Einführung in das mathematische Beweisen

Inhaltsverzeichnis

1 Umgangssprachliche Logik

Anders als in anderen Wissenschaften, wird eine Aussage in der Mathematik erst dann als wahr akzeptiert, wenn man einen für alle Beteiligten nachvollziehbaren *Beweis* für diese Aussage gefunden hat. Unter einem „mathematischen Beweis“ versteht man im Wesentlichen eine logisch fehlerfreie Herleitung einer Aussage aus bestimmten als wahr vorausgesetzten Grundannahmen (sogenannten *Axiomen*) oder anderen bereits bewiesenen Aussagen. Um diese sehr grobe Annäherung an den Begriff des mathematischen Beweises ein wenig zu präzisieren, wollen wir uns in diesem Kapitel zunächst mit ein paar logischen Grundbegriffen beschäftigen.

Dabei ist es von großer Bedeutung, zwischen zwei verschiedenen Arten von „Logik“ zu unterscheiden. Während man in der sogenannten *formalen Logik* zunächst eine formale Sprache definiert und für diese Sprache anschließend einen *formalen Kalkül*, also ein präzise bestimmtes System von logischen Schlussregeln und Axiomen konstruiert, werden mathematische Beweise in der Regel umgangssprachlich formuliert, weshalb man in diesem Zusammenhang auch von *umgangssprachlicher* oder *informeller Logik* spricht. Zu wissen, welche Schlüsse in einem umgangssprachlichen oder informellen Beweis erlaubt sind und welche Aussagen dabei als „selbstverständlich“ vorausgesetzt werden dürfen, ist normalerweise einfach eine Frage der Übung.

Umgangssprachliche und formale Logik stehen in einer sehr engen Beziehung zueinander: Zum einen lassen sich viele umgangssprachliche Beweise in formale Beweise umwandeln, also in einem entsprechenden formalen System nachvollziehen und so auf ihre Richtigkeit hin überprüfen; zum anderen können umgangssprachliche Beweistechniken auch dazu verwendet werden, formale logische Systeme aus einer „Metaperspektive“ heraus zu untersuchen und so wiederum Aussagen *über* diese Systeme zu beweisen (dies ist im Wesentlichen Inhalt der Vorlesung *Logiksysteme*). Um in diesem Fall den Unterschied zwischen dem gerade untersuchten logischen System (bzw. der zugehörigen formalen Sprache) und der bei der Untersuchung verwendeten umgangssprachlichen Logik zu kennzeichnen, bezeichnet man die untersuchte Sprache auch als *Objektsprache* und die Sprache, mit der die Objektsprache untersucht wird, als *Metasprache*. Entsprechend unterscheidet man zwischen *objektsprachlicher Logik* und *metasprachlicher Logik*.

Bevor wir uns in Kapitel 2 mit den wichtigsten Techniken und Strategien umgangssprachlicher bzw. metasprachlicher Beweise vertraut machen können, müssen wir uns zunächst mit *Aussagen und Aussageverknüpfungen* (Abschnitt 1.1) sowie mit *Aussageformen und Quantoren* (Abschnitt 1.2) auseinandersetzen.

1.1 Aussagen und Aussageverknüpfungen

Unter einer „Aussage“ versteht man in der Mathematik einen Satz, der entweder wahr oder falsch ist (aber niemals beides zugleich). Mathematische Aussagen unterscheiden sich im Wesentlichen dadurch von anderen Aussagen, dass sie von mathe-

matischen Objekten wie Zahlen, Mengen, Relationen oder Funktionen handeln. Ein typisches Beispiel für eine mathematische Aussage ist etwa der Satz „$\sqrt{2}$ ist eine rationale Zahl“ oder „Für alle geraden natürlichen Zahlen n und m ist die Summe $n + m$ eine gerade Zahl“. Wie sich zeigen lässt, ist der Satz „$\sqrt{2}$ ist eine rationale Zahl“ eine *falsche* und der Satz „Für alle geraden natürlichen Zahlen n und m ist die Summe $n + m$ eine gerade Zahl“ eine *wahre* Aussage.

Obwohl es sich bei mathematischen Beweisen um informelle Beweise handelt und die einzelnen Beweisschritte normalerweise nur umgangssprachlich formuliert werden, ist es von großer Bedeutung, alle wichtigen Begriffe präzise zu definieren und so potenzielle Missverständnisse und Zweideutigkeiten von vornherein auszuschließen. Darüber hinaus gibt es in der Mathematik viele „standardisierte“ Formulierungen, die mit einer genau festgelegten Bedeutung versehen sind. Hierzu gehören vor allem diejenigen Ausdrücke, die man verwendet, um einzelne Aussagen miteinander zu verknüpfen und so neue, komplexe Aussagen zu bilden.

Betrachten wir zur Veranschaulichung die beiden Aussagen „7 ist eine Primzahl“ und „$3 > 7$“. Offensichtlich handelt es sich bei der ersten Aussage um eine *wahre* und bei der zweiten um eine *falsche* Aussage. Mit Hilfe unterschiedlicher Aussageverknüpfungen können diese Aussagen zu neuen Aussagen zusammengesetzt werden, deren Wahrheitswert sich aus dem Wahrheitswert der enthaltenen Teilaussagen ergibt. Beispielsweise könnten wir die genannten Aussagen durch das Wort „und“ miteinander verbinden und so die neue Aussage

„7 ist eine Primzahl und $3 > 7$“

bilden, die man auch als die (*logische*) *Konjunktion* der beiden Aussagen „7 ist eine Primzahl“ und „$3 > 7$“ bezeichnet. Die Konjunktion „7 ist eine Primzahl und $3 > 7$“ ist genau dann wahr, wenn sowohl „7 ist eine Primzahl“ als auch „$3 > 7$“ eine wahre Aussage ist (da letzteres nicht der Fall ist, ist die Konjunktion „7 ist eine Primzahl und $3 > 7$“ also falsch).

Weil der Wahrheitswert einer Konjunktion nur vom Wahrheitswert der enthaltenen Teilaussagen, nicht aber von deren Inhalt abhängt, können wir auf die Betrachtung konkreter Aussagen verzichten und stattdessen einfach die Platzhalterbuchstaben P und Q verwenden, die im Folgenden für *beliebige* Aussagen stehen sollen. Ferner können wir anstelle des Wortes „und“ auch das kürzere und übersichtlichere Symbol & verwenden. Die Bedeutung der logischen Konjunktion P & Q lässt sich dann präzise in Form einer sogenannten *Wahrheitstafel* angeben. Dabei tragen wir zunächst die verschiedenen möglichen Wahrheitswertkombinationen für die Teilaussagen P und Q untereinander in eine Tabelle und geben dann in der Spalte rechts daneben an, ob die Konjunktion P & Q für die jeweilige Kombination wahr oder falsch ist. Schreiben wir „W“ für „wahr“ und „F“ für „falsch“, so erhalten wir für P & Q die folgende Wahrheitstafel:

P	Q	P & Q
W	W	W
W	F	F
F	W	F
F	F	F

Neben der logischen Konjunktion existieren verschiedene andere wichtige Aussageverbindungen, die in der Mathematik eine genau festgelegte Bedeutung besitzen. Wir geben einen kurzen Überblick:

- Die (*logische*) *Disjunktion* „P oder Q“ soll im Folgenden mit „$P \parallel Q$“ abgekürzt werden und ist genau dann wahr, wenn mindestens eine der Aussagen P und Q wahr ist. Die Wahrheitstafel der Disjunktion hat also die Form

P	Q	$P \parallel Q$
W	W	W
W	F	W
F	W	W
F	F	F

- Die (*logische*) *Implikation* „Wenn P, dann Q“ wird oft in der Form „$P \Rightarrow Q$“ geschrieben und ist genau dann wahr, wenn P falsch oder Q wahr ist. Die Wahrheitstafel der Implikation hat also die Gestalt

P	Q	$P \Rightarrow Q$
W	W	W
W	F	F
F	W	W
F	F	W

- Die (*logische*) *Äquivalenz* „P genau dann, wenn Q“ wird auch in der Form „$P \Leftrightarrow Q$“ aufgeschrieben und ist genau dann wahr, wenn P und Q denselben Wahrheitswert besitzen. Die logische Äquivalenz besitzt also die folgende Wahrheitstafel:

P	Q	$P \Leftrightarrow Q$
W	W	W
W	F	F
F	W	F
F	F	W

- Die (*logische*) *Negation* „Nicht-P“ oder kurz „$\sim P$“ ist genau dann wahr, wenn P falsch ist. Wir erhalten für die Negation also die folgende Wahrheitstafel:

P	$\sim P$
W	F
F	W

Durch die Kombination und Verschachtelung dieser Aussageverknüpfungen können wir aus einfachen Aussagen beliebig komplexe Aussagen zusammensetzen, deren Wahrheitswert sich dann mit Hilfe von Wahrheitstafeln aus dem Wahrheitswert der enthaltenen Teilaussagen ermitteln lässt. Betrachten wir als Beispiel die Aussage „$((P \Rightarrow Q)\ \&\ P) \Rightarrow Q$“. Um den Wahrheitswertverlauf dieser Aussage zu ermitteln,

können wir zunächst die verschiedenen möglichen Wahrheitswertkombinationen für P und Q in eine Tabelle schreiben und anschließend Wahrheitstafeln für alle enthaltenen Teilaussagen aufstellen. Dabei kann man sich Schritt für Schritt von den weniger komplexen Teilaussagen zu den stärker verschachtelten Teilaussagen vorarbeiten, bis man schließlich den Wahrheitswertverlauf für die Gesamtaussage ermittelt hat. Schreiben wir die Ergebnisse der einzelnen Teilschritte von links nach rechts in verschiedene Spalten einer einzigen Tabelle, so erhalten wir die folgende große Wahrheitstafel:

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q)\ \&\ P$	$((P \Rightarrow Q)\ \&\ P) \Rightarrow Q$
W	W	W	W	W
W	F	F	F	W
F	W	W	F	W
F	F	W	F	W

Wie sich aus der letzten Spalte der Wahrheitstafel ablesen lässt, ist die Aussage „$((P \Rightarrow Q)\ \&\ P) \Rightarrow Q$“ für *alle* Wahrheitswertkombinationen der Teilaussagen P und Q wahr. Eine solche Aussage wird auch als *Tautologie* bezeichnet.

Definition 1.1.1 (Tautologie)**.** Eine *Tautologie* ist eine Aussage, die immer wahr ist, für die in jeder Zeile der zugehörigen Wahrheitstafel also der Wert „W“ steht.

Neben Aussagen, die immer wahr sind, gibt es auch Aussagen, die immer *falsch* sind. Solche Aussagen bezeichnet man als *Kontradiktionen*.

Definition 1.1.2 (Kontradiktion)**.** Eine *Kontradiktion* ist eine Aussage, die stets falsch ist, für die in jeder Zeile der zugehörigen Wahrheitstafel also der Wert „F“ steht.

Zwischen Tautologien und Kontradiktionen besteht ein enger Zusammenhang, denn offensichtlich ist die Negation einer Tautologie immer eine Kontradiktion und die Negation einer Kontradikation immer eine Tautologie. Die folgende Liste enthält einige sehr bekannte und wichtige Tautologien.

Satz 1.1.3 (Beispiele für Tautologien)**.** Bei den folgenden Aussagen handelt es sich um Tautologien:
(1) $P \Rightarrow (P \parallel Q)$
(2) $(P\ \&\ Q) \Rightarrow P$
(3) $((P \Rightarrow Q)\ \&\ P) \Rightarrow Q$
(4) $((P \Rightarrow Q)\ \&\ {\sim}Q) \Rightarrow {\sim}P$
(5) $(P \Rightarrow Q) \Leftrightarrow ({\sim}Q \Rightarrow {\sim}P)$
(6) $(P \Rightarrow Q) \Leftrightarrow ({\sim}P \parallel Q)$
(7) $(P \Rightarrow Q) \Leftrightarrow {\sim}(P\ \&\ {\sim}Q)$
(8) $((P \Rightarrow Q)\ \&\ (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$
(9) $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q)\ \&\ (Q \Rightarrow P))$

Der Beweis von Satz 1.1.3 ist eine gute Übung, um sich weiter mit der Methode der Wahrheitstafeln vertraut zu machen (nach Definition einer Tautologie genügt es, Wahrheitstafeln für die Aussagen (1)–(9) aufzustellen und sich zu vergewissern, dass diese Aussagen tatsächlich in jeder Zeile den Wahrheitswert „W“ besitzen).

Will man eine mathematische Aussage beweisen, so ist es oft einfacher, eine andere Aussage zu beweisen, die „dieselbe Bedeutung“ hat wie die ursprüngliche Aussage, die also in jeder Zeile der zugehörigen Wahrheitstafel denselben Wahrheitswert besitzt. Aussagen, die denselben Wahrheitswertverlauf besitzen, werden als (logisch) äquivalent bezeichnet.

Definition 1.1.4 (Äquivalenz von Aussagen)**.** Zwei (beliebig komplexe) Aussagen P und Q heißen *logisch äquivalent*, falls $P \Leftrightarrow Q$ eine Tautologie ist. Sind P und Q äquivalent, so schreiben wir auch $P \equiv Q$.

Es folgt unmittelbar aus der Definition der Aussageverknüpfung $\Leftrightarrow$, dass zwei Aussagen P und Q genau dann äquivalent sind, wenn sie in jeder Zeile der zugehörigen Wahrheitstafel denselben Wahrheitswert besitzen. Wie sich leicht mit Hilfe der Wahrheitstafelmethode überprüfen lässt, gelten zum Beispiel die folgenden Äquivalenzen:

Satz 1.1.5 (Wichtige Äquivalenzen)**.**
(1) Doppelnegationsgesetz:

$$\sim\sim P \equiv P$$

(2) Kontraposition:

$$(P \Rightarrow Q) \equiv (\sim Q \Rightarrow \sim P)$$

(3) Weitere Äquivalenzen für die Implikation:

$$(P \Rightarrow Q) \equiv (\sim P \parallel Q)$$
$$(P \Rightarrow Q) \equiv \sim(P \,\&\, \sim Q)$$

(4) Kommutativität:

$$(P \,\&\, Q) \equiv (Q \,\&\, P)$$
$$(P \parallel Q) \equiv (Q \parallel P)$$

(5) Assoziativität:

$$(P \,\&\, (Q \,\&\, R)) \equiv ((P \,\&\, Q) \,\&\, R)$$
$$(P \parallel (Q \parallel R)) \equiv ((P \parallel Q) \parallel R)$$

(6) De Morgansche Regeln:

$$\sim(P \,\&\, Q) \equiv (\sim P \parallel \sim Q)$$
$$\sim(P \parallel Q) \equiv (\sim P \,\&\, \sim Q)$$

Aufgaben

1.1.1 Analysieren Sie die logische Form der folgenden Aussagen mit Hilfe der in diesem Abschnitt besprochenen Aussageverknüpfungen. Bestimmen Sie darüber hinaus den Wahrheitswert der Aussagen.

a) „3 ist ein gemeinsamer Teiler von 6, 9 und 10."
b) „Wenn 15 ein Teiler von 45 ist, dann ist auch jeder positive Teiler von 15 ein Teiler von 45."
c) „Mindestens eine der Zahlen 4, 5 und 6 ist durch 3 teilbar."
d) „Sowohl 2 als auch -2 ist eine Lösung der Gleichung $x^2 = 4$."
e) „Wenn die Zahl 1 zwischen den Zahlen 2 und 5 liegt, dann liegt der Nachfolger von 1 zwischen dem Nachfolger von 2 und dem Nachfolger von 5."

1.1.2 Wir wollen eine Aussage P als *kontingent* bezeichnen, wenn P weder eine Tautologie noch eine Kontradiktion ist. Benutzen Sie Wahrheitstafeln, um zu bestimmen, welche der folgenden Aussagen Tautologien, welche Kontradiktionen und welche kontingent sind:

a) $(P \parallel Q)\ \&\ (\sim P \parallel \sim Q)$
b) $(P \parallel Q) \parallel (\sim P \parallel \sim Q)$
c) $(P \parallel Q)\ \&\ (\sim P\ \&\ \sim Q)$
d) $(P\ \&\ (Q \parallel \sim R)) \parallel (\sim P \parallel R)$

1.1.3 Zeigen Sie mit Hilfe der Wahrheitstafelmethode die folgenden Äquivalenzen:

a) $(P\ \&\ P) \equiv P$
b) $(P \parallel P) \equiv P$
c) $(P\ \&\ (Q \parallel R)) \equiv ((P\ \&\ Q) \parallel (P\ \&\ R))$
d) $(P \parallel (Q\ \&\ R)) \equiv ((P \parallel Q)\ \&\ (P \parallel R))$
e) $P\ \&\ (P \parallel Q) \equiv P$
f) $P \parallel (P\ \&\ Q) \equiv P$

1.1.4 Wir betrachten eine neue Aussageverknüpfung $\downarrow$, die durch die folgende Wahrheitstafel gegeben ist:

P	Q	$P \downarrow Q$
W	W	F
W	F	F
F	W	F
F	F	W

a) Welcher umgangssprachliche Ausdruck entspricht der Verknüpfung $\downarrow$?
b) Finden Sie eine Aussage, die zu $P \downarrow Q$ äquivalent ist und nur die Verknüpfungszeichen $\sim$ und $\parallel$ enthält.
c) Finden Sie eine zu $P \downarrow Q$ äquivalente Aussage, die nur die Verknüpfungszeichen $\sim$ und & enthält.
d) Finden Sie Aussagen, die nur das Verknüpfungszeichen $\downarrow$ enthalten und zu $\sim P$, $P\ \&\ Q$, $P \parallel Q$ bzw. $P \Rightarrow Q$ äquivalent sind.

1.1.5 Wir betrachten eine neue zweistellige Aussagenverknüpfung $P \uparrow Q$ mit der umgangssprachlichen Bedeutung „P und Q sind nicht beide wahr“.

a) Erstellen Sie eine Wahrheitstafel für $\uparrow$.
b) Finden Sie eine Aussage, die nur die Verknüpfungszeichen $\sim$ und & enthält und logisch äquivalent zu $P \uparrow Q$ ist.
c) Finden Sie eine zu $P \uparrow Q$ äquivalente Aussage, die nur die Verknüpfungszeichen $\sim$ und $\|$ enthält.
d) Finden Sie Aussagen, die nur das Verknüpfungszeichen $\uparrow$ enthalten und zu $\sim P$, $P \,\&\, Q$, $P \,\|\, Q$ bzw. $P \Rightarrow Q$ äquivalent sind.

1.1.6

a) Zeigen Sie: Ist P eine Tautologie, dann gilt $(P \,\&\, Q) \equiv Q$ und $(P \,\|\, Q) \equiv P$.
b) Benutzen Sie Aufgabenteil a), um zu zeigen, dass es unendlich viele Tautologien gibt.
c) Folgern Sie, dass es unendlich viele Kontradiktionen gibt.

