Grundlagen der Mathematik

Juli 2019

Inhaltsverzeichnis

1 Grundbegriffe der Mathematik

1.1 Aussagenlogik

1.1.1 Aussagenlogische Formeln

Aussagen in der Aussagenlogik sind entweder wahr oder falsch, etwas dazwischen gibt es nicht, das nennt man auch das *Prinzip der Zweiwertigkeit*. 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:

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

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

$$A \land B \implies C.$$

In der Formel treten Verknüfungen von Aussagen auf, das sind $\land$ und $\Rightarrow$. Es gibt die grundlegenden Verknüpfungen $\neg, \land, \lor, \Rightarrow, \Leftrightarrow$. Die Bindungsstärke der gelisteten Verknüfpungen ist absteigend, so wie Punktrechnung vor Strichrechnung gilt. Das $\neg$ bindet stärker als $\land$, bindet stärker als $\lor$, bindet stärker als $\Rightarrow$, bindet stärker als $\Leftrightarrow$. Die Verknüpfungen sind in Tabelle 1.1 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 1.1: 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 1.2: Wahrheitstafel zu $A \wedge B \Rightarrow B \wedge A$.

Definition 1.1. Tautologie.
Ist φ eine Formel, die bezüglich jeder möglichen Variablenbelegung erfüllt ist, dann nennt man φ eine Tautologie und schreibt dafür kurz $\models \varphi$.

Z. B. gilt

$$\models A \wedge B \implies B \wedge A.$$

Es lässt sich leicht überprüfen, ob eine Formel tautologisch ist. Dazu wird einfach die Wahrheitstafel zu dieser Formel aufgestellt, hier Tabelle 1.2. 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 1.1. 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 1.2. 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 1.3. 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 1.4. 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 1.5. 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**	**Gesetze**
$A \wedge B \equiv B \wedge A$	$A \vee B \equiv B \vee A$	Kommutativgesetze
$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$	$A \vee (B \vee C) \equiv (A \vee B) \vee C$	Assoziativgesetze
$A \wedge A \equiv A$	$A \vee A \equiv A$	Idempotenzgesetze
$A \wedge 1 \equiv A$	$A \vee 0 \equiv A$	Neutralitätsgesetze
$A \wedge 0 \equiv 0$	$A \vee 1 \equiv 1$	Extremalgesetze
$A \wedge \overline{A} \equiv 0$	$A \vee \overline{A} \equiv 1$	Komplementärgesetze
$\overline{A \wedge B} \equiv \overline{A} \vee \overline{B}$	$\overline{A \vee B} \equiv \overline{A} \wedge \overline{B}$	De Morgansche Gesetze
$A \wedge (A \vee B) \equiv A$	$A \vee (A \wedge B) \equiv A$	Absorptionsgesetze

Tabelle 1.3: Die Regeln der booleschen Algebra.

Definition 1.2. 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 1.6.
Die Relation $\varphi \equiv \psi$ ist eine Äquivalenzrelation, d. h. es gilt

$$\varphi \equiv \varphi, \qquad \text{(Reflexivität)} \tag{1.1}$$
$$(\varphi \equiv \psi) \implies (\psi \equiv \varphi), \qquad \text{(Symmetrie)} \tag{1.2}$$
$$(\varphi \equiv \psi) \wedge (\psi \equiv \chi) \implies (\varphi \equiv \chi). \qquad \text{(Transitivität)} \tag{1.3}$$

1.1.2 Boolesche Algebra

Die Regeln in Tabelle 1.3 gewinnt man alle mittels Warheitstafel. Gemäß der Einsetzungsregel dürfen für die Variablen auch Formeln eingesetzt werden, die griechischen Formelvariablen benötigt man somit nicht mehr.

Weiterhin gelten die Distributivgesetze

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C), \tag{1.4}$$
$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C). \tag{1.5}$$

Schließlich gibt es noch das Involutionsgesetz

$$\overline{\overline{A}} \equiv A. \tag{1.6}$$

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

$$A \Rightarrow B \equiv \overline{A} \vee B, \tag{1.7}$$
$$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A). \tag{1.8}$$

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 Warheitstafel auch

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

überprüfen.

