Brückenkurs

Mathematik für Informatiker

im Wintersemester 2016/17

Freie Universität Berlin

Institut für Informatik

Klaus Kriegel (bearbeitet von Max Willert)

Ergänzende Literatur:

C. Meinel, M. Mundhenk, Mathematische Grundlagen der Informatik, B.G.Teubner

K. Rosen, Discrete Mathematics and its Applications McGraw-Hill

P. Hartmann, Mathematik für Informatiker, Vieweg-Verlag

D. Hachenberger, Mathematik für Informatiker, Pearson

Einführende Bemerkungen

Dieser Brückenkurs soll Studienanfängern der Informatik und der Bioinformatik den Einstieg in das Studium erleichtern. Leider wird der Anteil und das Gewicht der Mathematikausbildung in den genannten Studiengängen von vielen Studierenden bei der Wahl des Fachs unterschätzt. Später bilden die Mathematikvorlesungen für die Mehrheit der Studenten eine der größten Herausforderungen im Studium. Das liegt zum Einen an den mitgebrachten Vorkenntnissen und Fertigkeiten, die leider häufig - selbst bei sehr elementaren Themen - große Lücken aufweisen. Es geht aber jetzt nicht darum, diesen Zustand zu beklagen, sondern ausgehend von diesem Fakt nach Wegen zu suchen, um die vorhandenen Defizite möglichst effektiv abzubauen. Als zweite Ursache für die Probleme insbesondere am Studienanfang kann man den Umstieg von der Schulmathematik (in deren Realität sich das Rechnen von Beispielen oft so in den Vordergrund schiebt, dass die dahinter stehende Theorie ungenügend wahrgenommen wird) auf die Art der Mathematikvermittlung, wie sie an der Universität üblich ist (in der Vorlesung geht es vorwiegend um die theoretischen Grundlagen des entsprechenden Gebiets und Beispiele werden vor allem in den Tutorien besprochen), ausmachen.

Der Brückenkurs versucht an beiden Punkten anzusetzen. Einerseits werden wir einige Themen aus der Schulmathematik auffrischen und zum Teil aus einem neuen, mehr theoretischen Blickwinkel betrachten. Letzteres bedeutet, dass man nicht nur die Fakten kennt, sondern sie auch beweisen kann, denn das macht einen Hauptunterschied zwischen der Schulmathematik und der Mathematik im Studium aus. Andererseits wird der Brückenkurs aber auch schon einen Vorgriff auf einige Inhalte aus den ersten Mathematik-Vorlesungen machen, um die steile Lernkurve im ersten Semester etwas abzuflachen. Es geht dabei aber nicht um eine Doppelvermittlung der Inhalte. Vielmehr werden wir uns im Brückenkurs auf die Vorstellung von Ideen und Konzepten anhand von Beispielen konzentrieren, so dass die theoretische Untermauerung dieser Inhalte in den Vorlesungen leichter verständlich wird.

Keinesfalls sollte man sich dazu verleiten lassen, nach dem Brückenkurs die ersten Vorlesungen ausfallen zu lassen, weil man meint, die Inhalte schon ausreichend zu kennen. Dabei geht der rote Faden sehr schnell verloren und gerade das sollte auf keinen Fall passieren. Deshalb ein paar Ratschläge zum Schlus:

- Lassen Sie sich von der kritischen Zustandsbeschreibung aus dem oberen Abschnitt nicht entmutigen. Sie haben es selbst in der Hand, die Mathematik-Module erfolgreich abzuschließen, sogar dann, wenn Sie Ihre mathematische Vorbildung als eher schwach einschätzen. Sie müssen dafür nur ausreichende Zeitressourcen einplanen und bereit sein, sich auf abstraktes Denken einzulassen. In der Regel fehlt es nämlich nicht an der Fähigkeit zum abstrakten Denken sondern an dem Mut und der Bereitschaft, es einfach zu tun.

- Besuchen Sie die Vorlesungen und bemühen Sie sich schon im laufenden Semester, den Stoff reglmäßig nachzuarbeiten. Die Inhalte bauen aufeinander auf und wer

die Definitionen aus der letzten Vorlesung nicht kennt, wird beim nächsten Termin bald nicht mehr folgen können und irgendwann nur noch gelangweilt auf das Ende der Vorlesung warten - das ist vergeudete Zeit. Wer aber in der Lage ist, den Gedankengängen in der Vorlesung wenigstens in den wesentlichen Zügen zu folgen, für den sollte der Vorlesungsbesuch ein echter Gewinn sein, den man nicht einfach duch ein zweifaches Lesen des Vorlesungsskripts kompensieren kann.

- Nutzen Sie auf eine aktive Weise die vielfältigen Angebote, die im Fachbereich für Studienanfänger zur Verfügung gestellt werden. Das aufmerksame Zuhören in den Lehrveranstaltungen ist gut, aber Sie sollten auch Fragen stellen und gemeinsam mit anderen Probleme diskutieren. Der Brückenkurs ist nur ein erster Baustein. Im Semester werden ergänzend zur Vorlesung und den Tutorien auch noch die sogenannten Wunschkonzerte angeboten, in denen man Hinweise zu seinen Problemen in den Vorlesungen und Übungen bekommen kann.

1 Grundbegriffe der Logik

1.1 Aussagen

Die Grundlagen der Aussagenlogik gehen bereits auf die alten Griechen zurück. So beschrieb Aristoteles eine Aussage als einen Satz, von dem es sinnvoll sei zu sagen, dass er wahr oder falsch ist. Diesen Gedanken findet man auch in der heute verwendeten Definition wieder:

Definition: Eine *Aussage* ist ein (formal-) sprachliches Gebilde, das entweder wahr oder falsch ist.

Der Zusatz formalsprachlich weist darauf hin, dass man auch mathematische Symbole und andere Zeichen einer formalen Sprache verwenden kann. Die klassische Aussagenlogik beruht auf zwei Grundprinzipien, dem bereits genannten *Zweiwertigkeitsprinzip*, welches fordert, dass jede Aussage einen eindeutig bestimmten Wahrheitswert hat, der nur *wahr* oder *falsch* sein kann, und dem *Extensionalitätsprinzip*, nach dem der Wahrheitswert einer zusammengesetzten Aussage nur von den Wahrheitswerten ihrer Bestandteile abhängt.

Wir werden im Folgenden (wie in der Informatik üblich) eine 1 für den Wahrheitswert *wahr* und eine 0 für *falsch* verwenden. Das Zusammensetzen von Aussagen erfolgt durch die Verwendung von Verknüpfungswörtern wie *und, oder, nicht, wenn ... dann*, welche auf formal-sprachlicher Ebene durch sogenannte *logische Junktoren* - das sind spezielle Verknüpfungssymbole - dargestellt werden.

Beispiele:

1. Der Satz *"7 ist eine Primzahl."* und der Satz *"7 ist eine ungerade Zahl."* sind wahre Aussagen. Dagegen ist der Satz *"7 ist eine gerade Zahl."* eine falsche Aussage. Genauer gesehen ist der letzte Satz die Negation des zweiten Satzes, denn *nicht ungerade* zu sein, ist (zumindest für ganze Zahlen) das gleiche, wie *gerade* zu sein.

