Brückenkurs

Mathematik für Informatiker

im Wintersemester 2015/16

FU Berlin

Institut für Informatik

Klaus Kriegel

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 möglichts 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 auch 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 zu Schluß:

- 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 zusammengestezten Aussagen durch sogenannte Wahrheitsswerttabellen (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.

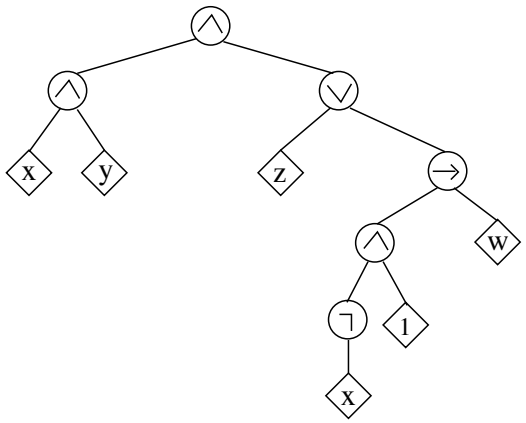
3. Sind s und t Formeln der Aussagenlogik, dann sind auch die Ausdrücke $(s \wedge t)$, $(s \vee t)$, $(s \rightarrow t)$ sowie $(s \leftrightarrow t)$ Formeln der Aussagenlogik.

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: Ein 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 $\beta = \neg x_1 \wedge \neg x_2$ 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:

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

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.

3) Logik-Puzzle: A(lice), B(ob), C(arol) und D(ave) fahren mit dem Zug und haben Platzkarten für ein Viererabteil, wobei die Plätze 1 und 2 (3 und 4) vorwärts (rückwärts) zur Fahrtrichtung liegen und 1 und 3 Fensterplätze sind. Folgende Wünsche sind zu berücksichtigen:

a) D will nicht rückwärts fahren,

b) B und C wollen nebeneinander sitzen,

c) A wünscht einen Fensterplatz

d) B und D wollen sich nicht gegenüber sitzen.

- Finden Sie eine Platzverteilung die alle Wünsche berücksichtigt. Ist sie eindeutig?
- Formulieren ein Modell, in dem sich die Bedingungen 1) bis 4) als Boolesche Terme audrücken lassen. Gibt es eine eindeutige Belegung der Variablen, die diese Terme wahr macht?
- Wenn nicht, formulieren Boolesche Terme für weitere Bedingungen, die erfüllt sein müssen, um Eindeutigkeit zu erzwingen.

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 solche 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:

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

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:

$l \mid m$ und $m \mid n$	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 $k' = k \cdot j$
$l \mid n$	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.

Übungen:
Beweisen Sie, dass die folgenden einfachen Fakten für beliebige $m, n \in \mathbb{N}$ und $k \in \mathbb{N}^+$ gelten:

1) $k \mid m \wedge k \mid n \rightarrow k \mid (m + n)$

2) Ist m ungerade und n gerade, dann ist $m + n$ ungerade.

3) Ist $m \bmod 7 = 2$ und $n \bmod 7 = 4$, dann ist die Zahl $x = 3m + 2n$ durch 7 teilbar.

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 $p \rightarrow q$ die logisch äquivalente Aussage $\neg q \rightarrow \neg p$ bewiesen. Beim Widerspruchs-Beweis wird an Stelle von $p \rightarrow q$ die logisch äquivalente Aussage $(p \wedge \neg q) \rightarrow 0$ 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.

Übung: Zeigen Sie mit einem indirekten Beweis, dass wenn k Teiler von m aber kein Teiler von n ist, auch m kein Teiler von n sein kann.

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.

Übung: Beweisen Sie mit Fallunterscheidung, dass $n^3 - n$ für beliebige $n \in \mathbb{N}$ durch 6 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 zu 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:

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

2 Grundbegriffe der Mengenlehre

2.1 Mengen und Operationen auf Mengen

Moderne Mengentheorie wird in Form eines axiomatischen Kalküls betrieben. Dieser Ansatz hat aber den Nachteil, daß einfache inhaltliche Fragen oft durch einen technisch komplizierten Apparat verdeckt werden. Wir werden uns deshalb auf die Entwicklung einer "naiven" Mengenlehre beschränken, die als sprachliches Werkzeug für die nachfolgenden Teile der Vorlesung völlig ausreichend ist.
Nach Georg Cantor ist eine *Menge* "eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die Elemente der Menge genannt werden) zu einem Ganzen".
Der Sachverhalt, dass ein Objekt a Element einer Menge A ist, wird durch $a \in A$ dargestellt, anderenfalls schreibt man $a \notin A$. Zwei Mengen A und B sind *gleich*, wenn sie die gleichen Elemente besitzen, d.h. wenn für alle a gilt: $a \in A$ dann und nur dann, wenn $a \in B$.

Darstellungen von Mengen

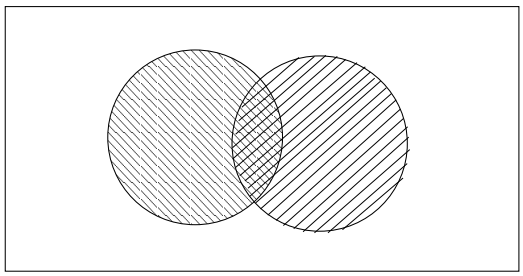
a) Mengen können durch *Auflistung ihrer Elemente* in geschweiften Klammern dargestellt werden. Das betrifft insbesondere endliche Mengen, wie z.B. $A = \{2, 3, 5, 7\}$ oder $B = \{rot, gelb, blau\}$. Dabei ist die Reihenfolge der Elemente in der Auflistung ohne Bedeutung. Auch die Mehrfachnennung von Elementen ist erlaubt (sollte aber zur Vermeidung von Missverständnissen möglichst vermieden werden), sie hat aber nur Einfluss auf die Darstellung der Menge und nicht auf die Menge selbst, z.B. $\{2, 3, 5, 7\} = \{5, 7, 3, 2, 2, 5, 2\}$.
Wir vereinbaren, dass auch unendliche Mengen durch Auflistung dargestellt werden können, sofern dies unmissverständlich ist, wie z.B. $\{0, 1, 2, 3, \ldots\}$ für die natürlichen Zahlen oder $\{2, 4, 6, 8, \ldots\}$ für die positiven, geraden Zahlen.

b) Die in der Mathematik gebräuchlichste Darstellungsform von Mengen beruht auf dem sogenannten *Abstraktionsprinzip*, nach dem man Mengen – im Sinne der Cantorschen Definition – durch wohlbestimmte Eigenschaften definieren kann. Dazu werden Prädikate $P(x)$ über einem festgelegten Individuenbereich für x benutzt. Dann wird mit $\{x \mid P(x)\}$ oder (wenn der Bereich B explizit genannt werden soll) mit $\{x \in B \mid P(x)\}$ die Menge bezeichnet, die sich aus allen Individuen aus dem Bereich zusammensetzt, für die $P(x)$ wahr ist. Man bezeichnet diese Darstellungsart von Mengen nach den Mathematikern Ernst Zermelo und Abraham Fraenkel auch als ZF-Notation.

c) Zur Veranschaulichung können Mengen durch sogenannte *Venn–Diagramme* als Kreisscheiben oder andere Flächen in der Ebene dargestellt werden.

Oft ist es sinnvoll, den zu betrachtenden Individuenbereich generell festzulegen, z.B. wenn man nur Mengen von natürlichen Zahlen betrachten will. Ein solcher Bereich wird *Universum* genannt und allgemein mit U bezeichnet. Es ist klar, dass Aussageformen über U immer Teilmengen von U definieren. Im folgenden Venn-Diagramm sind zwei Mengen A und B als Kreisflächen in dem durch das Rechteck symbolisierten

Universum U dargestellt:



Bemerkung: In manchen Anwendungen (z.B. für die Buchstaben in einem Wort) benötigt man ein Konstrukt, in dem Elemente auch mehrfach auftreten können. In diesem Fall sprechen wir von einer *Multimenge*. Obwohl sich diese konzeptionell wesentlich von einer Menge unterscheidet, wird in der Regel die gleiche Notation verwendet, was natürlich zu Missverständnissen führen kann. Deshalb werden wir bei Verwendung von Multimengen diesen Begriff explizit nennen, anderenfalls ist immer eine Menge gemeint. Demnach sind $\{b, a, b, b\}$ und $\{a, b\}$ (ohne Zusatz) zwei identische Mengen, die Multimengen $\{b, a, b, b\}$ und $\{a, b\}$ unterscheiden sich, aber die Multimengen $\{b, a, b, b\}$ und $\{a, b, b, b\}$ sind wiederum identisch.

Definition: Eine Menge A ist *Teilmenge* (oder *Untermenge*) einer Menge B (Schreibweise $A \subseteq B$), wenn aus $a \in A$ auch $a \in B$ folgt.

