

Lineare Algebra (Informatik)

Übungsblatt 5

Aufgabe 1 (Abzählbar und überabzählbar unendliche Mengen)

- (i) Zeigen Sie: Es gibt unendlich viele Primzahlen. Folgern Sie daraus, dass die Menge der Primzahlen abzählbar unendlich ist.

Hinweis: Benutzen Sie, dass sich jede natürliche Zahl als Produkt von Primzahlen schreiben lässt (siehe Blatt) und widerlegen Sie damit die Annahme, dass es nur endlich viele Primzahlen gibt.

- (ii) Zeigen Sie: Die Menge der reellen Zahlen $\mathbb{R}$ ist überabzählbar unendlich.

Hinweis: Betrachten Sie die Menge der reellen Zahlen im offenen Intervall $(0, 1)$. Schreiben Sie jede reelle Zahl $r \in (0, 1)$ als Dezimalzahl. Betrachten Sie nun eine beliebige Folge $(r_i)_{i \in \mathbb{N}}$ reeller Zahlen mit $r_i \in (0, 1)$ für alle $i \in \mathbb{N}$. Die Elemente dieser Folge kann man abzählen. Zeigen Sie, dass man eine Zahl konstruieren kann, die nicht in dieser Folge enthalten ist (und dies für jede beliebige Folge). Folgern Sie daraus: die reellen Zahlen sind überabzählbar unendlich: $|\mathbb{R}| > |\mathbb{N}|$.

Lösung 1

- (i) Widerspruchsbeweis.

Angenommen, es gäbe nur endlich viele Primzahlen $p_1, \dots, p_N$. Sei

$$M = \left(\prod_{i=1}^N p_i \right) + 1 \in \mathbb{N}$$

M ist strikt größer als jede unserer N Primzahlen, also ist M nicht prim. Andererseits bekommen wir für alle $p \in \{p_1, \dots, p_N\}$ den Rest 1, wenn wir M durch p_i mit Rest dividieren. Dies bedeutet, dass M keine Primfaktoren außer sich selbst hat, und ist somit nach Definition prim. Dies ist ein Widerspruch. $\square$

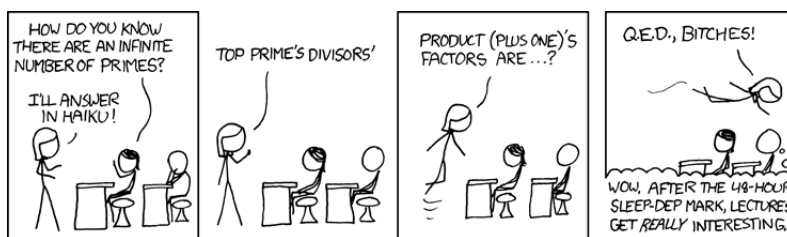


Abbildung 1: <https://xkcd.com/622/>

- (ii) Widerspruchsbeweis (Cantors 2. Diagonalargument).

Wir nehmen an, $\mathbb{R}$ wäre abzählbar. Dann wäre insbesondere das Intervall $(0, 1) \subseteq \mathbb{R}$ auch abzählbar. Sei $f : \mathbb{N} \rightarrow (0, 1)$ eine Bijektion.

Für alle $n \in \mathbb{N}$ können wir $f(n)$ eindeutig als Dezimalzahl $0, d_1^n d_2^n d_3^n, \dots$ mit abzählbar unendlich vielen Nachkommastellen schreiben, sodass diese nicht mit $\bar{9}$ endet. Die folgende abzählbar unendliche Liste sollte also alle reellen Zahlen in $(0, 1)$ enthalten:

$f(1)$	d_1^1	d_2^1	d_3^1	$\dots$	d_n^1	$\dots$
$f(2)$	d_1^2	d_2^2	d_3^2	$\dots$	d_n^2	$\dots$
$f(3)$	d_1^3	d_2^3	d_3^3	$\dots$	d_n^3	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$f(n)$	d_1^n	d_2^n	d_3^n	$\dots$	d_n^n	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Wir konstruieren eine reelle Zahl r in $(0, 1)$ wie folgt: Die k -te Nachkommastelle r_k von r wird so gewählt, dass sie mit d_k^k nicht übereinstimmt; zusätzlich verlangen wir, dass r nicht mit $\overline{9}$ endet, z.B. indem wir

$$r_k := \begin{cases} 1, & \text{falls } d_k^k \neq 1 \\ 2, & \text{sonst} \end{cases}$$

wählen.

