Tutorium: Diskrete Mathematik

Vorbereitung der Bonusklausur am 19.01.2023 (Teil 1)

11. Januar 2023

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

Mengen

Definition

Eine *Menge* ist eine ungeordnete Ansammlung von Elementen:

- Die Reihenfolge der Elemente spielt keine Rolle.
- Jedes Element ist genau einmal enthalten.

Dürfen die Elemente mehrfach vorkommen, so spricht man von einer *Multimenge*.

Enthält die Menge keine Elemente, so nennt man sie die *leere Menge* und bezeichnet sie mit $\emptyset$.

Mächtigkeit einer Menge

Unter der *Mächtigkeit* $|M|$ einer (endlichen) Menge M versteht man die Anzahl der in M enthaltenen Elemente. Die Mächtigkeit einer Menge wird auch als *Kardinalität* bezeichnet.

Für die Mächtigkeit einer unendlichen Menge schreibt man häufig ∞.

Beispiele:

$$A = \left\{11, 13, 17, 19\right\}$$

$$\left|A\right| = 4$$

$$B = \left\{\dots, -4, -2, 0, 2, 4, \dots\right\}$$

$$\left|B\right| = \infty$$

Vergleichen von Mengen I

Mengen können miteinander verglichen werden.

- *Inklusion*: $A \subseteq B$

  Die Menge A ist vollständig in der Menge B enthalten. Es ist außerdem möglich, dass A und B identisch sind.
  Sprechweise: A ist eine *Teilmenge* von B.

- *Gleichheit*: $A = B$

  Die Mengen A und B sind identisch. Dies ist genau dann der Fall, wenn sowohl $A \subseteq B$ als auch $B \subseteq A$ gilt.
  Sprechweise: A ist gleich B.

Vergleichen von Mengen II

- *strenge Inklusion*: $A \subset B$

  Die Menge A ist vollständig in der Menge B enthalten. Die Mengen A und B sind jedoch nicht identisch. Jedes Element $a \in A$ ist folglich in B enthalten, es gibt jedoch mindestens ein Element $b \in B$, dass nicht in der Menge A enthalten ist. **Sprechweise**: A ist eine *echte Teilmenge* von B.

Trifft keine der genannten Eigenschaften zu, so sind die Mengen *unvergleichbar*.

Operationen auf Mengen I

- *Vereinigung*: $A \cup B$

  In der Menge $A \cup B$ sind alle Elemente enthalten, die entweder in der Menge A, in der Menge B oder in beiden Mengen vorkommen:

$$A \cup B = \Big\{ x \;\Big|\; x \in A \text{ oder } x \in B \Big\}.$$

  Die *Vereinigungsmenge* von $n \geq 2$ Mengen $A_1, \ldots, A_n$ kann auch wie folgt geschrieben werden:

$$\begin{aligned} \bigcup_{i=1}^{n} A_i &= A_1 \cup A_2 \cup \ldots \cup A_n \\ &= \Big\{ x \;\Big|\; x \in A_1 \text{ oder } x \in A_2 \text{ oder } \ldots \text{ oder } x \in A_n \Big\}. \end{aligned}$$

Operationen auf Mengen II

- *Schnitt*: $A \cap B$

  In der Menge $A \cap B$ sind alle Elemente enthalten, die sowohl in der Menge A als auch in der Menge B vorkommen:

  $$A \cap B = \left\{ x \mid x \in A \text{ und } x \in B \right\}.$$

  Die *Schnittmenge* von $n \geq 2$ Mengen $A_1, \ldots, A_n$ kann auch wie folgt geschrieben werden:

  $$\begin{aligned} \bigcap_{i=1}^{n} A_i &= A_1 \cap A_2 \cap \ldots \cap A_n \\ &= \left\{ x \mid x \in A_1 \text{ und } x \in A_2 \text{ und } \ldots \text{ und } x \in A_n \right\}. \end{aligned}$$

Operationen auf Mengen III

- *Exklusion*: $A \setminus B$

  In der Menge $A \setminus B$ sind alle Elemente enthalten, die in der Menge A, aber nicht in der Menge B vorkommen:

$$A \setminus B = \left\{ x \;\middle|\; x \in A \text{ und } x \notin B \right\}.$$

