Skriptum Mathematische Logik

T. von der Twer

Inhaltsverzeichnis

1. Was ist Logik, was ist Mathematische Logik?

Traditionell beschäftigt sich Philosophie mit Logik, länger schon als die Mathematik. Man denkt an Aristoteles. Andererseits ist aber das Werk Euklids der bahnbrechende Versuch axiomatischen Denkens und damit der erste Meilenstein der Logik im tieferen mathematischen Sinn. So verhält es sich auch heute noch, nach den Entwicklungen des 18. nis 20. Jahrhunderts, dass die Mathematik mit ihren Anforderungen an Logik die treibende Kraft zur Entwicklung von Logik ist und daher ihre eigene Disziplin 'Mathematische Logik' bildete. Es ist durchaus in Ordnung, weitergehende Gesichtspunkte mit Logik zu verbinden oder zur Logik zu zählen, die in der Mathematischen Logik keine Rolle spielen. Allerdings sind unter diesen Gesichtspunkten eher schwierige Fragen als Antworten aufgetreten. Mathematische Logik indessen hat entwickelte mathematische Methoden, mit denen ebenfalls schwierige Fragen - durchaus auch von philosophischer Tragweite - mit mathematischer Genauigkeit präzisiert und beantwortet werden konnten. Die Mathematik musste so etwas entwickeln, um sich bei der Abstraktheit ihrer Gegenstände nicht im Widersprüchlichen zu verfangen ('mathematische Grundlagenkrise' zu Beginn des 20. Jahrhunderts). Aber schon die Abstraktion selbst zwingt zu logischer Reflexion:

Man möchte nicht von einem Körper sprechen, sondern von allen Körpern und ihren Beziehungen. Also definiert man Klassen interessanter wichtiger mathematischer Strukturen durch Axiomensysteme. Dann fragt man nach allen Folgerungen aus diesen Systemen, die also für alle Strukturen der axiomatisch definierten Klasse gültig sind und in jedem Beispiel angewandt werden dürfen. Das fordert, den Begriff 'Gültigkeit einer Aussage in einer Struktur' genau zu klären und ebenso den Begriff der Folgerung. Daran schließt sich natürlich die Frage, ob man alle Folgerungen aus einem Axiomensystem effektiv herstellen und durch ein handhabbares System von logischen Regeln in den Griff bekommen kann. Diese Unternehmungen kennzeichnen das Gebiet der Prädikatenlogik (eine Teildisziplin der Mathematischen Logik), und letztere Frage konnte für die Prädikatenlogik erster Stufe (worin sich das Meiste der Mathematik abspielt) positiv beantwortet werden. Wegen dieses Aspektes der Selbstreflexion spricht man auch von 'Metamathematik' (worin also über Mathematik gesprochen wird). Die Besonderheit ist nun aber, dass Metamathematik nicht etwas Anderes ist als Mathematik, sondern völlig im Rahmen der Mathematik selbst fruchtbar zu behandeln. Sinnvolle Aussagen über Mathematik sind stets nur von der Mathematik selbst gemacht und begründet worden. (Ein unrühmliches Beispiel von Aussagen über Mathematik von außerhalb wird vom Physiker Barrows in 'Himmel der Zahlen' gegeben, glücklicherweise ist das eine Ausnahme bei Physikern, eher schon sind unrühmliche Beispiele bei Philosophen gewissen Typs (Beispiel: Hegel) zu erwarten. - Stets ist in solchen Fällen das Fazit: 'Hat nichts verstanden'.)

Ferner war genauer zu klären, was 'effektiv berechenbar' heißt. Das macht in der Mathematischen Logik das Teilgebiet der Rekursionstheorie (oder auch Theorie der Berechenbarkeit und Entscheidbarkeit) aus, das seinerseits wieder eng mit Informatik oder Computerwissenschaft verbunden ist - die wesentlichen theoretischen Einsichten darüber, was man prinzipiell mit einem Computer tun kann (und dass dies deutlich weniger ist als 'Mathematik treiben'), waren in der Mathematik bekannt, bevor man die ersten müden Computer bauen konnte.

Dazu kommt eine gewissse Art, die Beziehungen zwischen Klassen algebraischer Strukturen und ihren Axiomensystemen bzw. deren Folgerungen zu untersuchen, auch dabei den Aspekt der Berechenbarkeit zu berücksichtigen. Dies aus der Prädikatenlogik gewachsene Teilgebiet der Mathematischen Logik heißt Modelltheorie.

Mit der Entwicklung der Mathematik entstand das System der Mengenlehre, und zur Selbstreflexion der Mathematik gehört es, diese zu untersuchen. Dazu gehören insbesondere die Fragen nach Konsistenz und Vollständigkeit, auch nach der Rechtfertigung von Axiomen wie Auswahlaxion und Kontinuumshypothese. Weil diese Axiome so wichtig sind, wollen wir sie hier schon einmal erklären: Das Auswahlaxiom besagt: Wenn eine Familie $(A_i)_{i\in I}$ von nicht leeren Mengen gegeben ist, so gibt es eine Menge M, die aus jeder der Mengen A_i jeweils genau ein Element enthält.' Es gibt viele gleichwertige Formulierung, wie Existenz von Wohlordnungen auf jeder Menge oder Zornsches Lemma. Die spezielle Kontinuumshypothese besagt: 'Es gibt keine Teilmenge von $\mathbb{R}$, deren Kardinalzahl echt zwischen der von $\mathbb{N}$ und der von $\mathbb{R}$ liegt'. Die allgemeine Kontinuumshypothese besagt, dass es auch niemals eine Kardinalzahl zwischen der einer unendlichen Menge M und der Kardinalzahl der Potenzmenge von M gibt. (Man sollte wissen, dass speziell $\mathbb{R}$ dieselbe Kardinalzahl wie die Potenzmenge von $\mathbb{N}$ besitzt.) Dieser Komplex erzeugte wieder eine eigene Teildisziplin der Mathematischen Logik, die Mengenlehre. Auf die genannten Fragen waren

die Antworten zum Teil verblüffend negativ: Man hat keinerlei Chance, diese Fragen zu entscheiden, die Mengenlehre als das umfassende System aller logischen Mittel, mit denen man mathematisch arbeitet, ist wesentlich unvollständig und kann auch nicht vervollständigt werden, wenn es konsistent bleiben soll. Insbesondere die Frage der Konsistenz selbst kann darin nicht entschieden werden. Ferner: Wenn überhaupt das herauskristallisierte System der Mengenlehre konsistent ist, so ist es mit Auswahlaxiom ebenso konsistent wie mit dessen Verneinung, mit Kontinuumshypothese ebenso wie mit ihrer Verneinung.

Eine letzte Disziplin enthält Vieles der zuvor genannten, obgleich im Zentrum ihres Interesses eine ganz konkrete Struktur steht, die der natürlichen Zahlen mit Nachfolgerbildung, Addition und Multiplikation. Diese bildet den Ausgangspunkt der Mathematik 'von unten', alles Kombinatorische, alles 'Rechnen' spielt sich darin ab, auch die Klärung des Begriffs der Berechenbarkeit selbst. Sie ist ursprünglicher Gegenstand der Zahlentheorie, die sich als unerhört schwierig erwiesen hat. Diese Disziplin heißt im Rahmen der Mathematischen Logik 'Peano-Arithmetik', und sie hat einige Verbindungen mit der Rekursionstheorie, aber auch mit der Zahlentheorie. Das wollen wir einmal konkreter illustrieren: 1900 stellte Hilbert der mathematischen Gemeinschaft 100 schwierige und besonders relevante Probleme. Viele davon sind ein Quell der mathematischen Fortentwicklung geworden, wegen ihrer Interessantheit und Schwierigkeit. Die Probleme sebst und diejenigen, die erfolgreich daran gearbeitet haben, auch deren neu entwickelte Methoden, sind mit Recht berühmt geworden. Das 10. Hilbertsche Problem lautete: Man entwickle ein Verfahren, zu entscheiden, ob eine Polynomgleichung (mit ganzzahligen Koeffizienten) in ganzen Zahlen lösbar ist. Die Antwort war 1970 fertig, aufgrund jahrzehntelanger Arbeit von Julia Robinson, Martin Davis und Juri Matiasevitsch: Ein solches Verfahren kann es nicht geben. Dies Resultat ist das bedeutendste der Peanoarithmetik, und es gibt eine konkrete Erklärung für die Schwierigkeit der Zahlentheorie (die von Hilbert offensichtlich noch unterschätzt wurde, wie man am Optimismus seiner Formulierung erkennt). Eine andere Beleuchtung bekam diese Schwierigkeit durch das Resultat von Tarski, dass der Begriff der Wahrheit in der Zahlentheorie unendlich viele Stufen oberhalb des Entscheidbaren (oder von einem Computer Berechenbaren) liegt. Vom Gödelschen Unvollständigkeitssatz für die Peanoarithmetik kommt man übrigens unmittelbar dazu, dass die Konsistenz der Mengenlehre nicht im System der Mengenlehre bewiesen werden kann. Dies wirft noch einmal ein Licht darauf, wie allgemein die Bedeutung der Zahlentheorie im engeren Sinne ist.

Dies war eine sehr kurze Beschreibung dessen, womit sich mathematische Logik beschäftigt. Ich hoffe, dass am Ende für alle beteiligten Studierenden ein befriedigendes Grundverständnis entsteht.

Diese Vorlesung ist eine Ergänzungsveranstaltung. Sie möchte einen Beitrag zur mathematischen Allgemeinbildung leisten. Daher soll ein Einblick in alle Teilgebiete der Mathematischen Logik gegeben werden, zu jedem sollen auch wichtige Resultate bewiesen und die zugehörigen Methoden kenntlich gemacht werden. Dabei soll auch der enge Zusammenhang zwischen den verschiedenen Aspekten des Gebietes deutlich werden. Allerdings soll es durchaus vom Interesse der jeweiligen Hörer abhängen, was besonders betont und was nur gestreift wird. Ebenso wird Rücksicht auf die jeweilige mathematische Erfahrung genommen. Es ist durchaus erwünscht, dass ein genaueres logisches Verständnis der mathematischen Praxis herauskommt, indem der logische Aspekt besser gesehen wird, also kompliziertere Aussagen formal und inhaltlich besser verstanden werden, ebenso das Beweisen selbst. Aber es sollten auch ein paar tiefere mathematische Resultate verstanden und in Zusammenhang gebracht werden.

2. Aussagenlogik: Eine Bemerkung

Man denkt unter dem Stichwort 'Logik' vielleicht zunächst an das Elementarste davon, die pure 'Aussagenlogik'. Die wollen wir hier als trivial abtun und uns darauf verlassen, das alles Wichtige davon aus dem mathematischen Grundstudium bekannt ist. Es handelt sich nur darum, dass man Aussagen mittels der Junktoren 'nicht', 'und', 'oder', 'wenn-so', 'genau dann, wenn' verbindet, symbolisch $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$. Dass man hier algorithmisch entscheiden kann, ob eine formale Aussage mit Aussagenvariablen und diesen Junktoren gebildet, ist mit den Wahrheitstafeln bekannt. Ferner sollte man die Wahrheitsdefinition insbesondere von $\alpha \rightarrow \beta$ kennen und auch intuitiv einsehen, dass logisch gültig ist, z.B.: $\neg (\alpha \wedge \beta) \leftrightarrow \neg \alpha \vee \neg \beta$, entsprechend mit Vertauschen von $\wedge, \vee$. Auch sollten die hier bereits benutzten Regeln des Einsparens von Klammern bekannt sein, wonach $\neg$ am stärksten bindet, dann $\wedge, \vee$, am schwächsten $\rightarrow, \leftrightarrow$, die im Beispiel benutzt wurden. Auch sollte die Analogie der Struktur des Rechnens

mit den Junktoren $\rightharpoonup, \wedge, \vee$ zum Rechnen mit Mengenalgebra mit den Operationen Komplement, Durchschnitt, Vereinigung bekannt sein. Studienanfänger lernen bereits in ihrem Grundstudium notwendigerweise, dass die Aussagenlogik keineswegs genügt und die logische Analyse von Aussagen feiner sein muss, dass insbesondere ein gewisser Umgang mit den Quantoren $\forall, \exists$ dazu gehört, die wesentliche Bestandteile jeder methematischen Aussage bilden. Man kennt also die logische Gültigkeit von $\forall x \rightharpoonup \alpha$ zu $\rightharpoonup \exists x \alpha$ usw. Man kennt Formulierungen in den Axiomen der Körpertheorie wie $\forall x \forall y \forall z \left(x \left(y + z\right) = xy + xz\right)$ usw. Aber auf dieser Stufe der Analyse (man nennt sie Prädikatenlogik erster Stufe) gibt es bereits einige nichttriviale Erkenntnisse, die man im Grundstudium gewöhnlich nicht zur Kenntnis nimmt. Wir werden - unerlässlich für jede weitergehende Beschäftigung mit Mathematischer Logik - den Aufbau der Prädikatenlogik im ersten Kapitel sehr systematisch und vollständig betreiben und dabei wesentliche logische bzw. metamathematische Grundbegriffe bilden. Zuvor wollen wir jedoch recht informell beschreiben, warum man von 'Prädikatenlogik 1. Stufe' und etwa 'Prädikatenlogik 2. Stufe' (auch höherer Stufe) spricht.

3. Prädikatenlogik 1. Stufe und 2. Stufe: Eine Vorbemerkung

Die gewöhnlichen Axiomensysteme für Gruppen, Körper, Ringe, Vektorräume sehen so aus: Man hat Symbole für die Verknüpfungen wie $+, \cdot$ und bildet Gleichungen zwischen Termen, verbindet mit aussagenlogischen Junktoren, setzt Quantoren mit Angabe der freien Variablen davor, worauf sie sich beziehen, wie $\forall x, \exists x$. Mehr nicht. Das Wesentliche: Es wird nur über die Objekte der Grundmenge quantifiziert. Die Logik, welche sich in diesem sprachlichen Rahmen bewegt, heißt Prädikatenlogik erster Stufe. Es wird nicht über Mengen quantifiziert. Axiome wie die bekannten, mit denen die Struktur der natürlichen, aber auch der rellen Zahlen, eindeutig beschrieben werden können, sind in diesem Rahmen nicht formulierbar. Man denke an das Induktionsaxiom: 'Jede nicht leere Menge natürlicher Zahlen hat ein kleinstes Element'. Formalisiert wäre das:

$$\forall S \left(\exists x \left(x \in S\right) \rightarrow \exists y (y \in S \wedge \forall z \left(z \in S \rightarrow y \leq z\right)\right).$$

Das Entscheidende ist hier: Quantifiziert wird über Teilmengen der Grundmenge, und der Quantor $\forall S$ bezieht sich definitionsgemäß auf die Menge aller Teilmengen der Grundmenge. Einzig dieser Quantor führt aus der Prädikatenlogik hinaus. Den neuen Rahmen nennt man 'Prädikatenlogik 2. Stufe'. Darin kann man auch formulieren: 'Es gibt eine Abbildung der Grundmenge in sich selbst, die injektiv ist, aber nicht surjektiv', und damit kann man den Begriff der Unendlichkeit der Grundmenge formulieren. Ebenso sind Formulierungen von Eigenschaften wie den reellen Zahlen bekannt wie 'Jede Teilmenge, welche nach oben [unten] beschränkt ist, hat eine kleinste obere [größte untere] Schranke'. (Das bedeutet die Vollständigkeit der reellen Zahlen.)

Wir wollen noch kurz erklären, dass die Bildung '$x \in S$' nicht über die Logik 1. Stufe hinausführt. Denn die Menge S kann man ohne weiteres als Prädikat auffassen und schreiben 'Sx' statt '$x \in S$', gerade so, wie man eine zweistellige Ordnungsrelation $<$ als Menge von Paaren auffassen kann oder auch 'Px' für 'x ist positiv', also für 'x ist Element der Menge der positiven Zahlen', sagen kann. Einstellige und mehrstellige Relationen als 'Prädikate' gehören durchaus auch in die Prädikatenlogik erster Stufe, aber nur als Konstanten (im Bereich der entsprechenden Potenzmenge), nicht als Objekte, über die quantifiziert wird.

Entsprechend entsteht Logik höherer Stufe, indem man über Elemente der Potenzmenge der Potenzmenge...der Grundmenge quantifiziert. Wir werden einsehen, dass die Logik 2. Stufe sich völlig anders verhält als die erster Stufe: Die Frage nach der Existenz eines vollständigen Systems logischer Regeln lässt sich für die Logik 1. Stufe positiv beantworten, für die Logik 2. Stufe fällt die Antwort negativ aus!

KAPITEL 1

Prädikatenlogik erster Stufe

1. Einleitung: Motivierung und Ausblick auf typische Grundbegriffe und Fragestellungen

Typische mathematische Aussagen lauten so: Wenn für ein $a \in A$ gilt: $\beta(a)$, dann gilt für ein $b \in A$: $\gamma(b)$. Dabei sind β, γ Aussageformen (die wir hier 'Formeln' nennen werden). Simples Beispiel: Wenn es eine ganze Zahl a gibt mit $4a = c$, dann gibt es eine ganze Zahl b mit $2b = c$. Offenbar ist diese Aussage logisch wahr unter den typischen Voraussetzungen, wie sie für die ganzen Zahlen mit Multiplikation gelten: Man argumentiert natürlich: Sei a_0 so, dass $4a_0 = c$, dann setze $b_0 = 2a_0$. Damit gilt $2b_0 = 2(2a_0) = (2 \cdot 2) a_0 = 4a_0 = c$. Erkennbar ist, dass man im Wesentlichen das Assoziativgesetz benötigt, ferner nur, dass 4 ein Name für das Resultat von $2 \cdot 2$ ist. Außerdem haben wir ein typisches logisches Verfahren der Mathematik benutzt: Aus der Formel $\exists a (4a = c)$ benutzen wir als Voraussetzung, indem wir den Quantor $\exists$ beseitigen und sagen: Sei a_0 ein Beispiel, also $4a_0 = c$. Hier ist a_0 eine (neu eingeführte) Konstante. Ebenso typisch ist das weitere Vorgehen: Aus dem Beispiel a_0 machen wir ein Beispiel, die Zahl $2a_0$, für die Existenzaussage, auf die wir hinauswollen. Wir etablieren also die Formel:

$$4x = c \implies 2(2x) = c.$$

Nun kommt mit rein logischem Schließen:

$$4x = c \implies \exists x (2x = c),$$

dann weiter:

$$\exists x (4x = c) \implies \exists x (2x = c).$$

Das sind Formeln, die wir nach rein schematischem Verfahren aus $4x = c \implies 2(2x) = c$ gewinnen: Hintere Existenzeinführung - Schluss aus einem Beispiel auf die Existenz, dann vordere Existenzeinführung: Wenn x nicht frei in β vorkommt, dann kann man von

$$\alpha(x) \implies \beta$$

schließen auf

$$\exists x \alpha(x) \implies \beta.$$

Diese Beispiele sollten so viel illustrieren:

(1) Man muss für die logische Analyse des mathematischen Argumentierens weiter gehen als die Aussagenlogik und die Quantoren mit erfassen, dazu das Innere von Aussageformen weiter analysieren. (Man beachte, dass aussagenlogische Analyse der Formel $\exists x (4x = c) \implies \exists x (2x = c)$ nur ergibt: $\alpha \implies \beta$. Diese Formel ist offensichtlich nicht als wahr zu erkennen, auch nicht unter den gegebenen mathematischen Voraussetzungen (Assoziativgesetz und $2 \cdot 2 = 4$), denn diese wären hier nur 'γ, δ', und offenbar ist nicht allgemeingültig, dass $\gamma \wedge \delta \implies (\alpha \implies \beta)$. Dafür muss man zunächst einmal die **Syntax** (also den Umgang mit Formeln als formalen Zeichenreihen) klären - was sind Formeln, wie sind sie zusammenzusetzen zu neuen, was heißt 'x kommt nicht frei in der Formel α vor' usw.

(2) Für den Umgang mit den Quantoren $\forall, \exists$ ('für alle', 'es exisiert') hat man weitergehende logische Regeln, die offensichtlich mit dem tatsächlich geübten mathematischen Schließen viel zu tun haben und eigentlich nur die mathematische Praxis formalisieren und in dem Sinne analysieren, dass man dann etwa nach Aufstellen eines Systems solcher Regeln die Frage stellen könnte: Ist das alles, was die Mathematik benötigt?

Man beachte, dass die zweite Frage nicht banal ist: Man beobachtet einige gültige formallogische Regeln wie

$$\forall x (\alpha \implies \beta) \implies (\forall x \alpha \implies \forall x \beta)$$

und stellt mit einigen davon ein System zusammen. Dann fragt man sich, ob es weitere Regeln gibt, die das System nicht abdeckt. Wir werden auf diese Frage für geeignete Systeme eine positive Antwort für die Logik 1. Stufe oder auch Prädikatenlogik 1. Stufe bekommen, eine negative dagegen für *alle gültigen* Systeme der Logik 2. Stufe. Diese Resultate nennt man Vollständigkeit der Prädikatenlogik 1. Stufe und Unvollständigkeit der Logik 2. Stufe. Hier ist von **Semantik** die Rede, von der *inhaltlichen Bedeutung* der Formeln: Dass eine formallogische Regel gültig ist, bedeutet 'gültig für alle mathematischen Strukturen, über welche die in der Regel vorkommenden Formeln reden können'. Hier ist offenbar der grundlegende sematische Begriff 'Gültigkeit einer Formel in einer Struktur' zu klären, dazu der Begriff der mathematischen Struktur selbst. Aber es geht noch weiter: Der Begriff der 'Vollständigkeit' eines Systems formallogischer Regeln stellt eine Beziehung zwischen Syntax und Semantik dar, dass alle *inhaltlich gültigen Folgerungen* (aus einem Axiomensystem etwa) auch *mittels der rein formalen Regeln ableitbar* sind. Es fragt sich also, ob der semantische Begriff der Folgerbarkeit mit dem syntaktischen Begriff der Ableitbarkeit übereinstimmt oder nicht.

Übrigens entwickelt man selbstverständlich auch die grundlegende Syntax nicht, ohne an die beabsichtige semantische Deutung zu denken.

2. Syntax: Terme und Formeln, und eine wichtige Technik für Definitionen und Beweise

Wir wollen zunächst den Begriff 'Sprache der Logik 1. Stufe für einen bestimmten Typ mathematischer Strukturen' erkären, dafür zunächst der Begriff 'Struktur eines Typs':

DEFINITION 1. *Eine* ***mathematische Struktur*** *ist ein Tripel*

$$\mathcal{A} = \left\langle A, \left(\left(f_i^k\right)^{\mathcal{A}}\right)_{k\in\mathbb{N}_0,\ i\in I_k}, \left(\left(R_j^k\right)^{\mathcal{A}}\right)_{k\in\mathbb{N},\ j\in J_k} \right\rangle .$$

Dabei ist A eine nichtleere (!) 'Trägermenge' (darin sind die mathematischen Objekte, von denen die Rede sein soll), ferner ist $\left(f_i^k\right)^{\mathcal{A}}$ für $k \geq 1$ eine Abbildung $A^k \to A$, für $k = 0$ ist $\left(f_i^k\right)^{\mathcal{A}}$ eine Konstante, schließlich sind die $\left(R_j^k\right)^{\mathcal{A}}$ k-stellige Relationen auf A, also $R_j^k \subset A^k$. Speziell für $k = 1$ ist das eine ausgezeichnete Teilmenge der Trägermenge A. Die Mengen I_k und J_k sind Indexmengen, die auch leer sein können. Unter dem ***Typ der Struktur*** *$\mathcal{A}$ versteht man das Paar $(I_k)_{k\geq 0}$,$(J_k)_{k\geq 1}$ der Folgen der Indexmengen.*

Erläuterung: Der Begriff sieht etwas sperrig aus, aber an folgenden Beipielen sieht man schnell, worum es geht: Betrachten wir einen Körper K (in der mathematischen Praxis bezeichnet man offenbar die Trägermenge und die Struktur gleich, was sie offenbar nicht sind, aber da macht diese Ungenauigkeit nichts aus), dann schreiben wir im Sinne der Definition ausführlicher $\mathcal{K} = \left\langle K, 0^{\mathcal{K}}, 1^{\mathcal{K}}, +^{\mathcal{K}}, \cdot^{\mathcal{K}} \right\rangle$. Wir zählen also die Konstanten und die Funktionen $\left(f_i^k\right)^{\mathcal{K}}$ auf, hier hat man: $I_0 = I_2 = \{1, 2\}$, $I_k = \varnothing$ für alle $k \neq 0, 2$, und $J_k = \varnothing$ für alle $k \geq 1$. Übrigens werden wir später auch im Sinne der mathematischen Praxis bequemer werden und einfach $\langle K, 0, 1, +, \cdot\rangle$ schreiben, obwohl gerade die Unterscheidung zwischen $\left(f_i^k\right)^{\mathcal{K}}$ und f_i^k wichtig ist: $\left(f_1^2\right)^{\mathcal{K}}$, $\left(f_2^2\right)^{\mathcal{K}}$ sind hier die Addition und die Multiplikation im Körper, dagegen werden f_i^k die Symbole der formalen Sprache sein, welche geeignet ist, über Körper zu reden.

Zwei weitere Beipiele: $\langle \mathbb{Q}, <\rangle$ ist nicht der Körper der rationalen Zahlen, sondern nur die Menge der rationalen Zahlen mit ihrer Anordnung, also haben wir nur die zweistellige Ordnungsrelation. Nun können wir Beides zusammenfassen und die Strukturen 'angeordnete Körper' bilden, Beispiele sind: $\langle \mathbb{Q}, 0, 1, +, \cdot, <\rangle$, $\langle \mathbb{R}, 0, 1, +, \cdot, <\rangle$. Natürlich können wir auch eine Ordnungsrelation auf $\mathbb{C}$ einführen, z.B. lexikographisch, und diese $<^{Quatsch}$nennen und die Struktur $\left\langle \mathbb{C}, 0, 1, +, \cdot, <^{Quatsch}\right\rangle$ bilden, aber das ist bekanntlich kein angeordneter Körper, bei dem man verlangt, dass die Ordnung mit den Operationen zusammenpasst.

Man erkennt nun leicht, dass wir es in der mathematischen Praxis meist mit Strukturen zu tun haben, bei denen lediglich Konstanten, ein- und zweistellige Operationen (fast immer nur zweistellige) und zweistelligen Relationen vorkommen, und von diesen nur sehr wenige. Dennoch sei schon einmal vorweggenommen, dass darin durchaus so viel Komplexität vorkommt, wie es nur geben kann. Eine Ausnahme ist allerdings zu erwähnen: Wenn die Struktur nur von einstelligen Relationen ausgemacht wird (also ausgezeichneten Teilmengen der Trägermenge), dann ist sie trivial. (Das kann man auch verstehen, wenn man einsieht, dass in diesem Fall die ganze Logik auf pure Aussagenlogik reduziert wird, und

diese ist bekanntlich trivial.) Mit 'trivial' ist hier zweierlei gemeint, einmal 'langweilig','uninteressant', zum Anderen auch die genauere technische Aussage: Man kann mit einem Algorithmus entscheiden, ob eine vorgelegt (formale) Aussage logisch gültig ist oder nicht, *wenn man sich beschränkt auf Aussagen,* welche nur einstellige Relationssymbole enthalten, dazu keinerlei Funktionssymbole außer Konstanten. Wir werden noch sehen, dass dies nicht für die allgemeine Prädikatenlogik gilt.

Oben haben wir informell bereits zwischen formal aufgefassten Aussagen und ihrer Gültigkeit in einer Struktur unterschieden. Das müssen wir nun genauer ausführen. Dazu führen wir eine formale Sprache der Prädikatenlogik erster Stufe ein und zeichnen darin Zeichenreihen als Terme und Formeln bzw. Aussagen aus, völlig getrennt von einer Bedeutung. Erst dann kommt die Semantik ins Spiel, also die Bedeutung in Strukturen. In der mathematischen Umgangssprache als Metasprache reden wir über die formalen Sprachen als Objektsprachen und über die Beziehung der Gültigkeit einer Formel in einer Struktur. Um diesen Unterschied deutlich hervorzuheben, führen wir für die Symbole $=, \Longrightarrow, \Longleftrightarrow$ der mathematischen Umgangssprache in der Objektsprache die formalen Symbole $\doteq, \to, \leftrightarrow$ ein.

Nun ist es sehr leicht zu sehen, wie eine formale Sprache aussehen muss, welche geeignet ist, über Stukturen eines gewissen Typs zu 'reden': Man braucht für jede Relation das entsprechende Relationssymbol R_j^k, für jede Operation das entsprechende Funktionssymbol f_i^k. Meist fassen wir dabei die nullstelligen Funktionssymbole als Symbole $(c_i)_{i\in I}$ für Konstanten gesondert auf. Ferner braucht man Symbole $x_1, x_2, ...$ für die Variablen und Symbole $\neg, \wedge, \vee, \to, \leftrightarrow$ (nicht, und, oder, wenn - so, genau dann, wenn) und eventuell Klammern.

Dann bildet man wie in der Mathematik sonst üblich Terme und Formeln (die deutsch auch gern 'Aussageformen' genannt werden). Das wollen wir nun allerdings sehr genau ausführen:

DEFINITION 2. *Eine Sprache L der Prädikatenlogik erster Stufe besteht aus einem Alphabet von Symbolen und speziellen Symbolfolgen (synonym: Zeichreihen, Zeichenketten), die Terme oder Formeln heißen (diese werden in den folgenden Definitionen erklärt). Das Alphabet umfasst:*

(*i*) *Variablen v_i, $i \in \mathbb{N}$,*

(*ii*) *Konstantensymbole c_i, $i \in I$,*

(*iii*) *logische Symbole $\neg, \wedge, \vee, \to, \leftrightarrow, \forall, \exists$,*

(*iv*) *das logische Relationssymbol $\doteq$, das stets die Identität bedeuten wird,*

(*v*) *die mathematischen Operationssymbole f_i^k, $i \in I_k$, $k \geq 1$,*

(*vi*) *die mathematischen $k-$ stelligen mathematischen Relationssymbolde R_j^k, $j \in J_k$, $k \geq 1$.*

Dabei sind I, I_k, J_k Indexmengen, die auch leer sein können. Diese Indexmengen bestimmen den Typ der Sprache wie zuvor den Typ einer Struktur. (Struktur und Sprache passen genau dann zusammen, wenn sie denselben Typ haben.)

Es folgen Definitionen und Beweise mit der Technik der Rekursion. Es handelt sich um Terme und Formeln, daher sprechen wir dann auch von 'Rekursion über den Termaufbau' bzw. 'Rekursion über den Formelaufbau', wenn wir allgemeine Aussagen über Terme bzw. Formeln beweisen oder neue allgemeine Definitionen von syntaktischen und später semantischen Grundbegriffen geben.

DEFINITION 3 (rekursive Definition der Terme einer Sprache L).

(*i*) *Jede Variable v_i und jedes Konstantensymbol c_i von L ist ein Term.*

(*ii*) *Wenn $t_1, ..., t_n$ Terme sind und f ein $n-$ stelliges Funktionssymbol von L, dann ist $ft_1...t_n$ ein Term.*

(*iii*) *Nur die Zeichenfolgen sind Terme, die nach endlich vielen Anwendungen von $(i), (ii)$ entstehen.*

Bemerkung: Wir schreiben Terme nicht nur in der hier definierten Form, sondern statt $+ * xyz$ auch wie allgemein üblich $(x * y) + z$ ($+, *$ sind zweistellige Operationssymbole). Es ist nur festzuhalten:

LEMMA 1. *Jeder Term ist eindeutig lesbar, d.h. er ist eine Variable oder Konstantensymbol oder eine Zeichenfolge $ft_1...t_n$ mit eindeutiger Folge von Termen $t_1, ..., t_n$ und einem $n-$ stelligen Funktionssymbol f.*

DEFINITION 4 (rekursive Definition der Formeln von L).

(i) Sind t_1 und t_2 Terme von L, so ist $\doteq t_1 t_2$ eine Formel von L,

(ii) Sind $t_1, ..., t_n$ Terme von L und P ein $n-$stelliges Relationssymbol von L, so ist $Pt_1...t_n$ eine Formel von L,

(iii) Sind α, β Formeln von L, x eine Variable von L, so sind auch Formeln von L :
$\neg\, \alpha,\ \wedge \alpha\beta,\ \vee \alpha\beta,\ \rightarrow \alpha\beta,\ \leftrightarrow \alpha\beta,\ \forall x\alpha,\ \exists x\alpha$

(iv) Nur die Zeichenfolgen sind Terme, die nach endlich vielen Anwendungen von $(i), (ii), (iii)$ entstehen.

Zusätzlich definiert man folgende wichtigen Klassen von Formeln: *Die Formeln gemäß $(i), (ii)$ heißen atomare Formeln. Eine Formel ohne $\forall, \exists$ heißt quantorenfrei. Eine Formel $\exists x_1 \exists x_2 ... \exists x_n \alpha$ mit quantorenfreier Formel α heißt **Existenzformel**, analog bildet man die **Allformeln** mit einem Block von Allquantoren vor einer quantorenfreien Formel.*

Bemerkungen:

1.) Wir schreiben wiederum in üblicherer Form: $\alpha \wedge \beta$, $\alpha \rightarrow \beta$ usw., ebenso $t_1 \doteq t_2$, ferner gern für zweistellige Relationssymbole wie $<$: $t_1 < t_2$ statt $< t_1 t_2$. Dann benötigen wir allerdings Klammern und verabreden wie üblich, dass $\neg, \exists x, \forall x$ am stärksten binden, dann $\wedge, \vee$ stärker binden als $\rightarrow, \leftrightarrow$.

2.) Man kann, wie wir aus mathematischer Erfahrung wissen, alle Formeln allein mit $\neg, \wedge, \forall$ bilden. Für Beweise über den Formelaufbau ist es dann bequemer, eine solche Beschränkung des Symbolvorrats vorzunehmen. Für die Lesbarkeit von Formeln ist indessen der größere Vorrat nützlich.

3.) Für Blöcke $\exists x_1 \exists x_2 ... \exists x_n$ von Quantoren schreibt man gern kürzer $\exists x_1 x_2 ... x_n$ oder sogar $\exists \overrightarrow{\mathbf{x}}$, analog für Blöcke von Allquantoren.

Analog zum Fall der Terme haben wir das

LEMMA 2. *Formeln sind eindeutig lesbar.*

Wir benötigen eine für den Begriff der formalen Ableitbarkeit und auch für die Semantik sehr wichtigen weiteren syntaktischen Grundbegriff:

DEFINITION 5 (Menge der in einer Formel vorkommenden freien Variablen). *Die Menge $Fr(\alpha)$ der in α vorkommenden freien Variablen ist rekursiv wie folgt definiert:*

Für eine atomare Formel α ist $Fr(\alpha)$ die Menge der in α vorkommenden Variablen,
$Fr(\exists x\alpha) = Fr(\alpha) \setminus \{x\},\ Fr(\forall x\alpha) = Fr(\alpha) \setminus \{x\},$
$Fr(\neg\, \alpha) = Fr(\alpha),\ Fr(\alpha \square \beta) = Fr(\alpha) \cup Fr(\beta)$ *für* $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

Beispiele: $\forall xPxyz \wedge Qxy$ hat die freien Variablen x, y, z, $\forall xPxyz$ hat die freien Variablen y, z, $\forall x \exists y Pxy$ hat überhaupt keine freien Variablen, ebenso hat $c_1 \doteq c_2$ keine freien Variablen. Sinn der Definition: Eine Variable ist genau dann frei in einer Formel, wenn sie sich nicht im Einflussbereich eines zugehörigen Quantors befindet.

DEFINITION 6. *Eine Formel α heißt Aussage genau dann, wenn $Fr(\alpha) = \varnothing$.*

Jeder Mensch mit etwas mathematischer Erfahrung benutzt: Aus einer allgemeingültigen Formel darf man jede Formel schließen, die durch Termeinsetzung für eine der freien Variablen entsteht, also schließt man aus

$$\forall x \forall y \forall z\, (x\,(y+z) = xy + xz)$$

auf

$$\forall y \forall z\, ((y+z)\,(y+z) = (y+z)\,y + (y+z)\,z)$$

und dann auf die bekannte binomische Formel. Der Vorgang heißt Termeinsetzung und wird rekursiv nach dem nunmehr bekannten Muster definiert:

DEFINITION 7 (Termeinsetzung in eine Formel für eine freie Variable, symbolisch $\alpha(x/t)$). *Zunächst definieren wir Termeinsetzung in einen Term: x, y seien Variablen, $t, t_1, ..., t_n$ Terme, c ein Konstantensymbol, f ein $n-$stelliges Operationssymbol, dann wird definiert:*

$$\begin{aligned} x[x/t] &= t, \\ y[x/t] &= y \text{ für } y \neq x, \\ c[x/t] &= c, \\ ft_1...t_n[x/t] &= ft_1[x/t]...t_n[x/t]. \end{aligned}$$

Daraus ergibt sich folgende Definition für die Einsetzung in eine Formel:

$$\begin{aligned} t_1 &\doteq t_2[x/t] = t_1[x/t] \doteq t_2[x/t] \\ Pt_1...t_n[x/t] &= Pt_1[x/t]...t_n[x/t], \\ &\neg \alpha[x/t] = \neg(\alpha[x/t]) \ ^*) \\ \alpha \wedge \beta[x/t] &= \alpha[x/t] \wedge \beta[x/t], \\ \forall x\alpha[x/t] &= \forall x\alpha, \\ \forall y\alpha[x/t] &= \forall y(\alpha[x/t]) \ ^*) \text{ für } y \neq x. \end{aligned}$$

Bemerkungen:

1. Offenbar wird damit die vertraute mathematische Operation formalisiert.

2. Zu *) : Gemeint ist für die Negation: Man entfernt das voranstehende Negationszeichen, bildet $\alpha[x/t]$ und setzt wieder das Negationszeichen voran. Es sollen nicht etwa Klammern eingefügt werden, wenn wir die klammerfreie Version wählen - ansonsten benötigt man Klammern bei Negationen wie $\neg(\alpha \wedge \beta)$ ohnehin. Für den Fall des Allquantors ist dieselbe Bemerkung anzubringen.

3. Es ist bereits bei der Termeinsetzung in Terme die Notwendigkeit der Setzung von Klammern um den eingesetzten Term zu beachten, wenn man nicht überhaupt die klammerfreie Version benutzt: Man betrachte

$$x * y(x/u + v) = (u + v) * y, \text{ nicht etwa } u + v * y \ (x, y, u, v \text{ Variablen}),$$

wohl aber

$$*xy[x/ + uv] = * + uvy,$$

hier entsteht keinerlei Notwendigkeit, Klammern einzuführen, das Beabsichtigte kommt automatisch heraus, wenn man das Symbol x einfach durch den Term $+uv$ ersetzt.

4. Analoge Definitionen sind für $\vee, \rightarrow, \longleftrightarrow$ und $\exists x\alpha$,$\exists y\alpha$ anzuführen.

3. Die semantischen Grundbegriffe

Die semantischen Grundbegriffe überhaupt sind: Interpretation eines Terms in einer Struktur unter einer Belegung h der Variablen und Interpretation einer Formel unter h. Dazu definieren wir zunächst den Begriff der Belegung:

DEFINITION 8. *Eine Belegung h der Variablen in einer Struktur $\mathcal{A}$ ist eine Abbildung $h : Var \rightarrow A$ der Menge aller Variablen in die Trägermenge A von $\mathcal{A}$. Im Folgenden wird noch benötigt: Ist h eine solche Belegung, x eine freie Variable und $a \in A$, dann ist*

$$h(x/a)$$

die Belegung h', welche auf $Var \setminus \{x\}$ mit h übereinstimmt und für die $h'(x) = a$ gilt.

DEFINITION 9 (Interpretation eines Terms in der Struktur $\mathcal{A}$ unter einer Belegung h, symbolisch $t^{\mathcal{A}}[h]$). *Diese Definition läuft wieder rekursiv über den Termaufbau:*

$$\begin{aligned} x^{\mathcal{A}}[h] &= h(x) \text{ für eine Variable } x, \\ c^{\mathcal{A}}[h] &= c^{\mathcal{A}} \text{ für ein Konstantensymbol } c, \\ (ft_1...t_n)^{\mathcal{A}}[h] &= (f)^{\mathcal{A}}\left(t_1^{\mathcal{A}}, ..., t_n^{\mathcal{A}}\right) \text{ für Terme } t_1, ..., t_n \text{ und ein } n-\text{stelliges Funktionssymbol } f. \end{aligned}$$

Sinn der Definition ist der: Wenn die Deutung der Variablen gegeben ist, so ist ein Term eindeutig durch ein Objekt der Trägermenge zu deuten, vorausgesetzt, die Sprache passt zur Struktur. Im mathematischen Umgangston sagt man dazu, man 'setze Objekte der Trägermenge für die Variablen ein', bilde z.B. x^y mit $x = 2$ und $y = 3$ und bekomme $2^3 = 8$. Man sollte sich aber klar machen, dass dies genau genommen ziemlicher Unsinn ist: Setzt man Objekte der Trägermenge in einen formalen Ausdruck für Variablen ein, so entsteht ein Unding, eine Folge, welche Symbole der Sprache und Objekte der mathematischen Welt in bunt durcheinander enthält und gar nichts Sinnvolles bedeutet. Gemeint ist vielmehr: Man setzt Konstantensymbole für die Variablen ein, erhält einen Term (im Sinne der oben stehenden formalen Definition!) und kann diesen Term eindeutig deuten durch ein Objekt der Trägermenge genau im Sinne der oben angeführten Definition, die nun allerdings insofern praktischer ist, als sie nicht für jedes ins Auge gefasste Objekt der Trägermenge ein Konstantensymbol einzuführt. Symbol und Bedeutung, Term und seine Bedeutung müssen hier genau auseinandergehalten werden.

