Κεφάλαιο 13

13.1 13^{η} Εβδομάδα

Το τεταρτοβάθμιο πολυώνυμο (συνέχεια)

Στην απόδειξη του Θεωρήματος, παρακάτω, θα γίνει χρήση των εξής προτάσεων της Θεωρίας Ομάδων:

Πρόταση 13.1. *Αν $H \leq S_n$ και $[S_n : H] = 2$, τότε $H = A_n$, δηλαδή, η μόνη υποομάδα της S_n με δείκτη 2 στην S_n είναι η εναλλάσουσα ομάδα A_n.*

Πρόταση 13.2. *Έστω πεπερασμένη ομάδα G τάξεως $p^n m$, όπου ο p είναι πρώτος, $n \geq 1$ και $p \nmid m$. Αν H_1, H_2 είναι υποομάδες της G τάξεως p^n (δηλαδή, οι H_1, H_2 είναι p-υποομάδες Sylow της G[1]), τότε αυτές είναι ισόμορφες* [2].

Με δεδομένα τους συμβολισμούς και τα αποτελέσματα της ενότητας «Το τεταρτοβάθμιο πολυώνυμο» του προηγούμενου μαθήματος [3] έχομε το εξής:

Θεώρημα 13.3. (1) *Αν $m = 6$, τότε $G = S_4$.*
(2) *Αν $m = 3$, τότε $G = A_4$.*
(3) *Αν $m = 1$, τότε $G = V$.*
(4) *Αν $m = 2$ και το f είναι ανάγωγο πάνω από το K, τότε $G \cong D_4$.*
(5) *Αν $m = 2$ και το f δεν είναι ανάγωγο πάνω από το K, τότε $G \cong \mathbb{Z}_4$.*

Απόδειξη. Έστω $m \in \{3, 6\}$. Τότε, από την 4^{η} και την 1^{η} σχέσης στην (12.6), έπεται ότι $|G| \in \{12, 24\}$. Αν $|G| = 24$, τότε, προφανώς, $G = S_4$. Αν $|G| = 12$, τότε $[S_4 : G] = 2$ και από την Πρόταση 13.1 συμπεραίνομε ότι $G = A_4$. Τα στοιχεία της υποομάδας V είναι άρτιες μεταθέσεις, άρα, και στις δύο περιπτώσεις, $V \leq G$ και, συνεπώς, $G \cap V = V$, άρα $|G \cap V| = 4$. Τότε, από την 4^{η} σχέση στην (12.6), $|G| = 4m$. Από αυτή τη σχέση, σε συνδυασμό και με τα παραπάνω συμπεράσματα, γίνεται φανερό ότι, $m = 6 \Rightarrow G = S_4$ και $m = 3 \Rightarrow G = A_4$. Έτσι αποδείχθηκαν τα (1) και (2).

Έστω $m = 1$. Τότε, στο διάγραμμα αμέσως μετά την απόδειξη του Λήμματος 12.9, είναι $K = F$, άρα $G \cap V = V$. Αυτό σημαίνει ότι $G \leq V$. Η G δεν μπορεί να είναι γνήσια υποομάδα της $G \cap V$, διότι η τάξη της G είναι πολλαπλάσιο του 4, άρα $G = V$, οπότε αποδείχθηκε και το (3).

Έστω $m = 2$. Από την 1^{η}, 2^{η} και 4^{η} στη (12.6) έπεται ότι $|G| \in \{4, 8\}$. Σύμφωνα με την άσκηση 13.5, η S_4 έχει υποομάδες ισόμορφες με τη D_4, οπότε, αν $|G| = 8$, τότε, από την Πρόταση 13.2, $G \cong D_4$ (δεν μπορούμε να ξέρομε με ποια από τις D_4-υποομάδες της S_4 είναι ίση η G). Αν $|G| = 4$, τότε, από

[1] Η G περιέχει τέτοιες υποομάδες βάσει του *Πρώτου Θεωρήματος Sylow*.
[2] Βάσει του *Δεύτερου Θεωρήματος Sylow*.
[3] Υπενθυμίζεται ότι η G θεωρείται υποομάδα της S_4, καθώς η S_4 έχει ταυτιστεί με την ομάδα μεταθέσεων των τεσσάρων ριζών $t_1, \ldots, t_4$ του f.

