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

Formelsammlung
WiSe 2012/13 : v11

Technische Universität Berlin

Uwe Nestmann

4. Februar 2013

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.

[Ros07] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill, 2007.

[Sch01] Carol Schumacher. *Chapter Zero — Fundamental Notions of Abstract Mathematics*. Addison Wesley, 2001.

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

[Vel06] Daniel J. Velleman. *How to Prove It — A Structured Approach*. Cambridge University Press, 2006.

Inhaltsverzeichnis

1 Grundlagen (des Formalisierens)

1.1 Mengen

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)

- $\mathbb{N} \triangleq \{ 0, 1, 2, 3, \ldots \}$ und $\mathbb{N}^+ \triangleq \{ 1, 2, 3, \ldots \}$
- 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 $\#(A) \in \mathbb{N}$ oder $\#(A) = \infty$.

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.

- Die Angabe von B kann manchmal entfallen, wird aber empfohlen.
- Das Symbol „$|$“ kann dabei als „so dass“ gelesen werden.
- Die Angabe von $P(x)$ erfolgt entweder umgangssprachlich oder durch eine logische Formel (siehe 1.1.7 sowie § 1.2 und 1.3).

Sowohl $\{ x \in B \mid P(x) \}$ als auch $\{ x \mid P(x) \}$ definieren nur dann Mengen, wenn für alle betroffenen x die Wahrheit von $P(x)$ überprüfbar 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 logische Konnektive zunächst semi-formal als symbolische Abkürzungen natürlichsprachlicher Begriffe ein.

1.1.7 Notation („Logik-Sprache“ durch Junktor-Symbole)

- *Verum* $\top$ steht für „wahr“
- *Falsum* $\perp$ steht für „falsch“
- *Negation* $\neg$ steht für „nicht“
- *Konjunktion* $\wedge$ steht für „und“
- *Disjunktion* $\vee$ steht für „oder“
- *Implikation* $\rightarrow$ steht für „impliziert“ (d.h. „läßt schließen auf“)
- *Äquivalenz* $\leftrightarrow$ steht für „genau dann, wenn“ („g.d.w.“)
- *Universelle Quantifikation* $\forall$ steht für „für alle“
- *Existentielle Quantifikation* $\exists$ steht für „es gibt“

1.1.8 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.

1.1.9 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.

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

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

Potenzmenge von A.

1.1.11 Proposition Sei A eine beliebige Menge. Dann gilt:

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

1.2 Aussagenlogik

1.2.1 Definition (Syntax der Aussagenlogik)
Sei V eine Menge von *aussagenlogischen Variablen*.
Sei $V \cap \{ \top, \bot, \neg, \wedge, \vee, \rightarrow, \leftrightarrow \} = \emptyset$.
Dann ist die *Menge* $\mathbf{A}(V)$ *der aussagenlogischen Formeln zu* V
definiert als kleinste Menge mit:

- $V \cup \{ \top, \bot \} \subseteq \mathbf{A}(V)$;
- wenn $\varphi \in \mathbf{A}(V)$, dann auch $\neg\varphi \in \mathbf{A}(V)$;
- wenn $\{ \varphi_1, \varphi_2 \} \subseteq \mathbf{A}(V)$,
  dann auch $\{ (\varphi_1 \wedge \varphi_2), (\varphi_1 \vee \varphi_2), (\varphi_1 \rightarrow \varphi_2), (\varphi_1 \leftrightarrow \varphi_2) \} \subseteq \mathbf{A}(V)$.

Wir verwenden $p, q, \ldots$ als Metavariablen für aussagenlogische Variablen.
Wir verwenden $\varphi, \psi, \ldots$ als Metavariablen für aussagenlogische Formeln.
Formeln in $\mathbf{A}(V)$, die Variablen beinhalten, heißen *Aussagenschemata*.
Formeln in $\mathbf{A}(V)$, die keine Variablen beinhalten, heißen *Aussagen*.

1.2.2 Notation Zur leichteren Lesbarkeit können manche Klammern entfallen.
Dazu gelten folgende Regeln des *Operatorenvorrangs*.

- $\neg$ bindet stärker als alle anderen Konnektive;
- $\wedge$ und $\vee$ binden gleich stark;[1]
- $\wedge$ und $\vee$ binden stärker als $\rightarrow$ und $\leftrightarrow$;
- $\rightarrow$ und $\leftrightarrow$ binden gleich stark.

Außenklammern dürfen immer weggelassen werden.

1.2.3 Definition (Semantik der Aussagenlogik)
Sei V eine Menge von aussagenlogischen Variablen.
Eine *Variablenbelegung* β weist jedem Element $p \in V$
genau ein Element $\beta(p) \in \mathbb{B} \triangleq \{\mathsf{W}, \mathsf{F}\}$ der *Wahrheitswerte* zu.
Die zu β gehörige *Auswertung* $[\![\cdot]\!]^\beta$ weist jedem Element $\varphi \in \mathbf{A}(V)$
genau ein Element $[\![\varphi]\!]^\beta \in \mathbb{B}$ zu. ($[\![\psi]\!]^\beta$ darf kurz als $[\![\psi]\!]$ geschrieben werden, wenn keine Verwechslungsgefahr besteht.)
Zur Definition von $[\![\cdot]\!]^\beta$ gilt:

- $[\![\top]\!]^\beta \triangleq \mathsf{W}$
- $[\![\bot]\!]^\beta \triangleq \mathsf{F}$
- $[\![p]\!]^\beta \triangleq \beta(p)$

[1] Abweichend von TechGI1.

Wahrheitstabellen definieren die Semantik zusammengesetzter Formeln:

$[\![\varphi]\!]$	$[\![\neg\varphi]\!]$
F	W
W	F

$[\![\varphi_1]\!]$	$[\![\varphi_2]\!]$	$[\![\varphi_1 \wedge \varphi_2]\!]$
F	F	F
F	W	F
W	F	F
W	W	W

$[\![\varphi_1]\!]$	$[\![\varphi_2]\!]$	$[\![\varphi_1 \vee \varphi_2]\!]$
F	F	F
F	W	W
W	F	W
W	W	W

$[\![\varphi_1]\!]$	$[\![\varphi_2]\!]$	$[\![\varphi_1 \rightarrow \varphi_2]\!]$
F	F	W
F	W	W
W	F	F
W	W	W

$[\![\varphi_1]\!]$	$[\![\varphi_2]\!]$	$[\![\varphi_1 \leftrightarrow \varphi_2]\!]$
F	F	W
F	W	F
W	F	F
W	W	W

1.2.4 Definition

Sei V eine Menge von *aussagenlogischen Variablen*.

