Grundlagen der Mathematik

(Arbeitstitel, work in progress)

Juni 2023

Inhaltsverzeichnis

1 Logisches Schließen

1.1 Grundbegriffe

1.1.1 Schlussregeln

Logisches Schließen findet in einzelnen Schritten statt. Ein Schritt stellt hierbei immer die Ableitung einer Schlussfolgerung aus einer oder mehreren Voraussetzungen dar. Die Voraussetzungen heißen *Prämissen*, die Schlussfolgerung *Konklusion*. Darstellen wollen wir den Schritt durch eine waagerechte Linie, wobei die Prämissen oberhalb befindlich sein sollen, und die Konklusion unterhalb. Der Schritt

$$\frac{\text{Wenn es regnet, wird die Straße nass} \qquad \text{Es regnet}}{\text{Die Straße wird nass}}$$

beschreibt beispielsweise, dass aus den Prämissen »Wenn es regnet, wird die Straße nass« und »Es regnet« die Konklusion »Die Straße wird nass« gefolgert wird.

Schlüsse wie der Obige treten in der Mathematik ständig auf. Ihnen allen liegt ein bestimmtes Muster zugrunde, welches sich durch eine als *Modus ponens* oder *Abtrennungsregel* bezeichnete schematische *Schlussregel* beschreiben lässt. Es bezeichne hierzu $A \Rightarrow B$ die Implikation »wenn A, dann B«. Es dürfen nun in

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

für A, B beliebige Aussagen eingesetzt werden. So darf »Es regnet» für A und »Die Straße wird nass« für B eingesetzt werden.

1.1.2 Sequenzen

Das Schließen von Aussagen allein genügt nicht. Um freier argumentieren zu können, würden wir gerne den Umstand beschreiben können, dass eine Aussage unter bestimmten Annahmen abgeleitet werden konnte. Diese Annahmen A_k sind selbst Aussagen. Wir fassen sie zu einer endlichen Ansammlung

$$\Gamma := [A_1, A_2, \ldots, A_n]$$

zusammen, worunter wir eine endliche Liste, oder auch eine endliche Menge verstehen wollen, denn man soll mit dieser Liste umgehen können wie mit einer Menge. Das heißt, es ist nicht von Bedeutung, wie oft eine Aussage vorkommt oder in welcher Reihenfolge die Aussagen stehen. Man bezeichnet Γ als die *Antezedenz* oder die Liste der *Antezedenzen*. Es wird Γ auch der *Kontext* oder die *Umgebung* genannt, das sind auf die Typentheorie zurückzuführende Sprechweisen, die einen ganz ähnlichen Formalismus besitzt. Wir bezeichnen die Symbolik

$$\Gamma \vdash A$$

als *Sequenz*. Sie drückt das *Urteil* aus, dass die Aussage A aus den Annahmen vermittels Schlussregeln ableitbar ist. Der Modus ponens wird nun in der allgemeinen Form

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$$

beschrieben. Wir argumentieren beim Schließen also ab jetzt nicht mehr mit den Aussagen selbst, sondern mit den Sequenzen. Dies hat einen wichtigen Grund, nämlich dass die Berücksichtigung der Abhängigkeit von Annahmen expliziter Teil des Schließens wird.

Ein Kontext kann auch eine leere Liste sein. Besitzt eine vermittels Schlussregeln ableitbare Sequenz einen leeren Kontext, so bezeichnet man die Antezedenz als ein *Theorem* im engeren Sinne. Ein Theorem ist also eine Aussage, die für sich allein gilt, ohne dass dafür irgendwelche Annahmen getroffen werden müssen.

Für Sequenzen gilt die *Abschwächungsregel*. Sie besagt, dass falls die Aussage A bereits aus Γ ableitbar ist, diese Aussage erst recht ableitbar ist, wenn zu Γ weitere Annahmen Γ' hinzugefügt werden. Kurzum gilt die Regel

$$\frac{\Gamma \vdash A}{\Gamma, \Gamma' \vdash A}.$$

Hierbei bedeutet Γ, Γ' die Konkatenation der Listen Γ und Γ', also im Wesentlichen dasselbe wie die Vereinigung $\Gamma \cup \Gamma'$, insofern man die Kontexte als Mengen betrachtet.

1.1.3 Zulässige Schlussregeln

Wiewohl die Regeln des Schließens den Mechanismus zum Beweis von Aussagen bilden, ist ihre Rolle sogar noch ein wenig tiefgreifender. Wir können sie nämlich ebenfalls zur Ableitung *weiterer Regeln* nutzen. Das heißt, wir können sie dazu

nutzen, den logischen Kalkül selbst zu erweitern. Erweiterungen dieser Art nennen wir *zulässige Schlussregeln.*

Mit den bisherigen Regeln ist bereits die zulässige Regel

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma' \vdash A}{\Gamma, \Gamma' \vdash B}$$

ableitbar, die eine allgemeinere Form des Modus ponens darstellt. Man erhält sie kurzerhand, indem den Prämissen des Modus ponens jeweils die Abschwächungsregel vorgesetzt wird:

$$\frac{\dfrac{\Gamma \vdash A \Rightarrow B}{\Gamma, \Gamma' \vdash A \Rightarrow B} \quad \dfrac{\Gamma' \vdash A}{\Gamma, \Gamma' \vdash A}}{\Gamma, \Gamma' \vdash B}$$

Die einfache Form des Modus ponens erhält man mit $\Gamma' := \Gamma$ als Spezialfall unter Anwendung der Kontraktionsregel.

1.1.4 Implikationseinführung

Ich möchte mich nun der Frage zuwenden, wie eine Implikation $A \Rightarrow B$ bewiesen wird. Intuitiv ist hierzu aus der Annahme A die Aussage B zu folgern. Das heißt, es genügt die Ableitung der Sequenz $A \vdash B$. Ein weiteres Mal gilt es noch zu berücksichtigen, dass ein Beweis auch auf einen vorausgesetzten Kontext Γ beschränkt sein dürfen soll. Reflektiert man darüber eine Weile, dürfte es der Überlegung nach wohl genügen, dass A einfach dem Kontext Γ hinzugefügt wird, woraus B zu folgern ist. Man gelangt zur Regel

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}.$$

Wer diese Regel nicht so leicht fassbar findet, insbesondere nicht direkt plausibel, ob sie bedenkenlos eingesetzt werden darf, der ist nicht allein. Es gibt auch logische Kalküle, die diese Regel nicht explizit enthalten. Sie tritt dennoch als *Deduktionstheorem* in Erscheinung, ein metalogisches Theorem, dessen Beweis erst erbracht werden muss. Ich möchte diesen Weg allerdings aus einem bestimmten Grund nicht gehen. Nämlich ist beim Beweis eigentlich natürliches Schließen auf der metalogischen Ebene zu verwenden, wenn dies auch in informaler Weise stattfinden mag. Aber nicht jeder Leser weiß zu diesem Zeitpunkt, wie akkurates logisches Schließen geht. Der Leser benötigt am Anfang etwas, um sich an den eigenen Haaren aus dem Sumpf zu ziehen.

1.1.5 Axiome

Zur Komplettierung des Kalküls gesellen sich schließlich auch noch *Axiome* hinzu, das sind gemachte Grundannahmen, die nicht weiter bewiesen werden müssen. Sie sollten daher möglichst plausibel, oder besser noch zweifelsfrei einsichtig sein. Für die Logik selbst genügt das Axiom

$$A \vdash A.$$

Der Kalkül funktioniert dergestalt, dass für A eine beliebige Aussage eingesetzt werden darf, worunter auch zusammengesetzte Aussagen fallen. Eine gern gewählter Weg der Definition des logischen Kalküls sieht A als eine metasprachliche Variable, für die eine beliebige Formel eingesetzt werden darf. Unter dieser Sichtweise spricht man von einem *Axiomenschema*. Wie eine Schablone produziert es für jede Einsetzung einer konkreten logischen Formel ein eigenes Axiom.

Anstelle A, B, C werden für metasprachliche Variablen zuweilen auch die griechischen Buchstaben φ, ψ, χ benutzt. Man muss sie von atomaren logischen Variablen unterscheiden, für die wir in diesem Buch, um Missverständnissen aus dem Weg zu gehen, kleine Buchstaben a, b, c oder p, q, r verwenden werden. Sprachlich suggestiv steht φ für *Formel* oder *formula*, a für *Aussage* und p für *proposition*.

In diesem Sinne sind auch die Schlussregeln Schemata. Sofern man Schlussregeln mit null Prämissen gestattet, lässt sich das Axiomenschema auch als Regel

$$\frac{}{A \vdash A}$$

auffassen. In dieser Weise wollen wir die Anwendung von Axiomen in den Beweisbäumen darstellen.

Axiome in der Form von Sequenzen heißen auch *Grundsequenzen*.

Wir haben nun die Mittel in der Hand, um erste Theoreme beweisen zu können. Es ist $A \Rightarrow A$ ein Theorem. Der Beweisbaum ist:

$$\dfrac{\dfrac{}{A \vdash A}\,\text{Axiom}}{\vdash A \Rightarrow A}\,\text{Implikationseinführung}$$

Unter der Lesung, dass A eine Metavariable ist, handelt es eigentlich nicht nur um ein Theorem, sondern um ein Schema von Theoremen. Setzt man für A bspw. die konkrete Formel $p \Rightarrow q$ ein, bekommt man das konkrete Theorem

$$\vdash (p \Rightarrow q) \Rightarrow (p \Rightarrow q).$$

1.1.6 Junktoren

Bisher traten zusammengesetzte Aussagen alleinig in Form einer Implikation auf. Will man logische Zusammenhänge beschreiben können, muss die logische Sprache um weitere Junktoren bereichert werden. Unter einem *Junktor* versteht man einen logischen Operator, der Aussagen zu einer zusammengesetzten Aussage verknüpft. Von Belang sind zunächst fünf Stück.

Wir werden einen Junktor durch *Einführungsregeln* und *Beseitigungsregeln* charakterisieren. Die Regeln der Implikation wurden bereits beschrieben; die Einführung geschieht per Implikationseinführung, die Beseitigung per Modus ponens. Für die restlichen Junktoren der Aussagenlogik lassen sich die Regeln wahlweise in Form von Axiomenschemata oder in Form von Schlussregeln darstellen. Ich möchte das per Schemata machen, weil diese ein wenig kompakter sind, was sie hoffentlich ein wenig leichter einsichtig macht. Die entsprechenden Schlussregeln leiten wir anschließend als zulässige Regeln ab.

Die Konjunktion $A \wedge B$, auch Und-Verknüpfung genannt, sprich »A und B«, ist charakterisiert durch die Sequenzen

$$A, B \vdash A \wedge B; \qquad A \wedge B \vdash A; \qquad A \wedge B \vdash B.$$

Aus dem Fall von sowohl Regen als auch Schnee ist der Fall von Schneeregen ableitbar. Aus dem Fall von Schneeregen ist der Fall von Regen ableitbar. Aus dem Fall von Schneeregen ist der Fall von Schnee ableitbar. So sind diese Sequenzen zu verstehen.

Die Einführung der Konjunktion geschieht mit der Regel

$$\frac{\Gamma \vdash A \qquad \Gamma' \vdash B}{\Gamma, \Gamma' \vdash A \wedge B}.$$

Denn es findet sich der Beweisbaum:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A, B \vdash A \wedge B}\,\text{Axiom}}{A \vdash B \Rightarrow A \wedge B}\,\text{Impl-Einf.}}{\vdash A \Rightarrow (B \Rightarrow A \wedge B)}\,\text{Impl-Einf.} \qquad \Gamma \vdash A}{\dfrac{\Gamma \vdash B \Rightarrow A \wedge B \qquad \Gamma' \vdash B}{\Gamma, \Gamma' \vdash A \wedge B}\,\text{MP}}\,\text{MP}$$

Es steht MP als Abkürzung für Modus ponens, und Impl-Einf. für Implikationseinführung. Man schreibt alternativ auch das Kürzel ⇒E anstelle Impl-Einf. und das Kürzel ⇒B anstelle von MP. Hierbei steht E offenkundig für *Einführung* und B für *Beseitigung*. Aber Vorsicht, in der englischsprachigen Literatur sind das I für *introduction* und E für *elimination*.

Die beiden Regeln zur Beseitigung der Konjunktion sind

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}, \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}.$$

Denn es findet sich:

$$\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A}\,\text{Axiom}}{\vdash A \wedge B \Rightarrow A}\,\text{Impl-Einf.} \qquad \Gamma \vdash A \wedge B}{\Gamma \vdash A}\,\text{MP}$$

Die Disjunktion $A \vee B$, auch Oder-Verknüpfung genannt, sprich »A oder B«, ist charakterisiert durch die Sequenzen

$$A \vdash A \vee B; \qquad B \vdash A \vee B; \qquad A \vee B, (A \Rightarrow C), (B \Rightarrow C) \vdash C.$$

So ist »Die Erde des Beetes ist nass« ableitbar aus »Es hat geregnet oder das Beet wurde gegossen«. Denn sowohl »Es hat geregnet« als auch »Das Beet wurde gegossen« impliziert »Die Erde des Beetes ist nass«.

Die beiden Regeln zur Einführung der Disjunktion sind

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}, \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}.$$

Die Regel zur Beseitigung der Disjunktion ist

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma', A \vdash C \qquad \Gamma'', B \vdash C}{\Gamma, \Gamma', \Gamma'' \vdash C}.$$

Die Beweise dieser Regeln seien dem Leser überlassen.

Eine Aussage wie »Bertram wird seine Hausaufgaben nicht machen« formuliert man gern in der Form »Wenn Bertram seine Hausaufgaben macht, färbt sich der Mond grün«. In gleichartiger Weise lässt sich die Verneinung auch in der formalen Logik definieren. Hierzu legt man als Hilfsbegriff zunächst $\bot$ als die *Kontradiktion* fest, sie steht für eine widersprüchliche Formel.

Die Negation $\neg A$, auch Verneinung genannt, sprich »nicht A«, definiert man als identisch mit $A \Rightarrow \bot$. Hierdurch sind die Regeln zu ihrer Einführung und Beseitigung auf die der Implikation zurückführbar. Es ergibt sich

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}, \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma' \vdash A}{\Gamma, \Gamma' \vdash \bot}.$$

Alternativ ließe sich die Negation durch die Sequenzen

$$(A \Rightarrow \bot) \vdash \neg A; \qquad A, \neg A \vdash \bot$$

charakterisieren. Man überzeuge sich, dass dies aufs selbe hinausläuft.

Die Äquivalenz $A \Leftrightarrow B$, sprich »A genau dann, wenn B«, definiert man als identisch mit $(A \Rightarrow B) \wedge (B \Rightarrow A)$. Insofern sind die Regeln zu ihrer Einführung und Beseitigung auf die der Konjunktion zurückführbar. Es ergibt sich

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma' \vdash B \Rightarrow A}{\Gamma, \Gamma' \vdash A \Leftrightarrow B}, \qquad \frac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash A \Rightarrow B}, \qquad \frac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash B \Rightarrow A}.$$

Die entsprechenden charakterisierenden Sequenzen sind

$$(A \Rightarrow B), (B \Rightarrow A) \vdash A \Leftrightarrow B; \qquad (A \Leftrightarrow B), A \vdash B; \qquad (A \Leftrightarrow B), B \vdash A.$$

1.1.7 Quantoren

Eine logische Sprache, die der freien Formulierung mathematischer Zusammenhänge dienlich sein soll, muss hinreichend reichhaltig sein. Ebenfalls schrieb der Philosoph Ludwig Wittgenstein in seinem *Tractatus* den ähnlichen Gedanke »Die Grenzen meiner Sprache bedeuten die Grenzen meiner Welt.« Bislang fehlt das wichtige Konzept der Quantifizierung, das die Aussagenlogik zur Prädikatenlogik erweitert.

In der Prädikatenlogik treten *Aussageformen* auf. Das sind Formeln, die *freie Variablen* enthalten. Erst wenn jede der freien Variablen mit einem Wert belegt wird, entsteht eine Aussage. Außerdem treten Quantoren auf. Ein *Quantor* bindet eine freie Variable, und macht eine Aussageform dabei ebenfalls zu einer bestimmten Aussage.

Es sei $A(x)$ eine Aussageform mit der freien Variable x. Anstelle von $A(x)$ schreibt man auch kurzum A. Anstelle von $A(t)$ schreibt man auch $A[x := t]$ oder $A[t/x]$, womit die Ersetzung jedes Vorkommens von x durch den Term t gemeint ist. Genauer gesagt die Ersetzung jedes *freien* Vorkommens, wobei man außerdem einer möglichen Überschattung einer der in t enthaltenen Variablen aus dem Weg gehen muss. Diese Spitzfindigkeiten tauchen allerdings erst auf, wenn man mit Verschachtelungen von Quantoren hantiert. Ich will später genauer darauf eingehen.

Die wesentlichen beiden Quantoren sind der *Allquantor* $\forall$ und der *Existenzquantor* $\exists$. Man ließt $\forall x\colon A(x)$ als »für alle x gilt $A(x)$« oder »jedes x hat die Eigenschaft $A(x)$«. Man ließt $\exists x\colon A(x)$ als »es gibt mindestens ein x, für das $A(x)$ gilt« oder »mindestens ein x hat die Eigenschaft $A(x)$«.

Quantifiziert wird immer über ein bestimmtes *Diskursuniversum*. Darunter versteht man die Gesamtheit der Objekte, auf die sich »für alle« und »es gibt« bezieht. Um bestimmten Komplikationen aus dem Weg zu gehen, muss es nichtleer sein.

Zur Veranschaulichung des Übergangs von der Aussagenlogik zur Prädikatenlogik wählen wir ein endliches, das lediglich die Zahlen von eins bis vier enthält. Die Aussage $\forall x\colon A(x)$ bedeutet nun insofern dasselbe wie

$$A(1) \wedge A(2) \wedge A(3) \wedge A(4).$$

Diese schlichte Konjunktion gibt Anlass zu der Schlussregel

$$\frac{\Gamma \vdash \forall x\colon A(x)}{\Gamma \vdash A(t)}. \qquad (t \text{ muss eine der Zahlen von eins bis vier sein})$$

Die Beseitigung der Allquantifizierung darf insofern als Analogon zur Beseitigung der Konjunktion verstanden werden.

Im Fortgang soll $\Gamma \vdash A(a)$ bedeuten, dass die Aussageform $A(a)$ aus dem Kontext Γ ableitbar ist, wobei a beliebig gelassen wird. Man leitet die vier Sequenzen

$$\Gamma \vdash A(1); \quad \Gamma \vdash A(2); \quad \Gamma \vdash A(3); \quad \Gamma \vdash A(4)$$

sozusagen in einen Zug ab. Es stellt sich nun die Frage

$$\frac{\Gamma \vdash A(a)}{\Gamma \vdash \forall x\colon A(x)}?$$

Betrachten wir dazu $a = 1 \vdash A(a)$. Mit der bedenklichen Regel erhielte man aus ihr $a = 1 \vdash \forall x\colon A(x)$. Diese trifft insbesondere im Fall $a := 1$ zu. Nun braucht man $1 = 1$ nicht vorauszusetzen, womit man $\vdash \forall x\colon A(x)$ erhält. Den Quantor beseitigen wir nun noch mit $x := a$, und erhalten $\vdash A(a)$. Die Annahme wurde also aus der Sequenz herausgemogelt. Um dies zu unterbinden, legen wir fest, dass a keine freie Variable einer der Antezedenzen sein darf.

Die Regel zur Einführung ist demnach zu formulieren als

$$\frac{\Gamma \vdash A(a)}{\Gamma \vdash \forall x\colon A(x)} (a \notin \mathrm{FV}(\Gamma, \forall x\colon A(x))).$$

Hierbei steht die Symbolik $\mathrm{FV}(\Gamma)$ für die Menge der freien Variablen von Γ. Mit elementarer Mengenlehre definiert man sie präzise als Rekursion über den Formelaufbau. Man legt fest

$$\begin{aligned}
&\mathrm{FV}(A \wedge B) = \mathrm{FV}(A \vee B) = \mathrm{FV}(A \Rightarrow B) = \mathrm{FV}(A \Leftrightarrow B) = \mathrm{FV}(A) \cup \mathrm{FV}(B),\\
&\mathrm{FV}(\neg A) = \mathrm{FV}(A), \qquad \mathrm{FV}(\forall x\colon A) = \mathrm{FV}(\exists x\colon A) = \mathrm{FV}(A) \setminus \{x\},\\
&\mathrm{FV}(\bot) = \mathrm{FV}(\top) = \emptyset, \quad \mathrm{FV}(P(t_1, \ldots, t_n)) = \mathrm{FV}(t_1) \cup \ldots \cup \mathrm{FV}(t_n).
\end{aligned}$$

Hierbei steht P für ein n-stelliges Prädikat. Und es ist $\mathrm{FV}(t)$ die Menge der Variablen des Terms t. Man legt sie abermals rekursiv fest als

$$\mathrm{FV}(t_1 + t_2) = \mathrm{FV}(t_1 - t_2) = \mathrm{FV}(t_1 \cdot t_2) = \mathrm{FV}(t_1) \cup \mathrm{FV}(t_2),$$
$$\mathrm{FV}(-t) = \mathrm{FV}(t), \quad \mathrm{FV}(v) = \{v\}, \quad \mathrm{FV}(c) = \emptyset,$$

wobei v für eine Variable und c für eine Konstante steht.

Die Aussage $\exists x\colon A(x)$ ist gleichwertig mit

$$A(1) \vee A(2) \vee A(3) \vee A(4).$$

Diese Perspektive gibt Anlass zur Einführungsregel

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x\colon A(x)}. \quad (t \text{ muss eine der Zahlen von eins bis vier sein})$$

Bei der Beseitigung müssen wir nun gewissermaßen eine Fallunterscheidung in die vier Fälle vornehmen und bestätigen, dass jeder Fall dieselbe Aussage B impliziert. Dies soll allerdings parametrisch in einer einzigen Ableitung stattfinden. Man gelangt zu

$$\frac{\Gamma \vdash \exists x\colon A(x) \qquad \Gamma', A(a) \vdash B}{\Gamma, \Gamma' \vdash B}(a \notin \mathrm{FV}(\Gamma, \Gamma', B, \exists x\colon A(x))).$$

Diese Regel wird wie folgt interpretiert. Mit der Existenzaussage $\exists x\colon A(x)$ liegt ein Zeuge a mit $A(a)$ vor. Unter Verwendung von $A(a)$ wird nun eine Aussage B abgeleitet, in der a nicht frei vorkommt. Somit gilt B unabhängig vom gewählten Zeugen, was notwendig ist, da unbekannt bleibt, welcher der Zahlen von eins bis vier als Zeuge vorliegt.

Ohne die Bedingung an a ließe sich leicht Schabernack vollführen. Man könnte beispielsweise kurzerhand eine Existenzaussage zu einer Allaussage machen:

$$\dfrac{\dfrac{\vdash \exists x\colon A(x) \quad \overline{A(a) \vdash A(a)}}{\vdash A(a)}}{\vdash \forall x\colon A(x)}$$

Abschließend verbleibt noch näher zu erläutern, wie Substitution vonstatten geht. Ersetzt wird nur jedes freie Vorkommen einer Variablen. Ein durch einen Quantor gebundenes Vorkommen der Variable bleibt dagegen erhalten. So resultiert die Substitution

$$(A(x) \wedge \forall x : B(x))[x := y] \quad \text{in} \quad A(y) \wedge \forall x\colon B(x).$$

Außerdem darf es bei einer Substitution nicht zu einer Überschattung durch eine gebundene Variable kommen. Die Substitution

$$(\forall y\colon A(x) \wedge B(y))[x := y]$$

darf beispielsweise nicht direkt ausgeführt werden. Man geht der Überschattung aus dem Weg, indem die gebundene Variable y zuerst in eine frische, nehmen wir z, umbenannt wird. Das Resultat der Substitution ist also

$$\forall z\colon A(y) \wedge B(z), \quad \text{nicht} \quad \forall y\colon A(y) \wedge B(y).$$

1.1.8 Substitution

Es ist noch zu präzisieren, wie Substitution genau vonstatten geht. Substituiert werden können sowohl atomare logische Variablen gegen Formeln als auch Individuenvariablen gegen Terme. Betrachten wir zunächst die logischen.

Allgemein definiert man ihre Substitution

$$A[v_1 := C_1, \ldots v_n := C_n], \text{ kurz } A[S] \text{ oder } S(A)$$

rekursiv über den Formelaufbau als

$$\begin{aligned} (\neg A)[S] &:= \neg(A[S]), & (\forall x\colon A)[S] &:= (\forall x\colon (A[S])),\\ (A \circ B)[S] &:= ((A[S]) \circ (B[S])), & (\exists x\colon A)[S] &:= (\exists x\colon (A[S])). \end{aligned}$$

wobei $\circ$ jeder der zweistelligen Junktoren $\wedge, \vee, \Rightarrow, \Leftrightarrow$ ist. Die Basisfälle sind für die atomaren Variablen $v_1, \ldots, v_n$ und w definiert gemäß

$$w[v_1 := C_1, \ldots, v_n := C_n] := \begin{cases} C_k, & \text{wenn sich } k \text{ mit } v_k = w \text{ findet,}\\ w, & \text{sonst.} \end{cases}$$

Für $n \geq 2$ spricht man von *simultaner Substitution.*

Für $n = 1$ vereinfacht sich die Substitution zu

$$w[v := C] := \begin{cases} C, & \text{wenn } v = w,\\ w, & \text{wenn } v \neq w. \end{cases}$$

Beispielsweise ist

$$(a \wedge b \Rightarrow a)[a := a \vee b] = ((a \vee b) \wedge b \Rightarrow (a \vee b)).$$

Simultane Substitution darf im Allgemeinen nicht schrittweise durchgeführt werden, weil dadurch ein anderes Resultat entstehen kann. Zum Beispiel ist

$$(a \wedge b)[a := b, b := c] \quad = (b \wedge c),$$
$$(a \wedge b)[a := b][b := c] = (c \wedge c).$$

Implementiert man die Substitution als Computerprogramm, bildet sie üblicherweise abstrakte Syntaxbäume auf abstrake Syntaxbäume ab.

Die Substitution von Individuenvariablen gegen Terme definiert man ganz analog. Hier ist allerdings hinsichtlich der Quantoren zu beachten, dass nur freie Variablen substituiert werden, und man eine unter Umständen entstehende Überschattung durch Umbenennung der gebundenen Variablen umgehen muss.

1.1.9 Zur Syntax

So wie »Punktrechnung vor Strichrechnung« gilt, legt man für jeden Junktor zur Einsparung von Klammern eine Stufe der Priorität fest. In absteigender Rangfolge sind dies $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$. So wird die Formel

$$\neg A \wedge B \vee C \Rightarrow D \quad \text{gelesen als} \quad (((\neg A) \wedge B) \vee C) \Rightarrow D.$$

Weiterhin legt man die Implikation als rechtsassoziativ fest. So wird

$$A \Rightarrow B \Rightarrow C \quad \text{gelesen als} \quad A \Rightarrow (B \Rightarrow C).$$

Wie den Junktoren kommt auch den Quantoren eine Rangstufe zu. Weil diese aber präfix sind, ist bei ihnen lediglich die rechte Seite zu berücksichtigen. Hier sind zwei Varianten verbreitet. In der Schreibweise $(\forall x)A(x)$ oder kurz $\forall x A(x)$ haben sie wie die Verneinung die höchste Rangstufe. In der Schreibweise $\forall x\colon A(x)$ oder $\forall x.\, A(x)$ dagegen die niedrigste, also eine Stufe niedriger als das Bikonditional, so dass alles hinter dem Doppelpunkt in den Wirkungsbereich des Quantors fällt. So wird

$$\forall x\colon A(x) \wedge B \Rightarrow C \quad \text{gelesen als} \quad \forall x\colon ((A(x) \wedge B) \Rightarrow C).$$

Manche Schüler haben Schwierigkeiten, die Struktur von Termen zu durchschauen. Infolge kann es bei ihnen zu Flüchtigkeitsfehlern bei der Ersetzung von Variablen durch Terme kommen. Sie vergessen, dass ein Term vor der Einfügung zunächst geklammert werden muss. Erst die Operatorrangfolge gewährt es, die Klammern unter Umständen nachträglich entfallen zu lassen. Für diese Schüler mag es förderlich sein, einen Term als *abstrakten Syntaxbaum* darzustellen. Gleichermaßen

verhält es sich mit der Programmiersprache Lisp, die Terme als Schachtelung von Listen darstellt, deren Klammern obligatorisch sind. Die Aussage $A \wedge B \Rightarrow C$ ist beispielsweise beschreibbar als

```
(implies (and A B) C).
```

Im Wesentlichen veranschaulicht diese Schachtelung nichts anderes als den abstrakten Syntaxbaum. Man kann gewissermaßen sagen, dass Lisp eine Programmiersprache ohne Syntax ist. Fast ohne, im höheren Sinne ohne.

Um sich unmissverständlich auszudrücken, formalisieren Logiker die logische Sprache gern. Es wird hierzu eine *formale Sprache* spezifiziert, was vermittels sogenannter *Produktionsregeln* gemacht werden kann. Insofern Produktionsregeln etwas kryptisch anmuten mögen, beschreiben Logiker die syntaktische Struktur auch in Worten. Für die Aussagenlogik üblicherweise folgendermaßen.

1. Die atomaren Variablen a, b, c usw. sind Formeln.
2. Die Symbole $\bot, \top$ sind Formeln.
3. Ist $\neg A$ eine Formel, so ist auch $(\neg A)$ eine.
4. Sind A, B Formeln, so ist auch $(A \wedge B)$ eine.
5. Sind A, B Formeln, so ist auch $(A \vee B)$ eine.
6. Sind A, B Formeln, so ist auch $(A \Rightarrow B)$ eine.
7. Sind A, B Formeln, so ist auch $(A \Leftrightarrow B)$ eine.
8. Nichts anderes ist eine Formel.

Schreibt man viele logische Formeln auf, drängt es, zumindest bei privaten Notizen und Rechnungen, nach Kurzschreibweisen. In der Logik ist für das Konditional $A \Rightarrow B$ auch die Schreibweise $A \to B$ gebräuchlich, für das Bikonditional $A \Leftrightarrow B$ entsprechend $A \leftrightarrow B$. Insbesondere in der Schaltalgebra schreibt man auch $\overline{A}$ anstelle von $\neg A$, und AB anstelle von $A \wedge B$ sowie $A + B$ anstelle von $A \vee B$. Hierbei darf die Disjunktion $A + B$ allerdings nicht mit der Kontravalenz $A \oplus B$ verwechselt werden. Für die Quantifizierung $\forall x\colon A(x)$ bietet sich $\forall_x A_x$ oder $\forall x.\, A_x$ als kurzschriftliche Form an.

1.2 Natürliches Schließen

1.2.1 Darstellungsformen

Abgeleitet werden soll das Theorem

$$\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A).$$

Meine favorisierte und in diesem Buch genutzte Form der Darstellung des natürlichen Schließens fügt die aus den Schlussregeln erhaltenen Schlüsse wie Legosteine zu einem Baum zusammen, dem *Beweisbaum* oder *Herleitungsbaum*. Im Eigentlichen stehen in den Blättern die Grundsequenzen, und in der Wurzel das Theorem. Wie wir es bereits getan haben, arbeitet man allerdings auch mit Exemplaren, die irgendwelche Sequenzen in irgendwelche Sequenzen überführen, womit man zulässige Schlussregeln erhält. Allgemeiner ginge ferner die Formulierung als gerichteter azyklischer Graph, die bei einigen Beweisen ein wenig den Schreibaufwand reduzieren würde.

Der Beweisbaum des genannten Theorems ist:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg B \vdash \neg B}\,\text{Axiom} \quad \dfrac{\dfrac{}{A \Rightarrow B \vdash A \Rightarrow B}\,\text{Axiom} \quad \dfrac{}{A \vdash A}\,\text{Axiom}}{A \Rightarrow B, A \vdash B}\,{\Rightarrow}\text{B}}{A \Rightarrow B, \neg B, A \vdash \bot}\,\neg\text{B}}{A \Rightarrow B, \neg B \vdash \neg A}\,\neg\text{E}}{A \Rightarrow B \vdash \neg B \Rightarrow \neg A}\,{\Rightarrow}\text{E}}{\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)}\,{\Rightarrow}\text{E}$$

Die Ausformulierung der Sequenzen verlangt langwieriges erneutes Aufschreiben der Antezedenzen. Sobald man das Prozedere einmal verstanden hat, erscheint es überausführlich. Man kann sich daher verkürzte Darstellungen der Beweisbäume überlegen:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{1 \equiv \neg B} \quad \dfrac{\overline{2 \equiv A \Rightarrow B} \quad \overline{3 \equiv A}}{2, 3 \vdash B}}{1, 2, 3 \vdash \bot}}{1, 2 \vdash \neg A}}{2 \vdash \neg B \Rightarrow \neg A}}{\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\neg B}\,1 \quad \dfrac{\overline{A \Rightarrow B}\,2 \quad \overline{A}\,3}{B}}{\bot}}{\neg A}\,{\sim}3}{\neg B \Rightarrow \neg A}\,{\sim}1}{(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)}\,{\sim}2$$

Die linke Form kürzt die Antezedenzen durch Nummern ab. In der rechten Form entfallen die Antezedenzen vollständig. Stattdessen tauchen sie als in den Blättern gemachte nummerierte *Annahmen* auf, die im Fortgang zur Wurzel irgendwann zu tilgen sind. Ihre Tilgung erscheint nun als Randnotiz.

Tabelle 1.1: Beweis in Form einer Liste von Tabellenzeilen

Abh.	Nr.	Aussage	Regel	auf
1	1	$\neg B$	Axiom	
2	2	$A \Rightarrow B$	Axiom	
3	3	A	Axiom	
2, 3	4	B	$\Rightarrow$B	2, 3
1, 2, 3	5	$\bot$	$\neg$B	1, 4
1, 2	6	$\neg A$	$\neg$E	5
2	7	$\neg B \Rightarrow \neg A$	$\Rightarrow$E	6
$\emptyset$	8	$(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$	$\Rightarrow$E	7

Eine weitere, sehr systematische Darstellung setzt den Beweis aus einer Liste von Tabellenzeilen zusammen. Allerdings ist sie ein wenig mühevoll zu lesen. Jede Zeile enthält eine Aussage und dahinter zusätzlich die Information, wie und woraus die Aussage abgeleitet wurde. Jede der Aussagen bekommt eine Nummer, siehe Tabelle 1.1. Die Nummerierung der Abhängigkeiten ist in derselben Reihenfolge wie zuvor bei den Bäumen angegeben. Wer die Liste genauer betrachtet, erkennt, dass die jeweilige Zeile nichts anderes als die Sequenz Abh. $\vdash$ Nr. darstellt.

