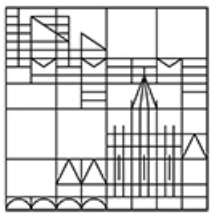
Fachbereich Informatik und
Informationswissenschaft

Universität
Konstanz



Skriptum

zur Vorlesung

Mathematische Grundlagen 1

gehalten im Wintersemester 2009/2010

von

Sven Kosub

5. Februar 2010

Version v0.22

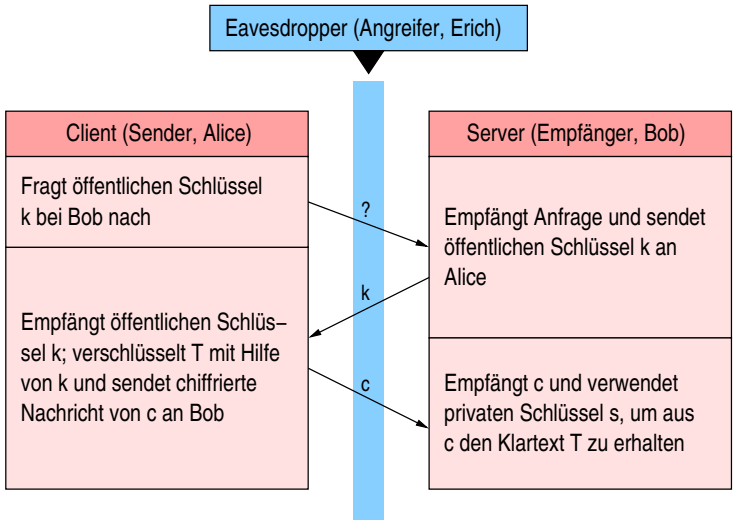
Inhaltsverzeichnis

Prolog

Wir wollen an einem Beispiel aus der Kryptographie für die Informatik typische mathematische Methoden erläutern. Die systematische Einführung erfolgt in den nachfolgenden Kapiteln.

In der Kryptographie unterscheidet man zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren. Im Gegensatz zu den symmetrischen Verschlüsselungsverfahren, bei denen zur Verschlüsselung und Entschlüsselung geheime (private) Schlüssel verwendet werden, efolgt bei einem asymmetrischen Verfahren die Verschlüsselung mit einem öffentlich bekannten Schlüssel. Nur für die Entschlüsselung wird ein privater Schlüssel verwendet.

Ein wichtiges asymmetrisches Verschlüsselungsverfahren ist das Diffie-Hellman-Protokoll. Hierbei möchte Alice einen Klartext T sicher vor Erich, der T natürlich erfahren möchte, an Bob schicken. Dazu verfügt Bob über einen öffentlichen Schlüssel k sowie einen privaten Schlüssel s. Die Kommunikation erfolgt dann wie in folgendem Szenario skizziert:



Das Diffie-Hellman-Protokoll ist noch keine vollständige Beschreibung eines Protokolls. Vielmehr ist noch gar nicht sicher, dass sich das Verfahren tatsächlich implementieren lässt. Diese Frage wird durch das berühmte RSA-Verfahren beantwortet, dessen Umsetzung wir sehr stark vereinfacht kurz darstellen:

- öffentlicher Schlüssel ist das Produkt $k = p \cdot q$ zweier großer Primzahlen p und q,

- privater Schlüssel ist das Paar $s = (p, q)$ der Primzahlen, d.h. die Primzahlenzerlegung von k,
- Verschlüsselung von T: Wandle T in eine Zahl t (zum Beispiel unter Verwendung der ASCII-Codes), oder in eine Folge von Zahlen um, so dass für alle Zahlen $t < k$ gilt; setze $c =_{\text{def}} \text{mod}(t^3, k)$.
- Entschlüsselung von c erfolgt mit Hilfe von $s = (p, q)$, die ohne Kenntnis von p und q genauso schwierig ist, wie k in seine Primfaktoren p und q zu zerlegen.

Die Anschauung hinter dem RSA-Verfahren ist wie folgt: Ist $p \cdot q$ klein, dann ist die Zerlegung in p und q einfach, z.B. $111 = 3 \cdot 37$. Für größe Primzahl ist es dagegen schwierig auf die entsprechenden Primfaktoren zu kommen. Um einen Eindruck von der Schwierigkeit zu bekommen, bestimme man die beiden Primfaktoren p und q in dem folgenden Produkt:

$$pq = 3785215325463769362329054949889672046279794815860 1\backslash$$
$$27761136816982888921764999850721920649197641542929$$

Für die Sicherheit des RSA-Verfahrens ist eine notwendige Voraussetzung, dass es unendlich viele Primzahlen gibt. Anderenfalls könnten (theoretisch) alle Produkte zweier Primzahlen in einer Datenbank gesammelt und somit aus allen öffentlichen Schlüsseln die privaten bestimmet werden.

Im Folgenden wollen wir uns davon überzeugen, dass es tatsächlich unendliche viele Primzahlen gibt.

Definition 0.1 *Es seien p und q natürliche Zahlen.*

1. *Die Zahl p* teilt *q (symbolisch: $p|q$), falls es eine natürliche Zahl k gibt mit $q = k \cdot p$.*
2. *Die Zahl p heißt* Primzahl*, falls $p \geq 2$ und nur 1 und p die Zahl p teilen.*

Die in nachfolgendem Lemma verwendete Methode der Induktion ist zentral für die Informatik und wird in einem eigenen Kapitel ausführlich behandelt werden.

Lemma 0.2 *Zu jeder natürlichen Zahl $n \geq 2$ existiert eines Primzahl p, die n teilt.*

Beweis: (*Induktion*) Wir beweisen das Lemman mittels vollständiger Induktion über n.

- (IA, *Induktionsanfang*): Für $n = 2$ gilt die Aussage mit $p = n$.
- (IS, *Induktionsanfang*): Es sei $n > 2$ eine beliebige natürliche Zahl. Angenommen wir hätten die Aussage bereits für alle $2 \leq k < n$ bewiesen (IV, *Induktionsvoraussetzung*). Wir unterscheiden zwei Fälle für n:
  1. Ist n eine Primzahl, so gilt die Aussage für $p = n$.

2. Ist n keine Primzahl, so gibt es natürliche Zahlen k, ℓ mit $n = k \cdot \ell$ und $2 \leq k, \ell < n$. Nach Induktionsvoraussetzung gibt es somit eine Primzahl p, die k teilt, d.h. $k = p \cdot r$ für ein geeignetes r. Also gilt $n = k \cdot \ell = p \cdot (r \cdot \ell)$. Mithin teilt p auch n.

Damit ist das Lemma bewiesen. ■

Mit Hilfe von Lemma 0.2 kann nun bewiesen werden, dass es unendlich viele Primzahlen gibt. Dazu verwenden wir ein zweites wichtiges Beweisprinzip – den Widerspruchsbeweis.

Theorem 0.3 (Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis: (*Widerspruch*) Angenommen die Aussage ist falsch, d.h., es gibt nur endliche viele Primzahlen $2 \leq p_1 < p_2 < \cdots < p_k$. Wir definieren die Zahl

$$n =_{\text{def}} 1 + \prod_{j=1}^{k} p_j.$$

Wegen $n \geq 2$ folgt aus Lemma 0.2, dass eine Primzahl p_ℓ mit $1 \leq \ell \leq k$ existiert, die n teilt. Auf der anderen Seite gilt jedoch $\text{mod}(n, p_\ell) = 1$. Dies ist ein Widerspruch. Somit ist die Annahme falsch und es gibt unendlich viele Primzahlen. Damit ist das Theorem bewiesen. ■

Logik 1

1.1 Aussagen

Eine (mathematische) *Aussage* ist ein sprachlicher Ausdruck (Satz), dem eindeutig einer der Wahrheitswerte w (für „wahr“) oder f (für „falsch“) zugeordnet werden kann. Üblicherweise werden Aussagen mit großen Buchstaben bezeichnet und wie folgt beschrieben:

$$X =_{\text{def}} \text{ Beschreibung}$$

Beispiel: Die folgenden Beispiel verdeutlichen die obige Begriffsbildung:

- $A =_{\text{def}}$ „Zu jeder natürlichen Zahl gibt es eine Primzahl, die größer ist“ ist eine wahre Aussage.
- $B =_{\text{def}}$ „Zu jeder natürlichen Zahl gibt es eine Primzahl, die kleiner ist“ ist eine falsche Aussage, da die Zahl 2 ein Gegenbeispiel ist.
- $C =_{\text{def}}$ „Jede gerade Zahl größer als 2 ist die Summe zweier Primzahlen“ ist eine Aussage, da der Satz entweder gültig oder nicht gültig ist. Der Wahrheitswert ist noch offen; bei der Aussage handelt es sich um die bekannte GOLDBACH'sche Vermutung.
- $D =_{\text{def}}$ „Diese Aussage ist falsch“ ist keine Aussage, da kein Wahrheitswert zugeordnet werden kann: Ist D wahr, dann ist D falsch; ist D falsch, dann ist D wahr.

1.2 Logische Verknüpfungen

Aussagen können mittels logischer Operationen verknüpft werden. Dabei entstehen wieder Aussagen. Unverknüpfte Aussagen heißen *Elementaraussagen* (oder aussagenlogische Variablen). Verknüpfte Aussagen heißen *zusammengesetzte Aussagen*.

Die wichtigsten logischen Verknüpfungen mit ihren Sprech- und Leseweisen sind wie folgt:

$\neg A$	steht für:	nicht A	(Negation)
$A \wedge B$	steht für:	A und B	(Konjunktion)
$A \vee B$	steht für:	A oder B	(Disjunktion)
$A \rightarrow B$	steht für:	wenn A, dann B	(Implikation)
$A \leftrightarrow B$	steht für:	genau dann A, wenn B	(Äquivalenz)
$A \oplus B$	steht für:	entweder A oder B	(Antivalenz)

Neben $\rightarrow$ und $\leftrightarrow$ werden auch $\Rightarrow$ und $\Leftrightarrow$ für Implikation und Äquivalenz verwendet, wenn wir Aussagen über Aussagen formulieren.

Ähnlich der Addition und Multiplikation („Punktrechnung geht vor Strichrechnung“) gibt es Bindungsregeln bei der Verwendung der logischen Verknüpfungen, um die Klammerungen in zusammengesetzten Ausdrücken wegzulassen. Für die gebräuchlichsten Verknüpfungen $\neg, \wedge$ und $\vee$ vereinbaren wir: „$\neg$ geht vor $\wedge$“ und „$\wedge$ geht vor $\vee$“.

Beispiel: $\neg A \wedge B \vee C$ ist die gleiche Aussage wie $((\neg A) \wedge B) \vee C$.

Um Missverständnissen in komplizierteren Zusammenhängen vorzubeugen, werden wir jedoch auch weiterhin Klammern setzen, wo sie eigentlich nach den Bindungsregeln nicht notwendig wären.

Die Wahrheitswerte der durch logische Verknüpfungen entstandenen zusammengesetzten Aussagen werden durch Wertetabellen definiert.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$	$A \oplus B$	–
f	f	w	f	f	w	w	f	w
f	w	w	f	w	w	f	w	w
w	f	f	f	w	f	f	w	w
w	w	f	w	w	w	w	f	f
Funktionsname		NOT	AND	OR	–	–	XOR	NAND

Bei digitalen Schaltungen entsprechen diese Wertetabellen den *booleschen Funktionen*, wobei w mit 1 und f mit 0 identifiziert wird. Die Namen der den Verknüpfungen zugehörigen booleschen Funktionen sind in der untersten Zeile angegeben.

1.3 Rechnen mit logischen Verknüpfungen

Definition 1.1 *Zwei Aussagen A und B heißen genau dann (logisch)* äquivalent*, symbolisch $A \equiv B$, wenn $A \leftrightarrow B$ eine wahre Aussage ist, d.h.*

$$A \equiv B \Longleftrightarrow_{\text{def}} \quad A \leftrightarrow B \text{ ist wahr.}$$

Logisch äquivalente Aussagen können in zusammengesetzten Aussagen beliebig gegeneinander ausgetauscht werden. Die wichtigsten logischen Äquivalenzen sind in folgendem Theorem zusammengefasst.

Theorem 1.2 *Es seien A, B und C beliebige Aussagen. Dann gilt:*

$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ $(A \vee B) \vee C \equiv A \vee (B \vee C)$	*Assoziativgesetze*
$A \wedge B \equiv B \wedge A$ $A \vee B \equiv B \vee A$	*Kommutativgesetze*
$\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$ $\neg(A \vee B) \equiv (\neg A) \wedge (\neg B)$	De Morgan*'sche Regeln*
$(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C)$ $(A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)$	*Distributivgesetze*
$A \wedge (\neg A) \equiv \mathsf{f}$ $A \vee (\neg A) \equiv \mathsf{w}$	tertium non datur
$A \vee \mathsf{w} \equiv \mathsf{w}$ $A \vee \mathsf{f} \equiv A$ $A \wedge \mathsf{w} \equiv A$ $A \wedge \mathsf{f} \equiv \mathsf{f}$	*Dominanzgesetze*
$A \to B \equiv (\neg A) \vee B$	*Alternative Darstellung der Implikation*
$\equiv (\neg B) \to (\neg A)$	*Kontraposition*
$A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$	*Alternative Darstellung der Äquivalenz*
$\neg(\neg A) \equiv A$	*Doppelte Negation*

Beweis: Wir beweisen nur die erste De Morgan'sche Regel $\neg(A \wedge B) \equiv (\neg A) \vee (\neg B)$. Dazu definieren wir zunächst die Hilfsaussagen $H_1 =_{\text{def}} \neg(A \wedge B)$ und $H_2 =_{\text{def}} (\neg A) \vee (\neg B)$. Die Überprüfung der Aussage $H_1 \leftrightarrow H_2$ erfolgt mittels einer Wertetabelle:

A	B	$A \wedge B$	H_1	$\neg A$	$\neg B$	H_2	$H_1 \leftrightarrow H_2$
f	f	f	w	w	w	w	w
f	w	f	w	w	f	w	w
w	f	f	w	f	w	w	w
w	w	w	f	f	f	f	w

Somit ist $H_1 \leftrightarrow H_2$ eine wahre Aussage. Also sind H_1 und H_2 logisch äquivalent. Alle anderen logischen Äquivalenzen können ebenfalls mittels Berechnung der Wertetabellen gezeigt werden. Damit ist das Theorem bewiesen. ■

Mit Hilfe von Theorem 1.2 können Aussagen umgeformt, genauso wie es von der algebraischen Umformung von Gleichungen her bekannt ist.

Beispiel: Zur Demonstration der Anwendung von Theorem 1.2 wollen wir die Aussage

$$C =_{\text{def}} (A \wedge (A \to B)) \to B$$

vereinfachen. Wir formen die Aussage wie folgt logisch äquivalent um:

$$\begin{aligned}
C &\equiv (A \wedge (\neg A \vee B)) \to B && \text{(AD Implikation)}\\
&\equiv ((A \wedge \neg A) \vee (A \wedge B)) \to B && \text{(Distributivgesetz)}\\
&\equiv (\mathsf{f} \vee (A \wedge B)) \to B && (\textit{tertium non datur})\\
&\equiv (A \wedge B) \to B && \text{(Dominanzgesetz)}\\
&\equiv \neg(A \wedge B) \vee B && \text{(AD Implikation)}\\
&\equiv (\neg A \vee \neg B) \vee B && \text{(De Morgan)}\\
&\equiv \neg A \vee (\neg B \vee B) && \text{(Assoziativgesetz)}\\
&\equiv \neg A \vee \mathsf{w} && (\textit{tertium non datur})\\
&\equiv \mathsf{w} && \text{(Dominanzgesetz)}
\end{aligned}$$

Die Aussage C ist also stets wahr unabhängig von den Wahrheitswerten der Aussagen A und B.

Definition 1.3 *Es sei A eine zusammengesetzte Aussage.*

1. *A heißt genau dann* Tautologie *(oder allgemeingültig), wenn A wahr für alle möglichen Wahrheitswerte der Elementaraussagen ist.*
2. *A heißt genau dann* Kontradiktion *(oder unerfüllbar), wenn A falsch für alle möglichen Wahrheitswerte der Elementaraussagen ist.*

Wir nennen auch wahre Elementaraussagen (die Konstante w) allgemeingültig und falsche Elementaraussagen (die Konstante f) unerfüllbar.

Wie leicht einzusehen ist, ist eine Aussage A genau dann eine Tautologie, wenn die negierte Aussage $\neg A$ eine Kontradiktion ist.

1.4 Aussageformen

Eine *Aussageform* über den Universen $U_1, \ldots, U_n$ ist ein Satz $A(x_1, \ldots, x_n)$ mit den freien Variablen $x_1, \ldots, x_n$, der zu einer Aussage wird, wenn jedes x_i durch ein Objekt aus dem Universum U_i ersetzt wird.