Die Teilmengenrelation entspricht also einer Implikation der definierenden Prädikate. Deshalb kann man aus den Eigenschaften der logischen Implikation zwei elementare Eigenschaften der Teilmengenrelation ableiten:

- Die Mengen A und B sind gleich genau dann, wenn $A \subseteq B$ und $B \subseteq A$.
- Ist A eine Teilmenge von B und B eine Teilmenge von C, dann ist auch A eine Teilmenge von C.

Für die Grundmengen der natürlichen, ganzen, rationalen und reellen Zahlen werden die Symbole $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ verwendet. Es gilt $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$. Mit $\mathbb{N}^+, \mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ werden die entsprechenden Teilmengen der positiven Zahlen (echt größer als 0) bezeichnet.

Übungen:

1) Erkennen Sie, welche Mengen im Folgenden definiert sind, und geben Sie jeweils eine verbale Beschreibung dazu an!

- $A = \{q \in \mathbb{Q} \,|\, \exists m \in \mathbb{N}^+ \; \exists \in \mathbb{N}^+ \; m \leq n \wedge q = \frac{m}{n}\}$
- $B = \{q \in \mathbb{Q} \,|\, \exists m \in \mathbb{N}^+ \; \exists \in \mathbb{N}^+ \; ggT(m, n) = 1 \wedge q = \frac{m}{n}\}$
- $C = \{r \in \mathbb{R} \,|\, \exists s \in \mathbb{R} \; r = s^2\}$
- $D = \{r \in \mathbb{R} \,|\, 2 \leq r^2 \leq 3\}$

2) Beschreiben Sie die folgenden Mengen in ZF-Notation!

- Die Menge P aller Primzahlen und die Menge S aller Zahlen, die das Produkt von zwei verschiedene Primzahlen sind.
- Die Menge T aller positiven rationalen Zahlen, in deren gekürzter Darstellung im Nenner eine 2 steht.
- Die Menge U aller reellen Zahlen, die echt kleiner als 3 und Quadratwurzel aus einer rationalen Zahl sind.

Definition (Operationen auf Mengen):

- Zwei Mengen A und B sind *disjunkt*, wenn sie keine gemeinsamen Elemente besitzen, d.h wenn aus $a \in A$ folgt $a \notin B$.
- Die *Vereinigung* $A \cup B$ der Mengen A und B besteht aus allen Objekten, die Elemente von A oder von B sind, dh. $A \cup B = \{x \mid x \in A \ \vee \ x \in B\}$.
- Der *Durchschnitt* $A \cap B$ der Mengen A und B besteht aus allen Objekten, die Elemente von A und von B sind, dh. $A \cap B = \{x \mid x \in A \ \wedge \ x \in B\}$.
- Die *Differenz* $A \setminus B$ der Mengen A und B besteht aus allen Objekten, die Elemente von A, aber nicht von B sind, dh. $A \setminus B = \{x \mid x \in A \ \wedge \ x \notin B\}$.
- Die Vereingung der Mengendifferenzen $A \setminus B$ und $B \setminus A$ wird die *symmetrische Differenz* aus A und B genannt und mit $A \oplus B$ oder auch mit $A \div B$ bezeichnet.
- Die Menge, die kein Element enthält, wird *leere Menge* genannt und mit $\emptyset$ bezeichnet.
- Ist A Teilmenge eines festgelegten Universums U, dann ist das *Komplement* von A definiert als $U \setminus A$. Es wird mit $\overline{A}$ bezeichnet.

Der Zusammenhang zwischen Teilmengenbeziehungen sowie Operationen auf Mengen und den entsprechenden logischen Operationen wird noch einmal in der folgenden Tabelle zusammengefasst:

Mengenlehre		Logik	
Gleichheit	$A = B$	$x \in A \leftrightarrow x \in B$	Äquivalenz
Inklusion	$A \subseteq B$	$x \in A \rightarrow x \in B$	Implikation
Vereinigung	$A \cup B$	$x \in A \vee x \in B$	Disjunktion
Durchschnitt	$A \cap B$	$x \in A \wedge x \in B$	Konjunktion
Komplement	$A = \overline{B}$	$x \in A \leftrightarrow \neg(x \in B)$	Negation
symmetr. Differenz	$A \oplus B = A \div B$	$x \in A \oplus x \in B$	Antivalenz
Universum	U	1	wahr
leere Menge	$\emptyset$	0	falsch

Damit können auch - wie im nachfolgenden Satz formuliert - die bekannten Gesetze der Aussagenlogik in die Mengenlehre übertragen werden.

Satz: Folgende Identitäten gelten für alle Untermengen A, B, C eines Universums U:

Kommutativität:	$A \cup B$	$= B \cup A$
	$A \cap B$	$= B \cap A$
Assoziativität:	$A \cup (B \cup C)$	$= (A \cup B) \cup C$
	$A \cap (B \cap C)$	$= (A \cap B) \cap C$
Distributivität:	$A \cap (B \cup C)$	$= (A \cap B) \cup (A \cap C)$
	$A \cup (B \cap C)$	$= (A \cup B) \cap (A \cup C)$
Idempotenz:	$A \cup A$	$= A$
	$A \cap A$	$= A$
Dominanz:	$A \cup U$	$= U$
	$A \cap \emptyset$	$= \emptyset$
Identität:	$A \cup \emptyset$	$= A$
	$A \cap U$	$= A$
Absorption:	$A \cup (A \cap B)$	$= A$
	$A \cap (A \cup B)$	$= A$
De Morgan'sche Regel:	$\overline{A \cup B}$	$= \overline{A} \cap \overline{B}$
	$\overline{A \cap B}$	$= \bar{A} \cup \bar{B}$
Komplementierung:	$A \cup \overline{A}$	$= U$
	$A \cap \overline{A}$	$= \emptyset$
	$\overline{(\overline{A})}$	$= A$
	$A \setminus B$	$= A \cap \overline{B}$

Auf Grund der Assoziativität kann man bei der Vereinigung (bzw. beim Durchschnitt) von n Mengen $A_1, A_2, \ldots, A_n$ auf Klammerungen verzichten und die folgende Schreibweise nutzen:

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

Definition: Ist I eine beliebige Menge und ist für jedes $i \in I$ eine Menge A_i gegeben, dann nennen wir die Menge dieser Mengen eine *Mengenfamilie über der Indexmenge* I und bezeichnen sie durch $\{A_i \mid i \in I\}$. Die Vereinigung (bzw. der Durchschnitt) dieser Mengenfamilie ist definiert durch

$$\bigcup_{i \in I} A_i = \{x \mid \text{es gibt ein } i \in I, \text{ so dass } x \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{x \mid \text{für alle } i \in I, \text{ gilt } x \in A_i\}$$

Übung: Bestimmen Sie für die folgende Mengenfamilie die Vereinigung und den Durchschnitt!

$$\{A_n \mid n \in \mathbb{N}^+\} \text{ mit } A_n = \left\{\frac{m}{n} \mid m \in \mathbb{N}^+\right\}$$

Definition: Eine Familie $\{A_i \mid i \in I\}$ von nichtleeren Mengen wird *Partition* oder *Zerlegung* einer Menge A genannt, falls

1. $A = \bigcup_{i \in I} A_i$
2. Für beliebige, voneinander verschiedene $i, j \in I$ gilt $A_i \cap A_j = \emptyset$.

Definition: Ist A eine Menge, dann wird die Menge aller Untermengen von A die *Potenzmenge* von A genannt und mit $\mathcal{P}(A)$ bezeichnet.

Satz: Ist A eine endliche, n-elementige Menge, dann hat die Potenzmenge $\mathcal{P}(A)$ genau 2^n Elemente.

Übung: Beschreiben Sie die Menge $\mathcal{P}(\{1,2,3,4\}) \setminus \mathcal{P}(\{1,2,3\})$ durch Auflistung.

2.2 Das Kartesische Produkt und Relationen

Definition: Ein *geordnetes Paar* (a, b) ist eine (den Objekten a und b zugeordnetes) Konstrukt mit der folgenden Eigenschaft: $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$.

Definition: Das *kartesische Produkt* $A \times B$ von zwei Mengen A und B ist definiert als die Menge aller geordneten Paare (a, b) mit $a \in A$ und $b \in B$, als Formel:

$$A \times B = \{\, (a, b) \mid a \in A \wedge b \in B \,\}$$

Beispiel: $\{1,2,3\} \times \{2,4\} = \{(1,2),(1,4),(2,2),(2,4),(3,2),(3,4)\}$

Wie dieses Beispiel deutlich suggeriert, hat bei zwei endlichen Mengen A und B mit m und n Elementen das kartesische Produkt $A \times B$ genau $m \cdot n$ Elemente.

Definition: Eine Untermenge R eines kartesischen Produkts $A \times B$ wird *binäre Relation* oder kurz *Relation* zwischen A und B genannt. Für $(a, b) \in R$ kann auch $a\, R\, b$ geschrieben werden. In diesem Fall sagt man, dass a in Relation zu b steht.
Eine Untermenge R eines kartesischen Produkts der Form $A \times A$ wird (binäre) Relation auf A (oder über A) genannt.