Unabhängig von Gentzen entwickelte Stanisław Jaśkowski das natürliche Schließen einige Jahre zuvor. Während Gentzen Beweise als Bäume darstellte, nutzte Jaśkowski zunächst eine grafische Darstellung, die später von Frederic Brenton Fitch adaptiert wurde und in dieser Form nun als *Fitch-Style* bekannt ist. Die Abhängigkeit von einer Annahme wird hier kenntlich gemacht, indem die aus der Annahme abgeleiteten Aussagen hinter einer senkrechten Linie eingerückt stehen. Die Annahme selbst steht am Anfang der Einrückung, und zwar bereits innerhalb, weil sie ja von sich selbst abhängig ist. Siehe Tabelle 1.2.

Zu guter Letzt muss die klassische Darstellung der Beweisführung aufgeführt werden. Die in Worten. Sie zeichnet sich durch die Auslassung mühseliger technischer Details und blumige Formulierungen aus, soll aber genug Information enthalten, dass der Leser im Zweifel eine Formalisierung des Beweises erstellen und verifizieren kann.

Satz 1.1. Es gilt $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$.

Beweis. Aus der Annahme von sowohl $A \Rightarrow B$ als auch $\neg B$ als auch A ist ein Widerspruch abzuleiten. Man erhält B zunächst per Modus ponens aus $A \Rightarrow B$ und A. Nun steht $\neg B$ bereits im Widerspruch zu B. □

Tabelle 1.2: Beweis im Fitch-Style

1	$A \Rightarrow B$	
2	$\quad \neg B$	
3	$\quad\quad A$	
4	$\quad\quad B$	$\Rightarrow$B, 1, 3
5	$\quad\quad \bot$	$\neg$B, 2, 4
6	$\quad \neg A$	$\neg$E, 5
7	$\neg B \Rightarrow \neg A$	$\Rightarrow$E, 6
8	$(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$	$\Rightarrow$E, 7

Als komfortablen Bonus erhält man mit dem Theorem nun im Anschluss kurzerhand eine weitere zulässige Regel, die *Kontrapositionsregel*

$$\frac{\Gamma \vdash A \Rightarrow B}{\Gamma \vdash \neg B \Rightarrow \neg A}, \quad \text{denn} \quad \frac{\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A) \quad \Gamma \vdash A \Rightarrow B}{\Gamma \vdash \neg B \Rightarrow \neg A}.$$

Fügt man ihr den Modus ponens an, findet sich der *Modus tollens*

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma' \vdash \neg B}{\Gamma, \Gamma' \vdash \neg A}.$$

1.2.2 Theoreme der Prädikatenlogik

In einer Formelsammlung zur Prädikatenlogik findet man eine Reihe von Äquivalenzen und Implikationen vor, von denen wir einige beweisen wollen.

Satz 1.2. Es ist $A \wedge \forall x\colon B(x)$ äquivalent zu $\forall x\colon A \wedge B(x)$, sofern die Variable x nicht frei in A vorkommt.

Beweis. Zur Implikation von links nach rechts findet sich der Baum:

$$\dfrac{\dfrac{\dfrac{\overline{A \wedge \forall x\colon B(x)}^{\,1}}{A} \quad \dfrac{\dfrac{\overline{A \wedge \forall x\colon B(x)}^{\,1}}{\forall x\colon B(x)}}{B(x)}}{A \wedge B(x)}}{\forall x\colon A \wedge B(x)}}{(A \wedge \forall x\colon B(x)) \Rightarrow (\forall x\colon A \wedge B(x))}\,{}^{\sim 1} \qquad \dfrac{\dfrac{\dfrac{\overline{A \wedge \forall x\colon B(x)}^{\,1}}{A} \quad \dfrac{\dfrac{\overline{A \wedge \forall x\colon B(x)}^{\,1}}{\forall x\colon B(x)}}{B(u)}}{A \wedge B(u)}}{\forall x\colon A \wedge B(x)}}{(A \wedge \forall x\colon B(x)) \Rightarrow (\forall x\colon A \wedge B(x))}\,{}^{\sim 1}$$

Beide Formen sind zulässig. Die rechte Form gibt dem Parameter den eigenen Bezeichner u, die linke nennt diesen ebenfalls so wie die gebundene Variable. In Worten würde man diesen Beweis wie folgt führen. Es sei u fest, aber beliebig, woraus $A \wedge B(u)$ abzuleiten ist. Laut Voraussetzung gilt sowohl A als auch $\forall x\colon B(x)$. Spezialisierung $x := u$ liefert $B(u)$. Ergo gilt sowohl A als auch $B(u)$, und somit $A \wedge B(u)$.

Zur Implikation von rechts nach links findet sich:

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{\forall x\colon A \wedge B(x)}^{\,1}}{A \wedge B(x)}}{A} \qquad \dfrac{\dfrac{\overline{\forall x\colon A \wedge B(x)}^{\,1}}{A \wedge B(x)}}{B(x)}}{\dfrac{A \wedge \forall x\colon B(x)}{(\forall x\colon A \wedge B(x)) \Rightarrow (A \wedge \forall x\colon B(x))}\,{\scriptstyle\sim 1}}}{\forall x\colon B(x)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\overline{\forall x\colon A \wedge B(x)}^{\,1}}{A \wedge B(u)}}{A} \qquad \dfrac{\dfrac{\overline{\forall x\colon A \wedge B(x)}^{\,1}}{A \wedge B(u)}}{B(u)}}{\dfrac{A \wedge \forall x\colon B(x)}{(\forall x\colon A \wedge B(x)) \Rightarrow (A \wedge \forall x\colon B(x))}\,{\scriptstyle\sim 1}}}{\forall x\colon B(x)}$$

In Worten: Es ist $A \wedge \forall x\colon B(x)$ abzuleiten, also sowohl A als auch $\forall x\colon B(x)$, was sich mit $B(u)$ für ein festes, aber beliebiges u bestätigt. Laut Voraussetzung erhält man $A \wedge B(u)$ per Spezialisierung $x := u$. Ergo gilt sowohl A als auch $B(u)$. □

Die ausführliche Besprechung verdeutlicht nochmals, wie die Floskel *fest, aber beliebig* einen Parameter, über den die Argumentation verläuft, einführt. Der Parameter steht für ein *festes* Objekt, insofern er während der Argumentation für nur ein Objekt steht. Weil das Objekt *beliebig* ist, also keine Einschränkungen an dessen Beschaffenheit gemacht wurden, darf anschließend ohne Weiteres die Einführung einer Allquantifizierung vorgenommen werden. Es besteht im logischen System, wie es in diesem Buch dargelegt wurde, kein formaler Unterschied zwischen einem Parameter und einer Variable. Ein Parameter verhält sich als freie Variable.

1.2.3 Bezug zum Sequenzenkalkül

Einige Regeln des natürlichen Schließens bieten bei der Lesung eines Beweisbaums von der Wurzel aus zu den Blättern hin routinemäßige Zurückführung eines Ziels auf Unterziele. Jedoch nicht jede der Regeln, womit das Schließen dennoch zum Denksport wird. Aufgrund dessen gestaltet sich auch die Auffindung eines Algorithmus' zur automatischen Erzeugung eines Beweisbaums als schwierig.

Der Sequenzenkalkül macht das Schließen nun gänzlich zur Routine. Mithin ist zu diesem Kalkül ein Algorithmus zur Erzeugung von Beweisbäumen vergleichsweise leicht zu finden.

Man darf als dienlich erachten, dass die Darstellung des natürlichen Schließens, wie sie in diesem Buch dargelegt wurde, mit dem Sequenzenkalkül kompatibel ist. In ihm dürfen Sequenzen von der allgemeineren Form

$$A_1 \ldots, A_m \vdash B_1, \ldots, B_n$$

Tabelle 1.3: Die Regeln des Sequenzenkalküls

	Linke Regel	**Rechte Regel**	
$\dfrac{\Gamma \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta}$	$\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}$	$\dfrac{\Gamma \vdash A, \Delta \qquad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'}$	$\dfrac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \Delta'}$
$\dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}$	$\dfrac{\Gamma, A \vdash \Delta \qquad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'}$	$\dfrac{\Gamma \vdash A, B, \Delta}{\Gamma \vdash A \vee B, \Delta}$	$\dfrac{\Gamma \vdash B, B, \Delta}{\Gamma \vdash B, \Delta}$
$\dfrac{\Gamma, \top \vdash \Delta}{\Gamma \vdash \Delta}$	$\dfrac{\Gamma \vdash A, \Delta \qquad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \Rightarrow B \vdash \Delta, \Delta'}$	$\dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}$	$\dfrac{\Gamma \vdash \Delta, \bot}{\Gamma \vdash \Delta}$
$\dfrac{}{\Gamma, \bot \vdash \Delta}$	$\dfrac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}$	$\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}$	$\dfrac{}{\Gamma \vdash \top, \Delta}$

sein, die für die Aussage

$$A_1 \wedge \ldots \wedge A_m \Rightarrow B_1 \vee \ldots \vee B_n$$

steht. Um die Regeln des Sequenzenkalküls vermittels natürlichem Schließen als zulässige Regeln herzuleiten, wird man daher zunächst die Übersetzungsregeln

$$\frac{\Gamma \vdash B_1 \vee \ldots \vee B_n}{\Gamma \vdash B_1, \ldots, B_n}, \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash}, \qquad \frac{\Gamma \vdash B_1, \ldots, B_n}{\Gamma \vdash B_1 \vee \ldots \vee B_n}, \qquad \frac{\Gamma \vdash}{\Gamma \vdash \bot}.$$

fordern. Eine Auflistung der wesentlichen Regeln zeigt die Tabelle 1.3. Sie untergliedern sich in linke und rechte Regeln. Die linken gestatten es dabei, Ziele ebenfalls bezüglich Antezedenzen auf Unterziele zurückzuführen. Jede der Ansammlungen $\Gamma, \Gamma', \Delta, \Delta'$ darf leer sein. Eine algorithmische Umsetzung der Beweissuche mag $\Gamma = \Gamma'$ und $\Delta = \Delta'$ setzen, für den Menschen entstünde dadurch aber umständlicher Schreibaufwand. Exemplarisch soll die linke Regel zur Disjunktion als zulässig bestätigt werden. Für sie findet sich der Baum:

$$\dfrac{\dfrac{}{A \vee B \vdash A \vee B} \quad \dfrac{\dfrac{\Gamma, A \vdash \Delta}{\Gamma, A \vdash \Delta, \Delta'} \quad \dfrac{\Gamma', B \vdash \Delta'}{\Gamma', B \vdash \Delta, \Delta'}}{\Gamma, A \vdash C} \quad \dfrac{\Gamma', B \vdash \Delta'}{\Gamma', B \vdash C}}{\Gamma, \Gamma', A \vee B \vdash C}}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'}$$

Hierbei soll C die Disjunktion der Aussagen von Δ, Δ' sein.

Es folgt am Beispiel des Theoremschemas zur Kontraposition, wie das Schließen vonstatten geht. Die Beweisbäume wären von unten nach oben zu lesen, weil das, was weiter oben steht, eigentlich noch unbekannt ist:

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{A \vdash A}}{\vdash A, \neg A} \quad \dfrac{\overline{B \vdash B}}{B, \neg B \vdash}}{A \Rightarrow B, \neg B \vdash \neg A}}{A \Rightarrow B \vdash \neg B \Rightarrow \neg A}}{\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\overline{B \vdash B}}{\vdash \neg B, B} \quad \dfrac{\overline{A \vdash A}}{\neg A, A \vdash}}{\neg B \Rightarrow \neg A, A \vdash B}}{\neg B \Rightarrow \neg A \vdash A \Rightarrow B}}{\vdash (\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)}$$

Der Kalkül muss ein klassischer sein, sonst wäre die Kontraposition nicht rückgängig zu machen. Noch drastischere Einsicht diesbezüglich schaffen die Bäume:

$$\dfrac{\dfrac{\overline{A \vdash A}}{\vdash A, \neg A}\,\neg\mathrm{R}}{\vdash A \vee \neg A}\,\vee\mathrm{L} \qquad \dfrac{\dfrac{\overline{A \vdash A}}{\vdash \neg A, A}\,\neg\mathrm{L}}{\neg\neg A \vdash A}\,\neg\mathrm{R}$$

Es gibt auch Varianten des Sequenzenkalküls, die ausschließlich die Ableitung von Theoremen der intuitionistischen Logik gestatten. Sie sind allerdings umständlicher zu verwenden, da es sich um Einschränkungen des klassischen Kalküls handelt. Bereits Gentzen beschrieb so einen als LJ in [1]. Eine sorgfältige Diskussion findet man in [11].

Alternative Formen der Regeln zur Implikation sind

$$\frac{\Gamma, \neg A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \Rightarrow B \vdash \Delta}, \qquad \frac{\Gamma \vdash \neg A, B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}.$$

Die Regeln der Allquantifizierung sind

$$\frac{\Gamma, A(t) \vdash \Delta}{\Gamma, \forall x\colon A(x) \vdash \Delta}, \qquad \frac{\Gamma \vdash A(u), \Delta}{\Gamma \vdash (\forall x\colon A(x)), \Delta}\,(u \notin \mathrm{FV}(\Gamma, \Delta, A(x))),$$

die der Existenzquantifizierung sind

$$\frac{\Gamma, A(u) \vdash \Delta}{\Gamma, \exists x\colon A(x) \vdash \Delta}\,(u \notin \mathrm{FV}(\Gamma, \Delta, A(x))), \qquad \frac{\Gamma \vdash A(t), \Delta}{\Gamma \vdash (\exists x\colon A(x)), \Delta}.$$

Eine besondere Bedeutung besitzt die Schnittregel

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}.$$

Laut Gentzens Hauptsatz findet sich zu jedem Beweis einer Sequenz, in dem die Schnittregel zur Anwendung kommt, ein alternativer Beweis, der auf sie verzichtet. Kurzum ist sie zulässig, aber redundant. Dieses Resultat ist von großer Bedeutung für die Beweistheorie.

1.2.4 Bezug zum Tableaukalkül

Der *Tableaukalkül* ist ein systematisches Beweisverfahren, bei dem durch abermalige Zurückführung einer Formel auf kleinere Formeln ein Baum entsteht. In einer geläufigen Form des Verfahrens kommt der Beweis einer Aussage zustande, indem ihre Verneinung widerlegt wird. Die Widerlegung stellt sich dadurch her, dass jeder Pfad eine Formel enthält, deren Verneinung bereits auf dem direkten Pfad zur Wurzel vorkam, was auch als *Schließung* des Pfades bezeichnet wird. Der Baum verzweigt sich nicht bei jeder Formel. Man unterscheidet zwischen Formeln vom Typ einer Konjunktion und Formeln vom Typ einer Disjunktion. Lediglich bei den Formeln vom Typ einer Disjunktion findet eine Verzweigung statt.

Es stellt sich im Fortgang heraus, dass der Tableaukalkül in der Logik nicht abgeschieden steht. Ganz im Gegenteil lässt sich ein enger Bezug zum Schließen von Sequenzen herstellen. Genauer gesagt gehört zu jeder Regel des Tableaukalküls eine zulässige Regel des Schließens von Sequenzen, womit sich dieser als ein Teilsystem des allgemeinen Sequenzenkalküls erweist.

Laut der Reductio ad absurdum ist $\Gamma \vdash A$ auf $\Gamma, \neg \vdash \bot$ zurückführbar. Im Weiteren wird $\Gamma \vdash$ als Abkürzung für $\Gamma \vdash \bot$ geschrieben. Man ruft sich nun die Äquivalenz der Aussagen $A \Rightarrow B$ und $\neg A \vee B$ in Erinnerung. Weiterhin befindet man mit den de morganschen Gesetzen die Aussage $\neg(A \wedge B)$ zu $\neg A \vee \neg B$ äquivalent, sowie $\neg(A \vee B)$ zu $\neg A \wedge \neg B$. Aus diesen Überlegungen heraus gelangt man zu den unverzweigenden zulässigen Regeln

$$\frac{\Gamma, A, B \vdash}{\Gamma, A \wedge B \vdash}, \qquad \frac{\Gamma, \neg A, \neg B \vdash}{\Gamma, \neg(A \vee B) \vdash}, \qquad \frac{\Gamma, A, \neg B \vdash}{\Gamma, \neg(A \Rightarrow B) \vdash},$$

und den verzweigenden zulässigen Regeln

$$\frac{\Gamma, A \vdash \quad \Gamma, B \vdash}{\Gamma, A \vee B \vdash}, \qquad \frac{\Gamma, \neg A \vdash \quad \Gamma, \neg B \vdash}{\Gamma, \neg(A \wedge B) \vdash}, \qquad \frac{\Gamma, \neg A \vdash \quad \Gamma, B \vdash}{\Gamma, (A \Rightarrow B) \vdash}.$$

Schließlich wäre noch festzustellen, dass $\Gamma, A, \neg A \vdash$ mit $\Gamma, A \vdash A$ gleichbedeutend ist, und somit die Rolle einer Grundsequenz einnehmen darf.

Ein Beispiel. Mit den aufgestellten Regeln ergibt sich für die Kontraposition der folgende Beweisbaum:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg A, \neg B, \neg\neg A \vdash} \quad \dfrac{}{B, \neg B, \neg\neg A \vdash}}{A \Rightarrow B, \neg B, \neg\neg A \vdash}}{A \Rightarrow B, \neg(\neg B \Rightarrow \neg A) \vdash}}{\neg((A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)) \vdash}}{\vdash (A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)}$$

Wird dieser Baum nun auf den Kopf gestellt und die Notation dergestalt verkürzt, dass jede der Formeln nur einmal aufgeschrieben werden muss, ergibt sich der Tableaukalkül. Man mag das Schließen von Sequenzen insofern als vielseitig bewerten. Die dazugewonnene Sichtweise schafft überdies ein tiefergründiges Verständnis des Tableaukalküls.

1.3 Bemerkungen zur Beweisführung

1.3.1 Widerspruchsbeweise

Beim *Beweis durch Widerspruch* widerlegt man eine Aussage, indem gezeigt wird, dass die Annahme der Aussage zu einem logischen Widerspruch führt. In manchen Situationen bietet diese Art der Argumentation eine große Hilfe. So schreibt der britische Mathematiker Godfrey Harold Hardy in seinem Essay *A Mathematician's Apology* die Worte

> »The proof is by *reductio ad absurdum*, and *reductio ad absurdum*, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers *the game*.«

Zur Schaffung von Klarheit muss man zunächst zwei inhaltlich verschiedene Arten des Widerspruchsbeweises unterscheiden. Präzisieren lässt sich diese Unterscheidung anhand der Regeln

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}, \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}.$$

Die linke Regel stellt die stets verfügbare Negationseinführung dar, die man auch als *Widerlegung durch Widerspruch* bezeichnen kann. In der rechten Regel, der klassischen *Reductio ad absurdum*, gelangt man zunächst per Negationseinführung von $\Gamma, \neg A \vdash \bot$ zu $\Gamma \vdash \neg\neg A$, und daraufhin zu $\Gamma \vdash A$. Die Beseitigung der Doppelnegation ist allerdings lediglich in der klassischen Logik verfügbar, in der intuitionistischen gilt sie dagegen als unzulässig.

Manche stellen die Regeln in einer Form dar, in der die Kontradiktion nicht explizit auftaucht. Wir erhalten sie als zulässige Regeln, indem der Einführung der Kontradiktion direkt ihre Beseitigung angeschlossen wird. Es findet sich

$$\frac{\Gamma, A \vdash \neg B \qquad \Gamma' \vdash B}{\Gamma, \Gamma' \vdash \neg A}, \qquad \frac{\Gamma, \neg A \vdash \neg B \qquad \Gamma' \vdash B}{\Gamma, \Gamma' \vdash A}.$$

Wie zuvor ist die linke Form allgemein verfügbar, die rechte dagegen nur bei Vorhandensein der Beseitigung der Doppelnegation.

1.3.2 Klassische Kontraposition

Eine weitere Regel ist die umgekehrte Kontraposition

$$\frac{\Gamma \vdash \neg A \Rightarrow \neg B}{\Gamma \vdash B \Rightarrow A}.$$

Sie verlangt ebenfalls die klassische Logik. Mit ihr lässt sich nämlich die klassische Reductio ad absurdum herleiten:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma, \neg A, \top \vdash \bot}\,\text{Abschwächung}}{\Gamma, \neg A \vdash \neg\top}\,\text{Neg-Einf.}}{\Gamma \vdash \neg A \Rightarrow \neg\top}\,\text{Impl-Einf.}}{\Gamma \vdash \top \Rightarrow A}\,\text{bedenklich} \qquad \dfrac{}{\top \vdash \top}\,\text{Axiom}}{\Gamma, \top \vdash A}\,\text{Modus ponens}}{\Gamma \vdash A}\,\text{Kürzung der Tautologie}$$

Weil alle anderen Schlüsse unbedenklich sind, kann die umgekehrte Kontraposition als der bedenkliche Schritt identifiziert werden. In der klassischen Logik ist sie allerdings zulässig. Die Herleitung unter Verwendung der Beseitigung der Doppelnegation sei dem Leser überlassen. Als kleiner Tipp sei aber gegeben, dass die Einführung der Doppelnegation unter allen Umständen zulässig ist, wie man sich unschwer überzeugt.

Wir schreiben die Abkürzungen DNE für die Beseitigung der Doppelnegation, LEM für den Satz vom ausgeschlossenen Dritten und EFQ für ex falso quodlibet. Eine Alternative zu DNE bietet LEM zuzüglich EFQ. Manche Beweise verkürzen sich damit, andere verlängern sich. Tatsächlich lässt sich DNE aus LEM zuzüglich EFQ herleiten. Umgekehrt lässt sich sowohl LEM als auch EFQ aus DNE herleiten. Es tut sich die Frage auf, ob sich EFQ aus LEM herleiten lässt. Die Antwort darauf lautet nein. Eine ausführliche Untersuchung findet man in [6].

1.3.3 Notwendige und hinreichende Bedingungen

Manchmal trifft man auf die Ausdrucksweise, eine Bedingung B sei für eine Aussage A notwendig. Sie sagt aus, dass $\neg B$ zu $\neg A$ führt. Falls die Bedingung verletzt ist, kann die Aussage unmöglich gelten. Es liegt demnach die Implikation $\neg B \Rightarrow \neg A$ vor. Sie wird im Sinne der klassischen Logik verstanden. Man hat also

$$(A \Rightarrow B) \iff (B \text{ ist notwendig für } A).$$

Die Ausdrucksweise, eine Bedingung B sei für A hinreichend, sagt aus, dass B die Aussage A bereits nach sich zieht. Es liegt demnach die Implikation $B \Rightarrow A$ vor. Man hat also

$$(B \Rightarrow A) \iff (B \text{ ist hinreichend für } A).$$

Ist eine Bedingung B sowohl notwendig als auch hinreichend für A, liegt eine Äquivalenz vor. Man hat also

$$(A \Leftrightarrow B) \iff (B \text{ ist notwendig und hinreichend für } A).$$

1.3.4 Die zulässige Ersetzungsregel

Mit der Äquivalenz zweier Aussagen verhält es sich in gewisser Weise wie mit einer Gleichheit. Und zwar vermittelt die *zulässige Ersetzungsregel*, eine Teilformel gegen eine zu ihr äquivalente Formel ersetzen zu dürfen, analog wie bei der Termumformung eines Teilterms. Sie ermöglicht die bequeme Äquivalenzumformung von Aussagen, womit man sie als besonders nützlich erachten darf.

Satz 1.3 (Zulässige Ersetzungsregel).
Es gelten die beiden gleichwertigen Regeln

$$\frac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash C(A) \Leftrightarrow C(B)}, \qquad \frac{\Gamma \vdash A \Leftrightarrow B \qquad \Gamma' \vdash C(A)}{\Gamma, \Gamma' \vdash C(B)}.$$

Beweis. Zunächst zur Gleichwertigkeit der beiden Regeln:

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash C(A) \Leftrightarrow C(B)}}{\Gamma \vdash C(A) \Rightarrow C(B)} \quad \Gamma' \vdash C(A)}{\Gamma, \Gamma' \vdash C(B)} \qquad \dfrac{\dfrac{\Gamma \vdash A \Leftrightarrow B \quad \overline{C(A) \vdash C(A)}}{\Gamma, C(A) \vdash C(B)}}{\Gamma \vdash C(A) \Rightarrow C(B)} \quad \dfrac{\dfrac{\Gamma \vdash A \Leftrightarrow B \quad \overline{C(B) \vdash C(B)}}{\Gamma, C(B) \vdash C(A)}}{\Gamma \vdash C(B) \Rightarrow C(A)}}{\Gamma \vdash C(A) \Leftrightarrow C(B)}$$

Wir führen nun eine strukturelle Induktion über den Formelaufbau durch. Die Behauptung wird hierbei in der Form

$$\frac{\Gamma \vdash F \Leftrightarrow F'}{\Gamma, C(F) \vdash C(F')}, \quad C(F) := C[X := F], \quad C(F') := C[X := F']$$

geschrieben. Weil F, F' vertauscht werden dürfen, erhält man somit auch die umgekehrte Folgerung, so dass die Äquivalenz von $C(F)$ und $C(F')$ hergestellt wird. Wir definieren die Abkürzungen

$$A := C(F), \quad A' := C(F'), \quad B := D(F), \quad B' := D(F').$$

Zunächst die Basisfälle. Die Formeln $C := \bot$, $C := \top$ und $C := v$ mit atomarer Variable $v \neq X$ bleiben von der Substitution unbetroffen und sind offenkundig zu sich selbst äquivalent. Für $C = X$ erhält man schlicht die Prämisse.

Zum Induktionsschritt. Man hat nun

$$(C \wedge D)[X{:=}F] \iff C[X{:=}F] \wedge D[X{:=}F] \iff A \wedge B$$

usw. Induktionsvoraussetzung sei also $\Gamma \vdash A \Leftrightarrow A'$ und $\Gamma \vdash B \Leftrightarrow B'$. Zu zeigen ist

$$\Gamma, A \wedge B \vdash A' \wedge B', \qquad \Gamma, A \Rightarrow B \vdash A' \Rightarrow B', \qquad \Gamma, \forall x\colon A \vdash \forall x\colon A',$$
$$\Gamma, A \vee B \vdash A' \vee B', \qquad \Gamma, A \Leftrightarrow B \vdash A' \Leftrightarrow B', \qquad \Gamma, \exists x\colon A \vdash \exists x\colon A'$$

und $\Gamma, \neg A \vdash \neg A'$. Es findet sich:

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash A \Leftrightarrow A'}{\Gamma, A' \vdash A} \quad \dfrac{}{\neg A \vdash \neg A}}{\Gamma, \neg A, A' \vdash \bot}}{\Gamma, \neg A \vdash \neg A'} \qquad \dfrac{\dfrac{\dfrac{\Gamma \vdash A \Leftrightarrow A'}{\Gamma \vdash A \Rightarrow A'} \quad \dfrac{}{A \wedge B \vdash A \wedge B}}{A \wedge B \vdash A} \quad \dfrac{\dfrac{\Gamma \vdash B \Leftrightarrow B'}{\Gamma \vdash B \Rightarrow B'} \quad \dfrac{}{A \wedge B \vdash A \wedge B}}{A \wedge B \vdash B}}{\Gamma, A \wedge B \vdash A' \qquad \Gamma, A \wedge B \vdash B'}}{\Gamma, A \wedge B \vdash A' \wedge B'}$$

Die Erstellung der restlichen Bäume sei dem Leser überlassen.

Für die Quantoren findet sich:

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash A \Leftrightarrow A'}{\Gamma \vdash A \Rightarrow A'} \quad \dfrac{}{\forall x\colon A \vdash \forall x\colon A}}{\forall x\colon A \vdash A}}{\Gamma, \forall x\colon A \vdash A'}}{\Gamma, \forall x\colon A \vdash \forall x\colon A'}\ x \notin \mathrm{FV}(\Gamma) \qquad \dfrac{\dfrac{\dfrac{\Gamma \vdash A \Leftrightarrow A'}{\Gamma \vdash A \Rightarrow A'} \quad \dfrac{}{A \vdash A}}{\Gamma, A \vdash A'}}{\exists x\colon A \vdash \exists x\colon A} \quad \dfrac{}{\Gamma, A \vdash \exists x\colon A'}}{\Gamma, \exists x\colon A \vdash \exists x\colon A'}\ x \notin \mathrm{FV}(\Gamma)$$

Es darf hierbei $x \notin \mathrm{FV}(\Gamma)$ vorausgesetzt werden, weil die gebundene Variable andernfalls ja vor der Betrachtung in eine frische umbenannt werden kann. □

Es wäre noch zu erwähnen, dass die Regel bei den modalisierenden Operatoren für gewöhnlich unzulässig ist. So ist in den modallogischen Systemen K, B, D, S4, S5 keine der Formeln

$$(a \Leftrightarrow b) \Rightarrow (\Box a \Leftrightarrow \Box b),$$
$$(a \Leftrightarrow b) \Rightarrow (\Diamond a \Leftrightarrow \Diamond b)$$

ein Theorem. Ein Gegenmodell ist jeweils schnell gefunden, dafür bedarf es nicht mehr als zwei Welten.

1.4 Logik mit Gleichheit

1.4.1 Axiome der Gleichheit

Im Folgenden Abschnitt geht es um allgemeingültige Erwägungen zur Gleichheit. Das wären Gesetzmäßigkeiten, die die Gleichheit immer erfüllen soll, ungeachtet, ob sie zwischen zwei Zahlen, zwei Mengen, oder zwei wie auch immer gearteten Objekten besteht.

Moderne Formulierungen charakterisieren die Gleichheit durch die Axiome

$$\vdash \forall x\colon x = x, \qquad \text{(Reflexivität)}$$
$$\vdash \forall x\colon \forall y\colon x = y \Rightarrow A(x) \Rightarrow A(y). \qquad \text{(Ersetzung)}$$

Das zweite Axiom ist eigentlich ein Schema, weil dieses für jede Formel A gilt. Es meint $A(u)$ eine Aussageform, wobei $A(t)$ als $A(u)[u := t]$ zu verstehen sein soll. Man gewinnt aus dem Schema kurzerhand die Regel

$$\frac{\Gamma \vdash t = t' \qquad \Gamma' \vdash A(t)}{\Gamma, \Gamma' \vdash A(t')}. \qquad (t, t' \text{ sind beliebige Terme})$$

Das erste Axiom charakterisiert insofern die Regel zur Einführung der Gleichheit, das zweite die Regel zur Beseitigung. Die Symmetrie der Gleichheit lässt sich aus den beiden Regeln ableiten. Sei hierzu $A(u) :\Leftrightarrow (u = x)$. Nun ist $A(x) \Leftrightarrow (x = x)$ und $A(y) \Leftrightarrow (y = x)$. Man setze $t := x$ und $t' := y$. Es findet sich:

$$\frac{\overline{x = y \vdash x = y} \quad \overline{\vdash x = x}}{x = y \vdash y = x}$$

Aus dieser Sequenz erhält man anschließend

$$\vdash \forall x\colon \forall y\colon x = y \Rightarrow y = x.$$

Bezüglich $A(u) :\Leftrightarrow (f(x) = f(u))$ führt die Ausübung der soeben gemachten Vorgehensweise auf

$$\vdash \forall x\colon \forall y\colon x = y \Rightarrow f(x) = f(y).$$

Es induziert die Ersetzungsregel für Funktionen,

$$\frac{\Gamma \vdash t = t'}{\Gamma \vdash f(t) = f(t')}.$$

Zu beachten wäre allerdings, dass f hierfür auf dem gesamten Diskursuniversum definiert sein muss. Würde das Symbol f mit einer Funktion belegt, die für eine bestimmte Belegung von x nicht definiert ist, was soll $f(x)$ dann sein?

Mehrmalige Anwendung des Ersetzungsaxioms ermöglicht darüber hinaus mehrstellige Ersetzungen wie

$$\vdash \forall x, x', y, y' \colon x = x' \wedge y = y' \Rightarrow A(x, y) \Rightarrow A(x', y'),$$
$$\vdash \forall x, x', y, y' \colon x = x' \wedge y = y' \Rightarrow f(x, y) = f(x', y').$$

Ferner implizieren die Axiome das Transitivgesetz

$$\vdash \forall x, y, z \colon x = y \wedge y = z \Rightarrow x = z.$$

Es steht $\forall x, y, z \colon A$ als Abkürzung für $\forall x \colon \forall y \colon \forall z \colon A$.

Ganz allgemein gilt

$$\vdash \forall x \colon \forall y \colon x = y \Rightarrow s(x) = s(y)$$

für jeden Term s. Dies bestätigt sich unschwer folgendermaßen. Sei h eine frische Hilfsvariable, die nicht frei in s vorkommt und

$$A :\Leftrightarrow (s[u := x] = s[u := h]),$$

wobei $s(x) = s[u := x]$ und $s(y) = s[u := y]$ ist. Der Schluss

$$\frac{\Gamma \vdash x = y \quad \vdash A[h := x]}{\Gamma \vdash A[h := y]}$$

vereinfacht sich nun zu

$$\frac{\Gamma \vdash x = y \quad \overline{\vdash s[u := x] = s[u := x]}}{\Gamma \vdash s[u := x] = s[u := y]}, \quad \text{kurz} \quad \frac{\Gamma \vdash x = y \quad \overline{\vdash s(x) = s(x)}}{\Gamma \vdash s(x) = s(y)}.$$

Es genügt übrigens, das Ersetzungsaxiom für atomare Aussageformen zu fordern. Seien hierzu P, Q Prädikate. Sei $A(x)$ zum Beispiel die Formel $P(x) \wedge Q(x)$. Dann ist die Regel

$$\frac{\Gamma \vdash x = y \qquad \Gamma' \vdash A(x)}{\Gamma, \Gamma' \vdash A(y)}$$

zulässig, denn:

$$\dfrac{\dfrac{\Gamma \vdash x = y \qquad \dfrac{\Gamma' \vdash P(x) \wedge Q(x)}{\Gamma' \vdash P(x)}}{\Gamma, \Gamma' \vdash P(y)} \qquad \dfrac{\Gamma \vdash x = y \qquad \dfrac{\Gamma' \vdash P(x) \wedge Q(x)}{\Gamma' \vdash Q(x)}}{\Gamma, \Gamma' \vdash Q(y)}}{\Gamma, \Gamma' \vdash P(y) \wedge Q(y)}$$

Für die anderen Junktoren klappt es analog. Per struktureller Induktion über den Formelaufbau bestätigt sich die Regel daraufhin in allgemeiner Weise als zulässig.