Dies bedeutet, dass r nicht auf der obigen Liste liegen kann. Denn r unterscheidet sich von $f(n)$ in der n -ten Nachkommastelle, für *alle* $n \in \mathbb{N}$. Also ist r nicht im Bild der Bijektion f , was ein Widerspruch ist. $\square$

Aufgabe 2 (Rechnen in $\mathbb{Z}/7\mathbb{Z}$)

Welche Lösungen haben die folgenden Gleichungen in $\mathbb{Z}/7\mathbb{Z}$?

- (i) $3z = 5$
- (ii) $z^2 = 2$
- (iii) $z^2 = 3$
- (iv) $2z^2 = 1$

Begründen Sie Ihre Antwort.

Lösung 2 Die Multiplikationstabelle für $\mathbb{Z}/7\mathbb{Z}$ lautet

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Daraus können wir ablesen:

- (i) $z = 4$ ist die einzige Lösung dieser Gleichung
- (ii) $z = 3$ und $z = 4$ sind die einzigen Lösungen dieser Gleichung
- (iii) Diese Gleichung hat keine Lösungen
- (iv) Die Diagonaleinträge der Tabelle sind

$$0, 1, 4, 2, 2, 4, 1$$

also, wenn man diese um 2 multipliziert (mod 7), erhält man

$$0, 2, 1, 4, 4, 1, 2.$$

Also sind $z = 2$ und $z = 5$ die einzigen Lösungen dieser Gleichung.

Aufgabe 3 (Kommutative Gruppe)

Sei p eine Primzahl. Zeigen Sie: $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ mit der Verknüpfung $[a]_p \cdot [b]_p = [a \cdot b]_p$ ist eine kommutative Gruppe mit $p - 1$ Elementen.

Lösung 3

Wir müssen zeigen, dass die Verknüpfung in $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ assoziativ ist, dass es ein neutrales Element gibt, und dass jedes $x \in \{[1]_p, \dots, [p-1]_p\}$ ein inverses Element besitzt.

Assoziativität: Seien $[a]_p, [b]_p, [c]_p$ beliebige Elemente in $\mathbb{Z}_p \setminus \{[0]_p\}$.

$$\begin{aligned} ([a]_p \cdot [b]_p) \cdot [c]_p &= [a \cdot b]_p \cdot [c]_p \\ &= [(a \cdot b) \cdot c]_p \\ &= [a \cdot (b \cdot c)]_p \\ &= [a]_p \cdot [b \cdot c]_p \\ &= [a]_p \cdot ([b]_p \cdot [c]_p) \end{aligned}$$

Neutrales Element: Wir behaupten, dass $[1]_p$ das neutrale Element ist. Denn für $[a]_p \in \mathbb{Z}_p \setminus \{[0]_p\}$ beliebig gilt:

$$[a]_p \cdot [1]_p = [a \cdot 1]_p = [a]_p = [1 \cdot a]_p = [1]_p \cdot [a]_p$$

Inversen: Sei $[a]_p \in \mathbb{Z}_p \setminus \{[0]_p\}$ beliebig. Wir suchen ein $[b]_p \in \mathbb{Z}_p \setminus \{[0]_p\}$, sodass $[a]_p \cdot [b]_p = [1]_p$. Da p prim ist, ist $\text{ggT}(a, p) = 1$. Nach Übungsblatt 3, Aufgabe 4 (i), gibt es ganze Zahlen k, ℓ mit

$$1 = k \cdot a + \ell \cdot p. \quad (*)$$

Dies ist äquivalent zu

$$k \cdot a = (-\ell) \cdot p + 1$$

Mit anderen Worten: ganzzahlige Division von $k \cdot a$ durch p hat Rest 1, und somit ist $[k]_p$ das gesuchte inverse Element zu $[a]_p$, solange $k \neq 0$ ist. Aber k kann nicht 0 gewesen sein, denn wäre $k = 0$, dann würde aus Gleichung $(*)$ folgen, dass $1 = \ell \cdot p$. Dies ist aber für keine ganze Zahl ℓ der Fall, da $p \geq 2$.

