Theoretische Grundlagen der Informatik 1 (TheGI1)
— Grundlagen und Algebraische Strukturen —

Formelsammlung
WiSe 2011/12 : v9

Technische Universität Berlin

Uwe Nestmann

24. Januar 2012

Zusammenfassung

Wir halten uns in diesem Dokument weitgehend an die Notationen des Lehrbuches *Mathematisch-strukturelle Grundlagen der Informatik* [EMC+01], da dieses Buch bisher auch in den TheGI-Kursen 3 und 4 verwendet wird.

Literatur

[EMC+01] H. Ehrig, B. Mahr, F. Cornelius, M. Grosse-Rhode, and P. Zeitz. *Mathematisch-strukturelle Grundlagen der Informatik, 2. überarbeitete Auflage*. Springer, 2001.

[Sch03] Uwe Schöning. *Theoretische Informatik — kurzgefasst*. Spektrum Lehrbuch. Spektrum Akademischer Verlag, 2003. 4. Auflage, korrigierter Nachdruck.

Inhaltsverzeichnis

1 Grundlagen

1.1 Grundbegriffe der Mengenlehre und Logik

Standardmengen verwenden einen anderen Schriftsatz als Metavariablen für Mengen; für letztere bevorzugen wir $A, B, C, \ldots$, möglicherweise mit Indizes (Zahlen oder anderen Buchstaben) versehen.

1.1.1 Notation (Beschreibungsformen) Eine Menge A kann durch

$$A \triangleq \{ a_1, a_2, a_3, \ldots \}$$

als die explizite Aufzählung unterscheidbarer Elemente a_i definiert werden. Die Aussage „$a \in A$“ bezeichnet den Sachverhalt, dass a ein Element der Menge A ist. Die eindeutig gegebene *leere Menge* enthält keine Elemente; sie wird entweder durch $\emptyset$ oder auch $\{\}$ bezeichnet. Gelegentlich ist es bequem, die Elemente einer Menge durch die Elemente einer sogenannten *Indexmenge* abstrakt zu benennen. Dann heißt

$$\{ x_i \mid i \in I \}$$

über I indizierte Menge.

1.1.2 Definition (Zahlenmengen)

- $\mathbb{N} \triangleq \{ 0, 1, 2, 3, \ldots \}$
- $\mathbb{N}^+ \triangleq \{ 1, 2, 3, \ldots \}$
- Mit $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bezeichnen wir die gebräuchlichen Mengen von *ganzen Zahlen*, *rationalen Zahlen*, *reellen Zahlen*.

1.1.3 Definition (Größe von Mengen) Sei A eine beliebige Menge.
$\#(A)$ bezeichnet die Anzahl der Elemente in A. Es gilt $\#(A) \in \mathbb{N} \cup \{\infty\}$.

1.1.4 Notation (Beschreibungsformen) Eine Menge A kann mit

$$A \triangleq \{ x \in B \mid P(x) \}$$

durch die Angabe eines definierenden „Prädikats“ P zur *Variablen* x in Bezug auf eine andere Menge B definiert werden. Das Symbol „|“ kann dabei als „so dass“ gelesen werden. Die Angabe von $P(x)$ erfolgt entweder umgangssprachlich oder durch eine logische Formel (siehe 1.1.7ff). Die Angabe von B kann entfallen, jedoch beschreibt $\{ x \mid P(x) \}$ nur dann eine Menge, wenn $P(x)$ für alle x entweder wahr oder falsch ist.

1.1.5 Definition (Zahlenmengen)

- $[m, n] \triangleq \{ i \in \mathbb{N} \mid m \leq i \text{ und } i \leq n \}$ für $m, n \in \mathbb{N}$

1.1.6 Bemerkung (Russell'sches Paradox)
$\{ x \mid x \notin x \}$ ist keine Menge.

Wir führen aussagen- und prädikatenlogische Konnektive zunächst semi-formal als symbolische Abkürzungen natürlichsprachlicher Begriffe ein. Eine Aussage φ ist eine Formel mit wohldefiniertem *Wahrheitswert*, also entweder „wahr“ (kurz: T oder $\top$) oder „falsch“ (kurz: F oder $\bot$). Anstelle von ϕ oder ψ verwenden wir auch $p, q, \ldots$ als Metavariablen für logische Formeln. $\mathbb{B} \triangleq \{\mathsf{T}, \mathsf{F}\}$ bezeichnet die Menge der Wahrheitswerte.

1.1.7 Notation (Aussagenlogik) [1]

- *Konjunktion* $\wedge$ bezeichnet „und“
- *Disjunktion* $\vee$ bezeichnet „oder“
- *Negation* $\neg$ bezeichnet „nicht“
- *Implikation* $\Rightarrow$ bezeichnet „impliziert“ (d.h. „läßt schließen auf“)
- *Äquivalenz* $\Leftrightarrow$ bezeichnet „genau dann, wenn“ („g.d.w.“)

1.1.8 Definition Die Bedeutung der aussagenlogischen Konnektive wird durch Wahrheitstabellen definiert:

φ_1	φ_2	$\varphi_1 \wedge \varphi_2$
F	F	F
F	T	F
T	F	F
T	T	T

φ_1	φ_2	$\varphi_1 \vee \varphi_2$
F	F	F
F	T	T
T	F	T
T	T	T

φ	$\neg\varphi$
F	T
T	F

φ_1	φ_2	$\varphi_1 \Rightarrow \varphi_2$
F	F	T
F	T	T
T	F	F
T	T	T

φ_1	φ_2	$\varphi_1 \Leftrightarrow \varphi_2$
F	F	T
T	F	F
F	T	F
T	T	T

Wenn verschiedene Aussagenschemata die gleiche Bedeutung haben, sprechen wir von *logischer Äquivalenz*, häufig bezeichnet mit $\equiv$. Aussagenschemata, die maximal eine Aussagenvariable oder maximal einen Operator betreffen, nennen wir *trivial*; entsprechende Äquivalenzen dürfen ohne Beweis benutzt werden (z.B.: $\mathsf{T} \wedge p \equiv p$, $p \vee \mathsf{F} \equiv p$, $p \Rightarrow p \equiv \mathsf{T}$, $\ldots$).

1.1.9 Notation Für Formeln, die mehr als ein Konnektiv enthalten, verwenden wir Klammerpaare $(\cdot)$, um die Eindeutigkeit der Interpretation von Formeln sicherzustellen. Um die Klammerzahl zu reduzieren und die Lesbarkeit der Formeln zu unterstützen, gelten darüberhinaus sogenannte Regeln des *Operatorenvorrangs*. Hier gelten die folgenden:

- $\neg$ bindet stärker als alle anderen Konnektive;
- $\wedge$ und $\vee$ binden gleich stark;
- $\wedge$ und $\vee$ binden stärker als $\Rightarrow$ und $\Leftrightarrow$;
- $\Rightarrow$ und $\Leftrightarrow$ binden gleich stark.

[1] Anstelle der Symbole $\Rightarrow$ und $\Leftrightarrow$ werden im Rahmen logischer Formeln oft die damit eng verwandten Symbole $\rightarrow$ und $\leftrightarrow$ verwendet. Für eine präzise Klärung des Unterschieds, sowohl intuitiv-informell als auch formal, verweisen wir auf TheGI3.

1.1.10 Proposition (Logische Äquivalenz (I))

$$\begin{array}{rcl@{\qquad}rcl}
p \wedge q & \equiv & q \wedge p & p \wedge p & \equiv & p \vee p \\
p \vee q & \equiv & q \vee p & \neg\neg p & \equiv & p \\
(p \vee q) \vee r & \equiv & p \vee (q \vee r) & \neg(p \wedge q) & \equiv & \neg p \vee \neg q \\
(p \wedge q) \wedge r & \equiv & p \wedge (q \wedge r) & \neg(p \vee q) & \equiv & \neg p \wedge \neg q \\
(p \wedge q) \vee r & \equiv & (p \vee r) \wedge (q \vee r) & p \wedge \neg p & \equiv & \mathsf{F} \\
(p \vee q) \wedge r & \equiv & (p \wedge r) \vee (q \wedge r) & p \vee \neg p & \equiv & \mathsf{T}
\end{array}$$

$$\begin{array}{rcl}
p \Rightarrow q & \equiv & \neg p \vee q \\
p \Rightarrow q & \equiv & \neg q \Rightarrow \neg p \\
p \Leftrightarrow q & \equiv & (p \Rightarrow q) \wedge (q \Rightarrow p)
\end{array}$$

1.1.11 Notation (Prädikate)
Wir schreiben $\phi(x)$, um anzudeuten, dass die Formel ϕ einen variablen Anteil x, eine sogenannte *Variable* bzw. einen *Platzhalter*, enthält.
$\phi(x)$ heißt auch *Prädikat*.

1.1.12 Notation (Quantoren)

- *Universelle Quantifikation* $\forall$ bezeichnet „für alle“
  $\forall x.\phi(x)$ bedeutet „für alle x gilt die Aussage $\phi(x)$“
- *Existentielle Quantifikation* $\exists$ bezeichnet „es gibt“
  $\exists x\,.\,\phi(x)$ bedeutet „es gibt ein x für das $\phi(x)$ gilt.“

$\exists! x\,.\,\phi(x)$ ist eine Abkürzung für „es gibt *genau* ein x für das $\phi(x)$ gilt.“

1.1.13 Notation Für Quantoren gelten folgende Regeln des *Operatorenvorrangs*:

- $\forall$ und $\exists$ binden gleich stark;
- $\forall$ und $\exists$ binden schwächer als alle anderen Konnektive.

1.1.14 Proposition (Logische Äquivalenz (II))

$$\begin{array}{rcl}
\neg(\forall x\,.\,P(x)) & \equiv & \exists x\,.(\neg P(x)) \\
\neg(\exists x\,.\,P(x)) & \equiv & \forall x\,.(\neg P(x))
\end{array}$$

$$\exists! x\,.\,P(x) \quad \equiv \quad \Big(\exists x\,.(P(x))\Big) \;\wedge\; \Big(\forall x, y\,.\,P(x) \wedge P(y) \Rightarrow x = y\Big)$$

1.1.15 Definition (Teilmengen, Gleichheit von Mengen)
Seien A und B zwei beliebige Mengen.
A heißt *Teilmenge* von B, geschrieben $A \subseteq B$, wenn für alle x gilt:

$$(x \in A) \Rightarrow (x \in B)$$

A und B heißen *gleich*, geschrieben $A = B$, wenn gilt:

$$A \subseteq B \;\wedge\; B \subseteq A$$

A heißt *echte Teilmenge* von B, geschrieben $A \subset B$, wenn gilt:

$$A \subseteq B \;\wedge\; A \neq B$$

Wenn A (echte) Teilmenge von B, dann heisst B *(echte) Obermenge* von A.