Satz 1.7. Formel zum Modus ponens.
Es gilt $\models A \wedge (A \Rightarrow B) \Rightarrow B$

Beweis. Gemäß den Regeln der booleschen Algebra ergibt sich

$$\begin{aligned}
&A \wedge (A \Rightarrow B) \Rightarrow B && && (1.9)\\
&\equiv A \wedge (\overline{A} \vee B) \Rightarrow B && \text{(Zerlegung von »⇒«)} && (1.10)\\
&\equiv \overline{A \wedge (\overline{A} \vee B)} \vee B && \text{(Zerlegung von »⇒«)} && (1.11)\\
&\equiv \overline{A} \vee \overline{\overline{A} \vee B} \vee B && \text{(De Morgan)} && (1.12)\\
&\equiv \overline{A} \vee (\overline{\overline{A}} \wedge \overline{B}) \vee B && \text{(De Morgan)} && (1.13)\\
&\equiv \overline{A} \vee (A \wedge \overline{B}) \vee B && \text{(Involutionsgesetz)} && (1.14)\\
&\equiv ((\overline{A} \vee A) \wedge (\overline{A} \vee \overline{B})) \vee B && \text{(Distributivgesetz)} && (1.15)\\
&\equiv (1 \wedge (\overline{A} \vee \overline{B})) \vee B && \text{(Komplementärgesetz)} && (1.16)\\
&\equiv (\overline{A} \vee \overline{B}) \vee B && \text{(Absorptionsgesetz)} && (1.17)\\
&\equiv \overline{A} \vee (\overline{B} \vee B) && \text{(Assoziativgesetz)} && (1.18)\\
&\equiv \overline{A} \vee 1 && \text{(Komplementärgesetz)} && (1.19)\\
&\equiv 1. \ \square && \text{(Absorptionsgesetz)} && (1.20)
\end{aligned}$$

Von der Ersetzungsregel (Satz 1.2), also

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

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

Satz 1.8. Regel zur Kontraposition.
Es gilt $A \Rightarrow B \equiv \overline{B} \Rightarrow \overline{A}$.

Beweis. Man findet

$$\begin{aligned}
&A \Rightarrow B && && (1.21)\\
&\equiv \overline{A} \vee B && \text{(Zerlegung von »⇒«)} && (1.22)\\
&\equiv B \vee \overline{A} && \text{(Kommutativgesetz)} && (1.23)\\
&\equiv \overline{\overline{B}} \vee \overline{A} && \text{(Involutionsgesetz)} && (1.24)\\
&\equiv \overline{B} \Rightarrow \overline{A}. \ \square && \text{(Zerlegung von »⇒«)} && (1.25)
\end{aligned}$$

1.1.3 Formale Beweise

Definition 1.3. 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 erüllt.

Das klingt etwas kompliziert, ist es aber eigentlich nicht. Man schaut sich die große Wahrheitstafel an, in der alle Formeln vorkommen. Ergibt sich in einer Zeile bei allen Formeln in M eine 1, dann muss auch ψ in dieser Zeile den Warheitswert 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 Warheitswert 0, dann ist $\varphi \Rightarrow \psi$ immer erfüllt, ohne dass der Warheitswert 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 1.9. Deduktionstheorem.
Es gilt $M \cup \{\varphi\} \models \psi$ genau dann, wenn $M \models \varphi \Rightarrow \psi$.

