# Grundbegriffe der mathematischen Logik

## Vorlesung WS 2005/2006

Jakob Kellner
http://www.logic.univie.ac.at/~kellner

Kurt Gödel Research Center for Mathematical Logic

7. Vorlesung, 2005-11-30

# Prädikatenlogik Ausblick

- Syntax: Definition der Sätze (als Zeichenketten), freie Variablen, Substitution.
- Semantik: Bedeutung eines Satzes (in einer konkreten Struktur), Begriff der semantischen Folgerung.
- Kalkül: Ableitungs- bzw. Beweissystem (syntaktisch, d.h. Manipulation von Zeichenketten), Begriff der formalen Ableitbarkeit bzw. Beweisbarkeit.
- Vollständigkeitssatz: Semantischen Folgerung und formalen Ableitbarkeit ist das selbe.
- Folgerungen: Kompaktheitssatz, nonstandard Modelle, Unvollständigkeitssatz.
- Beschränkungen der Prädikatenlogik, Ausweg mit Mengenlehre.

# Wiederholung: Syntax der Prädikatenlogik

- $\mathcal{L}$ ist Menge von Konstanten-, Relations- und Funktionssymbolen (mit Stelligkeiten).
- Bsp: $\mathcal{L} = \{e, \cdot\}$ (Gruppentheorie) oder $\mathcal{L} = \{0, 1, +, \cdot, <\}$ (Analysis).
- $\mathcal{L}$-Terme: Alle Variablen- und Konstantensymbole, abgeschlossen unter Zusammensetzung mit Funktionssymbolen. (Zeichenketten)
- Bsp: $\mathcal{L} = \{e, \cdot\}$: $e \cdot e$ und $x_0 \cdot x_1$
  $\mathcal{L} = \{0, 1, +, \cdot, <\}$: $\cancel{x_1 \cdot x_2 + (1 + 1 + 1) \cdot x_3}$ $\quad (x_1 \cdot x_2) + ((1 + (1 + 1)) \cdot x_3)$.
- $\mathcal{L}$-Atomformeln: $t_1 = t_2$ und $R(t_1, \dots t_n)$ für $t_i$ Terme und $R$ Relationss.
- $\mathcal{L}$-Formeln: Atomformeln, abgeschlossen unter aussagenlogischen Junktoren ($\neg$, $\vee$, $\wedge$, $\rightarrow$) und Quantifikation: Wenn $v$ Variablensymbol und $\varphi$ Formel, dann sind $(\forall v \varphi)$ und $(\exists v \varphi)$ Formeln.
- Bsp: $\mathcal{L} = \{e, \cdot\}$: $e \cdot x = y$ Atomformel, $\forall x\, e \cdot x = y$ Formel.
  $\mathcal{L} = \{0, 1, +, \cdot, <\}$: $y \cdot y = x$ Atomf., $\forall x\, (x > 0 \rightarrow (\exists y\, y \cdot y = x))$ Formel.

# Wiederholung: Freie Variablen, Substitution

- Sei $\varphi$ die Formel $g(x) = 1 \wedge (\forall x(f(x) > 1))$.
- Notation: $\varphi \;\equiv\; g(x) = 1 \wedge (\forall x(f(x) > 1))$
- In $\varphi$ tritt $x$ zuerst frei, dann gebunden auf.
- Formel ohne freie Variable heißt Satz.
- (Wir interessieren uns eigentlich nur für Sätze.)
- $\varphi[v \mapsto t]$ ($v$ Var., $t$ Term): Ersetze freie Vorkommen von $v$ durch $t$.
- Bsp: $\varphi[x \mapsto f(y)] \;\equiv\; g(f(y)) = 1 \wedge (\forall x(f(x) > 1))$.
- Notation: Schreibe $\varphi(x)$ (statt $\varphi$), und $\varphi(t)$ (statt $\varphi[x \mapsto t]$).
- Substitution kann semantisch unerwünschte Effekte haben, wenn eine Variable von $t$ in $\varphi(t)$ gebunden wird:
- Bsp: $\varphi(x) \;\equiv\; \exists y\, y \neq x$.
  Besagt (für jedes $x$): Das Universum hat zumindest 2 Elemente.
  $\varphi(y) \;\equiv\; \exists y\, y \neq y$ (immer falsch).

