Elementare Begriffe und Schreibweisen

Logische Verknüpfungen.

Wir schreiben:

$\neg$	für	*nicht*
$\wedge$	für	*und*
$\vee$	für	*oder*
$\rightarrow$ und $\Rightarrow$	für	*wenn ... so*
$\leftrightarrow$ und $\Leftrightarrow$	für	*genau dann, wenn*
$\exists$	für	*es existiert*
$\forall$	für	*für alle*

Elementbeziehung und Enthaltenseinsrelation (Inklusion).

- $a \in M \Leftrightarrow_{\text{def}} a$ ist ein Element der Menge M
- $a \notin M \Leftrightarrow_{\text{def}} a$ ist kein Element der Menge M
- $M \subseteq N \Leftrightarrow_{\text{def}}$ aus $a \in M$ folgt $a \in N$ (M ist Teilmenge von N)
- $M \not\subseteq N \Leftrightarrow_{\text{def}}$ es gilt nicht $M \subseteq N$ (M ist keine Teilmenge von N)
- $M \subset N \Leftrightarrow_{\text{def}} M \subseteq N$ und $M \neq N$ (M ist echte Teilmenge von N)

Definition spezieller Mengen.

- Durch Angabe der Elemente:
  $\{a_1, a_2, \ldots, a_n\}$ ist die Menge, die aus den Elementen $a_1, a_2, \ldots, a_n$ besteht.
  Beispiele: $\{0, 1\}$
  $\{2, 3, 5, 7, 11, 13, 17, 19, 13, 19, 31, 37\}$
  $\mathbb{N} =_{\text{def}} \{0, 1, 2, 3, 4, 5, \ldots\}$ (Menge der natürlichen Zahlen)
- Durch eine Eigenschaft E:
  $\{a : E(a)\}$ ist die Menge aller Elemente, die die Eigenschaft E besitzen.
  Beispiele: $\{n : n \in \mathbb{N}$ und durch 3 teilbar$\}$
  $\{n : n \in \mathbb{N}$ und n Primzahl und $n \leq 50\}$
  $\emptyset =_{\text{def}} \{a : a \neq a\}$ (leere Menge)

Operationen auf Mengen.

$A \cap B$	$=_{\text{def}}$	$\{a : a \in A$ und $a \in B\}$	(Durchschnitt von A und B)
$A \cup B$	$=_{\text{def}}$	$\{a : a \in A$ oder $a \in B\}$	(Vereinigung von A und B)
$A \setminus B$	$=_{\text{def}}$	$\{a : a \in A$ und $a \notin B\}$	(Differenz von A und B)
$\overline{A}$	$=_{\text{def}}$	$M \setminus A$	(Komplement von A relativ zu einer festen Grundmenge M)
$\mathcal{P}(A)$	$=_{\text{def}}$	$\{B : B \subseteq A\}$	(Potenzmenge von A)

Gesetze für Mengenoperationen.

$A \cap B$	$=$	$B \cap A$	Kommutativgesetz für den Durchschnitt
$A \cup B$	$=$	$B \cup A$	Kommutativgesetz für die Vereinigung
$A \cap (B \cap C)$	$=$	$(A \cap B) \cap C$	Assoziativgesetz für den Durchschnitt
$A \cup (B \cup C)$	$=$	$(A \cup B) \cup C$	Assoziativgesetz für die Vereinigung
$A \cap (B \cup C)$	$=$	$(A \cap B) \cup (A \cap C)$	Distributivgesetz
$A \cup (B \cap C)$	$=$	$(A \cup B) \cap (A \cup C)$	Distributivgesetz
$A \cap A = A \cup A$	$=$	A	Duplizitätsgesetz
$A \cap (A \cup B)$	$=$	A	Absorptionsgesetz
$A \cup (A \cap B)$	$=$	A	Absorptionsgesetz
$\overline{A \cap B}$	$=$	$(\overline{A} \cup \overline{B})$	de-Morgansche Regel
$\overline{A \cup B}$	$=$	$(\overline{A} \cap \overline{B})$	de-Morgansche Regel
$\overline{\overline{A}}$	$=$	A	Gesetz des doppelten Komplements

Tupel (Vektoren) und Kreuzprodukt.

