1. AXIOMENSYSTEME UND SEMI-FORMALE BEWEISE

In diesem Kapitel werden die Axiome einiger Theorien aufgelistet und es wird der Begriff eines *semi-formalen* Beweises eingeführt.

AXIOMENSYSTEME

Gruppentheorie GT. Die Signatur der Gruppentheorie ist $\mathscr{L}_{\mathsf{GT}} = \{\mathtt{e}, \circ\}$, wobei $\mathtt{e}$ ein Konstantensymbol und $\circ$ ein 2-stelliges Funktionssymbol ist.

Die Axiome der Gruppentheorie sind:

GT_0:	$\forall x \forall y \forall z \big(x \circ (y \circ z) = (x \circ y) \circ z\big)$	($\circ$ ist *assoziativ*)
GT_1:	$\forall x (\mathtt{e} \circ x = x)$	($\mathtt{e}$ ist *links-neutral*)
GT_2:	$\forall x \exists y (y \circ x = \mathtt{e})$	(jedes Element hat ein *links-Inverses*)

Strenggenommen sind die Erläuterungen in den Klammern nicht korrekt: Zum Beispiel kann das Funktionssymbol $\circ$ als *Symbol* nicht assoziativ sein. Erst, wenn das Funktions*symbol* $\circ$ in einem *Modell* $\mathbf{M}$ als 2-stellige *Funktion* $\circ^{\mathbf{M}} : A \times A \to A$ interpretiert wird, kann die Funktion $\circ^{\mathbf{M}}$ assoziativ sein, und das ist, was mit GT_0 gemeint ist.

Es sei nochmals erwähnt, dass es auf der syntaktischen (oder formalen) Ebene, auf der wir uns befinden, weder Konstanten, noch Funktionen oder Relationen gibt, sondern nur verschiedene, bedeutungslose Typen von Symbolen. Es gibt auch kein wahr und falsch, sondern nur syntaktisch korrekt geformte Terme und Formeln. Erst auf der semantischen Ebene, die im nächsten Kapitel behandelt wird, werden den Termen Objekte zugeordent, den Funktionssymbolen Funktionen, und den Relationssymbolen Relationen.

Ringtheorie RT. Die Signatur der Ringtheorie (für Ringe mit 1) ist $\mathscr{L}_{\mathsf{RT}} = \{\mathtt{0}, \mathtt{1}, +, \cdot\}$, wobei $\mathtt{0}$ und $\mathtt{1}$ Konstantensymbole sind und $+, \cdot$ zwei 2-stellige Funktionssymbole sind.

Die Axiome der Ringtheorie (für Ringe mit 1) sind:

RT_0:	$\forall x \forall y \forall z \big(x + (y + z) = (x + y) + z\big)$	($+$ ist *assoziativ*)
RT_1:	$\forall x \forall y (x + y = y + x)$	($+$ ist *kommutativ*)
RT_2:	$\forall x (\mathtt{0} + x = x)$	($\mathtt{0}$ ist *links-neutral* bzgl. $+$)
RT_3:	$\forall x \exists y (y + x = \mathtt{0})$	(*links-Inverse* bzgl. $+$)
RT_4:	$\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$	($\cdot$ ist *assoziativ*)
RT_5:	$\forall x (\mathtt{1} \cdot x = x \wedge x \cdot \mathtt{1} = x)$	($\mathtt{1}$ ist *neutral* bzgl. $\cdot$)
RT_6:	$\forall x \forall y \forall z \big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$	($\cdot$ ist *links-distributiv* über $+$)
RT_7:	$\forall x \forall y \forall z \big((x + y) \cdot z = (x \cdot z) + (y \cdot z)\big)$	($\cdot$ ist *rechts-distributiv* über $+$)

Lässt man RT_5 weg, so erhält man auf der semantischen Ebene Ringe ohne 1, und verlangt man zusätzlich RT_8: $\forall x \forall y (x \cdot y = y \cdot x)$, so erhält man auf der semantischen Ebene *kommutative Ringe* (mit bzw. ohne 1).

Da die Operation $+$ mit RT_1 kommutativ ist, ist $\mathtt{0}$ auch rechts-neutral (also neutral) bzgl. $+$ und jedes Element hat bzgl. $+$ ein rechts-Inverses (also ein Inverses).

Körpertheorie KT**.** Die Signatur der Körpertheorie ist $\mathscr{L}_{\mathsf{KT}} = \{\mathtt{0}, \mathtt{1}, +, \cdot\}$, wobei $\mathtt{0}$ und $\mathtt{1}$ Konstantensymbole sind und $+, \cdot$ zwei 2-stellige Funktionssymbole sind.

