ΘΕΩΡΙΑ ΣΩΜΑΤΩΝ

Σημειώσεις προπτυχιακοῦ μαθήματος [1]

Ν.Γ. Τζανάκης

Τμῆμα Μαθηματικῶν

Πανεπιστήμιο Κρήτης - Ἡράκλειο

[1]Τελευταία ἔκδοση 25-10-2016

Περιεχόμενα

Κεφάλαιο 1

Ἐπεκτάσεις Σωμάτων

1.1 Βασικες Προτασεις

Ἔστω ὅτι τὸ σῶμα K εἶναι ὑπόσωμα τοῦ σώματος L. Λέμε τότε ὅτι τὸ L εἶναι μία ἐπέκταση τοῦ K, τὴν ὁποία συμβολίζομε L/K.

Ὁρισμὸς 1.1.1. *1) Τὸ $v \in L$ λέγεται ἀλγεβρικὸ πάνω ἀπὸ τὸ K, ἂν εἶναι ρίζα ἑνὸς μὴ μηδενικοῦ πολυωνύμου μὲ συντελεστὲς ἀπὸ τὸ K.*
2) Ἡ ἐπέκταση L/K χαρακτηρίζεται ἀλγεβρικὴ ἐπέκταση ἂν κάθε στοιχεῖο της εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K.

Εἶναι προφανὲς ὅτι κάθε στοιχεῖο u τοῦ K εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K, ἀφοῦ εἶναι ρίζα τοῦ $X - u \in K[X]$.

Μία ἰδιαιτέρως σημαντικὴ παρατήρηση εἶναι ὅτι τὸ σῶμα L μπορεῖ νὰ θεωρηθεῖ ὡς K-διανυσματικὸς χῶρος (ἀνεξαρτήτως τοῦ ἂν ἡ ἐπέκταση L/K εἶναι ἢ ὄχι ἀλγεβρική).

Ὁρισμὸς 1.1.2. *Βαθμὸς τῆς ἐπέκτασης L/K εἶναι, ἐξ ὁρισμοῦ, ἡ διάσταση τοῦ K-διανυσματικοῦ χώρου L, ἡ ὁποία καὶ συμβολίζεται $[L : K]$· ἂν εἶναι πεπερασμένος ἀριθμός, ἡ ἐπέκταση χαρακτηρίζεται πεπερασμένη, διαφορετικά, ἄπειρη.*

Παραδείγματα. Γιὰ τὶς ἀνάγκες αὐτῶν τῶν παραδειγμάτων, καὶ μόνο, θεωροῦμε γνωστὰ κάποια βασικὰ πράγματα ἀπὸ τοὺς πραγματικοὺς καὶ τοὺς μιγαδικοὺς ἀριθμούς, ὅπως ἡ ὕπαρξη στὸ $\mathbb{R}$ τετραγωνικῆς ρίζας τοῦ 2 καὶ ἡ ὕπαρξη στὸ $\mathbb{C}$ τῆς n-οστῆς ρίζας τοῦ 2, γιὰ ὁποιονδήποτε φυσικὸ n.

1. Ἔστω $L = \{a + b\sqrt{2} \;:\; a, b \in \mathbb{Q}\}$. Εἶναι φανερὸ ὅτι τὸ L εἶναι κλειστὸ ὡς πρὸς τὴν πρόσθεση, τὴν ἀφαίρεση καὶ τὸν πολλαπλασιασμό. Ὡς πρὸς τὴν ὕπαρξη ἀντιστρόφου, παρατηροῦμε ὅτι ὁ πραγματικός ἀριθμός, ποὺ εἶναι ἀντίστροφος τοῦ $a + b\sqrt{2}$, εἶναι ὁ

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}\,,$$

ποὺ προφανῶς ἀνήκει στὸ L. Ἄρα, τὸ L εἶναι ὑπόσωμα τοῦ $\mathbb{R}$ καὶ $L/\mathbb{Q}$ εἶναι ἐπέκταση σωμάτων, τῆς ὁποίας ὁ βαθμὸς εἶναι 2. Πράγματι, ἀπὸ αὐτὸν τοῦτο τὸν ὁρισμὸ τοῦ L προκύπτει ὅτι τὰ $1, \sqrt{2}$ παράγουν τὸ L πάνω ἀπὸ τὸ $\mathbb{Q}$. Ἀκόμη, τὰ στοιχεῖα αὐτὰ εἶναι $\mathbb{Q}$-γραμμικῶς ἀνεξάρτητα διότι, διαφορετικά, θὰ ὑπῆρχαν $a, b \in \mathbb{Q}$, ὄχι καὶ τὰ δύο μηδέν, τέτοια ὥστε $a + b\sqrt{2} = 0$. Ἀλλὰ αὐτὸ θὰ σήμαινε (λύνοντας ὡς πρὸς $\sqrt{2}$) ὅτι $\sqrt{2} \in \mathbb{Q}$, ἄτοπο, ἀφοῦ εἶναι γνωστὸ ἀπὸ τὰ ἀρχαῖα χρόνια ὅτι ὁ $\sqrt{2}$ δὲν εἶναι ρητὸς ἀριθμός. Συνεπῶς, μία

βάση τῆς ἐπέκτασης $L/\mathbb{Q}$ εἶναι ἡ $\{1, \sqrt{2}\}$, ὁπότε, εἰδικώτερα, $[L:\mathbb{Q}] = 2$.
2. Ἡ ἐπέκταση $\mathbb{C}/\mathbb{R}$ ἔχει βάση τὴν $\{1, i\}$, ὁπότε $[\mathbb{C}:\mathbb{R}] = 2$. Ἡ ἀπόδειξη εἶναι ἀνάλογη μὲ αὐτὴ τοῦ προηγουμένου παραδείγματος.
3. Ἡ μελέτη τῆς ἐπέκτασης $\mathbb{C}/\mathbb{Q}$ εἶναι ἀρκετὰ δυσκολώτερη. Στὴν πραγματικότητα, θὰ δείξομε ὅτι ἡ ἐπέκταση αὐτὴ εἶναι ἄπειρη. Ἀρκεῖ νὰ δείξομε ὅτι, γιὰ ὁσοδήποτε μεγάλο φυσικὸ ἀριθμὸ n, ὑπάρχουν n τὸ πλῆθος μιγαδικοὶ ἀριθμοί, ποὺ εἶναι $\mathbb{Q}$-γραμμικῶς ἀνεξάρτητοι. Πρὸς τοῦτο, θεωροῦμε τὸ πολυώνυμο $f(X) = X^n - 2$ καὶ ἔστω $z \in \mathbb{C}$ μία ρίζα του, π.χ. $z = \sqrt[n]{2}(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n})$. Ἰσχυριζόμαστε ὅτι οἱ μιγαδικοὶ ἀριθμοὶ $1, z, z^2, \ldots, z^{n-1}$ εἶναι $\mathbb{Q}$-γραμμικῶς ἀνεξάρτητοι. Πραγματικά, σὲ ἀντίθετη περίπτωση, θὰ ὑπῆρχαν ρητοὶ $c_0, c_1, \ldots, c_{n-1}$, ὄχι ὅλοι μηδέν, τέτοιοι ὥστε $c_0 + c_1 z + \cdots + c_{n-1}z^{n-1} = 0$, δηλαδή, $g(z) = 0$, ὅπου $g(X) = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1}$. Συνεπῶς, τὰ μὴ μηδενικὰ πολυώνυμα $f(X)$ καὶ $g(X)$ θὰ εἶχαν κοινὴ ρίζα τὴ z, ἄρα ἀπὸ τὸ 2 τῆς πρότασης Α′.4 (παράρτημα Α′), θὰ συμπεραίναμε ὅτι τὰ $f(X)$ καὶ $g(X)$ δὲν εἶναι πρῶτα μεταξύ τους. Ἀλλὰ τὸ $f(X)$ εἶναι ἀνάγωγο, καθὼς φαίνεται ἀμέσως ἀπὸ τὸ κριτήριο τοῦ Eisenstein, συνεπῶς, ἀπὸ τὸ 1 τῆς πρότασης Α′.4 (παράρτημα Α′), θὰ ἔπρεπε νὰ συμπεράνομε ὅτι $f(X)|g(X)$. Αὐτό, ὅμως, εἶναι ἀδύνατο, διότι τὸ μὴ μηδενικὸ πολυώνυμο $g(X)$ ἔχει βαθμὸ μικρότερο ἀπὸ τὸν βαθμὸ τοῦ $f(X)$.

Ἔστω τώρα $v \in L$ καὶ $K[v]$ τὸ σύνολο ὅλων τῶν στοιχείων τῆς μορφῆς $a_0 + a_1 v + \ldots + a_n v^n$ · τὸ n μπορεῖ νὰ εἶναι ὁποιοσδήποτε μὴ ἀρνητικὸς ἀκέραιος καὶ τὰ a_i ἀνήκουν στὸ K. Εἶναι ἁπλούστατο νὰ διαπιστώσει κανεὶς ὅτι τὸ $K[v]$ εἶναι ἀκέραια περιοχή, ὑποδακτύλιος τοῦ σώματος L, ἐν γένει ὅμως, δὲν εἶναι σῶμα. Μὲ $K(v)$ συμβολίζομε τὸ σῶμα πηλίκων τῆς ἀκεραίας περιοχῆς $K[v]$. Τὰ στοιχεῖα δηλαδὴ τοῦ $K(v)$ εἶναι τῆς μορφῆς $(a_0 + a_1 v + \ldots + a_n v^n)/(b_0 + b_1 v + \ldots + b_m v^m)$ μὲ τὰ n καὶ m ὁποιουσδήποτε μὴ ἀρνητικοὺς ἀκεραίους καὶ τὰ στοιχεῖα a_i, b_j ἀπὸ τὸ σῶμα K (ὁ παρονομαστὴς ὑποτίθεται $\neq 0$).

Θεώρημα 1.1.3. *Ἂν τὸ $v \in L$ εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K, τότε ὁ δακτύλιος $K[v]$ εἶναι σῶμα (ὑπόσωμα τοῦ L)· εἰδικώτερα, $K[v] = K(v)$ [1]. Στὴν περίπτωση αὐτή, ὑπάρχει ἕνα μοναδικὸ ἀνάγωγο, μονικὸ πολυώνυμο $q(X) \in K[X]$, τέτοιο ὥστε $q(v) = 0$. Τὸ $K[v]$ εἶναι πεπερασμένη ἐπέκταση τοῦ K, βαθμοῦ $n = \deg q$ καὶ τὰ στοιχεῖα $1, v, \ldots, v^{n-1}$ παράγουν τὸν K-διανυσματικὸ χῶρο $K[v]$.*

Ἀπόδειξη. Γιὰ νὰ δείξομε ὅτι τὸ $K[v]$ εἶναι ὑπόσωμα τοῦ L, ἀρκεῖ νὰ δείξομε ὅτι κάθε μὴ μηδενικὸ στοιχεῖο του ἔχει ἀντίστροφο. Κάθε τέτοιο στοιχεῖο εἶναι τῆς μορφῆς $g(v)(\neq 0)$ γιὰ κάποιο μὴ μηδενικὸ πολυώνυμο $g(X) \in K[X]$. Ἀφοῦ τὸ v ἔχει ὑποτεθεῖ ἀλγεβρικὸ πάνω ἀπὸ τὸ K, ὑπάρχει μὴ μηδενικὸ $f(X) \in K[X]$, τέτοιο ὥστε $f(v) = 0$. Ἀναλύοντας τὸ f σὲ γινόμενο ἀναγώγων πολυωνύμων τοῦ $K[X]$ βλέπομε ὅτι ἕνας τοὐλάχιστον ἐξ αὐτῶν, ἂς τὸν ποῦμε $q(X)$, ἔχει ρίζα του τὸ v. Ἐπειδὴ μποροῦμε νὰ διαιρέσομε τὸ $q(X)$ μὲ τὸν συντελεστὴ τοῦ μεγιστοβαθμίου ὅρου του, ἂν αὐτὸς δὲν εἶναι 1, ἕπεται ὅτι τὸ $q(X)$ μπορεῖ νὰ ὑποτεθεῖ καὶ μονικό. Τώρα θὰ κάνομε χρήση τῆς πρότασης Α′.4 (παράρτημα Α′). Ἰσχυριζόμαστε ὅτι τὰ πολυώνυμα g καὶ q εἶναι πρῶτα μεταξύ τους. Πράγματι, σὲ ἀντίθετη περίπτωση, ἐπειδὴ τὸ q εἶναι ἀνάγωγο πολυώνυμο, θὰ ἔπρεπε νὰ διαιρεῖ τὸ g· ἀλλὰ τότε $g(v) = 0$ (ἀφοῦ καὶ $q(v) = 0$) καὶ ἀντιφάσκομε μὲ τὴν ὑπόθεσή μας γιὰ τὸ $g(v)$. Ἀφοῦ λοιπὸν τὰ g καὶ q εἶναι πρῶτα μεταξύ τους, ὑπάρχουν πολυώνυμα h καὶ r στὸ $K[X]$, τέτοια ὥστε $q(X)r(X) + g(X)h(X) = 1$. Ἡ ἀντικατάσταση $X \leftarrow v$ δίνει τώρα $g(v)h(v) = 1$, ποὺ σημαίνει ὅτι τὸ στοιχεῖο $h(v) \in K[v]$ εἶναι τὸ ἀντίστροφο τοῦ $g(v)$.

[1] Ἔτσι, στὸ ἑξῆς, ὅταν π.χ. τὸ v εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K, θὰ μποροῦμε νὰ χρησιμοποιοῦμε ἀδιακρίτως τὸ συμβολισμὸ $K[v]$ εἴτε $K(v)$.

Τώρα θὰ ἀποδείξομε ὅτι, ἐκτὸς ἀπὸ τὸ q, δὲν ὑπάρχει ἄλλο ἀνάγωγο, μονικὸ πολυώνυμο q_1, ποὺ νὰ ἔχει ρίζα τὸ v. Γιατί, σὲ τέτοια περίπτωση, ἀποκλείεται νὰ εἶναι τὰ q, q_1 πρῶτα μεταξὺ τους: ἂν ἦταν, θὰ εἴχαμε μία σχέση τῆς μορφῆς $q(X)r(X) + q_1(X)r_1(X) = 1$ καὶ ἡ ἀντικατάσταση $v \leftarrow X$ θὰ μᾶς ὁδηγοῦσε στὴν ἀδύνατη σχέση $0 + 0 = 1$. Ἔτσι, ἀφοῦ τὸ q εἶναι ἀνάγωγο καὶ ὄχι πρῶτο πρὸς τὸ q_1, πρέπει $q|q_1$. Ἐντελῶς συμμετρικὰ ὅμως, ἀφοῦ καὶ τὸ q_1 εἶναι ἀνάγωγο, $q_1|q$. Ἔτσι, τὰ q, q_1, εἶναι μονικὰ καὶ ἀλληλοδιαιροῦνται, ἄρα ταυτίζονται.

Ἔστω τώρα $q(X) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + X^n$. Μένει νὰ δείξομε ὅτι τὰ $1, v, \ldots, v^{n-1}$ ἀποτελοῦν βάση τοῦ K-διανυσματικοῦ χώρου $K[v]$. Τὰ n αὐτὰ στοιχεῖα εἶναι K-γραμμικῶς ἀνεξάρτητα· διαφορετικά, θὰ εἴχαμε μία σχέση τῆς μορφῆς $b_0 + b_1v + \ldots + b_{n-1}v^{n-1}$ γιὰ κάποια στοιχεῖα $b_0, b_1, \ldots, b_{n-1}$, ποὺ δὲν εἶναι ὅλα μηδέν, δηλαδή, θὰ ὑπῆρχε πολυώνυμο $h(X)$ βαθμοῦ $\leq n-1$ καὶ τὸ v θὰ ἦταν ρίζα τοῦ h. Τὰ q καὶ h δὲν θὰ ἦταν τότε πρῶτα μεταξὺ τους (αὐτὸ προκύπτει ἀκριβῶς ὅπως καὶ παραπάνω μὲ τὰ q καὶ q_1), ἄρα τὸ q θὰ διαιροῦσε τὸ h, ἄτοπο, ἀφοῦ $\deg h < \deg q$. Τέλος, τὰ $1, v, \ldots, v^{n-1}$ παράγουν τὸ $K[v]$. Ἀρκεῖ νὰ δείξομε ὅτι κάθε v^m, $m \geq n$ εἶναι K-γραμμικὸς συνδυασμὸς τῶν $1, v, \ldots, v^{n-1}$: Γιὰ $m = n$ αὐτὸ ἰσχύει, ἀφοῦ ἀπὸ τὴ σχέση $q(v) = 0$ ἕπεται ὅτι $v^n = -a_0 - a_1v - \ldots - a_{n-1}v^{n-1}$ $(*)$. Ἐπαγωγικὰ τώρα, ἂν $v^r = b_0 + b_1v + \ldots + b_{n-1}v^{n-1}$, μὲ τὰ $b_i \in K$, τότε $v^{r+1} = b_0v + b_1v^2 + \ldots + b_{n-2}v^{n-1} + b_{n-1}v^n$ καὶ ἀντικαθιστώντας τὸ v^n ἀπὸ τὴν $(*)$ ἐκφράζομε τὸ v^{r+1} μόνο συναρτήσει τῶν $1, v, \ldots, v^{n-1}$. □

Τὸ $q(X) \in K[X]$, ποὺ περιγράφεται στὴν ἐκφώνηση τοῦ Θεωρήματος 1.1.3, λέγεται *ἐλάχιστο πολυώνυμο* τοῦ v πάνω ἀπὸ τὸ K.

Ἔστω τώρα ὅτι $v_1, \ldots, v_r \in L$. Μὲ $K[v_1, \ldots, v_r]$ συμβολίζομε τὸ ὑποσύνολο τοῦ L, ποὺ ἀποτελεῖται ἀπὸ ὅλα τὰ πεπερασμένα ἀθροίσματα στοιχείων τοῦ L τῆς μορφῆς $av_1^{n_1} \cdots v_r^{n_r}$ ὅπου $a \in K$ καὶ $n_i \geq 0$ γιὰ κάθε $i = 1, \ldots, r$. Τὸ $K[v_1, \ldots, v_r]$ εἶναι, προφανῶς, δακτύλιος (ἀντιμεταθετικός).

Θεώρημα 1.1.4. *Ἔστω ὅτι L/K καὶ M/L εἶναι πεπερασμένες ἐπεκτάσεις. Τότε καὶ ἡ M/K εἶναι πεπερασμένη ἐπέκταση καί, μάλιστα $[M : K] = [M : L] \cdot [L : K]$.*

Ἀπόδειξη. Ἔστω $[L : K] = l$, $[M : L] = m$, $u_1, \ldots, u_l$ μία K-βάση τοῦ L καὶ $v_1, \ldots, v_m$ μία L-βάση τοῦ M. Ἀρκεῖ νὰ δείξομε ὅτι τὰ u_iv_j, $1 \leq i \leq l$, $1 \leq j \leq m$ εἶναι μία K-βάση τοῦ M. Πρῶτα δείχνομε ὅτι τὰ στοιχεῖα αὐτὰ παράγουν τὸ M πάνω ἀπὸ τὸ K. Ἔστω $v \in M$, ὁπότε

$$v = \sum_{i=1}^{m} a_iv_i\,, \qquad \text{γιὰ κάποια} \quad a_i \in L\,.$$

Ἀλλὰ γιὰ κάθε $i = 1, \ldots, m$,

$$a_i = \sum_{j=1}^{l} b_{ij}u_j\,, \qquad \text{γιὰ κάποια} \quad b_{ij} \in K\,.$$

Ἀντικαθιστώντας τὰ a_i ἀπὸ τὴν τελευταία σχέση στὴν προηγούμενη βλέπομε ὅτι τὸ v εἶναι K-γραμμικὸς συνδυασμὸς τῶν v_iu_j. Ὅσον ἀφορᾶ στὴν K-ἀνεξαρτησία αὐτῶν τῶν στοιχείων, ἄς θεωρήσομε τὴ σχέση

$$\sum_{1\leq i\leq l\,,\,1\leq j\leq m} b_{ij}u_iv_j = 0\,, \qquad \text{γιὰ κάποια} \quad b_{ij} \in K\,.$$

Αὐτὴ γράφεται

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{l} b_{ij}u_i\right)v_j = 0\,.$$

Λόγῳ τῆς L-γραμμικῆς ἀνεξαρτησίας τῶν v_j, πρέπει κάθε ἐσωτερικὸ ἄθροισμα στὴν τελευταία σχέση νὰ εἶναι μηδέν: Δηλαδή, γιὰ κάθε $j = 1, \dots, m$,
$b_{1j}u_1 + \ldots + b_{lj}u_l = 0$, καὶ ἀπὸ τὴν K-ἀνεξαρτησία τῶν u_i, ἕπεται τώρα ὅτι ὅλα τὰ b_{ij} εἶναι μηδέν. □

Θεώρημα 1.1.5. *Ἂν $v_1, \dots, v_r \in L$, τὸ v_1 εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K καὶ γιὰ κάθε $i = 2, \dots, r$ τὸ v_i εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ $K[v_1, \dots, v_{i-1}]$* [2] *(εἰδικώτερα, ἂν ὅλα τὰ v_i εἶναι ἀλγεβρικὰ πάνω ἀπὸ τὸ K), ὁ δακτύλιος $K[v_1, \dots, v_r]$ εἶναι ὑπόσωμα τοῦ L, πεπερασμένη ἐπέκταση τοῦ K.*

Ἀπόδειξη. Σύμφωνα μὲ τὸ Θεώρημα 1.1.3, ἡ $K[v_1]/K$ εἶναι πεπερασμένη ἐπέκταση. Εὔκολα διαπιστώνεται ὅτι $K[v_1, v_2] = (K[v_1])[v_2]$ καὶ ἐπειδή, ἐξ ὑποθέσεως, τὸ v_2 εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ $K[v_1]$, τὸ Θεώρημα 1.1.3 συνεπάγεται ὅτι ἡ ἐπέκταση $K[v_1, v_2]$ εἶναι, ἐπίσης, σῶμα καί, μάλιστα, πεπερασμένη ἐπέκταση τοῦ $K[v_1]$. Τώρα, ἔχομε τὶς διαδοχικὲς πεπερασμένες ἐπεκτάσεις $K[v_1]/K$ καὶ $K[v_1, v_2]/K[v_1]$, ἄρα, ἀπὸ τὸ Θεώρημα 1.1.4 συμπεραίνομε ὅτι ἡ ἐπέκταση $K[v_1, v_2]/K$ εἶναι πεπερασμένη. Στὴ συνέχεια προχωροῦμε ἐντελῶς ἀνάλογα, βασιζόμενοι στὸ ὅτι $K[v_1, v_2, v_3] = (K[v_1, v_2])[v_3]$ καὶ στὴν ὑπόθεση ὅτι τὸ v_3 εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ $K[v_1, v_2]$, κ.ὅ.κ. μέχρις ὅτου καταλήξομε στὸ ὅτι ἡ $K[v_1, \dots, v_r]/K$ εἶναι ἀλγεβρικὴ ἐπέκταση. □

Θεώρημα 1.1.6. *Κάθε πεπερασμένη ἐπέκταση τοῦ K εἶναι ἀλγεβρικὴ ἐπέκταση τοῦ K.*

Ἀπόδειξη. Ἔστω L/K πεπερασμένη ἐπέκταση καὶ $v \in L$. Ἐπειδὴ εἶναι ἀδύνατον νὰ ὑπάρχουν ἄπειρα στοιχεῖα τοῦ L γραμμικῶς ἀνεξάρτητα πάνω ἀπὸ τὸ K, ἕπεται ὅτι ὑπάρχει ἀκέραιος $n \geq 1$, τέτοιος ὥστε τὰ $1, v, \dots, v^n$ νὰ εἶναι K-γραμμικῶς ἐξηρτημένα. Αὐτὸ σημαίνει ὅτι ὑπάρχουν $a_0, \dots, a_n \in K$, ὄχι ὅλα μηδέν, τέτοια ὥστε $a_0 + a_1v + \ldots + a_nv^n = 0$, δηλαδὴ τὸ v εἶναι ρίζα ἑνὸς μὴ μηδενικοῦ πολυωνύμου μὲ συντελεστὲς ἀπὸ τὸ K· ἄρα τὸ τυχὸν $v \in L$ εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K. □

Θεώρημα 1.1.7. *Ἂν τὸ K εἶναι ὑπόσωμα τοῦ σώματος L, τότε τὸ ὑποσύνολο A τοῦ L, τὸ ἀποτελούμενο ἀπὸ τὰ στοιχεῖα τοῦ L, τὰ ὁποῖα εἶναι ἀλγεβρικὰ πάνω ἀπὸ τὸ K, εἶναι ὑπόσωμα τοῦ L (προφανῶς, $K \subseteq A$).*

Ἀπόδειξη. Ἀρκεῖ νὰ δειχθεῖ ὅτι, ἂν $x, y \in A$ τότε $x - y, xy \in A$, καθὼς καὶ $x^{-1} \in A$ γιὰ $x \neq 0$. Ἀπὸ τὸ Θεώρημα 1.1.5 ἔχομε ὅτι τὸ $K[x, y]$ εἶναι σῶμα, πεπερασμένη ἐπέκταση τοῦ K, ἄρα καὶ ἀλγεβρικὴ ἐπέκταση τοῦ K, λόγῳ τοῦ Θεωρήματος 1.1.6. Συνεπῶς, κάθε στοιχεῖο τοῦ $K[x, y]$ εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K. Ἀλλὰ ἀφοῦ τὸ $K[x, y]$ εἶναι σῶμα, τὰ $x - y, xy, x^{-1}$ ἀνήκουν σὲ αὐτό, ἄρα εἶναι ἀλγεβρικὰ πάνω ἀπὸ τὸ K, δηλαδὴ ἀνήκουν στὸ A. □

Ἂν θεωρήσομε ὡς L τὸ $\mathbb{C}$ καὶ ὡς K τὸ $\mathbb{Q}$, τότε τὸ σύνολο A τοῦ θεωρήματος 1.1.7 συμβολίζομε μὲ $\mathbf{A}$ καὶ τὸ ὀνομάζομε *σῶμα τῶν ἀλγεβρικῶν ἀριθμῶν*. Δηλαδή:

> Ἕνας μιγαδικὸς ἀριθμὸς χαρακτηρίζεται *ἀλγεβρικὸς* ἂν εἶναι ρίζα ἑνὸς μὴ μηδενικοῦ πολυωνύμου μὲ ρητοὺς συντελεστές· στὴν ἀντίθετη περίπτωση χαρακτηρίζεται *ὑπερβατικός*.

[2] Πρόκειται περὶ σώματος, ὅπως θὰ φανεῖ στὴν ἀπόδειξη.

Ὁ ἁπλούστερος τρόπος γιὰ νὰ ἀποδείξομε ὅτι τὸ σύνολο τῶν ὑπερβατικῶν ἀριθμῶν εἶναι μὴ κενὸ εἶναι συνολοθεωρητικὸς καὶ ἔμμεσος καὶ ὀφείλεται στὸν Cantor: Δείχνει κανεὶς πρῶτα ὅτι τὸ $\mathbb{R}$ εἶναι μὴ ἀριθμήσιμο σύνολο καὶ μετὰ ὅτι τὸ σύνολο $\mathbf{A}$ εἶναι ἀριθμήσιμο, ὁπότε προκύπτει ὅτι τὸ $\mathbb{R}-\mathbf{A}$, δηλαδὴ τὸ σύνολο τῶν πραγματικῶν ὑπερβατικῶν ἀριθμῶν, εἶναι μὴ κενό. Τὸ μειονέκτημα αὐτῆς τῆς μεθόδου εἶναι ὅτι δὲν μᾶς παρέχει τρόπο κατασκευῆς ἔστω καὶ ἑνὸς ὑπερβατικοῦ ἀριθμοῦ. Ἦταν ὁ Liouville, ὁ ὁποῖος, γιὰ πρώτη φορά, στὰ 1844, ἔδωσε παράδειγμα ὑπερβατικοῦ ἀριθμοῦ. Συγκεκριμένα, ἀπέδειξε ὅτι ὁ ἀριθμὸς $\xi = \sum_{n=1}^{\infty} 10^{-n!}$ εἶναι ὑπερβατικός. Στὰ 1873, ὁ Hermitte ἀπέδειξε τὴν ὑπερβατικότητα τοῦ e, ἐνῶ ἡ ὑπερβατικότητα τοῦ π ἀποδείχθηκε ἀπὸ τὸν Lindemann στὰ 1882.

Ἀσκήσεις

1. Νὰ βρεθοῦν βάσεις καὶ οἱ βαθμοὶ τῶν ἑξῆς ἐπεκτάσεων:

$$\mathbb{C}/\mathbb{Q},\ \ \mathbb{R}(\sqrt{5})/\mathbb{R},\ \ \mathbb{Q}(\sqrt{(3]2)})/\mathbb{Q},\ \ \mathbb{Q}(\sqrt{5},\ \sqrt{7})/\mathbb{Q},\ \ \mathbb{Q}(\sqrt[7]{3})/\mathbb{Q}\ .$$

2. Ἂν $[L : K] = 1$, τότε $L = K$.

3. Ἂν $[L : K]$ εἶναι πρῶτος, τότε δὲν ὑπάρχει *γνήσια* ἐπέκταση τοῦ K, ἡ ὁποία νὰ περιέχεται *γνησίως* στὸ L.

4. Ἂν ἡ L/K εἶναι πεπερασμένη ἐπέκταση καὶ ἔχομε τὶς διαδοχικὲς ἐπεκτάσεις

$$L/K_r/K_{r-1}/\ldots/K_1/K,$$

τότε

$$[L : K] = [L : K_r][K_r : K_{r-1}]\ldots[K_2 : K_1][K_1 : K]\ .$$

5. Δεῖξτε ὅτι ἡ ἐπέκταση L/K εἶναι πεπερασμένη ἂν καὶ μόνο ἂν ὑπάρχει ἕνας φυσικὸς ἀριθμὸς r καὶ $a_1, \ldots, a_r \in L$, ἀλγεβρικὰ πάνω ἀπὸ τὸ K, ἔτσι ὥστε $L = K(a_1, \ldots, a_r)$.

6. Ἂν $\mathbf{A}$ εἶναι τὸ σῶμα τῶν ἀλγεβρικῶν ἀριθμῶν, δεῖξτε ὅτι ἡ ἐπέκταση $\mathbf{A}/\mathbb{Q}$ δὲν εἶναι πεπερασμένη.
Ὑπόδειξη. Χρησιμοποιῆστε τὸ κριτήριο Eisenstein προκειμένου νὰ ἀποδείξετε ὅτι ὑπάρχουν ἀνάγωγα πολυώνυμα πάνω ἀπὸ τὸ $\mathbb{Q}$ ὁσοδήποτε μεγάλου βαθμοῦ.

7. Ἔστω A τὸ σῶμα τῶν μιγαδικῶν ἀλγεβρικῶν ἀριθμῶν (μιγαδικοὶ ἀριθμοί, ἀλγεβρικοὶ πάνω ἀπὸ τὸ $\mathbb{Q}$). Θεωρώντας γνωστὸ ὅτι κάθε μιγαδικὸ πολυώνυμο ἔχει μιγαδικὴ ρίζα, ἀποδεῖξτε ὅτι κάθε πολυώνυμο μὲ συντελεστὲς ἀπὸ τὸ $\mathbf{A}$ ἔχει ρίζα στὸ $\mathbf{A}$. Ὡς συνέπεια αὐτοῦ δεῖξτε ὅτι δὲν ὑπάρχει γνήσια ἀλγεβρικὴ ἐπέκταση τοῦ $\mathbf{A}$.

8. Δεῖξτε ὅτι $\mathbb{Q}(\sqrt{3},\ \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

9. Βρεῖτε μία βάση καὶ τὸ βαθμὸ τῆς ἐπέκτασης $\mathbb{Q}\left(\sqrt{1+\sqrt{3}}\right)/\mathbb{Q}$.

10. Ἂν ὁ βαθμὸς $[L : K]$ εἶναι πρῶτος, τότε ὑπάρχει $u \in L$, τέτοιο ὥστε $L = K(u)$ (εἶναι, δηλαδή, ἡ ἐπέκταση L/K *ἁπλῆ*).

1.2 Κατασκευές με κανόνα και διαβήτη

Ἔστω S_0 ἕνα σύνολο σημείων τοῦ $\mathbb{R}^2$ (ἐπίπεδο). Λέμε ὅτι ἕνα σημεῖο τοῦ ἐπιπέδου εἶναι *ἄμεσα κατασκευάσιμο* (μὲ κανόνα καὶ διαβήτη) ἀπὸ τὸ S_0 ἂν εἶναι σημεῖο τομῆς δύο εὐθειῶν, ἢ μιᾶς εὐθείας καὶ ἑνὸς κύκλου, ἢ δύο κύκλων, ποὺ προκύπτουν ὡς ἑξῆς: Ἡ μὲν εὐθεία διέρχεται ἀπὸ δύο σημεῖα τοῦ S_0, ὁ δὲ κύκλος ἔχει ὡς κέντρο του ἕνα σημεῖο τοῦ S_0 καὶ ἡ ἀκτίνα του ἰσοῦται μὲ τὴν ἀπόσταση δύο σημείων τοῦ S_0. Λέμε ὅτι ἕνα σημεῖο τοῦ ἐπιπέδου *κατασκευάζεται* (μὲ κανόνα καὶ διαβήτη) ἀπὸ τὸ S_0 ἂν ὑπάρχει πεπερασμένο πλῆθος σημείων $s_1, s_2, \ldots, s_n$, ἔτσι ὥστε (1) τὸ s_1 νὰ εἶναι ἄμεσα κατασκευάσιμο ἀπὸ τὸ S_0, (2) γιὰ κάθε $i = 2, \ldots, n$, τὸ s_i νὰ εἶναι ἄμεσα κατασκευάσιμο ἀπὸ τὸ $S_0 \cup \{s_1, \ldots, s_{i-1}\}$ καὶ (3) $s_n = s$.

Συμβολίζομε τώρα μὲ K_0 τὸ ὑπόσωμα τοῦ $\mathbb{R}$ ποὺ παράγεται ἀπὸ τὶς συντεταγμένες ὅλων τῶν σημείων τοῦ S_0. Εἶναι δηλαδὴ τὸ K_0 τὸ ἐλάχιστο ὑπόσωμα τοῦ $\mathbb{R}$ ποὺ περιέχει τὶς συντεταγμένες ὅλων τῶν σημείων τοῦ S_0.

Θεώρημα 1.2.1. *Ἂν οἱ συντεταγμένες ὅλων τῶν σημείων ἑνὸς συνόλου $S \subset \mathbb{R}^2$ περιέχονται σὲ ἕνα ὑπόσωμα K τοῦ $\mathbb{R}$ καὶ τὸ σημεῖο $s = (x, y)$ εἶναι ἄμεσα κατασκευάσιμο ἀπὸ τὸ S, τότε τὰ x, y εἶναι ἀλγεβρικὰ πάνω ἀπὸ τὸ K καὶ ἡ ἐπέκταση $K(x, y)/K$ εἶναι βαθμοῦ 1, 2 ἢ 4.* [3]

Ἀπόδειξη. Ἂς θεωρήσομε τὴ 'δυσκολότερη' περίπτωση ποὺ τὸ s εἶναι τομὴ δύο κύκλων. Ἂν $(x_1, y_1), (x_2, y_2)$ εἶναι τὰ κέντρα τους, τότε ἡ ὑπόθεση γιὰ τὸ s μᾶς λέει ὅτι $x_1, y_1, x_2, y_2 \in K$. Ἐπίσης, ἂν r_1, r_2 εἶναι οἱ ἀκτίνες τῶν κύκλων, ἕπεται, πάλι ἀπὸ τὴν ὑπόθεση γιὰ τὸ s, ὅτι κάθε $r_n, (n = 1, 2)$ ἰσοῦται μὲ τὴν ἀπόσταση δύο σημείων $(a_n, b_n), (c_n, d_n)$, ὅπου $a_n, b_n, c_n, d_n \in K$· ἄρα $r_n^2 = (a_n - c_n)^2 + (b_n - d_n)^2$. Οἱ συντεταγμένες (x, y) τοῦ s ἐπαληθεύουν τὶς σχέσεις

$$(x - x_1)^2 + (y - y_1)^2 = r_1^2 \ , \ (x - x_2)^2 + (y - y_2)^2 = r_2^2$$

ἤ, ἰσοδύναμα,

$$\begin{aligned} (x - x_1)^2 + (y - y_1)^2 &= r_1^2 \\ 2(x_2 - x_1)x + 2(y_2 - y_1)y + x_1^2 - x_2^2 + y_1^2 - y_2^2 &= r_1^2 - r_2^2 \ . \end{aligned}$$

Ἐδῶ ἔχομε ἕνα σύστημα δευτέρου βαθμοῦ, ὡς πρὸς τοὺς ἀγνώστους x, y μὲ συντελεστὲς ἀπὸ τὸ K. Ἀπαλείφοντας π.χ. τὸ x μεταξὺ τῶν δύο ἐξισώσεων, βρίσκομε μία ἐξίσωση ὡς πρὸς y δευτέρου βαθμοῦ, τὸ πολύ, μὲ συντελεστὲς ἀπὸ τὸ K. Συνεπῶς, τὸ y εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K καὶ μάλιστα, $[K(y) : K] = 1$ ἢ 2. Ὁμοίως, $[K(x) : K] =1$ ἢ 2· ὁπότε (Θεώρημα 1.1.5) ἡ ἐπέκταση $K(x, y)/K$ εἶναι πεπερασμένη καὶ (βλ. Θεώρημα 1.1.4)

$$[K(x, y) : K] = [K(x, y) : K(y)] \cdot [K(y) : K] \ .$$

Ἀλλὰ ἀφοῦ τὸ x εἶναι ρίζα ἑνὸς δευτεροβαθμίου, τὸ πολύ, πολυωνύμου μὲ συντελεστὲς ἀπὸ τὸ K, τὸ ὁποῖο, βέβαια, μποροῦμε νὰ τὸ δοῦμε καὶ ὡς πολυώνυμο μὲ συντελεστὲς ἀπὸ τὸ $K(y)$, ἕπεται ὅτι ὁ βαθμὸς $[K(x, y) : K(y)]$ εἶναι 1 ἢ 2. Ἔτσι, ἡ παραπάνω σχέση συνεπάγεται ὅτι $[K(x, y) : K] =1, 2$ ἢ 4. □

Ἔστω τώρα ὅτι τὸ s εἶναι κατασκευάσιμο ἀπὸ τὸ σύνολο S_0 καὶ τὰ σημεῖα $s_1, s_2, \ldots, s_n = s$ μᾶς ὁδηγοῦν ἀπὸ τὸ S_0 στὴν κατασκευὴ τοῦ s. Θέτομε $s_i = (a_i, b_i)$ καὶ ἔστω K_0

[3] Μὲ τὶς ἴδιες ὑποθέσεις μπορεῖ νὰ ἀποδειχθεῖ, ἀκριβέστερα, ὅτι ἡ ἐπέκταση εἶναι βαθμοῦ 1 ἢ 2, ἀλλὰ αὐτὸ δὲν μᾶς εἶναι ἀπαραίτητο.

τὸ ὑπόσωμα τοῦ $\mathbb{R}$, ποὺ ὁρίσαμε στὴν ἀρχή. Ἔχομε τότε τὶς ἑξῆς διαδοχικὲς ἐπεκτάσεις: K_1/K_0, ὅπου $K_1 = K_0(a_1, b_1)$, K_2/K_1, ὅπου $K_2 = K_1(a_2, b_2)$, κ.λ.π. K_n/K_{n-1}, ὅπου $K_n = K_{n-1}(a_n, b_n)$. Ἀπὸ τὴν ἄσκηση 4 καὶ τὸ Θεώρημα 1.2.1,

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \dots [K_2 : K_1][K_1 : K_0] = \text{δύναμη τοῦ } 2\,.$$

Ἀποδείξαμε δηλαδὴ τὸ ἑξῆς

Θεώρημα 1.2.2. *Ἂν τὸ σημεῖο s κατασκευάζεται ἀπὸ τὸ σύνολο σημείων S_0 καὶ K_0 εἶναι τὸ ἐλάχιστο σῶμα ποὺ περιέχει τὶς συντεταγμένες ὅλων τῶν σημείων τοῦ S_0, τότε ὑπάρχει πεπερασμένη ἐπέκταση τοῦ K_0, ποὺ περιέχει τὶς συντεταγμένες τοῦ s καὶ εἶναι βαθμοῦ ἴσου μὲ δύναμη τοῦ 2.*

Τώρα ἔχομε ὅλα τὰ ἀπαραίτητα ἐφόδια γιὰ ν' ἀποδείξομε ὅτι εἶναι ἀδύνατον νὰ δοθεῖ λύση μὲ κανόνα καὶ διαβήτη στὰ τρία περίφημα γεωμετρικὰ προβλήματα τῆς ἀρχαιότητας: *Διπλασιασμὸς τοῦ κύβου, τριχοτόμηση γωνίας, τετραγωνισμὸς τοῦ κύκλου.*

Θεώρημα 1.2.3. *Ὁ διπλασιασμὸς τοῦ κύβου μὲ κανόνα καὶ διαβήτη εἶναι ἀδύνατος.*

Ἀπόδειξη. Ἂς ὑποθέσομε ὅτι μᾶς δίνεται ὁ μοναδιαῖος κῦβος. Γιὰ νὰ πετύχομε τὸ διπλασιασμό του, πρέπει νὰ κατασκευάσομε ἕνα εὐθύγραμμο τμῆμα (τὴν ἀκμὴ τοῦ νέου κύβου) μὲ μῆκος $\sqrt[3]{2}$. Ἐδῶ, τὸ μόνο μας δεδομένο εἶναι τὸ μοναδιαῖο μῆκος (ἡ ἀκμὴ τοῦ ἀρχικοῦ κύβου). Ἄρα, $S_0 = \{(0,0),(1,0)\}$, ὁπότε $K_0 = \mathbb{Q}$. Πρέπει νὰ κατασκευάσομε μὲ κανόνα καὶ διαβήτη τὸ σημεῖο $s = (x, 0)$, ὅπου $x = \sqrt[3]{2}$. Ἂν αὐτὸ γινόταν, θὰ ὑπῆρχε πεπερασμένη ἐπέκταση K τοῦ $\mathbb{Q}$ μὲ $x \in K$ καὶ $[K : \mathbb{Q}] =$ δύναμη τοῦ 2 (Θεώρημα 1.2.2). Ἐπειδὴ τὸ x εἶναι ρίζα τοῦ ἀναγώγου πολυωνύμου $X^3 - 2 \in \mathbb{Q}[X]$, εἶναι $[\mathbb{Q}(x) : \mathbb{Q}] = 3$. Λόγῳ τῶν διαδοχικῶν ἐπεκτάσεων $K/\mathbb{Q}(x)/\mathbb{Q}$ καὶ τοῦ Θεωρήματος 1.1.4, θὰ ἔπρεπε,

$$\text{δύναμη τοῦ } 2 \; = [K : \mathbb{Q}] = [K : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}] = \; \text{πολλαπλάσιο τοῦ } 3\,,$$

ἄτοπο. □

Θεώρημα 1.2.4. *Ἡ γωνία $\pi/3$ δὲν εἶναι δυνατὸν νὰ τριχοτομηθεῖ μὲ κανόνα καὶ διαβήτη. Συνεπῶς, δὲν ὑπάρχει γενικὴ γεωμετρικὴ μέθοδος τριχοτομήσεως γωνιῶν μὲ τὴ χρήση κανόνα καὶ διαβήτη.*

Ἀπόδειξη. Ἔχομε στὴ διάθεσή μας τὸ μοναδιαῖο τριγωνομετρικὸ κύκλο, ὁπότε, μία γωνία εἶναι κατασκευάσιμη ἄν, καὶ μόνο ἄν, τὸ συνημίτονο τῆς γωνίας (θεωρούμενο ὡς εὐθύγραμμο τμῆμα στὸν ἄξονα τῶν συνημιτόνων) εἶναι κατασκευάσιμο. Ἐδῶ, $S_0 = \{(0,0),(1,0)\}, K_0 = \mathbb{Q}$ καὶ ζητοῦμε νὰ κατασκευάσομε τὸ σημεῖο $s = (x, 0), x = \cos\frac{\pi}{9}$. Ἂν αὐτὸ ἦταν δυνατόν, θὰ ὑπῆρχε ἐπέκταση $K/\mathbb{Q}$ μὲ $x \in K$ καὶ $[K : \mathbb{Q}] =$ δύναμη τοῦ 2 (Θεώρημα 1.2.2). Ὅμως, λόγῳ τῆς σχέσεως

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

ἔχομε, γιὰ $\theta = \pi/9$,

$$\frac{1}{2} = 4x^3 - 3x \;\text{ ἢ }\; 8x^3 - 6x - 1 = 0\,.$$

Τὸ x εἶναι, λοιπόν, ρίζα ἑνὸς κυβικοῦ ἀναγώγου (ὅπως διαπιστώνεται εὔκολα) πολυωνύμου τοῦ $\mathbb{Q}[X]$. Ἄρα, $[\mathbb{Q}(x) : \mathbb{Q}] = 3$, καὶ ὅπως στὸ Θεώρημα 1.2.3, ὁδηγούμαστε σὲ ἄτοπο. □

Θεώρημα 1.2.5. *Ὁ τετραγωνισμὸς τοῦ κύκλου εἶναι ἀδύνατος μὲ κανόνα καὶ διαβήτη.*

Ἀπόδειξη. Μποροῦμε νὰ ὑποθέσομε ὅτι μᾶς δίνουν ἕνα κύκλο μοναδιαίας ἀκτίνας, ὁπότε ἔχομε νὰ κατασκευάσομε ἕνα τετράγωνο ἐμβαδοῦ π, ἄρα νὰ κατασκευάσομε εὐθύγραμμο τμῆμα (πλευρὰ τοῦ τετραγώνου) μήκους $\sqrt{\pi}$. Ξεκινοῦμε πάλι ἀπὸ τὸ $S_0 = \{(0,0),(1,0)\}, K_0 = \mathbb{Q}$. Ἡ δυνατότητα κατασκευῆς εὐθυγράμμου τμήματος μήκους $\sqrt{\pi}$ συνεπάγεται (μὲ τὴ βοήθεια τῶν στοιχειωδῶν γεωμετρικῶν κατασκευῶν τῆς Εὐκλείδιας Γεωμετρίας) τὴ δυνατότητα κατασκευῆς εὐθυγράμμου τμήματος μήκους π. Συνεπῶς (Θεώρημα 1.2.2), ὑπάρχει πεπερασμένη ἐπέκταση τοῦ $\mathbb{Q}$, ποὺ περιέχει τὸν ἀριθμὸ π· εἰδικώτερα, λόγῳ τοῦ Θεωρήματος 1.1.6, αὐτὸ συνεπάγεται ὅτι ὁ ἀριθμὸς π εἶναι ἀλγεβρικός. Ὅμως, ὅπως ἀναφέραμε προηγουμένως, ἔχει ἀποδειχθεῖ ὅτι ὁ π εἶναι ὑπερβατικὸς καὶ αὐτὴ ἡ ἀντίφαση ὁλοκληρώνει τὴν ἀπόδειξη. □ὑπερβατικότητα τοῦ π ἀποδείχθηκε ἀπὸ τὸν Lindemann στὰ 1882.

