2. Aussagenlogik (Vorlesungen 3 & 4)

2.1. **Boolsche Algebren.** Ein besonderer Fall einer algebraischen Theorie, die für uns wichtig wird in den folgenden Kapiteln, ist die Theorie der Boolschen Algebren. Die Boolschen Algebren haben das funktionale Vokabular

$$\{\top, \bot, \neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$$

wobei $\alpha(\top) = \alpha(\bot) = 0$, $\alpha(\neg) = 1$ und $\alpha(\wedge) = \alpha(\vee) = \alpha(\rightarrow) = \alpha(\leftrightarrow) = 2$. Die zweielementige Menge $2 = \{0, 1\}$ ist eine Struktur für das funktionale Vokabular der Boolschen Algebren durch die folgenden Interpretationen:

$$\begin{aligned}
\top_2 &= 1 \\
\bot_2 &= 0 \\
\neg_2(a) &= 1 - a \\
\wedge_2(a, b) &= \min\{a, b\} \\
\vee_2(a, b) &= \max\{a, b\} \\
\rightarrow_2(a, b) &= 0 \Leftrightarrow a = 1 \text{ und } b = 0 \\
\leftrightarrow_2(a, b) &= 1 \Leftrightarrow a = b.
\end{aligned}$$

Wir denken uns, dass 1 und 0 für 'wahr' und 'falsch' stehen, $\neg$ für 'nicht', $\wedge$ und $\vee$ für 'und' und 'oder', und $\rightarrow$ für 'impliziert'. Eine Boolsche Algebra ist ein (Ω, E)-Modell, wobei E aus allen Gleichungen besteht, die in 2 erfüllt sind.

Im Folgenden schreiben wir in der für Binäroperationen gebräuchlichen Weise $x \wedge y$ anstatt $\wedge(x, y)$. Wir bemerken, dass die obige Präsentation nicht sehr effizient ist, denn E enthält die folgenden Gleichungen:

$$\begin{gathered}
(\top \equiv (\bot \rightarrow \bot)) \\
(\neg x \equiv (x \rightarrow \bot)) \\
((x \vee y) \equiv (\neg x \rightarrow y)) \\
((x \wedge y) \equiv \neg(\neg x \vee \neg y)) \\
((x \leftrightarrow y) \equiv ((x \rightarrow y) \wedge (y \rightarrow x)))
\end{gathered}$$

Insbesondere ist jeder Ω-Term $\sim_E$-äquivalent zu einem Term, der nur die Funktionssymbole $\rightarrow$ und $\bot$ benutzt. Ab sofort werden wir also $\{\bot, \rightarrow\}$ as das funktionale Vokabular für Boolsche Algebren betrachten. Wir beobachten auch, dass $(s \equiv t) \in E$ genau dann, wenn $((s \leftrightarrow t) \equiv \top) \in E$. Also können wir unsere Aufmerksamkeit auf Gleichungen der Form $(t \equiv \top)$ beschränken. Ein Term t heißt *Tautologie* (oder *allgemeingültig*), falls $(t \equiv \top) \in E$ (äquivalent, falls $t_2 \colon 2^n \rightarrow 2$ die konstante Einsfunktion ist, wobei n die Zahl verschiedener Variablen von t bezeichnet).

Wir bemerken, dass die folgenden Terme Tautologien sind:

- $t = (x \rightarrow (y \rightarrow x))$ (Wahrheit wird immer impliziert).
- $s = (x \rightarrow (y \rightarrow z)) \rightarrow ((x \rightarrow y) \rightarrow (x \rightarrow z))$
- $u = (((x \rightarrow \bot) \rightarrow \bot) \rightarrow x)$ (Satz vom ausgeschlossenen Dritten).

(Die letzte Tautologie ist also $\neg\neg x \rightarrow x$). Um nachzuprüfen, dass zum Beispiel t wirklich eine Tautologie ist, bemerken wir, dass t ein Term in zwei Variablen x und y ist. Also ist $t_2 \colon 2^2 \rightarrow 2$, und wir müssen vier verschiedene Fälle für x und y wie folgt prüfen.

x	y	$(y \rightarrow x)$	$(x \rightarrow (y \rightarrow x))$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

Die anderen Fälle gehen ähnlich. Im Folgenden werden wir diese *aussagenlogischen Verknüpfungen* im Detail betrachten.

