1 Mathematische Grundlagen

Wir geben hier einige mathematische Grundbegriffe, die eigentlich aus der Mathematik bekannt sind. Deshalb können die Kapitel 1.1–1.5 problemlos übersprungen werden.

Im Kapitel 1.6 werden Begriffe bereitgestellt, die im Scriptum verwendet werden.

1.1 Elementare Aussagenlogik

Bevor wir zu einigen Grundaussagen der elementaren Aussagenlogik kommen, führen wir hier den Begriff der Menge ein.

Definition 1.1 *Jede Zusammenfassung von bestimmten, wohlunterschiedenen Objekten zu einem Ganzen wird Menge genannt. Die so zusammengefassten Objekte heißen Elemente der Menge.*

In der Regel bezeichnen wir Mengen mit großen lateinischen Buchstaben und Elemente mit kleinen lateinischen Buchstaben. Es folgen einige Beispiele von Mengen.

Beispiel 1.2 (i) M_1 sei die Menge der Vokale im deutschen Alphabet.

(ii) M_2 ist die Menge der natürlichen Zahlen, die kleiner als 10 sind.

(iii) M_3 ist die Menge der ganzen Zahlen, die Lösung der Gleichung $2x^2 + 3x - 2 = 0$ sind.

Die Zugehörigkeit eines Objektes zu einer Menge wird durch das Element-Zeichen „$\in$“ beschrieben. Entsprechend besagt „$\notin$“, dass ein Objekt nicht Element der Menge ist. So schreibt man zum Beispiel:

$$\begin{array}{lll} a \in M_1 & 5 \in M_2 & -2 \in M_3 \\ s \notin M_1 & 10 \notin M_2 & \frac{1}{2} \notin M_3 \end{array}$$

Sprechweisen sind z. B.: „a ist Element von M_1“, „s ist nicht Element von M_1“ oder „a ist kein Element von M_1“.

Im Folgenden bezeichnen wir die Menge der natürlichen Zahlen, die Menge der ganzen Zahlen, die Menge der rationalen Zahlen und die Menge der reellen Zahlen mit $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ bzw. $\mathbb{R}$.

Wir wollen jetzt einige Grundbegriffe der Aussagenlogik zusammenstellen, insbesondere auch eine Symbolik einführen, die es uns erleichtert, umgangssprachlich kompliziertere Wendungen sauber und präzise aufzuschreiben.

Definition 1.3 *Unter einer Aussage verstehen wir ein sprachliches Gebilde, das die Eigenschaft hat, eindeutig entweder wahr oder falsch zu sein oder – wie wir auch sagen – genau einen der Wahrheitswerte „wahr“ $(W, 1)$ oder „falsch“ $(F, 0)$ zu haben.*

Beispiel 1.4 Wir geben hier einige Beispiele für Aussagen:

(i) 15 ist eine Primzahl.

(ii) Zu keiner natürlichen Zahl n mit $n > 2$ lassen sich drei positive ganze Zahlen x, y, z angeben, dass $x^n + y^n = z^n$ ist.

(iii) $\int_0^\pi \sin x \, \mathrm{d}x = 2.$

(iv) Es gibt unendlich viele Primzahlzwillinge.

Die Aussagen 2 und 3 sind wahr, die Aussage 1 ist falsch, von der Aussage 4 wissen wir leider nicht, ob sie wahr oder falsch ist. Aus der Aussage 3 erkennen wir, dass wir natürlich bei der Formulierung von Aussagen eine mathematische Formelsprache oder andere eindeutige Vereinbarungen zulassen.

Beispiel 1.5 Wir wollen auch einige Sätze angeben, die leicht erkennbar keine Aussagen sind, da man ihnen nicht eindeutig genau einen Wahrheitswert zuordnen kann:

(i) x ist eine Primzahl.

(ii) Heute ist Dienstag.

Betrachtet man im Beispiel 1.5 den Satz 1, so erkennt man, dass es sich zwar um keine Aussage handelt, aber wenn man die Variable x durch konkrete Werte ersetzt, so erhält man eine Aussage. Damit kommen wir zur nächsten Definition.

Definition 1.6 *Eine Aussageform hat die Gestalt einer Aussage, in der eine oder mehrere Variable auftreten und besitzt die Eigenschaft, dass man jedesmal eine Aussage erhält, wenn man für diese Variablen beliebige Elemente eines Variablengrundbereiches einsetzt. Wir bezeichnen eine Aussageform mit den Variablen $x_1, x_2, \ldots, x_n$ mit $p(x_1, x_2, \ldots, x_n)$.*

Also handelt es sich im Beispiel 1.5 bei dem Satz 1 mit der Variablen x z. B. aus dem Grundbereich $\mathbb{N}$ um eine Aussageform. Sie wird wahr, wenn wir z. B. für x die Zahlen $2, 3, 31$ oder $2\,147\,483\,647$ einsetzen. Sie wird falsch, wenn wir z. B. für x die Zahlen $1, 4, 18$, oder $89\,687\,671\,441$ einsetzen.

Durch Aussageverbindungen können wir aus gegebenen Aussagen neue Aussagen konstruieren.

Definition 1.7 *Sei p eine Aussage, so ist $\neg p$ wiederum eine Aussage, deren Wahrheitswert genau der entgegengesetzte von p ist. Die einstellige Aussageverbindung $\neg p$ heißt Negation von p, gesprochen: „nicht p“ oder „non p“.*

Wir können die Definition durch folgende so genannte *Wahrheitstabelle* veranschaulichen.

p	$\neg p$
1	0
0	1

Definition 1.8 *Seien p und q Aussagen, so führen wir folgende zweistellige Aussageverbindungen ein.*

(i) *$p \wedge q$ heißt Konjunktion von p und q und besitzt genau dann den Wahrheitswert 1, wenn sowohl p als auch q den Wahrheitswert 1 besitzen. Gesprochen: „p und q“.*

(ii) *$p \vee q$ heißt Alternative oder Disjunktion von p und q und besitzt genau dann den Wahrheitswert 0, wenn sowohl p als auch q den Wahrheitswert 0 besitzen. Gesprochen: „p oder q“.*

(iii) *$p \Rightarrow q$ heißt Implikation von p und q und besitzt genau dann den Wahrheitswert 0, wenn p den Wahrheitswert 1 und q den Wahrheitswert 0 besitzen. Gesprochen: „p impliziert q“ oder aus „p folgt q“ oder auch „Wenn p, so q“.*

(iv) *$p \Leftrightarrow q$ heißt Äquivalenz von p und q und besitzt genau dann den Wahrheitswert 1, wenn p und q den gleichen Wahrheitswert besitzen. Gesprochen: „p genau dann, wenn q“.*

Wir können die Definitionen wiederum durch folgende Wahrheitstabellen verdeutlichen.

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Entsprechend den Aussageverbindungen können wir auch von Aussageformen Verbindungen bilden, deren Variable durch Elemente ein und desselben Variablengrundbereichs ersetzt werden dürfen.

In der Menge der Aussageverbindungen definieren wir:

Definition 1.9 *Zwei Aussageverbindungen p und q heißen logisch äquivalent, wenn sie unabhängig von der Belegung der Einzelaussagen stets den gleichen Wahrheitswert liefern. In Zeichen: $p \equiv q$.*

Es folgen ohne Wertigkeit der Reihenfolge und ohne Anspruch auf Vollständigkeit einige logische Äquivalenzen von Aussageverbindungen.