Ἀσκήσεις

1. Ἀποδεῖξτε ὅτι ἡ κατασκευὴ τοῦ κανονικοῦ 9-γώνου μὲ κανόνα καὶ διαβήτη εἶναι ἀδύνατη.

2. Ἀποδεῖξτε ὅτι ἡ γωνία θ μπορεῖ νὰ τριχοτομηθεῖ μὲ κανόνα καὶ διαβήτη ἂν καὶ μόνο ἂν τὸ πολυώνυμο $4X^3 - 3X - \cos\theta \in \mathbb{Q}(\cos\theta)[X]$ εἶναι σύνθετο (δηλαδή, ὄχι ἀνάγωγο) πάνω ἀπὸ τὸ $\mathbb{Q}(\cos\theta)$.

3. Κάνοντας χρήση τοῦ τύπου γιὰ τὸ $\cos 5\theta$ περιγράψτε μέθοδο γεωμετρικῆς κατασκευῆς (μὲ κανόνα καὶ διαβήτη) τοῦ κανονικοῦ πενταγώνου.

1.3 Κατασκευη πεπερασμενων επεκτασεων δοθεντος σωματος

Μέχρι τώρα, ὅλα τὰ παραδείγματα ἐπεκτάσεων, ποὺ ἔχομε 'δεῖ, εἶναι ἐπεκτάσεις τοῦ $\mathbb{Q}$, οἱ ὁποῖες προέκυψαν μὲ ἐπισύναψη στὸ $\mathbb{Q}$ ἀριθμῶν ὅπως οἱ $\sqrt{2}$, $\sqrt{5}$, $\sqrt[3]{2}$ κλπ. Αὐτὸ πιθανὸν νὰ δίνει τὴ λανθασμένη ἐντύπωση ὅτι, γιὰ νὰ ἐπεκτείνομε ἕνα σῶμα K –γιὰ παράδειγμα, τὸ $\mathbb{Q}$– χρειαζόμαστε ἕνα μεγαλύτερο σῶμα –γιὰ παράδειγμα, τὸ $\mathbb{R}$ ἢ τὸ $\mathbb{C}$– ἀπὸ τὸ ὁποῖο νὰ ἐφοδιασθοῦμε μὲ τὰ στοιχεῖα ἐκεῖνα, μέσῳ τῶν ὁποίων θὰ ἐπεκταθεῖ τὸ " μικρὸ" σῶμα. Αὐτὸ δὲν εἶναι σωστό: Γιὰ παράδειγμα, ἂν θέλομε νὰ δημιουργήσομε ἕνα σῶμα, στὸ ὁποῖο τὸ πολυώνυμο $X^2 - 2 \in \mathbb{Q}[X]$ νὰ ἔχει ρίζα, δὲν χρειαζόμαστε τοὺς πραγματικοὺς ἀριθμούς, προκειμένου νὰ πάρομε ἀπ' αὐτοὺς τὴν τετραγωνικὴ ρίζα τοῦ 2 ($= 1.41421356\ldots$). Στὴν πραγματικότητα, ἀντὶ νὰ ξεκινήσομε ἀπὸ μία ἤδη γνωστὴ ἐπέκταση τοῦ K, παίρνοντας ἀπ' αὐτ'ην ἕνα στοιχεῖο καὶ ἐπισυνάπτοντάς το στὸ K, ξεκινοῦμε ἀπὸ τὸ K καὶ κατασκευάζομε, μὲ τὴ βοήθεια, καὶ μόνο, τοῦ K, ἕνα μεγαλύτερο σῶμα, ἔστω L, τὸ ὁποῖο ἔχει τὶς ἰδιότητες ποὺ ἐπιθυμοῦμε, π.χ. περιέχει ρίζα ἑνὸς δοθέντος ἀναγώγου πολυωνύμου τοῦ $K[X]$. Ἡ διαδικασία κατασκευῆς τοῦ " μεγαλύτερου" σώματος ἀπὸ τὸ μικρότερο δικαιολογεῖ τὴν ὁρολογία «τὸ L εἶναι ἐπέκταση τοῦ K» ἀντὶ τῆς ἰσοδύναμης ὁρολογίας «τὸ K εἶναι ὑπόσωμα τοῦ L». Αὐτὴ ἡ διαδικασία θὰ γίνει σαφέστερη μὲ ἕνα παράδειγμα. Θὰ ξεκινήσομε μὲ ἕνα σῶμα, ὅπως τὸ $\mathbb{Z}_3$, τοῦ ὁποίου καμμία γνήσια ἐπέκταση δὲν μᾶς εἶναι γνωστή (μὲ τὶς μέχρι τὶς μέχρι τώρα γνώσεις μας).

Θεωροῦμε τὸ $f(X) = X^2 + 1 \in \mathbb{Z}_3[X]$. Πρὶν προχωρήσομε, τονίζομε ὅτι τὰ στοιχεῖα τοῦ $\mathbb{Z}_3$ δὲν πρέπει νὰ συγχέονται μὲ τοὺς ἀκεραίους ἀριθμούς, παρὰ τὸ ὅτι συμβολίζονται μὲ σύμβολα ἀκεραίων ἀριθμῶν. Γιὰ παράδειγμα, ἂς θυμηθοῦμε ὅτι, στὸ σῶμα $\mathbb{Z}_3$ ἰσχύει $1 + 2 = 0$, $-1 = 2$ κλπ κάτι, βέβαια, ποὺ δὲν ἰσχύει στοὺς ἀκεραίους. Ἕνας ἁπλὸς ὑπολογισμὸς μᾶς πείθει ὅτι τὸ $f(X)$ δὲν ἔχει ρίζα στὸ $\mathbb{Z}_3$. Ἀπὸ τὴν ἄλλη, πάλι, δὲν ἔχομε πάνω ἀπ' τὸ $\mathbb{Z}_3$ ἕνα " πλούσιο" σῶμα, ὅπως εἴχαμε τὸ $\mathbb{C}$, στὴν περίπτωση ποὺ μελετούσαμε τὸ $X^2 + 1$ ὡς πολυώνυμο τοῦ $\mathbb{Q}[X]$, γιὰ ν' " ἁπλώσομε τὸ χέρι" καὶ νὰ πάρομε ἀπὸ αὐτὸ τὸν ἀριθμὸ $i = \sqrt{-1}$. Τὸ ἐρώτημα, λοιπόν εἶναι: *Ὑπάρχει κάποιο σῶμα K, ποὺ νὰ περιέχει τὸ $\mathbb{Z}_3$, ἐντὸς τοῦ ὁποίου τὸ $f(X)$ νὰ ἔχει ρίζα;*

Ἂς ὑποθέσομε ὅτι ὑπάρχει ἕνα τέτοιο σῶμα L. Θὰ ἔχομε, λοιπόν, $L \supseteq \mathbb{Z}_3$ καὶ τὸ L περιέχει κάποιο στοιχεῖο ρ, τέτοιο ὥστε $\rho^2 + 1 = 0$ (σχέση στὸ L). Ἀλλά, ἀφοῦ τὸ L εἶναι σῶμα καὶ περιέχει τὸ $\mathbb{Z}_3$ καὶ τὸ ρ, " εἶναι ὑποχρεωμένο" νὰ περιέχει καὶ ὅλα τὰ στοιχεῖα $a + b\rho$ μὲ $a, b \in \mathbb{Z}_3$. Οἱ πιθανὲς τιμὲς τῶν a, b εἶναι $0, 1, 2 \in \mathbb{Z}_3$, ἄρα τὸ L " ὀφείλει" νὰ περιέχει τοὐλάχιστον τὰ ἑξῆς 9 στοιχεῖα:

$$0,\ 1,\ 2,\ \rho,\ 1+\rho,\ 2+\rho,\ 2\rho,\ 1+2\rho,\ 2+2\rho.$$

Ἐπίσης, δεδομένου ὅτι τὸ L εἶναι σῶμα, οἱ πράξεις τοῦ L πρέπει νὰ εἶναι ἀντιμεταθετικὲς καὶ νὰ ἱκανοποιοῦν τὶς ἑξῆς ἀπαιτήσεις (ἔχοντας πάντα κατὰ νοῦ ὅτι τὰ $0, 1, 2$ εἶναι στοιχεῖα τοῦ $\mathbb{Z}_3$, ἐνῶ $\rho^2 + 1 = 0$):

$$(a_1 + b_1\rho) + (a_2 + b_2\rho) = (a_1 + a_2) + (b_1 + b_2)\rho \tag{1.1}$$

καὶ

$$\begin{aligned}(a_1 + b_1\rho)\cdot(a_2 + b_2\rho) &= a_1a_2 + a_1(b_2\rho) + (b_1\rho)a_2 + (b_1\rho)(b_2\rho)\\ &= a_1a_2 + a_1b_2\rho + b_1a_2\rho + b_1b_2\rho^2\\ &= (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)\rho\,. \qquad (1.2)\end{aligned}$$

Μὲ βάση τὰ παραπάνω, οἱ πίνακες πρόσθεσης καὶ πολλαπλασιασμοῦ τῶν 9 στοιχείων εἶναι οἱ ἑξῆς:

Πίνακας πρόσθεσης

$+$	0	1	2	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$
0	0	1	2	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$
1	1	2	0	$1+\rho$	$2+\rho$	ρ	$1+2\rho$	$2+2\rho$	2ρ
2	2	0	1	$2+\rho$	ρ	$1+\rho$	$2+2\rho$	2ρ	$1+2\rho$
ρ	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$	0	1	2
$1+\rho$	$1+\rho$	$2+\rho$	ρ	$1+2\rho$	$2+2\rho$	2ρ	1	2	0
$2+\rho$	$2+\rho$	ρ	$1+\rho$	$2+2\rho$	2ρ	$1+2\rho$	2	0	1
2ρ	2ρ	$1+2\rho$	$2+2\rho$	0	1	2	ρ	$1+\rho$	$2+\rho$
$1+2\rho$	$1+2\rho$	$2+2\rho$	2ρ	1	2	0	$1+\rho$	$2+\rho$	ρ
$2+2\rho$	$2+2\rho$	2ρ	$1+2\rho$	2	0	1	$2+\rho$	ρ	$1+\rho$

Πίνακας πολλαπλασιασμοῦ

$\cdot$	1	2	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$
1	1	2	ρ	$1+\rho$	$2+\rho$	2ρ	$1+2\rho$	$2+2\rho$
2	2	1	2ρ	$2+2\rho$	$1+2\rho$	ρ	$2+\rho$	$1+\rho$
ρ	ρ	2ρ	2	$2+\rho$	$2+2\rho$	1	$1+\rho$	$1+2\rho$
$1+\rho$	$1+\rho$	$2+2\rho$	$2+\rho$	2ρ	1	$1+2\rho$	2	ρ
$2+\rho$	$2+\rho$	$1+2\rho$	$2+2\rho$	1	ρ	$1+\rho$	2ρ	2
2ρ	2ρ	ρ	1	$1+2\rho$	$1+\rho$	2	$2+2\rho$	$2+\rho$
$1+2\rho$	$1+2\rho$	$2+\rho$	$1+\rho$	2	2ρ	$2+2\rho$	ρ	1
$2+2\rho$	$2+2\rho$	$1+\rho$	$1+2\rho$	ρ	2	$2+\rho$	1	2ρ

Μιὰ προσεκτικὴ μελέτη τῶν παραπάνω πινάκων δείχνει ὅτι οἱ πράξεις $+$ καὶ $\cdot$ στὸ σύνολο τῶν 9 στοιχείων $\{0,\ 1,\ 2,\ \rho,\ 1+\rho,\ 2+\rho,\ 2\rho,\ 1+2\rho,\ 2+2\rho\}$ εἶναι κλειστές, οὐδέτερο στοιχεῖο τῆς πράξης $+$ εἶναι τὸ $0 \in \mathbb{Z}_3$ καὶ οὐδέτερο στοιχεῖο τῆς $\cdot$ εἶναι τὸ $1 \in \mathbb{Z}_3$. Ἐπίσης, κάθε ἕνα ἀπὸ τὰ 9 στοιχεῖα ἔχει ἀντίθετο καὶ κάθε ἕνα ἀπὸ τὰ 8 μὴ μηδενικὰ στοιχεῖα ἔχει ἀντίστροφο. Ὁ ἔλεγχος τῆς προσεταιριστικότητας μὲ τὴ βοήθεια τῶν πινάκων θὰ ἦταν ἐξαιρετικὰ κοπιαστικὸς καὶ ἀνιαρός! Εἶναι πολὺ εὐκολώτερο ν' ἀποδείξομε τὴν προσεταιριστικότητα μὲ τὴ βοήθεια τῶν σχέσεων (1.1) καὶ (1.2).

Τὸ συμπέρασμα εἶναι ὅτι τὰ παραπάνω 9 στοιχεῖα, ἐφοδιασμένα μὲ τὶς πράξεις $+$ καὶ $\cdot$ φτιάχνουν ἕνα σῶμα, ποὺ ἱκανοποιεῖ τὶς ἀπαιτήσεις μας: Περιέχει τὸ $\mathbb{Z}_3$, καθὼς καὶ μία ρίζα τοῦ πολυωνύμου X^2+1 (ἄρα περιέχει καὶ τὴ δεύτερη ρίζα, ποὺ εἶναι ἡ ἀντίθετη τῆς πρώτης).

Ἂν τώρα ἔχομε ἕνα *ὁποιοδήποτε σῶμα* K καὶ ἕνα *ὁποιοδήποτε ἀνάγωγο πολυώνυμο* $f(X) \in K[X]$, τότε μιὰ διαδικασία ἀνάλογη μὲ τὴν παραπάνω γιὰ τὴν κατασκευὴ σώματος, ποὺ περιέχει συγχρόνως τὸ K καὶ μία ρίζα τοῦ $f(X)$, "φαίνεται" ὅτι μπορεῖ νὰ ἐπαναληφθεῖ. Θὰ προτιμούσαμε, ὅμως, μιὰ γενικὴ ἀπόδειξη αὐτοῦ τοῦ ἰσχυρισμοῦ πιὸ αὐστηρὴ καὶ ἀνεξάρτητη ἀπὸ πράξεις καὶ πίνακες, τοὺς ὁποίους, ἄλλωστε, δὲν μποροῦμε νὰ φτιάξομε, καθὼς τὰ K καὶ $f(X)$ δὲν εἶναι πιὰ συγκεκριμένα. Ἐδῶ εἶναι μία ἀπὸ τὶς περιπτώσεις στὴν ὁποία γίνεται φανερὴ ἡ σπουδαιότητα τῆς ἀφαίρεσης στὰ Μαθηματικά.

Ξεκινοῦμε, λοιπόν, μὲ ἕνα σῶμα K καὶ ἕνα ἀνάγωγο πολυώνυμο $p(X) \in K[X]$. Ἡ ἐνδιαφέρουσα περίπτωση εἶναι ὅταν $\deg p = n > 1$, ὁπότε τὸ $p(X)$ δὲν ἔχει ρίζα στὸ K. Θέλομε νὰ κατασκευάσομε μία ἐπέκταση L τοῦ K, ὅσο τὸ δυνατὸν πιὸ μικρή, μέσα στὴν ὁποία τὸ $p(X)$ νὰ ἔχει ρίζα. Στὸ $K[X]$ ὁρίζομε τὴν ἑξῆς σχέση:

$$f(X) \equiv g(X) \quad \Leftrightarrow \quad p(X) \mid (f(X) - g(X)) \tag{1.3}$$

Εἶναι τετριμμένο ν' ἀποδείξει κανεὶς ὅτι αὐτὴ εἶναι σχέση ἰσοδυναμίας. Τὴν κλάση ἰσοδυναμίας ἑνὸς ὁποιουδήποτε $f(X) \in K[X]$ συμβολίζομε μὲ $\overline{f(X)}$. Τὸ σύνολο τῶν κλάσεων ἰσοδυναμίας (σύνολο-πηλῖκο τοῦ $K[X]$, ὡς πρὸς αὐτὴ τὴ σχέση ἰσοδυναμίας) συμβολίζομε μὲ L. Ἄρα, στὸ L, ἡ ἰσότητα $\overline{f(X)} = \overline{g(X)}$ σημαίνει ὅτι $f(X), g(X) \in K[X]$ καὶ τὸ $p(X)$ διαιρεῖ τὴ διαφορὰ $f(X) - g(X)$. Παρατηρῆστε ὅτι, ἂν $a, b \in K$ καὶ τὰ δοῦμε ὡς σταθερὰ πολυώνυμα τοῦ $K[X]$, τότε $\overline{a} = \overline{b}$ ἄν, καὶ μόνο ἄν, $a = b$, διότι τὸ $p(X)$ δὲν μπορεῖ νὰ διαιρεῖ τὸ σταθερὸ πολυώνυμο $a - b$, ἐκτὸς ἂν $a - b = 0$. Αὐτὸ σημαίνει ὅτι ἡ ἀπεικόνιση $K \to L$, ποὺ στέλνει τὸ $a \in K$ στὸ $\overline{a} \in L$, εἶναι 1-1.

Τώρα θα κάνομε τὸ L σῶμα, ὁρίζοντας πρόσθεση καὶ πολλαπλασιασμὸ ὡς ἑξῆς:

$$\overline{f(X)} + \overline{g(X)} = \overline{f(X) + g(X)}, \quad \overline{f(X)} \cdot \overline{g(X)} = \overline{f(X) \cdot g(X)}. \tag{1.4}$$

Οἱ πράξεις αὐτὲς εἶναι καλὰ ὁρισμένες καὶ καθιστοῦν τὸ L ἀντιμεταθετικὸ δακτύλιο μὲ μοναδιαῖο στοιχεῖο (ἄσκηση ...). Γιὰ νὰ εἶναι σῶμα τὸ L μένει νὰ δείξομε ὅτι κάθε μὴ μηδενικὸ στοιχεῖο $\overline{f(X)} \in L$ ἔχει ἀντίστροφο, δηλαδή, ὑπάρχει $\overline{f'(X)} \in L$, τέτοιο ὥστε $\overline{f'(X)} \cdot \overline{f(X)} = \overline{1}$. Ἀλλὰ $\overline{f(X)} \neq \overline{0}$ σημαίνει ὅτι τὸ $f(X)$ δὲν διαιρεῖται ἀπὸ τὸ $p(X)$. Καὶ ἀφοῦ τὸ $p(X)$ εἶναι ἀνάγωγο καὶ δὲν διαιρεῖ τὸ $f(X)$, ἕπεται ὅτι τὰ $f(X)$ καὶ $p(X)$ εἶναι πρῶτα μεταξύ τους (βλ. Παράρτημα Α΄), ὁπότε, ἀπὸ τὸ 3 τῆς Πρότασης Α΄.2, ὑπάρχουν $f'(X), p'(X) \in K[X]$, τέτοια ὥστε $f'(X)f(X) + p'(X)p(X) = 1$. Ἄρα, τὸ $p(X)$ διαιρεῖ τὸ $f'(X)f(X) - 1$, ποὺ σημαίνει ὅτι $\overline{f'(X)f(X)} = \overline{1}$, ἄρα τὸ $\overline{f'(X)}$ εἶναι τὸ ἀντίστροφο τοῦ $\overline{f(X)}$. Εἴδαμε πιὸ πάνω ὅτι τὸ σῶμα K εἶναι σὲ 1-1 ἀντιστοιχία μὲ τὸ ὑποσύνολο $\{\overline{a} : a \in K\}$. Στὴν πραγματικότητα, τὸ τελευταῖο αὐτὸ σύνολο εἶναι "ἀκριβὲς ἀντίγραφο" τοῦ K: Πρόκειται γιὰ ὑπόσωμα τοῦ L, τοῦ ὁποίου τὰ στοιχεῖα εἶναι τὰ ἴδια μὲ τοῦ K, ἔχοντας, ἁπλῶς, μιὰ "γραμμούλα" πάνω τους[4]. Ἔτσι, μποροῦμε νὰ θεωρήσομε τὸ K ὡς ὑπόσωμα τοῦ L –ἤ, ἰσοδύναμα, τὸ L ἐπέκταση τοῦ K– καὶ ἀντὶ νὰ γράφομε $\overline{a}$ (ὅταν $a \in K$) θὰ γράφομε ἁπλῶς a.

Ἂς δοῦμε τώρα προσεκτικὰ τὰ στοιχεῖα τοῦ L. Θέτομε $\lambda = \overline{X} \in L$. Τὸ τυπικὸ στοιχεῖο τοῦ L εἶναι τῆς μορφῆς $\overline{f(X)}$, ὅπου $f(X) \in K[X]$, ἔστω $f(X) = a_0 + a_1X + \cdots + a_nX^n$. Τότε (ἔχοντας πάντα στὸν νοῦ τὴ σύμβαση, ποὺ κάναμε παραπάνω ὅτι, δηλαδή, ἁπλοποιοῦμε τὸ $\overline{a}$ σὲ a, ὅταν $a \in K$),

$$\begin{aligned}
\overline{f(X)} &= \overline{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n} = \overline{a_0} + \overline{a_1}\,\overline{X} + \overline{a_2}\,\overline{X^2} + \cdots + \overline{a_n}\,\overline{X^n} \\
&= a_0 + a_1\overline{X} + a_2\overline{X}^2 + \cdots + a_n\overline{X}^n = a_0 + a_1\lambda + a_2\lambda^2 + \cdots a_n\lambda^n \\
&= f(\lambda).
\end{aligned}$$

Ἄρα, κάθε στοιχεῖο τοῦ L εἶναι πολυωνυμικὴ παράσταση τοῦ λ μὲ συντελεστὲς ἀπὸ τὸ K, δηλαδή, ἀνήκει στὸ $K(\lambda)$, ὁπότε $L \subseteq K(\lambda)$. Ἀλλὰ καὶ ἀντιστρόφως, ἀφοῦ τὸ K περιέχεται στὸ L καὶ $\lambda \in L$, ἕπεται ὅτι $K(\lambda) \subseteq L$, ἄρα $L = K(\lambda)$.

[4] Σὲ πιὸ τυπικὴ μαθηματικὴ γλῶσσα: Ἡ ἀπεικόνιση $K \to L$, ποὺ στέλνει τὸ $a \in K$ στὸ $\overline{a} \in L$ εἶναι μονομορφισμὸς σωμάτων.

Τέλος, ἂς ὑπόλογίσομε τὸ $p(\lambda)$. Ὅπως εἴδαμε λίγο πιὸ πάνω, γιὰ ὁποιοδήποτε $f(X) \in K[X]$, ἰσχύει ὅτι $f(\lambda) = \overline{f(X)}$, ἄρα, $p(\lambda) = \overline{p(X)} = \overline{0} = 0$ (μὴ ξεχνᾶτε τὴ σύμβαση $\overline{a} = a$!). Μ' ἄλλα λόγια, τὸ $\lambda \in L$ εἶναι ρίζα τοῦ πολυωνύμου $p(X)$ κι ἔτσι καταλήξαμε στὸ ἑξῆς θεώρημα.

Θεώρημα 1.3.1. *Ἔστω σῶμα K καὶ πολυώνυμο $p(X)$ ἀνάγωγο πάνω ἀπ' τὸ K. Τότε μποροῦμε νὰ κατασκευάσομε σῶμα L μὲ τὶς ἑξῆς ἰδιότητες: (1) Τὸ K περιέχεται στὸ L ὡς ὑπόσωμά του. (2) Ὑπάρχει $\lambda \in L$, τέτοιο ὥστε $p(\lambda) = 0$ καὶ $L = K(\lambda)$.*

Τὸ θεώρημα αὐτὸ μᾶς ἐπιτρέπει νὰ θεμελιώσομε αὐστηρὰ τὴν κατασκευὴ ἐπεκτάσεων, ὅπως αὐτὴ ποὺ κάναμε στὸ παραπάνω παράδειγμα μὲ τὸ $\mathbb{Z}_3$ καὶ τὸ $X^2 + 1 \in \mathbb{Z}_3[X]$, ὡς ἑξῆς: Τὸ $p(X) = X^2 + 1 \in \mathbb{Z}_3[X]$ εἶναι ἀνάγωγο, ἄρα, βάσει τοῦ Θεωρήματος 1.3.1, ὑπάρχει ἐπέκταση L τοῦ $\mathbb{Z}_3$ καὶ $\rho \in L$, ἔτσι ὥστε $L = \mathbb{Z}_3(\rho)$ καὶ $\rho^2 + 1 = 0$. Ἀπὸ τὸ Θεώρημα 1.1.3, μία βάση τῆς ἐπέκτασης $L/\mathbb{Z}_3$ ἀποτελοῦν τὰ $1, \rho$, ἄρα $L = \{a + b\rho : a, b \in \mathbb{Z}_3\}$. Ἀπὸ τὴν τελευταία σχέση προκύπτει, μεταξὺ ἄλλων, ὅτι τὸ L ἔχειἀκριβῶς 9 στοιχεῖα. Ἐπίσης, τὸ θεώρημα μᾶς ἀπαλλάσσει ἀπὸ τὰ πολλὰ καὶ κάπως ἀμφίβολης αὐστηρότητας λόγια μὲ τὰ ὁποῖα καταλήξαμε στὶς σχέσεις (1.1), (1.2) καί, τελικά, στοὺς πίνακες τῶν πράξεων.

Ἀσκήσεις

1. Ἔστω σῶμα K καὶ $p(X) \in K[X]$ ἀνάγωγο. Ἀποδεῖξτε ὅτι ἡ σχέση (1.3) εἶναι ἰσοδυναμία στὸ $K[X]$. Ἔστω L τὸ σύνολο τῶν κλασεων ἰσοδυναμίας· τὴν κλάση ἰσοδυναμίας ἑνὸς $f(X) \in K[X]$ συμβολίζομε, ὅπως παραπάνω, μὲ $\overline{f(X)}$). Ὁρίζομε πράξεις στὸ L ἀπὸ τὶς σχέσεις (1.4). Ἀποδεῖξτε ὅτι οἱ πράξεις αὐτὲς εἶναι καλὰ ὁρισμένες καὶ καθιστοῦν τὸ L ἀντιμεταθετικὸ δακτύλιο μὲ μοναδιαῖο στοιχεῖο.

2. Κατασκευᾶστε σῶμα μὲ 8 στοιχεῖα. Δηλαδή, περιγρᾶψτε τὴν κατασκευή του καὶ φτιάξτε τοὺς πίνακες τῶν πράξεών του.
   Ὑπόδειξη. Θεωρῆστε τὸ πολυώνυμο $p(X) = X^3 + X + 1 \in \mathbb{Z}_2[X]$ καὶ διαπιστῶστε ὅτι εἶναι ἀνάγωγο. Ἐφαρμόστε τὸ Θεώρημα 1.3.1, ἐπιχειρηματολογώντας κατ' ἀναλογία μὲ τὸ σχόλιο ποὺ ἀκολουθεῖ τὸ θεώρημα αὐτό.

1.4 Σωμα ριζων πολυωνυμου

Στὸ ἐδάφιο 1.3 εἴδαμε ὅτι, ἂν ἔχομε ἕνα σῶμα K καὶ ἕνα ἀνάγωγο $p(X) \in K[X]$, τότε ὑπάρχει ἐπέκταση L τοῦ K, μέσα στὴν ὁποία τὸ $p(X)$, θεωρούμενο ὡς πολυώνυμο τοῦ $L[X]$, ἔχει μία τοὐλάχιστον ρίζα, ἔστω $\lambda \in L$ καὶ μάλιστα, $L = K(\lambda)$. Δὲν ἀποκλείεται νὰ περιέχει τὸ L κι ἄλλες ρίζες τοῦ $p(X)$, ἀλλὰ αὐτὸ δὲν εἶναι ὁ κανόνας. Πολὺ περισσότερο δὲν εἶναι κανόνας νὰ περιέχονται *ὅλες* οἱ ρίζες τοῦ $p(X)$ στὸ L. Τί σημαίνει, ὅμως, νὰ περιέχονται ὅλες οἱ ρίζες τοῦ $p(X)$ στὸ L; Ὁ παρακάτω ὁρισμὸς δίνει μιὰ πρώτη ἰδέα γιὰ τὸ πῶς θὰ προσεγγίσομε αὐτὸ τὸ ζήτημα.

Ὁρισμὸς 1.4.1. *Ἔστω σῶμα K καὶ μὴ σταθερὸ $f(X) \in K[X]$ βαθμοῦ n. Ἡ ἐπέκταση L τοῦ K λέγεται σῶμα ριζῶν τοῦ $f(X)$ ἂν ὑπάρχουν $\rho_1, \ldots, \rho_n \in L$, τέτοια ὥστε, $f(X) = c(X-\rho_1)\ldots(X-\rho_n)$ γιὰ κάποιο $c \in K$ (ὁ συντελεστὴς τοῦ μεγιστοβαθμίου ὅρου τοῦ f) καὶ $L = K[\rho_1, \ldots, \rho_n]$.*

Σημείωση: Προσοχή! Τὸ σῶμα ριζῶν ἐξαρτᾶται οὐσιωδῶς ἀπὸ τὸ σῶμα K· δεῖτε, ὁπωσδήποτε, τὴν ἄσκηση 2. Γι' αὐτό, ἀκριβέστερο (καὶ ἀσφαλέστερο) εἶναι νὰ λέμε π.χ. ὅτι τὸ L εἶναι σῶμα ριζῶν τοῦ f *πάνω ἀπὸ τὸ* K, ἤ, συντομώτερα, ὅτι τὸ L εἶναι σῶμα ριζῶν τοῦ $f(X) \in K[X]$, ὑποδηλώνοντας σαφῶς ποιὸς εἶναι ὁ βασικὸς δακτύλιος πολυωνύμων στὸν ὁποῖο θεωροῦμε ὅτι ἀνήκει τὸ $f(X)$.

Θεώρημα 1.4.2. *Κάθε μὴ σταθερὸ πολυώνυμο μὲ συντελεστὲς ἀπὸ ἕνα σῶμα K ἔχει σῶμα ριζῶν πάνω ἀπὸ τὸ K.*

Ἀπόδειξη. Ἐπαγωγικὰ ἐπὶ τοῦ βαθμοῦ τοῦ πολυωνύμου. Κατ' ἀρχάς, εἶναι προφανὲς ὅτι ὅλα τὰ πολυώνυμα πρώτου βαθμοῦ μὲ συντελεστὲς ἀπὸ ἕνα ὁποιοδήποτε σῶμα K ἔχουν σῶμα ριζῶν τὸ ἴδιο τὸ K. Ἄς ὑποθέσομε ὅτι, γιὰ κάποιο $n \geq 2$, ὅλα τὰ πολυώνυμα βαθμοῦ $< n$ μὲ συντελεστὲς ἀπὸ ὁποιοδήποτε σῶμα, ἔχουν σῶμα ριζῶν. Θεωροῦμε τώρα ἕνα πολυώνυμο $f(X)$ βαθμοῦ n μὲ συντελεστὲς ἀπὸ κάποιο σῶμα K. Ἔστω $p(X)$ ἕνας ἀνάγωγος παράγων τοῦ $f(X)$. Σύμφωνα μὲ τὸ Θεώρημα 1.3.1, ὑπάρχει ἐπέκταση L/K καὶ $\rho_1 \in L$, ἔτσι ὥστε $L = K[\rho_1]$ καὶ τὸ ρ_1 εἶναι ρίζα τοῦ $p(X)$. Τότε $f(X) = (X-\rho_1)g(X)$, $g(X) \in L[X]$ καὶ ὁ βαθμὸς τοῦ $g(X)$ εἶναι $= n-1$. Λόγῳ τῆς ἐπαγωγικῆς ὑποθέσεως, ὑπάρχει ἐπέκταση M τοῦ L καὶ $\rho_2, \ldots, \rho_n \in M$ ἔτσι ὥστε $g(X) = c(X-\rho_2)\ldots(X-\rho_n)$, $c \in L$ καὶ $M = L[\rho_2, \ldots, \rho_n]$. Τότε ὅμως, $f(X) = c(X-\rho_1)(X-\rho_2)\ldots(X-\rho_n)$ (ἄρα τὸ c εἶναι ὁ συντελεστὴς τοῦ μεγιστοβαθμίου ὅρου τοῦ $f(X)$ καί, συνεπῶς, εἶναι στοιχεῖο τοῦ σώματος K) καὶ $M = K[\rho_1, \rho_2, \ldots, \rho_n]$. □

Θεώρημα 1.4.3. *Ἔστω ἕνας ἰσομορφισμὸς σωμάτων $\sigma : K \to K'$ καὶ $p(X) = a_0 + a_1X + \ldots + a_nX^n \in K[X]$ μὴ σταθερὸ ἀνάγωγο πολυώνυμο. Ἔστω $p'(X) = \sigma(a_0) + \sigma(a_1)X + \ldots + \sigma(a_n)X^n \in K'[X]$. Ἂν u, v εἶναι ρίζες τῶν $p(X)$ καὶ $p'(X)$ (σὲ κάποιες κατάλληλες ἐπεκτάσεις τῶν K καὶ K'), ἀντιστοίχως, τότε ὁ σ μπορεῖ νὰ ἐπεκταθεῖ σὲ ἕνα ἰσομορφισμὸ $\tilde{\sigma} : K[u] \to K'[v]$ ὁ ὁποῖος, ἐπιπλέον, ἱκανοποιεῖ τὴν $\tilde{\sigma}(u) = v$.*

Ἀπόδειξη. Γιὰ νὰ ἁπλουστεύσομε τὸ συμβολισμὸ γράφομε, γιὰ κάθε $u \in K, \sigma(u) = u'$ καὶ ἀντιστρόφως, τὰ στοιχεῖα τοῦ K' τὰ γράφομε μὲ τὴ μορφὴ $u' = \sigma(u)$ γιὰ κάποιο (ἀκριβῶς ἕνα) $u \in K$. Πρῶτα παρατηροῦμε ὅτι τὸ $p'(X)$ εἶναι ἀνάγωγο. Πράγματι, διότι ἂν ἦταν $p'(X) = (a'_0 + a'_1X + \ldots + a'_kX^k)(b'_0 + b'_1X + \ldots + b'_mX^m)$ μὲ $k, m \geq 1$, τότε καὶ $p(X) = (a_0 + a_1X + \ldots + a_kX^k)(b_0 + b_1X + \ldots + b_mX^m)$,[5] ὁπότε θὰ ἐρχόμασταν σὲ ἀντίφαση μὲ τὴν ὑπόθεσή μας γιὰ τὸ $p(X)$. Ἐπίσης, ἐπειδὴ ὁ πολλαπλασιασμὸς ἑνὸς πολυωνύμου ἐπὶ μὴ

[5] Αὐτό, ὅσο κι ἂν εἶναι εὔλογο διαισθητικά, δὲν εἶναι ἐντελῶς τετριμμένο· βλ. ἄσκηση 3.

μηδενικὴ σταθερὰ δὲν ἐπηρεάζει τὶς ρίζες του, μποροῦμε, χωρὶς βλάβη τῆς γενικότητος, νὰ ὑποθέσομε μονικὸ τὸ $p(X)$ (ἄρα καὶ τὸ $p'(X)$). Τὰ πολυώνυμα $p(X), p'(X)$ ἔχουν τὸν ἴδιο βαθμό, ἔστω n, ὁπότε (Θεώρημα 1.1.3) τὰ $1, u, \ldots, u^{n-1}$ ἀποτελοῦν βάση τῆς $K[u]/K$, ἐνῶ τὰ $1, v, \ldots, v^{n-1}$ βάση τῆς $K'[v]/K'$. Εὔκολα ἐλέγχεται τώρα ὅτι ἡ ἀπεικόνιση $\tilde{\sigma} : K[u] \to K'[v]$, ἡ ὁποία ὁρίζεται ἀπὸ τὴ σχέση

$$\tilde{\sigma}(c_0 + c_1 u + \ldots + c_{n-1} u^{n-1}) = c'_0 + c'_1 v + \ldots + c'_{n-1} v^{n-1}$$

γιὰ ὅλα τὰ $c_0, c_1, \ldots, c_{n-1} \in K$, ἔχει ὅλες τὶς ἰδιότητες ποὺ ἀπαιτεῖ τὸ θεώρημα (βλ. ἄσκηση 4). □

Τὸ ὑπόλοιπο αὐτῆς τῆς ἑνότητας ἀφιερώνεται, οὐσιαστικά, στὴν ἀπόδειξη τῆς μοναδικότητος τοῦ σώματος ριζῶν ἑνὸς πολυωνύμου, ἡ ὕπαρξη τοῦ ὁποίου ἐξασφαλίζεται ἀπὸ τὸ Θεώρημα 1.4.2. Στὸ θεώρημα ποὺ ἀκολουθεῖ, ἀλλὰ καὶ στὴ συνέχεια τούτων τῶν σημειώσεων, ὅταν ἔχομε ἕνα ἰσομορφισμὸ σωμάτων (ἢ καὶ δακτυλίων) $\phi : K \to L$ καὶ τὰ πολυώνυμα $f(X) \in K[X]$ καὶ $g(X) \in L[X]$, τότε θὰ λέμε ὅτι τὰ πολυώνυμα αὐτὰ ἀντιστοιχοῦν μέσῳ τοῦ ϕ, ἂν $g(X) = \phi f(X)$ (γιὰ τὸ συμβολισμὸ τοῦ δεξιοῦ μέλους βλ. ἄσκηση 3).

Θεώρημα 1.4.4. *Ἔστω $\phi : K \to K'$ ἰσομορφισμὸς σωμάτων. Ἂν τὰ $f(X) \in K[X]$ καὶ $f'(X) \in K'[X]$ ἀντιστοιχοῦν μέσῳ τοῦ ϕ καὶ L/K, L'/K' εἶναι σώματα ριζῶν τῶν $f(X)$ καὶ $f'(X)$, ἀντιστοίχως, τότε ὁ ἰσομορφισμὸς ϕ μπορεῖ νὰ ἐπεκταθεῖ σὲ ἰσομορφισμὸ $L \to L'$.*

Ἀπόδειξη. Μὲ ἐπαγωγὴ στὸ βαθμὸ $[L : K]$, ὁ ὁποῖος εἶναι πεπερασμένος λόγῳ τοῦ ὁρισμοῦ τοῦ σώματος ριζῶν καὶ τοῦ Θεωρήματος 1.1.5. Ἔστω ὅτι $[L : K] = 1$, ὁπότε $L = K$. Ἐξ ὁρισμοῦ τοῦ L, αὐτὸ σημαίνει ὅτι ὑπάρχουν $c, u_1, \ldots, u_m \in K$, τέτοια ὥστε $f(X) = c(X - u_1)\cdots(X - u_k)$. Τότε $f'(X) = c'(X - u'_1)\cdots(X - u'_m)$, ὅπου $c' = \phi(c) \in K'$ καὶ $u'_i = \phi(u_i) \in K'$ γιὰ $i = 1, \ldots, m$. Ἐξ ὁρισμοῦ τοῦ L', ὑπάρχουν $k' \in K'$ καὶ $\lambda'_1, \ldots, \lambda'_m \in L'$, τέτοια ὥστε $f'(X) = k'(X - \lambda'_1)\cdots(X - \lambda'_m)$ καὶ $L' = K'[\lambda'_1, \ldots, \lambda'_m]$. Στὸ $L'[X]$ ἰσχύει ἡ μονοσήμαντη ἀνάλυση σὲ ἀνάγωγα πολυώνυμα, ἄρα ἡ σχέση $c'(X - u'_1)\cdots(X - u'_m) = k'(X-\lambda'_1)\cdots(X-\lambda'_m)$ συνεπάγεται ὅτι $k = c'$ καὶ τὰ $\lambda'_1, \ldots, \lambda'_m$ εἶναι μετ;αθεση τῶν $u'_1, \ldots, u'_m$. Συνεπῶς, $L' = K'[\lambda'_1, \ldots, \lambda'_m] = K'[u'_1, \ldots, u'_m] = K'$, ὁπότε $\phi : L \to L'$ εἶναι ἰσομορφισμός, ποὺ ἐπεκτείνει (ἐδῶ ταυτίζεται μὲ) τὸν ἰσομορφισμὸ $\phi : K \to K'$.

Ἔστω τώρα ἀκέραιος $n > 1$ κι ἂς ὑποθέσομε ὅτι τὸ θεώρημα ἰσχύει ὅταν τὸ πολυώνυμο $f(X)$ εἶναι τέτοιο ὥστε $[L : K] < n$. Θεωροῦμε, στὴ συνέχεια, πολυώνυμο $f(X) \in K[X]$, γιὰ τὸ ὁποῖο $[L : K] = n$, καὶ ἔστω $p(X)$ ἀνάγωγος παράγοντάς του βαθμοῦ > 1. Μέσῳ τοῦ ἰσομορφισμοῦ ϕ τὸ $p(X)$ ἀντιστοιχεῖ σὲ ἕνα πολυώνυμο $p'(X) \in K'[X]$. Ἀπὸ τὸν ὁρισμὸ τοῦ L ἕπεται ὅτι ὑπάρχει $u \in L$, τέτοιο ὥστε $p(u) = 0$ καί, ἐντελῶς ἀνάλογα, ὑπάρχει $v \in L'$, τέτοιο ὥστε $p'(v) = 0$. Ἀπὸ τὸ Θεώρημα 1.4.3 ξέρομε ὅτι ὁ ϕ ἐπεκτείνεται σὲ ἕναν ἰσομορφισμὸ $\tilde{\phi} : K[u] \to K'[v]$ [6]. Θέτομε $K_1 = K[u]$ καὶ $K'_1 = K'[v]$ καὶ ἀπὸ τὴν ἄσκηση 5 ξέρομε ὅτι, ἂν δοῦμε τὰ $f(X)$ καὶ $f'(X)$ ὡς πολυώνυμα τῶν $K_1[X]$ καὶ $K'_1[X]$, τὰ L, L' ἐξακολουθοῦν νὰ εἶναι σώματα ριζῶν τους, ἀντιστοίχως. Ὅμως τώρα, $[L : K_1]$ =(Θεώρημα 1.1.4) $[L : K]/[K_1 : K] < [L : K] = n$, ὁπότε ἡ ἐπαγωγικὴ ὑπόθεση συνεπάγεται ὅτι ὁ $\tilde{\phi}$ ἐπεκτείνεται σὲ ἰσομορφισμὸ $L \to L'$. Προφανῶς, αὐτὸς ὁ ἰσομορφισμός, ὡς ἐπέκταση τοῦ $\tilde{\phi}$, εἶναι καὶ ἐπέκταση τοῦ ϕ. □

Ἂν τώρα στὸ Θεώρημα 1.4.4 τεθεῖ ὅπου K' τὸ K καὶ ὅπου ϕ ὁ ταυτοτικὸς ἰσομορφισμός, τότε συμπεραίνομε ὅτι ὑπάρχει ἕνας ἰσομορφισμὸς μεταξὺ δύο ὁποιωνδήποτε σωμάτων ριζῶν L καὶ L' τοῦ $f(X) \in K[X]$, ὁ ὁποῖος, μάλιστα, ἀφήνει ἀναλλοίωτα ὅλα τὰ στοιχεῖα

[6] Ὁ $\tilde{\phi}$ στέλνει τὸ u στὸ v, ἀλλὰ αὐτὸ δὲν μᾶς ἐνδιαφέρει ἐδῶ.

