1 Grundstrukturen der Mathematik

1.1 Mathematische Logik Eine Formel oder ein Satz der Alltagssprache heißt *Aussage*, wenn sie wahr oder falsch sein kann. Einige Beispiele:

$$2 < 5, \quad 3 = 5, \quad \text{Sokrates hatte eine Glatze.}$$

Einer Aussage kann man daher prinzipiell einen *Wahrheitswert* „wahr“ oder „falsch“ zuordnen, wobei es im Beispiel rechts vermutlich nie mehr möglich sein wird, über den Wahrheitswert dieser Aussage zu entscheiden. Denn Platon hat viele Gespräche und Reden des Sokrates aufgezeichnet, aber niemals kam es zu einem Satz wie „Sokrates fasste sich an die Glatze“.

Logische Konjunktionen verbinden Aussagen, die einfachsten sind

$$\begin{aligned} (A \textit{ oder } B) \text{ wahr} &\quad\Leftrightarrow\quad A \text{ wahr oder } B \text{ wahr oder beide wahr,} \\ (A \textit{ und } B) \text{ wahr} &\quad\Leftrightarrow\quad A \text{ wahr und } B \text{ wahr.} \end{aligned}$$

Für *oder* und *und* sowie für die Verneinung schreiben wir

$\vee$	oder (nicht ausschließend) (von lat. vel)
$\wedge$	und
$\neg$	Verneinungszeichen

In Tafelform können wir die obigen Regeln so schreiben:

A∨B	w	f
w	w	w
f	w	f

A∧B	w	f
w	w	f
f	f	f

.

Bei der Verneinung kehrt sich der Wahrheitswert einfach um. Ferner gelten die Verneinungsregeln für Aussagen A, B

$$\begin{aligned} \neg(A \vee B) &\quad\Leftrightarrow\quad \neg A \wedge \neg B, \\ \neg(A \wedge B) &\quad\Leftrightarrow\quad \neg A \vee \neg B, \end{aligned}$$

Schwieriger ist die Implikation, weil es hier Unterschiede zwischen den natürlichen Sprachen (auch untereinander) und der Sprache der Mathematik gibt. Klar ist noch das Beispiel

„Wenn es regnet, dann ist die Straße nass.“

Ob es nun regnet oder nicht, der Satz ist immer wahr und er behauptet nichts, wenn es nicht regnet. Genau so wird die Implikation in der Mathematik verwendet: Ist die Voraussetzung (hier: Es regnet) nicht erfüllt, so ist es gleichgültig, was in der Behauptung (hier: Die Straße ist nass) steht, die Implikation selber ist in diesem Fall wahr.

Zur Kollision zwischen Mathematik und natürlichen Sprachen kommt es in Sätzen wie

„Wenn Albert Einstein den Nobelpreis nicht bekommen hätte,
dann wäre er an Hänschen Klein verliehen worden.“

Was würden Sie sagen, ist der Satz wahr oder falsch? Oder wir betrachten den Fall, dass es für einen Preis zwei heiße Kandidaten E. und K. gibt. Nach der Preisverleihung lesen wir in der Zeitung

„Wenn E den Preis nicht bekommen hätte,
dann wäre er an K verliehen worden.“

Ist der Satz wahr oder falsch? Offenbar sind die beiden letzten Sätze logisch vollkommen identisch,

sie besitzen aber einen unterschiedlichen Kontext. In der Mathematik muss der Wahrheitswert einer Konjunktion aus den Wahrheitswerten der beteiligten Aussagen bestimmbar sein, der Kontext darf keine Rolle spielen. Daher orientiert sich die Wahrheitstafel für die Implikation an der Aussage „Wenn es regnet, dann ist die Straße nass“:

A⇒B	w	f
w	w	f
f	w	w

.

Eine Implikation ist daher immer wahr, wenn die Voraussetzung falsch ist. Damit sind alle Aussagen über mögliche Preisträger wahr.

Aufgrund der Wahrheitstafeln ist

$$(A \Rightarrow B) \quad \Leftrightarrow \quad (\neg A \vee B)$$

Daraus folgt für die Verneinung der Implikation

$$\neg(A \Rightarrow B) \quad \Leftrightarrow \quad (A \wedge \neg B)$$

Zwei Aussagen A und B heißen *äquivalent*, Schreibweise $A \Leftrightarrow B$, wenn $A \Rightarrow B$ und $A \Leftarrow B$.

