Vorlesung

# Automatisches Beweisen

Sommersemester 2002

**Dr. Bernhard Beckert**

beckert@ira.uka.de

Institut für Logik, Komplexität
und Deduktionssysteme

Universität Karlsruhe (TH)

# Organisatorisches

**Semesterwochenstunden:** drei

**Vertiefungsfächer:**
- Logik und Grundlagen
- Deduktionssysteme

**Web-Seite zur Vorlesung:**
`http://i12www.ira.uka.de/~beckert/Lehre/automatisches-beweisen/`

**Folien:** Auf der Web-Seite

**Skriptum:** Vorläufige Version auf der Web-Seite; endgültige Version zum Ende des Semesters

**Sprechstunde:** Donnerstags nach der Vorlesung (Zi. 309)

# Voraussichtliche Vorlesungstermine

| Dienstag | | Donnerstag | |
|---|---|---|---|
| 16.04. | Vorlesung | 18.04. | Vorlesung |
| 23.04. | Vorlesung | 25.04. | Vorlesung |
| 30.04. | Vorlesung | 02.05. | Vorlesung |
| 07.05. | Vorlesung | 09.05. | — (Chr. Himmelf.) |
| 14.05. | Vorlesung | 16.05. | Vorlesung |
| 21.05. | Vorlesung | 23.05. | Vorlesung |
| 28.05. | Vorlesung | 30.05. | — (Fronleichnam) |
| 04.06. | Vorlesung | 06.06. | Vorlesung |
| 11.06. | — (Konferenz) | 13.06. | — (Konferenz) |
| 18.06. | Vorlesung | 20.06. | Vorlesung |
| 25.06. | Vorlesung | 27.06. | Vorlesung |
| 02.07. | Vorlesung | 04.07. | — (ggf. Vorl.) |
| 09.07. | — | 11.07. | — |
| 16.07. | — (Konferenz) | 18.07. | — (Konferenz) |

