Mengenlehre und Logik

1 Was sind Mengen?

Die Welt, in der wir leben, enthält viele verschiedene Objekte. Wir benutzen Worte, um Gedanken über diese Objekte zu formulieren. Zum Beispiel sind typische Worte für Objekte: "Apfel", "Birne", "Auto", "Tisch", "Haus", u.s.w. Aber man sieht sofort, daß diese Worte eigentlich nicht die *einzelnen* Objekte beschreiben. Vielmehr sind es Worte, die allgemeine *Klassen* von Objekten beschreiben. Es gibt kein besonderes Wort, daß gerade den Tisch, an dem Sie momentan sitzen, bezeichnet. Das Wort "Tisch" bezeichnet jeden Tisch. Daher ist es für uns eine Selbstverständlichkeit, die verschiedenen Gegenstände, denen wir begegnen, in allgemeine Klassen einzuordnen.

Für Platon war die "Form" einer Sache das Wesentliche. Zum Beispiel ist die geometrische Idee eines Kreises etwas, das jeder kennt. Wenn ich versuchen würde, einen Kreis auf die Tafel zu zeichnen, dann würden Sie feststellen, daß mein Kreis falsch ist. Wackelig. Nicht ganz rund. Nur eine Annährung an den perfekten, idealen Kreis. Platon glaubte, daß jeder Mensch schon im voraus alle Formen der Natur kennt. Das einzige, was ein Lehrer zu tun hat, ist zu versuchen, die Formen beim Schüler wieder in Erinnerung zu rufen.

Die Arithmetik geht eine Stufe weiter. Eine Zahl ist eine noch abstraktere Klasse von Dingen. Nehmen wir zum Beispiel die Zahl 3. Das bedeutet nicht etwa drei Äpfel, oder drei Birnen. Nein, "3" ist eine Klasse von Klassen. Nämlich die Klasse aller Sammlungen — oder sagen wir lieber "Mengen" — die drei Objekte enthalten. Die Zahl 3 bezeichnet etwas Abstraktes. Wir können, wie bei Platon, über die "Form" 3 reden, ohne gleichzeitig an Äpfel oder Birnen zu denken.

Nun, das Wort "Menge" bezeichnet im alltäglichen Gebrauch eine Sammlung von spezifischen Objekten. Etwa eine besondere Menge von Äpfeln, die man gerade nach Hause trägt. Manchmal werden Mengen durch die darin enthaltenen Objekte bezeichnet, etwa

- $\{2, 3, 5, 7, 11, \dots\}$, oder
- $\{Apfel, Birne, Kirsche\}$, oder
- $\{rot, gelb, grün\}$, u.s.w.

Wenn wir aber die Theorie der Mengenlehre studieren, dann ist auch eine Menge eine abstrakte, ideale Form. Warum sollten wir etwa die zwei Mengen $\{Apfel, Birne, Kirsche\}$ und $\{rot, gelb, grün\}$ auseinander halten? Wie wir gerade gesehen haben, ist die Zahl 3 noch abstrakter, idealer als die Gedanken "drei Früchte" oder "drei Farben". Genauso müssen wir sagen, daß die zwei Mengen $\{Apfel, Birne, Kirsche\}$ und $\{rot, gelb, grün\}$ eigentlich einer abstrakten Klasse angehören, nämlich der Klasse aller Sammelungen von Objekten, die drei Dinge enthalten.

Daher wird in der abstrakten Mengenlehre eine einfache Vereinbarung getroffen. Statt über komplizierte Objekte wie "Kirsche", oder die Eigenschaft "rot" zu reden, wird vereinbart, nur über Mengen zu reden. Eine Menge enthält zwar Elemente, aber diese Elemente sind dann selbst abstrakte Mengen.

Es gibt eine besondere Menge, die leere Menge, die mit dem Symbol $\emptyset$ bezeichnet wird. Alle weiteren Mengen werden dann mit Hilfe von $\emptyset$ konstruiert. Hier sind Beispiele einiger verschiedener Mengen.

- $\emptyset$,
- $\{\emptyset\}$,
- $\{\emptyset, \{\emptyset\}\}$,
- $\{\{\emptyset, \{\emptyset\}\}, \{\emptyset\}\}$, u.s.w.

Diese Schreibweise ist sicherlich ziemlich umständlich. Daher werden Variablen benutzt, die stellvertretend für Mengen sind. Zum Beispiel, wenn wir vereinbaren, daß $a = \emptyset$ und $b = \{\emptyset\}$ sind, dann ist die Menge

$$\{\{\emptyset, \{\emptyset\}\}, \{\emptyset\}\}$$

einfacher zu schreiben als $\{\{a, b\}, b\}$.

2 Die Axiome der Mengenlehre

Zuerst zur Notation. Seien A und B Mengen.

- Falls x ein Element von A ist, dann schreibt man $x \in A$. Falls x *kein* Element von A ist, dann schreibt man $x \notin A$.
- $A \cup B$ ist die Vereinigung von A und B. D.h. die Menge aller Elemente x, wobei entweder $x \in A$ oder $x \in B$.
- $A \cap B$ ist der Durchschnitt von A und B. D.h. die Menge aller Elemente x, wobei sowohl $x \in A$ als auch $x \in B$.
- $A \setminus B$ ist die Differenz von A und B. D.h. die Menge aller Elemente x, wobei $x \in A$ und $x \notin B$.
- $A \subset B$ heißt A ist eine Teilmenge von B. D.h. falls $x \in A$, dann ist auch $x \in B$. Manchmal wird auch $A \subseteq B$ geschrieben, um die Möglichkeit, daß A gleich B sein kann, zu betonen.
- Das Standardsymbol "$\forall$" kommt in dieser Theorie öfters vor. "$\forall$" heißt "für alle".
- "$\exists$" heißt "es existiert".

Die folgenden Axiome (von Zermelo und Fraenkel) werden üblicherweise benutzt, um die Theorie der Mengen festzulegen.

1. **Axiom der Leermenge**: Die Menge $\emptyset$ existiert. $\emptyset$ enthält keine Elemente.

2. **Axiom der Extensionalität**: Zwei Mengen sind gleich genau dann, wenn sie dieselben Elemente enthalten.

3. **Axiom der Paare**: Falls A und B Mengen sind, dann gibt es eine Menge C, die genau die Mengen A und B als Elemente enthält. D.h. $C = \{A, B\}$.

4. **Axiom der Vereinigung**: Gegeben eine Menge A, dann gibt es eine weitere Menge B, deren Elemente genau die Elemente von Elementen aus A sind. Man schreibt

$$\cup A = B = \cup_{x \in A} x = \{z \in x : x \in A\}.$$

Z.B. wenn $A = \{\{a, b\}, \{a, c\}\}$ ist, dann ist $\cup A = \{a, b, c\}$.

5. **Axiom der Unendlichkeit**: Es gibt eine Menge A, die $\emptyset$ enthält, und falls x ein Element von A ist, dann ist auch die Menge $x \cup \{x\}$ ein Element von A.

6. **Axiom der Potenzmenge**: Für jede Menge A gibt es eine weitere Menge P, wobei die Elemente von P genau die Teilmengen von A sind.

   Eine *Teilmenge* $B \subset A$ hat die Eigenschaft: falls $x \in B$, dann ist auch $x \in A$.

7. **Axiom der Regularität**: Jede nichtleere Menge A enthält ein Element B, so daß A und B disjunkt sind.

   (Die Mengen A and B heißen *disjunkt*, falls $A \cap B = \emptyset$.)

8. **Aussonderungsaxiom**: Angenommen, eine "Eigenschaft" (oder *Funktion*) ϕ sei vorgegeben mit den Werten "wahr" oder "falsch", wobei für alle Mengen x gilt, entweder $\phi(x)$ ist wahr oder $\phi(x)$ ist falsch. Dann ist für jede Menge A die Menge aller $x \in A$, wobei $\phi(x)$ wahr ist, tatsächlich eine Menge. Man schreibt

$$\{x \in A : \phi(x)\}.$$

9. **Auswahlaxiom**: Angenommen, A ist eine Menge von paarweise disjunkten nichtleeren Mengen. Dann gibt es eine Menge, die genau ein Element aus jedem Element von A enthält.

3 Die "naive" Mengenlehre

Warum ist gerade das Axiomensystem von Zermelo-Fraenkel das richtige? Woher kommt es überhaupt? Vielleicht ist es das beste, wenn wir zunächst einfach versuchen, einiges über Mengen zu verstehen, ohne uns um diese komplizierten Axiome viele Gedanken zu machen.

Definition 1. *Seien A und B Mengen. Eine* Abbildung $f : A \to B$ *ist eine Zuordnung der Elemente aus A zu Elementen aus B. D.h. für jedes Element $a \in A$ gibt es ein eindeutiges Element $f(a) \in B$. Die Teilmenge $f(A) \subset B$ ist die Menge $\{f(a) : a \in A\}$.*

Beispiel 1. *Seien A und B beide gleich die Menge der (natürlichen) Zahlen $\mathbb{N} = \{1, 2, 3, 4, \dots\}$. Für jedes $n \in \mathbb{N}$ sei $f(n) = n^2$. Dann ist f eine Abbildung von $\mathbb{N}$ nach $\mathbb{N}$. In diesem Fall sagt man auch, daß es sich um eine Abbildung von $\mathbb{N}$ in sich selbst handelt*

Definition 2. *Sei $f : A \to B$ eine Abbildung.*

- *Falls aus $a_1, a_2 \in A$ mit $a_1 \neq a_2$ stets folgt $f(a_1) \neq f(a_2)$, dann heißt f eine* Injektion.
- *Falls für jedes Element $b \in B$ ein entsprechendes Element $a \in A$ existiert mit $f(a) = b$, dann heißt f eine* Surjektion.

Satz 1. *Sei $f : A \to B$ eine Abbildung, wobei $A \neq \emptyset \neq B$.*

- *Falls f eine Injektion ist, dann existiert auch eine Surjektion $g : B \to A$.*
- *Falls f eine Surjektion ist, dann existiert auch eine Injektion $h : B \to A$.*

Beweis. Zunächst sei $f : A \to B$ eine Injektion. Eine Surjektion $g : B \to A$ wird wie folgt konstruiert. Da $A \neq \emptyset$, wähle ein Element $a_0 \in A$. Dann gibt es für jedes Element $b \in B$ zwei Möglichkeiten.

1. Falls ein Element $a \in A$ existiert mit $f(a) = b$, dann sei $g(b) = a$. Bemerkung: Da f eine Injektion ist, ist das Element $a \in A$ eindeutig festgelegt.
2. Andernfalls gibt es kein solches Element von A. In diesem Fall sei $g(b) = a_0$.

Warum ist die so definierte Abbildung $g : B \to A$ eine Surjektion? Nun, sei $a \in A$ irgendein beliebiges Element von A. Dann ist $f(a)$ irgendein Element von B. Und nach unsere Konstruktion ist dann $g(f(a)) = a$.