Ein mathematischer Beweis besteht aus einer Folge von Aussagen, die entweder von vorneherein als richtig angesehen werden oder aus der folgenden Schlussregel, dem *modus ponens*, abgeleitet werden können:

„Wenn es regnet, dann ist die Straße nass“	$A \Rightarrow B$
„Es regnet“	A
„Die Straße ist nass“	B

Wir nehmen an, es gibt nur Lügner, die immer lügen, und Wahrheitssprecher, die immer die Wahrheit sagen.

Ein Kreter sagt: „Alle Kreter lügen“.

Dies ist die *Antinomie des Epimenides*. Allgemeiner wird eine Aussage (?) Antinomie genannt, wenn die Zuweisung eines der Wahrheitswerte wahr oder falsch in jedem Fall zu einem Widerspruch führt. Die Antinomie des Epimenides stammt aus der Bibel, der Apostel Paulus behauptet in einem Brief: Die Kreter sind alle Lügner und faule Bäuche, das sagt sogar ihr eigener Prophet. Erst später erkannten die Kirchenlehrer, dass es sich hier um eine problematische logische Konstruktion handelt und sie versuchten, diesen kretischen Propheten zu ermitteln. Anscheinend existieren nur wenige bekannte Kreter. Sie mussten etwa 500 Jahre v.Ch. zurückgehen, um auf Epimenides zu treffen, über den fast nichts bekannt ist.

Warum handelt es sich hier un eine Antinomie? Ist die Aussage „Alle Kreter lügen“ wahr, so behauptet der Kreter, dass er ein Lügner ist. Ist die Aussage falsch, so ist er demnach gar kein Lügner. Was ist an dieser Argumentation falsch?

Die Antinomie beruht darauf, dass in der Alltagslogik der Satz

„Alle Kreter lügen“.

verneint wir durch

„Alle Kreter lügen nicht“.

Die Alltagslogik ist daher *Aussagenlogik*. Wir stellen uns zu einer Aussage den Kosmos der Möglichkeiten vor, in diesem Fall 3000 Kreter, von denen ein jeder ein Wahrheitssprecher oder ein Lügner sein kann. Jede Aussage über kretische Wahrheitssprecher und Lügner greift eine Teilmenge dieses

Kosmos heraus. Die korrekte Verneinung einer solchen Aussage muss das Komplement der durch die Aussage festgelegten Teilmenge beschreiben. Die Aussage „Alle Kreter lügen“ greift eine Teilmenge heraus, die nur aus einem Element besteht, dass namlich die Kreter $1, 2, \ldots, 3000$ alle Lügner sind. Das Komplement dieser Teilmenge wird dadurch charakterisiert, dass es dort mindestens einen Wahrheitsprecher gibt. Damit liegt gar keine Antinomie vor: Es gibt sowohl Lügner als auch Wahrheitssprecher. Der Satz „Alle Kreter lügen“ ist daher falsch und der Kreter, der ihn ausspricht, ist ein Lügner.

Interessant ist natürlich, dass die Antinomie des Epimenides, die ja vom Lügen handelt, weder eine Antinomie ist, noch von Epimenides stammt.

Die Grundidee der Antinomie kann aber gerettet werden. Wenn jemand sagt „Ich lüge“ oder präziser „Der Satz, den ich gerade ausspreche, ist falsch“, so lässt sich diesen Sätzen in der Tat kein Wahrheitswert zuordnen.

Die Logik der Mathematik und Informatik ist eine *Prädikatenlogik*. Ein (einstelliges) Prädikat ist von der Form $A(x)$ mit einer Variablen x aus einem Definitionsbereich D. Wenn wir in $A(x)$ ein konkretes $x \in D$ einsetzen, so muss eine Aussage entstehen. Ein Beispiel ist

$$x \text{ ist ein Mensch}, \quad D = \text{Lebewesen}.$$

Für x können wir hier Sokrates oder den Hund Lupo einsetzen, in jedem Fall entsteht eine Aussage.

