Grundlagen der Mathematik

Februar 2020

Inhaltsverzeichnis

1 Repititorium

1.1 Gleichungen

1.1.1 Begriff der Gleichung

Bei einer Gleichung verhält es sich wie bei einer Balkenwaage. Liegt in einer der Waagschalen eine Masse von 2g und in der anderen Waagschale zwei Massen von jeweils 1g, dann bleibt die Waage im Gleichgewicht. Als Gleichung gilt

$$2 = 1 + 1.$$

Eine Gleichung kann wahr oder falsch sein, z. B. ist $2 = 2$ wahr, während $2 = 3$ falsch ist. Das bedeutet aber nicht, dass man eine falsche Gleichung nicht aufschreiben dürfe. Vielmehr ist eine Gleichung ein mathematisches Objekt, dem sich ein Wahrheitswert zuordnen lässt. Zumindest sollte man eine falsche Gleichung nicht ohne zusätzliche Erklärung aufschreiben, so dass der Eindruck entstünde, sie könnte wahr sein.

1.1.2 Äquivalenzumformungen

Fügt man zu beiden Schalen einer Balkenwaage das gleiche Gewicht hinzu, dann bleibt die Waage so wie sie vorher war. War sie im Gleichgewicht, bleibt sie dabei. War sie im Ungleichgewicht, bleibt sie auch dabei. Ebenso verhält es sich mit einer Gleichung. Addition der gleichen Zahl auf beide Seiten einer Gleichung bewirkt keine Veränderung des Aussagengehalts der Gleichung.

Diese Überlegung gilt natürlich auf für die Subtraktion einer Zahl auf beiden Seiten, welche dem Entfernen des gleichen Gewichtes von beiden Waagschalen entspricht.

Satz 1.1. Äquivalenzumformungen.
Seien a, b, c beliebige Zahlen. Dann gilt

$$a = b \iff a + c = b + c,$$
$$a = b \iff a - c = b - c.$$

Auch eine Verdopplung des Gewichtes in beiden Schalen der Balkenwaage ändert nicht ihr Gleichgewicht oder Ungleichgewicht.

Satz 1.2. Äquivalenzumformungen.
Seien a, b beliebige Zahlen und $n \in \mathbb{Z}$ mit $n \neq 0$. Dann gilt

$$a = b \iff na = nb.$$

Beweis. Gemäß Satz 1.1 gilt

$$\begin{aligned} na = nb &\iff 0 = na - nb = n(a-b) \iff n = 0 \vee a - b = 0 \\ &\iff a - b = 0 \iff a = b. \end{aligned}$$

Dabei wurde ausgenutzt, dass ein Produkt nur null sein kann, wenn einer der Faktoren null ist. Gemäß Voraussetzung $n \neq 0$ muss dann aber $a - b = 0$ sein. □

Satz 1.3. Äquivalenzumformungen.
Seien a, b beliebige Zahlen und $r \in \mathbb{Q}$ mit $r \neq 0$. Dann gilt

$$a = b \iff ra = rb \iff a/r = b/r.$$

Beweis. Die Zahl r ist von der Form $r = m/n$, wobei $m, n \in \mathbb{Z}$ und $m, n \neq 0$. Daher gilt

$$\begin{aligned} ra = rb &\iff \frac{m}{n}a = \frac{m}{n}b \overset{\text{Satz 1.2}}{\iff} n \cdot \frac{m}{n}a = n \cdot \frac{m}{n}b \\ &\iff ma = mb \overset{\text{Satz 1.2}}{\iff} a = b. \end{aligned}$$

Daraufhin gilt auch

$$\frac{a}{r} = \frac{b}{r} \iff r \cdot \frac{a}{r} = r \cdot \frac{b}{r} \iff a = b. \quad \square$$

Satz 1.4. Äquivalenzumformungen.
Seien $a, b, r \in \mathbb{R}$ und sei $r \neq 0$. Dann gilt

$$a = b \iff ra = rb \iff a/r = b/r.$$

Beweis. Man rechnet wieder

$$\begin{aligned} ra = rb &\iff ra - rb = 0 \iff (a-b)r = 0 \iff r = 0 \vee a - b = 0 \\ &\iff a - b = 0 \iff a = b. \end{aligned}$$

Es wurde wieder ausgenutzt, dass ein Produkt nur dann null sein kann, wenn einer der Faktoren null ist. Daraufhin gilt auch

$$\frac{a}{r} = \frac{b}{r} \iff r \cdot \frac{a}{r} = r \cdot \frac{b}{r} \iff a = b. \quad \square$$

1.2 Ungleichungen

1.2.1 Begriff der Ungleichung

Man stelle sich zwei Körbe vor, in die Äpfel gelegt werden. In den rechten Korb werden zwei Äpfel gelegt, in den linken drei. Dann befinden sich im rechten Korb weniger Äpfel als im linken. Man sagt, zwei ist kleiner als drei, kurz $2 < 3$. Man spricht von einer *Ungleichung*, in Anbetracht dessen, dass die beiden Körbe nicht die gleiche Anzahl von Äpfeln enthalten.

Der Aussagengehalt einer Ungleichung kann wahr oder falsch sein. Die Ungleichung $2 < 3$ ist wahr, die Ungleichungen $3 < 3$ und $4 < 3$ sind falsch.

Definition 1.1. Ungleichungsrelation.
Die Notation $a < b$ bedeutet »Die Zahl a ist kleiner als die Zahl b«. Die Notation $a \leq b$ bedeutet »Die Zahl a ist kleiner als oder gleich der Zahl b«. Die Notation $b > a$ ist eine andere Schreibweise für $a < b$ und bedeutet »Die Zahl b ist größer als die Zahl a«. Die Notation $b \geq a$ ist eine andere Schreibweise für $a \leq b$ und bedeutet »Die Zahl b ist größer oder gleich der Zahl a«.

1.2.2 Äquivalenzumformungen

Wir stellen uns wieder einen linken Korb mit zwei Äpfeln und einen rechten Korb mit drei Äpfeln vor. Legt man nun in beide Körbe jeweils zusätzlich 10 Äpfel hinein, dann befinden sich im linken Korb 12 Äpfel und im rechten 13. Der linke Korb enthält also immer noch weniger Äpfel als im rechten.

Befindet sich eine Balkenwaage im Ungleichgewicht, und legt man in beide Waagschalen zusätzlich die gleiche Masse von Gewichten, dann wird sich das Ungleichgewicht der Balkenwaage nicht verändern.

Für die Herausnahme von Äpfeln oder Gewichten ist diese Argumentation analog. Ist stattdessen eine falsche Ungleichung gegeben, dann lässt sich durch Addition derselben Zahl auf beiden Seiten daraus keine wahre Ungleichung gewinnen. Die analoge Argumentation gilt für die Subtraktion derselben Zahl. Anstelle von ganzen Äpfeln kann man natürlich auch Apfelhälften hinzufügen, oder allgemein Apfelbruchteile. Die Argumentation gilt unverändert.

Wir halten fest.

Satz 1.5. Äquivalenzumformungen von Ungleichungen.
Seien a, b, c beliebige Zahlen. Dann sind die folgenden Äquivalenzen gültig:

$$a < b \iff a + c < b + c, \tag{1.1}$$
$$a < b \iff a - c < b - c, \tag{1.2}$$
$$a \leq b \iff a + c \leq b + c, \tag{1.3}$$
$$a \leq b \iff a - c \leq b - c. \tag{1.4}$$

In Worten: Wenn auf beiden Seiten einer Ungleichung die gleiche Zahl addiert oder subtrahiert wird, dann ändert sich der Aussagengehalt dieser Ungleichung nicht.

Gibt es noch andere Äquivalenzumformungen?

Im linken Korb seien wieder zwei Äpfel, im rechten drei. Verdoppelt man nun die Anzahl in beiden Körben, dann sind linken vier Äpfel, im rechten sechs. Verzehnfacht man die Anzahl, dann sind im linken 20 Äpfel, im rechten 30. Offenbar verändert sich der Aussagengehalt nicht, wenn die Anzahl auf beiden Seiten der Ungleichung mit der gleichen natürlichen Zahl n multipliziert wird.

Jedoch muss $n = 0$ ausgeschlossen werden. Wenn $a < b$ ist, und man multipliziert auf beiden Seiten mit null, dann ergibt sich $0 < 0$, was falsch ist. Aus der wahren Ungleichung wurde damit eine falsche gemacht, also kann es sich nicht um eine Äquivalenzumformung handeln.

Auch bei der Ungleichung $a \leq b$ muss $n = 0$ ausgeschlossen werden. Warum muss man das tun? Die Ungleichung $0 \leq 0$ ist doch auch wahr?

Nun, wenn der Aussagengehalt von $a \leq b$ falsch ist, z. B. $4 \leq 3$, und man multipliziert auf beiden Seiten mit null, dann ergibt sich $0 \leq 0$, also eine wahre Ungleichung. Aus einer falschen wurde damit eine wahre gemacht. Bei einer Äquivalenzumformung ist dies ebenfalls verboten.

Satz 1.6. Äquivalenzumformungen von Ungleichungen.
Seien a, b beliebige Zahlen und sei $n > 0$ eine natürliche Zahl. Dann sind die folgenden Äquivalenzen gültig:

$$a < b \iff na < nb, \tag{1.5}$$
$$a \leq b \iff na \leq nb. \tag{1.6}$$

Beweis. Aus der Ungleichung $a < b$ erhält man mittels (1.2) die äquivalente Ungleichung $0 < b - a$, indem auf beiden Seiten a subtrahiert wird. Die Zahl $b - a$ ist also positiv. Durch Multiplikation mit einer positiven Zahl lässt sich das Vorzeichen einer Zahl aber nicht umkehren. Demnach ist $0 < n(b - a)$ genau dann, wenn $0 < b - a$ war. Ausmultiplizieren liefert nun $0 < nb - na$ und Anwendung von (1.1) bringt dann $na < nb$.

In Kürze formuliert:

$$a < b \iff 0 < b - a \iff 0 < n(b - a) = nb - na \iff na < nb. \tag{1.7}$$

Für $a \leq b$ gilt diese Überlegung analog. □

Alternativer Beweis. Mittels (1.1) ergibt sich zunächst:

$$a < b \iff \begin{Bmatrix} a + a < b + a \\ a + b < b + b \end{Bmatrix} \iff 2a < a + b < 2b. \tag{1.8}$$

Unter nochmaliger Anwendung von (1.1) ergibt sich nun

$$a < b \iff \begin{Bmatrix} 2a < a + b \iff 3a < 2a + b \\ 2a < 2b \iff 2a + b < 3b \end{Bmatrix} 3a < 2a + b < 3b \tag{1.9}$$

Dieses Muster lässt sich induktiv alle natürlichen Zahlen hochschieben: Aus $na < (n-1)a+b < nb$ sollte sich $(n+1)a < na+b < (n+1)b$ schlussfolgern lassen und umgekehrt. Das ist richtig, denn Addition von a gemäß (1.1) bringt

$$na < (n - 1)a + b \iff (n + 1)a < na + b \tag{1.10}$$

und Addition von b gemäß (1.1) bringt

$$na < nb \iff na + b < (n+1)b. \tag{1.11}$$

Zusammen ergibt sich daraus der behauptete Induktionsschritt. Daraus erhält man $a < b \iff na < nb$. Für $a \leq b$ sind diese Überlegungen analog. □

Wir können sogleich einen Schritt weiter gehen.

Satz 1.7. Äquivalenzumformungen von Ungleichungen.
Seien a, b beliebige Zahlen und sei $r > 0$ eine rationale Zahl, dann gelten die folgenden Äquivalenzen:

$$a < b \iff ra < rb \iff a/r < b/r, \tag{1.12}$$
$$a \leq b \iff ra \leq rb \iff a/r \leq b/r. \tag{1.13}$$

Beweis. Eine rationale Zahl $r > 0$ lässt sich immer Zerlegen in einen Quotienten $r = m/n$, wobei m, n positive natürliche Zahlen sind. Gemäß (1.5) gilt

$$\frac{m}{n} \cdot a < \frac{m}{n} \cdot b \iff n \cdot \frac{m}{n} \cdot a < n \cdot \frac{m}{n} \cdot b \iff ma < mb. \tag{1.14}$$

Gemäß (1.5) gilt aber auch

$$a < b \iff ma < mb. \tag{1.15}$$

Die Zusammenfassung beider Äquivalenzen ergibt

$$a < b \iff \frac{m}{n} \cdot a < \frac{m}{n} \cdot b \iff ra < rb. \tag{1.16}$$

Für $a \leq b$ ist die Argumentation analog. Da die Division durch eine rationale Zahl r die Multiplikation mit ihrem Kehrwert $1/r$ ist, sind auch die Äquivalenzen für die Division gültig. □

Da sich eine reelle Zahl beliebig gut durch eine rationale annähern lässt, müsste auch der folgende Satz gültig sein.

Satz 1.8. Äquivalenzumformungen von Ungleichungen.
Seien a, b beliebige Zahlen und sei $r > 0$ eine reelle Zahl, dann gelten die folgenden Äquivalenzen:

$$a < b \iff ra < rb \iff a/r < b/r, \tag{1.17}$$
$$a \leq b \iff ra \leq rb \iff a/r \leq b/r. \tag{1.18}$$

Der Satz wird sich als richtig erweisen, der Beweis kann in Analysis-Lehrbüchern nachgeschlagen werden.

Aus den Äquivalenzumformungen lassen sich nun noch einige Folgerungen gewinnen. Hat man zwei unausgeglichene Balkenwaagen, sind die beiden leichteren Inhalte zusammen offenbar leichter als die beiden schwereren Inhalte zusammen.

Korollar 1.9. Addition von Ungleichungen.
Für beliebige Zahlen a_1, a_2, b_1, b_2 gilt:

$$a_1 < b_1 \land a_2 < b_2 \implies a_1 + a_2 < b_1 + b_2, \tag{1.19}$$
$$a_1 \leq b_1 \land a_2 \leq b_2 \implies a_1 + a_2 \leq b_1 + b_2. \tag{1.20}$$

Beweis. Nach (1.1) folgt aus der ersten Prämisse $a_1 + a_2 < b_1 + a_2$, und aus der zweiten $b_1 + a_2 < b_1 + b_2$. Aufgrund der Transitivität ist daher $a_1 + a_2 < b_1 + b_2$. Für $\leq$ ist der Beweis analog. □

1.2.3 Lineare Ungleichungen

Interessant werden Ungleichungen nun, wenn in ihnen einen Variable vorkommt. Beispielsweise sei die Ungleichung $x + 2 < 4$ gegeben. Wird in diese Ungleichung für die Variable x eine Zahl eingesetzt, dann kann wird die Ungleichung entweder wahr oder falsch sein. Für $x := 1$ ergibt sich die wahre Ungleichung $1 + 2 < 4$. Für $x := 2$ ergibt sich jedoch die falsche Ungleichung $2 + 2 < 4$.

Wir interessieren uns nun natürlich für die Menge aller Lösungen dieser Ungleichung. Das sind die Zahlen, welche die Ungleichung erfüllen, wenn sie für x eingesetzt werden. Gesucht ist also die Lösungsmenge

$$L = \{x \mid x + 2 < 4\},$$

d. h. die Menge der x, welche die Ungleichung $x + 2 < 4$ erfüllen.

Gemäß Äquivalenzumformung (1.2) kommt man aber sofort zu

$$x + 2 < 4 \iff x + 2 - 2 < 4 - 2 \iff x < 2.$$

Demnach kann die Lösungsmenge als $L = \{x \mid x < 2\}$ angegeben werden, denn Äquivalenzumformungen lassen die Lösungsmenge einer Ungleichung unverändert.

Die Ungleichung $x + 2 < 4$ ist sicherlich von so einfacher Gestalt, dass man diese auch gedanklich lösen kann, ohne Äquivalenzumformungen bemühen zu müssen. Bei komplizierteren Ungleichungen kommen wir dabei aber mehr oder weniger schnell an unsere mentalen Grenzen.

Schon ein wenig schwieriger ist bspw.

$$\begin{aligned} & 5x + 2 < 3x + 10 && \mid -2 \\ \iff & 5x < 3x + 8 && \mid -3x \\ \iff & 2x < 8 && \mid /2 \\ \iff & x < 4. \end{aligned}$$

1.2.4 Monotone Funktionen

Definition 1.2. Streng monoton steigende Funktion.
Eine Funktion $f : G \to \mathbb{R}$ heißt streng monoton steigend, wenn

$$a < b \implies f(a) < f(b)$$

für alle Zahlen $a, b \in G$ erfüllt ist.

Streng monotone Abbildungen sind von besonderer Bedeutung, weil sie gemäß ihrer Definition auch Äquivalenzumformungen sind:

Satz 1.10. Allgemeine Äquivalenzumformung.
Eine streng monoton steigende Funktionen f ist umkehrbar eindeutig. Die Umkehrfunktion ist auch streng monoton steigend. D. h.

$$a < b \iff f(a) < f(b).$$

Demnach ist die Anwendung einer streng monoton steigenden Funktion eine Äquivalenzumformung.

Beweis. Zu zeigen ist $a \neq b \implies f(a) \neq f(b)$. Wenn aber $a \neq b$ ist, dann ist entweder $a < b$ und daher nach Voraussetzung $f(a) < f(b)$ oder $b < a$ und daher nach Voraussetzung $f(b) < f(a)$. In beiden Fällen ist $f(a) \neq f(b)$.

Seien nun y_1, y_2 zwei Bilder der streng monotonen Funktion f. Zu zeigen ist $y_1 < y_2 \implies f^{-1}(y_1) < f^{-1}(y_2)$. Stattdessen kann auch die Kontraposition $f^{-1}(y_2) \leq f^{-1}(y_1) \implies y_2 \leq y_1$ gezeigt werden. Das lässt sich nun aus der strengen Monotonie von f schließen:

$$f^{-1}(y_2) \leq f^{-1}(y_1) \implies \underbrace{f(f^{-1}(y_2))}_{=y_2} \leq \underbrace{f(f^{-1}(y_1))}_{=y_1}. \quad \square \tag{1.21}$$

Definition 1.3. Streng monoton fallende Funktion.
Eine Funktion $f : G \to \mathbb{R}$ heißt streng monoton fallend, wenn

$$a < b \implies f(a) > f(b)$$

für alle Zahlen $a, b \in G$ erfüllt ist.

Ein entsprechender Satz gilt auch für diese:

Satz 1.11. Allgemeine Äquivalenzumformung.
Eine streng monoton fallende Funktion f ist umkehrbar eindeutig. Die Umkehrfunktion ist auch streng monoton fallend. D. h.

$$a < b \iff f(a) > f(b).$$

Demnach ist die Anwendung einer streng monoton fallenden Funktion eine Äquivalenzumformung bei der sich das Relationszeichen umdreht.

Tatsächlich haben wir schon streng monoton steigende Funktionen kennengelernt. Z. B. ist (1.1) nichts anderes als die strenge Monotonie für $f(x) := x + c$. Und (1.5) ist die strenge Monotonie für $f(x) := nx$.

Die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) := x^2$ ist nicht streng monoton steigend. Zum Beispiel ist $-4 < -2$, aber $16 = f(-4) > f(-2) = 4$. Auch ist die Funktion nicht streng monoton fallend,

denn $2 < 4$, aber $4 = f(2) < f(4) = 16$. Schränkt man f auf den Definitionsbereich $\mathbb{R}_{>0}$ ein, so ergibt sich jedoch eine streng monoton steigende Funktion. Das lässt sich wie folgt zeigen.

Nach Voraussetzung sind $a, b \in \mathbb{R}_{>0}$, d. h. $a, b > 0$. Also kann gemäß (1.18) einerseits mit a und andererseits mit b multipliziert werden:

$$a < b \iff \begin{Bmatrix} a^2 < ab \\ ab < b^2 \end{Bmatrix} \iff a^2 < ab < b^2.$$

2 Grundbegriffe der Mathematik

2.1 Aussagenlogik

2.1.1 Aussagenlogische Formeln

Zur Aussagenlogik findet man zwei Zugänge, zwischen denen eine enge Beziehung besteht. Der erste Zugang ist ein *syntaktischer*, womit gemeint ist, dass logische Formeln als Zeichenketten betrachtet werden, aus denen unter Anwendung von Schlussregeln weitere Zeichenketten gewonnen werden. Der zweite Zugang ist ein *semantischer*, womit gemeint ist, dass logische Formeln inhaltlich Wahrheitswerte zugeordnet bekommen. Im Folgenden wird zunächst nur der semantische Zugang erläutert, weil mir dieser für das grundlegende Verständnis ein wenig leichter zugänglich erscheint.

Aussagen in der Aussagenlogik sind entweder wahr oder falsch, etwas dazwischen gibt es nicht. Dies ist als *Prinzip der Zweiwertigkeit* geläufig. Wir schreiben 0 = falsch und 1 = wahr, das ist schön kurz und knapp.

Für die Aussage »n ist ohne Rest durch m teilbar« bzw. »m teilt n«, schreibt man kurz $m|n$. Aus Aussagen lassen sich in der Aussagenlogik zusammengesetzte Aussagen bilden, z. B.

> Aus $2|n$ und $3|n$ folgt, dass $6|n$,

als Formel:

$$2|n \wedge 3|n \implies 6|n.$$

Streng genommen handelt es sich hierbei um eine Aussageform, da die Aussage von einer Variable abhängig ist. Nachdem für n eine Zahl eingesetzt wurde, ergibt sich daraus eine Aussage, in diesem Fall immer eine wahre Aussage.

Eine zusammengesetzte Aussage wird auch *aussagenlogische Formel* genannt. Aussagenlogische Formeln haben eine innere Struktur. Um diese untersuchen zu können, werden logische Variablen betrachtet, das sind solche Variablen, die für eine Aussage stehen. Eine logische Variable wird durch einen lateinischen Großbuchstaben am Anfang des Alphabetes beschrieben und kann nur mit den Wahrheitswerten falsch oder wahr belegt werden. Die genannte Formel besitzt die Struktur

$$A \wedge B \implies C.$$

In der Formel treten Verknüpfungen von Aussagen auf, das sind $\wedge$ und $\Rightarrow$. Es gibt die grundlegenden Verknüpfungen $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$. Die Bindungsstärke der gelisteten Verknüpfungen ist absteigend, so wie Punktrechnung vor Strichrechnung gilt. Das $\neg$ bindet stärker als $\wedge$, bindet stärker als $\vee$, bindet stärker als $\Rightarrow$, bindet stärker als $\Leftrightarrow$. Die Verknüpfungen sind in Tabelle 2.1 definiert. Anstelle von $\neg A$ schreibt man auch $\overline{A}$.

Es gibt Formeln, die immer wahr sind, unabhängig davon, mit welchen Wahrheitswerten die Variablen belegt werden.

