M2426 – Εφαρμοσμένη Άλγεβρα
Επαναληπτικές ασκήσεις

Θεόδουλος Γαρεφαλάκης

May 17, 2017

1. Δείξτε ότι το πολυώνυμο $f = X^3 - X - 2 \in \mathbb{F}_5[X]$ είναι ανάγωγο.
   (a) Έστω $\alpha \in \mathbb{F}_{5^3}$ μία ρίζα του f. Εκφράστε όλες τις ρίζες του f ως προς τη βάση $\{1, \alpha, \alpha^2\}$.
   (b) Υπολογίστε το $\mathrm{Tr}(\alpha)$.
   (c) Βρείτε ένα στοιχείο $\beta \in \mathbb{F}_{5^3}$, με $\mathrm{Tr}(\beta) = 1$.
   (d) Υπολογίστε μία βάση του $\ker(\mathrm{Tr})$.

2. Έστω $\alpha \in \mathbb{F}_{p^n}$ στοιχείο τέτοιο ώστε το σύνολο $\{\alpha, \ldots, \alpha^{p^{n-1}}\}$ είναι βάση της επέκτασης $\mathbb{F}_{p^n}/\mathbb{F}_p$.
   (a) Αποδείξτε ότι $\mathrm{Tr}(\alpha) \neq 0$.
   (b) Αποδείξτε ότι
   $$\ker(\mathrm{Tr}) = \left\{ c_1(\alpha^p - \alpha) + c_2(\alpha^{p^2} - \alpha) + \cdots + c_{n-1}(\alpha^{p^{n-1}} - \alpha) : c_1, c_2, \ldots, c_{n-1} \in \mathbb{F}_p \right\}.$$

3. Έστω C ένας γραμμικός $[n, k, d]$ κώδικας πάνω από το $\mathbb{F}_q$.
   (a) Δείξτε ότι για κάθε συντεταγμένη $1 \leq i \leq n$, είτε όλα τα διανύσματα του κώδικα έχουν 0 στην i συνεταγμένη ή κάθε στοιχείο $a \in \mathbb{F}_q$ εμφανίζεται στην i συντεταγμένη σε ακριβώς q^{k-1} διανύσματα του C.
   (b) Δείξτε ότι
   $$\sum_{c \in C} \|c\| \leq n(q-1)q^{k-1}.$$
   (c) Δείξτε ότι
   $$d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}.$$

4. Έστω C ένας γραμμικός $[n, k, d]$ κώδικας πάνω από το $\mathbb{F}_2$. Ορίζουμε τον κώδικα
   $$\bar{C} = \left\{ \left(c_1, \ldots, c_n, \sum_{i=1}^{n} c_i \right) \ : \ (c_1, \ldots, c_n) \in C \right\}.$$
   (a) Αποδείξτε ότι ο $\bar{C}$ έχει παραμέτρους $[n+1, k, \bar{d}]$, με
   $$\bar{d} = \begin{cases} d & , \text{αν } d \text{ άρτιος} \\ d+1 & , \text{αν } d \text{ περιττός.} \end{cases}$$
   (b) Έστω ότι ο C είναι MDS. Αποδείξτε ότι ο $\bar{C}$ είναι MDS αν και μόνο αν το d είναι περιττός.

5. Έστω q δυναμή πρώτου. Ένα πολυώνυμο $f \in \mathbb{F}_q[X]$ βαθμού n ονομάζεται πρωταρχικό εάν κάθε ρίζα του παράγει την ομάδα $\mathbb{F}_{q^n}^*$. Δείξτε ότι κάθε πρωταρχικό πολυώνυμο είναι και ανάγωγο. Δείξτε, με ένα αντιπαράδειγμα, ότι το αντίστροφο δεν ισχύει.

6. Έστω n ένας περιττός πρώτος. Δείξτε ότι *κάθε* ανάγωγο πολυώνυμο του $\mathbb{F}_q[X]$ είναι πρωταρχικό αν και μόνο αν $q = 2$ και $2^n - 1$ είναι πρώτος αριθμός.

7. Έστω n ένας σύνθετος αριθμός. Δείξτε ότι υπάρχει ανάγωγο πολυώνυμο του $\mathbb{F}_q[X]$ το οποίο δεν είναι πρωταρχικό.

8. Εξετάστε πόσα μονικά ανάγωγα πολυώνυμα βαθμού 4 υπάρχουν στο δακτύλιο $\mathbb{F}_2[X]$, των οποίων οι ρίζες δεν είναι γεννήτορες της ομάδας $\mathbb{F}_{16}^*$.

9. Έστω p πρώτος αριθμός και $n \in \mathbb{N}$. Το σώμα $\mathbb{F}_{p^m}$ θα το ονομάζουμε *γνήσια* ενδιάμεση επέκταση των $\mathbb{F}_p$ και $\mathbb{F}_{p^n}$ εάν $\mathbb{F}_p \subsetneq \mathbb{F}_{p^m} \subsetneq \mathbb{F}_{p^n}$.

   (a) Έστω ℓ_1, ℓ_2 διακεκριμένοι πρώτοι και $n = \ell_1\ell_2^2$. Υπολογίστε το πλήθος των γνήσιων ενδιάμεσων επεκτάσεων των $\mathbb{F}_p$, $\mathbb{F}_{p^n}$.

   (b) Βρείτε τον ελάχιστο φυσικό $n \geq 10$, με την ιδιότητα ότι υπάρχει ακριβώς μία γνήσια ενδιάμεση επέκταση των $\mathbb{F}_p$ και $\mathbb{F}_{p^n}$.

10. Έστω p πρώτος αριθμός και $n, m \in \mathbb{N}$. Ορίζουμε τη σύνθεση, $\mathbb{F}_{p^n} \cdot \mathbb{F}_{p^m}$ των δύο σωμάτων $\mathbb{F}_{p^n}$ και $\mathbb{F}_{p^m}$ να είναι το "ελάχιστο" σώμα που περιέχει τα $\mathbb{F}_{p^n}$ και $\mathbb{F}_{p^m}$, δηλαδή είναι (το μοναδικό) σώμα F με τις ιδιότητες:

    (a) $\mathbb{F}_{p^n} \subseteq F$ και $\mathbb{F}_{p^m} \subseteq F$,

    (b) Αν K σώμα και $\mathbb{F}_{p^n} \subseteq K$ και $\mathbb{F}_{p^m} \subseteq K$, τότε $F \subseteq K$.

    Αποδείξτε ότι $\mathbb{F}_{p^n} \cdot \mathbb{F}_{p^m} = \mathbb{F}_{p^k}$, οπου $k = \text{εκπ}(n, m)$.

11. Υπολογίστε την ελάχιστη επέκταση του $\mathbb{F}_3$ η οποία περιέχει όλες τις ρίζες του πολυωνύμου $(X^4 + X^3 + X^2 + X + 1)(X^3 - X - 1)$.

12. Έστω C ένας κώδικας πάνω από το $\mathbb{F}_2$ με παραμέτρους $[n, k, d]$ και την ιδιότητα $C = C^\perp$.

    (a) Δείξτε ότι το μήκος n είναι άρτιος αριθμός.

    (b) Δείξτε ότι το διάνυσμα $\mathbf{1} = (1, \ldots, 1)$ ανήκει στον C.
    Υπόδειξη: δείξτε ότι $\langle x, x\rangle = \langle x, \mathbf{1}\rangle$ για κάθε $x \in \mathbb{F}_2^n$.

    (c) Δείξτε ότι όλα τα διανύσματα του C έχουν άρτιο βάρος.