Satz 1.10 *Seien p, q und r Aussagen, dann gelten folgende logische Äquivalenzen.*

$$\neg(\neg p) \equiv p \quad (\textit{Doppelte Negation}), \tag{1.1}$$
$$p \wedge q \equiv q \wedge p \quad (\textit{Kommutativität von } \wedge), \tag{1.2}$$
$$p \vee q \equiv q \vee p \quad (\textit{Kommutativität von } \vee), \tag{1.3}$$
$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \quad (\textit{Assoziativität von } \wedge), \tag{1.4}$$
$$(p \vee q) \vee r \equiv p \vee (q \vee r) \quad (\textit{Assoziativität von } \vee), \tag{1.5}$$
$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \quad (\textit{Distributivität von } \wedge \textit{ bezüglich } \vee), \tag{1.6}$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \quad (\textit{Distributivität von } \vee \textit{ bezüglich } \wedge), \tag{1.7}$$
$$p \Rightarrow q \equiv \neg p \vee q \quad (\textit{Darstellung der Implikation durch eine Alternative}), \tag{1.8}$$
$$p \Rightarrow q \equiv \neg q \Rightarrow \neg p \quad (\textit{Kontraposition}), \tag{1.9}$$
$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p), \tag{1.10}$$
$$\neg(p \wedge q) \equiv \neg p \vee \neg q \quad (\textit{De Morgansche Regel}), \tag{1.11}$$
$$\neg(p \vee q) \equiv \neg p \wedge \neg q \quad (\textit{De Morgansche Regel}), \tag{1.12}$$
$$p \wedge (q \vee \neg q) \equiv p, \tag{1.13}$$
$$p \vee (q \wedge \neg q) \equiv p. \tag{1.14}$$

Man kann logische Äquivalenzen (also auch die im Satz 1.10) über Wahrheitstabellen oder durch die Benutzung bereits bewiesener logischer Äquivalenzen beweisen. Wir geben je ein Beispiel:

Wir beweisen die logische Äquivalenz (1.8) durch eine Wahrheitstabelle. Wir gehen also einfach alle Fälle der Belegungen der Einzelaussagen durch und zeigen, in jedem Fall liefern die beiden Aussageverbindungen $p \Rightarrow q$ und $\neg p \vee q$ den gleichen Wahrheitswert:

p	q	$\boldsymbol{p \Rightarrow q}$	$\neg p$	$\boldsymbol{\neg p \vee q}$
1	1	**1**	0	**1**
1	0	**0**	0	**0**
0	1	**1**	1	**1**
0	0	**1**	1	**1**

Wir führen jetzt den Beweis für die Aussage (1.9) durch die Benutzung bekannter logischer Äquivalenzen, wobei wir annehmen, die logischen Äquivalenzen (1.1), (1.3) und (1.8). seien schon bewiesen:

$$\begin{aligned} p \Rightarrow q &\equiv \neg p \vee q && \text{nach (1.8)},\\ &\equiv q \vee \neg p && \text{nach (1.3)},\\ &\equiv \neg(\neg q) \vee \neg p && \text{nach (1.1)},\\ &\equiv \neg q \Rightarrow \neg p && \text{nach (1.8)}. \end{aligned}$$

Schließlich können wir aufgrund der Transitivität der logischen Äquivalenz $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ schließen, womit die Gleichung (1.9) bewiesen ist.

Definition 1.11 *Eine Aussageverbindung heißt Tautologie, wenn sie unabhängig von der Belegung der Einzelaussagen stets den Wahrheitswert* 1 *besitzt.*

Definition 1.12 *Eine Aussageverbindung heißt Kontradiktion, wenn sie unabhängig von der Belegung der Einzelaussagen stets den Wahrheitswert* 0 *besitzt.*

Satz 1.13 *Es seien p und q Aussagen. Folgende Aussageverbindungen sind Tautologien:*

$$p \vee \neg p \quad (\textit{Satz vom ausgeschlossenen Dritten}), \tag{1.15}$$
$$(p \Rightarrow \neg p) \Rightarrow \neg p, \tag{1.16}$$
$$(p \wedge (p \Rightarrow q)) \Rightarrow q, \tag{1.17}$$
$$(p \wedge q) \Rightarrow p, \tag{1.18}$$
$$p \Rightarrow (p \vee q), \tag{1.19}$$
$$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r)), \tag{1.20}$$
$$(((p \Rightarrow q) \wedge (q \Rightarrow r)) \wedge p) \Rightarrow r. \tag{1.21}$$

Man kann Tautologien (also auch die im Satz 1.13) über Wahrheitstabellen oder aber durch Benutzung von logischen Äquivalenzen beweisen. Beispiele seien dem Leser überlassen.

Wir nennen hier noch einen Zusammenhang zwischen den Begriffen *Tautologie* und *logischer Äquivalenz*:

Satz 1.14 *Es seien $\alpha(p_1, p_2, \ldots, p_n)$ und $\beta(p_1, p_2, \ldots, p_n)$ Aussageverbindungen über den Einzelaussagen $p_1, p_2, \ldots, p_n$. Dann gilt*

$$\alpha(p_1, p_2, \ldots, p_n) \equiv \beta(p_1, p_2, \ldots, p_n)$$

genau dann, wenn

$$\alpha(p_1, p_2, \ldots, p_n) \Leftrightarrow \beta(p_1, p_2, \ldots, p_n)$$

eine Tautologie ist.

Wir haben oben eine Möglichkeit kennengelernt, aus Aussageformen Aussagen zu machen, nämlich durch das Belegen der Variablen mit Objekten aus dem Variablengrundbereich. Eine weitere Möglichkeit besteht in der *Quantifizierung* von Variablen. Wir führen den *Allquantor* $\forall$ („Für alle ...“) und den *Existenzquantor* $\exists$ („es gibt ein ...“) ein, die manchmal auch *Generalisator* bzw. *Partikularisator* genannt werden.

Definition 1.15 *Es sei $p(x)$ eine Aussageform mit der Variablen x. Dann ist $\forall x \in G\ (p(x))$ eine Aussage und ist wahr genau dann, wenn $p(x)$ mit jeder Belegung $x \in G$ zu einer wahren Aussage wird.*

Definition 1.16 *Es sei $p(x)$ eine Aussageform mit der Variablen x. Dann ist $\exists x \in G\ (p(x))$ eine Aussage und ist wahr genau dann, wenn es eine Belegung $x \in G$ gibt, die $p(x)$ zu einer wahren Aussage macht.*

Oft wird bei Quantoren der Variablengrundbereich G nicht mit genannt, falls er aus dem Kontext zweifelsfrei ersichtlich ist. Wir benutzen also $\forall x\ (p(x))$ bzw. $\exists x\ (p(x))$ statt $\forall x \in G\ (p(x))$ und $\exists x \in G\ (p(x))$.

Für Quantifizierungen mehrstelliger Aussageformen verzichten wir auf die Klammern um die jeweilige äußere Aussageform und schreiben:

$$\begin{aligned}
&\forall x\ \forall y\ (p(x,y)) \ \text{ statt } \ \forall x\ (\forall y\ (p(x,y))),\\
&\exists x\ \exists y\ (p(x,y)) \ \text{ statt } \ \exists x\ (\exists y\ (p(x,y))),\\
&\forall x\ \exists y\ (p(x,y)) \ \text{ statt } \ \forall x\ (\exists y\ (p(x,y))),\\
&\exists x\ \forall y\ (p(x,y)) \ \text{ statt } \ \exists x\ (\forall y\ (p(x,y))).
\end{aligned}$$

Es gilt folgender Satz.