2.2. **Aussagenlogik.** Für den Rest dieses Kapitels ändern wir unsere Notation leicht ab, und verwenden nun eine feste Menge $P = \{p, q, r, \ldots\}$ als Variablen, die wir auch als *Elementaraussagen* bezeichnen. Wir betrachten das funktionelle Vokabular $\Omega = \{\perp, \to\}$ für Boolsche Algebren. Eine *zusammengesetzte Aussage* ist ein Ω-Term über der Menge P von Elementaraussagen. Wir können uns denken, dass eine solche zusammengesetzte Aussage t ein Element der freien Boolschen Algebra $F_\Omega(P)$ ist. Die Elemente $0, 1$ der Fundamentalalgebra 2 nennen wir auch *Wahrheitswerte*.

Eine *Belegung* von P ist eine Funktion $v\colon P \to 2$. Dies ist also eine Funktion, die jeder unserer Elementaraussagen einen Wahrheitswert (1 oder 0, also wahr oder falsch) zuordnet. Nach Theorem 1.7 über freie Ω-Strukturen lässt sich v eindeutig fortsetzen zu einer Funktion $\overline{v}\colon F_\Omega P \to 2$, die jeder zusammengesetzten Aussage einen eindeutiger Wahrheitswert zuordnet.

Definition 2.1 (Semantisches Folgern)**.** *Es sei $S \subset F_\Omega(P)$ eine Menge von Aussagen und t eine einzelne Aussage. Wir sagen, dass t* semantisch aus S folgt *(geschrieben: $S \models t$), wenn für jede Belegung v von P mit $\overline{v}(s) = 1$ für alle $s \in S$ gilt, dass $\overline{v}(t) = 1$.*

Es sei $S \subset F_\Omega(P)$ eine Menge an Aussagen. Wir sagen, dass S *erfüllbar ist*, wenn eine Belegung v existiert, so dass $\overline{v}(s) = 1$ für alle $s \in S$. Ein Term t ist also genau dann eine Tautologie, wenn $\emptyset \models t$. In diesem Fall schreiben wir auch $\models t$.

Bemerkung 2.2. *Für endliches S ist es einfach zu entscheiden, ob $S \models t$. Man betrachte eine Wahrheitstabelle für die Aussagen in $S \cup \{t\}$ und streiche alle Zeilen in denen $\overline{v}(s) = 0$ vorkommt für ein $s \in S$. Dann gilt $S \models t$ genau dann, wenn nur noch Einsen übrig bleiben.*

Ein wichtiges Beispiel für eine semantische Folgerung ist $\{p, (p \to q)\} \models q$, wie die folgende Tabelle zeigt.

p	q	$(p \to q)$
~~0~~	~~0~~	~~1~~
~~0~~	~~1~~	~~1~~
~~1~~	~~0~~	~~0~~
1	1	1

Wir kommen jetzt zum Konzept eines formalen Beweises. Unsere *Axiome* sind Substitutionen der folgenden drei Aussagen:

(1) $(p \to (q \to p))$,
(2) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$,
(3) $(\neg\neg p \to p)$,

welche alle, wie wir im letzten Kapitel eingesehen haben, Tautologien sind. Desweiteren haben wir die folgende Ableitungsregel (Modus Ponens): Aus p und $(p \to q)$ können wir q ableiten (und wiederum gilt diese Regel für alle Substitutionen).

Definition 2.3 (Formale Ableitung, Syntaktische Implikation)**.** *Es sei $S \subset F_\Omega(P)$ eine Menge von Aussagen und t eine einzelne Aussage. Eine formale Ableitung von t aus S ist eine Folge von Aussagen $t_0, t_1, \ldots, t_n$ mit $t_n = t$, sodass jedes t_i*

- *ein Axiom ist, oder*
- *ein Element aus S ist, oder*
- *durch Anwendung des Modus Ponens aus zwei früheren t_k, t_j erhalten wurde; also wenn $k, j < i$ existieren mit $t_j = (t_k \to t_i)$.*

In diesem Fall sagen wir, dass t syntaktisch aus S folgt, *und schreiben $S \vdash t$.*

In einer solchen formalen Ableitung nennen wir S auch die Menge unserer *Prämissen.* Im Fall $\emptyset \vdash t$ schreiben wir auch $\vdash t$, und nennen t ein *Theorem* (der Aussagenlogik).