Andererseits, falls $f : A \to B$ eine Surjektion ist, dann gibt es für jedes $b \in B$ mindestens ein entsprechendes $a_b \in A$ mit $f(a_b) = b$. Wähle irgendein solches $a_b \in A$, und sei dann $h(b) = a_b$. Dadurch wird eine Abbildung $h : B \to A$ definiert. Offensichtlich ist h eine Injektion. □

Bemerkung. *Es ist eine interessante Übung, zu überlegen, welche Axiome hier in diesem Beweis eigentlich benötigt werden. Zum Beispiel wird bei der Konstruktion von h das Auswahlaxiom benutzt.*

Wenn die Menge A (und/oder B) endlich ist, dann ist klar, daß A größer oder zumindest gleich groß ist wie B, falls eine Surjektion $f : A \to B$ existiert. Nach unserem Satz ist demzufolge auch A kleiner, oder zumindest gleich klein, falls eine entsprechende Injektion existiert. Um diese Idee auszudrücken, werden wir die folgende Notation benutzen. Wir schreiben

$$A \preceq B$$

wenn eine Injektion von A nach B existiert. Umgekehrt werden wir schreiben $A \succeq B$, falls eine Surjektion von A nach B existiert. Wir werden diese Schreibweise auch benützen, wenn sowohl A als auch B unendlich groß sind.

Nun, manches widerspricht der einfachen Intuition, wenn es sich um unendlich große Mengen handelt.

Beispiel 2. *Sei $G = \{2, 4, 6, 8, \dots\}$ die Menge der positiven geraden Zahlen. Die Abbildung $f : \mathbb{N} \to G$ sei gegeben durch $f(n) = 2n$, für alle $n \in \mathbb{N}$. Dann ist f eine Injektion. D.h. $\mathbb{N} \preceq G$, obwohl G doch nur die Hälfte aller Zahlen in $\mathbb{N}$ enthält!*

Auf der anderen Seite ist die Inklusionsabbildung $i : G \to \mathbb{N}$ mit $i(g) = g$ für alle $g \in G$ eine Injektion. Daher ist auch $G \preceq \mathbb{N}$.

Definition 3. *Falls $f : A \to B$ sowohl eine Injektion als auch eine Surjektion ist, dann heißt f eine* Bijektion.

Satz 2 (Schröder-Bernstein)**.** *Angenommen, A und B sind nicht-leere Mengen, wobei sowohl eine Injektion $f : A \to B$ als auch eine Surjektion $g : A \to B$ existieren. Dann existiert eine Bijektion $h : A \to B$.*

Beweis. Da eine Surjektion von A nach B existiert, gibt es auch eine Injektion $k : B \to A$. Nun sei $a \in A$ ein beliebiges Element aus A. Falls $a \in k(B)$, dann gibt es ein eindeutiges Element $k^{-1}(a) \in B$. Falls $k^{-1}(a) \in f(A)$, dann gibt es ein eindeutiges Element $f^{-1}(k^{-1}(a)) \in A$. Im allgemeinen gibt es eine Kette von Elementen

$$\{a, k^{-1}(a), f^{-1}(k^{-1}(a)), k^{-1}(f^{-1}(k^{-1}(a))), \dots\}.$$

Vielleicht ist diese Kette nur endlich lang, wobei wir ein Element erreichen, das weder in $f(A)$ noch in $k(B)$ liegt. Andernfalls ist die Kette unendlich lang. Daher haben wir zwei verschiedene Teilmengen von A:

- Sei nämlich A_1 die Menge aller $a \in A$, wobei die Kette, die mit a anfängt, nur endlich lang ist.
- Dann ist $A_2 = A \setminus A_1$ die Menge aller Elemente mit unendlich langen Ketten.

Wir zerlegen auch die Teilmenge A_1 in zwei weitere Teilmengen, und zwar

- A_1^1 ist die Menge aller $a \in A_1$, wobei das letzte Glied der Kette in A liegt.
- A_1^2 ist die Menge aller $a \in A_1$, wobei das letzte Glied der Kette in B liegt.

Die Bijektion $h : A \to B$ wird dann wie folgt festgelegt,

$$h(a) = \begin{cases} f(a), & \text{falls } a \in A_2 \cup A_1^1, \\ k^{-1}(a), & \text{falls } a \in A_1^2. \end{cases}$$

Ist h tatsächlich eine Bijektion? Nun, sei $b \in B$ ein beliebiges Element von B. Um zu zeigen, daß h eine Surjektion ist, genügt es, zu zeigen, daß $b \in h(A)$.

- Falls $k(b) \in A_1^2$, dann ist $h(k(b)) = k^{-1}(k(b)) = b$. Daher ist $b \in h(A)$.
- Sonst ist $k(b) \in A_2 \cup A_1^1$. Daher muß die Kette, die mit $k(b)$ anfängt, auch wieder zurück in A springen. D.h. ein $a \in A$ existiert, mit $a = f^{-1}(k^{-1}(k(b))) = f^{-1}(b)$. Dann ist $h(a) = f(a) = f(f^{-1}(b)) = b$. Folglich ist auch in diesem Fall $b \in h(A)$.

Ist h auch eine Injektion? Seien $a_1, a_2 \in A$ mit $h(a_1) = h(a_2)$. D.h. sei $h(a_1) = h(a_2) = b \in B$.

Falls beide a_1 und a_2 zusammen in der Menge $A_2 \cup A_1^1$ liegen, dann gilt $h(a_1) = f(a_1)$ und $h(a_2) = f(a_2)$. Aber f ist eine Injektion. Daher ist $a_1 = a_2$.

Falls beide a_1 und a_2 zusammen in der Menge A_1^2 liegen, dann gilt $h(a_1) = k^{-1}(a_1)$ und $h(a_2) = k^{-1}(a_2)$. Aber auch k^{-1} ist eine Injektion. Daher ist wieder $a_1 = a_2$.

Schließlich, falls etwa $a_1 \in A_2 \cup A_1^1$ und $a_2 \in A_1^2$, dann betrachten wir das Element $k(b) \in A$. Da $b = h(a_2) = k^{-1}(a_2)$, aber auch $k^{-1}(k(b)) = b$, und k^{-1} eine Injektion ist, muß gelten $k(b) = a_2$. Andererseits gilt $h(a_1) = f(a_1) = b$. D.h. $f^{-1}(b) = f^{-1}(k^{-1}(a_2)) = a_1$. Daher muß die Kette, die mit a_2 anfängt, doch auch durch a_1 führen. Folglich muß auch $a_2 \in A_2 \cup A_1^1$. Ein Widerspruch. Daher kann dieser Fall gar nicht vorkommen. □

Satz 3 (Cantor)**.** *Sei A eine nicht-leere Menge und sei $P(A)$ die Potenzmenge von A. D.h. $P(A)$ ist die Menge aller Teilmengen von A. Dann gibt es* keine *Surjektion $A \to P(A)$. Wir können auch schreiben $P(A) \not\preceq A$.*

Beweis. Um einen Widerspruch zu finden, sei doch angenommen, daß eine Surjektion $f : A \to P(A)$ existiert. D.h. für alle $a \in A$ ist $f(a)$ irgendeine Teilmenge von A. Wir können insbesondere die Teilmenge

$$S = \{a \in A : a \notin f(a)\}$$

betrachten.[1] Da f eine Surjektion ist, muß irgendein Element $a_0 \in A$ existieren, mit $f(a_0) = S$. Die Frage ist nun, ob a_0 ein Element von S ist, oder auch nicht.

- Falls $a_0 \in S$, dann ist $a_0 \in f(a_0) = S$. Daher, nach der Definition von S, gilt $a_0 \notin S$.
- Andernfalls, ist $a_0 \notin S = f(a_0)$. Aber wieder nach der Definition von S muß gelten $a_0 \in S$.

Beides führt zum Widerspruch. □

Definition 4. *Falls A und B Mengen sind und* keine *Surjektion $A \to B$ existiert, dann sagt man, daß die* Kardinalität *von A kleiner ist als die* Kardinalität *von B. Man schreibt $A \prec B$. Andernfalls, wenn eine Bijektion zwischen A und B existiert, dann schreibt man $\overline{\overline{A}} = \overline{\overline{B}}$. D.h. A und B besitzen dieselbe Kardinalität.*

4 Wie groß sind $\mathbb{N}$, $\mathbb{Q}$ und $\mathbb{R}$?

Hier ist $\mathbb{N}$ die Menge der natürlichen Zahlen $\{1, 2, 3, \dots\}$. Die Menge aller ganzen Zahlen heißt $\mathbb{Z}$, wobei

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Daher ist offensichtlich, daß $\mathbb{N} \subset \mathbb{Z}$.

Definition 5. *Die Menge der rationalen Zahlen $\mathbb{Q}$ ist die Menge aller Zahlen der Art $\frac{a}{b}$, wobei $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$. (Natürlich ist diese Darstellung im allgemeinen nicht eindeutig. Z.B. sind $\frac{1}{2}$ und $\frac{2}{4}$ zwei verschiedene Darstellungen derselben rationalen Zahl.)*

[1] Es kann sein, daß $S = \emptyset$. Aber die leere Menge ist auch eine Teilmenge von A. D.h. $\emptyset \in P(A)$.

Satz 4. *Es gilt* $\overline{\overline{\mathbb{N}}} = \overline{\overline{\mathbb{Q}}}$. *Mit anderen Worten, es gibt eine Bijektion zwischen* $\mathbb{N}$ *und* $\mathbb{Q}$.

Beweis. Es genügt, eine Injektion $f : \mathbb{N} \to \mathbb{Q}$ und eine Surjektion $g : \mathbb{N} \to \mathbb{Q}$ zu finden. Die Injektion ist trivial. Wir brauchen nur $f(n) = n$ für alle $n \in \mathbb{N}$ zu nehmen.

Eine Surjektion $g : \mathbb{N} \to \mathbb{Q}$ zu finden ist etwas komplizierter. Wir schreiben zunächst alle möglichen rationalen Zahlen in eine unendlich große Tabelle, wie folgt.

$$\begin{array}{ccccccc}
\frac{0}{1} & \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \cdots \\
\frac{-1}{1} & \frac{0}{2} & \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \cdots \\
\frac{-2}{1} & \frac{-1}{2} & \frac{0}{3} & \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \cdots \\
\frac{-3}{1} & \frac{-2}{2} & \frac{-1}{3} & \frac{0}{4} & \frac{1}{4} & \frac{2}{4} & \cdots \\
\frac{-4}{1} & \frac{-3}{2} & \frac{-2}{3} & \frac{-1}{4} & \frac{0}{5} & \frac{1}{5} & \cdots \\
\frac{-5}{1} & \frac{-4}{2} & \frac{-3}{3} & \frac{-2}{4} & \frac{-1}{5} & \frac{0}{6} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Dann müssen wir einfach systematisch durch diese Tabelle gehen. Etwa in der Reihenfolge

$$\frac{0}{1}, \quad \frac{1}{1}, \quad \frac{-1}{1}, \quad \frac{2}{1}, \quad \frac{0}{2}, \quad \frac{-2}{1}, \quad \frac{3}{1}, \quad \frac{1}{2}, \quad \frac{-1}{2}, \quad \frac{-3}{1}, \quad \frac{4}{1}, \quad \text{u.s.w.}$$

$g(n)$ ist dann die n-te rationale Zahl in dieser Reihenfolge. D.h. $g(1) = \frac{0}{1}$, $g(2) = \frac{1}{1}$, $g(3) = \frac{-1}{1}$, $g(4) = \frac{2}{1}$, u.s.w. $\square$

Wie ist es mit den reellen Zahlen?. Nun, wie wir alle wissen, werden diese Zahlen meistens als Dezimalzahlen dargestellt. Zum Beispiel die bekannte Zahl Pi ist

$$3,141592653589793\ldots$$

Wir können eigentlich sagen, daß diese Zahl aus zwei getrennten Teilen besteht. Zuerst kommt eine *endliche* Liste von Ziffern vor dem Komma: in diesem Falle nur die $\{3\}$. Dann kommt eine *unendliche* Folge von Ziffern nach dem Komma: in diesem Falle die Liste

$$\{1,4,1,5,9,2,6,5,3,5,8,9,7,9,3,\ldots\}$$

Aber auch jede einfache Zahl, etwa die 1, kann als ein solches Paar von Listen dargestellt werden. Hier hätten wir die Darstellung

$$1 = 1,0000000\cdots = [\{1\},\ \{0,0,0,0,0,0,0,0\ldots\}]$$

Nach diesem Schema ist dann auch

$$\pi = [\{3\},\ \{1,4,1,5,9,2,6,5,3,5,8,9,7,9,3,\ldots\}].$$

Definition 6. *Die Menge der reellen Zahlen* $\mathbb{R}$ *ist die Menge aller Ziffernpaare, wobei die erste Liste von Ziffern (mit Vorzeichen) endlich ist, während die zweite Liste unendlich lang ist.*[2]

Satz 5. $\mathbb{N} \prec \mathbb{R}$.