Noch wichtiger und kritischer ist das Auseinanderhalten von einer Aussage einer formalen Sprache und ihrer Bedeutung im Sinne von 'wahr' oder 'falsch' in einer Struktur. In der mathematischen Umgangssprache fällt das manchmal nicht so sehr auf, zumal im konkreten Kontext. Man 'liest'

$$\forall x \forall y \forall z \, (x < y \wedge y < z \longrightarrow x < z)$$

wohl zumeist direkt als konkrete wahre Aussage und denkt dabei an die Ordnung in den reellen Zahlen. Aber bereits auf der Stufe des elementarsten axiomatischen Denkens nennt man eine beliebige Relation auf einer beliebigen Struktur, welche diese Eigenschaft besitzt, eine transitive Relation und wendet diesen Begriff völlig allgemein an. Man denke ferner an axiomatisch definierte Grundbegriffe wie 'Gruppe', 'Körper' usw. Tatsächlich ist es hier eine logische Voraussetzung, an welcher der ganze Sinn hängt, dass man unter Aussagen wie $\forall x \forall y \forall z \, (x < y \wedge y < z \longrightarrow x < z)$ rein formale Zeichenreihen versteht, also nicht etwa konkrete Behauptungen über eine Struktur. Vielmahr fragt man dann, in welchen Strukturen solche Aussagen gelten und welche allgemeinen Eigenschaften solche Strukturen haben. Wenn das im Laufe der mathematischen Erfahrung ohne die folgende präzise Definition durch allmähliche 'Infiltration' verstanden wird, so wird man am Ende (im glücklichen Fall) genau den Inhalt folgender präzisen Definition verstanden haben, meist wohl ohne eine solche angeben zu können:

DEFINITION 10 (Gültigkeit einer Formel α in einer Struktur $\mathcal{A}$ unter einer Belegung h der Variablen, symbolisch $\mathcal{A} \models \alpha[h]$). *Auch diese Definition wird wieder rekursiv über den Aufbau von α:*

$$\begin{array}{lll}
\mathcal{A} & \models & t_1 \doteq t_2[h] : \Longleftrightarrow \; t_1^{\mathcal{A}}[h] = t_2^{\mathcal{A}}[h], \\
\mathcal{A} & \models & Pt_1 ... t_n : \Longleftrightarrow \; \left(t_1^{\mathcal{A}}, ..., t_n^{\mathcal{A}}\right) \in P^{\mathcal{A}}, \\
\mathcal{A} & \models & \neg \, \alpha[h] : \Longleftrightarrow \; \textit{nicht } \mathcal{A} \models \alpha[h], \\
\mathcal{A} & \models & \alpha \wedge \beta[h] : \Longleftrightarrow \; \mathcal{A} \models \alpha[h] \textit{ und } \mathcal{A} \models \beta[h], \\
\mathcal{A} & \models & \exists x \alpha[h] : \Longleftrightarrow \; \textit{es gibt } a \in A : \mathcal{A} \models \alpha[h(x/a)], \\
\mathcal{A} & \models & \forall x \alpha[h] : \Longleftrightarrow \; \textit{für alle } a \in A : \mathcal{A} \models \alpha[h(x/a)].
\end{array}$$

Wir verallgemeinern noch für eine Menge Γ von Formeln:

$$\mathcal{A} \models \Gamma[h] : \Longleftrightarrow \; \mathcal{A} \models \gamma[h] \textit{ für alle } \gamma \in \Gamma.$$

Bemerkungen:

1. Die Definition ist für $\rightarrow, \leftrightarrow$ sinngemäß zu vervollständigen, indem man auf der rechten (mathemathisch umgangssprachlichen Seite!) die Bedeutungen $\Longrightarrow$, $\Longleftrightarrow$ einfügt. Ebenso steht im definitorischen $:\Longleftrightarrow$ die umgangssprachliche Symbolik.

2. Die Gültigkeit der Formel α in $\mathcal{A}$ unter h hängt natürlich nur von $h_{|Fr(\alpha)}$ ab. Daher schreibt man oft

$$\mathcal{A} \models \alpha[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}]$$

und meint damit die Belegung h, welche die Folge $\overrightarrow{\mathbf{x}}$ der freien Variablen von α mit der Folge $\overrightarrow{\mathbf{a}}$ von Elementen von A belegt. Daher hängt die Gültigkeit einer Aussage α, da sie gar keine freien Variablen hat, auch von keiner Belegung h ab, und wir schreiben dann

$$\mathcal{A} \models \alpha, \text{ falls } \alpha \text{ in } \mathcal{A} \text{ gültig ist, sonst verneinend } \mathcal{A} \not\models \alpha, \text{ was dasselbe beduetet wie} \mathcal{A} \models \neg \, \alpha.$$

Man beachte: Diese Beziehungen hat man nur bei Aussagen! Wir werden auch kürzer noch $\mathcal{A} \models \alpha[\overrightarrow{\mathbf{a}}]$ schreiben und damit meinen, dass ein zu $\overrightarrow{\mathbf{a}} \in A^n$ passender Vektor $\overrightarrow{\mathbf{x}}$ von freien Variablen in α mit $\overrightarrow{\mathbf{a}}$ belegt wird.

3. Man unterscheide die Bildung $\alpha[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}]$, die nur im Kontext mit $\mathcal{A} \models \alpha[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}]$ vorkommt, von der Bildung $\alpha[x/t]$: Letztere ist die rein syntaktische Termeinsetzung, eine neue Formel. $\alpha[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}]$ dagegen ist ein Paar aus einer Formel und einer Belegung. Allerdings haben die beiden doch eine enge Verbindung: $\alpha[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}]$ sieht fast (nicht ganz!) so aus, als hätte man formal für die Variablen $x_1, ..., x_n$ Konstanten eingesetzt, die der Reihe nach $a_1, ..., a_n$ bezeichnen. Die würden wir dann aber als $c_{a_1}, ..., c_{a_n}$ bezeichnen. Wenn wir nun die Struktur $\mathcal{A}$ um die Interpretationen dieser (neuen) Konstanten c_{a_i} durch die Elemente a_i ergänzen und diese erweiterte Struktur mit $\mathcal{A}'$ bezeichnen, dann haben wir:

$$\mathcal{A}' \models \alpha[x_1...x_n/c_{a_1}...c_{a_n}] \iff \mathcal{A} \models \alpha[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}].$$

Das ist auch der Grund dafür, dass man sich vielfach ohne Schaden leisten kann, von der Einsetzung von Elementen der Trägermenge für die freien Variablen einer Formel ungenau zu sprechen.

4. Man verallgemeinert noch für Formeln α mit freien Variablen:

$$\mathcal{A} \models \alpha : \iff \text{ für alle Belegungen } h \text{ gilt } \mathcal{A} \models \alpha[h].$$

Also hat man für $Fr(\alpha) = \{x_1, ..., x_n\}$:

$$\mathcal{A} \models \alpha : \iff \mathcal{A} \models \forall x_1...x_n \alpha.$$

Erläuterung zum Verständnis: Man sehe ein:

$$\begin{aligned} \langle \mathbb{R}, <^{\mathbb{R}} \rangle &\models v_1 < v_2[(v_1, v_2)\,/\,(0,1)], \\ \langle \mathbb{R}, <^{\mathbb{R}} \rangle &\not\models v_1 < v_2, \text{ aber auch } \langle \mathbb{R}, <^{\mathbb{R}} \rangle \not\models \neg\, v_1 < v_2, \\ \langle \mathbb{R}, 0^{\mathbb{R}}, 1^{\mathbb{R}}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, <^{\mathbb{R}} \rangle &\models \forall x\,(0 < x \vee 0 = x \leftrightarrow \exists y\,(x \doteq y \cdot y)). \end{aligned}$$

. Wir haben uns hier erlaubt, die bekannte Trägermenge der reellen Zahlen mit demselben Symbol zu bezeichnen wie die Struktur, weil es die Einführung von $\mathcal{R} := \langle \mathbb{R}, <^{\mathcal{R}} \rangle$ erspart und wohl nicht schadet. Späterhin werden wir auch in einer so bekannten oder frisch definierten Struktur im Rahmen einer Struktur wie $\langle A, +, < \rangle$ die oberen Indizes fortlassen, weil in den eckigen Klammern nur die Konstanten, Operationen, Relationen (also die üblichen mathematischen Gegenstände) stehen und keine Symbole. In Formeln der formalen Sprache kommen keine eckigen Klammern vor, so dass Verwechslungen ausgeschlossen sind.

Definition 11 (die Theorie einer Struktur, Modellklasse einer Aussagenmenge, elementare Äquivalenz). *Die Theorie einer Struktur ist die Menge der in dieser Struktur wahren Aussagen in der Sprache zu dieser Struktur. Also*

$$Th(\mathcal{A}) := \{\alpha |\, \alpha \text{ Aussage in der Sprache zu } \mathcal{A} \text{ und } \mathcal{A} \models \alpha\}.$$

Die Modellklasse der Aussagenmenge Γ in der Sprache L ist die Klasse aller Strukturen $\mathcal{A}$ zu L, in denen alle $\gamma \in \Gamma$ gelten. Also

$$\mathcal{A} \in Mod(\Gamma) : \iff \mathcal{A} \text{ ist Struktur zur Sprache von } \Gamma \text{ und } \mathcal{A} \models \Gamma.$$

Zwei Strukturen heißen elementar äquivalent, symbolisch $\mathcal{A} \equiv \mathcal{B}$, genau dann, wenn sie dieselben Aussagen der Logik erster Stufe erfüllen, also wenn $Th(\mathcal{A}) = Th(\mathcal{B})$.

Es folgt nunmehr der Begriff, der mittels der Relation $\mathcal{A} \models \alpha[h]$ aufgebaut ist und ohne Verwechslungsgefahr mit demselben Symbol bezeichnet wird:

Definition 12 (der semantische Folgerungsbegriff). *Aus einer Menge Γ von Formeln folgt die Formel α, symbolisch: Es gilt $\Gamma \models \alpha$ definitionsgemäß genau dann, wenn für jede Struktur $\mathcal{A}$ zur Sprache, in der Γ und α liegen, gilt:*

$$\text{Für alle } h\text{: Wenn } \mathcal{A} \models \Gamma[h], \text{ dann } \mathcal{A} \models \alpha[h].$$

*Insbesondere ist auch der Fall $\Gamma = \varnothing$ eingeschlossen, dann schreibt man auch $\models \alpha$, und das bedeutet die **logische Allgemeingültigkeit** von α, gleichwertig mit der logischen Allgemeingültigkeit von $\forall \overrightarrow{\mathbf{x}} \alpha$, wobei $\overrightarrow{\mathbf{x}}$ die Folge aller freien Variablen von α ist. (Eine gleichwertige Definition der Allgemeingültigkeit einer Formel folgt weiter unten.)*

Der Folgerungsbegriff interessiert in der Anwendung vor allem für Aussagen, dann hat man nichts mit Belegungen zu schaffen. Die Bedeutung des Begriffs erkennt man daran, dass es in der gesamten Mathematik stets um die Frage geht, welche Eigenschaften allgemein alle Strukturen einer Klasse haben, welche durch ein Axiomensystem Γ charakterisiert ist. Allerdings wollen wir hier zum zweiten Mal bemerken, dass einerseits nicht alle wichtigen Strukturklassen durch Axiomensysteme der Logik erster Stufe beschrieben werden können, ein wichtiges Beispiel bilden die topologischen Räume, ein weiteres die Noetherschen Ringe. Diese nehmen Bezug auf alle Teilmengen der Trägermengen, welche gewisse Eigenschaften haben, enthalten also Quantifikation über Teilmengen. Andererseits spielt sich die **gesamte** Mathematik im Rahmen der Mengenlehre im üblichen ZFC-Sytem ab ('Zermelo-Fraenkel mit Auswahlaxiom', dies System wird später ausführlich eingeführt), das wiederum in der Logik erster Stufe formuliert ist.

Bemerkung zum Folgerungsbegriff - eine Warnung: Die üblichsten mathematischen Axiome haben die Form $\forall \vec{\mathbf{x}} \alpha$ mit quantorenfreiem α, das gewöhnlich nur eine Gleichung ist. Nun lässt man bequem die Allquantoren weg und meint immer noch die Allaussage. Gemäß dieser Praxis folgt $t_1 \doteq t_2\,[x/t]$ aus $t_1 \doteq t_2$, für alle Variablen x und alle Terme t. Wir haben einen viel allgemeineren Rahmen, in dem dieser Brauch keineswegs naheliegt und größte Verwirrung anrichtet: So wird man aus $x < y$ sicher nicht schließen wollen, dass $x < x$ (was diesem Brauch exakt entspricht). Hier ist der Folgerungsbegriff gerade so angelegt, dass dieselbe Belegung durchgezogen wird.

Ein prinzipielles Problem des Folgerungsbegriffes: Wie kann man überhaupt eine Folgerung als solche erkennen, es ist doch völlig unmöglich, alle erdenklichen Strukturen durchzuprüfen, jedenfalls dann, wenn es solche mit unendlicher Trägermenge sind oder auch nur mit beliebig großen endlichen Trägermengen? Die Antwort ist aus mathematischer Praxis wohlbekannt: Tatsächlich benutzt man über weite Strecken ein formales Schließen, mit dem man in syntaktisch-kombinatorischer Weise aus endlich vielen Formeln von Γ nach formalen Regeln die Formel α erzeugt, um $\Gamma \models \alpha$ zu beweisen. Wir werden im nächsten Abschnitt genau einsehen, worauf sich so etwas gründet. Aber dann stellt sich ein neues Problem, ob man alle Folgerungen so bekommt - und diese Frage wird dann positiv beantwortet für die Prädikatenlogik erster Stufe. Doch auch der semantische Folgerungsbegriff hat als solcher seinen Wert bereits stark im 19. Jahrhundert erwiesen, er ist sehr effizient, wenn es darum geht, zu zeigen, dass eine Aussage α aus einer Menge Γ von Aussagen eben **nicht folgt**: Dann genügt es, eine einzige Struktur $\mathcal{A}$ zu konstruieren, in welcher alle $\gamma \in \Gamma$ gelten, die Aussage α aber eben nicht. So konnte man zeigen, dass das Parallelenaxiom der Euklidischen Geometrie nicht aus den übrigen folgt. Da hilft nun wieder das formale Schließen gar nichts: Hat man beliebig viele (aber notwendig nur endlich viele) solcher formalen Beweise angefangen und misslangen sie alle, dann besagt das noch gar nichts darüber, ob nicht doch ein solcher Beweis möglich wäre. (Auch diese Aussage werden wir mathematisch genau formulieren und beweisen!) Bei Problemen dieser Art ist der semantische Folgerungbegriff also dem Begriff des formalen Ableitens gänzlich überlegen. Natürlich brauchen solche Gegenbeispiel-Konstruktionen unter Umständen geniale Gedanken, aber man weiß jedenfalls, was zu tun ist.

An den Begriff der Folgerung schließen sich noch zwei naheliegende Definitionen an, deren Inhalte auch bereits von Beispielen her bekannt sein dürften:

DEFINITION 13 (Allgemeingültigkeit und Erfüllbarkeit von Formeln). *Eine Formel α heißt **allgemeingültig**, wenn*

$$\mathcal{A} \models \alpha[h] \text{ für alle Strukturen } \mathcal{A} \text{ zur Sprache von } \alpha \text{ und alle Belegungen } h.$$

Eine Formel α heißt erfüllbar, wenn es eine Struktur $\mathcal{A}$ und eine Belegung h über $\mathcal{A}$ gibt, so dass

$$\mathcal{A} \models \alpha[h].$$

Man dehnt diese Definitionen auch auf Mengen von Formeln aus: Eine Menge von Formeln Γ heißt allgemeingültig, wenn alle Formeln in Γ es sind. Eine Menge Γ von Formeln heißt erfüllbar oder (semantisch) konsistent, wenn es eine Struktur $\mathcal{A}$ und eine Belegung h über $\mathcal{A}$ gibt, so dass

$$\mathcal{A} \models \gamma[h] \text{ für alle } \gamma \in \Gamma.$$

Zum Verständnis der Definitionen zeige man folgende kleinen Beobachtungen:

1. α ist genau dann allgemeingültig, wenn $\neg \alpha$ nicht erfüllbar ist.
2. α ist genau dann allgemeingültig, wenn $\varnothing \models \alpha$.
3. $\Gamma \not\models \alpha$ genau dann, wenn $\Gamma \cup \{\neg \alpha\}$ erfüllbar ist.
4. Die Aussage: 'Γ ist erfüllbar' ist nicht gleichwertig mit: Alle $\gamma \in \Gamma$ sind erfüllbar.

Aus jedem mathematischen Grundstudium kennt man eine Fülle von logisch allgemeingültigen Formeln, Beispiele sind aussagenlogische Tautologien wie $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$, aber auch identitätslogische allgemeingültige Aussagen wie $\forall x \forall y \forall u \forall v\,(u \doteq x \wedge v \doteq y \to (Pxy \to Puv))$ oder auch wichtige logisch allgemeingültige Aussagen, die mit dem Quantorengebrauch zusammenhängen, wie $\forall x \alpha \to \neg \exists x \neg \alpha$. Systematisch wird logische Allgemeingültigkeit für Formeln der Prädikatenlogik 1. Stufe unter anderem in den nächsten beiden Abschnitten untersucht.

DEFINITION 14. *Eine Menge Γ von Aussagen heißt* ***vollständig****, wenn für jede Aussage α der Sprache von Γ gilt:*

$$\Gamma \models \alpha \text{ oder } \Gamma \not\models \neg \alpha.$$

Sonst heißt die Menge Γ unvollständig.

Substantielle mathematische Beispiele, später erst einzusehen:

1. Sei Γ die Menge der Axiome für die algebraisch abgeschlossenen Körper der Charakteristik 0. Dann gilt für jede Aussage α der Sprache der Körper: $\Gamma \models \alpha$ oder $\Gamma \not\models \alpha$. Γ ist also vollständig.

2. Aus den sonstigen Axiomen der Mengenlehre folgt weder das Auswahlaxiom noch seine Verneinung. Die Mengenlehre ist also unvollständig, und mehr noch: Eine 'vernünftige' vollständige Axiomatisierung, also konsistent und mit effektiv 'aufschreibbarer' Menge von Axiomen, kann es für die Mengenlehre nicht geben (einer der Gödelschen Sätze).

Ein banales Beispiel vollständiger Mengen hat man natürlich mit widersprüchlichen (synonym: inkonsistenten) Mengen von Aussagen, die überhaupt kein Modell haben.

Zum Abschluss beweisen wir mit der Technik der Rekursion über den Formelaufbau einen elementaren Satz. Bekanntlich sind zwei Strukturen (desselben Typs) isomorph, wenn es einen Isomorphismus zwischen ihnen gibt, wir definieren das genau für den ganz allgemeinen Fall:

DEFINITION 15 (Isomorphismus, Relation der Isomorphie). *Hat man zwei Strukturen $\mathcal{A}$, $\mathcal{B}$ desselben Typs, so ist ein Isomorphismus eine Bijektion f der Trägermenge A von $\mathcal{A}$ auf die Trägermenge B von $\mathcal{B}$, so dass*

$$\mathcal{A} \models \alpha[h] \iff \mathcal{B} \models \alpha[f \circ h] \text{ für alle atomaren Formeln } \alpha.$$

Wir sagen $\mathcal{A} \simeq \mathcal{B}$ ($\mathcal{A}$ ist isomorph zu $\mathcal{B}$) genau dann, wenn es einen Isomorphismus von $\mathcal{A}$ auf $\mathcal{B}$ gibt. (Die Umkehrabbildung ist dann auch ein Isomorphismus von $\mathcal{B}$ auf $\mathcal{A}$.)

Isomorphe Strukturen sind offenbar mathematisch genau gleich, sie sind ununterscheidbar.

Beispiele: Der Körper $\langle \mathbb{R}, 0, 1, +, \cdot \rangle$ ist nicht isomorph zum Körper $\langle \mathbb{C}, 0, 1, +, \cdot \rangle$. (Warum das so ist, wird gleich begründet.) Die Gruppe $\langle \mathbb{R}_+, 1, \cdot \rangle$ ist isomorph zur Gruppe $\langle \mathbb{R}, 0, + \rangle$ mit dem bekannten Isomorphismus ln.

Wie zeigt man, dass zwei Strukturen nicht isomorph sind? Typisch sucht man eine Aussage, die in der einen gilt, in der anderen nicht, man zeigt also, dass sie nicht elementar äquivalent sind. (Übrigens reicht auch eine Aussage der Logik höherer Stufe, in deren Erfüllung sich beide unterscheiden.) Zur Rechtfertigung dieses Verfahrens beweisen wir folgenden

SATZ 1. *Zwei isomorphe Strukturen sind elementar äquivalent.*

Beweis: Es ist hier bequemer, allgemeiner zu zeigen: Für alle Formeln $\alpha\left(\overrightarrow{\mathbf{x}}\right)$ und alle $\overrightarrow{\mathbf{a}}$ von Elementen von A gilt:

$$(*)\ \mathcal{A} \models \alpha\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \iff \mathcal{B} \models \alpha\left[\overrightarrow{\mathbf{x}}/f\left(\overrightarrow{\mathbf{a}}\right)\right],$$

wenn f ein Isomorphismus von $\mathcal{A}$ auf $\mathcal{B}$ ist. Denn diese Aussage kann man rekursiv über den Formelaufbau beweisen. Der Induktionsanfang, die Gültigkeit für atomare Formeln, steckt in der Definition des Isomorphismus. Nun sei $\beta = \neg \alpha$, und für α gelte die Aussage bereits. Dann hat man

$$\mathcal{A} \models \neg \alpha\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \iff \text{nicht } \mathcal{A} \models \alpha\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \iff_{I.-V.} \text{nicht } \mathcal{B} \models \alpha\left[\overrightarrow{\mathbf{x}}/f(\overrightarrow{\mathbf{a}})\right] \iff \mathcal{B} \models \neg \alpha\left[\overrightarrow{\mathbf{x}}, f\left(\overrightarrow{\mathbf{a}}\right)\right].$$

Ebenso

$$\begin{aligned} \mathcal{A} \quad \models \quad & \alpha \wedge \beta\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \iff \mathcal{A} \models \alpha\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \text{ und } \mathcal{A} \models \beta\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \\ \iff \quad & {}_{I.-V.}\ \mathcal{B} \models \alpha\left[\overrightarrow{\mathbf{x}}/f(\overrightarrow{\mathbf{a}})\right] \text{ und } \mathcal{B} \models \beta\left[\overrightarrow{\mathbf{x}}/f(\overrightarrow{\mathbf{a}})\right] \\ \iff \quad & \mathcal{B} \models \alpha \wedge \beta\left[\overrightarrow{\mathbf{x}}, f\left(\overrightarrow{\mathbf{a}}\right)\right]. \end{aligned}$$

Ferner für $y \in Fr(\alpha)$:

$$\begin{aligned}\mathcal{A} \quad &\models \quad \forall y\alpha\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \iff \text{für alle } a \in A : \mathcal{A} \models \alpha\left[y/a, \overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \\ &\iff \quad {}_{I.-V.}\ \text{für alle } a \in A : \mathcal{B} \models \alpha\left[y/f(a), \overrightarrow{\mathbf{x}}/f(\overrightarrow{\mathbf{a}})\right] \\ &\iff \quad {}_{*}\ \text{für alle } b \in B : \mathcal{B} \models \alpha\left[y/b, \overrightarrow{\mathbf{x}}/f(\overrightarrow{\mathbf{a}})\right] \ (^*) : f \text{ surjektiv!})\end{aligned}$$

Schließlich für $y \notin Fr(\alpha)$:

$$\begin{aligned}\mathcal{A} \quad &\models \quad \forall y\alpha\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \iff {}_{*}\ \mathcal{A} \models \alpha\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{a}}\right] \iff {}_{I.-V.}\ \mathcal{B} \models \alpha\left[\overrightarrow{\mathbf{x}}/f(\overrightarrow{\mathbf{a}})\right] \\ &\iff \quad {}_{*}\ \mathcal{B} \models \forall y\alpha\left[\overrightarrow{\mathbf{x}}/f(\overrightarrow{\mathbf{a}})\right] \ (^*) : y \notin Fr(\alpha)\ ).\blacksquare\end{aligned}$$

Damit ist der Satz bewiesen durch einfaches 'rekursives Hochziehen', was der Standardbeweis ist für derartige Aussagen. Wir haben wieder mit der sprachlichen Minimalausstattung gearbeitet und müssen daher nicht völlig Analoges wiederholen.

Bemerkungen: Völlig analog kann man zeigen, dass zwei isomorphe Strukturen auch dieselben Aussagen höherer Stufe als der ersten erfüllen, also dieselben überhaupt erdenklich *formulierbaren* Eigenschaften haben. Indessen ist die Umkehrung nicht richtig: Zwei Strukturen, welche elementar äquivalent sind, müssen keineswegs isomorph sein, damit ist im Gegenteil kaum je zu rechnen. Die einzige wesentliche Ausnahme bilden Strukturen mit endlicher Trägermenge. Bei ihnen folgt Isomorphie aus elementarer Äquivalenz. Wir geben für den Sachverhalt bei unendlichen Strukturen nichttriviale

Beispiele: Zwei algebraisch abgeschlossene Körper der Charakteristik Null sind stets elementar äquivalent, aber z.B. sind der Körper $\mathbb{C}$ und der Körper der algebraischen Zahlen (über $\mathbb{Q}$, also der algebraische Abschluss von $\mathbb{Q}$) nicht isomorph. Zwei Ordnungsstrukturen mit dichter Ordnung ohne erstes und letztes Element sind ebenfalls elementar äquivalent, aber natürlich sind $\langle \mathbb{R}, < \rangle$ und $\langle \mathbb{Q}, < \rangle$ nicht isomorph. In diesen Beispielen ist die Nichtexistenz eines Isomorphismus jeweils trivial (Kardinalzahlgründe), aber die elementare Äquivalenz ist nichttrivial und kann erst später eingesehen werden. Aber man findet auch jeweils Beispiele derselben Kardinalzahl für beide vollständigen Theorien, welche nicht isomorph sind. Z. B. können sich abzählbare algebraisch abgeschlossene Körper in ihrem Transzendenzgrad über $\mathbb{Q}$ unterscheiden und sind dann nicht isomorph.

4. Der syntaktische Ableitungsbegriff

Wir wollen einen formalen Ableitungsbegriff haben mit folgenden Eigenschaften: $\Gamma \vdash \alpha$ gilt für eine Menge Γ von Formeln und eine Formel α nur dann, wenn $\Gamma \models \alpha$, das nennt man die Korrektheit des Ableitungsbegriffs oder Ableitungskalküls. Ferner soll der Begriff der Ableitung finit sein, also $\Gamma \vdash \alpha$ genau dann, wenn α am Ende einer 'Beweisfolge aus Γ' steht, das ist nach Definition eine endliche Folge von Formeln, in welcher jede Formel ein logisches Axiom oder eine Formel von Γ ist oder aus einer / zweien der vorangehenden Formeln mittels einer der logischen Ableitungsregeln erzeugt wird. Schließlich soll von einem Computerprogramm entschieden werden können, ob eine Folge von Formeln eine korrekt gebildete Beweisfolge ist. Dies Unternehmen kann z.B. auf folgende Weise realisiert werden:

Zunächst benötigen wir eine technische

Definition 16. *Die Variable x ist frei für den Term t in der Formel α genau dann, wenn keine Variable von t in α gebunden vorkommt.*

Beispiel: In der Formel $\alpha = \forall x\,(x \doteq y)$ kommt y frei vor, aber nicht frei für x. Die Konsequenz ist die, dass man aus $\alpha\,[y/x] = \forall x\,(x \doteq x)$ (was offenbar logisch allgemeingültig ist) nicht korrekt schließen kann auf $\exists y \forall x\,(x \doteq y) = \exists y \alpha$ (diese Aussage besagt, dass die Trägermenge nur ein Element besitzt). Wir wollen aber logisch korrekte Axiome der Form $\alpha\,[y/t] \to \exists y \alpha$ haben. Dann müssen wir offenbar das freie Vorkommen von y für t verlangen.

Definition 17. *Eine Formel α ist genau dann ein **logisches Axiom**, wenn sie von einer der folgenden Arten ist:*

(i) *α ist aussagenlogische Tautologie,*

d.h. α entsteht aus einer aussagenlogisch wahren Formel $f(p_1,...,p_n)$ mit Aussagenvariablen $p_1,...,p_n$ durch Einsetzen von beliebigen Formeln für die $p_1,...,p_n$.

(ii) α ist eines der folgenden Gleichheitsaxiome :

$$\forall x\,(x \doteq x)$$

$$\forall x \forall y\,(x \doteq y \longrightarrow y \doteq x)$$

$$\forall x \forall y \forall z\,(x \doteq y \wedge y \doteq z \longrightarrow x \doteq z)$$

$$\forall x_1...x_n \forall y_1...y_n \left(\bigwedge_{i=1}^{n} x_i \doteq y_i \longrightarrow f x_1...x_n = f y_1...y_n \right)$$

$$\forall x_1...x_n \forall y_1...y_n \left(\bigwedge_{i=1}^{n} x_i \doteq y_i \longrightarrow (P x_1...x_n \longrightarrow P y_1...y_n) \right)$$

Erklärung: Die ersten drei Axiome drücken aus, dass Gleichheit eine Äquivalenzrelation aus, die letzten beiden drücken aus, dass sie auch bezüglich aller Operationen und Relationen eine Kongruenzrelation ist. Es folgen Axiome für die Quantoren:

$$\begin{array}{lrcl}
(iii) & \alpha[x/t] & \longrightarrow & \exists x\alpha, \text{ wenn } x \text{ frei für } t \text{ in } \alpha \text{ (Existenzquantor und Termeinsetzung)} \\
(iv) & (\alpha \longrightarrow \beta) & \longrightarrow & (\exists x\alpha \longrightarrow \beta), \text{ wenn } x \text{ nicht frei in } \beta \text{ (Existenzeinführung vorn)} \\
(v) & \forall x\alpha & \longrightarrow & \alpha[x/t], \text{ wenn } x \text{ frei für } t \text{ in } \alpha \text{ (Allquantor und Termeinsetzung)} \\
(vi) & (\alpha \longrightarrow \beta) & \longrightarrow & (\alpha \longrightarrow \forall x\beta), \text{ wenn } x \text{ nicht frei in } \alpha \text{ (Alleinführung hinten).}
\end{array}$$

Definition 18. *Die einzige logischen Ableitungsregel ist:*

$$\textit{(Modus-Ponens-Regel)} \quad \frac{\alpha \longrightarrow \beta \qquad \alpha}{\beta}$$

Bemerkung: Manchmal kann es bequem sein, nur mit dem Existenzquantor und also auch nur mit den dazu gehörigen Axiomen und Regeln zu arbeiten. Dann fasst man $\forall x\alpha$ nur als Abkürzung für $\neg \exists x \neg \alpha$ auf.

Wir kommen nun zur oben bereits angekündigten Formulierung des Beweisbarkeitsbegriffs:

Definition 19. *Die Formel α heißt aus der Formelmenge Γ beweisbar, symbolisch $\Gamma \vdash \alpha$, wenn es eine endliche Folge $\alpha_1,...,\alpha_n = \alpha$ von Formeln gibt, so dass für jede Formel α_i der Folge gilt: α_i ist aus Γ, oder α_i ist ein logisches Axiom (gemäß obenstehender Definition), oder α_i entsteht aus α_j, α_k mit $j,k < i$ durch Anwenden der Modus-Ponens-Regel.*

Bemerkung: Speziell für die leere Menge Γ heißt α einfach 'beweisbar' oder auch kompletter 'aus der leeren Menge beweisbar'.

Für das Folgende brauchen wir noch folgende beiden Lemmata:

Lemma 3. *Man hat $\Gamma \vdash \alpha$ genau dann, wenn es endlich viele Formeln $\gamma_1,...,\gamma_n \in \Gamma$ gibt, so dass $\vdash \gamma_1 \wedge ... \wedge \gamma_n \to \alpha$.*

Beweis: Aus einem Beweis für $\gamma_1 \wedge ... \wedge \gamma_n \to \alpha$ aus der leeren Menge macht man durch Anhängen der Folge $\gamma_1,...,\gamma_n$ sofort unter Nutzung der Tautologie

$$(\gamma_1 \wedge ... \wedge \gamma_n \to \alpha) \leftrightarrow (\gamma_1 \to (\gamma_2 \wedge ... \wedge \gamma_n \to \alpha)),$$

einen Beweis für $\gamma_2 \wedge ... \wedge \gamma_n \to \alpha$ aus γ_1. Nun fährt man fort mit

$$(\gamma_2 \wedge ... \wedge \gamma_n \to \alpha) \leftrightarrow (\gamma_2 \to (\gamma_3 \wedge ... \wedge \gamma_n \to \alpha))),$$

bekommt einen Beweis von

$$\gamma_3 \wedge ... \wedge \gamma_n \to \alpha$$

aus γ_1, γ_2. So fährt man fort und gewinnt einen Beweis von α aus $\gamma_1,...,\gamma_n$. Umgekehrt sei ein Beweis für α aus Γ gegeben, in dem die Regel, dass in der Beweisfolge ein Element aus Γ einfach hingeschrieben werden kann, genau für $\gamma_1,...,\gamma_n$ benutzt wird. Dann kann man die gesamte Beweisfolge $\alpha_1,...,\alpha_n = \alpha$ zu einer Beweisfolge für $\gamma_1 \wedge ... \wedge \gamma_n \to \alpha$ aus der leeren Menge machen, indem man bildet: $\beta_1,...,\beta_n$ mit

$\beta_k = \gamma_1 \wedge ... \wedge \gamma_n \to \alpha_k$, $1 \leq k \leq n$. Das ist genau genommen noch nicht ganz eine Beweisfolge aus der leeren Menge, kann aber mit aussagenlogischen Tautologien und Modus Ponens zu einer solchen ergänzt werden, das geht im Einzelnen so:

Wenn $\alpha_k = \gamma_j$, dann ist $\gamma_j \to \alpha_k$ aussagenlogisches Axiom.

Wenn α_k aussagenlogisches Axiom ist, so gilt das auch für $\beta_k = \gamma_1 \wedge ... \wedge \gamma_n \to \alpha_k$.

Wenn α_k eines der anderen Axiome ist wie Identitätsaxiom oder Axiom für die Quantoren, so ist α_k im ursprünglichen Beweis durch folgende Kette von drei Formeln zu ersetzen:

$$\begin{aligned} &\alpha_k \ \to \ (\gamma_1 \wedge ... \wedge \gamma_n \to \alpha_k) \ \text{(aussagenlog. Axiom)} \\ &\alpha_k \\ &\gamma_1 \wedge ... \wedge \gamma_n \ \to \ \alpha_k. \end{aligned}$$

Wenn α_k in der ursprünglichen Beweisfolge durch Modus Ponens entstand, also mit $i < k$ und $j < k$ und

$$\alpha_j = \alpha_i \ \to \ \alpha_k :$$

j

$$\begin{aligned} &\alpha_i \ \to \ \alpha_k \\ &\alpha_i \\ &\alpha_k, \end{aligned}$$

dann können wir nach Induktionsvoraussetzung (Induktion über die Länge des ursprünglichen Beweises) bereits annehmen, dass wir (aus der leeren Menge) beweisen können:

$$\begin{aligned} &\gamma_1 \wedge ... \wedge \gamma_n \ \to \ \left(\alpha_i \ \to \ \alpha_k\right), \\ &\gamma_1 \wedge ... \wedge \gamma_n \ \to \ \alpha_i. \end{aligned}$$

Wir schreiben nun kurz γ^* für $\gamma_1 \wedge ... \wedge \gamma_n$. Nun ersetzen wir die Zeile α_k (die dritte oben) durch:

$$\begin{aligned} &(\gamma^* \to \alpha_i) \to ((\gamma^* \to (\alpha_i \to \alpha_k)) \to (\gamma^* \to \alpha_k)) \quad \text{(aussagenlog. Axiom)} \\ &\gamma^* \to \alpha_i \quad \text{(liegt bereits vor)} \\ &(\gamma^* \to (\alpha_i \to \alpha_k)) \to (\gamma^* \to \alpha_k) \quad \text{(Modus Ponens)} \\ &(\gamma^* \to (\alpha_i \to \alpha_k)) \quad \text{(liegt bereits vor)} \\ &\gamma^* \to \alpha_k \quad \text{(Modus Ponens).}\blacksquare \end{aligned}$$

LEMMA 4. *Wenn* $\vdash \alpha(c_1, ..., c_n)$, *dann* $\vdash \forall x_1 ... \forall x_n \alpha(x_1, ..., x_n)$.

Beweis: Aus einem Beweis für $\alpha(c_1, ..., c_n)$ bekommt man sofort einen Beweis für $\alpha(x_1, ..., x_n)$, indem man die Konstantensymbole c_i durch *neue* freie Variablen $x_1, ..., x_n$ ersetzt, die in $\alpha(c_1, ..., c_n)$ und allen Formeln des vorgelegten Beweises für $\alpha(c_1, ..., c_n)$ nicht vorkommen. Dann kann man mit Aussagenlogik $\forall x(x \doteq x) \to \alpha(x_1, ..., x_n)$ bekommen und nun der Reihe nach mit der Alleinführungsaxiom und Modus-Ponens-Regel die Quantoren $\forall x_i$ einführen. Dann hat man $\forall x(x \doteq x) \to \forall x_1 ... \forall x_n \alpha(x_1, ..., x_n)$ und kann nunmehr aus dem Axiom $\forall x(x \doteq x)$ mit Modus Ponens die gewünschte Formel $\forall x_1 ... \forall x_n \alpha(x_1, ..., x_n)$ erhalten. Es sei bemerkt, dass man auch aus den Alleinführungsaxiomen und Modus Ponens die abgeleitete Regel

$$\begin{aligned} \alpha \ &\to \ \beta \\ \alpha \ &\to \ \forall x \beta, \ \text{wenn } x \text{ nicht frei in } \alpha \end{aligned}$$

erhält und dann direkt in $\forall x(x \doteq x) \to \alpha(x_1, ..., x_n)$ die Allquantoren hinten einführen kann. Modus Ponens ergibt dann wieder das Resultat.$\blacksquare$

5. Der Vollständigkeitssatz und Folgerungen daraus

Wir wollen nunmehr auf folgende beiden Sätze hinaus - der erste ist einfach, der zweite raffiniert zu beweisen:

SATZ 2 (Korrektheit des logischen Kalküls). *Für jede Menge* Γ *von Formeln und jede Formel* α *gilt: Wenn* $\Gamma \vdash \alpha$, *dann* $\Gamma \models \alpha$. *Das heißt: Die logischen Axiome und Regeln sind allgemeingültig.*

SATZ 1 (Vollständigkeit des logischen Kalküls). *Für jede Menge* Γ *von Formeln und jede Formel* α *gilt: Wenn* $\Gamma \models \alpha$, *dann* $\Gamma \vdash \alpha$. *Das heißt: Der Ableitungskalkül liefert alle Folgerungen. Zusammen mit der Korrektheit hat man also die volle Äquivalenz von syntaktischem Ableitungsbegriff und semantischem Folgerungsbegriff.*

Beweis der Korrektheit: Dazu nimmt man sich die einzelnen Axiome vor und zeigt, dass sie in jeder Struktur gültig sind. Das ist klar für die aussagenlogischen Tautologien und auch für die Identitätsaxiome (Identität ist eben eine Kongruenzrelation für jede Struktur, bezüglich aller Relationen und Operationen). Nun zeigen wir beispielhaft, dass die Existenzaxiome und die Axiome der vorderen Existenzeinführung korrekt sind, d.h. für jede Struktur gültig, unter jeder Belegung der freien Variablen: Aus

$$\mathcal{A} \models \alpha[x/t][h]$$

folgt mit x frei für $t = t(\overrightarrow{\mathbf{u}})$, wobei $\overrightarrow{\mathbf{u}}$ die Folge der (freien) Variablen von t sein soll, dass

$$\mathcal{A} \models \alpha[x/t][\overrightarrow{\mathbf{z}}/\overrightarrow{\mathbf{a}}, \overrightarrow{\mathbf{y}}/\overrightarrow{\mathbf{b}}],$$

und dabei sei $\overrightarrow{\mathbf{y}}$ die Folge der freien Variablen von α ohne x, $\overrightarrow{\mathbf{z}}$ die Folge der freien Variablen von t ohne die von $\overrightarrow{\mathbf{y}}$. Weiter sei h die Belegung, die $\overrightarrow{\mathbf{y}}$ mit $\overrightarrow{\mathbf{b}}$ belegt und $\overrightarrow{\mathbf{z}}$ durch $\overrightarrow{\mathbf{a}}$. Es folgt

$$\mathcal{A} \models \exists x \alpha[\overrightarrow{\mathbf{y}}/\overrightarrow{\mathbf{b}}].$$

Da die x, $\overrightarrow{\mathbf{z}}$ nicht in $\exists x\alpha$ vorkommen, gilt damit auch

$$\mathcal{A} \models \exists x \alpha[h].$$

Also gilt in jeder Struktur $\mathcal{A}$ zur Sprache, in der α und $\alpha[x/t]$ liegen: $\mathcal{A} \models \alpha[x/t] \to \exists x\alpha$, wenn nur x frei für t in α ist.