A	$\neg A$
0	1
1	0

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

Tabelle 2.1: Definition der grundlegenden logischen Verknüpfungen.

A	B	$A \wedge B$	$B \wedge A$	$A \wedge B \Rightarrow B \wedge A$
0	0	0	0	1
1	0	0	0	1
0	1	0	0	1
1	1	1	1	1

Tabelle 2.2: Wahrheitstafel zu »$A \wedge B \Rightarrow B \wedge A$«.

Definition 2.1. Tautologie.
Ist φ eine Formel, die bezüglich jeder möglichen Variablenbelegung erfüllt ist, dann nennt man φ eine Tautologie und schreibt dafür kurz $\models \varphi$.

Beispielsweise gilt die Tautologie

$$\models A \wedge B \Rightarrow B \wedge A.$$

Es lässt sich leicht überprüfen ob eine Formel tautologisch ist. Dazu wird einfach die Wahrheitstafel zu dieser Formel aufgestellt, hier Tabelle 2.2. Die Wahrheitstafel ist eine Wertetabelle, die zu jeder Variablenbelegung den Wahrheitswert der Formel angibt. Bei einer tautologischen Formel enthält die Ergebnisspalte in jeder Zeile den Wert 1.

Zwei wichtige Metaregeln, die Einsetzungsregel und die Ersetzungsregel, ermöglichen das Rechnen mit aussagenlogischen Formeln. Die Einsetzungsregel ermöglicht es, aus schon bekannten Tautologien neue bilden zu können, ohne jedes mal eine Wahrheitstafel aufstellen zu müssen. Die Ersetzungsregel ermöglicht die Umformung von Formeln.

Satz 2.1. Einsetzungsregel.
Sei v eine logische Variable. Ist φ eine tautologische Formel, dann ergibt sich wieder eine tautologische Formel, wenn man jedes Vorkommen von v in φ durch eine Formel ψ ersetzt. Kurz:

$$(\models \varphi) \implies (\models \varphi[v := \psi]).$$

Das gilt auch für die simultane Substitution:

$$(\models \varphi) \implies (\models \varphi[v_1 := \psi_1, \ldots, v_n := \psi_n]).$$

Begründung. Die Variable v kann in φ frei mit einem Wahrheitswert belegt werden, nach Voraussetzung ist φ dabei immer erfüllt. Somit ist φ auch erfüllt, wenn v mit dem Wahrheitswert von ψ belegt wird. Dann muss aber auch $\varphi[v := \psi]$ unter einer beliebigen Belegung wahr sein. □

Satz 2.2. Ersetzungsregel.
Sei $F(\varphi)$ eine Formel, welche von der Teilformel φ abhängig ist. Sei außerdem φ äquivalent zu ψ. Dann sind auch $F(\varphi)$ und $F(\psi)$ äquivalent. Kurz:

$$(\models \varphi \Leftrightarrow \psi) \implies (\models F(\varphi) \Leftrightarrow F(\psi)).$$

Begründung. Die Äquivalenz von φ und ψ erzwingt, dass ψ unter einer beliebigen Belegung den gleichen Wahrheitswert besitzt wie φ. Da $F(0) \Leftrightarrow F(0)$ und $F(1) \Leftrightarrow F(1)$ gilt, muss also $F(\varphi) \Leftrightarrow F(\psi)$ gelten. □

Satz 2.3. Kleine Metaregel.
Es gilt $\models \varphi$ und $\models \psi$ genau dann, wenn $\models \varphi \wedge \psi$.

Beweis. Sind φ, ψ tautologisch, dann dürfen sie durch den Wahrheitswert wahr ersetzt werden. Unter dieser Voraussetzung ist $\varphi \wedge \psi$ gleichbedeutend mit $1 \wedge 1$, demnach auch tautologisch.

Sei nun umgekehrt $\varphi \wedge \psi$ tautologisch. Es müssen zwingend auch φ und ψ wahr sein, denn sonst wäre $\varphi \wedge \psi$ falsch. □

Satz 2.4. Kleine Abtrennungsregel.
Aus $\models \varphi$ und $\models \varphi \Rightarrow \psi$ folgt $\models \psi$.
Aus $\models \varphi$ und $\models \varphi \Leftrightarrow \psi$ folgt $\models \psi$.

Beweis. Ist φ tautologisch, dann darf es durch den Wahrheitswert wahr ersetzt werden. Unter dieser Voraussetzung ist $\varphi \Rightarrow \psi$ gleichbedeutend mit $1 \Rightarrow \psi$. Diese Formel kann nur erfüllt sein, wenn auch ψ wahr ist. Da aber $\varphi \Rightarrow \psi$ tautologisch sein soll, muss damit zwingend auch ψ tautologisch sein. Für $\varphi \Leftrightarrow \psi$ ist die Argumentation analog. □

Satz 2.5. Abtrennung von Implikationen.
Aus $\models \varphi \Leftrightarrow \psi$ folgt $\models \varphi \Rightarrow \psi$.

Beweis. Man zeigt

$$\models (A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$$

mittels Wahrheitstafel. Gemäß der Einsetzungsregel gilt dann auch

$$\models (\varphi \Leftrightarrow \psi) \Leftrightarrow (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi).$$

Mit der kleinen Abtrennungsregel und der Voraussetzung erhält man

$$\models (\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi).$$

Gemäß der kleinen Metaregel ergibt sich schließlich $\models \varphi \Rightarrow \psi$. □

UND	ODER	Bezeichnung
$A \wedge 0 \equiv 0$	$A \vee 1 \equiv 1$	Extremalgesetze
$A \wedge \overline{A} \equiv 0$	$A \vee \overline{A} \equiv 1$	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
$\overline{A \wedge B} \equiv \overline{A} \vee \overline{B}$	$\overline{A \vee B} \equiv \overline{A} \wedge \overline{B}$	De morgansche Gesetze
$A \wedge (A \vee B) \equiv A$	$A \vee (A \wedge B) \equiv A$	Absorptionsgesetze

Tabelle 2.3: Die Regeln der booleschen Algebra.

Definition 2.2. Äquivalente Formeln.
Zwei Formeln φ, ψ heißen äquivalent, wenn die Äquivalenz $\varphi \Leftrightarrow \psi$ tautologisch ist, kurz

$$(\varphi \equiv \psi) \ :\Longleftrightarrow \ (\models \varphi \Leftrightarrow \psi).$$

Satz 2.6. Die Relation $\varphi \equiv \psi$ ist eine Äquivalenzrelation, d. h. es gilt

$$\varphi \equiv \varphi, \qquad \text{(Reflexivität)} \tag{2.1}$$
$$(\varphi \equiv \psi) \implies (\psi \equiv \varphi), \qquad \text{(Symmetrie)} \tag{2.2}$$
$$(\varphi \equiv \psi) \wedge (\psi \equiv \chi) \implies (\varphi \equiv \chi). \qquad \text{(Transitivität)} \tag{2.3}$$

2.1.2 Boolesche Algebra

Die Regeln in Tabelle 2.3 gewinnt man alle mittels Wahrheitstafel. Gemäß der Einsetzungsregel dürfen für die Variablen auch Formeln eingesetzt werden, die griechischen Formelvariablen benötigt man somit nicht mehr.

Weiterhin gelten die Distributivgesetze

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C), \tag{2.4}$$
$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C). \tag{2.5}$$

Schließlich gibt es noch das Involutionsgesetz

$$\overline{\overline{A}} \equiv A. \tag{2.6}$$

Die Implikation und die Äquivalenz lassen sich auf NICHT, UND, ODER zurückführen:

$$A \Rightarrow B \equiv \overline{A} \vee B, \tag{2.7}$$
$$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A). \tag{2.8}$$

Mit den bisher genannten Regeln lassen sich aussagenlogische Formeln auf einfache Art umformen. Z. B. ist die Formel $1 \Rightarrow A$ äquivalent zu A. Man findet

$$1 \Rightarrow A \quad \equiv \quad \overline{1} \vee A \quad \equiv \quad 0 \vee A \quad \equiv \quad A.$$

Natürlich kann man alternativ mittels Wahrheitstafel auch

$$\models (1 \Rightarrow A) \Leftrightarrow A$$

überprüfen.

Satz 2.7. Formel zum Modus ponens.
Es gilt $\models A \wedge (A \Rightarrow B) \Rightarrow B$.

Beweis. Gemäß den Regeln der booleschen Algebra ergibt sich

$$A \wedge (A \Rightarrow B) \Rightarrow B \tag{2.9}$$
$$\equiv A \wedge (\overline{A} \vee B) \Rightarrow B \qquad \text{(Zerlegung von »⇒«)} \tag{2.10}$$
$$\equiv \overline{A \wedge (\overline{A} \vee B)} \vee B \qquad \text{(Zerlegung von »⇒«)} \tag{2.11}$$
$$\equiv \overline{A} \vee \overline{\overline{A} \vee B} \vee B \qquad \text{(De Morgan)} \tag{2.12}$$
$$\equiv \overline{A} \vee (\overline{\overline{A}} \wedge \overline{B}) \vee B \qquad \text{(De Morgan)} \tag{2.13}$$
$$\equiv \overline{A} \vee (A \wedge \overline{B}) \vee B \qquad \text{(Involutionsgesetz)} \tag{2.14}$$
$$\equiv ((\overline{A} \vee A) \wedge (\overline{A} \vee \overline{B})) \vee B \qquad \text{(Distributivgesetz)} \tag{2.15}$$
$$\equiv (1 \wedge (\overline{A} \vee \overline{B})) \vee B \qquad \text{(Komplementärgesetz)} \tag{2.16}$$
$$\equiv (\overline{A} \vee \overline{B}) \vee B \qquad \text{(Absorptionsgesetz)} \tag{2.17}$$
$$\equiv \overline{A} \vee (\overline{B} \vee B) \qquad \text{(Assoziativgesetz)} \tag{2.18}$$
$$\equiv \overline{A} \vee 1 \qquad \text{(Komplementärgesetz)} \tag{2.19}$$
$$\equiv 1. \; \square \qquad \text{(Absorptionsgesetz)} \tag{2.20}$$

Von der Ersetzungsregel (Satz 2.2), also

$$\varphi \equiv \psi \;\text{ impliziert }\; F(\varphi) \equiv F(\psi),$$

wurde ständig stillschweigend Gebrauch gemacht, nämlich bei jeder Umformung einer Teilformel.

Satz 2.8. Regel zur Kontraposition.
Es gilt $A \Rightarrow B \equiv \overline{B} \Rightarrow \overline{A}$.

Beweis. Man findet

$$A \Rightarrow B \tag{2.21}$$
$$\equiv \overline{A} \vee B \qquad \text{(Zerlegung von »⇒«)} \tag{2.22}$$
$$\equiv B \vee \overline{A} \qquad \text{(Kommutativgesetz)} \tag{2.23}$$
$$\equiv \overline{\overline{B}} \vee \overline{A} \qquad \text{(Involutionsgesetz)} \tag{2.24}$$
$$\equiv \overline{B} \Rightarrow \overline{A}. \; \square \qquad \text{(Zerlegung von »⇒«)} \tag{2.25}$$

2.1.3 Formale Beweise

Definition 2.3. Semantische Implikation.
Sei $M = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ eine Menge von Formeln und sei ψ eine weitere Formel. Man sagt dann, M impliziert ψ, kurz $M \models \psi$, wenn jede Belegung von logischen Variablen, die alle Formeln in M erfüllt, auch ψ erfüllt.

Das klingt etwas kompliziert, ist es aber eigentlich nicht. Man schaut sich die große Wahrheitstafel an, in der alle Formeln vorkommen, jede Formel in einer neuen Spalte. Ergibt sich in einer Zeile bei allen Formeln in M eine 1, dann muss auch ψ in dieser Zeile den Wahrheitswert 1 besitzen.

Die Aussage $\models \varphi$ ist mit $\{\} \models \varphi$ gleichbedeutend, denn bei einer leeren Formelmenge werden keine Belegungen ausgeschlossen, φ muss also jede Belegung erfüllen. Der Definition nach ist φ dann eine Tautologie.

Man beobachtet außerdem, dass $\{\varphi\} \models \psi$ mit $\models \varphi \Rightarrow \psi$ übereinstimmt. Hat nämlich φ den Wahrheitswert 0, dann ist $\varphi \Rightarrow \psi$ immer erfüllt, ohne dass der Wahrheitswert von ψ dabei eine Rolle spielt. Solche Belegungen entfallen auch bei $\{\varphi\} \models \psi$. Nun darf φ als wahr vorausgesetzt werden. Wäre ψ nun falsch, dann ist $\varphi \Rightarrow \psi$ nicht mehr erfüllt, also auch $\models \varphi \Rightarrow \psi$ falsch. In diesem Fall ist aber auch $\{\varphi\} \models \psi$ falsch. Es verbleibt nun die Situation, dass sowohl φ also auch ψ wahr sind. Mit diesen Belegungen bleibt dann auch $\{\varphi\} \models \psi$ unverletzt.

Satz 2.9. Deduktionstheorem.
Es gilt $M \cup \{\varphi\} \models \psi$ genau dann, wenn $M \models \varphi \Rightarrow \psi$.

Beweis. Man hat

$$M \cup \varphi = \{\varphi_1, \ldots, \varphi_n, \varphi\}. \tag{2.26}$$

Dass alle diese Formeln unter einer Belegung erfüllt sein sollen, ist aber gleichbedeutend damit, dass die Aussage

$$\varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi \tag{2.27}$$

unter dieser Belegung erfüllt ist. Wie bereits erläutert, gilt

$$(\{\varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi\} \models \psi) \iff (\models \varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi \Rightarrow \psi). \tag{2.28}$$

Mittels boolescher Algebra findet man nun

$$\varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi \Rightarrow \psi \tag{2.29}$$
$$\equiv \overline{\varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi} \vee \psi \tag{2.30}$$
$$\equiv \overline{\varphi_1 \wedge \ldots \wedge \varphi_n} \vee \overline{\varphi} \vee \psi \tag{2.31}$$
$$\equiv \overline{\varphi_1 \wedge \ldots \wedge \varphi_n} \vee (\varphi \Rightarrow \psi) \tag{2.32}$$
$$\equiv \varphi_1 \wedge \ldots \wedge \varphi_n \Rightarrow (\varphi \Rightarrow \psi) \tag{2.33}$$

Schließlich gilt aber auch wieder

$$(\models \varphi_1 \wedge \ldots \wedge \varphi_n \Rightarrow (\varphi \Rightarrow \psi)) \iff (\{\varphi_1 \wedge \ldots \wedge \varphi_n\} \models \varphi \Rightarrow \psi). \; \square \tag{2.34}$$

Definition 2.4. Schlussregel.
Sei M eine Menge von Formeln, die Formelvariablen enthalten und ψ eine Formelvariable. Ist die Aussage $M \models \psi$ wahr, unabhängig davon, welche Formeln für die Formelvariablen eingesetzt werden, dann spricht man von einer Schlussregel.

Satz 2.10. Modus ponens.
Es gilt die Schlussregel $\{\varphi, \varphi \Rightarrow \psi\} \models \psi$.

Beweis. Gemäß Deduktionstheorem gilt

$$(\{\varphi, \varphi \Rightarrow \psi\} \models \psi) \iff (\models \varphi \wedge (\varphi \Rightarrow \psi) \Rightarrow \psi).$$

Gemäß Satz 2.7 ist die rechte Seite wahr. □

Schlussregeln ermöglichen es uns, aus wahren Aussagen weitere wahre Aussagen zu gewinnen. Die Belegung mit logischen Variablen tritt nun in den Hintergrund, besonders dann, wenn die Formeln keine logischen Variablen mehr enthalten. Sind A und $A \Rightarrow B$ wahre Aussagen, dann muss gemäß Modus ponens auch B eine wahre Aussage sein.

Ein Beispiel dazu. Sei $A(n) := (2|n)$ die Aussage »2 teilt n« und $B(n) := (4|n^2)$ die Aussage »4 teilt n^2«. Nun gilt $A(n) \Rightarrow B(n)$ für jede beliebige ganze Zahl, welche für n eingesetzt wird. Gemäß Modus ponens ist der Schluss

$$\{A(n), A(n) \Rightarrow B(n)\} \models B(n)$$

richtig. Ausgehend von »2 teilt 10« können wir damit »4 teilt 100« schlussfolgern.

Definition 2.5. Beweis.
Eine Aussage ist sicher dann wahr, wenn sie mittels Schlussregeln aus schon bekannten wahren Aussagen gefolgert werden kann. Die Kette von Schlüssen heißt Beweis dieser Aussage.

Ein Beispiel dazu. Angenommen wir wissen, dass die Aussage A wahr ist. Außerdem ist bekannt, dass $A \Rightarrow B$ und $B \Rightarrow C$ wahr sind. Gemäß Modus ponens ist dann auch B wahr. Nochmalige Anwendung des Modus ponens liefert die Wahrheit von C.

Der formale Beweis von C schaut so aus:

1. A, (Prämisse)
2. $A \Rightarrow B$, (Prämisse)
3. $B \Rightarrow C$, (Prämisse)
4. B, (MP, 1, 2)
5. C (MP, 4, 3)

In Klammern steht immer die Begründung für die jeweilige Aussage. Der Modus ponens wurde mit MP abgekürzt.

2.1.4 Notwendige und hinreichende Bedingungen

Manchmal sagt man, eine Bedingung ist für eine bestimmte Aussage notwendig. Das ist ein schon bekannter logischer Zusammenhang. Sei B die Bedingung und A die Aussage. Ist B falsch, dann kann A niemals wahr sein. Ist B wahr, dann ist A beliebig, denn nur weil die notwendige Bedingung B zutrifft, heißt das nicht, dass die Aussage A zwingend wahr sein muss. Dieser Zusammenhang wird nun gerade genau durch die Wahrheitstafel von $A \Rightarrow B$ wiedergegeben. Man erhält

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

Die Sprechweise »B ist hinreichend für A« drückt dagegen aus, dass die Wahrheit von A mit der Wahrheit von B sichergestellt ist. Falls B jedoch falsch ist, ist der Wahrheitsgehalt von A beliebig. Dieser Zusammenhang wird gerade durch die Wahrheitstafel von $B \Rightarrow A$ wiedergegeben. Man erhält

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

Um sich pedantischer ausdrücken, sprechen manche von notwendigen, aber nicht hinreichenden Bedingungen, bzw. von hinreichenden, aber nicht notwendigen Bedingungen.

Gemäß $(A \Leftrightarrow B) \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$ ergibt sich

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

Weitere Sprechweisen für $A \Rightarrow B$ sind »A impliziert B« und »A zieht B nach sich« sowie »aus A folgt B«.

Ist B hinreichend für A, dann kann man sich bei A sicher sein, sofern die Bedingung B überprüft wurde.

Ist B nur notwendig für A, dann ist durch eine Überprüfung von B nicht viel Wissen über A gewonnen, man darf sich nicht sicher sein, dass A wahr ist. Lediglich falls B falsch ist, lässt sich mittels Kontraposition

$$A \Rightarrow B \;\equiv\; \overline{B} \Rightarrow \overline{A}$$

ableiten, dass dann auch A falsch sein muss.

Man gewinnt den folgenden Zusammenhang:

$$(B \text{ ist notwendig für } A) \;\equiv\; (\overline{B} \text{ ist hinreichend für } \overline{A}).$$

Sind für eine Aussage A mehrere Bedingungen B_k notwendig, dann heißt das, A ist schon falsch, wenn nur eine der B_k falsch ist. Die Formel dazu ist

$$A \Rightarrow B_1 \wedge B_2 \wedge \ldots \wedge B_n.$$

Sind für eine Aussage A mehrere Bedingungen B_k hinreichend, dann heißt das, A ist schon dann richtig, wenn nur eine der B_k richtig ist. Die Formel dazu ist

$$B_1 \vee B_2 \vee \ldots \vee B_n \Rightarrow A.$$

2.1.5 Widerspruchsbeweise

Mittels boolescher Algebra oder einer Wahrheitstafel überzeugt man sich leicht von

$$\models (A \Rightarrow B) \wedge (A \Rightarrow \overline{B}) \Rightarrow \overline{A}.$$

Unter Heranziehung des Deduktionstheorems ist das äquivalent zu

$$\{A \Rightarrow B,\ A \Rightarrow \overline{B}\} \models \overline{A}.$$

Angenommen, man konnte die Aussagen B und $\overline{B}$ unter Annahme von A beweisen, dann gilt $\{A\} \models B$ und $\{A\} \models \overline{B}$. Gemäß Deduktionstheorem bedeutet das jedoch $\models A \Rightarrow B$ und $\models A \models \overline{B}$. Da diese Bedingungen tautologisch sind, können sie entfallen, übrig bleibt $\models \overline{A}$.

Wir gelangen zur folgenden Schlussregel.

Satz 2.11. Reductio ad absurdum.
Kann man unter Annahme einer Prämisse φ sowohl ψ als auch $\overline{\psi}$ beweisen, dann muss die Negation von φ tautologisch sein:

$$\{\varphi\} \models \psi \text{ und } \{\varphi\} \models \overline{\psi} \text{ impliziert } \models \overline{\varphi}.$$

Diese Schlussregel lässt sich noch ein wenig verallgemeinern. Man überzeugt sich mittels boolescher Algebra oder Wahrheitstafel von

$$\models (K \wedge A \Rightarrow B) \wedge (K \wedge A \Rightarrow \overline{B}) \Rightarrow (K \Rightarrow \overline{A}).$$

Nochmals wird das Deduktionstheorem angewendet:

$$\{K \wedge A \Rightarrow B,\ K \wedge A \Rightarrow \overline{B}\} \models K \Rightarrow \overline{A}.$$

Für K lässt sich eine konjunktive Aussage $\varphi_1 \wedge \ldots \wedge \varphi_n$ einsetzen. Definiert man $M := \{\varphi_1, \ldots, \varphi_n\}$, dann gilt

$$(M \cup \{A\} \models \psi) \iff (\models K \wedge A \Rightarrow \psi)$$

gemäß Deduktionstheorem. Die restliche Überlegung gestaltet sich wie zuvor. Insgesamt erhält man das folgende Ergebnis.

Satz 2.12. Reductio ad absurdum.
Sei M eine endliche Formelmenge. Es gilt:

$$M \cup \{\varphi\} \models \psi \text{ und } M \cup \{\varphi\} \models \overline{\psi} \text{ impliziert } M \models \overline{\varphi}.$$

Aus der Reductio ad absurdum lässt sich nun ein Beweisverfahren erstellen. Man setzt $\varphi \equiv \overline{A}$ ein und beachtet $A \equiv \neg\neg A$. Aus $\overline{A} \models \psi$ und $\overline{A} \models \overline{\psi}$ lässt sich wie gezeigt $\models A$ schlussfolgern. Nimmt man also $\overline{A}$ an, und zeigt damit den Widerspruch, dass sowohl ψ als auch $\overline{\psi}$, dann hat man einen Beweis für A.