1.1.7 Finden Sie Aussagen, die neben den Platzhalterbuchstaben P und Q nur die Verknüpfungen &, $\|$ und $\sim$ enthalten und die folgenden Wahrheitstafeln besitzen:

a)

P	Q	???
W	W	W
W	F	W
F	W	F
F	F	W

b)

P	Q	???
W	W	F
W	F	W
F	W	W
F	F	W

c)

P	Q	???
W	W	F
W	F	W
F	W	W
F	F	F

1.2 Aussageformen und Quantoren

Bislang haben wir lediglich einfache Aussagen der Art „2 ist eine Primzahl“ oder „4 ist größer als 3“ betrachtet, in denen nur über einzelne Objekte wie etwa die Zahlen 2, 3 oder 4 etwas ausgesagt wird. Aus solchen abgeschlossenen Aussagen lassen sich sogenannte *Aussageformen* bilden, indem man einen oder mehrere der Namen für bestimmte Gegenstände durch Variablen wie x, y oder z ersetzt. So lässt sich beispielsweise aus der Aussage „2 ist eine Primzahl“ die Aussageform „x ist eine Primzahl“ bilden. Diese Aussageform ist nun selbst keine Aussage mehr, kann aber durch Einsetzen entsprechender Werte für die Variable x zu einer wahren oder falschen Aussage gemacht werden. Ob die Aussage, die auf diese Weise entsteht,

wahr oder falsch ist, hängt dabei von den jeweils für x eingesetzten Werten ab. Beispielsweise ist „3 ist eine Primzahl“ eine *wahre* und „4 ist eine Primzahl“ eine *falsche* Aussage.

Auch aus der Aussage „4 ist größer als 3“ lassen sich nach diesem Prinzip Aussageformen bilden. Je nachdem, welche und wie viele der enthaltenen Gegenstandsnamen wir durch Variablen ersetzen, erhalten wir aus „4 ist größer als 3“ die Aussageformen „x ist größer als 3“, „4 ist größer als x“ und „x ist größer als y“. Diese Aussageformen unterscheiden sich dadurch voneinander, dass sie für verschiedene Werte der enthaltenen Variablen wahr bzw. falsch sind. Beispielsweise ist die Aussageform „4 ist größer als x“ für $x = 2$ eine *wahre* Aussage, während die Aussageform „x ist größer als 3“ für diesen Wert *falsch* ist.

Üblicherweise werden Aussageformen mit nur einer einzigen Variable x dabei durch Platzhalterbuchstaben wie $P(x)$, $Q(x)$, $R(x)$ usw. abgekürzt. Für Aussageformen mit zwei Variablen x und y verwendet man die Bezeichnungen $P(x, y)$, $Q(x, y)$, $R(x, y)$ etc. Allgemein schreibt man $P(x_1, \ldots, x_n)$, $Q(x_1, \ldots, x_n)$, $R(x_1, \ldots, x_n)$ usw. für Aussageformen mit n Variablen $x_1, \ldots, x_n$.

Beispiel 1.2.1.

(1) Es sei $P(x)$ die Aussageform „x ist eine Primzahl“. Setzen wir für x den Wert 5 ein, so erhalten wir die wahre Aussage $P(5)$, also „5 ist eine Primzahl“. Die Aussage $P(4)$, also „4 ist eine Primzahl“, ist dagegen falsch.

(2) Es sei $P(x, y)$ die Aussageform „x ist größer oder gleich y“ bzw. kurz „$x \geq y$“. Offensichtlich ist $P(x, y)$ für die Zahlenpaare $(2, 1)$, $(4, 2)$, $(0, -2)$ eine wahre Aussage und für die Zahlenpaare $(1, 2)$, $(2, 4)$ und $(-2, 0)$ falsch. Darüber hinaus ist die Aussageform $P(x, 2)$ für die x-Werte $2, 3, 4, 5, \ldots$ wahr und für die x-Werte $1, 0, -1, -2, \ldots$ falsch.

(3) Es sei $P(x, y, z)$ die Aussageform $x(y + z) = xy + xz$. Da es sich hierbei um das gewöhnliche Distributivgesetz für die Addition und die Multiplikation handelt, ist diese Aussageform für alle (reellen) Zahlentripel (x, y, z) eine wahre Aussage.

Ebenso wie Aussagen können auch Aussageformen mit Hilfe der in Abschnitt 1.1 besprochenen Aussageverknüpfungen zu komplexen Aussageformen zusammengesetzt werden. Betrachten wir zur Veranschaulichung die Aussageformen „x ist durch 3 teilbar“ und „x ist größer als 10“, die wir mit $P(x)$ bzw. $Q(x)$ bezeichnen wollen. Durch Verknüpfung der beiden Aussageformen können wir unter anderem die folgenden komplexen Aussageformen bilden:

- $P(x)$ & $Q(x)$. Diese Aussageform kann gelesen werden als „x ist durch 3 teilbar und größer als 10“ und ist für die x-Werte $12, 15, 18, 21, \ldots$ eine wahre Aussage.

- $P(x) \parallel Q(x)$. Dies entspricht der Aussageform „x ist durch 3 teilbar oder größer als 10“. Folglich ist $P(x) \parallel Q(x)$ sowohl für die x-Werte $9, 6, 3, 0, -3, -6, -9, \ldots$ als auch für die x-Werte $11, 12, 13, 14, 15, \ldots$ eine wahre Aussage.

- $\sim P(x)$. Diese Aussageform kann gelesen werden als „x ist nicht durch 3 teilbar“ und ist unter anderem für die x-Werte $1, 2, 4, 5, 7, \ldots$ wahr. Analog steht $\sim Q(x)$ für die Aussageform „x ist nicht größer als 10“, was gleichbedeutend ist mit „x ist kleiner oder gleich 10“. Somit ist $\sim Q(x)$ für die x-Werte $10, 9, 8, 7, 6, \ldots$ wahr.

Statt die in einer Aussageform enthaltenen Variablen durch konkrete Werte zu ersetzen, können Aussageformen auch dadurch zu Aussagen gemacht werden, dass man die in der Aussageform enthaltenen Variablen *quantifiziert*. Hierzu verwendet man sogenannte *Quantoren*, mit denen ausgedrückt werden kann, wie viele Gegenstände einer zugrunde liegenden Menge eine bestimmte Aussageform erfüllen, wobei auf die Angabe konkreter Werte verzichtet wird. Die folgenden beiden Quantoren spielen eine besonders wichtige Rolle:

- Der *Existenzquantor* $\exists$. Mit Hilfe des Existenzquantors kann ausgedrückt werden, dass es mindestens einen Gegenstand gibt, der eine gegebene Aussageform erfüllt. Ist $P(x)$ also eine (beliebig komplexe) Aussageform, so steht $\exists x P(x)$ für die Aussage „Es existiert mindestens ein Gegenstand x, für den $P(x)$ eine wahre Aussage ist".

- Der *Allquantor* $\forall$. Mit dem Allquantor kann ausgedrückt werden, dass eine Aussageform $P(x)$ für alle Gegenstände (aus einer bestimmten Menge) wahr ist. Die Aussage $\forall x P(x)$ kann also gelesen werden als „Für alle x ist $P(x)$ eine wahre Aussage".

Üblicherweise wird bei der Quantifizierung von Variablen angegeben, über welche zugrundeliegende Menge von Gegenständen man spricht, welche Werte die quantifizierte Variable also annehmen kann. Ist M eine beliebige Menge, so schreibt man dabei $\exists x(x \in M \ \& \ P(x))$ für „Es gibt einen Gegenstand x in der Menge M, so dass $P(x)$ wahr ist" oder „Für mindestens ein Element x von M ist $P(x)$ wahr". Analog schreibt man $\forall x(x \in M \Rightarrow P(x))$ für „Für alle Gegenstände x aus M ist $P(x)$ wahr" oder „Für alle $x \in M$ gilt $P(x)$". Anstelle von $\exists x(x \in M \ \& \ P(x))$ bzw. $\forall x(x \in M \Rightarrow P(x))$ schreibt man dabei abgekürzt auch $\exists x \in M\,(P(x))$ bzw. $\forall x \in M\,(P(x))$. Folgende Mengen spielen in der Mathematik oft eine wichtige Rolle:

- Die Menge der natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$,
- Die Menge der ganzen Zahlen $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$,
- Die Menge der rationalen Zahlen $\mathbb{Q} = \{\frac{n}{m} \mid n, m \in \mathbb{Z}, m \neq 0\}$,
- Die Menge der Primzahlen $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$.

Indem man Existenz- und Allquantoren miteinander kombiniert und einfache Aussageformen mit Hilfe logischer Verknüpfungen zu komplexen Aussageformen zusammensetzt, lassen sich viele mathematische Aussagen sehr präzise aufschreiben. Wir geben einige Beispiele.

Beispiel 1.2.2.

(1) Die Aussage „Jede natürliche Zahl besitzt einen Nachfolger" lässt sich in der Form $\forall x(x \in \mathbb{N} \Rightarrow \exists y(y \in \mathbb{N} \ \& \ (y = x+1)))$ oder kurz $\forall x \in \mathbb{N}\, \exists y \in \mathbb{N}(y = x+1)$ darstellen.

(2) Die Aussage „Die Menge der natürlichen Zahlen ist eine Teilmenge der Menge der ganzen Zahlen" oder „Jede natürliche Zahl ist auch eine ganze Zahl" kann in der Form $\forall x(x \in \mathbb{N} \Rightarrow x \in \mathbb{Z})$ aufgeschrieben werden.

(3) Die Aussage „Ein Vielfaches einer ganzen Zahl ist stets wieder eine ganze Zahl“ lässt sich in der Form $\forall x(x \in \mathbb{Z} \Rightarrow \forall y(\exists z(z \in \mathbb{Z} \;\&\; (y = z \cdot x)) \Rightarrow y \in \mathbb{Z}))$ ausdrücken.

Ebenso kann auch die Aussage „Zu jeder Primzahl gibt es eine größere Primzahl“ in der Form $\forall x(x \in \mathbb{P} \Rightarrow \exists y(y \in \mathbb{P} \;\&\; y > x))$ oder auch $\forall x \in \mathbb{P}\, \exists y \in \mathbb{P}(y > x)$ aufgeschrieben werden. Diese Aussage ist offensichtlich gleichbedeutend mit der Aussage „Es gibt keine größte Primzahl“, die sich durch $\sim\exists x(x \in \mathbb{P} \;\&\; \forall y(y \in \mathbb{P} \Rightarrow \sim(y > x)))$ bzw. durch $\sim\exists x \in \mathbb{P}\, \forall y \in \mathbb{P} \sim(y > x)$ ausdrücken lässt. Derartige Umformungen von Aussagen mit Quantoren folgen bestimmten Regeln, die sich aus der Tatsache ergeben, dass Existenzquantoren auch durch Allquantoren und Allquantoren auch durch Existenzquantoren ausgedrückt werden können, so dass es zu jeder Aussage mit Existenzquantor eine äquivalente Aussage mit Allquantor und umgekehrt zu jeder Aussage mit Allquantor eine äquivalente Aussage mit Existenzquantor gibt. Da wir die Äquivalenz von Aussagen mit Quantoren nicht mehr allein mit Hilfe von Wahrheitstafeln definieren können, legen wir hier die folgende verallgemeinerte Definition zugrunde.

Definition 1.2.3 (Äquivalenz von Aussagen)**.** Zwei Aussagen P und Q heißen *äquivalent*, falls P genau dann wahr ist, wenn Q wahr ist, d. h. immer wenn P wahr ist, ist auch Q wahr und immer wenn Q wahr ist, ist auch P wahr. Sind P und Q äquivalent, dann schreiben wir auch $P \equiv Q$.

Neben den bereits in Satz 1.1.5 genannten Äquivalenzen gelten für Aussagen mit Quantoren die folgenden Umformungsregeln:

Satz 1.2.4 (Wichtige Äquivalenzen für Aussagen mit Quantoren)**.**
(1) Regeln der Quantorendualität:

$$\sim\exists x P(x) \equiv \forall x \sim P(x)$$
$$\sim\forall x P(x) \equiv \exists x \sim P(x)$$

(2) Vertauschungsregeln:

$$\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$$
$$\exists x \exists y P(x, y) \equiv \exists y \exists x P(x, y)$$

(3) Distributivität der Quantoren:

$$\forall x(P(x) \;\&\; Q(x)) \equiv (\forall x P(x) \;\&\; \forall x Q(x))$$
$$\exists x(P(x) \parallel Q(x)) \equiv (\exists x P(x) \parallel \exists x Q(x))$$

Man beachte, dass die Regeln der Quantorendualität intuitiv sehr einleuchtend sind, wenn wir uns die umgangssprachliche Bedeutung der Quantoren vor Augen halten. So kann leicht nachvollzogen werden, dass eine Aussage der Form $\sim\exists x P(x)$, also „Für kein x ist $P(x)$ wahr“, genau dasselbe bedeutet wie $\forall x \sim P(x)$, d. h. „Für alle x ist $P(x)$ falsch“. Ebenso ist es unmittelbar einleuchtend, dass $\sim\forall x P(x)$ bzw. „Nicht für alle x ist $P(x)$ wahr“ dieselbe Bedeutung haben muss wie $\exists x \sim P(x)$, also „Es gibt ein x, für das $P(x)$ falsch ist“.

Aufgaben

1.2.1 Analysieren Sie die logische Form der folgenden Aussagen und Aussageformen:
a) „x und y sind ganze Zahlen und x ist ein Teiler von y“.
b) „Ist x eine Primzahl, dann ist x nur durch 1 und sich selbst teilbar“.
c) „Jede ganze Zahl ist auch eine rationale Zahl, aber es gibt rationale Zahlen, die keine ganzen Zahlen sind“.
d) „Es gibt eine ganze Zahl, die kleiner ist als jede natürliche Zahl“.

1.2.2 Gegeben sei die Menge $M = \{1, 2, 3, 4, 5\}$. Entscheiden Sie für jede der folgenden Aussagen, ob diese wahr oder falsch ist, wenn davon ausgegangen wird, dass nur über die Menge M quantifiziert wird, dass also die Variablen als Werte nur die Elemente aus M annehmen können. Begründen Sie Ihre Antworten.
a) $\forall x \exists y (x = y)$.
b) $\exists x \forall y (x = y)$.
c) $\forall x \exists y \sim (x = y)$.
d) $\exists x \forall y \sim (x = y)$.

1.2.3 Statt die Elemente einer Menge einzeln anzugeben, können Mengen auch mit Hilfe von *Aussageformen* beschrieben werden. Ist $P(x)$ eine Aussageform, so schreibt man dabei $\{x \mid P(x)\}$ für die Menge aller Gegenstände x, für die $P(x)$ eine wahre Aussage ist. Benutzen Sie diese Schreibweise, um die folgenden Mengen zu charakterisieren:
a) Die *leere Menge* $\emptyset$, d. h. die Menge, die keine Elemente enthält.
b) Die *Schnittmenge* $A \cap B$ zweier Mengen A und B, also die Menge aller Gegenstände, die sowohl in A als auch in B liegen.
c) Die *Vereinigungsmenge* $A \cup B$ zweier Mengen A und B, d. h. die Menge aller Gegenstände, die in A oder in B liegen.
d) Die *Differenzmenge* $A - B$, d. h. die Menge aller Gegenstände, die in A, aber nicht in B liegen.

1.2.4 Benutzen Sie Ihre Definitionen der Mengen $\emptyset$, $A \cap B$ und $A \cup B$ aus der vorigen Aufgabe, um die folgenden Gleichungen zu beweisen:
a) $A \cap B = B \cap A$
b) $A \cup B = B \cup A$
c) $A \cap (B \cap C) = (A \cap B) \cap C$
d) $A \cup (B \cup C) = (A \cup B) \cup C$
e) $A \cap A = A$
f) $A \cup A = A$
g) $A \cap \emptyset = \emptyset$
h) $A \cup \emptyset = A$.

1.2.5 Eine Menge T heißt *Teilmenge* einer Menge A, falls jedes Element von T auch Element von A ist. Ist T eine Teilmenge von A, so schreibt man auch $T \subseteq A$.
a) Wie lässt sich die logische Form der Aussage $T \subseteq A$ analysieren? (Vgl. hierzu Punkt (2) aus Beispiel 1.2.2.)
b) Begründen Sie, warum die leere Menge Teilmenge jeder Menge ist.
c) Begründen Sie, warum jede Menge sich selbst als Teilmenge enthält.

d) Die *Potenzmenge* $\mathcal{P}(A)$ einer Menge A ist definiert als die Menge aller Teilmengen von A. Finden Sie eine Aussageform $P(x)$, so dass $\mathcal{P}(A) = \{x \mid P(x)\}$ gilt.

e) Nach dem sogenannten *Extensionalitätsaxiom* sind zwei Mengen A und B genau dann gleich, wenn sie genau dieselben Elemente besitzen. Formal lässt sich dieses Prinzip in der Form $A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B)$ ausdrücken. Nutzen Sie das Extensionalitätsaxiom, um zu zeigen, dass $A = B$ genau dann gilt, wenn sowohl $A \subseteq B$ als auch $B \subseteq A$ gilt.

1.2.6 In Satz 1.2.4 haben wir die Äquivalenzen $\forall x(P(x)\ \&\ Q(x)) \equiv (\forall x P(x)\ \&\ \forall x Q(x))$ und $\exists x(P(x) \parallel Q(x)) \equiv (\exists x P(x) \parallel \exists x Q(x))$ kennengelernt. Sind die folgenden Aussagen ebenfalls äquivalent?

a) $\forall x(P(x) \parallel Q(x))$ und $\forall x P(x) \parallel \forall x Q(x)$.

b) $\exists x(P(x)\ \&\ Q(x))$ und $\exists x P(x)\ \&\ \exists x Q(x)$.

Begründen Sie Ihre Antwort, indem Sie die Äquivalenz entweder mit Hilfe der Umformungsregeln für die Quantoren und die Aussageverknüpfungen nachweisen oder – im Falle der Nichtäquivalenz – konkrete Beispiele für Aussageformen $P(x)$ und $Q(x)$ sowie eine zugrundeliegende Menge M angeben, so dass jeweils die eine der beiden Aussagen wahr und die andere falsch ist, sofern davon ausgegangen wird, dass die Variablen nur Werte aus M annehmen können.

2 Mathematische Beweistechniken

Eine Aussage wird in der Mathematik erst dann als wahr anerkannt, wenn ein logisch korrekter Beweis für diese Aussage vorliegt. Dementsprechend besteht das Ziel mathematischer Untersuchungen in der Regel darin, Beweise für mathematische Aussagen zu finden. Obwohl solche Beweise sehr unterschiedlich sein können und es oft verschiedene Möglichkeiten gibt, ein und dieselbe Aussage zu beweisen, gibt es ein paar grundlegende Beweistechniken, denen in der mathematischen Praxis besonders große Bedeutung zukommt.

