



Paula Reichert, Tamas Makai

Wintersemester 2025/26

Lineare Algebra (Informatik)

Übungsblatt 3

Aufgabe 1 (Mengen)

- (i) Geben Sie alle Teilmengen der Menge $\{1, 2, 3, 4\}$ an.
- (ii) Wieviele dieser Teilmengen A erfüllen die Bedingung $\{1, 2\} \subsetneq A$?
- (iii) Für wieviele Teilmengen A gilt $2 \in A$, aber nicht $\{1, 2\} \subseteq A$?

Lösung 1

- (i) Die Menge $\{1, 2, 3, 4\}$ hat genau 16 Teilmengen

$$\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \\ \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}$$

- (ii) Das sind genau die Teilmengen, die die Elemente 1 und 2 enthalten, und selber nicht $\{1, 2\}$ sind, also:

$$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 2, 3, 4\}$$

- (iii) Das sind die Teilmengen, die 2 enthalten und gleichzeitig 1 *nicht* enthalten. Es gibt vier davon, nämlich:

$$\{2\}, \{2, 3\}, \{2, 4\}, \{2, 3, 4\}.$$

Aufgabe 2 (Darstellungen von Mengen)

- (i) Vereinfachen Sie: $\mathcal{P}\left(\left(\{0, 1\} \times \{0, 1\}\right) \setminus \left(\{(0, 1)\} \cup \{(1, 1)\}\right)\right)$
- (ii) Vereinfachen Sie: $(\mathbb{N}_0 \setminus \{2n - 1 : n \in \mathbb{N}\}) \times (\mathbb{N} \setminus \{2n : n \in \mathbb{N}_0\})$

Geben Sie dabei alle Schritte an.

Lösung 2

- (i) Wir vereinfachen:

$$\begin{aligned} & \mathcal{P}\left(\left(\{0, 1\} \times \{0, 1\}\right) \setminus \left(\{(0, 1)\} \cup \{(1, 1)\}\right)\right) \\ &= \mathcal{P}(\{(0, 0), (0, 1), (1, 0), (1, 1)\} \setminus \{(0, 1), (1, 1)\}) && [\text{Def. Kreuzprodukt, Vereinigungsmenge}] \\ &= \mathcal{P}(\{(0, 0), (1, 0)\}) && [\text{Def. Differenzmenge}] \\ &= \{\emptyset, \{(0, 0)\}, \{(1, 0)\}, \{(0, 0), (1, 0)\}\} && [\text{Def. Potenzmenge}] \end{aligned}$$

- (ii) Wir vereinfachen

$$\begin{aligned} & (\mathbb{N}_0 \setminus \{2n - 1 : n \in \mathbb{N}\}) \times (\mathbb{N} \setminus \{2n : n \in \mathbb{N}_0\}) \\ &= \{2m : m \in \mathbb{N}_0\} \times \{2n + 1 : n \in \mathbb{N}_0\} && [\text{Def. Differenzmenge}] \\ &= \{(2m, 2n + 1) : m, n \in \mathbb{N}_0\} && [\text{Def. Kreuzprodukt}] \end{aligned}$$

Aufgabe 3 (Rechenregeln auf Mengen)

Sei Ω eine Grundmenge und $A, B, C \subseteq \Omega$. Zeigen Sie:

- (i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- (ii) $(A \cup B)^c = A^c \cap B^c$
- (iii) Sei $\mathcal{I}$ eine nichtleere Indexmenge und $\forall i \in \mathcal{I} : A_i \subseteq \Omega$. Dann gilt:

$$\left(\bigcup_{i \in \mathcal{I}} A_i \right)^c = \bigcap_{i \in \mathcal{I}} A_i^c.$$

Überlegen Sie sich, dass (i)-(iii) analog gelten, wenn man jeweils $\cap$ und $\cup$ vertauscht.

Lösung 3

- (i) Wir müssen zeigen, dass

$$x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C).$$

Es gilt

$$\begin{aligned} & x \in A \cup (B \cap C) \\ \iff & (x \in A) \vee (x \in B \cap C) \\ \iff & (x \in A) \vee (x \in B \wedge x \in C) \end{aligned} \tag{1}$$

und

$$\begin{aligned} & x \in (A \cup B) \cap (A \cup C) \\ \iff & (x \in A \cup B) \wedge (x \in A \cup C) \\ \iff & (x \in A \vee x \in B) \wedge (x \in A \vee x \in C). \end{aligned} \tag{2}$$

Wir zeigen die Äquivalenz der Aussagen (1) und (2) mittels Wahrheitstafeln.

