

M2426 – Εφαρμοσμένη Άλγεβρα

Θεόδουλος Γαρεφαλάκης

March 17, 2017

- Έστω το πολυώνυμο $f = X^2 - X - 1 \in \mathbb{F}_3[X]$.
 - Δείξτε ότι το f είναι ανάγωγο πάνω από το \mathbb{F}_3 .
 - Βρείτε το ελάχιστο πολυώνυμο πάνω από το \mathbb{F}_3 κάθε στοιχείου του \mathbb{F}_9 .
 - Κατατάξτε τα στοιχεία του \mathbb{F}_9^* ανάλογα με την τάξη τους.
- Έστω το πολυώνυμο $f = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$.
 - Δείξτε ότι το f είναι ανάγωγο πάνω από το \mathbb{F}_2 .
 - Δείξτε ότι οι ρίζες του είναι γραμμικώς ανεξάρτητες πάνω από το \mathbb{F}_2 .
- Βρείτε ένα ανάγωγο πολυώνυμο του $\mathbb{F}_2[X]$ βαθμού 4, οι ρίζες του οποίου να είναι γραμμικώς ανεξάρτητες πάνω από το \mathbb{F}_2 .
- Έστω p πρώτος αριθμός. Δείξτε ότι το $f = X^p - X + c \in \mathbb{F}_p[X]$ είναι ανάγωγο για κάθε $c \neq 0$.
- Στην άσκηση αυτή θα περιγράψουμε την παραγοντοποίηση του πολυωνύμου $f = X^{p^2} - X - 1 \in \mathbb{F}_p[X]$, όπου p είναι περιττός πρώτος.
 - Έστω α μία ρίζα του f . Δείξτε ότι για κάθε $j \in \mathbb{N}$ ισχύει $\alpha^{p^{2j}} = \alpha + j$ και $\alpha^{p^{2j+1}} = \alpha^p + j$.
 - Δείξτε ότι $\alpha \in \mathbb{F}_{p^{2p}}$.
 - Συμβολίζουμε με P_α το $\min(\alpha, \mathbb{F}_p)$. Εξετάστε ποιές είναι οι δυνατότητες για το $\deg P_\alpha$. Ειδικότερα, δείξτε ότι $\deg P_\alpha \in \{p, 2p\}$.
 - Δείξτε ότι αν $\deg P_\alpha = p$, τότε $P_\alpha = X^p - X - 2^{-1} \in \mathbb{F}_p[X]$.
 - Δείξτε ότι το f παραγοντοποιείται ως γινόμενο του P_α και $\frac{p-1}{2}$ αναγώγων βαθμού $2p$.