Zwei sehr wichtige dieser Verfahren beruhen auf der Beobachtung, dass die zu beweisenden Aussagen sehr oft von der Form $P \Rightarrow Q$ bzw. $\forall x(P(x) \Rightarrow Q(x))$ sind. Um eine solche Aussage zu beweisen, bieten sich unter anderem die folgenden Möglichkeiten:

- Die erste Möglichkeit besteht darin, von der Aussage P bzw. $P(x)$ für ein beliebiges x als Annahme auszugehen und dann zu versuchen, die Aussage Q bzw. $Q(x)$ aus dieser Annahme herzuleiten. Dieses Vorgehen entspricht einem *direkten Beweis* für die Aussage $P \Rightarrow Q$ bzw. $\forall x(P(x) \Rightarrow Q(x))$ und wird in Abschnitt 2.1 behandelt.

- Die zweite Möglichkeit beruht auf der Überlegung, dass wir eine Aussage der Form $P \Rightarrow Q$ bzw. $\forall x(P(x) \Rightarrow Q(x))$ auch logisch äquivalent in der Form $\sim Q \Rightarrow \sim P$ bzw. $\forall x(\sim Q(x) \Rightarrow \sim P(x))$ aufschreiben können (vgl. Satz 1.1.5). Statt also P bzw. $P(x)$ anzunehmen und daraus Q bzw. $Q(x)$ herzuleiten, könnte man alternativ auch $\sim Q$ bzw. $\sim Q(x)$ annehmen und daraus $\sim P$ bzw. $\sim P(x)$ folgern. Diese Strategie entspricht einem *Beweis durch Kontraposition* und wird in Abschnitt 2.2 erläutert.

Während direkte Beweise und Beweise durch Kontraposition allein für Aussagen der Form $P \Rightarrow Q$ bzw. $\forall x(P(x) \Rightarrow Q(x))$ genutzt werden können, stellt die Methode des *Widerspruchsbeweises* keine Anforderungen an die logische Form der zu beweisenden Aussage. Bei einem Widerspruchsbeweis wird eine Aussage P dadurch bewiesen, dass gezeigt wird, dass ihre Negation $\sim P$ auf einen Widerspruch führt. Die zugrunde liegende Idee ergibt sich dabei aus der Äquivalenz $P \equiv (\sim P \Rightarrow (Q \;\&\; \sim Q))$. Wir werden die Methode des Widerspruchsbeweises in Abschnitt 2.3 behandeln.

Neben direkten Beweisen, Beweisen durch Kontraposition und Widerspruchsbeweisen spielen schließlich auch die sogenannten *Induktionsbeweise* in der Mathematik und speziell auch in der Untersuchung logischer Systeme eine wichtige Rolle. Eng verwandt mit der Methode der mathematischen Induktion ist das Prinzip der *induktiven* (oder auch *rekursiven*) *Definition*. Wir werden Induktionsbeweise und induktive Definitionen in Abschnitt 2.4 behandeln.

2.1 Direkte Beweise

Bei einem *direkten Beweis* zeigt man die Wahrheit einer Aussage der Form $\forall x(P(x) \Rightarrow Q(x))$ bzw. $P \Rightarrow Q$, indem man zuerst annimmt, dass der vordere Teil der Implikation wahr ist, und anschließend folgert, dass dann auch der hintere Teil der Implikation gelten muss. Betrachten wir zur Veranschaulichung die folgende Aussage:

Lemma 2.1.1. Das Quadrat n^2 einer geraden Zahl n ist stets gerade.

Um herauszufinden, wie wir Lemma 2.1.1 beweisen können, müssen wir uns zunächst überlegen, wie die logische Struktur dieser Aussage zu interpretieren ist. Offensichtlich können wir Lemma 2.1.1 auch in der Form

Für alle n gilt: Wenn n eine gerade Zahl ist, dann ist n^2 eine gerade Zahl

aufschreiben. Wählen wir für $P(n)$ also die Aussageform „n ist eine gerade Zahl“, so hat die Aussage aus Lemma 2.1.1 die Struktur $\forall n(P(n) \Rightarrow P(n^2))$. Ferner sollten wir uns klarmachen, was man unter einer „geraden Zahl“ versteht. Üblicherweise legt man hier die folgende Definition zugrunde:

Definition 2.1.2 (Gerade und ungerade Zahlen)**.** Eine ganze Zahl $n \in \mathbb{Z}$ heißt *gerade*, falls es eine Zahl $k \in \mathbb{Z}$ gibt, so dass $n = 2k$ gilt. Eine ganze Zahl $n \in \mathbb{Z}$ heißt *ungerade*, falls n nicht gerade ist, d. h. falls $n = 2k + 1$ für ein $k \in \mathbb{Z}$ gilt.

Um einen direkten Beweis für Lemma 2.1.1 zu führen, müssen wir nun annehmen, dass der vordere Teil der Implikation wahr ist, dass also n in der Tat eine gerade Zahl ist. Da in Lemma 2.1.1 eine Aussage über *alle* geraden Zahlen gemacht wird, sollten wir „n“ dabei als Bezeichnung für eine *beliebige* derartige Zahl verwenden und dies auch sprachlich kennzeichnen, indem wir unseren Beweis mit einer Formulierung wie

Sei n eine beliebige gerade Zahl

beginnen. Um deutlich zu machen, dass es sich hierbei um eine *Annahme* handelt, hätten wir stattdessen auch eine Formulierung wie etwa „Wir nehmen an, n ist eine beliebige gerade Zahl“ wählen können. Da wir die Aussage aus Lemma 2.1.1 direkt beweisen wollen, müssen wir nun versuchen, den hinteren Teil der Implikation, also die Aussage „n^2 ist eine gerade Zahl“ aus dieser Annahme herzuleiten. Dazu bietet es sich an, zunächst einmal die Definition einer geraden Zahl zu nutzen und sich klarzumachen, was aus dieser in Bezug auf unsere Annahme, dass n eine gerade Zahl ist, folgt. Der zweite Schritt unseres Beweises für Lemma 2.1.1 könnte also wie folgt formuliert werden:

Es gibt eine Zahl $k \in \mathbb{Z}$, so dass $n = 2 \cdot k$ gilt.

Nun müssen wir uns fragen, was sich aus dieser Feststellung für das Quadrat von n ergibt, denn unser Ziel ist es ja, zu zeigen, dass n^2 eine gerade Zahl ist. Ist $n = 2 \cdot k$ für ein $k \in \mathbb{Z}$, so folgt daraus offenbar, dass $n^2 = n \cdot n = 2 \cdot k \cdot 2 \cdot k$ für ebendieses $k \in \mathbb{Z}$ gilt. Somit könnten wir als dritten Schritt die Aussage

Es ist $n^2 = 2 \cdot k \cdot 2 \cdot k$ für ein $k \in \mathbb{Z}$

aufschreiben. Um nun zu zeigen, dass n^2 bzw. $2 \cdot k \cdot 2 \cdot k$ ebenfalls gerade ist, müssen wir nach Definition 2.1.2 eine ganze Zahl $m \in \mathbb{Z}$ angeben, für die $n^2 = 2 \cdot m$ gilt. Dabei können wir uns die Tatsache zunutze machen, dass die Multiplikation über den ganzen Zahlen *assoziativ* ist, dass also ein Term der Form $2 \cdot k \cdot 2 \cdot k$ genau dasselbe bedeutet wie $2 \cdot (k \cdot 2 \cdot k)$. Setzen wir also $m := k \cdot 2 \cdot k$, so gilt offensichtlich $n^2 = 2 \cdot (k \cdot 2 \cdot k) = 2 \cdot m$ (das Zeichen „:=“ steht hierbei für die *Gleichheit per Definition*, eine Aussage der Form „$a := b$“ bedeutet also „a wird definiert als b“). Dies stellt den vierten Schritt unseres Beweises dar:

$$\text{Es gilt } n^2 = 2 \cdot m \text{ für } m = k \cdot 2 \cdot k.$$

Um deutlich zu machen, dass wir mit dieser Folgerung tatsächlich das Beweisziel erreicht haben und unser Beweis nun zu Ende ist, sollten wir in einem letzten Schritt noch einmal zusammenfassen, was wir aus unserer Annahme gefolgert haben. Wir könnten also unseren Beweis mit einem Satz der Art

$$\text{Folglich ist } n^2 \text{ eine gerade Zahl}$$

abschließen. Da wir n in unserem Beweis als Bezeichnung für eine *beliebige* gerade Zahl verwendet haben, ist damit nun in der Tat gezeigt, dass das Quadrat *jeder* geraden Zahl stets gerade ist. Beim endgültigen Aufschreiben von Beweisen versucht man, logische Abhängigkeiten zwischen Aussagen möglichst deutlich zu kennzeichnen, indem man die Ergebnisse der einzelnen Teilschitte durch Wörter wie „also“, „daher“, „somit“, „folglich“, „deshalb“ oder „daraus folgt“ miteinander verbindet und Begründungen für einzelne Aussagen explizit angibt (hierzu lassen sich Formulierungen wie „Da ... wahr ist, gilt ...“ oder auch „Weil ... gilt, ist ... wahr“ verwenden). Den kompletten Beweis für Lemma 2.1.1 können wir kompakt in der folgenden Form aufschreiben:

Beweis zu Lemma 2.1.1. Sei n eine beliebige gerade Zahl, d. h. es gilt $n = 2 \cdot k$ für ein $k \in \mathbb{Z}$. Dann ist $n^2 = 2 \cdot k \cdot 2 \cdot k = 2 \cdot (k \cdot 2 \cdot k)$. Für $m := k \cdot 2 \cdot k$ gilt somit $n^2 = 2 \cdot m$. Folglich ist n^2 eine gerade Zahl. □

Um das hier zum Tragen kommende Vorgehen noch klarer zu machen, wollen wir ein weiteres Beispiel für einen direkten Beweis angeben. Betrachten wir die folgende Aussage:

Lemma 2.1.3. Die Summe dreier aufeinanderfolgender ganzer Zahlen ist immer durch 3 teilbar.

Zunächst sollten wir uns wieder überlegen, wie die logische Struktur dieser Aussage zu verstehen ist. Offensichtlich können wir Lemma 2.1.3 auch in der folgenden Form ausdrücken:

$$\text{Für alle } n \text{ gilt: Wenn } n \in \mathbb{Z}, \text{ dann ist } n + (n+1) + (n+2) \text{ durch 3 teilbar.}$$

Nun sollten wir uns fragen, was gemeint ist, wenn man sagt, dass eine Zahl „durch 3 teilbar“ ist. Hier wird in der Regel die folgende Definition verwendet:

Definition 2.1.4 (Teiler)**.** Seien $a, b \in \mathbb{Z}$ ganze Zahlen. Die Zahl a ist ein *Teiler* von b, falls es eine ganze Zahl $k \in \mathbb{Z}$ gibt, so dass $b = a \cdot k$ ist. Ist a ein Teiler von b, so schreibt man $a \mid b$ und spricht auch davon, dass b durch a *teilbar* ist.

Eine Zahl m ist somit durch 3 teilbar, wenn $m = 3 \cdot k$ für eine ganze Zahl $k \in \mathbb{Z}$ gilt. Um nun die Behauptung aus Lemma 2.1.3 per direktem Beweis zu zeigen, sollten wir wieder den vorderen Teil der Implikation als Annahme voraussetzen und anschließend den hinteren Teil aus dieser Annahme herleiten. Nehmen wir also zunächst an, dass $n \in \mathbb{Z}$ eine beliebige ganze Zahl ist. Durch Zusammenfassen der Summe $n + (n + 1) + (n + 2)$ erhalten wir $n + (n + 1) + (n + 2) = 3 \cdot n + 3$. Da wir zeigen wollen, dass $n + (n + 1) + (n + 2)$ bzw. $3 \cdot n + 3$ durch drei teilbar ist, sollten wir nun versuchen, eine Zahl $k \in \mathbb{Z}$ zu finden, für die $n + (n + 1) + (n + 2) = 3 \cdot k$ gilt. Wie sich leicht erkennen lässt, können wir in dem Term $3 \cdot n + 3 = 3 \cdot n + 3 \cdot 1$ den gemeinsamen Faktor 3 ausklammern. Auf diese Weise erhalten wir die Gleichung $3 \cdot n + 3 = 3 \cdot (n + 1)$. Setzen wir also $k := n + 1$, so gilt offensichtlich $n + (n + 1) + (n + 2) = 3 \cdot n + 3 = 3 \cdot (n + 1) = 3 \cdot k$, womit gezeigt ist, dass $n + (n + 1) + (n + 2)$ durch 3 teilbar ist. Zusammengefasst lässt sich dieser Beweis wie folgt aufschreiben:

Beweis zu Lemma 2.1.3. Wir nehmen an, $n \in \mathbb{Z}$ ist eine beliebige ganze Zahl. Dann gilt $n + (n + 1) + (n + 2) = 3 \cdot n + 3 = 3 \cdot (n + 1)$. Für die ganze Zahl $k := n + 1$ erhalten wir also $n + (n + 1) + (n + 2) = 3 \cdot k$. Folglich gilt $3 \mid n + (n + 1) + (n + 2)$, d. h. $n + (n + 1) + (n + 2)$ ist durch 3 teilbar. □

Aufgaben

2.1.1 Geben Sie direkte Beweise für die folgenden Aussagen an:
a) Das Quadrat n^2 einer ungeraden Zahl ist stets ungerade.
b) Die Summe zweier ungerader Zahlen ist stets gerade.
c) Ist a ein Teiler von b und b ein Teiler von c, so ist a auch ein Teiler von c.
d) Die Summe zweier benachbarter ungerader Zahlen ist durch 4 teilbar. (Zwei ungerade Zahlen heißen dabei *benachbart*, falls zwischen ihnen nur eine einzige weitere ganze Zahl liegt, die dann selbstverständlich gerade ist.)
e) Jede ganze Zahl, deren letzte Dezimalstelle eine 5 ist, ist durch 5 teilbar.

2.1.2 Finden Sie einen direkten Beweis für die folgende Behauptung: Für alle rationalen Zahlen $a, b \in \mathbb{Q}$ mit $a < b$ gibt es eine weitere rationale Zahl $c \in \mathbb{Q}$, so dass $a < c < b$.

2.1.3 Der *Binomialkoeffizient* $\binom{n}{k}$ zweier natürlicher Zahlen $n, k \in \mathbb{N}$ mit $k \leq n$ ist definiert als die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge. Er kann mit Hilfe der Formel

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$$

berechnet werden. Dabei steht $m!$ für die *Fakultät* einer natürlichen Zahl $m \in \mathbb{N}$, also für das Produkt aller ganzen Zahlen von 1 bis m, d. h. es gilt $m! := 1 \cdot 2 \cdot \ldots \cdot m$. Für den Spezialfall $m = 0$ wird dabei $m! := 1$ gesetzt. Geben Sie direkte Beweise für die folgenden Behauptungen an (n und k sind jeweils beliebige natürliche Zahlen mit $k \leq n$):
a) $\binom{n}{k} = \binom{n}{n-k}$.
b) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

2.2 Beweise durch Kontraposition

Bei einem *Beweis durch Kontraposition* beweist man eine Aussage der Form $\forall x(P(x) \Rightarrow Q(x))$ bzw. $P \Rightarrow Q$, indem man zunächst annimmt, dass der hintere Teil der Implikation falsch ist, und anschließend folgert, dass dann auch der vordere Teil der Implikation falsch sein muss. Die Rechtfertigung für dieses Vorgehen ergibt sich aus der Äquivalenz $(P \Rightarrow Q) \equiv (\sim Q \Rightarrow \sim P)$ bzw. $\forall x(P(x) \Rightarrow Q(x)) \equiv \forall x(\sim Q(x) \Rightarrow \sim P(x))$ (vgl. Satz 1.1.5). Statt also eine Aussage der Form $\forall x(P(x) \Rightarrow Q(x))$ direkt zu beweisen, können wir auch zeigen, dass die äquivalente und unter Umständen leichter zu beweisende Aussage $\forall x(\sim Q(x) \Rightarrow \sim P(x))$ wahr ist. Wir betrachten das folgende Beispiel:

Lemma 2.2.1. Sei $n \in \mathbb{Z}$. Wenn n^2 eine gerade Zahl ist, dann ist auch n gerade.

Wie sich leicht erkennen lässt, handelt es sich bei dieser Aussage um die Umkehrung der Aussage aus Lemma 2.1.1, denn wir können Lemma 2.2.1 auch in der Form

Für alle $n \in \mathbb{Z}$ gilt: Wenn n^2 eine gerade Zahl ist, dann ist n eine gerade Zahl

aufschreiben. Wegen der Äquivalenz $\forall x(P(x) \Rightarrow Q(x)) \equiv \forall x(\sim Q(x) \Rightarrow \sim P(x))$ ist diese Aussage nun gleichbedeutend mit

Für alle $n \in \mathbb{Z}$ gilt: Wenn n nicht gerade ist, dann ist n^2 nicht gerade.

Um Lemma 2.2.1 zu beweisen, können wir also annehmen, dass n eine beliebige ungerade Zahl ist, und dann daraus folgern, dass n^2 ebenfalls ungerade sein muss. Der erste Schritt unseres Beweises besteht somit aus folgender Annahme:

Wir nehmen an, n ist eine beliebige ungerade Zahl.

Mit Hilfe der Definition einer ungeraden Zahl ergibt sich daraus die Behauptung

Es gibt eine ganze Zahl $k \in \mathbb{Z}$, so dass $n = 2k + 1$.

Für das Quadrat n^2 von n folgt hieraus die Aussage

$$\text{Es gilt } n^2 = (2k + 1) \cdot (2k + 1) = 4k^2 + 4k + 1.$$

Durch Ausklammern von 2 erhalten wir $4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1$. Es gilt also

$$n^2 = 2 \cdot (2k^2 + 2k) + 1.$$

Für die ganze Zahl $m := 2k^2 + 2k$ ergibt sich folglich

$$n^2 = 2m + 1,$$

womit wir gezeigt haben, dass n^2 ungerade ist. Den kompletten Beweis können wir noch einmal in der folgenden Form aufschreiben:

Beweis zu Lemma 2.2.1. Wir zeigen die Kontraposition: Wenn n ungerade ist, dann ist n^2 ungerade. Sei $n \in \mathbb{Z}$ eine beliebige ungerade Zahl. Dann gibt es ein $k \in \mathbb{Z}$, so dass $n = 2k+1$ gilt. Somit ist $n^2 = (2k+1) \cdot (2k+1) = 4k^2+4k+1 = 2 \cdot (2k^2+2k)+1$. Für die ganze Zahl $m := 2k^2 + 2k$ erhalten wir also $n^2 = 2m + 1$. Folglich ist n^2 ungerade. □

Wie zu sehen ist, weisen wir in der endgültigen Fassung unseres Beweises noch einmal ausdrücklich darauf hin, dass wir die Kontraposition von Lemma 2.2.1 beweisen. Derartige „Regieanweisungen“ sind oft sehr nützlich, um das Lesen mathematischer Beweise zu erleichtern, denn durch sie kann die logische Struktur des Beweises schneller erkannt und die zugrunde liegende Beweisidee besser nachvollzogen werden.

Da es sich bei Lemma 2.2.1 um die Umkehrung der Aussage aus Lemma 2.1.1 handelt, haben wir nun zusammengenommen die folgende Aussage bewiesen:

Lemma 2.2.2. Eine Zahl $n \in \mathbb{Z}$ ist genau dann gerade, wenn n^2 gerade ist.