Beweis. Um einen Widerspruch zu finden, sei doch angenommen, daß eine Surjektion $f : \mathbb{N} \to \mathbb{R}$ existiert. Dann ist $f(n)$ die n-te reelle Zahl, und dadurch werden *alle* möglichen reellen Zahlen aufgezählt. Sei etwa $f(n) = r_n \in \mathbb{R}$. Diese reelle Zahl r_n kann in unserem Schema wie folgt dargestellt werden.

$$r_n = [\{r_{n,-m_n}, r_{n,-m_n+1}, \dots, r_{n,-1}\},\ \{r_{n,1}, r_{n,2}, r_{n,3}, \dots\}]$$

Der Widerspruch besteht darin, daß es sehr einfach ist, eine reelle Zahl zu finden, die verschieden ist von *allen* möglichen r_n. Wir brauchen nur die Zahl

$$s = [\{0\},\ \{s_1, s_2, s_3, \dots\}]$$

zu nehmen, wobei für jedes i die Ziffer s_i anders ist als die Ziffer $r_{i,i}$. Ganz offensichtlich ist dann $s \neq r_n$ für alle n, da zumindest an der n-ten nach-Komma Stelle die zwei Zahlen verschieden sind. $\square$

5 Russel's Paradoxon

Die Menge aller positiven ganzen Zahlen $\mathbb{N}$ ist natürlich unendlich groß. Aber wie wir gerade gesehen haben, ist $\mathbb{R} \succ \mathbb{N}$, daher ist $\mathbb{R}$ noch größer. Es gilt auch, daß die Potenzmenge $P(\mathbb{N}) \succ \mathbb{N}$. Aber dann ist die Potenzmenge von der Potenzmenge immer noch größer: $P(P(\mathbb{N})) \succ P(\mathbb{N}) \succ \mathbb{N}$. Es gibt daher eine *unendliche* Folge von immer größeren unendlichen Mengen.

$$\mathbb{N} \prec P(\mathbb{N}) \prec P(P(\mathbb{N})) \prec P(P(P(\mathbb{N}))) \prec P(P(P(P(\mathbb{N})))) \prec \cdots .$$

Wo endet das alles? Die einfachste Idee ist zu sagen, daß alle möglichen Mengen enthalten sind in einer *Universalmenge* $\mathcal{U}$, nämlich die Menge *aller* Mengen.

Nun, wenn wir annehmen, daß $\mathcal{U}$ wirklich eine Menge ist, dann können wir die folgende Frage stellen. Wir unterscheiden zwei verschiedene Typen von Mengen.

- Die "guten" Mengen A sind so, daß $A \notin A$.
- Die "schlechten" Mengen B sind hingegen so, daß $B \in B$.

Wir interessieren uns insbesondere für die Menge G *aller* guten Mengen. (Falls $\mathcal{U}$ eine Menge ist, dann ist G einfach eine Teilmenge von $\mathcal{U}$.[3]) Die Frage ist nun, ist G selbst gut oder schlecht?

[2] Um die Zweideutigkeit etwa zwischen den zwei Darstellungen $1,00000000\dots$ und $0,99999999\dots$ auszuschließen, wird angenommen, daß die zweite Liste nicht in einer unendlichen 9er-Folge endet.

[3] Wir benutzen hier das Aussonderungsaxiom, was sicherlich ein wesentlicher Bestandteil jeder "naiven" Mengenlehre sein muß.

- Falls G gut ist, dann ist $G \notin G$. Aber $\mathcal{U} \setminus G = S$. Daher folgt $G \in S$. D.h. G ist schlecht.
- Falls G schlecht ist, dann ist $G \in G$. D.h. G ist gut. Wieder ein Widerspruch.

Was können wir aus Russel's Paradoxon schließen? Es ist klar, daß die "Menge aller Mengen" nicht existieren kann. Gödel hat ein anderes Axiomensystem eingeführt, wobei nicht nur Mengen, sondern auch "Klassen" vorkommen. In Gödel's System ist dann die *Klasse* aller Mengen eine zulässige Idee. Eine Klasse enthält Elemente genauso wie Mengen, und jedes Element in einer Klasse ist wiederum eine Menge. Mehr noch, jede Menge ist auch eine Klasse.

Für uns ist wichtig festzuhalten, daß im allgemeinen ein Aussage von der Art "Die Menge aller Mengen mit der Eigenschaft xxx" unzulässig ist. Nach dem Aussonderungsaxiom ist jedoch die Aussage "Sei A eine Menge. Dann ist B die Menge aller Elemente von A mit der Eigenschaft xxx" doch zulässig. Dieses Axiom ist von Ernst Zermelo eingeführt. Später hat A. Fraenkel gezeigt, daß ein noch allgemeineres Axiom — das "Ersetzungsaxiom" — stattdessen auch funktioniert.

6 Geordnete Mengen

Definition 7. *Seien A und B Mengen. Das Kartesische Produkt $A \times B$ ist die Menge aller Paare (a, b), wobei $a \in A$ und $b \in B$.*

Definition 8. *Sei A eine Menge. Eine* Halbordnung *auf A ist eine Teilmenge $\mathcal{O} \subset A \times A$, wobei*

1. *$(a, a) \in \mathcal{O}$, für alle $a \in A$.*
2. *Falls $(a_1, a_2) \in \mathcal{O}$ und $(a_2, a_1) \in \mathcal{O}$, dann folgt $a_1 = a_2$.*
3. *Falls $(a_1, a_2) \in \mathcal{O}$ und $(a_2, a_3) \in \mathcal{O}$, dann folgt auch $(a_1, a_3) \in \mathcal{O}$.*

Falls auch für alle a_1, $a_2 \in A$ gilt: entweder $(a_1, a_2) \in \mathcal{O}$ oder $(a_2, a_1) \in \mathcal{O}$, dann heißt die Ordnung eine totale *(oder* lineare*) Ordnung.*

Eigentlich ist es üblicher, eine Ordnung auf einer Menge mit dem Symbol "$\leq$" zu bezeichnen. Daher wird statt $(a_1, a_2) \in \mathcal{O}$ normalerweise $a_1 \leq a_2$ geschrieben. Man schreibt auch $a_1 < a_2$ wenn klar ist, daß auch $a_1 \neq a_2$. Die *geordnete Menge A* zusammen mit der Ordnung "$\leq$" wird oft als Paar $(A, \leq)$ geschrieben.

Gegeben zwei geordnete Mengen $(A_1, \leq_1)$ und $(A_2, \leq_2)$; eine Abbildung $f : A_1 \to A_2$ heißt *ordnungstreu*, falls $f(x) \leq_2 f(y)$ genau dann, wenn $x \leq_1 y$, für alle x, $y \in A_1$.

Definition 9. *Sei wiederum A eine Menge. Eine* Wohlordnung *auf A ist eine Halbordnung, wobei in dieser Halbordnung jede Teilmenge $B \subset A$ ein kleinstes Element besitzt. D.h. es existiert ein Element $b_0 \in B$, wobei für alle $b \in B$ gilt $b_0 \leq b$. Die Menge A zusammen mit einer Wohlordnung heißt eine* wohlgeordnete Menge.

Bemerkung. *Eine Wohlordnung ist immer eine totale Ordnung. Denn gegeben a_1, $a_2 \in A$, dann ist auch $\{a_1, a_2\} \subset A$ eine Teilmenge. Wenn etwa a_1 das kleinste Element der Teilmenge wäre, dann würde gelten $a_1 \leq a_2$. Umgekehrt, wenn a_2 das kleinste Element ist, dann gilt $a_2 \leq a_1$.*

Der berühmte *Wohlordnungssatz* besagt, daß jede Menge eine Wohlordnung besitzt. Zur Vorbereitung brauchen wir den folgenden Satz über *Anfangssegmente*. Zuerst

Definition 10. *Sei $(T, \leq)$ eine totalgeordnete Menge. Die Teilmenge $S \subset T$ heißt* Anfangssegment*, falls für alle $s \in S$ gilt $\{r \in T : r < s\} \subset S$.*

Definition 11. *Dieses Mal sei $(T, \leq)$ eine wohlgeordnete Menge. Sei $W \subset T$, wobei*

$$B = \{x \in T : w < x, \forall w \in W\} \neq \emptyset.$$

Dann ist $B \subset T$ eine Teilmenge, und da $(T, \leq)$ wohlgeordnet ist, gibt es ein kleinstes Element t_0 von B. Dieses kleinste Element t_0 heißt das Supremum *von W, geschrieben $Sup(W)$.*

Satz 6. *Seien $(Y_1, \leq_1)$ und $(Y_2, \leq_2)$ wohlgeordnete Mengen. Dann gibt es entweder eine eindeutige ordnungstreue Abbildung $Y_1 \to Y_2$ auf ein Anfangssegment von Y_2, oder umgekehrt.*[4] *(Einfachheitshalber werden wir eine ordnungstreue Abbildung auf ein Anfangssegment eine "gute Abbildung" nennen.)*

Beweis. Um die Eindeutigkeit zu zeigen, sei angenommen, daß $f : Y_1 \to Y_2$ eine gute Abbildung ist. Behauptung: es gilt $f(x) = Sup(\{f(u) : u <_1 x\})$ für alle $x \in Y_1$. Dies folgt, da

- $f(u) \leq_2 f(x)$ für alle $u \in Y_1$ mit $u \leq_1 x$, denn f ist ordnungstreu. Folglich muß $f(x) \geq_2 Sup(\{f(u) : u <_1 x\})$.
- Andererseits, sei $t = Sup(\{f(u) : u <_1 x\})$. Falls $f(x) >_2 t$, dann gibt es ein $x_1 <_1 x$ in Y_1 mit $f(x_1) = t$. Aber das heißt $t \in \{f(u) : u <_1 x\}$, ein Widerspruch.

