

Einleitung

Algorithmen



ALGORITHMEN sind endliche Abfolgen von genau spezifizierten Schritten, um ein mathematisches oder logisches Problem zu lösen. Die Frage, vor der Hilbert stand, lautete: wenn man die Mathematik formalisiert, sind dann alle wahren Aussagen durch einen Algorithmus beweisbar? Oder: kann man durch einen Algorithmus, der alle möglichen Aussagen durchschreitet, von jeder Einzelnen in endlicher Zeit herausfinden, ob sie wahr ist oder nicht?

Für Hilbert schien die Sache klar zu sein: es musste so sein. Nur fehlte ihm der Beweis dafür. Erst Gödel zeigte, dass die Sache viel vertrackter ist und so nicht geht.

Beweisbarkeit und Gödelnummern

Was heißt ›beweisbar‹? Beweise sind Zurückführungen auf einzelne Axiome mithilfe von syntaktischen Veränderungsregeln. So kann man jede mathematische Aussage als Zeichenkette auffassen und schauen, ob man – durch erlaubte Veränderungen der Axiome des Systems – irgendwie auf diese Zeichenkette kommt. Hierbei ist Gödel ein großer Vorreiter der modernen Informatik, denn Computer können auch nur nach fest definierten Regeln Zeichenketten bearbeiten. Die mathematische Formel wird dabei nur sekundär inhaltlich betrachtet und primär als Ansammlung von Zeichen, die nach Regeln bearbeitet werden. Jede bewiesene mathematische Aussage lässt sich prinzipiell als sehr lange Zeichenkette darstellen, die nur aus den Grundoperationen besteht (z. B. XOR, AND und NOT in der modernen Computertechnik). Daraus lassen sich Operationen wie das Addieren herleiten, woraus sich das Multiplizieren herleiten lässt (mit ganzen Zahlen) usw. Aber das sind alles nur Vereinfachungen, damit wir als Menschen, die damit arbeiten, besser damit klarkommen. Inhaltlich ist ein $a + b$ gleichbedeutend mit einer langen Kette an UND, XOR und NICHT-Operationen im CPU eines Computers.

Gödel zeigte, dass es nicht möglich ist, alle wahren Aussagen zu beweisen, in dem er einen Algorithmus anbietet, der – komplett zurückführbar auf die logischen Grundaussagen –, immer Sätze konstruieren kann, die zwar durch metamathematische Überlegungen von ›außerhalb‹ des Systems als geltend gezeigt werden können, die aber nicht innerhalb des Systems beweisbar sind.

Die *Principia Mathematica* und die Typentheorie

Russell und Whitehead haben erkannt, dass man solche Sätze mit selbstreferenziellen Aussagen generieren kann, z. B. ›dieser Satz ist falsch‹, und daher haben sie in der Principia Mathematica solche Sätze, die sich auf sich selbst beziehen, ›verboten‹. Aber selbst, wenn man das verbietet, lassen sich dennoch vergleichbare Sätze konstruieren.

(Vereinfachtes) Beispiel für einen gödelisierten Satz

Wieder ein vereinfachtes Beispiel: wir nehmen an, dass jeder mit den Grundzeichen der Mathematik definierbare Satz eine Nummer bekommt. Dort sind nun alle nur überhaupt definierbaren Sätze, sinnvoll wie sinnlos, falsch wie richtig, wie z. B. › $45 + 16 = 1$ ‹, › $1 + 1 = 2$ ‹, aber auch ›der Satz mit der

1: Für die Spezifikationen der Schritte von Algorithmen siehe Knuth, TAOCP 1, S. 4f. Die Punkte sind:

- Finiteness
- Defineteness
- Input
- Output
- (Effectiveness; eingeklammert, weil Knuth Computer und praktische Algorithmen im Kopf hat; Gödels Beweise aufzuschreiben wäre alles andere als effizient; es ist aber *prinzipiell* möglich.)

2: Zumindest lassen sie sich analog zu solchen Regeln behandeln, wie die moderne Computertechnik eindrucksvoll zeigt. Vgl. Kommentar 29. Vgl. auch <https://www.youtube.com/watch?v=qT8NyyRgLDQ> für ein Weiterdenken in eine alternative Richtung, die aber auch das ›Gödelproblem‹ hat.

3: Die inhaltliche Betrachtung findet erst beim Menschen statt, der versucht, das, was die Formel aussagt, zu verstehen. Der Formel selbst liegt diese inhaltliche Deutung nicht bei, was unter Anderem zur extrem breiten Verwendbarkeit der Mathematik folgt. Vereinfacht gesagt: mit der gleichen Formel kann man berechnen, wie ein Atomkraftwerk funktioniert, aber auch eine Atombombe; zwei sehr unterschiedliche Anwendungsbereiche mit ähnlicher mathematische Struktur.

4: Vgl. Kommentar 42.

5: Kommentar 16 ist falsch.

6: \longrightarrow Typentheorie

Nummer 4922* ist nicht beweisbar«. Wenn aber letzterer Satz gerade ›zufällig« tatsächlich die zugewiesene Nummer 4922 hat, dann behauptet der Satz seine eigene Unbeweisbarkeit, und das mehr oder weniger zufällig, ohne dass eine selbstreferenzielle-Strukturen-verbietende Typentheorie das verbieten könnte.

Unbeweisbar heißt hier, dass der Satz nicht hergeleitet werden kann aus den gewählten Axiomen. Aber durch metamathematische Überlegungen können wir ihn doch als wahr anerkennen, weil er eben nicht aus den Axiomen herleitbar ist (d. h. unbeweisbar, was der Satz ja auch behauptet).

Das letzte Ressort könnte sein, ihn als Axiom zu setzen. Aber da alle potenziell möglichen Sätze generiert werden, dürfen wir den Satz mit der Nummer 559321 nicht aus den Augen verlieren, er besagt: ›der Satz mit der Nummer 559321 ist nicht beweisbar«. Wir stehen also wieder vor dem gleichen Problem und müssten wieder ein Axiom setzen. Das geht ewig so weiter. Wir haben (nach unendlich viel vergangener Zeit und unendlich vielen neuen Axiomen) also wieder ein System, das aber nicht mehr algorithmisch lösbar ist, weil Algorithmen, die etwas lösen sollen, keine unendliche Menge an Axiomen abarbeiten können.

Gödels Algorithmus bietet die Möglichkeit, jedem sinnvollen und sinnlosen Satz eine eindeutige Nummer zuzuordnen, indem er einige Konstanten definiert, z. B. wird ›0« zu 1, ›f« zu 3, ›~« zu 5 usw. Außerdem nutzt er die Eineindeutigkeit von Primfaktorzerlegungen aus. So kann man den (sinnlosen) Satz: ›es gilt nicht, dass 4« folgendermaßen umwandeln:

1. ›es gilt nicht, dass 4«
2. ›~ 4«
3. ›~ f f f f 0« (mit der peano'schen Nachfolgerfunktion *f*)
4. Nun nehmen wir die Position *p* im String (angefangen von links mit 1) und nehmen die *pte* Primzahl als Basis (*p*(*p*)), die Ziffer für das Zeichen als Exponent: *p*(1)⁵ × *p*(2)³ × *p*(3)³ × *p*(3)³ × *p*(4)³ × *p*(5)¹. Wir erhalten: 2⁵ × 3³ × 5³ × 7³ × 11³ × 13¹ = 640972332000. Dies können wir, da es unendlich viele Primzahlen gibt, für jede beliebig lange Zeichenkette bestehend aus den Grundzeichen machen. Die Zahl 640972332000 lässt sich durch Primfaktorzerlegung prinzipiell wieder 1:1 in den Ursprungssatz zurückwandeln, so dass gilt:

640972332000 ≡ ›es gilt nicht, dass 4«

Die Zahl 640972332000 ist damit eindeutig ebendiesem Satz zugeordnet und mit dem gewählten Alphabet keinem anderen (→ Eineindeutigkeit).

Der Begriff der Beweisbarkeit lässt sich im System der Principia Mathematica selbst darstellen als die Möglichkeit der Herleitung aus den Axiomen. Nehmen wir die Abkürzungen von Gödel selbst, dann können wir die Beweisbarkeit eines Satzes folgendermaßen darstellen: Bew(*x*). Wenn wir also einen Satz der Form:

$$n \vdash \sim \text{Bew}(m)$$

(wobei *n* seine gödelisierte Satznummer und ›zufälligerweise« *n* = *m*, d. h. eine lange Zahl, die eindeutig dem Satz zugeordnet ist, ist[†], der rein zufällig auf sich

*Die Nummern sind nur beispielhaft gewählt und entsprechen nicht der wirklichen Gödelisierung der Sätze.

†Wie Gödel es selbst sagt, wäre es kein Problem, diese Zahl für jede Aussage tatsächlich aufzuschreiben; es wäre nur sehr umständlich, siehe Fußnote 10.

7: Siehe dazu Fußnote 15.

8: Dieser Satz könnte auch aussagen: ~~~ Bew(4922), wenn man mehr als die absolute Minimalmenge nimmt. Vgl. dazu Kommentar 52. Aber das würde die Sache nur komplizierter machen.

9: Siehe dazu S. 177. Die gewählten Grundzeichen hängen vom System ab, das man als Grundlage nehmen möchte. Gödel nimmt das System der Peano-Axiome mit dem System der Principia Mathematica zusammen zur Vereinfachung seines Beweises.

10: Jede natürliche Zahl ist entweder selbst Prim oder das Produkt aus *n* Primzahlen. Die Zerlegung einer Zahl in Primzahlen ist eindeutig und jede Zahl hat exakt eine ihr zugeordnete Primfaktorzerlegung. Nimmt man die Position *p* als *pte* Primzahl hoch einer Zahl, die ein spezielles Zeichen symbolisiert, so lässt sich diese Zahl jederzeit zurückwandeln in den ursprünglichen Satz, weil die Primfaktorzerlegung immer eindeutig bleibt.

11: Siehe dazu § 16 (0 N x)

12: Siehe dazu § 17 (Z(n))

13: Die Eineindeutigkeit der Zuordnung von Zahlenwerten zu Zeichenketten bedeutet de facto, dass jede mögliche Zeichenkette existiert; diese Eineindeutigkeit Zahl ↔ Satz ist wichtig, denn in diesen unendlich vielen Sätzen wären alle Texte nach ›mathematischer Grammatik« entstanden. Vgl. dazu die Idee der ›Library of Babel«, wo zwar (wahrscheinlich) nicht alle Texte gespeichert werden, sie aber im Bereich der mathematischen Hashfunktion, die angewandt wird, um die Seiten ›statisch« zu erzeugen, dennoch bereits alle ›existieren«; hierzu auch eine metaphysische Anmerkung: damit wird ein platonischer Realismus der mathematischen Welt vorausgesetzt, in der das Ergebnis jeder Gleichung schon ›existiert«, unabhängig davon, ob ausgerechnet oder nicht. In einem z. B. ultrafinitistischen Denkmodell wäre Gödel gar kein Problem (womit ich nicht dafür argumentieren möchte, sondern eher Platonist bin).

14: Vgl. § 44 (Bw)

15: Vgl. § 46 (Bew)

16: Kommentar 5 ist richtig.

selbst verweist), dann haben wir einen solchen Satz, der seine eigene Unbeweisbarkeit behauptet und im System nicht entscheidbar ist. Wäre er beweisbar, wäre er per definitionem richtig, weil nur richtige Sätze beweisbar sind, aber wäre er beweisbar, wäre er auch per definitionem unbeweisbar. Seine Richtigkeit lässt sich aber eben durch metamathematische Überlegungen zeigen.

17: Vgl. Kommentar 42.

› . . . *und verwandter Syteme* ‹

Für solche Sätze sind Systeme wie das der Principia Mathematica prinzipiell überflüssig, weil diese nur auf den logischen Axiomen aufbauen und Abkürzungen für lange Reihen von Zeichenketten darstellen. Daher sind alle logisch-formalen Systeme betroffen und die Principia ist nur ein ›Einstiegspunkt‹ zur Vereinfachung der Thesen.

Benötigt zum Erzeugen solcher Sätze sind nur die logischen Schlussregeln und die potenzielle Möglichkeit, etwas wie natürliche Zahlen herzuleiten, sowie die Möglichkeit, im System selbst herauszufinden, ob ein Satz ein Beweis eines anderen Satzes ist, ohne dabei auf ein Metasystem zurückzugreifen.

18: Siehe wieder Fußnote 10

ω-Widerspruchsfreiheit

Ein System, in dem die Axiome keine Widersprüchlichkeiten aufweisen, heißt ›widerspruchsfrei‹. Aber nicht jedes widerspruchsfreie System ist auch *ω*-widerspruchsfrei. Die *ω*-Widerspruchsfreiheit ist rigoroser als die allgemeine Widerspruchsfreiheit, denn in der *ω*-Widerspruchsfreiheit gilt – neben der allgemeinen Widerspruchsfreiheit –, dass auch keine kontraintuitiven Schlüsse gezogen werden können dürfen (z. B. Sätze, die wahr sind, ohne dass ihre Wahrheit aus den Axiomen herleitbar ist).

Die Axiome der PM sind widerspruchsfrei, aber mit der Methode der Gödelisierung lassen sich ebensolche Existenzaussagen treffen, die das System *ω*-widersprüchlich machen. Dies gilt für alle ausreichend komplexen Systeme. Wenn ein System ausreichend komplex ist, dann ist es notwendigerweise unvollständig, d. h. es gibt Existenzaussagen, die nicht aus den Axiomen herleitbar sind (erster Unvollständigkeitssatz). Kann man jedoch die Vollständigkeit des ausreichend-komplexen Systems beweisen, ist es notwendigerweise widersprüchlich (zweiter Unvollständigkeitssatz).

19: Dazu muss es nur *irgendwie* möglich sein, aus dem System etwas wie die natürlichen Zahlen und Addition herleiten zu können, was auf fast alle praktisch-relevanten logisch-widerspruchsfreien Systeme zutrifft. Dazu muss es auch möglich sein, dass im genannten System der Begriff ›die Formel *f* ist beweisbar im System *S*‹ definierbar ist.

20: Vgl. Satz VIII auf S. 190.

21: Vgl. Satz XI auf S. 193.

Vollständigkeit und Entscheidbarkeit

Ein formales System *P* ist vollständig, wenn jede Aussage *p* ∈ *P* entweder exakt *wahr* oder *falsch* ist. Wenn im System für jeden Wert von *p* der Wahrheitswert algorithmisch anhand der Regeln des formalen Systems bestimmt werden kann, heißt das System ›entscheidbar‹.

Es gibt Systeme, auf die die gödelschen Unvollständigkeitssätze nicht zutreffen, beispielsweise die Presburger-Arithmetik; diese sind aber sehr eingeschränkt (z. B. unterstützt die Presburger-Arithmetik keine Aussagen über Multiplikation, Division oder Primzahlen).

22: Ohne Primzahlen lassen sich die gödelschen Unvollständigkeitssatzbeweise nicht konstruieren, weil es keine sonstige Möglichkeit gibt, jedem Satz eine eindeutige, algorithmisch bestimmbare Nummer zuzuweisen.

Die beiden Unvollständigkeitssätze

Aus der Arbeit Gödels folgen zwei fundamentale Sätze zur Metamathematik:

1. Jedes ausreichend komplexe System beinhaltet immer Sätze, die innerhalb des Systems nicht bewiesen werden können.

2. Jedes ausreichend komplexe System kann seine eigene Widerspruchsfreiheit nicht beweisen; wenn es das kann, dann ist es notwendigerweise widersprüchlich.

