

Algebra I, WS 04/05

Blatt 14**Aufgabe 56 (2+2+2+9 Punkte).**

Sei K ein unendlicher Körper, sei $E|K$ eine Galoiserweiterung von Grad $n := [E : K]$, und sei $a \in E$ ein primitives Element, d.h. sei $E = K(a)$. Sei $\text{Gal}(E|K) = \{\sigma_1, \dots, \sigma_n\}$ durchnummeriert, wobei $\sigma_1 = \text{id}$.

- (1) Sei $f(X) := \frac{\mu_{a,K}(X)}{(X-a)\mu'_{a,K}(a)} \in E[X]$. Zeige, daß $f(a) = 1$ und daß $f^{\sigma_i}(a) = 0$ für $i \in [2, n]$.
- (2) Sei $d(X) := \det \left(f^{\sigma_i^{-1} \circ \sigma_j}(X) \right)_{i,j \in [1,n]} \in E[X]$. Zeige, daß $d(a) = 1$. Folgere, daß $d(X) \neq 0$.
- (3) Zeige, daß es ein $b \in K$ gibt mit $d(b) \neq 0$. Zeige, daß für $c := f(b) \in E$ das Tupel $(\sigma_1(c), \dots, \sigma_n(c))$ eine Basis von E über K bildet. Eine Basis dieser Form heißt auch *Normalbasis*.
(Hinweis: Zeige lineare Unabhängigkeit; wende auf diesbezüglichen Ansatz Automorphismen an.)
- (4) Bestimme Normalbasen für die folgenden Galoiserweiterungen.
 - (i) $\mathbb{C}|\mathbb{R}$.
 - (ii) $\mathbb{Q}(\zeta_8)|\mathbb{Q}$.
 - (iii) $\mathbb{Q}(X_1, X_2, X_3)|\mathbb{Q}(s_1, s_2, s_3)$, vgl. Aufgabe 54.

Aufgabe 57 (4+6+4+6 Punkte).

- (1) Sei $\mathbf{F}_8 := \mathbf{F}_2[T]/(T^3 + T + 1)$ und schreibe $\beta := \bar{T}$. Berechne β^i für $i \in [0, 7]$ als Linearkombinationen in $(\beta^0, \beta^1, \beta^2)$.
- (2) Bestimme alle irreduziblen normierten Polynome von Grad 2 in $\mathbf{F}_8[X]$. Konstruiere mit einem von ihnen den Körper $\mathbf{F}_{64}$.
- (3) Bestimme Erzeuger über $\mathbf{F}_2$ für alle echten Zwischenkörper zwischen $\mathbf{F}_2$ und $\mathbf{F}_{64}$.
- (4) Konstruiere mittels eines irreduziblen Polynoms von Grad 3 in $\mathbf{F}_8[X]$ den Körper $\mathbf{F}_{512}$. Verwende ein primitives Element in $\mathbf{F}_{512}$ über $\mathbf{F}_2$ zur Bestimmung eines irreduziblen Polynoms von Grad 9 in $\mathbf{F}_2[X]$.

Aufgabe 58 (2+2+2 Punkte).

Sei p eine Primzahl, sei $r \geq 1$ und sei $q = p^r$. Sei l eine weitere Primzahl (gleich oder ungleich p), und sei $m \geq 1$.

- (1) Wieviele Zwischenkörper gibt es zwischen $\mathbf{F}_q$ und $\mathbf{F}_{q^{(l^m)}}$?
- (2) Wieviele normierte irreduzible Polynome von Grad l^m gibt es in $\mathbf{F}_q[X]$?
- (3) In wieviele normierte irreduzible Faktoren zerfällt $X^{q^{(l^m)}} - X \in \mathbf{F}_q[X]$?
Sind diese Faktoren paarweise verschieden?

Aufgabe 59 (3 Punkte).

Sei p eine Primzahl, sei $r \geq 1$ und sei $q = p^r$. Zeige oder widerlege.

- (1) Sei $f(X) \in \mathbf{F}_q[X]$ irreduzibel von Grad $n \geq 1$. Es hat $f(X)$ in $\mathbf{F}_{q^n}$ genau n verschiedene Nullstellen.
- (2) Es gibt einen Teilkörper von $\mathbf{F}_q(X)$ isomorph zu $\mathbf{F}_{q^2}$.
- (3) Sei $E|K$ eine Galoiserweiterung. Es ist $E^* \longrightarrow K^*$, $x \longmapsto N_{E|K}(x)$ surjektiv.