2. Der Satz *"7 ist eine Primzahl und 7 ist ungerade."* sowie der Satz *"7 ist eine Primzahl oder 7 ist gerade."* sind wahre Aussagen. Achtung: Auch der Satz *"7 ist eine Primzahl oder 7 ist ungerade."* ist eine wahre Aussage, denn das logische *oder* ist kein ausschließendes *entweder oder*. Dagegen ist der Satz *"7 ist eine Primzahl und 7 ist gerade."* eine falsche Aussage, denn die zweite Aussage ist falsch.

3. Der Satz *"$\sqrt{2}$ ist eine rationale Zahl."* ist – wie man aus der Schulmathematik weiß – eine falsche Aussage, aber es bedarf schon einiger Überlegungen, um das zu zeigen.

4. Der Satz *"Jede gerade Zahl größer als 2 ist die Summe zweier Primzahlen"* ist eine Aussage, denn entweder gibt es eine gerade Zahl, die sich nicht als Summe zweier Primzahlen darstellen lässt - dann ist die Aussage falsch, oder es gibt keine solche Zahl - dann ist die Aussage wahr. Man nimmt an, dass die

Aussage wahr ist (Goldbachsche Vermutung), konnte das aber bisher noch nicht beweisen.

5. Der Satz *"Dieser Satz ist falsch."* ist als Russels Paradoxon bekannt. Durch die spezielle Art des Bezugs auf sich selbst kann er weder wahr noch falsch sein und ist deshalb **keine** Aussage.

6. Ein typischer Vertreter für eine ganze Klasse von sprachlichen Gebilden, die keine Aussagen sind, ist der Satz *"Die natürliche Zahl n ist eine Primzahl."*. Setzen wir für n den Wert 7 ein, so entsteht offensichtlich eine wahre Aussage, dagegen für $n = 8$ eine falsche Aussage. Sprachliche Gebilde dieses Typs nennt man auch Aussageformen oder Prädikate - wir werden sie später genauer besprechen.

Nach dem Extensionalitätsprinzip ergibt sich der Wahrheitswert einer zusammengesetzten Aussage ausschließlich aus den Wahrheitswerten der Ausgangskomponenten. Deshalb werden wir uns zuerst damit beschäftigen, welche Operationen zum Zusammensetzen neuer Aussagen verwendet werden sollen und wie diese Operationen auf Wahrheitswerten wirken. Dazu werden Aussagevariable eingeführt und die Wahrheitwerte von zusammengesetzten Aussagen durch sogenannte Wahrheitswerttabellen (kurz Wahrheitstafeln) zu beschreiben. Die Negation einer Aussage x wird mit $\neg(x)$ bezeichnet. Diese Operation kehrt den Wahrheitswert von x um, d.h. man kann sie als Wahrheitswertfunktion $\neg : \{0,1\} \longrightarrow \{0,1\}$ mit $\neg(0) = 1$ und $\neg(1) = 0$ beschreiben. Zur Verknüpfung von zwei Aussagen x und y stehen die folgenden Konstrukte zur Verfügung:

- die *Konjunktion* $x \wedge y$, gesprochen "x *und* y";
- die *Disjunktion* $x \vee y$, gesprochen "x *oder* y";
- die *Implikation* $x \rightarrow y$, gesprochen "$aus\ x\ folgt\ y$"
- die *Äquivalenz* $x \leftrightarrow y$, gesprochen "$x\ genau\ dann,\ wenn\ y$"),
- die *Antivalenz* $x \oplus y$, gesprochen "*entweder* x *oder* y".

Die dazu korrespondierenden Funktionen auf Wahrheitswerten werden als Operationen (unter Verwendung der gleichen Symbole) in der folgenden Tabelle beschrieben:

x	y	$x \wedge y$	$x \vee y$	$x \rightarrow y$	$x \leftrightarrow y$	$x \oplus y$
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	0

Aus der Tabelle kann man ablesen, dass die Konjunktion $x \wedge y$ dann und nur dann wahr ist, wenn beide Aussagen x und y wahr sind. Die Disjunktion $x \vee y$ ist dann und

nur dann wahr, wenn mindestens eine der Aussagen x und y wahr ist. Die Implikation ist dann und nur dann wahr, wenn x falsch oder y wahr ist. Versuchen Sie selbst, die Äquivalenz und die Antivalenz verbal zu beschreiben!

Ausdrücke, die durch (wiederholtes) Anwenden der Verknüpfungsoperationen aus Variablen gewonnen werden, nennt man *Formeln* (oder *Terme*) der Aussagenlogik. Um eine Formel eindeutig erkennen zu können, müsste man jeweils nach Anwendung einer Verknüpfung die neue Formel durch ein Klammerpaar einschließen. Das führt zur folgenden Definition von Formeln der Aussagenlogik über eine Variablenmenge Var:

1. Alle Variablen aus der Menge Var sowie die Symbole 0 und 1 sind Formeln der Aussagenlogik. Diese Formeln nennt man auch Primformeln.

2. Ist t eine Formel der Aussagenlogik, dann ist auch $(\neg t)$ eine Formel der Aussagenlogik.

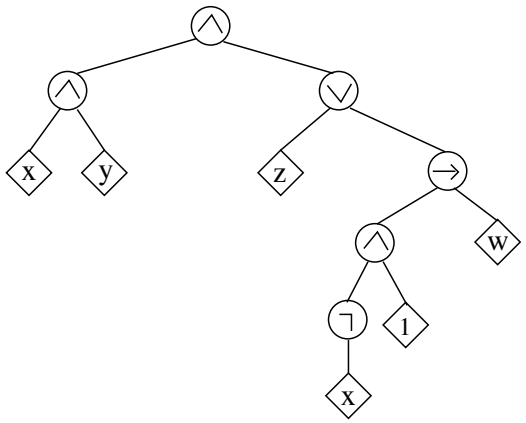
3. Sind s und t Formeln der Aussagenlogik, dann sind auch die Ausdrücke $(s \wedge t)$, $(s \vee t)$, $(s \rightarrow t)$ sowie $(s \leftrightarrow t)$ Formeln der Aussagenlogik.

4. Jede Formel der Aussagenlogik kann aus den Variablen und den Symbolen 0 und 1 durch eine endliche Folge von Anwendungen der Regeln 2) und 3) erzeugt werden.

Anmerkungen zur Defintion:

1. Formeln, die nur durch Negation, Konjunktion und Disjunktion gebildet werden, nennt man Boolesche Formeln. Sie spielen eine besondere Rolle, denn wie wir später sehen werden, kann man alle Formeln der Aussagenlogik durch logisch äquivalente Boolesche Formeln ausdrücken. Die Antivalenz wird üblicherweise nicht zu den Standardoperationen der Aussagenlogik gezählt, aber da sie in der Informatik eine wichtige Rolle spielt, wurde sie in unsere Übersicht der logischen Verknüpfungsoperationen aufgenommen.