Beweis. Man hat

$$M \cup \varphi = \{\varphi_1, \ldots, \varphi_n, \varphi\}. \tag{1.26}$$

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

$$\varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi \tag{1.27}$$

unter dieser Belegung erfüllt ist. Wie bereits erläutert, gilt

$$(\{\varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi\} \models \psi) \iff (\models \varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi \Rightarrow \psi). \tag{1.28}$$

Mittels boolescher Algebra findet man nun

$$\begin{aligned}
&\varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi \Rightarrow \psi && (1.29)\\
&\equiv \overline{\varphi_1 \wedge \ldots \wedge \varphi_n \wedge \varphi} \vee \psi && (1.30)\\
&\equiv \overline{\varphi_1 \wedge \ldots \wedge \varphi_n} \vee \overline{\varphi} \vee \psi && (1.31)\\
&\equiv \overline{\varphi_1 \wedge \ldots \wedge \varphi_n} \vee (\varphi \Rightarrow \psi) && (1.32)\\
&\equiv \varphi_1 \wedge \ldots \wedge \varphi_n \Rightarrow (\varphi \Rightarrow \psi) && (1.33)
\end{aligned}$$

Schließlich gilt aber auch wieder

$$(\models \varphi_1 \wedge \ldots \wedge \varphi_n \Rightarrow (\varphi \Rightarrow \psi)) \iff (\{\varphi_1 \wedge \ldots \wedge \varphi_n\} \models \varphi \Rightarrow \psi). \quad \square \tag{1.34}$$

Definition 1.4. Schlussregel.
Sei M eine Menge von Formelvariablen 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 1.10. 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 1.7 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 1.5. 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.

1.1.4 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

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

1.1.5 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, übrigt bleibt $\models \overline{A}$.

Wir gelangen zur folgenden Schlussregel.

Satz 1.11. 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

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

Wiedermalig 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 1.12. 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.

1.2 Prädikatenlogik

1.2.1 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 1.6. 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 1.7. 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. In allen diesen Schreibweisen haben die Quantoren die gleiche Operatorrangfolge wie die Negation. Z. B. wird die Formel

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

gelesen als

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

Davon zu unterscheiden ist die Formel

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

Satz 1.13. 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 1.14. 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 1.15. 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 1.16. 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. Indunktionsanfang:

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

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 1.15.

Für den Existenzquantor ist die Argumentation analog. □

1.2.2 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 1.8. Allquantor.
Es gilt $(\forall x)P(x)$ genau dann, wenn $P(x)$ für jedes beliebige x wahr ist.

Definition 1.9. 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 Warheitstafeln 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 1.17.
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 1.18. 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 1.19. 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

$$\neg(\forall x)P(x) \equiv \neg 1 \equiv 0 \equiv (\exists x)0 \equiv (\exists x)\,\neg 1 \equiv (\exists x)\,\neg P(x). \tag{1.35}$$

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

$$\neg(\forall x)P(x) \equiv \neg 0 \equiv 1 \equiv (\exists x)1 \equiv (\exists x)\,\neg P(x). \tag{1.36}$$

Die Argumentation für den Existenzquantor ist analog. □

Satz 1.20. 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

$$(\forall x)(P(x) \wedge Q(x)) \equiv 1 \equiv 1 \wedge 1 \equiv (\forall x)P(x) \wedge (\forall x)Q(x). \tag{1.37}$$

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

$$(\forall x)P(x) \wedge (\forall x)Q(x) \equiv 0. \tag{1.38}$$

Für den Existenzquantor ist die Argumentation analog. Alternativ ergibt sich nach den De Morgenschen und verallgemeinerten De Morganschen Gesetzen

$$(\exists x)(P(x) \vee Q(x)) \equiv \neg(\forall x)\,\neg(P(x) \vee Q(x)) \tag{1.39}$$
$$\equiv \neg(\forall x)(\neg P(x) \wedge \neg Q(x)) \equiv \neg((\forall x)\,\neg P(x) \wedge (\forall x)\,\neg Q(x)) \tag{1.40}$$
$$\equiv \neg(\forall x)\,\neg P(x) \vee \neg(\forall x)\,\neg Q(x) \equiv (\exists x)P(x) \vee (\exists x)Q(x).\ \square \tag{1.41}$$

1.2.3 Beschränkte Quantifizierung

Definition 1.10. 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 sogar

$$(\forall R(x))P(x) :\equiv (\forall x)(R(x) \Rightarrow P(x)), \tag{1.42}$$
$$(\exists R(x))P(x) :\equiv (\exists x)(R(x) \wedge P(x)), \tag{1.43}$$

solange klar bleibt, dass x die gebundene Variable ist.