**Änderungen möglich!**

**Dienstags:** 11:30, SR 301

**Donnerstags:** 14:00 Uhr, SR 301

## Einführung [1]

## Logische Grundlagen [3]

### Aussagenlogik

### Prädikatenlogik

### Formalisierung in Logik erster Stufe

### Normalformen

### Metaresultate

## Die Tableaumethode [16]

### Konstruktionselemente des Automatischen Beweisens mit der Tableaumethode [4]

### Implementierung (in Prolog) [2]

### Klauseltableaux [2]

### Varianten von Klauseltableaus [8]

#### Konnektions-, Reguläre Tableaux [3]

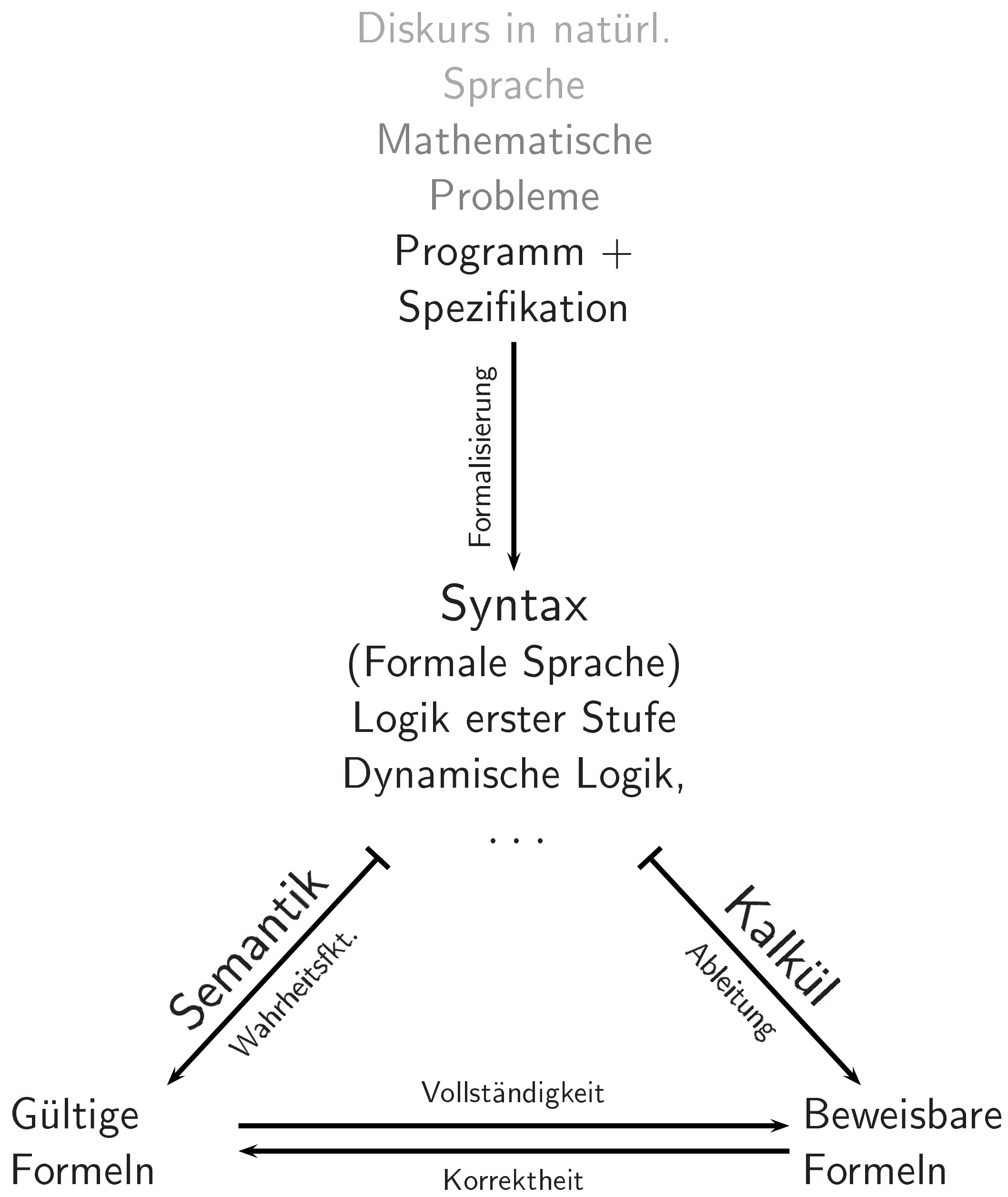
#### Geordnete Tableaus [2]