Satz 1.17 *Es seien $p(x)$ und $p(x,y)$ Aussageformen mit den Variablen x und y. Dann gilt*

$$\neg\forall x \in G\ (p(x)) \equiv \exists x \in G\ (\neg p(x)), \tag{1.22}$$
$$\neg\exists x \in G\ (p(x)) \equiv \forall x \in G\ (\neg p(x)), \tag{1.23}$$
$$\forall x \in G_1\ \forall y \in G_2\ (p(x,y)) \equiv \forall y \in G_2\ \forall x \in G_1\ (p(x,y)), \tag{1.24}$$
$$\exists x \in G_1\ \exists y \in G_2\ (p(x,y)) \equiv \exists y \in G_2\ \exists x \in G_1\ (p(x,y)), \tag{1.25}$$
$$\exists x \in G_1\ \forall y \in G_2\ (p(x,y)) \Rightarrow \forall y \in G_2\ \exists x \in G_1\ (p(x,y)). \tag{1.26}$$

1.2 Elementare Mengenlehre

Im Kapitel 1.1 wurden bereits die Begriffe *Menge* und *Element* einer Menge eingeführt. Wir wollen uns in diesem Kapitel mit einigen Aspekten der elementaren Mengenlehre beschäftigen, insbesondere mit Operationen auf Mengen.

Aber zuerst zu möglichen Beschreibungsarten von Mengen. Im Beispiel 1.2 haben wir bereits die verbale Beschreibung kennengelernt. Oft ist sie unzweckmäßig und unübersichtlich. Manchmal ist es günstiger, die Menge durch die Aufzählung aller ihrer Elemente anzugeben:

$$M_4 = \{a, e, i, o, u\},$$
$$M_5 = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Die Aufzählung aller Elemente ist wiederum ungünstig, wenn es sehr viele sind und gar nicht möglich, wenn es unendlich viele Elemente sind (man nennt eine Menge mit unendlich vielen Elementen *unendlich*, sonst *endlich*). In diesem Fall ist die Beschreibung der Menge durch eine definierende Eigenschaft angebracht:

$$M_6 = \{x \in \mathbb{N} \mid x^2 < 400\},$$
$$M_7 = \{x \in \mathbb{R} \mid 0 \le x \le 1\}.$$

gelesen als: „M_6 ist die Menge aller natürlichen Zahlen x für die $x^2 < 400$ gilt“. Mathematisch gesehen handelt es sich um die allgemeine Form

$$M = \{x \in G \mid H(x)\},$$

wobei G ein gewisser Variablengrundbereich ist und die „definierende Eigenschaft“ $H(x)$ eine Aussageform mit der Variablen x.

Es kann vorkommen, dass die Aussageform $H(x)$ durch kein Element x aus dem Variablengrundbereich G zu einer wahren Aussage gemacht wird, so dass wir von der *leeren Menge* sprechen, also von der Menge, die kein Element enthält. Sie wird mit dem Symbol $\emptyset$ bezeichnet.

Eine Bemerkung: die Menge $\{\emptyset\}$ ist nicht die leere Menge, da sie ein Element enthält, nämlich die leere Menge.

Definition 1.18 *Mit $|M|$ bezeichnen wir die Kardinalzahl einer Menge M.*

Für endliche Mengen M ist die Kardinalzahl $|M|$ die Anzahl ihrer Elemente. Insbesondere gilt $|\emptyset| = 0$. Für unendliche Mengen weise ich darauf hin, dass $|\mathbb{N}| \neq |\mathbb{R}|$ gilt. Wir kommen später darauf zurück.

Jetzt kommen einige wichtige Definitionen für Beziehungen zwischen Mengen.

Definition 1.19 *Zwei Mengen M_1 und M_2 in einem Variablengrundbereich G heißen gleich genau dann (in Zeichen $M_1 = M_2$), wenn*

$$\forall x \in G \ (x \in M_1 \Leftrightarrow x \in M_2)$$

gilt.

Definition 1.20 *Eine Menge M_1 heißt Teilmenge einer Menge M_2 in einem Variablengrundbereich G (in Zeichen $M_1 \subseteq M_2$), falls*

$$\forall x \in G \ (x \in M_1 \Rightarrow x \in M_2)$$

gilt.

Definition 1.21 *Eine Menge M_1 heißt echte Teilmenge einer Menge M_2 in einem Variablengrundbereich G (in Zeichen $M_1 \subsetneq M_2$), falls*

$$M_1 \subseteq M_2 \quad \textit{und} \quad M_1 \neq M_2$$

gilt.

Definition 1.22 *Sei M eine Menge. Die Menge aller Teilmengen von M heißt Potenzmenge und wird mit 2^M oder auch mit $\mathcal{P}(M)$ bezeichnet.*

Beispiel 1.23 Sei $M = \{1, 2, 3\}$, so ist $2^M = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Die Bezeichnung 2^M leitet sich von folgender Tatsache ab.

Folgerung 1.24 *Sei M eine endliche Menge mit $|M| = n$, $n \in \mathbb{N}$, so gilt $|2^M| = 2^n$.*

Wir betrachten folgende Operationen auf Mengen, das heißt, wir konstruieren aus gegebenen Mengen neue Mengen.

Definition 1.25 *Es sind die Mengen M_1 und M_2 in einem Grundbereich G gegeben, dann gelte:*

$$\begin{aligned}
\overline{M_1} &:= \{x \in G \mid x \notin M_1\} && (\textit{Komplement von } M_1 \textit{ bez. } G),\\
M_1 \cup M_2 &:= \{x \in G \mid x \in M_1 \vee x \in M_2\} && (\textit{Vereinigung von } M_1 \textit{ und } M_2),\\
M_1 \cap M_2 &:= \{x \in G \mid x \in M_1 \wedge x \in M_2\} && (\textit{Durchschnitt von } M_1 \textit{ und } M_2),\\
M_1 \setminus M_2 &:= \{x \in G \mid x \in M_1 \wedge x \notin M_2\} && (\textit{Differenz von } M_1 \textit{ und } M_2).
\end{aligned}$$

Beispiel 1.26 Es seien der Grundbereich $G = \{x \in \mathbb{N} \mid x < 6\}$ und die Mengen $M_1 = \{1, 2, 3\}$ und $M_2 = \{2, 3, 4\}$ gegeben. Dann ist $\overline{M_1} = \{4, 5, 6\}$, $M_1 \cup M_2 = \{1, 2, 3, 4\}$, $M_1 \cap M_2 = \{2, 3\}$ sowie $M_1 \setminus M_2 = \{1\}$.

Die oben definierten Operationen auf Mengen kann man durch so genannte VENN-Diagramme veranschaulichen (siehe Abbildung 1.1). Man möge aber beachten, dass solche graphischen Veranschaulichungen nicht geeignet sind, Allaussagen über Mengen zu beweisen. Allerdings kann man mit solchen Diagrammen Existenzaussagen beweisen, da die Darstellungen nämlich Punktmengen in der Ebene verkörpern.

Für die definierten Mengenoperationen können wir folgende Aussagen aufstellen (ohne Anspruch auf Vollständigkeit).

