Übungsblatt 4

Aufgabe 1

a) Bestimmen Sie alle Ideale in $\mathbb{Z}/15\mathbb{Z}$.

b) Sei p eine Primzahl. Bestimmen Sie die Primideale sowie die maximalen Ideale in $\mathbb{Z}_{(p)}$ (vgl. Blatt 3 Aufgabe 4).

c) Geben Sie ein maximales Ideal in $\mathbb{Z}[X]$ an.

Aufgabe 2

Sei R ein kommutativer Ring, und sei $g \in R[X]$ ein Polynom, dessen Höchstkoeffizient eine Einheit ist, d.h.

$$g = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \text{ mit } a_n \in R^\times .$$

Zeigen Sie, dass sich Elemente aus $R[X]$ eindeutig mit Rest durch g dividieren lassen. In anderen Worten, zeigen Sie, dass zu $f \in R[X]$ Polynome $h, r \in R[X]$ existieren, welche den Bedingungen $f = gh + r$ und $\deg r < n$ genügen, und dass h, r durch diese Bedingungen eindeutig bestimmt sind.

Aufgabe 3

a) Geben Sie alle Elemente von $(\mathbb{Z}/11\mathbb{Z})^\times$ an, welche diese Gruppe erzeugen.

b) Geben Sie ein $m \in \mathbb{N}$ an, für welches die Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ nicht zyklisch ist.

Aufgabe 4

Sie $p \geq 3$ eine Primzahl. Zeigen Sie, dass die Zuordnung $x \mapsto x^{\frac{p-1}{2}}$ einen Homomorphismus

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \{1, -1\}$$

erklärt. Zeigen Sie ferner, dass die Menge der Quadrate in $(\mathbb{Z}/p\mathbb{Z})^\times$ mit dem Kern dieses Homomorphismus übereinstimmt. Sie dürfen verwenden, dass $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch ist.

(bitte wenden)

Zusatzaufgabe

Ist G eine endliche Gruppe und ist $n \in \mathbb{N}_{\geq 1}$, so bezeichne $\psi_G(n)$ die Anzahl der Elemente von G, welche die Ordnung n besitzen.

a) Zeigen Sie, dass $\psi_{\mathbb{Z}/n\mathbb{Z}}(n)$ mit der Mächtigkeit der Menge

$$\{d \in \mathbb{N}\,;\, 1 \leq d \leq n\,,\, (d,n) = 1\}$$

der zu n teilerfremden ganzen Zahlen zwischen 1 und n übereinstimmt. Die Funktion

$$\varphi : \mathbb{N}_{\geq 1} \to \mathbb{N} \quad , \quad n \mapsto \psi_{\mathbb{Z}/n\mathbb{Z}}(n)$$

heißt die Eulersche φ-Funktion.

b) Zeigen Sie

$$\sharp G \;=\; \sum_{1 \leq d} \psi_G(d) \quad \text{sowie} \quad n \;=\; \sum_{1 \leq d | n} \varphi(d) \quad \forall n \in \mathbb{N}\,.$$

Verwenden Sie zum Beweis der zweiten Gleichheit die Tatsache, dass die Gruppe $\mathbb{Z}/n\mathbb{Z}$ für $1 \leq d | n$ genau eine Untergruppe der Ordnung d besitzt.

c) Sei p eine Primzahl, und sei $G = (\mathbb{Z}/p\mathbb{Z})^\times$ die Einheitengruppe des Körpers $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Zeigen Sie die Abschätzung

$$\psi_G(d) \leq \varphi(d) \quad \forall 1 \leq d | p-1\,;$$

verwenden Sie hierzu die Tatsache, dass ein Polynom $f \in \mathbb{F}_p[X]$ vom Grad d nicht mehr als d Nullstellen in $\mathbb{F}_p$ besitzen kann. Folgern Sie, dass $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch ist.