- $(a_1, a_2, \ldots, a_n) =_{\text{def}}$ Menge der Elemente $a_1, a_2, \ldots, a_n$ in dieser festgelegten Reihenfolge (n-Tupel, n-stelliger Vektor)
- $A_1 \times A_2 \times \ldots \times A_n =_{\text{def}} \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$ (Kreuzprodukt der Mengen $A_1, A_2, \ldots, A_n$)
- $A^n =_{\text{def}} \underbrace{A \times A \times \ldots \times A}_{n-\text{mal}}$ (n-faches Kreuzprodukt der Menge A)

Anzahl.

$\#A =_{\text{def}}$ Anzahl der Elemente der endlichen Menge A

Es gilt:
- $\#(A^n) = (\#A)^n$
- $\#\mathcal{P}(A) = 2^{\#A}$
- $\#A + \#B = \#(A \cup B) + \#(A \cap B)$
- $\#A = \#(A \setminus B) + \#(A \cap B)$

Funktionen.

- f ist Funktion von A nach $B \Leftrightarrow_{\text{def}} f \subseteq A \times B$ und für jedes $a \in A$ gibt es höchstens ein $b \in B$ mit $(a, b) \in f$.
  Schreibweise: $f : A \to B$.
  Ist $(a, b) \in f$, so schreibt man $f(a) = b$.
- Funktion f ist eineindeutig oder injektiv $\Leftrightarrow_{\text{def}}$ aus $f(a_1) = f(a_2)$ folgt $a_1 = a_2$.
- Definitionsbereich der Funktion f ist $D_f =_{\text{def}} \{a :$ es existiert ein b mit $f(a) = b\}$.
- Wertebereich der Funktion f ist $W_f =_{\text{def}} \{b :$ es existiert ein a mit $f(a) = b\}$.
- Funktion $f : A \to B$ ist total $\Leftrightarrow_{\text{def}} D_f = A$.
- Funktion $f : A \to B$ ist surjektiv $\Leftrightarrow_{\text{def}} W_f = B$.
- Funktion f ist bijektiv $\Leftrightarrow_{\text{def}} f$ ist injektiv und surjektiv.
- Ist $f : A \to B$ bijektiv, so existiert die Umkehrfunktion f^{-1} mit
  $f^{-1}(y) =_{\text{def}}$ dasjenige $x \in A$ mit $f(x) = y$.
  Es gilt $f^{-1}(f(x)) = x$ für $x \in A$ und $f(f^{-1}(y)) = y$ für $y \in B$.
- Für $f : A \to B$ und $g : B \to C$ sei $g \circ f : A \to C$ definiert durch $(g \circ f)(x) =_{\text{def}} g(f(x))$.

Relationen.

- R ist n-stellige Relation über $(A_1, A_2, \ldots, A_n) \Leftrightarrow_{\text{def}} R \subseteq A_1 \times A_2 \times \ldots \times A_n$.
- R ist n-stellige Relation über $A \Leftrightarrow_{\text{def}} R \subseteq A^n$.
- Zweistellige Relation R über A ist
  - reflexiv $\Leftrightarrow_{\text{def}} (a, a) \in R$ für alle $a \in A$
  - transitiv $\Leftrightarrow_{\text{def}}$ aus $(a, b), (b, c) \in R$ folgt $(a, c) \in R$
  - symmetrisch $\Leftrightarrow_{\text{def}}$ aus $(a, b) \in R$ folgt $(b, a) \in R$
  - antisymmetrisch $\Leftrightarrow_{\text{def}}$ aus $(a, b), (b, a) \in R$ folgt $a = b$
  - linear $\Leftrightarrow_{\text{def}}$ es gilt $(a, b) \in R$ oder $(b, a) \in R$
  - eine Halbordnung $\Leftrightarrow_{\text{def}}$ R ist reflexiv, transitiv und antisymmetrisch
  - eine Ordnung $\Leftrightarrow_{\text{def}}$ R ist eine lineare Halbordnung
  - eine Äquivalenzrelation $\Leftrightarrow_{\text{def}}$ R ist reflexiv, transitiv und symmetrisch

Wörter und Wortmengen

Alphabet – beliebige Menge von Symbolen (Zeichen, Buchstaben).

Sei Σ beliebiges endliches Alphabet, $n \geq 0$, $a_1, a_2, \ldots, a_n \in \Sigma$.

