Übungsblatt 8 - Musterlösung

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

Aufgabe 1

a) Die Wertetabelle der Funktion ist:

x	$f(x) = 3 \cdot x \bmod 7$
0	0
1	3
2	6
3	2
4	5
5	1
6	4

Jedes Element aus $\{0, 1, .., 6\}$ wird genau einmal getroffen, also ist f injektiv und surjektiv, mithin bijektiv.

b)

Man liest ab (oder rechnet nach) $f^{-1}(\{2, 3\}) = \{1, 3\}$ (weil $f(1) = 3, f(3) = 2$).

c)

Die Wertetabelle der Funktion ist:

x	$f(x) = 3 \cdot x \bmod 6$
0	0
1	3
2	0
3	3
4	0
5	3

Die Funktion ist weder injektiv (weil 0 öfter als einmal als Bild vorkommt) noch surjektiv (weil $1, 2, 4, 5$ nicht als Bilder vorkommen), also auch nicht bijektiv.

d) Man liest ab: $f^{-1}(\{2, 3\}) = \{1, 3, 5\}$.

e)

Der ggT von 3 und 7 ist 1. Daher hat 3 ein multiplikatives Inverses mod 7. Man rechnet aus oder probiert aus: $5 \cdot 3 \equiv 1 \mod 7$.
Ist nun $f : \{0, 1, 2, ..., 6\} \to \{0, 1, 2, ..., 6\}$ die Abbildung, die jedem x die Zahl $3x \mod 7$ zuordnet, so ist die Abbildung, die jedem x die Zahl $5x \mod 7$, die Umkehrabbildung von f, denn es ist $5 \cdot 3 \cdot x \equiv x \mod 7$ für jedes $x \in \{0, 1, 2, ..., 6\}$. Eine Umkehrabbildung gibt es nur für bijektive Abbildungen. Daher ist f bijektiv.

Der ggT von 3 und 6 ist hingegen nicht 1. Es gibt mod 6 sogenannte „Nullteiler“ - Zahlen, deren Produkt Null ist , die aber beide nicht Null sind.
Wird mod 6 gerechnet, besteht das Urbild der Null aus der Null und der 2 (und der 4). Die Abbildung ist also nicht injektiv, also nicht bijektiv.

f) Behauptung: $f : \{0, 1, ..., n-1\} \to \{0, 1, ..., n-1\}, x \mapsto 3x \bmod n$, ist genau dann bijektiv, wenn n kein Vielfaches von 3 ist.

Beweis:

$\Rightarrow$: Sei f bijektiv.
Angenommen, n ist ein Vielfaches von 3. Dann gibt es ein $q \in \{1, ..., n-1\}$ mit $n = 3 \cdot q$.
Damit ist $f(0) = 0$ und $f(q) = 0$, d.h., f ist nicht injektiv.
Dies ergibt einen Widerspruch zur Bijektivität, also kann n nicht Vielfaches von 3 sein.

$\Leftarrow$: Sei n nicht Vielfaches von 3.
Um zu zeigen, dass f bijektiv ist, reicht es zu zeigen, dass f injektiv ist.
Denn dann muß f auch surjektiv sein, weil Definitionsbereich und Wertebereich endlich sind und die gleiche Anzahl Elemente haben.

Angenommen, f ist nicht injektiv.
Dann gibt es $x_1 \neq x_2 \in \{0, .., n-1\}$ mit $3 \cdot x_1 \equiv 3 \cdot x_2 \bmod n$, d.h. $3 \cdot (x_1 - x_2) \equiv 0 \bmod n$.
Somit ist $3 \cdot (x_1 - x_2)$ Vielfaches von n, und, da 3 kein Teiler von n ist, ist $x_1 - x_2$ Vielfaches von n. Somit ist $x_1 - x_2 = 0$ oder $x_1 - x_2 \geqslant n$.
Da aber $x_1, x_2 \in \{0, ..., n-1\}$ ist $x_1 - x_2 < n$, also $x_1 = x_2$, im Widerspruch zur Annahme.
Also ist f injektiv, und damit bijektiv.

Aufgabe 2

$\Rightarrow$: Sei f eine bijektive Abbildung von D nach M.

Weil f injektiv ist, ist $|M| \geq |D|$.

Weil f surjektiv ist, ist $|M| \leq |D|$.

Also ist $|M| = |D|$.

$\Leftarrow$: Es sei $|M| = |D|$.

Wir benennen die Elemente von D und M, sodass $D = \{d_1, ..., d_n\}$ und $M = \{m_1, ..., m_n\}$.

