Mathematische Logik

Dennis Müller
www.jazzpirate.com

Anmerkung: Alle kursiven Begriffe sollten auf Wikipedia zu finden sein, sollte jemand mehr darüber erfahren wollen. Ich empfehle außerdem:

- *Logicomix – Eine epische Suche nach Wahrheit*[1]. Ein Comicbuch über das Leben Bertrand Russells und die Entdeckung der mathematischen Logik.
- *Gödel, Escher, Bach – Ein Endlos Geflochtenes Band*[2] von Douglas Hofstadter. Ein ziemlich dicker Wälzer für das breite Publikum über formale Systeme und rekursive Strukturen in der Mathematik, Informatik, Biologie, Neurologie, Koginitionswissenschaft, Kunst und Musik. Die „Bibel für theoretische Informatiker“ und der wohlverdiente Gewinner eines Pulitzer-Preises.

Ich sollte außerdem anmerken, dass ich weder Mathematik-Historiker, noch Pädagoge, noch Mathematik-Professor bin – mit Fehlern muss also gerechnet werden. Außerdem habe ich versucht, Alles so einfach wie möglich darzustellen, was sich teilweise (und notwendigerweise) auf die formale Exaktheit auswirkt.

Inhaltsverzeichnis

[1] http://www.amazon.de/Logicomix-Eine-epische-Suche-Wahrheit/dp/3855350698/ref=sr_1_3
[2] http://www.amazon.de/Gdel-Escher-Bach-Endloses-Geflochtenes/dp/3423300175/ref=sr_1_1

1 Was soll der Kram?

Der zentralste Begriff der Mathematik (und das, was im Großen und Ganzen die Mathematik von nahezu allen anderen Wissenschaften absetzt) ist der *Beweis*. Zumindest in der Theorie ist eine einmal streng bewiesene Aussage unabstreitbar für alle Zeiten „wahr". Entsprechend wichtig ist es für Mathematiker sich darüber einig zu sein, was ein streng gültiger Beweis überhaupt ist. Dazu kommt das weitere Problem, dass jeder Beweis von vorneherein bestimmte Annahmen machen muss – seien es entweder bereits zuvor bewiesene Aussagen oder *Axiome*, also so grundlegende Aussagen, dass niemand, der noch halbwegs geradeaus denken kann ohne sich zu verlaufen, sie abstreiten würde. Vor 200 Jahren war das noch relativ unproblematisch – Euklid hatte bereits die Geometrie axiomatisiert und den Goldstandard für geometrische Beweise geliefert, und der Rest der Mathematik hatte letztenendes eh nur mit Zahlen zu tun, bei denen man sich (von Streitereien über imaginäre Zahlen und ähnliche Spaße abgesehen) halbwegs sicher sein konnte, dass die grundlegenden Annahmen („Jede reelle Zahl ist entweder größer oder kleiner oder gleich 0"– ach nee, echt?) ziemlich gesichert sind. Sonstige Fragestellungen bezüglich der Wahrheit mathematischer Konzepte war was für Philosophen, aber die Mathematik funktionierte an für sich recht gut.

Problematisch wurde das Ganze erst wirklich, als gegen Ende des 19. Jahrhunderts mehrere unbequeme Fragestellungen auftauchten. Zum einen war da die Entdeckung *nicht-euklidischer Geometrien*, wie der hyperbolischen Geometrie. Nicht-euklidische Geometrien erhält man, indem man ein bestimmtes Axiom, das Euklid für offensichtlich wahr erachtete, einfach verneinte. Konkret war das das *Parallelenpostulat*:

> In jeder Ebene A gibt es zu jeder Geraden g und jedem Punkt S außerhalb von g genau eine Gerade, die zu g parallel ist und durch den Punkt S geht.

Das Axiom war schon lange etwas suspekt, weil es im Gegensatz zu den anderen euklidischen Axiomen irgendwie hässlich wirkte; so, als sollte es irgendwie mit den anderen Axiomen beweisbar sein. Im 19. Jahrhundert wurde schließlich klar, dass das nicht nur nicht der Fall ist, sondern, dass man das Axiom wunderbar verneinen kann, ohne irgendwelche Widersprüche zu erzeugen. Die Frage, die sich damit stellte war also: Wie kann das Parallelenpostulat (offensichtlich) „wahr" sein, wenn ich es genausogut verneinen kann, und trotzdem mathematisch sinnvolle Ergebnisse damit erhalte? Was soll denn dann „wahr" überhaupt noch bedeuten? Und was ist eigentlich mit vierdimensionaler (oder höherer) Geometrie? Warum führt die nicht zu Widersprüchen? In welchem Sinne ist die dann weniger „wahr" als die klassische zwei- oder dreidimensionale?

Ein weiteres Problem war die gesamte Analysis. Leibniz und Newton hatten gleichzeitig und unabhängig voneinander im 17. Jahrhundert die Differential- und Integralrechnung erfunden – allerdings benutzten sie dafür *infinitesimale* (also „unendlich kleine") Zahlen. Ein Ausdruck wie $\frac{df}{dx}$ war für Leibniz tatsächlich ein echter Bruch, und nicht (wie heutzutage) einfach nur eine Notation für $\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}$, nur, dass man sich die „Zahlen" df und dx als „unendlich klein" vorzustellen hatte – was immer das überhaupt heißen sollte. Genauso stand $\int f(x)dx$ bei Leibniz für „Die Summe über alle Flächenabschnitte der Form $[f(x+dx)-f(x)]\cdot dx$ für unendlich kleine dx" (daher das Symbol $\int$ – das sollte ein langgezogenes S für „Summe" sein). Dedekind, Weierstrass und andere stellten zwar später die Analysis auf ein sicheres Fundament, indem sie den ganzen infinitesimalen Kram durch unproblematischere ϵ-δ-Kriterien[3] ersetzten, aber was Newton und Leibniz damals trieben machte irgendwie Sinn. Und mehr noch: Es funktionierte! Also was zum Geier ist mit diesen infinitesimalen Zahlen? Gibt es die jetzt oder nicht?

[3]Siehe *Epsilontik*

Aber nicht nur Definitionen und Axiome wurden langsam fragwürdig und angreifbar. Auch gewisse Beweistechniken wurden manchen Mathematikern langsam zu Blödsinnig, insbesondere der *Satz vom ausgeschlossenen Dritten (Tertium non datur):* Jede Aussage ist entweder wahr, oder sie ist falsch und ihre Negation ist wahr. Ein klassisches Beispiel wäre Folgendes:

Satz. *Es gibt zwei irrationale Zahlen $a, b \in \mathbb{R}$ so, dass a^b rational ist.*

Beweis. Wir wissen, dass $\sqrt{2}$ irrational ist. Betrachte $x = \sqrt{2}^{\sqrt{2}}$. Dann ist x entweder rational, oder irrational (Satz vom ausgeschlossenen Dritten). In ersterem Falle haben wir mit $a = b = \sqrt{2}$ den Satz bewiesen. Nehmen wir also an, x ist irrational. Dann gilt aber $x^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$, und das ist rational, also haben wir mit $a = x$ und $b = \sqrt{2}$ den Satz bewiesen. $\square$

Das Problem mit diesem Beweis ist, dass er uns immer noch nicht sagt, *wie a und b jetzt eigentlich aussehen!* Er sagt zwar „Es gibt zwei Zahlen a und b...“, gibt aber keinerlei Aufschluss darüber, wie wir diese Zahlen finden. Einigen Mathematikern (sogenannte *Intuitionisten* oder *Konstruktivisten*) wurde das zu bunt, und sie lehnten entsprechend den Satz vom ausgeschlossenen Dritten ab. David Hilbert trieb das Spiel schließlich auf die Spitze, indem er per Widerspruch bewies, dass ein allgemeines Lösungsverfahren für eine bestimmte Klasse von Gleichungen existiert; es gibt also ein Verfahren, dass jede dieser Gleichungen löst. Das Problem war, dass sein Beweis einem nicht sagte, wie dieses Lösungsverfahren überhaupt aussieht, ergo konnte es auch niemand nutzen, und das Resultat selbst hatte ergo keine praktische Bewandnis.

Anfang des 20. Jahrhunderts kulminierte all das in den sogenannten *Grundlagenstreit der Mathematik*, der David Hilbert dazu veranlasste, sein *Hilbert-Programm* auszurufen. Dies war der Versuch, mit streng formalen Methoden folgendes zu erreichen:

1. Eine rein formale Sprache zu entwerfen, die mit mathematischen Methoden analysiert werden kann und mit der jede mathematische Aussage formuliert werden kann, so dass ihre Bedeutung eindeutig und unmisverständlich ist.

2. Einen *Beweiskalkül* für diese Sprache zu finden, der *vollständig* ist. Das bedeutet, eine Anzahl fundamentaler Beweisschritte zu finden, die

   a) so grundlegend sind, dass sie jeder für gültig erachten würde, der nicht gerade Intuitionist ist (Hilbert und die meisten anderen Mathematiker erachteten den Satz vom ausgeschlossenen Dritten und Widerspruchsbeweise als viel zu nützlich um darauf zu verzichten),

   b) ausschließlich von der *Syntax* einer Formel abhängig sind; ich also nicht wissen muss, was irgendwelche Sätze der formalen Sprache „bedeuten“, um überprüfen zu können, ob ein Beweisschritt gültig ist oder nicht (insbesondere sollte ein *Algorithmus* (wie z.B. ein Computerprogramm) existieren, mit dem man die Gültigkeit eines Beweises überprüfen kann),

   c) widerspruchsfrei sind, also niemals zu einem Widerspruch führen, wenn nicht die Axiome bereits widersprüchlich sind,

   d) einem erlauben, jede gültige Folgerung abzudecken; das heißt: Wenn aus irgendwelchen Axiomen ein bestimmter Satz logisch folgt, dann sollte auch ein Beweis in dem Beweiskalkül existieren.

3. Ein in dieser Sprache ausdrückbares System von Axiomen für die *gesamte Mathematik* zu finden, das nicht zu Widersprüchen führt (also *konsistent* ist) und das jeden

formulierbaren Satz *entscheidet*, d.H. jeder Satz, den ich in der formalen Sprache ausdrücken kann sollte entweder beweisbar oder widerlegbar sein (das Axiomensystem sollte *vollständig* sein).[4]

> „Wir müssen wissen; wir *werden* wissen. In der Mathematik gibt es kein Ignorabimus!“
> – *David Hilbert*

Die ersten zwei Punkte schaffte Hilbert; die resultierende Sprache war die *Prädikatenlogik (erster Stufe)* und er selbst stellte auch den ersten Beweiskalkül dafür auf (der sogenannte *Hilbert-Kalkül.* Wer hätte das geadacht...). Kurt Gödel bewies schließlich auch in seiner Doktorarbeit, dass dieser Kalkül tatsächlich vollständig im gewünschten Sinne ist. Man lasse sich das kurz auf der Zunge zergehen:

- (So ziemlich) **Jede** mathematische Aussage lässt sich *als Formel ausdrücken.*
- **Jede** Aussage, die tatsächlich aus irgendwelchen Axiomen folgt, *lässt sich auch beweisen.*
- **Jeder** Beweis lässt sich so ausdrücken, dass ein Computer *nur aufgrund des formalen Aufbaus der Formeln, ohne jegliches mathematisches Verständnis*[5] entscheiden kann, ob der Beweis gültig ist!

Für Hilberts Wunsch Nummer 3, das vollständige und widerspruchsfreie Axiomensystem, gab es auch bereits einen plausiblen und vielversprechenden Kandidaten: Georg Cantor hatte nicht lange vorher die höchst kontroverse Mengenlehre entdeckt, die unter Anderem zu so augenscheinlich absurden Ergebnissen führte wie, dass es unterschiedliche Unendlichkeiten gibt, manche davon „größer“ als andere. Gleichzeitig schien sie aber mächtig genug zu sein, um die gesamte herkömmliche Mathematik zu beschreiben - Zahlen, Funktionen, alles ließ sich mit Hilfe von Mengen darstellen. Hilbert war davon hellauf begeistert, auch wenn viele Mathematiker damals die Mengenlehre als absurde Spinnerei abtaten. Aber:

> „Aus dem Paradies, das Cantor uns geschaffen hat, soll uns niemand vertreiben können!“
> – *David Hilbert*

Ungünstigerweise bewies Gödel kurz darauf, dass was Hilbert sich da zusammengeträumt hatte gar nicht möglich ist. Dieses Resultat ist nun als die *Gödelschen Unvollständigkeitssätze* bekannt und besagt genauer:

> *1. Gödelscher Unvollständigkeitssatz:* Jedes Axiomensystem, das mindestens die Existenz natürlicher Zahlen, die Addition und die Multiplikation liefert, ist entweder unvollständig (es gibt also Sätze, die sich weder beweisen noch widerlegen lassen) oder widersprüchlich (also komplett nutzlos).
> *2. Gödelscher Unvollständigkeitssatz:* In keinem solchen Axiomensystem lässt sich beweisen, dass das Axiomensystem selbst (oder jede beliebige Erweiterung davon) widerspruchsfrei ist, außer, es ist *nicht* widerspruchsfrei.

Glücklicherweise war das Abhaken der ersten beiden Punkte auf Hilberts Liste schon fruchtbar genug, dass die „Alltagsmathematik“ sich keine großartigen existentialistischen

[4] Man beachte, dass wir jetzt zwei unterschiedliche Konzepte der Vollständigkeit haben: Das eine bezieht sich auf einen Beweiskalkül, das andere auf ein Axiomensystem.
[5] Was auch immer das heißen soll

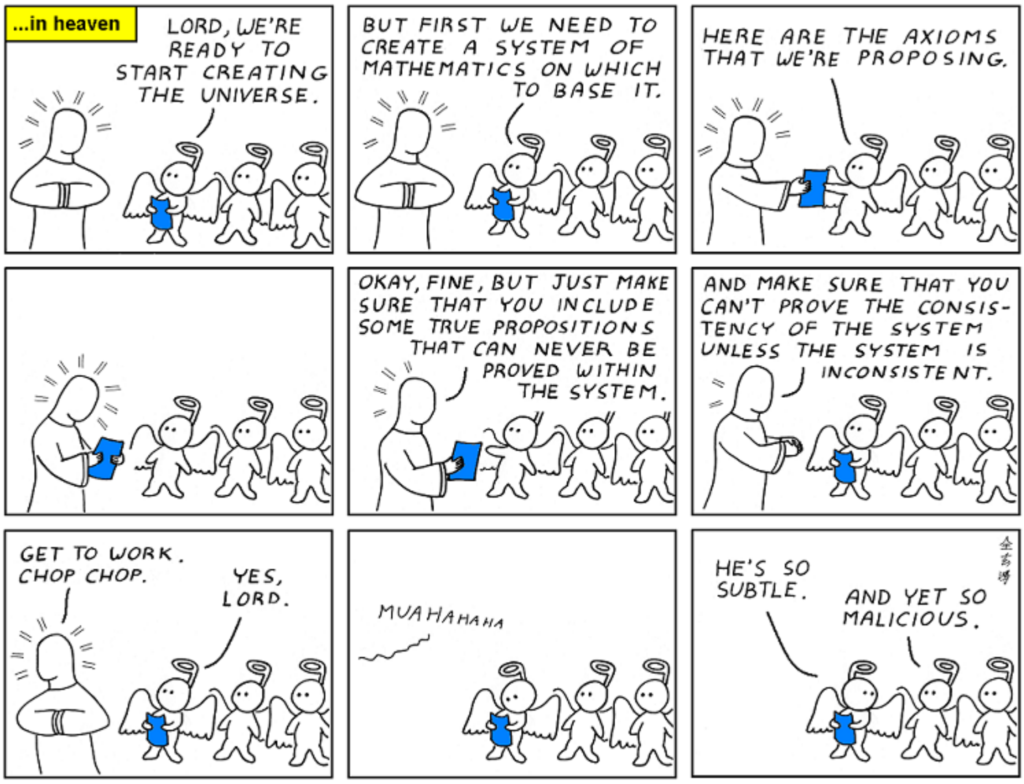

Abbildung 1: Die Gödelschen Unvollständigkeitssätze `http://abstrusegoose.com/244`

Sorgen mehr machen muss; und an die Unvollständigkeitssätze hat man sich heutzutage gewöhnt. Das Axiomensystem, in dem die übliche Mathematik stattfindet nennt sich *ZFC* (Für **Z**ermelo-**F**ränkel-Mengenlehre mit Auswahlaxiom (Axiom of **C**hoice)), und auch wenn die darin unentscheidbaren Sätze für Logiker und insbesondere Mengentheoretiker spannend sind und man sich entsprechend darüber streiten kann (und tut), welche davon man als zusätzliche Axiome akzeptieren sollte oder nicht, stellen die Unvollständigkeitssätze außerhalb der Logik für die meisten Mathematiker keine Hürde oder auch nur Sorge dar.

> „In der Mathematik **versteht** man Dinge nicht – man **gewöhnt** sich einfach an sie.“
> \- *John von Neumann*

1 Aussagenlogik

Bevor wir uns die Prädikatenlogik anschauen können, ziehen wir uns erstmal auf die viel einfachere Aussagenlogik zurück. Die ist zwar bei weitem nicht so Ausdrucksstark (eigentlich kann sie nur *zusammengesetzte Aussagen* analysieren), aber viele Konzepte der Logik kommen hier bereits ins Spiel und ersparen uns entsprechend später viel Arbeit.

Das wichtigste ist der Unterschied zwischen *Syntax* und *Semantik*: Die Syntax beschreibt, wie eine gültige Formel der Aussagenlogik aufgebaut sein muss; sie beschäftigt sich also nur mit dem strukturellen Aufbau. Die Semantik dagegen sagt uns, wie wir eine Formel zu interpretieren haben, damit sie auch eine echte Bedeutung hat. Das Ziel ist es letztenendes, jeden Beweis auf eine rein syntaktische Ebene zu reduzieren; aber Formeln sind natürlich sinnlos, wenn wir ihnen keine Bedeutung zuschreiben können.

1 Syntax

Wir beginnen mit einer Menge $\mathcal{V}$ von Aussagenvariablen. Diese sollen natürlich Aussagen repräsentieren, wir sollten also wenn es um Semantik geht jeder Aussagenvariablen einen eindeutigen Wahrheitswert (wahr oder falsch) zuordnen können; aber auf syntaktischer Ebene sind Aussagenvariablen erstmal nur *beliebige Symbole*. Üblicherweise benutzt man die Großbuchstaben $A, B, C, ...$

Die Definition einer Formel ist *rekursiv*. Das bedeutet: Wir werden einen Basisfall für eine Formel definieren (nämlich einfach Aussagenvariablen) und anschließend festlegen, wie wir bereits vorhandene Formeln so miteinander verbinden dürfen, dass wieder eine Formel entsteht:

Definition 1.1. Sei $\mathcal{V}$ eine Menge von Aussagenvariablen. Folgendes *und nur folgendes* ist eine $\mathcal{V}$-Formel:

- Jede Aussagenvariable $A \in \mathcal{V}$ ist eine Formel.
- Wenn φ und ψ beliebige $\mathcal{V}$-Formeln sind, dann sind auch
  - $\neg\varphi$ („Nicht φ")
  - $(\varphi \wedge \psi)$ („φ und ψ")
  - $(\varphi \vee \psi)$ („φ oder ψ")
  - $(\varphi \rightarrow \psi)$ („Aus φ folgt ψ" oder „φ impliziert ψ") und
  - $(\varphi \leftrightarrow \psi)$ („φ genau dann, wenn ψ" oder „φ ist äquivalent zu ψ")

  jeweils $\mathcal{V}$-Formeln.

Man beachte dabei die Klammerung – die Definition gibt einem genau vor, wie man Klammern zu setzen hat.

Übungsaufgabe Sei $\{A, B, C, ...\}$ eine Menge von Aussagenvariablen. Welche der folgenden Zeichenketten sind Formeln?

1. E
2. $F \wedge G$
3. $(F \wedge G)$
4. $(\neg B)$
5. $((A \vee B) \rightarrow \neg(C \leftrightarrow D))$
6. $\neg C$
7. $\neg A \rightarrow (B \wedge C)$
8. $\neg(A \wedge \neg A)$

Die Definition und die exakte Vorgabe der Klammerung garantieren, dass jede Formel eindeutig interpretierbar ist, führt aber manchmal zu ziemlich hässlichen Klammerschachtelungen. Ähnlich wie bei Punkt-vor-Strich einigt man sich deshalb üblicherweise auf die folgende Konvention:
$\neg$ vor $\wedge$ vor $\vee$ vor $\rightarrow$ vor $\leftrightarrow$
Die Zeichenkette $\neg A \rightarrow B \wedge C$ würde man also als Formel $(\neg A \rightarrow (B \wedge C))$ interpretieren.

2 Semantik

Wir wollen uns jetzt überlegen, wie wir aussagenlogischen Formeln eine Bedeutung zuordnen können. Dazu müssen wir zunächst mal den einzelnen Aussagenvariablen einen Wahrheitswert, also Wahr oder Falsch, zuweisen. Wir tun dies mit Hilfe einer Belegungsfunktion:

Definition 1.2. Sei $\mathcal{V}$ eine Menge von Aussagenvariablen. Eine *Belegung* ist eine Funktion $\mathcal{F} : \mathcal{V} \to \{0, 1\}$, also eine Funktion so, dass für jede Aussagenvariable $A \in \mathcal{V}$ entweder $\mathcal{F}(A) = 1$ oder $\mathcal{F}(A) = 0$ ist. Wir interpretieren 1 als „Wahr" und 0 als „Falsch".

Nur Aussagenvariablen Wahrheitswerte zuzuordnen bringt uns aber natürlich bei komplexeren Formeln nichts. Um auch diesen einen Wert zuzuordnen müssen wir festlegen, was mit den ganzen Verknüpfungen passiert:

Definition 1.3. Sei $\mathcal{V}$ eine Menge von Aussagenvariablen und $\mathcal{F}$ eine Belegung. Seien außerdem φ und ψ beliebige $\mathcal{V}$-Formeln. Wir erweitern $\mathcal{F}$ auf beliebige Formeln wie folgt:

- Wir setzen $\mathcal{F}(\neg\varphi) = 1$ genau dann, wenn $\mathcal{F}(\varphi) = 0$ ist.
- Wir setzen $\mathcal{F}(\varphi \wedge \psi) = 1$ genau dann, wenn $\mathcal{F}(\varphi) = 1$ und $\mathcal{F}(\psi) = 1$ ist.
- Wir setzen $\mathcal{F}(\varphi \vee \psi) = 1$ genau dann, wenn $\mathcal{F}(\varphi) = 1$ oder $\mathcal{F}(\psi) = 1$ ist (oder beides).
- Wir setzen $\mathcal{F}(\varphi \to \psi) = 1$ genau dann, wenn $\mathcal{F}(\psi) = 1$ oder $\mathcal{F}(\varphi) = 0$ ist (oder beides).
- Wir setzen $\mathcal{F}(\varphi \leftrightarrow \psi) = 1$ genau dann, wenn $\mathcal{F}(\varphi) = \mathcal{F}(\psi)$ ist.

