Brückenkurs

Mathematik für Informatiker

im Wintersemester 2011/12

FU Berlin

Institut für Informatik

Klaus Kriegel

Ergänzende Literatur:

C. Meinel, M. Mundhenk, Mathematische Grundlagen der Informatik, B.G.Teubner 2000

G. Haggard, J. Schlipf, S. Whitesides, Discrete Mathematics for Computer Science, Brooks Cole

1 Einführung: 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.
2. Ist t eine Formel der Ausagenlogik, dann ist auch $(\neg t)$ eine Formel der Aussagenlogik.
3. Sind s und t Formeln der Aussagenlogik, dann sind auch die Ausdrücke $(s \wedge t)$, $(s \vee t)$, $(s \to t)$, $(s \leftrightarrow t)$ sowie $(s \oplus t)$ 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.

Formeln, die nur durch Negation, Konjunktion und Disjunktion gebildet werden, nennt man Boolesche Formeln.

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 $\neg, \wedge, \vee, \to, \leftrightarrow$ 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.

Man kann also $((\neg x_1) \vee (x_2 \wedge x_3))$ 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.

Legt man für alle in einer Formel auftretenden Variablen Wahrheitswerte fest, so induziert eine solche Belegung auch einen Wahrheitswert für die Formel. Man nennt diesen induktiven Prozess auch *Auswertung* der Formel. Die Ergebnisse der Auswertungen einer Formel unter allen möglichen Belegungen werden in einer Wahrheitstafel zusammengefasst.

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.

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
Absorbtion:	$s \wedge (s \vee t)$	$\equiv$	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 Absorbtion und die doppelte Negation zur Ersetzung von Subformeln, so erhält man einen einfachen und kurzen Beweis.

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

Die folgende Liste enthält weitere Äquivalenzen, welche zum Beweis der Äquivalenz von komplexen Formeln häufig angewendet werden:

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

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

1.2 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 "$\forall x \in \mathbb{Z}\ \exists y \in \mathbb{Z} \quad y < x$".

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

$$\begin{aligned}
\neg\forall x\ P(x) &\equiv \exists x \neg P(x) \\
\neg\exists x\ P(x) &\equiv \forall x \neg P(x) \\
\forall x\ P(x) \wedge \forall x\ Q(x) &\equiv \forall x\ (P(x) \wedge Q(x)) \\
\exists x\ P(x) \vee \exists x\ Q(x) &\equiv \exists x\ (P(x) \vee Q(x)) \\
\forall x \forall y\ R(x, y) &\equiv \forall y \forall x\ R(x, y) \\
\exists x \exists y\ R(x, y) &\equiv \exists y \exists x\ R(x, y)
\end{aligned}$$

Achtung: Die folgenden Formelpaare sind im allgemeinen nicht äquivalent:

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

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

1.3 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.

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 Äquivalenzen und Implikationen, 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 das folgende Beispiel zeigt, 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 zurückgreifen kann.

Satz: Ist eine natürliche Zahl n durch 6 teilbar, so ist ihr Quadrat durch 9 teilbar.

Beweis: Die Idee ist offensichtlich – ist n durch 6 teilbar, so kann man den Faktor 6 und damit auch den Faktor 3 von n abspalten. Folglich kann man den Faktor 3 mindestens zwei mal von n^2 abspalten. Wenn wir diese Idee etwas formaler umsetzen wollen, müssen wir mit der Definition von Teilbarkeit beginnen:

$$n \in \mathbb{N} \text{ ist durch } k \in \mathbb{N} \text{ teilbar, falls ein } l \in \mathbb{N} \text{ existiert, so dass } n = k \cdot l.$$

Damit kann man die Voraussetzung des Satzes durch eine einfache Formel ausdrücken und die folgende Beweiskette bilden:

n ist durch 6 teilbar		Hypothese
$\exists l \in \mathbb{N}$	$n = 6 \cdot l$	Teilbarkeitsdefinition
$\exists l \in \mathbb{N}$	$n = (3 \cdot 2) \cdot l$	$6 = 3 \cdot 2$
$\exists l \in \mathbb{N}$	$n^2 = ((3 \cdot 2) \cdot l)((3 \cdot 2) \cdot l)$	Quadrieren
$\exists l \in \mathbb{N}$	$n^2 = (3 \cdot 3)((2 \cdot 2) \cdot (l \cdot l))$	Muliplikation ist assoziativ und kommutativ
$\exists l \in \mathbb{N}$	$n^2 = 9 \cdot (4 \cdot l^2)$	$3 \cdot 3 = 9$ und $2 \cdot 2 = 4$
$\exists l' \in \mathbb{N}$	$n^2 = 9 \cdot l'$	$l' = 4l^2$
n^2 ist durch 9 teilbar		Teilbarkeitsdefinition

Genau betrachtet haben wir beim Schritt von der vierten zur fünften Zeile sogar mehrere Elementarschritte zu einem Schritt zusammengefasst.