Wir verwenden

$\forall$ „für alle“
$\exists$ „es existiert“.

Ist $A(x)$ ein einstelliges Prädikat, so gelten die Verneinungsregeln

$$\neg\, \forall x\ A(x) \quad \Leftrightarrow \quad \exists x\ \neg A(x),$$

$$\neg\, \exists x\ A(x) \quad \Leftrightarrow \quad \forall x\ \neg A(x).$$

Man mache sich diese Regeln an Hand von lügenden oder wahrheitssprechenden Kretern klar.

1.2 Satz und Beweis Ein mathematischer Satz ist meist von der Form $A \Rightarrow B$ und besteht aus einer Voraussetzung A und einer Behauptung B. Der *Beweis* des Satzes besteht aus einer Folge von wahren Aussagen, deren letzte die Behauptung ist.

Beispiel 1.1 Man zeige für $a, b \geq 0$

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Das geschieht häufig so:

$$\Rightarrow \quad a + b \geq 2\sqrt{ab} \quad \Rightarrow \quad (a+b)^2 \geq 4ab$$

$$\Rightarrow \quad a^2 - 2ab + b^2 \geq 0 \quad \Rightarrow \quad (a-b)^2 \geq 0.$$

Hier hat man den Fehler gemacht, dass man von der zu beweisenden Aussage ausgeht und so lange folgert, bis eine wahre Aussage entsteht. Korrekt ist natürlich die umgekehrte Reihenfolge. □

Aus den Wahrheitstafeln folgt

$$A \Rightarrow B \quad \Leftrightarrow \quad \neg A \vee B$$

und entsprechend

$$\neg(A \Rightarrow B) \quad \Leftrightarrow \quad A \wedge \neg B$$

Im *indirekten Beweis* zeigen wir, dass $A \wedge \neg B$ falsch ist. Dazu nehmen wir die Verneinung der Behauptung als wahr an und zeigen, dass nicht gleichzeitig die Voraussetzung wahr ist.

Beispiel 1.2 Man zeige für $a, b \geq 0$

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Als Voraussetzung können wir hier $(a-b)^2 \geq 0$ nehmen. Um mit dem indirekten Beweis zu beginnen, nehmen wir die Verneinung der Behauptung an,

$$\frac{a+b}{2} < \sqrt{ab}$$

und erhalten

$$\Rightarrow \quad a+b < 2\sqrt{ab} \quad \Rightarrow \quad (a+b)^2 < 4ab$$

$$\Rightarrow a^2 - 2ab + b^2 < 0 \quad \Rightarrow \quad (a-b)^2 < 0.$$

mit Widerspruch zur Voraussetzung. Wie so oft ist hier der indirekte Beweis komplizierter als der direkte. Daher: Immer zuerst direkt versuchen! □

Aus der Wahrheitstafel für die Implikation folgt

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

Man nennt $\neg B \Rightarrow \neg A$ die *Kontraposition* zu $A \Rightarrow B$.

Beispiel 1.3 Man zeige:

Wenn n^2 gerade ist, so ist auch n gerade.

Die Kontraposition ist:

Wenn n ungerade ist, so ist auch n^2 ungerade.

Beweis der Kontraposition:

$$n = 2k+1 \quad \Rightarrow \quad n^2 = 4k^2 + 4k + 1.$$

□

1.3 Mengen, Relationen, Abbildungen Unter einer Menge verstehen wir eine Zusammenfassung von Gegenständen. Wir schreiben $a \in A$, wenn a in der Menge A liegt, ansonsten schreiben wir $a \notin A$. Für die Menge $A_2 = \{1, 2\}$ gilt beispielsweise $1 \in A_2$ und $3 \notin A_2$.

Die *natürlichen Zahlen*

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

werden später noch genauer untersucht. Für kompliziertere Mengen gibt es eine Vielzahl von Beschreibungen. So lässt sich die Menge G der geraden natürlichen Zahlen schreiben als

$$2\mathbb{N}, \quad G = \{2n : n \in \mathbb{N}\}, \quad G = \{n \in \mathbb{N} : n \text{ ist gerade}\}.$$

In der *leeren Menge* $\emptyset = \{\}$ begegnet uns der horror vacui: Die Aussage $a \in \emptyset$ ist für jedes a falsch.

