GRUPPEN UND SYMMETRIEN
8. ÜBUNGSBLATT

JULIA SAUTER

Abgabe bis Do, 5.12.19, 12:00h in den Postfächern Ihrer Tutoren im Kopierraum.

Aufgabe 8.1 Wir betrachten die folgenden beiden Elemente in S_6

$$\sigma_1 = (1,2) \circ (3,4) \circ (1,3) \circ (1,2,3) \circ (2,4) \circ (1,2,6)$$
$$\sigma_2 = (1,3,5) \circ (1,4,3) \circ (1,3,6) \circ (2,4) \circ (1,3,6,4,2,5)$$

(a) Schreiben Sie σ_1 und σ_2 als Produkt disjunkter Zykel. Berechnen Sie dann die Ordnung und das Vorzeichen der beiden Permutationen.
(b) Schreiben Sie $\sigma_1\sigma_2\sigma_1^{-1}$ und $\sigma_2\sigma_1\sigma_2^{-1}$ als Produkt disjunkter Zykel.

Aufgabe 8.2 Es seien $\sigma, \tau \in S_n$.

(1) Zeigen Sie: $\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\tau\sigma)$ und $\mathrm{sign}(\sigma) = \mathrm{sign}(\sigma^{-1})$.
(2) Zeigen Sie: $\mathrm{sign}(\tau\sigma\tau^{-1}) = \mathrm{sign}(\sigma)$.
Folgern Sie, dass gilt $\tau A_n \tau^{-1} \subset A_n$. Benutzen Sie dann, dass A_n und $\tau A_n \tau^{-1}$ gleich viele Elemente haben, um zu folgern, dass $\tau A_n \tau^{-1} = A_n$ gilt.

Aufgabe 8.3 In dieser Aufgabe betrachten wir bijektive Abbildungen $\mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$, die bei der Verschlüsselung betrachtet werden, als Permutationen von $\{1, 2, \ldots, 10\}$, also als Elemente in S_{10}.

(1) (RSA) Wir betrachten die Abbildung

$$f\colon \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z},\ \overline{x} \mapsto \overline{x}^3.$$

Folgern Sie aus dem RSA Algorithmus, dass f bijektiv ist. Schreiben Sie f als Element von S_{10} als Produkt disjunkter Zykel und berechnen Sie seine Ordnung.
(2) (Caesar Verschlüsselung) Es sei $n \in \mathbb{N}_{>0}$ und $a, b \in \mathbb{Z}$ mit $\mathrm{ggT(a,n)} = 1$. Hier betrachtet man eine Abbildung

$$f_{a,b}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ \overline{x} \mapsto \overline{ax+b}.$$

Für $a' \in \mathbb{Z}$ mit $aa' \equiv 1 \pmod{\mathrm{n}}$ zeigen Sie: $f_{a',(-a'b)}$ ist die Inverse Abbildung zu $f_{a,b}$.
Betrachten Sie nun die Abbildung

$$f\colon \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z},\ \overline{x} \mapsto \overline{3x+1}.$$

Schreiben Sie f als Element von S_{10} als Produkt disjunkter Zykel und berechnen Sie seine Ordnung.

Aufgabe 8.4 Wir betrachten die folgenden vier Permutationen in S_{10}

$$\sigma_1 = (1,4,3,10) \circ (2,7) \circ (5,6,9,8)$$
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 10 & 4 & 3 & 7 & 9 & 8 & 1 & 2 & 6 \end{pmatrix}$$
$$\sigma_3 = (6,5) \circ (6,8) \circ (6,9) \circ (3,1) \circ (3,4) \circ (3,10) \circ (2,7)$$
$$\sigma_4 = (1,4) \circ (3,10) \circ (2,7) \circ (5,6) \circ (9,8)$$

(a) Finden Sie alle Paare σ_i und σ_j, die zueinander konjugiert sind.

(b) Wann immer σ_i und σ_j zueinander konjugiert sind, finden Sie eine Permutation τ, so dass

$$\sigma_i = \tau\sigma_j\tau^{-1} \quad \text{(bzw.} \quad \sigma_j = \tau^{-1}\sigma_i(\tau^{-1})^{-1} \quad)$$

gilt.