Satz 1.21. 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

$$A \vee (\forall x \in M)P(x) \equiv A \vee (\forall x)(x \in M \Rightarrow P(x)) \tag{1.44}$$
$$\equiv A \vee (\forall x)(\neg x \in M \vee P(x)) \equiv (\forall x)(A \vee \neg x \in M \vee P(x)) \tag{1.45}$$
$$\equiv (\forall x)(x \in M \Rightarrow A \vee P(x)) \equiv (\forall x \in M)(A \vee P(x)). \tag{1.46}$$

Für den Existenzquantor gilt

$$A \wedge (\exists x \in M)P(x) \equiv A \wedge (\exists x)(x \in M \wedge P(x)) \tag{1.47}$$
$$\equiv (\exists x)(A \wedge x \in M \wedge P(x)) \equiv (\exists x)(x \in M \wedge A \wedge P(x)) \tag{1.48}$$
$$\equiv (\exists x \in M)(A \wedge P(x)). \square \tag{1.49}$$

Satz 1.22. 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

$$\neg(\forall x \in M)P(x) \equiv \neg(\forall x)(x \in M \Rightarrow P(x)) \equiv \neg(\forall x)(\neg x \in M \vee P(x)) \tag{1.50}$$
$$\equiv (\exists x)(x \in M \wedge \neg P(x)) \equiv (\exists x \in M)\ \neg P(x). \tag{1.51}$$

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

1.3 Mengenlehre

1.3.1 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 das selbe Objekt immer nur ein einziges mal im Beutel enthalten ist. Legt man zweimal das selbe 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

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

1.3.2 Teilmengen

Definition 1.11. 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.

1.3.3 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:

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

Die Menge der natürlichen Zahlen ohne die Null:

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

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 1.4: 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 Zifferengruppe 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.

1.3.4 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 1.12. 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 1.23.
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. □

1.3.5 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:

$$\begin{aligned} \mathbb{N}_0 &= \{n \in \mathbb{Z} \mid n \geq 0\}, \\ \mathbb{N} &= \{n \in \mathbb{Z} \mid n > 0\}. \end{aligned}$$

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

Definition 1.13. Beschränkte Beschreibung einer Menge.
Die Menge der $x \in M$, welche die Aussage $P(x)$ erfüllen, ist definiert durch die folgende logische Äquivalenz:

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

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 graden 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 1.14. 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 1.24.
Es gilt

$$a \in \{x \mid P(x)\} \iff P(a), \tag{1.52}$$
$$\{x \in A \mid P(x)\} = \{x \mid x \in A \wedge P(x)\}. \tag{1.53}$$

Beweis. Gemäß Definition 1.14 und 1.13 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 (1.53) wird mit Satz 1.23 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 1.13 und der schon bewiesenen Aussage (1.52) aber vereinfacht werden kann zu

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

1.3.6 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 umgehen, indem man nur logisch die Existenz eines Bildes zu jedem $x \in A$ verlagt, 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.

1.3.7 Mengenoperationen

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

Definition 1.15. 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 1.16. 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 1.25.
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 1.23 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 (1.52) und Definition 1.13 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:

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

1.3.8 Produktmengen

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

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

Definition 1.17. 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 1.26.
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 1.23 und (1.52) 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 1.27.
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 $X \times Y$. □

1.4 Abbildungen

1.4.1 Grundbegriffe

Seien zwei beliebige Mengen A, B gegeben. Eine Abbildung $f\colon A \to B$ ist eine Zuordnug, 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 $f\colon A \to B$ 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 1.18. 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 1.19. Bildmenge.
Sei $f\colon A \to B$ 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 1.20. Urbildmenge.
Sei $f\colon A \to B$ 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.