1.4.2 Von der Identität des Ununterscheidbaren

Dem Gleichheitsbegriff wohnt das *Principium identitatis indiscernibilium* inne, das *Prinzip der Identität des Ununterscheidbaren*, englisch *Identity of indiscernibles*. Es besagt, dass man keine zwei ungleichen Objekte finden kann, die in allen ihren Eigenschaften übereinstimmen. Man nennt es auch *Gleichheit nach Leibniz*, weil Wilhelm Gottfried Leibniz dieses im 27. Kaptiel von *Nouveaux Essais sur L'entendement humain II* im Bezug zum Kosmos beschrieb. Am Ende findet man das Wesentliche nochmals in fasslicher, bildhafter Form,

> »Ich erinnere mich, dass eine große Prinzessin, die von erhabenem Geist ist, einmal sagte, als sie in ihrem Garten spazieren ging, dass sie nicht glaube, dass es zwei vollkommen ähnliche Blätter gebe. Ein geistreicher Herr, der mit auf dem Spaziergang war, glaubte, dass es leicht sein würde, solche zu finden; aber obwohl er viel suchte, wurde er durch seine Augen davon überzeugt, dass man immer einen Unterschied bemerken könne. Aus diesen bisher vernachlässigten Erwägungen wird ersichtlich, wie weit man sich in der Philosophie von den natürlichsten Begriffen entfernt hat und wie weit man von den großen Prinzipien der wahren Metaphysik entfernt war.«

Formalisierung erfährt das Prinzip durch die Aussage

$$(\forall P\colon P(x) \Leftrightarrow P(y)) \implies x = y.$$

Man sollte bedenken, dass diese Formulierung die Prädikatenlogik zweiter Stufe erfordert, da hier über Prädikate quantifiziert wird. Die Umkehrung

$$x = y \implies (\forall P\colon P(x) \Leftrightarrow P(y)).$$

wird als unbedenklich angesehen, so dass man das Prinzip auch als Äquivalenz formuliert. Die Umkehrung ist fast trivial aus den Axiomen ableitbar, weil es sich bereits um eine gewisse Form des Ersetzungsaxioms handelt. Umgekehrt können wir aus der Äquivalenz die beiden Axiome zurückgewinnen. Reflexivität besteht offenkundig, weil $P(x)$ immer äquivalent zu $P(x)$ ist. Und zum Ersetzungsaxiom wurde bereits ausgeführt, dass es genügt, dieses für Prädikate zu fordern.

Es verbleibt zu untersuchen, ob das Prinzip aus den Axiomen herleitbar ist. Hierzu wird $P(u) := (x = u)$ als Prädikat gewählt, womit $x = x$ als äquivalent zu $x = y$ vorausgesetzt wird. Weil $x = x$ gemäß Reflexivität vorliegt, erhält man wie gewünscht $x = y$.

1.5 Induktion

1.5.1 Einfache Induktion

In der Philosophie bezeichnet man als *Induktion* eine Art von Schlussfolgerung, die da ist der Schluss vom Speziellen auf das Allgemeine. Folgendes Beispiel verdeutlicht die Idee der Überlegung. Ein Gegenstand wird einmal fallen gelassen, man beobachtet wie dieser zu Boden fällt. Wiederholung des Experiments führt abermals zum selben Resultat. Induktiv schließt man daraus, dass dieses Resultat *immer* eintreten wird. Jedoch kann Induktion zu Fehlschlüssen führen, weshalb es nicht als mathematisches Beweisverfahren brauchbar ist. Nur weil bereits dreimal eine Toastbrotscheibe auf die Marmeladenseite gefallen ist, heißt das nicht, dass dieses Resultat immer eintreten müsse. In der Mathematik bieten die Borwein-Integrale ein prägnantes Beispiel, wo leichtfertige Argumentation verfänglich wäre.

Mit der bedenklichen Induktion in der Philosophie teilt sich die *vollständige Induktion* den Namen. Sie ist allerdings unfehlbar. Das Verfahren ist für die moderne Mathematik und Informatik von wesentlicher Bedeutung.

Die vollständige Induktion wird vermittelt durch das Axiomenschema

$$\vdash A(0) \land (\forall n \in \mathbb{N}\colon A(n) \Rightarrow A(n+1)) \Rightarrow (\forall n \in \mathbb{N}\colon A(n)).$$

Es induziert die Regel

$$\frac{\Gamma \vdash A(0) \qquad \Gamma', n \in \mathbb{N}, A(n) \vdash A(n+1)}{\Gamma, \Gamma' \vdash \forall n \in \mathbb{N}\colon A(n)}.$$

Zur Veranschaulichung wird gerne eine endlose Dominoreihe herangezogen. Fällt der erste Dominostein um, und ist sicher, dass mit einem Dominostein ebenso dessen Nachfolger umfällt, muss *jeder* Dominostein irgendwann umfallen.

Man bezeichnet $A(0)$ als den *Induktionsanfang*. Die Ableitung von $A(n+1)$ aus $A(n)$ heißt *Induktionsschritt*, wobei $A(n)$ darin die Bezeichnung *Induktionsvoraussetzung* trägt.

Ein erstes Beispiel. Man definiert die Potenz einer Zahl a rekursiv als

$$a^0 := 1, \qquad a^{n+1} := aa^n.$$

Zu beweisen sei das Potenzgesetz

$$A(n) \ :\Longleftrightarrow \ (ab)^n = a^n b^n.$$

Der Anfang $A(0)$ bestätigt sich via

$$(ab)^0 = 1 = 1 \cdot 1 = a^0 b^0.$$

Den Induktionsschritt $(A(n) \Rightarrow A(n+1))$ bestätigt die Rechnung

$$(ab)^{n+1} \overset{(1)}{=} (ab)(ab)^n \overset{\text{IV}}{=} aba^n b^n = aa^n bb^n \overset{(2)}{=} a^{n+1}b^{n+1}.$$

Die Stelle, wo $A(n)$ zur Anwendung kam, wurde mit IV annotiert, was für *Induktionsvoraussetzung* steht. Die Umformungen (1), (2) gelten laut Definition.

Bislang trat die Induktion so auf, dass der Anfang in der Zahl Null liegt. Aus der Regel folgt aber bereits, dass man den Anfang in jede beliebige natürliche Zahl legen kann.

Satz 1.4. Es gilt für $n, n_0 \in \mathbb{N}$ das allgemeine Schema

$$\vdash A(n_0) \wedge (\forall n \geq n_0 \colon A(n) \Rightarrow A(n+1)) \Rightarrow (\forall n \geq n_0 \colon A(n)).$$

Beweis. Die Prämisse wird spezialisiert mit $n := u + n_0$, wobei u beliebig sein darf, da $u + n_0 \geq n_0$ für jedes $u \in \mathbb{N}$ erfüllt ist. Es sei nun $B(u) :\Leftrightarrow A(u+n_0)$. Demnach ist $A(n_0)$ äquivalent zu $B(0)$. Und es ist $A(u+n_0+1)$ äquivalent zu $B(u+1)$. Insgesamt erhält man aus der Prämisse also

$$B(0) \wedge (\forall u \colon B(u) \Rightarrow B(u+1)).$$

Per herkömmlicher Induktion gilt also $B(u)$ bzw. $A(u+n_0)$ für jedes natürliche u. Wird dies nun mit der Resubstitution $u := n - n_0$ mit $n \geq n_0$ spezialisiert, erhält man $A(n)$, und somit schließlich die gesuchte Konklusion $(\forall n \geq n_0 \colon A(n))$. □

Spezialisieren ist hier formal zu verstehen. Das Resultat der Substitution ist eigentlich nicht weniger allgemein als die ursprüngliche Aussage.

Befasst man sich im Weiteren mit der Mengenlehre, wo gemeinhin mit Mengen argumentiert wird, bietet sich an, auch die Induktion bezüglich einer Menge zu formulieren. Sei hierzu $M \subseteq \mathbb{N}$ definiert als die Aussonderung

$$M := \{n \in \mathbb{N} \mid A(n)\}.$$

Mit $A(n) \Leftrightarrow n \in M$ nimmt das Schema der Induktion daraufhin die Form

$$\vdash 0 \in M \wedge (\forall n \in \mathbb{N} \colon n \in M \Rightarrow n+1 \in M) \Rightarrow M = \mathbb{N}$$

an. Man verwendet diese Variante vorwiegend, um die axiomatische Charakterisierung der natürlichen Zahlen in Bezug zur Mengenlehre zu bringen. Sie wurde Ende des 19. Jahrhunderts von Richard Dedekind und Giuseppe Peano erdacht. Das Axiom der Induktion ist darin als letzte und komplizierteste. Es lautet

$$\vdash (\forall P \colon P(0) \wedge \forall n \colon P(n) \Rightarrow P(S(n))) \Rightarrow (\forall n \colon P(n)).$$

Hiermit wird allerdings die Prädikatenlogik zweiter Stufe vorausgesetzt, weil über alle Prädikate P quantifiziert wird. Ein Verzicht auf die Logik zweiter Stufe ist aber möglich, indem das Axiom wie bisher als Schema formuliert wird. Das so in die Prädikatenlogik erster Stufe gebrachte System nennt man die *Peano-Arithmetik*.

1.5.2 Starke Induktion

Die starke Induktion verstärkt die Induktionsvoraussetzung dahingehend, dass sie nicht nur für den unmittelbaren Vorgänger, sondern für sämtliche Vorgänger vorausgesetzt werden darf. Damit wird der Induktionsbeweis unter Umständen erleichtert. Die starke muss nicht extra axiomatisch gefordert werden, sie ist aus der herkömmlichen ableitbar.

Satz 1.5 (Starke Induktion). Es gilt das Schema

$$\vdash A(0) \land (\forall n \in \mathbb{N}\colon (\forall k \leq n\colon A(k)) \Rightarrow A(n+1)) \Rightarrow (\forall n \in \mathbb{N}\colon A(n))$$

Beweis. Sei hierzu

$$C(n) :\Leftrightarrow (\forall k \leq n\colon A(k)).$$

Die Prämissen seien angenommen. Es ist $A(0)$ gleichbedeutend mit $C(0)$. Wir überzeugen uns nun von der Folgerung

$$(\forall n \in \mathbb{N}\colon C(n) \Rightarrow A(n+1)) \Rightarrow (\forall n \in \mathbb{N}\colon C(n) \Rightarrow C(n+1)).$$

Sei also $n \in \mathbb{N}$ und $C(n)$ angenommen, dann haben wir auch $A(n+1)$ und somit $C(n) \land A(n+1)$, was äquivalent zu $C(n+1)$ ist. Per herkömmlicher Induktion gilt also $C(n)$ für jedes natürliche n. Aus $C(n)$ folgt aber $A(n)$, womit erst recht $A(n)$ für jedes natürliche n gilt. □

Ein wenig eleganter formuliert sich das Schema auch in der Form

$$\vdash (\forall n \in \mathbb{N}\colon (\forall k < n\colon A(k)) \Rightarrow A(n)) \Rightarrow (\forall n \in \mathbb{N}\colon A(n)).$$

Weil keine natürliche Zahl kleiner als null existiert, greift hier das Prinzip der leeren Wahrheit, womit $A(0)$ trotzdem zu bestätigen ist.

1.5.3 Strukturelle Induktion

Die herkömmliche Induktion verläuft über die natürlichen Zahlen. Sie beginnt ohne Beschränkung der Allgemeinheit in der Null, und setzt sich dann schrittweise

auf den Nachfolger fort. Es wird also $A(0)$ bestätigt, und $A(n+1)$ unter Annahme von $A(n)$.

Strukturelle Induktion verläuft allgemeiner über Knoten. Es gibt ein oder mehrere Anfangsknoten v_0, für die jeweils der Induktionsanfang $A(v_0)$ zu bestätigen ist. Außerdem liegen Regeln vor, wie aus bereits vorhandenen Knoten neue Knoten abzuleiten sind. Die neuen Knoten nehmen die Rolle der Nachfolger ein. So entsteht ein Baum oder ein gerichteter Graph. Leitet sich v aus v_1 bis v_n ab, so besteht der zugehörige Induktionsschritt darin, dass $A(v)$ unter Annahme von $A(v_1)$ bis $A(v_n)$ gezeigt wird. Bei einem Baum verläuft die Induktion von den Blättern aus zu einer Wurzel hin. Die gewöhnliche Induktion verlief von der Null zu einer Zahl hin. Wurde alles gezeigt, ist die Induktion also *vollständig*, darf die Wurzel wie die Zahl beliebig sein.

Ich will versuchen, das Prinzip so mit Dominosteinen zu veranschaulichen, wie die herkömmliche Induktion als Fallen einer Dominoreihe verständlich wird. Man kann sich eine Regel als ein Plättchen bestimmter Art vorstellen. Sofern alle notwendigen Dominosteine das Plättchen erreichen, fällt es um, womit auch der auf das Plättchen folgende Dominostein umfällt. Abermals erreichen notwendige Steine, worunter auch oder nur Nachfolger zu finden sind, ein weiteres Plättchen, worauf auch dieses fällt. Das läuft zumindest solange, bis man das gewünschte Fallen des begehrten Wurzelsteins beobachtet. Als dynamischer Prozess gesehen, hat man hier eine kausale Struktur, bei der Wirkungen nur unter einer oder mehreren passenden Ursachen auftreten.

Die herkömmliche Induktion stellt einen Spezialfall der strukturellen Induktion dar, bei der die Bäume endliche Listen sind. Bei der strukturellen Induktion über den Formelaufbau verläuft die Induktion über Formeln. Sie beginnt in den atomaren Formeln. Die Regeln zur Ableitung sind die Produktionsregeln. Bei der strukturellen Induktion über die Konstruktion eines Beweises verläuft die Induktion über Sequenzen. Sie beginnt in den Grundsequenzen. Die Regeln zur Ableitung sind die Schlussregeln.

Ein weiteres Beispiel bietet die Induktion über die Punkte des Gitters $\mathbb{Z}_{\geq 0} \times Z_{\geq 0}$. Sagen wir, der einzige Anfang ist $A(0,0)$. Die erste Schrittweise bestehe in $A(m+1,n)$ unter Annahme $A(m,n)$. Die zweite Schrittweise bestehe in $A(m,n+1)$ unter Annahme $A(m,n)$. Diese Art von struktureller Induktion ist gleichwohl gegen die herkömmliche ersetzbar. Der Beweis untergliedert sich dabei in zwei Induktionsbeweise. Es wird zunächst $A(m,0)$ für jedes m bestätigt und $A(m,0)$ anschließend als Anfang für $A(m,n)$ benutzt. Der zweite Induktionsbeweis ist so gesehen durch m parametrisiert, was nichts Schlimmes ist, denn parametrisierte Argumentation kennzeichnet ja das übliche Vorgehen zur Bestätigung allquantifizierter Aussagen.

1.6 Modallogik

1.6.1 Das System K

Die Modallogik handelt von den Weisen, wie eine Aussage ausgeprägt sein kann, was durch modalisierende Operatoren ausgedrückt wird. Es gibt unterschiedliche Systeme der Modallogik. In vielen Systemen finden sich zwei Modalitäten, die *Notwendigkeit* der Aussage und die *Möglichkeit* der Aussage. Allerdings artikulieren diese Sprechweisen nur die *alethische* Deutung der Modalitäten. Je nach System und Anwendung sind unterschiedliche Deutungen der Modalitäten zuträglich.

Ist A die Aussage »Es regnet«, drückt $\Box A$ die Aussage »Es regnet notwendigerweise« und $\Diamond A$ die Aussage »Es regnet möglicherweise« aus.

Die Modallogik scheint wichtiger für Philosophen als für Mathematiker. Indessen kamen mit der Zeit Anwendungen in der Mathematik und der Informatik zum Vorschein. Dem Basiswissen besonders dienlich ist meines Erachtens die *dynamische Logik* mit ihrer engen Beziehung zum Hoare-Kalkül bzw. zum dijkstraschen wlp-Kalkül. Diese Kalküle geben uns die Mittel in die Hand, Algorithmen auf ihre Korrektheit hin zu untersuchen. Die Funktion, die der Algorithmus darstellt, bekommt hierzu eine *Spezifikation*, bestehend aus einer *Vorbedingung* und einer *Nachbedingung*. Man zeigt nun, dass der Algorithmus auch das tut, was er soll, dergestalt dass der Wert der Funktion immer die Nachbedingung erfüllt, sofern ihre Argumente die Vorbedingung erfüllen.

Der Modallogik kommt somit auch eine gewisse Bedeutung für die praktische Arbeit zu, nicht nur für höhere mathematische respektive philosophische Erwägungen und Betrachtungen.

Wir wollen uns zunächst mit dem *System K* beschäftigen, dem Grundsystem der *normalen Modallogiken*. Spezifischere Systeme entstehen durch Hinzunahme weiterer Axiome. Das System K enthält sämtliche Regeln und Axiome der klassischen Aussagenlogik. Hinzu kommt die Regel

$$\frac{\vdash A}{\vdash \Box A} \qquad \text{(Nezessisierungsregel)}$$

und das Schema

$$\vdash \Box(A \Rightarrow B) \Rightarrow (\Box A \Rightarrow \Box B). \qquad \text{(Axiomenschema K)}$$

Wie gehabt induziert das Schema sogleich eine zulässige Regel,

$$\frac{\Gamma \vdash \Box(A \Rightarrow B)}{\Gamma \vdash \Box A \Rightarrow \Box B}. \qquad \text{(Regel K)}$$

Wichtig ist, dass nur Theoreme Nezessisierung erfahren dürfen. Dagegen ist

$$\frac{a \vdash a}{a \vdash \Box a} \qquad \text{(verboten)}$$

ein unzulässiger Schluss. So ist $a \Rightarrow \Box a$ kein Theorem. Man wird mit der Semantik für das System K leicht ein Gegenmodell dieser Formel finden.

Man definiert $\Diamond A$ als äquivalent zu $\neg\Box\neg A$.

Statt der einfachen Nezessisierung und Schema K kann man auch eine einzige allgemeine Nezessisierungsregel voraussetzen. Mit $n \geq 0$ lautet sie

$$\frac{A_1, \ldots, A_n \vdash B}{\Box A_1, \ldots, \Box A_n \vdash \Box B}.$$

Man beweist die Regel per Induktion über n als zulässig. Im Anfang $n = 0$ nimmt sie schlicht die Form der Nezessisierungsregel an. Der Induktionsschritt wird durch den Beweisbaum

$$\dfrac{\dfrac{\dfrac{\dfrac{A_1, \ldots, A_n, A_{n+1} \vdash B}{A_1, \ldots, A_n \vdash A_{n+1} \Rightarrow B}}{\Box A_1, \ldots, \Box A_n \vdash \Box(A_{n+1} \Rightarrow B)}\,\text{IV}}{\Box A_1, \ldots, \Box A_n \vdash \Box A_{n+1} \Rightarrow \Box B}\,\text{K} \qquad \dfrac{}{\Box A_{n+1} \vdash \Box A_{n+1}}}{\Box A_1, \ldots, \Box A_n, \Box A_{n+1} \vdash \Box B}\,\text{Modus ponens}$$

bestätigt.

Auch dem Fitch-Style wurde eine Darstellung der Schlüsse der Modallogik hinzugefügt. Sie ist meines Erachtens etwas schwieriger zu durchschauen als das Schließen von Sequenzen. Ich will in diesem Buch nicht näher darauf eingehen.

1.6.2 Das System S4

Das System S4 formt sich aus den Schemata KT4, siehe Tabelle 1.4.

Die Übersetzung nach Gödel-McKinsey-Tarski ist

$$\begin{aligned} v' &= \Box v, & (A \wedge B)' &= A' \wedge B', & (A \Rightarrow B)' &= \Box(A' \Rightarrow B'), \\ \bot' &= \bot, & (A \vee B)' &= A' \vee B', & (\neg A)' &= \Box\neg A'. \end{aligned}$$

Man deutet $\Box A$ als »A ist beweisbar«. Es ist A genau dann ein Theorem der intuitionistischen Logik, wenn A' ein Theorem im System S4 ist.

Tabelle 1.4: Übersicht über zusätzliche Schemata

	Schema	**Relationen**	**Formel**
K	$\Box(A \Rightarrow B) \Rightarrow (\Box A \Rightarrow \Box B)$	sämtliche	keine Einschränkung
T	$\Box A \Rightarrow A$	reflexive	$\forall x\colon R_{xx}$
B	$A \Rightarrow \Box\Diamond A$	symmetrische	$\forall x, y\colon R_{xy} \Rightarrow R_{yx}$
D	$\Box A \Rightarrow \Diamond A$	serielle	$\forall x\colon \exists y\colon R_{xy}$
4	$\Box A \Rightarrow \Box\Box A$	transitive	$\forall x, y, z\colon R_{xy} \wedge R_{yz} \Rightarrow R_{xz}$
5	$\Diamond A \Rightarrow \Box\Diamond A$	euklidische	$\forall x, y, z\colon R_{xy} \wedge R_{xz} \Rightarrow R_{yz}$

2 Elemente der Modelltheorie

2.1 Die klassische Semantik der Aussagenlogik

2.1.1 Die Erfüllungsrelation

Bislang trat die Logik in der Form eines formalen Systems in Erscheinung. Gegenstand eines solchen Systems sind im Allgemeinen *Wörter* einer formalen Sprache; im natürlichen Schließen sind das die Sequenzen. Einige Wörter, die *Axiome*, werden als gegeben vorausgesetzt. Unter Anwendung von *Ableitungsregeln*, auch *Inferenzregeln* genannt, das sind die Schlussregeln, leitet man aus bereits abgeleiteten Wörtern weitere Wörter der Sprache ab. In diesem Sinne handelt es sich um ein rein syntaktisches System.

Zum tieferen Verständnis muss man sich im Fortgang damit beschäftigen, welche inhaltliche Bedeutung den logischen Aussagen beigemessen wird. Der hierfür wesentliche Schritt besteht in der Definition einer passenden *Semantik*.

Gegenstand der Semantik der Logik ist der Wahrheitsgehalt von Aussagen. Man hat gefunden, dass es sich mit der Frage nach dem Wesen der Wahrheit schwierig verhält. Wir wollen daher an dieser Stelle gar nicht erst versuchen, sie zu ergründen. Stattdessen tritt Wahrheit für uns zunächst lediglich im leicht fassbaren Rahmen der zweiwertigen booleschen Algebra auf.

In der klassischen Semantik der Aussagenlogik herrscht das *Bivalenzprinzip*, das besagt, dass jede Aussage entweder *wahr* oder *falsch* sein muss, also einen von zwei Wahrheitswerten haben muss. Eine Aussage kann nicht *ein wenig wahr* oder *halbwegs wahr* sein, noch kann sie eine von mehreren unterschiedlichen gleichwertigen Wahrheiten haben. Wir schreiben kurz 0 für falsch und 1 für wahr. Enthält eine Formel logische Variablen, kommt ihr ein Wahrheitswert zu, sobald alle Variablen durch eine Interpretation mit einem Wahrheitswert belegt wurden.

Die Art und Weise, wie einer Formel ein Wahrheitswert zukommt, präzisiert die Erfüllungsrelation. Sie wird als Rekursion über den Formelaufbau definiert. Der Wahrheitswert einer Formel ist hierbei einzig und allein durch die Wahrheitswerte ihrer Teilformeln bestimmt.

Tabelle 2.1: Wahrheitstafel der Junktoren

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	1	0	0	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
1	1	0	1	1	1	1

Definition 2.1 (Erfüllungsrelation).
Eine Interpretation I ist eine Funktion, die jede atomare logische Variable v mit einem Wahrheitswert $I(v) \in \{0, 1\}$ belegt. Man definiert $I \vDash A$, sprich »I erfüllt A«, rekursiv als

$$\begin{aligned}
(I \vDash \bot) &:\Leftrightarrow 0, & (I \vDash A \wedge B) &:\Leftrightarrow ((I \vDash A) \wedge (I \vDash B)),\\
(I \vDash \top) &:\Leftrightarrow 1, & (I \vDash A \vee B) &:\Leftrightarrow ((I \vDash A) \vee (I \vDash B)),\\
(I \vDash v) &:\Leftrightarrow I(v), & (I \vDash A \Rightarrow B) &:\Leftrightarrow ((I \vDash A) \Rightarrow (I \vDash B)),\\
(I \vDash \neg A) &:\Leftrightarrow \neg(I \vDash A), & (I \vDash A \Leftrightarrow B) &:\Leftrightarrow ((I \vDash A) \Leftrightarrow (I \vDash B)).
\end{aligned}$$

Die rechte Seite der jeweiligen Festsetzung ist metalogisch zu verstehen und per Wahrheitstafel definiert, siehe Tabelle 2.1. Die Schreibweise $I \nvDash A$ ist gleichbedeutend mit $\neg(I \vDash A)$. Eine Interpretation wird auch als *Modell* bezeichnet. Man nennt sie *Modell* einer Formel, falls sie die Formel erfüllt. Andernfalls spricht man von einem *Kontramodell* oder *Gegenmodell* der Formel.

Definition 2.2. Für einen Kontext $\Gamma = \{A_1, \ldots, A_n\}$ setzt man

$$(I \vDash \Gamma) \;:\Longleftrightarrow\; (I \vDash A_1) \wedge \ldots \wedge (I \vDash A_n).$$

2.1.2 Gültigkeit einer Formel

Eine wichtige Rolle spielen *allgemeingültige* Formeln, die man in der Aussagenlogik auch als *Tautologien* bezeichnet. Sie sind immer wahr, unabhängig davon, mit welchem Wahrheitswert ihre logischen Variablen belegt werden.

Als allgemeinere Begrifflichkeit wollen wir auf einen Kontext Γ bezogen gültige Formeln A betrachten. Die Idee hierbei ist, dass wenn die Formeln des Kontextes als wahr angenommen werden, die Formel A ebenfalls wahr sein muss. Trifft dies auf A zu, schreibt man $\Gamma \vDash A$, gelesen »im Kontext Γ ist A gültig«, oder auch »Γ zieht A nach sich«. Die Bezeichnung *logische Folgerung* oder *logische Konsequenz* ist ebenfalls verbreitet.

Tabelle 2.2: Wahrheitstafel der Tautologie zur Kontraposition

a	b	$\neg b$	$\neg a$	$a \Rightarrow b$	$\neg b \Rightarrow \neg a$	$(a \Rightarrow b) \Leftrightarrow (\neg b \Rightarrow \neg a)$
0	0	1	1	1	1	1
1	0	1	0	0	0	1
0	1	0	1	1	1	1
1	1	0	0	1	1	1

Definition 2.3 (Gültige Formel).
Eine Formel A heißt genau dann gültig im Kontext Γ, wenn jede Interpretation, die sämtliche Formeln von Γ erfüllt, auch A erfüllt. Metalogisch

$$(\Gamma \vDash A) \;:\Longleftrightarrow\; \forall I\colon (I \vDash \Gamma) \Rightarrow (I \vDash A).$$

Eine im leeren Kontext gültige aussagenlogische Formel A nennt man wie gesagt Tautologie. Statt $\emptyset \vDash A$ schreibt man auch kurz $\vDash A$. Wie bei Sequenzen schreibt man auch $\Gamma, A, B \vDash C$ anstelle von $\Gamma \cup \{A, B\} \vDash C$.

2.1.3 Wahrheitstafeln

Obgleich der Variablenvorrat unendlich groß sein darf, enthält eine Formel von den Variablen nur endlich viele. Insofern sind für eine Formel in einem Kontext auch nur endlich viele Interpretationen relevant. Sind insgesamt n Variablen vorhanden, sind es 2^n Interpretationen.

Eine Interpretation I mit der Auswertung $I \vDash A$ ist nichts anderes als eine Zeile der Wahrheitstafel der Formel A. Eine Formel ist genau dann tautologisch, wenn in der Ergebnisspalte in jeder Zeile eine 1 steht.

Ein Beispiel. Die Wahrheitstafel 2.2 bestätigt

$$\vDash (a \Rightarrow b) \Leftrightarrow (\neg b \Rightarrow \neg a).$$

Die Tafel führt zusätzlich die Teilformeln auf, was bei längeren Formeln recht mühselig erscheinen mag. Eine geschickte Methode zur Reduzierung des Schreibaufwands erspart die Teilformeln, und setzt ihre Wahrheitswerte dafür schlicht unter die Junktoren, denn Ziffern benötigen nicht viel Platz.

Die Prüfung einer logischen Folgerung per Wahrheitstafel ermöglicht die metalogische Beziehung

$$(A_1, \ldots, A_n \vDash A) \iff (\vDash A_1 \wedge \ldots \wedge A_n \Rightarrow A).$$

Nämlich findet sich die äquivalente Umformung

$$\begin{aligned}(A_1, \ldots, A_n \vDash A) &\iff_{(1)} (\forall I\colon (I \vDash A_1) \wedge \ldots \wedge (I \vDash A_n) \Rightarrow (I \vDash A))\\ &\iff_{(2)} (\forall I\colon (I \vDash A_1 \wedge \ldots \wedge A_n) \Rightarrow (I \vDash A))\\ &\iff_{(3)} (\forall I\colon I \vDash A_1 \wedge \ldots \wedge A_n \Rightarrow A)\\ &\iff_{(4)} (\vDash A_1 \wedge \ldots \wedge A_n \Rightarrow A).\end{aligned}$$

Hierbei gilt (1), (4) gemäß Def. 2.3, 2.2 und (2), (3) gemäß Def. 2.1.

2.1.4 Korrektheit des natürlichen Schließens

Jede Schlussregel und jedes Axiom besitzt eine semantische Entsprechung. Die Beweise dafür werden nun auf metalogischer Ebene mittels natürlichem Schließen selbst erbracht, was wie eine Art Zirkelschluss erscheinen mag.

Zu den Grundsequenzen und zur Abschwächungsregel findet sich:

$$\dfrac{\dfrac{\dfrac{\overline{I \vDash \Gamma \cup \{A\}}\,{}^{1}}{(I \vDash \Gamma) \wedge (I \vDash A)}\,\text{Def. 2.2}}{I \vDash A}}{\dfrac{(I \vDash \Gamma \cup \{A\}) \Rightarrow (I \vDash A)}{\Gamma \cup \{A\} \vDash A}\,{}^{\sim 1}\,\text{Def. 2.3}}\,\text{Def. 2.3}$$

$$\dfrac{\dfrac{\dfrac{\Gamma \vDash A}{(I \vDash \Gamma) \Rightarrow (I \vDash A)}\,\text{Def. 2.3}\quad \dfrac{\overline{I \vDash \Gamma \cup \Gamma'}\,{}^{1}}{I \vDash \Gamma}\,\text{Def. 2.2}}{I \vDash A}}{\dfrac{(I \vDash \Gamma \cup \Gamma') \Rightarrow (I \vDash A)}{\Gamma \cup \Gamma' \vDash A}\,{}^{\sim 1}\,\text{Def. 2.3}}\,\text{Def. 2.3}$$

Die Prüfung der restlichen Entsprechungen sei dem Leser überlassen.

Satz 2.1 (Korrektheit des natürlichen Schließens).
Ist die Sequenz $\Gamma \vdash A$ ableitbar, so muss auch $\Gamma \vDash A$ gelten.

Beweis. Strukturelle Induktion über die Konstruktion von Beweisbäumen. Induktionsanfänge sind die semantischen Entsprechungen der Grundsequenzen. Induktionsschritte sind die semantischen Entsprechungen der Schlussregeln. Die Beweise der Entsprechungen wurden bereits diskutiert. □

2.1.5 Logische Äquivalenz

Definition 2.4 (Äquivalente Formeln).
Die Äquivalenz zweier Formeln A, B ist definiert als

$$(A \equiv B) \;:\iff\; (\vDash A \Leftrightarrow B).$$

Eine Äquivalenz besteht genau dann, wenn jede der beiden Formeln eine logische Folgerung der anderen ist. Das heißt, es besteht die metalogische Beziehung

$$(\vDash A \Leftrightarrow B) \iff (A \vDash B) \wedge (B \vDash A).$$

Tabelle 2.3: Einbettung in die gewöhnliche Algebra

Modern	$\neg a$	$a \wedge b$	$a \vee b$	$a \Rightarrow b$
Boole	$1 - a$	ab	$a + b(1 - a)$	$1 - a + ab$

Mit den semantischen Entsprechungen der Schlussregeln findet sich nämlich:

$$\dfrac{\dfrac{\vDash A \Leftrightarrow B}{\vDash A \Rightarrow B} \quad \dfrac{}{A \vDash A}}{A \vDash B} \qquad \dfrac{\dfrac{A \vDash B}{\vDash A \Rightarrow B} \quad \dfrac{B \vDash A}{\vDash B \Rightarrow A}}{\vDash A \Leftrightarrow B}$$

Satz 2.2. Es ist $A \equiv B$ eine Äquivalenzrelation. Das heißt, es gilt

$$A \equiv A, \qquad \text{(Reflexivität)}$$
$$(A \equiv B) \Rightarrow (B \equiv A), \qquad \text{(Symmetrie)}$$
$$(A \equiv B) \wedge (B \equiv C) \Rightarrow (A \equiv C). \qquad \text{(Transitivität)}$$

Der Beweis sei dem Leser als kleine Übung überlassen.

Der Satz 2.2 vermittelt, dass Formeln mit Äquivalenzen so umgeformt werden dürfen, wie Terme mit Termumformungen. Es finden sich im Fortgang eine Reihe von grundlegenden Äquivalenzen, die Regeln der *booleschen Algebra*. Sie wurde erstmals in der Mitte des 19. Jahrhunders vom britischen Mathematiker George Boole in seiner Abfassung *The Mathematical Analysis of Logic* und seinem späteren Buch *An Investigation of The Laws of Thought* beschrieben. Boole beschreibt allerdings, anders als heute üblich, eine Einbettung der logischen Operationen in die gewöhnliche Algebra, siehe Tabelle 2.3.

Logische Äquivalenz im absoluten Sinne ist nicht unter allen Umständen der Weisheit letzter Schluss. In der Schaltalgebra tun sich Problemstellungen auf, wo der Wahrheitswert einer Formel A in einzelnen Zeilen der Wahrheitstafel keine Rolle spielt, man spricht von *Don't-Care-Zellen*. Es sei X eine Formel, die genau in diesen Zeilen wahr ist, in allen anderen falsch. Man möchte A nun beispielsweise zu B vereinfachen. Unter normalen Umständen sollte diese Vereinfachung die Äquivalenz $A \equiv B$ einhalten. Bei Vorhandensein der irrelevanten Zellen genügt jedoch die weniger strenge Forderung

$$\neg X \vDash A \Leftrightarrow B.$$

Wir haben es hier mit einer relativen Äquivalenz zu tun. Auch bei ihr handelt es sich um eine Äquivalenzrelation, wobei X beliebig ist, aber fest sein muss.