1.1.16 Definition (Vereinigung, Durchschnitt, Komplement, Produkt)
Seien A und B zwei beliebige Mengen. Wir definieren:
Vereinigung[smenge] von A und B:

$$A \cup B \triangleq \{\, x \mid x \in A \vee x \in B \,\}$$

Schnitt[menge] von A und B:

$$A \cap B \triangleq \{\, x \mid x \in A \wedge x \in B \,\}$$

Komplement von A in Bezug auf B:

$$B \setminus A \triangleq \{\, x \mid x \in B \wedge x \notin A \,\}$$

[kartesisches] Produkt von A und B:

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

disjunkte Vereinigung von A und B:

$$A \uplus B \triangleq (A \times \{1\}) \ \cup \ (B \times \{2\})$$

Die Wahl von $\{1, 2\}$ in der Definition disjunkter Vereinigung ist willkürlich. Beliebige andere Werte hätten verwendet werden können.

1.1.17 Definition (Potenzmenge) Sei A eine beliebige Menge. Dann heißt

$$\mathcal{P}(A) \triangleq \{\, B \mid B \subseteq A \,\}$$

Potenzmenge von A.

1.1.18 Proposition Sei A eine beliebige Menge. Dann gilt:

$$\#(\mathcal{P}(A)) = \begin{cases} 2^{\#(A)} & \text{falls } \#(A) < \infty \\ \infty & \text{falls } \#(A) = \infty \end{cases}$$

1.1.19 Proposition (Mathematische Induktion)
Sei $P(n)$ ein Prädikat über den natürlichen Zahlen $\mathbb{N}$. Falls

1. $P(0)$
2. $P(n) \Rightarrow P(n{+}1)$ für alle $n \in \mathbb{N}$

beide gelten (bzw. bewiesen werden können), dann gilt auch:

$$\forall n \in \mathbb{N} \,.\, P(n)$$

1.1.20 Notation Sei $P(n)$ ein Prädikat über den natürlichen Zahlen $\mathbb{N}$.
Das Prinzip aus Proposition kann knapp in einer einheitlichen Formel, genannt *Induktionsschema*, zusammengefasst werden.

$$\Big(\ P(0) \ \wedge \ \Big(\ \forall n \in \mathbb{N}. \big(P(n) \Rightarrow P(n{+}1) \big) \ \Big) \ \Big) \Rightarrow (\ \forall n \in \mathbb{N}. P(n) \ )$$

1.1.21 Proposition (Werteverlaufsinduktion)
Sei $P(n)$ ein Prädikat über den natürlichen Zahlen $\mathbb{N}$. Dann gilt:

$$\Big(\ \forall n \in \mathbb{N}. \Big(\ \big(\forall m < n. P(m) \big) \Rightarrow P(n) \ \Big) \ \Big) \Rightarrow (\ \forall n \in \mathbb{N}. P(n) \ )$$

1.2 Relationen, Ordnungen

1.2.1 Definition (Kartesisches Produkt)
Seien $A_1, \ldots, A_n$ Mengen. Dann heißt

$$\begin{array}{rcl} \prod_{i\in[1,n]} A_i & \triangleq & A_1 \times \ldots \times A_n \\ & \triangleq & \{\, (a_1, \ldots, a_n) \mid \forall i \in [1, n] \,.\, a_i \in A_i \,\} \end{array}$$

das *(kartesische) Produkt* der A_i.
$A_1 \times A_2$ heißt *binäres Produkt*.
Die Elemente eines kartesischen Produkts heißen *Tupel*.
$()$ heißt *leeres Tupel*; es wird häufig auch mit λ bezeichnet.

1.2.2 Definition (Spezialfälle)
Sei A eine beliebige Menge.

- $A^n \triangleq \prod_{i\in[1,n]} A$ für $n \in \mathbb{N}$.
- $A^0 \triangleq \{\, \lambda \,\}$

1.2.3 Definition (Relation)
Seien $A_1, \ldots, A_n$ Mengen.
Eine Teilmenge $R \subseteq \prod_{i\in[1,n]} A_i$ heißt *n-stellige Relation*;
die Schreibweise „Relation R mit *Typ* $\prod_{i\in[1,n]} A_i$“

$$R : \prod_{i\in[1,n]} A_i$$

erlaubt es, Relationen [nur] aufgrund ihres Typs zu unterscheiden.
Im Gegensatz zu Definition 1.2.1 unterscheiden wir
bei der Typbestimmung zwischen $A \times \emptyset$ und $\emptyset \times A$ von $\emptyset$.
R heißt *homogen*, falls $A_i = A_j$ für alle $1 \leq i, j \leq n$.

1.2.4 Definition (Spezialfälle)
Seien A und B beliebige Mengen.

- $\nabla_{A,B} \triangleq A \times B$
  bezeichnet die *universelle Relation* bzw. *Allrelation* mit Typ $A \times B$.
- $\emptyset_{A,B} \triangleq \emptyset$
  bezeichnet die *leere Relation* mit Typ $A \times B$.
- $\Delta_A \triangleq \mathrm{Id}_A \triangleq \{(a, a) \mid a \in A\}$
  bezeichnet die *Diagonalrelation* bzw. *Identität* mit Typ A.

Wenn der Typ implizit klar ist, kann der Index weggelassen werden.

1.2.5 Notation In manchen Lehrbüchern, so auch in [EMC+01], wird eine Relation Rel als Paar $\langle \mathrm{Typ}(Rel), \mathrm{Graph}(Rel) \rangle$ definiert. Dies entspricht in unserem Fall der Schreibweise $\mathrm{Graph}(Rel) : \mathrm{Typ}(Rel)$.

Der Spezialfall der zweistelligen Relation heißt auch *binäre Relation*. Hier benutzen wir oft die Infixschreibweise aRb anstelle von $(a, b) \in R$.

1.2.6 Definition (Totalität und Eindeutigkeit)
Sei $R : A \times B$. R heißt

1. *linkstotal*, falls:
$$\forall a{\in}A \,.\, \exists b{\in}B \,.\, aRb$$
2. *rechtstotal*, falls:
$$\forall b{\in}B \,.\, \exists a{\in}A \,.\, aRb$$
3. *linkseindeutig*, falls:
$$\forall a_1, a_2{\in}A \,.\, \forall b{\in}B \,.\, \big(\; a_1Rb \wedge a_2Rb \Rightarrow a_1{=}a_2 \;\big)$$
4. *rechtseindeutig*, falls:
$$\forall a{\in}A \,.\, \forall b_1, b_2{\in}B \,.\, \big(\; aRb_1 \wedge aRb_2 \Rightarrow b_1{=}b_2 \;\big)$$

1.2.7 Definition (Komposition) Seien A, B, C drei beliebige Mengen. Seien $P : A \times B$ und $Q : B \times C$ zwei beliebige Relationen. Dann ist die *Komposition* $P;Q$ definiert wie folgt:
$$P;Q \;\triangleq\; \{\, (a, c) \mid \exists b{\in}B \,.\, aPb \wedge bQc \,\}$$

1.2.8 Notation Aus Bequemlichkeit schreiben wir oft PQ anstelle von $P;Q$. Aus Gründen der Konsistenz mit dem Kompositionsbegriff für Funktionen (siehe §1.3) verwenden wir auch die Notation: $Q \circ P \triangleq P;Q$

1.2.9 Proposition (Assoziativität der Komposition)
Seien A, B, C, D beliebige Mengen.
Seien $P : A \times B$, $Q : B \times C$ und $R : C \times D$ drei beliebige Relationen.
Dann gilt:
$$P;(Q;R) = (P;Q);R$$

1.2.10 Definition (Umkehrrelation)
Seien A und B zwei beliebige Mengen. Sei $R : A \times B$.
Die *Umkehrrelation* von R, geschrieben R^{-1}, ist definiert durch:
$$R^{-1} \;\triangleq\; \{\, (b, a) \mid (a, b) \in R \,\}$$

1.2.11 Proposition (Eigenschaften der Umkehrrelation)
Seien A, B, C drei beliebige Mengen. Seien $R : A \times B$ und $Q : B \times C$ zwei beliebige Relationen. Dann gilt:

1. $(R^{-1})^{-1} = R$
2. $(RQ)^{-1} = Q^{-1}R^{-1}$
3. $(Q \circ R)^{-1} = R^{-1} \circ Q^{-1}$

1.2.12 Definition (Eigenschaften homogener Relationen)
Sei $R : A \times A$ eine beliebige homogene Relation. Dann heißt R:

reflexiv	falls	$\forall a{\in}A \,.\, aRa$	bzw	$\Delta_A \subseteq R$
irreflexiv	falls	$\forall a{\in}A \,.\, \neg(aRa)$	bzw	$\Delta_A \cap R = \emptyset$
symmetrisch	falls	$\forall a, b{\in}A \,.\, aRb \Rightarrow bRa$	bzw	$R^{-1} = R$
antisymmetrisch	falls	$\forall a, b{\in}A \,.\, aRb \wedge bRa \Rightarrow a{=}b$	bzw	$R^{-1} \cap R \subseteq \Delta_A$
transitiv	falls	$\forall a, b, c{\in}A \,.\, aRb \wedge bRc \Rightarrow aRc$	bzw	$R \circ R \subseteq R$
linear	falls	$\forall a, b{\in}A \,.\, aRb \vee bRa$	bzw	$R^{-1} \cup R = \nabla_{A,A}$

1.2.13 Definition (Ordnungen)
Sei $R : A \times A$ eine beliebige homogene Relation. Die Tabelle benennt die Mindestkriterien, so dass für R der jeweilige Ordnungsbegriff gilt.

Ordnungsbegriff	reflexiv	transitiv	antisymmetrisch	linear
Quasiordnung	•	•		
partielle Ordnung	•	•	•	
totale Ordnung	•	•	•	•

1.2.14 Notation (Ordnungsbegriffe)

- Quasiordnungen heißen auch *Präordnungen*.
- Partielle Ordnungen heißen auch *Halbordnungen*.
- Totale Ordnungen heißen auch *lineare Ordnungen*.
- Irreflexive Ordnungen heißen auch *streng* oder *strikt*.