Man beachte, dass Lemma 2.2.2 die Form $\forall x(P(x) \Leftrightarrow Q(x))$ hat und dass wir diese Aussage vermöge der Äquivalenz $\forall x(P(x) \Leftrightarrow Q(x)) \equiv \forall x(P(x) \Rightarrow Q(x))$ & $\forall x(Q(x) \Rightarrow P(x))$ auch in der Form

Für alle $n \in \mathbb{Z}$ gilt: Wenn n gerade ist, dann ist n^2 gerade
und
Für alle $n \in \mathbb{Z}$ gilt: Wenn n^2 gerade ist, dann ist n gerade

ausdrücken können. Da das erste Glied der Konjunktion der Aussage aus Lemma 2.1.1 entspricht und wir das zweite Glied mit Lemma 2.2.1 bewiesen haben, können wir uns beim Beweis zu Lemma 2.2.2 einfach auf diese bereits bewiesenen Resultate berufen. Welches Lemma für welche Richtung der Äquivalenz zuständig ist, wird dabei oft durch die Symbole „$\Rightarrow$“ und „$\Leftarrow$“ kenntlich gemacht.

Beweis zu Lemma 2.2.2.
„$\Rightarrow$“: Nach Lemma 2.1.1.
„$\Leftarrow$“: Nach Lemma 2.2.1. □

Aufgaben

2.2.1 Beweisen Sie die folgenden Aussagen durch Kontraposition:

a) Seien $a, b, c \in \mathbb{Z}$ ganze Zahlen mit $a \neq b$. Dann gilt $a + c \neq b + c$.
b) Seien $a, b \in \mathbb{Z}$, so dass $a + b$ und $a - b$ teilerfremd sind. Dann sind auch a und b teilerfremd. (Zwei Zahlen $a, b \in \mathbb{Z}$ heißen dabei *teilerfremd*, wenn es keine Zahl $c \in \mathbb{Z}$ gibt mit $c \neq 1$, $c \mid a$ und $c \mid b$).
c) Sei $n \in \mathbb{Z}$. Wenn n^2 bei der Division durch 3 nicht den Rest 1 lässt, dann lässt auch n bei der Division durch 3 nicht den Rest 1.
d) Seien $m, n \in \mathbb{Z}$. Wenn $t \mid m$ für alle Teiler t von n gilt, dann gilt $n \mid m$.
e) Wenn eine Zahl $n \in \mathbb{Z}$ nicht durch 2 oder 5 teilbar ist, dann ist sie auch nicht durch 10 teilbar.
f) Sei $n \in \mathbb{Z}$. Wenn n^2 nicht durch 4 teilbar ist, dann lässt n bei Division durch 4 nicht den Rest 2.
g) Seien $n, m, t \in \mathbb{Z}$ ganze Zahlen. Wenn t kein Teiler von $n + m$ ist, dann ist t kein Teiler von n oder kein Teiler von m.
h) Seien $a, b \in \mathbb{Z}$. Ist $a + b$ ungerade, dann ist eine der Zahlen a und b gerade und die andere ungerade.

2.3 Widerspruchsbeweise

Bei einem *Widerspruchsbeweis* beweist man eine Aussage P, indem man aus der Negation von P einen Widerspruch herleitet. Dass damit tatsächlich gezeigt werden kann, dass die zu beweisende Aussage wahr ist, ergibt sich aus der Äquivalenz $P \equiv (\sim P \Rightarrow (Q \ \& \ \sim Q))$ (eine Aussage P ist genau dann wahr, wenn aus ihrer Negation ein Widerspruch folgt). Wir wollen das Prinzip des Widerspruchsbeweises an folgendem Beispiel verdeutlichen:

Lemma 2.3.1. Sind $a, b \in \mathbb{Z}$ gerade Zahlen, dann ist auch das Produkt $a \cdot b$ gerade.

Offensichtlich können wir Lemma 2.3.1 auch in der Form

Für alle a und b gilt: Wenn a und b gerade Zahlen sind, dann ist $a \cdot b$ eine gerade Zahl

aufschreiben. Um per Widerspruchsbeweis zu zeigen, dass diese Aussage gilt, müssen wir ihre Negation annehmen und daraus einen Widerspruch herleiten. Wie man sich leicht mit Hilfe der in Satz 1.1.5 und 1.2.4 genannten Äquivalenzen vergewissern kann, ist die Negation von Lemma 2.3.1 äquivalent zu der Aussage

Es gibt a und b, so dass gilt: a und b sind gerade Zahlen und $a \cdot b$ ist keine gerade Zahl.

Um Lemma 2.3.1 zu beweisen, nehmen wir also an, dass es gerade Zahlen a und b gibt, deren Produkt $a \cdot b$ *keine* gerade Zahl, also ungerade ist. Da die Zahl a gerade ist, gibt es laut Definition ein $k \in \mathbb{Z}$, so dass $a = 2k$ gilt. Daraus folgt für das Produkt von a und b:

$$a \cdot b = 2k \cdot b = 2 \cdot (k \cdot b) = 2n \text{ für } n := k \cdot b,$$

d. h. das Produkt $a \cdot b$ ist eine gerade Zahl. Damit haben wir bereits den herzuleitenden Widerspruch gefunden, denn laut unserer Annahme ist $a \cdot b$ ungerade. Weil wir diesen Widerspruch aus der Annahme hergeleitet haben, dass Lemma 2.3.1 falsch ist, folgt nun, dass diese Annahme selbst falsch sein muss, also die Aussage

Für alle a und b gilt: Wenn a und b gerade Zahlen sind, dann ist $a \cdot b$ eine gerade Zahl

wahr ist. Unser Beweis zu Lemma 2.3.1 ist damit abgeschlossen. Zusammenfassend können wir ihn noch einmal in der folgenden Form aufschreiben:

Beweis zu Lemma 2.3.1. Wir führen einen Widerspruchsbeweis. Angenommen, es gibt gerade Zahlen a und b, so dass das Produkt $a \cdot b$ ungerade ist. Da a eine gerade Zahl ist, gibt es eine ganze Zahl $k \in \mathbb{Z}$, so dass $a = 2k$. Daraus ergibt sich $a \cdot b = 2k \cdot b = 2 \cdot (k \cdot b)$. Für $n := k \cdot b$ gilt folglich $a \cdot b = 2n$, d. h. $a \cdot b$ ist eine gerade Zahl. Dies ist ein Widerspruch, denn nach unserer Annahme ist $a \cdot b$ ungerade. □

Aufgaben

2.3.1 Geben Sie Widerspruchsbeweise für die folgenden Aussagen:
a) Wenn die Wurzel einer geraden natürlichen Zahl n selbst eine natürliche Zahl ist, dann ist die Wurzel gerade.
b) Wenn n^3 eine gerade Zahl ist, dann ist auch n gerade.
c) Sei $n \in \mathbb{N}$ und p eine Primzahl. Gilt $p \mid n^2$, dann gilt auch $p \mid n$. Sie dürfen für den Beweis die folgende Aussage benutzen (ein Spezialfall des Lemmas von Bézout): Besitzen zwei Zahlen $a, b \in \mathbb{Z}$ außer 1 keinen gemeinsamen Teiler, dann gibt es Zahlen $s, t \in \mathbb{Z}$, so dass $1 = sa + tb$ gilt.

2.3.2 Eine reelle Zahl x heißt *irrational*, wenn sie nicht rational ist, d. h. wenn es keine ganzen Zahlen $m, n \in \mathbb{Z}$ gibt, so dass $x = \frac{m}{n}$ gilt. Zeigen Sie, dass $\sqrt{2}$ eine irrationale Zahl ist. Führen Sie hierzu einen Widerspruchsbeweis.

2.3.3 Zeigen Sie per Widerspruchsbeweis die folgende Verallgemeinerung der Aussage aus Aufgabe 2.3.2: Für jede Primzahl $p \in \mathbb{P}$ ist $\sqrt{p}$ irrational.

2.3.4 Führen Sie einen Widerspruchsbeweis für die folgende Aussage: Jede natürliche Zahl $n \in \mathbb{Z}$ mit $n \geq 2$ kann als Produkt von Primzahlen geschrieben werden, d. h. für jede solche Zahl n gibt es Primzahlen $p_1, p_2, \ldots, p_m \in \mathbb{P}$, so dass

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$$

gilt für natürliche Zahlen $k_1, \ldots, k_m \in \mathbb{N}$ mit $k_i \geq 1$ für alle $1 \leq i \leq m$.

2.3.5 Zeigen Sie per Widerspruchsbeweis, dass es unendlich viele Primzahlen gibt. Sie können hierfür Aufgabe 2.3.4 nutzen.

2.4 Induktionsbeweise

Ein in vielen Fällen sehr leistungsstarkes Werkzeug ist die Beweismethode der *mathematischen Induktion*. Induktionsbeweise spielen in sehr unterschiedlichen mathematischen Zusammenhängen eine wichtige Rolle und werden dazu verwendet, Aussagen für alle Elemente einer vorgegebenen Menge zu beweisen. Dabei ist es im Grunde unwesentlich, ob es sich bei den Elementen der Menge um Zahlen oder um sonstige Objekte handelt – entscheidend für die Anwendbarkeit induktiver Beweistechniken ist vielmehr, dass sich die Objekte, über die man eine Aussage beweisen möchte, *induktiv* definieren oder beschreiben lassen. Bevor wir uns also den induktiven Beweisverfahren zuwenden, wollen wir uns zunächst mit den Grundlagen induktiver Definitionen vertraut machen.

2.4.1 Induktive Mengendefinitionen

Bei der *induktiven* oder *rekursiven Definition* einer Menge wird zunächst angegeben, welche Grundobjekte zu der Menge gehören, und anschließend beschrieben, wie man alle anderen Elemente der Menge schrittweise aus diesen Grundobjekten erzeugen kann. Eine induktive Definition einer Menge M besteht also im Allgemeinen aus den folgenden beiden Schritten:

(1) Man legt zunächst fest, dass gewisse Basisobjekte $x_1, x_2, \ldots$ in der Menge M liegen sollen,
(2) Man gibt an, nach welchen Regeln sich die anderen Elemente von M aus den Basisobjekten $x_1, x_2, \ldots$ erzeugen lassen.

Um diese recht abstrakt klingende Erläuterung ein wenig zu veranschaulichen und zu zeigen, wie diese beiden Schritte im Einzelfall aussehen können, wollen wir nun eine induktive Definition für die Menge $G = \{0, 2, 4, 6, \ldots\}$, also für die Menge der geraden natürlichen Zahlen entwickeln.

Zunächst müssen wir eines oder mehrere Basisobjekte angeben, aus denen sich durch Anwendung geeigneter Regeln alle anderen Elemente von G erzeugen lassen. Wir sollten uns zu diesem Zweck die Frage stellen, nach welchen Bildungs- oder Erzeugungsregeln man aus einer gegebenen geraden Zahl weitere gerade Zahlen gewinnen kann, um so zu entscheiden, welche Basisobjekte wir für unsere induktive Definition benötigen. Wie man leicht sehen kann, liegt zwischen zwei aufeinander folgenden geraden Zahlen immer genau eine weitere Zahl (die dann natürlich ungerade ist). Ist n also eine gerade Zahl, so erhält man die nächstgrößere gerade Zahl durch Addition von 2 aus n. Daraus ergibt sich das allgemeine Schema

$$\begin{aligned} 0 &= 0 \\ 2 &= 0 + 2 \\ 4 &= 0 + 2 + 2 \\ 6 &= 0 + 2 + 2 + 2 \\ &\vdots \\ 2k &= 0 + \underbrace{2 + \ldots + 2}_{k \text{ mal}} \end{aligned}$$

Wie dieses Schema zeigt, können wir alle geraden natürlichen Zahlen durch wiederholte Addition von 2 aus der Zahl 0 erzeugen. Es bietet sich bei der induktiven Definition der Menge G also an, als Basisobjekt zunächst die Zahl 0 festzulegen und anschließend die Erzeugungsregel

Wenn n eine gerade natürliche Zahl ist, dann ist auch $n + 2$ eine gerade natürliche Zahl

anzugeben. Es ist an dieser Stelle von Vorteil, sich noch einmal genau zu überlegen, wie sich mit Hilfe dieser Regel die geraden natürlichen Zahlen aus dem Basisobjekt 0 erzeugen lassen. Wenden wir unsere Erzeugungsregel im ersten Schritt auf das Basisobjekt 0 an, so erhalten wir die Zahl $0 + 2$, also 2. Nun können wir die Erzeugungsregel ein zweites Mal anwenden, diesmal allerdings auf das Ergebnis des ersten Schrittes, also auf die Zahl 2. Auf diese Weise erhalten wir die Zahl $2 + 2$, d. h. 4. Setzen wir diese Prozedur fort, so kommen wir im dritten Schritt auf $4 + 2$ (also auf 6), im vierten auf $6 + 2$ (also auf 8) usw. Wie sich leicht nachvollziehen lässt, kann auf diese Weise tatsächlich jede gerade natürliche Zahl erreicht werden.

Unser induktive Definition für die Menge G können wir in der folgenden Form aufschreiben:

Definition 2.4.1 (Die Menge der geraden natürlichen Zahlen)**.** Die Menge G der geraden natürlichen Zahlen wird induktiv definiert durch:

(1) 0 ist eine gerade natürliche Zahl, d. h. $0 \in G$,
(2) Wenn die Zahl n in G liegt, dann liegt auch $n + 2$ in G.

Um die Funktionsweise induktiver Definitionen noch ein wenig deutlicher zu machen, wollen wir ein weiteres Beispiel betrachten und eine induktive Definition für die Menge aller Zweierpotenzen entwickeln. Unter einer Zweierpotenz verstehen wir dabei eine Zahl, die sich in der Form 2^n für ein $n \in \mathbb{N}$ schreiben lässt. Die Menge aller Zweierpotenzen soll mit Z bezeichnet werden und ist die Menge $Z = \{2^n \mid n \in \mathbb{N}\} = \{1, 2, 4, 8, 16, \ldots\}$.

Überlegen wir uns zunächst, nach welchen allgemeinen Erzeugungsregeln die Zweierpotenzen gebildet werden können. Ist uns eine Zweierpotenz 2^n gegeben, so können wir offensichtlich immer die nächstgrößere Zweierpotenz erreichen, indem wir 2^n mit 2 multiplizieren und so den Exponenten um 1 erhöhen. Im Allgemeinen folgen die Zweierpotenzen also dem folgenden Muster:

$$\begin{aligned} 2^0 &= 1 \\ 2^1 &= 1 \cdot 2 \\ 2^2 &= 1 \cdot 2 \cdot 2 \\ 2^3 &= 1 \cdot 2 \cdot 2 \cdot 2 \\ &\vdots \\ 2^k &= 1 \cdot \underbrace{2 \cdot \ldots \cdot 2}_{k \text{ mal}} \end{aligned}$$

Offensichtlich lässt sich somit jede Zweierpotenz durch wiederholte Multiplikation mit 2 aus der Zahl 1 erzeugen. Um die Menge Z der Zweierpotenzen induktiv zu definieren, können wir also zunächst festlegen, dass das Basiselement 1 in Z liegen soll, und anschließend die Erzeugungsregel

Wenn n in Z liegt, dann liegt auch $n \cdot 2$ in Z

angeben. Wir erhalten auf diese Weise die folgende induktive Definition für Z:

Definition 2.4.2 (Die Menge der Zweierpotenzen)**.** Die Menge Z aller Zweierpotenzen wird induktiv definiert durch:
(1) Die Zahl 1 ist eine Zweierpotenz, d. h. es gilt $1 \in Z$,
(2) Wenn eine Zahl n in Z liegt, dann liegt auch $n \cdot 2$ in Z.

Es ist ratsam, sich auch in diesem Fall noch einmal klarzumachen, wie unsere induktive Definition der Menge Z genau funktioniert und wie die Zweierpotenzen mit Hilfe der Erzeugungsregel in Punkt (2) aus dem Basiselement 1 gewonnen werden können.

Der aufmerksame Leser dürfte bemerkt haben, dass sich das Prinzip induktiver Definitionen keineswegs auf Mengen wie G und Z beschränkt, sondern auch auf die natürlichen Zahlen selbst übertragen werden kann. Statt also lediglich Teilmengen der natürlichen Zahlen nach dieser Methode zu definieren, können wir auch die Menge $\mathbb{N}$ induktiv beschreiben. Betrachten wir die Folge $0, 1, 2, 3, 4, \ldots$, so fällt auf, dass sich jede natürliche Zahl durch wiederholte Addition von 1 aus dem Basiselement 0

erzeugen lässt. Der Aufbau der natürlichen Zahlen folgt somit dem folgenden Schema:

$$\begin{aligned} 1 &= 0 + 1 \\ 2 &= 0 + 1 + 1 \\ 3 &= 0 + 1 + 1 + 1 \\ &\vdots \\ n &= 0 + \underbrace{1 + \ldots + 1}_{n \text{ mal}} \end{aligned}$$

Wollen wir die Menge der natürlichen Zahlen induktiv beschreiben, so können wir zunächst das Basiselement 0 angeben und anschließend festlegen, dass man alle anderen Elemente nach der Regel

$$\text{Wenn } n \in \mathbb{N}, \text{ dann } n + 1 \in \mathbb{N}$$

erzeugen kann. Für die Menge $\mathbb{N}$ der natürlichen Zahlen erhalten wir auf diese Weise die folgende induktive Charakterisierung:
(1) 0 ist eine natürliche Zahl,
(2) Wenn n eine natürliche Zahl ist, dann ist auch $n + 1$ eine natürliche Zahl.

Die besondere Bedeutung induktiver Definitionen besteht darin, dass sie das Führen *induktiver Beweise* ermöglichen, mit denen man auf elegante und einfache Weise zeigen kann, dass alle Elemente einer induktiv definierten Menge eine bestimmte Aussageform erfüllen. Grundsätzlich gilt dabei, dass man mit der induktiven Definition einer Menge immer bereits ein passendes induktives Beweisprinzip „mitgeliefert" bekommt. So stellt etwa der induktive Aufbau der natürlichen Zahlen sicher, dass wir induktive Beweise über die Menge der natürlichen Zahlen führen können. Da sich jedoch nicht nur Zahlen, sondern auch andere Objekte wie etwa Funktionen, Graphen oder formale Sprachen induktiv definieren lassen, ist das Konzept der mathematischen Induktion keineswegs auf Zahlenmengen beschränkt. Im folgenden Abschnitt soll das Grundprinzip induktiver Beweise zunächst am Beispiel der natürlichen Zahlen verdeutlicht werden. In Abschnitt 2.4.3 werden wir dann eine weitere Form induktiver Beweise kennenlernen, die in ähnlicher Form auch bei der Untersuchung logischer Systeme eine wichtige Rolle spielt.