Nun können wir die Eindeutigkeit von f beweisen. Denn falls $f_1, f_2 : Y_1 \to Y_2$ zwei verschiedene gute Abbildungen sind, sei

$$U = \{x \in Y_1 : f_1(x) \neq f_2(x)\}.$$

Sei x_0 das kleinste Element von U. Dann gilt

$$f_1(x_0) = Sup(\{f_1(u) : u <_1 x_0\}) = Sup(\{f_2(u) : u <_1 x_0\}) = f_2(x_0),$$

ein Widerspruch.

Es bleibt, die Existenz einer guten Abbildung zu beweisen. Im allgemeinen, falls X_1 und X_2 totalgeordnete Mengen sind und $f : X_1 \to X_2$ eine gute Abbildung ist, dann ist für jedes Anfangssegment $B \subset X_1$ auch $f(B)$ ein Anfangssegment von X_2. Insbesondere ist die eingeschränkte Abbildung $f_{|B} : B \to X_2$ auch eine gute Abbildung.

[4] D.h. $f(Y_1) = \{f(y) : y \in Y_1\} \subset Y_2$ ist ein Anfangssegment von Y_2, oder umgekehrt.

Sei nun $C \subset Y_1$ die Menge aller $x \in Y_1$, wobei eine gute Abbildung vom Anfangssegement $B_x = \{u \in Y_1 : u \leq_1 x\}$ nach Y_2 existiert. Dann ist C selbst ein Anfangssegment von Y_1. Für jedes $x \in C$ sei $f_x : B_x \to Y_2$ die gute Abbildung von B_x nach Y_2. Wir definieren dann die Abbildung $f : C \to Y_2$ durch die Regel $f(x) = f_x(x)$, für alle $x \in C$. Dann ist f eine gute Abbildung.

- Falls $C = Y_1$, dann sind wir fertig.
- Andernfalls ist C eine echte Teilmenge von Y_1 (d.h. $Y_1 \setminus C \neq \emptyset$). Falls $f(C) = Y_2$, dann sei $g = f^{-1}$ (offensichtlich wäre dann f eine Bijektion). In diesem Fall ist $g : Y_2 \to Y_1$ eine gute Abbildung.

  Kann es sein, daß $f(C) \neq Y_2$? Falls ja, sei $u = Sup(C)$ und $v = Sup(f(C))$. Dann können wir die Abbildung f erweitern mit der Regel $f(u) = v$. Dadurch bekommen wir eine gute Abbildung von $C \cup \{u\}$ nach Y_2. Aber dies widerspricht doch der Definition von C.

$\square$

7 Der Wohlordnungssatz

Die eigentliche Voraussetzung für diesen Satz ist der Auswahlaxiom. Am Ende des 19-ten Jahrhunderts äußerten viele Mathematiker Zweifel an der Richtigkeit dieses Satzes und daher auch an der Richtigkeit des Auswahlaxioms. Heute bezweifelt kaum jemand, daß die Axiome von Zermelo-Fraenkel die richtige Grundlage für die Mengenlehre bieten.

Nun, um den Wohlordnungssatz zu beweisen, sei A irgendeine Menge. Wir suchen dann eine Wohlordnung "$\leq$" für A. Dazu sei $P(A)$ die Potenzmenge von A.

Satz 7. *Sei $f : P(A) \to A$ eine Abbildung. Dann gibt es eine eindeutige Teilmenge $W \subset A$ und eine eindeutige Wohlordnung "$\leq$" auf W, wobei*

1. *für jedes $x \in W$ gilt $f(\{y \in W : y < x\}) = x$, und*
2. *$f(W) \in W$.*

Beweis. Wir suchen eine bestimmte Ordnung "$\leq$" auf einer bestimmten Teilmenge $W \subset A$. Dafür müssen wir verschiedene mögliche Ordnungen — die wir mit "$\leq_1$" und "$\leq_2$" bezeichnen werden — zusammen mit verschiedenen möglichen Teilmengen Y_1, $Y_2 \subset A$ untersuchen.

Sei daher $(Y_1, \leq_1)$ irgendeine wohlgeordnete Teilmenge von A. Wir werden sagen, daß $(Y_1, \leq_1)$ eine f-Teilmenge von A ist, falls für jedes $x \in Y_1$ die Gleichung $f(\{y \in Y_1 : y <_1 x\}) = x$ gilt.

Seien nun $(Y_1, \leq_1)$ und $(Y_2, \leq_2)$ beide f-Teilmengen von A. Nach unserem letzten Satz gibt es entweder eine ordnungstreue Abbildung $\phi : Y_1 \to Y_2$, wobei $\phi(Y_1)$ ein Anfangssegment von Y_2 ist, oder umgekehrt. Behauptung: ϕ ist eigentlich die Identitätsabbildung $\phi(x) = x$, für alle $x \in Y_1$. Denn andernfalls sei $t \in Y_1$ das kleinste Element (bzgl. der Ordnung $\leq_1$), wobei $\phi(t) \neq t$. Es gilt einerseits

$$\{u \in Y_1 : u <_1 t\} = \{v \in Y_2 : v <_2 \phi(t)\}.$$

Andererseits, da beide Y_1 und Y_2 f-Teilmengen von A sind, muß gelten

$$\phi(t) = f(\{v \in Y_2 : v <_2 \phi(t)\}) = f(\{u \in Y_1 : u <_1 t\}) = t.$$

Ein Widerspruch. Daher ist doch ϕ die Identitätsabbildung auf Y_1. D.h. Y_1 ist einfach ein Anfangssegment von Y_2 und die Ordnung "$\leq_1$" ist identisch mit der Ordnung "$\leq_2$" auf Y_1.

Sei nun W die Vereinigung aller f-Teilmengen von A. Dann muß W selbst eine f-Teilmenge sein. Falls $f(W) \notin W$, dann kann die Ordnung "$\leq$" auf W zu einer Ordnung auf $W \cup \{f(W)\}$ erweitert werden, indem die Relation $w < f(W)$, für alle $w \in W$, hinzugefügt wird. Dann ist $W \cup \{f(W)\}$ eine f-Teilmenge, die größer ist als W. Dies widerspricht der Definition von W. $\square$

Satz 8 (Wohlordnungssatz)**.** *Jede Menge A besitzt eine Wohlordnung.*

Beweis. Nach dem Auswahlaxiom gibt es eine Abbildung $f : P(A) \to A$, wobei $f(U) \in U$, für alle Teilmengen $U \subset A$. Sei dann eine neue Abbildung ϕ gegeben durch

$$\phi(V) = f(A \setminus V) \in A \setminus V,$$

für alle Teilmengen $V \subset A$ mit $V \neq A$. Schließlich sei $\phi(A) = a_0$, wobei $a_0 \in A$ irgendein ausgewähltes Element ist. Dann gibt uns unser letzter Satz eine bestimmte Wohlordnung auf einer ϕ-Teilmenge $W \subset A$, wobei $\phi(W) \in W$.

Kann es sein, daß $W \neq A$? Falls ja, dann ist doch $f(A \setminus W) \in A \setminus W$. D.h. $\phi(W) \notin W$, ein Widerspruch. $\square$

8 Mathematische Logik

Damals, um 1904, haben viele Mathematiker (insbesondere Lesbegue, Poincaré und Banach) gesagt, daß dieser Beweis des Wohlordnungssatzes irgendwie falsch sein muß. Z.B. eine Konsequenz ist, daß nicht messbare Teilmengen von $\mathbb{R}$ existeren, was den Vorstellungen von Lesbegue wiedersprach. Heute wird der Wohlordnungssatz nicht mehr angezweifelt. Im Gegenteil, es gibt eine enge Verbindung zwischen der Mengenlehre und der mathematischen Logik

Eine Vorstellung ist, daß ein mathematischer Beweis wie ein Computerprogramm funktionieren sollte. Die Hypothesen einer mathematischen Theorie werden in den Computer eingegeben, dann läuft der Computer nach festgelegten Regeln der Logik, und am Ende werden wahre mathematische Sätze ausgegeben. Solche Sätze werden dann allgemein akzeptiert, da keine menschliche Willkür mit im Spiel ist.

Daher wird, wie bei einer Computersprache, eine logische Sprache für die Mathematik definiert. Diese Sprache besteht aus Symbolen, und zwar:

$\sim$	:	"nicht"
&	:	"und"
$\vee$	:	"oder"
$\to$	:	"es folgt"
$\leftrightarrow$	:	"genau dann, wenn"
$\forall$	:	"für alle"
$\exists$	:	"es existiert"
$=$	:	"gleich"
(,)	:	"Klammer"
$x, x', \ldots$	:	"Variablen"
$c, c', \ldots$	:	"Konstanten"

Nun, es gibt unendlich viele mögliche Variablen und Konstanten in dieser Sprache, nämlich $x, x', x'', x''', x'''', \ldots$ und $c, c', c'', c''', c'''', \ldots$. Jedoch ist diese Art, Variablen und Konstanten zu beschreiben, doch ziemlich umständlich. Daher werden auch x, y, z, und auch $x_1, x_2, \ldots$ zugelassen für die Beschreibung von Variablen. Als Konstanten können auch a, b, c, u.s.w. genommen werden.

Es gibt auch *Relationen*. Eine mathematische Theorie enthält höchstens endlich viele verschiedene Relationen. Eine n-fache Relation wird wie folgt geschrieben: $R(t_1, \ldots, t_n)$. Hierbei sind die t_i *Terme*. Terme können entweder Variablen oder Konstanten als Werte annehmen.

Zum Beispiel gibt es die Relation "$\in$" in der Mengenlehre. Wir schreiben "$a \in b$", um zu sagen, daß a ein Element aus b ist. Hier sind "a" und "b" Konstanten, und die Relation $a \in b$ ist dann entweder wahr oder falsch in einem bestimmten System — oder Modell.

Statt "$a \in b$" zu schreiben, ist es eigentlich konsequenter

$$\in (a, b)$$

zu schreiben. Oder vielleicht noch besser wäre

$$R_\in(a, b).$$

Ein anderes Beispiel ist die Addition in der Arithmetik von $\mathbb{Z}$. Es gilt etwa $2 + 2 = 4$. Dies ist eine Relation zwischen den drei Konstanten 2, 2 und 4. Man könnte daher diese dreifache Relation wie folgt beschreiben:

$$R_+(2, 2, 4).$$

Wir wissen, daß $R_+(2, 2, 4)$ den Wert "wahr" besitzt. Andererseits besitzt die Relation $R_+(2, 2, 3)$ den Wert "'falsch". Die Relation $R_+(2, 2, x)$ besitzt keinen Wahrheitswert. Erst wenn die Variable x durch einen Quantoren festgelegt wird, entsteht auch ein Wahrheitswert. Z.B. die Aussage

$$\exists x R_+(2, 2, x)$$

ist wahr. Aber die Aussage

$$\forall x R_+(2, 2, x)$$

ist falsch.

8.1 Wohlgeformte Formeln

Es ist nicht so, daß jede Zeichenkette irgendeinen Sinn macht. Z.B. die Zeichenkette

$$((, \to \forall$$

ist sicherlich völlig sinnlos. Unser "Compiler" wird sofort eine Fehlermeldung produzieren.

Eine sinnvolle Zeichenkette heißt eine *Wohlgeformte Formel*, abgekürtz "WFF".[5] Wohlgeformte Formeln werden durch die folgenden Regeln bestimmt.