Tabelle 2.4: Die Regeln der booleschen Algebra.

Konjunktion	Disjunktion	Bezeichnung
$A \wedge 0 \equiv 0$	$A \vee 1 \equiv 1$	Extremalgesetze
$A \wedge \neg A \equiv 0$	$A \vee \neg A \equiv 1$	Komplementärgesetze
$A \wedge A \equiv A$	$A \vee A \equiv A$	Idempotenzgesetze
$A \wedge 1 \equiv A$	$A \vee 0 \equiv A$	Neutralitätsgesetze
$A \wedge B \equiv B \wedge A$	$A \vee B \equiv B \vee A$	Kommutativgesetze
$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$	$A \vee (B \vee C) \equiv (A \vee B) \vee C$	Assoziativgesetze
$\neg(A \wedge B) \equiv \neg A \vee \neg B$	$\neg(A \vee B) \equiv \neg A \wedge \neg B$	De morgansche Gesetze
$A \wedge (A \vee B) \equiv A$	$A \vee (A \wedge B) \equiv A$	Absorptionsgesetze

2.1.6 Die Einsetzungsregel

Satz 2.3 (Einsetzungsregel).
Ist die Formel A allgemeingültig, so führt die simultane Ersetzung einiger atomarer Variablen durch Formeln bei ihr zu einer weiteren allgemeingültigen Formel. Metalogisch

$$(\vDash A) \implies (\vDash A[v_1 := B_1, \ldots, v_n := B_n]).$$

Beweis. Die Bestimmung von $I \vDash A[\ldots]$ läuft in derselben Weise ab wie die von $I \vDash A$, außer dass $I(v_k)$ durch $I \vDash B_k$ zu ersetzen ist. Sofern A allgemeingültig ist, gilt $I \vDash A$ unabhängig davon, ob $I(v_k)$ wahr oder falsch ist. Ergo muss $I \vDash A[\ldots]$ unabhängig davon gelten, ob $I \vDash B_k$ wahr oder falsch ist. □

Ich mag daran erinnern, dass bei der Substitution *jedes* Vorkommen der Variable durch dieselbe Formel zu ersetzen ist.

Zum Beispiel erhält man zu der simultanen Ersetzung $a := A$ und $b := B$ aus

$$\vDash (a \Rightarrow b) \Leftrightarrow (\neg b \Rightarrow \neg a) \quad \text{das Schema} \quad \vDash (A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A).$$

Mit dem Vollständigkeitssatz infolge das Theoremschema

$$\vdash (A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A).$$

Hiermit gewinnt man kurzum die Regeln

$$\frac{\Gamma \vdash A \Rightarrow B}{\Gamma \vdash \neg B \Rightarrow \neg A}, \qquad \frac{\Gamma \vdash \neg B \Rightarrow \neg A}{\Gamma \vdash A \Rightarrow B}.$$

Die Vorgehensweise ermöglicht summa summarum die Auffindung von zulässigen Schlussregeln durch geistloses Ausfüllen von Wahrheitstafeln, was allerdings auf die klassische Aussagenlogik beschränkt bleibt.

2.1.7 Wahrheitsfunktionen

Mit der Bindung ihrer atomaren Variablen gehen aus den Formeln der Aussagenlogik Wahrheitsfunktionen hervor. Die Disjunktion vermittelt zum Beispiel die Funktion

$$f\colon \{0,1\} \times \{0,1\} \to \{0,1\}, \quad f(a,b) := (a \vee b).$$

Jede Wahrheitsfunktion in n Variablen ist durch ihre Wahrheitstafel charakterisiert, die aus 2^n Zeilen besteht, da der Definitionsbereich so viele unterschiedliche Tupel enthält. Ein Tupel von Wahrheitswerten wird auch als Bitfolge betrachtet.

Zwei Formeln A, B sind genau dann äquivalent, wenn sie durch dieselben Interpretationen erfüllt werden, sich also in der Wahrheitstafel gleich verhalten. Man überzeugt sich davon unschwer mit der metalogischen Umformung

$$\begin{aligned}(A \equiv B) &\iff (\vDash A \Leftrightarrow B) \iff (\forall I\colon I \vDash A \Leftrightarrow B)\\ &\iff (\forall I\colon (I \vDash A) \Leftrightarrow (I \vDash B)).\end{aligned}$$

Demnach charakterisieren äquivalente Formeln dieselbe Wahrheitsfunktion. Man kann dies auch so betrachten, dass die Wahrheitsfunktion die Äquivalenzklasse all ihrer Formeln repräsentiert. Unter den Formeln gibt es nun einen besonderen Vertreter, die *disjunktive Normalform*, kurz DNF, die eigentlich nichts anderes als eine direkte Kodierung der Wahrheitstafel ist. Insofern ließt sich an der Wahrheitstafel unmittelbar die DNF der Formel ab.

Die Normalform einer Formel lässt sich unter Umständen vereinfachen. Bei der DNF der Disjunktion ist bereits klar, welche Formel Resultat der Vereinfachung sein müsste. Es findet sich

$$\begin{aligned}&(a \wedge \neg b) \vee (\neg a \wedge b) \vee (a \wedge b) \equiv (a \wedge \neg b) \vee ((\neg a \vee a) \wedge b)\\ &\equiv (a \wedge \neg b) \vee (1 \wedge b) \equiv (a \wedge \neg b) \vee b \equiv (a \vee b) \wedge (\neg b \vee b)\\ &\equiv (a \vee b) \wedge 1 \equiv a \vee b.\end{aligned}$$

In der Schaltalgebra ist die Vereinfachung der DNF von großer Wichtigkeit, da sie den maßgeblichen Schritt zur Ermittelung von Schaltungen mit einer minimalen Zahl von Gattern darstellt. Aus dieser Anforderung heraus wurden systematische

Verfahren zur Vereinfachung entwickelt. Für wenige Variablen stellt das sogenannte Karnaugh-Veitch-Diagramm ein geschicktes Hilfsmittel dar.

Mit dem Verfahren nach Quine und McCluskey lassen sich Formeln mit beliebig vielen Variablen mit einem Computer automatisch vereinfachen. Der Algorithmus ist allerdings von exponentieller Laufzeit, dessen Ausführung also von einer kombinatorischen Explosion überschattet. Eine wesentliche Verbesserung darf man auch nicht erwarten, da die Problemstellung der Vereinfachung als NP-vollständig befunden wurde. Für die Formeln mit sehr vielen Variablen liegt das Wissen über die beste Vereinfachung somit im Schleier der Dunkelheit.

3 Mengenlehre

3.1 Grundbegriffe

3.1.1 Der Mengenbegriff

Eine *Menge* darf man sich wie einen Beutel vorstellen, der einzelne Objekte enthält. Die Objekte heißen *Elemente* der Menge. Jedoch gilt es hierbei zu beachten, dass es sich mit einer Menge nicht gänzlich wie mit einem Beutel verhält, in dem dasselbe Objekt mehrmals zu finden sein kann.

> »*Unter einer Menge verstehen wir jede Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.*«
> — Georg Cantor, 1895 (redigiert aus [15])

Obwohl blumig anmutend, fassen diese Worte das Konzept recht gut auf den Punkt. Wichtig ist hier das Wort *wohlunterschieden*, das uns zu verstehen gibt, dass ein Element nicht mehrmals in einer Menge enthalten sein kann. *Eine Menge ist genau dadurch festgelegt, welche Elemente sie enthält. Sie enthält Elemente weder mehrmals, noch in einer bestimmten Reihenfolge.*

Es gibt die *leere Menge*, notiert als $\emptyset$ oder $\{\}$. Man darf sie sich wie einen leeren Beutel vorstellen. Dagegen enthält die Menge $\{\emptyset\}$ genau ein Element. Es ist ein Beutel, der den leeren Beutel enthält.

Wir schreiben kurz $x \in A$ für »x ist ein Element von A«, auch »x gehört zu A« oder »x liegt in A«. Es steht $x \notin A$ für $\neg x \in A$.

Für eine endliche Menge definiert man

$$x \in \{x_1, \ldots, x_n\} \;:\Longleftrightarrow\; x = x_1 \vee \ldots \vee x = x_n.$$

3.1.2 Gleichheit von Mengen

Es wurde gesagt, eine Menge ist dadurch charakterisiert, welche Elemente sie enthält. Um diesen Gedanke näher zu erfassen, sollten wir klären, wie es sich mit der Gleichheit von Mengen verhält. Insofern Mengen durch ihre Elemente bestimmt

sind, darf man doch sagen, zwei Mengen A, B sind genau dann gleich, falls A, B ein Objekt gemeinsam enthalten oder gemeinsam nicht enthalten. Das heißt, betrachtet man ein beliebiges Objekt x, so ist x genau dann in A enthalten, wenn x in B enthalten ist.

Definition 3.1 (Gleichheit von Mengen).
Für zwei Mengen A, B definiert man

$$A = B \;:\Longleftrightarrow\; (\forall x\colon x \in A \Leftrightarrow x \in B).$$

Der Leser wird mühelos bestätigen, dass die Gleichheit die Axiome einer Äquivalenzrelation erfüllt. Wobei der Begriff der Relation noch zu definieren wäre. Weil die Gesamtheit aller Mengen eine sogenannte echte Klasse ist, handelt es sich nicht um eine Äquivalenzrelation im engeren Sinne.

Es ist zulässig, ein Element bei der aufzählenden Angabe einer Menge mehrmals aufzuführen. Dies ändert allerdings nichts daran, dass ein Element stets nur einmal in einer Menge enthalten ist. Zum Beispiel gilt $\{\emptyset, \emptyset\} = \{\emptyset\}$. Mit der Definition der aufzählenden Angabe und dem Idempotenzgesetz der Aussagenlogik findet sich nämlich die äquivalente Umformung

$$x \in \{\emptyset, \emptyset\} \iff x = \emptyset \vee x = \emptyset \iff x = \emptyset \iff x \in \{\emptyset\}.$$

3.1.3 Beschränkte Quantifizierung

In der Mathematik erstreckt sich die Quantifizierung meist nicht über das gesamte Diskursuniversum, sondern bleibt auf eine bestimmte Menge beschränkt. Eine extra Notation macht dies ergonomisch, wobei eine Erweiterung der logischen Sprache hierfür nicht nötig ist. Die beschränkte Quantifizierung wird logisch auf eine unbeschränkte zurückgeführt.

Definition 3.2 (Beschränkte Quantifizierung).
Für jede Menge M und jede Aussageform $A(x)$ setzt man

$$(\forall x \in M\colon A(x)) \;:\Longleftrightarrow\; (\forall x\colon x \in M \Rightarrow A(x)),$$
$$(\exists x \in M\colon A(x)) \;:\Longleftrightarrow\; (\exists x\colon x \in M \wedge A(x)).$$

Die Aussage $\forall x \in \emptyset\colon A(x)$ ist allgemeingültig, man spricht von der *leeren Wahrheit*, engl. *vacuous truth*. Via ex falso quodlibet erhält man nämlich:

$$\dfrac{\dfrac{\dfrac{}{\vdash \neg x \in \emptyset} \quad \dfrac{}{x \in \emptyset \vdash x \in \emptyset}}{x \in \emptyset \vdash \bot}}{x \in \emptyset \vdash A(x)}\,\text{EFQ}$$
$$\vdash \forall x\colon x \in \emptyset \Rightarrow A(x)$$

Viele Regeln zur beschränkten Quantifizierung sind analog zu den Regeln der unbeschränkten. Beispielsweise gilt

$$(\forall x \in M\colon A(x) \land B(x)) \iff (\forall x \in M\colon A(x)) \land (\forall x \in M\colon B(x)).$$

Man muss allerdings Vorsicht walten lassen. Nicht bei jeder Äquivalenz liegt eine direkte Analogie vor. Zwar besteht für eine Formel A, in der x nicht frei vorkommt, die Äquivalenz

$$(\exists x\colon A) \iff A.$$

Die Analogie ist jedoch von der ein klein wenig intrikateren Form

$$(\exists x \in M\colon A) \iff M \neq \emptyset \land A.$$

Diese Beziehung erklärt sich durch die Umformung

$$(\exists x \in M\colon A) \Leftrightarrow (\exists x\colon x \in M \land A) \Leftrightarrow (\exists x\colon x \in M) \land A \Leftrightarrow M \neq \emptyset \land A.$$

Die letzte Umformung gilt, weil $M \neq \emptyset$ gleichbedeutend mit $\exists x\colon x \in M$ ist.

3.1.4 Komprehension

Es wird $\{x \mid A(x)\}$ gelesen als »die Klasse der x, für die $A(x)$ gilt« oder »die Menge der x, für die $A(x)$ gilt«.

Definition 3.3 (Komprehension).
Zu einer Aussageform $A(x)$ definiert man die Klasse $\{x \mid A(x)\}$ gemäß

$$a \in \{x \mid A(x)\} \ :\iff A(a).$$

Man muss mit der Komprehension ein wenig vorsichtig umgehen, denn nicht jede Klasse ist eine Menge. Die russellsche Klasse $R := \{x \mid x \notin x\}$ ist das klassische Beispiel. Angenommen, R wäre eine Menge. Dann dürfte man eine Aussage wie $R \in M$ bezüglich einer Menge M formulieren, also speziell $R \in R$. Gemäß Definition von R findet sich die folgende Ableitung:

$$\dfrac{\dfrac{\dfrac{}{R \in R \vdash R \in R}}{R \in R \vdash R \notin R}\ \text{laut Def.} \qquad \dfrac{\dfrac{}{R \notin R \vdash R \notin R}}{R \notin R \vdash R \in R}\ \text{laut Def.}}{\vdash R \in R \Leftrightarrow R \notin R}$$

Für jede Formel A gilt allerdings das Theorem

$$\vdash (A \Leftrightarrow \neg A) \Rightarrow \bot.$$

Insgesamt ergibt sich so ein Beweis der Kontradiktion. Irgendetwas kann also nicht gut sein. Diese von Bertrand Russell im Jahre 1901 entdeckte Verwicklung, die seit jeher den Namen *russellsche Antinomie* trägt, brachte Gottlob Freges logizistisches Programm in unangenehme Schwierigkeiten. Frege versuchte, eine Reduktion der Mathematik auf die Logik zu unternehmen, wurde daraufhin aber von Russell brieflich in Kenntnis gesetzt, dass sein Werk *Grundgesetze der Arithmetik* in wesentlicher Weise von der Antinomie unterhöhlt wird. Russell führte das Programm fort, und veröffentlichte schließlich die *Principia Mathematica*, die der Antinomie mithilfe einer Typentheorie aus dem Weg geht.

Man begegnet der Problematik, indem man R als eine echte Klasse ansieht. Für sie darf die Aussage $R \in M$ nicht formuliert werden. Man definiert weiterhin eine weniger allgemeine Form der Komprehension, die *Aussonderung*. Sie verhält sich gutartig, da sie nicht mehr ermöglicht, als das Ausfiltern von Elementen aus einer gegebenen Menge.

Definition 3.4 (Aussonderung).
Zu einer Menge M und einer Aussageform $A(x)$ definiert man

$$a \in \{x \in M \mid A(x)\} \ :\Longleftrightarrow\ a \in M \wedge A(a).$$

3.1.5 Teilmengen

Gehört jedes Element einer Menge A auch zu einer Menge B, nennt man A eine *Teilmenge* von B. Man sagt auch, B umfasse A, oder B sei eine Obermenge von A. Eine *echte Teilmenge* sei A dann, wenn zusätzlich $A \neq B$ gilt. Die Menge der geraden Zahlen ist eine echte Teilmenge der ganzen Zahlen. Jede Menge ist eine Teilmenge von sich selbst, jedoch keine echte.

Die Menge der Quadrate ist eine Teilmenge der Vierecke, genauer eine Teilmenge der Rechtecke und auch eine Teilmenge der Rhomben. Weder ist die Menge der Rechtecke eine Teilmenge der Rhomben, noch ist die Menge der Rhomben eine Teilmenge der Rechtecke. Allerdings ist sowohl die Menge der Rechtecke als auch die der Rhomben eine Teilmenge der Parallelogramme.

Definition 3.5 (Teilmengenbeziehung).
Man definiert $A \subseteq B$, gelesen »A ist eine Teilmenge von B«, als

$$A \subseteq B \ :\Longleftrightarrow\ (\forall x\colon x \in A \Rightarrow x \in B).$$

Unschwer bestätigt sich die Äquivalenz

$$A = B \iff A \subseteq B \wedge B \subseteq A.$$

Definition 3.6 (Potenzmenge).
Die Potenzmenge einer Menge M ist definiert als

$$\mathcal{P}(M) \coloneqq \{A \mid A \subseteq M\}.$$

Zum Beispiel ist $\mathcal{P}(\emptyset) = \{\emptyset\}$ und $\mathcal{P}(\{0\}) = \{\emptyset, \{0\}\}$. Des Weiteren

$$\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\},$$
$$\mathcal{P}(\{0,1,2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}.$$

Die Teilmengenbeziehung darf als eine Art Ordnung zwischen Mengen betrachtet werden, jedoch nicht als eine Totalordnung, das heißt, bei einigen Mengen A, B gilt weder $A \subseteq B$ noch $B \subseteq A$. So ist wie gesagt weder die Menge der Rechtecke eine Teilmenge der Rhomben, noch umgekehrt.

Die Potenzmenge einer Grundmenge G bildet mit der Teilmengenbeziehung eine halbgeordnete Menge, engl. *poset* für *partially ordered set*. Das heißt, alle Mengen $A, B, C \in \mathcal{P}(G)$ erfüllen die drei Axiome

$$A \subseteq A, \qquad \text{(Reflexivität)}$$
$$A \subseteq B \land B \subseteq A \Rightarrow A = B, \qquad \text{(Antisymmetrie)}$$
$$A \subseteq B \land B \subseteq C \Rightarrow A \subseteq C. \qquad \text{(Transitivität)}$$

3.1.6 Mengenoperationen

Definition 3.7 (Schnitt, Vereinigung, Differenz).
Zu zwei Mengen A, B definiert man

$$A \cap B \coloneqq \{x \mid x \in A \land x \in B\}, \qquad \text{(Schnittmenge)}$$
$$A \cup B \coloneqq \{x \mid x \in A \lor x \in B\}, \qquad \text{(Vereinigungsmenge)}$$
$$A \setminus B \coloneqq \{x \mid x \in A \land x \notin B\}. \qquad \text{(Differenzmenge)}$$

Sind A, B Teilmengen einer Grundmenge G, so sind auch $A \cap B$, $A \cup B$ und $A \setminus B$ Teilmengen der Grundmenge. Der Beweis zu $A \cap B \subseteq G$ ist:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{x \in A \cap B \vdash x \in A \cap B}}{x \in A \cap B \vdash x \in A \land x \in B}}{x \in A \cap B \vdash x \in A} \qquad \dfrac{\dfrac{\dfrac{}{A \subseteq G \vdash A \subseteq G}}{A \subseteq G \vdash \forall x \colon x \in A \Rightarrow x \in G}}{A \subseteq G \vdash x \in A \Rightarrow x \in G}}{\dfrac{A \subseteq G, x \in A \cap B \vdash x \in G}{\dfrac{A \subseteq G \vdash \forall x \colon x \in A \cap B \Rightarrow x \in G}{A \subseteq G \vdash A \cap B \subseteq G}}}$$

In so pedantischer Ausführlichkeit findet man Beweise in Büchern nicht vor. Erstens wird man stillschweigend zulässige Schlussregeln zur Verkürzung aufstellen. So nimmt der Baum die konzise Form

$$\dfrac{\dfrac{\dfrac{}{x \in A \cap B \vdash x \in A \cap B}}{x \in A \cap B \vdash x \in A} \qquad \dfrac{}{A \subseteq G \vdash A \subseteq G}}{\dfrac{A \subseteq G, x \in A \cap B \vdash x \in G}{A \subseteq G \vdash A \cap B \subseteq G}} \qquad \dfrac{\dfrac{\dfrac{}{x \in A \cap B}\,{}^{1}}{x \in A} \qquad A \subseteq G}{\dfrac{x \in G}{A \cap B \subseteq G}\,{}^{\sim 1}}$$

an. Zweitens formuliert der Mathematiker den Beweis meist in Worten: Um $A \cap B \subseteq G$ zu zeigen, muss $x \in G$ aus $x \in A \cap B$ abgeleitet werden. Mit $x \in A \cap B$ gilt erst recht $x \in A$. Wegen $A \subseteq G$ ist somit $x \in G$, was zu zeigen war. □

Definition 3.8 (Komplement).
Bezüglich einer Grundmenge G heißt $A^{\mathrm{c}} := G \setminus A$ Komplementärmenge.

Es zeigt sich elementar, dass die Potenzmenge einer Grundmenge G mit den Operationen $A \cap B$, $A \cup B$ die Axiome einer booleschen Algebra erfüllt, wobei $\emptyset$ das Nullelement und G selbst das Einselement ist. Es gelten somit analoge Regeln wie in der klassischen Aussagenlogik. Wie die Notation suggeriert, entspricht der Schnitt der Konjunktion, die Vereinigung der Disjunktion und das Komplement der Negation.

Wie in jedem Verband ist in einer booleschen Algebra $(M, \wedge, \vee)$ für $a, b \in M$ eine Halbordnung $a \leq b$ definiert, indem $a \leq b$ und $a \wedge b = a$ als äquivalent angesehen werden. Bei der Mengenalgebra entpuppt sie sich als die Teilmengenrelation. Das heißt, es gilt

$$A \subseteq B \iff A \cap B = A \iff A \cup B = B.$$

Die Beziehung $A \setminus B = A \cap B^{\mathrm{c}}$ ist eine recht dienliche. Vermöge ihr können die Operationen mit der Differenzmenge ebenfalls mit der booleschen Algebra diskutiert werden. So ermöglicht sie die Rechnung

$$\begin{aligned} A \setminus (B \cap C) &= A \cap (B \cap C)^{\mathrm{c}} = A \cap (B^{\mathrm{c}} \cup C^{\mathrm{c}}) \\ &= (A \cap B^{\mathrm{c}}) \cup (A \cap C^{\mathrm{c}}) = (A \setminus B) \cup (B \setminus C). \end{aligned}$$

Dieses flippende Distributivgesetz ist also dadurch zu erklären, dass das Distributivgesetz des Schnittes an das de morgansche Gesetz angefügt wird. Mit dem Idempotenzgesetz $A = A \cap A$, zuzüglich dem Kommutativ- und Assoziativgesetz des Schnittes findet sich weiterhin

$$\begin{aligned} A \setminus (B \cup C) &= A \cap (B \cup C)^{\mathrm{c}} = A \cap B^{\mathrm{c}} \cap C^{\mathrm{c}} = A \cap A \cap B^{\mathrm{c}} \cap C^{\mathrm{c}} \\ &= A \cap B^{\mathrm{c}} \cap A \cap C^{\mathrm{c}} = (A \setminus B) \cap (B \setminus C). \end{aligned}$$

Tabelle 3.1: Logische Entsprechungen der Mengenoperationen

0	1	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$	$A \oplus B$
$\emptyset$	G	A^c	$A \cap B$	$A \cup B$	$A^c \cup B$	$(A \triangle B)^c$	$A \triangle B$

Die alternative Bestätigung dieser Formeln mittels natürlichem Schließen oder logischer Äquivalenzumformung bietet eine leichte Übung. Die Bestätigung von

$$(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C),$$
$$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$$

verläuft analog.

In gewisser Hinsicht spiegeln Mengen logische Aussagen wider. Zu jeder logischen Verknüpfung gehört eine Mengenoperation, siehe Tabelle 3.1. Die Subjunktion $A \Rightarrow B$ wird dabei via $\neg A \vee B$ übersetzt, was die klassische Logik verlangt. Man kann nun darüber hinaus einen Zusammenhang zwischen der Teilmengenbeziehung und den Sequenzen herstellen. Und zwar verhält sich die Beziehung

$$A_1 \cap \ldots \cap A_m \subseteq B_1 \cup \ldots \cup B_n.$$

analog zur allgemeinen Sequenz

$$A_1, \ldots, A_m \vdash B_1, \ldots, B_n.$$

Mehr noch, jede Schlussregel des natürlichen Schließens besitzt eine direkte Entsprechung. So verhält sich die Regel

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \quad \text{analog zu} \quad \Gamma \subseteq A \cap B \Rightarrow \Gamma \subseteq A.$$

Aber Vorsicht, die Sequenz $\Gamma \cup \Gamma' \vdash A$ entspricht $\Gamma \cap \Gamma' \subseteq A$.

Diese Sichtweise ermöglicht es, das natürliche Schließen durch Eulerdiagramme zu veranschaulichen. Umgekehrt hilft die Betrachtung als Sequenz beim Urteilen, ob Mengen in Teilmengenbeziehung stehen.

Für mehrere Mengen definiert man

$$\bigcap_{i=1}^{n} A_i := A_1 \cap A_2 \cap \ldots \cap A_n, \qquad \bigcup_{i=1}^{n} A_i := A_1 \cup A_2 \cup \ldots \cup A_n.$$

Pedantiker mögen die Schreibweise mit den Auslassungspunkten als ungenau empfinden. Zufriedenstellend ist für sie die Erklärung, dass es sich um die rekursive Festlegung

$$\bigcap_{i=1}^{1} A_i := A_1, \qquad \bigcap_{i=1}^{n} A_i := A_n \cap \bigcap_{i=1}^{n-1} A_i$$

handelt. Regeln wie $B \cup \bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} (B \cup A_i)$ kann man nun per Induktion über n beweisen. Es geht fast trivial vonstatten, sobald man das Prinzip verstanden hat. Im Wesentlichen weiten sich hier die Regeln der booleschen Algebra von den zweistelligen auf die mehrstelligen Operationen aus.

Definition 3.9 (Allgemeine Vereinigung).
Sei M eine Menge von Mengen. Die Vereinigung der $A \in M$ ist

$$\bigcup M = \bigcup_{A \in M} A := \{x \mid \exists A \in M \colon x \in A\}.$$

Für $M = \emptyset$ ist $\bigcup M = \emptyset$. Die Disjunktion findet ihre Entsprechung genau in der Vereinigung von zwei Mengen. Dazu passend findet der Existenzquantor seine Entsprechung genau in der Vereinigung beliebig vieler Mengen. Aus diesem Grund weiten sich die Regeln der booleschen Algebra auf die allgemeine Vereinigung aus. Zum Beispiel lautet das Distributivgesetz für Mengen

$$B \cap \bigcup_{A \in M} A = \bigcup_{A \in M} (B \cap A).$$

Entfaltung der Definition führt nämlich zur logischen Äquivalenz

$$x \in B \wedge (\exists A \in M \colon x \in A) \iff (\exists A \in M \colon x \in B \wedge x \in A).$$

Ihr Beweis gelingt mühelos.

Definition 3.10 (Allgemeiner Schnitt).
Sei M eine nichtleere Menge von Mengen. Der Schnitt der $A \in M$ ist

$$\bigcap M = \bigcap_{A \in M} A := \{x \mid \forall A \in M \colon x \in A\}.$$

Im Gegensatz zur Vereinigung wurde der Schnitt $\bigcap M$ für $M = \emptyset$ undefiniert gelassen. Hier gibt es zwei Möglichkeiten. Zum einen könnte man die Bedingung $M \neq \emptyset$ einfach fallen lassen, dann ergibt im allgemeinen Mengenuniversum beim leeren Schnitt die Allklasse $\{x \mid \top\}$, die jedoch keine Menge ist.

Aus diesen Grund gibt es noch die alternative Definition

$$\bigcap M := \{x \in G \mid \forall A \in M\colon x \in A\}.$$

Hierzu ist eine Grundmenge G festzulegen, so dass $M \subseteq \mathcal{P}(G)$ gilt, oder man setzt $G := \bigcup M$, wobei sich da die Frage nach der Nützlichkeit stellt.

Eine Menge von Mengen nennt man ein *Mengensystem*, wobei aber einige Autoren diese Begrifflichkeit für eine Familie von Mengen benutzen, die von einer Menge von Mengen zu unterscheiden ist. Eine Familie stellt eine Verallgemeinerung einer Folge von Mengen dar. In ihr darf dieselbe Menge mehrmals vorkommen. Man kann Schnitt und Vereinigung auch für Familien definieren, was aber eigentlich keine wesentliche Verallgemeinerung zu den obigen Festlegungen darstellt, wie ich im Folgenden diskutieren möchte.

Eine *Familie* (A_i) von Mengen A_i mit $i \in I$ ist eine Abbildung $A\colon I \to Z$, wobei Z eine Zielmenge ist, welche die A_i als Elemente enthält. Die Menge I wird in diesem Zusammenhang auch *Indexmenge* genannt. Man definiert

$$\bigcup_{i\in I} A_i := \bigcup A(I) = \bigcup \{X \mid \exists i \in I\colon X = A_i\} = \{x \mid \exists i \in I\colon x \in A_i\},$$

wobei mit $A(I)$ das Bild von I unter A gemeint ist. Man bekommt

$$\begin{aligned}\bigcup_{i\in I} A_i &= \{x \mid \exists X\colon X \in \{X \mid \exists i \in I\colon X = A_i\} \wedge x \in X\}\\ &= \{x \mid \exists X\colon (\exists i \in I\colon X = A_i) \wedge x \in X\}\\ &= \{x \mid \exists X\colon \exists i \in I\colon X = A_i \wedge x \in X\} = \{x \mid \exists i \in I\colon x \in A_i\}.\end{aligned}$$

Für $I \neq \emptyset$ definiert man entsprechend

$$\bigcap_{i\in I} A_i := \bigcap A(I) = \{x \mid \forall i \in I\colon x \in A_i\}.$$

Die Operation über eine Familie $(A_i)_{i\in I}$ kann also auf die jeweilige Operation über das System $A(I)$ zurückgeführt werden.

Später nützlich ist der

Satz 3.1. Es gilt $\bigcup_{i\in I\cup J} A_i = (\bigcup_{i\in I} A_i) \cup (\bigcup_{i\in J} A_j)$.

Beweis. Es findet sich die äquivalente Umformung

$$\begin{aligned}x \in \textstyle\bigcup_{i\in I\cup J} A_i &\iff (\exists i\colon i \in I \cup J \wedge x \in A_i)\\ &\iff (\exists i\colon (i \in I \wedge x \in A_i) \vee (i \in J \wedge x \in A_i))\\ &\iff (\exists i\colon i \in I \wedge x \in A_i) \vee (\exists i\colon i \in J \wedge x \in A_i)\\ &\iff x \in \textstyle\bigcup_{i\in I} A_i \vee x \in \bigcup_{i\in J} A_i\\ &\iff x \in (\textstyle\bigcup_{i\in I} A_i) \cup (\bigcup_{i\in J} A_i).\ \square\end{aligned}$$

Gelegentlich hat man es mit einer *disjunkten Vereinigung* zu tun. Sie ist bedeutsam in der Theorie der Kardinalzahlen und in der Informatik bei algebraischen Datentypen sowie deren Bezug zur Beweistheorie. Genauer gesagt hantiert man in der Informatik nicht mit Mengen, sondern mit Typen, die sich in gewissen Zügen analog zu Mengen verhalten. Die disjunkte Vereinigung zweier Mengen kennzeichnet jedes Element vor der Vereinigung mit einem Tag, das die Information liefert, aus welcher der Mengen es entstammt. Man setzt

$$A \sqcup B := \{(0, a) \mid a \in A\} \cup \{(1, b) \mid b \in B\}.$$

Die Zahlen $0, 1$ sind hier die *Tags* oder *Diskriminatoren*. Anstelle der Zahlen könnten genauso gut zwei beliebige unterschiedliche Elemente als Tags verwendet werden. Beispielsweise ginge auch

$$A \sqcup B = \{(\text{Grün}, a) \mid a \in A\} \cup \{(\text{Blau}, b) \mid b \in B\}.$$

In der Informatik verwendet man gern left, right als Tags.

Mit jeder disjunkten Vereinigung ist eine Fallunterscheidung verbunden. Liegt ein $x \in A \sqcup B$ vor, so muss entweder $x = (0, a)$ für ein $a \in A$ oder $x = (1, b)$ für ein $b \in B$ sein. Bei einer gewöhnlichen Vereinigung besteht dagegen kein ausschließendes Oder.

Wir fassen zwei Objekte x, y zu einem *geordneten Paar* (x, y) zusammen. Die beiden Objekte müssen nicht unbedingt etwas miteinander zu tun haben, sie dürfen völlig verschiedener Art sein. Im Unterschied zu einer Menge spielt bei Paaren die Reihenfolge eine Rolle, auch darf dasselbe Objekt zweimal vorkommen. Im Paar $t = (x, y)$ ist genau die Information über x, y enthalten. Das heißt, es lassen sich x, y aus dem Paar extrahieren. Man schreibt dafür $t_1 = x$ und $t_2 = y$. Die Schreibweise t_i heißt *Indizierung*, es ist darin i der *Index*.

Zwei Paare seien definitionsgemäß genau dann gleich, wenn sie komponentenweise gleich sind,

$$(x, y) = (x', y') \iff x = x' \wedge y = y'.$$

Die genannten Eigenschaften charakterisieren den Begriff Paar im Wesentlichen, mehr müssen wir nicht wissen. Man hat sich trotzdem auch mal überlegt, wie Paare in der reinen Mengenlehre dargestellt werden können, wo alle Objekte Mengen sein sollen. Nach Kuratowski sind Paare kodierbar als

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

Unter dem allgemeineren Begriff *Tupel* fassen wir eine beliebige endliche Zahl von Objekten in einer bestimmten Reihenfolge zusammen. Tupel aus drei Objekten heißen *Tripel*, die aus vier heißen *Quadrupel*. Analog zu den Paaren ist ihre Gleichheit definiert als

$$(x_1, \ldots, x_n) = (x'_1, \ldots, x'_n) \;:\Longleftrightarrow\; x_1 = x'_1 \wedge \ldots \wedge x_n = x'_n.$$

Zu zwei Mengen X, Y kann man nun die Menge aller Paare betrachten, deren erste Komponente X entstammt, und deren zweite Komponente Y entstammt. Sie heißt *Produktmenge* oder *kartesisches Produkt* der Mengen X, Y.

Definition 3.11 (Produktmenge).
Das kartesische Produkt zweier Mengen X, Y ist die Menge

$$X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}.$$

Genau genommen handelt es sich hierbei um eine Bildmenge, was bedeutet, dass sich im rechten Term Existenzquantoren verstecken. Ausführlich ausgeschrieben lautet der Term

$$\begin{aligned} X \times Y &= \{t \mid \exists x \in X \colon \exists y \in Y \colon t = (x, y)\} \\ &= \{t \mid \exists x \colon \exists y \colon x \in X \wedge y \in Y \wedge t = (x, y)\}. \end{aligned}$$

Wie jede Bildmenge ist das Produkt als Vereinigung darstellbar. Es ist

$$X \times Y = \bigcup_{x \in X} \bigcup_{y \in Y} \{(x, y)\}.$$

Die beiden kurzen Identitäten $X \times \emptyset = \emptyset$ und $\emptyset \times Y = \emptyset$ gehen unmittelbar aus der Definition hervor. Es verhält sich analog wie mit der Multiplikation einer Zahl mit null. Eine sinnvolle Sichtweise, wie die Theorie der Kardinalzahlen lehrt.