Wir können dies auch in Form einer Wahrheitstabelle angeben:

φ	ψ	$\neg\varphi$	$(\varphi \wedge \psi)$	$(\varphi \vee \psi)$	$(\varphi \to \psi)$	$(\varphi \leftrightarrow \psi)$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Man kann Wahrheitstabellen auch wunderbar benutzen um zu zeigen, dass zwei Formeln *logisch äquivalent* sind, also unter jeder Belegung den selben Wahrheitswert erhalten. Nehmen wir zum Beispiel die zwei Formeln $(\varphi \to \psi)$ und $\neg(\varphi \wedge \neg\psi)$ (Man überlege kurz - warum sind die Formeln äquivalent? Was besagen die Formeln in Worten?):

φ	ψ	$(\varphi \to \psi)$	$\neg\psi$	$(\varphi \wedge \neg\psi)$	$\neg(\varphi \wedge \neg\psi)$
1	1	1	0	0	1
1	0	0	1	1	0
0	1	1	0	0	1
0	0	1	1	0	1

Man sieht, die beiden Spalten unter $(\varphi \to \psi)$ und $\neg(\varphi \wedge \neg\psi)$ sind identisch. Man schreibt dafür auch $(\varphi \to \psi) \equiv \neg(\varphi \wedge \neg\psi)$.

Es ist vielleicht kommentarwürdig, dass die Formel $(A \to B)$ („Aus A folgt B") per Definition immer wahr ist, wenn A falsch ist. Der Satz „Wenn der Mond aus Käse ist, dann ist der Himmel grün" wäre in der Aussagenlogik also wahr, auch wenn natürlich weder der Mond aus Käse noch der Himmel grün ist. Dieser Sachverhalt nennt sich *Ex falso quodlibet* („Aus Falschem folgt Beliebiges", im Englischen „Principle of explosion") und er erlaubt uns erst Widerspruchsbeweise sowie den Satz vom ausgeschlossenen Dritten.

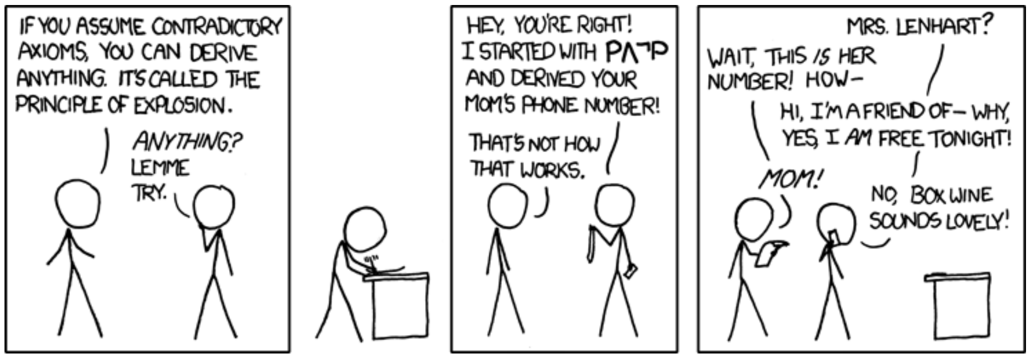

Abbildung 2: Ex falso quodlibet `http://xkcd.com/704/`

Das lässt sich folgendermaßen rechtfertigen: Es sollte nachvollziehbar sein, dass „Aus A folgt B“ gleichwertig sein sollte zu „Es kann nicht sein, dass A wahr ist, aber B falsch“. Letzteres liefert die Formel $\neg(A \wedge \neg B)$ was, wie wir gerade gezeigt haben, genau die Wahrheitstabellenspalte liefert, die unser $(A \to B)$ auch hat.

Nehmen wir außerdem an, wir wollten beweisen, dass eine Aussage A gilt. Wir machen einen Widerspruchsbeweis; gehen also von $\neg A$ aus und erhalten eine falsche Aussage B. Wir haben also gezeigt, dass $\neg A$ falsch und somit A wahr ist – aber *nur*, wenn wir weiterhin davon ausgehen dürfen, dass die Herleitung $(\neg A \to B)$ wirklich gültig war! Wäre sie das nicht, wäre ja unser Beweis unter der neuen Annahme, dass $\neg A$ falsch ist, nicht gültig. Wollen wir also Widerspruchsbeweise akzeptieren, müssen wir auch akzeptieren, dass wir aus etwas Falschem alles beliebige herleiten dürfen.

Definition 1.4. Seien φ und ψ zwei beliebige Formeln.

- φ und ψ heißen *logisch äquivalent* ($\varphi \equiv \psi$) genau dann, wenn für jede Belegung $\mathcal{F}$ der Aussagenvariablen gilt $\mathcal{F}(\varphi) = \mathcal{F}(\psi)$.
- φ heißt *Tautologie*, wenn für jede Belegung $\mathcal{F}$ gilt $\mathcal{F}(\varphi) = 1$. Wir schreiben dafür auch $\varphi \equiv \top$ und definieren $\top = (A \vee \neg A)$ für eine beliebige Aussagenvariable A.
- φ heißt *erfüllbar*, wenn es mindestens eine Belegung $\mathcal{F}$ gibt, mit $\mathcal{F}(\varphi) = 1$. Andernfalls heißt die Formel *unerfüllbar* oder *Antilogie* und wir schreiben $\varphi \equiv \bot$ und definieren $\bot = (A \wedge \neg A)$ für eine beliebige Aussagenvariable A.

Übungsaufgaben Seien wie bisher $A, B, C...$ Aussagenvariablen und φ und ψ Formeln.

1. Zeige, dass tatsächlich $(A \vee \neg A)$ eine Tautologie und $(A \wedge \neg A)$ eine Antilogie ist.
2. Zeige, dass $\varphi \equiv \psi$ gilt genau dann, wenn $(\varphi \leftrightarrow \psi)$ eine Tautologie ist.
3. Zeige, dass $(\varphi \to \psi) \equiv (\neg\varphi \vee \psi)$.
4. Zeige, dass $(\varphi \leftrightarrow \psi) \equiv ((\varphi \to \psi) \wedge (\psi \to \varphi))$.
5. Zeige, dass jede der Formeln $(A \vee B), (A \to B), (A \leftrightarrow B)$ eine logisch äquivalente Formel besitzt, die nur die Aussagenvariablen A, B und die Symbole $\neg, \wedge$ enthält (von Klammern natürlich abgesehen).
6. Welche der folgenden Formeln sind erfüllbar/Tautologien/Antilogien?
   a) $(A \to (A \wedge B))$
   b) $(A \to (\neg A \to B))$

c) $\neg((A \wedge B) \rightarrow A)$
d) $\neg((A \vee B) \rightarrow B)$
e) $(((A \rightarrow B) \rightarrow A) \rightarrow A)$

3 Metaebenen

An der Stelle sollte man sich kurz bewusst machen, was wir hier eigentlich tun: Die Aussagenlogik (bzw. die Logik im allgemeinen) soll eine formale Beschreibung des logischen Schlussfolgerns liefern. Das erfordert aber natürlich selbst logisches Schlussfolgern. Eine Aussage wir „Die Formeln $(\varphi \rightarrow \psi)$ und $\neg(\varphi \wedge \neg\psi)$ sind äquivalent“ ist eine Aussage, die sich logisch rechtfertigen lässt, und entsprechend mit Hilfe der Aussagenlogik beschrieben werden können sollte, also als Formel ausdrückbar sein sollte (nämlich $((\varphi \rightarrow \psi) \leftrightarrow \neg(\varphi \wedge \neg\psi))$). Es ist aber gleichzeitig eine Aussage *über* Formeln. Es ist also wichtig, sich darüber Gedanken zu machen, auf welcher *Metaebene* man sich gerade befindet. Dadurch, dass wir das Symbol $\equiv$ für logische Äquivalenz eingeführt haben, haben wir nun drei verschiedene Metaebenen: Einmal die Ebene der aussagenlogischen Formeln, auf der sich die Formel $((\varphi \rightarrow \psi) \leftrightarrow \neg(\varphi \wedge \neg\psi))$ befindet. Diese Formel hat ohne eine Belegung zunächst keine eigene Bedeutung. Wir können jedoch eine Metaebene höher gehen und erhalten z.B. die Aussage „Die Formel $((\varphi \rightarrow \psi) \leftrightarrow \neg(\varphi \wedge \neg\psi))$ ist eine Tautologie“. Dies ist nun eine Aussage *über* Formeln; sie ist also nicht mehr Gegenstand der formalen Aussagenlogik, sondern befindet sich eine Metabene höher; genauso wie die (äquivalente) Aussage $((\varphi \rightarrow \psi) \equiv \neg(\varphi \wedge \neg\psi))$ – dadurch, dass diese das Symbol $\equiv$ enthält, das nicht in der formalen Definition des Begriffs „Formel“ vorkommt, ist dies *keine gültige Formel der Aussagenlogik*. Wir können außerdem noch eine Ebene höher gehen, indem wir den Satz formulieren „Es gilt $\varphi \equiv \psi$ genau dann, wenn $\varphi \leftrightarrow \psi$ eine Tautologie ist“. Dies ist nun eine Aussage *über Aussagen über aussagenlogische Formeln*, man könnte diesen Satz also einer dritten Metaebene zuordnen.

Letztenendes gehorcht aber unsere Argumentation auf allen drei Ebenen irgendwie den Gesetzen der Aussagenlogik. Man sollte sich also immer bewusst machen (oder zumindest aufpassen), auf welcher Ebene man gerade argumentiert, damit man nicht Gefahr läuft, z.B. den Ausdruck $\varphi \equiv \psi$ als aussagenlogische Formel zu betrachten, obwohl er keine ist.

4 Aussagenlogische Formeln als Boolesche Algebra

Wir wollen uns nun anschauen, was wir für allgemeine Äquivalenzen zwischen aussagenlogischen Formeln finden können. Das macht es deutlich einfacher zu prüfen, ob eine Formel eine Tautologie oder überhaupt erfüllbar ist. Nachdem wir wissen, dass $(A \leftrightarrow B) \equiv ((A \rightarrow B) \wedge (B \rightarrow A))$ gilt, sowie $(A \rightarrow B) \equiv (\neg A \vee B)$ können wir die Symbole $\rightarrow$ und $\leftrightarrow$ dabei ignorieren – jede Formel lässt sich entsprechend schließlich so umschreiben, dass sie nur noch $\neg, \wedge$ und $\vee$ enthält.[6]

Seien im Folgenden φ, ψ, χ beliebige aussagenlogische Formeln:

- $\wedge$ und $\vee$ sind *assoziativ*, das bedeutet:

$$(\varphi \wedge (\psi \wedge \chi)) \equiv ((\varphi \wedge \psi) \wedge \chi) \qquad (\varphi \vee (\psi \vee \chi)) \equiv ((\varphi \vee \psi) \vee \chi)$$

  Wir können also auf viele Klammern verzichten, indem wir einfach $A \wedge B \wedge C \wedge D \wedge ...$ schreiben statt z.B: $(A \wedge (B \wedge ((C \wedge D) \wedge ...$

[6] Um genauer zu sein könnten wir uns sogar komplett auf $\neg$ und $\wedge$ reduzieren, da $(A \vee B) \equiv \neg(\neg A \wedge \neg B)$ gilt; oder wir schreiben alle Formeln so um, dass wir nur noch die Symbole $\neg$ und $\rightarrow$ verwenden und eliminieren alle $\wedge$ und $\vee$...

- $\wedge$ und $\vee$ sind *kommutativ*, das bedeutet:

$$(\varphi \wedge \psi) \equiv (\psi \wedge \varphi) \qquad (\varphi \vee \psi) \equiv (\psi \vee \varphi)$$

  Die Reihenfolge der Teilformeln ist also auch egal.

- Es gelten die folgenden zwei *Absorptionsgesetze*:

$$(\varphi \vee (\varphi \wedge \psi)) \equiv \varphi \qquad (\varphi \wedge (\varphi \vee \psi)) \equiv \varphi$$

- Man erinnere sich, dass $\top$ für eine beliebige Tautologie steht, und $\bot$ für eine beliebige Antilogie. Es gilt:

$$(\varphi \vee \bot) \equiv \varphi \qquad (\varphi \wedge \top) \equiv \varphi$$

  Man sagt auch „$\top$ ist *neutral* bzgl. $\wedge$“, beziehungsweise „$\bot$ ist neutral bzgl. $\vee$“.

- $\wedge$ und $\vee$ sind zueinander *distributiv*, das heißt:

$$(\varphi \wedge (\psi \vee \chi)) \equiv ((\varphi \wedge \psi) \vee (\varphi \wedge \chi)) \qquad (\varphi \vee (\psi \wedge \chi)) \equiv ((\varphi \vee \psi) \wedge (\varphi \vee \chi))$$

- Es gelten die sogenannten *DeMorganschen Regeln:*

$$\neg(\varphi \wedge \psi) \equiv (\neg\varphi \vee \neg\psi) \qquad \neg(\varphi \vee \psi) \equiv (\neg\varphi \wedge \neg\psi)$$

Übungsaufgaben

1. Überzeuge dich (z.B. mit Hilfe von Wahrheitstabellen), dass die obigen Äquivalenzen tatsächlich alle gelten!

2. Angenommen, wir ersetzen $\wedge$ durch die übliche Multiplikation $\cdot$, $\vee$ durch die Addition $+$, $\bot$ durch 0, $\top$ durch 1 und $\neg$ durch die Negation $-$ (aus $(A \wedge B) \vee \neg C \vee \top$ würde z.B. $AB + (-C) + 1$). Welche der Regeln gelten dann, wenn wir Aussagenvariablen als „normale Variablen“ für Zahlen betrachten (und die Äquivalenz $\equiv$ als echte Gleichheit $=$)?

Wir waren bisher formal sehr vorsichtig und haben bei allen Regeln immer brav $\equiv$ geschrieben, statt $=$. Das macht auch Sinn, denn so, wie wir aussagenlogische Formeln definiert haben, sind natürlich $\neg(A \wedge B)$ und $(\neg A \vee \neg B)$ nicht die selbe Formel – sie sind „nur“ logisch äquivalent. Aber wenn wir mal ehrlich sind – eigentlich interessieren wir uns doch nicht dafür, ob zwei Formeln *technisch gesehen* verschieden sind, wenn sie logisch äquivalent sind. Wir können also eigentlich auch so tun, als ob logisch äquivalente Formeln tatsächlich *gleich* sind. Formal können wir das tun, indem wir mit z.B. dem Ausdruck $(A \wedge B)$ nicht mehr die aussagenlogische Formel selbst bezeichnen, sondern stattdessen *die Menge aller aussagenlogischen Formeln φ, für die gilt $\varphi \equiv (A \wedge B)$*. Diese Menge nennt sich dann *Äquivalenzklasse*, und wir können sie genauso behandeln wie aussagenlogische Formeln selbst; aber das ist nur formaler Firlefanz. Wichtig ist nur: Wir können so tun, als ob äquivalente Formeln gleich wären.

Mit den Äquivalenzregeln, die wir gerade betrachtet haben, haben wir übrigens gezeigt, dass Aussagenlogische Formeln (bzw. deren Äquivalenzklassen) eine *Boolesche Algebra* bilden. Damit verhalten sich Formeln sehr ähnlich wie Mengen, wenn wir $\wedge$ und $\vee$ als Schnitt- bzw. Vereinigungsmenge interpretieren, $\bot$ als die leere Menge, $\neg$ als das Komplement und $\top$ als eine gemeinsame Obermenge aller betrachteten Mengen (aus Paradoxiegründen versuche ich gerade sowas wie eine „Menge aller Mengen“ zu vermeiden, weil dahinter der Wahnsinn verborgen liegt).

Praktischerweise können wir jetzt die ganzen obigen Äquivalenzen ausnutzen, um deutlich eleganter und (meistens) einfacher Formeln zu analysieren. Nehmen wir z.B. die Formel $A \wedge \neg(\neg B \vee \neg(C \wedge D) \vee A)$. Diese enthält 4 Aussagenvariablen, die unter einer Belegung jeweils einen von zwei Wahrheitswerten annehmen können. Eine Wahrheitstabelle bräuchte also bereits $2^4 = 16$ Zeilen. Aber indem wir die obigen Regeln ausnutzen, können wir schnell umformen:

$$A \wedge \neg(\neg B \vee \neg(C \wedge D) \vee A) \equiv A \wedge \neg(\neg B \vee \neg C \vee \neg D \vee A) \equiv A \wedge B \wedge C \wedge D \wedge \neg A$$

$$\equiv \underbrace{A \wedge \neg A}_{\equiv \perp} \wedge B \wedge C \wedge D \equiv \perp \wedge ... \equiv \perp$$

...die Formel ist also eine Antilogie.

Übungsaufgaben Zeige nur mit Umformungen und bereits bekannten Tautologien, dass die folgenden Formeln Tautologien sind:

1. $(A \to ((B \to C) \to (B \to (A \wedge C))))$
2. $(A \to (B \to C) \to ((A \wedge B) \to C))$
3. $(((A \wedge B) \to C) \to (A \to (B \to C)))$
4. $(((A \to C) \wedge (B \to C)) \to ((A \vee B) \to C))$
5. $((A \to B) \vee (B \to A))$

5 Axiome und Theorien

Wir kennen jetzt zwei Methoden, aussagenlogische Formeln zu analysieren: Einmal die semantische Variante, bei der wir betrachten, was mit Formeln unter irgendwelchen Belegungen passiert (Wahrheitstabellen fallen zum Beispiel darunter); und zum anderen, indem wir Formeln in äquivalente Formeln umformen. Beide Methoden funktionieren wunderbar, solange wir nur einzelne Formeln betrachten. Interessanter wird die Sache, wenn wir anfangen, *Mengen* von Formeln zu betrachten.

In vielen Fällen lässt sich das auf einzelne Formeln reduzieren. Betrachten wir zum Beispiel die Formel $\varphi = (A \to B) \to B$. Diese Formel kann „wahr“ sein oder „falsch“. Wenn wir zum Beispiel $\mathcal{F}(A) = 0$ und $\mathcal{F}(B) = 0$ setzen, gilt $\mathcal{F}(\varphi) = 0$. Setzen wir dagegen $\mathcal{F}(A) = 0$ und $\mathcal{F}(B) = 1$, so gilt $\mathcal{F}(\varphi) = 1$ (Überzeuge dich davon, dass das tatsächlich stimmt!). Was aber, wenn wir gar nicht wissen, wie A und B belegt werden, aber wir wissen, wie bestimmte andere Formeln belegt werden? Nehmen wir zum Beispiel an, dass $\mathcal{F}(A \to B) = 1$ und $\mathcal{F}(A) = 1$ gilt — was ist dann $\mathcal{F}(\varphi)$?

Wir kennen also die Belegung von zwei Formeln A und $(A \to B)$ und interessieren uns für die Belegung einer dritten Formel, nämlich $\varphi = (A \to B) \to B$. Wir können jetzt natürlich entweder die Formeln einzeln analysieren („Wenn $\mathcal{F}(A) = 1$ und $\mathcal{F}(A \to B) = 1$, dann muss $\mathcal{F}(B) = 1$ sein, und damit $\mathcal{F}(\varphi) = 1$“) oder wir können sie zu einer einzelnen Formel zusammensetzen $((A \wedge (A \to B)) \to \varphi)$ und überprüfen, ob das eine Tautologie ist (Ist sie das?). Aber was passiert, wenn wir *unendlich viele* Formeln haben? Dann wird die Analyse umständlich oder vielleicht sogar unmöglich[7], und zu einer einzelnen Formel zusammensetzen wird komplett unmöglich, da Formeln per Definition nur endlich sind.

[7] es wird *nicht* unmöglich, dank dem *Kompaktheitssatz der Aussagenlogik*, aber das betrachten wir später erst ;-)

Hier kommen jetzt Beweiskalküle ins Spiel. Denn diese ermöglichen es uns, beliebige Mengen von Formeln zu betrachten; egal ob endlich oder unendlich. Die Formeln, deren Wahrheitsbelegungen wir kennen, nennen wir dann *Axiome*, und die Menge all unserer Axiome nennen wir (wenn sie nicht widersprüchlich sind) eine *Theorie*:

Definition 1.5. Sei T eine Menge von aussagenlogischen Formeln und φ irgendeine Formel.

- Wir sagen „*φ folgt logisch aus T*“, wenn für jede Belegung $\mathcal{F}$, die jede Formel aus T erfüllt (also $\mathcal{F}(\psi) = 1$ für alle $\psi \in T$), auch $\mathcal{F}(\varphi) = 1$ gilt. Wir schreiben dafür $T \models \varphi$.
- Wir nennen die Formeln in T *Axiome* und T eine *Theorie*, wenn *nicht* $T \models \bot$ gilt.[8]

Man beachte, dass diese Definition *semantisch* ist, weil sie Belegungen beinhaltet. Unser letztendliches Ziel ist es, eine Möglichkeit zu finden, diese Definition auf die reine Syntax der Formeln zu reduzieren.

Übungsaufgaben

1. Angenommen $\varphi \in T$. Gilt dann $T \models \varphi$?
2. Sei $T = \{\varphi_1, ..., \varphi_n\}$ endlich. Überlege, dass tatsächlich $T \models \psi$ gilt genau dann, wenn $(\varphi_1 \wedge ... \wedge \varphi_n) \rightarrow \psi$ eine Tautologie ist.
3. *Ex falso quodlibet:* Angenommen $T \models \bot$. Begründe, dass dann $T \models \varphi$ gilt, egal wie φ aussieht (beachte die Fußnote unten).
4. Sei $\mathcal{V} = \{A_1, A_2, A_3, ...\}$ unsere (unendliche!) Menge von Aussagenvariablen und
$$T = \{(A_1 \wedge A_2), (A_2 \wedge A_3), (A_3 \wedge A_4), ...\}$$
Zeige, dass dann für je zwei beliebige natürliche Zahlen n, m gilt $T \models (A_n \wedge A_m)$.
5. Überlege, dass $T \models \varphi$ gilt genau dann, wenn $(T \cup \{\neg\varphi\}) \models \bot$.

In der Aussagenlogik sind unendliche Theorien eigentlich relativ unsinnig - in der Prädikatenlogik werden sie aber tatsächlich interessant, denn dort gibt es viele Dinge, die man mit nur endlich vielen Formeln leider nicht ausdrücken kann.

