Kurt Gödel und die Grundlagen der Mathematik

Helmut Schwichtenberg

Mathematisches Institut der LMU

5. November 2007

Kurt Gödel 1906 – 1978

Geboren am 28. April 1906 in Brünn (heute Brno)
Studium der Mathematik und Physik in Wien, 1924 – 1930
Mitglied des „Wiener Kreises“ (Moritz Schlick), 1926 – 1928
Promotion 1930
Emigration in die USA 1940
Mitglied des „Institute for Advanced Study“ (Princeton), ab 1940

Kurt Gödel: wichtige Arbeiten (Auswahl)

- Die Vollständigkeit der Axiome des logischen Funktionenkalküls, 1930
- Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter Systeme I, 1931
- Über eine bisher noch nicht benützte Erweiterung des finiten Standpunkts, 1958

Collected Works (Hrsg. S. Feferman et al.), Oxford University Press, 1986

Was machen Mathematiker?

„Sie entwickeln immer leistungsfähigere Computer.“
Ziel: alle Fragen mathematischer Natur durch Berechnung lösen.

Gödel konnte beweisen, daß das

- möglich bzw.
- unmöglich ist,

je nachdem, was genau das Ziel ist.

Ars magna

Raimundus Lullus (Spanien, um 1300): Idee einer „ars magna“, einer Kunst zur schematischen Lösung nicht nur mathematischer Probleme, sondern aller Probleme überhaupt.

Leibniz (1646 – 1716) hat sich intensiv mit dem Problem der ars magna befaßt, insbesondere auch mit dem Verhältnis von algorithmischer Aufzählbarkeit („ars inveniendi“) und Entscheidbarkeit („ars iudicandi“)

Beispiel eines Algorithmus: Dezimalbruchentwicklung von π. Kommt eine vorgegebene Ziffernfolge – wie $0, 1, \ldots, 9$ – darin vor?

Leibniz konnte trotz vieler Bemühungen seine Projekte nicht realisieren. Hauptproblem: Verwendung der Umgangssprache.

Gottlob Frege (1848 – 1925) veröffentlichte 1879 seine

> *„Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens“.*

Es war der erste brauchbare Logikkalkül.

Variablen:	x, y, z
Prädikatensymbole	P, Q, R
Funktionssymbole	f, g, h
Terme:	$x \mid f(r_1 \dots r_n)$

Logische Formeln werden aus Primformeln $P(r_1 \dots r_n)$ aufgebaut:

$A \wedge B$	„A und B“	$\neg A$	„Nicht A“
$A \vee B$	„A oder B“	$\forall_x A$	„Für alle x gilt A“
$A \to B$	„Wenn A, so B“	$\exists_x A$	„Es gibt ein x mit A“

Formales Schließen

Ausgehend von einem Axiomensystem Ax leitet man Sätze her, und zwar durch Anwendung von Schlußregeln.

Beispiel:

$$\frac{A \to B \qquad A}{B} \qquad \text{(modus ponens)}$$

Dieser Ansatz (Axiome und Schlußregeln) geht auf Aristoteles zurück.

Interpretationen

Was „bedeuten“ Formeln? Man braucht eine Interpretation der Prädikaten- und Funktionssymbole, oder genauer:

Eine zur Sprache passende Struktur $\mathcal{M} = (|\mathcal{M}|, P^{\mathcal{M}}, \ldots, f^{\mathcal{M}}, \ldots)$.

Es ist einfach zu sehen, daß eine herleitbare Formel bei jeder Interpretation gültig ist. Gilt das auch umgekehrt? Oder: Haben wir eine wichtige Regel vergessen?