Satz 3.2. Ist $A \subseteq X$ und $B \subseteq Y$, dann ist $A \times B \subseteq X \times Y$.

Beweis. Es liege t in $A \times B$. Laut Definition existieren mithin $a \in A$ und $b \in B$, so dass $t = (a, b)$. Wegen $A \subseteq X$ ist aber auch $a \in X$ und wegen $B \subseteq Y$ ist auch $b \in Y$. Daher existieren $a \in X$ und $b \in Y$, so dass $t = (a, b)$. Gemäß Definition heißt das, $t \in X \times Y$. Gemäß Definition ist $A \times B$ somit eine Teilmenge von $X \times Y$. □

Satz 3.3. Es gilt $X \times (A \cup B) = (X \times A) \cup (X \times B)$.

Beweis. Es ginge zu Fuß. Aber Satz 3.1 ermöglicht die kurze Termumformung

$$X \times (A \cup B) = \bigcup_{x \in X} \bigcup_{y \in A \cup B} \{(x,y)\} = \bigcup_{x \in X} \left(\left(\bigcup_{y \in A} \{(x,y)\} \right) \cup \left(\bigcup_{y \in B} \{(x,y)\} \right) \right)$$
$$= \left(\bigcup_{x \in X} \bigcup_{y \in A} \{(x,y)\} \right) \cup \left(\bigcup_{x \in X} \bigcup_{y \in B} \{(x,y)\} \right) = (X \times A) \cup (X \times B). \square$$

Da sich die Existenzquantifizierung nicht in allgemeiner Weise distributiv bezüglich der Konjuktion verhält, mag es intrikat erscheinen, dass der folgende Satz dennoch gilt.

Satz 3.4. Es gilt $X \times (A \cap B) = (X \times A) \cap (X \times B)$.

Beweis. Wir wollen sodann auch einmal den Beweis betrachten, um zu verstehen, was da vonstatten geht.

Es sei $t \in X \times (A \cap B)$. Dann existieren $x \in X$ und $y \in A \cap B$, so dass $t = (x,y)$. Ergo ist sowohl $y \in A$ als auch $y \in B$. Und somit sowohl $t \in X \times A$ als auch $t \in X \times B$. Ergo ist $t \in (X \times A) \cap (X \times B)$. Diese Implikation schafft der Existenzquantor auch in allgemeiner Weise. Betrachten wir nun die kritische umgekehrte Richtung.

Es sei $t \in (X \times A) \cap (X \times B)$. Dann ist sowohl $t \in X \times A$ als auch $t \in X \times B$. Ergo existiert ein $x \in X$ und $y \in A$ mit $t = (x,y)$. Weiterhin ein $x' \in X$ und $y' \in B$ mit $t = (x',y')$. Hier liegt der Hase im Pfeffer: Wegen $(x,y) = t = (x',y')$ muss $x = x'$ und $y = y'$ sein. Wir wissen nun, $y \in A \cap B$, ergo $t \in X \times (A \cap B)$. $\square$

Ob eine Aussageform in zwei Variablen über das Durchlaufen aller Paare Allquantifizierung erfährt, oder über das Durchlaufen der Variablen selbst, macht keinen Unterschied. Dieses Schönfinkeln der auf Produktmengen beschränkten Quantifizierung mag am Beispiel endlicher Mengen recht einsichtig sein. Die allgemeine Bestätigung vermittelt der

Satz 3.5. Es ist $\forall t \in X \times Y \colon A(t)$ äquivalent zu $\forall x \in X \colon \forall y \in X \colon A(x,y)$.

Beweis. Zur Implikation von links nach rechts. Aus festen, aber beliebigen $x \in X$ und $y \in Y$ muss $A(x,y)$ abgeleitet werden. Mit dem aus ihnen geformten Paar $t := (x,y)$ bezeugen sie $t \in X \times Y$. Hiermit erhält man $A(t)$, also $A(x,y)$ aus der Voraussetzung.

Zur Implikation von rechts nach links. Aus festem, aber beliebigem $t \in X \times Y$ ist $A(t)$ abzuleiten. Mit $t \in X \times Y$ existieren $x \in X$ und $y \in Y$ mit $t = (x,y)$. Hiermit erhält man $A(x,y)$ aus der Voraussetzung. Wegen der Gleichheit von t und (x,y) stimmt $A(x,y)$ mit $A(t)$ überein. $\square$

Ein analoger Sachverhalt besteht bei der Existenzquantifizierung.

Satz 3.6. Es ist $\exists t \in X \times Y \colon A(t)$ äquivalent zu $\exists x \in X \colon \exists y \in Y \colon A(x,y)$.

Beweis. Zur Implikation von links nach rechts. Laut der Voraussetzung ist irgendein $t \in X \times Y$ mit $A(t)$ vorhanden, infolge $x \in X$ und $y \in X$ mit $t = (x,y)$, womit $A(x,y)$ gilt. Ergo existieren $x \in X$ und $y \in Y$ mit $A(x,y)$.

Zur Implikation von rechts nach links. Laut Voraussetzung sind $x \in X$ und $y \in Y$ mit $A(x,y)$ vorhanden. Mit dem aus ihnen geformten Paar $t := (x,y)$ bezeugen sie $t \in X \times Y$. Laut Festlegung ist $A(x,y)$ dasselbe wie $A(t)$, womit t die Existenz eines $t \in X \times Y$ mit $A(t)$ bezeugt. □

Mithin bestehen die korrespondierenden Termumformungen

$$\bigcap_{t \in I \times J} A_t = \bigcap_{i \in I} \bigcap_{j \in J} A_{ij}, \qquad \bigcup_{t \in I \times J} A_t = \bigcup_{i \in I} \bigcup_{j \in J} A_{ij}.$$

Sie bestätigen sich mühelos via

$$\begin{aligned} x \in \textstyle\bigcap_{t \in I \times J} A_t &\iff \forall t \in I \times J \colon x \in A_t \iff \forall i \in I \colon \forall j \in J \colon x \in A_{ij} \\ &\iff \forall i \in I \colon x \in \textstyle\bigcap_{j \in J} A_{ij} \iff x \in \textstyle\bigcap_{i \in I} \bigcap_{j \in J} A_{ij}. \end{aligned}$$

Hier ist A_{ij} eine Kurzschreibweise für $A_{(i,j)}$ bzw. $A_{i,j}$.

3.2 Abbildungen

3.2.1 Der Abbildungsbegriff

Unter einer *Abbildung*, auch *Funktion* genannt, verstehen wir ganz allgemein eine Zuordnung von Elementen einer Definitionsmenge zu Elementen einer Zielmenge, bei der zu *jedem* Element der Definitionsmenge *genau ein* Element der Zielmenge gehört. Es hat allerdings ein wenig gedauert, bis diese Vorstellung als die Förderliche erkannt wurde.

In der historischen Entwicklung ging ihr die speziellere Vorstellung voran, dass eine Größe, etwa eine physikalische Größe, in einer rechnerischen Abhängigkeit von einer anderen Größe steht. So steht die Periodendauer der Schwingung eines Pendels in einer bestimmten rechnerischen Abhängigkeit von der Pendellänge.

Eine recht pragmatische Vorstellung von einer Funktion vermittelt das Modell der Black Box, das soll eine Rechenmaschine sein, deren innere Mechaniken bzw. Elektroniken unbekannt bleiben. Speist man ein Argument x in die Black Box ein, spuckt sie daraufhin einen Wert $f(x)$ aus. Speist man abermals dasselbe Argument ein, spuckt sie abermals denselben Wert aus.

Der Begriff der Abbildung ist für die Mathematik zentral.

Definition 3.12 (Abbildung).
Eine Abbildung $f\colon X \to Y$ ist eine Relation $f = (X, Y, G)$ mit $G \subseteq X \times Y$, die die beiden Eigenschaften

$$\forall x \in X\colon \exists y \in Y\colon (x, y) \in G,$$
$$\forall x \in X\colon \forall y, y' \in Y\colon (x, y) \in G \land (x, y') \in G \Rightarrow y = y'$$

erfüllt. Man nennt G den Graph, X die Definitions- und Y die Zielmenge.

Genau genommen möchte man die Abbildung f eigentlich nicht als mit dem Tripel (X, Y, G) identisch sehen, sondern als dasjenige Objekt, dessen innere Information aus diesem Tripel besteht.

Zuweilen wird der Graph von f auch einfach als f bezeichnet. Sollte dies verwirrend sein, schreibt man ausführlicher G_f oder $\mathrm{Graph}(f)$.

Statt $(x, y) \in G_f$ schreibt man üblicherweise $y = f(x)$. Es wird $f(x)$ gelesen als »f von x« oder »das Bild von x unter f«. Es wird $f\colon X \to Y$ gelesen als »f ist eine Abbildung von X nach Y«. Besitzt ein $y \in Y$ ein $x \in X$ mit $y = f(x)$, nennt man x ein Urbildelement zu y.

Alle denkbaren Abbildungen $X \to Y$ fasst man wiederum zu einer Menge zusammen, die Y^X oder $\mathrm{Abb}(X, Y)$ notiert wird. Zu jeder Menge M sei $|M|$ die Anzahl

ihrer Elemente. Es seien X, Y endlich. Zu jedem Argument $x \in X$ gibt es nun $|Y|$ Möglichkeiten, einen Funktionswert festzulegen. Hat X zwei Elemente, gibt es für das erste Elemente $|Y|$ Möglichkeiten, und für das zweite auch nochmals $|Y|$. Da man beide unabhängig wählen kann, multiplizieren sich die Möglichkeiten zu $|Y|^2$. Allgemein betrachtet findet sich $|Y^X| = |Y|^{|X|}$, was eine gewisse Rechtfertigung für die gewählte Notation liefert.

Es stellt sich die Frage, ob die Formel denn auch im Trivialfall $X = \emptyset$ stimmt. Insofern man $0^0 := 1$ definiert, so dass allgemein $|Y|^0 = 1$ gilt, lautet die Antwort ja, weil $Y^\emptyset = \{\emptyset\}$ ist. Überzeugung leistet die folgende kurze Überlegung. Soll $f\colon \emptyset \to Y$ sein, muss f als Relation eine Teilmenge von $\emptyset \times Y = \emptyset$ sein. Die einzige Teilmenge der leeren Menge ist die leere Menge selbst. Sie ordnet wie gefordert jedem Element der leeren Definitionsmenge genau einen Wert zu. Das mag eigenartig wirken, ist aber, wir erinnern uns an das Prinzip der leeren Wahrheit, der richtige Schluss.

Anders verhält es sich mit $Y = \emptyset$ bei $X \neq \emptyset$. Hier gilt $0^{|X|} = 0$. Auch in diesem Fall stimmt die Formel, weil $\emptyset^X = \emptyset$ ist. Wie zuvor ist die einzige mögliche Relation die leere. Sie müsste allerdings jedem $x \in X$ ein $y \in \emptyset$ zuordnen, was widersprüchlich ist. Ergo ist die Menge der Abbildungen $X \to \emptyset$ leer, sofern X nichtleer ist.

3.2.2 Bild, Urbild

Wird ein jedes Element einer Teilmenge der Definitionsmenge in eine Abbildung geschickt, formen die Werte eine neue Menge, die *Bildmenge* der Teilmenge unter der Abbildung.

Definition 3.13 (Bild).
Die Bildmenge einer Menge $A \subseteq X$ unter der Abbildung $f\colon X \to Y$ ist

$$f(A) := \{f(x) \mid x \in A\} = \{y \mid \exists x \in A\colon y = f(x)\}.$$

Insofern $y = f(x)$ als äquivalent zu $y \in \{f(x)\}$ befunden wird, ergibt sich auch die Darstellung $f(A) = \bigcup_{x\in A}\{f(x)\}$. Insbesondere in Programmiersprachen treten endliche Mengen als Objekte auf. Die Berechnung verläuft mithin gemäß der rekursiven Festlegung

$$f(\emptyset) := \emptyset, \qquad f(\{x_1, \ldots, x_n\}) := f(\{x_1, \ldots, x_{n-1}\}) \cup \{f(x_n)\},$$

für die auch die Bezeichnung $\mathrm{map}(f, A)$ gebräuchlich ist.

Die analytische Geometrie sieht Figuren als Punktmengen. Abbildungen transformieren die Punktmengen, woraus neue Figuren hervorgehen. Ein einfaches Bei-

spiel bietet die Abbildung

$$f\colon \mathbb{R} \to \mathbb{R}^2, \quad f(t) := \begin{pmatrix} p_x + v_x t \\ p_y + v_y t \end{pmatrix}.$$

In der Hinsicht, dass die reellen Zahlen $\mathbb{R}$ als eine Zahlengerade aufgefasst werden, formt ihr Bild $f(\mathbb{R})$ eine Gerade der euklidischen Ebene. Die passende Wahl der Parameter (p_x, p_y) als Basispunkt und (v_x, v_y) als Geschwindigkeitsvektor gestattet es, jede beliebige Gerade der Ebene zu beschreiben. Man nennt in der üblichen Terminologie aber auch t den Parameter und f eine Parametergerade, wobei das Bild $f(\mathbb{R})$ auch Spur genannt wird. Diese Sprechweisen entspringen der Sichtweise, dass $f(t)$ ein durch die Zeit t parametrisierter Punkt ist, der mit dem Lauf der Zeit eine Spur zieht. Der Geschwindigkeitsvektor charakterisiert die Bewegung des Punktes, für die Spur ist dagegen nur dessen Richtung von Bedeutung.

Das *Urbild* eines Wertes gibt Auskunft, welche Elemente der Definitionsmenge unter der Abbildung zu dem Wert führen. Allgemeiner gibt das Urbild einer Menge von Werten Auskunft, welche Elemente der Definitionsmenge in die Menge führen.

Definition 3.14 (Urbild).
Das Urbild einer Menge B unter $f\colon X \to Y$ ist

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\} = \{x \in X \mid \exists y \in B\colon y = f(x)\}.$$

Dem Wesen des Abbildungsbegriffs entspringend, zeichnet sich die Urbildoperation durch Verträglichkeit mit den Mengenoperationen aus, was bei der Bildoperation nur zum Teil stimmt.

Satz 3.7. Für jede Abbildung f und beliebige Mengen A, B, A_i gilt

$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B), \qquad f^{-1}\Big(\bigcap_{i\in I} A_i\Big) = \bigcap_{i\in I} f^{-1}(A_i),$$
$$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B), \qquad f^{-1}\Big(\bigcup_{i\in I} A_i\Big) = \bigcup_{i\in I} f^{-1}(A_i).$$

Beweis. Den Beweis verschafft die äquivalente Umformung

$$x \in f^{-1}\Big(\bigcap_{i\in I} A_i\Big) \iff f(x) \in \bigcap_{i\in I} A_i \iff (\forall i \in I\colon f(x) \in A_i)$$
$$\iff (\forall i \in I\colon x \in f^{-1}(A_i)) \iff x \in \bigcap_{i\in I} f^{-1}(A_i).$$

Bei der Vereinigung verläuft die Umformung analog. □

Der Satz lehrt die wichtige Folgerung, dass die Urbilder zweier disjunkter Mengen ebenfalls disjunkt sind. Allgemein überführt die Urbildoperation eine disjunkte

Zerlegung einer Menge in disjunkte Urbilder. Ist die Zielmenge am feinsten zerlegt, besteht sie also aus einelementigen Mengen, nennt man die Urbilder dieser Mengen auch Fasern. Man beachte, dass ein Urbild oder eine Faser leer sein kann.

Ist die Zielmenge bezüglich einer Ordnungsrelation angeordnet, nennt man die Fasern auch *Niveaumengen*. Diese Begrifflichkeit betrifft vor allem die Funktionen $f\colon X \to \mathbb{R}$ mit $X \subseteq \mathbb{R}^n$. Eine Faser $f^{-1}(\{c\})$, auch als $f(x) = c$ beschrieben, nennt man auch eine *implizite Funktion*. Sie sind in der analytischen Geometrie und der mehrdimensionalen Analysis von großer Bedeutung.

3.2.3 Komposition

Definition 3.15 (Komposition).
Sei $f\colon X \to Y$ und $g\colon Y \to Z$. Ihre Verkettung, gelesen »g nach f«, ist

$$(g \circ f)\colon X \to Z, \quad (g \circ f)(x) := g(f(x)).$$

Oft liegt die Situation $f\colon X \to Y$ und $g\colon Y' \to Z$ mit $Y \subseteq Y'$ vor. Das ist aber nicht weiter schlimm. Es darf dann $g \circ f := g|_Y \circ f$ gesetzt werden, wobei mit $g|_Y$ die Einschränkung des Definitionsbereichs von g auf Y gemeint ist.

Definition 3.16 (Einschränkung).
Sei $f\colon X \to Y$ und $A \subseteq X$. Die Einschränkung von f auf A ist

$$f|_A\colon A \to Y, \quad f|_A(x) := f(x).$$

Die Abbildung $\mathrm{id}_X\colon X \to X$ mit $\mathrm{id}_X(x) := x$ heißt *identische Abbildung*. Sie verhält sich bei der Komposition neutral, das heißt, bezüglich $f\colon X \to Y$ gilt $f \circ \mathrm{id}_X = f$ und $\mathrm{id}_Y \circ f = f$.

Mit der Bildmenge unter einer Komposition verhält es sich ganz analog wie mit dem Funktionswert eines einzelnen Elements. Sie lässt sich als die Hintereinanderschaltung der jeweiligen Mengenabbildungen darstellen, denn es gilt der

Satz 3.8. Es gilt $(g \circ f)(A) = g(f(A))$ für jede Menge $A \subseteq \mathrm{dom}(f)$.

Beweis. Mit der Entfaltung von Def. 3.13, 3.3, 3.1 nimmt die Aussage die Form

$$(\exists x \in A\colon z = (g \circ f)(x)) \iff (\exists y \in f(A)\colon z = g(y))$$

an. Angenommen, die linke Seite gilt. Dann liegt ein $x \in A$ mit $z = g(f(x))$ vor. Sei nun $y := f(x)$, dann gilt $y \in f(A)$ und $z = g(y)$, womit die Existenzaussage der rechten Seite erfüllt wird.

Angenommen, die rechte Seite gilt. Dann liegt ein $y \in f(A)$ mit $z = g(y)$ vor. Infolge existiert laut Def. 3.13 ein $x \in A$ mit $y = f(x)$. Nun gilt $z = g(f(x))$, womit x ebenfalls ein Zeuge für die linke Existenzaussage ist. □

Beim Urbild unter einer Komposition dreht sich die Reihenfolge um.

Satz 3.9. Es gilt $(g \circ f)^{-1}(B) = f^{-1}(g^{-1}(B))$ für jede Menge $B \subseteq \operatorname{cod}(g)$.

Beweis. Die äquivalente Umformung

$$\begin{aligned} x \in (g \circ f)^{-1}(B) &\iff (g \circ f)(x) \in B \iff g(f(x)) \in B \\ &\iff f(x) \in g^{-1}(B) \iff x \in f^{-1}(g^{-1}(B)). \end{aligned}$$ □

Man kann diesen Beweis aber auch so führen, dass die Abbildungen in allgemeiner Weise als Relationen betrachtet werden. Die Gleichheit $y = f(x)$ ist bei einer Relation nicht erklärt, man hat nur $(x, y) \in f$. Unbeschadet dessen bleibt die Umformung durchführbar via

$$\begin{aligned} x \in (g \circ f)^{-1}(B) &\iff (\exists z \in B\colon (x, z) \in g \circ f) \\ &\iff (\exists z \in B\colon \exists y\colon (y, z) \in g \wedge (x, y) \in f) \\ &\iff (\exists y\colon (\exists z \in B\colon (y, z) \in g) \wedge (x, y) \in f) \\ &\iff (\exists y\colon y \in g^{-1}(B) \wedge (x, y) \in f) \\ &\iff x \in f^{-1}(g^{-1}(B)). \end{aligned}$$

3.2.4 Injektionen, Surjektionen, Bijektionen

Definition 3.17 (Injektion).
Eine Abbildung $f\colon X \to Y$ heißt injektiv, wenn

$$\forall x, x' \in X\colon f(x) = f(x') \Rightarrow x = x'.$$

Erinnern wir uns an den Abschnitt *Logik mit Gleichheit*, fällt auf, dass die Definition der Injektivität als Umkehrung der Ersetzungsregel betrachtbar ist. Das heißt, für eine auf den Werten der Terme t, t' definierte Injektion f gilt die Äquivalenz

$$t = t' \iff f(t) = f(t').$$

Die Injektionen vermitteln somit genau die *Äquivalenzumformungen* von Gleichungen. Wie sich aus Def. 3.1 in Verbindung mit Def. 3.4 ergibt, erfährt die Lösungsmenge einer Bestimmungsgleichung durch sie keine Veränderung. Man notiert

$$L := \{x \in G \mid t = t'\} = \{x \in G \mid f(t) = f(t')\}$$

für die Lösungsmenge L der Gleichung $t = t'$ in der Variable x, die die Werte der Grundmenge G durchläuft. Aufgrund dessen schaffen sie ein wesentliches Werkzeug zum Lösen von Bestimmungsgleichungen.

Es muss X bei $f\colon X \to Y$ nicht notwendigerweise die Grundmenge sein. Wichtig ist allein, dass die Terme t, t' ausschließlich Werte in X annehmen können. Beispielsweise ist das Quadrieren auf den reellen Zahlen zwar nicht injektiv, bei Einschränkung der Definitionsmenge auf die nichtnegativen reellen Zahlen allerdings schon. So initiiert es die äquivalente Umformung

$$|x| = |x-2| \Leftrightarrow x^2 = (x-2)^2 = x^2 - 4x + 4 \Leftrightarrow 0 = -4x + 4 \Leftrightarrow x = 1.$$

Außerdem darf die Variable der Bestimmungsgleichung in einer Äquivalenzumformung als Parameter auftauchen. Die injektive Funktion

$$f_a\colon \mathbb{R} \to \mathbb{R}, \quad f_a(\xi) := \xi + a$$

beschreibt zum Beispiel den Sachverhalt, dass eine Zahl a zu beiden Seiten einer Gleichung addiert werden darf,

$$t = t' \iff t + a = t' + a.$$

Hier darf insbesondere auch $a := x$ als Parameter eingesetzt werden. Bei

$$f_a\colon \mathbb{R} \to \mathbb{R}, \quad f_a(\xi) := a\xi$$

gilt es allerdings $a \neq 0$ zu berücksichtigen. Das heißt, die Setzung $a := x$ liefert nur dann eine Äquivalenzumformung, wenn die Grundmenge, die x durchläuft, eine Teilmenge von $\mathbb{R} \setminus \{0\}$ ist. Andernfalls müsste man diesen Umstand durch eine Fallunterscheidung künstlich herstellen.

Erwähnenswert ist weiterhin, dass die gemachten Begriffe bereits Gleichungen in mehreren Variablen und Gleichungssysteme umfassen. Eine Gleichung in zwei Variablen liegt vor, wenn die Grundmenge aus Paaren besteht. Ein System von zwei Gleichungen liegt vor, wenn die die Terme t, t' jeweils ein Paar zum Wert haben. Diese formale Beschreibung müsste man allerdings als ein wenig oberflächlich befinden, kämen nicht weitere Erörterungen hinzu. Tiefersinnig wäre es an sich ohne Pointe, tauchte nur eine der Variablen in der Gleichung auf. Gleichermaßen mag ein System in zwei Variablen erst reizvoll sein, wenn die Gleichungen in nichttrivialer Weise miteinander verwoben sind.

Satz 3.10. Eine Abbildung g mit $g \circ f = \mathrm{id}$ heißt Linksinverse von f. Eine Abbildung $f\colon X \to Y$ mit nichtleerem X ist genau dann injektiv, wenn sie mindestens eine Linksinverse besitzt.

Beweis. Sei g eine Linksinverse von f. Seien x, x' fest, aber beliebig, und sei $f(x) = f(x')$. Mithin gilt $g(f(x)) = g(f(x'))$. Weil g eine Linksinverse ist, hat man aber $g(f(x)) = x$ und $g(f(x')) = x'$, womit sich wie gewünscht $x = x'$ ergibt.

Sei f injektiv. Mit $X \neq \emptyset$ liegt irgendein $a \in X$ vor. Sofern $y \in f(X)$ ist, liegt außerdem ein x mit $y = f(x)$ vor. Es wird g festgelegt per Fallunterscheidung

$$g(y) := \begin{cases} x, & \text{wenn } y \in f(X), \\ a, & \text{wenn } y \notin f(X). \end{cases}$$

Sie ist verhält sich so, dass $g(f(x)) = x$ für jedes $x \in X$ gilt, denn mit $x \in X$ ist $f(x) \in f(X)$. Somit existiert mit g eine Linksinverse. □

Definition 3.18 (Surjektion).
Eine Abbildung $f\colon X \to Y$ heißt surjektiv, wenn $f(X) = Y$ ist.

Weil $f(X) \subseteq Y$ allgemeingültig ist, genügt es generell, $Y \subseteq f(X)$ zu zeigen.

Definition 3.19 (Bijektion).
Eine Abbildung heißt bijektiv, wenn sie sowohl injektiv als auch surjektiv ist.

Satz 3.11. Jede Bijektion f besitzt eine eindeutig bestimmte Abbildung, welche sowohl ihre einzige Linksinverse als auch ihre einzige Rechtsinverse ist. Man nennt sie die Umkehrabbildung f^{-1}.

Beweis. Sei $f\colon X \to Y$ bijektiv. Es existiert somit mindestens eine Linksinverse g und mindestens eine Rechtsinverse h. Weil die Verkettung das Assoziativgesetz erfüllt, darf man rechnen

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_X \circ h = h.$$

Sei nun g' eine weitere Linksinverse und h' eine weitere Rechtsinverse. Wiederholt man die obige Rechnung abermals, erhält man $g' = h$ und $g' = h'$. Ergo gilt $g = h = g' = h'$. □

3.2.5 Allgemeines Mengenprodukt

Nachdem nun der Begriff der Abbildung bereits erklärt wurde, kann eine Begriffsverallgemeinerung des kartesischen Produktes erörtert werden, die Tupel mit Folgen und Funktionen in Beziehung setzt. Eine Folge darf man einerseits als Funktion betrachten, deren Definitionsbereich die natürlichen Zahlen sind. Andererseits ist eine Folge indizierbar wie ein Tupel. Das bringt uns auf die Idee, Tupel wie Folgen als Funktionen aufzufassen.

Die Ziffern der Zahl 2520 sind in Little-Endian-Konvention das Tupel

$$t = (0, 2, 5, 2) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}.$$

Die Indexmenge $I := \{0, 1, 2, 3\}$ enthält die Stellenwerte der Ziffern. Es verhält sich nun so, dass die Funktion

$$f\colon I \to \mathbb{N}, \quad f(0) := 0,\ f(1) := 2,\ f(2) := 5,\ f(3) := 2$$

genau die Information enthält, die das Tupel charakterisiert. Es ist $f(i) = t_i$ die Indizierung des Tupels. So gesehen ist jedes Tupel durch eine Funktion kodiert. Führt man diese Überlegung fort, gelangt man schließlich zum allgemeinen kartesischen Produkt

$$\prod_{i\in I} X_i := \{f\colon I \to \bigcup_{i\in I} X_i \mid \forall i \in I\colon f(i) \in X_i\}.$$

Der Formelsalat sagt im Wesentlichen nur, dass eine Abbildung $f \in \prod_{i\in I} X_i$ einen in X_i liegenden Funktionswert $f(i)$ besitzt.

Diese allgemeine Produkte von Mengen treten in der Mathematik nur sehr sporadisch in Erscheinung. Eine Rolle spielen sie in der Theorie der Kardinalzahlen. In der abhängigen Typentheorie besitzen sie allerdings ein direktes allgegenwärtiges Analogon, den *Typ abhängiger Funktionen*.

Bei einer Gleichsetzung wie $\prod_{i\in\{1,2\}} X_i \cong X_1 \times X_2$ ist zu beachten, dass es sich eigentlich nicht um eine Gleichung handelt, denn Abbildungen sind ja nicht dasselbe wie Paare. Allerdings gehört zu jedem Paar wie gesagt in kanonischer Weise genau eine gleichartige Abbildung. Es besteht eine Isomorphie, was durch die Tilde über dem Gleichheitszeichen angedeutet wird. Damit verbunden liegt ein Isomorphismus vor, mit dem sich ein Objekt der einen Seite in ein Objekt der anderen Seite überführen lässt. Das ist so ähnlich wie die Übersetzung eines Textes von der einen in die andere Sprache. Die Gestalt ändert sich, aber der Inhalt bleibt gleich.

Intuitiv sollte $\prod_{i\in I} X_i$ nichtleer sein, sofern jedes X_i nichtleer ist. Dennoch lässt sich dieser Sachverhalt nicht ohne Weiteres ableiten. Es handelt sich um ein Axiom der Mengenlehre, das sogenannte *Auswahlaxiom*. Es besagt, dass zu jeder Familie (X_i) nichtleerer Mengen eine Auswahlfunktion f existiert, die zu jeder Menge

X_i ein Element $f(i) \in X_i$ auswählt. Eine gründliche Untersuchung des Auswahlaxioms zeigt auf, dass es sich mit den Unendlichkeiten schwierig verhält. Unter bestimmten Umständen ist das Axiom nicht vonnöten. Außerdem, so lässt sich zeigen, impliziert es den Satz vom ausgeschlossenen Dritten.

3.3 Relationen

3.3.1 Relationen im Allgemeinen

Beim Erlangen von tieferliegenden Einsichten in Probleme und Zusammenhänge spielt das Aufspüren und Klären unterschiedlicher Beziehungen eine wesentliche Rolle. Zwei Objekte können auf unterschiedliche Art und Weise in Beziehung stehen. In der Mathematik beschäftigt man sich mit Beziehungen, die zu den zwei Objekten eine Aussage trifft, der ein Wahrheitsgehalt beigemessen wird. Zwei Zahlen x, y sind gleich. Eine Zahl x ist kleiner als eine Zahl y. Der Betrag der Differenz zweier Zahlen x, y ist kleiner als eine bstimmte Konstante. Der Abstand der Punkte $x = (x_1, x_2)$ und $y = (y_1, y_2)$ ist kleiner als eine bestimmte Konstante. Zwei Stühle x, y eines Stuhlkreises sind benachbart. Die Schüler x, y gehen in dieselbe Klasse. Es gibt einen Weg, der vom Ort x zum Ort y führt.

Die eindrückliche Vielfalt möglicher Beziehungen macht es ja unerlässlich, eine allgemeine Auffassung von ihnen zu erhalten. Eine zweistellige Relation R schafft ein Beziehungsgefüge zwischen zwei Mengen X, Y. Wir sagen, ein Objekt $x \in X$ steht bezüglich R zu einem Objekt $y \in Y$ in Beziehung, wenn die Aussage $R(x, y)$ eine wahre ist. Ein Beispiel wäre $R(x, y) := (x < y)$, wobei $X = Y$ die Menge der ganzen Zahlen sei.

Definition 3.20 (Zweistellige Relation).
Es seien X, Y zwei Mengen. Jede Teilmenge $R \subseteq X \times Y$ heißt Relation zwischen X und Y. Zur Relation soll die Kenntnis von X, Y dazugehören. Insofern ist das durch das Tripel (X, Y, R) kodierte Objekt die Relation und R ihr Graph.

Eine Relation ist auch interpretierbar als wahrheitswertige Funktion

$$1_R \colon X \times Y \to \{0, 1\}, \quad 1_R(x, y) := [(x, y) \in R].$$

Sie ist die Indikatorfunktion der Teilmenge R bezüglich der Grundmenge $X \times Y$. Anstelle $(x, y) \in R$ oder $1_R(x, y) = 1$ schreiben wir schlicht $R(x, y)$ für die Aussage, dass x und y bezüglich R in Relation stehen.

Eine Relation mit $X \neq Y$ heißt *heterogen*, eine mit $X = Y$ heißt *homogen*. Wir werden uns fast ausschließlich mit homogenen Relationen beschäftigen. Man darf

allerdings sagen, dass auch die heterogenen in der Mathematik weit verbreitet sind, denn jede Abbildung ist betrachtbar als Relation mit speziellen Eigenschaften. Genauer ist eine Abbildung eine linkstotale und rechtseindeutige Relation. Linkstotal heißt, dass jedes $x \in X$ zu mindestens einem $y \in Y$ in Beziehung steht. Rechtseindeutig heißt, dass ein $y \in Y$ höchstens zu einem $x \in X$ in Beziehung steht. Es handelt sich also lediglich um eine Sprechweise für die bereits bekannten definierenden Eigenschaften.

Relationen lassen sich in Pfeildiagrammen darstellen. Man man zweichnet hierbei einem Pfeil von einem $x \in X$ zu einem $y \in Y$, falls x, y in Relation stehen.

3.3.2 Äquivalenzrelationen

Manchmal interessiert man sich nicht für die gänzliche Gleichheit zweier Objekte. Die *Äquivalenzrelationen* verallgemeinern den Gleichheitsbegriff dahingehend, dass zwei Objekte schon dann als *gleichartig* angesehen werden, wenn sie in in einer bestimmten Eigenschaft übereinstimmen. Um welche Eigenschaft es sich dabei handelt, bestimmt die Relation.

Definition 3.21 (Äquivalenzrelation).
Seien A eine Menge und seien $x, y, z \in A$. Sei $R(x, y) := (x \sim y)$ eine Relation. Man nennt R Äquivalenzrelation, wenn gilt:

$$\begin{aligned} &x \sim x, && \text{(Reflexivität)} \\ &x \sim y \implies y \sim x, && \text{(Symmetrie)} \\ &x \sim y \wedge y \sim z \implies x \sim z. && \text{(Transitivität)} \end{aligned}$$

Definition 3.22 (Äquivalenzklasse).
Sei M eine Menge und $x \sim y$ eine Äquivalenzrelation für $x, y \in M$. Die Menge

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

nennt man die Äquivalenzklasse zum Repräsentanten $a \in M$.

Satz 3.12 (Äquivalenzrelation induziert Zerlegung).
Eine Menge wird durch eine Äquivalenzrelation in disjunkte Äquivalenzklassen zerlegt, lat. partitioniert.