Wir setzen

$$A = B \quad \Leftrightarrow \quad (x \in A \Leftrightarrow x \in B)$$

$$A \subset B \quad \Leftrightarrow \quad (x \in A \Rightarrow x \in B) \quad (Teilmenge),$$

$$A \cap B \quad \Leftrightarrow \quad \{x : x \in A \wedge x \in B\} \quad (Schnittmenge),$$

$$A \cup B \quad \Leftrightarrow \quad \{x : x \in A \vee x \in B\} \quad (Vereinigungsmenge),$$

$$A \setminus B \quad \Leftrightarrow \quad \{x : x \in A,\ x \notin B) \quad (Komplement).$$

Die Definition der Teilmenge ist wörtlich zu nehmen. Es gilt $B \subset B$ und $\emptyset \subset B$ für alle Mengen B. Denn die Voraussetzung $x \in \emptyset$ ist falsch und daher ist $x \in \emptyset \Rightarrow x \in B$ wahr. Sind die zu untersuchenden Mengen alle Teilmengen einer Menge M, so schreibt man auch A^c an Stelle von $M \setminus A$.

Man beachte den Unterschied zwischen $A = \{a\}$ und $A' = \{\{a\}\}$. Es gilt $\{a\} \in A'$, aber $a \notin A'$. Die *Potenzmenge* einer Menge A ist

$$\mathcal{P}(A) = 2^A = \{B : B \subset A\}.$$

Für die Menge $A_2 = \{1, 2\}$ gilt beispielsweise

$$\mathcal{P}(A_2) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

$\mathcal{P}(A_2)$ besteht daher aus 4 Elementen, die alle selber Mengen sind.

Für eine nichtleere Menge I, die hier *Indexmenge* genannt wird, gebe es für jedes $i \in I$ eine Menge A_i. Dann kann man Durchschnitt und Vereinigung eines solchen Mengensystems ähnlich wie zuvor definieren:

$$\cap_{i\in I} A_i = \{x : \forall i \in I : x \in A_i\}, \quad \cup_{i\in I} A_i = \{x : \exists i \in I : x \in A_i\}.$$

Für zwei Elemente a, b heißt (a, b) *geordnetes Paar*. Im Unterschied zur Menge $A = \{a, b\} = \{b, a\}$ kommt es hier auf die Reihenfolge an. Es gilt $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$. Analog ist das (geordnete) n-tupel $(a_1, a_2, \ldots, a_n)$ definiert. Für Mengen $A_1, \ldots, A_n$ ist das *kartesische Produkt*

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : \ a_i \in A_i \text{ für } i = 1, 2, \ldots, n\}$$

definiert.

Für eine Menge A heißt $R \subset A \times A$ *Relation*. Ist $(a, b) \in R$, so schreibt man meist aRb und sagt, dass a und b in der Relation R stehen. Als einfaches Beispiel können wir die natürlichen Zahlen nehmen, die nach Größe geordnet werden. Die zugehörige Relation ist dann

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \leq b\}.$$

Statt aRb schreibt man dann gleich $a \leq b$.

Eine Relation R heißt

(a) *reflexiv*, wenn aRa für alle $a \in A$,

(b) *symmetrisch*, wenn mit aRb auch bRa gilt,

(c) *antisymmetrisch*, wenn aus aRb und bRa folgt, dass $a = b$,

(d) *transitiv*, wenn aus aRb und bRc folgt, dass aRc.

Eine Relation R heißt *Ordnungsrelation* oder *Halbordnung*, wenn sie reflexiv, antisymmetrisch und transitiv ist. Eine Ordnungsrelation heißt *total*, wenn zusätzlich gilt: Für alle $a, b \in A$ gilt aRb oder bRa.

Aus einer Ordnungsrelation $\leq$ erhält man eine *strenge Ordnungsrelation*, indem man setzt

$$a < b \ \Leftrightarrow \ a \leq b \text{ und } a \neq b.$$

Ordnungsrelationen auf Mengen von Zahlen wie die oben beschriebene sind meist totale Ordnungsrelationen.