Die ersten drei Relationen in den folgenden Beispielen sind generisch, d.h. man kann sie über beliebigen Grundmengen betrachten:

- $\emptyset \subseteq A \times B$ wird *leere Relation* genannt.
- $A \times B$ wird *Allrelation* zwischen A und B genannt.
- Die Menge $\{(a, a) \mid a \in A\}$ wird die *identische Relation* über A genannt und kurz mit Id_A bezeichnet.
- Die Teilbarkeitsrelation $\mid$ kann man als Relation über den natürlichen Zahlen (aber auch über den ganzen Zahlen) betrachten. Wie bereits besprochen, ist diese Relation wie folgt definiert:

$$\forall\, a, b \in \mathbb{N} \quad (\, a \mid b \iff \exists c \in \mathbb{N} \qquad b = a \cdot c)$$

- Über den natürlichen Zahlen $\mathbb{N}$, den ganzen Zahlen $\mathbb{Z}$, den rationalen Zahlen $\mathbb{Q}$ und den reellen Zahlen $\mathbb{R}$ kennen wir eine Reihe von Vergleichsrelationen, nämlich $<, \leq, \geq, >$.

- Ist A die Menge aller Informatikstudenten an der FU Berlin und B die Menge aller Pflichtmodule im Informatikstudium, dann ist
  $R = \{(a, b) \in A \times B \mid$ Student a hat das Modul b abgeschlossen $\}$ eine binäre Relation.

- Jede Abbildung $f : A \longrightarrow B$ kann auch als binäre Relation
  $f = \{(a, b) \in A \times B \mid a \in A \wedge b = f(a)\}$ gesehen werden.

Zur Darstellung von Relationen sind verschiedene Methoden gebräuchlich:

- Darstellungen in Tabellenform, bei denen für jedes $a \in A$ eine Spalte und für jedes $b \in B$ eine Zeile angelegt wird. Die Zelle in der Spalte von a und der Zeile von b wird mit einer 1 gefüllt, wenn $a\,R\,b$ gilt, und sonst mit einer 0. (Verwendung in relationalen Datenbanken);

- Anschauliche Darstellungen durch Diagramme in einem Rechteck;

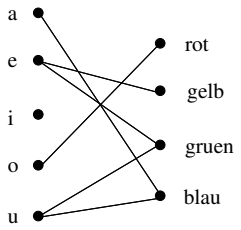
- Sogenannte bipartite Graphen, bei denen die Elemente aus A und B als Knoten getrennt auf zwei Seiten gezeichnet werden, wobei zwei Elemente, die zueinander in Relation stehen, durch eine Kante (Verbindungsstrecke) verbunden werden.

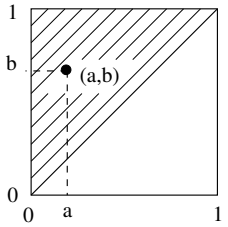
Beispiel: Die Relation R zwischen der Vokalmenge $A = \{a, e, i, o, u\}$ und der Wortmenge $B = \{rot, gelb, gruen, blau\}$ gibt an, welcher Vokal in welchem Wort vorkommt:

$$R = \{(a, blau), (e, gelb), (e, gruen), (o, rot), (u, gruen), (u, blau)\}$$

In der folgenden Abbildung sieht man die Relation R in Tabellenform (links) und als bipartiter Graph (Mitte). Auf der rechten Seite ist die Relation $\leq$ über dem reellen Intervall $[0, 1]$ als Diagramm dargestellt:

blau	1	0	0	0	1
gruen	0	1	0	0	1
gelb	0	1	0	0	0
rot	0	0	0	1	0
	a	*e*	*i*	*o*	*u*





Übung:
1) Aus wie vielen Paaren bestehen die Teilbarkeitsrelation | bzw. die Kleiner-Gleich-Relation $\leq$ über der Menge $\{1, 2, \ldots, 12\}$?
2) Wie viele Relationen zwischen zwei endlichen Menge A und B mit m bzw. n Elementen gibt es?

Relationsoperationen

1. Sind R und R' Relationen zwischen A und B, dann sind auch die Vereinigung $R \cup R'$, der Durchschnitt $R \cap R'$ sowie das Komplement $\overline{R} = (A \times B) \setminus R$ Relationen zwischen A und B.

2. Die zu einer Relation $R \subseteq A \times B$ *inverse Relation* $R^{-1} \subseteq B \times A$ ist definiert durch $R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$.

3. Die *Verkettung* oder *Komposition* $R \circ S$ von zwei Relationen $R \subseteq A \times B$ und $S \subseteq B \times C$ ist definiert durch

$$\{(a, c) \in A \times C \mid \text{es gibt ein } b \in B \text{ mit } (a, b) \in R \text{ und } (b, c) \in S\}.$$

Beispiele:

1) Wir betrachten die Vergleichsrelationen $<$, $\leq$, $\geq$ und die identische Relation $=$ über den natürlichen Zahlen $\mathbb{N}$. Offensichtlich ist die Vereinigung der Relationen $<$ und $=$ die Relation $\leq$. Das Komplement der Relation $<$ ist die Relation $\geq$. Der Durchschnitt der Relationen $\leq$ und $\geq$ ist die identische Relation $=$. Die zu $\leq$ inverse Relation ist $\geq$, die identische Relation ist zu sich selbst invers.

2) Sei M die Menge aller Menschen und $R \subseteq M \times M$ "Elternrelation", also $a\,R\,b$, falls a Vater oder Mutter von b ist. Dann kann man die inverse Relation R^{-1} sowie die Verkettungen $R \circ R$, $R \circ R^{-1}$ und $R^{-1} \circ R$ wie folgt charakterisieren:

- $a\,R^{-1}\,b$, falls a Kind von b ist,
- $a\,R \circ R\,b$, falls a Großvater oder Großmutter von b ist,
- $a\,R \circ R^{-1}\,b$, falls a und b ein gemeinsames Kind haben oder falls $a = b$ und a hat ein Kind,
- $a\,R^{-1} \circ R\,b$, falls $a = b$ oder a und b Geschwister oder Halbgeschwister sind.

Eigenschaften von Relationen über Mengen

Definition: Sei R eine Relation über A.

- R ist *reflexiv*, falls für jedes $a \in A$ gilt, dass $a\,R\,a$, d.h. $Id_A \subseteq R$.
- R ist *symmetrisch*, falls aus $a\,R\,b$ folgt, dass $b\,R\,a$, d.h. $R^{-1} \subseteq R$.
- R ist *transitiv*, falls aus $a\,R\,b$ und $b\,R\,c$ folgt, dass $a\,R\,c$, d.h. $R \circ R \subseteq R$.
- R ist *antisymmetrisch*, falls aus $a\,R\,b$ und $b\,R\,a$ die Gleichheit von a und b folgt, d.h. $R \cap R^{-1} \subseteq Id_A$.
- R ist *asymmetrisch*, falls aus $a\,R\,b$ folgt, dass $(b, a) \notin R$, d.h. $R \cap R^{-1} = \emptyset$.

Beispiele:

1) Die Vergleichsrelationen $\leq$ und $\geq$ sind über $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ reflexiv, transitiv und antisymmetrisch. Die Relationen $<$ und $>$ sind nicht reflexiv, aber transitiv, antisymmetrisch und asymmetrisch.

2) Die oben definierte Teilbarkeitsrelation ist reflexiv und transitiv über $\mathbb{N}$ und über $\mathbb{Z}$. Sie ist antisymmetrisch über $\mathbb{N}$, aber als Relation über $\mathbb{Z}$ ist sie nicht antisymmetrisch, denn $1|-1$ und $-1|1$, aber $1 \neq -1$.

Übung: Wie viele symmetrische und wie viele reflexiv-symmetrische Relationen gibt es über einer n-elementigen Menge A?

2.3 Äquivalenzrelationen

Definition: Eine Relation über einer Menge A wird *Äquivalenzrelation* genannt, wenn sie reflexiv, symmetrisch und transitiv ist.

Beispiele:

1) Sei $\mathbb{N}$ die Menge der natürlichen Zahlen und R definiert durch $a\,R\,b$, genau dann wenn a und b beim Teilen durch 5 den gleichen Rest haben. Dann ist R eine Äquivalenzrelation auf $\mathbb{N}$.

2) Die logische Äquivalenz $\equiv$ ist eine Äquivalenzrelation auf der Menge der Booleschen Formeln.

3) Die Kongruenz von Dreiecken ist eine Äquivalenzrelation.

Definition: Ist $R \subseteq A \times A$ eine Äquivalenzrelation und ist $a \in A$, dann nennt man die Menge $\{x \in A \mid xRa\}$ die *Äquivalenzklasse* von a (bezüglich R). Sie wird mit $[a]_R$ oder auch mit $a/_R$ bezeichnet. Ein Element einer Äquivalenzklasse wird *Repräsentant* dieser Klasse genannt.

Lemma: Sei R eine Äquivalenzrelation, dann sind zwei Äquivalenzklassen $[a]_R$ und $[b]_R$ entweder gleich oder disjunkt. Sie sind genau dann gleich, wenn $a\,R\,b$ gilt.

