Serie 18

ENDLICHE KÖRPER II

---

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

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

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

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

(c) Sei $r_d := |I_d|$. Folgere aus (b), dass $\sum_{d|n} \big(d \cdot r_d\big) = q$ gilt.

(d) Zeige: Das Polynom $X^q - X$ ist über $\mathbb{F}_p$ das Produkt aller normierten irreduziblen Polynome vom Grad m mit $m \mid n$.

(e) Zeige: Die Summe der Grade der irreduziblen Polynome aus (d) ist gleich q.

100. Sei p eine Primzahl, sei K ein Körper der Charakteristik p und sei $K \to K, x \mapsto x^p$ der Frobeniushomomorphismus.

(a) Zeige: Der Frobeniushomomorphismus ist injektiv.

(b) Zeige: Ist K ein endlicher Körper, so ist der Frobeniushomomorphismus ein Automorphismus des Körpers K.

101. Finde für $q = 8$, 9, 16 das Minimalpolynom über $\mathbb{F}_2$ *bzw.* $\mathbb{F}_3$ eines Erzeugers von $\mathbb{F}_q^*$.

102. Sei $q = 3^3$ und sei $\mathbb{F}_q := \mathbb{F}_3[X]/(X^3 + X^2 + X + 2)$ ein Körper der Ordnung q.

(a) Bestimme die Nullstellen des Polynoms $(Y^3 + Y^2 + Y + 2) \in \mathbb{F}_q[Y]$.

(b) $Y = (2\,X + 1)$ ist eine Nullstelle des Polynoms $g = (Y^3 + 2\,Y^2 + 1) \in \mathbb{F}_q[Y]$. Bestimme die anderen Nullstellen von g.

(c) Zeige, dass das Polynom $(Y^2 + Y + 2) \in \mathbb{F}_q[Y]$ keine Nullstellen in $\mathbb{F}_q$ hat.

103. Zeige, dass ein endlicher Körper nie algebraisch abgeschlossen ist.