ΑΛΓΕΒΡΑ ΙΙ

Φθινοπωρινὸ ἑξάμηνο 2011

Καθηγητὴς Ν. Γ. Τζανάκης

Φυλλάδιο ἀσκήσεων 5

Παραδοτέο μέχρι 20-12-2011,πρὶν ἀπὸ τὸ μάθημα

1. Ἔστω L/K πεπερασμένη ἐπέκταση, $\theta \in L$ καὶ $f(X) \in K[X]$ τὸ ἐλάχιστο πολυώνυμο τοῦ θ πάνω ἀπὸ τὸ K. Δεῖξτε ὅτι τὸ πλῆθος τῶν μονικῶν πολυωνύμων $g(X) \in L[X]$, τὰ ὁποῖα διαιροῦν τὸ $f(X)$ (διαιρετότητα στὸ $L[X]$) εἶναι πεπερασμένο.

   Ὑπόδειξη. Θεωρῆστε τὴν κανονικὴ κλειστότητα, ἔστω M, τοῦ L πάνω ἀπὸ τὸ K καὶ ἀναλῦστε τὸ $f(X)$ σὲ πρωτοβάθμιους παράγοντες τοῦ $M[X]$. Τί μορφὴ ἔχει τὸ $g(X) \in L[X]$ ὅταν $g(X)|f(X)$;

2. Ἀποδεῖξτε καὶ μὲ τοὺς τρεῖς κατωτέρω τρόπους ὅτι $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Ὁ πρῶτος τρόπος εἶναι σαφῶς πολὺ ἁπλούστερος, ἀλλὰ ἔχει τὸ μειονέκτημα ὅτι μπορεῖ νὰ ἐφαρμοστεῖ σὲ εἰδικές, μόνο, περιπτώσεις.

   Πρῶτος τρόπος: Ἐκφρᾶστε τὸ β^{-1} χωρὶς ριζικὰ στὸν παρονομαστὴ καὶ συνδυᾶστε τὸ β μὲ τὸ β^{-1}.

   Δεύτερος τρόπος: Θέτοντας $\beta = \sqrt{2} + \sqrt{3}$, ὑπολογῖστε ἕνα πολυώνυμο μὲ ἀκέραιους συντελεστές, τὸ ὁποῖο ἔχει ρίζα τὸ β καὶ μετὰ ἀποδεῖξτε ὅτι τὸ πολυώνυμο αὐτὸ εἶναι ἀνάγωγο πάνω ἀπὸ τὸ $\mathbb{Q}$. Συμπεράνατε τὸν βαθμὸ τοῦ β, ἄρα ....

   Τρίτος τρόπος: Ἔστω $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Ἀποδεῖξτε ὅτι ἡ ἐπέκταση $L/\mathbb{Q}$ εἶναι Galois καὶ ἡ ὁμάδα Galois $\mathcal{G}(L/\mathbb{Q})$ εἶναι ἰσόμορφη μὲ τὴν *ὁμάδα τῶν τεσσάρων τοῦ Klein* $V = \langle \sigma, \tau : \sigma^2 = \tau^2 = 1, \, \sigma\tau = \tau\sigma \rangle$. Γνωρίζοντας τὸ πλῆθος τῶν γνησίων ὑποομάδων τῆς V συμπεράνατε πόσες εἶναι οἱ ἐνδιάμεσες ἐπεκτάσεις τῆς $L/\mathbb{Q}$ βαθμοῦ 2 καὶ προσδιορίσετε ποιές, συγκεκριμένα, εἶναι αὐτές. Ἀποδεῖξτε μετὰ ὅτι ἡ ἐπέκταση $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ δὲν μπορεῖ νὰ συμπίπτει μὲ καμμία ἀπὸ αὐτὲς τὶς ἐπεκτάσεις βαθμοῦ 2, ἄρα....

   Στὴ συνέχεια, ἀποδεῖξτε ὅτι $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\alpha)$, ὅπου $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$, ὡς ἑξῆς (ἂν ἐσεῖς βρεῖτε κάποιον ἄλλο τρόπο, δεκτός):

   Εἶναι $\beta = \alpha - \sqrt{5}$· τὸ β ὅπως παραπάνω. Τὸ ἐλάχιστο πολυώνυμο, ἔστω $f(X)$ τοῦ β πάνω ἀπὸ τὸ $\mathbb{Q}$ τὸ ἔχετε ἤδη ὑπολογίσει. Δεῖξτε γιατὶ ἡ σχέση $f(\alpha - \sqrt{5}) = 0$ συνεπάγεται ὅτι $\sqrt{5} \in \mathbb{Q}(\alpha)$ καί, συνεπῶς, καὶ $\beta \in \mathbb{Q}(\alpha)$. Ἄρα,....