# Syntaktische Abkürzungen

Wir verwenden einige Abkürzungen:

- $\varphi \leftrightarrow \psi$ steht für $(\varphi \to \psi) \wedge (\psi \to \varphi)$.
- $t_1 \neq t_2$ steht für $\neg t_1 = t_2$
- Klammern werden oft weggelassen, wenn Eindeutigkeit garantiert ist.
- Bei manchen 2stelligen Funktionssymbolen schreiben wir $t_1\ f\ t_2$ statt $f(t_1, t_2)$, z.B. $x_0 + x_2$ statt $+(x_0, x_2)$.
- Wir verwenden manchmal andere Variablensymbole, z.B. $x, y, z$ statt $x_0, x_1, x_2$.
- $(\forall x < t)\varphi$ steht für $\forall x(x < t \to \varphi)$, und analog für andere 2stellige Relationssymbole (z.B. $\in$).
- $(\exists x < t)\varphi$ steht für $\exists x(x < t \wedge \varphi)$ etc.
- $(\exists! x)\varphi(x)$ steht für: $\exists x(\varphi(x) \wedge (\forall y(\varphi(y) \to y = x)))$.
  D.h.: Es gibt genau ein $x$ mit $\varphi(x)$.
- Wir schreiben $\varphi[x \mapsto s, y \mapsto t]$ für $(\varphi[x \mapsto s])[y \mapsto s]$ (kommutativ, wenn keine Variablensymbole in $s$ und $t$).
- Alternativ: $\varphi(x, y)$ und $\varphi(s, t)$.

# Semantik der Prädikatenlogik: $\mathcal{L}$-Strukturen

## Eine $\mathcal{L}$-Struktur $\mathcal{M}$

Eine $\mathcal{L}$-Struktur $\mathcal{M}$ besteht aus einer Grundmenge (Universum) $M \neq \emptyset$ zusammen mit:

- Für jedes Konstantensymbol $c$ ein Element $c^{\mathcal{M}}$,
- Für jedes $n$-stelliges Funktionssymbol $f$ eine Funktion $f^{\mathcal{M}} : M^n \to M$,
- Für jedes $n$-stelliges Relationssymbol $R$ eine Relation $R^{\mathcal{M}} \subseteq M^n$.

Beispiele:

- $(\mathbb{Z}, 0, +)$ ist eine $\{e, \cdot\}$-Struktur.
- $(\mathbb{N}, 0, \cdot)$ ist eine $\{e, \cdot\}$-Struktur.
- $(\mathbb{Z}, <)$ ist eine $\{<\}$-Struktur.
- $(\mathbb{Q}, <)$ ist eine $\{<\}$-Struktur.
- $(\mathbb{Q}, <)$ ist eine $\{\in\}$-Struktur.
- $(\mathbb{R}, 0, 1, +, \cdot, <)$ ist eine $\{0, 1, +, \cdot, <\}$-Struktur.

# Isomorphe $\mathcal{L}$-Struktur

## Isomorphismus

$f$ ist ein Isomorphismus der $\mathcal{L}$-Strukturen $\mathcal{M}$ und $\mathcal{N}$, wenn

- $f : M \to N$ bijektiv,
- $f(c^{\mathcal{M}}) = c^{\mathcal{N}}$ für Konstantensymbole $c$,
- $f(g^{\mathcal{M}}(x_1, \dots, x_n)) = g^{\mathcal{N}}(f(x_1), \dots, f(x_n))$ für Funktionss. $g$ und $x_i \in M$,
- $R^{\mathcal{M}}(x_1, \dots, x_n)$ gdw $R^{\mathcal{N}}(f(x_1), \dots, f(x_n))$ für Relationss. $R$ und $x_i \in M$.