Kommutativität:

$$[a]_p \cdot [b]_p = [a \cdot b]_p = [b \cdot a]_p = [b]_p \cdot [a]_p$$

□

Aufgabe 4 (Permutationen)

Sei X eine beliebige Menge, $A = \{f : X \rightarrow X\}$ die Menge aller Abbildungen von X nach X und $\circ$ die Verkettung zweier Abbildungen, d.h. für $f, f' \in A$ und $\forall x \in X$:

$$(f' \circ f)(x) = f'(f(x)).$$

- (i) Prüfen Sie, ob $(A, \circ)$ eine Gruppe ist.
- (ii) Sei $B = \{f : X \rightarrow X \mid f \text{ bijektiv}\} \subset A$ die Menge aller bijektiven Abbildungen von X auf X . Prüfen Sie, ob $(B, \circ)$ eine Gruppe ist.
- (iii) Sei X endlich. Was ist $f \in B$ anschaulich?

- (iv) Betrachten Sie die beiden Permutationen $f : \{1, 2, 3, 4, 5, 6\} \rightarrow \{1, 2, 3, 4, 5, 6\}$, $k \mapsto f(k)$, und $g : \{1, 2, 3, 4, 5, 6\} \rightarrow \{1, 2, 3, 4, 5, 6\}$, $j \mapsto g(j)$ mit

$$f : \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{Bmatrix}, \quad g : \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{Bmatrix}$$

Bestimmen Sie $f \circ g$ und $g \circ f$.

Lösung 4

- (i) Die Identitätsabbildung id_X ist neutral:

$$(\text{id}_X \circ f)(x) = \text{id}_X(f(x)) = f(x) = f(\text{id}_X(x)) = (f \circ \text{id}_X)(x)$$

Also die Inversen stimmen mit den Umkehrabbildungen überein. Daher ist $(A, \circ)$ i.A. keine Gruppe (außer $|A| = 0, 1$), da nicht jeder Abbildung hat eine Umkehrfunktion. Zum Beispiel, sei $X = \{a, b\}$. Dann enthält A die nicht-invertierbare Abbildung

$$f : X \rightarrow X, \quad f(a) = f(b) = a$$

Da f nicht injektiv ist, kann man kein $g : X \rightarrow X$ finden, sodass gleichzeitg $g(f(a)) = g(a) = a$ und $g(f(b)) = g(a) = b$.

- (ii) B ist eine Gruppe:

- Bemerkung: die Verknüpfung von zwei bijektiven Abbildungen ist wieder bijektiv (Satz 2.5.4)
- Verknüpfung von Funktionen ist (immer) assoziativ: Seien $f, g, h \in B$ und $x \in X$ beliebig. Dann:

$$\begin{aligned} ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \\ &= h((g \circ f)(x)) \\ &= (h \circ (g \circ f))(x) \end{aligned}$$

- Die Identitätsabbildung id_X ist bijektiv (und liegt somit in B) und ist neutral:

$$(\text{id}_X \circ f)(x) = \text{id}_X(f(x)) = f(x) = f(\text{id}_X(x)) = (f \circ \text{id}_X)(x)$$

- Jede bijektive Abbildung f hat eine eindeutige Umkehrabbildung f^{-1} (Sätze 2.5.3 und 2.5.4), die nach Definition

$$f^{-1} \circ f = f \circ f^{-1} = \text{id}_X$$

erfüllt.

- (iii) f beschreibt eine Umordnung (Permutation) der Elemente von X .

- (iv)

$$\begin{aligned} f \circ g &: \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ f(g(1)) & f(g(2)) & f(g(3)) & f(g(4)) & f(g(5)) & f(g(6)) \end{Bmatrix} \\ &= \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ f(5) & f(6) & f(1) & f(2) & f(3) & f(4) \end{Bmatrix} \\ &= \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 2 & 1 & 6 \end{Bmatrix}, \end{aligned}$$

und

$$\begin{aligned} g \circ f &: \left\{ \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ g(f(1)) & g(f(2)) & g(f(3)) & g(f(4)) & g(f(5)) & g(f(6)) \end{array} \right\} \\ &= \left\{ \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ g(3) & g(2) & g(1) & g(6) & g(5) & g(4) \end{array} \right\} \\ &= \left\{ \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{array} \right\}. \end{aligned}$$