LMU

LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MATHEMATISCHES INSTITUT

Paula Reichert, Siddhant Das

Wintersemester 2023/24

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 $A \subseteq \{1, 2\}$?

Lösung:

zu (a) Die Menge $\{1, 2, 3, 4\}$ besitzt insgesamt 16 Teilmengen:

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

zu (b) Dies gilt für die Teilmengen $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 2, 3, 4\}$, also für drei Stück.

zu (c) Wir sondern zunächst die Mengen aus, die $2 \in A$ nicht erfüllen. Übrig bleiben

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

Nun müssen noch die Mengen A mit $A \subseteq \{1, 2\}$ aussortiert werden. Dadurch erhalten wir

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

Es gibt also genau sechs Teilmengen $A \subseteq \{1, 2, 3, 4\}$ für die $2 \in A$, aber nicht $A \subseteq \{1, 2\}$ gilt.

Aufgabe 2 (Darstellungen von Mengen)

(i) Vereinfachen Sie: $\mathcal{P}((\{0, 1\} \times \{0, 1\}) \setminus (\{(0, 1)\} \cup \{(1, 1)\}))$

(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:

(i) Vereinfachen Sie: $\mathcal{P}((\{0, 1\} \times \{0, 1\}) \setminus (\{(0, 1)\} \cup \{(1, 1)\}))$

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

(ii) Vereinfachen Sie: $(\mathbb{N}_0 \setminus \{2n - 1 : n \in \mathbb{N}\}) \times (\mathbb{N} \setminus \{2n : n \in \mathbb{N}_0\})$

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

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 $\bigcap$ und $\bigcup$ vertauscht.

Lösung:

(i)

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow x \in A \vee x \in (B \cap C) \Leftrightarrow (x \in A) \vee (x \in B \wedge x \in C) \\ &\overset{\textbf{Satz 2.1.1} \text{ (Rechenregeln)}}{\Leftrightarrow} \Big((x \in A) \vee (x \in B)\Big) \wedge \Big((x \in A) \vee (x \in C)\Big) \\ &\Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C) \Leftrightarrow (A \cup B) \cap (A \cup C) \ni x. \end{aligned}$$

(ii)

$$\begin{aligned} x \in (A \cup B)^c &\Leftrightarrow \neg(x \in A \cup B) \Leftrightarrow \neg\Big((x \in A) \vee (x \in B)\Big) \\ &\overset{\textbf{Satz 2.1.1} \text{ (De-Morgan-Regeln)}}{\Leftrightarrow} \neg(x \in A) \wedge \neg(x \in B) \\ &\Leftrightarrow (x \in A^c) \wedge (x \in B^c) \Leftrightarrow A^c \cap B^c \ni x. \end{aligned}$$

(See also (iii) below for $\mathcal{I} = \{1, 2\}$ and $A_1 = A$ and $B_1 = B$.)

(iii)

$$x \in \left(\bigcup_{i\in\mathcal{I}} A_i\right)^c \Leftrightarrow \neg\,(\exists\, i \in \mathcal{I} \,:\, x \in A_i) \Leftrightarrow \Big(\forall\, i \in \mathcal{I} \,:\, \neg(x \in A_i)\Big) \Leftrightarrow (\forall\, i \in \mathcal{I} \,:\, x \in A_i^c) \Leftrightarrow \bigcap_{i\in\mathcal{I}} A_i^c \ni x.$$

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 $\forall a \in \mathbb{N} : a$ 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:

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

(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:

1) We prove the following statement using mathematical induction

$$\mathcal{A}(n): \ n \text{ has a prime factorization } \forall\, n \in \mathbb{N} \,\wedge\, n \geq 2.$$

First, $\mathcal{A}(2)$ is true since 2 is a prime number. Now, suppose $\mathcal{A}(k)$ holds $\forall\, k \in \mathbb{N} : 2 \leq k < n$ (induction hypothesis). To complete the proof, we show that the induction hypothesis $\Rightarrow \mathcal{A}(n)$. If n is prime, $\mathcal{A}(n)$ holds trivially. Otherwise, there exists $a, b \in \mathbb{N} \,\wedge\, a, b < n : n = ab$ (i.e., n is a composite number). By the induction hypothesis, $a = p_1 p_2 \ldots p_k$ and $b = q_1 q_2 \ldots q_j$ are products of primes. This implies, $n = ab = p_1 p_2 \ldots p_k q_1 q_2 \ldots q_j$ is a product of finitely many primes.