2. Um eine anschauliche Darstellung des Aufbaus einer Formel zu bekommen, kann man den sogenannten Syntaxbaum der Formel zeichnen. Primformeln bestehen nur aus einem rautenförmingen Knoten mit der Bezeichnung der entsprechenden Variable bzw. dem Symbol 0 oder 1. Ein Term der Form $(\neg t)$ wird durch einen kreisförmigen Knoten mit den Negationssymbol dargestellt unter dem der Syntaxbaum von t gezeichnet wird. Ein Term der Form $(s \wedge t)$ (und analog für die andere Operationen) wird durch einen kreisförmigen Knoten mit dem entsprechenden Symbol dargestellt unter dem linksseitig der Syntaxbaum von s und rechtsseitig der Syntaxbaum von t gezeichnet wird. Das folgende Beispiel zeigt den Syntaxbaum der Formel $((x \vee y) \wedge (z \vee (((\neg x) \wedge 1) \rightarrow w)))$.



3. In der Aussagenlogik kann man die Begriffe Formel und Term als Synomyme verwenden, das erklärt auch die Wahl der Bezeichner s und t für Formeln der Aussagenlogik. Man sollte aber schon an dieser Stelle daruaf hinweisen, dass es in der sogenannten Prädikatenlogik sehr wohl einen Unterschied zwischen Termen und Formeln gibt.

4. Weil die Formeln durch die Klammersetzung sehr unübersichtlich werden können, vereinbart man einige Regeln zur Vereinfachung der Notation (ähnlich wie die bekannte Regel, dass Punktrechnung vor Strichrechnung geht):

   - Außenklammern können weggelassen werden.
   - In der Reihenfolge $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ trennen die hinteren Junktoren stärker als alle vorangehenden, d.h. die *Bindungsstärke* nimmt in dieser Reihenfolge ab. Alle Klammerungen, die mit dieser Hierarchie der Bindungsstärke in Übereinstimmung stehen, können auch weggelassen werden.

Beispiel: Man kann $((\neg x_1) \vee (x_2 \wedge x_3))$ auch $\neg x_1 \vee x_2 \wedge x_3$ schreiben. Dagegen würde das Weglassen der Klammern in der Formel $\neg(x \vee y)$ eine andere Formel erzeugen.

Übung:
1) Streichen Sie aus der Formel $((x \vee y) \wedge (z \vee (((\neg x) \wedge 1) \rightarrow w)))$ alle verzichtbaren Klammerpaare!
2) Ergänzen Sie in der Formel $\neg x_1 \vee x_2 \wedge x_3 \leftrightarrow x_1 \wedge x_3 \vee x_4 \rightarrow \neg x_2$ die vollständige Klammerung!

1.2 Semantik der Ausagenlogik

Bisher haben wir nur die Regeln besprochen, wie man Boolesche Formeln bzw. Formeln der Aussagenlogik korrekt als rein formale Ausdrücke bilden kann. Solche Regeln zur Beschreibung der äußeren Gestalt von formalen Ausücken nennt man *syntaktische Regeln* und das in der Defintion zusammengestellt Gesamtregelwerk die *Syntax der Aussagenlogik*.

Man verfolgt aber mit diesem Ansatz ein gößeres Ziel: Eine Formel hat auch einen Inhalt, sie bekommt eine innere Bedeutung dadurch, dass jede Belegung der Variablen der Formel mit konkreten Wahrheitswerten zu einem Wahrheitswert der gesamten Formel ausgewertet werden kann. Diese Interpretation von Formeln nennt man die Semantik der Aussagenlogik.

Eine ähnliche Vorgehensweise kennen wir bereits von arithmetischen Termen. So ist beispielsweise $t = x^2 + xy$ ein (nach vereinbarten Vereinfachungsregeln) korrekter arithmetischer Term, der in ursprünglicher Form die Gestalt $t = ((x \cdot x) + (x \cdot y))$ hatte (im Gegensatz dazu sind $x + \cdot z$ und $z+$ keine syntaktisch korrekten Terme). Die Interpretation von t erfolgt durch Einsetzen von Werten (Zahlen) für x und y und Auswertung von t durch Ausführung der arithmetischen Operationen wie z.B. $2 \mapsto x, 3 \mapsto y \rightsquigarrow (2 \cdot 2) + (2 \cdot 3) = 4 + 6 = 10 \mapsto t$.

Analog kann man für alle in einer Booleschen Formel auftretenden Variablen Wahrheitswerte festlegen und durch Auswertung der einzelnen logischen Operationen einen Wahrheitswert für die Formel berechnen. Man nennt diesen induktiven Prozess auch *Auswertung* der Formel. Da der Auswertungsprozess im Syntaxbaum von den Blättern hin zur Wurzel erfolgt, spricht man hier von einer Bottom-up-Prozedur. Im Gegensatz zu arithmetischen Termen gibt es für Formeln der Aussagenlogik nur endlich viele Belegungen der Variablen mit Wahrheitswerten, denn jede Variable kann nur zwei verschiedene Werte annehmen. Man kann sich leicht davon überzeugen, dass es für eine Formel mit k verschiedenen Variablen genau 2^k Belegungen gibt. Somit können die Ergebnisse der Auswertungen dieser Formel unter allen möglichen Belegungen in einer sogenannten Wahrheitstafel mit 2^k Zeilen zusammengefasst werden.

Definition: Zwei Formeln s und t sind *logisch äquivalent*, wenn jede beliebige Belegung der Variablen für beide Formeln den gleichen Wahrheitswert induziert. Wir schreiben dafür $s \equiv t$.

Wie das folgende Beispiel zeigt, kann die Äquivalenz von zwei Formeln prinzipiell durch Wahrheitstafeln überprüft werden: Man stelle fest, ob die Formeln
$s = \neg(x_1 \vee ((x_1 \vee x_2) \wedge x_2))$ und $t = \neg x_1 \wedge \neg x_2$ logisch äquivalent sind!

x_1	x_2	$x_1 \vee x_2$	$(x_1 \vee x_2) \wedge x_2$	$x_1 \vee ((x_1 \vee x_2) \wedge x_2)$	s
0	0	0	0	0	1
0	1	1	1	1	0
1	0	1	0	1	0
1	1	1	1	1	0

x_1	x_2	$\neg x_1$	$\neg x_2$		t
0	0	1	1		1
0	1	1	0		0
1	0	0	1		0
1	1	0	0		0

Wie man sieht, ist der Wahrheitswerteverlauf für s und t identisch, die Formeln sind also äquivalent.

Übung: Überprüfen Sie, ob die Formeln $s = x \wedge y \to x \wedge z$ und $t = y \to z$ logisch äquivalent sind!