1.2.15 Definition Sei $R : A \times A$ eine beliebige homogene Relation. Dann heißt R^n für $n \in \mathbb{N}$ die n-fache Komposition von R, definiert durch:

$$\begin{aligned} R^0 &\triangleq \Delta_A \\ R^{n+1} &\triangleq RR^n \end{aligned}$$

1.2.16 Bemerkung Die n-fache Komposition einer Relation kann gleichwertig links- bzw rechts-induktiv definiert werden:

$$R^{n+1} \triangleq RR^n \qquad \text{versus} \qquad R^{n+1} \triangleq R^n R$$

([Sch03] komponiert von links, [EMC+01] komponiert von rechts.)
Je nach Kontext erlauben wir uns beide Varianten.

1.2.17 Definition (Abschluss)
Sei $R : A \times A$ eine beliebige homogene Relation.

1. Der *reflexive Abschluss* von R ist definiert durch:
$$\mathrm{r}(R) \triangleq R \cup \Delta_A$$
2. Der *symmetrische Abschluss* von R ist definiert durch:
$$\mathrm{s}(R) \triangleq R \cup R^{-1}$$
3. Der *transitive Abschluss* von R ist definiert durch:
$$\mathrm{t}(R) \triangleq \bigcup_{n \in \mathbb{N}^+} R^n$$

Der Typ der Abschlussrelationen entspricht dem Typ der Basisrelation: $\mathrm{Typ}(\mathrm{r}(R)) = \mathrm{Typ}(\mathrm{s}(R)) = \mathrm{Typ}(\mathrm{t}(R)) = \mathrm{Typ}(R)$.

1.2.18 Definition Sei $\boldsymbol{M}$ eine Menge von Mengen. Dann gilt:

$$\begin{aligned} \bigcup \boldsymbol{M} &\triangleq \{\, x \mid \exists m \in \boldsymbol{M} \;.\; x \in m \,\} \\ \bigcap \boldsymbol{M} &\triangleq \{\, x \mid \forall m \in \boldsymbol{M} \;.\; x \in m \,\} \end{aligned}$$

Als Spezialfälle werden häufig indizierte Vereinigungen verwendet.

$$\begin{aligned} \textstyle\bigcup_{i \in I} m_i &\triangleq \{\, x \mid \exists i \in I \;.\; x \in m_i \,\} \\ \textstyle\bigcap_{i \in I} m_i &\triangleq \{\, x \mid \forall i \in I \;.\; x \in m_i \,\} \end{aligned}$$

1.3 Funktionen, Abbildungen, Kardinalitäten

1.3.1 Definition (Partielle Abbildung)
Sei $f : A \times B$ eine rechtseindeutige Relation. Dann heißt f *partielle Abbildung* f *vom Typ* $A \rightharpoonup B$, geschrieben $f : A \rightharpoonup B$.

1. Wir schreiben $f(a) = b$, falls $(a, b) \in f$.
2. $f(a)$ ist *Funktionswert von* f *an der Stelle* a.
3. A heißt *Argumentbereich* bzw. *Domain* von f, geschrieben $\mathrm{dom}(f)$.
   B heißt *Zielbereich* bzw. *Codomain* von f, geschrieben $\mathrm{cod}(f)$.
4. Seien $A_0 \subseteq A$ und $B_0 \subseteq B$. Dann heißen die Mengen
$$\begin{aligned} f(A_0) &\triangleq \{\, b \in B \mid \exists a \in A_0 \,.\, f(a) = b \,\} \\ f^{-1}(B_0) &\triangleq \{\, a \in A \mid \exists b \in B_0 \,.\, f(a) = b \,\} \end{aligned}$$
   Bild von A_0 *bzgl.* f, sowie *Urbild von* B_0 *bzgl.* f.
5. Die Mengen
$$\begin{aligned} \mathrm{Bild}(f) &\triangleq f(A) \\ \mathrm{Def}(f) &\triangleq f^{-1}(B) \end{aligned}$$
   heißen *Bildbereich* $\mathrm{Bild}(f) \subseteq B$ und *Definitionsbereich* $\mathrm{Def}(f) \subseteq A$.
6. Darüberhinaus heißt f *(totale) Abbildung*, geschrieben $f : A \to B$, falls f linkstotal ist.
7. Wir vewenden die Begriffe *Abbildung* und *Funktion* synonym.

1.3.2 Notation Anstelle von Paaren (a, b) verwendet man im Kontext von Abbildungen häufig auch die Schreibweise $a \mapsto b$. Partielle Abbildungen können dann auch durch folgende Schreibweise definiert werden:

$$f : A \rightharpoonup B; a \mapsto \mathrm{Ber}_f(a) \qquad \text{bzw.} \qquad f : A \rightharpoonup B; \begin{cases} a \mapsto \mathrm{Ber}_1(a) \,;\, P_1(a) \\ a \mapsto \mathrm{Ber}_2(a) \,;\, P_2(a) \\ \ldots \end{cases}$$

wobei die $P_1, P_2, \ldots$ eine Fallunterscheidung definieren und Ber_f sowie die $\mathrm{Ber}_1, \mathrm{Ber}_2, \ldots$ jeweilige Berechnungsvorschriften repräsentieren.

1.3.3 Definition (Gleicheit partieller Abbildungen)
Zwei partielle Abbildungen $f_1 : A_1 \rightharpoonup B_1$ und $f_2 : A_2 \rightharpoonup B_2$ heißen *gleich*, geschrieben $f_1 = f_2$, falls

$$A_1 = A_2 \quad \wedge \quad B_1 = B_2 \quad \wedge \quad \forall a \in A_1 \cap A_2 \,.\, f_1(a) = f_2(a)$$

1.3.4 Theorem (Komposition partieller Abbildungen)
Seien $f : A \rightharpoonup B$ und $g : B \rightharpoonup C$ partielle Abbildungen. Dann ist deren Komposition $(g \circ f) : A \rightharpoonup C$ wieder eine partielle Abbildung.

1.3.5 Definition (Eigenschaften partieller Abbildungen)

Begriff	LT	LE	RE	RT
partielle Abbildung			•	
Abbildung	•		•	
injektive partielle Abbildung		•	•	
surjektive partielle Abbildung			•	•
bijektive partielle Abbildung		•	•	•
Bijektion	•	•	•	•

1.3.6 Proposition (Umkehrabbildung I)
Sei $f : A \rightharpoonup B$ eine partielle Abbildung. Ist f injektiv, dann ist auch die Umkehrrelation $f^{-1} : B \times A$ eine injektive partielle Abbildung.
Außerdem gilt: $(f^{-1})^{-1} = f$.

1.3.7 Definition (Isomorphie)
Seien A und B Mengen. Wenn eine Bijektion $f : A \to B$ existiert, dann heißen A und B *isomorph*, geschrieben $A \cong B$.

1.3.8 Proposition (Umkehrabbildung II)
Eine Relation $f : A \times B$ ist genau dann eine Bijektion, wenn es eine Relation $g : B \times A$ gibt mit: $f \circ g = \Delta_B$ und $g \circ f = \Delta_A$ .Dann gilt zudem $g = f^{-1}$.

1.3.9 Theorem (Kürzbarkeit)
Seien A, B, C, D Mengen.
Seien $f : A \to B$, $g_1, g_2 : B \to C$, und $h : C \to D$ Abbildungen.

1. Falls f surjektiv, dann gilt: $(\ g_1 \circ f = g_2 \circ f\ ) \ \Rightarrow\ g_1 = g_2$
2. Falls h injektiv, dann gilt: $(\ h \circ g_1 = h \circ g_2\ ) \ \Rightarrow\ g_1 = g_2$

1.3.10 Theorem (Abbildungssatz)
Sei $f : A \to B$ eine Abbildung. Dann existieren

- eine Menge C (eindeutig bestimmt „bis auf Isomorphie“),
- eine surjektive Abbildung $g : A \to C$,
- eine injektive Abbildung $h : C \to B$,

so dass $f = h \circ g$.

1.3.11 Definition (Größe von Mengen (II))
Eine Menge A heißt *endlich*, falls es eine Bijektion vom Typ $A \to [1, n]$ für $n \in \mathbb{N}$ gibt; dann bezeichnet $\#(A) \triangleq n$ die entsprechende Anzahl der Elemente in A. Falls ein solches n nicht existiert, heißt A *unendlich* und wir notieren $\#(A) \triangleq \infty$.
Für $n \in \mathbb{N}$ definieren wir $\infty + n = \infty$, $\infty - n = \infty$, sowie $\infty \cdot n = \infty$.
Außerdem gelte: $\forall n \in \mathbb{N} \,.\, n < \infty$.

1.3.12 Proposition
Seien A und B endliche Mengen. Dann gilt:

$$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$$

1.3.13 Definition (Kardinalität; Vergleich von Mengengrößen)
Seien A und B zwei Mengen.

1. A und B haben die gleiche Kardinalität, $\mathrm{card}(A) = \mathrm{card}(B)$, falls es eine *Bijektion* vom Typ $A \to B$ gibt.
   A und B heißen dann auch *äquipotent*.
2. A hat höchstens die Kardinalität von B, $\mathrm{card}(A) \leq \mathrm{card}(B)$, falls es eine *injektive* Abbildung vom Typ $A \to B$ gibt.
3. A hat eine echt kleinere Kardinalität als B, $\mathrm{card}(A) < \mathrm{card}(B)$, falls $\mathrm{card}(A) \leq \mathrm{card}(B)$ und $\mathrm{card}(A) \neq \mathrm{card}(B)$.

1.3.14 Notation In der Literatur werden häufig sowohl die Anzahl $\#(A)$ als auch die Kardinalität $\mathrm{card}(A)$ einer Menge A mit $|A|$ bezeichnet. Das führt gelegentlich zu Mehrdeutigkeiten bei unendlichen Mengen.

1.3.15 Definition (Abzählbarkeit) Sei A eine Menge.

1. A heißt *abzählbar*, falls A endlich oder äquipotent zu $\mathbb{N}$ ist.
2. A heißt *abzählbar unendlich*, falls A äquipotent zu $\mathbb{N}$ ist.
3. A heißt *überabzählbar*, falls $\mathrm{card}(\mathbb{N}) < \mathrm{card}(A)$.

1.3.16 Proposition (Größe von Zahlenmengen)

1. $\#(\mathbb{N}) = \#(\mathbb{Z}) = \#(\mathbb{Q}) = \#(\mathbb{R}) = \infty$
2. $\mathrm{card}(\mathbb{N}) = \mathrm{card}(\mathbb{Z}) = \mathrm{card}(\mathbb{Q})$
3. $\mathrm{card}(\mathbb{Q}) < \mathrm{card}(\mathbb{R})$

1.3.17 Theorem (Cantor)
Sei A eine Menge. Dann gilt:

$$\mathrm{card}(A) < \mathrm{card}(\mathcal{P}(A))$$

1.3.18 Definition (Charakteristische Funktion)
Seien T, A zwei Mengen mit $T \subseteq A$.
Dann heißt die Abbildung $\chi_T : A \to \{0, 1\}$, definiert durch

$$\chi_T(a) \triangleq \begin{cases} 1 & \text{falls } a \in T \\ 0 & \text{falls } a \notin T \end{cases}$$

die *charakteristische Funktion von T bzgl. A*.

