Mathematisches Arbeiten für Informatik und Wirtschaftsinformatik

Stefan Hetzl
stefan.hetzl@tuwien.ac.at

TU Wien

WS 2025/26

Version vom 11. Dezember 2025

Vorwort

Dieses Skriptum begleitet die an der TU Wien gehaltene Lehrveranstaltung *Mathematisches Arbeiten für Informatik und Wirtschaftsinformatik*, in der elementare mathematische Methodik vermittelt wird. Nach einer Einführung in die Aussagen- und Prädikatenlogik werden die für die Mathematik zentralen Begriffe der Definition und des Beweises besprochen. In weiterer Folge werden elementare Aspekte des mathematischen Arbeitens durchgenommen, wie z.B. die Mengennotation, der Umgang mit Gleichungen und Ungleichungen, Induktionsbeweise, Abstraktionen und das Arbeiten mit Vermutungen.

Der mathematische Inhalt dieses Skriptums beschränkt sich auf einige wenige grundlegende Begriffe der elementaren Zahlentheorie sowie einzelne wichtige Klassen binärer Relationen. Der intendierte Zweck dieser inhaltlichen Sparsamkeit ist es, die Konzentration auf die Methodik zu erleichtern.

Die folgende Literatur kann als Ergänzung zu diesem Skriptum bzw. zu dieser Lehrveranstaltung empfohlen werden: [4] mit der zugehörigen Webseite auf der auch einige gut gestaltete Videos zu finden sind sowie das Skriptum [6] werden für Einführungen in das mathematische Arbeiten für Studenten der Mathematik verwendet. Ein empfehlenswertes englischsprachiges Lehrbuch zum Übergang von der Schulmathematik zur Universitätsmathematik ist [5]. [1] bietet nützliche Erklärungen zu vielen Aspekten der mathematischen Sprache und Notation. Ein Klassiker zum mathematischen Arbeiten ist [3], ein deutschsprachiges und aktuelleres Buch mit ähnlicher Zielsetzung wie [3] ist [2].

Inhaltsverzeichnis

Kapitel 1

Aussagen

Eine **Aussage** ist ein Satz, dem man einen objektiven Wahrheitswert zuweisen kann, der entweder *wahr* oder *falsch* ist. Wir identifizieren den Wahrheitswert *wahr* mit der Zahl 1 und *falsch* mit 0. Einige Beispiele von Aussagen und ihren Wahrheitswerten sind:

Aussage	Wahrheitswert
Wale sind Säugetiere.	1
$2+2=4$	1
10 *ist eine Primzahl.*	0
4 *ist größer als* 3.	1

Bei einer Aussage muss es sich also um einen ganzen Satz, z.B. der deutschen Sprache, handeln. So ist etwa "*Zwei plus zwei ist fünf.*" eine Aussage, "*zwei plus zwei*" aber nicht.

"*Hoffentlich regnet es bald.*" oder "*Lesen Sie das Skriptum.*" sind zwar Sätze der deutschen Sprache, aber keine Aussagen in unserem Sinn da ihnen kein Wahrheitswert zugewiesen werden kann.

Ein weiteres wichtiges Element dieser Definition ist die Objektivität. Es gibt zwar viele interessante Aussagen denen kein objektiver Wahrheitswert zugewiesen werden kann, wie z.B. "*Avocado schmeckt gut.*", aber solche Aussagen sind nicht Gegenstand der Mathematik und deshalb schließen wir sie hier aus.

Weiters ist es für die Frage ob ein Satz eine Aussage ist unerheblich ob der Wahrheitswert bekannt ist. So ist z.B. auch der folgende Satz eine Aussage

"*Jede gerade Zahl die größer gleich* 4 *ist kann als Summe zweier Primzahlen geschrieben werden.*"

Diese Aussage ist auch als Goldbachsche Vermutung bekannt. Es ist in der Mathematik nicht bekannt ob diese Aussage wahr oder falsch ist. Eine Aussage ist es trotzdem weil ihr ein objektiver Wahrheitswert zugewiesen werden kann, auch wenn niemand weiß welcher es ist.

Es gibt eine Reihe von Möglichkeiten um Aussagen zu verknüpfen und daraus neue Aussagen zu erhalten.

Konjunktion (und-Verknüpfung). Falls A und B Aussagen[1] sind, so ist auch $A \wedge B$ (ausgesprochen als "A und B") eine Aussage. Wir sagen auch dass $A \wedge B$ die Konjunktion von A und B ist und dass die Aussagen A und B die Konjunkte von $A \wedge B$ sind. Die Aussage $A \wedge B$ ist wahr genau dann

[1] In der Mathematik verwendet man gerne Buchstaben die daran erinnern wofür sie stehen, z.B. A, B, ... für Aussagen weil das Wort "Aussage" mit einem A beginnt.

wenn sowohl A wahr ist als auch B wahr ist. Die Bedeutung der Konjunktion kann durch die folgende **Wahrheitstafel** definiert werden. Auf der linken Seite werden alle (vier) Möglichkeiten für die Wahrheitswerte von A und B eingetragen. Auf der rechten Seite wird, für jede dieser Möglichkeiten, der Wahrheitswert von $A \wedge B$ eingetragen.

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

Warnung 1.1. Das Symbol $\wedge$ darf nicht auf naive Weise als Abkürzung des Wortes "und" benutzt werden. So kann z.B. die Aussage "*x und y sind größer als* 0" nicht geschrieben werden als $x \wedge y > 0$ da $x \wedge y$ keine Zahl ist. Richtig ist stattdessen: $x > 0 \wedge y > 0$. Ähnliches gilt für die im Weiteren vorgestellten Verknüpfungen auch.

Disjunktion (oder-Verknüpfung). Falls A und B Aussagen sind, so ist auch $A \vee B$ (ausgesprochen als "A oder B") eine Aussage[2]. Die Aussage $A \vee B$ heißt Disjunktion von A und B und die Aussagen A und B heißen Disjunkte von $A \vee B$. Die Aussage $A \vee B$ ist wahr genau dann wenn A wahr, wenn B wahr ist oder wenn sowohl A als auch B wahr sind. Durch eine Wahrheitstafel kann das wie folgt dargestellt werden:

A	B	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

Es handelt sich dabei also um eine inklusive Disjunktion, d.h. falls beide Disjunkte wahr sind ist auch die Disjunktion wahr. Bei einer exklusive Disjunktion wäre in diesem Fall die Disjunktion falsch. In der Alltagssprache wird das Wort "oder" sowohl für inklusive als auch für exklusive Disjunktion verwendet wie der folgende Dialog veranschaulicht:

> *Kellner: Wollen Sie Kaffee oder Tee? (exklusives oder)*
>
> *Gast: Kaffee bitte.*
>
> *Kellner: Wollen Sie Zucker oder Milch dazu? (inklusives oder)*
>
> *Gast: Beides, danke.*

In der Mathematik werden wir mit "oder" immer das inklusive oder meinen.

Negation (Verneinung). Falls A eine Aussage ist, dann ist auch $\neg A$ (ausgesprochen als "nicht A") eine Aussage. Die Aussage $\neg A$ heißt auch Negation oder Verneinung von A und ist wahr wenn A falsch ist und umgekehrt, siehe folgende Wahrheitstafel:

A	$\neg A$
0	1
1	0

[2] Das Symbol $\vee$ kommt vom lateinischen Wort *vel* (oder).

Die Verneinung wird dabei in einem streng logischen Sinn verstanden. Sei z.B. A die Aussage "*Die Wand ist weiß*". Dann ist die Verneinung $\neg A$ von A die Aussage "*Die Wand ist nicht weiß*", nicht aber die Aussage "*Die Wand ist schwarz*". Die Verneinung ist also nicht dasselbe wie das Gegenteil.

Implikation. Sind A und B Aussagen, dann ist auch $A \Rightarrow B$ (ausgesprochen als "A impliziert B", "wenn A dann B, "aus A folgt B", ...) eine Aussage. Ein Beispiel für eine Implikation ist die Aussage "*Falls es regnet, dann ist die Straße nass.*" Man beachte dass die Implikation (anders als Konjunktion und Disjunktion) nicht kommutativ ist, d.h. $A \Rightarrow B$ hat eine andere Bedeutung als $B \Rightarrow A$. Falls die Straße nass ist, bedeutet das nicht dass es regnet; sie könnte auch gerade gewaschen worden sein. Die Interpretation von Implikationen wird durch die folgende Wahrheitstafel definiert.

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

Falls also A wahr ist, dann hat $A \Rightarrow B$ den Wahrheitswert von B. Falls A falsch ist dann ist es egal was rechts steht, $A \Rightarrow B$ hat immer den Wahrheitswert wahr. Die Definition der Implikation, insb. für falsches A, lässt sich auch dadurch erklären, dass die Implikation Wahrheit erhalten soll: $A \Rightarrow B$ bedeutet dass B "mindestens so wahr" wie A ist. Falls A nun falsch ist, d.h. den Wahrheitswert 0 hat, dann gilt das unabhängig von B.

Man beachte, dass dadurch $A \Rightarrow B$ auch wahr ist wenn sowohl A als auch B falsch sind, und zwar unabhängig davon, ob zwischen A und B überhaupt ein Zusammenhang besteht. Z.B. ist die Aussage "*Falls der Mond aus Käse ist, dann ist* $2 + 2 = 5$." wahr. In der Mathematik spielt dieses Phänomen aber praktisch keine Rolle, da man typischerweise solche Implikationen betrachtet wo 1. ein Zusammenhang zwischen Voraussetzung und Folgerung besteht und 2. die Voraussetzung wahr ist.

Äquivalenz. Die letzte Verknüpfung von Aussagen die wir betrachten wollen ist die logische Äquivalenz. Sind A und B Aussagen so ist auch $A \Leftrightarrow B$ (ausgesprochen als "A genau dann wenn B" oder "A dann und nur dann wenn B") eine Aussage. Die Wahrheitstafel für die Äquivalenz ist:

A	B	$A \Leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Formeln. Eine Aussage kann also durch die **Konnektive** $\wedge$, $\vee$, $\neg$, $\Rightarrow$ und $\Leftrightarrow$ aus einfacheren Aussagen zusammengesetzt werden. Diese bezeichnet man auch als **atomare Aussagen** der zusammengesetzten Aussage. So sind z.B. A und B die atomaren Aussagen der zusammengesetzten Aussage $(\neg A \vee B) \Leftrightarrow (A \Rightarrow B)$. Wie Sie es vom Rechnen mit Zahlen gewöhnt sind gibt es auch hier Klammersetzungsregeln: am stärksten bindet die Negation $\neg$, dann kommen die "Punktrechnungen" $\wedge$ und $\vee$ vor den "Strichrechnungen" $\Rightarrow$ und $\Leftrightarrow$. Damit kann die obige Aussage auch geschrieben werden als $\neg A \vee B \Leftrightarrow (A \Rightarrow B)$ oder als $((\neg A) \vee B) \Leftrightarrow (A \Rightarrow B)$.

Ist der Wahrheitswert der atomaren Aussagen bekannt so kann daraus der Wahrheitswert der zusammengesetzten Aussage berechnet werden. Damit können auch für komplexere zusammengesetzte Aussagen Wahrheitstafeln erstellt werden. Ein Beispiel für eine Wahrheitstafel ist:

A	B	$\neg A$	$\neg A \vee B$	$A \Rightarrow B$	$(\neg A \vee B) \Leftrightarrow (A \Rightarrow B)$
0	0	1	1	1	1
0	1	1	1	1	1
1	0	0	0	0	1
1	1	0	1	1	1

Beim Erstellen einer Wahrheitstafel ist es oft praktisch auch die Wahrheitswerte von Teilaussagen als Zwischenergebnisse zu berechnen (wie das hier z.B. für $\neg A \vee B$ gemacht wurde).

Eine Aussage heißt **erfüllbar**, wenn es eine Wahrheitswertbelegung ihrer atomaren Aussagen gibt, die sie wahr macht, d.h., wenn es eine Zeile in der Wahrheitstafel gibt, die 1 ergibt. Eine Aussage heißt **unerfüllbar** wenn das nicht der Fall ist, d.h., wenn alle Zeilen der Wahrheitstafel 0 ergeben. Eine Aussage heißt **gültig**, wenn sie unter allen Wahrheitswertbelegungen ihrer atomaren Aussagen wahr ist, d.h., wenn alle Zeilen ihrer Wahrheitstafel 1 ergeben. So ist etwa im obigen Beispiel die Aussage $A \Rightarrow B$ erfüllbar und die Aussage $(\neg A \vee B) \Leftrightarrow (A \Rightarrow B)$ gültig.

Das Teilgebiet der Logik, das sich mit Aussagen beschäftigt die aus atomaren Aussagen durch Operationen wie diesen zusammengesetzt sind, bezeichnet man als **Aussagenlogik**. Eine zusammengesetzte Aussage bezeichnet man auch als **aussagenlogische Formel**.

Rechenregeln. Innerhalb einer zusammengesetzten Aussage kann man, wie beim Rechnen mit Gleichungen, eine Teilaussage durch eine andere äquivalente Teilaussage ersetzen ohne ihre Bedeutung zu verändern. Z.B. wissen wir aufgrund obiger Wahrheitstafel dass $\neg A \vee B$ und $A \Rightarrow B$ für alle Aussagen A und B äquivalent sind. Daraus folgt z.B. dass die Aussagen

$$F \Rightarrow ((C \wedge D) \Rightarrow E) \quad \text{und} \quad F \Rightarrow (\neg(C \wedge D) \vee E)$$

ebenfalls äquivalent sind. Für Aussagen gelten die folgenden Rechenregeln:

Kommutativität:	$A \wedge B \Leftrightarrow B \wedge A$	$A \vee B \Leftrightarrow B \vee A$
Assoziativität:	$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$	$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$
Idempotenz:	$A \wedge A \Leftrightarrow A$	$A \vee A \Leftrightarrow A$
Distributivität:	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
Regeln von de Morgan:	$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$	$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
Zur Implikation:	$\neg A \vee B \Leftrightarrow A \Rightarrow B$	$(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$
Doppelnegation:	$\neg\neg A \Leftrightarrow A$	

All diese Rechenregeln können durch Wahrheitstafeln bewiesen werden.

Das Wichtigste in Kürze.

- Eine Aussage ist ein Satz, dem man einen objektiven Wahrheitswert zuweisen kann, der entweder wahr oder falsch ist.
- Aussagen werden durch Verknüpfungen, wie z.B. $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, zu neuen Aussagen zusammengesetzt.
- Mit einer Wahrheitstafel kann festgestellt werden, ob eine gegebenen Aussage (un)erfüllbar oder (un)gültig ist.
- Gültige Äquivalenzen können wie Rechenregeln verwendet werden.

Kapitel 2

Quantoren

Ein **Prädikat** ist ein Satz, der Variablen enthält und der für jede Festlegung der Werte dieser Variablen zu einer Aussage wird. Beispiele für Prädikate sind:

$n \geq 5$

n ist gerade.

a ist Großmutter von b.

$n \leq k \Rightarrow n < k + 1$

Hier sind n, a und b, bzw. n und k die Variablen dieser Prädikate. Je nachdem wie die Werte der Variablen gewählt werden, kann die entstehende Aussage wahr oder falsch werden. Sei $P(n)$ das Prädikat $n \geq 5$. Dann ist z.B. die Aussage $P(2)$, also $2 \geq 5$, falsch, die Aussage $P(7)$, also $7 \geq 5$, aber wahr.

Prädikate können, genauso wie Aussagen, mit Hilfe von aussagenlogischen Verknüpfungen wie $\wedge$, $\vee$, $\neg$, ... zu neuen Prädikaten zusammengesetzt werden. So ist z.B.

$$n \geq 5 \wedge n \text{ ist gerade}$$

ein Prädikat das für alle geraden Zahlen größer gleich 5 wahr ist.

Ein **Quantor** erlaubt die Bildung eines neuen Prädikats oder einer neuen Aussage aus einem bereits bestehenden Prädikat, indem er angibt wie mit einer der Variablen zu verfahren ist. Prädikate und Quantoren sind für die Sprache der Mathematik von zentraler Bedeutung, da sie die Bildung allgemeiner Aussagen ermöglichen. Erst dadurch lassen sich viele Zusammenhänge überhaupt erst auf angemessene Weise ausdrücken. Es gibt zwei (für uns wichtige) Quantoren: den Allquantor und den Existenzquantor.

Allquantor. Der Allquantor bedeutet, dass das betrachtete Prädikat für **alle** Werte der betreffenden Variable gelten soll. So können wir mit Hilfe des Allquantors z.B. die folgende Aussage bilden:

$$\text{Für alle } n \text{ gilt } n \geq 5.$$

Eine Kurznotation für den Allquantor ist $\forall$, ein gespiegeltes A. Mit dieser kann diese Aussage als

$$\forall n \; n \geq 5$$

geschrieben werden. Eine Aussage, die mit einem Allquantor beginnt, bezeichnen wir auch als **Allaussage**.

Die Aussage $\forall n\ n \geq 5$ ist wahr genau dann wenn $n \geq 5$ für alle möglichen Werte von n wahr ist. Das ist nicht der Fall. Zwar ist z.B. $8 \geq 5$ oder $9 \geq 5$, nicht aber $3 \geq 5$. Deshalb ist die Aussage $\forall n\ n \geq 5$ falsch. Der Allquantor ist mit der Konjunktion verwandt, da die Aussage $\forall n\ P(n)$, unter der Voraussetzung dass wir für n nur natürliche Zahlen einsetzen wollen, äquivalent zur "unendlichen Aussage" $P(0) \wedge P(1) \wedge P(2) \wedge \cdots$ ist. Daran sehen wir auch, dass die Verwendung von Wahrheitstafeln für die Bestimmung des Wahrheitswertes einer Allaussage nicht mehr zielführend sein wird, da diese Wahrheitstafel unendlich groß sein müsste.

Existenzquantor. Der zweite wichtige Quantor ist der Existenzquantor. Wenn man auf ein Prädikat einen Existenzquantor anwendet, drückt man dadurch aus, dass das betrachtete Prädikat für (mindestens) **einen** Wert der betreffenden Variable gelten soll. So können wir z.B. die folgenden Aussage bilden:

$$\text{Es gibt ein } n \text{ so dass } n \geq 5.$$

Die symbolische Kurznotation für den Existenzquantor ist $\exists$, ein gespiegeltes E. Mit dieser können wir die obige Aussage als

$$\exists n\ n \geq 5$$

schreiben. Eine Aussage die mit einem Existenzquantor beginnt bezeichnen wir auch als **Existenzaussage**.

Die Aussage $\exists n\ n \geq 5$ ist wahr, da es ein n gibt, so dass $n \geq 5$, z.B. ist $7 \geq 5$. Dass es mehrere solche n gibt stört hier nicht weiter. Auch wenn es viele n gibt mit $n \geq 5$, so ändert das nichts daran, dass es ein n gibt mit $n \geq 5$. Wir können uns einen Existenzquantor wie eine "unendliche Disjunktion" vorstellen. So ist die Aussage $\exists n\ P(n)$, wiederum unter der Voraussetzung, dass n eine natürliche Zahl sein soll, äquivalent zur "unendlichen Aussage" $P(0) \vee P(1) \vee P(2) \vee \cdots$. Da $\vee$ eine inklusive Disjunktion ist bedeutet $\exists n\, P(n)$ dass es mindestens ein n gibt mit $P(n)$.

Mehrere Quantoren. Mit dem Allquantor haben wir bereits oben aus dem Prädikat $n \geq 5$ die Aussage $\forall n\ n \geq 5$ gebildet. Der Allquantor hat also die Variable n **quantifiziert** und die so erhaltene Aussage hängt also nicht mehr von der Variable n ab. Genau so können wir auch mit Prädikaten verfahren, die von mehreren Variablen abhängen. Ist z.B. $P(n, k)$ das Prädikat

$$n \leq k \Rightarrow n < k + 1$$

das von den Variablen n und k abhängt, dann können wir das neue Prädikat $Q(n)$

$$\forall k\, (n \leq k \Rightarrow n < k + 1)$$

erzeugen, das jetzt nur noch von n abhängig ist. In weiterer Folge erzeugen wir die Aussage A

$$\forall n \forall k\, (n \leq k \Rightarrow n < k + 1)$$

durch eine zweite Anwendung eines Allquantors.

Die Quantoren $\forall$ und $\exists$ sind, genauso wie z.B. die Negation $\neg$, unäre Operatoren und binden dadurch stärker als binäre Operatoren. So ist z.B. $\forall x\, A \Rightarrow B$ eine Abkürzung für $(\forall x\, A) \Rightarrow B$. Soll sich der Quantor $\forall x$ auch auf B beziehen, müssen die Klammern wie in $\forall x\ (A \Rightarrow B)$ gesetzt werden. Gelegentlich wird auch ein Doppelpunkt geschrieben, um auszudrücken dass der Quantor so schwach wie möglich binden soll. Damit ist $\forall x : A \Rightarrow B$ eine andere Schreibweise für $\forall x\ (A \Rightarrow B)$.

Bei der Verwendung mehrerer Allquantoren ist die Reihenfolge irrelevant. So gilt die Äquivalenz

$$\forall n \forall k\, R(n,k) \Leftrightarrow \forall k \forall n\, R(n,k)$$

für jedes beliebige Prädikat $R(n,k)$. Analog gilt für Existenzquantoren auch

$$\exists n \exists k\, R(n,k) \Leftrightarrow \exists k \exists n\, R(n,k).$$

Diese Äquivalenzen können wir auch jederzeit als Rechenregeln anwenden.

Aber Achtung: zwei unterschiedliche Quantoren dürfen nicht vertauscht werden! So kann z.B. der Satz "*Für jeden Topf gibt es einen passenden Deckel.*" formalisiert werden als:

$$\forall T \exists D : D \text{ passt auf } T.$$

Vertauscht man diese beiden Quantoren, erhält man die Aussage

$$\exists D \forall T : D \text{ passt auf } T,$$

also: "*Es gibt einen Deckel, der auf alle Töpfe passt.*", was klarerweise nicht äquivalent ist.

Freie und gebundene Variablen. Wir haben gesehen, dass der Wahrheitswert eines Prädikats von gewissen Variablen bestimmt wird. Diese werden auch als **freie Variablen** des Prädikats bezeichnet. So sind z.B. im Prädikat $k \leq n$ die beiden Variablen k und n frei. Wir drücken das aus, indem wir für dieses Prädikat eine Kurznotation wie $P(k,n)$ verwenden, in dem die beiden freien Variablen explizit angegeben sind. Der Wahrheitswert dieses Prädikat wird also durch k und n bestimmt. Quantoren sind Operatoren, die Variablen **binden**. In dem aus $P(k,n)$ gebildeten Prädikat $\exists n\, k \leq n$ ist k frei, aber n (durch den Quantor $\exists n$) gebunden. Die Variable n wird dann als **gebundene Variable** bezeichnet. Wir verwenden dann für $\exists n\, k \leq n$ eine Kurznotation wie z.B. $Q(k)$ um auszudrücken, dass der Wahrheitswert nur noch von k abhängt.

