

Musterlösung Serie 9

RINGE, EINHEITENGRUPPE

49. Sei $(G, +)$ eine additive abelsche Gruppe und sei $\text{End}(G)$ die Menge der Endomorphismen von G .

Zeige, dass $(\text{End}(G), +, \circ)$ mit

$$(f_1 + f_2)(g) := f_1(g) + f_2(g) \quad \text{und} \quad (f_1 \circ f_2)(g) := f_1(f_2(g))$$

zu einem Ring wird.

Lösung: Offensichtlich sind $+$ und \circ wohldefiniert und assoziativ. Auch Kommutativität der Addition folgt offensichtlich daraus, dass $(G, +)$ abelsch ist. Das neutrale Element der Addition ist die Abbildung, die jedes Element aus G auf $0 \in G$ schickt. Für ein $f \in \text{End}(G)$ gilt klarerweise $(-f)(g) = -f(g)$. Das neutrale Element der Multiplikation ist die Identität. Um Distributivität nachzuprüfen, seien $f_1, f_2, f_3 \in \text{End}(G)$ und sei $g \in G$ beliebig. Dann gilt

$$\begin{aligned} (f_1 \circ (f_2 + f_3))(g) &= f_1((f_2 + f_3)(g)) = f_1(f_2(g) + f_3(g)) \stackrel{f_1 \in \text{End}(G)}{=} f_1(f_2(g)) + f_1(f_3(g)) \\ &= (f_1 \circ f_2)(g) + (f_1 \circ f_3)(g) = (f_1 \circ f_2 + f_1 \circ f_3)(g) \end{aligned}$$

und

$$\begin{aligned} ((f_1 + f_2) \circ f_3)(g) &= (f_1 + f_2)(f_3(g)) = f_1(f_3(g)) + f_2(f_3(g)) \\ &= (f_1 \circ f_3)(g) + (f_2 \circ f_3)(g) = (f_1 \circ f_3 + f_2 \circ f_3)(g). \end{aligned}$$

Somit haben wir alle Ringaxiome nachgeprüft.

50. Sei S eine nicht-leere Menge. Auf der Potenzmenge $\mathcal{P}(S)$ (d.h. der Menge aller Teilmengen von S) definieren wir zwei binäre Operationen $+$ und $*$ wie folgt:

$$X * Y := X \cap Y, \quad X + Y := (X \setminus Y) \cup (Y \setminus X).$$

- (a) Zeige, dass $(\mathcal{P}(S), \emptyset, S, +, *)$ ein kommutativer Ring ist.
- (b) Sei $\mathfrak{a} \subseteq \mathcal{P}(S)$ eine nicht-leere Teilmenge von $\mathcal{P}(S)$ mit folgenden beiden Eigenschaften:
- Für $X, Y \in \mathfrak{a}$ ist auch $X \cup Y \in \mathfrak{a}$.
 - Ist $X \in \mathfrak{a}$, so ist $\mathcal{P}(X) \subseteq \mathfrak{a}$.

Zeige, dass dann für alle $X, Y \in \mathfrak{a}$ und $Z \in \mathcal{P}(S)$ gilt:

$$X + Y \in \mathfrak{a} \quad \text{und} \quad Z * X \in \mathfrak{a}.$$

Lösung: (a) Offensichtlich sind $+$ und $*$ wohldefiniert.

Wir prüfen nun nach, dass $(\mathcal{P}(S), +)$ eine abelsche Gruppe ist. Kommutativität von $+$ ist offensichtlich. Für die Assoziativität, seien $X, Y, Z \subseteq S$. Dann gilt

$$\begin{aligned} X + (Y + Z) &= (X \setminus ((Y \setminus Z) \cup (Z \setminus Y))) \cup (((Y \setminus Z) \cup (Z \setminus Y)) \setminus X) \\ &= (X \setminus (Y \cup Z)) \cup (Y \setminus (Z \cup X)) \cup (Z \setminus (X \cup Y)) \cup (Z \cup X) \cup (X \cap Y \cap Z) \\ &= (((X \setminus Y) \cup (Y \setminus X)) \setminus Z) \cup (Z \setminus ((X \setminus Y) \cup (Y \setminus X))) \\ &= (X + Y) + Z. \end{aligned}$$

Weiter ist \emptyset das neutrale Element und jedes $X \subseteq S$ offensichtlich sein eigenes Inverses.