Ferner hat man mit $\mathcal{A} \models \alpha \to \beta[h]$ auch $\mathcal{A} \models \exists x\alpha \to \beta[h]$, wenn x nicht frei in β vorkommt. Denn mit $\mathcal{A} \models \alpha \to \beta[h]$ gilt: Wenn $\mathcal{A} \models \alpha[h]$, so $\mathcal{A} \models \beta[h]$. Nun gelte $\mathcal{A} \models \exists x\alpha[h]$. Dann hat man mit einem Element $a \in A$, dass $\mathcal{A} \models \alpha[h\,(x/a)]$. Es folgt $\mathcal{A} \models \beta[h\,(x/a)]$ nach Voraussetzung. Aber da x nicht frei in β vorkommt, gilt auch $\mathcal{A} \models \beta[h]$, da für die Gültigkeit von β in $\mathcal{A}$ unter einer Belegung die Belegung von x irrelevant ist. Völlig analog verläuft die Sache für den Umgang mit dem Allquantor.■

Bevor wir zum Beweis der Vollständigkeit kommen, wollen wir die Idee dazu beschreiben:

Idee des Vollständigkeitsbeweises: Zunächst legt man sich zurecht:

LEMMA 5. *Wenn jede syntaktisch widerspruchsfreie Menge* Γ *von Formeln (das heißt* $\Gamma \nvdash \beta \wedge \neg\beta$ *für bel.* β *oder auch nur eines) ein Modell hat (also eine Struktur* $\mathcal{A}$ *mit* $\mathcal{A} \models \Gamma[h]$ *für eine Belegung* h*), dann ist der Ableitungskalkül vollständig.*

Beweis: Wenn $\Gamma \nvdash \alpha$, dann ist $\Gamma \cup \{\neg\alpha\}$ widerspruchsfrei, sonst hätte man sofort $\Gamma \vdash \alpha$, weil man aus $\Gamma \vdash \neg\alpha \to \alpha$ und $\Gamma \vdash \alpha \to \alpha$ auf $\Gamma \vdash \alpha$ schließen kann. Nun habe die widerspruchsfreie Menge $\Gamma \cup \{\neg\alpha\}$ ein Modell $\mathcal{A}$, so dass also $\mathcal{A} \models \Gamma \cup \{\neg\alpha\}\,[h]$. Damit $\mathcal{A} \models \Gamma[h]$, aber nicht $\mathcal{A} \models \alpha[h]$, somit $\Gamma \not\models \alpha$. Aus $\Gamma \nvdash \alpha \implies \Gamma \not\models \alpha$ folgt wiederum $\Gamma \models \alpha \implies \Gamma \vdash \alpha$.■

Es genügt also zu beweisen: Jede syntaktisch widerspruchsfreie Menge von Formeln hat ein Modell. Hier nun ist die eigentliche Idee vonnöten: Wie soll man zu Aussagen, die über beliebige Strukturen reden, welche man gar nicht kennt und auch niemals alle kennen kann, ein Modell konstruieren? Man hat dafür zu viele Möglichkeiten, um das allgemein zu machen. Nun die Idee: Vervollständige eine syntaktisch widerspruchsfreie Menge Γ zu Δ so, dass gar keine Wahl mehr bleibt, also für jede Formel α gilt: Entweder $\alpha \in \Delta$ oder $\neg\alpha \in \Delta$. Zweite Idee: Nimm die Menge der Variablen (und Konstanten) der Sprache selbst als Trägermenge. Dann definiere die Operationen und Relationen so:

$$\begin{aligned} (t_1, ..., t_n) \quad &\in \quad P^{\mathcal{A}} : \Longleftrightarrow\ Pt_1...t_n \in \Delta \text{ für atomare Terme } t_1...t_n, \\ f^{\mathcal{A}}(t_1, ..., t_n) \quad &= \quad s : \Longleftrightarrow\ ft_1...t_n \doteq s \in \Delta \text{ für atomare Terme } t_1, ..., t_n. \end{aligned}$$

Das führt zu einer eindeutigen Strukturdefinition. Zunächst liegt die Vereinfachung nahe, dass wir für etwa in Γ auftretende freie Variablen jeweils *neue* Konstanten einsetzen und künftig nur von Konstanten reden müssen und von Aussagenmangen ohne freie Variablen. Aber dann ist die angegebene Strukturdefinition noch ungenügend hinsichtlich der Gleichheitsrelation. Wenn etwa $c_1 \doteq c_2 \in \Delta$, dann müsste man c_1 und c_2 als Elemente der Trägermenge identifizieren. Das führt auf folgende Äquivalenzklassenbildung:

$$[c_i] := \{\, c_k \mid c_i \doteq c_k \in \Delta \,\}.$$

Da in Δ alle Identitätsaxiome liegen, also die Kongruenzrelationseigenschaft der Identität, so hat man die korrekten, weil nicht von den Repräsentanten abhängigen Definitionen:

$$\begin{aligned} ([c_1],...,[c_n]) &\in P^{\mathcal{A}} :\Longleftrightarrow Pc_1...c_n \in \Delta, \\ f^{\mathcal{A}}([c_1],...,[c_n]) &= [c_k] :\Longleftrightarrow fc_1...c_n \doteq c_k \in \Delta. \end{aligned}$$

Das ist so weit gut - nach diesen Definitionen gelten die atomaren Formeln von Δ in $\mathcal{A}$. Fehlt nur noch ein wichtiger Schritt: Man möchte nun ausgehend von den atomaren Formeln auch zeigen, dass alle zusammengesetzten Formeln aus Δ ist $\mathcal{A}$ gelten, induktiv über den Formelaufbau. Das macht nun bei $\exists x\alpha$ unüberwindliche Schwierigkeiten. Eine schöne Lösung dieses Problems ist die von Leon Henkin: Man führt für jede Formel $\exists x\alpha \in \Delta$ eine neue Konstante ein, so dass $\alpha[x/c] \in \Delta$. Dann kann man, weil $\alpha[x/c]$ kleineren Aufbau hat als $\exists x\alpha$, auf $\mathcal{A} \models \alpha[x/c]$ schließen und dann wieder auf $\mathcal{A} \models \exists x\alpha$. Wenn man aber diese 'Zeugen' für Existenzaussagen einführt, so hat man wieder nicht die logische Vollständigkeit. Nun könnte man abwechselnd vervollständigen und Zeugen einführen, im Limes hätte man dann das Gewünschte. Aber das geht etwas eleganter 'auf einmal'. Nun kommen wir zum

Beweis des Vollständigkeitssatzes in der Form: Jede abzählbare syntaktisch konsistente Menge Γ von Aussagen hat ein Modell. Sei L die zunächst nur abzählbare Sprache von Γ und sei $C = \{c_1, c_2, ...\}$ eine abzählbar unendliche neue Konstantenmenge, sei ferner $\alpha_1, \alpha_2, ...$ eine Aufzählung aller Aussagen der Sprache L_C, also mit den Symbolen von L und den neuen Konstanten. Dann definieren wir:

$$\begin{aligned} \Delta_0 &:= \Gamma, \\ \Delta_{n+1} &:= \begin{cases} \Delta_n \cup \{\alpha_n\}, \text{ falls dies konsistent ist und } \alpha_n \text{ nicht von der Form } \exists x\beta, \\ \Delta_n \cup \{\alpha_n\} \cup \{\beta[x/c]\}, \text{ falls } \Delta_n \cup \{\alpha_n\} \text{ konsistent und } \alpha_n = \exists x\beta, \\ \text{mit der ersten Konstanten } c \text{ aus } C, \text{ die nicht in } \Delta_n \cup \{\alpha_n\} \text{ vorkommt,} \\ \Delta_n \cup \{\neg\, \alpha_n\}, \text{ falls } \Delta_n \cup \{\alpha_n\} \text{ inkonsistent ist.} \end{cases}, \\ \Delta &:= \bigcup_{n=0}^{\infty} \Delta_n. \end{aligned}$$

Wir behaupten nun:

Lemma 6. *Δ hat folgende Eigenschaften:*

(i) Δ ist konsistent (d.h. syntaktisch widerspruchsfrei),

(ii) Δ ist vollständig (d.h. für jede Aussage γ aus L_C gilt $\gamma \in \Delta$ oder $\neg\, \gamma \in \Delta$).

(iii) Δ hat Zeugen, d.h. mit $\exists x\beta \in \Delta$ gilt für eine Konstante aus $c \in C : \beta[x/c] \in \Delta$.

Aus (ii) ergibt sich zusammen mit (i), dass für jede Aussage α in L_C gilt: $\alpha \in \Delta \Longleftrightarrow \neg\, \alpha \notin \Delta$.

Beweis des Lemmas: Zunächst die Konsistenz: Wenn alle Δ_n konsistent sind, so offenbar auch Δ. Nun ist $\Delta_0 = \Gamma$ konsistent nach Voraussetzung. Sei Δ_n konsistent. Wir zeigen, dass dann auch Δ_{n+1} konsistent ist. Wenn α_n keine Existenzaussage ist, so würde aus $\Delta_n \cup \{\alpha_n\}$ inkonsistent und $\Delta_n \cup \{\neg\, \alpha_n\}$ inkonsistent folgen, dass $\Delta_n \cup \{\alpha_n \vee \neg\, \alpha_n\}$ inkonsistent ist, mithin Δ_n inkonsistent. Wenn $\alpha_n = \exists x\beta$ und $\Delta_n \cup \{\alpha_n\}$ konsistent und $\Delta_n \cup \{\alpha_n\} \cup \{\beta[x/c]\}$ inkonsistent, so hätte man bereits $\Delta_n \cup \{\beta[x/c]\}$ inkonsistent, also, da c nicht in $\Delta_n \cup \{\alpha_n\}$ vorkommt. Daraus folgt aber $\Delta_n \vdash \neg\, \beta(x)$ und damit $\Delta_n \vdash \forall x \neg\, \beta(x)$, somit $\Delta_n \vdash \neg\, \exists x\beta(x)$, im Widerspruch dazu, dass $\Delta_n \cup \{\alpha_n\}$ konsistent ist.

Die Vollständigkeit ergibt sich unmittelbar aus der Konstruktion von Δ.

Wenn $\exists x\beta \in \Delta$, dann hat man $\exists x\beta = \alpha_n$ für ein n. Da Δ konsistent ist, ist insbesondere $\Delta_n \cup \{\alpha_n\}$ konsistent. Also ist nach Konstruktion für eine der neuen Konstanten c auch $\beta[x/c] \in \Delta_{n+1} \subset \Delta$.■

Definition 20. *Wir definieren nunmehr eine Struktur $\mathcal{A}$ zur Sprache L_C :*

$$\begin{aligned} A &:= \{[c] | \, c \in C\} \text{ mit } [c] := \{d \in C | \, c \doteq d \in \Delta\}. \\ &([d_1],...,[d_n]) \in P^{\mathcal{A}} :\Longleftrightarrow Pd_1...d_n \in \Delta, \\ &f^{\mathcal{A}}([d_1],...,[d_n]) = d :\Longleftrightarrow fd_1...d_n \doteq d \in \Delta. \end{aligned}$$

Beweis der Korrektheit der Definition von $\mathcal{A}$: Wir haben für alle $c, d, e \in C$ und alle $d_1, ..., d_n \in C$ und alle $e_1, ..., e_n \in C$:

(i) $c \doteq c \in \Delta$

(ii) $c \doteq d \in \Delta \iff d \doteq c \in \Delta$

(iii) $c \doteq d \in \Delta$ und $d \doteq e \in \Delta \implies c \doteq e \in \Delta$

(iv) $d_i \doteq e_i \in \Delta$ für $1 \leq i \leq n$ und $Pd_1...d_n \in \Delta \implies Pe_1...e_n \in \Delta$

(v) $d_i \doteq e_i \in \Delta$ für $1 \leq i \leq n$, dann $fd_1...d_n \doteq fe_1...e_n \in \Delta$.

Denn die entsprechenden logischen Wahrheiten sind automatisch in Δ. Aus $(i) - (iii)$ folgt also, dass mit $[c]$ eine Klasseneinteilung gegeben ist. Aus (iv) und (v) folgt, dass die Definitionen von $P^{\mathcal{A}}$ und von $f^{\mathcal{A}}$ unabhängig von den Repräsentanten sind. Zu berücksichtigen ist dabei, dass mit $\exists x\,(fd_1...d_n \doteq x)$ auch eine Formel der Gestalt $fd_1...d_n \doteq c$ in Δ ist und mit (v) die Definition von $f^{\mathcal{A}}$dann eindeutig wird.■

Beweis dafür, dass $\mathcal{A} \models \Delta$ in der Form: Für alle Aussagen γ in L_C hat man:

$$\mathcal{A} \models \gamma \iff \gamma \in \Delta.$$

Diese Aussage beweisen wir durch Induktion über den Formelaufbau von $\gamma \in \Delta$:

Induktionsanfang:

Für atomare γ gilt die Aussage nach Konstruktion.

Das ist unmittelbar klar für eine Sprache ohne Funktionssymbole (außer den nullstelligen, den Konstanten von C). Für eine Sprache mit Funktionssymbolen wird das ein wenig mühsam, es geht besser, wenn man anstelle der Konstanten-Klassen gleich die Termklassen nimmt, also definiert: $A := \{\,[t] |\, t \text{ Term}\}$ mit

$$[t] := \{\,s|\ \ s \text{ Term mit } s \doteq t \in \Delta\}\,.$$

Dann ist wieder der Induktionsanfang einfach. Natürlich hat man für jeden Term t stets eine der neuen Konstanten c_i in C, so dass $[t] = [c_i]$, weil $t \doteq c_i$ mit einer solchen Konstanten jedenfalls in Δ liegt, weil $\exists x t \doteq x$ als ableitbare Formel jedenfalls in Δ liegt und Δ Zeugen hat.

Nun zum Induktionsschluss: Mit * wird jeweils die Stelle markiert, an welcher man die Induktionsvoraussetzung benutzt. Die anderen Argumente ergeben sich jeweils aus der Definition der Gültigkeit einer Aussage in einer Struktur sowie aus den Abgeschlossenheitseigenschaften von Δ.

Sei nun $\gamma = \neg\neg\alpha$. Dann hat man

$$\mathcal{A} \models \neg\neg\gamma \iff \mathcal{A} \not\models \gamma \iff {}^*\gamma \notin \Delta \iff \neg\neg\gamma \in \Delta.$$

Sei $\gamma = \alpha \wedge \beta$. Dann hat man:

$$\begin{array}{lll} \mathcal{A} & \models & \alpha \wedge \beta \\ & \iff & \mathcal{A} \models \alpha \text{ und } \mathcal{A} \models \beta \\ & \iff & {}^*\alpha \in \Delta \text{ und } \beta \in \Delta \\ & \iff & \alpha \wedge \beta \in \Delta. \end{array}$$

Sei $\gamma = \exists x \alpha$. Dann hat man:

$$\begin{array}{lll} \mathcal{A} & \models & \exists x \alpha \\ & \iff & \mathcal{A} \models \alpha[h(x/[c])] \text{ für ein } c \in C \\ & \iff & \mathcal{A} \models \alpha[x/c] \text{ für ein } c \in C \\ & \iff & \alpha[x/c] \in \Delta \text{ für ein } c \in C \\ & \iff & \exists x \alpha \in \Delta. \end{array}$$

Damit ist der Vollständigkeitsbeweis abgeschlossen für abzählbare Formelmengen Γ.

Bemerkung zur Verallgemeinerung auf überabzählbare Formelmengen: Wir benutzen nunmehr das Auswahlaxiom. Dann wählen wir eine Menge C neuer Konstanten, deren Kardinalzahl κ die von Γ ist. Nun haben wir mit dem Auswahlaxiom eine Aufzählung α_β der Formelmenge von L_C, mit den Ordinalzahlen β in κ. Diese bildet eine Wohlordnung. D.h. entweder ist β gleich Null, oder $\beta = \beta_1 + 1$, oder β ist eine Limesordinalzahl, $\beta = \cup_{\alpha<\beta}\alpha$. Dann setzt man $\Delta_{\alpha+1}$ wie oben an, ferner $\Delta_\beta = \cup_{\alpha<\beta}\Delta_\alpha$

für Limesordinalzahlen $\beta < \kappa$. Schließlich definiert man $\Delta := \cup_{\alpha<\kappa}\Delta_\alpha$. Dann läuft die Konstruktion eines Modells von Δ wie zuvor, und dies Modell hat eine Kardinalzahl $\leq \kappa$.

Aus den Konstruktionen der Modelle entnehmen wir noch als Korollar:

FOLGERUNG 1. *Eine konsistente Menge Γ von Formeln hat ein Modell, dessen Trägermenge höchstens die Mächtigkeit der Sprache von Γ hat. Hat die Menge Γ höchstens die Mächtigkeit κ, so gibt es ein Modell von Γ, das höchstens die Mächtigkeit $\aleph_0 + |\Gamma|$ hat. Dabei ist $\aleph_0$ die Mächtigkeit von $\mathbb{N}$, und $|\Gamma|$ ist die Mächtigkeit von Γ.*

Hier ist eine unmittelbare wichtige Folgerung des Vollständigkeitssatzes:

SATZ 3 (Kompaktheitssatz). *Wenn $\Gamma \models \alpha$, so gilt für eine endliche Teilmenge $\Gamma' \subset \Gamma : \Gamma' \models \alpha$.*

Beweis: Aus $\Gamma \models \alpha$ folgt mit dem Vollständigkeitssatz $\Gamma \vdash \alpha$, daraus folgt unmittelbar mit der Definition des Ableitungsbegriffs, dass für eine endliche Teilmenge $\Gamma' \subset \Gamma$ gilt: $\Gamma' \vdash \alpha$, daraus hat man mit der Korrektheit dann wieder $\Gamma' \models \alpha$.■

6. Anwendungen des Kompaktheitssatzes

Wir geben ein paar typische kleine Anwendungen, dann den Satz von Löwenheim-Skolem, der allerdings auch die Konstruktion des Vollständigkeitsbeweises benutzt.

Erstes Beispiel: Wenn ein Axiomensystem Γ beliebig große endliche Modelle hat, dann hat es ein unendliches Modell. Denn seien $\exists_{\geq n}$ die Aussagen

$$\exists x_1 ... x_n \bigwedge_{i\neq j} \neg\, x_i \doteq x_j,$$

dann ist nach Voraussetzung jede endliche Teilmenge von

$$\Gamma \cup \{\, \exists_{\geq n} |\, n \in \mathbb{N}_{\geq 1}\}$$

erfüllbar, also ist diese Menge selbst erfüllbar, ein Modell von ihr ist aber unendliches Modell von Γ.

Zweites Beispiel: Es gibt eine Oberstruktur $\mathbb{R}^*$ von $\mathbb{R}$, welche alle mit Konstanten in $\mathbb{R}$ gültigen Aussagen in

$$\left\langle \mathbb{R}, 0, 1, +, \cdot, (r)_{r\in\mathbb{R}} \right\rangle$$

erfüllt und außerdem infinitesimale Elemente besitzt, also Zahlen $\alpha > 0$, welche kleiner als jede reelle Zahl $r > 0$ sind. Dazu bilden wir die Aussagenmenge

$$Th\left(\left\langle \mathbb{R}, 0, 1, +, \cdot, (r)_{r\in\mathbb{R}} \right\rangle\right) \cup \{\, c < r |\, r > 0\}\,.$$

Jede endliche Teilmenge davon ist offenbar in $\left\langle \mathbb{R}, 0, 1, +, \cdot, (r)_{r\in\mathbb{R}} \right\rangle$ selbst erfüllt. Denn zu allen reellen Zahlen $r_1, ..., r_n > 0$ gibt es eine reelle Zahl s mit $0 < s < \min(r_1, ..., r_n)$. Damit ist aber die gesamte Aussagenmenge erfüllt, und in einem Modell muss die Interpretation von c die gewünschte Eigenschaft haben.

Drittes Beispiel: Es gibt ein Modell von $Th\left(\left\langle \mathbb{N}, 0, 1, +, \cdot, (n)_{n\in\mathbb{N}} \right\rangle\right)$, das ein 'unendlich großes' Element besitzt, also größer als alle natürlichen Zahlen. Das folgt sofort aus der endlichen Erfüllbarkeit von

$$Th\left(\left\langle \mathbb{N}, 0, 1, +, \cdot, (n)_{n\in\mathbb{N}} \right\rangle\right) \cup \{\, c > c_n |\, n \in \mathbb{N}\}\,,$$

wobei in $Th\left(\left\langle \mathbb{N}, 0, 1, +, \cdot, (n)_{n\in\mathbb{N}} \right\rangle\right)$ die Konstante c_n durch n gedeutet wird. Ein Modell dieser Art sei nun

$$\mathcal{A} = \left\langle A, 0^{\mathcal{A}}, 1^{\mathcal{A}}, +^{\mathcal{A}}, \cdot^{\mathcal{A}}, \left(c_n^{\mathcal{A}}\right)_{n\in\mathbb{N}}, c^{\mathcal{A}} \right\rangle.$$

Dann erfüllt

$$\mathcal{A}' = \left\langle A, 0^{\mathcal{A}}, 1^{\mathcal{A}}, +^{\mathcal{A}}, \cdot^{\mathcal{A}}, \left(c_n^{\mathcal{A}}\right)_{n\in\mathbb{N}} \right\rangle$$

also dieselben Aussagen wie $\left\langle \mathbb{N}, 0, 1, +, \cdot, (n)_{n\in\mathbb{N}} \right\rangle$, ist aber nicht isomorph zu $\left\langle \mathbb{N}, 0, 1, +, \cdot, (n)_{n\in\mathbb{N}} \right\rangle$. Denn die Aussage der Prädikatenlogik 2. Stufe:

$$\forall S\,(0 \in S \wedge \forall x\,(x \in S \to x + 1 \in S) \to \forall y\,(y \in S))$$

ist in $\langle \mathbb{N}, 0, 1, +, \cdot \rangle$ erfüllt, nicht aber in $\left\langle A, 0^{\mathcal{A}}, 1^{\mathcal{A}}, +^{\mathcal{A}}, \cdot^{\mathcal{A}} \right\rangle$ (deute S in $\mathcal{A}'$ als $\left\{ c_n^{\mathcal{A}} \middle|\, n \in \mathbb{N} \right\}$), weshalb beide nicht isomorph sein können. Es folgt, dass die Logik 1. Stufe weniger aussagekräftig ist als die Logik 2. Stufe.

SATZ 4 (Löwenheim-Skolem). *Es sei* Γ *eine Menge von Aussagen, die ein Modell in einer Kardinalzahl* $\kappa \geq |L(\Gamma)|$ *hat. Dann hat* Γ *ein Modell in jeder Mächtigkeit* $\lambda \geq \min(\kappa, |L(\Gamma)|)$.

Beweis: Wenn $\mathcal{A}$ ein Modell von Γ der Kardinalzahl κ ist, nach Voraussetzung κ unendlich, dann ist folgende Aussagenmenge endlich erfüllbar (d.h. jede endliche Teilmenge ist erfüllbar):

$$\Gamma \cup \{ \multimap c_i \doteq c_j | \, i \neq j, i, j \in I \},$$

mit einer Menge $\{ c_i | \, i \in I \}$ von neuen Konstanten, $|I| = \lambda$. Denn man kann die Konstanten bereits in $\mathcal{A} \models \Gamma$ so deuten, dass die endliche Teilmenge wahr wird in $\langle \mathcal{A}, a_1, ..., a_n \rangle$. Also ist die Menge syntaktisch widerspruchsfrei und hat daher ein Modell der Mächtigkeit λ nach Konstruktion des Vollständigkeitsbeweises.■

Anwendungen des Löwenheim-Skolem-Satzes:

1. Wenn man weiß, dass es einen algebraisch abgeschlossenen Körper der Mächtigkeit $|\mathbb{R}|$ gibt, nämlich $\mathbb{C}$, dann weiß man auch ohne weitere konkrete Konstruktion, dass es algebraisch abgeschlossene Körper in allen unendlichen Mächtigkeiten gibt. Hier ist das Axiomensystem Γ abzählbar unendlich zu wählen, zu den Körperaxiomen kommen noch alle Axiome der Form:

$$\forall x_0 ... x_n \left(\multimap x_n \doteq 0 \to \exists y \left(x_n y^n + x_{n-1} y^{n-1} + ... + x_0 = 0 \right) \right), \; n \geq 1.$$

Dabei sollte man sich denken, dass y^n abkürzend für $y \cdot ... \cdot y$ (n Faktoren) steht für $n \geq 1$. Zusammen besagen die Axiome also: Jedes Polynom (mit beliebigen Koeffizienten im Körper) vom Grade $n \geq 1$ hat mindestens eine Nullstelle, für alle Polynomgrade $n \geq 1$. Die Sprache ist also nur abzählbar, und so folgt aus der Existenz eines Modells in einer unendlichen Kardinalzahl mit dem Satz die Existenz in jeder unendlichen Kardinalzahl.

2. Ebenso folgt die Existenz von Modellen von $Th\left(\left\langle \mathbb{N}, 0, 1, +, \cdot, (n)_{n \in \mathbb{N}} \right\rangle \right)$ in jeder unendlichen Kardinalzahl.

7. Der Satz von Herbrand und ein weiterer Ansatz des Vollständigkeitsbeweises

DEFINITION 21. *Eine Formel* α *hat pränexe Normalform genau dann, wenn mit einer quantorenfreien Formel* β *gilt:*

$$\alpha = \forall \overrightarrow{\mathbf{x}}_1 \exists \overrightarrow{\mathbf{y}}_1 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \beta.$$

Dabei können die Quantorenblöcke auch leer sein, insbesondere kann α *auch mit einem Block von Existenzquantoren beginnen. Ferner sollen die Quantorenblöcke so eingerichtet werden, dass sich dabei keine Variable wiederholt.*

Beispiel: $\forall x \exists y \, (x < y)$ ist in pränexer Normalform. $\forall x \, (Px \to \exists y Q x y)$ ist nicht in pränexer Normalform, kann aber gleichwertig in pränexe Normalform umgeformt werden zu $\forall x \exists y \, (Px \to Qxy)$. Das folgende Lemma besagt, dass dies stets gelingt:

LEMMA 7. *Jede Formel ist gleichwertig zu einer Formel in pränexer Normalform.*

Beweis: Man hat $\models \forall x \alpha \wedge \beta \leftrightarrow \forall x \, (\alpha \wedge \beta)$, wenn x nicht in β. Sonst wähle y nicht in β, dann $\models \forall x \alpha \wedge \beta \leftrightarrow \forall y \alpha [x/y] \wedge \beta$ und $\models \forall y \alpha [x/y] \wedge \beta \leftrightarrow \forall y \, (\alpha [x/y] \wedge \beta)$, also $\models \forall x \alpha \wedge \beta \leftrightarrow \forall y \, (\alpha [x/y] \wedge \beta)$. Dasselbe gelingt mit $\models \forall x \alpha \vee \beta \leftrightarrow \forall y \, (\alpha [x/y] \vee \beta)$. Völlig analog verläuft die Sache für den Existenzquantor. Schließlich hat man $\models \multimap \forall x \alpha \leftrightarrow \exists x \multimap \alpha$ und $\models \multimap \exists x \alpha \leftrightarrow \forall x \multimap \alpha$. Auf diese Weise kann man die Quantoren stets ganz nach außen schieben. Es sei bemerkt, dass wir nicht nur mit dem Vollständigkeitssatz die Gleichwertigkeit auch im Sinne der Beweisbarkeit haben, also existiert zu beliebiger Formel α eine pränexe Formel β mit $\vdash \alpha \leftrightarrow \beta$. Sondern wir können auch die oben angeführten Äquivalenzen formale Ableitungen geben.

Wir werden nunmehr eine Formel α, nach deren Erfüllbarkeit oder Allgemeingültigkeit wir fragen, noch weiter reduzieren durch 'Skolemisierung' (benannt nach Thoralf Skolem).

SATZ 5. *Zu jeder Formel* α *gibt es eine Allformel* $\beta = \forall \overrightarrow{\mathbf{x}} \varphi$, φ *quantorenfrei (in einer um geeignete Funktionssymbole erweiterten Sprache der Prädikatenlogik 1. Stufe), so dass*

$$\alpha \text{ erfüllbar} \iff \beta \text{ erfüllbar.}$$

Zu jeder Formel α *gibt es eine Existenzformel* $\gamma = \exists \overrightarrow{\mathbf{x}} \varphi$, φ *quantorenfrei (in einer um geeignete Funktionssymbole erweiterten Sprache der Prädikatenlogik 1. Stufe), so dass*

$$\alpha \text{ allgemeingültig} \iff \gamma \text{ allgemeingültig.}$$

Die Formeln β, γ sind dabei als Skolemsche Normalformen effektiv konstruierbar aus α. (Die Quantorenblöcke der Allformel / Existenzformel können auch fehlen im trivialen Fall.)

Beweis: Wir können nach dem vorigen Lemma annehmen, dass α bereits in pränexer Form ist. Außerdem können wir für freie Variablen in α neue Konstanten einsetzen und annehmen, dass α ein Aussage ist. Dann konstruieren wir zu

$$\alpha = \forall \overrightarrow{\mathbf{x}}_1 \exists \overrightarrow{\mathbf{y}}_1 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi,\ \psi \text{ quantorenfrei},$$

mit Induktion über n zunächst für $n = 1$:

$$\widetilde{\alpha} := \forall \overrightarrow{\mathbf{x}}_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi \left[\overrightarrow{\mathbf{y}}_1 / \overrightarrow{\mathbf{f}} \left(\overrightarrow{\mathbf{x}}_1 \right) \right]$$

Dabei ist für $\overrightarrow{\mathbf{y}}_1 = (v_{i_1} ... v_{i_k})$ eine Folge $(f_{i_1} ... f_{i_k})$ von neuen Funktionssymbolen eingeführt, alle mit der Stellenzahl m, wobei $\overrightarrow{\mathbf{x}}_1 = (v_{j_1}, ..., v_{j_m})$. Die Termfolge $\overrightarrow{\mathbf{f}} \left(\overrightarrow{\mathbf{x}}_1 \right)$ ist damit

$$\left(f_{i_1} \left(v_{j_1}, ..., v_{j_m} \right), ..., f_{i_k} \left(v_{j_1}, ..., v_{j_m} \right) \right).$$

Nun verfährt man induktiv so weiter für die Formel $\forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi \left[\overrightarrow{\mathbf{y}}_1 / \overrightarrow{\mathbf{f}} \left(\overrightarrow{\mathbf{x}}_1 \right) \right]$, für jeden Schritt benutzt man jeweils neue Funktionssymbole. Wir erwähnen noch, dass man in dem Fall, dass

$$\alpha = \exists \overrightarrow{\mathbf{y}}_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi,\ \psi \text{ quantorenfrei},$$

einfach beginnt mit

$$\widetilde{\alpha} := \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi \left[\overrightarrow{\mathbf{y}}_1 / \overrightarrow{\mathbf{c}} \right],$$

mit neuen Konstanten $\overrightarrow{\mathbf{c}}$. Sei nun α^* das Endprodukt dieser Umformungen von α.

Wir behaupten nunmehr: α ist genau dann erfüllbar, wenn α^* es ist. Für den Beweis genügt es, dass wir das für jeden einzelnen der Umformungsschritte zeigen, also α erfüllbar genau dann, wenn $\widetilde{\alpha}$ erfüllbar. Offenbar haben wir:

$$\mathcal{A} \models \forall \overrightarrow{\mathbf{x}}_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi [\left[\overrightarrow{\mathbf{y}}_1 / \overrightarrow{\mathbf{f}} \left(\overrightarrow{\mathbf{x}}_1 \right) \right] \implies \mathcal{A} \models \forall \overrightarrow{\mathbf{x}}_1 \exists \overrightarrow{\mathbf{y}}_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi.$$

Denn $\overrightarrow{\mathbf{y}}_1$ ist frei für $\overrightarrow{\mathbf{f}} \left(\overrightarrow{\mathbf{x}}_1 \right)$, und so haben wir sogar

$$\vdash \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi \left[\overrightarrow{\mathbf{y}}_1 / \overrightarrow{\mathbf{f}} \left(\overrightarrow{\mathbf{x}}_1 \right) \right] \rightarrow \forall \overrightarrow{\mathbf{x}}_1 \exists \overrightarrow{\mathbf{y}}_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi.$$

Umgekehrt: Es gelte

$$\mathcal{A} \models \forall \overrightarrow{\mathbf{x}}_1 \exists \overrightarrow{\mathbf{y}}_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi.$$

Dann hat man

$$\mathcal{A} \models \exists \overrightarrow{\mathbf{y}}_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi [\overrightarrow{\mathbf{x}}_1 / \overrightarrow{\mathbf{a}}] \text{ für alle Folgen } \overrightarrow{\mathbf{a}}$$

von Elementen von A, der Länge von $\overrightarrow{\mathbf{x}}_1$. Nun weiter: Zu solcher beliebiger Folge $\overrightarrow{\mathbf{a}}$ gibt es eine Folge $\overrightarrow{\mathbf{b}}$ von Elementen von A, der Länge von $\overrightarrow{\mathbf{y}}_1$ entsprechend, so dass

$$\mathcal{A} \models \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi [\overrightarrow{\mathbf{x}}_1 / \overrightarrow{\mathbf{a}}, \overrightarrow{\mathbf{y}} / \overrightarrow{\mathbf{b}}].$$

Wenn $\mathcal{A}$ abzählbar ist, so können wir sagen: Zu $\overrightarrow{\mathbf{a}}$ sei b_1 das kleinste Element in der Numerierung von A, so dass

$$\mathcal{A} \models \exists \overrightarrow{\mathbf{y}}'_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi [\overrightarrow{\mathbf{x}}_1 / \overrightarrow{\mathbf{a}}_1, u_1 / b_1],$$

wobei $\overrightarrow{\mathbf{y}}_1 = v_{i_1} v_{i_2} ... v_{i_k}$ und $\overrightarrow{\mathbf{y}}'_1 = v_{i_2} ... v_{i_k}$. So verfahren wir weiter mit allen Variablen von $\overrightarrow{\mathbf{y}}_1$. Dann definieren wir die Funktionen

$$f_{i_j}^{\mathcal{A}'} \left(\overrightarrow{\mathbf{a}} \right) := b_j,\ 1 \leq j \leq k.$$

Dann gilt $\mathcal{A}' = \left\langle \mathcal{A}, \left(f_{i_j}^{\mathcal{A}'} \right)_{1 \leq j \leq k} \right\rangle \models \forall \overrightarrow{\mathbf{x}}_1 \forall \overrightarrow{\mathbf{x}}_2 ... \forall \overrightarrow{\mathbf{x}}_n \exists \overrightarrow{\mathbf{y}_n} \psi \left[\overrightarrow{\mathbf{y}}_1 / \overrightarrow{\mathbf{f}} \left(\overrightarrow{\mathbf{x}}_1 \right) \right]$ mit $\overrightarrow{\mathbf{f}} = (f_{i_1}, ..., f_{i_k})$.

Es sei bemerkt, dass für überabzählbare $\mathcal{A}$ das Auswahlaxiom herangezogen werden müsste, um die verlangten Skolemfunktionen zu konstruieren.

Somit haben wir eine Allformel α^* konstruiert, die genau dann erfüllbar ist, wenn α es ist.

Für den zweiten Teil des Satzes überlegt man: α ist genau dann allgemeingültig, wenn $\neg \alpha$ nicht erfüllbar ist. Also ist α genau dann allgemeingültig, wenn $(\neg \alpha)^*$ nicht erfüllbar ist. Aber $(\neg \alpha)^* = \forall \overrightarrow{\mathbf{x}} \psi$ ist nicht erfüllbar genau dann, wenn $\neg \forall \overrightarrow{\mathbf{x}} \psi$ allgemeingültig ist, d.h. wenn $\exists \overrightarrow{\mathbf{x}} \neg \psi$ allgemeingültig ist.■

Wir kommen nunmehr zu folgendem

SATZ 6 (von Herbrand). *Sei $\alpha = \exists\overrightarrow{\mathbf{x}}\psi$, ψ quantorenfrei, eine Aussage in einer Sprache der Prädikatenlogik 1. Stufe ohne Identität mit mindestens einer Konstanten. Dann ist α genau dann allgemeingültig, wenn es konstante Termfolgen $\overrightarrow{\mathbf{t}}_1, ..., \overrightarrow{\mathbf{t}}_n$ gibt, alle von der Länge von $\overrightarrow{\mathbf{x}}$, so dass*

$$\bigvee_{i=1}^{n} \psi\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i\right] \text{ allgemeingültig ist.}$$

Beweis: Wir haben

$$\vdash \bigvee_{i=1}^{n} \psi\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i\right] \to \exists\overrightarrow{\mathbf{x}}\psi,$$

weil alle Variablen von $\overrightarrow{\mathbf{x}}$ frei für alle $\overrightarrow{\mathbf{t}}_i$ sind. Interessant ist die umgekehrte Richtung: Sei $\exists\overrightarrow{\mathbf{x}}\psi$ allgemeingültig. Wäre nun $\bigvee_{i=1}^{n} \psi\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i\right]$ für alle Folgen konstanter Terme $\overrightarrow{\mathbf{t}}_i$ nicht allgemeingültig, so wäre

$$\bigwedge_{i=1}^{n} \neg\, \psi\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i\right] \text{ erfüllbar,}$$

also wäre nach Kompaktheitssatz auch erfüllbar:

$$\left\{ \neg\, \psi\left[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}\right] \middle| \overrightarrow{\mathbf{t}} \text{ Folge konstanter Terme} \right\}.$$

Nun sei $\mathcal{A}$ ein Modell, das diese Menge von Aussagen erfüllt. Dann erfüllt auch die folgende Struktur $\mathcal{B}$ diese Aussagenmenge:

$$B := \left\{ t^{\mathcal{A}} \middle| \, t \text{ konstanter Term} \right\},$$

$$\mathcal{B} = \left\langle B, \left(\left(R_j^k\right)_{k,j}\right)^{\mathcal{A}} \cap B^k, \left(\left(f_i^n\right)_{n,i}\right)^{\mathcal{A}}_{|B^n} \right\rangle.$$

Denn nach Konstruktion ist $\mathcal{B}$ eine Unterstruktur von $\mathcal{A}$, und eine quantorenfreie Formel gilt in $\mathcal{B}$ genau dann, wenn sie in $\mathcal{A}$ gilt. Nun haben wir aber

$$\mathcal{B} \models \neg\, \exists\overrightarrow{\mathbf{x}}\psi,$$

so dass $\exists\overrightarrow{\mathbf{x}}\psi$ nicht allgemeingültig sein kann.■

Daraus ergibt sich folgende Idee, von einer Formel, welche allgemeingültig ist, algorithmisch zu entscheiden, dass sie es ist: Man bringt sie in die Skolemform $\exists\overrightarrow{\mathbf{x}}\psi$ mit quantorenfreiem ψ, dann bringt man mit Termfolgen $\overrightarrow{\mathbf{t}}_i$, wobei $\left(\overrightarrow{\mathbf{t}}_i\right)_i$ eine mit einem Computerprogramm zu erzeugende Aufzählung aller Termfolgen der Länge von $\overrightarrow{\mathbf{x}}$ ist, der Reihen nach für alle n die Formeln

$$\bigvee_{i=1}^{n} \psi[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i]$$

in die konjunktiven Normalformen

$$\bigwedge_{j=1}^{m} \bigvee_{i=1}^{n} \bigvee_{k=1}^{u_j} \psi_{jk}[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i]$$

bringt, mit atomaren oder negiert atomaren ψ_{ij}. Das geht so: Sei

$$\psi = \bigwedge_{j=1}^{m} \bigvee_{k=1}^{u_j} \psi_{jk} \text{ (konjunktive Normalform,}$$

mit atomaren oder negiert atomaren ψ_{jk}. Dann hat man

$$\vdash \bigvee_{i=1}^{n} \psi[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i] \leftrightarrow \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \bigvee_{k=1}^{u_j} \psi_{jk}[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i],$$

also mit Distributivgesetz der Aussagenlogik:

$$\vdash \bigvee_{i=1}^{n} \psi[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i] \leftrightarrow \bigwedge_{j=1}^{m} \bigvee_{i=1}^{n} \bigvee_{k=1}^{u_j} \psi_{jk}[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i].$$

Wenn nun $\bigvee_{i=1}^{n} \psi[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i]$ allgemeingültig ist, so bekommt man, dass für alle j mit $1 \leq j \leq m$ gelten muss:

$$\bigvee_{i=1}^{n} \bigvee_{k=1}^{u_j} \psi_{jk}[\overrightarrow{\mathbf{x}}/\overrightarrow{\mathbf{t}}_i]$$

ist aussagenlogische Tautologie, enthält also eine atomare Formel zusamt ihrer Verneinung. Dies kann also algorithmisch festgestellt werden. Wir haben damit den ersten Teil des folgenden Satzes bewiesen:

SATZ 7. *Man kann von einer allgemeingültigen Formel der Prädikatenlogik 1. Stufe algorithmisch feststellen, dass sie allgemeingültig ist. Man kann mit einem Computerprogramm alle allgemeingültigen Formeln algorithmisch aufzählen. (Aber Vorsicht: Man kann nicht mit einem Computerprogramm entscheiden, ob eine vorgelegte Formel allgemeingültig ist oder nicht.)*

Beweis des Zusatzes: Man führt alle Formeln systematisch auf, ersetzt sie durch ihre Skolemformen für Erfüllbarkeit. Dann führt man für die erste Formel eine Termeinsetzung ein und stellt wie oben fest, ob sie allgemeingültig ist. Dann führt man für die erste und die zweite Formel zwei Termeinsetzungen durch, dann für die erste bis dritte Formel je drei Termeinsetzungen, usw. Dabei notiert man jede Formel, deren Allgemeingültigkeit erwiesen wurde.■

Zum negativen Zusatz: Ein Beweis dafür wird erst im Abschnitt über rekursive Funktionen zugänglich.