2.2 Prädikatenlogik

2.2.1 Endliche Bereiche

In diesem Abschnitt wird der Übergang von der Aussagenlogik in die Prädikatenlogik beschrieben. Eine Prädikat P ist eine Aussageform, die einem Objekt x einen Wahrheitswert $P(x)$ zuordnet. Z. B. ist $P(x) \equiv (x < 4)$ ein Prädikat. Je nachdem was für eine Zahl für x eingesetzt wird, ergibt sich entweder wahr oder falsch.

Definition 2.6. Allquantor.
Der Allquantor für endliche Objektbereiche ist rekursiv definiert gemäß

$$\bigwedge_{k=1}^{0} P(x_k) :\equiv 1, \qquad \bigwedge_{k=1}^{n} P(x_k) :\equiv P(x_n) \wedge \bigwedge_{k=1}^{n-1} P(x_k).$$

Definition 2.7. Existenzquantor.
Der Existenzquantor für endliche Objektbereiche ist rekursiv definiert gemäß

$$\bigvee_{k=1}^{0} P(x_k) :\equiv 0, \qquad \bigvee_{k=1}^{n} P(x_k) :\equiv P(x_n) \vee \bigvee_{k=1}^{n-1} P(x_k).$$

Das allquantifizierte Prädikat ist nur dann wahr, wenn $P(x_k)$ für jedes x_k erfüllt ist. Man bekommt die aussagenlogische Formel

$$\bigwedge_{k=1}^{n} P(x_k) \quad \equiv \quad P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n).$$

Meistens benutzen wir die Schreibweisen

$$(\forall x \in M)P(x) \equiv \bigwedge_{k=1}^{n} P(x_k), \qquad (\exists x \in M)P(x) \equiv \bigvee_{k=1}^{n} P(x_k),$$

wobei $M = \{x_1, x_2, \ldots, x_n\}$ die Zusammenfassung der Objekte ist. Auch Kurzformen wie $\forall x P(x)$ oder $\forall_x P_x$ sind üblich, sie sparen vor allem Schreibaufwand beim Rechnen.

Nun muss man für diese Operatoren auch eine Operatorrangfolge festlegen. Da die Operatoren präfix sind, ist dabei leglich die rechte Seite zu berücksichtigen. Alle bisher genannten Schreibweisen haben die höchste Rangfolge, werden also gelesen wie die Negation. D. h. $(\forall x)P(x)$ wird gelesen wie $\neg P(x)$. Z. B. wird die Formel

$$(\forall x \in M)P(x) \wedge A \quad \text{gelesen als} \quad ((\forall x \in M)P(x)) \wedge A,$$

Davon zu unterscheiden ist die Formel

$$(\forall x \in M)(P(x) \wedge A).$$

Daneben gibt es noch die Schreibweisen $\forall x\colon P(x)$ und $\exists x\colon P(x)$, die in der Mathematik außerhalb der Logik üblicher sind. Eine gängige Festlegung ist hierbei, dass alles hinter dem Doppelpunkt in den Wirkungsbereich des Quantors fällt. Weil das der ersten Festlegung widerspricht und sich nicht jeder daran hält, werden wir diese Schreibweise nur dann benutzen, wenn es nicht zu Zweideutigkeiten kommt. Bei all der Umständlichkeit geht es nur um das Einsparen von Klammern, einen tieferen Grund gibt es nicht.

Satz 2.13. Distributivgesetze.
Ist M endlich, A eine Aussage und $P(x)$ ein Prädikat auf M, dann gilt

$$A \vee (\forall x \in M)P(x) \equiv (\forall x \in M)(A \vee P(x)),$$
$$A \wedge (\exists x \in M)P(x) \equiv (\exists x \in M)(A \wedge P(x)).$$

Beweis. Induktiv mittels boolescher Algebra. Induktionsanfang:

$$A \vee \bigwedge_{k=1}^{0} P(x_k) \equiv A \vee 1 \equiv 1 \equiv \bigwedge_{k=1}^{0} (A \vee P(x_k)).$$

Induktionsschritt:

$$A \vee \bigwedge_{k=1}^{n} P(x_k) \equiv A \vee (P(x_n) \wedge \bigwedge_{k=1}^{n-1} P(x_k)) \equiv (A \vee P(x_n)) \wedge (A \vee \bigwedge_{k=1}^{n-1} P(x_k))$$
$$\equiv (A \vee P(x_n)) \wedge \bigwedge_{k=1}^{n-1} (A \vee P(x_k)) \equiv \bigwedge_{k=1}^{n} (A \vee P(x_k)).$$

Für den Existenzquantor ist die Argumentation analog. □

Satz 2.14. De morgansche Gesetze.
Ist M endlich und $P(x)$ ein Prädikat auf M, dann gilt

$$\neg(\forall x \in M)P(x) \equiv (\exists x \in M)\ \neg P(x),$$
$$\neg(\exists x \in M)P(x) \equiv (\forall x \in M)\ \neg P(x).$$

Beweis. Induktionsanfang:

$$\neg \bigwedge_{k=1}^{0} P(x_k) \equiv \neg 1 \equiv 0 \equiv \bigvee_{k=1}^{0} \neg P(x_k).$$

Induktionsschritt:

$$\neg \bigwedge_{k=1}^{n} P(x_k) \equiv \neg(P(x_n) \wedge \bigwedge_{k=1}^{n-1} P(x_k)) \equiv \neg P(x_n) \vee \neg \bigwedge_{k=1}^{n-1} P(x_k)$$
$$\equiv \neg P(x_n) \vee \bigvee_{k=1}^{n-1} \neg P(x_k) \equiv \bigvee_{k=1}^{n} \neg P(x_k).$$

Für den Existenzquantor ist die Argumentation analog. □

Satz 2.15. Verträglichkeitsgesetze.
Ist M endlich und sind $P(x), Q(x)$ Prädikate auf M, dann gilt

$$(\forall x \in M)(P(x) \wedge Q(x)) \equiv (\forall x \in M)P(x) \wedge (\forall x \in M)Q(x),$$
$$(\exists x \in M)(P(x) \vee Q(x)) \equiv (\exists x \in M)P(x) \vee (\exists x \in M)Q(x).$$

Beweis. Induktionsanfang:

$$\bigwedge_{k=1}^{0}(P(x_k) \wedge Q(x_k)) \equiv 1 \equiv 1 \wedge 1 \equiv \bigwedge_{k=1}^{0} P(x_k) \wedge \bigwedge_{k=1}^{0} Q(x_k).$$

Induktionsschritt:

$$\bigwedge_{k=1}^{n}(P(x_k) \wedge Q(x_k)) \equiv (P(x_n) \wedge Q(x_n)) \wedge \bigwedge_{k=1}^{n-1}(P(x_k) \wedge Q(x_k))$$
$$\equiv P(x_n) \wedge Q(x_n) \wedge \bigwedge_{k=1}^{n-1} P(x_k) \wedge \bigwedge_{k=1}^{n-1} Q(x_k)$$
$$\equiv P(x_n) \wedge \bigwedge_{k=1}^{n-1} P(x_k) \wedge Q(x_n) \wedge \bigwedge_{k=1}^{n-1} Q(x_k) \equiv \bigwedge_{k=1}^{n} P(x_k) \wedge \bigwedge_{k=1}^{n} Q(x_k).$$

Die Argumentation für den Existenzquantor ist analog. □

Satz 2.16. Vertauschbarkeit gleichartiger Quantoren.
Sind M, N endlich, dann gilt

$$(\forall x \in M)(\forall x \in N)P(x,y) \equiv (\forall x \in N)(\forall x \in M)P(x,y),$$
$$(\exists x \in M)(\exists x \in N)P(x,y) \equiv (\exists x \in N)(\exists x \in M)P(x,y).$$

Beweis. Induktionsanfang:

$$\bigwedge_{i=1}^{0}\bigwedge_{j=1}^{n} P(x_i,y_j) \equiv 1 \equiv \bigwedge_{j=1}^{n} 1 \equiv \bigwedge_{j=1}^{n}\bigwedge_{i=1}^{0} P(x_i,y_j).$$

Induktionsschritt:

$$\bigwedge_{i=1}^{m}\bigwedge_{j=1}^{n} P(x_i,y_j) \equiv \bigwedge_{j=1}^{n} P(x_m,y_j) \wedge \bigwedge_{i=1}^{m-1}\bigwedge_{j=1}^{n} P(x_i,y_j)$$
$$\equiv \bigwedge_{j=1}^{n} P(x_m,y_j) \wedge \bigwedge_{j=1}^{n}\bigwedge_{i=1}^{m-1} P(x_i,y_j)$$
$$\overset{(*)}{\equiv} \bigwedge_{j=1}^{n}\left(P(x_m,y_j) \wedge \bigwedge_{i=1}^{m-1} P(x_i,y_j)\right) \equiv \bigwedge_{j=1}^{n}\bigwedge_{i=1}^{m} P(x_i,y_j).$$

Die Äquivalenz $(*)$ gilt gemäß Satz 2.15.

Für den Existenzquantor ist die Argumentation analog. □

2.2.2 Allgemeine Regeln

Man denkt sich nun ein Universum U, das alle denkbaren Objekte enthält. Das Prädikat $P(x)$ sei für jedes $x \in U$ definiert. Anstelle von $(\forall x \in U)P(x)$ schreibt man kürzer $(\forall x)P(x)$. Anstelle von $(\exists x \in U)P(x)$ schreibt man kürzer $(\exists x)P(x)$. Das Universum darf unendlich sein, aber nicht leer, es muss immer mindestens ein Element enthalten.

Definition 2.8. Allquantor.
Es gilt $(\forall x)P(x)$ genau dann, wenn $P(x)$ für jedes beliebige x wahr ist.

Definition 2.9. Existenzquantor.
Es gilt $(\exists x)P(x)$ genau dann, wenn ein x gefunden werden kann, das $P(x)$ erfüllt.

Das Problem das sich jetzt stellt, ist, dass zur Überprüfung von prädikatenlogischen Formeln unendlich viele Wahrheitstafeln aufgestellt werden müssten, nämlich für jedes der unendlich vielen Objekte, welche für eine Objektvariable eingesetzt werden können, und das auch noch für jedes Prädikat, welches in eine Prädikatvariable eingesetzt werden kann. Wir müssen also anders vorgehen.

Zunächst überzeugt man sich davon, dass die Einsetzungsregel und die Ersetzungsregel gültig bleiben. Außerdem definiert man für zwei prädikatenlogische Formeln φ, ψ die Äquivalenz als

$$(\varphi \equiv \psi) \ :\Longleftrightarrow \ (\{\varphi\} \models \psi) \wedge (\{\psi\} \models \varphi).$$

Bei der semantischen Implikation werden nun nicht nur Aussagenvariablen mit Wahrheitswerten belegt. Auch Prädikatvariablen werden mit Prädikaten belegt. Da es unendlich viele Prädikate gibt, lässt sich das natürlich praktisch nicht mehr durchführen.

Satz 2.17. Es gilt $A \equiv (\forall x)A$ und $A \equiv (\exists x)A$.

Beweis. Im Fall $A \equiv 0$ ist auch $(\forall x)0$ falsch, da 0 für kein x erfüllt ist. Im Fall $A \equiv 1$ ist auch $(\forall x)1$ wahr, da 1 für jedes beliebige x erfüllt ist. Für den Existenzquantor ist die Argumentation analog. □

Vorsicht, das Universum darf nicht leer sein, denn $(\forall x{\in}\{\})\, 0 \equiv 1$.

Satz 2.18. Verallgemeinerte Distributivgesetze.
Es gilt

$$A \vee (\forall x)P(x) \equiv (\forall x)(A \vee P(x)),$$
$$A \wedge (\exists x)P(x) \equiv (\exists x)(A \wedge P(x)).$$

Beweis. Im Fall $A \equiv 0$ ergibt sich

$$A \vee (\forall x)P(x) \equiv 0 \vee (\forall x)P(x) \equiv (\forall x)P(x) \equiv (\forall x)(0 \vee P(x)) \equiv (\forall x)(A \vee P(x)).$$

Im Fall $A \equiv 1$ ergibt sich

$$A \vee (\forall x)P(x) \equiv 1 \vee (\forall x)P(x) \equiv 1 \equiv (\forall x)1 \equiv (\forall x)(1 \vee P(x)) \equiv (\forall x)(A \vee P(x)).$$

Für den Existenzquantor ist die Argumentation analog. □

Satz 2.19. Verallgemeinerte de morgansche Gesetze.
Es gilt

$$\neg(\forall x)P(x) \equiv (\exists x)\ \neg P(x),$$
$$\neg(\exists x)P(x) \equiv (\forall x)\ \neg P(x).$$

Beweis. Gilt $(\forall x)P(x)$, dann ist $P(x) \equiv 1$. Es ergibt sich

$$\neg(\forall x)P(x) \equiv \neg 1 \equiv 0 \equiv (\exists x)0 \equiv (\exists x)\ \neg 1 \equiv (\exists x)\ \neg P(x). \tag{2.35}$$

Gilt $(\forall x)P(x)$ nicht, dann muss es ein x mit $\neg P(x) \equiv 1$ geben und es gilt

$$\neg(\forall x)P(x) \equiv \neg 0 \equiv 1 \equiv (\exists x)1 \equiv (\exists x)\ \neg P(x). \tag{2.36}$$

Die Argumentation für den Existenzquantor ist analog. □

Satz 2.20. Verträglichkeitsgesetze.
Es gilt

$$(\forall x)(P(x) \wedge Q(x)) \equiv (\forall x)P(x) \wedge (\forall x)Q(x),$$
$$(\exists x)(P(x) \vee Q(x)) \equiv (\exists x)P(x) \vee (\exists x)Q(x).$$

Beweis. Angenommen, die linke Seite ist wahr. Dann muss $P(x) \wedge Q(x) \equiv 1$ sein, und daher auch $P(x) \equiv 1$ und $Q(x) \equiv 1$. Dann ist aber auch $(\forall x)P(x) \equiv 1$ und $(\forall x)Q(x) \equiv 1$. Somit gilt

$$(\forall x)(P(x) \wedge Q(x)) \equiv 1 \equiv 1 \wedge 1 \equiv (\forall x)P(x) \wedge (\forall x)Q(x). \tag{2.37}$$

Angenommen, die linke Seite ist falsch. Dann gibt es ein x, für welches $P(x) \wedge Q(x) \equiv 0$ ist. Für dieses x muss also $P(x) \equiv 0$ oder $Q(x) \equiv 0$ sein, oder beides. Dann ist auch $(\forall x)P(x) \equiv 0$ oder $(\forall x)Q(x) \equiv 0$. Somit ist

$$(\forall x)P(x) \wedge (\forall x)Q(x) \equiv 0. \tag{2.38}$$

Für den Existenzquantor ist die Argumentation analog. Alternativ ergibt sich nach den de morganschen und verallgemeinerten de morganschen Gesetzen

$$(\exists x)(P(x) \vee Q(x)) \equiv \neg(\forall x)\ \neg(P(x) \vee Q(x)) \tag{2.39}$$
$$\equiv \neg(\forall x)(\neg P(x) \wedge \neg Q(x)) \equiv \neg((\forall x)\ \neg P(x) \wedge (\forall x)\ \neg Q(x)) \tag{2.40}$$
$$\equiv \neg(\forall x)\ \neg P(x) \vee \neg(\forall x)\ \neg Q(x) \equiv (\exists x)P(x) \vee (\exists x)Q(x).\ \square \tag{2.41}$$

2.2.3 Beschränkte Quantifizierung

Definition 2.10. Beschränkte Quantifizierung.
Ist P ein Prädikat auf U und $M \subseteq U$ eine Teilmenge von U, dann definiert man

$$(\forall x \in M)P(x) :\equiv (\forall x)(x \in M \Rightarrow P(x)),$$
$$(\exists x \in M)P(x) :\equiv (\exists x)(x \in M \wedge P(x)).$$

Zuweilen schreibt man auch

$$(\forall R(x))P(x) :\equiv (\forall x)(R(x) \Rightarrow P(x)), \tag{2.42}$$
$$(\exists R(x))P(x) :\equiv (\exists x)(R(x) \wedge P(x)), \tag{2.43}$$

solange klar bleibt, dass x die gebundene Variable ist. Z. B. $(\forall x{<}4)P(x)$ und ähnlich.

Satz 2.21. Verallgemeinerte Distributivgesetze.
Es gilt

$$A \vee (\forall x \in M)P(x) \equiv (\forall x \in M)(A \vee P(x)),$$
$$A \wedge (\exists x \in M)P(x) \equiv (\exists x \in M)(A \wedge P(x)).$$

Beweis. Für den Allquantor gilt

$$A \vee (\forall x \in M)P(x) \equiv A \vee (\forall x)(x \in M \Rightarrow P(x)) \tag{2.44}$$
$$\equiv A \vee (\forall x)(\neg x \in M \vee P(x)) \equiv (\forall x)(A \vee \neg x \in M \vee P(x)) \tag{2.45}$$
$$\equiv (\forall x)(x \in M \Rightarrow A \vee P(x)) \equiv (\forall x \in M)(A \vee P(x)). \tag{2.46}$$

Für den Existenzquantor gilt

$$A \wedge (\exists x \in M)P(x) \equiv A \wedge (\exists x)(x \in M \wedge P(x)) \tag{2.47}$$
$$\equiv (\exists x)(A \wedge x \in M \wedge P(x)) \equiv (\exists x)(x \in M \wedge A \wedge P(x)) \tag{2.48}$$
$$\equiv (\exists x \in M)(A \wedge P(x)). \square \tag{2.49}$$

Satz 2.22. Verallgemeinerte de morgansche Gesetze.
Es gilt

$$\neg(\forall x \in M)P(x) \equiv (\exists x \in M)\ \neg P(x),$$
$$\neg(\exists x \in M)P(x) \equiv (\forall x \in M)\ \neg P(x).$$

Beweis. Es gilt

$$\neg(\forall x \in M)P(x) \equiv \neg(\forall x)(x \in M \Rightarrow P(x)) \equiv \neg(\forall x)(\neg x \in M \vee P(x)) \tag{2.50}$$
$$\equiv (\exists x)(x \in M \wedge \neg P(x)) \equiv (\exists x \in M)\ \neg P(x). \tag{2.51}$$

Die Argumentation für den Existenzquantor ist analog. $\square$

2.3 Mengenlehre

2.3.1 Der Mengenbegriff

Eine Menge ist im Wesentlichen ein Beutel, der unterschiedliche Objekte enthält. Es gibt die leere Menge, das ist der leere Beutel. Das besondere an einer Menge ist nun, dass dasselbe Objekt immer nur ein einziges mal im Beutel enthalten ist. Legt man zweimal dasselbe Objekt in den Beutel, dann ist dieses darin trotzdem nur einmal zu finden.

Man kann sich dabei z. B. einen Einkaufsbeutel vorstellen, in welchem sich nur ein Apfel, eine Birne, eine Weintraube usw. befinden darf. Möchte man mehrere Birnen im Einkaufsbeutel haben, dann müssen diese unterschieden werden, z. B. indem jede Birne eine unterschiedliche Nummer bekommt.

Möchte man eine Menge aufschreiben, werden die Objekte einfach in einer beliebigen Reihenfolge aufgelistet und diese Liste in geschweifte Klammern gesetzt. Z. B.:

$$\{\text{Afpel}, \text{Birne}, \text{Weintraube}\}.$$

Nennen wir den Apfel A, die Birne B und die Weintraube W. Eine Menge mit zwei Äpfeln und drei Birnen würde man so schreiben:

$$\{A_1, A_2, B_1, B_2, B_3\}.$$

Erlaubt sind auch Beutel in Beuteln. Eine Menge mit zwei Äpfeln und einer Menge mit vier Weintrauben wird beschrieben durch

$$\{A_1, A_2, \{W_1, W_2, W_3, W_4\}\}.$$

Die Reihenfolge spielt wie gesagt keine Rolle:

$$\{A_1, A_2\} = \{A_2, A_1\}.$$

Ein leerer Beutel ist etwas anderes als ein Beutel, welcher einen leeren Beutel enthält:

$$\{\} \neq \{\{\}\}.$$

Die Notation $x \in M$ bedeutet, dass x in der Menge M enthalten ist. Man sagt, x ist ein Element von M. Z. B. ist

$$A_1 \in \{A_1, A_2\}.$$

2.3.2 Teilmengen

Definition 2.11. Teilmengenrelation.
Hat man zwei Mengen M, N, dann nennt man M eine Teilmenge von N, wenn jedes Element von M auch ein Element von N ist. Als Formel:

$$M \subseteq N \ :\Longleftrightarrow \text{ für jedes } x \in M \text{ gilt } x \in N.$$

Anders formuliert, aber gleichbedeutend:

$$M \subseteq N \ :\Longleftrightarrow \text{ für jedes } x \text{ gilt: } (x \in M \implies x \in N).$$

Z. B. ist die Aussage $\{1, 2\} \subseteq \{1, 2, 3\}$ wahr. Die Aussage $\{1, 2, 3\} \subseteq \{1, 2\}$ ist jedoch falsch, weil 3 kein Element von $\{1, 2\}$ ist. Für jede Menge M gilt $M \subseteq M$, denn die Aussage

$$x \in M \implies x \in M$$

ist immer wahr, da die Formel »$\varphi \Rightarrow \varphi$« tautologisch ist.

2.3.3 Mengen von Zahlen

Einige Mengen kommen häufiger vor, was dazu führte, dass man für diese Mengen kurze Symbole definiert hat.

Die Menge der natürlichen Zahlen mit der Null, kurz *nichtnegative* ganze Zahlen:

$$\mathbb{N}_0 := \{0, 1, 2, 3, 4, \ldots\}.$$

Die Menge der natürlichen Zahlen ohne die Null, kurz *positive* ganze Zahlen:

$$\mathbb{N}_1 := \{1, 2, 3, 4, \ldots\}.$$

Die Menge der ganzen Zahlen:

$$\mathbb{Z} := \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

Dann gibt es noch die rationalen Zahlen $\mathbb{Q}$, das sind alle Brüche der Form m/n, wobei m, n ganze Zahlen sind und $n \neq 0$ ist. Rationale Zahlen lassen sich immer als Dezimalbruch schreiben, dessen Ziffern irgendwann periodisch werden.