την άσκηση 13.6, είναι $G \cong \mathbb{Z}_4$ ή $G = V$. Το δεύτερο ενδεχόμενο αποκλείεται για τον εξής λόγο: Αν $G = V$, τότε $|G \cap V| = 4$ και,συνεπώς, από την 4^{η} σχέση (12.6), $|G| = 8$, αντίφαση. Συνεπώς, μέχρι στιγμής καταλήξαμε στο εξής συμπέρασμα: Αν $m = 2$ τότε $G \cong D_4$ ή $G \cong \mathbb{Z}_4$. Θα έχομε ολοκληρώσει την απόδειξη των (4) και (5) αν αποδείξομε ότι $G \cong D_4 \Leftrightarrow f$ είναι ανάγωγο πάνω από το K.

Απόδειξη του τελευταίου ισχυρισμού. Έστω ότι το f είναι ανάγωγο πάνω από το K. Τότε $[E : K] = 4$, άρα, από το διάγραμμα αμέσως μετά την απόδειξη του Λήμματος 12.9 είναι $[E : F] = 8$, οπότε $|G| = 8$, άρα $G \cong D_4$. Αντιστρόφως, έστω $G \cong D_4$. Τότε, η 4^{η} σχέση (12.6) συνεπάγεται ότι $|G \cap V| = 4$, άρα $G \cap V = V$, δηλαδή, $\mathcal{G}(E/K) = V$. Το E είναι, προφανώς, σώμα διάσπασης του f πάνω από το K και για κάθε $i \in \{1, 2, 3, 4\}$ υπάρχει $\sigma \in V$ με $\sigma(t_1) = t_i$, άρα, από την άσκηση 12.10, το f είναι ανάγωγο πάνω από το K. □

Παράδειγμα 13.4. Με τη βοήθεια του Θεωρήματος 13.3 θα υπολογίσομε τον ισομορφικό τύπο της ομάδας Galois G του $f(X) = X^4 + 5X + 5 \in \mathbb{Q}[X]$.

Βασισμένος στην άσκηση 11.12 (4) υπολογίζω $g(X) = X^3 - 20X + 25 = (X+5)(X^2 - 5X + 5)$. Άρα $m = 2$ και K είναι το σώμα διάσπασης του g πάνω από το $\mathbb{Q}$, δηλαδή, το σώμα διάσπασης του $X^2 - 5X + 5$. Συνεπώς, $K = \mathbb{Q}(\sqrt{5})$. Τώρα πρέπει να αποφασίσω αν $G \cong D_4$ ή $G \cong \mathbb{Z}_4$. Σύμφωνα με το θεώρημα, αυτό εξαρτάται από το αν το f είναι ή όχι ανάγωγο πάνω από το $\mathbb{Q}(\sqrt{5})$. Είναι $[F(t_i) : F] = 4$ για κάθε $i = 1, \dots, 4$, άρα το f δεν έχει ρίζα μέσα στο $K = \mathbb{Q}(\sqrt{5})$. Συνεπώς, το f δεν είναι ανάγωγο πάνω από το K αν και μόνο αν $f(X) = (X^2 + aX + b)(X^2 + cX + d)$ με τα $a, b, c, d \in K$. Αναπτύσσοντας το δεξιό μέλος και εξισώνοντας συντελεστές των ίσων δυνάμεων του X στα δύο μέλη, οδηγούμαι στις σχέσεις

$$c + a = 0, \quad ac + b + d = 0, \quad ad + bc = 5, \quad bd = 5.$$

Οι δύο πρώτες δίνουν $c = -a$ και $d = -b - ac = a^2 - b$. Αντικαθιστώντας στην τρίτη παίρνω $b = (a^3 - 5)/(2a)$ και τώρα η τελευταία γίνεται

$$5 = bd = \frac{a^3 - 5}{2a}(a^2 - b) = \frac{a^3 - 5}{2a}\left(a^2 - \frac{a^3 - 5}{2a}\right) = \frac{a^6 - 25}{4a^2}.$$

Έτσι, $a^6 - 20a^2 - 25 = 0$. Και παρατηρώ ότι η τιμή $a = \sqrt{5}$ επαληθεύει την τελευταία σχέση. Γι' αυτή την τιμή του a είναι και $c, b, d \in \mathbb{Q}(\sqrt{5} = K$, άρα το f δεν είναι ανάγωγο πάνω από το K. Συνεπώς, σύμφωνα με το Θεώρημα 13.3 (5), είναι $G \cong \mathbb{Z}_4$.

Παρατήρηση. Αν και το πολυώνυμο $X^3 + 3X + 3 \in \mathbb{Q}[X]$ είναι «εντελώς όμοιο» με το f αυτού του παραδείγματος, έχει ομάδα Galois διαφορετικού ισομορφικού τύπου. Δείτε την άσκηση 13.7 (4).

