Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

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

Sicherheit und Kryptographie – Übung 2

Aufgabe 1 (Gruppe U_8)

Gegeben sei die Menge U_8 als

$$U_8 := \{x \in \mathbf{C} | x^8 = 1\}.$$

a) Überzeugen Sie sich anhand der Definition von U_8, daß $(U_8, \cdot)$ eine Gruppe ist.

b) Raten Sie vier Elemente von U_8 und begründen Sie, daß diese zu U_8 gehören.

c) Sei ξ eine Lösung von $x^2 = i$, wobei i die imaginäre Einheit von $\mathbf{C}$ ist. Zeigen Sie $\xi \in U_8$.

d) Raten Sie die restlichen Gruppenelemente von U_8 und begründen Sie, daß diese zu U_8 gehören.

e) Berechnen Sie die Ordnung aller Gruppenelemente.

Aufgabe 2 (Nullstellen von Polynomen)

Wenn ein Polynom vom Grad n

$$f(X) := X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$$

in einem Körper n Nullstellen $\xi_1, \ldots, \xi_n$ besitzt, dann läßt es sich in Linearfaktoren zerlegen

$$f(X) = (X - \xi_1)(X - \xi_2) \cdots (X - \xi_n).$$

a) Welchen Wert hat das Produkt aller ξ_i?

b) Welchen Wert hat die Summe aller ξ_i?

c) Überprüfen Sie Ihre Aussagen anhand eines Beispiels für $n = 2$.

d) Welchen Wert hat die Summe aller Elemente aus U_3, aus U_4, aus U_8?