Beispiel: Die Begriffsbildung verdeutlichen wir durch folgende Aussageformen:

- $A(x) =_{\text{def}}$ „x ist eine gerade Zahl“ ist eine Aussageform über den natürlichen Zahlen: $A(2) =$ „2 ist eine gerade Zahl“ ist eine wahre Aussage; $A(3) =$ „3 ist eine gerade Zahl“ ist eine falsche Aussage.
- $B(x, y) =_{\text{def}}$ „Das Wort x ist y Buchstaben lang“ ist eine Aussageform über den Universen U_1 aller Wörter (über einem Alphabet) und U_2 aller natürlichen Zahlen. So ist $B(\text{Konstanz}, 8) =$ „Das Wort Konstanz ist 8 Buchstaben lang“ eine wahre Aussage.
- $C(x) =_{\text{def}}$ „$x < x + 1$“ ist als Aussageform über den natürlichen Zahlen stets wahr unabhängig davon, welche natürliche Zahl n für x eingesetzt wird. Als Aussageform über der Java-Klasse `Integer` gilt dies nicht: $C($`Integer.MAX_VALUE`$)$ ist eine falsche Aussage.

Wenn wir es mit einer Aussageform $A(x_1, \ldots, x_n)$ mit mehreren freien Variablen $x_1, \ldots, x_n$ zu tun haben, die wir alle über dem gleichen Universum $U_1 = U_2 = \ldots = U_n$ betrachten, so sprechen wir von einer Aussageform über dem Universum U_1.

1.5 Aussagen mit Quantoren

Das Einsetzen konkreter Objekte aus einem Universum macht aus einer Aussageform eine Aussage. Ein weitere Möglichkeit dafür ist die *Quantifizierung* von Aussagen mittels Quantoren. Im Unterschied zum konkreten Einsetzen müssen wir dabei die Objekte nicht kennen, deren Einsetzen den Wahrheitswert bestimmt. Wir können nur sagen, dass es solche Objekte gibt oder nicht gibt.

Die beiden wichtigsten Quantoren sind:

- *Existenzquantor* (oder existenzieller Quantor) $\exists$ (manchmal auch $\bigvee$ geschrieben)
- *Allquantor* (oder universeller Quantor) $\forall$ (manchmal auch $\bigwedge$ geschrieben)

Die Quantoren werden wie folgt verwendet, um aus Aussageformen mit einer freien Variablen Aussagen zu machen. Dazu sei $A(x)$ eine Aussageform über dem Universum U.

1. $(\exists x)[A(x)]$ steht für „es gibt ein x, für das $A(x)$ gilt“ und für den Wahrheitswert gilt

   $$(\exists x)[A(x)] \text{ ist wahr } \iff_{\text{def}} \text{ es gibt ein } u \text{ aus } U, \text{ für das } A(u) \text{ wahr ist}$$

2. $(\forall x)[A(x)]$ steht für „für alle x gilt $A(x)$ “ und für den Wahrheitswert gilt

$$(\forall x)[A(x)] \text{ ist wahr } \iff_{\text{def}} \text{ für alle } u \text{ aus } U \text{ ist } A(u) \text{ wahr}$$

Beispiele: Folgende quantifiziere Aussagen verdeutlichen die Begriffsbildung.

- Für die Aussageform $A(x) =_{\text{def}}$ „x ist eine ungerade Zahl“ über dem Universum der natürlichen Zahlen ist $(\exists x)[A(x)]$ eine wahre Aussage, da $A(3) =$ „3 ist eine ungerade Zahl“ wahr ist, und ist $(\forall x)[A(x)]$ eine falsche Aussage, da $A(2) =$ „2 ist eine ungerade Zahl“ falsch ist.
- Für die Aussageform $C(x) =_{\text{def}}$ „$x < x + 1$ “ über dem Universum der natürlichen Zahlen ist $(\forall x)[C(x)] = (\forall x)[x < x + 1]$ eine wahre Aussage.
- Es sei U ein endliches Universum mit den Objekten $u_1, \ldots, u_n$. Dann gilt:

$$(\exists x)[A(x)] \equiv A(u_1) \vee A(u_2) \vee \ldots \vee A(u_n) =_{\text{def}} \bigvee_{i=1}^{n} A(u_i)$$

$$(\forall x)[A(x)] \equiv A(u_1) \wedge A(u_2) \wedge \ldots \wedge A(u_n) =_{\text{def}} \bigwedge_{i=1}^{n} A(u_i)$$

  Der Existenzquantor stellt somit eine endliche oder unendliche Disjunktion und der Allquantor eine endliche oder unendliche Konjunktion dar.

Wir erweitern nunmehr die Anwendung von Quantoren auf Aussageformen mit mehr als einer Variablen. Dabei entstehen nicht sofort wieder Aussagen, vielmehr wir pro Anwendung eines Quantors die Anzahl freier Variablen um eine Variable reduziert. Erst wenn alle Variablen durch Quantoren oder Einsetzen konkreter Objekte gebunden sind, können wir der nun entstandenen Aussage einen Wahrheitswert zuordnen.

Es sei $A(x_1, \ldots, x_n)$ eine Aussageform mit n Variablen über den Universen $U_1, \ldots, U_n$. Dann sind $(\exists x_i)[A(x_1, \ldots, x_n)$ und $(\forall x_i)[A(x_1, \ldots, x_n)]$ Aussageformen mit den $n - 1$ Variablen $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$.

In $(\exists x_i)[A(x_1, \ldots, x_n)]$ bzw. $(\forall x_i)[A(x_1, \ldots, x_n)]$ heißt $A(x_1, \ldots, x_n)$ der *Wirkungsbereich* des Quantors $\exists x_i$ bzw. $\forall x_i$.

Beispiele: Wir setzen unsere Beispiele für quantifzierte Aussage fort.

- Es seien $A(x) =_{\text{def}}$ „x ist eine ungerade Zahl“ und $B(x, y) =_{\text{def}}$ „$x \cdot y$ ist eine ungerade Zahl“ Aussageformen über dem Universum der natürlichen Zahlen. Dann sind
  - $C_x(y) =_{\text{def}} (\exists x)[A(x) \rightarrow B(x, y)]$ eine Aussageform mit der freien Variable y und
  - $C_y(x) =_{\text{def}} (\forall y)[A(x) \rightarrow B(x, y)]$ eine Aussageform mit der freien Variable x,

und es gilt beispielsweise:

- $C_x(3) =_{\text{def}} (\exists x)[A(x) \to B(x,3)]$ ist eine wahre Aussage
- $C_y(3) =_{\text{def}} (\forall y)[A(3) \to B(3,y)]$ ist eine falsche Aussage, da $A(3)$ zwar wahr aber $B(3,2)$ falsch ist.

Für vollständig quantifizierte Aussagen erhalten wir:

- $(\exists y)(\forall x)[A(x) \to B(x,y)]$ ist eine wahre Aussage
- $(\exists x)(\forall y)[A(x) \to B(x,y)]$ ist eine wahre Aussage
- $(\forall y)(\forall x)[A(x) \to B(x,y)]$ ist eine falsche Aussage
- $(\forall x)(\forall y)[A(x) \to B(x,y)]$ ist eine falsche Aussage

In der Aussage $(\exists y)(\forall x)[A(x) \to B(x,y)]$ ist $A(x) \to B(x,y)$ Wirkungsbereich von $\forall x$ und $(\forall x)[A(x) \to B(x,y)]$ der Wirkungsbereich von $\exists y$.

- Für die Aussageform „$x < y$“ über dem Universum der natürlichen Zahlen ist $(\forall x)(\exists y)[x < y]$ (lies: „für alle x gibt es ein y mit $x < y$“) eine wahre Aussage, da $A(x, x+1)$ stets wahr ist, und $(\exists y)(\forall x)[x < y]$ (lies: „es gibt ein $y$mit $x < y$ für alle x“) eine falsche Aussage, da $A(y,y)$ stets falsch ist. Das letzte macht deutlich, dass bei geschachtelten quantifizierten Aussagen ganz entscheidend auf die Stellung der Existenz- und Allquantoren zueinander ankommt.

Die Namen von Variablen, die zur Quantifizierung verwendet werden, sind nur innerhalb der Wirkungsbereiche der Quantoren relevant: Zum Beispiel ist $(\exists x)(\forall x)[x < x]$ keine korrekte Quantifizierung, da bei der Einsetzung von Objekten nicht klar ist, welches für welches x die Einsetzung erfolgt; $(\exists x)[x < y] \wedge (\forall x)[x < y]$ ist dagegen unmissverständlich, da $\exists x$ und $\forall x$ überschneidungsfreie Wirkungsbereiche besitzen.

Auch für quantifizierte Aussagen können wir Rechenregeln (d.h. logische Äquivalenzen) angeben. Wir tun dies hier nur auszugsweise, ohne Beweise und deshalb auch nicht in Form eines Theorems:

$$\left.\begin{array}{rcl} (\exists x)[A(x)] \vee (\exists x)[B(x)] & \equiv & (\exists x)[A(x) \vee B(x)] \\ (\forall x)[A(x)] \wedge (\forall x)[B(x)] & \equiv & (\forall x)[A(x) \wedge B(x)] \end{array}\right\} \text{Assoziativität}$$

$$\left.\begin{array}{rcl} (\exists x)(\exists y)[A(x,y)] & \equiv & (\exists y)(\exists x)[A(x,y)] \\ (\forall x)(\forall y)[A(x,y)] & \equiv & (\forall y)(\forall x)[A(x,y)] \end{array}\right\} \text{Kommutativität}$$

$$\left.\begin{array}{rcl} \neg(\exists x)[A(x)] & \equiv & (\forall x)[\neg A(x)] \\ \neg(\forall x)[A(x)] & \equiv & (\exists x)[\neg A(x)] \end{array}\right\} \text{De Morgan'sche Regeln}$$

Die Stichhaltigkeit und Namensgebung der Rechenregeln ist leicht einzusehen, wenn wir endliche Universen für die Aussage zu Grunde legen und endliche Konjunktionen und Disjunktionen betrachten.

Beispiel: Es sei $P(x) =_{\text{def}}$ „x ist eine Primzahl“ eine Aussageform über dem Universum der natürlichen Zahlen. Wir formulieren die Aussage, dass es unendlich viele Primzahlen gibt, wie folgt:

$$A =_{\text{def}} (\forall x)(\exists y)[P(y) \wedge x < y]$$

Die Negation der Aussage ist: „Es gibt endlich viele Primzahlen“. Wir negieren die Aussage A dazu formal:

$$\begin{aligned} \neg A &\equiv \neg(\forall x)(\exists y)[P(y) \wedge x < y] \\ &\equiv (\exists x)\Big[\neg(\exists y)[P(y) \wedge x < y]\Big] \\ &\equiv (\exists x)(\forall y)[\neg(P(y) \wedge x < y)] \\ &\equiv (\exists x)(\forall y)[\neg P(y) \vee x \geq y] \end{aligned}$$

Intuitiv ausgedrückt bedeutet dies Aussage: „Es gibt eine größte Primzahl“.

Quantifizierte Aussagen in komplexeren Domänen werden in der Regel schnell unübersichtlich. Deshalb finden sich oft Abkürzungen für häufig benutzte Redewendungen. Wir wollen diesen Abschnitt mit einigen davon beschließen.

1. „Es gibt $x_1, \ldots, x_n$, sodass $A(x_1, \ldots, x_n)$ gilt“: Die zugehörige Abkürzung für die exakte logische Definition ist:

$$(\exists x_1, \ldots, x_n)[A(x_1, \ldots, x_n)] =_{\text{def}} (\exists x_1)(\exists x_2) \cdots (\exists x_n)[A(x_1, \ldots, x_n]$$

2. „Für alle $x_1, \ldots, x_n$ gilt $A(x_1, \ldots, x_n)$“: Die zugehörige Abkürzung für die exakte logische Definition ist:

$$(\forall x_1, \ldots, x_n)[A(x_1, \ldots, x_n)] =_{\text{def}} (\forall x_1)(\forall x_2) \cdots (\forall x_n)[A(x_1, \ldots, x_n]$$

3. „Für alle x mit $A(x)$ gilt $B(x)$“: Die zugehörige Abkürzung für die exakte logische Definition ist:

$$(\forall x; A(x))[B(x)] =_{\text{def}} (\forall x)[A(x) \to B(x)]$$

4. „Es gibt ein x mit $A(x)$, sodass $B(x)$ gilt“: Die zugehörige Abkürzung für die exakte logische Definition ist:

$$(\exists x; A(x))[B(x)] =_{\text{def}} (\forall x)[A(x) \wedge B(x)]$$

Die beiden letzten Regeln sind verträglich mit den De Morgan'schen Regeln:

$$\begin{aligned}\neg(\exists x; A(x))[B(x)] &\equiv \neg(\exists x)[A(x) \wedge B(x)] \\ &\equiv (\forall x)[\neg(A(x) \wedge B(x))] \\ &\equiv (\forall x)[(\neg A(x)) \vee (\neg B(x))] \\ &\equiv (\forall x)[A(x) \rightarrow (\neg B(x))] \\ &\equiv (\forall x; A(x))[\neg B(x)]\end{aligned}$$

Beispiel: Das Pumping-Lemma für reguläre Sprachen ist ein wichtiges Hilfsmittel im Bereich der Automatentheorie und Formaler Sprachen. Die übliche Formulierung als Theorem ist (vgl. z.B. [Wag03, S. 191]):

> „Für jede reguläre Sprache L gibt es ein $n_0 > 0$ mit folgender Eigenschaft: Für jedes z aus L mit $|z| \geq n_0$ gibt es eine Zerlegung $z = uvw$ mit $|uv| \leq n_0$ und $|v| > 0$, sodass $uv^k w$ zu L gehört für alle $k \geq 0$."

Mit Hilfe unserer Quantorennotationen ist das Theorem wie folgt ausdrückbar:

$$\begin{aligned}&(\forall L; L \text{ ist regulär})\ (\exists n_0; n_0 > 0)\ (\forall z; z \text{ gehört zu } L \wedge |z| \geq n_0) \\ &\quad (\exists u, v, w; z = uvw \wedge |uv| \leq n_0 \wedge |v| > 0)\ (\forall k; k \geq 0)\ [uv^k w \text{ gehört zu } L]\end{aligned}$$

Die Handhabung des Theorems (abgesehen vom Wissen um die verwendeten Begriffe und Notationen) bedarf einiger Übung, da die Quantorenstruktur $\forall\exists\forall\exists\forall$ der Aussage vier Wechsel zwischen All- und Existenzquantoren aufweist.

1.6 Beweise

Unter einem Beweis wollen wir eine Folge von allgemeingültigen Implikationen (Regeln) verstehen, die aufallgemeingültigen Anfangsaussagen (Prämissen) basieren und zu der Zielaussage (Folgerung) führen, deren Allgemeingültigkeit damit nachgewiesen wird.

Wichtige Beweisregeln (Implikationen) für den mathematischen Alltagsgebrauch sind:

- *Abtrennungsregel (modus ponens)*: Sind A und $A \rightarrow B$ allgemeingültig, so ist B allgemeingültig.

  Korrektheit folgt aus der Allgemeingültigkeit von $(A \wedge (A \rightarrow B)) \rightarrow B$.

- *Fallunterscheidung*: Sind $A \rightarrow B$ und $\neg A \rightarrow B$ allgemeingültig, so ist B allgemeingültig.

  Korrektheit folgt aus der Allgemeingültigkeit von $((A \rightarrow B) \wedge ((\neg A) \rightarrow B)) \rightarrow B$.

- *Kettenschluss*: Sind $A \rightarrow B$ und $B \rightarrow C$ allgemeingültig, so ist $A \rightarrow C$ allgemeingültig.

  Korrektheit folgt aus der Allgemeingültigkeit von $((A \rightarrow B) \wedge (B \rightarrow C)) \rightarrow (A \rightarrow C)$.

- *Kontraposition*: Ist $A \to B$ allgemeingültig, so ist $(\neg B) \to (\neg A)$ allgemeingültig.

  Korrektheit folgt aus der Allgemeingültigkeit von $(A \to B) \to ((\neg B) \to (\neg A))$.

- *Indirekter Beweis*: Sind $A \to B$ und $A \to \neg B$ allgemeingültig, so ist $\neg A$ allgemeingültig.

  Korrektheit folgt aus der Allgemeingültigkeit von $((A \to B) \wedge (A \to (\neg B))) \to (\neg A)$.

Im Folgenden wollen an dem Beweis der Irrationalität von $\sqrt{2}$ die logische Struktur und das Zusammenspiel der verschiedenen Beweisregeln offenlegen.

