Véges testek és alkamazásaik / 2006 ősz / Küronya Alex

## 2. Házi feladat

1. ∘ (Véges test feletti polinominterpoláció) Határozzuk meg azt a negyedfokú fokú $f \in \mathbb{F}_7[X]$ polinomot, amelyre $f(0) = 0, f(1) = 3, f(2) = 1, f(3) = 2,\ f(4) = -1$.

Definíció: Legyenek $\mathbb{E} \subseteq \mathbb{F}$ véges testek, $\mathbb{E}$ $q$ elemmel, $\mathbb{F}$ pediq $q^k$ elemmel. Tetszőleges $a \in \mathbb{F}$ esetén az $a$ elem *nyom*át, illetve *norm*áját az alábbi módon definiáljuk:

$$\mathrm{Tr}_{\mathbb{F}/\mathbb{E}} : \mathbb{F} \to \mathbb{E} \qquad a \mapsto \sum_{i=0}^{k-1} a^{q^i}$$

$$\mathrm{Nm}_{\mathbb{F}/\mathbb{E}} : \mathbb{F} \to \mathbb{E} \qquad a \mapsto \prod_{i=0}^{k-1} a^{q^i} \ ,$$

2. * $(i)$ Igazoljuk, hogy az imént definiált nyom egy $\mathbb{E}$-lineáris leképezés, ami valóban $\mathbb{E}$-be képez. Mutassuk meg továbbá azt is, hogy a nyom szürjektív.
$(ii)$ Hasonlóképpen bizonyítsuk be, hogy a norma jóldefiniált, multiplikatív, $k$-adfokú homogén, és $\mathbb{E}^\times$-t $\mathbb{F}^\times$-re képzi.

3. * Legyen $p$ prímszám, $q = p^k$, $\zeta \in \mathbb{C}$ egy primitív $p$-edik egységgyök. Jelölje $\psi : \mathbb{F}_q \to \mathbb{C}$ a

$$\psi(a) \stackrel{\mathrm{def}}{=} \zeta^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}$$

függvényt. Mutassuk meg az alábbiakat:

(1) Minden $a, b \in \mathbb{F}_q$ esetén $\psi(a+b) = \psi(a)\psi(b)$.
(2) Létezik olyan $a \in \mathbb{F}_q$, amelyre $\psi(a) \neq 1$.
(3) $\sum_{a \in \mathbb{F}_q} \psi(a) = 0$.

4. Tekintsük véges testek bővítéseinek egy $\mathbb{E} \subseteq \mathbb{F} \subseteq \mathbb{K}$ sorozatát. Mutassuk meg, hogy minden $a \in \mathbb{K}$-ra

(1) $\mathrm{Tr}_{\mathbb{K}/\mathbb{E}}(a) = \mathrm{Tr}_{\mathbb{F}/\mathbb{E}}(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(a))$ ,
(2) $\mathrm{Nm}_{\mathbb{K}/\mathbb{E}}(a) = \mathrm{Nm}_{\mathbb{F}/\mathbb{E}}(\mathrm{Nm}_{\mathbb{K}/\mathbb{F}}(a))$ .

5. Legyenek ismét $\mathbb{E} \subseteq \mathbb{F}$ véges testek, $[\mathbb{F} : \mathbb{E}] = n$, $a \in \mathbb{F}$ tetszőleges. Jelölje

$$f(X) \stackrel{\mathrm{def}}{=} X^d - c_1 X^{d-1} + \cdots + (-1)^d c_d \in \mathbb{E}[X]$$

az $a$ elem minimálpolinomját $\mathbb{E}$ felett. Bizonyítsuk be, hogy

$$\mathrm{Tr}_{\mathbb{F}/\mathbb{E}}(a) \ = \ \frac{n}{d} c_1 \ , \ \mathrm{Nm}_{\mathbb{F}/\mathbb{E}}(a) \ = \ c_d^{n/d} \ .$$

6. Írjuk le az $\mathbb{F}_3 \subseteq \mathbb{F}_9$ bővítéshez tartozó nyomot és normát.

Definíció: Legyen $\mathbb{E} \subseteq \mathbb{F}$ véges testek egy bővítése. A hozzá tartozó $G(\mathbb{F}/\mathbb{E})$ ún. *normagráf*ot az alábbi módon definiáljuk: a gráf csúcspontjai az $\mathbb{F}$ test elemei, és az $a, b \in \mathbb{F}$ pontok között pontosan akkor megy él, ha $\mathrm{Nm}_{\mathbb{F}/\mathbb{E}}(a+b) = 1$.

7. * Számítsuk ki az $\mathbb{F}_3 \subseteq \mathbb{F}_9$, és az $\mathbb{F}_2 \subseteq \mathbb{F}_8$ testbővítésekhez tartozó normagráfokat.

8. ** Legyen $q$ prímhatvány, $n$ természetes szám, amelyekre $q \equiv 1 \pmod{n}$. Legyen továbbá $\mathbb{K}/\mathbb{F}_q$ $n$-edfokú testbővítés. Mutassuk meg, hogy minden $a \in \mathbb{F}^\times$ esetén az $x^n = a$ egyenletnek van $n$ $\mathbb{K}$-beli megoldása.

9. Legyen $\mathbb{K}$ tetszőleges test, $f \in \mathbb{K}[X]$ 1-főegyüttható̋s $n$-edfokú polinom, $A \stackrel{\mathrm{def}}{=} \mathbb{K}[X]/(f)$ az $f$ szerinti faktor-$\mathbb{K}$-algebra. Adjunk $O(n^3)$ $\mathbb{K}$-beli műveletet használó algoritmust egy $\alpha \in A$ elem $\mathbb{K}$ feletti minimálpolinomjának kiszámítására.