Teil I

Grundlagen

1

Grundlagen der Aussagenlogik

Mathematische Logik und Mengenlehre sind grundlegend für den Aufbau, die Entwicklung und die einheitliche Darstellung der mathematischen Disziplinen. Die mathematische Logik formalisiert die Sprache, in der mathematische Aussagen formuliert werden, und stellt Regeln auf, um aus gegebenen Aussagen neue herzuleiten.

1.1 Aussagen

In der Mathematik werden Aussagen in einer formalisierten Sprache wiedergegeben, die nur noch die logisch relevanten Elemente der Umgangssprache enthält.

Aussagenbegriff

Eine *Aussage* ist eine sprachliche Formulierung, die einen Wahrheitswert besitzt. Eine Aussage ist entweder *wahr* (w) oder *falsch* (f). Die Aussagen "$3+2=5$" und "*7 ist eine Primzahl*" sind wahr, während die Aussagen "*New York ist die Hauptstadt der USA*" und "*Paris liegt in England*" falsch sind. Keine Aussagen sind "*Wohin gehst Du?*" oder "*Sei x eine Primzahl*".

Verknüpfung von Aussagen

Seien P und Q Aussagen. Zusammengesetzte Aussagen sind

- *Negation*: $\neg P$ oder $\overline{P}$, sprich "*nicht P*".
- *Konjunktion*: $P \wedge Q$, sprich "*P und Q*".
- *Disjunktion*: $P \vee Q$, sprich "*P oder Q*".
- *Implikation*: $P \Rightarrow Q$, sprich "*wenn P, dann Q*"; die Aussage P heißt *Prämisse* und die Aussage Q *Konklusion.*
- *Äquivalenz*: $P \Leftrightarrow Q$, sprich "*P genau dann, wenn Q*".

Die vermittelnden Wörter in zusammengesetzten Aussagen, "*nicht*", "*und*", "*oder*", "*wenn...dann*", und "*genau dann, wenn...*", heißen *Junktoren*. Der Wahrheitswert einer zusammengesetzten Aussage wird durch eine *Wahrheitstafel* definiert

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
f	f	w	f	f	w	w
f	w		f	w	w	f
w	f	f	f	w	f	f
w	w		w	w	w	w

Beispiel 1.1. Die Aussage "*Wenn New York ist die Hauptstadt der USA, dann gibt es keine Marsmännchen*" besteht aus zwei Teilaussagen

P: "*New York ist die Hauptstadt der USA*"
Q: "*Es gibt Marsmännchen*"

Die zusammengesetzte Aussage lautet $P \Rightarrow (\neg Q)$; sie ist wahr, weil die Prämisse falsch ist.

1.2 Aussageformen

Aussageformen sind die zentralen Sprachelemente der Aussagenlogik.

Aussageformen

Aussagenvariablen sind Variablen, in die Aussagen eingesetzt werden können. *Aussageformen* sind durch Junktoren verknüpfte Aussagen oder Aussagenvariablen und sind wie folgt definiert:

- Aussagen und Aussagenvariablen sind Aussageformen.
- Sind P und Q Aussageformen, dann sind Aussageformen

$$(\neg P),\ (P \wedge Q),\ (P \vee Q),\ (P \Rightarrow Q),\ (P \Leftrightarrow Q). \tag{1.1}$$

Beispiel 1.2. Seien P und Q Aussagenvariablen. Aussageformen sind $((P \wedge (P \Rightarrow Q)) \Rightarrow Q)$ und $(w \vee ((P \Rightarrow Q) \Rightarrow Q))$, wobei w für eine beliebige wahre Aussage steht.

Vereinfachung von Aussageformen

Aussageformen werden vereinfacht, indem die äußeren Klammern weggelassen werden. Weitere Klammern werden durch eine Konvention eingespart, nach der bei Fehlen von Klammern gewisse Junktoren stets vor anderen auszuführen sind. Die Negation hat Vorrang vor Konjunktion und Disjunktion, die beide gleichberechtigt sind und ihrerseits Vorrang haben vor der Implikation, während die Implikation hat Vorrang vor der Äquivalenz.

Beispiel 1.3. Die Aussageform $P \wedge (Q \vee R) \Rightarrow \neg Q \wedge P$ bedeutet $((P \wedge (Q \vee R)) \Rightarrow (\neg(Q) \wedge P))$.

Die Vorrangregeln greifen nicht bei Aussageformen mit lauter gleichen Junktoren. Die Aussageformen $P \wedge Q \wedge R$, $P \vee Q \vee R$, und $P \Leftrightarrow Q \Leftrightarrow R$ werden links geklammert, d.h., interpretiert als $(P \wedge Q) \wedge R$, $(P \vee Q) \vee R$ und $(P \Leftrightarrow Q) \Leftrightarrow R$. Die Aussageform $P \Rightarrow Q \Rightarrow R$ wird rechts geklammert, d.h., interpretiert als $P \Rightarrow (Q \Rightarrow R)$.

1.3 Erfüllbarkeit und Gültigkeit

Zustände

Sei P eine Aussageform, die Aussagenvariablen enthält. Wird jeder solchen Aussagenvariable ein Wahrheitswert zugeordnet, so wird der Aussageform P ein Wahrheitswert anhand einer Wahrheitstafel zugewiesen. Eine Liste von Gleichungen $Q = v$, in der jede Aussagenvariable Q in der Aussageform P mit einem Wahrheitswert v belegt wird, heißt ein *Zustand* von P.

Beispiel 1.4. Die Aussageform $P \Rightarrow Q \wedge P$ ist im Zustand $P = w$ und $Q = f$ falsch und im Zustand $P = f$ und $Q = f$ wahr.

Erfüllbarkeit

Eine Aussageform P heißt *erfüllbar* in einem Zustand, wenn P wahr ist in diesem Zustand. Eine Aussageform P heißt *erfüllbar*, wenn es einen Zustand von P gibt, in dem P erfüllbar ist.

Beispiel 1.5. Die Aussageform $P \Rightarrow Q \wedge P$ ist erfüllbar, weil sie im Zustand $P = f$ und $Q = f$ wahr ist.

Gültigkeit

Eine Aussageform P heißt *gültig* oder eine *Tautologie*, wenn P in jedem Zustand erfüllbar ist.

Beispiel 1.6. Die Aussageform $P \wedge (P \Rightarrow Q) \Rightarrow Q$ ist gültig, wie die folgende Wahrheitstafel zeigt

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$P \wedge (P \Rightarrow Q) \Rightarrow Q$
f	f	w	f	w
f	w	w	f	w
w	f	f	f	w
w	w	w	w	w

Formalisierung von Umgangssprache

Eine umgangssprachliche zusammengesetzte Aussage wird anhand folgender *Faustregel* formalisiert: Wähle die jeweils kürzesten Aussagen, die keine Junktoren enthalten. Für jede solche Aussage beantworte die Frage, ob sie wahr oder falsch ist. Verknüpfe diese Aussagen mithilfe entsprechender Junktoren und ermittle den Wahrheitswert der zusammengesetzten Aussage anhand einer Wahrheitstafel.

Beispiel 1.7. Die zusammengeetzte Aussage "*Um trocken zu bleiben, ist es hinreichend einen Regenmantel zu tragen.*" besagt "*Wenn Du einen Regenmantel trägst, dann bleibst Du trocken*". Sie besteht aus den Aussagen

P: "*Regenmantel tragen*"
Q: "*trocken bleiben*"

und hat die Form $P \Rightarrow Q$. Die umgekehrte Aussage $Q \Rightarrow P$ bedeutet "*Um trocken zu bleiben, ist es notwendig einen Regenmantel zu tragen.*". Sie ist falsch, denn man könnte auch einen Regenschirm benutzen.

1.4 Äquivalenz

Äquivalenz von Aussageformen

Zwei Aussageformen P und Q heißen *äquivalent*, wenn die Aussageform $P \Leftrightarrow Q$ gültig ist. Äquivalente Aussageformen P und Q haben in jedem Zustand den gleichen Wahrheitswert. Für jede gültige Aussageform P gilt also

$$P \Leftrightarrow w, \tag{1.2}$$

wobei w eine beliebige wahre Aussage bezeichnet.

Beispiel 1.8. Die Aussageformen $P \Rightarrow Q$ und $\neg P \vee Q$ sind äquivalent, wie die folgende Wahrheitstafel zeigt

P	Q	$P \Rightarrow Q$	$\neg P \vee Q$	$(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$
f	f	w	w	w
f	w	w	w	w
w	f	f	f	w
w	w	w	w	w

Satz 1.9. *Für alle Aussageformen P, Q und R gelten folgende Rechengesetze*

- *Kommutativgesetz:*

$$P \vee Q \Leftrightarrow Q \vee P$$
$$P \wedge Q \Leftrightarrow Q \wedge P$$

- *Assoziativgesetz:*

$$P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$$
$$P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$$

- *Idempotenzgesetz:*

$$P \vee P \Leftrightarrow P$$
$$P \wedge P \Leftrightarrow P$$

- *Distributivgesetz:*

$$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$$
$$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$$

- *Gesetze von De Morgan (1806-1878):*

$$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$$
$$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$$

- *Absorptionsgesetz:*

$$P \vee (P \wedge Q) \Leftrightarrow P$$
$$P \wedge (P \vee Q) \Leftrightarrow P$$

- *Gesetz von der doppelten Verneinung:*

$$\neg(\neg P) \Leftrightarrow P.$$

- *Gesetze mit wahren und falschen Aussagen:*

$$\neg P \wedge P \Leftrightarrow f$$
$$\neg P \vee P \Leftrightarrow w$$
$$P \vee f \Leftrightarrow P$$
$$P \vee w \Leftrightarrow w.$$

Beweis. Wir zeigen exemplarisch das erste Gesetz von De Morgan anhand einer Wahrheitstafel:

P	Q	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
f	f	w	w	w
f	w	w	w	w
w	f	w	w	w
w	w	f	f	w

□

Umformen von Aussageformen

Die Rechengesetze können dazu benutzt werden, um komplizierte Aussageformen schrittweise zu vereinfachen.

Beispiel 1.10. Für die Aussageform $\neg(P \wedge Q) \vee P$ gilt

$$\begin{aligned}
\neg(P \wedge Q) \vee P &\Leftrightarrow (\neg P \vee \neg Q) \vee P && \text{De Morgan}\\
&\Leftrightarrow \neg P \vee (\neg Q \vee P) && \text{Assoziativität}\\
&\Leftrightarrow \neg P \vee (P \vee \neg Q) && \text{Kommutativität}\\
&\Leftrightarrow (\neg P \vee P) \vee \neg Q && \text{Assoziativität}\\
&\Leftrightarrow w \vee \neg Q && \text{Gesetz mit } w\text{, Kommutativität}\\
&\Leftrightarrow w && \text{Gesetz mit } w.
\end{aligned}$$

Syntax und Semantik der Aussagenlogik

Die Verknüpfung von logischen Ausdrücken wirkt auf zwei logischen Ebenen, Syntax und Semantik. Die *Syntax* bezieht sich auf die Form von Aussagen und die *Semantik* auf den Inhalt oder den Wahrheitswert von Aussagen. Syntax und Semantik lassen sich anhand der Frage unterscheiden, ob eine Aussageform eine Tautologie ist. Auf semantischer Ebene wird diese Frage durch Aufstellen einer Wahrheitstafel, also das Zuordnen von Bedeutung beantwortet. Auf syntaktischer Ebene kann diese Frage anhand eines vollständigen Axiomensystems der Aussagenlogik beantwortet werden. Wenn die Aussageform aus dem Axiomensystem herleitbar ist, dann wird gefolgert, dass es sich um eine Tautolgie handelt.

1.5 Schaltungsentwurf

Die Aussagenlogik ist grundlegend für den Entwurf von elektronischen Schaltungen.

Gatter

Logische Schaltungen werden mithilfe der logischer Grundfunktionen *und*, *oder* und *nicht* realisiert. Diese Grundfunktionen werden *Gatter* genannt. Sie können miteinander zu komplizierten integrierten Schaltungen kombiniert werden, die arithmetische, speicher- oder steuerungsbezogene Aufgaben lösen.

UND- und ODER-Gatter haben jeweils zwei Eingabeleitungen und eine Ausgabeleitung, während das NICHT-Gatter (oder Inverter) eine Eingabe- und eine Ausgabeleitung besitzt. Auf den Leitungen kann Strom fließen. Das Fließen von Strom auf einer Leitung wird durch den Wahrheitswert wahr dargestellt, das Nichtfließen von Strom durch den Wahrheitswert falsch. Mit dieser Interpretation entspricht das UND-Gatter der Konjunktion, das ODER-Gatter der Disjunktion und das NICHT-Gatter der Negation (Abb. 1.1).

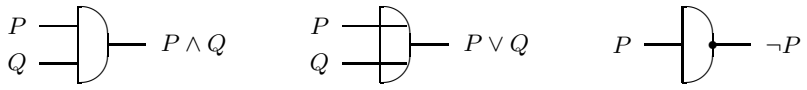

Abb. 1.1. Schaltsymbole für UND-Gatter, ODER-Gatter und NICHT-Gatter.

Verknüpfung von Gattern

An einem Beispiel wird gezeigt, wie Gatter zu komplizierten logischen Schaltkreisen zusammengefügt werden können.

Beispiel 1.11. Eine Lampe soll von zwei Schaltern unabhängig voneinander ein- und ausgeschaltet werden können. Der die Lampe steuernde logische Schaltkreis hat zwei Eingabeleitungen und eine Ausgabeleitung. Die Eingabeleitungen entsprechen den Schaltern und die Ausgabeleitung der Lampe. Jeder Schalter hat zwei Stellungen. Es stehe wahr (oder 1) für Schalter "ein" und falsch (oder 0) für Schalter "aus". Die Ausgabeleitung gibt an, ob die Lampe brennt: wahr, falls die Lampe brennt, und falsch, wenn sie nicht brennt.

Anfangs seien beide Schalter "aus" und die Lampe brenne in dieser Stellung nicht. Wenn einer der beiden Schalter betätigt wird, soll das Licht angehen. Aus dieser Stellung heraus soll das Licht durch irgendeinen der beiden Schalter wieder ausgeschaltet werden können. Somit wird die gesuchte Schaltung durch folgende Wahrheitstafel beschrieben:

P	Q	$s(P,Q)$
f	f	f
w	f	w
f	w	w
w	w	f

Um die logische Schaltung der Lampensteuerung mit Hilfe von Gattern zu realisieren, muss die Aussageform $s(P,Q)$ vermöge Gatter aus den Eingabesignalen kombiniert werden. Dabei ist nur auf die Zustände zu achten, in denen die Schaltung $s(P,Q)$ den Wert wahr annimmt, also $P = w$ und $Q = f$ sowie $P = f$ und $Q = w$. Die Aussageform $s(P,Q)$ ist äquivalent zur Aussageform

$$(P \wedge \neg Q) \vee (\neg P \wedge Q). \tag{1.3}$$

Die zugehörige logische Schaltung ist in Abb. 1.2 skizziert. Die beiden Inverter sind durch Punkte an den Eingängen der beiden UND-Gatter angedeutet.

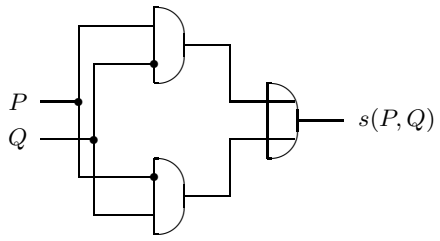

Abb. 1.2. Logischer Schaltkreis für eine Lampensteuerung.

Selbsttestaufgaben

1.1. Sei P die Aussage "*Susi ist reich*" und Q die Aussage "*Susi ist gesund*". Formuliere damit die Aussagen $\neg P \wedge Q$, $\neg P \wedge \neg Q$ und $\neg P \vee (P \wedge \neg Q)$.

1.2. Stelle die Wahrheitstafel für die Aussageform $P \vee \neg Q$ auf.

1.3. Zeige, dass die Aussageform $P \vee \neg(P \wedge Q)$ eine Tautologie ist.

1.4. Vereinfache mittels De Morgan die Aussage "*Es ist nicht wahr, dass ihre Mutter Britin oder ihr Vater Deutscher ist*".

1.5. Negiere die Aussage "*Wenn es kalt ist, trägt er einen Mantel, aber kein T-Shirt*".

1.6. Vereinfache die Aussageform $(P \rightarrow Q) \wedge (P \wedge \neg Q)$. Handelt es sich um eine Tautologie?

1.7. Vereinfache die Aussageform $(P \Rightarrow Q) \Rightarrow ((P \Rightarrow \neg Q) \Rightarrow \neg P)$.

1.8. Zeige, dass die Aussageformen $\neg(P \vee Q) \vee (\neg P \wedge Q)$ und $\neg P$ äquivalent sind, erstens durch Aufstellen einer Wahrheitstafel und zweitens durch Umformen.

1.9. Entwirf eine logische Schaltung für die Aussageform $(P \wedge Q) \vee (\neg P \wedge \neg Q)$.

2

Grundlagen der Prädikatenlogik

In diesem Kapitel wird die Aussagenlogik zur Prädikatenlogik erster Stufe erweitert. Die Prädikatenlogik formalisiert die Sprache, in der mathematische Aussagen gemacht werden. Sie stellt Beweisverfahren bereit und wird unter anderem dazu benutzt, um korrekte Computerprogramme zu entwickeln.

2.1 Objekte, Prädikate und Quantoren

Objekte und Prädikate

In der Aussagenlogik wird die innere Struktur von Aussagen unterdrückt, weil es nur auf den Wahrheitsgehalt der Aussagen ankommt. In der Prädikatenlogik wird in einer Aussage zwischen Objekt und Prädikat unterschieden. Beispielsweise haben die Aussagen "*Betty ist eine Frau*" und "*Claire ist eine Frau*" ein gemeinsames Prädikat, nämlich "*Frau sein*". Sie beziehen sich aber auf unterschiedliche Objekte, "*Betty*" und "*Claire*". Die Aussage "*Claire ist eine Frau*" wird formal symbolisiert durch den Ausdruck $F(c)$. Kleinbuchstaben stehen für Objekte und Großbuchstaben für Prädikate.

Quantoren

Aussagen können sich auf mehrere Objekte beziehen. Die Aussage "*Jeder Mensch hat eine Seele*" wird symbolisiert durch

$$\forall x[M(x) \Rightarrow S(x)], \tag{2.1}$$

d. h., "*Für alle x gilt: Wenn x ein Mensch ist, dann hat x eine Seele*". Das Zeichen $\forall$ heißt *Allquantor* und steht für die Redewendung "*für alle*".

Die Aussage "*Es gibt Genies*" wird ausgedrückt durch

$$\exists x[M(x) \wedge G(x)], \tag{2.2}$$

d. h., "*Es gibt ein x, so dass x ein Mensch und x ein Genie ist*". Das Zeichen $\exists$ heißt *Existenzquantor* und steht für die Redewendung "*es gibt ein*".

Hier sind weitere Beispiele für einstellige Prädikate

"*Alle Primzahlen größer als 2 sind ungerade.*"	$\forall x[P(x) \wedge (x > 2) \Rightarrow U(x)]$
"*Es gibt eine gerade Primzahl.*"	$\exists x[P(x) \wedge G(x)]$

Hier sind Beispiele mit zweistelligen Prädikaten

"*Alle lieben Betty.*"	$\forall x[M(x) \Rightarrow L(x, b)]$
"*Jemand liebt Claire.*"	$\exists x[M(x) \wedge L(x, c)]$
"*Jeder, der Betty mag, mag auch Claire.*"	$\forall x[M(x) \Rightarrow (L(x, b) \Rightarrow L(x, c))]$
"*Betty mag alle Teddies.*"	$\forall x[T(x) \Rightarrow L(x, b)]$

2.2 Existentielle und universelle Quantifizierung

Mehrfache Quantifizierung

Viele Aussagen erfordern mehr als einen Quantor. Die Aussage "*Jeder mag irgendjemanden*" wird symbolisiert durch

$$\forall x[\exists y[L(x, y)]], \tag{2.3}$$

d. h., "*Für jedes x existiert ein y, so dass y von x gemocht wird*". Da sich das Objekt x auf Menschen bezieht, wird die Aussage auch geschrieben in der Form

$$\forall x[M(x) \Rightarrow \exists y[M(y) \wedge L(x, y)]], \tag{2.4}$$

d. h., "*Für alle x gilt: Wenn x ein Mensch ist, dann existiert ein y, so dass y ein Mensch ist und von x gemocht wird*".

Mehrere hintereinander auftretende Quantoren werden von innen nach außen angewendet, wodurch Klammern eingespart werden. Etwa wird das Prädikat $\forall x\,[\forall y\,[P(x, y)]]$ kürzer geschrieben als $\forall x\,\forall y\,[P(x, y)]$.

Hintereinander stehende, gleichartige Quantoren sind stets vertauschbar

$$\forall x\,\forall y\,[P(x, y)] \Longleftrightarrow \forall y\,\forall x\,[P(x, y)] \tag{2.5}$$

$$\exists x\,\exists y\,[P(x, y)] \Longleftrightarrow \exists y\,\exists x\,[P(x, y)] \tag{2.6}$$

Es macht keinen Unterschied, ob wir "*Für alle x und für alle y gilt*" oder "*Für alle y und für alle x gilt*" zum Ausdruck bringen.

Verschiedenartige Quantoren sind nicht vertauschbar. Wenn in der Aussage (2.3) die Quantoren vertauscht werden, dann ergibt sich die Aussage

$$\exists x[\forall y[L(x,y)]], \tag{2.7}$$

d. h., "*Es existiert ein x, so dass jedes y von x gemocht wird*". Diese Aussage bedeutet "*Jemand mag jeden*".

Konjunktion und Disjunktion

Die Aussage "*Die Zahlen 2, 3, 5 und 7 sind Primzahlen*" lässt sich auf zwei Arten ausdrücken. Erstens durch die Konjunktion $P(2) \wedge P(3) \wedge P(5) \wedge P(7)$ und zweitens durch die allquantifizierte Aussage $\forall x[M(x) \Rightarrow P(x)]$, wobei $M(x)$ die Aussage "*x ist eine der Zahlen 2, 3, 5 und 7*" bezeichnet und $P(x)$ für die Aussage "*x ist prim*" steht. Also ist eine allquantifizierte Aussage mit endlichem Gültigkeitsbereich äquivalent zu einer Konjunktion.

Die Aussage "*Eine der Zahlen 2, 4, 6 und 9 ist ein Primzahl*" lässt sich auf zwei Weisen symbolisieren. Einerseits durch die Disjunktion $P(2) \vee P(4) \vee P(6) \vee P(9)$ und andererseits anhand der existenziell quantifizierten Aussage $\exists x[M(x) \wedge P(x)]$, wobei $M(x)$ die Aussage "*x ist eine der Zahlen 2, 4, 6 und 9*" bezeichnet. Somit ist eine existenziell quantifizierte Aussage mit endlichem Gültigkeitsbereich äquivalent zu einer Disjunktion.

Werden universelle Quantifizierung als Konjuktion und existenzielle Quantifizierung als Disjunktion aufgefasst, ergeben sich die Äquivalenzen

$$\forall x\,[P(x) \wedge Q(x)] \Longleftrightarrow \forall x\,[P(x)] \wedge \forall x\,[Q(x)] \tag{2.8}$$

$$\exists x\,[P(x) \vee Q(x)] \Longleftrightarrow \exists x\,[P(x)] \vee \exists x\,[Q(x)]. \tag{2.9}$$

Beziehung zwischen All- und Existenzquantor

Die Aussage "*Nicht jeder ist verliebt*" wird ausgedrückt durch

$$\neg\forall x[M(x) \Rightarrow V(x)], \tag{2.10}$$

d. h., "*Es trifft nicht zu, dass für alle Menschen die Tatsache zutrifft, dass sie Menschen sind, auch impliziert, dass sie verliebt sind*". Die Implikation $P \Rightarrow Q$ ist äquivalent zu $\neg(P \wedge \neg Q)$. Also kann die Aussage "*Nicht jeder ist verliebt*" symbolisiert werden anhand

$$\neg\forall x[\neg(M(x) \wedge \neg V(x))]. \tag{2.11}$$

Der Ausdruck $\neg\forall x\neg$ bedeutet "*Es trifft nicht zu, dass für alle x nicht gilt*" und ist äquivalent zur Redewendung "*Es existiert ein x, so dass gilt*". Somit ist die Aussage (2.10) äquivalent zu

$$\exists x[M(x) \wedge \neg V(x)], \tag{2.12}$$

d. h., "*es gibt Menschen, die nicht verliebt sind*".

Die Aussage "*Es gibt keine Menschen, die nicht sterblich sind*" wird ausgedrückt anhand

$$\neg\exists x[M(x) \wedge \neg S(x)]. \tag{2.13}$$

Der Ausdruck $\neg\exists x\neg$ besagt "*Es trifft nicht zu, dass es ein x gibt, so dass nicht gilt*" und ist äquivalent zur Redewendung "*Für alle x gilt*". Also ist die Aussage (2.13) äquivalent zu

$$\forall x[\neg(M(x) \wedge \neg S(x))], \tag{2.14}$$

die wiederum gleichwertig ist zu

$$\forall x[M(x) \Rightarrow S(x))], \tag{2.15}$$

d. h., "*Alle Menschen sind sterblich*".

2.3 Variablen

Freie und Gebundene Variablen

Die Aussage "*Für alle x und für alle y existiert ein z, so dass* $x+y=z$" wird symbolisiert durch das Prädikat

$$\forall x\,\forall y\,\exists z\,[x+y=z]. \tag{2.16}$$

Die Variablen x, y und z sind jeweils mit einem Quantor verknüpft und werden deshalb *gebunden* genannt.

Die Aussage "*Es existiert ein z, so dass* $x+y=z$" wird ausgedrückt anhand

$$\exists z\,[x+y=z]. \tag{2.17}$$

Die Variable z ist an einen Quantor gebunden, die Variablen x und y jedoch nicht. Die in einem Prädikat nicht an einen Quantor gebundenen Variablen heißen *frei*.