Lemma A. *Ist n eine ungerade Zahl, so ist n^2 eine ungerade Zahl.*

Beweis: *(direkt)* Es sei n eine ungerade Zahl, d.h.

$$n = 2\lfloor n/2 \rfloor + 1. \qquad =_{\text{def}} \mathsf{A}$$

A (für eine konkrete Zahl) ist allgemeingültige Prämisse

Wir müssen zeigen:

$$n^2 = 2\left\lfloor n^2/2 \right\rfloor + 1. \qquad =_{\text{def}} \mathsf{Z}$$

Z ist die Zielaussage

Mit $n = 2\lfloor n/2 \rfloor + 1$ gilt:

$$\begin{aligned} n^2 &= (2\lfloor n/2 \rfloor + 1)^2 && =_{\text{def}} \mathsf{B} \\ &= 4\lfloor n/2 \rfloor^2 + 4\lfloor n/2 \rfloor + 1 && =_{\text{def}} \mathsf{C} \\ &= 2\left(2\lfloor n/2 \rfloor^2 + 2\lfloor n/2 \rfloor\right) + 1 && =_{\text{def}} \mathsf{D} \end{aligned}$$

A → B ist allgemeingültig

B → C ist allgemeingültig

C → D ist allgemeingültig

Wir zeigen zunächst die Hilfsaussage:

$$\left\lfloor n^2/2 \right\rfloor = 2\lfloor n/2 \rfloor^2 + 2\lfloor n/2 \rfloor \qquad =_{\text{def}} \mathsf{H}$$

Wegen $n = 2\lfloor n/2 \rfloor + 1$ gilt:

$$\begin{aligned} \lfloor n^2/2 \rfloor &= \left\lfloor (2\lfloor n/2 \rfloor + 1)^2 / 2 \right\rfloor && =_{\text{def}} \mathsf{E} \\ &= \left\lfloor \left(4\lfloor n/2 \rfloor^2 + 4\lfloor n/2 \rfloor + 1\right) / 2 \right\rfloor && =_{\text{def}} \mathsf{F} \\ &= \left\lfloor 2\lfloor n/2 \rfloor^2 + 2\lfloor n/2 \rfloor + 1/2 \right\rfloor && =_{\text{def}} \mathsf{G} \\ &= 2\lfloor n/2 \rfloor^2 + 2\lfloor n/2 \rfloor && = \mathsf{H} \end{aligned}$$

E → F ist allgemeingültig

F → G ist allgemeingültig

G → H ist allgemeingültig

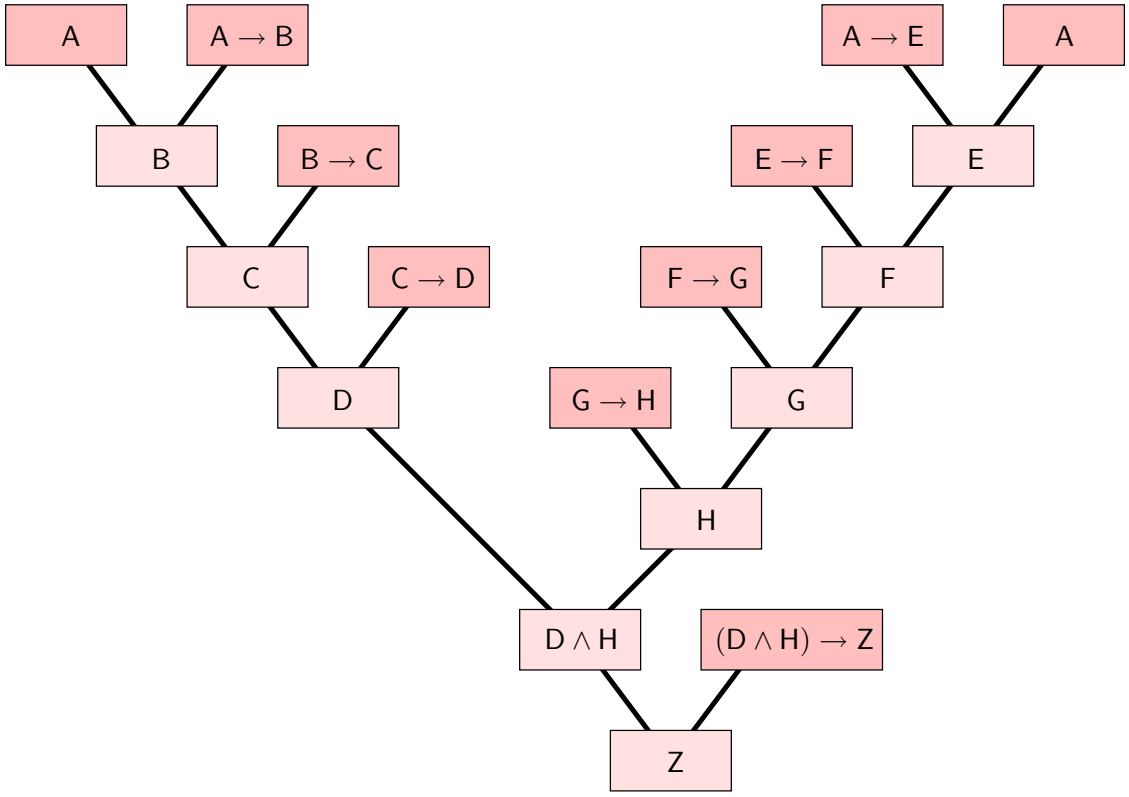
Einsetzen der Hilfsaussage in D ergibt:

$$n^2 = 2\left\lfloor n^2/2 \right\rfloor + 1. \qquad = \mathsf{Z}$$

(D ∧ H) → Z ist allgemeingültig

d.h. n^2 ist ungerade. ■

Die logische Struktur des Beweises kann schematisch in Form eines Ableitungsbaumes dargestellt werden:



Hierbei sind die heller unterlegten Aussagen (bis auf $\mathsf{D} \wedge \mathsf{H}$) durch Anwendung der Abtrennungsregel aus den beiden darüber liegenden Aussagen abgeleitet worden. Die dunkler unterlegten Aussagen sind per Voraussetzung allgemeingültig (Aussage A) oder durch Anwendung algebraischer Umformungsregeln allgemeingültig.

Durch Kontraposition von Lemma A lässt sich nun direkt Korollar B folgern.

Korollar B. *Ist n^2 eine gerade Zahl, so ist n eine gerade Zahl.*

Beweis: *(Kontraposition)*

Ist n eine ungerade Zahl, $=_{\text{def}} \mathsf{A}$
so ist n^2 eine ungerade Zahl $=_{\text{def}} \mathsf{B}$
(nach Lemma A).

Damit gilt nach Kontraposition:
Ist n^2 eine gerade Zahl, $\equiv \neg\mathsf{B}$
so ist n eine gerade Zahl. $\equiv \neg\mathsf{A}$

Damit ist das Korollar bewiesen. ■

$\mathsf{A} \rightarrow \mathsf{B}$ ist allgemeingültig

$\neg\mathsf{B} \rightarrow \neg\mathsf{A}$ ist allgemeingültig

Mit Hilfe von Korollar B kann nun die Irrationalität von $\sqrt{2}$ mittels Widerspruchbeweis gezeigt werden.

Theorem C. *$\sqrt{2}$ ist irrational.*

Beweis: *(indirekt)* Wir nehmen an: $\sqrt{2}$ ist eine rationale Zahl, d.h.

$$(\exists p)(\exists q)\Big[\underbrace{\mathrm{ggT}(p,q)=1}_{=_{\text{def}}\ \mathsf{Z}} \ \wedge\ \sqrt{2}=p/q\Big] \quad =_{\text{def}}\ \mathsf{A}$$

$\mathsf{A} \to \mathsf{Z}$ ist allgemeingültig

Dann gilt

$$2q^2 = p^2, \qquad =_{\text{def}}\ \mathsf{B}$$

$\mathsf{A} \to \mathsf{B}$ ist allgemeingültig

d.h. p^2 ist gerade.

Nach Korollar B ist p gerade, d.h.

$$p = 2\lfloor p/2 \rfloor. \qquad =_{\text{def}}\ \mathsf{C}$$

$\mathsf{B} \to \mathsf{C}$ ist allgemeingültig

Wollen zeigen, dass auch q^2 gerade ist, d.h.

$$q^2 = 2\lfloor q^2/2 \rfloor. \qquad =_{\text{def}}\ \mathsf{D}$$

Mit $2q^2 = p^2$ und $p = 2\lfloor p/2 \rfloor$ folgt

$$\begin{aligned} q^2 &= p^2/2 && =_{\text{def}}\ \mathsf{E} && \mathsf{B} \to \mathsf{E} \text{ ist allgemeingültig} \\ &= \left(2\lfloor p/2 \rfloor\right)^2/2 && =_{\text{def}}\ \mathsf{F} && (\mathsf{C} \wedge \mathsf{E}) \to \mathsf{F} \text{ ist allgemeingültig} \\ &= 2\left\lfloor p/2 \right\rfloor^2 && =_{\text{def}}\ \mathsf{G} && \mathsf{F} \to \mathsf{G} \text{ ist allgemeingültig} \end{aligned}$$

und somit

$$\begin{aligned} 2\left\lfloor q^2/2 \right\rfloor &= 2\left\lfloor 2\lfloor p/2 \rfloor^2/2 \right\rfloor && =_{\text{def}}\ \mathsf{H} && \mathsf{G} \to \mathsf{H} \text{ ist allgemeingültig} \\ &= 2\lfloor \lfloor p/2 \rfloor^2 \rfloor && =_{\text{def}}\ \mathsf{I} && \mathsf{H} \to \mathsf{I} \text{ ist allgemeingültig} \\ &= 2\lfloor p/2 \rfloor^2 && =_{\text{def}}\ \mathsf{J} && \mathsf{I} \to \mathsf{J} \text{ ist allgemeingültig} \\ &= q^2 && \equiv\ \mathsf{D} && \mathsf{J} \to \mathsf{D} \text{ ist allgemeingültig} \end{aligned}$$

Nach Korollar B ist q gerade. $=_{\text{def}}\ \mathsf{K}$ — $\mathsf{D} \to \mathsf{K}$ ist allgemeingültig

Damit gilt $\mathrm{ggT}(p,q) \geq 2$. $\equiv \neg\mathsf{Z}$ — $\mathsf{K} \to \neg\mathsf{Z}$ ist allgemeingültig

$\mathsf{A} \to \neg\mathsf{Z}$ ist allgemeingültig

Dies ist ein Widerspruch, d.h. die Annahme ist falsch und $\sqrt{2}$ ist irrational. $\equiv \neg\mathsf{A}$ — $\neg\mathsf{A}$ ist allgemeingültig

Damit ist das Theorem bewiesen. ■

Neben den Beweisregeln, die ganz allgemein für beliebige Aussagen anwendbar sind, gibt es noch eine ganze Menge spezieller Beweisregeln für Aussagen mit bestimmter Quantorenstruktur und bestimmter Universen. Zwei wichtige unter diesen sind die folgenden:

- *Spezialisierung (Substitution)*: Ist $(\forall x)[A(x)]$ allgemeingültig, so ist $A(y)$ allgemeingültig, falls y nicht in einem Wirkungsbereich eines Quantors in $A(x)$ vorkommt.

  Korrektheit folgt aus Allgemeingültigkeit von $(\forall y)\left[(\forall x)[A(x)] \to A(y)\right]$ (mit obiger Einschränkung).

- *Vollständige Induktion*: Es sei $A(n)$ eine Aussageform über dem Universum der natürlichen Zahlen. Sind $A(0)$ und $A(n-1) \to A(n)$ für alle $n > 0$ allgemeingültig, so ist $A(n)$ für alle n allgemeingültig.

Wir wollen die Korrektheit der vollständigen Induktion überprüfen.

Theorem 1.4 *Es sei $A(n)$ eine Aussageform mit der freien Variable n über dem Universum der natürlichen Zahlen. Dann ist die Aussage*

$$\Big(A(0) \wedge (\forall n; n > 0)[A(n-1) \to A(n)]\Big) \to (\forall n)[A(n)]$$

allgemeingültig.

Beweis: *(indirekt)* Es gelte $A(0)$ und $A(n-1) \to A(n)$ für alle $n > 0$. Zum Widerspruch nehmen wir an, dass es ein n gibt, sodass $A(n)$ nicht gilt. Dann gibt es auch eine kleinste natürliche Zahl n_0, für die $A(n_0)$ nicht wahr ist, d.h. es gilt $\neg A(n_0) \wedge (\forall n; n < n_0)[A(n)]$. Wir unterscheiden zwei Fälle für n_0:

- *1. Fall*: Ist $n_0 = 0$, so ist $\neg A(0)$ wahr. Dies steht jedoch im Widerspruch zur Voraussetzung, dass $A(0)$ gilt.

- *2. Fall*: Ist $n_0 > 0$, so ist $\neg A(n_0) \wedge A(n_0 - 1) \equiv \neg(A(n_0 - 1) \to A(n_0))$ wahr. Dies steht jedoch im Widerspruch zur Voraussetzung, dass $A(n-1) \to A(n)$ für alle $n > 0$ gilt, also insbesondere auch $A(n_0 - 1) \to A(n_0)$.

Also ist die Annahme falsch und es gilt $A(n)$ für alle n. Damit ist das Theorem bewiesen. ■

Die logische Struktur des Beweises für Theorem 1.4 ist typisch für einen Widerspruchsbeweis einer Implikation. Wenn wir die Allgemeingültigkeit von $A \to B$ beweisen wollen, so nehmen wir an, dass A aber nicht B gilt. Damit folgt sofort die Allgemeingültigkeit der Aussage $(A \wedge (\neg B)) \to A$. Anschließend müssen wir noch beweisen, dass auch $(A \wedge (\neg B)) \to (\neg A)$ allgemeingültig ist, d.h. wir konstruieren einen Widerspruch zur eigentlichen Prämisse A unserer zu beweisender Implikation. Nach der Regel vom indirekten Beweis folgt nun, dass $\neg(A \wedge (\neg B)) \equiv A \to B$ allgemeingültig ist.

Mengen 2

In diesem Kapitel beschäftigen wir uns mit den grundlegenden Begriffen der Mengenlehre. Hierbei folgen wir im Wesentlichen der naiven Mengenlehre, wie sie im mathematischen Alltagsgeschäft eines Informatikers ausreichend ist. Unter einer streng mathematischen Sichtweise ist die naive Mengenlehre nicht widerspruchsfrei; jedoch können Widersprüche mit einer gewissen Umsicht vermieden werden.

2.1 Definitionen

Eine *Menge* A besteht aus paarweise verschiedenen Objekten. Damit wird ein mehrfaches Vorkommen von Objekten ignoriert – im Gegensatz z.B. zu Listen als Datenstruktur.

Bei der Beschreibung einer Menge A unterscheiden wir zwei Formen der Darstellung:

- *extensionale Darstellung:* Die in der Menge A enthaltenen Objekte werden aufgezählt (soweit dies möglich ist), wobei die Reihenfolge keine Rolle spielt – auch hier im Gegensatz zu Listen; symbolisch:

  $$A = \{a_1, a_2, \ldots\}$$

- *intensionale Darstellung:* Es werden alle Objekte a selektiert, die aus dem zu einer Aussageform $E(x)$ gehörenden Universum stammen, sodass $E(a)$ eine wahre Aussage ist; symbolisch:

  $$A = \{\ a \mid E(a)\ \}$$

  Mit anderen Worten enthält die Menge A alle Objekte a, die eine gewisse Eigenschaft E erfüllen.

Extensionale Darstellungen sind für die Fälle endlicher Mengen häufig einsichtiger als intensionale Darstellungen, da die Selektion der Objekte bereits ausgeführt vorliegt. Für unendliche Mengen sind extensionale Darstellungen im Allgemeinen nicht mehr möglich.

Beispiele: Die folgenden Darstellung derselben (endlichen) Menge verdeutlichen die unterschiedlichen Beschreibungsaspekte:

- $\{3, 5, 7, 11\} = \{11, 5, 7, 3\}$
- $\{3, 5, 7, 11\} = \{3, 3, 3, 5, 5, 7, 11, 11\}$
- $\{3, 5, 7, 11\} = \{\ a \mid a \in \mathbb{N} \wedge 2 < a < 12 \wedge\ a \text{ ist eine Primzahl}\ \}$

Im Folgenden vereinbaren die Schreib- und Sprechweisen für mengenbezogene Aussagen. Positive Aussagen sind die folgenden:

$a \in A$	steht für:	a ist Element von A
$A \subseteq B$	steht für:	A ist Teilmenge von B
$B \supseteq A$	steht für:	a ist Obermenge von A
$A = B$	steht für:	A und B sind gleich
$A \subset B$	steht für:	A ist echte Teilmenge von B
$B \supset A$	steht für:	B ist echte Obermenge von A

Die zugehörigen negativen Aussagen sind:

$a \notin A$	steht für:	a ist kein Element von A
$A \not\subseteq B$	steht für:	A ist keine Teilmenge von B
$B \not\supseteq A$	steht für:	a ist keine Obermenge von A
$A \neq B$	steht für:	A und B sind verschieden
$A \not\subset B$	steht für:	A ist keine echte Teilmenge von B
$B \not\supset A$	steht für:	B ist keine echte Obermenge von A

Die exakte Bedeutungen der Bezeichnungen werden aussagenlogisch festgelegt. Dazu setzen wir im Folgenden für die verwendeten Aussageformen stets ein Universum voraus.

$a \in A$	$=_{\text{def}}$	a gehört zur Menge A	$a \notin A$	$=_{\text{def}}$	$\neg(a \in A)$
$A \subseteq B$	$=_{\text{def}}$	$(\forall a)[a \in A \to a \in B]$	$A \not\subseteq B$	$=_{\text{def}}$	$\neg(A \subseteq B)$
$B \supseteq A$	$=_{\text{def}}$	$A \subseteq B$	$B \not\supseteq A$	$=_{\text{def}}$	$\neg(B \supseteq A)$
$A = B$	$=_{\text{def}}$	$A \subseteq B \wedge B \subseteq A$	$A \neq B$	$=_{\text{def}}$	$\neg(A = B)$
$A \subset B$	$=_{\text{def}}$	$A \subseteq B \wedge A \neq B$	$A \not\subset B$	$=_{\text{def}}$	$\neg(A \subset B)$
$B \subset A$	$=_{\text{def}}$	$A \subset B$	$B \not\subset A$	$=_{\text{def}}$	$\neg(B \subset A)$

Aussagen über Mengen werden also als Abkürzungen für quantifizierte Aussagen über ihren Elementen eingeführt.

