

**Lösungsvorschläge zu Lineare Algebra für Informatiker und Statistiker**

**Blatt 1**

**Zu Aufgabe 1:**

a) Zu zeigen ist, daß die Aussage

$$(\mathcal{A} \Rightarrow \mathcal{B}) \Longleftrightarrow (\neg \mathcal{A} \vee \mathcal{B})$$

allgemeingültig ist, d.h. der Äquivalenzpfeil unabhängig von den Belegungen von  $\mathcal{A}$  und  $\mathcal{B}$  mit Wahrheitswerten immer den Wahrheitswert "w" (wahr) erhält. Dies erkennt man an der letzten Spalte der folgenden Wahrheitstafel:

| $\mathcal{A}$ | $\mathcal{B}$ | $\mathcal{A} \Rightarrow \mathcal{B}$ | $\neg \mathcal{A}$ | $\neg \mathcal{A} \vee \mathcal{B}$ | $(\mathcal{A} \Rightarrow \mathcal{B}) \Longleftrightarrow (\neg \mathcal{A} \vee \mathcal{B})$ |
|---------------|---------------|---------------------------------------|--------------------|-------------------------------------|---|
| w             | w             | <u>w</u>                              | f                  | <u>w</u>                            | w   |
| w             | f             | <u>f</u>                              | f                  | <u>f</u>                            | w   |
| f             | w             | <u>w</u>                              | w                  | <u>w</u>                            | w   |
| f             | f             | <u>w</u>                              | w                  | <u>w</u>                            | w   |

Die letzte Spalte enthält nur den Wahrheitswert "w", wie gewünscht. Die Wahrheitswerte der letzten Spalte ergeben sich daraus, daß in den Spalten 3 und 5 die (unterstrichenen) Werte jeweils übereinstimmen: genau dann ist nach Vorlesung die Äquivalenz  $\Longleftrightarrow$  wahr.

b) Die Aussage

$$(\mathcal{A} \Rightarrow \mathcal{B}) \Longleftrightarrow (\neg \mathcal{A} \Rightarrow \neg \mathcal{B})$$

ist nicht allgemeingültig, wenn es eine Belegung von  $\mathcal{A}$  und  $\mathcal{B}$  mit Wahrheitswerten gibt, so daß der Äquivalenzpfeil den Wahrheitswert "f" (falsch) erhält. Das ist der folgenden Wahrheitstafel zu entnehmen:

| $\mathcal{A}$ | $\mathcal{B}$ | $\mathcal{A} \Rightarrow \mathcal{B}$ | $\neg \mathcal{A}$ | $\neg \mathcal{B}$ | $\neg \mathcal{A} \Rightarrow \neg \mathcal{B}$ | $(\mathcal{A} \Rightarrow \mathcal{B}) \Longleftrightarrow (\neg \mathcal{A} \Rightarrow \neg \mathcal{B})$ |
|---------------|---------------|---------------------------------------|--------------------|--------------------|---|---|
| w             | w             | <u>w</u>                              | f                  | f                  | <u>w</u>  | w   |
| w             | f             | <u>f</u>                              | f                  | w                  | <u>w</u>  | f   |
| f             | w             | <u>w</u>                              | w                  | f                  | <u>f</u>  | f   |
| f             | f             | <u>w</u>                              | w                  | w                  | <u>w</u>  | w   |

Haben also  $\mathcal{A}$  und  $\mathcal{B}$  verschiedene Wahrheitswerte, so ist die Äquivalenz nicht erfüllt. Damit liegt keine Tautologie vor.

## Zu Aufgabe 2:

Für die Beweise benutzen wir die folgenden Tautologien:

- $\mathcal{A} \wedge \mathcal{A} \iff \mathcal{A} \quad (\star)$
- $\mathcal{A} \vee f \iff \mathcal{A} \quad (\star\star)$

wobei “f” für eine (beliebige) falsche Aussage steht.