- $a_1a_2\ldots a_n$ heißt *Wort über* Σ
- $|a_1a_2\ldots a_n| =_{\text{def}} n$ ist die *Länge* des Wortes $a_1a_2\ldots a_n$
- $\Sigma^n =_{\text{def}} \{a_1a_2\ldots a_n : \text{ und } a_1, a_2, \ldots, a_n \in \Sigma\}$
  (alle Wörter über Σ der Länge n)
- $\Sigma^* =_{\text{def}} \{a_1a_2\ldots a_n : n \geq 0 \text{ und } a_1, a_2, \ldots, a_n \in \Sigma\} = \bigcup_{n=0}^{\infty} \Sigma^n$
  (alle Wörter über Σ)
- $\varepsilon =_{\text{def}}$ das Wort, das aus keinem Buchstaben besteht (leeres Wort)
  ($\implies \Sigma^0 = \{\varepsilon\}$)

$L \subseteq \Sigma^*$ heißt *Wortmenge* oder *Sprache* über Σ^*. Seien $L, L' \subseteq \Sigma^*$ und $n \geq 0$.

- $L{\cdot}L' =_{\text{def}} \{wv : w \in L \text{ und } v \in L'\}$ (die *Konkatenation* von L und L')
- $L^n =_{\text{def}} \{w_1w_2\ldots w_n : \text{ und } w_1, w_2, \ldots, w_n \in L\}$
- $L^* =_{\text{def}} \{w_1w_2\ldots w_n : n \geq 0 \text{ und } w_1, w_2, \ldots, w_n \in L\} = \bigcup_{n=0}^{\infty} \mathrm{L}^n$

Binärdarstellung natürlicher Zahlen.

Voraussetzung: Jede natürliche Zahl $n \geq 1$ ist eindeutig darstellbar als
$n = \sum_{i=0}^{k} a_i{\cdot}2^i$ mit $a_k = 1$ und $a_0, a_1, \ldots, a_{k-1} \in \{0,1\}$.

Binärdarstellung $\mathrm{bin} : \mathbb{N} \to \{0,1\}^*$ definiert durch:

- $\mathrm{bin}(0) =_{\text{def}} 0$
- $\mathrm{bin}(n) =_{\text{def}} a_ka_{k-1}\ldots a_1a_0$, falls $n \geq 1$, $n = \sum_{i=0}^{k} a_i{\cdot}2^i$, $a_k = 1$, $a_0, \ldots, a_{k-1} \in \{0,1\}$

Dyadische Darstellung natürlicher Zahlen.

Voraussetzung: Jede natürliche Zahl $n \geq 1$ ist eindeutig darstellbar als
$n = \sum_{i=0}^{k} a_i{\cdot}2^i$ mit $a_0, a_1, \ldots, a_k \in \{1,2\}$.

Dyadische Darstellung $\mathrm{dya} : \mathbb{N} \to \{1,2\}^*$ definiert durch:

- $\mathrm{dya}(0) =_{\text{def}} \varepsilon$
- $\mathrm{dya}(n) =_{\text{def}} a_ka_{k-1}\ldots a_1a_0$, falls $n \geq 1$, $n = \sum_{i=0}^{k} a_i{\cdot}2^i$ und $a_0, a_1, \ldots, a_k \in \{1,2\}$.

$\mathrm{dya} : \mathbb{N} \to \{1,2\}^*$ ist bijektiv. Also gibt es eine Umkehrfunktion $\mathrm{dya}^{-1} : \{1,2\}^* \to \mathbb{N}$. Es gilt

- $\mathrm{dya}(2n{+}a) = \mathrm{dya}(n)a$ für $n \geq 0$ und $a = 1,2$.
- $\mathrm{dya}^{-1}(xa) = 2\mathrm{dya}^{-1}(x){+}a$ für $x \in \{1,2\}^*$ und $a = 1,2$.

Hüllenoperatoren.

Die totale Funktion $\Gamma : \mathcal{P}(M) \to \mathcal{P}(M)$ heißt *Hüllenoperator* über der Menge M, falls für alle Teilmengen $A, B \subseteq M$ gilt:

- $A \subseteq \Gamma(A)$ (Einbettung)
- Aus $A \subseteq B$ folgt $\Gamma(A) \subseteq \Gamma(B)$ (Monotonie)
- $\Gamma(\Gamma(A)) = \Gamma(A)$ (Abgeschlossenheit)

Sei M eine Menge, $A \subseteq M$, $f_i : M^{s_i} \to M$ für $i = 1, \dots k$ und $m > 0$.