Beispiele: Wir verdeutlichen den Zusammenhang zwischen Aussagen über Mengen und den definierenden quantifizierten Aussagen über den Elementen an Hand zweier Mengenaussagen:

$$\begin{aligned} A \not\subseteq B &\equiv \neg(A \subseteq B) \\ &\equiv \neg(\forall a)[a \in A \to a \in B] \\ &\equiv (\exists a)[\neg(a \in A \to a \in B)] \end{aligned}$$

$$\begin{aligned} & \equiv (\exists a)[\neg(a \notin A \vee a \in B)] \\ & \equiv (\exists a)[a \in A \wedge a \notin B] \end{aligned}$$

$$\begin{aligned} A = B & \equiv A \subseteq B \wedge A \supseteq B \\ & \equiv A \subseteq B \wedge B \subseteq A \\ & \equiv (\forall a)[a \in A \rightarrow a \in B] \wedge (\forall a)[a \in B \rightarrow a \in A] \\ & \equiv (\forall a)[(a \in A \rightarrow a \in B) \wedge (a \in B \rightarrow a \in A)] \\ & \equiv (\forall a)[(a \in A \leftrightarrow a \in B)] \end{aligned}$$

Häufig muss die Gleichheit zweier Mengen A und B, die in intensionaler Darstellung gegeben sind, gezeigt werden. Nach Definition des Wahrheitswertes der Aussage $A = B$ müssen dafür stets zwei Richtungen gezeigt werden. Ein einfaches Beispiel soll dies verdeutlichen.

Beispiel: Es seien die beiden Mengen $A =_{\text{def}} \{\ n \mid n \text{ ist gerade}\ \}$ und $B =_{\text{def}} \{\ n \mid n^2 \text{ ist gerade}\ \}$ als Teilmengen natürlicher Zahlen gegeben. Wir wollen zeigen, dass $A = B$ gilt. Dazu zeigen wir zwei Inklusionen:

- $\subseteq$: Es sei $n \in A$. Dann ist n ist gerade, d.h., es gibt ein $k \in \mathbb{N}$ mit $n = 2k$. Es gilt $n^2 = (2k)^2 = 2(2k^2)$. Somit ist n^2 gerade. Folglich gilt $n \in B$. Damit gilt $A \subseteq B$.
- $\supseteq$: Es sei $n \in B$. Dann ist n^2 gerade. Nach Korollar B (Abschnitt 1.6) ist n gerade. Also gilt $n \in A$. Somit gilt $B \subseteq A$.

Damit ist die Gleichheit der Mengen bewiesen.

Eine ausgezeichnete Menge (in jedem Universum) ist die leere Menge: Eine Menge A heißt *leer* genau dann, wenn A kein Element enthält. Logisch ausgedrückt bedeutet die Bedingung: $(\forall a)[a \notin A]$.

Proposition 2.1 *Es gibt nur eine leere Menge (in jedem Universum).*

Beweis: *(Kontraposition)* Wir wollen zeigen: Sind A und B leere Mengen, so gilt $A = B$. Dafür zeigen wir: Gilt $A \neq B$, so ist A nicht leer oder B nicht leer. Es gilt:

$$\begin{aligned} A \neq B & \equiv A \not\subseteq B \vee B \not\subseteq A \\ & \equiv (\exists a)[a \in A \wedge a \notin B] \vee (\exists a)[a \in B \wedge a \notin A] \\ & \equiv (\exists a) \underbrace{[(a \in A \wedge a \notin B) \vee (a \in B \wedge a \notin A)]}_{=_{\text{def}}\ D(a)} \end{aligned}$$

Es sei x ein Objekt im Universum, so dass $D(x)$ eine wahre Aussage ist. Dann gilt $x \in A$ oder $x \in B$. Also ist A oder B nicht leer. ■

Damit ist gerechtfertigt, dass ein eigenes Symbol $\emptyset$ für die Bezeichnung der leeren Menge eingeführt wird.

$\|A\|$ (oder auch: $|A|, \#A$) ist die Anzahl der Elemente von A bzw. die *Kardinalität* von A. Die Kardinalität der leeren Menge ist also stets 0. Ist $\|A\| < \infty$, so heißt A *endliche* Menge, sonst *unendliche* Menge. Mengen mit nur einem Element werden *Einermengen* genannt.

2.2 Mengenoperationen

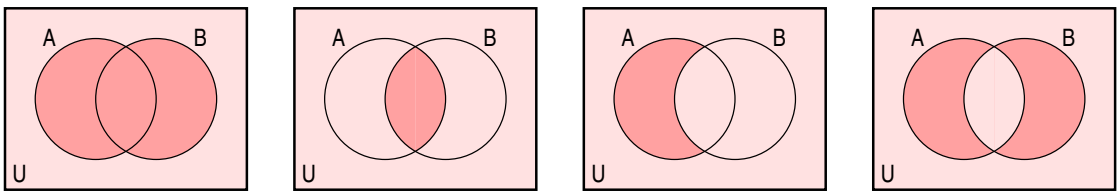
Wir definieren die folgenden Operationen, die aus zwei Mengen A und B eines Universums U wieder eine Menge desselben Universums U formen:

Vereinigung:	$A \cup B =_{\text{def}} \{ x \mid x \in A \vee x \in B \}$
Durchschnitt:	$A \cap B =_{\text{def}} \{ x \mid x \in A \wedge x \in B \}$
Differenz:	$A \setminus B =_{\text{def}} \{ x \mid x \in A \wedge x \notin B \}$
symmetrische Differenz:	$A \triangle B =_{\text{def}} (A \setminus B) \cup (B \setminus A)$

Eine besondere Differenzoperation ist die Komplementierung einer Menge A:

Komplement:	$\overline{A} =_{\text{def}} U \setminus A$

Üblicherweise werden Mengenoperationen zur Veranschaulichung durch die aus der Schule bekannten Venn-Diagramme dargestellt. Die vier obigen Operationen auf zwei Mengen lassen sich wie folgt visualisieren:



$A \cup B$ $A \cap B$ $A \setminus B$ $A \triangle B$

Dabei sind die dunkler dargestellt Punktmengen immer das Ergebnis der jeweiligen Mengenoperationen auf den durch die Kreis A und B eingefassten Punktmengen. Diese Darstellungsformen sind zwar illustrativ; sie sind jedoch *keinesfalls* ausreichend für Beweise.

Beispiele: Es seien $A = \{2, 3, 5, 7, 11\}$ und $B = \{2, 3, 4, 5, 6\}$. Dann gilt:

- $A \cup B = \{2, 3, 4, 5, 6, 7, 11\}$
- $A \cap B = \{2, 3, 5\}$

- $A \setminus B = \{7, 11\}$
- $B \setminus A = \{4, 6\}$
- $A \triangle B = \{4, 6, 7, 11\}$
- $(A \setminus B) \cap B = \{7, 11\} \cap \{2, 3, 4, 5, 6\} = \emptyset$

Zwei Mengen A und B heißen *disjunkt* genau dann, wenn $A \cap B = \emptyset$ gilt.

2.3 Verallgemeinerung von Vereinigung und Durchschnitt*

In einigen Fällen werden auch Verallgemeinerungen von Vereinigung und Durchschnitt auf eine beliebige, auch unendliche, Anzahl von Mengen betrachtet.

Dazu betrachten wir Teilmengen eines Universums U. Weiterhin sei I eine beliebige Menge (Indexmenge). Für jedes $i \in I$ sei eine Menge $A_i \subseteq U$ gegeben. Dann sind Vereinigung und Durchschnitt aller A_i definiert als:

$$\bigcup_{i \in I} A_i \quad =_{\text{def}} \quad \{\ a \mid (\exists i \in I)[a \in A_i]\ \}$$

$$\bigcap_{i \in I} A_i \quad =_{\text{def}} \quad \{\ a \mid (\forall i \in I)[a \in A_i]\ \}$$

Für $I = \mathbb{N}$ schreiben wir auch $\bigcup_{i=0}^{\infty} A_i$ bzw. $\bigcap_{i=0}^{\infty} A_i$.

Beispiele: Folgende Beispiele und Spezialfälle sollen die Wirkungsweise von allgemeiner Vereinigung und Durchschnitt demonstrieren:

- Es seien $U = \mathbb{R}$, $I = \mathbb{N}_+$ und

$$A_k =_{\text{def}} \left\{ x \;\middle|\; |x^2 - 1| \leq \frac{1}{k} \right\}$$

Dann gilt:

$$\begin{aligned} \bigcup_{k \in I} A_k \;=\; \bigcup_{k=1}^{\infty} A_k \;&=\; \left\{ x \;\middle|\; |x^2 - 1| \leq 1 \right\} \\ &=\; \left\{ x \;\middle|\; -\sqrt{2} \leq x \leq \sqrt{2} \right\} \;\overset{\text{def}}{=}\; \left[-\sqrt{2}, \sqrt{2}\right] \end{aligned}$$

$$\bigcap_{k \in I} A_k \;=\; \bigcap_{k=1}^{\infty} A_k \;=\; \{-1, 1\}$$

- Es gilt stets $\bigcup_{i \in \emptyset} A_i = \emptyset$.
- Es gilt stets $\bigcap_{i \in \emptyset} A_i = M$.

2.4 Potenzmenge

Eine Operation von einem anderen Typ als Vereinigung, Durchschnitt und Differenzen ist die Potenzierung einer Menge: Die *Potenzmenge* einer Menge A ist definiert als

$$\mathcal{P}(A) =_{\text{def}} \{ X \mid X \subseteq A \}$$

Für die Potenzmenge von A gelten folgenden Aussagen:

Proposition 2.2 *Es sei A eine beiliebige Menge.*

1. $X \in \mathcal{P}(A) \Longleftrightarrow X \subseteq A$
2. $\emptyset, A \in \mathcal{P}(A)$
3. *Ist A endlich, so gilt* $\|\mathcal{P}(A)\| = 2^{\|A\|}$.

Beweis: Die erste beiden Aussagen folgen direkt aus der Definition. Die dritte Aussage werden wir im Kapitel über Kombinatorik beweisen. ■

Die Elemente der Potenzmenge sind also Mengen aus dem Universum $\mathcal{P}(A)$. Der letzte Sachverhalt lässt die mitunter auch verwendete Bezeichnung 2^A für die Potenzmenge von A plausibel erscheinen.

Beispiele: Folgende Mengen verdeutlichen die Potenzmengenkonstruktion.

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

Die Teilmengen der Potenzmenge heißen *Mengenfamilien*.

2.5 Kreuzprodukt

Es seien $A_1, \ldots, A_n$ beliebige Mengen. Das *Kreuzprodukt* (oder kartesisches Produkt) von $A_1, \ldots, A_n$ ist definiert als:

$$A_1 \times \cdots \times A_n =_{\text{def}} \{\ (a_1, \ldots, a_n) \mid \text{für alle } i \in \{1, \ldots, n\} \text{ gilt } a_i \in A_i\ \}$$

Die Elemente von $A_1 \times \cdots \times A_n$ heißen *n-Tupel* (*Paare* für $n = 2$, *Tripel* für $n = 3$, *Quadrupel* für $n = 4$).

Im Gegensatz zu Mengen sind Tupel geordnet (und damit eine Formalisierung von Listen): Für zwei n-Tupel $(a_1, \ldots, a_n)$ und $(a'_1, \ldots, a'_n)$ gilt

$$(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n) \iff \text{für alle } i \in \{1, \ldots, n\} \text{ gilt } a_i = a'_i$$

Sind alle Mengen gleich, so schreibt man:

$$A^n =_{\text{def}} \underbrace{A \times \cdots \times A}_{n\text{-mal}}$$

Beispiele: Folgende Mengen verdeutlichen die Kreuzproduktkonstruktion.

- Mit $A = \{1, 2, 3\}$ und $B = \{a, b\}$ gilt

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$$

- Mit $A = \{5, 7\}$ und $n = 3$ gilt

$$\begin{aligned} A^3 &= \{5, 7\} \times \{5, 7\} \times \{5, 7\} \\ &= \{(5, 5, 5), (5, 5, 7), (5, 7, 5), (5, 7, 7), \\ &\qquad (7, 5, 5), (7, 5, 7), (7, 7, 5), (7, 7, 7)\} \end{aligned}$$

- $\emptyset \times A = \emptyset$ (*beachte:* Die rechte leere Menge ist die Menge in der kein Paar enthalte ist)
- $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ beschreibt den dreidimensionalen Raum

Relationen 3

Relationen beschreiben die Beziehungen zwischen Mengen und sind somit der eigentliche Gegenstand der Mathematik.

3.1 Definitionen

Es seien $A_1, \ldots, A_n$ beliebige Mengen. Eine Menge $R \subseteq A_1 \times \cdots \times A_n$ heißt *Relation*.

Beispiel: Eine relationale Datenbank ist eine Sammlung von Tabellen mit einer gewissen Struktur. Eine Tabelle wiederum ist eine (extensionale Darstellung einer) Relation. Beispielsweise sei folgender Auszug einer Tabelle gegeben:

Vorname	Name	Geburtsdatum
Max	Mustermann	07.07.1977
Erika	Mustermann	12.09.1945
John	Smith	05.05.1955
Johanna	König-Hock	27.03.1921
Lyudmila	Dyakovska	02.04.1976
Peter	Draisaitl	07.12.1965
Thomas	Holtzmann	01.04.1927
Weiwei	Ai	28.08.1957
Robert	Palfrader	11.11.1968
Nikon	Jevtic	03.06.1993
Leslie	Valiant	28.03.1949
⋮	⋮	⋮

Wir fassen die Tabelle als Teilmenge eines Kreuzproduktes auf. Dazu seien:

$$\begin{aligned} A_1 &=_{\text{def}} \text{Menge aller Vornamen in der Tabelle} \\ A_2 &=_{\text{def}} \text{Menge aller Namen in der Tabelle} \\ A_3 &=_{\text{def}} \text{Menge aller Geburtsdaten in der Tabelle} \end{aligned}$$

Dann ist $(\texttt{Max}, \texttt{Mustermann}, \texttt{07.07.1977}) \in A_1 \times A_2 \times A_3$ und die Menge aller Zeilen der Tabelle ist eine Relation $R \subseteq A_1 \times A_2 \times A_3$.

Eine Relation $R \subseteq A_1 \times A_2$ heißt *binäre Relation*.

Binäre Relationen R werde auch in Infix-Notation geschrieben:

$$xRy \iff_{\text{def}} (x, y) \in R$$

Der Ausdruck „xRy“ steht dabei für die Leseweise: „x steht in Relation R zu y.“

Beispiele: Wir betrachten binäre Relationen über der Menge $A = \mathbb{N}$.

- $R_1 =_{\text{def}} \mathbb{N} \times \mathbb{N}$
- $R_2 =_{\text{def}} \{(0,0), (2,3), (5,1), (5,3)\}$
- $R_3 =_{\text{def}} \{\ (n_1, n_2) \mid n_1 \leq n_2\ \} = \{(0,0), (0,1), (1,1), (0,2), \ldots\}$
- $R_4 =_{\text{def}} \{\ (n_1, n_2) \mid n_1 \text{ teilt } n_2\ \} = \{(1,2), (2,4), (2,6), (7,0), \ldots\}$
- $R_5 =_{\text{def}} \{\ (n_1, n_2) \mid 2 \text{ teilt } |n_1 - n_2|\ \} = \{(0,2), (2,2), (1,1), (3,1), \ldots\}$
- $R_6 =_{\text{def}} \{\ (n_1, n_2) \mid 2n_1 = n_2\ \} = \{(0,0), (1,2), (2,4), (3,6), \ldots\}$

Die Relationen R_3 und R_4 sind *Ordnungsrelationen*. Relation R_5 ist eine *Äquivalenzrelation*. Relation R_6 ist eine *Funktion*.

In den folgenden Abschnitten wenden wir uns den im Beispiel erwähnten Relationentypen systematisch zu.

3.2 Ordnungsrelationen

Ordnungsrelationen extrahieren den mathematischen Gehalt von natürlichen Ordnungen, wie sie beispielsweise beim Sortieren benötigt werden. Dafür werden die folgenden vier Begriffe definiert.

Definition 3.1 *Eine binäre Relation $R \subseteq A \times A$ heißt*

1.	reflexiv	$\iff_{\text{def}}$	$(\forall a \in A)[(a, a) \in R]$
2.	transitiv	$\iff_{\text{def}}$	$(\forall a, b, c \in A)[((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R]$
3.	antisymmetrisch	$\iff_{\text{def}}$	$(\forall a, b \in A)[((a, b) \in R \wedge (b, a) \in R) \rightarrow a = b]$
4.	total	$\iff_{\text{def}}$	$(\forall a, b \in A)[a \neq b \rightarrow ((a, b) \in R \vee (b, a) \in R)]$

Die Eigenschaft der Antisymmetrie wird anschaulicher, wenn für alle $a, b \in A$ die Kontraposition

$$a \neq b \rightarrow ((a, b) \notin R \vee (b, a) \notin R)$$

betrachtet wird. Mit anderen Worten darf für verschiedene Elemente a und b höchstens eines der Paare (a, b) oder (b, a) zu R gehören. Zu beachten ist weiterhin, dass die Eigenschaft der Antisymmetrie nicht Negation der Symmetrie ist, wie sie im Kapitel über Äquivalenzrelationen eingeführt wird.