Zur Gültigkeit des Satzes auch für die Prädikatenlogik mit Identität: Eine Formel α der Prädikatenlogik mit Identität kann man ersetzen durch eine Formel der Prädikatenlogik ohne Identität, so dass sich an Allgemeingültigkeit oder Erfüllbarkeit nichts ändert, und die Zuordnung ist wiederum rein schematisch: Alle $t_1 \doteq t_2$ in α ersetze man durch Rt_1t_2, mit einem neuen Relationssymbol R. Dann füge man mit Konjunktion die Aussage an, welche besagt, dass eine Interpretation von R eine Äquivalenzrelation ist, die mit allen Relationen (außer der Identität) und Operationen verträglich ist, deren Symbole in α vorkommen. Kurz gesagt ist das die Aussage, dass R eine Kongruenzrelation bezüglich aller Relationen und Operationen darstellt, von denen α spricht. Dann ist diese neue Aussage erfüllbar [allgemeingültig] genau dann, wenn α es ist.

Konkretes Beispiel: Abschließend wollen wir das erwähnte Programm für folgende allgemeingültige Formel durchführen:

$$\exists x \forall y \left(Px \to Py\right).$$

Diese Formel ist bereits in pränexer Form. Wir müssen vor 'Skolemisierung' die Verneinung bilden und diese pränex machen, das ergibt:

$$\forall x \exists y \left(Px \wedge \neg Py\right),$$

nun mit Skolemfunktion:

$$\forall x \left(Px \wedge \neg Pf\left(x\right)\right).$$

Dass $\exists x \forall y \left(Px \to Py\right)$ allgemeingültig ist, bedeutet nun dasselbe wie:

$$\exists x \left(\neg Px \vee Pf\left(x\right)\right)$$

ist allgemeingültig. Nun nehmen wir die Konstante c und bilden

$$\neg Px \vee Pf\left(x\right)[x/c],$$

das ergibt

$$\psi[x/c] = \neg Pc \vee Pf\left(c\right),$$

diese Formel ist nicht allgemeingültig. Setzen wir nunmehr aber ein:

$$\neg Px \vee Pf\left(x\right)[x/f(c)],$$

so haben wir

$$\psi[x/f\left(c\right)] = \neg Pf\left(c\right) \vee Pf\left(f\left(c\right)\right),$$

und nun sehen wir:

$$\psi[x/c] \vee \psi[x/f\left(c\right)] = \neg Pc \vee Pf\left(c\right) \vee \neg Pf\left(c\right) \vee Pf\left(f\left(c\right)\right),$$

und diese Formel ist bereits aussagenlogisch allgemeingültig, wie im Herbrandschen Satz versprochen. In diesem Beispiel lag bereits konjunktive Normalform vor.

Wir bemerken abschließend, dass Gödels ursprünglicher Vollständigkeitsbeweis für die Prädikatenlogik über die Herbrandsche Normalform / Reduktion auf Aussagenlogik lief. Die semantischen Argumente dieses Abschnitts waren dafür syntaktisch nachzuzeichnen.

KAPITEL 2

Rekursive Funktionen, Berechenbarkeit und rekursive Aufzählbarkeit

1. Einleitung: Die Idee der Berechenbarkeit

Wir wollen beschreiben, was man prinzipiell mit einem Computerprogramm berechnen kann. Zunächst: Man kann offenbar einige Dinge der Zahlentheorie, aber auch der Linearen Algebra oder der reellen Analysis 'berechnen' nach schematischem Verfahren. Beispiele: Berechne die n.Primzahl bei Eingabe von n, berechne die Ableitung einer elementaren Funktion bei Eingabe eines Rechenausdrucks für sie, berechne das Produkt zweier Matrizen. Auch gewisse Dinge der mathematischen Logik kann man berechnen, z.B. die Gültigkeit einer aussagenlogischen Formel, oder auch eine pränexe Normalform zu einer Formel. Stets benötigt man dabei so etwas wie eine Codierung, und da zeigt sich, dass man eine solche Codierung stets mit natürlichen Zahlen vornehmen kann. Wir werden später auch ausdrücklich Formeln der Prädikatenlogik durch natürliche Zahlen codieren. Daher fragen wir genauer, welche Funktionen $\mathbb{N}^k \to \mathbb{N}$ berechenbar sind in dem Sinne, dass man ein Computerprogramm schreiben kann, welches die Rechnung für jede eingegebene Zahl ausführt. Dabei wollen wir weder auf die benötigte Rechenzeit eingehen, noch darauf, ob der Computer Speicherplatz genug hat, die Rechnung auszuführen.

Es ist klar, dass es auch berechenbare Funktionen $f : \mathbb{N}^k \to \mathbb{N}^m$ gibt und dass eine solche Funktion genau dann berechenbar ist, wenn jede Komponentenfunktion es ist. Also

$$\begin{aligned} f(x_1, ..., x_k) \quad &= \quad (f_1(x_1, ...x_k), ..., f_m(x_1, ..., x_k)) \text{ berechenbar} \\ &\iff \quad \text{für alle } 1 \leq i \leq m: \ f_i \text{ berechenbar.} \end{aligned}$$

Wir werden auch noch sehen, wie man Zahlentupel mit einer einzigen Zahl codieren kann, so dass Codierung und Decodierung berechenbar sind, so dass der Unterschied zwischen ein- und mehrstelligen Funktionen bzw. skalaren oder vektorwertigen Funktionen sich als unwesentlich erweist für Probleme der Berechenbarkeit.

Eine letzte Vorbemerkung ist noch anzubringen hinsichtlich der Frage, was man unter einer berechenbaren Funktion $\mathbb{R} \to \mathbb{R}$ zu verstehen hätte. Beispielsweise sollte doch $f(x) = p(x)$ für ein Polynom p oder sogar sin 'berechenbar' sein. Klar ist doch auch, dass man für das Vektorprodukt $\mathbb{R}^3 \to \mathbb{R}^3$ ein Programm schreiben kann. Zunächst widerspricht das der Aussage, dass alle Objekte, mit denen man im algorithmischen Sinne rechnen kann, durch natürliche Zahlen codiert werden können, allein schon aus Kardinalzahlgründen. Tatsächlich kann eine Funktion $\mathbb{R} \to \mathbb{R}$ nicht algorithmisch berechenbar sein. Das liegt allein schon daran, dass man nicht zu jeder reellen Zahl x ein Computerprogramm angeben kann, das jede Stelle der Dezimaldarstellung von x berechnet. Ein Weg ist nun, den Begriff 'berechenbare reelle Zahl' zu bilden. Dann werden wir aber wieder auf Codierung durch natürliche Zahlen zurückgeführt - man wähle als Code gerade die Nummer des betreffenden Programms. Eine andere Auffassung besteht darin, dass man von Berechenbarkeit des Outputs einer Funktion relativ zum Input spricht, also gegeben ein 'Orakel' für die Stellen der Eingabezahl. In beiderlei Sinn sind die erwähnten Funktionen dann 'berechenbar'.

Wir gehen nunmehr so vor, dass wir drei Versionen von Berechenbarkeit für Funktionen $\mathbb{N}^k \to \mathbb{N}$ präzisieren und deren Gleichwertigkeit zeigen. Anschließend bringen wir ein paar tiefer liegende Resultate der Rekursionstheorie und Anwendungen auf Prädikatenlogik erster Stufe sowie Peanoarithmetik.

Die drei Versionen sind folgende - (i) ist ein wenig informell, wir meinen ein Programm in einer gängigen Computersprache und denken nur daran, dass wir die typischen Ein- und Ausgabefunktionen, Verzweigungsbefehle sowie Unterprogrammstrukturen darin zur Verfügung haben:

(i) Berechenbarkeit im Sinne dessen, dass man ein passendes Computerprogramm schreiben kann

(ii) Berechenbarkeit im Sinn des Begriffs der $\mu-$ Rekursivität

(iii) Berechenbarkeit als Berechenbarkeit durch eine Turing-Maschine.

Mit (i) knüpfen wir an schon Bekanntes an, was das Ganze verständlicher machen sollte.

2. Die Klasse der $\mu-$ rekursiven Funktionen

Zunächst überzeugen wir uns, dass folgende Funktionen berechenbar sind, indem wir uns Computerprogramme dafür ausdenken:

$$\begin{array}{rccc} P_i^k: & \mathbb{N}^k & \to & \mathbb{N} \\ & (n_1,...,n_k) & \mapsto & n_i \end{array}, \text{ die Projektionen, } k \geq 1$$

C_0^0, die konstante Funktion mit Wert Null, als nullstellige Funktion,

$$\begin{array}{rccc} S: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & n+1 \end{array}, \text{ die Nachfolgerfunktion.}$$

Ferner ist klar, dass mit berechenbaren Funktionen $f, g_1, ..., g_m$ mit $m-stelligem\ f$ und $k-stelligen$ $g_1, ..., g_m$ auch gilt:

(**Einsetzung:**) $h(n_1, ..., n_k) = f(g_1(n_1, ..., n_k), ..., g_m(n_1, ..., n_k))$ ist wieder berechenbar.

Weiter ist mit berechenbaren f, g der offensichtlich passenden Stellenzahlen auch die durch Rekursion wie folgt definierte Funktion h berechenbar:

Primitive Rekursion ($\overrightarrow{\mathbf{x}}$ darf die leere Folge sein) **:**

$$\begin{array}{l} h\left(\overrightarrow{\mathbf{x}}, 0\right) = f\left(\overrightarrow{\mathbf{x}}\right), \\ h\left(\overrightarrow{\mathbf{x}}, n+1\right) = g\left(\overrightarrow{\mathbf{x}}, n, h\left(\overrightarrow{\mathbf{x}}, n\right)\right) \end{array}.$$

Bemerkung: Für die leere Folge $\overrightarrow{\mathbf{x}}$ ist $f\left(\overrightarrow{\mathbf{x}}\right)$ eine Konstante im Sinne einer nullstelligen Funktion, darum war es bequem, mit C_0^0 als nullstelliger Funktion zu beginnen. Wir sehen sofort, dass die nullstelligen Funktionen mit beliebigem konstantem Wert d dann durch die Terme $S...SC_0^0$ darstellbar sind. Insbesondere versteht man die nullstelligen Funktionen gut aus der Sicht von Computerprogrammen: Man definiert eine Funktion ohne Eingabe und gibt einfach den konstanten Wert aus.

Schließlich ist mit berechenbarem f mit der Eigenschaft $\forall \overrightarrow{\mathbf{x}} \exists y f\left(\overrightarrow{\mathbf{x}}, y\right) = 0$ die Funktion

$$\begin{array}{l} (\mu- \textbf{ Operator:}) \\ g\left(\overrightarrow{\mathbf{x}}\right) \ = \ \mu_y f\left(\overrightarrow{\mathbf{x}}, y\right) \ = \ 0 \end{array}$$

wieder berechenbar. Wir definieren daher:

Definition 22 (primitiv rekursive und rekursive Funktionen). *Die primitiv rekursiven Funktionen bilden die kleinste Klasse von Funktionen, welche S, C_0^0 und die U_i^k enthalten und unter den Funktionsbildungsprozessen der Einsetzung und der primitiven Rekursion abgeschlossen sind. Die rekursiven Funktionen sind die, welche sich aus denselben Grundfunktionen mit den Aufbauschemata eineschließlich des $\mu-$Operators ergeben.*

Dass die rekursiven Funktionen mit Computerprogrammen prinzipiell zu berechnen sind, ist ziemlich klar. Wir wissen aus mathematischer Erfahrung, wie Rekursion funktioniert. Machen wir uns das noch für den $\mu-$*Operator* klar: $\overrightarrow{\mathbf{x}}$ ist eingegeben. Nun wird der Reihe nach gebildet (man denkt an ein Unterprogramm): $f\left(\overrightarrow{\mathbf{x}}, 0\right), ..., f\left(\overrightarrow{\mathbf{x}}, n\right), ...$, so lange, bis man die kleinste Zahl k mit $f\left(\overrightarrow{\mathbf{x}}, k\right) = 0$ gefunden hat. Dann gibt man diese Zahl k aus. Wendet man dagegen den $\mu-$*Operator* an, ohne $\forall \overrightarrow{\mathbf{x}} \exists y f\left(\overrightarrow{\mathbf{x}}, y\right) = 0$ voraussetzen zu können, so wird dies Programm bei Eingabe einiger Werte von $\overrightarrow{\mathbf{x}}$ nicht stoppen, bei Eingabe anderer Werte von $\overrightarrow{\mathbf{x}}$ ein Resultat liefern. Die Funktion ist in diesem Sinne nur partiell definiert. Wir definieren daher:

Definition 23 (partielle rekursive Funktionen). *Die Menge der partiellen rekursiven Funktionen ist die kleinste Menge von Funktionen, welche die Grundfunktionen enthält und unter Einsetzung, Rekursion und $\mu-$Operator ohne die einschränkende Bedingung $\forall \overrightarrow{\mathbf{x}} \exists y f\left(\overrightarrow{\mathbf{x}}, y\right) = 0$ abgeschlossen ist.*

Wir wenden uns nunmehr zunächst der Klasse der rekursiven Funktionen zu, die wir verdeutlichend auch totale rekursive Funktionen nennen. Einmal zur Ilustration, dann aber auch für theoretische Zwecke zeigen wir von einer Reihe konkreter Funktionen, dass sie (total) rekursiv sind:

SATZ 8. *Die folgenden Funktionen sind rekursiv:*

$$\begin{aligned} & \textit{Die konstante nullstellige Funktion mit Wert } c, \\ f\left(\overrightarrow{\mathbf{x}}\right) &= c,\ \overrightarrow{\mathbf{x}} \in \mathbb{N}^k,\ k \geq 1 \textit{ fest, für jede Zahl } c \in \mathbb{N}, \\ f(x,y) &= x \overset{\bullet}{-} y := \begin{cases} x-y, \textit{ wenn } x-y \geq 0, \\ 0, \textit{ wenn } x < y \end{cases} \\ f(x,y) &= x+y, \\ f(x,y) &= x \cdot y,\ f(n) = n!, \\ f(x,y) &= x^y. \end{aligned}$$

Beweis: Die konstante Funktion auf $\mathbb{N}^k$ für $k \geq 1$ mit Wert c erhält man mit $f\left(\overrightarrow{\mathbf{x}}\right) = \underbrace{S...S}_{c \text{ mal}} C_0^0$. Dabei denkt man sich $f\left(\overrightarrow{\mathbf{x}}\right) = C_0^0$ als Grenzfall des Einsetzungsschemas, null Funktionen von $\overrightarrow{\mathbf{x}}$ werden in die nullstellige C_0^0 eingesetzt. (Wenn das nicht so genehm ist, denke man schadlos alle Funktionen $C_0^n\left(\overrightarrow{\mathbf{x}}\right) = 0$ als Grundfunktionen.)

Die Addition bekommt man mit dem Rekursionsschema

$$\begin{aligned} h(x,0) &= x+0 = x \\ h(x,n+1) &= x+(n+1) = S(x+n) = S(h(x,n)). \end{aligned}$$

Dabei ist $g(x) = x = P_1^1(x)$ bereits rekursiv. Ferner ist im Schema zu wählen: $g(x,n,y) = S\left(P_3^3(x,n,y)\right)$, damit wird $h(x,n+1) = g(x,n,h(x,n))$. (Vgl. auch das verallgemeinerte Einsetzungsschema im nächsten Satz.)

Die Multiplikation und Exponentiation definiert man dann aufbauend mit dem Rekursionsschema (Übung).

zu $x \overset{\bullet}{-} y$ definiert man zuerst

$$g(x) = x \overset{\bullet}{-} 1$$

durch Rekursion mit

$$\begin{aligned} g(0) &= 0 \\ g(n+1) &= n, \end{aligned}$$

dann gelingt die Definition von $h(x,y) = x \overset{\bullet}{-} y$ durch Rekursion so:

$$\begin{aligned} h(x,0) &= x \overset{\bullet}{-} 0 = x, \\ h(x,n+1) &= x \overset{\bullet}{-} (n+1) = \left(x \overset{\bullet}{-} n\right) \overset{\bullet}{-} 1. \end{aligned}$$

Wir haben auch noch einen Satz, der die Abgeschlossenheit der Klasse der rekursiven Funktionen noch unter einigen weiteren Funktionsbildungsprozessen zeigt:

SATZ 9. *Folgendes Schema definiert eine rekursive Funktion f:*

$$\begin{aligned} & \textbf{\textit{Verallgemeinerte Einsetzung}} \textit{ } (g, g_1, ..., g_m \textit{ rekursiv}) : \\ f(x_1,...,x_n) &= g\left(x_{i_1},...,x_{i_k}, g_1\left(x_{k_1(1)},...,x_{k_1(n_1)}\right),...,g_m\left(x_{k_m(1)},...,x_{k_m(n_m)}\right)\right), \\ \textit{mit } k_j(s) &\in \{1,...n\} \textit{ für } 1 \leq j \leq m,\ 1 \leq s \leq n_j. \end{aligned}$$

Beweis: Für die verallgemeinerte Einsetzung setze man für x_{i_r} [bzw. $x_{k_j(s)}$] ein: $P_{i_r}^n\left(\overrightarrow{\mathbf{x}}\right)$ bzw. $P_{k_j(s)}^n\left(\overrightarrow{\mathbf{x}}\right)$, wobei $\overrightarrow{\mathbf{x}} = (x_1,...,x_n)$. Damit ist das Schema auf die normierte zunächst eingeführte Einsetzung zurückgeführt.■

Für den systematischen Aufbau, aber auch für die Definition spezieller wichtiger rekursiver Funktionen benötigen wir den Umgang mit rekursiven Relationen.

DEFINITION 24 (primitiv rekursive und rekursive Relationen, Entscheidbarkeit einer Relation). *Für eine Relation $R \subset \mathbb{N}^k$, $k \geq 1$, definieren wir die charakteristische Funktion*

$$\chi_R\left(\overrightarrow{\mathbf{x}}\right) = \begin{cases} 0, \text{ wenn } \overrightarrow{\mathbf{x}} \in R, \\ 1 \text{ sonst.} \end{cases}$$

R heißt (primitiv) rekursiv, wenn χ_R es ist. Wir werden auch $R\overrightarrow{\mathbf{x}}$ schreiben für $\overrightarrow{\mathbf{x}} \in R$. Man nennt rekursive Relationen auch entscheidbar, da man mit der Berechenbarkeit ihrer charakteristischen Funktion auch ein algorithmisches Entscheidungsverfahren besitzt, mit dem entschieden werden kann, ob ein $\overrightarrow{\mathbf{x}} \in \mathbb{N}^k$ zur Menge gehört oder nicht.

Beispiele: $R = \{0\}$ ist primitiv rekursiv, da $\chi_R(0) = 0$, $\chi_R(n+1) = 0$. $U = \{(x,y) | x < y\}$ ist primitiv rekursiv, da $\chi_U(x,y) = 1 \overset{\bullet}{-} \chi_R\left(y \overset{\bullet}{-} x\right)$ (das nächste Lemma zeigt u.a. die Einsetzbarkeit rekursiver Funktionsterme).

LEMMA 8. *(i) Die Klassen der rekursiven bzw. primitiv rekursiven Relationen sind abgeschlossen unter Vereinigung, Durchschnitt und Komplement. Ferner definiert mit (pr.) rekursiver Relation $R \subset \mathbb{N}^k$ und rekursiven Funktionen auch $W = \left\{\overrightarrow{\mathbf{x}} \middle| \left(f_1\left(\overrightarrow{\mathbf{x}}\right), ..., f_k\left(\overrightarrow{\mathbf{x}}\right)\right) \in R\right\}$ eine (pr.) rekursive Relation.*
(ii) Die Klassen sind auch unter Definition durch Fallunterscheidung mit rekursiver Partition $\mathbb{N} = Q_1 \cup ... \cup Q_n$ (disjunkte Vereinigung) abgeschlossen, wenn Q_i (pr.) rekursiv für $1 \leq i \leq n$. Ebenso wird duch solche Fallunterscheidung eine (pr.) rekursive Funktion definiert. Die zugehörigen Schemata sind:

$$\begin{aligned} W &= (R_1 \cap Q_1) \cup ... \cup (R_n \cap Q_n), \text{ alle } R_i \text{ (pr.) rekursiv,} \\ f\left(\overrightarrow{\mathbf{x}}\right) &= \sum_{i=1}^{n} f_i\left(\overrightarrow{\mathbf{x}}\right)\left(1 \overset{\bullet}{-} \chi_{Q_i}\left(\overrightarrow{\mathbf{x}}\right)\right), \text{ alle } f_i \text{ (pr.) rekursiv} \end{aligned}$$

(iii) Seien die Relation R und die Funktion f (pr.) rekursiv. dann sind $D = \left\{\overrightarrow{\mathbf{x}} \middle| \left(\exists y \leq f\left(\overrightarrow{\mathbf{x}}\right)\right) R\overrightarrow{\mathbf{x}}y\right\}$ und $E = \left\{\overrightarrow{\mathbf{x}} \middle| \left(\forall y \leq f\left(\overrightarrow{\mathbf{x}}\right)\right) R\overrightarrow{\mathbf{x}}y\right\}$ (pr.) rekursiv. (Insbesondere gilt das dann auch für die konstanten Funktionen $f\left(\overrightarrow{\mathbf{x}}\right) = a$.)
(iv) Wenn f eine primitiv rekursive Funktion ist und R eine primitiv rekursive Relation, dann ist

$$g\left(\overrightarrow{\mathbf{x}}\right) = \mu_{y \leq f\left(\overrightarrow{\mathbf{x}}\right)} R\overrightarrow{\mathbf{x}}y$$

eine primitiv rekursive Funktion, falls gilt: $\forall \overrightarrow{\mathbf{x}}\left(\exists y \leq f\left(\overrightarrow{\mathbf{x}}\right)\right) R\overrightarrow{\mathbf{x}}y$.

Beweis: *(i)* $\chi_{R\cap Q}\left(\overrightarrow{\mathbf{x}}\right) = 1 \overset{\bullet}{-} \left(1 \overset{\bullet}{-} \chi_R\left(\overrightarrow{\mathbf{x}}\right)\right)\left(1 \overset{\bullet}{-} \chi_Q\left(\overrightarrow{\mathbf{x}}\right)\right)$, $\chi_{R\cup Q} = \chi_R \cdot \chi_Q$, $\chi_{\overline{R}}\left(\overrightarrow{\mathbf{x}}\right) = 1 \overset{\bullet}{-} \chi_R\left(\overrightarrow{\mathbf{x}}\right)$.
Für die Einsetzung hat man

$$\chi_W\left(\overrightarrow{\mathbf{x}}\right) = \chi_R\left(f_1\left(\overrightarrow{\mathbf{x}}\right), ..., f_k\left(\overrightarrow{\mathbf{x}}\right)\right).$$

Dabei kann man dann auch noch verallgemeinerte Einsetzung wie oben für die rekursiven Funktionen eingeführt benutzen.
(ii) Die Definitionen wurden bereits so geschrieben, dass die Behauptung klar ist.
(iii) Wir definieren durch primitive Rekursion:

$$\begin{aligned} g\left(\overrightarrow{\mathbf{x}}, 0\right) &= \chi_R\left(\overrightarrow{\mathbf{x}}, 0\right), \\ g\left(\overrightarrow{\mathbf{x}}, y+1\right) &= g\left(\overrightarrow{\mathbf{x}}, y\right) \cdot \chi_R\left(\overrightarrow{\mathbf{x}}, y+1\right). \end{aligned}$$

Dann hat man $\overrightarrow{\mathbf{x}} \in D \iff g\left(\overrightarrow{\mathbf{x}}, f\left(\overrightarrow{\mathbf{x}}\right)\right) = 0$. Daraus ergibt sich das Resultat für E über $E\overrightarrow{\mathbf{x}} \iff \neg \left(\exists y \leq f\left(\overrightarrow{\mathbf{x}}\right)\right) \neg R\overrightarrow{\mathbf{x}}y$ mit den Booleschen Operationen.
(iv) Definiere

$$\begin{aligned} h\left(\overrightarrow{\mathbf{x}}, 0\right) &= \begin{cases} 1, \text{ wenn } \neg R\overrightarrow{\mathbf{x}}0, \\ 0 \text{ sonst.} \end{cases}, \\ h\left(\overrightarrow{\mathbf{x}}, y+1\right) &= \begin{cases} h\left(\overrightarrow{\mathbf{x}}, y\right) + 1, \text{ wenn } (\forall z \leq y+1) \neg R\overrightarrow{\mathbf{x}}y, \\ h\left(\overrightarrow{\mathbf{x}}, y\right) \text{ sonst.} \end{cases} \end{aligned}$$

Das ist eine primitiv rekursive Funktion, wenn R primitiv rekursives Prädikat ist, gemäß *(iii)*. Nun ist die gewünschte Funktion

$$g\left(\overrightarrow{\mathbf{x}}\right) = h\left(\overrightarrow{\mathbf{x}}, f\left(\overrightarrow{\mathbf{x}}\right)\right)$$

und damit wieder primitiv rekursiv.■

Das Lemma erlaubt nunmehr leicht, eine Fülle von Funktionen oder Relationen als (primitiv) rekursiv zu erweisen:

SATZ 10. *Folgende Funktionen sind primitiv rekursiv:*

$$\begin{aligned}
(i)\ p(n) &= n.\ \textit{Primzahl}\\
(ii)\ f(n_0,...,n_{k-1}) &= \langle n_0,...,n_{k-1}\rangle = 2^{n_0}\cdot 3^{n_1}\cdot ...\cdot p(k-1)^{n_{k-1}+1}-1\ \textit{(Folgen-Nummer)}\\
(iii)\ L(\langle n_0,...,n_{k-1}\rangle) &= k,\ \textit{(Länge der Folge)}\\
(iv)\ \langle n_0,...,n_{k-1}\rangle_i &= n_i,\ 0\le i\le k-1.\ \textit{(Komponenten der Folge)}
\end{aligned}$$

Beweis: $x \mid y \iff (\exists u\le y)(u\cdot x = y)$, für $y>0$. Also ist mit dem Lemma die Teilbarkeit eine primitiv rekursive Relation. Daraus folgt, dass das Prädikat 'Primzahl' primitiv rekursiv ist, nämlich

$$Px \iff x\ge 2\wedge(\forall y\le x)(y\mid x \implies y=1\vee y=x).$$

Daraus ergibt sich (i) mit dem Lemma (iv) so:

$$\begin{aligned}
p(0) &= 2\\
p(n+1) &= \mu_{y\le n!+1}(y>p(n)\wedge Py).
\end{aligned}$$

(ii) ergibt sich daraus, dass $p(n)$ rekursiv ist und ebenso das Produkt, Nachfolgerbildung und Abziehen von 1.

(iii) stimmt mit (wieder wird das Lemma angewandt):

$$L(n) = \left(\mu_{m\le n} p(m) \nmid n+1\right) - 1.$$

(iv) Man hat für $i<k-1$: $n_i = \max_{y\le n}(p(i)^y \mid n+1) = \mu_{z\le n} p(i)^z \nmid n+1$. Für $i=k-1$ ist noch 1 abzuziehen. Für $i>k-1$ definieren wir den Wert als Null.■

Bemerkung: Wir werden von der eingeführten primitiv rekursiven Folgencodierung starken Gebrauch machen, wenn es um Gödelisierung der nun einzuführenden Turingmaschinen geht, dann auch für die Gödelisierung der Prädikatenlogik.

3. Turing-Berechenbarkeit

Der Begriff der Turing-Berechenbarkeit dient einmal dazu, ihre Äquivalenz mit der $\mu-$ Rekursivität zu zeigen und den Begriff der 'Computer-Berechnbarkeit' dabei durch einen vollständig präzisen zu ersetzen. Damit soll die folgende These von Church gestützt werden. Die wichtige Frage lautet: Erschöpfen die rekursiven Funktionen wirklich alles Berechenbare? Wenn es nun gelingt, für verschiedene Versionen von 'Berechenbarkeit' zu zeigen: Stets kommt dieselbe Klasse von Funktionen heraus, und das ist die der rekursiven Funktionen. Dies Resultat hat man auf erdenkliche Weisen gesichert, für noch einige Versionen mehr als hier besprochen werden, und das führt auf die

These von Church: Alle intuitiv 'berechenbaren' Funktionen sind rekursiv.

Niemand kann mehr daran glauben, etwas 'Berechenbares' zu finden, das nicht eine rekursive Funktion ist.

Aber die Turing-Berechenbarkeit führt auch technisch weiter, wir können damit präzise die systematisch wichtigen universellen rekursiven Funktion und dann auch universelle rekursiv aufzählbare Prädikate konstruieren, woraus die wichtigsten Resultate fließen.

3.1. Begriff der Turingmaschine. Es gibt mehrere Versionen davon ('Einband', 'Mehrband'), der Erfinder ist Alan Turing, erste Hälfte 20.Jh., von ihm stammen auch wesentliche theoretische Resultate dazu. Berühmt wurde er auch durch seine Mitarbeit bei der Entschlüsselung der 'Enigma'-Maschine im 2. Weltkrieg.

Hier die Einband-Version:

DEFINITION 25 (Einband-Turing-Maschine). *Eine solche Maschine besteht aus einem Datenträger, das ist ein eindimensionales* ***Band****, das in klare Felder (oder Zellen) eingeteilt ist. Das Band ist (potentiell) beidseitig unendlich, es werden jeweils nur endlich viele Felder genutzt, und die Felder sind mit ganzen Zahlen numeriert.*
Die Felder haben Inhalte aus einem Alphabet, es genügt das Alphabet $\{\square,*\}$, *Leerzeichen und Stern. Stets sind alle bis auf endlich viele Felder leer.*

*Zum Band gehört ein einziger '**Lesekopf**', der jeweils auf einem wohlbestimmten Feld sitzt und den Inhalt des Feldes liest.*
Das Verhalten der Maschine wird von einem Programm gesteuert, das endlich viele Befehlszeilen der Form

$$c_1bac_2$$

enthält, mit der Bedeutung: Bei internem Zustand c_1 und Inhalt $b \in \{\square, *\}$ des Beobachtungsfeldes führe Aktion $a \in \{d\square, d*, r, l, s\}$ aus und gehe in internen Zustand c_2 über. Dabei sind die Aktionen im Einzelnen: Drucke Leerzeichen auf das aktive Feld, drucke $*$ auf das aktive Feld, gehe nach rechts / nach links (ohne den Bandinhalt zu ändern), schließlich s für 'stoppe'. Die internen Zustände sind natürliche Zahlen, es gibt einen Anfangszustand 0, *und einen Endzustand, der mit der größten Zahl repräsentiert wird und auf Aktion s folgt. Er tritt nicht als Anfang einer Befehlszeile auf. Wesentlich ist folgende Konsistenzbedingung, welche das Verhalten der Maschine deterministisch macht: In einem Programm darf es höchstens eine Befehlszeile beginnend mit c_1b geben.*

Hinweis zum Verständnis: Die internen Zustände sind so etwas wie Befehlszeilen-Nummern in üblichen (etwas altertümlichen) Programmen. Was heißt es nun, dass eine Funktion $f : \mathbb{N}^k \to \mathbb{N}$ durch eine Turingmaschine berechnet wird?

DEFINITION 26. *Die Turingmaschine M (dargestellt durch die Folge ihrer Befehlszeilen-Quadrupel) berechnet $f : \mathbb{N}^k \to \mathbb{N}$ genau dann, wenn für alle $x_1, ..., x_k \in \mathbb{N}$ Folgendes gilt: Angesetzt auf den Bandinhalt $x_1 + 1$ Sterne in Folge, Leerzeichen, $x_2 + 1$ Sterne in Folge, Leerzeichen,..., $x_k + 1$ Sterne in Folge, Leerzeichen, startend auf dem letzten Leerzeichen, stoppt M nach endlich vielen Schritten, und dann steht der Funktionswert $f(x_1, ..., x_k)$ hinter dem letzten Leerzeichen der Argumentfolge in der Form von $f(x_1, ..., x_k) + 1$ Sternen, und der Lesekopf steht auf dem Leerzeichen hinter dem Funktionswert.*

DEFINITION 27. *Die Turingmaschine M stellt die partielle Funktion $A \to \mathbb{N}$ mit $A \subset \mathbb{N}^k$ genau dann dar, wenn sie für $\overrightarrow{\mathbf{x}} \in A$ wie in der vorigen Definition nach endlich vielen Schritten den Funktionswert produziert und für $\overrightarrow{\mathbf{x}} \notin A$ nicht stoppt.*

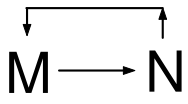
Für das Folgende ist es wichtig, Turingmaschinen sinnvoll zu verketten, um aus einfachen neue zu definieren, die verlangte größere Arbeiten bewältigen. Dazu definieren wir:

DEFINITION 28. *Die Verkettung M_1M_2 (Reihenfolge, wie man sie liest, zuerst also M_1) ist die Maschine, deren Programm einfach das von M_2 hinter das von M_1 schreibt, aber so, dass alle Zustände der Tafel von M_2 durch neue ersetzt werden, außer dem Endzustand. Ferner werden Endzustandszeilen von M_1, also c_kbsc' ersetzt durch $dbad'$, wobei $dbad'$ die (frühere) Anfangsbefehlszeile von M_2 beginnend mit db ist.*

DEFINITION 29. *Eine Diagrammdarstellung einer Turingmaschine ist ein Flussdiagramm aufgebaut aus Vekrettungen von von Maschinensymbolen als Knoten und mit Verzweigungen der Form*

$$\begin{array}{l} M_1...M_{k_1} \overset{*}{\to} N_1...N_{k_2} \\ \downarrow \square \\ U_1...U_{k_3} \end{array}$$

und Rückkopplungen der Form (auch verzweigt je nach Beobachtung von $*$ oder $\square$).



.

Offensichtlich haben wir:

LEMMA 9. *Jedes Diagramm, das mit Symbolen bereits definierter Turingmaschinen gebildet wird, definiert eine neue Turingmaschine, eindeutig in der Wirkungsweise.*

Für den anschließenden Satz der Äquivalenz von Rekursivität und Turing- Berechenbarkeit benötigen wir einige elementare Turing-Maschinen, aus denen wir dann genug zusammensetzen können, um alle $\mu - rekursiven$ Funktionen als Turing-berechenbar zu erkennen:

LEMMA 10. *Es gibt Turing-Maschinen (d.h. hier Programme), welche Folgendes leisten:*

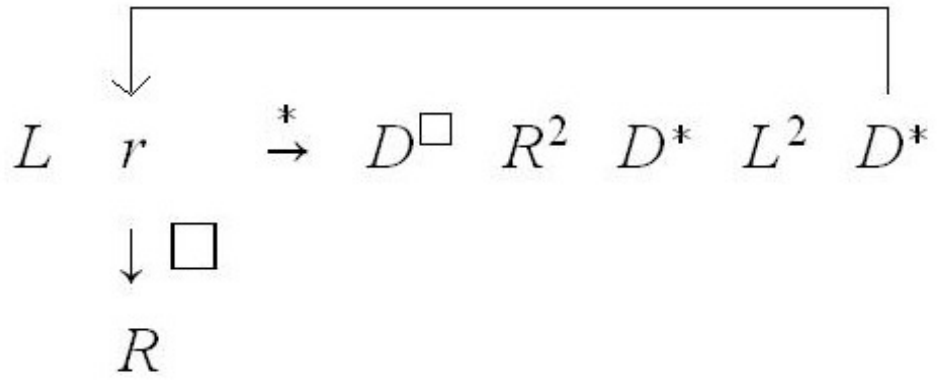
$D^*, D^\square$	*druckt auf das Arbeitsfeld* $*$ */ druckt auf das Arbeitsfeld Leerzeichen*
l	*Der Lesekopf geht ein Feld nach links, sonst nichts*
r	*analog, nach rechts*
L	*geht nach links bis zum ersten Leerfeld, bleibt dort stehen*
R	*analog, bleibt auf erstem Leerfeld rechts stehen*
K_n	*kopiert n Blöcke von Sternsymbolen, durch* $\square$ *getrennt, links vom Lesekopf, rechts von der Stelle des Lesekopfes, bleibt auf dem Leerfeld unmittelbar rechts von der Kopie stehen. Also macht* K_n *aus* $\square S_1\square S_2 ... \square S_n \overset{\downarrow}{\square}$ *Folgendes:* $\square S_1\square S_2 ... \square S_n\square S_1\square S_2 ... \square S_n \overset{\downarrow}{\square}$
T	*verschiebt einen Block von Sternsymbolen ein Feld nach links, angesetzt rechts von diesem Block, bleibt rechts vom neuen Sternblock stehen. (Das 'eingesetzte' Feld ist leer.)*
V	*tilgt für* $\overset{m.\ Feld}{\square}\ S_1\square S_2 \overset{\downarrow}{\square}$ *den Sternblock* S_1 *und schiebt* S_2 *darüber, endet so:* $\overset{m.\ Feld}{\square}\ \overset{\downarrow}{S_2}\square$
E	*Endmaschine, startend mit* $\overset{m.\ Feld}{\square}\ \square W \square \overset{\downarrow}{S}\square$ *mit einem Wort W aus Sternblöcken, welche durch* $\square$ *getrennt sind, endet mit* $\overset{m.\ Feld}{\square}\ \overset{\downarrow}{S}\square$

Zur Bedeutung der Maschinen: Der Kopiervorgang wird offenbar wichtig für die Projektionsfunktionen und die Nachfolgerfunktion, ebenso dann auch für das Einsetzen und die Rekursion. Die Translationsmaschine (allerdings nach rechts, das geht natürlich analog) wird benötigt, um '$\square\square$' als Wegmarke zu setzen. Dann können mit V, E Zwischenrechnungen getilgt und das Endresultat an die Argumentfolge gehängt werden. Das gibt dann schon den Plan für den Nachweis der Turing-Berechenbarkeit $\mu - rekursiver$ Funktionen.