τοῦ K – εἶναι, ὅπως λέμε, *K-ἰσομορφισμός*. Ἔτσι, σὲ συνδυασμὸ καὶ μὲ τὸ Θεώρημα 1.4.2 ἔχομε τὸ ἑξῆς:

Θεώρημα 1.4.5. *Κάθε μὴ σταθερὸ πολυώνυμο μὲ συντελεστὲς ἀπὸ ἕνα σῶμα K ἔχει σῶμα ριζῶν πάνω ἀπὸ τὸ K. Δύο σώματα ριζῶν τοῦ ἴδιου πολυωνύμου, πάνω ἀπὸ τὸ ἴδιο σῶμα K, εἶναι K-ἰσόμορφα μεταξὺ τους. Ὑπάρχει δηλαδὴ ἕνας ἰσομορφισμὸς ἀπὸ τὸ ἕνα στὸ ἄλλο, ὁ ὁποῖος ἀφήνει τὰ στοιχεῖα τοῦ K ἀναλλοίωτα.*

Ὑπ' αὐτὴ τὴν ἔννοια, τὸ σῶμα ριζῶν ἑνὸς πολυωνύμου εἶναι μοναδικό, γι' αὐτὸ καὶ λέμε π.χ. “ ἔστω L τὸ σῶμα ριζῶν τοῦ πολυωνύμου $f(X) \in K[X]$” καὶ ὄχι “ ἔστω L (ἕνα ἢ κάποιο) σῶμα ριζῶν τοῦ πολυωνύμου $f(X) \in K[X]$”.

Ἀσκήσεις

1. Ἂν τὸ $f(X) \in \mathbb{Q}[X]$ εἶναι ἀνάγωγο, $d \in \mathbb{Q}$ μὲ $\sqrt{d} \notin \mathbb{Q}$ καὶ $a + b\sqrt{d}, a, b \in \mathbb{Q}$ εἶναι ρίζα τοῦ $f(X)$, δεῖξτε ὅτι καὶ $a - b\sqrt{d}$ εἶναι ρίζα τοῦ $f(X)$.

2. Στὴν ἄσκηση αὐτὴ χρησιμοποιεῖστε ἐλεύθερα πραματικοὺς καὶ μιγαδικοὺς ἀριθμούς. Ἔστω $\sqrt[3]{2}$ ἡ πραγματικὴ κυβικὴ ρίζα τοῦ 2 καὶ $\omega = (-1 + i\sqrt{3})/2$. Παρατηρῆστε ὅτι $\omega^2 + \omega + 1 = 0$, ἄρα $\omega^3 = 1$. Ἀποδεῖξτε ὅτι τὸ $L = \mathbb{Q}[\sqrt[3]{2}, \omega]$ εἶναι σῶμα ριζῶν τοῦ $X^3 - 2$ πάνω ἀπὸ τὸ $\mathbb{Q}$, ἐνῶ, πάνω ἀπὸ τὸ $\mathbb{R}$, τὸ ἴδιο πολυώνυμο ἔχει σῶμα ριζῶν τὸ $M = \mathbb{R}[\omega]$.

3. Ἔστω $\phi : K \to L$ ἰσομορφισμὸς σωμάτων. Γιὰ κάθε πολυώνυμο $f(X) = a_0 + a_1X + \ldots + a_mX^m \in K[X]$ γράφομε $\phi f(X)$ γιὰ νὰ δηλώσομε τὸ πολυώνυμο $\phi(a_0) + \phi(a_1)X + \ldots + \phi(a_m)X^m \in L[X]$. Δεῖξτε ὅτι ἡ ἀπεικόνιση $K[X] \ni f(X) \mapsto \phi!f(X) \in L[X]$ εἶναι ἰσομορφισμὸς δακτυλίων. Συνεπῶς, ἂν γιὰ τὰ πολυώνυμα $f(X), g(X), h(X)$ τοῦ $K[X]$ ἰσχύει $f(X) = g(X)h(X)$, τότε καὶ $\phi f(X) = \phi g(X)\phi h(X)$. Εἰδικώτερα, ἂν τὸ $f(X)$ εἶναι ἀνάγωγο στὸ $K[X]$, τότε καὶ τὸ $\phi f(X)$ εἶναι ἀνάγωγο στὸ $L[X]$.

4. Δῶστε μὲ λεπτομέρειες τὴν ἀπόδειξη τοῦ ὅτι ἡ ἀπεικόνιση $\tilde{\sigma}$ στὴν ἀπόδειξη τοῦ θεωρήματος 1.4.3 ἱκανοποιεῖ τὶς ἀπαιτήσεις τοῦ θεωρήματος. Ποῦ ἔπαιξε ρόλο ὅτι τὸ $p(X)$ εἶναι ἀνάγωγο;

5. Ἔστω L σῶμα ριζῶν τοῦ πολυωνύμου $f(X) \in K[X]$. Ἂν M εἶναι ἐνδιάμεση μεταξὺ τῶν K καὶ L ἐπέκταση (δηλαδή, ἔχομε τὶς διαδοχικὲς ἐπεκτάσεις $L/M/K$), καὶ θεωρήσομε τὸ $f(X)$ ὡς πολυώνυμο τοῦ $M[X]$, πάλι τὸ L εἶναι σῶμα ριζῶν του.

6. Ἔστω $K = \mathbb{Z}_5$ τὸ σῶμα τῶν κλάσεων ὑπολοίπων mod 5. Ἀποδεῖξτε ὅτι τὸ $f(X) = X^2 - 2 \in K[X]$ εἶναι ἀνάγωγο. Ἀπὸ τὴ Θεωρία ξέρομε ὅτι ὑπάρχει τὸ σῶμα ριζῶν, ἔστω L, αὐτοῦ τοῦ πολυωνύμου. Ἔστω $\theta \in L$ μία ρίζα τοῦ $f(X)$. Ἀποδεῖξτε ὅτι $L = K[\theta]$ καὶ καταγράψτε ὅλα τὰ στοιχεῖα τοῦ L (εἶναι 25 συνολικά). Ἐκτελέστε τὶς ἑξῆς πράξεις στὸ L:

$$(3 + 4\theta) + (2 + 2\theta), \quad (3 + 2\theta)(2 + \theta), \quad (2 + \theta)^3, \quad (1 + 2\theta)^{-1}\ .$$

7. Ἔστω τὸ $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$ καὶ L τὸ σῶμα ριζῶν του. Ἔστω $\rho \in L$ μία ρίζα τοῦ $f(X)$. Ποιὰ εἶναι ἡ γενικὴ μορφὴ τῶν στοιχείων τοῦ σώματος $\mathbb{Q}(\rho)$; Δεῖξτε ὅτι τὸ στοιχεῖο $-2 + \rho^2$ εἶναι, ἐπίσης, ρίζα τοῦ $f(X)$· ποιὰ εἶναι ἡ τρίτη ρίζα; (Θυμηθεῖτε

τοὺς τύπους τοῦ Viète γιὰ τὶς σχέσεις ριζῶν καὶ συντελεστῶν.) Συμπεράνατε ὅτι $L = \mathbb{Q}(\rho)$ καὶ $[L : Q] = 3$. Ἐκτελέστε τὶς ἑξῆς πράξεις:

$$(2 - 3\rho + 4\rho^2)(7 + 11\rho + 5\rho^2), \quad (-1 + 2\rho + 3\rho^2)^2, \quad (2 + \rho^2)^{-1} .$$

8. Ἔστω τὸ $f(X) = X^3 + X + 1 \in \mathbb{Q}[X]$. Ἀποδεῖξτε ὅτι εἶναι ἀνάγωγο καὶ ἔχει ἀκριβῶς μία πραγματικὴ ρίζα. Ἔστω ὅτι $\rho_1, \rho_2, \rho_3 \in \mathbb{C}$, $\rho_1 \in \mathbb{R}$ εἶναι οἱ ρίζες τοῦ $f(X)$. Δεῖξτε ὅτι τὸ $\mathbb{Q}[\rho_1, \rho_2]$ εἶναι σῶμα ριζῶν τοῦ $f(X)$ καὶ $[\mathbb{Q}[\rho_1, \rho_2] : \mathbb{Q}] = 6$. Συμπεράνατε ὅτι ἂν L εἶναι ἕνα *ὁποιοδήποτε* σῶμα ριζῶν τοῦ $f(X) \in \mathbb{Q}[X]$, τότε $[L : Q] = 6$. Βλέπετε τὴν ἀντίθεση μὲ τὸ παράδειγμα τῆς προηγούμενης ἀσκήσεως; Ἔστω τώρα ὅτι ρ καὶ θ εἶναι δύο διαφορετικὲς ρίζες τοῦ $f(X)$, ποὺ ἀνήκουν στὸ L. (Ξεχᾶστε τοὺς μιγαδικοὺς τώρα!) Βρεῖτε ἕνα δευτεροβάθμιο πολυώνυμο τοῦ $\mathbb{Q}(\rho)[X]$, τὸ ὁποῖο νὰ ἔχει ρίζα τὸ θ. Βρεῖτε μία βάση τῆς ἐπέκτασης $L/\mathbb{Q}$ συναρτήσει τῶν ρ, θ. Ἐκφράστε τὸ στοιχεῖο $(-1 + 2\rho + \rho^2 - \theta)^2$ συναρτήσει τῆς βάσεως ποὺ βρήκατε.

9. *Ὁρισμοί.* (1) Δύο στοιχεῖα μιᾶς ἐπεκτάσεως L τοῦ σώματος K, ἀλγεβρικὰ πάνω ἀπὸ τὸ K, λέγονται *συζυγῆ πάνω ἀπὸ τὸ K* ἤ, ἁπλῶς, *K-συζυγῆ*, ἂν εἶναι ρίζες τοῦ ἴδιου *ἀναγώγου* πολυωνύμου μὲ συντελεστὲς ἀπὸ τὸ K. (2) Ἂν τὸ λ εἶναι ἕνα στοιχεῖο μιᾶς ἐπέκτασης τοῦ K, ἀλγεβρικὸ πάνω ἀπὸ τὸ K, καὶ θεωρήσομε τὸ ἐλάχιστο πολυώνυμό του $p(X)$ (πάνω ἀπὸ τὸ K), τότε οἱ ρίζες αὐτοῦ τοῦ πολυωνύμου (οἱ ὁποῖες ἀνήκουν, βέβαια, στὸ σῶμα ριζῶν τοῦ $p(X)$) εἶναι, ἐξ ὁρισμοῦ, *οἱ ἀλγεβρικοὶ συζυγεῖς τοῦ λ πάνω ἀπὸ τὸ K* ἤ, μὲ ἁπλούστερη διατύπωση, οἱ *K-ἀλγεβρικοὶ συζυγεῖς τοῦ λ*.
Ἀποδεῖξτε τὰ ἑξῆς: ἔστω ὅτι ἔχομε τὶς διαδοχικὲς ἐπεκτάσεις $L/M/K$, τὸ $\lambda \in L$ εἶναι ἀλγεβρικὸ πάνω ἀπὸ τὸ K, καὶ τὸ ἐλάχιστο πολυώνυμό του πάνω ἀπὸ τὸ K εἶναι τὸ $q(X)$. Τότε, τὸ λ εἶναι ἀλγεβρικὸ καὶ πάνω ἀπὸ τὸ M (τετριμμένο), ὁπότε ἔστω $p(X)$ τὸ ἐλάχιστο πολυώνυμο τοῦ λ πάνω ἀπὸ τὸ M. Βλέποντας καὶ τὸ $q(X)$ ὡς πολυώνυμο τοῦ $M[X]$, ἀποδεῖξτε ὅτι τὸ $p(X)$ διαιρεῖ τὸ $q(X)$. Δεῖξτε ἐπίσης ὅτι, ἂν τὸ $\mu \in M$ εἶναι ἀλγεβρικὸ συζυγὲς τοῦ λ πάνω ἀπὸ τὸ M, τότε εἶναι ἀλγεβρικὸ συζυγὲς τοῦ λ καὶ πάνω ἀπὸ τὸ K.

10. Ἔστω ὅτι τὰ στοιχεῖα u, v τῆς ἐπέκτασης L τοῦ σώματος K εἶναι K-συζυγῆ (βλ. ἄσκηση 9). Δεῖξτε ὅτι ὑπάρχει ἕνας K-αὐτομορφισμὸς τοῦ L (δηλαδή, ἕνας αὐτομορφισμὸς τοῦ L, ὁ ὁποῖος ἀφήνει ἀναλλοίωτα ὅλα τὰ στοιχεῖα τοῦ K), ὁ ὁποῖος στέλνει τὸ u στὸ v.

1.5 Σωμα ριζων κυβικου πολυωνυμου

Σ' αὐτὴ τὴν ἑνότητα θὰ ὑποθέσομε ὅτι τὸ σῶμα K ἔχει χαρακτηριστικὴ $\neq 2$, θὰ θεωρήσομε ἕνα ἀνάγωγο $g(X) = X^3 + pX^2 + qX + r \in K[X]$ καὶ θὰ μελετήσομε τὸ σῶμα ριζῶν τοῦ $g(X)$. Στὴν περίπτωση ποὺ $p \neq 0$, θὰ ὑποθέσομε ὅτι ἡ χαρακτηριστικὴ τοῦ K εἶναι $\neq 3$. Αὐτὸ μᾶς ἐπιτρέπει νὰ θεωρήσομε τὸ πολυώνυμο $g(X - p/3)$,[7] ὁπότε θεωροῦμε τὸ ἁπλούστερης μορφῆς πολυώνυμο

$$f(X) = g(X - p/3) = X^3 + aX + b, \qquad a = -3p^2 + q,\ b = 2p^3 - qp + r.$$

Παρατηρῆστε ὅτι ἕνα στοιχεῖο ρ (σὲ κάποια ἐπέκταση τοῦ K) εἶναι ρίζα τοῦ $f(X)$ ἂν καὶ μόνο ἂν τὸ $\rho - p/3$ εἶναι ρίζα τοῦ $g(X)$, ἄρα, πάνω ἀπ' τὸ K, ἕνα σῶμα ριζῶν τοῦ $f(X)$ εἶναι καὶ σῶμα ριζῶν τοῦ $g(X)$. Παρατηρῆστε, ἐπίσης, ὅτι, ἀφοῦ τὸ $f(X)$ ἔχει ὑποτεθεῖ ἀνάγωγο πάνω ἀπὸ τὸ K, τὸ ἴδιο ἰσχύει καὶ γιὰ τὸ $f(X)$. Θὰ ἑστιάσομε, λοιπόν, τὴ μελέτη μας στὸ παραπάνω $f(X)$.

Ἂς δοῦμε πρῶτα τὴν περίπτωση ποὺ $a = 0$ *καὶ* ἡ χαρακτηριστικὴ τοῦ K εἶναι 3. Τότε, ἂν L εἶναι σῶμα ριζῶν τοῦ $f(X)$ καὶ $\rho \in L$ εἶναι μία ρίζα τοῦ $f(X)$, παρατηροῦμε ὅτι $0 = f(\rho) = \rho^3 + b$ ἄρα $b = -\rho^3$ καὶ $f(X) = X^3 + b = X^3 - \rho^3 = (X - \rho)^3$.[8] Ἄρα, σ' αὐτὴ τὴν περίπτωση τὸ $f(X)$ ἔχει μία μόνο ρίζα, ἔστω ρ, καὶ τὸ σῶμα ριζῶν τοῦ $f(X)$ πάνω ἀπ' τὸ K εἶναι $L = K[\rho]$. Αὐτὴ ἡ περίπτωση, λοιπόν, δὲν ἔχει κάποια δυσκολία ἢ οὐσιαστικὸ ἐνδιαφέρον.

> Στὸ ἑξῆς, θὰ ὑποθέτομε ὅτι, ἡ χαρακτηριστικὴ τοῦ K εἶναι $\neq 2$ καί, στὴν περίπτωση ποὺ $a = 0$, θὰ κάνομε καὶ τὴν *ἐπιπλέον* ὑπόθεση ὅτι ἡ χαρακτηριστικὴ τοῦ K εἶναι $\neq 3$.

Ἔστω $L = K[\rho, \rho', \rho'']$ σῶμα ριζῶν τοῦ $f(X)$, ὅπου $f(X) = (X - \rho)(X - \rho')(X - \rho')'$. Ἂς παρατηρήσομε πρῶτα ὅτι $3\rho^2 + a \neq 0$, κάτι ποὺ θὰ μᾶς χρειαστεῖ παρακάτω. Πράγματι, ἂν ἦταν $3\rho^2 + a = 0$, αὐτὸ θὰ σήμαινε ὅτι τὸ ρ εἶναι καὶ ρίζα τοῦ $3X^2 + a$, ὁπότε, ἀπ' τὴν Πρόταση Α΄.4 (2), $f(X)|(3X^2 + a)$. Ἀλλὰ τὸ $f(X)$ εἶναι βαθμοῦ 3, ἄρα ἡ τελευταία σχέση εἶναι δυνατὴ μόνο ἂν τὸ $3X^2 + a$ εἶναι τὸ μηδενικὸ πολυώνυμο. Αὐτὸ μπορεῖ νὰ συμβεῖ μόνον ὅταν ἡ χαρακτηριστικὴ τοῦ K εἶναι 3 καὶ τὸ $a = 0$, περίπτωση ποὺ ἤδη ἀποκλείσαμε. Συνεχίζομε δείχνοντας ὅτι οἱ ρίζες ρ, ρ', ρ'' εἶναι διαφορετικές. Πράγματι, ἔστω ὅτι $\rho = \rho'$. Τότε, λόγῳ τῶν τύπων τοῦ Viète, $\rho'' = -\rho - \rho' = -2\rho$, ἄρα $X^3 + aX + b = (X - \rho)(X - \rho')(X - \rho'') = (X - \rho)^2(X + 2\rho)$, ἀπ' ὅπου παίρνομε $a = -3\rho^2$, ἄρα $3\rho^2 + a = 0$, σχέση ποὺ ἀποκλείσαμε λίγο παραπάνω.

Θεωροῦμε τώρα τὴν ποσότητα

$$\delta = (\rho - \rho')(\rho - \rho'')(\rho' - \rho'') \ .$$

Θεωροῦμε, ἐπίσης, τὶς σχέσεις $f(\rho) = 0$ καὶ $f(\rho') = 0$. Ἀφαιρώντας τις κατά μέλη καὶ διαιρώντας μετὰ διὰ $\rho - \rho' \neq 0$, παίρνομε τὴ σχέση

$$\rho^2 + \rho\rho' + \rho'^2 = -a \ . \tag{1.5}$$

[7] Ὅταν γράφομε, στὴν Ἄλγεβρα, $p/3$, ὅπου p εἶναι στοιχεῖο ἑνὸς σώματος K, ἐννοοῦμε $p \cdot (3 \cdot 1_K)^{-1}$, ὅπου 1_K εἶναι τὸ μοναδιαῖο στοιχεῖο τοῦ K. Αὐτὸ τὸ στοιχεῖο ἔχει νόημα, ἐφ' ὅσον τὸ $3 \cdot 1_K$ εἶναι μὴ μηδενικό, κάτι ποὺ ἰσχύει ὅταν ἡ χαρακτηριστικὴ τοῦ K δὲν εἶναι 3.

[8] Στὴν τελευταία ἰσότητα παίζει ρόλο τὸ ὅτι ἡ χαρακτηριστικὴ τοῦ K εἶναι 3.

Ἀπὸ τὴν τελευταία καὶ τὴν $-\rho'' = \rho + \rho'$ ἔχομε:

$$\begin{aligned}
\delta &= (\rho - \rho')(2\rho + \rho')(\rho + 2\rho') \\
&= (\rho - \rho')(2\rho^2 + 5\rho\rho' + 2\rho'^2) = (\rho - \rho')[3\rho\rho' + 2(\rho^2 + \rho\rho' + \rho'^2)] \\
&\overset{(1.5)}{=} (\rho - \rho')(3\rho\rho' - 2a) = -3\rho\rho'^2 + (3\rho^2 + 2a)\rho' - 2a\rho \\
&= 3\rho(-\rho'^2) + (3\rho^2 + 2a)\rho' - 2a\rho \\
&\overset{(1.5)}{=} 3\rho(\rho^2 + \rho\rho' + a) + (3\rho^2 + 2a)\rho' - 2a\rho \\
&= (6\rho^2 + 2a)\rho' + (3\rho^3 + a\rho) = (6\rho^2 + 2a)\rho' + 3(-a\rho - b) + a\rho \\
&= -2a\rho - 3b + (6\rho^2 + 2a)\rho' .
\end{aligned}$$

Ὁ συντελεστὴς $2(3\rho^2 + a)$ τοῦ ρ' στὴν τελευταία ἰσότητα εἶναι $\neq 0$, ἐπειδὴ ἔχομε ὑποθέσει ὅτι ἡ χαρακτηριστικὴ τοῦ K εἶναι $\neq 2$ καί, ἐπίσης, ἔχομε ἀποδείξει ὅτι $3\rho^2 + a \neq 0$. Συνεπῶς,

$$\rho' = \frac{\delta + 2a\rho + 3b}{2a + 6\rho^2} ,$$

ἀπ' ὅπου γίνεται φανερὸ ὅτι $\rho', \rho'' \in K(\rho, \delta)$ καὶ, συνεπῶς, τὸ σῶμα ριζῶν τοῦ $f(X)$ πάνω ἀπ' τὸ K εἶναι τὸ $K(\rho, \delta)$. Ποιὰ εἶναι ὅμως ἡ χρησιμότητα αὐτοῦ τοῦ συμπεράσματος; Γιατὶ νὰ μὴν ποῦμε ἁπλῶς ὅτι τὸ σῶμα ριζῶν εἶναι τὸ $K(\rho, \rho', \rho'') = K(\rho, \rho')$; Τὸ παραπάνω συμπέρασμά μας δὲν θὰ εἶχε καμμία σημασία ἂν, ὅπως θὰ δοῦμε ἀμέσως παρακάτω, τὸ δ δὲν εἶχε τὴν ὡραία ἰδιότητα νὰ εἶναι τεραγωνικὴ ρίζα ἑνὸς στοιχείου τοῦ K.

Θεώρημα 1.5.1. *Ἔστω K σῶμα χαρακτηριστικῆς διάφορης τοῦ 2 καὶ τὸ ἀνάγωγο $f(X) = X^3 + aX + b \in K[X]$. Στὴν περίπτωση ποὺ $a = 0$ ὑποθέτομε ὅτι ἡ χαρακτηριστικὴ τοῦ σώματος K δὲν εἶναι οὔτε 3. Συμβολίζομε μὲ L τὸ σῶμα ριζῶν τοῦ $f(X)$ πάνω ἀπὸ τὸ K καὶ μὲ $\rho, \rho', \rho'' \in L$ τὶς ρίζες τοῦ $f(X)$ καὶ θέτομε*

$$\delta = (\rho - \rho')(\rho - \rho'')(\rho' - \rho'') .$$

Τότε, οἱ ρίζες ρ, ρ', ρ'' εἶναι διαφορετικές, $L = K(\rho, \delta)$ καὶ

$$\begin{aligned}
\rho' &= \frac{\delta + 2a\rho + 3b}{2a + 6\rho^2} = \frac{-4a^2 + (9b - \delta)\rho - 6a\rho^2}{2\delta} \\
\rho'' &= \frac{-\delta + 2a\rho + 3b}{2a + 6\rho^2} = \frac{4a^2 - (9b + \delta)\rho + 6a\rho^2}{2\delta} \\
\delta^2 &= -4a^3 - 27b^2 \neq 0 .
\end{aligned}$$

Ἀπόδειξη. Ἔχομε ἤδη ἀποδείξει ὅτι οἱ ρίζες ρ, ρ', ρ'' εἶναι διαφορετικές, καθὼς καὶ τὴν ἔκφραση γιὰ τὸ ρ'. Ἀπὸ τὴν ἔκφραση αὐτὴ τοῦ ρ' προκύπτει ἀμέσως ἡ ἀντίστοιχη ἔκφραση τοῦ ρ'', ἀρκεῖ νὰ ἐναλλάξομε τὰ ρ' καὶ ρ'' καὶ νὰ παρατηρήσομε ὅτι ἡ ἐναλλαγὴ αὐτὴ μετατρέπει τὸ δ στὸ $-\delta$.

Ἀπὸ τὶς ἐκφράσεις αὐτὲς τῶν ρ' καὶ ρ'' ἔχομε (λόγῳ καὶ τῆς $\rho\rho'\rho'' = -b$),

$$\frac{(2a\rho + 3b)^2 - \delta^2}{(2a + 6\rho^2)^2} = \rho'\rho'' = -\frac{b}{\rho} = \rho^2 + a .$$

Λύνοντας ὡς πρὸς δ^2, παίρνομε ὕστερα ἀπὸ ἁπλὲς πράξεις (λαμβάνοντας ὑπ' ὄψιν τὴ σχέση $\rho^3 = -a\rho - b$) τὴν τρίτη ἀπὸ τὶς ἀποδεικτέες σχέσεις. Ἡ σχέση $\delta^2 \neq 0$, φυσικά, προκύπτει ἀπὸ τὸ ὅτι οἱ ρίζες ρ, ρ', ρ'' εἶναι διαφορετικές. Γιὰ ἕνα διαφορετικὸ τρόπο ἀπόδειξης τοῦ τύπου $\delta^2 = -4a^3 - 27b^2$ δεῖτε τὴν ἄσκηση 5. □

Ἀσκήσεις

1. Ἀποδεῖξτε ὅτι (μὲ τοὺς συμβολισμοὺς αὐτῆς τῆς ἑνότητας) τὸ σῶμα ριζῶν τοῦ $f(X)$ ὅταν τὸ $-4a^3 - 27b^2$ δὲν εἶναι τέλειο τετράγωνο τοῦ K, εἶναι ἕκτου βαθμοῦ πάνω ἀπ' τὸ K· διαφορετικά, εἶναι τρίτου βαθμοῦ.

   Ὑπόδειξη. Ἔστω $D = -4a^3 - 27b^2$. Δεῖξτε ὅτι τὸ $X^3 - D$ εἶναι ἀνάγωγο, ὄχι μόνο πάνω ἀπ' τὸ K, ἀλλὰ καὶ πάνω ἀπ' τὸ $K[\rho]$.

2. Ἔστω τὸ $f(X) = X^3 + aX + b \in K[X]$. Δὲν κάνομε καμμία ὑπόθεση γιὰ τὸ ἂν τὸ $f(X)$ εἶναι ἢ ὄχι ἀνάγωγο, οὔτε θέτομε κανένα περιορισμὸ στὴ χαρακτηριστικὴ τοῦ K. Παρατηρῆστε ὅτι, καὶ πάλι, οἱ σχέσεις τοῦ Θεωρήματος 1.5.1 ἰσχύουν. Ἡ ποσότητα $\Delta = -4a^3 - 27b^2$ λέγεται *διακρίνουσα* τοῦ $f(X)$. Ἀποδεῖξτε τὰ ἑξῆς: (α) Τὸ $f(X)$ ἔχει πολλαπλῆ ρίζα ἂν καὶ μόνο ἂν $\Delta = 0$. (β) Ἂν τὸ K εἶναι ὑπόσωμα τοῦ $\mathbb{R}$ καὶ $\Delta > 0$, τότε οἱ τρεῖς ρίζες τοῦ $f(X)$ εἶναι πραγματικές, ἐνῶ ἂν $\Delta < 0$, μία ἀκριβῶς ρίζα εἶναι πραγματική.

3. Ἂν ρ εἶναι μία ρίζα τοῦ $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$, ὑπολογῖστε, μὲ βάση τὰ ἐκτεθέντα στὴν προηγηθεῖσα ἑνότητα, τὶς δύο ἄλλες ρίζες τοῦ $f(X)$ ὡς πολυωνυμικὲς ἐκφράσεις τοῦ ρ (πρβλ. ἄσκηση 7 τῆς ἑνότητας 1.4). Ὅμοιο ζήτημα γιὰ τὸ $X^3 - 7X + 7$.

4. Ἂν ρ εἶναι μία ρίζα τοῦ $X^3 - 6X + 2 \in \mathbb{Q}[X]$, ἐκφράστε τὶς ἄλλες δύο ρίζες ὡς πολυωνυμικὲς ἐκφράσεις τοῦ ρ καὶ μιᾶς τετραγωνικῆς ρίζας ρητοῦ ἀριθμοῦ. Ἂν ξέρετε ὅτι μία προσεγγιστικὴ τιμὴ γιὰ τὸ ρ εἶναι -2.60167913, ὑπολογῖστε προσεγγιστικὲς τιμὲς γιὰ τὶς ἄλλες δύο ρίζες. Ὅμοιο ζήτημα γιὰ τὸ $X^3 + 3X + 5$, τοῦ ὁποίου μία ρίζα ἔχει τὴν προσεγγιστικὴ τιμὴ -1.15417149.

5. *Ὑπολογισμὸς τῆς διακρίνουσας κυβικοῦ πολυωνύμου.* Ἔστω $f(X) = X^3 + aX + b \in K[X]$ (K σῶμα) καὶ $f(X) = (X - \rho)(X - \rho')(X - \rho'')$, σὲ κάποια ἐπέκταση τοῦ K (παρατηρῆστε ὅτι δὲν γίνεται καμμιὰ ὑπόθεση γιὰ τὸ ἂν οἱ ρίζες ρ, ρ', ρ'', εἶναι διαφορετικές). Ἀποδεῖξτε ὅτι

$$D = (\rho - \rho')^2(\rho - \rho'')^2(\rho' - \rho'')^2 = -4a^3 - 27b^2.$$

   Ὑπόδειξη. Χρησιμοποιῆστε τοὺς τύπους τοῦ Viète $\rho + \rho' + \rho'' = 0$ καὶ $\rho\rho'\rho'' = -b$. Παρατηρῆστε ὅτι $(\rho - \rho')^2 = (\rho + \rho')^2 - 4\rho\rho' = \rho''^2 + 4b/\rho'' = (\rho''^3 + 4b)/\rho'' = (-a\rho'' + 3b)/\rho''$. Κάνετε τὸ ἀνάλογο καὶ γιὰ τοὺς ὑπόλοιπους δύο παράγοντες τοῦ D, ὁπότε $D = (3b - a\rho'')(3b - a\rho')(3b - a\rho)/(\rho''\rho'\rho)$. Ἂν $a = 0$, βλέπομε ἀμέσως ὅτι $D = -27b^2$. Ἂν $a \neq 0$, τότε παρατηρῆστε ὅτι $(3b - a\rho'')(3b - a\rho')(3b - a\rho) = a^3(3b/a - \rho'')(3b/a - \rho')(3b/a - \rho) = f(3b/a)$ κλπ.

1.6 Τὸ Θεμελιῶδες Θεώρημα τῆς Ἄλγεβρας

Τὸ γεγονὸς ὅτι, δοθέντος ἑνὸς ὁποιουδήποτε μὴ σταθεροῦ πολυωνύμου μὲ συντελεστὲς ἀπὸ ἕνα τυχὸν σῶμα K, ὑπάρχει ἕνα σῶμα 'πλουσιώτερο' (ἐν γένει) ἀπὸ τὸ K, ἐντὸς τοῦ ὁποίου μποροῦμε νὰ μιλοῦμε γιὰ τὶς ρίζες τοῦ θεωρουμένου πολυωνύμου (βλ. Θεώρημα 1.4.5), παίζει βασικό – ἂν καὶ μᾶλλον ἀφανῆ – ρόλο, στὴν ἀπόδειξη τοῦ Θεμελιώδους Θεωρήματος τῆς Ἄλγεβρας:

Κάθε μὴ σταθερὸ πολυώνυμο μὲ μιγαδικοὺς συντελεστὲς ἔχει μιγαδικὴ ρίζα.

Ὁρισμένες προκαταρκτικὲς γνώσεις (πολὺ χρήσιμες καὶ σὲ ἀρκετὲς ἄλλες περιπτώσεις) εἶναι ἀπαραίτητες πρῶτα. Ἔστω δακτύλιος R. Τὸ πολυώνυμο (πολλῶν μεταβλητῶν) $f(X_1,\ldots,X_n) \in R[X_1,\ldots,X_n]$ λέγεται *συμμετρικό*, ἂν κάθε μετάθεση τῶν $X_1,\ldots,X_n$ τὸ ἀφήνει ἀναλλοίωτο. Τὰ λεγόμενα *στοιχειώδη συμμετρικὰ πολυώνυμα τῶν* $X_1,\ldots,X_n$ εἶναι τὰ πολυώνυμα

$$S_1 = \sum_{i=1}^{n} X_i\ ,\quad S_2 = \sum_{1\le i<j\le n} X_iX_j\ ,$$

$$S_3 = \sum_{1\le i<j<k\le n} X_iX_jX_k\ ,\ \ldots,\ S_n = X_1X_2\cdots X_n\ .$$

Ἔστω τώρα ὅτι τὰ $u_1,\ldots,u_n$ εἶναι στοιχεῖα κάποιου δακτυλίου, τοῦ ὁποίου ὁ R εἶναι ὑποδακτύλιος (π.χ. τὰ u_i θὰ μποροῦσε νὰ ἦταν οἱ μεταβλητὲς $X_1,\ldots,X_n$). Λέγοντας ὅτι τὸ στοιχεῖο u τοῦ δακτυλίου $R[u_1,\ldots,u_n]$ εἶναι συμμετρικὴ παράσταση τῶν $u_1,\ldots,u_n$, ἐννοοῦμε ὅτι, ὅταν ἐκφράσομε τὸ u ὡς $f(u_1,\ldots,u_n)$, γιὰ κάποιο κατάλληλο πολυώνυμο $f(X_1,\ldots,X_n) \in R[X_1,\ldots,X_n]$, τὸ πολυώνυμο αὐτὸ εἶναι συμμετρικό. Ἐπίσης, λέγοντας στοιχειώδεις συμμετρικὲς παραστάσεις τῶν $u_1,\ldots,u_n$, ἐννοοῦμε τὰ στοιχεῖα $S_1(u_1,\ldots,u_n), S_2(u_1,\ldots,u_n),\ldots,S_n(u_1,\ldots,u_n)$. Ἕνα πολὺ σημαντικὸ θεώρημα, τοῦ ὁποίου μία κάπως ἀκριβέστερη μορφὴ ἀποδεικνύεται στὸ Παράρτημα Γ΄ (βλ. Θεώρημα Γ΄.1), εἶναι τὸ ἑξῆς:

Θεώρημα 1.6.1. *(Θεμελιῶδες Θεώρημα τῶν συμμετρικῶν πολυωνύμων). Ἂν τὸ* $u \in R[u_1,\ldots,u_n]$ *εἶναι συμμετρικὴ παράσταση τῶν* $u_1,\ldots,u_n$*, τότε* $u \in R[v_1,\ldots,v_n]$*, ὅπου* $v_1,\ldots,v_n$ *εἶναι οἱ στοιχειώδεις συμμετρικὲς παραστάσεις τῶν* $u_1,\ldots,u_n$.

Συχνά, τὸ θεώρημα αὐτὸ διατυπώνεται καὶ ὡς ἑξῆς: *Ἂν τὸ* $f \in R[X_1,\ldots,X_n]$ *εἶναι συμμετρικό, τότε μπορεῖ νὰ ἐκφραστεῖ καὶ ὡς πολυώνυμο τῶν* $S_1,\ldots,S_n$ *μὲ συντελεστὲς ἀπὸ τὸ* R.

Παράδειγμα στὶς δύο μεταβλητές: $f = X_1^2 + X_2^2$, προφανῶς συμμετρικό. Ἐδῶ $S_1 = X_1 + X_2, S_2 = X_1X_2$ καὶ $f = S_1^2 - 2S_2$.

Παράδειγμα στὶς τρεῖς μεταβλητές: $f = X_1^3 + X_2^3 + X_3^3$. Εἶναι $S_1 = X_1 + X_2 + X_3, S_2 = X_1X_2+X_1X_3+X_2X_3, S_3 = X_1X_2X_3$ καὶ εὔκολα βρίσκεται ἀπὸ τὴν ἀνάπτυξη τοῦ $(X_1+X_2+X_3)^3$ ὅτι $f = S_1^3 - 3S_1S_2 - 3S_3$.

Ἡ διαδικασία γιὰ νὰ ἐκφράσει κανεὶς ἕνα συμμετρικὸ πολυώνυμο ὡς πολυώνυμο τῶν στοιχειωδῶν συμμετρικῶν παραστάσεων τῶν μεταβλητῶν του, ἂν καὶ ἀλγοριθμική, εἶναι, μερικὲς φορές, κοπιαστική. Ἂς ἔλθομε τώρα στὸ βασικὸ θέμα αὐτῆς τῆς ἑνότητας.

Θεώρημα 1.6.2. *(Θεμελιῶδες Θεώρημα τῆς Ἄλγεβρας). Κάθε μὴ σταθερὸ πολυώνυμο τοῦ* $\mathbb{C}[X]$ *ἔχει μία, τοὐλάχιστον, μιγαδικὴ ρίζα.*

Ἀπόδειξη. Ἔστω μὴ σταθερὸ $f(X) \in \mathbb{C}[X]$. Μὲ $\overline{f}(X)$ συμβολίζομε τὸ πολυώνυμο ποὺ προκύπτει ἂν τοὺς συντελεστὲς τοῦ $f(X)$ ἀντικαταστήσομε ἀπὸ τοὺς μιγαδικοὺς συζυγεῖς τους. Ἀρκεῖ νὰ δείξομε ὅτι τὸ $g(X) = f(X)\overline{f}(X)$ ἔχει ρίζα στὸ $\mathbb{C}$. Γιατί, ἂν $g(z) = 0$, τότε ἢ $f(z) = 0$, ὁπότε ἔχομε τελειώσει, ἢ $\overline{f}(z) = 0$, ὁπότε, παίρνοντας μιγαδικοὺς συζυγεῖς, $f(\overline{z}) = 0$. Μιὰ δεύτερη παρατήρηση εἶναι ὅτι $g(X) \in \mathbb{R}[X]$, ὅπως φαίνεται ὕστερα ἀπὸ ἁπλὲς πράξεις (ἄσκηση 1).

Μὲ τοὺς παραπάνω συλλογισμοὺς βλέπομε, λοιπόν, ὅτι ἀρκεῖ ν' ἀποδείξομε τὴν ὕπαρξη μιγαδικῆς ρίζας γιὰ κάθε μὴ σταθερὸ πολυώνυμο μὲ *πραγματικοὺς συντελεστές*. Ἔστω μὴ σταθερὸ $g(X) \in \mathbb{R}[X]$. Ὁ βαθμὸς τοῦ $g(X)$ μπορεῖ νὰ γραφεῖ $\deg g = 2^n m$, ὅπου m περιττὸς καὶ $n \geq 0$. Ἡ ἀπόδειξη θὰ γίνει ἐπαγωγικὰ ἐπὶ τοῦ n. Ἂν $n = 0$ τὸ $g(X)$ εἶναι περιττοῦ βαθμοῦ καὶ ὁ στοιχειώδης Ἀπειροστικὸς Λογισμὸς μᾶς λέει ὅτι τὸ πολυώνυμό μας ἔχει ρίζα καί, μάλιστα, πραγματική [9]. Ἔστω τώρα ὅτι ὁ l εἶναι ἀκέραιος ≥ 1 καὶ ὁ ἰσχυρισμὸς μας ἀληθεύει γιὰ κάθε πολυώνυμο μὲ πραγματικοὺς συντελεστές, τοῦ ὁποίου ὁ βαθμὸς εἶναι τῆς μορφῆς $2^{l-1}\cdot$ περιττός. Θεωροῦμε τώρα $g(X) \in \mathbb{R}[X]$, $\deg g = d = 2^l \cdot$ περιττὸς καὶ ἔστω L τὸ σῶμα ριζῶν τοῦ $g(X)$ πάνω ἀπὸ τὸ $\mathbb{C}$. Χωρὶς βλάβη τῆς γενικότητος, ἂς ὑποθέσομε τὸ $g(X)$ μονικό, ὁπότε $g(X) = (X - u_1)\ldots(X - u_d)$, ὅπου $u_1, \ldots, u_d \in L$ οἱ ρίζες τοῦ $g(X)$ (ὄχι, κατ' ἀνάγκη, διαφορετικές). Γιὰ κάθε πραγματικὸ ἀριθμὸ a σχηματίζομε τὰ ἑξῆς στοιχεῖα τοῦ L:

$$v_{ij} = u_i + u_j + au_iu_j \ , \ 1 \leq i, j \leq d \ ,$$

καθὼς καὶ τὸ πολυώνυμο $h(X) \in \mathbb{L}[X]$, ποὺ τὰ ἔχει ὡς ρίζες,

$$h(X) = \prod_{1 \leq i \leq j \leq d} (X - v_{ij}) \ .$$

Εὔκολα διαπιστώνεται ὅτι $\deg h = d(d+1)/2 = 2^{l-1} \cdot$ περιττός. Θὰ δείξομε ἀκόμη ὅτι τὸ $h(X)$ ἔχει πραγματικοὺς συντελεστές. Πράγματι, κάθε μετάθεση τῶν $u_1, \ldots u_d$ προκαλεῖ, ἁπλῶς, μία μετάθεση στὶς ρίζες τοῦ $h(X)$ (βλ. ἄσκηση 2), ἄρα ἀφήνει ἀναλλοίωτο τὸ $h(X)$, δηλαδή, τοὺς συντελεστές του. Ὅμως, οἱ συντελεστὲς τοῦ $h(X)$ εἶναι, κατὰ προσέγγιση προσήμου, οἱ στοιχειώδεις συμμετρικὲς παραστάσεις τῶν v_{ij} (τῦποι τοῦ Viète), ἄρα εἶναι πολυωνυμικὲς ἐκφράσεις τῶν $u_1, \ldots, u_d$ καί, μόλις τώρα, εἴδαμε ὅτι μένουν ἀναλλοίωτες ἀπὸ τὶς μεταθέσεις τῶν $u_1, \ldots, u_d$. Συνεπῶς (Θεώρημα 1.6.1), οἱ συντελεστὲς τοῦ $h(X)$ εἶναι πολυωνυμικὲς ἐκφράσεις μὲ πραγματικοὺς συντελεστὲς τῶν στοιχειωδῶν συμμετρικῶν παραστάσεων τῶν $u_1, \ldots, u_n$. Αὐτὲς οἱ τελευταῖες, ὅμως, εἶναι, κατὰ προσέγγιση προσήμου, ἴσες μὲ τοὺς συντελεστὲς τοῦ $g(X)$ (πάλι οἱ τῦποι τοῦ Viète), ἄρα εἶναι πραγματικοὶ ἀριθμοί· ἕπεται ὅτι καὶ οἱ συντελεστὲς τοῦ $h(X)$ εἶναι πραγματικοί. Ἐφαρμόζομε τώρα τὴν ἐπαγωγικὴ ὑπόθεση στὸ $h(X)$ καὶ συμπεραίνομε ὅτι μία ἀπὸ τὶς ρίζες του ἀνήκει στὸ $\mathbb{C}$· ἂς τὴ συμβολίσομε μὲ z_a (προφανῶς, ἐξαρτᾶται ἀπὸ τὸ a).

Μέχρι στιγμῆς συμπεράναμε λοιπὸν ὅτι, γιὰ κάθε $a \in \mathbb{R}$, ὑπάρχουν δεῖκτες i_a, j_a μὲ $1 \leq i_a \leq j_a \leq d$, τέτοιοι ὥστε τὸ στοιχεῖο $z_a = v_{i_a j_a} = u_{i_a} + u_{j_a} + au_{i_a}u_{j_a}$ τοῦ L νὰ ἀνήκει, ἐπίσης καὶ στὸ $\mathbb{C}$. Καθὼς τὸ a μπορεῖ νὰ πάρει ἄπειρες τιμές, ἐνῶ οἱ δεῖκτες i_a, j_a μόνο πεπερασμένες, συμπεραίνομε (ἀρχὴ τοῦ περιστερώνα) ὅτι σὲ δύο διαφορετικὰ a, a' ἀντιστοιχοῦν οἱ ἴδιοι δεῖκτες i, j, δηλαδὴ

$$u_i + u_j + au_iu_j \in \mathbb{C} \ , \ u_i + u_j + a'u_iu_j \in \mathbb{C} \ , \ a \neq a' \ .$$

[9] Ἐδῶ εἶναι τὸ μόνο σημεῖο τῆς ἀποδείξεως, στὸ ὁποῖο χρησιμοποιοῦμε κάτι ἀπὸ τὴν Ἀνάλυση.

Ἀπὸ ἐδῶ ἕπεται ἀμέσως ὅτι $u_i + u_j \in \mathbb{C}$ καὶ $u_i u_j \in \mathbb{C}$. Ἀλλὰ τότε (ἄσκηση 4), οἱ ρίζες u_i, u_j τοῦ $g(X)$ ἀνήκουν στὸ $\mathbb{C}$. □

Ἀσκήσεις

1. Ἔστω μὴ σταθερὸ $f(X) \in \mathbb{C}[X]$ καὶ $\overline{f}(X)$ τὸ πολυώνυμο ποὺ προκύπτει ἂν τοὺς συντελεστὲς τοῦ $f(X)$ ἀντικαταστήσομε ἀπὸ τοὺς μιγαδικοὺς συζυγεῖς τους. Ἀποδεῖξτε ὅτι $f(X)\overline{f}(X) \in \mathbb{R}[X]$.

2. Θεωρῆστε τὰ στοιχεῖα v_{ij}, ὅπως ὁρίσθηκαν στὴν ἀπόδειξη τοῦ Θεωρήματος 1.6.2 καὶ τὸ σύνολο V ἐκείνων τῶν v_{ij}, γιὰ τὰ ὁποῖα $i \le j$. Δεῖξτε ὅτι κάθε ἀντιμετάθεση $u_i \leftrightarrow u_j$ προκαλεῖ μία μετάθεση τῶν στοιχείων τοῦ V. Συμπεράνατε ὅτι κάθε μετάθεση τῶν $u_1, \ldots, u_d$ προκαλεῖ μετάθεση τῶν στοιχείων τοῦ V.

3. Ἐστω ὅτι τὸ $g(X)$, ποὺ ἐμφανίζεται στὴν ἀπόδειξη τοῦ Θεωρήματος 1.6.2 εἶναι τὸ $X^2 + pX + q$ καὶ $a = 1$ στὸν ὁρισμὸ τῶν v_{ij}. Σύμφωνα μὲ τὴν ἀπόδειξη (ξανακοιτάξτε την στὸ σημεῖο ποὺ μιλᾶμε γιὰ τοὺς συντελεστὲς τοῦ $h(X)$), τὸ ἀντίστοιχο $h(X)$ εἶναι τρίτου βαθμοῦ καὶ οἱ συντελεστές του εἶναι πολυωνυμικὲς ἐκφράσεις τῶν p, q. Ὑπολογῖστε τους.

4. Ἔστω L ἐπέκταση τοῦ $\mathbb{C}$ καὶ καὶ $\lambda_1, \lambda_2 \in L$, τέτοια ὥστε $\lambda_1 + \lambda_2$ καὶ $\lambda_1\lambda_2$ εἶναι στοιχεῖα τοῦ $\mathbb{C}$. Δεῖξτε ὅτι τότε καὶ $\lambda_1, \lambda_2 \in \mathbb{C}$.

5. Δεῖξτε ὅτι κάθε μὴ σταθερὸ πολυώνυμο μὲ μιγαδικοὺς συντελεστὲς ἔχει *ὅλες* τὶς ρίζες του στὸ $\mathbb{C}$. Συμπεράνατε ὅτι τὸ $\mathbb{C}$ εἶναι *ἀλγεβρικὰ κλειστό*. Ὁ γενικὸς ὁρισμὸς τοῦ ἀλγεβρικὰ κλειστοῦ σώματος εἶναι ὁ ἑξῆς: *Τὸ σῶμα K χαρακτηρίζεται ἀλγεβρικὰ κλειστό, ἂν δὲν ὑπάρχει γνήσια ἀλγεβρικὴ ἐπέκταση τοῦ K.*

Κεφάλαιο 2

Θεωρία Galois

2.1 Βασικες εννοιες και Προτασεις

῾Ορισμὸς 2.1.1. *῎Εστω L/K ἐπέκταση σωμάτων. ῾Ο αὐτομορφισμὸς σ τοῦ L λέγεται K-αὐτομορφισμὸς τοῦ L ἂν $\sigma(u) = u$ γιὰ κάθε $u \in K$.*

Τὴ σύνθεση $L \overset{\sigma_2}{\to} L \overset{\sigma_1}{\to} L$ τῶν αὐτομορφισμῶν σ_1, σ_2 τοῦ L συμβολίζομε μὲ $\sigma_1\sigma_2$.

Θεώρημα - ῾Ορισμὸς 2.1.2. *᾿Αν L/K εἶναι ἐπέκταση σωμάτων, τότε τὸ σύνολο τῶν K-αὐτομορφισμῶν τοῦ L εἶναι ὑποομάδα τῆς ὁμάδας ὅλων τῶν αὐτομορφισμῶν τοῦ L μὲ πράξη τὴ σύνθεση αὐτομορφισμῶν.*
῾Η ὑποομάδα αὐτὴ συμβολίζεται μὲ $\mathcal{G}(L/K)$ καὶ λέγεται ὁμάδα Galois *τῆς L/K. ᾿Αν ἡ L/K εἶναι πεπερασμένη ἐπέκταση, τότε καὶ ἡ ὁμάδα $\mathcal{G}(L/K)$ εἶναι πεπερασμένη. Στὴν περίπτωση ποὺ τὸ L εἶναι τὸ σῶμα ριζῶν κάποιου πολυωνύμου $f(X) \in K[X]$, ἡ ὁμάδα $\mathcal{G}(L/K)$ λέγεται καὶ* ὁμάδα Galois τοῦ πολυωνύμου *$f(X)$ πάνω ἀπὸ τὸ K.*

᾿Απόδειξη. Εἶναι γνωστὸ ἀπὸ τὴ βασικὴ ῎Αλγεβρα ὅτι τὸ σύνολο τῶν αὐτομορφισμῶν ἑνὸς σώματος, μὲ πράξη τὴ σύνθεση ἀπεικονίσεων, ἀποτελεῖ ὁμάδα. Συνεπῶς, ἀρκεῖ νὰ δείξομε ὅτι τὸ $\mathcal{G}(L/K)$ εἶναι μὴ κενό, κλειστὸ ὡς πρὸς τὴν πράξη τῆς ὁμάδος καὶ ἂν $\sigma \in \mathcal{G}(L/K)$, τότε $\sigma^{-1} \in \mathcal{G}(L/K)$. Πράγματι, εἶναι μὴ κενό, διότι ὁ ταυτοτικὸς αὐτομορφισμὸς τοῦ L εἶναι, προφανῶς, K-αὐτομορφισμός, ἐνῶ ἡ κλειστότητα τῆς σύνθεσης εἶναι ἐξ ἴσου προφανής (ἂν οἱ σ_1, σ_2 ἀφήνουν ἀναλλοίωτα τὰ στοιχεῖα τοῦ K, τὸ ἴδιο θὰ συμβαίνει καὶ μὲ τὴ σύνθεσή τους). ῎Εστω τώρα K-αὐτομορφισμὸς σ καὶ $u \in K$, τυχόν. Πρέπει νὰ δείξομε ὅτι $\sigma^{-1}(u) = u$. ῎Εστω $\sigma^{-1}(u) = v$, ὁπότε $\sigma(v) = u$. ῞Ομως, καὶ $\sigma(u) = u$, ἀφοῦ ὁ σ εἶναι K-αὐτομορφισμός. ῎Ετσι, $\sigma(v) = \sigma(u)$, ὁπότε $v = u$.

Πρὶν προχωρήσομε στὴν περίπτωση πεπερασμένης L/K, κάνομε τὴν ἑξῆς παρατήρηση, ἡ ὁποία θὰ χρησιμοποιεῖται στὸ ἑξῆς πάρα πολλὲς φορές: ῎Εστω ὅτι τὸ $u \in L$ εἶναι ρίζα κάποιου $g(X) \in K[X]$ καὶ σ εἶναι ἕνας K-αὐτομορφισμὸς τοῦ L. Τότε τὸ $\sigma(u)$ εἶναι, ἐπίσης, ρίζα τοῦ $g(X)$. Διότι, ἂν $g(X) = a_dX^d + \cdots + a_1X + a_0$ καὶ ἐφαρμόσομε τὸν σ στὰ δύο μέλη τῆς σχέσεως $0 = a_du^d + \cdots + a_1u + a_0$ τότε, λόγῳ τοῦ ὅτι ὁ σ ἀφήνει ἀναλλοίωτα ὅλα τὰ a_i, καθὼς καὶ τὸ 0, θὰ πάρομε $0 = a_d\sigma(u)^d + \cdots + a_1\sigma(u) + a_0$.

῎Ας ὑποθέσομε τώρα ὅτι ἡ L/K εἶναι πεπερασμένη καὶ $u_1, \ldots, u_m$ εἶναι μία βάση της. Τὸ τυπικὸ στοιχεῖο v τοῦ L ἔχει τὴ μορφὴ $v = a_1u_1 + \cdots + a_mu_m$, ὁπότε, ἂν σ εἶναι ἕνας K-αὐτομορφισμὸς τοῦ L, $\sigma(v) = a_1\sigma(u_1) + \cdots + a_m\sigma(u_m)$. Συνεπῶς, ὁ σ καθορίζεται πλήρως ἀπὸ τὶς τιμές του στὰ στοιχεῖα u_i τῆς βάσεως. ῞Ομως, γιὰ κάθε i, οἱ πιθανὲς τιμὲς τοῦ $\sigma(u_i)$ εἶναι, τὸ πολύ, ὅσες καὶ οἱ ρίζες τοῦ ἐλαχίστου πολυωνύμου τοῦ u_i πάνω ἀπὸ τὸ K, σύμφωνα μὲ τὴν παραπάνω παρατήρηση. Ἂν λοιπὸν d_i εἶναι ὁ βαθμὸς αὐτοῦ τοῦ πολυωνύμου, τότε τὸ πλῆθος τῶν πιθανῶν τιμῶν τῆς m-άδας $(\sigma(u_1), \ldots, \sigma(u_m))$, ἄρα καὶ ἡ τάξη τῆς $\mathcal{G}(L/K)$, εἶναι, τὸ πολύ, $d_1 \cdots d_m$. □

Προκειμένου νὰ δώσομε κάποια ἐνδιαφέροντα παραδείγματα ὁμάδων Galois, χρειαζόμαστε τὴν παρακάτω πρόταση.

Πρόταση 2.1.3. *Ἔστω K σῶμα, ἀνάγωγο πολυώνυμο $f(X) \in K[X]$ καὶ M τὸ σῶμα ριζῶν του πάνω ἀπὸ τὸ K. Ἔστω καὶ τὸ πολυώνυμο $g(X) \in K[X]$, τὸ ὁποῖο εἶναι ἀνάγωγο πάνω ἀπὸ τὸ M* [1] *καὶ L τὸ σῶμα ριζῶν τοῦ $g(X)$ πάνω ἀπὸ τὸ M. Τότε, γιὰ κάθε ζεῦγος ριζῶν α, α' τοῦ $f(X)$ καὶ κάθε ζεῦγος ριζῶν β, β' τοῦ $g(X)$ ὑπάρχει $\sigma \in \mathcal{G}(L/K)$ τέτοιο ὥστε $\sigma(\alpha) = \alpha'$ καὶ $\sigma(\beta) = \beta'$.*

Ἀπόδειξη. Τὸ Θεώρημα 1.4.3 μᾶς ἐξασφαλίζει ὅτι ὁ ταυτοτικὸς ἰσομορφισμὸς $K \to K$ ἐπεκτείνεται σὲ ἰσομορφισμὸ $\sigma_1 : K(\alpha) \to K(\alpha')$, τέτοιον ὥστε $\sigma_1(\alpha) = \alpha'$. Μέσῳ τοῦ σ_1 τὸ $f(X)$ ἀντιστοιχεῖ στὸν ἑαυτό του. Ἐπίσης, εἶναι φανερὸ ὅτι τὸ σῶμα ριζῶν τοῦ $f(X)$ πάνω ἀπὸ τὸ $K(\alpha)$, καθὼς καὶ πάνω ἀπὸ τὸ $K(\alpha')$, εἶναι τὸ M. Ἄρα τὸ Θεώρημα 1.4.4 μᾶς ἐξασφαλίζει ὅτι ὁ σ_1 ἐπεκτείνεται σὲ αὐτομορφισμὸ $\sigma_2 : M \to M$. Μέσῳ τοῦ σ_2 τὸ $g(X)$ ἀντιστοιχεῖ στὸν ἑαυτό του ἄρα, ἀπὸ τὸ Θεώρημα 1.4.3, ὁ σ_2 ἐπεκτείνεται σὲ ἰσομορφισμὸ $\sigma_3 : M(\beta) \to M(\beta')$, τέτοιον ὥστε $\sigma_3(\beta) = \beta'$. Τέλος, ἐπειδὴ μέσῳ τοῦ σ_3 τὸ $g(X)$ ἀντιστοιχεῖ στὸν ἑαυτό του, ἐνῶ τὸ σῶμα ριζῶν τοῦ $g(X)$ πάνω ἀπὸ τὸ $M(\beta)$, καθὼς καὶ πάνω ἀπὸ τὸ $M(\beta')$, εἶναι τὸ L, ἕπεται ἀπὸ τὸ Θεώρημα 1.4.4 ὅτι ὁ σ_3 ἐπεκτείνεται σὲ ἰσομορφισμὸ $\sigma : L \to L$. Αὐτός, 'κληρονομεῖ' τὶς ἰδιότητες τῶν $\sigma_3, \sigma_2, \sigma_1$, ἄρα ἀφήνει ἀναλλοίωτα τὰ στοιχεῖα τοῦ K καὶ στέλνει τὸ α στὸ α' καὶ τὸ β στὸ β'. □

Παράδειγμα 1. Ἔστω ἡ ἐπέκταση $L/\mathbb{Q}$, ὅπου $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Μὲ τὸ συμβολισμὸ τῆς Προτάσεως 2.1.3, $K = \mathbb{Q}$, $f(X) = X^2 - 2$, $M = \mathbb{Q}(\sqrt{2})$, $g(X) = X^2 - 3$. Τὸ $g(X)$ εἶναι ἀνάγωγο πάνω ἀπὸ τὸ M διότι, ὅπως εὔκολα διαπιστώνεται, δὲν ἔχει ρίζα μέσα στὸ M (δηλαδή, τῆς μορφῆς $a + b\sqrt{2}$ μὲ $a, b \in \mathbb{Q}$). Συνεπῶς, παίρνοντας $\alpha = \sqrt{2}, \alpha' = -\sqrt{2}, \beta = \beta' = \sqrt{3}$, συμπεραίνομε ὅτι ὑπάρχει $\sigma \in \mathcal{G}(L/\mathbb{Q})$, τέτοιος ὥστε $\sigma(\sqrt{2}) = -\sqrt{2}$ καὶ $\sigma(\sqrt{3}) = \sqrt{3}$. Ἐντελῶς ἀνάλογα, παίρνοντας $\alpha = \alpha' = \sqrt{2}, \beta = \sqrt{3}, \beta' = -\sqrt{3}$, συμπεραίνομε ὅτι ὑπάρχει $\tau \in \mathcal{G}(L/\mathbb{Q})$, τέτοιος ὥστε $\tau(\sqrt{2}) = \sqrt{2}$ καὶ $\tau(\sqrt{3}) = -\sqrt{3}$. Τώρα, $\sigma\tau \in \mathcal{G}(L/\mathbb{Q})$ καὶ $\sigma\tau(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma\tau(\sqrt{3}) = \sigma(-\sqrt{3}) = -\sigma(\sqrt{3}) = -\sqrt{3}$. Ἔτσι, μέχρι στιγμῆς ἔχομε βρεῖ τὰ ἑξῆς στοιχεῖα τῆς $\mathcal{G}(L/\mathbb{Q})$: $\mathbf{id}_L, \sigma, \tau, \sigma\tau$, ὅπου $\mathbf{id}_L$ συμβολίζει τὸν ταυτοτικὸ αὐτομορφισμὸ τοῦ L. Ἐπειδὴ μία βάση τῆς $L/\mathbb{Q}$ εἶναι ἡ $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}$, ἕπεται ὅτι κάθε $\sigma \in \mathcal{G}(L/\mathbb{Q})$ καθορίζεται πλήρως ἀπὸ τὴ δράση του ἐπὶ τῶν $\sqrt{2}$ καὶ $\sqrt{3}$. Ἄρα, ἂν ϕ εἶναι τυχὸν στοιχεῖο τῆς $\mathcal{G}(L/\mathbb{Q})$, οἱ μόνες δυνατότητες γιὰ τὸ ζεῦγος τιμῶν $(\phi(\sqrt{2}), \phi(\sqrt{3}))$ εἶναι: $(\sqrt{2}, \sqrt{3}), (-\sqrt{2}, \sqrt{3}), (\sqrt{2}, -\sqrt{3}), (-\sqrt{2}, -\sqrt{3})$. Στὴν πρώτη περίπτωση ὁ ϕ ταυτίζεται μὲ τὸν $\mathbf{id}_L$, στὴ δεύτερη μὲ τὸν σ, στὴν τρίτη μὲ τὸν τ καὶ στὴν τέταρτη μὲ τὸν $\sigma\tau$ (παρατηρῆστε ὅτι $\tau\sigma = \sigma\tau$). Τὸ τελικὸ συμπέρασμα εἶναι ὅτι

$$\mathcal{G}(L/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = \mathbf{id}_L \ , \ \sigma\tau = \tau\sigma \rangle \ ,$$

ἄρα $\mathcal{G}(L/\mathbb{Q}) \cong \mathbf{V}_4$ (" ὁμάδα τῶν 4 τοῦ Klein").

Παράδειγμα 2. Ἔστω K σῶμα χαρακτηριστικῆς διάφορης τοῦ 2 καὶ τὸ ἀνάγωγο πολυώνυμο $f(X) = X^3 + aX + b \in K[X]$. Στὴν περίπτωση ποὺ $a = 0$ ὑποθέτομε, ἐπιπλέον, ὅτι ἡ χαρακτηριστικὴ τοῦ σώματος K δὲν εἶναι οὔτε 3. Ἔστω L τὸ σῶμα ριζῶν τοῦ $f(X)$ πάνω ἀπὸ τὸ K. Σύμφωνα μὲ τὸν συμβολισμὸ τῆς ἑνότητας 1.5 καὶ τὰ συμπεράσματα τοῦ

[1] Εἰδικώτερα, τὸ $g(X)$ εἶναι πρῶτο πρὸς τὸ $f(X)$.

Θεωρήματος 1.5.1 τῆς ἴδιας ἑνότητας, οἱ ρίζες ρ, ρ', ρ'' τοῦ $f(X)$ εἶναι διαφορετικές καὶ $L = K(\rho, \delta) = K(\rho', \delta)$. Ἀπὸ τὸ Θεώρημα 1.4.3 συνάγομε τὴν ὕπαρξη ἰσομορφισμοῦ $\sigma : K(\delta, \rho) \to K(\delta, \rho')$ τέτοιου ὥστε $\sigma(\rho) = \rho'$, ὁ ὁποῖος ἐπεκτείνει τὸν ταυτοτικὸ ἰσομορφισμὸ $K(\delta) \to K(\delta)$,[2], ὁπότε, $\sigma \in \mathcal{G}(L/K)$. Θὰ δοῦμε τώρα ποῦ ἀπεικονίζονται οἱ ρίζες ρ καὶ ρ' μέσῳ τοῦ σ. Ἐπειδὴ $\sigma(\rho) = \rho'$, ἀποκλείεται ἡ σχέση $\sigma(\rho') = \rho'$, ἄρα, $\sigma(\rho') = \rho''$ ἢ ρ.

Θεωροῦμε πρῶτα τὴν περίπτωση $\delta \in K$ καὶ θὰ ἀποκλείσομε τὸ ἐνδεχόμενο $\sigma(\rho') = \rho$. Παρατηροῦμε ὅτι, στὸ Θεώρημα 1.5.1, ἡ ρίζα ρ' ἐκφράζεται ρητῶς συναρτήσει τῆς ρ καὶ τοῦ δ. Ἐναλλάσοντας τὸ ρόλο τῶν ρ, ρ' μποροῦμε νὰ ἔχομε, κατ' ἀναλογίαν μὲ τὸν προηγούμενο τῦπο, τὴ ρητὴ ἔκφραση τοῦ ρ συναρτήσει τῶν ρ' καὶ δ. Ἔτσι, κάνοντας ἐπιπλέον τὴν παρατήρηση ὅτι ἡ ἐναλλαγὴ τῶν ρ, ρ' προκαλεῖ ἀλλαγὴ τοῦ προσήμου τοῦ δ, καταλήγομε στὸν τῦπο

$$\rho = \frac{-\delta + 2a\rho' + 3b}{2a + 6\rho'^2}\ .$$

Ἂν λοιπὸν $\sigma(\rho') = \rho$ τότε, ἐφαρμόζοντας τὸν σ στὸν τῦπο τοῦ Θεωρήματος 1.5.1 ἔχομε

$$\rho = \frac{\delta + 2a\rho' + 3b}{2a + 6\rho'^2}$$

καί, συγκρίνοντας μὲ τὶς δύο τελευταῖες σχέσεις καταλήγομε στὸ ὅτι $\delta = 0$, ἐν ἀντιθέσει μὲ ὅ, τι παρατηρήσαμε ἀρχικά. Κατ' ἀνάγκη λοιπόν, $\sigma(\rho') = \rho''$, ὁπότε $\sigma(\rho'') = \rho$. Ἄρα, ὁ σ μπορεῖ νὰ ταυτισθεῖ μὲ τὴ μετάθεση $(\rho\,\rho'\,\rho')$ καὶ ὁ σ^2, κατὰ συνέπεια, μὲ τὴν $(\rho\,\rho''\,\rho')$· παρατηροῦμε ἀκόμη ὅτι $\sigma^3 = \mathbf{id}_L$. Ἐπίσης, σύμφωνα μὲ ὅ, τι ἀποδείξαμε παραπάνω, ἀποκλείεται ἕνας αὐτομορφισμός, ποὺ στέλνει τὸ δ στὸν ἑαυτό του, νὰ ταυτίζεται μὲ τὴν ἀντιμετάθεση $(\rho\,\rho')$ ἄρα, κατ' ἀναλογίαν, οὔτε καὶ μὲ κάποια ἀπὸ τὶς ἀντιμεταθέσεις $(\rho\,\rho')$ ἢ $(\rho'\,\rho'')$.

Συνεπῶς, ὅταν $\delta \in K$, δηλαδὴ ὅταν ἡ διακρίνουσα$-4a^3 - 27b^2$ τοῦ $f(X)$ (βλ. ἄσκηση 2 τῆς ἑνότητας 1.5 καὶ τελευταία σχέση τοῦ Θεωρήματος 1.5.1) εἶναι τετράγωνο ρητοῦ, ὁπότε κάθε K-αὐτομορφισμὸς τοῦ L στέλνει τὸ δ στὸν ἑαυτό του, τότε ἡ ὁμάδα Galois τοῦ $f(X)$ πάνω ἀπὸ τὸ K παράγεται ἀπ' τὸν αὐτομορφισμὸ σ καὶ εἶναι ἰσόμορφη μὲ τὴν *ἐναλλάσουσα* ὁμάδα $\mathbf{A}_3 = \langle(1\ 2\ 3)\rangle$ (ἀντιστοιχῆστε ἁπλῶς τοὺς ἀριθμοὺς 1, 2, 3 στὶς ρίζες ρ, ρ', ρ'', ὁπότε ὁ $\sigma = (\rho\,\rho'\rho'')$ ταυτίζεται μὲ τὴ μετάθεση (1 2 3)).

Ἔστω τώρα ὅτι $\delta \notin K$. Τότε, τὸ $X^2 - D$ (ὅπου $D = \delta^2 = -4a^3 - 27b^2 \in K$) εἶναι ἀνάγωγο καὶ πάνω ἀπὸ τὸ $K(\rho)$ (γιατί, ἀλλοιῶς, ἡ κυβικὴ ἐπέκταση $K(\rho)$ τοῦ K θὰ περιεῖχε τὴν τετραγωνικὴ ἐπέκταση $K(\delta)$, ποὺ ἀντιβαίνει στὸ Θεώρημα 1.1.4). Ἄρα, ἀπὸ τὸ Θεώρημα 1.4.3, ὁ ταυτοτικὸς αὐτομορφισμὸς $K(\rho) \to K(\rho)$ ἐπεκτείνεται σὲ αὐτομορφισμὸ $\tau : K(\rho, \delta) \to K(\rho, \delta)$, τέτοιον ὥστε $\tau(\delta) = -\delta$ καί, φυσικά, $\tau(\rho) = \rho$. Ἀπὸ τοὺς τύπους τοῦ Θεωρήματος 1.5.1 εἶναι τώρα πολὺ εὔκολο νὰ διαπιστώσομε ὅτι $\tau(\rho') = \rho''$, $\tau(\rho'') = \rho'$, ἄρα μποροῦμε νὰ ταυτίσομε τὸν τ μὲ τὴν ἀντιμετάθεση $(\rho'\rho'')$ ἤ, ἀκόμη καὶ μὲ τὴν ἀντιμετάθεση (2 3). Στὴν περίπτωση, δηλαδή, ποὺ ἐξετάζομε τώρα, ἡ ὁμάδα Galois τοῦ $f(X)$ παράγεται ἀπ' τοὺς αὐτομορφισμοὺς σ καὶ τ, τοὺς ὁποίους μποροῦμε νὰ ταυτίσομε, ἀντιστοίχως, μὲ τὶς μεταθέσεις (1 2 3) καὶ (2 3). Ἄρα, ἡ ὁμάδα Galois τοῦ $f(X)$ εἶναι ἰσόμορφη μὲ τὴ συμμετρικὴ ὁμάδα $\mathbf{S}_3$. Ἀφ' ἑτέρου, αὐτὴ ἡ ὁμάδα δὲν μπορεῖ νὰ περιέχει περισσότερες μεταθέσεις, ἀφοῦ κάθε K-αὐτομορφισμὸς τοῦ L εἴδαμε ὅτι ταυτίζεται μὲ μία μετάθεση τῆς $\mathbf{S}_3$. Συνοψίζοντας ὅλα τὰ προηγούμενα καταλήγομε στὸ ἑξῆς συμπέρασμα:

[2] Παρατηρῆστε ὅτι $K(\delta) = K$ στὴν περίπτωση ποὺ $\delta \in K$. Παρατηρῆστε, ἐπίσης, ὅτι, γιὰ τὴν ἐφαρμογὴ τοῦ Θεωρήματος 1.4.3, πρέπει νὰ βεβαιωθοῦμε ὅτι τὸ $f(X)$ εἶναι ἀνάγωγο πάνω ἀπὸ τὸ $K(\delta)$· βλ. ἄσκηση.

Ἂν ἡ διακρίνουσα ἑνὸς ἀναγώγου κυβικοῦ πολυωνύμου $f(X)$ ὅπως παραπάνω εἶναι τετράγωνο στοιχείου τοῦ K, τότε ἡ ὁμάδα Galois τοῦ πολυωνύμου πάνω ἀπὸ τὸ K εἶναι ἰσόμορφη μὲ τὴν $\mathbf{A}_3$, διαφορετικά, εἶναι ἰσόμορφη μὲ τὴν $\mathbf{S}_3$.

Παράδειγμα 3. Τώρα θεωροῦμε τὸ $f(X) = X^4 - 2 \in \mathbb{Q}[X]$ καὶ θέτομε $\rho = \sqrt[4]{2}$. Ὅλες οἱ ρίζες τοῦ $f(X)$ εἶναι $\pm\rho, \pm i\rho$ καί, συνεπῶς, τὸ σῶμα ριζῶν, ἔστω L, τοῦ πολυωνύμου αὐτοῦ πάνω ἀπὸ τὸ $\mathbb{Q}$ εἶναι τὸ $\mathbb{Q}(\rho, i)$. Εἶναι ἁπλὸ νὰ δείξει κανεὶς ὅτι $[L : \mathbb{Q}] = 8$ (ἄσκηση 1). Ἐπίσης, μὲ τὴ βοήθεια τοῦ Θεωρήματος 1.4.3 ἢ μὲ τὴν Πρόταση 2.1.3 μποροῦμε νὰ δείξομε ὅτι ὑπάρχουν $\sigma, \tau \in \mathcal{G}(L/\mathbb{Q})$ τέτοια ὥστε

$$\sigma(\rho) = i\rho\,,\ \sigma(i) = i \qquad \tau(\rho) = \rho\,,\ \tau(i) = -i\,.$$

(ἄσκηση 2). Τότε εὔκολα κατασκευάζομε τὸν παρακάτω πίνακα:

αὐτομορφισμός	δράση στὸ ρ	δράση στὸ i
$\mathbf{id}_L$	ρ	i
σ	$i\rho$	i
σ^2	$-\rho$	i
σ^3	$-i\rho$	i
τ	ρ	$-i$
$\sigma\tau$	$i\rho$	$-i$
$\sigma^2\tau$	$-\rho$	$-i$
$\sigma^3\tau$	$-i\rho$	$-i$

Ἐπειδὴ κάθε στοιχεῖο τῆς $\mathcal{G}(L/\mathbb{Q})$, (1) στέλνει τὸ ρ σὲ ἕνα ἀπὸ τὰ $\rho, -\rho, i\rho, -i\rho$ καὶ τὸ i σὲ ἕνα ἀπὸ τὰ $i, -i$ καὶ (2) καθορίζεται πλήρως ἀπὸ τὴ δράση του στὰ ρ καὶ i, ἕπεται ὅτι οἱ ὀκτὼ αὐτομορφισμοὶ τοῦ παραπάνω πίνακα καλύπτουν ὁλόκληρη τὴν ὁμάδα $\mathcal{G}(L/\mathbb{Q})$. Ἡ ὁμάδα αὐτὴ εἶναι ἡ *διεδρικὴ* $\mathbf{D}_4$ τῆς ὁποίας ἡ ἀφηρημένη περιγραφὴ εἶναι

$$\mathbf{D}_4 = \langle \sigma, \tau\ :\ \sigma^4 = 1\,,\ \tau^2 = 1\,,\ \tau\sigma = \sigma^3\tau \rangle\,.$$

Ἀσκήσεις

1. Μὲ τὸ συμβολισμὸ τοῦ Παραδείγματος 3, ἀποδεῖξτε ὅτι $[L : \mathbb{Q}] = 8$.

2. Ἀποδεῖξτε τὴν ὕπαρξη τῶν αὐτομορφισμῶν σ καὶ τ τοῦ Παραδείγματος 3.

3. Ὑπολογῖστε τὴν ὁμάδα Galois τοῦ $X^3 - 2 \in \mathbb{Q}[X]$ δίχως νὰ χρησιμοποιήσετε τὰ συμπεράσματα τοῦ Παραδείγματος 2.

4. Μὲ τὰ δεδομένα καὶ τὶς ὑποθέσεις τοῦ Παραδείγματος 2, ἀποδεῖξτε ὅτι τὸ πολυώνυμο $f(X)$ εἶναι ἀνάγωγο πάνω ἀπὸ τὸ σῶμα $K(\delta)$.

2.2 Η ΑΝΤΙΣΤΟΙΧΙΑ GALOIS

Ἔστω L/K *πεπερασμένη* ἐπέκταση. Κάθε ὑπόσωμα τοῦ L, τὸ ὁποῖο εἶναι συγχρόνως καὶ ἐπέκταση τοῦ K, λέγεται *ἐνδιάμεση ἐπέκταση* τῆς L/K. Συμβολίζομε μὲ $\mathcal{E}$ τὸ σύνολο τῶν ἐνδιαμέσων ἐπεκτάσεων τῆς L/K. Ἔστω $G = \mathcal{G}(L/K)$. Σύμφωνα μὲ τὸ Θεώρημα 2.1.2, ἡ G εἶναι πεπερασμένη ὁμάδα καὶ συμβολίζομε μὲ $\mathcal{O}$ τὸ σύνολο ὅλων τῶν ὑποομάδων τῆς G.

Πρόταση 2.2.1. *Ἂν $H \in \mathcal{O}$, τότε τὸ*

$$\mathcal{F}_L(H) \stackrel{o\rho\sigma}{=} \{u \in L : \sigma(u) = u \ \ \forall \sigma \in H\}$$

ἀνήκει στὸ $\mathcal{E}$.

Ἀπόδειξη. Πρῶτ' ἀπ' ὅλα, $1 \in \mathcal{F}_L(H)$, ἀφοῦ τὸ 1 παραμένει ἀναλλοίωτο ἀπὸ ὅλους τοὺς αὐτομορφισμούς. Ἀκόμη, ἂν $u, v \in \mathcal{F}_L(H)$ τότε, γιὰ κάθε $\sigma \in H$, $\sigma(uv) = \sigma(u)\sigma(v) = uv$, ἄρα $uv \in \mathcal{F}_L(H)$. Ἐντελῶς ἀνάλογα, ἂν $u \in \mathcal{F}_L(H)$, τότε καὶ $u^{-1} \in \mathcal{F}_L(H)$. □

Ὁρίζομε τώρα τὶς ἑξῆς ἀπεικονίσεις μεταξὺ τῶν $\mathcal{E}$ καὶ $\mathcal{O}$.

$$\mathcal{G}(L/\cdot) : \ \mathcal{E} \ni E \longrightarrow \mathcal{G}(L/E) \in \mathcal{O}$$

$$\mathcal{F}_L : \ \mathcal{O} \ni H \longrightarrow \mathcal{F}_L(H) \in \mathcal{E}\ .$$

Εὔκολα βλέπει κανεὶς ὅτι $\mathcal{G}(L/\mathcal{F}_L(H)) \supseteq H$ γιὰ κάθε ὑποομάδα H τῆς $\mathcal{G}(L/K)$. Πράγματι, ἔστω $\sigma \in H$. Ὁ σ ἀνήκει στὴν ὁμάδα $\mathcal{G}(L/\mathcal{F}_L(H))$ ἄν, καὶ μόνο ἄν, ἀφήνει ἀναλλοίωτα ὅλα τὰ στοιχεῖα τοῦ σώματος $\mathcal{F}_L(H)$. Ἐξ ὁρισμοῦ ὅμως, αὐτὰ τὰ στοιχεῖα μένουν ἀναλοίωτα ἀπὸ κάθε αὐτομορφισμὸ ποὺ ἀνήκει στὴν H, ἄρα καὶ ἀπὸ τὸ σ. Τὸ ἀντίστροφο, ὅτι δηλαδὴ $\mathcal{G}(L/\mathcal{F}_L(H)) \subseteq H$, ἔχει μεγάλη ἀπόδειξη, τὴν ὁποία παραλείπομε. Διατυπώνομε ὅμως τὸ συμπέρασμά μας ὡς ἑξῆς:

> Ἔστω L/K πεπερασμένη ἐπέκταση. Γιὰ κάθε ὑποομάδα H τῆς $\mathcal{G}(L/K)$ ἰσχύει $\mathcal{G}(L/\mathcal{F}_L(H)) = H$.

Κατ' ἀναλογίαν μὲ τὴν $\mathcal{G}(L/\mathcal{F}_L(H)) \supseteq H$ ἀποδεικνύεται, τὸ ἴδιο εὔκολα καὶ ἡ σχέση $\mathcal{F}_L(\mathcal{G}(L/E)) \supseteq E$ γιὰ κάθε ἐνδιάμεση ἐπέκταση E τῆς L/K (δηλαδή, γιὰ κάθε $E \in \mathcal{E}$). Ἀποδεικνύεται ὅτι ἡ ἀντίστροφη σχέση, δηλαδὴ ἡ $\mathcal{F}_L(\mathcal{G}(L/E)) \subseteq E$, δὲν ἰσχύει, παρὰ μόνο ἂν ἡ ἐπέκταση L/K εἶναι *ἐπέκταση Galois*, ὅπως λέμε.

Ὁρισμὸς 2.2.2. *Μία ἐπέκταση L/K λέγεται Galois ἂν εἶναι κανονικὴ καὶ διαχωρίσιμη.*

Παρακάτω, ὁρίζομε καὶ ἐπεξηγοῦμε αὐτὲς τὶς δύο ἔννοιες.

Ὁρισμὸς 2.2.3. *Ἡ ἐπέκταση L/K λέγεται κανονική, ἂν κάθε ἀνάγωγο πολυώνυμο τοῦ $K[X]$, ποὺ ἔχει ἕνα πρωτοβάθμιο παράγοντα στὸ $L[X]$, ἀναλύεται πλήρως σὲ πρωτοβάθμιους παράγοντες τοῦ $L[X]$.*
Μὲ λιγότερο αὐστηρή, ἀλλὰ πιὸ παραστατικὴ διατύπωση: Ἡ ἐπέκταση L/K λέγεται κανονική, ἂν κάθε ἀνάγωγο πολυώνυμο τοῦ $K[X]$, ποὺ ἔχει μία ρίζα μέσα στὸ L ἔχει καὶ ὅλες τὶς ὑπόλοιπες ρίζες στὸ L.

Δηλαδή, ἡ ἐπέκταση K/L εἶναι κανονικὴ ἂν *κάθε ἀνάγωγο πολυώνυμο τοῦ $K[X]$ ἢ ἔχει ὅλες τὶς ρίζες του μέσα στὸ L, ἢ καμμία ρίζα μέσα στὸ L.* Ὅλα ἢ τίποτα!
Γιὰ παράδειγμα, ἂν $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{d})$, ὅπου $d \in \mathbb{Q}$ δὲν εἶναι τετράγωνο ρητοῦ, ἡ L/K

εἶναι κανονική. Πράγματι, ἔστω $f(X) \in \mathbb{Q}[X]$ ἀνάγωγο, τοῦ ὁποίου μία ρίζα ἀνήκει στὸ L. Τότε ἡ ρίζα αὐτὴ ἔχει τὴ μορφὴ $a + b\sqrt{d}$, $a, b \in \mathbb{Q}, b \neq 0$. Ἂν στὴ σχέση $f(a + b\sqrt{d}) = 0$ ἐφαρμοστεῖ ὁ $\mathbb{Q}$-αὐτομορφισμὸς ποὺ στέλνει τὸ $a + b\sqrt{d}$ στὸ $a - b\sqrt{d}$, συμπεραίνομε ὅτι καὶ τὸ $a - b\sqrt{d}$ εἶναι ρίζα τοῦ $f(X)$, συνεπῶς $f(X) = (X - (a + b\sqrt{d}))(X - (a - b\sqrt{d}))g(X)$ γιὰ κάποιο $g(X) \in L[X]$. Ἄρα $f(X) = (X^2 - 2aX + (a^2 - db^2))g(X)$, ἀπ' ὅπου φαίνεται ὅτι τὸ $g(X)$ ἔχει ρητοὺς συντελεστές, ὡς πηλῖκο δύο πολυωνύμων μὲ ρητοὺς συντελεστές. Ὅμως τὸ $f(X)$ ἔχει ὑποτεθεῖ ἀνάγωγο, ἄρα τὸ $g(X)$ εἶναι σταθερὸ πολυώνυμο καί, συνεπῶς, οἱ μόνες ρίζες τοῦ $f(X)$ εἶναι οἱ $a \pm b\sqrt{d}$, πού, ὅπως εἴδαμε ἤδη, ἀνήκουν στὸ L. Εὐτυχῶς, ὑπάρχει ἕνα πολὺ βολικὸ κριτήριο [3] γιὰ νὰ ἐξετάζομε ἂν μία πεπερασμένη ἐπέκταση εἶναι κανονική.

Θεώρημα 2.2.4. *Ἡ πεπερασμένη ἐπέκταση L/K εἶναι κανονική, ἂν καὶ μόνο ἂν τὸ L εἶναι σῶμα ριζῶν ἑνὸς μὴ μηδενικοῦ πολυωνύμου τοῦ $K[X]$.*

Μὲ αὐτὸ τὸ κριτήριο, τὸ συμπέρασμα τοῦ παραπάνω παραδείγματος εἶναι προφανές, διότι $L = \mathbb{Q}(\sqrt{d})$ καὶ, συνεπῶς τὸ L εἶναι τὸ σῶμα ριζῶν πάνω ἀπὸ τὸ $\mathbb{Q}$ τοῦ $X^2 - d \in \mathbb{Q}[X]$. Ἄλλη ἐφαρμογὴ τοῦ Θεωρήματος 2.2.4 εἶναι στὴν ἐπέκταση $L/\mathbb{Q}$ μὲ $L = \mathbb{Q}(\rho)$ καὶ ρ ρίζα τοῦ $f(X) = X^3 - 3X + 1$. Σύμφωνα μὲ τὴν ἄσκηση 1.3.7, τὸ σῶμα ριζῶν τοῦ $f(X)$ εἶναι τὸ $\mathbb{Q}(\rho)$, ἄρα ἡ ἐπέκταση $L/\mathbb{Q}$ εἶναι κανονική. Ἀντιθέτως, ἡ $L/\mathbb{Q}$ μὲ $L = \mathbb{Q}(\rho)$ καὶ ρ ρίζα τοῦ $f(X) = X^3 - 2$, δὲν εἶναι κανονική, διότι οἱ ἄλλες ρίζες τοῦ $f(X)$, πλὴν τῆς ρ, δὲν εἶναι πραγματικὲς καί, συνεπῶς, δὲν ἀνήκουν στὸ L. Ἐδῶ, ὅπως καὶ σὲ κάθε περίπτωση ποὺ θέλομε νὰ δείξομε ὅτι μία ἐπέκταση L/K δὲν εἶναι κανονική, δὲν χρειάζεται νὰ ἐφαρμόζομε τὸ Θεώρημα 2.2.4· σύμφωνα μὲ τὸν ὁρισμό, ἀρκεῖ νὰ δείξομε ὅτι ἕνα ὁποιοδήποτε ἀνάγωγο πολυώνυμο τοῦ $K[X]$ ἔχει κάποια ρίζα του ἐκτὸς τοῦ L.

Ὁρισμὸς 2.2.5. *(α΄) Ἔστω σῶμα K καὶ μὴ μηδενικὸ $f(X) \in K[X]$. Λέμε ὅτι τὸ $f(X)$ εἶναι* διαχωρίσιμο πολυώνυμο *ἂν ὅλες οἱ ρίζες του εἶναι ἁπλές.*
(β΄) Ἔστω L/K μία ἐπέκταση. Τὸ ἀλγεβρικὸ στοιχεῖο $u \in L$ λέγεται διαχωρίσιμο πάνω ἀπὸ τὸ K, ἂν τὸ ἐλάχιστο πολυώνυμό του πάνω ἀπὸ τὸ K εἶναι διαχωρίσιμο. Ἡ ἀλγεβρικὴ ἐπέκταση L/K λέγεται διαχωρίσιμη ἂν κάθε στοιχεῖο της εἶναι διαχωρίσιμο πάνω ἀπὸ τὸ K.

Γιὰ τὴ μελέτη τῶν διαχωρισίμων πολυωνύμων εἶναι χρήσιμη ἡ ἔννοια τῆς *τυπικῆς παραγώγου* πολυωνύμου.

Ὁρισμὸς 2.2.6. *Ἔστω σῶμα K καὶ $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, τότε ὡς τυπικὴ παράγωγο, ἢ ἁπλῶς, παράγωγο τοῦ $f(X)$ ὁρίζομε τὸ πολυώνυμο $f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1$.* [4].

Μὲ ἀλγεβρικὲς πράξεις μόνο ἀποδεικνύονται οἱ ἑξῆς ἰδιότητες:[5] Ἂν $f, g \in K[X]$, τότε

$$(f+g)' = f' + g' \,,\ (f \cdot g)' = f' \cdot g + f \cdot g' \,,\ (f^m)' = m \cdot f^{m-1} \cdot f' \,. \tag{2.1}$$

Πρόταση 2.2.7. *Ἔστω σῶμα K καὶ $f(X) \in K[X]$. Ἔστω ἐπέκταση L τοῦ K καὶ $\lambda \in L$. Τότε, τὸ λ εἶναι πολλαπλῆ ρίζα τοῦ $f(X)$ ἂν καὶ μόνο ἂν $f'(\lambda) = 0$.*

[3] Δὲν ἀποδεικνύεται σὲ αὐτὲς τὶς σημειώσεις.

[4] Τὴν ἰδέα γιὰ νὰ ὁρίσομε τὸ f' παίρνομε, φυσικά, ἀπὸ τὸν Ἀπειροστικὸ Λογισμό.

[5] Ὄχι Ἀνάλυση ! Ἄλλωστε, δὲν μποροῦμε νὰ 'κάνομε Ἀνάλυση' στὸ M, ἀφοῦ αὐτὸ τὸ σῶμα εἶναι τυχαῖο καὶ δὲν ἔχει τοπολογία, ἄρα, σ' αὐτὸ δὲν ὑπάρχει ἔννοια συγκλίσεως.

Ἀπόδειξη Ἔστω ὅτι τὸ $f(X)$ ἔχει ρίζα τὸ λ μὲ πολλαπλότητα r. Τότε $f(X) = (X - \lambda)^r g(X)$, ὅπου $g(X) \in L[X]$, $r \geq 1$ καὶ $g(\lambda) \neq 0$. Ἐφαρμόζοντας κατάλληλα τοὺς τύπους (2.1) ἔχομε $f'(X) = r(X-\lambda)^{r-1}g(X) + (X-\lambda)^r g'(X)$.
Ἂν τὸ λ εἶναι πολλαπλῆ ρίζα τοῦ $f(X)$, τότε $r \geq 2$, καὶ ἀπὸ τὴν παραπάνω ἔκφραση τοῦ $f'(X)$ βλέπομε ὅτι $f'(\lambda) = 0$.
Ἀντιστρόφως, ἂν $f'(\lambda) = 0$, τότε, $r \geq 2$. Πράγματι, σὲ ἀντίθετη περίπτωση, θὰ ἦταν $r = 1$, ὁπότε ἡ παραπάνω ἔκφραση τοῦ $f'(X)$ θὰ μᾶς ἔδινε $f'(X) = g(X) + (X-\lambda)^r g'(X)$ καὶ τότε, $f'(\lambda) = g'(\lambda) \neq 0$· ἀντίφαση. □

Ἀμέσως παρακάτω θὰ δείξομε ὅτι τὰ ἀνάγωγα πολυώνυμα μὲ συντελεστὲς ἀπὸ δύο σημαντικὲς κατηγορίες σωμάτων εἶναι ἀνάγωγα. Ἡ πρώτη κατηγορία περιλαμβάνει τὰ σώματα χαρακτηριστικῆς 0 καὶ ἡ δεύτερη τὰ πεπερασμένα σώματα. Τῶν σωμάτων τῆς δεύτερης κατηγορίας ἡ χαρακτηριστικὴ εἶναι πρῶτος ἀριθμός καὶ θὰ ἀποδείξομε τὴν ἑξῆς σημαντικὴ πρόταση.

Πρόταση 2.2.8. *Ἔστω πεπερασμένο σῶμα K χαρακτηριστικῆς p.*[6] *Τότε ἡ ἀπεικόνιση $\phi : K \to K$, ποὺ ὁρίζεται $\phi(a) = a^p$ γιὰ κάθε $a \in K$, εἶναι αὐτομορφισμὸς τοῦ K καὶ ὀνομάζεται αὐτομορφισμὸς Frobenius. Εἰδικώτερα, ἀφοῦ ἡ ϕ εἶναι "ἐπί", γιὰ κάθε $a \in K$ ὑπάρχει $b \in K$, τέτοιο ὥστε $a = b^p$.*

Ἀπόδειξη. Γιὰ κάθε $a, b \in K$ ἰσχύει ἡ ταυτότητα (διώνυμο του Newton) $(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k$. Σὰν ἄσκηση Θεωρίας Αριθμῶν μπορεῖ νὰ δείξει κανεὶς ὅτι καθένας ἀπὸ τοὺς διωνυμικοὺς συντελεστὲς μέσα στὸ ἄθροισμα $\sum_{k=1}^{p-1}(\cdots)$ εἶναι 0 (παίζει ρόλο τὸ ὅτι ὁ p εἶναι πρῶτος) καί, ἐπειδὴ ἡ χαρακτηριστικὴ τοῦ K εἶναι p, ὅλοι οἱ ὅροι αὐτοῦ τοῦ ἀθροίσματος μηδενίζονται. Ἄρα, $(a+b)^p = a^p + b^p$. Προφανῶς $(ab)^p = a^p b^p$, ὁπότε αὐτὲς οἱ δύο τελευταῖες σχέσεις μᾶς λένε ὅτι ἡ ἀπεικόνιση ϕ εἶναι ὁμομορφισμός. Ὁ πυρήνας τοῦ ϕ εἶναι ὁ τετριμμένος, διότι, ἂν $\phi(a) = 0$, τότε $a^p = 0$, ἄρα[7] $a = 0$. Συνεπῶς, ὁ ϕ εἶναι μονομορφισμός. Τέλος, ἀφοῦ ἡ ϕ ἀπεικονίζει πεπερασμένο σύνολο στὸν ἑαυτό του καὶ εἶναι 1-1, ὑποχρεωτικὰ εἶναι καὶ "ἐπί".
Παρατήρηση. Ἡ ταυτότητα $(a+b)^p = a^p + b^p$ ἰσχύει σὲ κάθε μεταθετικὸ δακτύλιο μὲ μοναδιαῖο, τοῦ ὁποίου ἡ χαρακτηριστικὴ εἶναι p. Ἡ σχέση αὐτὴ γενικεύεται: $(a_1 + a_2 + \cdots + a_k)^p = a_1^p + a_2^p + \cdots + a_k^p$ (ἁπλῆ ἐπαγωγικὴ ἀπόδειξη). Συνεπῶς, ἂν τὸ σῶμα K ἔχει χαρακτηριστικὴ p, τότε $K[X]$ εἶναι μεταθετικὸς δακτύλιος μὲ μοναδιαῖο καὶ ἡ χαρακτηριστική του εἶναι p. Ἄρα, στὴν περίπτωση αὐτή, ἰσχύει στὸν $K[X]$ ἡ ταυτότητα $(f_1(X) + f_2(X) + \cdots + f_k(X))^p = f_1(X)^p + f_2(X)^p + \cdots + f_k(X)^p$.

Θεώρημα 2.2.9. *Ἔστω σῶμα K. Ἂν ἡ χαρακτηριστικὴ τοῦ K εἶναι 0, εἴτε τὸ K εἶναι πεπερασμένο, τότε κάθε ἀνάγωγο πολυώνυμο τοῦ $K[X]$ εἶναι διαχωρίσιμο. Συνεπῶς, κάθε ἀλγεβρικὴ ἐπέκταση πάνω ἀπὸ ἕνα τέτοιο σῶμα K εἶναι διαχωρίσιμη.*

Ἀπόδειξη. Ἔστω ἀνάγωγο $f(X) = \sum_{k=1}^{n} a_k X^k$, ὅπου $n \geq$ καὶ $a_n \neq 0$. Ἂς ὑποθέσομε ὅτι τὸ $f(X)$ δὲν εἶναι διαχωρίσιμο καὶ ἔστω λ μία ρίζα τοῦ $f(X)$ σὲ κάποια ἐπέκταση L/K, τῆς ὁποίας ἡ πολλαπλότητα εἶναι > 1. Θὰ καταλήξομε σὲ ἄτοπο.

Ἔστω, πρῶτα, ὅτι ἡ χαρακτηριστικὴ τοῦ K εἶναι 0. Ἀπὸ τὴν Πρόταση 2.2.7 ἔχομε ὅτι $f'(\lambda) = 0$. Ἀπὸ τὴν Πρόταση Α΄.4(2) τοῦ Παραρτήματος Α΄ συμπεραίνομε ὅτι $f(X) | f'(X)$. Αὐτὴ ἡ σχέση, ὅμως, εἶναι ἀδύνατη διότι, $f'(X) = na_n X^{n-1} +$ (*ὅροι βαθμοῦ* $< n-1$) καὶ

[6] Ὁ p εἶναι, ὑποχρεωτικά, πρῶτος.
[7] Εἴμαστε σὲ σῶμα, ἄρα δὲν ὑπάρχουν μηδενοδιαιρέτες.

$na_n \neq 0$ (σ' αὐτὴ τὴν τελευταία σχέση παίζει ρόλο τὸ ὅτι ἡ χαρακτηριστικὴ εἶναι 0) , ὁπότε τὸ $f(X)$ διαιρεῖ ἕνα μὴ μδενικὸ πολυώνυμο μικροτέρου βαθμοῦ· ἄτοπο.

Ἔστω τώρα ὅτι τὸ K εἶναι πεπερασμένο καὶ ἡ χαρακτηριστική του εἶναι p. Ὅπως καὶ στὴν περίπτωση τῆς χαρακτηριστικῆς 0, καταλήγομε στὴ σχέση $f(X)|f'(X)$. Ἂν τὸ $f'(X)$ ἦταν μὴ μηδενικό, θὰ ὁδηγούμαστε σὲ ἄτοπο διότι τὸ $f(X)$ θὰ διαιροῦσε ἕνα μὴ μηδενικὸ πολυώνυμο μικροτέρου βαθμοῦ. Ἄρα, ἀναγκαζόμαστε νὰ δεχθοῦμε ὅτι τὸ $f'(X)$ εἶναι μηδενικὸ πολυώνυμο. Τώρα γράφομε τὸ $f(X)$ ὡς ἑξῆς:

$$f(X) = a_{n_1}X^{n_1} + a_{n_2}X^{n_2} + \cdots + a_{n_k}X^{n_k}, \qquad n_1 > n_2 > \cdots > n_k \geq 0, \quad a_{n_1}a_{n_2}\cdots a_{n_k} \neq 0,$$

ὁπότε

$$f'(X) = n_1a_{n_1}X^{n_1-1} + n_2a_{n_2}X^{n_2-1} + \cdots + n_ka_{n_k}X^{n_k-1}.$$

Ἐπειδὴ τὸ $f'(X)$ εἶναι μηδενικό, συμπεραίνομε ὅτι $n_1a_{n_1} = n_2a_{n_2} = \ldots n_ka_{n_k} = 0$. Ὅμως, τὰ $a_{n_1}, a_{n_2}, \ldots, a_{n_k}$ εἶναι $\neq 0$, ἄρα ὅλοι οἱ ἀκέραιοι $n_1, n_2, \ldots, n_k$ εἶναι πολλαπλάσια τοῦ p. Θέτομε $n_i = pm_i$ γιὰ $i = 1, \ldots, k$. Ἐπίσης, λόγῳ τῆς Πρότασης 2.2.8, ὑπάρχουν $b_1, b_2, \ldots, b_k$, τέτοια ὥστε $a_{n_i} = b_i^p$. Συνεπῶς,

$$f(X) = b_1^p(X^{m_1})^p + b_2^p(X^{m_2})^p + \cdots + b_k^p(X^{m_k})^p = (b_1X^{m_1} + b_2X^{m_2} + \cdots b_kX^{m_k})^p,$$

ὅπου ἡ τελευταία ἰσότητα εἶναι συνέπεια τῆς παρατήρησης ἀμέσως μετὰ τὴν Πρόταση 2.2.8. Βλέπομε, δηλαδή, ὅτι τὸ $f(X)$ εἶναι p-δύναμη ἑνὸς ἄλλου πολυωνύμου τοῦ $K[X]$ καὶ αὐτὸ ἀντιβαίνει στὴν ὑπόθεση ὅτι τὸ $f(X)$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ K. □

Πόρισμα 2.2.10. *Ἂν τὸ K εἶναι σῶμα χαρακτηριστικῆς 0, εἴτε πεπερασμένο σῶμα, τότε οἱ ἔννοιες «κανονικὴ ἐπέκταση τοῦ K» καὶ «Galois ἐπέκταση τοῦ K» εἶναι ἰσοδύναμες. Ἄρα, συνδυάζοντας μὲ τὸ Θεώρημα 2.2.4, συμπεραίνομε ὅτι:*

> *Ἂν τὸ K εἶναι σῶμα χαρακτηριστικῆς 0, εἴτε πεπερασμένο σῶμα καὶ τὸ L εἶναι σῶμα ριζῶν πάνω ἀπ' τὸ K μὴ μηδενικοῦ πολυωνύμου $f(X) \in K[X]$, τότε ἡ ἐπέκταση L/K εἶναι Galois.*

Ἂς ἐπανέλθομε τώρα στὸ ἐρώτημα ποὺ εἶχε μείνει ἀναπάντητο: Πότε ἴσχύει ἡ ἰσότητα στὴ σχέση $\mathcal{F}_L(\mathcal{G}(L/E)) \supseteq E$;

> Ἔστω L/K πεπερασμένη, κανονικὴ καὶ διαχωρίσιμη ἐπέκταση, δηλαδή, πεπερασμένη ἐπέκταση Galois. Τότε, γιὰ κάθε ἐνδιάμεση ἐπέκταση E ἰσχύει $\mathcal{F}_L(\mathcal{G}(L/E)) = E$.

Σὲ αὐτὲς τὶς σημειώσεις παραλείπομε τὴν ἀπόδειξη. Τὰ δύο βασικὰ συμπεράσματα, ὅσον ἀφορᾶ στὶς συνθέσεις τῶν ἀπεικονίσεων $\mathcal{G}(L/\cdot)\circ\mathcal{F}_L$ καὶ $\mathcal{F}_L\circ\mathcal{G}(L/\cdot)$, στὰ ὁποῖα καταλήξαμε μέχρι τώρα, συνδυαζόμενα μᾶς ὁδηγοῦν στὸ ἑξῆς συμπέρασμα:

Θεώρημα 2.2.11. *Ἔστω L/K πεπερασμένη ἐπέκταση Galois, $\mathcal{E}$ τὸ σύνολο τῶν ἐνδιαμέσων ἐπεκτάσεων καὶ $\mathcal{O}$ τὸ σύνολο τῶν ὑποομάδων τῆς $\mathcal{G}(L/K)$. Τότε οἱ ἀπεικονίσεις*

$$\mathcal{G}(L/\cdot) : \mathcal{E} \ni E \longrightarrow \mathcal{G}(L/E) \in \mathcal{O}$$

$$\mathcal{F}_L : \mathcal{O} \ni H \longrightarrow \mathcal{F}_L(H) \in \mathcal{E}\,.$$

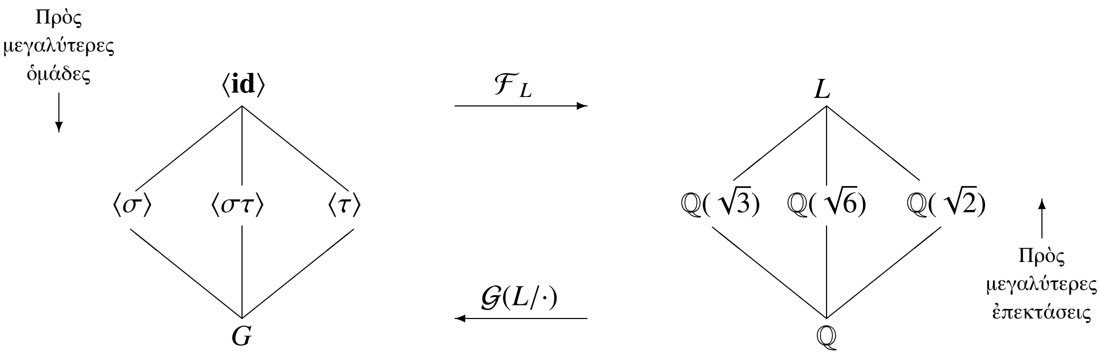
εἶναι ἀντίστροφες ἡ μία τῆς ἄλλης. Εἰδικώτερα, κάθε μία ἀπὸ αὐτὲς τὶς ἀπεικονίσεις εἶναι ἀμφιμονοσήμαντη, ἐπί. Αὐτὴ ἡ 1-1 ἀντιστοιχία μεταξὺ ἐνδιαμέσων ἐπεκτάσεων καὶ ὑποομάδων τῆς ὁμάδος Galois ὀνομάζεται ἀντιστοιχία Galois.

Ἂς δοῦμε τώρα τὰ τρία παραδείγματα τῆς ἑνότητας 2.1 ὑπὸ τὸ πρῖσμα τοῦ Θεωρήματος 2.2.11, χρησιμοποιώντας τοὺς συμβολισμοὺς κλπ καθενὸς ἀπὸ αὐτά.

Παράδειγμα 1. (Βλ. Παράδειγμα 1, σελ. 26.) Ἡ ἐπέκταση $L/\mathbb{Q}$ εἶναι τὸ σῶμα ριζῶν τοῦ πολυωνύμου $(X^2-2)(X^2-3) \in \mathbb{Q}[X]$, ἄρα εἶναι κανονική (Θεώρημα 2.2.4). Εἶναι καὶ διαχωρίσιμη (Θεώρημα 2.2.9), ἄρα, σύμφωνα μὲ τὸ Θεώρημα 2.2.11, οἱ ὑποομάδες τῆς $G \overset{o\rho\sigma}{=} \mathcal{G}(L/\mathbb{Q})$ ἔρχονται σὲ 1-1 ἀντιστοιχία μὲ τὶς ἐνδιάμεσες ἐπεκτάσεις τῆς $L/\mathbb{Q}$. Οἱ ὑποομάδες τῆς G βρίσκονται ἁπλούστατα: Εἶναι οἱ $\langle \mathbf{id} \rangle, \langle \sigma \rangle, \langle \tau \rangle, \langle \sigma\tau \rangle, G$. Ἄρα, ὑπάρχουν ἀκριβῶς 5 ἐνδιάμεσες ἐπεκτάσεις. Ἂς τὶς δοῦμε: Προφανῶς $\mathcal{F}_L(\langle \mathbf{id} \rangle) = L$, διότι ὅλα τὰ στοιχεῖα τοῦ L παραμένουν ἀναλλοίωτα ἀπὸ τὸν ταυτοτικὸ αὐτομορφισμό. Ἂς ὑπολογίσομε τώρα τὸ $\mathcal{F}_L(\langle \sigma \rangle)$. Τὸ τυπικὸ στοιχεῖο τῆς L εἶναι $u = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3},\ a, b, c, d \in \mathbb{Q}$. Ἔχομε, ἐξ ὁρισμοῦ τοῦ σ,

$$
\begin{aligned}
u \in \mathcal{F}_L(\langle \sigma \rangle) &\Leftrightarrow \sigma(u) = u \\
&\Leftrightarrow a - b\sqrt{2} + c\sqrt{3} - d\sqrt{2}\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \\
&\Leftrightarrow b = d = 0 \\
&\Leftrightarrow u \in \mathbb{Q}(\sqrt{3})\,.
\end{aligned}
$$

Μὲ ἀνάλογο τρόπο ἀποδεικνύεται ὅτι $\mathcal{F}_L(\langle \tau \rangle) = \mathbb{Q}(\sqrt{2})$ καὶ $\mathcal{F}_L(\langle \sigma\tau \rangle) = \mathbb{Q}(\sqrt{6})$ (ἄσκηση 3). Μία ἀπὸ τὶς συνέπειες τοῦ Θεωρήματος 2.2.11 εἶναι ὅτι $\mathcal{F}_L(G) = \mathbb{Q}$. Στὸ συγκεκριμένο παράδειγμα αὐτὸ ἀποδεικνύεται καὶ δίχως τὸ Θεώρημα (βλ. ἄσκηση 3) καί, μάλιστα, εὔκολα [8]. Ἡ ἀντιστοιχία μεταξὺ τῶν ὑποομάδων τῆς G καὶ τῶν ἐνδιαμέσων ἐπεκτάσεων φαίνεται πολὺ καθαρὰ στὸ παρακάτω διάγραμμα:



Παράδειγμα 2. (Βλ. Παράδειγμα 2, σελ. 26.) Στὴν περίπτωση ποὺ ἡ διακρίνουσα τοῦ τριτοβαθμίου πολυωνύμου $f(X)$ εἶναι τετράγωνο ρητοῦ, τὸ $L = \mathbb{Q}(\rho)$ εἶναι τὸ σῶμα ριζῶν τοῦ $f(X)$ πάνω ἀπὸ τὸ $\mathbb{Q}$, ὁπότε ἡ $L/\mathbb{Q}$ εἶναι ἐπέκταση Galois. Ἡ ὁμάδα $G \overset{o\rho\sigma}{=} \mathcal{G}(L/\mathbb{Q})$ εἶναι ἰσόμορφη μὲ τὴν ἐναλλάσουσα ὁμάδα $\mathbf{A}_3$, ὁπότε ἔχει μόνο τὶς τετριμμένες ὑποομάδες. Αὐτὸ σημαίνει ὅτι δὲν ὑπάρχουν γνήσιες ἐνδιάμεσες ἐπεκτάσεις.

Ἂς θεωρήσομε τώρα τὴν περίπτωση ποὺ ἡ διακρίνουσα τοῦ $f(X)$ δὲν εἶναι τετράγωνο ρητοῦ. Τότε, τὸ σῶμα ριζῶν L τοῦ $f(X)$ πάνω ἀπὸ τὸ $\mathbb{Q}$ εἴδαμε ὅτι εἶναι τὸ $\mathbb{Q}(\rho, \delta) = \mathbb{Q}(\rho', \delta) = \mathbb{Q}(\rho'', \delta)$ καὶ ἡ $G \overset{o\rho\sigma}{=} \mathcal{G}(L/\mathbb{Q})$ εἶναι ἰσόμορφη μὲ τὴ συμμετρικὴ ὁμάδα $\mathbf{S}_3$. Οἱ ὑποομάδες τῆς $\mathbf{S}_3$ εἶναι γνωστές: Ἐκτὸς ἀπὸ τὶς τετριμμένες, ἔχει καὶ τὶς $\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle, \langle(1\ 2\ 3)\rangle$. Ἔτσι, ἂν ἀριθμήσομε τὶς ρίζες ρ, ρ', ρ'' μὲ 1, 2, 3, ἀντιστοίχως, συμπεραίνομε ὅτι οἱ ὑποομάδες τῆς G εἶναι: $\langle \mathbf{id} \rangle, \langle(\rho\,\rho')\rangle, \langle(\rho\,\rho'')\rangle, \langle(\rho'\,\rho'')\rangle, \langle(\rho\,\rho'\,\rho'')\rangle, G$.

[8] Ὡς πρὸς αὐτό, τὸ συγκεκριμένο παράδειγμα ἀποτελεῖ μία εὐτυχῆ ἐξαίρεση.

Ἀπὸ τὸν τρόπο ποὺ ὁρίσαμε τοὺς αὐτομορφισμοὺς σ καὶ τ, βλέπομε ὅτι οἱ μεταθέσεις $(\rho\ \rho'\ \rho'')$, $(\rho'\ \rho'')$, $(\rho\ \rho')$, $(\rho\ \rho'')$ ταυτίζονται, ἀντιστοίχως, μὲ τοὺς αὐτομορφισμοὺς $\sigma, \tau, \sigma\tau, \sigma^2\tau$. Ἀπὸ τὸ Θεώρημα 2.2.11 συμπεραίνομε τώρα ὅτι, ἐκτὸς τῶν τετριμμένων ἐνδιαμέσων ἐπεκτάσεων τῆς $L/\mathbb{Q}$, ὑπάρχουν ἄλλες τέσσερις ἀκόμη. Ἂς τὶς δοῦμε: Ὁ τ ἔχομε 'δεῖ ὅτι ἀφήνει ἀναλλοίωτο τὸ ρ καὶ στέλνει τὸ δ στὸ $-\delta$. Ἄρα, ἂν θεωρήσομε ὡς βάση τῆς $L/\mathbb{Q}$ τὴν $1, \rho, \rho^2, \delta, \delta\rho, \delta\rho^2$, γράφομε τὸ τυπικὸ στοιχεῖο τῆς L ὡς $u = a_0 + a_1\rho + a_2\rho^2 + b_0\delta + b_1\delta\rho + b_2\delta\rho^2$ καί, συνεπῶς,

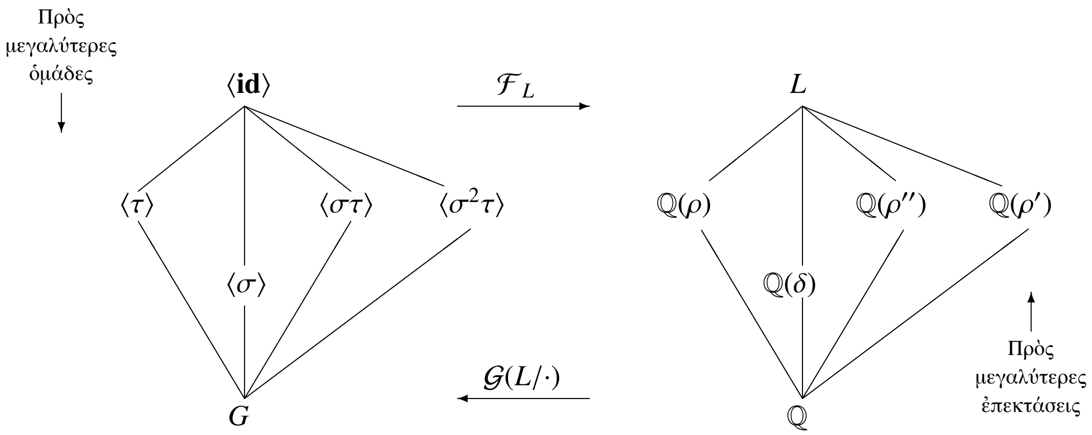
$$\begin{aligned}
u \in \mathcal{F}_L(\langle\tau\rangle) &\Leftrightarrow \tau(u) = u \\
&\Leftrightarrow a_0 + a_1\rho + a_2\rho^2 - b_0\delta - b_1\delta\rho - b_2\delta\rho^2 \\
&\qquad = a_0 + a_1\rho + a_2\rho^2 + b_0\delta + b_1\delta\rho + b_2\delta\rho^2 \\
&\Leftrightarrow b_0 = b_1 = b_2 = 0 \\
&\Leftrightarrow u \in \mathbb{Q}(\rho)\ .
\end{aligned}$$

Ἂν ἐπιχειρήσομε νὰ ἀποδείξομε τὶς ἰσότητες $\mathcal{F}_L(\langle\sigma\tau\rangle) = \mathbb{Q}(\rho'')$ καὶ $\mathcal{F}_L(\langle\sigma^2\tau\rangle) = \mathbb{Q}(\rho')$ κάνοντας χρήση τῆς ἴδιας βάσης γιὰ τὴν ἐπέκταση $L/\mathbb{Q}$, δηλαδή, τῆς $1, \rho, \rho^2, \delta, \delta\rho, \delta\rho^2$, θὰ ὁδηγηθοῦμε σὲ ἐξαιρετικὰ περίπλοκες πράξεις. Εἶναι πολὺ πιὸ ἔξυπνο, ὅταν θέλομε ν' ἀποδείξομε τὴ σχέση $\mathcal{F}_L(\langle\sigma\tau\rangle) = \mathbb{Q}(\rho'')$, νὰ μιμηθοῦμε τὴν παραπάνω ἀπόδειξη χρησιμοποιώντας ὡς βάση τῆς $L/\mathbb{Q}$ τὴν $1, \rho'', \rho''^2, \delta, \delta\rho'', \delta\rho''^2$, ἀφοῦ πρῶτα ἀποδείξομε ὅτι $\sigma\tau(\delta) = -\delta$. Ἀνάλογα, γιὰ ν' ἀποδείξομε τὴ σχέση $\mathcal{F}_L(\langle\sigma^2\tau\rangle) = \mathbb{Q}(\rho')$, θὰ χρησιμοποιήσομε τὴ βάση $1, \rho', \rho'^2, \delta, \delta\rho', \delta\rho'^2$. Μία ἀκόμη ἁπλούστερη ἀπόδειξη, ἡ ὁποία, ὅμως κάνει χρήση τοῦ Θεμελιώδους Θεωρήματος τῆς Θεωρίας Galois (θεώρημα 2.2.12), ὑποδεικνύεται στὴν ἄσκηση 4.

Μένει νὰ βροῦμε τὸ $\mathcal{F}_L(\langle\sigma\rangle)$. Αὐτὸ μπορεῖ νὰ γίνει χωρὶς κανένα ὑπολογισμό, χάρη στὸ Θεώρημα 2.2.11. Πράγματι, τὸ Θεώρημα μᾶς λέει ὅτι τὰ στοιχεῖα τοῦ $\mathcal{E}$ εἶναι τόσα ἀκριβῶς ὅσα καὶ τοῦ $\mathcal{O}$ καί, μέχρι στιγμῆς, τὰ ἔχομε βρεῖ ὅλα πλὴν τοῦ $\mathcal{F}_L(\langle\sigma\rangle)$. Ἀφ' ἑτέρου, τὸ $\mathbb{Q}(\delta)$ εἶναι μία ἐνδιάμεση ἐπέκταση, τὴν ὁποία δὲν ἔχομε ἀκόμη ἀντιστοιχήσει σὲ καμμία ὑποομάδα τῆς G, ἄρα $\mathcal{F}_L(\langle\sigma\rangle) = \mathbb{Q}(\delta)$. Μποροῦμε καὶ μὲ ἄμεσο τρόπο, δίχως νὰ καταφύγομε στὸ Θεώρημα 2.2.11, νὰ καταλήξομε στὸ ἴδιο συμπέρασμα ὡς ἑξῆς: Ἐπειδὴ $\sigma(\rho) = \rho'$ καὶ $\sigma(\delta) = \delta$, ἔχομε $u \in \mathcal{F}_L(\langle\sigma\rangle) \Leftrightarrow \sigma(u) = u$ καὶ ἡ τελευταία σχέση ἰσοδυναμεῖ, διαδοχικά, μὲ τὶς ἑξῆς:

$$\begin{aligned}
&a_0 + a_1\rho' + a_2{\rho'}^2 + b_0\delta + b_1\delta\rho' + b_2\delta{\rho'}^2 \\
&\quad = \ a_0 + a_1\rho + a_2\rho^2 + b_0\delta + b_1\delta\rho + b_2\delta\rho^2\ , \\
&a_1(\rho - \rho') + a_2(\rho^2 - {\rho'}^2) = \delta(b_1(\rho - \rho') + b_2(\rho^2 - {\rho'}^2))\ , \\
&a_1 + a_2(\rho + \rho') = \delta(b_1 + b_2(\rho + \rho'))\ , \\
&a_1 - a_2\rho'' = \delta(b_1 - b_2\rho'')\ , \\
&a_1 - a_2\rho'' - \delta b_1 + \delta b_2\rho'' = 0\ .
\end{aligned}$$

Ἐφαρμόζοντας τὸν σ στὴν τελευταία παίρνομε $a_1 - a_2\rho - b_1\delta + b_2\delta\rho = 0$. Ἄρα, ἀφοῦ τὰ $1, \rho, \delta, \delta\rho$ εἶναι ἀνεξάρτητα πάνω ἀπὸ τὸ $\mathbb{Q}$, ἕπεται ὅτι $a_1 = a_2 = b_1 = b_2 = 0$, δηλαδὴ $u \in \mathbb{Q}(\delta)$. Τώρα ποὺ ἔχομε τὴν πλήρη ἀντιστοιχία ὑποομάδων τῆς G καὶ ἐνδιαμέσων ἐπεκτάσεων τῆς $L/\mathbb{Q}$ μποροῦμε νὰ κατασκευάσομε τὸ παρακάτω παραστατικὸ διάγραμμα:



Παράδειγμα 3. (Βλ. Παράδειγμα 3, σελ. 28.) Σὲ αὐτὸ τὸ παράδειγμα εἴδαμε ὅτι ἡ ὁμάδα Galois $\mathcal{G}(L/\mathbb{Q}) \stackrel{o\rho\sigma}{=} G$ εἶναι ἡ $\langle \sigma, \tau \rangle$), ποὺ εἶναι ἰσόμορφη μὲ τὴ διεδρικὴ ὁμάδα $\mathbf{D}_4$. Οἱ ὑποομάδες της εἶναι,

Τάξεως 1: $\langle \mathbf{id} \rangle$
Τάξεως 2: $\langle \sigma^2 \rangle$, $\langle \tau \rangle$, $\langle \sigma\tau \rangle$, $\langle \sigma^2\tau \rangle$, $\langle \sigma^3\tau \rangle$
Τάξεως 4: $\langle \sigma \rangle \cong \mathbb{Z}_4$, $\langle \sigma^2, \tau \rangle \cong \mathbf{V}_4$, $\langle \sigma^2, \sigma\tau \rangle \cong \mathbf{V}_4$
Τάξεως 8: $G \cong \mathbf{D}_4$

Γιὰ νὰ ὑπολογίσομε τὶς ἐνδιάμεσες ἐπεκτάσεις ποὺ ἀντιστοιχοῦν στὶς μὴ τετριμμένες ὑποομάδες γράφομε τὸ τυπικὸ στοιχεῖο $u \in L$ ὑπὸ τὴ μορφὴ

$$u = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 + b_0 i + b_1 i\rho + b_2 i\rho^2 + b_3 i\rho^3 \ ,$$

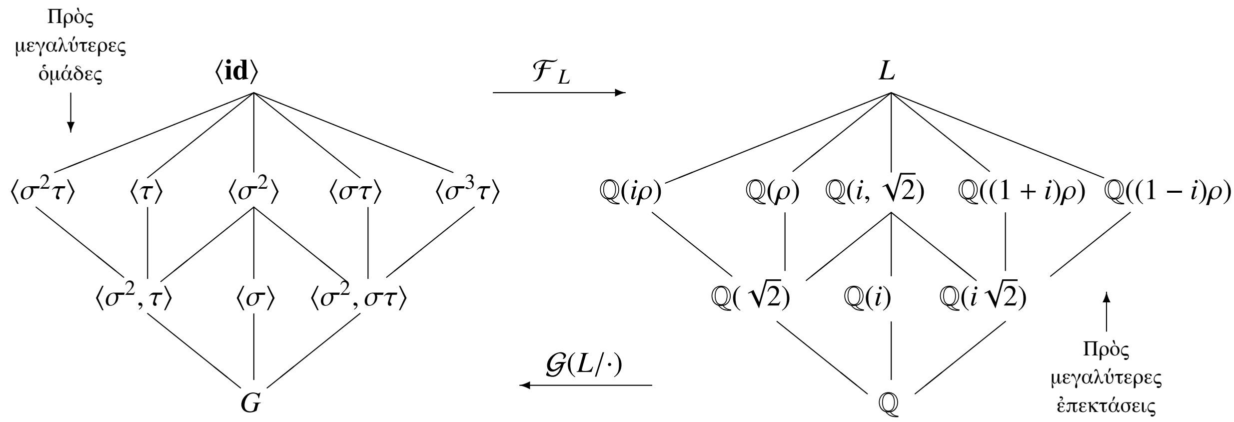
μὲ τοὺς συντελεστὲς a_i, b_i ρητοὺς καὶ ἐξετάζομε, βοηθούμενοι καὶ ἀπὸ τὸν πίνακα ποὺ ἔχομε φτιάξει, ποιὲς συνθῆκες πρέπει νὰ πληροῦν αὐτοὶ οἱ συντελεστὲς γιὰ νὰ μένει ἀναλλοίωτο τὸ u ἀπὸ διάφορους αὐτομορφισμούς. Γιὰ παράδειγμα, ἡ σχέση $\sigma^2(u) = u$ συνεπάγεται, λόγῳ τῶν $\sigma^2(\rho) = -\rho$ καὶ $\sigma^2(i) = i$, ὅτι $a_1 = a_3 = b_1 = b_3 = 0$. Ἄν, ἐπιπλέον, θέλω καὶ $\tau(u) = u$ τότε, λόγῳ τῶν $\tau(\rho) = \rho, \tau(i) = -i$, εἶναι $b_0 = b_2 = 0$, ὁπότε $u = a_0 + a_2\rho^2 = a_0 + a_2\sqrt{2}$· ἔτσι, $\mathcal{F}_L(\langle \sigma^2, \tau \rangle) = \mathbb{Q}(\sqrt{2})$. Μὲ ἀνάλογο τρόπο ὑπολογίζομε (ἄσκηση 5) ὅτι $\mathcal{F}_L(\langle \sigma^2, \sigma\tau \rangle) = \mathbb{Q}(i\sqrt{2})$ καὶ $\mathcal{F}_L(\langle \sigma \rangle) = \mathbb{Q}(i)$. Μερικὲς φορὲς δὲν εἶναι πολὺ εὔκολο νὰ ὑπολογιστεῖ ἡ ἐνδιάμεση ἐπέκταση ποὺ ἀντιστοιχεῖ σὲ κάποια ὑποομάδα. Γιὰ παράδειγμα, ἂς ὑπολογίσομε τὸ $\mathcal{F}_L(\langle \sigma\tau \rangle$: Ἡ σχέση $u = \sigma\tau(u)$ ἰσοδυναμεῖ μὲ τὴν

$$\begin{gathered}
a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 + b_0 i + b_1 i\rho + b_2 i\rho^2 + b_3 i\rho^3 = \\
a_0 + a_1 i\rho - a_2\rho^2 - a_3 i\rho^3 - b_0 i + b_1(-i)i\rho - b_2 i(i\rho)^2 - b_3 i(i\rho)^3 = \\
a_0 + b_1\rho - a_2\rho^2 - b_3\rho^3 - b_0 i + a_1 i\rho + b_2 i\rho^2 - a_3 i\rho^3 \ ,
\end{gathered}$$

ἀπ' ὅπου $a_1 = b_1$, $a_2 = -a_2$, $a_3 = -b_3$, $b_0 = -b_0$ καὶ

$$\begin{aligned}
u &= a_0 + a_1(1+i)\rho + b_2 i\rho^2 + a_3(1-i)\rho^3 \\
&= a_0 + a_1\{(1+i)\rho\} + \frac{b_2}{2}\{(1+i)\rho\}^2 - \frac{a_3}{2}\{(1+i)\rho\}^3 \ .
\end{aligned}$$

Ἄρα $\mathcal{F}_L(\langle \sigma\tau \rangle) = \mathbb{Q}((1+i)\rho)$. Κάποια δυσκολία ὑπάρχει στὸ νὰ ὑποψιαστοῦμε ὅτι $i\rho^2 = \{(1+i)\rho\}^2/2$ καὶ $(1-i)\rho^3 = -\{(1+i)\rho\}^3/2$. Μποροῦμε νὰ διαπιστώσομε μὲ ἀνάλογο τρόπο ὅτι $\mathcal{F}_L(\langle\sigma^3\tau\rangle) = \mathbb{Q}((1-i)\rho)$ (ἄσκηση 5). Ἁπλούστερο εἶναι νὰ διαπιστώσομε ὅτι $\mathcal{F}_L(\langle\sigma^2\rangle) = \mathbb{Q}(i, \sqrt{2})$, $\mathcal{F}_L(\langle\sigma^2\tau\rangle) = \mathbb{Q}(i\rho)$ καὶ $\mathcal{F}_L(\langle\tau\rangle) = \mathbb{Q}(\rho)$ (ἄσκηση 5). Τέλος, $\mathcal{F}_L(\langle\mathbf{id}\rangle) = G$, ἐνῷ λόγῳ τοῦ Θεωρήματος 2.2.11, $\mathcal{F}_L(G) = \mathbb{Q}$. Ὅπως καὶ στὰ προηγούμενα παραδείγματα, κατασκευάζομε τὸ παραστατικὸ διάγραμμα ἐνδιαμέσων ἐπεκτάσεων καὶ ὑποομάδων.



Θεμελιῶδες Θεώρημα τῆς Θεωρίας Galois 2.2.12. *Ἔστω L/K πεπερασμένη ἐπέκταση Galois, $\mathcal{E}$ τὸ σύνολο τῶν ἐνδιαμέσων ἐπεκτάσεών της καὶ $\mathcal{O}$ τὸ σύνολο τῶν ὑποομάδων τῆς $G \overset{ορσ}{=} \mathcal{G}(L/K)$. Τότε*

1. *Ὑπάρχει ἀμφιμονοσήμαντη, ἐπὶ ἀντιστοιχία μεταξὺ τῶν $\mathcal{E}$ καὶ $\mathcal{O}$, ὅπως περιγράφεται στὸ Θεώρημα 2.2.11 (ἀντιστοιχία Galois).*

2. *Ἡ τάξη τῆς G ἰσοῦται μὲ τὸ βαθμὸ τῆς L/K : $|G| = [L : K]$.*

3. *Γιὰ κάθε ἐνδιάμεση ἐπέκταση E, ἡ ἐπέκταση L/E εἶναι ἐπέκταση Galois,*
$$[L : E] = |\mathcal{G}(L/E)| \qquad \textit{καὶ} \qquad [E : K] = \frac{|G|}{|\mathcal{G}(L/E)|}\,.$$

4. *Γιὰ κάθε ἐνδιάμεση ἐπέκταση E, ἡ ἐπέκταση E/K εἶναι ἐπέκταση Galois ἂν καὶ μόνο ἂν ἡ ὑποομάδα $\mathcal{G}(L/E)$ τῆς G εἶναι κανονική. Στὴν περίπτωση αὐτή,*
$$\mathcal{G}(E/K) \cong G/\mathcal{G}(L/E)\,.$$

Ἂς δοῦμε κάποιες ἐφαρμογὲς τοῦ Θεωρήματος αὐτοῦ στὰ προηγούμενα παραδείγματα.

Στὸ παράδειγμα 2, ὅταν $\delta \notin \mathbb{Q}$, θὰ μπορούσαμε νὰ βροῦμε χωρὶς κανένα ὑπολογισμὸ τὴν ἐπέκταση $\mathcal{F}_L(\langle\sigma\rangle)$ ὡς ἑξῆς: Ἐπειδὴ ἡ ἐναλλάσουσα ὁμάδα $\langle\sigma\rangle \cong \mathbf{A}_3$ εἶναι ἡ μοναδικὴ ὑποομάδα τῆς συμμετρικῆς ὁμάδας $G \cong \mathbf{S}_3$ τάξεως 3, ἕπεται ἀπὸ τὰ (1) καὶ (3) τοῦ Θεωρήματος ὅτι ἡ ἐνδιάμεση ἐπέκταση $\mathcal{F}_L(\langle\sigma\rangle)/\mathbb{Q}$ εἶναι ἡ μοναδικὴ τάξεως $6 : 3 = 2$. Ὅμως, μία προφανὴς ἐνδιάμεση ἐπέκταση τάξεως 2 εἶναι ἡ $\mathbb{Q}(\delta)/\mathbb{Q}$, ἄρα $\mathcal{F}_L(\langle\sigma\rangle) = \mathbb{Q}(\delta)$.

Ἂς δοῦμε πῶς ἐπαληθεύεται τὸ Θεώρημα στὸ παράδειγμα 3. Οἱ ὑποομάδες $\langle\sigma^2, \tau\rangle$, $\langle\sigma\rangle$ καὶ $\langle\sigma^2, \sigma\tau\rangle$ εἶναι τάξεως 4, ἄρα ἔχουν δείκτη $8 : 4 = 2$ στὴ G. Ἄρα, ἀπὸ γνωστὴ ἄσκηση τῆς Θεωρίας Ὁμάδων ἕπεται ὅτι εἶναι κανονικὲς ὑποομάδες τῆς G. Συνεπῶς, ἀπὸ τὸ (4) τοῦ Θεωρήματος, οἱ ἀντίστοιχες σὲ αὐτὲς τὶς ὑποομάδες ἐπεκτάσεις (βλ. καὶ τὸ σχετικὸ παραστατικὸ διάγραμμα) εἶναι Galois. Πράγματι, διότι εἶναι σώματα ριζῶν, ἀντιστοίχως, τῶν πολυωνύμων X^2-2, X^2+1 καὶ X^2+2. Ἀντιθέτως, ἡ ἐπέκταση $\mathbb{Q}(\rho)/\mathbb{Q}$ δὲν εἶναι κανονικὴ (ἄρα, οὔτε Galois) διότι, ἐνῶ περιέχει τὴ ρίζα ρ τοῦ X^4-2, δὲν περιέχει τὴ ρίζα του $i\rho$. Σύμφωνα λοιπὸν μὲ τὸ (4) τοῦ Θεωρήματος, ἡ ὑποομάδα $\langle\tau\rangle$, ποὺ ἀντιστοιχεῖ στὴν ἐπέκταση αὐτή, δὲν εἶναι κανονικὴ ὑποομάδα τῆς G, κάτι ποὺ διαπιστώνεται καὶ μὲ ἄμεσο τρόπο: $\sigma\langle\tau\rangle = \{\sigma, \sigma\tau\} \neq \{\sigma, \tau\sigma\} = \langle\tau\rangle\sigma$, ἀφοῦ $\tau\sigma = \sigma^3\tau$. Ἐπίσης, δὲν εἶναι προφανὲς ἂν οἱ ἐπεκτάσεις $\mathbb{Q}((1+i)\rho)$ καὶ $\mathbb{Q}((1-i)\rho)$ εἶναι ἢ ὄχι κανονικὲς [9]. Πολὺ εὐκολώτερο εἶναι νὰ ἐξετάσομε ἂν οἱ ἀντίστοιχες ὑποομάδες τῆς G εἶναι ἢ ὄχι κανονικές: $\langle\sigma\tau\rangle\tau = \{\tau, (\sigma\tau)\tau\} = \{\tau, \sigma\}$ καὶ $\tau\langle\sigma\tau\rangle = \{\tau, \tau(\sigma\tau)\} = \{\tau, (\tau\sigma)\tau\} = \{\tau, (\sigma^3\tau)\tau\} = \{\tau, \sigma^3\}$. Ἄρα ἡ $\langle\sigma\tau\rangle$ δὲν εἶναι κανονικὴ ὑποομάδα τῆς G, ὁπότε ἡ ἐπέκταση $\mathbb{Q}((1+i)\rho)$ δὲν εἶναι κανονική· ὁμοίως καὶ γιὰ τὴν $\mathbb{Q}((1-i)\rho)$.

Ὅσον ἀφορᾶ στὴν $E/\mathbb{Q}$, ὅπου $E = \mathbb{Q}(i, \sqrt{2})$, αὐτὴ εἶναι, προφανῶς, Galois ὡς σῶμα ριζῶν τοῦ $(X^2-2)(X^2+1) \in \mathbb{Q}[X]$. Σύμφωνα λοιπὸν μὲ τὸ (4) τοῦ Θεωρήματος, ἡ ὑποομάδα $\langle\sigma^2\rangle$ τῆς G εἶναι κανονικὴ καὶ $\mathcal{G}(E/\mathbb{Q}) \cong G/\langle\sigma^2\rangle \cong \mathbf{D}_4/\mathbb{Z}_2$. Ἡ τελευταία ὁμάδα, εἶναι τάξεως 4, ἀλλὰ ὄχι κυκλική, ὅπως διαπιστώνεται εὔκολα, ὁπότε εἶναι ἰσόμορφη μὲ τὴν ὁμάδα τοῦ Klein $\mathbf{V}_4$. Αὐτὸ σημαίνει ὅτι ἡ $\mathcal{G}(E/\mathbb{Q})$ παράγεται ἀπὸ δύο αὐτομορφισμούς, ἔστω ϕ καὶ ψ, τέτοιους ὥστε $\phi^2 = \psi^2 = \mathbf{id}$. Ἂν σκεφτοῦμε λίγο, λαμβάνοντας ὑπ' ὄψιν τὸ Θεώρημα 2.1.3, βλέπομε ὅτι μποροῦμε νὰ πάρομε ὡς ϕ τὸν αὐτομορφισμὸ ποὺ στέλνει τὴν $\sqrt{2}$ στὴν $-\sqrt{2}$ καὶ ἀφήνει ἀναλλοίωτο τὸ i καὶ ὡς ψ τὸν αὐτομορφισμὸ ποὺ στέλνει τὸ i στὸ $-i$ καὶ ἀφήνει ἀναλλοίωτη τὴν $\sqrt{2}$.

Ἀσκήσεις

1. Ἂν $E_1, E_2 \in \mathcal{E}$ καὶ $E_1 \subseteq E_2$, τότε $\mathcal{G}(L/E_1) \supseteq \mathcal{G}(L/E_2)$. Ἐπίσης, ἂν $H_1, H_2 \in \mathcal{O}$ καὶ $H_1 \subseteq H_2$, τότε $\mathcal{F}_L(H_1) \supseteq \mathcal{F}_L(H_2)$.

2. Ἔστω σῶμα K.
(α′) Ἂν $f(X), g(X)$ εἶναι *μονώνυμα* τοῦ $K[X]$ δεῖξτε ὅτι $(f+g)' = f' + g'$ καὶ $(f \cdot g)' = f' \cdot g + g' \cdot f$.
(β′) Ἔστω τώρα $f(X), g(X)$ ὁποιαδήποτε πολυώνυμα τοῦ $K[X]$. Γρᾶψτε τὸ καθένα ὡς ἄθροισμα μονωνύμων (π.χ., ἂν $f(X) = a_nX^n + \cdots + a_1X + a_0$, τότε $f = f_n + \cdots + f_1 + f_0$, ὅπου $f_n = a_nX^n, \ldots, f_1 = a_1X$, $f_0 = a_0$) καὶ ἐφαρμόστε τὸ (α′) γιὰ ν' ἀποδείξετε ὅτι $(f+g)' = f' + g'$ καὶ $(f \cdot g)' = f' \cdot g + g' \cdot f$.
(γ′) Βασιζόμενοι στὸ (β′), ἀποδεῖξτε ἐπαγωγικά, ὅτι, γιὰ κάθε $f \in K[X]$ καὶ κάθε ἀκέραιο $m \geq 2$ ἰσχύει $(f^m)' = m \cdot f^{m-1} \cdot f'$.

3. Ἀναφερόμενοι στὸ παράδειγμα 1, ἀποδεῖξτε, δίχως νὰ χρησιμοποιήσετε τὸ Θεώρημα 2.2.12, ὅτι
$$\mathcal{F}_L(\langle\tau\rangle) = \mathbb{Q}(\sqrt{2}), \quad \mathcal{F}_L(\langle\sigma\tau\rangle) = \mathbb{Q}(\sqrt{6}), \quad \mathcal{F}_L(G) = \mathbb{Q}.$$

4. Ἀναφερόμενοι στὸ παράδειγμα 2, ἀποδεῖξτε ὅτι $\mathcal{F}_L(\langle\sigma\tau\rangle) = \mathbb{Q}(\rho'')$ ὡς ἑξῆς: Παρατηρῆστε ὅτι ἡ σχέση αὐτὴ ἰσοδυναμεῖ μὲ τὴν $\mathcal{G}(L/\mathbb{Q}(\rho'')) = \langle\sigma\tau\rangle$, ὁπότε ἀρκεῖ νὰ δείξετε αὐτὴ τὴν τελευταία, κάτι ἀρκετὰ ἁπλό, ἂν κάνετε χρήση τοῦ θεωρήματος 2.2.12. Ἀνάλογα, δεῖξτε ὅτι $\mathcal{F}_L(\langle\sigma^2\tau\rangle) = \mathbb{Q}(\rho')$.

[9] Παρατηρῆστε ὅτι, ἀφοῦ κάθε ἀλγεβρικὴ ἐπέκταση τοῦ $\mathbb{Q}$ εἶναι διαχωρίσιμη, λόγῳ τοῦ Θεωρήματος 2.2.9, οἱ ἔννοιες *διαχωρίσιμη* καὶ *κανονικὴ* συμπίπτουν.

5. Ἀναφερόμενοι στὸ παράδειγμα 3, ἀποδεῖξτε ὅτι

$$\begin{aligned}\mathcal{F}_L(\langle\sigma^3\tau\rangle) &= \mathbb{Q}((1-i)\rho)\\ \mathcal{F}_L(\langle\sigma^2\rangle) &= \mathbb{Q}(i, \sqrt{2})\\ \mathcal{F}_L(\langle\sigma^2\tau\rangle) &= \mathbb{Q}(i\rho)\\ \mathcal{F}_L(\langle\tau\rangle) &= \mathbb{Q}(\rho).\end{aligned}$$

Ἀποδεῖξτε, ἐπίσης, ὅτι τὰ $(1+i)\rho$ καὶ $(1-i)\rho$ εἶναι ρίζες τοῦ X^4+8, τὸ ὁποῖο εἶναι ἀνάγωγο πάνω ἀπὸ τὸ $\mathbb{Q}$.

6. Ἀποδεῖξτε ὅτι οἱ ρίζες τοῦ $X^4 - X^2 + 1 \in \mathbb{Q}[X]$ εἶναι οἱ ἕκτες ρίζες τοῦ -1. Μετά, ὑπολογῖστε τὸ σῶμα ριζῶν τοῦ πολυωνύμου αὐτοῦ, τὴν ὁμάδα Galois καὶ τὰ ἀντίστοιχα διαγράμματα ὑποομάδων καὶ ἐνδιαμέσων ἐπεκτάσεων.

7. Ἔστω $\rho = \sqrt[3]{(1+\sqrt{5})/2}$ καὶ $\omega \neq 1$ μία κυβικὴ ρίζα τοῦ 1. Ὑπολογῖστε τὶς ρίζες τοῦ $f(X) = X^6 - X^3 - 1 \in \mathbb{Q}[X]$ συναρτήσει τοῦ ρ καὶ τοῦ ω καὶ δεῖξτε ὅτι ἡ ὁμάδα Galois τοῦ $f(X)$ πάνω ἀπὸ τὸ $\mathbb{Q}$ εἶναι ἡ $\mathbf{D}_6$. Κατασκευάστε τὰ διαγράμματα ὑποομάδων καὶ ἐνδιαμέσων ἐπεκτάσεων.

2.3 Δύο ἐφαρμογές

Θεώρημα 2.3.1. *Κάθε πεπερασμένη ἐπέκταση ἑνὸς σώματος χαρακτηριστικῆς 0 εἶναι ἁπλῆ.*

Ἀπόδειξη. Ἔστω K σῶμα χαρακτηριστικῆς 0 [10] καὶ L/K πεπερασμένη ἐπέκταση. Πρῶτα θὰ δείξομε ὅτι ὑπάρχει ἐπέκταση N/L τέτοια ὥστε ἡ ἐπέκταση N/K εἶναι κανονική, ἄρα καὶ Galois (βλ. Θεώρημα 2.2.9). Πράγματι, ὑπάρχει πεπερασμένο πλῆθος στοιχείων $\alpha, \beta, \gamma, \ldots$ τῆς L, τέτοιων ὥστε $L = K(\alpha, \beta, \gamma, \ldots)$. Ἔστω ὅτι τὰ ἐλάχιστα πολυώνυμα αὐτῶν τῶν στοιχείων πάνω ἀπὸ τὸ K εἶναι $f_\alpha, f_\beta, f_\gamma, \ldots$, ἀντιστοίχως καὶ f τὸ γινόμενό τους. Ἂν N εἶναι τὸ σῶμα ριζῶν τοῦ f πάνω ἀπὸ τὸ K, ἡ ἐπέκταση N/K εἶναι κανονικὴ (Θεώρημα 2.2.4) καὶ περιέχει τὸ L, ὁπότε ἀποδείχτηκε ὁ προκαταρτκτικὸς μας ἰσχυρισμός.

Ἀπὸ τὸ Θεώρημα 2.2.12 ξέρομε ὅτι $|\mathcal{G}(N/K)| = [N : K]$, ἄρα ἡ ὁμάδα $\mathcal{G}(N/K)$ εἶναι πεπερασμένη. Ἕπεται ὅτι τὸ πλῆθος τῶν ὑποομάδων της εἶναι πεπερασμένο ἄρα, ἀπὸ τὸ (1) τοῦ ἴδιου Θεωρήματος, καὶ τὸ πλῆθος τῶν ἐνδιαμέσων ἐπεκτάσεων τῆς N/K εἶναι πεπερασμένο. Ἀλλὰ τότε, τὸ ἴδιο θὰ συμβαίνει καὶ μὲ τὴ μικρότερη ἐπέκταση L/K. Χρησιμοποιήσαμε τὴ βοηθητικὴ ἐπέκταση N γιὰ ν' ἀποδείξομε ὅτι τὸ πλῆθος τῶν ἐνδιαμέσων ἐπεκτάσεων τῆς L/K εἶναι πεπερασμένο καί, στὸ ἑξῆς, ξεχνᾶμε τὴν N.

Θεωροῦμε τὸ σύνολο τῶν ἁπλῶν ἐνδιαμέσων ἐπεκτάσεων τῆς L/K· πρόκειται γιὰ μὴ κενὸ σύνολο, ἀφοῦ ἡ τετριμμένη ἐπέκταση K/K εἶναι ἁπλῆ, τὸ ὁποῖο, ἐπιπλέον, εἶναι καὶ πεπερασμένο, βάσει τοῦ συμπεράσματος τῆς ἀμέσως προηγουμένης ἑνότητας. Ἔστω, λοιπόν, ἕνα maximal στοιχεῖο αὐτοῦ τοῦ συνόλου, δηλαδή, μία ἁπλῆ ἐνδιάμεση ἐπέκταση $K(u)$, ἡ ὁποία δὲν περιέχεται *γνησίως* σὲ καμμία ἐνδιάμεση ἁπλῆ ἐπέκταση τῆς L/K, ἐκτός, ἴσως, ἀπὸ τὴν ἴδια τὴν L. Ἂν ὑπάρχουν $a \in K$ καὶ $v \in L$ τέτοια ὥστε $K(au + v) = L$, τότε ἔχομε τελειώσει. Ἂν ὄχι, τότε, γιὰ κάθε $(a, v) \in K \times L$ τὸ $K(au + v)$ εἶναι γνήσιο ὑπόσωμα τοῦ L. Κρατώντας αὐτὸ τὸ συμπέρασμα, θὰ δείξομε τώρα ὅτι κάθε $v \in L$ ἀνήκει στὸ $K(u)$, συμπεραίνοντας ἔτσι ὅτι $L = K(u)$. Πράγματι, ἔστω τυχὸν $v \in L$. Ἀφοῦ τὸ K περιέχει ἄπειρα στοιχεῖα, τὸ σύνολο $\{au + v \ : \ a \in K\}$ εἶναι ἄπειρο. Ἀπὸ τὴν ἄλλη, τὸ πλῆθος τῶν ἁπλῶν ἐνδιαμέσων ἐπεκτάσεων εἶναι πεπερασμένο, ἄρα ὑπάρχουν $a, b \in K$, $a \neq b$, τέτοια ὥστε $K(au + v) = K(bu + v)$. Εἰδικότερα, αὐτὸ συνεπάγεται ὅτι $bu + v \in K(au + v)$, ὁπότε $(bu + v) - (au + v) \in K(au + v)$, ἄρα $(b - a)u \in K(au + v)$ καί, τελικά, $u \in K(au + v)$. Συνεπῶς, $K \subseteq K(u) \subseteq K(au + v) \subset L$, μὲ τὴν τελευταία σχέση ἐγκλεισμοῦ γνήσια. Ἀπὸ τὴ maximal ἰδιότητα τοῦ $K(u)$ συνάγομε τὸ συμπέρασμα ὅτι $K(u) = K(au + v)$, ἄρα $au + v \in K(u)$ καί, τελικά, $v \in K(u)$. □

Θεώρημα 2.3.2. *Ἔστω p περιττὸς πρῶτος. Τὸ κανονικὸ p-γωνο κατασκευάζεται μὲ κανόνα καὶ διαβήτη ἄν, καὶ μόνο ἄν, ὁ p εἶναι πρῶτος τοῦ Fermat, δηλαδὴ τῆς μορφῆς $2^{2^n} + 1$.*

Ἀπόδειξη. Μία πρώτη παρατήρηση εἶναι ὅτι ἂν ὁ $p = 2^k + 1$ εἶναι πρῶτος, τότε ὁ k εἶναι δύναμη τοῦ 2. Γιατί, στὴν ἀντίθετη περίπτωση, ὁ k ἔχει κάποιο περιττὸ διαιρέτη d ὁπότε, θέτοντας $k = dm$ ἔχομε $p = (2^m)^d + 1 = (2^m + 1)(2^{m(d-1)} - 2^{m(d-2)} + \cdots - 2^m + 1)$· ἀντίφαση μὲ τὸ ὅτι ὁ p εἶναι πρῶτος. Συνεπῶς, ἀρκεῖ νὰ ἀποδείξομε ὅτι τὸ κανονικὸ p-γωνο κατασκευάζεται ἄν, καὶ μόνο ἄν, ὁ p εἶναι τῆς μορφῆς $2^k + 1$.

Πρὶν προχωρήσομε στὴν κυρίως ἀπόδειξη θέτομε

$$\theta = \frac{2\pi}{p}, \ \zeta = \cos\theta + i\sin\theta, \ L = \mathbb{Q}(\zeta), \ E = \mathbb{Q}(\cos\theta),$$

[10] Εἰδικώτερα, αὐτὸ συνεπάγεται ὅτι τὸ K ἔχει ἄπειρα στοιχεῖα.

Τὸ ζ εἶναι p-τάξεως ρίζα τῆς μονάδος καί, ἀπὸ τὴν πρόταση Β′.3 (παράρτημα Β′), ἔχει ἐλάχιστο πολυώνυμο τὸ *κυκλοτομικὸ πολυώνυμο* $f_p(X) = (X^p - 1)/(X - 1) =$ $X^{p-1} + X^{p-2} + \cdots + X + 1$, τοῦ ὁποίου οἱ ρίζες εἶναι: $\zeta, \zeta^2, \ldots, \zeta^{p-1}$.

Ἔστω πρῶτα ὅτι τὸ κανονικὸ p-γωνο κατασκευάζεται. Τότε ὁ ἀριθμὸς $\cos\theta$ κατασκευάζεται ἄρα, ἀπὸ τὸ Θεώρημα 1.2.2, $[E : \mathbb{Q}] = 2^n$ γιὰ κάποιο μὴ ἀρνητικὸ ἀκέραιο n. Ἐπειδὴ $\cos\theta = (\zeta + \zeta^{-1})/2$, τὸ ζ εἶναι ρίζα τοῦ $X^2 - 2\cos\theta \cdot X + 1 \in E[X]$. Τὸ πολυώνυμο αὐτὸ εἶναι ἀνάγωγο στὸ $E[X]$ διότι οἱ ρίζες τοῦ ζ, ζ^{-1} δὲν εἶναι πραγματικές, ἄρα δὲν ἀνήκουν στὸ E. Συνεπῶς, $[L : \mathbb{Q}] = 2^{n+1}$. Ὅμως $[L : \mathbb{Q}] = \deg f_p = p - 1$, ἄρα $p = 2^{n+1} + 1$.

Ἀντιστρόφως, ἔστω $p = 2^k + 1$. Θὰ δείξομε ὅτι ὁ ἀριθμὸς $\cos\theta$ κατασκευάζεται μὲ κανόνα καὶ διαβήτη. Ἀπὸ τὴ στοιχειώδη Εὐκλείδιο Γεωμετρία ξέρομε νὰ κατασκευάζομε μὲ κανόνα καὶ διαβήτη τὶς ρίζες ὁποιασδήποτε δευτεροβάθμιας ἐξισώσεως, τῆς ὁποίας οἱ συντελεστὲς εἶναι κατασκευάσιμα μήκη. Ἂν λοιπὸν καταφέρομε νὰ δείξομε ὅτι ὑπάρχει μία πεπερασμένη ἁλυσσίδα διαδοχικῶν ἐπεκτάσεων

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n = E\,, \tag{2.2}$$

εἰς τρόπον ὥστε κάθε $[E_j : E_{j-1}] = 2$, τότε θὰ ἔχομε τὴν ἑξῆς κατάσταση: Τὰ στοιχεῖα τοῦ E_1 θὰ εἶναι κατασκευάσιμα, ὡς ρίζες δευτεροβαθμίων πολυωνύμων μὲ συντελεστὲς ἀπὸ τὸ $\mathbb{Q}$. Μετά, τὰ στοιχεῖα τοῦ E_2 εἶναι κατασκευάσιμα, ὡς ρίζες δευτεροβαθμίων πολυωνύμων μὲ συντελεστὲς ἀπὸ τὸ E_1 κ.ὄ.κ., μέχρις ὅτου καταλήξομε στὴν κατασκευασιμότητα τῶν στοιχείων τοῦ E_n, ἄρα καὶ τοῦ $\cos\theta$. Μένει λοιπὸν νὰ ἀποδείξομε τὴν ὕπαρξη μιᾶς ἁλυσσίδος ἐπεκτάσεων (2.2) μὲ τὶς προαναφερθεῖσες ἰδιότητες.

Τὸ L εἶναι σῶμα ριζῶν τοῦ f_p πάνω ἀπ' τὸ $\mathbb{Q}$, ἄρα ἡ ἐπέκταση $L/\mathbb{Q}$ εἶναι Galois. Ἡ ὁμάδα Galois $\mathcal{G}(L/\mathbb{Q})$ εἶναι ἰσόμορφη μὲ τὴν $\mathbb{Z}_p^*$ (πολλαπλασιαστικὴ ὁμάδα τῶν μὴ μηδενικῶν κλάσεων ὑπολοίπων mod p)· βλ. πρόταση (1) στὴν ἑνότητα 2.4.1. Εἰδικώτερα, ἡ $\mathcal{G}(L/\mathbb{Q})$ εἶναι κυκλική, ἄρα ἡ $\mathcal{G}(L/E)$, εἶναι κανονικὴ ὑποομάδα της. Τότε, τὸ (4) τοῦ Θεωρήματος 2.2.12, ἐφαρμοζόμενο στὴν ἐνδιάμεση ἐπέκταση E τῆς $L/\mathbb{Q}$ μᾶς δίνει ὅτι ἡ ἐπέκταση $E/\mathbb{Q}$ εἶναι Galois. Ἐπιπλέον, ὁ βαθμὸς $[E : \mathbb{Q}]$ εἶναι διαιρέτης τοῦ $[L : \mathbb{Q}]$ καί, λόγῳ τοῦ (2) τοῦ Θεωρήματος 2.2.12, $[L : \mathbb{Q}] = |\mathcal{G}(L/\mathbb{Q})| = |\mathbb{Z}_p^*| = p - 1 = 2^k$. Ἄρα, $[E : \mathbb{Q}] = 2^n$ γιὰ κάποιο ἀκέραιο n.[11] Τότε $|\mathcal{G}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 2^n$ καί, ἀκόμη, ἀπὸ τὸ (4) τοῦ Θεωρήματος 2.2.12, ἡ ὁμάδα $\mathcal{G}(E/\mathbb{Q})$ εἶναι ἰσόμορφη μὲ μία ὁμάδα-πηλῖκο τῆς κυκλικῆς ὁμάδας $\mathcal{G}(L/\mathbb{Q})$, ἄρα εἶναι κυκλική, τάξεως 2^n. Ἀπὸ τὸ (3) τῆς ἑνότητας 2.4.1, συμπεραίνομε τότε ὅτι ὑπάρχει μία ἁλυσσίδα ὑποομάδων

$$G_n = \langle \mathbf{id} \rangle \triangleleft G_{n-1} \triangleleft G_{n-2} \triangleleft \cdots \triangleleft G_0 = G\,,$$

μὲ $|G_j| = 2^{n-j}$ γιὰ κάθε $j = 0, 1, \ldots, n$.

Ἀφ' ἑτέρου, τὸ Θεώρημα 2.2.12, λέει ὅτι σὲ αὐτὴ τὴν ἁλυσσίδα ὑποομάδων ἀντιστοιχεῖ ἡ ἁλυσσίδα τῶν ἐνδιαμέσων ἐπεκτάσεων

$$E = E_n \supseteq E_{n-1} \supseteq E_{n-2} \supseteq \cdots \supseteq E_0 = \mathbb{Q}\,,$$

ὅπου, βεβαίως, $\mathcal{G}(E/E_j) = G_j$. Θὰ δείξομε ὅτι, γιὰ κάθε $j = 1, \ldots, n$, ἰσχύει $[E_j : E_{j-1}] = 2$.

[11] Ἐπειδὴ $[L : E] = 2$, εἶναι $n = k - 1$, ἀλλὰ αὐτὸ δὲν μᾶς χρειάζεται στὴν ἀπόδειξη.

Ἐφαρμόζομε τὸ Θεώρημα 2.2.12 στὴν ἐπέκταση $E/\mathbb{Q}$.

$$\begin{tikzcd}
E = E_n \arrow[r, leftrightarrow] \arrow[d, dash, "|G_k|"'] & G_n = \langle \mathbf{id} \rangle \arrow[d, dash] \\
E_k \arrow[r, leftrightarrow] \arrow[d, dash] & G_k \arrow[d, dash] \\
\mathcal{G}(E/\mathbb{Q}) = G_0 \arrow[r, leftrightarrow] & E_0 = \mathbb{Q}
\end{tikzcd} \qquad |G_k| = 2^{n-k}$$

Ἀπὸ τὸ (3) συμπεραίνομε ὅτι $[E : E_j] = |\mathcal{G}(E/E_j)| = |\mathcal{G}_j| = 2^{n-j}$ καί, ὁμοίως, $[E : E_{j-1}] = |\mathcal{G}(E/E_{j-1})| = |\mathcal{G}_{j-1}| = 2^{n-j+1}$. Ἄρα, $[E_j : E_{j-1}] = [E : E_{j-1}]/[E : E_j] = 2$.

□

2.4 Επιλυση πολυωνυμικων εξισωσεων με ριζικα

Ἔστω $f(X) \in \mathbb{Q}[X]$. Θέλομε νὰ βροῦμε ἀναγκαῖες συνθῆκες γιὰ νὰ ἐκφράζονται οἱ λύσεις τῆς $f(x) = 0$ μὲ ριζικά, ἤ, ὅπως θὰ λέμε γιὰ συντομία, νὰ εἶναι τὸ $f(X)$ *ἐπιλύσιμο μὲ ριζικά*.[12] Αὐτὸ σημαίνει ὅτι ὅλες οἱ ρίζες τοῦ $f(X)$ θὰ μοιάζουν, γιὰ παράδειγμα, μὲ κάτι σὰν τὴν παρακάτω ἔκφραση:

$$\sqrt[3]{q}\sqrt[5]{\frac{r+\sqrt{s}}{t}} + \sqrt[4]{u+\sqrt[3]{v}}\,,$$

ὅπου $q, r, s, t, u, v \in \mathbb{Q}$. Γενικά, ὅταν τὸ $f(X)$ εἶναι ἐπιλύσιμο μὲ ριζικά, ἐμφανίζονται πεπερασμένα τὸ πλῆθος ριζικά, τῶν ὁποίων οἱ τάξεις μπορεῖ νὰ ὑποτεθοῦν, χωρὶς βλάβη τῆς γενικότητος, πρῶτοι ἀριθμοὶ $p_1, p_2, p_3, \ldots p_\nu$, λόγῳ τῆς σχέσεως $\sqrt[lm]{a} = \sqrt[l]{\sqrt[m]{a}}$. Γιὰ νὰ διατυπώσομε σὲ πιὸ αὐστηρὴ τυπικὴ γλῶσσα αὐτὴ τὴν ἔννοια ἐπιλυσιμότητας, χρειαζόμαστε δύο ὁρισμούς:

Ὁρισμὸς 2.4.1. *Μία πεπερασμένη ἐπέκταση L/K λέγεται ριζική, ἂν ὑπάρχει ἁλυσίδα ἐπεκτάσεων*

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{j-1} \subseteq K_j \subseteq \ldots \subseteq K_n = L$$

ποὺ ἱκανοποιεῖ τὴν ἑξῆς συνθήκη: Γιὰ κάθε $j = 1, \ldots, n$ ὑπάρχει $\alpha_j \in K_j$ καὶ πρῶτος p_j, τέτοιοι ὥστε $a_j^{p_j} \in K_{j-1}$.

Ἂν, στὸν παραπάνω ὁρισμό, θέσομε $a_j^{p_j} = b_{j-1} \in K_{j-1}$ $(j = 1, \ldots, n)$, τότε, ἡ σχέση $a_j^{p_j} \in K_{j-1}$ διατυπώνεται, παραστατικώτερα: $a_j = \sqrt[p_j]{b_{j-1}}$, ἄρα, ἡ ἁλυσίδα, ποὺ ἐμφανίζεται στὸν ὁρισμό, γράφεται

$$K = K_0 \subseteq K_0(\sqrt[p_1]{b_0}) = K_1 \subseteq \ldots \subseteq K_{j-1}(\sqrt[p_j]{b_{j-1}}) = K_j \subseteq \ldots \subseteq K_{n-1}(\sqrt[p_n]{b_{n-1}}) = K_n.$$

Προσοχὴ ὅμως! Αὐτὴ ἡ διατύπωση τοῦ ὁρισμοῦ εἶναι μὲν πιὸ παραστατική, ἀλλὰ ἔχει τὸ σοβαρὸ μειονέκτημα τοῦ συμβολισμοῦ $\sqrt[p]{b}$. Διότι, ὅταν ἐμφανίζεται σ' ἕνα τῦπο τὸ σύμβολο $\sqrt[p]{b}$, δὲν εἶναι σαφὲς ποιὰ ἀπ' ὅλες τὶς p τὸ πλῆθος p-τάξεως ρίζες τοῦ b ἐννοεῖται. Γιὰ τὸν λόγο αὐτό, προτιμώτερη εἶναι ἡ διατύπωση τοῦ ὁρισμοῦ 2.4.1.

Τὴν ἐπιλυσιμότητα μὲ ριζικὰ ἑνὸς πολυωνύμου $f(X)$ μποροῦμε νὰ διατυπώσομε τώρα σὲ πιὸ τυπικὴ γλῶσσα ὡς ἑξῆς:

Ὁρισμὸς 2.4.2. *Τὸ μὴ σταθερὸ πολυώνυμο $f(X) \in \mathbb{Q}[X]$ λέμε ὅτι εἶναι ἐπιλύσιμο μὲ ριζικὰ ἤ, ἰσοδύναμα, ὅτι ἡ ἐξίσωση $f(x) = 0$ ἐπιλύεται (εἶναι ἐπιλύσιμη) μὲ ριζικά, ἂν ὑπάρχει μία πεπερασμένη ριζικὴ ἐπέκταση τοῦ $\mathbb{Q}$, ἡ ὁποία περιέχει ὅλες τὶς ρίζες τοῦ $f(X)$.*[13]

Στόχος αὐτῆς τῆς ἑνότητας εἶναι ν' ἀποδείξομε τὸ ἑξῆς:

Θεώρημα 2.4.3. *Γιὰ κάθε πρῶτο $p \geq 5$ ὑπάρχει πολυώνυμο βαθμοῦ p, μὲ ρητοὺς συντελεστές, τὸ ὁποῖο δὲν εἶναι ἐπιλύσιμο μὲ ριζικά.*

Ἡ ἀπόδειξη τοῦ θεωρήματος αὐτοῦ θὰ δοθεῖ στὴ σελίδα 47 καὶ θὰ προκύψει ὡς συνέπεια μιᾶς σειρᾶς προτάσεων, οἱ ὁποῖες ἀκολουθοῦν ἀμέσως παρακάτω.

[12] Παρατηρεῖστε τὴ διαφορὰ τοῦ x ἀπὸ τὸ X. Εἶναι σοβαρὸ "ὀρθογραφικὸ" λάθος νὰ γράφομε $f(X) = 0$, διότι αὐτὸ σημαίνει ὅτι τὸ *πολυώνυμο* $f(X)$ εἶναι μηδενικὸ καί, ἄρα, ὅλοι οἱ συντελεστές του εἶναι 0.

[13] Θεωροῦμε ὅτι ἐργαζόμαστε μέσα στὸ $\mathbb{C}$.

Λῆμμα 2.4.4. *Ἂν τὸ μὴ σταθερὸ $f(X) \in \mathbb{Q}[X]$ εἶναι ἐπιλύσιμο μὲ ριζικά, τότε ὑπάρχουν:*
(1) Ἐπέκταση $K_0 = \mathbb{Q}(\zeta_1, \ldots, \zeta_n)$, ὅπου, γιὰ κάθε $j = 1, \ldots, n$, εἶναι ζ_j πρωταρχικὴ p_j-τάξεως ρίζα τῆς μονάδας γιὰ κάποιον πρῶτο p_j.
(2) Ἁλυσίδα ἐπεκτάσεων

$$K_0 \subset K_1 \subset \ldots \subset K_{j-1} \subset K_j \subset \ldots \subset K_m,$$

στὴν ὁποία κάθε ἐπέκταση K_j/K_{j-1} εἶναι Galois, ὁ βαθμός της εἶναι πρῶτος ($j = 1, \ldots, m$) καὶ ὅλες οἱ ρίζες τοῦ $f(X)$ ἀνήκουν στὸ K_m.

Ἀπόδειξη Σύμφωνα μὲ τὸν Ὁρισμὸ 2.4.2, ὑπάρχει ἁλυσίδα ἐπεκτάσεων

$$\mathbb{Q} = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_{j-1} \subseteq K'_j \subseteq \ldots \subseteq K'_n,$$

μὲ τὶς ἑξῆς ἰδιότητες: (1) Τὸ K'_n περιέχει ὅλες τὶς ρίζες τοῦ $f(X)$, καὶ (2) γιὰ κάθε $j = 1, \ldots, n$ ὑπάρχει πρῶτος p_j καὶ $\alpha_j \in K'_j$, ἔτσι ὥστε $K'_j = K'_{j-1}(\alpha_j)$ καὶ $\alpha_j^{p_j} \in K'_{j-1}$.
Ἔστω ὅτι, γιὰ $j = 1, \ldots, n$, εἶναι ζ_j πρωταρχικὴ p_j-ρίζα τῆς μονάδος. Θέτομε $K_0 = K'_0(\zeta_1, \ldots, \zeta_n) = \mathbb{Q}(\zeta_1, \ldots, \zeta_n)$ καὶ $K_j = K'_j(\zeta_1, \ldots, \zeta_n)$ γιὰ $j = 1, \ldots, n$. Ἔτσι, παίρνομε τὴν ἁλυσίδα

$$K_0 = \mathbb{Q}_0 \subseteq K_1 \subseteq \ldots \subseteq K_{j-1} \subseteq K_j \subseteq \ldots \subseteq K_n. \tag{2.3}$$

Προφανῶς, τὸ K_n περιέχει ὅλες τὶς ρίζες τοῦ $f(X)$. Ἐπίσης, $K_j = K_{j-1}(\alpha_j)$ γιὰ κάθε $j = 1, \ldots, n$. Πράγματι,

$$K_{j-1}(\alpha_j) = K'_{j-1}(\zeta_1, \ldots, \zeta_n, \alpha_j) = K'_{j-1}(\alpha_j)(\zeta_1, \ldots, \zeta_n) = K'_j(\zeta_1, \ldots, \zeta_n) = K_j.$$

Ἔστω ὅτι γιὰ κάποιο j εἶναι $K_j \neq K_{j-1}$. Αὐτὸ ἰσοδυναμεῖ μὲ τὸ ὅτι $\alpha_j \notin K_{j-1}$. Σ' αὐτὴ τὴν περίπτωση θὰ ἀποδείξομε ὅτι ἡ ἐπέκταση K_j/K_{j-1} εἶναι Galois καὶ ὁ βαθμός της εἶναι p_j.

Ἀπόδειξη τοῦ ἰσχυρισμοῦ αὐτοῦ: Γιὰ ἁπλοποίηση τοῦ συμβολισμοῦ, ἂς θέσομε $\alpha_j = \alpha, p_j = p, \zeta = \zeta_j$. Παρατηρῆστε ὅτι $\zeta \in K_{j-1} \subset K_j$. Ἐξ ὑποθέσεως, $\alpha^p = b$ γιὰ κάποιο $b \in K_{j-1}$, δηλαδὴ τὸ α εἶναι ρίζα τοῦ $g(X) = X^p - b \in K_{j-1}[X]$. Οἱ ρίζες αὐτοῦ τοῦ πολυωνύμου εἶναι οἱ $\alpha, \alpha\zeta, \ldots, \alpha\zeta^{p-1}$ καὶ ὅλες ἀνήκουν στὸ K_j. Εἶναι φανερὸ τώρα ὅτι τὸ K_j εἶναι σῶμα ριζῶν τοῦ $g(X)$ πάνω ἀπὸ τὸ K_{j-1}, ἄρα ἡ ἐπέκταση K_j/K_{j-1} εἶναι Galois. Γιὰ νὰ δείξομε ὅτι ὁ βαθμὸς της εἶναι p, ἀρκεῖ νὰ δείξομε ὅτι τὸ $g(X)$ εἶναι ἀνάγωγο στὸ $K_{j-1}[X]$. Ἂν δὲν ἦταν, θὰ εἶχε ἕνα ἀνάγωγο παράγοντα $h(X) \in K_{j-1}[X]$, τοῦ ὁποίου οἱ ρίζες θὰ ἦταν κάποια, *ἀλλὰ ὄχι ὅλα*, ἐκ τῶν $\alpha\zeta^k$. Δηλαδή, $h(X) = (X - \alpha\zeta^{k_1}) \ldots (X - \alpha\zeta^{k_m})$ ὅπου $1 \leq m < p$. Εἰδικώτερα, ὁ σταθερὸς ὅρος τοῦ $h(X)$ ἀνήκει στὸ K_{j-1}. Ἄρα, $(-1)^m \alpha^m \zeta^k \in K_{j-1}$, ὅπου $k = k_1 + \ldots + k_m$. Ὅμως $\zeta \in K_{j-1}$, ἄρα $\alpha^m \in K_{j-1}$. Ἐπειδὴ $(m, p) = 1$, ὑπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ὥστε $mx + py = 1$, ὁπότε $\alpha = (\alpha^m)^x (\alpha^p)^y$. Ἀλλὰ $\alpha^m, \alpha^p \in K_{j-1}$, ἄρα $\alpha \in K_{j-1}$, ποὺ ἀντίκειται στὴν ὑπόθεση ὅτι $K_{j-1} \neq K_j$. Αὐτὸ ὁλοκληρώνει τὴν ἀπόδειξη τοῦ ἰσχυρισμοῦ.

Σύμφωνα μὲ ὅ,τι μόλις ἀποδείξαμε, ἂν στὴν ἁλυσίδα (2.3) διαγράψομε τυχὸν ἐπαναλήψεις –δηλαδή, ἂν γιὰ κάποιο j εἶναι $K_j = K_{j-1}$, τότε διαγράφομε τὸ ἕνα ἐκ τῶν K_j, K_{j-1}– τότε καταλήγομε σὲ μιὰ ἁλυσίδα

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{j-1} \subseteq K_j \subseteq \ldots \subseteq K_m,$$

($m \leq n$), γιὰ τὴν ὁποία ἰσχύει ὅτι ἡ ἐπέκταση K_j/K_{j-1} εἶναι Galois καὶ ὁ βαθμός της εἶναι πρῶτος γιὰ κάθε $j = 1, \ldots, m$. □

Λῆμμα 2.4.5. *Ἂν K_0 εἶναι τὸ σῶμα, ποὺ ἀναφέρεται στὴν ἐκφώνηση τοῦ Λήμματος 2.4.4, τότε ὑπάρχει μία ἁλυσίδα ἐπεκτάσεων*

$$\mathbb{Q} = M_0 \subset M_1 \subset \cdots \subset M_r = K_0,$$

τέτοια ὥστε κάθε ἐπέκταση M_i/M_{i-1} εἶναι Galois καὶ ὁ βαθμὸς εἶναι πρῶτος.

Ἀπόδειξη. Ἔχομε τὴν ἑξῆς ἁλυσίδα ἐπεκτάσεων:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_1) \subset \mathbb{Q}(\zeta_1, \zeta_2) \subset \mathbb{Q}(\zeta_1, \zeta_2, \zeta_3) \subset \cdots \subset \mathbb{Q}(\zeta_1, \zeta_2, \ldots, \zeta_\nu) = K\ .$$

Τώρα, ἡ βοηθητικὴ πρόταση δ′ τοῦ ὑπο-ἐδαφίου 2.4.1 (βλ. παρακάτω, στὴ σελίδα 47 «Βοηθητικὲς προτάσεις, ποὺ χρησιμοποιήθηκαν») ἐφαρμοζόμενο σὲ κάθε μία ἀπὸ τὶς ἐπεκτάσεις

$$\mathbb{Q}(\zeta_1)/\mathbb{Q}, \quad \mathbb{Q}(\zeta_1, \zeta_2)/\mathbb{Q}(\zeta_1), \quad \mathbb{Q}(\zeta_1, \zeta_2, \zeta_3)/\mathbb{Q}(\zeta_1, \zeta_2), \ldots$$

ἀποδεικνύει τὸν ἰσχυρισμό μας. □

Πρόταση 2.4.6. *Ἂν τὸ μὴ σταθερὸ $f(X) \in \mathbb{Q}[X]$ εἶναι ἐπιλύσιμο μὲ ῥιζικά, τότε ὑπάρχει μία ἁλυσίδα ἐπεκτάσεων*

$$\mathbb{Q} = E_0 \subset E_1 \subset \ldots \subset E_{j-1} \subset E_j \ldots \subset E_s,$$

τέτοια ὥστε, κάθε ἐπέκταση E_j/E_{j-1} εἶναι Galois βαθμο ῦ πρώτου καὶ τὸ E_s περιέχει ὅλες τὶς ῥίζες τοῦ $f(X) \in \mathbb{Q}[X]$.

Ἀπόδειξη. Ἔστω ἡ ἁλυσίδα ἐπεκτάσεων $K_0 \subset K_1 \subset \ldots \subset K_m$, ποὺ μᾶς ἐξασφαλίζει τὸ Λῆμμα 2.4.4 καὶ $\mathbb{Q} = M_0 \subset M_1 \subset \cdots \subset M_r = K_0$ ἡ ἁλυσίδα ἐπεκτάσεων τοῦ Λήμματος 2.4.5. Τότε οἱ διαδοχικὲς ἐπεκτάσεις

$$\mathbb{Q} \subset M_1 \subset \cdots \subset M_r = K_0 \subset K_1 \subset \ldots \subset K_m$$

ἀποτελοῦν μία ἁλυσίδα, ποῦ ἱκανοποιεῖ τὶς ἀπαιτήσεις τῆς ἐκφώνησης (μὲ $s = r + m$ καὶ $E_s = K_m$). □

Πρόταση 2.4.7. *Ἂν τὸ μὴ σταθερὸ $f(X) \in \mathbb{Q}[X]$ εἶναι ἐπιλύσιμο μὲ ῥιζικὰ καὶ L εἶναι τὸ σῶμα ῥιζῶν τοῦ $f(X)$ πάνω ἀπὸ τὸ $\mathbb{Q}$, τότε ὑπάρχει μία ἁλυσίδα ἐπεκτάσεων*

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = L,$$

τέτοια ὥστε κάθε ἐπέκταση L_i/L_{i-1} εἶναι Galois, τῆς ὁποίας ὁ βαθμὸς εἶναι πρῶτος.

Ἀπόδειξη. Θεωροῦμε τὴν ἁλυσίδα τῆς Πρότασης 2.4.6 καὶ θέτομε $L_i = E_i \cap L$, ὁπότε ἔχομε τὴν ἁλυσίδα

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_s = L.$$

Διαγράφοντας τυχὸν ἐπαναλήψεις στὴν παραπάνω ἁλυσίδα, παίρνομε μία ἁλυσίδα (μικροτέρου μήκους ἐνδεχομένως)

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = L\ ,$$

$t \leq s$ ὅπου $L_{i-1} \neq L_i$ γιὰ ὅλα τὰ i. Λόγῳ τοῦ Θεωρήματος 2.3.1, γιὰ κάθε i ὑπάρχει $\lambda_i \in L_i$ τέτοιο ὥστε $L_i = L_{i-1}(\lambda_i)$. Θὰ δείξομε ὅτι $E_i = E_{i-1}(\lambda_i)$. Ἔχομε τὶς διαδοχικὲς ἐπεκτάσεις

$E_{i-1} \subseteq E_{i-1}(\lambda_i) \subseteq E_i$. Ἐπειδὴ ὁ βαθμὸς $[E_i : E_{i-1}]$ εἶναι πρῶτος, θὰ πρέπει $E_{i-1}(\lambda_i) = E_i$ εἴτε E_{i-1}. Στὴ δεύτερη περίπτωση, $\lambda_i \in E_{i-1}$. Ὅμως $\lambda_i \in L$, ἄρα $\lambda_i \in L \cap E_{i-1} = L_{i-1}$ καὶ $L_i = L_{i-1}$, ἄτοπο· ἔτσι, μένει ἡ περίπτωση $E_i = E_{i-1}(\lambda_i)$. Ὕστερα ἀπὸ αὐτὸ μποροῦμε νὰ δείξομε ὅτι ἡ ἐπέκταση L_i/L_{i-1} εἶναι Galois καὶ ὁ βαθμὸς της εἶναι πρῶτος. Πράγματι, ἔστω $h(X) \in E_{i-1}[X]$ τὸ ἐλάχιστο πολυώνυμο τοῦ λ_i πάνω ἀπὸ τὸ E_{i-1}. Ἐπειδὴ ἡ E_i/E_{i-1} εἶναι Galois, ὅλες οἱ ρίζες τοῦ $h(X)$ ἀνήκουν στὸ E_i. Ἐπειδὴ ἡ $L/\mathbb{Q}$ εἶναι Galois (ὡς σῶμα ριζῶν τοῦ $f(X) \in \mathbb{Q}[X]$), ἡ L/E_{i-1} εἶναι ἐπίσης Galois, ἄρα (ἀφοῦ $\lambda_i \in L$) ὅλες οἱ ρίζες τοῦ $h(X)$ ἀνήκουν καὶ στὸ L· ἕπεται ὅτι ὅλες οἱ ρίζες τοῦ $h(X)$ ἀνήκουν στὸ $L \cap E_i = L_i$. Εἰδικώτερα, οἱ συντελεστὲς τοῦ $h(X)$ ἀνήκουν στὸ L, ἄρα καὶ στὸ $L \cap E_{i-1} = L_{i-1}$. Ἀλλὰ τὸ $h(X)$ εἶναι ἀνάγωγο πάνω ἀπὸ τὸ E_{i-1}, ἄρα, κατὰ μείζονα λόγο, εἶναι ἀνάγωγο καὶ πάνω ἀπὸ τὸ L_{i-1}. Ἔτσι, τὸ ἐλάχιστο πολυώνυμο τοῦ λ_i πάνω ἀπὸ τὸ E_{i-1} καὶ πάνω ἀπὸ τὸ L_{i-1} εἶναι, καὶ στὶς δύο περιπτώσεις, τὸ $h(X)$ καί, ὅπως εἴδαμε, οἱ ρίζες τοῦ $h(X)$ ἀνήκουν ὅλες στὸ L_i. Συνεπῶς, τὸ L_i εἶναι σῶμα ριζῶν τοῦ $h(X) \in L_{i-1}[X]$, ποὺ σημαίνει ὅτι ἡ L_i/L_{i-1} εἶναι Galois. Ἐπίσης, $[L_i : L_{i-1}] = \deg h = [E_i : E_{i-1}] =$ πρῶτος. □

Πρόταση 2.4.8. *Ὑπάρχει μία ἁλυσίδα ὑποομάδων τῆς $G = \mathcal{G}(L/\mathbb{Q})$ ὡς ἑξῆς:*

$$G = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_t = \langle \mathbf{id} \rangle$$

($A \rhd B$ σημαίνει B κανονικὴ ὑποομάδα τῆς *A), τέτοια ὥστε, γιὰ κάθε $j = 1, \ldots, t$, ἡ τάξη τῆς ὁμάδας πηλῖκο G_{j-1}/G_j εἶναι πρῶτος ἀριθμός.*

Ἀπόδειξη. Ἐπειδὴ ἡ ἐπέκταση $L/\mathbb{Q}$ εἶναι Galois, στὴν ἁλυσίδα ἐνδιαμέσων ἐπεκτάσεων τῆς Πρότασης 2.4.7 ἀντιστοιχεῖ μέσῳ τῆς ἀντιστοιχίας Galois μία ἁλυσίδα ὑποομάδων

$$G = \mathcal{G}(L/\mathbb{Q}) = G_0 > G_1 > \cdots > G_{j-1} > G_j > \ldots > G_{t-1} > G_t = \langle \mathbf{id} \rangle,$$

ὅπου $G_j = \mathcal{G}(L/L_j)$. Ἔστω ἕνα ὁποιοδήποτε $j \in \{1, \ldots, \}t$. Ἡ ἐπέκταση $L/\mathbb{Q}$ εἶναι Galois, ἄρα καὶ ἡ ἐπέκταση L/L_{j-1} εἶναι Galois, βάσει τοῦ Θεωρήματος 2.2.12 (3). Θεωροῦμε τώρα τὶς διαδοχικὲς ἐπεκτάσεις $L \supset L_j \supset L_{j-1}$ καὶ ἐφαρμόζομε τὸ Θεώρημα 2.2.12. Ἐπειδὴ ἡ L_{j-1}/L_j εἶναι Galois, τὸ Θεώρημα 2.2.12 (4) συνεπάγεται ὅτι ἡ $\mathcal{G}(L/L_j)$ εἶναι κανονικὴ ὑποομάδα τῆς $\mathcal{G}(L/L_{j-1})$, δηλαδή, ἡ G_j εἶναι κανονικὴ ὑποομάδα τῆς G_{i-1} καὶ $G_{j-1}/G_j \cong \mathcal{G}(L_j/L_{j-1})$. Ἐπίσης, ἀφοῦ ἡ ἐπέκταση L_j/L_{j-1} εἶναι Galois, ἡ τάξη τῆς ὁμάδος $\mathcal{G}(L_j/L_{j-1})$ ἰσοῦται μὲ τὸ βαθμὸ $[L_j : L_{j-1}]$ –λόγῳ τοῦ Θεωρήματος 2.2.12 (2)– ἄρα εἶναι πρῶτος ἀριθμός, ὁπότε καὶ ἡ τάξη τῆς ὁμάδας G_{j-1}/G_j εἶναι πρῶτος ἀριθμός. □

Ὁρισμὸς 2.4.9. *Μία πεπερασμένη ὁμάδα G λέγεται ἐπιλύσιμη ἂν ὑπάρχει ἁλυσσίδα ὑποομάδων*

$$G = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_t = \langle \mathbf{id} \rangle,$$

τέτοια ὥστε, γιὰ κάθε $j = 1, \ldots, t$, ἡ ὁμάδα-πηλῖκο G_{j-1}/G_j νὰ εἶναι ἀβελιανή.

Ἄμεση συνέπεια τῆς Πρότασης 2.4.8 εἶναι τὸ ἑξῆς:

Θεώρημα 2.4.10. *Ἂν τὸ μὴ μηδενικὸ $f(X) \in \mathbb{Q}[X]$ εἶναι ἐπιλύσιμο μὲ ριζικά, τότε ἡ ὁμάδα Galois τοῦ πολυωνύμου $f(X)$ εἶναι ἐπιλύσιμη ὑπὸ τὴν ἔννοιαν τοῦ Ὁρισμοῦ 2.4.9.*

Ἀπόδειξη. Ἔστω L τὸ σῶμα ριζῶν τοῦ ἐπιλύσιμου μὲ ριζικὰ πολυωνύμου $f(X) \in \mathbb{Q}[X]$, ὁπότε ἡ ὁμάδα Galois τοῦ $f(X)$ εἶναι ἡ $\mathcal{G}(L/\mathbb{Q})$ (βλ. Θεώρημα-Ὁρισμὸς 2.1.2). Θεωροῦμε τὴν ἁλυσίδα ἐπεκτάσεων, ποὺ μᾶς ἐξασφαλίζει ἡ Πρόταση 2.4.8. Γιὰ κάθε $j = 1, \ldots, t$, ἡ τάξη τῆς ὁμάδας G_{j-1}/G_j εἶναι πρῶτος ἄριθμός, ὁπότε ἡ ὁμάδα αὐτὴ εἶναι κυκλική[14], ἄρα καὶ ἀβελιανή. □

Στὸ ὑπόλοιπο αὐτῆς τῆς ἑνότητας θὰ δείξομε ὅτι ὑπάρχουν πολυώνυμα μὲ ρητοὺς συντελεστές, βαθμοῦ ≥ 5, τῶν ὁποίων ἡ ὁμάδα Galois δὲν εἶναι ἐπιλύσιμη. Συνεπῶς, βάσει τοῦ Θεωρήματος 2.4.10, θὰ ὁδηγηθοῦμε στὸ συμπέρασμα ὅτι τὰ πολυ;ωνυμα αὐτὰ δὲν εἶναι ἐπιλύσιμα μὲ ριζικά.

Θεώρημα 2.4.11. *Ἔστω πρῶτος p. Κάθε πολυώνυμο βαθμοῦ p μὲ ρητοὺς συντελεστές, ἀνάγωγο πάνω ἀπὸ τὸ $\mathbb{Q}$, τοῦ ὁποίου ἀκριβῶς $p-2$ ρίζες εἶναι πραγματικές, ἔχει ὁμάδα Galois τὴ συμμετρικὴ ὁμάδα $\mathbf{S}_p$.*

Ἀπόδειξη. Ἔστω $\rho_1, \rho_2 = \overline{\rho_1}$ τὸ (μοναδικὸ) ζεῦγος τῶν μὴ πραγματικῶν ριζῶν καὶ $\rho_3, \ldots, \rho_p$ οἱ ὑπόλοιπες $p-2$ ρίζες (οἱ ὁποῖες εἶναι πραγματικές) ἑνὸς ἀναγώγου πολυωνύμου $f(X) \in \mathbb{Q}[X]$ βαθμοῦ p. Ἔστω L τὸ σῶμα ριζῶν τοῦ $f(X)$ πάνω ἀπὸ τὸ $\mathbb{Q}$ καὶ $G = \mathcal{G}(L/\mathbb{Q})$, ἡ ὁμάδα Galois τοῦ $f(X)$, τὴν ὁποία βλέπομε ὡς ὑποομάδα τῆς $\mathbf{S}_p$. Ἂν δείξομε ὅτι κάθε ἀντιμετάθεση $(\rho_i\,\rho_j) \in \mathbf{S}_p$, αὐτὸ θὰ σημαίνει ὅτι ἡ G ταυτίζεται μὲ τὴν $\mathbf{S}_p$.

Παρατηροῦμε πρῶτα ὅτι $(\rho_1\,\rho_2) \in G$. Πράγματι, ὁ περιορισμὸς στὸ L τοῦ αὐτομορφισμοῦ $z \to \overline{z}$ τοῦ $\mathbb{C}$ εἶναι $\mathbb{Q}$-αὐτομορφισμὸς τοῦ L, δηλαδή, στοιχεῖο τῆς G, στέλνει τὴ ρ_1 στὴ ρ_2 καὶ ἀντιστρόφως, καὶ ἀφήνει ἀναλλοίωτες τὶς ὑπόλοιπες ρίζες· συνεπῶς ταυτίζεται μὲ τὴν ἀντιμετάθεση $(\rho_1\,\rho_2)$. Στὸ σύνολο $P = \{1, 2, \ldots, p\}$ ὁρίζομε τώρα τὴν ἑξῆς σχέση:

$$i \sim j \Leftrightarrow i = j \;\text{ εἴτε }\; (\rho_i\,\rho_j) \in G\,.$$

Παρατηρῆστε ὅτι ἡ τελευταία συνθήκη $(\rho_i\,\rho_j) \in G$ εἶναι συντομογραφία τῆς συνθήκης:

$$\exists\sigma \in G\;:\;\sigma(\rho_i) = \rho_j \;\&\; \sigma(\rho_j) = \rho_i \;\&\; \sigma(\rho_k) = \rho_k \;\forall\, k \in P,\; k \neq i, j\,.$$

Ἡ σχέση αὐτὴ εἶναι, προφανῶς, αὐτοπαθὴς καὶ συμμετρική. Εἶναι καὶ μεταβατική, λόγῳ τῆς σχέσεως $(\rho_i\,\rho_k) = (\rho_i\,\rho_j)(\rho_j\,\rho_k)(\rho_i\,\rho_j)$, ἡ ὁποία συνεπάγεται ὅτι, ἂν $i \sim j$ καὶ $j \sim k$ τότε $i \sim k$. Ἔτσι, ἡ σχέση $\sim$ εἶναι ἰσοδυναμία στὸ P. Στὸ τέλος θὰ δείξομε ὅτι ὅλες οἱ κλάσεις ἰσοδυναμίας εἶναι ἰσοπληθεῖς. Μὲ δεδομένο αὐτό, συμπεραίνομε ὅτι ὁ κοινὸς πληθάριθμος τῶν κλάσεων ἰσοδυναμίας διαιρεῖ τὸ p, ἄρα εἶναι ἢ 1 ἢ p. Τὸ πρῶτο ἐνδεχόμενο ἀποκλείεται, γιατὶ ἡ κλάση τοῦ 1 περιέχει, ἐκτὸς ἀπὸ τὸ 1, καὶ τὸ 2 (λόγῳ τοῦ ὅτι $(\rho_1\,\rho_2) \in G$). Ἄρα μένει τὸ δεύτερο ἐνδεχόμενο, ποὺ σημαίνει ὅτι ὑπάρχει μόνο μία κλάση, δηλαδή, γιὰ κάθε ζεῦγος i, j στοιχείων τοῦ P, $(\rho_i\,\rho_j) \in G$. Μένει νὰ δείξομε ὅτι ὅλες οἱ κλάσεις ἰσοδυναμίας εἶναι ἰσοπληθεῖς. Ἔστω $\widehat{i}, \widehat{j}$ δύο κλάσεις, ὅπου $i, j \in P$. Θὰ δείξομε ὅτι ὑπάρχει ἀμφιμονοσήμαντη ἀντιστοιχία $\widehat{i} \to \widehat{j}$. Πρῶτ' ἀπ' ὅλα, λόγῳ τοῦ Θεωρήματος 1.4.3, ὑπάρχει $\mathbb{Q}$-ἰσομορφισμὸς $\mathbb{Q}(\rho_i) \to \mathbb{Q}(\rho_j)$, ὁ ὁποῖος στέλνει τὴ ρ_i στὴ ρ_j. Αὐτός, λόγῳ τοῦ Θεωρήματος 1.4.4, ἐπεκτείνεται σὲ αὐτομορφισμὸ τοῦ L. Ἄρα, ὑπάρχει αὐτομορφισμὸς $\sigma \in G$, τέτοιος ὥστε $\sigma(\rho_i) = \rho_j$. Ἔστω τώρα $m \in \widehat{i}$ καὶ $\sigma(\rho_m) = \rho_{m'}$. Εἶναι $m' \in \widehat{j}$. Πράγματι, ἡ σχέση $m \in i$ λέει ὅτι ὑπάρχει $\tau \in G$ τέτοιο ὥστε $\tau(\rho_i) = \rho_m \;\;\&\;\; \tau(\rho_m) = \rho_i \;\;\&\;\; \tau(\rho_l) = \rho_l\,\forall l \in P,\; l \neq i, m$. Τότε, εἶναι ἁπλὸ νὰ δοῦμε ὅτι $\sigma\tau\sigma^{-1}(\rho_j) = \rho_{m'}$ καὶ $\sigma\tau\sigma^{-1}(\rho_{m'}) = \rho_j$. Ἀκόμη, γιὰ $k \in P$, $k \neq j, m'$ εἶναι $\sigma\tau\sigma^{-1}(\rho_k) = \sigma\tau(\rho_l)$ (γιὰ κάποιο $l \in P$, $l \neq i, m$) $= \sigma(\rho_l) = \rho_k$. Συνεπῶς, ἡ ἀντιμετάθεση $(\rho_j, \rho_{m'})$ ταυτίζεται μὲ τὸν αὐτομορφισμὸ $\sigma\tau\sigma^{-1} \in G$, δηλαδὴ $m' \in \widehat{j}$.

[14] Ἁπλῆ ἄσκηση ὁμάδων: Ἂν μιᾶς ὁμάδας ἡ τάξη εἶναι πρῶτος ἀριθμός, τότε ἡ ὁμάδα αὐτὴ εἶναι κυκλική.

Στὸ $m \in \widehat{i}$, λοιπόν, μποροῦμε νὰ ἀντιστοιχήσομε τὸ $m' \in \widehat{j}$ καί, λόγῳ τῆς $\sigma(\rho_m) = \rho_{m'}$, διαφορετικὰ m ἀντιστοιχοῦν σὲ διαφορετικὰ m'. Ἄρα ὁρίζεται ἀμφιμονοσήμαντη ἀπεικόνιση $\widehat{i} \to \widehat{j}$. Ἐντελῶς ἀνάλογα ὅμως, ὑπάρχει καὶ ἀμφιμονοσήμαντη ἀπεικόνιση $\widehat{j} \to \widehat{i}$, ἄρα οἱ κλάσεις $\widehat{i}$ καὶ $\widehat{j}$ εἶναι ἰσοπληθεῖς. □

Θεώρημα 2.4.12. *Γιὰ $n \geq 5$, ἡ συμμετρικὴ ὁμάδα $\mathbf{S}_n$ δὲν εἶναι ἐπιλύσιμη.*

Ἀπόδειξη. Ἔστω ὅτι γιὰ κάποιο $n \geq 5$ ἡ $\mathbf{S}_n$ εἶναι ἐπιλύσιμη. Αὐτὸ σημαίνει ὅτι ὑπάρχει μία ἁλυσίδα ὑπομάδων τῆς $\mathbf{S}_n$

$$S_n = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_t = \langle \mathbf{id} \rangle$$

ὅπου G_i/G_{i-1} εἶναι ἀβελιανὴ ὁμάδα γιὰ κάθε $i = 1, \ldots, t$. Θὰ δείξομε ὅτι κάθε G_i, $i = 0, 1, \ldots, m$ περιέχει ὅλους τοὺς κύκλους μήκους 3 τῆς $\mathbf{S}_n$, κάτι προφανῶς ἄτοπο γιὰ $i = t$. Γιὰ $i = 0$ ὁ ἰσχυρισμὸς εἶναι τετριμμένος. Ἔστω τώρα ὅτι γιὰ κάποιο $\nu \geq 0$ ($\nu \leq t-1$) ἡ G_ν περιέχει ὅλους τοὺς κύκλους μήκους 3. Θὰ δείξομε ὅτι, γιὰ ὁποιουσδήποτε διαφορετικοὺς δεῖκτες i, j, k μεταξὺ 1 καὶ n, ὁ κύκλος $(i\,j\,k)$ ἀνήκει στὴν $G_{\nu+1}$. Γιὰ τὸ σκοπὸ αὐτὸ ἐπιλέγομε δύο δεῖκτες l, m μεταξὺ 1 καὶ n διαφορετικοὺς μεταξύ τους, ἀλλὰ καὶ διαφορετικοὺς ἀπὸ τοὺς i, j, k (αὐτὸ εἶναι δυνατόν, διότι $n \geq 5$). Ἐξ ὑποθέσεως, $(j\,k\,m), (i\,l\,j), (m\,k\,j), (j\,l\,i) \in G_\nu$, ἄρα ἡ ὁμάδα $G_\nu/G_{\nu+1}$ περιέχει τὰ $(j\ k\ m)G_{\nu+1}, (i\ l\ j)G_{\nu+1}, (m\ k\ j)G_{\nu+1}, (j\ l\ i)G_{\nu+1}$. Ἐπειδὴ ἡ ὁμάδα αὐτὴ εἶναι ἀβελιανή,

$$\begin{aligned}(j\ k\ m)G_{\nu+1} \cdot (i\ l\ j)G_{\nu+1} \cdot (m\ k\ j) \cdot G_{\nu+1} \cdot (j\ l\ i)G_{\nu+1} = \\ (j\ k\ m)G_{\nu+1} \cdot (m\ k\ j)G_{\nu+1} \cdot (i\ l\ j) \cdot G_{\nu+1} \cdot (j\ l\ i)G_{\nu+1}\ .\end{aligned}$$

Ὅμως $(j\ k\ m)(m\ k\ j)$ καὶ $(i\ l\ j)(j\ l\ i)$ εἶναι οἱ ταυτοτικὲς μεταθέσεις, ὁπότε τὸ δεξιὸ μέλος ἰσοῦται μὲ $G_{\nu+1}$, ἐνῶ τὸ ἀριστερό, ἐξ ὁρισμοῦ τῆς πράξεως στὴν $G_\nu/G_{\nu+1}$, ἰσοῦται μὲ $(j\ k\ m)(i\ l\ j)(m\ k\ j)(j\ l\ i)G_{\nu+1} = (i\ j\ k)G_{\nu+1}$. Ἔτσι, $(i\ j\ k)G_{\nu+1} = G_{\nu+1}$, ποὺ σημαίνει ὅτι $(i\ j\ k) \in G_{\nu+1}$. □

Συμπέρασμα Μία ἄμεση συνέπεια τῶν δύο τελευταίων θεωρημάτων εἶναι ὅτι κάθε ἀνάγωγο πολυώνυμο πέμπτου βαθμοῦ μὲ ρητοὺς συντελεστές, τὸ ὁποῖο ἔχει ἀκριβῶς τρεῖς πραγματικὲς ρίζες, δὲν εἶναι ἐπιλύσιμο μὲ ριζικά. Ἕνα τέτοιο πολυώνυμο, γιὰ παράδειγμα, εἶναι τὸ $X^5 - 17X - 17$. Εἶναι ἀνάγωγο, ὅπως προκύπτει ἀπὸ τὸ κριτήριο τοῦ Eisenstein, καὶ τὸ ὅτι ἔχει τρεῖς ἀκριβῶς πραγματικὲς ρίζες εἶναι ἁπλῆ ἄσκηση Ἀπειροστικοῦ Λογισμοῦ.

2.4.1 Βοηθητικὲς προτάσεις, ποὺ χρησιμοποιήθηκαν

(α′) Ἂν p εἶναι πρῶτος καὶ $\zeta \neq 1$ ρίζα τῆς μονάδος τάξεως p, τότε $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \mathbb{Z}_p^*$.
(β′) Ἂν p εἶναι πρῶτος καὶ $\zeta \neq 1$ ρίζα τῆς μονάδος τάξεως p καὶ M ὁποιοδήποτε ὑπόσωμα τοῦ $\mathbb{C}$, τότε ἡ ὁμάδα $\mathcal{G}(M(\zeta)/M)$ εἶναι κυκλική.
(γ′) Γιὰ κάθε κυκλικὴ πεπερασμένη ὁμάδα G ὑπάρχει ἁλυσίδα ὑπομάδων της

$$\langle \mathbf{id} \rangle = G_k \lhd G_{k-1} \lhd G_{k-2} \cdots \lhd G_0 = G\ ,$$

ὅπου κάθε G_{i-1}/G_i ἔχει τάξη πρῶτο ἀριθμό.
(δ′) Ἔστω p, ζ καὶ M ὅπως στὸ (2), παραπάνω. Τότε ὑπάρχει μία ἁλυσίδα ἐνδιαμέσων ἐπεκτάσεων

$$M = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_r = M(\zeta)\ ,$$

τέτοια ὥστε, κάθε ἐπέκταση M_i/M_{i-1} εἶναι Galois καὶ ὁ βαθμὸς της εἶναι πρῶτος.

Ἀπόδειξη τῆς (α΄). Ὅλες οἱ διάφορες τοῦ 1 p-τάξεως ρίζες τῆς μονάδος εἶναι οἱ $\zeta, \zeta^2, \dots, \zeta^{p-1}$ καὶ ταυτίζονται μὲ τὶς ρίζες τοῦ πολυωνύμου $g(X) = X^{p-1} + \cdots + X + 1$, τὸ ὁποῖο, ὅπως ξέρομε, εἶναι ἀνάγωγο. Κάθε $\sigma \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ χαρακτηρίζεται ἀπὸ τὴν τιμὴ τοῦ $\sigma(\zeta)$. Ἀλλὰ $\sigma(\zeta)$ πρέπει νὰ εἶναι ρίζα τοῦ $g(X)$, ἄρα ἰσοῦται μὲ ζ^k, γιὰ κάποιο $k \in \{1, \dots, p-1\}$. Ἐπειδὴ $k_1 \equiv k_2 \pmod p \Rightarrow \zeta^{k_1} = \zeta^{k_2}$, ἡ ἀπεικόνιση $\sigma \to k \bmod p$ μεταξὺ τῶν ὁμάδων $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ καὶ $\mathbb{Z}_p^*$ εἶναι μονομορφισμός. Ἐπιπλέον, ὁ $\phi(\sigma)$ εἶναι καὶ ἐπί. Πράγματι, γιὰ κάθε $k \in \{1, \dots, p-1\}$, ἡ ζ^k εἶναι ἀρχικὴ ρίζα τῆς μονάδος, ἄρα $\mathbb{Q}(\zeta^k) = \mathbb{Q}(\zeta)$ ἐνῶ, λόγῳ τοῦ Θεωρήματος 1.4.3, ὑπάρχει ἰσομορφισμὸς $\sigma : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta^k)$, ὁ ὁποῖος ἀφήνει ἀναλλοίωτα ὅλα τὰ στοιχεῖα τοῦ $\mathbb{Q}$ καὶ στέλνει τὸ ζ στὸ ζ^k. Δηλαδή, $\sigma \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ καὶ $\sigma(\zeta) = \zeta^k$, ποὺ σημαίνει ὅτι, κατὰ τὸν παραπάνω ὁρισθέντα μονομορφισμὸ ὁμάδων, ὁ σ ἀντιστοιχεῖ στὴν κλάση $k \bmod p$.

Ἀπόδειξη τῆς (β΄). Ὁρίζομε τὸν ἑξῆς ὁμομορφισμὸ ὁμάδων:

$$\mathcal{G}(M(\zeta)/M) \ni \sigma \xrightarrow{\phi} \sigma|_{\mathbb{Q}(\zeta)} \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q}) \ .$$

Εὔκολα διαπιστώνεται ὅτι ὁ $\phi(\sigma)$ εἶναι $\mathbb{Q}$-μονομορφισμὸς $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$. Ἐπιπλέον, εἶναι καὶ 'ἐπί'. Ἁπλῶς, παρατηρῆστε ὅτι, ἂν $\sigma(\zeta) = \zeta^k$ καὶ $kl \equiv 1 \pmod p$, τότε $\sigma(\zeta^l) = \zeta$. Συνεπῶς, $\phi(\sigma) \in \mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ καὶ ὁ ϕ εἶναι καλὰ ὁρισμένος μονομορφισμὸς ὁμάδων, ὁπότε $\mathcal{G}(M(\zeta)/M) \cong \operatorname{Im}\phi$. Ὅμως, ἀπὸ τὴν (1), ἡ ὁμάδα $\mathcal{G}(\mathbb{Q}(\zeta)/\mathbb{Q})$ εἶναι ἰσόμορφη μὲ τὴν $\mathbb{Z}_p^*$, ἡ ὁποία εἶναι κυκλική, διότι κάθε πρῶτος p διαθέτει ἀρχικὲς ρίζες mod$p$ [15]. Ἄρα ἡ $\mathcal{G}(M(\zeta)/M)$ εἶναι κυκλική, ὡς ἰσόμορφη μὲ ὑποομάδα κυκλικῆς ὁμάδος.

Ἀπόδειξη τῆς (γ΄). Ἔστω $G = \langle g \rangle$ καὶ ἡ τάξη τοῦ g (ἄρα καὶ τῆς G) εἶναι n. Ἔστω $n = p_1 \cdots p_k$ ἡ ἀνάλυση τοῦ n σὲ πρώτους (ὄχι κατ' ἀνάγκη διαφορετικοὺς) παράγοντες. Ἂν θέσομε

$$G = G_0 = \langle g \rangle,\ G_1 = \langle g^{p_1} \rangle,\ G_2 = \langle g^{p_1 p_2} \rangle,\ \dots G_k = \langle g^{p_1 \cdots p_k} \rangle = \langle g^n \rangle = \langle \mathbf{id} \rangle \ ,$$

τότε

$$\langle \mathbf{id} \rangle = G_k \lhd G_{k-1} \lhd G_{k-2} \cdots \lhd G_0 = G$$

καὶ γιὰ κάθε i, $|G_i| = n/p_1 \cdots p_i$, ὁπότε ἡ τάξη τῆς G_{i-1}/G_i ἰσοῦται μὲ

$$\frac{n}{p_1 \cdots p_{i-1}} : \frac{n}{p_1 \cdots p_i} = p_i \ .$$

Ἀπόδειξη τῆς (δ΄). Θέτομε $L = M(\zeta)$. Ἡ ἐπέκταση L/M εἶναι κανονική, ὡς σῶμα ριζῶν τοῦ $X^p - 1 \in M[X]$, ἄρα καὶ Galois. Ἔστω $G = \mathcal{G}(L/M)$. Λόγῳ τῆς (2), ἡ G εἶναι κυκλική, ὁπότε θεωροῦμε τὴν ἁλυσίδα ποὺ μᾶς ἐξασφαλίζει ἡ (3). Σὲ αὐτὴν ἀντιστοιχεῖ, μέσῳ τῆς ἀντιστοιχίας Galois, ἡ ἁλυσίδα ἐπεκτάσεων

$$M = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_k = L = M(\zeta) \ ,$$

ὅπου $M_i = \mathcal{F}_L(G_i)$ (ἤ, ἰσοδύναμα, $\mathcal{G}(L/M_i) = G_i$). Γιὰ κάθε i θεωροῦμε τὶς διαδοχικὲς ἐπεκτάσεις $L \supset M_i \supset M_{i-1}$ καὶ ἐφαρμόζομε τὸ Θεώρημα 2.2.12. Ἐπειδὴ ἡ L/M εἶναι ἐπέκταση Galois, τὸ ἴδιο συμβαίνει καὶ μὲ τὴν L/M_{i-1}. Ἐπειδὴ ἡ ὁμάδα G_i (ἡ ὁποία ἀντιστοιχεῖ

[15] Δηλαδή, γιὰ κάθε πρῶτο p ὑπάρχει g, τέτοιο ὥστε οἱ κλάσεις $1, 2, \dots, p-1 \mod p$ νὰ ταυτίζονται (μὲ διαφορετική, ἐν γένει, σειρά) μὲ τὶς κλάσεις g^k, $k = 0, 1, \dots, p-2$. Παραδείγματα: $(p, g) = (7,3), (13,2), (17,3), (23,5), (41,6), (71,7), (1741,2), (3881,13), (3943,3)$

στὸ M_i) εἶναι κανονικὴ ὑποομάδα τῆς G_{i-1} (ἡ ὁποία ἀντιστοιχεῖ στὸ M_{i-1}), ἕπεται ἀπὸ τὸ Θεώρημα 2.2.12(4) ὅτι ἡ ἐπέκταση M_i/M_{i-1} εἶναι Galois, μὲ ὁμάδα Galois ἰσόμορφη πρὸς τὴν G_{i-1}/G_i, ἡ ὁποία ἔχει τάξη πρῶτο ἀριθμό. Ὅμως, ἡ τάξη αὐτῆς τῆς ὁμάδος Galois ἰσοῦται μὲ $[M_i : M_{i-1}]$, ἀπ' ὅπου ἔχομε τὸ ἀποδεικτέο.

Ἀσκήσεις

1. Ἔστω $K \subseteq L \subseteq M$ διαδοχικὲς ἐπεκτάσεις, τέτοιες ὥστε, οἱ L/K καὶ M/L εἶναι ριζικές. Δεῖξτε ὅτι καὶ ἡ M/K εἶναι ριζική.

2. Ἔστω K ὑπόσωμα τοῦ $\mathbb{C}$,[16] καὶ ἀκέραιος $n \geq 2$, $n = p_1 \cdots p_k$, ὅπου $p_1, \dots, p_k$ εἶναι πρῶτοι, ὄχι κατ' ἀνάγκη διαφορετικοί. Ἔστω L τὸ σῶμα ριζῶν πάνω ἀπ' τὸ K τοῦ $X^n - 1 \in K[X]$. Γιὰ κάθε $j \in \{1, \dots, k\}$ θέτομε
$$z_j = \cos \frac{2\pi}{p_1 \cdots p_{j-1} p_j} + i \sin \frac{2\pi}{p_1 \cdots p_{j-1} p_j}.$$
Ἀποδεῖξτε ὅτι, $z_j^{p_j} = z_{j-1}$ γιὰ κάθε $j \in \{2, \dots, k\}$ καὶ συμπεράνατε ὅτι ἡ ἐπέκταση L/K εἶναι ριζική.

3. Ἔστω K ὑπόσωμα τοῦ $\mathbb{C}$, $a \in K$ καὶ ἀκέραιος $n \geq 2$. Ἔστω $b \in \mathbb{C}$, τέτοιο ὥστε $b^n = a$ καὶ L τὸ σῶμα ριζῶν πάνω ἀπ' τὸ $K(b)$ τοῦ $X^n - a$. Ἀποδεῖξτε ὅτι ἡ ἐπέκταση L/K εἶναι ριζική.
Ὑπόδειξη. Ἔστω L τὸ σῶμα ριζῶν τοῦ $X^n - 1$ πάνω ἀπ' τὸ $K(b)$. Δεῖξτε ὅτι τὸ L εἶναι σῶμα ριζῶν τοῦ $X^n - a$ πάνω ἀπ' τὸ K. Θεωρῆστε τὶς διαδοχικὲς ἐπεκτάσεις $K \subseteq K(b) \subseteq L$ καὶ ἐφαρμόστε τὴν ἄσκηση 2 μὲ τὸ $K(b)$ στὴ θέση τοῦ K, καθὼς καὶ τὴν ἄσκηση 1.

4. Ἔστω ὅτι τὸ $f(X) \in \mathbb{Q}[X]$ εἶναι ἐπιλύσιμο μὲ ριζικά. Ἔστω ἀκέραιος $n \geq 2$ καὶ $g(X) = f(X^n)$. Ἀποδεῖξτε ὅτι καὶ τὸ $g(X)$ εἶναι ἐπιλύσιμο μὲ ριζικά.
Ὑπόδειξη. Ἔστω ὅτι $a_1, \dots, a_r \in \mathbb{C}$ εἶναι ὅλες οἱ ρίζες τοῦ $f(X)$ καὶ $K = \mathbb{Q}(a_1, \dots, a_r)$ τὸ σῶμα ριζῶν τοῦ $f(X)$ πάνω ἀπ' τὸ K. Ἐξ ὑποθέσεως, ἡ ἐπέκταση $K/\mathbb{Q}$ εἶναι ριζική. Θεωροῦμε $b_1, \dots, b_r \in \mathbb{C}$, τέτοια ὥστε $b_j^n = a_j$ γιὰ κάθε $j = 1, \dots, r$. Ἔστω K_1 τὸ σῶμα ριζῶν τοῦ $X^n - a_1$ πάνω ἀπ' τὸ $K(b_1)$. Ἀπὸ τὴν ἄσκηση 3, ἡ ἐπέκταση K_1/K εἶναι ριζική. Μετά, ἔστω K_2 τὸ σῶμα ριζῶν τοῦ $X^n - a_2$ πάνω ἀπ' τὸ $K_1(b_2)$. Πάλι ἀπ' τὴν ἄσκηση 3, ἡ ἐπέκταση K_2/K_1 εἶναι ριζική. Ποιὸ εἶναι τὸ ἑπόμενο βῆμα; Προχωρώντας ἔτσι, βῆμα-βῆμα, δεῖτε ὅτι θὰ φτάσετε μέσῳ διαδοχικῶν ριζικῶν ἐπεκτάσεων στὸ σῶμα ριζῶν πάνω ἀπ' τὸ K τοῦ $g(X)$. Φυσικά, θὰ χρησιμοποιήσετε καὶ τὴν ἄσκηση 1.

[16] Εἶναι ἁπλὸ νὰ δείξει κανεὶς ὅτι κάθε ὑπόσωμα τοῦ $\mathbb{C}$ εἶναι ἐπέκταση τοῦ $\mathbb{Q}$, ἄρα $\mathbb{Q} \subseteq K$.

2.5 Επιλυση εξισωσεων βαθμου 3 και 4

Θὰ ἀσχοληθοῦμε μὲ τὴν ἐπίλυση πολυωνυμικῶν ἐξισώσεων τρίτου καὶ τετάρτου βαθμοῦ μὲ μιγαδικοὺς συντελεστές.

2.5.1 *Ἡ ἐξίσωση τρίτου βαθμοῦ.*

Ὅπως εἴδαμε στὴν ἑνότητα 1.5, ἀρκεῖ νὰ μποροῦμε νὰ λύνομε τριτοβάθμιες ἐξισώσεις τῆς μορφῆς $x^3 + ax + b = 0$ (λείπει τὸ x^2). Ἂν $x_1, x_2, x_3 \in \mathbb{C}$ εἶναι οἱ ρίζες της, τότε

$$x_1 + x_2 + x_3 = 0\ ,\ x_1x_2 + x_2x_3 + x_3x_1 = a\ ,\ x_1x_2x_3 = -b\ . \tag{2.4}$$

Θέτομε

$$x = z - \frac{a}{3z}\ , \tag{2.5}$$

ὁπότε ἡ ἀρχικὴ ἐξίσωση μετασχηματίζεται στὴν $27z^6 + 27bz^3 - a^3 = 0$, ἡ ὁποία εἶναι δευτεροβάθμια ὡς πρὸς z^3 καὶ λύνοντάς την παίρνομε

$$z^3 = -\frac{b}{2} + \epsilon\sqrt{R}\ ,\ R = \left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3\ ,\ \epsilon \in \{-1, +1\}\ . \tag{2.6}$$

Ἐδῶ $\sqrt{R}$ ὑποδηλώνει ὁποιαδήποτε ἀπὸ τὶς δύο τετραγωνικὲς ρίζες τοῦ μιγαδικοῦ ἀριθμοῦ R. Ἔστω ζ μία ὁποιαδήποτε ἀπὸ τὶς τρεῖς μιγαδικὲς ρίζες τοῦ $-(b/2)+\epsilon\sqrt{R}$. Ἂν $\omega \neq 1$ εἶναι μία κυβικὴ ρίζα τῆς μονάδος, τότε, λόγῳ τῆς (2.6), οἱ πιθανὲς τιμὲς τοῦ z εἶναι $\zeta, \omega\zeta, \omega^2\zeta$, ἄρα ἀπὸ τὴν (2.5), οἱ πιθανὲς τιμὲς γιὰ τὸ x εἶναι

$$\zeta - \frac{a}{3\zeta}\ ,\ \zeta\omega - \frac{a}{3\zeta\omega} = \zeta\omega - \frac{a}{3\zeta}\omega^2\ ,\ \zeta\omega^2 - \frac{a}{3\zeta\omega^2} = \zeta\omega^2 - \frac{a}{3\zeta}\omega\ . \tag{2.7}$$

ἕνας ὑπολογισμὸς (βλ. ἄσκηση 1) δείχνει ὅτι οἱ στοιχειώδεις συμμετρικὲς παραστάσεις τῶν τριῶν ἀριθμῶν στὴν (2.7) εἶναι ἴσες, ἀντιστοίχως, μὲ $0, a, -b$. ἄρα, ἀπὸ τὴν (2.4) καὶ τὴν ἄσκηση 2, συμπεραίνομε ὅτι αὐτοὶ οἱ ἀριθμοὶ εἶναι οἱ τρεῖς λύσεις τῆς ἐξισώσεως $x^3 + ax + b = 0$. Ἐπειδὴ τὸ ἴδιο ἀποτέλεσμα προκύπτει ἀνεξαρτήτως τοῦ ἂν ϵ εἶναι 1 ἢ -1, συμπεραίνομε ὅτι μποροῦμε στὴν (2.7) νὰ πάρομε, χωρὶς βλάβη τῆς γενικότητος, $\epsilon = 1$. Οἱ τρεῖς ἀριθμοὶ στὴν (2.7) γράφονται καὶ ὡς ἑξῆς:

$$\zeta\omega^j - \frac{a}{3\zeta}\omega^{2j}\ ,\ j \in \{0, 1, 2\}\ . \tag{2.8}$$

Ὅπως εἴπαμε προηγουμένως, ζ εἶναι μία ὁποιαδήποτε ρίζα τοῦ $-(b/2) + \sqrt{R}$. Αὐτὸ τὸ γράφομε συμβολικῶς

$$\zeta = \sqrt[3]{-\frac{b}{2} + \sqrt{R}}\ . \tag{2.9}$$

Ἔστω τώρα ζ' μία ὁποιαδήποτε ρίζα τοῦ $-(b/2) - \sqrt{R}$. Τότε,

$$(\zeta\zeta')^3 = (-\frac{b}{2} + \sqrt{R})(-\frac{b}{2} - \sqrt{R}) = \frac{b^2}{4} - R = \left(-\frac{a}{3}\right)^3\ .$$

Ἄρα, $\zeta\zeta' = -\omega^k a/3$ γιὰ κάποιο $k \in \{0,1,2\}$. Ὁ ἀριθμὸς $\omega^{-k}\zeta'$ εἶναι κυβικὴ ρίζα τοῦ $-(b/2) - \sqrt{R}$, τὴν ὁποία συμβολίζομε

$$\sqrt[3]{-\frac{b}{2} - \sqrt{R}}\,. \tag{2.10}$$

Δηλαδὴ δείξαμε ὅτι, ἅπαξ καὶ οριστεῖ (αὐθαιρέτως) ἡ τιμὴ τῆς (2.9), ἡ τιμὴ τῆς (2.10) μπορεῖ νὰ ἐπιλεγεῖ ἔτσι ὥστε

$$\sqrt[3]{-\frac{b}{2} + \sqrt{R}} \cdot \sqrt[3]{-\frac{b}{2} - \sqrt{R}} = -\frac{a}{3}\,. \tag{2.11}$$

Λόγῳ τῆς (2.8) τώρα, οἱ τρεῖς ρίζες ἐκφράζονται ἀπὸ τοὺς παρακάτω *τύπους τοῦ Cardano*

$$\omega^j \sqrt[3]{-\frac{b}{2} + \sqrt{R}} + \omega^{2j} \sqrt[3]{-\frac{b}{2} - \sqrt{R}}\,, \qquad j = 0,1,2\,,$$

ὑπὸ τὸν περιορισμό, οἱ τιμὲς τῶν κυβικῶν ριζῶν νὰ ἐπιλέγονται ἔτσι ὥστε νὰ ἰσχύει ἡ (2.11).

Σημείωση: Παρατηρῆστε ὅτι $R = -D/108$, ὅπου D ἡ διακρίνουσα τοῦ πολυωνύμου $X^3 + aX + b$ (βλ. ἄσκηση 1.4.2).

2.5.2 *Ἡ ἐξίσωση τετάρτου βαθμοῦ*

Γράφομε τὴ γενικὴ τεταρτοβάθμια ἐξίσωση μὲ τὴ μορφὴ

$$f(x) = x^4 + 4ax^3 + 6bx^2 + 4cx + d = 0 \tag{2.12}$$

καὶ ἐπιδιώκομε νὰ ἐκφράσομε τὸ πολυώνυμο $f(X)$ ὡς διαφορὰ τετραγώνων. Θέτομε

$$h_1(X) = 2mX + n\,,\ \ h_2(X) = X^2 + 2aX + b + 2l\,, \tag{2.13}$$

ὅπου l, m, n εἶναι παράμετροι, ποὺ θὰ προσδιορίσομε, ἀπὸ τὴν ἀπαίτηση νὰ ἰσχύει

$$f(X) = h_2(X)^2 - h_1(X)^2\,. \tag{2.14}$$

Ἡ (2.14) γράφεται

$$(2mX + n)^2 = 4(l + a^2 - b)X^2 + 4(ab + 2al - c)X + (b + 2l)^2 - d\,, \tag{2.15}$$

ἡ ὁποία λέει ὅτι τὸ δεξιὸ μέλος εἶναι τέλειο τετράγωνο, ὁπότε ἡ διακρίνουσά του εἶναι 0:

$$4(ab + 2al - c)^2 - 4(l + a^2 - b)[(b + 2l)^2 - d] = 0\,.$$

ὕστερα ἀπὸ τὶς πράξεις καταλήγομε στὴν

$$4l^3 - g_2 l + g_3 = 0\,, \tag{2.16}$$

ὅπου g_2, g_3 εἶναι οἱ λεγόμενες *ἀναλλοίωτες* (βλ. ἄσκηση 3) τοῦ $f(X)$:

$$g_2 = d - 4ac + 3b^2\,,\ \ g_3 = bd + 2abc - b^3 - c^2 - a^2 d = \begin{vmatrix} 1 & a & b \\ a & b & c \\ b & c & d \end{vmatrix}\,. \tag{2.17}$$

Ἀρκεῖ, λοιπόν, νὰ βροῦμε μία ὁποιαδήποτε λύση l τῆς *ἐπιλύουσας* τριτοβάθμιας ἐξίσωσης (2.16) καὶ μετὰ νὰ προσδιορίσομε τὰ m, n ἀπὸ τὴν πολυωνυμικὴ ἰσότητα (2.15), δηλαδή,

$$m^2 = l + a^2 - b\ ,\ mn = ab + 2al - c\ ,\ n^2 = (b + 2l)^2 - d\ . \tag{2.18}$$

Προσδιορίζοντας κατ' αὐτὸν τὸν τρόπο, τὰ l, m, n μποροῦμε, στὴ συνέχεια, λόγῳ τῆς (2.13), νὰ γράψομε τὴν (2.12) ὡς $(h_2(x) + h_1(x))(h_2(x) - h_1(x)) = 0$, ἀνάγοντας τὴν ἐπίλυσή της στὴν ἐπίλυση δύο δευτεροβαθμίων ἐξισώσεων.

2.5.3 Ἡ διακρίνουσα ἑνὸς πολυωνύμου

Ἔστω τὸ πολυώνυμο

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots a_1X + a_0$$

μὲ συντελεστὲς ἀπὸ ὁποιοδήποτε σῶμα καὶ $x_1, \dots, x_n$ οἱ ρίζες του σὲ κάποια κατάλληλη ἐπέκταση (σῶμα ριζῶν). Ὁρίζομε ὡς *διακρίνουσα* τοῦ $f(X)$ τὴν ποσότητα

$$D = \prod_{1 \le i < j \le n} (x_i - x_j)^2\ .$$

Παρατηροῦμε ὅτι $D \in \mathbb{Z}[x_1, \dots, x_n]$ καὶ εἶναι συμμετρικὴ παράσταση τῶν $x_1, \dots, x_n$, ἄρα ἀπὸ τὸ Θεώρημα Γ′.1 καὶ τοὺς τύπους τοῦ Viète συμπεραίνομε ὅτι $D \in \mathbb{Z}[a_1, \dots, a_n]$, δηλαδή,

> Ἡ διακρίνουσα τοῦ $f(X)$ εἶναι πολυωνυμικὴ ἔκφραση τῶν $a_1, \dots, a_n$ μὲ ἀκέραιους συντελεστές.

Ἐπίσης, παρατηροῦμε ὅτι

> Ἡ διακρίνουσα τοῦ $f(X)$ εἶναι μηδέν, ἂν καὶ μόνο ἄν, τὸ $f(X)$ ἔχει μία τοὐλάχιστον πολλαπλῆ ρίζα.

Ἡ διακρίνουσα τοῦ $f(X) = X^2 + aX + b$ εἶναι $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = (-a)^2 - 4b = a^2 - 4b$, ἐνῶ ἀπὸ τὰ ἐκτεθέντα στὴν ἑνότητα 1.5, ἡ διακρίνουσα τοῦ $X^3 + aX + b$ εἶναι $-4a^3 - 27b^2$.

Παρακάτω θὰ ὑπολογίσομε τὴ διακρίνουσα τοῦ πολυωνύμου $X^4+4aX^3+6bX^2+4cX+d$. Χρειαζόμαστε πρῶτα τὸ ἑξῆς λῆμμα:

Λῆμμα 2.5.1. *Ἔστω $f_1(X) = X^2 + aX + b$, $f_2(X) = X^2 + cX + d$ καὶ $f(X) = f_1(X)f_2(X)$. Ἂν x_1, x_2 εἶναι οἱ ρίζες τοῦ $f_1(X)$ τότε ἡ διακρίνουσα τοῦ $f(X)$ εἶναι*

$$D = D_1D_2(f_2(x_1)f_2(x_2))^2\ ,$$

ὅπου D_1, D_2 οἱ διακρίνουσες τῶν $f_1(X)$, $f_2(X)$, ἀντιστοίχως.

Ἀπόδειξη. Ἂς συμβολίσομε μὲ x_3, x_4 τὶς ρίζες τοῦ $f_2(X)$. Εἶναι $D_1 = (x_1 - x_2)^2$, $D_2 = (x_3 - x_4)^2$ καὶ $x_3 + x_4 = -c$, $x_3x_4 = d$. Οἱ ρίζες τοῦ $f(X)$ εἶναι $x_1, \dots, x_4$, ἄρα

$$\begin{aligned}
D &= [(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)]^2 \\
&= (x_1 - x_2)^2(x_3 - x_4)^2[(x_1 - x_3)(x_1 - x_4)]^2[(x_2 - x_3)(x_2 - x_4)]^2 \\
&= D_1D_2[x_1^2 - (x_3 + x_4)x_1 + x_3x_4]^2[x_2^2 - (x_3 + x_4)x_2 + x_3x_4]^2 \\
&= D_1D_2(x_1^2 + cx_1 + d)^2(x_2^2 + cx_2 + d)^2 \\
&= D_1D_2(f_2(x_1)f_2(x_2))^2
\end{aligned}$$

□

Ἔστω τώρα $f(X) = X^4 + 4aX^3 + 6bX^2 + 4cX + d$. Σύμφωνα μὲ τὴν προηγούμενη ἑνότητα, $f(X) = f_1(X)f_2(X)$, ὅπου $f_1(X) = h_2(X) + h_1(X)$, $f_2(X) = h_2(X) - h_1(X)$ καὶ τὰ $h_1(X), h_2(X)$ δίνονται ἀπὸ τὴν 2.13. Ἂν D_1, D_2 εἶναι, ἀντιστοίχως, οἱ διακρίνουσες τῶν $f_1(X), f_2(X)$,

$$D_1 = 4[(a+m)^2 - (b+n+2l)]\ ,\ D_2 = 4[(a-m)^2 - (b-n+2l)]\ .$$

Ἐπίσης, $f_1(x_1) = 0 = f_1(x_2)$, ἄρα $h_2(x_1) = -h_1(x_1)$ καὶ $h_2(x_2) = -h_1(x_2)$. Συνεπῶς, $f_2(x_1) = h_2(x_1) - h_1(x_1) = -2h_1(x_1)$ καί, ἀνάλογα, $f_2(x_2) = -2h_1(x_2)$, ὁπότε, σύμφωνα μὲ τὸ Λῆμμα 2.5.1,

$$D = 2^8[(a+m)^2 - (b+n+2l)][(a-m)^2 - (b-n+2l)](2mx_1+n)(2mx_2+n)\ .$$

Τὰ x_1, x_2, ὡς ρίζες τοῦ $f_1(X)$, ἱκανοποιοῦν τὶς σχέσεις $x_1 + x_2 = -2(a+m)$, $x_1x_2 = b+n+2l$, ὁπότε $(2mx_1+n)(2mx_2+n) = 4m^2(b+n+2l) - 4mn(a+m) + n^2$ καὶ ἡ D, ὕστερα ἀπὸ κάποιες πράξεις παίρνει τὴ μορφὴ

$$\begin{aligned} D &= 2^8[(a+m)^2 - (b+n+2l)][(a-m)^2 - (b-n+2l)] \\ &\quad \times[4m^2(b+n+2l) - 4mn(a+m) + n^2]^2 \\ &= 2^8[(b+2l)^2 - 2(a^2+m^2)(b+2l) + (a^2-m^2)^2 + 4amn - n^2] \\ &\quad \times[4m^2(b+2l) - (4amn - n^2)]^2\ . \end{aligned}$$

Λόγῳ τῶν (2.16) καὶ (2.17) ἔχομε $4l^3 = g_2l - g_3$ καὶ $4l^4 = g_2l^2 - g_3l$. Ἐπίσης, ἰσχύουν οἱ (2.18), ὁπότε, μετὰ τὶς πράξεις βρίσκομε

$$D = 2^8(-3l^2 + g_2)(12l^2 - g_2)^2 = 2^8(g_2^3 - 27g_3^2)\ .$$

Ἀποδείξαμε ἔτσι τὸ ἑξῆς θεώρημα.