Ein formaler Beweis dieses Lemmas wird später in der Vorlesung vorgestellt.

Übung: Wie viele Äquivalenzrelationen gibt es auf einer drei- bzw. vierelementigen Menge A? Klassifizieren Sie dazu die Äquivalenzrelationen nach Anzahl ihrer Äquivalenzklassen.

Die erste Aussage des folgenden Satzes kann als einfache Schlussfolgerung aus dem Lemma abgeleitet werden.

Satz: Ist $R \subseteq A \times A$ eine Äquivalenzrelation, dann bildet die Menge aller Äquivalenzklassen eine Partition von A. Umgekehrt, ist eine Partition $\{A_i \mid i \in I\}$ von A gegeben, dann ist die durch

$$a\,R\,b \iff \exists i \in I \qquad a \in A_i \ \wedge \ b \in A_i$$

definierte Relation R eine Äquivalenzrelation.

Definition: Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Eine Untermenge von A wird *Repräsentantensystem* für R genannt, wenn sie aus jeder Äquivalenzklasse genau ein Element enthält.

Beispiele:
1) Wir betrachten noch einmal die Relation R über $\mathbb{N}$, die zwei Zahlen a und b genau dann in Beziehung setzt, wenn sie beim Teilen durch 5 den gleichen Rest haben. Dann werden die einzelnen Äquivalenzklassen jeweils durch die Zahlen mit gleichem Rest gebildet, was zu der folgenden Partition von $\mathbb{N}$ führt:

$$\{\{0, 5, 10 \ldots\}, \{1, 6, 11, \ldots\}, \{2, 7, 12, \ldots\}, \{3, 8, 13, \ldots\}, \{4, 9, 14, \ldots\}\}$$

Offensichtlich bilden die Reste {0,1,2,3,4} ein Repräsentantensystem (das sogenannte Standard–Repräsentantensystem), aber auch die Menge $\{3, 10, 7, 21, 9\}$ ist ein Repräsentantensystem.

2) Natürlich hätten wir an Stelle der 5 auch jede andere Zahl $n \in \mathbb{N}^+$ als Teiler wählen können und an Stelle von $\mathbb{N}$ wäre auch $\mathbb{Z}$ als Grundmenge geeignet gewesen. Man bezeichnet die dadurch entstehenden Relationen als Kongruenzen modulo n und schreibt für zwei Zahlen a, b, die beim Teilen durch n den gleichen Rest haben auch $a \equiv b \pmod{n}$. In diesem Fall bilden die möglichen Reste $\{0, 1, \ldots, n-1\}$ das Standard–Repräsentantensystem.

3) Wir betrachten $\mathbb{R}$ (oder auch $\mathbb{Q}$) als Grundmenge und definieren eine Äquivalenzrelation $\sim \subseteq \mathbb{R} \times \mathbb{R}$ durch: $r \sim s \overset{def}{\Leftrightarrow} r - s \in \mathbb{Z}$. Zeigen Sie zunächst als kleine Übung, dass $\sim$ eine Äquivalenzrelation ist und dass die reellen Zahlen aus dem halboffenen Intervall $[0, 1)$ ein Repräsentantensystem bilden. Dann sollten wir uns die Frage stellen, ob man eine gemeinsame Grundidee in diesen drei Beispielen erkennen kann.

Satz: Die identische Relation Id_A und die Allrelation $A \times A$ sind Äquivalenzrelationen. Sind R und R' Äquivalenzrelationen auf A, dann ist auch $R \cap R'$ eine Äquivalenzrelation auf A.

Achtung: Die letzte Aussage gilt im Allgemeinen nicht für Vereinigungen. Als Gegenbeispiel kann man die Kongruenzrelationen modulo 2 und modulo 3 betrachten. Offensichtlich ist das Paar $(1, 6)$ nicht in der Vereinigung, denn 1 und 6 haben sowohl beim Teilen durch 2 als auch beim Teilen durch 3 verschiedene Reste. Andererseits sind die Paare $(1, 4)$ - gleicher Rest beim Teilen durch 3 - und $(4, 6)$ - gleicher Rest beim Teilen durch 2 - in der Relationsvereinigung. Folglich ist diese Vereinigung nicht transitiv.

Allgemein kann jede Relation $R \subseteq A \times A$ durch die folgenden 3 Schritte zu einer Äquivalenzrelation erweitert werden:

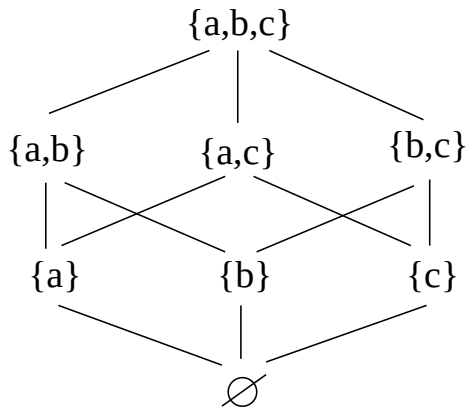
1) reflexiver Abschluss: $R_r = R \cup Id_A$
2) symmetr. Abschluss: $R_{rs} = R_r \cup R_r^{-1} = R \cup R^{-1} \cup Id_A$
3) transitiver Abschluss: $R_{rst} = R_{rs} \cup R_{rs} \circ R_{rs} \cup R_{rs} \circ R_{rs} \circ R_{rs} \cup \ldots = \bigcup_{i=1}^{\infty} R_{rs}^i$

wobei R_{rs}^i die i-fache Verkettung von R_{rs} ist.

2.4 Ordnungsrelationen

Definition: Eine Relation R über einer Menge A, die reflexiv, transitiv und antisymmetrisch ist, wird *Halbordnungsrelation* oder auch *partielle Ordnungsrelation* genannt. Das Paar (A, R) nennt man eine *halb– (partiell) geordnete Menge* oder kurz *poset* als Abkürzung für partially ordered set.

Endliche, halbgeordnete Mengen werden oft durch sogenannte *Hasse–Diagramme* dargestellt. Dabei werden die Elemente der Menge als Punkte in der Ebene gezeichnet, wobei direkte Nachfolger jeweils höher als ihre Vorgänger liegen und mit ihnen durch ein Liniensegment verbunden sind. Formal betrachtet beschreibt das Hasse–Diagramm eines Posets (A, R) die kleinste Unterrelation von R, deren reflexiver und transitiver Abschluss R ergibt. Die folgende Abbildung zeigt das Hasse–Diagramm der Potenzmenge einer 3–elementigen Menge $M = \{a, b, c\}$:



Beispiele:

1) Für jede beliebige Menge M ist $(\mathcal{P}(M), \subseteq)$ eine halbgeordnete Menge.

2) Die Teilbarkeitsrelation $|$ ist eine Halbordnungsrelation in der Menge der positiven ganzen Zahlen $\mathbb{Z}^+$.

3) In der Menge der reellen Zahlen $\mathbb{R}$ ist die Relation $\leq$ eine Halbordnungsrelation.

4) Die Menge der Wörter einer Sprache wird durch die "lexikographische Ordnung" geordnet.

5) Sei P Menge von Punkten in der Ebene. Jeder Punkt $p \in P$ ist als Koordinatenpaar (p_x, p_y) gegeben. Dann ist die durch

$$p = (p_x, p_y) \preceq q = (q_x, q_y) \stackrel{def}{\Longleftrightarrow} p_x \leq q_x \wedge p_y \leq q_y$$

definierte Relation eine partielle Ordnungsrelation auf P.

Übung: Zeichnen Sie die Hasse-Diagramme der Teilbarkeitsrelation über der Menge $\{1, 2, \ldots, 12\}$ und der Relation $\preceq$ aus 5) über der Punktmenge
$P = \{(1,1), (2,7), (3,0), (3,6), (3,8), (4,1), (4,4), (6,3), (7,7)\}$.

Zwei Begriffe sind eng verwandt mit partiellen Ordnungsrelationen: totale Ordnungsrelationen und strikte (oder strenge) Ordnungsrelationen. Diese Begriffe werden durch die folgenden Definitionen genauer erläutert.

Definition: Zwei Elemente a und b einer halbgeordneten Menge (A, R) nennt man *vergleichbar*, falls $a\,R\,b$ oder $b\,R\,a$ gilt. Anderenfalls nennt man sie unvergleichbar. Eine Halbordnungsrelation R in einer Menge A wird *totale* (oder auch *lineare*) *Ordnungsrelation* genannt, wenn jedes Paar von Elementen vergleichbar ist.

Beispiele: In den obigen Beispielen sind die Relationen aus 1) und 2) keine totalen Ordnungsrelationen. So sind für $M = \{a, b, c\}$ die Untermengen $\{a\}$ und $\{c\}$ unvergleichbar bezüglich der Teilmengenrelation. Die Zahlen 6 und 20 sind unvergleichbar bezüglich der Teilbarkeitsrelation. Dagegen ist $\leq$ eine totale Ordnungsrelation für die reellen Zahlen. Die lexikographische Ordnung ist eine totale Ordnungsrelation.