Beweis für diese Tautologien durch die Wahrheitstafeln:

| $\mathcal{A}$ | $\mathcal{A} \wedge \mathcal{A}$ | $\mathcal{A} \iff \mathcal{A} \wedge \mathcal{A}$ | $\mathcal{A}$ | $\mathcal{A} \vee f$ | $\mathcal{A} \vee f \iff \mathcal{A}$ |
|---------------|----------------------------------|---|---------------|----------------------|---------------------------------------|
| w             | w                                | w   | w             | w                    | w                                     |
| w             | w                                | w   | w             | w                    | w                                     |
| f             | f                                | w   | f             | f                    | w                                     |
| f             | f                                | w   | f             | f                    | w                                     |

a)  $M \setminus (A \cup B) = (M \setminus A) \cap (M \setminus B)$

Wir beweisen dies mit Hilfe der Definition 0.4 a):

$$\begin{aligned}
 \forall x : x \in M \setminus (A \cup B) & \stackrel{\text{Def.}}{\iff} x \in M \wedge \neg(x \in A \cup B) \\
 & \stackrel{\text{Differenz}}{\iff} \\
 & \stackrel{\text{Def.}}{\iff} x \in M \wedge \neg(x \in A \vee x \in B) \\
 & \stackrel{\cup}{\iff} \\
 & \stackrel{\text{Satz 0.1}}{\iff} x \in M \wedge (\neg(x \in A) \wedge \neg(x \in B)) \\
 & \stackrel{\text{de Morgan}}{\iff} \\
 & \stackrel{\text{Tautologie}}{\iff} (x \in M) \wedge (x \in M) \wedge (\neg(x \in A) \wedge \neg(x \in B)) \\
 & \stackrel{\star}{\iff} \\
 & \stackrel{\text{Satz 0.1}}{\iff} (x \in M \wedge \neg(x \in A)) \wedge (x \in M \wedge \neg(x \in B)) \\
 & \stackrel{\text{Kommutat.}}{\iff} \stackrel{\text{Assoz.}}{\iff} \\
 & \stackrel{\text{Def.}}{\iff} (x \in M \setminus A) \wedge (x \in M \setminus B) \\
 & \stackrel{\text{Differenz}}{\iff} \\
 & \stackrel{\text{Def.}}{\iff} x \in (M \setminus A) \cap (M \setminus B)
 \end{aligned}$$

b)  $M \setminus (A \cup B \cup C) = (M \setminus A) \cap (M \setminus B) \cap (M \setminus C)$

Wir können diese Aussage natürlich wieder anhand der Definition 0.4 a) beweisen, wir können aber auch bereits bewiesene Aussagen der Vorlesung oder der Tutorien oder aus den Übungen zum Beweis verwenden. Hier ziehen wir die Aussage aus Teil a) zum Beweis heran; dafür substituieren wir

$$U := A \cup B$$

$$\begin{aligned}
 M \setminus (A \cup B \cup C) &= M \setminus (U \cup C) \\
 &\stackrel{\text{Teil}}{=} \stackrel{a)}{=} (M \setminus U) \cap (M \setminus C) \\
 &\stackrel{\text{Rück-}}{=} \stackrel{\text{Substitut.}}{=} (M \setminus (A \cup B)) \cap (M \setminus C) \\
 &\stackrel{\text{Teil}}{=} \stackrel{a)}{=} ((M \setminus A) \cap (M \setminus B)) \cap (M \setminus C) \\
 &\stackrel{\text{Satz 0.6}}{=} \stackrel{\text{Assoz.}}{=} (M \setminus A) \cap (M \setminus B) \cap (M \setminus C) \quad \text{q.e.d.}
 \end{aligned}$$

c)  $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$

Beweis:

$$\forall x : x \in (A \cup B) \setminus (A \cap B) \iff$$

$$\begin{array}{l} \text{Def.} \\ \iff \\ \text{Differenz} \end{array} \quad x \in (A \cup B) \wedge \neg(x \in A \cap B)$$

$$\begin{array}{l} \text{Def.} \\ \iff \\ \cup, \cap \end{array} \quad (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B)$$

$$\begin{array}{l} \text{de} \\ \iff \\ \text{Morgan} \end{array} \quad \underbrace{(x \in A \vee x \in B) \wedge (\neg(x \in A) \vee \neg(x \in B))}_{\text{Substituiere}}$$

$$\begin{array}{l} \text{Satz 0.1} \\ \iff \\ \text{Distrib.} \end{array} \quad \left[ (x \in A \vee x \in B) \wedge \neg(x \in A) \right] \vee \left[ (x \in A \vee x \in B) \wedge \neg(x \in B) \right]$$

$$\begin{array}{l} \text{Satz 0.1} \\ \iff \\ \text{Distrib.} \end{array} \quad \underbrace{\left[ (x \in A \wedge \neg(x \in A)) \vee (x \in B \wedge \neg(x \in A)) \right]}_f \vee \underbrace{\left[ (x \in A \wedge \neg(x \in B)) \vee (x \in B \wedge \neg(x \in B)) \right]}_f$$