Prädikate, die freie Variablen enthalten, sind keine Aussagen. Ein Prädikat mit freien Variablen wird zu einer Aussage, indem die freien Variable an einen Quantor gebunden oder durch (entsprechende) Konstanten ersetzt werden. Beispielsweise wird das Prädikat (2.17) zu einer Aussage, wenn die Variable x an einen Allquantor gebunden und die Variable y durch eine Konstante ersetzt wird

$$\forall x\exists z\,[x+1=z]. \tag{2.18}$$

Umbenennen von freien Variablen

Gebundene Variablen können problemlos in andere, noch nicht weiter vorkommende Variablen umbenannt werden. Beispielsweise gilt folgende Äquivalenz

$$\forall x[x^2 \geq 0] \quad \Longleftrightarrow \quad \forall y[y^2 \geq 0]. \tag{2.19}$$

Beim Umbenennen von freien Variablen ist jedoch Vorsicht geboten. Als Beispiel wird das folgende Prädikat mit den freien Variablen x und y betrachtet

$$x \leq 1 \wedge 2 \leq y. \tag{2.20}$$

Wenn beide Variablen durch Konstanten ersetzt werden, etwa $x = 1$ und $y = 2$, so ergibt sich die wahre Aussage

$$1 \leq 1 \wedge 2 \leq 2. \tag{2.21}$$

Wird die Variable y in x umbenannt, entsteht das Prädikat

$$x \leq 1 \wedge 2 \leq x. \tag{2.22}$$

Dieses Prädikat liefert immer eine falsche Aussage, ganz gleich, welche Zahl in die Variable x eingesetzt wird.

2.4 Programmierung

Die Prädikatenlogik wird unter anderem dazu benutzt, um korrekte Computerprogramme zu entwickeln.

Einfache Ausdrücke

Die Syntax von *einfachen Ausdrücken* ist wie folgt definiert:

- Jede Konstante oder Variable ist ein Ausdruck.
- Ist E ein Ausdruck, so ist auch (E) ein Ausdruck.
- Ist $\circ$ ein einstelliger Operator und E ein Ausdruck, dann ist auch $(\circ E)$ ein Ausdruck.
- Ist $*$ ein zweistelliger Operator und sind E und F Ausdrücke, so ist auch $(E * F)$ ein Ausdruck.

Die zugelassenen Operatoren sind in Tab. 2.1 angegeben. In einem einfachen Ausdruck können die äußeren Klammern weggelassen werden. Weitere Klammern können eingespart werden, indem Operatoren mit höherem Vorrang stets zuerst ausgewertet werden. Ein Operator $*_1$ hat *Vorrang* vor einem Operator $*_2$, wenn $*_1$ oberhalb von $*_2$ in der Tabelle 2.1 steht. Insbesondere geht Punkt-

$[x := e]$ (höchste Priorität)
$+ - \neg$ (unäre Operatoren)
$**$ (Exponentiation)
$\cdot \; / \; \div$ mod ggT kgV
$+ - \cup \cap \times$
$= \leq < \geq > \in \subset \subseteq$
$\wedge \vee$
$\Rightarrow$
$\equiv$ (niedrigste Priorität)

Tabelle 2.1. Operatoren für einfache Ausdrücke.

vor Strichrechnung, etwa kann $((3 \cdot x) + 2)$ kürzer geschrieben werden in der Form $3 \cdot x + 2$.

Einem einfachen Ausdruck E wird ein Wert zugewiesen, wenn jede in E vorkommende Variable einen Wert besitzt. Eine Liste von Gleichungen $x = v$, in der jede Variable x in E mit einem Wert v verknüpft wird, heißt ein *Zustand* von E. Beispielsweise hat der Ausdruck $x \cdot y + 3$ im Zustand $x = 2$ und $y = 5$ den Wert $2 \cdot 5 + 3 = 13$.

Textuelle Substitution

Seien E und R Ausdrücke und sei x eine Variable. Bezeichne $E[x := R]$ denjenigen Ausdruck, der aus E entsteht, in dem jedes Vorkommen von x in E durch den Ausdruck (R) ersetzt wird.

Beispiele 2.1. Die folgende Tabelle fasst einige textuelle Substitutionen zusammen

Ausdruck	Ergebnis	Vereinfachung
$x[x := x + 1]$	$(x + 1)$	$x + 1$
$(x + 2 \cdot y)[y := x + 1]$	$(x + 2 \cdot (x + 1))$	$x + 2 \cdot (x + 1)$
$(x \cdot y)[y := x \cdot z]$	$(x \cdot (x \cdot z))$	$x \cdot (x \cdot z)$

Zuweisungsbefehl und Hoare-Tripel

Der Zuweisungsbefehl

$$x := E \tag{2.23}$$

wertet den Ausdruck E aus und speichert seinen Wert in der Variable x. Durch die Zuweisung ändert sich der Zustand der Variable x. Beispielsweise führt die Zuweisung $x := y+2$ den Zustand $x = 3$ und $y = 5$ über in den Zustand $x = 7$ und $y = 5$.

Die Semantik eines Befehls S wird durch ein *Hoare-Tripel* nach Sir Antony Hoare (1934+) beschrieben

$$\{P\} \quad S \quad \{Q\}. \tag{2.24}$$

wobei P und Q Prädikate sind, die den Zustand vor der Ausführung bzw. nach der Beendigung des Befehls S charakterisieren. Dabei wird P *Vorbedingung* und Q *Nachbedingung* von S genannt. Ein Hoare-Tripel heißt *gültig*, wenn sein Befehl in einem Zustand ausgeführt, in dem die Vorbedingung wahr ist, und in einem Zustand terminiert, in dem die Nachbedingung wahr ist.

Beispiele 2.2. Das folgende Hoare-Tripel ist gültig

$$\{x \geq 0\} \quad x := x + 1 \quad \{x > 0\}.$$

Denn der im Zustand $x \geq 0$ ausgeführte Befehl $x := x + 1$ endet im Zustand $x > 0$. Hier sind weitere gültige Hoare-Tripel

$$\begin{array}{ll} \{x > 9\} & x := x + 1 \; \{x > 0\} \\ \{x + 1 > 0\} & x := x + 1 \; \{x > 0\}. \end{array}$$

Das folgende Hoare-Tripel ist hingegen nicht gültig

$$\{x = 3\} \quad x := x + 1 \quad \{x = 5\}$$

Semantik des Zuweisungsbefehls

Die *Semantik* des Zuweisungsbefehls (2.23) wird definiert durch das Hoare-Tripel

$$\{Q[x := E]\} \quad x := E \quad \{Q\}. \tag{2.25}$$

Hierbei wird die Vorbedingung durch textuelle Substitution aus der Nachbedingung erhalten.

Satz 2.3. *Das Hoare-Tripel (2.25) ist gültig und für jedes gültige Hoare-Tripel* $\{P\}\ x := E\ \{Q\}$ *gilt*

$$P \Rightarrow Q[x := E]. \tag{2.26}$$

Die zweite Aussage besagt, dass die Vorbedingung $Q[x := E]$ die *schwächste Vorbedingung* für den mit der Nachbedingung Q versehenen Befehl $x := E$ ist.

Beispiele 2.4. Hier sind drei Hoare-Tripel mit schwächsten Vordingungen

$$\begin{array}{lll} \{x + 1 > 3\} & x := x + 1 & \{x > 3\} \\ \{2 \cdot x = 5\} & x := 2 \cdot x & \{x = 5\} \\ \{-x \cdot y + 1 < y\} & x := -x \cdot y + 1 & \{x < y\} \end{array}$$

Sequenzen von Zuweisungsbefehlen

Die Semantik einer Sequenz von Zuweisungsbefehlen wird analog definiert. Als Beispiel wird eine Sequenz von zwei Zuweisungen mit einer gegebenen Nachbedingung betrachtet

$$\{P\} \quad x := x + 1;\ y := x \cdot y \quad \{x > 3 \wedge y > 0\}. \tag{2.27}$$

Die schwächste Vorbedingung wird schrittweise hergeleitet. Zuerst wird die schwächste Vorbedingung für die zweite Zuweisung aufgestellt

$$\{x > 3 \wedge x \cdot y > 0\} \quad y := x \cdot y \quad \{x > 3 \wedge y > 0\}. \tag{2.28}$$

Diese Vorbedingung dient als Nachbedingung für die erste Zuweisung. Die zugehörige schwächste Vorbedingung ist die schwächste Vorbedingung der zusammengesetzten Anweisung

$$\{x + 1 > 3 \wedge (x + 1) \cdot y > 0\} \quad x := x + 1 \quad \{x > 3 \wedge x \cdot y > 0\}. \tag{2.29}$$

2.5 Beweistechnik

Um Aussagen zu beweisen, gibt es eine Reihe von Methoden, die zum Rüstzeug des Mathematikers gehören. Zuerst wird der Mechanismus des Definierens erörtert.

Definitionen

Eine Definition wird in Form einer logischen Äquivalenz angegeben. Die linke Seite dieser Äquivalenz, *Definiendum* genannt, soll ein Prädikat sein, das die zu definierende Konstante enthält. Die rechte Seite, das *Definiens*, ist ein Prädikat, das nur vorher erklärte Konstanten enthalten darf.

Soll beispielsweise das Zeichen "$\leq$" mit Hilfe des (als bekannt vorausgesetzten) Zeichens "$>$" definiert werden, so lautet das Definiendum

$$x \leq y$$

und das Definiens

$$\textit{es ist nicht der Fall, dass } x > y,$$

zusammen also " *Wir wollen sagen, dass* $x \leq y$ *genau dann, wenn es nicht der Fall ist, dass* $x > y$" oder "$x \leq y$ *ist definitionsgemäß äquivalent zu* $\neg(x > y)$", kürzer

$$x \leq y \quad :\Longleftrightarrow \quad \neg(x > y).$$

Beweis einer allquantifizierten Aussage

Eine allquantifizierte Aussage

$$\forall x[A(x) \Rightarrow P(x)] \tag{2.30}$$

wird in zwei Schritten bewiesen: Zuerst wird der Allquantor *aufgelöst*, indem ein beliebiges Objekt x gewählt wird. Es wird angenommen, dass für das Objekt x die Aussage $A(x)$ wahr ist. Der Beweis beginnt dann wie folgt: "Sei x beliebig gewählt, so dass $A(x)$ gilt". Es ist dann zu zeigen, dass $P(x)$ wahr ist.

Direkter Beweis einer Äquivalenz

Eine Äquivalenz $P \Leftrightarrow Q$ kann auf zwei Arten bewiesen werden. Erstens, indem die Aussage P durch Äquivalenzumformung in die Aussage Q transformiert wird (siehe 1.10). Zweitens, indem die Äquivalenz durch die logisch äquivalente Aussage $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ ersetzt wird, denn es gilt

$$(P \Leftrightarrow Q) \Longleftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P)). \tag{2.31}$$

Beide Implikationen $P \Rightarrow Q$ und $Q \Rightarrow P$ sind als wahr nachzuweisen. Eine Implikation $P \Rightarrow Q$ wird bewiesen, indem die Prämisse P als wahr angenommen wird und gezeigt wird, dass die Konklusion Q wahr ist.

Indirekter Beweis oder Beweis durch Widerspruch

Eine Aussage P kann dadurch bewiesen werden, indem sie negiert wird und von der negierten Aussage $\neg P$ auf eine falsche Aussage geschlossen wird. Diese Vorgehensweise beruht auf dem *Gesetz der Kontraposition*

$$(\neg P \Rightarrow f) \Longleftrightarrow P. \tag{2.32}$$

Beweis einer Existenzaussage

Existenziell quantifizierte Aussagen wie

$$\exists x\,[P(x)] \tag{2.33}$$

lassen sich oft dadurch beweisen, indem ein Objekt a konstruiert wird, so dass die Aussage $P(a)$ wahr ist. Ein solcher Beweis heißt *konstruktiv*. Manchmal kann die Existenz eines solchen Objektes nur mit Hilfe von Abschätzungen nachgewiesen werden, ohne es explizit angeben zu können. Derartige Existenzbeweise sind meist schwierig.

Ableitungsregel Modus Ponens

Logische Ableitungsregeln werden dazu benutzt, das intuitive menschliche Denken auf formale Art darzustellen. Eine wichtige Ableitungsregel ist der *Modus Ponens*. Sie besagt, dass aus wahren Aussagen P und $P \Rightarrow Q$ die wahre Aussage Q gefolgert werden kann. Formal wird der Modus Ponens dargestellt durch

$$\frac{\begin{array}{l} P \\ P \Rightarrow Q \end{array}}{Q} \tag{2.34}$$

Hier ein Beispiel

$$\frac{\begin{array}{l} \text{"}\textit{Claire wird Urlaub machen}\text{"} \\ \text{"}\textit{Wenn Claire Urlaub macht, dann wird Claire glücklich sein}\text{"} \end{array}}{\text{"}\textit{Claire wird glücklich sein}\text{"}}$$

Der Modus Ponens wird häufig kombiniert mit dem *Konjunktionsschluss*

$$P \wedge Q \Rightarrow P \tag{2.35}$$

und dem *Disjunktionsschluss*

$$P \Rightarrow P \vee Q. \tag{2.36}$$

Beide Aussageformen sind Tautologien. Beispielsweise ergeben sich mit dem Konjunktionsschluss

$$\frac{\begin{array}{l} \text{"}\textit{Claire ist reich und schön}\text{"} \\ \text{"}\textit{Wenn Claire reich und schön ist, dann ist Claire schön}\text{"} \end{array}}{\text{"}\textit{Claire ist schön}\text{"}}$$

und dem Disjunktionsschluss

$$\frac{\begin{array}{l} \text{"}\textit{Claire ist reich}\text{"} \\ \text{"}\textit{Wenn Claire reich ist, dann ist Claire reich oder gesund}\text{"} \end{array}}{\text{"}\textit{Claire ist reich oder gesund}\text{"}}$$

Selbsttestaufgaben

2.1. Gib Prädikate für folgende Aussagen an

- "*Menschen sind sterblich*".
- "*Manche Schlangen sind giftig*".
- "*Susi kennt jeden*".
- "*Jeder wird von irgendjemandem geliebt*".

2.2. Sei $P(x)$ das Prädikat "*x ist schön*" und $Q(x)$ das Prädikat "*x ist reich*", wobei x für eine Person stehe. Formalisiere die Aussagen "*Niemand ist reich und schön*" und "*Jemand, der reich ist, ist auch schön*".

2.3. Überlege zu jeder der folgenden Aussagen ein Beispiel, das zeigt, dass die umgekehrte Implikation falsch ist

$$\forall x\,[P(x)] \vee \forall x\,[Q(x)] \Rightarrow \forall x\,[P(x) \vee Q(x)]$$
$$\exists x\,[P(x) \wedge Q(x)] \Rightarrow \exists x\,[P(x)] \wedge \exists x\,[Q(x)].$$

2.4. Gib die freien und gebundenen Variablen in den folgenden Prädikaten an

- "*x ist durch y teilbar*".
- "*Für alle x gilt $x - y = x + (-y)$*".
- "*Für beliebiges x gibt es ein y, so dass $y > 2^x$*".
- "*Zu jeder Umgebung u von a gibt es eine natürliche Zahl n, so dass x_k in u liegt für alle k größer als n.*".

2.5. Sei $A(x)$ das Prädikat "*x ist eine der Zahlen 1, 2, 3, 4 oder 5*". Bestimme den Wahrheitswert der folgenden Aussagen

- $\exists x[A(x) \wedge x + 3 = 10]$.
- $\exists x[A(x) \wedge x + 3 < 5]$.
- $\forall x[A(x) \Rightarrow x + 3 < 10]$.
- $\forall x[A(x) \Rightarrow x + 3 \leq 7]$.

2.6. Ermittle die schwächste Vorbedingung für folgende Zuweisungen und Nachbedingungen

Zuweisung	Nachbedingung
$x := x + 7$	$x + y > 20$
$x := x - 1$	$x^2 + 2 \cdot x = 3$
$x := x - 1$	$(x + 1) \cdot (x - 1) = 0$
$y := x + y$	$y = x$
$y := x + y$	$y = x + y$

2.7. Berechne die schwächste Vorbedingung P für folgendes Programmstück

$$\{P\} \quad x := x + y;\ y := x - y;\ x := x - y \quad \{x = X \wedge y = Y\}$$

3

Mengenlehre

Die Mengenlehre formalisiert den Mengenbegriff und behandelt die Verknüpfung von Mengen. Die Mengenlehre bildet zusammen mit der Prädikatenlogik das sprachliche Gerüst der modernen Mathematik. In diesem Kapitel wird die Mengenlehre aus intuitiver und axiomatischer Sicht eingeführt.

3.1 Mengen und Elemente

Der intuitive Mengenbegriff

Die Mengenlehre wurde begründet von Georg Cantor (1845-1918). Von ihm stammt die folgende "Definition" einer Menge:

> Eine *Menge* ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

Dies ist keine Definition im mathematischen Sinne, weil sich der Begriff *Menge* auf mathematisch nicht weiter definierten Begriffen abstützt.

Darstellung von Mengen

Es gibt zwei Darstellungsformen von Mengen. In der *aufzählenden Form* werden alle Objekte einer Menge aufgelistet. Eine Menge A, die aus den Objekten $a_1, \ldots, a_n$ besteht, wird geschrieben als

$$A = \{a_1, \ldots, a_n\}. \tag{3.1}$$

Ein Objekt x einer Menge A wird auch *Element* von A genannt, abgekürzt $x \in A$.

In der *beschreibenden Form* wird eine Menge durch ein einstelliges Prädikat $P(x)$ beschrieben

$$A = \{x \mid P(x)\}, \tag{3.2}$$

d. h., die Menge A besteht aus allen Objekten x, für die die Aussage $P(x)$ wahr ist. Beispielsweise sei $P(x)$ das Prädikat "*x ist Tochter von Britta*". Dann besteht die Menge $A = \{x \mid P(x)\}$ aus allen Töchtern von Britta.

Eine Menge mit endlich vielen Elementen heißt *endlich*, andernfalls *unendlich*.

Gleichheit von Mengen

Zwei Mengen A und B heißen *gleich*, kurz $A = B$, wenn sie elementweise übereinstimmen

$$A = B \quad :\Longleftrightarrow \quad \forall x\,[x \in A \Leftrightarrow x \in B]. \tag{3.3}$$

Beispielsweise gilt

$$\{1, 2, 1, 1, 3\} = \{3, 1, 2\},$$

weil jedes Element in der linken Menge in der rechten Menge enthalten ist und umgekehrt. Die Elemente einer Menge dürfen also wiederholt und in beliebiger Reihenfolgen aufgelistet werden.

Satz 3.1. *Für alle Mengen A, B und C gilt*

- *Reflexivität:* $A = A$.
- *Symmetrie:* $A = B \Rightarrow B = A$.
- *Transivität:* $A = B \wedge B = C \Rightarrow A = C$.

Teilmengen

Sei A eine Menge und $P(x)$ ein einstelliges Prädikat. Sei B diejenige Menge, die aus allen Elementen $a \in A$ besteht, für die die Aussage $P(a)$ wahr ist, also

$$B = \{a \mid a \in A \wedge P(a)\}. \tag{3.4}$$

Die Menge B heißt eine *Teilmenge* von A, kurz $B \subseteq A$, und die Menge A eine *Obermenge* von B. Eine n-elementige Teilmenge einer Menge wird auch als *n-Teilmenge* bezeichnet. Die Relation $\subseteq$ wird *Inklusion* genannt.

Seien $a_1, \ldots, a_n$ Elemente einer Menge A. Diese Elemente bilden eine Teilmenge von A, denn es gilt

$$\{a_1, \ldots, a_n\} = \{a \mid a \in A \wedge (a = a_1 \vee \ldots \vee a = a_n)\}. \tag{3.5}$$

Beispielsweise ist die Menge aller ganzen Zahlen, die durch 3 teilbar sind, gegeben durch

$$\{x \mid x \in \mathbb{Z} \wedge \exists y\,[y \in \mathbb{Z} \wedge x = 3 \cdot y]\}. \tag{3.6}$$

Satz 3.2. *Für alle Mengen A und B gilt $A = B$ genau dann, wenn $A \subseteq B$ und $B \subseteq A$.*

Beweis. Sei $A = B$. Dann gilt $A = \{a \mid a \in A \wedge a \in B\}$ und $B = \{b \mid b \in B \wedge b \in A\}$. Also ist definitionsgemäß $B \subseteq A$ (mit dem Prädikat $x \in B$) und $A \subseteq B$ (mit dem Prädikat $x \in A$).

Umgekehrt seien $A \subseteq B$ und $B \subseteq A$. Dann gibt es Prädikate $P(x)$ und $Q(y)$ mit $A = \{b \mid b \in B \wedge P(b)\}$ und $B = \{a \mid a \in A \wedge Q(a)\}$. D.h., es gilt $x \in A \Leftrightarrow x \in B \wedge P(x)$. Mit der Auflösung der Äquivalenz (2.31) und dem Konjunktionsschluss (2.35) folgt $x \in A \Rightarrow x \in B$. Analog ergibt sich $x \in B \Rightarrow x \in A$. Nach (2.31) erhellt sich $x \in A \Leftrightarrow x \in B$ und somit $A = B$. □

Satz 3.3. *Für alle Mengen A, B und C gilt*

- *Reflexivität: $A \subseteq A$*
- *Transitivität: $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$*
- *Antisymmetrie: $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$.*

Die leere Menge

Sei A eine Menge. Die *leere Teilmenge* von A besteht aus allen Elementen $a \in A$ mit der Eigenschaft $a \notin A$, also

$$\emptyset_A = \{a \mid a \in A \wedge a \notin A\}. \tag{3.7}$$

Lemma 3.4. *Für beliebige Mengen A und B gilt $\emptyset_A = \emptyset_B$.*

Beweis. Es gilt

$$a \in \emptyset_A \Leftrightarrow a \in A \wedge a \notin A \Leftrightarrow a \in B \wedge a \notin B \Leftrightarrow a \in \emptyset_B,$$

wobei in der zweiten Äquivalenz eine falsche Aussage durch eine andere falsche Aussage ersetzt wurde. Aus der Definition der Mengengleichheit folgt die Behauptung. □

Die Menge $\emptyset_A$ ist also unabhängig von der Obermenge A. Sie wird *leere Menge* genannt und mit $\emptyset$ bezeichnet. Die leere Menge ist Teilmenge einer jeden Menge.

3.2 Verknüpfung von Mengen

Die algebraischen Verknüpfungen mit Mengen wurden von George Boole (1815-1864) eingeführt. Sie basieren auf den logischen Junktoren.

Durchschnitt und Vereinigung

Seien A und B Mengen. Der *Durchschnitt* von A und B ist diejenige Teilmenge von A, deren Elemente auch in B liegen

$$A \cap B = \{a \mid a \in A \wedge a \in B\}. \tag{3.8}$$

Das *Komplement* von B in A ist diejenige Teilmenge von A, deren Elemente nicht zu B gehören

$$A \setminus B = \{a \mid a \in A \wedge a \notin B\}. \tag{3.9}$$

Der Durchschnitt von endlich vielen Mengen $A_1, \ldots, A_n$ ist analog definiert

$$\begin{aligned} A_1 \cap \ldots \cap A_n &= \{a \mid a \in A_1 \wedge \ldots \wedge a \in A_n\} \\ &= \{a \mid a \in A_1 \wedge (a \in A_1 \wedge \ldots \wedge a \in A_n\}. \end{aligned} \tag{3.10}$$

Also ist der Durchschnitt $A_1 \cap \ldots \cap A_n$ eine Teilmenge von A_1 und aufgrund der Kommutativität und Assoziativität der Konjunktion eine Teilmenge jeder der beteiligten Mengen.

Die *Vereinigung* von A und B ist eine Menge, die genau die Elemente enthält, die in A oder B liegen

$$A \cup B = \{a \mid a \in A \vee a \in B\}. \tag{3.11}$$

Beispiel 3.5. Für die Mengen $A = \{1, 2, 3\}$ und $B = \{2, 4, 5\}$ gilt $A \cap B = \{2\}$, $A \setminus B = \{1, 3\}$ und $A \cup B = \{1, 2, 3, 4, 5\}$ (Abb. 3.1).

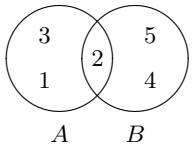

Abb. 3.1. Venn-Diagramm der Mengen A und B.

Satz 3.6. *Für alle Mengen A und B gilt*

$$A \cap B \subseteq A \subseteq A \cup B. \tag{3.12}$$

Beweis. Aus $A \cap B = \{a \mid a \in A \wedge a \in B\}$ und dem Prädikat $x \in B$ folgt $A \cap B \subseteq A$. Weiter gilt

$$\begin{aligned} A &= \{a \mid a \in A\} \\ &= \{a \mid (a \in A \vee a \in B) \wedge a \in A\} \quad \text{Absorption} \\ &= \{a \mid a \in A \cup B \wedge a \in A\} \\ &\subseteq A \cup B \quad \text{Prädikat } a \in A. \end{aligned}$$

□

Satz 3.7. *Für alle Mengen A, B und C gelten folgende Rechengesetze:*

- *Kommutativgesetz:*

$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \end{aligned}$$

- *Assoziativgesetz:*

$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C \\ A \cap (B \cap C) &= (A \cap B) \cap C \end{aligned}$$

- *Idempotenzgesetz:*

$$\begin{aligned} A \cup A &= A \\ A \cap A &= A \end{aligned}$$

- *Distributivgesetz:*

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \end{aligned}$$

- *Gesetze von De Morgan:*

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

- *Absorptionsgesetz:*

$$\begin{aligned} A \cup (A \cap B) &= A \\ A \cap (A \cup B) &= A \end{aligned}$$

- *Eigenschaften der leeren Menge:*

$$A \cup \emptyset = A$$
$$A \cap \emptyset = \emptyset.$$

Diese Aussagen werden anhand der korrespondierenden aussagenlogischen Rechengesetze bewiesen. Als Beispiel zeigen wir das erste Gesetz von De Morgan:

$$\begin{aligned} x \in A \setminus (B \cap C) &\Leftrightarrow x \in A \wedge \neg(x \in B \cap C) \\ &\Leftrightarrow x \in A \wedge \neg(x \in B \wedge x \in C) \\ &\Leftrightarrow x \in A \wedge (\neg x \in B \vee \neg x \in C) \quad \text{De Morgan} \\ &\Leftrightarrow x \in A \wedge (x \notin B \vee x \notin C) \\ &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \quad \text{Distributivität} \\ &\Leftrightarrow (x \in A \setminus B) \vee (x \in A \setminus C) \\ &\Leftrightarrow x \in (A \setminus B) \cup (A \setminus C). \end{aligned}$$

Die Durchschnitts- und Vereinigungsbildung sind monoton bezüglich Inklusion.

