Was ist beweisbar?

In diesem Kapitel befassen wir uns mit Eigenschaften von Theorien.

- Gültigkeit vs. Beweisbarkeit
- Widerspruchsfreiheit / Konsistenz
- Vollständigkeit
- Vollständigkeits- und Unvollständigkeitssatz

Wir bewegen uns in der Sprache der Prädikatenlogik erster Stufe (vgl. Vorlesung zur mathematischen Logik).

Sei $\mathcal{A}$ eine Menge von (geschlossenen) Aussagen (Formeln). Die **Theorie** von $\mathcal{A}$, $\mathcal{T}(\mathcal{A})$, ist die Menge aller Aussagen, welche sich aus $\mathcal{A}$ mittels logischer Schlussregeln herleiten lassen.

Eine Aussage A in $\mathcal{T}(\mathcal{A})$ ist also aus der **Axiomenmenge** A **beweisbar** bzw. **herleitbar**. Wir schreiben

$$\mathcal{A} \vdash A$$

In einem früheren Kapitel haben wir einige Aussagen gesehen, welche aus den Peanoaxiomen (Peano Arithmetik $\mathcal{PEA}$) für $\mathbb{N}$ beweisbar sind.

$\mathcal{PEA}$ ist nicht entscheibar; d.h. es gibt kein Computerverfahren, mit dem man in endlich vielen Schritten für jede Formel A entscheiden könnte, ob A aus $\mathcal{PEA}$ beweisbar ist.

Die **Presburger Arithmetik** $\mathcal{PRA}$ ist eine in der Prädikatenlogik erster Stufe formulierte Theorie der natürlichen Zahlen $\mathbb{N}$ mit Addition (also ohne Multiplikation). Die Presburger Arithmetik ist schwächer als die Peano Arithmetik, in welcher auch die Multiplikation ausgedrückt werden kann.

Die Presburger Arithmetik ist eine entscheidbare Theorie; für jede Formel A in $\mathcal{PRA}$ lässt sich in endlich vielen Schritten entscheiden, ob $\mathcal{PRA} \vdash A$.

Sei $\mathcal{A}$ eine Axiomenmenge.
Ein **Modell** von $\mathcal{A}$ ist eine Struktur (Menge mit Operationen), welche die in $\mathcal{A}$ vorkommenden Funktionen und Prädikate interpretieren, und für welche die Aussagen in $\mathcal{A}$ zutreffen.

Modelle für [P 1 – 4] (die ersten 4 Peano Axiome) sind etwa:

- $\mathbb{N}$
- $\mathbb{N} \cup -\mathbb{N}$ (die beiden Stränge der natürlichen Zahlen, sowie der negativen Zahlen)
- $\mathbb{Z}_{12}$, die Ziffern auf einer Uhr

Axiome der Gruppentheorie $\mathcal{G}$:

$$\forall a, b, c : (a * b) * c = a * (b * c)$$

$$\exists e \forall a : a * e = a = e * a$$

$$\forall a \exists b : a * b = e = b * a$$

Modelle der Gruppentheorie (also Gruppen) sind etwa

$(\mathbb{Z}, +)$, die ganzen Zahlen mit Addition

$(\mathbb{Q}^*, \cdot)$, die rationalen Zahlen (Bruchzahlen) ohne die Null mit Multiplikation

für die ersten beiden Axiome:

$(\mathcal{P}(\mathbb{N}), \cup)$, die Potenzmenge von $\mathbb{N}$ mit Mengenvereinigung

Folgerungen aus einer Theorie:

Eine Aussage A **gilt (ist gültig)** in einer Theorie $\mathcal{T}$ wenn sie in jedem Modell von $\mathcal{T}$ gilt.