Beispiel 2.4. $\{(p \to q), (q \to r)\} \vdash (p \to r)$.

Lösung. Wir geben eine formale Ableitung an.

1.	$(p \to (q \to r)) \to ((p \to q) \to (p \to r))$	(Axiom (2))
2.	$(q \to r)$	(Prämisse)
3.	$((q \to r) \to (p \to (q \to r)))$	(Axiom (1))
4.	$(p \to (q \to r))$	(MP aus 2 und 3)
5.	$((p \to q) \to (p \to r))$	(MP aus 1 und 4)
6.	$(p \to q)$	(Prämisse)
7.	$(p \to r)$	(MP aus 5 und 6) □

Beispiel 2.5. $\vdash (p \to p)$.

Lösung. Wir geben eine formale Ableitung an.

1.	$(p \to ((p \to p) \to p) \to ((p \to (p \to p)) \to (p \to p)))$	(Axiom (2))
2.	$(p \to ((p \to p) \to p))$	(Axiom (1))
3.	$((p \to (p \to p)) \to (p \to p))$	(MP aus 1 und 2)
4.	$(p \to (p \to p))$	(Axiom (1))
5.	$(p \to p)$	(MP aus 3 und 4) □

2.3. **Der Vollständigkeitssatz der Aussagenlogik.**

Theorem 2.6 (Korrektheitssatz / Soundness Theorem)**.** *Wenn $S \vdash t$, dann $S \models t$.*

Beweis. Es sei S die Menge unsere Prämissen. Wenn $S \vdash t$, so gibt es also eine formale Ableitung $t_0, t_1, \ldots, t_n = t$. Wir zeigen nun durch Induktion nach i, dass $S \models t_i$.

- Falls t_i ein Axiom ist, so gilt $\models t_i$, und deswegen erst recht $S \models t_i$,
- falls t_i eine Prämisse ist, dann gilt $S \models t_i$ trivialerweise, und
- falls t_i durch (MP) gewonnen wurde, so existieren $k, j < i$ mit $t_k = (t_j \to t_i)$. Nach Induktionshypothese gilt $S \models t_j$ und $S \models (t_j \to t_i)$. Da $\{t_j, (t_j \to t_i)\} \models t_i$ gilt auch $S \models t_i$.[3] □

Insbesondere ist jedes Theorem also eine Tautologie. Als nächstes wollen wir die Umkehrung zeigen, also dass die Relationen $\models$ und $\vdash$ wirklich übereinstimmen (dies ist der sogenannte *Vollständigkeitssatz der Aussagenlogik*). Ein nützlicher Schritt ist dabei das folgende Resultat.

Theorem 2.7 (Deduktionstheorem)**.** *Es gilt $S \vdash (s \to t)$ genau dann, wenn $S \cup \{s\} \vdash t$.*

Beweis. Zuerst die Hinrichtung. Wir nehmen an, wir haben eine formale Ableitung von $(s \to t)$ aus S. Dann füge der Ableitung die Prämisse s hinzu, und wende schließlich Modus Ponens auf die letzten zwei Elemente unserer Ableitung an, um t zu erhalten. Dies ist dann eine formale Ableitung von t aus $S \cup \{s\}$.

Für die Rückrichtung nehmen wir an, es existiert eine formale Ableitung $t_0, t_1, \ldots, t_n = t$ von t aus $S \cup \{s\}$. Wir zeigen mithilfe von Induktion nach i, dass $S \vdash (s \to t_i)$ for all $i \leq n$. Für $i = n$ ist das die zu zeigende Aussage.

[3] Ausführlich: Für jede Belegung, die S erfüllt, ist auch $\{t_j, (t_j \to t_i)\}$ erfüllt. Aber für jede Belegung, die $\{t_j, (t_j \to t_i)\}$ erfüllt, ist auch t_i erfüllt, wie wir oben gesehen haben.