6 Ein Kalkül für die Aussagenlogik

Wir werden jetzt einen Kalkül betrachten, der es uns erlaubt streng formal und rein syntaktisch zu definieren, was ein gültiger Beweis innerhalb der Aussagenlogik ist, also wann eine Formel φ aus den Axiomen T beweisbar ist. Ein Kalkül besteht aus zwei verschiedenen „Regeln“:

1. Elementaren *Axiomen*, also Formeln, die *immer* als beweisbar betrachtet werden (egal wie T aussieht).
2. *Inferenzregeln* der Form „Wenn φ aus T folgt, dann folgt auch ψ aus T“.

[8] Anmerkung: Es gibt natürlich keine Belegung, für die $\mathcal{F}(\bot) = 1$ gilt. Die Behauptung $T \models \bot$ (also, dass *jede* Belegung, *die* T erfüllt, auch $\bot$ erfüllt) bedeutet also letztenendes, dass es keine Belegung *gibt*, die T erfüllt, weil diese dann ja auch $\bot$ erfüllen müsste, was nicht geht.

Es gibt jede Menge verschiedener Kalküle, und alle haben die selben beweisbaren Formeln; welchen man benutzt ist aus mathematischer Sicht also völlig egal. Ich habe deswegen einen ausgewählt, der mit relativ wenigen Regeln auskommt.

Inferenzregeln werden üblicherweise als Bruch dargestellt, wir schreiben also $\frac{\varphi_1, \varphi_2}{\psi}$ um zu sagen „Wenn φ_1 und φ_2 beweisbar sind, dann dürfen wir ψ folgern". Ein Beweis in T für eine Formel φ_n ist dann nichts anderes mehr als eine (endliche) Folge von Formeln $(\varphi_1, ..., \varphi_n)$ so, dass jede der Formeln φ_i entweder ein Axiom ist (egal ob ein Kalkülaxiom oder eines aus T) oder es eine Inferenzregel gibt, die es erlaubt φ_i aus vorherigen Formeln der Folge herzuleiten.

Definition 1.6. Sei T eine Theorie und φ eine Formel. Wir sagen „φ ist *beweisbar* in T" und schreiben $T \vdash \varphi$ genau dann, wenn es eine endliche Folge von Formeln $(\varphi_1, ..., \varphi_n)$ gibt so, dass $\varphi_n = \varphi$ und für jedes der φ_i gilt:

1. $\varphi_i \in T$ oder
2. φ_i ist ein Axiom des Kalküls oder
3. Es gibt $j, k < i$ so, dass $\frac{\varphi_j, \varphi_k}{\varphi_i}$ eine Inferenzregel des Kalküls ist.

Der Kalkül, den wir betrachten wollen, benutzt ausschließlich die Symbole $\neg$ und $\rightarrow$. Wir betrachten also $(\varphi \wedge \psi)$ als „Abkürzung" für $\neg(\varphi \rightarrow \neg\psi)$ und $(\varphi \vee \psi)$ steht für $(\neg\varphi \rightarrow \psi)$. Man überzeuge sich, dass diese Formeln tatsächlich logisch äquivalent sind!

Definition 1.7. (Lukasiewicz-Kalkül) Seien φ, ψ, χ beliebige Formeln der Aussagenlogik.

- Folgende Formeln sind Axiome:
  1. $(\varphi \rightarrow (\psi \rightarrow \varphi))$
  2. $((\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi)))$
  3. $((\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi))$
- Es gibt nur eine Inferenzregel, den *Modus Ponens*:

$$\frac{\varphi, (\varphi \rightarrow \psi)}{\psi}$$

Übungsaufgabe Zeige, dass die Kalkülaxiome tatsächlich Tautologien sind und überlege, warum die Inferenzregel tatsächlich Sinn macht!

Ich zeige als Beispiel, dass $\vdash (A \vee \neg A)$ gilt, also, dass die Formel $(A \vee \neg A)$ (ohne zusätzliche Axiome) beweisbar ist:

1. Nach unserer Abkürzung ist $(A \vee \neg A) = (\neg A \rightarrow \neg A)$, wir müssen also zeigen, dass diese Formel beweisbar ist.
2. Nach Axiom 1 gilt mit $\varphi = \neg A$ und $\psi = (\neg A \rightarrow \neg A)$:
$$\vdash (\neg A \rightarrow ((\neg A \rightarrow \neg A) \rightarrow \neg A))$$
3. Nach Axiom 2 gilt mit $\varphi = \neg A, \psi = (\neg A \rightarrow \neg A)$ und $\chi = \neg A$:
$$\vdash ((\neg A \rightarrow ((\neg A \rightarrow \neg A) \rightarrow \neg A)) \rightarrow ((\neg A \rightarrow (\neg A \rightarrow \neg A)) \rightarrow (\neg A \rightarrow \neg A)))$$

4. Wenden wir den Modus Ponens auf die letzten zwei Formeln an erhalten wir:
$$\vdash (\neg A \to (\neg A \to \neg A)) \to (\neg A \to \neg A))$$

5. Nach Axiom 1 gilt mit $\varphi = \psi = \neg A$:
$$\vdash (\neg A \to (\neg A \to \neg A))$$

6. Wenden wir wieder Modus Ponens auf die letzten zwei Formeln an erhalten wir endlich
$$\vdash (\neg A \to \neg A)$$

Man sieht zweierlei: Zum einen, dass Beweise in dem Kalkül *extrem umständlich und hässlich sind* und zweitens, dass jeder Beweisschritt ausschließlich mit dem Aufbau der Formeln zu tun hat, unabhängig davon, was sie „aussagt", was genau unser Ziel war. Es gibt Kalküle, in denen die Beweisführung deutlich angenehmer ist (z.B. *Systeme natürlichen Schließens/Natural deduction*), die haben aber den großen Nachteil, dass sie üblicherweise deutlich mehr Regeln erfordern. Aber eigentlich ist der Kalkül selbst völlig unwichtig – interessant ist eigentlich nur, dass es überhaupt einen gibt, der folgendes erlaubt:

Satz. *Der Beweiskalkül ist* vollständig*, das heißt: Für jede Menge von Formeln T und Formel φ gilt $T \models \varphi$ genau dann, wenn $T \vdash \varphi$.*

Der Beweis dafür ist etwas aufwendiger und würde den Rahmen sprengen, steht aber auf Wikipedia. Der Vollständigkeitssatz hat aber auch sehr praktische Folgerungen:

Satz 1.1. ***(Kompaktheitssatz der Aussagenlogik)***

1. *Wenn $T \models \varphi$ gilt, dann gibt es bereits eine endliche Teilmenge $T' \subset T$ so, dass $T' \models \varphi$.*

2. *Wenn jede endliche Teilmenge von T erfüllbar ist, dann ist auch T erfüllbar.*

Beweis.

1. Angenommen $T \models \varphi$, dann gilt nach dem Vollständigkeitssatz auch $T \vdash \varphi$; es gibt also einen Beweis, dass φ aus den Axiomen von T folgt. So ein Beweis ist endlich und kann also nur endlich viele Axiome $\varphi_1, ..., \varphi_n$ aus T benutzen. Also $\{\varphi_1, ..., \varphi_n\} = T' \vdash \varphi$ und damit $T' \models \varphi$.

2. Folgt direkt aus dem vorherigen per Kontraposition: Wenn T *nicht* erfüllbar ist, gilt also $T \vdash \bot$, und damit gibt es eine endliche Teilmenge T' so, dass $T' \vdash \bot$. Also gibt es eine nicht-erfüllbare endliche Teilmenge.

□

Letzteres ist unheimlich nützlich, um zu zeigen, dass eine unendliche Formelmenge wirklich eine Theorie ist; und gerade in der Prädikatenlogik kann man damit ziemlich absurde (also interessante) Theorien zusammensetzen.

2 Prädikatenlogik

> *Gottlob Frege:* Von Aristoteles bis Boole, alle Logiker benutzen Syllogismen wie „Sokrates ist ein Mensch". Aber wenn wir die **Mathematik selbst** logisch untersuchen wollen, werden wir mehr brauchen!
> *Bertrand Russell:* Hm... was denn genau?
> *Gottlob Frege:* Wir müssen **Variablen** einführen! Wir müssen Dinge sagen können wie „x ist ein Mensch"... was wahr ist, wenn zum Beispiel x gleich „Russell" ist, aber falsch, wenn es einer dieser drei Kekse hier ist...
> – *Logicomix - An epic search for truth*

Die Aussagenlogik ist (wie bereits gesagt) ziemlich beschränkt, was ihre Aussagekraft betrifft. Nachdem die grundlegenden Objekte, die Aussagenvariablen, bereits als „fertige“ Aussagen mit Wahrheitswert interpretiert werden, können wir nur analysieren was passiert, wenn wir Aussagen zu komplexeren Aussagen zusammensetzen. Als Basis für die gesamte Mathematik reicht das natürlich nicht; wir brauchen eine Sprache, die mächtig genug ist um mehr oder minder jeden mathematische Sachverhalt ausdrücken zu können, wie zum Beispiel *Es gibt unendlich viele Primzahlen*, oder *Zu jeder reellen Zahl $a \neq 0$ gibt es eine reelle Zahl b so, dass $a \cdot b = 1$.*

Ein grundlegendes Problem, das sich dabei ergibt ist, dass es natürlich viele verschiedene Bereiche gibt, über die wir reden können wollen – Zahlen, Funktionen, Knoten innerhalb eines Graphen, geometrische Objekte... unsere Sprache muss also sehr flexibel sein. Außerdem gibt es natürlich Sätze, die in manchen Bereichen wahr sind, und in anderen wiederum falsch! Der Satz *Für je zwei Zahlen a, b mit $a < b$ gibt es eine dritte Zahl c mit $a < c < b$* ist zum Beispiel wahr, wenn wir rationale oder reelle Zahlen betrachten. Wenn wir aber nur von ganzen Zahlen reden ist er falsch - Es gibt zwischen 2 und 3 keine ganze Zahl. Die Sprache muss also nicht nur sehr flexibel sein, sondern wenn wir die Semantik betrachten müssen wir auch sicherstellen können, dass ein Satz sich nur auf eine bestimmte Menge von Objekten beziehen soll, und nicht auf andere. Dazu müssen wir zunächst klären, was *mathematische Strukturen* eigentlich sind.

1 Konstanten, (innere) Funktionen, Relationen, Strukturen

Sei M irgendeine Menge, zum Beispiel $M = \mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$. Was können wir dann über diese Menge aussagen? Sie ist zum Beispiel unendlich groß, aber uns interessieren ja nicht nur die Zahlen selbst, sondern unter anderem auch, was wir mit ihnen so machen können – wir können sie zum Beispiel addieren, multiplizieren, bezüglich ihrer Größe vergleichen etc. Aus Sicht der Logik bedeutet das, wir wollen die Menge mit einer *Struktur* $(\mathbb{Z}, +, \cdot, <)$ versehen, die uns mehr über unsere Menge verrät als nur, welche Objekte sie enthält. Eine Struktur ist hier ein Tupel[9] bestehend aus einer Menge (dem *Universum* der Struktur) und beliebig vielen *inneren Funktionen* (oder *Verknüpfungen*) und *Relationen* auf dieser Menge. Die Objekte unserer Menge nennen wir *Konstanten.*

Definition 2.1. Sei M eine beliebige Menge.

- Die Elemente $a \in M$ heißen *Konstanten.*
- Eine *n-stellige innere Funktion f* auf M ist eine Funktion, die n Elemente aus M auf *ein* Element aus M abbildet. Die Funktion muss dafür wohldefiniert sein, das heißt, für je n beliebige Konstanten $a_1, ..., a_n \in M$ muss ein Funktionswert $f(a_1, ..., a_n)$ existieren, eindeutig bestimmt sein und in M liegen.
- Eine *n-stellige Relation R* auf M (auch *Prädikat* genannt) ist eine Eigenschaft von Tupeln von Elementen $a_1, ..., a_n \in M$ so, dass $R(a_1, ..., a_n)$ entweder „wahr“ ist oder „falsch“, bzw. R auf jedes Tupel $(a_1, ..., a_n)$ entweder zutrifft oder nicht.
- Eine *mathematische Struktur* ist ein Tupel bestehend aus einer Menge M und einer beliebigen Anzahl von inneren Funktionen und Relationen auf M.

Eine Funktion f, die jedes Tupel aus n beliebigen Elementen einer Menge A auf m Elemente aus einer Menge B abbildet bezeichnet man in der Mathematik mit $f : A^n \to B^m$. Die Definition einer n-stelligen inneren Funktion ließe sich also auch kurz so formulieren:

Eine *n-stellige innere Funktion M* ist eine Funktion $f : M^n \to M$.

[9] Ein *Tupel* ist eine endlich lange, geordnete Folgen von Objekten. Also sowas wie (a, b, c, d) oder $(1, 2, 3, ..., 17403)$. Ein Tupel der Länge 2 wird (vernünftigerweise) auch einfach „Paar“ genannt ;-)

Diese Definitionen sind zugegebenermaßen bereits sehr abstrakt; deswegen betrachten wir ein paar Beispiele:

- Die Addition $+$ und die Multiplikation $\cdot$ sind zweistellige innere Funktionen auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Sie sind auch innere Funktionen auf *manchen, aber nicht allen* Teilmengen davon: Betrachte zum Beispiel $M = \{0, 2, 4, 6, ...\}$ die Menge der geraden Zahlen. Die Summe zweier gerader Zahlen ist wieder gerade, genauso wie das Produkt zweier gerader Zahlen. $+$ und $\cdot$ sind also innere Funktionen auf M. Sei umgekehrt $M' = \{1, 3, 5, 7, ...\}$ die Menge der ungeraden Zahlen - das Produkt zweier ungerader Zahlen ist wieder ungerade, wodurch $\cdot$ eine innere Funktion auf M' darstellt; die Summe zweier ungerader Zahlen ist jedoch gerade! Das bedeutet $+$ ist keine innere Funktion $M'^2 \to M'$ und somit ist $(M', +)$ keine mathematische Struktur – $(M', \cdot)$ dagegen schon.

- Auf den rationalen Zahlen $\mathbb{Q}$ ist die Funktion x^{-1} eine einstellige innere Funktion, weil für jede rationale Zahl q die Zahl q^{-1} auch wieder rational ist. Genauso ist die Exponentialfunktion e^x eine einstellige innere Funktion auf den reellen Zahlen $\mathbb{R}$, jedoch nicht auf den rationalen Zahlen, da zum Beispiel e^1 irrational ist, also nicht in $\mathbb{Q}$ liegt. Damit sind $(\mathbb{Q}, x^{-1}), (\mathbb{R}, x^{-1})$ und $(\mathbb{R}, e^x)$ Strukturen, aber $(\mathbb{Q}, e^x)$ nicht.

- Die Funktion $\sqrt{x}$ ist eine einstellige innere Funktion auf den komplexen Zahlen $\mathbb{C}$, aber nicht auf $\mathbb{R}$, da wir aus negativen reellen Zahlen keine Wurzel ziehen können. Aus positiven dagegen schon - nennen wir die positiven reellen Zahlen $\mathbb{R}^+$, dann sind also $(\mathbb{C}, \sqrt{x})$ und $(\mathbb{R}^+, \sqrt{x})$ Strukturen, aber $(\mathbb{R}, \sqrt{x})$ nicht.

- $<$ ist eine zweistellige Relation auf den Zahlenräumen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Für je zwei Zahlen a, b ist schließlich $a < b$ entweder wahr oder nicht, also ist zum Beispiel $(\mathbb{Q}, <)$ eine Struktur. Relationen sind außerdem immer auch Relationen auf allen Teilmengen, das heißt für jede Teilmenge $M \subset \mathbb{R}$ ist auch $(M, <)$ eine Struktur.

- Ein *ungerichteter Graph* ist eine Menge von Punkten (*Knoten* genannt), die je paarweise durch eine *Kante* verbunden sind oder nicht. Wir können die Knoten als Universum M einer Struktur nehmen und die Kanten in Form einer zweistelligen Relation R beschrieben – für zwei Knoten a, b heißt dann $R(a, b)$, dass a und b mit einer Kante verbunden sind. **Definition:** Ein ungerichteter Graph ist eine Menge M mit einer zweistelligen *symmetrischen* Relation R. Das heißt, dass für alle $a, b \in M$ gilt: $R(a, b)$ trifft zu genau dann, wenn auch $R(b, a)$ zutrifft.
  Nachdem jede Relation auf jeder Teilmenge wieder eine Relation darstellt folgt daraus: *Jede Teilmenge eines ungerichteten Graphen ist wieder ein ungerichteter Graph.*

- Die Eigenschaft „*x ist prim*“ lässt sich als einstellige Relation P auf $\mathbb{N}$ darstellen. Es soll also gelten $P(n)$ genau dann, wenn n eine Primzahl ist. Damit ist $(\mathbb{N}, P)$ eine Struktur.

- Aus all dem folgt, dass z.B. $(\mathbb{R}, +, \cdot, <, e^x)$ oder $(\mathbb{N}, +, \cdot, <, P)$ Strukturen sind.

- Sei $M = \{Papier, Stein, Schere\}$ und $\succ$ die zweistellige Relation, die sagt, wer gegen wen gewinnt, also: $Papier \succ Stein, Stein \succ Schere, Schere \succ Papier$. Dann ist also $(M, \succ)$ eine Struktur.

- Zu jeder n-stelligen Funktion f gibt es eine $(n + 1)$-stellige Relation R_f, indem wir definieren: $R_f(a_1, ..., a_{n+1})$ trifft zu genau dann, wenn $f(a_1, ..., a_n) = a_{n+1}$. So erhalten wir zum Beispiel die Relation R_+, für die $R_+(2, 4, 6), R_+(1, 1, 2), R_+(7, 3, 10)$ jeweils wahr sind, aber zum Beispiel $R_+(2, 1, 1)$ falsch.

Jede Form von Mathematik beschäftigt sich letztenendes nur mit bestimmten Strukturen, den Gesetzen, denen diese gehorchen und den Beziehungen *zwischen* solchen Strukturen.

Häufig werden auch Konstanten mit in die Struktur aufgenommen, um zum Beispiel darauf hinzuweisen, dass diese Konstanten besondere Eigenschaften haben. Dies wird sinnvoll, wenn wir Definitionen durchführen wollen, bei denen wir möglichst wenig über das Universum einer Struktur aussagen wollen, aber fordern, dass bestimmte Konstanten existieren sollen. Beispiel:

Definition. Ein *punktierter ungerichteter Graph* ist eine Struktur (M, R, e) so, dass R eine zweistellige symmetrische Relation ist (also $R(a, b)$ gilt genau dann, wenn auch $R(b, a)$ gilt) und $e \in M$ eine Konstante ist mit der Eigenschaft, dass für jedes $a \in M$ gilt $R(a, e)$ (also jeder Knoten ist mit e verbunden).

Definition. Eine *Gruppe* ist eine Struktur $(M, \circ, e)$ so, dass $\circ$ eine zweistellige assoziative Funktion auf M ist (also so, dass gilt: $a \circ (b \circ c) = (a \circ b) \circ c$), für jedes $a \in M$ gilt $a \circ e = a$ (e ist *neutral*) und für jedes $a \in M$ ein $b \in M$ existiert mit $a \circ b = e$ (jedes Element hat ein *inverses*).

Beispielsweise sind $(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0)$ oder $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ Gruppen (warum?).

Wir erhalten auch noch folgendes schönes Beispiel: Sei F die Menge aller aussagenlogischen Formeln über einer Menge von Aussagenvariablen $\mathcal{V}$. Dann ist $(F, \wedge, \vee, \neg, \rightarrow, \top, \bot, \equiv)$ eine Struktur: $\wedge, \vee, \rightarrow$ sind zweistellige Funktionen, $\neg$ ist eine einstellige Funktion, $\top$ und $\bot$ sind Konstanten und $\equiv$ ist eine zweistellige Relation auf F.

2 Signaturen

Wie wir gesehen haben gibt es sehr viele verschiedene Strukturen; selbst wenn das Universum das gleich ist. Unsere Sprache muss also flexibel genug sein, um damit umgehen zu können. Die Idee hinter der Prädikatenlogik ist die: Wir werden abhängig von der Struktur, die wir betrachten, für Funktionen, Relationen und Konstanten jeweils individuelle Symbole und zusätzlich noch Variablen einführen. Mit denen können wir dann Terme bilden (wie z.B. $7 \cdot (3 + 17x)$) und Aussagen über diese Terme bilden (wie z.B. $3 + 5 > 7$). Außerdem werden wir *Quantoren* einführen, die es uns erlauben, mit Hilfe von Variablen Dinge zu sagen wie „Es gibt (mindestens) ein Element x (des Universums) für das gilt...“ und „Für alle Elemente (unseres Universums) gilt...“. Das ist dann tatsächlich ausreichend um (nahezu) jeden mathematischen Sachverhalt als Formel auszudrücken!

Die benötigte sprachliche Flexibilität erreichen wir durch sogenannte *Signaturen*. Wenn wir Formeln der Prädikatenlogik definieren wollen, wird die zugrundeliegende Syntax (oder Grammatik, wenn man so will) immer die gleiche bleiben; je nachdem, was für Strukturen wir betrachten wollen, werden wir jedoch unterschiedliche Signaturen benutzen. Eine Signatur ist dabei nur eine Menge von *prinzipiell bedeutungslosen Symbolen* - allerdings mit einer vorher festgelegten Stelligkeit. Genauer:

Definition 2.2. Eine *Signatur (der Prädikatenlogik erster Stufe)* ist eine Menge L von Symbolen. Jedes Symbol hat einen von drei Typen. Es gibt:

- Konstantensymbole
- Funktionssymbole einer bestimmten Stelligkeit $n \in \mathbb{N}$
- Relationssymbole einer bestimmten Stelligkeit $n \in \mathbb{N}$.

Wir brauchen diese Symbole, um Formeln der Prädikatenlogik definieren und aufstellen zu können. Die Semantik funktioniert dann so, dass wir jedem Konstanten-/Funktions-/Relationssymbol eine Konstante/Funktion/Relation einer bestimmten Struktur zuordnen. Es ist jedoch wichtig, zwischen Symbolen und ihren Interpretationen zu unterscheiden! Ein zweistelliges Funktionssymbol ist *nur ein Symbol*, und nicht das selbe wie eine konkrete zweistellige Funktion! Das selbe gilt für Konstanten und Relationen. Wir können zum Beispiel bald die folgende prädikatenlogische Formel aufstellen:

$$\overline{2}\overline{+}\overline{3}\overline{<}\overline{7}$$

Dabei sollen $\overline{2}, \overline{3}, \overline{7}$ Konstantensymbole, $\overline{<}$ ein zweistelliges Relationssymbol und $\overline{+}$ ein zweistelliges Funktionssymbol sein. Wir dürfen diese nicht verwechseln mit den Konstanten $2, 3, 7$, der Relation $<$ und der Funktion $+$! Die Formel wäre natürlich in der Struktur $(\mathbb{N}, 2, 3, 7, <, +)$ wahr - in der Struktur $(\mathbb{R}, 7.315, \frac{7}{4}, 0.00001, =, \cdot)$ dagegen würde die gleiche Formel interpretiert werden als die Behauptung

$$7.315 \cdot \frac{7}{4} = 0.00001$$

, was offensichtlich falsch ist.