Satz: Für beliebige Formeln s, t, r gelten die folgenden Äquivalenzen:

Assoziativität:	$(s \wedge t) \wedge r$	$\equiv$	$s \wedge (t \wedge r)$
	$(s \vee t) \vee r$	$\equiv$	$s \vee (t \vee r)$
Kommutativität:	$s \wedge t$	$\equiv$	$t \wedge s$
	$s \vee t$	$\equiv$	$t \vee s$
Distributivität:	$s \wedge (t \vee r)$	$\equiv$	$(s \wedge t) \vee (s \wedge r)$
	$s \vee (t \wedge r)$	$\equiv$	$(s \vee t) \wedge (s \vee r)$
Idempotenz:	$s \wedge s$	$\equiv$	s
	$s \vee s$	$\equiv$	s
Dominanz:	$s \wedge 0$	$\equiv$	0
	$s \vee 1$	$\equiv$	1
Neutralität:	$s \wedge 1$	$\equiv$	s
	$s \vee 0$	$\equiv$	s
Absorption:	$s \wedge (s \vee t)$	$\equiv$	s
	$s \vee (s \wedge t)$	$\equiv$	s
deMorgansche Regel:	$\neg(s \wedge t)$	$\equiv$	$\neg s \vee \neg t$
	$\neg(s \vee t)$	$\equiv$	$\neg s \wedge \neg t$
Komplementierung:	$s \wedge \neg s$	$\equiv$	0
	$s \vee \neg s$	$\equiv$	1
(doppelte Negation)	$\neg\neg s$	$\equiv$	s

Diese Äquivalenzen können leicht mit Wahrheitstafeln bewiesen werden. Der Wahrheitstafelmethode sind jedoch enge Grenzen gesetzt, wenn die Anzahl n der verwendeten Variablen groß wird, denn die entsprechende Wahrheitstafel hat dann 2^n Zeilen.

Beispiel: Der Beweis der folgenden Äquivalenz mit Wahrheitstafeln würde 16 Zeilen erfordern. Verwendet man dagegen die Absorption und die doppelte Negation zur Ersetzung von Subformeln, so erhält man einen einfachen und kurzen Beweis.

$$\begin{aligned} x_1 \vee ((x_2 \vee x_3) \wedge \neg(\neg x_1 \wedge (\neg x_1 \vee x_4))) &\equiv x_1 \vee ((x_2 \vee x_3) \wedge \neg\neg x_1) \\ &\equiv x_1 \vee ((x_2 \vee x_3) \wedge x_1) \\ &\equiv x_1 \end{aligned}$$

Übungen:
1) Untersuchen Sie, ob die Operationen $\to$ und $\leftrightarrow$ assoziativ und/oder kommutativ sind.
2) Gibt es für die Operation $\leftrightarrow$ ein neutrales Element?

Die folgende Liste enthält weitere Äquivalenzen, welche zum Beweis der Äquivalenz

von komplexen Formeln häufig angewendet werden:

$$\begin{array}{lrcl}
(1) & s \to t & \equiv & \neg s \vee t \\
(2) & s \leftrightarrow t & \equiv & s \wedge t \vee \neg s \wedge \neg t \\
(3) & s \to t \wedge r & \equiv & (s \to t) \wedge (s \to r) \\
(4) & s \to t \vee r & \equiv & (s \to t) \vee (s \to r) \\
(5) & s \wedge t \to r & \equiv & (s \to r) \vee (t \to r) \\
(6) & s \vee t \to r & \equiv & (s \to r) \wedge (t \to r)
\end{array}$$

Definition: Eine Formel s wird erfüllbar genannt, wenn es eine Belegung der Variablen von s gibt, die für s den Wert 1 induziert. Die Formel s wird *allgemeingültig, logisch gültig* oder eine *Tautologie* genannt, wenn sie für jede Belegung den Wert 1 annimmt. Eine Formel, die unerfüllbar ist, wird *Kontradiktion* genannt.

Übungen:
1) Begriffsverständnis: Begründen Sie, dass zwei aussagenlogische Formeln s und t genau dann logisch äquivalent sind, wenn die Formel $r = s \leftrightarrow t$ eine Tautologie ist.
2) Beweisen Sie, dass die Formeln $(x \to y \wedge z) \wedge (y \to x \wedge z) \wedge (z \to x \wedge y) \wedge (x \vee y \vee z)$ und $x \wedge y \wedge z$ logisch äquivalent sind.

1.3 Prädikate und Quantoren

Definition: Ein *Prädikat* ist eine Aussageform, die eine (oder mehrere) Variable enthält, so dass bei Ersetzung der Variablen durch Elemente aus einem gegebenen Individuenbereich U eine Aussage mit eindeutig bestimmtem Wahrheitswert entsteht, z.B. $P(x)$: "$x = 0$" oder $Q(x)$:"$x + 0 = x$" oder $R(x, y)$:"$x + y = x$" für den Bereich der ganzen Zahlen.

Die Belegung der Variablen durch konkrete Objekte ermöglicht somit (durch Betrachtung eines Spezialfalls), ein Prädikat in eine Aussage umzuwandeln. So sind $P(2)$ und $R(1, 1)$ falsche Aussagen, wogegen $Q(4)$ und $R(2, 0)$ wahr sind.

Die sogenannten *Quantoren* erlauben es, aus diesen Spezialfällen allgemeinere Aussagen abzuleiten: Durch das Hinzufügen der Wendungen "für alle ...", symbolisch durch den *Allquantor* $\forall$, oder "es gibt ein ...", symbolisch durch den *Existenzquantor* $\exists$, werden die Variablen in einem Prädikat *gebunden*. Sind alle Variablen eines Prädikats gebunden, entsteht eine Aussage, also ein Satz, der wahr oder falsch ist.

Die Ausssage "$\forall x \in U \quad P(x)$" ist wahr, wenn für jedes Element $a \in U$ die Aussage $P(a)$ wahr ist. Dagegen ist "$\exists x \in U \quad P(x)$" eine wahre Aussage, wenn (mindestens) ein Element $a \in U$ existiert, so dass die Aussage $P(a)$ wahr ist.

Beispiele:

- Die Aussagen "$\forall x \in \mathbb{N} \quad x + 0 = x$" und "$\exists x \in \mathbb{N} \quad x^2 = x$" sind wahr, aber die Aussagen "$\exists x \in \mathbb{N} \quad x + 1 = x$" und "$\forall x \in \mathbb{N} \quad x^2 = x$" sind falsch.

- Die Aussage "$\forall x \in \mathbb{N}\ \exists y \in \mathbb{N} \quad y \leq x$" ist wahr, denn für einen beliebigen Wert $x = a$ erfüllt der Wert $y = a$ die Ungleichung $y \leq x$. Dagegen ist die Aussage

"$\forall x \in \mathbb{N}\ \exists y \in \mathbb{N} \quad y < x$" falsch, denn für $x = 0$ gibt es keine kleinere natürliche Zahl.

- Die falsche Aussage im letzten Punkt ist ein typisches Beispiel dafür, dass der Bereich, über dem die Aussage gemacht wird, von entscheidender Bedeutung sein kann: Wenn man den Bereich $\mathbb{N}$ der natürlichen Zahlen gegen die Bereiche $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ der ganzen, rationalen bzw. reellen Zahlen austauscht, entstehen offensichtlich wahre Aussagen wie "$\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z} \quad y < x$".