Es gibt viele andere Operatoren in der Mathematik und der Informatik, die Variablen binden, z.B. den Summenoperator. Im arithmetischen Ausdruck $i(i+1)$ ist die Variable i frei, im Ausdruck $\sum_{i=1}^{n} i(i+1)$ ist i durch $\sum$ gebunden. Das ist analog zum Verhältnis zwischen globalen und lokalen Variablen bzw. zum Geltungsbereich (scope) einer Deklaration in Programmiersprachen. So sind etwa im Code

```
x := x + i
```

die beiden Variablen `x` und `i` frei, in

```
for i := 1 to n {
  x := x + i
}
```

ist nur noch `x` frei, `i` ist durch den Schleifenkopf gebunden.

Im Prinzip kann eine Variable auch frei und gebunden auftreten. Z.B. kommt im Prädikat

$$R(x,y) \quad \Leftrightarrow \quad x \leq y \wedge \exists x\, x^2 = y.$$

die Variable x sowohl frei als auch gebunden vor[1]. Gebundene Variablen dürfen immer umbenannt werden. Damit ist

$$R(x,y) \quad \Leftrightarrow \quad x \leq y \wedge \exists z\, z^2 = y.$$

eine äquivalente Definition von $R(x,y)$. In der Praxis bemüht man sich auch darum, solche Doppelverwendungen zu vermeiden, da sie oft verwirrend sind.

[1] $R(x,y)$ ist genau dann erfüllt, falls y eine Quadratzahl ist, die größer oder gleich x ist.

Die Grundmenge eines Quantors. Damit die Bedeutung eines Quantors eindeutig festgelegt ist, muss klar sein, über welche Menge von Objekten er quantifiziert. Diese Menge nennt man auch **Grundmenge** eines Quantors. So ist zum Beispiel die Aussage $\exists x\,(1 < x \wedge x < 2)$ wahr, wenn die Grundmenge von $\exists x$ die Menge der rationalen Zahlen ist und falsch, wenn die Grundmenge von $\exists x$ die Menge der ganzen Zahlen ist. Falls die Grundmenge nicht aus dem Kontext heraus ersichtlich ist, dann wird sie explizit angegeben wie z.B. in $\exists x \in \mathbb{Q}\,(1 < x \wedge x < 2)$ bzw. $\exists x \in \mathbb{Z}\,(1 < x \wedge x < 2)$.

Ein weiteres gebräuchliches Mittel zur Angabe der Grundmenge eines Quantors ist die Verwendung gewisser Buchstaben für gewisse Arten von Objekten, z.B. steht n oft für eine natürliche Zahl, x für eine reelle Zahl und z für eine komplexe Zahl. Damit ist dann z.B. $\forall n\ P(n)$ eine Abkürzung für $\forall n \in \mathbb{N}\ P(n)$. Für diese Abkürzung gilt, so wie für Abkürzungen im Allgemeinen: drücken Sie sich so knapp wie möglich aus aber nicht knapper. Wenn die Gefahr von Missverständnissen besteht, schreiben Sie lieber ausführlicher und verzichten Sie auf Abkürzungen.

Formeln, die sich dieser Notationen bedienen, können auch ohne sie geschrieben werden:

$$\begin{array}{rll} \forall m \in \mathbb{Z}\ P(m) & \text{steht für} & \forall m\,(m \in \mathbb{Z} \Rightarrow P(m)) \\ \exists m \in \mathbb{Z}\ P(m) & \text{steht für} & \exists m\,(m \in \mathbb{Z} \wedge P(m)) \\ \forall n \geq 1\ P(n) & \text{steht für} & \forall n\,(n \geq 1 \Rightarrow P(n)) \end{array}$$

wobei die Grundmenge der Quantoren auf der rechten Seite alle erwähnten Mengen inkludieren muss. Analoges gilt natürlich auch für Notationen wie z.B. $\exists x \in \mathbb{R}\ P(x)$ oder $\forall x > 0\ P(x)$, ...

Warnung 2.1. Verwechseln Sie nicht $\forall m\,(m \in \mathbb{Z} \Rightarrow P(m))$ mit $\forall m\,(m \in \mathbb{Z} \wedge P(m))$. Ersteres bedeutet "Alle ganzen Zahlen erfüllen P." . Zweiteres bedeutet "Für alle m gilt: $m \in \mathbb{Z}$ und m erfüllt P." und ist in dieser Form fast nie sinnvoll. Eine analoge Warnung gilt für $\exists m\,(m \in \mathbb{Z} \wedge P(m))$ und $\exists m\,(m \in \mathbb{Z} \Rightarrow P(m))$. Die erste Form kommt häufig vor und bedeutet "Es gibt eine ganze Zahl, die P erfüllt." . Zweiteres ist äquivalent zu $\exists m\,(m \notin \mathbb{Z} \vee P(m))$ und bedeutet also: "Es gibt ein m, das keine ganze Zahl ist oder P erfüllt." . Das ist ebenfalls fast nie sinnvoll.

Prädikatenlogik und natürliche Sprache. Das Teilgebiet der Logik, das sich mit Aussagen beschäftigt, die aus den aussagenlogischen Operationen und den Quantoren aufgebaut sind, bezeichnet man als **Prädikatenlogik**. Einen aus diesen Operationen bestehenden Ausdruck bezeichnet man als **prädikatenlogische Formel**. Dabei müssen die Quantoren nicht immer am Anfang stehen. Wir dürfen, wie z.B. in

$$\forall x \exists y\,(x \leq y \wedge \exists z\, z^2 = y)$$

aussagenlogische Operationen und Quantoren beliebig ineinander verschachteln. Im Prinzip lassen sich alle mathematischen Aussagen als prädikatenlogische Formeln ausdrücken. In der Praxis verwendet man aber aus Gründen der Lesbarkeit häufig die natürliche Sprache. Bei der Übertragung von Aussagen aus der natürlichen Sprache in die Prädikatenlogik muss man sorgfältig vorgehen. Wir wollen dazu ein Beispiel betrachten. Es seien die folgenden atomaren Prädikate gegeben:

$$\begin{array}{rl} G(x,y) & x \text{ und } y \text{ sind Geschwister} \\ W(x) & x \text{ ist weiblich} \\ L(x,y) & x \text{ lebt in } y \end{array}$$

Damit können wir z.B. die folgenden Übersetzungen deutscher Sätze in die Prädikatenlogik vornehmen. Die Grundmenge der Quantoren soll dabei die Menge aller Menschen sein.

$$\begin{array}{rl} \text{Anna hat eine Schwester in Graz.} & \exists x\ (G(\text{Anna}, x) \wedge W(x) \wedge L(x, \text{Graz})) \\ \text{Die Geschwister von Bernhard leben in Wien.} & \forall x\ (G(\text{Bernhard}, x) \Rightarrow L(x, \text{Wien})) \\ \text{Caro hat keine Geschwister.} & \neg\exists x\, G(\text{Caro}, x) \end{array}$$

Warnung 2.2. Prädikate können nicht verschachtelt werden. Ausdrücke wie etwa $G(W(x), y)$ ergeben keinen Sinn, da $W(x)$ ja entweder wahr oder falsch ist und damit $G(W(x), y)$ etwas bedeuten würde wie "falsch und y sind Geschwister" oder "wahr und y sind Geschwister".

Verneinung. Für die Verneinung von quantifizierten Aussagen gelten Rechenregeln, die zu den Regeln von de Morgan analog sind. So gilt für die Verneinung des Allquantors:

$$\neg\forall n\, P(n) \Leftrightarrow \exists n\, \neg P(n).$$

Die Gültigkeit dieser Äquivalenz können wir so einsehen: wenn es nicht so ist, dass für alle n die Aussage $P(n)$ gilt, dann muss es ein n geben, für das $P(n)$ nicht gilt. Und umgekehrt: wenn es ein n gibt, für das $P(n)$ nicht gilt, dann ist es nicht so, dass $P(n)$ für alle n gilt.

Symmetrisch dazu gilt auch

$$\neg\exists n\, Q(n) \Leftrightarrow \forall n\, \neg Q(n)$$

was wir genauso wie oben begründen können, oder, alternativ, durch die folgende Kette von Äquivalenzen

$$\neg\exists n\, Q(n) \Leftrightarrow \neg\exists n\neg\neg Q(n) \Leftrightarrow \neg\neg\forall n\neg Q(n) \Leftrightarrow \forall n\neg Q(n)$$

in der wir im 1. und 3. Schritt die Rechenregel $\neg\neg A \Leftrightarrow A$ der Aussagenlogik benutzen und im 2. Schritt die obige Äquivalenz $\neg\forall n\, P(n) \Leftrightarrow \exists n\, \neg P(n)$.

Eindeutige Existenz. Manchmal will man auch ausdrücken, dass es genau ein Objekt gibt, das ein gewisses Prädikat erfüllt. Dafür kann man den eindeutigen Existenzquantor, dessen symbolische Notation $\exists!$ ist, benutzen. Die Aussage $\exists! n\ P(n)$ bedeutet dann, dass es genau ein n gibt, so dass $P(n)$ wahr ist. So ist z.B. $\exists! n\ 2 + n = 5$ wahr, aber $\exists! n\ n \geq 5$ ist falsch (wiederum unter der Voraussetzung dass n für eine natürliche Zahl steht). Der eindeutige Existenzquantor $\exists!$ kann durch $\forall$ und $\exists$ wie folgt definiert werden:

$$\exists! x\, P(x) \quad \Leftrightarrow \quad \exists x\, \big(P(x) \wedge \forall y\, (P(y) \Rightarrow y = x)\big)$$

Die Verneinung des eindeutigen Existenzquantors $\exists! n\, P(n)$ ist etwas komplizierter: $\neg\exists! n\, P(n)$ ist äquivalent zu: es gibt kein n mit $P(n)$ oder es gibt zwei verschiedene n mit $P(n)$. In symbolischer Notation ist das:

$$\neg\exists! x\, P(x) \quad \Leftrightarrow \quad \big(\forall x\, \neg P(x)\big) \vee \big(\exists x_1 \exists x_2 : x_1 \neq x_2 \wedge P(x_1) \wedge P(x_2)\big)$$

Das Wichtigste in Kürze.

- Ein Prädikat ist ein Satz, der Variablen enthält und der für jede Festlegung der Werte dieser Variablen zu einer Aussage wird.
- Prädikate können durch aussagenlogische Verknüpfungen sowie durch den Allquantor $\forall$ und den Existenzquantor $\exists$ zu neuen Prädikaten und Aussagen zusammengesetzt werden.
- Ein Quantor bindet eine vormals freie Variable. Ein durch Quantifizierung erhaltenes Prädikat hat also eine freie Variable weniger als das Ausgangsprädikat. Ein Prädikat ohne freie Variablen ist eine Aussage.
- Für jeden Quantor ist, entweder aus dem Kontext oder durch die Verwendung entsprechender Notation, eindeutig festgelegt, über welche Grundmenge er quantifiziert.

Kapitel 3

Definitionen

Eine **Definition** etabliert die Bedeutung eines Ausdrucks, indem sie ihn zu anderen Ausdrücken, deren Bedeutung bereits bekannt ist, in Beziehung setzt. Eine Definition hat also immer zwei Teile: den Ausdruck den sie definiert (lat. Definiendum) und das wodurch sie ihn definiert, das Definierende (lat. Definiens). Beispiele für Definitionen sind:

$$\text{Ein } \underbrace{\text{Junggeselle}}_{\textit{Definiendum}} \text{ ist ein } \underbrace{\text{unverheirateter Mann}}_{\textit{Definiens}}.$$

$$\underbrace{n \text{ teilt } m}_{\textit{Definiendum}} \text{ falls}[1] \underbrace{\text{ein } k \text{ existiert so dass } n \cdot k = m}_{\textit{Definiens}}.$$

Wird eine Definition angegeben muss also die Bedeutung des Definiens bereits bekannt sein. Durch die Definition wird üblicherweise postuliert, dass das Definiendum synonym zum Definiens ist. Wir dürfen also immer das eine durch das andere ersetzen. In konkreten Beweisen ist das auch sehr oft notwendig. So können wir z.B. beweisen, dass die Zahl 3 die Zahl 15 teilt, indem wir ein k angeben, so dass $3 \cdot k = 15$ ist.

Oft schreiben wir in der Mathematik eine Definition in abgesetzter Notation wie z.B.:

Definition. Eine Zahl n heißt gerade, falls ein k existiert so dass $2 \cdot k = n$.

Oft wird auch das Definiendum typographisch hervorgehoben wie in

Definition. Eine Zahl n heißt **gerade**, falls ein k existiert so dass $2 \cdot k = n$.

In der Mathematik werden Definitionen auch oft durch logische Formeln angegeben. So können wir Definitionen auch wie folgt schreiben:

$$\begin{aligned} \text{Junggeselle}(x) &:\Leftrightarrow \text{Mann}(x) \wedge \neg\text{Verheiratet}(x) \\ n \mid m &:\Leftrightarrow \exists k \; n \cdot k = m && \text{(Teilbarkeit)} \\ \overline{a + ib} &:= a - ib && \text{(Konjugation komplexer Zahlen)} \end{aligned}$$

Warnung 3.1. Verwechseln Sie nicht "$:\Leftrightarrow$" und "$:=$". Die Notation "$:\Leftrightarrow$" wird für Prädikate verwendet und bedeutet "wird definiert als äquivalent zu". Die Notation "$:=$" wird für Terme verwendet und bedeutet "wird definiert als gleich zu". Der Unterschied besteht darin, dass Terme Objekte (der Mathematik) bezeichnen und Prädikate Eigenschaften dieser Objekte.

[1] In dieser Definition steht nur "falls". Im Kontext einer Definition ist aber "genau dann wenn" damit gemeint. Das ist eine geringfügige Inkonsistenz im Verhältnis zwischen Logik und natürlicher Sprache in der Mathematik.

Die Bezeichnung des Definiens kann vom Autor einer Definition frei gewählt werden. Um das Lesen eines Texts zu erleichtern wird man sich aber üblicherweise darum bemühen, sinnvolle Bezeichnungen zu verwenden, so ist es z.B. üblich, für **n**atürliche Zahlen den Buchstaben n zu verwenden, für einen **I**ndex den Buchstabe i, usw. Es ist dabei auch möglich, und gar nicht so unüblich wie man vielleicht glauben würde, sehr bildliche Bezeichnungen zu verwenden. So gibt es in der Zahlentheorie z.B. *fröhliche* Zahlen oder Paare *befreundeter* Zahlen. Sie können auch selbst definieren, was sie wollen. Häufig ist das durchaus nützlich oder sogar notwendig, um Lösungen von Übungsbeispielen gut zu strukturieren.

Einfache Definition eines Prädikats. Eine der gebräuchlichsten Formen einer Definition in der Mathematik besteht darin, ein neues Prädikat $P(x_1, \dots, x_n)$ durch Angabe einer prädikatenlogischen Formel[2] $A(x_1, \dots, x_n)$ zu definieren:

$$P(x_1, \dots, x_n) :\Leftrightarrow A(x_1, \dots, x_n).$$

Dabei ist P ein neues[3] Symbol oder eine neue Bezeichnung. Ein Beispiel für eine solche Definitionen war die der Teilbarkeit. Ein anderes Beispiel wäre die folgende Definition der Ordnung "kleiner-gleich" aus "kleiner":

$$x \leq y :\Leftrightarrow x < y \vee x = y$$

Warnung 3.2. Beachten Sie, dass die Menge freier Variablen im Definiendum mit der Menge freier Variablen im Definiens überstimmen muss. Wollen wir z.B. Teilbarkeit definieren, schreiben wir das Definiendum als $n \mid m$. Als Definiens kommt also nur ein Prädikat in Frage, das die beiden freien Variablen n und m hat. Etwas wie z.B.

$$n \mid m :\Leftrightarrow n \cdot k = m$$

zu schreiben wäre falsch, weil k auf der rechten Seite frei vorkommt. Analoges gilt auch für die weiter unten besprochenen Formen von Definitionen.

Einfache Definition einer Funktion. Die einfachste Definition einer Funktion besteht aus der Angabe eines Terms. Das ist von der logischen Form

$$f(x_1, \dots, x_n) := t(x_1, \dots, x_n)$$

wobei f ein neues Symbol oder eine neue Bezeichnung ist und alle Symbole in t bekannt sind. So wurde z.B. die Konjugation komplexer Zahlen aus dem bekannten Symbol $-$ (minus) definiert. Ein anderes Beispiel wäre die folgende Definition des kleinsten gemeinsamen Vielfachen:

$$\mathrm{kgV}(n, m) := \min\{k \in \mathbb{N} \mid n \mid k \text{ und } m \mid k\} \qquad \text{(kleinstes gemeinsames Vielfaches)}$$

Etwas komplexer, aber auch gebräuchlich, ist die folgende Form

$$y = f(x_1, \dots, x_n) :\Leftrightarrow A(x_1, \dots, x_n, y)$$

[2] oder eines Satzes der in eine prädikatenlogische Formel übersetzt werden kann

[3] "neu" bedeutet hier, dass das Symbol im aktuellen Stand der Entwicklung der mathematischen Theorie, von der die Rede ist noch nicht vorkommt.

wobei f ein neues Symbol ist und $A(x_1, \dots, x_n, y)$ eine prädikatenlogische Formel deren Symbole alle bekannt sind. Damit die Funktion f dadurch wohldefiniert ist, muss $\forall x_1 \cdots \forall x_n \exists! y\, A(x_1, \dots, x_n, y)$ gelten. Ein Beispiel für eine Definition dieser Form ist etwa die folgende Definition der Subtraktionsfunktion in den ganzen Zahlen:

$$y = m - n :\Leftrightarrow n + y = m \qquad \text{(Subtraktion ganzer Zahlen)}$$

Wohldefiniertheit. Nicht immer ist auf den ersten Blick klar, ob ein Satz eine Definition ist oder nicht. Eine Bedingung ist leicht zu überprüfen: alle im Definiens vorkommenden Begriffe müssen bekannt sein. Aber selbst dann können noch Schwierigkeiten auftreten. Die Äquivalenz

$$y = m - n :\Leftrightarrow n + y = m$$

definiert die Subtraktionsfunktion $-$ weil $\forall m \forall n \exists! y\ n + y = m$. Wir drücken die Tatsache, dass es sich beim vorangehenden Satz um eine Definition handelt aus indem wir sagen: "Damit ist $-$ wohldefiniert." Vergleichen Sie das mit:

$$y = m \odot n :\Leftrightarrow m \leq y \wedge n \leq y$$

Hier wird vorgeblich eine Funktion $\odot$ definiert. Auch hier sind alle Begriffe, die im Definiens vorkommen bekannt. Weiters gilt auch $\forall m \forall n \exists y\, (m \leq y \wedge n \leq y)$, z.B. können wir für y einfach das Maximum von m und n verwenden. Allerdings gilt nicht $\forall m \forall n \exists! y\, (m \leq y \wedge n \leq y)$. In diesem Fall gibt es also mehr als ein y und damit ist $\odot$ nicht wohldefiniert. Wenn es die Intention war, $\odot$ als das Maximum zu definieren, dann kann diese Definition z.B. wie folgt repariert werden:

$$y = m \odot n :\Leftrightarrow m \leq y \wedge n \leq y \wedge (y = m \vee y = n)$$

Betrachten wir nun die folgenden Beispiele:

$$\mathrm{ggT}(n, m) := \max\{k \in \mathbb{N} \mid k \mid n \text{ und } k \mid m\} \qquad \text{(größter gemeinsamer Teiler)}$$

Wir können uns wie folgt überlegen, dass durch den obigen Satz der ggT zweier natürlicher Zahlen $n, m \geq 1$ wohldefiniert ist: Zunächst einmal ist die Menge $\{k \in \mathbb{N} \mid k \mid n \text{ und } k \mid m\}$ endlich, da jede Zahl ≥ 1 nur endliche viele Teiler hat. Weiters ist die Menge nicht leer, da 1 jede Zahl teilt. Eine nicht-leere endliche Menge natürlicher Zahlen hat genau ein Maximum. Dieses ist der ggT. Betrachten wir nun:

$$\mathrm{kgV}(n, m) := \min\{k \in \mathbb{N} \mid n \mid k \text{ und } m \mid k\} \qquad \text{(kleinstes gemeinsames Vielfaches)}$$

Dieser Definition des kleinsten gemeinsamen Vielfachen liegt die Menge $\{k \in \mathbb{N} \mid n \mid k \text{ und } m \mid k\}$ zugrunde. Diese Menge ist nicht leer, da sie z.B. $n \cdot m$ enthält. Allerdings ist diese Menge unendlich groß. Trotzdem ist das Minimum wohldefiniert, da jede nicht-leere (möglicherweise auch unendliche) Teilmenge der natürlichen Zahlen ein eindeutig definiertes Minimum hat. Dieses ist das kgV. Was ist aber z.B. mit der folgenden Zeile?

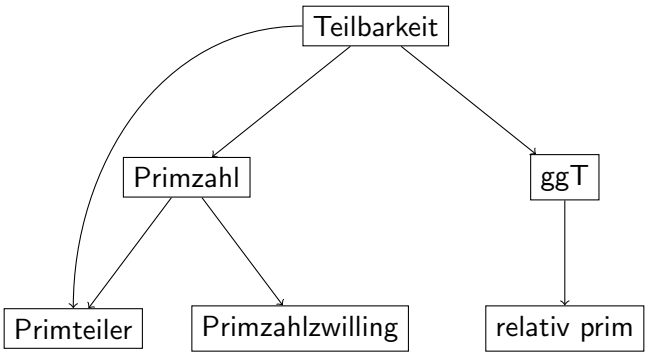
$$\mathrm{ggV}(n, m) := \max\{k \in \mathbb{N} \mid n \mid k \text{ und } m \mid k\} \qquad \text{("größtes gemeinsames Vielfaches")}$$

Auch dieser vorgeblichen Definition liegt die Menge $\{k \in \mathbb{N} \mid n \mid k \text{ und } m \mid k\}$ zugrunde, von der wir uns bereits überlegt haben, dass sie unendlich ist. Eine unendliche Teilmenge der natürlichen Zahlen hat aber kein Maximum. Damit ist ggV nicht wohldefiniert.

Definitionsgebäude. Wir wissen bereits, dass in einer Definition alle im Definiens vorkommenden Begriffe bekannt sein müssen. Sobald ein Begriff aber definiert wurde, kann er natürlich in weiteren Definitionen verwendet werden, um seinerseits bei der Definition neuer Begriffe mitzuwirken. Auf diese Weise kann man ganze Definitionsgebäude mit aufeinander aufbauenden Begriffen erstellen. Das ist auch durchaus typisch in der Mathematik. Das folgende Defintionsgebäude entstammt z.B. der elementaren Zahlentheorie.

$$n \mid m :\Leftrightarrow \exists k\ n \cdot k = m \qquad \text{(Teilbarkeit)}$$
$$n \text{ heißt Primzahl} :\Leftrightarrow \forall k\ (k \mid n \Rightarrow k = 1 \vee k = n) \wedge n \neq 1$$
$$p \text{ heißt Primteiler von } n :\Leftrightarrow p \text{ Primzahl und } p \mid n$$
$$(p_1, p_2) \text{ heißt Primzahlzwilling} :\Leftrightarrow p_1, p_2 \text{ Primzahlen und } p_1 + 2 = p_2$$
$$\mathrm{ggT}(n, m) := \max\{k \in \mathbb{N} \mid k \mid n \text{ und } k \mid m\} \qquad \text{(größter gemeinsamer Teiler)}$$
$$n, m \text{ heißen relativ prim} :\Leftrightarrow \mathrm{ggT}(n, m) = 1$$

Wir können die Abhängigkeiten dieser Definitionen analysieren, indem wir eine Skizze machen, in der ein Pfeil von einem Begriff A zu einem Begriff B führt wenn A im Definiens der Definition von B vorkommt.