23: Zweiter Unvollständigkeitssatz, vgl. Kommentar 131.

Auswirkungen

Die Auswirkungen auf das Verständnis der Mathematik waren gewaltig, denn plötzlich war klar, dass man nicht jede wahre Aussage auch beweisen kann. Aber auch für die Berechenbarkeitstheorie und die später aufkommende Informatik sind betroffen. Gödels Ansatz, mathematische Aussagen als Ansammlungen von nach Regeln gebildeter Zeichen zu sehen und nicht primär inhaltlich zu deuten, hat die moderne Informatik überhaupt erst möglich gemacht. Kein Computer kann mehr als ebendies: Zeichenketten nach genau vorgelegten Regeln zu manipulieren, ohne dabei auch nur im Ansatz inhaltlich auf diese einzugehen. Gödel hat gezeigt, dass es immer Aussagen gibt, die ein Computer nicht zurückführen kann auf seine Axiome, d. h. dass es immer Aussagen gibt, die mit einem Computer nicht überprüfbar sind. Das setzt – ähnlich wie das Halteproblem – der Theorie der Algorithmen sowie der Beweistheorie überhaupt enge Grenzen.

Ziel dieser Arbeit

Im Rahmen dieser Arbeit würde ich gern versuchen, den Originalalgorithmus soweit es mir möglich ist nachzuvollziehen. Dazu habe ich die Arbeit von Gödel soweit ich es konnte exakt abgetippt und mit \LaTeX , einem Textsatzsystem für mathematische Texte, komplett neu gesetzt, um einige Dinge wie eingefärbte passende Klammern zur besseren Lesbarkeit einzuführen und Kommentare hinzuzufügen, die die gödel'schen Formeln in eine modernere Schreibweise übertragen. Trotz größtmöglicher Mühe und Bemühung um Genauigkeit kann ich dabei natürlich nicht vermeiden, dass sich eventuell Tipp- oder Verständnisfehler eingeschlichen haben.

Lizenz

Da es meiner Recherchen nach noch keine solche Version gab, habe ich sie der Forschung auf meinem GitHub-Account unter der GPL2-Lizenz zur Verfügung gestellt[‡]. Jeder kann diese Version forken und eigene Änderungen hinzufügen, um das Dokument möglichst vollständig zu machen und meine Fehler zu korrigieren. Es unterliegt keinen Einschränkungen für Forschung und Lehre, außer dass (wie in der GPL2 mit *Copyleft* üblich) jede Änderung selbst wieder öffentlich gemacht und unter die GPL2 gestellt werden muss.

Juristisch beziehe ich mich auf § 3 des Urheberrechtsgesetzes, das eine Bearbeitung und Kommentierung eines Werkes mit eigener Schöpfungshöhe erlaubt.

[‡]Siehe <https://github.com/NormanTUD/GoedelLaTeX/>.

Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I¹

Von **Kurt Gödel** in Wien.

1.

Die Entwicklung der Mathematik in der Richtung zu größerer Exaktheit hat bekanntlich dazu geführt, daß weite Gebiete von ihr formalisiert wurden, in der Art daß das Beweisen nach einigen wenigen mechanischen Regeln vollzogen werden kann. Die umfassendsten derzeit aufgestellten formalen Systeme sind das System der Principia Mathematica (PM)² einerseits, das Zermelo-Fraenkelsche (von J. v. Neumann weiter ausgebildete) Axiomensystem der Mengenlehre³ andererseits. Diese beiden Systeme sind so weit, daß alle heute in der Mathematik angewendeten Beweismethoden in ihnen formalisiert, d. h. auf einige wenige Axiome und Schlußregeln zurückgeführt sind. Es liegt daher die Vermutung nahe, daß diese Axiome und Schlußregeln dazu ausreichen, alle mathematischen Fragen, die sich in den betreffenden Systemen überhaupt formal ausdrücken lassen, auch zu entscheiden. Im folgenden wird gezeigt, daß dies nicht der Fall ist, sondern daß es in den beiden angeführten Systemen sogar relativ einfache Probleme aus der Theorie der gewöhnlichen Zahlen gibt⁴, die sich aus den Axiomen nicht entscheiden lassen. Dieser Umstand liegt nicht etwa an der speziellen Natur der aufgestellten Systeme, sondern gilt für eine sehr weite Klasse formaler Systeme, zu denen insbesondere alle gehören, die aus den beiden angeführten durch Hinzufügung endlich vieler Axiome entstehen⁵, vorausgesetzt, daß durch die hinzugefügten Axiome keine falschen Sätze von denen in der Fußnote 4 angegebenen Art beweisbar werden.

Wir skizzieren, bevor wir auf Details eingehen, zunächst den Hauptgedanken des Beweises, natürlich ohne auf Exaktheit Anspruch zu erheben. Die Formeln eines formalen Systems (wir beschränken uns hier auf das System PM) sind äußerlich betrachtet endliche Reihen der Grundzeichen (Variable, logische Konstante und Klammern bzw. Trennungspunkte) und man kann leicht genau präzisieren, welche Reihen von Grundzeichen sinnvolle Formeln sind und welche nicht⁶.

24: Das Hilbert-Programm forderte, dass alle mathematischen Sachverhalte zurückführbar sein müssen auf einfache logische Operationen. In der Principia Mathematica haben Russell und Whitehead genau das zu erreichen versucht.

25: Das ist die Grundfrage vom Hilbertprogramm: lassen sich alle mathematischen Fragestellungen von innerhalb eines formalisierten Systems aus lösen?

26: Alle Systeme, die komplex genug sind, dass sich aus ihnen etwas wie natürliche Zahlen und Addition auch nur `h e r l e i t e n` lassen, und in denen selbst definierbar ist, dass eine Aussage ein Beweis einer anderen Aussage ist, sind betroffen

27: Durch das Hinzufügen von *unendlich* vielen Axiomen wäre das System praktisch nicht mehr verwendbar und es gäbe potenziell gar keine unbewiesenen Aussagen. Daher der Fokus auf die Systeme mit endlich vielen Axiomen.

28: Es geht erstmal um eine rein syntaktische Betrachtung, ohne auf den Inhalt Bezug zu nehmen

¹Vgl. die im Anzeiger der Akad. d. Wiss. in Wien (math.-naturw. Kl.) 1930, Nr. 19 erschienene Zusammenfassung der Resultate dieser Arbeit.

²A. Whitehead und B. Russell, Principia Mathematica, 2. Aufl., Cambridge 1925. Zu den Axiomen des Systems PM rechnen wir insbesondere auch: Das Unendlichkeitsaxiom (in der Form: es gibt genau abzählbar viele Individuen), das Reduzibilitäts- und das Auswahlaxiom (für alle Typen).

³Vgl. A. Fraenkel, Zehn Vorlesungen über die Grundlegung der Mengenlehre, Wissensch. u. Hyp. Bd. XXXI. J. v. Neumann, die Axiomatisierung der Mengenlehre. Math. Zeitschr. 27, 1928. Journ. f. reine u. angew. Math. 154 (1925), 160 (1929). Wir bemerken, daß man zu den in der angeführten Literatur gegebenen mengentheoretischen Axiomen noch die Axiome und die Schlußregeln des Logikkalküls hinzufügen muß, um die Formalisierung zu vollenden. – Die nachfolgenden Überlegungen gelten auch für die in den letzten Jahren von D. Hilbert und seinen Mitarbeitern aufgestellten formalen Systeme (soweit diese bisher vorliegen). Vgl. D. Hilbert, Math. Ann. 88, Abh. aus d. math. Sem. der Univ. Hamburg I (1922), VI (1928). P. Bernays, Math. Ann. 93.

⁴D. h. genauer, es gibt unentscheidbare Sätze, in denen außer den logischen Konstanten: `(nicht)`, `∨` (oder), `(x)` (für alle), `=` (identisch mit) keine anderen Begriffe vorkommen als `+` (Addition), `.` (Multiplikation), beide bezogen auf natürliche Zahlen, wobei auch die Präfixe `(x)` sich nur auf natürliche Zahlen beziehen dürfen.

⁵Dabei werden in PM nur solche Axiome als verschieden gezählt, die aus einander nicht bloß durch Typenwechsel entstehen.

⁶Wir verstehen hier und im folgenden Unter „Formel aus PM“ immer eine ohne Abkürzungen (d. h. ohne Verwendung von Definitionen) geschriebene Formel. Definitionen dienen ja nur der kürzeren Schreibweise und sind daher prinzipiell überflüssig.

Analog sind Beweise vom formalen Standpunkt nichts anderes als endliche Reihen von Formeln (mit bestimmten angebbaren Eigenschaften). Für metamathematische Betrachtungen ist es natürlich gleichgültig, welche Gegenstände man als Grundzeichen nimmt, und wir entschließen uns dazu, natürliche Zahlen⁷ als solche zu verwenden. Dementsprechend ist dann eine Formel eine endliche Folge natürlicher Zahlen⁸ und eine Beweisfigur eine endliche Folge von endlichen Folgen natürlicher Zahlen. Die metamathematischen Begriffe (Sätze) werden dadurch zu Begriffen (Sätzen) über natürliche Zahlen bzw. Folgen von Solchen⁹ und daher (wenigstens teilweise) in den Symbolen des Systems PM selbst ausdrückbar. Insbesondere kann man zeigen, daß die Begriffe „Formel“, „Beweisfigur“, „beweisbare Formel“ innerhalb des Systems PM definierbar sind, d. h. man kann z. B. eine Formel $F(\nu)$ aus PM mit einer freien Variablen ν (vom Typus einer Zahlenfolge) angeben¹⁰, so daß $F(\nu)$ inhaltlich interpretiert besagt: ν ist eine beweisbare Formel. Nun stellen wir einen unentscheidbaren Satz des Systems PM, d. h. einen Satz A , für den weder A noch $\textit{non-}A$ beweisbar ist, folgendermaßen her:

Eine Formel aus PM mit genau einer freien Variable, u. zw. vom Typus der natürlichen Zahlen (Klasse von Klassen) wollen wir ein `K l a s s e n z e i c h e n` nennen. Die Klassenzeichen denken wir uns irgendwie in eine Folge geordnet¹¹, bezeichnen das n -te mit $R(n)$ und merken, daß sich der Begriff „Klassenzeichen“ sowie die ordnende Relation R im System PM definieren lassen. Sei α ein beliebiges Klassenzeichen, mit $[\alpha ; n]$ bezeichnen wir diejenige Formel, welche aus dem Klassenzeichen α dadurch entsteht, daß man die freie Variable durch das Zeichen für die natürliche Zahl n ersetzt. Auch die Tripel-Relation $\alpha = [y ; z]$ erweist sich als innerhalb von PM definierbar. Nun definieren wir eine Klasse K natürlicher Zahlen folgendermaßen:

$$n \epsilon K \equiv \overline{Bew} [R(n) ; n]^{11a}$$

(1)

(wobei $Bew\ x$ bedeutet: x ist eine beweisbare Formel). Da die Begriffe, welche im Definiens vorkommen, sämtlich in PM definierbar sind, so auch der daraus zusammengesetzte Begriff K , d. h. es gibt ein Klassenzeichen S ¹², so daß die Formel $[S ; n]$ inhaltlich gedeutet besagt, daß die natürliche Zahl n zu K gehört. S ist als Klassenzeichen mit einem bestimmten $R(q)$ identisch, d. h. es gilt

$$S = R(q)$$

für eine bestimme natürliche Zahl q . Wir zeigen nun, daß der Satz $[R(q) ; q]$ ¹³ in

⁷D. h. wir bilden die Grundzeichen in eineindeutiger Weise auf die natürlichen Zahlen ab (Vgl. die Durchführung auf S. 177.)

⁸D. h. eine Belegung eines Abschnittes der Zahlenreihe mit natürlichen Zahlen. (Zahlen können ja nicht in räumliche Anordnung gebracht werden.)

⁹m. a. W.: Das oben beschriebene Verfahren liefert ein isomorphes Bild des Systems PM im Bereich der Arithmetik und man kann alle metamathematischen Überlegungen ebenso gut an diesem isomorphen Bild vornehmen. Dies geschieht in der folgenden Beweisskizze, d. h. unter „Formel“, „Satz“, „Variable“ etc. sind immer die entsprechenden Gegenstände des isomorphen Bildes zu verstehen.

¹⁰Es wäre sehr leicht (nur etwas umständlich), diese Formel tatsächlich hinzuschreiben.

¹¹Etwa nach steigender Gliedersumme und bei gleicher Summe lexikographisch.

^{11a}Durch Überstreichen wird die Negation bezeichnet.

¹²Es macht wieder nicht die geringsten Schwierigkeiten, die Formel S tatsächlich hinzuschreiben.

¹³Man beachte, daß „ $[R(q) ; q]$ “ (oder was dasselbe bedeutet „ $[S ; q]$ “) bloß eine `m e t a m a t h e m a t i s c h e B e s c h r e i b u n g` des unentscheidbaren Satzes ist. Doch kann man, sobald man die Formel S ermittelt hat, natürlich auch die Zahl q bestimmen und damit den unentscheidbaren Satz selbst effektiv hinschreiben.

29: Ein Beweis ist eine für den Computer nachvollziehbare Kette an a., entweder Axiomen oder b., Schlussfolgerungen aus den Axiomen (vgl. Tractatus Logico Philosophicus, § 6.126 und § 6.1262)

30: Natürliche Zahlen sind relativ einfach über die Peano-Axiome herleitbar und zu verstehen. Es könnten aber auch andere mathematische Strukturen genommen werden, wenn sie aus den Axiomen folgen, die dann analoge Schlüsse zulassen.

31: Vgl. Kommentar 13

32: Vgl. § 32 (Logische Operatoren), 44 (Bw), 46 (Bew)

33: Das ist eine rein-syntaktische Definition, die zahlentheoretisch aus den Axiomen überprüft werden kann (zumindest im Beispielsystem der PM). Vgl. § 46 (Bew)

34: Da jede Zahl eineindeutig einer Formel zugeordnet werden kann (durch Primfaktorzerlegung), gibt es in \mathbb{N} alle sinnvollen und sinnlosen Formeln, die denkbar sind. Das heißt, dort gibt es alle beweisbaren Formeln, aber auch alle die, die nicht beweisbar sind. Gödel definiert hier ein $n \in K$ so, dass $n \leftrightarrow$ eine nicht beweisbare Formel ist.

35: $\exists n : n \in K \wedge \sim Bew [R(n) ; n]$, vgl. § 46 (Bew)

36: Vgl. § 46 (Bew)

37: $n \in K$

PM unentscheidbar ist. Denn angenommen, der Satz $[R(q); q]$ wäre beweisbar, dann wäre er auch richtig, d. h. aber nach dem obigen q würde zu K gehören, d. h. nach 1 es würde $\overline{Bew}[R(q); q]$ gelten, im Widerspruch mit der Annahme. Wäre dagegen die Negation von $[R(q); q]$ beweisbar, so würde $n\epsilon K$, d. h. $Bew[R(q); q]$ gelten. $[R(q); q]$ wäre also zugleich mit seiner Negation beweisbar, was wiederum unmöglich ist.

Die Analogie dieses Schlusses mit der Antinomie Richard springt in die Augen. Auch mit dem „Lügner“ besteht eine nahe Verwandtschaft¹⁴, denn der unentscheidbare Satz $[R(q); q]$ besagt ja, daß q zu K gehört, d. h. nach 1, daß $[R(q); q]$ nicht beweisbar ist. Wir haben also einen Satz vor uns, der seine eigene Unbeweisbarkeit behauptet¹⁵.