Satz 3.8. *Seien A, B und C Mengen. Aus $A \subseteq B$ folgt $A \cup C \subseteq B \cup C$ und $A \cap C \subseteq B \cap C$.*

Zwei nichtleere Mengen heißen *disjunkt*, wenn ihr Durchschnitt leer ist.

Satz 3.9. *Seien A und B disjunkte Mengen. Ist A' eine nichtleere Teilmenge von A, dann sind A' und B disjunkt.*

Beweis. Für die Menge $A' \cap B = \{x \mid x \in A' \wedge x \in B\}$ folgt wegen $A' \subseteq A$ mit dem Konjunktionsschluss $A' \cap B = \{x \mid x \in A' \wedge x \in A \wedge x \in B\} = \{x \mid x \in A' \wedge x \in A \cap B\}$, woraus wegen $A \cap B = \emptyset$ sofort $A' \cap B = \emptyset$ folgt. □

Oft werden Mengen relativ bezüglich einer festen Obermenge G untersucht. Die Menge G wird dann *Grundmenge* genannt und tritt in der Notation nicht mehr auf (Abb. 3.2). Sei A eine Teilmenge von G. Die *Komplementärmenge* von A in G ist

$$\bar{A} = \{g \mid g \in G \wedge g \notin A\}. \tag{3.13}$$

Die Menge $\bar{A}$ ist definitionsgemäß eine Teilmenge von G.

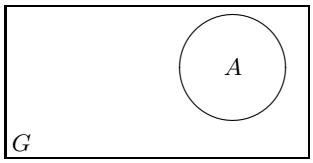

Abb. 3.2. Venn-Diagramm.

3.3 Mengensysteme

Ein *Mengensystem* (oder eine *Menge höherer Ordnung*) ist eine Menge, deren Elemente ebenfalls Mengen sind. Zu den prominentesten Mengensystemen gehören die Potenzmengen.

Potenzmengen

Die *Potenzmenge* einer Menge A ist ein Mengensystem $P(A)$, das aus allen Teilmengen von A besteht, also

$$P(A) = \{B \mid B \subseteq A\}. \tag{3.14}$$

Für jede Menge A gilt $A \in P(A)$. Also tritt jede Menge auch als Element auf. Beispielsweise ist die Potenzmenge von $A = \{1, 2, 3\}$ gegeben durch

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Satz 3.10. *Die Potenzmenge einer n-elementigen Menge besitzt 2^n Elemente.*

Beweis. Die Aussage wird durch vollständige Induktion nach n bewiesen. Sei $n = 0$, also die Menge leer. Es gilt $P(\emptyset) = \{\emptyset\}$. Sei $n \geq 0$ und $A = \{a_1, \ldots, a_{n+1}\}$. Für die n-elementige Teilmenge $B = \{a_1, \ldots, a_n\}$ von A gilt

$$P(A) = \{T \mid T \subseteq B\} \cup \{T \cup \{a_{n+1}\} \mid T \subseteq B\}.$$

Beide Menge auf der rechten Seite besitzen je n Elemente. Nach Induktionsannahme hat die Potenzmenge jeder dieser Mengen 2^n Elemente. Da beide Menge auf der rechten Seite disjunkt sind, besteht $P(A)$ aus $2 \cdot 2^n = 2^{n+1}$ Elementen. □

Sei M ein Mengensystem. Der *Durchschnitt* von $M \neq \emptyset$ ist die Menge

$$\bigcap M = \{a \mid \forall A[A \in M \Rightarrow a \in A]\}. \tag{3.15}$$

Sie enthält alle Objekte, die Elemente in allen Elementen von M sind. Für jedes Element A_0 des Mengensystems M gilt

$$\bigcap M = \{a \mid a \in A_0 \wedge \forall A[A \in M \Rightarrow a \in A]\}. \tag{3.16}$$

Das Mengensystem $\bigcap M$ ist also eine Teilmenge von A_0 und somit eine Teilmenge jedes Elements von M.

Die *Vereinigung* von M ist die Menge

$$\bigcup M = \{a \mid \exists A[A \in M \wedge a \in A]\}. \tag{3.17}$$

Sie besteht aus allen Objekten, die als Elemente in allen Elementen von M enthalten sind. Etwa gilt für das Mengensystem $M = \{\{1,2\},\{2,3\},\{1,2,4\}\}$

$$\bigcup M = \{1,2,3,4\} \quad \text{und} \quad \bigcap M = \{2\}.$$

Satz 3.11. *Für alle Mengen A und B gilt*

- $A \subseteq B \Rightarrow P(A) \subseteq P(B)$.
- $P(A) \cap P(B) = P(A \cap B)$.
- $P(A) \cup P(B) \subseteq P(A \cup B)$.
- $\bigcup P(A) = A$.
- $\bigcap P(A) = \emptyset$.

Beweis. Seien A und B Mengen mit $A \subseteq B$. Es gilt $P(A) = \{C \mid C \subseteq B \wedge C \subseteq A\} = \{C \mid C \in P(B) \wedge C \in P(A)\}$ Also ist $P(A)$ eine Teilmenge von $P(B)$ (mit dem Prädikat $x \in P(A)$).

Seien A und B Mengen. Sei $T \in P(A) \cap P(B)$, also $T \subseteq A$ und $T \subseteq B$. Dies ist gleichbedeutend mit $T \subseteq A \cap B$, d. h., $T \in P(A \cap B)$.

Seien A und B Mengen. Aus $A \subseteq A \cup B$ und $B \subseteq A \cup B$ folgt $P(A) \subseteq P(A \cup B)$ und $B \subseteq A \cup B$. Wegen Satz 3.8 ergibt sich $P(A) \cup P(B) \subseteq P(A \cup B)$.

Sei A eine Menge. Es gilt $x \in \bigcup P(A)$ genau dann, wenn es ein $T \in P(A)$ gibt mit $x \in T$, was gleichbedeutend ist mit $x \in A$.

Jedes Element von $\bigcap P(A)$ liegt in jeder Teilmenge von A, also auch in der leeren Menge. Folglich ist die Menge $\bigcap P(A)$ leer. □

Partitionen

Eine *Partition* einer Menge A ist ein Mengensystem P mit folgenden Eigenschaften:

- $\bigcup P = A$.
- $\emptyset \notin P$.
- Je zwei verschiedene Elemente von P sind disjunkt.

Die Elemente einer Partition werden auch *Blöcke* genannt. Alle Partitionen von $A = \{1, 2, 3\}$ sind $\{\{1\}, \{2\}, \{3\}\}, \{\{1, 2\}, \{3\}\}, \{\{1, 3\}, \{2\}\}, \{\{2, 3\}, \{1\}\}$ und $\{\{1, 2, 3\}\}$.

Antinomien

Es gibt Prädikate, die sich nicht zur Definition einer Menge eignen. Bertrand Russell (1872-1970) bemerkte als Erster, dass dies zu Widersprüchen führen kann.

Beispielsweise gibt es zu jedem Mengensystem A eine Menge B, die nicht Element von A ist. Eine solche Menge ist etwa

$$B = \{a \mid a \in A \wedge a \notin a\}. \tag{3.18}$$

Die Aussage $a \notin a$ macht Sinn, weil a eine Menge ist und Mengen auch Elemente sind. Wir zeigen, dass $B \notin A$. Angenommen, es wäre $B \in A$. Ist $B \notin B$, dann folgt nach Definition von B widersprüchlicherweise $B \in B$. Ist $B \in B$, dann ergibt sich nach Definition von B widersprüchlicherweise $B \notin B$.

Also macht es keinen Sinn, von der "Menge aller Mengen" zu reden. Diese und weitere *Antinomien* haben zur Entwicklung der *Klassentheorie* geführt, in der widerspruchsfrei von der Klasse aller Mengen gesprochen werden kann. Im axiomatischen Aufbau der Mengenlehre werden Antinomien vermieden, indem neue Mengen nur aus schon definierten Mengen abgeleitet werden.

3.4 Axiomatische Mengenlehre

Die Mengenlehre kann anhand eines Axiomensystems aufgebaut werden. *Axiome* sind Lehrsätze, die als wahr erkannt werden, ohne sie auf irgendeine Weise zu begründen. Aus Axiomen werden weitere wahre Aussagen anhand von mathematischen Schlussregeln (z.B. Modus Ponens) hergeleitet. Diese Aussagen heißen *Sätze*. Das Axiomensystem der Mengenlehre fußt auf den nicht weiter definierten Begriffen *Menge* und *Element*.

Axiome der Elementebeziehung und Existenz

M1 Für jedes Element x und jede Menge A besteht genau eine der beiden Beziehungen: $x \in A$ oder $x \notin A$.
M2 Es existiert mindestens eine Menge.
M3 Zu jedem Element x gibt es mindestens eine Menge A mit $x \in A$.

Das Axiom M3 entspricht unserer intuitiven Vorstellung, Elemente nur als zu einer Menge gehörig anzusehen.

Axiom der Gleichheit

M4 Zwei Mengen A und B sind *gleich*, wenn sie elementweise übereinstimmen

$$A = B \quad :\Longleftrightarrow \quad \forall x\,[x \in A \Leftrightarrow x \in B]. \tag{3.19}$$

Teilmengenaxiom

M5 Sei A eine Menge und $P(x)$ ein einstelliges Prädikat in der freien Variablen x, das für jedes Element von A eine Aussage liefert. Dann gibt es eine Menge B, die genau diejenigen Elemente a von A enthält, für die die Aussage $P(a)$ wahr ist. Für die Menge B wird geschrieben

$$B = \{x \mid x \in A \wedge P(x)\}. \tag{3.20}$$

Das Axiom M2 fordert die Existenz einer Menge A. Diese Menge besitzt als Teilmenge die leere Menge. Dabei ist der Fall $A = \emptyset$ nicht ausgeschlossen, weshalb bislang nur die Existenz der leeren Menge gesichert ist. Die Existenz weiterer Mengen wird später mit dem Potenzmengenaxiom erschlossen.

Der *Durchschnitt* von Mengen A und B ist diejenige Teilmenge von A, deren Elemente auch in B liegen

$$A \cap B = \{a \mid a \in A \wedge a \in B\}. \tag{3.21}$$

Das *Komplement* von B in A ist diejenige Teilmenge von A, deren Elemente nicht zu B gehören

$$A \setminus B = \{a \mid a \in A \wedge a \notin B\}. \tag{3.22}$$

Beide Mengen existieren aufgrund des Teilmengenaxioms. Aus dem gleichen Grunde existiert der Durchschnitt endlich vieler Mengen $A_1, \ldots, A_n$

$$\begin{aligned} A_1 \cap \ldots \cap A_n &= \{a \mid a \in A_1 \wedge \ldots \wedge a \in A_n\} \\ &= \{a \mid a \in A_1 \wedge (a \in A_1 \wedge \ldots \wedge a \in A_n\}. \end{aligned} \tag{3.23}$$

Vereinigungsmengenaxiom

M6 Sind A und B Mengen, dann gibt es eine Menge $A \cup B$, die *Vereinigung* von A und B, die aus allen Elementen besteht, die in A oder B liegen

$$A \cup B = \{a \mid a \in A \vee a \in B\}. \tag{3.24}$$

Die Vereinigung von endlich vielen Mengen $A_1, \ldots, A_n$ existiert ebenfalls

$$A_1 \cup \ldots \cup A_n = \{a \mid a \in A_1 \vee \ldots \vee a \in A_n\}. \tag{3.25}$$

Dies folgt aus dem Vereinigungsmengenaxiom und vollständiger Induktion nach n.

Potenzmengenaxiom

M7 Zu jeder Menge A existiert eine Menge $P(A)$, die *Potenzmenge* von A, die sich aus allen Teilmengen von A zusammensetzt

$$P(A) = \{B \mid B \subseteq A\}. \tag{3.26}$$

Für jede Menge A gilt $A \in P(A)$. Also ist jede Menge auch ein Element einer Menge. Folglich kann auf das Axiom M3 beim Aufbau der Mengenlehre verzichtet werden.

Bisher war lediglich garantiert, dass die leere Menge existiert. Mithilfe des Potenzmengenaxioms ergeben sich weitere Mengen

$$\begin{aligned} P(\emptyset) &= \{\emptyset\}, \\ P(P(\emptyset)) &= P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}, \\ P(P(P(\emptyset))) &= P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}. \end{aligned}$$

Mit dem Potenzmengenaxiom und Satz 3.10 folgt, dass es zu jeder natürlichen Zahl n eine Menge mit 2^n Elementen gibt. Mit dem Teilmengenaxiom und (3.5) lässt sich erschließen, dass zu jeder natürlichen Zahl m eine Menge mit m Elementen existiert.

Sind $A_1, \ldots, A_n$ Mengen, dann existiert eine Menge, die genau $A_1, \ldots, A_n$ als Elemente enthält. Denn mit der Menge $A = A_1 \cup \ldots \cup A_n$ existiert nach dem Potenzmengen- und Teilmengenaxiom auch die Menge

$$\{A_1, \ldots, A_n\} = \{B \mid B \in P(A) \wedge (B = A_1 \vee \ldots \vee B = A_n)\}. \tag{3.27}$$

Der Durchschnitt endlich vieler Mengen existiert nach dem Teilmengenaxiom. Allgemeiner existiert der Durchschnitt beliebig vieler Mengen. Der *Durchschnitt* eines Mengensystems $M \neq \emptyset$ ist die Menge

$$\bigcap M = \{a \mid \forall A[A \in M \Rightarrow a \in A]\}. \tag{3.28}$$

Diese Menge existiert aufgrund des Teilmengenaxioms, denn für jedes Element A_0 von M gilt

$$\bigcap M = \{a \mid a \in A_0 \wedge \forall A[A \in M \Rightarrow a \in A]\}. \tag{3.29}$$

Vereinigungsmengenaxiom

Nach Axiom M6 existiert die Vereinigung endlich vieler Mengen. Daraus kann nicht gefolgert werden, dass die Vereinigung beliebig vieler Mengen existiert.

M8 Ist M ein Mengensystem, dann gibt es eine Menge $\bigcup M$, die *Vereinigung* von M, die genau die Elemente enthält, die zu allen Elementen von M gehören

$$\bigcup M = \{a \mid \exists A[A \in M \wedge a \in A]\}. \tag{3.30}$$

Selbsttestaufgaben

3.1. Beschreibe formal die folgenden Mengen:

- Die Menge aller ganzzahligen Zweierpotenzen.
- Die Menge aller ganzen Zahlen, die zwischen 10 und 30 liegen, und nicht durch 3 oder 5 teilbar sind.
- Die Menge aller ungeraden ganzen Zahlen.

3.2. Welche der folgenden Mengen sind untereinander gleich?

$$\{w, x, y\}, \quad \{w, x, w\}, \quad \{x, x, w\}, \quad \{x, w, x, x, w, y\}.$$

3.3. Welche Teilmengenbeziehungen sind zwischen zwei Mengen A und B möglich? Veranschauliche alle Möglichkeiten anhand eines Venn-Diagramms.

3.4. Beweise den Satz 3.1.

3.5. Seien A, B und C nichtleere Mengen mit $A \subseteq B$, $B \subseteq C$ und $C \subseteq A$. Was kann daraus für die drei Mengen gefolgert werden?

3.6. Beweise den Satz 3.3.

3.7. Zeige, dass die Mengen $A \setminus B$ und B disjunkt sind und die Identität $A \cup B = (A \setminus B) \cup B$ gilt.

3.8. Ist die folgende Aussage wahr? Wenn sowohl A und B als auch B und C disjunkt sind, dann sind auch A und C disjunkt.

3.9. Beweise den Satz 3.8.

3.10. Zeige, dass für alle Teilmengen A und B einer Grundmenge G gilt

$$\overline{A \cap B} = \bar{A} \cup \bar{B} \quad \text{und} \quad \overline{A \cup B} = \bar{A} \cap \bar{B}.$$

3.11. Zeige, dass für jede Teilmenge A einer Grundmenge G gilt

- $\overline{\overline{A}} = A$.
- $A \cap \bar{A} = \emptyset$.
- $A \cup \bar{A} = G$.

3.12. Sei $M = \{\{1,2,3\},\{4,5\},\{6,7,8\}\}$. Welche der folgenden Aussagen sind wahr?

- $1 \in M$
- $\{1,2,3\} \subseteq M$
- $\{6,7,8\} \in M$
- $\{\{4,5\}\} \subseteq M$
- $\emptyset \notin M$
- $\emptyset \subseteq M$.

3.13. Bestimme die Potenzmenge von $A = \{\{1,2,3\},\{1,2\},\{4,5\}\}$.

3.14. Für jede Zahl $n \in \mathbb{N}$ sei $A_n = \{m \cdot n \mid m \in \mathbb{N}\}$. Berechne $\bigcup\{A_n \mid n \in \mathbb{N}\}$, $\bigcap\{A_n \mid n \in \mathbb{N}\}$ und $\bigcup\{A_n \mid p \text{ ist prim}\}$.

3.15. Sei $M = \{\{1,2\},\{2,3\},\{1,2,3,4\},\{2,4,5\},\{2,3\}\}$. Bestimme $\bigcup M$ und $\bigcap M$.

4

Relationen

Relationen beschreiben Beziehungen zwischen Elementen von Mengen. In diesem Kapitel wird die Darstellung und Verknüpfung von Relationen behandelt und der Bezug zu relationalen Datenbanken erläutert.

4.1 Das kartesische Produkt

Geordnete Paare

Das *geordnete Paar* oder kurz *Paar* zweier Objekte x und y ist eine Menge (x, y), die aus den Elementen $\{x\}$ und $\{x, y\}$ besteht

$$(x, y) = \{\{x\}, \{x, y\}\}. \tag{4.1}$$

In einem Paar kommt es im Gegensatz zu einer Menge auf die Reihenfolge der Elemente an.

Satz 4.1. *Für beliebige Paare (x, y) und (u, v) gilt $(x, y) = (u, v)$ genau dann, wenn $x = u$ und $y = v$.*

Beweis. Seien $x = u$ und $y = v$. Dann gilt $\{x\} = \{u\}$ und $\{x, y\} = \{u, v\}$, woraus sofort $(x, y) = (u, v)$ folgt.

Sei $(x, y) = (u, v)$. Es werden zwei Fälle unterschieden. Sei $x = y$ Dann ist (x, y) einelementig. Also ist auch (u, v) einelementig, d. h. $\{u\} = \{u, v\}$, woraus sich $u = v$ ergibt. Aus $\{\{x\}\} = \{\{u\}\}$ folgt $\{x\} = \{u\}$, also $x = u$. Somit ist $y = x = u = v$.

Sei $x \neq y$. Dann ist $\{x, y\}$ zweielementig, d. h., $\{x, y\} = \{u, v\}$ und $\{x\} = \{u\}$. Daraus folgt $x = u$, also $\{x, y\} = \{x, v\}$. Folglich ist $y = v$. □

Paarmengen

Seien A und B Mengen. Das *Produkt* oder die *Paarmenge* von A und B ist

$$A \times B = \{(x, y) \mid x \in A \wedge y \in B\}. \tag{4.2}$$

Beispiel 4.2. Für die Mengen $A = \{0, 1\}$ und $B = \{a, b, c\}$ gilt

$$A \times B = \{(0, a), (0, b), (0, c), (1, a), (1, b), (1, c)\}.$$

Die Paarmengenbildung ist monoton bzgl. mengentheoretischer Inklusion.

Satz 4.3. *Seien A, B, C und D Mengen. Aus $A \subseteq B$ und $C \subseteq D$ folgt $A \times C \subseteq B \times D$.*

n-Tupel

Ein *geordnete n-Tupel* oder kurz *n-Tupel* von Objekten $x_1, \ldots, x_n$ ist ein Paar, das aus dem $(n-1)$-Tupel $(x_1, \ldots, x_{n-1})$ und dem Element x_n besteht

$$(x_1, \ldots, x_{n-1}, x_n) = ((x_1, \ldots, x_{n-1}), x_n), \quad n \geq 3. \tag{4.3}$$

Das Element x_i wird *i-te Komponente* des n-Tupels genannt.

Satz 4.4. *Seien $(x_1, \ldots, x_n)$ und $(y_1, \ldots, y_n)$ n-Tupel. Es gilt $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ genau dann, wenn $x_i = y_i$ für alle $1 \leq i \leq n$.*

Beweis. Die Aussage wird per vollständiger Induktion nach n gezeigt. Für $n = 2$ ist die Aussage bereits nachgewiesen. Für $(n+1)$-Tupel $(x_1, \ldots, x_n, x_{n+1})$ und $(y_1, \ldots, y_n, y_{n+1})$ gilt

$$\begin{aligned}
&(x_1, \ldots, x_n, x_{n+1}) = (y_1, \ldots, y_n, y_{n+1}) \\
&\Leftrightarrow ((x_1, \ldots, x_n), x_{n+1}) = ((y_1, \ldots, y_n), y_{n+1}) \\
&\Leftrightarrow (x_1, \ldots, x_n) = (y_1, \ldots, y_n) \wedge x_{n+1} = y_{n+1} \quad \text{nach Satz 4.1} \\
&\Leftrightarrow x_1 = y_1 \wedge \ldots \wedge x_n = y_n \wedge x_{n+1} = y_{n+1} \quad \text{nach Induktionsannahme.}
\end{aligned}$$

□

Kartesische Produkte

Seien $A_1, \ldots, A_n$ Mengen. Das *kartesische Produkt* von $A_1, \ldots, A_n$ ist

$$A_1 \times \ldots \times A_n = \{(x_1, \ldots, x_n) \mid \forall i \in \underline{n}\, [x_i \in A_i]\}. \tag{4.4}$$

Bei lauter gleicher Mengen $A = A_1 = \ldots = A_n$ wird auch vom *n-fachen kartesischen Produkt* von A gesprochen

$$A^n = \underbrace{A \times \ldots \times A}_{n-\text{mal}}. \tag{4.5}$$

4.2 Der Relationsbegriff

Mit dem Begriff der Relation ist umgangssprachlich das "*in Beziehung stehen*" zwischen Objekten gemeint.

Homogene und inhomogene Relationen

Sei A eine Menge. Eine Teilmenge R von $A \times A$ heißt eine *(homogene) Relation* auf A. Für $(a, b) \in R$ wird kürzer aRb geschrieben. Beispiele für homogene Relationen sind das Senkrechtstehen auf der Menge aller Geraden einer Ebene, das Sichschneiden auf der Menge aller geometrischen Figuren, die Kongruenz auf der Menge aller Vielecke und die Verwandtschaft von Menschen.

Allgemeiner sind Beziehungen, die zwischen Elementen unterschiedlicher Mengen bestehen. Seien A und B Mengen. Eine Teilmenge R von $A \times B$ heißt eine *(heterogene) Relation* von A nach B. Beispiele für heterogene Relationen sind das Enthaltensein eines Punktes auf einer Geraden und die Zugehörigkeit eines Mitarbeiter zu einer Firma.

Spezielle Relationen

Die Paarmenge $R = A \times B$ wird *Allrelation* von A nach B genannt und die leere Menge $R = \emptyset$ *Nullrelation*. Die Allrelation besteht zwischen irgendzwei Elementen und die Nullrelation zwischen keinen Elementen. Wenn jedes Element einer Menge A nur zu sich selbst in Beziehung steht, dann liegt die *Gleichheitsrelation* auf A vor

$$I_A = \{(a, a) \mid a \in A\}. \tag{4.6}$$

Inverse Relation

Sei R eine Relation von A nach B. Die *inverse Relation* von R ist eine Relation R^{-1} von B nach A, die aus allen Elementen (b, a) besteht, für die $(a, b) \in R$ gilt

$$R^{-1} = \{(b, a) \mid aRb\}. \tag{4.7}$$

Beispielsweise gehört zur Relation "*ist früher als*" auf der Menge aller physikalischen Ereignisse die inverse Relation "*ist später als*".

Definitions- und Wertebereich

Der *Definitionsbereich* einer Relation R von A nach B besteht aus allen Elementen in A, die mit mindestens einem Element aus B in Beziehung stehen

$$\mathrm{dom}(R) = \{a \mid a \in A \wedge \exists b[b \in B \wedge aRb]\}. \tag{4.8}$$

Der *Wertebereich* einer Relation R von A nach B setzt sich aus allen Elementen in B zusammen, die mit mindestens einem Element aus A verknüpft sind

$$\mathrm{ran}(R) = \{b \mid b \in B \wedge \exists a[a \in A \wedge aRb]\}. \tag{4.9}$$

Urbild- und Bildmenge

Sei R eine Relation von A nach B und sei T eine Teilmenge von A. Die *Bildmenge* von T unter R ist die Menge $R(T)$ aller Elemente von B, die mit wenigstens einem Element in T verwoben sind

$$R(T) = \{b \mid b \in B \wedge \exists a[a \in T \wedge aRb]\}. \tag{4.10}$$

Ist T eine Teilmenge von B, dann gilt definitionsgemäß

$$\begin{aligned} R^{-1}(T) = &\{a \mid a \in A \wedge \exists b[b \in T \wedge bR^{-1}a]\} \\ &\{a \mid a \in A \wedge \exists b[b \in T \wedge aRb]\}. \end{aligned} \tag{4.11}$$

Die Menge $R^{-1}(T)$ heißt *Urbildmenge* von T unter R.