Die Tatsache, dass im Definiens nur bekannte Begriffe vorkommen dürfen übersetzt sich hier in die Eigenschaft dieser Skizze keinen Zyklus zu enthalten.

Sinn von Definitionen. Neben Aussagen (und Beweisen, die wir in Kapitel 4 kennen lernen werden) spielen Definition eine der wichtigsten Rollen in der Mathematik. Die Verwendung einer Definition hat (mindestens) die folgenden zwei Effekte: Erstens bietet sie die Möglichkeit, eine Abkürzung zu verwenden. Es ist schlicht kürzer zu sagen "*Sei p eine Primzahl.*" als zu sagen "*Sei p eine natürliche Zahl, die nur durch* 1 *und sich selbst teilbar ist und ungleich* 1 *ist.*". Zweitens aber, und das ist der wesentlich wichtigere Effekt, führt eine Definition einen mathematischen Begriff ein, mit dem wir eine gewisse mentale Vorstellung verbinden. Diese erlaubt es uns, über den Begriff auf eine Art und Weise nachzudenken, die, mit zunehmender Klarheit der Vorstellung, mehr und mehr von der formalen Definition abgelöst ist, und dadurch effizienter ist. Kurz gesagt: die mentale Vorstellung erlaubt uns, eine Intuition für den Begriff zu entwickeln. Tatsächlich ist es eine der zentralen Schwierigkeiten am Beginn der Beschäftigung mit Mathematik, die Fähigkeit zu erlernen, aus einer (formalen) Definition eine mentale Vorstellung zu entwickeln, oder, anders formuliert: den definierten Begriff zu verstehen. Um den durch eine Definition eingeführten Begriff zu verstehen, ist es nützlich, sich z.B. die folgenden Fragen zu stellen:

- Gibt es überhaupt Objekte die unter die Definition fallen? Normalerweise wohl "ja", aber auch der Fall "nein" kann interessant sein. Welche Objekte fallen "knapp" nicht unter die

Definition? Was sind Standardbeispiele für solche Objekte, was sind Trivialbeispiele, was sind Extrembeispiele?

- Gibt es viele solcher Objekte, oder vielleicht genau eines, oder sind alle, die es gibt in irgendeinem Sinn ähnlich?
- Was kann man mit Objekten die unter die Definition fallen machen? Kann man vielleicht in ganz simpler Weise aus gegebenen Objekten andere konstruieren, die auch unter die Definition fallen?
- Wie steht dieser Begriff mit anderen, bereits bekannten, Begriffen in Zusammenhang?

Definitionen mit Nebenbedingungen. Gelegentlich ist es notwendig, den Gültigkeitbereich einer Definition durch eine Nebenbedingung einzuschränken. So wird z.B. der Kehrwert in den reellen Zahlen wie folgt definiert: Für $x \neq 0$ ist der Kehrwert $\frac{1}{x}$ definiert als jenes y, das $x \cdot y = 1$ erfüllt. Als prädikatenlogische Formel geschrieben:

$$x \neq 0 \Rightarrow (y = \frac{1}{x} :\Leftrightarrow x \cdot y = 1)$$

Damit ist der Kehrwert wohldefiniert da $\forall x\ (x \neq 0 \Rightarrow \exists! y\ x \cdot y = 1)$.

Rekursive Definitionen. Zum Abschluss wollen wir noch eine weitere Form von Definitionen betrachten, die für die Informatik, aber auch für die Mathematik, von großer Bedeutung sind: **rekursive Definitionen**. Das sind Definitionen, die auf sich selbst verweisen, ohne dabei aber zyklisch zu sein. Der Selbstverweis enthält üblicherweise einen Parameter, der im rekursiven Aufruf kleiner wird. So wird z.B. die Fakultät auf allen natürlichen Zahlen durch die Definition

$$0! := 1$$
$$(n+1)! := (n+1)n!$$

erklärt. Das Definiendum dieser Definition ist die Funktion ! die eine natürliche Zahl auf eine natürliche Zahl abbildet. Hier kommt zwar im Definiens ebenfalls die zu definierende Funktion ! vor, aber nur in eingeschränkter Form: mit einem kleineren Parameter (n statt $n+1$). Um also z.B. den Wert 3! zu berechnen muss man nicht die ganze Funktion ! kennen, sondern nur den Wert 2!. Um weiters den Wert von 2! zu berechnen, reicht es den Wert von 1! zu kennen. Um schließlich 1! zu berechnen reicht es den Wert 0! zu kennen. Dieser ist explizit als 1 definiert. Damit kann also 1! sowie, in weiterer Folge, 2! und 3! berechnet werden.

Ein weiteres Beispiel ist die Fibonacci-Folge. Diese wird durch die rekursive Definition

$$F_0 := 0$$
$$F_1 := 1$$
$$F_{n+2} := F_{n+1} + F_n$$

gegeben. Diese ist etwas komplizierter, da für die Berechnung eines Wertes F_n die beiden vorherigen Werte benutzt werden und nicht nur, wie bei der Fakultät, der direkt vorhergehende.

Rekursive Definitionen sind eng verwandt mit rekursiver Programmierung: ein rekursives Programm ist im Wesentlichen eine rekursive Definition einer Funktion.

Das Wichtigste in Kürze.

- Eine Definition etabliert die Bedeutung eines Ausdrucks, indem sie ihn zu anderen Ausdrücken, deren Bedeutung bereits bekannt ist, in Beziehung setzt.
- Definitionen können verschiedene logische Formen haben.
- Der Zweck einer Definition besteht in der Mathematik üblicherweise darin, einen Begriff einzuführen, mit dem wir eine gewisse mentale Vorstellung verbinden. Das Verstehen einer Definition ist der Prozess der Entwicklung dieser Vorstellung.
- Um eine Definition zu verstehen ist es nützlich, sich elementare Fragen über den definierten Begriff zu stellen, wie etwa: Welche Objekte fallen unter diesen Begriff? Welche nicht? ...

Kapitel 4

Beweise

Ein wesentlicher, wenn nicht der zentrale, Aspekt des mathematischen Arbeitens ist es, wahre Aussagen von falschen Aussagen zu unterscheiden. Für die Aussagenlogik haben wir bereits Wahrheitstafeln kennengelernt die es (sogar auf algorithmische Weise) erlauben festzustellen, ob eine Aussage gültig ist. In der Prädikatenlogik ist die Situation aber wesentlich komplizierter.

Stellen wir uns z.B. vor, dass wir überprüfen wollen, ob die folgende Aussage für alle natürlichen Zahlen n gilt: falls n gerade ist, dann ist auch n^2 gerade. Dazu könnten wir, inspiriert von der vollständigen Fallunterscheidung in Wahrheitstafeln, wie folgt vorgehen: Wir überprüfen die Aussage für $n = 0$: 0 ist gerade, $0^2 = 0$ ist ebenfalls gerade. 1 ist nicht gerade, also ist die Implikation für $n = 1$ wahr. 2 ist gerade, $2^2 = 4$ ist ebenfalls gerade usw. Klar ist aber dabei: auf diese Weise werden wir in endlicher Zeit nicht zum Ziel kommen. Dieser Ansatz des Durchprobierens aller Möglichkeiten ist also in der Prädikatenlogik grundsätzlich zum Scheitern verurteilt, da sich Quantoren typischerweise auf unendliche Grundmengen beziehen. Um solche Situationen in den Griff zu bekommen, verwendet man in der Mathematik Beweise[1].

Ein **Beweis** ist eine Ableitung einer Aussage aus anderen Aussagen durch logische Schlüsse. Die einzelnen Schritte eines Beweises, die logischen Schlüsse, werden so gewählt dass sie offensichtlich korrekt sind. Ein **logischer Schluss** (oder eine logische Schlussfolgerung) besteht dabei aus mehreren Voraussetzungen und einer Konklusion, welche die folgende Bedingung erfüllen: sind die Voraussetzungen wahr, so ist auch die Konklusion wahr[2].

Voraussetzungen und Behauptung. Wir wollen damit beginnen, eines der bekanntesten Beispiele für einen Beweis zu analysieren: *Sokrates ist ein Mensch. Alle Menschen sind sterblich. Also ist Sokrates sterblich.* Wir wollen diesen Beweis nun in der Prädikatenlogik formalisieren. Dazu verwenden wir die zwei Prädikate

$$S(x) :\Leftrightarrow x \text{ ist sterblich}$$
$$M(x) :\Leftrightarrow x \text{ ist ein Mensch}$$

und außerdem schreiben wir s für Sokrates. Hier gibt es also zwei Voraussetzungen: $M(s)$ und $\forall x\,(M(x) \Rightarrow S(x))$. Eine **Voraussetzung** (oder **Prämisse**) ist eine Aussage aus der wir etwas

[1] Das Verhältnis zwischen Wahrheit und Beweisbarkeit ist kompliziert und kann im Rahmen dieser Lehrveranstaltung nicht ausführlich behandelt werden. Für den Beweisbegriff der Mathematik – und dieser wird hier diskutiert – gilt aber jedenfalls: jede bewiesene Aussage ist wahr.

[2] Es ist möglich formal zu definieren was ein Beweis (in der Prädikatenlogik) ist. Beweise ähneln dann insofern einer Programmiersprache als dass es gewisse Zeichenketten gibt, die Beweise sind und gewisse, die es nicht sind, genauso wie gewisse Zeichenketten C-Programme sind und andere nicht. Für das Erlernen des mathematischen Arbeitens, das ja das Ziel dieser Lehrveranstaltung ist, ist eine solche Definition aber nicht zweckmäßig.

ableiten wollen. Die Behauptung ist hier: $S(s)$. Die **Behauptung** ist jene Aussage die wir (aus den Voraussetzungen) ableiten wollen. Der formale Beweis sieht dann, Zeile für Zeile, wie folgt aus:

1: $M(s)$ (Voraussetzung)	
2: $\forall x\ (M(x) \Rightarrow S(x))$ (Voraussetzung)	zz: $S(s)$
3: $M(s) \Rightarrow S(s)$ (aus 2 mittels Instanziierung I)	"
4: $S(s)$ (aus 1 und 3 mittels Modus Ponens MP)	"

Die dabei verwendeten logischen Schlüsse sind:

$$\frac{\forall x\, P(x)}{P(c)}\ \mathrm{I} \qquad \frac{A \quad A \Rightarrow B}{B}\ \mathrm{MP}$$

Eine zentrale Eigenschaft von Beweisen ist: an jeder Stelle eines Beweises gibt es gewisse Voraussetzungen, die zur Verfügung stehen, und eine Behauptung, die wir aus diesen Voraussetzungen beweisen wollen. In einem formalen Beweis schreiben wir Voraussetzungen in die linke Spalte und die aktuelle Behauptung in die rechte Spalte. Dabei stehen, außer den ursprünglichen Voraussetzungen, natürlich auch alle bereits bewiesenen Zwischenaussagen als Voraussetzungen für den nächsten logischen Schluss zur Verfügung. So sind z.B. die zwischen Zeile 3 und Zeile 4 zur Verfügung stehenden Voraussetzungen: $M(s)$, $\forall x\,(M(x) \Rightarrow S(x))$ und $M(s) \Rightarrow S(s)$. Die Behauptung an der Stelle zwischen Zeile 3 und Zeile 4 ist: $S(s)$.

Die Korrektheit eines Beweises ergibt sich daraus, dass erstens nur korrekte Schlussregeln verwendet werden und dass zweitens diese nur auf, an der jeweiligen Stelle, verfügbare Voraussetzungen angewandt werden. Der obige Beweis kann nach Zeile 4 abgeschlossen werden, da in dieser Zeile die zu zeigende Behauptung bereits abgeleitet wurde. Das Ende eines Beweises wird in mathematischen Texten oft durch eine kleine Box $\square$ oder durch die Abkürzung q.e.d. ("quod erat demonstrandum", lat. für "was zu beweisen war") markiert.

Verwendung von Quantoren. Im obigen Beispiel haben wir gesehen wie wir eine Voraussetzung der Form $\forall x\ P(x)$ in einem Beweis verwenden. Wie durch die Instanziierungsregel beschrieben, dürfen wir jederzeit und für jedes beliebige Objekt c einfach $P(c)$ voraussetzen. Wann das für welches Objekt sinnvoll ist, müssen bzw. dürfen wir selbst entscheiden.

Eine Voraussetzung der Form $\exists x\ P(x)$ zu verwenden bedeutet, die Existenz eines Objekts zu verwenden das die Eigenschaft $P(\cdot)$ hat, von dem wir sonst aber nichts wissen. Das geschieht in Beweisen mit Formulierungen wie z.B. "Sei x_0 so dass $P(x_0)$ gilt.", die dann typischerweise gefolgt sind von weiteren Berechnungen oder Argumenten, die auf x_0 Bezug nehmen, z.B. "Dann hat $f(x_0)$ die Eigenschaft ...". Dabei ist es natürlich wichtig, dass der Name x_0 noch nicht verwendet wurde, da wir über dieses neue Objekt ja nichts voraussetzen dürfen, außer dass es die Eigenschaft $P(\cdot)$ hat.

Definitionen in Beweisen. In Beweisen müssen wir oft mit definierten Begriffen umgehen. Typischerweise legt eine Definition, womöglich unter einer Nebenbedingung, fest, dass ihr Definiendum äquivalent zu ihrem Definiens ist. In einem Beweis dürfen (und müssen) wir diese Definition dann verwenden, indem wir, gegebenenfalls nach einer Überprüfung der Nebenbedingung, ihr Definiendum durch ihr Definiens ersetzen und umgekehrt. Das bezeichnen wir als **Expansion** oder Auffaltung einer Definition.

Veränderung der Behauptung. Im obigen Beweis haben wir die Behauptung nicht verändert. Sie war zu Beginn, genauso wie am Ende, des Beweises "*Sokrates ist sterblich.*" Oft ist es allerdings in einem Beweis nützlich, auch die Behauptung zwischendurch zu verändern bzw. zu vereinfachen.

Auch Veränderungen der Behauptung werden durch logische Schlüsse durchgeführt. Im folgenden wollen wir uns überlegen, wie das für Behauptungen die Allsätze bzw. Existenzsätze sind durchgeführt werden kann.

Wollen wir eine Behauptung der Form $\forall x\, P(x)$ beweisen, so setzen wir einfach ein beliebiges x_0 voraus und zeigen von diesem, dass es die Eigenschaft $P(\cdot)$ haben muss. Wichtig dabei ist, so wie oben, dass der Name x_0 noch nicht vergeben ist, da wir über dieses beliebige(!) Objekt nichts voraussetzen dürfen. Das ist die direkteste Methode, um Behauptungen zu behandeln, die Allaussagen sind. Es gibt aber auch andere Methoden, deren Verwendung manchmal zu bevorzugen ist, z.B. die Induktion, die wir in Kapitel 8 besprechen werden.

Wollen wir eine Behauptung der Form $\exists x\, P(x)$ beweisen, so reicht es, ein Objekt anzugeben, das die Eigenschaft $P(\cdot)$ hat. Auch in dieser Situation sind manchmal andere Vorgehensweisen sinnvoller, z.B. der indirekte Beweis, den wir in Kapitel 5 besprechen werden.

Ändern wir die Behauptung von A zu B, so drücken wir das oft aus, indem wir etwas sagen wie "es reicht also zu zeigen dass B".

Wir wollen nun einen Beweis durchführen, in dem wir mit Existenzaussagen und Definition arbeiten und auch die Behauptung verändern.

Satz. *Falls n gerade ist, dann ist auch n^2 gerade.*

Wir geben zunächst einen detaillierten Beweis an und übersetzen ihn dann in einen formalen Beweis. Der Zusammenhang zwischen diesen beiden Darstellungen wird durch die Verwendung von Farben illustriert.

Beweis (detailliert). Sei n gerade. D.h. es gibt ein k so dass $2 \cdot k = n$. Sei k_0 ein solches k, d.h., $2 \cdot k_0 = n$. Dann ist $n^2 = 4 \cdot k_0^2$. Es reicht zu zeigen, dass ein l existiert mit $2 \cdot l = n^2$. Sei $l = 2 \cdot k_0^2$. Dann reicht es zu zeigen, dass $4k_0^2 = n^2$. Das ist bereits bekannt. □

Beweis (formal).

1: n gerade (Voraussetzung)	zz: n^2 gerade
2: $\exists k\ 2 \cdot k = n$ (Expansion Definition)	"
3: $2 \cdot k_0 = n$ ($\exists$-Voraussetzung)	"
4: $n^2 = 4 \cdot k_0^2$ (Rechnung)	"
5:	es reicht zz: $\exists l\ 2 \cdot l = n^2$ (Expansion Definition)
6:	es reicht zz: $4 \cdot k_0^2 = n^2$ ($\exists$-Behauptung, $l = k_0^2$)

Nun sind wir fertig, da die Behauptung bereits eine Voraussetzung ist. □

Beide der obigen Darstellungen dieses Beweises sind sehr ausführlich und dienen nur dem Verständnis des Beweisbegriffs. Eine realistische Darstellung dieses Beweises, etwa im Kontext eines Lehrbuchs für das erste Studienjahr, wäre z.B.:

Beweis (realistisch). Sei $n = 2k$, dann ist $n^2 = 4k^2 = 2 \cdot 2k^2$, also ist auch n^2 gerade. □

Warnung 4.1. Geben Sie bei der Verwendung von $\exists$-Voraussetzungen auf die Variablennamen acht. Zwar ist das Prädikat "n ist gerade" definiert als $\exists k\, n = 2 \cdot k$, trotzdem wäre es aber falsch, in einem Beweis etwas zu schreiben wie: Seien n und m gerade. D.h. es gibt ein k mit $n = 2 \cdot k$ und ein k mit $m = 2 \cdot k$. Das "zweite k" muss einen anderen Namen haben, da es sich ja um ein anderes Objekt handelt. Korrekt müsste es zum Beispiel heißen: Seien n und m gerade. D.h. es gibt ein k mit $n = 2 \cdot k$ und ein l mit $m = 2 \cdot l$.

In einem realistischen Beweis werden viele Schritte, z.B. die Expansion von Definitionen, implizit durchgeführt. Es wird von Ihnen erwartet, dass Ihnen eine derartige Darstellung reicht, um den Beweis zu verstehen und insbesondere, um von ihm eine detaillierte oder formale Darstellung anzugeben.

Aussagenlogische Konnektive. Auch aussagenlogische Konnektive werden in Beweisen mit natürlichen Schlussregeln behandelt. Wie auch bei den Quantoren ist es dabei wichtig, zu unterscheiden, ob man eine Voraussetzung verwendet oder ob man die aktuelle Behauptung verändert.

Haben wir eine Voraussetzung der Form $A \wedge B$ können wir sowohl A als auch B als Voraussetzung verwenden. Die Verwendung einer Voraussetzung der Form $A \vee B$ bedeutet eine Fallunterscheidung zu machen: zunächst beweisen wir unsere Behauptung aus der Voraussetzung A, danach aus der Voraussetzung B. Diese Beweisstruktur werden wir in Kapitel 5 noch genauer behandeln. Eine Voraussetzung der Form $A \Rightarrow B$ verwenden wir wie im Sokrates-Beispiel mit dem logischen Schluss des Modus Ponens.

Haben wir eine Behauptung der Form $A \wedge B$, so kann diese gezeigt werden indem zunächst A und dann B gezeigt wird. Eine Behauptung der Form $A \vee B$ kann gezeigt werden indem A gezeigt wird oder indem B gezeigt wird, aber auch hier sind oft indirekte Beweise, siehe Kapitel 5, nützlich. Eine Behauptung der Form $A \Rightarrow B$ wird gezeigt indem unter der Voraussetzung A die Behauptung B gezeigt wird. Auch für Behauptungen der Form $A \Rightarrow B$ gibt es wichtige alternative Beweisformen, etwa den indirekten Beweise oder den Beweis der Kontraposition, siehe Kapitel 5.

Widerlegungen. Oft sind wir in der Mathematik auch in einer Situation, wo wir von einer gewissen Aussage A zeigen wollen dass sie falsch ist, d.h. wo wir A **widerlegen** wollen. Das ist gleichbedeutend damit zu zeigen dass $\neg A$ wahr ist. Wie wir Aussagen verneinen können und wie wir die dadurch erhaltenen Aussagen dann beweisen können wissen wir bereits. Damit ist also im Grunde vollständig erklärt was eine Widerlegung ist. Zur Verbesserung des Verständnisses wollen wir uns aber den wichtigen Spezialfall der Allaussagen ansehen.

Sei also A eine Aussage der Form $\forall x\ P(x)$. Dann ist die Verneinung von A äquivalent zu $\exists x\ \neg P(x)$. Um also zu zeigen dass A falsch ist, reicht es ein konkretes Objekt c anzugeben und zu zeigen dass $\neg P(c)$ gilt. Ein solches Objekt das die Eigenschaft $P(\cdot)$ nicht hat heißt auch **Gegenbeispiel** für die Behauptung $\forall x\ P(x)$.

Aufbau einer mathematischen Theorie. Damit haben wir nun die drei zentralen Elemente der mathematischen Sprache kennengelernt: Aussagen, Definitionen und Beweise. Eine mathematische Theorie ist im Wesentlichen eine Abfolge von Aussagen, Definitionen und Beweisen, die der Einschränkung genügen, dass zu jedem Zeitpunkt immer nur auf bereits Bekanntes aufgebaut wird: So dürfen, wie wir in Kapitel 3 gesehen haben, in einer Definition nur Begriffe verwendet werden, die bereits bekannt sind. Analog dazu dürfen in einem Beweis nur Aussagen verwendet werden, die wir bereits bewiesen haben oder die wir voraussetzen wollen.

Ein mathematischer Text enthält viele Aussagen. Es gibt eine ganze Reihe von Bezeichnungen für Aussagen, welche die Rolle der jeweiligen Aussage im Gesamttext andeuten sollen. Die wichtigste Bezeichnung für eine Aussage ist **Satz**. Ein Satz ist eine Aussage, die der Autor eines mathematischen Texts behauptet. Typischerweise folgt unmittelbar auf einen Satz ein Beweis dieses Satzes. Alternativ dazu wird auch manchmal die Bezeichnung **Theorem** verwendet. Oft werden besonders wichtige Sätze als Theoreme bezeichnet. Gelegentlich wird auch die Bezeichnung **Proposition** dafür verwendet. Oft sind Propositionen weniger wichtige Aussagen als Sätze. Ein **Lemma** (Plural "Lemmata") ist ein Hilfssatz: eine Aussage die zwar für sich genommen vielleicht nicht besonders interessant ist, die aber nützlich ist, um andere Aussagen zu beweisen. Ein **Korollar** ist eine Folgerung, die ganz

einfach aus einem (meist dem unmittelbar vorhergehenden) Satz bewiesen werden kann. Ein **Axiom** ist eine Grundaussage einer Theorie, die wir voraussetzen ohne sie zu beweisen. Axiome sind in mathematischen Texten eher selten, sie spielen vor allem bei der logischen Analyse der Grundlagen der Mathematik eine Rolle.

Das Wichtigste in Kürze.