Die eben auseinandergesetzte Beweismethode läßt sich offenbar auf jedes formale System anwenden, das erstens inhaltlich gedeutet über genügen Ausdrucksmittel verfügt, um die in der obigen Überlegung vorkommenden Begriffe (insbesondere den Begriff „beweisbare Formel“) zu definieren, und in dem zweitens jede beweisbare Formel auch inhaltlich richtig ist. Die nun folgende exakte Durchführung des obigen Beweises wird unter anderem die Aufgabe haben, die zweite der eben angeführten Voraussetzungen durch eine rein formale und weit schwächere zu ersetzen.

Aus der Bemerkung, daß $[R(q); q]$ seine eigene Unbeweisbarkeit behauptet, folgt sofort, daß $[R(q); q]$ richtig ist, denn $[R(q); q]$ ist ja unbeweisbar (weil unentscheidbar). Der im System PM unentscheidbare Satz wurde also durch metamathematische Überlegungen doch entschieden. Die genaue Analyse dieses merkwürdigen Umstandes führt zu überraschenden Resultaten, bezüglich der Widerspruchsfreiheitsbeweise formaler System, die in Abschn. 4. (Satz XI) näher behandelt werden.

2.

Wir gehen nun an die exakte Durchführung des oben skizzierten Beweises und geben zunächst eine genaue Beschreibung des normalen Systems P , für welches für die Existenz unentscheidbarer Sätze nachweisen wollen. P ist im wesentlichen das System, welches man erhält, wenn man die Peanoschen Axiome mit der Logik der PM¹⁶ überbaut (Zahlen als Individuen, Nachfolgerrelation als undefinierten Grundbegriff).

Die Grundzeichen des Systems P sind die folgenden:

- I. Konstante: „ \sim “ (nicht), „ \vee “ (oder), „ Π “ (für alle), „ 0 “ (Null), „ f “ (der Nachfolger von), „ $($, „ $)$ “ (Klammern),
- II. Variable ersten Typs (für Individuen, d. h. natürliche Zahlen inklusive 0): „ x_1 “, „ y_1 “, „ z_1 “, \dots ,
Variable zweiten Typs (für Klassen von Individuen): „ x_2 “, „ y_2 “, „ z_3 “, \dots ,
Variable dritten Typs (für Klassen von Klassen von Individuen): „ x_3 “, „ y_3 “, „ z_3 “, \dots usw. für jede natürliche Zahl als Typus¹⁷.

¹⁴Es läßt sich überhaupt jede epistemologische Antinomie zu einem derartigen Unentscheidbarkeitsbeweis verwenden.

¹⁵Ein solcher Satz hat entgegen dem Anschein nichts Zirkelhaftes an sich, denn er behauptet zunächst die Unbeweisbarkeit einer ganz bestimmten Formel (nämlich der q -ten in der lexikographischen Anordnung bei der bestimmten Einsetzung), und erst nachträglich (gewissermaßen zufälligen) stellt sich heraus, daß diese Formel gerade die ist, in der er selbst ausgedrückt wurde.

¹⁶Die Hinzufügung der Peanoschen Axiome ebenso wie alle anderen am System PM angebrachten Abänderungen dienen lediglich zur Vereinfachung des Beweises und sind prinzipiell entbehrlich.

¹⁷Es wird vorausgesetzt, daß für jeden Variablentypus abzählbar viele Zeichen zur Verfügung stehen.

38: Wäre der Satz beweisbar, wäre er per definitionem wahr und damit unbeweisbar. Ein logischer Widerspruch.

39: Der Satz bezieht sich nicht direkt auf sich selbst, sondern nur „zufällig“, weil er eine von unendlich vielen Möglichkeiten in \mathbb{N} ist, von denen einige sich auf sich selbst beziehen müssen. Damit ist die Typentheorie Russells ›ausgehebelt‹, die nur explizite Eigenbezüge verbieten kann, aber keine rein-zufälligen.

40: Damit sind extrem viele Systeme betroffen, denn in fast allen komplexeren Systemen sind die Mittel dafür irgendwie zumindest prinzipiell herleitbar; das reicht.

41: Die Bedingungen für die Unvollständigkeit: der Begriff ›beweisbare Formel‹ muss im System definiert sein, jede beweisbare Formel muss inhaltlich richtig sein.

42: Wenn der Satz $S = [R(q); q]$ unbeweisbar ist und er nicht bewiesen werden kann, dann ist er wahr. Das kann dann durch die metamathematische Überlegung gezeigt werden, dass man eben sieht, dass die Aussage wahr ist, weil sie eben nicht beweisbar ist.

43: $P = \text{PM} + \text{Peano-Axiome}$

44: Wieder erstmal rein syntaktisch

45: Siehe die auf S. 177 definierten Grundzeichen, die je konstant einer Zahl zugeordnet sind.

46: Für Individuenvariablen.

47: Für Klassen, die aus einzelnen Individuenvariablen bestehen.

48: Für Klassen, deren Elemente selbst wieder Klassen sind.

Anm.: Variable für zwei- und mehrstellige Funktionen (Relationen) sind als Grundzeichen überflüssig, da man Relationen als Klassen geordneter Paare definieren kann und geordnete Paare wiederum als Klassen von Klasse, z. B. das geordnete Paar a, b durch $((a), (a, b))$, wo (x, y) bzw. (x) die Klassen bedeuten, deren einzige Elemente x, y bzw. x sind¹⁸.

Unter einem Zeichen ersten Typs verstehen wir eine Zeichenkombination der Form:

$a, fa, ffa, fffa \dots$ usw.

wo a entweder 0 oder eine Variable ersten Typs ist. Im ersten Fall nennen wir ein solches Zeichen Zahlzeichen. Für $n > 1$ verstehen wir unter einem Zeichen n -ten Typs dasselbe wie Variable n -ten Typs. Zeichenkombinationen der Form $a(b)$, wobei b ein Zeichen n -ten und a ein Zeichen $n + 1$ -ten Typs ist, nennen wir Elementarformeln. Die Klasse der Formeln definieren wir als die kleinste Klasse¹⁹, zu welcher sämtliche Elementarformeln gehören und zu welcher zugleich mit a, b stets auch $\sim (a)$, $(a) \vee (b)$, $x\Pi(a)$ gehören (wobei x eine beliebige Variable ist)^{18a} $(a) \vee (b)$. nennen wir Disjunktion aus a und b , $\sim (a)$ die Negation und $x\Pi(a)$ eine Generalisation von a . Satzformel heißt eine Formel, in der keine freie Variable vorkommt (freie Variable in der bekannten Weise definiert). Eine Formel mit genau n -freien Individuenvariablen (und sonst keinen freien Variablen) nennen wir n -stelliges Relationszeichen, für $n = 1$ auch Klassenzeichen.

Unter Subst $a \left(\begin{smallmatrix} v \\ b \end{smallmatrix} \right)$ (wo a eine Formel, v eine Variable und b ein Zeichen vom selben Typ wie v bedeutet) verstehen wir die Formel, welche aus a entsteht, wenn man darin v überall, wo es frei ist, durch b ersetzt²⁰. Wir sagen, daß eine Formel a eine Typenerhöhung einer anderen b ist, wenn a aus b dadurch entsteht, daß man den Typus aller in b vorkommenden Variablen um die gleiche Zahl erhöht.

Folgende Formeln (I bis V) heißen Axiome (sie sind mit Hilfe der in bekannter Weise definierten Abkürzungen: $\cdot, \supset, \equiv, (Ex)$, =²¹ und mit der Verwendung der üblichen Konventionen über das Weglassen von Klammern geschrieben²²):

- I. 1. $\sim (fx_1 = 0)$
2. $fx_1 = fy_1 \supset x_y = y_1$
3. $x_2(0) \cdot x_1\Pi(x_2(x_1) \supset x_2(fx_1)) \supset x_1\Pi(x_2(x_1))$.

¹⁸Auch inhomogene Relationen können auf diese Weise definieren werden, z. B. eine Relation zwischen Individuen und Klassen als eine Klasse aus Elementen der Form: $((x_2), ((x_1), x_3))$. Alle in den PM über Relationen beweisbaren Sätze sind, wie eine einfache Überlegung lehrt, auch bei dieser Behandlungsweise beweisbar.

¹⁹Bez. dieser Definition (und analoger später vorkommender), vgl. J. Łukasiewicz und A. Tarski, Untersuchungen über den Aussagenkalkül, Comptes Rendus des séances de la Société de Sciences et Lettres de Varsovie XXIII, 1930, Cl. III.

^{18a} $x\Pi(a)$ ist also auch dann eine Formel, wenn x in a nicht oder nicht frei vorkommt. In diesem Fall bedeutet $x\Pi(a)$ natürlich dasselbe wie a .

²⁰Falls v in a nicht als freie Variable vorkommt, soll Subst $a \left(\begin{smallmatrix} v \\ b \end{smallmatrix} \right) = a$ sein. Man beachte, daß „Subst“ ein Zeichen der Metamathematik ist.

²¹ $x_1 = y_1$ ist, wie in PM I, * 13 durch $x_2\Pi(x_2(x_1) \supset x_2(y_1))$ definiert zu denken (ebenso für die höheren Typen).

²²Um aus den angeschriebenen Schemata die Axiome zu erhalten, muß man also (in II, II, IV nach Ausführung der erlaubten Einsetzungen) noch

1. die Abkürzungen elimieren,
2. die unterdrückten Klammern hinzufügen.

Man beachte, daß die so entstehenden Ausdrücke „Formeln“ im obigen Sinn sein müssen. (Vgl. auch die exakten Definitionen der metamathe. Begriffe S. 180fg.)

49: Somit wird $f(x, y, z, \dots)$ zu $f(\mathfrak{r})$ und \mathfrak{r} expandiert zu (x, y, z, \dots) , vgl. Fußnote 30.

50: Damit sind mit der peanoschen Nachfolgerfunktion gemeint: $0, 1, 2, 3, \dots$. Daher auch der Name »Zahlzeichen«.

52: Dann ist die Metamathematik eine vollständige Theorie, die alle Formeln (oder Meinungen, Mengen, zu Mengen, $x : (a)$ mit x als beliebigem Zahlzeichen. Praktisch ist das dann ein großes Array von langen Zahlen, deren Verneinungen, deren Adjunktion und deren Generalisierung(auch alles Zahlen).

53: Subst $a \left(\begin{smallmatrix} v \\ b \end{smallmatrix} \right) = \$a \text{ } = \sim \text{ } s/\backslash bv \backslash b/b/g$

54: a ist Typenerhöhung von b , wenn man a aus b konstruieren kann, indem man die Typen (Zahlzeichen oder Klasse oder Klasse von Klassen) aller in b vorkommenden Variablen erhöht.

55: 0 ist nicht Nachfolger irgendeiner natürlichen Zahl

56: Wenn die Nachfolger gleich sind, ist die Zahl gleich

II. Jede Formel, die aus den folgenden Schemata durch Einsetzung beliebiger Formeln für p, q, r entsteht.

1. $p \vee p \supset p$
2. $p \supset p \vee p$
3. $p \vee q \supset q \vee p$
4. $(p \supset q) \supset (r \vee p \supset r \vee q)$

III. Jede Formel, die aus einem der beiden Schemata

1. $\nu \Pi(a) \supset \text{Subst } a \begin{pmatrix} \nu \\ c \end{pmatrix}$
2. $\nu \Pi(b \vee a) \supset b \vee \nu \Pi(a)$

dadurch entsteht, daß man für a, ν, b, c folgende Einsetzungen vornimmt (und in 1. die durch „Subst“ angezeigte Operation ausführt):

Für a eine beliebige Formel, für ν eine beliebige Variable, für b eine Formel, in der ν nicht frei vorkommt, für c ein Zeichen vom selben Typ wie ν , vorausgesetzt, daß c keine Variable enthält, welche in a an einer Stelle gebunden ist, an der ν frei ist²³.

IV. Jede Formel, die aus dem Schema

1. $(Eu)(\nu \Pi(u(\nu) \equiv a))$

dadurch entsteht, daß man für ν bzw. u beliebige Variablen vom Typ n bzw. $n + 1$ und für a eine Formel, die u nicht frei enthält, einsetzt. Dieses Axiom vertritt das Reduzibilitätsaxiom (Komprehensionsaxiom der Mengenlehre).

V. Jede Formel, die aus der folgenden durch Typenerhöhung entsteht (und diese Formel selbst):

1. $x_1 \Pi(x_2(x_1) \equiv y_2(x_1)) \supset x_2 = y_2$.

Dieses Axiom besagt, daß eine Klasse durch ihre Elemente vollständig bestimmt ist.

Eine Formel c heißt unmittelbare Folge aus a und b (bzw. aus a), wenn a die Formel $(\sim(b)) \vee (c)$ ist (bzw. wenn c die Formel $\nu \Pi(a)$ ist, wo ν eine beliebige Variable bedeutet). Die Klasse der beweisbaren Formeln wird definiert als die kleinste Klasse von Formeln, welche die Axiome enthält und gegen die Relation „unmittelbare Folge“ abgeschlossen ist²⁴.

Wir ordnen nun den Grundzeichen des Systems P in folgender Weise eineindeutig natürliche Zahlen zu:

„0“...1 „ \vee “...7 „(“...11
 „ f “...3 „ Π “...9 „)“...13
 „ \sim “...5

57: Aus p oder p folgt p

58: Aus p folgt p oder p

59: p und q sind im ODER vertauschbar

60: Wenn aus p q folgt, kann man an beide ein beliebiges r ran-ODERN und der Wahrheitswert bleibt gleich

61: Formeln dieser Art werden der ›Einfachheit‹ halber als Axiome gesetzt.

62: $\forall \nu : a \supset \text{Subst } \begin{pmatrix} \nu \\ c \end{pmatrix}$; ν Variable, c selber Typus wie ν

63: $\forall \nu : (b \vee a) \supset b \vee \forall \nu : a$

64: $\exists u : \forall \nu : u(\nu) \equiv a$

65: $\forall x_y : (x_2(x_1) \equiv y_2(x_1)) \supset x_2 = y_2$. Hier wird die Äquivalenz von zwei Mengen darüber definiert, dass all ihre Elemente gleich sind.

66: $\forall \nu : a$

67: Es geht um eine rein syntaktische Betrachtung zum Umwandeln von Formeln in natürliche Zahlen. Gödel bietet einen generalisierten Algorithmus an, um in jedem ausreichend komplexen System Sätze zu formulieren, die nicht nicht-beweisbar sind. Dazu nutzt er zur Vereinfachung die Peano-Axiome, die aber, da sie selbst Folgen der logischen Annahmen sind, an sich entbehrlich sind.

²³ c ist also entweder eine Variable oder 0 oder ein Zeichen der Form $f \dots f u$, wo u entweder 0 oder eine Variable 1. Typs ist. Bez. des Begriffs „frei (gebunden) an einer Stelle von a “, vgl. die Fußnote 24 zitierte Arbeit I A 5.