Allgemein ist die Frage, ob eine durch Quantoren gebildete Aussage wahr oder falsch ist, algorithmsch nicht entscheidbar. Die Goldbachsche Vermutung ist ein Beispiel einer Aussage, deren Wahrheitswert nicht bekannt ist. In vielen anderen Fällen kann man die Frage aber durch genauere Überlegungen beantworten. Wie kann man in solchen Fällen sich selbst und andere von der Richtigkeit seiner Überlegungen überzeugen? Der typische Beweis dafür, dass eine quantisierte Aussage wahr ist, erfolgt in drei Stufen. Zuerst wird die Aussage durch Anwendung von äquivalenten Umformungen aus der Aussagenlogik und aus dem nachfolgenden Satz in eine Standardform gebracht, bei der alle auftretenden Quantoren am Anfang stehen (man nennt dies eine *Pränexform*). Danach erfolgt die Belegung der Variablen in Form eines Spiels zwischen zwei Parteien: Einem *Beweiser* und seinem *Gegenspieler*, der nachzuweisen versucht, dass die Ausage falsch ist. Dabei darf der Gegenspieler bei jedem Allquantor die entsprechende Variable x durch ein beliebiges Objekt a aus dem Individuenbereich belegen. Sollte die Aussage doch falsch sein (also nicht für alle Objekte gelten), würde der Gegenspieler gerade ein solches Objekt wählen. Ist die Aussage wahr, dann ist es (für den Beweiser) egal, welches Objekt a der Gegenspieler gewählt hat. Der Beweiser ist bei allen Existenzquantoren am Zuge und muss ein passendes Objekt (in Abhängigkeit von den vorher vom Gegenspieler gewählten Objekten) finden, für welches die nachfolgende Ausssage wahr ist. Nachdem alle Variablen belegt sind, haben wir eine (variablenfreie) Aussage. Im letzten Schritt muss diese Aussage verifiziert (als wahr bewiesen) werden.

Bevor wir uns die Umformungsregeln genauer ansehen, wollen wir das Spiel zwischen dem Beweiser und seinem Gegenspieler an einem einfachen Beispiel besprechen, das bereits in Pränexform ist:

$$\forall x \in \mathbb{N} \quad \exists y \in \mathbb{N} \quad (x+1)^2 < y < (x+2)^2$$

Mit anderen Worten beschreibt das die Behauptung, dass man zwischen zwei Gliedern der Quadratzahlenfolge $1, 4, 9, 16, \ldots$ immer eine natürliche Zahl finden kann. Uns ist natürlich klar, dass es sich hier um eine wahre Aussage handelt, aber wir müssen dafür einen Beweis finden. Die Idee dazu ist ganz einfach: Für jedes $x \in \mathbb{N}$ ist $(x+1)^2 = x^2 + 2x + 1$ und $(x+2)^2 = x^2 + 4x + 4$. Somit kann man z.B. mit $y = x^2 + 2x + 2$ eine Zahl angeben, die dazwischen liegt. Der formale Beweis läuft dann wie folgt ab:

- Der Gegenspieler setzt $x = a$ wobei a eine natürliche Zahl ist.

- Der Beweiser setzt $y = a^2 + 2a + 2 \in \mathbb{N}$.
- Zur Verifikation muss man die Umgleichungen $(a+1)^2 < a^2 + 2a + 2$ und $a^2 + 2a + 2 < (a+2)^2$ nachweisen wofür man zur Ungleichung $0 < 1$ auf beiden Seiten $(a+1)^2$ adddiert bzw. zur Ungleichung $0 < 2a + 2$ auf beiden Seiten $a^2 + 2a + 2$ adddiert.

Man könnte die gerade bewiesene Aussage noch weiter verschärfen und zeigen, dass man zwischen zwei Quadratzahlen aus $1, 4, 9, \ldots$ immer eine gerade Zahl finden kann. Welches y sollte der Beweiser dann in Abhängigkeit von $x = a$ wählen?
In diesen Beispielen ist der Bereich $\mathbb{N}$ von entscheidender Bedeutung, denn bezogen auf den Bereich $\mathbb{Z}$ ergeben sich falsche Aussagen. Um das zu beweisen, bildet man die negierte Aussage und beweist diese wieder mit dem Wechselspiel zwischen Beweiser und Gegenspieler. Die Negationen von quantifizierten Formel sind Teil der folgenden Umformungsregeln.

Satz: Für beliebige Prädikate $P(x), Q(x)$ und $R(x, y)$ gelten die folgenden Äquivalenzen:

$$\begin{array}{lrcl}
(1) & \neg\forall x\ P(x) & \equiv & \exists x \neg P(x) \\
(2) & \neg\exists x\ P(x) & \equiv & \forall x \neg P(x) \\
(3) & \forall x\ P(x) \wedge \forall x\ Q(x) & \equiv & \forall x\ (P(x) \wedge Q(x)) \\
(4) & \exists x\ P(x) \vee \exists x\ Q(x) & \equiv & \exists x\ (P(x) \vee Q(x)) \\
(5) & \forall x \forall y\ R(x, y) & \equiv & \forall y \forall x\ R(x, y) \\
(6) & \exists x \exists y\ R(x, y) & \equiv & \exists y \exists x\ R(x, y)
\end{array}$$

Achtung: Die folgenden Formelpaare sind im allgemeinen nicht äquivalent:

$$\begin{array}{lcl}
\forall x\ P(x) \vee \forall x\ Q(x) & \textit{und} & \forall x\ (P(x) \vee Q(x)) \\
\exists x\ P(x) \wedge \exists x\ Q(x) & \textit{und} & \exists x\ (P(x) \wedge Q(x)) \\
\forall x\quad (\exists y\ R(x, y)) & \textit{und} & \exists y\quad (\forall x\ R(x, y))
\end{array}$$

Konkrete Gegenbeispiele für das erste und zweite Paar erhält man für den Bereich der ganzen Zahlen, wenn $P(x)$ (bzw. $Q(x)$) aussagt, dass x eine gerade (bzw. ungerade) Zahl ist. Für das dritte Paar kann man das Prädikat $R(x, y)$:"$x \leq y$" über den reellen Zahlen verwenden.