Zahl	als Dezimalzahl	kurz
$1/2$	$0.5000000000\ldots$	$0.5\overline{0}$
$1/3$	$0.3333333333\ldots$	$0.\overline{3}$
$1241/1100$	$1.1281818181\ldots$	$0.12\overline{81}$

Tabelle 2.4: Jeder Bruch lässt sich als Dezimalzahl schreiben, deren Ziffern in eine periodische Zifferngruppe münden. Über die periodische Zifferngruppe setzt man einen waagerechten Strich.

Schließlich gibt es noch die reellen Zahlen $\mathbb{R}$. Darin enthalten sind alle Dezimalzahlen – auch solche, deren Ziffern niemals in eine periodische Zifferngruppe münden. Die reellen Zahlen haben eine recht komplizierte Struktur, und wir benötigen Mittel der Analysis um diese verstehen zu können. Solange diese Werkzeuge noch nicht bekannt sind, kann man die reellen Zahlen einfach als kontinuierliche Zahlengerade betrachten. Die rationalen Zahlen haben Lücken in dieser Zahlengerade, z. B. ist die Zahl $\sqrt{2}$ nicht rational, wie sich zeigen lässt. Die reellen Zahlen schließen diese Lücken.

2.3.4 Vergleich von Mengen

Wie können wir denn wissen, wann zwei Mengen A, B, gleich sind? Zwei Mengen sind ja gleich, wenn sie beide die gleichen Elemente enthalten. Aber wie lässt sich das als mathematische Aussage formulieren?

Jedes Element von A muss doch auch ein Element von B sein, sonst gäbe es Elemente in A, die nicht in B enthalten wären. Umgekehrt muss auch jedes Element von B ein Element von A sein. Also ist $A \subseteq B$ und $B \subseteq A$ eine notwendige Bedingung. Diese Bedingung ist sogar hinreichend.

Gehen wir mal von der Kontraposition aus – sind die beiden Mengen A, B verschieden, dann muss es ein Element in A geben, welches nicht in B enthalten ist, oder eines in B, welches nicht A enthalten ist. Als Formel:

$$A \neq B \implies (\exists x \in A)(x \notin B) \vee (\exists x \in B)(x \notin A).$$

Hiervon bildet man wieder die Kontraposition. Gemäß den de morganschen Gesetzen und den verallgemeinerten de morganschen Gesetzen ergibt sich

$$(\forall x \in A)(x \in B) \wedge (\forall x \in B)(x \in A) \implies A = B.$$

Auf der linken Seite stehen aber nach Definition Teilmengenbeziehungen, es ergibt sich

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

Definition 2.12. Gleichheit von Mengen.
Zwei Mengen A, B sind genau dann gleich, wenn jedes Element von A auch in B enthalten ist, und jedes von B auch in A enthalten:

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

Satz 2.23. Es gilt

$$A = B \iff (\forall x)(x \in A \iff x \in B).$$

Beweis. Wir müssen ein wenig Prädikatenlogik bemühen:

$$\begin{aligned} A \subseteq B \wedge B \subseteq A &\iff (\forall x \in A)(x \in B) \wedge (\forall x \in B)(x \in A) \\ &\iff (\forall x)(x \in A \implies x \in B) \wedge (\forall x)(x \in B \implies x \in A) \\ &\iff (\forall x)((x \in A \implies x \in B) \wedge (x \in B \implies x \in A)) \\ &\iff (\forall x)(x \in A \iff x \in B). \end{aligned}$$

Im letzten Schritt wurde ausgenutzt, dass die Äquivalenz $\varphi \Leftrightarrow \psi$ gleichbedeutend mit der Formel $(\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi)$ ist. □

2.3.5 Beschreibende Angabe von Mengen

Umso mehr Elemente eine Menge enthält, umso umständlicher wird die Auflistung all dieser Elemente. Außerdem hantiert man in der Mathematik normalerweise auch ständig mit Mengen herum, die unendlich viele Elemente enthalten. Eine explizite Auflistung ist demnach unmöglich.

Wir entgehen der Auflistung aller Elemente durch eine Beschreibung der Menge. Die Menge der ganzen Zahlen, welche kleiner als vier sind, wird so beschrieben:

$$\{n \in \mathbb{Z} \mid n < 4\}.$$

In Worten: Die Menge der $n \in \mathbb{Z}$, für die gilt: $n < 4$.

Mit dieser Notation kann man nun z. B. schreiben:

$$\mathbb{N}_0 = \{n \in \mathbb{Z} \mid n \geq 0\},$$
$$\mathbb{N}_1 = \{n \in \mathbb{Z} \mid n > 0\}.$$

Mit der folgenden formalen Definition wird die beschreibende Angabe auf ein festes Fundament gebracht.

Definition 2.13. Beschränkte Beschreibung einer Menge.
Die Menge der $x \in M$, welche die Aussage $P(x)$ erfüllen, ist definiert durch die folgende logische Äquivalenz:

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

Das schaut ein wenig kompliziert aus, ist aber ganz einfach zu benutzen. Sei z. B. $A := \{n \in \mathbb{Z} \mid n < 4\}$. Zu beantworten ist die Frage, ob $2 \in A$ gilt. Eingesetzt in die Definition ergibt sich

$$2 \in \{n \in \mathbb{Z} \mid n < 4\} \iff 2 \in \mathbb{Z} \wedge 2 < 4.$$

Da $2 \in \mathbb{Z}$ und $2 < 4$ wahre Aussagen sind, ist die rechte Seite erfüllt, und damit auch die linke Seite der Äquivalenz.

Die geraden Zahlen lassen sich so definieren:

$$2\mathbb{Z} := \{n \in \mathbb{Z} \mid \text{es gibt ein } k \in \mathbb{Z} \text{ mit } n = 2k\}.$$

Es lässt sich zeigen:

$$a \in 2\mathbb{Z} \implies a^2 \in 2\mathbb{Z}.$$

Nach Definition von $2\mathbb{Z}$ gibt es $k \in \mathbb{Z}$ mit $a = 2k$. Dann ist $a^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Benennt man $k' := 2k^2$, dann gilt also $a^2 = 2k'$. Also gibt es es ein $k' \in \mathbb{Z}$ mit $a^2 = 2k'$, und daher ist $a^2 \in 2\mathbb{Z}$.

Die geraden Zahlen sind ganze Zahlen, welche ohne Rest durch zwei teilbar sind. Die ganzen Zahlen, welche ohne Rest durch m teilbar sind, lassen sich formal so definieren:

$$m\mathbb{Z} := \{n \in \mathbb{Z} \mid \text{es gibt ein } k \in \mathbb{Z} \text{ mit } n = mk\}.$$

Man zeige:

(1.) $a \in 2\mathbb{Z} \implies a^2 \in 4\mathbb{Z}$,
(2.) $a \in 4\mathbb{Z} \implies a \in 2\mathbb{Z}$,
(3.) $2\mathbb{Z} \subseteq \mathbb{Z}$,
(4.) $4\mathbb{Z} \subseteq 2\mathbb{Z}$.

Definition 2.14. Beschreibende Angabe einer Menge.
Stellt man sich unter G die Grundmenge vor, welche alle Elemente enthält, die überhaupt in Betracht kommen können, dann schreibt man kurz

$$\{x \mid P(x)\} := \{x \in G \mid P(x)\}$$

und nennt dies die Beschreibung einer Menge.

Satz 2.24. Es gilt

$$a \in \{x \mid P(x)\} \iff P(a), \tag{2.52}$$
$$\{x \in A \mid P(x)\} = \{x \mid x \in A \wedge P(x)\}. \tag{2.53}$$

Beweis. Gemäß Definition 2.14 und 2.13 gilt

$$a \in \{x \mid P(x)\} \iff a \in \{x \in G \mid P(x)\} \iff a \in G \wedge P(a) \iff P(a),$$

denn $a \in G$ ist immer erfüllt, wenn G die Grundmenge ist. Die Aussage $a \in G$ kann daher in der Konjunktion gemäß dem Neutralitätsgesetz der booleschen Algebra entfallen.

Aussage (2.53) wird mit Satz 2.23 expandiert. Zu zeigen ist nun

$$a \in \{x \in A \mid P(x)\} \iff a \in \{x \mid x \in A \wedge P(x)\},$$

was gemäß Definition 2.13 und der schon bewiesenen Aussage (2.52) aber vereinfacht werden kann zu

$$a \in A \wedge P(a) \iff a \in A \wedge P(a). \square$$

2.3.6 Bildmengen

Oft kommt auch die Angabe einer Menge als Bildmenge vor, dabei handelt es sich um eine spezielle Beschreibung der Menge. Ist $T(x)$ ein Term und $A := \{a_1, a_2, \ldots, a_n\}$ eine endliche Menge, dann wird das Bild von A unter $T(x)$ so beschrieben:

$$\{T(x) \mid x \in A\} := \{T(a_1), T(a_2), \ldots, T(a_n)\}.$$

Lies: Die Menge der $T(x)$, für die $x \in A$ gilt. Für $T(x) := x^2$ und $A := \{1, 2, 3, 4\}$ ist z. B.

$$\{T(x) \mid x \in A\} = \{T(1), T(2), T(3), T(4)\} = \{1^2, 2^2, 3^2, 4^2\} = \{1, 4, 9, 16\}.$$

Nun kann es aber sein, dass die Menge A unendlich viele Elemente enthält, eine Auflistung dieser somit unmöglich ist. Eine Auflistung lässt sich umgehen, indem man nur logisch die Existenz eines Bildes zu jedem $x \in A$ verlangt, dieses aber nicht mehr explizit angibt. Man definiert also allgemein

$$\{T(x) \mid x \in A\} := \{y \mid \text{es gibt ein } x \in A, \text{für das gilt: } y = T(x)\}.$$

Das hatten wir bei den geraden Zahlen

$$2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\} = \{n \mid \text{es gibt ein } k \in \mathbb{Z}, \text{für das gilt: } n = 2k\}$$

schon kennengelernt. Hierbei ist es unwesentlich, ob man $n \in \mathbb{Z}$ verlangt oder nicht, denn dies wird bereits durch $k \in \mathbb{Z}$ erzwungen.

Man spricht auch von einer sogenannten *Komprehension*, die Bildung einer Bildmenge ist ein Spezialfall davon.

Definition 2.15. Komprehension. Für ein beliebiges Prädikat P ist

$$\{T(x) \mid P(x)\} := \{y \mid (\exists x)(P(x) \wedge y = T(x))\}.$$

Die zuvor angegebene Bildmenge erhält man mit $P(x) := (x \in A)$.

In dieser Definition muss $P(x)$ auf der gesamen betrachteten Grundmenge G definiert sein und $T(x)$ muss auf $\{x \in G \mid P(x)\}$ einen Sinn ergeben. Möchte man sich auf die Menge M beschränken, dann betrachtet man

$$\{T(x) \mid x \in M \wedge P(x)\} = \{y \mid (\exists x \in M)(P(x) \wedge y = T(x))\}.$$

D. h. für ein auf M definiertes Prädikat P ergibt sich ein auf ganz G definiertes Prädikat Q mit $P(x) = Q(x)$ auf M und sonst $Q(x) = 0$, indem man $Q(x) := (x \in M \wedge P(x))$ setzt.

2.3.7 Mengenoperationen

Mengen sind mathematische Objekte, mit denen sich rechnen lässt. So wie es für Zahlen Rechenoperationen gibt, gibt es auch für Mengen Rechenoperationen.

Definition 2.16. Vereinigungsmenge.
Die Vereinigungsmenge von zwei Mengen A, B ist die Menge aller Elemente, welche in A oder in B vorkommen:

$$A \cup B := \{x \mid x \in A \vee x \in B\}.$$

Man nimmt also einen neuen Beutel und schüttet den Inhalt von A und B in diesen Beutel.
Beispiele:

$$\{1,2\} \cup \{5,7,9\} = \{1,2,5,7,9\},$$
$$\{1,2\} \cup \{1,3,5\} = \{1,2,3,5\}.$$

Definition 2.17. Schnittmenge.
Die Schnittmenge von zwei Mengen A, B ist die Menge aller Elemente, welche sowohl in A also auch in B vorkommen:

$$A \cap B := \{x \mid x \in A \wedge x \in B\}.$$

Satz 2.25. Bei der Beschreibung der Schnittmenge $A \cap B$ genügt es, $A \cup B$ als Grundmenge zu verwenden, denn es gilt

$$A \cap B = \{x \in A \cup B \mid x \in A \wedge x \in B\}$$

Beweis. Die Formel wird mit Satz 2.23 expandiert. Zu zeigen ist demnach

$$a \in A \cap B \iff a \in \{x \in A \cup B \mid x \in A \wedge x \in B\}.$$

Das ist nach (2.52) und Definition 2.13 gleichbedeutend mit

$$\begin{aligned} a \in A \wedge a \in B &\iff a \in A \cup B \wedge a \in A \wedge a \in B \\ &\iff (a \in A \vee a \in B) \wedge a \in A \wedge a \in B. \end{aligned}$$

Nun gilt für beliebige Aussagen φ, ψ gemäß boolescher Algebra aber

$$\begin{aligned} (\varphi \vee \psi) \wedge \varphi \wedge \psi &\iff (\varphi \wedge \varphi \wedge \psi) \vee (\psi \wedge \varphi \wedge \psi) \\ &\iff (\varphi \wedge \psi) \vee (\varphi \wedge \psi) \\ &\iff \varphi \wedge \psi. \end{aligned}$$

Auf beiden Seiten der Äquivalenz steht jetzt die gleiche Aussage:

$$a \in A \wedge a \in B \iff a \in A \wedge a \in B. \quad \square$$

Definition 2.18. Vereinigung beliebig vieler Mengen.
Sei M eine Menge von Mengen. Die Vereinigung der $A \in M$ ist definiert gemäß

$$\bigcup M = \bigcup_{A \in M} A := \{x \mid (\exists A)(A \in M \wedge x \in A)\}.$$

Für $M = \{\}$ ist $\bigcup_{A \in M} A = \{\}$.

Das logische ODER findet seine 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 lassen sich Regeln der booleschen Algebra direkt auf die Mengenoperationen übertragen. Z. B. lautet das Distributivgesetz für Mengen

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

Diese Gleichung lässt sich nämlich expandieren in die logische Formel

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

Die Äquivalenz ist wie gesagt gültig gemäß Satz 2.21.

Definition 2.19. Schnitt beliebig vieler Mengen.
Sei M eine nichtleere Menge von Mengen. Der Schnitt der $A \in M$ ist definiert gemäß

$$\bigcap M = \bigcap_{A \in M} A := \{x \mid (\forall A)(A \in M \Rightarrow x \in A)\}.$$

Im Gegensatz zur Vereinigung wurde der Schnitt $\bigcap_{A \in M} A$ für $M = \{\}$ undefiniert gelassen. Hier gibt es zwei Möglichkeiten. Zum einen könnte man die Bedingung $M \neq \{\}$ einfach fallen lassen, dann ergibt sich beim leeren Schnitt immer die Grundmenge $G = \{x \mid 1\}$. Im allgemeinen Mengenuniversum ist G die Allklasse. Diese ist nach den ZFC-Axiomen jedoch keine Menge mehr.

Aus diesen Grund gibt es noch die alternative Definition

$$\bigcap_{A \in M} A := \{x \in \bigcup_{A \in M} A \mid (\forall A)(A \in M \Rightarrow x \in A)\}.$$

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 dafür

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

wobei mit $A(I)$ das Bild von I unter A gemeint ist. Gemäß Def. 2.24 bekommt man

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

Für $I \neq \{\}$ definiert man entsprechend

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

Definition 2.20. Differenzmenge.
Für zwei Mengen A, B ist $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$.

Definition 2.21. Komplementärmenge.
Ist G eine festgelegte Grundmenge und $A \subseteq G$, dann ist $A^{\mathrm{c}} := G \setminus A$.

Die Komplementärmenge entspricht der logischen Negation, denn

$$A^{\mathrm{c}} = \{x \mid x \in G \wedge x \notin A\} = \{x \in G \mid x \notin A\}.$$

Hat man eine Grundmenge festgelegt, so dass alle betrachteten Mengen Teilmengen dieser Grundmenge sind, dann genügen die Operationen A^{c}, $A \cap B$, $A \cup B$ den gleichen Regeln wie ihre logischen Entsprechungen $\neg A$, $A \wedge B$, $A \vee B$. Nämlich bilden diese eine boolesche Algebra. Definiert man axiomatisch, was unter einer booleschen Algebra zu verstehen ist, dann lassen sich damit Regeln herleiten, die sowohl für die Aussagenlogik als auch für die Mengenlehre gültig sein müssen.

Um eine axiomatische Präzisierung kümmern wir uns später. Zunächst übertragen wir weitere wichtige Rechenregeln ausgehend von der Aussagenlogik.

Aus $\neg\neg A \equiv A$ für eine Aussage A folgt $(A^{\mathrm{c}})^{\mathrm{c}} = A$ für eine Menge A, denn

$$\begin{aligned} x \in (A^{\mathrm{c}})^{\mathrm{c}} &\iff x \in G \wedge \neg x \in \{x \mid x \in G \wedge \neg x \in A\} \\ &\iff x \in G \wedge \neg(x \in G \wedge \neg x \in A) \iff x \in G \wedge (\neg x \in G \vee \neg\neg x \in A) \\ &\iff 0 \vee x \in G \wedge x \in A \iff x \in G \wedge x \in A \iff x \in A. \end{aligned}$$

Die letzte Äquivalenz gilt wegen $A \subseteq G$. Käme die Grundmenge dabei nicht in den Weg, würde sich die Rechnung zu

$$x \in (A^{\mathrm{c}})^{\mathrm{c}} \iff \neg x \in \{x \mid \neg x \in A\} \iff \neg\neg x \in A \iff x \in A$$

vereinfachen. Zum einen müsste man dann aber die Allklasse als »Grundmenge« benutzen, zum anderen ist die Regel so nicht für jede beliebige Grundmenge G mit $A \subseteq G$ gezeigt.

Die trivialen Regeln $\{\}^{\mathrm{c}} = G$ und $G^{\mathrm{c}} = \{\}$ entsprechen $\neg 0 \equiv 1$ und $\neg 1 \equiv 0$. Dem logischen Wert wahr entspricht demnach die Grundmenge und dem logischen Wert falsch die leere Menge.

Der Leser zeige zur Übung auch die Übertragung der de morganschen Gesetze

$$(A \cup B)^{\mathrm{c}} = A^{\mathrm{c}} \cap B^{\mathrm{c}}, \qquad (A \cap B)^{\mathrm{c}} = A^{\mathrm{c}} \cap B^{\mathrm{c}}.$$

Die Komplementärgesetze:

$$A \cup A^{\mathrm{c}} = G, \qquad A \cap A^{\mathrm{c}} = \{\}.$$

Der Kontraposition entspricht die Formel $A^{\mathrm{c}} \cup B = (B^{\mathrm{c}})^{\mathrm{c}} \cup A^{\mathrm{c}}$. Im Zusammenhang mit der Teilmengenrelation hat die Kontraposition aber auch noch ein anderes Analogon, das ist

$$A \subseteq B \iff B^{\mathrm{c}} \subseteq A^{\mathrm{c}}.$$

2.3.8 Produktmengen

Zwei Objekte a, b kann man zu einem geordneten Paar (a, b) zusammenfassen. Zwei Paare sind definitionsgemäß genau dann gleich, wenn sie komponentenweise gleich sind:

$$(a_1, b_1) = (a_2, b_2) \ :\Longleftrightarrow\ a_1 = a_2 \wedge b_1 = b_2.$$

Definition 2.22. Kartesisches Produkt.
Das kartesische Produkt der Mengen A, B ist die Menge der Paare (a, b), für die $a \in A$ und $b \in B$ ist, kurz

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

Zu beachten ist, dass hier eine Bildmenge vorliegt, d. h. es gilt

$$\begin{aligned} A \times B &= \{t \mid (\exists a \in A)(\exists b \in B)(t = (a, b))\} \\ &= \{t \mid (\exists a)(\exists b)(a \in A \wedge b \in B \wedge t = (a, b))\}. \end{aligned}$$

Satz 2.26. Für das kartesische Produkt mit der leeren Menge gilt $A \times \emptyset = \emptyset$ und $\emptyset \times B = \emptyset$.

Beweis. Das kann man einfach nachrechnen. Unter Anwendung von Satz 2.23 und (2.52) bekommt man zunächst die äquivalente Aussage

$$t \in A \times \emptyset \iff (\exists a)(\exists b)(a \in A \wedge b \in \emptyset \wedge t = (a, b)).$$

Nun ist aber $b \in \emptyset$ niemals wahr, da die leere Menge keine Elemente enthält. Demnach ergibt sich

$$(\exists a)(\exists b)(a \in A \wedge b \in \emptyset \wedge t = (a, b)) \iff (\exists a)(\exists b)\, 0 \iff (\exists a)\, 0 \iff 0.$$

Die Aussage $t \in A \times \emptyset$ ist also immer falsch, daher kann $A \times \emptyset$ keine Elemente enthalten. □

Satz 2.27. Ist $A \subseteq X$ und $B \subseteq Y$, dann ist $A \times B \subseteq X \times Y$.

Beweis. Sei t ein Paar, das in $A \times B$ enthalten ist. Dann gibt es nach Definition $a \in A$ 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 gibt es $a \in X$ und $b \in Y$, so dass $t = (a, b)$. Gemäß Definition heißt das $t \in X \times Y$. Gemäß Definition ist $A \times B$ daher eine Teilmenge von $X \times Y$. □

2.4 Abbildungen

2.4.1 Grundbegriffe

Seien zwei beliebige Mengen A, B gegeben. Eine Abbildung $f : A \to B$ ist eine Zuordnung, die jedem Element $x \in A$ genau ein Element $y \in B$ zuordnet. Man schreibt $y = f(x)$ oder $x \mapsto y$, um auszudrücken, dass dem Element x das Element y zugeordnet wird.

Ausgesprochen wird $f(x)$ als »f von x«, oder auch »das Bild von x unter f«. Die Schreibweise $x \mapsto y$ wird ausgesprochen als »x zu y«, oder auch »x wird abgebildet auf y«. Die Schreibweise $f : A \to B$ wird ausgesprochen als »f ist eine Abbildung von A nach B«.

Man nennt A die Definitionsmenge oder den Definitionsbereich der Abbildung und B die Zielmenge der Abbildung. Gibt es zu einem $y \in B$ ein $x \in A$, so dass $y = f(x)$, dann nennt man x ein Urbildelement zu y.

Abbildungen sind für die Mathematik fundamental. Eine Formalisierung dieses Begriffs mittels Prädikatenlogik und Mengenlehre erscheint deshalb erstrebenswert.