Als nächstes zeigen wir, dass $(\mathcal{P}(X), *)$ ein kommutativer Monoid mit 1 ist. Offensichtlich ist $*$ kommutativ. Assoziativität von $*$ ist bekannt. Das neutrale Element von $*$ ist offensichtlich X .

Für die Distributivität seien $X, Y, Z \subseteq X$. Dann gilt

$$\begin{aligned} X * (Y + Z) &= X \cap ((Y \setminus Z) \cup (Z \setminus Y)) = (X \cap (Y \setminus Z)) \cup (X \cap (Z \setminus Y)) \\ &= ((X \cap Y) \setminus Z) \cup ((X \cap Z) \setminus Y) \\ &= ((X \cap Y) \setminus (X \cap Z)) \cup ((X \cap Z) \setminus (X \cap Y)) \\ &= X * Y + X * Z. \end{aligned}$$

Wegen Kommutativität von $*$ folgt damit auch sofort $(X + Z) * Z = X * Z + Y * Z$.

(b) Seien $X, Y \in \mathfrak{a}$ und $Z \in \mathcal{P}(S)$ beliebig. Dann ist $X \setminus Y \subseteq X$ eine Teilmenge und nach Eigenschaft (ii) ist $X \setminus Y \in \mathfrak{a}$. Ähnlich argumentieren wir um $Y \setminus X \in \mathfrak{a}$ zu erhalten, so dass dank (i) gilt

$$X + Y = (X \setminus Y) \cup (Y \setminus X) \in \mathfrak{a}.$$

Betrachte nun $Z * X = Z \cap X \subset X$. Wegen (ii) ist das ebenfalls ein Element von \mathfrak{a} , und somit erhalten wir Teil (b) der Aufgabe.

51. Sei n eine positive natürliche Zahl. Definiere die **Eulersche φ -Funktion** durch

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*|.$$

(a) Zeige: Für jede ganze Zahl a , die teilerfremd ist zu n , gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{d.h. } n \mid (a^{\varphi(n)} - 1).$$

(b) Zeige: Existiert eine Zerlegung $n = q_1 \cdot \dots \cdot q_r$ mit paarweise teilerfremden positiven Zahlen q_i , so ist $\varphi(n) = \prod_{i=1}^r \varphi(q_i)$.

(c) Zeige: Ist $n = p_1^{l_1} \cdot \dots \cdot p_r^{l_r}$ mit paarweise verschiedenen Primzahlen p_i und $l_i > 0$ (für alle i), so gilt

$$\varphi(n) = n \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Lösung: Aus der Vorlesung wissen wir $(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} : 0 < a \leq n, \text{ggT}(a, n) = 1\}$.

(a) Da $(\mathbb{Z}/n\mathbb{Z})^*$ eine Gruppe ist, folgt

$$\bar{a}^{\varphi(n)} = \bar{a}^{|\mathbb{Z}/n\mathbb{Z}^*|} = \bar{1} \in (\mathbb{Z}/n\mathbb{Z})^*.$$

Das ist äquivalent zu $n \mid (a^{\varphi(n)} - 1)$.

