

**Aufgabe 1:** Seien  $R_1$  und  $R_2$  Ringe und  $\varphi : R_1 \rightarrow R_2$  ein Ringhomomorphismus. Zeigen Sie, dass  $K_\varphi := \{x \in R_1 \mid \varphi(x) = 0\}$  ein Ideal von  $R_1$  ist.

Wir müssen zeigen, dass die Menge  $K_\varphi$  abgeschlossen unter Addition, sowie abgeschlossen unter Multiplikation mit beliebigen Elementen von  $R_1$ .

Die Abgeschlossenheit der Menge unter Addition mit Elementen aus ihr selbst, folgt aber sofort aus der Eigenschaft, dass  $\varphi$  ein Ringhomomorphismus ist:  $\varphi(x) = 0, \varphi(y) = 0 \Rightarrow 0 = \varphi(x) + \varphi(y) = \varphi(x + y)$ , also  $x + y \in K_\varphi$ .

Für beliebige  $x \in K_\varphi, r \in R_1$  gilt weiter:  $\varphi(xr) = \varphi(x) \cdot r = 0 \cdot r = 0$ , also auch  $x \cdot r \in K_\varphi$ .

Damit ist  $K_\varphi$  ein Ideal von  $R_1$ .

**Aufgabe 2:** Sei  $R$  ein Ring und  $I$  ein Ideal von  $R$ .

Zeigen Sie, dass die Verknüpfung  $\odot$  auf  $R/I$  mit  $x \odot y := (x + I) \cdot (y + I) = (xy + I)$  unabhängig von der Wahl der Repräsentanten  $x \in (x + I)$  und  $y \in (y + I)$ , also wohldefiniert, ist.

Es seien  $i, j \in I$  und  $x' := x + i$  sowie  $y' := y + j$  zwei weitere Repräsentanten der Restklassen  $(x + I)$  und  $(y + I)$ . Wir zeigen, dass  $x' \odot y' \in (xy + I)$  ist.

Es ist  $x' \odot y' = (x' + I)(y' + I) = (x + i + I)(y + j + I) = (x + I)(y + I) = (xy + I)$ .

Die Definition von  $\odot$  ist somit wohldefiniert.

**Aufgabe 3:** Auf  $\mathbb{Z}$  werden zwei Verknüpfungen  $\oplus$  und  $\odot$  festgelegt. Für  $a, b \in \mathbb{Z}$  sei  $a \oplus b := a + b + 1$  und  $a \odot b := a + b + ab$ .

1. Was ist das neutrale Element bzgl.  $\oplus$ ?
2. Was ist das neutrale Element bzgl.  $\odot$ ?
3. Zeigen Sie: Es ist  $(\mathbb{Z}, \oplus, \odot)$  ein kommutativer Ring mit 1 ist.
  1. Wir suchen ein Element  $z \in \mathbb{Z}$  mit  $z \oplus a = a$  für alle  $a \in \mathbb{Z}$ : es ist  $z \oplus a = z + a + 1$ . Das neutrale Element bzgl.  $\oplus$  ist  $z := -1$ .
  2. Wir suchen ein Element  $u \in \mathbb{Z}$  mit  $u \odot a = a$  für alle  $a \in \mathbb{Z} \setminus \{z\}$ . Es ist  $u \odot a = u + a + ua$ . Damit ist  $u := 0$  das neutrale Element von  $\odot$ .

3. Wir müssen die Ringeigenschaften nachweisen:

1.  $(\mathbb{Z}, \oplus)$  ist eine abelsche Gruppe:

- Es ist  $a \oplus b = b \oplus a$ , da  $\mathbb{Z}$  kommutativ ist.
- Es ist  $(a \oplus b) \oplus c = (a+b+1) + c + 1 = a + (b+c+1) + 1 = a \oplus (b \oplus c)$ , da  $\mathbb{Z}$  assoziativ ist.
- Das neutrale Element ist  $z = -1$ .
- Das Inverse Element zu  $a$  ist  $a' := -a - 2$ .

2. Wir müssen zeigen, dass  $\odot$  assoziativ ist:

$$(a \odot b) \odot c = (a + b + ab) + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc.$$

$$a \odot (b \odot c) = a + (b + c + bc) + a(b + c + bc) = a + b + c + ab + ac + bc + abc.$$

Das neutrale Element ist  $u = 0$ , wie bereits gezeigt.

3. Jetzt müssen wir noch die Distributivgesetze zeigen:

$$\begin{aligned} (a \oplus b) \odot c &= (a + b + 1) \odot c = (a + b + 1) + c + (a + b + 1)c \\ &= a + b + 2c + ac + bc + 1 \end{aligned}$$

$$\begin{aligned} (a \odot c) \oplus (b \odot c) &= (a + c + ac) \oplus (b + c + bc) \\ &= (a + c + ac) + (b + c + bc) + 1 \\ &= a + b + 2c + ac + bc + 1, \quad \text{sowie} \end{aligned}$$

$$\begin{aligned} c \odot (a \oplus b) &= c \odot (a + b + 1) = c + (a + b + 1) + c(a + b + 1) \\ &= a + b + 2c + 1 + ac + bc \end{aligned}$$

$$\begin{aligned} (c \odot a) \oplus (c \odot b) &= (c + a + ca) \oplus (c + b + cb) \\ &= (c + a + ca) + (c + b + cb) + 1 \\ &= a + b + 2c + 1 + ac + bc. \end{aligned}$$

(Da  $a \odot b = b \odot a$  ist, hätten wir uns den zweiten Teil auch sparen können.)