- *Symmetrische Differenz*: $A \triangle B$

  In der Menge $A \triangle B$ sind alle Elemente enthalten, die entweder nur in der Menge A oder nur in der Menge B vorkommen:

$$A \triangle B = \left(A \setminus B \right) \cup \left(B \setminus A \right).$$

Operationen auf Mengen IV

- *Kartesisches Produkt*: $A \times B$

Es seien A und B zwei Mengen. Das *kartesische Produkt* dieser Mengen ist wie folgt definiert:

$$A \times B = \Big\{(a, b) \;\Big|\; a \in A \text{ und } b \in B\Big\}.$$

Es seien A, B und C drei Mengen. Das *kartesische Produkt* dieser Mengen ist wie folgt definiert:

$$A \times B \times C = \Big\{(a, b, c) \;\Big|\; a \in A,\ b \in B \text{ und } c \in C\Big\}.$$

Analog definiert man das *kartesische Produkt* für eine beliebige Anzahl von Mengen $A_1, \ldots, A_n$:

$$A_1 \times \ldots \times A_n = \Big\{(a_1, \ldots, a_n) \;\Big|\; a_1 \in A_1,\ \ldots,\ a_n \in A_n\Big\}.$$

Operationen auf Mengen V

- *Potenzmenge*: $\mathcal{P}(A)$

  Die Potenzmenge $\mathcal{P}(A)$ ist die Menge aller Teilmengen der Menge A. Enthält die Menge A insgesamt $|A| = n$ Elemente, so enthält die Potenzmenge $\mathcal{P}(A)$ insgesamt $|\mathcal{P}(A)| = 2^n$ Elemente.

Operationen auf Mengen VI

- *Komplement*: $\overline{A}$

  Sei $A \subseteq M$ eine Teilmenge von M. Beim Komplement $\overline{A}$ bzgl. der Menge M handelt es sich um diejenigen Elemente, die in M, aber nicht in A enthalten sind.

$$\overline{A} = M \setminus A$$

Aufgaben

Aufgabe 1

Bestimme die Potenzmenge $\mathcal{P}(M)$ der Menge $M = \{1, a, \emptyset\}$.

Aufgaben

Aufgabe 2

Gegeben seien die Mengen $A = \emptyset$, $B = \{1, 2, 3\}$ und $C = \{2, 3, 4\}$. Bestimme die Menge $\mathcal{P}(\mathcal{P}(A)) \times (B \triangle C)$.

Aufgaben

Aufgabe 3

Es sei $M = \{1, 2\}$. Welche der folgenden Aussagen sind wahr? Welche sind falsch?

(i) $1 \in \mathcal{P}(M)$

(ii) $2 \subseteq \mathcal{P}(M)$

(iii) $\{1, 2\} \in \mathcal{P}(M)$

(iv) $\{1, 2\} \subseteq \mathcal{P}(M)$

(v) $\{1, \{1\}\} \in \mathcal{P}(M)$

(vi) $\{\{1\}, \{2\}\} \in \mathcal{P}(\mathcal{P}(M))$

(vii) $\{\{1\}, \{2\}\} \subseteq \mathcal{P}(M)$

(viii) $\{\{1\}, \{2\}\} \in \mathcal{P}(M)$

(ix) $\{(1, 2)\} \subseteq \mathcal{P}(M)$

Aufgaben

Aufgabe 4

Zeige mithilfe des Wahrheitstafelverfahrens die Gültigkeit des folgenden Distributivgesetzes.

$$A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$$

Abbildungen

Definition I

Eine *Funktion* (oder *Abbildung*) $f : A \to B$ stellt eine *Abbildungsvorschrift* dar, die jedem Element der Menge A ein Element der Menge B zuordnet.

Eine Funktion kann formal wie folgt geschrieben werden:

$$\begin{aligned} f : A &\to B \\ a &\mapsto f(a). \end{aligned}$$

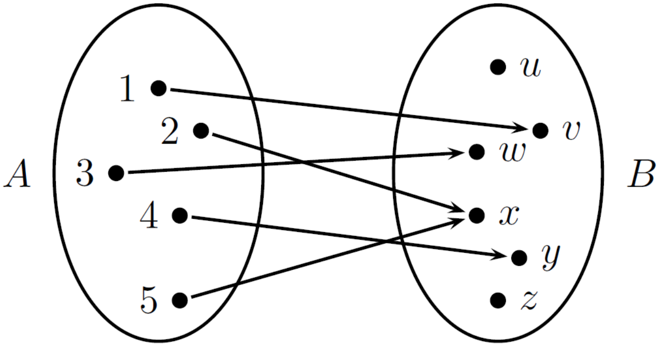
Definition II

Bezeichnungen:

- A: *Definitionsbereich, Urbildmenge*
- B: *Bildmenge, Bildbereich*
- $A \to B$: *Signatur*
- $a \mapsto f(a)$: *Funktionsvorschrift, Abbildungsvorschrift*
- *Wertebereich*: $W_f := f(A) = \Big\{ f(a) : a \in A \Big\}$.
  Nicht alle Elemente von B müssen ein Urbild haben. Es gilt $f(A) \subseteq B$.

Definition III

Grafisch lässt sich eine Abbildung wie folgt veranschaulichen:



Eigenschaften von Abbildungen I

Man nennt eine Abbildung $f : A \to B$

- *injektiv*, falls für alle $a_1, a_2 \in A$ gilt: Aus $a_1 \neq a_2$ folgt stets $f(a_1) \neq f(a_2)$;
- *surjektiv*, falls es zu jedem $b \in B$ mindestens ein $a \in A$ gibt, für das $f(a) = b$ gilt;
- *bijektiv*, falls sie injektiv und surjektiv ist.

Aufgaben

Aufgabe 5

Entscheide für die folgenden Abbildungen, ob sie injektiv sind. Gib jeweils eine (kurze) Begründung.

a) $\mathbb{Z} \to \mathbb{Z},\ f(n) = 23n - 6$

b) $\mathbb{Z} \to \mathbb{Z},\ f(n) = \left(n + 5\right)^2$

c) $\mathbb{N} \to \mathbb{Z},\ f(n) = \left(n - 5\right)^2$

d) $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z},\ f(n) = \left((n + 2)^2, n^2 - 1\right)$

e) $\mathbb{N} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z},\ f(a, b) = \left(ba, 5a + 1\right)$

f) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ f(n, m) = 5n - 2m$

g) $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q},\ f(x, y) = \left(2xy^3, xy^3 + 4y - 1, (y^2 - 6)x\right)$

Aufgaben

Aufgabe 6

Entscheide für die folgenden Abbildungen, ob sie surjektiv sind. Gib jeweils eine (kurze) Begründung.

a) $\mathbb{Z} \to \mathbb{Z},\ f(n) = 42n - 11$

b) $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z},\ f(n) = \left((n+5)^2, n^2\right)$

c) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z},\ f(n, m) = \left(2n + m - 3, n + 5\right)$

d) $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \times \mathbb{Q},\ f(n, m) = \left(2n + m, n - 3m\right)$

e) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ f(n, m) = 5n - m$

f) $\mathbb{N} \times \mathbb{N} \to \mathbb{N},\ f(n, m) = n + m$

Aufgaben

Aufgabe 7

Gibt es bijektive Abbildungen $\mathbb{N} \to \mathbb{Z}$?

Gib im Falle der Existenz eine solche Abbildung an; begründe im Fall der Nicht-Existenz, wieso eine solche Abbildung nicht existiert.

Aufgaben

Aufgabe 8

Gibt es bijektive Abbildungen $\mathbb{Z} \to \mathbb{Z}^2$?

Gib im Falle der Existenz eine solche Abbildung an; begründe im Fall der Nicht-Existenz, wieso eine solche Abbildung nicht existiert.

Vollständige Induktion

Vollständige Induktion I

Vollständige Induktion als Beweismethode wird bei Problemen der folgenden Art angewandt: Für jede natürliche Zahl n sei $A(n)$ eine Aussage. Es soll bewiesen werden, dass $A(n)$ für alle natürlichen Zahlen n gilt, d.h., es soll die Gültigkeit der unendlich vielen Aussagen $A(1)$, $A(2)$, $A(3)$, $\ldots$ nachgewiesen werden.

Vollständige Induktion II

Um eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ zu beweisen, genügt es, Folgendes zu zeigen:

(I) *Induktionsanfang*

$A(1)$ ist richtig.

(II) *Induktionsschritt*

Für jedes $n \in \mathbb{N}$ gilt: Falls $A(n)$ richtig ist, so ist auch die Aussage $A(n+1)$ richtig.

