



Sicherheit und Kryptographie – Übung 2

Aufgabe 1 (Gruppe U_3)

Gegeben sei die Menge U_3 als

$$U_3 := \{x \in \mathbf{R} \mid x^3 = 1\}.$$

- Zeigen Sie, daß (U_3, \cdot) eine Gruppe ist.
- Berechnen Sie die Elemente der Gruppe explizit.
- Geben Sie die Multiplikationstafel der Gruppe an.
- Berechnen Sie die Ordnung aller Gruppenelemente.

Aufgabe 2 (Gruppe U_8)

Gegeben sei die Menge U_8 als

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

- Überzeugen Sie sich (ohne Rechnung), daß auch (U_8, \cdot) eine Gruppe ist.
- Raten Sie vier Elemente von U_8 und begründen Sie, daß diese zu U_8 gehören.
- Sei ξ eine Lösung von $x^2 = i$, wobei i die imaginäre Einheit von \mathbf{C} ist. Zeigen Sie $\xi \in U_8$.
- Raten Sie die restlichen Gruppenelemente von U_8 und begründen Sie, daß diese zu U_8 gehören.
- Berechnen Sie die Ordnung aller Gruppenelemente.

Aufgabe 3 (Nullstellen von Polynomen)

Wenn ein Polynom vom Grad n

$$f(X) := X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$$

in einem Körper n Nullstellen ξ_1, \dots, ξ_n besitzt, dann läßt es sich in Linearfaktoren zerlegen

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

- Welchen Wert hat das Produkt aller ξ_i ?
- Welchen Wert hat die Summe aller ξ_i ?
- Überprüfen Sie Ihre Aussagen anhand eines Beispiels für $n = 2$.
- Welchen Wert hat die Summe aller Elemente aus U_3 , aus U_4 , aus U_8 ?