Theorem (Gödels Vollständigkeitssatz)

$\mathrm{Ax} \vdash A$ *genau dann, wenn bei jeder Interpretation der Prädikaten- und Funktionssymbole, bei der alle Axiome des Axiomensystems* Ax *gelten, auch die Formel* A *gilt.*

Formale Sprache der Arithmetik

Variablen: x, y, z (für natürliche Zahlen)

Funktionssymbole: $+$, $\cdot$, S, 0 (S die „Nachfolgerfunktion“)

Terme: $x \mid 0 \mid r + s \mid r \cdot s \mid S(r)$

Ziffern sind spezielle Terme: für $a \in \mathbb{N}$ sei $\underline{a}$ definiert durch

$$\underline{0} := 0, \quad \underline{n+1} := \mathrm{S}(\underline{n}).$$

Beispiel: $\underline{2}$ ist $S(S(0))$.

Formeln: $r = s \mid A \wedge B \mid A \vee B \mid A \to B \mid \neg A \mid \forall_x A \mid \exists_x A$

Sätze: geschlossene Formeln, also Formeln ohne freie Variable

Beispiele

$$x < y := \exists_z (z \neq 0 \land x + z = y)$$
$$y \mid x := \exists_z (y \cdot z = x) \quad (y \text{ teilt } x)$$
$$P(x) := 1 < x \land \forall_y (y \mid x \to y = 1 \lor y = x) \quad (x \text{ ist Primzahl})$$

Es gibt unendlich viele Primzahlen:

$$\forall_x \exists_{y>x} P(y)$$

Interpretation unserer formalen Sprache der Arithmetik:

Allgemein: durch eine passende Struktur $\mathcal{N} = (|\mathcal{N}|, 0^{\mathcal{N}}, \mathrm{S}^{\mathcal{N}})$.

Hier Standardinterpretation:

$$|\mathcal{N}| := \mathbb{N}, \quad 0^{\mathcal{N}} := 0, \quad \mathrm{S}^{\mathcal{N}}(a) := a + 1.$$

Eine Teilmenge $M \subseteq \mathbb{N}$ heißt definierbar, wenn

es eine Formel $A_M(z)$ gibt so daß $M = \{\, a \mid \mathcal{N} \models A_M(\underline{a}) \,\}$

Beispiel: $\{\, a \mid \mathcal{N} \models P(\underline{a}) \,\}$ ist die Menge der Primzahlen.

Undefinierbarkeit des Wahrheitsbegriffs

Numerierung der Formeln: $A \mapsto \ulcorner A \urcorner$
($\ulcorner A \urcorner$ heißt Gödelnummer der Formel A).

Theorem (Tarski)

Die Menge der Gödelnummern in $\mathcal{N}$ wahrer Sätze

$$\ulcorner \mathrm{W}(\mathcal{N}) \urcorner := \{ \ulcorner A \urcorner \mid A \text{ Satz mit } \mathcal{N} \models A \}$$

(der „Wahrheitsbegriff“ von $\mathcal{N}$) ist nicht definierbar.

Lemma (Fixpunktlemma)

Zu jeder Formel $B(z)$ findet man einen Satz A mit

$$\mathcal{N} \models A \quad gdw \quad \mathcal{N} \models B(\ulcorner A \urcorner).$$

Beweis des Undefinierbarkeitssatzes

Annahme: $\ulcorner \mathrm{W}(\mathcal{N}) \urcorner$ ist definierbar, etwa durch $B_W(z)$.
Dann gilt für alle Sätze A

$$\mathcal{N} \models A \quad \text{gdw} \quad \mathcal{N} \models B_W(\ulcorner A \urcorner). \tag{1}$$

Betrachte die Formel $\neg B_W(z)$. Nach dem Fixpunktlemma hat man einen Satz A mit

$$\mathcal{N} \models A \quad \text{gdw} \quad \mathcal{N} \models \neg B_W(\ulcorner A \urcorner). \tag{2}$$

A besagt die eigene Falschheit: „Ich bin nicht wahr“.
(1) und (2) widersprechen sich. Also ist die Annahme unhaltbar:
$\ulcorner \mathrm{W}(\mathcal{N}) \urcorner$ ist nicht definierbar.