Indirekte Beweise

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

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

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

Satz: Für jede natürliche Zahl n gilt: Ist $\sqrt{n}$ keine ganze Zahl, dann ist $\sqrt{n}$ auch nicht rational.

Beweis durch Widerspruch: Man geht von der Annahme aus, dass $\sqrt{n}$ keine natürliche Zahl, aber eine rationale Zahl ist, und muss daraus einen Widerspruch ableiten. Sei $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$ die eindeutige Primzahlzerlegung von n, wobei $p_1, \ldots, p_l$ die paarweise verschiedenen Primfaktoren von n sind und $k_1, \ldots, k_l$ die Vielfachheiten dieser Primfaktoren. Wären alle Werte $k_1, \ldots, k_l$ gerade Zahlen, dann wäre $\sqrt{n}$ eine ganze Zahl, nämlich $p_1^{k_1/2} \cdot \ldots \cdot p_l^{k_l/2}$. Nach unserer Annahme muss also mindestens einer dieser Werte ungerade sein, o.B.d.A. (d.h. ohne Beschränkung der Allgemeinheit) sei das k_1.
Darüber hinaus soll $\sqrt{n}$ rational, also als Quotient aus zwei natürlichen Zahlen m und m' darstellbar sein. Damit ist $n = \left(\frac{m}{m'}\right)^2$ und $n \cdot m'^2 = m^2$. Kombiniert man diese Gleichung mit den Primzahlzerlegungen von $m = q_1^{i_1} \cdot \ldots \cdot q_j^{i_j}$ und $m' = r_1^{i'_1} \cdot \ldots \cdot r_{j'}^{i'_{j'}}$, ergibt sich:

$$p_1^{k_1} \cdot \ldots \cdot p_l^{k_l} \cdot r_1^{2i'_1} \cdot \ldots \cdot r_{j'}^{2i'_{j'}} = q_1^{2i_1} \cdot \ldots \cdot q_j^{2i_j}.$$

Folglich tritt der Primfaktor p_1 auf der linken Seite in ungerader Vielfachheit auf und auf der rechten Seite in gerader Vielfachheit (unabhängig davon, ob p_1 überhaupt in m oder m' vorkommt). Das ist aber ein Widerspruch zur eindeutigen Primzahlzerlegung von natürlichen Zahlen.

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 $\neg r$.

Beispiel: Wir beweisen durch Fallunterscheidung, dass für jede Primzahl $p \geq 5$ die Zahl $p^2 - 1$ durch 24 teilbar ist.
Zuerst formen wir $p^2 - 1$ in $(p+1)(p-1)$ um und beobachten, dass von drei aufeinanderfolgenden ganzen Zahlen genau eine durch 3 teilbar ist. Da $p > 3$ und Primzahl ist, muss $p-1$ oder $p+1$ und damit auch p^2-1 durch 3 teilbar sein. Bleibt zu zeigen, dass $p^2 - 1$ durch 8 teilbar ist. Da p ungerade ist sind sowohl $p - 1$ als auch $p + 1$ gerade und damit ist $p^2 - 1$ durch 4 teilbar. Den noch fehlenden Faktor 2 kann man durch Fallunterscheidung nachweisen:
1. Fall: Ist $p - 1$ durch 4 teilbar, so ist $p - 1 = 4k$ und $p + 1 = 4k + 2 = 2(2k + 1)$ und damit $p^2 - 1 = 8k(2k + 1)$ für eine natürliche Zahlen k.
2. Fall: Ist $p - 1$ nicht durch 4 teilbar, so hat es die Form $4m + 2 = 2(2m + 1)$ für

eine natürliche Zahl m und folglich ist $p+1 = 4m+4 = 4(m+1)$. Damit erhalten wir $p^2 - 1 = 8(2m+1)(m+1)$.