1.3.19 Definition (Multimengen) Sei A eine Menge. Dann bezeichnet die Abbildung $M_T : A \to \mathbb{N}$ eine eindeutig gegebene *Multimenge* T. Für jedes $a \in A$ heißt $M_T(a)$ die *Häufigkeit* bzw. *Multiplizität* von a in T.

1.3.20 Definition (Mengenfamilie)
Sei M eine Menge von Mengen.
Sei I eine sogenannte *Indexmenge*.
Eine surjektive Abbildung $A : I \to M$ heißt auch *Mengenfamilie* $(A_i)_{i \in I}$.

1.3.21 Bemerkung Mengenfamilien verwendet man oft, wenn man M implizit lassen möchte.

1.3.22 Definition (Divison mit Rest)
Sei $n \in \mathbb{N}$. Sei $k \in \mathbb{N}$. Dann gilt folgende Zerlegung:

$$\exists! m \in \mathbb{N} \ . \ \exists! r \in [0, k-1] \ . \ n = \underbrace{m}_{n \operatorname{div} k} \cdot \ k \quad + \underbrace{r}_{n \bmod k}$$

Wegen der Eindeutigkeit der angegebenen Zerlegung mittels m und r bezeichnen div und mod wohldefinierte Abbildungen.
Die Abbildung $n \bmod k$ wird oft auch mit $n \,\%\, k$ bezeichnet.

1.4 Äquivalenzen, Quotienten

1.4.1 Definition (Äquivalenzrelation)
Sei $R : A \times A$ eine beliebige homogene Relation.
R heißt *Äquivalenzrelation* bzw. *Äquivalenz*,
wenn R sowohl (1) reflexiv, (2) symmetrisch, als auch (3) transitiv ist.

1.4.2 Notation
Äquivalenzen sind binäre Relationen, also Mengen (von Paaren).
Wir können daher Äquivalenzrelationen vergleichen,
bzgl. Mengeninklusion („$\subseteq$“) und Mengengrößen ($\#(\cdot)$ und $\mathrm{card}(\cdot)$).

1.4.3 Lemma
Sei A eine beliebige Menge. Dann sind eindeutig bestimmt:

- $\nabla_{A,A}$ als $\subseteq$-größte Äquivalenz in $A \times A$;
- Δ_A als $\subseteq$-kleinste Äquivalenz in $A \times A$.

1.4.4 Proposition (Erzeugte Äquivalenz)
Sei $R : A \times A$ eine beliebige homogene Relation.
Unter allen Relationen, die Obermenge von R sind, ist:

1. $\mathrm{r}(R)$ die $\subseteq$-kleinste reflexive Relation,
2. $\mathrm{s}(R)$ die $\subseteq$-kleinste symmetrische Relation,
3. $\mathrm{t}(R)$ die $\subseteq$-kleinste transitive Relation, und
4. $\mathrm{t}(\mathrm{s}(\mathrm{r}(R)))$ die $\subseteq$-kleinste Äquivalenz.

1.4.5 Definition (Äquivalenzklassen)
Sei $R : A \times A$ eine Äquivalenz. Sei $a \in A$. Dann heißt:

$$[a]_R \triangleq \{\, x \in A \mid (a, x) \in R \,\}$$

Äquivalenzklasse von a bzgl. R.

1.4.6 Notation Wenn die intendierte Äquivalenz R aus dem Kontext eindeutig hervorgeht, schreiben wir auch $[a]$ anstelle von $[a]_R$.

1.4.7 Proposition
Sei $R : A \times A$ eine Äquivalenz. Sei $a \in A$. Dann gilt:

1. $a \in [a]$
2. $(a_1, a_2) \in R \iff [a_1] = [a_2]$
3. $(a_1, a_2) \notin R \iff [a_1] \cap [a_2] = \emptyset$

1.4.8 Definition (Quotient)
Sei $R : A \times A$ eine Äquivalenz.
Dann heißt die Menge aller Äquivalenzklassen, gegeben durch

$$A/R \triangleq \{\, [a]_R \mid a \in A \,\}$$

der *Quotient von A bzgl. R.*
Die Anzahl $\#(A/R)$ der Äquivalenzklassen von R heißt *Index von R.*

1.4.9 Definition (Repräsentantensystem)
Sei $R : A \times A$ eine Äquivalenz. Sei $S \subseteq A$.
S heißt *Repräsentantensystem von* A/R, falls gilt:

$$\forall a \in A \ . \ \exists! s \in S \ . \ s \in [a]$$

1.4.10 Proposition
Sei S *Repräsentantensystem von* A/R. Dann gilt:

1. $S \cong A/R$
2. $A = \bigcup_{x \in S} [x]_R$

1.4.11 Definition (Kern einer Abbildung)
Sei $f : A \to B$ eine Abbildung. Dann heißt die Relation

$$\mathrm{Ker}(f) \triangleq \{ \, (a_1, a_2) \in A \times A \mid f(a_1) = f(a_2) \, \}$$

der *Kern von* f.

1.4.12 Proposition (Kern einer Abbildung)
Sei $f : A \to B$ eine Abbildung.
Dann ist $\mathrm{Ker}(f)$ eine Äquivalenz.

1.4.13 Definition
Sei $R : A \times A$ eine beliebige Äquivalenz. Sei

$$\begin{array}{rccc} \mathrm{nat}_R & : & A & \to & A/R \\ & & a & \mapsto & [a]_R \end{array}$$

die *natürliche Abbildung zu* R. Dann gilt $\mathrm{Ker}(\mathrm{nat}_R) = R$.

1.4.14 Theorem (Faktorisierungssatz)
Sei $f : A \to B$ eine Abbildung.
Seien $\mathrm{nat}_f \triangleq \mathrm{nat}_{\mathrm{Ker}(f)}$, d.h.

$$\begin{array}{rccc} \mathrm{nat}_f & : & A & \to & A/\mathrm{Ker}(f) \\ & & a & \mapsto & [a]_{\mathrm{Ker}(f)} \end{array}$$

die *natürliche Abbildung von* f, und

$$\begin{array}{rccc} \mathrm{val}_f & : & A/\mathrm{Ker}(f) & \to & B \\ & & [a]_{\mathrm{Ker}(f)} & \mapsto & f(a) \end{array}$$

Es gilt:

1. nat_f ist surjektiv, val_f ist injektiv.
2. $f = \mathrm{val}_f \circ \mathrm{nat}_f$
3. $\mathrm{Bild}(f) \cong A/\mathrm{Ker}(f)$

1.4.15 Bemerkung Im Faktorisierungssatz ist
$\mathrm{Bild}(f)$ isomorph zu einem Repräsentantensystem für $A/\mathrm{Ker}(f)$.

2 Algebraische Strukturen – Klassisch

2.1 Wörter, Sprachen

2.1.1 Definition (Wörter)
Sei $\mathcal{A}$ eine Menge ($\neq \emptyset$), genannt *Alphabet*.
Die Elemente $s_i \in \mathcal{A}$ werden auch *Symbol*, *Zeichen*, *Buchstabe* genannt.

1. Ein *Wort* w über $\mathcal{A}$ ist eine endliche Sequenz $(a_1, \ldots, a_n)$ mit $n \in \mathbb{N}$ und $a_i \in \mathcal{A}$ für alle $1 \leq i \leq n$.
2. Wir bezeichnen mit $|w| = n$ die Länge des Wortes $w = (a_1, \ldots, a_n)$.
3. Wir bezeichnen das *leere Wort* (für $n = 0$) mit λ.
4. Die Notation $(w)_i$ bezeichnet die *Projektion* des Wortes w auf das i-te Symbol, definiert lediglich für $1 \leq i \leq |w|$.
5. $\mathcal{A}^*$ bezeichnet die Menge aller [endlichen] Wörter über $\mathcal{A}$.

Häufig vereinfachen wir $(a_1, \ldots, a_n)$ zu $a_1 \cdots a_n$.

2.1.2 Definition (Operationen auf Wörtern)
Seien $v = (a_1, \ldots, a_m)$ und $w = (b_1, \ldots, b_n)$ zwei Wörter aus $\mathcal{A}^*$.

1. Die *Konkatenation* von v und w ist definiert durch:
$$v \cdot w \triangleq (a_1, \ldots, a_m, b_1, \ldots, b_n)$$
Oft schreiben wir auch kurz vw.
2. v heißt *Präfix* von w, falls es $u \in \mathcal{A}^*$ gibt, so dass $v \cdot u = w$.
3. v heißt *Suffix* von w, falls es $u \in \mathcal{A}^*$ gibt, so dass $u \cdot v = w$.
4. v heißt *Teilwort* von w, falls es $u_1, u_2 \in \mathcal{A}^*$ gibt, so dass $u_1 \cdot v \cdot u_2 = w$.

2.1.3 Notation
Seien $v \in \mathcal{A}^*$ und $a \in \mathcal{A}$.
Anstelle von $(a) \cdot v$ schreiben wir oft av.
Anstelle von $v \cdot (a)$ schreiben wir oft va.

2.1.4 Lemma (Dekomposition) Sei w ein Wort über dem Alphabet $\mathcal{A}$.
Dann gilt genau einer der beiden folgenden Fälle:

1. $w = \lambda$ (also $|w| = 0$), oder
2. es gibt $a \in \mathcal{A}$ und $v \in \mathcal{A}^*$ und mit $|v| = |w| - 1$, so dass $w = av$.

Die obige Dekomposition „von links“ entspricht den in der Informatik üblichen Listenstrukturen. Alternativ—und völlig gleichwertig—kann man die Dekomposition auch „von rechts“ ausführen. In jedem Fall läßt sich damit ein Induktionsprinzip herleiten.

$$\left.\begin{array}{l} P(\lambda) \ \wedge \ \Big(\forall v{\in}\mathcal{A}^*.\big(P(v) \Rightarrow \forall a{\in}\mathcal{A} \ . \ P(av)\big) \Big) \\ \\ P(\lambda) \ \wedge \ \Big(\forall v{\in}\mathcal{A}^*.\big(P(v) \Rightarrow \forall a{\in}\mathcal{A} \ . \ P(va)\big) \Big) \end{array}\right\} \Rightarrow \big(\forall w{\in}\mathcal{A}^*.P(w) \big)$$

Ebenso wird häufig das Prinzip der Induktion über die Wortlänge verwendet; es unterscheidet sich dann nicht von der natürlichen Induktion.