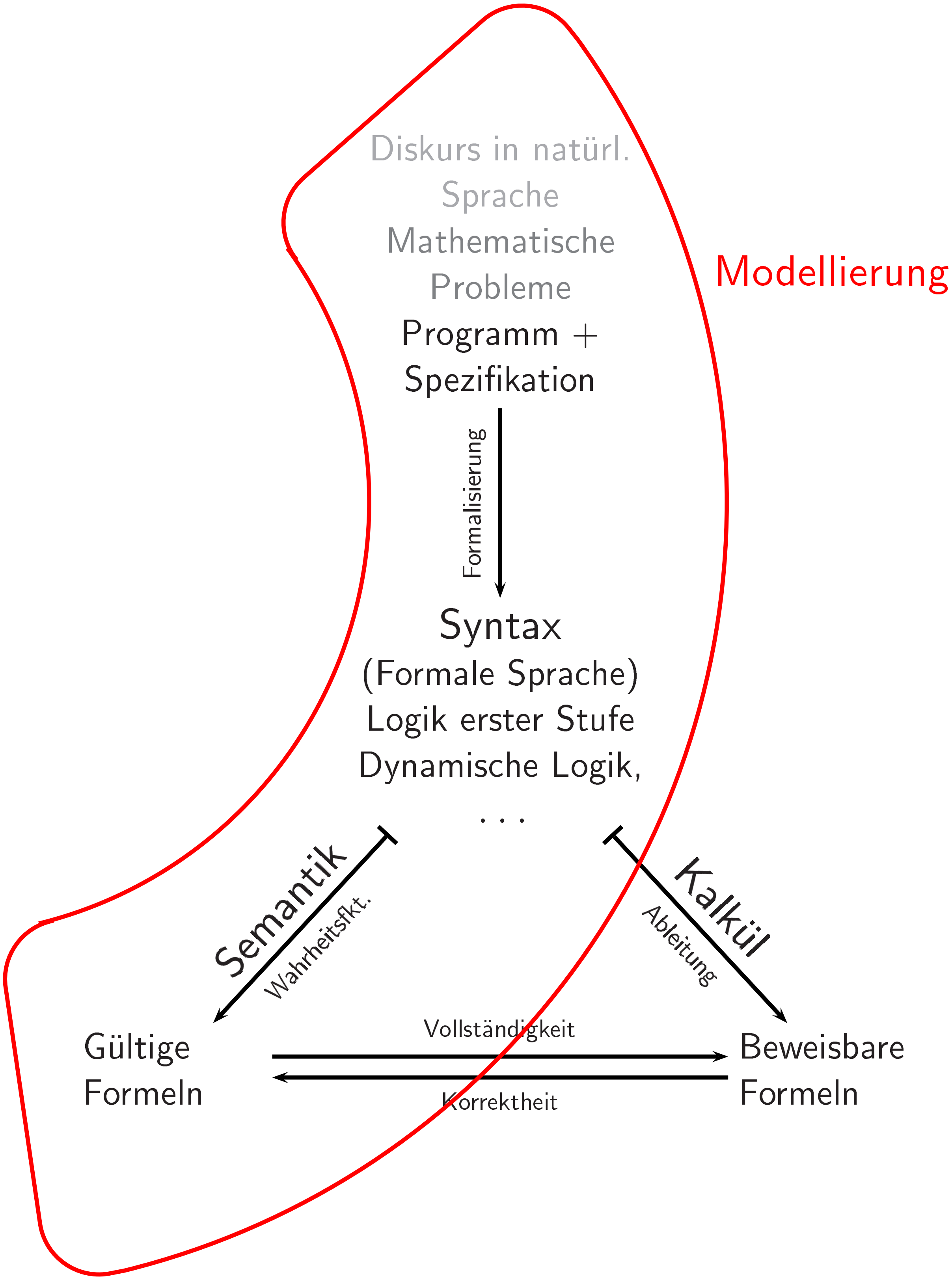
#### Konnektionsmethode, Modellelim. [1]