$\Gamma^0_{f_1,\dots,f_k}(A) =_{\text{def}} A$

$\Gamma^m_{f_1,\dots,f_k}(A) =_{\text{def}} \Gamma^{m-1}_{f_1,\dots,f_k}(A) \cup \bigcup_{i=1}^k \{f_i(a_1,\dots,a_{s_i}) : a_1,\dots,a_{s_i} \in \Gamma^{m-1}_{f_1,\dots,f_k}(A)\}$

(Die Menge der Elemente von M, die durch höchstens m-fache Anwendung der Funktionen $f_1,\dots,f_k$ aus A erzeugt werden können)

$\Gamma_{f_1,\dots,f_k}(A) =_{\text{def}} \bigcup_{m=0}^\infty \Gamma^m_{f_1,\dots,f_k}(A)$

(Die Menge der Elemente von M, die durch endlichoftmalige Anwendung der Funktionen $f_1,\dots,f_k$ aus A erzeugt werden können)

Es gilt: Die Funktion $\Gamma_{f_1,\dots,f_k} : \mathcal{P}(M) \to \mathcal{P}(M)$ ist ein Hüllenoperator
$\Gamma_{f_1,\dots,f_k} : \mathcal{P}(M) \to \mathcal{P}(M)$ heißt *der durch $f_1,\dots,f_k$ erzeugte algebraischer Hüllenoperator.*

Die Menge $B \subseteq M$ heißt unter $f : M^s \to M$ abgeschlossen, wenn aus $a_1,\dots,a_s \in B$ stets $f(a_1,\dots,a_s) \in B$ folgt. Es gilt:

1. $\Gamma_{f_1,\dots,f_k}(A)$ ist die bzgl. $\subseteq$ kleinste Menge, die A enthält und unter $f_1,\dots,f_k$ abgeschlossen ist.
2. $\Gamma_{f_1,\dots,f_k}(A) = \bigcap\{B : A \subseteq B \text{ und } B \text{ unter } f_1,\dots,f_k \text{ abgeschlossen}\}$

Induktion.
Es geht darum nachzuweisen, daß jedes Element a einer Menge B die Eigenschaft E besitzt.
Wir schreiben kurz $E(a)$ für: a besitzt die Eigenschaft E.

(IA) - Induktionsanfang, (IS) - Induktionsschritt.

1. Variante. Sei M eine Menge, $f_i : M^{s_i} \to M$ für $i = 1, \dots k$, $A \subseteq M$ und $B = \Gamma_{f_1,\dots,f_k}(A)$.

Induktionsprinzip zum Nachweis von $E(a)$ für alle $a \in B$:

Wenn gilt (IA) $E(a)$ für alle $a \in A$ und (IS) aus $E(a_1),\dots,E(a_{s_i})$ folgt $E(f_i(a_1,\dots,a_{s_i}))$ für $i = 1,\dots,k$ und $a_1,\dots,a_{s_i} \in M$, so gilt $E(a)$ für alle $a \in B$.

2. Variante. Es gibt eine totale Funktion $\beta \colon B \to \mathbb{N}$.

Induktionsprinzip zum Nachweis von $E(a)$ für alle $a \in B$:

Wenn gilt (IA) $E(a)$ für alle $a \in B$ mit $\beta(a) \leq n_0$ und (IS) für alle $a \in B$ mit $\beta(a) > n_0$: ist $E(b)$ für alle $b \in B$ mit $\beta(b) < \beta(a)$, so auch $E(a)$, so gilt $E(a)$ für alle $a \in B$.

Ist $B = \mathbb{N}$ und β die Identitätsfunktion, so erhält man den häufig verwendeten Spezialfall des *Induktionsprinzips* zum Nachweis von $E(n)$ für alle $a \in \mathbb{N}$:

Gibt es ein $n_0 \in \mathbb{N}$ mit (IA) $E(n)$ für alle $n \leq n_0$ und (IS) für alle $n > n_0$ gilt: ist $E(m)$ für alle $m < n$ so auch $E(n)$, so gilt $E(n)$ für alle $n \in \mathbb{N}$.