Beispiel 4.5. Für die Relation $R = \{(1,a),(1,b),(1,c),(2,a)\}$ von $A = \{1,2,3\}$ nach $B = \{a,b,c,d\}$ gilt $R^{-1} = \{(a,1),(b,1),(c,1),(a,2)\}$, $\mathrm{dom}(R) = \{1,2\}$, $\mathrm{ran}(R) = \{a,b,c\}$, $R(\{2\}) = \{a\}$ und $R^{-1}(\{a\}) = \{1,2\}$.

4.3 Darstellung von Relationen

Relationen werden bildhaft durch Pfeildiagramme und formal mithilfe von Matrizen dargestellt.

Pfeildiagramme

Sei R eine Relation von A nach B. In einem *Pfeildiagramm* von R werden die Elemente von A und B durch Punkte der Zeichenebene und die Relationsbeziehungen durch stetige, gerichtete Streckenzüge dargestellt. Etwa wird die Relation $R = \{(1,b),(1,c),(3,b),(4,a),(4,c)\}$ von $A = \{1,2,3,4\}$ nach $B = \{a,b,c,d\}$ durch das Pfeildiagramm in Abb. 4.1 veranschaulicht.

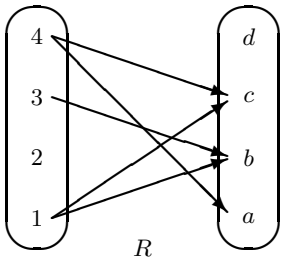

Abb. 4.1. Pfeildiagramm einer Relation R.

Adjazenzmatrizen

Sei R eine Relation von $A = \{a_1, \ldots, a_m\}$ nach $B = \{b_1, \ldots, b_n\}$. Die *Adjazenzmatrix* von R ist eine $m \times n$-Matrix $M_R = (m_{ij})$ mit

$$m_{ij} = \begin{cases} 1 \text{ falls } a_i R b_j, \\ 0 \text{ sonst.} \end{cases} \tag{4.12}$$

Beispielsweise gehört zur obigen Relation R die Adjazenzmatrix

$$M_R = \begin{pmatrix} 0\,1\,1\,0 \\ 0\,0\,0\,0 \\ 0\,1\,0\,0 \\ 1\,0\,1\,0 \end{pmatrix}, \tag{4.13}$$

wobei die Zeilen bzw. Spalten der Reihe nach mit den Elementen $1, 2, 3, 4$ bzw. a, b, c, d markiert sind.

Die Adjazenzmatrix der inversen Relation von R ist die *Transponierte* der Adjazenzmatrix $M_R = (m_{ij})$ von R, also

$$M_{R^{-1}} = (M_R)^T = (m_{ji}). \tag{4.14}$$

4.4 Komposition

Die Komposition ist die gebräuchlichste Operation, um Relationen zu verknüpfen. Sei R eine Relation von A nach B und S eine Relation von B nach C. Die *Komposition* (oder das *relative Produkt*) von R und S ist definiert durch

$$R \circ S = \{(a, c) \mid (a, c) \in A \times C \wedge \exists b[b \in B \wedge aRb \wedge bSc]\}. \tag{4.15}$$

Die Komposition $R \circ S$ besteht zwischen Elementen $a \in A$ und $c \in C$ genau dann, wenn es ein Element $b \in B$ gibt, so dass zugleich die Beziehungen aRb und bSc bestehen.

Beispiel 4.6. Die Komposition der Relationen

$$R = \{(1, c), (2, a), (2, b), (3, c)\} \quad \text{und} \quad S = \{(a, \alpha), (a, \beta), (b, \gamma), (c, \beta)\}$$

ergibt die Relation

$$R \circ S = \{(1, \beta), (2, \alpha), (2, \beta), (2, \gamma), (3, \beta)\}.$$

Die Komposition kann anhand eines Pfeildiagramms berechnet werden, in dem jeweils hintereinander gesetzte Pfeile durchgeschaltet werden (Abb. 4.2).

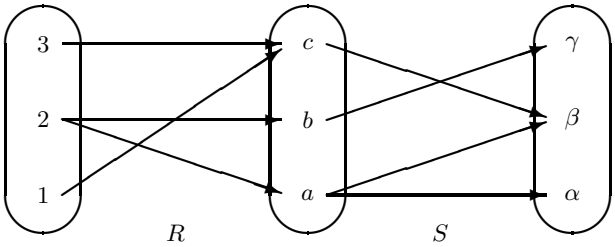

Abb. 4.2. Pfeildiagramm der Relationen R und S.

Satz 4.7. *Für beliebige Relationen $R \subseteq A \times B$, $S \subseteq B \times C$ und $T \subseteq C \times D$ gilt*

- $(R^{-1})^{-1} = R$.
- $(R \circ S) \circ T = R \circ (S \circ T)$.
- $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.
- $I_A \circ R = R = R \circ I_B$.

Beweis. Seien $a \in A$ und $b \in B$. Die Aussage $a(R^{-1})^{-1}b$ ist gleichwertig zu $bR^{-1}a$, die wiederum äquivalent ist zu aRb.

Seien $a \in A$ und $d \in D$. Aus $a((R \circ S) \circ T)d$ folgt die Existenz von $c \in C$, so dass $a(R \circ S)c$ und cTd. Daraus ergibt sich aRb, bSc und cTd für ein $b \in B$. Dies impliziert aRb und $b(S \circ T)d$, was $a(R \circ (S \circ T))d$ zur Folge hat. Diese Beweiskette ist umkehrbar.

Seien $a \in A$ und $c \in C$. Aus $a(R \circ S)c$ folgt aRb und bSc für ein $b \in B$. Per definitionem ergibt sich $bR^{-1}a$ und $cS^{-1}b$, was $c(S^{-1} \circ R^{-1})a$ impliziert. Diese Beweiskette ist umkehrbar.

Seien $a \in A$ und $b \in B$. Die Aussage $a(I_A \circ R)b$ ist gleichbedeutend mit aI_Aa und aRb. Weil aI_Aa wahr ist, ist letztere Aussage äquivalent zu aRb. Die zweite Identität ergibt sich analog. □

Die Komposition von Relationen ist monoton bzgl. mengentheoretischer Inklusion.

Satz 4.8. *Seien P und Q Relationen von A nach B sowie R und S Relationen von B nach C. Aus $P \subseteq Q$ und $R \subseteq S$ folgt $P \circ R \subseteq Q \circ S$.*

4.5 Relationale Datenbanken

Bei relationalen Datenbanken treten typischerweise mehrstellige Beziehungen auf. Wir betrachten eine relatione Datenbank mit der Relation (Tabelle) 'Mitarbeiter'

Nachname	Vorname	Geburtsdatum	Projekt
Huber	Anna	31.12.67	EDV
Schmidt	Gerd	22.11.77	Marketing
Müller	Fritz	11.01.82	Business
Meier	Berta	07.07.72	EDV

und der Relation 'Projekte'

Projekt	Ort	Kosten
Business	Hamburg	200.000,00
EDV	Köln	1.000.000,00
Marketing	Nürnberg	100.000,00

Aus einer relationalen Datenbank können Daten mithilfe einer geeigneten Abfragesprache, wie etwa der Sprache SQL (Structured Query Language), herausgesucht werden.

Selektion

Mit der Selektion werden Datensätze in einer Tabelle ausgewählt, die einer bestimmten Bedingung genügen. Beispielsweise liefert die SQL-Anweisung

```
SELECT * FROM Mitarbeiter WHERE Projekt = 'EDV'
```

alle Zeilen von 'Mitarbeiter', die der Bedingung, Projekt = 'EDV', genügen

Nachname	Vorname	Geburtsdatum	Projekt
Huber	Anna	31.12.67	EDV
Meier	Berta	07.07.72	EDV

Projektion

Mit der Projektion werden Spalten einer Tabelle ausgewählt. Beispielsweise liefert die SQL-Anweisung

```
SELECT Nachname, Vorname FROM Mitarbeiter
```

die Tabelle

Nachname	Vorname
Huber	Anna
Schmidt	Gerd
Müller	Fritz
Meier	Berta

Verbund

Mit dem (natürlichen) Verbund werden Datensätze aus mehreren Tabellen verknüpft, sofern ein gemeinsames Feld vorliegt, das jeweils gleiche Werte enthält. Beispielsweise vergleicht die SQL-Anweisung

```
SELECT * FROM Mitarbeiter JOIN Projekte ON
       Mitarbeiter.Projekt = Projekte.Projekt
```

auf übereinstimmende Projektbezeichungen und liefert die Tabelle

Nachname	Vorname	Geburtsdatum	Projekt	Ort	Kosten
Huber	Anna	31.12.67	EDV	Köln	1.000.000,00
Schmidt	Gerd	22.11.77	Marketing	Nürnberg	100.000,00
Müller	Fritz	11.01.82	Business	Hamburg	200.000,00
Meier	Berta	07.07.72	EDV	Köln	1.000.000,00

Gleichlautende Spalten werden nur einmal angegeben.

Selbsttestaufgaben

4.1. Zeige, dass die Festlegung des geordneten Paares (x, y) vom axiomatischen Aufbau der Mengenlehre getragen wird.

4.2. Berechne das kartesische Produkt $A \times B \times C$ der Mengen $A = \{1, 2\}$, $B = \{a, b, c\}$ und $C = \{1, 3\}$.

4.3. Beweise den Satz 4.3.

4.4. Seien A, B und C Mengen. Beweise $(A \times B) \cap (A \times C) = A \times (B \cap C)$ und $(A \times B) \cup (A \times C) = A \times (B \cup C)$.

4.5. Wie viele Relationen von $A = \{a, b, c\}$ nach $B = \{1, 2\}$ gibt es?

4.6. Bestimme die zu $R = \{(a, 1), (a, 2), (b, 2)\}$ inverse Relation.

4.7. Sei $R = \{(1, y), (1, z), (3, z), (4, x), (4, z)\}$ eine Relation von $\{1, 2, 3, 4\}$ nach $\{x, y, z\}$. Ermittle $\mathrm{dom}(R)$ und $\mathrm{ran}(R)$.

4.8. Bestimme alle Paare der Relation $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x + 3y = 13\}$.

4.9. Gegeben sei die Relation Sei $R = \{(1, a), (1, b), (3, b), (3, d), (4, b)\}$ eine Relation von $\{1, 2, 3, 4\}$ nach $\{a, b, c, d\}$. Berechne $R(\{1, 3\})$ und $R^{-1}(\{b\})$.

4.10. Betrachte die folgenden sieben Relationen zwischen Menschen, dass ein Mensch Vater, Mutter, Kind, Bruder, Schwester, Ehemann, Ehefrau eines anderen ist. Wir bezeichnen diese Relationen der Reihe nach mit V, M, K, B, S, E und F. Drücke die Relationen Elternteil, Tante, Geschwister, Schwiegermutter und Cousin oder Cousine zu sein anhand obiger Relationen mithilfe des relativen Produkts und mengentheoretischer Operationen aus.

4.11. Sei $R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\}$ eine Relation von $A = \{1, 2, 3, 4\}$ nach $B = \{a, b, c, d\}$ und $S = \{(b, x), (b, z), (c, y), (d, z)\}$ eine Relation von B nach $C = \{x, y, z\}$. Stelle beide Relationen durch Pfeildiagramme und Adjazenzmatrizen dar und berechne $R \circ S$.

4.12. Beweise den Satz 4.8.

4.13. (Schrödersche Äquivalenz) Zeige, dass für Relationen R, S und T Relationen auf A gilt

$$R \circ S \subseteq T \iff R^{-1} \circ \bar{T} \subseteq \bar{S}.$$

5

Homogene Relationen

In diesem Kapitel wird die Darstellung homogener Relationen durch Digraphen behandelt und die wichtigsten homogenen Relationen, Äquivalenzen und Ordnungen, werden untersucht.

5.1 Darstellung von homogenen Relationen

Digraphen

Sei V eine endliche Menge und E eine Relation auf V. Das Paar $D = (V, E)$ heißt ein *Digraph* (oder *gerichteter Graph*). Die Elemente von V heißen *Knoten* und die Elemente von E *Kanten*. Ein *Diagramm* eines Digraphen D ist eine zeichnerische Darstellung von D, in der die Knoten durch Punkte und die Kanten durch stetige, gerichtete Streckenzüge dargestellt werden.

Beispiel 5.1. Der Digraph $D = (V, E)$ mit der Knotenmenge $V = \{a, b, c, d\}$ und der Kantenmenge $E = \{(a, b), (b, c), (c, d), (d, b)\}$ wird durch das Diagramm in Abb. 5.1 repräsentiert.

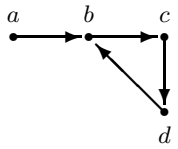

Abb. 5.1. Diagramm eines Digraphen.

Eine Kante $e = (u, v) \in E$ heißt *inzident* mit ihren Knoten u und v, die Knoten u und v werden dann auch *adjazent* genannt, u heißt dann *Startknoten* und v *Endknoten* von e. Eine Kante mit gleichem Start- und Endknoten wird als *Schlinge* bezeichnet.

Wege und Kreise

Sei $D = (V, E)$ ein Digraph. Ein *gerichteter Weg* der Länge n in D ist ein $(n+1)$-Tupel $W = (v_0, \ldots, v_n)$, so dass jedes Paar aufeinanderfolgender Knoten (v_i, v_{i+1}) eine Kante in D repräsentiert. Der Knoten v_0 heißt *Startknoten* und der Knoten v_n *Endknoten* von W. Ein gerichteter Weg W in D heißt *einfach*, wenn jeder Knoten höchstens einmal vorkommt.

Ein *gerichteter Kreis* in D ist ein Weg in D, der denselben Start- und Endknoten besitzt. Ein gerichteter Kreis $K = (v_0, \ldots, v_{n-1}, v_n)$ in D heißt *einfach*, wenn K die Länge $n \geq 2$ hat und der Weg $(v_0, \ldots, v_{n-1})$ in D einfach ist. Ein einfacher Kreis enthält also jeden Knoten in D (bis auf Start- und Endknoten) höchstens einmal.

Beispiel 5.2. Der Digraph in Abb. 5.1 enthält folgende gerichtete Wege der Länge drei: (a, b, c, d), (b, c, d, b), (c, d, b, c) und (d, b, c, d), wobei der erste Weg einfach ist und die anderen drei Wege einfache Kreise darstellen.

5.2 Äquivalenzen

Äquivalenzen sind homogene Relationen, die Beziehungen zwischen gleichartigen Objekten beschreiben.

Begriff der Äquivalenz

Sei A eine Menge. Eine *Äquivalenz* auf A ist eine Relation $\equiv$ auf A mit folgenden Eigenschaften:

- *Reflexivität*: $\forall x[x \in A \Rightarrow x \equiv x]$.
- *Transitivität*: $\forall x \forall y \forall z[x, y, z \in A \Rightarrow (x \equiv y \wedge y \equiv z \Rightarrow x \equiv z)]$.
- *Symmetrie*: $\forall x \forall y[x, y \in A \Rightarrow (x \equiv y \Rightarrow y \equiv x)]$.

Beispiele 5.3. Die Relation $\{(a, b), (a, c)\}$ ist transitiv, während die Relation $\{(a, b), (b, c)\}$ aufgrund des fehlenden Paares (a, c) nicht transitiv ist. Alle Äquivalenzen auf der Menge $A = \{a, b, c\}$ sind

$$
\begin{aligned}
R_0 &= \{(a, a), (b, b), (c, c)\} \\
R_1 &= \{(a, a), (b, b), (b, c), (c, b), (c, c)\} \\
R_2 &= \{(a, a), (a, b), (b, a), (b, b), (c, c)\} \\
R_3 &= \{(a, a), (a, c), (b, b), (c, a), (c, c)\} \\
R_4 &= \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}.
\end{aligned}
$$

Äquivalenzen als Partitionen

Sei $\equiv$ eine Äquivalenz auf A und $a \in A$. Die *Äquivalenzklasse* von a (bzgl. $\equiv$) ist eine Menge $\overline{a}$, die aus allen Elementen von A besteht, die mit a in Beziehung stehen

$$\overline{a} = \{b \mid b \in A \wedge a \equiv b\}. \tag{5.1}$$

Die *Quotientenmenge* von $\equiv$ ist die Menge $\overline{A}$ aller Äquivalenzklassen bzgl. $\equiv$

$$\overline{A} = \{\overline{a} \mid a \in A\}. \tag{5.2}$$

Beispiele 5.4. • Zu den obigen Äquivalenzen auf $A = \{a, b, c\}$ lauten die Äquivalenzklassen

$$\begin{array}{llll} R_0: & \overline{a} = \{a\}, & \overline{b} = \{b\}, & \overline{c} = \{c\} \\ R_1: & \overline{a} = \{a\}, & \overline{b} = \{b, c\}, & \overline{c} = \{b, c\} \\ R_2: & \overline{a} = \{a, b\}, & \overline{b} = \{a, b\}, & \overline{c} = \{c\} \\ R_3: & \overline{a} = \{a, c\}, & \overline{b} = \{b\}, & \overline{c} = \{a, c\} \\ R_4: & \overline{a} = \{a, b, c\}, & \overline{b} = \{a, b, c\}, & \overline{c} = \{a, b, c\} \end{array}$$

und die Quotientenmengen

$$\begin{array}{ll} R_0: & \overline{A} = \{\{a\}, \{b\}, \{c\}\} \\ R_1: & \overline{A} = \{\{a\}, \{b, c\}\} \\ R_2: & \overline{A} = \{\{a, b\}, \{c\}\} \\ R_3: & \overline{A} = \{\{a, c\}, \{b\}\} \\ R_4: & \overline{A} = \{\{a, b, c\}\}. \end{array}$$

- Sei $A = \{\text{giorno}, \text{domani}, \text{sabato}, \text{notte}, \text{sera}, \text{tempo}\}$. Die Relation "*hat dieselbe Anzahl von Buchstaben wie*" ist eine Äquivalenz auf A mit der Quotientenmenge

$$\overline{A} = \{\{\text{sera}\},\ \{\text{tempo}, \text{notte}\},\ \{\text{giorno}, \text{domani}, \text{sabato}\}\}.$$

Satz 5.5. *Ist $\equiv$ eine Äquivalenz auf A, dann ist die Quotientenmenge $\overline{A}$ eine Partition von A.*

Beweis. Für jedes $a \in A$ gilt $a \equiv a$, weil $\equiv$ reflexiv ist. Also ist $a \in \overline{a}$. Somit sind die Äquivalenzklassen nichtleer.

Ferner ist $\bigcup \overline{a} = A$. Denn einerseits ist jede Äquivalenzklasse $\overline{a}$ eine Teilmenge von A und andererseits liegt jedes $a \in A$ in der Äquivalenzklasse $\overline{a}$.

Schließlich seien $a, b \in A$ mit $c \in \overline{a} \cap \overline{b}$, d. h., $a \equiv c$ und $b \equiv c$. Da $\equiv$ symmetrisch ist, folgt $c \equiv b$. Weil $\equiv$ transitiv ist, ergibt sich $a \equiv b$. Sei $d \in \overline{b}$, d. h., $b \equiv d$. Da $\equiv$ transitiv ist, folgt $a \equiv d$ und somit $d \in \overline{a}$. Mithin ist $\overline{b} \subseteq \overline{a}$. Analog erhellt sich $\overline{a} \subseteq \overline{b}$, was $\overline{a} = \overline{b}$ impliziert. Folglich sind zwei Äquivalenzklassen entweder gleich oder disjunkt. Damit ist gezeigt, dass die Quotientenmenge $\overline{A}$ eine Partition von A ist. □

Partitionen als Äquivalenzen

Umgekehrt wird gezeigt, dass jede Partition einer Menge A eine Äquivalenz auf A induziert.

Satz 5.6. *Sei P eine Partition von A. Die Relation*

$$R = \{(a, b) \mid a, b \in A \wedge \exists T[T \in P \wedge a, b \in T]\}$$

ist eine Äquivalenz auf A, deren Quotientenmenge $\overline{A}$ mit P übereinstimmt.

Beweis. Zuerst wird gezeigt, dass R eine Äquivalenz auf A ist. Die Relation R ist definitionsgemäß symmetrisch. Sei $a \in A$. Da P eine Partition ist, gibt es ein Element $T \in P$ mit $a \in T$. Aus der Definition von R folgt aRa. Also ist R reflexiv. Seien $a, b, c \in A$ mit aRb und bRc. Dann gibt es per definitionem Elemente T und T' von P mit $a, b \in T$ und $b, c \in T'$. Also ist $b \in T \cap T'$. Weil aber P eine Partition ist, müssen T und T' identisch sein, was definitionsgemäß aRc zur Folge hat. Somit ist R transitiv.

Sei $a \in A$. Da P eine Partition von A ist, gibt es ein $T \in P$ mit $a \in T$. Wir zeigen, dass $\overline{a} = T$. Für jedes $b \in T$ gilt per Definition aRb, woraus $T \subseteq \overline{a}$ folgt. Umgekehrt sei $b \in \overline{a}$. Wegen $a \in \overline{a}$ ist aRb und demzufolge $b \in T$, mithin $\overline{a} \subseteq T$, zusammen also $\overline{a} = T$. □

Sei $\equiv$ eine Äquivalenz auf A. Ein *Vertetersystem* von $\equiv$ ist eine Teilmenge von A, die aus jeder Äquivalenzklasse bzgl. $\equiv$ genau ein Element enthält.

Beispiel 5.7. Für die obigen Äquivalenzen auf $\{a, b, c\}$ lauten die Vertretersysteme

$R_0 : \{a, b, c\}$
$R_1 : \{a, b\}$ und $\{a, c\}$
$R_2 : \{a, c\}$ und $\{b, c\}$
$R_3 : \{a, b\}$ und $\{b, c\}$
$R_4 : \{a\}$ und $\{b\}$ und $\{c\}$.

Konstruktive Wissenschaftstheorie

Die konstruktive Wissenschaftstheorie ist ein Gebiet der Philosophie, das sich mit der schrittweise gerechtfertigten Wissenschafts- und Sprachkonstruktion beschäftigt. In der konstruktiven Wissenschaftstheorie wird ein Begriff dadurch definiert, indem in einem Abstraktionsschritt in Beziehung stehende Elemente einer Menge zu Äquivalenzklassen zusammengefasst und dadurch in einer bestimmten Weise als gleich angesehen werden. Beispielsweise führt die Parallelität von Geraden zum Begriff "*Richtung*", die Kongruenz von Strecken zu "*Länge*", die Gleichmächtigkeit von Mengen zu "*Kardinalzahl*" die Gleichaltrigkeit von Menschen zu "*Alter*" und die Synonymie von Wörtern zu "*Bedeutung*".

5.3 Ordnungen

Ordnungsrelationen beschreiben hierarchische Beziehungen zwischen den Objekten einer Menge.

Begriff der Ordnung

Sei A eine Menge. Eine *Halbordnung* auf A ist eine Relation $\preceq$ auf A mit folgenden Eigenschaften:

- *Reflexivität*: $\forall x[x \in A \Rightarrow x \preceq x]$.
- *Transitivität*: $\forall x \forall y \forall z[x, y, z \in A \Rightarrow (x \preceq y \wedge y \preceq z \Rightarrow x \preceq z)]$.
- *Antisymmetrie*: $\forall x \forall y[x, y \in A \Rightarrow (x \preceq y \wedge y \preceq x \Rightarrow x = y)]$.

Ist $\preceq$ eine Halbordnung auf A, dann wird das Paar $(A, \preceq)$ eine *halbgeordnete Menge* genannt.

Beispiele 5.8.
- Die Inklusion ist nach Satz 3.3 eine Halbordnung auf der Potenzmenge einer Menge.
- Seien $m, n \in \mathbb{N}_0$. Wir sagen, m ist *kleiner gleich* n, kurz $m \leq n$, wenn es ein $l \in \mathbb{N}_0$ gibt mit $m + l = n$. Wir sagen, m *teilt* n, kurz $m \mid n$, wenn es ein $l \in \mathbb{N}_0$ gibt mit $m \cdot l = n$. Beide Relationen sind Halbordnungen auf $\mathbb{N}_0$.

Satz 5.9. *Der Digraph $D = (A, \preceq)$ einer Halbordnung $\preceq$ auf A enthält keine einfachen gerichteten Kreise.*

Beweis. Angenommen, der Digraph D enthielte einen einfachen gerichteten Kreis $K = (v_0, v_1, \ldots, v_n)$ der Länge $n \geq 2$. Dann gibt es in K neben v_0 noch ein weiterer Knoten v. Also existiert einen gerichteten Weg von v_0 nach v und einen gerichteten Weg von v nach $v_n = v_0$. Da $\preceq$ transitiv ist, erhellt sich $v_0 \preceq v$ und $v \preceq v_0$ Weil aber $\preceq$ antisymmetrisch ist, folgt widersprüchlicherweise $v = v_0$. □

Hasse-Diagramm

Ein *Hasse-Diagramm* einer halbgeordneten Menge $(A, \preceq)$ ist ein Diagramm, in dem alle Kanten nach oben gerichtet sind. Aufgrund dieser Vereinbarung können Pfeile weggelassen werden. Ferner wird eine Kante (a, b) weggelassen, wenn es einen Weg der Länge ≥ 2 von a nach b gibt. D.h., eine Kante (a, b) im Hasse-Diagramm erfüllt die Bedingung

$$a \preceq b \text{ und es gibt kein weiteres Element } c \in A \text{ mit } a \preceq c \preceq b. \qquad (5.3)$$

In Hasse-Diagrammen werden transitive Beziehungen also durch gerichtete Wege dargestellt (Abb. 5.2).

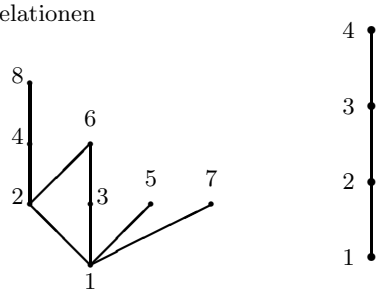

Abb. 5.2. Hasse-Diagramme der halbgeordneten Mengen $(\underline{8}, |)$ und $(\underline{4}, \leq)$.