- Ein Beweis ist eine Ableitung einer Aussage aus anderen Aussagen durch logische Schlüsse.
- An jeder Stelle eines Beweises gibt es gewisse Voraussetzungen, die zur Verfügung stehen, und eine Behauptung, die wir aus diesen Voraussetzungen beweisen wollen. Diese werden Schritt für Schritt durch logische Schlüsse transformiert.
- In einem realistischen Beweis werden viele Schritte implizit durchgeführt. Einen Beweis zu verstehen bedeutet auch, diese Schritte explizit machen zu können.
- Aussagen, Definitionen und Beweise sind die drei zentralen Elemente der mathematischen Sprache.

Kapitel 5

Beweistechniken

In Kapitel 4 haben wir bereits viele einfache logische Schlüsse kennengelernt, z.B. die Verwendung von All- und Existenzvoraussetzungen, Modifikationen von All- und Existenzbehauptungen, Expansion von Definitionen, Rechnungen, usw. In diesem Kapitel werden wir etwas komplexere Beweistechniken besprechen, die eine Auswirkung auf die globale Struktur eines Beweises haben. Eine dazu notwendige Vorarbeit besteht im Verständnis von Unterbeweisen.

Unterbeweise. Wir haben bereits Implikationen, also Aussagen der Form $A \Rightarrow B$ bewiesen, indem wir unter der Voraussetzung A die Behauptung B bewiesen haben. Dieser Vorgang kann auch verschachtelt werden. Angenommen wir stehen beim Schreiben eines formalen Beweises in der Zeile X, wo unter gewissen Voraussetzungen die Behauptung F zu zeigen ist. Dann können wir uns dazu entscheiden, in Zeile $X+1$ einen neuen **Unterbeweis** zu beginnen. In diesem können wir dann eine Voraussetzung A und eine Behauptung B frei wählen. Im Unterbeweis sind alle Voraussetzungen, die an der Zeile X vorhanden sind ebenfalls verwendbar. Sobald dieser Unterbeweis abgeschlossen ist, springen wir wieder zurück zur darüberliegenden Ebene. Wir erhalten damit, in der Zeile Y, aus dem Unterbeweis die neue Voraussetzung $A \Rightarrow B$. Die Behauptung ist wieder jene der darüberliegenden Ebene: F. Die Voraussetzung A steht ab Zeile Y nicht mehr zur Verfügung. Die Voraussetzung A und die Behauptung B haben also lediglich innerhalb des Unterbeweises Gültigkeit. Als formaler Beweis wird das wie folgt geschrieben:

X: ...	zz: F
$\quad \vert \quad X+1$: A	zz: B
$\quad \vert \quad \vdots$	$\vdots$
Y: $A \Rightarrow B$	zz: F

Ein Unterbeweis, der mit der Voraussetzung A und der Behauptung B beginnt, endet also immer mit $A \Rightarrow B$ als neuer Voraussetzung auf der darüberliegenden Ebene. Natürlich kann man in einem Unterbeweis auch mehrere Voraussetzungen $A_1, \dots, A_n$ einführen, indem man z.B. A auf $A_1 \wedge \cdots \wedge A_n$ setzt. Auch ist es möglich, innerhalb eines Unterbeweises einen neuen Unterbeweis zu beginnen. Diese Struktur kann also beliebig verschachtelt werden, ähnlich wie das z.B. auch beim Programmieren mit verschachtelten Schleifen möglich ist.

Fallunterscheidung. Eine Beweistechnik die in der Mathematik sehr häufig ist und sich Unterbeweisen bedient ist die Fallunterscheidung. Wir wollen zunächst einen Beweis mittels Fallunterscheidung führen und diesen dann im Detail analysieren.

Satz. *Für alle $n \in \mathbb{N}$ gilt:* $\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n+1}{2} \right\rfloor = n$.

Beweis. Wir machen eine Fallunterscheidung.

1. Falls n gerade ist, dann existiert ein $k \in \mathbb{N}$ mit $n = 2k$ und wir erhalten
$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} \right\rfloor + \left\lfloor \frac{2k+1}{2} \right\rfloor = \lfloor k \rfloor + \left\lfloor k + \frac{1}{2} \right\rfloor = 2k = n.$$
2. Falls n ungerade ist, dann existiert ein $k \in \mathbb{N}$ mit $n = 2k+1$ und wir erhalten
$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n+1}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor + \left\lfloor \frac{2k+2}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor + \lfloor k+1 \rfloor = k + k + 1 = n.$$

□

Wir wollen uns nun die Struktur eines formalen Beweises mittels Fallunterscheidung genauer überlegen. Im Allgemeinen haben wir eine Voraussetzung der Form $A \vee B$ und eine Behauptung C. Im obigen Beispiel wäre etwa $A \Leftrightarrow n$ ist gerade, $B \Leftrightarrow n$ ist ungerade und $C \Leftrightarrow \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n+1}{2} \right\rfloor = n$. Zunächst müssen wir, in Zeile X, die Aussage $A \vee B$ beweisen. Dann beweisen wir C aus der Voraussetzung A und danach C aus der Voraussetzung B. Damit haben wir also C aus $A \vee B$ bewiesen. Da $A \vee B$ bereits bewiesen ist, siehe Zeile X, ist damit auch C bewiesen. Als formaler Beweis sieht das wie folgt aus:

X: $A \vee B$	zz: C
$\quad \vert$ $X+1$: A	zz: C
$\quad \vert \quad \vdots$	$\quad \vdots$
Y: $A \Rightarrow C$	zz: C
$\quad \vert$ $Y+1$: B	zz: C
$\quad \vert \quad \vdots$	$\quad \vdots$
Z: $B \Rightarrow C$	zz: C
$Z+1$: C (aus X, Y, Z mittels Fallunterscheidung)	zz: C

Die Korrektheit des logisches Schlusses mit dem C in Zeile $Z+1$ abgeleitet wird basiert auf der Gültigkeit der Äquivalenz
$$(A \vee B \Rightarrow C) \Leftrightarrow (A \Rightarrow C) \wedge (B \Rightarrow C).$$
Auf Basis dieser Äquivalenz erhalten wir zunächst $A \vee B \Rightarrow C$ aus den Zeilen Y und Z und sodann C aus der Zeile X mittels Modus Ponens.

Fallunterscheidungen können allgemeiner als im obigen Beispiel gewählt werden. So müssen Fallunterscheidungen nicht immer disjunkt sein, z.B. können wir für eine reelle Zahl x die Fallunterscheidung $x \leq 0 \vee x \geq 0$ verwenden. Dann wird der Fall $x = 0$ doppelt behandelt, was aber genauso zu einem logisch korrekten (wenn auch etwas redundantem) Beweis führt. Auch können wir in mehr als zwei Fälle aufspalten, z.B. kann für eine reelle Zahl x auch die Fallunterscheidung $x < 0 \vee x = 0 \vee x > 0$ verwenden. Andere häufige Fallunterscheidungen sind z.B. für $x, y \in \mathbb{R}$: $x \leq y \vee y \geq x$, für $n \in \mathbb{N}$: $n \equiv 0 \pmod 3 \vee n \equiv 1 \pmod 3 \vee n \equiv 2 \pmod 3$ oder entsprechend für die Restklassen modulo $m > 3$, für eine Primzahl p und eine natürliche Zahl n: $p \mid n$ oder $p \nmid n$.

Essentiell ist allerdings dass eine Fallunterscheidung vollständig ist, d.h. dass alle Möglichkeiten abgedeckt werden. So ist etwa für $n \in \mathbb{N}$ die Fallunterscheidung "n ist gerade oder n ist Primzahl" nicht vollständig, da ungerade zusammengesetzte Zahlen wie z.B. 9 nicht abgedeckt sind. Eine unvollständige Fallunterscheidung $A \vee B$ kann nicht bewiesen werden und damit kann $A \vee B$ in Zeile X nicht als Voraussetzung zur Verfügung stehen.

Kontraposition. Eine Aussage der Form $A \Rightarrow B$ wird meistens bewiesen indem unter der Voraussetzung A die Behauptung B gezeigt wird. Gelegentlich ist es aber einfacher stattdessen unter der Voraussetzung $\neg B$ die Behauptung $\neg A$ zu zeigen. Das ist ebenfalls ein Beweis von $A \Rightarrow B$ da die Formel

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

gültig ist. Die Formel $\neg B \Rightarrow \neg A$ heißt **Kontraposition** der Formel $A \Rightarrow B$. Betrachten wir ein Beispiel.

Satz. *Wenn $3n + 1$ ungerade ist, dann ist n gerade.*

Beweis. Sei n ungerade. Dann ist $n = 2k + 1$. Damit ist $3n + 1 = 6k + 4 = 2(3k + 2)$. Also ist $3n + 1$ gerade. □

Im Allgemeinen sehen formale Beweise mittels Kontraposition wie folgt aus: Wir haben eine Behauptung der Form $A \Rightarrow B$. Wir führen einen neuen Unterbeweis mit der Voraussetzung $\neg B$ und der Behauptung $\neg A$. Sobald dieser abgeschlossen ist erhalten wir $\neg B \Rightarrow \neg A$ was wir mittels Kontraposition zu $A \Rightarrow B$ ändern. Als formalen Beweis schreibt man das wie folgt.

X: ...	zz: $A \Rightarrow B$
$\quad \vert \; X + 1$: $\neg B$	zz: $\neg A$
$\quad \vert \quad \vdots$	$\quad \vdots$
Y: $\neg B \Rightarrow \neg A$	zz: $A \Rightarrow B$
$Y + 1$: $A \Rightarrow B$ (aus Y mittels Kontraposition)	zz: $A \Rightarrow B$

Warnung 5.1. Die Implikation $A \Rightarrow B$ ist zwar äquivalent zu ihrer Kontraposition $\neg B \Rightarrow \neg A$, nicht aber zu $\neg A \Rightarrow \neg B$, wie sich leicht mit einer Wahrheitstafel nachrechnen lässt.

Stehen zu Beginn eines Beweises mittels Kontraposition mehrere Voraussetzungen zur Verfügung, kann man sich aussuchen welche man invertiert, da ja z.B. die Formel

$$(A_1 \wedge A_2 \Rightarrow B) \Leftrightarrow (A_1 \wedge \neg B \Rightarrow \neg A_2) \Leftrightarrow (A_2 \wedge \neg B \Rightarrow \neg A_1)$$

gültig ist.

Indirekter Beweis. Ein **indirekter Beweise** einer Behauptung A geht so vor, dass wir aus der Voraussetzung $\neg A$ einen Widerspruch ableiten. Das ist ein Beweis von A, da die Äquivalenz

$$A \Leftrightarrow (\neg A \Rightarrow \bot) \qquad (*)$$

gültig ist, wie sich leicht mit einer Wahrheitstafel nachrechnen lässt. Das Zeichen $\bot$ (ausgesprochen als "Falsum", lat. für Unwahrheit) steht für einen logischen Widerspruch. Der Wahrheitswert von $\bot$ ist immer 0. Ein berühmtes Beispiel für einen indirekten Beweis ist der Euklidsche Beweis für die Unendlichkeit der Primzahlen:

Satz. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, es gäbe nur endlich viele Primzahlen. Dann können wir sie als $p_1, \ldots, p_n$ bezeichnen. Sei $m = \prod_{i=1}^{n} p_i + 1$. Dann gilt für alle $i = 1, \ldots, n$ dass $p_i \nmid m$. Nun hat aber jede Zahl einen Primteiler, also hat auch m einen Primteiler q. Dann ist aber q keines der p_i. Widerspruch. □

Ein weiteres bekanntes Beispiel für einen indirekten Beweis ist der Beweis der Irrationalität von $\sqrt{2}$. In diesem nehmen wir an, dass $\sqrt{2}$ rational ist, d.h. eine Darstellung als (gekürzter) Bruch hat. Daraus leiten wir mit einigen elementaren Überlegungen einen Widerspruch ab, womit also gezeigt ist dass $\sqrt{2}$ nicht rational ist, d.h. also irrational ist.

Im Allgemeinen sieht ein indirekter formaler Beweis wie folgt aus: Wir haben eine Behauptung A und beginnen einen neuen Unterbeweis mit der Annahme $\neg A$ und der Behauptung $\bot$. Durch Abschluss dieses Unterbeweises erhalten wir die Implikation $\neg A \Rightarrow \bot$ als Voraussetzung. Daraus erhalten wir mittels $(*)$ sofort A. Als formaler Beweis geschrieben hat ein indirekter Beweis die folgende Form:

X: ...	zz: A
$\quad \vert \; X+1$: $\neg A$	zz: $\bot$
$\quad \vert \qquad \vdots$	$\qquad \vdots$
Y: $\neg A \Rightarrow \bot$	zz: A
$Y+1$: A (aus Y mittels $(*)$)	zz: A

Beweise von Äquivalenzen. Die Äquivalenz von Aussagen spielt in der Mathematik eine große Rolle. Dementsprechend ist es oft notwendig zu zeigen dass zwei gegebene Aussagen A und B äquivalent sind, das heißt also die Formel $A \Leftrightarrow B$ zu beweisen. Dies geschieht oft, indem zuerst $A \Rightarrow B$ und dann $B \Rightarrow A$ bewiesen wird. Das ist ein vollständiger Beweis von $A \Leftrightarrow B$, da ja die folgende Formel gültig ist:

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

Diese Vorgehensweise lässt sich auf Beweise der Äquivalenz mehrerer Aussagen verallgemeinern. Um zu zeigen dass die Aussagen $A_1, A_2, \dots, A_n$ äquivalent sind, reicht es die folgenden Aussagen zu zeigen: $A_1 \Rightarrow A_2, \dots, A_{n-1} \Rightarrow A_n, A_n \Rightarrow A_1$. Damit folgen die Implikationen also einer Kreisform von A_1 bis nach A_n und dann wieder zurück zu A_1. Betrachten wir ein Beispiel:

Satz. *Seien $n, m \geq 1$. Die folgenden Aussagen sind äquivalent:*

1. *$n \mid m$.*
2. *Es gibt ein $k \geq 1$ so dass $n = \mathrm{ggT}(m, k)$.*
3. *Jeder Teiler von n ist ein Teiler von m.*

Beweis. $1 \Rightarrow 2$: Wir nehmen $n \mid m$ an. Wir setzen $k = n$. Dann gilt $\mathrm{ggT}(m, k) = n$.

$2 \Rightarrow 3$: Wir nehmen $n = \mathrm{ggT}(m, k)$ an. Dann gilt auch $n \mid m$. Sei nun l ein beliebiger Teiler von n. Dann haben wir $l \mid n$ und $n \mid m$, also $l \mid m$.

$3 \Rightarrow 1$: Wir nehmen an dass jeder Teiler von n ein Teiler von m ist. Nun ist aber n ein Teiler von sich selbst. Also gilt $n \mid m$. □

In diesem Beweis gibt es also drei Unterbeweise: für jede der Implikationen $1 \Rightarrow 2$, $2 \Rightarrow 3$ und $3 \Rightarrow 1$ einen. Mit einem solchen Beweis kann man sich im Vergleich zum Nachweis aller paarweisen Äquivalenzen einiges an Arbeit ersparen. Konkret mussten wir im obigen Beweis nur drei Implikationen beweisen. Hätten wir die Äquivalenzen $1 \Leftrightarrow 2$, $1 \Leftrightarrow 3$ sowie $2 \Leftrightarrow 3$ über jeweils zwei Implikationen bewiesen, hätten wir insgesamt sechs Implikationen zu beweisen gehabt.

Sinn von Beweisen. Der primäre Sinn eines Beweises besteht darin, zu überzeugen **dass** die behauptete Aussage wahr ist. Zunächst einmal geht es dabei darum, dass der Autor eines Beweis sich selbst davon überzeugt, dass die Aussage, und zwar ohne den geringsten Rest eines Zweifels zu erlauben, wahr ist. Um das zu erreichen bietet eine rigide und detaillierte Beweisführung genau den richtigen Rahmen.

In weiterer Folge erfüllt ein Beweis aber auch den Zweck, einen Leser oder einen Zuhörer davon zu überzeugen, dass die behauptete Aussage wahr ist. In diesem Sinn ist ein Beweis ein Akt der Kommunikation. In diesem gibt es einen Sender, einen Empfänger und einen Kontext. So betrachtet überrascht es nicht dass, je nach Situation, Beweise unterschiedlich dargestellt werden, insbesondere was ihren Detailliertheitsgrad angeht. So wird z.B. ein Lehrbuch für das erste Studienjahr Beweise detaillierter präsentieren als weiterführende Werke, die schon viel mathematisches Wissen voraussetzen. Auch macht es für die Darstellung einen Unterschied, ob ein Beweis mündlich oder schriftlich präsentiert wird. In diesem Zusammenhang ist auch die Frage "Wie genau muss ich das beweisen?" zu beantworten: so genau nämlich, wie es dem Kontext angemessen ist. Um Missverständnisse nach Möglichkeit auszuschließen, ist man aber im Zweifel lieber zu genau als nicht genau genug.

Der zweite wichtige Sinn von Beweisen besteht darin zu erklären, **wieso** die behauptete Aussage wahr ist. Derartige Einsichten sind nicht nur wesentlich für das Verständnis einer mathematischen Theorie, sie erlauben es in weiterer Folge auch, ähnliche Aussagen mit ähnlichen Beweisen selbst zu zeigen, was auch für Anwendungen von großer Bedeutung ist. Deswegen ist es auch wichtig, Beweise genau zu lesen: man versteht nicht nur die Zusammenhänge besser, sondern man lernt auch, von den grundlegenden Beweisideen bis zu Details der Formulierung, wie man selbst Beweise entwickeln kann. Durch bloßes Auswendiglernen der bewiesenen Sätze ist das nicht möglich. Diese zweite Funktion von Beweisen erklärt auch, wieso es in der Mathematik üblich ist, von wichtigen Sätzen mehrere Beweise zu betrachten. So hat z.B. C. F. Gauß selbst acht verschiedene Beweise des quadratischen Reziprozitätsgesetzes, eines wichtigen Resultats der Zahlentheorie, angegeben.

Das Wichtigste in Kürze.

- In einem Beweis mittels Fallunterscheidung wird die Behauptung in jedem der Fälle gesondert bewiesen. Die Vollständigkeit der Fallunterscheidung ist für die Korrektheit des Beweises unverzichtbar.
- Ein Beweis durch Kontraposition beruht auf der Äquivalenz $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$.
- Ein indirekter Beweis beruht auf der Äquivalenz $A \Leftrightarrow (\neg A \Rightarrow \bot)$.
- Eine Äquivalenz $A \Leftrightarrow B$ wird typischerweise gezeigt, indem $A \Rightarrow B$ und, getrennt davon, $B \Rightarrow A$ gezeigt wird.

Kapitel 6

Mengen

Der Begriff der Menge spielt eine zentrale Rolle in der Mathematik. Mengen sind, in informatischer Terminologie ausgedrückt, die wichtigste Datenstruktur der Mathematik. G. Cantor definierte den Mengenbegriff wie folgt: Eine **Menge** ist eine Zusammenfassung von wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen[1]. Die in einer Menge M zusammengefassten Objekte heißen **Elemente** von M.

Dass die Elemente einer Menge "wohlunterschieden" sind, bedeutet nichts anderes als dass jedes Objekt höchstens ein Mal in der Menge vorkommt: entweder es kommt vor oder nicht, es kann aber nicht mehrfach vorkommen. Dass es sich bei einer Menge um eine "Zusammenfassung" handelt bedeutet, dass es auf die Reihenfolge der Elemente einer Menge nicht ankommt. Zwei Mengen sind also genau dann gleich, wenn sie die selben Elemente haben.

Intuitiv können wir uns also eine Menge vorstellen wie ein Sack, der gewisse Gegenstände, die Elemente, enthält. Natürlich kann ein Sack auch weitere Säcke enthalten – ebenso können die Elemente einer Menge wieder Mengen sein. Die leere Menge, die wir uns vorstellen als "leeren Sack" ist definiert als die eindeutige Menge die gar kein Element hält.

Wir schreiben "$x \in M$", um auszudrücken dass das Objekt x ein Element der Menge M ist. Wir sagen dann auch: "M enthält x" oder "x ist in M enthalten". Wenn wir ausdrücken wollen, dass mehrere Objekte, z.B. x, y und z in der Menge M sind, so können wir das tun indem wir schreiben "$x \in M$ und $y \in M$ und $z \in M$" oder, kürzer, "$x, y, z \in M$". Wir schreiben "$x \notin M$", um auszudrücken, dass x nicht in M enthalten ist. Wir schreiben $\emptyset$, oder manchmal auch $\{\}$, für die leere Menge. Damit gilt also $x \notin \emptyset$ für alle x.

Definition von Mengen. Eine Menge kann auf verschiedene Arten definiert werden: Die einfachste Form besteht darin, einfach all ihre Elemente explizit **aufzählen**. So können wir etwa die Mengen $A = \{1, 2, 3, 4, 5\}$, $B = \{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$ oder $C = \{A, B\}$ definieren. Diese Vorgehensweise ist nur bei (kleinen) endlichen Mengen sinnvoll. Da es bei Mengen nicht auf die Reihenfolge ankommt und jedes Element nur vorkommt oder nicht vorkommt, nicht aber mehrere Male vorkommen kann, ist z.B. $\{2, 2, 1\} = \{1, 2\}$. Auch wenn dieses Beispiel etwas künstlich erscheint, ist es in einer Situation wo über unbekannte Objekte $x_1, \ldots, x_n$ gesprochen wird eine Erleichterung, eine Menge als $\{x_1, \ldots, x_n\}$

[1] Aus heutiger Perspektive ist diese Definition überholt, da sie zu verschiedenen Paradoxien führt. Wir geben sie hier trotzdem an, da sie die Intention der Begriffsbildung kurz und bündig klarstellt und die erwähnten Paradoxien für uns keine Rolle spielen werden. Ein solider Mengenbegriff kann auf Basis der axiomatischen Mengenlehre entwickelt und als Grundlage der Mathematik verwendet werden.

anschreiben zu können, ohne vorher zeigen zu müssen, dass $x_1, \dots, x_n$ paarweise unterschiedlich[2] sind.

Wesentlich häufiger wird eine Menge durch eine **Beschreibung** definiert, d.h. durch Angabe eines definierenden Prädikats. Die dazu verwendete Notation hat die Form

$$A = \{x \mid P(x)\}$$

was gelesen wird als "A ist die Menge aller x für die $P(x)$ gilt.". Alternativ zu dieser Notation wird oft auch $A = \{x : P(x)\}$ oder gelegentlich auch $A = \{x / P(x)\}$ geschrieben. Auf diese Weise können wir z.B. die Menge aller geraden ganzen Zahlen definieren als $G = \{n \mid n \in \mathbb{Z} \wedge n \text{ ist gerade}\}$. Man beachte dass eine solche Definition drei Teile hat: 1. den Namen A der definierten Menge, 2. den Namen x einer Variablen die für die Elemente der Menge steht und 3. ein Prädikat $P(x)$ das von der freien Variable x abhängt. Diese Notation bindet die Variable x, so dass x im Ausdruck $\{x \mid P(x)\}$ nur mehr gebunden vorkommt.