- Falls t_i ein Axiom ist oder ein Element von S, so gilt

1.	t_i	(Axiom oder Prämisse)
2.	$t_i \to (s \to t_i)$	(Axiom (1))
3.	$(s \to t_i)$	(MP)

- Falls $t_i = s$, beobachten wir, dass $(s \to s)$ gemäß Beispiel 2.5 ein Theorem ist.
- Falls t_i aus t_j, t_k (für $j, k < i$) durch Modus Ponens gewonnen wurde, so haben wir ohne Einschränkung, dass $t_k = (t_j \to t_i)$. Unsere Induktionsannahme besagt, dass wir formale Ableitungen für $(s \to t_j)$ und für $(s \to (t_j \to t_i))$ haben. An diese beiden Ableitungen fügen wir dann die folgenden Zeilen an:

1.	$(s \to (t_j \to t_i)) \to ((s \to t_j) \to (s \to t_i))$	(Axiom (2))
2.	$((s \to t_j) \to (s \to t_i))$	(MP + Induktionsannahme)
3.	$(s \to t_i)$	(MP + Induktionsannahme)

Somit existiert eine formale Ableitung von $(s \to t_i)$ aus S. □

Lemma 2.8. *Wenn $S \models \bot$, dann $S \vdash \bot$.*

Eine Menge S an Aussagen nennen wir auch eine *Theorie*. Wir sagen eine Theorie S ist *widerspruchsvoll*, falls $S \vdash \bot$. Andernfalls heißt S *widerspruchsfrei*. Die Kontraposition dieses Lemmas besagt also, dass jede widerspruchsfreie Theorie erfüllbar ist. Bevor wir dieses Lemma beweisen, wollen wir sehen, dass es den Vollständigkeitssatz impliziert.

Theorem 2.9 (Vollständigkeitssatz der Aussagenlogik)**.** *Es gilt $S \models t$ genau dann, wenn $S \vdash t$.*

Beweis. Die Rückrichtung ist der Korrektheitsatz 2.6. Für die andere Richtung nehmen wir an, dass $S \models t$. Da $\{t, \neg t\} \models \bot$ folgt, dass $S \cup \{\neg t\} \models \bot$. Aus Lemma 2.8 folgt $S \cup \{\neg t\} \vdash \bot$, und aus dem Deduktionstheorem folgt $S \vdash (\neg t \to \bot)$, d.h. $S \vdash \neg\neg t$.

Aber dann können wir eine formale Ableitung von $\neg\neg t$ aus S aufschreiben, und die Zeilen

$(\neg\neg t \to t)$	(Axiom (3))
t	(MP)

anfügen. Somit haben wir gezeigt, dass $S \vdash t$. □

Beweis von Lemma 2.8. Wir müssen zeigen, dass jede widerspruchsfreie Theorie erfüllbar ist. Sei also S eine widerspruchsfrei Theorie. Wir beweisen erst folgende Hilfsbehauptungen:

(a) S ist genau dann widerspruchsfrei, wenn jede endliche Teilmenge von S widerspruchsfrei ist.
(b) Ist S widerspruchsfrei und t eine Aussage, so ist mindestens eine der Mengen $S \cup \{t\}$ oder $S \cup \{\neg t\}$ widerspruchsfrei.
(c) Ist S widerspruchsfrei, so gibt es eine maximal widerspruchsfreie Theorie $\overline{S}$ mit $S \subseteq \overline{S}$.
(d) Jede maximale widerspruchsfreie Menge S ist deduktiv abgeschlossen, i.e $S \vdash t$ impliziert schon $t \in S$.

Zu (a) '⇒'. Gibt eine endliche Teilmenge $S' \subset S$ mit $S' \vdash \bot$, dann folgt auch $S \vdash \bot$, denn dieselbe formale Ableitung funktioniert.

'⇐'. Gibt eine umgekehrt eine formale Ableitung von $\bot$ aus S, so werden, da formale Ableitungen aber nur endlich viele Zeilen haben können, auch nur endlich viele Prämissen $S' \subset S$ in dieser Ableitung erwähnt. Dann ist dieselbe Ableitung für $S \vdash \bot$ aber auch eine Ableitung für $S' \vdash \bot$.