²⁴Die Einsetzungsregel wird dadurch überflüssig, daß wir alle möglichen Einsetzungen bereits in den Axiomen selbst vorgenommen haben (analog bei J. v. Neumann, Zur Hilbertschen Beweistheorie, Math. Zeitschr. 26, 1927.)

ferner den Variablen n -ten Typs die Zahlen der Form p^n (wo p eine Primzahl > 13 ist). Dadurch entspricht jeder endlichen Reihe von Grundzeichen (also auch jeder Formel) in eindeutiger Weise eine endliche Reihe natürlicher Zahlen. Die endlichen Reihen natürlicher Zahlen bilden wir nun (wieder eindeutig) auf natürliche Zahlen ab, indem wir der Reihe n_1, n_2, \dots, n_k die Zahl $2^{n_1}, 3^{n_2}, \dots, p_k^{n_k}$ entsprechen lassen, wo p_k die k -te Primzahl (der Größe nach) bedeutet. Dadurch ist nicht nur jeder endlichen Reihe von solchen in eindeutiger Weise eine natürliche Zahl zugeordnet. Die Grundzeichen (bzw. der Grundzeichenreihe) a zugeordnete Zahl bezeichnen wir mit $\Phi(a)$. Sei nun irgend eine Klasse oder Relation $R(a_1, a_2, \dots, a_n)$ zwischen Grundzeichen oder Reihen von solchen gegeben. Wir ordnen ihr diejenige Klasse (Relation) $R'(x_1, x_2, \dots, x_n)$ zwischen natürlichen Zahlen zu, welche dann und nur dann zwischen x_1, x_2, \dots, x_n besteht, wenn es solche a_1, a_2, \dots, a_n gibt, daß $x_i = \Phi(a_i)$ ($i = 1, 2, \dots, n$) und $R(a_1, a_2, \dots, a_n)$ gilt. Diejenigen Klassen und Relationen natürlicher Zahlen, welche auf dieser Weise den bisher definierten metamathematischen Begriffen, z. B. „Variable“, „Formel“, „Satzformel“, „Axiom“, „beweisbare Formel“ usw. zugeordnet sind, bezeichnen wir mit denselben Worten in Kursivschrift. Der Satz, daß es im System P unentscheidbare Probleme gibt, lautet z. B. folgendermaßen: es gibt *Satzformeln* a , so daß weder a noch die *Negation* von a *beweisbare Formeln* sind.

Wir schalten nun eine Zwischenbetrachtung ein, die mit dem formalen System P vorderhand nichts zu tun hat, und geben zunächst folgende Definition: eine zahlentheoretische Funktion²⁵ $\phi(x_1, x_2, \dots, x_n)$ heißt *rekursiv definiert* aus den zahlentheoretischen Funktionen $\psi(x_1, x_2, \dots, x_{n-1})$ und $\mu(x_1, x_2, \dots, x_{n+1})$, wenn für alle x_2, \dots, x_n , k ²⁶ folgendes gilt:

$$\begin{aligned} \phi(0, x_2 \dots x_n) &= \psi(x_2 \dots x_n) \\ \phi(k+1, x_2 \dots x_n) &= \mu(k, \phi(k, x_2 \dots x_n), x_2 \dots x_n) \end{aligned} \tag{2}$$

Eine zahlentheoretische Funktion ϕ heißt *rekursiv*, wenn es eine endliche Reihe von zahlentheor. Funktionen $\phi_1, \phi_2, \dots, \phi_n$ gibt, welche mit ϕ endet und die Eigenschaft hat, daß jede Funktion ϕ_k der Reihe entweder aus zwei vorhergehenden rekursiv definiert ist oder aus irgend welchen der vorhergehenden durch Einsetzung entsteht²⁷ oder schließlich eine Konstante oder die Nachfolgerfunktion $x+1$ ist. Die Länge der kürzesten Reihe von ϕ_i , welche zu einer rekursiven Funktion ϕ gehört, heißt ihre Stufe. Eine Relation zwischen natürlichen Zahlen $R(x_1 \dots x_n)$ heißt *rekursiv*²⁸, wenn es eine rekursive Funktion $\phi(x_1 \dots x_n)$ gibt, so daß für alle x_1, x_2, \dots, x_n

$$R(x_1 \dots x_n) \sim [\phi(x_1 \dots x_n) = 0] \tag{29}$$

Es gelten folgende Sätze:

²⁵D. h. ihr Definitionsbereich ist die Klasse der nicht negativen ganzen Zahlen (bzw. der n -tupel von solchen) und ihre Werte sind nicht negative ganze Zahlen.

²⁶Kleine lateinische Buchstaben (ev. mit Indizes) sind im folgenden immer Variable für nicht negative ganze Zahlen (falls nicht ausdrücklich das Gegenteil bemerkt ist).

²⁷Genauer: durch Einsetzung gewisser der vorhergehenden Funktionen an die Leerstellen einer der vorhergehenden, z. B. $\phi_k(x_1, x_2) = \phi_p[\phi_q(x_1, x_2), \phi_r(x_2)]$ ($p, q, r < k$). Nicht alle Variable der linken Seite müssen auch rechts vorkommen (ebenso im Rekursionsschema (2)).

²⁸Klassen rechnen wir mit zu den Relation (einstellige Relationen). Rekursive Relation R haben natürlich die Eigenschaft, daß man für jedes spezielle Zahlen- n -tupel entscheiden kann, ob $R(x_1 \dots x_n)$ gilt oder nicht.

²⁹Für alle inhaltlichen (insbes. auch die metamathematischen) Überlegungen wird die Hilbertsche Symbolik verwendet. Vgl. Hilbert-Ackermann, Grundzüge der theoretischen Logik, Berlin 1928.

68: Gödelisierung: Zahl \leftrightarrow Formel

69: „ $f(0)$ “ $= 2^1 + 3^{11} + 5^1 + 7^{13} = 96\,889\,187\,561$, $96\,889\,187\,561$ ist eindeutig zugeordnet zu „ $f(0)$ “

70: Es existiert eine Menge an Aussagen mit der Mindestkardinalität 1, so dass die Einzelaussagen nicht beweisbar sind, aber auch das Gegenteil nicht gezeigt werden kann.

71: Eine Funktion ist rekursiv, wenn sie intern dargestellt werden kann als Aufrufe anderer Funktionen („Wrapper“ in der Informatik).

72: Die minimale „Call Depth“ der Funktion ist ihre Stufe

- I. Jede aus rekursiven Funktionen (Relationen) durch Einsetzung rekursiver Funktionen an Stelle der Variablen entstehende Funktion (Relation) ist rekursiv; ebenso jede Funktion, die aus rekursiven Funktionen durch rekursive Definition nach dem Schema (2) entsteht.
- II. Wenn R und S rekursive Relationen sind, dann auch $R, R \vee S$ (daher auch $R \& S$).
- III. Wenn die Funktionen $\phi(\mathfrak{x}), \psi(\mathfrak{y})$ rekursiv sind, dann auch die Relation $\phi(\mathfrak{x}) = \psi(\mathfrak{y})$ ³⁰.
- IV. Wenn die Funktion $\phi(\mathfrak{x})$ und die Relation $R(\mathfrak{x}, \mathfrak{y})$ rekursiv sind, dann auch die Relationen S, T

$$S(\mathfrak{x}, \mathfrak{y}) \sim (Ex) [x \leq \phi(\mathfrak{x}) \& R(\mathfrak{x}, \mathfrak{y})]$$

$$T(\mathfrak{x}, \mathfrak{y}) \sim [x \leq \phi(\mathfrak{x}) \longrightarrow R(\mathfrak{x}, \mathfrak{y})]$$

sowie die Funktion ψ

$$\psi(\mathfrak{x}, \mathfrak{y}) = ex [x \leq \phi(\mathfrak{x}) \& R(\mathfrak{x}, \mathfrak{y})],$$

wobei $exF(x)$ bedeutet: Die kleinste Zahl x , für welche $F(x)$ gilt und 0, falls es keine solche Zahl gibt.

Satz I folgt unmittelbar aus der Definition von „rekursiv“. Satz II und III beruhen darauf, daß die den logischen Begriffen $\overline{}$, \vee , $=$ entsprechenden zahlentheoretischen Funktionen

$$\alpha(x), \beta(x, y), \gamma(x, y)$$

nämlich:

$$\alpha(0) = 1; \alpha(x) = 0 \text{ für } x \neq 0$$

73:

$$\sim x \equiv \alpha(x) = \begin{cases} 1, & \text{wenn } x = 0 \\ 0, & \text{sonst} \end{cases}$$

$$\beta(0, x) = \beta(x, 0) = 0; \beta(x, y) = 1, \text{ wenn } x, y \text{ beide } \neq 0 \text{ sind}$$

74:

$$x \wedge b \equiv \beta(x, y) = \begin{cases} 1, & \text{wenn } x \wedge y \\ 0, & \text{sonst} \end{cases}$$

$$\gamma(x, y) = 0, \text{ wenn } x = y; \gamma(x, y) = 1, \text{ wenn } x \neq y$$

75:

$$\sim (x = y) \equiv \gamma(x, y) = \begin{cases} 0, & \text{wenn } x = y \\ 1, & \text{sonst} \end{cases}$$

rekursiv sind, wie man sich leicht überzeugen kann. Der Beweis für Satz IV ist kurz der folgende: Nach der Voraussetzung gibt es ein rekursives $\rho(\mathfrak{x}, \mathfrak{y})$, so daß:

$$R(\mathfrak{x}, \mathfrak{y}) \sim [\rho(\mathfrak{x}, \mathfrak{y}) = 0].$$

Wir definieren nun nach dem Rekursionsschema (2) eine Funktion $\chi(\mathfrak{x}, \mathfrak{y})$ folgendermaßen:

$$\chi(0, \mathfrak{y}) = 0$$

76: Zweistufig-rekursive Funktionsdefinition

$$\chi(n+1, \mathfrak{y}) = (n+1).a + \chi(n, \mathfrak{y}).\alpha(a)$$
³¹

77: Gleichbedeutend mit $\chi(n, \mathfrak{y}) = n \times \chi((n-1), \mathfrak{y}) \times \alpha(a)$, für a siehe Kommentar 73

³⁰ Wir verwenden deutsche Buchstaben $\mathfrak{x}, \mathfrak{y}$ als abkürzende Bezeichnung für beliebige Variablen- n -tupel, z.B. $x_1 x_2 \dots x_n$

³¹ Wir setzen als bekannt voraus, daß die Funktionen $x + y$ (Addition), $x \cdot y$ (Multiplikation) rekursiv sind.

wobei $a = \alpha \left[\alpha \left(\rho \left(0, \eta \right) \right) \right] . \alpha \left[\rho \left(n + 1, \eta \right) \right] . \alpha \left[\chi \left(n, \eta \right) \right]$.
 $\chi \left(n + 1, \eta \right)$ ist daher entweder $= n + 1$ (wenn $a = 1$) oder $= \chi \left(n, \eta \right)$ (wenn $a = 0$)³².
Der erste Fall tritt offenbar dann und nur dann ein, wenn sämtliche Faktoren von a 1 sind, d. h. wenn gilt:

$$\overline{R} \left(0, \eta \right) \& R \left(n + 1, \eta \right) \& \left[\chi \left(n, \eta \right) = 0 \right]$$

Daraus folgt, daß die Funktion $\chi \left(n, \eta \right)$ (als Funktion von n betrachtet) 0 bleibt bis zum kleinsten Wert von n , für den $R \left(n, \eta \right)$ gilt, und von da ab gleich diesem Wert ist (falls schon $R \left(0, \eta \right)$ gilt, ist dementsprechend $\chi \left(n, \eta \right)$ konstant und $= 0$).
Demnach gilt:

$$\psi \left(\mathfrak{x}, \eta \right) = \chi \left(\phi \left(\mathfrak{x} \right), \eta \right)$$

$$S \left(\mathfrak{x}, \eta \right) \sim R \left[\psi \left(\mathfrak{x}, \eta \right), \eta \right]$$

Die Relation T läßt sich durch Negation auf einen zu S analogen Fall zurückführen, womit Satz IV bewiesen ist.
Die Funktionen $x + y, x.y, x^y$, ferner die Relationen $x < y, x = y$ sind, wie man sich leicht überzeugt, rekursiv und wir definieren nun, von diesen Begriffen ausgehend, eine Reihe von Funktionen (Relationen) 1–45, deren jede au den vorhergehenden mittels der in den Sätzen I bis IV genannten erfahren definiert ist. Dabei sind meistens mehrere der nach Satz I bis IV erlaubten Definitionsschritte in einem zusammengefaßt. Jede der Funktionen (Relationen) 1–45, unter denen z. B. die Begriffe „*Formel*“, „*Axiom*“, „*unmittelbare Folge*“ vorkommen, ist daher rekursiv.

1. $x/y \equiv (Ez) \left[z \leq x \& x = y.z \right]$ ³³
 x ist teilbar durch y ³⁴
2. Prim $(x) \equiv \overline{(Ez)} \left[z \leq x \& z \nmid 1 \& z \neq x \& x/z \right] \& x > 1$
 x ist eine Primzahl.
3. $0Pr\ x \equiv 0$
 $(n + 1)Pr\ x \equiv \epsilon y \left[y \leq x \& \text{Prim} \left(y \right) \& x/y \& y > nPr\ x \right]$
 $nPr\ x$ ist die n -te (der Größe nach) in x enthaltene Primzahl^{34a}.
4. $0! \equiv 1$
 $(n + 1)! \equiv (n + 1) . n!$
5. $Pr\ (0) \equiv 0$
 $Pr\ (n + 1) \equiv \epsilon y \left[y \leq \{Pr\ (n)\}! + 1 \& \text{Prim} \left(y \right) \& y > Pr\ (n) \right]$
 $Pr\ (n)$ ist die n -te Primzahl (der Größe nach).

³²Andere Werte als 0 und 1 kann a , wie aus der Definition für α ersichtlich ist, nicht annehmen.
³³Das Zeichen \equiv wird im Sinne von „Definitionsgleichheit“ verwendet, vertritt also bei Definitionen entweder $=$ oder \sim (im übrigen ist die Symbol die H i l b e r tsche).
³⁴Überall, wo in den folgenden Definitionen eines der Zeichen $(x), (Ex), \epsilon x$ auftritt, ist es von einer Abschätzung für x gefolgt. Diese Abschätzung dient lediglich dazu, um die rekursive Natur des definierten Begriffes (vgl. Satz IV) zu sichern. Dagegen würde sich der Umgang der definierten Begriffe durch Weglassung dieser Abschätzung meistens nicht ändern.
^{34a}Für $0 < n \leq z$, wenn z die Anzahl der verschiedenen in x aufgehenden Primzahlen ist. Man beachte, daß für $n = z + 1 \quad nPr\ x = 0$ ist!

78: Es folgt die Liste der Axiome und Definitionen aus diesen Axiomen zum Herleiten der Unvollständigkeitssätze (§§ 1 (x/y) – 46 (Bew)).

$$79: x/y \equiv \exists z \left(z \leq x \wedge x = y \times z \right)$$

$$80: \text{Prim} \left(x \right) \equiv \sim \exists z : \left(z \leq x \wedge z \neq 1 \wedge z \neq x \wedge x/z \right) \wedge x > 1$$

81: In der 0 sind keine Primfaktoren

82: $nPr\ x \equiv \exists y : y \leq x \wedge \text{Prim} \ x \wedge x/y \wedge y > (n - 1)Pr\ x$. Beschreibt den n ten Primfaktor von x , vgl. 1 (x/y), 2 (Prim), 3 (0 Pr x)

83: Fakultät, zweistufig-rekursive Funktionsdefinition

84: Gleich mit $(n)! \equiv (n - 1) \times n!$

85: $Pr\ (n) \equiv \exists y : y \leq (Pr\ (n))! + 1 \wedge \text{Prim} \left(y \right) \wedge y > Pr\ (n)$, vgl. §§ 2 (Prim), 4 (Fakultät), 5 (Pr)

6. $nGl\ x \equiv \epsilon y \left[y \leq x \& x / (nPr\ x)^y \& \overline{x / nPr\ x}^{y+1} \right]$
 $nGl\ x$ ist das n -te Glied der der Zahl x zugeordneten Zahlenreihe (für $n > 0$ und n nicht größer als die Länge dieser Reihe).