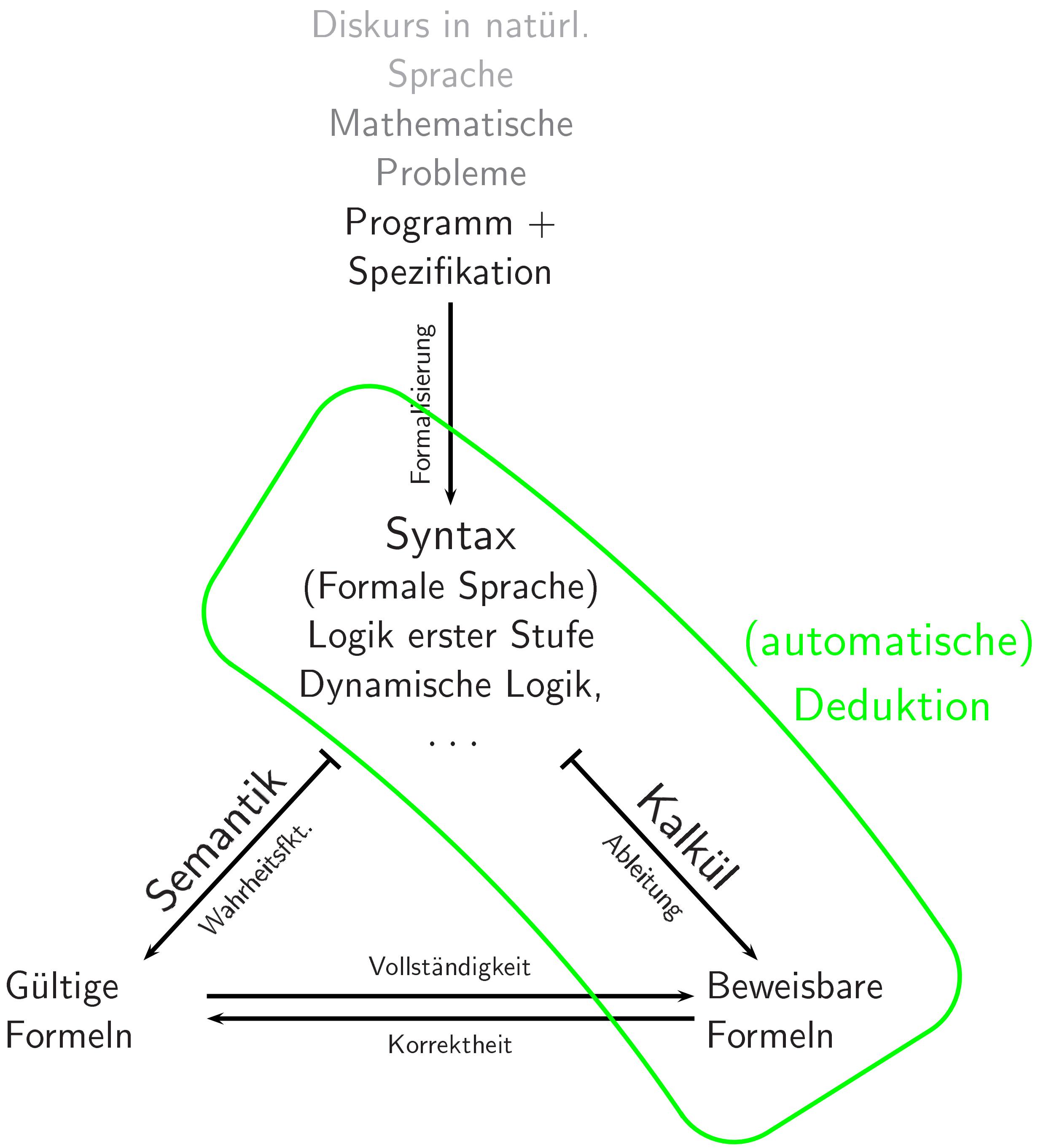
#### Verstärkungen des Tableaukalküls [2]

- **Resolution [10]**
  - **Grundlagen [3]**
  - **Varianten von Resolution [7]**
    - **Redundanzkriterien [1]**
    - **Geordnete, Lockresolution [1]**
    - **Lineare Resolution [3]**
    - **Semantische, Hyperresolution [2]**
- **Theorischließen (insbes. Gleichheit) [4]**
- **Evaluierung von Theorembeweisern [3]**
  - **Relative Beweiskomplexität [1]**
  - **Suchraumgröße [1]**
  - **Diskussion: Tableaus versus Resolution [1]**
- **Einige Implementierungen [0.5]**
- **Weitere Themen im Autom. Bew. [0.5]**

# Deduktion: Einordnung




Diskurs in natürl. Sprache
Mathematische Probleme
Programm + Spezifikation
Modellierung
Formalisierung
Syntax
(Formale Sprache)
Logik erster Stufe
Dynamische Logik,
. . .
Semantik
Wahrheitsfkt.
Kalkül
Ableitung
Gültige Formeln
Vollständigkeit
Korrektheit
Beweisbare Formeln