Entscheidbarkeit, Aufzählbarkeit

$M \subseteq \mathbb{N}$ entscheidbar: es gibt einen Algorithmus, der bei Eingabe der Zahl a terminiert und feststellt, ob $a \in M$ ist oder nicht.

Leicht: M entscheidbar $\Rightarrow$ M definierbar.

Folgerung. Der Wahrheitsbegriff von $\mathcal{N}$ ist nicht entscheidbar. Also: Leibniz' „ars iudicandi" kann es nicht geben.

$M \subseteq \mathbb{N}$ aufzählbar: es gibt einen Algorithmus, der bei Eingabe von a genau dann terminiert, wenn $a \in M$.

Leicht: M aufzählbar $\Rightarrow$ M definierbar.

Folgerung. Der Wahrheitsbegriff von $\mathcal{N}$ ist nicht aufzählbar. Also: Leibniz' „ars inveniendi" kann es nicht geben.

Wahrheit $\mapsto$ Beweisbarkeit in einer formalen Theorie T.

Axiome: z.B. $A(0) \land \forall_x(A(x) \to A(\mathrm{S}(x))) \to \forall_x A(x)$.
Schlußregeln: z.B. modus ponens:

$$\frac{A \to B \qquad A}{B}$$

Annahmen über T:

- T ist axiomatisiert, d.h., $\mathrm{Bew}_T(n, m)$ ist entscheidbar.
- T ist widerspruchsfrei.
- T beweist die Axiome von Robinsons Theorie Q.

Ziel: T is unvollständig.

Robinsons Theorie Q

ist bestimmt durch die Axiome

$$\mathrm{S}(x) \neq 0,$$
$$\mathrm{S}(x) = \mathrm{S}(y) \to x = y,$$
$$x + 0 = x,$$
$$x + \mathrm{S}(y) = \mathrm{S}(x + y),$$
$$x \cdot 0 = 0,$$
$$x \cdot \mathrm{S}(y) = x \cdot y + x,$$
$$\exists_z\,(x + \mathrm{S}(z) = y) \vee x = y \vee \exists_z\,(y + \mathrm{S}(z) = x).$$

Unvollständigkeit

Theorem (Gödel, Rosser)

Man findet einen Satz A mit $T \nvdash A$ und $T \nvdash \neg A$.

Der Beweis verwendet als Hilfsmittel:

Lemma

Jede entscheidbare Relation R ist in T „repräsentierbar“ durch eine Formel $B_R(\vec{x})$.

Lemma (Syntaktisches Fixpunktlemma)

Zu jeder Formel $B(z)$ findet man einen Satz A mit

$$T \vdash A \leftrightarrow B(\ulcorner A \urcorner).$$

$\mathrm{Bew}_T(n, m)$ entscheidbar $\Rightarrow$ $\mathrm{Wdl}_T(n, m)$ entscheidbar.

Beweis des Unvollständigkeitssatzes

Eigenschaften von T:

$$T \vdash \forall_x \big(x < \underline{n} \to x = \underline{0} \vee \cdots \vee x = \underline{n-1}\big),$$
$$T \vdash \forall_x \big(x = \underline{0} \vee \cdots \vee x = \underline{n} \vee \underline{n} < x\big).$$

Seien $B_{\mathrm{Bew}_T}(x_1, x_2)$ und $B_{\mathrm{Wdl}_T}(x_1, x_2)$ repräsentierende Formeln zu Bew_T und Wdl_T. Fixpunktlemma: Satz A mit

$$T \vdash A \leftrightarrow \forall_x \big(B_{\mathrm{Bew}_T}(x, \underline{\ulcorner A \urcorner}) \to \exists_{y<x} B_{\mathrm{Wdl}_T}(y, \underline{\ulcorner A \urcorner})\big).$$

A besagt die eigene Unbeweisbarkeit: „Zu jedem Beweis von mir gibt es einen kürzeren Beweis meiner Negation“.