Wir erlauben uns gelegentlich von der strikten Form $A = \{x \mid P(x)\}$ dieser Definition abzuweichen. Die folgenden beiden Kurznotationen sind nützlich und werden in der Mathematik häufig verwendet:

1. Falls die Definition von der Form

$$A = \{x \mid x \in M \wedge P(x)\}$$

ist, d.h. falls es eine Grundmenge, ein Universum M, gibt aus dem die Elemente entnommen werden, dann schreibt man diese Definition auch, etwas kürzer, als

$$A = \{x \in M \mid P(x)\}.$$

Das wird ausgesprochen als "A ist die Menge aller x in M mit $P(x)$.". Damit können wir also z.B. die Definition von G kürzer darstellen als $G = \{n \in \mathbb{Z} \mid n \text{ ist gerade}\}$. Auch Varianten dieser Notation sind gebräuchlich. So würde man z.B. die Menge aller Mengen ganzer Zahlen, die keine Primzahlen enthalten, wie folgt anschreiben: $\{A \subseteq \mathbb{Z} \mid A \cap \mathbb{P} = \emptyset\}$.

2. Ist die Definition einer Menge von der Form

$$A = \{y \mid \exists x\, (y = f(x) \wedge P(x))\}$$

für eine Funktion f, so schreibt man diese Definition auch als

$$A = \{f(x) \mid P(x)\}.$$

Das wird ausgesprochen als "A ist die Menge aller $f(x)$ mit $P(x)$." Die Menge der Quadratzahlen kann so z.B. definiert werden durch $Q = \{n^2 \mid n \in \mathbb{N}\}$ da $n \mapsto n^2$ eine Funktion ist.

Wir haben also gesehen dass ein Prädikat mit einer freien Variable eine Menge definiert. Umgekehrt definiert auch eine Menge A ein Prädikat mit einer freien Variable, nämlich $x \in A$. Wir können also Mengen mit Prädikaten mit einer freien Variable identifizieren.

Teilmengen. Eine Menge A heißt **Teilmenge** einer Menge B falls jedes Element von A auch Element von B ist. Wir schreiben auch $A \subseteq B$ für "A ist Teilmenge von B". $A \subseteq B$ bedeutet also nichts anderes als $\forall x\ (x \in A \Rightarrow x \in B)$. Dementsprechend zeigt man eine Aussage der Form $A \subseteq B$ meistens indem man von einem beliebigen x annimmt dass $x \in A$ ist und dann aus dieser Voraussetzung die Behauptung $x \in B$ beweist.

[2]Wir sagen von Objekten $x_1, \dots, x_n$ dass sie paarweise unterschiedlich sind falls $x_i \neq x_j$ für alle i, j mit $i \neq j$ gilt. So sind z.B. $1, 2$ paarweise unterschiedlich, $2, 2, 1$ aber nicht.

Ähnlich ist es mit der Gleichheit zweier Mengen: $A = B$ ist äquivalent zu $\forall x\,(x \in A \Leftrightarrow x \in B)$, was wiederum äquivalent ist zu $A \subseteq B \wedge B \subseteq A$. Dementsprechend ist auch eine der verbreitetsten Beweistechniken zum Nachweis einer Identität $A = B$ von Mengen, zunächst $A \subseteq B$ und dann $B \subseteq A$ zu zeigen.

Wir sagen dass A eine **echte Teilmenge** von B ist falls $A \subseteq B$ ist und außerdem $A \neq B$ ist. Das wird oft als $A \subset B$ oder auch als $A \subsetneq B$ geschrieben.

Boolesche Operationen auf Mengen. Es ist oft nützlich auf Basis von bereits vorhandenen Mengen weitere Mengen zu definieren. Wir werden jetzt einige Operationen auf Mengen kennenlernen. Seien A und B Mengen. Dann definieren wir:

Der **Durchschnitt** von A und B ist die Menge $A \cap B = \{x \mid x \in A \wedge x \in B\}$. Der Durchschnitt von A und B enthält also genau die gemeinsamen Elemente von A und B. Zwei Mengen A und B heißen **disjunkt**, falls sie keine gemeinsamen Elemente haben, das heißt also falls $A \cap B = \emptyset$.

Die **Vereinigung** von A und B ist die Menge $A \cup B = \{x \mid x \in A \vee x \in B\}$. Die Vereinigung zweier Mengen besteht also aus all jenen Objekten die Element von mindestens einer der beiden Mengen sind.

Die **Differenzmenge** von A und B ist die Menge $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$. Die Differenzmenge wird auch ausgesprochen als "A ohne B". Eine andere gebräuchliche Notation für $A \setminus B$ ist $A - B$.

Warnung 6.1. Während zwar $A \cup B = B \cup A$ und $A \cap B = B \cap A$ gilt, ist im Allgemeinen $A \setminus B \neq B \setminus A$.

Oft arbeiten wir mit einer bestimmten Grundmenge, einem Universum M. Das **Komplement** einer Menge $A \subseteq M$ bezüglich M ist die Menge $A^c = M \setminus A = \{x \in M \mid x \notin A\}$. Oft ist M aus dem Kontext heraus klar und wird nicht mehr explizit erwähnt. Alternative Notationen für das Komplement der Menge A sind A' sowie $\overline{A}$.

Zur Veranschaulichung von Situationen die eine geringe Anzahl von Mengen involvieren zeichnet man oft **Venn-Diagramme**, siehe Abbildung 6.1.

Man sieht leicht, dass diese Operationen auf Mengen eng verwandt mit der Aussagenlogik sind. So entspricht die Vereinigung $\cup$ der Disjunktion $\vee$, der Durchschnitt $\cap$ der Konjunktion $\wedge$ und das Komplement $\cdot^c$ der Negation $\neg$. Auf Basis dieser Korrespondenz können wir auch Wahrheitstafeln benutzen um Mengenidentitäten und -inklusionen zu beweisen. So übersetzt sich z.B. die de Morgan Regel $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ für beliebige Aussagen A und B direkt in die Mengengleichheit $(\mathcal{A} \cup \mathcal{B})^c = \mathcal{A}^c \cap \mathcal{B}^c$ indem wir ein beliebiges Objekt x fixieren und dann beobachten, dass

$$x \in (\mathcal{A} \cup \mathcal{B})^c \Leftrightarrow \neg(\underbrace{x \in \mathcal{A}}_{A} \vee \underbrace{x \in \mathcal{B}}_{B}) \Leftrightarrow \neg x \in \mathcal{A} \wedge \neg x \in \mathcal{B} \Leftrightarrow x \in \mathcal{A}^c \cap \mathcal{B}^c.$$

Dabei haben wir die Aussage $x \in \mathcal{A}$ als A und $x \in \mathcal{B}$ als B abgekürzt. Das lässt sich auch direkt mit einer Wahrheitstafel wie folgt nachrechnen:

$x \in \mathcal{A}$	$x \in \mathcal{B}$	$x \in \mathcal{A} \cup \mathcal{B}$	$x \in (\mathcal{A} \cup \mathcal{B})^c$	$x \in \mathcal{A}^c$	$x \in \mathcal{B}^c$	$x \in \mathcal{A}^c \cap \mathcal{B}^c$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

Jede aussagenlogische Äquivalenz induziert also eine Mengenidentität.

Analog dazu können aus gültigen aussagenlogischen Implikationen Mengeninklusionen abgelesen werden. So ist z.B. $A \wedge B \Rightarrow A \wedge (B \vee C)$ eine gültige Formel woraus sofort folgt dass, für beliebige

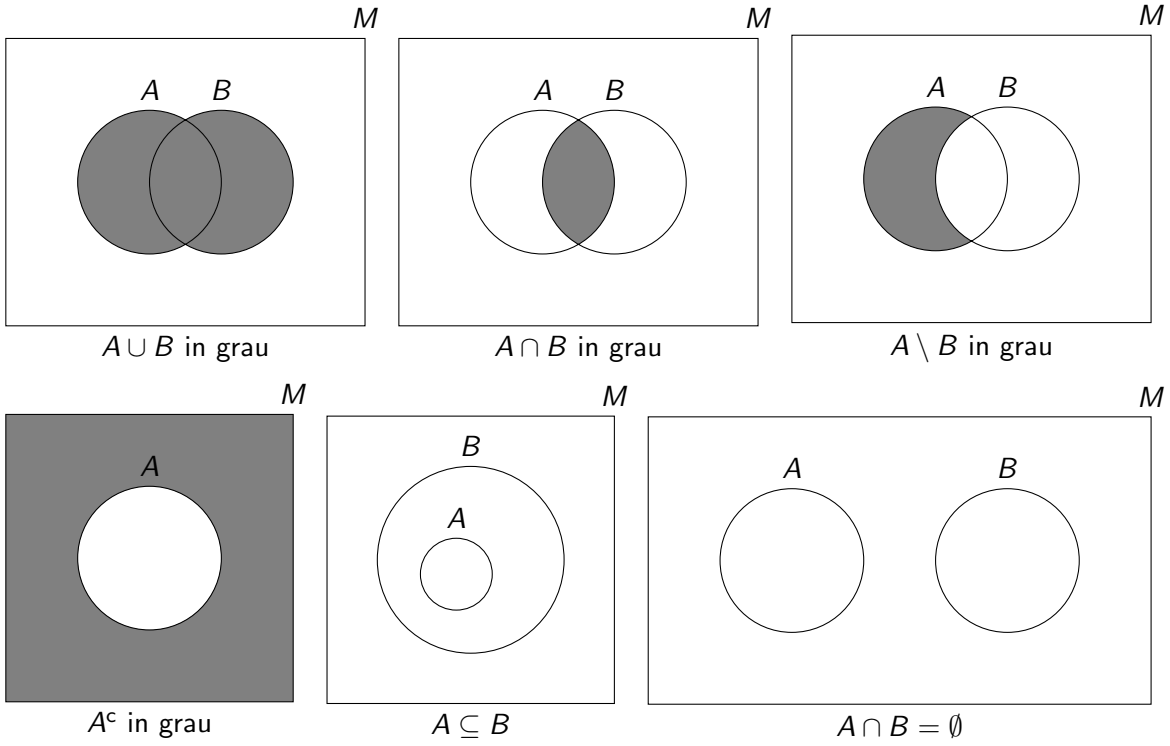


Abbildung 6.1: Venn-Diagramme

Mengen $\mathcal{A}$, $\mathcal{B}$ und $\mathcal{C}$ gilt: $\mathcal{A} \cap \mathcal{B} \subseteq \mathcal{A} \cap (\mathcal{B} \cup \mathcal{C})$ indem wir ein beliebiges Objekt x fixieren und, so wie oben, für A die Aussage $x \in \mathcal{A}$ verwenden, für B die Aussage $x \in \mathcal{B}$ und für C die Aussage $x \in \mathcal{C}$.

Weitere Operationen auf Mengen. Gegeben zwei beliebige Objekte x und y können wir das **geordnete Paar** (x, y) bilden. Das Adjektiv geordnet bezieht sich auf die Eigenschaft $(x, y) \neq (y, x)$. Da in der Mathematik meistens geordnete Paare betrachtet werden, wird ein geordnetes Paar oft auch einfach als **Paar** bezeichnet. Diese Form der Zusammenfassung von Objekten kann verallgemeinert werden: Wir können Objekte $x_1, \dots, x_n$ in das n-Tupel $(x_1, \dots, x_n)$ zusammenfassen. 2-Tupel sind also Paare, 3-Tupel heißen auch **Tripel**. Anders als bei einer Menge kommt es also bei einem Tupel auf die Reihenfolge an. Außerdem kann ein Tupel das selbe Element mehrfach enthalten.

Das **kartesische Produkt** zweier Mengen A und B ist die Menge $A \times B = \{(x, y) \mid x \in A \wedge y \in B\}$, also die Menge aller geordneter Paare deren erste Komponente aus A und deren zweite Komponente aus B kommt. So ist z.B. $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$. Oft spricht man auch einfach nur vom **Produkt**. Das Produkt der Mengen $A_1, \dots, A_n$ ist die Menge $A_1 \times \cdots \times A_n = \{(x_1, \dots, x_n) \mid x_1 \in A_1, \dots, x_n \in A_n\}$.

Warnung 6.2. Verwechseln Sie nicht $(a, b) \in M$ mit $a, b \in M$ Die Schreibweise $a, b \in M$ ist eine Abkürzung für $a \in M \wedge b \in M$ und bedeutet also, dass die beiden Objekte a und b Elemente von M sind. Die Schreibweise $(a, b) \in M$ bedeutet, dass das (geordnete) Paar (a, b) ein Element von M ist.

Die **Kardinalität** einer Menge A ist die Anzahl der Elemente von A und wird als $|A|$ geschrieben. Für eine endliche Menge A ist $|A|$ einfach eine natürliche Zahl. So ist z.B. $|\{n \in \mathbb{N} \mid n \text{ teilt } 10\}| = 4$. Oft schreibt man $|A| = \infty$ um auszudrücken dass die Menge A unendlich viele Elemente hat[3].

[3] Auch im Unendlichen kann man noch verschieden große Mengen unterscheiden. So haben z.B. $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ die

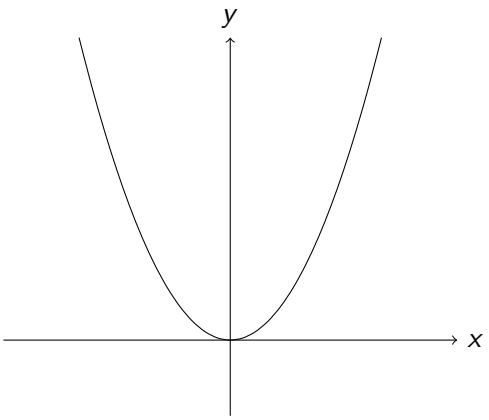


Abbildung 6.2: Graph der Funktion $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$

Die **Potenzmenge** einer Menge A ist die Menge $\mathcal{P}(A) = \{B \mid B \subseteq A\}$. Die Potenzmenge von A ist also die Menge aller Teilmengen von A. So ist z.B.

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

Für eine endliche Menge A gilt $|\mathcal{P}(A)| = 2^{|A|}$.

Relationen. Seien A und B Mengen. Eine Menge Menge $R \subseteq A \times B$ heißt **Relation zwischen** A **und** B. Eine Relation R zwischen A und B ist also eine Menge von geordneten Paaren. Für $x \in A$ und $y \in B$ sagen wir "x steht in der Relation R zu y" falls $(x, y) \in R$ gilt. In Symbolen schreiben wir das als $x\,R\,y$. Häufig betrachten wir Relationen im Fall wo $A = B$ ist. Dann sprechen wir einfach von einer **Relation auf** A. Für eine Relation R auf A ist auch die Notation (A, R) gebräuchlich, z.B. $(\mathbb{Z}, \equiv_2)$ für die Äquivalenz modulo 2 auf den ganzen Zahlen.

Wir kennen bereits viele Beispiele für Relationen. So ist z.B. $\leq$ (kleiner-gleich) auf $\mathbb{R}$ eine Relation und für jede natürliche Zahl $m \geq 2$ ist $\equiv_m$ (kongruent modulo m) eine Relation auf $\mathbb{Z}$. Wir werden in Kapitel 9 noch weitere Relationen und Klassen von Relationen kennenlernen.

Funktionen. In vielen Situation spielen mehrere Größen eine Rolle und wir wissen, oder können beobachten, dass eine Größe dabei von einer oder mehreren anderen eindeutig bestimmt wird. In der Mathematik wird eine solche Abhängigkeit durch den Begriff der Funktion, oder synonym dazu auch: der Abbildung, modelliert. Betrachten wir z.B. den Bremsweg eines Autos, so hat das Auto zu jedem Zeitpunkt eine eindeutig bestimmte Geschwindigkeit. Wir schreiben dann die Geschwindigkeit zum Zeitpunkt t als $v(t)$ um diese Abhängigkeit auszudrücken. Funktionen bzw. Abbildungen spielen eine zentrale Rolle in der gesamten Mathematik

Wir haben bereits gelegentlich mit Funktionen gearbeitet und über Funktionen gesprochen. Formal können wir Funktionen über Relationen definieren. Seien A und B Mengen. Eine **Funktion** oder **Abbildung** von A nach B ist ein Tripel $f = (A, B, G)$ wobei $G \subseteq A \times B$ und $\forall x \in A \exists! y \in B : \; x\,G\,y$. A heißt dann **Definitionsmenge** der Abbildung f, B heißt **Zielmenge** von f und G heißt **Graph** von f. Der Graph einer Funktion von $\mathbb{R}$ nach $\mathbb{R}$ kann auf die bekannte Weise visualisiert werden, siehe z.B. Abbildung 6.2. Das einem $x \in A$ durch G eindeutig zugeordnete y heißt **Bild von** x und wird

selbe Kardinalität. Außerdem haben $\mathbb{R}$ und $\mathbb{C}$ die selbe Kardinalität. Diese beiden Kardinalitäten unterscheiden sich aber. Eine detailliertere Beschreibung dieser Situation würde hier aber zu weit führen.

als $f(x)$ geschrieben. Die **Bildmenge** von f ist $f(A) = \{f(x) \mid x \in A\}$. Achtung: Die Bildmenge ist immer eine Teilmenge der Zielmenge ,d.h. es gilt $f(A) \subseteq B$, sie muss aber nicht gleich der Zielmenge sein.

Zur Definition von Funktionen gibt es zwei gebräuchliche Kurznotationen. Um z.B. das Quadrieren in den reellen Zahlen zu definieren kann man $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ schreiben. Das wird ausgesprochen als "Sei f die Funktion von den reellen Zahlen in die reellen Zahlen die x auf x^2 abbildet.". Eine alternative Notation ist $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$, was wie folgt ausgesprochen wird: "Sei f die Funktion von den reellen Zahlen in die reellen Zahlen mit $f(x) = x^2$.".

Warnung 6.3. Vermischen Sie diese beiden Notationen nicht. Ausdrücke wie $f(x) \mapsto x^2$ ergeben keinen Sinn, da ja nicht $f(x)$ auf x^2 abgebildet wird, sondern x.

Das Wichtigste in Kürze.

- Eine Menge ist eine Zusammenfassung von wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.
- Mengen können mit einstelligen Prädikaten identifizert werden. So definiert ein Prädikat $P(x)$ die Menge aller Objekte, die P erfüllen (geschrieben als $\{x \mid P(x)\}$). Umgekehrt definiert eine Menge A das Prädikat Element dieser Menge zu sein (geschrieben als $x \in A$).
- Boolesche Operationen, die ja bereits von Prädikaten bekannt sind, können direkt auf Mengen angewandt werden. Andere wichtige Operation auf Mengen sind das kartesische Produkt und die Potenzmenge.
- Relationen und Funktionen können als Mengen aufgefasst, bzw. über Mengen definiert werden.

Kapitel 7

Gleichungen

Gleichungen sind eine der wichtigsten Arten von Aussagen in der Mathematik. Eine **Gleichung** ist ein Ausdruck der Form $t = s$, wobei t und s Terme sind, die mathematische Objekte beschreiben. Die Gleichung $t = s$ drückt aus, dass die beiden Terme t und s das selbe Objekt bezeichnen. Wenn eine Gleichung keine Variablen enthält, dann ist sie eine Aussage. Z.B. ist die Gleichung $2 + 2 = 3 + 1$ eine wahre Aussage und die Gleichung $2 + 2 = 3$ eine falsche Aussage. Falls die Gleichung Variablen enthält, ist sie ein Prädikat. So ist z.B. die Gleichung $y = x^2$ ein Prädikat, das von genau jenen Paaren (x, y) erfüllt wird, bei denen y das Quadrat von x ist. Die Terme t und s müssen nicht unbedingt Zahlen beschreiben. Auch Gleichungen zwischen Mengen sind häufig nützlich. Z.B. drückt die Gleichung

$$\mathbb{P} \cap \{n \in \mathbb{Z} \mid n \text{ ist gerade}\} = \{2\}$$

aus, dass 2 die einzige gerade Primzahl ist.

Warnung 7.1. Obwohl eine Gleichung mit freien Variablen an sich ein Prädikat spezifiziert, ist damit, je nach Kontext, manchmal auch die allquantifizierte Aussage gemeint. So ist z.B. in der Definition $H_x := \{y \in G \mid x + y = y + x\}$ mit "$x + y = y + x$" das Prädikat mit den zwei freien Variablen x und y gemeint. In einer Formulierung wie etwa der folgenden "$G = (\mathbb{Z}_m, +)$ ist eine Gruppe. Wir wollen nun $x + y = y + x$ zeigen." ist mit "$x + y = y + x$" die Aussage $\forall x, y \in G : x + y = y + x$ gemeint.

Aufeinanderfolgende Gleichungen. In Beweisen werden häufig Gleichungen benutzt. Die Konventionen für aufeinanderfolgende Gleichungen sind die selben wie für aufeinanderfolgende Aussagen, vor allem: die Richtung der logischen Implikation ist vorwärts. Das heißt also: wenn in einem Beweis mehrere Gleichungen in Folge angegeben werden und sonst nichts dazu gesagt wird, so wird damit ausgedrückt, dass jede Gleichung aus der vorherigen Gleichung folgt. So hat z.B. die folgende Liste von Gleichungen

$$\begin{aligned} 4a + 2 &= 2a - 6 \\ 2a &= -8 \\ a &= -4 \end{aligned}$$

die logische Bedeutung:

$$\begin{aligned} & 4a + 2 = 2a - 6 \\ \Rightarrow \quad & 2a = -8 \\ \Rightarrow \quad & a = -4, \end{aligned}$$

das heißt: "aus $4a + 2 = 2a - 6$ folgt $2a = -8$ und aus $2a = -8$ folgt $a = -4$". Durch Weglassen des Zwischenschritts erhalten wir $4a + 2 = 2a - 6 \Rightarrow a = -4$. Gelegentlich will man angeben, dass auch die umgekehrte Richtung der Implikation gilt. Das kann dann wie folgt getan werden:

$$\begin{aligned} & 4a + 2 = 2a - 6 \\ \Leftrightarrow \quad & 2a = -8 \\ \Leftrightarrow \quad & a = -4 \end{aligned}$$

Damit haben wir also sogar $4a + 2 = 2a - 6 \Leftrightarrow a = -4$ gezeigt. Aber Achtung: nicht alle Transformationen lassen sich umkehren. Wird etwa die obige Rechnung mit $a^2 = 16$ fortgesetzt, so gilt zwar

$$\begin{aligned} & 4a + 2 = 2a - 6 && (1) \\ \Leftrightarrow \quad & 2a = -8 && (2) \\ \Leftrightarrow \quad & a = -4 && (3) \\ \Rightarrow \quad & a^2 = 16 && (4) \end{aligned}$$

aber $a^2 = 16 \Rightarrow a = -4$ ist nicht wahr (Gegenbeispiel: $a = 4$). Beim Arbeiten mit Gleichungen ist es also besonders wichtig, sich immer im Klaren darüber zu sein, was woraus folgt[1].

Warnung 7.2. Ein häufiger Fehler beim Beweis einer Gleichung $t = s$ besteht darin, eine Liste von Gleichungen der Form

$$\begin{aligned} t &= s \\ &\vdots \\ u &= u \end{aligned}$$

anzugeben. Diese Liste beweist, wenn sie nicht weiter kommentiert wird, $u = u$ aus der Voraussetzung $t = s$. Das ist nutzlos, da damit die wahre Aussage $u = u$ aus der behaupteten Gleichung gezeigt wurde. Gefragt ist die Umkehrung: ein Beweis der behaupteten Gleichung $t = s$ aus wahren Aussagen.

Umformungen. Eine Umformung einer Gleichung, die zu einer äquivalenten Gleichung führt, heißt **Äquivalenzumformung**. Z.B. gilt

$$x = y \Leftrightarrow x + z = y + z.$$

Die Implikation von links nach rechts erhalten wir durch addieren von z, die von rechts nach links durch subtrahieren von z. Diese Äquivalenzumformung haben wir z.B. oben verwendet, um von Gleichung (1) zu Gleichung (2) zu gelangen (indem wir $x = 4a + 2$, $y = 2a - 6$ und $z = -2a - 2$ gesetzt haben).