1. Zwei Formeln $\{ \varphi, \psi \} \subseteq \mathbf{A}(V)$ heißen *logisch äquivalent*, geschrieben $\varphi \equiv \psi$,[2] wenn für alle Variablenbelegungen β gilt: $[\![\varphi]\!]^\beta = [\![\psi]\!]^\beta$.
2. Eine Formel φ heißt *allgemeingültig*, wenn $\varphi \equiv \top$.
3. Eine Formel φ heißt *kontradiktorisch*, wenn $\varphi \equiv \bot$.
4. Eine Formel φ heißt *erfüllbar*, wenn es eine Variablenbelegung β gibt mit $[\![\varphi]\!]^\beta = \mathsf{W}$.
5. Formeln, die maximal eine Aussagenvariable und außer $\top$ und $\bot$ maximal einen weiteren Operator betreffen, nennen wir *trivial*.

Äquivalenzen zu trivialen Aussagenschemata dürfen ohne Beweis benutzt werden (z.B.: $\top \wedge p \equiv p$, $p \vee \bot \equiv p$, $p \rightarrow p \equiv \top, \ldots$).

1.2.5 Proposition (Logische Äquivalenz (I))

$$
\begin{aligned}
p \wedge q &\equiv q \wedge p \\
p \vee q &\equiv q \vee p \\
(p \vee q) \vee r &\equiv p \vee (q \vee r) \\
(p \wedge q) \wedge r &\equiv p \wedge (q \wedge r) \\
(p \wedge q) \vee r &\equiv (p \vee r) \wedge (q \vee r) \\
(p \vee q) \wedge r &\equiv (p \wedge r) \vee (q \wedge r)
\end{aligned}
$$

$$
\begin{aligned}
p \wedge p &\equiv p \\
p \vee p &\equiv p \\
\neg\neg p &\equiv p \\
\neg(p \wedge q) &\equiv \neg p \vee \neg q \\
\neg(p \vee q) &\equiv \neg p \wedge \neg q \\
p \wedge \neg p &\equiv \bot \\
p \vee \neg p &\equiv \top
\end{aligned}
$$

$$
\begin{aligned}
p \rightarrow q &\equiv \neg p \vee q \\
p \rightarrow q &\equiv \neg q \rightarrow \neg p \\
p \leftrightarrow q &\equiv (p \rightarrow q) \wedge (q \rightarrow p)
\end{aligned}
$$

[2]Vorsicht: Im Gegensatz zu TechGI1, wo $\equiv$ als Synonym für $\leftrightarrow$ betrachtet wird, benutzen wir in TheGI1 $\leftrightarrow$ ausschließlich als Junktor *innerhalb* einer Formel, dagegen ist $\equiv$ ein Symbol, das wir nur *außerhalb* von Formeln benutzen, wenn wir — in der so genannten *Metasprache* — *über* Formeln sprechen.

1.3 (Syntax der) Prädikatenlogik

1.3.1 Notation (Prädikate)
In der Aussagenlogik beinhaltet $V \cup \{ \top, \bot \}$ die atomaren Ausdrücke. In der Prädikatenlogik werden aussagenlogische Variablen aus V ersetzt durch so genannte *Prädikate* in $\mathrm{Pr}(X)$, die wiederum parametrisiert sind über eine Menge X von *Termvariablen*.

Typischerweise enthält $\mathrm{Pr}(X)$ Ausdrücke der Form $\mathrm{r}(t_1, \ldots, t_n)$ mit $n \in \mathbb{N}^+$, wobei r zu einer anzugebenden Menge S_{rel} so genannter Relationssymbole gehört[3] (siehe § 2.1) und die t_i aus Variablen in X sowie Elementen einer ebenfalls anzugebenden Menge S_{fun} so genannter Funktionssysmbole (siehe § 2.2) zusammengesetzt werden.

Wir schreiben $\vec{x}$ für $x_1, \ldots, x_n$ und $\vec{t}$ für $t_1, \ldots, t_n$.

1.3.2 Definition (Syntax der Prädikatenlogik)
Sei X eine Menge von *Termvariablen*.
Sei $\mathrm{Pr}(X)$ eine Menge von *Prädikaten* über X.
Dann ist die *Menge* $\mathbf{P}(X)$ *der prädikatenlogischen Formeln zu* X
definiert als kleinste Menge mit und:

- $\mathrm{Pr}(X) \cup \{ \top, \bot \} \subseteq \mathbf{P}(X)$;
- wenn $\varphi \in \mathbf{P}(X)$,
  dann auch $\neg\varphi \in \mathbf{P}(X)$;
- wenn $\{ \varphi_1, \varphi_2 \} \subseteq \mathbf{P}(X)$,
  dann auch $\{ (\varphi_1 \land \varphi_2), (\varphi_1 \lor \varphi_2), (\varphi_1 \to \varphi_2), (\varphi_1 \leftrightarrow \varphi_2) \} \subseteq \mathbf{P}(X)$,
- wenn $\varphi \in \mathbf{P}(X)$,
  dann auch $\{ (\forall x.\varphi), (\exists x.\varphi) \} \subseteq \mathbf{P}(X)$.

Wir verwenden $\varphi, \psi, \ldots$ als Metavariablen für logische Formeln.

1.3.3 Notation (Quantoren und Variablen)
In den Formeln $(\forall x.\varphi)$ und $(\exists x.\varphi)$ „binden" die Quantoren jeweils die Variable x in der Formel φ. Um Missverständnisse durch verschachtelte Mehrfachbindung zu vermeiden, benutzen wir immer paarweise verschiedene Variablen in den vorkommenden Quantoren.

Quantoren werden gelegentlich in eingeschränkter Form verwendet:

$$\begin{array}{lcl} (\forall x{\in}A \,.\, \varphi) & \triangleq & (\forall x \,.\, x{\in}A \to \varphi) \\ (\exists x{\in}A \,.\, \varphi) & \triangleq & (\exists x \,.\, x{\in}A \land \varphi) \end{array}$$

Oft werden Formeln φ zusammen mit den in ihnen frei (d.h. nicht durch Quantoren gebunden) vorkommenden Variablen $\vec{x}$ notiert als $\varphi(\vec{x})$. Das erleichtert die Notation zur Instanziierung der Variablen bzw. zum Einsetzen von konkreten Termen in entsprechender Form als $\varphi(\vec{t})$.

1.3.4 Notation (Quantoren und Klammerung)
Für Quantoren gelten folgende Regeln des *Operatorenvorrangs*:

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

[3] Üblicherweise ist das Gleichheitssymbol $=$ in S_{rel} enthalten.