$x \in A$	$x \in B$	$x \in C$	$x \in B \wedge x \in C$	(1)	$x \in A \vee x \in B$	$x \in A \vee x \in C$	(2)
w	w	w	w	w	w	w	w
w	w	f	f	w	w	w	w
w	f	w	f	w	w	w	w
w	f	f	f	w	w	w	w
f	w	w	w	w	w	w	w
f	w	f	f	f	w	f	f
f	f	w	f	f	f	w	f
f	f	f	f	f	f	f	f

□

- (ii) Wir müssen zeigen, dass

$$x \in (A \cup B)^c \iff x \in A^c \cap B^c.$$

Es gilt

$$\begin{aligned} & x \in (A \cup B)^c \\ \iff & x \notin A \cup B \\ \iff & \neg(x \in A \cup B) \\ \iff & \neg(x \in A \vee x \in B) \end{aligned} \tag{3}$$

und

$$\begin{aligned}x &\in A^c \cap B^c \\ \iff (x \in A^c) \wedge (x \in B^c) \\ \iff (x \notin A) \wedge (x \notin B) \\ \iff \neg(x \in A) \wedge \neg(x \in B).\end{aligned}\tag{4}$$

Die Äquivalenz von (3) und (4) haben wir in Übungsblatt 2, Aufgabe 1 (i) gezeigt; das ist die zweite De Morgan Regel. $\square$

(iii) Es gilt

$$\begin{aligned}x &\in \left(\bigcup_{i \in \mathcal{I}} A_i\right)^c \\ \iff \neg \left(x \in \bigcup_{i \in \mathcal{I}} A_i\right) \\ \iff \neg(\exists i \in \mathcal{I} : x \in A_i) \\ \iff \forall i \in \mathcal{I} : \neg(x \in A_i) \\ \iff \forall i \in \mathcal{I} : x \in A_i^c \\ \iff x \in \bigcap_{i \in \mathcal{I}} A_i^c.\end{aligned}$$

$\square$

Aufgabe 4 (Fundamentalsatz der Arithmetik)

Zeigen Sie: Jede natürliche Zahl $n \in \mathbb{N}, n \geq 2$, ist eindeutig als Produkt endlich vieler Primzahlen darstellbar.

Dabei gilt: p ist eine Primzahl $\Leftrightarrow p \in \mathbb{N}, p \geq 2$ und $\forall a \in \mathbb{N} : a \text{ teilt } p \Rightarrow a = 1 \vee a = p$.

Gehen Sie bei Ihrem Beweis wie folgt vor. Zeigen Sie 1) die *Existenz* der Primfaktorzerlegung mittels vollständiger Induktion. Zeigen Sie 2) die *Eindeutigkeit* der Primfaktorzerlegung in den folgenden Schritten:

- (i) Benutzen Sie den Euklidischen Algorithmus (Wechselwegnahme) um zu zeigen, dass für je zwei natürliche Zahlen m, n zwei ganze Zahlen p, q existieren, sodass:

$$\text{ggT}(m, n) = p \cdot m + q \cdot n.$$

- (ii) Benutzen Sie (i), um zu zeigen, dass für natürliche Zahlen m, n und Primzahl p gilt:

$$p \text{ teilt } m \cdot n \Leftrightarrow p \text{ teilt } m \text{ oder } p \text{ teilt } n.$$

Verallgemeinern Sie diese Aussage auf Produkte von mehr als zwei Zahlen.

- (iii) Nehmen Sie nun an, dass es zwei verschiedene Primfaktorzerlegungen gibt und benutzen Sie das Resultat aus (ii) um zu zeigen, dass beide Zerlegungen in allen Faktoren übereinstimmen.

Lösung 4 Wir beweisen zuerst die Existenz einer Primfaktorzerlegung für jede natürliche Zahl $n \geq 2$ mit vollständiger Induktion über n .

Induktionsanfang ($n = 2$): 2 ist prim, also insbesondere ein Produkt von Primzahlen.

Induktionsannahme (IA): alle Zahlen $m \in \mathbb{N}, m \geq 2, m \leq n$ lassen sich als Produkt von Primzahlen darstellen, für festes n .

Induktionsschritt: Angenommen, (IA) gilt für n , und betrachten wir die natürliche Zahl $n + 1$.

Fall 1 $n + 1$ ist prim. Dann ist $n + 1$ der Produkt von Primzahlen.

