Serie 11

Der Polynomring $\mathbb{F}_p[X]$

Im Folgenden sei p eine Primzahl und $\mathbb{F}_p[X]$ sei der Ring der Polynome mit der Unbestimmten X und Koeffizienten in $\mathbb{F}_p$. Für Polynome

$$f = a_0 + a_1X + \ldots + a_nX^n \in \mathbb{F}_p[X]$$

ist der **Grad** von f die Zahl $\deg(f) := \max\{k \in \mathbb{N} : a_k \neq 0\}$, falls solch eine Zahl existiert, sonst sei $\deg(f) := -\infty$.

38. Für $f, g \in \mathbb{F}_p[X]$ sei $d \in \mathbb{F}_p[X]$ ein ggT von f und g, falls $d \mid f$ und $d \mid g$ sowie aus $h \mid f$ und $h \mid g$ folgt $h \mid d$.

(a) Bestimme einen ggT der beiden Polynome

$$2X^4 + 5X^3 + 6X^2 + 6X + 1,\ X^3 + 6X + 1 \in \mathbb{F}_7[X]$$

Hinweis: Verwende den vEA.

(b) Zeige: Ist $d \in \mathbb{F}_p[X]$ ein ggT von $f, g \in \mathbb{F}_p[X]$, so ist für alle $a \in \mathbb{F}_p \backslash \{0\}$ auch $a \cdot d$ ein ggT von f und g.

(c) Zeige: Sind d_1 und d_2 zwei ggT von $f, g \in \mathbb{F}_p[X]$, dann existiert ein $a \in \mathbb{F}_p$ mit $a \cdot d_1 = d_2$.

39. Für $f \in \mathbb{F}_p[X]$ sei $(f) := \{g \cdot f : g \in \mathbb{F}_p[X]\}$.

(a) Zeige, dass für alle $f \in \mathbb{F}_p[X]$, $(f) \subseteq \mathbb{F}_p[X]$ ein Ideal ist.

(b) Bestimme $\mathbb{F}_p[X]/(0)$, $\mathbb{F}_p[X]/(r)$ für $r \in \mathbb{F}_p \backslash \{0\}$, $\mathbb{F}_p[X]/(X)$, $\mathbb{F}_p[X]/(X+1)$, und $\mathbb{F}_p[X]/(X^5)$.

(c) Zeige: Das Ideal $(f) \subseteq \mathbb{F}_p[X]$ für $f \in \mathbb{F}_p[X]$ mit $\deg(f) > 0$ ist genau dann maximal, wenn aus $g \cdot h = f$ für $g, h \in \mathbb{F}_p[X]$ folgt $\deg(g) = 0$ oder $\deg(h) = 0$.

40. Sei $f = X^3 + X + 1 \in \mathbb{F}_7[X]$.

(a) Zeige, dass das Ideal $(f) \subseteq \mathbb{F}_7[X]$ ein maximales Ideal ist.

(b) Wie viele Elemente besitzt der Körper $\mathbb{F}_7[X]/(f)$?

(c) Berechne $(X^2 + 2)^{-1}$ im Körper $\mathbb{F}_7[X]/(f)$.
Hinweis: Vergleiche mit Aufgabe 37.

41. Konstruiere einen Körper mit 8 Elementen.