7. $l(x) \equiv \epsilon y \left[y \leq x \& yPr\ x > 0 \& (y+1)Pr\ x = 0 \right]$
 $l(x)$ ist die Länge der x zugeordneten Zahlenreihe.

8. $x*y \equiv \left\{ z \leq \left[Pr(l(x) + l(y)) \right]^{x+1} \& (n) \left[n \leq l(x) \longrightarrow nGl\ z = nGl\ x \right] \& (n) \left[0 < n \leq l(y) \longrightarrow (n + l(x))Gl\ z = nGl\ y \right] \right\}$
 $x*y$ entspricht der Operation des „Aneinanderfügens“ zweier endlicher Zahlenreihen.

9. $R(x) \equiv 2^x$
 $R(x)$ entspricht der nur aus der Zahl x bestehenden Zahlenreihe (für $x > 0$).

10. $E(x) \equiv R(11)*x*R(13)$
 $E(x)$ entspricht der Operation des „Einklammerns“ [11 und 13 sind den Grundzeichen „(“ und „)“ zugeordnet].

11. $n\ Var\ x \equiv (Ez) \left[13 < z \leq x \& Prim(z) \& x = z^n \right] \& n \neq 0$
 x ist eine *Variable n-ten Typs*.

12. $Var(x) \equiv (En) \left[n \leq x \& n\ Var\ x \right]$
 x ist eine *Variable*.

13. $Neg(x) \equiv R(5)*E(x)$
 $Neg(x)$ ist die *Negation* von x .

14. $x\ Dis\ y \equiv E(x)*R(7)*E(y)$
 $x\ Dis\ y$ ist die *Disjunktion* aus x und y .

15. $x\ Gen\ y \equiv R(x)*R(9)*E(y)$
 $x\ Gen\ y$ ist die *Generalisation* von y mittels der Variablen x (vorausgesetzt, daß x eine *Variable* ist).

16. $0Nx \equiv x$
 $(n+1)Nx \equiv R(3)nNx$
 nNx entspricht der Operation „ n -maliges Vorsetzen des Zeichens ‚ f ‘ vor x “.

17. $Z(n) \equiv nN[R(1)]$ $Z(n)$ ist das *Zahlzeichen* für die Zahl n .

18.

$$Typ'_1(x) \equiv (Em, n) \left\{ m, n \leq x \& \left[m = 1 \vee 1\ Var\ m \right] \& x = nN[R(m)] \right\}^{34b}$$

 x ist *Zeichen ersten Typs*.

19.

$$Typ_n(x) \equiv \left[n = 1 \& Typ'_1(x) \right] \vee \left[n > 1 \& (Ev) \left\{ v \leq x \& n\ Var\ v \& x = R(v) \right\} \right]$$

 x ist *Zeichen n-ten Typs*.

^{34b} $m, n \leq x$ steht für: $m \leq x \& n \leq x$ (ebenso für mehr als 2 Variable).

86: $nGl\ x \equiv \exists y: y \leq x \wedge x / (nPr\ x)^y \wedge \sim \left((x / nPr\ x)^{x+1} \right)$, vgl. §§ 1 (x/y), 3 (0 Pr x)

87: $l(x) \equiv \exists y: y \leq x \wedge yPr\ x > 0 \wedge (y+1)Pr\ x = 0$

88: Konkatinieren von Zahlen

89: Für alle $n \in \mathbb{N}$ erzeugt das eine eindeutige Zahl, die immer wieder ›zurückkonvertiert‹ werden kann zu ihrer Ursprungszahl. Diese Methode ist ein Spezialfall der generalisierten Methode $p(n)^x$, wobei $p(n)$ die Position im Zeichenstring kodiert (n) und $p(x)$ die x te Primzahl zurückgibt. Multiplikativ zusammengefügt ist eine eindeutige Zerlegung von Strings in eine Zahlenkette möglich.

90: $E(x) \equiv$ „(“. x . „)“, vgl. § 8 (Konkat)

91: $n\ Var\ x \equiv \exists z: \left[\text{„} \right] < z \leq x \wedge Prim(z) \wedge x = z^n \right] n \neq 0$, die 13 ist die Gödelnummer für „)“, vgl. § 2 (Prim)

92: $Var(x) \equiv \exists n: \left(n \leq x \wedge (n\ Var\ x) \right)$, vgl. § 11 (n Var x)

93: $Neg(x) \equiv \sim x$, vgl. 8 (Konkat).

94: $x\ Dis\ y \equiv x$. „ \vee “. y , vgl. § 8 (Konkat)

95: $x\ Gen\ y \equiv x$. „ Π “. y , oder in modern: $x\ Gen\ y \equiv \forall x: y$, vgl. § 8 (Konkat)

96: Zweistufig-rekursive Funktion zum Vorsetzen des Zeichens „ f “

97: $(n)Nx \equiv$ „ f “. $(n-1)Nx$, die 3 ist das „ f “, vgl. § 8 (Konkat)

98: Konvertiert „normale“ Zahlen zu einem Zahlzeichen. So wird die „5“ zu $ffff1$.

99: $Typ_1(x) \equiv \exists m \exists n: n \leq x \wedge m \leq x \wedge (m = 1 \vee 1\ Var\ m) \wedge x = nN[R(m)]$

100: Siehe § 18 (Typ1') für Spezialfall $n = 1$

20.

$$Elf(x) \equiv (Ey, z, n) [y, z, n \leq x \& Typ_n(y) \& Typ_{n+1}(z) \& x = z * E(y)]$$

101: $Elf(x) \equiv \exists y : \exists z : \exists n : y, z, n \leq x \wedge Typ_n(y) \wedge Typ_{n+1}(z) \wedge x = z * E(y)$, vgl. §§ 8 (Konkat), 19 (Typ), 10 (E(x)).

x ist *Elementarformel*.

102: Vgl. Kommentar 51

21. $Op(x \ y \ z) \equiv x = Neg(y) \vee x = y \ Dis \ z \vee (Ev) [v \leq x \& Var(x) \& x = v \ Gen \ y]$

22.

$$FR(x) \equiv (n) \{ 0 < n \leq l(x) \longrightarrow Elf(nGl \ x) \vee (Ep, q) [0 < p, q < n \& Op(nGl \ x, pGl \ x, qGl \ x)] \} \& l(x) > 0$$

x ist eine Reihe von *Formeln*, deren jede entweder *Elementarformel* ist oder aus vorhergehenden durch die Operationen der *Negation*, *Disjunktion*, *Generalisation* hervorgeht.

23.

$$Form(x) \equiv (En) \left\{ n \leq (Pr [l(x)^2])^{x \cdot [l(x)]^2} \& FR(n) \& x = [l(n)] \ Gl n \right\}^{35}$$

x ist *Formel* (d. h. letztes Glied einer *Formelreihe* n).

24.

$$v \text{ Geb } n, x \equiv Var(v) \& Form(x) \& (Ea, b, c) [a, b, c \leq x \& xa = *(v \ Gen \ b) * c \& Form(b) \& l(a) + 1 \leq n \leq l(a) + l(v \ Gen \ b)]$$

Die *Variable* v ist in x an n -ter Stelle *gebunden*.

25. $vFr \ n, x \equiv Var(v) \& Form(x) \& v = nGl \ x \& n \leq l(x) \& v \text{ Geb } n, x$

Die *Variable* v ist in x an n -ter Stelle *frei*.

26. $vFr \ x \equiv (En) [n \leq l(x) \& vFr \ n, x]$

v kommt in x als *freie Variable* vor.

103: $vFr \ x \equiv \exists n : n \leq l(x) \wedge vFr \ n, x$, vgl. §§ 7 (l(x)), 25 (v Fr n, x). Macht aus dem Satz 25 (v Fr n, x), der herausfindet, ob v in x an n ter Stelle frei ist die generalisierte Aussage: die Variable v befindet sich überhaupt in x oder nicht.

27.

$$Su \ x \binom{n}{y} \equiv \epsilon z \{ z \leq [Pr(l(x) + l(y))]^{x+y} \& (Eu, v) u, v \leq x \& x = u * R(nGl \ x) \ v \& z = u * y * v \& n = l(u) + 1 \}$$

$Su \ x \binom{n}{y}$ entsteht aus x , wenn man an Stelle des n -ten Gliedes von $x \ y$ einsetzt (vorausgesetzt, daß $0 < n \leq l(x)$).

³⁵Die Abschätzung $n \leq (Pr [l(x)^2])^{x l(x)^2}$ erkennt man so: Die Länge der kürzesten zu x gehörigen Formelreihe kann höchstens gleich der Anzahl der Teilformeln von x sein. Es gibt aber höchstens $l(x)$ Teilformeln der Länge 1, höchstens $l(x) - 1$ der Länge 2 usw., im Ganzen als höchstens $\frac{l(x)[l(x)+1]}{2} \leq l(x)^2$. Die Primzahlen aus n können also sämtlich kleiner als $Pr \{[l(x)]^x\}$ angenommen werden, ihre Anzahl $\leq l(x)^2$ und ihre Exponenten (welche Teilformeln von x sind) $\leq x$.

28.

$$0St\ v, x \equiv \{n \leq l(x) \& vFr\ n, x \\ \& \overline{(Ep)} [n < p \leq l(x) \& vFr\ px]\}$$

$$(k+1)St\ v, x \equiv \epsilon n \{n < kSt\ v, x \& vFr\ n, x \\ \& \overline{(Ep)} [n < p < kSt\ v, x \& vFr\ p, x]\}$$

$kSt\ v, x$ ist die $k+1$ -te Stelle in x (vom Ende der *Formel* x an gezählt), an der v in x *frei* ist (und 0, falls es keine solche Stelle gibt).

$$29. A(v, x) \equiv \epsilon n \{n \leq l(x) \& nSt\ v, x = 0\}$$

$A(v, x)$ ist die Anzahl der Stellen, an denen v in x *frei* ist.

$$30. Sb_0(x_y^v) \equiv \alpha$$

$$Sb_{k+1}(x_y^v) \equiv Su [Sb_k(x_y^v)] ({}^k St_{\ y} v, x)$$

$$31. Sb(x_y^v) \equiv Sb_{A(v, x)}(x_y^v)^{36}$$

$Sb(x_y^v)$ ist der oben definierte Begriff *Subst* $a({}_b^v)^{37}$.

$$32. x \text{ Imp } y \equiv [\text{Neg } (x)] \text{ Dis } y$$

$$x \text{ Con } y \equiv \text{Neg } \{[\text{Neg } (x)] \text{ Dis } [\text{Neg } (y)]\}$$

$$x \text{ Aeq } y \equiv (x \text{ Imp } y) \text{ Con } (y \text{ Imp } x)$$

$$\nu \text{ Ex } y \equiv \text{Neg } \{\nu \text{ Gen } [\text{Neg } (y)]\}$$

33.

$$nTh\ x \equiv \epsilon y \left\{ y \leq x^{(x^n)} \& (k) [k \leq l(x) \longrightarrow \right. \\ \left. (kGl\ x \leq 13 \& kGl\ y = kGl\ x) \vee \right. \\ \left. (kGl\ x > 13 \& kGl\ y = kGl\ x. [1Pr\ (kGl\ x)^n]) \right\}$$

$nTh\ x$ ist die n -te *Typenerhöhung* von x (falls x und $nTh\ x$ *Formeln* sind).

Den Axiomen I, 1 bis 3 entsprechen drei bestimmte Zahlen, die wir mit z_1, z_2, z_3 bezeichnen un wir definieren:

$$34. Z - Ax(x) \equiv (x = z_1 \vee x = z_2 \vee x = z_3)$$

$$35. A_1 - Ax(x) \equiv (Ey) [y \leq x \& \text{Form } (y) \& x = (y \text{ Dis } y) \text{ Imp } y]$$

x ist eine durch Einsetzung in das Axiomenschema II, 1 entstehende *Formel*. Analog werden $A_2 - Ax, A_3 - Ax, A_4 - Ax$ entsprechend den Axiomen II, 2 bis 4 definiert.

$$36. A - Ax(x) \equiv A_1 - Ax(x) \vee A_2 - Ax(x) \vee A_3 - Ax(x) \vee A_4 - Ax(x)$$

x ist eine durch Einsetzung in ein Aussagenaxiom entstehende *Formel*.

37.

$$Q(z, y, v) \equiv \overline{(En, m, w)} [n \leq l(y) \& m \leq l(z) \& w \leq z \& \\ w = mGlz \& w \text{ Geb } n, y \& vFr\ n, y]$$

z enthält keine Variable, die in y an einer Stelle *gebunden* ist, an der v *frei* ist.

³⁶Falls v keine *Variable* oder x keine *Formel* ist, ist $Sb(x_y^v) = x$.

³⁷Statt $Sb[Sb(x_y^v) {}^w_z]$ schreiben wir: $Sb({}_y^v {}^w_z)$ (analog für mehr als zwei Variable).

$$104: A(v, x) \equiv \exists n : n \leq l(x) \wedge nSt\ v, x = 0, \text{ vgl. } 29\ (n\ St\ v, x),\ 7\ (l(x))$$

$$105: \text{Rekursive Funktion zum Ersetzen von Variablen, letzter Rekursionsschritt ist immer die 0 (daher spezial definiert)}$$

$$106: \text{Expandiert die Variablen bis in die unterste Formelebene zu ihrem Ersatz}$$

$$107: x \text{ Imp } y \equiv (\sim x) \vee y. \text{ Bedeutet: } x \supset y$$

$$108: x \text{ Con } y \equiv (x \supset y) \vee \sim y. \text{ Bedeutet } x \vee y$$

$$109: x \text{ Aeq } y \equiv (x \supset y) \wedge (y \supset x). \text{ Bedeutet: } x \text{ iff } y$$

$$110: \nu \text{ Ex } y \equiv \sim (\forall \nu : \neg y). \text{ Bedeutet „alle } y \text{ in } \nu \text{ sind wahr“, vgl. §§ } 13\ (\text{Neg}),\ 15\ (\text{Gen})$$

$$111: A_1 - Ax(x) \equiv \exists y : y \leq x \wedge \text{Form } (y) \wedge x = (y \vee y) \supset y, \text{ vgl. \$ } 14\ (\text{Dis}),\ 23\ (\text{Form}),\ 23\ (\text{Form}),\ 14\ (\text{Dis}),\ 32a\ (\text{Imp}),\ 34\ (\text{Z} - \text{Ax}(x))$$

38.

$$L_1 - Ax(x) \equiv (Ev, y, z, n) \{v, y, z, n \leq x \& n \text{ Var } v \& \\ \text{Typ}_n(z) \& \text{Form}(y) \& Q(z, y, v) \& \\ x = (v \text{ Gen } y) \text{ Imp } [Sb(y_z^v)]\}$$

x ist eine aus dem Axiomenschema III, 1 durch Einsetzung entstehende *Formel*.

39.

$$L_2 - Ax(x) \equiv (Ev, q, p) \{v, q, p \leq x \& \text{Var}(v) \\ \& \text{Form}(p) \& vFr\ p \& \text{Form}(x) \& \\ x = [v \text{ Gen } (p \text{ Dis } q)]\}$$

x ist eine aus dem Axiomenschema III, 2 durch Einsetzung entstehende *Formel*.

40.

$$R - Ax(x) \equiv (Eu, v, y, n) [u, v, y, n \leq x \& n \text{ Var } v \& \\ (n+1) \text{ Var } u \& uFr\ y \& \text{Form}(y) \& \\ x = u \text{ Ex } \{v \text{ Gen } [R(u) * E(R(v))] \text{ Aeq } y]\}$$

x ist eine aus dem Axiomenschema IV, 1 durch Einsetzung entstehende *Formel*.

