FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2024/25
30.10.2024

Musterlösung zum 5. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Zunächst muss überprüft werden, dass die Operationen nicht aus G hinausführen. Da die Summe gerader Zahlen offensichtlich wieder eine gerade Zahl ist, ist das für "+" klar. Seien nun $a, b \in G$. Zu zeigen ist, dass $a \odot b$ eine gerade Zahl ist. Mit $a = 2a'$ und $b = 2b'$ folgt

$$a \odot b \;=\; -\frac{2a' \cdot 2b'}{2} \;=\; -2a'b',$$

d.h. $a \odot b \in G$.

Beh.: $(G, +, \odot)$ ist ein(kommutativer) Ring. Zu zeigen ist:

1. $(G, +)$ ist eine kommutative Gruppe,
2. $\odot$ ist assoziativ
3. das Distributivgesetz gilt.

Zu 1.: Da $(\mathbb{Z}, +)$ eine kommutative Gruppe ist, und $G \subseteq \mathbb{Z}$, ist $(G, +)$ eine kommutative Gruppe.

Zu 2.: Seien $a, b, c \in G$ dann gilt:

$$(a \odot b) \odot c \;=\; \left(-\frac{a \cdot b}{2}\right) \odot c \;=\; -\frac{-\frac{a \cdot b}{2} \cdot c}{2} \;=\; -\frac{a \cdot \left(-\frac{b \cdot c}{2}\right)}{2} \;=\; a \odot \left(-\frac{b \cdot c}{2}\right) \;=\; a \odot (b \odot c)$$

$\Rightarrow$ $\odot$ ist assoziativ.

Zu 3.: Seien $a, b, c \in G$ dann gilt:

$$a \odot (b + c) \;=\; -\frac{a \cdot (b + c)}{2} \;=\; -\frac{a \cdot b + a \cdot c}{2} \;=\; -\frac{a \cdot b}{2} - \frac{a \cdot c}{2} \;=\; (a \odot b) + (a \odot c)$$

Da $\odot$ kommutativ ist, gilt auch $(b + c) \odot a = (b \odot a) + (b \odot c)$, und das Distributivgesetz gilt.

Beh.: -2 ist Einselement in g.

Tatsächlich gilt für alle $a \in G$: $-2 \odot a \;=\; a \odot (-2) \;=\; -\frac{a \cdot (-2)}{2} \;=\; a$.

Übung 2

a) Für alle $a, b \in R$ gilt

$$n \;=\; a \boxdot n \;=\; a \boxdot (b \oplus \bar{b}) \;=\; (a \boxdot b) \oplus (a \boxdot \bar{b}).$$

Also ist $(a \boxdot \bar{b})$ das $\oplus$-Inversezu $a \boxdot b$, d.h $\overline{a \boxdot b} \;=\; a \boxdot \bar{b}$.

Damit folgt nun

$$\bar{a} \boxdot \bar{b} \overset{\text{wie oben}}{=} \overline{a \boxdot \bar{b}} \overset{\text{ähnlich}}{=} \overline{\overline{a \boxdot b}} \overset{x=\bar{\bar{x}}}{=} a \boxdot b.$$

b) $\forall\, a, b \in \mathbb{Z}$:

$$a \cdot (-b) \;=\; -(a \cdot b) \qquad \text{und} \qquad (-a) \cdot (-b) \;=\; a \cdot b.$$

c) In $\mathbb{Z}_8$ gilt:

$$2 \cdot \bar{3} \;=\; 2 \cdot 5 \;=\; 2,$$
$$\overline{2 \cdot 3} \;=\; \bar{6} \;=\; 2.$$

$$\bar{2} \cdot \bar{3} \;=\; 6 \cdot 5 \;=\; 6,$$
$$2 \cdot 3 \;=\; 6.$$

d) „$(-1) \cdot a = -a$“, entspricht allgemein $\bar{e} \boxdot a = \bar{a}$. Dies gilt wegen

$$\bar{e} \boxdot a \overset{\text{Üb. 2a}}{=} \overline{e \boxdot a} \;=\; \bar{a}.$$

Übung 3

1. $(M, \oplus)$ ist eine kommutative Gruppe (s. Blatt 1, Übung 5d)).
2. Um zu prüfen ob $\odot$ assoziativ ist, müssen nicht alle 4^3 Möglichkeiten ausprobiert werden. Mann kann folgende Beobachtungen ausnutzen:

   Die $\odot$-Verknüpfung mit 0 ergibt stets 0.

   Die $\odot$-Verknüpfung mit 1 ergibt die Zahl selbst.

   $\odot$ ist kommutativ.

   Damit sieht man leicht, dass $(a \odot b) \odot c = a \odot (b \odot c)$ gilt, falls mindestens eines der beteiligten Elemente gleich 0 oder gleich 1 ist. Es bleiben also nur noch die Fälle $a, b, c \in \{2, 3\}$. Bei $a = c$ folgt die Gleichheit aus der Kommutativität. Damit muss nur lediglich $(2 \odot 2) \odot 3 = 2 \odot (2 \odot 3)$ und $(2 \odot 3) \odot 3 = 2 \odot (3 \odot 3)$ überprüft werden (die Fälle $a = 3$, $b = 2$, $c = 2$ und $a = 3$, $b = 3$, $c = 2$ ergeben sich daraus wiederum wegen der Kommutativität). Da diese Gleichungen stimmen, ist $\odot$ assoziativ.
3. Ähnliche wie oben helfen allgemeine Überlegungen zu $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$ die zu testenden Fälle zu reduzieren:

   Ist eines der Elemente gleich 0 oder ist $c = 1$, so ist die Gleichung klar. Wegen der Kommutativität reicht es, $a \leq b$ zu betrachten. Da jedes Element zu sich selbst $\oplus$-Inverses ist, ist auch der Fall $a = b$ klar. Es bleiben also 6 Fälle ($(a, b) = (1, 2)$, $(a, b) = (1, 3)$, $(a, b) = (2, 3)$ und jeweils $c = 2$ oder $c = 3$). Die Überprüfung zeigt, dass für diese Fälle die Gleichungen stimmen.

Damit ist $(M, \oplus, \odot)$ ein kommutativer Ring. Das Einselement $e = 1$ und die Invertierbarkeit für alle Zahlen außer der 0 bzgl. $\odot$ kann man an der Tabelle leicht erkennen. Somit ist $(M, \oplus, \odot)$ sogar ein Körper.

Übung 4

a) 4 Lösungen: $1, 3, 5, 7$ erfüllen die Gleichung.

b) In einem Körper $(K, +, \cdot)$ mit Einselement 1 und Nullelement 0 gilt:

$$\begin{aligned} & x^2 = 1 \\ \Leftrightarrow\ & x^2 + \bar{1} = 0 \\ \Leftrightarrow\ & (x+1) \cdot (x+\bar{1}) = 0. \end{aligned}$$

Da Körper nullteilerfrei sind, folgt hieraus, dass $x + 1 = 0$ oder $x + \bar{1} = 0$ ist, also $x = \bar{1}$ oder $x = 1$. Weitere Lösungen sind nicht möglich.