Vorlesung 13

Aussagenlogik, Mengenlehre

13.1 Aussagenlogik

Sei p eine Aussage. Diese ist entweder wahr (w) oder falsch (f). $p \equiv (5+3=8)$ ist wahr, $p \equiv (5+3=7)$ hingegen ist falsch. $5+3$ ist keine Aussage, $5+3=8$ ist eine Aussage. Beispiele für Aussagen sind Gleichungen oder Ungleichungen.

Die Negation einer Aussage p bezeichnen wir mit $\neg p$. Wir haben folgende Wahrheitstafel:

p	$\neg p$
w	f
f	w

Seien nun p und q Aussagen. Diese können wir logisch miteinander verknüpfen und wir erhalten eine neue Aussage. Es gibt

- Konjunktion „und“ $p \wedge q$
- nicht ausschließende Disjunktion „oder“ $p \vee q$
- Implikation „wenn, ..., dann“ $p \Rightarrow q$
- Äquivalenz „genau dann ..., wenn“ $p \Leftrightarrow q$

vermöge der folgenden Wahrheitstafeln:

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	f	w	w	f
f	f	f	f	w	w

Für gewöhnlich benutzen wir die nicht-ausschließende Disjunktion. Die ausschließende Disjunktion „entweder oder“ definieren wir vermöge

p	q	$p\dot{\vee}q$
w	w	f
w	f	w
f	w	w
f	f	f

Wegen

p	q	$p\dot{\vee}q$	$p \vee q$
w	w	f	w
w	f	w	w
f	w	w	w
f	f	f	f

gilt $p\dot{\vee}q \Rightarrow p \vee q$.

Es seien p, q, r Aussagen. Dann gelten für die Elementarverknüpfungen $\neg$, $\wedge$, $\vee$, $\Rightarrow$ und $\Leftrightarrow$ folgende Grundgesetze:

- doppelte Negation: $\neg(\neg p) \Leftrightarrow p$
- Kommutativität (Symmetrie): $p \wedge q \Leftrightarrow q \wedge p$
  $p \vee q \Leftrightarrow q \vee p$
- Assoziativität: $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$
  $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$
- Distributivität: $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
  $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
- De Morgan: $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$
  $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$
- Kontraposition: $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$
- Transitivität: $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$.

Die Grundgesetze werden mittels Wahrheitstafeln bewiesen.

Beispiel:

Beweis von De Morgan $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$. Wir haben folgende Wahrheitstafeln:

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
w	w	f	f	w	f	f
w	f	f	w	f	w	w
f	w	w	f	f	w	w
f	f	w	w	f	w	w

Die Wahrheitswerte in den rechten beiden Spalten stimmen in jeder Zeile überein, deshalb gilt $\neg(p \vee q) \Leftrightarrow \neg p \vee \neg q$. Ebenso gilt $(p \Rightarrow q) \Leftrightarrow \neg p \vee q$.

Das Gesetz der Kontraposition benutzen wir beim Widerspruchsbeweis.

Ausgangsposition: Bezeichnet p die Voraussetzung und q die Behauptung, so ist „$p \Rightarrow q$“ zu zeigen. Stattdessen können wir aber auch die äquivalente Aussage „$\neg q \Rightarrow \neg p$“ zeigen.

Wir nehmen an, die zu beweisende Aussage q ist falsch und folgern, dass dann die Voraussetzung p falsch ist. Widerspruch, da wir wissen, dass p wahr ist.

Beispiel:

Behauptung: Jede natürliche Zahl n besitzt eine Zerlegung als Produkt von Primzahlen, d.h.

$$n = \prod_{k=1}^{m} p_k^{l_k} \quad \text{mit } p_k \text{ prim.}$$

Beweis: Für $n = 1$ haben wir das leere Produkt. Sei nun $n > 1$. Angenommen, es gibt Zahlen, die sich nicht als Produkt von Primzahlen schreiben lassen. Dann gibt es eine kleinste solche Zahl n_0. Somit ist $n_0 > 1$ und keine Primzahl. Da n_0 keine Primzahl ist, gibt es $a, b \in \mathbb{N}$ mit $a, b < n_0$ und $a \cdot b = n_0$. Da n_0 *kleinste* Zahl ohne Primfaktorzerlegung ist, gilt

$$a = \prod p_j \quad \text{und} \quad b = \prod q_k,$$

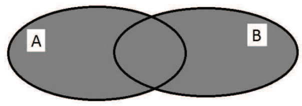
wobei p_j und q_k Primzahlen sind. Damit ist $n_0 = \Pi p_j \cdot \Pi q_k$. Dies ist ein Widerspruch!

13.2 Mengenlehre

Es seien A und B Teilmengen einer Menge X. Mittels logischer Verknüpfungen definieren wir

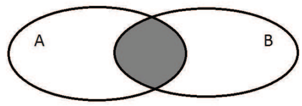
Vereinigung von A und B

$A \cup B := \{x \in X : x \in A \vee x \in B\}$



Schnitt von A und B

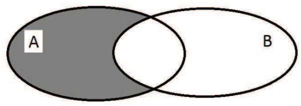
$A \cap B := \{x \in X : x \in A \wedge x \in B\}$



Differenz von A und B

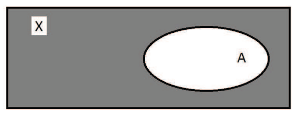
$A \backslash B := A - B := \{x \in A : x \notin B\}$

Bemerke: $A \backslash B = A \cap B^{\mathrm{c}}$



Komplement von A

$A^{\mathrm{c}} := \{x \in X : x \notin A\} (:= {}^{\mathrm{c}}A)$



Die leere Menge, also die Menge, die kein Element enthält, bezeichnen wir mit $\emptyset$ oder auch $\{\}$. Zwei Mengen A und B sind disjunkt, wenn ihr Schnitt leer ist, d.h. $A \cap B = \emptyset$. Mit $\mathfrak{P}(X)$ bezeichnen wir die *Potenzmenge* von X, dies ist die Menge aller Teilmengen von X.