Lineare Ordnungen

Eine *lineare Ordnung* auf A ist eine Halbordnung $\preceq$ auf A, in der für je zwei Elemente $a, b \in A$ wenigstens eine der Beziehungen $a \preceq b$ oder $b \preceq a$ gilt. Ist $\preceq$ eine lineare Ordnung auf A, dann wird das Paar $(A, \preceq)$ eine *linear geordnete Menge* oder *Kette* genannt.

Beispiele 5.10.
- Die halbgeordnete Menge $(\mathbb{N}_0, \leq)$ ist linear geordnet. Der Beweis fußt auf der Arithmetik der natürlichen Zahlen (Abs. 7.2).
- Die halbgeordnete Menge $(\mathbb{N}_0, |)$ ist nicht linear geordnet, weil etwa weder $2 \mid 3$ noch $3 \mid 2$ gilt.
- Die halbgeordnete Menge $(P(A), \subseteq)$ ist nur dann linear geordnet, wenn A höchstens einelementig ist.
- Die lexikografische Ordnung auf der Menge der Wörter des lateinischen Alphabets ist linear, sie erleichtert das Suchen nach Einträgen in Lexika.

Spezielle Elemente in Halbordnungen

Sei $(A, \preceq)$ eine halbgeordnete Menge. Ein Element $a \in A$ heißt *minimal*, wenn für jedes $b \in A$ aus $b \preceq a$ sofort $a = b$ folgt. Entsprechend heißt $a \in A$ *maximal*, wenn für jedes $b \in A$ aus $a \preceq b$ direkt $a = b$ folgt.

Ein Element $a \in A$ heißt *kleinstes Element*, wenn für jedes $b \in A$ gilt $a \preceq b$. Analog heißt $a \in A$ *größtes Element*, wenn für jedes $b \in A$ gilt $b \preceq a$.

Beispiele 5.11. Die halbgeordnete Menge $(\mathbb{N}_0, \leq)$ hat 0 als kleinstes Element, aber kein maximales Element. Die halbgeordnete Menge $(\mathbb{N}_0, |)$ hat 1 als kleinstes und 0 als größtes Element. Die halbgeordnete Menge $(\underline{8}, |)$ hat 1 als kleinstes Element und 5, 6, 7 und 8 als maximale Elemente (Abb. 5.2). Die halbgeordnete Menge $(P(\{a, b\}), \subseteq)$ hat $\emptyset$ als kleinstes und $\{a, b\}$ als größtes Element.

Lemma 5.12. *Jede endliche halbgeordnete Menge besitzt wenigstens ein minimales und ein maximales Element.*

Beweis. Sei $(A, \preceq)$ eine endliche halbgeordnete Menge und sei $a_0 \in A$. Beginnend mit a_0 wird eine echt absteigende Kette von Elementen aus A konstruiert: $\ldots \prec a_2 \prec a_1 \prec a_0$. Diese Kette muss abbrechen, weil A endlich ist. Ist $a_n \prec \ldots \prec a_1 \prec a_0$ die konstruierte Kette, dann ist a_n minimal. Die Existenz eines maximalen Elements wird anhand einer echt aufsteigenden Kette gezeigt. □

Lemma 5.13. *Sei $(A, \preceq)$ eine halbgeordnete Menge. Jedes kleinste bzw. größte Element $a \in A$ ist auch minimales bzw. maximales Element. Das kleinste bzw. größte Element $a \in A$ ist eindeutig bestimmt, falls es existiert.*

Beweis. Die erste Aussage folgt aus den Definitionen. Seien $a, b \in A$ kleinste Elemente. Dann folgt per definitionem $a \preceq b$ und $b \preceq a$. Mit der Antisymmetrie ergibt sich $a = b$. □

5.4 Hüllen

Sei R eine Relation auf A. Die *reflexive (symmetrische, transitive) Hülle* von R ist eine Relation R' auf A mit den folgenden Eigenschaften:

- R' ist reflexiv (symmetrisch, transitiv).
- $R \subseteq R'$.
- Ist R'' eine reflexive (symmetrische, transitive) Relation auf A mit $R \subseteq R''$, dann ist $R' \subseteq R''$.

Wir schreiben $\rho(R)$ für die reflexive Hülle, $\sigma(R)$ für die symmetrische Hülle, R^+ für die transitive Hülle und R^* für die reflexive, transitive Hülle.

Beispiel 5.14. Die Relation "*ist Elternteil von*" ist nicht transitiv. Ihre transitive Hülle ist die Relation "*ist Ahne von*".

Die transitive Hülle einer Relation R wird anhand der Potenzen von R konstruiert (Abs. 7.2).

Satz 5.15. *Ist R eine Relation auf A, dann gilt*

- $\rho(R) = R \cup I_A$.
- $\sigma(R) = R \cup R^{-1}$.
- $R^+ = \bigcup_{n \geq 1} R^n$.
- $R^* = \bigcup_{n \geq 0} R^n$.

Beweis. Wir zeigen nur die dritte Aussage. Sei $R' = \bigcup_{n \geq 1} R^n$. Zuerst wird gezeigt, dass R' transitiv ist. Seien $a, b, c \in A$ mit $aR'b$ und $bR'c$. Dann gibt es natürliche Zahlen m und n mit $aR^m b$ und $bR^n c$. Also folgt $aR^{m+n}c$ und somit $aR'c$.

Es gilt $R = R^1$ und somit $R \subseteq R'$.

Sei R'' eine transitive Relation auf A, die R enthält. Wir zeigen, dass $R' \subseteq R''$. Seien $a, b \in A$ mit $aR'b$. Dann existiert eine natürliche Zahl n mit $aR^n b$. Folglich gibt es Elemente $a_1, \ldots, a_{n-1}$ von A mit aRa_1, a_iRa_{i+1} für $1 \leq i \leq n-2$, und $a_{n-1}Rb$. Da R in R'' enthalten ist, erhellt sich $aR''a_1$, $a_iR''a_{i+1}$ für $1 \leq i \leq n-2$, und $a_{n-1}R''b$. Weil aber R'' transitiv ist, folgt $aR''b$. □

Selbsttestaufgaben

5.1. Wir betrachten Relationen $R = \{(1,1),(2,2),(3,3)\}$, $S = \{(1,2),(2,1),(3,3)\}$ und $T = \{(1,2),(2,3),(1,3)\}$ auf $\{1,2,3\}$. Welche dieser Relationen sind reflexiv, transitiv, symmetrisch oder antisymmetrisch?

5.2. Zeige, dass die Relation $R = \{(a,b) \mid a,b \in \mathbb{N}_0 \wedge (a+b \text{ ist gerade})\}$ eine Äquivalenz auf $\mathbb{N}_0$ ist. Wie lautet die Quotientenmenge?

5.3. Gegeben sei die Wortmenge $W = \{\text{auto}, \text{iso}, \text{mori}, \text{motto}, \text{omni}, \text{otto}\}$. Bestimme die Quotientenmenge von W bzgl. der Äquivalenzen "*hat dieselbe Anzahl von Buchstaben wie*" und "*beginnt mit dem gleichen Buchstaben wie*".

5.4. Zeige, dass die Relation $R = \{(a,b) \mid a,b \in \mathbb{Z} \wedge (a^2 - b^2 \text{ ist teilbar durch } 3)\}$ eine Äquivalenz auf $\mathbb{Z}$ ist. Bestimme die zugehörige Quotientenmenge.

5.5. Welche der folgenden Relationen sind Ketten: $(\{3,12,36\},|)$, $(\{7,21,15\},|)$, $(\{9\},|)$, $(\{2,16,64,14\},|)$.

5.6. Seien $(A_1,\preceq_1)$ und $(A_2,\preceq_2)$ halbgeordnete Mengen. Wir definieren eine Relation $\preceq$ auf $A_1 \times A_2$ durch

$$(x_1,x_2) \preceq (y_1,y_2) \quad :\Longleftrightarrow \quad x_1 \preceq_1 y_1 \wedge x_2 \preceq y_2,$$

Zeige, dass $\preceq$ eine Halbordnung ist. Diese Halbordnung wird *Produktordnung* auf $A_1 \times A_2$ genannt.

5.7. Zeichne das Hasse-Diagramm der unter Teilbarkeit halbgeordneten Menge $\{1,2,3,4,6,8,9,12,18,24\}$ und bestimme alle minimalen und maximalen Elemente. Gibt es ein kleinstes oder größtes Element?

5.8. Berechne die transitive Hülle der Relation $R = \{(1,2),(2,4),(3,2),(3,4),(4,1)\}$ auf $\{1,2,3,4\}$.

5.9. Vervollständige den Beweis von Satz 5.15.

5.10. Zeige, dass eine reflexive (symmetrische, transitive) Relation identisch ist mit ihrer reflexiven (symmetrischen, transitiven) Hülle.

5.11. Seien R und S homogene Relationen auf A. Zeige:

- $(R^*)^{-1} = (R^{-1})^*$,
- $(R \cup S)^* = (R^*S)^*R^*$,
- $R^*S^* \subseteq (R \cup S)^*$.

6

Abbildungen

Abbildungen treten in allen mathematischen Theorien auf. Wir untersuchen die grundlegenden Eigenschaften von Abbildungen, stellen injektive, surjektive und bijektive Abbildungen vor und behandeln spezielle Abbildungen wie Permutationen, Familien, Folgen und Multimengen. Abschließend wird mithilfe von Folgen das Laufzeitverhalten von Algorithmen analysiert.

6.1 Der Abbildungsbegriff

Seien A und B Mengen. Eine Relation f von A nach B heißt eine *Abbildung* (oder *Funktion* oder *Operation*), wenn f linkstotal und rechtseindeutig ist. Eine Relation f von A nach B heißt *linkstotal*, wenn es zu jedem $a \in A$ ein $b \in B$ mit afb gibt, also $\mathrm{dom}(f) = A$. Eine Relation f von A nach B heißt *rechtseindeutig*, wenn für alle $a \in A$ und $b_1, b_2 \in B$ aus afb_1 und afb_2 stets $b_1 = b_2$ folgt. Eine Abbildung f von A nach B wird mit $f : A \to B$ bezeichnet, A ist die *Quellmenge* und B die *Zielmenge* von f. In einer Abbildung f gibt es zu jedem $a \in A$ *genau* (mindestens und höchstens) ein $b \in B$ mit afb; mindestens wegen Linkstotalität und höchstens wegen Rechtseindeutigkeit (Abb. 6.1). Deshalb wird die Beziehung afb auch als *Abbildungsvorschrift* geschrieben

$$b = f(a) \quad \text{oder} \quad f : a \mapsto b. \tag{6.1}$$

Beispiele 6.1. • Die *identische Abbildung* $id_A : A \to A$, definiert durch $id_A(a) = a$ für alle $a \in A$, ist der Gleichheitsrelation auf A.

- Eine *konstante Abbildung* $f : A \to B$ ordnet jedem Element von A ein festes Element b_0 von B zu, d. h. $f(a) = b_0$ für alle $a \in A$.
- Sei A eine Teilmenge einer Menge B. Die Abbildung $\iota : A \to B$, definiert durch $\iota(a) = a$ für alle $a \in A$, wird *Inklusionsabbildung* von A nach B genannt.

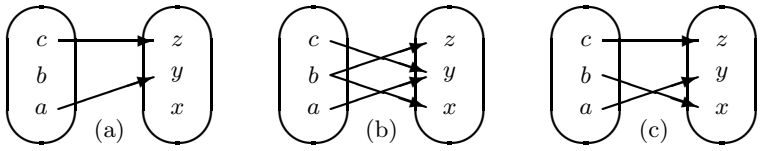

Abb. 6.1. Relationen: (a) nicht linkstotal, (b) nicht rechtseindeutig, (c) Abbildung.

Eigenschaften von Abbildungen

Satz 6.2. *Sind $f : A \to B$ und $g : A \to B$ Abbildungen, dann gilt $f = g$ genau dann, wenn $f(a) = g(a)$ für alle $a \in A$.*

Beweis. Wir schreiben f und g als Relationen

$$f = \{(a, f(a)) \mid a \in A\} \quad \text{und} \quad g = \{(a, g(a)) \mid a \in A\}.$$

Nach Definition der Mengengleichheit und der Eindeutigkeit von Paaren sind f und g genau dann gleich, wenn $f(a) = g(a)$ für alle $a \in A$. □

Satz 6.3. *Sind $f : A \to B$ und $g : B \to C$ Abbildungen, dann ist die Komposition $f \circ g$ eine Abbildung von A nach C.*

Beweis. Die Komposition $f \circ g$ ist definitionsgemäß eine Relation von A nach C.

Wir zeigen, dass $f \circ g$ linkstotal ist. Sei $a \in A$. Da f linkstotal ist, gibt es ein $b \in B$ mit $b = f(a)$. Weil aber auch g linkstotal ist, existiert ein $c \in C$ mit $c = g(b)$. Also ist $a(f \circ g)c$.

Wir beweisen, dass $f \circ g$ rechtseindeutig ist. Seien $a \in A$ und $c_1, c_2 \in C$ mit $a(f \circ g)c_1$ und $a(f \circ g)c_2$. Dann gibt es $b_1, b_2 \in B$ mit $b_1 = f(a)$, $c_1 = g(b_1)$, $b_2 = f(a)$ und $c_2 = g(b_2)$. Weil f rechtseindeutig ist, folgt $b_1 = b_2$, also $c_1 = g(b_1) = g(b_2) = c_2$. Da auch g rechtseindeutig ist, ergibt sich $c_1 = c_2$. □

Für die Komposition von $f : A \to B$ und $g : B \to C$ ist $c = (f \circ g)(a)$ gleichbedeutend mit $c = g(f(a))$, denn aus $c = (f \circ g)(a)$ folgt die Existenz von $b \in B$ mit $b = f(a)$ und $c = g(b)$, was $c = g(f(a))$ zur Folge hat. Deshalb wird im Folgenden für die Komposition $f \circ g$ kürzer gf geschrieben.

Aus den Rechengesetzen für die Komposition von Relationen ergibt sich unmittelbar der folgende

Satz 6.4. *Sind $f : A \to B$, $g : B \to C$ und $h : C \to D$ Abbildungen, dann gilt*

- $h(gf) = (hg)f$.
- $f\, id_A = f = id_B\, f$.

Abbildungsdiagramme

Die Komposition von Abbildungen wird bildlich in einem *Abbildungsdiagramm* dargestellt, das Abbildungen mitsamt ihrer Quell- und Zielmengen beschreibt. Ein Abbildungsdiagramm heißt *kommutativ*, wenn alle gerichteten Wege mit gleichem Start- und Endknoten dieselbe Abbildung liefern, wobei beim Durchlaufen eines gerichteten Weges die Abbildungen durch Komposition verknüpft werden.

Beispielsweise zeigt die Abb. 6.2 ein Abbildungsdiagramm mit den Abbildungen $f : A \to B$, $g : B \to C$ und $h : A \to C$, das im Falle $h = gf$ kommutativ ist.

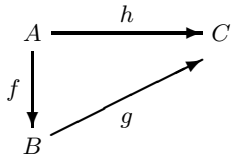

Abb. 6.2. Ein Abbildungsdiagramm.

6.2 Spezielle Abbildungen

Eine Abbildung $f : A \to B$ heißt *injektiv* (oder *linkseindeutig*), wenn es zu jedem $b \in B$ höchstens ein $a \in A$ gibt mit $f(a) = b$, d. h. für alle $a_1, a_2 \in A$ aus $f(a_1) = f(a_2)$ stets $a_1 = a_2$ folgt. Nach dem Gesetz der Kontraposition ist diese Bedingung gleichwertig dazu, dass für alle $a_1, a_2 \in A$ aus $a_1 \neq a_2$ stets $f(a_1) \neq f(a_2)$ folgt.

Eine Abbildung $f : A \to B$ heißt *surjektiv* (oder *rechtstotal* oder eine Abbildung von A *auf* B), wenn es zu jedem $b \in B$ mindestens ein $a \in A$ gibt mit $f(a) = b$, d. h. $f(A) = \mathrm{ran}(f) = B$. Eine injektive und surjektive Abbildung $f : A \to B$ heißt *bijektiv*. Eine Abbildung $f : A \to B$ ist bijektiv genau dann, wenn es zu jedem $b \in B$ genau ein $a \in A$ gibt mit $f(a) = b$ (Abb. 6.3).

Beispiele 6.5. Die identische Abbildung id_A ist bijektiv, die Inklusionsabbildung $\iota : A \to B$ ist injektiv und die Konstantenabbildung $f : A \to \{b_0\}$ ist surjektiv.

Zu jeder Abbildung $f : A \to B$ kann eine injektive bzw. surjektive Abbildung durch Einschränken ihres Definitions- bzw. Wertebereichs erhalten werden. Die Sinus-Funktion ist weder injektiv noch surjektiv (Abb. 6.4). Sie wird injektiv, wenn die Quellmenge auf das reellwertige Intervall $[-\frac{\pi}{2}, +\frac{\pi}{2}]$ eingeschränkt wird, und sie wird surjektiv, wenn die Zielmenge auf den Wertebereich $[-1, +1]$ beschränkt wird.

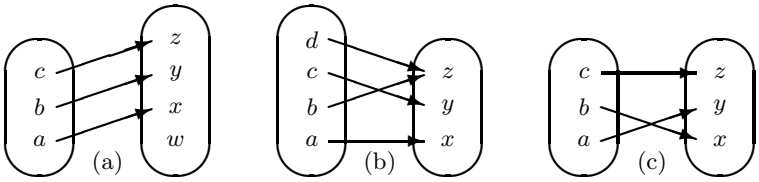

Abb. 6.3. Abbildungen: (a) injektiv, (b) surjektiv, (c) bijektiv.

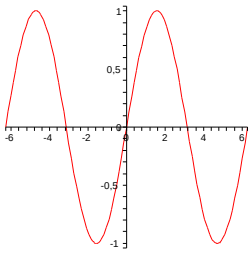

Abb. 6.4. Graph der Abbildung $[-2\pi, 2\pi] \to \mathbb{R} : x \mapsto \sin(x)$.

Satz 6.6. *Seien $f : A \to B$ und $g : B \to C$ Abbildungen.*

- *Sind f und g injektiv bzw. surjektiv, dann ist gf injektiv bzw. surjektiv.*
- *Ist gf injektiv, dann ist f injektiv.*
- *Ist gf surjektiv, dann ist g surjektiv.*

Beweis. Seien f und g injektiv. Seien $a_1, a_2 \in A$ mit $(gf)(a_1) = (gf)(a_2)$, also $g(f(a_1)) = g(f(a_2))$. Da g injektiv ist, folgt $f(a_1) = f(a_2)$. Weil f injektiv ist, ergibt sich $a_1 = a_2$. Also ist gf injektiv.

Seien f und g surjektiv und $c \in C$. Da g surjektiv ist, gibt es ein $b \in B$ mit $g(b) = c$. Weil f surjektiv ist, existiert ein $a \in A$ mit $f(a) = b$. Folglich ist $(gf)(a) = c$ und somit gf surjektiv.

Sei gf injektiv und seien $a_1, a_2 \in A$ mit $a_1 \neq a_2$. Dann ist $g(f(a_1)) = (gf)(a_1) \neq (gf)(a_2) = g(f(a_2))$. Weil g rechtseindeutig ist, folgt $f(a_1) \neq f(a_2)$. Also ist f injektiv.

Sei gf surjektiv und sei $c \in C$. Dann gibt es ein $a \in A$ mit $c = (gf)(a)$. Wird $b = f(a) \in B$ gesetzt, dann ist $c = g(b)$ und somit g surjektiv. □

Satz 6.7. *Ist $f : A \to B$ bijektiv, dann ist $f^{-1} : B \to A$ bijektiv und es gilt*

- $f^{-1}f = id_A$ *und* $ff^{-1} = id_B$.
- $(f^{-1})^{-1} = f$.

Beweis. Sei $f : A \to B$ bijektiv. Zu f kann die inverse Relation $f^{-1} = \{(f(a), a) \mid a \in A\}$ gebildet werden. Die Relation f^{-1} ist rechtstotal bzw. linkstotal, weil f linkstotal bzw. rechtstotal ist. Die Relation f^{-1} ist rechtseindeutig bzw. linkseindeutig, da f linkseindeutig bzw. rechtseindeutig ist. Also ist f^{-1} bijektiv.

Nach Definition von f^{-1} gilt $(f^{-1}f)(a) = f^{-1}(f(a)) = a$ für jedes $a \in A$ und $(ff^{-1})(b) = f(f^{-1}(b)) = b$ für jedes $b \in B$. Die letzte Aussage folgt aus dem Satz 4.7. □

Bei Abbildungen zwischen endlichen Mengen mit gleicher Elementeanzahl fallen die Begriffe surjektiv, injektiv und bijektiv zusammen.

Satz 6.8. *Sind A und B endliche Mengen mit gleicher Elementeanzahl, dann sind für jede Abbildung $f : A \to B$ äquivalent:*

1. *f ist surjektiv.*
2. *f ist injektiv.*
3. *f ist bijektiv.*

Beweis. Seien A und B n-elementige Mengen. Die Äquivalenzen werden durch einen *Ringschluss* bewiesen.

1. ⇒ 2. Sei f surjektiv, also $f(A) = B$. Dann ist $f(A)$ auch n-elementig. Seien $A = \{a_1, \ldots, a_n\}$ und $f(A) = \{f(a_1), \ldots, f(a_n)\}$. Die Mengen A und $f(A)$ können nur dann n-elementig sein, wenn $f(a_i) \neq f(a_j)$ für $a_i \neq a_j$ gilt. Also ist f injektiv.

2. ⇒ 3. Sei f injektiv. Dann sind $f(A)$ und A jeweils n-elementig. Da B ebenfalls n-elementig ist, folgt $f(A) = B$. Also ist f surjektiv, mithin bijektiv.

3. ⇒ 1. ist klar. □

6.3 Familien, Folgen und Multimengen

Familien und Folgen

Familien und Folgen sind Abbildungen, in denen es vor allem auf die Bilder ankommt. Seien A und I Mengen. Eine *Familie zur Indexmenge I mit Koeffizienten in A* ist eine Abbildung $f : I \to A$. Für eine solche Abbildung wird geschrieben

$$f = (f(i))_{i \in I} = (f_i)_{i \in I} \quad \text{mit } f_i = f(i) \tag{6.2}$$

oder kürzer

$$f = (f(i)) = (f_i). \tag{6.3}$$

Die Elemente f_i werden *Glieder* von f genannt. Eine Familie zur Indexmenge $I = \mathbb{N}$ oder $I = \mathbb{N}_0$ heißt eine *unendliche Folge*. Ein Familie zur Indexmenge $I = \underline{n}$ wird eine *Folge der Länge* n genannt, wobei f auch geschrieben wird in der Form

$$f = (f_1, \ldots, f_n). \tag{6.4}$$

Beispiele 6.9. Wir betrachten zwei typische Familien.

- Ein *Wort* der Länge n über einer endlichen Menge A ist eine Folge $w = (w_1, \ldots, w_n)$ der Länge n mit Koeffizienten in A. Für ein Wort w wird kürzer geschrieben

  $$w = w_1 \ldots w_n. \tag{6.5}$$

  Die Menge A heißt *Zeichenvorrat* und die Elemente von A *Buchstaben*. Das *leere Wort* ist die leere Abbildung (Relation), sie wird mit ϵ bezeichnet. Die Wörter der Länge ≤ 2 über $\{a, b\}$ sind ϵ, a, b, aa, ab, ba und bb.
- Eine $m \times n$*-Matrix* über einer Menge A ist eine Familie $(a_{(i,j)})$ zur Indexmenge $I = \underline{m} \times \underline{n}$ mit Koeffizienten in A. Die Einträge $a_{(i,j)}$ der Matrix werden kürzer in der Gestalt a_{ij} geschrieben.

Folgen vs. n-Tupel

Es gibt einen feinen Unterschied zwischen n-Tupeln und Folgen der Länge n. Dazu wird die Menge aller Folgen der Länge n betrachtet, deren i-te Glieder in einer Menge A_i liegen

$$A_1 * \ldots * A_n = \{f \mid f : \underline{n} \to \bigcup_{i=1}^{n} A_i \wedge \forall i[i \in \underline{n} \Rightarrow f(i) \in A_i]\}. \tag{6.6}$$

Satz 6.10. *Die Abbildung* $\varphi : A_1 * \ldots * A_n \to A_1 \times \ldots \times A_n$*, definiert durch*

$$f \mapsto (f(1), \ldots, f(n)), \tag{6.7}$$

ist bijektiv.

Beweis. Sei $(a_1, \ldots, a_n) \in A_1 \times \ldots \times A_n$. Für die Familie $f : \underline{n} \to \bigcup_{i=1}^{n} A_i$, definiert durch $f(i) = a_i$, gilt

$$\varphi(f) = (f(1), \ldots, f(n)) = (a_1, \ldots, a_n). \tag{6.8}$$

Also ist φ surjektiv. Seien $f, g \in A_1 * \ldots * A_n$ mit $\varphi(f) = \varphi(g)$. Dann ist $(f(1), \ldots, f(n)) = (g(1), \ldots, g(n))$. Wegen Satz 4.4 folgt $f(i) = g(i)$ für $1 \leq i \leq n$. Nach Satz 6.2 ergibt sich $f = g$. Also ist φ injektiv. □

Das kartesische Produkt $A_1 \times \ldots \times A_n$ entspricht also der Menge aller Folgen der Länge n, deren i-te Glieder in A_i liegen. Sind die Mengen A_i allesamt identisch, also $A = A_i$ für alle $1 \leq i \leq n$, dann ist das Produkt $A_1 * \ldots * A_n$ identisch mit der Menge aller Abbildungen von I nach A

$$A^I = \{f \mid f : I \to A\}. \tag{6.9}$$

Beispielsweise ist $A^{\overline{m} \times \overline{n}}$ definitionsgemäß die Menge aller $m \times n$-Matrizen über A. Diese Menge kann nach Satz 6.10 mit dem kartesischen Produkt $A^{m \times n}$ identifiziert werden.

