



Mathematik und Logik

2008W

Institut für Algebra
Johannes Kepler Universität Linz

Vorlesung im 2008W

<http://www.algebra.uni-linz.ac.at/Students/Win/ml>

Logik

Aussagenlogik

Logische Implikation, \Rightarrow

Logische Konjunktion, \wedge

Logische Äquivalenz,
 \iff

Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall

Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow

Logische Konjunktion, \wedge

Logische Disjunktion, \vee

Curry-Howard-
Isomorphismus

Logik

Aussagenlogik

Logische Implikation, \Rightarrow

Logische Konjunktion, \wedge

Logische Äquivalenz, \iff

Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall

Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow

Logische Konjunktion, \wedge

Logische Disjunktion, \vee

Curry-Howard-Isomorphismus

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

Die **mathematische Logik** verwendet mathematische Methoden, um das logische Denken formal zu beschreiben.

- ▶ **Populäre Definition:** Eine Aussage ist ein Satz, der entweder falsch oder wahr ist.
- ▶ **Problem:** Wie definiert man *wahr* und *falsch*?
- ▶ Ein **Beweis** stellt sicher, daß eine Aussage wahr ist.
- ▶ **DEFINITION:** Eine **Aussage** ist eine Konstruktion, durch welche festgelegt wird, wie ihre Beweise zu konstruieren sind.
- ▶ Eine Aussage, die wir nicht beweisen können, muß nicht unbedingt falsch sein.

Definition der Implikation, \Rightarrow

FORMATION

Sind P und Q Aussagen, dann bezeichnet $P \Rightarrow Q$ ebenfalls eine Aussage, die **Implikation** von P und Q .

INTRODUKTION

Um $P \Rightarrow Q$ zu beweisen, muß man Q beweisen, wobei man einen Beweis von P voraussetzen darf.

ELIMINATION

Hat man einen Beweis von $P \Rightarrow Q$, so reicht ein Beweis von P , um auch Q zu beweisen.

SCHLUSSREGELN

$$\frac{\begin{array}{|c|} \hline P \\ \hline \vdots \\ \hline Q \\ \hline \end{array}}{P \Rightarrow Q} \Rightarrow I$$

$$\frac{P \Rightarrow Q \quad P}{Q} \Rightarrow E$$

Definition der Konjunktion, \wedge

FORMATION

Sind P und Q Aussagen, dann bezeichnet $P \wedge Q$ ebenfalls eine Aussage, die **Konjunktion** von P und Q .

INTRODUKTION

Um $P \wedge Q$ zu beweisen, muß man sowohl P als auch Q beweisen.

ELIMINATION

Hat man einen Beweis von $P \wedge Q$ so auch einen Beweis von P , und auch einen Beweis von Q .

SCHLUSSREGELN

$$\frac{P \quad Q}{P \wedge Q} \wedge I$$

$$\frac{P \wedge Q}{P} \wedge E_0$$

$$\frac{P \wedge Q}{Q} \wedge E_1$$

Kommutativität der Konjunktion

SATZ

Die logische Konjunktion ist kommutativ, d.h. die Aussage

$$A \wedge B \Rightarrow B \wedge A$$

ist allgemeingültig.

BEWEIS.

$$\frac{
 \frac{
 \frac{A \wedge B}{B} \wedge \mathcal{E}_1 \quad \frac{A \wedge B}{A} \wedge \mathcal{E}_0
 }{B \wedge A} \wedge \mathcal{I}
 }{A \wedge B \Rightarrow B \wedge A} \Rightarrow \mathcal{I}$$



Definition der Äquivalenz, \iff

NOTATION

Die logische **Äquivalenz** wird mit $P \iff Q$ bezeichnet und ist lediglich eine Abkürzung für $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

BEMERKUNG

Zwei Aussagen sind äquivalent wenn sie vom logischen Standpunkt aus betrachtet gleichwertig sind.

Definition der Disjunktion, \vee

FORMATION

Sind P und Q Aussagen, dann bezeichnet $P \vee Q$ ebenfalls eine Aussage, die **Disjunktion** von P und Q .

INTRODUKTION

Um $P \vee Q$ zu beweisen, genügt es, P zu beweisen, oder Q zu beweisen.

ELIMINATION

Folgt irgendeine Aussage R sowohl aus P als auch aus Q , dann folgt sie auch aus $P \vee Q$ (Beweis durch Fallunterscheidung).