Zum Beweis des Lemmas: Zur Illustration geben wir ein Programm für R (Übung: Progemme für r, l, L):

$$0 * r1$$
$$0\square r1$$
$$1\square s2$$
$$1 * r1$$

Wir geben in Diagrammform die Maschine K_1 (Exponenten bedeuten Iteration derselben Maschine):



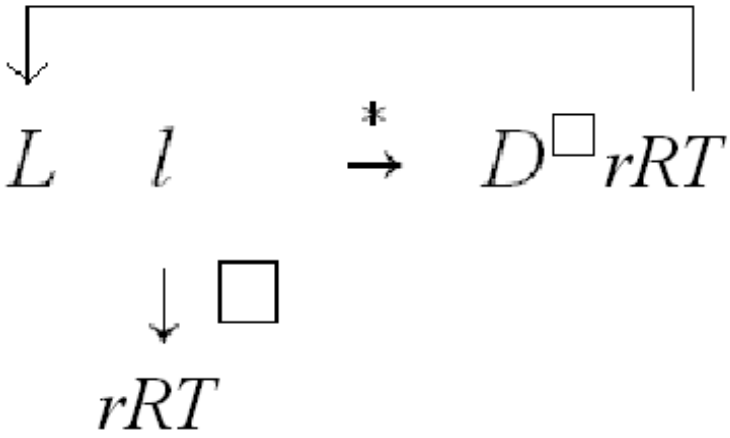
Erläuterung der Funktionsweise: Die Maschine geht mit L zum Leerzeichen vor dem zu kopierenden Block von Sternsymbolen, dann ein Feld nach rechts, findet dort $*$, löscht diesen, geht mit R^2 auf das Feld, auf das der erste Stern zu kopieren ist, druckt dort $*$, geht mit L^2 auf das Feld, auf dem der mittlerweile gelöschte Stern des Ursprungblock lag, erneuert diesen, geht nach rechts, nun wiederholt sich der Vorgang mit dem zweiten Stern des Ursprungsblocks. Ist der Ursprungsblock zu Ende, landet man mit r auf dem Leerfeld hinter dem (rekonstruierten) Ursprungsblock und geht mit R auf das Leerfeld rechts hinter dem kopierten Block.

Für das Diagramm für K_n bildet man zunächst M_n, indem man im Diagramm für K_1 einfach R, L ersetzt durch R^n, L^n. Die Maschine M_n kopiert also den n. Sternblock links vom Arbeitsfeld dahinter. Dann bekommt man

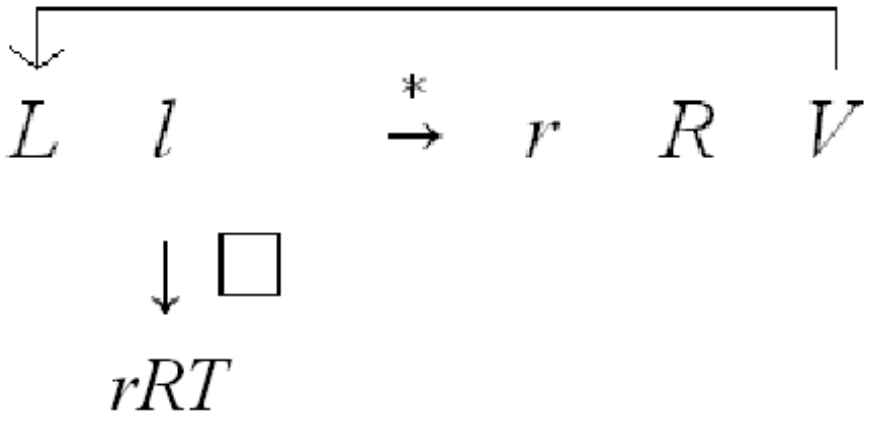
$$K_n = M_n^n.$$

Ein Diagramm für T zu bilden, lassen wir als Übung.

Hier ist ein Diagramm für V :



Schließlich lässt sich E so realisieren:



Wir kommen nunmehr zum angestrebten

SATZ 2. *Eine (totale) Funktion $f : \mathbb{N}^k \to \mathbb{N}$ ist genau dann $\mu-$ rekursiv, wenn sie Turing-berechenbar ist.*

Beweis:

Erster Teil: Jede $\mu-$ rekursive Funktion ist Turing-berechenbar. Das wird natürlich induktiv über den Aufbau der rekursiven Funktion gezeigt. Für die technische Durchführung ist es sehr wichtig,

neben der erwähnten Normierung (Argumentfolge als Folge von Sternblöcken, durch Leerfelder getrennt, $n+1$ Sterne für die Darstellung der Zahl n, Maschine steht auf dem Leerfeld hinter den Argumenten und bleibt hinter dem nachgestellten Funktionswert stehen) noch folgende anzubringen: Ein etwa vorhandener Bandinhalt **vor** den Argumenten bleibt völlig unberührt.

Wir zeigen also:

a) Die Funktionen P_k^n, C_0^0 und S sind Turing-berechenbar. Für C_0^0 ist das unmittelbar klar. Für S muss man hinter dem Start-Leerfeld den Argumentwert reproduzieren und dann noch ein Feld mit $*$ beschreiben. Also wird S dargestellt durch

$$K_1 D^* r.$$

Die Projektionsfunktionen P_k^n bekommt man mit

$$M_{n-k+1},$$

M_i wurde oben eingeführt als Verallgemeinerung von K_1.

b) Wir setzen Maschinen $M_f, M_{g_1}, ..., M_{g_k}$ voraus, welche $f, g_1, ..., g_k$ berechnen, alle g_i $n-stellig$, f $k-stellig$.Wir wollen eine Maschine für $f\left(g_1\left(\overrightarrow{\mathbf{x}}\right), ..., g_k\left(\overrightarrow{\mathbf{x}}\right)\right)$ produzieren. Eine Idee ist folgende: Angesetzt auf $\overrightarrow{\mathbf{x}}$ berechnen wir zunächst $g_1\left(\overrightarrow{\mathbf{x}}\right)$, dann kopieren wir $\overrightarrow{\mathbf{x}}$ über den Wert $g_1\left(\overrightarrow{\mathbf{x}}\right)$ hinweg, berechnen $g_2\left(\overrightarrow{\mathbf{x}}\right)$, kopieren die vorige Kopie von $\overrightarrow{\mathbf{x}}$ über $g_2\left(\overrightarrow{\mathbf{x}}\right)$ hinweg, schließlich steht da:

$$\overrightarrow{\mathbf{x}}\square g_1\left(\overrightarrow{\mathbf{x}}\right)\square\overrightarrow{\mathbf{x}}\square g_2\left(\overrightarrow{\mathbf{x}}\right)...\overrightarrow{\mathbf{x}}\square g_n\left(\overrightarrow{\mathbf{x}}\right),$$

und die Maschine sitzt auf dem Leerfeld rechts von $g_n\left(\overrightarrow{\mathbf{x}}\right)$. Nennen wir die Maschine, welche jeweils $\overrightarrow{\mathbf{x}}$ über den nächsten Sternblock hinweg kopiert, $K_{n,1}$. Dann wird das Beschriebene realisiert von

$$M_{g_1} K_{n,1} M_{g_2} K_{n,1} ... M_{g_n}.$$

Wir machen dabei Gebrauch von der angegebenen Normierung, dass die Berechnung von $g_2\left(\overrightarrow{\mathbf{x}}\right)$ den Inhalt links von der ersten Kopie von $\overrightarrow{\mathbf{x}}$ nicht verändert, usw.

Anschließend werden alle Zwischenkopien von $\overrightarrow{\mathbf{x}}$ gelöscht, mit

$$\left(V^n L\right)^{k-1}, \text{ für } k>1, \text{ für } k=1 \text{ ergibt sich konsequent } \left(V^n L\right)^0,$$

für $k=1$ ergibt sich konsequent $\left(V^n L\right)^0$, also die Maschine, die gar nichts tut, dann entfällt dieser Schritt einfach.

Nunmehr wird M_f angewandt, es bleiben nur noch die Funktionswerte $g_i\left(\overrightarrow{\mathbf{x}}\right)$ zu löschen und $f\left(g_1\left(\overrightarrow{\mathbf{x}}\right), ..., g_k\left(\overrightarrow{\mathbf{x}}\right)\right)$ heranzurücken durch

$$V^k.$$

Die Maschine

$$M_{g_1} K_{n,1} M_{g_2} K_{n,1} ... M_{g_n} \left(V^n L\right)^{k-1} V^k$$

leistet also das Verlangte. Zu beachten ist, dass Verschiebungen nach links niemals in das ursprüngliche Argument hineinragen.

c) Wir setzen Maschinen M_f für f und M_g für g voraus, und h entstehe aus f, g durch primitive Rekursion. Wir wollen eine Turingmaschine M_h für h konstruieren.

Die Idee der folgenden Konstruktion ist einfach die: Berechne der Reihe nach (dabei führen wir vereinfachte Notation ein):

$$f\left(\overrightarrow{\mathbf{x}}\right) = f_0, g\left(\overrightarrow{\mathbf{x}}, 1, f_0\right) = f_1, ..., usw., g\left(\overrightarrow{\mathbf{x}}, y, f_{y-1}\right) = f_y.$$

Der zu berechnende Funktionswert ist f_y, anschließend muss dieser Wert über die zu löschenden Zwischenergebnisse an die Argumente herangerückt werden. Die Ausführung macht ein wenig Mühe, weil man stets zur Berechnung von $h\left(\overrightarrow{\mathbf{x}}, y-k, h\left(\overrightarrow{\mathbf{x}}, y-k-1\right)\right)$ die Argumente an die richtige Stelle bringen muss, dazu kontrollieren, wann die Iteration abbricht, schließlich noch 'Aufräumen'.

Dazu gehen wir so vor: Die Startposition ist

$$\square\overrightarrow{\mathbf{x}}\square\overset{\downarrow}{y}\square.$$

Es sei noch einmal erinnert, dass $\overrightarrow{\mathbf{x}}$ genau lautet:

$$\underbrace{*...*}_{x_1+1}\square\underbrace{*...*}_{x_1+1}\square...\square\underbrace{*...*}_{x_n+1}$$

Zunächst produzieren wir aus technischen Gründen noch einmal y mit K_1 zu

$$\Box\vec{\mathbf{x}}\Box y\Box y\overset{\downarrow}{\Box}$$

mit $K_{n,2}$:

$$\Box\vec{\mathbf{x}}\Box y\Box y\Box\vec{\mathbf{x}}\overset{\downarrow}{\Box}.$$

Dann berechnen wir mit M_f :

$$\Box\vec{\mathbf{x}}\Box y\Box y\Box\vec{\mathbf{x}}\Box f\left(\vec{\mathbf{x}}\right)\overset{\downarrow}{\Box}.$$

Wir bezeichnen nun der Einfachheit halber $f\left(\vec{\mathbf{x}}\right) = f_0$, $g\left(\vec{\mathbf{x}}, 1, f_0\right) = f_1, ..., usw.$, $g\left(\vec{\mathbf{x}}, y, f_{y-1}\right) = f_y$. Nun verschieben wir den Block $f\left(\vec{\mathbf{x}}\right)$ um zwei Felder nach rechts und hinterlassen in den Lücken Leerfelder:

$$\Box\vec{\mathbf{x}}\Box y\Box y\Box\vec{\mathbf{x}}\Box\Box\Box f\left(\vec{\mathbf{x}}\right)\overset{\downarrow}{\Box}.$$

Mit LlD^*R^2 bekommen wir

$$\Box\vec{\mathbf{x}}\Box y\Box y\Box\vec{\mathbf{x}}\Box * \Box f\left(\vec{\mathbf{x}}\right)\overset{\downarrow}{\Box} \text{ oder}$$
$$\Box\vec{\mathbf{x}}\Box y\Box y\Box\vec{\mathbf{x}}\Box 0\Box f_0\overset{\downarrow}{\Box}.$$

Mit L^5T ergibt das

$$\Box\vec{\mathbf{x}}\overset{\downarrow}{\Box}\Box y\Box y\Box\vec{\mathbf{x}}\Box 0\Box f_0,$$

mit R^2T dann

$$\Box\vec{\mathbf{x}}\Box y\overset{\downarrow}{\Box}\Box y\Box\vec{\mathbf{x}}\Box 0\Box f_0.$$

Die 'Marke' Doppelleerfeld wurde technisch für die später anzusetzende Endmaschine angelegt, also für das Aufräumen. Nun kommt R^5, und es entsteht

$$(0)\ \Box\vec{\mathbf{x}}\Box y\Box\Box y\Box\vec{\mathbf{x}}\Box 0\Box f_0\overset{\downarrow}{\Box}.$$

Nun sind wir in der Lage, die Iteration systematisch anzulegen, wir fügen rechts neben dem Arbeitsfeld an - der erste Sternblock ist dabei unwichtig, erleichtert jedoch die technische Durchführung:

$$\Box f_1\Box y - 1\Box\vec{\mathbf{x}}\Box 1\Box f_1,$$

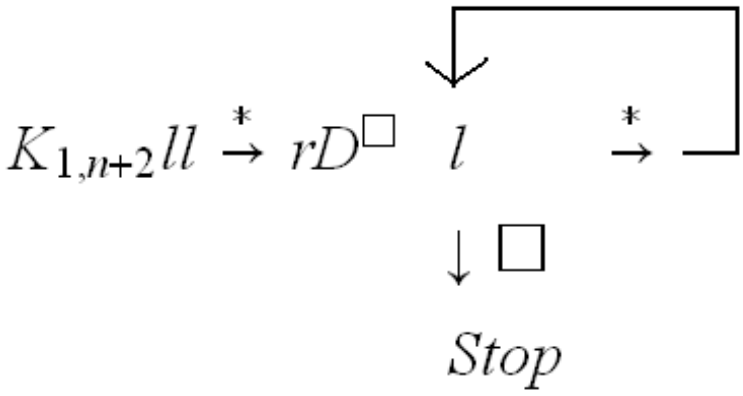
bleiben auf dem Leerfeld hinter dem Angefügten stehen, bis

$$f_y\Box 0\Box\vec{\mathbf{x}}\Box y - 1\Box f_y.$$

Vor jedem Anfügen wird geprüft, ob der erste Wert dieses Viererblocks Null ist. Dazu prüfen wir, beginnend mit der Situation (0) , ob der erste Wert des Viererblocks Null ist, und setzen dann die Endmaschine an, auf diese Weise:

$$K_{1,n+2}ll \overset{\Box}{\rightarrow} E.$$

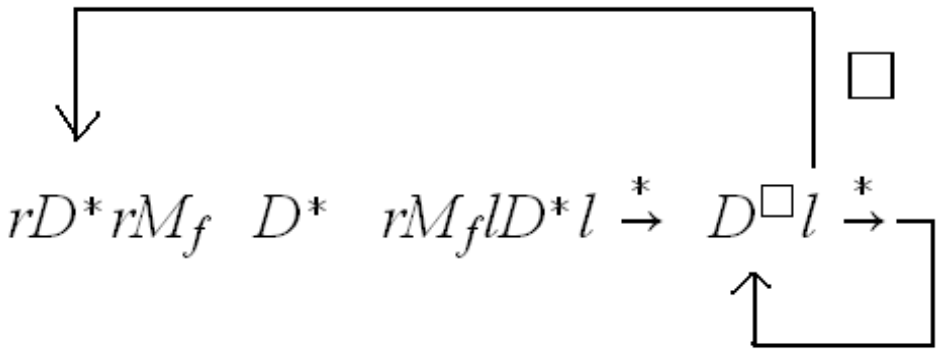
Für den Fall, dass der im Viererblock vorn stehende Wert y^i nicht Null ist, löschen wir den kopierten Wert und stellen die Ausgangssituation vor der Prüfung wieder her mit:



Anschließend wird der nächste Viererblock angehängt mittels:

$$M_g K_{1,n+3} l D^{\square} K_{n,4} K_{1,n+3} D^* r K_{1,n+2}.$$

d) Für den $\mu-$ Operator setzen wir eine Maschine M_f für $f\left(\overrightarrow{\mathbf{x}}, y\right)$ voraus und wollen unter Voraussetzung von $\forall \overrightarrow{\mathbf{x}} \exists y f\left(\overrightarrow{\mathbf{x}}, y\right) = 0$ die Funktion $g\left(\overrightarrow{\mathbf{x}}\right) = \mu_y f\left(\overrightarrow{\mathbf{x}}, y\right) = 0$ berechnen. Die Idee ist ähnlich, aber einfacher als die zu **c**. Man probiert $y = 0$, wenn das nicht klappt, $y = 1$, usw. Folgende Maschine leistet das Verlangte:



Übung: Erläutern Sie, dass dies korrekt ist.

Zweiter Teil: Jede Turing-berechenbare Funktion ist rekursiv.

Beweis: Die Idee zum Beweis ist die Gödelisierung der Turingmaschinen. Das bedeutet eine Zahlencodierung einmal des Maschinenprogramms, sodann der (bereits von Turing so betrachteten) Konfigurationen. Jedes Programm besteht aus Zeilen $cbac'$, man stellt die beiden möglichen Beobachtungen $\square, *$ etwa durch die Zahlen $0, 1$ dar, ebenso die Aktionen $r, l, d\square, d*, s$ durch die Zahlen $2, 3, 4, 5, 6$, schließlich die Zustände $0, ..., l$ durch die Zahlen $7, ..., 7 + l$, anschließend das gesamte Programm durch

$$t = \langle n_0, ..., n_m \rangle,$$

also die oben eingeführte Zahlencodierung der Folge $(n_0, ..., n_m)$ dar, mit

$$n_i = \langle \ulcorner c \urcorner, \ulcorner b \urcorner, \ulcorner a \urcorner, \ulcorner c' \urcorner \rangle,$$

wobei n_i die i. Programmzeile ist und mit den Häkchen wie üblich 'Gödelnummer von ...' gemeint ist. Die Zahl t ist dann die Gödelnummer der Maschine, welche ihr Programm codiert. Dabei ist wichtig, dass sowohl die Folgencodierung (als auch das Auslesen der Komponenten) als auch die Funktion 'Gödelnummer von ...' primitiv rekursiv sind.

Was wir nun benötigen, ist die Konfiguration der Maschine mit Nummer t, angesetzt auf $\overrightarrow{\mathbf{x}}$, im y. Rechenschritt. Diese Konfiguration ist jeweils das in einer Zahl codierte Tripel $(\ulcorner c\urcorner, \ulcorner B\urcorner, \ulcorner f\urcorner)$, wobei c der jeweils aktive Zustand, B der gesamte Bandinhalt und f das jeweils beobachtete Feld ist, $\ulcorner f\urcorner$ also dessen Nummer. Dabei ist wichtig, dass der Bandinhalt stets nur endlich viele Symbole '$*$' aufweist und die Bandfelder geeignet numeriert werden, etwa von einem Feld an mit $0, 1, 2, ...$, links davon mit Paaren $\langle 1,1\rangle, \langle 1,2\rangle$ usw. (Wir berücksichtigen im Folgenden nur Felder ab dem Feld mit der Nummer Null.) Den Bandinhalt codieren wir mit der Zahl

$$\ulcorner B\urcorner = \prod_{k=0}^{\infty} p(k)^{\ulcorner B(k)\urcorner},$$

mit $\ulcorner B(k)\urcorner = 0$ für $B(k) = \square$ und $\ulcorner B(k)\urcorner = 1$ für $B(k) = *$. Es ist also jeweils

$$\exp(\ulcorner B\urcorner, p(k)) = \ulcorner B(k)\urcorner.$$

Wir definieren nunmehr eine primitiv rekursive Funktion K durch Rekursion:

$$K\left(t, \overrightarrow{\mathbf{x}}, 0\right) = \left\langle \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, 0\right)\urcorner, \ulcorner B\left(t, \overrightarrow{\mathbf{x}}, 0\right)\urcorner, \ulcorner f\left(t, \overrightarrow{\mathbf{x}}, 0\right)\urcorner \right\rangle,$$

dabei ist $c\left(t, \overrightarrow{\mathbf{x}}, 0\right)$ der Startzustand 0, $B\left(t, \overrightarrow{\mathbf{x}}, 0\right)$ der Bandinhalt, der ab dem Leerfeld mit der Nummer Null die Sternfolgen für die Argumentwerte umfasst, durch Leerfeld jeweils getrennt, und $f\left(t, \overrightarrow{\mathbf{x}}, 0\right)$ ist das leere Startfeld dahinter, auf das die Maschine angesetzt ist - wir haben also $\ulcorner f\left(t, \overrightarrow{\mathbf{x}}, 0\right)\urcorner = f\left(t, \overrightarrow{\mathbf{x}}, 0\right)$ usw., da wir nur Felder ab 0 betrachten. Nun der Rekursionsschritt:

$$K\left(t, \overrightarrow{\mathbf{x}}, y+1\right) = \left\langle \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y+1\right)\urcorner, \ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y+1\right)\urcorner, \ulcorner f\left(t, \overrightarrow{\mathbf{x}}, y+1\right)\urcorner \right\rangle,$$

wobei

$$\begin{aligned} \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y+1\right)\urcorner &= \mu_{u\leq t}[(\exists v \leq t)\left(((t)_v)_1 = \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner \wedge (t)_v)_4 = u \wedge \right. \\ ((t)_v)_2 &= \left. \exp\left(\ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, p\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right)\right], \end{aligned}$$

Nun mit Fallunterscheidung:

$$\begin{aligned} & f\left(t, \overrightarrow{\mathbf{x}}, y+1\right) = f\left(t, \overrightarrow{\mathbf{x}}, 0\right), \text{ wenn} \\ (\exists v \leq t)[((t)_v)_1 &= \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner \wedge ((t)_v)_2 = \exp\left(\ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, p\left(\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right)\right) \wedge ((t)_v)_3 \neq 2, 3], \\ & f\left(t, \overrightarrow{\mathbf{x}}, y+1\right) = f\left(t, \overrightarrow{\mathbf{x}}, 0\right) - 1, \text{ wenn} \\ (\exists v \leq t)[((t)_v)_1 &= \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner \wedge ((t)_v)_2 = \exp\left(\ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, p\left(\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right)\right) \wedge ((t)_v)_3 = 3], \\ & f\left(t, \overrightarrow{\mathbf{x}}, y+1\right) = f\left(t, \overrightarrow{\mathbf{x}}, 0\right) + 1, \text{ wenn} \\ (\exists v \leq t)[((t)_v)_1 &= \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner \wedge ((t)_v)_2 = \exp\left(\ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, p\left(\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right)\right) \wedge ((t)_v)_3 = 2]. \end{aligned}$$

Ebenso mit Fallunterscheidung der neue Bandinhalt - in Codierungsnummer:

$$\begin{aligned} & \ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y+1\right)\urcorner = \ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, \text{ wenn} \\ (\exists v \leq t)[((t)_v)_1 &= \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner \wedge ((t)_v)_2 = \exp\left(\ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, p\left(\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right)\right) \wedge ((t)_v)_3 \neq 4, 5], \\ & \ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y+1\right)\urcorner = p\left(\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right) \cdot \ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, \text{ wenn} \\ (\exists v \leq t)[((t)_v)_1 &= \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner \wedge 0 = ((t)_v)_2 = \exp\left(\ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, p\left(\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right)\right) \wedge ((t)_v)_3 = 5], \\ & \ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y+1\right)\urcorner = \ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner / p\left(\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right), \text{ wenn} \\ (\exists v \leq t)[((t)_v)_1 &= \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner \wedge 1 = ((t)_v)_2 = \exp\left(\ulcorner B\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, p\left(\left(K\left(t, \overrightarrow{\mathbf{x}}, y\right)\right)_3\right)\right) \wedge ((t)_v)_3 = 4]. \end{aligned}$$

Die inhaltliche Bedeutung ist jeweils einfach: Man sucht die Programmzeile auf, welche in Codierung die Gestalt

$$\left\langle \ulcorner c\left(t, \overrightarrow{\mathbf{x}}, y\right)\urcorner, 0[1], ... \right\rangle$$

hat und ändert gemäß der Aktionsnummer und dem Folgezustand die Nummer des beobachteten Feldes und den (codierten) Bandinhalt und stellt die Nummer des Folgezustands fest. Das geschieht in einfacher Weise, und zusammen ergibt sich $K\left(t, \overrightarrow{\mathbf{x}}, y+1\right)$.

Nun gibt es zwei Möglichkeiten: Entweder stoppt die Maschine, indem man auf den Stopbefehl stößt. Dann setzen wir $K\left(t,\overrightarrow{\mathbf{x}},z\right)=K\left(t,\overrightarrow{\mathbf{x}},y\right)$ für alle $z\geq y$, wenn im Schritt y der Stopbefehl auftritt. Oder aber die Maschine kommt nicht zum Stopbefehl. Wenn das für irgendwelche Eingabetupel $\overrightarrow{\mathbf{x}}$ auftritt, so definiert die Maschine mit der Nummer t eben eine partielle rekursive Funktion, wie wir noch genauer sehen.

Was haben wir erreicht? $K\left(t,\overrightarrow{\mathbf{x}},y\right)$ ist eine primitiv rekursive Funktion, definiert für alle $t,\overrightarrow{\mathbf{x}},y$. Wenn die Maschine mit der Nummer t eine totale Funktion definiert, dann ist diese Funktion rekursiv, nämlich von der Form

$$\varphi_t\left(\overrightarrow{\mathbf{x}}\right)=W\left(K\left(t,\overrightarrow{\mathbf{x}},\mu_y T\left(t,\overrightarrow{\mathbf{x}},y\right)\right)\right).$$

Dabei ist T das berühmte Kleenesche primitiv rekursive Prädikat.

$$\begin{aligned} T\left(t,\overrightarrow{\mathbf{x}},y\right) \quad &: \quad \Longleftrightarrow \\ (\exists v\leq t)\left[((t)_v)_1 \quad &= \quad \ulcorner c\left(t,\overrightarrow{\mathbf{x}},y\right)\urcorner\wedge((t)_v)_2=\exp\left(\ulcorner B\left(t,\overrightarrow{\mathbf{x}},y\right)\urcorner,p\left(\left(K\left(t,\overrightarrow{\mathbf{x}},y\right)\right)_3\right)\right)\wedge((t)_v)_3=6\right] \end{aligned}$$

Die Funktion W ist auf einfache Weise zu konstruieren: Man schaut nach, auf welchem Feld die Maschine im Stop-Rechenschritt steht. Dies Feld ist leer, und am Bandinhalt wird nachgesehen, wie viele Sterne davor stehen bis zum nächsten Leerfeld. Die Funktion W ist wiederum primitiv rekursiv. Wenn also eine Funktion Turing-berechenbar ist, so ist sie $\mu-$rekursiv, und mehr noch: Es genügt eine einzige Anwendung des $\mu-Operators$. Dieser Zusatz ergibt sich aus der letzteren Darstellung.■

Übung: Man überzeuge sich durch eine kleine formale Überlegung davon, dass die oben angegebene Definition von $K\left(t,\overrightarrow{\mathbf{x}},y\right)$ als primitive Standard-Rekursion geschrieben werden kann und K daher eine primitiv rekursive Funktion ist.

4. Rekursivität, rekursive Aufzählbarkeit, Kleene-Mostowski-Hierarchie und Rekursionssatz

4.1. Universalität und Grundlegendes zur rekursiven Aufzählbarkeit. Das Phänomen der Universalität ist von großer systematischer Bedeutung: Wir haben gerade eine universelle partielle rekursive Funktion gesehen:

SATZ 11. *Folgende Funktion ist universell für alle partiellen rekursiven Funktionen von* $\overrightarrow{\mathbf{x}}$:

$$\varphi\left(t,\overrightarrow{\mathbf{x}}\right)=\begin{array}{l}\textit{Wert der Turingmaschine mit Nummer } t\textit{, angesetzt auf } \overrightarrow{\mathbf{x}}\textit{, wenn sie stoppt.}\\ \textit{undefiniert sonst (insbesondere wenn keine Turingmaschinen-Nummer ist.}\end{array}$$

Wenn $\overrightarrow{\mathbf{x}}$ *die Länge* n *hat, so haben wir also eine universelle rekursive für alle partiellen rekursiven Funktionen* $\mathbb{N}^n\to\mathbb{N}$, *insbesondere für alle total rekursiven Funktionen.*

Aus solcher Universalität ergibt sich sofort ein 'Diagonalargument' für die Konstruktion nicht rekursiver Funktionen, die wesentlich handfester ist als das nichtkonstruktive Kardinalzahlargument:

SATZ 12. *Die Funktion* $g(t)=\varphi(t,t)+1$ *ist keine partielle rekursive Funktion. Ebenso ist die totale Funktion*

$$h(t)=\begin{cases}\varphi(t,t)+1, & \textit{wenn } \varphi(t,t) \textit{ definiert ist,}\\ 0 & \textit{sonst (insbesondere wenn } t \textit{ keine Nummer einer Turingmaschine ist)}\end{cases}$$

nicht $\mu-rekursiv$.

Beweis: Wäre g partiell rekursiv, so hätte man für ein t_0 :

$$\begin{aligned} g(t) &= \varphi(t_0,t) \text{ für alle } t, \text{ für die } g(t) \text{ definiert ist, also}\\ \varphi(t,t)+1 &= \varphi(t_0,t) \text{ für alle } t, \text{ somit}\\ \varphi(t_0,t_0)+1 &= \varphi(t_0,t_0). \end{aligned}$$

Dann müsste g nirgends definiert sein. Aber g ist für alle t definiert, welche Maschinennummer einer Turingmaschine für eine totale rekursive Funktion darstellen.■

DEFINITION 30. *Ein Prädikat (oder eine Relation)* $R\overrightarrow{\mathbf{x}}$ *heißt rekursiv aufzählbar, wenn es von der Form ist:*

$$R\overrightarrow{\mathbf{x}}\iff\exists yS\overrightarrow{\mathbf{x}}y,$$

mit rekursivem Prädikat S.

Daran schließen sich unmittelbar folgende Beobachtungen:

LEMMA 11. *Jede rekursiv aufzählbare Relation ist der Definitionsbereich einer partiellen rekursiven Funktion. Eine Relation ist genau dann rekursiv aufzählbar, wenn sie leer ist oder ihre Elemente durch eine partielle rekursive Funktion aufgezählt werden können. (In jedem Fall ist sie also das Bild einer partiellen rekursiven Funktion.) Wenn sie nicht leer ist, dann ist sie auch das Bild einer totalen rekursiven Funktion. Eine Relation ist genau dann rekursiv, wenn sie selbst und auch ihr Komplement rekursiv aufzählbar sind.*

Zum Beweis der ersten beiden Aussagen definiert man einfach $f\left(\overrightarrow{\mathbf{x}}\right) = \begin{cases} \overrightarrow{\mathbf{x}}, \text{ wenn } \exists y S \overrightarrow{\mathbf{x}} y, \\ \text{undefiniert sonst.} \end{cases}$.

Will man eine nicht vektorwertige Funktion haben, muss man bei Länge von $\overrightarrow{\mathbf{x}}$ größer als 1 zu den Folgennummern übergehen. Aber man kann eine nichtleere rekursiv aufzählbare Relation stets auch aufzählen mit einer totalen rekursiven Funktion (dritte Aussage): Definiere mit $R\overrightarrow{\mathbf{x}}_0$ folgende Funktion: $f\left(n, \overrightarrow{\mathbf{x}}\right) = \begin{cases} \overrightarrow{\mathbf{x}}, \text{ wenn } (\exists y \leq n)\, S\overrightarrow{\mathbf{x}} y, \\ \overrightarrow{\mathbf{x}}_0 \text{ sonst.} \end{cases}$. f ist offensichtlich totale rekursive Funktion, und ihr Bild ist R.■

Auch für rekursiv aufzählbare Relationen haben wir universelle, mit anschließendem Diagonalargument:

SATZ 3. *Folgendes rekursiv aufzählbare Prädikat ist universell für alle $n-$stelligen rekursiv aufzählbaren Prädikate:*

$$T_s\left(t, \overrightarrow{\mathbf{x}}\right) :\Longleftrightarrow \textit{ die Turingmaschine mit Nummer } t \textit{ stoppt angesetzt auf } \overrightarrow{\mathbf{x}} \ \left(\overrightarrow{\mathbf{x}} \in \mathbb{N}^n\right).$$

Beweis: Zunächst ist T_s rekursiv aufzählbar, weil

$$T_s\left(t, \overrightarrow{\mathbf{x}}\right) \iff \exists y T\left(t, \overrightarrow{\mathbf{x}}, y\right),$$

und T ist sogar primitiv rekursiv. (T ist das berühmte Kleene-Prädikat, hier das mit $2+n$ unabhängigegn Variablen.) Die Universalität sehen wir so: Sei $R\overrightarrow{\mathbf{x}} \iff \exists y Q \overrightarrow{\mathbf{x}} y$ mit rekursivem Q. Dann haben wir die Turingmaschine, welche mit dem kleinsten Wert y stoppt, so dass $Q\overrightarrow{\mathbf{x}} y$, falls es einen solchen gibt, sonst nicht stoppt. Diese habe die Nummer t_0. Damit gilt $T_s\left(t_0, \overrightarrow{\mathbf{x}}\right) \iff R\overrightarrow{\mathbf{x}}$ für alle $\overrightarrow{\mathbf{x}}$.■

Nun folgern wir mit Diagonalargument:

SATZ 4. *Die Relation $\rightharpoonup T_s t \overrightarrow{\mathbf{x}}$ ist nicht rekursiv aufzählbar, also ist $T_s t \overrightarrow{\mathbf{x}}$ nicht rekursiv. Das ist das klassische Resultat: 'Das Halteproblem von Turingmschinen ist (algorithmisch) unentscheidbar'.*

Beweis: Wäre $\rightharpoonup T_s t x$ rekursiv aufzählbar, so wäre es insbesondere $Ut \iff \rightharpoonup T_s t t$, also hätte man mit Universalität eine Turingmaschinen-Nummer t_0 mit $T_s t_0 t \iff \rightharpoonup T_s t t$ für alle t, was mit Einsetzen von t_0 für t einen Widerspruch liefert. Dass $T_s t \overrightarrow{\mathbf{x}}$ nicht rekursiv ist, folgt mit dem vorigen Lemma.■

4.2. Ein naheliegendes Problem, und der Satz von Friedberg-Muchnik. Wir haben nunmehr rekursiv aufzählbare Prädikate kennengelernt, die nicht rekursiv sind. Dabei wurde mit der Universalität gespielt, also gerade damit, dass $T_s t \overrightarrow{\mathbf{x}}$ alle Komplexität des rekursiv Aufzählbaren enthält. Daher liegt das Problem nahe, ob es weniger komplexe rekursiv aufzählbare Prädikate gibt, die immer noch nicht rekursiv sind. Dies Problem präzisiert man z.B. so: Gegeben eine 'Orakelmaschine' für $S\overrightarrow{\mathbf{x}}$ (als beliebig 'kompliziert' anzusehen, dann definiert man für $U\overrightarrow{\mathbf{x}}$:

$$U \leq_T S :\Longleftrightarrow U \text{ ist Turing-reduzierbar auf } S,$$

d.h. mit der Orakelmaschine für S kann man eine Turingmaschine basteln, die U berechnet (natürlich sind die charakteristischen Funktionen gemeint). Definiere nun

$$U \sim_T S :\Longleftrightarrow U \leq_T S \wedge S \leq_T U.$$

Das definiert die Äquivalenzrelation 'Turing-äquivalent'. Eine Äquivalenzklasse heißt 'degree of unsolvability'. Die Klasse der rekursiven Prädikate ist dabei der einfachste Grad.

Das Problem lautet also präzisiert: Gibt es Grade der Unlösbarkeit, welche weder gleich dem der rekursiven Funktionen, noch gleich dem der universellen rekursiv aufzählbaren Prädikate sind, sondern echt dazischen? Der Satz von Friedberg und Muchnik besagt, dass es solche gibt. Wir beweisen ihn hier nicht und verweisen auf die Literaturliste, insbesondere H. Rogers jr.. Es gibt weitere Resultate, welche die unerhörte Kompliziertheit des Verbandes der 'degrees of unsolvability' zeigen. Diese Theorie wurde in der zweiten Hälfte des 20. Jahrhunderts entwickelt. Wesentliche Autoren sind Sacks, Shoenfield, Rogers jr. und andere.

4.3. Hilberts zehntes Problem. In der berühmten Hilbertschen Liste vordringlicher mathematischer Probleme aus dem Jahre 1900 gab es eines, das Hilbert sinngemäß so formulierte: Man finde ein Entscheidungsverfahren für die Frage, ob eine Polynomgleichung (oder 'diophantischen Gleichung' $p\left(\overrightarrow{\mathbf{x}}\right) = q\left(\overrightarrow{\mathbf{x}}\right)$ mit Polynomen p, q eine *ganzzahlige* Lösung besitzt. Dies Problem war erst 1970 gelöst nach jahrzehntelanger Arbeit, an der insbesondere Julia Robinson, Martin Davis und Yuri Matiasevic beteiligt waren. Das Resultat war - entgegen der Erwartung von Hilbert - negativ: Ein solches Entscheidungsverfahren kann es nicht geben. Wir können nunmehr die Linie des Beweises so weit verstehen: Zunächst stellt man fest, dass ein derartigen Entscheidungsverfahren auch ein Entscheidungsverfahren für die Lösbarkeit einer diophantischen Gleichung in *natürlichen Zahlen* nach sich zöge, weil man in $\mathbb{Z}$ die natürlichen Zahlen so definieren kann: Eine ganze Zahl ist genau dann natürlich, wenn sie Summe von höchstens vier Quadraten ist. Denn nach einem Satz der elementaren Zahlentheorie ist jede natürliche Zahl Summe von höchstens vier Quadraten natürlicher Zahlen.

Nunmehr war die Beweisidee die: Eine Relation $R\overrightarrow{\mathbf{x}} \iff \exists \overrightarrow{\mathbf{u}} p\left(\overrightarrow{\mathbf{x}}, \overrightarrow{\mathbf{u}}\right) = q\left(\overrightarrow{\mathbf{x}}, \overrightarrow{\mathbf{u}}\right)$ (auf $\mathbb{N}^k$) mit Polynomen p, q ist offenbar rekursiv aufzählbar. Es genügte also, zu beweisen, dass **jede** rekursiv aufzählbare Relation so dargestellt werden kann. Dafür wiederum reicht es aus, dass jede rekursive Relation S in die Form der Gültigkeit einer Polynomgleichung gebracht werden kann, also $S\overrightarrow{\mathbf{y}} \iff p\left(\overrightarrow{\mathbf{y}}\right) = q\left(\overrightarrow{\mathbf{y}}\right)$. Dies gelang tatsächlich. Dass dies nicht so einfach ist, kann man sich leicht daran klarmachen, dass dann auch etwa Polynome p, q existieren müssen, so dass

$$n \text{ ist Primzahl } \iff \exists \overrightarrow{\mathbf{u}} p\left(n, \overrightarrow{\mathbf{u}}\right) = q\left(n, \overrightarrow{\mathbf{u}}\right) \text{ für alle } n.$$

Denn 'Primzahl' ist sogar ein rekursives Prädikat. Dass Lösungen einer Polynomgleichung alle Primzahlen erzeugen, ist schon eine Sensation. Wie zu erwarten, ist diese Polynomgleichung sehr kompliziert. Man hätte sie als solche nie gefunden, wenn man nicht über den allgemeinen Beweis die universellen rekursiv aufzählbare Relationen in diophantischer Form besessen hätte.

Zunächst überzeugt man sich relativ einfach davon, dass man alle primitiv rekursiven Relationen arithmetisch ausdrücken kann, allein die Folgencodierung macht dann Probleme, die man für eine Explizierung der primitiven Rekursion benötigt. Lange Zeit blieb die Sache dabei stehen, dass man in der Sprache zu $\langle, 0, 1, +, \cdot, (\cdot)^x\rangle$, also mit der Operation y^x, die primitiv rekursiven Relationen ausdrücken konnte, dann gelang Matiasevic die Reduktion auf $+, \cdot$ mittels konkreter elementarer Zahlentheorie, insbesondere über Betrachtung Pellscher Gleichungen.

4.4. Die Kleene-Mostowski-Hierarchie oder arithmetische Hierarchie. Wir kehren zurück zur Theorie, die noch in der ersten Hälfte des 20. Jahrhunderts geformt wurde: Man kann die Quantorenwechsel als Maß immer größerer Komplexität nehmen und definiert:

DEFINITION 31. *Ein Prädikat heißt Σ_n, wenn es die Form hat, mit rekursivem R:*

$$S\overrightarrow{\mathbf{u}} \iff \exists x_1 \forall x_2 ... \exists x_{n-1} \forall x_n R\left(\overrightarrow{\mathbf{u}}, \overrightarrow{\mathbf{x}}\right) \text{ bzw. } \exists x_1 \forall x_2 ... \forall x_{n-1} \exists x_n R\left(\overrightarrow{\mathbf{u}}, \overrightarrow{\mathbf{x}}\right) \text{ für } n \text{ ungerade}$$

Ein Prädikat heißt Π_n, wenn es die Form hat, mit rekursivem R:

$$S\overrightarrow{\mathbf{u}} \iff \forall x_1 \exists x_2 ... \forall x_{n-1} \exists x_n R\left(\overrightarrow{\mathbf{u}}, \overrightarrow{\mathbf{x}}\right) \text{ bzw. } \forall x_1 \exists x_2 ... \exists x_{n-1} \forall x_n R\left(\overrightarrow{\mathbf{u}}, \overrightarrow{\mathbf{x}}\right)$$

Ein Prädikat heißt Δ_n, wenn es sowohl Σ_n als auch Π_n ist. Also

$$\Delta_n := \Sigma_n \cap \Pi_n.$$

Konsequent hat man $\Sigma_0 = \Pi_0 = \Delta_0 =$ Menge der rekursiven Prädikate.