Beispiele: Wir überprüfen die Eigenschaften für die folgenden endlichen Relationen über der Menge $A = \{0, 1, 2\}$:

Relation	reflexiv	transitiv	antisymmetrisch	total
$\{ (0,0), (0,1), (0,2), (1,1), (1,2), (2,2) \}$	X	X	X	X
$\{ (0,0), (0,1), (2,0), (1,1), (1,2), (2,2) \}$	X		X	X
$\{ (0,0), (0,1), (2,0), (0,2), (1,1), (1,2), (2,2) \}$	X			X
$\{ (0,0), (0,1), (2,0), (0,2), (1,1), (2,2) \}$	X			
$\{ (0,1), (2,0), (0,2), (1,1), (2,2) \}$				
$\{ (0,1), (1,2), (0,2) \}$		X	X	X
$\{ (0,0), (0,1), (1,0), (1,1), (2,2) \}$	X	X		
$\{ (0,0), (0,1), (0,2), (1,1), (2,2) \}$	X	X	X	
$\{ (0,1), (1,2), (2,1), (2,0) \}$				X

Durch die Analyse der obigen Beispiele bekommt man ein technisches Gefühl für die Definitionen. Im Folgenden wollen wir auch die Intuitivität von Definition 3.1 durch weitere Beispiele verdeutlichen.

Beispiele: Die folgenden Beispiele repräsentieren im Allgemeinen unendliche Relationen.

- Wir betrachten die Relation $R_1 =_{\text{def}} \{ (m, n) \mid m \leq n \} \subseteq \mathbb{N}^2$. Zur Erinnerung halten wir fest: $m \leq n \Leftrightarrow (\exists c \in \mathbb{N})[n = m + c]$. Dann besitzt R alle Eigenschaften von Definition 3.1:
  - R_1 ist reflexiv, denn für alle $n \in \mathbb{N}$ gilt $n = n + 0$ bzw. $n \leq n$.

  - R_1 ist transitiv, denn gilt $k \leq m$ und $m \leq n$, so gibt es $c_1, c_2 \in \mathbb{N}$ mit $m = k + c_1$ sowie $n = m + c_2$ und es gilt $n = k + (c_2 + c_1)$ bzw. $k \leq n$.
  - R_1 ist antisymmetrisch, denn gilt $m \leq n$ und $n \leq m$, so gibt es $c_1, c_2 \in \mathbb{N}$ mit $n = m + c_1$ sowie $m = n + c_2$ und mit $n = n + c_1 + c_2$ folgt $c_1 = c_2 = 0$ und mithin $n = m$.
  - R_1 ist total, denn $n - m \in \mathbb{N}$ oder $m - n \in \mathbb{N}$.

- Wir betrachten die Relation $R_2 =_{\text{def}} \{ (m, n) \mid m \text{ teilt } n \}$. Auch hier halten wir zur Erinnerung fest: m teilt $n \Leftrightarrow (\exists c \in \mathbb{N})[n = c \cdot m]$. Für R_2 gelten folgende Aussagen:
  - R_2 ist reflexiv, denn für alle $n \in \mathbb{N}$ gilt $n = 1 \cdot n$ bzw. n teilt n.
  - R_2 ist transitiv, denn teilt k die Zahl m und teilt m die Zahl n, so gibt es $c_1, c_2 \in \mathbb{N}$ mit $m = c_1 \cdot k$ sowie $n = c_2 \cdot m$ und es gilt $n = (c_2 \cdot c_1) \cdot k$ bzw. k teilt n.
  - R_2 ist antisymmetrisch, denn teilt m die Zahl n und teilt n die Zahl m, so gibt es $c_1, c_2 \in \mathbb{N}$ mit $n = c_1 \cdot m$ sowie $m = c_2 \cdot n$ und mit $n = c_1 \cdot c_2 \cdot n$ folgt $c_1 = c_2 = 1$ und mithin $m = n$.
  - R_2 ist nicht total, denn weder teilt 2 die Zahl 3 noch teilt 3 die Zahl 2.

- Wir betrachten die Relation $R_3 =_{\text{def}} \{ (A, B) \mid A \subseteq B \} \subseteq \mathcal{P}(X)^2$ für eine Grundmenge X. Für R gelten folgende Eigenschaften:
  - R_3 ist reflexiv, denn es gilt $A \subseteq A$ für alle $A \subseteq X$.
  - R_3 ist transitiv, denn gilt $A \subseteq B$, d.h. $(\forall a \in A)[a \in B]$, und gilt $B \subseteq C$, d.h. $(\forall a \in B)[a \in C]$, so gilt nach dem Kettenschluss auch $(\forall a \in A)[a \in C]$, d.h. $A \subseteq C$.
  - R_3 ist antisymmetrisch, denn mit $A \subseteq B$ und $B \subseteq A$ gilt $A = B$.
  - R_3 ist nicht total, falls $\|X\| \geq 2$: Es seien $a, b \in X$ mit $a \neq b$, dann gilt $\{a\} \cap \{b\} = \emptyset$.

Definition 3.2 *Es sei $R \subseteq A \times A$ eine binäre Relation über A.*

1. *R heißt* Halbordnung *(oder* partielle Ordnung*), falls R reflexiv, transitiv und antisymmetrisch ist.*

2. *R heißt* Ordnung *(oder* totale Ordnung*), falls R eine Halbordnung und zusätzlich total ist.*

3. *Ist R eine Halbordnung, so heißt das Paar (A, R)* halbgeordnete *(oder* partiell geordnete*)* Menge*.*

4. *Ist R eine Ordnung, so heißt das Paar (A, R)* geordnete *(oder* total geordnete*)* Menge*.*

Beispiele (Fortsetzung): Für die drei Relationen aus obigem Beispiel gilt:

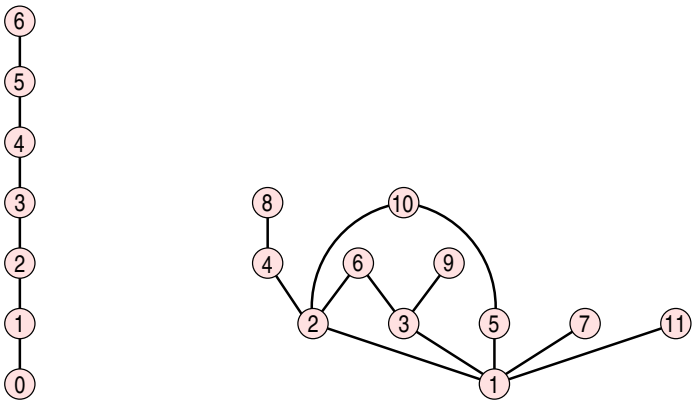
- R_1 ist eine Ordnung; wir schreiben die geordnete Menge als $(\mathbb{N}, \leq)$.
- R_2 ist eine Halbordnung; wir schreiben die halbgeordnete Menge als $(\mathbb{N}, |)$.
- R_3 ist eine Halbordnung für jede Grundmenge X; wir schreiben die halbgeordnete Menge als $(\mathcal{P}(X), \subseteq)$.

Endliche Halbordnungen lassen sich durch HASSE-Diagramme graphisch darstellen. Diese Diagramme sind wie folgt für eine halbgeordnete Menge (A, R) definiert:

- Elemente der Grundmenge A werden durch Punkte (Knoten) in der Ebene dargestellt
- Ist $(x, y) \in R$ für $x \neq y$, so wird der Knoten y oberhalb von Knoten x gezeichnet
- Genau dann, wenn $(x, y) \in R$ für $x \neq y$ gilt und es kein $z \notin \{x, y\}$ mit $(x, z) \in R$ und $(z, y) \in R$ gibt, werden x und y durch eine Linie (Kante) verbunden

Bei dieser Darstellungsform werden gerade alle Paare einer Halbordnung nicht mit dargestellt, deren Zugehörigkeit zur Relation sich wegen der Transitivität sowieso aus den anderen Paaren ergeben würde. Eine derart vollständig reduzierte Relation heißt auch *transitive Reduktion* einer Halbordnung.

Beispiele: Die folgende Abbildung zeigt HASSE-Diagramme für die endlichen, halbgeordneten Mengen $\left(\{0, 1, \ldots, 6\}^2, \leq\right)$ und $\left(\{1, \ldots, 11\}^2, |\right)$:



$\left(\{0, 1, \ldots, 6\}^2, \leq\right)$ $\left(\{1, \ldots, 11\}^2, |\right)$

Im Folgenden verwenden wir $x \leq_R y$ für $(x, y) \in R$, falls R eine Halbordnung ist.

Definition 3.3 *Es seien $R \subseteq A \times A$ eine Halbordnung und $K \subseteq A$.*

1. *Ein Element $a \in K$ heißt* Minimum *(bzw.* Maximum*) von K, falls $a \leq_R b$ (bzw. $a \geq_R b$) für alle $b \in K$ gilt.*
2. *Ein Element $a \in A$ heißt* untere Schranke *(bzw.* obere Schranke*) von K, falls $a \leq_R b$ (bzw. $a \geq_R b$) für alle $b \in K$ gilt.*
3. *Ein Element $a \in A$ heißt* Infimum *(bzw.* Supremum*) von K, falls a eine untere Schranke (bzw. obere Schranke) von K und $a \geq_R b$ (bzw. $a \leq_R b$) für alle unteren Schranken (bzw. oberen Schranken) von K gilt.*

Der Unterschied zwischen einer unteren Schranke von K und einem Minimum von K liegt darin, dass die untere Schranke nicht zur Mengen K gehören muss, was für das Minimum verlangt ist. Gleiches gilt natürlich auch für obere Schranken von K und einem Maximum von K. Darüber hinaus sind Minima, Maxima, Infima und Suprema stets eindeutig, falls sie überhaupt existieren.

Proposition 3.4 *Es seien $R \subseteq A \times A$ eine Halbordnung und $K \subseteq A$. Existiert das Minimum (Maximum, Infimum, Supremum) von K, so ist es eindeutig.*

Beweis: (*nur für das Minimum*) Es seien $a, a' \in K$ Minima von K. Dann gilt $a \leq_R a'$, da a ein Minimum von K ist, und es gilt $a' \leq_R a$, da a' ein Minimum von K ist. Wegen der Antisymmetrie von $\leq_R$ gilt $a = a'$. Damit ist die Proposition bewiesen. ■

Die Eindeutigkeit dieser Elemente ermöglicht uns spezielle Notationen einzuführen:

$\min(K)$	steht für das Minimum von K
$\max(K)$	steht für das Maximum von K
$\inf(K)$	steht für das Infimum von K
$\sup(K)$	steht für das Supremum von K

Anschaulich ist das Infimum die größte untere Schranke und das Supremum die kleinste obere Schranke. Im Allgemeinen müssen Minimum, Maximum, Infimum und Supremum nicht existieren.

Beispiele: Folgende Beispiele verdeutlichen die Begriffsbildungen.

- $\min(\emptyset)$ und $\max(\emptyset)$ existieren für keine Halbordnung.
- Es sei $A =_{\text{def}} \mathbb{Q}$ und $R =_{\text{def}} \{ (m, n) \mid m \leq n \}$. Für die Mengen

$$\begin{aligned} K_+ &=_{\text{def}} \{ x \mid 0 < x \} \subseteq A \\ K_- &=_{\text{def}} \{ x \mid x < 0 \} \subseteq A \end{aligned}$$

gelten die folgenden Aussagen:

- $\min(K_+)$ und $\min(K_-)$ existieren nicht
- $\max(K_+)$ und $\max(K_-)$ existieren nicht
- Die Menge der unteren Schranken von K_+ ist $K_- \cup \{0\}$
- Die Menge der unteren Schranken von K_- ist $\emptyset$
- Die Menge der oberen Schranken von K_+ ist $\emptyset$
- Die Menge der oberen Schranken von K_- ist $K_+ \cup \{0\}$
- $\inf(K_+) = \max(K_- \cup \{0\}) = 0$
- $\inf(K_-)$ existiert nicht
- $\sup(K_+)$ existiert nicht
- $\sup(K_-) = \min(K_+ \cup \{0\}) = 0$

- Wir setzen das vorangehende Beispiel fort. Bei veränderter Grundmenge $A =_{\text{def}} \mathbb{Q} \setminus \{0\}$ sowie unverändertem R, K_+ und K_- gelten die folgenden Aussagen:
  - Die Menge der unteren Schranken von K_+ ist K_-
  - $\inf(K_+)$ existiert nicht, da K_- kein Maximum besitzt
- Es seien $A =_{\text{def}} \{0, 1, \ldots, 10\}$ und $R =_{\text{def}} \{ (m, n) \mid m \leq n \} \subseteq A \times A$. Dann gelten folgende Aussagen:
  - $\inf(\emptyset) = 10$
  - $\sup(\emptyset) = 0$

Definition 3.5 *Es seien $R \subseteq A \times A$ eine Halbordnung und $K \subseteq A$. Ein Element $a \in K$ heißt* minimal *(bzw.* maximal*) in K, falls für alle $b \in K$ gilt: Ist $b \leq_R a$ (bzw. $b \geq_R a$), so ist $a = b$.*

Beispiel: Es seien $A =_{\text{def}} \mathbb{N}$ und $R =_{\text{def}} \{ (m, n) \mid m \text{ teilt } n \} \subseteq A \times A$. Für

$$K_1 =_{\text{def}} \mathbb{N} \quad \text{und} \quad K_2 =_{\text{def}} \mathbb{N} \setminus \{1\}$$

gelten die Aussagen:

- Die Menge der minimalen Elemente von K_1 ist $\{1\}$
- Die Menge der minimalen Elemente von K_2 ist die Menge der Primzahlen

Proposition 3.6 *Es seien $R \subseteq A \times A$ eine Ordnung und $K \subseteq A$. Ist $a \in K$ minimal (bzw. maximal) in K, so ist a ein Minimum (bzw. Maximum) von K.*

Beweis: (*nur für die Minimalität*) Es sei $a \in K$ ein minimales Element. Für $b \in K$ gilt $a \leq_R b$ oder $b \leq_R a$ wegen der Totalität von R. Gilt $b \leq_R a$, so folgt $a = b$ (bzw. $a \leq_R b$) wegen der Minimalität von a. Somit gilt in jedem Fall $a \leq_R b$ für alle $b \in K$. Somit ist a das Minimum von K. Damit ist die Proposition bewiesen. ∎

3.3 Äquivalenzrelationen

Definition 3.7 *Eine binäre Relation $R \subseteq A \times A$ heißt*

1. symmetrisch $\quad \Longleftrightarrow_{\text{def}} \quad (\forall a, b \in A)[(a,b) \in R \rightarrow (b,a) \in R]$
2. Äquivalenzrelation $\quad \Longleftrightarrow_{\text{def}} \quad$ *R ist reflexiv, transitiv und symmetrisch*

Bei einer Äquivalenzrelation R verwenden wir statt $(a,b) \in R$ die Infix-Schreibweise $a \sim_R b$ (oder $a \approx_R b$, $a \equiv_R b$).

Beispiele: Wir überprüfen die Eigenschaften für die folgenden endlichen Relationen über der Menge $A = \{0,1,2\}$:

Relation	reflexiv	transitiv	symmetrisch	Äquivalenzrelation
$\{\ (0,1),(1,0),(0,2),(2,0)\ \}$			X	
$\{\ (0,0),(0,1),(1,0),(1,1),(0,2),(2,0),(2,2)\ \}$	X		X	
$\{\ (0,0),(0,1),(1,0),(1,1),(2,2)\ \}$	X	X	X	X
$\{\ (0,0),(0,1),(1,0),(1,1)\ \}$		X	X	
$\{\ (0,0),(0,1),(1,1),(2,2)\ \}$	X	X		

Wir wollen die Intuitivität des Äquivalenzrelationenbegriff an komplexeren Relationen verdeutlichen.

Beispiele: Folgende Beispiele sind typisch für die Bildung von Äquivalenzrelationen.

- Es seien $A =_{\text{def}}$ Menge aller (logischen) Aussagen und

$$R =_{\text{def}} \{\ (H, H') \mid H \leftrightarrow H' \text{ ist eine Tautologie } \} \subseteq A \times A.$$

Dann ist R eine Äquivalenzrelation, denn es gelten folgende Aussagen (z.B. mittels Überprüfung durch Wertetabellen):

- R ist reflexiv: $H \leftrightarrow H$ ist eine Tautologie für alle Aussagen H
- R ist transitiv: Sind $H \leftrightarrow H'$ und $H' \leftrightarrow H''$ Tautologien, so ist auch $H \leftrightarrow H''$ eine Tautologie (wegen doppelter Anwendung der Kettenschlussregel)
- R ist symmetrisch: Ist $H \leftrightarrow H'$ eine Tautologie, so ist auch $H' \leftrightarrow H$ eine Tautologie.