Beispiele 1.4 (i) Sei B eine nichtleere Menge. Auf der Potenzmenge $\mathcal{P}(B)$ ist die Teilmengenbeziehung $\subset$ eine Ordnungsrelation, die aber, sofern B mehr als ein Element enthält, keine totale Ordnung ist.

(ii) Auf einer Menge A existiere eine totale Ordnung $\leq$. Wie kann man die n-tupel $(a_1, a_2, \ldots, a_n) \in A^n = A \times \ldots \times A$ sinnvoll ordnen? Eine Möglichkeit ist die *komponentenweise Ordnung* $\leq_k$

$$(a_1, \ldots, a_n) \leq_k (b_1, \ldots, b_n) \;\Leftrightarrow\; a_i \leq b_i \text{ für } i = 1, \ldots, n.$$

Diese ist zwar eine Ordnungrelation, aber bereits für die Menge $A_2 = \{1, 2\}$ und $n = 2$ nicht total, wie die Unvergleichbarkeit von $(1, 2)$ und $(2, 1)$ zeigt.

Eine totale Ordnung ist die *lexikographische* Ordnung

$$(a_1, \ldots, a_n) <_l (b_1, \ldots, b_n) \;\Leftrightarrow\; \exists i_0\ a_i = b_i \text{ für } i = 1, \ldots, i_0 - 1 \text{ und } a_{i_0} < b_{i_0},$$

Wörterbücher verwenden eine leicht modifizierte lexikographische Ordnung, leicht modifiziert deshalb, weil die Wörter unterschiedlich lang sind. □

Sei A mit einer Halbordnung $\leq$ versehen. Wir nennen $m \in A$ *minimal*, wenn es kein $a \in A \setminus \{m\}$ gibt mit $a \leq m$. $m \in A$ heißt *Minimum* von A, wenn $m \leq a$ für alle $a \in A$ gilt. In diesem Fall schreiben wir $m = \min A$. Das Minimum ist, falls es existiert, eindeutig bestimmt und minimal. Jede endliche, total geordnete Menge A besitzt ein Minimum.

$T \subset A$ heißt *nach unten beschränkt in* A, wenn es ein $u \in A$ gibt mit $u \leq t$ für alle $t \in T$. In diesem Fall heißt u *untere Schranke* von T. Die ganzen Zahlen $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ mit der natürlichen Ordnung sind nach unten unbeschränkt.

Die Begriffe maximal, Maximum, obere Schranke sind analog definiert. Wenn T nach unten und nach oben beschränkt in A ist, so heißt T *beschränkt in* A.

Eine reflexive, symmetrische und transitive Relation heißt *Äquivalenzrelation*. In diesem Fall schreiben wir meist $\sim$ statt R. Jedem $a \in A$ ordnen wir die *Äquivalenzklasse*

$$\overline{a} = \{x \in A : a \sim x\}$$

zu. Wegen der Reflexivität ist $a \in \overline{a}$. Weiter folgt aus der Transitivität, dass $\overline{a} = \overline{b}$ genau dann, wenn $a \sim b$. Hier deutet sich schon an, dass A in Äquivalenzklassen zerfällt. Das wollen wir im Folgenden präzisieren.

Sei A nichtleer. Eine Menge von Teilmengen $A_i \subset A$, $A_i \neq \emptyset$, $i \in I$, heißt *Partition* oder *disjunkte Zerlegung* von A, wenn $A_i \cap A_j = \emptyset$ für $i \neq j$ (disjunkt!) und $A = \cup_{i \in I} A_i$ (Zerlegung!). Es gilt

Satz 1.5 *Die Begriffe „Äquivalenzrelation“ und „disjunkte Zerlegung“ sind im folgenden Sinne äquivalent:*

(a) *Zu einer disjunkten Zerlegung $\{A_i : i \in I\}$ von A definiere*

$$a \sim b \;\Leftrightarrow\; \exists i \in I \text{ mit } a, b \in A_i.$$

Dann ist $\sim$ Äquivalenzrelation mit Äquivalenzklassen A_i.