Wir kommen jetzt noch einmal zum Beispiel von oben zurück und wollen beweisen, dass

$$\forall x \in \mathbb{Z} \quad \exists y \in \mathbb{Z} \quad (x+1)^2 < y < (x+2)^2$$

eine falsche Aussage ist. Dazu bilden wir zuerst die Negation:

$$\begin{array}{rl}
 & \neg(\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z} \quad (x+1)^2 < y < (x+2)^2) \\
\iff & \exists x \in \mathbb{Z}\ \neg(\exists y \in \mathbb{Z} \quad (x+1)^2 < y < (x+2)^2) \\
\iff & \exists x \in \mathbb{Z}\ \forall y \in \mathbb{Z}\ \neg((x+1)^2 < y \wedge y < (x+2)^2) \\
\iff & \exists x \in \mathbb{Z}\ \forall y \in \mathbb{Z}\ (\neg((x+1)^2 < y) \vee \neg(y < (x+2)^2)) \\
\iff & \exists x \in \mathbb{Z}\ \forall y \in \mathbb{Z}\ ((x+1)^2 \geq y \vee y \geq (x+2)^2)
\end{array}$$

Jetzt folgt der eigentliche Beweis:

- Der Beweiser setzt $x = -2$.
- Der Gegenspieler setzt $y = b$ für ein $b \in \mathbb{Z}$.
- Man muss $(-2+1)^2 = 1 \geq b \vee b \geq (-2+1)^2 = 0$ verifizieren, aber das ist leicht, denn wenn die erste Bedingung $1 \geq b$ nicht gilt, dann ist mit $b > 1 > 0$ die zweite Bedingung erfüllt.

1.4 Beweistechniken

In diesem Abschnitt geht es darum, einige grundlegende Beweisstrategien kennenzulernen. Da das prinzipielle Verständnis im Mittelpunkt stehen soll, sind die in den Beispielen bewiesenen Aussagen sehr einfach gewählt. Gerade bei diesen scheinbaren Selbstverständlichkeiten wird ein weiteres Problem deutlich: Bevor man an einen Beweis geht, muss man sich klarmachen, was man schon als Basiswissen voraussetzen kann, und was man noch beweisen muss. Oft ist als erster hilfreicher Schritt eine geeignete Formalisierung der Aussage notwendig. Wir wollen hier als Basiswissen nur die wichtigsten bekannten Fakten über das Rechnen mit natürlichen Zahlen voraussetzen:

- $\mathbb{N}$ bezeichnet die Menge aller natürlichen Zahlen (mit Null) und $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$ die Menge der positiven natürlichen Zahlen. Die Addition und Multiplikation von natürlichen Zahlen sind assoziativ und kommutativ und es gilt das Distributivgesetz in der Form $\quad \forall x, y, z \in \mathbb{N}\ x(y+z) = xy + xz$.
- $n \in \mathbb{N}$ ist durch $d \in \mathbb{N}^+$ *teilbar* (oder man sagt, d ist ein *Teiler* von n), wenn ein $k \in \mathbb{N}$ existiert, so dass $n = k \cdot d$. In diesem Fall kann man $d|n$ als Kurzschreibweise dafür verwenden, dass d ein Teiler von n ist. Eine natürliche Zahl $p \geq 2$ ist eine Primzahl, wenn sie nur die Teiler 1 und p hat.
- Natürliche Zahlen, die durch 2 teilbar sind, nennt man *gerade* Zahlen, d.h. n ist genau dann gerade, wenn $n = 2k$ für ein $k \in \mathbb{N}$. Zahlen, die nicht gerade sind, nennt man *ungerade*. Jede ungerade Zahl n kann durch $n = 2k + 1$ für ein $k \in \mathbb{N}$ dargestellt werden.
- Satz über die ganzzahlige Division mit Rest: Für beliebige $n \in \mathbb{N}$ und $d \in \mathbb{N}^+$ gibt es eindeutige natürliche Zahlen q und r, so dass $n = qd + r$ und $0 \leq r < d$ gilt. Man nennt q den ganzzahligen Quotienten aus n und d und r den Rest bei dieser Division. Um direkt auf die Werte q und r zu verweisen, können auch die Notationen $q = \left\lfloor \frac{n}{d} \right\rfloor$ und $r = n \bmod d$ verwendet werden.
- Wir setzen auch den Fakt voraus, dass jede natürliche Zahl $n \geq 2$ eine eindeutige Darstellung als Produkt aus Primfaktoren besitzt (wenn n selbst Primzahl ist, besteht das Produkt nur aus einem Faktor). Man sollte an dieser Stelle anmerken, dass dieser Fakt zwar wohlbekannt, aber doch recht tiefliegend und schwer zu beweisen ist.

Wir kommen nun zu den Beweistechniken. Viele mathematische Sätze haben die Form einer Implikation. Sie sagen, dass aus einer bestimmten Voraussetzung in Form einer Aussage p eine Behauptung in Form einer Aussage q folgt. Wir wollen uns zuerst mit den verschiedenen Techniken zum Beweis von solchen Implikationen beschäftigen. Basis für die Gültigkeit solcher Beweise sind einige einfache Tautologien, die man leicht mit der Wahrheitstafelmethode nachweisen kann.

Direkte Beweise

Der *direkte Beweis* beruht darauf, die Implikation $p \to q$ in mehrere elementare Teilschritte zu zerlegen, wobei man die folgende Tautologie nutzt:

$$((p \to r) \wedge (r \to q)) \to (p \to q).$$

Natürlich kann man die zwei Teilschritte auf der linken Seite weiter unterteilen, bis man bei einer Kette elementarer Implikationen angekommen ist. Wie die folgenden Beispiele demonstrieren, bewegt man sich bei der Begründung der Elementarschritte in einem System, das sich auf einigen Axiomen (Grundannahmen) aufbaut und in dem man auf bereits bewiesene Tatsachen (in unserem Fall sind das die oben aufgelisteten Eigenschaften der natürlichen Zahlen) zurückgreifen kann.

Satz: Für beliebige $l, m, n \in \mathbb{N}^+$ gilt: Wenn l ein Teiler von m und m ein Teiler von n ist, dann ist l auch ein Teiler von n.

Beweis: Da wir eine formale Defintion für die Teilbarkeit eingeführt haben, kann man die Voraussetzung des Satzes durch eine einfache Formel ausdrücken und die folgende Beweiskette bilden:

$l\|m$ und $m\|n$	Prämisse
$\exists j \in \mathbb{N} \quad m = j \cdot l \wedge \exists k \in \mathbb{N} \quad n = k \cdot m$	Teilbarkeitsdefinition
$\exists j \in \mathbb{N}\ \exists k \in \mathbb{N} \quad m = j \cdot l \wedge n = k \cdot m$	Zusammenfassen
$\exists j \in \mathbb{N}\ \exists k \in \mathbb{N} \quad n = k \cdot (j \cdot l)$	Einsetzen
$\exists j \in \mathbb{N}\ \exists k \in \mathbb{N} \quad n = (k \cdot j) \cdot l$	Assoziativgesetz
$\exists k' \in \mathbb{N} \quad n = k' \cdot l$	Teilbarkeitsdefinition mit $k' = k \cdot j$
$l\|n$	Konklusion

Satz: Das Produkt aus zwei ungeraden Zahlen ist eine ungerade Zahl.