$$\begin{array}{l} \text{Tautologie} \\ \iff \\ \star\star \end{array} \quad [x \in B \wedge \neg(x \in A)] \vee [x \in A \wedge \neg(x \in B)]$$

$$\begin{array}{l} \text{Def.} \\ \iff \\ \text{Differenz} \end{array} \quad (x \in B \setminus A) \vee (x \in A \setminus B)$$

$$\begin{array}{l} \text{Kommu-} \\ \iff \\ \text{tativitat} \end{array} \quad (x \in A \setminus B) \vee (x \in B \setminus A)$$

$$\begin{array}{l} \text{Def.} \\ \iff \\ \cup \end{array} \quad x \in (A \setminus B) \cup (B \setminus A) \quad \text{q.e.d.}$$

Dabei kennzeichnet “f” wie gewonlich den Wahrheitswert “falsch”.

### Zu Aufgabe 3:

Fur  $p \in \mathbb{N}$  mit  $p \geq 2$  ist zu zeigen:

a)  $p$  ist Primzahl  $\iff [\forall m \in \{1, \dots, p\} : m|p \implies m = 1 \vee m = p]$

Beweis:

Nach Vorlesung Definition 0.12 gilt:

$$p \text{ ist Primzahl} \iff [\forall m \in \mathbb{N} : m|p \implies m = 1 \vee m = p]$$

Zu zeigen ist also mit Satz 0.2 b) der Vorlesung (Transitivitat von „ $\iff$ “):

$$[\forall m \in \mathbb{N} : m|p \implies m = 1 \vee m = p] \iff [\forall m \in \{1, \dots, p\} : m|p \implies m = 1 \vee m = p]$$

Dabei ist die Implikationsrichtung „ $\implies$ “ einfach, denn wenn eine Aussage fur alle  $m \in \mathbb{N}$  richtig ist, so sicher auch fur alle  $m \in \{1, \dots, p\} \subset \mathbb{N}$ .

Es bleibt also nur die Umkehrung „ $\impliedby$ “ zu beweisen, d.h. es ist noch zu zeigen:

$$\forall m \in \mathbb{N} : m|p \implies m = 1 \vee m = p,$$

und zwar unter der Voraussetzung der Richtigkeit der Aussage auf der rechten Seite.

Diese sagt aber gerade, da die Aussage fur  $m \in \{1, \dots, p\}$  wahr ist. Wir machen also eine

Fallunterscheidung:

**Falls**  $1 \leq m \leq p$  : Aussage wahr nach Voraussetzung

**Falls**  $m > p$  : Nach den Teilbarkeitsregeln aus der Vorlesung (0.9) gilt:

$$m|p \implies m \leq |p| = p$$

Mit dem im Tutorium bewiesenen Kontrapositionsgesetz (Satz 0.3 b)) folgt damit:

$$\neg(m \leq p) \implies \neg(m|p)$$

und das heißt gleichwertig:

$$m > p \implies \neg(m|p)$$

Also gilt im Falle  $m > p$ , daß  $\neg(m|p)$  wahr ist, und damit ist nach der Regel „ex falso quodlibet“ die Implikation

$$m|p \implies m = 1 \vee m = p$$

wahr, und das war im zweiten Fall noch zu zeigen. q.e.d.

b)  $p$  ist keine Primzahl  $\iff \exists m \in \{2, \dots, p-1\} : m|p$ .

Beweis:

Wir benutzen die im Teil a) bewiesene Aussage:

$$\begin{array}{ll}
 p \text{ ist keine Primzahl} & \iff \neg(p \text{ ist Primzahl}) \\
 & \stackrel{\substack{\text{Teil} \\ a)}}{\iff} \neg \left[ \forall m \in \{1, \dots, p\} : m|p \implies m = 1 \vee m = p \right] \\
 & \stackrel{\substack{\iff \\ \text{Negation}}}{\iff} \exists m \in \{1, \dots, p\} : m|p \wedge \neg(m = 1 \vee m = p) \\
 & \iff \exists m \in \{1, \dots, p\} : m|p \wedge \neg(m \in \{1, p\}) \\
 & \stackrel{\substack{\text{Definition} \\ \text{Kommutat.}}}{\iff} \exists m : m \in \{1, \dots, p\} \wedge \neg(m \in \{1, p\}) \wedge m|p \\
 & \stackrel{\substack{\iff \\ \text{Assoz.}}}{\iff} \exists m : [m \in \{1, \dots, p\} \wedge \neg(m \in \{1, p\})] \wedge m|p \\
 & \stackrel{\substack{\iff \\ \text{Def.} \\ \text{Differenz}}}{\iff} \exists m : m \in \{1, \dots, p\} \setminus \{1, p\} \wedge m|p \\
 & \iff \exists m : m \in \{2, \dots, p-1\} \wedge m|p \\
 & \stackrel{\substack{\iff \\ \text{Def.}}}{\iff} \exists m \in \{2, \dots, p-1\} : m|p \quad \text{q.e.d.}
 \end{array}$$