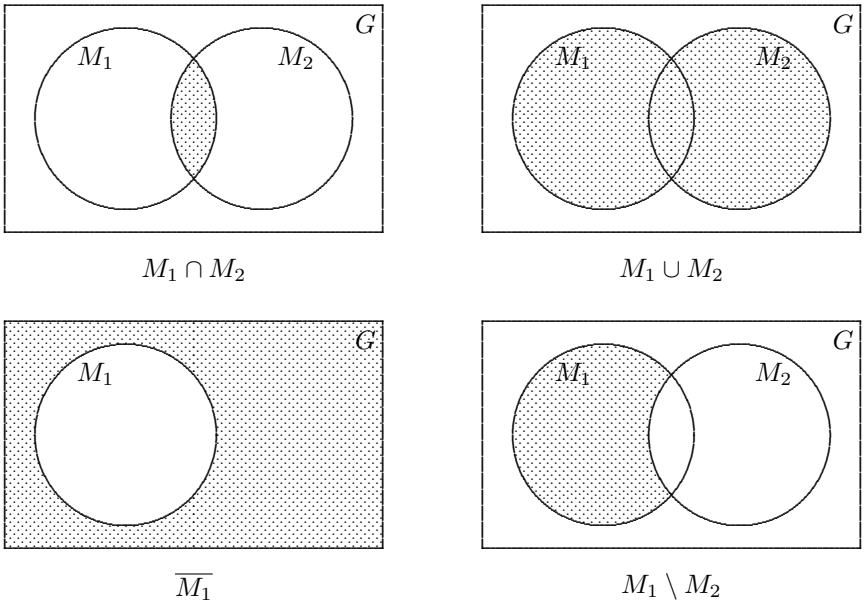

Abbildung 1.1: VENN-Diagramme zur graphischen Darstellung von Operationen auf Mengen

Satz 1.27 *Seien A, B und C Mengen in einem Grundbereich G, dann gelten folgende Aussagen.*

$$(A = B) \Leftrightarrow (A \subseteq B \wedge B \subseteq A), \tag{1.27}$$
$$\overline{\overline{A}} = A, \tag{1.28}$$
$$A \cup B = B \cup A \quad \textit{(Kommutativität bezüglich } \cup\textit{)}, \tag{1.29}$$
$$(A \cup B) \cup C = A \cup (B \cup C) \quad \textit{(Assoziativität bezüglich } \cup\textit{)}, \tag{1.30}$$
$$\emptyset \cup A = A, \tag{1.31}$$
$$A \cup A = A, \tag{1.32}$$
$$(A \subseteq B) \Longrightarrow (A \cup B = B), \tag{1.33}$$
$$A \cap B = B \cap A \quad \textit{(Kommutativität bezüglich } \cap\textit{)}, \tag{1.34}$$
$$(A \cap B) \cap C = A \cap (B \cap C) \quad \textit{(Assoziativität bezüglich } \cap\textit{)}, \tag{1.35}$$
$$\emptyset \cap A = \emptyset, \tag{1.36}$$
$$A \cap A = A, \tag{1.37}$$
$$(A \subseteq B) \Longrightarrow (A \cap B = A), \tag{1.38}$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \textit{(Distributivität)}, \tag{1.39}$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \textit{(Distributivität)}, \tag{1.40}$$
$$\overline{A \cup B} = \overline{A} \cap \overline{B} \quad \textit{(De Morgansche Regel)}, \tag{1.41}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad \textit{(De Morgansche Regel)}, \tag{1.42}$$
$$(A \cap B = \emptyset) \Leftrightarrow (A \subseteq \overline{B}), \tag{1.43}$$
$$(A \cup B = G) \Leftrightarrow (\overline{A} \subseteq B), \tag{1.44}$$
$$A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C) \quad \textit{(Distributivität)}, \tag{1.45}$$
$$(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C) \quad \textit{(Distributivität)}, \tag{1.46}$$
$$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C) \quad \textit{(Distributivität)}, \tag{1.47}$$
$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \quad \textit{(Distributivität)}, \tag{1.48}$$
$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C) \quad \textit{(Distributivität)}. \tag{1.49}$$

Bemerkung: $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$ gilt **nicht** allgemein.

Die Sachverhalte in obigem Satz kann man sich an so genannten *Venn-Diagrammen* verdeutlichen, zum Beweis sind sie allerdings nicht geeignet. Die Beweise aller Aussagen aus obigem Satz werden geführt, indem auf die entsprechenden Gesetzmäßigkeiten der Aussagenlogik zurückgegriffen wird.

Wir wollen hier den Beweis der Aussage 1.49 aus obigem Satz angeben. Zu zeigen ist $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$. Aufgrund der Definition der Gleichheit haben wir also folgende äquivalente Aussage für alle $x \in G$ zu beweisen:

$$x \in (A \setminus (B \cap C)) \Leftrightarrow x \in ((A \setminus B) \cup (A \setminus C)).$$

Das machen wir folgendermaßen:

$$\begin{aligned} x \in (A \setminus (B \cap C)) &\Leftrightarrow x \in A \wedge x \notin (B \cap C) \\ &\Leftrightarrow x \in A \wedge \neg(x \in (B \cap C)) \\ &\Leftrightarrow x \in A \wedge \neg(x \in B \wedge x \in C) \\ &\Leftrightarrow x \in A \wedge (\neg(x \in B) \vee \neg(x \in C)) \\ &\Leftrightarrow (x \in A \wedge \neg(x \in B)) \vee (x \in A \wedge \neg(x \in C)) \\ &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \\ &\Leftrightarrow x \in (A \setminus B) \vee x \in (A \setminus C) \\ &\Leftrightarrow x \in ((A \setminus B) \cup (A \setminus C)) \end{aligned}$$

und schließlich folgt die Aussage für alle $x \in G$ aus der Transitivität der aussagenlogischen Äquivalenz („$\Leftrightarrow$“).

Eine besondere Verknüpfung bei Mengen ist das so genannte *Kreuzprodukt* von Mengen oder auch *Kartesisches Produkt* oder einfach *Produkt* von Mengen. Dazu benötigen wir aber noch den Begriff des n-Tupels:

Ein Element $(x_1, x_2, \ldots, x_n)$ heißt *n-Tupel*. Für $n = 2$ heißt es auch (*geordnetes*) *Paar*, für $n = 3$ *Tripel*, für $n = 4$ *Quadrupel*, für $n = 5$ *Quintupel* u. s. w.

Definition 1.28 *Sind M_1 und M_2 zwei Mengen, so ist ihr Kreuzprodukt $M_1 \times M_2$ definiert durch*

$$M_1 \times M_2 := \{(x, y) \mid (x \in M_1) \wedge (y \in M_2)\},$$

das heißt $M_1 \times M_2$ ist eine Menge geordneter Paare.

Das Ganze kann man auf n Mengen verallgemeinern:

Definition 1.29 *Sei $n > 0$ eine natürliche Zahl, $M_1, M_2, \ldots, M_n$ Mengen, so ist ihr Kreuzprodukt $M_1 \times M_2 \times \cdots \times M_n$ definiert durch*

$$M_1 \times M_2 \times \cdots \times M_n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in M_i \text{ für } 1 \leq i \leq n\}.$$

Definition 1.30 *Gilt $M_1 = M_2 = \cdots = M_n = M$, so schreiben wir $M_1 \times M_2 \times \cdots \times M_n = M^n$.*

Ist $n = 0$, so ist $M^n = M^0 = \{\emptyset\}$.

Satz 1.31 *Seien A, B und C Mengen in einem Grundbereich G, dann gelten folgende Aussagen.*

$$A \times (B \times C) = (A \times B) \times C \quad \textit{(Assoziativität)}, \tag{1.50}$$

$$A \times (B \cup C) = (A \times B) \cup (A \times C) \quad \textit{(Distributivität)}, \tag{1.51}$$

$$A \times (B \cap C) = (A \times B) \cap (A \times C) \quad \textit{(Distributivität)}, \tag{1.52}$$

$$A \times \emptyset = \emptyset \times A = \emptyset. \tag{1.53}$$

Beachte, dass im Allgemeinen $M_1 \times M_2 \neq M_2 \times M_1$ gilt.

1.3 Relationen und Funktionen

Definition 1.32 *Eine Teilmenge $R \subseteq M_1 \times M_2 \times \cdots \times M_n$ nennt man eine n-stellige Relation zwischen den Mengen $M_1 \times M_2 \times \cdots \times M_n$.*

Gilt speziell $M_1 = M_2 = \cdots = M_n = M$, so nennt man $R \subseteq M^n$ eine n-stellige Relation in M.