1.4.2 Verkettung von Abbildungen

Definition 1.21. 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 1.22. 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 1.28. Bildmenge unter Verkettungen.
Seien $f\colon A \to B$ und $g\colon B \to C$, dann gilt $(g \circ f)(M) = g(f(M))$.

Beweis. Die Gleichung gemäß Definition expandieren:

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

Auf der rechten Seite ergibt sich nun

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

1.4.3 Injektionen, Surjektionen, Bijektionen

Definition 1.23. 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 1.24. 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 1.25. Bijektive Abbildung.
Eine Abbildung heißt bijektiv, wenn sie sowohl injektiv als auch surjektiv ist.

Satz 1.29.
Sei $f : A \to B$ und $g : B \to C$. 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 1.28. Somit ist auch $g \circ f$ surjektiv. □

1.5 Relationen

1.5.1 Grundbegriffe

Definition 1.26. 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 $A \times B$.

1.5.2 Äquivalenzrelationen

Definition 1.27. 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 1.28. 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 1.30. 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 1.31. 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 1.29. 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 1.30. Quotientenabbildung.
Für eine gegebene Äquivalenzrelation ist die Projektion

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

surjektiv und wird Quotientenabbildung genannt.

Definition 1.31. 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.

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

$$\begin{aligned} f^{-1}(\{y_1\}) \cap f^{-1}(\{y_2\}) &= \{x \mid f(x) = y_1\} \cap \{x \mid f(x) = y_2\} \\ &= \{x \mid f(x) = y_1 \wedge f(x) = y_2\} = \{\}. \end{aligned}$$

Im letzten Schritt wurde beachtet, dass eine Abbildung für das selbe Argument definitionsgemäß keine zwei unterschiedlichen Werte annehmen kann.

Demnach ist gemäß

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

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

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

Satz 1.32. Charakterisierung von Äquivalenzklassen.
Sei auf der Menge M eine Äquivalenzrelation gegeben. Eine Teilmenge $A \subseteq M$ ist genau dann eine Äquivalenzklasse, wenn

1. $A \neq \{\}$,
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 $A \neq \{\}$. 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 $A = \{x \in M \mid x \sim a\}$. □

1.6 Gleichungen

1.6.1 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.

1.6.2 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 1.33. Äquivalenzumformungen.
Seien a, b, c beliebige Zahlen. Dann gilt

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

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

Satz 1.34. 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 1.33 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 1.35. 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

$$\begin{aligned} ra = rb &\iff \frac{m}{n}a = \frac{m}{n}b \overset{\text{Satz 1.34}}{\iff} n \cdot \frac{m}{n}a = n \cdot \frac{m}{n}b \\ &\iff ma = mb \overset{\text{Satz 1.34}}{\iff} a = b. \end{aligned}$$

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 1.36. 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

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

1.7 Ungleichungen

1.7.1 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 1.32. 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«.

1.7.2 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 der selben Zahl auf beiden Seiten daraus keine wahre Ungleichung gewinnen. Die analoge Argumentation gilt für die Subtraktion der selben Zahl. Anstelle von ganzen Äpfeln kann man natürlich auch Apfelhälften hinzufügen, oder allgmein Apfelbruchteile. Die Argumentation gilt unverändert.

Wir halten fest.

Satz 1.37. Äquivalenzumformungen von Ungleichungen.

Seien a, b, c beliebige Zahlen. Dann sind die folgenden Äquivalenzen gültig:

$$a < b \iff a + c < b + c, \tag{1.54}$$
$$a < b \iff a - c < b - c, \tag{1.55}$$
$$a \leq b \iff a + c \leq b + c, \tag{1.56}$$
$$a \leq b \iff a - c \leq b - c. \tag{1.57}$$

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

$$a < b \iff na < nb, \tag{1.58}$$
$$a \leq b \iff na \leq nb. \tag{1.59}$$

Beweis. Aus der Ungleichung $a < b$ erhält man mittels (1.55) 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 (1.54) bringt dann $na < nb$.

