

Übungsblatt 8

Technische Hochschule Mittelhessen, Fachbereich MNI, Diskrete Mathematik, Prof. Dr. B. Just

Aufgabe 1

- Es sei $f : \{0, 1, \dots, 6\} \rightarrow \{0, 1, \dots, 6\}$, $x \mapsto 3 \cdot x \bmod 7$. Bitte entscheiden Sie (mit Begründung), ob f injektiv, bijektiv und / oder surjektiv ist.
- Bitte bestimmen Sie das Urbild $f^{-1}(\{2, 3\})$ für die Abbildung f aus Teil a..
- Es sei $f : \{0, 1, \dots, 5\} \rightarrow \{0, 1, \dots, 5\}$, $x \mapsto 3 \cdot x \bmod 6$. Bitte entscheiden Sie (mit Begründung), ob f injektiv, bijektiv und / oder surjektiv ist.
- Bitte bestimmen Sie das Urbild $f^{-1}(\{2, 3\})$ für die Abbildung f aus Teil c..
- Warum sind die Ergebnisse aus Teil a. und c. unterschiedlich?
- (Anspruchsvoll) Für welche $n \in \mathbb{N}$ ist $f : \{0, 1, \dots, n-1\} \rightarrow \{0, 1, \dots, n-1\}$, $x \mapsto 3 \cdot x \bmod n$ bijektiv?

Aufgabe 2

Es seien D und M endliche Mengen. Bitte zeigen Sie, dass genau dann eine bijektive Abbildung von D nach M existiert, wenn die Anzahl der Elemente von D und die Zahl der Elemente von M gleich ist.

(Anmerkung: „genau dann“ bedeutet, dass beide Aussagen äquivalent sind.)

Aufgabe 3

Bitte machen Sie sich mit einer Zeichnung und selbst gewählter Abbildungen f und g klar:

- Ist f bijektiv, so ist $f^{-1} \circ f$ die Identität, die jedem Element es selbst zuordnet.
- Sind f und g bijektiv, so ist $g \circ f$ auch bijektiv, und es ist $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Aufgabe 4

Im Unendlichen geschehen Dinge, die der Anschauung zunächst widersprechen: Es kann surjektive Abbildungen einer Menge M in die Menge $M \times M$ geben. Hier kommt ein Beispiel.

M sei die Menge aller Dezimaldarstellungen mit einer 0 vor dem Komma, also $M = \{0.x_1x_2x_3x_4\dots : \forall i \in \mathbb{N} : x_i \in \{0, 1, 2, \dots, 9\}\}$.

Bitte zeigen Sie, dass die Abbildung

$$f : M \rightarrow M \times M \\ 0.x_1x_2x_3x_4\dots \mapsto (0.x_1x_3x_5x_7\dots, 0.x_2x_4x_6x_8\dots),$$

die x „aufspaltet“ in die ungeraden und die geraden Dezimalstellen, surjektiv ist.

Aufgabe 5

(Excel-Funktion Rest(Zahl, Modul) oder zumindest ein Taschenrechner empfohlen)

Wie wird im RSA-Verschlüsselungssystem verschlüsselt und entschlüsselt, wenn der Empfänger als öffentlichen Schlüssel $n = 187$ und $e = 13$ bekannt gegeben hat, und der Sender die Nachricht $x = 57$ an ihn schicken möchte?

Viel Spass und Erfolg!