Κεφάλαιο 8

8.1 8^{η} Εβδομάδα

Κυκλοτομικά σώματα (συνέχεια)

Σύμφωνα με την Πρόταση 7.21, το Ψ_n είναι μονικό πολυώνυμο του $\mathbb{Z}[X]$. Θα αποδείξομε ότι, επιπλέον, είναι και ανάγωγο πάνω από το $\mathbb{Q}$. Θα χρειασθούμε τα εξής (δίχως απόδειξη).

Λήμμα 8.1 (Παραλλαγή του «Λήμματος του Gauss»). *Αν $f, g \in \mathbb{Q}[X]$ μονικά και $fg \in \mathbb{Z}[X]$, τότε $f, g \in \mathbb{Z}[X]$.*

Λήμμα 8.2 (Αναγωγή $\bmod p$). *Έστω p πρώτος. Για κάθε $a \in \mathbb{Z}$ συμβολίζω με $\overline{a}$ την κλάση $a \bmod p$. Η απεικόνιση*

$$\mathbb{Z}[X] \ni a_n X^n + \cdots + a_1 X + a_0 \mapsto \overline{a_n} X^n + \cdots + \overline{a_1} X + \overline{a_0} \in \mathbb{F}_p[X]$$

είναι ομορφισμός δακτυλίων $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ και λέγεται «αναγωγή $\bmod p$».
Επίσης, ισχύει $\overline{f(X^p)} = \overline{f(X)^p} = \overline{f(X)}^p$.

Θεώρημα 8.3. *Για κάθε $n \in \mathbb{N}$, το Ψ_n είναι ανάγωγο πάνω από το $\mathbb{Q}$.*

Απόδειξη. Έστω ω πρωταρχική n-οστή ρίζα της μονάδος, $\Phi_n(X) = X^n - 1$ και $f = \operatorname{Irr}(\omega, \mathbb{Q})$. Στόχος να δείξω ότι $f = \Psi_n$. Το ω είναι κοινή ρίζα των Φ_n και f και το f είναι ανάγωγο, άρα $f \mid \Phi_n$. Συνεπώς, $\Phi_n = fg$ για κάποιο $g \in \mathbb{Q}[X]$. Τα Φ_n και f είναι μονικά, άρα και το g είναι μονικό. Από το Λήμμα 8.1 έπεται ότι $g \in \mathbb{Z}[X]$. Θα δείξω τα εξής:

(1) Για κάθε πρώτο p που δεν διαιρεί το n ισχύει $f(\omega^p) = 0$. (Η απόδειξη στο τέλος.)
(2) Για κάθε k πρώτο προς τον n ισχύει $f(\omega^k) = 0$.

Η απόδειξη βασίζεται στο (1): Έστω $k = p_1 \cdots p_r$ η ανάλυση του k σε πρώτους (δεν είναι, κατ' ανάγκη διαφορετικοί). