# ΘΕΩΡΙΑ ΣΩΜΑΤΩΝ

Ἐαρινὸ Ἑξάμηνο 2016

Καθηγητὴς Ν. Γ. Τζανάκης

## Ἀσκήσεις τῆς 2ης ἑβδομάδας

*Ὑποδειγματικὴ ἄσκηση.* Ἔστω $M = \mathbb{Q}[v, w]$, ὅπου $v = \sqrt{2}$ καὶ $w = \sqrt[3]{2}$.
(α΄) Ὑπολογῖστε τὸν βαθμὸ τῆς ἐπέκτασης $M/\mathbb{Q}$.
(β΄) Ἀποδεῖξτε ὅτι τὸ $g(X) = X^3 - 2$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ $\mathbb{Q}[v]$ καὶ τὸ $f(X) = X^2 - 2$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ $\mathbb{Q}[w]$.
(γ΄) Ὑπολογῖστε μία βάση τῆς ἐπέκτασης $M/\mathbb{Q}$.

*Λύση.* (α΄) Θεωρῶ τὸ παρακάτω διάγραμμα, ὅπου τὰ $d_1, d_2, 2, 3$ δηλώνουν τοὺς βαθμοὺς τῶν ἀντιστοίχων ἐπεκτάσεων· π.χ. $d_1 = [M : L]$.

$$\begin{tikzcd}
M \arrow[d, dash, "d_1"] \arrow[dr, dash, "d_2"] & \\
L \arrow[dr, dash, "3"] & K \arrow[d, dash, "2"] \\
& \mathbb{Q}
\end{tikzcd}
\qquad K = \mathbb{Q}[v],\ v = \sqrt{2}, \quad L = \mathbb{Q}[w], w = \sqrt[3]{2}$$

Οἱ βαθμοὶ 2 καὶ 3 δικαιολογοῦνται ὡς ἑξῆς: Εἶναι $L = \mathbb{Q}[w]$ καὶ τὸ $w$ εἶναι ρίζα τοῦ $g(X)$, τὸ ὁποῖο εἶναι ἀνάγωγο πάνω ἀπ' τὸ $\mathbb{Q}$, λόγῳ τοῦ *Κριτηρίου Eisenstein* μὲ $p = 2$. Ἄρα, τὸ ἐλάχιστο πολυώνυμο τοῦ $w$ πάνω ἀπ' τὸ $\mathbb{Q}$ εἶναι τὸ $g(X)$. Ἀπὸ τὸ Θεώρημα 1.1.3 ξέρω ὅτι $[L : \mathbb{Q}] = \deg g = 3$. Μὲ ἀνάλογο τρόπο ἀποδεικνύω ὅτι $[K : \mathbb{Q}] = 2$.
Κοιτάζοντας τὸ ἀριστερὸ τμῆμα τοῦ διαγράμματος βλέπω ὅτι, λόγῳ τοῦ Θεωρήματος 1.1.4, εἶναι: $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = d_1 \cdot 3$, ἄρα $[M : \mathbb{Q}]$ εἶναι πολλαπλάσιο τοῦ 3.
Μὲ ἀνάλογο τρόπο, ἀλλὰ κοιτάζοντας τὸ δεξιὸ τμῆμα τοῦ διαγράμματος, συμπεραίνω ὅτι $[M : \mathbb{Q}]$ εἶναι πολλαπλάσιο τοῦ 2. Ἐπειδή $(2, 3) = 1$, ἕπεται ὅτι $[M : \mathbb{Q}]$ εἶναι πολλαπλάσιο τοῦ $2 \cdot 3 = 6$.
Τώρα θὰ δείξω ὅτι $[M : \mathbb{Q}]$ εἶναι ἀκριβῶς 6. Εἶναι $M = \mathbb{Q}[w, v] = (\mathbb{Q}[w])[v] = L[v]$. Ἔστω ὅτι τὸ ἐλάχιστο πολυώνυμο τοῦ $v$ πάνω ἀπὸ τὸ $L$ εἶναι $q(X)$. Τότε (Θεώρημα 1.1.3) $\deg q = [M : L] = d_1$. Τὸ ἀνάγωγο πολυώνυμο $q(X) \in L[X]$ ἔχει κοινὴ ρίζα (τὴ $v$) μὲ τὸ $X^2 - 2 \in L[X]$, ἄρα ἀπὸ τὸ "ἐργαλεῖο" 3 τῆς *ἐργαλειοθήκης*, $q(X) | (X^2 - 2)$, ὁπότε $\deg q \leq 2$, δηλαδή, $d_1 \leq 2$. Ἀλλὰ τότε, $[M : \mathbb{Q}] = d_1 \cdot 3 \leq 6$. Ὅμως δείξαμε παραπάνω ὅτι $[M : \mathbb{Q}]$ εἶναι πολλαπλάσιο τοῦ 6, ἄρα $[M : \mathbb{Q}] = 6$.

(β΄) Τώρα ξέρω ὅτι $[M : \mathbb{Q}] = 6$, ἄρα $6 = [M : \mathbb{Q}] = d_1 \cdot 3$, ὁπότε $d_1 = 2$. Συνεπῶς, $\deg q = 2$, ὅπου, ὑπενθυμίζω, $q(X) \in L[X]$ εἶναι τὸ ἐλάχιστο πολυώνυμο τοῦ $v$ πάνω ἀπ' τὸ $L$. Στὸ (α΄) εἴδαμε ὅτι $q(X) | (X^2 - 2)$. Ἐπειδὴ καὶ τὰ δύο πολυώνυμα εἶναι μονικὰ καὶ τοῦ ἴδιου βαθμοῦ, συμπεραίνω ὅτι εἶναι ἴσα. Ἔτσι $X^2 - 2 = q(X)$, ἄρα τὸ $X^2 - 2$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ $L$.
Μὲ ἀνάλογο τρόπο, ἀποδεικνύω ὅτι $d_2 = 3$, θεωρῶ τὸ ἐλάχιστο πολυώνυμο, ἔστω $r(X) \in K[X]$

τοῦ $w$ πάνω ἀπ' τὸ $K$ καὶ ἀποδεικνύω ὅτι $r(X) = X^3 - 2$, ὁπότε τὸ $X^3 - 2$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ $K$.

(γ′) Ἀφοῦ $L = \mathbb{Q}[w]$ καὶ τὸ ἐλάχιστο πολυώνυμο τοῦ $w$ πάνω ἀπ' τὸ $\mathbb{Q}$ εἶναι $X^3 - 2$, ἕπεται (Θεώρημα 1.1.3) ὅτι $1, w, w^2$ εἶναι βάση τῆς $L/\mathbb{Q}$.
Ἀπὸ τὸ (β′) ξέρω ὅτι τὸ $X^2 - 2$ εἶναι τὸ ἐλάχιστο πολυώνυμο τοῦ $v$ πάνω ἀπ' τὸ $L$, ἄρα τὰ $1, v$ ἀποτελοῦν βάση τῆς $L[v]/L$, δηλαδή τῆς $M/L$.
Τώρα, $1, w, w^2$ εἶναι βάση τῆς $L/\mathbb{Q}$ καὶ $1, v$ εἶναι βάση τῆς $M/L$. Σύμφωνα μὲ τὴν ἀπόδειξη τοῦ Θεωρήματος 1.1.4, ἕπεται ὅτι ὅλα τὰ δυνατὰ γινόμενά τους, δηλαδή, $1, w, w^2, v, vw, vw^2$ ἀποτελοῦν βάση τῆς $M/\mathbb{Q}$.

Ἀσκήσεις γιὰ δική σας ἐξάσκηση.

1. Θεωρῆστε τὰ $f(X) = X^5 + 3X^4 - 30X^3 + 39X^2 - 6X + 141 \in \mathbb{Q}[X]$, $g(X) = X^7 - 13 \in \mathbb{Q}[X]$ καὶ $v, w \in \mathbb{C}$, τέτοια ὥστε $f(v) = 0$ καὶ $g(w) = 0$. Ἔστω $M = \mathbb{Q}[v, w]$.
   (α′) Ἀποδεῖξτε ὅτι $[M : \mathbb{Q}] = 35$ καὶ περιγρᾶψτε μία βάση τῆς ἐπέκτασης $M/\mathbb{Q}$.
   (β′) Ἐξηγῆστε γιατὶ τὸ $f(X)$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ $\mathbb{Q}[w]$ καὶ $g(X)$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ $\mathbb{Q}[v]$.

2. Ἔστω σῶμα $K$, $f(X) \in K[X]$ ἀνάγωγο τετάρτου βαθμοῦ καὶ $L$ ἐπέκταση τοῦ $K$ βαθμοῦ 6. Ἀποδεῖξτε ὅτι τὸ $L$ εἶναι ἀδύνατον νὰ περιέχει ρίζα τοῦ $f(X)$.
   Ὑπόδειξη: Ἔστω $v \in L$ ρίζα τοῦ $f(X)$. Συμπληρῶστε τοὺς βαθμοὺς στὸ διάγραμμα

$$\begin{array}{c} L \\ | \\ K[v] \\ | \\ K \end{array}$$

3. Γιὰ καθέναν ἀπὸ τοὺς παρακάτω ἀριθμοὺς ὑπολογῖστε πολυώνυμο μὲ ρητοὺς συντελεστές, ποὺ νὰ ἔχει ὡς ρίζα τον ἀριθμὸ αὐτό.

$$\sqrt{2} + \sqrt{3}, \qquad \sqrt{3} + \sqrt[3]{2}, \qquad \frac{2\sqrt{3} + 3\sqrt{2}}{\sqrt{3} - \sqrt{2}}.$$