(b) *Die Äquivalenzklassen bilden eine disjunkte Zerlegung von A.*

Beweis: (a) $a \sim a$ gilt wegen $A = \cup_i A_i$, a muss daher zu einem A_i gehören. $a \sim b \Leftrightarrow b \sim a$ ist offensichtlich. $a \sim b$ bedeutet $a, b \in A_i$ und $b \sim c$ bedeutet $b, c \in A_j$. Da die Mengen A_i und A_j disjunkt sind und b zu beiden Mengen gehört, muss $i = j$ gelten.

(b) Wegen $a \in \overline{a}$ sind die Äquivalenzklassen nichtleer. Mit $\cup_{a \in A}\{a\} = A$ ist auch $\cup_{a \in A}\overline{a} = A$. Ist $\overline{a} \cap \overline{b} \neq \emptyset$, so gibt es ein c mit $c \in \overline{a}$, $c \in \overline{b}$. Damit folgt $a \sim c$ und $b \sim c$, mit der Transitivität auch $a \sim b$. □

Das Konzept der Relation lässt sich auf vielfältige Weise erweitern. Zunächst kann man auch Relationen zwischen verschiedenen Mengen definieren, also $R \subset A \times B$. A könnte hier eine Menge von Personen sein und B eine Menge von Firmen. aRb könnte dann bedeuten, dass a ein Kunde der Firma b ist. Auch der Übergang zu mehr als zweistelligen Relationen ist manchmal sinnvoll.

Seien A und B nichtleere Mengen. Eine *Abbildung* f zwischen diesen Mengen ordnet jedem Element $a \in A$ genau ein Element $b \in B$ zu. Wir schreiben für diese Zuordnung $f(a) = b$ und $a \mapsto b$ sowie $f : A \to B$. A heißt Definitions- und B Werte- oder Zielbereich der Abbildung f. Man kann eine Abbildung auch als Relation auffassen vermöge der Beziehung

$$f(a) = b \;\Leftrightarrow\; (a, b) \in G_f \subset A \times B.$$

G_f heißt *Graph* von f.

Abbildungen zwischen Zahlbereichen werden oft als *Funktionen* bezeichnet, was hauptsächlich historische Gründe hat.

Für $A' \subset A$ setzen wir

$$f(A') = \{f(a) : a \in A'\}.$$

$f(A')$ heißt *Bild von* A' und ist auch im Fall $A' = A$ eine sinnvolle Bezeichung. Es gilt für $A_1, A_2 \subset A$

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2), \quad f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

Solche Beziehungen beweist man durch Rückgriff auf die einzelnen Elemente. Als Beispiel beweisen wir die Aussage rechts. Ist $b \in f(A_1 \cap A_2)$, so gibt es ein $a \in A_1 \cap A_2$ mit $f(a) = b$. Dann gilt aber auch $b \in f(A_1)$ und $b \in f(A_2)$. Als Gegenbeispiel, dass keine Gleichheit herrschen muss, nehmen wir $A_1 = \{a_1\}$, $A_2 = \{a_2\}$ und $f(a_1) = f(a_2) = b$.

Für $B' \subset B$ heißt

$$f^{-1}(B') = \{a \in A : f(a) \in B'\} \tag{1.1}$$

das *Urbild von* B'. Für $B_1, B_2 \subset B$ gilt

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2), \quad f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2).$$

Sei $f : A \to B$ eine Abbildung. f heißt *surjektiv*, wenn $f(A) = B$. f heißt *injektiv*, wenn aus $f(a_1) = f(a_2)$ folgt, dass $a_1 = a_2$. Anders ausgedrückt werden verschiedene Elemente des Urbildbereichs auf verschiedene Elemente des Zielbereichs abgebildet. Eine Abbildung heißt *bijektiv*, wenn sie injektiv und surjektiv ist. Anschaulich hat in diesem Fall jedes Element $a \in A$ genau einen Partner $b = f(a) \in B$ und umgekehrt hat jedes $b \in B$ genau einen Partner $a \in A$. Damit existiert die *Umkehrabbildung* oder *Inverse* von f

$$f^{-1} : B \to A \text{ mit } f^{-1}(f(a)) = a \text{ und } f(f^{-1}(b)) = b.$$

Diese Umkehrabbildung unterscheidet sich in der Notation nicht von der Definition des Urbilds in (1.1), im Gegensatz zu letzterer ist sie aber eine echte Abbildung.

