 Algebra I 

# Serie 9

RINGE, EINHEITENGRUPPE

---

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

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

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

zu einem Ring wird.

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

$$X*Y := X\cap Y\,, \qquad X+Y := (X\backslash Y)\cup(Y\backslash X)\,.$$

(a) Zeige, dass $\big(\mathscr{P}(S),\varnothing,S,+,*\big)$ ein kommutativer Ring ist.

(b) Sei $\mathfrak{a}\subseteq\mathscr{P}(S)$ eine nicht-leere Teilmenge von $\mathscr{P}(S)$ 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 $\mathscr{P}(X)\subseteq\mathfrak{a}$.

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

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

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

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

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

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

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

**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 $R$.