Beweis: Wir nutzen den Fakt $(*)$, dass eine Zahl n genau dann ungerade ist, wenn sie sich in der Form $2k + 1$ darstellen lässt:

m und n sind ungerade	Prämisse
$\exists j \in \mathbb{N} \quad m = 2j + 1 \wedge \exists k \in \mathbb{N} \quad n = 2k + 1$	$(*)$
$\exists j \in \mathbb{N}\ \exists k \in \mathbb{N} \quad mn = (2j + 1) \cdot (2k + 1)$	Zusammenfassen
$\exists j \in \mathbb{N}\ \exists k \in \mathbb{N} \quad mn = 4jk + 2j + 2k + 1$	Ausmultiplizieren
$\exists j \in \mathbb{N}\ \exists k \in \mathbb{N} \quad mn = 2(2jk + j + k) + 1$	2 ausklammern
$\exists k' \in \mathbb{N} \quad mn = 2k' + 1$	$(*)$ mit $k' = 2jk + j + k$
mn ist ungerade	Konklusion

Bei den Schritten Ausmultiplizieren und Ausklammern kamen das Distributiv-, Assoziativ- und Kommutativgesetz zum Einsatz.

Indirekte Beweise

Manchmal ist es schwierig, den Beweis direkt zu führen. Als Alternativen bieten sich indirekte Beweise durch Kontraposition oder in der Form von Widerspruchs-Beweisen an. Beim *Beweis durch Kontraposition* wird anstelle von $p \to q$ die logisch äquivalente Aussage $\neg q \to \neg p$ bewiesen. Beim Widerspruchs-Beweis wird an Stelle von $p \to q$ die logisch äquivalente Aussage $(p \wedge \neg q) \to 0$ bewiesen. Wir demonstrieren beide Beweisverfahren an einfachen Beispielen.

Satz: Für jede natürliche Zahl n gilt: Ist n^2 ungerade, so ist auch n ungerade.

Beweis durch Kontraposition: Da die Negation von *"ungerade sein"* die Eigenschaft *"gerade sein"* ist, lautet die Kontraposition *"Ist n gerade, so ist auch n^2 gerade"*. und dafür gibt es einen einfachen direkten Beweis:
Ist n gerade, so gibt es ein $k \in \mathbb{N}$ mit $n = 2k$. Folglich ist $n^2 = (2k)^2 = 2 \cdot (2k^2)$ und somit ist n^2 gerade.

Satz: Sind $m \geq n$ natürliche Zahlen, so dass $m + n$ und $m - n$ durch 3 teilbar sind, dann ist auch m durch 3 teilbar.

Beweis durch Widerspruch: Man geht von der Annahme aus, dass 3 ein Teiler von $m + n$ und $m - n$, aber kein Teiler von m ist. Dann kommt der Primteiler 3 nicht als Faktor in der eindeutigen Primzahlzerlegung von m vor. Wir wissen, dass $k, k' \in \mathbb{N}$ mit $m + n = 3k$ und $m - n = 3k'$ existieren. Nun bertrachten wir die Primzahlzerlegung der Zahl $x = 2m$, die offensichtlich alle Primfaktoren von m und eine zusätzliche 2 enthält, also nach Voraussetzung keine 3. Andererseits ist $x = (m + n) + (m - n) = 3(k + k')$ und somit enhält die Primzahlzerlegung von x alle Primfaktoren von $k + k'$ und zusätzlich eine 3 - ein Widerspruch.

Beweise durch Fallunterscheidung

Häufig ist es notwendig, verschiedene Fälle zu analysieren. Das dabei verwendete logische Prinzip ist Äquivalenz der Aussagen $p \to q$ und $(p \wedge r \to q) \wedge (p \wedge \neg r \to q)$, wir unterscheiden also die Fälle r und $\neg r$.

Satz: Ist $n \in \mathbb{N}$ ungerade, dann ist $n^2 - 1$ durch 8 teilbar.

Beweis: Zunächst machen wir uns klar, dass $n^2 - 1 = (n-1) \cdot (n+1)$ gilt (entweder man kennt es schon als binomische Formel oder man rechnet es durch Ausmultiplizieren nach). Da n ungerade ist, sind $n-1$ und $n+1$ gerade und enthalten jeweils den Faktor 2 und folglich ist das Produkt durch 4 teilbar. Für die Teilbarkeit des Produkts durch 8 muss einer der Faktoren duch 4 teilbar sein und das beweist man mit einer Fallunterscheidung:
1. Fall: Ist $n - 1$ durch 4 teilbar, so ist $n - 1 = 4k$ und $n + 1 = 4k + 2 = 2(2k + 1)$ und damit $n^2 - 1 = 8k(2k + 1)$, also durch 8 teilbar.
2. Fall: Ist $n - 1$ nicht durch 4 teilbar, so muss es (als gerade Zahl!) das Doppelte einer ungeraden Zahl sein, also die Form $2(2m + 1) = 4m + 2$ für eine natürliche Zahl m haben. Folglich ist $p + 1 = 4m + 4 = 4(m + 1)$ und damit erhalten wir, dass

$p^2 - 1 = 8(2m + 1)(m + 1)$ durch 8 teilbar ist.

1.5 Beweise mit vollständiger Induktion

Der Begriff *vollständige Induktion* bezeichnet eine Beweistechnik, die häufig zum Beweis von Aussagen verwendet wird, die für alle natürlichen Zahlen (oder für alle natürlichen Zahlen ab einem bestimmten Anfangswert) gültig sind. Grundlage dafür sind die auf Richard Dedekind und Giuseppe Peano zurückgehenden Axiome der natürlichen Zahlen:

1. 0 ist eine natürliche Zahl.
2. Jede natürliche Zahl n hat einen eindeutigen Nachfolger $S(n)$, der auch eine natürliche Zahl ist.
3. Aus $S(n) = S(m)$ folgt $n = m$.
4. 0 ist kein Nachfolger einer natürlichen Zahl.
5. Jede Menge X, die 0 enthält und für die gilt, dass aus $n \in X$ auch $S(n) \in X$ folgt, enthält alle natürlichen Zahlen.

Achtung: Wir schreiben für den Nachfolger $S(n)$ auch $n + 1$, aber das ist als symbolische Schreibweise und nicht als Anwendung der Operation Addition zu verstehen. Im Gegenteil, wie die folgenden Betrachtungen zeigen, kann die Addition durch Anwendung der Nachfolgerfunktion rekursiv definiert werden.

Konsequenz 1: Man kann Funktionen $f : \mathbb{N} \longrightarrow A$ definieren, indem man $f(0)$ festlegt und $f(S(n))$ auf $f(n)$ zurückführt. Dieses Prinzip der Definition von Funktionen nennt man *Rekursion*.

Beispiel: Um die Addition von natürlichen Zahlen einzuführen, definieren wir für jede fest gewählte Zahl m die Funktion $m+ : \mathbb{N} \longrightarrow \mathbb{N}$, die jedem n aus dem Definitionsbereich die Summe $m + n$ zuordnen soll. Diese Funktion hat die folgende rekursive Definition: $m + (0) := m$ und $m + (S(n)) := S(m + n)$. Das entspricht den Regeln $m + 0 := m$ und $m + (n + 1) := (m + n) + 1$.
Analog kann man die Multiplikation durch $m\cdot : \mathbb{N} \longrightarrow \mathbb{N}$ mit $m \cdot (0) := 0$ und $m \cdot (S(n)) := (m \cdot (n)) + m$ definieren, was den Regeln $m \cdot 0 := 0$ und $m \cdot (n + 1) := (m \cdot n) + m$ entspricht.