1. Zeichenketten der Art $x = x'$ oder $x = c$ oder $c = c'$ sind WFFs.
2. Sei R eine n-fache Relation. Dann ist $R(t_1, \ldots, t_n)$ ein WFF, wobei jedes t_i entweder eine Variable oder eine Konstante ist.
3. Falls A und B WFFs sind, dann auch $\sim (A)$, $(A)\&(B)$, $(A) \vee (B)$, $(A) \to (B)$ und $(A) \leftrightarrow (B)$.
4. Falls A ein WFF ist, dann sind auch $\exists x A$ und $\forall x A$ beide WFFs.

8.2 Aussagen

Variablen werden entweder als "frei" oder als "gebunden" bezeichnet. Sei x eine Variable. Dann ist x zunächst *frei* in allen WFFs von der Art $x = x'$, $x = c$, oder $R(t_1, \ldots, t_n)$, wobei t_i gleich x ist für irgendein i. Falls die WFF A eine freie Variable x enthält (man schreibt $A(x)$), dann ist x immer noch frei in der WFF $\sim (A(x))$. Auch die anderen Verbindungen wie in Regel 3 für WFFs ändern die Freiheit nicht.

Andererseits wird x *gebunden* in Formeln der Art $\exists x A(x)$, und auch in $\forall x A(x)$. D.h. eine freie Variable wird durch einen *Quantor* gebunden. Die Quantoren sind die zwei Zeichen "$\exists$" und "$\forall$". Eine gebundene Variable ist nicht mehr frei.

Eine *Aussage* ist dann eine WFF ohne freie Variablen.

8.3 Wahrheitstabellen

Aussagen in einem vorgegebenen Modell sind entweder wahr "W" oder falsch "F". Seien P und Q mögliche Aussagen. Dann gibt es die folgenden Schemen, um die Wahrheitswerte für weitere Aussagen zu bestimmen.

$$
\begin{array}{cc||c|c}
 & & Q & \to \\
 & \& & W & F \\
\hline\hline
P & W & W & F \\
\hline
\downarrow & F & F & F
\end{array}
\qquad
\begin{array}{cc||c|c}
 & & Q & \to \\
 & \vee & W & F \\
\hline\hline
P & W & W & W \\
\hline
\downarrow & F & W & F
\end{array}
\qquad
\begin{array}{cc||c|c}
 & & Q & \to \\
 & \to & W & F \\
\hline\hline
P & W & W & F \\
\hline
\downarrow & F & W & W
\end{array}
\quad \text{und} \quad
\begin{array}{cc||c|c}
 & & Q & \to \\
 & \leftrightarrow & W & F \\
\hline\hline
P & W & W & F \\
\hline
\downarrow & F & F & W
\end{array}
$$

[5] Ich folge hier der Notation in Cohen's Buch: "*Set Theory and the Continuum Hypothesis*".

D.h. etwa die Aussage $(P)\&(Q)$ ist nur dann wahr, wenn sowohl P als auch Q gleichzeitig wahr sind. Auch $(P) \vee (Q)$ ist nur dann falsch, wenn sowohl P als auch Q gleichzeitig falsch sind. $(P) \to (Q)$ ist nur dann falsch, wenn P falsch und Q wahr ist. Wenn P falsch ist, dann ist $(P) \to (Q)$ immer wahr, egal welchen Wert Q hat.

Vielleicht ist diese Festlegung für die Beziehung $(P) \to (Q)$ zunächst etwas verwirrend. Ein Beispiel aus der Arithmetik zeigt jedoch, daß diese Regel eigentlich nicht so abwegig ist.

Beispiel 3. *Sei P die Aussage "$1 = 2$". Daher ist P offensichtlich falsch. Sei Q die Aussage "$\sqrt{2} = 5$". Aber wenn $1 = 2$, dann folgt sicherlich $0 = 1$. Wir multiplizieren beide Seiten mit $\sqrt{2}$. Dann folgt $\sqrt{2} = 0$. Ebenso folgt $5 = 0$. Dann ist $\sqrt{2} = 0 = 5$ und die gesamte Aussage*

$$(1 = 0) \to (\sqrt{2} = 5)$$

stimmt.

Nun, das Beispiel 3 ist sicherlich kein Beispiel aus der mathematischen Praxis. Aber das folgende Beispiel kommt tatsächlich vor.

Beispiel 4. *Das vielleicht grösste, noch ungelöste Problem in der Mathematik ist die "Riemannsche Vermutung". Es handelt sich um eine bestimmte Aussage in der Zahlentheorie. Sei R die Riemannsche Vermutung. Dann ist R entweder wahr oder falsch. Da R noch nicht bewiesen ist, wissen wir doch nicht, welchen Wahrheitswert R eigentlich besitzt. Die meisten Mathematiker glauben wohl, daß R wahr ist. Nun, es gibt natürlich viele andere mögliche Aussagen in der Zahlentheorie. Manche davon könnten bewiesen werden, wenn tatsächlich R wahr wäre. Sei Q eine solche Aussage. Dann gibt es den Satz "$R \to Q$". Dieser Satz ist dann richtig im Falle $R = wahr$, wobei gezeigt wird, daß dann $Q = wahr$ sein muß. Andererseits, falls $R = falsch$ ist, dann fehlen die eigentlichen Voraussetzungen, um Q zu beweisen. Daher kann Q entweder wahr oder falsch sein. Trotzdem bleibt die Feststellung $R \to Q$ wahr.*

8.4 Tautologien

Eigentlich brauchen wir nur die zwei Symbole "$\sim$" und "$\vee$", denn die Wahrheitstabelle für $(P)\&(Q)$ ist identisch mit der Wahrheitstabelle für $\sim((\sim P) \vee (\sim Q))$. Auch $(P) \to (Q)$ ist nichts anderes als $(\sim P) \vee Q$. Schließlich ist $(P) \leftrightarrow (Q)$ identisch mit $((P) \to (Q))\&((Q) \to (P))$.

Dies sind *Tautologieschemen.* Wir schreiben

$$\begin{aligned}
(P)\&(Q) &\equiv \sim((\sim P) \vee (\sim Q)) \\
(P) \to (Q) &\equiv (\sim P) \vee Q \\
(P) \leftrightarrow (Q) &\equiv ((P) \to (Q))\&((Q) \to (P))
\end{aligned}$$

Dadurch ist es möglich, in einem Beweis, verschiedene Aussagen umzuformen.

Hier sind einige weitere gebräuchliche Tautologieschemen

$$
\begin{aligned}
\sim(\sim P) &\equiv P \\
P\&P &\equiv P \\
P \vee P &\equiv P \\
(P\&Q)\&R &\equiv P\&(Q\&R) \\
(P \vee Q) \vee R &\equiv P \vee (Q \vee R) \\
P \vee Q &\equiv Q \vee P \\
P\&Q &\equiv Q\&P \\
(P\&Q) \vee R &\equiv (P \vee Q)\&(Q \vee R) \\
(P \vee Q)\&R &\equiv (P\&Q) \vee (Q\&R) \\
\sim(P\&Q) &\equiv (\sim P) \vee (\sim Q) \\
\sim(P \vee Q) &\equiv (\sim P)\&(\sim Q) \\
(P \to Q) &\equiv ((\sim Q) \to (\sim P)) \\
(P \to (Q \to R)) &\equiv (Q \to (P \to R)) \\
((P\&Q) \to R) &\equiv (Q \to (P \to R))
\end{aligned}
$$

Im allgemeinen ist eine *Tautologie* definiert als eine Aussage, die immer wahr ist. Daher ist $P \vee (\sim P)$ eine Tautologie. Diese Aussage ist immer wahr, egal was die Aussage P ist.

8.5 Gültige Aussagen

Zunächst gibt es in jeder mathematischen Theorie ein System von Axiomen. Dies sind einfach Aussagen, die als gültig angenommen werden. Zum Beispiel haben wir am Anfang dieser Vorlesung eine informale Beschreibung der Axiome der Mengenlehre nach Zermelo-Fraenkel gesehen. In der Theorie der Mengenlehre sind diese Axiome dann gültig.

Nun, aus gültigen Aussagen werden weitere gültige Aussagen abgeleitet nach festen Regeln. Diese abgeleiteten Aussagen sind die Sätze der Theorie. Die Regeln sind wie folgt.

1. Eine Tautologie ist eine gültige Aussage. Insbesondere gilt: falls A und B gültig, dann ist auch $A\&B$ gültig.

2. Falls A und auch $(A) \to (B)$ gültig sind, dann ist auch B gültig.

3. (a) i. $c = c$,
      ii. $(c = c') \to (c' = c)$ und
      iii. $((c = c')\&(c' = c'')) \to (c = c'')$ sind gültige Aussagen.
   (b) Falls c in der WFF A vorkommt, und die WFF A' ist die Aussage A, wobei c durch c' ersetzt wird, dann ist $(c = c') \to ((A) \to (A'))$ gültig.
   (c) Falls x in der WFF A vorkommt, und die WFF A' ist die Aussage A, wobei x durch x' ersetzt wird, dann ist die Aussage $A \leftrightarrow A'$ gültig.

4. Sei $A(x)$ eine WFF, wobei die Variable x als freie Variable vorkommt. Dann ist

$$(\forall x A(x)) \to A(c)$$

gültig.

5. Sei B eine Aussage, wobei weder x noch c vorkommt. Dann, falls $A(c) \to B$ gültig ist, dann folgt auch, daß $(\exists x A(x)) \to B$ gültig ist.

6. Die Aussage $\sim (\forall x A(x))$ ist gültig genau dann wenn die Aussage $\exists x(\sim A(x))$ gültig ist.

7. Sei $A(x)$ eine WFF mit freien Variablen x, und sei B eine weitere WFF, wobei x in B nicht vorkommt. Dann ist

   (a) $(\forall x A(x))\&(B)$ gültig genau dann, wenn $\forall x((A(x))\&(B))$ gültig ist, und

   (b) $(\exists x A(x))\&(B)$ gültig genau dann, wenn $\exists x((A(x))\&(B))$ gültig ist.

8.6 Konsistenz, Widerspruch

Ein *Widerspruch* ist eine Aussage, die immer falsch ist. Insbesondere ist die Aussage $P\&(\sim P)$ ein Widerspruch, egal ob P wahr oder falsch ist.

Angenommen, eine vorgegebene mathematische Theorie wird durch ein System von Axiomen $A_1, \ldots, A_n$ beschrieben. Falls daraus ein Widerspruch entsteht, d.h. es gibt eine Aussage P, wobei die gesamte Aussage

$$(A_1 \& \cdots A_n) \to ((P)\&(\sim P))$$

gültig ist, dann ist diese Theorie widersprüchlich. Mit anderen Worten, die Theorie ist schlecht, nicht mehr zu gebrauchen. Andererseits, falls *kein* solcher Widerspruch als Satz in der Theorie abgeleitet werden kann, dann heißt die Theorie *konsistent*.

In früheren Zeiten ist man davon ausgegangen, daß die *übliche* Mathematik — insbesondere die einfache, normale Arithmetik in $\mathbb{Z}$ — selbstverständlich eine konsistente Theorie ist. Um so grösser war die Bestürzung, als Gödel gezeigt hat, daß die Konsistenz der Arithmetik unbeweisbar ist. Da $\mathbb{Z}$ im Rahmen der Zermelo-Fraenkel Mengenlehre beschrieben werden kann folgt, daß auch die Konsistenz der Mengenlehre unbeweisbar ist.