Θεώρημα 2.5.2. *Ἡ διακρίνουσα τοῦ πολυωνύμου $X^4 + 4aX^3 + 6bX^2 + 4cX + d$ εἶναι*

$$D = 2^8(g_2^3 - 27g_3^2)\ ,$$

ὅπου τὰ g_2, g_3 δίνονται ἀπὸ τὴν (2.17)

Παρατήρηση. Ἡ διακρίνουσα τοῦ κυβικοῦ πολυωνύμου $X^3 - (g_2/4)X + (g_3/4)$, τὸ ὁποῖο ἔχει ὡς ρίζες τὶς λύσεις τῆς ἐπιλύουσας (2.16), εἶναι $4(g_2/4)^3 - 27(g_3/4)^2) = 2^{-4}(g_2^3 - 27g_3^2)$, ἄρα

> Ἡ διακρίνουσα τοῦ τεταρτοβαθμίου πολυωνύμου ἰσοῦται μὲ 2^{12} φορὲς τὴ διακρίνουσα τοῦ ἀντιστοίχου ἐπιλύοντος κυβικοῦ πολυωνύμου.

Ἀσκήσεις

1. Ἀποδεῖξτε ὅτι οἱ στοιχειώδεις συμμετρικὲς παραστάσεις τῶν τριῶν ἀριθμῶν στὴν (2.7) εἶναι ἴσες μὲ $0, a, -b$, ἀντιστοίχως.

2. Ἂς ὑποθέσομε ὅτι $x_1, \ldots, x_n$ καὶ $y_1, \ldots, y_n$ εἶναι στοιχεῖα ἑνὸς σώματος καὶ οἱ στοιχειώδεις συμμετρικὲς παραστάσεις τῆς πρώτης n-άδας εἶναι ἴσες μὲ τὶς ἀντίστοιχες τῆς δεύτερης n-άδας. Δεῖξτε τότε ὅτι ἡ δεύτερη n-άδα ἀποτελεῖ μετάθεση τῆς πρώτης. (Ὑπόδειξη: Θεωρῆστε τὰ πολυώνυμα μὲ ρίζες $x_1, \ldots, x_n$ καὶ $y_1, \ldots, y_n$, ἀντιστοίχως. Ἐφαρμόστε τοὺς τύπους τοῦ Viète.)

3. Ἡ ὀνομασία *ἀναλλοίωτες* γιὰ τὶς παραστάσεις g_2, g_3 δικαιολογεῖται ἀπὸ τὸ ὅτι, ἂν στὴν ἐξίσωση 2.12 γίνει ἡ ἀλλαγὴ μεταβλητῆς $x = y + k$, στὴ νέα, ὡς πρὸς y, ἐξίσωση ποὺ θὰ προκύψει, θὰ ἀντιστοιχοῦν g_2, g_3 ἴσα μὲ τὰ ἀρχικά. Ἀποδεῖξτε αὐτὸ τὸν ἰσχυρισμό.

4. Αὐτὴ ἡ ἄσκηση περιγράφει ἕνα κάπως διαφορετικὸ τρόπο ἐπιλύσεως τῆς (2.12). Δεῖξτε ὅτι ἡ ἀλλαγὴ μεταβλητῆς $x = y - a$ μετασχηματίζει τὴν (2.12) σὲ ἐξίσωση τῆς μορφῆς $y^4 + py^2 + qy + r = 0$ καὶ γράψτε τὸ ἀριστερὸ μέλος τῆς τελευταίας ὡς διαφορὰ τετραγώνων μὲ τὸν ἑξῆς τρόπο: Παρατηρῆστε ὅτι, γιὰ κάθε l, ἰσχύει ἡ ταυτότητα

$$y^4 + py^2 + qy + r = \left(y + \frac{l}{2}\right)^2 - \left\{(l - p)y^2 - qy + \left(\frac{l^2}{4} - r\right)\right\}$$

   καὶ βρεῖτε κατάλληλο l, ὥστε ἡ παράσταση μέσα στὰ ἄγκυστρα νὰ γίνεται τέλειο τετράγωνο. Ἐφαρμόστε τὴν παραπάνω μέθοδο γιὰ τὴν ἐπίλυση μιᾶς συγκεκριμένης τεταρτοβάθμιας ἐξίσωσης ποὺ θὰ διαλέξετε. Τὴν ἴδια ἐξίσωση ἐπιλύστε καὶ μὲ τὴ μέθοδο ποὺ περιγράφεται στὴ Θεωρία.

Παράρτημα Α΄

Μέγιστος Κοινὸς Διαιρέτης Πολυωνύμων

Ὁρισμὸς Α΄.1. *Ἔστω K σῶμα καὶ $f(X), g(X) \in K[X]$. Τὸ πολυώνυμο $d(X) \in K[X]$ λέγεται μέγιστος κοινὸς διαιρέτης (ΜΚΔ) τῶν $f(X)$ καὶ $g(X)$ ἂν εἶναι κοινὸς διαιρέτης τους, ὁ ὁποῖος, ἐπιπλέον, διαιρεῖται ἀπὸ κάθε κοινὸ διαιρέτη τῶν $f(X)$ καὶ $g(X)$.*

Ἀπὸ τὸν ὁρισμὸ αὐτὸ προκύπτουν (ὄχι μὲ ἐντελῶς ἄμεσο τρόπο) τὰ ἑξῆς.

Πρόταση Α΄.2.

1. *Ἂν $d(X)$ εἶναι ΜΚΔ τῶν $f(X), g(X)$, τότε κανένας ἄλλος κοινὸς διαιρέτης αὐτῶν τῶν πολυωνύμων δὲν ἔχει μεγαλύτερο βαθμὸ ἀπὸ ἐκεῖνο τοῦ $d(X)$.*

2. *Ἂν $d(X)$ εἶναι ΜΚΔ τῶν $f(X), g(X)$, τότε, γιὰ κάθε $c \in K^*$ τὸ πολυώνυμο $c \cdot d(X)$ εἶναι, ἐπίσης ΜΚΔ τῶν $f(X), g(X)$· ἀντιστρόφως, ἂν $d'(X)$ εἶναι ἕνας ἄλλος ΜΚΔ τῶν $f(X), g(X)$, τότε ὑπαρχει $c \in K^*$, ἔτσι ὥστε $d'(X) = c \cdot d(X)$.*

3. *Ἂν $d(X)$ εἶναι ΜΚΔ τῶν $f(X), g(X)$, τότε ὑπάρχουν $f_1(X), g_1(X) \in K[X]$, τέτοια ὥστε $f_1(X)f(X) + g_1(X)g(X) = d(X)$.*

4. *Ἔστω ὅτι ἀναλύομε τὰ μὴ σταθερὰ πολυώνυμα $f(X), g(X)$ σὲ ἀνάγωγα πολυώνυμα τοῦ $K[X]$ καὶ ἔστω ὅτι τὰ ἀνάγωγα πολυώνυμα $p_1(X), \ldots, p_n(X)$ εἶναι, ἀκριβῶς, αὐτὰ τὰ ἀνάγωγα, ποὺ ἐμφανίζονται στὴν ἀνάλυση* καὶ τῶν δύο *πολυωνύμων, μὲ ἐκθέτες $a_1, \ldots, a_n$ στὴν ἀνάλυση τοῦ $f(X)$ καὶ μὲ ἐκθέτες $b_1, \ldots, b_n$ στὴν ἀνάλυση τοῦ $g(X)$· δηλαδή,*

$$f(X) = p_1(X)^{a_1} \cdots p_n(X)^{a_n} f_1(X), \quad g(X) = p_1(X)^{b_1} \cdots p_n(X)^{b_n} g_1(X),$$

ὅπου τὰ πολυώνυμα $f_1(X)$ καὶ $g_1(X)$ δὲν ἔχουν κοινὰ ἀνάγωγα πολυώνυμα. Τότε, τὸ πολυώνυμο

$$d(X) = p_1(X)^{c_1} \cdots p_n(X)^{c_n}, \quad c_i = \min\{a_i, b_i\} \;\; i = 1, \ldots, n$$

εἶναι ΜΚΔ τῶν $f(X), g(X)$.

Οἱ δύο πρῶτες ἀπὸ τὶς παραπάνω προτάσεις εἶναι ἄμεσες συνέπειες τοῦ ὁρισμοῦ, ἐνῶ ἡ ἀπόδειξη τῆς τρίτης εἶναι ἀρκετὰ πιὸ σύνθετη. Ἐπίσης, λόγῳ τῆς δεύτερης – ἡ ὁποῖα, οὐσιαστικά, μᾶς λέει ὅτι, ὅταν ξέρομε ἕνα ΜΚΔ δύο πολυωνύμων, τοὺς ξέρομε ὅλους – λέμε συχνὰ «$d(X)$ εἶναι ὁ ΜΚΔ τῶν $f(X), g(X)$» καὶ ἐννοοῦμε, φυσικά, ὅτι καὶ κάθε $c \cdot d(X)$ εἶναι ΜΚΔ τῶν $f(X), g(X)$.

῾Ορισμὸς Α′.3. *῎Εστω K σῶμα καὶ $f(X), g(X) \in K[X]$. Τὰ πολυώνυμα αὐτὰ λέγονται πρῶτα μεταξύ τους, ἂν ἕνας ΜΚΔ τους εἶναι σταθερὸ πολυώνυμο· μ' ἄλλα λόγια, ἂν οἱ μόνοι κοινοὶ διαιρέτες τῶν δύο πολυωνύμων εἶναι τὰ σταθερὰ πολυώνυμα.*

Στὴν παρακάτω πρόταση, τὸ (1) ἀποδεικνύεται πολὺ εὔκολα ἀπ' τοὺς ὁρισμούς· ἡ ἀπόδειξη τοῦ (2) εἶναι σχεδὸν ἄμεση συνέπεια τοῦ (3) τῆς πρότασης Α′.2.

Πρόταση Α′.4. *1. ῎Αν $f(X), g(X) \in K[X]$ καὶ τὸ $g(X)$ εἶναι ἀνάγωγο, τότε, τὰ πολυώνυμα αὐτά, ἢ εἶναι πρῶτα μεταξύ τους, ἢ $g(X)|f(X)$· στὴ δεύτερη περίπτωση, τὸ $g(X)$ εἶναι ΜΚΔ τῶν δύο πολυωνύμων.*

2. ῎Εστω ὅτι $f(X), g(X) \in K[X]$. ῎Αν ὑπάρχει ἐπέκταση L τοῦ K, ἡ ὁποία νὰ περιέχει μία κοινὴ ρίζα τῶν $f(X), g(X)$, τότε τὰ πολυώνυμα αὐτὰ δὲν εἶναι πρῶτα μεταξύ τους. ῎Αν, ἐπιπλέον, τὸ $g(X)$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ K, τότε $g(X)|f(X)$.

῎Αν, γιὰ παράδειγμα, ξέρομε ὅτι δύο πολυώνυμα μὲ ρητοὺς συντελεστὲς ἔχουν μία κοινὴ μιγαδικὴ ρίζα (ἐδῶ $K = \mathbb{Q}$ καὶ $L = \mathbb{C}$), τότε ἀποκλείεται νὰ εἶναι πρῶτα μεταξύ τους: ὁ ΜΚΔ τους εἶναι μὴ σταθερὸ πολυώνυμο μὲ ρητοὺς συντελεστές. ῎Αν, ἐπιπλέον, τὸ ἕνα ἀπὸ τὰ δύο πολυώνυμα εἶναι ἀνάγωγο, πάνω ἀπ' τὸ $\mathbb{Q}$, τότε αὐτὸ τὸ πολυώνυμο διαιρεῖ (στὸ $\mathbb{Q}[X]$) τὸ ἄλλο πολυώνυμο.

Εύρεση του ΜΚΔ

῾Η εὕρεση τοῦ ΜΚΔ δύο πολυωνύμων $f(X), g(X) \in K[X]$ γίνεται μὲ τὸν *Εὐκλείδειο ᾿Αλγόριθμο*, ἐκτελώντας διαδοχικὲς διαιρέσεις μέχρις ὅτου βροῦμε ὑπόλοιπο 0 [1], ὡς ἑξῆς:

$$\begin{aligned}
f(X) &= g(X)q(X) + r_1(X)\\
g(X) &= r_1(X)q_1(X) + r_2(X)\\
r_1(X) &= r_2(X)q_2(X) + r_3(X)\\
r_2(X) &= r_3(X)q_3(X) + r_4(X)\\
\vdots\ & \quad \vdots\\
r_{n-2}(X) &= r_{n-1}(X)q_{n-1}(X) + r_n(X)\\
r_{n-1}(X) &= r_n(X)q_n(X) + 0
\end{aligned}$$

Τὸ τελευταῖο μὴ μηδενικὸ ὑπόλοιπο, ἔστω $r_n(X)$, εἶναι ΜΚΔ τῶν $f(X), g(X)$.

Παράδειγμα 1. ῎Εστω $f(X) = X^3 - 1$, $g(X) = X^3 + 3X + 3 \in \mathbb{Q}[X]$. ᾿Εδῶ $q(X) = 1$ καὶ $r(X) = -3X - 4$, ἄρα $f_1(X) = g(X) = X^3 + 3X + 3$ καὶ $g_1(X) = r(X) = -3X - 4$. ῾Η εὐκλείδεια διαίρεση τοῦ $f_1(X)$ μὲ τὸ $g_1(X)$ δίνει $q_1(X) = -\frac{1}{3}X^2 + \frac{4}{9}X - \frac{43}{27}$ καὶ $r_1(X) = -\frac{91}{27}$. Τὸ $r_1(X)$ εἶναι τὸ τελευταῖο μὴ μηδενικὸ ὑπόλοιπο. Διότι, ἂν θέσομε $f_2(X) = g_1(X)$ καὶ $g_2(X) = r_1(X)$, ἐπειδὴ τὸ $r_1(X)$ εἶναι σταθερὸ πολυώνυμο, ἡ εὐκλείδεια διαίρεση τοῦ $f_2(X)$ μὲ τὸ σταθερὸ πολυώνυμο θὰ δώσει ὑπόλοιπο 0.[2] ῎Αρα, ὁ μέγιστος κοινὸς διαιρέτης τῶν $X^3 - 1$ καὶ $X^3 + 3X + 3$ εἶναι $-\frac{91}{27}$. ᾿Αλλὰ τότε, τὸ σύνολο τῶν μεγίστων κοινῶν διαιρετῶν τῶν $X^3 - 1$ καὶ $X^3 + 3X + 3$ εἶναι τὸ σύνολο $\{c(-\frac{91}{27}) : c \in \mathbb{Q}\} = \mathbb{Q}$ (ἄρα, ἕνας μέγιστος κοινὸς διαιρέτης εἶναι καὶ τὸ σταθερὸ πολυώνυμο 1). Τὰ συγκεκριμένα πολυώνυμα, λοιπόν, εἶναι *πρῶτα μεταξύ τους*.

[1] ᾿Αποδεικνύεται εὔκολα ὅτι αὐτὸ θὰ συμβεῖ ὁπωσδήποτε.

[2] Γενικά, ἡ εὐκλείδεια διαίρεση τοῦ $f(X) \in K[X]$ μὲ τὸ σταθερὸ ($\neq 0$) πολυώνυμο c εἶναι $f(X) = cg(X) + 0$, ὅπου $g(X) = c^{-1}f(X)$.

Ἡ διαδικασία εὑρέσεως τοῦ μεγίστου κοινοῦ διαιρέτη, μᾶς ἐπιτρέπει νὰ βροῦμε πολυώνυμα $f'(X)$ καὶ $g'(X)$, τέτοια ὥστε $f'(X)f(X) + g'(X)g(X) = \text{μκδ} = 1$. Πράγματι, ἔχομε

$$(\text{Α}'.1)\quad f(X) = g(X)\cdot 1 + (-3X-4) \quad \text{καὶ} \quad X^3+3X+3 = (-3X-4)(-\frac{1}{3}X^2+\frac{4}{9}X-\frac{43}{27})-\frac{91}{27}.$$

Ἡ δεύτερη σχέση (Α΄.1) γράφεται

$$(\text{Α}'.2)\qquad -\frac{91}{27} = X^3 + 3X + 3 + (-3X-4)(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}).$$

Πολλαπλασιάζοντας τὴν πρώτη σχέση (Α΄.1) μὲ $(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27})$ βλέπομε ὅτι

$$(-3X-4)(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}) = (f(X) - g(X))(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}),$$

καὶ τότε, ἀπὸ τὴν (Α΄.2),

$$\begin{aligned} -\frac{91}{27} &= g(X) + (f(X)-g(X))(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}) \\ & f(X)(\frac{1}{3}X^2 - \frac{4}{9}X + \frac{43}{27}) + g(X)(-\frac{1}{3}X^2 + \frac{4}{9}X - \frac{16}{27}). \end{aligned}$$

Πολλαπλασιάζοντας τὴν τελευταία σχέση ἐπὶ $-\frac{27}{91}$ βρίσκομε

$$1 = f(X)\underbrace{(-\frac{9}{91}X^2 + \frac{12}{91}X - \frac{43}{91})}_{f'(X)} + g(X)\underbrace{(\frac{9}{91}X^2 - \frac{12}{91}X + \frac{16}{91})}_{g'(X)}.$$

Παράδειγμα 2. Ἂς θεωρήσομε τὰ πολυώνυμα τοῦ προηγουμένου παραδείγματος, ἀλλὰ τώρα πάνω ἀπὸ τὸ σῶμα $\mathbb{Z}_5$: $f(X) = X^3 - 1 = X^3 + 4$, $g(X) = X^3 + 3X + 3 \in \mathbb{Z}_5[X]$. Ἡ εὐκλείδεια διαίρεση τοῦ $f(X)$ διὰ $g(X)$ δίνει πηλῖκο $q(X) = 1$ καὶ ὑπόλοιπο $r(X) = 2X - 1$, ἄρα $f(X) = g(X) + (2X + 1)$. Μετά, $f_1(X) = g(X) = X^3 + 3X + 3$, $g_1(X) = r(X) = 2X + 1$ καὶ ἡ σχέση τῆς εὐκλείδειας διαίρεσης εἶναι $X^3 + 3X + 3 = (2X + 1)(3X^2 + X + 1) + 2$ ($q_1(X) = 3X^2 + X + 1$ καὶ $r_1(X) = 2$). Ἀφοῦ καταλήξαμε σὲ ὑπόλοιπο, ποὺ εἶναι σταθερὸ πολυώνυμο, ἕπεται ὅτι αὐτὸ εἶναι ὁ ζητούμενος μέγιστος κοινὸς διαιρέτης (ὅπως καὶ στὸ παράδειγμα 1). Οἱ σχέσεις

$$f(X) = g(X) + (2X+1), \quad g(X) = (2X+1)(3X^2+X+1) + 2$$

μᾶς ἐπιτρέπουν νὰ γράψομε τὸ 2 ὡς γραμμικὸ συνδυασμὸ τῶν $f(X)$ καὶ $g(X)$:

$$\begin{aligned} 2 &= g(X) - (2X+1)(3X^2+X+1) = g(X) - (f(X)-g(X))(3X^2+X+1) \\ &= f(X)(-3X^2 - X - 1) + (3X^2 + X + 2) \\ &= (2X^2 + 4X + 4)f(X) + (3X^2 + X + 2)g(X). \end{aligned}$$

Ἂν προτιμοῦμε στὴ θέση τοῦ 2 νὰ ἔχομε τὸ 1, πολλαπλασιάζομε τὴν παραπάνω σχέση ἐπὶ 3 ($3 \cdot 2 = 1$ στὸ $\mathbb{Z}_5$), ὁπότε παίρνομε τὴ σχέση

$$1 = (X^2 + 2X + 2)f(X) + (4X^2 + 3X + 1)g(X).$$

Ἀσκήσεις

1. Γιὰ κάθ' ἕνα ἀπὸ τὰ παρακάτω ζεύγη πολυωνύμων $f(X), g(X)$ ὑπολογῖστε, μὲ τὸν εὐκλείδειο ἀλγόριθμο, τὸν ΜΚΔ τους, καθὼς καὶ πολυώνυμα $f'(X), g'(X)$, τέτοια ὥστε $f'(X)f(X) + g'(X)g(X) = \text{ΜΚΔ}(f(X), g(X))$.

   - $f(X) = X^4 + X^3 + X + 1,\ g(X) = X^2 + X + 1 \in \mathbb{Q}[X]$
   - $f(X) = X^4 + X^3 + X + 1,\ g(X) = X^2 + X + 1 \in \mathbb{Z}_5[X]$
   - $f(X) = X^5 + 2X^4 + X^2 + 3X + 2,\ g(X) = X^3 + 2X^2 + X + 2 \in \mathbb{Q}[X]$
   - $f(X) = X^5 + 2X^4 + X^2 + 3X + 2,\ g(X) = X^3 + 2X^2 + X + 2 \in \mathbb{Z}_5[X]$
   - $f(X) = X^5 + 2X^4 + X^2 + 3X + 2,\ g(X) = X^3 + 2X^2 + X + 2 \in \mathbb{Z}_7[X]$

2. Ἔστω ὅτι τὰ $f(X), g(X) \in K[X]$ εἶναι πρῶτα μεταξύ τους καὶ L εἶναι ἐπέκταση τοῦ K. Ἀποδεῖξτε ὅτι τὰ $f(X), g(X)$, θεωρούμενα ὡς πολυώνυμα τοῦ $L[X]$, ἐξακολουθοῦν νὰ παραμένουν πρῶτα μεταξύ τους.

   Ὑπόδειξη. Χρησιμοποιεῖστε τὴν Πρόταση 3.

Παράρτημα Β΄

Χρήσιμες προτάσεις γιὰ πολυώνυμα

Ἔστω σῶμα K. Θὰ δώσομε κάποιες χρήσιμες προτάσεις γιὰ πολυώνυμα μὲ συντελεστὲς ἀπὸ τὸ K. Κάποιες προτάσεις ἰσχύουν μόνο γιὰ $K = \mathbb{Q}$.

Πρόταση Β΄.1. *1. Τὸ νὰ ἔχει τὸ $f(X) \in K[X]$ πρωτοβάθμιο παράγοντα μὲ συντελεστὲς ἀπὸ τὸ K, ἰσοδυναμεῖ μὲ τὸ νὰ ὑπάρχει ρίζα τοῦ $f(X)$ στὸ K.*

2. Ἂν ὁ βαθμὸς τοῦ $f(X) \in K[X]$ εἶναι 2 ἢ 3 καὶ τὸ $f(X)$ δὲν εἶναι ἀνάγωγο στὸ $K[X]$, τότε, τὸ $f(X)$ ἔχει ρίζα στὸ K. Ἄρα, ἂν διαπιστώσομε ὅτι ἕνα τέτοιο πολυώνυμο δὲν ἔχει ρίζα στὸ K, τότε τὸ πολυώνυμο εἶναι ἀνάγωγο.

Προσοχή! Ἂν τὸ $f(X)$ ἔχει βαθμὸ τοὐλάχιστον 4, τότε, ἡ μὴ ὕπαρξη ρίζας στὸ K δὲν σημαίνει ὅτι τὸ $f(X)$ εἶναι ἀνάγωγο. Γιὰ παράδειγμα, τὸ $f(X) = X^4 - 5X^2 + 6 \in \mathbb{Q}[X]$ δὲν ἔχει ρίζα στὸ $\mathbb{Q}$, ἀλλὰ δὲν εἶναι ἀνάγωγο, ἀφοῦ $f(X) = (X^2 - 2)(X^2 - 3)$.

Σὲ κάποιες εἰδικές, ἀλλὰ σημαντικὲς περιπτώσεις, ἡ εὕρεση τοῦ συνόλου ὅλων τῶν ριζῶν τοῦ $f(X)$, οἱ ὁποῖες ἀνήκουν στὸ K (αὐτὸ τὸ σύνολο μπορεῖ νὰ εἶναι κενό), εἶναι πεπερασμένη διαδικασία. Προφανῶς, αὐτὸ εἶναι ἀληθὲς ὅταν $K = \mathbb{Z}_p$, p πρῶτος καί, γενικότερα, ὅταν τὸ K εἶναι πεπερασμένο σῶμα. Τότε, γιὰ κάθε $u \in K$ ἐξετάζομε κατα πόσον $f(u) = 0$ καὶ τὸ πλῆθος των δοκιμῶν μας εἶναι πεπερασμένο, ἀφοῦ τὸ K εἶναι πεπερασμένο.

Μία ἄλλη σημαντικὴ περίπτωση εἶναι ὅταν $K = \mathbb{Q}$. Ἐπειδὴ ἕνα πολυώνυμο $f(X) \in \mathbb{Q}[X]$ μπορεῖ νὰ πολλαπλασισαθεῖ μὲ κατάλληλο ἀκέραιο d γιὰ νὰ διαγραφοῦν οἱ τυχὸν παρονομαστὲς τῶν συντελεστῶν του, καὶ τὸ $d \cdot f(X)$ ἔχει τὶς ἴδιες ρίζες μὲ τὸ $f(X)$, γι' αὐτό, ἀρκεῖ νὰ ἐξετάσομε πολυώνυμα μὲ ἀκέραιους συντελεστές.

Πρόταση Β΄.2. *Ἔστω $f(X) \in \mathbb{Z}[X]$ μὲ συντελεστὴ μεγιστοβαθμίου ὅρου a καὶ σταθερὸ ὅρο c. Ἂν τὸ $f(X)$ ἔχει ρητὴ ρίζα καὶ τὴν γράψομε μὲ τὴ μορφὴ ἀναγώγου κλάσματος m/n (δηλαδή, $(m, n) = 1$), τότε $m|c$ καὶ $n|a$.*

Γιὰ παράδειγμα, ἂν τὸ πολυώνυμο $f(X) = 10X^5 + 3X^4 - X^3 + 7X^2 - 2X + 4 \in \mathbb{Z}[X]$ ἔχει ρητὴ ρίζα, αὐτὴ πρέπει νὰ ἀναζητηθεῖ μεταξὺ τῶν ἀριθμῶν τῆς ἑξῆς λίστας:
$\pm\frac{1}{1} = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{5}, \pm\frac{1}{10}, \pm\frac{2}{1} = \pm 2, \pm\frac{2}{2} = \pm 1, \pm\frac{2}{5}, \pm\frac{2}{10} = \pm\frac{1}{5}, \pm\frac{4}{1} = \pm 4, \pm\frac{4}{2} = \pm 2, \pm\frac{4}{5}, \pm\frac{4}{10} = \pm\frac{2}{5}$.
Δοκιμάζοντας ἕναν-ἕναν αὐτοὺς τοὺς ἀριθμούς, βλέπομε ποιοὶ εἶναι ρίζες τοῦ $f(X)$. Στὴ συγκεκριμένη περίπτωση, διαπιστώνομε ὅτι οὐδεὶς ἀπὸ αὐτοὺς τοὺς ἀριθμοὺς εἶναι ρίζα τοῦ $f(X)$, ἄρα, σύμφωνα μὲ τὴν πρόταση Β΄.2, τὸ πολυώνυμο αὐτὸ δὲν ἔχει ρητὲς ρίζες.

Ὅσον ἀφορᾶ στὴν ἐξέταση τοῦ κατὰ πόσον ἕνα πολυώνυμο μὲ ἀκέραιους συντελεστὲς εἶναι ἀνάγωγο πάνω ἀπὸ τὸ $\mathbb{Q}$, ἐξαιρετικὰ χρήσιμο εἶναι τὸ

Λῆμμα τοῦ Gauss. *Γιὰ νὰ ἐξετάσομε ἂν τὸ μὴ σταθερὸ $f(X) \in \mathbb{Z}[X]$ εἶναι ἀνάγωγο πάνω ἀπὸ τὸ $\mathbb{Q}$, ἀρκεῖ νὰ ἐξετάσομε ἂν ὑπάρχει ἀνάλυση $f(X) = g(X)h(X)$ μὲ τὰ $g(X), h(X) \in \mathbb{Z}[X]$ μὴ σταθερά.*

Γιὰ παράδειγμα, ἔστω ὅτι θέλομε νὰ ἐξετάσομε κατὰ πόσον τὸ $f(X) = X^4 - 6X^3 + kX^2 + 3X + 4$, ὅπου $k \in \mathbb{Z}$, εἶναι ἀνάγωγο πάνω ἀπὸ τὸ $\mathbb{Q}$. Ἐξετάζομε πρῶτα ἂν ἔχει πρωτοβάθμιο παράγοντα. Ἀπὸ τὸ 1 τῆς πρότασης Β′.1 ἀρκεῖ νὰ ἐξετάσομε ἂν τὸ $f(X)$ ἔχει ρητὲς ρίζες. Οἱ μόνες *πιθανὲς* ρητὲς ρίζες, σύμφωνα μὲ τὴν πρόταση Β′.2 εἶναι $\pm1, \pm2, \pm4$. Ὑπολογίζομε $f(1) = 2+k$, $f(-1) = 8+k$, $f(2) = -22+4k$, $f(-2) = 62+4k$, $f(4) = -112+16k$ καὶ $f(-4) = 632+16k$. Οὐδεμία ἀκέραια τιμὴ τοῦ k μηδενίζει τὰ $f(\pm2)$, $f(-4)$, ἐνῶ τὰ $f(1)$, $f(-1)$, $f(4)$ μηδενίζονται γιὰ $k = -2, -8, 7$, ἀντιστοίχως. Συνεπῶς, γιὰ $k = -2, -8, 7$, τὸ $f(X)$ ἔχει πρωτοβάθμιο παράγοντα καί, συνεπῶς, δὲν εἶναι ἀνάγωγο. Γιὰ τὶς ὑπόλοιπες ἀκέραιες τιμὲς τοῦ k δὲν μποροῦμε *ἀκόμη* νὰ ἀποφανθοῦμε μὲ βεβαιότητα. Πρέπει νὰ ἐξετάσομε ἂν τὸ $f(X)$ ἀναλύεται σὲ δευτεροβάθμιους παράγοντες, πρᾶγμα τὸ ὁποῖο κάνομε ἀμέσως παρακάτω: $f(X) = (aX^2 + bX + c)(a'X^2 + b'X + c')$. Τὸ λῆμμα τοῦ Gauss μᾶς λέει ὅτι, ἀρκεῖ νὰ ὑποθέσομε τοὺς a, b, c, a', b', c' ἀκεραίους. Ἀλλὰ τότε, συγκρίνοντας τοὺς μεγιστοβαθμίους ὅρους, ἔχομε $aa' = 1$, ἄρα, καθὼς τὰ a, a' εἶναι ἀκέραιοι, συμπεραίνομε ὅτι $a = a' = \pm1$. Χωρὶς βλάβη τῆς γενικότητας, μποροῦμε νὰ πάρομε $a = a' = 1$ καὶ τώρα,

$$X^4 - 6X^3 + kX^2 + 3X + 4 = X^4 + (b + b')X^3 + (c + c' + bb')X^2 + (bc' + cb')X + cc' ,$$

ὁπότε

$$b + b' = -6 , \quad bc' + cb' = 3 , \quad b + b' + cc' = k , \quad cc' = 4 .$$

Ἀπὸ τὴν τελευταία, λόγῳ τοῦ ὅτι οἱ c, c' εἶναι ἀκέραιοι, παίρνομε

$$(c, c') = (4, 1), (-4, -1), (2, 2), (-2, -2).$$

Οἱ δύο τελευταῖες περιπτώσεις πρέπει νὰ ἀποκλεισθοῦν, γιατὶ συνεπάγονται ὅτι $3 = bc' + cb' = \pm2(b + b')$, ἀδύνατον, ἀφοῦ οἱ b, b' εἶναι ἀκέραιοι. Ἂν $c = 4, c' = 1$, τότε, λύνοντας ὡς πρὸς b, b' τὸ σύστημα τῶν δύο πρώτων ἐξισώσεων, παίρνομε $b = -9, b' = 3$, ὁπότε ἡ τρίτη σχέση δίνει $-22 = k$. Ἂν $c = -4, c' = -1$, τότε, μὲ ἀνάλογο τρόπο βρίσκομε $b = -7, b' = 1$ καὶ $-12 = k$.
Συμπέρασμα. Γιὰ $k \neq -2, -8, 7, -12, -22$ τὸ $f(X)$ εἶναι ἀνάγωγο στὸ $\mathbb{Q}[X]$, ἐνῶ γιὰ τὶς ἐξαιρεθεῖσες τιμές, τὸ $f(X)$ παραγοντοποιεῖται ὡς ἑξῆς:

$$\begin{aligned}
k = -2 &: \quad f(X) = (X - 1)(X^3 - 5X^2 - 7X - 4) \\
k = -8 &: \quad f(X) = (X + 1)(X^3 - 7X^2 - X + 4) \\
k = 7 &: \quad f(X) = (X - 4)(X^3 - 2X^2 - X - 1) \\
k = -12 &: \quad f(X) = (X^2 + X - 1)(X^2 - 7X - 4) \\
k = -22 &: \quad f(X) = (X^2 + 3X + 1)(X^2 - 9X + 4)
\end{aligned}$$

Κριτήριο τοῦ Eisenstein. *Ἔστω $f(X) = a_nX^n + a_{n_1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$, $n \geq 2$. Ἂν ὑπάρχει πρῶτος p, τέτοιος ὥστε*

$$p | a_i \quad \text{γιὰ ὅλα τὰ } i = 0, 1, \ldots, n-1 , \quad p \nmid a_n , \quad p^2 \nmid a_0 ,$$

τότε τὸ $f(X)$ εἶναι ἀνάγωγο στὸ $\mathbb{Q}[X]$.

Μία ἄμεση, πολὺ ἐνδιαφέρουσα ἐφαρμογὴ τοῦ κριτηρίου τοῦ Eisenstein εἶναι ὅτι, γιὰ κάθε ἀκέραιο $n \geq 2$, κάθε πρῶτο p καὶ κάθε ἀκέραιο a, ὁ ὁποῖος δὲν διαιρεῖται διὰ p, τὸ πολυώνυμο $X^n - pa$ εἶναι ἀνάγωγο στὸ $\mathbb{Q}[X]$.

Τὸ παρακάτω τέχνασμα, παρὰ τὴν ἁπλότητά του, εἶναι πολὺ χρήσιμο.

Τέχνασμα. *Ἔστω $c \in k$ καὶ $f(X) \in K[X]$. Τὸ $f(X)$ εἶναι ἀνάγωγο στὸ $K[X]$ ἄν, καὶ μόνο ἄν, τὸ $f(X + c)$ εἶναι ἀνάγωγο στὸ $K[X]$.*

Μία ἐνδιαφέρουσα ἐφαρμογὴ αὐτοῦ τοῦ τεχνάσματος, σὲ συνδυασμὸ μὲ τὸ κριτήριο τοῦ Eisenstein, εἶναι ἡ ἑξῆς:

Πρόταση Β΄.3. *Ἔστω p πρῶτος. Τὸ p-τάξεως κυκλοτομικὸ πολυώνυμο $f_p(X) = X^{p-1} + \cdots + X + 1$ εἶναι ἀνάγωγο στὸ $\mathbb{Q}[X]$.*

Πράγματι, εἶναι $f_p(X) = \dfrac{X^p - 1}{X - 1}$, ὁπότε

$$f_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1} X^{p-2} + \cdots \binom{p}{p-1}.$$

Εἶναι γνωστὴ ἄσκηση τῆς στοιχειώδους Θεωρίας Ἀριθμῶν ὅτι, γιὰ κάθε $k = 1, \ldots, p-1$, ὁ διωνυμικὸς συντελεστὴς $\binom{p}{k}$ εἶναι πολλαπλάσιο τοῦ p. Ἄρα, τὸ κριτήριο τοῦ Eisenstein, ἐφαρμόζεται στὸ τελευταῖο πολυώνυμο (τοῦ ὁποίου ὁ σταθερὸς ὅρος ἰσοῦται μὲ p), ὁπότε συμπεραίνομε ὅτι τὸ $f_p(X+1)$ εἶναι ἀνάγωγο, ἄρα καὶ τὸ $f_p(X)$ εἶναι ἀνάγωγο στὸ $\mathbb{Q}[X]$.

Παράρτημα Γ′

Συμμετρικὰ πολυώνυμα

Σὲ αὐτὸ τὸ Παράρτημα δίνομε τὴν ἀπόδειξη τοῦ Θεωρήματος 1.6.1. Στὴν πραγματικότητα, ἀποδεικνύομε κάτι περισσότερο· βλ. τὴν ἐκφώνηση παρακάτω. Ἔστω R ἕνας δακτύλιος καὶ μὴ μηδενικὸ $f \in R[X_1, \ldots, X_n]$. Ὁρίζομε τὸ *βάρος* τοῦ f ὡς ἑξῆς: Τὸ βάρος ἑνὸς μονωνύμου $X_1^{j_1} \cdots X_n^{j_n}$ τοῦ f εἶναι, ἐξ ὁρισμοῦ, ὁ ἀριθμὸς $j_1 + 2j_2 + \ldots + nj_n$. Βάρος τοῦ f ὁρίζεται νὰ εἶναι τὸ μέγιστο τῶν βαρῶν ὅλων τῶν μονωνύμων ποὺ ἐμφανίζονται στὸ f (ἐννοεῖται, μὲ μὴ μηδενικὸ συντελεστή). Ἂν τὸ f εἶναι σταθερό (μὴ μηδενικό), τὸ βάρος του εἶναι 0. Θὰ ἀποδείξομε τὸ θεμελιῶδες θεώρημα τῶν συμμετρικῶν πολυωνύμων ὑπὸ τὴν ἑξῆς ἀκριβέστερη μορφή:

Θεώρημα Γ′.1. *Ἔστω $f \in R[X_1, \ldots, X_n]$ συμμετρικὸ βαθμοῦ d. Τότε, γιὰ κάποιο $g \in R[X_1, \ldots, X_n]$ βάρους $\leq d$, $f(X_1, \ldots, X_n) = g(S_1, \ldots, S_n)$, ὅπου $S_1, \ldots, S_n$ εἶναι τὰ στοιχειώδη συμμετρικὰ πολυώνυμα τῶν $X_1, \ldots, X_n$.*

Ἀπόδειξη. Μὲ ἐπαγωγὴ ἐπὶ τοῦ n. Ἂν $n = 1$, ὁ ἰσχυρισμὸς τοῦ θεωρήματος εἶναι τετριμμένος. Ὑποθέτομε ὅτι ἀληθεύει γιὰ ὅλα τὰ συμμετρικὰ πολυώνυμα $n-1$ μεταβλητῶν ($n > 1$) κι ἂς θεωρήσομε ἕνα συμμετρικὸ πολυώνυμο $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$. Μὲ $S_1, \ldots, S_n$ συμβολίζομε τὰ στοιχειώδη συμμετρικὰ πολυώνυμα τῶν $X_1, \ldots, X_n$ καὶ μὲ $S'_1, \ldots, S'_{n-1}$ τὰ ἀντίστοιχα γιὰ τὶς μεταβλητὲς $X_1, \ldots, X_{n-1}$. Προφανῶς, γιὰ κάθε $i = 1, \ldots, n-1$,

$$S'_i(X_1, \ldots, X_{n-1}) = S_i(X_1, \ldots, X_{n-1}, 0)\ . \tag{Γ′.1}$$

Τώρα κάνομε ἐπαγωγὴ ἐπὶ τοῦ d. Γιὰ $d = 0$ δὲν ἔχομε τίποτε νὰ ἀποδείξομε. Ἔστω ὅτι $d \geq 1$ καὶ τὸ θεώρημα ἔχει ἤδη ἀποδειχθεῖ γιὰ ὅλα τὰ πολυώνυμα τοῦ $R[X_1, \ldots, X_{n-1}]$ βαθμοῦ $< d$. Τὸ $f(X_1, \ldots, X_{n-1}, 0) \in R[X_1, \ldots, X_{n-1}]$ εἶναι συμμετρικὸ πολυώνυμο ὁπότε, λόγῳ ἐπαγωγικῆς ὑποθέσεως,

$$f(X_1, \ldots, X_{n-1}, 0) = g_1(S'_1, \ldots, S'_{n-1}) \tag{Γ′.2}$$

γιὰ κάποιο $g_1 \in R[X_1, \ldots, X_{n-1}]$ βάρους $\leq d$. Ἂν $X_1^{j_1} \cdots X_{n-1}^{j_{n-1}}$ εἶναι τὸ μονώνυμο τοῦ g_1 μὲ τὸ μέγιστο βάρος, τότε $j_1 + 2j_2 + \ldots + (n-1)j_{n-1} \leq d$. Ἂς θεωρήσομε τώρα τὸ πολυώνυμο $g_1(S_1, \ldots, S_{n-1}) \in R[X_1, \ldots, X_n]$. Ἂν τὸ δοῦμε ὡς R-γραμμικὸ συνδυασμὸ ὅρων τῆς μορφῆς $S_1^{k_1} \cdots S_{n-1}^{k_{n-1}}$, ὁ ὅρος μὲ τὸ μέγιστο βαθμὸ (ὡς πρὸς $X_1, \ldots, X_n$) εἶναι, προφανῶς, ὁ $S_1^{j_1} \cdots S_{n-1}^{j_{n-1}}\cdot$ ὁ βαθμός του εἶναι, φυσικά, $j_1 + 2j_2 + \ldots + (n-1)j_{n-1} \leq d$. Ὁρίζομε τώρα τὸ πολυώνυμο

$$f_1(X_1, \ldots, X_n) = f(X_1, \ldots, X_n) - g_1(S_1, \ldots, S_{n-1})\ , \tag{Γ′.3}$$

τὸ ὁποῖο εἶναι συμμετρικό, βαθμοῦ $\leq d$. Λόγῳ τῶν (Γ′.1), (Γ′.2),

$$f_1(X_1, \ldots, X_{n-1}, 0) = 0 ,$$

ποὺ σημαίνει ὅτι τὸ f_1 διαιρεῖται ἀπὸ τὸ X_n. Συνεπῶς, λόγῳ συμμετρίας, τὸ f_1, διαιρεῖται ἐπίσης ἀπὸ τὰ $X_1, \ldots, X_{n-1}$, ἄρα

$$f_1(X_1, \ldots, X_n) = S_n \cdot f_2(X_1, \ldots, X_n) \tag{Γ′.4}$$

γιὰ κάποιο $f_2 \in R[X_1, \ldots, X_n]$ συμμετρικό, βαθμοῦ $\leq d - n < d$. Ἡ ἐπαγωγικὴ ὑπόθεση στὸ d συνεπάγεται ὅτι ὑπάρχει $g_2 \in R[X_1, \ldots, X_n]$ βάρους $\leq d - n$, τέτοιο ὥστε

$$f_2(X_1, \ldots, X_n) = g_2(S_1, \ldots, S_n) .$$

Ἡ τελευταία σχέση, ἐν συνδυασμῷ, μὲ τὶς (Γ′.3) καὶ (Γ′.4) δίνουν

$$f(X_1, \ldots, X_n) = g_1(S_1, \ldots, S_{n-1}) + g_2(S_1, \ldots, S_n) \cdot S_n .$$

Τὸ δεξιὸ μέλος προκύπτει ὅταν στὸ πολυώνυμο

$$g(X) \overset{ορσ}{=} g_1(X_1, \ldots, X_{n-1}) + g_2(X_1, \ldots, X_n) \cdot X_n$$

τὰ $X_1, \ldots, X_n$ ἀντικατασταθοῦν ἀπὸ τὰ $S_1, \ldots, S_n$, ἀντιστοίχως. Ἐπιπλέον, τὸ βάρος τοῦ g_1, ὅπως εἴδαμε παραπάνω, εἶναι $\leq d$ καὶ τὸ βάρος τοῦ $g_2(X_1, \ldots, X_n) \cdot X_n$ εἶναι $\leq (d-n) + n \cdot 1 \leq n$. Συνεπῶς τὸ βάρος τοῦ g εἶναι $\leq d$. □

Ἀσκήσεις

1. Ἐκφράστε τὰ πολυώνυμα $X_1^2 + X_2^2$ καὶ $X_1^3 + X_2^3$ συναρτήσει τῶν στοιχειωδῶν συμμετρικῶν πολυωνύμων $S_1 = X_1 + X_2, S_2 = X_1 X_2$.

2. Ἐκφράστε τὰ πολυώνυμα $X_1^2 + X_2^2 + X_3^2$ καὶ $X_1^3 + X_2^3 + X_3^3$ συναρτήσει τῶν στοιχειωδῶν συμμετρικῶν πολυωνύμων $S_1 = X_1 + X_2 + X_3, S_2 = X_1 X_2 + X_2 X_3 + X_3 X_1, S_3 = X_1 X_2 X_3$.

3. Ἂν u_1, u_2 εἶναι οἱ ρίζες τοῦ $aX^2 + bX + c$, ἐκφράστε τὴν παράσταση

   $$(u_1 - u_2)^2$$

   συναρτήσει τῶν a, b, c.
   Ὑπόδειξη. Παρατηρῆστε ὅτι ἡ παράσταση αὐτὴ εἶναι συμμετρικὴ ὡς πρὸς τὰ u_1, u_2. Χρησιμοποιῆστε, ἐπίσης, τοὺς τύπους τοῦ Viète γιὰ τὶς σχέσεις ριζῶν καὶ συντελεστῶν ἑνὸς πολυωνύμου.

4. Ἂν u_1, u_2, u_3 εἶναι οἱ ρίζες τοῦ $X^3 + pX + q$, ἐκφράστε τὴν παράσταση

   $$((u_1 - u_2)(u_1 - u_3)(u_2 - u_3))^2$$

   συναρτήσει τῶν p, q.
   Ὑπόδειξη. Ὅπως καὶ στὴν ἄσκηση 3.

Εὑρετήριο