#### Zu Aufgabe 4:

Jede natürliche Zahl  $n \geq 2$  läßt sich als Produkt von Primzahlen schreiben.

Zunächst formalisieren wir diese Aussage:

$$\forall n \in \{2, 3, \dots\} \subset \mathbb{N} \exists N \in \mathbb{N} \exists q_1, \dots, q_N : (\forall 1 \leq i \leq N : q_i \text{ Primzahl}) \wedge n = q_1 \cdot q_2 \cdot \dots \cdot q_N$$

Beweis: (mit vollständiger Induktion)

Induktionsanfang:  $n = 2$  :

Wähle  $N = 1$  und  $q_1 = 2$ ; dann ist  $n = 2 = q_1$  geeignet, da 2 selbst Primzahl ist.

Induktionsschritt:  $n \mapsto n + 1$

Induktionsvoraussetzung: Für ein  $n \in \mathbb{N}$  mit  $n \geq 2$  gelte: Für alle  $k \in \mathbb{N}$  mit  $2 \leq k \leq n$  läßt sich  $k$  schreiben als Produkt von Primzahlen, wie in der Formalisierung oben beschrieben, d.h. wir nehmen an, daß die Behauptung für alle Vorgänger  $k \geq 2$  von  $n + 1$  erfüllt ist.

Nun unterscheiden wir zwei Fälle:

**1.Fall:**  $n + 1$  ist eine Primzahl.

Dann wähle wieder  $N = 1$  und  $q_1 = n + 1$ , und dann ist  $n + 1 = q_1$  eine geeignete Darstellung.

**2.Fall:**  $n + 1$  ist keine Primzahl.

Mit Aufgabe 3 b) gibt es dann ein  $m \in \mathbb{N}$  mit  $2 \leq m \leq (n + 1) - 1 = n$  mit  $m|(n + 1)$ ,

d.h. es gibt ein  $k \in \mathbb{Z}$ , so daß  $n + 1 = k \cdot m$ .

Weil  $n + 1$  und  $m$  positiv sind, ist auch  $k$  positiv, d.h.  $k \in \mathbb{N}$  und natürlich  $k|(n + 1)$ , d.h. mit (0.9 a) aus der Vorlesung:  $1 \leq k \leq |n + 1| = n + 1$ .

Wäre  $k = 1$ , so  $n + 1 = k \cdot m = 1 \cdot m = m$ , und das ist falsch, da  $m \in \{2, \dots, n\}$ . Da nach der Definition der Implikation aus einer wahren Aussage niemals eine falsche Aussage folgen kann, muß also  $k = 1$  falsch sein, folglich muß  $k \geq 2$  gelten.

Analog erschließt man  $k < n + 1$ , denn es gilt:

$$k = n + 1 \implies n + 1 = k \cdot m = (n + 1) \cdot m \implies m = 1 \quad \nmid_{m \in \{2, \dots, n\}}.$$

Also gilt  $2 \leq k \leq n$  und  $2 \leq m \leq n$ .

Nun liefert aber die Induktionsvoraussetzung, daß es ein  $N \in \mathbb{N}$  und Primzahlen  $q_1, \dots, q_N \in \mathbb{N}$  gibt mit  $k = q_1 \cdot q_2 \cdot \dots \cdot q_N$  sowie ein  $M \in \mathbb{N}$  und Primzahlen  $p_1, \dots, p_M \in \mathbb{N}$  mit  $m = p_1 \cdot \dots \cdot p_M$

Also:

$$n + 1 = k \cdot m = (q_1 \cdot \dots \cdot q_N) \cdot (p_1 \cdot \dots \cdot p_M)$$

mit Primzahlen  $q_1, \dots, q_N, p_1, \dots, p_M$ ; folglich ist  $n + 1$  als Produkt von Primzahlen darstellbar wie gewünscht.