1.3.5 Notation (Eindeutigkeit)
Die Aussage „es gibt *genau* ein x für das $\varphi(x)$ gilt“ wird abgekürzt durch:

$$\exists! x \,.\, \varphi(x) \quad \triangleq \quad \Big(\exists z \,.(\varphi(z))\Big) \;\wedge\; \Big(\forall x, y \,.\, \varphi(x) \wedge \varphi(y) \to x = y\Big)$$

1.3.6 Proposition (Logische Äquivalenz (II))

$$\begin{aligned} \neg(\forall x \,.\, \varphi) &\equiv \exists x \,.\, \neg\varphi \\ \neg(\exists x \,.\, \varphi) &\equiv \forall x \,.\, \neg\varphi \end{aligned}$$

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

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

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

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

1.3.8 Bemerkung Weitere Varianten existieren und können je nach Bedarf definiert werden. Dazu gehören Varianten mit mehreren Induktionsanfängen, oder auch mit mehreren Induktionsschritten, je nachdem über welchen induktiv aufgebauten Datenbereich man argumentieren möchte.

1.3.9 Notation (Induktionsschemata) Sei $P(n)$ ein Prädikat über den natürlichen Zahlen $\mathbb{N}$.
Das Prinzip aus Proposition 1.3.7 kann knapp in einer einheitlichen Formel, genannt *Induktionsschema*, zusammengefasst werden.

$$\left(P(0) \;\wedge\; \Big(\forall n \in \mathbb{N}. \big(P(n) \to P(n{+}1)\big) \Big) \right) \to (\forall x \in \mathbb{N}. P(x))$$

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

$$\left(\forall n \in \mathbb{N}. \Big((\forall m \in [0, n{-}1]. P(m)) \to P(n) \Big) \right) \to (\forall x \in \mathbb{N}. P(x))$$

2 Grundlagen (des Strukturierens)

2.1 Relationen, Ordnungen

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

$$\prod_{i\in[1,n]} A_i \quad \triangleq \quad \{ (a_1, \ldots, a_n) \mid \forall i \in [1,n] \,.\, a_i{\in}A_i \}$$

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

2.1.2 Bemerkung Seien A_1, A_2 Mengen.
Dann heißt $A_1 \times A_2 = \prod_{i\in[1,2]} A_i$ *binäres [kartesisches] Produkt*.

2.1.3 Definition (Spezialfälle)
Sei A eine beliebige Menge.

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

2.1.4 Definition (Relation)
Seien $A_1, \ldots, A_n$ nicht-leere 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 aufgrund ihres Typs zu klassifizieren.
R heißt *homogen*, falls $A_i = A_j$ für alle $1 \leq i, j \leq n$.
Zwei Relationen $R_A : \prod_{i\in[1,n]} A_i$ und $R_B : \prod_{i\in[1,m]} B_i$ sind *gleich*, falls (1) $n = m$, (2) für alle $1 \leq i \leq n$: $A_i = B_i$, und (3) $R_A = R_B$.

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

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

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

2.1.6 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 $a\ R\ b$ anstelle von $(a,b){\in}R$.

2.1.7 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:
$$\forall a_1, a_2{\in}A\,.\,\forall b{\in}B\,.\,\big(\,a_1Rb \wedge a_2Rb \to a_1{=}a_2\,\big)$$
4. *rechtseindeutig*, falls:
$$\forall a{\in}A\,.\,\forall b_1, b_2{\in}B\,.\,\big(\,aRb_1 \wedge aRb_2 \to b_1{=}b_2\,\big)$$

2.1.8 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* $P;Q : A \times C$ definiert wie folgt:
$$P;Q \quad \triangleq \quad \{\,(a,c) \in A \times C \mid \exists b{\in}B\,.\,aPb \wedge bQc\,\}$$

2.1.9 Notation Aus Bequemlichkeit schreiben wir oft PQ anstelle von $P;Q$. Aus Gründen der Konsistenz mit dem Kompositionsbegriff für Funktionen (siehe §2.2) verwenden wir auch die Notation: $Q \circ P \triangleq P;Q$

2.1.10 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:
$$P;(Q;R) = (P;Q);R$$

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

2.1.12 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. $(Q \circ R)^{-1} = R^{-1} \circ Q^{-1}$

2.1.13 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	$\forall a,b{\in}A\,.\,aRb \to bRa$	bzw	$R^{-1} = R$
antisymmetrisch	falls	$\forall a,b{\in}A\,.\,aRb \wedge bRa \to a{=}b$	bzw	$R^{-1}{\cap}R \subseteq \Delta_A$
transitiv	falls	$\forall a,b,c{\in}A\,.\,aRb \wedge bRc \to aRc$	bzw	$R \circ R \subseteq R$
linear	falls	$\forall a,b{\in}A\,.\,aRb \vee bRa$	bzw	$R^{-1}{\cup}R = \nabla_{A,A}$

2.1.14 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	•	•	•	•

2.1.15 Notation (Ordnungsbegriffe)

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

2.1.16 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.

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

2.1.17 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:

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

2.1.18 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.

2.1.19 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: $\mathrm{Typ}(\mathrm{r}(R)) = \mathrm{Typ}(\mathrm{s}(R)) = \mathrm{Typ}(\mathrm{t}(R)) = \mathrm{Typ}(R)$.

2.2 Funktionen, Abbildungen, Kardinalitäten

2.2.1 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 verwenden die Begriffe *Abbildung* und *Funktion* synonym.

2.2.2 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.

2.2.3 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 $f_1 : A_1 \times B_1$ und $f_2 : A_2 \times B_2$ gleiche Relationen sind. Inbesondere gilt: $\mathrm{Def}(f_1) = \mathrm{Def}(f_2)$ und $\forall x \in \mathrm{Def}(f_1) \,.\, f_1(x) = f_2(x)$.

2.2.4 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.
Außerdem gilt: $(g \circ f)(x) = g(f(x))$ für alle $x \in A$.

2.2.5 Definition (Eigenschaften partieller Abbildungen)

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

2.2.6 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: $(f^{-1})^{-1} = f$.

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

2.2.8 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 $g \circ f = \Delta_A$.
Außerdem gilt: $g = f^{-1}$.

2.2.9 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: $(\ g_1 \circ f = g_2 \circ f\ ) \ \to\ g_1 = g_2$
2. Falls h injektiv, dann gilt: $(\ h \circ g_1 = h \circ g_2\ ) \ \to\ g_1 = g_2$

2.2.10 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 $f = h \circ g$.

2.2.11 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: $\forall n \in \mathbb{N} \,.\, n < \infty$.

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

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

2.2.13 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 $\mathrm{card}(A) \neq \mathrm{card}(B)$.

2.2.14 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.

2.2.15 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 $\mathrm{card}(\mathbb{N}) < \mathrm{card}(A)$.

2.2.16 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. $\mathrm{card}(\mathbb{Q}) < \mathrm{card}(\mathbb{R})$

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

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

2.2.18 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*.

2.2.19 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.

Wir definieren die *Größe* von T durch die Summe der Häufigkeiten aller Elemente von A in T durch:

$$\#(T) \triangleq \sum_{a \in A} M_T(a)$$

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

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

2.2.22 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 $\bmod$ wohldefinierte Abbildungen.
Die Abbildung $n \bmod k$ wird oft auch mit $n \,\%\, k$ bezeichnet.