Weiters gilt:

$$z \neq 0 \Rightarrow (x = y \Leftrightarrow x \cdot z = y \cdot z).$$

Von links nach rechts multiplizieren wir mit z, von rechts nach links dividieren wir durch z, wofür wir auch annehmen müssen dass $z \neq 0$ ist. Diese Äquivalenzumformung haben wir oben verwendet,

[1] An diesem Beispiel sieht man auch noch einmal gut, was der Unterschied zwischen $=$ und $\Leftrightarrow$ ist und wie diese beiden Verknüpfungen gemeinsam verwendet werden können.

um von Gleichung (2) zu Gleichung (3) zu gelangen (indem wir $x = 2a$, $y = -8$ und $z = 2$ gesetzt haben).

Eine häufig gebrauchte, und sehr allgemeine, Transformation von Gleichungen besteht in der Anwendung einer Funktion. Ist nämlich f eine Funktion dann gilt:

$$x = y \Rightarrow f(x) = f(y).$$

Aber Achtung: Im Allgemeinen ist die Umkehrung nicht wahr Sei z.B. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ dann gilt zwar $x = y \Rightarrow f(x) = f(y)$ aber $f(x) = f(y) \not\Rightarrow x = y$, wie wir auch oben am Beispiel bei den Gleichungen (3) und (4) gesehen haben.

Ungleichungen. Eine **Ungleichung** ist ein Ausdruck der Form $t \leq s$ oder $t < s$, wobei t und s Terme sind, die mathematische Objekte, meistens reelle Zahlen, beschreiben. Ebenso wie Gleichungen sind Ungleichungen, je nachdem ob sie Variable enthalten oder nicht, Prädikate oder Aussagen. Dabei ist natürlich $s \geq t$ äquivalent zu $t \leq s$ und $s > t$ äquivalent zu $t < s$.

Im Kontext von Ungleichungen können wir, wie bei Gleichungen, auch addieren und subtrahieren. Auch beim multiplizieren und dividieren kann man ähnlich vorgehen: nach wie vor darf aber natürlich nicht durch 0 dividiert werden. Zusätzlich ist noch zu beachten dass bei der Multiplikation mit einer negativen Zahl die Richtung der Ungleichung umgekehrt wird. Zusammenfassend haben wir also:

$$\begin{aligned} x \leq y &\Leftrightarrow x + z \leq y + z \\ z > 0 &\Rightarrow (x \leq y \Leftrightarrow x \cdot z \leq y \cdot z) \\ z < 0 &\Rightarrow (x \leq y \Leftrightarrow x \cdot z \geq y \cdot z) \end{aligned}$$

Die Anwendung von Funktionen muss im Kontext von Ungleichungen wesentlich restriktiver gehandhabt werden. Eine Funktion f mit der Eigenschaft

$$x \leq y \Rightarrow f(x) \leq f(y)$$

wird als monoton wachsend bezeichnet. Erfüllt f sogar die Eigenschaft

$$x < y \Rightarrow f(x) < f(y)$$

wird sie als streng monoton wachsend bezeichnet. In diesen Fällen können wir f benutzen um eine Ungleichung umzuformen. Viele Funktionen sind allerdings nicht monoton wachsend.

Beweise von Gleichungen. Gleichungen können auf verschiedene Arten bewiesen werden. Wir wollen nun vier wichtige Vorgehensweisen zum Beweis einer Gleichung betrachten.

1. Umformung bekannter Gleichung: Wir können eine Gleichung $t_n = s_n$ zeigen indem wir eine bekannte Gleichung $t_1 = s_1$ voraussetzen und diese schrittweise zu $t_2 = s_2, t_3 = s_3, \ldots$ umformen bis wir $t_n = s_n$ erreichen. Diese Vorgehensweise haben wir oben angewandt um $a^2 = 16$ aus $4a + 2 = 2a - 6$ zu beweisen.

2. Gleichungskette: Wir können eine Gleichung $t_1 = t_n$ zeigen, indem wir Terme $t_2, \ldots, t_{n-1}$ angeben mit $t_1 = t_2, t_2 = t_3, \ldots, t_{n-1} = t_n$. Ein solcher Beweis wird als Gleichungskette

$$t_1 = t_2 = \cdots = t_{n-1} = t_n$$

geschrieben. Betrachten wir ein Beispiel in den komplexen Zahlen: Wir wissen dass (1) $|z|^2 = z \cdot \overline{z}$ und (2) $\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$. Daraus erhalten wir

$$|z_1 \cdot z_2|^2 =^{(1)} z_1 \cdot z_2 \cdot \overline{z_1 \cdot z_2} =^{(2)} z_1 \cdot z_2 \cdot \overline{z_1} \cdot \overline{z_2} = z_1 \cdot \overline{z_1} \cdot z_2 \cdot \overline{z_2} =^{(1)} |z_1|^2 \cdot |z_2|^2 = (|z_1| \cdot |z_2|)^2,$$

d.h. also $|z_1 \cdot z_2|^2 = (|z_1| \cdot |z_2|)^2$. Da nun der Betrag einer komplexen Zahl niemals negativ ist, können wir die Injektivität der Funktion $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$, d.h. die Eigenschaft $f(x) = f(y) \Rightarrow x = y$, ausnützen um daraus $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ zu erhalten.

Diese Vorgehensweise zum Beweis einer Gleichung wird meistens zur Darstellung von Beweisen bevorzugt, da sie am elegantesten und am leichtesten zu lesen ist. Allerdings sind Beweise in dieser Form nicht immer leicht zu finden, so dass eine häufige Vorgehensweise darin besteht, einen in anderer Form gefundenen Beweis in diese Form einer Gleichungskette zu bringen.

3. Ausrechnen beider Seiten: Wir können eine Gleichung $t = s$ zeigen indem wir zunächst t ausrechnen, dann s ausrechnen und schließlich beobachten, dass wir in beiden Fällen das selbe Ergebnis erhalten haben. So kann etwa die Gleichung $(n+1)(n+2) = (n+2)^2 - (n+2)$ gezeigt werden durch (die beiden Gleichungsketten)

$$(n+1)(n+2) = n^2 + 2n + n + 2 = n^2 + 3n + 2$$
$$(n+2)^2 - (n+2) = n^2 + 4n + 4 - n - 2 = n^2 + 3n + 2$$

Diese Vorgehensweise bietet sich an, wenn "ausrechnen" eine vernünftige Bedeutung hat, z.B. bei Polynomen. Im Prinzip kann man solche Beweise durch ausrechnen beider Seiten auch in die Form einer einzigen Gleichungskette bringen, indem man die erste Gleichungskette von links nach rechts aufschreibt und dann die zweite, von rechts nach links, daran anhängt.

Für die oben durch eine Gleichungskette bewiesene Aussage $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ könnten man auch einen Beweis durch Ausrechnen beider Seiten angeben indem man $z_1 = a_1 + ib_1$ und $z_2 = a_2 + ib_2$ setzt. Dieser wäre aber deutlich länger und weniger elegant.

4. Antisymmetrie: Im Prinzip kann für $x, y \in \mathbb{R}$ auch $x = y$ gezeigt werden, indem $x \leq y \wedge y \leq x$ gezeigt wird. Dann folgt nämlich $x = y$ mittel Antisymmetrie. Das ist allerdings für Zahlen nur in Ausnahmesituationen zweckmäßig. Bei Mengen wird diese Strategie allerdings oft angewandt: eine Mengengleichheit $A = B$ wird oft bewiesen, indem $A \subseteq B$ und $B \subseteq A$ bewiesen werden. Dafür haben wir in Kapitel 6 schon einige Beispiele gesehen.

Abstrakte Gleichheitsinferenz. Das Rechnen mit Gleichungen kann rein formal durchgeführt werden. Es ist zwar im Normalfall nützlich, aber nicht immer zwingend erforderlich, eine genaue Vorstellung von den Objekten, die man behandelt, und den Transformationen, denen man sie durch die Anwendung von Gleichungen unterwirft, zu haben. So haben wir z.B. etwas weiter oben die Gleichung (1): $|z|^2 = z \cdot \overline{z}$ angewandt, um die Gleichung (1′): $|z_1 \cdot z_2|^2 = (z_1 \cdot z_2) \cdot (\overline{z_1 \cdot z_2})$ zu zeigen. Dafür war es nicht notwendig zu wissen, was der Betrag einer komplexen Zahl ist, oder wie man komplexe Zahlen multipliziert. Es war nicht einmal notwendig zu wissen, was eine komplexe Zahl überhaupt ist. Rein formal geschieht hier nur eine Substitution: Da ja für alle z die Gleichung (1) gilt, so gilt sie insbesondere auch für $z = z_1 \cdot z_2$. Und somit folgt (1′) aus (1).

Als ein rein formales Beispiel wollen wir nun Funktionen f, g sowie ein Objekt a betrachten für die die folgenden Gleichungen gelten:

$$g(f(x), x) = a \tag{1}$$
$$g(a, x) = x \tag{2}$$
$$g(x, g(y, z)) = g(g(x, y), z) \tag{3}$$
$$g(x, f(x)) = a \tag{4}$$

Damit können wir wie folgt die Gleichung $g(v, a) = v$ zeigen:

$$g(v, a) =^{(1)} g(v, g(f(v), v)) =^{(3)} g(g(v, f(v)), v) =^{(4)} g(a, v) =^{(2)} v.$$

Um diesen Beweis durchzuführen, ist es nicht notwendig, zu erkennen, dass man damit zeigt, dass ein Rechtseinheitselement in einem Monoid mit Inversen auch ein Linkseinheitselement ist.

Das Summenzeichen. Gleichungen in den Zahlen handeln oft von Summen und Produkten. Das Summenzeichen $\sum$ dient dazu eine Summe kompakt darzustellen. Die allgemeine Form lautet

$$\sum_{i=1}^{n} a_i$$

was eine Abkürzung ist für

$$a_1 + a_2 + ... + a_n.$$

So ist z.B.

$$\sum_{i=2}^{5} \frac{1}{i} = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5}$$

Die Variable i bezeichnet man als **Laufvariable**. Die Laufvariable wird durch das Summenzeichen $\sum$ gebunden, im Ergebnis kommt sie nicht mehr vor. 1 ist die untere Grenze und n ist die obere Grenze. Diese Notation erinnert also an eine `for`-Schleife aus einer imperativen Programmiersprache.

Solche Summen können auf vielfältige Weise umgeschrieben werden. Zunächst einmal kann die Laufvariable, da sie ja eine gebundene Variable ist, beliebig umbenannt werden, d.h.

$$\sum_{i=1}^{n} a_i = \sum_{j=1}^{n} a_j$$

Weiters können Summen beliebig aufgespalten werden. Das heißt für $k \leq n$ gilt

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n} a_i.$$

Auch oft nützlich ist die Anwendung des Distributivgesetzes, das heißt

$$c \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} c a_i.$$

Achtung: Dabei ist es natürlich notwendig dass c die Laufvariable i nicht enthält.

Durch eine **Indexverschiebung** kann gelegentlich die Darstellung der Summanden a_i vereinfacht werden. Für $k \in \mathbb{Z}$ gilt nämlich:

$$\sum_{i=m}^{n} a_i = \sum_{j=m+k}^{n+k} a_{j-k}.$$

Hier wird also $j = i + k$ gesetzt. So ist z.B.

$$\sum_{i=1}^{4} (i+2) = 3 + 4 + 5 + 6 = \sum_{j=3}^{6} j.$$

Statt Summanden der Form $i + 2$ haben wir es also jetzt nur noch mit Summanden der Form j zu tun.

Weitere Operationszeichen. Viele weitere Operationen erlauben eine ähnliche Schreibweise wie Summen. So wird z.B. ein Produkt als

$$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \dots \cdot a_n$$

geschrieben. Für Produkte gelten analoge Rechenregeln. Auch Operationen auf Mengen wie Vereinigung und Durchschnitt werden oft mit großen Operationszeichen geschrieben:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \dots \cup A_n$$
$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \dots \cap A_n$$

Auch hier gelten analoge Rechenregeln.

Das Wichtigste in Kürze.

- Gleichungen können auf verschiedene Arten bewiesen werden, u.a. durch 1. Umformung einer bekannten Gleichung, 2. eine Gleichungskette, 3. Ausrechnen beider Seiten, 4. Antisymmetrie.
- Gleichungsketten sind in den meisten Fällen für die Darstellung eines Beweises aufgrund ihrer leichten Lesbarkeit zu bevorzugen.
- Bei der Umformung einer bekannten Gleichung läuft die logische Implikation, wenn nichts anderes erwähnt wird, nur vorwärts, d.h. von oben nach unten.

Kapitel 8

Induktion

In diesem Kapitel beschäftigen wir uns mit einer der wichtigsten Beweistechniken für Allaussagen über natürliche Zahlen (und verwandte Strukturen): mit der Induktion. Sei $P(n)$ ein Prädikat auf den natürlichen Zahlen. Dann besagt das **Induktionsprinzip**:

$$P(0) \wedge \forall n\ (P(n) \Rightarrow P(n+1)) \Rightarrow \forall k\ P(k), \tag{I}$$

in Worten: "Wenn P für 0 gilt und für jede beliebige natürliche Zahl n die Gültigkeit von P für n die Gültigkeit von P für $n+1$ impliziert, dann gilt P für alle natürlichen Zahlen." Dieses Prinzip wird als Axiom über die natürlichen Zahlen postuliert und benötigt als solches keinen Beweis im strengen Sinn. Allerdings ist es natürlich angemessen sich die "offensichtliche" Wahrheit eines Axioms zumindest plausibel zu machen.

Nehmen wir dazu an, dass $P(0)$ sowie $\forall n\ (P(n) \Rightarrow P(n+1))$ gilt. Wie können wir dann z.B. zeigen, dass $P(1)$ gilt? Ganz einfach: aus $\forall n\ (P(n) \Rightarrow P(n+1))$ erhalten wir, indem wir $n = 0$ setzen, $P(0) \Rightarrow P(1)$. $P(0)$ ist bereits bekannt, also folgt mittels Modus Ponens $P(1)$. Wie können wir zeigen, dass $P(2)$ gilt? Wie oben erhalten wir $P(1)$. Zusätzlich erhalten wir, indem wir $n = 1$ setzen, auch $P(1) \Rightarrow P(2)$. Insgesamt also: $P(2)$ Diese Vorgehensweise lässt sich bis zu jeder beliebigen natürlichen Zahl k fortsetzen. Also gilt $P(k)$ für alle $k \in \mathbb{N}$.

Die Benutzung des Induktionsprinzips kann man sich so vorstellen wie die Benutzung einer Leiter. Kann man die erste Sprosse einer Leiter erklimmen (d.h. also $P(0)$) und weiß man wie man von einer Sprosse auf die nächste kommt (d.h. also $\forall n\ (P(n) \Rightarrow P(n+1))$, dann kann man auf eine beliebig hohe Leiter hinaufklettern.

Induktionsbeweise. Um das Induktionsprinzip in einem Beweis zu verwenden, geht man üblicherweise folgendermaßen vor. Zuerst wird $P(0)$ bewiesen. Das bezeichnet man als **Induktionsanfang (IA)**. Danach wird $\forall n\ (P(n) \Rightarrow P(n+1))$ bewiesen. Das bezeichnet man als **Induktionsschritt (IS)**. Der Induktionsschritt geschieht durch Eröffnung eines neues Unterbeweises in dem, für ein beliebiges n, aus der Voraussetzung $P(n)$ die Behauptung $P(n+1)$ bewiesen wird. Im Kontext dieses Unterbeweises bezeichnet man $P(n)$ auch als **Induktionsvoraussetzung (IV)** und $P(n+1)$ als **Induktionsbehauptung (IB)**. Schließlich kann aus $P(0)$ und $\forall n\ (P(n) \Rightarrow P(n+1))$ mittels Induktion(sprinzip) die Aussage $\forall k\ P(k)$ geschlossen werden[1]. In unserer Notation für formale Beweise sieht ein Induktionsbeweis also wie folgt aus:

[1] Wie die gebundene Variable in dieser Aussage heißt, ist, wie immer bei gebundenen Variablen, egal. Sie können also mittels Induktion genauso gut $\forall n\ P(n)$ schließen.

$$
\begin{array}{ll}
\vdots & \\
X\colon P(0) & \text{zz: } A \\
\quad \left|\begin{array}{l} X+1\colon P(n) \\ \qquad \vdots \end{array}\right. & \begin{array}{l} \text{zz: } P(n+1) \\ \qquad \vdots \end{array} \\
Y\colon \forall n\ (P(n) \Rightarrow P(n+1)) & \text{zz: } A \\
Y+1\colon \forall k\ P(k) \text{ (aus } X \text{ und } Y \text{ mittels Induktion)} & \text{zz: } A
\end{array}
$$

Wir wollen nun ein einfaches Beispiel für einen Induktionsbeweis betrachten wobei wir seine Struktur und seine einzelne Elemente deutlich kennzeichnen.

Satz. *Für alle $n \in \mathbb{N}$ gilt:* $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Beweis. Mittels Induktion:

IA: $\displaystyle\sum_{i=0}^{0} i = 0 = \frac{0 \cdot 1}{2}.$

IS: IV: $\displaystyle\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

IB: $\displaystyle\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$

Beweis der IB aus der IV:

$$
\begin{aligned}
\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) &=^{(\mathrm{IV})} \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}
$$

□

Das Prinzip der kleinsten Zahl. Wir wollen nun ein mit dem Induktionsprinzip verwandtes Prinzip betrachten: Das Prinzip der kleinsten Zahl. Sei $Q(n)$ ein Prädikat auf den natürlichen Zahlen. Das Prinzip der kleinsten Zahl ist die folgende Aussage:

$$\exists k\ Q(k) \Rightarrow \exists j\ (Q(j) \wedge \forall i < j\ \neg Q(i)), \tag{PKZ}$$

in Worten: "Wenn es eine Zahl gibt, für die Q gilt, dann gibt es eine kleinste solche Zahl." Dieses Prinzip ist offensichtlich wahr. Wir wollen nun zeigen, dass man durch logische Äquivalenzumformungen des Prinzips der kleinsten Zahl eine starke Form der Induktion erhält. Das Prinzip der kleinsten Zahl lautet:

$$\underbrace{\exists k\ Q(k)}_{A} \Rightarrow \underbrace{\exists j\ (Q(j) \wedge \forall i < j\ \neg Q(i))}_{B}$$

Wir betrachten die Kontraposition $\neg B \Rightarrow \neg A$ von $A \Rightarrow B$ und mit den üblichen Rechenregeln für die Negation erhalten wir

$$\forall j\ (\neg Q(j) \vee \neg \forall i < j\ \neg Q(j)) \Rightarrow \forall k\ \neg Q(k),$$

was weiter umgeschrieben werden kann zu

$$\forall j\ (\forall i < j\ \neg Q(i) \Rightarrow \neg Q(j)) \Rightarrow \forall k\ \neg Q(k).$$

Definieren wir nun $P(x) :\Leftrightarrow \neg Q(x)$, so erhalten wir

$$\forall j\ (\forall i < j\ P(i) \Rightarrow P(j)) \Rightarrow \forall k\ P(k). \tag{SI}$$

Die Aussage (SI) ist eng mit dem bereits bekannten Induktionsprinzip (I) verwandt, da sie auch eine hinreichende Voraussetzung für $\forall k\ P(k)$ bietet, nämlich: $\forall j\ (\forall i < j\ P(i) \Rightarrow P(j))$. Man bezeichnet die Aussage (SI) auch als **starke Induktion**. Diese Bezeichnung erklärt sich wie folgt: Setzen wir für den Induktionsschritt $j = n + 1$, so erlaubt die starke Induktion im Beweis von $P(n + 1)$ die Verwendung aller Aussagen $P(0), P(1), \ldots, P(n)$ als Voraussetzungen, die gewöhnliche Induktion aber nur die der Aussage $P(n)$. Um die Rolle des Induktionsanfangs zu verstehen betrachten wir den Fall $j = 0$. Dann ist zu zeigen dass $\forall i < 0\ P(i) \Rightarrow P(0)$. Nun gibt es aber keine $i \in \mathbb{N}$ mit $i < 0$. Die linke Seite dieser Implikation ist also trivialerweise wahr, d.h. es ist bleibt $P(0)$ ohne zusätzliche Voraussetzung zu zeigen, was genau dem üblichen Induktionsanfang entspricht.

Varianten des Induktionsprinzips. Es ist häufig auch tatsächlich notwendig, wie bei der starken Induktion, mehr als nur den unmittelbaren Vorgänger zu verwenden. Aus der starken Induktion lassen sich entsprechende Induktionsprinzipien leicht ableiten, z.B.:

$$P(0) \wedge P(1) \wedge \forall n\ (P(n) \wedge P(n + 1) \Rightarrow P(n + 2)) \Rightarrow \forall k\ P(k).$$

Hier besteht die Induktionsbasis auf $P(0)$ und $P(1)$, der Induktionsschritt aus $\forall n\ (P(n) \wedge P(n+1) \Rightarrow P(n + 2))$. Dieses Induktionsprinzip ist z.B. nützlich beim Beweis von Eigenschaften von Folgen wie der Fibonacci-Folge die durch eine Abhängigkeit eines Folgenglieds von den zwei vorherigen Folgengliedern definiert ist.

Manche Eigenschaften natürlicher Zahlen sind zwar für 0 nicht wahr, aber ab einem gewissen m dann für alle $n \geq m$. Z.B. gilt $2^n \geq n^2$ für alle $n \geq 4$ aber nicht für $n = 3$. Auch solche Eigenschaften kann man mit Induktion zeigen. Dazu ist es lediglich notwendig den Induktionsanfang zu verschieben. Wir erhalten dann das einfache Induktionsprinzip

$$P(m) \wedge \forall n \geq m\ (P(n) \Rightarrow P(n + 1)) \Rightarrow \forall k \geq m\ P(k).$$

aus dem Prinzip der kleinsten Zahl angewandt auf das Prädikat $n \geq m \Rightarrow P(n)$.

Diese beiden Varianten lassen sich natürlich auch kombinieren zu einem Induktionsprinzip ab einem gewissen m das die Verwendung mehrerer Vorgänger erlaubt.

Wohlfundierte Induktion. Im obigen Beweis der logischen Äquivalenz zwischen (PKZ) und (SI) haben wir keinerlei Eigenschaften der natürlichen Zahlen verwendet. Der selbe Beweis kann für eine beliebige Halbordnung[2] durchgeführt werden. Daraus erhalten wir wie folgt ein sehr allgemeines Induktionsprinzip.