Beispiel 6.11. Sei $A = \{a, b\}$. Die Menge $A^{\underline{2}}$ besteht aus den Abbildungen

f_1	1	2
	a	a

f_2	1	2
	a	b

f_3	1	2
	b	a

f_4	1	2
	b	b

Die bijektive Abbildung $\varphi : A^{\underline{2}} \to A^2$ ist definiert durch folgende Zuordnung

f	f_1	f_2	f_3	f_4
$\varphi(f)$	(a,a)	(a,b)	(b,a)	(b,b)

Multimengen

Sei A eine Menge. Eine *Multimenge* über A ist eine Abbildung $f : A \to \mathbb{N}_0$. Der Funktionswert $f(a)$ von $a \in A$ wird als Häufigkeit interpretiert, mit der a in der Multimenge auftritt. Eine Multimenge wird wie eine Menge $\{\ldots\}_M$ (mit nachgestelltem Index M) geschrieben. Zwei Multimengen über A sind gleich, wenn sie als Abbildungen gleich sind. Gewöhnliche Mengen sind Multimengen mit dem Wertebereich $f(A) \subseteq \{0, 1\}$.

Beispiele 6.12. Die Abbildung $f : \underline{3} \to \mathbb{N}_0$ mit $f(1) = 2$, $f(2) = 1$ und $f(3) = 1$ definiert die Multimenge $\{1, 1, 2, 3\}_M$. Die Multimengen $\{1, 1, 2, 3\}_M$ und $\{1, 3, 2, 1\}_M$ sind gleich, nicht aber die Multimengen $\{1, 1, 2, 3\}_M$ und $\{1, 2, 2, 3\}_M$.

Beispiel 6.13. Mit Multimengen lassen sich etwa alle Möglichkeiten beschreiben, k Elemente aus einer n-elementigen Menge auszuwählen, wobei Elemente mehrfach ausgewählt werden dürfen und es auf die Reihenfolge der Elemente nicht ankommt. Im Falle $k = 3$ und $n = 2$ ergeben sich folgende Möglichkeiten: $\{1, 1, 1\}_M$, $\{1, 1, 2\}_M$, $\{1, 2, 2\}_M$ und $\{2, 2, 2\}_M$.

6.4 Permutationen

Permutationen sind bijektive Abbildungen auf endlichen Mengen. Sie spielen u. a. in der Kombinatorik und der Gruppentheorie eine wichtige Rolle.

Darstellung von Permutationen

Sei A eine endliche Menge. Eine bijektive Abbildung $f : A \to A$ heißt eine *Permutation* von A. Eine Permutation von $\underline{n}$ wird eine *Permutation vom Grad* n genannt.

Eine Permutation π vom Grad n wird als zweireihige Matrix dargestellt

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}. \tag{6.10}$$

Die inverse Abbildung von π wird dadurch erhalten, indem die erste und zweite Zeile der Matrix vertauscht werden

$$\begin{pmatrix} \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \\ 1 & 2 & 3 & \dots & n \end{pmatrix} \tag{6.11}$$

und anschließend die Spalten gemäß der ersten Zeile aufsteigend sortiert werden. Beispielsweise gilt

$$\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,1\,4\,5\,6\,7\,3 \end{pmatrix}^{-1} = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,1\,7\,3\,4\,5\,6 \end{pmatrix}.$$

Permutationen vom Grad n werden auch als Produkte von Zykeln dargestellt. Beispielsweise bildet die Permutation

$$\pi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,4\,5\,7\,3\,6\,1 \end{pmatrix} \tag{6.12}$$

das Element 1 auf 2, 2 auf 4, 4 auf 7 und 7 auf 1 ab. Diese Abbildungsfolge wird durch den *Zykel* (1247) repräsentiert. Das Element 3 wird auf 5 und 5 auf 3 abgebildet, dies ergibt den Zykel (35). Das Element 6 wird auf sich selbst abgebildet, dies wird durch den Zykel (6) ausgedrückt. Damit ergibt sich die *Zykeldarstellung* von π:

$$\pi = (1247)(35)(6). \tag{6.13}$$

In der Zykeldarstellung kommt es nicht auf die Reihenfolge der Zykeln an und in einem Zykel kann mit jedem beliebigen Element begonnen werden

$$(35)(6)(1247) = (1247)(35)(6) = (4712)(53)(6). \tag{6.14}$$

Die *Länge* eines Zykels ist die Anzahl seiner Elemente. Ein Zykel der Länge n wird auch n*-Zykel* genannt. Insbesondere heißen 2-Zykeln *Transpositionen* und 1-Zykeln *Fixpunkte*. Die Fixpunkte werden in einer Zykeldarstellung unterdrückt, wenn der Grad der Permutation bekannt ist. Im obigen Beispiel wird anstelle (35)(6)(1247) auch (35)(1247) geschrieben.

Beispiel 6.14. Die Permutationen vom Grad 3 sind

$$id = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix} = (1)(2)(3),\ \delta_1 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix} = (123),$$
$$\delta_2 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix} = (132), \qquad \sigma_1 = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix} = (1)(23),$$
$$\sigma_2 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix} = (13)(2), \quad \sigma_3 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix} = (12)(3).$$

Diese Permutationen beschreiben alle Drehungen und Spiegelungen eines gleichseitigen Dreiecks, die das Dreieck wieder zur Deckung bringen. Sind die Ecken des Dreiecks im Uhrzeigersinn mit 1, 2 und 3 nummeriert, so bewirkt δ_1 bzw. δ_2 ist eine Drehung des Dreiecks um 120^o bzw. 240^o im Uhrzeigersinn, während σ_i eine Spiegelung am Lot durch die Ecke i beschreibt.

Permutationen als Produkte von Zykeln

Die Zykeldarstellung zeigt, dass sich jede Permutation vom Grad n als *Produkt von disjunkten Zykeln* schreiben lässt. *Disjunkt* bedeutet, dass jedes Element in höchstens einem Zykel vorkommt. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zykeln und zyklisches Vertauschen der Elemente eines Zykels.

Satz 6.15. *Jede Permutation vom Grad n ist darstellbar als ein Produkt von Transpositionen.*

Beweis. Es bleibt zu zeigen, dass jeder Zykel $(x_1, \ldots, x_m)$ ein Produkt von Transpositionen ist. Wir beweisen

$$(x_1, \ldots, x_m) = (x_1 x_m) \ldots (x_1 x_3)(x_1 x_2). \tag{6.15}$$

Der Beweis wird durch vollständige Induktion nach m geführt. Für $m = 2$ ist die Identität klar. Sei $m \geq 2$. Für den m-Zykel $\pi = (x_1, \ldots, x_m)$ und die Transposition $\rho = (x_1, x_{m+1})$ gilt

$$\begin{aligned} \rho\pi &= \begin{pmatrix} x_1 & x_2 \ldots x_m & x_{m+1} \\ x_{m+1} & x_2 \ldots x_m & x_1 \end{pmatrix} \begin{pmatrix} x_1\ x_2 \ldots x_{m-1}\ x_m\ x_{m+1} \\ x_2\ x_3 \ldots\ x_m\ \ x_1\ x_{m+1} \end{pmatrix} \\ &= \begin{pmatrix} x_1\ x_2 \ldots x_{m-1} & x_m & x_{m+1} \\ x_2\ x_3 \ldots\ x_m & x_{m+1} & x_1 \end{pmatrix} \\ &= (x_1, \ldots, x_m, x_{m+1}). \end{aligned}$$

Da π nach Induktionsannahme als Produkt von Transpositionen darstellbar ist, hat auch $(x_1, \ldots, x_{m+1})$ eine solche Darstellung. □

Die Darstellung einer Permutation als Produkt von Transpositionen ist nicht eindeutig bestimmt, denn etwa gilt $(123) = (13)(12) = (12)(23)$.

Satz 6.16. *Ist eine Permutation vom Grad n darstellbar als ein Produkt von r und s Transpositionen, dann sind r und s entweder beide gerade oder beide ungerade.*

Beweis. Sei π eine Permutation von Grad n, die aus k disjunkten Zykeln besteht. Sei (ij) eine Transposition mit $1 \leq i < j \leq n$. Gehören i und j zum selben Zykel von π, dann ist

$$(ij)\pi = (ij)(ia \dots bj \dots c) \dots = (ia \dots b)(j \dots c) \dots$$

Liegen i und j in verschiedenen Zykeln von π, so gilt

$$(ij)\pi = (ij)(ia \dots b)(j \dots c) \dots = (ia \dots bj \dots c) \dots$$

Die Permutation $(ij)\pi$ hat im ersten Fall $k+1$ Zykeln und im zweiten Fall $k-1$ Zykeln.

Nach Satz 6.15 ist π darstellbar als Produkt von Transpositionen $\tau_r \dots \tau_1$. Die Transposition τ_1 besteht aus $1+(n-2) = n-1$ Zykeln, einer Transposition und $n-2$ Fixpunkten. Durch sukzessives Komponieren von τ_1 mit $\tau_2, \dots, \tau_r$ ergibt sich π. Wie oben gezeigt, erhöht oder erniedrigt sich in jedem Schritt die Anzahl der Zykeln um Eins. Bei insgesamt l Vergrößerungen und m Verkleinerungen besteht π aus $k = (n-1) + l - m$ Zykeln. Wegen $l + m = r - 1$ folgt

$$r = l + m + 1 = l + (n - 1 + l - k) + 1 = n + 2l - k.$$

Ist π als Produkt von s Transpositionen darstellbar, dann ergibt sich bei insgesamt l' Vergrößerungen

$$s = n + 2l' - k.$$

Folglich ist

$$r - s = 2(l - l').$$

Also ist die Zahl $r - s$ gerade und die Behauptung beweisen. □

Gerade und ungerade Permutationen

Eine Permutation π vom Grad n heißt *gerade*, wenn π darstellbar ist als ein Produkt einer geraden Anzahl von Transpositionen. Das *Signum* von π ist definiert durch

$$\operatorname{sgn}(\pi) = \begin{cases} +1 \text{ falls } \pi \text{ gerade,} \\ -1 \text{ sonst.} \end{cases} \tag{6.16}$$

Die identische Abbildung hat das Signum

$$\operatorname{sgn}(id) = (-1)^0 = 1. \tag{6.17}$$

Sei π eine als Produkt von r Transpositionen darstellbare Permutation vom Grad n. Für das Signum von π gilt dann

$$\operatorname{sgn}(\pi) = (-1)^r. \tag{6.18}$$

Ist ρ eine als Produkt von s Transpositionen darstellbare Permutation vom Grad n, dann ist $\pi\rho$ ein Produkt von $r+s$ Transpositionen und hat somit das Signum

$$\operatorname{sgn}(\pi\rho) = (-1)^{r+s} = (-1)^r(-1)^s = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho). \tag{6.19}$$

Daraus folgt

$$1 = \operatorname{sgn}(id) = \operatorname{sgn}(\pi^{-1}\pi) = \operatorname{sgn}(\pi^{-1})\operatorname{sgn}(\pi). \tag{6.20}$$

Also hat die inverse Permutation von π das Signum

$$\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi). \tag{6.21}$$

Für die zu π konjugierte Permutation $\rho^{-1}\pi\rho$ gilt also

$$\operatorname{sgn}(\rho^{-1}\pi\rho) = \operatorname{sgn}(\rho^{-1})\operatorname{sgn}(\pi)\operatorname{sgn}(\rho) = \operatorname{sgn}(\pi). \tag{6.22}$$

Determinanten

Die *Determinante* einer reellwertigen $n \times n$-Matrix $A = (a_{ij})$ ist definiert durch

$$\det A = \sum_{\pi} \operatorname{sgn}(\pi) a_{1,\pi(1)} \cdots a_{n,\pi(n)}, \tag{6.23}$$

wobei die Summe über alle Permutationen π vom Grad n läuft.

Beispiel 6.17. Die Determinante einer reellwertigen 3×3-Matrix $A = (a_{ij})$ lautet

$$\begin{aligned}
\det A = {} & +a_{11}a_{22}a_{33} && (\pi = id) \\
& -a_{12}a_{21}a_{33} && (\pi = (12)(3)) \\
& -a_{13}a_{22}a_{31} && (\pi = (13)(2)) \\
& -a_{11}a_{23}a_{32} && (\pi = (1)(23)) \\
& +a_{12}a_{23}a_{31} && (\pi = (123)) \\
& +a_{13}a_{21}a_{32} && (\pi = (132)).
\end{aligned}$$

Der Lehmer-Code

Die Permutationen vom Grad n sind anhand des so genannten Lehmer-Codes leicht computergestützt konstruierbar. Der *Lehmer-Code* einer Permutation π vom Grad n ist

$$L(\pi) = (l_1(\pi) \dots l_n(\pi)), \tag{6.24}$$

wobei für alle $i \in \underline{n}$ gilt

$$l_i(\pi) = |\{j \in \underline{n} \mid j > i \wedge \pi(j) < \pi(i)\}|. \tag{6.25}$$

Beispiele 6.18.
- Der Lehmer-Code der Permutation $\pi = (1345)(2)(67)$ ist $L(\pi) = (2, 1, 1, 1, 0, 1, 0)$.
- Für die in 6.14 dargestellten Permutationen vom Grad 3 gilt $L(id) = (0, 0, 0)$, $L(\sigma_1) = (0, 1, 0)$, $L(\sigma_2) = (2, 0, 0)$, $L(\sigma_3) = (1, 0, 0)$, $L(\delta_1) = (1, 1, 0)$ und $L(\delta_2) = (2, 1, 0)$.

Satz 6.19. *Sei S_n die Menge aller Permutationen vom Grad n und sei $\Lambda_n = \{(x_1, \dots, x_n) \mid \forall i \in \underline{n}[x_i \in \mathbb{N}_0 \wedge 0 \leq x_i \leq n - i]\}$. Die Abbildung $S_n \to \Lambda_n : \pi \mapsto L(\pi)$ ist bijektiv.*

Beweis. Der Lehmer-Code von $\pi \in S_n$ liegt in Λ_n, weil für die i-te Komponente von $L(\pi)$ stets $l_i(\pi) \leq n - i$ gilt. Die Abbildung ist injektiv, weil jedes π aus seinem Lehmer-Code $L(\pi)$ rekonstruierbar ist: $\pi(1)$ ist das $(l_1(\pi) + 1)$-te Element von $\underline{n}$, $\pi(2)$ ist das $(l_2(\pi) + 1)$-te Element von $\underline{n} \setminus \{\pi(1)\}$, usw. Da Λ_n ebenso wie S_n die Mächtigkeit $n!$ besitzt (Korollar 10.14), ist diese Abbildung nach Satz 6.8 sogar bijektiv. □

6.5 Analyse von Algorithmen

Der Aufwand von Computerprogrammen kann mithilfe von Folgen abgeschätzt werden.

Laufzeit von Algorithmen

Die Rechenzeit eines Computerprogramms ist in Millisekunden messbar. Diese Größe ist aber abhängig von vielen Parametern wie dem verwendeten Rechner, Compiler, Betriebssystem, Programmiertricks, usw. Außerdem ist die Rechenzeit nur für Programme messbar, nicht aber für Algorithmen. Deshalb wird die Rechenzeit eines Programms auf folgende Art gemessen:

- Für die gegebene Eingabe werden die durchgeführten Elementaroperationen gezählt.
- Die Rechenzeit wird durch eine Funktion angegeben, die die Anzahl der durchgeführten Elementaroperationen in Abhängigkeit von der "Komplexität" der Eingabe darstellt.

Die *Elementaroperationen* sind Zuweisungen ($x := 3$), Vergleiche ($x < y$), arithmetische Operationen ($x + y$) und Arrayzugriffe ($a[i]$). Nichtelementare Operationen sind Schleifen, bedingte Anweisungen und Prozeduraufrufe.

Beispiel 6.20. Das Sortierverfahren BUBBLESORT beruht auf der Idee, zwei benachbarte Elemente einer Liste zu vertauschen, wenn sie nicht richtig gereiht sind (Alg. 6.1). BUBBLESORT besteht aus einer zweifach geschachtelten

Algorithmus 6.1 BUBBLESORT(L)

Eingabe: n-elementige Liste L ganzer Zahlen
Ausgabe: Liste L aufsteigend sortiert

```
1: for i = 2 to n do
2:    for j = n downto i do
3:       if L[j − 1] > L[j] then
4:          h := L[j]
5:          L[j] := L[j − 1]
6:          L[j − 1] := h
7:       end if
8:    end for
9: end for
```

Laufschleife, deren Rumpf für folgende Paare (i, j) ausgeführt wird

$$(2, n), (2, n-1), \ldots, (2, 2), (3, n), \ldots, (3, 3), \ldots, (n, n).$$

Dies sind insgesamt $n(n-1)/2$ Paare. Der Rumpf besteht aus insgesamt vier Elementaroperationen, einem Vergleich und drei Zuweisungen. Wir nehmen an, dass jede Elementaranweisung die Rechenzeit t erfordert. Dann hat der Algorithmus die Rechenzeit $4tn(n-1)/2$.

Landau-Notation

In der Praxis ist nur das Wachstum einer Rechenzeitfunktion von Interesse. Seien $f = (f(n))$ und $g = (g(n))$ unendliche Folgen mit positiven reellen Werten. Der Ausdruck $f = O(g)$ besagt, dass f durch g nach oben asymptotisch beschränkt ist, d. h.,

$$f = O(g) \ :\Longleftrightarrow\ \exists\, n_0 \in \mathbb{N}\ \exists\, c \in \mathbb{R}^+\ \forall\, n[n \geq n_0 \Rightarrow f(n) \leq c \cdot g(n)]. \quad (6.26)$$

Das *Landau-Symbol* O wird nach E. Landau (1877-1938) "groß O" gesprochen. Die Schreibweise $f = O(g)$ hat sich für die präzisere Notation $f \in O(g)$ eingebürgert, wobei $O(g)$ für die Menge aller Folgen f mit $f = O(g)$ steht.

Beispiele 6.21. • $f(n) = 3 = O(1)$, da $3 \leq 3 \cdot 1$.
- $f(n) = n + 4 = O(n)$, da $n + 4 \leq 2n$ für alle $n \geq 4$.
- $f(n) = 4n + 6 = O(n)$, da $4n + 6 \leq 5n$ für alle $n \geq 6$.
- $f(n) = n(n-1)/2 = O(n^2)$, da $n(n-1)/2 \leq n^2$ für alle $n \geq 1$.
- $f(n) = 2n^2 + 4n + 6 = O(n^2)$, da $2n^2 + 4n + 6 \leq 3n^2$ für alle $n \geq 6$.

Mit der O-Notation werden Abbildungen vergröbernd betrachtet, indem Konstanten eliminiert und obere Schranken gebildet werden. Rechenzeitfunktionen werden vermöge der O-Notation in Klassen eingeteilt (Tab. 6.1).

Tabelle 6.1. Einteilung von Laufzeitfunktionen.

	Sprechweise	Typische Algorithmen
$O(1)$	konstant	Elementaroperationen
$O(\log n)$	logarithmisch	Suchen in einer Menge
$O(n)$	linear	Bearbeiten jedes Elements einer Menge
$O(n \log n)$	log-linear	gute Sortierverfahren, schnelle Fouriertransformation
$O(n^2)$	quadratisch	primitive Sortierverfahren
$O(n^k), k \geq 2$	polynomial	Netzwerkalgorithmen
$O(2^n)$	exponentiell	Backtracking

Beispiel 6.22. Wir nehmen an, dass alle Elementaroperationen die Rechenzeit $O(1)$ haben. BubbleSort besitzt dann die Rechenzeit $O(n^2)$, weil der Schleifenrumpf die Rechenzeit $O(1)$ hat und die zweifach geschachtelte Schleife $n(n-1)/2$ mal durchlaufen wird.

Der Ausdruck $f = o(g)$ besagt, dass f gegenüber g asymptotisch vernachlässigbar ist, d. h.,

$$f = o(g) \ :\Longleftrightarrow \ \forall\, c > 0\ \exists\, n_0\ \forall\, n[n \geq n_0 \Rightarrow |f(n)| < c \cdot |g(n)|]. \quad (6.27)$$

Das *Landau-Symbol* o wird "klein o" gesprochen. Ähnlich wie $O(g)$ repräsentiert $o(g)$ die Menge aller Folgen f mit $f = o(g)$.

Beispiel 6.23. Es gilt $\frac{1}{n} = o\left(\frac{1}{\sqrt{n}}\right)$, $n^2 = o(e^n)$ und $\log n = o(n)$.

Selbsttestaufgaben

6.1. Welche der folgenden Relationen auf $A = \{a, b, c, d\}$ sind Abbildungen?

- $\{(a, d), (c, d), (d, a), (c, d), (b, a)\}$.
- $\{(d, b), (a, b), (c, a), (d, d)\}$.
- $\{(d, b), (c, b), (b, b), (a, b)\}$.
- $\{(d, a), (c, d), (a, b), (b, a), (a, a)\}$.

6.2. Berechne die Kompositionen fg und gf der reellwertigen Abbildungen $f(x) = 3x - 1$ und $g(x) = x^2 + 2$.

6.3. Das Diagramm in Abb. 6.5 sei kommutativ. Stelle die Abbildung $h_1 \circ h_2$ auf so viele Arten wie möglich dar.

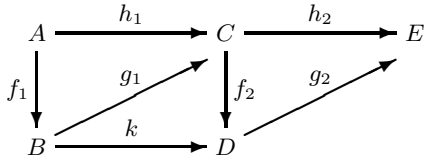

Abb. 6.5. Abbildungsdiagramm.

6.4. Welche der folgenden reellwertigen Abbildungen sind injektiv, surjektiv oder bijektiv?

- $f(x) = 2^x$.
- $g(x) = x^3$.
- $h(x) = x^3 - x$.

6.5. Beweise den Satz 6.4.

6.6. Sei $f : A \to B$ eine surjektive Abbildung. Zeige, dass das Mengensystem $\overline{A} = \{f^{-1}(\{b\}) \mid b \in B\}$ der Urbildmengen $f^{-1}(\{b\}) = \{a \mid a \in A \wedge f(a) = b\}$ eine Partition von A ist.

6.7. (Abbildungssatz) Sei $f : A \to B$ eine surjektive Abbildung mit $\overline{A} = \{f^{-1}(\{b\}) \mid b \in B\}$. Zeige, dass die Abbildung $g : \overline{A} \to B : \overline{a} \mapsto f(a)$ eine Bijektion ist.

6.8. Invertiere die Permutation

$$\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 2\,4\,6\,8\,1\,3\,5\,7\,9 \end{pmatrix}.$$

6.9. Seien $\pi = (1357)(246)(89)$ und $\rho = (1248)(35)(6)(79)$ Permutationen von Grad 9. Berechne $\rho\pi\rho^{-1}$.

6.10. Zeige, dass für jedes Polynom $p(n) = a_m n^m + a_{m-1} n^{m-1} + \ldots + a_1 n + a_0$ mit reellwertigen Koeffizienten gilt $p(n) = O(n^m)$.

6.11. (Binäre Suche) Sei $L = (l_1, \ldots, l_m)$, $m = 2^n - 1$, mit Einträgen $l_1 < \ldots < l_m$. Um zu bestimmen, ob ein Element a in der Liste vorkommt, wird wie folgt vorgegangen: a wird zuerst mit $l_{2^{n-1}}$ verglichen. Falls $a = l_{2^{n-1}}$, so wird die Suche mit `true` beendet. Im Falle $a < l_{2^{n-1}}$ bzw. $a > l_{2^{n-1}}$ wird a mit $l_{2^{n-2}}$ bzw. $l_{2^{n-1}+2^{n-2}}$ verglichen, usw. Bestimme die Laufzeit dieses Algorithmus.

7

Die natürlichen Zahlen

In diesem Kapitel wird das Beweisprinzip der vollständigen Induktion eingeführt. Damit lassen sich Aussagen beweisen, die für alle natürlichen Zahlen gelten. Dieses Beweisprinzip wird auf fundierte Mengen verallgemeinert, wodurch sich Eigenschaften von Datenstrukturen und Programmen verifizieren lassen.

7.1 Vollständige Induktion

Die Aussage "*Die Summe der ersten n ungeraden natürlichen Zahlen ist gleich n^2*" ist formal gegeben durch ein Prädikat $P(n)$ in der freien Variable n

$$\sum_{i=0}^{n-1}(2i+1) = n^2. \tag{7.1}$$

Wir zeigen, dass $P(n)$ für alle natürlichen Zahlen n gilt

$$\forall n[n \in \mathbb{N}_0 \Rightarrow P(n)]. \tag{7.2}$$

Als Fahrplan für den Beweis wird zuerst gezeigt, dass $P(0)$ wahr ist. Dann wird für alle natürlichen Zahlen $n \geq 0$ bewiesen, dass $P(n+1)$ wahr ist, sofern $P(0), \ldots, P(n)$ wahr sind

$$\forall n[n \in \mathbb{N}_0 \Rightarrow (P(0) \wedge \ldots \wedge P(n) \Rightarrow P(n+1))]. \tag{7.3}$$

Wenn die Aussagen $P(0)$ und (7.3) wahr sind, wird gefolgert, dass $P(n)$ wahr ist für jede natürliche Zahl n. Denn $P(n)$ kann für jede beliebige natürliche Zahl n bewiesen werden, indem der Reihe nach $P(0), \ldots, P(n-1)$ gezeigt werden:

- Sind $P(0)$ und $P(0) \Rightarrow P(1)$ wahr, dann ist vermöge Modus Ponens auch $P(1)$ wahr.

- Sind $P(0)$, $P(1)$ und $P(0) \wedge P(1) \Rightarrow P(2)$ wahr, dann ist vermittels Modus Ponens auch $P(2)$ wahr usw.

Diese Beweistechnik heißt *vollständige Induktion über den natürlichen Zahlen*

$$P(0) \wedge \forall n \in \mathbb{N}_0[P(0) \wedge \ldots \wedge P(n) \Rightarrow P(n+1)] \Rightarrow \forall n \in \mathbb{N}_0[P(n)]. \quad (7.4)$$

Die Aussage $P(0)$ heißt *Induktionsanfang* und die Aussage

$$\forall n \in \mathbb{N}_0[P(0) \wedge \ldots \wedge P(n) \Rightarrow P(n+1)] \quad (7.5)$$

Induktionsschluss. Die Prämisse $P(0) \wedge \ldots \wedge P(n)$ des Induktionsschlusses wird *Induktionsannahme* genannt.