Bemerkung: Es kommt auf die Quantorenwechsel an, nicht auf die Länge der Quantorenblöcke - einen Block von lauter Quantoren des gleichen Typs kann man zu einem einzigen Quantor verschmelzen über Folgencodierung. Außerdem 'zählen' zur Komplexität nur solche Quantoren, die nicht beschränkt sind - beschränkte kann man zum rekursiven Kern schlagen.

Dass damit eine immer weiter streng aufsteigende Hierarchie definiert wird, besagt der folgende Satz:

SATZ 5. *Für $n \geq 0$ hat man*

$$\begin{array}{lllll} (i) & \Delta_{n+1} & \subsetneq & \Sigma_{n+1}, \Pi_{n+1} \\ (ii) & \Delta_{n+1} & \not\supseteq & \Sigma_n \cup \Pi_n. \end{array}$$

Insbesondere hat man $\Sigma_{n+1} \supsetneq \Sigma_n$ und $\Pi_{n+1} \supsetneq \Pi_n$ für alle $n \geq 0$.

Beweis: (i) Mit dem Kleeneprädikat T (passender Variablenzahl) hat man:

$$U\left(t,\overrightarrow{\mathbf{u}}\right) \iff \exists x_1 ... \forall(\exists) x_{n+1} T\left(t,\overrightarrow{\mathbf{u}},\overrightarrow{\mathbf{x}}\right)$$

$(\overrightarrow{\mathbf{x}} = (x_1, ..., x_{n+1}))$ universell Σ_{n+1} für Σ_{n+1}, mit demselben Argument wie für Σ_1. Mit dem Diagonalargument ist es nicht in Π_{n+1}, und seine Verneinung in $\Pi_{n+1} \setminus \Sigma_{n+1}$. Also $\Delta_{n+1} \subsetneq \Sigma_{n+1} \cup \Pi_{n+1}$.

(ii) Zunächst ist klar $\Sigma_n \cup \Pi_n \subset \Sigma_{n+1} \cap \Pi_{n+1} = \Delta_{n+1}$, dazu braucht man nur den zusätzlichen Quantor vorn leerlaufen zu lassen. Jetzt bildet man

$$\begin{array}{rcl} Vt\overrightarrow{\mathbf{u}} & \iff & \exists x_1 ... \forall(\exists) x_{n+1} \left(T\left(t,\overrightarrow{\mathbf{u}},x_1,...,x_n\right) \wedge x_1 = 0\right) \\ \vee & \multimap & \exists x_1 ... \forall(\exists) x_{n+1} \left(T\left(t,\overrightarrow{\mathbf{u}},x_1,...,x_n\right) \wedge x_1 = 1\right). \end{array}$$

Das ist offenbar in Δ_{n+1}, weil beide Glieder ohne den ersten Quantor zu schreiben sind. Aber es ist nicht in $\Sigma_n \cup \Pi_n$, weil $\forall x_2 ... T\left(t,\overrightarrow{\mathbf{u}},0,x_2,..,x_n\right)$ in $\Pi_n \setminus \Sigma_n$ und $\exists x_2 ... \multimap T\left(t,\overrightarrow{\mathbf{u}},1,x_2,..,x_n\right)$ in $\Sigma_n \setminus \Pi_n$.■

4.5. Der Rekursionssatz. Es handelt sich dabei um einen Fixpunktsatz. Wir haben eine Aufzählung aller partiellen rekursiven Funktionen:

$$\varphi_t\left(\overrightarrow{\mathbf{x}}\right),$$

durch die Nummern t der Turingmaschinen. Nun sollte klar sein, dass es jeweils unendlich viele Zahlen t gibt, welche in diesem Sinne dieselbe partielle Funktion liefern. Der angestrebte Satz lautet:

Satz 13 (Rekursionssatz). *Für jede (totale) rekursive Funktion $f(t)$ gibt es eine Zahl n, so dass*

$$\varphi_n = \varphi_{f(n)}.$$

Beweis: Definiere

$$\eta\left(t,\overrightarrow{\mathbf{x}}\right) = \begin{cases} \varphi_{\varphi_t(t)}\left(\overrightarrow{\mathbf{x}}\right), \text{ wenn } \varphi_t(t) \text{ definiert,} \\ \text{undefiniert sonst.} \end{cases}.$$

Die Gödelnummer einer zugehörigen Turingmaschine findet man mit einer totalen rekursiven Funktion g, also

$$\eta\left(t,\overrightarrow{\mathbf{x}}\right) = \varphi_{g(t)}\left(\overrightarrow{\mathbf{x}}\right).$$

Mit f ist $f \circ g$ totale rekursive Funktion. Also mit der Gödelnummer v für $f \circ g$:

$$\begin{array}{rcl} & & \varphi_v(v) \text{ definiert, also} \\ \eta\left(v,\overrightarrow{\mathbf{x}}\right) & = & \varphi_{\varphi_v(v)}\left(\overrightarrow{\mathbf{x}}\right) \end{array}$$

$$\varphi_{f(g(v))}\left(\overrightarrow{\mathbf{x}}\right) = \varphi_{\varphi_v(v)}\left(\overrightarrow{\mathbf{x}}\right) = \eta\left(v,\overrightarrow{\mathbf{x}}\right) = \varphi_{g(v)}\left(\overrightarrow{\mathbf{x}}\right).$$

Damit ist $g(v)$ eine Zahl der gewünschten Art.■

5. Folgerungen der Rekursionstheorie

Es liegen nach den bisherigen Begriffsbildungen folgende Problemstellungen nahe:

1.) Ist die Menge der allgemeingültigen Formeln der Prädikatenlogik 1. Stufe entscheidbar?

2.) Ist die Menge der aus der Peanoarithmetik 1. Stufe folgenden Aussagen entscheidbar?

3.) Ist die Peanoarithmetik 1. Stufe vollständig?

4.) Welchen Status in der arithmetischen Hierarchie hat die Menge der in $\langle \mathbb{N}, 0, 1, +, \cdot \rangle$ wahren Aussagen?

Die Antworten werden alle negativ sein, zum zweiten Problem von der Form, dass die Menge der wahren Aussagen nicht einmal arithmetisch ist, also $\Delta_\omega = \bigcup_{n=0}^{\infty} \Delta_n$, aber in keinem der Δ_n.

Zum Verständnis und zur Behandlung der gestellten Probleme benötigen wir eine Gödelisierung der Prädikatenlogik. Es ist klar, dass man die Symbole mit Gödelnummern versehen kann, etwa $\ulcorner v_k \urcorner = 2k$ für die Variablen, $\ulcorner \forall \urcorner = 1$, $\ulcorner \exists \urcorner = 3$, $\ulcorner \doteq \urcorner = 5$, $\ulcorner \wedge \urcorner = 7$, $\ulcorner \multimap \urcorner = 9$, $\ulcorner + \urcorner = 11$, $\ulcorner \cdot \urcorner = 13$, $\ulcorner 0 \urcorner = 15$, $\ulcorner 1 \urcorner = 17$, anschließend gibt man einer Formel dann die Folgennummer zur Folge der Zeichen-Nummern. Der Begriff der Formel der Prädikatenlogik - genauer: 'Gödelnummer einer Formel der Prädikatenlogik' - in der Sprache zu $\langle \mathbb{N}, 0, 1, +, \cdot \rangle$ ist dann primitiv rekursiv. Nun wird ein Beweis, d.h. eine Beweisfolge $\alpha_1, ..., \alpha_n$, so gödelisiert:

$$\ulcorner (\alpha_1, ..., \alpha_n) \urcorner = \langle \ulcorner \alpha_1 \urcorner, ..., \ulcorner \alpha_n \urcorner \rangle \text{ (Folgennummer).}$$

Nunmehr ist der Begriff 'n ist Gödelnummer einer Beweisfolge, deren letzte Formel die Gödelnummer m hat' primitiv rekursiv. Dazu benötigt man nur Folgendes:

1.) 'n ist Gödelnummer eines Axioms' ist eine primitiv rekursive Menge.

2.) 'die Formel mit Gödelnummer n geht aus den Formeln mit Gödelnummern k, l durch Anwendung der

Modus-Ponens-Regel hervor' ist eine primitiv rekursive Relation.

Es folgt dann:

SATZ 14. *Die Menge der Gödelnummern der allgemeingültigen Aussagen der Prädikatenlogik einer abzählbaren Sprache ist rekursiv aufzählbar. Dasselbe gilt für die Menge der Aussagen, welche aus einem rekursiv aufzählbaren Axiomensystem ableitbar sind (bzw. daraus folgen)..*

Wir erläutern einen **intuitiven Beweis** für diese Tatsache: Offenbar können wir alle Beweise (auch solche die aus einem rekursiven Axiomensystem) mit Gödelnummern $\leq n$ aufschreiben - das sind nur endlich viele, tun wir das für $n = 1, 2, 3, ...$ der Reihe nach, so erhalten wir eine rekursive Aufzählung aller Beweise und mit deren Endformeln auch aller allgemeingültigen Formeln (die nach dem Vollständigkeitssatz dieselbe ist wie die Menge der beweisbaren Formeln)

Bemerkung: In der Praxis sind Axiomensysteme stets sogar rekursiv, vielfach endlich.

Zu bemerken ist nur, dass wir eine Gödelisierung nach dem oben gegebenen Muster auch für eine Sprache mit abzählbar unendlich vielen Relations- und Funktionssymbolen durchführen können.

Damit wäre noch nicht ausgeschlossen, dass die Menge der allgemeingültigen Formeln sogar rekursiv wäre. Man kann aber einsehen, dass sie nicht rekursiv ist, bereits für eine Sprache mit nur endlich vielen nichtlogischen Symbolen:

5.1. Die Unentscheidbarkeit der Prädikatenlogik.

SATZ 15. *Die Menge der Gödelnummern der allgemeingültigen Ausdrücke der Prädikatenlogik einer Sprache mit Operationssymbolen $0, S+, \cdot$ und Relationssymbol $<$ ist nicht rekursiv.*

Beweis: Robinson-Arithmetik ist definiert durch folgendes endliche Axiomensystem RA:

$$\begin{aligned}
&\forall x \ \neg \ 0 \doteq Sx \\
&\forall x \forall y \left(Sx \doteq Sy \rightarrow x \doteq y \right) \\
&\forall x \left(x + 0 \doteq x \right) \\
&\forall x \forall y \left(x + Sy \doteq S \left(x + y \right) \right) \\
&\forall x \left(x \cdot 0 \doteq 0 \right) \\
&\forall x \forall y \left(x \cdot Sy \doteq x \cdot y + x \right) \\
&\forall x \left(x < y \leftrightarrow \exists z \left(\neg \ z \doteq 0 \wedge x + z \doteq y \right) \right).
\end{aligned}$$

Darin ist also alles Wesentliche zu $0, S, +, \cdot$ enthalten, was in $\mathbb{N}$ gültig ist, mit der üblichen Deutung. Die entscheidende Beobachtung ist nun: Alle rekursiven Relationen sind durch $\Sigma_1^{RA}-$ Formeln der Sprache von RA ausdrückbar. Das sind die Formeln der Form $Q_1 x_1 ... Q_n x_n \varphi$, mit quantorenfreier Formel φ und Quantoren Q_i, die entweder Existenzquantoren oder aber beschränkte Quantoren sind. Nun hat man folgende Lemmata:

LEMMA 12. *Alle in $\mathbb{N}$ wahren $\Sigma_1^{RA}-$ Aussagen sind in RA beweisbar.*

LEMMA 13. *Alle rekursiv aufzählbaren Relationen R sind durch $\Sigma_1^{RA}-$ Formeln darstellbar, also*

$$\mathbb{N} \models R\overrightarrow{\mathbf{x}} \iff \mathbb{N} \models \varphi_R \left[\overrightarrow{\mathbf{u}} / \overrightarrow{\mathbf{c}}_{\overrightarrow{\mathbf{x}}} \right]$$

mit der zu $\overrightarrow{\mathbf{x}} \in \mathbb{N}^k$ passenden Folge konstanter Terme $\overrightarrow{\mathbf{c}}_{\overrightarrow{\mathbf{x}}}$ (S...S0 für jedes Folgenglied von $\overrightarrow{\mathbf{x}}$) und einer $\Sigma_1^{RA}-$ Formel $\varphi_R \left(\overrightarrow{\mathbf{u}} \right)$.

Wir zeigen nun, wie die Behauptung des Satzes aus beiden Lemmata folgt:

Sei $T_s \left(t, \overrightarrow{\mathbf{x}} \right)$ das rekursiv aufzählbare Prädikat, das nicht rekursiv ist (Halteproblem bei Turingmaschinen). Dann hat man mit dem zweiten Lemma:

$$T_s \left(t, \overrightarrow{\mathbf{x}} \right) \iff \mathbb{N} \models \varphi_{T_s} \left[\overrightarrow{\mathbf{u}} / \overrightarrow{\mathbf{c}}_{t, \overrightarrow{\mathbf{x}}} \right],$$

mit dem ersten Lemma daher

$$T_s\left(t,\overrightarrow{\mathbf{x}}\right) \iff RA \vdash \varphi_{T_s}\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{t,\overrightarrow{\mathbf{x}}}\right].$$

Sei nun α die Konjunktion aller Axiome von RA. Dann gilt

$$RA \vdash \varphi_{T_s}\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{t,\overrightarrow{\mathbf{x}}}\right] \iff \vdash \alpha \to \varphi_{T_s}\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{t,\overrightarrow{\mathbf{x}}}\right].$$

Wäre nun die Menge der Formeln β mit $\vdash \beta$ entscheidbar, so wäre auch die Menge der Aussagen der Form

$$\alpha \to \varphi_{T_s}\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{t,\overrightarrow{\mathbf{x}}}\right], \text{ welche ableitbar sind,}$$

entscheidbar und damit die Menge der Tupel $\left(t,\overrightarrow{\mathbf{x}}\right) \in \mathbb{N}^k$, für die T_s zutrifft.■

Es bleiben noch die beiden Lemmata zu beweisen:

Das erste zeigt man leicht über Induktion. Die Axiome von RA garantieren sofort die Ableitbarkeit der quantorenfreien wahren $RA-$ Aussagen. Für die Existenzen hat man Beispiele in $\mathbb{N}$, für die beschränkten Allquantoren kann man mit endlichen Disjunktionen arbeiten.

Das zweite Lemma verlangt mehr:

Beweis des zweiten Lemmas: Es genügt, alle rekursiven Funktionen $f\left(\overrightarrow{\mathbf{x}}\right)$ darzustellen in der Form:

$$f\left(\overrightarrow{\mathbf{x}}\right) = y \iff RA \vdash \varphi_f\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{\overrightarrow{\mathbf{x}},y}\right]$$

mit $\Sigma_1^{RA}-$ Formeln φ_f. Für die Grundfunktionen und die Einsetzung ist das klar, für

$$f\left(\overrightarrow{\mathbf{x}}\right) = \mu y\left(R\overrightarrow{\mathbf{x}}y\right)$$

mit rekursivem R sieht man das so:

$$f\left(\overrightarrow{\mathbf{x}}\right) = y \iff R\overrightarrow{\mathbf{x}}y \wedge \forall z < y \rightharpoonup R\overrightarrow{\mathbf{x}}z,$$

nun verwendet man die induktiv vorauszusetzende Darstellbarkeit von R (deren charakteristischer Funktion).

Der entscheidende Teil ist die Darstellung der primitiven Rekursion. Nun ist

$$\begin{aligned} h\left(\overrightarrow{\mathbf{x}},0\right) &= f\left(\overrightarrow{\mathbf{x}}\right), \\ h\left(\overrightarrow{\mathbf{x}},Sy\right) &= g\left(y,\overrightarrow{\mathbf{x}},h\left(\overrightarrow{\mathbf{x}},y\right)\right) \end{aligned}$$

so umzuformulieren:

$$\begin{aligned} h\left(\overrightarrow{\mathbf{x}},y\right) &= z \iff \text{es gibt eine Zahlenfolge } (h_0,...,h_y) \text{ mit:} \\ h_0 &= f\left(\overrightarrow{\mathbf{x}}\right), \text{ und } h_{i+1} = g\left(i,\overrightarrow{\mathbf{x}},h_i\right) \text{ für alle } i < y, \text{ und} \\ &\quad \text{das letzte Glied der Folge ist } z. \end{aligned}$$

Dafür hat man Gödels $\beta-$ Funktion mit der Eigenschaft:

$$\beta(a,b,i) = \mu z\left(a \bmod (b\cdot(i+1)+1) = z\right).$$

Diese Funktion ist offenbar $\Sigma_1^{RA}-$ darstellbar, und man hat:

$$\forall(x_0...x_n)\,\exists a\exists b\left(\beta(a,b,i) = x_i\right).$$

Man wähle $b = (n+1)!\cdot(1+\max(x_i))$ und a so, dass $a \bmod (b\cdot(i+1)+1) = x_i$. Das geht mit dem 'chinesischen Restsatz', weil die $b(i+1)+1$ paarweise teilerfremd sind. Nunmehr haben wir

$$h\left(\overrightarrow{\mathbf{x}},y\right) = z \iff \exists a\exists b\forall i < y\left(\beta(a,b,0) = f\left(\overrightarrow{\mathbf{x}}\right) \wedge \beta(a,b,i+1) = g\left(i,\overrightarrow{\mathbf{x}},\beta(a,b,i)\right) \wedge \beta(a,b,y) = z\right).$$

Damit ist h wie gewünscht ausgedrückt, unter induktiver Voraussetzung entsprechender Ausdrücke für f und g.■

5.2. Unentscheidbarkeit der Peanoarithmetik. Zu präzisieren ist: Die Frage lautet, ob man algorithmisch entscheiden kann, ob eine Formel aus der Peanoarithmetik folgt oder nicht. Die Peanoarithmetik PA (erster Stufe!) hat folgendes Axiomensystem: Zu den Axiomen von RA kommt das allgemeine Rekursionsschema:

$$(\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(Sx)) \to \forall x(\varphi(x))),$$

für alle Formeln der Sprache der Peaonoarithmetik, was dieselbe Sprache wie die von RA ist.

Die Formulierung 'für alle Mengen' in der Logik 2. Stufe ist zu ersetzen durch: 'für alle erststufig definierbaren Mengen', und das ergibt das angegebene Schema.

Die Menge der Folgerungen aus dem Axiomensystem von PA ist nach früherem Satz rekursiv aufzählbar, da wir ein rekursives Axiomensystem haben. Aber sie ist nicht entscheidbar, weil PA eine konsistente Erweiterung von RA ist. Damit folgt aus

$$T_s\left(t, \overrightarrow{\mathbf{x}}\right) \iff RA \vdash \varphi_{T_s}\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{t,\overrightarrow{\mathbf{x}}}\right],$$

dass

$$T_s\left(t, \overrightarrow{\mathbf{x}}\right) \iff PA \vdash \varphi_{T_s}\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{t,\overrightarrow{\mathbf{x}}}\right].$$

Denn einmal ist PA stärker als RA, andererseits ist PA im Modell der natürlichen Zahlen erfüllt, also folgt aus

$$PA \vdash \varphi_{T_s}\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{t,\overrightarrow{\mathbf{x}}}\right]$$

auch, dass $\varphi_{T_s}\left[\overrightarrow{\mathbf{u}}/\overrightarrow{\mathbf{c}}_{t,\overrightarrow{\mathbf{x}}}\right]$ in $\mathbb{N}$ wahr ist, somit folgt $T_s\left(t, \overrightarrow{\mathbf{x}}\right)$. Damit haben wir:

Satz 16. *Die Menge der Folgerungen aus dem Axiomensystem für PA ist nicht entscheidbar.*

Bemerkung: So kann man für jede konsistente Erweiterung von RA vorgehen, die in $\mathbb{N}$ erfüllt ist.

5.3. Die Unvollständigkeit der Peanoarithmetik erster Stufe. Erinnerung: Die Peanoarithmetik wäre vollständig genau dann, wenn für jede Aussage ihrer Sprache (erststufig!) α der Fall wäre:

$$PA \vdash \alpha \text{ oder } PA \vdash \neg \alpha.$$

Zunächst haben wir ein abstraktes rekursionstheoretisches Argument: Wäre die Peanoarithmetik vollständig, so ergäbe sich aus der rekursiven Axiomatisierbarkeit, dass sie entscheidbar wäre. Ganz allgemein hat man:

Satz 17. *Eine vollständige rekursiv axiomatisierbare Theorie T ist entscheidbar.*

Beweis: Nach dem früheren Satz ist die Menge aller Aussagen aus T rekursiv aufzählbar. Sei $(\alpha_i)_{i\in\mathbb{N}}$ eine rekursive Aufzählung dafür. Man stelle zu beliebig vorgelegter Aussage β effektiv diese Liste so weit her, bis β oder aber $\neg \beta$ darin aufgetreten ist. So kann man für jede Aussage β entscheiden, ob β folgt oder nicht. (Sollte T inkonsistent sein, so ist sie banal entscheidbar - alle Formeln gehören dann dazu.■

Somit folgt aus dem oben bewiesenen Satz über die Unentscheidbarkeit von PA sofort ihre Unvollständigkeit:

Satz 18. *Die Peanoarithmetik ist unvollständig.*

Wir können die Aussage verschärfen: Es gibt Π_1- Aussagen, die in $\mathbb{N}$ wahr, aber nicht aus dem Axiomensystem für PA beweisbar sind.

Aber es fragt sich doch, angesichts der gewaltigen Vielfalt dessen, was man alles im System PA beweisen kann, ob man spezifische mathematisch interessante in $\mathbb{N}$ gültige Aussagen angeben kann, die man nicht darin beweisen kann. Zu dieser Frage sind einige erweiternde Bemerkungen anzubringen:

5.3.1. *Gödels Aussage: 'ich bin nicht beweisbar'.* Gödel gab eine konkrete 'künstliche' Aussage an, die wahr und unbeweisbar ist: Es ist eine Aussage φ, die ihre eigene Unbeweisbarkeit behauptet, in folgender Weise zu präzisieren, hart an bekannte Form semantischer Antinomie schrammend:

$$\mathbb{N} \vdash \varphi \leftrightarrow \neg\, Bew\left(c_{\ulcorner\varphi\urcorner}\right).$$

Dabei ist $Bew(x)$ das oben beschriebene Prädikat, das die Beweisbarkeit der Formel mit der Nummer x ausdrückt. $c_{\ulcorner\varphi\urcorner}$ ist der konstante Term $S...S0$ für $\ulcorner\varphi\urcorner$. Das Argument für die Existenz einer solchen Aussage ist eng mit dem Argument beim Rekursionssatz verwandt. Nehmen wir nun eine solche Gödelsche Aussage φ. dann sieht man sofort, dass φ wahr ist, aber nicht beweisbar. Wäre sie falsch, so wäre sie beweisbar, aber nur wahre Aussagen sind beweisbar. Wäre sie beweisbar, so wäre sie falsch.

Wir wollen einsehen, wie man eine solche 'Gödel-Aussage' φ konstruieren kann: Offenbar ist folgende Funktion rekursiv:

$\sigma(m,n)$: = Gödelnummer der Formel, die aus der Formel $\alpha(x)$ mit Gödelnummer m entsteht, wenn man für x einsetzt : c_n (den konstanten Term für n), also

$\sigma(m,n)$: $= \ulcorner \alpha(x/c_n) \urcorner$, mit $\ulcorner \alpha(x) \urcorner = m$.

Sei nun

$$m = \ulcorner \rightharpoonup Bew(x) \urcorner,$$

dann

$$\sigma(m,m) = \ulcorner \rightharpoonup Bew(c_m) \urcorner.$$

Also hat man mit

$$\varphi := \rightharpoonup Bew(c_m)$$

Folgendes:

$$\mathbb{N} \models \varphi \leftrightarrow \rightharpoonup Bew\left(c_{\sigma(m,m)}\right).$$

Das heißt wegen $\sigma(m,m) = \ulcorner \rightharpoonup Bew(c_m) \urcorner$ aber, dass die Aussage φ ihre eigene Unbeweisbarkeit ausdrückt.

5.3.2. *Gödels zweiter Unvollständigkeitssatz: Unbeweisbarkeit der Konsistenz von PA in PA.* Gödel bewies später auch, dass $PA \nvdash con(PA)$. Dabei ist die Aussage $Con(PA) : \exists x\,(Fml(x) \wedge \rightharpoonup Bew(x))$. Er sah auch: Jede widerspruchsfreie Theorie, in der man über Zahlen wie in PA reden kann, ist unvollständig in dem Sinne, dass ihre eigene Konsistenz nicht in ihr bewiesen werden kann. Das hat eine starke Konsequenz für die Mengenlehre, das umfassende System (Genaueres dazu im letzten Kapitel über Mengenlehre), in dem die gesamte Mathematik arbeitet: Man kann die Widerspruchsfreiheit der Mathematik nicht beweisen.

5.3.3. *Interessante mathematische Aussagen über die natürlichen Zahlen, die wahr sind, aber nicht beweisbar in PA.* Nun wirkt das eine Beispiel von Gödel künstlich, das andere ist ein von Hilbert als drängend gestelltes Problem, aber eben doch 'metamathematisch' und nicht von der Art, wie man typische mathematisch interessante Probleme in der Zahlentheorie hat. Hier führte zunächst die Lösung von Hilberts zehntem Problem weiter: Es sind diophantische Probleme (der ganzzahligen Lösbarkeit von Polynomgleichungen), die man nicht in PA lösen kann. Aber auch da ist noch die Frage, ob es mathematisch interessante Gleichungen sind. Tatsache ist allerdings, dass man nicht etwa in der elementaren Zahlenthoerie von PA das Fermatproblem gelöst hat, sondern mit wesentlich 'höheren' Methoden. Auf der Suche nach mathematisch interessanten Unabhängigkeiten von PAgelang es (Mitte der 70er Jahre) Paris und Harrington, ein kombinatorisches 'Ramsey-' Prinzip als unabhängig von PA zu erweisen.

5.4. Der Satz von Tarski: Wahrheit in der Zahlentheorie ist nicht einmal arithmetisch. Wir kommen zum letzten der gestellten Probleme: Welchen Status (oder welche Komplexität) hat die Menge der in $\mathbb{N}$ gültigen Aussagen? Zugleich kommen wir an ein Beispiel einer so komplexen Menge von natürlichen Zahlen, dass sie nicht einmal viel weiter oben in der arithmetischen Hierarchie dargestellt werden kann. Das Argument lässt sich völlig parallelisieren zu dem ersten Gödelschen für die Unvollständigkeit von PA.

Gäbe es eine arithmetische Formel, welche 'Wahrheit in $\mathbb{N}$' ausdrückt, nennen wir sie $tr(x)$, dann hätten wir

$$\mathbb{N} \models tr(c_{\ulcorner \varphi \urcorner}) \leftrightarrow \varphi$$

für alle Aussagen φ in der Sprache von PA. (Wir schreiben hier kürzer nur $\ulcorner \varphi \urcorner$, wenn genauer der zugehörige konstante Term gemeint ist.) Dann hätten wir (mit demselben Argument wie bei der 'Gödel-Aussage' für die Unbeweisbarkeit auch eine Formel, die von sich selbst sagt, sie sei falsch, also

$$\mathbb{N} \models \rightharpoonup tr(c_{\ulcorner \varphi \urcorner}) \leftrightarrow \varphi.$$

Wäre φ wahr, so

$$\mathbb{N} \models \rightharpoonup tr(c_{\ulcorner \varphi \urcorner}).$$

Dann wäre φ also falsch in $\mathbb{N}$. Wäre φ falsch in $\mathbb{N}$, also

$$\mathbb{N} \models \rightharpoonup \varphi,$$

so hätte man

$$\mathbb{N} \models tr\left(\ulcorner \varphi \urcorner\right),$$

und φ müsste falsch sein. Hier kommt also heraus, dass es keine solche Formel $tr\left(x\right)$ geben kann. (Bei Gödels Argument war es andersherum: Es gibt die Aussage, die ihre eigene Unbeweisbarkeit behauptet, und es kam heraus, dass sie wahr und unbeweisbar sein muss.)

KAPITEL 3

Mengenlehre

1. Einige Bemerkungen zur Bedeutung der Mengenlehre

Mengenlehre ist ein unentbehrliches Hilfsmittel zur Darstellung komplexerer Mathematik. Das erkannte schon D. Hilbert, kurz nachdem Cantor Ende des 19. Jahrhunderts die Mengenlehre entwickelte. Erste Einsichten stammen von Cantor selbst, insbesondere die Gleichmächtigkeit von $\mathbb{N}$ und $\mathbb{Q}$ (d.h. es gibt eine Bijektion zwischen ihnen) und die höhere Mächtigkeit von $\mathbb{R}$ als die von $\mathbb{N}$, allgemeiner: Die Potenzmenge einer Menge ist mächtiger als diese Menge selbst.

Aber es sind nicht nur gewisse Mengen wir die genannten und einige mehr (mit Strukturen darauf) mathematisch wichtige Objekte, sondern auch die Beziehungen zwischen ihnen, also insbesondere ihre Abbildungen bzw. strukturerhaltende Abbildungen (Homomorphismen). Ferner gehören Operationen, also Abbildungen, sowie Relationen auf den Mengen zur Definition von Strukturen. Wo aber stehen die grundlegenden Definitionen der Begriffe 'Abbildung', 'Relation'? Sie stehen in der Mengenlehre - eine $k-$*stellige* Relation auf A ist eine Teilmenge von $A^k = A \times ... \times A$, und

$$A \times B = \{\, (a,b) |\, a \in A, b \in B \}\,.$$

Was aber ist ein Paar (a,b)? Das ist definiert durch

$$(a,b) := \{a, \{a,b\}\}.$$

Eine Funktion (Abbildung) von A nach B ist eine Teilmenge $R \subset A \times B$, die Folgendes erfüllt:

$$\forall a \in A \exists b \in B \forall c \in B \,((a,b) \in R \wedge ((a,c) \in R) \implies c = b)\,.$$

Damit sollte bereits klar sein, dass die grundlegenden Begriffe der Mathematik nur in der Mengenlehre haben definiert werden können. Zu diesem Komplex gehören auch die Grundobjekte 'natürliche Zahlen', aus denen bekanntlich dann die rationalen und die reellen sowie komplexen aufgebaut sind: In der Mengenlehre kann man sie à la von Neumann so definieren:

$$\begin{aligned} 0 &: = \emptyset, \\ Sn &: = n \cup \{n\}. \end{aligned}$$

Also $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\} = \{0,1\}$, $3 = \{0,1,2\}$ usw.

Insgesamt gelingt die Konstruktion aller mathematischen Objekte in der Mengenlehre aus der leeren Menge. Man kann demnach alle mathematischen Objekte als Mengen auffassen.

Nun fungieren die natürlichen Zahlen sowohl als Ordnungszahlen und als die endlichen Kardinalzahlen (Mächtigkeiten). So bekommt man auch bereits die Wohlordnung der Menge aller natürlichen Zahlen, welche Induktion erlaubt. Eine tiefgehende Frage ist, ob man das auch für unendliche Mengen durchführen kann. Die Antwort ist im Wesentlichen positiv, aber mit einem negativen Beigeschmack. Sie führt auf Fragen, die erst von Cohen 1966 beantwortet wurden.

Wir sind bereits bei einigen für die Mathematik grundlegenden Beweisprinzipien angelangt. Dazu gehören insbesondere das Auswahlaxiom (bzw. Varianten davon) und dann auch die Kontinuumshypothese. Es sei vorab ein wenig davon aufgezählt, was man ohne das Auswahlaxiom alles nicht kann bzw. hat:

- Beliebige Mengen hinsichtlich ihrer Mächtigkeit vergleichen,

- die Gleichwertigkeit von 'die Menge A hat eine echte Injektion in sich' und 'A hat eine zu $\mathbb{N}$ gleichmächtige Teilmenge',

- Anordnungsfähigkeit oder sogar Wohlordnung einer beliebigen Menge,

- die erwartete große Anzahl (statt Null) von Elementen in einem unendlichen Produkt topologischer Räume,

- Basen beliebiger Vektorräume,
- allgemeiner das Zornsche Lemma, das man gern in der Mathematik benutzt.

Das bisher Ausgeführte sollte klargestellt haben, dass eigentlich alle fundamentale Mathematik in der Mengenlehre (und nur darin) formulierbar ist. Man könnte dabei einzuwenden denken, dass es doch bereits vor der Mengenlehre (sehr ordentliche und reichhaltige) Mathematik gegeben habe. Die Erklärung ist sehr einfach: Man hat dabei gewissermaßen mit größeren Molekülen statt mit Atomen oder Elementarteilchen gearbeitet, d.h. komplexere Grundobjekte - typisches Beispiel: Folgen, Abbildungen - als Ganze erfasst und damit nach korrekten Regeln gearbeitet. Zu einem großen Teil geschieht das auch heute so: Jemand lernt Mathematik auf der Hochschule und lernt dabei, mit Zahlen und Funktionen umzugehen, lernt sogar Algebra und Topologie und sogar algebraische Topologie und algebraische Geometrie, ohne die Rückführung auf 'Atome', weiß nicht einmal davon. Das ist (glücklicherweise) möglich, aber manchmal auch ein Schaden: Es wird von mir als unglücklich angesehen, dass es heute vielfach üblich ist, die reellen Zahlen nur als 'gottgegeben' mit ihren axiomatischen Eigenschaften anzugeben, ohne sie aus den natürlichen Zahlen zu konstruieren. Bei solchem Vorgehen geht auch viel Verständnis verloren. Aber hier ist ein noch grundsätzlicherer Einwand:

Das unbekümmerte Arbeiten mit mathematischen Objekten hat tatsächlich schon einmal dazu geführt, dass man den Bogen überspannte und mitten in einer widersprüchlichen 'Theorie' landete. Witzigerweise geschah das gerade mit der Mengenlehre selbst: Man bildete mit irgendwelchen definierbaren Eigenschaften E jeweils die Menge

$$\{x|\, x \text{ hat Eigenschaft } E\}\,.$$ (Allgemeine 'Komprehension' der 'naiven Mengenlehre'.

Aber das ist grober Unfug und führt zu folgendem Widerspruch ('Russelsche Antinomie'): Bilde nach dieser Regel

$$u = \{x|\, x \notin x\}\,.$$

(In Worten: Die Menge aller Mengen, die sich selbst nicht als Elemente enthalten.) Nun hat man

$$u \in u \iff u \notin u.$$

Also darf es eine solche Menge nicht geben, ohne dass die ganze Mathematik widersprüchlich wird.

Das löste die berühmte 'Grundlagenkrise der Mathematik' zu Beginn des 20. Jahrhunderts aus, und es gab hitzige Debatten darüber, was zu tun sei (von 'Mengenlehre verwerfen' bis zu 'Mengenlehre retten', beim Retten von restriktiveren bis zu sehr liberalen Lösungen). Die Debatte endete pragmatisch: Man konnte mit viel Arbeit Systeme aufstellen, welche den Widerspruch vermeiden (wir wissen schon, dass man die Widerspruchsfreiheit einer solchen Mengenlehre keinesfalls in dieser selbst beweisen kann, mit Gödels zweitem Unvollständigkeitssatz), also ist 'Widerspruch ist vermieden' eine nur empirische Aussage: Auch größte bisherige Strapazierung hat nie mehr zu einem Widerspruch geführt. Hinzu kommt: Man ging dabei überzeugend so vor, dass man eine Version der Mengenlehre lieferte (gleich stellen wir das gebräuchlichste System ZF (für 'Zermelo-Fraenkel-Mengenlehre') vor), welche solch problematische Aussagen wie das Auswahlaxiom oder die Kontinuumshypothese aussparte und dann zeigte: Wenn dies widerspruchsfrei ist, dann ist auch das um diese 'Problemfälle' angereicherte System widerspruchsfrei (Gödel). Man kann aus dem ganzen Vorgang die Lehre ziehen: Konkrete (und harte, schwierige) mathematische Arbeit führte zu einer weitgehenden Klärung, so weit gehend, wie sie (beweisbar) nur sein kann. Typisch philosophische Debatten der Art, welche Denkprinzipien zulässig oder unzulässig sei, je nach dem 'Wesen' der Mathematik, sei sie nun menschliches Konstrukt oder eine platonische Welt, die unabhängig vom Menschen und seiner Erkenntnis existiere, führten zu gar nichts. Lediglich kann man mit Gewinn nach dem 'Konstruierbaren' im Sinne des Berechenbaren fragen und damit mehr Licht auf diesen Aspekt der Mathematik werfen. (In der Logik ist das der Abschnitt 'Rekursive Funktionen usw.', aber auch in der gesamten Mathematik achtet man seither gern darauf, ob eine Aussage 'effektiv' ist, also ein Konstruktionsverfahren liefert.) Ansonsten hat man keinen Anlass, die Mathematik unnötig kompliziert zu machen, indem man sich solcher Errungenschaften wie des Auswahlaxioms begibt. (Wir werden noch konkreter sehen, welch merkwürdige Dinge passieren, wenn das Auswahaxiom nicht zugegen ist.)

Eine letzte Bemerkung: Wie verhält sich die mathematische Grundlage 'Prädikatenlogik', die wir kennenlernten, zur Grundlage 'Mengenlehre'? Einerseits ist die Prädikatenlogik eine Grundlage für die Mengenlehre, wie wir noch deutlich sehen werden: ZF ist als Theorie der Prädikatenlogik erster Stufe formuliert, und es sich sehr nützlich, sich darüber klar zu sein. Das bedeutet: Es ziehen alle Überlegungen zur Existenz einer Vielzahl von Modellen jeder Theorie erster Stufe, wenn es nur ein unendliches Modell

gibt. Daraus ergibt sich sofort die Einsicht: Es gibt kein 'absolutes' Mengenuniversum, kein irgendwie ausgezeichnetes Modell. Aber positiv wirkte sich die Anwendung der Modelltheorie (der Modelle erststufiger Theorien) darin aus, dass man aus der Existenz von Modellen von ZF auf die Existenz von Modellen von ZF mit Auswahlaxiom und auch auf die Existenz von Modellen von ZF schließen konnte, welche das Auswahlaxiom verletzen. (Ebenso für die Kontinuumshypothese.) Dabei hatte man allerdings die für algebraische Zwecke übliche Modelltheorie um einige neue Methoden zu erweitern.

Hier soll noch ein anderer Aspekt der $ZF-$ Mengenlehre angesprochen werden. Eng verwandt mit der Russelschen Antinomie sind auch semantische Antinomien wie die des Lügners: Jemand sagt: 'Ich lüge'. (Klassische Form: Ein Kreter sagt: 'Alle Kreter lügen'.) Hier ist die Auflösung die, dass man zwischen Objekt- und Metasprache unterscheidet, also: Wenn man sagt: 'Der Satz φ ist falsch', dann redet man über den Satz φ, dieser ist Objekt einer Betrachtung, welche in der Aussage 'φ ist falsch' mündet. Dieser Satz spricht über φ, gehört also der Metasprache an. Durch diese Unterscheidung wird der Unfug vermieden, dass ein Satz von sich selbst sagt, er sei falsch. Übrigens hat die Gödelsche Konstruktion des Satzes, der seine eigene Unbeweisbarkeit behauptet, diesen Charakter, vermeidet aber den Widerspruch dadurch, dass zur Objektsprache nur die Gödelnummer eines Satzes gehört. Nun hat man aber auch in der Mathematik zunächst die Notwendigkeit, sogar unendlich viele Metaebenen einzuführen: Unten stehen die Grundobjekte, typisch Zahlen, dann kommen die Relationen und Funktionen darüber, dann die Relationen zwischen Relationen und Funktionen von Funktionen, usw., usw. In diesem Sinne heißt es in der klassishcen Mathematik: sin ist eine Funktion, das Integral ist ein Funktional, die Ableitung ist ein Operator. Systematisch haben Russel und Whitehead die Typentheorie entwickelt, diesen Aufbau systematisch darzustellen. Man sieht recht schnell, dass dies entsetzlich kompliziert wird. Im Sinne der Mengenlehre kann man es so verdeutlichen: Man hat Mengen von Zahlen, dann Mengen höherer Stufe, die Mengen von Zahlenmengen sind, dann wieder Mengen von Mengen von Mengen. Man hätte Mengen aller Stufen zu unterscheiden und damit auch 'leere Menge' für jede Stufe zu unterscheiden. Die $ZF-$ Mengenlehre macht deutlich, dass dies glücklicherweise völlig unnötig ist, ohne dass notwendige Unterscheidungen zu Bruch gehen: Alle Objekte sind Mengen, es sind also keine Objekte nötig, die keine Mengen sind und von diesen zu unterscheiden. Relationen höherer Stufen und Abbildungen höherer Stufen sind alle ebenso nur einfach: Mengen. Aber die Unterschiede werden daran erkennbar, wie viele ineinander geschachtelte Mengenklammern man hat. Es ist also eine große Leistung solcher Systeme wie ZF, dass man die gesamte Mathematik in ein relativ einfaches überschaubares System bringen kann, ohne Vernachlässigung wichtiger Unterscheidungen. Die Prädikatenlogiken höherer Stufen werden damit unnötig, das erststufige System tut alles. Die Mengenlehre ist auch eine Grundlage zur Formulierung der Prädikatenlogik erster Stufe: Eine Struktur ist eine nicht leere Menge mit Relationen und Operationen..., diese Objekte setzt die Prädikatenlogik voraus aus der Mengenlehre. Ebenso möchte man präzise formulieren, was eine Zeichenreihe, eine Formel ist - wiederum sind diese Objekte nur in der Mengenlehre wiederum formulierbar. Also ergänzen sich Prädikatenlogik erster Stufe und Mengenlehre wechselseitig zu dem, was man Grundlagen der Mathematik nennen kann.

