Serie 18

ENDLICHE KÖRPER I

---

91. (a) Zeigen Sie: Ist K ein endlicher Körper mit $|K| = p^n$ (für $n \geqslant 1$ und p prim), so ist K der Zerfällungskörper von $X^{p^n} - X$ über $\mathbb{F}_p$.

(b) Zeigen Sie: Sind K und K' endliche Körper mit $|K| = |K'|$, so sind K und K' isomorph.

92. Bestimmen Sie die Anzahl der irreduziblen Polynome $f \in \mathbb{F}_3[X]$ vom Grad 6.

93. Wir definieren das irreduzible Polynom $f := X^3 + X + 1$ über $\mathbb{F}_7$. Berechnen Sie $(X^2+2)^{-1}$ im Körper $\mathbb{F}_7[X]/(f)$.

94. Sei $\mathbb{F}_q$ ein Körper der Ordnung $q = p^n$ für $n \geqslant 1$ und p prim, und seien $a, b \in \mathbb{F}_q$. Zeigen Sie, dass in $\mathbb{F}_q$ folgendes gilt:

(a) $(a+b)^p = a^p + b^p$.

(b) $a^p = a \iff a \in \mathbb{F}_p$.

95. Sei p eine Primzahl und sei $q = p^n$ für eine positive ganze Zahl n.

(a) Zeigen Sie: Ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ teilt $X^q - X$ in $\mathbb{F}_p[X]$ genau dann, wenn der Grad von f ein Teiler von n ist.

(b) Sei I_d die Menge der normierten, irreduziblen Polynome vom Grad d in $\mathbb{F}_p[X]$. Beweisen Sie die Gleichung

$$X^q - X = \prod_{d|n} \prod_{f \in I_d} f.$$

(c) Sei $r_d := |I_d|$. Schliessen Sie $\sum_{d|n} \big(d \cdot r_d\big) = q$ aus (b).

(d) Zeigen Sie: Die Summe der Grade aller normierten, irreduziblen Polynome, deren Grad n teilt, ist gleich q.