Sei $(X, \leq)$ eine Halbordnung. Dann heißt $(X, \leq)$ **wohlfundiert**, falls jede nicht-leere Teilmenge $A \subseteq X$ ein (bezüglich $\leq$) minimales Element enthält, d.h.

$$A \neq \emptyset \Rightarrow \exists x \in A \forall y < x : y \notin A,$$

wobei $y < x$ eine Abkürzung für $y \leq x \wedge y \neq x$ ist. Das Prinzip der kleinsten Zahl in den natürlichen Zahlen erkennen wir also als die Aussage dass $(\mathbb{N}, \leq)$ wohlfundiert ist. Ist $(X, \leq)$ eine wohlfundierte Halbordnung, so gilt also dem obigen Beweis folgend auch

$$\forall j\ (\forall i < j\ P(i) \Rightarrow P(j)) \Rightarrow \forall k\ P(k)$$

[2]Eine Relation (X, R) heißt **Halbordnung**, falls sie die folgenden Eigenschaften hat: 1. **Reflexivität**, d.h. $\forall x\, x\, R\, x$, 2. **Antisymmetrie**, d.h. $\forall x \forall y\, (x\, R\, y \wedge y\, R\, x \Rightarrow x = y)$ und 3. **Transitivität**, d.h. $\forall x \forall y \forall z\, (x\, R\, y \wedge y\, R\, z \Rightarrow x\, R\, z)$.

für jedes Prädikat $P(x)$ auf X. Wir erhalten also ein Induktionsprinzip auf $(X, \leq)$ das wir wie gewohnt zum Führen von Induktionsbeweisen verwenden können.

Wir wissen bereits, dass $(\mathbb{N}, \leq)$ eine wohlfundierte Halbordnung ist. Andere Beispiele sind $(\mathcal{P}(A), \subseteq)$ für eine endliche Menge A oder $(\mathbb{N}^+, |)$, die Teilbarkeit in den natürlichen Zahlen[3]. Induktion entlang einer beliebigen wohlfundierten Halbordnung ist ein sehr allgemeines Prinzip das nicht nur für die Mathematik zentral ist, sondern auch in diversen Anwendungen direkte Verwendung findet, z.B. bei Beweisen der Termination von Programmen.

Ein Beispiel für die direkte Verwendung der Wohlfundiertheit einer Halbordnung ist der folgende Beweis.

Satz. *Jede natürliche Zahl $n \geq 2$ hat einen Primteiler.*

Beweis. $(\mathbb{N}^+, |)$ ist eine wohlfundierte Halbordnung. Sei $T_n = \{k \in \mathbb{N}^+ \mid k \geq 2, k \mid n\}$. Dann ist $\emptyset \neq T_n \subseteq \mathbb{N}^+$, also enthält T_n ein (bezüglich $|$) kleinstes Element p, d.h.:

$$p \in T_n \wedge \forall q \in \mathbb{N}^+ : q \mid p \Rightarrow q \notin T_n$$

Dann ist $p \mid n$ und $p \neq 1$. Außerdem ist sogar $p \in \mathbb{P}$. Wäre nämlich $p \notin \mathbb{P}$ dann hätte p noch einen Teiler $q \in \{2, \ldots, p-1\}$ der wegen $q \mid p$ und $p \mid n$ auch $q \in T_n$ erfüllen müsste. Widerspruch. □

Induktive Definitionen. Wir haben bereits einige rekursive Definitionen von Funktionen gesehen. Auch für die Definition von Mengen kann man analog dazu vorgehen: dabei spricht man meist von einer induktiven Definition einer Menge. So ist z.B. die Menge der aussagenlogischen Formeln induktiv wie folgt definiert:

1. eine atomare Aussage p ist eine aussagenlogische Formel.
2. Falls A eine aussagenlogische Formel ist, dann ist auch $\neg A$ eine aussagenlogische Formel.
3. Falls A und B aussagenlogische Formeln sind, dann sind auch $A \wedge B$, $A \vee B$, $A \Rightarrow B$ und $A \Leftrightarrow B$ aussagenlogische Formeln.

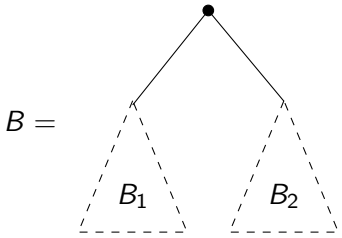
Bei Angabe einer solchen Definition ist natürlich gemeint, dass **nur** solche Objekte aussagenlogische Formeln sind. Das heißt: Die Menge der aussagenlogischen Formeln ist die kleinste Menge, welche die Bedingungen 1.-3. erfüllt. Man beachte, dass die Bedingungen 2. und 3. Voraussetzungen über die Menge der aussagenlogischen Formeln enthalten, die Bedingung 1. aber nicht. Bedingungen wie 1. entsprechen somit dem Induktionsanfang, Bedingungen wie 2. und 3. dem Induktionsschritt.

Viele in der Mathematik und Informatik wichtigen Mengen sind induktiv definiert, z.B. die Menge der arithmetischen Terme, die Menge der Programme in einer typischen Programmiersprache, die von gewissen Elementen erzeugte Untergruppe einer Gruppe, die Menge der Listen, ...

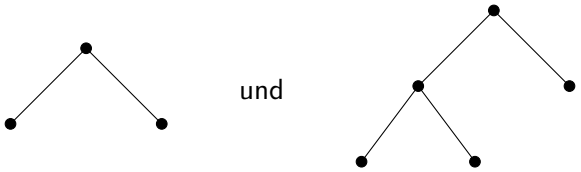
Strukturelle Induktion Um eine Aussage für alle Elemente einer induktiv definierten Menge zu zeigen, kann man strukturelle Induktion verwenden. Wir wollen dazu nun ein Beispiel betrachten. Die Menge der Binärbäume wird induktiv wie folgt definiert: 1. Ein einziger Knoten

[3] wobei $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$

ist ein Binärbaum. 2. Falls B_1 und B_2 Binärbäume sind, dann ist auch



ein Binärbaum. So sind z.B.



Binärbäume. Wir können nun eine Aussage über alle Binärbäume zeigen, indem wir eine strukturelle Induktion auf der Menge der Binärbäume durchführen. Dabei entspricht die Bedingung 1. dem Induktionsanfang und die Bedingung 2. dem Induktionsschritt.

Wir definieren weiters rekursiv die Größe eine Binärbaums durch

$$|\bullet| = 1 \qquad\qquad |B| = |B_1| + |B_2| + 1$$

und die Höhe eines Binärbaums durch

$$h(\bullet) = 0 \qquad\qquad h(B) = \max\{h(B_1), h(B_2)\} + 1.$$

Satz. *Für jeden Binärbaum B gilt:* $|B| \leq 2^{h(B)+1} - 1$.

Beweis. Wir gehen mit struktureller Induktion über die Definition der Menge der Binärbäume vor.

IA: $|\bullet| = 1$ und $2^{h(\bullet)+1} - 1 = 1$.

IS: IV: $|B_1| \leq 2^{h(B_1)+1} - 1$ und $|B_2| \leq 2^{h(B_2)+1} - 1$

IB: $|B| \leq 2^{h(B)+1} - 1$

Beweis der IB aus der IV:

$$|B| = |B_1| + |B_2| + 1 \leq^{\text{IV}} 2^{h(B_1)+1} + 2^{h(B_2)+1} - 1$$

Nun ist aber $h(B) = \max\{h(B_1) + 1, h(B_2) + 1\}$ und damit erhalten wir

$$|B| \leq 2^{h(B)} + 2^{h(B)} - 1 = 2^{h(B)+1} - 1.$$

□

Das Wichtigste in Kürze.

• Die Induktion ist eine der wichtigsten Beweistechniken für Allaussagen über natürliche Zahlen und verwandte Strukturen.

• Ein typischer Induktionsbeweis besteht aus einem Induktionsanfang (IA) und einem Induktionsschritt (IS). Der Induktionsschritt besteht darin, die Induktionsbehauptung (IB) aus der Induktionsvoraussetzung (IV) zu beweisen.

• Es gibt verschiedene Varianten des Induktionsprinzips, und damit der Form eines Induktionsbeweises. Die allgemeinste davon ist die wohlfundierte Induktion.

• Um Aussagen über alle Elememente einer induktiv definierten Menge, wie z.B. der Menge der Binärbäume, zu zeigen, verwendet man strukturelle Induktion. Diese folgt der Struktur der induktiven Definition.

Kapitel 9

Abstraktion

Bisher haben wir vor allem mit ganzen Zahlen gearbeitet. Eine ganze Zahl, genauso wie eine natürliche Zahl oder eine rationale Zahl, ist ein Objekt das durch endlich viel Information, also z.B. durch einen endlich langen Bitstring, dargestellt werden kann. So kann jedes $n \in \mathbb{N}$ oder $m \in \mathbb{Z}$ durch (sein Vorzeichen und) seine Dezimal- oder auch Binärdarstellung angegeben werden, jedes $q \in \mathbb{Q}$ durch einen Bruch. Wenn wir gedanklich mit solchen Objekten hantieren, können wir uns, zumindest im Prinzip, vorstellen, dass diese Objekte vollständig spezifiziert vor unserem geistigen Auge liegen. In diesem Sinn handelt es sich dabei um konkrete Objekte. Das entspricht bis zu einem gewissen Grad der Situation, in der man sich beim Programmieren befindet. Auch dort hat man mit unbekannten Objekten, z.B. der Eingabe eines Programms, zu tun die, in der Regel, endlich viel Information enthalten und damit durch einen Bitstring endlicher Länge spezifiziert werden können.

In der Mathematik ist man aber nicht darauf beschränkt. Weite Teile der Mathematik beschäftigen sich mit Objekten, die nicht durch endlich viel Information vollständig spezifiziert werden können. In diesem Sinn handelt es sich um abstrakte Objekte. Die durch diesen Übergang ins Abstrakte entstehenden Theorien und die sich dadurch eröffnenden Zusammenhänge sind auch für Anwendungen im Konkreten, etwa in der Informatik, unverzichtbar. In diesem Kapitel werden wir die elementare Zahlentheorie verlassen, um uns mit abstrakten Objekten zu beschäftigen. Wenn sich auch die Natur der Objekte mit denen wir arbeiten dadurch verändert, so bleibt doch eines gleich: die Art und Weise wie wir mathematisch arbeiten. Im Abstrakten bedeuten Begriffe wie Aussage oder Prädikat das selbe wie im Konkreten und die selben logischen Schlussfolgerungen und Beweistechniken finden Anwendung.

Quasiordnungen. Wir beginnen mit einem konkreten Beispiel: Wir betrachten eine Menge W von Webseiten und zeichnen einen Pfeil[1] von einer Webseite x zu einer Webseite y falls ein Hyperlink von x zu y führt, siehe Abbildung 9.1. Wir können uns nun für die Frage interessieren, von welcher Webseite zu welcher man alleine durch das Folgen von Hyperlinks gelangen kann. Klar dabei ist: wenn man von x nach y gelangen kann und auch von y nach z, dann kann man auch von x nach z gelangen. Außerdem will man wohl sagen, dass man von x nach x gelangen kann, indem man gar nichts tut.

Während dieses Beispiel konkret und anwendungsnah ist, führt eine Abstraktion und damit eine Reduktion auf die mathematisch wesentlichen Eigenschaften schnell zum folgenden Begriff einer Quasiordnung:

Definition. Sei A eine Menge und sei $R \subseteq A \times A$ eine Relation auf A. R heißt ...

[1] Eine solche Darstellung von Punkten und Pfeilen zwischen diesen Punkten bezeichnet man auch als gerichteten Graphen.

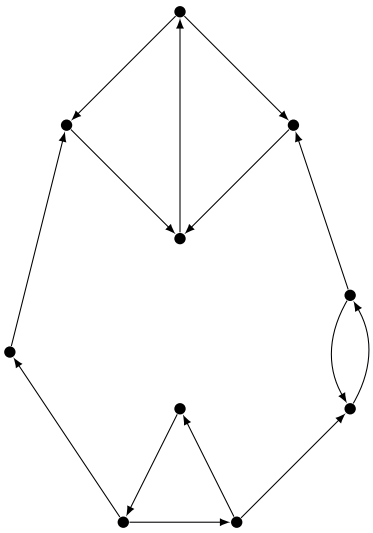


Abbildung 9.1: Webseiten und Hyperlinks

1. **reflexiv** falls $\forall x \in A : x \, R \, x$,

2. **transitiv** falls $\forall x \forall y \forall z : x \, R \, y \wedge y \, R \, z \Rightarrow x \, R \, z$,

3. **Quasiordnung** falls R reflexiv und transitiv ist.

Wir erhalten also eine Quasiordnung $(W, \rightsquigarrow)$ indem wir $x \rightsquigarrow y$ definieren als: es gibt einen Pfad von Hyperlinks von x nach y. Diese Relation ist auch reflexiv weil der leere Pfad auch ein Pfad ist. Diese Relation ist transitiv weil die Verkettung zweier Pfade selbst wieder ein Pfad ist.

Ein weiteres Beispiel für eine Quasiordnung ist die Relation $(\mathbb{C}, \preccurlyeq)$ auf den komplexen Zahlen, die durch $z_1 \preccurlyeq z_2 :\Leftrightarrow |z_1| \leq |z_2|$ definiert ist. Weiter unten werden wir im Detail zeigen, dass $(\mathbb{C}, \preccurlyeq)$ transitiv ist. Quasiordnungen sind also abstrakte Objekte in unserem Sinn, da sie sich im Allgemeinen nicht durch endlich viel Information darstellen lassen.

Abstrakte Objekte in Beweisen. Wir wollen uns nun mit der Verwendung von abstrakten Objekten in Beweisen beschäftigen. Zu diesem Zweck erinnern wir uns noch kurz an den folgenden Begriff aus der elementaren Zahlentheorie:

Definition. Zwei natürliche Zahlen $a, b \geq 1$ heißen **teilerfremd** falls $\forall d \in \mathbb{N} : d \mid a \wedge d \mid b \Rightarrow d = 1$.

Was ist der Unterschied zwischen dem Begriff der Teilerfremdheit und dem Begriff der Quasiordnung? a, b, d können jeweils durch endlich viel Information spezifiziert werden. Mit (A, R) sowie $x, y, z \in A$ ist das im Allgemeinen nicht möglich, wie man am Beispiel $(\mathbb{C}, \preccurlyeq)$ sieht. Dies ist allerdings ein rein inhaltlicher Unterschied. Auf die Ebene des logischen Umgangs mit diesen Begriffen hat er keine Auswirkung. Um das zu illustrieren, wollen wir formale Beweise zweier Aussagen angeben und gegenüberstellen.

Satz. 10 *und* 21 *sind teilerfremd.*

Beweis (formal).

1:		zz: 10 und 21 sind teilerfremd
2:		zz: $\forall d \in \mathbb{N} : d \mid 10 \wedge d \mid 21 \Rightarrow d = 1$ (Exp. Def.)
3:	Sei $d' \in \mathbb{N}$, es reicht	zz: $d' \mid 10 \wedge d' \mid 21 \Rightarrow d' = 1$ ($\forall$-Behauptung)
4:	$d' \mid 10,\ d' \mid 21$	zz: $d' = 1$ (Aussagenlogik)
5:	$d' \in \{1, 2, 5, 10\}, d' \in \{1, 3, 7, 21\}$	zz: " (Rechnung)
6:	$d' \in \{1\}$	zz: " (Rechnung)

Nun sind wir fertig, da die Behauptung bereits eine Voraussetzung ist. □

Satz. $(\mathbb{C}, \preccurlyeq)$ *ist transitiv.*

Beweis (formal).

1:		zz: $(\mathbb{C}, \preccurlyeq)$ ist transitiv
2:		zz: $\forall z_1, z_2, z_3 \in \mathbb{C} : z_1 \preccurlyeq z_2 \wedge z_2 \preccurlyeq z_3 \Rightarrow z_1 \preccurlyeq z_3$ (Exp. Def.)
3:	Seien $z_1', z_2', z_3' \in \mathbb{C}$, es reicht	zz: $z_1' \preccurlyeq z_2' \wedge z_2' \preccurlyeq z_3' \Rightarrow z_1' \preccurlyeq z_3'$ ($\forall$-Behauptung)
4:	$z_1' \preccurlyeq z_2',\ z_2' \preccurlyeq z_3'$	zz: $z_1' \preccurlyeq z_3'$ (Aussagenlogik)
5:	$\lvert z_1' \rvert \leq \lvert z_2' \rvert,\ \lvert z_2' \rvert \leq \lvert z_3' \rvert$	zz: $\lvert z_1' \rvert \leq \lvert z_3' \rvert$ (Expansion Definition)
6:	$\lvert z_1' \rvert \leq \lvert z_3' \rvert$	zz: " (da $(\mathbb{R}, \leq)$ transitiv)

Nun sind wir fertig, da die Behauptung bereits eine Voraussetzung ist. □

Die Zeilen 1 bis 4 dieser beiden Beweise bestehen aus den selben Schritten. Lediglich in den letzten beiden Zeilen 5 und 6 muss problemspezifisch argumentiert werden. Ein gewisses Ausmaß problemspezifischer Argumentation ist natürlich unvermeidlich, da es sich ja um zwei verschiedene Aussagen handelt. Allerdings ändert sich am Umgang mit diesen Aussagen durch ihren Abstraktionsgrad nichts: Die Expansion von Definitionen, die Beweisstrategie für $\forall$-Behauptungen, die Verwendung der Aussagenlogik, usw. geschieht auf genau die selbe Art und Weise.

Produkt von Relationen Wir gehen jetzt noch einen Schritt weiter und betrachten eine Operation auf Relationen: das Produkt zweier Relationen. Durch dieses Produkt wird also ein abstraktes Objekt aus zwei gegebenen abstrakten Objekten erzeugt.

Definition. Seien (A_1, R_1) und (A_2, R_2) Relationen. Dann ist das **Produkt** von (A_1, R_1) und (A_2, R_2) definiert als die Relation $(A_1 \times A_2, R)$ mit $(x_1, x_2)\ R\ (y_1, y_2) :\Leftrightarrow x_1\ R_1\ y_1 \wedge x_2\ R_2\ y_2$.

Beispiel. Das Produkt von $(\mathbb{R}, \leq)$ mit sich selbst ist die Relation $(\mathbb{R} \times \mathbb{R}, L)$ mit $(x, y)\ L\ (u, v) \Leftrightarrow x \leq u \wedge y \leq v$, siehe Abbildung 9.2.

Auch auf dieser Abstraktionsebene ändert sich an der logischen Behandlung der mathematischen Objekte nichts. Wir werden für einen einfachen Satz über das Produkt zweier beliebiger Relationen einen formalen, einen detaillierten und einen realistischen Beweis betrachten.

Satz. *Seien* (A_1, R_1) *und* (A_2, R_2) *reflexiv. Dann ist auch deren Produkt* $(A_1 \times A_2, R)$ *reflexiv.*

Man beachte, dass wir es in diesem Satz mit beliebigen Mengen A_1, A_2 sowie beliebigen Relationen R_1 und R_2 darauf zu tun haben, nicht mit einer fixen Menge $\mathbb{C}$ und einer fixen Relation $\preccurlyeq$ wie oben.

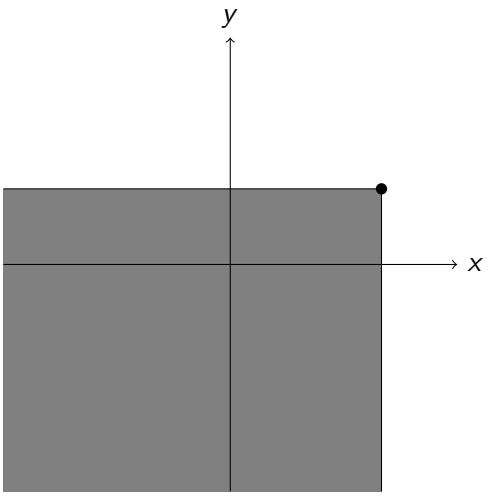


Abbildung 9.2: Die Menge $\{(x, y) \in \mathbb{R}^2 \mid (x, y) \leq (2, 1)\}$

Beweis (formal).

1:	zz: (A_1, R_1) r. $\wedge$ (A_2, R_2) r. $\Rightarrow$ $(A_1 \times A_2, R)$ r.
2: (A_1, R_1) reflexiv, (A_2, R_2) reflexiv	zz: $(A_1 \times A_2, R)$ reflexiv (Aussagenlogik)
3: $\forall x_1 \in A_1\, x_1\, R_1\, x_1$, $\forall x_2 \in A_2\, x_2\, R_2\, x_2$	zz: $\forall (x_1, x_2) \in A_1 \times A_2\ (x_1, x_2)\ R\ (x_1, x_2)$ (Exp. Def.)
4:	zz: $\forall x_1 \in A_1 \forall x_2 \in A_2$: $x_1\, R_1\, x_1 \wedge x_2\, R_2\, x_2$. (Exp. Def.)
5: Seien $x_1' \in A_1$, $x_2' \in A_2$, es reicht	zz: $x_1'\, R_1\, x_1' \wedge x_2'\, R_2\, x_2'$ ($\forall$-Behauptung)
6: $x_1'\, R_1\, x_1'$, $x_2'\, R_2\, x_2'$	zz: " ($\forall$-Voraussetzung)

Nun sind wir fertig, da die Behauptung bereits eine Voraussetzung ist. □

Beweis (detailliert). Seien (A_1, R_1) und (A_2, R_2) reflexiv, d.h. $\forall x_1 \in A_1 : x_1\, R_1\, x_1$ und $\forall x_2 \in A_2 : x_2\, R_2\, x_2$. Zu zeigen ist $\forall (x_1, x_2) \in A_1 \times A_2 : (x_1, x_2)\ R\ (x_1, x_2)$, d.h. $\forall x_1 \in A_1 \forall x_2 \in A_2$: $x_1\, R_1\, x_1 \wedge x_2\, R_2\, x_2$. Seien $x_1' \in A_1$ und $x_2' \in A_2$. Dann reicht es zu zeigen, dass $x_1'\, R_1\, x_1'$ und $x_2'\, R_2\, x_2'$. Aus den Voraussetzungen erhalten wir $x_1'\, R_1\, x_1'$ und $x_2'\, R_2\, x_2'$. Damit ist die Behauptung bewiesen. □

Beweis (realistisch). Seien $(x_1, x_2) \in A_1 \times A_2$. Da (A_1, R_1) reflexiv ist, ist $x_1\, R_1\, x_1$. Da (A_2, R_2) reflexiv ist, ist $x_2\, R_2\, x_2$. Damit ist also $(x_1, x_2)\ R\ (x_1, x_2)$. D.h. $(A_1 \times A_2, R)$ ist reflexiv. □

Ein Satz wie dieser, "Reflexivität wird durch Produktbildung beibehalten", ist ein typisches Beispiel für die Art von einfachen Resultaten, die oft auf Definitionen (in diesem Fall: des Produkts zweier Relationen) folgen. Sie sind nützlich, um den neu definierten Begriff besser zu verstehen, vgl. dazu auch die Fragen über Definitionen in Kapitel 3.

Man beachte auch, dass dieser Satz einen hohen Abstraktionsgrad hat. Er trifft auf beliebige reflexive Relationen zu, ob diese nun als Grundmenge eine endliche Menge von Webseiten, die ganzen Zahlen $\mathbb{Z}$, die komplexen Zahlen $\mathbb{C}$, oder irgendeine andere Menge haben. Dass die Mathematik in den Naturwissenschaften und Ingenieurswissenschaften wie z.B. der Informatik einen so hohen Nutzen hat, liegt vor allem an dieser Fähigkeit zur Abstraktion.

Äquivalenzrelationen. Eine der wichtigsten Klassen von Relationen sind Äquivalenzrelationen. Wie der Name schon sagt, geht es dabei um eine Formalisierung des Begriffs der Äquivalenz als

Relation. Diese Intention führt zur folgenden Definition.

Definition. Sei A eine Menge und sei $R \subseteq A \times A$ eine Relation auf A. R heißt ...