Beispiel 7.1. Wir beweisen (7.1) für alle natürlichen Zahlen.

- Induktionsanfang:
$$\sum_{i=0}^{-1}(2i+1) = 0 = 0^2,$$
denn eine leere Summe ist stets 0.
- Induktionsschluss: Sei n eine natürliche Zahl. Es wird $P(n+1)$ gezeigt und hierbei angenommen, dass $P(0), \ldots, P(n)$ wahr sind
$$\sum_{i=0}^{n}(2i+1) = \left(\sum_{i=0}^{n-1}(2i+1)\right) + 2n + 1 = n^2 + 2n + 1 = (n+1)^2.$$
Dabei fließt in die zweite Gleichung die Induktionsannahme ein.

7.2 Arithmetik

Peanosches Axiomensystem

Die Menge der natürlichen Zahlen $\mathbb{N}_0$ wurde von Guiseppe Peano (1858-1932) axiomatisch begründet. Die Menge $\mathbb{N}_0$ ist wie folgt definiert:

P1 Die Zahl 0 (Null) ist eine natürliche Zahl: $0 \in \mathbb{N}_0$.
P2 Es gibt eine Abbildung $S : \mathbb{N}_0 \to \mathbb{N}_0$, die jeder natürlichen Zahl n einen *Nachfolger* $S(n) \in \mathbb{N}_0$ zuordnet.
P3 Die Null ist nicht Nachfolger einer natürlichen Zahl.
P4 Verschiedene natürliche Zahlen haben verschiedene Nachfolger, d.h., S ist injektiv.
P5 Wenn eine Teilmenge N von $\mathbb{N}_0$ die Null und die Nachfolger all ihrer Elemente enthält, dann ist $N = \mathbb{N}_0$, d. h.,
$$N \subseteq \mathbb{N}_0 \wedge 0 \in N \wedge \forall n[n \in N \Rightarrow S(n) \in N] \Rightarrow N = \mathbb{N}_0. \quad (7.6)$$

Diese fünf Bedingungen sind notwendig, um die Menge der natürlichen Zahlen bis auf Umbenennung der Elemente (Bijektion) eindeutig festzulegen. Die letzte Bedingung wird *Induktionsaxiom* genannt.

Darstellung der natürlichen Zahlen

Satz 7.2. *Es gilt* $\mathbb{N}_0 = \{0, S(0), S(S(0)), S(S(S(0))), \ldots\}$.

Beweis. Wir setzen $N = \{0, S(0), S(S(0)), S(S(S(0))), \ldots\}$. Die Null liegt in N und mit jedem $n \in \mathbb{N}_0$ gehört per definitionem auch $S(n)$ zu N. Also folgt mit dem Induktionsaxiom $N = \mathbb{N}_0$. □

Die Nachfolger von Null werden wie üblich benannt

$$1 := S(0), \quad 2 := S(S(0)), \quad 3 := S(S(S(0))), \ldots \tag{7.7}$$

Addition und Multiplikation

Auf der Menge der natürlichen Zahlen werden *Addition* und *Multiplikation* definiert:

- Für jede natürliche Zahl m sei

$$m + 0 := m \quad \text{und} \quad m \cdot 0 := 0. \tag{7.8}$$

- Für alle natürlichen Zahlen m und n sei

$$m + S(n) := S(m + n) \quad \text{und} \quad m \cdot S(n) := (m \cdot n) + m. \tag{7.9}$$

  Das Produkt $m \cdot n$ wird kürzer mn geschrieben.

Die Definition der Addition und Multiplikation besteht jeweils aus zwei Teilen. Im ersten Teil wird die Operation direkt für ein Argument festgelegt, während im zweiten Teil die Operation für alle übrigen Argumente rekursiv definiert wird. Solche Definitionen ähneln der vollständigen Induktion und werden deshalb *induktiv* genannt.

Für den Nachfolger einer natürlichen Zahl n gilt $S(n) = n + 1$, denn für jedes n gilt

$$n + 1 = n + S(0) = S(n + 0) = S(n). \tag{7.10}$$

Beispiel 7.3. Es gilt $2 + 1 = 2 + S(0) = S(2 + 0) = S(2) = 3$. Damit folgt $2 + 2 = 2 + S(1) = S(2 + 1) = S(3) = 4$.

Satz 7.4. *Die Summe und das Produkt zweier natürlicher Zahlen sind natürliche Zahlen.*

Beweis. Die Aussage

$$\forall m \forall n [m \in \mathbb{N}_0 \wedge n \in \mathbb{N}_0 \Rightarrow m + n \in \mathbb{N}_0] \tag{7.11}$$

ist gleichwertig zur Aussage $\forall n[n \in \mathbb{N}_0 \Rightarrow P(n)]$, wobei $P(n)$ das folgende Prädikat bezeichnet

$$\forall m[m \in \mathbb{N}_0 \Rightarrow m + n \in \mathbb{N}_0]. \tag{7.12}$$

Letztere Aussage wird durch vollständige Induktion gezeigt: Induktionsanfang $P(0)$: Für beliebiges $m \in \mathbb{N}_0$ gilt $m+0 = m \in \mathbb{N}_0$. Induktionsschluss $P(n+1)$: Für beliebiges $m \in \mathbb{N}_0$ gilt $m + (n+1) = m + S(n) = S(m+n) \in \mathbb{N}_0$, wobei im letzten Schritt die Aussage $P(n)$ benutzt wurde. □

Satz 7.5. *Für alle natürlichen Zahlen l, m und n gelten folgende Rechenregeln:*

- *Kommutativgesetz:*

$$m + n = n + m$$
$$m \cdot n = n \cdot m$$

- *Assoziativgesetz:*

$$l + (m + n) = (l + m) + n$$
$$l \cdot (m \cdot n) = (l \cdot m) \cdot n$$

- *Distributivgesetz:*

$$l \cdot (m + n) = l \cdot m + l \cdot n$$
$$(l + m) \cdot n = l \cdot n + m \cdot n$$

- *Kürzungsregeln:*

$$l + m = l + n \Rightarrow m = n$$
$$l \cdot m = l \cdot n \Rightarrow m = n, \quad \textit{falls } l \neq 0.$$

Induktiv definierte Folgen

Die *Fibonacci-Folge*, benannt nach ihrem Entdecker, Leonardo von Pisa (1170+), ist die bekannteste, induktiv definierte Folge (F_n). Sie wird festgelegt durch

- $F_0 = 0$ und $F_1 = 1$,
- $F_n = F_{n-1} + F_{n-2}$ für alle natürlichen Zahlen $n \geq 2$.

Die ersten Glieder der Folge sind 0, 1, 1, 2, 3, 5, 8, 13, 21.

Beispiel 7.6. Die Fibonacci-Zahlen sind eng verknüpft mit dem *goldenen Schnitt*

$$\phi = (1 + \sqrt{5})/2 = 1.6180339887\ldots \tag{7.13}$$

Für den goldenen Schnitt gilt bekanntermaßen

$$\phi^2 = \phi + 1. \tag{7.14}$$

Für alle natürlichen Zahlen $n \geq 1$ gilt

$$F_n \leq \phi^{n-1}. \tag{7.15}$$

Beweis. Das Prädikat (7.15) sei mit $P(n)$ bezeichnet. Induktionsanfang $P(1)$ und $P(2)$: Es gilt $F_1 = 1 = \phi^0$ und $F_2 = 1 \leq \phi^1$. Induktionsschluss $P(n+1)$: Für $n \geq 2$ gilt $F_{n+1} = F_n + F_{n-1} \leq \phi^{n-1} + \phi^{n-2} = \phi^{n-2}(\phi+1) = \phi^n$, wobei in der ersten Ungleichung die Induktionsannahme und in der letzten Gleichung die Beziehung (7.14) benutzt wurden. □

Die Potenzen einer Relation

Sei R eine Relation auf einer Menge A. Die *Potenzen* von R werden induktiv definiert:

- $R^0 = I_A$,
- $R^{n+1} = R^n \circ R$ für alle natürlichen Zahlen $n \geq 0$.

Die Relation R^n wird *n-te Potenz* von R genannt. Nach Satz 4.7 gilt

$$R^1 = I_A \circ R = R. \tag{7.16}$$

Satz 7.7. *Sei R eine Relation auf A und n eine natürliche Zahl. Die n-te Potenz von R beschreibt die Menge aller gerichteten Wege der Länge n in $D = (A, R)$.*

Beweis. Die Aussage wird durch vollständige Induktion über die Weglänge gezeigt. Die Wege der Länge 1 entsprechen den Kanten in D, also $R^1 = R$. Sei $(a, b) \in R^{n+1}$. Dann gibt es nach Definition ein $c \in A$ mit aR^nc und cRb. Nach Induktionsannahme gibt es einen gerichteten Weg der Länge n von a nach c und einen gerichteten Weg der Länge 1 von c nach b. Mithin gibt es einen gericheteten Weg in D der Länge $n+1$ von a nach b. Dieser Schluss ist umkehrbar, woraus die Behauptung folgt. □

Beispiel 7.8. Die Relation $R = \{(a,b),(b,c),(c,d),(d,b)\}$ auf $A = \{a,b,c,d\}$ wird durch den Digraphen in Abb. 7.1 illustriert. Für die Potenzen von R gilt

$$\begin{aligned} R^1 &= \{(a,b),(b,c),(c,d),(d,b)\} \\ R^2 &= \{(a,c),(b,d),(c,b),(d,c)\} \\ R^3 &= \{(a,d),(b,b),(c,c),(d,d)\} \\ R^4 &= \{(a,b),(b,c),(c,d),(d,b)\}. \end{aligned}$$

Die gerichteten Wege der Länge $3i+j$ werden wegen $R^4 = R$ durch gerichtete Wege der Länge j beschrieben, wobei $i \geq 0$ und $1 \leq j \leq 3$.

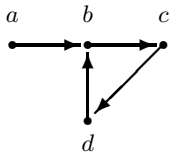

Abb. 7.1. Ein Digraph.

7.3 Induktion und fundierte Mengen

Das Beweisprinzip der vollständigen Induktion erweist sich als Spezialfall der Induktion auf fundierten Mengen.

Fundierte Mengen

Sei A eine nichtleere Menge und $\preceq$ eine Relation auf A. Ein Paar $(A, \preceq)$ heißt *fundiert*, wenn jede nichtleere Teilmenge von A ein minimales Element bzgl. $\preceq$ enthält.

Beispiele 7.9. Die halbgeordnete Menge $(\mathbb{N}_0, \leq)$ ist fundiert, weil $\mathbb{N}_0$ wohlgeordnet ist (Selbsttestaufgabe 7.5.).

Sei A die Menge aller Aussageformen. Für beliebige Aussageformen P und Q soll $P \preceq Q$ bedeuten, dass P ein Teilausdruck von Q ist. Beispielsweise enthält die Aussageform $(P \Rightarrow Q)$ die Teilausdrücke $P \Rightarrow Q$, P und Q. Da jede Aussageform mindestens eine Aussage oder Aussagenvariable enthält, ist die Menge aller Aussageformen fundiert.

Induktion über fundierten Mengen

Das Beweisprinzip der *Induktion über einer fundierten Menge* $(A, \prec)$ lautet

$$\forall a[a \in A \Rightarrow [\forall b[b \in A \Rightarrow (b \prec a \Rightarrow P(b))] \Rightarrow P(a)]]. \tag{7.17}$$

Im Beweis der Aussage $P(a)$ wird angenommen, dass die Aussage $P(b)$ für alle $b \prec a$ gilt. Dies ist die *Induktionsannahme*

$$\forall b[b \in A \Rightarrow (b \prec a \Rightarrow P(b))]. \tag{7.18}$$

Für die fundierte Menge $(\mathbb{N}_0, \leq)$ wird die Aussage (7.17) zur Aussage (7.3). Denn für $a = 0$ wird (7.17) zu $P(0)$ und die Induktionsannahme (7.3) deckt sich mit (7.18). Mithin verallgemeinert das Beweisprinzip der fundierten Induktion das der vollständigen Induktion.

Induktiv definierte Ausdrücke

Sei A die Menge aller wie folgt induktiv definierten *Ausdrücke*:

- Jede Ziffer 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 ist ein Ausdruck.
- Sind E und F Ausdrücke, dann ist $E + F$ ein Ausdruck.
- Ist E ein Ausdruck, dann ist (E) ein Ausdruck.

Für beliebige Ausdrücke E und F besage $E \preceq F$, dass E ein Teilausdruck von F ist. Beispielsweise hat der Ausdruck $(1 + 2)$ die Teilausdrücke $(1 + 2)$, $1 + 2$, 1 und 2. Nach 7.9 ist das Paar $(A, \preceq)$ fundiert.

Satz 7.10. *Jeder Ausdruck in A enthält die gleiche Anzahl öffnender und schließender Klammern.*

Beweis. Für jeden Ausdruck E bezeichne $l(E)$ bzw. $r(E)$ die Anzahl der öffnenden bzw. schließenden Klammern in E. Wir beweisen, dass $l(E) = r(E)$ für jeden Ausdruck E in A gilt. Für jede Ziffer d gilt $l(d) = 0 = r(d)$. Seien E und F Ausdrücke. Für den Ausdruck $E + F$ gilt

$$l(E + F) = l(E) + l(F) = r(E) + r(F) = r(E + F),$$

wobei in der mittleren Gleichung die Induktionsannahme verwendet wurde. Für den Ausdruck (E) ergibt sich

$$l((E)) = l(E) + 1 = r(E) + 1 = r((E)),$$

wobei in der mittleren Gleichung die Induktionsannahme benutzt wurde. □

7.4 Schleifenprogrammierung

Die meisten Programmierfehler treten in `while`-Schleifen auf. Solche Schleifen lassen sich mithilfe der induktiven Methode korrekt programmieren. Eine `while`-Schleife hat die Form

```
while  B  do
S                                   (7.19)
od
```

Dabei ist B ein boolescher Ausdruck, d. h. ein Prädikat in den Programmvariablen, und S eine Folge von Anweisungen. In einer `while`-Schleife wird zuerst der Ausdruck B ausgewertet. Ist der Ausdruck falsch, dann terminiert die Schleife. Andernfalls wird der Rumpf S ausgeführt und der Prozess wiederholt. Jedes Durchlaufen des Rumpfs wird *Iteration* genannt. Die Semantik einer `while`-Schleife wird durch ein Hoare-Tripel spezifiziert. Um die Gültigkeit eines solchen Hoare-Tripels zu beweisen, wird eine *Schleifeninvariante* benutzt. Dies ist ein Prädikat P, das vor und nach jeder Iteration eine wahre Aussage liefert. Dieses so erweitere Hoare-Tripel ist gültig, wenn folgende Aussagen gelten:

- Das Prädikat P ist vor Eintritt in die Schleife wahr, d. h., es gilt das Hoare-Tripel

$$\{Q\} \quad \text{Initialisierungen} \quad \{P\}. \tag{7.20}$$

- Das Prädikat P ist eine Schleifeninvariante, d. h., es gilt das Hoare-Tripel

$$\{P \wedge B\} \quad S \quad \{P\}. \tag{7.21}$$

- Die Schleife terminiert.
- Sobald die Schleife beendet ist, gilt die Nachbedingung R, also

$$P \wedge \neg B \Rightarrow R. \tag{7.22}$$

Algorithmus 7.1 Division mit Rest

Eingabe: natürliche Zahlen a und $b > 0$
Ausgabe: natürliche Zahlen q und r mit $a = qb + r$ und $0 \leq r < b$

```
1: q := 0 {Vorbedingung Q: {a ≥ 0 ∧ b > 0}}
2: r := a
3: while r ≥ b do
4:     q := q + 1 {Invariante P: {a = qb + r ∧ r ≥ 0}}
5:     r := r − b
6: end while
7: return (q, r) {Nachbedingung R: {a = qb + r ∧ 0 ≤ r < b}}
```

Satz 7.11. *Das Hoare-Tripel in Algorithmus 7.1 ist gültig.*

Beweis. • Für das Hoare-Tripel $\{Q\}\ q, r := 0, a\ \{P\}$ ergibt sich als schwächste Vorbedingung

$$P[q, r := 0, a] = (a = 0 \cdot b + a \wedge a \geq 0).$$

Für die Vorbedingung Q ergibt sich

$$Q \Rightarrow P[q, r := 0, a].$$

Also ist das Hoare-Tripel $\{Q\}\ q, r := 0, a\ \{P\}$ gültig.

- Die schwächste Vorbedingung des Hoare-Tripels $\{P \wedge B\}\ S\ \{P\}$ lautet

$$\begin{aligned} P[q, r := q + 1, r - b] &= (a = (q + 1)b + (r - b) \wedge r - b \geq 0) \\ &= (a = qb + r \wedge r \geq b). \end{aligned}$$

Für die Vorbedingung $P \wedge B$ gilt aber

$$P \wedge B \Rightarrow P[q, r := q + 1, r - b].$$

Somit ist das Hoare-Tripel $\{P \wedge B\}\ S\ \{P\}$ gültig.

- In jeder Iteration wird r um $b > 0$ dekrementiert, so dass nach endlich vielen Iterationen $r < b$ erreicht wird. Folglich terminiert die Schleife.
- Es gilt

$$P \wedge \neg B = (a = qb + r \wedge r \geq 0 \wedge b < r).$$

Diese Aussage ist äquivalent zur Nachbedingung R. □

Selbsttestaufgaben

7.1. Wie lässt sich vollständige Induktion für eine Teilmenge $\{n_0, n_0 + 1, \ldots\}$ von $\mathbb{N}_0$ durchführen?

7.2. Beweise durch vollständige Induktion, dass für alle natürlichen Zahlen $n \geq 1$ gilt

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(n+2)}{6}.$$

7.3. Sei A eine Menge. Eine Relation auf A heißt *wohlgeordnet*, wenn jede nichtleere Teilmenge von A ein kleinstes Element besitzt. Zeige, dass jede wohlgeordnete Relation total geordnet ist.

7.4. Beweise, dass die Relation $\leq$ auf $\mathbb{N}_0$ wohlgeordnet ist.

7.5. Zeige, dass die Relation $\leq$ auf $\mathbb{N}_0$ fundiert ist.

7.6. Die Folge $(n!)$ wird induktiv definiert durch $0! = 1$ und $(n+1)! = (n+1)n!$ für alle $n \geq 0$. Zeige, dass für alle natürlichen Zahlen $n \geq 0$ gilt $n! = \prod_{i=1}^{n} i$.

7.7. Beweise, dass für alle natürlichen Zahlen $n \geq 3$ gilt $n! > 2^{n-1}$.

7.8. Sei $D = (V, E)$ ein Digraph und seien $u, v \in V$. Zeige, dass es zu jedem gerichteten Weg in D von u nach v einen einfachen gerichteten Weg von u nach v gibt.

7.9. Sei M eine Multimenge über der Menge der positiven reellen Zahlen. Auf M wird folgende Operation erklärt: Entferne zufällig zwei Zahlen x und y und füge deren Mittelwert $(x + y)/2$ zweifach wieder ein. Dieses Spiel terminiert, wenn alle Zahlen der Multimenge gleich sind. Terminiert dieses Spiel immer?

8

Unendliche Mengen

Es gibt unendliche Mengen, deren Elemente in Form eines Tabelle aufgelistet werden können, und es gibt unendliche Mengen, für die dies nicht gilt. Zu ersteren Mengen gehören die natürlichen, ganzen und rationalen Zahlen, zu letzteren die reellen Zahlen. Grundlegend für die Unterscheidung zwischen diesen Mengenarten waren die Arbeiten von Cantor. Dass die Menge der reellen Zahlen nicht tabellarisch aufgelistet werden kann, wirkt sich auf die Berechenbarkeit von reellen Zahlen aus.

8.1 Endliche und unendliche Mengen

Eine Menge A heißt *endlich*, wenn es eine natürliche Zahl n gibt, so dass die Abbildung $f : \underline{n} \to A$ bijektiv ist. Die Zahl n wird dann als *Mächtigkeit* von A bezeichnet. Gibt es keine derartige Bijektion, dann heißt A *unendlich*.

Satz 8.1. *Die Menge der natürlichen Zahlen $\mathbb{N}_0$ ist unendlich.*

Beweis. Sei n eine natürliche Zahl, so dass die Abbildung $f : \underline{n} \to \mathbb{N}_0$ injektiv ist. Dann hat der Wertebereich von f die Mächtigkeit n, weshalb f nicht surjektiv sein kann. □

Die Mächtigkeit von $\mathbb{N}_0$ wird mit $\aleph_0$, sprich "Aleph Null", bezeichnet.

Satz 8.2. *Zu jeder unendlichen Menge A gibt es eine injektive Abbildung $f : \mathbb{N}_0 \to A$.*

Beweis. Wir definieren eine Abbildung $f : \mathbb{N}_0 \to A$ induktiv:

- Wähle ein beliebiges Element $a_0 \in A$ und setze $f(0) = a_0$.
- Seien die Elemente $a_0, \ldots, a_{n-1} \in A$ schon gewählt, also $f(i) = a_i$ für $0 \leq i \leq n-1$. Wähle ein noch nicht ausgewähltes Element $a_n \in A$ und setze $f(n) = a_n$.

Die so definierte Abbildung f ist injektiv, weil jedes Element in A höchstens einmal zugeordnet wird. □

Satz 8.3. *Eine Menge A ist unendlich genau dann, wenn es eine injektive Abbildung gibt, die $\mathbb{N}_0$ auf eine echte Teilmenge von A abbildet.*

Beweis. Sei A eine unendliche Menge. Nach Satz 8.2 gibt es eine injektive Abbildung $f : \mathbb{N}_0 \to A$. Ist f nicht surjektiv, dann ist alles bewiesen. Andernfalls definieren wir eine Abbildung $g : A \to A \setminus \{f(0)\}$ durch

$$g(f(n)) = f(n+1) \quad \text{für alle } n \in \mathbb{N}_0.$$

Wir zeigen, dass g injektiv ist. Seien $a, b \in A$ mit $g(a) = g(b)$. Da f surjektiv ist, existieren $m, n \in \mathbb{N}_0$ mit $f(m) = a$ und $f(n) = b$. Folglich gilt

$$f(m+1) = g(f(m)) = g(a) = g(b) = g(f(n)) = f(n+1).$$

Weil f injektiv ist, folgt $m = n$ und somit $a = b$. Also ist g injektiv. Die gesuchte Abbildung, $gf : \mathbb{N}_0 \to A$, ist nach Satz 6.6 injektiv, aber wegen $f(0) \notin \operatorname{ran}(gf)$ nicht surjektiv. Die umgekehrte Aussage ist klar. □

Zwei Mengen A und B heißen *gleichmächtig*, kurz $|A| = |B|$, wenn es eine bijektive Abbildung $f : A \to B$ gibt. Die Gleichmächtigkeit von Mengen ist eine Äquivalenz auf der Klasse aller Mengen.

8.2 Abzählbare und überabzählbare Mengen

Eine Menge A heißt *abzählbar*, wenn A gleichmächtig ist zur Menge der natürlichen Zahlen. Eine Menge A heißt *überabzählbar*, wenn A weder endlich noch abzählbar ist.

Abzählbare Mengen

Satz 8.4. *Die Menge $\mathbb{N}_0$ ist abzählbar.*

Beweis. Die identische Abbildung $id_{\mathbb{N}_0}$ ist bijektiv. □

Satz 8.5. *Die Menge $\mathbb{N}$ ist abzählbar.*

Beweis. Die Nachfolgerabbildung $S : \mathbb{N}_0 \to \mathbb{N} : n \mapsto n+1$ ist bijektiv. □

Satz 8.6. *Die Menge der ganzen Zahlen ist abzählbar.*

Beweis. Eine bijektive Abbildung $f : \mathbb{N}_0 \to \mathbb{Z}$ wird definiert durch

$$f(n) = \begin{cases} -n/2 & \text{falls } n \text{ gerade,} \\ (n+1)/2 & \text{sonst.} \end{cases}$$

Einige Werte dieser Abbildung zeigt die folgende Tabelle

n	0	1	2	3	4	5	...
$f(n)$	0	1	−1	2	−2	3	...

□

Satz 8.7. *Die Menge der rationalen Zahlen ist abzählbar.*

Beweis. Wir verwenden die *erste Diagonalmethode* von Cantor. Hierzu werden alle Brüche p/q, $p \in \mathbb{Z}$ und $q \in \mathbb{N}$, in einem 2-dimensionalen Schema angeordnet

$$
\begin{array}{llllll}
0/1 & 1/1 & -1/1 & 2/1 & -2/1 & 3/1 \ -3/1 \ \ldots \\
0/2 & 1/2 & -1/2 & 2/2 & -2/2 & 3/2 \ -3/2 \ \ldots \\
0/3 & 1/3 & -1/3 & 2/3 & -2/3 & 3/3 \ -3/3 \ \ldots \\
0/4 & 1/4 & -1/4 & 2/4 & -2/4 & 3/4 \ -3/4 \ \ldots \\
0/5 & 1/5 & -1/5 & 2/5 & -2/5 & 3/5 \ -3/5 \ \ldots \\
\ldots
\end{array}
$$

Die Brüche werden mit dem Bruch $0/1$ beginnend im Zickzack durchlaufen: (1) ein Schritt nach rechts, (2) diagonal bis zum linken Rand, (3) ein Schritt nach unten und (4) diagonal bis zum oberen Rand. Hierbei werden Brüche überschlagen, wenn sie zu früher schon durchlaufenen Brüchen gleichwertig sind. Dadurch resultiert eine bijektive Abbildung $f : \mathbb{N}_0 \to \mathbb{Q}$, die in folgender Tabelle angedeutet ist

n	0	1	2	3	4	5	6	7	8	9	10	...
$f(n)$	0	1	1/2	−1	2	−1/2	1/3	1/4	−1/3	−2	3	...