Aufgaben

Aufgabe 9

Beweise durch vollständige Induktion!

a) Für alle $n \in \mathbb{N}_0$ gilt: $\sum\limits_{k=0}^{n} 2^k = 2^{n+1} - 1$.

b) Für alle $n \in \mathbb{N}$ gilt: $\sum\limits_{i=1}^{n} \left(4i - 1\right) = 2n^2 + n$.

c) Für alle $n \in \mathbb{N}_0$ gilt: $9 \mid \left(n^3 + (n+1)^3 + (n+2)^3\right)$.

d) Für alle $n \in \mathbb{N}_0$ gilt: $7 \mid \left(2^{3n} + 13\right)$.

Aufgaben

Aufgabe 10

Beweise durch vollständige Induktion!

a) Für alle $n \in \mathbb{N}$ mit $n \geq 4$ gilt: $\displaystyle\sum_{k=4}^{n} \binom{k}{4} = \binom{n+1}{n-4}$.

b) Für alle $n \in \mathbb{N}_0$ gilt: $\sum_{i=0}^{n} q^i = \frac{1-q^{n+1}}{1-q}$.

c) Für alle $n \in \mathbb{N}$ mit $n > n_0$ gilt: $2^n > n^5$. (Das Finden des Werts n_0 ist Teil der Aufgabe.)

Teilbarkeit

Teilbarkeit I

Man nennt b einen *Teiler* von a und schreibt $b \mid a$, falls es ein c gibt, für das $a = b \cdot c$ gilt (für $a, b, c \in \mathbb{Z}$).

Teilbarkeit II

Es gelten die folgenden Eigenschaften:

- Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.
- Aus $a_1 \mid b_1$ und $a_2 \mid b_2$ folgt $a_1 \cdot a_2 \mid b_1 \cdot b_2$.
- Aus $a \mid b_1$ und $a \mid b_2$ folgt für alle $c_1, c_2 \in \mathbb{Z}$ die Beziehung $a \mid (c_1 b_1 + c_2 b_2)$.

Teilbarkeit III

Bei der Teilbarkeitsrelation $|$ handelt es sich um eine Ordnungsrelation.

Teilbarkeit IV

Aufgabe 11

Beweise die folgende Aussage!

Aus $a \mid b_1$ und $a \mid b_2$ folgt für alle $c_1, c_2 \in \mathbb{Z}$ die Beziehung $a \mid (c_1 b_1 \pm c_2 b_2)$.

Teilbarkeit V

Aufgabe 12

Was ist von der folgenden Aussage zu halten? Begründe deine Antwort!

$$\text{Aus } a_1 \mid b_1 \text{ und } a_2 \mid b_2 \text{ folgt } (a_1 - a_2) \mid (b_1 + b_2).$$

Größter gemeinsamer Teiler

Der *größte gemeinsame Teiler (ggT)* zweier Zahlen kann über ihre *Primfaktorzerlegung* bestimmt werden. Hierfür verwendet man die Primfaktoren, die in beiden Zerlegungen vorkommen, und als zugehörigen Exponenten den jeweils kleineren der Ausgangsexponenten:

$$3.780 = 2^{2} \cdot 3^{3} \cdot 5^{1} \cdot 7^{1}$$
$$3.600 = 2^{4} \cdot 3^{2} \cdot 5^{2}$$

Für den ggT ergibt sich folglich:

$$\mathrm{ggT}(3.600, 3.780) = 2^{2} \cdot 3^{2} \cdot 5^{1} = 180.$$

Alternativ kann der ggT mithilfe des *Euklidischen Algorithmus* berechnet werden.

Kleinstes gemeinsames Vielfaches

Das *kleinste gemeinsame Vielfache (kgV)* zweier Zahlen kann über ihre *Primfaktorzerlegung* bestimmt werden. Hierfür verwendet man die Primfaktoren, die in den Zerlegungen vorkommen, und als zugehörigen Exponenten den jeweils größeren der Ausgangsexponenten:

$$3.780 = 2^{2} \cdot 3^{3} \cdot 5^{1} \cdot 7^{1}$$
$$3.600 = 2^{4} \cdot 3^{2} \cdot 5^{2}$$

Für den kgV ergibt sich folglich:

$$\text{kgV}(3.600, 3.780) = 2^{4} \cdot 3^{3} \cdot 5^{2} \cdot 7^{1} = 75.600.$$

Alternativ kann der kgV mithilfe des ggT berechnet werden.