Definition 2.23. Abbildung.
Sei $G \subseteq A \times B$. Man nennt ein Tripel $f = (G, A, B)$ eine Abbildung, wenn die folgenden zwei Bedingungen erfüllt sind. 1. Zu jedem $x \in A$ gibt es mindestens ein Bild:

$$(\forall x \in A)(\exists y \in B)((x, y) \in G).$$

2. Zu jedem $x \in A$ gibt es höchstens ein Bild:

$$(\forall (x_1, y_1), (x_2, y_2) \in G)(x_1 = x_2 \implies y_1 = y_2).$$

Man definiert außerdem

$$y = f(x) \ :\Longleftrightarrow \ (x, y) \in G.$$

Definition 2.24. Bildmenge.
Sei $f : A \to B$ eine Abbildung. Für eine Menge $M \subseteq A$ nennt man die Menge

$$f[M] := \{y \mid (\exists x \in M)(y = f(x))\}$$

das Bild von M unter f.

Definition 2.25. Urbildmenge.
Sei $f : A \to B$ eine Abbildung. Für eine Menge N nennt man

$$f^{-1}[N] := \{x \in A \mid f(x) \in N\}$$

das Urbild von N bezüglich f.

Sofern keine Verwechslungsgefahr besteht, benutzt man auch die Schreibweise $f(M)$ anstelle von $f[M]$ bzw. $f^{-1}(N)$ anstelle von $f^{-1}[N]$.

Die Urbildoperation zeichnet sich durch Verträglichkeit mit Mengenoperationen aus, wie im Folgenden nachgerechnet wird. Man könnte nun denken, diese Verträglichkeiten müssten auch für die Bildoperation gelten, was jedoch nur zum Teil stimmt.

Korollar 2.28. Für jede beliebige Abbildung f gilt:

$$\begin{aligned} f^{-1}[B_1 \cup B_2] &= f^{-1}[B_1] \cup f^{-1}[B_2], \\ f^{-1}[B_1 \cap B_2] &= f^{-1}[B_1] \cap f^{-1}[B_2], \\ f^{-1}[B_1 \setminus B_2] &= f^{-1}[B_1] \setminus f^{-1}[B_2]. \end{aligned}$$

Beweis. Es gilt

$$\begin{aligned} x \in f^{-1}[B_1 \cup B_2] &\iff f(x) \in B_1 \cup B_2 \iff f(x) \in B_1 \vee f(x) \in B_2 \\ &\iff x \in f^{-1}[B_1] \vee x \in f^{-1}[B_2] \iff x \in f^{-1}[B_1] \cup f^{-1}[B_2]. \end{aligned}$$

Beim Schnitt ist die Rechnung analog. Und es gilt

$$\begin{aligned} x \in f^{-1}[B_1 \setminus B_2] &\iff f(x) \in B_1 \setminus B_2 \iff f(x) \in B_1 \wedge \neg f(x) \in B_2 \\ &\iff x \in f^{-1}[B_1] \wedge \neg x \in f^{-1}[B_2] \iff x \in f^{-1}[B_1] \setminus f^{-1}[B_2]. \end{aligned}$$ □

Allgemeiner sind diese Verträglichkeiten sogar für Vereinigungen und Schnitte von unendlich vielen Mengen gültig.

Korollar 2.29. Für jede beliebige Abbildung f gilt:

$$\begin{aligned} f^{-1}[\bigcup_{i \in I} B_i] &= \bigcup_{i \in I} f^{-1}[B_i], \\ f^{-1}[\bigcap_{i \in I} B_i] &= \bigcap_{i \in I} f^{-1}[B_i]. \end{aligned}$$

Beweis. Es gilt

$$\begin{aligned} x \in f^{-1}[\bigcup_{i \in I} B_i] &\iff f(x) \in \bigcup_{i \in I} B_i \iff (\exists i \in I)(f(x) \in B_i) \\ &\iff (\exists i \in I)(x \in f^{-1}[B_i]) \iff x \in \bigcup_{i \in I} f^{-1}[B_i]. \end{aligned}$$

Für den Schnitt ist das wieder analog. □

Diese Beweise waren ziemlich angenehm zu führen, vergleichsweise fast ein Kinderspiel, braucht man doch ohne viel Nachdenken lediglich dem Formalismus folgen. Wer besonders spitzfindig ist, mag darin allerdings die fehlende Definition für »$f(x) \in B$« erkennen. Wir haben zwar $y = f(x)$ definiert als $(x, y) \in f$, allerdings nicht $f(x)$ als solches. Die Bedeutung von $f(x)$ mag klar sein, aber wir wollen ja so gut es geht alle Formeln zu prädikatenlogischen Ausdrücken reduzieren können, die nur vorher bereits definierte Begriffe enthalten. Nun siehe da, aus dem Kaninchenbau kommen neue Quantoren hervor, die die Argumentation ein wenig verkomplizieren:

$$f(x) \in B \ :\iff \ (\exists y \in B)(y = f(x)).$$

Wir müssen nun zeigen

$$f(x) \in B_1 \cap B_2 \iff f(x) \in B_1 \wedge f(x) \in B_2.$$

Expandiert man dies, ist zu zeigen

$$(\exists y)(y \in B_1 \wedge y \in B_2 \wedge y = f(x)) \iff (\exists y)(y \in B_1 \wedge y = f(x)) \wedge (\exists y)(y \in B_2 \wedge y = f(x)).$$

Die Implikation von links nach rechts ist wahr, denn es gilt ganz allgemein

$$(\exists y)(P(y) \wedge Q(y)) \implies (\exists y)P(y) \wedge (\exists y)Q(y).$$

Zur Bestätigung der Implikation von rechts nach links muss man allerdings die Bedingung $y = f(x)$ ausnutzen. Nur dadurch ist gesichert, dass das $y \in B_1$ das gleiche ist wie das $y \in B_2$.

2.4.2 Verkettung von Abbildungen

Definition 2.26. Verkettung.
Sei $f\colon A \to B$ und $g\colon B \to C$. Die Abbildung

$$(g \circ f)\colon A \to C, \quad (g \circ f)(x) := g(f(x))$$

heißt Verkettung von f und g, sprich »g nach f«.

Oft hat man die Situation vorliegen, bei der $f\colon A \to B$ und $g\colon B' \to C$, wobei $B \subseteq B'$ ist. Das ist aber nicht so schlimm. Man nimmt die folgende unproblematische Definitionserweiterung vor:

$$(g \circ f)\colon A \to C, \quad g \circ f := g|_B \circ f.$$

Mit $g|_B$ ist hierbei die Einschränkung der Abbildung g auf den Definitionsbereich B gemeint.

Definition 2.27. Einschränkung.
Für $f\colon A \to B$ und $M \subseteq A$ nennt man

$$f|_M\colon M \to B, \quad f|_M(x) := f(x)$$

die Einschränkung von f auf M.

Schwerwiegender ist die Situation $f\colon A \to B$ und $g\colon B' \to C$ mit $B' \subseteq B$. Hier dürfen nur solche $x \in A$ im neuen Definitionsbereich vorkommen, bei denen $f(x) \in B'$ ist. Gemäß der Definition des Urbildes gilt wiederum

$$f(x) \in B' \iff x \in f^{-1}(B').$$

Man kann nun die Verkettung definieren gemäß

$$h\colon f^{-1}(B') \to C, \quad h(x) := g(f(x)).$$

Satz 2.30. Bildmenge unter Verkettung.
Seien $f : A \to B$ und $g : B \to C$, dann gilt $(g \circ f)[M] = g[f[M]]$.

Beweis. Die Gleichung gemäß Definition expandieren:

$$(\exists x)(x \in M \land z = (g \circ f)(x)) \iff (\exists y)(y \in f[M] \land z = g(y)).$$

Auf der rechten Seite ergibt sich nun

$$\begin{aligned}
&(\exists y)(y \in f[M] \land z = g(y)) \equiv (\exists y)((\exists x)(x \in M \land y = f(x)) \land z = g(y)) \\
&\equiv (\exists y)(\exists x)(x \in M \land y = f(x) \land z = g(y)) \\
&\equiv (\exists x)(x \in M \land (\exists y)(y = f(x) \land z = g(y))) \\
&\equiv (\exists x)(x \in M \land z = g(f(x))). \square
\end{aligned}$$

Bei der Urbildoperation dreht sich die Reihenfolge um.

Satz 2.31. Urbildmenge unter Verkettung.
Seien $f : A \to B$ und $g : B \to C$, dann gilt $(g \circ f)^{-1}[N] = f^{-1}[g^{-1}[N]]$.

Beweis. Es gilt

$$\begin{aligned}
x \in (g \circ f)^{-1}[N] &\iff (g \circ f)(x) \in N \iff g(f(x)) \in N \\
&\iff f(x) \in g^{-1}[N] \iff x \in f^{-1}[g^{-1}[N]]. \square
\end{aligned}$$

2.4.3 Injektionen, Surjektionen, Bijektionen

Definition 2.28. Injektive Abbidlung.
Eine Abbildung $f : A \to B$ heißt injektiv, wenn

$$(\forall x_1, x_2 \in A)(f(x_1) = f(x_2) \implies x_1 = x_2)$$

bzw.

$$(\forall x_1, x_2 \in A)(x_1 \neq x_2 \implies f(x_1) \neq f(x_2)).$$

Definition 2.29. Surjektive Abbildung.
Eine Abbildung $f : A \to B$ heißt surjektiv, wenn $f(A) = B$ ist.

Bemerkung: Da immer $f(A) \subseteq B$ ist, braucht man bloß $B \subseteq f(A)$ zu zeigen.

Definition 2.30. Bijektive Abbildung.
Eine Abbildung heißt bijektiv, wenn sie sowohl injektiv als auch surjektiv ist.

Satz 2.32. Sei $f\colon A \to B$ und $g\colon B \to C$. Es gilt:

1. Sind f und g injektiv, dann auch $g \circ f$.
2. Sind f und g surjektiv, dann auch $g \circ f$.
3. Sind f und g bijektiv, dann auch $g \circ f$.

Beweis. Mühelos. Seien f, g injektiv, dann gilt

$$\begin{aligned} & g(f(x_1)) = (g \circ f)(x_1) = (g \circ f)(x_2) = g(f(x_2)) \\ \implies\ & f(x_1) = f(x_2) \\ \implies\ & x_1 = x_2. \end{aligned}$$

Somit ist auch $g \circ f$ injektiv. Seien f, g nun surjektiv, dann ergibt sich

$$(g \circ f)(A) = g(f(A)) = g(B) = C$$

gemäß Satz 2.30. Somit ist auch $g \circ f$ surjektiv. □

2.4.4 Allgemeines Produkt von Mengen

Die folgende Begriffsverallgemeinerung des Produktes von Mengen ist eigentlich erst in der Kardinalzahlarithmetik bedeutsam, rundet allerdings als intuitiv deutbarer Hilfsbegriff das Verständnis ab.

Entsprechend dem Produkt von zwei Mengen ist das Produkt von n Mengen die Menge der n-Tupel, das ist

$$\prod_{k=1}^{n} A_k := \{(a_1, \ldots, a_n) \mid (\forall k)\ a_k \in A_k\}. \tag{2.54}$$

Sei $K := \{1, \ldots, n\}$. Die n-Tupel sind Funktionen $f\colon K \to \bigcup_{k\in K} A_k$ mit $f(k) \in A_k$. Offenbar besteht die Produktmenge aus allen solchen Funktionen. Die Definition lässt sich demnach umformulieren zu

$$\prod_{k\in K} A_k := \{f\colon K \to \bigcup_{k\in K} A_k \mid (\forall k \in K)\, f(k) \in A_k\}. \tag{2.55}$$

So unschuldig die letzte Umformulierung auch daher kam, hält uns nun nichts mehr davon ab, für K eine beliebige Menge einzusetzen.

Die Elemente der Produktmenge nennt man Auswahlfunktionen. Ist also $(A_k)_{k\in K}$ eine Familie von Mengen, wählt eine Auswahlfunktion f dazu für jeden »Index« $k \in K$ ein $f(k) \in A_k$ aus.

Die intuitiv klar erscheinende Überlegung

$$(\forall k \in K)(A_k \neq \emptyset) \implies \prod_{k\in K} A_k \neq \emptyset \tag{2.56}$$

hat es in sich, sie wird als *Auswahlaxiom* bezeichnet. Man hat herausgefunden, dass dieses Axiom wahr oder auch falsch sein darf, ohne dabei im Widerspruch zu den übrigen Axiomen

der ZFC-Mengenlehre zu stehen. Der Spezialfall $K \subseteq \mathbb{N}_0$ wird als *abzählbares Auswahlaxiom* bezeichnet.

Für das Produkt einer konstanten Mengenfamilie gilt

$$A^K := \prod_{k \in K} A = \mathrm{Abb}(K, A). \tag{2.57}$$

2.5 Relationen

2.5.1 Grundbegriffe

Definition 2.31. Relation.
Seien A, B zwei Mengen und sei $G \subseteq A \times B$. Das Tripel $R = (G, A, B)$ heißt Relation zwischen A und B. Man schreibt

$$R(x, y) \ :\Longleftrightarrow \ (x, y) \in G.$$

Eine Relation lässt sich natürlich als wahrheitswertige Funktion interpretieren:

$$R\colon A \times B \to \{0, 1\}, \quad R(x, y) := ((x, y) \in G).$$

Eine Relation ist somit auch ein Prädikat auf $A \times B$.

2.5.2 Äquivalenzrelationen

Definition 2.32. 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 2.33. 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 2.33. 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

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

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

Satz 2.34. 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 $A_i \cap A_j = \{\}$ für $i \neq j$ ist. Dann ist

$$x \sim y \;:\Longleftrightarrow\; (\exists k)(x \in A_k \wedge y \in A_k)$$

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

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

Wegen

$$A_i \cap A_j = \{\} \iff (\forall y)(y \in A_i \wedge y \in A_j \iff 0)$$

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

$$(\exists i)(x \in A_i \wedge z \in A_i),$$

d. h. $x \sim z$. □

Definition 2.34. 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 2.35. Quotientenabbildung.
Für eine gegebene Äquivalenzrelation ist die Projektion

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

surjektiv und wird Quotientenabbildung genannt.

Definition 2.36. 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 2.35. 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. $x \in A \wedge y \in M \wedge x \sim y \implies y \in A$.

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 $f\colon M \to N$, 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

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

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

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

Ist f zudem surjektiv, dann gehört zu jedem Element von N genau eine Äquivalenzklasse. Demnach definiert f dann eine verallgemeinerte Quotientenabbildung, da die Elemente von N die Äquivalenzklassen charakterisieren. Die Bijektion $\varphi\colon Z \to N$ hat dabei die Eigenschaft $f = \varphi \circ \pi$. Sofern N 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 N ein vollständiges Repräsentantensystem.

Was bisher erläutert wurde mag recht abstrakt erscheinen. Wir haben aber eigentlich ein recht intuitives Verständnis für diese Begrifflichkeiten. Das typische Beispiel für eine Äquivalenzrelation ist, wenn zwei Schüler in die gleiche Schulklasse gehen. Die Äquivalenzklasse ist dann schlicht diese Schulklasse. Die Menge der Schüler der Schule wird in disjunkte Schulklassen zerlegt. Die Menge dieser Schulklassen bildet die Quotientenmenge. Ein vollständiges Repräsentantensystem ist z. B. 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.

Äquivalenzrelationen haben in der Mathematik eine fundamentale Bedeutung, da sie den Begriff der Gleichheit abstrahieren und verallgemeinern. Wir können nun umgekehrt den philosophischen Standpunkt einnehmen, dass es Identität in der wirklichen Welt, was damit auch immer gemeint sein soll, nirgendwo gibt, dass die Welt also überall eine reichhaltige Tiefe besitzt mit welcher keine zwei Dinge dieselben sind. Ein Vergleich setzt dann von vornherein eine Äquivalenzrelation voraus. Man könnte einwenden, in unserem Kosmos sei eine in die Hand genommene Tasse dieselbe Tasse. Dies ist aber wieder bloß eine Relation zwischen zwei Objekten in der Raumzeit. Die Tasse ist außerdem eine Ansammlung von Atomen, die sich in diesem Zeitraum wahrscheinlich an irgendeiner Stelle verändert haben wird. Ein neuerlicher Einwand wäre, dass eine Struktur in der Raumzeit identisch zu sich selbst sein muss. Diese Struktur ist denkbar, aber für uns niemals so zugänglich, als würden wir eine Tasse in die Hand nehmen und betrachten.

Diesem Gedankengang liegt die Idee zugrunde, dass es zu jeder Äquivalenzrelation weitere Äquivalenzrelationen gibt, welche die Äquivalenzklassen wiederum in feinere Äquivalenzklassen zerlegen. Die unendliche Fortsetzung von Verfeinerungen setzt voraus, dass jede Äquivalenzklasse unendlich groß ist. In dieser Vorstellung einer wirklichen Welt gibt es daher nichts was endlich wäre.

2.5.3 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

$$f\colon M/\sim \longrightarrow M'/\sim',\ f([a]) := [f(a)] \tag{2.58}$$

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

$$\forall x \in [a]\colon f(x) \in [f(a)] \tag{2.59}$$

muss erfüllt sein. Anders formuliert:

$$x \sim a \implies f(x) \sim' f(a). \tag{2.60}$$

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

$$f\colon (M/\sim)^2 \to M'/\sim',\ f([a],[b]) := [f(a,b)], \tag{2.61}$$

sofern

$$x \sim a \wedge y \sim b \implies f(x,y) \sim' f(a,b). \tag{2.62}$$

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.

2.5.4 Kongruenzrelationen

Definition 2.37. 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 2.36. 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 2.37. Satz 2.36 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 2.36 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 2.36 hervorgeht. □

3 Elemente der Algebra

3.1 Gruppentheorie

3.1.1 Elementare Gesetzmäßigkeiten

Definition 3.1. 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 3.2. 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 $(\forall a, b \in G)(a * b = b * a)$ erfüllt ist.

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

Satz 3.1. 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 3.2. In jeder Gruppe gilt die Linkskürzbarkeit $ga = gb \implies a = b$ und die Rechtskürzbarkeit $ag = bg \implies a = b$.

Beweis. Die Gleichung $ga = gb$ multipliziert man auf beiden Seiten mit g^{-1}, dann gilt

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

Für die Gleichung $ag = bg$ geht das 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

$$l_g : G \to G, \quad l_g(x) := gx, \tag{3.1}$$
$$r_g : G \to G, \quad r_g(x) := xg \tag{3.2}$$

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 3.3. Zu jedem Element ist das inverse Element eindeutig bestimmt, d. h. 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 3.3. 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 3.4. 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 3.4. Homomorphismus zwischen Gruppen.
Seien $(G, *)$ und $(G', *')$ zwei Gruppen. Eine Abbildung $\varphi : G \to G'$ wird Homomorphismus genannt, wenn die Gleichung $\varphi(a * b) = \varphi(a) *' \varphi(b)$ für alle $a, b \in G$ erfüllt ist.

Satz 3.5. Sei $\varphi : G \to G'$ 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 3.6. 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 3.6.

3.1.2 Gruppenaktionen

Definition 3.5. 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 3.6. 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 (3.1) eine Linksaktion und die Rechtstranslation (3.2) eine Rechtsaktion.

Korollar 3.7. 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

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

3.1.3 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 $X := \{1, \ldots, n\}$ und $S_n := S(X)$ setzen, das heißt eigentlich bloß, dass jedem Element von X eine Nummer gegeben wird.

3.2 Ringtheorie

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.

3.2.1 Elementare Gesetzmäßigkeiten

Definition 3.7. 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 3.8. 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 3.8. 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 3.9. 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 3.10. Sei R ein Ring und $a, b \in R$, dann gilt $(-a)(-b) = ab$.

Beweis. Mit dem letzten Korollar und $-(-x) = x$ rechnet man

$$(-a)(-b) = -((-a)b) = -(-(ab)) = ab. \quad \square$$

Definition 3.9. 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, d. h. 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.

4 Zahlenbereiche

4.1 Ganze Zahlen

4.1.1 Konstruktion

Definition 4.1. Ganze Zahlen.
Auf $\mathbb{N}_0 \times \mathbb{N}_0$ wird die folgende Äquivalenzrelation definiert:

$$(x_1, y_1) \sim (x_2, y_2) \ :\Longleftrightarrow\ x_1 + y_2 = x_2 + y_1.$$

Die Quotientenmenge $\mathbb{Q} := (\mathbb{N}_0 \times \mathbb{N}_0)/\sim$ nennt man die ganzen Zahlen.

Satz 4.1. Ring der ganzen Zahlen.
Die Operationen

$$[(x_1, y_1)] + [(x_2, y_2)] := [(x_1 + x_2, y_1 + y_2)],$$
$$[(x_1, y_1)] \cdot [(x_2, y_2)] := [(x_1 x_2 + y_1 y_2, x_1 y_2 + x_2 y_1)]$$

sind auf $\mathbb{Q}$ wohldefiniert und $(\mathbb{Q}, +, \cdot)$ bildet einen kommutativen unitären Ring.

Beweis. Wohldefiniert heißt, dass das Ergebnis der Operationen nicht von den gewählten Repräsentanten der Argumente abhängig ist. Sei dazu $(x_1, y_1) \sim (a_1, b_1)$ und $(x_2, y_2) \sim (a_2, b_2)$. Zu zeigen ist nun

$$\begin{aligned}&(x_1 + x_2, y_1 + y_2) \sim (a_1 + a_2, b_1 + b_2)\\ \Longleftrightarrow\ &(x_1 + x_2) + (b_1 + b_2) = (a_1 + a_2) + (y_1 + y_2).\end{aligned}$$

Gemäß Voraussetzung ist $x_1 + b_1 = a_1 + y_1$ und $x_2 + b_2 = a_2 + y_2$. Man bekommt damit auf der linken Seite

$$x_1 + x_2 + b_1 + b_2 = a_1 + y_1 + a_2 + y_2,$$

was wiederum mit der rechten Seite übereinstimmt.