2.3 Äquivalenzen, Quotienten

2.3.1 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.

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

2.3.3 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 $A \times A$.

2.3.4 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.

2.3.5 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.

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

2.3.7 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. $(a_1, a_2) \notin R \iff [a_1] \cap [a_2] = \emptyset$

2.3.8 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.*

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

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

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

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

2.3.11 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*.

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

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

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

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

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

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

die *natürliche Abbildung von f*, und

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

Es gilt:

1. nat_f ist surjektiv, val_f ist injektiv.

2. $f = \mathrm{val}_f \circ \mathrm{nat}_f$

3. $\mathrm{Bild}(f) \cong A/\mathrm{Ker}(f)$

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

3 Diskrete / Algebraische Strukturen

3.1 Wörter, Sprachen

3.1.1 Definition (Wörter)
Sei Σ eine Menge ($\neq \emptyset$), genannt *Alphabet*.
Die Elemente $s_i \in \Sigma$ werden auch *Symbol*, *Zeichen*, *Buchstabe* genannt.

1. Ein *Wort* w über Σ ist eine endliche Sequenz $(a_1, \ldots, a_n)$ mit $n \in \mathbb{N}$ und $a_i \in \Sigma$ 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. Σ^* bezeichnet die Menge aller [endlichen] Wörter über Σ.

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

3.1.2 Definition (Operationen auf Wörtern)
Seien $v = (a_1, \ldots, a_m)$ und $w = (b_1, \ldots, b_n)$ zwei Wörter aus Σ^*.

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 $u \in \Sigma^*$ gibt, so dass $v \cdot u = w$.
3. v heißt *Suffix* von w, falls es $u \in \Sigma^*$ gibt, so dass $u \cdot v = w$.
4. v heißt *Teilwort* von w, falls es $u_1, u_2 \in \Sigma^*$ gibt, so dass $u_1 \cdot v \cdot u_2 = w$.

3.1.3 Notation
Seien $v \in \Sigma^*$ und $a \in \Sigma$.
Anstelle von $(a) \cdot v$ schreiben wir oft av.
Anstelle von $v \cdot (a)$ schreiben wir oft va.

3.1.4 Lemma (Dekomposition) Sei w ein Wort über dem Alphabet Σ.
Dann gilt genau einer der beiden folgenden Fälle:

1. $w = \lambda$ (also $|w| = 0$), oder
2. es gibt $a \in \Sigma$ und $v \in \Sigma^*$ 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.

$$\left(P(\lambda) \ \wedge \ \Big(\forall v{\in}\Sigma^*. \big(P(v) \rightarrow \forall a{\in}\Sigma \ . \ P(av)\big) \Big) \right) \rightarrow \big(\forall w{\in}\Sigma^*. P(w) \big)$$

$$\left(P(\lambda) \ \wedge \ \Big(\forall v{\in}\Sigma^*. \big(P(v) \rightarrow \forall a{\in}\Sigma \ . \ P(va)\big) \Big) \right) \rightarrow \big(\forall w{\in}\Sigma^*. P(w) \big)$$

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

3.1.5 Definition (Ordnungen auf Wörtern)
Sei Σ ein Alphabet. Sei $R : \Sigma \times \Sigma$ eine beliebige homogene Relation.

1. Die *lexikographische Ordnung* $\ll_R : \Sigma^* \times \Sigma^*$ ist definiert durch:

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

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

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

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

3.1.7 Definition (Sprachen)
Sei Σ ein Alphabet.
Dann heißt jede Teilmenge $A \subseteq \Sigma^*$ *Sprache über* Σ.

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

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

Die *n-fache Konkatenation* ist definiert durch:

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

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

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

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

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

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

definiert die zugehörige Sprache eines regulären Ausdrucks.

3.2 (Abzählende) Kombinatorik

3.2.1 Definition („Schubfachprinzip“ bzw. „Pigeonhole Principle“)
Sei m eine endliche Zahl von Schubfächern mit unbegrenzter Kapazität.
Sei n eine Zahl von Objekten mit $n > m$.
Wenn die n Objekte komplett auf die m Schubfächer verteilt werden,
so gibt es danach mindestens ein Schubfach,
in dem mindestens zwei Objekte liegen.

3.2.2 Definition (Verallgemeinertes „Schubfachprinzip“)
Sei m eine endliche Zahl von Schubfächern mit unbegrenzter Kapazität.
Sei n eine Zahl von Objekten.
Wenn die n Objekte komplett auf die m Schubfächer verteilt werden,
so gibt es danach mindestens ein Schubfach,
in dem mindestens $\lceil \frac{n}{m} \rceil$ Objekte liegen.

3.2.3 Definition (Fakultät)
Sei $n \in \mathbb{N}$. Wir definieren:

$$n! \quad \triangleq \quad \begin{cases} 1 & \text{falls } n = 0 \\ n\,(n-1)! & \text{falls } n > 0 \end{cases}$$

3.2.4 Definition (Binomialkoeffizienten)
Seien $k, n \in \mathbb{N}$. Wir definieren:

$$\binom{n}{k} \quad \triangleq \quad \begin{cases} \dfrac{n!}{k!(n-k)!} & \text{falls } k \leq n \\ \\ 0 & \text{falls } k > n \end{cases}$$

3.2.5 Lemma Es gelten: $0! = 1$ und $\binom{0}{0} = 1$ und $\binom{n}{0} = 1$ und $\binom{n}{n} = 1$.

3.2.6 Lemma (Pascal'sches Dreieck)
Seien $k, n \in \mathbb{N}$. Dann gelten:

1. $\binom{n}{n-k} = \binom{n}{k}$, falls $k \leq n$
2. $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$, falls $n \geq k > 0$
3. $\sum_{i \in [0,n]} \binom{n}{i} = 2^n$

3.2.7 Definition (Binomischer Satz)
Sei $n \in \mathbb{N}$. Dann gilt:

$$(x+y)^n = \underbrace{\sum_{i \in [0,n]} \binom{n}{i} x^i \, y^{n-i}}_{\textit{Expansion} \text{ von } (x+y)^n}$$

3.2.8 Proposition (Permutationen / Anordnungen)
Sei $n \in \mathbb{N}$. Dann ist

$$\mathrm{P}(n) \quad \triangleq \quad n!$$

die Anzahl der *Permutationen von n verschiedenen Objekten*.

3.2.9 Proposition (Permutationen modulo Äquivalenz)
Sei O eine endliche Menge von Objekten mit $\#(O) = n \in \mathbb{N}$.
Sei $\equiv : O \times O$ eine Äquivalenzrelation mit Index $p \in [1, n]$.
Seien $n_i \in \mathbb{N}$ für $i \in [1, p]$ die Größen der Äquivalenzklassen von $\equiv$.
Dann ist

$$\mathrm{P}_{\equiv}(n) \quad \triangleq \quad \frac{n!}{n_1!\, n_2!\, \cdots\, n_p!}$$

die Anzahl der Permutationen von n Objekten modulo $\equiv$.