Bemerkung: Taucht in der Literatur der Begriff "Ordnungsrelation" auf, so ist darunter in der Regel eine "Halbordnungsrelation" zu verstehen.

Definition: Eine Relation R über einer Menge A wird *strikte* oder *strenge Ordnungsrelation* genannt, wenn sie transitiv und asymmetrisch ist.

Typische Beispiele für strikte Ordnungsrelationen sind die "echt–kleiner"–Relation $<$ oder die Relation, ein echter Teiler zu sein. Generell kann man aus jeder Halbordnungsrelation R über einer Menge A eine strikte Ordnungsrelation $R' = R \setminus Id_A$ ableiten und umgekehrt kann aus jeder strikten Ordnungsrelation durch Vereinigung mit Id_A eine Halbordnungsrelation gemacht werden.

3 Funktionen

3.1 Definition und grundlegende Eigenschaften

Definition: Unter einer *Funktion* (oder *Abbildung*) f von einer Menge A in eine Menge B versteht man eine Zuordnung, bei der jedem Element aus A ein eindeutig bestimmtes Element aus B entspricht. Formal kann f als eine Relation zwischen A und B charakterisiert werden, so dass für jedes $a \in A$ genau ein $b \in B$ existiert mit $a\,f\,b$. Als übliche Schreibweise verwenden wir $f : A \longrightarrow B$ um auszudrücken, dass f eine Funktion von A nach B ist, und $f(a) = b$, um auszudrücken, dass dem Element a durch die Funktion f der Wert b zugeordnet wird. Die Menge A wird *Definitionsbereich* von f und die Menge B wird *Wertebereich* oder *Wertevorrat* von f genannt.

Definition: Ist $f : A \longrightarrow B$ eine Funktion, $M \subseteq A$ und $N \subseteq B$, dann nennt man die Menge

$f(M) = \{y \in B \mid \text{es gibt ein } x \in M \text{ mit } f(x) = y\}$ das *Bild* von M unter f und die Menge
$f^{-1}(N) = \{x \in A \mid f(x) \in N\}$ das *vollständige Urbild* von N unter f.

Definition:

- Eine Funktion $f : A \longrightarrow B$ heißt *surjektiv*, falls jedes Element von B im Bild von A auftritt, d.h. wenn $f(A) = B$.
- Eine Funktion $f : A \longrightarrow B$ heißt *injektiv* oder *eineindeutig*, falls je zwei verschiedene Elemente aus A auch verschiedene Bilder haben, d.h. wenn aus $f(a) = f(a')$ die Gleichheit von a und a' folgt.
- Eine Funktion wird *bijektiv* genannt, wenn sie injektiv und surjektiv ist.

Beispiel: Wir betrachten die Funktion $f(x) = x^2 + 1$. Als Funktion von den reellen Zahlen in die reellen Zahlen ist $f : \mathbb{R} \longrightarrow \mathbb{R}$ weder injektiv noch surjektiv.
Durch Einschränkungen von Definitions– und/oder Wertebereich kann man diese Eigenschaften erzwingen:

- $f : \mathbb{R} \longrightarrow [1, \infty)$ ist surjektiv, aber nicht injektiv.
- $f : [0, \infty) \longrightarrow \mathbb{R}$ ist injektiv, aber nicht surjektiv
- $f : [0, \infty) \longrightarrow [1, \infty)$ ist bijektiv.

Betrachtet man eine Funktion $g : A \longrightarrow B$ als Relation, dann ist die zu g inverse Relation g^{-1} genau dann eine Funktion, wenn g bijektiv ist. In diesem Fall wird g^{-1} die zu g *inverse Funktion* genannt.

Beispiel: Wir betrachten noch einmal $f(x) = x^2 + 1$ als eine bijektive Funktion $f : [0, \infty) \longrightarrow [1, \infty)$. Durch äquivalentes Umformen kann man in diesem Fall die Umkehrfunktion $f^{-1} : [1, \infty) \longrightarrow [0, \infty)$ explizit angeben durch $f^{-1}(x) = \sqrt{x - 1}$.

Definition: Sind $f : A \longrightarrow B$ und $g : B \longrightarrow C$ Funktionen, dann ist die Relationsverkettung $f \circ g$ eine Funktion von A in C. Sie wird *Verknüpfung* oder *Komposition* von f und g genannt und durch $gf : A \longrightarrow C$ bezeichnet, wobei $gf(a) = g(f(a))$ gilt. Man beachte, dass Relationsverkettungen von links nach rechts und Funktionsverknüpfungen von rechts nach links geschrieben werden.

Satz: Die folgenden Fakten ergeben sich als einfache Schlussfolgerungen aus den Definitionen. Seien $f : A \longrightarrow B$ und $g : B \longrightarrow C$ zwei Funktionen, dann gilt:

- Ist f bijektiv, dann ist $f^{-1}f = Id_A$ und $ff^{-1} = Id_B$.
- f ist genau dann injektiv, wenn eine Funktion $h : B \longrightarrow A$ existiert mit $hf = Id_A$.
- f ist genau dann surjektiv, wenn eine Funktion $h : B \longrightarrow A$ existiert mit $fh = Id_B$.

- Sind f und g injektiv, dann ist auch gf injektiv.
- Sind f und g surjektiv, dann ist auch gf surjektiv.
- Sind f und g bijektiv, dann ist auch gf bijektiv und es gilt $(gf)^{-1} = f^{-1}g^{-1}$.

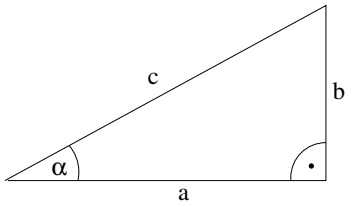
Satz: Jede Funktion $f : A \longrightarrow B$ induziert eine Äquivalenzrelation $\sim_f$ auf A durch

$$a \sim_f b \quad \text{genau dann, wenn} \quad f(a) = f(b).$$

Diese Äquivalenzrelation wird auch *Faserung* von A durch f genannt.

3.2 Winkelfunktionen

Dieser Abschnitt ist eine reine Wiederholung von Schulstoff, der nach unserer Erfahrung häufig etwas verschüttet ist. Die bekannten Winkelfunktionen $\sin, \cos, \tan$ und cot machen Aussagen zu den Seitenverältnissen in rechtwinkligen Dreiecken in Abhängigkeit von einem (nichtrechten) Winkel α in dem Dreieck. Sei dabei a die Länge der am Winkel α anliegenden Kathete (Ankathete), b die Länge der dem Winkel α gegenüberliegende Seite (Gegenkathete) und c die Länge der Hypothenuse. Dann werden die Winkelfunktionen durch folgende Seitenverhältnisse definiert:



$$\sin\alpha = \frac{b}{c} \qquad \cos\alpha = \frac{a}{c}$$

$$\tan\alpha = \frac{b}{a} \qquad \cot\alpha = \frac{a}{b}.$$

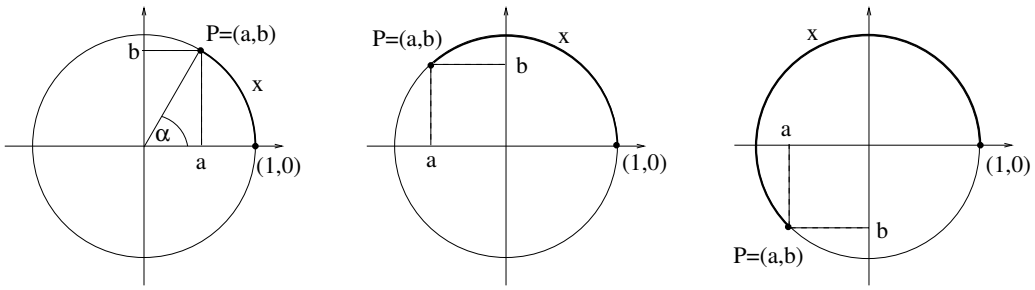
Da Skalierungen die Seitenverhältnisse nicht verändern, kann man die Betrachtung auch auf Dreiecke mit der Hypothenusenlänge $c = 1$ reduzieren. Würde man sich nur auf die Interpretation in (nicht-entarteten) rechtwinkligen Dreiecken beschränken, dann wäre der Definitionsbereich für alle vier Funktionen das offene Intervall zwischen $0°$ und $90°$ im Gradmaß bzw. zwischen 0 und $\frac{\pi}{2}$ im Bogenmaß.
Wir werden in den weiteren Betrachtungen immer das Bogenmaß verwenden. Um es besser zu verstehen und um den Defintionsbereich der Sinus- und Cosinusfunktions auf ganz $\mathbb{R}$ ausweiten zu können, betrachten wir einen Einheitskreis (d.h. mit Radius 1) um den Koordinatenursprung in der Ebene und $(1, 0)$ als Startposition für einen Punkt, der sich auf dem Einheitskreis bewegt, wobei Drehungen gegen die Uhrzeigerrichtung positiv und in Uhrzeigerrichtung negativ gemessen werden. Man kann eine Drehung entweder durch den Winkel α im Gradmaß oder durch die Länge des Kreisbogenabschnitts x messen, wobei man Letzteres das Bogenmaß des Winkels nennt. Da eine volle Umdrehung im Gradmaß $360°$ um im Bogenmaß 2π (Kreisumfang) ist, ergibt sich eine einfache Umrechnungsformel

$$\alpha = \frac{x \cdot 360}{2\pi} = \frac{x \cdot 180}{\pi} \quad \text{und} \quad x = \frac{2\alpha\pi}{360} = \frac{\alpha\pi}{180}.$$

