \iota, \circ\big)$ eine Gruppe. Es bleibt zu zeigen, dass $\big(S_n, \iota, \circ\big)$ nicht kommutativ ist. Dazu betrachten wir die Transpositionen $\tau_{i,j}$, welche jeweils nur die Elemente i, j vertauschen und alle anderen Elemente von S_n auf sich selbst abbilden. Sei $n \geqslant 3$, dann gilt $\tau_{1,2}, \tau_{2,3} \in S_n$. Nun sind die beiden Funktionen aber nicht kommutativ, denn es gilt:

$$(\tau_{1,2} \circ \tau_{2,3})(2) = \tau_{1,2}(3) = 3 \neq 1 = \tau_{2,3}(1) = (\tau_{2,3} \circ \tau_{1,2})(2).$$

11. Sei $\mathbb{Z}[X]$ die Menge aller Polynome mit Koeffizienten in $\mathbb{Z}$.

Zeige, dass $(\mathbb{Z}[X], 0, 1, +, \cdot\,)$ ein kommutativer Ring ist, wobei $0, 1 \in \mathbb{Z}$ und $+, \cdot$ die Polynomaddition bzw. Polynommultiplikation bezeichnet.

Lösung: Wir müssen zeigen, dass $\mathbb{Z}[X]$ die Axiome der Ringtheorie erfüllt und die Multiplikation in $\mathbb{Z}[X]$ kommutativ ist. Wir können zwar keine multiplikativen Inversen von Polynomen in $\mathbb{Z}[X]$ bestimmen. Aber abgesehen von dem, können wir in $\mathbb{Z}[X]$ rechnen, wie in einem Körper, was man einfach zeigen kann. Die Axiome der Ringtheorie sind somit erfüllt.

12. Für eine positive ganze Zahl m sei $\mathbb{Z}_m := \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. Auf $\mathbb{Z}_m$ seien die beiden binären Operationen "$+$" und "$\cdot$" wie folgt definiert:

$$\bar{a} + \bar{b} = \bar{c} \;:\Longleftrightarrow\; m \text{ teilt } (a+b) - c$$
$$\bar{a} \cdot \bar{b} = \bar{c} \;:\Longleftrightarrow\; m \text{ teilt } (a \cdot b) - c$$

(a) Zeige, dass für alle $m \geqslant 2$, $\left(\mathbb{Z}_m, \bar{0}, \bar{1}, +, \cdot\right)$ ein kommutativer Ring ist.

(b) Zeige, dass für Primzahlen p, $\left(\mathbb{Z}_p, \bar{0}, \bar{1}, +, \cdot\right)$ ein Körper ist.
Hinweis: Zeige, dass für $\bar{a} \in \mathbb{Z}_p$, $\bar{a} \neq \bar{0}$, die Elemente $\bar{1}\cdot\bar{a}, \bar{2}\cdot\bar{a}, \ldots, \overline{p-1}\cdot\bar{a}$ paarweise verschieden und verschieden von $\bar{0}$ sind.

Lösung: Wir zeigen zuerst, dass die Addition in $\mathbb{Z}_m$ wohldefiniert ist: Seien $a, b \in \{0, 1, \ldots, m-1\}$. Falls $a + b < m$, dann setze $c := a + b$. Ansonsten muss gelten $m \leqslant a + b < 2m$ und wir können $c := a + b - m$ setzen. Dies zeigt die Existenz von einem solchen c. Für die Eindeutigkeit nehmen wir an, dass es $c_1, c_2 \in \{0, 1, \ldots, m-1\}$ gibt, sodass $m \; a + b - c_i$ für $i = 1, 2$ teilt. Ohne Einschränkung können wir $c_1 \leqslant c_2$ annehmen. Dann teilt m auch deren Differenz $c_2 - c_1 \in \{0, 1, \ldots, m-1\}$. Das heisst $c_2 - c_1 = 0$, also $c_1 = c_2$. Analog lässt sich auch zeigen, dass die Multiplikation in $\mathbb{Z}_m$ wohldefiniert ist.

(a) Wir zeigen, dass $\mathbb{Z}_m$ mit den beiden Operationen die Axiome eines kommutativen Rings erfüllt: Die Kommutativität der Addidtion sowie der Multiplikativität in $\mathbb{Z}_m$ wird vererbt von der Kommutativität der Addition und Multiplikation in $\mathbb{Z}$ (siehe Definitionen der beiden Verknüpfungen). Ähnliches gilt auch für die Assoziativität und die Distributivität. Ebenso sind $\bar{0}$ und $\bar{1}$ neutral für die Addition respektive die Multiplikation in $\mathbb{Z}_m$, da 0 und 1 auch neutral sind für die Addition und Multiplikation in $\mathbb{Z}$. Sei $a \in \{0, 1, \ldots, m-1\}$ beliebig, dann lässt sich das additive Inverse zu a konstruieren durch $m - a$.