2.4.2 Induktion über die natürlichen Zahlen

Die Technik der *Induktion über die natürlichen Zahlen* wird verwendet, um zu beweisen, dass alle natürlichen Zahlen $n \in \mathbb{N}$ eine bestimmte Aussageform $P(n)$ erfüllen. Die dieser Beweistechnik zugrunde liegende Idee lässt sich allgemein wie folgt beschreiben: Um zu beweisen, dass $P(n)$ für alle $n \in \mathbb{N}$ wahr ist, muss gezeigt werden, dass die unendlich vielen Aussagen

$$P(0), P(1), P(2), P(3), P(4), \ldots$$

alle wahr sind. Oft erreicht man dies dadurch, dass man $P(n)$ für ein *beliebiges* $n \in \mathbb{N}$ beweist und etwas Ähnliches haben wir in den Abschnitten 2.1–2.3 gemacht als wir

Aussagen für *alle* geraden bzw. ungeraden Zahlen dadurch bewiesen haben, dass wir gezeigt haben, dass sie für eine *beliebige* gerade bzw. ungerade Zahl wahr sind. In vielen Fällen ist dieses Vorgehen jedoch äußerst umständlich und nicht selten kommt man auf diese Weise auch gar nicht zum Ziel.

Bei einem Induktionsbeweis wird stattdessen die Tatsache ausgenutzt, dass sich jede natürliche Zahl durch wiederholte Addition von 1 aus dem Startelement 0 erzeugen lässt, dass also die Menge $\mathbb{N}$, wie wir im letzten Abschnitt gesehen haben, induktiv durch die folgenden beiden Bedingungen beschrieben werden kann:
(1) 0 ist eine natürliche Zahl,
(2) Wenn n eine natürliche Zahl ist, dass ist auch $n+1$ eine natürliche Zahl.
Um also zu zeigen, dass für jede natürliche Zahl $n \in \mathbb{N}$ eine Aussage $P(n)$ gilt, ist es hinreichend, zu beweisen, dass die Aussage für das Basiselement 0 gilt und dass sie, wenn sie für eine natürliche Zahl k gilt, immer auch für deren Nachfolger $k+1$ gelten muss. Auf diese Weise wird sichergestellt, dass die Aussage $P(n)$ tatsächlich für *jede* natürliche Zahl wahr ist, denn gilt $P(0)$ und folgt für jede natürliche Zahl k aus $P(k)$ immer auch $P(k+1)$, so ergibt sich die Wahrheit der allgemeinen Aussage $\forall n \in \mathbb{N}\, P(n)$ aufgrund des entstehenden „Dominoeffekts“: Da $P(0)$ wahr ist, ist auch $P(1)$ wahr, da $P(1)$ wahr ist, ist auch $P(2)$ wahr usw. Insgesamt folgt, dass die unendlich vielen Aussagen

$$P(0), P(1), P(2), P(3), P(4), \ldots$$

tatsächlich alle wahr sind, dass also $P(n)$ für alle $n \in \mathbb{N}$ gilt.

Ebendiese Überlegung liegt dem Beweisprinzip der Induktion über die natürlichen Zahlen zugrunde: Will man beweisen, dass $P(n)$ für jedes $n \in \mathbb{N}$ wahr ist, so zeigt man zunächst, dass $P(0)$ wahr ist und beweist dann, dass für jedes $k \in \mathbb{N}$ die Implikation $P(k) \Rightarrow P(k+1)$ gilt. Insgesamt müssen bei dieser Beweismethode also die folgenden beiden Aussagen bewiesen werden:

(1) $P(0)$,
(2) $\forall k \in \mathbb{N}\,(P(k) \Rightarrow P(k+1))$.

Der erste Teil eines solchen Induktionsbeweises, der Beweis von $P(0)$, wird als *Induktionsanfang* bezeichnet. Den zweiten Teil, der Beweis von $\forall k \in \mathbb{N}\,(P(k) \Rightarrow P(k+1))$, bezeichnet man als *Induktionsschritt*. Im Induktionsschritt wird angenommen, dass $P(k)$ für ein *beliebiges* $k \in \mathbb{N}$ wahr ist und dann gezeigt, dass unter dieser Voraussetzung auch $P(k+1)$ gelten muss. Folglich besteht der Induktionsschritt selbst wiederum aus zwei Teilen: Der erste Teil, die Annahme, dass $P(k)$ für beliebiges $k \in \mathbb{N}$ wahr ist, wird als *Induktionsvoraussetzung* bezeichnet. Im zweiten Teil, dem *Induktionsschluss*, leitet man dann aus der Induktionsvoraussetzung die Aussage $P(k+1)$ her (dieser zweite Teil wird manchmal etwas irreführend ebenfalls als „Induktionsbeweis“ bezeichnet; wir benutzen den Namen „Induktionsbeweis“ hier jedoch nur für den kompletten Beweis bestehend aus dem Induktionsanfang und dem Induktionsschritt). Ein induktiver Beweis über die natürlichen Zahlen folgt also normalerweise dem folgenden Grundschema:

Um eine Aussage der Form $\forall n \in \mathbb{N}\, P(n)$ zu beweisen, genügt es, die folgenden Schritte abzuarbeiten:

(1) **Induktionsanfang:** Man beweist, dass die Aussage $P(0)$ gilt.

(2) **Induktionsschritt:**

  (2.1) *Induktionsvoraussetzung:* Man nimmt an, dass die Aussage $P(k)$ für ein beliebiges $k \geq 0$ wahr ist.

  (2.2) *Induktionsschluss:* Man beweist mit Hilfe der Induktionsvoraussetzung, dass die Aussage auch für den Nachfolger von k gilt, dass also $P(k+1)$ ebenfalls wahr ist.

Bevor wir uns einigen Abwandlungen dieses Grundschemas zuwenden, wollen wir die Beweistechnik der Induktion über die natürlichen Zahlen an einem Beispiel verdeutlichen und einen induktiven Beweis für die folgende Aussage führen:

Lemma 2.4.3 (Gausssche Summenformel)**.** Für alle $n \in \mathbb{N}$ gilt

$$0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

In Worten besagt Lemma 2.4.3, dass die Summe der natürlichen Zahlen von 0 bis n immer

$$\frac{n(n+1)}{2}$$

entspricht. Um einen Induktionsbeweis für diese Behauptung zu finden, können wir uns an obigem Grundschema orientieren und uns zunächst überlegen, welche Aussagen wir in den einzelnen Schritten zu beweisen haben und wie wir dabei vorgehen können.

(1) **Induktionsanfang:** Im ersten Schritt, dem Induktionsanfang, müssen wir zeigen, dass die Aussage für das Startelement 0 gilt. In unserem Beispiel hat die zu beweisende Aussage die Form

$$0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

und im Fall $n = 0$ bedeutet dies nichts anderes als

$$0 = \frac{0 \cdot (0+1)}{2}.$$

Da es sich hierbei um eine offensichtlich wahre Aussage handelt, haben wir nun gezeigt, dass die Behauptung tatsächlich für 0 gilt. Der Induktionsanfang ist somit abgeschlossen.

(2) **Induktionsschritt:** Der Induktionsschritt besteht aus zwei Teilen, nämlich der *Induktionsvoraussetzung* und dem *Induktionsschluss*. In der Induktionsvoraussetzung müssen wir annehmen, dass die Aussage aus Lemma 2.4.3 für eine beliebige natürliche Zahl k gilt. Im Induktionsschluss müssen wir dann mit Hilfe der Induktionsvoraussetzung zeigen, dass die Behauptung auch für den Nachfolger von k, also für $k+1$ wahr ist. Bezogen auf unser Beispiel können wir die Induktionsvoraussetzung und den Induktionsschluss also wie folgt formulieren:

(2.1) *Induktionsvoraussetzung:* Wir nehmen an, es gilt

$$0 + 1 + 2 + \ldots + k = \frac{k(k+1)}{2}$$

für eine beliebig gewählte natürliche Zahl $k \in \mathbb{N}$.

(2.2) *Induktionsschluss:* Wir müssen nun mit Hilfe der Induktionsvoraussetzung zeigen, dass die Behauptung auch für $k+1$ gilt, dass also

$$0 + 1 + 2 + \ldots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}$$

eine wahre Aussage ist.
Wir stellen zunächst fest, dass sich die linke Seite dieser Gleichung auch in der Form $(0 + 1 + 2 + \ldots + k) + (k+1)$ aufschreiben lässt, dass also $0{+}1{+}2{+}\ldots{+}k{+}(k{+}1)$ nichts anderes ist als die Summe von $0{+}1{+}2{+}\ldots{+}k$ und $(k{+}1)$. Nach der Induktionsvoraussetzung gilt aber für k die Gleichung

$$0 + 1 + 2 + \ldots + k = \frac{k(k+1)}{2}.$$

Wir können also den Term $0 + 1 + 2 + \ldots + k$ auch durch $\frac{k(k+1)}{2}$ ersetzen. Wenden wir dies auf die linke Seite der zu beweisenden Gleichung an, so erhalten wir

$$\begin{aligned} 0 + 1 + \ldots + k + (k+1) &= (0 + 1 + \ldots + k) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1). \end{aligned}$$

Nun sind wir bereits fast am Ziel, allerdings müssen wir noch zeigen, dass die rechte Seite dieser Gleichung tatsächlich dasselbe ist wie

$$\frac{(k+1)((k+1)+1)}{2}.$$

Wir erreichen dies durch die folgenden Umformungsschritte:

$$\begin{aligned} 0 + 1 + \ldots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(k+1)((k+1)+1)}{2}. \end{aligned}$$

Damit ist das Ziel unseres Beweises erreicht, denn wir haben aus der Induktionsvoraussetzung, also der Annahme, dass die Aussage aus Lemma 2.4.3 für ein beliebiges $k \in \mathbb{N}$ gilt, gefolgert, dass sie dann auch für den Nachfolger von k, also für $k+1$ gelten muss. Insgesamt haben wir im Induktionsschritt also für ein beliebig gewähltes $k \in \mathbb{N}$ gezeigt, dass aus der Annahme

$$0 + 1 + \ldots + k = \frac{k(k+1)}{2}$$

auch die Aussage

$$0 + 1 + \ldots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}$$

folgt. Zusammen mit dem Induktionsanfang ergibt sich daraus nun, dass die Gleichung

$$0 + 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

tatsächlich für alle natürlichen Zahlen $n \in \mathbb{N}$ gelten muss.

Es ist ratsam, sich noch einmal genau zu überlegen, was wir in den einzelnen Schritten dieses Induktionsbeweises getan haben und wie sich daraus die Wahrheit der allgemeinen Aussage aus Lemma 2.4.3 ergibt. Beim endgültigen Aufschreiben von Induktionsbeweisen sollte man darauf achten, die Struktur des Beweises transparent zu machen, indem gekennzeichnet wird, welche Teile des Beweises zum Induktionsanfang, welche zur Induktionsvoraussetzung und welche zum Induktionsschluss gehören. Unseren Induktionsbeweis für Lemma 2.4.3 können wir beispielsweise in der folgenden Form aufschreiben.

Beweis zu Lemma 2.4.3. Wir beweisen die Aussage mittels Induktion über die natürlichen Zahlen.
Induktionsanfang: Die Behauptung ist wahr für $n = 0$, denn es gilt

$$0 = \frac{0 \cdot (0+1)}{2}.$$

Induktionsschritt: Es sei nun $k \geq 0$ eine beliebige natürliche Zahl.
Induktionsvoraussetzung: Für k gelte die Aussage

$$0 + 1 + 2 + \ldots + k = \frac{k(k+1)}{2}.$$

Induktionsschluss: Wir zeigen, dass die Behauptung auch für den Nachfolger $k+1$ von k wahr ist, also die Gleichung

$$0 + 1 + 2 + \ldots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}$$

gilt. Mit Hilfe der Induktionsvoraussetzung erhalten wir:

$$\begin{aligned}
0 + 1 + 2 + \ldots + k + (k+1) &= (0 + 1 + 2 + \ldots + k) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) && \text{(Nach Ind.-Vor.)} \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)((k+1)+1)}{2}.
\end{aligned}$$

□

In der mathematischen Praxis ist es zuweilen von Vorteil, das hier besprochene Grundschema der Induktion über die natürlichen Zahlen ein wenig abzuwandeln. Besonders häufig kommen dabei die folgenden Induktionsvarianten zum Einsatz:

- *Induktion mit abweichendem Induktionsanfang:* Oft will man nicht nur Aussagen der Art „Für alle natürlichen Zahlen $n \in \mathbb{N}$ gilt $P(n)$“, sondern auch Aussagen wie etwa „Für alle $n \in \mathbb{N}$ mit $n \geq m$ gilt $P(n)$“ per Induktion beweisen. In diesem Fall muss man im Induktionsanfang den Fall $n = m$ (anstelle von $n = 0$) betrachten und für den Induktionsschritt ein beliebiges $k \geq m$ wählen.

- *Starke Induktion:* Manchmal ist es nötig, die Induktionsvoraussetzung ein wenig stärker zu formulieren. Statt also anzunehmen, dass $P(k)$ für ein beliebiges $k \in \mathbb{N}$ gilt, nimmt man in diesem Fall an, dass $P(m)$ für alle $m \in \mathbb{N}$ mit $0 \leq m \leq k$ gilt (dass die zu beweisende Aussage also für alle natürlichen Zahlen bis einschließlich k wahr ist). Diese Variante der Induktion über die natürlichen Zahlen wird als *starke Induktion* bezeichnet.

- *Induktion mit größerer Schrittweite:* Zuweilen ist es hilfreich, die Schrittweite im Induktionsschritt zu vergrößern, also nicht von $P(k)$ auf $P(k+1)$, sondern von $P(k)$ auf $P(k+s)$ für eine natürliche Zahl $s > 1$ zu schließen. Um in diesen Fällen sicherzustellen, dass die Behauptung dann trotzdem noch für *alle* $n \in \mathbb{N}$ gilt und nicht nur für jede s-te natürliche Zahl, müssen bei dieser Variante im Induktionsanfang die ersten s natürlichen Zahlen betrachtet werden (Beispiel: Man könnte im Induktionsanfang zunächst zeigen, dass die zu beweisende Behauptung für die ersten drei natürlichen Zahlen gilt, dass also $P(0)$, $P(1)$ und $P(2)$ wahr sind. Dann genügt es, im Induktionsschritt zu zeigen, dass für alle $k \in \mathbb{N}$ die Implikation $P(k) \Rightarrow P(k+3)$ gilt, denn $P(3)$ würde dann aus $P(0)$ folgen, $P(4)$ aus $P(1)$, $P(5)$ aus $P(2)$ usw.). Ein solches Vorgehen ist beispielsweise in Aufgabe 2.4.3 nötig.

2.4.3 Weitere Induktionsverfahren

Obwohl es sich bei der Induktion über die natürlichen Zahlen um das wohl bekannteste induktive Beweisverfahren handelt, ist die Beweismethode der mathematischen Induktion keineswegs auf die Menge der natürlichen Zahlen beschränkt. Vielmehr lassen sich Induktionsbeweise immer dann anwenden, wenn die Objekte, über die man eine Aussage beweisen möchte, *induktiv* definiert werden können. Um ein Gefühl für die vielfältigen Anwendungsmöglichkeiten induktiver Beweisverfahren zu bekommen, wollen wir in diesem Abschnitt eine weitere Form induktiver Beweise betrachten, die auf ähnliche Weise auch in der Untersuchung logischer Systeme eine wichtige Rolle spielt.

Wir führen zu diesem Zweck zunächst ein paar Begriffe ein. Wie wir in den zurückliegenden Abschnitten gesehen haben, werden mathematische Beweise üblicherweise umgangssprachlich aufgeschrieben. Formale logische Systeme zeichnen sich hingegen dadurch aus, dass in ihnen auf die Verwendung umgangssprachlicher Ausdrücke verzichtet und stattdessen eine *formale Sprache* verwendet wird. Eine solche formale Sprache ist im Grunde nichts anderes als eine Menge von Zeichenketten über einem genau festgelegten Alphabet von Grundsymbolen. Unter einem *Alphabet* versteht

man dabei eine endliche Menge, deren Elemente auch als *Buchstaben* bezeichnet werden. Es wird also die folgende Definition zugrunde gelegt:

Definition 2.4.4 (Alphabet)**.** Ein *Alphabet* Σ ist eine endliche Menge. Ist Σ eine Alphabet, so bezeichnen wir die Elemente von Σ als *Buchstaben*.

Alphabete, die vermutlich jeder schon einmal kennengelernt hat, sind zum Beispiel die folgenden endlichen Mengen:
(1) Das *lateinische Alphabet* $\Sigma_1 = \{a, b, c, d, e, f \ldots, x, y, z\}$,
(2) Das *griechische Alphabet* $\Sigma_2 = \{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \ldots, \chi, \psi, \omega\}$,
(3) Das *Morsealphabet* $\Sigma_3 = \{\cdot, -\}$.
Die Symbole innerhalb eines Alphabets können zu *Zeichenketten* oder *Wörtern* (engl. *strings*) zusammengesetzt werden. Dabei handelt es sich um endliche Folgen von Buchstaben eines Alphabets. Beispielsweise können wir aus den Buchstaben des lateinischen Alphabets Σ_1 die Wörter „*logik*“, „*jena*“ oder auch „*bggdrsn*“ bilden. Aus den Buchstaben des Morsealphabets Σ_3 lässt sich etwa das Wort „$\cdots - - - \cdots$“ („SOS“) zusammensetzen.

Eine Sonderstellung nimmt das sogenannte *leere Wort* ein, das mit λ bezeichnet wird und dasjenige Wort ist, das *gar keine* Buchstaben enthält (es handelt sich also um eine Buchstabenfolge der Länge 0). Hängt man das leere Wort λ rechts oder links an ein Wort w an, so ist das resultierende Wort immer identisch mit w, es gilt also für alle Wörter w die Aussage $w\lambda = w = \lambda w$ Die Menge aller Wörter über einem gegebenen Alphabet Σ wird die *Kleenesche Hülle* von Σ genannt und mit Σ^* bezeichnet. Sie lässt sich induktiv wie folgt definieren:

Definition 2.4.5 (Kleenesche Hülle)**.** Sei Σ ein Alphabet. Die *Kleenesche Hülle* Σ^* von Σ ist die Menge aller Wörter über dem Alphabet Σ und ist induktiv definiert durch:
(1) Das leere Wort λ liegt in Σ^*,
(2) Wenn $w \in \Sigma^*$ ein Wort ist und $x \in \Sigma$ ein Buchstabe, dann liegt auch wx in Σ^*.

Machen wir uns zunächst klar, wie diese induktive Definition der Menge Σ^* zu verstehen ist. Als Basisobjekt der Menge Σ^* haben wir in Punkt (1) das leere Wort λ angegeben. Aus dem leeren Wort können nach Punkt (2) nun sukzessive alle anderen Elemente aus Σ^* erzeugt werden, indem man rechts an ein bereits erzeugtes Wort $w \in \Sigma^*$ einen Buchstaben x aus dem Alphabet Σ anhängt.

