ΑΛΓΕΒΡΑ ΙΙ

Φθινοπωρινὸ ἐξάμηνο 2011

Καθηγητὴς Ν. Γ. Τζανάκης

Φυλλάδιο ἀσκήσεων 3

Παραδοτέο μέχρι τὴν Τρίτη 15/11 πρὶν ἀπὸ τὸ μάθημα

1. Ἔστω πρῶτος p καὶ ἀκέραιος $n = p^r m$, ὅπου $r \geq 0$ καὶ ὁ ἀκέραιος m δὲν διαιρεῖται ἀπὸ τὸν p. Δεῖξτε ὅτι ὑπάρχουν (σὲ κάποια ἐπέκταση τοῦ $\mathbb{F}_p$) ἀκριβῶς m διαφορετικὲς n-οστὲς ρίζες τοῦ $1 \in \mathbb{F}_p$.

2. Ἔστω σῶμα K, n περιττὸς ἀκέραιος καὶ $\zeta \in K$ πρωταρχικὴ n-ρίζα τοῦ $1 \in K$. Ἀποδεῖξτε ὅτι τὸ $-\zeta$ εἶναι πρωταρχικὴ $2n$-ρίζα τῆς μονάδος.

3. Ἀποδεῖξτε ὅτι κάθε πεπερασμένη ἐπέκταση K τοῦ $\mathbb{Q}$ περιέχει πεπερασμένο πλῆθος ριζῶν τῆς μονάδος.
   Ὑπόδειξη. Δεῖτε τὸ K ὡς ὑπόσωμα τοῦ $\mathbb{C}$. Τὸ σύνολο τῶν ριζῶν τῆς μονάδος, που περιέχονται στὸ K, εἶναι ὑποομάδα τῆς $(K^*, \cdot)$. Πάρετε ὡς δεδομένο (ἂν καὶ δὲν εἶναι δύσκολο νὰ τὸ ἀποδείξετε) ὅτι, ἂν ϕ εἶναι ἡ συνάρτηση τοῦ Euler, τότε $\lim_{n\to+\infty} \phi(n) = +\infty$.

4. Ἔστω σῶμα K χαρακτηριστικῆς $p > 0$ καὶ πρῶτος $\ell \neq p$. Δεῖξτε τὰ ἑξῆς:
   (α′) Ὑπάρχει ἐπέκταση L/K καὶ $\zeta \in L$, ἔτσι ὥστε ζ νὰ εἶναι πρωταρχικὴ ℓ-ρίζα τοῦ $1 \in K$ καὶ $L = K(\zeta)$.
   Ὑπόδειξη: Θεωρῆστε τὸ σῶμα ἀνάλυσης τοῦ $X^\ell - 1$ πάνω ἀπὸ τὸ K.
   (β′) Ἔστω $\Phi_\ell(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1 \in K[X]$. Ἀποδεῖξτε ὅτι τὸ $\Phi_\ell(X)$ ἀναλύεται πλήρως σὲ πρωτοβάθμιους παράγοντες τοῦ $L[X]$ καὶ ὅλες οἱ ρίζες του εἶναι πρωταρχικὲς ℓ-ρίζες τοῦ $1 \in K$.
   Ὑπόδειξη: Παρατηρῆστε ὅτι $(X-1)\Phi_\ell(X) = X^\ell - 1$.

5. Θεωροῦμε τὸ σῶμα $\mathbb{F}_p$ (p πρῶτος) καὶ ἕναν πρῶτο ℓ. Ἡ ἄσκηση αὐτὴ ἔχει σκοπὸ νὰ ἐξετάσει πῶς παραγοντοποιεῖται τὸ πολυώνυμο $\Phi_\ell(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1 \in \mathbb{F}_p[X]$ σὲ ἀνάγωγα πολυώνυμα τοῦ $\mathbb{F}_p[X]$.

   (α′) Ἂν $\ell = p$, τότε ἡ ἀνάλυση τοῦ $\Phi_\ell(X)$ εἶναι $\Phi_\ell(X) = (X-1)^{\ell-1}$.

   (β′) Ἔστω $\ell \neq p$, ζ πρωταρχικὴ ℓ-ρίζα τοῦ $1 \in \mathbb{F}_p$ στὴν ἀλγεβρικὴ κλειστότητα $\overline{\mathbb{F}}_p$ (βλ. προηγούμενη ἄσκηση) καὶ f ὁ ἐλάχιστος θετικὸς ἀκέραιος n μὲ τὴν ἰδιότητα $p^n \equiv 1 \pmod{\ell}$.

      i. Ἀποδεῖξτε ὅτι $\zeta \in \mathbb{F}_{p^f}$, ἐνῶ, γιὰ κάθε $1 \leq n < f$, $\zeta \notin \mathbb{F}_{p^n}$.

      ii. Συμπεράνατε ἀπὸ τὸ προηγούμενο ὅτι ὁ βαθμὸς τοῦ ζ πάνω ἀπὸ τὸ $\mathbb{F}_p$ εἶναι f, ἄρα τὸ ἐλάχιστο πολυώνυμο τοῦ ζ πάνω ἀπὸ τὸ $\mathbb{F}_p$ εἶναι βαθμοῦ f.

iii. Ἀπὸ τὴν ἄσκηση 4(β′), ὅλες οἱ ρίζες τοῦ $\Phi_\ell(X)$ εἶναι πρωταρχικὲς ℓ-ρίζες τοῦ $1 \in \mathbb{F}_p$. Συνδυᾶστε αὐτὸ μὲ τὸ ἀμέσως προηγούμενο ἐρώτημα καὶ συμπεράνατε ὅτι τὸ $\Phi_\ell(X)$ εἶναι γινόμενο $(\ell-1)/f$ διαφορετικῶν μεταξύ τους ἀναγώγων πολυωνύμων τοῦ $\mathbb{F}_p[X]$, καθένα ἀπὸ τὰ ὁποῖα εἶναι βαθμοῦ f.

iv. Βασισμένοι στὰ προηγούμενα, ἀποδεῖξτε ὅτι τὸ $\Phi_7(X) \in \mathbb{F}_p$ ἀναλύεται ὡς ἑξῆς σὲ ἀνάγωγα πολυώνυμα τοῦ $\mathbb{F}_p[X]$: Ἂν $p = 7$, τότε $\Phi_7(X) = (X-1)^6$. Ἂν $p \equiv 1 \pmod 7$, τὸ $\Phi_7(X)$ εἶναι γινόμενο ἕξι διαφορετικῶν πρωτοβαθμίων πολυωνύμων τοῦ $\mathbb{F}_p[X]$. Ἂν $p \equiv 6 \pmod 7$, τὸ $\Phi_7(X)$ εἶναι γινόμενο τριῶν διαφορετικῶν δευτεροβαθμίων ἀναγώγων πολυωνύμων τοῦ $\mathbb{F}_p[X]$. Ἂν $p \equiv 2, 4 \pmod 7$, τὸ $\Phi_7(X)$ εἶναι γινόμενο δύο διαφορετικῶν τριτοβαθμίων ἀναγώγων πολυωνύμων τοῦ $\mathbb{F}_p[X]$. Ἂν $p \equiv 3, 5 \pmod 7$, τὸ $\Phi_7(X)$ εἶναι ἀνάγωγο στὸ $\mathbb{F}_p[X]$.