(b) Es reicht zu zeigen, dass Inverse bezüglich Multiplikation existieren. Sei $\bar{a} \in \mathbb{Z}_p$, $\bar{a} \neq \bar{0}$ und $i, j \in \{0, 1, \ldots, m-1\}$ mit $\bar{i} \cdot \bar{a} = \bar{j} \cdot \bar{a}$ und sei ohne Einschränkung wieder $i \leqslant j$. Dann ist also $(\bar{j} - \bar{i}) \cdot \bar{a} = 0$, also wird das Produkt $(j - i) \cdot a$ von p geteilt. Da p eine Primzahl ist, teilt p somit auch $j - i$ und/oder a. Da $a, i, j \in \{0, 1, \ldots, p-1\}$ und $\bar{a} \neq 0$, kann a nicht von p geteilt werden und p teilt $j - i \geqslant 0$ nur, wenn $i = j$. Das heisst, die Elemente $\bar{0}\cdot\bar{a}, \bar{1}\cdot\bar{a}, \bar{2}\cdot\bar{a}, \ldots, \overline{p-1}\cdot\bar{a}$ sind in $\mathbb{Z}_p$ alle paarweise verschieden und somit muss es ein $k \in \{0, 1, \ldots, p-1\}$ geben mit $\bar{1} = \bar{k} \cdot \bar{a}$, was die Behauptung zeigt.

13. Auf der Menge $K = \{0, 1, \alpha, \beta\}$ werden zwei binäre Operationen "$+$" und "$\cdot$" wie folgt definiert:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Zeige, dass $\mathbb{K} = \big(K, 0, 1, +\, \cdot\big)$ ein Modell für KT ist, d.h. $\mathbb{K}$ ist eine Körper mit vier Elementen.

Lösung: Wir zeigen, dass $\mathbb{K}$ die Axiome der Körpertheorie erfüllt: Die Kommutativität der Addition und Multiplikation folgt aus den Diagonalsymmetrien (Diagonalen von oben links bis unten rechts) der beiden Tabellen. Dass 0 und 1 links-neutrale Elemente sind bezüglich der Addidtion repektive der Multiplikation, lässt sich an der ersten Spalte der Addidtionstabelle beziehungsweise an der zweiten Spalte der Multiplikationstabelle ableiten. Dass links-Inverse zu jedem Element in $\mathbb{K}$ bezüglich Addidtion existiert, folgt daraus, dass in jeder Spalte der Addidtionstabelle eine 1 steht (das Element ganz links aussen von der 1 in der Tabelle wäre dann das passende links-Inverse zum betrachteten Element oben in der Tabelle). Betrachten wir die Multiplikationstabelle ohne die 0, so können wir Analoges auch dort feststellen. Um die Assoziativität zu zeigen, müsste man theoretisch alle Kombinationen durchprobieren. Vereinfachen lässt es sich, indem man nur die Kombinationen durchgeht, welche bei der Addidtion keine 0 und bei der Multiplikation keine 1 enthält (diese können weggelassen werden da $0, 1$ jeweils neutral sind). Das wären dann immerhin noch je 27 Kombinationen pro Tabelle (ein paar können auch noch ausgelassen werden), welche man durch einsetzten überprüfen kann.

14. Sei $\mathsf{T}_0 = \{\sigma_0, \sigma_1, \sigma_2\}$ eine Theorie mit der Signatur $\mathscr{L}_{\mathsf{GT}}$, wobei gilt:

$$\begin{aligned}
\sigma_0 &\equiv \forall x \forall y \forall z \big(x \circ (y \circ z) = (x \circ y) \circ z\big) \\
\sigma_1 &\equiv \forall x (\mathsf{e} \circ x = x) \\
\sigma_2 &\equiv \forall x \exists y (x \circ y = \mathsf{e})
\end{aligned}$$

Die $\mathscr{L}_{\mathsf{GT}}$-Struktur $\mathbf{M}$ mit Bereich $A = \{\alpha, \beta\}$ sei definiert durch $\mathsf{e}^{\mathbf{M}} := \alpha$ und $x \circ y := y$ für alle $x, y \in A$.

(a) Zeige: $\mathbf{M} \models \mathsf{T}_0$.

(b) Zeige: $\mathbf{M} \not\models \mathsf{GT}$.

Bemerkung: Ist $\mathbb{G}$ eine Gruppe, so gilt $\mathbb{G} \models \mathsf{T}_0$, d.h. die Axiome von T_0 können aus GT bewiesen werden. Andererseits folgt aus (b), dass die Gruppenaxiome GT nicht aus T_0 bewiesen werden können.

Lösung:

(a) Anhand der Bedingung $\forall x \forall y (x \circ y = y)$ können wir für die $\mathscr{L}_{\mathsf{GT}}$-Struktur $\mathbf{M}$ eine Verknüpfungstafel erstellen:

$\circ$	α	β
α	α	β
β	α	β

Wir müssen nun zeigen, dass $\sigma_0, \sigma_1, \sigma_2$ erfüllt sind, wobei $\mathsf{e}^{\mathbf{M}} := \alpha$:

σ_0: Die Assoziativität muss erfüllt sein, denn es gilt für $x, y, z \in \{\alpha, \beta\}$:

$$x \circ (y \circ z) = y \circ z = z = (x \circ y) \circ z$$

σ_1: Da der Bereich von $\mathbf{M}$ nur aus zwei Elementen besteht, sieht man sofort:

$$\alpha \circ \alpha = \alpha$$
$$\alpha \circ \beta = \beta$$

σ_2: Auch hier lässt sich die Bedingung sehr schnell nachweisen:

$$\alpha \circ \alpha = \alpha$$
$$\beta \circ \alpha = \alpha$$

(b) Angenommen es gilt $\mathbf{M} \models \mathsf{GT}$, dann muss die $\mathscr{L}_{\mathsf{GT}}$-Struktur $\mathbf{M}$ alle Gruppenaxiome erfüllen. Dies ist aber nicht der Fall, denn β hat kein links-Inverses, was man an der Verknüpfungstafel oben leicht verifizieren kann.