Beweis. Sei M die Menge und $x \sim y$ die Äquivalenzrelation. Zu zeigen ist, dass kein Element von M in mehr als einer Äquivalenzklasse vorkommt. Seien $a, b, c \in M$,

sei $c \in [a]$ und $c \in [b]$. Aufgrund von $c \sim a$ sowie $c \sim b$ und der Transitivität gilt

$$x \in [a] \iff x \sim a \iff x \sim c \iff x \sim b \iff x \in [b].$$

Man hat also

$$(\forall x \in M\colon x \in [a] \Leftrightarrow x \in [b]) \iff [a] = [b].$$

Wenn also $[a] \neq [b]$ ist, kann nicht gleichzeitig $c \in [a]$ und $c \in [b]$ sein. □

Satz 3.13 (Zerlegung induziert Äquivalenzrelation).
Sei M eine Menge. Die Familie (A_k) von Mengen $A_k \subseteq M$ bilde eine Zerlegung von M, d. h. dass die Vereinigung aller A_k die Menge M überdeckt und dass paarweise $A_i \cap A_j = \emptyset$ für $i \neq j$ ist. Dann ist

$$x \sim y \ :\Longleftrightarrow\ \exists k\colon x \in A_k \wedge y \in A_k$$

eine Äquivalenzrelation auf M.

Beweis. Da die A_k die Menge M überdecken, muss es für ein beliebiges $x \in M$ mindestens eine Menge A_k geben, so dass $x \in A_k$. Daher gilt $x \sim x$.

Die Symmetrie ergibt sich trivial.

Zur Transitivität. Voraussetzung ist $x \sim y$ und $y \sim z$. Es gibt also ein i mit $x \in A_i$ und $y \in A_i$. Außerdem gibt es ein j mit $y \in A_j$ und $z \in A_j$. Somit gilt

$$\exists i\colon \exists j\colon x \in A_i \wedge y \in A_i \wedge y \in A_j \wedge z \in A_j.$$

Wegen

$$A_i \cap A_j = \emptyset \iff \forall y\colon (y \in A_i \wedge y \in A_j \Leftrightarrow 0)$$

für $i \neq j$ kann $y \in A_i \wedge y \in A_j$ aber nur erfüllt sein, wenn $i = j$ ist. Daher ergibt sich

$$\exists i\colon x \in A_i \wedge z \in A_i,$$

das heißt $x \sim z$. □

Definition 3.23 (Quotientenmenge).
Für eine gegebene Äquivalenzrelation wird die aus allen Äquivalenzklassen bestehende Menge

$$M/\!\sim \ := \{[x] \mid x \in M\}$$

als Quotientenmenge oder Faktormenge bezeichnet.

Definition 3.24 (Quotientenabbildung).
Für eine gegebene Äquivalenzrelation ist die Projektion

$$\pi\colon M \to M/\sim, \quad \pi(x) := [x]$$

surjektiv und wird Quotientenabbildung genannt.

Definition 3.25 (Repräsentantensystem).
Für eine gegebene Äquivalenzrelation auf M nennt man eine Teilemenge $A \subseteq M$ ein vollständiges Repräsentantensystem, wenn die Einschränkung $\pi|_A$ bijektiv ist, wobei mit π die Quotientenabbildung gemeint ist.

Repräsentantensysteme ermöglichen die einfache Handhabung von Äquivalenzklassen. Möchte man wissen, ob ein Element x in der Äquivalenklasse $[a]$ enthalten ist, dann braucht man bloß zu überprüfen, ob $x \sim a$ ist. Außerdem besitzt die Quotientenabbildung nun eine Darstellung $p\colon M \to A$, dergestalt dass $\pi = \pi|_A \circ p$. Warum sollte das von Bedeutung sein? Nun, Äquivalenzklassen fallen oft unendlich groß aus. In der Kombinatorik treten zwar auch endliche Äquivalenzklassen auf, diese werden trotzdem schnell unzugänglich groß. Die Äquivalenzklassen und die Quotientenabbildung muss man also als abstrakte mathematische Objekte betrachten. Abstrakte mathematische Objekte müssen wir erst über eine Darstellung zugänglich machen, und genau dies ermöglicht ein Repräsentantensystem.

Satz 3.14 (Charakterisierung von Äquivalenzklassen).
Sei auf der Menge M eine Äquivalenzrelation gegeben. Eine Teilmenge $A \subseteq M$ ist genau dann eine Äquivalenzklasse, wenn

1. $A \neq \emptyset$,
2. $x, y \in A \implies x \sim y$,
3. $x \in A \land y \in M \land x \sim y \implies y \in A$.

Beweis. Angenommen, A ist eine Äquivalenzklasse. Dann gibt es definitionsgemäß ein a mit $A = [a]$. Daher ist mindestens $a \in A$ und somit $A \neq \emptyset$. Mit $x, y \in A$ ergibt sich $A = [x] = [y]$. Aufgrund von

$$x \sim y \iff [a] = [b]$$

muss somit $x \sim y$ sein. Sei nun $x \in A$ und $y \in M$ mit $x \sim y$. Es folgt $A = [x] = [y]$. Daher muss $y \in A$ sein.

Umgekehrt angenommen, die drei Eigenschaften sind erfüllt. Zu zeigen ist, dass es ein a gibt mit $A = [a]$. Da A gemäß 1. nichtleer ist, enthält es mindestens ein Element, dieses nennen wir a. Für jedes weitere Element $x \in A$ ergibt sich $x \sim a$, da sonst 2. verletzt sein würde. Schließlich muss man noch wissen, ob $x \in A$, wenn $x \sim a$ und $x \in M$ ist. Dies ist aber mit 3. gesichert. Es gibt also tatsächlich ein a mit $A = \{x \in M \mid x \sim a\}$. □

Eine große Fülle von Äquivalenzrelationen lässt sich auf die folgende einfache Art konstruieren. Hat man eine beliebige Abbildung $f\colon X \to Y$, dann sind die Urbilder $f^{-1}(\{y_1\})$ und $f^{-1}(\{y_2\})$ disjunkt, sofern $y_1 \neq y_2$, denn

$$f^{-1}(\{y_1\}) \cap f^{-1}(\{y_2\}) = f^{-1}(\{y_1\} \cap \{y_2\}) = f^{-1}(\emptyset) = \emptyset.$$

Demnach ist gemäß

$$Z = X/\!\sim = \{f^{-1}(\{y\}) \mid y \in f(X)\}$$

eine Zerlegung des Definitionsbereichs X gegeben und somit auch eine Äquivalenzrelation. Für $x_1, x_2 \in X$ gilt

$$x_1 \sim x_2 \iff f(x_1) = f(x_2).$$

Ist f zudem surjektiv, dann gehört zu jedem Element von Y genau eine Äquivalenzklasse. Demnach definiert f dann eine verallgemeinerte Quotientenabbildung, da die Elemente von Y die Äquivalenzklassen charakterisieren. Die Bijektion $\varphi\colon Z \to Y$ hat dabei die Eigenschaft $f = \varphi \circ \pi$. Sofern Y für uns zugänglich ist, resultiert hieraus auch eine verallgemeinerte Darstellung der Quotientenabbildung, denn

$$f = \varphi \circ \pi = \varphi \circ (\pi|_A \circ p) = (\varphi \circ \pi|_A) \circ p.$$

Nun ist $\varphi \circ \pi|_A$ auch bijektiv, weil φ und $\pi|_A$ es sind. Somit charakterisiert Y ein vollständiges Repräsentantensystem.

Was bisher erläutert wurde, mag recht abstrakt erscheinen. Wir haben aber eigentlich ein recht intuitives Verständnis für diese Begrifflichkeiten. Ein Bilderbuchbeispiel für eine Quotientenmenge bieten die Klassen einer Schule. Zwei Schüler seien genau dann äquivalent, wenn sie in dieselbe Klasse gehen. Die Äquivalenzklasse eines Schülers ist dann schlicht seine Schulklasse. Die Menge der Schüler der Schule wird in disjunkte Schulklassen zerlegt. Die Menge dieser Schulklassen bildet die Quotientenmenge. Ein vollständiges Repräsentantensystem entsteht zum Beispiel durch die Wahl eines Klassensprechers in jeder Klasse.

Ein weiteres typisches Beispiel für eine Äquivalenzrelation ist die Kongruenz modulo m, die elementar in der Zahlentheorie und Gruppentheorie vorkommt. Die Äquivalenzklassen sind hier die Restklassen. Die Reste bilden ein kanonisches vollständiges Repräsentantensystem. Das Bilden des Restes zu einer Zahl ist eine Darstellung der Quotientenabbildung.

3.3.3 Operationen auf Äquivalenzklassen

Äquivalenzklassen werden später wichtig sein für die Formulierung von Konstruktionen. Bei diesen Konstruktionen ist eine Abbildung zwischen Quotientenmengen erforderlich. Weil die Äquivalenzklassen dabei über Repräsentanten dargestellt sind, liegt es nahe, auch die Abbildung über Repräsentanten zu definieren. Dies wirft die Frage nach der *Wohldefiniertheit* auf. Darunter versteht man, dass die Abbildung auch tatsächlich unabhängig von den gewählten Repräsentanten ist. Was das genau bedeutet, wird im folgenden Abschnitt erklärt.

Gegeben seien zwei Quotientenmengen $M/\sim$ und $M'/\sim'$. Eine vorhandene Abbildung $f\colon M \to M'$ induziert dann eventuell gemäß

$$f\colon M/\sim \longrightarrow M'/\sim', \quad f([a]) := [f(a)]$$

eine Abbildung zwischen den Quotientenmengen. Kommt es dabei nicht zu einem Widerspruch, liegt also eine Abbildung vor, spricht man von *Wohldefiniertheit*. Hierfür darf der Funktionswert nicht vom gewählten Repräsentant abhängen, d. h. die Bedingung

$$\forall x \in [a]\colon f(x) \in [f(a)]$$

muss erfüllt sein. Anders formuliert:

$$x \sim a \implies f(x) \sim' f(a).$$

Für mehrstellige Abbildungen ist das Vorgehen analog. Eine Abbildung $f\colon M^2 \to M'$ induziert

$$f\colon (M/\sim)^2 \to M'/\sim', \quad f([a],[b]) := [f(a,b)],$$

sofern

$$x \sim a \wedge y \sim b \implies f(x,y) \sim' f(a,b).$$

Bei den Konstruktionen kommen in der Regel zweistellige Abbildungen (mit $M = M'$) vor, weil die Verknüpfungen von Elementen der algebraischen Strukturen zweistellig sind. Diese Verknüpfungen werden im nächsten Abschnitt besprochen.

3.3.4 Kongruenzrelationen

Definition 3.26 (Kongruenzrelation).
Gegeben sei eine Menge M, auf der eine zweistellige Verknüpfung $*\colon M^2 \to M$ definiert ist. Eine Äquivalenzrelation auf M nennt man Kongruenzrelation, wenn die induzierte Verknüpfung $[a] * [b] := [a * b]$ wohldefiniert ist.

Bei einer Kongruenzrelation sagt man »a ist kongruent zu b« anstelle von »a ist äquivalent zu b« und schreibt $a \equiv b$ anstelle von $a \sim b$. Eigentlich kann man den Begriff für eine beliebige Stelligkeit definieren. Es besteht jedoch zunächst nur Bedarf an zweistelligen Verknüpfungen.

Im Folgenden schreiben wir für die Verknüpfung kurz ab anstelle $a*b$. Das spart ein wenig Schreibaufwand und ist so üblich, solange keine Verwechslungsgefahr mit einer bereits auf andere Art definierten Multiplikation besteht.

Satz 3.15. Sei M eine Struktur aus der Liste Magma, Monoid, Halbgruppe, Gruppe, kommutatives Monoid, kommutative Gruppe. Sei $\equiv$ eine Kongruenzrelation auf M und φ die zugehörige Quotientenabbildung. Dann bildet die Quotienmenge $M/\equiv$ bezüglich der induzierten Verknüpfung $\varphi(a)\varphi(b) := \varphi(ab)$ ebenfalls eine Struktur derselben Art und φ ist ein Homomorphismus.

Beweis. Im Folgenden seien a', b', c' beliebige Elemente der Quotientenmenge. Weil φ surjektiv ist, gibt es immer $a, b, c \in M$ mit $a' = \varphi(a)$, $b' = \varphi(b)$ und $c' = \varphi(c)$.

Die Verknüpfung auf M sei abgeschlossen. Dann ist

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in M/\equiv .$$

Somit ist die Quotientenmenge bezüglich der induzierten Verknüpfung abgeschlossen.

Die Verknüpfung auf M erfülle das Assoziativgesetz. Dann gilt

$$(a'b')c' = \varphi(ab)\varphi(c) = \varphi(abc) = \varphi(a)\varphi(bc) = a'(b'c').$$

Die induzierte Verknüpfung erfüllt somit ebenfalls das Assoziativgesetz.

Die Verknüpfung auf M habe ein neutrales Element e. Dann gilt

$$\varphi(a) = \varphi(ea) = \varphi(e)\varphi(a), \quad \varphi(a) = \varphi(ae) = \varphi(a)\varphi(e).$$

Demzufolge besitzt $M/\equiv$ mit $e' := \varphi(e)$ ebenfalls ein neutrales Element.

Zur Verknüpfung auf M gebe es zu jedem Element ein inverses. Dann gilt

$$\varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}), \quad \varphi(e) = \varphi(a^{-1}a) = \varphi(a^{-1})\varphi(a).$$

Demzufolge gibt es auf der Quotientenstruktur mit $\varphi(a)^{-1} := \varphi(a^{-1})$ ebenfalls zu jedem Element ein inverses.

Die Verknüpfung auf M sei kommutativ. Dann gilt

$$a'b' = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = b'a'.$$

Somit ist die Verknüpfung auf der Quotientenstruktur $M/\equiv$ ebenfalls kommutativ. □

Satz 3.16. Satz 3.15 gilt auch für Ringe, unitäre Ringe, kommutative Ringe und kommutative unitäre Ringe, sofern die Relation eine Kongruenzrelation sowohl bezüglich der additiven als auch der multiplikativen Verknüpfung ist.

Beweis. Sei $(R, +, \cdot)$ der Ring und $\equiv$ die Kongruenzrelation. Gemäß Satz 3.15 ist $(R/\equiv, +)$ eine kommutative Gruppe und $(R/\equiv, \cdot)$ eine Halbgruppe. Bei einem unitären Ring ist $(R/\equiv, \cdot)$ ein Monoid, und bei einem kommutativen unitären Ring ein kommutatives Monoid.

Es verbleiben noch die Distributivgesetze zu prüfen. Sei φ die Quotientenabbildung. Man rechnet

$$\begin{aligned} a'(b' + c') &= \varphi(a)(\varphi(b) + \varphi(c)) = \varphi(a)(\varphi(b + c)) = \varphi(a(b + c)) = \varphi(ab + ac) \\ &= \varphi(ab) + \varphi(ac) = \varphi(a)\varphi(b) + \varphi(a)\varphi(c) = a'b' + a'c'. \end{aligned}$$

Die Rechnung zum Rechtsdistributivgesetz ist analog.

Damit ist der Satz gezeigt, und ferner ist gezeigt dass φ ein Ringhomomorphismus ist. Und für einen unitären Ring ist φ Eins-erhaltend, wie bereits aus Satz 3.15 hervorgeht. □

3.3.5 Ordnungsrelationen

Bei vielen Untersuchungen genügt es nicht, Elemente einer Menge nur vergleichen zu können. Man möchte zusätzlich in Erfahrung bringen können, ob Elemente in einer bestimmten Weise geordnet sind, in einer bestimmten Weise in Reihenfolge stehen. Hierfür definiert man *Ordnungsrelationen*, von denen es verschiedene Arten gibt, je nachdem, welche Axiome sie erfüllen. Auf einer Menge können auch mehrere unterschiedliche Ordungsrelationen derselben Art definiert werden.

Eine in vielen Bereichen der Mathematik hiesige Art von Relation ist die *Halbordnung*, auch *Partialordnung* genannt. Eine wichtige Unterart der Halbordnungen stellen die *Totalordnungen* dar. So ist die Totalordnung der reellen Zahlen in der Analysis von zentraler Bedeutung.

Definition 3.27 (Halbordnung).
Eine auf einer Menge M definierte Relation $\leq$ heißt Halbordnung, wenn

$$\begin{aligned} &\forall x \in M\colon x \leq x, && \text{(Reflexivität)}\\ &\forall x, y \in M\colon x \leq y \wedge y \leq x \Rightarrow x = y, && \text{(Antisymmetrie)}\\ &\forall x, y, z \in M\colon x \leq y \wedge y \leq z \Rightarrow x \leq z. && \text{(Transitivität)} \end{aligned}$$

Ist $\leq$ eine Halbordnung auf M, nennt man M eine halbgeordnete Menge und kodiert dies als Struktur $(M, \leq)$, um klarzustellen, bezüglich welcher Relation die Menge halbgeordnet ist.

Die zu einer Halbordnung zugehörige strenge Halbordnung wird definiert durch

$$x < y \;:\Longleftrightarrow\; x \leq y \wedge x \neq y.$$

Eine Relation R auf M heißt *irreflexiv*, wenn

$$\neg\exists x \in M\colon R(x, x),$$

in Worten, wenn kein Element zu sich selbst in Relation steht. Man bestätigt mühelos, dass die strenge Halbordnung irreflexiv und transitiv ist.

Definition 3.28 (Totalordnung).
Eine Halbordnung $\leq$ auf M heißt Totalordnung, wenn

$$\forall x, y \in M\colon x \leq y \vee y \leq x. \qquad \text{(Totalität)}$$

Das geläufigste Beispiel für eine Totalordnung ist die herkömmliche Ordnung der reellen Zahlen.

Wie bei Halbordnungen ist die zu einer Totalordnung zugehörige strenge Totalordnung erklärt durch

$$x < y \;:\Longleftrightarrow\; x \leq y \wedge x \neq y.$$

Satz 3.17. Die strenge Totalordnung ist *trichotom*, das heißt,

$$\forall x, y \in M\colon (x < y) \oplus (x = y) \oplus (y < x).$$

Beweis. Zunächst machen wir uns klar,

$$A \oplus B \oplus C \iff (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C).$$

In dem Fall, wo eine der drei Aussagen gezeigt wird, sind also außerdem die beiden anderen Aussagen zu widerlegen.

Es wird eine Fallunterscheidung bezüglich der Gleichheit unternommen. Im Fall $x = y$ führt laut Definition der strengen Totalordnung sowohl $x < y$ als auch $y < x$ zu einem Widerspruch. Es sei nun $x \neq y$ der Fall. Laut Totalität liegt $x \leq y \vee y \leq x$ vor. Es sei $x \leq y$ der Unterfall. Sofort folgt $x < y$ gemäß Definition der strengen Totalordnung. Angenommen, es wäre $y < x$, dann wäre neben $x \leq y$ laut Definition der strengen Totalordnung mithin auch $y \leq x$, womit laut Antisymmetrie $x = y$ wäre, was aber im Widerspruch zu $x \neq y$ steht. Die Argumentation im Unterfall $y \leq x$ verläuft analog. □

Satz 3.18. Ist $\leq$ eine Totalordnung auf M, dann gilt

$$\forall x, y \in M \colon \neg(x \leq y) \Leftrightarrow y < x.$$

Beweis. Von links nach rechts. Es gelte $\neg(x \leq y)$. Laut Totalität muss dann $y \leq x$ sein. Angenommen, es wäre $x = y$, dann wäre insbesondere $x \leq y$, was widersprüchlich zur Voraussetzung ist. Also muss $x \neq y$ sein, und somit $y < x$.

Von rechts nach links. Es gelte $y < x$, also $y \leq x$ und $x \neq y$. Angenommen, es wäre $x \leq y$, dann wäre $x = y$ gemäß Antisymmetrie, was aber im Widerspruch zu $x \neq y$ steht. □

3.4 Kardinalzahlen

3.4.1 Gleichmächtigkeit

Definition 3.29 (Gleichmächtigkeit).
Zwei Mengen seien genau dann gleichmächtig, wenn zwischen diesen mindestens eine Bijektion existiert.

Die Aussage »A ist gleichmächtig zu B« notiert man kurz $|A| = |B|$.

Fast trivial ist, dass es sich bei der Gleichmächtigkeit um eine Äquivalenzrelation handelt. Seien dazu A, B, C beliebig. Eine Bijektion $A \to A$ liefert die identische Abbildung, womit Reflexivität besteht. Liegt eine Bijektion $A \to B$ vor, so auch ihre bijektive Umkehrabbildung $B \to A$, womit Symmetrie besteht. Schließlich ist die Verkettung einer Bijektion $A \to B$ mit einer Bijektion $B \to C$ ebenfalls bijektiv, womit Transitivität besteht.

Die kontraintuitive Eigenart des Unendlichen wird gerne anhand von *Hilberts Hotel* veranschaulicht. Es handelt sich um ein Hotel mit unendlich vielen Zimmern,

die mit den positiven ganzen Zahlen nummeriert sind. Anders als ein endliches, kann es auch dann weitere Gäste aufnehmen, wenn es bereits voll belegt ist.

Die Zimmer in Hilberts Hotel seien mit $1, 2, 3$ usw. nummeriert und gänzlich jeweils mit einem Gast belegt. Nun kommt ein neuer Gast mit der Nummer 0 hinzu. Um auch ihn im Hotel unterbringen zu können, wechselt jeder Gast in das nächste Zimmer. Formal handelt es sich um die Zuordnung

$$f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 1}, \quad f(n) := n + 1.$$

Hierbei kommt es, begründet durch die Endlosigkeit des Hotels, nie zu einer Komplikation. Es gibt kein letztes Zimmer, dessen Gast nun mangels freiem Zimmer im Flur stünde. Die Funktion f ist ersichtlich bijektiv, denn *jedes* Zimmer des Hotels wird belegt, und zwar von *nicht mehr als einem* Gast. Das bedeutet aber, dass die nichtnegativen ganzen Zahlen, obwohl sie ein weiteres Element enthalten, zu den positiven ganzen Zahlen gleichmächtig sind.

Allgemeiner kann auf diese Weise jede endliche Zahl weiterer Gäste im Hotel untergebracht werden. *Die Mächtigkeit einer abgezählten unendlichen Menge erhöht sich nicht durch die Hinzunahme einer endlichen Zahl weiterer Elemente.*

3.4.2 Kardinalzahlarithmetik

Satz 3.19. Die Addition $|A| + |B| := |A \cup B|$ ist für $A \cap B = \emptyset$ wohldefiniert.

Beweis. Zu zeigen ist, dass das Ergebnis nicht von der Wahl der Repräsentanten A, B abhängt. Das heißt, es ist zu zeigen, dass $|A \cup B| = |A' \cup B'|$ aus $|A| = |A'|$ und $|B| = |B'|$ mit $A' \cap B' = \emptyset$ folgt. Nach Voraussetzung existieren Bijektionen $f_1\colon A \to A'$ und $f_2\colon B \to B'$. Wie bei der Summe, dem algebraischen Datentyp zur disjunkten Vereinigung, konstruiert man eine Fallunterscheidung

$$f\colon A \cup B \to A' \cup B', \quad f(x) := \begin{cases} f_1(x) & \text{für } x \in A, \\ f_2(x) & \text{für } x \in B. \end{cases}$$

Die Abbildung f ist injektiv. Sei dazu y ein beliebiges Bild. Weil A', B' disjunkt sind, ist entweder $y \in A'$, womit

$$f(x_1) = f(x_2) = y \in A' \implies y = f_1(x_1) = f_1(x_2) \implies x_1 = x_2,$$

oder $y \in B'$, womit

$$f(x_1) = f(x_2) = y \in B' \implies y = f_2(x_1) = f_2(x_2) \implies x_1 = x_2.$$

Zusammengefasst folgt $x_1 = x_2$ aus $f(x_1) = f(x_2)$.

Auch ist f surjektiv. Sei dazu y ein beliebiges Element der Zielmenge. Weil A', B' disjunkt sind, ist entweder $y \in A'$, womit ein x mit $y = f_1(x)$ vorliegt, oder $y \in B'$, womit ein x mit $y = f_2(x)$ vorliegt. Zusammengefasst existiert zu jedem $y \in A' \cup B'$ ein x mit $y = f(x)$. □

Satz 3.20. Die Multiplikation $|A| \cdot |B| := |A \times B|$ ist wohldefiniert.

Beweis. Zu zeigen ist, dass $|A \times B| = |A' \times B'|$ aus $|A| = |A'|$ und $|B| = |B'|$ folgt. Nach Voraussetzung existieren Bijektionen $f_1 \colon A \to A'$ und $f_2 \colon B \to B'$. Man konstruiert mit ihnen die Bijektion

$$f \colon A \times B \to A' \times B', \quad f(a,b) := (f_1(a), f_2(b)).$$

Sie ist injektiv, denn für alle Paare $(a_1, b_1), (a_2, b_2) \in A \times B$ gilt

$$\begin{aligned} f(a_1,b_1) = f(a_2,b_2) &\iff (f_1(a_1), f_2(b_1)) = (f_1(a_2), f_2(b_2)) \\ &\iff f_1(a_1) = f_1(a_2) \wedge f_2(b_1) = f_2(b_2) \\ &\iff a_1 = a_2 \wedge b_1 = b_2 \iff (a_1,b_1) = (a_2,b_2). \end{aligned}$$

Sie ist auch surjektiv. Sei dazu $(a', b') \in A' \times B'$ beliebig. Wegen $a' \in A'$ existiert ein a mit $a' = f_1(a)$. Wegen $b' \in B'$ existiert ein b mit $b' = f_2(b)$. Laut Konstruktion liegt mit (a, b) somit ein Zeuge für $(a', b') = f(a, b)$ vor. □

Satz 3.21. Die Potenzierung $|B|^{|A|} := |B^A|$ ist wohldefiniert.

Beweis. Zu zeigen gilt, dass $\mathrm{Abb}(A, B) = \mathrm{Abb}(A', B')$ aus $|A| = |A'|$ und $|B| = |B'|$ folgt, wobei wir $\mathrm{Abb}(A, B)$ statt B^A schreiben. Nach Voraussetzung existieren Bijektionen $f_1 \colon A \to A'$ und $f_2 \colon B \to B'$. Man konstruiert mit ihnen die Bijektion

$$F \colon \mathrm{Abb}(A,B) \to \mathrm{Abb}(A',B'), \quad F(f) := f_2 \circ f \circ f_1^{-1}.$$

Sie ist injektiv, weil

$$F(f) = F(g) \iff f_2 \circ f \circ f_1^{-1} = f_2 \circ g \circ f_1^{-1} \iff f = g.$$

Die letzte Umformung gilt, weil Bijektionen ja linkskürzbar und rechtskürzbar sind.

Sie ist auch surjektiv. Dazu ist zu jedem f' ein Zeuge f für $f' = F(f)$ gesucht. Man darf $f := f_2^{-1} \circ f' \circ f_1$ setzen, denn

$$f_2^{-1} \circ f' \circ f_1 = f \iff f' \circ f_1 = f_2 \circ f \iff f' = f_2 \circ f \circ f_1^{-1} = F(f). \square$$

3.4.3 Der Satz von Cantor

Satz 3.22. Es sei X eine beliebige Menge. Ihre Potenzmenge $\mathcal{P}(X)$ ist zur Menge $\mathrm{Abb}(X, \{0,1\})$ der binärwertigen Abbildungen gleichmächtig.

Beweis. Jede Menge $A \subseteq X$ wird kodiert durch ihre Indikatorfunktion

$$1_A \colon X \to \{0,1\}, \quad 1_A(x) := [x \in A] = \begin{cases} 1, & \text{wenn } x \in A, \\ 0, & \text{wenn } x \notin A. \end{cases}$$

Sie vermitteln die kanonische Bijektion

$$\varphi \colon \mathcal{P}(X) \to \mathrm{Abb}(X, \{0,1\}), \quad \varphi(A) := 1_A.$$

Zur Injektivität. Definition 3.17 verlangt die Bestätigung von

$$\varphi(A) = \varphi(B) \Rightarrow A = B, \text{ das heißt } 1_A = 1_B \Rightarrow A = B.$$

Die linke seite enfaltet sich damit, dass zwei Abbildungen genau dann gleich sind, wenn sie in jedem ihrer Funktionswerte übereinstimmen. Die rechte Seite entfaltet sich per Extensionalität, das ist Def. 3.1. Dies führt zu

$$(\forall x \colon 1_A(x) = 1_B(x)) \Rightarrow (\forall x \colon x \in A \Leftrightarrow x \in B).$$

Die Aussage stimmt, denn man darf umformen

$$1_A(x) = 1_B(x) \iff [x \in A] = [x \in B] \iff (x \in A \Leftrightarrow x \in B).$$

Zur Surjektivität. Es ist hierfür zu prüfen, dass $\mathrm{Abb}(X, \{0,1\})$ eine Teilmenge der Bildmenge $\varphi(\mathcal{P}(X))$ ist. Entfaltung von Def. 3.5 und Def. 3.13 führt zu

$$\forall f \colon \Big(f \in \mathrm{Abb}(X, \{0,1\}) \Rightarrow \exists A \in \mathcal{P}(X) \colon f = \varphi(A) \Big).$$

Dem Existenzquantor genügt die »Einsfaser«

$$A := f^{-1}(\{1\}) = \{x \in X \mid f(x) \in \{1\}\} = \{x \in X \mid f(x) = 1\}.$$

Es gilt $f = 1_A$, denn

$$1_A(x) = [x \in A] = [x \in \{x \mid f(x) = 1\}] = [f(x) = 1] = f(x). \qquad \square$$

Eine Teilmenge wird durch ihre Indikatorfunktion charakterisiert. Stellen wir uns beispielsweise einen gedrückten Akkord als Teilmenge einer Klaviatur vor. Die Indikatorfunktion ist hier eine endliche Folge, entspricht also einem Tupel, welches genau in den gedrückten Tasten den Wert 1 besitzt. Das Tupel ist zwar nicht der Akkord selbst, kodiert aber genau die Information des Akkords.

Satz 3.23 (Satz von Cantor).
Jede Menge ist weniger mächtig als ihre Potenzmenge.

Beweis. Sei X eine Menge. Zu zeigen ist $|X| < |\mathcal{P}(X)|$. Mit $x \mapsto \{x\}$ liegt unschwer Einsichtig eine Injektion $X \to \mathcal{P}(X)$ vor, denn aus $\{x\} = \{x'\}$ folgt $x = x'$.

Die Widerlegung der Existenz einer Surjektion $f\colon X \to \mathcal{P}(X)$ klärt uns nun darüber auf, dass erst recht keine Bijektion bestehen kann. Man erreicht dies nach Cantor durch das Diagonalargument zweiter Art. Hierfür definiert man die Diagonalmenge

$$D := \{x \in X \mid x \notin f(x)\}.$$

Als Aussonderung aus X ist D eine Teilmenge von X, also ein Element von $\mathcal{P}(X)$. Weil f als surjektiv angenommen wird, muss $D \in f(X)$ sein. Das heißt, es muss ein $x \in X$ mit $D = f(x)$ vorliegen. Weil es sich dabei um eine Gleichheit zwischen Mengen handelt, ist insbesondere $x \in D$ äquivalent zu $x \in f(x)$. Laut der Definition von D ist $x \in D$ andererseits, weil $x \in X$ vorliegt, äquivalent zu $x \notin f(x)$. Summa summarum besteht die widersprüchliche Äquivalenz

$$x \in f(x) \Leftrightarrow x \notin f(x). \qquad \square$$

Hierneben gibt es auch noch die folgende speziellere Formulierung des Sachverhaltes. Es ist $\mathbb{N}$ weniger mächtig als $\{0,1\}^{\mathbb{N}}$. Angenommen, es wäre $f\colon \mathbb{N} \to \{0,1\}^{\mathbb{N}}$ eine Abzählung. Sie ordnet jeder natürlichen Zahl n eine Binärfolge

$$(f(n)_0, f(n)_1, f(n)_2, \ldots)$$

zu. Nun kann man allerdings eine weitere Binärfolge konstruieren, die sich von allen anderen unterscheidet, im Widerspruch zur Annahme, f würde alle Binärfolgen abzählen. Dies geschieht wieder per Cantors Diagonalargument zweiter Art. Man definiert dafür die Folge

$$d\colon \mathbb{N} \to \{0,1\}, \quad d_n := 1 - f(n)_n.$$

Listet man die Folgen tabellarisch auf, je Zeile eine Folge, handelt es sich bei (d_n) um die negierte Diagonale, womit sie sich von jeder Folge der Abzählung mindestens in dieser unterscheiden muss.

Zu klären verbleibt, wie die allgemeine Form des Beweises mit der speziellen zusammenhängt. Hierfür erinnern wir uns, dass zu jeder Teilmenge von $\mathbb{N}$ in natürlicher Weise genau eine Indikatorfunktion gehört, womit eine Bijektion zwischen

$\mathcal{P}(\mathbb{N})$ und $\{0,1\}^{\mathbb{N}}$ hergestellt wird. Diese Indikatorfunktionen sind nichts anderes als die Binärfolgen. Demnach konstituiert

$$D := \{n \in \mathbb{N} \mid f(n)_n = 0\}$$

die analoge Beschreibung der Diagonalmenge. Wäre f surjektiv, gäbe es ein n mit $1_D = f(n)$, womit insbesondere $1_D(n) = f(n)_n$ wäre. Demnach ist $f(n)_n = 1$ äquivalent zu $1_D(n) = 1$, was $n \in D$ heißt, also $f(n)_n = 0$. Die widersprüchliche Äquivalenz gestaltet sich nun also als

$$f(n)_n = 1 \Leftrightarrow f(n)_n = 0.$$

Die letztendliche Klärung liefert die Rechnung

$$1_D(n) = [f(n)_n = 0] = [\neg f(n)_n = 1] = 1 - [f(n)_n = 1] = 1 - f(n)_n = d_n.$$

Kurzum ist $1_D = d$. Die Folge der negierten diagonalen Bits entpuppt sich als Indikatorfunktion der Diagonalmenge.

Man kann sich so eine Binärfolge als einen Pfad eines unendlich großen Binärbaums vorstellen. Von jedem Knoten gehen zwei Zweige aus, wobei das jeweilige Bit der Binärfolge kodiert, welcher der Zweige zu beschreiten ist. Das Abzählbare stellt man sich vor wie eine unendliche Reihe von Straßenlaternen, die man alle auf einmal betrachtet. Die Potenzmenge des Abzählbaren dagegen wie die Blätter des Baums, von denen jedes in den unendlich vielen Schritten des Durchschreitens seiner kodierenden Binärfolge erreicht würde.

Ähnlich wie Hilberts Hotel hat so ein Baum die kontraintuitive Eigenschaft, dass jeder seiner Teilbäume genau so viele Blätter kodiert wie der gesamte Baum.