Dem Axiom V, 1 entspricht eine bestimmte Zahl z_4 und wir definieren:

$$41. \quad M - Ax(x) \equiv (En) [n \leq x \& x = nTh\ z_4]$$

$$112: M - Ax(x) \equiv \exists n : n \leq x \wedge x = nTh\ z_4, \text{ vgl. § 33 (Th)}$$

$$42. \quad Ax(x) \equiv Z - Ax(x) \vee A - Ax(x) \vee L_1 - Ax(x) \vee L_2 - Ax(x) \vee R - Ax(x) \vee M - Ax(x)$$

x ist ein *Axiom*.

$$43. \quad Fl(x\ y\ z) \equiv y = z \text{ Imp } x \vee (Ev) [v \leq x \& \text{Var}(v) \& x = v \text{ Gen } y]$$

x ist *unmittelbare Folge* aus y und z .

44.

$$Bw(x) \equiv (n) \{0 < n \leq l(x) \longrightarrow Ax(nGl\ x) \vee \\ (Ep, q) [0, < p, q < n \& Fl(nGl\ x, pGl\ x, qGl\ x)]\} \\ \& l(x) > 0$$

x ist eine *Beweisfigur* (eine endliche Folge von *Formeln*, deren jede entweder *Axiom* oder *unmittelbare Folge* aus der vorhergehenden ist).

$$45. \quad xB\ y \equiv Bw(x) \& [l(x)] Gl\ x = y$$

x ist ein *Beweis* für die *Formel* y .

$$113: x \text{ ist Beweis für } y \equiv (x \text{ ist Beweisfigur} \wedge (\text{die Länge von } x \text{ das } n\text{-te Glied der Zahl } x) = y), \text{ vgl. §§ 7 (l(x)), 6 (n Gl x), 44 (Bw)}$$

$$46. \quad \text{Bew}(x) \equiv (Ey) yBx$$

x ist eine *beweisbare Formel*. [Bew(x) ist der einzige unter den Begriffen 1–46, von dem nicht behauptet werden kann, er sei rekursiv.]

$$114: \text{Bew} \equiv \exists y : yBx, \text{ es existiert ein Beweis } y \text{ für } x, \text{ vgl. § 45 (x B y)}$$

Die Tatsache, die man vage so formulieren kann: Jede rekursive Relation ist innerhalb des Systems P (dieses inhaltlich gedeutet) definierbar, wird, ohne auf eine inhaltliche Deutung der Formeln aus P Bezug zu nehmen, durch folgenden Satz exakt ausgedrückt:

115: Die inhaltliche Deutung ist keine, die aus dem Formalismus entspringen kann. Erst in der inhaltlichen Deutung z. B. wird die Wahrheit der Aussage des Satzes n , dass n nicht beweisbar ist, als wahr erkannt; aus dem Formalismus allein heraus geht das nicht.

Satz V: Zu jeder rekursiven Relation $R(x_1 \dots x_n)$ gibt es ein n -stelliges *Relationszeichen* r (mit den *freien Variablen*³⁸ $u_1, u_2 \dots u_n$), so, dass für alle Zahlen- n -tupel $x_1 \dots x_n$ gilt:

$$R(x_1 \dots x_n) \longrightarrow \text{Bew} \left[Sb \left(r_{Z(x_1) \dots Z(x_n)}^{u_1 \dots u_n} \right) \right] \quad (3)$$

$$\overline{R}(x_1 \dots x_n) \longrightarrow \text{Bew} \left[\text{Neg } Sb \left(r_{Z(x_1) \dots Z(x_n)}^{u_1 \dots u_n} \right) \right] \quad (4)$$

Wir begnügen uns hier damit, den Beweis dieses Satzes, da er keine prinzipiellen Schwierigkeiten bietet und ziemlich umständlich ist, in Umrissen anzudeuten³⁹. Wir beweisen den Satz für alle Relationen $R(x_1 \dots x_n)$ der Form: $x_1 = \phi(x_2 \dots x_n)$ ⁴⁰ (wo ϕ eine rekursive Funktion ist) und wenden vollständige Induktion nach der Stufe von ϕ an. Für die Funktionen erste Stufe (d. h. Konstante und die Funktion $x + 1$) ist der Satz trivial. Habe also ϕ die m -te Stufe. Es entsteht aus Funktionen niedrigerer Stufe $\phi_1 \dots \phi_k$ durch die Operationen der Einsetzung oder der rekursiven Definition. Da für $\phi_1 \dots \phi_k$ nach induktiver Annahme bereits alles bewiesen ist, gibt es zugehörige *Relationszeichen* $r_1 \dots r_k$, so daß (3), (4) gilt. Die Definitionsprozesse, durch die ϕ aus $\phi_1 \dots \phi_k$ entsteht (Einsetzung und rekursive Definition), können sämtlich im System P formal nachgebildet werden. Tut man dies, so erhält man aus $r_1 \dots r_k$ ein neues *Relationszeichen* r ⁴¹, für welches man die Geltung von (3), (4) unter der Verwendung der induktiven Annahmen ohne Schwierigkeit beweisen kann. Ein *Relationszeichen* r , welches auf diesem Wege einer rekursiven Relation zugeordnet ist⁴², soll rekursiv heißen.

Wir kommen nun ans Ziel unserer Ausführungen. Sei χ eine beliebige Klasse von *Formeln*. Wir bezeichnen mit $\text{Flg}(\chi)$ (Folgerungsmenge von χ) die kleinste Menge von *Formeln*, die alle *Formeln* aus χ und alle *Axiome* enthält und gegen die Relation „*unmittelbare Folge*“ abgeschlossen ist. χ heißt ω -widerspruchsfrei, wenn es kein *Klassenzeichen* a gibt, so daß:

$$(n) \left[Sb \left(a_{Z(n)}^v \right) \in \text{Flg}(\chi) \right] \& \left[\text{Neg} (v \text{ Gen } a) \right] \in \text{Flg}(\chi)$$

wobei v die *freie Variable* des *Klassenzeichens* a ist.

Jedes ω -widerspruchsfreie System ist selbstverständlich auch widerspruchsfrei. Es gilt aber, wie später gezeigt werden wird, nicht das Umgekehrte.

Das allgemeine Resultat über die Existenz unentscheidbarer Sätze lautet:

Satz VI: Zu jeder ω -widerspruchsfreien rekursiven Klasse χ von *Formeln* gibt es rekursive *Klassenzeichen* r , so daß weder $v \text{ Gen } r$ noch $\text{Neg} (v \text{ Gen } r)$ zu $\text{Flg}(\chi)$ gehört (wobei v die *freie Variable* aus r ist).

Beweis: Sei χ eine beliebige rekursive ω -widerspruchsfreie Klasse von *Formeln*. Wir definieren:

$$Bw_x(x) \equiv (n) \left[n \leq l(x) \longrightarrow Ax(nGl\ x) \vee (nGl\ x) \in \chi \vee \right] \quad (5)$$

³⁸Die *Variablen* $u_1 \dots u_n$ können willkürlich vorgegeben werden. Es gibt z. B. immer ein r mit den *freien Variablen* 17, 19, 23 ... usw., für welches (3) und (4) gilt.

³⁹Satz V beruht natürlich darauf, daß bei einer rekursiven Relation R für jedes n -tupel von Zahlen aus den *Axiomen* des Systems P entscheidbar ist, ob dieses Relation R besteht oder nicht.

⁴⁰Daraus folgt sofort seine Geltung für jede rekursive Relation, da eine solche Gleichbedeutung ist mit $0 = \phi(x_1 \dots x_n)$, wo ϕ rekursiv ist.

⁴¹Bei der genauen Durchführung dieses Beweises wird natürlich r nicht auf dem Umweg über die inhaltliche Deutung, sondern durch seine rein formale Beschaffenheit definiert.

⁴²Welches also, inhaltlich gedeutet, das Bestehen dieser Relation ausdrückt.

116: Widerspruchsfreiheit von nicht ω -widerspruchsfreien Systemen heißt, dass allein die Axiome widerspruchsfrei sind.

$$(Ep, q) \{0 < p, q < n \& Fl(nGl\ x, pGl\ x, qGl\ x)\} \& l(x) > 0$$

(vgl. den analogen Begriff 44)

$$xB_x y \equiv B w_x(x) \& [l(x)] Gl\ x = y \quad (6)$$

$$\text{Bew}_x(x) \equiv (Ey) y B_x x \quad (6.1)$$

(vgl. die analogen Begriffe 45, 46).

Es gilt offenbar:

$$(x) [\text{Bew}_x(x) \sim x \epsilon \text{Flg}(\chi)] \quad (7)$$

$$(x) [\text{Bew}(x) \longrightarrow \text{Bew}_x(x)] \quad (8)$$

Nun definieren wir die Relation:

$$Q(x, y) \equiv \overline{xB_\chi \left[Sb \left(y_{Z(y)}^{19} \right) \right]}. \quad (8.1)$$

Da $xB_x y$ [nach (6), (5)] und $Sb \left(y_{Z(y)}^{19} \right)$ (nach Def. 17, 31) rekursiv sind, so auch $Q(xy)$. Nach Satz V und (8) gibt es also ein *Relationszeichen* q (mit den *freien Variablen* 17, 19), so daß gilt:

117: 17 entspricht x_1 , 19 entspricht y_1 .

$$\overline{xB_\chi \left[Sb \left(y_{Z(y)}^{19} \right) \right]} \longrightarrow \text{Bew}_\chi \left[Sb \left(q_{Z(x)Z(y)}^{17\ 19} \right) \right] \quad (9)$$

$$xB_\chi \left[Sb \left(y_{Z(y)}^{19} \right) \right] \longrightarrow \text{Bew}_\chi \left[\text{Neg } Sb \left(q_{Z(x)Z(y)}^{17\ 19} \right) \right] \quad (10)$$

Wir setzen:

$$p = 17 \text{ Gen } q \quad (11)$$

118: 17 ist die erste *freie Variable* (x_1)

(p ist ein *Klassenzeichen* mit der *freien Variablen* 19) und

$$r = Sb \left(q_{Z(p)}^{19} \right) \quad (12)$$

(r ist ein rekursives *Klassenzeichen* mit der *freien Variablen* 17⁴³). Dann gilt:

$$Sb \left(p_{Z(p)}^{19} \right) = Sb \left([17 \text{ Gen } q]_{Z(p)}^{19} \right) = 17 \text{ Gen } Sb \left(q_{Z(p)}^{19} \right) = 17 \text{ Gen } r^{44} \quad (13)$$

[wegen (11) und (12)] ferner:

$$Sb \left(q_{Z(x)Z(p)}^{17\ 19} \right) = Sb \left(r_{Z(x)}^{17} \right) \quad (14)$$

[nach (12)]. Setzt man nun in (9) und (10) p für y ein, so entsteht unter Berücksichtigung von (13) und (14):

$$\overline{xB_\chi (17 \text{ Gen } r)} \longrightarrow \text{Bew}_\chi \left[Sb \left(r_{Z(x)}^{17} \right) \right] \quad (15)$$

⁴³ r entsteht ja aus dem rekursiven *Relationszeichen* q durch Ersetzen einer *Variablen* durch eine Bestimmte Zahl (p).

⁴⁴Die Operationen Gen, Sb sind natürlich immer vertauschbar, falls sie sich auf verschiedene *Variablen* beziehen.

$$xB_\chi(17 \text{ Gen } r) \longrightarrow \text{Bew}_\chi[\text{Neg } Sb(r_{Z(x)}^{17})] \quad (16)$$

Daraus ergibt sich:

1. 17 Gen r ist nicht χ -beweisbar⁴⁵. Denn wäre dies der Fall, so gäbe es (nach 6.1) ein n , so daß $nB_\chi(17 \text{ Gen } r)$. Nach 17 gälte also: $\text{Bew}_\chi[\text{Neg } Sb(r_{Z(n)}^{17})]$, während andererseits aus der χ -Beweisbarkeit von 17 Gen r auch die von $Sb(r_{Z(n)}^{17})$ folgt. χ wäre also widerspruchsvoll (umso mehr ω -widerspruchsvoll).
2. Neg (17 Gen r) ist nicht χ -beweisbar. Beweis: wie eben bewiesen wurde, ist 17 Gen r nicht χ -beweisbar, d. h. (nach 6.1) es gilt $(n) \overline{nB_\chi(17 \text{ Gen } r)}$. Daraus folgt nach (15) $(n) \text{Bew}_\chi[Sb(r_{Z(n)}^{17})]$, was zusammen mit $\text{Bew}_\chi[\text{Neg } (17 \text{ Gen } r)]$ gegen die ω -Widerspruchsfreiheit von χ verstoßen würde.

17 Gen r ist also aus χ unentscheidbar, womit Satz IV bewiesen ist.

Man kann sich leicht überzeugen, daß der eben geführte Beweis konstruktiv ist^{45a}, d. h. es ist intuitionistisch einwandfrei folgendes bewiesen: Sei eine beliebige rekursiv definierte Klasse χ von *Formeln* vorgelegt. Wenn dann eine formale Entscheidung (aus χ) für die (effektiv aufweisbare) *Satzformel* 17 Gen r vorgelegt ist, so kann man effektive angeben:

1. Einen *Beweis* für Neg (17 Gen r).
2. Für jedes beliebige n einen Beweis für $Sb(r_{Z(n)}^{17})$, d. h. eine formale Entscheidung von 17 Gen r würde die effektive Aufweisbarkeit eines ω -Widerspruches zur Folge haben.

Wir wollen eine Relation (Klasse) zwischen natürlichen Zahlen $R(x_1 \dots x_n)$ entscheidungsdefinit nennen, wenn es ein n -stelliges *Relationszeichen* r gibt, so daß (3) und (4) (vgl. Satz V) gilt. Insbesondere ist also nach Satz V jede rekursive Relation entscheidungsdefinit. Analog soll ein *Relationszeichen* entscheidungsdefinit heißen, wenn es auf diese Weise einer entscheidungsdefiniten Relation zugeordnet ist. Es genügt nun für die Existenz unentscheidbarer Sätze, von der Klasse χ vorauszusetzen, daß sie ω -widerspruchsfrei und entscheidungsdefinit ist. Denn die Entscheidungsdefinitheit überträgt sich von χ auf $xB_\chi y$ (vgl. (5), (6)) und auf $Q(x, y)$ (vgl. (8.1)) und nur dies wurde im obigen Beweise verwendet. Der unentscheidbare Satz hat in diesem Fall die Gestalt $\nu \text{ Gen } r$, wo r ein entscheidungsdefinites *Klassenzeichen* ist (es genügt übrigens sogar, daß χ in dem durch χ erweiterten System entscheidungsdefinit ist).

Setzt man von χ statt ω -Widerspruchsfreiheit, bloß Widerspruchsfreiheit voraus, so folgt zwar nicht die Existenz eines unentscheidbaren Satzes, wohl aber die Existenz einer Eigenschaft (r) , für die weder ein Gegenbeispiel *a n g e b b a r*, noch beweisbar ist, daß sie allen Zahlen zukommt. Denn zum Beweise, dass 17 Gen r nicht χ -beweisbar ist, wurde nur die Widerspruchsfreiheit von χ verwendet (Vgl.

119: 17 Gen $r \equiv \forall x_1 : r$

120: n ist ein Beweis in χ für (17 Gen r).

121: Daraus würde folgen, dass $\forall x_1 : r$ sowohl beweisbar, als auch nicht-beweisbar wäre: ein Widerspruch.