Beispiel:

Sei $X = \{1, 2, 3\}$. Dann ist $\mathfrak{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{3, 2\}, X\}$. Die Potenzmenge von X enthält stets $\emptyset$ und X selbst. Beachte $\mathfrak{P}(\emptyset) = \{\emptyset\}$, damit ist $\{\emptyset\}$ einelementig, aber $\emptyset$ ist nullelementig.

B ist eine Teilmenge von A bzw. A ist eine Obermenge von B, Notation $B \subseteq A$, wenn $\forall x(x \in B \Rightarrow x \in A)$.

Für Mengenoperationen gelten die analogen Gesetze, die wir schon für die logischen Elementarverknüpfungen von Aussagen formuliert haben: Es seien A, B, C Mengen. Dann gilt:

- doppelte Komplementbildung: $(A^c)^c = A$
- Kommutativität : $A \cup B = B \cup A$
  (Symmetrie) $A \cap B = B \cap A$
- Assoziativität: $(A \cup B) \cup C = A \cup (B \cup C)$
  $(A \cap B) \cap C = A \cap (B \cap C)$
- Distributivität: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- De Morgan: $(A \cup B)^c = A^c \cap B^c$
  $(A \cap B)^c = A^c \cup B^c$
- Transitivität: $[(A \subseteq B) \wedge (B \subseteq C)] \Rightarrow A \subseteq C.$

Beispiel: Beweis der Transitivität.

Wir definieren $p \equiv \{x \in A\}$, $q \equiv \{x \in B\}$, $r \equiv \{x \in C\}$. Somit ist zu zeigen

$$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r),$$

aber dies ist die Transitivität für logische Verknüpfungen.

Quantoren

- Wir schreiben „$\exists x \in A : a(x)$" für: Es gibt ein Element aus A, so dass x die Aussage $a(x)$ erfüllt.
- Wir schreiben „$\forall x \in A : a(x)$" für: Für alle Elemente aus A gilt die Aussage $a(x)$.

Beachte:

$$\neg(\exists x \in A : a(x)) \Leftrightarrow \forall x \in A : \neg a(x)$$
$$\neg(\forall x \in A : a(x)) \Leftrightarrow \exists x \in A : \neg a(x)$$

Es sei $f : A \to B$ eine Abbildung. $f^{-1} : \mathfrak{P}(B) \to \mathfrak{P}(A)$ definiert durch

$$f^{-1}(N) := \{x \in A : f(x) \in N\}, \qquad N \in \mathfrak{P}(B) \text{ (d.h. } N \subseteq B)$$

heißt Urbildabbildung. $f^{-1}(N)$ ist das Urbild von N unter f.

Sei $f : A \to B$ eine Funktion. Dann ist f genau dann injektiv, wenn

$$\forall b \in B : |f^{-1}(\{b\})| \leq 1.$$

f ist genau dann surjektiv, wenn

$$\forall b \in B : |f^{-1}(\{b\})| \geq 1.$$

Für das Bild und Urbild von $f : A \to B$ gelten stets

$$f^{-1}(f(M)) \supseteq M \text{ für alle } M \subseteq A, \tag{13.1}$$
$$f(f^{-1}(N)) \subseteq N \text{ für alle } N \subseteq B. \tag{13.2}$$

(13.1) und (13.2) ergeben sich aus den Definitionen von Bild und Urbild.

Zu (13.1): Sei $M \subseteq A$. Nach Definition ist

$$f(M) = \{f(x) \in B : x \in M\}$$

und damit

$$f^{-1}(f(M)) = \{x \in A : f(x) \in f(M)\},$$

dies ist die Teilmenge aus A, die auf $f(M)$ abgebildet werden und enthält daher mindestens auch M selbst.

Analog zu (13.2): Sei $N \subseteq B$.

$$f^{-1}(N) = \{x \in A : f(x) \in N\}$$

und damit

$$\begin{aligned} f(f^{-1}(N)) &= \{f(x) \in B : x \in f^{-1}(N)\} \\ &= \{f(x) \in B : x \in \{x \in A : f(x) \in N\}\} \subseteq N. \end{aligned}$$

Es gelten

(i) f ist genau dann injektiv, wenn in (13.1) Gleichheit gilt.

(ii) f ist genau dann surjektiv, wenn in (13.2) Gleichheit gilt.

Beweis zu (i):

„$\Rightarrow$“:

Sei f injektiv und $M \subseteq A$. Zu zeigen: $f^{-1}(f(M)) = M$ für alle $M \subset A$.

Angenommen, $f^{-1}(f(M)) \supsetneq M$. Dann $f^{-1}(f(M)) = \{x \in A : f(x) \in f(M)\} \supsetneq M$, d.h. es gibt $a \in A \setminus M$ mit $f(a) \in f(M)$. Somit ist f nicht injektiv. Widerspruch!

„$\Leftarrow$“:

Es gelte $f^{-1}(f(M)) = M$ für alle $M \subseteq A$. Zu zeigen: f ist injektiv.

Angenommen, f ist nicht injektiv, d.h. es gibt $a, b \in A$ mit $y = f(a) = f(b)$ und $a \neq b$. Wähle $M = \{a\}$. Dann ist

$$f(M) = \{y\} \Rightarrow f^{-1}(f(M)) = f^{-1}(\{y\}) \supsetneq M,$$

Widerspruch, da $f^{-1}(\{y\})$ mindestens auch noch b enthält.