1.4 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

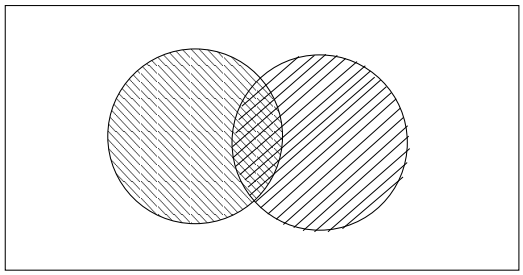
a) Mengen können durch *Auflistung ihrer Elemente* in geschweiften Klammern dargestellt werden. Das betrifft insbesondere endliche Mengen, wie z.B. $A = \{2, 3, 5, 7\}$ oder $B = \{rot, gelb, blau\}$. Dabei ist die Reihenfolge der Elemente in der Auflistung ohne Bedeutung. Auch die Mehrfachnennung von 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:



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.

Die folgende Definition enthält eine Zusammenfassung der wichtigsten Mengenoperationen. Man beachte insbesondere den Zusammenhang zu den entsprechenden logischen Operationen.

Definition:

- 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 Mengen, 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 Mengen, 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 Mengen, die Elemente von A, aber nicht von B sind, dh. $A \setminus B = \{x \mid x \in A \ \wedge \ x \notin B\}$.
- 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.

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:	$A \cup \emptyset$	$= A$
	$A \cap U$	$= A$
Absorbtion:	$A \cup (A \cap B)$	$= A$
	$A \cap (A \cup B)$	$= A$
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

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

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

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.

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:

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

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:

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

- 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.

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 $1 \neq -1$.

2.3 Äquivalenzrelationen

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

Beispiel: 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 über $\mathbb{N}$.

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.
Beweis: Wir verifizieren dazu die folgende Schlusskette:

$$[a]_R \cap [b]_R \neq \emptyset \quad \overset{(1)}{\Longrightarrow} \quad a\, R\, b \quad \overset{(2)}{\Longrightarrow} \quad [a]_R = [b]_R$$

(1) Sei $c \in [a]_R \cap [b]_R$, dann gilt cRa und cRb, wegen der Symmetrie auch aRc und wegen der Transitivität auch aRb.

(2) Sei d ein beliebiges Element aus $[a]_R$ und gelte aRb. Dann gilt dRa und wegen der Transitivität auch dRb. Damit liegt d in der Äquivalenzklasse $[b]_R$ und folglich ist $[a]_R \subseteq [b]_R$. Wegen der Symmetrie kann man aber auch die Rollen von a und b vertauschen und somit $[b]_R \subseteq [a]_R$ ableiten, woraus letztlich die Gleichheit der beiden Äquivalenzklassen folgt. □

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.

Beispiel: 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.

Natürlich hätten wir an Stelle der 5 auch jede andere Zahl $n \in \mathbb{N}^+$ als Teiler wählen können. 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.

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

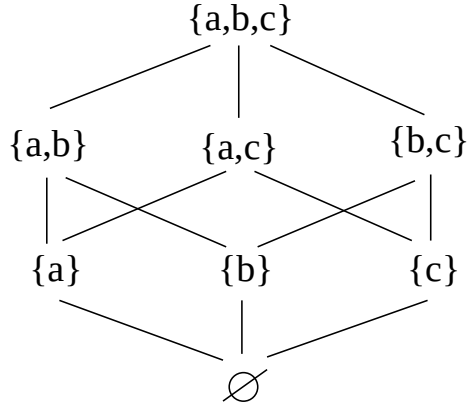
1) reflexiver Abschluss: $R_r = R \cup Id_A$
2) symmetr. Abschluss: $R_{rs} = R_r \cup R_r^{-1} = R \cup R^{-1} \cup Id_A$
3) transitiver Abschluss: $R_{rst} = R_{rs} \cup R_{rs} \circ R_{rs} \cup R_{rs} \circ R_{rs} \circ R_{rs} \cup \ldots = \bigcup_{i=1}^{\infty} R_{rs}^i$

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.

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 ie 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.

Weitere Begriffe, die wie das Maximum und Minimum aus der Schulmathematik bekannt sind, müssen im Kontext mit Halbordnungsrelationen noch einmal neu definiert werden.

Definition: Sei $(A, \prec)$ ein Poset, $B \neq \emptyset$ eine Teilmenge von A und $a \in A$.