$\mathcal{M}$ und $\mathcal{N}$ sind isomorph, wenn es so ein $f$ gibt.

(Bemerkung: Ausserhalb der Rekursionstheorie verwenden wir wie üblich wieder totale Funktionen.)

Beispiel: $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, (0,0), +)$ isomorph zu $(\mathbb{Z}/6\mathbb{Z}, 0, +)$ als $(e, \cdot)$-Struktur. (Weil isomorph als Gruppen, chinesischer Restsatz.)

Natürlich: Isomorphie Äquivalenzrelation, d.h. reflexiv, transitiv, symmetrisch.

# Semantik der Prädikatenlogik: $(\mathcal{L}, \mathcal{M})$-Formeln

## $(\mathcal{L}, \mathcal{M})$-Formeln und Terme

Sei $\mathcal{M}$ eine $\mathcal{L}$-Struktur. Ein $(\mathcal{L}, \mathcal{M})$-Term (Formel, Satz) ist ein Term (bzw Formel oder Satz) der Sprache $\mathcal{L}$ mit zusätzlich allen Elementen von $M$ als Konstanten.

Beispiele:

- $\mathcal{L} = \{e, \cdot\}$, $\mathcal{M} = (\mathbb{Z}, 0, +)$.
  $-3$ (das Element von $\mathbb{Z}$) ist neues Konstantensymbol.
  Daher: $-3 \cdot e$ ist $(\mathcal{L}, \mathcal{M})$-Term, und
  $\exists x(x \cdot -3 = e)$ ist $(\mathcal{L}, \mathcal{M})$-Formel.
- $\mathcal{L} = \{0, 1, +, \cdot, <\}$, $\mathcal{M} = (\mathbb{R}, 0, 1, +, \cdot, <)$.
  Es gibt überabzählbar viele neue Konstantensymbole!
  Z.B. $2.871418\ldots \in \mathbb{R}$.
  Daher: $(2.871418\ldots \cdot x_0) + x_1$ ist $(\mathcal{L}, \mathcal{M})$-Term,
  $\forall x_0(x_0 > 2.871418\ldots \to x_0 > e)$ ist $(\mathcal{L}, \mathcal{M})$-Formel.

# Semantik der Prädikatenlogik: Term-Auswertung

## Terme

Wenn $t$ ein $(\mathcal{L}, \mathcal{M})$-Term ohne Variablen ist, dann ist $t^{\mathcal{M}} \in M$ folgendermaßen induktiv definiert:

- Wenn $t$ ein Konstantensymbol $c$ ist, dann ist $t^{\mathcal{M}} = c^{\mathcal{M}}$.
- Wenn $t$ die Form $f(t_1, \ldots, t_n)$ hat, dann ist $t^{\mathcal{M}} = f^{\mathcal{M}}(t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}})$.

Beispiele:

- $\mathcal{L} = \{e, \cdot\}$, $t \;\equiv\; e \cdot e$.
  - $\mathcal{M} = (\mathbb{Z}, 0, +)$: $t^{\mathcal{M}} = 0 + 0 = 0$.
  - $\mathcal{M} = (\mathbb{Z}, 1, +)$: $t^{\mathcal{M}} = 1 + 1 = 2$.
  - $\mathcal{M} = (\mathbb{N}, 2, \cdot)$: $t^{\mathcal{M}} = 2 \cdot 2 = 4$.
- $\mathcal{L} = \{e, \cdot\}$, $\mathcal{M} = (\mathbb{R}, 1, +)$, $t \;\equiv\; 2.871418\ldots \cdot e$
  $t^{\mathcal{M}} = 2.871418\ldots + 1 = 3.871418\ldots$