3.2.10 Proposition (Kombinationen / Stichproben ohne Reihenfolge)
Seien $n \in \mathbb{N}$ und $k \in [0, n]$. Dann ist

$$\mathrm{K}_{\mathrm{oW}}(n, k) \quad \triangleq \quad \binom{n}{k}$$

die Anzahl der *k-Kombinationen von n verschiedenen Objekten*
(auch bekannt als *k-elementige Teilmengen einer n-elementigen Menge*).

3.2.11 Proposition (Variationen / Stichproben mit Reihenfolge)
Seien $n \in \mathbb{N}$ und $k \in [0, n]$. Dann ist

$$\begin{aligned} \mathrm{V}_{\mathrm{oW}}(n, k) \quad &\triangleq \quad n * \mathrm{V}_{\mathrm{oW}}(n{-}1, k{-}1) \\ \mathrm{V}_{\mathrm{oW}}(n, 0) \quad &\triangleq \quad 1 \end{aligned}$$

die Anzahl der *k-Variationen von n verschiedenen Objekten*
(auch bekannt als *k-elementige Permutationen einer n-elementigen Menge*,
sowie mit der Notation $n^{\underline{k}}$).

3.2.12 Proposition Seien $n \in \mathbb{N}$ und $k \in [0, n]$.
Dann gilt:

$$\mathrm{V}_{\mathrm{oW}}(n, k) \quad = \quad \binom{n}{k} k! \quad = \quad \frac{n!}{(n{-}k)!}$$

3.2.13 Proposition (Variationen mit Wiederholung)
Seien $n \in \mathbb{N}$ und $k \in [0, n]$. Dann ist

$$\mathrm{V}_{\mathrm{mW}}(n, k) \quad \triangleq \quad n^k$$

die Anzahl der *k-Variationen n verschiedener Objekte mit Wiederholung*.

3.2.14 Proposition (Kombinationen mit Wiederholung)
Seien $n \in \mathbb{N}$ und $k \in [1, n]$. Dann ist

$$\mathrm{K}_{\mathrm{mW}}(n, k) \quad \triangleq \quad \binom{n{+}k{-}1}{k}$$

die Anzahl der *k-Kombinationen n verschiedener Objekte mit Wiederholung*
(weniger bekannt als *k-elementige Multi-Mengen,*
die aus Elementen einer n-elementigen Menge gebildet werden können).

3.3 Monoide, Gruppen, Ringe, Halbverbände

3.3.1 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

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

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

$$\forall x, y \in X \; . \; x \circ y = y \circ x \tag{COMM}$$

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

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

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

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

$$\forall x \in X \; . \; e_\mathrm{l} \circ x = x \tag{NEUT-L}$$

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

$$\forall x \in X \; . \; x \circ e_\mathrm{r} = x \tag{NEUT-R}$$

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

3.3.5 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.

3.3.6 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:

$$x_\mathrm{l} \circ x = e \tag{INV-L}$$

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

$$x \circ x_\mathrm{r} = e \tag{INV-R}$$

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

3.3.7 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*.

3.3.8 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*.

3.3.9 Notation In Def 3.3.8 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.

3.3.10 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.

3.3.11 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*.

3.3.12 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.

3.4 Extremwerte, Schranken, Verbände

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

1. (a) $u \in A$ heißt *minimales Element in A*, falls gilt:

$$\forall a \in A \ . \ \big(a \leq u \to a = u\big)$$

   (b) $o \in A$ heißt *maximales Element in A*, falls gilt:

$$\forall a \in A \ . \ \big(o \leq a \to a = o\big)$$

2. (a) $k \in A$ heißt *kleinstes Element von A*, falls gilt:

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

   (b) $g \in A$ heißt *größtes Element von A*, falls gilt:

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

   Ein kleinstes Element heißt auch *Minimum von A*, ein größtes Element heißt auch *Maximum von A*, notiert als $\mathrm{Min}_{\leq}(A)$ bzw. $\mathrm{Max}_{\leq}(A)$.

3.4.2 Bemerkung Bezüglich einer Halbordnung $\leq: X \times X$ existieren Extremwerte nicht notwendigerweise für jede Teilmenge $A \subseteq X$. Minimale und maximale Elemente sind zudem nicht immer eindeutig.

3.4.3 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).

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

3.4.5 Lemma
Sei $\leq : X \times X$ eine totale Ordnung. Sei $A \subseteq X$ mit $\#(A) \in \mathbb{N}^+$.
Dann sind $\inf^X(A) \in A$ und $\sup^X(A) \in A$.
Somit sind $\mathrm{Min}_{\leq}(A)$ und $\mathrm{Max}_{\leq}(A)$ definiert.

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

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

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

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

   Die Halbordnungen $\leq_\sqcap$ und $\leq_\sqcup^{-1}$ gemäß Lemma 3.3.12
   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:

$$\begin{array}{ll} x \sqcap \bot = \bot & \quad x \sqcap \top = x \\ x \sqcup \top = \top & \quad x \sqcup \bot = x \end{array}$$

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

$$x \sqcap \bar{x} = \bot \qquad x \sqcup \bar{x} = \top$$

4. Ein Verband $(X, \sqcap, \sqcup)$ heißt *distributiv*, wenn
   die Gesetze (DIST-L) und (DIST-R) aus Def 3.3.8, bezogen auf $(+, *)$,
   sowohl für $(\sqcup, \sqcap)$ als auch für $(\sqcap, \sqcup)$ gelten.

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

3.4.7 Lemma
Sei $\leq : X \times X$ eine Halbordnung,
für die für jedes $A \subseteq X$ sowohl $\inf^X(A)$, als auch $\sup^X(A)$ existieren.
Seien $\sqcap : X \times X \to X$ und $\sqcup : X \times X \to X$ definiert durch:

$$x \sqcap y \triangleq \inf^X(\{\, x, y \,\})$$
$$x \sqcup y \triangleq \sup^X(\{\, x, y \,\})$$

Dann ist $(X, \sqcap, \sqcup)$ ein vollständiger Verband.

3.4.8 Proposition
Sei $\leq : X \times X$ eine totale Ordnung.
Sei $\min, \max : X \times X \to X$ definiert durch:

$$\min(x, y) \triangleq \mathrm{Min}_{\leq}(\{\, x, y \,\})$$
$$\max(x, y) \triangleq \mathrm{Max}_{\leq}(\{\, x, y \,\})$$

Dann ist $(X, \min, \max)$ ein distributiver Verband.