Andererseits gilt: eine Theorie ist konsistent genau dann, wenn ein Modell dafür existiert. Daher ist es jetzt sinnvoll für uns, daß wir uns Gedanken über die Theorie der Modelle machen.

9 Modelle

Modelle sind eigentlich Mengen. Aber diese Mengen werden ganz konkret beschrieben; die Axiome von Zermelo-Fraenkel spielen jetzt keine Rolle. Für diese Modelle gibt es nur eine Relation. Diese Relation wird durch unser mengentheoretischen Inklusionszeichen "$\in$" beschrieben.

9.1 Modelle als Mengen: ein Beispiel

Beispiel 5. *Zum Beispiel wird ein bestimmtes Modell — oder Menge — durch die zwei Konstirdanten a und b und die zwei Relationen $a \in a$ und $a \in b$ gegeben. (Genauer betrachtet sind dies eigentlich zwei verschiedene Instanzen der* einzigen *Relation "$\in$".)*

Die verschiedenen Instanzen der Inklusionsrelation dieses Modells können mittels einer Tabelle dargestellt werden.

$a \in a$	W
$b \in a$	W

Ein wahrer Satz in diesem Modell ist dann die Aussage

$$\exists x(x \in a).$$

Andererseits ist der Wahrheitswert der Aussage

$$\exists x(x \in b)$$

nicht bestimmt. Dieser Satz ist doch *unbeweisbar* in unserem Modell.

Nun, solche Formeln wie $a \in b$ sind sehr einfach und ursprünglich. Daher werden sie *Primformeln* genannt. Ein Modell heißt *prim-vollständig*, falls die Wahrheitswerte für alle möglichen Primformeln vorgegeben (oder zumindestens ableitbar) sind.

Unser Modell (Beispiel 5) ist prim-unvollständig, da z.B. der Wahrheitswert der Primformel $b \in a$ nicht bestimmt ist. Auch ist $b \in b$ nicht bestimmt. Wenn wir jedoch die zwei weiteren Relationen $a \notin b$ und $b \notin b$ hinzufügen[6], dann erhalten wir doch ein prim-vollständiges Modell. Die entsprechende Tabelle ist nun

$a \in a$	W
$b \in a$	W
$a \in b$	F
$b \in b$	F

Das neue Modell, das wir jetzt haben, ist vollständig beschrieben, da alle möglichen Inklusionsrelationen festgelegt sind. Das Modell ist konsistent, da keine Inklusionsrelation sowohl wahr als auch falsch gekennzeichnet ist. (Aber auch das ursprüngliche Modell, ohne die zusätzlichen Inklusionsrelationen $a \notin b$ und $b \notin b$, war offenbar konsistent, da keine Aussagen sowohl als wahr als auch als falsch gekennzeichnet werden.)

Da das Modell prim-vollständig ist, können wir uns auch mittels unserer üblichen Schreibweise

$$a = \{a, b\} \quad \text{und} \quad b = \emptyset$$

die Mengen a und b vorstellen.[7]

[6] Eigentlich gibt es keine Relation der Art "$\notin$". Die Beziehung $a \notin b$ ist $\sim (a \in b)$, oder noch besser: $\sim R_{\in}(a, b)$.

[7] In diesem Modell gilt $a \in a$, was nach Zermelo-Fraenkel's Axiom der Regularität ausgeschlossen wird. Dies ist jedoch *kein* Wiederspruch! Wir befinden uns jetzt auf einer viel ursprünglicheren Ebene als die komplizierte Zermelo-Fraenkel Mengenlehre.

9.2 Axiome in einem Modell: ein Beispiel

Beispiel 6. *In diesem Beispiel gibt es zwei Axiome, genannt A_1 und A_2.*

- A_1 *ist: Jede Menge enthält sich selbst.*
- A_2 *ist: Jede Menge besitzt mindestens zwei Elemente.*

Wir können diese Axiome auch durch formale Aussagen formulieren.

- $A_1 \quad : \quad \forall x(x \in x)$
- $A_2 \quad : \quad \forall x \exists y \exists z (\sim (y = z) \& (y \in x) \& (z \in x))$

Das System enthält auch drei Konstanten, genannt a, b und c.

Ist dieses System — definiert durch unsere zwei Axiome — konsistent? Diese Frage kann beantwortet werden, indem wir ein Modell suchen, wobei beide Axiome wahr sind.

Wir betrachten nun drei Modelle, die wir M_1, M_2 und M_3 nennen werden. Jedes Modell hier enthält die drei Konstanten (oder Mengen), a, b und c. Die Inklusionsrelationen sind wie folgt.

M_1 :

$a \in a$	W
$b \in a$	W
$b \in b$	W
$c \in b$	W
$a \in c$	W
$c \in c$	W

M_2 :

$a \in a$	W
$b \in a$	W
$c \in a$	F
$a \in b$	W
$b \in b$	W
$c \in b$	W
$a \in c$	F
$b \in c$	W
$c \in c$	W

M_3 :

$a \in a$	W
$b \in a$	W
$c \in a$	W
$a \in b$	W
$b \in b$	W
$c \in b$	F
$a \in c$	W
$b \in c$	W
$c \in c$	W

Das Modell M_1 ist prim-unvollständig. Trotzdem ist es ein Modell für unser System. Es ist möglich, M_1 zu ergänzen zu einem prim-vollständigen, indem wir die nicht behandelten Primformeln als wahr oder falsch bezeichnen. Zum Beispiel ist das Modell M_2 eine Möglichkeit. Das Modell M_3 ist hingegen *keine* Ergänzung von M_1. M_3 ist ein ganz anderes Modell für unser System.

9.3 Abhängigkeit, Unabhängigkeit

Wir betrachten nun zwei weitere Modelle, die die Konstanten a, b und c enthalten.

$$M_1^* : \begin{array}{c|c} & \\ \hline\hline a \in a & W \\ b \in a & F \\ c \in a & F \\ b \in b & W \\ c \in c & W \end{array} \qquad M_2^* : \begin{array}{c|c} & \\ \hline\hline a \in a & F \\ b \in a & W \\ c \in a & W \\ a \in b & W \\ b \in b & F \\ c \in b & W \\ a \in c & W \\ b \in c & W \\ c \in c & F \end{array}$$

Offensichtlich gilt Axiom A_1 für das Modell M_1^*, aber Axiom A_2 ist falsch in M_2^*. Andererseits gilt Axiom A_2 für das Modell M_2^*, jedoch Axiom A_2 ist falsch in M_1^*.

Dies zeigt, daß die Axiome A_1 und A_2 *unabhängig* voneinander sind. Gegeben ein beliebiges System $A_1, \dots, A_n$ von Axiomen, ein bestimmtes Axiom A in diesem System ist unabhängig von den anderen Axiomen, falls ein Modell existiert, wobei A falsch ist in dem Modell, während die anderen Axiomen alle wahr sind. Falls kein solches Modell existiert, dann ist A *abhängig* in Bezug auf den anderen Axiomen.

9.4 Die Beschreibung von Modellen; Unendliche Modelle

Gegeben ein prim-vollständiges, endliches Modell M, dann ist es, im Prinzip, kein Problem, das Modell zu beschreiben. Wir könnten eine Liste aufstellen, in der alle wahre Inklusionsrelationen stehen. Zum Beispiel, wenn das Modell die drei Mengen a, b und c enthält, und die Liste so aussieht

$$\begin{array}{ccc} a & \in & a \\ c & \in & a \\ b & \in & b \\ a & \in & c \\ b & \in & c \\ c & \in & c \end{array}$$

dann ist das Modell vollständig beschrieben. Die Inklusionsrelationen, die nicht auf der Liste stehen, etwa "$b \in a$", müssen dann falsch sein.

Eine alternative Art, das Modell zu beschreiben, wäre einfach eine Liste der Mengen aufzustellen, etwa wie

$$\begin{array}{rcl} a & = & \{a, c\} \\ b & = & \{b\} \\ c & = & \{a, b, c\} \end{array}$$

u.s.w.

Die Situation ist schwieriger, wenn es sich um unendliche Modelle handelt. Wir können versuchen eine partielle Liste zu beschreiben, etwa wie

$$\begin{array}{ccc} a_2 & \in & a_1 \\ a_3 & \in & a_2 \\ a_4 & \in & a_3 \\ a_5 & \in & a_4 \\ a_6 & \in & a_5 \\ & \vdots & \\ & u.s.w. & \end{array}$$

Aber letztendlich muß doch genau gesagt werden, was eigentlich "u.s.w." bedeuten soll in dieser Liste. Um dieses "u.s.w." zu beschreiben, brauchen wir irgendein System von Formeln — und dann kommen wir zurück zum *eigentlichen* Problem — nämlich, ist das System konsistent oder nicht?

Und tatsächlich hat Gödel gezeigt, daß wenn eine mathematische Theorie nur die übliche Arithmetik enthalten soll, es nicht möglich ist, ein konkretes, vorgegebenes Modell anzugeben.

9.5 Eine Definition

Nun wollen wir insgesamt sagen, was eine mathematische Theorie, und ein dazu passendes Modell sein soll. Für eine mathematische Theorie brauchen wir zunächst eine Liste der Konstanten für diese Theorie. Diese Liste kann endlich oder auch unendlich lang sein. Sei $c_1, c_2, c_3, \ldots$ die Liste der Konstanten.[8] Wir brauchen auch eine endliche Sammlung von möglichen Relationen $R_1, \ldots, R_m$ für unsere Theorie. Schliesslich brauchen wir noch eine endliche Sammlung von Axiomen $A_1, \ldots, A_n$. Damit wird eine mathematische Theorie definiert.

Um dieser Theorie Substanz zu geben, brauchen wir ein Modell. Ein Modell ist zunächst eine Menge M. Aber gemeint ist hier *nicht* die Idee von Mengen in der Zermelo-Fraenkel Theorie der Mengenlehre! Nein. Gemeint ist eine ganz konkrete Vorgabe von Mengen und Inklusionsrelationen, wie in unseren Beispielen. Wir nehmen an, daß M vorgegeben ist und auch konsistent ist. D.h. es gibt keine Primformel, die sowohl als wahr als auch als falsch gekennzeichnet wird.

Nun, jeder Konstante c_α wird ein Element $\overline{c}_\alpha \in M$ zugewiesen. Ebenso wird jeder Relation R_β eine bestimmte Teilmenge $\overline{R}_\beta \subset M^r$ des kartesischen Produkts[9] von M zugewiesen, wobei R_β eine r-fache Relation ist. D.h. R_β ist eine Relation mit r Termen $R_\beta(t_1, \ldots, t_r)$. Die verschiedenen Relationen der Theorie werden im Modell so festgelegt daß alle Axiome wahr sind nach den folgenden Regeln.

[8] Z.B. für die Zermelo-Fraenkel Theorie der Mengenlehre gibt es nur eine einzige Konstante, genannt "$\emptyset$".

[9] Das 2-fache kartesisches Produkt $M \times M$ (geschrieben M^2) haben wir schon gesehen. Das r-fache Produkt $\underbrace{M \times \cdots \times M}_{r-\text{fach}} = M^r$ besteht aus geordneten Listen $(m_1, \ldots, m_r)$, wobei $m_i \in M$ für jedes i.