Die Axiome der Körpertheorie sind:

KT_0:	$\forall x \forall y \forall z \big(x + (y + z) = (x + y) + z\big)$	($+$ ist *assoziativ*)
KT_1:	$\forall x \forall y (x + y = y + x)$	($+$ ist *kommutativ*)
KT_2:	$\forall x (\mathtt{0} + x = x)$	($\mathtt{0}$ ist *link-neutral* bzgl. $+$)
KT_3:	$\forall x \exists y (y + x = \mathtt{0})$	(*links-Inverse* bzgl. $+$)
KT_4:	$\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$	($\cdot$ ist *assoziativ*)
KT_5:	$\forall x \forall y (x \cdot y = y \cdot x)$	($\cdot$ ist *kommutativ*)
KT_6:	$\forall x (\mathtt{1} \cdot x = x)$	($\mathtt{1}$ ist *link-neutral* bzgl. $\cdot$)
KT_7:	$\forall x \exists y (x \neq \mathtt{0} \rightarrow y \cdot x = \mathtt{1})$	(*links-Inverse* bzgl. $\cdot$ für $x \neq \mathtt{0}$)
KT_8:	$\forall x \forall y \forall z \big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$	($\cdot$ ist *links-distributiv* über $+$)
KT_9:	$\mathtt{0} \neq \mathtt{1}$	($\mathtt{0}$ ist verschieden von $\mathtt{1}$)

Da die Operationen $+$ und $\cdot$ mit KT_1 bzw. KT_5 kommutativ sind, sind links-neutrale Elemente auch rechts-neutral (also neutral), links-Inverse auch rechts-Inverse (also Inverse), und $\cdot$ ist auch *rechts-distributiv* über $+$.

Dichte Lineare Ordnungen DLO**.** Die Signatur der Theorie der dichten linearen Ordnungen ist $\mathscr{L}_{\mathsf{DLO}} = \{<\}$, wobei $<$ ein 2-stelliges Relationssymbol ist.

Die Axiome der Theorie der dichten linearen Ordnungen sind:

DLO_0:	$\forall x \neg (x < x)$	($<$ ist nicht *reflexiv*)
DLO_1:	$\forall x \forall y \forall z \big((x < y \wedge y < z) \rightarrow x < z\big)$	($<$ ist *transitiv*)
DLO_2:	$\forall x \forall y \big(x < y \vee x = y \vee y < x\big)$	($<$ definiert eine *lineare* Ordnung)
DLO_3:	$\forall x \forall y \exists z \big(x < y \rightarrow (x < z \wedge z < y)\big)$	($<$ definiert eine *dichte* Ordnung)
DLO_4:	$\forall x \exists y \exists z \big(y < x \wedge x < z\big)$	(keine grössten bzw. kleinsten Elemente)

Peano-Arithmetik PA**.** Die Signatur der Peano-Arithmetik ist $\mathscr{L}_{\mathsf{PA}} = \{\mathtt{0}, \mathtt{s}, +, \cdot\}$, wobei das Symbol $\mathtt{0}$ ein Konstantensymbol ist, $\mathtt{s}$ ein 1-stelliges Funktionssymbol ist, und $+, \cdot$ zwei 2-stellige Funktionssymbole sind.

Die Axiome der Peano-Arithmetik sind:

PA_0:	$\neg \exists x (\mathtt{s}x = \mathtt{0})$	($\mathtt{0}$ ist kein Nachfolger)
PA_1:	$\forall x \forall y (\mathtt{s}x = \mathtt{s}y \rightarrow x = y)$	($\mathtt{s}$ ist *injektiv*)
PA_2:	$\forall x (x + \mathtt{0} = x)$	(definiert $x + \mathtt{0}$)
PA_3:	$\forall x \forall y (x + \mathtt{s}y = \mathtt{s}(x + y))$	(definiert $x + \mathtt{s}y$)
PA_4:	$\forall x (x \cdot \mathtt{0} = \mathtt{0})$	(definiert $x \cdot \mathtt{0}$)
PA_5:	$\forall x \forall y (x \cdot \mathtt{s}y = (x \cdot y) + x)$	(definiert $x \cdot \mathtt{s}y$)

Sei φ eine $\mathscr{L}_{\mathsf{PA}}$-Formel und ν eine Variable mit $\nu \in \mathrm{frei}(\varphi)$:

PA_6: $\big(\varphi(\mathtt{0}) \wedge \forall \nu (\varphi(\nu) \rightarrow \varphi(\mathtt{s}\nu))\big) \rightarrow \forall \nu \varphi(\nu)$

Beachte, dass PA_6 (im Gegensatz zu den Axiomen PA_0–PA_5) nicht ein einzelnes Axiom ist, sondern ein Axiomenschema, denn für jede $\mathscr{L}_{\mathsf{PA}}$-Formel φ mit einer freien Variablen erhalten wir eine Form von PA_6. Das Axiomenschema PA_6 wird **Induktions-Axiom** genannt und wird für Induktionsbeweise benutzt. Weil PA_6 ein Axiomenschema ist, besteht das Axiomensystem PA der Peano-Arithmetik aus unendlich vielen Axiomen.

Semi-formale Beweise

Wie schon erwähnt werden formale Beweise relativ schnell sehr lang. Das liegt daran, dass in einem formalen Beweis nicht nur die relevanten, theorieabhängigen Zusammenhänge vorkommen, welche durch die nicht-logischen Axiome gegeben sind, sondern auch alle inner-logischen Strukturen, welche aus den logischen Axiomen folgen. Wenn wir nun in einem formalen Beweis alle Schritte, bei denen wir mit logischen Axiomen gewisse Formeln umgeformt haben, weglassen, so beruhen die ausgeführten Schritte im Wesentlichen nur noch auf den nicht-logischen Axiomen. Wir nennen solche Beweise **semi-formale Beweise** (diese Definition ist naturgemäss ebenfalls semi-formal).

Als Beispiel für einen semi-formalen Beweis zeigen wir $\mathsf{PA} \vdash \mathtt{s0} + \mathtt{s0} = \mathtt{ss0}$ (vgl. mit Aufgabe 4):

$$\underbrace{\mathtt{s0} + \mathtt{s0}}_{=\mathtt{s0}+\mathtt{s(0)}} \overset{\mathsf{PA}_3}{=} \mathtt{s}(\underbrace{\mathtt{s0} + \mathtt{0}}_{=\mathtt{s0}}) \overset{\mathsf{PA}_2}{=} \mathtt{ss0}$$

Als Beispiel für einen semi-formalen Induktionsbeweis zeigen wir $\mathsf{PA} \vdash \forall x\big(\mathtt{ss0}\cdot x = x+x\big)$:

- Wir definieren: $\varphi(x) :\equiv \mathtt{ss0} \cdot x = x + x$
- $\mathsf{PA} \vdash \varphi(\mathtt{0})$: $\mathtt{ss0} \cdot x \overset{\mathsf{PA}_4}{=} \mathtt{0} \overset{\mathsf{PA}_2}{=} \mathtt{0} + \mathtt{0}$
- $\mathsf{PA} \vdash \varphi(x) \to \varphi(\mathtt{s}x)$: Wir nehmen an, dass $\mathtt{ss0} \cdot x = x + x$ gilt, verwenden den bereits bewiesenen Satz $\mathtt{ss0} = \mathtt{s0} + \mathtt{s0}$, und verwenden implizit, dass $+$ assoziativ und kommutativ ist (siehe Aufgaben 6.(b) und 6.(d)).

$$\mathtt{ss0} \cdot \mathtt{s}x \overset{\mathsf{PA}_5}{=} (\underbrace{\mathtt{ss0} \cdot x}_{=x+x}) + \underbrace{\mathtt{ss0}}_{=\mathtt{s0}+\mathtt{s0}} =$$
$$(x + \mathtt{s0}) + (x + \mathtt{s0}) \overset{\mathsf{PA}_3}{=} \mathtt{s}(x + \mathtt{0}) + \mathtt{s}(x + \mathtt{0}) \overset{\mathsf{PA}_2}{=} \mathtt{s}x + \mathtt{s}x$$

- Wir haben somit $\mathsf{PA} \vdash \varphi(\mathtt{0})$ und $\mathsf{PA} \vdash \forall x\big(\varphi(x) \to \varphi(\mathtt{s}x)\big)$, woraus wir (mit L_5) schliessen
$$\mathsf{PA} \vdash \varphi(\mathtt{0}) \wedge \forall x\big(\varphi(x) \to \varphi(\mathtt{s}x)\big),$$
und mit dem Induktionsaxiom PA_6 erhalten wir schliesslich:
$$\mathsf{PA} \vdash \forall x\big(\mathtt{ss0} \cdot x = x + x\big)$$