

## 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.

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:  
(i) Für  $X, Y \in \mathfrak{a}$  ist auch  $X \cup Y \in \mathfrak{a}$ .  
(ii) 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:

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

51. Sei  $n$  eine positive natürliche Zahl. Definiere die **Eulersche  $\varphi$ -Funktion** durch

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

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

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

- (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

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

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  $R$ .