11. Übungsblatt

Abgabe: Mittwoch, 22.7.09

Aufgabe 1 Beweisen Sie, dass S_3 die folgende Präsentation besitzt

$$\langle x, y \mid x^2 = y^2 = (xy)^3 = 1 \rangle.$$

Aufgabe 2 Es ist

$$\langle x_1, \ldots, x_{n-1} \mid x_i^2 = [x_i, x_j] = (x_k x_{k+1})^3 = 1, 1 \leq i \leq n-1, |i-j| > 1, 1 \leq k \leq n-2 \rangle$$

eine Präsentation von S_n.

Zeigen Sie, dass S_n ein homomorphes Bild der Zopfgruppe B_n ist.

Aufgabe 3 Sei $G = GL_3(F_5)$ und sei $w = \begin{pmatrix} 0 & 1 & 0 \\ 2 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$.

(a) Wählen Sie $a, b \in G$ und führen Sie Stickels Schlüsselaustausch aus.

(b) Seien Sie Eve und finden Sie mit Hilfe der Linearen Algebra Attacke den Schlüssel heraus.

Aufgabe 4 Sei $G = S_n, n \geq 5$, $k = 3$ und $m = 2$. Wählen Sie geeignete $a_1, \ldots, a_k$ und $b_1, \ldots b_m$ in G und führen Sie mit diesen Elementen den Anshel-Anshel-Goldfeld Schlüsselaustausch durch.