Beispiel 1.33 Wir betrachten folgende Beispiele von Relationen. Dabei gilt $x \mid y$ genau dann, wenn es ein $k \in \mathbb{Z}$ mit $y = k \cdot x$ gibt.

$$
\begin{array}{ll}
R_0 \subseteq M_1 \times M_2 \times \cdots \times M_n, & R_0 = \emptyset, \\
R_1 \subseteq M_1 \times M_2 \times \cdots \times M_n, & R_1 = M_1 \times M_2 \times \cdots \times M_n, \\
R_2 \subseteq M^2, & R_2 = \{(x,y) \in M^2 \mid x = y\}, \\
R_3 \subseteq \{a,b,c\}^2, & R_3 = \{(a,a),(b,c),(c,c)\}, \\
R_4 \subseteq \{a,b,c\}^2, & R_4 = \{(a,a),(a,b),(b,a),(b,b),(b,c)\}, \\
R_5 \subseteq \mathbb{Z}^2, & R_5 = \{(x,y) \in \mathbb{Z}^2 \mid x \mid y\}, \\
R_6 \subseteq \mathbb{N}^2, & R_6 = \{(x,y) \in \mathbb{N}^2 \mid x \mid y\}, \\
R_7^{(m)} \subseteq \mathbb{Z}^2,\ m \in \mathbb{N},\ m > 0, & R_7^{(m)} = \{(x,y) \in \mathbb{Z}^2 \mid m \mid (x-y)\}.
\end{array}
$$

Die Relationen R_0 und R_1 im obigen Beispiel nennen wir *Nullrelation* bzw. *Allrelation*. Die Relation R_2 heißt *Diagonale* oder auch *Identität* in M und wird oft mit Δ_M oder auch id_M bezeichnet.

Definition 1.34 *Eine Relation R heißt binär oder zweistellig, wenn $R \subseteq M_1 \times M_2$ gilt. Für die Elemente der Relation $(x,y) \in R$ schreiben wir dann auch xRy (gelesen: „x steht in Relation R zu y“).*

In den obigen Beispielen handelt es sich außer bei den Relationen R_0 und R_1 um binäre Relationen. Das deutet schon darauf hin, dass wir es oft mit binären Relationen zu tun haben. Es gibt natürlich auch wichtige Relationen, die mehr als zweistellig sind. Ein Beispiel ist die so genannte *Zwischenrelation*.

Endliche binäre Relationen kann man günstig graphisch veranschaulichen, indem man zwei Elemente, die zueinander in Relation stehen, durch einen Pfeil verbindet. In der Abbildung 1.2 ist die Relation R_4 aus Beispiel 1.33 dargestellt.

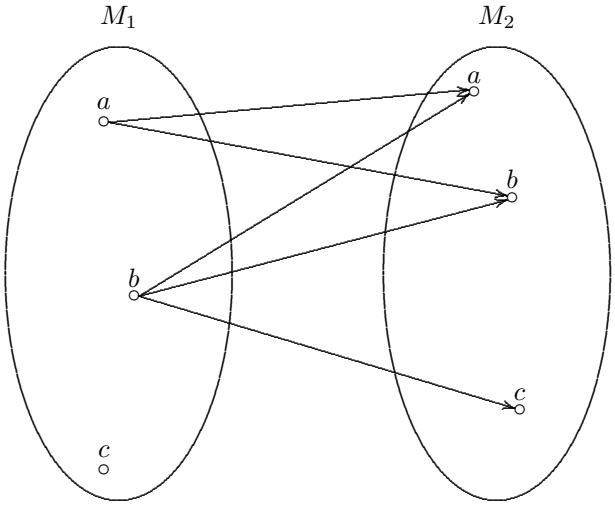

Abbildung 1.2: Graphische Darstellung einer Relation

Definition 1.35 *Sei $R \in M_1 \times M_2$ eine binäre Relationen, dann definieren wir:*

$$D(R) = \{x \in M_1 \mid \exists y \in M_2 \text{ mit } xRy\},$$
$$W(R) = \{y \in M_2 \mid \exists x \in M_1 \text{ mit } xRy\}.$$

Wir bezeichnen $D(R)$ als Definitionsbereich der Relation R und $W(R)$ als Wertebereich der Relation R.

Wir definieren im Folgenden einige Eigenschaften von Relationen, die für uns von Interesse sind, die aber auch in der Mathematik von herausragender Bedeutung sind. Es gibt außer den hier angeführten Eigenschaften natürlich auch noch weitere.

Definition 1.36 *Eine binäre Relation $R \in M_1 \times M_2$ heißt*

eindeutig genau dann, wenn $\forall x \in M_1,\ \forall y_1, y_2 \in M_2\ ((xRy_1 \wedge xRy_2) \Rightarrow (y_1 = y_2))$.

Eine binäre Relation $R \in M^2$ heißt

reflexiv	*genau dann, wenn* $\forall x \in M$	(xRx),
irreflexiv	*genau dann, wenn* $\forall x \in M$	$(\neg(xRx))$,
symmetrisch	*genau dann, wenn* $\forall x, y \in M$	$(xRy \Rightarrow yRx)$,
antisymmetrisch	*genau dann, wenn* $\forall x, y \in M$	$((xRy \wedge yRx) \Rightarrow (x = y))$,
transitiv	*genau dann, wenn* $\forall x, y, z \in M$	$((xRy \wedge yRz) \Rightarrow xRz)$.

Wir weisen noch mal ausdrücklich darauf hin, dass außer der Eigenschaft Eindeutigkeit alle anderen Eigenschaften nur für binäre Relationen **in** einer Menge definiert sind. Betrachten wir die binären Relationen aus Beispiel 1.33, so besitzen diese Relationen folgende Eigenschaften.

Eindeutigkeit:	R_2, R_3
Reflexivität:	R_2, R_5
Irreflexivität:	$--$
Symmetrie:	$R_2, R_5, R_6, R_7^{(m)}$
Antisymmetrie:	R_2, R_3, R_6
Transitivität:	$R_2, R_3, R_4, R_5, R_6, R_7^{(m)}$

Definition 1.37 *Eine Relation $R \in M^2$ heißt*

(i) *reflexive Halbordnung, falls sie reflexiv, antisymmetrisch und transitiv ist.*

(ii) *irreflexive Halbordnung, falls sie irreflexiv und transitiv ist.*

(iii) *Äquivalenzrelation, falls sie reflexiv, symmetrisch und transitiv ist.*

Definition 1.38 *Sei $R \in M^2$ eine Äquivalenzrelation, dann definieren wir*

$$[x]_R = \{y \in M \mid xRy\}$$

und bezeichnen $[x]_R$ als Äquivalenzklasse modulo R mit dem Repräsentanten x.

Die Menge aller Äquivalenzklassen von $R \in M^2$ heißt Faktormenge M/R und ist also definiert durch

$$M/R = \{[x]_R \mid x \in M\}$$

In einer Äquivalenzklasse einer Relation $R \in M^2$ befinden sich also alle Elemente der Menge M, die zueinander in Relation stehen. Wir können folgende Eigenschaften feststellen.

Satz 1.39 *Sei $R \in M^2$ eine Äquivalenzrelation, dann gilt*

(i) $\forall x \in M\ ([x]_R \neq \emptyset)$,

(ii) $\forall x, y \in M\ (([x]_R \neq [y]_R) \Rightarrow ([x]_R \cap [y]_R = \emptyset))$,

(iii) $\bigcup_{x \in M} [x]_R = M$.

Da Relationen Mengen sind, können wir natürlich die mengentheoretischen Operationen (Durchschnitt, Vereinigung, Differenz) auch auf Relationen anwenden. Wir führen jetzt zwei weitere Operationen in der Menge der binären Relationen ein.