(b) Angenommen, $S \cup \{t\} \vdash \bot$. Nach dem Deduktionstheorem 2.7 gilt dann $S \vdash (t \to \bot)$, also $S \vdash \neg t$. Es folgt, dass $S \cup \{\neg t\}$ widerspruchsfrei ist, denn in einer potentiellen Ableitung von $\bot$ aus $S \cup \{\neg t\}$ könnte die Prämisse $\neg t$ ja durch eine Ableitung aus S ersetzt werden.

(c) Wir führen den Beweis für den Fall, dass P, die Menge der primitiven Aussagen, abzählbar ist.[4] Es ist leicht einzusehen, dass mit P auch die Menge $F_\Omega(P)$ der zusammengesetzten Aussagen abzählbar ist. Somit können wir also eine Aufzählung $F_\Omega(P) = \{t_n : n \in \mathbb{N}\}$ finden. Wir setzen $S_0 = S$, und falls S_n schon definiert ist, setzen wir

$$S_{n+1} = \begin{cases} S_n \cup \{t_n\} & \text{falls widerspruchsfrei,} \\ S_n \cup \{\neg t_n\} & \text{sonst.} \end{cases}$$

Nach (2) ist somit jedes S_n widerspruchsfrei. Setze $\overline{S} = \bigcup_{n\in\mathbb{N}} S_n$. Mit (1) ist leicht einzusehen, dass $\overline{S}$ widerspruchsfrei ist. Sie ist auch maximal widerspruchsfrei, denn für jede Aussage t die nicht in $\overline{S}$ enthalten ist, ist ja $\neg t \in S$, und da $\{t, \neg t\} \vdash \bot$ folgt leicht, dass $\overline{S} \cup \{t\} \vdash \bot$, also können wir t nicht hinzufügen, ohne Widerspruchsfreiheit zu verlieren.

(d) Wenn $S \vdash t$ so ist $S \cup \{t\}$ widerspruchsfrei, denn in jedem Beweis von $\bot$ aus $S \cup \{t\}$ können wir die Prämisse t durch den Beweis $S \vdash t$ ersetzen. Aber dann folgt $t \in S$ aus der Maximalität von S. Somit sind alle Hilfsbehauptungen bewiesen.

Wir benutzen nun (c) und eine maximale widerspruchsfreie Theorie $\overline{S} \supseteq S$ zu finden. Wir definieren

$$\overline{v} \colon F_\Omega(P) \to 2,\ t \mapsto \begin{cases} 1 & \text{if } t \in \overline{S} \\ 0 & \text{sonst.} \end{cases}$$

Diese Funktion erfüllt anscheinend, dass $\overline{s} = 1$ für alle $s \in S \subset \overline{S}$. Es bleibt zu zeigen, dass $\overline{v}$ von einer Belegung von P kommt (dies würde zeigen, dass S erfüllbar ist, was ja unser Ziel war). Mit anderen Worten, wir müssen zeigen, dass $\overline{v}$ eine $\{\to, \bot\}$-Homomorphismus ist. Da $\bot \notin \overline{S}$ folgt, dass $\overline{v}(\bot) = 0$. Es reicht also zu zeigen, dass

$$\overline{v}(s \to t) = (\overline{v}(s) \to_2 \overline{v}(t)).$$

Dazu unterschieden wir die folgenden Fälle:

(i) $\overline{v}(s) = 1$ und $\overline{v}(t) = 0$ (d.h. $s, \neg t \in \overline{S}$). Wir wollen, dass $(s \to t) \notin \overline{S}$. Andernfalls folgt aber, da $\{s, (s \to t)\} \vdash t$ (Modus ponens), dass $t \in S$, ein Widerspruch. Somit gilt $(s \to t) \notin \overline{S}$ und $\overline{v}(s \to t) = 0 = (\overline{v}(s) \to_2 \overline{v}(t))$.

(ii) $\overline{v}(t) = 1$ (d.h. $t \in \overline{S}$). Da $t \vdash (s \to t)$ (Axiom 1 und Deduktionstheorem), folgt $S \vdash (s \to t)$, und somit $(s \to t) \in S$ aufgrund der deduktiven Abgeschlossenheit, d.h. $\overline{v}(s \to t) = 1 = (\overline{v}(s) \to_2 \overline{v}(t))$.