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

3.5 Graphen

3.5.1 Definition (Ungerichtete Graphen)
Sei V eine nicht-leere Menge von *Knoten*.
Sei $m : \mathcal{P}(V) \to \mathbb{N}$ die Multiplizität der *Kanten*.
Sei $E \triangleq \{e \in \mathcal{P}(V) \mid m(e) > 0\}$.
$G = (V, E, m)$ heißt *(ungerichteter) Graph*, falls $\forall e \in E \,.\, \#(e) \in \{\, 1, 2 \,\}$, andernfalls (d.h. $\exists e \in E \,.\, \#(e){>}2$) heißt G *Hypergraph*.
Für $e \in E$ heißen die Elemente $v \in e$ *Endpunkte von* e.
Im folgenden betrachten wir nur Graphen.
G heißt *endlich*, wenn $\#(V) \in \mathbb{N}^+$; andernfalls heißt G *unendlich*.
Eine Kante $e = \{\, v \,\}$ heißt *Schlinge*.
Ein Graph mit Schlingen heißt auch *Pseudograph*.
Sei G ein Graph ohne Schlingen.
Dann heißt G *einfach*, wenn $m(E){=}\{1\}$; andernfalls heißt G *multipel*.

3.5.2 Definition (Gerichtete Graphen)
Sei V eine nicht-leere Menge von *Knoten*.
Sei $m : (V \times V) \to \mathbb{N}$ die Multiplizität der *Kanten*.
Sei $E \triangleq \{e \in V \times V \mid m(e) > 0\}$.
Dann heißt $G = (V, E, m)$ *gerichteter Graph* oder *Digraph*.
Für $e \in E$ mit $e = (s, t)$ heißen

- $\mathrm{src}(e) \triangleq s$ der *Fuß* bzw. *Start (von e)*, und
- $\mathrm{trg}(e) \triangleq t$ der *Kopf* bzw. das *Ziel (von e)*.

G heißt *endlich*, wenn $\#(V) \in \mathbb{N}^+$; andernfalls heißt G *unendlich*.
Eine Kante $e = (v, v)$ heißt *Schlinge*.
Ein Digraph mit Schlingen heißt auch *Pseudodigraph*.
Sei G ein Digraph ohne Schlingen.
Dann heißt G *einfach*, wenn $m(E){=}\{1\}$; andernfalls heißt G *multipel*.

3.5.3 Notation
Wir notieren einfache [Di-]Graphen $G = (V, E, m)$ auch als (V, E).

3.5.4 Definition Zu jedem gerichteten Graphen $G = (V, E, m)$ ist der zugehörige ungerichtete Graph $\mathrm{u}(G) = (V, E', m')$ definiert durch

- $E' \triangleq \{\, \{\, u, v \,\} \mid (u, v) \in E \vee (v, u) \in E \,\}$ und
- $m'(\{u, v\}) \triangleq m((u, v)) + m((v, u))$.

3.5.5 Definition (Nachbarschaft (I))
Sei $G^{\mathrm{d}} = (V, E^{\mathrm{d}}, m^{\mathrm{d}})$ ein gerichteter Graph.
Sei $G^{\mathrm{u}} = (V, E^{\mathrm{u}}, m^{\mathrm{u}})$ ein ungerichteter Graph.
Zwei Knoten u und v heißen *benachbart*, falls sie durch eine Kante direkt miteinander *verbunden* sind:

- in G^{d}, falls $(u, v) \in E^{\mathrm{d}}$ oder $(v, u) \in E^{\mathrm{d}}$;
- in G^{u}, falls $\{u, v\} \in E^{\mathrm{u}}$.

Seien $v \in V$ und $A \subseteq V$.
Die Menge $\mathrm{N}(v)$ bezeichnet die Menge aller Nachbarn von v.
Die Menge $\mathrm{N}(A) \triangleq \bigcup_{v \in A} \mathrm{N}(v)$ bezeichnet die Menge aller Nachbarn von A.

3.5.6 Definition (Nachbarschaft (II))
Sei $G^{\mathrm{d}} = (V, E^{\mathrm{d}}, m^{\mathrm{d}})$ ein gerichteter Graph.
Sei $G^{\mathrm{u}} = (V, E^{\mathrm{u}}, m^{\mathrm{u}})$ ein ungerichteter Graph.
Sei $G \in \{ G^{\mathrm{d}}, G^{\mathrm{u}} \}$. Sei $v \in V$.
Der *Grad* $\deg_G(v)$ ist die Zahl der Kanten, mit denen v in G verbunden ist.

$$\deg_{G^{\mathrm{u}}}(v) \triangleq \sum_{e \in E^{\mathrm{u}} \mid e = \{u,v\} \wedge u \neq v} m(e) + \sum_{e \in E^{\mathrm{u}} \mid e = \{v\}} 2 * m(e)$$

$$\deg_{G^{\mathrm{d}}}(v) \triangleq \underbrace{\sum_{e \in E^{\mathrm{d}} \mid v = \mathrm{src}(e)} m(e)}_{\textit{Ausgangsgrad } \deg^{+}_{G^{\mathrm{d}}}(v)} + \underbrace{\sum_{e \in E^{\mathrm{d}} \mid v = \mathrm{trg}(e)} m(e)}_{\textit{Eingangsgrad } \deg^{-}_{G^{\mathrm{d}}}(v)}$$

Wenn $\deg_G(v) = 0$ heißt v *isoliert in G*.
Wenn $\deg^{-}_G(v) = 0$ heißt v *Quelle von G*.
Wenn $\deg^{+}_G(v) = 0$ heißt v *Senke von G*.

3.5.7 Definition (Pfade I)
Sei $G^{\mathrm{d}} = (V, E^{\mathrm{d}}, m^{\mathrm{d}})$ ein gerichteter Graph.
Sei $G^{\mathrm{u}} = (V, E^{\mathrm{u}}, m^{\mathrm{u}})$ ein ungerichteter Graph.
Sei $G \in \{ G^{\mathrm{d}}, G^{\mathrm{u}} \}$.
Die Menge aller *Pfade* bzw. *Wege* in Graphen ist definiert durch:

$$\mathrm{Pfade}^{\mathrm{E}}_{G^{\mathrm{d}}} \triangleq \big\{ (e_1, \ldots, e_n) \mid n \in \mathbb{N} \wedge \boxed{\exists v_0, \ldots, v_n \in V} \;.\; \forall k \in [1, n] \;.\; e_k \in E^{\mathrm{d}} \;\wedge\; e_k = (v_{k-1}, v_k) \big\}$$

$$\mathrm{Pfade}^{\mathrm{E}}_{G^{\mathrm{u}}} \triangleq \big\{ (e_1, \ldots, e_n) \mid n \in \mathbb{N} \wedge \boxed{\exists v_0, \ldots, v_n \in V} \;.\; \forall k \in [1, n] \;.\; e_k \in E^{\mathrm{u}} \;\wedge\; e_k = \{ v_{k-1}, v_k \} \big\}$$

Ein *Pfad* $(e_1, \ldots, e_n) \in \mathrm{Pfade}^{\mathrm{E}}_G$ hat die *Länge* $|(e_1, \ldots, e_n)| \triangleq n$.
Der Pfad $()$ bzw. λ heißt *leerer Pfad*.
Die Sequenz $(v_0, \ldots, v_n)$ der oben eingerahmten Knoten heißt zum entsprechenden Pfad $(e_1, \ldots, e_n)$ *zugehöriger Knotenpfad*; er ist nicht immer eindeutig gegeben.