Mit der Multiplikation verhält es sich etwas komplizierter. Zu Vereinfachung wird zunächst gezeigt:

$$\begin{aligned}&[(x_1, y_1)] \cdot [(x_2, y_2)] = [(a_1, b_1)] \cdot [(x_2, y_2)]\\ \Longleftrightarrow\ &(x_1 x_2 + y_1 y_2, x_1 y_2 + y_1 x_2) \sim (a_1 x_2 + b_1 y_2, a_1 y_2 + b_1 x_2)\\ \Longleftrightarrow\ &x_1 x_2 + y_1 y_2 + a_1 y_2 + b_1 x_2 = a_1 x_2 + b_1 y_2 + x_1 y_2 + y_1 x_2\\ \Longleftrightarrow\ &(x_1 + b_1) x_2 + (a_1 + y_1) y_2 = (a_1 + y_1) x_2 + (x_1 + b_1) y_2.\end{aligned}$$

Diese Gleichung ist gemäß Voraussetzung $(x_1, y_1) \sim (a_1, b_1)$ bzw. $x_1 + b_1 = a_1 + y_1$ erfüllt.
Analog bestätigt man

$$[(a_1, b_1)] \cdot [(x_2, y_2)] = [(a_1, b_1)] \cdot [(a_2, b_2)].$$

Gemäß Transitivität ergibt sich somit

$$[(x_1, y_1)] \cdot [(x_2, y_2)] = [(a_1, b_1)] \cdot [(a_2, b_2)].$$

Es ist nun zu bestätigen, dass $(\mathbb{Q}, +)$ eine kommutative Gruppe ist. Das Assoziativgesetz:

$$\begin{aligned}&([(x_1, y_1)] + [(x_2, y_2)]) + [(x_3, y_3)] = [(x_1 + x_2, y_1 + y_2)] + [(x_3, y_3)]\\ &= [(x_1 + x_2 + x_3, y_1 + y_2 + y_3)] = [(x_1, y_1)] + [(x_2 + x_3, y_2 + y_3)]\\ &= [(x_1, y_1)] + ([(x_2, y_2)] + [(x_3, y_3)]).\end{aligned}$$

Das neutrale Element ist $[(0, 0)]$:

$$[(x, y)] + [(0, 0)] = [(x + 0, y + 0)] = [(x, y)].$$

Das inverse Element zu $[(x, y)]$ ist $[(y, x)]$, denn es gilt

$$\begin{aligned}&[(x, y)] + [(y, x)] = [(x + y, y + x)] = [(0, 0)]\\ &\iff (x + y, y + x) \sim (0, 0) \iff x + y + 0 = y + x + 0.\end{aligned}$$

Das Kommutativgesetz:

$$\begin{aligned}&[(x_1, y_1)] + [(x_2, y_2)] = [(x_1 + x_2, y_1 + y_2)] = [(x_2 + x_1, y_2 + y_1)]\\ &= [(x_2, y_2)] + [(x_1, y_1)].\end{aligned}$$

Es ist nun zu bestätigen, dass $(\mathbb{Q}, \cdot)$ ein kommutatives Monoid bildet. Das Assoziativgesetz:

$$\begin{aligned}&([(x_1, y_1)] \cdot [(x_2, y_2)]) \cdot [(x_3, y_3)] = [(x_1x_2 + y_1y_2, x_1y_2 + x_2y_1)] \cdot [(x_3, y_3)]\\ &= [(x_1x_2x_3 + x_3y_1y_2 + x_1y_2y_3 + x_2y_1y_3,\ x_1x_2y_3 + y_1y_2y_3 + x_1x_3y_2 + x_2x_3y_1)]\\ &= [(x_1, y_1)] \cdot [(x_2x_3 + y_2y_3, x_2y_3 + x_3y_2)] = [(x_1, y_1)] \cdot ([(x_2, y_2)] \cdot [(x_3, y_3)]).\end{aligned}$$

Das Kommutativgesetz:

$$\begin{aligned}&[(x_1, y_1)] \cdot [(x_2, y_2)] = [(x_1x_2 + y_1y_2,\ x_1y_2 + y_1x_2)]\\ &= [(x_2x_1 + y_2y_1,\ x_2y_1 + x_1y_2)] = [(x_2, y_2)] \cdot [(x_1, y_1)].\end{aligned}$$

Das neutrale Element ist $[(1, 0)]$, denn es gilt

$$[(x, y)] \cdot [(1, 0)] = [(x \cdot 1 + y \cdot 0,\ 1 \cdot y + x \cdot 0)] = [(x, y)].$$

Schließlich ist noch das Distributivgesetz zu bestätigen. Man findet

$$\begin{aligned}&[(a, b)] \cdot ([(x_1, y_1)] + [(x_2, y_2)]) = [(a, b)] \cdot [(x_1 + x_2, y_1 + y_2)]\\ &= [(ax_1 + ax_2 + by_1 + by_2,\ ay_1 + ay_2 + bx_1 + bx_2)]\\ &= [(ax_1 + by_1, ay_1 + bx_1)] + [(ax_2 + by_2, ay_2 + bx_2)]\\ &= [(a, b)] \cdot [(x_1, y_1)] + [(a, b)] \cdot [(x_2, y_2)].\end{aligned}$$

Somit sind alle Axiome bestätigt. □

Definition 4.2. Monoidhomomorphismus.
Seien $(M, +)$ und $(M', +')$ zwei Monoide. Eine Abbildung $\varphi\colon M \to M'$ heißt Monoidhomomorphismus, wenn für alle $a, b \in M$ gilt

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

und $\varphi(0) = 0'$ ist.

Einen injektiven Homomorphismus nennt man Monomorphismus. Ein Monomorphismus charakterisiert eine Einbettung einer Struktur als Unterstruktur einer anderen.

Satz 4.2. Einbettung der natürlichen Zahlen in die ganzen.
Die Abbildung $\varphi\colon \mathbb{N}_0 \to \mathbb{Z}$ mit $\varphi(n) := [(n, 0)]$ ist ein Monoidmonomorphismus.

Beweis. Es ergibt sich

$$\varphi(a + b) = [(a + b, 0)] = [(a, 0)] + [(b, 0)] = \varphi(a) + \varphi(b).$$

Außerdem ist $\varphi(0) = [(0, 0)]$, und $[(0, 0)]$ ist das neutrale Element von $(\mathbb{Z}, +)$.
Schließlich ist noch die Injektivität zu prüfen:

$$[(a, 0)] = \varphi(a) = \varphi(b) = [(b, 0)] \iff (a, 0) \sim (b, 0)$$
$$\iff a + 0 = b + 0 \iff a = b. \square$$

Anstelle von $\varphi(n) = [(n, 0)]$ darf man daher einfach schreiben $n = [(n, 0)]$. Außerdem definiert man $a - b := a + (-b)$. Daraus ergibt sich nun

$$[(x, y)] = [(x, 0)] + [(0, y)] = [(x, 0)] - [(y, 0)] = x - y.$$

Die umständliche Schreibweise $[(x, y)]$ wird ab jetzt nicht mehr benötigt.

Definition 4.3. Totalordnung der ganzen Zahlen.
Auf $\mathbb{Z}$ wird die folgende strenge Totalordnung definiert:

$$[(x_1, y_1)] < [(x_2, y_2)] :\iff x_1 + y_2 < x_2 + y_1.$$

Satz 4.3. Einbettung der Totalordnung.
Die Abbildung φ aus Satz 4.2 genügt der Forderung

$$a < b \implies \varphi(a) < \varphi(b).$$

Beweis. Nach den Definitionen ist

$$\varphi(a) < \varphi(b) \iff [(a, 0)] < [(b, 0)] \iff a + 0 < 0 + b \iff a < b. \square$$

4.2 Rationale Zahlen

4.2.1 Konstruktion

Definition 4.4. Rationale Zahlen.
Auf $\mathbb{Z} \times \mathbb{N}_1$ wird die folgende Äquivalenzrelation definiert:

$$(x_1, y_1) \sim (x_2, y_2) \ :\Longleftrightarrow\ x_1 y_2 = x_2 y_1.$$

Die Quotientenmenge $\mathbb{Q} := (\mathbb{Z} \times \mathbb{N}_1)/\sim$ nennt man die rationalen Zahlen.

Für die Äquivalenzklasse $[(x, y)]$ schreibt man $\frac{x}{y}$.

Satz 4.4. Körper der rationalen Zahlen.
Die Operationen

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} := \frac{x_1 y_2 + x_2 y_1}{y_1 y_2}, \qquad \frac{x_1}{y_1} \cdot \frac{x_2}{y_2} := \frac{x_1 x_2}{y_1 y_2}$$

sind auf $\mathbb{Q}$ wohldefiniert und $(\mathbb{Q}, +, \cdot)$ bildet einen Körper.

Beweis. Wohldefiniert bedeutet, dass das Ergebnis der Operationen nicht von den gewählten Repräsentanten der Argumente abhängig ist. Sei dazu $(a_1, b_1) \sim (x_1, y_1)$ und $(a_2, b_2) \sim (x_2, y_2)$. Zu zeigen ist nun

$$\begin{aligned}
&(a_1 b_2 + a_2 b_1, b_1 b_2) \sim (x_1 y_2 + x_2 y_1, y_1 y_2) \\
&\quad\Longleftrightarrow\ (a_1 b_2 + a_2 b_1)(y_1 y_2) = (x_1 y_2 + x_2 y_1)(b_1 b_2) \\
&\quad\Longleftrightarrow\ a_1 b_2 y_1 y_2 + a_2 b_1 y_1 y_2 = x_1 y_2 b_1 b_2 + x_2 y_1 b_1 b_2.
\end{aligned}$$

Substituiert man $a_1 y_1 = x_1 b_1$ und $a_2 y_2 = x_2 b_2$ auf der linken Seite der Gleichung, ergibt sich die rechte Seite. Zu zeigen ist weiterhin

$$(a_1 a_2, b_1 b_2) \sim (x_1 x_2, y_1 y_2) \iff a_1 a_2 y_1 y_2 = x_1 x_2 b_1 b_2.$$

Wieder wird linke Seite der Gleichung über $a_1 y_1 = x_1 b_1$ und $a_2 y_2 = x_2 b_2$ in die rechte Seite überführt. Die Wohldefiniertheit der Operationen ist damit bestätigt.

Es bleibt zu prüfen, dass $(\mathbb{Q}, +, \cdot)$ allen Körperaxiomen genügt. Das neutrale Element der Addition ist $0/1$, denn es gilt

$$\frac{x}{y} + \frac{0}{1} = \frac{x \cdot 1 + 0 \cdot y}{y \cdot 1} = \frac{x}{y}.$$

Das neutrale Element der Multiplikation ist $1/1$, denn es gilt

$$\frac{x}{y} \cdot \frac{1}{1} = \frac{x \cdot 1}{y \cdot 1} = \frac{x}{y}.$$

Die Assoziativität der Addition ergibt sich ohne größere Umstände:

$$\begin{aligned}
\left(\frac{x_1}{y_1} + \frac{x_2}{y_2}\right) + \frac{x_3}{y_3} &= \frac{x_1 y_2 + x_2 y_1}{y_1 y_2} + \frac{x_3}{y_3} = \frac{x_1 y_2 y_3 + x_2 y_1 y_3 + x_3 y_1 y_2}{y_1 y_2 y_3}, \\
\frac{x_1}{y_1} + \left(\frac{x_2}{y_2} + \frac{x_3}{y_3}\right) &= \frac{x_1}{y_1} + \frac{x_2 y_3 + x_3 y_2}{y_2 y_3} = \frac{x_1 y_2 y_3 + x_2 y_1 y_3 + x_3 y_1 y_2}{y_1 y_2 y_3}.
\end{aligned}$$

Die Assoziativität der Multiplikation ist etwas einfacher:

$$\left(\frac{x_1}{y_1} \cdot \frac{x_2}{y_2}\right) \cdot \frac{x_3}{y_3} = \frac{x_1 x_2}{y_1 y_2} \cdot \frac{x_3}{y_3} = \frac{x_1 x_2 x_3}{y_1 y_2 y_3} = \frac{x_1}{y_1} \cdot \frac{x_2 x_3}{y_2 y_3} = \frac{x_1}{y_1} \cdot \left(\frac{x_2}{y_2} \cdot \frac{x_3}{y_3}\right).$$

Das Kommutativgesetz der Addition:

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} = \frac{x_1 y_2 + x_2 y_1}{y_1 y_2} = \frac{x_2 y_1 + x_1 y_2}{y_2 y_1} = \frac{x_2}{y_2} + \frac{x_1}{y_1}.$$

Das Kommutativgesetz der Multiplikation:

$$\frac{x_1}{y_2} \cdot \frac{x_2}{y_2} = \frac{x_1 x_2}{y_1 y_2} = \frac{x_2 x_1}{y_2 y_1} = \frac{x_2}{y_2} \cdot \frac{x_1}{y_1}.$$

Das additiv inverse Element zu x/y ist $(-x)/y$, denn es gilt

$$\frac{x}{y} + \frac{-x}{y} = \frac{xy + (-x)y}{y^2} = \frac{0}{y^2} = \frac{0}{1}.$$

Das multiplikativ inverse Element zu x/y mit $x \neq 0$ ist y/x, denn es gilt

$$\frac{x}{y} \cdot \frac{y}{x} = \frac{xy}{xy} = \frac{1}{1}.$$

Schließlich findet bestätigt man noch das Distributivgesetz:

$$\frac{a}{b} \cdot \left(\frac{x_1}{y_1} + \frac{x_2}{y_2}\right) = \frac{a}{b} \cdot \frac{x_1 y_2 + x_2 y_1}{y_1 y_2} = \frac{a x_1 y_2 + a x_2 y_1}{b y_1 y_2},$$
$$\frac{a x_1}{b y_1} + \frac{a x_2}{b y_2} = \frac{a x_1 b y_2 + a x_2 b y_1}{b y_1 b y_2} = \frac{b}{b} \cdot \frac{a x_1 y_2 + a x_2 y_1}{b y_1 y_2}.$$

Hierbei beachtet man, dass $b/b = 1/1$ das multiplikativ neutrale Element ist. □

Definition 4.5. Ringhomomorphismus.
Seien $(R, +, *)$ und $(R', +', *')$ zwei Ringe. Die Abbildung $\varphi\colon R \to R'$ heißt Ringhomomorphismus, wenn für alle $a, b \in R$ gilt:

$$\varphi(a + b) = \varphi(a) +' \varphi(b), \qquad \varphi(a * b) = \varphi(a) *' \varphi(b).$$

Besitzt R ein Einselement 1 und R' ein Einselement $1'$, dann nennt man φ Eins-erhaltend, wenn $\varphi(1) = 1'$ ist.

Einen injektiver Homomorphismus wird Monomorphismus genannt. Ein Monomorphismus charakterisiert eine Einbettung einer Unterstruktur in eine andere Struktur.

Satz 4.5. Einbettung der ganzen Zahlen in die rationalen.
Sei $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ mit $\varphi(z) := z/1$. Die Abbildung φ ist Eins-erhaltender Ringmonomorphismus.

Beweis. Die Erhaltung des Einselements ergibt sich trivial. Ferner findet man

$$\varphi(a+b) = \frac{a+b}{1} = \frac{a\cdot 1 + b\cdot 1}{1\cdot 1} = \frac{a}{1} + \frac{b}{1} = \varphi(a) + \varphi(b)$$

und

$$\varphi(ab) = \frac{ab}{1} = \frac{ab}{1\cdot 1} = \frac{a}{1}\cdot\frac{b}{1} = \varphi(a)\cdot\varphi(b). \qquad \square$$

Gemäß der Einbettung können wir die ganze Zahl z ab jetzt mit der rationalen Zahl $z/1$ identifizieren. D. h. man schreibt einfach $z = z/1$ anstelle von $\varphi(z) = z/1$.

Definition 4.6. Division rationaler Zahlen.
Wie in jedem Körper ist die Division für $a, b \in \mathbb{Q}$ definiert als $a/b := ab^{-1}$.

Die Division ist also gerade die Multiplikation des Kehrwertes des Nenners:

$$\frac{x_1}{y_1} \Big/ \frac{x_2}{y_2} = \frac{x_1}{y_1}\cdot\frac{y_2}{x_2}.$$

Die Division muss natürlich mit der Notation für rationale Zahlen kompatibel sein, sonst dürfte man nicht die gleiche Schreibweise verwenden. Zur Unterscheidung schreiben wir Division für einen Augenblick mit Doppelstrich als $a//b$. Man findet

$$\frac{x}{y} = \frac{x}{1}\cdot\frac{1}{y} = \frac{x}{1} // \frac{y}{1} = x//y.$$

Tatsächlich führt beides zum gleichen Ergebnis.

Da die rationalen Zahlen einen Körper bilden, gilt $a/a = aa^{-1} = 1$ für jede rationale Zahl a.

Satz 4.6. Addition, Subtraktion, Multiplikation von Brüchen.
Seien a, b, c, d rationale Zahlen mit $b \neq 0$ und $d \neq 0$. Es gilt

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}, \qquad \frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd}.$$

Der Beweis wird dem Leser überlassen.

5 Ansätze zur Problemlösung

5.1 Substitution

5.1.1 Quadratische Gleichungen

Vorgelegt ist eine quadratische Gleichung in Normalform

$$x^2 + px + q = 0. \tag{5.1}$$

Interessanterweise lässt sich der lineare Term px durch Darstellung der Gleichung über eine Translation $x = u + d$ eliminieren. Einsetzen dieser Substitution bringt

$$0 = (u+d)^2 + p(u+d) + q = u^2 + 2ud + d^2 + pu + pd + q \tag{5.2}$$

$$= u^2 + (p+2d)u + (d^2 + pd + q). \tag{5.3}$$

Setzt man nun $p + 2d = 0$, dann ergibt sich daraus $d = -p/2$ und somit

$$q' := d^2 + pd + q = \left(-\frac{p}{2}\right)^2 - p \cdot \frac{p}{2} + q = \frac{p^2}{4} - \frac{p^2}{2} + q \tag{5.4}$$

$$= \frac{p^2}{4} - 2\frac{p^2}{4} + q = -\frac{p^2}{4} + q. \tag{5.5}$$

Zu lösen ist nunmehr die quadratische Gleichung

$$u^2 + q' = 0. \tag{5.6}$$

Aber das ist ganz einfach, die Lösungen sind $u_1 = +\sqrt{-q'}$ und $u_2 = -\sqrt{-q'}$, sofern $q' \leq 0$, bzw. äquivalent $-q' \geq 0$. Wir schreiben kurz $u = \pm\sqrt{-q'}$. Resubstitution von $u = x - d$ und q' führt zu

$$x - d = x + \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q} = \pm\frac{1}{2}\sqrt{p^2 - 4q}. \tag{5.7}$$

Man erhält die Lösungsformel

$$x = -\frac{p}{2} \pm \frac{1}{2}\sqrt{p^2 - 4q}. \tag{5.8}$$

5.1.2 Biquadratische Gleichungen

Die biquadratische Gleichung

$$x^4 + px^2 + q = 0 \tag{5.9}$$

lässt sich über die Substitution $u = x^2$ auf die quadratische Gleichung

$$u^2 + pu + q \tag{5.10}$$

reduzieren. Für $p^2 - 4q \geq 0$ ergeben sich zwei Lösungen u_1, u_2, wobei eventuell $u_1 = u_2$ ist. Nun können sich bis zu vier Lösungen für die ursprüngliche Gleichung ergeben. Das ist der Fall, wenn $u_1 \neq u_2$ und $u_1, u_2 > 0$. Dann ergibt sich

$$x_1 = \sqrt{u_1}, \quad x_2 = -\sqrt{u_1}, \quad x_3 = \sqrt{u_2}, \quad x_4 = -\sqrt{u_2} \tag{5.11}$$

6 Kombinatorik

6.1 Endliche Summen

6.1.1 Definition

Definition 6.1. Summe.
Für eine Folge $a\colon \mathbb{Z} \to \mathbb{R}$ ist die Summe über die a_k von $k = m$ bis n rekursiv definiert gemäß

$$\sum_{k=m}^{m-1} a_k := 0, \qquad \sum_{k=m}^{n} a_k := a_n + \sum_{k=m}^{n-1} a_k.$$

Das schaut komplizierter aus als es ist. Man hat

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + a_3 + \ldots + a_n.$$

Z. B. ist

$$\sum_{k=1}^{4} k^2 = 1^2 + 2^2 + 3^2 + 4^2 = 1 + 4 + 9 + 16 = 30.$$

Die Berechnung gemäß der Definition:

$$\begin{aligned}\sum_{k=1}^{4} k^2 &= 4^2 + \sum_{k=1}^{3} k^2 = 4^2 + 3^2 + \sum_{k=1}^{2} k^2 = 4^2 + 3^2 + 2^2 + \sum_{k=1}^{1} k^2 \\ &= 4^2 + 3^2 + 2^2 + 1^2 + \sum_{k=1}^{0} k^2 = 4^2 + 3^2 + 2^2 + 1^2 + 0 = 30.\end{aligned}$$

6.1.2 Rechenregeln

Satz 6.1. Homogenität der Summenoperation.
Ist c eine Konstante, dann gilt

$$\sum_{k=m}^{n} ca_k = c \sum_{k=m}^{n} a_k.$$

Beweis. Der Induktionsanfang ist trivial:

$$\sum_{k=m}^{m-1} ca_k = 0 = c \cdot 0 = c \sum_{k=m}^{m-1} a_k.$$

Der Induktionsschritt »$A(n-1) \Rightarrow A(n)$« ist erfüllt, denn es gilt

$$\sum_{k=m}^{n} ca_k = ca_n + \sum_{k=m}^{n-1} ca_k = ca_n + c\sum_{k=m}^{n-1} a_k = c\left(a_n + \sum_{k=m}^{n-1} a_k\right) = c\sum_{k=m}^{n} a_k. \square$$

Satz 6.2. Additivität der Summenoperation.
Es gilt

$$\sum_{k=m}^{n} (a_k + b_k) = \sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k.$$

Beweis. Der Induktionsanfang ist trivial. Induktionsschritt:

$$\begin{aligned}\sum_{k=m}^{n} (a_k + b_k) &= (a_n + b_n) + \sum_{k=m}^{n-1} (a_k + b_k) = (a_n + b_n) + \sum_{k=m}^{n-1} a_k + \sum_{k=m}^{n-1} b_k \\ &= \left(a_n + \sum_{k=m}^{n-1} a_k\right) + \left(b_n + \sum_{k=m}^{n-1} b_k\right) = \sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k. \square\end{aligned}$$

Satz 6.3. Aufteilung von Summen.
Für $m \leq p \leq n$ gilt

$$\sum_{k=m}^{n} a_k = \sum_{k=m}^{p-1} a_k + \sum_{k=p}^{n} a_k.$$

Beweis. Für den Induktionsanfang setzt man $n = p$. Die Gleichung ist dann erfüllt, weil definitionsgemäß $\sum_{k=p}^{p} a_k = a_p$ gilt.