Bei endlichen Mengen A haben die Selbstabbildungen $f : A \to A$ eine Besonderheit. In diesem Fall gilt nämlich

$$f \text{ ist surjektiv } \Leftrightarrow\; f \text{ ist injektiv } \Leftrightarrow\; f \text{ ist bijektiv.} \tag{1.2}$$

Ist $g : A \to B$ und $f : B \to C$, so ist die *Hintereinanderausführung* oder *Verkettung* definiert durch

$$f \circ g : A \to C, \quad a \mapsto f(g(a)).$$

1.4 Mathematische Strukturen lassen sich in der Form

$$\mathbb{S} = \{S, e_1, \ldots, e_l, f_1, \ldots, f_m, R_1, \ldots, R_n\}$$

schreiben mit

S Grundmenge

e_i ausgezeichnete (meist neutrale) Elemente ,

f_j Abbildungen (meist zweistellige Operationen wie $+$),

R_k (meist zweistellige) Relationen.

Dies ist redundant, weil man alle Abbildungen auch als Relationen schreiben kann.

1.5 Gruppen Eine *Gruppe* $\mathbb{G} = (G, e, \circ)$ besteht aus einer Menge G, einer zweistelligen Operation $\circ$ mit $z = x \circ y \in G$, und einem ausgezeichneten Element $e \in G$, so dass:

(G1) (Assoziativgesetz) Für alle $x, y, z \in G$ gilt

$$(x \circ y) \circ z = x \circ (y \circ z).$$

(G2) (Neutrales Element) Für alle $x \in G$ gilt

$$e \circ x = x \circ e = x.$$

(G3) (Inverses Element) Zu jedem $x \in G$ gibt es ein $x^{-1} \in G$ mit

$$x^{-1} \circ x = x \circ x^{-1} = e.$$

Die Axiome sind in dieser Form redundant. Z.B. genügt es, an Stelle von (G2) nur $x \circ e = x$ zu fordern, was in der Literatur manchmal geschieht. In diesem Fall muss man $e \circ x = x$ mit Hilfe der anderen Axiome explizit beweisen, was wir uns ersparen möchten.

Endliche Gruppen gibt man mit einer *Gruppentafel* an, in der die Ergebnisse von $x \circ y$ eingetragen werden. Wir bezeichnen die Gruppenelemente mit $0, 1, 2, \ldots$, wobei 0 das neutrale Element ist. Die Gruppe mit 3 Elementen ist eindeutig bestimmt:

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.

Vierelementige Gruppen gibt es schon mehrere:

$\circ$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\circ$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Gruppen mit unendlicher Grundmenge sind die ganzen und die rationalen Zahlen

$$\mathbb{G} = (\mathbb{Z}, 0, +), \quad \mathbb{G} = (\mathbb{Q}, 0, +), \quad \mathbb{G} = (\mathbb{Q} \setminus \{0\}, 1, \cdot),$$

die in den nächsten Kapiteln besprochen werden. Dagegen bilden die natürlichen Zahlen mit der Addition keine Gruppe, weil wir die positiven Zahlen nicht invertieren können.

Also: Konkrete Gruppen können alles mögliche sein. Daher ist es hier wie meist in der Algebra wichtig, dass die Beweise streng aus den Axiomen folgen. Als Beispiel zeigen wir den folgenden

Satz 1.6 *In jeder Gruppe sind die Gleichungen $x \circ a = b$ und $a \circ x = b$ eindeutig nach x auflösbar.*

Beweis: Man muss hier vorsichtig sein, weil das Kommutativgesetz $x \circ y = y \circ x$ nicht unbedingt gelten muss. Als Lösung von $x \circ a = b$ vermuten wir $x = b \circ a^{-1}$,

$$x \circ a = (b \circ a^{-1}) \circ a \overset{(G1)}{=} b \circ (a^{-1} \circ a) \overset{(G3)}{=} b \circ e \overset{(G2)}{=} b.$$

Für den Beweis der Eindeutigkeit nehmen wir an, dass die Gleichung $x \circ a = b$ von zwei Gruppenelementen x, x' gelöst wird. Aus $x \circ a = x' \circ a$ folgt durch Multiplikation von rechts mit a^{-1}, dass $x = x'$.