122: Jaja, »leicht«...

123: »Konstruktivität« heißt in diesem Kontext: jeder, der genug Zeit und Mühe mitbringt, kann tatsächlich einen solchen Widerspruch real nach den gegebenen Regeln konstruieren und faktisch vor sich haben.

⁴⁵ x ist χ -beweisbar, soll bedeuten: $x \in \text{Flg}(\chi)$, was nach (7) dasselbe besagt wie: $\text{Bew}_\chi(x)$.

^{45a} Denn alle im Beweise vorkommenden Existentialbehauptungen beruhen auf Satz, der, wie leicht zu sehen, intuitionistisch einwandfrei ist.

S. 187) und aus $\overline{\text{Bew}_\chi}$ (17 Gen r) folgt nach (15), daß für jede Zahl x $Sb(r_{Z(x)}^{17})$, folglich für keine Zahl $\text{Neg } Sb(r_{Z(x)}^{17})$ χ -beweisbar ist.

Adjungiert man Neg (17 Gen r) zu χ , so erhält man eine widerspruchsfreie aber nicht ω -widerspruchsfreie *Formelklasse* χ' . χ' ist widerspruchsfrei, denn sonst wäre 17 Gen r χ -beweisbar. χ' ist aber nicht ω -widerspruchsfrei, denn wegen $\overline{\text{Bew}_\chi}$ (17 Gen r) und (15) gilt: $(x) \text{Bew}_\chi Sb(r_{Z(x)}^{17})$, umso mehr also: $(x) \text{Bew}_{\chi'} Sb(r_{Z(x)}^{17})$ und anderseits gilt natürlich: $\text{Bew}_{\chi'} [\text{Neg} (17 \text{ Gen } r)]^{46}$.

Ein Spezialfall von Satz VI ist der, daß die Klasse χ aus endlich vielen *Formeln* (und ev. den daraus durch *Typenerhöhung* entstehenden) besteht. Jede endliche Klasse α ist natürlich rekursiv. Sei a die größte in α enthaltene Zahl. Dann gilt in diesem Fall für χ :

$$x \epsilon \chi \sim (Em, n) \left[m \leq x \& n \leq a \& n \epsilon \alpha \& x = mTh n \right]$$

χ ist also rekursiv. Das erlaubt z. B. zu schließen, daß auch mit Hilfe des Auswahlaxioms (für alle Typen) oder der verallgemeinerten Kontinuumshypothese nicht alle Sätze entscheidbar sind, vorausgesetzt, daß diese Hypothesen ω -widerspruchsfrei sind.

Beim Beweise von Satz VI wurden keine anderen Eigenschaften des Systems P verwendet als die folgenden:

1. Die Klassen der Axiome und die Schlußregeln (d. h. die Relation „unmittelbare Folge“) sind rekursiv definierbar (sobald man die Grundzeichen in irgend einer Weise durch natürliche Zahlen ersetzt).
2. Jede rekursive Relation ist innerhalb des Systems P definierbar (im Sinn von Satz V).

Daher gibt es in jedem formalen System, das den Voraussetzungen 1, 2 genügt und ω -widerspruchsfrei ist, unentscheidbare Sätze der Form $(x) F(x)$, wo F eine rekursiv definierte Eigenschaft natürlicher Zahlen ist, un ebenso in jeder Erweiterung eines solchen Systems durch eine rekursiv definierbare ω -widerspruchsfreie Klasse von Axiomen. Zu den Systemen, welche die Voraussetzungen 1, 2 erfüllen, gehören, wie man leicht bestätigen kann, das Z e r m e l o - F r a e n k e l s c h e und das v. N e u m a n n s c h e Axiomensystem der Mengenlehre⁴⁷, ferner das Axiomensystem der Zahlentheorie, welches aus den P e a n o s c h e n Axiomen, der rekursiven Definition [nach Schema (2)] und den logischen Regeln besteht⁴⁸.

Die Voraussetzung 1. erfüllt überhaupt jedes System, dessen Schlußregeln die gewöhnlichen sind und dessen Axiome (analog wie in P) durch Einsetzung aus endlich vielen Schemata entstehen^{48a}.

⁴⁶Die Existenz widerspruchsfreie und nicht ω -widerspruchsfreier χ ist damit natürlich nur unter der Voraussetzung bewiesen, daß es überhaupt widerspruchsfreie χ gibt (d. h. daß P widerspruchsfrei ist).

⁴⁷Der Beweis von Voraussetzung 1. gestaltet sich hier sogar einfacher als im Falle des Systems P , da es nur eine Art von Grundvariablen gibt (bzw. zwei bei J. v. Neumann).

⁴⁸Vgl. Problem III in D. H i l b e r t s Vortrag: Probleme der Grundlegung der Mathematik. Math. Ann. 102.

^{48a}Der wahre Grund für die Unvollständigkeit, welche allen formalen Systemen der Mathematik liegt anhaftet, liegt, wie im II. Teil dieser Abhandlung gezeigt werden wird, darin, daß die Bildung immer höherer Typen sich ins Transfinite fortsetzen läßt. (Vgl. D. H i l b e r t, Über das Unendliche, Math. An. 95. S. 184), während in jedem formalen System höchstens abzählbar viele vorhanden sind. Man kann nämlich zeigen, daß die hier aufgestellten unentscheidbaren Sätze durch Adjunktion passender höherer Typen (z. B. des typus ω zum System P) immer entscheidbar werden. Analoges gilt auch für das Axiomensystem der Mengenlehre.

124: ›die größte in α enthaltene Zahl‹ bedeutet: der größte Primfaktor von α .

125: Lapsig gesagt ist die Kontinuumshypothese die Frage, ob es zwischen der Dichten der Mengen \mathbb{Q} und \mathbb{R} noch eine weitere Menge gibt.

126: Die von Gödel aufgedeckte Problematik gilt für extrem viele logische Systeme, vgl. Kommentar 26.

Wir ziehen nun aus Satz VI weitere Folgerungen und geben zu diesem Zweck folgende Definition:

Eine Relation (Klasse) heißt arithmetisch, wenn sie allein mittels der Begriffe $+$, \cdot [Addition und Multiplikation, bezogen auf natürliche Zahlen⁴⁹] und den logischen Konstanten \vee , $\overline{}$, (x) , $=$ definieren lässt, wobei (x) und $=$ sich nur auf natürliche Zahlen beziehen dürfen⁵⁰. Entsprechend wird der Begriff „arithmetischer Satz“ definiert. Insbesondere sind z. B. die Relation „größer“ und „kongruent nach einem Modul“ arithmetisch, denn es gilt:

$$x > y \sim \overline{(Ez)} \left[y = x + z \right]$$

127: D. h. sie zurückführbar ist auf einfach Integer-Arithmetik und einfache logische Aussagen.

$$x \equiv y \pmod{n} \sim (Ez) \left[x = y + z \cdot n \vee y = x + z \cdot n \right]$$

128: Wenn x größer y ist, existiert kein $z \in \mathbb{N}$, so dass $y = x + z$.

Es gilt der

Satz VII: J e d e r e k u r s i v e R e l a t i o n i s t a r i t h m e t i s c h.

Wir beweisen den Satz in der Gestalt: Jede Relation der Form $x_n = \phi(x_1 \dots x_n)$, wo ϕ rekursiv ist, ist arithmetisch, und wenden die vollständige Induktion nach der Stufe von ϕ an. ϕ habe die s -te Stufe ($s > 1$). Dann gilt entweder:

$$1. \phi(x_1 \dots x_n) = \rho \left[\chi_1(x_1 \dots x_n), \chi_2(x_1 \dots x_n) \dots \chi_m(x_1 \dots x_n) \right]^{51}$$

(wo ρ und sämtliche χ_i kleinere Stufen haben als s) oder:

$$2. \phi(0, x_2 \dots x_n) = \psi(x_2 \dots x_n)$$

$$\phi(k+1, x_2 \dots x_n) = \mu \left[k, \phi(k, x_2 \dots x_n), x_2 \dots x_n \right]$$

(wo ψ, μ niedrigere Stufen als s haben) oder:

$$2. \phi(0, x_2 \dots x_n) = \psi(x_2 \dots x_n)$$

$$\phi(k+1, x_2 \dots x_n) = \mu \left[k, \phi(k, x_2 \dots x_n), x_2 \dots x_n \right]$$

(wo ψ, μ niedrigere Stufen als s haben).

Im ersten Falle gilt:

$$x_0 = \phi(x_1 \dots x_n) \sim (Ey_1 \dots y_m) \left[R(x_0 y_1 \dots y_m) \& S_1(y_1, x_1 \dots x_n) \& \dots \& S_m(y_m, x_1 \dots x_n) \right],$$

⁴⁹Die Null wird hier und im folgenden immer mit zu den natürlichen Zahlen gerechnet.

⁵⁰Das Definieren eines solchen Begriffes muß sich also allein mittels der angeführten Zeichen, Variablen für natürliche Zahlen x, y, \dots und den Zeichen $0, 1$ aufbauen (Funktions- und Mengenvariable dürfen nicht vorkommen). (In den Präfixen darf statt x natürlich auch jede andere Zahlvariable stehen.)

⁵¹Es brauchen natürlich nicht alle $x_1 \dots x_n$ in den χ_i tatsächlich vorkommen [vgl. das Beispiel in Fußnote ²⁷].

wo R bzw. S_i die nach induktiver Annahme existierenden mit $x_0 = \rho(y_1 \dots y_m)$ bzw. $y = \chi_i(x_1 \dots x_n)$ äquivalenten arithmetischen Relationen sind. Daher ist $x_0 = \phi(x_1 \dots x_n)$ in diesem Fall arithmetisch.

Im zweiten Fall wenden wir folgendes Verfahren an: Man kann die Relation $x_0 = \phi(x_1 \dots x_n)$ mit Hilfe des Begriffes „Folge von Zahlen“ (f)⁵² folgendermaßen ausdrücken:

$$x_0 = \phi(x_1 \dots x_n) \sim (Ef) \{ f_0 = \psi(x_2 \dots x_n) \& (k) [k < x_1 \longrightarrow f_{k+1} = \mu(k, f_k, x_2 \dots x_n)] \& x_0 = f_{x_1} \}$$

Wenn $S(y, x_2 \dots x_n)$ bzw. $T(z, x_1 \dots x_{n+1})$ die nach induktiver Annahme existieren mit $y = \psi(x_2 \dots x_n)$ bzw. $z = \mu(x_1 \dots x_{n+1})$ äquivalenten arithmetische Relationen sind, gilt daher:

$$x_0 = \phi(x_1 \dots x_n) \sim (Ef) \{ S(f_0, x_2 \dots x_n) \& (k) [k < x_1 \longrightarrow T(f_{k+1}, k, f_k, x_2 \dots x_n)] \& x_0 = f_{x_1} \} \quad (17)$$

Nun ersetzen wir den Begriff „Folge von Zahlen“ durch „Paar von Zahlen“, indem wir dem Zahlenpaar n, d die Zahlenfolge $f^{(n,d)}_k \left(f^{n,d}_k = [n]_{1+(k+1)d} \right)$ zuordnen, wobei $[n]_p$ den kleinsten nicht negativen Rest von n modulo p bedeutet.

Es gilt dann der

Hilfssatz 1: ist f eine beliebige Folge natürlicher Zahlen und k eine beliebige natürliche Zahl, so gibt es ein paar von natürlichen Zahlen n, d , so daß $f^{(n,d)}$ und f in den ersten k Gliedern übereinstimmen.

Beweis: Sei l die größte der Zahlen $k, f_0, f_1 \dots f_{k-1}$. Man bestimme n so, daß:

$$n \equiv [\text{mod } (1 + (i+1) l!)] \text{ für } i = 0, 1 \dots k-1$$

was möglich ist, da jede der Zahlen $1 + (i+1) l!$ ($i = 0, 1 \dots k-1$) relativ prim sind. Denn eine in den zwei von diesen Zahlen enthaltene Primzahl müßte auch in der Differenz $i_1 - i_2$ $l!$ und daher wegen $|i_1 - i_2| < l$ in $l!$ enthalten sein, was unmöglich ist. Das Zahlenpaar $n, l!$ leistet dann das Verlangte.

Da die Relation $x = [n]_p$ durch:

$$x \equiv n \pmod{p} \& x < p$$

definiert und daher arithmetisch ist, so ist auch die folgendermaßen definierte Relation $P(x_0, x_1 \dots x_n)$:

$$P(x_0 \dots x_n) \equiv (En, d) \{ S([n]_{d+1}, x_2 \dots x_n) \& () [k < x_1 \longrightarrow T([n]_{1+1(k+2)}, k, [n]_{1+d(k+1)}, x_2 \dots x_n)] \& x_0 = [n]_{1+d(x_1+1)} \}$$

arithmetisch, welche nach (17) und Hilfssatz 1 mit: $x_0 = \phi(x_1 \dots x_n)$ äquivalent ist (es kommt bei der Folge f in (17) nur auf ihren Verlauf bis zum $x_1 + 1$ -ten Glied an). Damit ist der Satz VII bewiesen.

Gemäß Satz VII gibt es zu jedem Problem der Form $(x) F(x)$ (F rekursiv) ein äquivalentes arithmetisches Problem und da der ganze Beweis von Satz VII sich (für jedes spezielle F) innerhalb des Systems P formalisieren läßt, ist diese Äquivalenz in P beweisbar. Daher gilt:

⁵² f bedeutet hier eine Variable, deren Wertbereich die Folgen natürl. Zahlen sind. Mit f_k wird das $k + 1$ -te Glied einer Folge f bezeichnet (mit f_0 das Erste).

Satz VIII: In jedem der in Satz VI genannten formalen Systeme⁵³ gibt es unentscheidbare arithmetische Sätze.

Dasselbe gilt (nach der Bemerkung auf Seite 188) für das Axiomensystem der Mengenlehre und dessen Erweiterungen durch ω -widerspruchsfreie rekursive Klassen von Axiomen.

Wir leiten schließlich noch folgendes Resultat her:

Satz IX: In allen in Satz VI genannten formalen Systemen gibt es unentscheidbare Probleme des engeren Funktionenkalküls⁵⁴ (d.h. Formeln des engeren Funktionenkalküls, für die weder Allgemeingültigkeit noch Existenz eines Gegenbeispiels beweisbar ist)⁵⁵.

Dies beruht auf:

Satz X: Jedes Problem der Form $(x)F(x)$ (F rekursiv) läßt sich zurückführen auf die Frage nach der Erfüllbarkeit einer Formel des engeren Funktionenkalküls (d.h. zu jedem rekursiven F kann man eine Formel des engeren Funktionenkalküls angeben, deren Erfüllbarkeit mit der Richtigkeit von $(x)F(x)$ äquivalent ist).