2.1.5 Definition (Ordnungen auf Wörtern)
Sei $\mathcal{A}$ ein Alphabet. Sei $R : \mathcal{A} \times \mathcal{A}$ eine beliebige homogene Relation.

1. Die *lexikographische Ordnung* $\ll_R : \mathcal{A}^* \times \mathcal{A}^*$ ist definiert durch:

$$\begin{array}{lcl} \lambda \ll_R w & \Leftrightarrow & w \in \mathcal{A}^* \\ w \ll_R \lambda & \Leftrightarrow & w = \lambda \\ av \ll_R bw & \Leftrightarrow & a, b \in \mathcal{A} \wedge v, w \in \mathcal{A}^* \wedge \begin{cases} a \; R \; b & \text{falls } a \neq b \\ v \ll_R w & \text{falls } a = b \end{cases} \end{array}$$

2. Die *Standardordnung* $\ll_R^{\mathrm{S}} : \mathcal{A}^* \times \mathcal{A}^*$ ist definiert durch:

$$v \ll_R^{\mathrm{S}} w \quad \Leftrightarrow \quad \big(\; |v|<|w| \; \vee \; (\; |v|=|w| \; \wedge \; v \ll_R w \;) \; \big)$$

2.1.6 Proposition Sei $\mathcal{A}$ ein Alphabet.
Sei $R : \mathcal{A} \times \mathcal{A}$ eine beliebige homogene Relation. Wenn R eine totale Ordnung ist, dann sind auch $\ll_R$ und $\ll_R^{\mathrm{S}}$ totale Ordnungen.

2.1.7 Definition (Sprachen)
Sei $\mathcal{A}$ ein Alphabet.
Dann heißt jede Teilmenge $A \subseteq \mathcal{A}^*$ *Sprache über* $\mathcal{A}$.

2.1.8 Definition (Konkatenation von Sprachen)
Seien A und B Sprachen über dem Alphabet $\mathcal{A}$.
Die Konkatenation $A \cdot B$ (oder kurz: AB) ist definiert durch:

$$A \cdot B \triangleq \{ \, w \in \mathcal{A}^* \mid \exists w_1 \in A, w_2 \in B \, . \, w = w_1 \cdot w_2 \, \}$$

Die *n-fache Konkatenation* ist definiert durch:

$$\begin{array}{rclcrcl} A^0 & \triangleq & \{ \, \lambda \, \} & \qquad & A^* & \triangleq & \bigcup_{n \geq 0} A^n \\ A^{n+1} & \triangleq & A \cdot A^n & & A^+ & \triangleq & \bigcup_{n \geq 1} A^n \end{array}$$

2.1.9 Definition (Reguläre Ausdrücke)
Sei $\mathcal{A}$ ein Alphabet mit $\mathcal{A} \cap \{\mathbf{0}, \boldsymbol{\epsilon}\} = \emptyset$.
Die Sprache $\mathcal{E}^{\mathcal{A}}$ der *regulären Ausdrücke über* $\mathcal{A}$
ist als kleinste Menge definiert,
die die folgenden $\in$-Regeln erfüllt:

1. $\mathbf{0} \in \mathcal{E}^{\mathcal{A}}$, $\boldsymbol{\epsilon} \in \mathcal{E}^{\mathcal{A}}$, $a \in \mathcal{E}^{\mathcal{A}}$ für alle $a \in \mathcal{A}$
2. falls $e \in \mathcal{E}^{\mathcal{A}}$, dann auch $e^* \in \mathcal{E}^{\mathcal{A}}$
3. falls $e_1 \in \mathcal{E}^{\mathcal{A}}$ und $e_2 \in \mathcal{E}^{\mathcal{A}}$, dann auch $e_1 \cdot e_2 \in \mathcal{E}^{\mathcal{A}}$
4. falls $e_1 \in \mathcal{E}^{\mathcal{A}}$ und $e_2 \in \mathcal{E}^{\mathcal{A}}$, dann auch $e_1 + e_2 \in \mathcal{E}^{\mathcal{A}}$

Der Ausdruck $e_1 \cdot e_2$ wird oft durch $e_1 e_2$ abgekürzt.
Es gilt: * hat Vorrang vor $\cdot$ hat Vorrang vor $+$.

2.1.10 Definition (Sprache regulärer Ausdrücke)
Sei $\mathcal{A}$ ein Alphabet mit $\mathcal{A} \cap \{\mathbf{0}, \boldsymbol{\epsilon}\} = \emptyset$.
Die Abbildung $\mathrm{L} : \mathcal{E}^{\mathcal{A}} \to \mathcal{P}(\mathcal{A}^*)$ gegeben durch:

$$\begin{array}{lcll} \mathbf{0} & \mapsto & \emptyset & \\ \boldsymbol{\epsilon} & \mapsto & \{\lambda\} & \\ a & \mapsto & \{a\} & \text{für alle } a \in \mathcal{A} \\ e^* & \mapsto & \mathrm{L}(e)^* & \\ e_1 \cdot e_2 & \mapsto & \mathrm{L}(e_1) \cdot \mathrm{L}(e_2) & \\ e_1 + e_2 & \mapsto & \mathrm{L}(e_1) \cup \mathrm{L}(e_2) & \end{array}$$

definiert die zugehörige Sprache eines regulären Ausdrucks.

2.2 Monoide, Gruppen, Ringe, Halbverbände

2.2.1 Definition (Halbgruppe)
Sei X eine nichtleere Menge.
Sei $\circ : X \times X \to X$ eine so genannte *Verknüpfung[soperation]*.
Dann heißt $(X, \circ)$ *Halbgruppe*, falls mit

$$\forall x, y, z \in X \ . \ x \circ (y \circ z) = (x \circ y) \circ z \qquad \text{(ASSO)}$$

für $\circ$ das *Assoziativitäts-Gesetz* gilt.
$(X, \circ)$ heißt *kommutativ* bzw. *abelsch*, wenn darüberhinaus mit

$$\forall x, y \in X \ . \ x \circ y = y \circ x \qquad \text{(COMM)}$$

für $\circ$ das *Kommutativitäts-Gesetz* gilt.

2.2.2 Notation Das Symbol $\circ$ dient nur als Platzhalter. In konkreten Algebren verwenden wir auch andere Symbole wie $+$, $\sqcap$, etc.

2.2.3 Definition (Idempotenz)
Sei $(X, \circ)$ eine Halbgruppe.
Ein Element $x \in X$ heißt *idempotent*, wenn $x \circ x = x$.

2.2.4 Definition (Neutrales Element)
Sei $(X, \circ)$ eine Halbgruppe.
Ein Element $e_{\mathrm{l}} \in X$ heißt *linksneutral* (bzgl. $(X, \circ)$), wenn gilt:

$$\forall x \in X \ . \ e_{\mathrm{l}} \circ x = x \qquad \text{(NEUT-L)}$$

Ein Element $e_{\mathrm{r}} \in X$ heißt *rechtsneutral* (bzgl. $(X, \circ)$), wenn gilt:

$$\forall x \in X \ . \ x \circ e_{\mathrm{r}} = x \qquad \text{(NEUT-R)}$$

Ein Element $e \in X$ heißt *neutral* (bzgl. $(X, \circ)$),
wenn es sowohl links- als auch rechtsneutral (bzgl. $(X, \circ)$) ist.

2.2.5 Definition (Monoid)
Sei $(X, \circ)$ eine Halbgruppe.
Sei $e \in X$ neutral (bzgl. $(X, \circ)$).
Dann heißt $(X, \circ, e)$ *Monoid*.
$(X, \circ, e)$ heißt *kommutatives Monoid*, wenn darüberhinaus (COMM) gilt.

2.2.6 Definition (Inverses Element)
Sei $(X, \circ, e)$ ein Monoid.
Ein Element $x_{\mathrm{l}} \in X$ heißt *linksinvers zu* x (bzgl. $(X, \circ, e)$), wenn gilt:

$$x_{\mathrm{l}} \circ x = e \qquad \text{(INV-L)}$$

Ein Element $x_{\mathrm{r}} \in X$ heißt *rechtsinvers* (bzgl. $(X, \circ, e)$), wenn gilt:

$$x \circ x_{\mathrm{r}} = e \qquad \text{(INV-R)}$$

Ein Element $x^{-1} \in X$ heißt *invers zu* x (bzgl. $(X, \circ, e)$),
wenn es sowohl links- als auch rechtsinvers (bzgl. $(X, \circ, e)$) ist.

2.2.7 Definition (Gruppe)
Sei $(X, \circ, e)$ ein Monoid.
Sei $^{-1} : X \to X$ eine Operation mit x^{-1} invers zu x (bzgl. $(X, \circ, e)$).

1. Dann heißt $(X, \circ, e, ^{-1})$ *Gruppe*.
2. Ist $(X, \circ, e)$ ein kommutatives Monoid,
   dann heißt $(X, \circ, e, ^{-1})$ *kommutative Gruppe* bzw. *abelsche Gruppe*.

2.2.8 Definition (Ring)
Sei $(X, +, 0, ^{-1})$ eine kommutative Gruppe.
Sei $(X, *)$ eine Halbgruppe.

1. Dann heißt $(X, +, *, 0, ^{-1})$ *Ring*, wenn mit

$$\forall x, y, z \in X \ . \ x * (y + z) = x * y + x * z \qquad \text{(DIST-L)}$$

$$\forall x, y, z \in X \ . \ (y + z) * x = y * x + z * x \qquad \text{(DIST-R)}$$

   die *Distributivitäts-Gesetze für* $+$ *und* $*$ gelten.

2. Ist $(X, +, *, 0, ^{-1})$ ein Ring und
   ist $(X, *)$ eine kommutative Halbgruppe,
   so heißt $(X, +, *, 0, ^{-1})$ *kommutativer Ring*.

3. Ist $(X, +, *, 0, ^{-1})$ ein Ring und
   ist $(X, *, 1)$ ein Monoid,
   so heißt $(X, +, *, 0, 1, ^{-1})$ *Ring mit Eins* bzw. *unitärer Ring*.

2.2.9 Notation In Def 2.2.8 verwenden wir die Operatorensymbole $+$ und $*$, um an die Intuition der Standardbeispiele aus der Zahlentheorie zu erinnern. Je nach Kontext verwenden wir jedoch auch andere Symbole.