Fall 2 $n + 1$ ist nicht prim. Nach der Definition von einer Primzahl gibt es also ein $a \in \mathbb{N}$, sodass

1. a teilt $n + 1$, d.h. es gibt ein $b \in \mathbb{N}$ mit $n + 1 = b \cdot a$, und
2. $a \neq 1$ und $a \neq n + 1$.

[Überlegen Sie sich, warum die Verneinung der Definition einer Primzahl tatsächlich äquivalent zu diesen Bedingungen ist.]

Da a ein Teiler von $n + 1$ ist, ist $a \leq n + 1$. Da zusätzlich $a \neq n + 1$ muss $a \leq n$ sein. Und da $a \neq 1$ ist $a \geq 2$, also lässt sich a nach (IA) als Produkt von Primzahlen $a = \prod_{i=1}^k p_i$ schreiben.

Weil $n + 1 = a \cdot b$ und $a \notin \{1, n + 1\}$, können wir ähnlich argumentieren, dass $b \in \mathbb{N}, b \geq 2, b \leq n$, also lässt sich b nach (IA) auch als Primzahlprodukt $b = \prod_{j=1}^l q_j$ darstellen.

Also können wir insgesamt $n + 1$ als Produkt der Primzahlen

$$n + 1 = a \cdot b = p_1 \cdot \dots \cdot p_k \cdot q_1 \cdot \dots \cdot q_l$$

darstellen. □

Nun beweisen wir die Eindeutigkeit dieser Primfaktorzerlegung für alle $n \in \mathbb{N}, n \geq 2$.

- (i) Wir zeigen, dass für alle $m, n \in \mathbb{N}$ gibt es $p, q \in \mathbb{Z}$, sodass

$$\text{ggT}(m, n) = p \cdot m + q \cdot n.$$

(Diese Aussage ist als *Lemma von Bézout* bekannt)

Wir beweisen die Aussage mittels vollständiger Induktion über die Anzahl K der Schritte im euklidischen Algorithmus. Wir bemerken: Für natürliche Zahlen m, n terminiert das euklidische Algorithmus immer nach endlich vielen Schritten.

Wir nehmen oBdA an, dass $m \geq n$.

Induktionsanfang ($K = 1$): Falls der euklidische Algorithmus nach einem Schritt schon terminiert, also

$$m = n_0 \cdot n + 0,$$

dann ist $\text{ggT}(m, n) = n$, und somit gilt

$$\text{ggT}(m, n) = n = m - m + n = m - (n_0 - 1)n.$$

Induktionsannahme (IA): Wir nehmen an, dass für alle Zahlen $\tilde{m}, \tilde{n}$, sodass das euklidische Algorithmus nach höchstens K Schritten terminiert, gibt es ganze Zahlen $\tilde{p}, \tilde{q}$ mit

$$\text{ggT}(\tilde{m}, \tilde{n}) = \tilde{p} \cdot \tilde{m} + \tilde{q} \cdot \tilde{n}.$$

Induktionsschritt: Seien m, n natürliche Zahlen, und wir nehmen an, dass der euklidische Algorithmus nach $K + 1$ Schritten terminiert. Wir betrachten die $K + 1$ Gleichungen des euklidischen Algorithmus:

$$m = n_0 n + r_1 \tag{1}$$

$$n = n_1 r_1 + r_2 \tag{2}$$

$$r_1 = n_2 r_2 + r_3 \tag{3}$$

$\vdots$

$$r_{K-1} = n_K r_K + 0. \tag{K+1}$$

mit $ggT(m, n) = r_K$.

Bemerkung: Die K Gleichungen (2) bis $(K + 1)$ bilden das euklidische Algorithmus für die Zahlen n und r_1 . Somit gibt es nach (IA) ganze Zahlen $\tilde{p}$ und $\tilde{q}$ mit

$$ggT(m, n) = r_K = ggT(n, r_1) = \tilde{p}n + \tilde{q}r_1. \quad (*)$$

Wir können Gleichung (1) wie folgt umstellen:

$$r_1 = m - n_0n$$

Wenn wir die obige Gleichung in $(*)$ einsetzen, bekommen wir:

$$\begin{aligned} ggT(m, n) &= \tilde{p}n + \tilde{q}(m - n_0n) \\ &= \tilde{p}n + \tilde{q}m - \tilde{q}n_0n \\ &= \tilde{q}m + (\tilde{p} - \tilde{q}n_0)n. \end{aligned}$$

Wir haben also ganze Zahlen $p = \tilde{q}$ und $q = \tilde{p} - \tilde{q}n_0$ gefunden, sodass

$$ggT(m, n) = p \cdot m + q \cdot n.$$

(ii) Wir zeigen beide Implikationen.

