Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

Studiengang Kommunikationsinformatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie – Übung 1

Aufgabe 1 (Gruppe)

In dieser Aufgabe soll die Quaternionengruppe Q konstruiert werden.

Gegeben seien die beiden komplexen Matrizen $A, B \in \mathbf{C}^{2\times 2}$ als

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

wobei $i^2 = -1$.

a) Zeigen Sie:
$$BA = A^3B.$$

b) Geben Sie möglichst kleine Zahlen $a, b \in \mathbf{N}$ an mit
$$A^a = B^b = E,$$
wobei E die Einheitsmatrix ist.

c) Listen Sie nun alle Elemente auf, die mit Hilfe von A und B erzeugt werden können. Dies ist die Menge Q. Beweisen Sie dadurch, daß $|Q| = 8$.

d) Finden Sie zu jedem Element $\in Q$ sein inverses Element.

e) Zeigen Sie mit Hilfe von Teil a), daß jedes Element $\in Q$ die Form A^iB^j hat.

f) Zeigen Sie, daß Q zwar eine Gruppe, aber keine abelsche Gruppe ist.

g) Begründen Sie, daß es keine Matrix $G \in Q$ geben kann mit
$$Q = \{G^0, G^1, G^2, G^3, G^4, G^5, G^6, G^7\}.$$