2.2.10 Notation Häufig lassen wir in der Tupel-Bezeichnung von Halbgruppen, Monoiden, Gruppen und Ringen die konkreten Symbole für neutrale und inverse Elemente weg und listen nur die (zweistelligen) Verknüpfungsoperationen, z.B., Gruppe $(X, \circ)$ oder Ring $(X, +, *)$ auf.

2.2.11 Definition (Halbverband)
Eine kommutative Halbgruppe $(X, \circ)$, in der mit

$$\forall x \in X \ . \ x \circ x = x \qquad \text{(IDEM)}$$

das *Idempotenz-Gesetz* gilt, heißt *Halbverband*.

2.2.12 Lemma
Sei $(X, \circ)$ ein Halbverband.
Sei $\leq_\circ : X \times X$ definiert durch:

$$x \leq_\circ y \iff x \circ y = x$$

Dann ist $\leq_\circ : X \times X$ eine Halbordnung.

2.3 Extremwerte, Schranken, Verbände

2.3.1 Definition (Extremwerte)
Sei $\leq : X \times X$ eine Halbordnung. Sei $A \subseteq X$.

1. $k \in A$ heißt *kleinstes Element von* A, falls gilt:

$$\forall a \in A \ . \ k \leq a$$

$m \in A$ heißt *minimales Element in* A, falls gilt:

$$\forall a \in A \ . \ \big(a \leq m \Rightarrow a = m\big)$$

2. $g \in A$ heißt *größtes Element von* A, falls gilt:

$$\forall a \in A \ . \ a \leq g$$

$m \in A$ heißt *maximales Element in* A, falls gilt:

$$\forall a \in A \ . \ \big(m \leq a \Rightarrow a = m\big)$$

2.3.2 Bemerkung Bezüglich einer Halbordnung $\leq : X \times X$ existieren die genannten Extremwerte nicht notwendigerweise für jede Teilmenge $A \subseteq X$.
Kleinste und größte Elemente sind eindeutig, wenn sie existieren.
Minimale und maximale Elemente müssen nicht eindeutig bestimmt sein.

2.3.3 Definition (Schranken)
Sei $\leq : X \times X$ eine Halbordnung. Sei $A \subseteq X$.

1. $u \in X$ heißt *untere Schranke* von A (bzgl. X), falls gilt:

$$\forall a \in A \ . \ u \leq a$$

Eine *größte untere Schranke von A (bzgl. X)*
— auch als *Infimum von A (bzgl. X)* bezeichnet, kurz: $\inf^X(A)$ —
ist definiert als ein größtes Element
in der Menge der unteren Schranken von A (bzgl. X).

2. $o \in X$ heißt *obere Schranke* von A (bzgl. X), falls gilt:

$$\forall a \in A \ . \ a \leq o$$

Eine *kleinste obere Schranke von A (bzgl. X)*
— auch als *Supremum von A (bzgl. X)* bezeichnet, kurz: $\sup^X(A)$ —
ist definiert als ein kleinstes Element
in der Menge der oberen Schranken von A (bzgl. X).

2.3.4 Bemerkung Schranken werden aus X gewählt. Somit liegen sie nicht notwendigerweise innerhalb der Menge A, die sie beschränken.

2.3.5 Definition
Sei $\leq : X \times X$ eine Halbordnung. Sei $A \subseteq X$.

1. Ist $m = \inf^X(A) \in A$,
   so heißt m *Minimum von* A,
   bezeichnet mit $\mathrm{Min}_{\leq}(A)$. kurz $\mathrm{Min}(A)$.

2. Ist $m = \sup^X(A) \in A$,
   so heißt m *Maximum von* A,
   bezeichnet mit $\mathrm{Max}_{\leq}(A)$, kurz $\mathrm{Max}(A)$.

2.3.6 Definition (Verband)
Seien $(X, \sqcap)$ und $(X, \sqcup)$ zwei Halbverbände.

1. Dann heißt $(X, \sqcap, \sqcup)$ *Verband*, wenn mit

   $$\forall x, y \in X \ . \ x \sqcup (x \sqcap y) = x \qquad \text{(ABS-1)}$$
   $$\forall x, y \in X \ . \ x \sqcap (x \sqcup y) = x \qquad \text{(ABS-2)}$$

   die *Verschmelzungs-* bzw. *Absorptions-Gesetze* gelten.

   Die Halbordnungen $\leq_{\sqcap}$ und $\leq_{\sqcup}^{-1}$ gemäß Lemma 2.2.12
   sind dann identisch, so dass wir vereinfacht $\leq$ schreiben.

2. Existieren zudem, bezüglich $\leq$,
   $\inf^X(A) \in X$ und $\sup^X(A) \in X$ für beliebige $A \subseteq X$,
   so heißt $(X, \sqcap, \sqcup)$ *vollständiger Verband*.
   Für $\bot \triangleq \inf^X(X)$ und $\top \triangleq \sup^X(X)$ und beliebigem $x \in X$ gelten:

   $$x \sqcap \bot = \bot \qquad x \sqcap \top = x$$
   $$x \sqcup \top = \top \qquad x \sqcup \bot = x$$

3. Ein vollständiger Verband $(X, \sqcap, \sqcup)$ heißt *komplementär*,
   wenn es zu jedem Element x ein Inverses x^{-1} (bzgl. $\sqcap$ und $\sqcup$) gibt:

   $$x \sqcap x^{-1} = \bot \qquad x \sqcup x^{-1} = \top$$

4. Ein Verband $(X, \sqcap, \sqcup)$ heißt *distributiv*, wenn
   die Gesetze (DIST-L) und (DIST-R) für $\sqcup$ und $\sqcap$ gelten.

5. Ein vollständiger, komplementärer, distributiver Verband
   heißt auch *boolescher Verband* oder *boolesche Algebra*.

2.3.7 Proposition
Sei $\leq : X \times X$ eine totale Ordnung.
Sei $\min, \max : X \times X \to X$ definiert durch:
$\min(x, y) \in \{ x, y \} \wedge \min(x, y) \leq x \wedge \min(x, y) \leq y$ und
$\max(x, y) \in \{ x, y \} \wedge x \leq \max(x, y) \wedge y \leq \max(x, y)$.
Dann ist $(X, \min, \max)$ ein distributiver Verband.

2.3.8 Proposition
Sei M eine Menge.
Dann ist $(\mathcal{P}(M), \cap, \cup)$ ein boolescher Verband,
genannt *Potenzmengenverband*.

3 Algebraische Strukturen – Informatisch

3.1 Σ-Algebren

3.1.1 Definition (Algebraische Signatur)
Eine *[algebraische] Signatur* $\Sigma = (S, O, \mathrm{ar})$ besteht aus

- einer Menge $S = \{s_1, \ldots, s_n\}$ von *Sortenbezeichnern*,
- einer Menge $O = \{f_1, \ldots, f_m\}$ von *Operatorbezeichnern*, und
- einer Abbildung $\mathrm{ar} : O \to S^*$, genannt *Stelligkeit*, mit $|\mathrm{ar}(f)| > 0$ für alle $f \in O$.

Wir beschränken uns auf endliche Mengen S und O mit $S \neq \emptyset$.
Ein Operatorbezeichner f mit $\mathrm{ar}(f) = (s_1, \ldots, s_n, s)$ heißt n-stellig.
Ein 0-stelliger Operatorbezeichner c heißt *Konstante[nbezeichner]*.

3.1.2 Notation Sei $\Sigma = (S, O, \mathrm{ar})$ mit $f \in O$.
Wir schreiben kurz $f : w$, falls $\mathrm{ar}(f) = w$.
Man schreibt auch $f : s_1 \times \ldots \times s_n \to s$, falls $\mathrm{ar}(f) = (s_1, \ldots, s_n, s)$.
Gelegentlich schreibt man $f : w \to s$, falls $\mathrm{ar}(f) = w \cdot (s)$.
Wir schreiben $O_s \triangleq \{\, f \in O \mid \mathrm{ar}(f) = (s) \,\}$.
Wir schreiben $O_{w \to s} \triangleq \{\, f \in O \mid \mathrm{ar}(f) = w \cdot (s) \text{ und } |w| > 0 \,\}$.

3.1.3 Definition (Σ-Algebra)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Eine Σ-Algebra $A \triangleq \big((A_s)_{s \in S}, (f_A)_{f \in O} \big)$ besteht aus

1. *Trägermengen* A_s für alle $s \in S$,
2. (a) *Konstanten* $f_A \in A_s$ für alle $f \in O_s$ und
   (b) *Abbildungen* $f_A : A_{s_1} \times \ldots \times A_{s_n} \to A_s$ für alle $f \in O_{(s_1, \ldots, s_n) \to s}$.

3.1.4 Definition (Unteralgebra)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur. Seien A und A' beide Σ-Algebren.
A heißt *Unteralgebra* von A', geschrieben $A \subseteq A'$, falls:

- $A_s \subseteq A'_s$ für alle $s \in S$;
- $f_A \subseteq f_{A'}$ für alle $f \in O$.

A ist *echte Unteralgebra* von A', geschr. $A \subset A'$, falls $A \subseteq A'$ und $A \neq A'$.

3.1.5 Definition (Untersignatur)
Seien $\Sigma = (S, O, \mathrm{ar})$ und $\Sigma' = (S', O', \mathrm{ar}')$ Signaturen.
Σ heißt *Untersignatur von* Σ', geschrieben $\Sigma \subseteq \Sigma'$, wenn gilt:

- $S \subseteq S'$ und $O \subseteq O'$
- $\mathrm{ar} \subseteq \mathrm{ar}'$ (d.h., $\forall f \in O \,.\, \mathrm{ar}(f) = \mathrm{ar}'(f)$) (auch: $\mathrm{ar} = \mathrm{ar}' \restriction_O$)

Σ ist *echte Untersignatur von* Σ', geschr. $\Sigma \subset \Sigma'$, wenn $\Sigma \subseteq \Sigma'$ und $\Sigma \neq \Sigma'$.

3.1.6 Definition (Redukt)
Seien $\Sigma = (S, O, \mathrm{ar})$ und $\Sigma' = (S', O', \mathrm{ar}')$ Signaturen mit $\Sigma \subseteq \Sigma'$.
$A = A' \restriction_\Sigma$ heißt Σ-Redukt der Σ'-Algebra A', falls gilt:

- A ist Σ-Algebra;
- $A_s = A'_s$ für alle $s \in S$;
- $f_A = f_{A'}$ für alle $f \in O$.