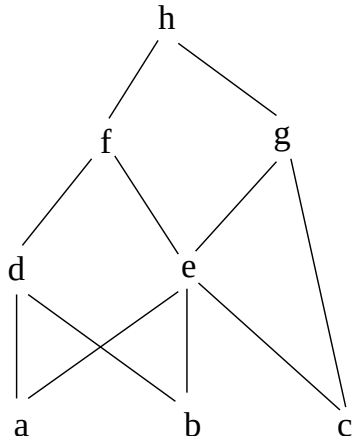
- a ist eine *obere* (bzw. *untere*) *Schranke* von B wenn $b \prec a$ (bzw. $a \prec b$) für alle $b \in B$ gilt.
- a wird das *Maximum* oder *größtes Element* von B (bzw. *Minimum* oder *kleinstes Element* von B) genannt, wenn a ein Element von B und eine obere (bzw. untere) Schranke von B ist.
- a wird *Supremum* oder *obere Grenze* von B (bzw. *Infimum* oder *untere Grenze* von B) genannt, wenn die Menge $O(B)$ der oberen Schranken von B (bzw. die Menge $U(B)$ der unteren Schranken von B) nicht leer ist und a das Minimum von $O(B)$ (bzw. das Maximum von $U(B)$) ist.

Achtung: Nicht in jedem Fall existiert ein Maximum, Minimum, Supremum oder Infimum einer Teilmenge B, aber wenn ein Element a existiert, das für einen dieser Begriffe, die in der Definition geforderten Eigenschaften hat, dann ist es auch eindeutig. Man kann deshalb die Bezeichnungen $max(B), min(B), sup(B), inf(B)$ einführen, die entweder für ein eindeutig existierendes Element oder für nicht existierend stehen.

Beobachtung: Wenn für eine Teilmenge B einer Halbordnung $(A, \prec)$ das Maximum (bzw. Minumum) existiert, dann existiert auch das Supremum (bzw. das Infimum) und es gilt $sup(B) = max(B)$ (bzw. $inf(B) = min(B)$).

Beispiel: In der durch das nachfolgende Hasse-Diagramm dargestellten Halbordnung gilt für die Teilmengen $B = \{d, e\}$ und $C = \{f, g, h\}$:

- B hat zwei obere Schranken, nämlich f und h und zwei untere Schranken, nämlich a und b.
- C hat eine obere Schranke, nämlich h und vier untere Schranken, nämlich a, b, c und e.
- B hat weder ein Maximum noch ein Minimum noch ein Infimum, aber ein Supremum $sup(B) = f$.
- C hat kein Minimum, aber $inf(C) = e$ und $sup(C) = max(C) = h$.



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 bekannte Sinusfunktion. Als Funktion von den reellen Zahlen in die reellen Zahlen ist $sin : \mathbb{R} \longrightarrow \mathbb{R}$ weder injektiv noch surjektiv.
Durch Einschränkungen von Definitions– und/oder Wertebereich kann man diese Eigenschaften erzwingen:

- $sin : \mathbb{R} \longrightarrow [-1, 1]$ ist surjektiv, aber nicht injektiv
- $sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow \mathbb{R}$ ist injektiv, aber nicht surjektiv
- $sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow [-1, 1]$ ist bijektiv.

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

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

$$a \sim_f b \quad genaudann, wenn \quad f(a) = f(b).$$

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

3.2 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 2. 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 $\sum_{k=0}^{\infty} \frac{1}{k!}$ konvergiert auch gegen den Grenzwert e. Diesen Fakt kann man auch so lesen, dass die Reihe $\sum_{k=0}^{\infty} \frac{1}{k!} 1^k$ 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 $\sum_{k=0}^{\infty} \frac{1}{k!} x^k$ 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 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.
Übung: Formulieren Sie eine Regel für die Teibarkeit durch 11.

4.2 Polynome und Polynomdivision

Eine (auf den ersten Blick) erstaunliche Parallele 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:

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

c_3, c_2, c_1, 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:

$$\begin{array}{lccccccc} f(x) \mapsto & a_n & a_{n-1} & a_{n-1} & \dots & a_2 & a_1 & a_0 \\ & & & & & & & \\ + & & c_n \cdot r & c_{n-1} \cdot r & \dots & c_3 \cdot r & c_2 \cdot r & c_1 \cdot r \\ \hline & c_n & c_{n-1} & c_{n-2} & & c_2 & c_1 & c_0 \end{array}$$

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!

$$\begin{array}{lccccc} & 2 & -4 & 0 & 3 & 10 \\ + & & 6 & 6 & 18 & 63 \\ \hline & 2 & 2 & 6 & 21 & 73 \end{array}$$

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 $b_{n-1} = c_n, b_{n-2} = c_{n-1}, \dots, b_1 = c_2, b_0 = c_1$ 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.