# Semantik der Prädikatenlogik: Satz-Auswertung

## Wahrheit in einer Struktur

Wir definieren mit Induktion nach Aufbau vom $(\mathcal{L}, \mathcal{M})$-Satz $\varphi$ die Egenschaft: $\mathcal{M}$ erfüllt $\varphi$, bzw. $\varphi$ gilt in $\mathcal{M}$, bzw. $\mathcal{M} \vDash \varphi$:

- $\mathcal{M} \vDash (t_1 = t_2)$ gdw $t_1^{\mathcal{M}} = t_2^{\mathcal{M}}$.
- $\mathcal{M} \vDash (R(t_1, \dots, t_n))$ gdw. $R^{\mathcal{M}}(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}})$ gilt (d.h. $(t_1^{\mathcal{M}}, \dots, t_n^{\mathcal{M}}) \in R^{\mathcal{M}}$).
- $\mathcal{M} \vDash (\psi_1 \wedge \psi_2)$ gdw $\mathcal{M} \vDash \psi_1$ und $\mathcal{M} \vDash \psi_2$.
- Analog für $\wedge$, $\neg$, $\rightarrow$.
- $\mathcal{M} \vDash (\forall x_i \psi)$ gdw $\mathcal{M} \vDash \psi[x_i \mapsto c]$ für alle $c \in M$.
- $\mathcal{M} \vDash (\exists x_i \psi)$ gdw $\mathcal{M} \vDash \psi[x_i \mapsto c]$ für ein $c \in M$.

# Beispiele für Wahrheit in einer Struktur

$cL = \{<\}$, $\varphi \equiv [\forall x \forall y (x < y \rightarrow \exists z (x \neq z \& y \neq z \& x < z \& z < y))]$.
$(\mathbb{Q}, <) \vDash \varphi$: Per definition gdw
Für jedes $q_x \in Q$ gilt:
$(\mathbb{Q}, <) \vDash [\forall y (q_x < y \rightarrow \exists z (q_x \neq z \& y \neq z \& q_x < z \& z < y))]$.
Gdw für jedes $q_x \in Q$ und $q_y \in Q$ gilt:
$(\mathbb{Q}, <) \vDash q_x < q_y \rightarrow \exists z (q_x \neq z \& q_y \neq z \& q_x < z \& z < q_y))$.
Gdw für jedes $q_x \in Q$ und $q_y \in Q$ gilt:
Wenn $(\mathbb{Q}, <) \vDash q_x < q_y$,
dann $(\mathbb{Q}, <) \vDash \exists z (q_x \neq z \& q_y \neq z \& q_x < z \& z < q_y))$.
Gdw für jedes $q_x < q_y \in Q$ gilt:
$(\mathbb{Q}, <) \vDash \exists z (q_x \neq z \& q_y \neq z \& q_x < z \& z < q_y))$.
Gdw es für jedes $q_x < q_y \in Q$ ein $q_z \in Q$ gibt mit:
$(\mathbb{Q}, <) \vDash q_x \neq q_z \& q_y \neq q_z \& q_x < q_z \& z < q_y$.
...
Gdw es für jedes $q_x < q_y \in Q$ ein $q_z \in Q$ gibt mit
$q_x \neq q_z \& q_y \neq q_z \& q_x < q_z \& z < q_y$.

# Beispiele für Wahrheit in einer Struktur

$\mathcal{L} = \{<\}, \varphi \equiv [\forall x \forall y (x < y \rightarrow \exists z (x \neq z \& y \neq z \& x < z \& z < y))]$.

- $(\mathbb{Q}, <) \vDash \varphi$
- $(\mathbb{Q}, \leq) \vDash \varphi$ gilt nicht.
  Das schreiben wir auch: $(\mathbb{Q}, \leq) \nvDash \varphi$.
- $(\mathbb{N}, <) \nvDash \varphi$
- Setze $R(a, b)$ wenn $a \equiv b \mod 2$.
  $(\mathbb{N}, R) \vDash \varphi$

## Isomorphe Strukturen haben gleiche wahre Sätze

Wenn $\mathcal{M}$ und $\mathcal{M}'$ isomorphe $\mathcal{L}$-Strukturen sind, und $\varphi$ ein $\mathcal{L}$-Satz, dann gilt $\mathcal{M} \vDash \varphi$ gdw $\mathcal{M}' \vDash \varphi$.