Ασκήσεις

Άσκηση 13.5. Έστω $i, j \in \{1, 2, 3, 4\}$ με $i \neq 1$ και $j \neq 1, i$. Αποδείξτε ότι η υποομάδα $\langle (1\,i),\ (1\,i)(1\,j) \rangle$ της S_4 είναι ισόμορφη με τη διεδρική ομάδα D_4.

Άσκηση 13.6. (1) Έστω σώμα F, ανάγωγο διαχωρίσιμο $f \in F[X]$ βαθμού n και E σώμα διάσπασης του f πάνω από το F. Έστω $T = \{t_1, \dots, t_n\} \subset E$ το σύνολο των ριζών του f και $G = \mathcal{G}(E/F)$. Δείξτε ότι η G δρά μεταβατικά επί του T, δηλαδή, για κάθε ζεύγος (i, j) με $1 \leq i, j \leq n$ υπάρχει $\sigma \in G$ με την ιδιότητα $\sigma(t_i) = t_j$.

(2) Έστω $n = 4$ στο προηγούμενο ερώτημα. Θεωρήστε δεδομένο ότι όλες οι υποομάδες τάξεως 4 της S_4 είναι οι εξής:

$$\langle (1\,2\,3\,4) \rangle,\ \langle (1\,2\,4\,3) \rangle,\ \langle (1\,3\,2\,4) \rangle,\ \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle,\ \langle (1\,3), (2\,4) \rangle,\ \langle (1\,4), (2\,3) \rangle,\ \langle (1\,2), (3\,4) \rangle,$$

και αποδείξτε, με τη βοήθεια και του (1), ότι , αν $|G| = 4$, τότε $G \cong \mathbb{Z}_4$ ή $G = V = \langle (t_1\,t_2)(t_3\,t_4), (t_1\,t_3)(t_2\,t_4) \rangle$.

Άσκηση 13.7. Με τη βοήθεια του Θεωρήματος 13.3 υπολογίστε τον ισομορφικό τύπο των ομάδων Galois καθενός από τα παρακάτω πολυώνυμα του $\mathbb{Q}[X]$:

1. $X^4 + 8X + 12$
2. $X^4 + 4X^2 - 2$
3. $X^4 - X - 1$
4. $X^4 + 3X + 3$
5. $X^4 + 8X + 14$

Θέματα εκτός εξεταστέας ύλης, που συζητήθηκαν

1. Παραδείγματα γραφικής κατασκευής (με κανόνα και διαβήτη) κατασκευάσιμου αριθμού, όπως, για παράδειγμα, ο αριθμός
$$\frac{1}{3}\sqrt{2+\sqrt{15}}.$$

2. Αποδείχθηκε το Θεώρημα 4.2, το οποίο λέει ότι κάθε σώμα διαθέτει αλγεβρική κλειστότητα. Ακολούθησα τον T.W. Hungerford ("Algebra", Graduate Texts in Mathematics 73, Springer – Theorem 3.6), σχολιάζοντας διάφορες «λεπτομέρειες».

3. Σχόλιο στους υπερβατικούς αριθμούς. Ένα εύκολο συνολοθεωρητικό επιχείρημα δείχνει ότι το σύνολο των αλγεβρικών αριθμών είναι αριθμήσιμο. Αλλά το $\mathbb{R}$ είναι υπεραριθμήσιμο, άρα το σύνολο των πραγματικών αριθμών που δεν είναι αλγεβρικοί –δηλαδή, το σύνολο των πραγματικών υπερβατικών αριθμών– είναι υπεραριθμήσιμο. Ειδικότερα, αυτό συνεπάγεται ότι υπάρχουν άπειροι πραγματικοί υπερβατικοί αριθμοί. Ο πρώτος τέτοιος αριθμός κατασκευάσθηκε από τον Liouville. Η δεκαδική του ανάπτυξη είναι
$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0,110001000000000000000001\ldots,$$
δηλαδή το ψηφίο 1 υπάρχει στις θέσεις 1, 2, $3! = 6$, $4! = 24$, $5! = 120$ κλπ. και σε όλες τις άλλες θέσεις είναι το ψηφίο 0.

   Συνιστώ να δείτε τις ενότητες 11.6 και 11.7 (3 σελίδες συνολικά) του κλασσικού (και υπέροχου!) βιβλίου των G.H. Hardy & E.M. Wright "An introduction to the Theory of Numbers", Oxford at the Clarendon Press.