Konsequenz 2: Man kann allgemeine Aussagen über natürliche Zahlen nach dem folgenden Schema beweisen. Eine Aussageform $P(x)$ über dem Bereich der natürlichen Zahlen ist wahr für alle natürlichen Zahlen, wenn sie die folgenden zwei Bedingungen erfüllt:

1. $P(0)$ ist wahr.
2. Für beliebige $n \in \mathbb{N}$ gilt: Ist $P(n)$ wahr, dann ist auch $P(n + 1)$ wahr.

Dieses Beweisprinzip nennt man *vollständige Induktion*. Die erste Bedingung wird *Induktionsanfang*, oder *Induktionsbasis*, die zweite Bedingung *Induktionsschluss* genannt. Dabei ist $P(n)$ die *Induktionsvoraussetzung* oder die *Induktionsannahme* und $P(n+1)$ die *Induktionsbehauptung*.

Beispiele für Aussagen, die man mit Induktion beweisen kann:

- Für jede natürliche Zahl n ist die Zahl $a_n = n^3 + 2n$ durch 3 teilbar.
- Für beliebige reelle Zahlen a und $r \neq 1$ und für jede natürliche Zahl n gilt

$$\sum_{i=0}^{n} ar^i = \frac{ar^{n+1} - a}{r - 1}.$$

Exemplarisch für das zu verwendende Schema stellen wir hier den Beweis der ersten Aussage in einer sehr ausführlichen Version vor.

Induktionsanfang: Für $n = 0$ ist $a_n = 0^3 + 2 \cdot 0 = 0$ durch 3 teilbar (nach Teilbarkeitsdefinition: $a_n = 0 = 3 \cdot 0$).

Induktionsvoraussetzung: $a_n = n^3 + 2n$ ist durch 3 teilbar (für ein bestimmtes $n \in \mathbb{N}$), d.h. $a_n = 3k$ für ein $k \in \mathbb{N}$

Induktionsbehauptung: $a_{n+1} = (n+1)^3 + 2(n+1)$ ist durch 3 teilbar.

Induktionsschritt:

a_{n+1}	$= (n+1)^3 + 2(n+1)$	*Binomische Formel anwenden*
	$= (n^3 + 3n^2 + 3n + 1) + (2n + 2)$	*geeignet zusammenfassen*
	$= (n^3 + 2n) + 3n^2 + 3n + 3$	
	$= a_n + 3n^2 + 3n + 3$	*Induktionsvoraussetzung anwenden*
	$= 3k + 3n^2 + 3n + 3$	3 *ausklammern* (*Distributivgesetz*)
	$= 3(k + n^2 + n + 1)$	$k' = k + n^2 + n + 1$
	$= 3k'$	$k' \in \mathbb{N}$

Folglich ist auch a_{n+1} durch 3 teilbar und somit die Induktionsbehauptung bewiesen. □

Für mit dem Beweisschema vertraute Leser kann man diesen Induktionbeweis auch in einer verkürzten Form aufschreiben. Wir verwenden die Kürzel IA, IV, IB und IS für Induktionsanfang, Induktionsvoraussetzung, Induktionsbehauptung und Induktionsschritt. Da Induktionsvoraussetzung und Induktionsbehauptung sich im Allgemeinen schon aus der Formulierung der Aussage ablesen lassen, kann man darauf verzichten, sie noch einmal explizit aufzuschreiben. An Stelle dessen vermerkt man beim Induktionsschritt, ob sich die Voraussetzung auf n und die Behauptung auf $n+1$ bezieht oder ob man von $n-1$ auf n schließen will (was manchmal der bequemere Weg sein kann). Hier ist eine Kurzversioin des letzten Beweises:

IA: Für $n = 0$ ist $a_0 = 0$ durch 3 teilbar.

IS: $n \longrightarrow n+1$

$a_{n+1} = (n+1)^3 + 2(n+1) = n^3 + 3n^2 + 3n + 1 + 2n + 2 = a_n + 3(n^2 + n + 1)$

a_{n+1} ist durch 3 teilbar, weil a_n nach IV und der zweite Summand nach Definition durch 3 teilbar ist. □

Zwei Varianten des Induktionsprinzips werden häufig verwendet:

Variante 1: Wird die Induktionsbasis nicht für $n = 0$ sondern für einen anderen festen Anfangswert $k > 0$ bewiesen, so gilt die Aussage für alle natürlichen Zahlen $n \geq k$.

Beispiele:

- Für jede natürliche Zahl $n > 0$ ist die Summe der ungeraden Zahlen von 1 bis $2n - 1$ gleich n^2.
- Jeden ganzzahligen Wert $n \geq 8$ kann man durch Briefmarken mit den Werten 3 und 5 zusammenstellen.

Variante 2: Beim Induktionsschritt ist es erlaubt, nicht nur auf $P(n)$, sondern auf beliebige kleinere Zahlen zurückzugreifen, d.h. an Stelle von $P(n) \longrightarrow P(n+1)$ zeigt man $P(k) \wedge P(k+1) \wedge \ldots \wedge P(n) \longrightarrow P(n+1)$, wobei k der Anfangswert aus der Induktionsbasis ist. Dieses Prinzip wird *verallgemeinerte vollständige Induktion* genannt.

Der folgende Satz gibt ein typisches Beispiel für eine Aussage, die man mit verallgemeinerter Induktion beweisen kann.

Satz: Jede natürliche Zahl $n \geq 2$ kann man als Produkt von Primzahlen darstellen, wobei für Primzahlen selbst die Darstellung als Produkt mit nur einem Faktor zulässig ist.

Beweis (verallgemeinerte Induktion nach n):

IA: Für $n = 2$ haben wir die 1-Faktor-Darstellung $n = 2$.

IV: Jede Zahl k mit $2 \leq k < n$ ist Produkt von Primzahlen.

IS: $k < n \longrightarrow n$

Fall 1: Ist n eine Primzahl, dann gibt es die 1-Faktor-Darstellung $n = n$.

Fall 2: Ist n keine Primzahl, dann kann man n in zwei Faktoren $k, l < n$ zerlegen. Nach IV gibt es für k und l jeweils eine Zerlegung in Primfaktoren, $k = p_1 \cdot \ldots \cdot p_s$ und $l = q_1 \cdot \ldots \cdot q_t$. Daraus ergibt sich die folgende Zerlegung für n:

$$n = k \cdot l = p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \ldots \cdot q_t.$$ □

Übung: Beweisen Sie folgende Aussagen mithilfe der vollstndigen Induktion:

1. Jedes n-Eck besitzt die Innenwinkelsumme $(n-2) \cdot 180°$.
2. Jedes konvexe n-Eck besitzt $n(n-3)/2$ Diagonalen. (Hinweis: Ein n-Eck ist *konvex*, wenn die Innenwinkel aller Ecken kleiner als 180° sind.)