Definition 1.40 *Sei $R \subseteq M_1 \times M_2$, dann ist die zu R inverse Relation R^{-1} definiert durch*

$$R^{-1} = \{(x, y) \in M_2 \times M_1 \mid yRx\}.$$

Die Invertierung bedeutet also im Prinzip eine „Umkehrung“. Es gilt also:

$$xRy \Leftrightarrow yR^{-1}x.$$

Daraus ergibt sich sofort:

Folgerung 1.41 *Sei $R \in M_1 \times M_2$ eine binäre Relation. Dann gilt*

$$D(R^{-1}) = W(R) \quad \textit{und} \quad W(R^{-1}) = D(R).$$

Beispiel 1.42 Die inversen Relationen zu den Relationen R_4 und R_6 aus Beispiel 1.33 sind folgende:

$$R_4^{-1} = \{(a, a), (a, b), (b, a), (b, b), (c, b)\},$$
$$R_6^{-1} = \{(x, y) \in \mathbb{N}^2 \mid y \,/\, x\}.$$

Die zweite Operation in der Menge der Relationen ist die so genannte *Verkettung* oder *Verknüpfung* oder auch ganz einfach das *Produkt* zweier Relationen.

Definition 1.43 *Seien $R \subseteq M_1 \times M_2$ und $S \subseteq M_2 \times M_3$ zwei binäre Relationen, so ist ihre Verkettung $R \circ S$ definiert durch*

$$R \circ S = \{(x, z) \in M_1 \times M_3 \mid \exists y \in M_2 \textit{ mit } (x, y) \in R \wedge (y, z) \in S\}.$$

Beispiel 1.44 Gegeben sind $R \subseteq \{1, 2, 3, 4\} \times \{a, b, c, d\}$ sowie $S \subseteq \{a, b, c, d\} \times \{\alpha, \beta, \gamma, \delta\}$ durch $R = \{(1, a), (2, b), (2, d), (4, d), (4, e)\}$ und $S = \{(a, \alpha), (a, \beta), (c, \gamma), (d, \delta), (e, \delta)\}$. Dann ist $R \circ S = \{(1, \alpha), (1, \beta), (2, \delta), (4, \delta)\}$. Die graphischen Veranschaulichung ist in der Abbildung 1.3 dargestellt (R – gepunktete Pfeile, S – gestrichelte Pfeile, $R \circ S$ – durchgezogene Pfeile).

Wir kommen jetzt zu einem der wichtigsten Begriffe dieser Vorlesung, nämlich dem Begriff der *Funktion* oder *Abbildung*.

Definition 1.45 *Eine eindeutige Relation $R \subseteq M_1 \times M_2$ heißt Funktion oder auch Abbildung aus M_1 in M_2. Schreibweise: $R\colon M_1 \to M_2$.*

Für Funktionen benutzen wir in der Regel in Zukunft kleine lateinische Buchstaben. Falls $f\colon M_1 \to M_2$, so sagen wir, f ist eine Funktion „aus M_1 in M_2“.

Da bei einer Funktion $f : M_1 \to M_2$ jedem $x \in M_1$ höchstens ein $y \in M_2$ zugeordnet wird, schreiben wir

$$y = f(x) \ \text{ statt } \ \{y\} = f(x), \ \text{ falls } \ (x, y) \in f.$$

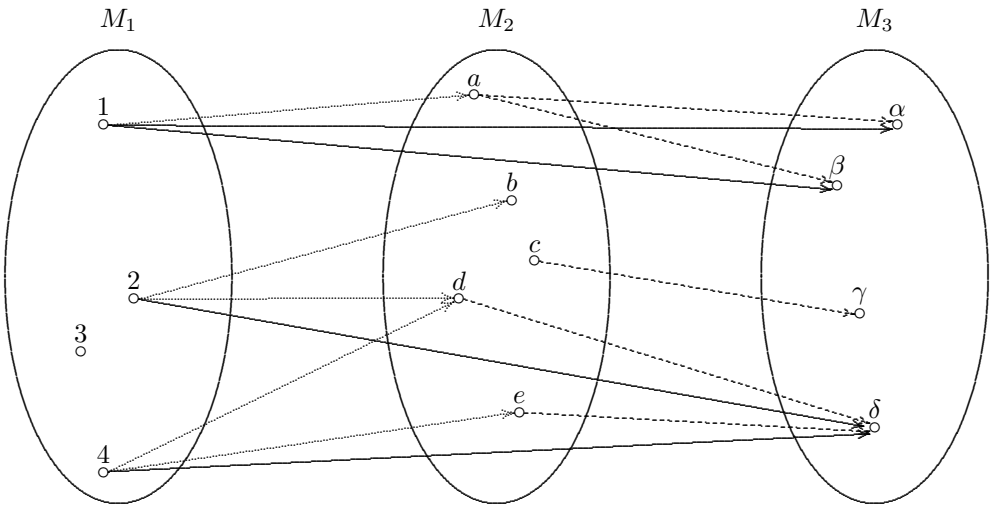

Abbildung 1.3: Graphische Darstellung einer Verknüpfung von Relationen

Definition 1.46 *Sei $f\colon M_1 \to M_2$ eine Funktion. Dann heißt f*

(i) *partiell, falls $D(f) \subseteq M_1$ ist,*

(ii) *total, falls $D(f) = M_1$ ist,*

(iii) *surjektiv, falls $W(f) = M_2$ ist,*

(iv) *injektiv oder umkehrbar eindeutig, falls für alle $x_1, x_2 \in M_1$ gilt*

$$(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2),$$

(v) *bijektiv, falls f injektiv und surjektiv ist.*

Wir führen folgende Sprechweisen ein. $f\colon M_1 \to M_2$ ist eine Funktion

aus M_1 in M_2,	falls f partiell,
von M_1 in M_2,	falls f total,
aus M_1 auf M_2,	falls f partiell und surjektiv,
von M_1 auf M_2,	falls f total und surjektiv.

Ich möchte bemerken, dass man beim Begriff der Funktion in der Literatur oft schon die totale Funktion meint, insbesondere in der Analysis. Für uns ist allerdings die partielle Funktion von besonderem Interesse, so dass wir mit Funktion immer die partielle Funktion meinen.

Jede Funktion ist ja eine Relation, deshalb gelten unsere für Relationen gemachten Definitionen natürlich genauso für Funktionen, insbesondere können wir also Funktionen verknüpfen und ihre inverse Relation bilden. Die Verknüpfung von Funktionen und die Invertierung von Funktionen liefern natürlich wieder Relationen. Es ergibt sich die Frage, ob es jedoch notwendig wieder Funktionen sind. Man erkennt relativ schnell folgende Sachverhalte:

Satz 1.47 *Seien $f\colon M_1 \to M_2$ und $g\colon M_2 \to M_3$ Funktionen. Dann ist ihre Verknüpfung $f \circ g\colon M_1 \to M_3$ eindeutig, also wieder eine Funktion.*

Satz 1.48 *Sei $f\colon M_1 \to M_2$ eine Funktion. Dann gilt: f^{-1} ist eine Funktion genau dann, wenn f injektiv ist.*

Im Allgemeinen ist also die Inverse einer Funktion nicht wieder eine Funktion. In der Literatur taucht oft der Begriff der „inversen Funktion“ oder „Umkehrfunktion“ auf, damit bezeichnet man

die Inverse, die wieder eine Funktion ist. Wir müssen also zwischen „Inversen einer Funktion“, die immer existiert, und „inverser Funktion“ (existiert nicht immer) wohl unterscheiden.

Ich möchte darauf hinweisen, dass die Verkettung von Funktionen nichts anderes ist als das bekannte *Einsetzen*.

