Θεωρία Σωμάτων
Φυλλάδιο ασκήσεων #6

Θεόδουλος Γαρεφαλάκης

8 Μαΐου 2015

1. Έστω p πρώτος αριθμός και $n, m \in \mathbb{N}$. Δείξτε ότι $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^d}$, όπου $d = \mu\kappa\delta(n, m)$.

2. Έστω F πεπερασμένο σώμα χαρακτηριστικής p και $F^p = \{a^p \ : \ a \in F\}$. Δείξτε ότι $F^p = F$. Δείξτε, με αντιπαράδειγμα, ότι η πρόταση δεν ισχύει εάν το σώμα F είναι χαρακτηριστικής p, αλλά όχι πεπερασμένο.

3. Δείξτε ότι τα πολυώνυμα $f = X^3 + X + 1, g = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ είναι ανάγωγα. Εάν α είναι μία ρίζα του f υπολογίστε την τάξη του στην ομάδα $\mathbb{F}_{2^3}^*$ και γράψτε τις ρίζες του g ως $\mathbb{F}_2$-γραμμικούς συνδυασμούς των $1, \alpha, \alpha^2$. Γενικότερα, εάν $f, g \in \mathbb{F}_p[X]$ είναι ανάγωγα πολυώνυμα βαθμού n δείξτε ότι κάθε ρίζα του g μπορεί να γραφεί ως $\mathbb{F}_p$-γραμμικός συνδυασμός των $1, \alpha, \ldots, \alpha^{n-1}$, όπου α είναι μία ρίζα του f.

4. Έστω q δύναμη πρώτου αριθμού, ℓ πρώτος αριθμός και $\nu \in \mathbb{N}$. Υπολογίστε το πλήθος των μονικών αναγώγων πολυωνύμων του $\mathbb{F}_q[X]$ βαθμού ℓ^ν.

5. Έστω $\mathbb{F}_q$ πεπερασμένο σώμα και $P \in \mathbb{F}_q[X]$ μονικό ανάγωγο πολυώνυμο βαθμού $n > 1$. Δείξτε ότι όλες οι ρίζες του P έχουν την ίδια τάξη στην ομάδα $\mathbb{F}_{q^n}^*$. Πόσα μονικά ανάγωγα πολυώνυμα βαθμού n έχουν ρίζες με τάξη $q^n - 1$;

6. Έστω K το σώμα ανάλυσης του $X^{15} - 1 \in \mathbb{F}_2[X]$. Υπολογίστε το βαθμό $[K : \mathbb{F}_2]$.

7. Έστω q δύναμη πρώτου και $f \in \mathbb{F}_q[X]$ ανάγωγο πολυώνυμο βαθμού n. Αποδείξτε ότι στην παραγοντοποίηση του f στο δακτύλιο $\mathbb{F}_{q^k}[X]$, όλοι οι ανάγωγοι παράγοντες του f έχουν τον ίδιο βαθμό, ο οποίος είναι ίσος με $n/(n, k)$.
   Υπόδειξη: Έστω $P \in \mathbb{F}_{q^k}[X]$ είναι ένας ανάγωγος παράγοντας του f και α μία ρίζα του. Εάν e είναι η τάξη του α, τότε το α είναι ρίζα του κυκλοτομικού πολυωνύμου Ψ_e, οπότε το f είναι ανάγωγος παράγοντας του Ψ_e στο δακτύλιο $\mathbb{F}_q[X]$. Όμοια το P είναι ανάγωγος παράγοντας του Ψ_e στο δακτύλιο $\mathbb{F}_{q^k}[X]$.