Betrachten wir zur Veranschaulichung das zweielementige Alphabet $\Sigma = \{a, b\}$. Nach Punkt (1) enthält die Kleenesche Hülle Σ^* zunächst als Basisobjekt das leere Wort λ, d. h. es gilt $\lambda \in \Sigma^*$. Wählen wir nun einen Buchstaben aus Σ, etwa a, und hängen wir diesen rechts an λ an, so erhalten wir das Wort λa bzw. a, das nach Punkt (2) ebenfalls in Σ^* liegt, d. h. es gilt $a \in \Sigma^*$. Nun können wir wieder einen Buchstaben wählen, zum Beispiel b, und diesen rechts an das Wort a anhängen. Auf diese Weise erhalten wir das Wort ab, das aus zwei Buchstaben besteht und nach Punkt (2) wieder in Σ^* liegt. Wir können diese Prozedur beliebig lange fortsetzen und so immer komplexere Wörter über dem Alphabet Σ bilden. Neben a und ab erhalten wir so etwa auch die Wörter aa, bba, aba und $abababbbaaa$.

Wie bereits in Abschnitt 2.4.1 angemerkt wurde, können induktive Beweisverfahren immer dann angewendet werden, wenn die Objekte, über die eine Aussage bewiesen werden soll, selbst induktiv aufgebaut sind, also vermittels einer induktiven

Definition beschrieben werden können. Da wir die Kleenesche Hülle Σ^* eines Alphabets induktiv definiert haben, sollte es uns nun möglich sein, den induktiven Aufbau der Wörter über einem Alphabet zu nutzen, um Aussagen über alle Elemente von Σ^* induktiv zu beweisen.

Wie jedoch könnte ein solcher Induktionsbeweis für eine Aussage der Form $\forall u \in \Sigma^* P(u)$ aussehen? Um dies herauszufinden, sollten wir noch einmal unsere induktive Definition von Σ^* betrachten und uns überlegen, welche Form der Induktionsanfang, die Induktionsvoraussetzung und der Induktionsschluss eines solchen Beweises haben müssen.

Grundsätzlich gilt dabei, dass die jeweiligen Basisobjekte einer induktiv definierten Menge im *Induktionsanfang* betrachtet werden sollten. In Definition 2.4.5 haben wir als einziges Basisobjekt der Menge Σ^* das leere Wort λ angegeben. Wollen wir also mittels Induktion zeigen, dass eine Aussageform $P(u)$ für jedes $u \in \Sigma^*$ gilt, so sollten wir im Induktionsanfang zunächst den Fall $u = \lambda$ betrachten und beweisen, dass $P(\lambda)$ eine wahre Aussage ist.

Die in einer induktiven Definition genannten Erzeugungsregeln, mit denen aus den Basisobjekten weitere Objekte erzeugt werden können, entsprechen dem *Induktionsschritt* eines Induktionsbeweises. In Definition 2.4.5 haben wir als einzige Erzeugungsregel die Vorschrift

Wenn $w \in \Sigma^*$ ein Wort ist und $x \in \Sigma$ ein Buchstabe, dann liegt auch wx in Σ^*

angegeben. Aus den Elementen von Σ^* können also nur dadurch neue Wörter gebildet werden, dass rechts an ein bereits gebildetes Wort w ein Buchstabe x aus dem Alphabet Σ angehängt wird. Können wir somit zeigen, dass für alle Wörter $w \in \Sigma^*$ und für alle Buchstaben $x \in \Sigma$ die Implikation $P(w) \Rightarrow P(wx)$ gilt, so folgt offenbar, dass $P(u)$ für *alle* $u \in \Sigma^*$ gilt, dass also die allgemeine Aussage $\forall u \in \Sigma^* P(u)$ wahr ist (vorausgesetzt natürlich, dass $P(\lambda)$ wahr ist). In der *Induktionsvoraussetzung* sollten wir daher ein beliebiges Wort $w \in \Sigma^*$ wählen und annehmen, dass $P(w)$ gilt. Im *Induktionsschluss* müssen wir dann mit Hilfe der Induktionsvoraussetzung zeigen, dass auch die Aussage $P(wx)$ für jeden Buchstaben $x \in \Sigma$ gilt.

Wir fassen unser Induktionsprinzip für die Menge Σ^* noch einmal in folgendem Grundschema zusammen:

Will man zeigen, dass eine Aussage der Form $\forall u \in \Sigma^* P(u)$ gilt, so genügt es, die folgenden Schritte abzuarbeiten:

(1) **Induktionsanfang:** Man beweist, dass die Aussage für das leere Wort λ gilt, dass also $P(\lambda)$ wahr ist.

(2) **Induktionsschritt:**

  (2.1) *Induktionsvoraussetzung:* Man nimmt an, dass die Aussage $P(w)$ für ein beliebiges Wort $w \in \Sigma^*$ gilt.

  (2.2) *Induktionsschluss:* Man beweist mit Hilfe der Induktionsvoraussetzung, dass auch die Aussage $P(wx)$ für alle Buchstaben $x \in \Sigma$ gilt.

Man beachte, dass sich dieses Grundschema induktiver Beweise für Σ^* unmittelbar aus der induktiven Definition von Σ^* ergibt und gewissermaßen derselben Struktur folgt. Diese sehr nützliche Eigenschaft induktiver Definitionen lässt sich auch ganz allgemein als Faustregel festhalten: Wann immer eine Menge induktiv

definiert wurde, lässt sich aus der jeweiligen induktiven Definition ein passendes induktives Beweisprinzip für die Menge ableiten.

Bevor wir ein Beispiel für einen Induktionsbeweis über Σ^* betrachten, soll zunächst der Begriff der *Länge* eines Wortes $u \in \Sigma^*$ eingeführt werden. Diese wird mit $|u|$ bezeichnet und entspricht der Anzahl der Buchstabenvorkommen in u. Ist beispielsweise Σ das zweielementige Alphabet $\{a, b\}$ und ist $u \in \Sigma^*$ das Wort *ababba*, so gilt $|u| = |ababba| = 6$. Ebenso wie die Menge Σ^* selbst, kann auch die Länge eines Wortes induktiv definiert werden. Dabei kann man den induktiven Aufbau der Wörter aus Σ^* ausnutzen und sich bei der Definition von $|u|$ auf die folgenden Angaben beschränken:

(1) Man definiert den Begriff der Länge zunächst für das Basiselement λ. Da das leere Wort keine Buchstaben enthält, können wir ihm die Länge 0 zuweisen, also $|\lambda| := 0$ setzen.
(2) Man gibt an, wie sich die Länge eines Wortes der Form wx mit $w \in \Sigma^*$ und $x \in \Sigma$ aus der Länge von w ergibt. Da alle Buchstabenvorkommen von w auch in wx enthalten sind und wx daneben noch ein weiteres Vorkommen des Buchstabens x enthält, können wir die Länge von wx durch $|wx| := |w| + 1$ definieren (in Worten: Die Länge eines Wortes wx entspricht der Länge von w plus Eins).

Die induktive Definition der Länge eines Wortes kann zusammengefasst wie folgt aufgeschrieben werden.

Definition 2.4.6 (Länge eines Wortes)**.** Sei Σ ein Alphabet und sei $u \in \Sigma^*$ ein Wort über Σ. Die *Länge von* u wird mit $|u|$ bezeichnet und ist induktiv definiert durch:
(1) Das leere Wort λ hat die Länge 0, d. h. es gilt $|\lambda| := 0$,
(2) Ist $w \in \Sigma^*$ ein Wort und $x \in \Sigma$ ein Buchstabe, so ist die Länge von wx definiert durch $|wx| := |w| + 1$.

Mit Hilfe unseres Induktionsprinzips für Σ^* und der induktiven Definition der Wortlänge können wir nun einen Induktionsbeweis für die folgende Aussage führen.

Lemma 2.4.7. Sei Σ ein Alphabet. Für alle Wörter $u, v \in \Sigma^*$ gilt $|uv| = |u| + |v|$.

Um diese Behauptung mittels Induktion zu beweisen, müssen wir uns zunächst überlegen, wie wir das oben dargestellte Grundschema induktiver Beweise über Σ^* auf die Aussageform $|uv| = |u| + |v|$ übertragen können. Es bietet sich hier an, nur den induktiven Aufbau des Wortes v zu berücksichtigen und u einfach als ein beliebiges, fest gewähltes Wort zu betrachten. Bezeichnen wir mit $P(v)$ also die Aussageform $\forall u \in \Sigma^* (|uv| = |u| + |v|)$, so beweisen wir mittels Induktion über Σ^*, dass die Aussage $P(v)$ für jedes $v \in \Sigma^*$ gilt. Machen wir uns ein paar Gedanken zu den einzelnen Beweisschritten:

(1) **Induktionsanfang:** Im Induktionsanfang müssen wir zeigen, dass die Behauptung für das leere Wort gilt, dass also für $v = \lambda$ die Aussage $\forall u \in \Sigma^* (|uv| = |u| + |v|)$ wahr ist. Wir wählen für u ein beliebiges Wort aus Σ^* und nehmen an, dass $v = \lambda$ gilt. Nach unserer Definition der Wortlänge ist dann $|v| = |\lambda| = 0$. Daraus ergibt sich die Gleichung

$$|uv| = |u\lambda| = |u| = |u| + 0 = |u| + |\lambda| = |u| + |v|.$$

(2) **Induktionsschritt:**
   (2.1) *Induktionsvoraussetzung:* Wir nehmen an, dass die Aussage $\forall u \in \Sigma^* \, (|uw| = |u| + |w|)$ für ein beliebiges $w \in \Sigma^*$ gilt.
   (2.2) *Induktionsschluss:* Im Induktionsschluss müssen wir mit Hilfe der Induktionsvoraussetzung zeigen, dass für jedes Wort $u \in \Sigma^*$ und für jeden Buchstaben $x \in \Sigma$ die Behauptung $|u(wx)| = |u| + |wx|$ gilt. Mit Hilfe der Definition der Wortlänge erhalten wir zunächst $|u(wx)| = |uwx| = |uw| + 1$. Nach Induktionsvoraussetzung gilt nun $|uw| = |u| + |w|$. Durch Einsetzen kommen wir auf $|u(wx)| = |uw| + 1 = |u| + |w| + 1$. Da nach Definition der Wortlänge $|w| + 1 = |wx|$ gilt, gelangen wir zu $|u(wx)| = |u| + |w| + 1 = |u| + |wx|$, womit der Induktionsschritt abgeschlossen ist.

Wir können den kompletten Induktionsbeweis noch einmal in der folgenden Form aufschreiben:

Beweis zu Lemma 2.4.7. Es seien Σ ein Alphabet und $u, v \in \Sigma^*$ beliebige Wörter über Σ. Wir beweisen die Behauptung mittels Induktion über den Aufbau von v.
Induktionsanfang: Sei $v = \lambda$. Unter Ausnutzung von $|\lambda| = 0$ erhalten wir dann

$$|uv| = |u\lambda| = |u| = |u| + 0 = |u| + |\lambda| = |u| + |v|.$$

Induktionsschritt: Sei nun $w \in \Sigma^*$ ein beliebiges Wort über Σ.
Induktionsvoraussetzung: Für w gelte die Aussage $|uw| = |u| + |w|$.
Induktionsschluss: Wir müssen zeigen, dass für jeden Buchstaben $x \in \Sigma$ die Aussage $|u(wx)| = |u| + |wx|$ gilt. Sei also $x \in \Sigma$ ein beliebiger Buchstabe aus Σ. Dann gilt:

$$\begin{aligned} |u(wx)| &= |uwx| \\ &= |uw| + 1 && \text{(nach Def. 2.4.6)} \\ &= |u| + |w| + 1 && \text{(nach Ind.-Vor.)} \\ &= |u| + |wx|. && \text{(nach Def. 2.4.6)} \end{aligned}$$

□

Aufgaben

2.4.1 Beweisen Sie folgende Aussagen mittels Induktion über die natürlichen Zahlen:
a) $0^2 + 1^2 + 2^2 + \ldots + n^2 = \frac{n \cdot (n+1)(2n+1)}{6}$ für alle $n \in \mathbb{N}$.
b) $0^3 + 1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ für alle $n \in \mathbb{N}$.
c) $n! > 2^n$ für alle $n \in \mathbb{N}$ mit $n \geq 4$.
d) $\sqrt{n} \cdot n > \sqrt{n} + n$ für alle $n \in \mathbb{N}$ mit $n \geq 4$.
e) Für alle $n \in \mathbb{N}$ ist $n^2 + n$ eine gerade Zahl.
f) Ist $x \in \mathbb{R}$ eine reelle Zahl, dann gilt $(1 + x)^n \geq 1 + nx$ für alle $n \in \mathbb{N}$.

2.4.2 Führen Sie einen Induktionsbeweis für die folgende Behauptung: Jeder Geldbetrag von mindestens 4 Cent kann allein mit Zwei- und Fünfcentmünzen bezahlt werden.

2.4.3 Zeigen Sie mittels Induktion, dass sich jede natürliche Zahl $n \in \mathbb{N}$ mit $n \geq 8$ als Summe von Dreien und Fünfen schreiben lässt.

2.4.4 Gegeben sei ein Schachbrett mit Seitenlänge 2^n für $n \geq 1$, aus dem ein beliebiges Feld entfernt wurde. Zeigen Sie per Induktion über n, dass man die $(2^n \cdot 2^n - 1)$ verbleibenden Felder vollständig mit L-förmigen Steinen bedecken kann. Dabei wird angenommen, dass ein L-förmiger Stein immer genau drei Felder des Schachbretts bedeckt.

2.4.5 Wir betrachten das zweielementige Alphabet $\Sigma = \{a, b\}$. Ist $u \in \Sigma^*$ ein Wort über Σ, so bezeichnen wir mit $|u|_a$ die Anzahl der a's in u und mit $|u|_b$ die Anzahl der b's in u. Geben Sie induktive Definitionen für $|u|_a$ und $|u|_b$.

2.4.6 Sei Σ das Alphabet $\{a, b\}$. Benutzen Sie Ihre induktive Definition von $|u|_a$ und $|u|_b$, um einen Induktionsbeweis für die folgende Behauptung zu führen: Für jedes Wort $u \in \Sigma^*$ gilt $|u| = |u|_a + |u|_b$.

3 Lösungen zu den Aufgaben

Lösungen zu Kapitel 1

1.1.1 Wir schreiben „$n \mid m$“ für „n ist ein Teiler von m“. Die genannten Aussagen können dann wie folgt analysiert werden:

a) „$(3 \mid 6)$ & $(3 \mid 9)$ & $(3 \mid 10)$“. Da „$3 \mid 10$“ eine falsche Aussage ist, ist die gesamte Konjunktion falsch.

b) „$(15 \mid 45) \Rightarrow ((1 \mid 45)$ & $(3 \mid 45)$ & $(5 \mid 45)$ & $(15 \mid 45))$“. Da der hintere Teil der Implikation wahr ist, ist die Aussage insgesamt wahr.

c) „$(3 \mid 4) \parallel (3 \mid 5) \parallel (3 \mid 6)$“. Da „$3 \mid 6$“ wahr ist, ist die gesamte Disjunktion wahr.

d) „$(2^2 = 4)$ & $((-2)^2 = 4)$“. Da beide Glieder der Konjunktion wahr sind, ist die Aussage wahr.

e) „$((1 > 2)$ & $(1 < 5)) \Rightarrow ((2 > 3)$ & $(2 < 6))$“. Da „$(1 > 2)$ & $(1 < 5)$“ eine falsche Aussage ist, ist die Implikation wahr.

1.1.2

a) Wie sich aus folgender Wahrheitstafel ablesen lässt, ist die Aussage $(P \parallel Q)$ & $(\sim P \parallel \sim Q)$ kontingent:

P	Q	$(P \parallel Q)$ & $(\sim P \parallel \sim Q)$
W	W	F
W	F	W
F	W	W
F	F	F

b) Die Aussage $(P \parallel Q) \parallel (\sim P \parallel \sim Q)$ ist eine Tautologie.

c) Die Aussage $(P \parallel Q)$ & $(\sim P$ & $\sim Q)$ ist eine Kontradiktion.

d) Die Aussage $(P$ & $(Q \parallel \sim R)) \parallel (\sim P \parallel R)$ ist eine Tautologie.

1.1.3 Um zu zeigen, dass die jeweiligen Aussagen äquivalent sind, genügt es zu zeigen, dass sie in jeder Zeile der Wahrheitstafel denselben Wahrheitswert besitzen. Die folgenden Wahrheitstafeln zeigen, dass dies tatsächlich für die genannten Aussagen der Fall ist:

a)

P	$(P$ & $P)$
W	W
F	F

b)

P	$(P \parallel P)$
W	W
F	F

c)

P	Q	R	$P \,\&\, (Q \parallel R)$	$(P \,\&\, Q) \parallel (P \,\&\, R)$
W	W	W	W	W
W	W	F	W	W
W	F	W	W	W
W	F	F	F	F
F	W	W	F	F
F	W	F	F	F
F	F	W	F	F
F	F	F	F	F

d)

P	Q	R	$P \parallel (Q \,\&\, R)$	$(P \parallel Q) \,\&\, (P \parallel R)$
W	W	W	W	W
W	W	F	W	W
W	F	W	W	W
W	F	F	W	W
F	W	W	W	W
F	W	F	F	F
F	F	W	F	F
F	F	F	F	F

e)

P	Q	$P \,\&\, (P \parallel Q)$
W	W	W
W	F	W
F	W	F
F	F	F

f)

P	Q	$P \parallel (P \,\&\, Q)$
W	W	W
W	F	W
F	W	F
F	F	F

1.1.4

a) Die Verknüpfung $\downarrow$ entspricht dem umgangssprachlichen „Weder... noch...“.

b) Es ist $\sim(P \parallel Q) \equiv P \downarrow Q$.

c) Es gilt $(\sim P \,\&\, \sim Q) \equiv (P \downarrow Q)$.

d) Es ist $\sim P \equiv (P \downarrow P)$, $(P \,\&\, Q) \equiv ((P \downarrow P) \downarrow (Q \downarrow Q))$, $(P \parallel Q) \equiv ((P \downarrow Q) \downarrow (P \downarrow Q))$ und $(P \Rightarrow Q) \equiv (((P \downarrow P) \downarrow Q) \downarrow ((P \downarrow P) \downarrow Q))$.

1.1.5

a) $P \uparrow Q$ hat die folgende Wahrheitstafel:

P	Q	$P \uparrow Q$
W	W	F
W	F	W
F	W	W
F	F	W

b) Es ist $\sim(P \,\&\, Q) \equiv (P \uparrow Q)$.

c) Es gilt $(\sim P \parallel \sim Q) \equiv (P \uparrow Q)$.

d) Es gilt $\sim P \equiv (P \uparrow P)$, $(P \,\&\, Q) \equiv ((P \uparrow Q) \uparrow (P \uparrow Q))$, $(P \parallel Q) \equiv ((P \uparrow P) \uparrow (Q \uparrow Q))$ und $(P \Rightarrow Q) \equiv (((P \uparrow P) \uparrow (P \uparrow P)) \uparrow (Q \uparrow Q))$.

