LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
MATHEMATISCHES INSTITUT

Paula Reichert, Siddhant Das

Wintersemester 2023/24

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 4) 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

(i) Assume there is a finite number n of primes, listed as $\{p_1, p_2, \ldots, p_n\}$. Now, consider the product of all the primes in the list, plus one: $q = p_1 p_2 \ldots p_n + 1$. By construction, q is not divisible by any of the p_i. Hence it is either prime itself (but not in our list of all primes) or is divisible by another prime not in the list of all primes, contradicting the assumption of the finitely many primes.

(ii) (Cantor's diagonal argument) Suppose that the set of real numbers $(0, 1)$ is countable. This implies, $\exists\, f : \mathbb{N} \to (0, 1)$ a bijection, with $f(1) = 0.d_{11}\, d_{12} \ldots$, $f(2) = 0.d_{21}\, d_{22} \ldots$, $f(3) = 0.d_{31}\, d_{32} \ldots$, and so on. Here, $d_{ij} \in \{0, 1, 2, \ldots, 9\}$ is the j^{th} digit in the decimal expansion of $f(i) \in (0, 1)$. Now, consider the number $r \in (0, 1)$ with decimal expansion $r = 0.d_1\, d_2,\, d_3 \ldots$ fulfilling $d_i \neq d_{ii}\, \forall\, i \in \mathbb{N}$. That is, the k^{th} digit in the decimal expansion of r is different from that of $f(k)$. It follows that $r \neq f(n)\, \forall n \in \mathbb{N}$, thus $f^{-1}(r) \notin \mathbb{N}$, therefore, f fails to be surjective (in turn, bijective). This means, no bijective map exists between the set $(0, 1) \subset \mathbb{R}$ and N, os $(0, 1)$ is not countable/denumerable.

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.

Verknüpfungstafel von $(\mathbb{Z}/7\mathbb{Z}, \cdot)$:

$\cdot$	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

Damit hat man a) $3 \cdot 4 = 5$ in $\mathbb{Z}/7\mathbb{Z}$

b) $3 \cdot 3 = 4 \cdot 4 = 2$ in $\mathbb{Z}/7\mathbb{Z}$

c) $X^2 = 3$ hat in $\mathbb{Z}/7\mathbb{Z}$ keine Lösung

d) $2^{-1} = 4$ in $\mathbb{Z}/7\mathbb{Z}$ und daher wird aus

$2X^2 = 1 \overset{\cdot 2^{-1}=4}{\Longrightarrow} X^2 = 4$ (in $\mathbb{Z}/7\mathbb{Z}$)

und $X^2 = 4$ hat in $\mathbb{Z}/7\mathbb{Z}$ die Lösungen $X = 2$ und $X = 5$.

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 The multiplicative group modulo p, denoted $(\mathbb{Z}_p \setminus \{[0]_p\})$, is the set of $p-1$ elements $\{[1]_p, [2]_p, \ldots, [p-1]_p\}$ with group (composition) operation $[a]_p \cdot [b]_p := [a \cdot b]_p$ (a, $b \in \mathbb{Z}_p \setminus \{[0]_p\}$), as defined in Satz 3.1.3. 1). Note that associativity, commutativity, and $[1]_p$ as a neutral element result in $\mathbb{Z}_p$ as in Satz 3.1.3. 1). We show the validity of the closure axiom, i.e., we show that the product of two elements can never be zero. Suppose, $[a]_p \cdot [b]_p = 0$ for two elements of the set. This implies that either a or b is divisible by p, which is not possible since $[c]_p$ is the equivalence class of elements that leave a remainder $c \in \{1, 2, \ldots p-1\}$ when divided by p. Finally, we show that an inverse exists for every element of the group. For this, observe that no element has a common factor with p or is divisible by it. Thus, for any element $[c]_p$, $ggT(c,p) = 1$. By the result from Ü. 3, Auf. 4(i), $\exists\, m, n \in \mathbb{Z} : 1 = pm + cn$. We can rewrite this as $cn = 1 - pm$, i.e., cn leaves a remainder 1 when divided by p. We therefore conclude that $[n]_p$ is the multiplicative inverse of $[c]_p$.

Aufgabe 4 (Permutationen)

Sei X eine beliebige Menge, $A = \{f : X \to X\}$ 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 $B = \{f : X \to X | f \text{ bijektiv}\} \subset A$ 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 $f : \{1,2,3,4,5,6\} \to \{1,2,3,4,5,6\}$, $k \mapsto f(k)$, und $g : \{1,2,3,4,5,6\} \to \{1,2,3,4,5,6\}$, $j \mapsto g(j)$ mit

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

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

Lösung

(i) First, note that $e \in A$ defined by $e(x) = x$, $\forall\, x \in X$ is the neutral (or identity) element of $(A, \circ)$. This is because, $\forall\, f \in A$ and any $x \in X$, we have $(f \circ e)(x) = f(e(x)) = f(x) = e(f(x)) = (e \circ f)(x)$—in short, $e \circ f = f \circ e = f$. However, $(A, \circ)$ is not a group because not all $f \in A$ have inverse elements, i.e., $f^{-1} \in A$ fulfilling $f^{-1} \circ f = f \circ f^{-1} = e$ need not exist $\forall\, f \in A$. For instance, let $x_0 \in X$ and consider the map $f_0 \in A$ defined by $f_0(x) = x_0\ \forall\, x \in X$. Evidently, no $f_0^{-1} \in A$ exists for this map, because $(f_0^{-1} \circ f_0)(x) = f_0^{-1}(f_0(x)) = f_0^{-1}(x_0) \neq x = e(x)\ \forall x \in X$.

(ii) $(B, \circ)$ is a group. The three group properties hold. 1. (Associativity.) $\forall\, f, g, h \in B : (f \circ g) \circ h = f \circ (g \circ h)$ [cf. Ü. 4, Auf. 4 (i)]. 2. (Existence of neutral element.) The neutral element $e \in B$ is same as in (i) above. 3. (Existence of inverse element.) $\forall\, f \in B\, \exists\, f^{-1} \in B : f^{-1} \circ f = f \circ f^{-1} = e$ (cf. Satz 2.5.3.).

(iii) Any bijective map $f : X \to X$ from a finite set X to itself is a permutation.

(iv) As per the given definitions of f and g, we have

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

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

and

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

$$= \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ g(3) & g(2) & g(1) & g(6) & g(5) & g(4) \end{Bmatrix} = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 4 \end{Bmatrix}.$$