Sei $A(x_1, \ldots, x_s)$ irgendeine WFF mit s freien Variablen $x_1, \ldots, x_s$. Seien $\overline{x}_1, \ldots, \overline{x}_s \in M$ irgendwelche Elemente von M. Dann ist der Wahrheitswert von A in $\overline{x}_1, \ldots, \overline{x}_s$ wie folgt festgelegt:

1. (a) Ist A eine Formel der Art $x = x'$, dann ist A wahr in $\overline{x}, \overline{x'}$, falls $\overline{x} = \overline{x}'$ in M.
   (b) Ist A eine Formel der Art $x = c$, dann ist A wahr in $\overline{x}, \overline{c}$, falls $\overline{x} = \overline{c}$ in M.
   (c) Ist A eine Formel der Art $c = c'$, dann ist A wahr in $\overline{c}, \overline{c'}$, falls $\overline{c} = \overline{c}'$ in M.

2. Falls $A = R_\beta(t_1, \ldots, t_s)$, dann ist A wahr in $\overline{x}_1, \ldots, \overline{x}_s$, falls $(\overline{x}_1, \ldots, \overline{x}_s) \in \overline{R}_\beta \subset M^s$. Dasselbe gilt, wenn einige Terme auch Konstanten sind.

3. Falls A zusammengesetzt wird aus Aussagen der Art 1. und 2., und alle diese Aussagen in den entsprechenden Variablen und Konstanten wahr sind[10], dann ist A wahr in $\overline{x}_1, \ldots, \overline{x}_s$.

4. Falls A von der Art $\forall y B(y, x_1, \ldots, x_s)$ ist, dann ist A wahr in $\overline{x}_1, \ldots, \overline{x}_s$, falls B wahr in $\overline{y}$ und $\overline{x}_1, \ldots, \overline{x}_s$, für alle $\overline{y} \in M$.

5. Falls A von der Art $\exists y B(y, x_1, \ldots, x_s)$ ist, dann ist A wahr in $\overline{x}_1, \ldots, \overline{x}_s$, falls B wahr in $\overline{y}$ und $\overline{x}_1, \ldots, \overline{x}_s$, für mindestens ein $\overline{y} \in M$.

Dann ist M (zusammen mit diesen Zuordnungen) ein *Modell* für unsere Theorie, falls alle Axiome $A_1, \ldots, A_n$ der Theorie wahr in M sind.

Bemerkung. *Falls die Variable y gar nicht in B vorkommt, gilt trotzdem (nach den Regeln 4 und 5), daß $\forall yB$ und $\exists yB$ wahr sind genau dann, wenn B wahr ist.*

10 Äquivalenzrelationen

Als nächstes werden wir Gödel's Vollständingkeitssatz behandeln. D dafür Äquivalenzrelationen und Äquivalenzklassen benötigt werden, werden wir diese aber zunächst definieren. Hier sei angemerkt, daß vieles in der Mathematik durch Äquivalenzrelationen beschrieben wird.

Definition 12. *Sei M eine Menge (gegeben als eine abstrakte Sammlung von Elementen, vielleicht mit Primformeln). Eine* Äquivalenzrelation *in M ist eine Teilmenge R des kartisischen Produkts $M \times M$, wobei folgendes gilt:*

1. *$(x, x) \in R$, für alle $x \in M$.*

2. *Falls $(x, y) \in R$ dann ist auch (y, x) in R.*

[10] Laut unseres Abschnitts 8.1 enthält eine wwf A zunächst Zeichenketten der Art $x = x'$, $x = c$, $c = c'$, oder auch $R(t_1, \ldots, t_s)$. Hinzu kommen zusammengesetzte Zeichenketten der Art $\sim A$, $A\&B$, $A \vee B$, $A \to B$, oder auch $A \leftrightarrow$. Die Wahrheitswerte für diese zusammengesetzten Zeichenketten in vorgegebenen Elementen von M wird durch die entsprechenden Wahrheitswerte von A und B bestimmt, und dann durch die Wahrheitstabellen für die Verbindungszeichen, die in Abschnitt 8.3 festgelegt sind.

3. *Falls $(x, y) \in R$ und $(y, z) \in R$, dann ist auch $(x, z) \in R$.*

Falls $(x, y) \in R$, dann schreibt man[11] üblicherweise $x \sim y$. Mit dieser Notation gilt

1. $x \sim x$, für alle $x \in M$.

2. $x \sim y$ genau dann, wenn $y \sim x$.

3. Falls $x \sim y$ und $y \sim z$, dann $x \sim z$.

Beispiel 7. *Sei $M = \mathbb{Z}$, die Menge der ganzen Zahlen.*

1. *Die einfachste Äquivalenzrelation ist Gleichheit. Trivialerweise gilt $x = x$, falls $x = y$ dann ist $y = x$, und falls $x = y$ und $y = z$ dann ist $x = z$.*

2. *Etwas weniger trivial ist die folgende Äquivalenzrelation. Seien x und $y \in \mathbb{Z}$. Dann ist $x \sim y$ genau dann, wenn $x - y$ eine gerade Zahl ist.*

3. *Andererseits ist die übliche "kleiner-gleich" Relation $x \leq y$* keine *Äquivalenzrelation, da die zweite Bedingung für eine Äquivalenzrelation nicht gilt. D.h. falls $x \leq y$, dann gilt im allgemeinen nicht, daß $y \leq x$.*

Gegeben $(M, \sim)$, d.h. eine Menge M mit einer Äquivalenzrelation "$\sim$", dann gibt es die entsprechenden Äquivalenzklassen.

Definition 13. *Sei $(M, \sim)$ eine Menge mit Äquivalenzrelation, und sei $x \in M$. Dann ist*

$$[x] = \{t \in M : t \sim x\}$$

die Äquivalenzklasse, die x enthält.

Satz 9. *Seien x und y Elemente von M. Falls $[x] \cap [y] \neq \emptyset$, dann gilt $[x] = [y]$.*

Beweis. Sei $z \in [x] \cap [y]$. D.h. $x \sim z$ und $z \sim y$. Folglich ist $x \sim y$. Aber dann gilt $t \sim x$ genau dann, wenn $t \sim y$, für alle möglichen Elemente $t \in M$. $\square$

Daher zerfällt die Menge M in eine Sammlung von disjunkten Äquivalenzklassen.

Die Menge der Äquivalenzklassen wird oft als $M/\sim$ bezeichnet. Die Abbildung $x \to [x]$ von $M \to M/\sim$ heißt die "kanonische Abbildung".

[11] Diese Notation ist leider etwas ungünstig, da wir das "$\sim$" Zeichen doch auch in der mathematischen Logik verwenden. Falls A eine Aussage ist, dann ist $\sim A$ "nicht A". In diesem Abschnitt heißt $x \sim y$ jedoch "x ist zu y äquivalent".

11 Vollständige Induktion

Die Beweismethode der vollständigen Induktion wird sehr oft in der Mathematik benutzt. An sich ist die Methode ganz einfach. Es handelt sich um eine Folgerung aus dem Wohlordnungssatz. Sei nämlich eine wohlgeordnete Menge $(M, \leq)$ vorgegeben, und sei $T \subset M$ eine Teilmenge mit der Eigenschaft, daß für alle $x \in M$ gilt: falls $\{z \in M : z < x\} \subset T$, dann folgt auch $x \in T$. Dann ist $T = M$. Warum? Sonst wäre $M \setminus T \neq \emptyset$. Sei $y \in M \setminus T$ das kleinste Element. Dann ist $\{z \in M : z < y\} \subset T$, und daher muß doch $y \in T$. Ein Widerspruch. Dies ist das Prinzip der *transfiniten Induktion*.

Die übliche vollständige Induktion, die in der Mathematik eingesetzt wird, beschränkt sich auf die Menge $\mathbb{N}$ der natürlichen Zahlen mit der üblichen Ordnung unter Zahlen. Die Formulierung ist die folgende.

Sei $P(n)$ eine Aussage, die von der Zahl n abhängig ist. Angenommen

1. $P(1)$ ist wahr, und

2. falls $P(k)$ wahr ist, dann folgt, daß auch $P(k+1)$ wahr ist,

dann ist $P(n)$ wahr für alle $n \in \mathbb{N}$.

Beispiel 8. *Es gilt*

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$$

Insbesondere ist dann etwa

$$1 + 2 + 3 + \cdots + 98 + 99 + 100 = 5050, \;\; u.s.w.$$

Beweis: (mittels vollständiger Induktion).

1. Zuerst gilt offensichlich im Falle $n = 1$, daß

$$\sum_{k=1}^{1} k = 1 = 1 \cdot (1+1)/2.$$

   Daher ist die Behauptung wahr, zumindest wenn $n = 1$.

2. Sei nun $k \in \mathbb{N}$ vorgegeben und sei $\sum_{j=1}^{k} j = \frac{k(k+1)}{2}$. Dann ist

$$\sum_{j=1}^{k+1} j = (k+1) + \sum_{j=1}^{k} j = (k+1) + \frac{k(k+1)}{2} = \frac{2k+2}{2} + \frac{k(k+1)}{2} = \frac{(k+1)((k+1)+1)}{2}.$$

12 Gödels Vollständigkeitssatz

Satz 10. *Sei A eine gültige Aussage in einer formalen mathematischen Theorie. Dann ist A wahr in jedem Modell M für diese Theorie.*

Beweis. Falls A eine Tautologie ist, dann ist A immer wahr, insbesondere in dem Modell M. Falls A ein Axiom des Modells ist, dann muss A wahr sein in M. Falls A abgeleitet wird aus den Regeln für gültige Aussagen (siehe Abschnitt 8.5), dann ist A wahr in M, da diese Regeln den Wahrheitstabellen (Abschnitt 8.3) entsprechen. $\square$

Satz 11. *Angenommen, ein Modell M existiert für ein System S von Aussagen (oder Axiome). Dann ist S konsistent.*

Beweis. Falls S *nicht* konsistent, dann gibt es endlich viele Aussagen $A_1, \ldots, A_n \in S$, wobei $(A_1 \& \cdots \& A_n) \to (P \& (\sim P))$ eine gültige Aussage ist, für eine Aussage P. Da alle A_i gültige Aussagen sind (daher wahr in M), ist auch $P \& (\sim P)$ wahr in M. Aber alle Aussagen in M sind letztendlich Aussagen über die Primformeln von M. Der Widerspruch $P \& (\sim P)$ zeigt dann, daß M nicht konsistent sein kann. D.h. M ist doch kein Modell für S. $\square$

Umgekehrt gilt *Gödel's Vollständigkeitssatz.*

Satz 12 (Gödel)**.** *Sei S eine konsistente Sammlung von Aussagen. Dann gibt es ein Modell M für S. Die Kardinalität von M ist nicht größer als die Kardinalität von S, falls S unendlich groß ist. Falls S endlich ist, dann ist M höchstens abzählbar groß.*

Um diesen Satz zu beweisen, brauchen wir zunächst das folgende Ergebnis.