Dann ist

$f : D \to M$, mit $f(d_i) = m_i$ für $i = 1, ...n$

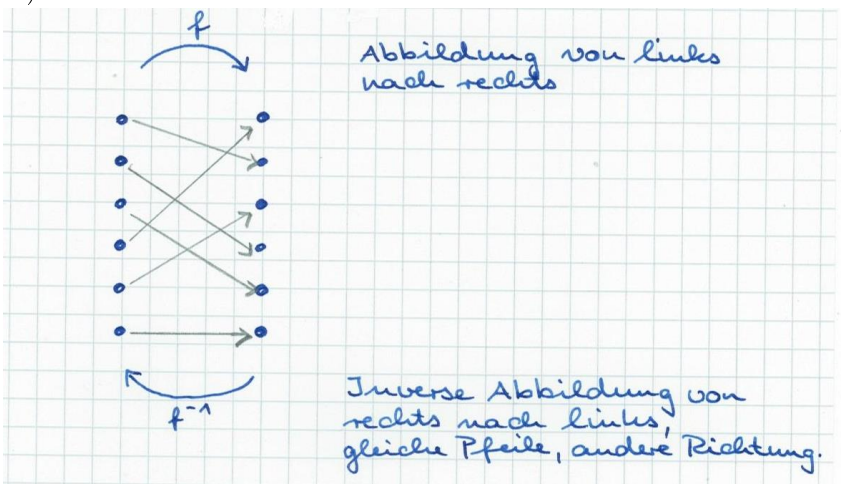
injektiv und surjektiv, also bijektiv.

Es existiert also eine bijektive Abbildung von D nach M.

Aufgabe 3

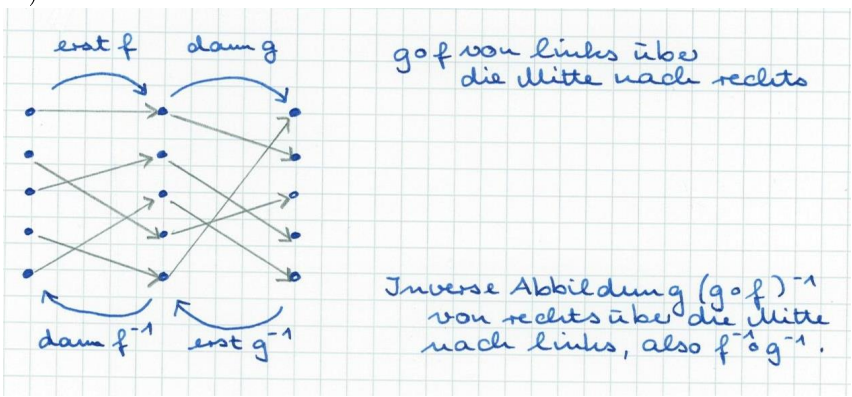
Eine wirkliche Musterlösung gibt es natürlich nicht, denn die Lösung hängt ja von der von Ihnen gewählten Funktion ab. Zeichnungen sehen aber etwa wie folgt aus:

a.)



$f^{-1} \circ f$ ist die Abbildung, die von jedem Element links aus den Pfeil nach rechts geht, und dann den Pfeil wieder zurück geht. So kommt man von jedem x auf der rechten Seite wieder zu x zurück.

b.)



$g \circ f$ ist die Abbildung, die von jedem Element links aus den Pfeil über die Mitte nach rechts geht. Da f bijektiv ist, wird jede Zwischenstation in der Mitte genau einmal angelaufen. Da g bijektiv ist, wird dann jedes Element rechts genau einmal erreicht. Jeder Weg kann also in eindeutiger Weise rückwärts gegangen werden, indem erst g^{-1} und dann g^{-1}, also $f^{-1} \circ g^{-1}$, angewendet wird. Deshalb ist $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Aufgabe 4

Sei $(a, b) = (0.a_1a_2a_3..., 0.b_1b_2b_3...) \in M \times M$.

Wir müssen zeigen, dass ein $x \in M$ existiert mit $f(x) = (a, b)$.

Ein solches x existiert, denn mit $x = 0.a_1b_1a_2b_2a_3b_3... \in M$ ist $f(x) = (a, b)$. Somit hat jeder Punkt ein Urbild, f ist surjektiv.

Aufgabe 5

Der Sender verschlüsselt seine Nachricht $x = 57$, indem er $x^e \mod n$, also $57^{13} \mod 187$, berechnet:

$57^{13} \equiv 57^{12} \cdot 57 \equiv (57^4)^3 \cdot 57 \equiv 38^3 \cdot 57 \equiv 129 \mod 187$.

Er sendet die verschlüsselte Nachricht $e(x) = 129$.

Der Empfänger besitzt die geheime Information $187 = 11 \cdot 17$, also die Faktorisierung von n.

Er weiß dann: $|\mathbb{Z}/187\mathbb{Z}^*| = (11 - 1) \cdot (17 - 1) = 10 \cdot 16 = 160$.

Er hat ein d bestimmt mit $d \cdot 13 \equiv 1 \mod 160$. Es ist $d = 37$, er hat es über die Gleichung $1 = (-3) \cdot 160 + 37 \cdot 13$ aus dem erweiterten euklidischen Algorithmus erhalten.

Wenn er die Nachricht $e(x) = 129$ erhält, berechnet er zum Entschlüsseln $e(x)^d \mod n$, also $129^{37} \mod 187$:

$129^{37} \equiv (129^2)^{18} \cdot 129 \equiv 185^{18} \cdot 129 \equiv (-2)^{18} \cdot 129 \equiv 157 \cdot 129 \equiv 57 \mod 187$.

So entschlüsselt der Empfänger die gesendete Nachricht $e(x) = 129$ und erhält die ursprüngliche Nachricht $x = 57$.