2. Das axiomatische System ZF der Mengenlehre

Es gibt verschiedene Formen dafür, wir wählen die von T. Jech, formulieren nur leicht abgewandelt, dass die erststufige Formulierung deutlicher wird. Die Sprache von ZF hat als einziges nichtlogisches Symbol nur ein zweistelliges Relationssymbol $\in$ (für '...ist Element von ...').

Damit die Formulierung leichter lesbar und unmittelbar verständlich wird, benutzen wir bereits folgende Abkürzungen:

$$\begin{array}{rcl} x & \subset & y \text{ für } \forall z\,(z \in x \to z \in y)\,, \\ x \cap y & : & = \{\, z |\, z \in x \wedge z \in y\} \\ & & (x, y) \text{ für } \{x, \{x, y\}\}, \text{ also die Menge mit den aufgeführten Elementen.} \\ & & \emptyset \text{ für die leere Menge, also } \forall x\,(\rightharpoonup x \in \emptyset) \\ & & f''x \text{ für das Bild von } x \text{ unter der Funktion } f. \end{array}$$

Erläuterung: Die erste ist klar, zur zweiten hat man zu bemerken, dass im folgenden Axiomensystem zu allen Mengen x, y die eindeutige Existenz von $x \cap y$ garantiert wird mit $M3$ und $M1$. **Übung:** Man führe das aus.

Unten fordert das Axiom $M2$, dass mit Mengen x, y auch die Menge $\{x, y\}$ existiert, erneute Anwendung von $M2$ liefert die Existenz von $\{x, \{x, y\}\}$, und die ist nach $M1$ (Extensionalitätsaxiom) eindeutig. Also ist die Bildung des Terms $\{x, \{x, y\}\}$ eine definitorische Erweiterung, und wir benutzen die in der Mathematik übliche Abkürzung (x, y).

Zur leeren Menge: Es schadet nicht, wenn man noch $\emptyset$ als Konstante hinzufügt und die Aussage $\forall x\,(\multimap x \in \emptyset)$ als Axiom. Tatsächlich ist das nicht nötig, weil in der Prädikatenlogik stets $\exists x\,(x \doteq x)$ ableitbar ist und dann mit Mengenkomprehension (Axiom $M3$) gebildet werden kann:

$$\exists y \forall u\,(u \in y \leftrightarrow u \in x \wedge \multimap u \doteq u)\,,$$

und die Formel

$$\forall u\,(u \in y \leftrightarrow u \in x \wedge \multimap u \doteq u)$$

definiert eindeutig mit dem Extensionalitätsaxiom $M1$ die leere Menge. Damit wird die Konstante $\emptyset$ und ein Axiom der Form $\forall x\,(\multimap x \in \emptyset)$ überflüssig. Alles kann ohne sie ausgedrückt und hergeleitet werden. Gerade in der Mengenlehre sind solche 'definitorischen Erweiterungen' von großer Wichtigkeit.

Eine besondere Bemerkung ist bei dem Bild von x unter der Funktion f anzubringen: In der Mathematik schreibt man stets $f(x)$ dafür. Also $f(A) = \{b|\,(\exists a \in A)\, f(a) = b\}$. Warum hier nicht? Das hat einen wirklichen Grund: Hier sind alle Objekte Mengen, und Funktionen ordnen *jeder* Menge eine Menge zu. Also ist $f(x)$ schon vergeben für die Menge, die durch f der Menge x zugeordnet ist. Und das ist nicht etwa die Menge der Objekte, die $f-$ Werte der Elemente von x sind. Daher wird die Unterscheidung zwischen $f(x)$ und $f''x$ nötig. Noch etwas zu den Funktionen: Es handelt sich wieder um definitorische Erweiterungen: Betrachtet werden Funktionen, die durch $ZF-$ Formeln definierbar sind, also ist $f(x) \doteq y$ eine Abkürzung für

$$\forall u \exists v \forall w\,\left(\varphi\left(\overrightarrow{\mathbf{p}}, u, v\right) \wedge \left(\varphi\left(\overrightarrow{\mathbf{p}}, u, w\right) \rightarrow w \doteq v\right)\right) \wedge \varphi\left(\overrightarrow{\mathbf{p}}, x, y\right),$$

mit einer $ZF-$ Formel φ. $f''x$ ist dann

$$(*)\quad \{y|\,\exists z \in x : f(z) \doteq y\}\,.$$

Dabei ist für $f(z) \doteq y$ der oben genannte Ausdruck einzusetzen. Nun verlangt das Ersetzungsaxiom $M6$, das dieser 'Klassenterm' $(*)$ tatsächlich eine Menge beschreibt.

Definition 32. *Das System ZF ist definiert durch folgendes Axiomensystem:*

$M1$ $\forall x \forall y\,(\forall z\,(z \in x \leftrightarrow z \in y) \rightarrow x \doteq y)$ *(Extensionalität)*

$M2$ $\forall x \forall y \exists z \forall u\,(u \in z \leftrightarrow u \doteq x \vee u \doteq y)$ *('Paarbildung', lieber 'Menge aus zwei Objekten')*

$M3$ $\forall \overrightarrow{\mathbf{p}} \forall x \exists y \forall u\left(u \in y \leftrightarrow u \in x \wedge \varphi\left(u, \overrightarrow{\mathbf{p}}\right)\right)$ *(Mengenkomprehension),*

dabei ist φ eine beliebige Formel der Sprache von ZF, in der nur $u, \overrightarrow{\mathbf{p}}$ frei sind.

$M4$ $\forall x \exists y \forall z \forall u\,(u \in z \wedge z \in x \rightarrow u \in y)$ *(Existenz der Vereinigung beliebiger Systeme von Mengen)*

$M5$ $\forall x \exists y \forall u\,(u \subset x \rightarrow u \in y)$ *(Existenz der Potenzmenge einer beliebigen Menge)*

$M6$ $\forall x \exists y\,(f''x \subset y)$ *(Ersetzungsaxiom), wobei*

f eine mit Parametern $ZF-$ definierbare Funktion ist, also $f \doteq \left\{(x, y)|\,\varphi\left(\overrightarrow{\mathbf{p}}, x, y\right)\right\}$

$M7$ $\exists x\,(\emptyset \in x \wedge \forall y\,(y \in x \rightarrow \{y\} \in x))$ *(Unendlichkeitsaxiom)*

$M8$ $\forall x\,(\multimap x \doteq \emptyset \rightarrow \exists y\,(y \in x \wedge x \cap y = \emptyset))$ *(Fundierungsaxiom)*

Erläuterungen: $M1$ ist aus dem allgemeinen mathematischen Gebrauch wohlbekannt, $M2$ wurde zuvor schon erklärt, wichtig ist $M3$: Es wurde im ersten Abschnitt gezeigt, dass allegemeine Mengenkomprehension widersprüchlich ist, und man sollte sehen, welche Einschränkungen, aber auch welche Freiheiten $M3$ noch gewährt: Man nimmt alle definierbaren Eigenschaften, das ist keine Einschränkung, da die Mengenlehre die allgemeinsten Definitionsmöglichkeiten liefert. Die Einschränkung liegt darin: 'Die Menge der Objekte mit Eigenschaft E' kann nicht mehr gebildet werden, sondern nur noch: 'Die Menge der Objekte aus der Menge x, welche die Eigenschaft E haben'. Die 'Menge aller Mengen' ist zu groß, das gibt Widersprüche. Andererseits wird mit dem Unendlichkeitsaxiom und dem Potenzmengenaxiom garantiert, dass es gewaltige Mengen gibt, weit über alles in der Mathematik Benötigte hinaus. Man mache sich klar, dass die Menge aller Operatoren, welche jeder Funktion $\mathbb{R} \rightarrow \mathbb{R}$ eine Funktion $\mathbb{R} \rightarrow \mathbb{R}$ zuordnen, dazu gehört.

Übung: Man erläutere, dass Vereinigungsaxiom, Potenzmengenaxiom und Ersetzungsaxiom nicht wörtlich das Erwartete formulieren, dass dies aber mit $M3$ folgt. Man erkäre, dass das Unendlichkeitsaxiom die Existenz einer unendlichen Menge garantiert.

Noch zu $M8$, dem Fundierungsaxiom: Damit werden überhaupt Mengen, welche sich selbst als Element enthalten, ausgeschlossen, mehr noch alle Ketten $x \in y \in ... \in x$. Denn mit einer solchen Kette hätte man eine unendliche absteigende Kette nicht leerer Mengen $x_0 \ni x_1 \ni x_2 ... \ni x_n \ni ...$, für alle n, und dann wäre

$$U = \{ x_i | \, i \in \mathbb{N} \}$$

eine Menge, die dem Fundierungsaxiom widerspricht: Für jedes Element x_n gilt $x_{n+1} \in U \cap x_n$. Dabei ist U eine Menge mit dem Ersetzungsaxiom, und $\mathbb{N}$ ist die bereits eingeführte Menge der natürlichen Zahlen, deren Existenz aus dem Unendlichkeitsaxiom folgt. Noch etwas folgt aus $M8$: Es existiert nicht die 'Menge aller Mengen', als Klassenterm wäre sie zu beschreiben durch $V = \{ x | \, x \doteq x \}$. Denn sonst $V \in V$.

Definition 33. *Das System ZFC (ZF mit Auswahlaxiom AC für 'axiom of choice') ist gegeben mit den Axiomen $M1$ bis $M8$ und zusätzlich*

$$AC \; \forall x \left(\rightharpoonup \emptyset \in x \rightarrow \exists f : x \rightarrow V \left((\forall u \in x) \, f \left(u \right) \in u \right) \right).$$

Bemerkung: Hier wurde wiederum eine dem mathematischen Sprachgebrauch naheliegende Formulierung gewählt. Inhaltliche Bedeutung: Wenn x ein System nichtleerer Mengen ist, dann gibt es eine Funktion, die jeder Menge u dieses Systems (also $u \in x$) genau ein Element von u zuordnet. Man kann das Axiom aber auch unmittelbar so in der Sprache von ZF formulieren: Zu jedem System nichtleerer Mengen gibt es eine 'Auswahlmenge', die aus jeder dieser Mengen genau ein Element enthält.

3. Wichtige gleichwertige Aussagen zu *AC*

Definition 34. *Eine Wohlordnung $<$ auf einer Menge A ist eine totale Ordnung, also*

$$\begin{aligned} &\forall a \; \rightharpoonup \; a \; < \; a, \\ &\forall a \forall b \forall c \left(a < b \wedge b < c \rightarrow a < c \right), \\ &\forall a \forall b \left(a \doteq b \vee a < b \vee b < a \right), \end{aligned}$$

die zusätzlich erfüllt: Jede Teilmenge von A, die nicht leer ist, hat ein kleinstes Element im Sinne von $<$.

Bemerkung: Die übliche Ordnung der natürlichen Zahlen ist eine Wohlordnung. Eine Wohlordnung ermöglicht stets Definitionen und Beweise durch Rekursion, auch bei größeren Kardinalzahlen als der von $\mathbb{N}$.

Problem: Kann man jede Menge wohlordnen?

Definition 35. *Eine partielle Ordnung $<$ auf einer Menge A erfüllt die ersten beiden Axiome der totalen Ordnung. Eine total geordnete Teilmenge von A heißt eine Kette. Eine obere Schranke für eine Kette K in A ist ein Element $a \in A$ mit $a \geq b$ für alle $b \in K$.*

Lemma 14 (Zornsches Lemma). *Eine partielle Ordnung auf einer nichtleeren Menge hat ein (im Allgemeinen nicht eindeutig bestimmtes) maximales Element, wenn jede Kette eine obere Schranke besitzt.*

Es geht hier nicht darum, dies Lemma zu beweisen, das geht auch gar nicht in ZF, wie wir noch sehen werden. Sondern wir haben folgendes

Satz 6. *Auswahlaxiom, Zornsches Lemma und die Existenz einer Wohlordnung auf jeder Menge sind äquivalent.*

Dieser Satz wird im nächsten Abschnitt bewiesen, wir benötigen dazu die Ordinalzahlen. Später werden wir noch sehen, dass auch die Aussage '$|x| = |x \times x|$ für alle unendlichen x' ein Äquivalent zum Auswahlaxiom ist.

Einige (für die Mathematik schöne) Folgerungen aus ZFC, die man ohne AC nicht zur Verfügung hat:

1.) Jeder Vektorraum W hat eine Basis. Der Beweis ist mit dem Zornschen Lemma einfach: Die linear unabhängigen Teilmengen bilden mit $\subset$ eine partielle Ordnung, wobei natürlich $\subset$ dem $\leq$ entspricht, und jede Kette hat eine obere Schranke, bilde einfach ihre Vereinigung. Ein ´maximales Element ist aber eine Basis. Denn das maximale Element ist nach Definition eine linear unabhängige Menge M, und zwar eine maximale. Das ist aber eine Basis, wenn es ein Erzeugendensystem ist. Wäre es das nicht, könnte man einen Vektor $v \in W$ nicht als endliche Linearkombination der Vektoren aus M darstellen, so hätte man mit $M \cup \{v\}$ eine linear unabhängige Menge, die der Maximalität von M widerspricht.

2.) Ebenso bekommt man für jeden Körper eine Transzendenzbasis über einem beliebigen Unterkörper, also insbesondere für $\mathbb{R}$ über $\mathbb{Q}$.

3.) Jedes Ideal in einer Booleschen Algebra ist zu einem maximalen Ideal zu erweitern. (Ein Ideal I in einer Booleschen Algebra B ist eine nichtleere *echte* Teilmenge von B, die unter $+$ abgeschlossen ist und mit einem Element jedes kleinere enthält. Eine Boolesche Algebra ist eine Struktur $(A, 0, 1, +, \cdot, -)$, in der dieselben Gesetze wie in einer Mengenalgebra $(M, \emptyset, M, \cup, \cap, \text{Komplementbildung})$ gelten, die definierbare Halbordnung ist $u \leq v \iff u + v = v$. Ein maximales Ideal ist ein solches, so dass für alle $x \in B$ stets genau eine der Aussagen $x \in I$ oder $-x \in I$ zutrifft.) Konkrete Anwendung: Jede konsistente Aussagenmenge kann zu einer vollständigen Aussagenmenge ergänzt werden, die konsistent ist.

4.) Jeder Filter lässt sich zu einem Ultrafilter erweitern. (Das ist dual zu 3, für sich sehr interessant, nämlich: Ein Mengensystem $F \subset \mathcal{P}(X)$ heißt Filter auf X, wenn F unter Obermengenbildung abgeschlossen ist und mit $A, B \in F$ auch $A \cap B \in F$ und $\emptyset \notin F$. Ein Ultrafilter auf X ist ein Filter, für den gilt: Für jede Teilmenge A von X gilt: $A \in F$ oder $\overline{A} \in F$. Dabei ist $\overline{A}$ das Komplement von A in X, also $X \setminus A$.)

5.) Jede Menge lässt sich total ordnen.

6.) Nun noch vier Aussagen zur Kardinalzahlarithmetik: $|x| = |x \times x|$ für alle unendlichen Mengen x. Wir bezeichnen mit $|x|$ allgemein die Mächtigkeit der Menge x, ihre Kardinalzahl. Genaueres zur Begriffsbildung folge weiter unten. $|x \cup y| = \max(|x|, |y|)$, wenn wenigstens eine der Mengen x, y unendlich ist. Für je zwei Mengen sind $|x|, |y|$ vergleichbar. Eine Menge ist Dedekind-endlich genau dann, wenn sie keine abzählbar unendliche Teilmenge besitzt. (Dedekind-endlich heißt eine Menge genau dann, wenn es keine echte Injektion der Menge in sich gibt.)

Eine unerwünschte Konsequenz des Auswahlaxioms mit ZF, also von ZFC :

Satz 19. *In ZFC ist ableitbar: Es gibt eine Teilmenge von $\mathbb{R}$, die nicht Lebesgue-messbar ist.*

Dazu benötigen wir die Definition, dass das Lebesguemaß μ folgende Eigenschaften hat:

$$\begin{aligned}
\mu(A) &\geq 0, \text{ wenn } \mu(A) \text{ existiert,} \\
\mu([a,b]) &= b - a \text{ für } a \leq b. \\
\mu(\cup_{i\in\mathbb{N}} A_i) &= \sum_{i\in\mathbb{N}} \mu(A_i), \text{ wenn } A_i \cap A_j = \emptyset \text{ für } i \neq j, \text{ und alle } \mu(A_i) \text{ existieren} \\
\mu(A) &= \mu(c + A), \text{ wenn } \mu(A) \text{ existiert.}
\end{aligned}$$

Beweis: Nenne zwei reelle Zahlen äquivalent, wenn die Differenz eine rationale Zahl ist. Das ist offenbar eine Äquivalenzrelation. Offenbar hat jede Klasse einen Repräsentanten in $[0, 1]$. Mit dem Auswahlaxiom exististiert also eine Menge $M \subset [0, 1]$, die von jeder Klasse genau einen Repräsentanten enthält. Damit existiert zu jeder reellen Zahl x genau ein $y \in M$ und genau ein $q \in \mathbb{Q}$, so dass $x = y + r$. Damit bildet

$$(M + r)_{r\in\mathbb{Q}}$$

eine Partition von $\mathbb{R}$. Wäre nun M messbar, dann wären es alle $M + r = \{y + r | \, y \in M\}$, und mit Translationsinvarianz $\mu(M_r) = \mu(M)$.

Erster Fall: $\mu(M) = 0$, dann wäre

$$\mu(\mathbb{R}) = \mu\left(\bigcup_{r\in\mathbb{Q}} (M + r)\right) = \sum_{r\in\mathbb{Q}} \mu(M + r) = 0.$$

. Das ist falsch, weil $\mu(\mathbb{R}) = \infty$ mit den Intervallmaßen.

Zweiter Fall: $\mu(M) > 0$. Dann

$$\mu([0,2]) \geq \mu\left(\bigcup_{0\leq r\leq 1,\ r\in\mathbb{Q}} (M+r)\right) = \sum_{0\leq r\leq 1,\ r\in\mathbb{Q}} \mu(M+r) = \infty.$$

Also führt die Annahme, M sei messbar, stets auf einen Widerspruch.■

4. Ordinalzahlen

DEFINITION 36 (Klasse aller Ordinalzahlen). *$On := \{x \in V \mid x$ transitiv und x durch $\in$ total geordnet $\}$. $x \in V$ heißt transitiv, wenn mit $u \in y \in x$ stets $u \in x$ folgt.*

Bemerkungen: On ist eine Klasse, keine Menge. Sonst hätte man $On \in On$ entgegen dem Fundierungsaxiom. $\emptyset$ ist offenbar die kleinste Ordinalzahl. mit $\alpha \in On$ ist $\alpha' := \alpha \cup \{\alpha\}$ offenbar wieder eine Ordinalzahl. Sie heißt Nachfolgerzahl von α. Ordinalzahlen, die weder $\emptyset$ noch Nachfolgerzahl sind, heißen Limeszahlen. Die kleinste Limeszahl ist

$$\omega = \{0, 1, 2, ...\}.$$

LEMMA 15. *Für jede Ordinalzahl α gilt: $\alpha = \{\beta \in On \mid \beta < \alpha\}$. Jede Ordinalzahl ist durch $\in$ wohlgeordnet. Die Klasse On selbst ist durch $\in$ wohlgeordnet, und man hat folgendes Rekursionsprinzip (für rekursives Definieren und Beweisen):*

$$\forall\alpha\,(\alpha \subset A \subset On \implies \alpha \in A) \implies A = On.$$

Beweis: Zur ersten Aussage beobachtet man, dass ein Element einer Ordinalzahl stets wieder eine Ordinalzahl ist, nämlich wieder transitiv und total geordnet. Und $\beta < \alpha$ bedeutet nach Definition $\beta \in \alpha$. Die zweite Aussage ergibt sich daraus, dass mit einer nichtleeren Teilmenge $y \subset x \in On$ ohne kleinstes Element im Sinne der Ordnung durch $\in$ eine unendliche absteigende $\in -$ Kette entstünde, entgegen dem Fundierungsaxiom. Für die dritte Aussage ist nur einzusehen, dass je zwei Ordinalzahlen α, β durch $\in$ $(<)$ vergleichbar sind: $\alpha \cap \beta \in On$, und wäre $\alpha \cap \beta < \alpha$ und $\alpha \cap \beta < \beta$, so hätte man $\alpha \cap \beta \in \alpha \cap \beta$, entgegen dem Fundierungsaxiom. Also $\alpha \cap \beta = \alpha$ oder $\alpha \cap \beta = \beta$. Damit $\alpha \leq \beta$ oder $\beta \leq \alpha$. Schließlich zum Rekursionsprinzip: Wenn $\alpha \notin A$ die kleinste Ordinalzahl ist (die gibt es mit der Wohlordnung von On), welche nicht in A liegt, dann gilt $\alpha \subset A$, also $\alpha \in A$. A ist nicht leer, weil $\emptyset \subset A$ und damit $\emptyset \in A$.■

DEFINITION 37 (des Kardinalzahlbegriffes in ZFC). *Eine Kardinalzahl ist eine Ordinalzahl, die zu keiner kleineren Ordinalzahl gleichmächtig ist. Die Kardinalzahl einer Menge x, symbolisch $|x|$, ist die kleinste Ordinalzahl, die zu x gleichmächtig ist. (Zwei Mengen heißen gleichmächtig, wenn es eine Bijektion zwischen ihnen gibt.)*

Bemerkung: Es sollte klar sein, dass in ZF allein diese Definition keineswegs funktioniert, dass man aber auf diese Weise in ZFC einen besonders eleganten Kardinalzahlbegriff besitzt. Wir werden noch sehen, dass sich bereits in ZFC, erst recht aber in $ZFC + GCH$ (ZFC mit verallgemeinerter Kontinuumshypothese) eine besonders einfache Kardinalzahlarithmetik ergibt.)

DEFINITION 38 (Rang einer Menge und von Neumannsche Hierarchie). *Rekursiv über $\alpha \in On$ lässt sich definieren:*

$$\begin{aligned} V_0 &:= \emptyset \\ V_{\alpha+1} &:= \mathcal{P}(V_\alpha) \\ V_\lambda &:= \bigcup_{\beta<\lambda} V_\beta \text{ für Limes-Ordinalzahlen } \lambda. \end{aligned}$$

Man hat $V = \bigcup_{\alpha\in On} V_\alpha$, und der Rang einer Menge x ist das kleinste $\alpha \in On$, so dass $x \in V_\alpha$.

Es sei bemerkt, dass der Sachverhalt am Fundierungsaxiom hängt.

5. Die Standard-Äquivalente des Auswahlaxioms

Wir werden den bereits ausgesprochenen Satz in folgender Art beweisen:

Satz 7. *AC* $\Longrightarrow$ *Wohlordnungssatz* $\Longrightarrow$ *Zornsches Lemma* $\Longrightarrow$ *AC. (Der Wohlordnungssatz besagt, dass jede Menge wohlgeordnet werden kann, was gleichwertig damit ist, dass jede Menge bijektiv auf eine Ordinalzahl abgebildet werden kann.)*

Beweis:

1.) *AC* $\Longrightarrow$ *Wohlordnungssatz* :

Sei A eine beliebige Menge. Wenn A leer ist, so ist nichts zu zeigen. Sei A nicht leer. Sei $a_0 \in A$ und $x \notin A$. Wir definieren folgende Abbildung, welche jeder Ordinalzahl α ein Element von $A \cup \{x\}$ zuordnet:

$$\begin{aligned} f(0) &= a_0, \text{ und für } \alpha > 0 : \\ f(\alpha) &= \begin{cases} \text{ein (mit Auswahlaxiom eindeutig bestimmbares) Element aus } A \setminus f''\alpha, \text{ wenn das existiert,} \\ x \text{ sonst.} \end{cases} \end{aligned}$$

Dann sei α die kleinste Ordinalzahl, für welche $f(\alpha) = x$ gilt. Eine solche muss es geben, weil sonst $f^{-1\prime\prime}A = On$, On müsste dann mit Ersetzungsaxiom eine Menge sein, was es nicht ist. Somit hat man für α:

$$f \restriction \alpha : \alpha \to A \text{ ist eine Bijektion.}$$

Mit $f \restriction x$ bezeichnet man gern die Einschränkung von f auf x, für eine Funktion f und eine Menge x. Daher ist die Wohlordnung von α über f auf A zu übertragen.

2.) *Wohlordnungssatz* $\Longrightarrow$ *Zornsches Lemma* :

Es sei $\langle A, < \rangle$ eine Halbordnung mit oberen Schranken für alle Ketten. Zu zeigen ist, dass es ein maximales Element gibt. Dazu zählen wir mit Voraussetzung des Wohlordnungssatzes die Menge A mit einer Ordinalzahl α auf:

$$A = \{ a_\beta | \, \beta \in \alpha \}, \; a_\beta \neq a_\gamma \text{ für } \beta \neq \gamma, \; \beta, \gamma \in \alpha.$$

Wir definieren:

$$\begin{aligned} b_0 &= a_0, \\ b_{\beta+1} &= \begin{cases} a_{\beta+1}, \text{ wenn } a_{\beta+1} > b_\beta \\ b_\beta \text{ sonst.} \end{cases}, \text{ für } \beta + 1 \in \alpha. \\ b_\lambda &= \begin{cases} a_\lambda, \text{ wenn } a_\lambda > b_\beta \text{ für alle } \beta \in \lambda, \\ a_\gamma \text{ mit kleinstem Index } \gamma \in \alpha, \text{ so dass } a_\gamma \geq b_\beta \text{ für alle } \beta \in \lambda \end{cases}, \text{ für Limeszahlen } \lambda \in \alpha. \end{aligned}$$

Bemerkung: In der Definition für b_λ hat man die Existenz einer oberen Schranke für alle b_β, $\beta \in \lambda$, nach der Voraussetzung des Zornschen Lemmas.

Nach Konstruktion bildet $\{ b_\beta | \, \beta \in \alpha \}$ selbst eine Kette. Sei nun a_γ eine obere Schranke dafür, γ minimal in dieser Eigenschaft. Wir behaupten, dass a_γ maximal ist. Wäre es das nicht, so hätten wir entweder $a_0 > a_\gamma$ oder für eine Nachfolgerzahl $\beta + 1 \in \alpha : a_{\beta+1} > a_\gamma$ oder für eine Limeszahl $\lambda \in \alpha : a_\lambda > a_\gamma$. All das kann aber nicht sein: $a_0 = b_0 \leq a_\gamma$, also nicht $a_0 > a_\gamma$. Wenn $a_{\beta+1} > a_\gamma$, dann $a_{\beta+1} > b_\beta$, weil $a_\gamma \geq b_\beta$. Dann wäre aber $b_{\beta+1} = a_{\beta+1} > a_\gamma$, somit a_γ keine obere Schranke für $\{ b_\beta | \, \beta \in \alpha \}$. Schließlich: Wenn $a_\lambda > a_\gamma$, dann $a_\lambda > b_\beta$ für alle $\beta \in \lambda$, also $b_\lambda = a_\lambda > a_\gamma \geq b_\lambda$, was wieder nicht sein kann.

3.) *Zornsches Lemma* $\Longrightarrow$ *AC* :

Sei A eine beliebige Menge von nicht leeren Mengen. Wir bilden die Menge aller Abbildungen

$$f : B \to \cup A \text{ mit } f(x) \in x \text{ für alle } x \in B.$$

Auf dieser Menge haben wir folgende Halbordnung:

$$f \leq g :\Longleftrightarrow dom(f) \subset dom(g) \text{ und } g \restriction dom(f) = f.$$

Zu jeder Kette K haben wir die obere Schranke $\cup K$. Nach dem Zornschen Lemma gibt es also eine maximale Abbildung im Sinne von $\leq$, die sei

$$f : B \to \cup A.$$

Wäre $B \subsetneqq A$, so hätte man mit $a \in B \setminus A$ und $x \in a$ die folgende Abbildung:

$$\begin{aligned} g &: B \cup \{a\} \to \cup A, \\ g(u) &= \begin{cases} f(u) \text{ für } u \in B, \\ x \text{ für } u = a. \end{cases} \end{aligned}$$

Damit wäre $g > f$ und somit f nicht maximal.■

Folgerung 2. *In ZFC gilt, dass irgend zwei Mengen hinsichtlich ihrer Mächtigkeit vergleichbar sind. Die Definition $|x| :=$ kleinste Ordinalzahl α, so dass es eine Bijektion $x \to \alpha$ gibt, ist zulässig.*

Beweis: Mit dem Wohlordnungssatz kann man jede Menge bijektiv auf eine Ordinalzahl abbilden, und die kleinste derartige Ordinalzahl ist dann die Kardinalzahl der Menge. Somit sind zwei Mengen stets vergleichbar, da die Ordinalzahlen es sind.■

6. Kardinalzahlarithmetik in ZFC

Mit der vorigen Folgerung aus ZFC, dass jede Kardinalzahl als spezielle Ordinalzahl zu verstehen ist, hat man zunächst folgende Definition:

Definition 39 (die Aleph-Kardinalzahlen, unabhängig von AC). *Die unendlichen Aleph-Kardinalzahlen definiert durch*

$$\begin{aligned} \aleph_0 &: = \omega = \text{ Menge der natürlichen Zahlen,} \\ \aleph_{\alpha+1} &: = \text{ kleinste Ordinalzahl } > \aleph_\alpha, \text{ die nicht gleichmächtig zu einer kleineren Ordinalzahl ist,} \\ \aleph_\lambda &: = \text{ kleinste Ordinalzahl } > \aleph_\alpha \text{ für alle } \alpha \in \lambda \text{ (Limeskardinalzahlen), die nicht gleichmächtig} \\ &\quad \text{zu einer kleineren Ordinalzahl ist.} \end{aligned}$$

Bemerkung: Man findet auch die Notation $\omega_\alpha := \aleph_\alpha$.

Satz 20. *In ZFC gilt: Jede Kardinalzahl ist eine Alephzahl.*

Zum Beweis ist nur daran zu erinnern, dass die Kardinalzahl einer unendlichen Menge x in ZFC zu definiert ist als kleinste zu x gleichmächtige Ordinalzahl. Jede solche ist ein Aleph.

Bemerkung: Allein in ZF noch gilt, dass es zu jeder Kardinalzahl p (mit der folgenden von AC unabhängigen Definition) noch eine kleinste Alephzahl $\not\leq p$ gibt, die man 'Hartogzahl von p' nennt und mit $\aleph(p)$ bezeichnet.

Definition 40 (Kardinalzahloperationen, unabhängig vom Auswahlaxiom).

$$\begin{aligned} p+q &: = |A \cup B|, \ |A| = p, |B| = q, A \cap B = \emptyset. \\ p \cdot q &: = |A \times B|, |A| = p, |B| = q. \\ 2^p &: = |\mathcal{P}(A)|, \ |A| = p, \\ p^q &: = |\{f | f : A \to B\}|, \ \textit{mit } |A| = q, |B| = p. \end{aligned}$$

Dabei ist die vom Auswahlaxiom unabhängige Definition der Kardinalzahl einer Menge vorauszusetzen, mit

$$|A| := \{B | \exists f : A \to B \text{ bijektiv und } B \text{ von kleinstem Rang}\} \text{ (das ist eine Menge!)}$$

Ferner definiert man unabhängig von AC

$$p \leq q :\iff \exists f : A \to B \text{ injektiv mit } p = |A| \text{ und } q = |B|.$$

Die Halbordnungseigenschaft für $\leq$ hat man mit folgendem Satz, den man ohne AC beweisen muss:

Satz 21. $p \leq q \wedge q \leq p \implies p = q$. *Oder: Wenn es eine Injektion einer Menge A in eine Menge B gibt und eine Injektion von B in A, dann gibt es eine Bijektion $A \to B$.*

SATZ 22 (elementare Rechenregeln für Kardinalzahlen ohne Benutzung von AC). *Man hat für Kardinalzahlen p, q, r :*

$$\begin{aligned}
p+q &= q+p,\ p\cdot q = q\cdot p,\\
p+(q+r) &= (p+q)+r,\\
p\cdot(q\cdot r) &= (p\cdot q)\cdot r,\\
(p+q)\cdot r &= p\cdot r + q\cdot r,\\
p &\leq p+q,\\
p &\leq p\cdot q,\ \textit{wenn } q\neq 0\\
p+q &\leq p\cdot q,\ \textit{wenn } p,q \textit{ unendlich,}\\
p &< 2^p\\
(p^q)^r &= p^{q\cdot r},\\
p^2 &= p\cdot p\\
(p+q)^2 &= p^2+2p\cdot q+q^2.\\
p &\leq q\wedge q
\end{aligned}$$

Der Beweis geht über elementare Konstruktionen von Abbildungen (Übung).

SATZ 8 (Rechenregeln für Kardinalzahlen mit AC). *Die einfache Kardinalzahlarithmetik mit AC sieht so aus: Für unendliche Kardinalzahlen p, q gilt:*

$$\begin{aligned}
&(i)\ p = p+p = p\cdot p,\\
&(ii)\ p\leq q\ \vee\ q\leq p,\\
&(iii)\ p+q = \max(p,q).
\end{aligned}$$

Beweis: (ii) hatten wir schon, aber es wurde noch einmal erwähnt als besonders wichtig (ungültig ohne AC (!)) und weil (ii) nötig ist, um $\max(p,q)$ zu bilden.

Zu (iii) : Wir folgern das aus (i) einfach so: Sei $p\leq q$, dann hat man $p+q\leq q+q=q=\max(p,q)$.

Zu (i) : Hier ist eine gewisse Arbeit nötig. Zunächst etablieren wir $p=p+p$, woraus sofort auch $p=p+p+p$ usw. folgt. Dazu denken wir uns (mit AC haben wir das) $p=\alpha$, α Ordinalzahl, und disjunkte Mengen A, B, beide mit α aufgezählt. Also

$$A=\{a_\beta|\,\beta\in\alpha\},\ B=\{a_\beta|\,\beta\in\alpha\},\ \text{natürlich } a_\beta\neq a_\gamma \text{ und } b_\beta\neq b_\gamma \text{ für } \beta\neq\gamma.$$

Dann hat man folgende Bijektion $h:\alpha\to A\cup B$:

$$\begin{aligned}
h(2n) &= a_n \text{ für alle } n\in\omega,\\
h(2n+1) &= b_n \text{ für alle } n\in\omega,\\
h(\lambda+2n) &= a_{\lambda+n},\\
h(\lambda+2n+1) &= b_{\lambda+n},\\
\text{für } n &\in \omega \text{ und Limeszahl } \lambda\in\alpha.
\end{aligned}$$

Nun zeigen wir die Aussage $p=p\cdot p$ mit dem Zornschen Lemma: Sei $|A|=p$. Dann betrachten wir die Abbildungen $B\to B\times B$ bijektiv mit $B\subset A$. Für $|B|=\aleph_0$ haben wir eine solche Bijektion (Cantor-Diagonalverfahren). Damit ist die Menge dieser Abbildungen nicht leer. Ferner ist sie induktiv geordnet (man kann Ketten vereinigen!), mit $f\leq g :\Longleftrightarrow dom(f)\subset dom(g)\wedge g\restriction dom(f)=f$. Mit dem Zornschen Lemma haben wir eine maximale Abbildung bzgl. $\leq$. Die sei $f:B\to B\times B$. B ist jedenfalls unendlich. Wir behaupten $|B|=|A|$. (Das genügt für den Beweis, warum?) Wäre $|B|<|A|$, so hätten wir eine Menge $X\subset A\setminus B$ mit $|X|=|B|$ und dann können wir definieren:

$$h:X\to X\times X \text{ bijektiv (induziert von } f \text{ und einer Bijektion von } B \text{ auf } X),$$

damit haben wir:

$$g:B\cup X\to (B\cup X)\times(B\cup X)=(B\times B)\cup(B\times X)\cup(X\times B)\ \text{bijektiv.}$$

(Man beachte, dass alle Vereinigungen hier disjunkte sind.) Denn

$$\begin{aligned} p &= p+p = |B \cup X|\,, \text{ und} \\ p &= p+p+p = |(B\times B)\cup(B\times X)\cup(X\times B)|\,. \end{aligned}$$

Die Bijektion g widerspricht aber der Maximaleigenschaft von f.■

7. Kardinalzahlarithmetik in ZF ohne AC und Beziehung zwischen GCH und AC

Im vorigen Abschnitt wurde gezeigt, wie sehr sich die Kardinalzahlarithmetik mit dem Auswahlaxiom vereinfacht. Hier soll bewiesen werden, dass AC dafür auch notwendig ist. Wir fassen das Hauptergebnis in folgenden

Satz 23.

$$\begin{aligned} &(i)\ \textit{Für alle unendlichen Kardinalzahlen } p,q\ :\ (p\le q \vee q\le p) \implies AC \\ &(ii)\ \textit{Für alle unendlichen Kardinalzahlen } p\ :\ (p=p\cdot p) \implies AC \end{aligned}$$

Bemerkungen: Wir haben zwar $p+p=p$ für unendliche Kardinalzahlen nur mit AC beweisen können, aber diese Aussage ist tatsächlich *schwächer* als AC, d.h. mit der Verneinung von AC verträglich.

Es sollte auch klar sein, dass man hat: Jede Kardinalzahl p ist eine Alephzahl $\implies AC$.

Beweis: (i) ist klar (Übung).

Zu (ii) : Wir benutzen das Auswahlaxiom in Gestalt der Aussage: Jede unendliche Kardinalzahl ist eine Alephzahl. Dafür ist nun hinreichend:

$$(*)\ \ p+\aleph(p)=p\cdot\aleph(p) \text{ für alle unendlichen Kardinalzahlen } p.$$

Dabei ist $\aleph(p)$ die Hartogzahl von p. Das folgt so: Mit $(*)$ hat man Mengen P,A und disjunkte Mengen P_1,A_1 mit $\aleph(p)=|A|=|A_1|$ und $|P|=|P_1|=p$, so dass $P\times A=P_1\cup A_1$. Nun gibt es $p_0\in P$ mit $(p_0,a)\in P_1$ für alle $a\in A$ - dann wäre $\aleph(p)\le p$, was falsch ist. Also muss die Verneinung gelten, d.h. für alle $p\in P$ gibt es $a\in A$, so dass $(p,a)\in A_1$. Nun ist A_1 wohlzuordnen (die Hartogzahl $\aleph(p)$ ist eine Alephzahl!), und es gibt daher eine Auswahlfunktion f, so dass

$$(p,f(p))\in A_1 \text{ für alle } p\in P.$$

Wir bilden damit die Injektion von P in A_1 :

$$p\longmapsto (p,f(p))\,.$$

Das ergibt $p\le\aleph(p)$. Damit ist p selbst eine Alephzahl, da P in die Ordinalzahl $\aleph(p)$ eingebettet werden kann.

Nun folgern wir aus $p=p\cdot p$ (für alle unendlichen Kardinalzahlen p) die Aussage $(*)$:

$$p+\aleph(p)=(p+\aleph(p))^2=p^2+2p\cdot\aleph(p)+(\aleph(p))^2\ge p\cdot\aleph(p)\,.$$

Da nun ohnehin $p+\aleph(p)\le p\cdot\aleph(p)$, hat man nunmehr $(*)$ und damit AC. Hinweis: Man benötigt dazu, dass für Kardinalzahlen p,q aus $p\le q\wedge q\le p$ *ohne* AC folgt: $p=q$ (siehe dazu entsprechende Übungsaufgabe).■

Die großen Resultate der Mengenlehre sind die Unabhängigkeit des Auswahlaxioms von ZF und der Kontinuumshypothese von ZFC. Aber es gibt zwischen der verallgemeinerten Kontinuumshypothese GCH und dem Auswahlaxiom doch eine überraschende Beziehung.