Es macht natürlich vollkommen Sinn, die Symbole die man verwendet so zu wählen, dass sie einem Aufschluss darüber geben, für welche konkreten Konstanten/Funktionen/Relationen sie eigentlich stehen sollen, und in der Praxis führt niemand ein eigenes Symbol $\overline{+}$ ein, wenn dieses Symbol letztenendes eh nur für die übliche Addition $+$ stehen soll – man muss sich also, sobald man sicher mit Formeln umgehen kann, keine Gedanken mehr über den Unterschied zwischen Symbolen und ihren Interpretationen machen. Bevor man einen sicheren Umgang hat, sollte man aber schärfstens aufpassen, Symbole und Interpretationen nicht zu verwechseln - sonst läuft man schnell Gefahr, manche Formeln als Tautologien anzusehen, weil sie „offensichtlich wahr“ zu sein scheinen, in Wirklichkeit aber die Symbole völlig anders interpretiert werden können, so dass die Formel in dieser Interpretation schlicht falsch ist. Das Problem ist eben, dass in obigem Beispiel für die Signatur $L = (\overline{2}, \overline{3}, \overline{7}, \overline{<}, \overline{+})$ sowohl $(\mathbb{N}, 2, 3, 7, <, +)$ als auch $(\mathbb{R}, 7.315, \frac{7}{4}, 0.00001, =, \cdot)$ sogenannte *L-Strukturen* sind:

Definition 2.3. Sei L eine Signatur. Eine *L-Struktur* ist eine Struktur $\mathfrak{A}$, die

- für jedes Konstantensymbol $c \in L$ genau eine Konstante $c^{\mathfrak{A}}$ enthält.
- für jedes n-stellige Funktionssymbol $f \in L$ genau eine n-stellige innere Funktion $f^{\mathfrak{A}}$ enthält und
- für jedes n-stellige Relationssymbol $R \in L$ genau eine n-stellige Relation $R^{\mathfrak{A}}$ enthält.

Wir bezeichnen also für eine Struktur $\mathfrak{A}$ die konkrete Interpretation eines Symbols z mit $z^{\mathfrak{A}}$. In dem obigen Beispiel mit $L = (\overline{2}, \overline{3}, \overline{7}, \overline{<}, \overline{+})$ und den Strukturen $\mathfrak{N} = (\mathbb{N}, 2, 3, 7, <, +)$ und $\mathfrak{R} = (\mathbb{R}, 7.315, \frac{7}{4}, 0.00001, =, \cdot)$ hätten wir also:

$$\overline{2}^{\mathfrak{N}} = 2, \overline{3}^{\mathfrak{N}} = 3, \overline{7}^{\mathfrak{N}} = 7, \overline{<}^{\mathfrak{N}} = <, \overline{+}^{\mathfrak{N}} = +$$

und

$$\overline{2}^{\mathfrak{R}} = 7.315, \overline{3}^{\mathfrak{R}} = \frac{7}{4}, \overline{7}^{\mathfrak{R}} = 0.00001, \overline{<}^{\mathfrak{R}} = „=“, \overline{+}^{\mathfrak{R}} = \cdot$$

(Ja, ich muss zugeben, sowas wie „$\overline{+}^{\mathfrak{R}} = \cdot$“ sieht schon gewaltig seltsam aus... lässt sich aber schwer vermeiden :-/)

Der Knackpunkt ist also: Sobald wir eine Signatur L festgelegt haben, um über eine bestimmte Struktur zu reden, müssen wir immer berücksichtigen, dass es auch völlig andere L-Strukturen geben kann, in denen die selben Formeln also auch völlig unterschiedlich interpretiert werden können/müssen.

3 Syntax - Terme

Bevor wir definieren können, was jetzt Formeln der Prädikatenlogik eigentlich genau sein sollen, müssen wir erstmal definieren, was eigentlich *Terme* sind. Beispiele für Terme sind

$$5+3 \qquad 17x^2-4y \qquad \int e^{17x}dx$$

...also mathematische Ausdrücke, die sich irgendwie „berechnen" lassen so, dass wir eine Konstante erhalten. Terme sind natürlich wichtig, weil wir ohne sie Formeln wie $a+b \geq a$ gar nicht ausdrücken können.

Es hat sich bei Termen (und Formeln auch) durchgesetzt, in der formalen Definition die *polnische Notation* zu verwenden. Diese funktioniert und begründet sich folgendermaßen:

Wenn wir die Terme $a+b, -3, (7+3)\cdot(4+(-x))$ und x^{-1} betrachten, rennen wir in folgendes Problem: $+$ und $\cdot$ sind zweistellige Funktionssymbole, $^{-1}$ könnte man als einstelliges Funktionssymbol betrachten und $-$ ebenfalls.[10] Aber wenn wir uns die Schreibweise anschauen und darauf achten, auf welche Objekte diese Funktionssymbole angewandt werden stellen wir fest: Bei $a+b$ und $7+3$ steht das Funktionssymbol $+$ *zwischen* den Objekten a, b bzw. $7, 3$. Bei x^{-1} steht das Funktionssymbol *hinter* dem Objekt x und bei -3 und $(-x)$ steht das Funktionssymbol $-$ *vor* den Objekten 3 bzw. x. Das ist irgendwie uneinheitlich und entsprechend unpraktisch. Außerdem brauchen wir bei $(7+3)\cdot(4+(-x))$ drei Klammerpaare, damit noch klar ist, welches Funktionssymbol sich jetzt auf welche Objekte bzw. Teilterme bezieht. Das ist auch irgendwie nicht so ganz befriedigend.

Die polnische Notation vermeidet all das - sie ist einheitlich und kommt komplett ohne Klammern aus. Dadurch ist sie sehr angenehm, um Terme formal zu untersuchen, insbesondere für z.B. einen Computer. Sie hat aber den Nachteil, dass sie etwas gewöhnungsbedürftig ist und nicht gerade angenehm zu lesen ist, wenn man kein Computerprogramm ist. Die Idee hinter der polnischen Notation ist die:

Wir wissen, was ein Funktionssymbol und was eine Variable oder ein Konstantensymbol ist. Außerdem wissen wir, welche Stelligkeit jedes Funktionssymbol hat, also ob die entsprechende Funktion einen, zwei oder 17 Parameter braucht. Es spricht also nichts dagegen, einfach das Funktionssymbol ganz an den Anfang zu setzen und die Parameter einfach dahinter zu schreiben. Aus dem Term $a+b$ wird damit $+ab$. Praktischerweise funktioniert das auch, wenn wir Funktionssymbole miteinander verketten: Nachdem die Parameter immer *nach* dem dazugehörigen Funktionssymbol kommen, können wir z.B. den Term $(a+(-b))$ so als $+a-b$ schreiben und wissen: das $-$ bezieht sich auf das b und das $+$ bezieht sich auf a und $-b$. Ein Term wie $(7+3)\cdot(4+5\cdot(a+(-9)))$ wird damit zu $\cdot+73+4\cdot5+a-9$, kommt komplett ohne Klammern aus und ist eindeutig (wenn auch hässlich) lesbar.[11] Verwirrend ist hier natürlich, dass aus $7+3$ auf einmal $+73$ wird, was einen dazu verführen könnte, 73 als *eine* Zahl zu lesen statt, wie beabsichtigt, die zwei Zahlen 7 und 3. Für die formale Definition ist das aber unproblematisch - wir gehen einfach davon aus, dass jede Zahl durch genau ein Symbol dargestellt wird statt durch potentiell mehrere Ziffern (Deswegen hab ich in den Termbeispielen auch nur einstellige Zahlen benutzt ;-)).

Wir können natürlich sobald wir Terme (und Formeln) formal definiert haben uns unsere eigenen Konventionen aussuchen, wie wir Terme darstellen. Wie so häufig ist es nur

[10] Mathematiker verabscheuen es, Subtraktion und Division als eigenständige Rechenoperationen zu betrachten. Formal sind sie das auch nicht: $2-5$ ist definitionsgemäß nur die Addition $2+(-5)$ und die Division 7%4 ist nur eine Multiplikation, nämlich $7\cdot\frac{1}{4}$ bzw. $7\cdot4^{-1}$, und $\frac{1}{4}$ bezeichnet eine eigenständige Zahl, keine Rechnung. Damit erledigt sich auch das ganze „Durch 0 teilen"-Problem: Ein Bruch $\frac{7}{0}$ ist schlicht nicht definiert, weil die Zahl $\frac{1}{0}$ nicht existiert.

[11] Terme in der polnischen Notation werden übrigens deutlich einfacher lesbar, wenn man von rechts nach links liest!

wichtig, dass wir prinzipiell „unsere“ Terme so umschreiben können, dass sie der polnischen Notation und somit der formalen Termdefinition entsprechen. Also legen wir los. Die Definition von Termen wird – wie schon die Definition aussagenlogischer Formeln, und die Definition prädikatenlogischer Formeln später auch – rekursiv gemacht:

Definition 2.4. Sei L eine Signatur und $V = \{v_1, v_2, ...\}$ eine Menge von *Variablen* (Also einfach irgendwelchen Symbolen, von denen wir wissen, dass sie Variablen sein sollen). Folgendes *und nur folgendes* ist ein L-Term:

- Jede Variable $v \in V$ ist ein L-Term.
- Jedes Konstantensymbol $c \in L$ ist ein L-Term.
- Sei $f \in L$ ein n-stelliges Funktionssymbol und $t_1, ..., t_n$ beliebige L-Terme, dann ist auch $ft_1...t_n$ ein L-Term.

Okay, das üben wir mal – in polnischer Notation, bitte:

Übungsaufgaben Sei $L = (+, \cdot, *, f, a, b, c)$, wobei $+, \cdot$ zweistellige, $*$ einstelliges und f ein dreistelliges Funktionssymbol ist und a, b, c Konstantensymbole. Außerdem seien x, y, z Variablen. Welche der folgenden Ausdrücke sind L-Terme?

1. fa
2. $faaa$
3. $*ab$
4. $fa * ab$
5. $\cdot + xya$
6. $*fxyab$
7. $\cdot + *faaaaa$

Schreibe folgende Terme in die polnische Notation um. Denk dir gegebenenfalls neue Funktionssymbole (z.B. für das „hoch“-rechnen) aus:

1. $17 + x^2$
2. $7^{3a} - \frac{2}{3}$
3. $a^2 + 2ab + b^2$
4. $(a + b) \cdot (c^{2+x} - 4)$

4 Syntax - Formeln

Jetzt wo wir Terme haben können wir auch endlich prädikatenlogische Formeln definieren. Wie bereits angekündigt ist auch diese Definition wieder rekursiv:

Definition 2.5. Sei L eine Signatur und V eine Menge von Variablen. Folgendes *und nur folgendes* ist eine L-Formel:

- Seien t_1 und t_2 L-Terme, dann ist $t_1 \doteq t_2$ eine L-Formel
- Seien $t_1, ..., t_n$ L-Terme und $R \in L$ ein n-stelliges Relationssymbol, dann ist $Rt_1...t_n$ eine L-Formel

(Formeln der Form $t_1 \doteq t_2$ bzw. $Rt_1...t_n$ heißen auch *Primformeln*

- Ist φ eine beliebige L-Formel, so ist auch $\neg\varphi$ eine L-Formel.
- Sind φ, ψ beliebige L-Formeln, dann ist auch $(\varphi \wedge \psi)$ eine L-Formel.
- ist φ eine Formel und $x \in V$ eine Variable, dann ist auch $\exists x\varphi$ („Es existiert (mindestens) ein x so, dass φ") eine L-Formel.

Auch hier haben wir in der Definition wieder die polnische Notation benutzt (da wir Relationszeichen *vor* den dazugehörigen Termen fordern: $Rt_1...t_n$). Wieder ist das in der Praxis insofern egal, dass wir ja „wissen", dass mit $a > b$ natürlich technisch gesehen die Formel $> ab$ gemeint wäre. Wichtig ist wieder nur, dass wir wissen, was gemeint ist, und wir entsprechend auch wissen, wie wir „unsere" Formel in eine echte, der Definition gemäßen Formel unschreiben.

Das Symbol $\exists$ heißt *Existenzquantor*, und hierin steckt eigentlich die große Ausdrucksstärke der Prädikatenlogik - mit ihm sind wir nicht mehr nur in der Lage, über konkrete Objekte zu sprechen, sondern wir können nun auch die Existenz von bestimmten Objekten behaupten. Und er erlaubt uns auch, auszusagen, dass irgendeine Eigenschaft auf *alle* Objekte eines Universums zutrifft: Wir definieren den *Allquantor* $\forall$ als Abkürzung $\forall v\varphi = \neg\exists v\neg\varphi$ – nachdem die Behauptung „Für alle v gilt φ" das Gleiche ist wie zu behaupten „Es gibt kein v so, dass *nicht* φ gilt".

Wir haben von den bereits bekannten aussagenlogischen Symbolen in der Definition nur $\neg$ und $\wedge$ benutzt - es gelten aber nach wie vor die gleichen Äquivalenzumformungen wie in der Aussagenlogik. Wir können also genauso wieder die Symbole $\vee, \rightarrow, \leftrightarrow$ benutzen, indem wir sie als Abkürzungen der Form $(\varphi \vee \psi) = \neg(\neg\varphi \wedge \neg\psi)$ etc. definieren.

Aus formalen Gründen haben wir in der Definition der ersten Primformel das Symbol $\doteq$ benutzt. Das liegt daran, dass wir unterscheiden wollen zwischen einer Gleichheit der Form $2 + 3 = 5$ und einer Formelbezeichnung wie $\varphi = a < b$. Der Ausdruck $2 + 3 = 5$ ist ja eine Formel, und dieser Formel könnten wir einen Namen geben wollen, wie eben zum Beispiel φ. Dann müssten wir aber schreiben $\varphi = 2 + 3 = 5$, was verwirrend würde, da man nun auch meinen könnte, dass $\varphi = 2 + 3$ ist, und somit $\varphi = 5$. Das war aber gar nicht unsere Absicht! Daher benutzen wir innerhalb von prädikatenlogischen Formeln das Symbol $\doteq$, womit wir nun unmisverständlich schreiben können $\varphi = 2 + 3 \doteq 5$.

Übungsaufgaben Sei $L = (+, \cdot, -, 0, 1, <)$ eine Signatur mit den üblichen Stelligkeiten (also $+$ ist zweistelliges Funktionszeichen, $-$ einstelliges, 0 ist Konstantensymbol etc.). Welche der folgenden Ausdrücke sind Formeln? (Terme sind in polnischer Notation)

An der Stelle ist es vermutlich sinnvoll, mal eine ernstzunehmende mathematische Aussage in der Prädikatenlogik auszudrücken. Nehmen wir den Satz „Es gibt unendlich viele Primzahlen". Wir nehmen dafür die Signatur $L = (+, \cdot, 1)$ (mehr brauchen wir tatsächlich nicht) und die Struktur $(\mathbb{N}, +, \cdot, 1)$. Wir sind also so dreist und unterscheiden nicht zwischen dem Symbol $+$ und der Funktion $+$, oder dem Symbol 1 und der Konstante 1.

Überlegen wir zuerst, was eigentlich eine Primzahl ist: Nämlich eine Zahl, die nur durch 1 und sich selbst teilbar ist (mit Außnahme der 1 selbst). Wir können mit dem Existenzquantor ausdrücken, dass eine Zahl a durch eine Zahl b teilbar ist, nämlich indem wir sagen: *Es gibt eine Zahl x so, dass $b \cdot x = a$ gilt*, also $\exists x\ b \cdot x \doteq a$. Der Satz *$x$ ist eine Primzahl* lässt sich somit ausdrücken als $x \neq 1$ *und für alle w, z gilt: Wenn $w \cdot z = x$, dann ist entweder $w = 1$ oder $z = 1$*, also:

$$\neg x \doteq 1 \wedge \forall w \forall z\ (w \cdot z \doteq x \rightarrow (w \doteq 1 \vee z \doteq 1))$$

Geben wir dieser Formel einen Namen - nämlich $P(x)$. Wir verstehen dann unter der Formel $P(a)$: „Die Formel, die entsteht, wenn wir in der Formel $P(x)$ die Variable x durch a ersetzen" (Mehr zum Ersetzen von Variablen später - da muss man ein paar Dinge beachten, die aber gerade unwichtig sind).

Jetzt können wir also von Zahlen behaupten, dass sie prim sind. Eine Möglichkeit, jetzt zu behaupten, dass es unendlich viele Primzahlen gibt, ist zu sagen, dass es zu jeder Zahl n eine Primzahl p gibt, die größergleich n ist. Dann folgt sofort, dass es unendlich viele geben muss. Dafür müssen wir nur rausfinden, wie wir „größergleich" ausdrücken können. Das ist aber gar kein Problem: a ist kleinergleich b genau dann, wenn es eine Zahl c gibt so, dass $a + c = b$. Wir drücken also x *ist kleinergleich* y aus als:

$$\exists z \; x + z \doteq y$$

und nennen diese Formel $K(x, y)$. Die Aussage *Zu jeder Zahl gibt es eine größere Primzahl* wird dann also:

$$\forall x \exists y \; (K(x, y) \wedge P(y))$$

...was eben eine Kurzschreibweise ist für:

$$\forall x \exists y \; (\exists z \; x + z \doteq y \wedge \neg y \doteq 1 \wedge \forall w \forall z \; (w \cdot z \doteq y \rightarrow (w \doteq 1 \vee z \doteq 1)))$$

Diese Formel ist also endlich gleichbedeutend mit *es gibt unendlich viele Primzahlen* - aber natürlich nur, wenn wir sie in der Struktur $(\mathbb{N}, +, \cdot, 1)$ interpretieren! In einer anderen Struktur sagt die Formel natürlich was völlig anderes aus.

Diese Formel mag aufwendig wirken, und sie aufzustellen mag einiges an Geistesleistung brauchen – das ist aber lediglich Gewöhnungssache. Ähnlich wie z.B. beim Programmieren hat man mit genug Übung irgendwann den Kniff raus, wie man eine alltagssprachliche mathematische Aussage in einer Formel ausdrückt, ohne dass man noch viel nachdenken müsste – insbesondere wenn man genug „Abkürzungen" kennt.

Übungsaufgaben Sei $L = (\circ, *, n, e)$ Drücke die folgenden Aussagen als L-Formel (interpretiert in der Struktur $(\mathbb{N}, +, \cdot, 0, 1)$) aus.[12]

1. Für jede Zahl x gilt $0 + x = x$.
2. Es gibt keine Zahl x so, dass nicht $0 \cdot x = 0$ ist.
3. Es gibt eine Zahl $x \neq 2$, die durch 2 teilbar ist.
4. Es gibt unendlich viele Zahlen, die durch 2 teilbar sind.[13].
5. Es gibt eine Primzahl, die durch 2 teilbar ist.
6. Es gibt *genau eine* Primzahl, die durch 3 teilbar ist.

5 Freie und gebundene Variablen, Variablensubstitution

In dem obigen Beispiel haben wir in der Formel $P(x) = \neg x \doteq 1 \wedge \forall w \forall z \; (w \cdot z \doteq x \rightarrow (w \doteq 1 \vee z \doteq 1))$ an einer Stelle einfach das x durch ein y ersetzt. Das machte Sinn, da die Formel übersetzt nur sagt „x ist eine Primzahl" und x als Variable nicht näher bestimmt war. Nachdem x eine Variable ist, erhalten wir erst einen gültigen *Satz*, der tatsächlich wahr oder falsch ist, wenn wir für x eine feste Zahl einsetzen. Man sagt dafür „Die Variable x ist *frei* in P(x)". Wir können aber auch anderweitig aus $P(x)$ einen Satz machen, nämlich indem wir die Variable x durch einen Quantor *binden*, also wir die Formel $\exists x \; P(x)$ („Es existiert eine Primzahl") oder $\forall x \; P(x)$ („Alle Zahlen sind prim") bilden. Also:

[12] Denke daran, dass ich z.B. die Zahl 3 auch als 1+1+1 darstellen kann - bzw. in der Signatur als $e \circ e \circ e$!

[13] Denke an das obige Beispiel, dass es unendlich viele Primzahlen gibt

Definition 2.6. Sei x eine Variable und φ eine Formel.

- x heißt *gebunden* in φ, wenn sie eine Teilformel der Form $\exists x \psi$ oder $\forall x \psi$ enthält.
- x heißt *frei* in φ, wenn es eine Teilformel ψ gibt so, dass x in ψ vorkommt, x in ψ nicht gebunden ist und φ keine Teilformel der Form $\exists x \psi'$ (oder $\forall x \psi'$) hat, bei der ψ eine Teilformel von ψ' ist.
- φ heißt *Satz*, wenn φ keine freien Variablen enthält.
- Ein Formel, die freie Variablen enthält, heißt auch *Prädikat*.

Auch diese Definitionen sind wieder nicht so ganz einfach, daher schauen wir sie uns jetzt mal mit ein paar Beispielen genauer an. Ein Satz ist eine vollständige Formel, der man in einer Struktur einen festen Wahrheitswert zuordnen kann - unser $P(x)$ von oben ist also kein Satz, sondern ein Prädikat. $P(2), P(5), P(6)$ etc. dagegen sind tatsächlich Sätze, genauso wie $\exists x\ P(x)$ und $\forall x\ P(x)$.

Aus den ersten beiden Definitionen folgt, dass eine Variable in einer Formel *sowohl* frei *als auch* gebunden sein kann: Betrachten wir zum Beispiel die Formel $\forall x\ x \geq 0 \wedge x \geq 5$. Die Formel besteht aus zwei (echten)[14] Teilformeln, nämlich $\forall x\ x \geq 0$ (in der die Variable x gebunden ist) und $x \geq 5$ (in der die Variable frei ist). Die Formel enthält also die Variable x einmal gebunden und einmal frei.

In der Praxis ist das natürlich eigentlich unsinnig - nachdem Variablen nur bedeutungslose Symbole sind, kann ich beliebig viele verschiedene Variablen benutzen. Es wäre also dämlich, eine Formel $\forall x\ x \geq 0 \wedge x \geq 5$ aufzustellen, wenn ich sie genausogut als $\forall x\ x \geq 0 \wedge y \geq 5$ oder $\forall y\ y \geq 0 \wedge x \geq 5$ aufstellen kann. Aussagen tun sie eh alle das selbe, also warum die verwirrendere Option nehmen, wenn ich genug Variablen zur Verfügung habe? Rein definitorisch verbietet mir aber niemand, die Formel $\forall x\ x \geq 0 \wedge x \geq 5$ aufzustellen – das ist schließlich per Definition eine gültige Formel, und wollte man Formeln so definieren, dass wir derartigen Unsinn *nicht* machen dürften, würde die Definition plötzlich seeehr aufwendig, und das will ja auch niemand!