**Aufgabe 4:** Auf der Menge  $\mathcal{P}(M)$  aller Teilmengen einer gegebenen Menge  $M$  definieren wir zwei Verknüpfungen: Für alle  $A, B \in \mathcal{P}(M)$  sei  $A \oplus B := A \cup B \setminus (A \cap B)$  und  $A \odot B := A \cap B$ .

1. Zeigen Sie, dass für eine  $n$ -elementige Menge  $M$  die abelsche Gruppe  $(\mathcal{P}(M), \oplus)$  isomorph zu  $(\mathbb{Z}/2\mathbb{Z})^n$  ist.
2. Zeigen Sie, dass  $(\mathcal{P}(M), \oplus, \odot)$  ein kommutativer Ring mit Eins ist.

1. Es sei  $M := \{m_1, \dots, m_n\}$ . Wir definieren die Abbildung  $\varphi : \mathcal{P}(M) \rightarrow (\mathbb{Z}/2\mathbb{Z})^n$  vermöge  $\varphi(X) = (z_1, \dots, z_n)$ , wobei

$$z_i := \begin{cases} 1 & m_i \in X \\ 0 & m_i \notin X \end{cases} \quad \text{gilt.}$$

Die Abbildung  $\varphi$  ist injektiv und surjektiv, da jeder Vektor von 0 und 1 der Länge  $n$  umkehrbar eindeutig einer Teilmenge von  $M$  entspricht. Damit ist  $\varphi$  eine Bijektion. Es ist dabei der Nullvektor das Bild der leeren Menge.

Wir zeigen nun noch, dass die Abbildung mit den Verknüpfungen verträglich ist.

Wir haben zu zeigen:  $\varphi(A \oplus B) = \varphi(A) + \varphi(B)$ . Dabei ist  $\varphi(A \oplus B) = \varphi(A \cup B \setminus (A \cap B)) =: \vec{z}$ . Für die  $i$ -te Komponente  $z_i$  von  $\vec{z}$  gilt:

$$z_i = \begin{cases} 1, & \text{falls } m_i \in A \text{ oder } m_i \in B \text{ und } m_i \notin A \cap B \\ 0, & \text{falls } m_i \notin A \text{ oder } m_i \notin B \text{ oder } m_i \in A \cap B \end{cases}$$

Das ist genau der gleiche Vektor, wie bei  $\varphi(A) + \varphi(B)$ .

Damit ist  $(\mathcal{P}(M), \oplus)$  isomorph zu  $((\mathbb{Z}/2\mathbb{Z})^n, +)$ .

2. Wegen der Isomorphie aus dem ersten Aufgabenteil haben wir bereits gezeigt, dass  $(\mathcal{P}(M), \oplus)$  eine abelsche Gruppe ist. Wir müssen noch zeigen, dass  $\odot$  assoziativ ist und die Distributivgesetze erfüllt sind.

Dazu betrachten wir für  $A, B, C \in \mathcal{P}(M)$ , die verschiedenen Möglichkeiten, ob  $m_i$  in  $A, B, C, A \cap B$  usw. enthalten ist.

**Assoziativität:**

A	B	C	$A \cap B$	$B \cap C$	$(A \cap B) \cup C$	$A \cap (B \cup C)$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
1	0	0	0	0	0	0
0	1	1	0	1	0	0
1	0	1	0	0	0	0
1	1	0	1	0	0	0
1	1	1	1	1	1	1

$$(A \oplus B) \odot C = A \odot C \oplus B \odot C:$$

A	B	C	$A \oplus B$	$(A \oplus B) \odot C$	$A \odot C$	$B \odot C$	$A \odot C \oplus B \odot C$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	1	0	1	0	0	0	0
1	0	0	1	0	0	0	0
0	1	1	1	1	0	1	1
1	0	1	1	1	1	0	1
1	1	0	0	0	0	0	0
1	1	1	0	0	1	1	0

Die Verknüpfungen kommutieren: Es ist  $A \oplus B = A \cup B \setminus (A \cap B) = B \cup A \setminus (B \cap A) = B \oplus A$ . Ebenfalls gilt  $A \odot B = A \cap B = B \cap A = B \odot A$ . Deswegen gilt auch das zweite Distributivgesetz  $C \odot (A \oplus B) = C \odot A \oplus C \odot B$ .

Die Menge  $M$  ist das neutrale Element bzgl.  $\odot$ .

**Aufgabe 5:** Es sei  $p$  eine Primzahl. Bestimmen Sie die Anzahl der Elemente von  $(\mathbb{Z}/p^2\mathbb{Z})^*$ .

Wir müssen diejenigen Elemente in  $\{0, \dots, p^2 - 1\}$  finden, die teilerfremd zu  $p^2$  sind. Nur  $p, p^2$  sind nichttriviale Teiler von  $p^2$ . Von den  $p^2$  Zahlen  $0, \dots, p^2 - 1$  müssen wir die Vielfachen von  $p$  ausschließen, das sind aber genau  $p$  Stück:  $0 \cdot p, 1 \cdot p, 2 \cdot p, \dots, (p - 1)p$ . Damit verfügt  $(\mathbb{Z}/p^2\mathbb{Z})^*$  über  $p^2 - p = p(p - 1)$  Elemente.