

5. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Sei G die Menge der geraden Zahlen: $G = \{\dots, -4, -2, 0, 2, 4, 6, \dots\}$.

Neben der üblichen Addition „+“ wird eine neue Multiplikation \odot auf G eingeführt durch

$$a \odot b := -\frac{a \cdot b}{2}.$$

Ist $(G, +, \odot)$ ein Ring? Gibt es ein Einselement?

Übung 2

In dieser Aufgabe sei R ein Ring mit den Verknüpfungen \boxplus und \boxminus . Zu $x \in R$ bezeichne \bar{x} das \boxplus -Inverse.

a) Zeigen Sie: Für alle $a, b \in R$ gilt:

$$a \boxminus \bar{b} = \overline{a \boxplus b} \quad \text{und} \quad \bar{a} \boxminus b = a \boxplus b.$$

b) Wie werden die Aussagen aus a) üblicherweise für $R = \mathbb{Z}$ formuliert?

c) Was besagt a) für $a = 2, b = 3$ in \mathbb{Z}_8 ?

d) Formulieren Sie den Sachverhalt „ $(-1) \cdot a = -a$ “ für einen allgemeinen Ring R mit Einselement e . Gilt dieser Zusammenhang immer?

Übung 3

Auf $M = \{0, 1, 2, 3\}$ seien zwei Verknüpfungen \oplus und \odot definiert durch

\oplus	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

\odot	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Ist M mit \oplus und \odot ein Ring oder sogar ein Körper? (Vgl. Blatt 1, Übung 5d))

Übung 4

a) Wieviel Lösungen hat die Gleichung $x^2 = 1$ in \mathbb{Z}_8 ?

b) Zeigen Sie: In einem Körper hat die Gleichung $x^2 = 1$ maximal zwei Lösungen.
(Tipp: Dritte binomische Formel)