Der Clou ist nun, dass Prädikate (also Formeln mit freien Variablen) nicht wirklich als wahr oder falsch interpretiert werden können, wenn wir die Variablen nicht durch irgendwelche konkreten Konstanten (oder Terme ohne Variablen) ersetzen – umgekehrt sind gebundene Variablen für die Interpretation wichtig und dürfen somit nicht einfach ersetzt werden. Wir brauchen also die Unterscheidung zwischen gebundenen und freien Variablen, damit wir sinnvoll Variablen ersetzen können.

Definition 2.7. (Substitution) Sei φ eine L-Formel mit freier Variable x und t ein L-Term, in dem *keine Variable vorkommt, die in φ gebunden ist.* Wir bezeichnen mit $\varphi\left[\frac{t}{x}\right]$ die Formel, die entsteht, wenn wir jedes freie Vorkommen der Variable x durch den Term t ersetzen.
Wir schreiben auch $\varphi(x)$ um zu betonen, dass φ die Variable x frei enthält und schreiben $\varphi(t)$ für $\varphi\left[\frac{t}{x}\right]$

Üblicherweise taucht der Nebensatz „in dem keine Variable vorkommt, die in φ gebunden ist“ in der Definition der Variablensubstitution gar nicht auf – das führt aber zu gewissen Problemen, die man dann extra später betonen muss. Ich halte es deshalb für sinnvoll, diesen Fall von vorneherein auszuschließen, da wieder gilt: Wir können so viele unteschiedliche Variablen benutzen wie wir wollen, es gibt also keinen Grund, in den Termen, die wir für Variablen einsetzen die selben Variablen zu benutzen wie die, die in der

[14] Eine *echte* Teilformel ist eine Formel, die nicht die ganze Formel selbst ist. Wollte man „Teilformel“ formal definieren, ergäbe sich, dass jede Formel eine Teilformel von sich selbst ist.

Formel schon auftauchen. Das führt nur zu unsinnigen Spezialfällen, die wir dann später gesondert betrachten müssen und die in der Praxis sowieso vermeidbar sind.

Übungsaufgaben Sei wieder $L = (+, \cdot, -, 0, 1, <)$ und x, y, z, v, w Variablen. In welchen der folgenden Formeln sind welche Variablen frei, welche gebunden und welche kommen sowohl frei als auch gebunden vor?

1. $\forall x\ x < x + y$
2. $\forall x\ x < x + x$
3. $(\forall x\ x < x + y \wedge \exists y\ x \cdot y \doteq x)$
4. $\forall x\ (x < x + y \wedge \exists y\ x \cdot y \doteq x)$
5. $x \doteq y$
6. $\forall x \forall y \forall z\ x + y \doteq w$

6 Semantik

Wir wollen nun formal definieren, wie wir Formeln in einer festen Struktur zu interpretieren haben, also wie Formeln eine Bedeutung erhalten. Das wird wieder etwas kompliziert, aber wir kennen ja zum Glück auch schon ein paar Beispiele, und wir wissen ja hoffentlich mittlerweile prinzipiell, was uns (sinnvolle) Formel mitteilen möchten, daher ist das Folgende in erster Linie der Versuch zu zeigen, dass wir die Bedeutung von Formeln tatsächlich formal definieren können.

Das Problem sind da zunächst mal Prädikate – die enthalten ja diese freien Variablen, die uns scheinbar daran hindern, der Formel einen Wahrheitswert zuzuordnen. Das müssen wir aber, wenn wir wirklich definieren wollen, was es bedeutet, dass eine Formel *wahr* ist. Das gilt auch für Sätze, da die Definition der Interpretation rekursiv sein wird und wir somit Teilformeln von Sätzen, die selbst vielleicht keine Sätze sind, ebenfalls Wahrheitswerte zuordnen können müssen. Insbesondere müssen wir Terme auswerten können, also aus den abstrakten Funktions- und Konstantensymbolen (und eben den Variablen auch) echte Konstanten machen. Beispielsweise müssen wir sicher gehen, dass der Term 2+2 tatsächlich als die Konstante 4 ausgewertet wird. Das tun wir, wie schon in der Aussagenlogik, mit Belegungsfunktionen:

Definition 2.8. Sei V eine Menge von Variablen und $\mathfrak{A}$ eine L-Struktur (für irgendeine Signatur L) mit Universum A. Eine *Belegungsfunktion* ist eine Funktion, die

1. jeder Variable in V eine Konstante aus A zuordnet.
2. jedem Konstantensymbol $z \in L$ seine Interpretation $z^{\mathfrak{A}}$ zuordnet.
3. (rekursiv) jedem Term $ft_1, ..., t_n$ für ein n-stelliges Funktionssymbol $f \in L$ den Funktionswert $f^{\mathfrak{A}}(\beta(t_1), ..., \beta(t_n))$ zuordnet.

Sei $\varphi(x_1, ..., x_n)$ eine L-Formel mit freien Variable $x_1, ..., x_n$, dann bezeichnen wir mit $\varphi[\beta]$ den (jetzt echten) Satz, der entsteht, wenn wir jeden Term t in φ durch seine Auswertung $\beta(t)$ ersetzen.

So können wir also aus jeder Formel einen Satz machen. Man beachte, dass in einer Formel eigentlich nur Konstantensymbole vorkommen dürfen und keine Konstanten selbst, eigentlich ist $\varphi\,[\beta]$ also gar keine L-Formel - aber jede Konstante ist ja letztenendes auch irgendwie ein Symbol, deshalb ist das zunächst mal kein Problem. Das größere Problem ist, dass nicht jede Konstante in unserer Signatur liegen muss! Wir haben schließlich nicht gefordert, dass für $\beta(t)$ auch ein Konstantensymbol $z \in L$ existieren muss. Aber auch das muss uns bei der Semantik nicht stören - uns interessiert ja gerade, wie wir Formeln in einer konkreten Struktur interpretieren können, deswegen kann uns der Unterschied zwischen Konstanten dieser Struktur und den abstrakten Konstantensymbolen herzlichst egal sein. Außerdem ist es nicht mehr schlimm, dass $\varphi\,[\beta]$ keine L(!)-Formel mehr ist, da wir unserer Signatur auch einfach alle Konstanten aus A hinzufügen können und damit auf jeden Fall eine Formel (der neuen Signatur halt) erhalten.

Betrachten wir für Belegungsfunktionen kurz ein Beispiel: Sei unsere Signatur $L = (\circ, *, e, z, d)$, die Struktur $\mathfrak{A} = (\mathbb{N}, +, \cdot, 1, 2, 3)$ und betrachten wir den hässlichen Term $t = * \circ * zzd \circ xe$. Wenn wir das aus der polnischen Notation in die übliche Notation übersetzen, erhalten wir damit $(x \circ e) * ((z * z) \circ d)$. Es gilt:

$$\circ^{\mathfrak{A}} = +, \qquad *^{\mathfrak{A}} = \cdot, \qquad e^{\mathfrak{A}} = 1, \qquad z^{\mathfrak{A}} = 2, \qquad d^{\mathfrak{A}} = 3.$$

Wir müssen also nur der Variable x irgendeinen Wert zuweisen. Sagen wir $\beta(x) = 4$, dann erhalten wir jetzt:

$$\begin{aligned}\beta(t) = \beta((x \circ e) * ((z * z) \circ d)) &= \beta(x \circ e) \cdot \beta((z * z) \circ d) = (\beta(x) + \beta(e)) \cdot (\beta(z * z) + \beta(d)) \\ &= (4 + 1) \cdot ((\beta(z) \cdot \beta(z)) + 3) = 5 \cdot ((2 \cdot 2) + 3) = 5 + 7 = 12\end{aligned}$$

So, jetzt wissen wir also, wie wir aus Prädikaten Sätze machen. Jetzt müssen wir nur noch die Sätze selbst interpretieren. Das passiert (wie so häufig) rekursiv:

Definition 2.9. Sei L eine Signatur, $\mathfrak{A}$ eine L-Struktur mit Universum A und β eine Belegungsfunktion aller Variablen. Wir sagen die L-Formel φ *gilt in* $\mathfrak{A}$ *unter der Belegung* β – und schreiben $\mathfrak{A} \models \varphi\,[\beta]$ – abhängig vom Aufbau von φ:

- Wenn $\varphi = t_1 \doteq t_2$, dann gilt $\mathfrak{A} \models \varphi\,[\beta]$ genau dann, wenn $\beta(t_1) = \beta(t_2)$.
- Wenn $\varphi = Rt_1, ..., t_n$, dann gilt $\mathfrak{A} \models \varphi\,[\beta]$ genau dann, wenn die Relation $R^{\mathfrak{A}}$ auf $\beta(t_1), ..., \beta(t_n)$ zutrifft.
- Wenn $\varphi = \neg\psi$ für eine L-Formel ψ, dann gilt $\mathfrak{A} \models \varphi\,[\beta]$ genau dann, wenn *nicht* $\mathfrak{A} \models \psi\,[\beta]$ gilt.
- Wenn $\varphi = (\psi_1 \wedge \psi_2)$ für zwei L-Formeln ψ_1, ψ_2 ist, dann gilt $\mathfrak{A} \models \varphi\,[\beta]$ genau dann, wenn $\mathfrak{A} \models \psi_1\,[\beta]$ und $\mathfrak{A} \models \psi_2\,[\beta]$ gilt.
- Wenn $\varphi = \exists x\psi$ für eine L-Formel ψ, dann gilt $\mathfrak{A} \models \varphi\,[\beta]$ genau dann, wenn es ein Element $a \in A$ gibt so, dass $\mathfrak{A} \models \left(\psi\left[\frac{a}{x}\right]\right)[\beta]$.[15]

Wir schreiben $\mathfrak{A} \models \varphi$ genau dann, wenn für jede Belegungsfunktion β gilt $\mathfrak{A} \models \varphi\,[\beta]$.

Ich möchte eins kurz anmerken: Es mag irgendwie unsinnig erscheinen, dass wir im Prinzip sagen, dass die Formel Rab wahr ist, wenn „die Relation $R^{\mathfrak{A}}$ auf a und b zutrifft“. Es ist ja gar nicht klar, was eine Relation formal eigentlich überhaupt ist, außer eben etwas, das auf irgendwelche Tupel „zutrifft“ oder nicht, oder was „zutreffen“ entsprechend bedeuten soll! Wir kennen zwar Beispiele für Relationen, aber vielleicht kommt einem das etwas arg geschummelt vor.

Pah! Gar kein Problem – wir können Relationen so formal definieren, dass völlig klar ist, was mit „die Relation trifft zu“ gemeint ist. Allerdings brauchen wir dafür speziellere

[15] Hier ist jetzt wichtig, dass *nur* freie Variablen überhaupt ersetzt werden. Wenn also x nicht frei in φ vorkommt, ändert das $\left[\frac{a}{x}\right]$ einfach gar nichts an φ.

Eigenschaften von Mengen, deswegen komme ich darauf zurück, wenn wir uns Mengen selbst etwas genauer anschauen.[16] Letztenendes ist das allerdings ja eh „nur“ eine semantische Betrachtung - Wenn wir ein Kalkül für die Prädikatenlogik haben, müssen wir uns eh nicht mehr wirklich darum kümmern, wie die Semantik definiert ist.

7 Axiome, Theorien, Modelle

Jetzt wo wir wissen, wie wir Formeln interpretieren können werden wir versuchen, uns (wie bei der Aussagenlogik) wieder von der Semantik zurückzuziehen und alles auf reine Syntax herunterzubrechen. Schließlich brauchen wir ja nicht eine konkrete Struktur zu betrachten, wenn wir es schaffen Axiome zu finden, die die gewünschte Struktur bereits (so weit möglich) eindeutig beschreiben! Dafür brauchen wir allerdings erstmal wieder Theorien, die wir ja aber zum Glück schon aus der Aussagenlogik kennen:

Definition 2.10. Sei L eine Signatur und T eine Menge von L-Sätzen(!).

- Sei $\mathfrak{A}$ eine L-Struktur. Wir schreiben $\mathfrak{A} \models T$ genau dann, wenn für jede Formel $\varphi \in T$ gilt $\mathfrak{A} \models \varphi$. Wir nennen $\mathfrak{A}$ ein *Modell* von T.
- Wir schreiben $T \models \varphi$ („Aus T folgt φ“) für einen L-Satz φ genau dann, wenn für jedes Modell $\mathfrak{A}$ von T gilt $\mathfrak{A} \models \varphi$. Man sagt dafür auch „$\varphi$ ist ein *Theorem* von T“.
- Wir nennen T eine *Theorie* genau dann, wenn sie ein Modell hat. Die Formeln in T nennen wir dann *Axiome*.

> „Ein Mathematiker ist ein Gerät, das Kaffee in Theoreme umwandelt.“
> \- *Paul Erdös*

Traumhaft wäre es jetzt natürlich, wenn wir jede Struktur $\mathfrak{A}$ so durch eine Theorie axiomatisieren könnten, dass diese nur $\mathfrak{A}$ als Modell hat; dann könnten wir jede Struktur durch eine Theorie eindeutig beschreiben und könnten uns entsprechend komplett auf die Syntax von Formeln reduzieren, ohne Strukturen überhaupt noch groß zu betrachten. Leider geht das prinzipiell nur bei endlichen Strukturen – allerdings kommt man bei vielen unendlichen Strukturen auch schon nahe genug ran. Mit Hilfe von Theorien (und Modellen) können wir jetzt immerhin schon einige Definitionen deutlich angenehmer formulieren. Man erinnere sich an die vorherigen Definitionen von Graphen und Gruppen:

Definition.

- Ein *ungerichteter Graph* ist eine Menge M mit einer zweistelligen *symmetrischen* Relation R. Das heißt, dass für alle $a, b \in M$ gilt: $R(a, b)$ trifft zu genau dann, wenn auch $R(b, a)$ zutrifft.
- Ein *punktierter ungerichteter Graph* ist eine Struktur (M, R, e) so, dass R eine zweistellige symmetrische Relation ist (also $R(a, b)$ gilt genau dann, wenn auch $R(b, a)$ gilt) und $e \in M$ eine Konstante ist mit der Eigenschaft, dass für jedes $a \in M$ gilt $R(a, e)$ (also jeder Knoten ist mit e verbunden).
- Eine *Gruppe* ist eine Struktur $(M, \circ, e)$ so, dass $\circ$ eine zweistellige assoziative Funktion auf M ist (also so, dass gilt: $a \circ (b \circ c) = (a \circ b) \circ c$), für jedes $a \in M$ gilt $a \circ e = a$ (e ist *neutral*) und für jedes $a \in M$ ein $b \in M$ existiert mit $a \circ b = e$ (jedes Element hat ein *inverses*).

Das können wir nun sehr viel kompakter folgendermaßen ausdrücken:

[16] Mengen sind die fundamentalsten Objekte der gesamten Mathematik – was genau wir unter Mengen verstehen (was üblicherweise durch das Axiomensystem ZFC festgelegt wird) bestimmt gewissermaßen, was man unter gültiger Mathematik überhaupt versteht.

Definition.
- Sei $L = (R)$. Ein ungerichteter Graph ist ein Modell der Theorie
$$\{\forall x \forall y\ (R(x,y) \leftrightarrow R(y,x))\}$$
- Sei $L = (R, e)$. Ein punktierter ungerichteter Graph ist ein Modell der Theorie
$$\{\forall x \forall y\ (R(x,y) \leftrightarrow R(y,x)),\ \forall x\ R(x,e)\}$$
- Sei $L = (\circ, e)$. Eine Gruppe ist ein Modell der Theorie
$$\{\forall x \forall y \forall z\, x \circ (y \circ z) \doteq (x \circ y) \circ z,\ \forall x\ x \circ e \doteq x,\ \forall x \exists y\ x \circ y \doteq e\}$$

Wenn wir jetzt also allgemein Graphen, Gruppen und ähnliche „Strukturentypen" betrachten wollen, können wir uns (zumindest in einem gewissen Rahmen) mit Hilfe eines Kalküls auf die rein syntaktische Ebene zurückziehen, Strukturen somit komplett ignorieren und nur noch überlegen, was die Theoreme der entsprechenden Theorien sind.

8 Der Hilbert-Kalkül

Wie bereits bei der Aussagenlogik besteht auch unser prädikatenlogisches Kalkül wieder aus Kalkülaxiomen und Inferenzregeln. Unser Wissen über Aussagenlogik hilft uns hier bereits deutlich weiter, da wir aussagenlogische Tautologien bereits als Axiome verwenden können. Dazu definieren wir eine (prädikatenlogische) Tautologie einfach als eine Formel, die entsteht, wenn wir in einer Aussagenlogischen Tautologie die Aussagenvariablen konsequent durch prädikatenlogische Formeln ersetzn. Die Formel $(x \doteq 0 \vee \neg x \doteq 0)$ ist dann zum Beispiel eine Tautologie, da sie entsteht, indem wir in der aussagenlogischen Tautologie $(A \vee \neg A)$ die Aussagenvariable A durch die Formel $x \doteq 0$ ersetzen.

Definition 2.11. Eine *Tautologie* ist eine prädikatenlogische Formel, die entsteht, indem wir jeder Aussagenvariable einer aussagenlogischen Tautologie eine prädikatenlogische Formel zuweisen und konsequent ersetzen.

Der Hilbert-Kalkül hat nun (unendliche viele) Axiome, die in drei Schemata fallen, nämlich Tautologien, Gleichheitsaxiome und Existenzaxiome. Die Gleichheitsaxiome müssen wir hierfür noch definieren, um die Existenzaxiome kümmern wir uns gleich anschließend:

Definition 2.12. Sei L eine Signatur. Die folgenden Formeln heißen *Gleichheitsaxiome*:

1. $\forall x\ x \doteq x$
2. $\forall x \forall y\ (x \doteq y \rightarrow y \doteq x)$
3. $\forall x \forall y \forall z\ ((x \doteq y \wedge y \doteq z) \rightarrow x \doteq z)$
4. Für jedes n-stellige Funktionssymbol $f \in L$:
   $\forall x_1 ... \forall x_n \forall y_1 ... \forall y_n\ ((x_1 \doteq y_1 \wedge ... \wedge x_n \doteq y_n) \rightarrow f x_1 ... x_n \doteq f y_1 ... y_n)$
5. Für jedes n-stellige Relationssymbol $R \in L$:
   $\forall x_1 ... \forall x_n \forall y_1 ... \forall y_n\ ((x_1 \doteq y_1 \wedge ... \wedge x_n \doteq y_n) \rightarrow (R x_1 ... x_n \leftrightarrow R y_1 ... y_n))$

Außerdem nehmen wir zwei Inferenzregeln, nämlich den bereits bekannten Modus Ponens und die Existenzeinführung:

Definition 2.13. (Hilbert-Kalkül) Sei L eine Signatur, φ eine L-Formel und T eine Menge von L-Sätzen. Wir sagen „φ ist beweisbar in T" und schreiben $T \vdash \varphi$ genau dann, wenn $\varphi \in T$ ist oder:

- φ eine Tautologie ist, oder
- φ ein Gleichheitsaxiom ist, oder
- (Existenzaxiom) φ die Form $(\psi\left[\frac{t}{x}\right] \to \exists x\psi)$ hat für eine L-Formel ψ und einen L-Term t, oder
- (Modus Ponens) Es zwei Formeln $\psi, (\psi \to \varphi)$ gibt mit $T \vdash \psi$ und $T \vdash (\psi \to \varphi)$. Also:

$$\frac{\psi, \quad (\psi \to \varphi)}{\varphi}$$

  oder

- (Existenzeinführung) φ die Form $(\exists x\psi \to \chi)$ hat, x *nicht* frei in χ vorkommt und $T \vdash (\psi \to \chi)$. Also:

$$\frac{(\psi \to \chi), \quad x \text{ nicht frei in } \chi}{(\exists x\psi \to \chi)}$$

Übungsaufgaben Überlege wieder, warum alle Axiome und Inferenzregeln des Hilbert-Kalküls tatsächlich Sinn machen.[17] Insbesondere überlege, warum die Bedingung „wenn x nicht frei in χ vorkommt“ bei der Existenzeinführung notwendig ist! Fallen dir Formeln ψ, χ und eine Belegungsfunktion β ein so, dass x frei in χ ist, $(\psi \to \chi)[\beta]$ (in irgendeiner Interpretation) wahr ist, aber $(\exists x\psi \to \chi)[\beta]$ nicht?

Der Modus Ponens, den wir auch in der Aussagenlogik hatten, erlaubt es uns übrigens mit Hilfe von aussagenlogischen Tautologien alle Äquivalenzumformungen durchzuführen, die wir in der Aussagenlogik auch schon hatten, ohne dabei die Beweisbarkeit zu „verlieren“. Das heißt, wenn φ beweisbar ist und (aussagenlogisch) $\varphi \equiv \psi$ gilt, dann ist auch ψ beweisbar, da dann $(\varphi \to \psi)$ eine Tautologie ist und wir mit Modus Ponens ψ herleiten dürfen.

Nachdem wir den Allquantor definiert haben über $\forall x\varphi = \neg\exists\neg\varphi$ erhalten wir auch noch die „dualen“ Formen der Existenzaxiom und -Einführung:

Satz 2.1. *Sei L eine Signatur, T eine Menge von L-Sätzen und ψ, χ irgendwelche L-Formeln.*

1. *(Allaxiom) Es gilt $T \vdash \left(\forall x\psi \to \psi\left[\frac{t}{x}\right]\right)$ für jeden L-Term t.*
2. *(Alleinführung) Wenn x nicht frei in χ ist und $T \vdash (\chi \to \psi)$, dann gilt auch $T\vdash (\chi \to \forall x\psi)$. Also:*

$$\frac{(\chi \to \psi), \quad x \textit{ nicht frei in } \chi}{(\chi \to \forall x\psi)}$$

Beweis. 1. Per Definition gilt $\left(\forall x\psi \to \psi\left[\frac{t}{x}\right]\right) = \left(\neg\exists x\neg\psi \to \psi\left[\frac{t}{x}\right]\right)$. Nach Aussagenlogik ist das äquivalent zu $\left(\neg\psi\left[\frac{t}{x}\right] \to \exists x\neg\psi\right)$, was genau die Form eines Existenzaxiomes ist.

