Algebra II

Serie 15

Endliche Körper Abgabe 20. März

Sei p eine Primzahl.

90. Sei $L := \mathbb{F}_p(t)$ der Körper der rationalen Funktionen über $\mathbb{F}_p$ in der Variablen t (d.h. der Quotientenkörper des Polynomrings $\mathbb{F}_p[t]$) und sei $K := \mathbb{F}_p(t^p)$.

Zeige: Das Polynom $X^p - t^p$ ist irreduzibel und inseparabel über K, und L ist sein Zerfällungskörper.

91. 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: Der Frobeniushomomorphismus ist genau dann surjektiv, wenn jedes Polynom in $K[X]$ separabel ist.

Bemerkung: Ein Körper, über den jedes Polynom separabel ist, heisst *perfekt*.

92. 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) Folgere daraus, dass $\sum_{d|n} \big(d \cdot |I_d|\big) = q$ gilt.

(d) Bestimme die Anzahl der irreduziblen Polynome vom Grad 6, 7, 8 in $\mathbb{F}_2[X]$.

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

94. (a) Zeige, dass das Polynom $f(X) = X^3 + 3X + 3$ irreduzibel in $\mathbb{F}_5[X]$ ist.

(b) Sei α eine Nullstelle von f in einem Zerfällungskörper von f. Sei $\mathbb{F}_{125} = \mathbb{F}_5(\alpha)$. Berechne die Darstellungsmatrix des Frobeniusautomorphismus $\mathrm{Frob}_5 \colon \mathbb{F}_{125} \to \mathbb{F}_{125}$ in der Basis $(1, \alpha, \alpha^2)$.

(c) Schreibe das Element $\beta := 1/(1-\alpha) \in \mathbb{F}_{125}$ als $\mathbb{F}_5$-Linearkombination von $1, \alpha$ und α^2.

(d) Zeige, dass α die zyklische Gruppe $\mathbb{F}_{125}^*$ erzeugt.