3.5.8 Notation Üblicherweise lassen wir den Superscript E weg.
In einfachen Graphen werden Pfade oft durch die Angabe des zugehörigen Knotenpfades angegeben, also $(v_0, \ldots, v_n)$ anstelle von $(e_1, \ldots, e_n)$.

3.5.9 Definition (Pfade II)
Sei $G^{\mathrm{d}} = (V, E^{\mathrm{d}}, m^{\mathrm{d}})$ ein gerichteter Graph.
Sei $G^{\mathrm{u}} = (V, E^{\mathrm{u}}, m^{\mathrm{u}})$ ein ungerichteter Graph.
Sei $G \in \{ G^{\mathrm{d}}, G^{\mathrm{u}} \}$.
Sei $p = (e_1, \ldots, e_n)$ ein Pfad in G.
Sei $(v_0, \ldots, v_n)$ der zugehörige Knotenpfad.

Dann heißt p auch *Pfad von v_0 nach v_n*.
Seien $u, v \in V$. Wenn es einen nicht-leeren Pfad von u nach v gibt, dann heißt u *Vorgänger* von v, sowie v *Nachfolger* von u.

3.5.10 Definition (Zyklus)
Sei $G^{\mathrm{d}} = (V, E^{\mathrm{d}}, m^{\mathrm{d}})$ ein gerichteter Graph.
Sei $G^{\mathrm{u}} = (V, E^{\mathrm{u}}, m^{\mathrm{u}})$ ein ungerichteter Graph.
Sei $G \in \{ G^{\mathrm{d}}, G^{\mathrm{u}} \}$.
Sei $p = (e_1, \ldots, e_n)$ ein Pfad in G.
Sei $(v_0, \ldots, v_n)$ der zugehörige Knotenpfad.

Wenn $n > 0$ und $v_0 = v_n$, dann heißt p auch *Zyklus*.
Wenn p keine Kante doppelt durchläuft,
d.h. wenn für alle $1 \leq i \neq j \leq n$ gilt: $e_i \neq e_j$,
dann heißt p *einfach*.
Wenn G mindestens einen einfachen Zyklus enthält,
dann heißt *zyklisch*; andernfalls heißt G *azyklisch*.
Ein *dag* ist ein gerichteter azyklischer Graph.

3.5.11 Proposition Sei $G = (V, E, m)$ ein dag.
Dann ist $\mathrm{t}(\mathrm{r}(E))$ eine Halbordnung auf V.

3.5.12 Definition
Sei $G^{\mathrm{d}} = (V, E^{\mathrm{d}}, m^{\mathrm{d}})$ ein gerichteter Graph.
Sei $G^{\mathrm{u}} = (V, E^{\mathrm{u}}, m^{\mathrm{u}})$ ein ungerichteter Graph.

1. G^{u} heißt *zusammenhängend*, falls es in G^{u} zwischen je zwei verschiedenen Knoten einen Pfad gibt.
2. G^{d} heißt *(schwach) zusammenhängend*, falls $\mathrm{u}(G)$ zusammenhängend ist.
3. G^{d} heißt *(stark) zusammenhängend*, falls es in G^{d} zwischen je zwei verschiedenen Knoten Pfade in beiden Richtungen gibt.

3.5.13 Definition (Partition)
Sei A eine beliebige Menge.
Seien $A_1, \ldots, A_n \subseteq A$ mit $A_i \neq \emptyset$ für alle $1 \leq i \leq n$.
Die Menge $\{ A_1, \ldots, A_n \}$ heißt *Partition* von A, falls gilt:

- $\forall i, j \in [1, n] \ . \ i \neq j \rightarrow A_i \cap A_j = \emptyset$
- $A = \bigcup_{i \in [1,n]} A_i$

3.5.14 Definition (Bipartite Graphen)
Sei $G = (V, E)$ ein einfacher Graph.
G heißt *bipartit*, falls es eine Partition $\{ V_1, V_2 \}$ von V gibt, so dass gilt:

$$\forall e \in E \ . \ \exists v_1 \in V_1 \ . \ \exists v_2 \in V_2 \ . \ e = \{ v_1, v_2 \}.$$

$\{ V_1, V_2 \}$ heißt dann *Bipartition* von V.

3.5.15 Definition (Färbung)
Sei $G = (V, E, m)$ ein gerichteter oder ungerichteter Graph.
Sei F eine endliche Menge von *Farben*.
Eine Abbildung $f : V \rightarrow F$ heißt *Färbung von G*.

3.5.16 Bemerkung Der Kern $\mathrm{Ker}(f)$ einer Färbung f bestimmt eine Partition der Knotenmenge des Graphen in Knotenmengen gleicher Farbe.

3.5.17 Definition (Teilgraph)
Seien $G = (V, E, m)$ und $G' = (V', E', m')$
(beide gerichtete oder beide ungerichtete) Graphen.
G heißt *Teilgraph von* G', falls gilt

- $V \subseteq V'$;
- $E \subseteq E'$;
- $\forall e \in E \,.\, m(e) \leq m'(e)$.

3.5.18 Definition (Einschränkung)
Sei $R : A \times B$ eine Relation.
Sei $f : A \to B$ eine Abbildung.
Seien $\emptyset \neq \underline{A} \subseteq A$ und $\emptyset \neq \underline{B} \subseteq B$. Dann bezeichnen

$$R\restriction_{\underline{A}\times\underline{B}} \quad \triangleq \quad R \cap (\underline{A} \times \underline{B})$$

und

$$f\restriction_{\underline{A}} \quad \triangleq \quad f \cap (\underline{A} \times B)$$

Einschränkungen von R und f bzgl. der Mengen $\underline{A}$ und $\underline{B}$.

3.5.19 Definition (Induzierter Teilgraph)
Sei $G^{\mathrm{d}} = (V, E^{\mathrm{d}}, m^{\mathrm{d}})$ ein gerichteter Graph.
Sei $G^{\mathrm{u}} = (V, E^{\mathrm{u}}, m^{\mathrm{u}})$ ein ungerichteter Graph.
Sei $\emptyset \neq W \subseteq V$.
Dann sind:

1. $(W, E^{\mathrm{u}} \cap \mathcal{P}(W), m^{\mathrm{u}}\restriction_{\mathcal{P}(W)})$ der durch W induzierte Teilgraph von G^{u};
2. $(W, E^{\mathrm{d}}\restriction_{W\times W}, m^{\mathrm{d}}\restriction_{W\times W})$ der durch W induzierte Teilgraph von G^{d}.