Diskurs in natürl. Sprache
Mathematische Probleme
Programm + Spezifikation
Formalisierung
Syntax
(Formale Sprache)
Logik erster Stufe
Dynamische Logik,
. . .
(automatische) Deduktion
Semantik
Wahrheitsfkt.
Kalkül
Ableitung
Gültige Formeln
Vollständigkeit
Korrektheit
Beweisbare Formeln

# Geschichtlicher Abriß

| | |
|---|---|
| vor 1950 | Beweistheoretische Vorarbeiten von Skolem, Herbrand, Gentzen |
| 1954 | Erster maschinengenerierter Beweis |
| 1955ff | Semantische Tableaus (Beth, Hintikka) |
| 1958 | Erster Beweiser für Prädikatenlogik (Prawitz) |
| 1959 | Weitere Beweiser (Gilmore, Wang) |
| 1960 | Davis-Putnam Verfahren |
| 1963 | Unifikation (J. A. Robinson) |
| 1963ff | Resolution, inverse Methode (Maslov) |
| 1963ff | Moderne Tableaus (Smullyan, Lis) |
| 1968 | Modellelimination (Loveland) |
| 1971ff | Konnektionsmethode (Bibel), Matings (Andrews) |
| 1970ff | PROLOG<br>Verfeinerungen von Resolution<br>SL-Resolution, cg-Resolution (Kowalski) |
| 1985ff | Beweisen in nichtklassischen Logiken<br>Renaissance von Tableaumethoden |
| 1987 | Tableaus mit Unifikation |

# Logische Grundlagen/Wiederholung Aussagenlogik

**Definition.** Menge der **Sonderzeichen**:

$$\{(,), \underline{\text{true}}, \underline{\text{false}}, \neg, \land, \lor, \rightarrow, \leftrightarrow\}$$

$\Sigma = \{p_0, p_1, \ldots\}$ aussagenlogische Variablen: **aussagenlogische (AL) Signatur**.

Menge $\text{For0}_\Sigma$ der **aussagenlogischen Formeln** über $\Sigma$ ist die kleinste Menge mit folgenden Eigenschaften:

1. $\underline{\text{true}}$, $\underline{\text{false}} \in \text{For0}_\Sigma$, $\Sigma \subset \text{For0}_\Sigma$.

2. Wenn $A$, $B \in \text{For0}_\Sigma$ dann auch $\neg A$, $(A \land B)$, $(A \lor B)$, $(A \rightarrow B)$, $(A \leftrightarrow B) \in \text{For0}_\Sigma$.

Formeln der Gestalt $\neg p$, $p$ mit $p \in \Sigma$ heißen **Literal**. ∎

Klammern weglassen unter Ausnutzung von Präzedenz:

$$\neg \;>\; \land \;>\; \lor \;>\; \rightarrow \;>\; \leftrightarrow$$

## **Primäre logische Operatoren (Konnektive)**:

$$\neg, \wedge, \vee, \rightarrow$$

**Unifizierende** oder **uniforme Notation**
(Smullyan, 1968)

Formeln der Gestalt

$$\neg\neg A \quad A \wedge B \quad \neg(A \vee B) \quad \neg(A \rightarrow B)$$

haben **Typ** $\alpha$ bzw. sind **konjunktiv**.

Formeln der Gestalt

$$\neg(A \wedge B) \quad A \vee B \quad A \rightarrow B$$

haben **Typ** $\beta$ bzw. sind **disjunktiv**.

Zuordnungsregeln Nichtliterale / Unterformeln

| $\alpha$ | $\alpha_1$ | $\alpha_2$ |
|---|---|---|
| $A \wedge B$ | $A$ | $B$ |
| $\neg(A \vee B)$ | $\neg A$ | $\neg B$ |
| $\neg(A \rightarrow B)$ | $A$ | $\neg B$ |
| $\neg\neg A$ | $A$ | $A$ |

| $\beta$ | $\beta_1$ | $\beta_2$ |
|---|---|---|
| $\neg(A \wedge B)$ | $\neg A$ | $\neg B$ |
| $A \vee B$ | $A$ | $B$ |
| $A \rightarrow B$ | $\neg A$ | $B$ |

## Aussagenlogische Interpretation

$$I : \Sigma \to \{W, F\}$$

$W, F$ heißen **Wahrheitswerte**.