Beispiel 1.49 Gegeben sind die Funktionen $f : \mathbb{R} \to \mathbb{R}$ vermöge $x \mapsto y = f(x) = \sqrt{x}$ und $g\colon \mathbb{R} \to \mathbb{R}$ vermöge $y \mapsto z = g(y) = \sin y$. Dann ist $f \circ g\colon \mathbb{R} \to \mathbb{R}$ vermöge $x \mapsto z = (f \circ g)(x) = g(f(x)) = \sin(\sqrt{x})$.

Es folgt noch eine Charakterisierung von Funktionen, die wir öfter in der Vorlesung benutzen werden.

Definition 1.50 *Sei $n \in \mathbb{N}$, dann heißt die Funktion $f\colon \mathbb{N}^n \to \mathbb{N}$ vermöge $(x_1, x_2, \ldots, x_n) \mapsto y = f(x_1, x_2, \ldots, x_n)$ n-stellige Funktion aus $\mathbb{N}^n$ in $\mathbb{N}$.*

Für $n = 0$ ist ja $\mathbb{N}^n = \mathbb{N}^0 = \{\emptyset\}$, so dass wir nur einen Funktionswert $f(\emptyset)$ haben. Durch solch eine 0-stellige Funktion wird also ein Wert $f(\emptyset)$ in $\mathbb{N}$ ausgezeichnet, also wird nichts anderes durch die Funktion realisiert, als eine Konstante zu vereinbaren.

1.4 Über die Mächtigkeit von Mengen

Im Unterkapitel 1.2 haben wir die Kardinalzahl $|M|$ einer Menge eingeführt und für endliche Mengen als die Anzahl der Elemente der Menge M vereinbart. Wir möchten in diesem Kapitel den Begriff der Kardinalzahl sauber definieren, so dass er auch für unendliche Mengen anwendbar ist.

Dazu benötigen wir zuerst den Begriff der Gleichmächtigkeit zweier Mengen.

Definition 1.51 *Zwei Mengen M_1 und M_2 heißen gleichmächtig, wenn es eine totale bijektive Funktion von M_1 auf M_2 gibt. Schreibweise: $M_1 \overset{\sim}{\longleftrightarrow} M_2$.*

Beispiel 1.52 Die endlichen Mengen $\{1, 2, 3, 4\}$ und $\{6, 7, 8, 9\}$ sind gleichmächtig, in Zeichen $\{1, 2, 3, 4\} \overset{\sim}{\longleftrightarrow} \{6, 7, 8, 9\}$, da die totale bijektive Funktion

$$f\colon \{1, 2, 3, 4\} \to \{6, 7, 8, 9\} \quad \text{mit} \quad f = \{(1, 6), (2, 7), (3, 8), (4, 9)\}$$

existiert. Die unendlichen Mengen $\mathbb{N}$ und $\{n \in \mathbb{N} \mid \exists k \in \mathbb{N} \text{ mit } n = 2k\}$ sind gleichmächtig, d. h. $\mathbb{N} \overset{\sim}{\longleftrightarrow} \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} \text{ mit } n = 2k\}$, da die totale bijektive Funktion

$$g\colon \mathbb{N} \to \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} \text{ mit } n = 2k\} \quad \text{vermöge} \quad x \mapsto g(x) = 2 \cdot x$$

existiert. Man beachte, dass zwei unendliche Mengen, von denen die eine Menge eine echte Teilmenge der anderen Menge ist, gleichmächtig sein können. Für endliche Mengen trifft das natürlich nicht zu.

Wie man sich leicht überlegen kann, gilt:

Folgerung 1.53 *Die Relation „$\overset{\sim}{\longleftrightarrow}$“ in der Menge aller Mengen ist eine Äquivalenzrelation.*

Folglich können wir die Äquivalenzklassen für diese Relation bilden. Diese Äquivalenzklassen $[M]_{\overset{\sim}{\longleftrightarrow}}$ sind genau die schon intuitiv eingeführten Kardinalzahlen von Mengen. Wir setzen also

$$|M| := [M]_{\overset{\sim}{\longleftrightarrow}}.$$

Man erkennt, dass für endliche Mengen der Kardinalzahlbegriff mit dem Anzahlbegriff übereinstimmt, dass es aber auch mindestens eine Kardinalzahl „Unendlich“ gibt. Das wollen wir näher spezifizieren.

Definition 1.54 *Eine Menge M heißt abzählbar unendlich, falls sie zur Menge der natürlichen Zahlen $\mathbb{N}$ gleichmächtig ist.*

Definition 1.55 *Eine Menge M heißt abzählbar, falls sie abzählbar unendlich oder endlich ist.*

Die in Beispiel 1.52 betrachteten Mengen sind somit abzählbar, insbesondere ist $\{n \in \mathbb{N} \mid \exists k \in \mathbb{N} \text{ mit } n = 2k\}$, die Menge der natürlichen geraden Zahlen, abzählbar unendlich. Weitere abzählbar unendliche Mengen sind zum Beispiel $\mathbb{Z}$, $\mathbb{Q}$, die Menge der gebrochenen Zahlen, die Menge der Primzahlen und viele andere. Die Beweise überlassen wir dem Leser.

Es gibt allerdings auch unendliche Mengen, die nicht abzählbar unendlich sind. Wir nennen sie *überabzählbar unendlich*. Dazu gehören zum Beispiel $\mathbb{R}$ sowie auch schon $\{x \in \mathbb{R} \mid 0 < x < 1\}$. Beweise dafür findet man in der mathematischen Literatur. Wir wollen hier von einer Menge zeigen, dass sie überabzählbar unendlich ist, die für uns später noch von Interesse sein wird.

Lemma 1.56 *Die Menge $F_{\mathbb{N}}$ aller einstelligen totalen Funktionen von $\mathbb{N}$ in $\mathbb{N}$ ist überabzählbar unendlich.*

Beweis. Wir führen den Beweis indirekt, d. h. wir machen die Annahme, die Menge aller einstelligen totalen Funktionen von $\mathbb{N}$ in $\mathbb{N}$ ist abzählbar unendlich. Nach Definition gibt es also eine totale bijektive Funktion g von der Menge $\mathbb{N}$ in die Menge $\{f : \mathbb{N} \to \mathbb{N} \mid D(f) = \mathbb{N}\}$. Für $n \in \mathbb{N}$ sei $g(n) = f_n$.

Wir konstruieren eine totale Funktion $f : \mathbb{N} \to \mathbb{N}$ durch $f(n) = f_n(n) + 1$. Da f total ist und eine Funktion von $\mathbb{N}$ in $\mathbb{N}$ ist, ist sie ein Element der Menge $F_{\mathbb{N}}$. Andererseits gilt für jedes $n \in \mathbb{N}$ $f \neq f_n$, da $f(n) = f_n(n) + 1 \neq f_n(n)$. Folglich haben wir einen Widerspruch konstruiert, somit ist unsere Annahme falsch und das Lemma bewiesen. □

Folgerung 1.57 *Die Menge aller Funktionen von $\mathbb{N}^n$ in $\mathbb{N}$, $n \in \mathbb{N}$, ist überabzählbar unendlich.*

Ich möchte an dieser Stelle bemerken, dass es in der Informatik den Begriff der *rekursiv aufzählbaren Menge* oder oft auch kurz den Begriff der *aufzählbaren Menge* gibt. Dieser ist mit dem Begriff der *Abzählbarkeit* nicht identisch. Allerdings gibt es Beziehungen. Wir werden später darauf zurückkommen.

1.5 Algebraische Strukturen

In diesem Kapitel wollen wir sehr kurz ganz wenige Begriffe aus der Algebra zur Verfügung stellen.

Zunächst wollen wir den Begriff der *Operation* einführen.