3.6 Bäume

3.6.1 Definition (Baum)
Sei $G = (V, E)$ ein einfacher ungerichteter Graph.
G heißt *(ungerichteter) Baum*,
wenn er zusammenhängend ist und keine einfachen Zyklen enthält.

3.6.2 Proposition Ein Baum mit n Konten hat $n{-}1$ Kanten.

3.6.3 Definition (Gerichteter Baum)
Sei $G = (V, E)$ ein einfacher gerichteter Graph.
Sei $r \in V$ ein beliebiger Knoten.

(G, r) heißt *gerichteter* oder *gewurzelter Baum (mit Wurzel r)*, wenn $\mathrm{u}(G)$ ein Baum ist und es in G für jeden Knoten $v \in V$ genau einen einfachen Pfad von r nach v gibt.

Seien $u, v \in V$ mit $(u, v) \in E$. Dann heißt u *Elternknoten* von v und v heißt *Kindknoten* von u. Zwei (verschiedene) Knoten heißen *Geschwisterknoten*, wenn sie den gleichen Elternknoten haben.

Sei $u \in V$. Dann bezeichnet $\mathrm{K}(u) \triangleq \{\, v \in V \mid (u, v) \in E \,\}$ die Menge der Kindknoten von u.

Alle Knoten auf einem nicht-leeren Pfad von der Wurzel zu einem Knoten v – außer v selbst – heißen *Vorfahren* von v. Alle Knoten, die einen Knoten u als Vorfahren haben, heißen *Nachfahren* von u.

Ein Knoten des Baumes, der keine Nachfahren hat, heißt *Blatt*. Knoten des Baumes, die keine Blätter sind, heißen *innere* bzw. *interne Knoten*.

3.6.4 Definition (Teilbaum, Unterbaum)
Sei $B = (G, r)$ ein gerichteter Baum zu $G = (V, E)$.
Sei $u \in V$.
Sei $V_u \subseteq V$ derart, dass V_u genau u und alle seine Nachfahren enthält.
Sei $E_u \subseteq E$ derart, dass E_u genau alle Kanten aus E enthält, die zwischen Knoten aus V_u existieren.
Dann heißt $\big((V_u, E_u), u\big)$ *Teilbaum (von) B*.
Sei $u \in \mathrm{K}(r)$. Dann heißt $\big((V_u, E_u), u\big)$ *(direkter) Unterbaum von B*.

3.6.5 Definition (Mehrstelliger Baum)
Sei B ein gerichteter Baum.
B heißt *k-stellig*, wenn jeder interne Knoten höchstens k Kinder hat.
B heißt *voll k-stellig*, wenn jeder interne Knoten genau k Kinder hat.
Ist B voll 2-stellig, so heißt B *binärer Baum*.

3.6.6 Definition (Geordneter Baum)
Sei $B = (G, r)$ ein gerichteter Baum mit $G = (V, E)$.
Sei $\mathrm{Int}_G \subseteq V$ die Menge der internen Knoten von G.
Sei $\leq^{\mathrm{K}} \triangleq (\leq_v)_{v \in \mathrm{Int}_G}$ eine Familie von totalen Ordnungen $\leq_v : \mathrm{K}(v) \times \mathrm{K}(v)$.
Dann heißt $(G, r, \leq^{\mathrm{K}})$ *geordneter gerichteter Baum*.

Der Ordnung der Kinder eines Knotens v induziert eine entsprechende Ordnung auf den direkten Unterbäumen von v.

3.6.7 Definition (Tiefe, Höhe, Balance)
Sei $B = (G, r)$ ein gerichteter Baum mit $G = (V, E)$.
Die *Tiefe* eines Knotens $v \in V$ ist die Länge des Pfades von r nach v.
Die Tiefe der tiefsten Knoten in B bestimmt dessen *Höhe*.
Sei h die Höhe von B.
Liegen alle Blätter von B in Tiefe h oder $h{-}1$, so heißt B *balanciert*.

3.6.8 Proposition Ein m-stelliger Baum der Höhe h hat höchstens m^h Blätter.

3.6.9 Definition (Adressierung)
Sei $B = (G, r, \leq^{\mathrm{K}})$ ein geordneter gerichteter Baum mit $G = (V, E)$.
Sei $\mathrm{Adr} \triangleq \{0\} \cup \left(\mathbb{N}^+ \cdot (\{.\} \cdot \mathbb{N}^+)^*\right)$ die Menge der *(Baum-)Adressen*.
Sei $k_v \triangleq \#(\mathrm{K}(v))$ für $v \in V$.
Die *universelle Adressierung* $\mathrm{uadr} : V \to \mathrm{Adr}$ ist definiert, wie folgt:

- r hat die Adresse 0;
- die k_r Kinder von r bekommen die Adressen $1, \ldots, k_r$ gemäß $\leq_r$.
- wenn A die Adresse eines Knotens v der Tiefe $n > 0$ ist,
  so bekommen seine k_v Kinder die Adressen $A.1, \ldots, A.k_v$ gemäß $\leq_v$.

3.6.10 Definition (Traversierung per Ordnung)
Sei $B = (G, r, \leq^{\mathrm{K}})$ ein geordneter gerichteter Baum mit $G = (V, E)$.
Tiefensuche in B bezeichnet die Traversierung von B entlang der lexikographischen Ordnung auf $\mathrm{uadr}(V)$.
Breitensuche in B bezeichnet die Traversierung von B entlang der Standardordnung auf $\mathrm{uadr}(V)$.

3.6.11 Definition (Traversierung per Rekursion)
Sei $B = (G, r, \leq^{\mathrm{K}})$ ein geordneter gerichteter Baum mit $G = (V, E)$.
Ein *Traversierungsalgorithmus* ist ein rekursives Verfahren, durch das jeder Knoten in V besucht wird. Seien $B_1, \ldots, B_n$ die direkten Unterbäume, die durch die Kindknoten von r bestimmt sind.

- *preorder* besucht
  1. zuerst r,
  2. dann in $\leq^{\mathrm{K}}$-Reihenfolge die $B_1, \ldots, B_n$, jeweils in preorder.
- *inorder* besucht
  1. zuerst B_1,
  2. dann r,
  3. dann in $\leq^{\mathrm{K}}$-Reihenfolge die $B_2, \ldots, B_n$, jeweils in inorder.
- *postorder* besucht
  1. zuerst in $\leq^{\mathrm{K}}$-Reihenfolge die $B_1, \ldots, B_n$, jeweils in postorder,
  2. dann (zuletzt) r.

3.6.12 Definition (Spannbaum)
Sei G ein einfacher Graph.
Ein Teilgraph von G, der ein Baum ist und jeden Knoten enthält, heißt *Spannbaum von G*.

3.6.13 Proposition Ein einfacher Graph G ist zusammenhängend genau dann, wenn es einen Spannbaum von G gibt.