1.1.6

a) Wir nehmen an, P ist eine Tautologie, d. h. P besitzt in jeder Zeile der entsprechenden Wahrheitstafel den Wert „W“. Dann erhalten wir für $P \,\&\, Q$ und $P \parallel Q$ die folgende Wahrheitstafel:

P	Q	$P \,\&\, Q$	$P \parallel Q$
W	W	W	W
W	F	F	W

Wie sich aus der Tafel ablesen lässt, hat $P \,\&\, Q$ denselben Wahrheitswertverlauf wie Q und $P \parallel Q$ denselben Wahrheitswertverlauf wie P. Folglich gilt $(P \,\&\, Q) \equiv Q$ und $(P \parallel Q) \equiv P$.

b) Nach Aufgabenteil a) gilt $(P \parallel Q) \equiv P$ für jede Tautologie P. Ist P also eine beliebige Tautologie (z. B. $Q \parallel \sim Q$), so sind die Aussagen $P \parallel Q$, $P \parallel (Q \,\&\, Q)$, $P \parallel ((Q \,\&\, Q) \,\&\, Q)$ usw. allesamt äquivalent zu P und damit ebenfalls Tautologien. Folglich gibt es unendlich viele Tautologien.

c) Nach Aufgabenteil b) gibt es unendlich viele Tautologien. Da die Negation einer Tautologie immer eine Kontradiktion ist, gibt es folglich auch unendlich viele Kontradiktionen.

1.1.7

a) $P \parallel \sim Q$

b) $\sim P \parallel \sim Q$ oder auch $\sim(P \,\&\, Q)$

c) $(P \parallel Q) \,\&\, \sim(P \,\&\, Q)$

1.2.1 Wir schreiben im Folgenden $x \mid y$ für die Aussageform $\exists z(z \in \mathbb{Z} \,\&\, y = x \cdot z)$, was so viel bedeutet wie „x ist ein Teiler von y“. Die genannten Aussagen können dann wie folgt aufgeschrieben werden:

a) $(x \in \mathbb{Z}) \,\&\, (y \in \mathbb{Z}) \,\&\, (x \mid y)$.

b) $(x \in \mathbb{P}) \Rightarrow ((1 \mid x) \,\&\, (x \mid x) \,\&\, \sim\exists y((y \mid x) \,\&\, \sim(y = 1) \,\&\, \sim(y = x)))$.

c) $\forall x((x \in \mathbb{Z}) \Rightarrow (x \in \mathbb{Q})) \,\&\, \exists y((y \in \mathbb{Q}) \,\&\, \sim(y \in \mathbb{Z}))$.

d) $\exists x((x \in \mathbb{Z}) \,\&\, \forall y((y \in \mathbb{N}) \Rightarrow (x < y)))$.

1.2.2

a) Die Aussage ist wahr, denn für jede Zahl $x \in M$ gibt es die Zahl $x \in M$, für die offensichtlich $x = x$ gilt.

b) Die Aussage ist falsch, denn da die Menge M mehr als ein Element enthält, gibt es für jede Zahl $x \in M$ eine Zahl y, so dass $\sim(x = y)$ gilt.

c) Die Aussage ist wahr, denn da die Aussage aus b) falsch ist, ist deren Negation $\sim\exists x \forall y(x = y)$ wahr. Durch zweimalige Anwendung der Quantorendualität (Satz 1.2.4) folgt daraus die Aussage $\forall x \exists y \sim(x = y)$.

d) Die Aussage ist falsch, denn wie sich mittels Quantorendualität zeigen lässt, ist sie zu der Negation von a) äquivalent.

1.2.3 Es gilt:

a) $\emptyset = \{x \mid \sim(x = x)\}$.

b) $A \cap B = \{x \mid (x \in A) \,\&\, (x \in B)\}$.

c) $A \cup B = \{x \mid (x \in A) \parallel (x \in B)\}$.

d) $A - B = \{x \mid (x \in A) \,\&\, \sim(x \in B)\}$.

1.2.4 Es gilt:
a) $A \cap B = \{x \mid x \in A \,\&\, x \in B\} = \{x \mid x \in B \,\&\, x \in A\} = B \cap A$.
b) $A \cup B = \{x \mid x \in A \parallel x \in B\} = \{x \mid x \in B \parallel x \in A\} = B \cup A$.
c) $A \cap (B \cap C) = \{x \mid x \in A \,\&\, x \in B \cap C\} = \{x \mid x \in A \,\&\, (x \in B \,\&\, x \in C)\} = \{x \mid (x \in A \,\&\, x \in B) \,\&\, x \in C\} = \{x \mid x \in A \cap B \,\&\, x \in C\} = (A \cap B) \cap C$.
d) $A \cup (B \cup C) = \{x \mid x \in A \parallel x \in B \cup C\} = \{x \mid x \in A \parallel (x \in B \parallel x \in C)\} = \{x \mid (x \in A \parallel x \in B) \parallel x \in C\} = \{x \mid x \in A \cup B \parallel x \in C\} = (A \cup B) \cup C$.
e) $A \cap A = \{x \mid x \in A \,\&\, x \in A\} = \{x \mid x \in A\} = A$.
f) $A \cup A = \{x \mid x \in A \parallel x \in A\} = \{x \mid x \in A\} = A$.
g) $A \cap \emptyset = \{x \mid x \in A \,\&\, x \in \emptyset\} = \{x \mid x \in A \,\&\, \sim(x = x)\} = \{x \mid \sim(x = x)\} = \emptyset$.
h) $A \cup \emptyset = \{x \mid x \in A \parallel x \in \emptyset\} = \{x \mid x \in A \parallel \sim(x = x)\} = \{x \mid x \in A\} = A$.

1.2.5
a) Die Aussage $T \subseteq A$ lässt sich in der Form $\forall x((x \in T) \Rightarrow (x \in A))$ ausdrücken.
b) Da die leere Menge per Definition *keine* Elemente enthält, ist $x \in \emptyset$ für alle Gegenstände x eine falsche Aussage. Nach Definition der Aussageverknüpfung $\Rightarrow$ ist $(x \in \emptyset) \Rightarrow (x \in A)$ somit für alle x wahr, d. h. es gilt $\forall x((x \in \emptyset) \Rightarrow (x \in A))$. Nach a) ist $\forall x((x \in \emptyset) \Rightarrow (x \in A))$ nun gleichbedeutend mit $\emptyset \subseteq A$. Da wir A beliebig gewählt haben, gilt folglich $\emptyset \subseteq A$ für *alle* Mengen A.
c) Offensichtlich ist $\forall x((x \in A) \Rightarrow (x \in A))$ für jede Menge A eine wahre Aussage. Mit Aufgabenteil a) folgt daraus nun $A \subseteq A$ für alle A.
d) Es gilt $\mathcal{P}(A) = \{x \mid x \subseteq A\} = \{x \mid \forall y((y \in x) \Rightarrow (y \in A))\}$.
e) Nach dem Extensionalitätsaxiom gilt $A = B$ genau dann, wenn $\forall x(x \in A \Leftrightarrow x \in B)$ gilt. Zufolge Satz 1.1.3 ist ferner $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \,\&\, (Q \Rightarrow P))$ eine Tautologie. Folglich ist $\forall x(x \in A \Leftrightarrow x \in B)$ genau dann wahr, wenn $\forall x((x \in A \Rightarrow x \in B) \,\&\, (x \in B \Rightarrow x \in A))$ gilt. Nach der Distributivitätsregel für den Allquantor (Satz 1.2.4) ist dies wiederum äquivalent zu $\forall x(x \in A \Rightarrow x \in B) \,\&\, \forall x(x \in B \Rightarrow x \in A)$, was nach a) dasselbe bedeutet wie $A \subseteq B \,\&\, B \subseteq A$.

1.2.6
a) Die Aussagen $\forall x(P(x) \parallel Q(x))$ und $\forall x P(x) \parallel \forall x Q(x)$ sind *nicht* äquivalent. Sei $P(x)$ die Aussageform „x ist eine gerade Zahl“ und $Q(x)$ die Aussageform „x ist eine ungerade Zahl“. Wählen wir als zugrundeliegende Menge M die Menge $\mathbb{N}$ der natürlichen Zahlen, so ist die Aussage $\forall x(P(x) \parallel Q(x))$ wahr, denn jede natürliche Zahl ist entweder gerade oder ungerade. Die Aussage $\forall x P(x) \parallel \forall x Q(x)$ allerdings ist *nicht* wahr, denn es stimmt weder, dass alle natürlichen Zahlen gerade, noch, dass alle natürlichen Zahlen ungerade sind.
b) Die Aussagen $\exists x(P(x) \,\&\, Q(x))$ und $\exists x P(x) \,\&\, \exists x Q(x)$ sind *nicht* äquivalent. Sei $P(x)$ wieder die Aussageform „x ist eine gerade Zahl“ und $Q(x)$ die Aussageform „x ist eine ungerade Zahl“. Als Grundmenge verwenden wir wieder die Menge $\mathbb{N}$ der natürlichen Zahlen. Dann ist die Aussage $\exists x P(x) \,\&\, \exists x Q(x)$ wahr, denn es existiert sowohl eine gerade als auch eine ungerade natürliche Zahl. Die Aussage $\exists x(P(x) \,\&\, Q(x))$ ist nun allerdings falsch, denn keine natürliche Zahl ist sowohl gerade als auch ungerade.

Lösungen zu Kapitel 2

2.1.1

a) Sei $n \in \mathbb{Z}$ eine beliebige ungerade Zahl. Dann gibt es ein $k \in \mathbb{Z}$, so dass $n = 2 \cdot k + 1$. Für dieses k gilt dann $n^2 = (2 \cdot k + 1) \cdot (2 \cdot k + 1) = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1$. Für die ganze Zahl $m := 2k^2 + 2k$ gilt folglich $n^2 = 2 \cdot m + 1$, d. h. n^2 ist ungerade.

b) Seien $a, b \in \mathbb{Z}$ zwei beliebige ungerade Zahlen. Dann gibt es ganze Zahlen $s, t \in \mathbb{Z}$, so dass $a = 2 \cdot s + 1$ und $b = 2 \cdot t + 1$ gilt. Daraus folgt $a + b = (2s + 1) + (2t + 1) = 2s + 2t + 2 = 2 \cdot (s + t + 1)$. Für $k := s + t + 1$ gilt somit $a + b = 2 \cdot k$. Also ist $a + b$ gerade.

c) Seien $a, b, c \in \mathbb{Z}$ beliebige ganze Zahlen mit $a \mid b$ und $b \mid c$. Dann gibt es ganze Zahlen $k_1, k_2 \in \mathbb{Z}$, so dass $b = a \cdot k_1$ und $c = b \cdot k_2$. Durch Einsetzen von $a \cdot k_1$ für b in $c = b \cdot k_2$ erhalten wir $c = a \cdot k_1 \cdot k_2$. Für die ganze Zahl $m := k_1 \cdot k_2$ gilt folglich $c = a \cdot m$, d. h. es gilt $a \mid c$.

d) Wir nehmen an, dass n eine beliebige ungerade Zahl ist und zeigen, dass $n + (n + 2)$ durch 4 teilbar ist. Sei $n \in \mathbb{Z}$ ungerade, d. h. es gilt $n = 2k + 1$ für ein $k \in \mathbb{Z}$. Dann gilt $n + (n + 2) = (2k + 1) + ((2k + 1) + 2) = 4k + 4 = 4 \cdot (k + 1)$. Für $m := k + 1$ gilt somit $n + (n + 2) = 4 \cdot m$ und daher $4 \mid n + (n + 2)$.

e) Es sei $n \in \mathbb{Z}$ eine beliebige ganze Zahl, deren letzte Dezimalstelle eine 5 ist. Wir schreiben im Folgenden „$z_1 z_2 \dots z_m$“ für die Dezimaldarstellung von n (ist n also beispielsweise die Zahl 245, so ist $m = 3$ und es gilt $z_1 = 2$, $z_2 = 4$ und $z_3 = 5$). Nach Voraussetzung ist dann $z_m = 5$. Sei nun p die Zahl mit Dezimaldarstellung $z_1 z_2 \dots z_{m-1}$. Dann gilt $n = 10 \cdot p + 5 = n = 5 \cdot 2 \cdot p + 5 = 5 \cdot (2p + 5)$. Für $k := 2p + 5$ erhalten wir somit $n = 5 \cdot k$. Folglich gilt $5 \mid n$.

2.1.2 Es seien $a, b \in \mathbb{Q}$ zwei beliebige rationale Zahlen mit $a < b$. Nach Definition der rationalen Zahlen gibt es dann ganze Zahlen $n_1, n_2, m_1, m_2 \in \mathbb{Z}$, so dass $a = \frac{n_1}{m_1}$ und $b = \frac{n_2}{m_2}$ gilt. Wir setzen $c := \frac{a+b}{2}$. Dann ist

$$c = \frac{\frac{n_1}{m_1} + \frac{n_2}{m_2}}{2} = \frac{n_1 m_2 + n_2 m_1}{2 m_1 m_2}.$$

Da offensichtlich sowohl $n_1 m_2 + n_2 m_1$ als auch $2 m_1 m_2$ ganze Zahlen sind, ist folglich c eine rationale Zahl. Es bleibt nun nur noch zu zeigen, dass $a < c$ und $c < b$ gilt. Wegen $a < b$ und $c = \frac{a+b}{2}$ gilt zunächst $\frac{a+a}{2} < c$ und $c < \frac{b+b}{2}$. Aus $\frac{a+a}{2} < c$ folgt $2a < 2c$ und damit $a < c$. Analog erhalten wir aus $c < \frac{b+b}{2}$ zunächst $2c < 2b$ und schließlich $c < b$. Somit gilt $a < c < b$ für $c \in \mathbb{Q}$.

2.1.3

a) Seien $n, k \in \mathbb{N}$ beliebig mit $k \leq n$. Es gilt:

$$\begin{aligned}
\binom{n}{k} &= \frac{n!}{(n-k)! \cdot k!} \\
&= \frac{n!}{(n-k)! \cdot (n-n+k)!} \\
&= \frac{n!}{(n-k)! \cdot (n-(n-k))!} \\
&= \frac{n!}{(n-(n-k))! \cdot (n-k)!}
\end{aligned}$$

$$= \binom{n}{n-k}.$$

b) Seien $n, k \in \mathbb{N}$ beliebig mit $k \leq n$. Es gilt:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(n-1-(k-1))! \cdot (k-1)!} + \frac{(n-1)!}{(n-1-k)! \cdot k!} \\
&= \frac{(n-1)!}{(n-1-k+1)! \cdot (k-1)!} + \frac{(n-1)!}{(n-1-k)! \cdot k!} \\
&= \frac{(n-1)!}{(n-k)! \cdot (k-1)!} + \frac{(n-1)!}{(n-1-k)! \cdot k!} \\
&= \frac{(n-1)! \cdot k}{(n-k)! \cdot (k-1)! \cdot k} + \frac{(n-k) \cdot (n-1)!}{(n-k) \cdot (n-k-1)! \cdot k!} \\
&= \frac{(n-1)! \cdot k}{(n-k)! \cdot k!} + \frac{(n-k) \cdot (n-1)!}{(n-k)! \cdot k!} \\
&= \frac{(n-1)! \cdot k + (n-k) \cdot (n-1)!}{(n-k)! \cdot k!} \\
&= \frac{(n-1)! \cdot (k+n-k)}{(n-k)! \cdot k!} \\
&= \frac{(n-1)! \cdot n}{(n-k)! \cdot k!} \\
&= \frac{n!}{(n-k)! \cdot k!} \\
&= \binom{n}{k}.
\end{aligned}$$

2.2.1

a) Seien $a, b, c \in \mathbb{Z}$. Wir nehmen an, es gilt $a + c = b + c$. Indem wir c auf beiden Seiten der Gleichung subtrahieren, erhalten wir dann $a = b$.

b) Seien $a, b \in \mathbb{Z}$ beliebig. Wir nehmen an, a und b sind nicht teilerfremd, d. h. es gibt ein $c \in \mathbb{Z}$ mit $c \neq 1$, so dass $c \mid a$ und $c \mid b$ gilt. Folglich gibt es Zahlen $m, n \in \mathbb{Z}$ mit $a = cm$ und $b = cn$. Daraus ergibt sich $a+b = cm+cn = c \cdot (m+n)$ und $a - b = cm - cn = c \cdot (m - n)$, d. h. sowohl $a + b$ als auch $a - b$ ist durch c teilbar. Somit sind $a + b$ und $a - b$ nicht teilerfremd.

c) Sei $n \in \mathbb{Z}$ beliebig. Wir nehmen an, n lässt bei der Division durch 3 den Rest 1, d. h. es gibt ein $k \in \mathbb{Z}$, so dass $n = 3k+1$ gilt. Dann ist $n^2 = (3k+1) \cdot (3k+1) = 9k^2 + 6k + 1 = 3 \cdot (3k^2 + 2k) + 1$, d. h. n^2 lässt bei Division durch 3 den Rest 1.

d) Seien $m, n \in \mathbb{Z}$ beliebig. Wir nehmen an, $n \nmid m$, d. h. n ist kein Teiler von m. Da n selbst ein Teiler von n ist, gibt es folglich einen Teiler t von n mit $t \nmid m$, d. h. es ist falsch, dass $t \mid m$ für alle Teiler t von n gilt.

e) Sei $n \in \mathbb{Z}$ beliebig. Wir nehmen an, n ist durch 10 teilbar, d. h. es gibt ein $k \in \mathbb{Z}$, so dass $n = 10k$. Dann gilt $n = 2 \cdot (5k)$ und $5 \cdot (2k)$. Folglich ist n sowohl durch 2 als auch durch 5 teilbar.

f) Sei $n \in \mathbb{Z}$ beliebig. Wir nehmen an, n lässt bei Division durch 4 den Rest 2, d. h. es gibt ein $k \in \mathbb{Z}$ mit $n = 4k + 2$. Dann gilt $n^2 = (4k + 2) \cdot (4k + 2) = 16k^2 + 16k + 4 = 4 \cdot (4k^2 + 4k + 1)$. Somit ist n^2 durch 4 teilbar.

g) Seien $n, m, t \in \mathbb{Z}$ beliebig. Wir nehmen an, t ist ein Teiler von n und m, d. h. es gibt ganze Zahlen $k_1, k_2 \in \mathbb{Z}$, so dass $n = tk_1$ und $m = tk_2$. Dann gilt $n + m = tk_1 + tk_2 = t \cdot (k_1 + k_2)$. Folglich ist t ein Teiler von $n + m$.

h) Seien $a, b \in \mathbb{Z}$ beliebig. Wir nehmen an, es ist falsch, dass eine der Zahlen a und b gerade und die andere ungerade ist, d. h. entweder a und b sind beide gerade oder beide ungerade. Sind a und b beide gerade, dann gilt $a = 2m$ und $b = 2n$ für ganze Zahlen $m, n \in \mathbb{Z}$ und es folgt $a + b = 2m + 2n = 2 \cdot (m + n)$, d. h. $a + b$ ist gerade. Sind a und b beide ungerade, dann gilt $a = 2m+1$ und $b = 2n+1$ für ganze Zahlen $m, n \in \mathbb{Z}$. Daraus folgt $a+b = (2m+1)+(2n+1) = 2m+2n+2 = 2 \cdot (m+n+1)$, d. h. $a + b$ ist abermals gerade.