# Semantische Folgerung/Wahrheit

Sei $\Sigma$ eine Menge von $\mathcal{L}$-Sätzen.

- $\Sigma \vDash \varphi$ heißt: Jede $\mathcal{L}$-Struktur $\mathcal{M}$, die jeden Satz aus $\Sigma$ erfüllt, erfüllt auch $\varphi$.
- Statt $\emptyset \vDash \varphi$ schreiben wir auch nur $\vDash \varphi$ (d.h. $\varphi$ gilt in allen $\mathcal{L}$-Strukturen.)

"nicht $\mathcal{M} \vDash \varphi$" (d.h. $\mathcal{M} \nvDash \varphi$) ist äquivalent zu "$\mathcal{M} \vDash \neg\varphi$".
Aber: $\Sigma \nvDash \varphi$ ist nicht äquivalent zu $\Sigma \vDash \neg\varphi$!

Beispiele:

- $\vDash \exists x : x = x$ (Das Universum ist nichtleer.)
- $\nvDash \exists x : x \neq x$
- $\nvDash \exists x \exists y\, x \neq y$ (Das Universum könnte Größe 1 haben.)
- $\nvDash \neg(\exists x \exists y\, x \neq y)$ (Das Universum kann auch größer sein.)

# Beispiele für Semantische Folgerung aus Axiomen

Beispiel:

- Sei $\mathcal{L} = \{e, \cdot\}$, $\Sigma = \{\mathrm{AG}, \mathrm{NE}, \mathrm{Inv}\}$ (die Gruppenaxiome).
- Eine $\mathcal{L}$-Struktur $\mathcal{M} = (M, e^M, \cdot^M)$ erfüllt $\Sigma$ heißt genau: $\mathcal{M}$ ist Gruppe.
- $\Sigma \models \varphi$ heißt also: Der Satz $\varphi$ gilt in jeder Gruppe.
- Bsp: $\Sigma \models \forall x\, \forall y\, \forall z\, (x \cdot y = x \cdot z \rightarrow y = z)$
- Bsp: $\Sigma \not\models \exists x\, x \neq e$

# Komplexität der Semantischen Folgerung

Auf den ersten Blick ist der Begriff der semantischen Folgerung enorm kompliziert.

Wenn $G$ eine komplizierte Gruppe ist, kann schon die Frage "gilt $\varphi$ in $G$?" schwierig zu beantworten sein.

Um festzustellen, ob $\varphi$ in allen Gruppen gilt, muß man im schlimmsten Fall wissen, wie die Klasse aller Gruppen aussieht. Das ist eine noch viel schwierigere Frage.

(Bsp: "Es gibt keine Gruppe, deren Größe zwischen $|\mathbb{N}|$ und $|\mathbb{R}|$ liegt." ist äquivalent zu CH.)

Die Pointe der Prädikatenlogik: "$\varphi$ gilt in allen Gruppen", wobei $\varphi$ ein first order Satz ist, ist (relativ) einfach festzustellen: Es ist äquvalent zu
"$\varphi$ ist aus den Gruppenaxiomen formal ableitbar",
wobei die Menge der aus einer r.e. Menge ableitbaren Sätze r.e. ist.

# Vollständigkeitssatz

Vollständigkeitssatz: Es gibt ein effektives Ableitungssystem, so daß die Menge der formal aus einer Axiomenmenge ableitbaren Sätze gleich der Menge der semantischen Folgerungen der Axiome ist.

Die konkrete Form des Ableitungssystems ist (für uns) nicht wichtig, genauso wie die konkrete Definition der URM nicht wichtig ist. Wichtig ist, daß es so ein universelles Ableitungssystem (und so ein universelles Computermodell) gibt.