- Es sei $f : A \to B$ eine beliebige Funktion (mit Argumenten aus A und Funktionswerten in B). Dann ist die Relation

$$R_f =_{\text{def}} \{\ (x, y) \mid f(x) = f(y)\ \} \subseteq A \times A$$

ganz offentsichtlich eine Äquivalenzrelation. Zum Beispiel ergeben sich für spezielle Funktionen folgende Äquivalenzrelationen:

- Auf der Menge $A =_{\text{def}} \mathbb{Z}$ sei die Funktion $f_n(x) = \text{mod}(x, n)$ mit Funktionswerten in der Menge $\{0, 1, \ldots, n-1\}$ definiert. Dann schreiben wir auch $x \equiv y \bmod n$ für $(x, y) \in R_{f_n}$ und sagen „x ist kongruent y modulo n“.
- Auf der Menge A aller Wörter eines Wörterbuches (wobei alle Wörter nur aus Kleinbuchstaben bestehen und keine Umlaute enthalten) sei f als Funktion definiert, die jedes Wort auf den ersten Buchstaben abbildet.

Definition 3.8 *Es seien $R \subseteq A \times A$ eine Äquivalenzrelation und $x \in A$ ein beliebiges Element. Dann heißt die Menge*

$$[x]_R =_{\text{def}} \{\ y \mid (x, y) \in R\ \} \subseteq A$$

Äquivalenzklasse *von x. Wir nennen x* Repräsentant *der Äquivalenzklasse.*

Beispiel: Wir betrachten die Kongruenz „ $\equiv \bmod 8$ “ auf den ganzen Zahlen. Dann gilt:

$$\begin{aligned} [13]_{\equiv} &= \{\ y \mid y \equiv 13 \bmod 8\ \} \\ &= \{\ y \mid \text{mod}(y - 13, 8) = 0\ \} \\ &= \{\ldots, -11, -3, 5, 13, 21 \ldots\ \} \\ &= [5]_{\equiv} \end{aligned}$$

Proposition 3.9 *Es seien $R \subseteq A \times A$ eine Äquivalenzrelation und $x, y \in A$. Dann gilt:*

1. *Ist $(x, y) \in R$, so gilt $[x]_R = [y]_R$.*
2. *Ist $(x, y) \notin R$, so sind $[x]_R$ und $[y]_R$ disjunkt.*

Beweis: Wir beweisen die Aussagen einzeln.

1. Es gelte $(x, y) \in R$, d.h. $y \in [x]_R$. Wegen der Transitivität von R gilt $(x, z) \in R$ für alle $z \in [y]_R$ (d.h. $(y, z) \in R$). Somit gilt $[y]_R \subseteq [x]_R$. Wegen der Symmetrie von R gilt $(y, x) \in R$. Somit können wir analog auch $[x]_R \subseteq [y]_R$ zeigen. Mithin gilt $[x]_R = [y]_R$.

2. Wir zeigen die Kontraposition der Aussage. Dazu gelte $[x]_R \cap [y]_R \neq \emptyset$. Dann gibt es ein $z \in A$ mit $z \in [x]_R$ und $z \in [y]_R$ bzw. $(x, z) \in R$ und $(y, z) \in R$. Wegen der Symmetrie von R gilt $(z, y) \in R$. Wegen der Transitivität gilt somit $(x, y) \in R$.

Damit ist die Proposition bewiesen. ■

Definition 3.10 *Es sei $R \subseteq A \times A$ eine Äquivalenzrelation. Eine Menge $K \subseteq A$ heißt* Repräsentantensystem *von R, falls folgende Bedingungen erfüllt sind:*

1. *Für alle $k_1, k_2 \in K$ mit $k_1 \neq k_2$ gilt $(k_1, k_2) \notin R$.*

2. $A = \bigcup_{k \in K} [k]_R$.

Beispiel: Wir betrachten die Kongruenz „ $\equiv \mod 8$ “ auf den ganzen Zahlen.

- $\{0, 1, 2, 3, 4, 5, 6, 7\}$ ist ein Repräsentantensystem
- $\{8, 1, 2, 19, -4, 13, 6, 7\}$ ist ebenfalls ein Repräsentantensystem

Die zu einem Repräsentantensystem gehörenden Äquivalenzklassen bilden eine Partition der Grundmenge. Zur Erinnerung (siehe Übungsblatt 8 für den endlichen Spezialfall): Eine Mengenfamilie $\mathcal{F} \subseteq \mathcal{P}(A)$ heißt *Partition* von A, falls $\mathcal{F}$ nur paarweise disjunkte Mengen enthält sowie die Vereinigung über alle zu $\mathcal{F}$ gehörenden Mengen gerade A ergibt.

Korollar 3.11 *Es seien $R \subseteq A \times A$ eine Äquivalenzrelation und $K \subseteq A$ ein Repräsentantensystem von R. Dann bilden die Äquivalenzklassen (der Elemente) von K eine Partition von A.*

Beweis: Wegen $(k_1, k_2) \notin R$ für $k_1, k_2 \in K$ mit $k_1 \neq k_2$ (die erste Eigenschaft eines Repäsentantensystems) folgt aus Proposition 3.9:

$$[k_1]_R \cap [k_2]_R = \emptyset$$

Aus der zweiten Eigenschaft eines Repräsentantensystem folgt für K weiterhin

$$\bigcup_{k \in K} [k]_R = A.$$

Somit ist die Mengenfamilie $\{ [k]_R \mid k \in K \}$ eine Partition von A. Damit ist das Korollar bewiesen. ■

Proposition 3.12 *Es sei $\mathcal{F} \subseteq \mathcal{P}(A)$ eine Partition von A. Dann ist die Relation $R \subseteq A \times A$ mit*

$$(x, y) \in R \quad \Longleftrightarrow_{\text{def}} \quad (\exists X \in \mathcal{F})[x \in X \wedge y \in X]$$

eine Äquivalenzrelation.

Beweis: Wir überprüfen die Eigenschaften von Äquivalenzrelationen:

- R ist reflexiv: Für jedes $x \in A$ gibt es ein $X \in \mathcal{F}$ mit $x \in X$, da $\mathcal{F}$ eine Partition ist. Somit gilt $(x, x) \in R$.
- R ist transitiv: Es seien $(x, y) \in R$ und $(y, z) \in R$. Dann gibt es $X_1, X_2 \in \mathcal{F}$ mit $x, y \in X_1$ sowie $y, z \in X_2$. Mithin gilt $y \in X_1 \cap X_2$. Also sind X_1 und X_2 nicht disjunkt. Da $\mathcal{F}$ eine Partition ist, gilt folglich $X_1 = X_2$. Somit gilt $x, z \in X_1$. Es folgt $(x, z) \in R$.
- R ist symmetrisch: Ist $(x, y) \in R$, so gilt $x, y \in X$ für ein geeignetes $X \in \mathcal{F}$. Also gilt auch $(y, x) \in R$.

Damit ist die Proposition bewiesen ■

3.4 Funktionen und Abbildungen

In diesem Abschnitt führen wir Begriffe ein, die Funktionen, oder synomym Abbildungen, als spezielle Relationen zwischen Mengen von Argumenten und Mengen von Werten charakterisieren.

Definition 3.13 *Eine binäre Relation $R \subseteq A \times B$ heißt*

1. linkstotal $\Longleftrightarrow_{\text{def}}$ $(\forall x \in A)(\exists y \in B)[(x, y) \in R]$
2. rechtseindeutig $\Longleftrightarrow_{\text{def}}$ $(\forall x \in A)(\forall y, z \in B)[((x, y) \in R \wedge (x, z) \in R) \rightarrow y = z]$
3. rechtstotal $\Longleftrightarrow_{\text{def}}$ $(\forall y \in B)(\exists x \in A)[(x, y) \in R]$
4. linkseindeutig $\Longleftrightarrow_{\text{def}}$ $(\forall x, y \in A)(\forall z \in B)[((x, z) \in R \wedge (y, z) \in R) \rightarrow x = y]$

Beispiele: Wir überprüfen die Eigenschaften für die folgenden endlichen Relationen über den Mengen $A = \{1, 2, 3\}$ und $B = \{1, 2, 3, 4\}$:

Relation	linkstotal	rechtseindeutig	rechtstotal	linkseindeutig
$\{ (1,1), (1,2), (2,2) \}$ 				
$\{ (1,1), (1,2), (2,2), (3,3) \}$ 	X			
$\{ (1,1), (2,1) \}$ 		X		
$\{ (1,1), (1,2), (1,3), (1,4), (2,4) \}$ 			X	
$\{ (1,1), (1,2) \}$ 				X
$\{ (1,1), (1,2), (2,2), (3,3), (3,4) \}$ 	X		X	
$\{ (1,1), (2,2), (3,2) \}$ 	X	X		
$\{ (1,1), (1,2), (1,3), (1,4) \}$ 			X	X
$\{ (1,1), (2,2), (3,3) \}$ 	X	X		X

Definition 3.14 *Es sei $R \subseteq A \times B$ eine binäre Relation.*

1. *R heißt (totale)* Funktion*, falls R linkstotal und rechtseindeutig ist.*
2. *R heißt* partielle Funktion*, falls R rechtseindeutig ist.*

Beispiele: Wir diskutieren an folgenden Relationen die Funktionenbegriffe.

- Die Relation $R =_{\text{def}} \{ (1,1), (2,2), (3,2) \} \subseteq \{1, 2, 3\} \times \{1, 2, 3, 4\}$ ist eine Funktion.

- Die Relation $R =_{\text{def}} \{ (1,1),(2,1) \} \subseteq \{1,2,3\} \times \{1,2,3,4\}$ ist eine partielle Funktion. Fassen wir R jedoch als Teilmenge von $\{1,2\} \times \{1,2,3,4\}$ auf, so ist F eine Funktion.
- Die Relation $R =_{\text{def}} \{ (x,y) \mid y = |x| \} \subseteq \mathbb{Z} \times \mathbb{N}$ ist eine Funktion.
- Die Relation $R =_{\text{def}} \{ (y,x) \mid y = |x| \} \subseteq \mathbb{N} \times \mathbb{Z}$ ist keine Funktion.
- Die folgende Methode einer in Java implementierten Klasse (siehe auch Übungsblatt 9)

```
int gcd(int x, int y) {
    if (y==0) return x;
    if (y>x) return gcd(y,x);
    return gcd(y,x%y);
}
```

  ist eine partielle Funktion als Teilmenge von $\texttt{int}^2 \times \texttt{int}$, wobei wir `gcd` als Relation $\{ (x,y,z) \mid z = \texttt{gcd}(x,y) \}$ auffassen.
  In Java gilt $\text{mod}(-1,-2) = -1$, d.h. (-1) % (-2) wird zu -1 ausgewertet. Damit wird beim Methodenaufruf $\texttt{gcd}(-1,-2)$ erst rekursiv $\texttt{gcd}(-2,-1)$ und dann wieder $\texttt{gcd}(-1,-2)$ aufgerufen. Somit terminiert $\texttt{gcd}(-1,-2)$ nicht, und es gibt folglich kein $z \in \texttt{int}$ mit $(-1,-2,z) \in \texttt{gcd}$. Die Methode ist also nicht linkstotal. Die Rechtseindeutigkeit ist gegeben (wenn der verwendete Java-Compiler und die verwendete *Java Virtual Machine* korrekt sind).

Für Funktionen werden üblicherweise eigene Schreibweisen verwendet (wie im letzten der obigen Beispiele):

- Funktionen werden häufig klein geschrieben: $f \subseteq A \times B$.
- Statt $f \subseteq A \times B$ schreiben wir auch $f : A \to B$; statt $(a,b) \in f$ schreiben wir auch $f(a) = b$.
- Kompakt notieren wir eine Funktion als $f : A \to B : a \mapsto f(a)$; für den dritten Fall in den obigen Beispielen schreiben wir also z.B. $f : \mathbb{Z} \to \mathbb{N} : x \mapsto |x|$.

Funktionen werden weiterhin danach klassifiziert, welche Eigenschaften sie zusätzlich zur Linkstotalität und Rechtseindeutigkeit erfüllen.

Definition 3.15 *Eine Funktion $f : A \to B$ heißt*

1. surjektiv $\iff_{\text{def}}$ *f ist rechtstotal*
2. injektiv $\iff_{\text{def}}$ *f ist linkseindeutig*
3. bijektiv $\iff_{\text{def}}$ *f ist rechtstotal und linkseindeutig*

Beispiele: Folgende Funktionen verdeutlichen die Begriffsbildung.

- Die Funktion $f : \mathbb{Z} \to \mathbb{N} : x \mapsto |x|$ ist surjektiv, aber nicht injektiv.
- Die Funktion $f : \mathbb{N} \to \mathbb{Z} : x \mapsto x^3$ ist injektiv, aber nicht surjektiv.
- Die Funktion $f : \mathbb{Z} \to \mathbb{Z} : x \mapsto -x$ ist bijektiv.

Wichtige Begriffe zur Beschreibung der Eigenschaften surjektiver, injektiver und bijektiver Funktionen sind die Bild- und Urbildmengen.

Definition 3.16 *Es seien $f : A \to B$ eine Funktion, $A_0 \subseteq A$ und $B_0 \subseteq B$.*

1. *Die Menge $f(A_0) \subseteq B$ ist definiert als*

$$f(A_0) =_{\text{def}} \{\ b \mid (\exists a \in A_0)[f(a) = b]\ \} \qquad _{\text{def}} = \{\ f(a) \mid a \in A_0\ \}$$

und heißt Bild(menge) *von A_0 unter f. Die Elemente von $f(A_0)$ heißen* Bilder *von A_0 unter f.*

2. *Die Menge $f^{-1}(B_0) \subseteq A$ ist definiert als*

$$f^{-1}(B_0) =_{\text{def}} \{\ a \mid (\exists b \in B_0)[f(a) = b]\ \} \quad _{\text{def}} = \{\ a \mid f(a) \in B_0\ \}$$

und heißt Urbild(menge) *von B_0 unter f. Die Elemente von $f^{-1}(B_0)$ heißen* Urbilder *von B_0 unter f.*

Beispiele: Wir verdeutlichen Bilder und Urbilder exemplarisch.

- Es sei die Funktion $f =_{\text{def}} \{\ (1,1),(2,2),(3,2)\ \} \subseteq \{1,2,3\} \times \{1,2,3,4\}$ gegeben. Unter anderem können folgende Bildmengen gebildet werden:

$$\begin{aligned} f(\{1\}) &= \{1\} \\ f(\{1,2\}) &= \{1,2\} \\ f(\{1,2,3\}) &= \{1,2\} \end{aligned}$$

  Beispiele für Urbildmengen sind unter anderem:

$$\begin{aligned} f^{-1}(\{1\}) &= \{1\} \\ f^{-1}(\{1,2\}) &= \{1,2,3\} \\ f^{-1}(\{3\}) &= \emptyset \end{aligned}$$

- Es sei die Funktion $f : \mathbb{Z} \to \mathbb{N} : x \mapsto |x|$ gegeben. Die Bildmenge das ganzzahligen Intervalls $[-1,1]$ unter f ist:

$$f([-1,1]) = f(\{-1,0,1\}) = \{0,1\}$$

Die Urbildmengen zu $\{2\}$ und $[2,4]$ unter f sind wie folgt:

$$\begin{aligned} f^{-1}(\{2\}) &= \{-2,2\} \\ f^{-1}([2,4]) &= \{-4,-,3,-2,2,3,4\} \end{aligned}$$

Proposition 3.17 *Es seien A und B endliche Mengen und $f : A \to B$ eine Funktion. Dann gilt:*

$$\|A\| = \sum_{b \in B} \left\| f^{-1}(\{b\}) \right\|$$

Beweis: Da f eine Funktion ist, bildet die Mengenfamilie $\{\ f^{-1}(\{b\}) \mid b \in B\ \}$ eine Partition von A. Damit folgt

$$\|A\| = \sum_{b \in B} \|f^{-1}(\{b\})\|$$

und die Proposition ist bewiesen. ■

Das folgende Lemma ergibt sich unmittelbar aus den Definition der Funktioneneigenschaften. Der Beweis bleibt dem Leser zur Übung überlassen.

Lemma 3.18 *Es sei $f : A \to B$ eine Funktion. Dann gilt:*

1. *f ist surjektiv* $\iff (\forall b \in B)\left[\ \left\|f^{-1}(\{b\})\right\| \geq 1\ \right]$
2. *f ist injektiv* $\iff (\forall b \in B)\left[\ \left\|f^{-1}(\{b\})\right\| \leq 1\ \right]$
3. *f ist bijektiv* $\iff (\forall b \in B)\left[\ \left\|f^{-1}(\{b\})\right\| = 1\ \right]$

Während das vorangegangene Lemma eine Charaktiersierung der Eigenschaften für eine konkrete Funktion angibt, stellt Theorem 3.19 eine Beziehung zwischen Mengen mit Hilfe von Funktioneneigenschaften her. Das durch das Theorem beschriebene Abzählprinzip ist eine fundamentale Technik beim Lösen kombinatorischer Fragestellungen.

Theorem 3.19 *Es seien A und B nicht-leere, endliche Mengen. Dann gilt:*

1. *Es gibt eine surjektive Funktion $f : A \to B$* $\iff \|A\| \geq \|B\|$
2. *Es gibt eine injektive Funktion $f : A \to B$* $\iff \|A\| \leq \|B\|$
3. *Es gibt eine bijektive Funktion $f : A \to B$* $\iff \|A\| = \|B\|$

Beweis: Wir beweisen die Äquivalenzen im Block.