Insbesondere sollte man sich die folgenden Werte einprägen:

α im Gradmaß	0	30	45	60	90	180	270	360
x im Bogenmaß	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π

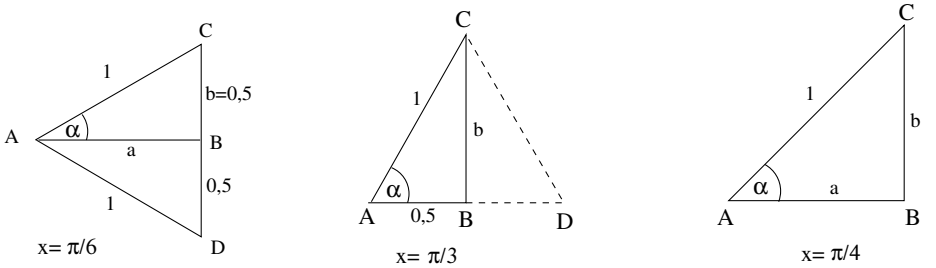
Sei $P = (a, b)$ der Punkt, den man startend von $(1, 0)$ mit dem Bogenmaß x auf dem Einheitskreis erreicht, dann definiert man $\sin x = b$ und $\cos x = a$ sowie $\tan x = \frac{b}{a}$ falls $a \neq 0$ und $\cot x = \frac{a}{b}$ falls $b \neq 0$. Die folgende Abbildung zeigt die Situationen für $x = \pi/3$, $x = 3\pi/4$ und $x = 5\pi/4$.



Da für jeden Punkt $P = (a, b)$ auf dem Einheitskreis $a^2 + b^2 = 1$ gilt, folgt daraus die bekannte Formel $\sin^2 x + \cos^2 x = 1$ für alle $x \in \mathbb{R}$. Auch viele andere Identitäten lassen sich aus diesem geometrischen Ansatz ableiten:

- $\sin(-x) = -\sin x$ und $\cos(-x) = \cos x$ für alle $x \in \mathbb{R}$
- $\sin(x + 2\pi) = \sin x$ und $\cos(x + 2\pi) = \cos x$ für alle $x \in \mathbb{R}$
- $\sin(x + \pi) = -\sin x$ und $\cos(x + \pi) = -\cos x$ für alle $x \in \mathbb{R}$
- $\cos x = \sin(x + \pi/2)$ und $\sin x = \cos(x - \pi/2)$ für alle $x \in \mathbb{R}$

Einige Werte der Winkelfunktionen kann man aus den Satz des Pythagoras und elementaren Fakten aus der Dreiecksgeometrie herleiten. In der folgenden Abbildung sind die drei Fälle mit den Winkeln $30°, 60°$ und $45°$, also $x = \pi/6$, $x = \pi/3$ und $x = \pi/4$ dargestellt.



Im ersten Fall betrachten wir ein rechtwinkliges Dreieck ABC mit Hypothenusenlänge 1, einem Winkel $\alpha = 30°$ und den Kathetenlängen b (Gegenkathete) und a (Ankathete). Wir spiegeln dieses Dreieck an der Ankathete und erhalten durch Vereinigung

ein Dreieck ADC, in dem alle Winkel gleich 60° sind. Folglich ist dieses Dreieck auch gleichseitig (Seitenlänge 1) und daraus folgt $b = \frac{1}{2}$. Jetzt nutzt man den Satz des Pythagoras mit $a^2 + b^2 = 1^2$ und erhält $a = \sqrt{1 - b^2} = \sqrt{\frac{3}{4}} = \frac{\sqrt{3}}{2}$. Daraus ergibt sich

$$\sin \tfrac{\pi}{6} = \tfrac{1}{2} \qquad \text{und} \qquad \cos \tfrac{\pi}{6} = \tfrac{\sqrt{3}}{2}.$$

Für den Fall $\alpha = 60°$ könnte man bereits die vierte Identität aus der obigen Liste nutzen, aber wir wollen es noch einmal geometrisch lösen. Wir starten mit einem rechtwinkligen Dreieck ABC, spiegeln es an der Gegenkathete und erhalten durch Vereinigung ein gleichseitiges Dreieck ADC mit Seitenlänge 1. Somit muss im ursprünglichen Dreieck $a = \frac{1}{2}$ sein. Daraus folgt $b = \sqrt{1 - a^2} = \frac{\sqrt{3}}{2}$ und letzlich

$$\sin \tfrac{\pi}{3} = \tfrac{\sqrt{3}}{2} \qquad \text{und} \qquad \cos \tfrac{\pi}{3} = \tfrac{1}{2}.$$

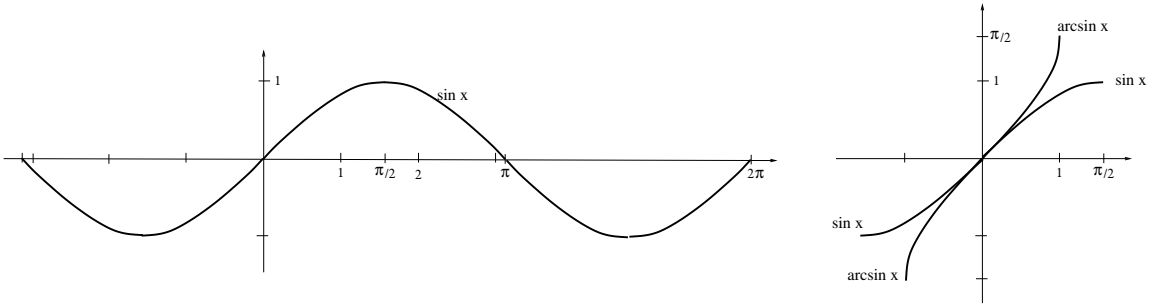
Der einfachste Fall ist $\alpha = 45°$, denn dann ist das rechtwinklige Dreieck gleichschenklig, also $a = b$. Daraus folgt $1 = a^2 + b^2 = 2a^2$ und $a = b = \sqrt{\frac{1}{2}} = \frac{\sqrt{2}}{2}$, also

$$\sin \tfrac{\pi}{4} = \tfrac{\sqrt{2}}{2} \qquad \text{und} \qquad \cos \tfrac{\pi}{4} = \tfrac{\sqrt{2}}{2}.$$

Die folgende Tabelle gibt eine Zusammenfassung von Werten der Winkelfunktionen, die in Übungsaufgaben häufig gebraucht werden.

α im Gradmaß	0	30	45	60	90
x im Bogenmaß	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\sin x$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\cos x$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
$\tan x$	0	$\frac{1}{\sqrt{3}} = \frac{\sqrt{3}}{3}$	1	$\sqrt{3}$	nicht def.

Auf der linken Seite der nächsten Abbildung sieht man bekannten Verlauf der Sinuskurve. Die Sinusfunktion ist als Funktion von $\mathbb{R}$ nach $\mathbb{R}$ ist weder injektiv noch surjektiv, aber durch geeignete Einschränkungen auf beiden Seiten wird die Teilfunktion $\sin : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1, 1]$ bijektiv. Die Umkehrfunktion ist die rechtsseitig dargestellte Arkussinusfunktion $\arcsin : [-1, 1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$.



Auf ähnliche Weise kann man die Cosinusfunktion auf das Intervall $[0, \pi]$ einschränken, um eine Umkehrfunktion $\arccos : [-1, 1] \to [0, \pi]$ zu bekommen.

3.3 Exponential- und Logarithmusfunktion

Die Exponentialfunktion $exp(x) = e^x$ ist eine Funktion, die jeder reellen Zahl x den positiven reellen Wert e^x zuordnet. Um sie verstehen, muss man wissen, welche Zahl sich hinter dem Symbol e verbirgt und wie man e in eine ganzzahlige, eine gebrochene oder sogar in eine beliebige reelle Potenz heben kann. Dahinter steht eine nicht ganz triviale Grenzwertbetrachtung, die eingehend im 3. Semester besprochen wird. Hier wollen wir nur stichpunktartig die wichtigsten Ideen nennen und uns danach einen mehr intuitiven Zugang zu dem Thema erarbeiten.

1. Die Folge $\left((1 + \frac{1}{n})^n\right)_{n \in \mathbb{N}^+}$ konvergiert. Der Grenzwert dieser Folge wird als Eulersche Zahl e bezeichnet und hat den Wert $2,71828\ldots$.