3.2 Grundterme, strukturelle Induktion

3.2.1 Definition (Grundterme und Grundtermalgebra)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Die Familie $(T_{\Sigma,s})_{s\in S}$ der *Grundterme zur Signatur* Σ ist definiert durch:

$$\begin{array}{rcl} T_{\Sigma,s} & \triangleq & O_s \\ & \cup & \{f(t_1,\ldots,t_n) \mid f \in O_{(s_1,\ldots,s_n)\to s} \ \wedge\ \forall i \in [1,n]\,.\, t_i \in T_{\Sigma,s_i}\} \end{array}$$

Für $w = (s_1,\ldots,s_n)$ und $n > 0$ definieren wir $T_{\Sigma,w} \triangleq T_{\Sigma,s_1} \times \ldots \times T_{\Sigma,s_n}$.
Wir definieren *Termkonstruktoren* bzw. *Termformer* durch:

$$\begin{array}{lll} c_{T_\Sigma} : T_{\Sigma,s} & \text{für } c \in O_s & \text{durch } \ c_{T_\Sigma} \triangleq c \\ f_{T_\Sigma} : T_{\Sigma,w} \to T_{\Sigma,s} & \text{für } f \in O_{(s_1,\ldots,s_n)\to s} & \text{durch } \ f_{T_\Sigma}(t_1,\ldots,t_n) \triangleq f(t_1,\ldots,t_n) \\ & & \text{für beliebige } (t_1,\ldots,t_n) \in T_{\Sigma,w} \end{array}$$

$T_\Sigma \triangleq (\ (T_{\Sigma,s})_{s\in S}, (f_{T_\Sigma})_{f\in O})$ heißt *Grundtermalgebra*
(bzw. *Syntaktische Algebra*) zur Signatur Σ.

3.2.2 Lemma (Dekomposition)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur. Sei $t \in T_{\Sigma,s}$ für $s \in S$.
Dann gilt genau einer der beiden folgenden Fälle für t:

1. $t = c$ für $c \in O_s$
2. $t = f(t_1,\ldots,t_n)$ für $f \in O_{(s_1,\ldots,s_n)\to s}$ und $\forall i \in [1,n]\,.\, t_i \in T_{\Sigma,s_i}$

Wegen dieses Lemmas ist es (per Definition) möglich, Aussagen über Grundterme via „Pattern-Matching“ zu analysieren, z.B., per Induktion.

3.2.3 Proposition (Strukturelle Induktion)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei $P(t)$ ein Prädikat über Grundtermen aus $(T_{\Sigma,s})_{s\in S}$.
Falls für alle $s \in S$

1. „für alle $c \in O_s$ gilt $P(c)$“, und
2. „für alle $f \in O_{(s_1,\ldots,s_n)\to s}$ gilt

$$\big(\ \forall i{\in}[1,n]\,.\, P(t_i)\ \big) \Rightarrow P\big(\ f(t_1,\ldots,t_n)\ \big)$$

für alle $t_1{\in}T_{\Sigma,s_1},\ldots,t_n{\in}T_{\Sigma,s_n}$“

beide gelten (bzw. bewiesen werden können), dann gilt auch:

$$\forall s \in S\,.\,\forall t \in T_{\Sigma,s}\,.\, P(t)$$

3.2.4 Definition (Auswertung)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur. Sei A eine Σ-Algebra.
Sei $s \in S$. Wir definieren $\mathrm{eval}^A_s : T_{\Sigma,s} \to A_s$ durch:

$$\begin{array}{rcll} \mathrm{eval}^A_s(c) & \triangleq & c_A & \text{falls } c \in O_s \\ \mathrm{eval}^A_s\big(f(t_1,\ldots,t_n)\big) & \triangleq & f_A\big(\mathrm{eval}^A_{s_1}(t_1),\ldots,\mathrm{eval}^A_{s_n}(t_n)\big) & \text{falls } f \in O_{(s_1,\ldots,s_n)\to s} \end{array}$$

Die Abbildungsfamilie $\mathrm{eval}^A \triangleq \big(\ \mathrm{eval}^A_s : T_{\Sigma,s} \to A_s\ \big)_{s\in S}$
heißt *Auswertung der Grundterme in* A.
Wir erlauben dazu auch die Notation $\mathrm{eval}^A : T_\Sigma \to A$.

3.3 Variablen, Terme, Gleichungen

3.3.1 Definition (Signatur mit Variablen)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei $X = (X_s)_{s \in S}$ eine S-indizierte Familie von Mengen,
deren Elemente wir *Variablen* nennen.
Gilt $X_s \cap O = \emptyset$ für alle $s \in S$,
sowie $X_{s_1} \cap X_{s_2} = \emptyset$ für alle $s_1, s_2 \in S$ mit $s_1 \neq s_2$,
so heißt X *Variablensystem [zur Signatur Σ]*.
Das Quadrupel (S, O, ar, X) heißt dann *Signatur mit Variablensystem*,
oder kurz: *Signatur mit Variablen*.

3.3.2 Notation Wir verwenden das Symbol Σ der Einfachheit halber sowohl für Signaturen mit als auch ohne Variablen. Im letzteren Fall bezieht sich der Begriff Σ-Algebra dann auf die ersten drei Komponenten.

3.3.3 Definition (Terme und Termalgebra)
Sei $\Sigma = (S, O, \mathrm{ar}, X)$ eine Signatur mit Variablen.
Die Familie $(T^X_{\Sigma,s})_{s \in S}$ der *[allgemeinen] Σ-Terme* ist definiert durch:

$$\begin{array}{rcl} T^X_{\Sigma,s} & \triangleq & X_s \\ & \cup & O_s \\ & \cup & \{\ f(t_1, \ldots, t_n) \mid f \in O_{(s_1,\ldots,s_n)\to s} \ \wedge\ \forall i \in [1,n]\,.\, t_i \in T^X_{\Sigma,s_i}\ \} \end{array}$$

Für $w = (s_1, \ldots, s_n)$ und $n > 0$ definieren wir $T^X_{\Sigma,w} \triangleq T^X_{\Sigma,s_1} \times \ldots \times T^X_{\Sigma,s_n}$.
Wir definieren *Termkonstruktoren* durch:

$$\begin{array}{lll} c_{T^X_\Sigma} : T^X_{\Sigma,s} & \text{für } c \in O_s & \text{durch} \quad c_{T^X_\Sigma} \triangleq c \\ f_{T^X_\Sigma} : T^X_{\Sigma,w} \to T^X_{\Sigma,s} & \text{für } f \in O_{(s_1,\ldots,s_n)\to s} & \text{durch} \quad f_{T^X_\Sigma}(t_1, \ldots, t_n) \triangleq f(t_1, \ldots, t_n) \\ & & \text{für beliebige } (t_1, \ldots, t_n) \in T^X_{\Sigma,w} \end{array}$$

$T^X_\Sigma \triangleq (\ (T^X_{\Sigma,s})_{s \in S}, (f_{T^X_\Sigma})_{f \in O})$ heißt *Termalgebra* zur Signatur Σ.

3.3.4 Proposition (Strukturelle Induktion)
Sei $\Sigma = (S, O, \mathrm{ar}, X)$ eine Signatur mit Variablen.
Sei $P(t)$ ein Prädikat über Termen aus $(T^X_{\Sigma,s})_{s \in S}$.
Falls für alle $s \in S$

1. „für alle $x \in X_s$ gilt $P(x)$“, und
2. „für alle $c \in O_s$ gilt $P(c)$“, und
3. „für alle $f \in O_{(s_1,\ldots,s_n)\to s}$ gilt

$$\big(\ \forall i \in [1,n]\,.\, P(t_i)\ \big) \Rightarrow P\big(\ f(t_1, \ldots, t_n)\ \big)$$

für alle $t_1 \in T^X_{\Sigma,s_1}, \ldots, t_n \in T^X_{\Sigma,s_n}$“

gelten (bzw. bewiesen werden können), dann gilt auch:

$$\forall s \in S\,.\, \forall t \in T^X_{\Sigma,s}\,.\, P(t)$$

3.3.5 Definition (Variablenbelegung)
Sei $\Sigma = (S, O, \mathrm{ar}, X)$ eine Signatur mit Variablen.
Sei A eine Σ-Algebra.
Eine S-indizierte Familie $\alpha = \big(\ \alpha_s : X_s \to A_s\ \big)_{s \in S}$ von Abbildungen, die jeder Variablen ein Element der Trägermenge derselben Sorte zuordnet, heißt *Variablenbelegung* bzw. *Variablenassignment*.
Wir erlauben dazu auch die Notation $\alpha : X \to A$.

3.3.6 Definition (Erweiterte Auswertung)
Sei $\Sigma = (S, O, \mathrm{ar}, X)$ eine Signatur mit Variablen.
Sei A eine Σ-Algebra.
Sei $\alpha : X \to A$ eine Variablenbelegung.
Die Abbildungsfamilie

$$\big(\ \mathrm{xeval}_s^{\alpha,A} : T_{\Sigma,s}^X \to A_s\ \big)_{s \in S}$$

mit

$$\begin{aligned}
\mathrm{xeval}_s^{\alpha,A}(x) &\triangleq \alpha_s(x) && \text{für alle } x \in X_s \\
\mathrm{xeval}_s^{\alpha,A}(c) &\triangleq c_A && \text{für alle } c \in O_s \\
\mathrm{xeval}_s^{\alpha,A}\big(f(t_1,\ldots,t_n)\big) &\triangleq f_A\big(\mathrm{xeval}_{s_1}^{\alpha,A}(t_1),\ldots,\mathrm{xeval}_{s_n}^{\alpha,A}(t_n)\big) \\
& && \text{für alle } f \in O_{(s_1,\ldots,s_n)\to s} \\
& && \text{und } t_i \in T_{\Sigma,s_i}^X \text{ für alle } i \in [1,n].
\end{aligned}$$

heißt *Auswertung* der Terme in A.
Wir erlauben dazu auch die Notation $\mathrm{xeval}^{\alpha,A} : T_\Sigma^X \to A$.

3.3.7 Definition (Gleichungen)
Sei $\Sigma = (S, O, \mathrm{ar}, X)$ eine Signatur mit Variablen.
Seien $t_\mathrm{l}, t_\mathrm{r} \in T_{\Sigma,s}^X$ beliebige Terme der gleichen Sorte $s \in S$.
Dann heißt

$$e \quad \triangleq \quad \big(\ t_\mathrm{l} =_s t_\mathrm{r}\ \big)$$

Gleichung [der Sorte s] zur Signatur Σ oder auch Σ*-Gleichung*.
Gelegentlich schreiben wir kurz $=$ anstelle von $=_s$.
Falls weder t_l noch t_r Variablen enthalten, heißt e *Grundgleichung*.