Der Induktionsschritt:

$$\sum_{k=m}^{n} a_k = a_n + \sum_{k=m}^{n-1} a_k = a_n + \sum_{k=m}^{p-1} a_k + \sum_{k=p}^{n-1} a_k = \sum_{k=m}^{p-1} a_k + \sum_{k=p}^{n} a_k. \square$$

Satz 6.4. Indexshift.
Für die Indexverschiebung der Distanz $d \in \mathbb{Z}$, kurz Indexshift, gilt

$$\sum_{k=m}^{n} a_k = \sum_{k=m+d}^{n+d} a_{k-d}.$$

Beweis. Für den Induktionsanfang $n = m - 1$ erhält man definitionsgemäß sofort

$$\sum_{k=m}^{m-1} a_k = 0 = \sum_{k=m+d}^{m+d-1} a_{k-d}.$$

Induktionsschritt:

$$\sum_{k=m}^{n} a_k = a_n + \sum_{k=m}^{n-1} a_k = a_{(n+d)-d} + \sum_{k=m+d}^{n+d-1} a_{k-d} = \sum_{k=m+d}^{n+d} a_{k-d}. \square$$

Herleitung. Substituiere $k := k' - d$. Man formt damit um:

$$\sum_{k=m}^{n} a_k = \sum_{m \le k \le n} a_k = \sum_{m \le k'-d \le n} a_{k'-d} = \sum_{m+d \le k' \le n+d} a_{k'-d} = \sum_{k'=m+d}^{n+d} a_{k'-d}. \square$$

Satz 6.5. Umkehrung der Reihenfolge.
Es gilt $\sum_{k=0}^{n} a_k = \sum_{k=0}^{n} a_{n-k}$.

Beweis. Der Induktionsanfang bei $n = 0$ ist trivial. Beim Induktionsschritt macht man sich Satz 6.4 (Indexshift) und Satz 6.3 (Aufteilung) zunutze:

$$\sum_{k=0}^{n} a_{n-k} = a_{n-n} + \sum_{k=0}^{n-1} a_{n-k} = a_0 + \sum_{k=0}^{n-1} a_{n-(n-1-k)} = a_0 + \sum_{k=0}^{n-1} a_{k+1}$$

$$\overset{[k:=k-1]}{=} a_0 + \sum_{k=1}^{n} a_k = \sum_{k=0}^{0} a_k + \sum_{k=1}^{n} a_k = \sum_{k=0}^{n} a_k. \square$$

Satz 6.6. Partialsumme der konstanten Folge.
Es gilt $\sum_{k=m}^{n} 1 = n - m + 1$.

Beweis. Induktionsanfang bei $n = m - 1$:

$$\sum_{k=m}^{m-1} 1 = 0, \qquad (m-1) - m + 1 = m - 1 - m + 1 = 0.$$

Induktionsschritt:

$$\sum_{k=m}^{n} 1 = 1 + \sum_{k=m}^{n-1} 1 = 1 + (n-1) - m + 1 = n - m + 1. \square$$

Satz 6.7. Partialsumme der arithmetischen Folge.
Es gilt $\sum_{k=0}^{n} k = \frac{n}{2}(n+1)$.

Beweis. Der Induktionsanfang $n = 0$ ist trivial. Induktionsschritt:

$$\sum_{k=0}^{n} k = n + \sum_{k=0}^{n-1} k = n + \frac{(n-1)}{2}(n-1+1) = \frac{2n}{2} + \frac{(n-1)\,n}{2}$$
$$= \frac{2n + n^2 - n}{2} = \frac{n^2 + n}{2} = \frac{n}{2}(n+1). \square$$

Herleitung und alternativer Beweis. Man addiert die Summe zu sich selbst, da muss das Doppelte der Summe bei herauskommen. Die Reihenfolge der einen Summe wird mittels Satz 6.5 umgekehrt. Danach wendet man Satz 6.2 (Additivität), Satz 6.1 (Homogenität) und Satz 6.6 an:

$$2\sum_{k=0}^{n} k = \sum_{k=0}^{n} k + \sum_{k=0}^{n} k = \sum_{k=0}^{n} k + \sum_{k=0}^{n} (n-k)$$
$$= \sum_{k=0}^{n} (k + n - k) = \sum_{k=0}^{n} n = n\sum_{k=0}^{n} 1 = n(n+1). \square$$

Satz 6.8. Partialsumme der geometrischen Folge.
Für $q \neq 1$ gilt $\sum_{k=a}^{b-1} q^k = \frac{q^b - q^a}{q-1}$

Herleitung und Beweis. Sei $s := \sum_{k=a}^{b-1} q^k$ die gesuchte Summe. Mittels Homogenität und Indexshift findet man

$$qs = q\sum_{k=a}^{b-1} q^k = \sum_{k=a}^{b-1} q^{k+1} = \sum_{k=a+1}^{b} q^k = q^b - q^a + \sum_{k=a}^{b-1} q^k = q^b - q^a + s.$$

Das ist nun aber lediglich eine lineare Gleichung in s. Die Lösung ist

$$s = \frac{q^b - q^a}{q-1}. \square$$

6.1.3 Anwendungen

Die gezeigten Rechenregeln ermöglichen die Vereinfachung einiger Summen, die in der Kombinatorik und Analysis ab und zu vorkommen. Die allgemeine arithmetischen Folge ist z. B. gegeben gemäß $a_k = Ak + B$, wobei A, B zwei Konstanten sind. Für die Summe findet man

$$\sum_{k=0}^{n} (Ak + B) = A\sum_{k=0}^{n} k + B\sum_{k=0}^{n} 1 = A\frac{n}{2}(n+1) + B(n+1) = \left(\frac{An}{2} + B\right)(n+1),$$

bzw.

$$\sum_{k=1}^{n} (Ak + B) = A\sum_{k=1}^{n} k + B\sum_{k=1}^{n} 1 = A\frac{n}{2}(n+1) + Bn = \left(\frac{A}{2}(n+1) + B\right)n.$$

6.1.4 Teleskopsummen

Satz 6.9. Teleskopsumme.
Es gilt $\sum_{k=m}^{n-1}(a_{k+1} - a_k) = a_n - a_m$.

Beweis. Mittels Indexshift stellt man die folgende Überlegung an:

$$\sum_{k=m}^{n-1} a_{k+1} = \sum_{k=m+1}^{n} a_k = a_n - a_m + \sum_{k=m}^{n-1} a_k.$$

Benutzung dieser Überlegung führt zu:

$$\sum_{k=m}^{n-1}(a_{k+1} - a_k) = \sum_{k=m}^{n-1} a_{k+1} - \sum_{k=m}^{n-1} a_k = a_n - a_m + \sum_{k=m}^{n-1} a_k - \sum_{k=m}^{n-1} a_k = a_n - a_m. \quad \square$$

Definition 6.2. Differenzoperator.
Für eine Folge (a_n) definiert man $(\Delta a)_n := a_{n+1} - a_n$.

Die Teleskopsumme lässt sich damit in der Form $\sum_{k=m}^{n-1}(\Delta a)_k = a_n - a_m$ schreiben. Der Leser wird jetzt vielleicht fragen, warum für diesen einfachen Zusammenhang explizit ein Operator definiert wurde. Nun ja, dieser Operator kann iteriert werden. Die Formeln die dabei herauskommen, sind nicht mehr ganz so einfach. Z. B. ist

$$\begin{aligned}(\Delta^2 a)_n &= (\Delta\Delta a)_n = (\Delta a)_{n+1} - (\Delta a)_n = (a_{n+2} - a_{n+1}) - (a_{n+1} - a_n)\\ &= a_{n+2} - 2a_{n+1} + a_n.\end{aligned}$$

Außerdem genügt der Differenzoperator selbst bestimmten Rechenregeln.

Satz 6.10. Der Operator Δ ist linear, d. h. für Folgen (a_n), (b_n) und eine Konstante c gilt

$$\Delta(c \cdot a) = c \cdot \Delta a, \qquad \Delta(a + b) = (\Delta a) + (\Delta b).$$

Beweis. Man findent

$$\Delta(ca)_n = ca_{n+1} - ca_n = c(a_{n+1} - a_n) = c\Delta a_n$$

und

$$\begin{aligned}\Delta(a + b)_n &= (a_{n+1} + b_{n+1}) - (a_n + b_n) = a_{n+1} - a_n + b_{n+1} - b_n\\ &= (\Delta a)_n + (\Delta b)_n. \quad \square\end{aligned}$$

Der Differenzoperator erlaubt es, nach vielen neuen Summenformeln zu fischen, nämlich indem man einen beliebigen Ausdruck nimmt und diesen als Teleskopsumme darstellt. Für $a_n = n^2$ ist z. B.

$$(\Delta a)_n = (n + 1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1.$$

Damit bekommt man

$$2\sum_{k=0}^{n-1} k + n = \sum_{k=0}^{n-1}(2k+1) = \sum_{k=0}^{n-1}(\Delta a)_k = n^2 - 0^2 = n^2.$$

Umformung bringt

$$\sum_{k=0}^{n-1} k = \frac{1}{2}(n^2 - n) = \frac{n}{2}(n-1).$$

Setzt man für n nun $n+1$ ein, dann ergibt sich die schon bekannte Formel von Satz 6.7.

Eine wichtige Formel für Teleskopsummen gilt bezüglich Def. 6.7.

Satz 6.11. Sei $k \geq 0$. Für $a_n := n^{\underline{k}}$ gilt $(\Delta a)_n = k n^{\underline{k-1}}$.

Beweis. Der Fall $k = 0$ ist trivial. Für $k \geq 1$ wendet man Satz 6.22 an:

$$(\Delta a)_n = (n+1)^{\underline{k}} - n^{\underline{k}} = (n-(k-1)+1)(n+1)^{\underline{k-1}} - (n+1-k)n^{\underline{k-1}}$$
$$= (n+1)n^{\underline{k-1}} - (n+1-k)n^{\underline{k-1}} = (n+1-n-1+k)n^{\underline{k-1}} = kn^{\underline{k-1}}. \quad \square$$

Für $a_n := \frac{k^{\underline{p+1}}}{p+1}$ ergibt sich demnach $(\Delta a_n) = k^{\underline{p}}$. Das führt zur Teleskopsumme

$$\sum_{k=m}^{n-1} k^{\underline{p}} = \frac{n^{\underline{p+1}} - m^{\underline{p+1}}}{p+1}.$$

Nun treten zumeist Summen über k^p auf und nicht über $k^{\underline{p}}$. Zwischen diesen gibt es aber einen einfachen Zusammenhang. Nämlich lässt sich x^n als Linearkombination

$$x^n = \sum_{k=0}^{n} S_k x^{\underline{k}}$$

darstellen. Die Linearfaktoren S_k sind von besonderer Bedeutung, es sind die Stirling-Zahlen zweiter Art.

Definition 6.3. Stirling-Zahlen zweiter Art.
Man definiert rekursiv

$$n > 0 \implies \left\{ n \atop k \right\} := k \left\{ n-1 \atop k \right\} + \left\{ n-1 \atop k-1 \right\},$$

mit den Anfangswerten

$$\left\{ n \atop n \right\} := 1, \qquad k = 0 < n \vee n < k \implies \left\{ n \atop k \right\} := 0.$$

Satz 6.12. Für $x \in \mathbb{R}$ und $n \in \mathbb{N}_0$ gilt

$$x^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} x^{\underline{k}}.$$

Unter Anwendung von Satz 6.12 und der Teleskopsumme zu Satz 6.11 gelangt man zu

$$\sum_{k=m}^{n-1} k^p = \sum_{k=m}^{n-1} \sum_{i=0}^{p} \left\{ {p \atop i} \right\} k^{\underline{i}} = \sum_{i=0}^{p} \left\{ {p \atop i} \right\} \sum_{k=m}^{n-1} k^{\underline{i}} = \sum_{i=0}^{p} \left\{ {p \atop i} \right\} \frac{n^{\underline{i+1}} - m^{\underline{i+1}}}{i+1}.$$

Hiermit lassen ich alle Potenzsummen vereinfachen. Der Leser rechne zur Übung die folgenden Resultate nach:

$$\sum_{k=0}^{n} k^2 = \tfrac{1}{3}n^3 + \tfrac{1}{2}n^2 + \tfrac{1}{6}n = \tfrac{n}{6}(n+1)(2n+1), \tag{6.1}$$

$$\sum_{k=0}^{n} k^3 = \tfrac{1}{4}n^4 + \tfrac{1}{2}n^3 + \tfrac{1}{4}n^2 = (\tfrac{n}{2}(n+1))^2. \tag{6.2}$$

6.1.5 Ungleichung zwischen Summen

Korollar 6.13. Für zwei Folgen (a_k), (b_k) gilt

$$(\forall k \geq m)(a_k \leq b_k) \implies \sum_{k=m}^{n} a_k \leq \sum_{k=m}^{n} b_k.$$

Beweis. Induktiv. Induktionsanfang ist $0 \leq 0$ wegen $\sum_{k=m}^{m-1} x_k = 0$. Gemäß (1.20) gilt

$$\sum_{k=m}^{n-1} a_k \leq \sum_{k=m}^{n-1} b_k \implies \underbrace{a_n + \sum_{k=m}^{n-1} a_k}_{\sum_{k=m}^{n} a_k} \leq \underbrace{b_n + \sum_{k=m}^{n-1} b_k}_{\sum_{k=m}^{n} b_k}. \quad \square$$

6.2 Endliche Produkte

6.2.1 Definition

Definition 6.4. Produkt.
Für eine Folge $a\colon \mathbb{Z} \to \mathbb{R}$ ist das Produkt der a_k für k von $k = m$ bis $k = n$ rekursiv definiert gemäß

$$\prod_{k=m}^{m-1} a_k := 1, \qquad \prod_{k=m}^{n} a_k := a_n \cdot \prod_{k=m}^{n-1} a_k.$$

6.2.2 Rechenregeln

Für Produkte gelten analoge Rechenregeln wie für Summen. Auch die Beweise sind analog, weshalb sie für den Leser als Übung dienen sollen.

Satz 6.14. Ist $c \in \mathbb{R}$ eine Konstante, dann gilt

$$\prod_{k=m}^{n} ca_k = c^n \prod_{k=m}^{n} a_k.$$

Satz 6.15. Es gilt

$$\prod_{k=m}^{n} a_k b_k = \prod_{k=m}^{n} a_k \prod_{k=m}^{n} b_k.$$

Satz 6.16. Aufteilung von Produkten. Für $m \leq p \leq n$ gilt:

$$\prod_{k=m}^{n} a_k = \prod_{k=m}^{p-1} a_k \prod_{k=p}^{n} a_k.$$

Satz 6.17. Indexshift. Für die Indexverschiebung der Distanz $d \in \mathbb{Z}$ gilt

$$\prod_{k=m}^{n} a_k = \prod_{k=m+d}^{n+d} a_{k-d}.$$

6.3 Potenzen

Definition 6.5. Sei $(M, \cdot, e)$ ein Monoid. Für $a \in M$ und $n \in \mathbb{N}_0$ ist die n-te Potenz von a rekursiv definiert gemäß

$$a^0 := e, \quad a^n = a \cdot a^{n-1}.$$

Satz 6.18. Es gilt $a^n = \prod_{k=1}^{n} a$.

Beweis. Induktionsanfang: $a^0 = e = \prod_{k=1}^{0} a$. Induktionsschritt:

$$a^n = a \cdot a^{n-1} = a \cdot \prod_{k=1}^{n-1} a = \prod_{k=1}^{n} a. \square$$

Satz 6.19. Es gilt $a^{m+n} = a^m a^n$.

Beweis. Induktionsanfang: $a^{0+n} = a^n = ea^n = a^0 a^n$. Induktionsschritt:

$$a^{m+n} = a^{(m-1)+n+1} = aa^{(m-1)+n} = aa^{m-1}a^n = a^m a^n. \square$$

Satz 6.20. Unter der Voraussetzung $ab = ba$ gilt $(ab)^n = a^n b^n$.

Beweis. Induktionsanfang: $(ab)^0 = e = ee = a^0 b^0$. Induktionsschritt:

$$(ab)^n = (ab)(ab)^{n-1} = aba^{n-1}b^{n-1} = aa^{n-1}bb^{n-1} = a^n b^n.$$

Achtung, wir müssen noch $ab^n = b^n a$ aufzeigen.
Induktionsanfang: $ab^0 = ae = a = ea = b^0 a$.
Induktionsschritt: $ab^n = abb^{n-1} = bab^{n-1} = bb^{n-1}a = b^n a. \square$

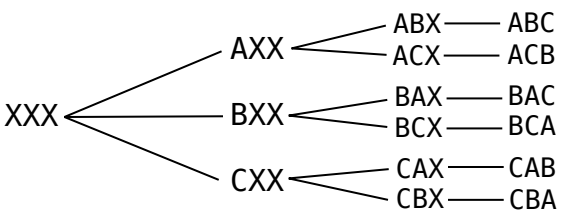
6.4 Permutationen und Variationen

6.4.1 Anzahl der Permutationen

Gegeben sind zwei unterschiedliche Buchstaben, sagen wir A, B. Diese Buchstaben sind auf zwei Plätze zu legen, wobei die Reihenfolge die wesentliche Rolle spielt. Wie viele Möglichkeiten gibt es dafür? Das sind zwei, nämlich AB und BA. Man sagt, es gibt zwei Permutationen der Buchstaben A, B.

Wie viele Möglichkeiten gibt es, die drei Buchstaben A, B, C auf drei Plätze zu legen? Es sind sechs, das sind ABC, BAC, ACB, BCA, CAB und CBA. Man sagt, es gibt sechs Permutationen der Buchstaben A, B, C.

Das ist schon recht unübersichtlich. Es gibt aber eine systematische Methode, alle Möglichkeiten aufzuzählen. Für den ersten Platz gibt es drei Möglichkeiten. Für den zweiten Platz gibt es dann jeweils nur noch zwei Möglichkeiten, weil nur noch zwei Buchstaben zur Verfügung stehen. Für den letzten Platz bleibt jeweils eine Möglichkeit. Somit ergibt sich die folgende Baumstruktur:



Gegeben sind nun n Buchstaben und genau so viele freie Plätze. Die Anzahl der Permutationen nennen wir $n!$, sprich n *Fakultät*. Für den ersten Platz gibt es n Möglichkeiten. Für den zweiten Platz sind nur noch jeweils $n-1$ Buchstaben übrig, es gibt deshalb nur noch jeweils $n-1$ Möglichkeiten. Für den dritten Platz gibt es noch jeweils $n-2$ Möglichkeiten, für den vierten Platz jeweils $n-3$ usw. Für den n-ten Platz gibt es schließlich jeweils nur noch eine Möglichkeit. Das macht insgesamt

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$$

Möglichkeiten. Außerdem ergibt sich die folgende Rekursionsformel:

$$n! = n \cdot (n-1)!.$$

Definition 6.6. Fakultät.
Für eine Zahl $n \in \mathbb{N}_0$ ist die Fakultät von n rekursiv definiert gemäß

$$0! := 1, \qquad n! := n \cdot (n-1)!.$$

Wir zuvor gezeigt, gibt es genau $n!$ Permutationen von n unterschiedlichen Objekten. Es gibt $4! = 24$ Permutationen der vier Buchstaben A, B, C, D, aber schon $5! = 120$ Permutationen der fünf Buchstaben A, B, C, D, E. Die Anzahl der Permutationen wächst rasant. Es gibt z. B. unzählige Möglichkeiten, Bücher in ein längeres Buchregel zu stellen.

6.4.2 Anzahl der Variationen ohne Wiederholung

Angenommen man hat wieder n unterschiedliche Buchstaben zur Verfügung, aber nur noch k freie Plätze, wobei $k \leq n$. Wie bei den Permutationen ergeben sich für den ersten Platz n Möglichkeiten, für den zweiten jeweils noch $n-1$, für den dritten jeweils noch $n-2$ usw. Im Gegensatz zum Baum der Permutationen bricht der Baum nun vorläufig nach dem k-ten Platz ab. Die Anzahl der Möglichkeiten schreiben wir $n^{\underline{k}}$ und sprechen von der absteigenden Faktoriellen von n mit k Faktoren. Man erhält

$$n^{\underline{k}} = \prod_{i=0}^{k-1}(n-i) = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1).$$

Offenbar gilt $n^{\underline{n}} = n!$, das ist der Spezialfall $k = n$.

Das Produkt haben wir ja rekursiv definiert. Durch Einsetzen dieser Definition lässt sich daraus die rekursive Definition der absteigenden Faktoriellen extrahieren:

Definition 6.7. Absteigende Faktorielle.
Die absteigende Faktorielle von n mit k Faktoren ist rekursiv definiert gemäß

$$n^{\underline{0}} := 1, \qquad n^{\underline{k}} := (n-k+1)\, n^{\underline{k-1}}.$$

Satz 6.21. Für $n, k \in \mathbb{N}_0$ und $k \leq n$ gilt

$$n^{\underline{k}} = \frac{n!}{(n-k)!}.$$

Beweis. Kann man ohne langes Überlegen induktiv machen.

Induktionsanfang:

$$n^{\underline{0}} = 1, \qquad \frac{n!}{(n-0)!} = \frac{n!}{n!} = 1.$$

Induktionsschritt »$A(k-1) \Rightarrow A(k)$«:

$$\begin{aligned} n^{\underline{k}} &= (n-k+1)\, n^{\underline{k-1}} = (n-k+1)\frac{n!}{(n-(k-1))!} = (n-k+1)\frac{n!}{(n-k+1)!} \\ &= (n-k+1)\frac{n!}{(n-k+1)(n-k)!} = \frac{n!}{(n-k)!}. \quad \square \end{aligned}$$

Hierbei wurde $(n-k+1)! = (n-k+1)(n-k)!$ benutzt, was gemäß der rekursiven Definition der Fakultät gilt.

Alternativer Beweis. Mittels Satz 6.16 (Produktaufteilung) und Satz 6.17 (Indexshift):

$$\begin{aligned} n! &= \prod_{i=0}^{n-1}(n-i) = \prod_{i=0}^{k-1}(n-i)\prod_{i=k}^{n-1}(n-i) = n^{\underline{k}}\prod_{i=k}^{n-1}(n-i) \\ &\overset{[i:=i+k]}{=} n^{\underline{k}}\prod_{i=0}^{n-k-1}(n-k-i) = n^{\underline{k}}(n-k)!. \quad \square \end{aligned}$$

Satz 6.22. Für $n, k \in \mathbb{Z}$ und $k \geq 0$ gilt

$$(n-k+1)(n+1)^{\underline{k}} = (n+1)n^{\underline{k}}.$$

Beweis. Für $k \geq 1$ gilt

$$(n-k+1)\prod_{i=0}^{k-2}(n-1) = (n-(k-1))\prod_{i=0}^{k-2}(n-i) = \prod_{i=0}^{k-1}(n-i).$$

Damit ergibt sich

$$(n-k+1)(n+1)^{\underline{k}} = (n-k+1)\prod_{i=0}^{k-1}(n+1-i) = (n-k+1)(n+1)\prod_{i=1}^{k-1}(n+1-i)$$

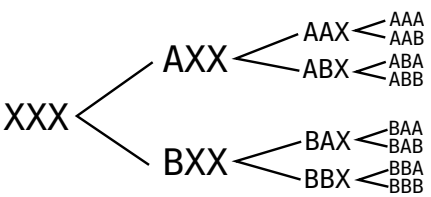
$$= (n+1)(n-k+1)\prod_{i=0}^{k-2}(n-i) = (n+1)\prod_{i=0}^{k-1}(n-i) = (n+1)n^{\underline{k}}.$$

Den Fall $k = 0$ verifiziert man separat:

$$(n-0+1)(n+1)^{\underline{0}} = (n-0+1)\cdot 1 = (n+1)\cdot 1 = (n+1)n^{\underline{0}}. \quad \square$$

6.4.3 Anzahl der Variationen mit Wiederholung

Lässt man die Möglichkeit zu, einen schon gelegten Buchstaben nochmals zu legen, dann ergeben sich offenbar mehr Möglichkeiten. Wie viele Möglichkeiten gibt es, die zwei Buchstaben A, B auf drei freie Plätze zu legen? Dazu ergibt sich der folgende Baum:



Offenbar darf jeder Platz unabhängig von den anderen mit A oder B belegt werden. Das macht zwei Möglichkeiten für den ersten Platz, dann jeweils zwei Möglichkeiten für den zweiten Platz, und dann jeweils zwei Möglichkeiten für den dritten Platz. Insgesamt sind es

$$8 = 2^3 = 2 \cdot 2 \cdot 2$$

Möglichkeiten.