Zum engeren Funktionenkalkül (e. F.) rechnen wir diejenigen Formeln, welche sich aus den Grundzeichen $\neg, \vee, (x), =, x, y, \dots$ (Individuenvariable) $F(x), G(xy), H(x, y, z), \dots$ (Eigenschafts- und Relationsvariable) aufbauen⁵⁶, wobei (x) und $=$ sich nur auf Individuen beziehen dürfen. Wir fügen zu diesen Zeichen noch eine dritte Art von Variablen $\phi(x), \psi(xy), \chi(xyz)$ hinzu, die Gegenstandsfunktionen vertreten (d.h. $\phi(x), \psi(xy)$ etc. bezeichnen eindeutige Funktionen, deren Argumente und Werte Individuen sind⁵⁷. Eine Formel, die außer den zuerst angeführten Zeichen des e. F. noch Variable dritter Art ($\phi(x), \psi(xy)$ etc.) enthält, soll eine Formel im weiteren Sinne (i. w. S.) heißen⁵⁸. Die Begriffe „erfüllbar“, „allgemeingültig“ übertragen sich ohneweiters auf die Formel i. w. S. und es gilt der Satz, daß man zu jeder Formel i. w. S. A eine gewöhnliche Formel des e. F. B angeben kann, so daß die Erfüllbarkeit von A mit der von B äquivalent ist. B erhält man aus A , indem man die in A vorkommenden Variablen dritter Art $\phi(x), \psi(xy), \dots$ durch Ausdrücke der Form $(1z)F(zx), (1z)G(z, xy), \dots$ ersetzt, die „beschreibenden“ Funktionen im Sinne der PM I * 14 auflöst und die so erhaltene Formel mit einem Ausdruck logisch multipliziert⁵⁹, der besagt, daß sämtliche an Stelle der ϕ, ψ, \dots gesetzte F, G, \dots hinsichtlich der ersten Leerstelle genau eindeutig sind.

Wir zeigen nun, daß es zu jedem Problem der Form $(x)F(x)$ (F rekursiv) ein

⁵³Das sind diejenigen ω -widerspruchsfreien Systeme, welche aus P durch Hinzufügung einer rekursiv definierbaren Klasse von Axiomen entstehen.

⁵⁴Vgl. Hilbert - Ackermann, Grundzüge der theoretischen Logik. Im System P sind unter Formeln des engeren Funktionenkalküls diejenigen zu verstehen, welche aus den Formeln des engeren Funktionenkalküls der PM durch die auf S. 175 angedeutete Ersetzung der Relationen durch Klassen höheren Typs entstehen.

⁵⁵In meiner Arbeit: Die Vollständigkeit der Axiome des logischen Funktionenkalküls, Monatsh. f. Math. u. Phys. XXXVII, 2, habe ich gezeigt, daß jede Formel des engeren Funktionenkalküls entweder als allgemeingültig nachweisbar ist oder ein Gegenbeispiel existiert; die Existenz dieses Gegenbeispiels ist aber nach Satz IX nicht immer nachweisbar (in den angeführten formalen Systemen).

⁵⁶D. Hilbert und W. Ackermann rechnen in dem eben zitierten Buch das Zeichen $=$ nicht zum engeren Funktionenkalkül. Es geht aber zu jeder Formel in der das Zeichen $=$ vorkommt, eine solche ohne dieses Zeichen, die mit der ursprünglichen gleichzeitig erfüllbar ist (vgl. die in Fußnote ⁵⁵ zitiert Arbeit).

⁵⁷Und zwar soll der Definitionsbereich immer der ganze Individuenbereich sein.

⁵⁸Variable dritter Art dürfen dabei an allen Leerstellen für Individuenvariable stehen, z. B.: $y = \phi(x), F(x, \phi(y)), G[\psi(x, \phi(y)), x]$ usw.

⁵⁹D.h. die Konjunktion bildet.

äquivalentes betreffend die Erfüllbarkeit einer Formel i. w. S. gibt, woraus nach der eben gemachten Bemerkung Satz X folgt.

Da F rekursiv ist, gibt es eine rekursive Funktion $\Phi(x)$, so daß $F(x) \sim [\Phi(x) = 0]$, und für Φ gibt es eine Reihe von Funktionen $\Phi_1, \Phi_2 \dots \Phi_n$, so daß: $\Phi_n = \Phi, \Phi_1(x) = x + 1$ und für jedes Φ_k ($1 < k \leq n$) entweder:

$$1. (x_2 \dots x_m) [\Phi_k(0, x_2 \dots x_m) = \Phi_p(x_2 \dots x_m)] \quad (18)$$

$$(x, x_2 \dots x_m) \{ \Phi_k[\Phi_1(x), x_2 \dots x_m] = \Phi_q[x, \Phi_k(x, x_2 \dots x_m), x_2 \dots x_m] \}$$

$$p, q < k$$

oder:

$$2. (x_1 \dots x_m) [\Phi_k(x_1 \dots x_m) = \Phi_r(\Phi_{i_1}(x_1) \dots \Phi_{i_s}(x_s))]^{60} \quad (19)$$

$$r < k, i_v < k \text{ (für } v = 1, 2 \dots s)$$

oder:

$$3. (x_1 \dots x_m) [\Phi_k(x_1 \dots x_m) = \Phi_1(\Phi_1 \dots \Phi_1(0))] \quad (20)$$

Ferner bilden wir die Sätze:

$$(x) \overline{\Phi_1(x) = 0} \& (xy) [\Phi_1(x) = \Phi_1(y) \longrightarrow x = y] \quad (21)$$

$$(x) [\Phi_n(x) = 0] \quad (22)$$

Wir ersetzen nun in allen Formeln (18), (19), (20) (für $k = 2, 3 \dots n$) und in (21) (22) die Funktionen Φ_i durch Funktionsvariable ϕ_i , die Zahl 0 durch eine sonst nicht vorkommende Individuenvariablen x_0 und bilden die Konjunktion C sämtlicher so erhaltener Formeln.

Die Formel $(Ex_0)C$ hat dann die verlangte Eigenschaft, d. h.

1. Wenn $(x) [\Phi(x) = 0]$ gilt, ist $(Ex_0)C$ erfüllbar, denn die Funktionen $\Phi_1, \Phi_2 \dots \Phi_n$ ergeben dann offenbar in $(Ex_0)C$ für $\phi_1, \phi_2 \dots \phi_n$ eingesetzt einen richtigen Satz.
2. Wenn $(Ex_0)C$ erfüllbar ist, gilt $(x) [\Phi(x) = 0]$.

Beweis: Seien $\Psi_1, \Psi_2 \dots \Psi_n$ die nach Voraussetzung existierende Funktionen, welche in $(Ex_0)C$ für $\phi_1, \phi_2 \dots \phi_n$ eingesetzt einen richtigen Satz liefern. Ihr Individuenbereich Sei \mathfrak{J} . Wegen der Richtigkeit von $(Ex_0)C$ für die Funktion Ψ_4 gibt es ein Individuum a (aus \mathfrak{J}), so, daß sämtliche Formeln (18) bis (22) bei der Ersetzung der Φ_i durch Ψ_i und von 0 durch a in richtige Sätze (18') bis (22') übergeben. Wir bilden nun die kleinste Teilklasse von \mathfrak{J} , welche a enthält und gegen die Operation $\Psi_1(x)$ abgeschlossen ist. Diese Teilklasse (\mathfrak{J}') hat die Eigenschaft, daß jede der Funktionen Ψ_i auf Elemente aus \mathfrak{J}' angewendet wieder

⁶⁰ x_i ($i = 1 \dots s$) vertreten irgend welche Komplexe der Variablen $x_1, x_2 \dots x_m$, z. B. $x_1 x_3 x_2$.

Elemente aus \mathfrak{J}' ergibt. Denn für Ψ_1 gilt dies nach Definition von \mathfrak{J}' und wegen (18'), (19'), (20') überträgt sich diese Eigenschaft von Ψ_i mit niedrigerem Index auf solche mit höherem. Die Funktion, welche aus Ψ_i durch Beschränkung auf den Individuenbereich \mathfrak{J}' entstehen, nennen wir Ψ'_i . Auch für diese Funktion gelten sämtliche Formeln (18) bis (22) (bei der Ersetzung von 0 durch a und Φ_i durch Ψ'_i).

Wegen der Richtigkeit von (21) für Ψ'_1 und a kann man die Individuen aus \mathfrak{J}' eindeutig auf die natürlichen Zahlen abbilden u. zw. so, daß a in 0 und die Funktion Ψ'_1 in die Nachfolgerfunktion Φ_1 übergeht. Durch diese Abbildung gehen aber sämtliche Funktionen Ψ'_i in die Funktionen Φ_i über und wegen der Richtigkeit von (22) für Ψ'_n und a gilt $(x) [\Phi_n(x) = 0]$ oder $(x) [\Phi(x) = 0]$, was zu beweisen war⁶¹.

Da man die Überlegungen, welche zu Satz X führen, (für jedes spezielle F) auch innerhalb des Systems P durchführen kann, so ist die Äquivalenz zwischen einem Satz der Form $(x) F(x)$ (F rekursiv) und der Erfüllbarkeit der entsprechenden Formel des e. F. in P beweisbar und daher folgt aus der Unentscheidbarkeit des einen die des anderen, womit Satz IX bewiesen ist.⁶²

4.

Aus den Ergebnissen von Abschnitt 2 folgt ein merkwürdiges Resultat, bezüglich eines Widerspruchslosigkeitsbeweises des Systems P (und seiner Erweiterungen), der durch folgenden Satz ausgesprochen wird:

Satz XI: Sei χ eine beliebige rekursive widerspruchsfreie⁶³ Klasse von *Formeln*, dann gilt: Die *Satzformel*, welche besagt, daß χ widerspruchsfrei ist, ist nicht χ -*beweisbar*; insbesondere ist die Widerspruchsfreiheit von P in P unbeweisbar⁶⁴, vorausgesetzt, daß P widerspruchsfrei ist (im entgegengesetzten Fall ist natürlich jede Aussage beweisbar).

Der Beweis ist (in Umrissen skizziert) der folgende: Sei χ eine beliebige für die folgenden Betrachtungen ein für allemal gewählte rekursive Klasse von *Formeln* (im einfachsten Falle die leere Klasse). Zum Beweise der Tatsache, daß 17 Gen r nicht χ -*beweisbar* ist⁶⁵, wurde, wie aus 1. Seite 187 hervorgeht, nur die Widerspruchsfreiheit von χ benutzt, d. h. es gilt:

$$\text{Wid } (x) \longrightarrow \overline{\text{Bew}_x(17 \text{ Gen } r)} \tag{23}$$

d. h. nach (6.1):

$$\text{Wid } (x) \longrightarrow (x) \overline{x B_x(17 \text{ Gen } r)}$$

Nach (13) ist $17 \text{ Gen } r = Sb\left(p_{Z(p)}^{19}\right)$ und daher:

$$\text{Wid } (x) \longrightarrow (x) \overline{x B_x Sb\left(p_{Z(p)}^{19}\right)}$$

d. h. nach (8.1):

⁶¹Aus Satz X folgt z. B., daß das F e r m a t s c h e und das G o l d b a c h s c h e Problem lösbar wären, wenn man das Entscheidungsproblem des e. F. gelöst hätte.

⁶²Satz IX gilt natürlich auch für das Axiomensystem der Mengenlehre und dessen Erweiterungen durch rekursiv definierbar ω -widerspruchsfreie Klassen von Axiomen, da es ja auch in diesem Systemen unentscheidbare Sätze der Form $(x) F(x)$ (F rekursiv) gibt

⁶³ χ ist widerspruchsfrei (abgekürzt als Wid (x)) wird folgendermaßen definiert: Wid $(x) \equiv (Ex) [\text{Form } (x) \& \text{Bew}_\chi(x)]$.

⁶⁴Dies folgt, wenn man für χ die leere Klasse von *Formeln* einsetzt.

⁶⁵ r hängt natürlich (ebenso wie p) von χ ab.

129: Zweiter Unvollständigkeitssatz: ein System kann aus sich selbst heraus seine eigene Widerspruchsfreiheit nicht beweisen.

$$\text{Wid}(x) \longrightarrow (x) Q(x, p) \tag{24}$$

Wir stellen nun folgendes fest: Sämtliche in Abschnitt 2⁶⁶ und Abschnitt 4 bisher definierten Begriffe (bzw. bewiesene Behauptungen) sind auch in P ausdrückbar (bzw. beweisbar). Denn es wurden überall nur die gewöhnlichen Definitions- und Beweismethoden der klassischen Mathematik verwendet, wie sie im System P formalisiert sind. Insbesondere ist χ (wie jede rekursive Klasse) in P definierbar. Sei w die *Satzformel*, durch welche in P $\text{Wid}(x)$ ausgedrückt wird. Die Relation $Q(x, y)$ wird gemäß (8.1), (9), (10) durch das *Relationszeichen* q ausgedrückt, folglich $Q(x, p)$ durch $r \left[\text{da nach (12) } r = Sb \left(q_{Z(p)}^{19} \right) \right]$ und der Satz $(x) Q(x, p)$ durch 17 Gen r .

Wegen (24) ist also $w \text{ Imp } (17 \text{ Gen } r)$ in P beweisbar⁶⁷ (umso mehr χ -*beweisbar*). Wäre nun w χ -*beweisbar*, so wäre auch 17 Gen r χ -*beweisbar* und daraus würde nach (23) folgen, daß χ nicht widerspruchsfrei ist.

Es sei bemerkt, daß auch dieser Beweis konstruktiv ist, d. h. er gestattet, falls ein *Beweis* aus χ für w vorgelegt ist, ein Widerspruch aus χ effektiv herzuleiten. Der ganze Beweis für Satz XI läßt sich wörtlich auch auf das Axiomensystem der Mengenlehre M und der klassischen Mathematik⁶⁸ A übertragen und liefert auch hier das Resultat: es gibt keinen Widerspruchlosigkeitsbeweis für M bzw. A , der innerhalb von M bzw. A formalisiert werden könnte, vorausgesetzt, daß M bzw. A widerspruchsfrei ist. Es sei ausdrücklich bemerkt, daß Satz XI (und die entsprechenden Resultate über M, A) in keinem Widerspruch zum H i l b e r t'schen formalistischen Standpunkt stehen. Denn dieser setzt nur die Existenz eines mit finiten Mitteln geführten Widerspruchsfreiheitsbeweises voraus und es wäre denkbar, daß es finite Beweise gibt, die sich in P (bzw. M, A) n i c h t darstellen lassen.

Da es für jede widerspruchsfreie Klasse χ w nicht χ -*beweisbar* ist, so gibt es schon immer dann (aus χ) unentscheidbare Sätze (nämlich w , wenn $\text{Neg}(w)$ nicht χ -beweisbar ist; m. a. W. kann man in Satz VI die Voraussetzung der ω -Widerspruchsfreiheit ersetzen durch die folgende: Die Aussage „ χ ist widerspruchsvoll“ ist nicht χ -beweisbar. (Man beachte, daß es widerspruchsfreie χ gibt, für die diese Aussage χ -beweisbar ist.)

Wir haben uns in dieser Arbeit im wesentlichen auf das System P beschränkt und die Anwendungen auf andere Systeme nur angedeutet. In voller Allgemeinheit werden die Resultate in einer demnächst erscheinenden Fortsetzung ausgesprochen und bewiesen werden. In dieser Arbeit wird auch der nur skizzenhaft geführte Beweis von Satz XI ausführlich dargestellt werden.

(Eingelangt: 17.XI.1930)

130: Man braucht keine extraordinäre ›Magie‹, um diese Sätze herzuleiten; es reichen die einfachen Grundlagen der logischen Systeme.

131: Der zweite gödel'sche Unvollständigkeitssatz; ein ausreichend komplexes System kann seine eigene Vollständigkeit nicht beweisen.

⁶⁶Von der Definition für „rekursiv“ auf Seite 178 bis zum Beweis von Satz VI inkl.

⁶⁷Daß aus (23) auf die Richtigkeit von $w \text{ Imp } (17 \text{ Gen } r)$ geschlossen werden kann, beruht einfach darauf, daß der unentscheidbare Satz17 Gen r , wie gleich zu Anfang bemerkt, seine eigene Unbeweisbarkeit behauptet.

⁶⁸Vgl. J. v. N e u m a n n, Zur H i l b e r t'schen Beweistheorie, Math. Zeitschr. 26, 1927.