Die eindeutige Lösbarkeit von $a \circ x = b$ zeigt man ganz analog. □

Aufgrund dieses Satzes sind das neutrale und das inverse Element eindeutig bestimmt. Ferner sind die Gruppentafeln *Lateinische Quadrate*, bei denen in jeder Zeile und in jeder Spalte jedes Element genau einmal vorkommt.

Eine Gruppe heißt *abelsch* oder *kommutativ*, wenn zusätzlich das Kommutativgesetz gilt:

(G4) Für alle $x, y \in G$ gilt

$$x \circ y = y \circ x.$$

Bei einer kommutativen Gruppe schreibt man meist + statt $\circ$ mit dem neutralen Element 0. Dies erinnert an die ganzen Zahlen $\mathbb{Z} = (Z, 0, +)$, die ja eine kommutative Gruppe bilden.

Satz 1.7 *Sei A eine nichtleere Menge. Dann bilden die bijektiven Selbstabbildungen $f : A \to A$ zusammen mit der Verkettung $f \circ g$ eine Gruppe mit neutralem Element $id_A : A \to A$, $id_A(a) = a$. Insbesondere ist mit f, g bijektiv auch $f \circ g$ bijektiv und*

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}.$$

Beweis: Die angegebene Formel für die Inverse von $f \circ g$ rechnet man nach. $f \circ id_A = id_A \circ f = f$ ist klar. Das inverse Element zu f ist die von uns definierte Umkehrabbildung. Ist $a \overset{h}{\mapsto} b \overset{g}{\mapsto} c \overset{f}{\mapsto} d$, so gilt gleichgültig wie man klammert, immer $f(g(h(a))) = d$. □

Hat die Menge A drei Elemente oder mehr, so ist die Gruppe der bijektiven Selbstabbildungen nicht kommutativ. Als Beispiel nehmen wir für $A_3 = \{1, 2, 3\}$

$$f(1) = 2,\ f(2) = 3,\ g(1) = 2,\ g(2) = 1 \ \Rightarrow\ f \circ g(1) = 3,\ g \circ f(1) = 1.$$

1.6 Ringe und Körper Ein *Ring* besteht aus einer Grundmenge R, zwei ausgezeichneten Elementen $0, 1$ und zwei zweistelligen Operationen „+“ und „$\cdot$“, kurz $\mathbb{R} = (R, 0, 1, +, \cdot)$. Die Ringaxiome sind so gefasst, dass man im Ring ähnlich rechnen kann wie mit Zahlen sonst auch. Genauer muss gelten:

(R1) $(R, 0, +)$ ist eine kommutative Grupppe.

(R2) $(R, 1, \cdot)$ ist eine Halbgruppe mit neutralem Element 1, d.h. es gilt das Assoziativgesetz sowie $x \cdot 1 = 1 \cdot x = x$.

(R3) Es gelten die Distributivgesetze

$$(x + y) \cdot z = x \cdot z + y \cdot z, \quad x \cdot (y + z) = x \cdot y + x \cdot z.$$

Ist die Operation „$\cdot$“ zusätzlich kommutativ, so heißt der Ring *kommutativ*.

Der bekannteste kommutative Ring sind die ganzen Zahlen $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ mit der üblichen Addition und Multiplikation.

Ein *Körper* $\mathbb{K} = (K, 0, 1, +, \cdot)$ ist ein kommutativer Ring, in dem zusätzlich $(K \setminus \{0\}, 1, \cdot)$ eine kommutative Gruppe ist. Zu jedem $x \neq 0$ gibt es daher ein x^{-1} mit $xx^{-1} = 1$.

Der einfachste Körper ist $\mathbb{Z}_2$, der nur aus den beiden neutralen Elementen 0 und 1 besteht. 0 ist ja neutral bezüglich der Addition und 1 ist neutral bezüglich der Multiplikation. Darüberhinaus setzen wir $1 + 1 = 0$ und $0 \cdot 0 = 0$. Damit ist 1 zu sich selbst invers bezüglich Addition und Multiplikation.