Allgemein hat man nun n unterschiedliche Buchstaben und k freie Plätze. Nach der gleichen Argumentation wie zuvor muss die Anzahl der Möglichkeiten

$$n^k = \underbrace{n \cdot n \cdot n \cdot \ldots \cdot n}_{k \text{ Faktoren}}$$

sein.

Z. B. kann man sich die Frage stellen, wie viele unterschiedliche Werte ein Byte annehmen kann. Ein Byte besitzt acht Bits, also $k = 8$, und jedes dieser Bits kann unabhängig von den anderen entweder 0 oder 1 sein, d. h. $n = 2$. Das macht $2^8 = 256$ Werte.

6.4.4 Deutung als Anzahl der Abbildungen

Betrachten wir nochmals die Variationen mit Wiederholung. Jedoch werden die Buchstaben nun nicht auf die Plätze gelegt, sondern den Plätzen werden Buchstaben zugeordnet. Das läuft natürlich aufs Selbe hinaus, bloß dass es aus der anderen Richtung betrachtet wird. Jeder Platz erhält eine Nummer, angefangen mit null. Jeder nummerierte Platz bekommt einen Buchstaben, das ist aber nichts anderes als eine Abbildung. Für zwei Buchstaben A, B und drei freie Plätze erhält man

$$f : X \to Y, \quad X := \{0, 1, 2\}, \quad Y := \{A, B\}.$$

Die Anzahl der Variationen mit Wiederholung ist genau die Anzahl der unterschiedlichen möglichen Abbildungen. Nennen wir die Menge aller Abbildungen $\mathrm{Abb}(X, Y)$, dann ist nach $|\mathrm{Abb}(X, Y)|$ gefragt. Wie schon bekannt ist, gilt

$$|\mathrm{Abb}(X, Y)| = |Y|^{|X|}.$$

Bei den Variationen ohne Wiederholung müssen alle Buchstaben unterschiedlich sein. Unter der neuen Sichtweise bedeutet das aber nichts anderes, als dass die Abbildung eine injektive sein muss. Nennt man die Menge aller Injektionen $\mathrm{Inj}(X, Y)$, dann gilt wie bereits gezeigt

$$|\mathrm{Inj}(X, Y)| = |Y|^{\underline{|X|}}.$$

Die Permutationen sind ein Spezialfall der Variationen, wo $|X| = |Y|$ ist. Weil die Injektion endlich ist, und es genau so viele Elemente im Definitionsbereich wie in der Zielmenge gibt, muss die Injektion auch surjektiv sein. Die Menge aller Bijektionen nennen wir $\mathrm{Bij}(X, Y)$. Man kann jetzt auch einfach die Buchstaben so nummerieren wie die Plätze, dann ist $X = Y$, man erhält eine Selbstabbildung. Wie schon bekannt, ergibt sich

$$|\mathrm{Bij}(X, X)| = |\mathrm{Inj}(X, X)| = |X|^{\underline{|X|}} = |X|!.$$

7 Zahlentheorie

7.1 Kongruenzen

Definition 7.1. Kongruenz. Zwei ganze Zahlen a, b heißen kongruent modulo m, wenn ihre Differenz $(b - a)$ durch m teilbar ist:

$$a \equiv b \pmod{m} \ :\Longleftrightarrow\ (\exists k \in \mathbb{Z})(b - a = km).$$

Anstelle von »(mod m)« schreibt man beim Rechnen meist kürzer »(m)«.

Satz 7.1. Die Kongruenz ist eine Äquivalenzrelation, d. h. es gilt

$$\begin{aligned} &a \equiv a \pmod{m}, && \text{(Reflexivität)}\\ &a \equiv b \implies b \equiv a \pmod{m}, && \text{(Symmetrie)}\\ &a \equiv b \wedge b \equiv c \implies a \equiv c \pmod{m}. && \text{(Transitivität)} \end{aligned}$$

Beweis. Für die Reflexivität ist ein k mit $0 = a - a = km$ zu finden. Setze $k = 0$.

Bei der Symmetrie gibt es nach Voraussetzung ein k mit $b - a = km$. Dann ist $a - b = -km$. Setze $k' = -k$. Es gibt also k' mit $a - b = k'm$, somit gilt $b \equiv a$.

Bei der Transitivität gibt es nach Voraussetzung k mit $b - a = km$ und l mit $b - c = lm$. Das heißt, es gilt

$$b = a + km = c + lm \implies c - a = km - lm = (k - l)m.$$

Setze $k' = k - l$. Es gibt also k' mit $c - a = k'm$. Somit gilt $a \equiv c$. □

Satz 7.2. Sind a, b, c ganze Zahlen, dann gilt

$$\begin{aligned} a \equiv b \pmod{m} &\iff a + c \equiv b + c \pmod{m},\\ a \equiv b \pmod{m} &\iff a - c \equiv b - c \pmod{m}. \end{aligned}$$

Beweis. Unter Beachtung von $(b + c) - (a + c) = b - a$ findet man

$$\begin{aligned} &a \equiv b \pmod{m} \iff (\exists k \in \mathbb{Z})(b - a = km)\\ &\iff (\exists k \in \mathbb{Z})((b + c) - (a + c) = km)\\ &\iff a + c \equiv b + c \pmod{m}. \end{aligned}$$

Für die Subtraktion von c ist die Überlegung analog. □

Satz 7.3. Sind a, b, c ganze Zahlen, dann gilt

$$a \equiv b \pmod{m} \implies ac \equiv bc \pmod{m}.$$

Beweis. Unter der Voraussetzung $a \equiv b \pmod{m}$ gibt es ein k mit $b - a = km$. Es gilt

$$b - a = km \iff (b-a)c = kcm \iff bc - ac = k'm$$

mit $k' := kc$. Man hat also

$$(\exists k' \in \mathbb{Z})(bc - ac = k'm) \iff ac \equiv bc \pmod{m}. \square$$

Satz 7.4. Gilt $a \equiv a' \pmod{m}$ und $b \equiv b' \pmod{m}$, dann gilt auch

$$\begin{aligned} a + b &\equiv a' + b' \pmod{m}, \\ a - b &\equiv a' - b' \pmod{m}, \\ ab &\equiv a'b' \pmod{m}. \end{aligned}$$

Beweis. Man findet

$$\left.\begin{aligned} a \equiv a' &\implies a + b \equiv a' + b \\ b \equiv b' &\implies a' + b \equiv a' + b' \end{aligned}\right\} \implies a + b \equiv a' + b \equiv a' + b' \pmod{m}. \tag{7.1}$$

Für die Subtraktion ist die Überlegung analog. Für die Multiplikation ebenfalls:

$$\left.\begin{aligned} a \equiv a' &\implies ab \equiv a'b \\ b \equiv b' &\implies a'b \equiv a'b' \end{aligned}\right\} \implies ab \equiv a'b \equiv a'b' \pmod{m}. \square \tag{7.2}$$

Satz 7.5. Addition des Moduls führt auf eine kongruente Zahl:

$$a \equiv a + m \equiv a - m \pmod{m}.$$

Beweis. Es gilt

$$a \equiv a + m \pmod{m} \iff (\exists k \in \mathbb{Z})(km = (a + m) - a = m).$$

Setze $k = 1$. Bei

$$a \equiv a - m \pmod{m} \iff (\exists k \in \mathbb{Z})(km = (a - m) - a = -m)$$

setze $k = -1$. $\square$

7.2 Der Restklassenring

Wir könnten nun beginnen, mit der Kongruenzenrechnung interessante Probleme zu lösen. Zunächst möchte ich aber erläutern, wie die Kongruenzenrechnung mit dem Restklassenring zusammenhängt. Unter diesem Blickwinkel bekommen wir ein tieferes Verständnis und können Mittel der Ringtheorie und Gruppentheorie anwenden.

Zu einer ganzen Zahl a ist die Restklasse modulo m definiert als

$$[a]_m := \{x \mid x \equiv a \pmod{m}\}.$$

Eine alternative Schreibweise für $[a]_m$ ist $a + m\mathbb{Z}$. Weil die Kongruenz eine Äquivalenzrelation ist, handelt es sich bei den Restklassen um Äquivalenzklassen. Wir betrachten nun die Quotientenmenge

$$\mathbb{Z}/m\mathbb{Z} := \{[a]_m \mid a \in \mathbb{Z}\}.$$

Nun können wir die Addition und Multiplikation von Restklassen definieren.

Satz 7.6. Auf $\mathbb{Z}/m\mathbb{Z}$ sind die beiden Operationen

$$\begin{aligned}[a]_m + [b]_m &:= [a + b]_m,\\ [a]_m \cdot [b]_m &:= [ab]_m\end{aligned}$$

wohldefiniert.

Beweis. Zu zeigen ist, dass $a + b \equiv x + y$ gilt, sofern $a \equiv x$ und $b \equiv y$ ist. Gemäß Satz 7.2 gilt

$$\begin{aligned}a \equiv x &\iff a + b \equiv x + b,\\ b \equiv y &\iff x + b \equiv x + y.\end{aligned}$$

Aus den beiden Prämssen erhalten wir demzufolge $a + b \equiv x + b \equiv x + y$. Die Argumentation zur Multiplikation ist analog, wobei Satz 7.3 zur Anwendung kommt. □

Die Struktur $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ nennt man den *Restklassenring* zum Modul m.

Korollar 7.7. Jeder Restklassenring ist ein kommutativer unitärer Ring.

Beweis. Bereits bewiesen wurde, dass die ganzen Zahlen einen kommutativen unitären Ring bilden. Aufgrund der Wohldefiniertheit der Addition und Multiplikation ist Kongruenz modulo m eine Kongruenzrelation. Satz 2.37 zeigt somit die Behauptung. □

Zudem ist die Quotientenabbildung

$$\varphi\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad \varphi(a) := [a]_m.$$

ein Eins-erhaltender Ringhomomorphismus, wie aus dem Beweis von Satz 2.37 hervorgeht.

7.3 Euklidische Division

Lemma 7.8. Lemma zur euklidischen Division.
Zu je zwei ganzen Zahlen a, b mit $b \neq 0$ gibt es zwei eindeutig bestimmte Zahlen q, r mit $0 \leq r < |b|$, so dass $a = bq + r$. Man nennt q den *Quotient* und r den *Rest*.

Beweis der Existenz. Betrachten wir zunächst den Fall, bei dem $a \geq 0$ und $b > 0$ ist. Man kann dann sooft b von a abziehen, bis sich eine Zahl ≥ 0 und $< b$ ergibt. Formal bilden wir die Folge $r_k := a - bk$. Nun muss für irgendein $k \geq 0$ schließlich $0 \leq r_k < b$ sein. Damit ist $q = k$ und $r = r_k$ gefunden.

Sei nun $a < 0$. Wie bereits gezeigt gibt es q, r mit $-a = bq + r$. Für $r = 0$ haben wir dann mit $q' := -q$ und $r' := 0$ einen Quotient und einen Rest. Sei nun $r \neq 0$. Dann gilt

$$a = -bq - r = -(q+1)b + b - r.$$

Mit $q' := -(q+1)$ und $r' := b - r$ gibt es somit auch in diesem Fall einen Quotient und einen Rest. Der Rest erfüllt auch die gewünschte Ungleichung, denn aus $r < b$ ergibt sich $0 < r'$ und aus $0 < r$ ergibt sich $r' < b$.

Sei nun a beliebig und $b < 0$. Dann gibt es q, r mit $a = (-b)q + r$. Setze also $q' := -q$ und $r' := r$. Damit gilt $a = bq' + r'$, womit auch in diesem Fall ein Quotient und ein Rest gefunden ist. □

Beweis der Eindeutigkeit. Das Paar q, r erfülle $a = bq + r$ und q', r' erfülle ebenfalls $a = bq' + r'$. Dann gilt

$$bq + r = bq' + r', \iff b(q - q') = r' - r, \implies |b||q - q'| = |r' - r|.$$

Aus $0 < r < |b|$ und $0 < r' < |b|$ erhält man außerdem $|r' - r| < |b|$. Somit muss $|b||q - q'| < |b|$ sein, also $|q - q'| < 1$. Eine nichtnegative ganze Zahl kann aber nur dann kleiner als eins sein, wenn sie null ist. Damit hat man

$$|q - q'| = 0, \iff q - q' = 0, \iff q = q'.$$

Entsprechend folgt $r = r'$. □

Bei der euklidischen Division $a : b$ ist $(a \bmod b)$ eine geläufige Schreibweise für den Rest. Das Lemma zur euklidischen Division sagt uns, dass jede Restklasse von $\mathbb{Z}/m\mathbb{Z}$ einen kanonischen Repräsentant besitzt. Nämlich besitzt die Restklasse $[a]_m$ den kanonischen Repräsentant $r = (a \bmod m)$, denn $a = mq + r$ bedeutet dass $a - r$ durch m teilbar ist, also

$$a \equiv r \pmod{m}, \quad \text{bzw.} \quad [a]_m = [r]_m.$$

8 Kategorientheorie

8.1 Grundbegriffe

Definition 8.1. Kategorie. Eine Kategorie ist ein Tripel $C = (\mathrm{Ob}, \mathrm{Hom}, \circ)$, sofern die folgenden beiden Axiome erfüllt sind:

1. Für $f : A \to B, g : B \to C, h : C \to D$ gilt das Assoziativgesetz $h \circ (g \circ f) = (h \circ g) \circ f$.
2. Für jedes Objekt X existiert die Identität $\mathrm{id}_X : X \to X$, so dass $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$ für alle Objekte A, B und $f : A \to B$.

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 $f : X \to Y$ 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 8.1. 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 8.2. 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.

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 8.2. Kovarianter Funktor.
Sind C, D Kategorien, dann nennt man $F\colon C \to D$ einen kovarianten Funktor, wenn jedem Objekt $X \in \mathrm{Ob}(C)$ ein Objekt $F(X) \in \mathrm{Ob}(D)$ zugeordnet wird und jedem Morphismus $f \in \mathrm{Hom}_C(X, Y)$ ein ein Morphismus $F(f) \in \mathrm{Hom}_D(F(X), F(Y))$ 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 8.3. 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 $F\colon \mathrm{Ob}(C) \to \mathrm{Ob}(D)$ zu unterscheiden von

$$\tilde{F}\colon \mathrm{Hom}_C(X, Y) \to \mathrm{Hom}_D(F(X), F(Y)).$$

Das Paar $(F, \tilde{F})$ kodiert dann eigentlich den Funktor $C \to D$.

Satz 8.3. 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 8.4. 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 2.30 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 8.4. Natürliche Transformation. Seien C, D Kategorien und $F, G\colon C \to D$ Funktoren. Dann schreibt man $\eta\colon F \to G$ und nennt η natürliche Transformation, wenn die folgenden beiden Axiome erfüllt sind:

1. Jedes Objekt $X \in \mathrm{Ob}(C)$ 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 (2.58). Eine Abbildung $f\colon M \to M'$ heiße *induzierend*, wenn

$$x \sim a \implies f(x) \sim' f(a). \tag{8.1}$$

Satz 8.5. 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

$$I(f)\colon M/\!\sim \to M'/\!\sim', \text{ so dass } I(f) \circ \pi = \pi' \circ f, \tag{8.2}$$

wobei π, π' jeweils die kanonische Projektion ist.

Satz 8.6. 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

$$I(f) \circ \pi = \pi' \circ f, \tag{8.3}$$
$$I(g) \circ \pi' = \pi'' \circ g, \tag{8.4}$$
$$I(g \circ f) \circ \pi = \pi'' \circ (g \circ f). \tag{8.5}$$

Damit kann man nun rechnen

$$I(g \circ f) \circ \pi = \pi'' \circ g \circ f = I(g) \circ \pi' \circ f = I(g) \circ I(f) \circ \pi. \tag{8.6}$$

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

$$(\lambda f)(x) := \lambda f(x), \tag{8.7}$$
$$(f_1 + f_2)(x) := f_1(x) + f_2(x), \tag{8.8}$$

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

$$\forall v_1, v_2 \in V\colon\ \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2), \tag{8.9}$$
$$\forall \lambda \in K, v \in V\colon\ \varphi(\lambda v) = \lambda \varphi(v). \tag{8.10}$$

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

$$\varphi\colon\ \mathrm{Abb}(X, Y) \to \mathrm{Abb}(X', Y), \quad \varphi(f) := f \circ g \tag{8.11}$$

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

$$\begin{aligned}\varphi(\lambda f)(x) &= ((\lambda f) \circ g)(x) = (\lambda f)(g(x)) = \lambda f(g(x)) && (8.12)\\ &= \lambda(f \circ g)(x) = \lambda(\varphi(f))(x) = (\lambda\varphi(f))(x), && (8.13)\end{aligned}$$

kurz $\varphi(\lambda f) = \lambda\varphi(f)$. Und es gilt

$$\begin{aligned}\varphi(f_1 + f_2)(x) &= ((f_1 + f_2) \circ g)(x) = (f_1 + f_2)(g(x)) = f_1(g(x)) + f_2(g(x)) && (8.14)\\ &= (f_1 \circ g)(x) + (f_2 \circ g)(x) = \varphi(f_1)(x) + \varphi(f_2)(x) && (8.15)\\ &= (\varphi(f_1) + \varphi(f_2))(x), && (8.16)\end{aligned}$$

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

$$\eta_p\colon \operatorname{Abb}(X, Y)^n \to \operatorname{Abb}(X, Y), \quad \eta_p(f)(x) := p(f_1(x), \ldots, f_n(x)), \tag{8.17}$$

wobei $f := (f_1, \ldots, f_n)$ ein Tupel von Funktionen ist. Sei außerdem

$$F(\varphi)(f) := (\varphi(f_1), \ldots, \varphi(f_n)). \tag{8.18}$$

Zeigen wollen wir für $\varphi(f) := f \circ g$ nun

$$\varphi(\eta_p(f))(x) = \eta_p(F(\varphi)(f))(x), \quad \text{kurz} \quad \varphi \circ \eta_p = \eta_p \circ F(\varphi). \tag{8.19}$$

Bei der Bestätigung folgt man wieder blind den Definitionen und dem Formalismus. Es gilt

$$\begin{aligned}\varphi(\eta_p(f))(x) &= \eta_p(f)(g(x)) = p(f_1(g(x)), \ldots, f_n(g(x))) && (8.20)\\ &= p(\varphi(f_1)(x), \ldots, \varphi(f_n)(x)) = \eta_p(\varphi(f_1), \ldots, \varphi(f_n))(x) && (8.21)\\ &= \eta_p(F(\varphi)(f))(x). && (8.22)\end{aligned}$$

Das bedeutet, dieses Diagramm kommutiert:

$$\begin{array}{ccc} \operatorname{Abb}(X, Y)^n & \xrightarrow{F(\varphi)} & \operatorname{Abb}(X', Y)^n \\ \Big\downarrow{\scriptstyle \eta_p} & & \Big\downarrow{\scriptstyle \eta_p} \\ \operatorname{Abb}(X, Y) & \xrightarrow[\varphi]{} & \operatorname{Abb}(X', Y) \end{array}$$

Das legt den Verdacht nahe, dass es sich bei F um einen Funktor und bei η_p um eine natürliche Transformation handelt.

Satz 8.7. Kategorie mit Kompositionsoperatoren als Morphismen.
Sei $Y \neq \emptyset$. Sei $\Omega := \{\mathrm{Abb}(X, Y) \mid X \text{ ist beliebig}\}$. Sei

$$\mathrm{Hom}(\mathrm{Abb}(X, Y), \mathrm{Abb}(X', Y)) := \{\varphi \mid \exists f \in \mathrm{Abb}(X, Y), g \in \mathrm{Abb}(X', X) \colon \varphi = f \circ g\}.$$

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

$$(\varphi_2 \circ \varphi_1)(f) = (f \circ g_1) \circ g_2 = f \circ g_1 \circ g_2 = f \circ (g_1 \circ g_2). \tag{8.23}$$

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

$$(\varphi \circ \mathrm{id})(f) = (f \circ \mathrm{id}) \circ g = f \circ g = \varphi(f), \tag{8.24}$$
$$(\mathrm{id} \circ \varphi)(f) = (f \circ g) \circ \mathrm{id} = f \circ g = \varphi(f). \quad \square \tag{8.25}$$

Satz 8.8. 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

$$F(\psi \circ \varphi)(f) = (\psi(\varphi(f_1)), \ldots, \psi(\varphi(f_n))) = F(\psi)(F(\varphi)(f)) = (F(\psi) \circ F(\varphi))(f), \tag{8.26}$$

kurz $F(\psi \circ \varphi) = F(\psi) \circ F(\varphi)$. Und es gilt

$$F(\mathrm{id})(f) = (\mathrm{id}(f_1), \ldots, \mathrm{id}(f_n)) = (f_1, \ldots, f_n) = f = \mathrm{id}(f), \tag{8.27}$$

kurz $F(\mathrm{id}) = \mathrm{id}$. $\square$

Satz 8.9. Die in (8.17) definierte Operation η_p ist eine natürliche Transformation.

Beweis. Wurde in (8.17) bis (8.22) schon gezeigt. $\square$

Literaturverzeichnis

[1] Dirk W. Hoffmann: »Grenzen der Mathematik«. Springer-Verlag, Berlin 2011.

[2] Felix Klein: »Elementarmathematik vom höheren Standpunkte aus«. Springer-Verlag, Berlin 1933.

[3] Jean E. Rubin: »Set Theory for the Mathematician«. Holden-Day, San Francisco 1967.

[4] Timothy Gowers (ed.): »The Princeton Companion to Mathematics«. Princeton University Press, Princeton 2008.

Index