2.3.1

a) Es sei $n \in \mathbb{N}$ eine gerade Zahl. Wir nehmen an, $\sqrt{n}$ ist eine natürliche Zahl und $\sqrt{n}$ ist ungerade. Da $\sqrt{n}$ ungerade ist, ist nach Aufgabe 2.1.1 auch $(\sqrt{n})^2 = n$ ungerade. Dies ist ein Widerspruch zu unserer Annahme, dass n gerade ist.

b) Wir nehmen an, n^3 ist eine gerade Zahl und n ist ungerade. Dann gibt es ein $k \in \mathbb{Z}$, so dass $n = 2k + 1$. Daraus folgt $n^3 = (2k + 1) \cdot (2k + 1) \cdot (2k + 1) = 8k^3 + 10k^2 + 6k + 1 = 2 \cdot (4k^3 + 5k^2 + 3k) + 1$, d. h. n^3 ist ungerade. Widerspruch zu unserer Annahme, dass n^3 gerade ist!

c) Sei $n \in \mathbb{N}$ und $p \in \mathbb{P}$. Wir nehmen an, $p \mid n^2$ und p ist kein Teiler von n. Da p eine Primzahl ist, besitzt p nur die Teiler 1 und p. Nach Annahme ist p kein Teiler von n. Folglich haben n und p außer 1 keinen gemeinsamen Teiler. Nach dem Lemma von Bézout gibt es nun Zahlen $s, t \in \mathbb{Z}$, so dass $1 = sp + tn$ gilt. Indem wir beide Seiten der Gleichung mit n multiplizieren, erhalten wir $n = nsp + tn^2$. Nach unserer Annahme ist n^2 durch p teilbar, d. h. es gibt ein $k \in \mathbb{Z}$ mit $n^2 = pk$. Durch Einsetzen erhalten wir dann $n = nsp+tpk = p \cdot (ns+tk)$, d. h. n ist durch p teilbar. Widerspruch zu unserer Annahme, dass p kein Teiler von n ist!

2.3.2 Wir nehmen an, $\sqrt{2}$ ist rational, d. h. es gibt ganze Zahlen $m, n \in \mathbb{Z}$, so dass $\sqrt{2} = \frac{m}{n}$. Wir können dabei ohne Beschränkung der Allgemeinheit davon ausgehen, dass der Bruch $\frac{m}{n}$ bereits vollständig gekürzt wurde, d. h. m und n besitzen außer 1 keinen gemeinsamen Teiler mehr. Es folgt nun

$$\frac{m^2}{n^2} = \left(\frac{m}{n}\right)^2 = (\sqrt{2})^2 = 2.$$

Durch Umformen erhalten wir

$$m^2 = 2n^2.$$

Da somit m^2 eine gerade Zahl ist, muss nun auch m gerade sein, denn wäre m ungerade, so wäre auch m^2 ungerade (vgl. Aufgabe 2.1.1). Folglich gibt es eine ganze Zahl $k \in \mathbb{Z}$, so dass $m = 2k$ gilt. Ersetzen wir in obiger Gleichung m durch $2k$, so kommen wir auf

$$2k \cdot 2k = 2n^2.$$

Indem wir beide Seiten der Gleichung durch 2 teilen, erhalten wir

$$2k^2 = n^2,$$

d. h. n^2 ist eine gerade Zahl und damit auch n. Also sind m und n beide gerade und folglich durch 2 teilbar. Dies ist ein Widerspruch zu unserer Annahme, dass m und n außer 1 keinen gemeinsamen Teiler haben. Also ist $\sqrt{2}$ irrational.

2.3.3 Sei p eine Primzahl. Wir nehmen an, $\sqrt{p}$ ist rational, d. h. es gibt Zahlen $m, n \in \mathbb{Z}$, so dass $\sqrt{p} = \frac{m}{n}$. Wir können ohne Beschränkung der Allgemeinheit davon ausgehen, dass der Bruch $\frac{m}{n}$ bereits vollständig gekürzt ist, d. h. m und n haben außer 1 keinen gemeinsamen Teiler. Es gilt nun

$$\frac{m^2}{n^2} = \left(\frac{m}{n}\right)^2 = (\sqrt{p})^2 = p.$$

Durch Umstellen erhalten wir

$$m^2 = pn^2,$$

d. h. m^2 ist durch p teilbar. Nach Aufgabenteil c) aus Aufgabe 2.3.1 ist dann aber auch m durch p teilbar, d. h. es gibt ein $k \in \mathbb{Z}$, so dass $m = pk$. Daraus ergibt sich

$$p^2k^2 = (pk)^2 = m^2 = pn^2.$$

Indem wir beide Seiten der Gleichung durch p teilen, erhalten wir

$$pk^2 = n^2,$$

d. h. auch n^2 ist durch p teilbar, woraus mit Aufgabe 2.3.1 folgt, dass n durch p teilbar ist. Dies ist ein Widerspruch, denn nach unserer Annahme besitzen m und n außer 1 keinen gemeinsamen Teiler. Folglich ist $\sqrt{p}$ irrational.

2.3.4 Wir nehmen an, es gibt natürliche Zahlen, die größer als 1 sind und für die keine Primfaktorzerlegung existiert. Es sei $n \in \mathbb{N}$ die kleinste derartige Zahl. Ist n eine Primzahl, dann wäre n selbst bereits eine Primfaktorzerlegung für n, was in Widerspruch zu unserer Annahme steht. Wir können also davon ausgehen, dass n keine Primzahl ist. Dann aber muss n nichttriviale Teiler $a, b \in \mathbb{N}$ besitzen, d. h. für a und b gilt $n = a \cdot b$ sowie $a \neq 1$ und $a \neq n$ (und folglich auch $b \neq 1$, $b \neq n$). Nun ist n nach unserer Annahme die *kleinste* natürliche Zahl, die keine Primfaktorzerlegung besitzt, d. h. alle natürlichen Zahlen, die kleiner sind als n, können als Produkt von Primzahlen geschrieben werden. Wegen $a \neq n$ und $b \neq n$ gilt $a < n$ und $b < n$. Also können wir a und b in der Form

$$a = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} \text{ und } b = q_1^{r_1} \cdot \ldots \cdot q_s^{r_s}$$

aufschreiben, wobei $p_1, \ldots, p_m, q_1, \ldots, q_2$ Primzahlen sind. Dann aber gilt

$$n = a \cdot b = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} \cdot q_1^{r_1} \cdot \ldots \cdot q_s^{r_s},$$

d. h. n kann ebenfalls als Produkt von Primzahlen geschrieben werden. Widerspruch!

2.3.5 Wir nehmen an, es gibt nur endlich viele Primzahlen. Sei $p_1, p_2, \ldots, p_k$ eine vollständige Auflistung aller Primzahlen. Wir definieren n als die Zahl $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$. Nach Aufgabe 2.3.4 können wir n nun in der Form $n = q_1^{r_1} \cdot \ldots \cdot q_s^{r_s}$ aufschreiben, wobei $q_1, \ldots, q_s$ Primzahlen sind. Nun ist n aber durch keine der Primzahlen $p_1 \ldots, p_k$ teilbar, denn n lässt bei der Division für jede dieser Zahlen den Rest 1. Also sind die Primfaktoren $q_1, \ldots, q_s$ von n nicht in der Liste $p_1 \ldots, p_k$ enthalten. Dies ist ein Widerspruch zu unserer Annahme, dass $p_1, \ldots, p_k$ eine *vollständige* Auflistung aller Primzahlen ist. Also gibt es unendlich viele Primzahlen.

2.4.1

a) *Induktionsanfang:* Es gilt

$$0^2 = 0 = \frac{0 \cdot (0+1)(2 \cdot 0 + 1)}{6}.$$

Induktionsschritt: Sei $k \geq 0$ beliebig.
Induktionsvoraussetzung: Für k gelte $0^2 + 1^2 + 2^2 + \ldots + k^2 = \frac{k \cdot (k+1)(2k+1)}{6}$.
Induktionsschluss: Es gilt

$$\begin{aligned}
0^2 + 1^2 + \ldots + k^2 + (k+1)^2 &= (0^2 + 1^2 + \ldots + k^2) + (k+1)^2 \\
&= \frac{k \cdot (k+1)(2k+1)}{6} + (k+1)^2 \qquad \text{(Ind.-Vor.)} \\
&= \frac{2k^3 + 3k^2 + k}{6} + \frac{6 \cdot (k^2 + 2k + 1)}{6} \\
&= \frac{2k^3 + 9k^2 + 13k + 6}{6} \\
&= \frac{(k^2 + 3k + 2)(2k + 3)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.
\end{aligned}$$

b) *Induktionsanfang:* Es gilt

$$0^3 = 0 = \left(\frac{0 \cdot (0+1)}{2}\right)^2.$$

Induktionsschritt: Sei $k \geq 0$ beliebig.
Induktionsvoraussetzung: Für k gelte $0^3 + 1^3 + 2^3 + \ldots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$.
Induktionsschluss: Es gilt

$$\begin{aligned}
0^3 + 1^3 + \ldots + k^3 + (k+1)^3 &= (0^3 + 1^3 + \ldots + k^3) + (k+1)^3 \\
&= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \qquad \text{(Ind.-Vor.)} \\
&= \frac{k^2(k+1)^2 + 4(k+1)^3}{4}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{(k^2 + 4(k+1))(k+1)^2}{4} \\
&= \frac{(k^2 + 4k + 4)(k+1)^2}{4} \\
&= \frac{(k+2)^2(k+1)^2}{4} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2.
\end{aligned}
$$

c) *Induktionsanfang:* Es ist $4! = 24 > 16 = 2^4$.
Induktionsschritt: Sei nun $k \geq 4$ beliebig.
Induktionsvoraussetzung: Es gelte $k! > 2^k$.
Induktionsschluss: Es ist $(k+1)! = k! \cdot (k+1)$. Mit Hilfe der Induktionsvoraussetzung folgt nun $(k+1)! = k! \cdot (k+1) > 2^k \cdot (k+1) > 2^k \cdot 2 = 2^{k+1}$.

d) *Induktionsanfang:* Es gilt $\sqrt{4} \cdot 4 = 2 \cdot 4 = 8 > 6 = 2 + 4 = \sqrt{4} + 4$.
Induktionsschritt: Sei nun $k \geq 4$ beliebig.
Induktionsvoraussetzung: Für k gelte $\sqrt{k} \cdot k > \sqrt{k} + k$.
Induktionsschluss: Es gilt

$$
\begin{aligned}
\sqrt{k+1} \cdot (k+1) &= \sqrt{k+1} \cdot k + \sqrt{k+1} \\
&> \sqrt{k} \cdot k + \sqrt{k+1} \\
&> \sqrt{k} + k + \sqrt{k+1} && \text{(Ind.-Vor.)} \\
&> k + 1 + \sqrt{k+1}.
\end{aligned}
$$

e) *Induktionsanfang:* Es ist $0^2 + 0 = 0$, also ist $0^2 + 0$ gerade.
Induktionsschritt: Sei nun $k \geq 0$ beliebig.
Induktionsvoraussetzung: Wir nehmen an, $k^2 + k$ ist eine gerade Zahl, d. h. es gibt ein $m \in \mathbb{Z}$, so dass $k^2 + k = 2m$.
Induktionsschluss: Es gilt

$$
\begin{aligned}
(k+1)^2 + k + 1 &= k^2 + 3k + 2 \\
&= (k^2 + k) + 2k + 2 \\
&= 2m + 2k + 2 && \text{(Ind.-Vor.)} \\
&= 2 \cdot (m + k + 1).
\end{aligned}
$$

Somit ist $(k+1)^2 + k + 1$ gerade.

f) *Induktionsanfang:* Für ein beliebiges $x \in \mathbb{R}$ gilt $(1+x)^0 = 1 \geq 1 = 1 + 0 \cdot x$.
Induktionsschritt: Sei nun $k \in \mathbb{N}$ beliebig.
Induktionsvoraussetzung: Für k gelte $(1+x)^k \geq 1 + kx$.
Induktionsschluss: Es gilt $(1+x)^{k+1} = (1+x)^k \cdot (1+x) \geq (1+kx)(1+x) = 1 + (k+1)x + kx^2 \geq 1 + (k+1)x$.

2.4.2 *Induktionsanfang:* Ein Geldbetrag von genau vier Cent kann mit zwei Zweicentstücken bezahlt werden.

Induktionsschritt:

Induktionsvoraussetzung: Wir nehmen an, ein beliebiger Geldbetrag von k Cent mit $k \geq 4$ lässt sich allein mit Zwei- und Fünfcentstücken bezahlen.

Induktionsschluss: Wir zeigen mit Hilfe der Induktionsvoraussetzung, dass auch ein Geldbetrag von $(k+1)$ Cent allein mit Zwei- und Fünfcentstücken bezahlt werden kann. Nach Induktionsvoraussetzung gibt es eine Stückelung von k Cent, die nur aus Zwei- und Fünfcentmünzen besteht. Da nach Voraussetzung $k \geq 4$ gilt, muss diese Stückelung ein Fünfcentstück oder zwei Zweicentstücke enthalten. Enthält die Stückelung von k ein Fünfcentstück, dann entfernen wir es und legen stattdessen drei Zweicentstücke hinzu. Auf diese Weise erhalten wir eine Stückelung für $(k+1)$ Cent. Enthält die Stückelung für k Cent zwei Zweicentstücke, dann entfernen wir diese und legen stattdessen ein Fünfcentstück hinzu. Auch in diesem Fall erhalten wir also eine Stückelung für $(k+1)$ Cent.

2.4.3 Wir müssen zeigen, dass für jedes $n \geq 8$ zwei natürliche Zahlen $s, t \in \mathbb{N}$ existieren, so dass $n = 3s + 5t$ gilt. Hierzu führen wir einen Induktionsbeweis mit Schrittweite 3, d. h. wir zeigen zunächst, dass die Aussage für die ersten drei Zahlen 8, 9 und 10 gilt und beweisen dann, dass sie, falls sie für eine Zahl $k \geq 8$ gilt, auch für $k + 3$ gelten muss.

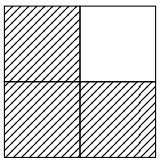
Induktionsanfang: Die Behauptung gilt für 8, 9 und 10, denn es ist $8 = 3 \cdot 1 + 5 \cdot 1$, $9 = 3 \cdot 3 + 5 \cdot 0$ und $10 = 3 \cdot 0 + 5 \cdot 2$.

Induktionsschritt: Sei nun $k \geq 8$ beliebig.

Induktionsvoraussetzung: Wir nehmen an, es gibt $s, t \in \mathbb{N}$, so dass $k = 3s + 5t$.

Induktionsschluss: Aus der Induktionsvoraussetzung folgt $k + 3 = 3s + 5t + 3 = 3(s + 1) + 5t$. Somit lässt sich $k + 3$ als Summe von Dreien und Fünfen schreiben.

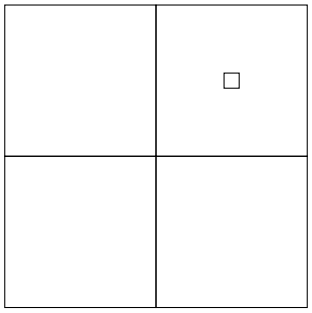
2.4.4 *Induktionsanfang:* Sei $n = 1$. Dann hat unser Schachbrett die Seitenlänge 2 und besteht aus 4 Feldern. Wir können ohne Beschränkung der Allgemeinheit davon ausgehen, dass das Feld oben rechts entfernt wurde. Offensichtlich können wir dann die drei verbleibenden Felder mit einem L-förmigen Stein wie folgt bedecken:



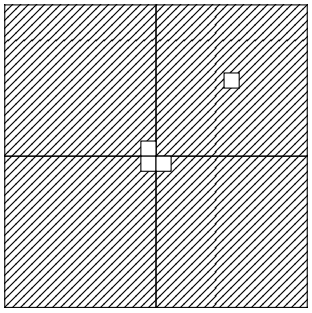
Induktionsschritt: Sei nun $k \geq 1$ beliebig.

Induktionsvoraussetzung: Wir nehmen an, wir können ein $(2^k \times 2^k)$-Schachbrett, aus dem ein beliebiges Feld entfernt wurde, vollständig mit L-förmigen Steinen bedecken.

Induktionsschluss: Wir betrachten nun ein Schachbrett mit Seitenlänge 2^{k+1}. Wegen $2^{k+1} = 2 \cdot 2^k$ besteht das Schachbrett aus vier kleineren Schachbrettern, die jeweils die Seitenlänge 2^k besitzen. Wir nehmen ohne Beschränkung der Allgemeinheit an, dass sich das entfernte Feld im oberen rechten Teil befindet:



Nach Induktionsvoraussetzung können wir nun jedes der vier $(2^k \times 2^k)$-Schachbretter so mit L-förmigen Steinen bedecken, dass ein beliebiges Feld frei bleibt. Insbesondere können wir also das gesamte Brett wie folgt bedecken:



Indem wir nun das Loch in der Mitte mit einem weiteren L-förmigen Stein füllen, erhalten wir die gewünschte Bedeckung des Schachbretts.

2.4.5 Die Anzahl der a's in $u \in \Sigma^*$ kann induktiv wie folgt definiert werden:
(1) $|\lambda|_a := 0$,
(2) $|wx|_a := \begin{cases} |w|_a + 1, & \text{falls } x = a, \\ |w|_a & \text{falls } x \neq a. \end{cases}$
Analog lässt sich die Anzahl der b's in $u \in \Sigma^*$ induktiv definieren:
(1) $|\lambda|_b := 0$,
(2) $|wx|_b := \begin{cases} |w|_b + 1, & \text{falls } x = b, \\ |w|_b & \text{falls } x \neq b. \end{cases}$

2.4.6 *Induktionsanfang:* Sei $u = \lambda$. Dann gilt $|u| = |\lambda| = 0 = 0 + 0 = |\lambda|_a + |\lambda|_b = |u|_a + |u|_b$.

Induktionsschritt:

Induktionsvoraussetzung: Für ein beliebiges Wort $w \in \Sigma^*$ gelte $|w| = |w|_a + |w|_b$.

Induktionsschluss: Wir zeigen, dass $|wx| = |wx|_a + |wx|_b$ für jeden Buchstaben $x \in \Sigma$ gilt. Sei also $x \in \Sigma$ ein beliebiger Buchstabe. Wir unterscheiden die folgenden Fälle:

1. Fall: $x = a$. Dann ist $|wx|_a = |w|_a + 1$ und $|wx|_b = |w|_b$. Damit erhalten wir

$$\begin{aligned} |wx| &= |w| + 1 \\ &= |w|_a + |w|_b + 1 && \text{(Ind-Vor.)} \\ &= |w|_a + 1 + |w|_b \\ &= |wx|_a + |wx|_b. \end{aligned}$$

2. Fall: $x \neq a$, d. h. $x = b$. Dann ist $|wx|_a = |w|_a$ und $|wx|_b = |w|_b + 1$. Damit erhalten wir

$$\begin{aligned} |wx| &= |w| + 1 \\ &= |w|_a + |w|_b + 1 && \text{(Ind-Vor.)} \\ &= |wx|_a + |wx|_b. \end{aligned}$$