3.3.8 Definition (Gültigkeit)
Sei $\Sigma = (S, O, \mathrm{ar}, X)$ eine Signatur mit Variablen.
Sei $e \triangleq (t_\mathrm{l} =_s t_\mathrm{r})$ eine Σ-Gleichung.
Sei A eine Σ-Algebra.
Dann heißt e *gültig in* A, geschrieben $A \models e$,
falls für alle Variablenbelegungen $\alpha : X \to A$ gilt:

$$\mathrm{xeval}_s^{\alpha,A}(t_\mathrm{l}) = \mathrm{xeval}_s^{\alpha,A}(t_\mathrm{r})$$

Andernfalls schreiben wir $A \not\models e$.

3.3.9 Definition (Algebraische Spezifikation)
Sei $\Sigma = (S, O, \mathrm{ar}, X)$ eine Signatur mit Variablen.
Sei E eine Menge von Σ-Gleichungen.
Dann heißt $(S, O, \mathrm{ar}, X, E)$ *Algebraische Spezifikation*.

3.4 Überladen von Operationsbezeichnern

[EMC+01] erlaubt Signaturen das Überladen von Operationsbezeichnern, solange deren Stelligkeit verschieden ist. Zur formalen Beschreibung werden dabei Mengenfamilien $(OP_{w,s})_{w\in S^*,s\in S}$ verwendet, deren Index bereits die Stelligkeit beinhaltet, so dass die Stelligkeitsfunktion ar entfällt. (Die Definitionen weiterführender Konzepte zu signaturbasierten Algebren müssen dann natürlich dementsprechend angepasst werden.)

3.4.1 Definition Eine *algebraische Signatur* $\Sigma = (S, OP)$ besteht aus

- einer Menge $S = \{s_1, \ldots, s_n\}$ von *Sorten*, und
- einer Familie $OP = (OP_{w,s})_{w\in S^*,s\in S}$ von *Operationssymbolmengen*.

Ein Operationssymbol $f \in OP_{s_1\cdots s_n,s}$ heißt n-stellig.
Ein 0-stelliges Operationssymbol $c \in OP_{\lambda,s}$ heißt *Konstante[nsymbol]*.

3.4.2 Bemerkung Besteht die Familie $(OP_{w,s})_{w\in S^*,s\in S}$ aus paarweise disjunkten Mengen, liegt also kein Überladen der Bezeichner vor, so gilt (S, O, ar) mit

$$\begin{array}{rcll} O & \triangleq & \{\, f \mid \exists w \in S^* \,.\, \exists s \in S \,.\, f \in OP_{w,s} \,\} & \\ \mathrm{ar}(f) & \triangleq & w \cdot (s) & \text{für } f \in OP_{w,s} \text{ mit } w \in S^*, s \in S \end{array}$$

als entsprechende Signatur in bisheriger Terminologie.

3.5 Homomorphismen

3.5.1 Definition (Homomorphismen)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Seien A, B zwei Σ-Algebren.
Ein Σ-*Homomorphismus* $h : A \to B$ ist
eine Familie von Abbildungen $(h_s : A_s \to B_s)_{s\in S}$, so dass

- für alle $c \in O_s$ gilt $h_s(c_A) = c_B$, und
- für alle $f \in O_{(s_1,\ldots,s_n)\to s}$ gilt für alle $i \in [1, n]$ und für alle $a_i \in A_{s_i}$:

$$h_s(f_A(a_1, \ldots, a_n)) = f_B(h_{s_1}(a_1), \ldots, h_{s_n}(a_n))$$

Homomorphismen heißen *injektiv/surjektiv/bijektiv*,
wenn dies jeweils für alle Teilabbildungen h_s für $s \in S$ gilt.
$\mathrm{id}_A : A \to A$ heißt *Identität*, falls $\forall s \in S \,.\, \forall a \in A_s \,.(\mathrm{id}_A)_s(a) = a$.

3.5.2 Definition (Komposition)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Seien A, B, C drei Σ-Algebren.
Seien $h : A \to B$ und $g : B \to C$ zwei Σ-Homomorphismen.
Dann ist die Komposition, geschrieben $g \circ h : A \to C$, definiert durch:

$$\forall s \in S \;.\; (g \circ h)_s \triangleq g_s \circ h_s$$

($g \circ h$ ist dann ebenfalls ein Σ-Homomorphismus.)

3.5.3 Definition (Isomorphismus)
Ein Σ-Homomorphismus $h : A \to B$ heißt *Isomorphismus*,
falls es einen Σ-Homomorphismus $h^{-1} : B \to A$ gibt, so dass:

$$h^{-1} \circ h = \mathrm{id}_A \qquad \text{und} \qquad h \circ h^{-1} = \mathrm{id}_B$$

3.5.4 Definition (Bildalgebra)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei $h : A \to B$ ein Σ-Homomorphismus.
Die Bildalgebra $h(A)$ ist die Unteralgebra von B, definiert durch:

1. $h(A)_s \triangleq h_s(A_s)$ für alle $s \in S$;
2. $f_{h(A)} \triangleq f_B$ für alle $f \in O_s$;
3. $f_{h(A)} \triangleq f_B \restriction_{h(A)_{s_1} \times \cdots \times h(A)_{s_n}}$ für alle $f \in O_{(s_1,\ldots,s_n)\to s}$.

3.5.5 Theorem (Abbildungssatz)
Sei $f : A \to B$ ein beliebiger Σ-Homomorphismus. Dann existieren

- eine Σ-Algebra C (eindeutig bestimmt „bis auf Isomorphie“),
- ein surjektiver Σ-Homomorphismus $g : A \to C$,
- ein injektiver Σ-Homomorphismus $h : C \to B$,

so dass $f = h \circ g$. (Die Zerlegung ist bis auf Isomorphie eindeutig.)

3.5.6 Proposition (Homomorphismen bewahren Grundterme)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei $h : A \to B$ ein Σ-Homomorphismus.
Dann gilt: $\forall s \in S \,.\, \forall t \in T_{\Sigma,s} \,.\, h_s\big(\mathrm{eval}^A_s(t)\big) = \mathrm{eval}^B_s(t)$

3.5.7 Proposition (Homomorphismen bewahren Grundgleichungen)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei $h : A \to B$ ein Σ-Homomorphismus.
Sei e eine Σ-Grundgleichung.
Dann gilt: wenn $A \models e$, dann auch $B \models e$.

3.5.8 Definition (Initiale und finale Algebra)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei $\mathrm{Xlg}(\Sigma)$ eine Menge von Σ-Algebren.

1. Eine Algebra $I \in \mathrm{Xlg}(\Sigma)$ heisst *initial* in $\mathrm{Xlg}(\Sigma)$,
   falls für alle Algebren $A \in \mathrm{Xlg}(\Sigma)$
   genau ein Homomorphismus $i : I \to A$ existiert,
   genannt *initialer Homomorphismus*.

2. Eine Algebra $F \in \mathrm{Xlg}(\Sigma)$ heisst *final* in $\mathrm{Xlg}(\Sigma)$,
   falls für alle Algebren $A \in \mathrm{Xlg}(\Sigma)$
   genau ein Homomorphismus $f : A \to F$ existiert,
   genannt *finaler Homomorphismus*.

3.5.9 Lemma
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei $\mathrm{Xlg}(\Sigma)$ eine Menge von Σ-Algebren.
Seien A und B initial (bzw. final) in $\mathrm{Xlg}(\Sigma)$.
Dann existiert ein Isomorphismus $h : A \to B$.

3.5.10 Theorem (Initialität)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei $\mathrm{Alg}(\Sigma)$ die Menge aller Σ-Algebren.
Dann gilt: die Grundtermalgebra T_Σ ist initial in $\mathrm{Alg}(\Sigma)$.

3.6 Kongruenzen

3.6.1 Definition (Kongruenz)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei A eine Σ-Algebra.
Sei $K = (K_s)_{s \in S}$ mit $K_s : A_s \times A_s$
eine Familie von Äquivalenzrelationen.
K heißt *Kongruenz[relation]*, falls
für alle $f \in O_{(s_1,\ldots,s_n)\to s}$ und
für alle $a_i, b_i \in A_{s_i}$ mit $i \in [1, n]$ gilt:

$$(a_1, b_1) \in K_{s_1} \ \wedge \ \ldots \ \wedge \ (a_n, b_n) \in K_{s_n}$$
$$\Longrightarrow \big(\ f_A(a_1, \ldots, a_n) \ , \ f_A(b_1, \ldots, b_n) \ \big) \in K_s$$

3.6.2 Bemerkung
Für Konstanten gibt es in Definition 3.6.1 offensichtlich keine Bedingung.

3.6.3 Definition (Quotientenalgebra)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Sei A eine Σ-Algebra.
Sei $K = (K_s)_{s \in S}$ eine Kongruenz.
Dann konstruieren wir die *Quotientenalgebra* A/K wie folgt:

1. $(A/K)_s \triangleq A_s/K_s$ für alle $s \in S$
   (Die Trägermenge $(A/K)_s$ ist der Quotient von A_s bzgl. K_s.)
   (Die Elemente der Trägermengen sind somit Äquivalenzklassen.)

2. (a) für alle $c \in O_s$ gilt:
   $$c_{A/K} \triangleq [c_A]_{K_s}$$
   (b) für alle $f \in O_{(s_1,\ldots,s_n)\to s}$
   und für alle $[a_i] \in (A/K)_{s_i}$ mit $i \in [1, n]$ gilt:
   $$f_{A/K}\big(\ [a_1], \ldots, [a_n] \ \big) \triangleq \big[\ f_A(a_1, \ldots, a_n) \ \big]_{K_s}$$

3.6.4 Definition (Kern eines Homomorphismus)
Sei $\Sigma = (S, O, \mathrm{ar})$ eine Signatur.
Seien A und B zwei Σ-Algebren.
Sei $h : A \to B$ ein Σ-Homomorphismus.
Dann heißt die Familie

$$\mathrm{Ker}(h) \triangleq \big(\ \mathrm{Ker}(h_s) \ \big)_{s \in S}$$

der *Kern von* h.

3.6.5 Bemerkung Mit Definition 1.4.11 gilt offensichtlich:
$\mathrm{Ker}(h)_s : A_s \times A_s$ und für alle $a_1, a_2 \in A_s$

$$(a_1, a_2) \in \mathrm{Ker}(h)_s \quad \Longleftrightarrow \quad h_s(a_1) = h_s(a_2)$$

3.6.6 Proposition (Kern eines Homomorphismus)
Sei Σ eine Signatur.
Seien A und B zwei Σ-Algebren.
Sei $h : A \to B$ ein Σ-Homomorphismus.
Dann ist $\mathrm{Ker}(h)$ eine Kongruenz.