Zusammenhang zwischen ggT und kgV

Für zwei Zahlen a und b gilt der folgende Zusammenhang zwischen dem größten gemeinsamen Teiler und dem kleinsten gemeinsamen Vielfachen:

$$a \cdot b = \text{ggT}(a, b) \cdot \text{kgV}(a, b).$$

Dieser kann insbesondere genutzt werden, um das kleinste gemeinsame Vielfache effizient mithilfe des Euklidischen Algorithmus zu bestimmen. Es gilt:

$$\text{kgV}(a, b) = \frac{a \cdot b}{\text{ggT}(a, b)}$$

Euklidischer Algorithmus I

Gegeben seien zwei natürliche Zahlen a und b mit $b \leq a$, deren *größter gemeinsamer Teiler* $\mathrm{ggT}(a, b)$ bestimmt werden soll. Hierzu wird zunächst eine *Zerlegung mit Rest* bestimmt, d.h., es werden ganze Zahlen q_1, r_1 mit $0 \leq r_1 < b$ bestimmt, für die gilt:

$$a = q_1 \cdot b + r_1.$$

Die Grundidee des Euklidischen Algorithmus beruht auf der Tatsache, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_1)$ gilt. Anstelle des größten gemeinsamen Teilers von a und b kann also auch der größte gemeinsame Teiler von $r_0 = b$ und r_1 berechnet werden. Hierzu wird wieder eine Zerlegung mit Rest vorgenommen:

$$r_0 = q_2 \cdot r_1 + r_2.$$

Euklidischer Algorithmus II

Wie zuvor gilt $\text{ggT}(r_0, r_1) = \text{ggT}(r_1, r_2)$ und somit auch $\text{ggT}(a, b) = \text{ggT}(r_1, r_2)$. Dieses Verfahren wird nun solange wiederholt, bis der Rest 0 auftritt.

$$r_1 = q_3 \cdot r_2 + r_3$$

$$\vdots$$

$$r_{n-1} = q_{n+1} \cdot r_n + 0$$

Die letzte Zeile bedeutet, dass r_{n-1} ein ganzzahliges Vielfaches von r_n ist – hieraus folgt direkt $\text{ggT}(r_{n-1}, r_n) = r_n$ und somit $\text{ggT}(a, b) = r_n$.

Aufgaben

Aufgabe 13

Gegeben seien die ganzen Zahlen $a = 420$ und $b = 900$. Bestimme das kleinste gemeinsame Vielfache $\mathrm{kgV}(a, b)$

a) mithilfe einer Primfaktorzerlegung;

b) mithilfe des Euklidischen Algorithmus.

Kongruenz I

Gegeben seien zwei ganze Zahlen $a, b \in \mathbb{Z}$ sowie eine natürliche Zahl $m \in \mathbb{N}$. Man nennt a und b

- *kongruent modulo* m und schreibt $a \equiv b \pmod{m}$, falls $m \mid (a - b)$ gilt;
- *inkongruent modulo* m und schreibt $a \not\equiv b \pmod{m}$, falls $m \nmid (a - b)$ gilt.

Sind a und b kongruent modulo m, so lassen a und b bei Ganzzahldivision durch m folglich denselben Rest.

Kongruenz II

Aufgabe 14

Wahr oder falsch? Gib jeweils eine kurze Begründung.

a) $27 \equiv 464 \pmod{23}$

b) $-4 \equiv 4 \pmod{9}$

c) $-213 \equiv 462 \pmod{3}$

d) $2048 \equiv 3172 \pmod{4}$

Kongruenz III

Es gelten die folgenden Rechenregeln:

(i) $a \equiv a \pmod{m}$

(ii) $a \equiv b \pmod{m} \Leftrightarrow b \equiv a \pmod{m}$

(iii) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

(iv) $a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$

(v) $a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$

(vi) $a_1 \equiv b_1 \pmod{m} \wedge a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$

(vii) $a \equiv b \pmod{m} \Leftrightarrow -a \equiv -b \pmod{m}$

(viii) Gilt $\mathrm{ggT}(c, m) = 1$, so folgt aus $c \cdot a \equiv c \cdot b \pmod{m}$ die Kongruenz $a \equiv b \pmod{m}$.