(iii) $\overline{v}(s) = 0$ (d.h. $\neg s \in \overline{S}$). In diesem Fall gilt $\neg s \vdash (s \to t)$ (Übungsaufgabe), und es folgt wie im vorherigen Fall, dass $\overline{v}(s \to t) = 1 = (\overline{v}(s) \to_2 \overline{v}(t))$. □

Wir beschreiben noch zwei Folgerungen aus dem Vollständigkeitssatz, die man erhält, indem man offensichtliche Aussagen bezüglich $\models$ durch $\vdash$ ersetzt und umgekehrt.

Korollar 2.10 (Kompaktheitssatz der Aussagenlogik)**.** *Falls $S \models t$, dann gibt es eine endliche Teilmenge $S' \subset S$ mit $S' \models t$.*

Beweis. Klar für $\vdash$, da jeder Beweis nur endlich viele Prämissen verwenden kann. □

Korollar 2.11 (Entscheidbarkeitsatz der Aussagenlogik)**.** *Es existiert ein Algorithmus, der für endliches S und eine Aussage t entscheidet, ob $S \vdash t$.*

Beweis. Nach Bemerkung 2.2 ist einfach zu entscheiden, ob $S \models t$. □

[4] Der allgemeine Fall folgt aus dem Lemma von Zorn, und wird in den Hausaufgaben im Detail betrachtet.

2.4. **Eine Anwendung des Kompaktheitssatzes.**

Theorem 2.12. *Ein unendlicher Graph G ist genau dann n-färbbar, wenn jeder seiner endlichen Teilgraphen n-färbbar ist.*

Wir erinnern uns, dass eine n-Färbung eines Graphen $G = (V, E)$ eine Funktion $c\colon V \to \{1, 2, \ldots, n\}$ ist, so dass $c(v) \neq c(w)$ für alle $vw \in E$.

Beweis. Wir definieren eine Formelmenge S, so dass jede Belegung, die S erfüllt, eine Färbung von G codiert. Für jede Ecke $v \in V$ betrachten wir n Aussagevariablen $p_v^1, \ldots p_v^n$, also $P = \left\{p_v^i\colon v \in V,\, 1 \leq i \leq n\right\}$. Es sei s_v die Aussage, dass *genau eine von* $p_v^1, \ldots, p_v^n$ wahr ist. Für eine Kante $vw \in E$ sei t_{vw} die Aussage, dass für alle $i \leq n$ die Variablen p_v^i und p_w^i nicht gleichzeitig wahr sind.

Setze $S = \{s_v\colon v \in V\} \cup \{t_{vw}\colon vw \in E\}$.

Es ist klar, dass jede Belegung die S erfüllt uns eine n-Färbung von G definiert. Wir müssen also nur noch einsehen, dass eine solche Belegung existiert. Nach dem Kompaktheitssatz reicht er hierfür zu zeigen, dass jedes endliche $S' \subset S$ erfüllbar ist. Für endliches S' wähle einen induzierten Teilgraphen H von G der alle Ecken enthält, die in S' erwähnt werden. Aber nach Annahme hat H eine n-Färbung. Diese gibt uns eine Belegung, welche S' erfüllt. □

2.5. **Vorschläge für die Nachbereitung zur Vorlesung.** Die folgenden Vorschläge könnten beim Nachbereiten des zweiten Kapitels hilfreich sein.

Vorschlag 10. *Prüfen Sie, dass die Terme $s = (x \to (y \to z)) \to ((x \to y) \to (x \to z))$ und $u = (((x \to \bot) \to \bot) \to x)$ wirklich Tautologien sind.*

Vorschlag 11. *Welche der folgenden Aussagen sind Tautologien?*

(1) $(((p \to q) \to p) \to p)$
(2) $(((p \vee q) \wedge \neg p) \to q)$
(3) $(p \to (\neg p \vee q))$
(4) $(((p \wedge \neg q) \to r) \to q)$
(5) $(((p \to q) \wedge (r \to s)) \to ((p \wedge r) \to (q \vee s)))$
(6) $(((p \to q) \vee (r \to s)) \to ((p \wedge r) \to (q \vee s)))$

Vorschlag 12. *Warum sind Substitutionen in Tautologien auch immer selbst Tautologien?*

Vorschlag 13. *Überzeugen Sie sich, dass mit P auch $F_\Omega(P)$ abzählbar ist.*