Definition 1.58 *Eine zweistellige totale Funktion $\circ : M^2 \to N$ heißt (binäre) Operation oder Verknüpfung.*

Gilt $N = M$, so nennen wir $\circ$ vollständig oder abgeschlossen und sprechen von einer Operation in M.

Für $\circ(x, y)$ schreibt man auch $x \circ y$ oder kurz xy, falls $\circ$ aus dem Kontext eindeutig hervorgeht.

Folgende Eigenschaften von Operationen sind oft von Interesse.

Definition 1.59 *Sei $\circ : M^2 \to M$ eine Operation.*

(i) *$\circ$ heißt assoziativ, wenn $(x \circ y) \circ z = x \circ (y \circ z)$ für alle $x, y, z \in M$ gilt.*

(ii) *$\circ$ heißt kommutativ, wenn $x \circ y = y \circ x$ für alle $x, y \in M$ gilt.*

Definition 1.60 *Sei M eine nichtleere Menge und $\circ : M^2 \to M$ eine Operation in M, so heißt $(M, \circ)$ (algebraische) Struktur mit der Trägermenge M.*

Algebraische Strukturen kommen in vielen Wissenschaftsdisziplinen vor und sind ein ausgezeichnetes Mittel der Abstraktion, das eine gemeine Sicht von Sachverhalten zulässt, die ursprünglich nichts miteinander zu tun haben.

Wir betrachten hier nur einen sehr, sehr kleinen Ausschnitt der algebraischen Strukturen. Folgende Strukturen sind insbesondere für uns von Interesse.

Definition 1.61 *Sei $(M, \circ)$ eine algebraische Struktur.*

(i) *$(M, \circ)$ heißt Halbgruppe, falls $\circ$ assoziativ ist.*

(ii) *$(M, \circ)$ heißt abelsch oder kommutativ, falls $\circ$ kommutativ ist.*

(iii) *Ist $(M, \circ)$ eine Halbgruppe, so heißt sie Monoid, falls*

$$\exists e \in M \ \forall x \in M \ (x \circ e = e \circ x = x).$$

e heißt neutrales Element der Struktur.

(iv) *Ist $(M, \circ)$ ein Monoid, so heißt es Gruppe, falls*

$$\forall x \in M \ \exists x^{-1} \in M \ (x \circ x^{-1} = x^{-1} \circ x = e)$$

gilt, wobei e das neutrale Element des Monoids ist.

Folgende Strukturen werden durch Zahlbereiche gebildet, wie man sich leicht überlegen kann.

Beispiel 1.62 (i) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$ sowie $(\{x \in \mathbb{Q} \mid x \geq 0\}, +)$ sind abelsche Monoide, aber keine Gruppen.

(ii) $(\mathbb{Z}, +)$ und $(\{x \in \mathbb{Q} \mid x \geq 0\}, +)$ sind abelsche Gruppen.

(iii) Die Mengen $\mathbb{Q}$ sowie $\mathbb{R}$ bilden sowohl mit der Addition als auch der Multiplikation abelsche Gruppen.

1.6 Alphabete, Wörter, Sprachen

Wir wollen hier einige Grundbegriffe für das folgende Kapitel geben.

Unter einem *Alphabet* verstehen wir eine *endliche nichtleere Menge*. Zum Beispiel ist $\Sigma = \{a, b, c\}$ ein Alphabet. Die Elemente eines Alphabets heißen Buchstaben, Zeichen oder Symbole. Endliche Folgen von Buchstaben des Alphabets nennen wir Wörter über dem Alphabet; sie werden durch einfaches Hintereinanderschreiben der Buchstaben angegeben. Zum Beispiel sind *aba*, *abba* und *aaaa* Wörter über dem Alphabet Σ. ε bezeichnet das Leerwort oder leere Wort, das der leeren Folge entspricht, also aus keinem Buchstaben besteht. Die Menge aller Wörter über einem Alphabet Σ (einschließlich ε) bezeichnen wir mit Σ^*. Wir setzen $\Sigma^+ = \Sigma^* \setminus \{\varepsilon\}$.

Folgerung 1.63 *Es sei Σ ein Alphabet. Dann enthält Σ^* abzählbar unendlich viele Elemente.*

Wir sind jetzt in der Lage, einen der beiden Begriffe aus dem Titel dieser Vorlesung zu definieren.

Definition 1.64 *Sei Σ ein Alphabet. Eine Teilmenge $L \subseteq \Sigma^*$ heißt formale Sprache über Σ.*

In Σ^* definieren wir das *Produkt* oder die *Konkatenation* $w_1 \cdot w_2$ (oder kurz $w_1 w_2$) der Wörter w_1 und w_1 durch einfaches Hintereinanderschreiben. Für $w_1 = abba$ und $w_2 = ba$ erhalten wir beispielsweise $w_1 \cdot w_2 = abbaba$.

Man sieht leicht folgenden Satz.

Satz 1.65 *Es sei Σ ein Alphabet. Für alle Wörter $w, w_1, w_2, w_3 \in \Sigma^*$ gelten dann folgende Beziehungen:*

$$w_1 \cdot (w_2 \cdot w_3) = (w_1 \cdot w_2) \cdot w_3 \quad (\textit{Assoziativgesetz}),$$
$$w\varepsilon = \varepsilon w = w \quad (\varepsilon \textit{ neutrales Element}).$$

Wie man sich aber leicht überzeugen kann, ist die Konkatenation nicht kommutativ. Für $w_1 = abba$ und $w_2 = ba$ gilt zum Beispiel $w_1 \cdot w_2 = abbaba$ und $w_2 \cdot w_1 = baabba$.

Die Konkatenation ist aber eine abgeschlossene Operation in Σ^*. Somit bildet $(\Sigma^*, \cdot)$ eine algebraische Struktur. Und wegen Satz 1.65 ist $(\Sigma^*, \cdot)$ sogar ein *Monoid*.

Wegen der Assoziativität der Konkatenation können wir folgende abkürzende Schreibweise einführen.

$$\underbrace{w \cdot w \cdot \cdots \cdot w}_{n\text{-mal}} = w^n$$

Es gilt $w^0 = \varepsilon$.

Wir erweitern die Konkatenation auf formale Sprachen.

Definition 1.66 *Sei Σ ein Alphabet, $L_1, L_2 \subseteq \Sigma^*$ Sprachen über Σ. Die Konkatenation $L_1 \cdot L_2$ ist definiert durch:*

$$L_1 \cdot L_2 = \{w_1 \cdot w_2 \mid w_1 \in L_1,\ w_2 \in L_2\}.$$

Unter der *Länge* $|w|$ eines Wortes w verstehen wir die Anzahl der in w vorkommenden Buchstaben, wobei jeder Buchstabe sooft gezählt wird wie er in w vorkommt. Es gilt zum Beispiel $|aba| = 3$, $|abba| = 4$, $|aaaa| = 4$ und $|\varepsilon| = 0$.

Aus der Definition der Länge ergibt sich sofort:

Folgerung 1.67 *Es sei Σ ein Alphabet. Für alle Wörter $w_1, w_2 \in \Sigma^*$ gilt dann*

$$|w_1 \cdot w_2| = |w_1| + |w_2|.$$

Zum Abschluss noch eine nützliche Definition.

Definition 1.68 *Sei $w \in \Sigma^*$ ein Wort mit $w = x \cdot y \cdot z$.*

(i) *y heißt Teilwort von w.*

(ii) *Falls $y \neq \varepsilon$ und $y \neq w$, heißt y echtes Teilwort von w.*

(iii) *y heißt Präfix von w, falls $x = \varepsilon$.*

(iv) *y heißt Suffix von w, falls $z = \varepsilon$.*