□

Satz 8.8. *Die Menge aller Wörter über einem endlichen Alphabet ist abzählbar.*

Beweis. Sei A eine endliche Menge. Sei B die Menge aller Wörter über A und B_i die Menge aller Wörter über A mit der Länge i. Die Mengen B_i sind endlich und bilden eine Partition von B. Seien $b_{i1}, b_{i2} \ldots, b_{im_i}$ die Elemente von B_i. Dann ist die Abbildung $f : A \to \mathbb{N}_0$, definiert durch $b_{ij} \mapsto m_0 + \ldots + m_{i-1} + j$, bijektiv. □

Satz 8.9. *Die Menge aller endlichen Folgen mit Einträgen aus einer abzählbaren Menge ist abzählbar.*

Beweis. O.B.d.A. betrachten wir die abzählbare Menge $\mathbb{N}$. Die Folge der Primzahlen $(p_n) = (2, 3, 5, 7, 11, \ldots)$ ist nach Satz 13.16 unendlich. Anhand dieser Folge wird eine Abbildung $f : \text{seq}(\mathbb{N}) \to \mathbb{N}$ von der Menge aller endlichen Folgen mit Einträgen aus $\mathbb{N}$ nach $\mathbb{N}$ durch $(i_1, \ldots, i_n) \mapsto p_1^{i_1} \cdots p_n^{i_n}$ definiert. Beispielsweise gilt $f(\epsilon) = 1$ und $f(121) = 2^1 3^2 5^1 = 90$. Nach Satz 13.15 ist jede natürliche Zahl eindeutig als Produkt von Primzahlen darstellbar. Somit ist f bijektiv. □

Überabzählbare Mengen

Satz 8.10. *Das abgeschlossene reellwertige Intervall* $[0,1]$ *ist überabzählbar.*

Beweis. Wir benutzen die *zweite Diagonalmethode* von Cantor. Angenommen, es gäbe eine bijektive Abbildung $f : \mathbb{N} \to [0,1]$, die jeder natürlichen Zahl n eine reelle Zahl $f(n) = r^{(n)} \in [0,1]$ zuordnete. Jede Zahl $r^{(n)}$ besitzt eine Dezimalbruchentwicklung

$$r^{(n)} = 0.r_1^{(n)} r_2^{(n)} r_3^{(n)} \ldots, \quad r_i^{(n)} \in \{0, \ldots, 9\}.$$

Mithilfe dieser Dezimalbrüche wird ein Dezimalbruch $x = 0.x_1x_2x_3\ldots$ wie folgt festgelegt

$$x_n = \begin{cases} 1 \text{ falls } r_n^{(n)} \text{ gerade,} \\ 0 \text{ sonst.} \end{cases}$$

Die Dezimalbruch x liegt in $[0,1]$, kommt aber in der durch f festgelegten Aufzählung nicht vor, weil sich x von $r^{(n)}$ an der n-ten Nachkommastelle $r_n^{(n)}$ unterscheidet. Also ist f widersprüchlicherweise nicht bijektiv. □

Die zweite Diagonalmethode von Cantor zeigt, dass in jeder Liste von reellen Zahlen wenigstens eine reelle Zahl nicht vorkommt. Angenommen, die Liste begänne wie folgt

$$\begin{aligned} r^{(1)} &= 0.\ \mathbf{3}\ 5\ 6\ 2\ldots \\ r^{(2)} &= 0.\ 2\ \mathbf{2}\ 0\ 9\ldots \\ r^{(3)} &= 0.\ 4\ 6\ \mathbf{7}\ 8\ldots \\ r^{(4)} &= 0.\ 7\ 3\ 0\ \mathbf{6}\ldots \\ &\ldots \end{aligned}$$

Dann würde gemäß des obigen Beweises folgende Zahl in der Liste fehlen

$$x = 0.\ 0\ 1\ 0\ 1\ldots$$

Satz 8.11. *Das offene reellwertige Intervall* $(0,1)$ *ist überabzählbar.*

Beweis. Es genügt zu zeigen, dass die Intervalle $(0,1)$ und $[0,1]$ gleichmächtig sind. Hierzu werden zwei unendliche Folgen

$$\begin{aligned} F &= (0, 1, 1/2, 1/3, 1/4, 1/5, \ldots) \\ G &= (1/2, 1/3, 1/4, 1/5, \ldots) \end{aligned}$$

benutzt, wobei F gegenüber G zwei zusätzliche Anfangsglieder enthält. Es gibt definitionsgemäß eine Menge A, so dass $[0,1] = F \cup A$ und $(0,1) = G \cup A$. Die Abbildung $f : [0,1] \to (0,1)$, definiert durch

$$f(x) = \begin{cases} 1/2 & \text{falls } x = 0, \\ 1/(n+2) & \text{falls } x = 1/n \text{ für ein } n \in \mathbb{N}, \\ x & \text{sonst,} \end{cases}$$

bildet alle Elemente von A auf sich ab und das n-te Glied von F auf das n-te Glied von G. Also ist f bijektiv. □

Satz 8.12. *Die Menge der reellen Zahlen ist überabzählbar.*

Beweis. Die Abbildung $f : (0,1) \to \mathbb{R} : x \mapsto \tan(\pi x - \pi/2)$ ist bijektiv. □

Satz 8.13. *Die Potenzmenge der Menge der natürlichen Zahlen ist überabzählbar.*

Beweis. Jedes Element A in $P(\mathbb{N}_0)$ wird durch einen Binärbruch $0.a_0a_1a_2a_3\ldots$ codiert, wobei

$$a_n = \begin{cases} 1 \text{ falls } n \in A, \\ 0 \text{ sonst.} \end{cases} \tag{8.1}$$

Mit der zweiten Diagonalmethode von Cantor folgt die Behauptung. □

Satz 8.14. *Die Menge der reellen Zahlen und die Potenzmenge der Menge der natürlichen Zahlen sind gleichmächtig.*

Beweis. Jede Zahl in $[0,1]$ ist durch einen Binärbruch darstellbar. Ebenso ist jedes Element A in $P(\mathbb{N}_0)$ vermöge eines Binärbruchs gemäß (8.1) codierbar. Die Abbildung $f : [0,1] \to P(\mathbb{N}_0)$, die jeder Zahl in $[0,1]$ diejenige Teilmenge von $\mathbb{N}_0$ zuordnet, die dieselbe Binärbruch-Codierung besitzt, ist bijektiv. □

Überabzählbarkeit ad infinitum

Seien A und B Mengen. Wir schreiben $|A| \leq |B|$, wenn es eine injektive Abbildung $f : A \to B$ gibt. Wir schreiben $|A| < |B|$, wenn es eine injektive Abbildung $f : A \to B$ gibt, die nicht surjektiv ist.

Satz 8.15. *Für jede Menge A gilt $|A| < |P(A)|$.*

Beweis. Die Abbildung $f : A \to P(A) : x \mapsto \{x\}$ ist injektiv. Also ist $|A| < |P(A)|$.

Wir zeigen noch, dass keine injektive Abbildung $f : A \to P(A)$ auch surjektiv sein kann. Sei $f : A \to P(A)$ injektiv. Wir betrachten die Menge $B = \{b \mid b \in A, a \notin f(a)\}$. Angenommen, es gäbe ein $b \in A$ mit $f(b) = B$. Die Aussage $b \in B$ ist per definitionem gleichbedeutend mit $b \notin f(b)$, die wiederum widersprüchlicherweise zu $b \notin B$ äquivalent ist. Also liegt B nicht im Wertebereich von f. Somit ist f nicht surjektiv. □

Der letzte Satz zeigt, dass es eine unendliche Folge von unendlichen Mengen mit echt aufsteigender Mächtigkeit gibt

$$|\mathbb{N}_0| < |P(\mathbb{N}_0)| < |P(P(\mathbb{N}_0))| < \ldots \tag{8.2}$$

Die *Kontinuumshypothese* besagt, dass es keine Menge gibt, deren Mächtigkeit zwischen $|\mathbb{N}_0|$ und $|P(\mathbb{N}_0)| = |\mathbb{R}|$ liegt.

8.3 Berechenbarkeit

Die Abzählbarkeit von Mengen hat wichtige Konsequenzen für die Informatik. Wir betrachten eine typische Programmiersprache L. Das Alphabet A der Zeichen, um ein Programm in der Sprache L zu schreiben, ist endlich. Jedes Programm in der Sprache L ist ein Wort über A. Also ist die Menge aller Programme in der Sprache L nach Satz 8.8 abzählbar.

Wir betrachten Programme in der Sprache L, deren Zweck es ist, eine reelle Zahl zu drucken. Im Allgemeinen kann eine reelle Zahl nicht wirklich durch ein Programm berechnet werden, weil ein Programm nach endlich vielen Schritten terminiert, während eine reelle Zahl unendlich viele Nachkommastellen besitzt.

Eine reelle Zahl $r = 0.r_1r_2r_3\ldots$ heißt *berechenbar* in der Sprache L, wenn es ein Programm in L gibt, das bei Eingabe einer natürlichen Zahl $n \geq 0$ eine Approximation von r in Form der ersten n Nachkommastellen $r_1, r_2, \ldots, r_n$ liefert. Auf diese Weise kann eine berechenbare reelle Zahl beliebig genau approximiert werden.

Sind alle reellen Zahlen berechenbar? Einerseits gibt es nach obiger Überlegung abzählbar viele Programme in der Sprache L und andererseits überabzählbar viele reelle Zahlen. Also sind nicht alle reellen Zahlen berechenbar.

Selbsttestaufgaben

8.1. Sei A eine abzählbare Menge und n eine natürliche Zahl. Zeige, dass A^n abzählbar ist.

8.2. Sei $A_1, A_2, \ldots$ eine abzählbare Anzahl von endlichen Mengen. Zeige, dass $\bigcup_i A_i$ abzählbar ist.

8.3. Beweise, dass eine abzählbare Vereinigung von abzählbaren Mengen abzählbar ist.

8.4. Sei P die Menge aller Polynome $p(x) = a_0 + a_1x + \ldots + a_nx^n$ mit ganzzahligen Koeffizienten $a_0, \ldots, a_n$. Zeige, dass P abzählbar ist.

8.5. Eine reelle Zahl r heißt *algebraisch*, wenn r eine Lösung einer polynomialen Gleichung $p(x) = a_0+a_1x+\ldots+a_nx^n = 0$ mit ganzzahligen Koeffizienten $a_0, \ldots, a_n$ ist. Zeige, dass die Menge aller algebraischen Zahlen abzählbar ist.

Teil II

Elementare Kombinatorik

9

Zählprinzipien

Zählprinzipien sind grundlegend für den Aufbau der Kombinatorik. Dazu gehören das Gleichheits-, Additions- und Multiplikationsprinzip, das Prinzip der doppelten Abzählung und das Prinzip der Inklusion-Exklusion. Mit dem Schubfachprinzip wird auch ein kombinatorisches Existenzprinzip behandelt. Alle Mengen in diesem Kapitel werden als endlich vorausgesetzt.

9.1 Elementare Zählprinzipien

Satz 9.1. (Gleichheitsprinzip) *Zwei Mengen A und B sind gleichmächtig, wenn es eine bijektive Abbildung $f : A \to B$ gibt.*

Der Beweis folgt direkt aus der Definition.

Satz 9.2. *Für disjunkte Mengen A und B gilt*

$$|A \cup B| = |A| + |B|. \tag{9.1}$$

Beweis. Seien $A = \{a_1, \ldots, a_m\}$ und $B = \{b_1, \ldots, b_n\}$ disjunkte Mengen. Dann gilt $A \cup B = \{a_1, \ldots, a_m, b_1, \ldots, b_n\}$ und folglich $|A| + |B| = m + n = |A \cup B|$. □

Mit vollständiger Induktion nach n ergibt sich der folgende

Satz 9.3. (Additionsprinzip) *Für paarweise disjunkte Mengen $A_1, \ldots, A_n$ gilt*

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i| \,. \tag{9.2}$$

9.2 Prinzip der doppelten Abzählung

Sei R eine Relation von $A = \{a_1, \ldots, a_m\}$ nach $B = \{b_1, \ldots, b_n\}$. Die Adjazenzmatrix $M_R = (m_{ij})$ von R ist eine $m \times n$-Matrix mit

$$m_{ij} = \begin{cases} 1 \text{ falls } a_i R b_j, \\ 0 \text{ sonst.} \end{cases} \tag{9.3}$$

Die Mächtigkeit von R entspricht der Anzahl der Einsen in M_R. Die Anzahl der Einsen in M_R kann durch zeilen- und spaltenweises Summieren ermittelt werden,

$$\sum_{i=1}^{m} r_i(R) = |R| = \sum_{j=1}^{n} c_j(R), \tag{9.4}$$

wobei $r_i(R)$ bzw. $c_j(R)$ die Anzahl der Einsen in der i-ten Zeile bzw. j-ten Spalte von M_R angibt.

Beispiel 9.4. An einer Vorlesung über "Diskrete Mathematik" nehmen 32 männliche Hörer teil. Jeder Student ist mit 5 Studentinnen befreundet und jede Studentin mit 8 Studenten. Wie viele Studentinnen besuchen die Vorlesung?

Diese Frage wird mit dem Prinzip der doppelten Abzählung beantwortet. Sei A die Menge aller Studenten und B die Menge aller Studentinnen in der Vorlesung. Sei R die "*Freundschaftsrelation*" zwischen männlichen und weiblichen Hörern der Vorlesung, d. h., xRy bedeutet, dass "*Student x mit Studentin y befreundet ist*". Die Adjazenzmatrix von R besteht aus $|A| = 32$ Zeilen und $n = |B|$ Spalten. Sie hat 5 Einseinträge pro Zeile und 8 Einseinträge pro Spalte. Also folgt durch zeilen- und spaltenweises Abzählen

$$32 \cdot 5 = \sum_{i=1}^{32} r_i(R) = |R| = \sum_{j=1}^{n} c_j(R) = n \cdot 8.$$

Die Vorlesung wird also von $n = 20$ Studentinnen besucht.

Multiplikationsprinzip

Seien A und B Mengen. Die Adjazenzmatrix der Allrelation $R = A \times B$ ist mit Einsen voll besetzt, d. h. jede Zeile hat $|B|$ Einsen und jede Spalte $|A|$ Einsen. Mit dem Prinzip der doppelten Abzählung folgt

$$|A \times B| = |A| \cdot |B|. \tag{9.5}$$

Mit vollständiger Induktion nach n ergibt sich der folgende

Satz 9.5. (Multiplikationsprinzip) *Für beliebige Mengen $A_1, \ldots, A_n$ gilt*

$$\left| \prod_{i=1}^{n} A_i \right| = \prod_{i=1}^{n} |A_i| \,. \tag{9.6}$$

Beispiel 9.6. Die Autokennzeichen für Nürnberg-Stadt `N-XY-ZZZ` bestehen aus einem Buchstabenbigramm `XY` und einer ein- bis dreistelligen Zahl `ZZZ`. Für die Anzahl dieser Autokennzeichen gilt nach dem Additions- und Multiplikationsprinzip $26 \cdot 26 \cdot [9 + 9 \cdot 10 + 9 \cdot 10 \cdot 10] = 675\,324$.

9.3 Schubfachprinzip

Das Schubfachprinzip ist ein kombinatorisches Existenzprinzip, das von P.G. Lejeune-Dirichlet (1805-1859) eingeführt wurde.

Proposition 9.7. (Schubfachprinzip) *Wenn $k + 1$ Kugeln auf k Fächer verteilt werden, dann enthält mindestens ein Fach zwei oder mehr Kugeln.*

Beispiel 9.8. In einem Basketball-Turnier spielen zehn Mannschaften um den Sieg, wobei jede Mannschaft einmal gegen jede andere Mannschaft anzutreten hat. Wir behaupten, dass nach dem ersten Spieltag mindestens zwei Mannschaften die gleiche Anzahl von Spielen absolviert haben.

Sei $A = \{a_1, \ldots, a_n\}$ die Menge aller teilnehmenden Mannschaften. Die Abbildung $f : A \to \{0, \ldots, n-1\}$ ordnet jeder Mannschaft $a \in A$ die Anzahl $f(a)$ ihrer Spiele am ersten Tag zu. Es ergeben sich drei Fälle:

- Es gibt eine Mannschaft a, die am ersten Tag kein Spiel absolviert hat, d. h., $f(a) = 0$. Dann gibt es keine Mannschaft, die am ersten Tag gegen alle anderen Mannschaften gespielt hat, d. h., $f(A) \subseteq \{0, \ldots, n-2\}$.
- Es gibt eine Mannschaft a, die am ersten Tag gegen alle anderen Mannschaften gespielt hat, d. h., $f(a) = n-1$. Dann existiert keine Mannschaft, die am ersten Tag kein Spiel absolviert hat, d. h., $f(A) \subseteq \{1, \ldots, n-1\}$.
- Ansonsten hat jede Mannschaft am ersten Tag mindestens ein und höchstens $n-2$ Spiele absolviert, d. h., $f(A) \subseteq \{1, \ldots, n-2\}$.

Der Wertebereich $f(A)$ von f hat also die Mächigkeit $\leq n-1$. Die Mannschaften werden als Kugeln und die Anzahl der absolvierten Spiele als Fächer interpretiert. Mit dem Schubfachprinzip folgt die Behauptung.

9.4 Prinzip der Inklusion-Exklusion

Für beliebige Mengen A und B gilt

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{9.7}$$

Denn die im Durchschnitt von A und B liegenden Elemente werden in der Partialsumme $|A|+|B|$ doppelt gezählt und werden deshalb einmal abgezogen.

Für beliebige Mengen A, B und C gilt

$$\begin{aligned}|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| \\ +|A \cap B \cap C|.\end{aligned} \tag{9.8}$$

Denn in $|A| + |B| + |C|$ werden die im Durchschnitt zweier Mengen enthaltenen Elemente doppelt und die im Durchschnitt aller drei Mengen liegenden Elemente dreimal gezählt. Wird davon $|A \cap B| + |A \cap C| + |B \cap C|$ subtrahiert, so werden die im Durchschnitt je zweier Mengen enthaltenen Elemente richtig gezählt. Die im Durchschnitt aller Mengen liegenden Elemente werden in $|A| + |B| + |C|$ dreimal gezählt und in $|A \cap B| + |A \cap C| + |B \cap C|$ dreimal abgezogen, weshalb noch $|A \cap B \cap C|$ hinzuzuaddieren ist. Von diesem Ein- und Ausschließen von Mengen rührt der Name des Prinzips her.

Satz 9.9. (Inklusion-Exklusion) *Für beliebige Mengen $A_1, \ldots, A_n$ gilt*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\substack{I \subseteq \underline{n} \\ I \neq \emptyset}} (-1)^{|I|-1} \left|\bigcap_{j \in I} A_j\right|. \tag{9.9}$$

Beweis. Die Summanden auf der rechten Seite werden entsprechend ihrer Mächtigkeit geordnet

$$\sum_{\substack{I \subseteq \underline{n} \\ I \neq \emptyset}} (-1)^{|I|-1} \left|\bigcap_{j \in I} A_j\right| = \sum_{l=1}^{n} (-1)^{l-1} \sum_{\substack{I \subseteq \underline{n} \\ |I|=l}} \left|\bigcap_{j \in I} A_j\right|. \tag{9.10}$$

Sei $a \in A$ in $A_{i_1}, \ldots, A_{i_k}$ enthalten. Dann ist der Beitrag von a zur Summe

$$\sum_{\substack{I \subseteq \underline{n} \\ |I|=l}} \left|\bigcap_{j \in I} A_j\right| \tag{9.11}$$

gleich dem Beitrag von a zur Summe

$$\sum_{\substack{I \subseteq \{i_1, \ldots, i_k\} \\ |I|=l}} \left|\bigcap_{j \in I} A_j\right|. \tag{9.12}$$

In dieser Summe trägt a Eins in jedem Summanden bei. D. h., der Beitrag von a ist gleich der Anzahl der l-elementigen Teilmengen I von $\{i_1, \ldots, i_k\}$. Nach (10.1) ist diese Anzahl gleich $\binom{k}{l}$. Also ist der Beitrag von a zur Summe (9.10) gleich

$$\sum_{l=1}^{n}(-1)^{l-1}\binom{k}{l} = \sum_{l=1}^{k}(-1)^{l-1}\binom{k}{l}. \tag{9.13}$$

Nach (10.6) ist aber

$$\sum_{l=0}^{k}(-1)^{l}\binom{k}{l} = 0. \tag{9.14}$$

Also hat die Summe (9.13) den Wert $\binom{k}{0} = 1$, d. h., a trägt Eins zur rechten Seite der behaupteten Gleichung bei. Ebenso liefert a den Beitrag Eins zur linken Seite der behaupteten Gleichung. □

Korollar 9.10. (Siebprinzip) *Seien $A_1, \ldots, A_n$ Teilmengen einer Menge A. Für die Anzahl der Elemente in A, die in keiner der Teilmengen $A_1, \ldots, A_n$ enthalten sind, gilt*

$$|A \setminus (\bigcup_{i=1}^{n} A_i)| = |A| - \sum_{\substack{I \subseteq n \\ I \neq \emptyset}} (-1)^{|I|-1} \left| \bigcap_{j \in I} A_j \right|. \tag{9.15}$$

Beispiel 9.11. Wie viele natürliche Zahlen zwischen 1 und 1000 gibt es, die nicht durch 2, 3 oder 5 teilbar sind? Sei $A = \{1, 2, \ldots, 1000\}$ und sei A_n die Menge aller ganzzahligen Vielfachen einer natürlichen Zahl n in A. Es gilt

$$A_n = \{m \cdot n \mid 1 \leq m \leq \lfloor \frac{1000}{n} \rfloor\}, \tag{9.16}$$

wobei $\lfloor x \rfloor$ die größte ganze Zahl bezeichnet, die kleiner oder gleich $x \in \mathbb{R}$ ist. Für die Mächtigkeit von A_n gilt also

$$|A_n| = \lfloor \frac{1000}{n} \rfloor. \tag{9.17}$$

Mit der Siebformel folgt

$$\begin{aligned} |A \setminus (A_2 \cup A_3 \cup A_5)| &= |A| - [|A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| \\ &\quad -|A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|] \\ &= |A| - |A_2| - |A_3| - |A_5| + |A_6| + |A_{10}| + |A_{15}| - |A_{30}| \\ &= 1000 - 500 - 333 - 200 + 166 + 100 + 66 - 33 = 266. \end{aligned}$$

Somit lautet die Antwort: 266.

Einen wichtigen Spezialfall der Siebformel birgt der folgende

Satz 9.12. *Seien $a_1, \ldots, a_n$ natürliche Zahlen, so dass für jede nichtleere Teilmenge I von $\underline{n}$ gilt*

$$a_{|I|} = \left| \bigcap_{j \in I} A_j \right|. \tag{9.18}$$

Dann gilt

$$\left| A \setminus (\bigcup_{i=1}^{n} A_i) \right| = |A| + \sum_{i=1}^{n} (-1)^i \binom{n}{i} a_i. \tag{9.19}$$

Beweis. Es gilt

$$\begin{aligned}
\left| A \setminus (\bigcup_{i=1}^{n} A_i) \right| &= |A| - \sum_{\substack{I \subseteq \underline{n} \\ I \neq \emptyset}} (-1)^{|I|-1} \left| \bigcap_{j \in I} A_j \right|, \quad \text{nach (9.15)} \\
&= |A| - \sum_{i=1}^{n} \sum_{\substack{I \\ |I|=i}} (-1)^{i-1} a_i, \quad \text{nach (9.18)} \\
&= |A| - \sum_{i=1}^{n} \binom{n}{i} (-1)^{i-1} a_i, \quad \text{nach (10.1)} \\
&= |A| + \sum_{i=1}^{n} \binom{n}{i} (-1)^{i} a_i.
\end{aligned}$$

□

Anwendungen der vereinfachten Siebformel (9.19) werden wir im nächsten Kapitel kennen lernen.

Selbsttestaufgaben

9.1. Sei M ein aus 4-Teilmengen der Menge $\underline{8}$ bestehendes Mengensystem mit der Eigenschaft, dass jedes ganze Zahl zwischen 1 und 8 in genau drei Elementen der Menge M enthalten ist. Bestimme die Mächtigkeit von M.

9.2. Gibt es ein aus 3-elementigen Teilmengen von $\underline{8}$ bestehendes Mengensystem M mit der Eigenschaft, dass jede Zahl zwischen 1 und 8 in genau fünf Elementen der Menge M liegt?

9.3. Zeige, dass es in jeder mindestens zweielementigen Menge von Personen mindestens zwei Personen gibt, die die gleiche Anzahl von Freunden in diesem Personenkreis haben.

9.4. Zeige, dass es in jeder 5-elementigen Teilmenge von $\underline{8}$ mindestens zwei Zahlen gibt, deren Summe 9 ist.

9.5. Bestimme die Anzahl der natürlichen Zahlen im Bereich 1 bis 1000, die nicht durch 5, 12 oder 20 teilbar sind.

9.6. Die 50 Teilnehmer eines Seminars wurden nach der Beherrschung der Fremdsprachen Englisch, Französisch und Russisch befragt. Dabeit ergaben sich folgende Ergebnisse:

- 27 können Englisch,
- 15 können Französisch,
- 10 können Russisch,
- 14 können nur Englisch,
- 8 können nur Französisch,
- 3 können nur Russisch.

Bestimme daraus die Anzahl der Teilnehmer, die keine der drei Sprachen beherrschen.

9.7. Die Anzahl der r-elementigen Teilmengen einer n-elementigen Menge, die eine feste m-elementige Menge enthalten, ist bekanntlich $\binom{n-m}{r-m}$. Folgere hieraus mit Hilfe des Prinzips der Inklusion-Exklusion

$$\binom{n-m}{r-m} = \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{n-i}{r}.$$

9.8. In 32 Haushalten werden Papier oder Flaschen oder beides (zu Zwecken des Recyclings) gesammelt. 30 Haushalte sammeln Papier und 14 sammeln Flaschen. Wie viele Haushalte sammeln Papier und Flaschen, wie viele sammeln nur Papier und wie viele sammeln nur Flaschen?