2. $(\chi \to \psi)$ ist nach Aussagenlogik äquivalent zu $(\neg\psi \to \neg\chi)$. Nach Vorraussetzung ist x nicht frei in χ, wir dürfen also eine Existenzeinführung machen und erhalten $T \vdash (\exists x\neg\psi \to \neg\chi)$. Das ist wiederum aussagenlogisch äquivalent zu $(\chi \to \neg\exists x\neg\psi)$ was per Definition des Allquantors das selbe ist wie $(\chi \to \forall x\psi)$.

□

[17] Vergiss nicht, dass wir bei der Substitution $\varphi\left[\frac{t}{x}\right]$ explizit festgelegt haben, dass t keine Variable enthalten darf, die in φ gebunden ist; sonst geht hier das Existenzaxiom kaputt. Fällt dir ein Beispiel hierfür ein?

Wir führen wieder einen Beispielbeweis durch:

Satz 2.2. *Sei T beliebig und x nicht frei in der Formel ψ. Dann gilt*

$$T \vdash (\exists x(\varphi(x) \vee \psi) \leftrightarrow (\exists x\varphi(x) \vee \psi))$$

für jede Formel $\varphi(x)$. (Was besagt die Formel? Ist „klar“, dass das in jeder Theorie gelten sollte?)

Beweis. Wir können beide Implikationen einzeln zeigen; die Äquivalenz folgt dann mit Aussagenlogik und Modus Ponens (weil $(((A \to B) \wedge (B \to A)) \to (A \leftrightarrow B))$ eine Tautologie ist).

- Wir zeigen $T \vdash (\exists x(\varphi(x) \vee \psi) \to (\exists x\varphi(x) \vee \psi))$. Diese Formel ist aussagenlogisch äquivalent zu
$$(\exists x(\neg\psi \to \varphi(x)) \to (\neg\psi \to \exists x\varphi(x)))$$
Wir brauchen also nur zu zeigen, dass diese Formel beweisbar ist. Nach Existenzaxiom gilt
$$T \vdash (\varphi(x) \to \exists x\varphi(x))$$
Außerdem ist $(B \to C) \to ((A \to B) \to (A \to C))$ eine Tautologie; mit $B = \varphi(x), C = \exists x\varphi(x)$ und $A = \neg\psi$ erhalten wir also dank Modus Ponens
$$T \vdash (\neg\psi \to \varphi(x)) \to (\neg\psi \to \exists x\varphi(x)))$$
In $\exists x\varphi(x)$ kommt x nur gebunden vor, und nach Vorraussetzung kommt x in ψ nicht frei vor – x ist also nicht frei in $(\neg\psi \to \exists x\varphi(x))$, und damit dürfen wir nun eine Existenzeinführung vornehmen und erhalten
$$T \vdash (\exists x(\neg\psi \to \varphi(x)) \to (\neg\psi \to \exists x\varphi(x)))$$
was zu zeigen war.

- Wir zeigen $T \vdash ((\exists x\varphi(x) \vee \psi) \to \exists x(\varphi(x) \vee \psi))$. Nach Aussagenlogik ist $A \to (A \vee B)$ eine Tautologie, wir haben also
$$T \vdash (\varphi(x) \to (\varphi(x) \vee \psi))$$
Außerdem erhalten wir mit Existenzaxiom
$$T \vdash ((\varphi(x) \vee \psi) \to \exists x(\varphi(x) \vee \psi))$$
Nach Aussagenlogik ist $(((A \to B) \wedge (B \to C)) \to (A \to C))$ eine Tautologie. Mit $A = \varphi(x), B = (\varphi(x) \vee \psi)$ und $C = \exists x(\varphi(x) \vee \psi)$ und Modus Ponens erhalten wir also
$$T \vdash (\varphi(x) \to \exists x(\varphi(x) \vee \psi))$$
und Nachdem x nicht frei in $\exists x(\varphi(x) \vee \psi)$ ist dürfen wir eine Existenzeinführung vornehmen und erhalten
$$T \vdash (\exists x\varphi(x) \to \exists x(\varphi(x) \vee \psi))$$
Auf genau die selbe Weise können wir außerdem zeigen, dass
$$T \vdash (\psi \to \exists x(\varphi(x) \vee \psi))$$
Jetzt benutzen wir wieder eine Tautologie, nämlich $(((A \to C) \wedge (B \to C)) \to ((A \vee B) \to C)$ und erhalten
$$T \vdash ((\exists x\varphi(x) \vee \psi) \to \exists x(\varphi(x) \vee \psi))$$
was zu zeigen war.

□

Man sieht wieder, dass Beweise im Hilbert-Kalkül relativ aufwendig wirken. Der Hilbert-Kalkül hat aber den großen Vorteil, dass viele Beweisschritte durch aussagenlogische Tautologien begründbar sind – wenn man also ein gutes Gespür für die Aussagenlogik hat, werden Hilbert-Kalkülbeweise vergleichsweise intuitiv. Dennoch sind wieder der konkrete Kalkül und seine Regeln (außer explizit für Beweistheoretiker, die sich mit so etwas auseinandersetzen) eigentlich egal – wichtig ist nur, dass es einen Kalkül gibt, der *vollständig* ist. Das folgt in dem Fall aus diesem an für sich schon sehr interessanten Resultat:

Satz 2.3. *Sei T eine Menge von L-Sätzen. Dann ist T eine Theorie (hat also ein Modell) genau dann, wenn nicht $T \vdash \bot$ gilt.*

Es sollte klar sein, dass eine Theorie, die ein Modell hat, keinen Widerspruch erzeugen kann – dann wäre ja das Modell an sich widersprüchlich, was wiederum so viel heißt wie, es konnte gar nicht existieren. Die interessantere Richtung ist also die umgekehrte: Wenn ich aus einer Menge von Formeln keinen Widerspruch ableiten kann, dann gibt es tatsächlich eine Struktur, die die Theorie erfüllt! Der Beweis hierfür ist entsprechend trickreich, denn man muss es schaffen, nur mit Hilfe der Formeln aus T ein Modell zu bauen. Hat man dies geschafft kann man aber tatsächlich die Vollständigkeit des Kalküls beweisen:

Satz 2.4. ***(Gödelscher Vollständigkeitssatz)*** *Sei T eine Menge von L-Sätzen und φ eine L-Formel. Dann gilt $T \models \varphi$ genau dann, wenn $T \vdash \varphi$.*

Beweis. Man kann sich leicht überlegen, dass $T \models \varphi$ gilt genau dann, wenn $T \cup \{\neg\varphi\}$ kein Modell hat – in einem Modell davon müsste ja dann sowohl φ als auch $\neg\varphi$ gelten, und das kann nicht passieren. Nach dem vorherigen Satz gilt also $T \models \varphi$ auch genau dann, wenn $T \cup \{\neg\varphi\} \vdash \bot$. Das wiederum gilt tatsächlich genau dann, wenn $T \vdash \varphi$:

Wenn $T \vdash \varphi$ gilt, folgt natürlich auch $T \cup \{\neg\varphi\} \vdash \varphi$ und damit $T \cup \{\neg\varphi\} \vdash (\varphi \wedge \neg\varphi) \equiv \bot$.

Gilt umgekehrt $T \cup \{\neg\varphi\} \vdash \bot$, dann gilt entweder bereits $T \vdash \bot$ oder nicht. In ersterem Fall gilt wegen Ex Falso Quodlibet insbesondere auch $T \vdash \varphi$, in zweiterem Falle ist T selbst konsistent, aber durch Hinzufügen von $\neg\varphi$ wird es inkonsistent. Das kann nur sein, wenn $T \vdash (\neg\varphi \to \bot)$ gilt, und das ist aussagenlogisch äquivalent zu $T \vdash \varphi$.

Wir erhalten also insgesamt: $T \models \varphi$ genau dann, wenn $T \cup \{\neg\varphi\}$ kein Modell hat, genau dann, wenn $T \cup \{\neg\varphi\} \vdash \bot$ genau dann, wenn $T \vdash \varphi$. □

9 Der Kompaktheitssatz und seine Folgen

Wie bereits in der Aussagenlogik führt auch in der Prädikatenlogik der Vollständigkeitssatz zum Kompaktheitssatz:

Satz 2.5. ***(Kompaktheitssatz der Prädikatenlogik)***

1. *Wenn $T \models \varphi$ gilt, dann gibt es bereits eine endliche Teilmenge $T' \subset T$ so, dass $T' \models \varphi$.*
2. *Wenn jede endliche Teilmenge von T ein Modell hat, dann hat auch T selbst ein Modell.*

Der Beweis ist dabei genau der selbe wie auch in der Aussagenlogik. Hier führt er jetzt aber dazu, dass wir sehr interessante Modelle bauen können, und er führt zu leicht unschönen, aber interessanten Resultaten:

Satz 2.6. *Die „Menge aller endlichen Strukturen“ ist nicht axiomatisierbar. Genauer: Jede Theorie T, die beliebig große endliche Modelle hat, hat auch ein unendliches Modell.*

Im Umkehrschluss folgt daraus: Jede Theorie, die nur endliche Modelle hat, hat ein maximal großes Modell – es gibt also eine natürliche Zahl n so, dass kein Modell von T mehr als n Elemente hat.

Beweis. Angenommen, T hat beliebig große endliche Modelle. Wir betrachten für jede natürliche Zahl n die folgende Formel:

$$\varphi_n = \exists x_1 ... \exists x_n (\neg x_1 \doteq x_2 \wedge \neg x_1 \doteq x_3 \wedge ... \wedge \neg x_1 \doteq x_n \wedge \neg x_2 \doteq x_3 \wedge ... \wedge \neg x_2 \doteq x_n \wedge ... \wedge \neg x_{n-1} \doteq x_n)$$

Dann besagt die Formel φ_n also „Es gibt mindestens n verschiedene Elemente“.

Sei T' die Menge aller Formeln φ_n für jede natürliche Zahl, also $T' = \{\varphi_n \mid n \in \mathbb{N}\}$. Jedes Modell von T' muss dann unendlich viele Elemente haben, da es für jede natürliche Zahl n die Formel φ_n erfüllen muss, und somit mindestens n Elemente besitzen. Wenn wir also zeigen können, dass $T \cup T'$ ein Modell hat, sind wir fertig, da dieses dann ein Modell sowohl von T als auch von T' sein muss, also ein unendliches Modell von T.

Wir benutzen dafür den Kompaktheitssatz. Dann müssen wir also nur zeigen, dass jede endliche Teilmenge von $T \cup T'$ ein Modell hat. Sei S so eine endliche Teilmenge, dann kann diese also nur endlich viele Formeln aus T' enthalten. Wenn wir aber nur endlich viele der φ_n haben, dann sagen diese nur für endlich viele natürliche Zahlen k, dass es „mindestens k Elemente gibt“. Nach Vorraussetzung hat T aber beliebig große endliche Modelle, es gibt also ein ausreichend großes Modell $\mathfrak{A}$ so, dass $\mathfrak{A} \models T$ und $\mathfrak{A} \models S$. S hat also ein Modell, und nachdem unsere endliche Teilmenge beliebig war, hat also jede endliche Teilmenge von $T \cup T'$ ein Modell.

Nach dem Kompaktheitssatz hat somit auch $T \cup T'$ ein Modell und das muss ein unendliches Modell von T sein. □

Wie bereits erwähnt können wir den Kompaktheitssatz auch nutzen, um sehr absurde Modelle zu bauen; insbesondere Modelle, die ununterscheidbar sind von „bekannten“ Modellen, aber zusätzliche sehr seltsame Elemente beinhalten:

Satz 2.7.
1. *Sei L irgendeine Signatur, die mindestens die Symbole $1, +$ und $<$ enthält und sei T die Menge aller L-Sätze, die in $\mathbb{N}$ wahr sind. Dann hat T ein Modell, in dem es Elemente gibt, die größer sind als jede natürliche Zahl. Das heißt: Es gibt eine Struktur, in der genau die selben Sätze gelten wie in $\mathbb{N}$,die aber „unendlich große“ Elemente enthält. Diese Elemente heißen* Nichtstandard-Zahlen*.*
2. *Eine solche Struktur enthält automatisch unendlich viele Nichstandard-Zahlen und es gibt keine kleinste Nichtstandard-Zahl.*
3. *Es gibt keine Formel $\varphi(x)$ so, dass $\varphi(n)$ nur für die „echten“ natürlichen Zahlen n gilt, aber nicht für die Nichstandard-Zahlen. Standard- und Nichtstandardzahlen sind also in der Prädikatenlogik* ununterscheidbar*.*

Beweis.
1. Sei T also die Menge aller Sätze, die in $\mathbb{N}$ wahr sind. Wir erweitern zunächst unsere Signatur um ein neues Konstantensymbol c und betrachten folgende Theorie:

$$T' = \{c > 1, c > 1+1, c > 1+1+1, ...\} = \{c > n \mid n \in \mathbb{N}\}.$$

Sei wieder S eine endliche Teilmenge von $T \cup T'$, dann enthält diese nur endlich viele Formeln der Form $c > n$, wir finden also eine ausreichend große natürliche Zahl k so, dass wenn wir das Konstantensymbol c als k interpretieren, $\mathbb{N}$ ein Modell von S ist. Somit hat jede endliche Teilmenge von $T \cup T'$ ein Modell und nach dem Kompaktheitssatz hat damit auch $T \cup T'$ selbst ein Modell $\mathfrak{A}$. Dann gilt aber $\mathfrak{A} \models T$, und somit gelten in $\mathfrak{A}$ alle Sätze, die auch in $\mathbb{N}$ gelten. Es gilt aber auch $\mathfrak{A} \models T'$, und somit muss es eine Konstante in $\mathfrak{A}$ geben, die die Interpretation des Symbols c ist, und die somit größer sein muss als jede natürliche Zahl.

2. In $\mathbb{N}$ gelten die Formeln $\forall x \exists y\ y \doteq x+1$ und $\forall x\ x+1 > x$. Für jede „unendlich große“ Nichtstandard-Zahl i gibt es also auch die Nichtstandard-Zahl $i+1$ und $i+1+1$ und $i+1+1+1...$ etc, also gibt es unendlich viele.

   Außerdem gilt in $\mathbb{N}$ die Formel $\forall x(x \doteq 0 \vee \exists y\ x \doteq y+1)$, also „Jede Zahl ist entweder 0 oder hat einen direkten Vorgänger“, insbesondere hat also auch jede Nichtstandard-Zahl i einen Vorgänger $i-1$, der natürlich keine Standardzahl sein kann, weil für jede Standardzahl n auch $n+1$ wieder eine Standard-Zahl ist. Es kann also keine kleinste Nichtstandard-Zahl geben.

3. Angenommen $\varphi(x)$ trifft auf alle Standard-Zahlen zu. Dann gilt also $\forall x \varphi(x) \in T$, also gilt die selbe Formel auch in $\mathfrak{A}$.

□

Allerdings können wir jetzt auch klären, was infinitesimale Zahlen sind, indem wir genau das selbe mit $\mathbb{R}$ machen:

Satz 2.8. 1. *Sei L wie vorher mit zusätzlich der Multiplikation $\cdot$. Es gibt eine Struktur, in der genau die selben Sätze gelten wie in $\mathbb{R}$, die aber „unendlich große“ Elemente enthält.*

2. *Die selbe Struktur enthält auch infinitesimale Elemente, also Zahlen ε, für die gilt $\varepsilon > 0$, aber $\varepsilon < \frac{1}{n}$ für jede natürliche Zahl n.*

3. *Die reellen Nichtstandard-Zahlen liegen* dicht *in $\mathbb{R}$, das bedeutet: zwischen je zwei beliebigen reellen Zahlen $a < b$ liegen unendlich viele Nichtstandard-Zahlen.*

Beweis. 1. Wie bei $\mathbb{N}$ auch – wir erweitern wieder L um ein Konstantensymbol c und betrachten wieder $T' = \{c > 1, c > 1+1, c > 1+1+1, ...\}$. Sei T die Menge aller L-Sätze, die in $\mathbb{R}$ gelten, dann hat wieder jede endliche Teilmenge von $T \cup T'$ ein Modell mit Universum $\mathbb{R}$ und einer hinreichend großen Zahl als Interpretation für c. Mit dem Kompaktheitssatz folgt wieder, dass $T \cup T'$ ein Modell $\mathfrak{A}$ hat und in diesem Modell existiert ein „unendlich großes“ Element i.

2. In $\mathbb{R}$ gilt die Formel

$$\forall x \exists y (x \cdot y \doteq 1 \wedge (x > 0 \rightarrow y > 0) \wedge \forall z ((x > z \wedge z > 0) \rightarrow y < z^{-1})).^{18}$$

   Es gibt also die Zahl $\frac{1}{c} = \varepsilon$ und es folgt, dass $\varepsilon > 0$ und für jede natürliche Zahl n gilt $c > n$ und somit $\varepsilon < \frac{1}{n}$.

3. Es lässt sich leicht überlegen, dass mit ε auch $2\varepsilon, 3\varepsilon, ...\frac{1}{2}\varepsilon, \frac{1}{3}\varepsilon$ usw.usf. existieren müssen und ebenfalls alle infinitesimal sind. Wir haben also unendliche viele infinitesimale Zahlen zwischen 0 und $\frac{1}{n}$ für jede natürliche Zahl n. Seien nun (Standard-) reelle Zahlen $a < b$ beliebig gegeben und δ eine beliebige infinitesimale Zahl, dann muss auch $a + \delta < b$ gelten. Für jede infinitesimale Zahl (wovon es unendlich viele gibt) gibt es also jeweils eine Nichtstandard-Zahl zwischen a und b.

□

Derartige Modelle der reellen Zahlen mit Nichtstandard-Zahlen nennen sich übrigens *hyperreelle Zahlen*, und mit diesen können wir tatsächlich die gesamte Differential- und Integralrechnung genau so aufziehen, wie Leibniz und Newton sich das damals vorgestellt hatten. Die Mathematik, die sich mit diesen Zahlen beschäftigt nennt sich *Nichtstandard-Analysis*.

[18] Ich benutze hier das Symbol z^{-1} als Abkürzung - ich brauche kein eigenes Symbol dafür, da ich auch die Teilformel $\exists w\ z \cdot w \doteq 1$ hätte einfügen können und dann statt z^{-1} einfach w benutzen. Dann würde die Formel aber länger und schwerer lesbar ;-) Man sagt dafür auch „Die Funktion $^{-1}$ ist in der Signatur *definierbar*“.

3 Fundamentale Theorien

Jetzt wo wir (halbwegs) wissen, wir Prädikatenlogik funktioniert, können wir mal ein paar *fundamentale* Theorien betrachten, die mehr oder minder unabdingbar für die gesamte Mathematik sind, nämlich zum einen die Peano-Axiome, die die natürlichen Zahlen axiomatisieren, und ZFC, die uns sagt, was Mengen eigentlich genau sind. Letztere Theorie hilft uns auch dabei zu verstehen, was eigentlich Funktionen, Relationen und somit Strukturen eigentlich genau sind.

1 Metamathematische Probleme

Wie bereits gesagt soll ZFC definieren was eine Menge ist. Dabei fällt vielleicht folgendes Problem auf: ZFC ist eine Theorie. Eine Theorie ist eine Menge von Formeln. ZFC ist also eine Menge, die uns sagen soll, was eine Menge ist. Das ist ein Zirkelschluss!

Mehr noch: Wir haben in diesem Dokument so oder so mehrfach Sätze aufgestellt und bewiesen. Diese Sätze lassen sich natürlich (prinzipiell innerhalb von ZFC) als prädikatenlogische Formeln formulieren und entsprechend im Hilbert-Kalkül beweisen. So können wir unsere Beweise auch formal überprüfen. Allerdings können wir wiederum den Kalkül und Formeln selbst gar nicht definieren, oder zumindest anwenden, ohne nicht manche dieser Sätze bereits aufgestellt und bewiesen zu haben. Auch hier haben wir wieder einen Zirkelschluss.

Außerdem haben wir des öfteren in allen Definition natürliche Zahlen benutzt, von denen wir gar nicht „wissen“, was sie sind, ohne nicht die Peano-Axiome zu formulieren, für die wir wiederum prädikatenlogische Formeln brauchen, für die wir wiederum u.A. natürliche Zahlen brauchen...

Kurz: In dem gesamten Konzept der mathematischen Logik haben wir immer das Problem, dass wir bereits auf irgendeinem Fundament stehen müssen, um sie zu betreiben. Und der ganze Sinn der mathematischen Logik ist es, so ein Fundament aufzubauen. Das ist notwendigerweise zirkulär und lässt sich unmöglich vermeiden. Wir müssen schließlich entweder *irgendwo* anfangen, um überhaupt irgendetwas zu formulieren/beweisen – dann haben wir unbewiesene Axiome. *Oder* wir haben einen Zirkelschluss, was auch unbefriedigend ist. *Oder* wir haben einen unendlichen Regress, also Sätze, die auf Sätzen beruhen, die wieder auf anderen Sätzen beruhen, die wiederum auf noch anderen Sätzen beruhen, etc.

Kurz: Wir müssen so oder so irgendwo die Zähne zusammenbeißen und akzeptieren, dass es nicht möglich ist, aus dem „Nichts“ die gesamte Mathematik aufzubauen, ohne jegliche Grundannahmen. Die noch am befriedigendste Rechtfertigung für alles, was wir hier tun, scheint mir somit die folgende zu sein:

Die Grundannahmen, die wir benötigen um die Logik als solche aufzubauen, scheinen mir grundlegend genug zu sein, dass sie kaum jemand abstreiten würde. Es ist *möglich*, sie abzustreiten und Intuitionisten beispielsweise tun das auch, und die haben auch ihre Gründe dafür, aber die *meisten* Grundannahmen, die wir bisher verwendet haben, sind grundlegend genug, dass die überwältigende Mehrheit der Mathematiker sie als gültig erachtet. Andere mathematische Philosophien haben natürlich andere Grundannahmen, und diese haben entsprechend auch andere Probleme, aber der Zirkelschluss steckt letztenendes in allen derartigen Systemen.

Wenn wir aber die Grundannahmen, auf denen wir die Logik aufgebaut haben akzeptieren, dann können wir *jetzt* die mathematische Logik, die wir aufgebaut haben benutzen, um diese Grundannahmen zu konkretisieren, zu verfeinern und darum herum neue Gesetzmäßigkeiten aufzubauen. Gewissermaßen haben wir also von „schwachen“ Axiomen aus ein System aufgebaut, dass es uns jetzt erlaubt, „starke“ Aussagen zu formulieren und zu beweisen, die nun unsere vorherigen schwachen Annahmen rechtfertigen.

Den Zirkelschluss zaubert das natürlich nicht weg, aber das lässt er sich nunmal auch nicht.