Satz 13. *Sei T eine konsistente Sammlung von Aussagen, und sei A eine beliebige Aussage. Dann ist entweder $T \cup \{A\}$ oder $T \cup \{\sim A\}$ konsistent.*

Beweis. Falls *beide* $T \cup \{A\}$ und $T \cup \{\sim A\}$ nicht konsistent sind, dann gibt es Aussagen $B_1, \ldots, B_n \in S$ und $B'_1, \ldots, B'_m \in S$, wobei sowohl

$$(B_1 \& \cdots \& B_n \& A) \to (C \& (\sim C))$$

als auch

$$(B'_1 \& \cdots \& B'_m \& (\sim A)) \to (D \& (\sim D))$$

gültig sind, wobei C und D Aussagen sind.

Da sowohl $C \& (\sim C)$ als auch $D \& (\sim D)$ falsch sind, mussen sowohl $B_1 \& \cdots \& B_n \& A$ als auch $B'_1 \& \cdots \& B'_m \& (\sim A)$ falsch sein. Aber unter der Annahme, dass $B_1 \& \cdots \& B_n$ und $B'_1 \& \cdots \& B'_m$ richtig sind, folgt dass sowohl A als auch $\sim A$ beide falsch sind. Ein Widerspruch. $\square$

Satz 14 (Vollständigkeitssatz; einfache Version)**.** *Sei S eine konsistente Sammlung von Aussagen* ohne *Quantoren. (D.h. ohne die Zeichen "$\forall$" und "$\exists$".) Dann gibt es ein Modell M für S, wobei die Kardinalität von M nicht größer ist als die Kardinalität von S.*

Beweis. Da die Aussagen von S keine Quantoren enthalten, folgt, daß S überhaupt keine Variablen besitzt.

Nun, jede Aussage in S ist eine endliche Zeichenkette. Folglich, falls S aus nur endlich vielen Aussagen besteht, dann gibt es insgesamt nur endlich viele mögliche Konstanten in S. Wir betrachten daher zunächst den Fall, daß S endlich ist. Sei

$$\{c_1, \ldots, c_n\}$$

die Menge aller Konstanten in S. Zudem gibt es nur endlich viele Relationen

$$R_1, \ldots, R_m,$$

die in S vorkommen.

Als nächstes wollen wir eine Liste

$$F_1, F_2, F_3, \ldots$$

von allen möglichen Aussagen aufstellen, die diese Konstanten und Relationen enthalten. Diese Liste wird systematisch aufgebaut. Z.B. werden zuerst alle möglichen Zeichenketten mit nur einem Zeichen untersucht. Es gibt nur endlich viele Möglichkeiten. Dann werden die Zeichenketten mit zwei Zeichen untersucht. u.s.w. Nur die Zeichenketten, die *Aussagen* darstellen werden zugelassen, wobei unsere Standardzeichen ("&", "$\vee$", u.s.w.) und vielleicht Zeichen aus der Sammlung $\{c_1, \ldots, c_n\}$ und $R_1, \ldots, R_m$, verwendet werden. Insbesondere stehen natürlich auch alle Aussagen aus S in unserer Liste.

Nun, sowohl alle gültigen Aussagen als auch alle ungültigen Aussagen werden in $F_1, F_2, F_3, \ldots$ aufgelistet. Aber wir wollen doch lieber eine Liste mit lauter gültigen Aussagen haben. Um dies zu erreichen, wird wie folgt verfahren. Sei G_1 entweder F_1 oder $\sim F_1$, je nachdem, ob $S \cup \{F_1\}$ oder $S \cup \{\sim F_1\}$ konsistent ist. Dann ist G_2 entweder F_2 oder $\sim F_2$, je nachdem, ob $S \cup \{G_1, F_2\}$ oder $S \cup \{G_1, \sim F_2\}$ konsistent ist. U.s.w. Allgemeinen gilt: G_i ist entweder F_i oder $\sim F_i$, wobei

$$S \cup \{G_j : j \leq i\}$$

konsistent ist. Sei jetzt

$$H = S \cup \{G_i : i \in \mathbb{N}\}.$$

Eine einfache Klasse von Aussagen, die in der Liste $F_1, F_2, F_3, \ldots$ vorkommt, ist die Menge aller möglichen Gleichungen der Art $c_i = c_j$. Aber nur die *gültigen* Gleichungen sind in H enthalten. Nach Regel 3(a) für gültige Aussagen (siehe Abschnitt 8.5) wird dadurch eine Äquivalenzrelation in der Menge der Konstanten $\{c_1, \ldots, c_n\}$ definiert. Sei M die Menge dieser Äquivalenzklassen. Die Relationen $R(t_1, \ldots, t_s)$ werden in M wie folgt festgelegt. Es gilt $([c_{i(1)}], \ldots, [c_{i(n)}]) \in R \subset M^n$ genau dann, wenn $R(c_{i(1)}, \ldots, c_{i(n)}) \in H$. Insbesondere ist dann G_i wahr in M, für jedes i.

Ist nun M ein Modell für S? D.h. ist A wahr in M, für jede gültige Aussage A?

Um diese Frage zu beantworten, sei A eine beliebige Aussage. Dann ist $A \equiv F_m$, für ein m. Angenommen, A sei gültig. Kann es sein, daß $\sim A$ wahr ist in M? Dann wäre $\sim A \equiv G_m$. D.h. $S \cup \{\sim A\}$ ist konsistent. Aber

$$S\&(\sim A) \to (\sim A)$$

ist offensichtlich eine gültige Aussage. Auch

$$S\&(\sim A) \to A,$$

da $S \to A$ eine gültige Aussage ist. Es folgt

$$S\&(\sim A) \to (A\&(\sim A)).$$

Ein Widerspruch, da $S \cup \{\sim A\}$ doch konsistent ist.

Falls S unendlich groß ist, dann gibt es möglicherweise unendlich viele Konstanten. Vielleicht sogar überabzählbar viele Konstanten. Trotzdem gibt es wieder Äquivalenzklassen, wie vorher, und der Beweis folgt genauso.[12] Offensichtlich ist die Kardinalität der Menge der Äquivalenzklassen nicht größer als die Kardinalität der Menge der Konstanten. □

Es bleibt noch, den Vollständigkeitssatz zu beweisen für ein System S von Axiomen, wobei die Axiome auch Quantoren besitzen können.

Satz 15. *Angenommen, S sei ein konsistentes System von Axiomen. Für jedes Axiom der Art $\forall x B(x)$ und jede Konstante c in S wird die neue Aussage $B(c)$ zu S hinzugefügt. Ebenso wähle für jedes Axiom der Art $\exists x B(x)$ ein neues Konstantensymbol c' (wobei c' noch nicht in S vorkommt) und füge die neue Aussage $B(c')$ zu S hinzu. Dadurch entsteht ein neues System von Axiomen S^*, wobei $S \subset S^*$. Dann ist auch S^* konsistent.*

Beweis. Es gilt nach Regel 4, Abschnitt 8.5, daß $\forall x B(x) \to B(c)$ eine gültige Aussage ist. Daher führt das Hinzufügen von $B(c)$ zu keinen neuen gültigen Aussagen. Insbesondere nicht zu einem Widerspruch. Nach Regel 5 gilt ebenso, falls ein Widersprich mit einer neuen Aussage der Art $B(c')$ erreicht werden kann, dann kann dieser Widerspruch auch erreicht werden durch die Aussage $\exists x B(x)$. Da aber S widerspruchsfrei ist, muß S auch widerspruchsfrei bleiben, nachdem die neue Aussage $B(c')$ hinzugefügt wird. □

Satz 16 (Vollständigkeitssatz; vollständige Version)**.** *Sei S eine konsistente Sammlung von Aussagen. Dann gibt es ein Modell M für S, wobei die Kardinalität von M nicht größer ist als die Kardinalität von S, falls S unendlich groß ist. Falls S endlich ist, ist die Kardinalität von M nicht größer als die Kardinalität von $\mathbb{N}$.*

Beweis. Sei $A \in S$ eine Aussage. Im allgemeinen hat A verschiedene Quantoren ("$\exists x$" und "$\forall x$"). Nun, wir können A ersetzen mit einer gleichwertigen Aussage der Art $Q_1 \cdots Q_r B$, wobei die Q_i jeweils Quantoren sind und B eine WFF mit entsprechenden freien Variablen ist, wobei B keine Quantoren besitzt. Dies gilt nach Regeln 3 und 7 in Abschnitt 8.5. Warum?

Falls etwa A die Aussage

$$(\forall x P(x)\&(\forall x Q(x))$$

[12] Allerdings setzt die Existenz von solchen Äquivalenzklassen das Auswahlaxiom voraus. Es gibt dann auch unendlich viele verschiedene Aussagen der Art "$c = c'$". Daher ist eine abzählbare Liste, $F_1, F_2, \ldots$, wie vorher im Allgemeinen nicht möglich. Aber wir können die Aussage $c = c'$ als eine einzige *Klasse* von Aussagen betrachten. Diese Aussage definiert dann unsere Äquivalenzrelation.

ist, dann kann x durch eine neue Variable x' in $\forall x Q(x)$ ersetzt werden. Wir bekommen dann die Aussage

$$(\forall x P(x) \& (\forall x' Q(x')).$$

Nach Regel 7 ist dies dann

$$\forall x (P(x) \& (\forall x' Q(x'))).$$

Dann wiederum nach Regel 7 ist dies

$$\forall x (\forall x' (P(x) \& Q(x'))).$$

Es ist eine Übung, zu zeigen, daß alle möglichen Aussagen mit Quantoren sich so umgestalten lassen, daß die Quantoren vorne stehen.

Sei nun $S_0 = S$, und für jedes $n \in \mathbb{N}$ sei $S_n = S^*_{n-1}$. Nach Satz 15 ist dann S_n auch konsistent, für jedes n. Sei

$$\overline{S} = \cup_{n \in \mathbb{N}} S$$

und sei T die Teilmenge von $\overline{S}$, bestehend aus den Elementen von $\overline{S}$ die *keine* Quantoren enthalten. T ist dann eine konsistente Sammlung von Aussagen, und es existiert nach Satz 14 ein Modell für T. Die Behauptung ist, daß M auch ein Modell für S ist.

Denn, sei A eine Aussage in S. Angenommen, A enthält r Quantoren. Falls $r = 0$, dann ist $A \in T$ und daher ist A wahr in M. Sei daher $r > 0$ und sei angenommen, daß M ein Modell ist für alle Aussagen in $\overline{S}$ mit $r - 1$ Quantoren. Nun, A ist entweder von der Art $\forall x B(x)$ oder von der Art $\exists x B(x)$, wobei $B(x)$ eine Formel ist mit $r - 1$ Quantoren. Wir betrachten den Fall $A \equiv \forall x B(x)$.

Sei c eine beliebige Konstante in S. Dann sind sowohl c als auch die Aussage A enthalten in S_n, für ein $n \in \mathbb{N}$. D.h. die Aussage $B(c)$ ist in $S^*_n \subset \overline{S}$ enthalten, und da $B(c)$ nur $r - 1$ Quantoren besitzt, folgt, daß $B(c)$ wahr ist in M. Dies gilt für alle Konstanten c in S. Daher ist A wahr in M.

Der Fall $A \equiv \exists x B(x)$ ist ähnlich. Daher folgt nach vollständiger Induktion über die Anzahl r der Quantoren in A, daß A wahr ist in M, für alle r. $\square$