4 Elemente der Algebra

4.1 Gruppentheorie

4.1.1 Elementare Gesetzmäßigkeiten

Die Gruppentheorie klärt uns tiefer über das Wesen von Symmetrien auf. Ich will Gruppen zunächst axiomatisch einführen, damit wir die elementaren Begriffe später bereits parat haben. Was unter einer Symmetrie zu verstehen sei, und in welchem Bezug sie zu Gruppen stehen, möchte ich daraufhin im Fortgang erörtern. Die Begriffe sollen eigentlich mit Blick auf die Idee der Symmetrie motiviert werden. Damit die längere Diskussion die Ausarbeitung der abstrakten Regeln nicht so sehr fragmentiert, möchte ich diese Ausarbeitung allerdings vorziehen.

Definition 4.1 (Gruppe).
Sei G eine Menge und $*\colon G \times G \to \Omega$ eine Verknüpfung. Die Menge G bildet bezüglich der Verknüpfung eine Gruppe $(G, *)$, wenn die folgenden Axiome erfüllt sind:

- **(E)** Es darf $\Omega = G$ sein, d. h., die Verknüpfung führt nicht aus G heraus.
- **(A)** Das Assoziativgesetz $a * (b * c) = (a * b) * c$ gilt für alle $a, b, c \in G$.
- **(N)** Es gibt ein neutrales Element e, so dass $g * e = e * g = g$ für jedes $g \in G$ gilt.
- **(I)** Zu jedem $g \in G$ gibt es ein Element $h \in G$ mit $g * h = h * g = e$, wobei e ein neutrales Element ist. Dieses h wird inverses Element zu g genannt.

Anstelle von $g * h$ schreibt man auch kurz gh. Für das inverse Element zu g schreibt man g^{-1}. Es gibt auch Gruppen, bei denen die Verknüpfung als Addition geschrieben wird, da schreibt man $g + h$ anstelle von gh und ng anstelle von g^n für $n \in \mathbb{Z}$. Für das inverse Element $-g$ anstelle von g^{-1}.

Definition 4.2 (Abelsche Gruppe).
Zwei Elemente a, b kommutieren, wenn $a * b = b * a$ ist. Eine Gruppe G heißt

abelsch oder kommutativ, wenn alle Elemente der Gruppe kommutieren, d. h. wenn das Kommutativgesetz $\forall a, b \in G\colon a * b = b * a$ erfüllt ist.

Bei den allermeisten Verknüpfungen, die als Addition geschrieben werden, ist das Kommutativgesetz erfüllt.

Satz 4.1. Das neutrale Element einer Gruppe ist eindeutig bestimmt, d. h. es kann keine zwei unterschiedlichen neutralen Elemente geben.

Beweis. Seien e und e' zwei neutrale Elemente. Zu zeigen ist, dass dann schon $e' = e$ gilt. Nach Voraussetzung gilt $ae = a$ und $e'b = b$ für alle a, b. Setzt man $a := e'$ und $b := e$ ein, dann ergibt sich $e' = e'e = e$. □

Satz 4.2. In jeder Gruppe gilt die Linkskürzbarkeit und die Rechtskürzbarkeit. Damit ist gemeint, sowohl aus $ga = gb$ als auch aus $ag = bg$ folgt $a = b$.

Beweis. Man multipliziert die Gleichung $ga = gb$ beidseitig mit g^{-1}. Anschließende Anwendung des Assoziativgesetzes, gefolgt von $g^{-1}g = e$ zuzüglich $ea = e$ und $eb = e$ stellt die Folgerung

$$ga = gb \implies g^{-1}ga = g^{-1}gb \implies ea = eb \implies a = b$$

her. Bei $ag = bg$ verläuft der Beweis analog. □

Kürzbarkeit bedeutet, eine Multiplikation auf beiden Seiten rückgängig machen zu können. Das Rückgänig-machen-können ist wiederum die charakteristische Eigenschaft einer injektiven Abbildung. Unter diesem Aspekt gesehen bedeutet die Kürzbarkeit, dass die Links- und Rechts-Translation

$$\begin{aligned} l_g &\colon G \to G, \quad l_g(x) := gx, \\ r_g &\colon G \to G, \quad r_g(x) := xg \end{aligned}$$

injektiv sind. Wie man leicht nachrechnet, sind sie sogar bijektiv. Für die Umkehrabbildungen gilt $(l_g)^{-1} = l_{g^{-1}}$ und $(r_g)^{-1} = r_{g^{-1}}$.

Satz 4.3. Zu jedem Element ist das inverse Element eindeutig bestimmt, das heißt, es kann keine zwei unterschiedlichen inversen Elemente geben.

Beweis. Seien h und h' invers zu g. Dann gilt $gh = e$ und $gh' = e$. Daher ist $gh = gh'$. Gemäß Linkskürzbarkeit folgt daraus $h = h'$. □

Definition 4.3 (Untergruppe).
Sei $(G, *)$ eine Gruppe und $U \subseteq G$. Man nennt U Untergruppe von G, kurz $U \leq G$, wenn $(U, *)$ die Gruppenaxiome bezüglich derselben Verknüpfung $*$ erfüllt.

Satz 4.4 (Untergruppenkriterium).
Sei G eine Gruppe. Eine nichtleere Teilmenge $H \subseteq G$ ist eine Untergruppe von G, wenn mit $a, b \in H$ auch $ab \in H$ und mit $a \in H$ auch $a^{-1} \in H$ ist.

Beweis. Da H nichtleer ist, gibt es mindestens ein Element $a \in H$. Nach Voraussetzung ist dann auch $a^{-1} \in H$, und daher auch das neutrale Element $e = aa^{-1} \in H$.

Das Assoziativgesetz gilt in H, weil es in G gilt. Die Abgeschlossenheit und die Existenz der inversen Elemente stehen direkt in der Voraussetzung. Damit sind alle Axiome überprüft. □

Definition 4.4 (Homomorphismus zwischen Gruppen).
Seien $(G, *)$ und $(G', *')$ zwei Gruppen. Eine Abbildung $\varphi\colon G \to G'$ wird Homomorphismus genannt, wenn die Gleichung $\varphi(a * b) = \varphi(a) *' \varphi(b)$ für alle $a, b \in G$ erfüllt ist.

Satz 4.5. Sei $\varphi\colon G \to G'$ ein Homomorphismus. Sind $e \in G$ und $e' \in G'$ die neutralen Elemente, dann gilt $e' = \varphi(e)$. Außerdem ist $\varphi(g)^{-1} = \varphi(g^{-1})$ für jedes $g \in G$.

Beweis. Es gilt $e'\varphi(e) = \varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$. Kürzen ergibt $e' = \varphi(e)$. Daraus folgt

$$e' = \varphi(e) = \varphi(g^{-1}g) = \varphi(g^{-1})\,\varphi(g).$$

Damit bekommt man

$$\varphi(g)^{-1} = e'\varphi(g)^{-1} = \varphi(g^{-1})\,\varphi(g)\,\varphi(g)^{-1} = \varphi(g^{-1})$$ □

Satz 4.6. Sei $\varphi\colon G \to G'$ ein Homomorphismus. Die Bildmenge $\varphi(G)$ ist eine Untergruppe von G'.

Beweis. Zu prüfen sind die Voraussetzungen des Untergruppenkriteriums. Wegen $\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(G)$ und $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(G)$ sind diese erfüllt. □

Für injektive, surjektive, bijektive Homomorphismen gibt es eigene Bezeichnungen. Die injektiven nennt man Monomorphismen, die surjektiven Epimorphismen und die bijektiven Isomorphismen.

Gibt es zwischen zwei Gruppen G, G' einen Isomorphismus, dann nennt man die beiden Gruppen isomorph zueinander, man schreibt dafür $G \simeq G'$. Zwei Gruppen die isomorph zueinander sind, sind im Wesentlichen gleich. Isomorphie ist eine Äquivalenzrelation.

Monomorphismen charakterisieren die Einbettung einer Gruppe in eine andere Gruppe. Man kann Einbettungen als Verallgemeinerung der Untergruppenbeziehung sehen. Hat man nämlich einen Monomorphismus $\varphi\colon H \to G$, dann erhält man bei Einschränkung der Zielmenge auf die Bildmenge einen Isomorphismus, d. h. es gilt $H \simeq \varphi(H)$. Die Gruppen H und $\varphi(H)$ sind also im Wesentlichen gleich. Andererseits ist $\varphi(H) \leq G$ gemäß Satz 4.6.

4.1.2 Gruppenaktionen

Definition 4.5 (Linksaktion).
Eine Abbildung $\varphi\colon G \times X \to X$ heißt Gruppenlinksaktion, kurz Linksaktion, wenn für das neutrale Element $e \in G$ und alle $g, h \in G$ gilt

$$\varphi(e, x) = x, \qquad \varphi(gh, x) = \varphi(g, \varphi(h, x)).$$

Anstelle von $\varphi(g, x)$ schreibt man für gewöhnlich einfach gx, bzw. $g + x$ bei einer additiv geschriebenen Verknüpfung.

Definition 4.6 (Rechtsaktion).
Eine Abbildung $\varphi\colon X \times G \to X$ heißt Gruppenrechtsaktion, kurz Rechtsaktion, wenn für das neutrale Element $e \in G$ und alle $g, h \in G$ gilt

$$\varphi(x, e) = x, \qquad \varphi(x, gh) = \varphi(\varphi(x, g), h).$$

Bei diesen Axiomen ist für X eine beliebige Menge zugelassen. Es kann auch $X = G$ sein. Beispiele dafür haben wir bereits kennengelernt, nämlich ist die Linkstranslation (4.1.1) eine Linksaktion und die Rechtstranslation (4.1.1) eine Rechtsaktion.

Korollar 4.7. Jede Aktion $\varphi\colon G \times X \to X$ ist ein Homomorphismus $\varphi\colon G \to S(X)$ mit $\varphi(g)(x) := \varphi(g, x)$. Hierbei ist $S(X)$ die Menge der Bijektionen $X \to X$, diese bildet bezüglich Verkettung eine Gruppe.

Beweis. Für jedes x gilt

$$\varphi(gh)(x) = \varphi(gh, x) = \varphi(g, \varphi(h, x)) = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x).$$

Folglich ist $\varphi(gh) = \varphi(g) \circ \varphi(h)$. Außerdem ist $\varphi(g)$ bijektiv mit $\varphi(g)^{-1} = \varphi(g^{-1})$, denn

$$\varphi(g^{-1}) \circ \varphi(g) = \varphi(g^{-1}g) = \varphi(e) = \mathrm{id},$$
$$\varphi(g) \circ \varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = \mathrm{id}\,. \square$$

4.1.3 Symmetrie

Nach längerer Beschäftigung mit der Gruppentheorie wird man sich irgendwann fragen, was Gruppen eigentlich sind. Wie sich herausstellt sind Gruppen eng mit dem Begriff Symmetrie verbunden. Um das erklären zu können, müssen wir erst einmal herausarbeiten, was man unter Symmetrie versteht.

In der Geometrie ist eine Symmetrie eines Objektes eine Deckabbildung, das ist eine Abbildung durch die dem Objekt keine Veränderung widerfährt, in dem Sinn dass sich das alte und das neue Objekt genau überdecken. Zwar darf dabei jedem Punkt des Objektes ein Punkt an anderem Ort zugeordnet werden, jedoch verändert sich das Objekt insgesamt nicht.

Sei also $M \subseteq \mathbb{R}^2$ ein geometrisches Objekt, dargestellt als Teilmenge der Koordinatenebene. Eine Symmetrie ist dann eine Abbildung $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ mit $f(M) = M$. Liegen zwei solche Abbildungen f, g vor, dann ist

$$(g \circ f)(M) = g(f(M)) = g(M) = M,$$

also ist $g \circ f$ auch eine Symmetrie. Drehungen und Spiegelungen lassen sich auch punktweise rückgängig machen, sind also bijektiv. Dies wollen wir für alle Symmetrien fordern. Klar ist außerdem, dass die identische Abbildung id eine Deckabbildung ist, und die Verkettung von Abbildungen das Assoziativgesetz erfüllt. Die Symmetrien eines Objektes bilden demnach eine Gruppe, die *Symmetriegruppe* dieses Objektes.

Die Symmetriegruppen sind Untergruppen einer allgemeinen Gruppe, der *symmetrischen Gruppe*. Die symmetrische Gruppe ist die Menge

$$S(X) := \{f\colon X \to X \mid f \text{ ist bijektiv}\},$$

in Worten: die Mengen der bijektiven Selbstabbildungen. Eine Abbildung $f\colon X \to Y$ heißt Selbstabbildung, wenn $X = Y$ gilt. In unserem Fall ist $X = \mathbb{R}^2$.

Die Menge $S(X)$ bildet bezüglich Verkettung eine Gruppe, das ist ganz klar, weil die Verkettung das Assoziativgesetz erfüllt und $S(X)$ genau so definiert ist, dass es zu jedem Element $f \in S(X)$ auch ein Inverses bezüglich Verkettung gibt, das ist f^{-1}, die Umkehrabbildung zu f.

Sei U eine Untergruppe von $S(X)$ und $\varphi\colon U \times X \to X$ mit $\varphi(f,x) := f(x)$. Bei φ handelt es sich um eine Gruppenaktion, denn $\varphi(\mathrm{id},x) = \mathrm{id}(x) = x$ und

$$\varphi(g \circ f, x) = (g \circ f)(x) = g(f(x)) = \varphi(g, \varphi(f,x)).$$

Für eine endliche Menge X bezeichnet man die Untergruppen von $S(X)$ als Permutationsgruppen. Man kann ohne Beschränkung der Allgemeinheit $X := \{1,\dots,n\}$ und $S_n := S(X)$ setzen, das heißt eigentlich bloß, dass jedem Element von X eine Nummer gegeben wird.

4.2 Ringtheorie

4.2.1 Elementare Gesetzmäßigkeiten

Es gibt in der Mathematik Objekte wie Restklassen, Matrizen und Polynome, für die wie bei den ganzen Zahlen eine Addition und eine Multiplikation definiert ist. Die Addition und Multiplikation von zwei Matrizen ergibt z. B. wieder eine Matrix. In jedem Fall genügen die Addition und Multiplikation einem bestimmten Muster, den Ring-Axiomen. Das legt nahe, aus den Axiomen allgemeine Rechenregeln und Gesetzmäßigkeiten abzuleiten, die somit in allen Ringen gültig sind.

Wir erhalten dadurch als neues Werkzeug ein verallgemeinertes Rechnen. Das ist für uns ganz besonders wichtig, da eine enorme Anzahl von mathematischen Strukturen die Struktur eines Rings enthält. Z. B. ist jeder Körper auch ein Ring. Die rationalen, reellen und komplexen Zahlen bilden jeweils einen Körper. Allein schon dieser Umstand, dass die wichtigsten grundlegenden Zahlenbereiche einen Körper bilden, macht es sinnvoll, Ringe und Körper näher zu studieren.

Ringe sind außerdem bedeutsam als Grundlage für die Konzepterweiterungen Modul und assoziative Algebra. Diesen beiden Begriffen ist auf bestimmte Art geometrische Information eingeimpft, sie sind von großer Tragweite in der linearen Algebra. Z. B. ist jeder Vektorraum, und damit insbesondere jeder euklidische Vektorraum ein Modul. Beispiele für assoziative Algebren sind die Tensoralgebra, die äußere Algebra und die Clifford-Algebra.

Überraschend treten auch in der Analysis solche geometrisch motivierten Konzepte auf. So wurde die Analysis zur Funktionalanalysis weiterentwickelt, die auch mit Vektorräumen arbeitet. Als assoziative Algebren kommen hier die Banachalgebren hinzu.

Neben kontinuierlichen Strukturen sind für die Algebra auch diskrete Strukturen wie Restklassenringe typisch. Die Restklassenringe bilden eine Grundlage für die Zahlentheorie.

Schließlich sind Ringe auch tief in der abstrakten Algebra verwurzelt. Es scheint so, als ergäbe sich dort eine nur schwer überschaubare Fülle von Strukturen. Das mag richtig sein, allerdings bringen die mit der axiomatischen Methode gewonnenen allgemeinen Gesetzmäßigkeiten eine gewisse Ordnung.

Definition 4.7 (Ring).
Eine Struktur $(R, +, \cdot)$ heißt Ring, wenn

1. $(R, +)$ eine kommutative Gruppe ist,
2. $(R, \cdot)$ eine Halbgruppe ist,
3. die Distributivgesetze $a(b + c) = ab + ac$ und $(a + b)c = ac + bc$ für alle $a, b, c \in R$ erfüllt sind.

Es gibt hier einen Unterschied zwischen Linksdistributivgesetz und Rechtsdistributivgesetz, weil die Multiplikation nicht kommutativ sein braucht.

Definition 4.8 (Unitärer Ring).
Ein Ring $(R, +, \cdot)$ heißt unitär oder Ring mit Eins, wenn $(R, \cdot)$ ein Monoid ist.

D. h. ein unitärer Ring ist ein Ring R, in dem es ein Einselement e gibt, so dass $e \cdot a = a \cdot e = a$ für alle $a \in R$. Man kann $e = 1$ schreiben, muss aber beachten, dass damit ein abstraktes Element gemeint ist. Unter Umständen verbietet sich das auch aufgrund von Zweideutigkeit. Z. B. ist im Matrizenring das Einselement die Einheitsmatrix. Diese schreibt man E oder I und nicht 1, um sie von der dort ebenfalls vorkommenden Skalarmultiplikation mit der Zahl 1 unterscheiden zu können.

Korollar 4.8. Sei R ein Ring und $0 \in R$ das Nullelement, dann gilt $0 \cdot a = 0$ und $a \cdot 0 = 0$ für jedes $a \in R$.

Beweis. Man rechnet

$$0a = 0a + 0 = 0a + 0a - 0a = (0 + 0)a - 0a = 0a - 0a = 0.$$

Für $a \cdot 0$ ist die Rechnung analog. □

Korollar 4.9. Sei R ein Ring und $a, b \in R$, dann gilt $(-a)b = -(ab) = a(-b)$.

Beweis. Man rechnet

$$\begin{aligned}(-a)b &= (-a)b + 0 = (-a)b + ab - (ab) = ((-a) + a)b - (ab)\\ &= 0b - (ab) = 0 - (ab) = -(ab).\end{aligned}$$

Für $a(-b)$ ist die Rechnung analog. □

Korollar 4.10. Sei R ein Ring und $a, b \in R$, dann gilt $(-a)(-b) = ab$.

Beweis. Mit dem letzten Korollar und $-(-x) = x$ rechnet man

$$(-a)(-b) = -((-a)b) = -(-(ab)) = ab. \qquad \square$$

Definition 4.9 (Einheitengruppe).
Ist R ein Ring mit Eins e, dann ist die Menge der Einheiten definiert als

$$R^* := \{a \in R \mid \text{es gibt ein } b \in R \text{ mit } ab = ba = e\}.$$

Weil $(R, \cdot)$ ein Monoid ist, muss $(R^*, \cdot)$ eine Gruppe sein, denn die Forderung dass jedes Element mutiplikativ invertierbar ist, ist das letzte Axiom einer multiplikativ geschriebenen Gruppe.

Die Gruppe $\mathbb{Z}^* = \{-1, 1\}$ ist trivial. Ein recht interessantes Beispiel für eine Einheitengruppe ist die allgemeine lineare Gruppe, das ist die Gruppe der invertierbaren quadratischen Matrizen. In der linearen Algebra weiß man, eine quadratische Matrix ist genau dann invertierbar, wenn ihre Determinante nicht verschwindet, das heißt, es gilt

$$(K^{n\times n})^* = \mathrm{GL}(n, K) := \{A \in K^{n\times n} \mid \det(A) \neq 0\}.$$

Hierbei ist K ein beliebiger Körper, z. B. $K = \mathbb{R}$ oder $K = \mathbb{C}$. Es ist ja so, dass der Matrizenraum $K^{m\times n}$ kanonisch isomorph zum Vektorraum $\mathrm{Hom}(K^n, K^m)$ ist, welcher aus allen linearen Abbildungen $K^n \to K^m$ besteht. Um es in einfachen Worten auszudrücken: Multiplikation mit einer Matrix ist eine lineare Abbildung, und jede lineare Abbildung zwischen Koordinatenräumen lässt sich eindeutig als Matrix darstellen. Für $m = n$ handelt es sich um Endomorphismen. Sind diese bijektiv, spricht man von Automorphismen. Demnach ist $\mathrm{GL}(n, K)$ kanonisch isomorph zur Automorphismengruppe $\mathrm{Aut}(K^{n\times n})$. Diese Gruppe besteht aus allen Symmetrien, welche die Vektorraumstruktur respektieren. Darin enthalten sind Untergruppen von Symmetrien wie Spiegelungen und Drehungen.

5 Ein kategorieller Blick auf die Logik

5.1 Grundbegriffe

5.1.1 Kategorien

Definition 5.1 (Kategorie). Eine Kategorie ist ein Tripel $\mathbf{C} = (\mathrm{Ob}, \mathrm{Hom}, \circ)$, sofern die folgenden beiden Axiome erfüllt sind:

1. Für $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$ gilt das Assoziativgesetz $h \circ (g \circ f) = (h \circ g) \circ f$.
2. Für jedes Objekt X existiert die Identität $\mathrm{id}_X\colon X \to X$, so dass $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$ für alle Objekte A, B und $f\colon A \to B$.

Die Elemente der Klasse Ob nennt man Objekte. Die Elemente der Klasse Hom nennt man Morphismen. Die Verknüpfung $g \circ f$, sprich g nach f, nennt man Verkettung von g und f.

Die Schreibweise ist $f\colon X \to Y$ gleichbedeutend mit $f \in \mathrm{Hom}(X, Y)$, wobei $X, Y \in \mathrm{Ob}$. Mit $\mathrm{Hom}(X, Y)$ ist die Teilklasse von Hom gemeint, die alle Morphismen von X nach Y enthält. Man schreibt $\mathrm{dom}(f) = X$ und $\mathrm{cod}(f) = Y$.

Nun gut, man macht hier zunächst zwei Beobachtungen. Erstens erinnern die Axiome an die Monoid-Axiome, haben aber den Unterschied, dass die Morphismen kompatibel sein müssen. D. h. um $g \circ f$ bilden zu können, muss $\mathrm{cod}(f) = \mathrm{dom}(g)$ sein.

Zweitens erinnern die Axiome an die Regeln für die Verkettung von Abbildungen. Tatsächlich bilden die Abbildungen eine Kategorie.

Satz 5.1 (Kategorie der Mengen).
Sei Ω das Mengenuniversum und für $A, B \in \Omega$ sei $\mathrm{Hom}(A, B) := \mathrm{Abb}(A, B)$. Sei $g \circ f$ die Verkettung von Abbildungen. Dann bildet **Set** $:= (\Omega, \mathrm{Hom}, \circ)$ eine Kategorie.

Beweis. Trivial. □

Satz 5.2 (Kategorie der Gruppen).
Sei Ω die Klasse aller Gruppen und für $G, H \in \Omega$ sei $\mathrm{Hom}(G, H)$ die Klasse der Homomorphismen von G nach H. Sei $g \circ f$ die Verkettung von Homomorphismen. Dann bildet **Group** $:= (\Omega, \mathrm{Hom}, \circ)$ eine Kategorie.

Beweis. Homomorphismen sind Abbildungen, die Axiome daher wie bei der Kategorie der Mengen erfüllt. Die Verkettung zweier Homomorphismen ist ja auch ein Homomorphismus. □

Entsprechend bilden Ringe mit Ringhomomorphismen, Körper mit Körperhomomorphismen, Vektorräume mit Vektorraumhomomorphismen usw. Kategorien. Des Weiteren bilden die endlichen Mengen, Gruppen, Ringe jeweils eine Kategorie.

5.1.2 Funktoren

Nun ist es so, dass Gruppen auch Mengen und Homomorphismen auch Abbildungen sind. Die Kategorie der Gruppen ist gewissermaßen in der Kategorie der Mengen enthalten. Um das zu präzisieren, benötigen wir den Begriff des Vergissfunktors.

Definition 5.2 (Kovarianter Funktor).
Sind $\mathbf{C}, \mathbf{D}$ Kategorien, dann nennt man $F\colon \mathbf{C} \to \mathbf{D}$ einen kovarianten Funktor, wenn jedem Objekt X von $\mathbf{C}$ ein Objekt $F(X)$ von $\mathbf{D}$ zugeordnet wird und jedem Morphismus $f \in \mathrm{Hom}_{\mathbf{C}}(X, Y)$ ein ein Morphismus $F(f) \in \mathrm{Hom}_{\mathbf{D}}(F(X), F(Y))$ zugeordnet wird, so dass die folgenden beiden Verträglichkeitsaxiome erfüllt sind:

$$F(g \circ f) = F(g) \circ F(f),$$
$$F(\mathrm{id}_X) = \mathrm{id}_{F(X)}\,.$$

Definition 5.3 (Kontravarianter Funktor).
Wie beim kovarianten Funktor, mit dem Unterschied $F(g \circ f) = F(f) \circ F(g)$.

Bemerkung. Die Notation ist überladen. Nämlich ist die Zuordnung $F\colon \mathrm{Ob}(\mathbf{C}) \to \mathrm{Ob}(\mathbf{D})$ zu unterscheiden von

$$\tilde{F}\colon \mathrm{Hom}_{\mathbf{C}}(X, Y) \to \mathrm{Hom}_{\mathbf{D}}(F(X), F(Y)).$$

Das Paar $(F, \tilde{F})$ kodiert dann eigentlich den Funktor $C \to D$.

Satz 5.3 (Vergissfunktor).
Sei $F\colon$ **Group** $\to$ **Set** mit $F((G,*,e)) := G$, und jedem Gruppenhomomorphismus

$$\varphi\colon (G,*,e) \to (G',*',e')$$

sei die Abbildung $F(\varphi)\colon G \to G'$ mit $F(\varphi)(x) := \varphi(x)$ zugeordnet. Bei F handelt es sich um einen kovarianten Funktor.

Beweis. Es gilt $F(\mathrm{id})(x) = \mathrm{id}(x)$, und daher $F(\mathrm{id}) = \mathrm{id}$. Außerdem gilt

$$F(\varphi_2\circ\varphi_1)(x) = (\varphi_2\circ\varphi_1)(x) = \varphi_2(\varphi_1(x)) = F(\varphi_2)(F(\varphi_1)(x)) = (F(\varphi_2)\circ F(\varphi_1))(x),$$

und daher $F(\varphi_2 \circ \varphi_1) = F(\varphi_2) \circ F(\varphi_1)$. □

Satz 5.4. Sei $P(X) = 2^X$ die Potenzmenge von X. Dann ist wie folgt ein kovarianter Funktor gegeben:

$$P\colon \textbf{Set} \to \textbf{Set}, \quad P(X) := 2^X, \quad P(f)(M) := f(M),$$

wobei f eine beliebige Abbildung und $f(M)$ die Bildmenge von M unter f ist.

Beweis. Nach Satz 3.8 gilt

$$P(g\circ f)(M) = (g\circ f)(M) = g(f(M)) = P(g)(P(f)(M)) = (P(g)\circ P(f))(M).$$

Daher ist $P(g \circ f) = P(g) \circ P(f)$. Außerdem ist

$$P(\mathrm{id}_X)(M) = \mathrm{id}_X(M) = M = \mathrm{id}_{P(X)}(M)$$

und daher $P(\mathrm{id}_X) = \mathrm{id}_{P(X)}$. □

Zum Funktor P kommt noch ein weiterer Aspekt hinzu. Für eine Abbildung f kann man ganz pedantisch das Bild $f(x)$ von der Bildmenge $f(\{x\})$ unterscheiden. Aufgrund der Gleichung $f(\{x\}) = \{f(x)\}$ verschwimmt diese Unterscheidung aber gewissermaßen. Die Abbildungen f und $P(f)$ verhalten sich also gewissermaßen gleich. Man kann sagen, dass f auf ganz natürliche Art und Weise die Abbildung $P(f)$ zugeordnet ist. Definiert man

$$\eta(X)\colon X \to 2^X, \quad \eta(X)(x) := \{x\},$$

dann kommutiert das folgende Diagramm:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \eta(X)}\downarrow & & \downarrow{\scriptstyle \eta(Y)} \\ 2^X & \xrightarrow[P(f)]{} & 2^Y \end{array}$$

D. h. es gilt $\eta(Y) \circ f = P(f) \circ \eta(X)$. Die Zuordnung η ist eine sogenannte natürliche Transformation.

Definition 5.4 (Natürliche Transformation).
Seien **C**, **D** Kategorien und $F, G\colon \mathbf{C} \to \mathbf{D}$ Funktoren. Dann schreibt man $\eta\colon F \to G$ und nennt η natürliche Transformation, wenn die folgenden beiden Axiome erfüllt sind:

1. Jedes Objekt X von **C** bekommt einen Morphismus $\eta(X)\colon F(X) \to G(X)$.
2. Für jeden Morphismus $f\colon X \to Y$ gilt $\eta(Y) \circ F(f) = G(f) \circ \eta(X)$.

Die zweite Bedingung lässt sich übersichtlich als kommutierendes Diagramm darstellen:

$$\begin{array}{ccc} F(X) & \xrightarrow{F(f)} & F(Y) \\ {\scriptstyle \eta(X)}\downarrow & & \downarrow{\scriptstyle \eta(Y)} \\ G(X) & \xrightarrow[G(f)]{} & G(Y) \end{array}$$

Ein weiteres Beispiel ergibt sich bezüglich Äquivalenzrelationen in Erinnerung an (**??**). Eine Abbildung $f\colon M \to M'$ heiße *induzierend*, wenn

$$x \sim a \implies f(x) \sim' f(a).$$

Satz 5.5. Die Paare $(M, \sim)$, bestehend aus Menge und Äquivalenzrelation, bilden mit den induzierenden Abbildungen als Morphismen bezüglich Verkettung eine Kategorie.

Beweis. Die identische Abbildung ist offensichtlich induzierend. Hat man neben $f\colon M \to M'$ eine weitere induzierende Abbildung $g\colon M' \to M''$, dann folgt $g(y) \sim'' g(b)$ aus $y \sim' b$. Aus $x \sim a$ folgt mit $y := f(x)$ und $b := f(a)$ somit $g(f(x)) \sim'' g(f(x))$. Daher ist auch $g \circ f$ induzierend. □

Genau dann wenn f induzierend ist, existiert eine induzierte Abbildung

$$I(f)\colon M/\!\sim \longrightarrow M'/\!\sim', \text{ so dass } I(f) \circ \pi = \pi' \circ f,$$

wobei π, π' jeweils die kanonische Projektion ist.

Satz 5.6. Bei der Induktion I handelt es sich um einen kovarianten Funktor.

Beweis. Man betrachte das folgende kommutierende Diagramm:

$$\begin{array}{ccccc} M & \xrightarrow{f} & M' & \xrightarrow{g} & M'' \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi''} \\ M/{\sim} & \xrightarrow[I(f)]{} & M'/{\sim'} & \xrightarrow[I(g)]{} & M''/{\sim''} \end{array}$$

Die Induktion I besitzt die Eigenschaften

$$\begin{aligned} &I(f) \circ \pi = \pi' \circ f, \\ &I(g) \circ \pi' = \pi'' \circ g, \\ &I(g \circ f) \circ \pi = \pi'' \circ (g \circ f). \end{aligned}$$

Damit kann man nun rechnen

$$I(g \circ f) \circ \pi = \pi'' \circ g \circ f = I(g) \circ \pi' \circ f = I(g) \circ I(f) \circ \pi. \tag{5.1}$$

Infolge gilt $I(g \circ f) = I(g) \circ I(f)$, da die kanonische Projektion π eine Surjektion ist. Aus der Forderung $I(\mathrm{id}) \circ \pi = \pi \circ \mathrm{id} = \pi$ ergibt sich $I(\mathrm{id}) = \mathrm{id}$, da π surjektiv ist. □

Die Abbildung $\eta((M, \sim)) := \pi$, die jeder Menge mit Äquivalenzrelation ihre kanonische Projektion zuordnet, ist eine natürliche Transformation.

Beispiel zur Vertiefung. Ein weiteres Beispiel berührt einen Grundbegriff der linearen Algebra. Hat man einen Vektorraum Y über dem Körper K, ohne dass wir jetzt genau verstehen müssen was das bedeutet – man stelle sich $Y := \mathbb{R}$ und $K := \mathbb{R}$ vor –, dann bildet für eine beliebige Menge $X \neq \emptyset$ auch $\mathrm{Abb}(X, Y)$ einen Vektorraum über diesem Körper bezüglich den punktweisen Operationen

$$\begin{aligned} &(\lambda f)(x) := \lambda f(x), \\ &(f_1 + f_2)(x) := f_1(x) + f_2(x), \end{aligned}$$

wobei $\lambda \in K$, $x \in X$, $f, f_1, f_2 \in \mathrm{Abb}(X, Y)$. Die lineare Algebra handelt von *linearen Abbildungen*. Seien V, W Vektorräume über dem Körper K, wobei auch $V = W$ sein darf. Eine Abbildung $\varphi\colon V \to W$ heißt linear, falls

$$\begin{aligned} &\forall v_1, v_2 \in V\colon\ \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2), \\ &\forall \lambda \in K, v \in V\colon\ \varphi(\lambda v) = \lambda \varphi(v). \end{aligned}$$

Man kann zeigen dass die Vektorräume mit den linearen Abbildungen als Morphismen auch eine Kategorie bilden, aber darauf will ich an dieser Stelle nicht hinaus. Hat man nun eine feste, aber beliebige Abbildung $g\colon X' \to X$, dann ist

$$\varphi\colon \operatorname{Abb}(X,Y) \to \operatorname{Abb}(X',Y), \quad \varphi(f) := f \circ g$$

eine lineare Abbildung, man spricht auch von einem *linearen Operator*, dem *Kompositionsoperator* $C_g = \varphi$. Die Bestätigung ist nicht sonderlich schwer, man muss bloß blind die Definitionen einsetzen und dem Formalismus folgen. Es gilt

$$\begin{aligned}\varphi(\lambda f)(x) &= ((\lambda f) \circ g)(x) = (\lambda f)(g(x)) = \lambda f(g(x)) \\ &= \lambda(f \circ g)(x) = \lambda(\varphi(f))(x) = (\lambda\varphi(f))(x),\end{aligned}$$

kurz $\varphi(\lambda f) = \lambda\varphi(f)$. Und es gilt

$$\begin{aligned}\varphi(f_1 + f_2)(x) &= ((f_1 + f_2) \circ g)(x) = (f_1 + f_2)(g(x)) = f_1(g(x)) + f_2(g(x)) \\ &= (f_1 \circ g)(x) + (f_2 \circ g)(x) = \varphi(f_1)(x) + \varphi(f_2)(x) \\ &= (\varphi(f_1) + \varphi(f_2))(x),\end{aligned}$$

kurz $\varphi(f_1 + f_2) = \varphi(f_1) + \varphi(f_2)$.

