Algebra I

Serie 8

Ringe, Ideale, Einheitengruppe Abgabe bis 25. November

---

50. Sei R ein Ring und sei $\mathrm{Mat}(n, R)$ der Ring der $n \times n$-Matrizen mit Koeffizienten in R mit der üblichen Addition und Multiplikation.

(a) Zeige: Ist $\mathfrak{a} \subseteq R$ ein Ideal, so ist $\mathrm{Mat}(n, \mathfrak{a})$ ein Ideal in $\mathrm{Mat}(n, R)$.

(b) Zeige: Jedes Ideal in $\mathrm{Mat}(n, R)$ ist von der Form $\mathrm{Mat}(n, \mathfrak{a})$ für ein geeignetes Ideal $\mathfrak{a} \subseteq R$.

(c) Sei $\mathfrak{a} \subseteq R$ ein Ideal in R.
Zeige:

$$\mathrm{Mat}(n, R/\mathfrak{a}) \;\cong\; \mathrm{Mat}(n, R)/\,\mathrm{Mat}(n, \mathfrak{a})\,.$$

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

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

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

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

(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 $(\bar{1}\bar{3}, \bar{1}\bar{3}, \bar{1}\bar{3})$ in R.

53. Sei $\mathbb{F}$ ein Körper und sei $P = a_n X^n + \ldots a_1 X^1 + a_0$ ein Polynom mit Koeffizienten a_i in $\mathbb{F}$ vom Grad $n \geq 1$ (*d.h.* $a_n \neq 0$).

(a) Zeige: Ist, für ein $q \in \mathbb{F}$, $P(q) = 0$, so existiert ein Polynom Q vom Grad $n - 1$ mit $P = (X - q) \cdot Q$.

(b) Zeige: P hat höchstens n verschiedene Nullstellen in $\mathbb{F}$.

54. Zeige: Ist $\mathbb{F}$ ein endlicher Köper, so ist die multiplikative Einheitengruppe $\mathbb{F}^*$ zyklisch.

Hinweis: Verwende den Hauptsatz über endlich erzeugte abelsche Gruppen und betrachte die Nullstellen des Polynoms $X^n - 1$ (für ein geeignetes n).

55. Zeige: Für $m \in \mathbb{N}$ ist $\mathbb{Z}/m\mathbb{Z}$ genau dann ein Körper wenn m prim ist.

56. (a) Seien $m, n \in \mathbb{N}$ zwei positive Zahlen und seien $\mathfrak{a} := (m)$ und $\mathfrak{b} := (n)$ die von m *bzw.* n erzeugten Ideale.
Zeige: $\mathfrak{a} + \mathfrak{b} = \mathbb{Z} \iff (m, n) = 1$.

(b) Finde die kleinste positive Zahl $a \in \mathbb{N}$ mit

$$\begin{aligned} a &\equiv 5 \pmod{9}, \\ a &\equiv 8 \pmod{11}, \\ a &\equiv 2 \pmod{14}. \end{aligned}$$