SCHLUSSREGELN

$$\frac{P}{P \vee Q} \vee \mathcal{I}_0$$

$$\frac{Q}{P \vee Q} \vee \mathcal{I}_1$$

$$\frac{\begin{array}{|c|} \hline P \\ \hline \vdots \\ \hline R \\ \hline \end{array} \quad \begin{array}{|c|} \hline Q \\ \hline \vdots \\ \hline R \\ \hline \end{array}}{P \vee Q} \vee \mathcal{E}$$

Beispiel: Distributivität

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

$$\begin{array}{c}
 \begin{array}{c}
 A \\
 \hline
 A \vee B \quad \forall \mathcal{I}_0
 \end{array}
 \quad
 \begin{array}{c}
 B \wedge C \\
 \hline
 \frac{B \wedge C}{B} \wedge \mathcal{E}_0 \\
 \hline
 A \vee B \quad \forall \mathcal{I}_1
 \end{array}
 \quad
 A \vee (B \wedge C) \\
 \hline
 A \vee B \quad \forall \mathcal{E}
 \end{array}$$

$$\begin{array}{c}
 A \vee (B \wedge C) \\
 \hline
 \begin{array}{cc}
 \vdots & \vdots \\
 \text{siehe oben} & \text{analog} \\
 \vdots & \vdots \\
 \frac{A \vee B}{(A \vee B) \wedge (A \vee C)} & \frac{A \vee C}{(A \vee B) \wedge (A \vee C)} \wedge \mathcal{I}
 \end{array} \\
 \hline
 A \vee (B \wedge C) \Rightarrow (A \vee B) \wedge (A \vee C) \quad \Rightarrow \mathcal{I}
 \end{array}$$

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

- ▶ Sei X ein Datentyp, und $P[x]$ für jedes $x \in X$ eine Aussage. Dann bezeichnet $\forall_{x \in X} P[x]$ eine **All-Aussage**.
- ▶ Die All-Aussage drückt eine universelle Quantifizierung aus.
- ▶ Ein Beweis von $\forall_{x \in X} P[x]$ konstruiert für jedes beliebige $x \in X$ einen Beweis von $P[x]$.
- ▶ Praktisch: Es sei $\forall_{x \in X} P[x]$ zu beweisen.
Vorgangsweise: Annahme $x \in X$; beweise $P[x]$.
- ▶ Hängt $P[x]$ nicht von x ab, dann liegt eine normale Implikation vor: $\forall_{x \in X} P$ ist dasselbe wie $X \rightarrow P$.

Allquantor, Einführung und Elimination

- ▶ Um $\forall x \in X P[x]$ zu beweisen, muß man $P[x]$ für ein beliebiges $x \in X$ beweisen.

- ▶ \forall -Einführung:

$$\frac{\begin{array}{c} x \in X \\ \boxed{\begin{array}{c} \vdots \\ P[x] \end{array}} \end{array}}{\forall x \in X P[x]} \forall I$$

- ▶ Wurde $\forall x \in X P[x]$ bewiesen, und ist $a \in X$, dann hat man einen Beweis von $P[a]$.

- ▶ \forall -Elimination:

$$\frac{\forall x \in X P[x] \quad a \in X}{P[a]} \forall E$$

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

$$\begin{array}{c}
 \forall x \in X A[x] \vee \forall y \in Y B[y] \\
 \hline
 \begin{array}{c}
 x \in X \\
 \hline
 \begin{array}{c}
 y \in Y \\
 \hline
 \begin{array}{c}
 \vdots \\
 A[x] \vee B[y]
 \end{array} \\
 \hline
 \forall y \in Y (A[x] \vee B[y]) \quad \forall \mathcal{I}
 \end{array} \\
 \hline
 \forall x \in X \forall y \in Y (A[x] \vee B[y]) \quad \forall \mathcal{I}
 \end{array} \\
 \hline
 \forall x \in X A[x] \vee \forall y \in Y B[y] \Rightarrow \forall x \in X \forall y \in Y (A[x] \vee B[y]) \quad \Rightarrow \mathcal{I}
 \end{array}$$

Allquantor: Beispiel (Fortsetzung)