($\Leftarrow$): Es seien $A = \{a_1, \ldots, a_n\}$ und $B = \{b_1, \ldots, b_m\}$ endliche Mengen. Wir definieren eine Funktion $f : A \to B$ wie folgt für $a_i \in A$:

$$f(a_i) =_{\text{def}} \begin{cases} b_i & \text{falls } i \leq m \\ b_1 & \text{falls } i > m \end{cases}$$

Dann gelten folgende Aussage in Abhängigkeit von A und B:

1. Ist $\|A\| \geq \|B\|$, d.h. $n \geq m$, so ist f surjektiv
2. Ist $\|A\| \leq \|B\|$, d.h. $n \leq m$, so ist f injektiv
3. Ist $\|A\| = \|B\|$, d.h. $n = m$, so ist f bijektiv

($\Rightarrow$): Es sei $f : A \to B$ eine Funktion. Dann gelten folgende Aussagen:

1. Ist f surjektiv, so gilt nach Proposition 3.17 und Lemma 3.18.1:
$$\|A\| = \sum_{b \in B} \left\| f^{-1}(\{b\}) \right\| \geq \sum_{b \in B} 1 = \|B\|$$
2. Ist f injektiv, so gilt nach Proposition 3.17 und Lemma 3.18.2:
$$\|A\| = \sum_{b \in B} \left\| f^{-1}(\{b\}) \right\| \leq \sum_{b \in B} 1 = \|B\|$$
3. Ist f bijektiv, so gilt nach Proposition 3.17 und Lemma 3.18.3:
$$\|A\| = \sum_{b \in B} \left\| f^{-1}(\{b\}) \right\| = \sum_{b \in B} 1 = \|B\|$$

Damit ist das Theorem bewiesen ■

Theorem 3.20 *Es seien A und B endliche Mengen mit $\|A\| = \|B\| > 0$. Dann sind folgende Aussagen äquivalent:*

1. *f ist surjektiv*
2. *f ist injektiv*
3. *f ist bijektiv*

Die logische Struktur des Theorems besagt, dass entweder alle Aussagen gelten oder keine.

Beweis: Wir zeigen die paarweise Äquivalenz aller Aussagen über einzelne Implikationen.

- (3) $\Rightarrow$ (1): Ist f bijektiv, so ist f surjektiv (nach Definition).

- (3) $\Rightarrow$ (2): Ist f bijektiv, so ist f injektiv (nach Definition).
- (1) $\Rightarrow$ (3): Es sei f surjektiv, d.h. für alle $b \in B$ gilt $\|f^{-1}(\{b\})\| \geq 1$ (nach Lemma 3.18.1). Dann gilt nach Proposition 3.17 und der Voraussetzung:

$$\|A\| = \sum_{b \in B} \|f^{-1}(\{b\})\| \geq \|B\| = \|A\|$$

  Somit gilt $\|f^{-1}(\{b\})\| = 1$ für alle $b \in B$. Folglich ist f bijektiv (nach Lemma 3.18.3).
- (2) $\Rightarrow$ (3): Es sei f injektiv, d.h. für alle $b \in B$ gilt $\|f^{-1}(\{b\})\| \leq 1$ (nach Lemma 3.18.2). Dann gilt nach Proposition 3.17 und der Voraussetzung:

$$\|A\| = \sum_{b \in B} \|f^{-1}(\{b\})\| \leq \|B\| = \|A\|$$

  Somit gilt $\|f^{-1}(\{b\})\| = 1$ für alle $b \in B$. Folglich ist f bijektiv (nach Lemma 3.18.3).

Damit ist das Theorem bewiesen. ■

Für eine Relation $R \subseteq A \times B$ definieren wir die *Umkehrrelation* $R^{-1} \subseteq B \times A$ wie folgt:

$$R^{-1} =_{\text{def}} \{\ (y, x) \mid (x, y) \in R\ \}$$

Die folgende Proposition ist einfach an Hand der Definitionen einzusehen.

Proposition 3.21 *Es sei R eine binäre Relation. Dann gelten die folgenden Aussagen:*

1. *R ist linkstotal* $\iff$ *R^{-1} ist rechtstotal*
2. *R ist rechtseindeutig* $\iff$ *R^{-1} ist linkseindeutig*
3. *R ist rechtstotal* $\iff$ *R^{-1} ist linkstotal*
4. *R ist linkseindeutig* $\iff$ *R^{-1} ist rechtseindeutig*

Korollar 3.22 *Ist f eine bijektive Funktion, so ist die Umkehrrelation f^{-1} eine bijektive Funktion.*

Definition 3.23 *Eine Funktion f heißt* invertierbar *(umkehrbar), falls die Umkehrrelation f^{-1} eine Funktion ist.*

Korollar 3.24 *Eine Funktion f ist genau dann invertierbar, wenn f bijektiv ist.*

Eine wichtige Operation auf Funktionen ist die *Hintereinanderausführung* (oder auch *Verkettung*, *Superposition* oder *Komposition* in anderen Zusammenhängen): Für Funktionen $f : A \to B$ und $g : B \to C$ definieren wir die Funktion $g \circ f : A \to C$ wie folgt für alle $x \in A$:

$$(g \circ f)(x) =_{\text{def}} g(f(x))$$

Beispiele: Wir beleuchten im Folgenden Aspekte der Hintereinanderausführung exemplarisch.

- Für die beiden Funktionen $f : \mathbb{N} \times \mathbb{N} : x \mapsto x^2$ und $g : \mathbb{N} \times \mathbb{N} : x \mapsto 2^x$ gilt

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) = g(x^2) = 2^{(x^2)} = 2^{x^2}\\ (f \circ g)(x) &= f(g(x)) = f(2^x) = (2^x)^2 = 2^{2x}\end{aligned}$$

  Mithin gilt $g \circ f \neq f \circ g$, denn wir erhalten $(g \circ f)(3) = 2^9 = 512$ und $(f \circ g)(3) = 2^6 = 64$.

- Wodurch unterscheiden sich Klassen- und Instanzenmethoden in Java (ohne Nebeneffekte) mathematisch? Zur Veranschaulichung sei dazu eine Methode `method` einerseits als Klassenmethode

```
public static int method (int x, int y)
```

  und andererseits als Instanzenmethode

```
public int method (int x, int y)
```

  deklariert. Im ersten Fall beschreibt die Methode eine Funktion

$$\texttt{method} : \texttt{int} \times \texttt{int} \to \texttt{int}.$$

  Im zweiten Fall dagegen wird eine Funktion

$$\texttt{method} : S \times \texttt{int} \times \texttt{int} \to \texttt{int}$$

  beschrieben, wobei S für die Menge der verfügbaren Speicheradressen steht. Bei der Instanziierung eines Objektes `obj` aus der entsprechenden Klasse ordnet die *Java Virtual Machine* eine Adresse $s(\texttt{obj}) \in S$ zu, d.h. die Instanzenmethode wird dann zu einer Funktion

$$\texttt{obj.method} : \texttt{int} \times \texttt{int} \to \texttt{int} : (x, y) \mapsto \texttt{method}(s(\texttt{obj}), x, y)$$

  als Hintereinanderausführung der Funktionen s und `method`.

Proposition 3.25 *Es seien $f : A \to B$ und $g : B \to C$ beliebige Funktionen.*

1. *Sind f und g injektiv, so ist $g \circ f$ injektiv.*
2. *Sind f und g surjektiv, so ist $g \circ f$ surjektiv.*
3. *Sind f und g bijektiv, so ist $g \circ f$ bijektiv.*

Beweis: Wir zeigen die Aussagen einzeln.

1. Es seien f und g injektive Funktionen. Wir müssen zeigen, dass $g \circ f$ linkseindeutig ist. Dazu seien $x, y \in A$ beliebig mit $(g \circ f)(x) = (g \circ f)(y) \in C$. Da g injektiv ist, folgt aus $g(f(x)) = g(f(y))$ die Gleichheit $f(x) = f(y)$. Da auch f injektiv ist, folgt aus $f(x) = f(y)$ wiederum die Gleichheit $x = y$. Mithin ist $g \circ f$ linkseindeutig und also injektiv.

2. Es seien f und g surjektive Funktionen. Wir müssen zeigen, dass $g \circ f$ rechtstotal ist. Es sei $x \in C$ beliebig. Da g surjektiv ist, gibt es ein $y \in B$ mit $y \in g^{-1}(\{x\}) \subseteq B$, d.h. $g(y) = x$. Da auch f surjektiv ist, gibt es ein $z \in A$ mit $z \in f^{-1}(\{y\}) \subseteq A$, d.h. $f(z) = y$. Insgesamt erhalten wir also

$$(g \circ f)(z) = g(f(z)) = g(y) = x.$$

   Somit gilt $\|(g \circ f)^{-1}(\{x\})\| \geq 1$ für alle $x \in C$. Mithin ist $g \circ f$ surjektiv (nach Lemma 3.18.1).

3. Direkte Folgerung aus der ersten und der zweiten Aussage dieser Proposition.

Damit ist die Proposition bewiesen. ■

Für eine Menge A heißt die Funktion $\mathrm{id}_A : A \to A : x \mapsto x$ *Identitätsfunktion* von A.

Proposition 3.26 *Es sei $f : A \to B$ eine bijektive Funktion. Dann gilt $f^{-1} \circ f = \mathrm{id}_A$ und $f \circ f^{-1} = \mathrm{id}_B$.*

Beweis: Es genügt $f^{-1} \circ f = \mathrm{id}_A$ zu zeigen (da wir f und f^{-1} vertauschen können). Es gilt $f^{-1} \circ f : A \to A$ wegen $f : A \to B$ und $f^{-1} : B \to A$. Außerdem gilt $f^{-1}(\{f(x)\}) = \{x\}$, da f bijektiv ist. Somit gilt $f^{-1}(f(x)) = x$ für alle $x \in A$, d.h. $f^{-1} \circ f = \mathrm{id}_A$. Damit ist die Proposition bewiesen. ■

Induktion 4

4.1 Vollständige Induktion

Die vollständige Induktion ist ein Beweisprinzip, um eine mit dem Allquantor versehene Aussage über dem Universum der natürlichen Zahlen zu beweisen. Die Korrektheit des Beweisprinzips haben wir im Kapitel 1 bewiesen. Zur Erinnerung zitieren wir das entsprechende Theorem 1.4 noch einmal als folgendes Theorem (aber ohne Beweis).

Theorem 4.1 *Es sei $A(n)$ eine Aussageform mit der freien Variable n über dem Universum der natürlichen Zahlen. Dann ist die Aussage*

$$\Big(A(0) \wedge (\forall n; n > 0)[A(n-1) \to A(n)]\Big) \to (\forall n)[A(n)]$$

allgemeingültig.

Die Anwendung von Theorem 4.1 als Beweisverfahren erfolgt in zwei Schritten:

- *Induktionsanfang* (IA): Zeige $A(0)$.
- *Induktionsschritt* (IS): Zeige $A(n)$ für ein allgemeines $n > 0$ unter der Annahme (*Induktionsvoraussetzung*, IV), dass $A(n-1)$ als wahr angenommen wird. (Dies entspricht dem wichtigen Fall für die Gültigkeit der Implikationen $A(n-1) \to A(n)$.

Wir wollen im Folgenden die vollständige Induktion an Beispielen, die wir als Propositionen beschreiben, demonstrieren.

Proposition 4.A *Für alle $n \in \mathbb{N}$ gilt $(n+1)! \geq 2^n$.*

Bevor wir den Induktionsbeweis angeben, wollen wir die Beziehung zwischen der Aussage der Proposition und Theorem 4.1 beschreiben: Die gegebene Aussageform über dem Universum $\mathbb{N}$ ist

$$A(n) =_{\text{def}} \text{„ } (n+1)! \geq 2^n \text{ “}.$$

Beweisen wollen wir die universelle Aussagen $(\forall n)[A(n)]$. Dafür überprüfen wir im Induktionsanfang die Aussage $A(0)$ und im Induktionsschritt die Implikation $A(n-1) \to A(n)$ für $n > 0$. Die Induktionsvoraussetzung ist dann also $A(n-1) \equiv$ „ $n! \geq 2^{n-1}$ “, die wir tatsächlich stets bilden können, da $n > 0$ gilt.

Beweis: (*Induktion über n*)

- *Induktionsanfang*: Für $n = 0$ gilt $(0+1)! = 1 \geq 1 = 2^0$, d.h. $A(0)$ ist wahr.
- *Induktionsschritt*: Für $n > 0$ gilt

$$\begin{aligned}(n+1)! &= (n+1) \cdot n! && \text{(nach Definition von } n!) \\ &\geq (n+1) \cdot 2^{n-1} && \text{(nach } \textit{Induktionsvoraussetzung}) \\ &\geq 2 \cdot 2^{n-1} && \text{(da } n \geq 1) \\ &= 2^n\end{aligned}$$

  Mithin ist $A(n)$ wahr unter der Annahme, dass $A(n-1)$ wahr ist.

Damit ist die Proposition bewiesen ■

Proposition 4.B *Für alle $n \in \mathbb{N}$ gilt $\log_2(n+1) \leq n$.*

Beweis: (*Induktion über n*)

- *Induktionsanfang*: Für $n = 0$ gilt $\log_2(0+1) = 0 \leq 0$.
- *Induktionsschritt*: Für $n > 0$ gilt

$$\begin{aligned}\log_2(n+1) &\leq \log_2(2n) && \text{(da } n \geq 1) \\ &\geq 1 + \log_2 n && \text{(nach } \textit{Induktionsvoraussetzung}) \\ &\geq 1 + (n-1) && \text{(da } n \geq 1) \\ &= n\end{aligned}$$

Damit ist die Proposition bewiesen ■

4.2 Erste verallgemeinerte Form der vollständigen Induktion

Mitunter genügt es nicht im Induktionsanfang nur den Fall $n = 0$ zu betrachten, sondern es müssen mehrere, aber nur endlich viele Einzelfälle überprüft werden. Die Korrektheit des zugehörigen verallgemeinerten Beweisprinzips halten wir in folgendem Theorem (ohne Beweis) fest.

Theorem 4.2 *Es seien $A(n)$ eine Aussageform mit der freien Variable n über dem Universum der natürlichen Zahlen und $n_0 \in \mathbb{N}$. Dann ist die Aussage*

$$\Big((\forall n; n \leq n_0)[A(n)] \ \wedge \ (\forall n; n > n_0)[A(n-1) \to A(n)]\Big) \to (\forall n)[A(n)]$$

allgemeingültig.

Die Anwendung von Theorem 4.1 als Beweisverfahren sieht diesmal wie folgt aus:

- *Induktionsanfang* (IA): Zeige $A(0), A(1), \ldots, A(n_0)$. (Da n_0 fest ist, sind dies nur endlich viele Fälle.)
- *Induktionsschritt* (IS): Zeige $A(n)$ für ein allgemeines $n > n_0$ unter der Annahme (*Induktionsvoraussetzung*, IV), dass $A(n-1)$ als wahr angenommen wird.

Der Fall $n_0 = 0$ entspricht gerade der Standardform der vollständigen Induktion.

Wir betrachten wiederum Beispiele für diese Form des Induktionsbeweises. Ein typischer Fall hierbei sind Aussagen, die nicht für alle natürlichen Zahlen gelten.

Proposition 4.C *Für alle $n \in \mathbb{N}$ mit $n \geq 4$ gilt $n! \geq 2^n$.*

Diese Proposition kann nicht auf alle natürlichen Zahlen $n \geq 3$ ausgedehnt werden, da $3! = 6 < 8 = 2^3$ gilt.

Die logische Struktur des Indukionsbeweises im Induktionsanfang ist hier so, dass die Aussageform $A(n)$ gerade

$$A(n) =_{\text{def}} \text{„ } n \geq 4 \ \rightarrow \ n! \geq 2^n \text{ “}$$

ist und $n_0 = 4$ gesetzt werden kann. Beweisen wollen wir die Aussage $(\forall n)[A(n)]$. Wegen der Implikationsstruktur von $A(n)$ sind die Aussagen $A(0), A(1), A(2), A(3)$ trivialerweise wahr. Als einziger Fall müssen wir also im Induktionsanfang $A(4)$ überprüfen.

Beweis: (*Induktion über n*)

- *Induktionsanfang*: Für $n = 4$ gilt $4! = 24 \geq 16 = 2^4$.
- *Induktionsschritt*: Für $n > 4$ gilt

$$\begin{array}{rcll} n! & = & n \cdot (n-1)! & \text{(nach Definition von } n!) \\ & \geq & n \cdot 2^{n-1} & \text{(nach } \textit{Induktionsvoraussetzung}) \\ & \geq & 2 \cdot 2^{n-1} & \text{(da } n \geq 1) \\ & = & 2^n & \end{array}$$

Damit ist die Proposition bewiesen. ∎

Es ist jedoch nicht immer so einfach ein geeignetes n_0 zu wählen, um eine Aussage mittels Induktion zu beweisen.

> **Beispiel:** Wir betrachten folgende Fragestellung: Gegeben $k \in \mathbb{N}$, für welches $n_0 \in \mathbb{N}$ gilt die Aussage: *Für alle $n \in \mathbb{N}$ mit $n \geq n_0$ gilt $n \leq 2^{n-k}$*?

