Universität Paderborn
INSTITUT FÜR MATHEMATIK
Prof. Dr. Bernhard Krötz, Dr. Job Kuit

Wintersemester 2024–2025

Lineare Algebra 1

4. Übungsblatt - Ausgewählte Lösungen

Präsenzaufgabe 4.3 Sei $n \in \mathbb{N}$ und sei $X_n := \{1, 2, \dots, n\}$. Weiter, sei

$$S_n := \{\sigma : X_n \to X_n : \sigma \text{ ist bijektiv}\}.$$

(a) Zeigen Sie, dass S_n zusammen mit der Komposition $\circ$ eine Gruppe bildet.
Beweis: Komposition ist assoziativ, denn

$$\big(\sigma \circ (\tau \circ \eta)\big)(x) = \sigma\big((\tau \circ \eta)(x)\big) = \sigma\Big(\tau\big(\eta(x)\big)\Big) = (\sigma \circ \tau)\big(\eta(x)\big) = \big((\sigma \circ \tau) \circ \eta\big)(x)$$

für alle $\sigma, \tau, \eta \in S_n$ und $x \in X_n$. Die Identitätsabbildung

$$\mathrm{Id}_{X_n} : X_n \to X_n, \quad x \mapsto x$$

ist ein neutrales Element für Komposition. Wenn $\sigma \in S_n$, dann ist σ bijektiv und besitzt darum eine Umkehrabbildung $\sigma^{-1} : X_n \to X_n$. Da σ^{-1} eine Bijektion ist, gilt $\sigma^{-1} \in S_n$. Es folgt, dass $(S_n, \circ)$ eine Gruppe ist.

Man nennt S_n die symmetrische Gruppe. Für $i, j \in X_n$ mit $i \neq j$ definieren wir

$$\tau_{i,j} : X_n \to X_n, \quad k \mapsto \begin{cases} j & (k = i) \\ i & (k = j) \\ k & (k \neq i, j) \end{cases}$$

Eine Element $\tau \in S_n$ wird eine Transposition genannt, wenn es $i, j \in X_n$ mit $i \neq j$ gibt, sodass $\tau = \tau_{i,j}$.

(b) Zeigen Sie, dass S_n durch Transpositionen erzeugt wird, d.h. für jedes Element $\sigma \in S_n$, gibt es ein $m \in \mathbb{N}_0$ und Transpositionen $\tau_1, \dots, \tau_m$, sodass

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_m.$$

Beweis mit Induktion nach n: Wenn $n = 1$, dann $S_n = \{\mathrm{Id}_{X_1}\}$. Die Aussage ist erfüllt mit $m = 0$. Sei $n \in \mathbb{N}$, sodass S_n durch Transpositionen erzeugt wird. Sei $\sigma \in S_{n+1}$. Wenn $\sigma(n+1) \neq n+1$, dann gibt es ein $k \in X_n$, sodass $\sigma(k) = n+1$. Es gilt

$$(\sigma \circ \tau_{k,n+1})(n+1) = \sigma\big(\tau(n+1)\big) = \sigma(k) = n+1.$$

Da $\tau_{k,n+1}^{-1} = \tau_{k,n+1}$ reicht es zu zeigen, dass es ein $m \in \mathbb{N}_0$ und Transpositionen $\tau_1, \dots, \tau_m$ gibt, sodass $\sigma = \tau_1 \circ \cdots \circ \tau_m$ unter der Annahme, dass $\sigma(n+1) = n+1$. Es gilt $\sigma(X_n) \subseteq X_n$. Weil σ bijektiv und X_n endlich ist, ist die Abbildung

$$\tilde{\sigma} : X_n \to X_n, \quad x \mapsto \sigma(x)$$

eine Bijektion und damit erhalten in S_n. Nach der Induktionsvoraussetzung gibt es ein $m \in \mathbb{N}_0$ und Transpositionen $\tilde{\tau}_1, \dots, \tilde{\tau}_m \in S_n$, sodas

$$\tilde{\sigma} = \tilde{\tau}_1 \circ \tilde{\tau}_2 \cdots \circ \tilde{\tau}_m$$

Für $1 \leq j \leq m$ definieren wir

$$\tau_j : X_{n+1} \to X_{n+1}, \quad \begin{cases} \tilde{\tau}_j(x) & (x \in X_n) \\ n+1 & (x = n+1) \end{cases}$$

Es gilt $\tau_j \circ \tau_j = \mathrm{Id}_{X_{n+1}}$. Darum sind die τ_j Transpositionen. Insbesondere sind die τ_j bijektiv und es gilt $\tau_j \in S_{n+1}$. Weiter gilt

$$\big(\tau_1 \circ \cdots \circ \tau_m\big)(x) = \big(\tilde{\tau}_1 \circ \tilde{\tau}_2 \cdots \circ \tilde{\tau}_m\big)(x) = \tilde{\sigma}(x) = \sigma(x)$$

für alle $x \in X_n$ und

$$\big(\tau_1 \circ \cdots \circ \tau_m\big)(n+1) = n+1 = \sigma(n+1).$$

Es folgt, dass $\sigma = \tau_1 \circ \cdots \circ \tau_m$.

Präsenzaufgabe 4.5 Der fermatsche Primzahltest ist ein Primzahltest, der auf dem kleinen fermatschen Satz beruht. Sei $n \in \mathbb{N}$ mit $n \geq 2$. Wähle ein $a \in \mathbb{Z}$. Wenn $[a]^{n-1} \neq [1]$, dann ist n keine Primzahl. Sonnst könnte n eine Primzahl sein.
Betrachten Sie $n = 57$ und berechnen Sie $[2]^{56}$. Zeigen Sie damit, dass 57 keine Primzahl ist.
Lösung: Es gilt

$$\begin{aligned} [2]^6 &= [2^6] = [64] = [7], \\ [2]^{12} &= [7]^2 = [49] = [-8], \\ [2]^{24} &= [-8]^2 = [64] = [7], \\ [2]^{48} &= [7]^2 = [49] = [-8] \end{aligned}$$

und damit

$$[2]^{56} = [2]^{48}[2]^6[2]^2 = [-8][7][4] = [-56][4] = [1][4] = [4] \neq [1].$$

Es folgt, dass 57 nicht prim ist.