(b) Wenn q_1, \dots, q_r teilerfremd sind, dann gilt $\mathbb{Z}/n\mathbb{Z} \cong \bigoplus_{i=1}^r \mathbb{Z}/q_i\mathbb{Z}$. Für die Einheitsgruppe folgt $(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{i=1}^r (\mathbb{Z}/q_i\mathbb{Z})^*$ und damit

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = \prod_{i=1}^r |(\mathbb{Z}/q_i\mathbb{Z})^*| = \prod_{i=1}^r \varphi(q_i).$$

(c) Zuerst berechnen wir

$$n \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^r p_i^{l_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^r p_i^{l_i-1} (p_i - 1).$$

Mit Aufgabe (b) genügt es nun zu zeigen, dass $\varphi(p_i^{l_i}) = p_i^{l_i-1} (p_i - 1) = p_i^{l_i} - p_i^{l_i-1}$ ist. Offensichtlich gilt

$$\{a \in \mathbb{N} : 0 < a \leq p_i^{l_i}, \text{ggT}(a, p_i^{l_i}) = 1\} = \{1, 2, \dots, p_i^{l_i}\} \setminus \{p_i, 2p_i, 3p_i, \dots, (p_i^{l_i-1})p_i\}.$$

Daraus folgt die Behauptung.

52. Sei $R = \mathbb{Z}/201\mathbb{Z} \oplus \mathbb{Z}/102\mathbb{Z} \oplus \mathbb{Z}/96\mathbb{Z}$.

- (a) Bestimme die Ordnung $|R^*|$ der Einheitengruppe von R .
 (b) Finde das multiplikativ Inverse von $(\overline{13}, \overline{13}, \overline{13})$ in R .

Lösung: (a) Es gilt

$$(\mathbb{Z}/201\mathbb{Z} \oplus \mathbb{Z}/102\mathbb{Z} \oplus \mathbb{Z}/96\mathbb{Z})^* \cong (\mathbb{Z}/201\mathbb{Z})^* \times (\mathbb{Z}/102\mathbb{Z})^* \times (\mathbb{Z}/96\mathbb{Z})^*.$$

Mit Aufgabe 57 berechnen wir

$$\begin{aligned} |(\mathbb{Z}/201\mathbb{Z})^*| &= \varphi(201) = \varphi(3) \cdot \varphi(67) = 2 \cdot 66 = 132 \\ |(\mathbb{Z}/102\mathbb{Z})^*| &= \varphi(102) = \varphi(2) \cdot \varphi(3) \cdot \varphi(17) = 1 \cdot 2 \cdot 16 = 32 \\ |(\mathbb{Z}/96\mathbb{Z})^*| &= \varphi(96) = \varphi(3) \cdot \varphi(2^5) = 2 \cdot 2^4(2-1) = 32. \end{aligned}$$

Daraus ergibt sich $|R^*| = 132 \cdot 32 \cdot 32 = 135168$.

(b) Wir wenden den Euklidischen Algorithmus an. Nämlich

$$\begin{array}{r} 201 = 15 \cdot 13 + 6 \\ 13 = 2 \cdot 6 + 1 \\ \hline 1 = 13 - 2 \cdot 6 = 13 - 2 \cdot (201 - 15 \cdot 13) \end{array}$$

Daraus ergibt sich

$$\overline{13}^{-1} = \overline{1 + 2 \cdot 15} = \overline{31}.$$

Genauso

$$102 = 7 \cdot 13 + 11$$

$$13 = 1 \cdot 11 + 2$$

$$11 = 5 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Wie in der Vorlesung berechnen wir nun

$$\begin{array}{c|cccc} & 7 & 1 & 5 & 2 \\ \hline 0 & 1 & 7 & 8 & 47 & 102 \end{array}$$

und daher gilt $\overline{13}^{-1} = \overline{(-1)^3 \cdot 47} = \overline{55}$.

Genauso berechnen wir

$$96 = 7 \cdot 13 + 5$$

$$13 = 2 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0,$$

also

$$\begin{array}{c|ccccc} & 7 & 2 & 1 & 1 & 2 \\ \hline 0 & 1 & 7 & 15 & 22 & 37 & 96 \end{array}$$

und daher $\overline{13}^{-1} = \overline{(-1)^4 \cdot 37} = \overline{37}$. Insgesamt ist also $(\overline{13}, \overline{13}, \overline{13})^{-1} = (\overline{31}, \overline{55}, \overline{37})$.