In Kürze formuliert:

$$a < b \iff 0 < b - a \iff 0 < n(b - a) = nb - na \iff na < nb. \tag{1.60}$$

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

Alternativer Beweis. Mittels (1.54) ergibt sich zunächst:

$$a < b \iff \begin{Bmatrix} a + a < b + a \\ a + b < b + b \end{Bmatrix} \iff 2a < a + b < 2b. \tag{1.61}$$

Unter nochmaliger Anwendung von (1.54) ergibt sich nun

$$a < b \iff \begin{Bmatrix} 2a < a + b \iff 3a < 2a + b \\ 2a < 2b \iff 2a + b < 3b \end{Bmatrix} 3a < 2a + b < 3b \tag{1.62}$$

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 (1.54) bringt

$$na < (n-1)a + b \iff (n+1)a < na + b \tag{1.63}$$

und Addition von b gemäß (1.54) bringt

$$na < nb \iff na + b < (n+1)b. \tag{1.64}$$

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

Wir können sogleich einen Schritt weiter gehen.

Satz 1.39. Äquivalenzumformungen von Ungleichungen.
Seien a, b beliebige Zahlen und sei $r > 0$ eine rationale Zahl, dann gelten die folgenden Äquivalenzen:

$$a < b \iff ra < rb \iff a/r < b/r, \tag{1.65}$$
$$a \leq b \iff ra \leq rb \iff a/r \leq b/r. \tag{1.66}$$

Beweis. Eine rationale Zahl $r > 0$ lässt sich immer Zerlegen in einen Quotienten $r = m/n$, wobei m, n positive natürliche Zahlen sind. Gemäß (1.58) gilt

$$\frac{m}{n} \cdot a < \frac{m}{n} \cdot b \iff n \cdot \frac{m}{n} \cdot a < n \cdot \frac{m}{n} \cdot b \iff ma < mb. \tag{1.67}$$

Gemäß (1.58) gilt aber auch

$$a < b \iff ma < mb. \tag{1.68}$$

Die Zusammenfassung beider Äquivalenzen ergibt

$$a < b \iff \frac{m}{n} \cdot a < \frac{m}{n} \cdot b \iff ra < rb. \tag{1.69}$$

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

$$a < b \iff ra < rb \iff a/r < b/r, \tag{1.70}$$
$$a \leq b \iff ra \leq rb \iff a/r \leq b/r. \tag{1.71}$$

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

1.7.3 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 (1.55) 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 z. B.

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

1.7.4 Monotone Funktionen

Definition 1.33. 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 1.41. 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:

$$f^{-1}(y_2) \leq f^{-1}(y_1) \implies \underbrace{f(f^{-1}(y_2))}_{=y_2} \leq \underbrace{f(f^{-1}(y_1))}_{=y_1}. \quad \square \tag{1.72}$$

Definition 1.34. 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 1.42. 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 (1.54) nichts anderes als die strenge Monotonie für $f(x) := x + c$. Und (1.58) 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 (1.71) 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 Ansätze zur Problemlösung

2.1 Substitution

2.1.1 Quadratische Gleichungen

Vorgelegt ist eine quadratische Gleichung in Normalform

$$x^2 + px + q = 0. \tag{2.1}$$

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

$$0 = (u + d)^2 + p(u + d) + q = u^2 + 2ud + d^2 + pu + pd + q \tag{2.2}$$

$$= u^2 + (p + 2d)u + (d^2 + pd + q). \tag{2.3}$$

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

$$q' := d^2 + pd + q = \left(-\frac{p}{2}\right)^2 - p \cdot \frac{p}{2} + q = \frac{p^2}{4} - \frac{p^2}{2} + q \tag{2.4}$$

$$= \frac{p^2}{4} - 2\frac{p^2}{4} + q = -\frac{p^2}{4} + q. \tag{2.5}$$

Zu lösen ist nunmehr die quadratische Gleichung

$$u^2 + q' = 0. \tag{2.6}$$

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

$$x - d = x + \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q} = \pm\frac{1}{2}\sqrt{p^2 - 4q}. \tag{2.7}$$