Interpretation $I$ erweitert zu **Auswertung**
$\mathsf{val}_I : \mathsf{For0}_\Sigma \to \{W, F\}$ vermöge:

$$\mathsf{val}_I(\underline{\mathsf{true}}) = W$$

$$\mathsf{val}_I(\underline{\mathsf{false}}) = F$$

Für Literale:

$$\mathsf{val}_I(p) = I(p)$$

$$\mathsf{val}_I(\neg p) = \begin{cases} W & \text{falls } I(p) = F \\ F & \text{falls } I(p) = W \end{cases}$$

## Für Nicht-Literale:

$$\mathsf{val}_I(\alpha) = \begin{cases} W & \text{falls } \mathsf{val}_I(\alpha_1) = W \\ & \text{und } \mathsf{val}_I(\alpha_2) = W \\ F & \text{falls } \mathsf{val}_I(\alpha_1) = F \\ & \text{oder } \mathsf{val}_I(\alpha_2) = F \end{cases}$$

$$\mathsf{val}_I(\beta) = \begin{cases} W & \text{falls } \mathsf{val}_I(\beta_1) = W \\ & \text{oder } \mathsf{val}_I(\beta_2) = W \\ F & \text{falls } \mathsf{val}_I(\beta_1) = F \\ & \text{und } \mathsf{val}_I(\beta_2) = F \end{cases}$$

$$\mathsf{val}_I(A \leftrightarrow B) = \begin{cases} W & \text{falls } \mathsf{val}_I(A) = \mathsf{val}_I(B) \\ F & \text{falls } \mathsf{val}_I(A) \neq \mathsf{val}_I(B) \end{cases}$$

Interpretation $I$ über $\Sigma$
ist **Modell** einer Formelmenge $M \subset \mathrm{For0}_\Sigma$,
in Symbolen $I \models_\Sigma M$,
falls $\mathrm{val}_I(A) = W$ für alle $A \in M$.

Falls es ein Modell für sie gibt,
heißen $A$ bzw. $M$ **erfüllbar**.

$A$ ist **semantisch folgerbar** aus $M$,
in Symbolen $M \models_\Sigma A$,
falls jedes Modell von $M$ auch Modell von $A$ ist.

$A$ ist **(aussagenlogische) Tautologie**,
in Zeichen $\models_\Sigma A$,
falls $I \models_\Sigma A$ für alle $I$.

$A, B \in \mathrm{For0}_\Sigma$ sind **logisch äquivalent**.
falls $\{A\} \models_\Sigma B$ und $\{B\} \models_\Sigma A$.

**Proposition.** Deduktions-Theorem.
Seien $A, B \in \text{For0}_\Sigma$.

$\{A\} \models_\Sigma B$ gdw $\models_\Sigma (A \to B)$.

$A$ und $B$ logisch äquivalent gdw $\models_\Sigma A \leftrightarrow B$. ■

**Proposition.** Seien $A, B \in \text{For0}_\Sigma, M \subset \text{For0}_\Sigma$.

$M \models_\Sigma A$ gdw $M \cup \{\neg A\}$ nicht erfüllbar.

Speziell: $A$ ist AL Tautologie gdw $\neg A$ nicht erfüllbar.

■

**Proposition.** Substitutions-Theorem.
$A, B, C, D \in \text{For0}_\Sigma$ und $\models C \leftrightarrow D$.

Es entstehe $B$ aus $A$, indem beliebige Vorkommen von $C$ in $A$ durch $D$ ersetzt werden.

Dann sind $A, B$ logisch äquivalent, d.h. $\models_\Sigma (A \leftrightarrow B)$.

■

Schreibweise: $B = A[D/C]$ für Ersetzung *aller* Vorkommen von $C$