Hermann Weyl (Über die neue Grundlagenkrise der Mathematik, 1921):

> *Ein Existentialsatz – etwa „es gibt eine gerade Zahl“ – ist überhaupt kein Urteil im eigentlichen Sinne, das einen Sachverhalt behauptet; Existentialsachverhalte sind eine leere Erfindung der Logiker.*
>
> *„2 ist eine gerade Zahl“, das ist ein wirkliches, einem Sachverhalt Ausdruck gebendes Urteil; „es gibt eine gerade Zahl“ ist nur ein aus diesem Urteil gewonnenes Urteilsabstrakt.*

Beispiel eines Existenzbeweises ohne Zeugen:

Es gibt irrationale Zahlen a, b mit a^b rational.

Beweis durch Fallunterscheidung. Betrachte $\sqrt{2}^{\sqrt{2}}$.

Fall 1: $\sqrt{2}^{\sqrt{2}}$ ist rational. Wähle $a := \sqrt{2}$ und $b := \sqrt{2}$.
Dann sind a, b irrational, und nach Annahme ist a^b rational.

Fall 2: $\sqrt{2}^{\sqrt{2}}$ ist irrational. Wähle $a := \sqrt{2}^{\sqrt{2}}$ und $b := \sqrt{2}$.
Dann sind nach Annahme a, b irrational, und

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2 \quad \text{ist rational.}$$

Der finite Standpunkt

Hilberts Programm ($\sim$ 1920): Man zeige, daß die Verwendung abstrakter (idealer, unendlicher) Objekte in Beweisen von Sätzen mit einer konkreten Bedeutung eliminierbar ist (Beispiel: Hilberts Nullstellensatz).

Gödels (zweiter) Unvollständigkeitssatz $\Rightarrow$ dies ist im allgemeinen nicht möglich.

Ausweg: Approximation unendlicher Objekte. Beispiel: Eine reelle Zahl – etwa π – ist ein unendliches Objekt. Approximationen sind Anfangsstücke der Dezimalbruchentwicklung.

Gödel „Über eine bisher noch nicht benützte Erweiterung des finiten Standpunkts“ (1958): berechenbare Funktionale.

Zwischenwertsatz

Seien $a < b$ rational. Ist $f : [a, b] \to \mathbb{R}$ Lipschitz-stetig mit $f(a) \leq 0 \leq f(b)$, so findet man $x \in [a, b]$ mit $f(x) = 0$.

Aus einem Beweis des Zwischenwertsatzes erhält man einen Algorithmus zur Berechnung der Nullstelle.

Beispiel: $f(x) := x^2 - 2$ auf dem Intervall $[1, 2]$. Nullstelle: $\sqrt{2}$.

Der aus dem Existenzbeweis extrahierte Algorithmus liefert (mit Fehlerschranke 2^{-20}) in 8 ms

$$\frac{19103926996735726 43}{13508517176729920 89}$$

also

$$1.41421347\ldots$$

Einwände

- Eine Algorithmus-Idee ist schon vor einem konstruktiven Beweis vorhanden.
  (Oft richtig, aber: (a) Programm korrekt nach Konstruktion, (b) Programmentwicklung wird möglich)
- Komplexität des extrahierten Programms?
  (Man erhält in polynomialer Zeit berechenbare Funktionen, bei geeigneter Einschränkung der Beweismittel).
- Sind auch Beweise „ohne Zeugen“ verwendbar?
  (Ja, aber eine genauere Analyse ist erforderlich. Gödel hat eine solche Analyse in seiner Arbeit von 1958 durchgeführt)

Ausblick

Unentscheidbar, ob ein Programm seine Spezifikation erfüllt.
Formaler Beweis: Korrektheit leicht zu prüfen. Beweis = Programm mit hinreichend vielen Kommentaren
(genauer: Programm extrahierbar). Vision: Verwende mathematische Kultur zum Organisieren komplexer Strukturen, zwecks Programmextraktion
(Zum Beispiel: Steuerprogramme im Anlagenbau oder in der Telekommunikation).