Annahmen: $\forall x \in X A[x] \vee \forall y \in Y B[y]$, $x \in X$, $y \in Y$

Zu beweisen:

$$\frac{\begin{array}{c} \forall x \in X A[x] \\ \vdots \\ A[x] \vee B[y] \end{array} \quad \begin{array}{c} \forall y \in Y B[y] \\ \vdots \\ A[x] \vee B[y] \end{array}}{\forall x \in X A[x] \vee \forall y \in Y B[y] \Rightarrow A[x] \vee B[y]} \forall \mathcal{E}$$

Die beiden Fälle:

$$\frac{\frac{\forall x \in X A[x] \quad x \in X}{A[x]} \forall \mathcal{E}}{A[x] \vee B[y]} \forall \mathcal{I}_0$$

$$\frac{\frac{\forall y \in Y B[y] \quad y \in Y}{B[y]} \forall \mathcal{E}}{A[x] \vee B[y]} \forall \mathcal{I}_1$$

Existenzquantor, \exists

- ▶ Sei X ein Datentyp, und $P[x]$ für jedes $x \in X$ eine Aussage. Dann bezeichnet $\exists x \in X P[x]$ eine **Existenz-Aussage**.
- ▶ Die Existenzaussage drückt eine existenzielle Quantifizierung aus.
- ▶ Ein Beweis von $\exists x \in X P[x]$ konstruiert ein $a \in X$ und einen Beweis von $P[a]$.
- ▶ Praktisch: Es sei $\exists x \in X P[x]$ zu beweisen.
Vorgangswise: Man wählt ein passendes $a \in X$, und versucht damit $P[a]$ zu beweisen.
- ▶ Hängt $P[x]$ nicht von x ab, dann liegt eine normale Konjunktion vor: $\exists x \in X P$ ist dasselbe wie $X \wedge P$.

Existenzquantor: Einführung und Elimination

- Um $\exists x \in X P[x]$ zu beweisen, muß man ein $a \in X$ finden und damit $P[a]$ beweisen.

- \exists -Einführung:
$$\frac{a \in X \quad P[a]}{\exists x \in X P[x]} \exists\mathcal{I}$$

- Wurde $\exists x \in X P[x]$ bewiesen, so kann man für's weitere annehmen, daß es ein solches Objekt gibt.

- \exists -Elimination:

$$\frac{\exists x \in X P[x] \quad \begin{array}{|c|} \hline y \in X \quad P[y] \\ \hline \vdots \\ \hline Q \\ \hline \end{array}}{Q} \exists\mathcal{E}$$

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

▶ Schlußregeln:

$$\frac{\begin{array}{c} x \in P \\ \vdots \\ t[x] \in Q \end{array}}{x \mapsto t[x] \in P \Rightarrow Q} \Rightarrow \mathcal{I} \qquad \frac{f \in P \Rightarrow Q \quad x \in P}{fx \in Q} \Rightarrow \mathcal{E}$$

- ▶ Der Beweis einer Implikation ist ein **Algorithmus**,
- ▶ der für jeden Input vom Typ P einen Output vom Typ Q liefert.
- ▶ **Funktionsdatentyp**: Schreibweise: $P \rightarrow Q$ oder Q^P .
- ▶ **Konstruktor**: Abstraktion: (\mapsto) ;
- ▶ **Selektor**: Funktionsanwendung: `apply`.

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

► Einführung und Elimination

$$\frac{x \in P \quad y \in Q}{(x, y) \in P \wedge Q} \wedge \mathcal{I}$$

$$\frac{z \in P \wedge Q}{\text{fst } z \in P} \wedge \mathcal{E}_0$$

$$\frac{z \in P \wedge Q}{\text{snd } z \in Q} \wedge \mathcal{E}_1$$

- Ein Beweis der Konjunktion $P \wedge Q$ ist ein **Paar**,
- dessen Komponenten die Typen P bzw. Q haben.
- **Verbunddatentyp (Direktes Produkt)**: $P \times Q$.
- **Konstruktor**: $(,) \in P \rightarrow Q \rightarrow P \times Q$;
- **Selektoren**: $\text{fst} \in P \times Q \rightarrow P$, $\text{snd} \in P \times Q \rightarrow Q$.