Man erhält die Lösungsformel

$$x = -\frac{p}{2} \pm \frac{1}{2}\sqrt{p^2 - 4q}. \tag{2.8}$$

2.1.2 Biquadratische Gleichungen

Die biquadratische Gleichung

$$x^4 + px^2 + q = 0 \tag{2.9}$$

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

$$u^2 + pu + q \tag{2.10}$$

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

$$x_1 = \sqrt{u_1}, \quad x_2 = -\sqrt{u_1}, \quad x_3 = \sqrt{u_2}, \quad x_4 = -\sqrt{u_2} \tag{2.11}$$

3 Kombinatorik

3.1 Endliche Summen

3.1.1 Definition

Definition 3.1. 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:

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

3.1.2 Rechenregeln

Satz 3.1. 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

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

Satz 3.2. 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:

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

Satz 3.3. 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:

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

Satz 3.4. 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 3.5. 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 3.4 (Indexshift) und Satz 3.3 (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 3.6. Summe 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 3.7. Summe 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 3.5 umgekehrt. Danach wendet man Satz 3.2 (Additivität), Satz 3.1 (Homogenität) und Satz 3.6 an:

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

3.1.3 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.

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

3.2 Endliche Produkte

3.2.1 Definition

Definition 3.2. 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

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

3.2.2 Rechenregeln

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

Satz 3.8.
Ist $c \in \mathbb{R}$ eine Konstante, dann gilt

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

Satz 3.9.
Es gilt

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

Satz 3.10. 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 3.11. Indexshift.
Für die Indexverschiebung der Distanz $d \in \mathbb{Z}$ gilt

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

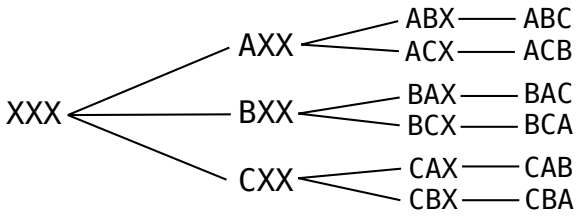
3.3 Permutationen und Variationen

3.3.1 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 3.3. 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.

3.3.2 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 3.4. 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 3.12.
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 »$A(k-1) \Rightarrow A(k)$«:

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

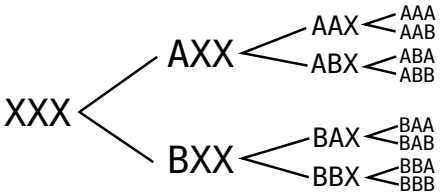
Hierbei wurde $(n-k+1)! = (n-k+1)(n-k)!$ benutzt, was gemäß der rekursiven Definition der Fakultät gilt.

Alternativer Beweis. Mittels Satz 3.10 (Produktaufteilung) und Satz 3.11 (Indexshift):

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

3.3.3 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. Ingesamt 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.

3.3.4 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 auf's 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

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

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

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

4 Zahlentheorie

4.1 Kongruenzen

Definition 4.1. 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 4.1.
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 $b - c = lm$. D. h. 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 4.2.
Sind a, b, c ganze Zahlen, dann gilt

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

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

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

Für die Subtraktion von c ist die Überlegung analog. □

Satz 4.3.
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 4.4.
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

$$\left.\begin{aligned} a \equiv a' &\implies a + b \equiv a' + b \\ b \equiv b' &\implies a' + b \equiv a' + b' \end{aligned}\right\} \implies a + b \equiv a' + b \equiv a' + b' \pmod{m}. \tag{4.1}$$

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

$$\left.\begin{aligned} a \equiv a' &\implies ab \equiv a'b \\ b \equiv b' &\implies a'b \equiv a'b' \end{aligned}\right\} \implies ab \equiv a'b \equiv a'b' \pmod{m}. \square \tag{4.2}$$

Satz 4.5.
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 $k = -1$. $\square$

Index