Zunächst versuchen wir n_0 so zu bestimmen, dass der Induktionsschritt funktioniert:

- *Induktionsschritt*: Für $n > n_0$ gilt

$$\begin{aligned} n &= (n-1)+1 \\ &\leq 2^{n-1-k}+1 && \text{(nach } \textit{Induktionsvoraussetzung}\text{)} \\ &\leq 2^{n-1-k}+2^{n_0-k} && \text{(falls } n_0 \text{ die Ungleichung } 1 \leq 2^{n_0-k} \text{ erfüllt)} \\ &\leq 2^{n-1-k}+2^{n-1-k} && \text{(da } n-1 \geq n_0\text{)} \\ &= 2^{n-k} \end{aligned}$$

Der Induktionsschritt kann also für jedes $n_0 \geq k$ durchgeführt werden. Setzen wir allerdings $n_0 = k$, so gilt im Induktionsanfang $k \leq 2^{k-k}$ lediglich für $k \in \{0, 1\}$. Wir müssen also *ein* n_0 so finden, dass

$$2 \leq k \leq n_0 \leq 2^{n_0-k}$$

gilt. Durch Experimentieren erhält man z.B. als Ansatz $n_0 = k^2$. In der Tat gelingt der Induktionsanfang mit dieser Wahl.

- *Induktionsanfang*: Für $n = n_0 = k^2$ gilt zunächst

$$\begin{aligned} 2\log_2 k &\leq k \cdot \log_2 k && \text{(da } k \geq 2\text{)} \\ &\leq k \cdot (k-1) && \text{(nach Proposition 4.B)} \\ &= k^2 - k \end{aligned}$$

  Damit gilt $k^2 = 2\log_2 k \leq 2^{k^2-k}$.

Wir können die Aussage also für alle $n \geq k^2$ beweisen.

Proposition 4.D *Es sei $k \in \mathbb{N}$. Dann gilt $n \leq 2^{n-k}$ für alle $n \in \mathbb{N}$ mit $n \geq k^2$.*

Der Induktionsbeweis ergibt sich aus obigem Beispiel.

4.3 Zweite verallgemeinerte Form der vollständigen Induktion

Mitunter genügt im Induktionsschritt für n nicht die Rückführung auf $n-1$.

Das Induktionsprinzip kann auch dahingehend verallgemeinert werden (ohne Beweis).

Theorem 4.3 *Es seien $A(n)$ eine Aussageform mit der freien Variable n über dem Universum der natürlichen Zahlen und $n_0 \in \mathbb{N}$. Dann ist die Aussage*

$$\Big((\forall n; n \leq n_0)[A(n)] \ \wedge \ (\forall n; n > n_0)\,[(\forall m; m < n)[A(m)] \to A(n)]\Big) \to (\forall n)[A(n)]$$

allgemeingültig.

Die Anwendung von Theorem 4.3 als Beweisverfahren sieht hier wie folgt aus:

- *Induktionsanfang* (IA): Zeige $A(0), A(1), \ldots, A(n_0)$.
- *Induktionsschritt* (IS): Zeige $A(n)$ für ein allgemeines $n > n_0$ unter der Annahme (*Induktionsvoraussetzung*, IV), dass $A(m)$ für alle $m < n$ gilt.

Wir betrachten wiederum Beispiele für diese Form des Induktionsbeweises. Ein typischer Fall für die Form des induktiven Beweises sind komplexere Rekursionen.

Die Folge der Fibonacci-Zahlen definieren wir in der folgenden Form:

$$\begin{aligned} F_0 &=_{\text{def}} 1, \\ F_1 &=_{\text{def}} 2, \\ F_n &=_{\text{def}} F_{n-1} + F_{n-2} \qquad \text{für } n \geq 2. \end{aligned}$$

Die ersten Zahlen dieser Folge sind $1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$. Wir wollen mittels Induktion beweisen, dass die Folge der Fibonacci-Zahlen exponentiell wächst.

Proposition 4.E *Für alle $n \in \mathbb{N}$ gilt $F_n \geq \left(\frac{\sqrt{5}+1}{2}\right)^n$.*

Beweis: (*Induktion über n*)

- *Induktionsanfang*: Für $n \leq 1$ gilt $F_0 = 1 \geq \left(\frac{\sqrt{5}+1}{2}\right)^0$ und $F_1 = 2 \ \geq \ \left(\frac{\sqrt{5}+1}{2}\right)^1$.
- *Induktionsschritt*: Für $n > 1$ erhalten wir

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} && \text{(nach Definition von } F_n) \\ &\geq \left(\frac{\sqrt{5}+1}{2}\right)^{n-1} + \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} && \text{(nach } \textit{Induktionsvoraussetzung}) \end{aligned}$$

$$
\begin{aligned}
&= \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} \cdot \left(\frac{\sqrt{5}+1}{2}+1\right) \\
&= \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} \cdot \left(\frac{\sqrt{5}+1}{2}\right)^{2} \\
&= \left(\frac{\sqrt{5}+1}{2}\right)^{n}
\end{aligned}
$$

Damit ist die Proposition bewiesen. ■

An einem weiteren Beispiel wollen wir auch auf die Fallstricke hinweisen, die zu fehlerhaften Induktionsbeweisen führen können.

Beispiel: Wir zeigen folgende, empirisch ganz offensichtlich falsche Aussage:

> *Alle Personen in einer Menge X von $\|X\| = n > 0$ Personen sind gleich groß.*

Wir beweisen diese Aussage mittels der zweite verallgemeinerten Form der vollständigen Induktion über n.

- *Induktionsanfang*: Für $n = 1$ ist die offensichtlich wahr.
- *Induktionsschritt*: Für $n > 1$ sei X eine beliebige Menge mit $\|X\| = n$ Personen. Dann zerlegen wir X in Mengen Y und Z mit folgenden Eigenschaften:
  1. $X = Y \cup Z$
  2. $\|Y \cap Z\| = 1$
  3. $\|Y\| < \|X\|$
  4. $\|Z\| < \|X\|$

  Nach Induktionsvoraussetzung folgt aus der Eigenschaft $\|Y\| < \|X\|$, dass alle Personen in Y gleich groß sind. Hierbei ist zu beachten, dass $1 \leq \|Y\| \leq n-1$ gilt; wir dürfen also die Induktionsvorausetzung anwenden. Gleichfalls folgt nach Induktionsvoraussetzung aus der Eigenschaft $\|Z\| < \|X\|$, dass alle Personen in Z gleich groß sind. Da $Y \cap Z \neq \emptyset$ gilt, gibt es eine Person in beiden Mengen Y und Z, zu der alle Personen der beiden Mengen gleich groß sind. Wegen $y \cup Z = X$ sind alle Personen in X gleich groß.

Damit wäre die Aussage bewiesen, hätten wir nicht einen Fehler gemacht. Wo liegt er?

4.4 Strukturelle Induktion

Wir wollen das Induktionsprinzip zu einer Beweismethode über induktiv definierten Mengen erweitern. Dabei führen wir nur den Spezialfall mittels einer Operation aus.

Definition 4.4 *Es sei $f : A^n \to A$ eine n-stellige Funktion (Operation). Dann sind die Abbildungen $\Gamma_f : \mathcal{P}(A) \to \mathcal{P}(A)$ sowie $\Gamma_f^k : \mathcal{P}(A) \to \mathcal{P}(A)$ für alle $k \in \mathbb{N}$ wie folgt definiert (für $B \subseteq A$):*

$$\begin{aligned}
\Gamma_f^0(B) &=_{\text{def}} B \\
\Gamma_f^k(B) &=_{\text{def}} \Gamma_f^{k-1}(B) \cup \left\{ f(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \Gamma_f^{k-1}(B) \right\} \\
\Gamma_f(B) &=_{\text{def}} \bigcup_{k=0}^{\infty} \Gamma_f^k(B)
\end{aligned}$$

Die Menge $\Gamma_f(B)$ heißt Abschluss *von B unter f.*

Anschaulich gehören zur Menge $\Gamma_f(B)$ alle diejenigen Elemente von A, die sich durch eine endliche Anzahl von Hintereinanderausführungen der Operation f aus den Elementen der Menge B konstruieren lassen.

Beispiele: Wir wollen Definition 4.4 an Beispielen nachvollziehen.

- Wenn wir die Operation $\text{inc} : \mathbb{N} \to \mathbb{N} : n \mapsto n + 1$ betrachten, so gilt:

$$\begin{aligned}
\Gamma_{\text{inc}}^0(\{0\}) &= \{0\} \\
\Gamma_{\text{inc}}^1(\{0\}) &= \{0\} \cup \{1\} = \{0, 1\} \\
\Gamma_{\text{inc}}^2(\{0\}) &= \{0, 1\} \cup \{1, 2\} = \{0, 1, 2\} \\
\Gamma_{\text{inc}}^3(\{0\}) &= \{0, 1, 2\} \cup \{1, 2, 3\} = \{0, 1, 2, 3\} \\
&\vdots \\
\Gamma_{\text{inc}}^k(\{0\}) &= \{0, 1, \ldots, k\} \\
&\vdots \\
\Gamma_{\text{inc}}(\{0\}) &= \mathbb{N}
\end{aligned}$$

  Der Beweis der Gleichheit $\Gamma_{\text{inc}}^k(\{0\}) = \{0, 1, \ldots, k\}$ für alle $k \in \mathbb{N}$ kann mittels vollständiger Induktion über k geführt werden.

- Wenn wir die Operation $+ : \mathbb{N}^2 \to \mathbb{N} : (n, m) \mapsto n + m$ betrachten, so gilt:

$$\begin{aligned}
\Gamma_{\text{inc}}^0(\{1\}) &= \{1\} \\
\Gamma_{\text{inc}}^1(\{1\}) &= \{1\} \cup \{2\} = \{1, 2\}
\end{aligned}$$

$$
\begin{aligned}
\Gamma^2_{\text{inc}}(\{1\}) &= \{1,2\} \cup \{2,3,4\} = \{1,2,3,4\} \\
\Gamma^3_{\text{inc}}(\{1\}) &= \{1,2,3,4\} \cup \{2,3,4,5,6,7,8\} = \{1,2,3,4,5,6,7,8\} \\
&\vdots \\
\Gamma^k_{\text{inc}}(\{1\}) &= \{1,2,\ldots,2^k\} \\
&\vdots \\
\Gamma_{\text{inc}}(\{1\}) &= \mathbb{N}_+
\end{aligned}
$$

Auch hier kann der Beweis der Gleichheit $\Gamma^k_{\text{inc}}(\{1\}) = \{1,2,\ldots,2^k\}$ für alle $k \in \mathbb{N}$ mittels vollständiger Induktion über k geführt werden.

Definition 4.5 *Eine Menge $B \subseteq A$ heißt* endlich erzeugt *(oder induktiv definiert) aus $B_0 \subseteq A$, falls es eine Funktion $f : A^n \to A$ gibt mit $B = \Gamma_f(B_0)$.*

Für endlich erzeugte Mengen können wir das Beweisprinzip der strukturelle Induktion formal angeben (ohne Beweis).

Theorem 4.6 *Es sei B eine endlich erzeugte Menge aus B_0 mittels f. Es sei $A(x)$ eine Aussageform mit der freien Variablen x über dem Universum B. Dann ist die Aussage*

$$
\Big((\forall x \in B_0)[A(x)] \ \wedge \ (\forall k; k > 0)\left[(\forall x \in \Gamma^{k-1}_f(B_0))[A(x)] \to (\forall x \in \Gamma^k_f(B_0))[A(x)]\right]\Big) \to (\forall x \in B)[A(x)]
$$

allgemeingültig.

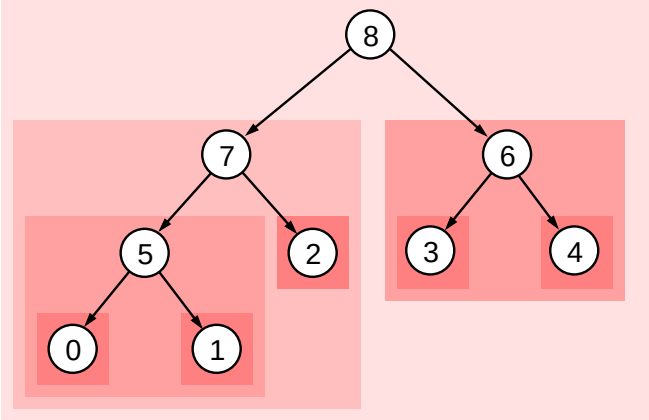
Die Anwendung dieser recht komplizierten Formulierung als Beweisprinzip ist wie folgt:

- *Induktionsanfang* (IA): Zeige $A(x)$ für alle $x \in B_0$.
- *Induktionsschritt* (IS): Zeige $A(x)$ für ein allgemeines $x \in B \setminus B_0$ unter der Annahme (*Induktionsvoraussetzung*, IV), dass $A(y_1), \ldots, A(y_n)$ für $x = f(y_1, \ldots, y_n)$ gilt. (Hier ist unter technischen Gesichtspunkten darauf zu achten, dass $y_1, \ldots, y_n$ einfacher sind, d.h. ist $x \in \Gamma^k_f(B_0)$, so muss $y_1, \ldots, y_n \in \Gamma^{k-1}_f(B_0)$ gelten.)

Zum Abschluss wollen wir uns ein Beispiel für die in der Informatik typische konstruktive Vorgehensweise anschauen.

Eine wichtige Datenstruktur in der Informatik sind Binärbäume als Verallgemeinerung von Listen. In einer Liste hat jedes Element bis auf das letzte genau einen Nachfolger und jedes Element bis auf das erste genau einen Vorgänger. Verlangt man nur die Eigenschaft das jedes Element bis auf eines genau einen Vorgänger besitzt (und Kreise ausgeschlossen

werden), gelangt man zu Bäumen. Eine Sonderklasse von Bäumen sind volle, gewurzelte Binärbäume. Eine Beispiel ist der folgende Baum:



Die Menge aller vollen, gewurzelten Binärbäume kann man wie folgt induktiv definieren. Bäume sind Tripel (V, E, r), wobei V für die Menge der Knoten, $E \subseteq V^2$ für die Menge der Kanten sowie $r \in V$ für die Wurzel stehen. Wir geben nun eine Menge B_0 und eine Operation f an:

$$\begin{aligned} B_0 &=_{\text{def}} \{\ (\{r\}, \emptyset, r) \mid r \in \mathbb{N}\ \} \\ f((V_1, E_1, r_1), (V_2, E_2, r_2)) &=_{\text{def}} (V_1 \cup V_2 \cup \{r\}, E_1 \cup E_2 \cup \{(r, r_1), (r, r_2)\}, r), \\ &\qquad \text{wobei } V_1 \cap V_2 = \emptyset \text{ sowie } r \notin V_1 \cup V_2 \text{ gilt} \end{aligned}$$

Die Menge der vollen, gewurzelten Binärbäume ist dann gerade die Menge $\Gamma_f(B_0)$.

Bevor wir unseren zu beweisende Eigenschaften formulieren, führen wir noch zwei Begriffe ein. Es sei $T = (V, E, r)$ ein voller, gewurzelter Binärbaum. Ein Element $v \in V$ heißt *Blatt*, falls es kein $u \in V$ mit $(v, u) \in E$ gibt; sonst heißt v *innerer Knoten*.

Proposition 4.F *Für einen vollen, gewurzelten Binärbaum T seien n_T die Anzahl innerer Knoten und m_T die Anzahl der Blätter. Dann gilt stets $n_T = m_T - 1$.*

Beweis: (*Induktion über den Aufbau der Bäume*)

- *Induktionsanfang*: Ist $T = (\{r\}, \emptyset, r)$, so gilt $n_T = 0$ und $m_T = 1$.
- *Induktionsschritt*: Es sei $T = f(T_1, T_2)$ für geeignete Bäume $T_1 = (V_1, E_1, r_1)$ und $T_2 = (V_2, E_2, r_2)$. Dann gilt insbesondere, dass die Blätter bzw. inneren Knoten von

T_1 und T_2 auch Blätter bzw. innere Knoten von T sind, da in T nur die Paare (r, r_1) und (r, r_2) hinzukommen. Mithin gilt:

$$\begin{aligned} n_T &= n_{T_1} + n_{T_2} + 1 && (r \text{ ist ein innerer Knoten von } T) \\ &= (m_{T_1} - 1) + (m_{T_2} - 1) + 1 && (\text{nach } \textit{Induktionsvoraussetzung}) \\ &= (m_{T_1} + m_{T_2}) - 1 \\ &= m_T - 1 \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Literaturverzeichnis

[MM06] Christoph Meinel und Martin Mundhenk. *Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen. Eine Einführung.* 3., überarbeitete und erweiterte Auflage. B. G. Teubner Verlag, Wiesbaden, 2006.

[Ste07] Angelika Steger. *Diskrete Strukturen. Band 1: Kombinatorik-Graphentheorie-Algebra.* 2. Auflage. Springer-Verlag, Berlin, 2007.

[SS02] Thomas Schickinger und Angelika Steger. *Diskrete Strukturen. Band 2: Wahrscheinlichkeitstheorie und Statistik.* Springer-Verlag, Berlin, 2002.

[Wag03] Klaus W. Wagner. *Theoretische Informatik. Eine kompakte Einführung.* 2. überarbeitete Auflage. Springer-Verlag, Berlin, 2003.

[WHK04] Manfred Wolff, Peter Hauck und Wolfgang Küchlin. *Mathematik für Informatik und Bioinformatik.* Springer-Verlag, Berlin, 2004.