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

SATZ

$$A \wedge B \Rightarrow B \wedge A.$$

► Beweis:

$$\begin{array}{c}
 c \in A \wedge B \\
 \boxed{
 \begin{array}{c}
 \frac{c \in A \wedge B}{\text{snd } c \in B} \wedge \mathcal{E}_1 \quad \frac{c \in A \wedge B}{\text{fst } c \in A} \wedge \mathcal{E}_0 \\
 \hline
 (\text{snd } c, \text{fst } c) \in B \wedge A \quad \wedge \mathcal{I}
 \end{array}
 } \\
 \hline
 c \mapsto (\text{snd } c, \text{fst } c) \in A \wedge B \Rightarrow B \wedge A \quad \Rightarrow \mathcal{I}
 \end{array}$$

► commute $\in A \times B \rightarrow B \times A$, $c \mapsto (\text{snd } c, \text{fst } c)$,► Intuitiver: $(a, b) \mapsto (b, a)$.

► Äquivalenz:

$$(c \mapsto (\text{snd } c, \text{fst } c), c \mapsto (\text{snd } c, \text{fst } c)) \in A \wedge B \Leftrightarrow B \wedge A.$$

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

► Einführung und Elimination

$$\frac{x \in P}{\text{Left } x \in P \vee Q} \vee I_0$$

$$\frac{y \in Q}{\text{Right } y \in P \vee Q} \vee I_1$$

$$\frac{f \in P \Rightarrow R \quad g \in Q \Rightarrow R}{\text{either } f \text{ } g \in P \vee Q \Rightarrow R} \vee E$$

- Ein Beweis der Disjunktion $P \vee Q$ ist einer von P oder von Q , *und als solcher gekennzeichnet.*
- **Disjunkte Vereinigung (Direkte Summe):** $P + Q$.
- **Konstruktoren:** $\text{Left} \in P \rightarrow P + Q$, $\text{Right} \in Q \rightarrow P + Q$;
- **Selektor:** $\text{either} \in (P \rightarrow R) \rightarrow (Q \rightarrow R) \rightarrow (P + Q \rightarrow R)$.

Beispiel: $A \vee (B \wedge C) \Rightarrow A \vee B$

$$\begin{array}{c}
 \frac{a \in A}{\text{Left } a \in A \vee B} \vee \mathcal{I}_0 \\
 \frac{y \in B \wedge C}{\text{fst } y \in B} \wedge \mathcal{E}_1 \\
 \frac{\text{Right } (\text{fst } y) \in A \vee B}{y \mapsto \text{Right } (\text{fst } y) \in B \wedge C \Rightarrow A \vee B} \vee \mathcal{I}_1 \\
 \frac{a \mapsto \text{Left } a \in A \Rightarrow A \vee B \quad y \mapsto \text{Right } (\text{fst } y) \in B \wedge C \Rightarrow A \vee B}{\text{either } (a \mapsto \text{Left } a) (y \mapsto \text{Right } (\text{fst } y)) \in A \vee (B \wedge C) \Rightarrow A \vee B} \Rightarrow \mathcal{I}
 \end{array}$$

Mit

$$\begin{array}{l}
 f \in A \vee (B \wedge C) \Rightarrow A \vee B \\
 g \in A \vee (B \wedge C) \Rightarrow A \vee C
 \end{array}$$

erhalten wir auch:

$$(f, g) \in A \vee (B \wedge C) \Rightarrow (A \vee B) \wedge (A \vee C)$$

Es gibt auch: $h \in (A \vee B) \wedge (A \vee C) \Rightarrow A \vee (B \wedge C)$

Logik

Aussagenlogik

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Äquivalenz,
 \iff Logische Disjunktion, \vee

Prädikatenlogik

Allquantor, \forall Existenzquantor, \exists

Datentypen

Logische Implikation, \Rightarrow Logische Konjunktion, \wedge Logische Disjunktion, \vee Curry-Howard-
Isomorphismus

Curry-Howard-Isomorphismus

- ▶ Eine Aussage legt den Datentyp ihrer Beweise fest.
- ▶ Ein Datentyp entspricht der Aussage, daß es ein Objekt dieses Typs gibt.
- ▶ Jeder Algorithmus, der ein Objekt eines bestimmten Datentyps konstruiert, ist ein Beweis, daß es ein solches gibt.
- ▶ Aussagen entsprechen Programmspezifikationen.
- ▶ Beweise entsprechen Programmen.
- ▶ Man kann Aussagen beweisen, indem man ein Objekt vom passenden Typ konstruiert.
- ▶ Aus mathematischen Beweisen lassen sich verifizierte Programme extrahieren.
- ▶ *Fehlerfreie Software beliebiger Komplexität ist möglich.*