

5. Übung Algebra II

1. Aufgabe Kreisteilungspolynome

(2 Punkte)

Zerlege die folgenden Polynome

(a) $\Phi_5(t)$ und $\Phi_{12}(t)$ über $\mathbb{F}_{11}$

(b) $\Phi_4(t)$ über $\mathbb{F}_5, \mathbb{F}_{13}$ und $\mathbb{F}_{17}$.

2. Aufgabe Kreisteilungspolynome

(6 Punkte)

Zeige folgende Aussagen:

(a) Für jede ungerade Zahl $n > 1$ gilt $\Phi_{2n}(t) = \Phi_n(-t)$.

(b) Ist p Primzahl und $m \in \mathbb{N}^{>0}$ mit $p|m$, so gilt $\Phi_{pm}(t) = \Phi_m(t^p)$

(c) Ist p Primzahl, so gilt

$$\Phi_{p^k}(t) = t^{(p-1)p^{k-1}} + t^{(p-2)p^{k-1}} + \dots + t^{p^{k-1}} + 1.$$

(d) Für jede Primzahl p und $n \in \mathbb{N}$ mit $\text{ggT}(p, n) = 1$ gilt

$$\Phi_{pn}(t) = \frac{\Phi_n(t^p)}{\Phi_n(t)}.$$

(e) Für alle $n \in \mathbb{N}$ mit $n > 1$ gilt

$$\Phi_n(t^{-1}) = \Phi_n(t)t^{-\phi(n)}$$

wobei ϕ die Eulersche Phi-Funktion ist.

3. Aufgabe Norm und Spur

(2 Punkte)

Es sei F/K eine endliche Körpererweiterung. Dann ist F ein K -Vektorraum der Dimension $n = [F : K]$. Für $\alpha \in F$ definieren wir $\phi_\alpha : F \rightarrow F$, $x \mapsto \alpha \cdot x$. Zeige folgende Aussagen:

- (a) Die Abbildung ϕ_α ist ein Vektorraumendomorphismus. Für $\alpha \neq 0$ ist diese Abbildung sogar ein Automorphismus.
- (b) Die Abbildung $F \rightarrow \text{End}(F)$, $\alpha \mapsto \phi_\alpha$ ist K -linear. Ferner gilt $\phi_\alpha \phi_\beta = \phi_{\alpha\beta}$.
- (c) Es sei m_α das Minimalpolynom von α über K , f das charakteristische Polynom von ϕ_α und M das Minimalpolynom von ϕ_α . Dann gilt $m_\alpha = M$ und $f = M^l$ mit $l \in \mathbb{N}$ geeignet.
- (d) Für eine beliebige Basis $b_1, \dots, b_n$ von F entspreche ϕ_α der Matrix M_α . Dann gilt

$$\det(M_\alpha) = N_{F/K}(\alpha) \quad \text{und} \quad \text{Tr}(M_\alpha) = \text{Tr}_{F/K}(\alpha).$$

4. Aufgabe Praktische Aufgabe

(6 Punkte)

Sei $p > 2$ Primzahl und $q = p^m$ mit $m \in \mathbb{N}$. Schreibe einen Algorithmus, der ein gegebenes normiertes quadratfreies Polynom f vom Grad n aus $\mathbb{F}_q[x]$ faktorisiert. Gehe dazu folgendermaßen vor:

- (a) Benutze den vorgegebenen Algorithmus *Faktorisierung.g* auf der Algebra2-Homepage, welcher ein Polynom f aus $\mathbb{F}_q[x]$ und euren Algorithmus erwartet. Der Algorithmus ruft euren Algorithmus mit dem quadratfreien Anteil von f auf.
- (b) Betrachte den Vektorraum $R := \mathbb{F}_q[x]/(f)$ der Dimension n über $\mathbb{F}_q$ und die $\mathbb{F}_q$ -lineare Abbildung

$$\beta : R \rightarrow R, \quad a \mapsto a^q - a. \quad (1)$$

Eine Basis des $\mathbb{F}_q$ -Vektorraumes R ist $1 \bmod f, x \bmod f, \dots, x^{n-1} \bmod f$. Ist $f = f_1 \cdots f_r$ die Faktorisierung von f in verschiedene irreduzible Faktoren $f_i \in \mathbb{F}_q[x]$, so ist

$$R \cong \mathbb{F}_q[x]/(f_1) \times \cdots \times \mathbb{F}_q[x]/(f_r). \quad (2)$$

- (c) Nun gilt für $a \in R$:

$$a \in \ker(\beta) \Leftrightarrow \chi(a) = (a_1, \dots, a_r)$$

mit $a_i \in \mathbb{F}_q$, $i = 1, \dots, r$ wobei χ der Isomorphismus von (??) ist.

- (d) Berechne nun den Kern von β mittels der Darstellungsmatrix. Ist dann $b_1, \dots, b_r$ eine Basis des Kern von β , so bilde $a := \sum_{i=1}^r c_i b_i$ mit $c_i \in \mathbb{F}_q$ zufällig gewählt.
- (e) Berechne nun den ggT(f, a) und ggT($b - 1, f$) wobei $b := a^{(q-1)/2} \bmod f$ ist.

Warum funktioniert dieser Algorithmus?