1. **symmetrisch** falls $\forall x \forall y : x\,R\,y \Rightarrow y\,R\,x$
2. **Äquivalenzrelation** falls R reflexiv, symmetrisch und transitiv ist.

Beispiel. Sei $m \in \mathbb{Z}, m \geq 1$. Dann ist die Relation "kongruent modulo m" für $a, b \in \mathbb{Z}$ definiert durch $a \equiv_m b :\Leftrightarrow m \mid a - b$. Diese Relation ist eine Äquivalenzrelation.[2]

Beispiel. Sei A die Menge der Studenten, die an dieser Lehrveranstaltung teilnehmen und sei, für $x, y \in A$ die Relation R definiert durch: $x\,R\,y$ genau dann wenn x und y im selben Jahr geboren sind. Dann ist (A, R) eine Äquivalenzrelation.[3]

Sei $(A, \sim)$ eine Äquivalenzrelation[4] und sei $x \in A$. Dann heißt die Menge $[x]_\sim = \{y \in A \mid x \sim y\}$ **Äquivalenzklasse** (oder oft auch nur einfach **Klasse**) von x bezüglich $\sim$. Die Menge aller Äquivalenzklassen schreibt man als $A/\sim = \{[x]_\sim \mid x \in A\}$. Die Äquivalenzklassen einer Äquivalenzrelation $(A, \sim)$ bilden eine Partition von A, d.h. jedes $x \in A$ liegt in genau einer Klasse $C \in A/\sim$, nämlich in $[x]_\sim$. Auch umgekehrt gilt, dass jede Partition einer Menge einer Äquivalenzrelation auf dieser Menge entspricht.

Eine Relation R auf einer Menge A ist eine Teilmenge $R \subseteq A \times A$. Damit hatten wir also schon, in Form von Relationen, mit Teilmengen einer beliebigen Menge A bzw. eben von $A \times A$ zu tun. Eine Relation ist also, in anderen Worten ein Element der Potenzmenge von $A \times A$, d.h. $R \in \mathcal{P}(A \times A)$. Mit der obigen Darstellung einer Äquivalenzrelation als Partition steigen wir noch eine Stufe höher: $A/\sim$ ist eine Menge von Mengen. Wir haben also $A/\sim \subseteq \mathcal{P}(A)$, d.h. $A/\sim \in \mathcal{P}(\mathcal{P}(A))$. Aber auch bei diesen "großen" Mengen ändert sich an der logischen Behandlung nichts: die selben logischen Schlussregeln, Beweistechniken, usw. werden in Beweisen verwendet.

Das Wichtigste in Kürze.

• Wenn wir statt mit konkreten mit abstrakten mathematischen Objekten arbeiten, bleibt die logische Ebene unverändert. Im Abstrakten genauso wie im Konkreten gelten die selben Regeln für Beweise, logische Schlussfolgerungen, Beweistechniken und den Umgang mit Definitionen.

[2] Zeigen Sie das als Übungsbeispiel.

[3] Zeigen Sie das als Übungsbeispiel.

[4] Für Äquivalenzrelationen (und andere symmetrische Relationen) verwendet man gerne symmetrische Zeichen wie z.B. $\sim$, $\approx$, $\equiv$, ...

Kapitel 10

Vermutungen

Bisher haben wir uns meist mit Aussagen beschäftigt, von denen wir bereits wussten, ob sie wahr oder falsch sind. Aufgaben der häufig vorkommenden Form "Zeigen Sie, dass ..." sind von dieser Art. In Aufgaben der Form "Beweisen oder widerlegen Sie ..." ist zwar der Wahrheitswert der gegebenen Aussage nicht bekannt, wohl aber die Aussage selbst.

Oft ist man beim mathematischen Arbeiten aber in einer Situation, wo selbst die zentralen Aussagen nicht bekannt sind. Das ist z.B. immer dann der Fall, wenn man mit neuen Begriffen konfrontiert wird und diese, oder deren Verhältnis zu bestehenden Begriffen, besser verstehen will. Wir wollen dann also nicht bestehende Aussagen beweisen, sondern wahre Aussagen selbst finden (und beweisen). Ein wichtiges Werkzeug zur systematischen Behandlung solcher Situationen sind Vermutungen.

Eine **Vermutung** ist eine Aussage, deren Wahrheitswert nicht bekannt ist, von der man aber glaubt dass sie wahr ist. Es gibt Vermutungen ganz unterschiedlicher Größenordnungen in der Mathematik: angefangen von einem Werkzeug zum Lösen einfacher Übungsbeispiele bis hin zu Vermutungen die Jahrhunderte unbewiesen waren (bzw. sind) und die Entwicklung ganzer Teilgebiete der Mathematik angetrieben haben. Für uns sind in dieser Lehrveranstaltung vor allem erstere von Relevanz. Bei solchen, also "kleinen", Vermutungen besteht der hauptsächliche Nutzen einer Vermutung in der Präzisierung einer, zunächst vielleicht noch unklaren, mathematischen Vorstellung. Ist eine konkrete Vermutung, und damit eine konkrete Aussage, erst einmal aufgestellt, kann sie bewiesen oder widerlegt werden was in jedem Fall zu einer Zunahme des Wissens über die Situation führt.

Vermutungen werden in der Mathematik von offenen Problemen unterschieden. Ein offenes **Problem** ist eine Aussage deren Wahrheitswert nicht bekannt ist. Man hat also, im Unterschied zu einer Vermutung, bei einem offenen Problem keinen hinreichenden Grund dafür, an einen bestimmten Wahrheitswert zu glauben.

Wir werden nun einige Techniken für den effektiven Umgang mit Vermutungen kennenlernen. Um diese im Beispiel am Ende des Kapitels leichter zu referenzieren, nummerieren wir sie hier durch.

(1) Aufstellen einer Vermutung. Das Aufstellen einer Vermutung ist immer dann angebracht, wenn man einen Grund dafür hat zu glauben, dass eine Aussage wahr ist. Worin dieser Grund besteht kann je nach Situation sehr unterschiedlich sein. Typisch sind etwa Beispiele oder Teilklassen, in denen die Vermutung wahr ist.

So könnte man z.B. auf Basis der folgenden Rechnungen[1]

$$4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, 10 = 7 + 3, \dots, 60 = 29 + 31$$

[1] oder ähnlicher, wesentlich umfangreicherer, von einem Computer durchgeführten Rechnungen

die Vermutung aufstellen, dass sich jede gerade Zahl ≥ 4 als Summe zweier Primzahlen schreiben lässt. Diese Aussage ist auch als Goldbachsche Vermutung bekannt und stammt aus dem Jahr 1742. Bis heute ist sie weder bewiesen noch widerlegt worden.

(2) Entwicklung eines Beweisplans. Um eine (etwas größere) Vermutung zu beweisen ist es oft sinnvoll, einen **Beweisplan** zu entwickeln, d.h. eine Unterteilung der großen Vermutung in mehrere kleinere und wie diese zusammen den Beweis der großen Vermutung ergeben.

Als Beispiel betrachten wir die folgende

Vermutung. *Jedes $n \in \mathbb{Z}$ das eine Quadratzahl und eine Kubikzahl ist*[2] *hat die Form $n = 7k$ oder $n = 7k + 1$.*

Hier geht es also um Quadratzahlen und Kubikzahlen modulo 7. Es ist also naheliegend, sich zunächst einmal zu überlegen welche Form Quadratzahlen und, unabhängig davon, Kubikzahlen modulo 7 überhaupt haben können. Konkret wollen wir die Aussagen

A. $a \in \mathbb{Z}_7 \Rightarrow a^2 \in Q \subseteq \mathbb{Z}_7$

B. $a \in \mathbb{Z}_7 \Rightarrow a^3 \in K \subseteq \mathbb{Z}_7$

für noch unbekannte Q und K zeigen. Im Zuge dieses Beweises erwarten wir konkrete Q und K zu finden. Damit reicht es dann zu zeigen dass

C. $Q \cap K = \{\overline{0}, \overline{1}\}$

Durch diesen Beweisplan haben wir also unsere Vermutung in drei kleinere Vermutungen zerlegt, aus denen gemeinsam die ursprüngliche Vermutung folgt.

(3) Revision der Vermutung. Findet man für eine Vermutung ein Gegenbeispiel wird die Vermutung widerlegt. Manchmal muss die Vermutung dann zur Gänze verworfen werden. Ein bekanntes Beispiel dafür ist die folgende Vermutung: Eine Zahl der Form $F_n = 2^{2^n} + 1$ heißt "Fermatzahl". Pierre de Fermat stellte fest dass $F_0, \ldots, F_4$ Primzahlen sind und vermutete (im Jahr 1640) dass alle F_n Primzahlen sind. Diese Vermutung wurde von Leonhard Euler (im Jahr 1732) widerlegt, indem er zeigte dass $641 \mid F_5$. Später sind noch etliche weitere Fermatzahlen entdeckt worden, die keine Primzahlen sind. Die ursprüngliche Vermutung wurde verworfen.

Wird ein Gegenbeispiel bekannt, ist es aber auch oft möglich, mit einer revidierten Vermutung weiterzuarbeiten, indem etwa das Gegenbeispiel, oder eine ganze Klasse zu der es gehört, ausgeschlossen wird. So könnte man z.B. nach Betrachtung einiger Beispiele die folgende Vermutung aufstellen: "Alle Primzahlen sind ungerade." Diese Vermutung kann leicht durch das Gegenbeispiel 2 widerlegt werden. Anstatt jetzt aber die Vermutung zur Gänze zu verwerfen ist es sinnvoll mit der revidierten Vermutung "Alle Primzahlen bis auf 2 sind ungerade." weiterzuarbeiten. Diese Aussage ist nämlich tatsächlich wahr.

(4) Abschwächung der Vermutung. Um einen Beweis für eine Vermutung zu finden ist es oft sinnvoll zunächst einmal die Vermutung zu abzuschwächen.[3] Eine Abschwächung ist meistens leichter zu beweisen. Wie diese Abschwächung aussieht hängt von der konkreten Situation ab. Oft ist es

[2] wie z.B. $64 = 8^2 = 4^3$

[3] Eine Aussage A heißt schwächer als eine Aussage A' falls $A' \Rightarrow A$ gilt.

z.B. sinnvoll, die Vermutung auf eine bestimmte, einfache Klasse von Objekten einzuschränken (z.B. Primzahlen statt beliebigen Zahlen, Rechtecke statt beliebigen Vierecken, etc.). Oft ist es auch sinnvoll, zusätzliche, vereinfachende, Annahmen zu treffen (z.B. die Vermutung für teilerfremde a, b statt für beliebige a, b zu zeigen, etc.). Und umgekehrt geschieht es oft, dass man beim Versuch einen bestimmten Beweis durchzuführen, eine zusätzliche Annahme trifft, unter der der Beweis gelingt. Damit ist zwar eine schwächere Vermutung bewiesen, aber dieser Beweis kann oft als erster Schritt zu einem Beweis der gesamten Vermutung dienen.

Ähnliches trifft zu, wenn man es mit einer mathematischen Frage, und damit noch nicht einer konkreten Vermutung, zu tun hat. Auch in diesem Fall ist es typischerweise nützlich, damit zu beginnen, eine eingeschränkte und dadurch einfachere Frage zu bearbeiten.

(5) Verallgemeinerung eines Beweises. Nach dem erfolgreichen Abschluss eines Beweises ist es sinnvoll, in Form einer Rückschau eine Analyse des Beweises durchzuführen. Vor allem ist es nützlich sich zu fragen, wovon das Argument wesentlich abhängt und ob es verallgemeinert werden kann. Ist das der Fall, kann vielleicht auch die Vermutung verallgemeinert werden und man hat ein stärkeres Resultat[4] als ursprünglich geplant erhalten. Es ist auch nützlich sich zu fragen, ob man den Beweis oder die Beweisstrategie für andere, verwandte, Probleme benutzen kann.

Differenzen zweier Quadrate. Wir wollen nun ein etwas längeres Beispiel besprechen, an dem wir die oben eingeführten Techniken zum Umgang mit Vermutungen illustrieren können.

Wir beschäftigen uns mit der folgenden Frage:

Welche Zahlen sind als Differenz zweier Quadrate darstellbar?

Das ist keine konkrete Aussage. Wir sind also in einer Situation wo wir erst überlegen müssen welche Aussagen wir überhaupt beweisen wollen.

Um zu einem Problem einen ersten Zugang zu finden, ist es oft nützlich, einige Beispiele zu betrachten. Das kann auch als Anwendung von Technik (4) gesehen werden: statt zu fragen: welche Zahlen sind als Differenz zweier Quadrate darstellbar? fragen wir zunächst für ein konkretes n: ist n als Differenz zweier Quadrate darstellbar? Wir beobachten also z.B.:

$$1 = 1^2 - 0^2$$
$$3 = 2^2 - 1^2$$
$$5 = 3^2 - 2^2$$
$$7 = 4^2 - 3^2$$

An dieser Stelle könnte man einmal, etwas naiv, die folgende Vermutung aufstellen. (1)

Definition. Sei $D = \{n \geq 1 \mid \exists k, l \geq 0 : n = k^2 - l^2\}$.

Vermutung 1. *Sei $n \geq 1$. Dann ist $n \in D$ genau dann wenn n ungerade ist.*

Der nächste Schritt besteht darin, einen Beweisplan zu entwickeln. Dazu sehen wir uns noch einmal die obigen Rechnungen an und versuchen sie zu verallgemeinern. Die linken Seiten $1, 3, 5, 7$ können geschrieben werden als $2k + 1$. Nun betrachten wir z.B. die Zeile $3 = 2^2 - 1^2$. In dieser Zeile ist $k = 1$. Damit kann die rechte Seite als $(k+1)^2 - k^2$ geschrieben werden. Unser Beweisplan besteht also darin 1. die Aussage (2) (5)

[4] Eine Aussage A heißt stärker als eine Aussage A' falls $A \Rightarrow A'$ gültig ist. A ist also stärker als A' genau dann wenn A' schwächer als A ist.

A. Für alle $k \geq 0$: $(k+1)^2 - k^2 = 2k+1$.

und 2. aus A dann Vermutung 1 zu zeigen.

A kann auch tatsächlich leicht durch die folgende Rechnung bewiesen werden:

$$(k+1)^2 - k^2 = k^2 + 2k + 1 - k^2 = 2k + 1.$$

Wie sieht es nun mit dem Beweis von Vermutung 1 aus A aus? Klar ist: Falls n ungerade ist, dann kann es als $n = 2k+1$ und damit als $n = 2k+1 = (k+1)^2 - k^2$ geschrieben werden. Damit ist gezeigt, dass alle ungeraden $n \geq 1$ in D sind. Wie sieht es mit der Inklusion in die andere Richtung aus? Ist jedes $n \in D$ ungerade? Für alle Differenzen benachbarter Quadrate ist die Antwort ja, da ja $(k+1)^2 - k^2$ ungerade ist. Wie sieht es aus, wenn die beiden Quadrate nicht benachbart sind? Wir betrachten das Beispiel $3^2 - 1^2 = 8$ und stellen fest, dass 8 keine ungerade Zahl ist. Wir haben also ein Gegenbeispiel zu Vermutung 1 gefunden.

(3) Wir müssen also die Vermutung auf Basis des Gegenbeispiels und des bekannten Beweises revidieren: Wir haben nur mit Quadraten von Zahlen mit Differenz $a = 1$ gearbeitet. Für diese hat unser Beweisplan funktioniert. Dieser Parameter a scheint also für das Problem eine zentrale Rolle zu spielen. Wir führen also die folgende Notation ein[5]:

Definition. Für $a \geq 1$ sei $D_a = \{n \geq 1 \mid \exists k \geq 0 : n = (k+a)^2 - k^2\}$.

(2) Dann ist $D = \bigcup_{a \geq 1} D_a$ und unser Plan für die Lösung der ursprünglichen Frage der Charakterisierung von D besteht jetzt darin, zunächst alle D_a zu charakterisieren und diese Ergebeniss dann zu einer Charakterisierung von D zusammenzuführen. Wir können nun präzisieren, wofür unser Beweis funktioniert:

Satz. *Sei $n \geq 1$. Dann ist $n \in D_1$ genau dann wenn n ungerade ist.*

Dieser Satz folgt nun unmittelbar aus A, da $D_1 = \{(k+1)^2 - k^2 \mid k \geq 0\} =^{A} \{2k+1 \mid k \geq 0\}$. Wir haben also jetzt eine schöne Charakterisierung der Menge D_1, nicht aber von ganz D.

(4) Wir betrachten nun die nächste Vereinfachung des ursprünglichen Problems: *Was ist D_2?* Wir führen wieder Rechnungen durch:

$$\begin{aligned} 2^2 - 0^2 &= 4 \\ 3^2 - 1^2 &= 8 \\ 4^2 - 2^2 &= 12 \\ 5^2 - 3^2 &= 16 \end{aligned}$$

(1) Das legt die Vermutung nahe, dass D_2 genau aus den Vielfachen von 4 (die > 0 sind) besteht, genauer:

Vermutung 2. $D_2 = \{4q \mid q \geq 1\}$.

(2) Wie oben entwickeln wir einen Beweisplan der auf einer Verallgemeinerung von Rechnungen basiert.
(5) Die linke Seite wird als $(k+2)^2 - k^2$ geschrieben, die rechte Seite als $4(k+1)$. Damit besteht unser Beweisplan daraus, 1. die Aussage

B. Für alle $k \geq 0$: $(k+2)^2 - k^2 = 4(k+1)$.

[5] Die Verwendung von Definitionen zur Einführung neuer Notationen und Begriffe ist beim Arbeiten mit Beweisplänen oft nützlich.

zu beweisen und 2. aus B dann Vermutung 2. B kann leicht durch die Rechnung

$$(k+2)^2 - k^2 = k^2 + 4k + 4 - k^2 = 4k + 4 = 4(k+1).$$

gezeigt werden. Daraus folgt auch Vermutung 2 da ja

$$D_2 = \{(k+2)^2 - k^2 \mid k \geq 0\} =^{\text{B}} \{4(k+1) \mid k \geq 0\} = \{4q \mid q \geq 1\}.$$

Damit ist also Vermutung 2 bewiesen.

Wir haben das Problem jetzt für D_1 und D_2 gelöst und betrachten als nächstes D_3, also wiederum eine Vereinfachung des allgemeinen Problems. Für $a = 3$ ergibt sich die Rechnung (4)

$$n = (k+3)^2 - k^2 = k^2 + 6k + 9 - k^2 = 6k + 9 = 3(2k+3).$$

Nun ist sowohl 3 als auch $2k+3$ ungerade, also ist auch n ungerade. Wir haben also gezeigt, dass alle $n \in D_3$ ungerade sind.

Überlegen wir uns nun, als Nachbetrachtung, wovon dieses Argument abhängt. $n = (k+a)^2 - k^2$ wird, unabhängig von a, immer zu $n = 2ak + a^2$. Im zweiten Schritt der Rechnung haben wir a herausgehoben, also $n = a(2k+a)$ erhalten. Danach haben wir festgestellt: "$a = 3$ *ist ungerade. Damit ist auch* $2k + a$ *ungerade und damit auch* $n = a(2k+a)$." Wir sehen also: dieses Argument funktioniert für *beliebige ungerade* a, nicht nur für $a = 3$. Durch diese Beobachtung haben wir den obigen Beweis verallgemeinert und daraus die folgende Aussage erhalten: (5)

Satz. *Falls a ungerade ist und $n \in D_a$, dann ist auch n ungerade.*

Damit ist das Problem für $a = 1, 2, 3, 5, 7, 9, \ldots$ gelöst. Uns fehlen also noch die geraden $a \geq 4$. Sei also $a = 2b$. Dann hat die für dieses Problem zentrale Rechnung die Form

$$n = (k+2b)^2 - k^2 = k^2 + 4bk + 4b^2 - k^2 = 4bk + 4b^2 = 4(bk + b^2).$$

Damit ist n ein Vielfaches von 4. Wir haben also bewiesen:

Satz. *Falls a gerade ist und $n \in D_a$, dann ist n ein Vielfaches von 4.*

Damit haben wir nun alle Möglichkeiten für a behandelt. Da $D = \bigcup_{a \geq 1} D_a$ erhalten wir:

Satz. *Sei $n \geq 1$. Dann ist $n \in D$ genau dann wenn n ungerade oder ein Vielfaches von 4 ist.*

Dieser Satz ist durch die obigen Überlegungen vollständig bewiesen. Allerdings ist dieser Beweis nicht gut lesbar, da er etliche Spezialfälle und Umwege enthält. Das ist typisch: oft ist das Format, in dem man einen Beweis findet nicht gut dazu geeignet, den Beweis zu präsentieren. Dem kann Abhilfe geschaffen werden, indem man eine Schönschrift des Beweises anfertigt. Wir tun das im Folgenden auf Basis der obigen Überlegungen:

Beweis. Für die Implikation von links nach rechts sei $n \in D$. Dann existieren $a \geq 1$, $k \geq 0$ so dass $n = (k+a)^2 - k^2 = k^2 + 2ak + a^2 - k^2 = 2ak + a^2$. Wir machen eine Fallunterscheidung: Falls a gerade ist, d.h. $a = 2b$ für ein $b \geq 1$, ist $n = 4bk + 4b^2 = 4(bk + b^2)$ ein Vielfaches von 4. Falls n ungerade ist, d.h. $a = 2b + 1$ für ein $b \geq 0$, dann ist $n = (2b+1)(2(k+b)+1)$ ungerade weil sowohl $2b+1$, als auch $2(k+b)+1$ ungerade sind.

Für die Implikation von rechts nach links sei zunächst n ungerade, d.h. $n = 2k+1$ für ein $k \geq 0$. Dann ist $n = 2k+1 = (k+1)^2 - k^2 \in D$. Sei n nun ein Vielfaches von 4, d.h. $n = 4q$ für ein $q \geq 1$. Dann ist $(q+1)^2 - (q-1)^2 = q^2 + 2q + 1 - (q^2 - 2q + 1) = 4q = n \in D$. □

Das Wichtigste in Kürze.

- Eine Vermutung ist eine Aussage, deren Wahrheitswert nicht bekannt ist, von der man aber glaubt, dass sie wahr ist.
- In einer unklaren mathematischen Situation besteht der entscheidene Beitrag einer Vermutung darin, eine (mathematisch klare) Aussage zur Verfügung zu stellen, die bewiesen oder widerlegt werden kann. In beiden Fällen erhält man neue Erkenntnisse über die Situation.
- Durch Anwendung verschiedener Standardtechniken im Umgang mit Vermutungen kann eine unklare mathematiche Situation systematisch verstanden werden.

Literaturverzeichnis

[1] Albrecht Beutelspacher. *Das ist o.B.d.A. trivial*. Vieweg+Teubner, 9 edition, 2009.

[2] Daniel Grieser. *Mathematisches Problemlösen und Beweisen*. Springer, 2 edition, 2017.

[3] George Polya. *How to Solve It: A New Aspect of Mathematical Method*. Princeton University Press, 2nd edition, 1988.

[4] Hermann Schichl and Roland Steinbauer. *Einführung in das mathematische Arbeiten*. Springer, 3. edition, 2018.

[5] Doug Smith, Maurice Eggen, and Richard St. Andre. *A Transition to Advanced Mathematics*. Cengage Learning, 8th edition, 2014.

[6] Harald Woracek. Einführung in das mathematische Arbeiten. Skriptum, TU Wien.

Index