2. Die Reihe $\displaystyle\sum_{k=0}^{\infty} \frac{1}{k!}$ konvergiert auch gegen den Grenzwert e. Diesen Fakt kann man auch so lesen, dass die Reihe $\displaystyle\sum_{k=0}^{\infty} \frac{1}{k!} 1^k$ gegen den Wert e^1 konvergiert.

3. Man kann die 1 in der obigen Reihe auch durch eine beliebige reelle Zahl x ersetzen und zeigen, dass auch die Reihe $\displaystyle\sum_{k=0}^{\infty} \frac{1}{k!} x^k$ konvergiert. Wir nennen den Grenzwert $exp(x)$.

4. Man kann weiterhin zeigen, dass die Funktion $exp : \mathbb{R} \longrightarrow \mathbb{R}^+$ stetig und streng monoton wachsend ist. Darüber hinaus gilt für beliebige reelle Zahlen x und y die Gleichung $exp(x + y) = exp(x) \cdot exp(y)$. Diese Gleichung ist auch als Exponentialgesetz bekannt. Alle bisher genannten Fakten werden durch Grenzwertbetrachtungen bewiesen.

5. Da die Funktion $exp(x) = \sum_{k=0}^{\infty} \frac{1}{k!} x^k$ das Exponentialgesetz erfüllt, können wir die folgenden Eigenschaften ableiten:
   $exp(2) = exp(1 + 1) = exp(1) \cdot exp(1) = e \cdot e = e^2$,
   $exp(3) = exp(1 + 2) = exp(1) \cdot exp(2) = e \cdot e^2 = e^3$ und allgemein
   $exp(n) = e^n$ für alle $n \in \mathbb{N}$.
   Auf diese Weise wird im Nachhinein deutlich, dass die Beschreibung $exp(x) = e^x$ ihre Berechtigung hat.

Wir wollen jetzt den letzten Gedanken noch einmal mit einem beliebigen positiven, reellen Werte a an Stelle von e nachvollziehen:

- Die natürlichen Potenzen von a werden rekursiv definiert durch
  $a^0 = 1$ als Verankerung und

$a^{n+1} = a \cdot a^n$ als Rekursionsschritt.
Daraus resultiert das Exponentialgesetz $a^{k+n} = a^k \cdot a^n$ für beliebige $k, n \in \mathbb{N}$.

- Wir erweitern das Potenzieren schrittweise auf ganze und rationale Potenzen wobei das Ziel darin besteht, die Gültigkeit des Exponentialgesetzes zu erhalten. Sei $z = -n$ eine negative ganze Zahl. Es gilt $-n + n = 0$ und die formale Anwendung des Exponentialgesetzes ergibt $1 = a^0 = a^{-n+n} = a^{-n} \cdot a^n$.
  Durch Umstellen dieser Gleichung erhält man die einzig sinnvolle Erweiterung der Definition, nämlich $a^{-n} = \frac{1}{a^n}$.

- Die Erweiterung auf rationale Zahlen erfolgt durch eine ähnliche Überlegung. Für jedes $k \in \mathbb{N}^+$ folgt aus $1 = \underbrace{\frac{1}{k} + \ \ldots \ + \frac{1}{k}}_{k \ mal}$ und der formalen Anwendung des Exponentialgesetzes die Gleichung $a = a^1 = \left(a^{\frac{1}{k}}\right)^k$.
  Folglich ergibt sich als einzig sinnvolle Erweiterung die Definition $a^{\frac{1}{k}} = \sqrt[k]{a}$ und für Brüche der Form $\frac{n}{k}$ mit $n \in \mathbb{Z}$ und $k \in \mathbb{N}$ der Ausdruck $a^{\frac{n}{k}} = (\sqrt[k]{a})^n$.

- Als weitere wichtige Eigenschaft dieser Exponentialfunktionen kann man die Regel $a^{p \cdot q} = (a^p)^q$ für alle $p, q \in \mathbb{Q}$ ableiten.

Die Erweiterung auf reelle Potenzen ist nur durch stetige Fortsetzung möglich. Danach sind für alle $a > 1$ die Funktionen $f(x) = a^x$ stetig und streng monoton wachsend und somit injektiv. Beschränkt man den Wertebereich auf das Bild der Funktion, nämlich die Menge $\mathbb{R}^+$ der positiven reellen Zahlen, so entsteht eine bijektive, also umkehrbare Funktion. Die Umkehrfunktion wird mit $\log_a x$ bezeichnet und *Logarithmusfunktion zur Basis a* genannt. Im Spezialfall $a = e$ ist das der sogenannte *natürliche Logarithmus*. Die folgende Regel kann man deshalb auch als eine Definition des Logarithmus ansehen:

$$\log_a x = y \iff a^y = x$$

Die wichtigsten Eigenschaften der Logarithmusfunktion ergeben sich aus der Übertragung des Exponentialgesetzes auf die Umkehrfunktion:

$$\log_a (x \cdot y) = \log_a x + \log_a y \qquad log_a \frac{1}{x} = -\log_a x \qquad log_a(x^y) = y \cdot \log_a x$$

Eine weitere nützliche Eigenschaft der Logarithmusfunktionen besteht darin, dass ein Basiswechsel lediglich eine Skalierung der Funktion, d.h. die Multiplikation der Funktionwerte mit einer bestimmeten Konstanten bewirkt. Die Umrechnung von der Basis a zur Basis b erfolgt mit der Formel

$$\log_b x = \frac{\log_a x}{\log_a b}$$

Übung: Beweisen Sie die vier genannten Eigenschaften der Logarithmusfunktion durch Verwendung der Eigenschaften der Exponentialfunktion und die Definition der Logarithmusfunktion.

4 Teilen mit Rest

4.1 Ganzzahlige Division und Kongruenzen

Der bereits genannte Satz über die ganzzahlige Division formuliert eine einfache und wohlbekannte Tatsache, nämlich dass die Schulmethode zur Division von ganzen Zahlen (genauer die Version der Methode, die beim Erreichen des Dezimalpunkts abricht) ein eindeutiges Ergebnis liefert. Dieser Fakt wird zusätzlich auf negativ ganzzahlige Dividenten übertragen.

Satz: Für beliebige $a \in \mathbb{Z}$ und $d \in \mathbb{Z}^+$ existieren eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < d$, so daß $a = qd + r$.

Definition: Sind $a, q, r \in \mathbb{Z}$, $d \in \mathbb{Z}^+$ mit $0 \leq r < d$ und $a = qd + r$, dann wird q der ganzzahlige Quotient aus a und d genannt und r als *Rest von a bezüglich (modulo) d* bezeichnet. Als Notation verwenden wir

$$q = \left\lfloor \frac{a}{d} \right\rfloor \quad \text{und} \quad r = a \bmod d.$$

Zwei ganze Zahlen a und b, die den gleichen Rest bezüglich d haben, werden *kongruent* bezüglich (modulo) d genannt, wofür die folgende Schreibweise vereinbart wird:

$$a \quad \equiv \quad b \pmod{d}$$

Es wurde bereits gesagt, dass man für positive a nur die Schulmethode zur Division anwenden muss, um die Werte von q und r zu bestimmen. Ist a negativ, bestimmen wir zuerst die Werte q' und r' für die positve Zahl $a' = -a$:

$$-a = a' = q'd + r' \text{ mit } q', r' \in \mathbb{Z} \text{ und } 0 \leq r' < d$$

Im Fall $r' = 0$ folgt daraus mit $a = (-q') \cdot d + 0$ die gesuchte Darstellung von a (also $q = -q'$ und $r = 0$). Im Fall $r > 0$ reicht die einfache Umstellung $a = (-q') \cdot d + (-r')$ noch nicht aus, denn $-r'$ liegt nicht in dem geforderten Bereich, aber es genügt der einfache Trick eine 0 in der Form $-d + d$ einzuschieben:

$$a = (-q')\cdot d+(-r') = (-q')\cdot d+0+(-r') = (-q')\cdot d-d+d+(-r') = \underbrace{(-q'-1)}_{=q}\cdot d+\underbrace{(d-r')}_{=r}$$

Satz: Die Relation $\equiv \pmod{d}$ ist eine Äquivalenzrelation und die Zahlenmenge $\{0, 1, \ldots, d-1\}$ bildet ein Repräsentantensystem für die Äquivalenzklassen. Darüber hinaus ist die Relation verträglich mit der Addition, Subtraktion und Multiplikation, d.h.:

ist	a	$\equiv$	a'	$\pmod{d}$
und	b	$\equiv$	b'	$\pmod{d}$
dann ist auch	$(a+b)$	$\equiv$	$(a'+b')$	$\pmod{d}$
und	$(a-b)$	$\equiv$	$(a'-b')$	$\pmod{d}$
und	ab	$\equiv$	$a'b'$	$\pmod{d}$

Mit den Eigenschaften aus diesem Satz kann man sehr gut die aus der Schulmathematik bekannten Teilbarkeitsregeln erklären. Offensichtlich ist n genau dann durch d teilbar, wenn der Rest $(n \bmod d)$ gleich Null ist.
Wir betrachten die Dezimaldarstellung $a_k a_{k-1} \ldots a_1 a_0$ einer $(k+1)$-stelligen natürlichen Zahl $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$. Nach den Kongruenzregeln ist n kongruent modulo d zu der "magischen" Zahl

$$magic_d(n) := a_k \cdot (10^k \bmod d) + a_{k-1} \cdot (10^{k-1} \bmod d) + \ldots + a_1 \cdot (10 \bmod d) + a_0.$$

Im konkreten Fall von $d = 3$ haben wir aber $(10 \bmod 3) = 1$ und folglich gilt auch $(10^j \bmod 3) = 1$ für alle $j \in \mathbb{N}$. Somit ist $magic_3(n)$ nichts anderes als die Quersumme von n.
Das gleiche Argument kann man für die Teilbarkeit durch 9 wiederholen.
Im Fall $d = 4$ ist $(10^2 \bmod 4) = 0$ und folglich $(10^j \bmod 4) = 0$ für alle $j \geq 2$. Der Wert $magic_4(n)$ hängt also nur von den letzten beiden Stellen ab und es folgt die bekannte Teilbarkeitsregel.
Analoge Argumente kann man für das Teilen durch 2, durch 5 und durch 8 verwenden.