2 Peano-Arithmetik

Bevor wir die Peano-Axiome selbst betrachten sollte eines erwähnt werden: Wir haben mit dem Kompaktheitssatz bereits gezeigt, dass sich die natürlichen Zahlen nicht eindeutig axiomatisieren lassen - schließlich kann ich für jede Theorie, die in den natürlichen Zahlen gilt, mit dem Kompaktheitssatz ein Modell finden, das zusätzliche Nichtstandard-Zahlen beinhaltet. In einem gewissen Sinne macht das jedoch nichts: Jedes Modell solch einer Theorie muss schließlich die 0 enthalten, genauso wie die 1 und die 2 und jede Standard-Zahl. Die Unterschiedlichen Modelle solch einer Theorie unterscheiden sich also nur um potentiell zusätzliche Elemente; die Standard-Zahlen sind somit genau die, die in *allen* Modellen solch einer Theorie vorkommen.

Die Peano-Axiome verwenden die Signatur $L_{PA} = (0, S, +, \cdot, <)$. Dabei ist 0 ein Konstantensymbol (ach, nee...), $+$ und $\cdot$ sind zweistellige Funktionssymbole (jaaa, wissen wir...), $<$ natürlich ein zweistelliges Relationssymbol und S ein einstelliges Funktionssymbol, das die Nachfolger-Funktion darstellen soll. Es soll also gelten $S(0) = 1, S(1) = 2, S(2) = 3$ etc.

Definition 3.1. (Peano-Axiome) Die Theorie PA besteht aus folgenden Axiomen:

1. $\forall x \neg S(x) \doteq 0$ (Die 0 ist kein Nachfolger)
2. $\forall x \forall y\ (S(x) \doteq S(y) \to x \doteq y)$ (keine zwei unterschiedlichen Zahlen haben den selben Nachfolger)
3. $\forall x\ x + 0 \doteq x$ und $\forall x \forall y\ x + S(y) \doteq S(x + y)$ (Diese zwei Axiome definieren rekursiv die Addition)
4. $\forall x\ x \cdot 0 \doteq 0$ und $\forall x \forall y\ x \cdot S(y) \doteq x \cdot y + x$ (Diese zwei Axiome definieren rekursiv die Multiplikation)
5. $\forall x \neg x < 0$ und $\forall x \forall y\ (x < S(y) \leftrightarrow (x \doteq y \vee x < y))$ (Diese zwei Axiome definieren rekursiv die $<$-Relation)
6. Für jede Formel $\varphi(x, y_1, ..., y_n)$ die Formel

   $$\forall y_1 ... \forall y_n\ ((\varphi(0, y_1, ..., x_n) \wedge \forall x(\varphi(x, y_1, ..., y_n) \to \varphi(x + 1, y_1, ..., y_n))) \to \forall x \varphi(x, y_1, ..., y_n))$$

   (Das *Induktionsschema*, das es erlaubt, Beweise per vollständiger Induktion zu führen)

Es lässt sich nun leicht zeigen, dass jedes Modell von PA (mindestens) die natürlichen Zahlen enthalten muss: Zunächst einmal muss natürlich eine 0 existieren, da diese Teil unserer Signatur ist. Außerdem gibt es kein kleineres Element als die 0, da Axiom 5 das explizit verbietet. Außerdem muss eine Zahl $S(0)$ existieren, die nicht die 0 ist, da die 0 kein Nachfolger ist (Axiom 1). Nennen wir also $S(0) = 1$. Dann gilt $1 = S(0)$ und damit $0 < 1$ nach Axiom 5. Außerdem muss $S(1)$ existieren und $S(1) \neq 0$ wegen Axiom 1 und $S(1) \neq 1$, da sonst aus Axiom 2 folgen würde $S(1) = 1 = S(0)$ und somit $1 = S(0) = 0$, was nicht sein kann, wie wir bereits gezeigt haben. Nennen wir also $S(1) = 2$, dann gilt außerdem nach Axiom 5 $1 < 2$ und $0 < 2$.

So können wir jetzt das Spielchen fortsetzen und Stück für Stück folgern, dass alle natürlichen Zahlen existieren müssen, paarweise verschieden sein müssen und die Ordnung tatsächlich die ist, die wir von $<$ erwarten.

Wir können außerdem zeigen, dass z.B. $2 + 2 = 4$ ist: Per Definition ist $2 = S(S(0))$ und $4 = S(S(S(S(0))))$. Nach Axiom 3 gilt dann:

$$2+2 = S(S(0))+S(S(0)) = S(S(S(0))+S(0)) = S(S(S(S(0))+0)) = S(S(S(S(0)))) = 4$$

Mit Hilfe des Induktionsschemas kann man außerdem Gesetze zeigen, wie z.B. dass die Addition und Multiplikation kommutativ sind, d.H.

$$\forall x \forall y\ x + y \doteq y + x \text{ bzw. } \forall x \forall y\ x \cdot y \doteq y \cdot x$$

Kurz: Es verhält sich alles genauso wie gewünscht. Außerdem können wir (wie vorhin bereits getan) definieren, was eine Primzahl ist und zeigen, dass es unendlich viele davon gibt. Und all dies funktioniert auf einer rein syntaktischen Ebene - zu keinem Zeitpunkt müssen wir eine Formel ernstzunehmend „interpretieren“ oder den Symbolen großartig eine Bedeutung geben, außer der Bedeutung, die ihnen rein durch die obigen Axiome ohnehin aufgezwungen wird!

3 Mengen

Die Peano-Axiome sagen uns nur, was natürliche Zahlen sein sollen. Das ist insofern bereits bemerkenswert, als dass die natürlichen Zahlen eine der wichtigsten (wenn nicht sogar *die* wichtigste) Strukturen der Mathematik überhaupt sind, und gleichzeitig eine der komplexesten. Sie liefern uns aber natürlich nicht irgendwelche Graphen, abstrakten Gruppen, reelle oder komplexe Zahlen, topologische Räume, geometrische Räume und all den anderen Kram, mit dem sich Mathematiker den ganzen Tag lang so beschäftigen.

Den Anspruch versucht ZFC zu erfüllen. ZFC sagt uns, was Mengen sind, und mit Hilfe von Mengen können wir all das beschreiben, solange wir beliebige Strukturen beschreiben können. Strukturen wiederum sind Tupel bestehend aus (einer Menge von) Konstanten, Funktionen und Relationen. Wenn wir also beliebige Tupel, Funktionen und Relationen als Mengen darstellen können haben wir unser Ziel erreicht. Dafür sollten wir aber erstmal ganz grob beschreiben, was Mengen sind:

> „Unter einer ‚Menge‘ verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die ‚Elemente‘ von M genannt werden) zu einem Ganzen.“
> - *Georg Cantor*

Aus moderner Sicht ist diese „Definition“ viel zu schwammig, um sinnvoll anwendbar zu sein – aber dafür gibt es ja ZFC. Wichtig sind aber zunächst folgende Dinge:

- Eine Menge wird durch ihre Elemente eindeutig beschrieben und es gibt nur zwei Möglichkeiten: Entweder ein Element liegt in der Menge, oder eben nicht. Das bedeutet, die Menge $\{a, b\}$ ist *die selbe Menge* wie die Menge $\{a, a, b, b, b\}$.
- Genauer: Zwei Mengen sind genau dann gleich, wenn sie die selben Elemente haben. Insbesondere haben Mengen auch keine feste Ordnung: Die Menge $\{1, 2, 3, 4, 5\}$ ist die selbe Menge wie die Menge $\{4, 2, 5, 1, 3\}$.
- Es folgt: Es gibt *genau eine* Menge ohne jegliche Elemente, nämlich die leere Menge $\emptyset$.
- Die Menge $a = \{1, 2, 3\}$ ist *nicht* die selbe Menge wie die Menge $b = \{\{1, 2, 3\}\}$ oder die Menge $c = \{\{1\}, \{2, 3\}\}$. Die Menge a hat drei Elemente, nämlich 1,2 und 3. Die Menge b hat nur ein Element, nämlich genau die Menge a. Die Menge c wiederum hat zwei Elemente, nämlich die Menge $\{1\}$ (was nicht das selbe ist wie die 1 selbst!) und die Menge $\{2, 3\}$.

Das sind alles Dinge, die wir im Folgenden im Hinterkopf behalten sollten. Wir wenden uns nun Tupeln zu und zeigen, wie wir diese als (ungeordnete!) Mengen darstellen können. Dabei helfen uns die sogenannten *Kuratowski-Paare*: Wir nehmen zwei beliebige Elemente a, b und wollen das Paar (a, b) darstellen. Das tun wir, indem wir definieren:

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

Ein Paar ist also eine Menge mit zwei Elementen $\{a\}$ und $\{a, b\}$ und durch den Aufbau der Menge ist eindeutig bestimmt, welches das erste und welches das zweite Element des Paares ist. Insbesondere ist $(a, b) \neq (b, a)$, weil $(a, b) = \{\{a\}, \{a, b\}\} \neq \{\{b\}, \{a, b\}\} = (b, a)$.

Diese Konzept können wir jetzt rekursiv weiterspinnen, indem wir definieren:

$$(a, b, c) = (a, (b, c)) \qquad (a, b, c, d) = (a, (b, c, d)) \qquad ...$$

...und so erhalten wir endliche Tupel beliebiger Länge.

So weit, so gut. Betrachten wir als nächstes Relationen. Sei dazu A eine beliebige Menge (also ein Universum einer Struktur). Wir bezeichnen mit A^n die *Menge aller Tupel der Länge n bestehend aus Elementen aus A*. Also ist A^2 die Menge aller Paare aus A, A^3 die Menge aller Dreiertupel usw. Sei z.B. $A = \{a, b, c\}$. Dann ist

$$A^2 = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$$

Damit können wir nun Relationen definieren:

Definition 3.2. Sei A eine beliebige Menge. Eine *n-stellige Relation R auf A* ist eine Teilmenge $R \subset A^n$. Wir sagen „Die Relation R trifft auf ein Tupel $(a_1, ..., a_n)$ zu“ genau dann, wenn $(a_1, ..., a_n) \in R$.

Und damit haben wir Relationen. Die Ordnung $<$ auf $\mathbb{N}$ ist somit einfach eine Teilmenge von $\mathbb{N}^2$, nämlich die Menge aller Paare $(a, b) \in \mathbb{N}^2$ für die gilt $a < b$. Also:

$$<= \{(0, 1), (0, 2), (0, 3), ..., (1, 2), (1, 3), ..., (2, 3), ...\}$$

Und jetzt, wo wir Relationen haben, können wir auch Funktionen definieren. Dafür brauchen wir nur noch kurz das *kartesische Produkt* zweier Mengen:

Definition 3.3. Seien A, B beliebige Mengen. Wir nennen das *kartesische Produkt aus A und B* (kurz: $A \times B$) die Menge aller Paare (a, b) für alle $a \in A$ und $b \in B$.

Wir definieren außerdem rekursiv weiter $A \times B \times C = A \times (B \times C)$, $A \times B \times C \times D = A \times (B \times C \times D)$ etc.

Seien als Beispiel $A = \{a_1, a_2\}$ und $B = \{b_1, b_2\}$. Dann ist also

$$A \times B = \{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2)\}$$

Damit können wir jetzt endlich Funktionen definieren:

Definition 3.4. Seien A, B Mengen. Eine *Funktion f von A nach B* (kurz: $f : A \to B$) ist eine Teilmenge $f \subset (A \times B)$ so, dass für jedes $a \in A$ *genau ein* $b \in B$ existiert mit $(a, b) \in f$. In Formeln:

$$\forall a \; (a \in A \to \exists b \; (b \in B \wedge (a, b) \in f \wedge \forall c \; ((a, c) \in f \to c \doteq b)))$$

oder mit den üblichen mathematischen Abkürzungen[19] auch

$$\forall a \in A \exists! b \in B \; (a, b) \in f$$

Wir schreiben für $(a, b) \in f$ auch einfach $f(a) = b$.

Damit haben wir also Funktionen, Relationen und Tupel alle abgedeckt. Es fehlen also nur noch die Konstanten selbst. Dazu sei aber folgendes angemerkt:

[19] Man liest $\exists! x$ als „Es gibt genau ein x“

Alles, was wir mit prädikatenlogischen Formeln über die Elemente des Universums aussagen können, liefert uns die Struktur selbst – also die spezifischen Eigenschaften der Funktionen und Relationen auf diesem Universum. Wie die Elemente des Universums selbst aussehen ist eigentlich völlig egal! Wir benutzen ja ohnehin nur *Symbole* für diese Elemente. Wir können also eigentlich *jede beliebige Menge*, die die passende Anzahl an Elementen hat als Universum nehmen, solange unsere Struktur darauf so definiert ist, dass sie das tut, was sie soll.

Nehmen wir zum Beispiel die Struktur $(\{Papier, Stein, Schere\}, \prec)$, wobei $\prec$ die Relation ist, die uns sagt, wer gegen wen gewinnt. Also

$$\prec = \{(Papier, Stein), (Stein, Schere), (Schere, Papier)\}$$

Alles, was wir jetzt über $Papier, Stein$ und $Schere$ aussagen können, ergibt sich nun aus der Relation $\prec$. Wir können also als Universum genausogut die Menge $\{a, b, c\}$ nehmen und darauf die Relation $\prec_2$ wie folgt definieren:

$$\prec_2 = \{(a, b), (b, c), (c, a)\}$$

Dann sind die zwei Strukturen $(\{Papier, Stein, Schere\}, \prec)$ und $(\{a, b, c\}, \prec_2)$ für alle praktischen Zwecke gleich! Man sagt dafür die Strukturen sind *isomorph* – in Symbolen:

$$(\{Papier, Stein, Schere\}, \prec) \cong (\{a, b, c\}, \prec_2)$$

Wir brauchen also im wahrsten Sinne des Wortes nur *irgendwelche* Mengen mit beliebig vielen (auch unendlich vielen) Elementen, um jede denkbare Struktur zu definieren, die sich Mathematiker ausdenken können. Kein Wunder also, dass Hilbert so unheimlich begeistert von Cantors Mengenlehre war! Das erleichtert uns jetzt enorm, eine Theorie aufzustellen, innerhalb der sich (fast) die gesamte Mathematik betreiben lässt.

4 Die ZFC-Axiome

Gut, jetzt wo wir mit Mengen halbwegs umgehen können, können wir die Axiome von ZFC betrachten. Die Signatur hat dabei erstmal nur ein einziges zweistelliges Relationssymbol, nämlich $\in$. Wir werden die Sprache aber Stück für Stück mit Abkürzungen erweitern, sobald wir diese definieren können.

Axiom 1. (Extensionalität) Zwei Mengen sind gleich genau dann, wenn sie die gleichen Elemente haben.

$$\forall x \forall y\ (x \doteq y \leftrightarrow \forall z\ (z \in x \leftrightarrow z \in y))$$

Wir definieren gleich die erste Abkürzung, nämlich $x \subset y$ für $\forall z\ (z \in x \to z \in y)$. Dann kann das Extensionalitätsaxiom auch geschrieben werden als

$$\forall x \forall y\ (x \doteq y \leftrightarrow (x \subset y \land y \subset x))$$

Axiom 2. (Aussonderungsschema) Für jede Formel $\varphi(x, y_1, ..., y_n)$, beliebige Mengen $a_1, ..., a_n$ und Menge b gibt es die Menge aller Elemente x aus b, die die Formel $\varphi(x, a_1, ..., a_n)$ erfüllen.

$$\forall a_1 ... \forall a_n \forall b \exists z \forall x\ (x \in z \leftrightarrow (x \in b \land \varphi(x, a_1, ..., a_n)))$$

Die Menge z, deren Existenz vom Aussonderungsschema verlangt wird, wird auch mit $\{x \in b \mid \varphi(x, a_1, ..., a_n)\}$ bezeichnet. So erhalten wir zum Beispiel die Menge aller geraden Zahlen als $\{x \in \mathbb{N} \mid \exists a\ x \doteq 2 \cdot a\}$. Wir können auch damit die nächsten Abkürzungen definieren, nämlich die leere Menge $\emptyset = \{x \in A \mid \neg x \doteq x\}$ für eine beliebige Menge A, und den Schnitt $a \cap b = \{x \in a \mid x \in b\}$.

Wir können jetzt übrigens beweisen, dass es keine „Menge aller Mengen" gibt:

Satz 3.1. ***(Russelsche Antinomie)*** *Es gibt keine Menge V aller Mengen.*

Beweis. Angenommen, es gäbe so eine Menge V. Betrachte die Formel $\neg x \in x$, dann gäbe es nach dem Aussonderungsschema die Menge $a = \{x \in V \mid \neg x \in x\}$. Es gilt entweder $a \in a$ oder $\neg a \in a$. Es folgt jedoch sofort $ZFC \vdash (a \in a \to \neg a \in a)$ und $ZFC \vdash (\neg a \in a \to a \in a)$, also $ZFC \vdash \perp$. □

Wir nennen das „Universum" aller Mengen trotzdem V. Solche „Mengen", die laut ZFC keine Mengen sind nennen wir *(echte) Klassen*. Die liegen dann natürlich nicht in unserem „Universum", sind aber Teilklassen davon.

Weiter mit den Axiomen:

Axiom 3. (Paarmenge) Zu je zwei Mengen a, b gibt es die Menge $z = \{a, b\}$.

$$\forall a \forall b \exists z \forall w \; (w \in z \leftrightarrow (z \doteq a \vee z \doteq b))$$

Damit können wir jetzt auch beweisen, dass für je zwei Mengen a, b das geordnete Paar (a, b) existiert: Nach dem Paarmengenaxiom gibt es die Mengen $\{a, a\} = \{a\}$ und $\{a, b\}$. Wenden wir das Paarmengenaxiom auf diese beiden Mengen wieder an, erhalten wir die Menge $\{\{a\}, \{a, b\}\} = (a, b)$.

Als nächstes fordern wir, dass wir Mengen *vereinigen* können:

Axiom 4. Für jede Menge (von Mengen) A gibt es die Vereinigungsmenge $B = \bigcup A$, also die Menge aller Elemente der Mengen in A.

$$\forall A \exists B \forall z \; (z \in B \leftrightarrow \exists w (z \in w \wedge w \in A))$$

Im Speziellen folgt daraus die Existenz der Vereinigung $a \cup b$ als $\bigcup \{a, b\}$.

Axiom 5. (Potenzmenge) Zu jeder Menge A gibt es die *Potenzmenge* $B = \mathcal{P}(A)$. Das ist die Menge aller Teilmengen von A.

$$\forall A \exists B \forall z \; (z \in B \leftrightarrow z \subset A)$$

Damit können wir jetzt zeigen, dass für je zwei Mengen A, B das kartesische Produkt $A \times B$ existiert:

Nach dem Vereinigungsmengenaxiom gibt es die Menge $A \cup B$ und nach dem Potenzmengenaxiom die Menge $\mathcal{P}(A \cup B)$. Diese enthält für jedes Paar $(a, b) \in A \times B$ die Elemente $\{a\}$ und $\{a, b\}$. Daraus folgt, dass $(a, b) = \{\{a\}, \{a, b\}\} \subset \mathcal{P}(A \cup B)$ ist und damit $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. Mit dem Aussonderungsaxiom erhalten wir also die Menge $\{(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid a \in A \wedge b \in B\} = A \times B$.

Axiom 6. (Ersetzungsschema) Für jede Formel $\varphi(x, y, z_1, ..., z_n)$ (und Mengen $c_1, ..., c_n$), die sich wie eine Funktion verhält (also wenn es für jedes a genau eine Menge b gibt so, dass $\varphi(a, b, c_1, ..., c_n)$ gilt) und für jede Menge A gibt es die *Bildmenge* B von A, also die Menge aller Mengen, auf die φ „abbildet".

$$\forall A, \forall c_1, ..., c_n \; (\forall x \exists! y \; \varphi(x, y, c_1, ..., c_n) \to \exists B \forall z \; (z \in B \leftrightarrow \exists a \; (a \in A \wedge \varphi(a, z, c_1, ..., c_n))))$$

Diese Menge wird üblicherweise $\varphi(A)$ genannt. Im Prinzip sagt das Axiom also: Ich kann durch jede beliebige als Formel ausdrückbare Vorschrift Elemente einer Menge A ersetzen und erhalte wieder eine Menge. Oder: Das Bild jeder Menge unter jeder als Formel beschreibbaren Funktion ist wieder eine Menge.

Das Axiom ist jetzt zugegebenermaßen schon etwas abstrakt. Aber man kann damit zum Beispiel zeigen, dass gewisse Ansammlungen von Mengen keine Mengen im Sinne von ZFC sind:

Satz 3.2. *Es gibt keine Menge aller einelementigen Mengen.*

Beweis. Angenommen es gäbe diese Menge; nennen wir sie A. Betrachte die Formel

$$\varphi(x, y, w) = (y \in x \land x \in w) \lor (\neg x \in w \land y \doteq \emptyset)$$

Dann gilt $ZFC \vdash \forall x \exists! y\ \varphi(x, y, A)$, denn wenn a nicht in A liegt gilt nur $\varphi(a, \emptyset, A)$ und wenn $a \in A$, dann hat a nur ein Element b und es gilt $\varphi(a, b, A)$.

Nach dem Ersetzungsschema gibt es also die Menge $\varphi(A) = \{x \in b \mid b \in A\}$. Nachdem es aber für jede Menge a die Menge $\{a\}$ gibt und $\{a\} \in A$ gilt, wäre $\varphi(A) = V$, was aber (wie bereits gezeigt) keine Menge ist, Widerspruch. □

Das nächste Axiom ist auch wieder etwas abstrakt:

Axiom 7. Jede Menge ist *fundiert*, das heißt:

$$\forall x\ (\neg x \doteq \emptyset \to \exists z\ (z \in x \land z \cap x \doteq \emptyset))$$

Sprich: Jede Menge a enthält mindestens eine Menge b so, dass a und b keine gemeinsamen Elemente haben. Das ist wichtig, weil es solche abstrusen Dinge verhindert wie Mengen, die sich selbst enthalten, oder komische Zirkel wie $a \in b \in c \in a$:

Satz 3.3. *Keine Menge enthält sich selbst.*

Beweis. Angenommen $a \in a$. Dann ist also $\{a\}$ eine Teilmenge von a und damit ist $\{a\} \cap a = a \neq \emptyset$, die Menge $\{a\}$ ist also nicht fundiert, existiert aber nach dem Paarmengenaxiom, Widerspruch. □

Das liefert uns auch einen kürzeren zweiten Beweis dafür, dass die Allklasse V keine echte Menge ist:

Beweis. Angenommen, V wäre eine echte Menge, dann müsste $V \in V$ gelten, Widerspruch zum vorherigen Satz. □

Das nächste Axiom garantiert, dass es unendliche Mengen gibt; und insbesondere, dass es eine Menge gibt, die sich wie die natürlichen Zahlen verhält:

Axiom 8. (Unendlichkeit) Es gibt eine Menge ω, die die leere Menge enthält und mit jeder Menge $a \in \omega$ auch die Menge $a \cup \{a\} \in \omega$.

$$\exists \omega\ (\emptyset \in \omega \land \forall x\ (x \in \omega \to x \cup \{x\} \in \omega))$$

Wir definieren $0 = \emptyset$. Dann gilt also $0 \in \omega$. Außerdem gilt $\emptyset \cup \{\emptyset\} = \{\emptyset\} \in \omega$, definieren wir also $1 = \{\emptyset\} = \{0\}$. Es gilt auch $1 \cup \{1\} = \{1, 0\} \in \omega$, also definieren wir $2 = \{1, 0\}$. Dann gilt auch wieder $2 \cup \{2\} = \{0, 1, 2\} \in \omega$, also definieren wir $3 = \{0, 1, 2\}$ und so weiter. So erhalten wir für jede natürliche Zahl eine Menge, und ω verhält sich genau wie die natürlichen Zahlen.