2) (i) Let $m \geq n$ without loss of generality. Applying the Euclidean algorithm:

$$\begin{aligned}
m &= q_1 \cdot n + r_1, & 0 \leq r_1 < n && (1)\\
n &= q_2 \cdot r_1 + r_2, & 0 \leq r_2 < r_1 && (2)\\
r_1 &= q_3 \cdot r_2 + r_3, & 0 \leq r_3 < r_2 && (3)\\
r_2 &= q_4 \cdot r_3 + r_4, & 0 \leq r_4 < r_3 && (4)\\
&\cdots \\
r_{N-1} &= q_{N-1} \cdot r_N + 0, & 0 \leq r_N. && (5)
\end{aligned}$$

It follows that $ggT(m, n) = r_N$. However, we have

$$r_1 \overset{(1)}{=} m - q_1 \cdot n \Rightarrow r_2 \overset{(2)}{=} n - q_2 \cdot r_1 = n - q_2 \cdot (m - q_1 \cdot n) = a_1 \cdot m + b_1 \cdot n, \tag{6}$$

where $a_1 := -\, q_2 \in \mathbb{Z}$ and $b_1 := 1 - q_1 \in \mathbb{Z}$. Similarly,

$$r_3 \overset{(3)}{=} r_1 - q_3 \cdot r_2 \overset{(1) \wedge (3)}{=} (m - q_1 \cdot n) - q_3 \cdot (a_1 \cdot m + b_1 \cdot n) = a_2 \cdot m + b_2 \cdot n, \tag{7}$$

introducing $a_2 := 1 - q_3 \cdot a_1 \in \mathbb{Z}$, and $b_2 := -\, q_1 - q_3 \cdot b_1 \in \mathbb{Z}$. Continuing in this way, one finds $r_4 = a_3 \cdot m + b_3 \cdot n$, where $a, b \in \mathbb{Z}$, and so on, until $r_N = a_{N-1} \cdot m + b_{N-1} \cdot n = ggT(m, n)$, $a_{N-1}, b_{N-1} \in \mathbb{Z}$. This completes the proof.

(ii) suppose a prime number p divides $m \cdot n \,(= mn)$ so that $mn = kp$, $k \in \mathbb{N}$. Furthermore, assume that p is not a divisor of m. Since p is prime, $ggT(p, m) = 1$, and using (i), $\exists\, a, b \in \mathbb{Z} : 1 = ap + bm$. It follows that

$$n \cdot 1 = n \cdot (ap + bm) = apn + bmn = apn + b(kp) = (an + bk)p$$

and p divides n. The case of products of several terms follows by induction at the length of the expression (i.e., the number of factors in the product).

(iii) Suppose, there exist integers with two *distinct* prime factorizations. Let n be the smallest such integer and write $n = p_1 p_2 \ldots p_l = q_1 q_2 \ldots q_k$, where each p_i and q_j is prime. We see that p_1 divides $q_1 q_2 \ldots q_k$, so p_1 divides some q_j by (ii). Without loss of generality, say, p_1 divides q_3. Since p_1 and q_3 are both prime, it follows that $p_1 = q_3$. Returning to our two factorizations of n, we may cancel these two factors to conclude that $p_2 \ldots p_l = q_1 q_2 q_4 \ldots q_k$. Note that the product of primes on the left-hand and right-hand sides are each strictly smaller than n following cancellation. Therefore, we now have two distinct prime factorizations of some integer strictly smaller than n, which contradicts the minimality of n.