3. Ὑπενθύμιση τοῦ Κινέζικου Θεωρήματος ὑπολοίπων: *Ἔστω ὅτι m, n εἶναι ἀκέραιοι > 1, πρῶτοι μεταξύ τους. Τότε, γιὰ κάθε ζεῦγος ἀκεραίων (a, b), ὑπάρχει $x_{a,b}$ μὲ τὴν ἰδιότητα $x_{a,b} \equiv a \pmod{m}$ καὶ $x_{a,b} \equiv b \pmod{n}$. Ὁ $x_{a,b}$ μὲ αὐτὴ τὴν ἰδιότητα εἶναι μονοσήμαντα ὁρισμένος $\pmod{mn}$.*

   Ὑπενθύμιση ἀπὸ τὸ εἰσαγωγικὸ (προπτυχιακὸ) μάθημα Ἄλγεβρας: Ἔστω

ἀκέραιος $n > 1$ καὶ ὁ δακτύλιος $\mathbb{Z}_n$. Τὰ ἀντιστρέψιμα στοιχεῖα ἤ, διαφορετικά, οἱ μονάδες τοῦ $\mathbb{Z}_n$ (τὸ συνολό τους συμβολίζεται $\mathbb{Z}_n^*$) εἶναι, ἀκριβῶς, οἱ κλάσεις $a \bmod n$, ὅπου a εἶναι πρῶτος πρὸς n. Τὸ σύνολο $\mathbb{Z}_n^*$, ἐφοδιασμένο μὲ τὴν πράξη πολλαπλασιασμοῦ κλάσεων $\bmod n$ εἶναι ὁμάδα τάξεως $\phi(n)$ (συνάρτηση ϕ τοῦ Euler).
(α′) Βάσει τῶν παραπάνω ἀποδεῖξτε ὅτι $\mathbb{Z}_m^* \times \mathbb{Z}_n^* \cong \mathbb{Z}_{mn}^*$.
(β′) Βάσει τοῦ (α′) ἀποδεῖξτε τὴ γενικευμένη πρόταση: Ἂν οἱ > 1 ἀκέραιοι $m_1, \ldots, m_k$ εἶναι ἀνὰ δύο πρῶτοι μεταξύ τους, τότε $\mathbb{Z}_{m_1 \cdots m_k}^* \cong \mathbb{Z}_{m_1}^* \times \cdots \times \mathbb{Z}_{m_k}^*$.
(γ′) Ἔστω ἀκέραιος $n > 1$ καὶ $n = p_1^{r_1} \cdots p_k^{r_k}$ ἡ κανονικὴ ἀνάλυση τοῦ n σὲ πρώτους παράγοντες (δηλαδή, οἱ πρῶτοι εἶναι διαφορετικοὶ μεταξύ τους καὶ ὅλοι οἱ ἐκθέτες εἶναι θετικοί). Ἂν $\zeta_n \in \mathbb{C}$ εἶναι πρωταρχικὴ n-οστὴ ρίζα τῆς μονάδος, ὁπότε $\mathbb{Q}(\zeta_n)$ εἶναι τὸ n-οστὸ κυκλοτομικὸ σῶμα, ἀποδεῖξτε ὅτι $\mathcal{G}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_{p^{r_1}}^* \times \cdots \times \mathbb{Z}_{p^{r_k}}^*$.
(δ′) Βάσει τοῦ (α′) ἀποδεῖξτε ὅτι $\mathcal{G}(\mathbb{Q}(\zeta_{72})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$.
Προσοχή! Στὸ δεξιὸ μέλος ἔχομε *προσθετικὲς* ὁμάδες. Γενικά, ἰσχύει ὁ ἑξῆς συμβολισμός στὴ συνάφεια τῶν ὁμάδων: $\mathbb{Z}_n^*$ εἶναι ἡ *πολλαπλασιαστικὴ* ὁμάδα τῶν κλάσεων $\bmod n$ ἀκεραίων *πρώτων πρὸς n* ἤ, ἀλλοιῶς, ἡ ὁμάδα τῶν μονάδων τοῦ δακτυλίου $(\mathbb{Z}_n, +, \cdot)$. Ἀπὸ τὴν ἄλλη, μὲ τὸ $\mathbb{Z}_n$ ἐννοοῦμε τὴν *προσθετικὴ* ὁμάδα τῶν κλάσεων $\bmod n$ (ὅλων τῶν ἀκεραίων). Θὰ δείξετε ὅτι $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (πολλαπλασιαστικὴ ὁμάδα στ' ἀριστερά, προσθετικὴ στὰ δεξιά) καὶ $\mathbb{Z}_9^* \cong \mathbb{Z}_6$.

4. Ἔστω p πρῶτος καὶ $\zeta \in \mathbb{C}$ πρωταρχικὴ p-ρίζα τῆς μονάδος. Ἀποδεῖξτε ὅτι μία βάση τῆς ἐπέκτασης $\mathbb{Q}(\zeta)/\mathbb{Q}$ εἶναι ἡ $\zeta, \zeta^2, \ldots, \zeta^{p-1}$.