Man bemerkt nun, dass diese Rechnungen lediglich auf der Eigenschaft der Operationen beruhen, punktweise zu sein. Dies soll im Folgenden präzisiert werden. Die Formulierung wollen wir allgemein für Operationen beliebiger Stelligkeit haben. Sei also $p\colon Y^n \to Y$ eine n-stellige Operation, man stelle sich dabei $Y := \mathbb{R}$ vor. Man definiert nun die punktweise Anwendung von p als

$$\eta_p\colon \operatorname{Abb}(X,Y)^n \to \operatorname{Abb}(X,Y), \quad \eta_p(f)(x) := p(f_1(x),\dots,f_n(x)),$$

wobei $f := (f_1,\dots,f_n)$ ein Tupel von Funktionen ist. Sei außerdem

$$F(\varphi)(f) := (\varphi(f_1),\dots,\varphi(f_n)).$$

Zeigen wollen wir für $\varphi(f) := f \circ g$ nun

$$\varphi(\eta_p(f))(x) = \eta_p(F(\varphi)(f))(x), \quad \text{kurz} \quad \varphi \circ \eta_p = \eta_p \circ F(\varphi).$$

Bei der Bestätigung folgt man wieder blind den Definitionen und dem Formalismus. Es gilt

$$\begin{aligned}\varphi(\eta_p(f))(x) &= \eta_p(f)(g(x)) = p(f_1(g(x)),\dots,f_n(g(x))) \\ &= p(\varphi(f_1)(x),\dots,\varphi(f_n)(x)) = \eta_p(\varphi(f_1),\dots,\varphi(f_n))(x) \\ &= \eta_p(F(\varphi)(f))(x).\end{aligned}$$

Das bedeutet, dieses Diagramm kommutiert:

$$\begin{array}{ccc} \mathrm{Abb}(X,Y)^n & \xrightarrow{F(\varphi)} & \mathrm{Abb}(X',Y)^n \\ \Big\downarrow{\scriptstyle \eta_p} & & \Big\downarrow{\scriptstyle \eta_p} \\ \mathrm{Abb}(X,Y) & \xrightarrow[\varphi]{} & \mathrm{Abb}(X',Y) \end{array}$$

Aller Voraussicht nach müsste es sich bei F um einen Funktor handeln. Dass η_p dabei die Rolle einer natürlichen Transformation einnimmt, wurde soeben gezeigt.

Satz 5.7 (Kategorie mit Kompositionsoperatoren als Morphismen).
Sei $Y \neq \emptyset$. Sei $\Omega := \{\mathrm{Abb}(X,Y) \mid X \text{ ist beliebig}\}$. Sei

$$\begin{aligned} &\mathrm{Hom}(\mathrm{Abb}(X,Y), \mathrm{Abb}(X',Y)) \\ &\quad := \{\varphi \mid \exists f \in \mathrm{Abb}(X,Y), g \in \mathrm{Abb}(X',X) \colon \varphi = f \circ g\}. \end{aligned}$$

Sei $\psi \circ \varphi$ die gewöhnliche Verkettung. Dann bildet **Komp** $:= (\Omega, \mathrm{Hom}, \circ)$ eine Kategorie.

Beweis. Zunächst müssen wir bestätigen, dass Hom bezüglich $\circ$ abgeschlossen ist. Sei $\varphi_1(f) := f \circ g_1$ und $\varphi_2(f) := f \circ g_2$ mit $\mathrm{dom}(\varphi_2) = \mathrm{cod}(\varphi_1)$, so dass man $\varphi := \varphi_2 \circ \varphi_1$ bilden kann. Gesucht ist ein g, so dass $\varphi = f \circ g$. Nun gilt

$$(\varphi_2 \circ \varphi_1)(f) = (f \circ g_1) \circ g_2 = f \circ g_1 \circ g_2 = f \circ (g_1 \circ g_2).$$

Man kann also $g := g_1 \circ g_2$ setzen. Nun verbleibt bloß noch die Existenz fester Identitäten id zu bestätigen. Man definiert dazu $\mathrm{id}(f) := f \circ \mathrm{id}$. Für $\varphi(f) := f \circ g$ gilt dann

$$\begin{aligned} &(\varphi \circ \mathrm{id})(f) = (f \circ \mathrm{id}) \circ g = f \circ g = \varphi(f), \\ &(\mathrm{id} \circ \varphi)(f) = (f \circ g) \circ \mathrm{id} = f \circ g = \varphi(f). \ \square \end{aligned}$$

Satz 5.8. Bei $F(\varphi)(f) := (\varphi(f_1), \ldots, \varphi(f_n))$ für $f = (f_1, \ldots, f_n)$ handelt es sich um einen kovarianten Funktor.

Beweis. Es gilt

$$F(\psi \circ \varphi)(f) = (\psi(\varphi(f_1)), \ldots, \psi(\varphi(f_n))) = F(\psi)(F(\varphi)(f)) = (F(\psi) \circ F(\varphi))(f),$$

kurz $F(\psi \circ \varphi) = F(\psi) \circ F(\varphi)$. Und es gilt

$$F(\mathrm{id})(f) = (\mathrm{id}(f_1), \ldots, \mathrm{id}(f_n)) = (f_1, \ldots, f_n) = f = \mathrm{id}(f),$$

kurz $F(\mathrm{id}) = \mathrm{id}$. □

Jetzt haben wir so viele Funktoren kennengelernt, dass allgemeine Regeln betreffend Funktoren gut motiviert sind. Der folgende Satz durchleuchtet die Funktoren ein wenig.

Satz 5.9. Wird ein Funktor auf einen Isomorphismus angewendet, ist das Resultat wieder ein Isomorphismus.

Beweis. Dieser ist direkt aus den Definitionen zu erhalten. Wir betrachten nur einen kovarianten Funktor F. Der Beweis für einen kontravarianten Funktor verläuft analog.

Sei $f\colon X \to Y$ ein beliebiger Isomorphismus im Definitionsbereich des Funktors. Laut Definition existert eine Inverse, das heißt, ein $g\colon Y \to X$ mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$. Gemäß der definierenden Eigenschaft eines Funktors darf man rechnen

$$\mathrm{id}_{F(X)} = F(\mathrm{id}_X) = F(g \circ f) = F(g) \circ F(f),$$
$$\mathrm{id}_{F(Y)} = F(\mathrm{id}_Y) = F(f \circ g) = F(f) \circ F(g).$$

Somit ist $F(f)$ ein Isomorphismus mit Inverse $F(g)$. □

Wird beispielsweise der Vergissfunktor von Gruppen zu Mengen auf einen Gruppenisomorphismus angewendet, ist das Resultat zwingend eine Bijektion, da die Bijektionen die Isomorphismen in der Kategorie der Mengen sind.

5.1.3 Anfangsobjekte und Endobjekte

Definition 5.5 (Anfangsobjekt, Endobjekt, Nullobjekt).
Es sei **C** eine Kategorie. Ein $A \in \mathrm{Ob}(\mathbf{C})$ heißt Anfangsobjekt, wenn es zu jedem Objekt $X \in \mathrm{Ob}(\mathbf{C})$ genau einen Morphismus $A \to X$ gibt. Ein $E \in \mathrm{Ob}(\mathbf{C})$ heißt Endobjekt, wenn es zu jedem Objekt $X \in \mathrm{Ob}(\mathbf{C})$ genau einen Morphismus $X \to E$ gibt. Ein Objekt heißt Nullobjekt, wenn es sowohl Anfangsobjekt als auch Endobjekt ist.

Mengen. Wir untersuchen zunächst die Kategorie der Mengen. Anfangsobjekt bedeutet hier eine Menge A, bei der es zu jeder Menge X genau eine Abbildung $A \to X$ gibt. Betrachten wir zunächst endliche Mengen, dann ergibt sich aufgrund von Gleichung (**??**) ja die Bedingung $|X|^{|A|} = 1$. Das geht nur, wenn $|A| = 0$ ist, und das bedeutet $A = \emptyset$. Die einzige Abbildung in $\mathrm{Abb}(\emptyset, X)$ ist die leere Abbildung, und dies bleibt auch dann richtig, wenn X gänzlich beliebig ist. Somit haben wir die leere Menge als einziges Anfangsobjekt identifiziert.

Endobjekt bedeutet eine Menge E, so dass es zu jeder Menge X genau eine Abbildung $X \to E$ gibt. Wieder beschränken wir uns zunächst auf endliche Mengen und

nutzen (??). Wir erhalten die Bedingung $|E|^{|X|} = 1$. Das geht nur, wenn $|E| = 1$ ist. Jede Menge mit einem Element ist also Endobjekt, denn allgemein gibt es dann nur eine einzige Abbildung, nämlich die konstante Abbildung. Dies bleibt auch dann richtig, wenn X gänzlich beliebig ist.

Ein Nullobjekt existiert offenbar nicht.

Benutzen wir doch $1 := \{\emptyset\}$ als kanonisches Endobjekt. Interessant ist, dass man zu einer Menge X jedes Element $x \in X$ mit der Abbildung $x\colon 1 \to X$ identifizieren kann, für die $x(\emptyset) = x$ gilt. Zu einer Abbildung $f\colon X \to Y$ können wir die Zuordnung $f(x) = y$ bzw. $(x, y) \in f$ nun in der Form $f \circ x = y$ beschreiben.

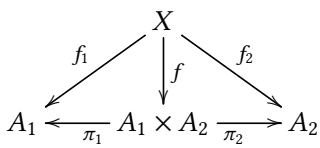
5.1.4 Produkt und Koprodukt

Ein wichtiger Begriff der Theorie ist das Produkt von Objekten. Weil es sich dabei um eine Verallgemeinerung des kartesischen Produktes von Mengen handelt, möchte ich die Zusammenhänge zunächst am vertrauten Schauplatz der Mengen betrachten.

Zu zwei Mengen A_1, A_2 können wir das Produkt $A_1 \times A_2$ bilden. Man definiert die Projektionen auf die Komponenten als

$$\pi_1\colon A_1 \times A_2 \to A_1, \quad \pi_1((x, y)) := x,$$
$$\pi_2\colon A_1 \times A_2 \to A_2, \quad \pi_2((x, y)) := y.$$

Nun betrachten wir Abbildungen $f_1\colon X \to A_1$ und $f_2\colon X \to A_2$. Zunächst sei $X := \{\emptyset\}$. Die jeweilige Abbildung pickt dann ein Element aus der jeweiligen Menge heraus, das sind $a_1 := f_1(\emptyset)$ und $a_2 := f_2(\emptyset)$. Nun ist eine Abbildung f gesucht, sodass das Diagramm



kommutiert. Die Bedingungen an f sind also $\pi_i \circ f = f_i$ für $i \in \{1, 2\}$. Damit ist aber eindeutig festgelegt, dass $f(\emptyset) = (a_1, a_2)$ sein muss, denn ein Tupel ist durch die Komponenten festgelegt, und die sind $\pi_i(f(\emptyset)) = f_i(\emptyset) = a_i$ für $i \in \{1, 2\}$. Somit ist f eindeutig bestimmt.

Die Betrachtung kann man genauso für eine allgemeine Menge X führen, weil die Argumentation dann jeweils für jedes Element von X gilt. Wieder ist f eindeutig bestimmt.

Gelegentlich wird f als $f = f_1 \times f_2$ notiert.

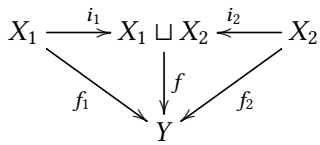
Definition 5.6 (Produkt).
Sei **C** eine Kategorie und seien Y_1, Y_2 Objekte von **C**. Ein Objekt Y von **C** mit Projektionen $\pi_1 \colon Y \to Y_1$ und $\pi_2 \colon Y \to Y_2$ heißt Produkt, wenn zu jedem Objekt X von **C** und allen Morphismen $f_1 \colon X \to Y_1$ und $f_2 \colon X \to Y_2$ genau ein Morphismus $f \colon X \to Y$ existiert, so dass $f_1 = \pi_1 \circ f$ und $f_2 = \pi_2 \circ f$.

Das kartesische Produkt $Y := Y_1 \times Y_2$ ist ein Produkt in der Kategorie der Mengen. Wir schreiben $f(x) = y$ mit $y = (y_1, y_2)$. Nun ist $\pi_1(y) = y_1$ und $\pi_2(y) = y_2$, laut Forderung soll also $y_1 = f_1(x)$ und $y_2 = f_2(x)$ sein. Dadurch ist f mit $f(x) := (f_1(x), f_2(x))$ eindeutig festgelegt.

Zu zwei Mengen können wir weiterhin die disjunkte Vereinigung $X_1 \sqcup X_2$ bilden. Wir rekapitulieren, dass zu ihr die beiden kanonischen Injektionen

$$\begin{aligned} i_1 &\colon X_1 \to X_1 \sqcup X_2, \quad & i_1(x) &:= (1, x), \\ i_2 &\colon X_2 \to X_1 \sqcup X_2, \quad & i_2(x) &:= (2, x) \end{aligned}$$

gehören. Man stellt sich nun die Frage, was das Wesensmerkmal der disjunkten Vereinigung ist. Das ist doch, dass zu jedem ihrer Elemente die Information vorliegt, ob es aus der linken oder der rechten Menge entstammt. Das heißt, es muss eine Abbildung geben, die auf den Tag projiziert. Betrachten wir dazu die Abbildungen $f_1 \colon X_1 \to Y$ und $f_2 \colon X_2 \to Y$ mit $Y := \{1, 2\}$ und $f_k(x) := k$. Mit der Abbildung f_k gelangt man von X_k also direkt zum Tag k. Nun ist eine Abbildung f gesucht, so dass das Diagramm



kommutiert. Das heißt, es soll $f \circ i_k = f_k$ für $k \in \{1, 2\}$ sein. Das macht $f((1, x)) = 1$ und $f((2, x)) = 2$. Dadurch ist f eindeutig bestimmt. Es ist die gesuchte Projektion auf den Tag.

Definition 5.7 (Koprodukt).
Sei **C** eine Kategorie und seien X_1, X_2 Objekte von **C**. Ein Objekt X von **C** mit Morphismen $i_1 \colon X_1 \to X$ und $i_2 \colon X_2 \to X$ heißt Koprodukt, wenn zu jedem Objekt Y von **C** und allen Morphismen $f_1 \colon X_1 \to Y$ und $f_2 \colon X_2 \to Y$ genau ein Morphismus $f \colon X \to Y$ existiert, so dass $f_1 = f \circ i_1$ und $f_2 = f \circ i_2$.

Die disjunkte Vereinigung $X := X_1 \sqcup X_2$ mit den Injektionen $i_1(x) := (1, x)$ und

$i_2(x) := (2, x)$ ist ein Koprodukt in der Kategorie der Mengen. Es gilt schon mal

$$f(x) = \textbf{match } x \begin{cases} (1, x) \mapsto y_1, \\ (2, x) \mapsto y_2. \end{cases}$$

Laut Forderung soll außerdem $y_1 = f_1(x)$ und $y_2 = f_2(x)$ sein, wodurch f eindeutig festgelegt ist.

5.1.5 Exponentialobjekte

Die Notation B^A stehe für die Menge der Abbildungen $A \to B$. Es soll nun die Applikation einer Abbildung auf ein Argument als eigenständige Operation

$$\varepsilon \colon B^A \times A \to B, \quad \varepsilon(f, a) := f(a)$$

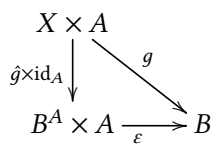
gedacht werden. Einer zweistelligen Abbildung $g \colon X \times A \to B$ lässt sich die Abbildung

$$\hat{g} \colon X \to B^A, \quad \hat{g}(x)(a) := g(x, a).$$

zuordnen. Diesen Vorgang nennen wir Currying. Man findet nun

$$g(x, a) = \hat{g}(x)(a) = \varepsilon(\hat{g}(x), a) = (\varepsilon \circ (\hat{g} \times \mathrm{id}_A))(x, a).$$

Die Gleichung $g = \varepsilon \circ (\hat{g} \times \mathrm{id}_A)$ ist also für jede Abbildung g erfüllt, was bedeutet, dass das Diagramm



kommutiert.

Definition 5.8 (Exponentialobjekt).
Sei **C** eine Kagegorie, in der das Produkt je zweier Objekte existiert. Zu zwei Objekten A, B von **C** heißt ein Objekt B^A von **C** zusammen mit einem Morphismus $\varepsilon \colon B^A \times A \to B$ Exponentialobjekt, wenn es zu jedem Objekt X von **C** und Morphismus $g \colon X \times A \to B$ genau einen Morphismus $\hat{g} \colon X \to B^A$ gibt, so dass $\varepsilon \circ (\hat{g} \times \mathrm{id}_A) = g$ gilt.

Satz 5.10. Es besteht die Isomorphie $\mathrm{Hom}_{\mathbf{C}}(X \times A, B) \cong \mathrm{Hom}_{\mathbf{C}}(X, B^A)$.

Beweis. Es sei $\lambda(g) := \hat{g}$ bezüglich Def. 5.8. Zu zeigen ist, dass es sich bei λ um einen Isomorphismus handelt. Für jedes $h\colon X \to B^A$ sei dazu

$$\lambda'(h) := \varepsilon \circ (h \times \mathrm{id}_A)\colon X \times A \to B.$$

Zu zeigen ist, dass λ' der inverse Morphismus zu λ ist. Def. 5.8 sichert nun direkt zu, dass $\lambda'(\lambda(g)) = g$ gelten muss. Zu bestätigen verbleibt $\lambda(\lambda'(h)) = h$. Die Allaussage in Def. 5.8 wird hierzu spezialisiert mit $g := \varepsilon \circ (h \times \mathrm{id}_A)$. Nun wissen wir aber nicht nur, dass $\hat{g}$ existieren muss, wir können es mit der Setzung $\hat{g} := h$ angeben, denn dieses erfüllt die Gleichung

$$\varepsilon \circ (\hat{g} \times \mathrm{id}_A) = \varepsilon \circ (h \times \mathrm{id}_A).$$

Infolge gilt

$$\lambda(\lambda'(h)) = \lambda(\varepsilon \circ (h \times \mathrm{id}_A)) = \lambda(\varepsilon \circ (\hat{g} \times \mathrm{id}_A)) = \lambda(g) = \hat{g} = h. \square$$

5.2 Kartesisch abgeschlossene Kategorien

Definition 5.9 (Kartesisch abgeschlossene Kategorie).
Eine Kategorie **C** heißt genau dann kartesisch abgeschlossen, wenn

1. sie ein Terminalobjekt enthält,
2. je zwei Objekte A, B von **C** ein Produkt $A \times B$ in **C** besitzen,
3. je zwei Objekte A, B von **C** ein Exponential B^A in **C** besitzen.

Dass die Kategorie der Mengen kartesisch abgeschlossen ist, wurde bereits während der Diskussion der drei Begrifflichkeiten nachgerechnet. Die Kategorie der endlichen Mengen ist ebenfalls kartesisch abgeschlossen. Sind A, B endlich, ist ja $A \times B$ und B^A ebenfalls eine endliche Menge.

6 Elemente der Stochastik

6.1 Grundbegriffe

6.1.1 Ereignisse

Die Wahrscheinlichkeitstheorie beschäftigt sich mit *Zufallsexperimenten*. Darunter versteht man ein Experiment mit zufälligem Ausgang, das, um der Wissenschaftlichkeit genüge zu tun, unter genau definierten Versuchsbedingungen durchgeführt wird. Der Ausgang führt immer zu einem *Ergebnis*. Alle erreichbaren Ergebnisse fasst man zur *Ergebnismenge* zusammen. Allgemeiner genügt es, wenn jedes Ergebnis in der Ergebnismenge liegt, wobei diese aber auch Elemente enthalten darf, die das Experiment niemals abwirft. Jede Teilmenge der Ergebnismenge nennt man ein *Ereignis*. Die Potenzmenge der Ergebnismenge heißt *Ereignisraum*, sie besteht aus allen denkbaren Ereignissen. Man sagt, ein Ereignis sei eingetreten, wenn das Ergebnis des Versuchs im diesem Ereignis liegt.

Zu beachten ist, dass wir dabei eine endliche oder höchstens abzählbar unendliche Ergebnismenge voraussetzen. Bei überabzählbaren Ergebnismengen kommt es zu Unwägbarkeiten, deren Klärung Gegenstand der Maßtheorie ist.

Ein schlichtes Experiment bietet der Wurf des Spielwüfels, ein mit Augenzahlen beschriftetes regelmäßiges Hexaeder. Die Ergebnismenge wird als

$$\Omega := \{1, 2, 3, 4, 5, 6\}$$

festgelegt. Betrachten wir die drei Ereignisse

$$A := \{2\}, \quad B := \{1, 2\}, \quad C := \{1, 3\}.$$

Ist $\omega = 2$ das Ergebnis des Versuchs, sind die Ereignisse A, B eingetreten. Zwei Ereignisse, die niemals gleichzeitig eintreten, heißen *disjunkt*. So sind die A, C disjunkt, weil ihre Schnittmenge leer ist.

6.1.2 Wahrscheinlichkeiten

Man kann nicht voraussagen, wie ein Experiment ausgehen wird. Das Wahrscheinlichkeitsmaß liefert dennoch ein Maß dafür, wie sicher der Eintritt eines Ereignis-

ses ist. Wahrscheinlichkeit wird tiefergründig verständlich, wenn dasselbe Zufallsexperiment abermals wiederholt wird. Wir zählen, wie häufig ein Elementarereignis eingetreten ist.

Es sei ein Versuch n mal durchgeführt worden, was zu den Ergebnissen a_i für $i = 1$ bis $i = n$ geführt hat. Wir definieren die *relative Häufigkeit* des Ereignisses A als die Zahl

$$r_{n,a}(A) := \frac{1}{n}|\{i \in \{1, \dots, n\} \mid a_i \in A\}|.$$

Relative Häufigkeiten bieten bei hinreichend großem n eine Näherung für die Wahrscheinlichkeit. Zur Vermessung eines Würfels wird man diesen also möglichst oft werfen wollen. Man erhält so die relativen Häufigkeiten der Elementarereignisse, und damit näherungsweise auch ihre Wahrscheinlichkeiten. So lässt sich feststellen, ob ein Würfel gezinkt wurde.

Fassen wir a als Funktion $i \mapsto a_i$ auf, können wir schreiben

$$\{i \mid a_i \in A\} = \{i \mid i \in a^{-1}(A)\} = a^{-1}(A).$$

Für disjunkte Ereignisse A, B erhält man nun

$$\begin{aligned} r_{n,a}(A \cup B) &= \tfrac{1}{n}|a^{-1}(A \cup B)| = \tfrac{1}{n}|a^{-1}(A) \cup a^{-1}(B)| \\ &= \tfrac{1}{n}|a^{-1}(A)| + \tfrac{1}{n}|a^{-1}(B)| = r_{n,a}(A) + r_{n,a}(B). \end{aligned}$$

6.1.3 Zufallsgrößen

Eine *Zufallsgröße* darf man sich als eine Funktion $X\colon \Omega \to \Omega'$ vorstellen, die eine kausale Verbindung zwischen den Ergebnismengen Ω, Ω' schafft. Ein Ergebnis $\omega \in \Omega$ führt zu $X(\omega)$. Ursächlich für ein $x \in \Omega'$ sind daher all die ω mit $x = X(\omega)$. Das heißt, ursächlich für das Elementarereignis $\{x\}$ ist dessen Urbild $X^{-1}(\{x\})$. Infolge muss die Wahrscheinlichkeit von $\{x\}$ die es Urbildes sein. Insofern definiert man auf Ω' das Wahrscheinlichkeitsmaß

$$P_X\colon \mathcal{P}(\Omega') \to [0, 1], \quad P_X(A) := P(X^{-1}(A)).$$

Man nennt P_X die *Verteilung* von X. Mit der identischen Zufallsgröße

$$\mathrm{id}\colon \Omega \to \Omega, \quad \mathrm{id}(\omega) := \omega$$

versteht sich auch das ursprüngliche Maß P als die Verteilung $P = P_{\mathrm{id}}$.

Geläufig sind die Schreibweisen

$$P(X = x) := P(X^{-1}(\{x\})), \qquad \{X = x\} := X^{-1}(\{x\}),$$
$$P(X \in A) := P(X^{-1}(A)), \qquad \{X \in A\} := X^{-1}(A).$$

Es ist $\{X = x\}$ dasselbe wie $\{X \in \{x\}\}$. Ist P die Gleichverteilung auf Ω, ergibt sich

$$P(X \in A) = \frac{|\{X \in A\}|}{|\Omega|}.$$

Standardbeispiel. Wir werfen zwei Spielwürfel. Die Ergebnismenge sei

$$\Omega := \{1, \ldots, 6\} \times \{1, \ldots, 6\},$$

und jedes der 36 elementaren Ereignisse sei gleich wahrscheinlich, habe also die Wahrscheinlichkeit $\frac{1}{36}$. Es bezeichne ω_1 das Ergebnis des ersten, und ω_2 das des zweiten Wurfs. Wir betrachten die Zufallsgröße

$$X \colon \Omega \to \{2, \ldots, 12\}, \quad X(\omega_1, \omega_2) := \omega_1 + \omega_2.$$

Gesucht sei $P(X = 4)$. Man ermittelt

$$\{X = 4\} = \{(1, 3), (2, 2), (3, 1)\}, \quad \text{ergo } P(X = 4) = \tfrac{3}{36}.$$

Allgemein zerfällt ein Ereignis A ja in seine disjunkten Elementarereignisse $\{x\}$, so dass $A = \bigcup_{x \in A} \{x\}$ gilt. Weil nun die Fasern $X^{-1}(\{x\})$ ebenfalls disjunkt sind, muss $P(X \in A)$ die Summe der $P(X = x)$ mit $x \in A$ sein. Das heißt, man rechnet

$$P(X \in A) = P(X^{-1}(\bigcup_{x \in A} \{x\})) = P(\bigcup_{x \in A} X^{-1}(\{x\})) = \sum_{x \in A} P(X = x).$$

Die Verteilung P_X ist demzufolge bereits eindeutig bestimmt, sobald $P(X = x)$ für jedes $x \in \Omega'$ vorliegt. Dies motiviert uns, die Funktion

$$p_X \colon \Omega \to [0, 1], \quad p_X(x) := P(X = x)$$

zu definieren, genannt die *Wahrscheinlichkeitsfunktion* der Zufallsgröße X.

6.2 Mehrstufige Experimente

6.2.1 Bedingte Wahrscheinlichkeiten

Es findet ein zweistufiges Experiment statt, welches sich sich aus einem ersten und einem zweiten Wurf eines Spielwürfels zusammensetzt. Bei jedem der Würfe bestehe eine Gleichverteilung. Zur Frage steht, wie wahrscheinlich das Ereignis $\{(6,6)\}$ ist. Ein Paar (ω_1, ω_2) fasse hierbei das Ergebnis ω_1 des ersten und ω_2 des zweiten Wurfs zusammen.

Die Wahrscheinlichkeit der ersten Sechs beträgt $\frac{1}{6}$, die der zweiten ebenfalls $\frac{1}{6}$. Sie multiplizieren sich zu zu $\frac{1}{36}$, richtig?

Es wäre doch möglich, dass zwischen den beiden Würfen eine, sagen wir, geisterhafte Beziehung besteht, dergestalt dass der zweite Wurf niemals in einer Sechs resultiert, sofern das Ergebnis des ersten eine war. Trotzdem sind die Wahrscheinlichkeiten bei jedem der Würfe für sich allein gesehen gleichverteilt. Dafür muss man nicht unbedingt die Wirklichkeit manipulieren. Das Phänomen ist bereits bei der Erzeugung von Zufallszahlen im Computer beobachtbar. War die erste Zufallszahl eine Sechs, braucht der Generator die zweite lediglich solange zu verwerfen, wie sie eine Sechs sein sollte. Umstände dieser Art stellen nicht nur ein Gedankenspiel dar, so dass wir uns notgedrungen mit ihnen auseinandersetzen müssen. Sie führen zum Begriff der *bedingten Wahrscheinlichkeit*.

Bisher wurde immer nur die Verteilung der Wahrscheinlichkeiten eines Würfels für sich allein betrachtet. Das war modelliert durch die Größe

$$X_0 \colon \Omega \to \Omega, \quad X_0(\omega) := \omega, \quad \Omega := \{1, \dots, 6\},$$

mit der Gleichverteilung P_0, so dass $P_0(X = 6) = \frac{1}{6}$.

Wir modellieren das zweistufige Experiment durch die Zufallsgröße

$$X \colon \Omega^2 \to \Omega^2, \quad X(\omega) := (X_1, X_2)(\omega) = (X_1(\omega), X_2(\omega)),$$

die sich mit $\omega = (\omega_1, \omega_2)$ aus den zwei Zufallsgrößen

$$\begin{aligned} X_1 &\colon \Omega^2 \to \Omega, \quad X_1(\omega_1, \omega_2) := \omega_1, \\ X_2 &\colon \Omega^2 \to \Omega, \quad X_2(\omega_1, \omega_2) := \omega_2 \end{aligned}$$

zusammensetzt. Es stellt $X_1(\omega)$ das Ergebnis des ersten und $X_2(\omega)$ das des zweiten Wurfs dar. Wie gewünscht gilt

$$(X_1(\omega), X_2(\omega)) = (X_0(\omega_1), X_0(\omega_2)) = (\omega_1, \omega_2).$$

Es bezeichne P die Verteilung auf Ω^2. Wir wissen hier allerdings lediglich

$$P(X_1 = \omega_1) = P_0(X_0 = \omega_1) = \tfrac{1}{6},$$
$$P(X_2 = \omega_2) = P_0(X_0 = \omega_2) = \tfrac{1}{6}.$$

Die Fehlannahme besteht nun darin, dass per se

$$P(\{X_1 = \omega_1\} \cap \{X_2 = \omega_2\}) = P(X_1 = \omega_1)P(X_2 = \omega_2)$$

gelten müsse. Ist diese Gleichung erfüllt, nennt man die Zufallsgrößen X_1, X_2 *unabhängig*. In der bisherigen Sichtweise, wo wir nur X_0 mit P_0 gesehen haben, war es uns nicht möglich, stochastische Abhängigkeit zu beschreiben. Man notiert allgemein

$$P(X = x, Y = y) := P(\{X = x\} \cap \{X = y\}) = P(X = x)P(Y = y \mid X = x).$$

Der letzte Faktor bezeichne hierbei die bedingte Wahrscheinlichkeit für das Ereignis $\{Y = y\}$, unter der Bedingung, dass $\{X = x\}$ bereits eingetreten ist.

Definition 6.1 (Bedingte Wahrscheinlichkeit).
Die bedingte Wahrscheinlichkeit für den Eintritt von A unter der Bedingung B ist für $P(B) \neq 0$ definiert gemäß

$$P(A \mid B) := \frac{P(A \cap B)}{P(B)}.$$

Wir setzen speziell $B := \{X = x\}$ und $A := \{Y = y\}$ ein, das macht

$$P(Y = y \mid X = x) = \frac{P(X = x, Y = y)}{P(X = x)}.$$

Sind X, Y unabhängig, gilt also

$$P(Y = y \mid X = x) = P(Y = y).$$

Mit der geisterhaften Beziehung zwischen den Würfeln wäre allerdings

$$0 = P(X_2 = 6 \mid X_1 = 6) \neq P(X_1 = 6) = \tfrac{1}{6}.$$

Literaturverzeichnis

[1] Gerhard Gentzen: *Untersuchungen über das logische Schließen.* In: *Mathematische Zeitschrift.* Band 39, 1935, S. 176–210, S. 405–431.

[2] Gerhard Gentzen: *Die Widerspruchsfreiheit der reinen Zahlentheorie.* In: *Mathematische Annalen.* Band 112, 1936, S. 493–565.

[3] Gerhard Gentzen: *Die gegenwärtige Lage in der mathematischen Grundlagenforschung. Neue Fassung des Widerspruchsfreiheitsbeweises für die reine Zahlentheorie.* In: *Forschungen zur Logik und zur Grundlegung der exakten Wissenschaften.* Heft 4, S. Hirzel, Leipzig 1938.

[4] Eckart Menzler-Trott: *Gentzens Problem. Mathematische Logik im nationalsozialistischen Deutschland.* Birkhäuser, Basel 2001.

[5] Ingebrigt Johansson: *Der Minimalkalkül, ein reduzierter intuitionistischer Formalismus.* In: *Compositio Mathematica.* Band 4, 1937, S. 119–136.

[6] Hannes Diener, Maarten McKubre-Jordens: *Classifying Material Implications over Minimal Logic.* In: *Archive for Mathematical Logic.* Band 59, 2020, S. 905–924. doi:10.1007/s00153-020-00722-x.

[7] Jan von Plato: *Gentzen's Logic.* In: *Handbook of The History of Logic.* Band 5, North-Holland, 2009.

[8] Francis Jeffry Pelletier, Allen P. Hazen: *A History of Natural Deduction.* In: *Handbook of The History of Logic.* Band 11, North-Holland, 2012.

[9] Francis Jeffry Pelletier, Allen Hazen: *Natural Deduction Systems in Logic.* In: *The Stanford Encyclopedia of Philosophy.*

[10] Andrzej Indrzejczak: *Natural Deduction.* In: *The Internet Encyclopedia of Philosophy.*

[11] Samuel Mimram: *Program = Proof.* Laboratoire d'Informatique de l'Ecole polytechnique, Palaiseau 2020.

[12] Dirk W. Hoffmann: *Grenzen der Mathematik*. Springer, Berlin 2011.

[13] Open Logic Project: *The Open Logic Text*. Complete Build, Oktober 2022.

[14] Jeremy Avigad: *Mathematical Logic and Computation*.
Cambridge University Press, 2023.

[15] Georg Cantor: *Beiträge zur Begründung der transfiniten Mengenlehre*.
In: *Mathematische Annalen*. Band 46, 1895, S. 481.

[16] Abraham Adolf Fraenkel: *Einleitung in die Mengenlehre*.
Springer, Berlin 1919, 3. Auflage 1928.

[17] Oliver Deiser: *Einführung in die Mengenlehre*. Springer, 2002, 3. Auflage 2010.

[18] Thomas Jech: *Set Theory: The Third Millennium Edition, revised and expanded*.
Springer, 2002.

[19] Tobias Glosauer: *Elementar(st)e Gruppentheorie*. Springer, 2016.

[20] Norbert Henze: *Stochastik für Einsteiger*. Springer, 1997, 12. Auflage 2018.

Index