Damit ist also jede natürliche Zahl einfach die Menge ihrer Vorgänger, es gilt also praktischerweise $n < m$ genau dann, wenn $n \in m$. Damit wären wir beim letzten Axiom angekommen, das wieder ein bisschen abstrakt ist:

Axiom 9. (Auswahl) Zu jeder Menge A nichtleerer Mengen gibt es eine Funktion f, die aus jeder Menge in A ein Element auswählt. Also $f(a) \in a$ für alle $a \in A$.

$$\forall A\ (\neg \emptyset \in A \to \exists f\ ((f : A \to V) \land \forall a \in A\ f(a) \in a))$$

Das Auswahlaxiom ist etwas kontrovers - manche Mathematiker lehnen es ab und entsprechend ist es guter Stil, bei Beweisen immer anzugeben, wenn man davon gebrauch macht. Die meisten Mathematiker halten es aber für „offensichtlich“ wahr, auch wenn es eine paar seltsame Folgerungen hat. Auf die einzugehen würde aber den Rahmen hier sprengen. In vielen Situationen braucht man es aber auch nicht, zum Beispiel wenn man für jede Menge $a \in A$ ein konkretes Element angeben kann - wichtig wird es erst, wenn A unendlich groß ist und die Elemente in den Mengen $a \in A$ nicht formal unterschieden werden können, oder ich kein formales Verfahren angeben kann, dass ein konkretes Element aus jeder Menge rauspickt:

> „Das Auswahlaxiom wird benötigt um eine Menge aus einer unendlichen Menge von Socken auszuwählen, aber nicht aus einer unendlichen Menge von Schuhen.“
> - *Bertrand Russell*

Das liegt daran, dass ich bei Schuhen einfach sagen kann „wähle jeweils den linken Schuh“ – bei einem Paar Socken sehen aber beide Socken genau gleich aus. Ich kann also kein Verfahren angeben, dass mir bei unendlich vielen Paaren von Socken aus jedem Paar genau eine spezifische Socke liefert. Daher brauche ich hier das Auswahlaxiom.

So, damit hätten wir alle ZFC-Axiome. Wir wissen bereits, dass es eine Struktur der natürlichen Zahlen in ZFC gibt (dank dem Unendlichkeitsaxiom) und man kann auch zeigen, dass die ganzen, rationalen, reellen, komplexen Zahlen etc. auch alle irgendwie in ZFC beschreibbar sind. Letztenendes lässt sich eben fast jede Form der Mathematik in ZFC beschreiben, weshalb sich ZFC als *das fundamentale Axiomensystem* der modernen Mathematik durchgesetzt hat.

5 Die Gödelschen Unvollständigkeitssätze

Die Peano-Arithmetik und ZFC haben eines gemeinsam, nämlich, dass wir endliche Folgen von Objekten wieder als Objekte codieren können, was es uns letztenendes erlaubt, Formeln und Beweise als Objekte zu codieren, womit wir Formeln bauen können, die über Formeln reden. Das ist die entscheidende Idee im Beweis der Gödelschen Unvollständigkeitssätze – die daraus entstehende Selbstbezüglichkeit. In ZFC ist das trivial – eine endliche Folge von Mengen ist eben per Definition wieder eine Menge. In der Peano-Arithmetik hilft mir dabei die Eindeutigkeit der Primfaktorzerlegung:

Definition 3.5. Sei $(a_1, ..., a_n)$ eine endliche Folge von natürlichen Zahlen und $P = \{p_1, p_2, p_3, ...\} = \{2, 3, 5, 7, 11, ...\}$ die Menge aller Primzahlen. Dann definieren wir

$$\ulcorner(a_1, ..., a_n)\urcorner = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_n^{a_n} = \prod_{i=1}^{n} p_i^{a_i}$$

Beispielsweise gilt $\ulcorner(1, 2, 3, 4, 5)\urcorner = 2^1 \cdot 3^2 \cdot 5^3 \cdot 7^4 \cdot 11^5 = 870037764750$. Die Rechnung alleine ist jetzt nicht soo spannend, allerdings können wir die Funktion auch umkehren! Wir können die Primfaktorzerlegung der Zahl 70037764750 aufstellen und erhalten wieder $2^1 \cdot 3^2 \cdot 5^3 \cdot 7^4 \cdot 11^5$, woraus wir wieder unsere ursprüngliche Folge $(1, 2, 3, 4, 5)$ erhalten. Die Zahl 870037764750 enthält also auf eine gewisse Weise die selbe Information wie die Folge $(1, 2, 3, 4, 5)$.

Was bringt mir das jetzt? Naja, Gödel erkannte, dass mir das erlaubt, jede Menge mathematischer Sachverhalte, wie zum Beispiel Formeln, als Zahlen zu codieren! Aus heutiger Sicht mag das unspannend wirken – Computer tun schließlich nichts anderes, als *alle*

Daten, die irgendwie von ihm verarbeitet werden als Folgen von Nullen und Einsen zu codieren. Und man muss sich nur anschauen, was Computer alles können um zu begreifen, wie viel man dementsprechend mit natürlichen Zahlen ausdrücken kann, wenn man kreativ genug ist.

Gödel war allerdings mehr oder minder der Erste, der realisierte, was das eigentlich bedeutet. Denn er begriff, dass man damit Formeln bauen kann, die über Formeln reden können. Und dann können jede Menge verrückter Dinge passieren. Betrachte folgenden Satz:

> „Dieser Satz ist falsch!“

Ist dieser Satz wahr? Wenn ja, muss er also falsch sein. Ist er aber falsch, muss er wahr sein – wir haben ein Paradoxon!

So ungefähr bastelte Gödel einen Satz, der seine eigene Unbeweisbarkeit behauptet. Das funktioniert folgendermaßen:

Wir wählen irgendeine Signatur L und ordnen jedem Symbol z der Signatur genau eine ungerade natürliche Zahl $\sigma(z)$ zu. Das Selbe machen wir mit jedem Symbol der Prädikatenlogik, wie $\forall, \exists, \wedge, \vee, \rightarrow, (,)$, etc. Damit sollten wir nur endlich viele natürliche Zahlen verbraucht haben, sagen wir, weniger als 100. Dann können wir jeder Variable eine ungerade Zahl größer als 100 zuordnen (womit wir immer noch unendlich viele Variablen benutzen können) und für natürliche Zahlen selbst sagen wir einfach $\sigma(n) = 2n$ – wir haben schließlich bisher nur die ungeraden natürlichen Zahlen benutzt.

Was wir jetzt machen können ist, jede Formel als eine Folge von Symbolen betrachten, also $\varphi = (z_1, z_2, z_3, ..., z_n)$, und diese Folge von Symbolen können wir jetzt mit σ und der obigen Codierung als eine einzelne natürliche Zahl codieren:

$$\ulcorner\varphi\urcorner = \ulcorner(\sigma(z_1), \sigma(z_2), ..., \sigma(z_n))\urcorner$$

Das ganze Verfahren garantiert uns, dass wir aus der Zahl $\ulcorner\varphi\urcorner$ tatsächlich wieder unsere ursprüngliche Formel φ konstruieren können – die „Umwandlung“ in eine natürliche Zahl hat also keinerlei Informationsverlust! Wir nennen die Zahl $\ulcorner\varphi\urcorner$ die *Gödelzahl* von φ und die Codierung von φ als Zahl heißt *Gödelisierung*.

Betrachten wir als Beispiel die Formel $\varphi = \forall x\ (x \doteq 0 \vee \exists y\ x \doteq y + 1)$. Wir weisen folgendermaßen jedem Symbol eine natürliche Zahl zu:

z	$\forall$	$\exists$	(	)	$\vee$	$\doteq$	$+$	x	y	0	1
$\sigma(z)$	1	3	5	7	9	11	13	101	103	0	2

Die Formel φ wird somit zu der Folge $[\forall, x, (, x, \doteq, 0, \vee, \exists, y, x, \doteq, y, +, 1,)]$, die wir mit der Tabelle umwandeln zu

$$(1, 101, 5, 101, 11, 0, 9, 3, 103, 101, 11, 103, 13, 2, 7)$$

Die Folge wiederum wandeln wir um in die Zahl:

$\ulcorner\varphi\urcorner = 2^1 \cdot 3^{101} \cdot 5^5 \cdot 7^{101} \cdot 11^{11} \cdot 13^0 \cdot 17^9 \cdot 19^3 \cdot 23^{103} \cdot 29^{101} \cdot 31^{11} \cdot 37^{103} \cdot 41^{13} \cdot 43^2 \cdot 47^7$

= 341 493 608 908 455 920 890 033 443 243 310 336 855 922 501 791 654 762
770 027 031 892 691 634 843 765 491 516 737 858 538 740 659 915 333 731
850 793 340 225 920 719 618 747 795 053 401 554 840 670 561 552 543 202
149 830 148 115 410 366 276 315 229 039 419 017 775 118 606 544 494 235
302 372 942 101 475 139 284 310 138 126 737 046 554 423 726 868 946 307
855 276 295 553 234 081 485 133 103 770 488 651 445 956 287 607 354 883
904 918 851 878 017 229 233 182 079 097 384 224 235 451 381 491 606 976
035 878 818 450 570 071 277 147 293 193 103 394 212 535 497 953 476 433

282 704 569 728 332 422 490 639 093 883 923 535 173 633 522 777 504 928 774 602 754 992 844 012 801 671 638 297 523 337 480 976 756 455 949 061 021 887 672 365 247 068 665 875 296 404 884 505 647 063 276 139 009 528 712 179 368 353 952 186 006 767 565 299 273 722 667 287 003 493 928 597 196 065 446 771 868 750.
...nicht, dass das konkrete Ergebnis irgendwen interessieren würde, aber jetzt sehen wir: wir haben eine gigantische Zahl, die eindeutig die obige Formel codiert ;-)

Nachdem wir aber *beliebige* Folgen von Zahlen so codieren können, können wir damit auch *ganze Beweise* als Zahlen codieren – Ein Beweis ist schließlich (dank Hilbert-Kalkül) nichts anderes, als eine endliche Folge von Formeln, die wir ja bereits als Zahlen codieren können. Wir können also folgendes Definieren:

Definition 3.6. Wir definieren *bew* als eine zweistellige Relation auf $\mathbb{N}$ so, dass $bew(x, \ulcorner\varphi\urcorner)$ gilt genau dann, wenn die Zahl x einen Beweis für die Formel φ codiert.

So einfach geht das natürlich eigentlich nicht, aber Gödel zeigte, dass diese Relation *bew* tatsächlich *berechenbar* ist – ich kann alleine mit den üblichen Rechenoperationen auf $\mathbb{N}$ stur ausrechnen, ob die Relation $bew(a, b)$ auf zwei beliebige Zahlen a, b zutrifft oder nicht! Das ist natürlich mordsmäßig kompliziert und aufwendig, aber es geht. Insbesondere wird damit eine Formel wie $\exists x\ bew(x, a)$ eine völlig gültige Formel der Prädikatenlogik, die innerhalb der Peano-Axiome definierbar ist. Wir definieren:

$$BEW(a) = \exists y\ bew(y, a)$$

Dann besagt $BEW(a)$ also, dass die Formel mit der Gödelzahl a beweisbar ist. Es gelten nun die folgenden sogenannten *Loeb-Axiome*:

L1 Wenn $PA \vdash \varphi$, dann $PA \vdash BEW(\ulcorner\varphi\urcorner))$

L2 $PA \vdash ((BEW(\ulcorner\varphi\urcorner) \wedge BEW(\ulcorner\varphi \to \psi\urcorner)) \to BEW(\ulcorner\psi\urcorner))$

L3 $PA \vdash (BEW(\ulcorner\varphi\urcorner) \to BEW(\ulcorner BEW(\ulcorner\varphi\urcorner)\urcorner))$

L4 Wenn $PA \vdash (\varphi \to \psi)$, dann $PA \vdash BEW(\ulcorner\varphi\urcorner) \to BEW(\ulcorner\psi\urcorner)$

L5 $PA \vdash (BEW(\ulcorner\varphi \wedge \psi\urcorner) \leftrightarrow (BEW(\ulcorner\varphi\urcorner) \wedge BEW(\ulcorner\psi\urcorner)))$

Genauso zeigte Gödel, dass die folgende Funktion berechenbar ist:

Definition 3.7. Sei $\varphi(x)$ eine Formel mit freier Variable x. *sub* ist die Funktion $\mathbb{N}^2 \to \mathbb{N}$ so, dass $sub(\ulcorner\varphi\urcorner, b) = \ulcorner\varphi\left[\frac{b}{x}\right]\urcorner$.

Die Funktion *sub* nimmt also eine Gödelzahl $\ulcorner\varphi\urcorner$ und eine beliebige andere Zahl b, und liefert uns die Gödelzahl der Formel, die entsteht, wenn wir die freie Variable in φ durch b ersetzen.

Das führt uns zu:

Satz 3.4. *Es gibt eine Formel $\mathcal{G}$ so, dass $\mathcal{G}$ in der Peano-Arithmetik gilt, genau dann, wenn es keinen formalen Beweis für $\mathcal{G}$ aus den Peano-Axiomen gibt.*

Beweis. Betrachte die Formel $\varphi = \neg BEW(sub(x, x))$. Die Formel besagt also „Es gibt keinen Beweis für die Formel, die entsteht, wenn ich in der Formel mit der Gödelzahl x die freie Variable durch x ersetze“. Dann definieren wir jetzt $\mathcal{G} = \varphi\left[\frac{\ulcorner\varphi\urcorner}{x}\right]$ – wir setzen also in der Formel φ für die freie Variable *ihre eigene Gödelzahl ein*! Natürlich gilt jetzt

$\ulcorner\mathcal{G}\urcorner = sub(\ulcorner\varphi\urcorner, \ulcorner\varphi\urcorner)$ und damit $\mathcal{G} = \neg BEW(sub(\ulcorner\varphi\urcorner, \ulcorner\varphi\urcorner))$, also $\mathcal{G} = \neg BEW(\ulcorner\mathcal{G}\urcorner)$. Wir haben also eine Formel, die ihre eigene Unbeweisbarkeit behauptet, und somit

$$PA \vdash (\mathcal{G} \leftrightarrow \neg BEW(\ulcorner\mathcal{G}\urcorner))$$

□

Das führt uns zu den Gödelschen Unvollständigkeitssätzen:

Satz 3.5.

- ***Erster Gödelscher Unvollständigkeitssatz:*** *Entweder PA ist unvollständig oder widerprüchlich.*
- ***Zweiter Gödelscher Unvollständigkeitssatz:*** *Es gibt in PA keinen formalen Beweis, dass PA widerspruchsfrei ist, außer PA ist widersprüchlich.*

Unvollständig bedeutet in dem Kontext: Es gibt eine Formel φ so, dass weder $PA \vdash \varphi$, noch $PA \vdash \neg\varphi$.

Beweis. Wir wissen, dass $PA \vdash (\mathcal{G} \leftrightarrow \neg BEW(\ulcorner\mathcal{G}\urcorner))$.

Angenommen $PA \vdash \mathcal{G}$. Dann gilt also $PA \vdash \neg BEW(\ulcorner\mathcal{G}\urcorner)$. Nach L1 folgt aber aus $PA \vdash \mathcal{G}$ auch $PA \vdash BEW(\ulcorner\mathcal{G}\urcorner)$ – wir erhalten also insbesondere:

$$PA \vdash (BEW(\ulcorner\mathcal{G}\urcorner) \wedge \neg BEW(\ulcorner\mathcal{G}\urcorner))$$

also $PA \vdash \bot$, also ist PA widersprüchlich.

Nehmen wir also an, dass $PA \vdash \neg\mathcal{G}$. Dann erhalten wir per Definition von $\mathcal{G}$ also $PA \vdash BEW(\ulcorner\mathcal{G}\urcorner)$ und wieder mit L1 auch $PA \vdash BEW(\ulcorner\neg\mathcal{G}\urcorner)$. Mit L5 folgt somit $PA \vdash BEW(\ulcorner\mathcal{G} \wedge \neg\mathcal{G}\urcorner)$ und somit $PA \vdash BEW(\ulcorner\bot\urcorner)$. Das ist noch kein direkter Widerspruch, aber wir können uns jetzt überlegen: Es gilt also $PA \vdash \exists y\ bew(y, \ulcorner\bot\urcorner)$, also gibt es eine Zahl y, die einen Beweis für $\bot$ codiert. Entweder ist y eine Standard natürliche Zahl – dann können wir diese „entgödelisieren“ und erhalten einen echten Beweis für $PA \vdash \bot$. Es könnte aber auch sein, dass y eine Nichtstandard-Zahl ist – Dann erzwingt PA aber, dass eine Nichtstandard-Zahl existiert, was der Tatsache widerspricht, dass $\mathbb{N} \models PA$, und $\mathbb{N}$ enthält keine Nichtstandard-Zahlen, Widerspruch.

Also: Entweder ist PA widersprüchlich, oder es gilt weder $PA \vdash \mathcal{G}$, noch $PA \vdash \neg\mathcal{G}$.

Für den zweiten Unvollständigkeitssatz definieren wir die Formel $Con_{PA} = \neg BEW(\ulcorner\bot\urcorner)$, die die Widerspruchsfreiheit von PA ausdrücken soll. Wir können jetzt zeigen, dass diese Formel in PA äquivalent ist zu $\mathcal{G}$:

Zunächst gilt wegen Ex Falso Quodlibet $PA \vdash (\bot \to \varphi)$ für jede Formel φ. Nach L4 gilt also auch

$$PA \vdash (BEW(\ulcorner\bot\urcorner) \to BEW(\ulcorner\varphi\urcorner))$$

und im Umkehrschluss

$$PA \vdash (\neg BEW(\ulcorner\varphi\urcorner) \to \neg BEW(\ulcorner\bot\urcorner))$$

Also: $PA \vdash (\neg BEW(\ulcorner\varphi\urcorner) \to Con_{PA})$. Was Sinn macht: Wenn ich eine Formel *nicht* beweisen kann, muss die Theorie konsistent sein – wär sie's nicht, könnt ich ja nach Ex Falso Quodlibet *jede* Formel beweisen!

Setzen wir jetzt $\varphi = \mathcal{G}$ erhalten wir

$$PA \vdash (\neg BEW(\ulcorner\mathcal{G}\urcorner) \to Con_{PA})$$

und wegen $\mathcal{G} = \neg BEW(\ulcorner\mathcal{G}\urcorner)$ ergo $PA \vdash (\mathcal{G} \to Con_{PA})$.

Außerdem gilt wegen $PA \vdash (\mathcal{G} \rightarrow \neg BEW(\ulcorner\mathcal{G}\urcorner))$ nach L4 auch:

$$PA \vdash (BEW(\ulcorner\mathcal{G}\urcorner) \rightarrow BEW(\ulcorner\neg BEW(\ulcorner\mathcal{G}\urcorner)\urcorner))$$

Und wegen L3 gilt:

$$PA \vdash (BEW(\ulcorner\mathcal{G}\urcorner) \rightarrow BEW(\ulcorner BEW(\ulcorner\mathcal{G}\urcorner)\urcorner))$$

Mit L5 können wir diese zwei Formeln zusammensetzen und erhalten:

$$PA \vdash (BEW(\ulcorner\mathcal{G}\urcorner) \rightarrow BEW(\ulcorner BEW(\ulcorner\mathcal{G}\urcorner) \wedge \neg BEW(\ulcorner\mathcal{G}\urcorner)\urcorner))$$

was äquivalent ist zu $PA \vdash (BEW(\ulcorner\mathcal{G}\urcorner) \rightarrow BEW(\ulcorner\bot\urcorner))$. Wegen $Con_{PA} = \neg BEW(\ulcorner\bot\urcorner)$, $\mathcal{G} = \neg BEW(\ulcorner\mathcal{G}\urcorner)$ und Kontraposition folgt also

$$PA \vdash (Con_{PA} \rightarrow \mathcal{G})$$

Somit gilt $PA \vdash (Con_{PA} \leftrightarrow \mathcal{G})$, und somit würde aus $PA \vdash Con_{PA}$ folgen $PA \vdash \mathcal{G}$, Widerspruch zum ersten Unvollständigkeitssatz. □

Wir haben also eine Formel $\mathcal{G}$ gefunden, die *unabhängig* von PA ist. Das ist erstmal kein Problem – wir können ja einfach entweder $\mathcal{G}$ oder $\neg\mathcal{G}$ als neues Axiom hinzufügen und erhalten eine neue Theorie PA'. Vielleicht ist die ja dann vollständig?

Die Antwort lautet nein. Denn in diesem neuen Axiomensystem PA' können wir genau den selben Spaß wieder fabrizieren und erhalten eine neue Formel $\mathcal{G}'$, die unabhängig von PA' ist. Jede (rekursive) Erweiterung von PA ist und bleibt entweder unvollständig oder widersprüchlich.

Auch das macht aber ja eigentlich nichts, denn wir haben ja ZFC. Und in ZFC haben wir die Menge ω, die ein Modell der Peano-Arithmetik ist. In ZFC können wir damit beweisen, dass PA widerspruchsfrei ist, denn wir haben ja ein Modell!

So weit so gut, allerdings können wir auch in ZFC genau das selbe machen, was wir hier mit PA gemacht haben – Formeln als Mengen codieren, die Relationen *bew* und BEW definieren und den selben Beweis wieder durchexerzieren. Die beiden Unvollständigkeitssätze gelten also für ZFC genauso wie für PA. Und genauso wie für PA und ZFC gelten die Unvollständigkeitssätze für jede beliebige Axiomensystem, das mindestens so „mächtig“ ist wie PA – und das ist jawohl das mindeste, was man von einem Kandidaten für ein fundamentales Axiomensystem erwarten können sollte. Daran muss man sich einfach gewöhnen, und wie bereits gesagt:

> „In der Mathematik **versteht** man Dinge nicht – man **gewöhnt** sich einfach an sie.“
> - *John von Neumann*