$\Leftarrow$: Angenommen p teilt m oder p teilt n . Ohne Beschränkung der Allgemeinheit können wir annehmen, dass p m teilt, d.h. es existiert ein $k \in \mathbb{N}$, sodass $m = p \cdot k$. Dann ist

$$mn = (pk)n = p \cdot kn,$$

also teilt p die Zahl mn .

$\Rightarrow$: Wir zeigen: Falls eine Primzahl p mn teilt und p m nicht teilt, dann muss p n teilen.

Sei also p eine solche Primzahl. Da p und m teilerfremd sind, ist $ggT(p, m) = 1$, also nach Teil (i) gibt es $a, b \in \mathbb{Z}$ mit.

$$1 = ap + bm$$

Wir multiplizieren auf beiden Seiten mit n und bekommen:

$$n = (ap + bm)n = apn + bmn.$$

– p teilt apn offenbar

– p teilt mn nach Annahme und mn teilt bmn , also teilt p auch bmn .

Somit teilt p auch $apn + bmn = n$. □

Dass die Aussage auch für endliche Produkte von natürlichen Zahlen gilt, beweisen wir mittels vollständiger Induktion.

Induktionsanfang (2 Faktoren) wurde gerade gezeigt.

Induktionsannahme (IA): Wenn eine Primzahl p das Produkt von n natürlichen $m_1 \cdot \dots \cdot m_n$ Zahlen teilt, dann existiert ein $i \in \{1, \dots, n\}$, sodass p m_i teilt.

Induktionsschritt: Seien $m_1, \dots, m_{n+1}$ natürliche Zahlen und p eine Primzahl, sodass p das Produkt $m_1 \cdot \dots \cdot m_{n+1}$ teilt.

$m_1 \cdot \dots \cdot m_{n+1} = m_1 \cdot (m_2 \cdot \dots \cdot m_{n+1})$, also können wir wie oben argumentieren und sehen, dass p m_1 teilt oder p $m_2 \cdot \dots \cdot m_{n+1}$ teilt. Im ersten Fall sind wir schon fertig, im zweiten Fall teilt p das Produkt von n Zahlen und somit existiert nach (IA) ein $i \in \{1, \dots, n\}$, sodass p m_i teilt. □

(iii) Sei n eine natürliche Zahl mit zwei Primfaktorzerlegungen

$$n = p_1 \cdot \dots \cdot p_k \tag{4}$$

$$n = q_1 \cdot \dots \cdot q_l \tag{5}$$

(Bemerkung: k und l müssen nicht a priori gleich sein. Wir nehmen O.B.d.A. an, dass $k \leq l$.)

p_1 ist ein Teiler von n , also teilt p_1 das Produkt $q_1 \cdot \dots \cdot q_l$. Weil p_1 prim ist muss p_1 nach Aufgabe 1 ein q_j in $\{q_1, \dots, q_l\}$ teilen. Da q_j prim ist (insbesondere ≥ 2) ist dann $p_1 = q_j$. O.B.d.A. können wir annehmen, dass $j = 1$ (ansonsten ordnen wir die Primfaktoren in der zweiten Gleichung um).

Wir können nun in beiden Gleichungen oben durch p_1 bzw. q_1 teilen und bekommen zwei Primfaktorzerlegungen der natürlichen Zahl $\frac{n}{p_1} = \frac{n}{q_1}$. Nach dem selben Argument wie im vorherigen Absatz können wir iterativ zu jedem p_i mit $i \in \{2, \dots, k\}$ den dazugehörigen Primfaktor q_i finden, sodass $p_i = q_i$, und anschließend dadurch teilen.

Also gilt $p_i = q_i$ für alle $i \leq k$. Da Primzahlen stets ≥ 2 sind und $1 = \frac{n}{p_1 \cdot \dots \cdot p_k} = q_{k+1} \cdot \dots \cdot q_l$ gilt, folgern wir, dass $k = l$. Somit haben wir gezeigt, dass beide Primfaktorzerlegungen gleich sind.

(Übung: Schreiben Sie diesen Beweis wie in den vorherigen Teilaufgaben als Induktionsbeweis über k auf.)