Definition 41. *Die spezielle Kontinuumshypothese CH besagt: Es gibt keine Kardinalzahl echt zwischen $\aleph_0=|\mathbb{N}|$ und $2^{\aleph_0}=|\mathbb{R}|$. Die verallgemeinerte Kontinuumshypothese GCH (für: 'generalised continuum hypothesis') besagt: Für alle unendlichen Kardinalzahlen p gibt es keine Kardinalzahl echt zwischen p und 2^p.*

Bemerkung: In ZFC hat man natürlich, dass GCH gleichwertig ist zu $\aleph_{\alpha+1}=2^{\aleph_\alpha}$, für alle $\alpha\in On$. Aber bewusst wurde GCH tauglich für ZF ohne AC formuliert.

Auswahlaxiom AC und GCH scheinen auf den ersten Blick nichts miteinander zu tun zu haben, außer der erwähnten speziellen Formulierung von GCH, die mit AC möglich wird. Aber es verhält sich nicht so:

Satz 24. *Aus ZF folgt: $GCH \Longrightarrow AC$. Die verallgemeinerte Kontinuumshypothese impliziert also das Auswahlaxiom.*

Bemerkung: $ZF + GCH$ ist also stärker als ZFC.

Beweis: Die Idee ist folgende: Man hat $p < 2^p$, aber ähnlich auch noch $2^p \not\leq p^2$ (das wird unten bewiesen). Nun hat man

$$p^2 \leq (2^p)^2 = 2^{2p} = 2^p,$$

weil zunächst aus GCH folgt, dass $2p = p$. Denn

$$p \leq 2p \leq 2^p,$$

also mit GCH: $2p = p$ oder $2p = 2^p$. Letzteres scheidet aus, da man mit $2p \leq p^2$ sofort hätte: $2^p \leq p^2$. Nun haben wir

$$p \leq p^2 \leq 2^p,$$

und mit GCH kann p^2 nicht echt zwischen p und 2^p liegen, also $p = p^2$, da $p^2 = 2^p$ ausgeschlossen ist. Nun haben wir mit GCH gefolgert, dass $p^2 = p$, und daraus folgt AC nach dem vorigen Satz.

Es fehlt nur noch die Aussage $2^p \not\leq p^2$ für alle unendlichen Kardinalzahlen p. Dazu nehmen wir an, es gäbe eine Injektion f von 2^A in $A \times A$, mit einer Menge A der (unendlichen) Kardinalzahl p. Wir werden damit eine Injektion g von $\aleph(p)$ in A bilden, die nach Definition von $\aleph(p)$ nicht existieren kann.

Erster Schritt: Man beschafft sich eine Menge $\{a_n | n \in \omega\} \subset A$ mit $a_n \neq a_m$ für $n \neq m$. (Mit AC ist das banal, aber für unser Vorhaben ist es entscheidend, AC nicht zu verwenden, stattdessen zeigt sich, dass man die vorausgesetzte Abbildung f dafür gebrauchen kann.) Zunächst seien $a_0, ..., a_4$ paarweise verschiedene Elemente von A. Für $n \geq 5$, $n \in \omega$, konstruieren wir nunmehr zu vorausgesetzten paarweise verschiedenen $a_0, ..., a_{n-1}$ ein neues Element a_n. Sei

$$C_n := \{a_0, ..., a_{n-1}\}.$$

Da $|C_n \times C_n| = n^2 < 2^n$ für $n \geq 5$, gibt es $U \subset C_n$ mit $f(U) \notin C_n \times C_n$. Wichtig ist, dass eine solche Menge U wegen der ohnehin (ohne AC) existierenden Wohlordnung aller endlichen Teilmengen von C_n konkret definiert werden kann. Also $U :=$ erste endliche Teilmenge von C_n, so dass $f(U) \notin C_n \times C_n$. Nun sei $f(U) = (x, y)$. Dann hat man $x \notin C_n$ oder sonst $y \notin C_n$. Im ersten Fall setzt man $a_n := x$, im zweiten Fall $a_n := y$. Wir haben damit

$$C_\omega = \{a_n | n \in \omega\}.$$

Zweiter Schritt: Für eine unendliche Ordinalzahl $\alpha < \aleph(p)$ sei bereits

$$C_\alpha = \{a_\beta | \beta \in \alpha\} \text{ mit } a_\beta \neq a_\gamma \text{ für } \beta \neq \gamma,\ \beta, \gamma \in \alpha, \text{ konstruiert.}$$

Dann findet man auf folgende Weise eine Fortsetzung der Folge in A mit $a_\alpha \neq a_\beta$ für alle $\beta \in \alpha$:

Wir behaupten, dass es zur vorausgesetzten Abbildung

$$f : 2^{C_\alpha} \to A \times A \text{ (Einschränkung von } f \text{ auf } 2^{C_\alpha})$$

eine (ohne AC definierbare) Menge $U \subset C_\alpha \subset A$ gibt mit

$$f(U) \notin C_\alpha \times C_\alpha.$$

Dann können wir mit $f(U) = (x, y)$ wieder setzen: $a_\alpha := x$, wenn $x \notin C_\alpha$, sonst $a_\alpha := y$. Jedenfalls hat a_α dann die geforderte Eigenschaft.

Wir kommen zur Definition von U, die wir uns unter Verwendung von GCH leicht machen können: Die Menge 2^{C_α} ist mit GCH von der Kardinalzahl $\aleph_{\gamma+1}$, wenn $|C_\alpha| = \aleph_\gamma$.Damit hat 2^{C_α} eine Wohlordnung, und wor wählen wie im endlichen Fall

$$U := \text{ kleinstes Element von } 2^{C_\alpha} \text{ mit } f(U) \notin C_\alpha \times C_\alpha.$$

Das klappt, weil die Menge

$$\left\{U \in 2^{C_\alpha} \middle| f(U) \notin C_\alpha \times C_\alpha\right\} \neq \emptyset,$$

was aus Kardinalzahlgründen stimmt, es ist $\left|2^{C_\alpha}\right| > |C_\alpha| = |C_\alpha \times C_\alpha|$. Man beachte, dass für wohlgeordnete Mengen wie C_α die Aussage $|C_\alpha| = |C_\alpha \times C_\alpha|$ stets gilt.

Abschließend setzen wir noch mit $f(U) = (x, y)$:

$$\begin{aligned} a_\alpha &: = x, \text{ wenn } x \notin C_\alpha, \\ a_\alpha &: = y, \text{ wenn } x \in C_\alpha, \text{ also dann } y \notin C_\alpha. \blacksquare \end{aligned}$$

KAPITEL 4

Modelle der Mengenlehre und Unabhängigkeitsfragen

1. Ein paar Vorbemerkungen zur Metamathematik der Mengenlehre

Die Konsistenz der Mengenlehre kann man ihr nicht beweisen, aus demselben Grund, weshalb das bereits mit der Peanoarithmetik schiefging. Denn die Mengenlehre ist ein System, das die Peanoarithmetik enthält, und der zweite Gödelsche Unollständigkeitssatz gilt für alle solchen Systeme.

Was ist noch möglich? Man verlässt sich auf die Erfahrung, dass ZF auch bei der vorangehenden überaus starken Strapazierung standgehalten hat, also auf reichhaltige empirische Evidenz der Widerspruchsfreiheit.

Wir setzen also die Widerspruchsfreiheit von ZF voraus. Dann gibt es ein Modell von ZF. Man kann ein solches natürlich nicht konstruieren, weil das wieder zu einem Widerspruchsfreiheitsbeweis führen würde. Aber was man tun kann und getan hat, ist Folgendes: Wenn man bereits ein Modell von ZF hat, so kann man darin 'innere Modelle' konstruieren und mit diesen zeigen: Wenn ZF konsistent ist, dann ist auch $ZFC + GCH$ konsistent (Gödel 1940). Gödel zeigte das mit einer Art 'Minimalmodell', das ist das Universum der 'konstruktiblen' Mengen. Ausgehend von $\emptyset$ bildet man gerade so viel, wie für die Erfüllung der $ZF-$ Axiome nötig ist. Man schließt unter den 'Gödel-Operationen' ab. Es hat sich gezeigt, ohne dass dies intuitiv naheläge, dass das so entstehende Universum der konstruktiblen Mengen auch AC und GCH erfüllt. 'Nicht naheliegend', weil das Auswahlaxiom z.B einerseits davon redet, dass es keine Mengen gibt, die nicht wohlgeordnet werden können, andererseits fordert es aber die Existenz von vielen Auswahlmengen, Abbildungen für $p = p^2$ usw. Dieser Gödelsche Zugang wird im nächsten Abschnitt skizziert, er ist bereits ziemlich mühsam.

Für die Unabhängigkeit vollends des AC von ZF und sogar der GCH von ZFC haben dann insbesondere Fraenkel und Mostowski 'Permutationsmodelle' entwickelt. Diese Methode wird ein wenig verständlich gemacht im zweiten Abschnitt dieses Kapitels. Allerdings funktionierte diese Methode nur für eine Mengenlehre, welche 'Urelemente' besitzt, d.h. eine unendliche Menge, deren Elemente keine Mengen sind. Das entspricht zwar eigentlich dem intuitiven mathematischen Denken, aber andererseits ist es eine Errungenschaft, keine Objekte nötig zu haben, die keine Mengen sind. Hinzu kommt, dass es keineswegs gelang, von den Resultaten zu 'ZF mit Urelementen' auf die entsprechenden für ZF selbst zu schließen. Genauere neuere Untersuchungen haben auch gezeigt, dass dies im Allgemeinen auch gar nicht gehen kann, d.h. dass beide Theorien doch wesentlich verschieden sind. So musste Cohen für die Unabhängigkeit des AC von ZF und der GCH (und sogar der CH) von ZFC eigens eine sehr raffinierte Methode für die Modelltheorie der Modelle der Mengenlehre finden (1963), die tatsächlich auf eine kontrollierbare Erweiterung eines $ZF-Modells$ hinausläuft. In solchen Modellen konnte Cohen dann $ZF \cup \{\neg\, AC\}$ sowie $ZFC \cup \{\neg\, CH\}$ realisieren, was mit dem Gödelschen Resultat zusammen die volle Unabhängigkeit bedeutet. Diese Methode heißt nach ihren zwei Aspekten 'Booleschwertige Modelle der Mengenlehre' bzw. 'forcing'. Diese Methode wird im letzten Abschnitt beschrieben. Man hat sie dann in der Folgezeit bis heute stark verallgemeinert und für speziellere technisch äußerst schwierige Probleme angepasst, mit dem Ergebnis, dass man sehr genaue Strukturkenntnisse über die Modelle der Mengenlehre hat und eine riesige Fülle von Unabhängigkeitsresultaten. Dieses extrem feine 'Uhrmacherhandwerk' beherscht die heute aktuelle Forschung in der Mengenlehre. Auch in die Modelltheorie im Kontext mit Algebra ist die Forcing-Methode eingegangen.

2. Gödels konstruktibles Universum und die Konsistenz von $ZFC + GCH$ relativ zur Konsistenz von ZF

Wie bereits erwähnt, besteht Gödels Idee zur Frage nach dem Status von AC und GCH darin, im Rahmen eines gegebenen Modells der Mengenlehre, sagen wir in einem Mengenuniversum V, ein besonders

schlankes Modell der 'konstruktiblen Mengen' $L \subset V$ zu definieren und zu beweisen, dass L selbst ein Modell von ZF ist und mehr noch sogar eines von AC und GCH.

Wenn man Substrukturen von $\langle V, \in \rangle$ betrachtet, so kann man beliebige Teilklassen von V nehmen und die $\in -$ Relation darauf einschränken. Aber man wird dann nicht erwarten, dass ein Modell von ZF herauskommt. Nun ist in den $ZF-$ Axiomen viel davon die Rede, dass zu vorgegebenen Mengen weitere existieren, wie z.B. die Vereinigung, das Bild unter einer Funktion, usw. Daher liegt es nahe, solche Teilklassen zu betrachten, die unter gewissen Mengenfunktionen abgeschlossen sind, z. B. sicher unter $\mathcal{F}_1(x, y) = \{x, y\}$. Denkt man allerdings an das Komprehensionsaxiom, so muss man nachschauen, was für Mengenoperationen man noch braucht, um einen Induktionsbeweis über den Formelausbau zu schaffen. Daher erklären sich die unmotivierter erscheinenden Gödel-Operationen wie vor allem $\mathcal{F}_6 - \mathcal{F}_8$, auf die man erst bei einem solchen Beweisversuch stößt. Eine andere Richtung hat das Extensionalitätsaxiom: Wenn nur die Elemente aus der Teilklasse $\mathcal{M} \subset V$ von x, y dieselben sind, dann müsste nicht $x = y$ gelten. Dasselbe Problem tritt beim Fundierungsaxiom auf. Beide Probleme und auch mehr lösen sich auf, wenn man von vornherein nur transitive Klassen $\mathcal{M}$ betrachtet. Wieder andere $ZF-$ Axiome verlangen die Existenz ziemlich großer Mengen, z.B. $\cup x$ oder $\mathcal{P}(x)$ oder auch Extistenz einer unendlichen Menge. Auch mit $x \in \mathcal{M}$ müssten sie nicht in $\mathcal{M}$ liegen. Man beachte noch einmal, dass die entsprechenden Axiome nur so formuliert wurden, dass eine $\cup x$ enthaltende Menge existiert, analog in anderen Fällen. (Der Rest wird vom Komprehensionsaxiom erledigt.) Nun kann man aber solch große Mengen nicht mit Gödeloperationen einfangen. Aber man kann von vornherein von einem Kandidaten $\mathcal{M}$ für ein Modell von ZF verlangen, dass die Klasse $\mathcal{M}$ die Eigenschaft hat, 'fast universell' zu sein, die so definiert ist:

DEFINITION 42. *$\mathcal{M} \subset V$ heißt fast universell, wenn für jede **Menge** $S \in V$ folgende Aussage in V gilt:*

$$S \subset \mathcal{M} \to (\exists Y \in \mathcal{M})\, S \subset Y.$$

Bemerkung: Wir interessieren uns nur für transitive fast universelle Klassen.

Nunmehr nimmt die Idee von Gödel folgende Gestalt an: Bilde eine transitive Klasse, die fast universell ist und unter geeigneten Mengenoperationen (den Gödeloperationen) abgeschlossen ist. Das ist dann ein Modell von ZF. Um das Auswahlaxiom und GCH zusätzlich zu erfüllen, konstruiere das Modell möglichst schlank, dass es gerade die Ordinalzahlen umfasst. 'Möglichst schlank' heißt, dass nicht wie in der Hierarchie V_a immer die Potenzmenge genommen wird, sondern nur das aus ihr, das für den Abschluss unter den Gödeloperationen notwendig ist.

Wir führen nunmehr die Gödeloperationen auf, bemerken erneut, das manche sich ein wenig technisch verstehen:

DEFINITION 43. *Die Gödeloperationen sind folgende:*

$$\begin{aligned}
\mathcal{F}_1(x, y) &= \{x, y\}, \\
\mathcal{F}_2(x, y) &= x \setminus y, \\
\mathcal{F}_3(x, y) &= x \times y, \\
\mathcal{F}_4(x) &= dom(x) \\
\mathcal{F}_5(x) &= \in \cap\, x^2 \\
\mathcal{F}_6(x) &= \{(a, b, c) |\, (b, c, a) \in x\} \\
\mathcal{F}_7(x) &= \{(a, b, c) |\, (c, b, a) \in x\} \\
\mathcal{F}_6(x) &= \{(a, b, c) |\, (a, c, b) \in x\}.
\end{aligned}$$

Bemerkung: Man mache sich klar, dass für Mengen x, y stets Mengen herauskommen.

Wir haben nun alle Zutaten zusammen, die wir zur Formulierung der Gödelschen Konstruktion eines Modells von $ZFC + GCH$ (ein Modell von ZF gegeben) und zur Formulierung der Hauptresultate benötigen:

DEFINITION 44 (Gödels konstruktible Hierarchie und L). *Definiert wird (mit transfiniter Induktion):*

$$\begin{aligned} L_0 &= \emptyset, \\ L_{\alpha+1} &: = \mathcal{P}(L_\alpha) \cap cl(V_\alpha \cup \{L_\alpha\}), \\ L_\lambda &: = \bigcup_{\alpha<\lambda} L_\alpha, \\ L &: = \bigcup_{\alpha\in On} L_\alpha. \end{aligned}$$

Dabei bezeichnet $cl(X)$ den Abschluss einer Menge unter allen Gödeloperationen, zu definieren durch:

$$\begin{aligned} X_0 &= X, \\ X_{n+1} &: = X_n \cup \{\mathcal{F}_i(x,y) | \, 1 \le i \le 3,\ x,y \in X_n\} \cup \{\mathcal{F}_i(x) | \, 4 \le i \le 8,\ x \in X_n\}, \text{ für } n \in \omega. \end{aligned}$$

Bemerkung: Damit wird L als Teilklasse von V im Rahmen von V definiert. Wir setzen $\langle V, \in\rangle \models ZF$ voraus. (Hinweis zur Notation: Wir werden knapper nur $V \models ZF$ usw. schreiben, da es klar ist, dass nur die $\in -$ Relation als einzige nichtlogische vorhanden ist. Dazu sei noch bemerkt, dass V **von innen** natürlich keine Menge ist, aber ein Modell von ZF mit einer Trägermenge gebildet werden kann, so dass V **von außen** eine Menge ist.)

Das ganze Programm dieses Abschnittes wird mit Satz umfassend realisiert:

SATZ 9.

(*i*) *L ist eine transitive und fast universelle Klasse, unter den Gödeloperationen abgeschlossen.*

(*ii*) *Eine transitive Klasse $\mathcal{M} \subset V \models ZF$, die fast universell ist und unter den Gödeloperationen abgeschlossen, bildet selbst ein Modell von ZF.*

(*iii*) *Folgerung : L ist ein transitives Modell von ZF.*

(*iv*) *L erfüllt zusätzlich AC und GCH.*

(*v*) *L ist das kleinste transitive $ZF-$Modell, das alle Ordinalzahlen enthält.*

Wir kommen zu den Beweisen.

Beweis von (*i*):

(*i*) ist ziemlich plausibel nach Konstruktion von L.

L ist fast universell: Sei $x \in V$ und $x \subset L$. Dann ist $x \in V_\alpha$ für eine Ordinalzahl α. Also

$$\begin{aligned} &\forall z (z \in x \implies z \in V_\alpha), \text{ somit} \\ &\forall z (z \in x \implies z \in L_\alpha). \end{aligned}$$

Daher $x \subset L_\alpha$, und so ist $L_\alpha \in L$ selbst eine Menge $\supset x$, wie gefordert ist.

L ist transitiv. Wir zeigen stärker, dass bereits alle L_α transitiv sind. Sonst sei α die kleinste Ordinalzahl, dass L_α nicht transitiv ist. Jedenfalls $\alpha > 0$, da L_0 offenbar transitiv ist. Nun hat man einerseits: Wenn alle L_α transitiv sind für $\alpha < \lambda$, λ Limesordinalzahl, dann L_λ transitiv. Andererseits: Wenn L_α transitiv ist, dann ist $L_\alpha \subset L_{\alpha+1}$ (denn: $x \in L_\alpha$, dann $x \subset L_\alpha$ mit Transitivität, damit $x \in \mathcal{P}(L_\alpha)$ und auch $x \in cl(L_\alpha)$, da $L_\alpha \subset cl(L_\alpha)$), und wenn $L_\alpha \subset L_{\alpha+1}$, dann ist $L_{\alpha+1}$ transitiv (denn: $y \in x \in L_{\alpha+1}$, dann $y \in L_\alpha$, also mit $L_\alpha \subset L_{\alpha+1}$ auch $y \in L_{\alpha+1}$). Daraus folgt: Mit L_α transitiv ist auch $L_{\alpha+1}$ transitiv. Damit sind alle L_α transitiv mit Rekursion.

L ist unter den Gödeloperationen abgeschlossen: Mit $x, y \in L_\alpha$ hat man $\mathcal{F}(x,y)$ oder $\mathcal{G}(x)$ (für beliebige Gödeloperationen $\mathcal{F}$, $\mathcal{G}$ entsprechender Stellenzahl), dass $\mathcal{F}(x,y), \mathcal{G}(x) \in cl(L_\alpha)$. Weiter gilt $\mathcal{F}(x,y), \mathcal{G}(x) \in \mathcal{P}(L_{\alpha+1})$, also jedenfalls $\mathcal{F}(x,y), \mathcal{G}(x) \in L_{\alpha+2}$.■

Der zweite Satz ist die Hauptsache, und wir beweisen ihn ausführlich, da er die Zusammenhänge in der Axiomatik der Mengenlehre sehr gut illustriert und außerdem exemplarisch die typischen Verfahren der Modelltheorie vorführt, vor allem die Induktion über den Formelaufbau bei der Verifikation des Komprehensionsaxioms.

Beweis von (*ii*):

Wir beginnen mit dem Schwierigsten, der Erfüllung des Komprehensionsaxioms. Dazu haben wir zu zeigen: Wennn $\varphi(\vec{\mathbf{u}}) = \varphi(u_1, ..., u_n)$ eine Formel der Sprache zur Mengenlehre ist und $x \in \mathcal{M}$, dann

$$\{\vec{\mathbf{u}} \in x^n | \, \mathcal{M} \models \varphi(\vec{\mathbf{u}})\} \in \mathcal{M}.$$

Technisch wird das so realisiert, und das nehmen wir als die Aussage, die wir induktiv über den Formelaufbau von φ beweisen: Es gibt eine Komposition $\mathcal{F}$ von Gödeloperationen, und es gibt ein k und Mengen $X_1, ..., X_k$, so dass

$$\left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \varphi\left(\overrightarrow{\mathbf{u}}\right) \right\} = \mathcal{F}\left(x, X_1, ..., X_k\right),$$

für beliebige Menge $x \in \mathcal{M}$.

Bemerkung: Genau genommen könnte φ noch Parameter in $\mathcal{M}$ enthalten. Diese aufzuführen, würde jedoch lediglich die Lese- und Schreibarbeit belasten, das sind Mengen in $\mathcal{M}$, die einfach 'mitgeschleppt würden. Ferner können wir auf atomare Formeln '$x \doteq y$' verzichten, da mit Extensionalität die Gleichheit durch die $\in -$ Relation ausgedückt werden kann.

1. Induktionsanfang: Sei φ atomar. Dann sei $\varphi = u_i \in u_j$ mit $i \neq j$.

1. Fall: Sei $i = n-1, j = n$. Dann

$$\begin{aligned} \left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \varphi\left(\overrightarrow{\mathbf{u}}\right) \right\} &= \left\{ (v, u_{n-1}, u_n) \middle| \, v \in x^{n-2} \wedge (u_{n-1}, u_n) \in \mathcal{F}_5(x) \right\} \\ &= \mathcal{F}_6\left(\mathcal{F}_5(x) \times x^{n-2}\right). \end{aligned}$$

2. Fall: Sei $i = n, j = n-1$. Dann

$$\begin{aligned} \left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \varphi\left(\overrightarrow{\mathbf{u}}\right) \right\} &= \left\{ (v, u_{n-1}, u_n) \middle| \, v \in x^{n-2} \wedge (u_n, u_{n-1}) \in \mathcal{F}_5(x) \right\} \\ &= \mathcal{F}_7\left(\mathcal{F}_5(x) \times x^{n-2}\right). \end{aligned}$$

3. Fall: $i, j \neq n$. Dann mit Induktionsvoraussetzung für n:

$$\begin{aligned} \left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \varphi\left(\overrightarrow{\mathbf{u}}\right) \right\} &= \left\{ \left((u_1, ..., u_{n-1}), u_n\right) \middle| \, (u_1, ..., u_{n-1}) \in \mathcal{G}(x) \wedge u_n \in x \right\} \\ &= \mathcal{G}(x) \times x. \end{aligned}$$

4. Fall: $i, j \neq n-1$. Dann mit Induktionsvoraussetzung

$$\begin{aligned} \left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \varphi\left(\overrightarrow{\mathbf{u}}\right) \right\} &= \left\{ \left((u_1, ..., u_{n-2}), u_n, u_{n-1}\right) \middle| \, (u_1, ..., u_{n-2}, u_n) \in \mathcal{G}(x) \wedge u_{n-1} \in x \right\} \\ &= \mathcal{F}_8\left(\mathcal{G}(x) \times x\right). \end{aligned}$$

Fortsetzung des Formelaufbaus von φ :

2. Sei $\varphi = \neg\psi$. Sei

$$\left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \psi\left(\overrightarrow{\mathbf{u}}\right) \right\} = \mathcal{G}\left(x, X_1, ..., X_k\right).$$

Dann

$$\left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \varphi\left(\overrightarrow{\mathbf{u}}\right) \right\} = x^n \setminus \mathcal{G}\left(x, X_1, ..., X_k\right) = \mathcal{F}_2\left(x^n, \mathcal{G}\left(x, X_1, ..., X_k\right)\right).$$

3. Sei $\varphi = \alpha \wedge \beta$. Dann seien

$$\begin{aligned} \left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \alpha\left(\overrightarrow{\mathbf{u}}\right) \right\} &= \mathcal{G}\left(x, X_1, ..., X_k\right) =: Y_1, \\ \left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \beta\left(\overrightarrow{\mathbf{u}}\right) \right\} &= \mathcal{H}\left(x, X_1, ..., X_k\right) =: Y_2. \end{aligned}$$

So ergibt sich

$$\left\{ \overrightarrow{\mathbf{u}} \in x^n \middle| \, \mathcal{M} \models \varphi\left(\overrightarrow{\mathbf{u}}\right) \right\} = \mathcal{F}_2\left(Y_1, \mathcal{F}_2\left(Y_1, Y_2\right)\right).$$

4. Sei $\varphi = \exists v \psi\left(u_1, ..., u_n, v\right)$. Wir zeigen zunächst, dass wir mit folgendem Lemma durchkommen:

$(*)$ Für alle Formeln $\psi\left(\overrightarrow{\mathbf{u}}, v\right)$ und alle Mengen s_0 gibt es $s \supset s_0$:
$\left(\forall \overrightarrow{\mathbf{u}} \in s\right)\left(\exists v \psi\left(\overrightarrow{\mathbf{u}}, v\right) \implies (\exists v \in s)\, \psi\left(\overrightarrow{\mathbf{u}}, v\right)\right)$.

Nun sei $x \in \mathcal{M}$. Mit dem Lemma gibt es $x \subset s \subset \mathcal{M}$, so dass für alle $\overrightarrow{\mathbf{u}} \in x$

$$(\exists v \in \mathcal{M})\, \mathcal{M} \models \psi\left(\overrightarrow{\mathbf{u}}, v\right) \iff (\exists v \in s)\, \mathcal{M} \models \psi\left(\overrightarrow{\mathbf{u}}, v\right).$$

Mit $\mathcal{M}$ fast universell existiert $x_{k+1} \in \mathcal{M}$, $x_{k+1} \supset s$, so dass für alle $\overrightarrow{\mathbf{u}} \in x$:

$$(i) \quad (\exists v \in \mathcal{M})\, \mathcal{M} \models \psi\left(\overrightarrow{\mathbf{u}}, v\right) \iff (\exists v \in x_{k+1})\, \mathcal{M} \models \psi\left(\overrightarrow{\mathbf{u}}, v\right).$$

Nun haben wir mit Induktionsvoraussetzung: Es gibt Mengen $X_1, ..., X_k \subset x_{k+1}$ und eine Komposition $\mathcal{G}$ von Gödeloperationen, so dass

$$(ii) \quad \mathcal{M} \models \psi\left(\overrightarrow{\mathbf{u}}, v\right) \iff \left(\overrightarrow{\mathbf{u}}, v\right) \in \mathcal{G}\left(x_{k+1}, X_1, ..., X_k\right).$$

Nun gilt mit (i) und (ii) und für $\overrightarrow{\mathbf{u}} \in x^n$:

$$\begin{aligned} \mathcal{M} \quad &\models \quad \exists v \psi\left(\overrightarrow{\mathbf{u}}, v\right) \iff_{(i)} \left(\exists v \in x_{k+1}\right) \mathcal{M} \models \psi\left(\overrightarrow{\mathbf{u}}, v\right) \\ &\iff_{(ii)} \left(\exists v \in x_{k+1}\right)\left(\left(\overrightarrow{\mathbf{u}}, v\right) \in \mathcal{G}\left(x_{k+1}, X_1, ..., X_k\right)\right) \\ &\iff \overrightarrow{\mathbf{u}} \in x^n \cap dom\left(\mathcal{G}\left(x_{k+1}, X_1, ..., X_k\right)\right). \end{aligned}$$

Es bleibt noch das Lemma $(*)$ zu beweisen: Setze

$$C_{\overrightarrow{\mathbf{u}}} := \left\{ v \middle| \, \psi\left(\overrightarrow{\mathbf{u}}, v\right), \ v \text{ von minimalem Rang} \right\}.$$

Das ist eine Menge wegen der Rangbeschränkung. Nun sei s_0 vorgegeben. Setze

$$\begin{aligned} s_{n+1} \ &: = \mathcal{F}\left(s_n\right), \text{ mit } \mathcal{F}(x) := x \cup \bigcup \left\{ C_{\overrightarrow{\mathbf{u}}} \middle| \, \overrightarrow{\mathbf{u}} \in x \right\}, \\ s \ &: = \bigcup_{n \in \omega} s_n. \end{aligned}$$

Dann hat s offenbar die gewünschte Eigenschaft.■

Beweis von (iv) :

Zum Auswahlaxiom: Aus einer Wohlordnung für L_α konstruiert man eine Wohlordnung von $L_{\alpha+1}$, indem man setzt: Innerhalb von L_α bleibt die Wohlordnung von L_α bestehen, $L_\alpha > x$ für alle $x \in L_\alpha$, und für alle Tripel (i, x, y) mit $i = 1, .., 8$ und $x, y \in L_\alpha \cup \{L_\alpha\}$ wählt man lexikographische Wohlordnung. Dann setzt man für $u, v \in L_{\alpha+1}$: $u < v :\iff$ das kleinste Tripel (i, x, y), das mit $\mathcal{F}_i(x, y)$ bzw. $\mathcal{F}_j(x)$ das Element u darstellt, liegt vor dem kleinsten Tripel (j, a, b), das mit $\mathcal{F}_i(a, b)$ bzw. $\mathcal{F}_j(a)$ das Element v darstellt. Man stellt dann noch fest, dass diese Wohlordnung durch eine Formel ausdrückbar ist. Damit ist L ein Modell von ZFC.

Zu GCH: Vorbemerkung: Wir können nicht benutzen, dass GCH das Auswahlaxiom impliziert, da unsere Argumentation (nach Jech) dafür, dass L ein Modell von GCH ist, die Gültigkeit des Auswahlaxioms benötigt.

Es gehen folgende Sätze als Lemmata ein, die wegen ihres großen systematischen Gewichts als Sätze aufgeführt werden:

SATZ 10 (Mostowskis Satz vom transitiven Kollaps). *Jedes Modell $\langle S, \in \rangle$, welches das Extensionalitätsaxiom sowie das Fundierungsaxiom erfüllt, ist isomorph zu einem* ***transitiven*** *Modell $\langle M, \in \rangle$. Zusatz: Der Isomorphismus ist eindeutig und hat die Eigenschaft, dass transitive Mengen $x \in S$ auf sich selbst abgebildet werden.*

Bemerkung: Das Modell $\langle M, \in \rangle$ erfüllt dann selbstverständlich auch wieder Extensionalitäts- und Fundierungsaxiom. Wir setzen voraus, dass sich alles in einem $ZF-$ Modell $\langle V, \in \rangle$ abspielt. Dann genügt es schon, dass $\langle S, \in \rangle$ das Extensionalitätsaxiom erfüllt.

Beweis: Da $\langle S, \in \rangle$ fundiert ist, kann man $\in -$ Induktion durchführen und den gesuchten Isomorphismus so definieren:

$$\pi(x) := \{ \pi(y) | \, y \in x \cap S \}.$$

M ist nun einfach das Bild von π. Somit ist π offenbar eine Surjektion von S auf M. Außerdem gilt nach Konstruktion für $x, y \in S$ sofort, dass $x \in y \iff \pi(x) \in \pi(y)$. Mit Extensionalität ist π auch injektiv. M ist transitiv: Sei nämlich $b \in M$, dann $b = \pi(y)$ mit einem $y \in S$, somit $b = \{ \pi(x) | \, x \in y \} \subset M$.■

SATZ 11 (Reflektionssatz). *Sei φ eine feste Formel der Sprache der Mengenlehre. Für jede Menge S existiert eine Menge $T \supset S$, so dass für alle $\overrightarrow{\mathbf{x}} \in T$ gilt:*

$$V \models \varphi\left(\overrightarrow{\mathbf{x}}\right) \iff T \models \varphi\left(\overrightarrow{\mathbf{x}}\right).$$

(Gemeint sind natürlich $\langle V, \in \rangle$ und $\langle T, \in \rangle$.) Erfüllt V das Auswahlaxiom, so kann $|T| = |S|$ gewählt werden, wenn S bereits unendlich ist.

Beweis: Für atomare Formeln ist das trivial, ebenso sind die Induktionsschritte für $\wedge, \neg$ trivial (wegen der Äquivalenzformulierung), und für all das ist S bw. das Zwischenstadium T' nicht zu erhöhen. Allein $\exists y \varphi\left(\overrightarrow{\mathbf{x}}, y\right)$ macht Schwierigkeiten, aber das wurde oben bereits erledigt im Lemma $(+)$, welches für das Komprehensionsaxiom in L benutzt wurde. Inspektion der Begründung für $(+)$ zeigt den Zusatz für die Kardinalzahl von T.■

SATZ 12. *Es gibt eine Aussage ϑ derart, dass für jedes transitive Modell $\langle M, \in\rangle$ von ϑ gilt: Für alle $x \in M$:*

$$V \models (\exists \beta \in On)\, x \in L_\beta \iff M \models (\exists \alpha \in On)\, x \in L_\alpha.$$

Insbesondere ist natürlich auch '$x \in L_\alpha$' überhaupt formulierbar und damit das Axiom '$V = L$', welches besagt, dass alle Mengen des Universums konstruktibel sind, in der Form $\forall x \exists (\alpha \in On)(x \in L_\alpha)$.

Beweis: Vorbemerkung: '$\alpha \in On$' ist als Abkürzung zu verstehen für die Formel, welche besagt, dass α transitiv und durch $\in$ wohlgeordnet ist. Der Satz besagt also, dass 'x ist konstruktibel' formulierbar ist und absolut für jedes transitive Modell von ϑ.

Zunächst zur Formulierung von '$x \in L_\alpha$':

Zur Vereinheitlichung der Stellenzahlen der Gödeloperationen zu nur einer Stelle wählt man

$$\mathcal{G}_i(x) := \mathcal{F}''(x \times x),\ i = 1, ..., 8.$$

Gut sieht man, dass die Gödeloperationen absolut sind für transitive Modelle. (Übung.)

Man hat nun folgende Formel $\varphi(g, x)$, welche ausdrückt, dass $g(x) = cl(x)$ (konstruktibler Abschluss von x):

$$dom(g) = \omega \wedge g(0) = x \wedge (\forall n \in \omega)\left(g(n+1) = g(n) \cup \bigcup_{i=1}^{8} \mathcal{G}_i(g(n))\right).$$

Diese Formel ist absolut, da *dom* absolut ist und nur beschränkte Quantifikation benutzt wird. Voraussetzung ist, dass ω zum Modell gehört.

Damit ist ausdrückbar und absolut:

$$\mathcal{H}(x) = \mathcal{P}(x) \cap cl(x \cup \{x\}).$$

Nun gibt es eine folgende Formel $\sigma(f, \alpha)$, welche für eine Ordinalzahl α ausdrückt, dass $f''\alpha = L_\alpha$:

$$\begin{aligned} dom(f) \quad = \quad & \alpha + 1 \wedge f(0) = 0 \wedge (\forall \beta \in dom(f))\,(Lim(\beta) \to f(\beta) = f''\beta) \\ & \wedge (\forall \beta < \alpha)\,(f(\beta+1) = \mathcal{H}(f(\beta))). \end{aligned}$$

Auch diese Formel ist offenbar absolut.

Damit haben wir '$x \in L_\alpha$' ausgedrückt, und zwar absolut für alle transitiven Modelle, welche die benötigten Objekte enthalten, also x, dann ω (als Element, nicht nur Teilmenge), ferner mit jedem y auch $\mathcal{G}_i(y)$ für $i = 1...8$ sowie $\mathcal{H}(y)$ (dazu gehört, dass mit jedem y auch eine Funktion g, so dass $\varphi(g, y)$ enthalten ist), mit jeder Ordinalzahl auch eine Funktion f, so dass $\sigma(f, \alpha)$.

Wir formulieren also die erwünschte Aussage ϑ so:

$$(\exists \alpha \in On)(\omega \in \alpha) \wedge \bigwedge_{i=1}^{8} \forall y \exists z (z = \mathcal{G}_i(v)) \wedge \forall y \exists z (z = \mathcal{H}(y)) \wedge (\forall \alpha \in On)\, \exists f \sigma(f, \alpha).$$

Nun ist klar, dass '$x \in L_\alpha$' absolut ist für alle transitiven Modelle, welche ϑ erfüllen.■

Bemerkung zum Verständnis des Satzes: Es ging hier hauptsächlich darum, dass ZF ein unendliches Axiomschema ist und nicht durch eine einzige Aussage ausgedrückt werden kann. Aber ϑ ist eine einzige Aussage, welche für transitive Modelle bereits ausreicht, die Absoluheit von 'x ist konstruktibel' zu garantieren.

Nun kommen wir zum Beweis für $ZF \vdash V = L \to GCH$. Wir setzen mit $ZF \vdash V = L \to AC$ das Auswahlaxiom voraus. Kardinalzahlen sind also spezielle Ordinalzahlen. Sei κ eine unendliche Kardinalzahl. Sei $x \subset \kappa$, d.h. $x \in \mathcal{P}(\kappa)$. Sei κ^+ die kleinste Kardinalzahl $> \kappa$. Wir werden zeigen, dass $x \in L_{\kappa^+}$. Daraus folgt mit $|L_{k^+}| = \kappa^+$, dass $|\mathcal{P}(\kappa)| = \kappa^+$. Mit $V = L$ hat man $x \in L_\beta$ für eine Ordinalzahl β (über deren Größe noch nichts gesagt ist!). Nun sei φ folgende Aussage:

$$Extensionalitätsaxiom\ \wedge \vartheta.$$

Mit dem Reflektionssatz gibt es ein Modell $\langle S, \in\rangle \models \varphi$, $S \supset \kappa \cup \{x\} \cup \{\beta\}$, $|S| = \kappa$. Nun braucht allerdings S noch nicht transitiv zu sein, aber mit dem Mostowskischen Isomorphiesatz hat man ein **transitives** Modell $\langle M, \in\rangle$ mit einem Isomorphismus

$$\pi : \langle S, \in\rangle \xrightarrow{\sim} \langle M, \in\rangle.$$

Als zu S isomorphes Modell erfüllt M wieder ϑ (wie wir aus den Anfängen der Modelltheorie wissen). Da κ selbst transitives Element von S ist, gilt mit dem Zusatz des Isomorphiesatzes:

$$(*)\ \ \pi \restriction \kappa = id \restriction \kappa.$$

Daraus folgt aber, dass $\pi(x) = x$, weil

$$\pi(x) = \{\pi(y) | \, y \in x \cap S\} =^{(\text{mit } \kappa \subset S \text{ und } x \subset \kappa)} \{\pi(y) | \, y \in x \subset \kappa\} =^{*} x.$$

Da $\langle M, \in \rangle$ transitiv ist und die Aussage ϑ erfüllt, ist die Aussage 'x ist konstruktibel' absolut für M, und daher

$$\langle M, \in \rangle \models (\exists \alpha \in On)(x \in L_\alpha).$$

Nun ist $|M| = |S| = \kappa$. Also gilt für $\alpha \in On$ mit $\langle M, \in \rangle \models x \in L_\alpha$, dass $\alpha \in \kappa^+$. Daher mit der Absolutheit von '$x = x \in L_\alpha$':

$$\langle V. \in \rangle \models x \in L_\alpha \wedge \alpha < \kappa^+.$$

Damit insgesamt:

$$\begin{array}{lll} \langle V, \in \rangle & \models & x \in L_{k^+}, \text{ also} \\ \langle V, \in \rangle & \models & \mathcal{P}(\kappa) \subset L_{k^+} \text{ und so } \langle V, \in \rangle \models |\mathcal{P}(\kappa)| = \kappa^+. \blacksquare \end{array}$$