Übungen:
1) Formulieren Sie eine Regel für die Teilbarkeit durch 11.
2) Man kann Laien durch Demonstration des folgenden Phänomens überraschen: Man würfelt mit zwei, drei (oder mehr) Würfeln setzt aus den gewürfelten Augen durch zwei verschiedene Reihenfolgen zwei Zahlen x und y zusammen, bildet die Differenz $x - y$ und kann dann feststellen, das diese Differenz durch 9 teilbar ist. Wenn man z.B. die Augenzahlen 1, 3 und 6 gewürfelt hat, sind die Differenzen $631 - 136 = 495$ und $613 - 361 = 252$ durch 9 teilbar. Finden Sie eine Begründung dafür.

4.2 Polynome und Polynomdivision

Eine (auf den ersten Blick) erstaunliche Parallele zum Teilen mit Rest ergibt sich bei der Betrachtung von Polynomen.

Definition: Ein *reelles Polynom* mit einer Variablen x ist ein formaler Ausdruck der Form

$$p(x) = \sum_{k=0}^{n} a_k x^k$$

wobei alle a_k reelle Zahlen sind und $a_n \neq 0$. Die Werte a_k nennt man die Koeffizienten des Polynoms $p(x)$. Der Grad dieses Polynoms ist n. Die Menge aller reellen Polynome mit der Variablen x wird mit $\mathbb{R}[x]$ bezeichnet.

Jedes Polynom bestimmt eine *Polynomfunktion* von $\mathbb{R}$ nach $\mathbb{R}$, die man an jeder Stelle $r \in \mathbb{R}$ durch Einsetzen des Wertes r für die Variable x und Auswertung der Operationen in $\mathbb{R}$ berechnen kann. Der Wert, der sich bei dieser Auswertung ergibt, wird mit $p(r)$ bezeichnet.

Man kann Polynome in naheleigender Weise addieren und einer multiplizieren. Die Operationen sind so definiert, dass sie verträglich mit den Operationen auf den Polynomfunktionen (Addition und Multiplikation der Funktionswerte) sind. In der folgenden Formel werden alle nicht in den Operanden definierten Werte a_k und b_k gleich 0 gesetzt.

$$\begin{aligned}\sum_{k=0}^{n} a_k x^k \pm \sum_{k=0}^{m} b_k x^k &= \sum_{k=0}^{max(n,m)} (a_k \pm b_k) x^k \\ \sum_{k=0}^{n} a_k x^k \cdot \sum_{k=0}^{m} b_k x^k &= \sum_{k=0}^{n+m} (\sum_{j=0}^{k} a_j b_{k-j}) x^k\end{aligned}$$

Das Horner-Schema

Der naive Ansatz zur Auswertung eines Polynoms von Grad n an einer Stelle r erfordert $2n-1$ Multiplikationen (Potenzen von r berechnen und mit den Koeffizienten multiplizieren) und n Additionen. Wesentlich effizienter ist die Polynomauswertung mit dem *Horner-Schema*, für die n Multiplikationen und n Additionen ausreichend sind. Die Grundidee beruht auf der folgenden Beobachtung:

$$\begin{aligned}f(r) &= \sum_{k=0}^{n} a_k r^k \\ &= a_n r^k + a_{n-1} r^{n-1} + \ldots + a_2 r^2 + a_1 r + a_0 \\ &= ((((\underbrace{a_n}_{c_n} r + a_{n-1}) \cdot r \ldots a_3) \cdot r + a_2) \cdot r + a_1) \cdot r + a_0\end{aligned}$$

$$\underbrace{\underbrace{\underbrace{\underbrace{\underbrace{a_n}_{c_n} r + a_{n-1}}_{c_{n-1}} \ldots a_3}_{c_3} \cdot r + a_2}_{c_2} \cdot r + a_1}_{c_1} \cdot r + a_0$$
$$c_0$$

Offensichtlich ist $c_n = a_n$ und für die Berechnung der Zwischenergebnisse $c_{n-1}, c_{n-2}, \ldots, c_0$ braucht man jeweils eine Multiplikation und eine Addition. Zur Rechnung auf dem Papier verwendet man das folgende (von links nach rechts auszufüllende) Schema:

$f(x) \mapsto$	a_n	a_{n-1}	a_{n-1}	$\ldots$	a_2	a_1	a_0
$+$		$c_n \cdot r$	$c_{n-1} \cdot r$	$\ldots$	$c_3 \cdot r$	$c_2 \cdot r$	$c_1 \cdot r$
	c_n	c_{n-1}	c_{n-2}		c_2	c_1	c_0

Der Wert von c_0 ist der Funktionswert von $f(x)$.

Beispiel: Bestimme $f(3)$ von $f(x) = 2x^4 - 4x^3 + 3x + 10$. Wichtig ist, dass für alle fehlenden Koeffizienten Nullen eingetragen werden!

	2	−4	0	3	10
+		6	6	18	63
	2	2	6	21	73

Damit ist $f(3) = 73$.

Das Horner-Schema kann man auch einsetzen, um einige spezielle Polynomdivisionen auszuführen, bei denen ein Polymon $p(x) = \sum_{k=0}^{n} a_k x^k$ durch ein Polynom der Form $(x - a)$ geteilt wird (der allgemeine Fall wird am Ende dieses Abschnitt behandelt). Ziel ist die Bestimmung eines Polynoms $q(x) = \sum_{k=0}^{n-1} b_k x^k$ und eines Rests $r' \in \mathbb{R}$, so dass

$$p(x) = q(x) \cdot (x - a) + r'.$$

Wertet man das Polynom $p(x)$ an der Stelle a mit dem Horner Schema aus und setzt $b_{n-1} = c_n, b_{n-2} = c_{n-1}, \ldots, b_1 = c_2, b_0 = c_1$ und $r' = c_0$, kann durch einen einfachen Koeffizientenvergleich nachgerechnet werden, dass die geforderte Identität erfüllt ist:
Für x^n steht auf der linken Seite (Polynom $p(x)$) der Koeffizient a_n, auf der rechten Seite (bei $q(x) \cdot (x - a) + r'$) der Koeffizient $b_{n-1} = c_n = a_n$.
Für x^{n-1} steht links der Koeffizient a_{n-1}, rechts der Koeffizient $b_{n-2} - a \cdot b_{n-1} = c_{n-1} - a \cdot c_n = a_{n-1}$, denn $c_{n-1} = a \cdot c_n + a_{n-1}$.
Analog setzt sich das fort bis zum Koeffizienten von x^0: Links steht a_0 und auf der rechten Seite $r' - a \cdot b_0 = c_o - a \cdot c_1 = a_0$, denn $c_0 = a \cdot c_1 + a_0$.

Nullstellen

Definition: $a \in \mathbb{R}$ ist Nullstelle des Polynoms $p(x) \in \mathbb{R}[x]$, falls $p(a) = 0$.

Satz: Ist a Nullstelle von $p(x)$, dann existiert ein Polynom $q(x)$, so dass

$$p(x) = (x - a) \cdot q(x)$$

Der Beweis folgt aus der Anwendung des Horner-Schemas zur Polynomdivision: c_0 ist einerseits der Rest aus der Polynomdivision durch $(x - a)$, andererseits der Wert der Polynomfunktion an der Stelle a. Deshalb ist a genau dann eine Nullstelle, wenn bei der Polynomdivision der Rest verschwindet.

Abschließend ein allgemeiner Satz zur Polynomdivision, dessen (algorithmischer) Beweis auf einem Schema beruht, das durch eine Adaption der Schulmethode der schriftlichen Division von ganzen Zahlen auf Polynome entsteht.

Satz: Für ein beliebiges Polynom $p(x)$ und ein Polynom $s(x)$ vom Grad $d \geq 1$ gibt es zwei eindeutig bestimmte Polynome $q(x)$ und $r(x)$, so dass $p(x) = q(x) \cdot s(x) + r(x)$ gilt und der Grad von $r(x)$ kleiner als d ist.