Eine Aussage A **folgt** aus einer Menge von Aussagen $\mathcal{A}$, wenn A in $\mathcal{T}(\mathcal{A})$, also der Theorie von A, gilt. Wir schreiben

$$\mathcal{A} \models A$$

eine unabdingbare Forderung an eine Theorie ist die

Widerspruchsfreiheit oder **Konsistenz**

aus einem Widerspruch folgt JEDE Aussage:
aus Def. der Implikation $\Longrightarrow$: eine falsche Aussage impliziert jede Aussage

eine widersprüchliche Theorie hat kein Modell

man kann also die Widerspruchsfreiheit nachweisen, indem an ein Modell angibt zur Widerspruchsfreiheit:

The idea that a contradiction is bad because absolutely anything follows from it might seem strange to a non-logician. Bertrand Russell was once trying to get this very point across at a public lecture when a heckler interrupted him. “So prove to me that if two plus two is five, I’m the Pope,” the heckler said.
“Very well,” Russell replied. “From two plus two equals five it follows, subtracting three from each side, that two equals one. You and the Pope are two, therefore you are one.”

J.Holt, When Einstein Walked with Gödel, p.278

eine weitere wünschenswerte Eigenschaft einer Theorie ist die

Vollständigkeit

eine Theorie $\mathcal{T}$ ist vollständig, wenn für jede Aussage A gilt:

$$A \in \mathcal{T} \qquad \text{oder} \qquad \neg A \in \mathcal{T}$$

ist also $\mathcal{T}$ konsistent, dann gilt

$$\mathcal{T} \models A \qquad \Longleftrightarrow \qquad \mathcal{T} \vdash A$$

David Hilbert wollte zu Anfang des 20. Jahrhunderts die Vollständigkeit der Peanoschen Theorie beweisen.

Gödel zeigte, dass das nicht möglich ist.

Vollständigkeitssatz von Gödel:

Hilbert-Kalkül: die Axiomenmenge besteht aus allen Tautologien und deren Spezialisierung durch prädikatenlogische Formeln (siehe Wikipedia).

Der Hilbert-Kalkül für die Prädikatenlogik erster Stufe ist vollständig. Also für jede Formelmenge (Aussagenmenge) $\mathcal{A}$ und für jede Formel A gilt:
A folgt genau dann aus $\mathcal{A}$, wenn A im Kalkül aus $\mathcal{A}$ herleitbar ist; also

$$\mathcal{A} \vdash A \quad \Longleftrightarrow \quad \mathcal{A} \models A \, .$$

Unvollständigkeitsatz von Gödel:

Jedes hinreichend mächtige[1], rekursiv aufzählbare[2] Axiomensystem (bzw. die zugehörige Theorie) ist entweder widersprüchlich oder unvollständig.

Der Hilbert-Kalkül erfüllt diese Bedingungen nicht.

[1] $\mathbb{N}$ mit Addition und Multiplikation kann beschrieben werden

[2] Axiome können durch einen Computer erkannt werden

Kurt Gödel hat die Vollständigkeit der Theorie der Prädikatenlogik in seiner Dissertation an der Universität Wien bewiesen.

Den Unvollständigkeitssatz hat er erstmals 1931 bei einer Konferenz in Königsberg vorgetragen.

John von Neumann sass im Auditorium und berichtete Hilbert davon. Hilbert war natürlich vom Ergebnis enttäuscht.

Als Ludwig Wittgenstein vom Unvollständigkeitssatz hörte, sagte er: “Das ist unakzeptabel!”

Einige Zeit dachte man, der **Satz von Fermat**

> es gibt keine positiven natürlichen Zahlen a, b, c, n, wobei $n > 2$, sodass $a^n + b^n = c^n$

sei vielleicht eine Aussage, die in $\mathcal{P}EA$ weder beweisbar noch widerlegbar ist.

Andrew Wiles hat aber 1992 den Satz von Fermat bewiesen.

Die **Goldbachsche Vermutung**

> jede gerade natürliche Zahl grösser als 2 ist Summe zweier Primzahlen

ist aber immer noch weder bewiesen noch widerlegt.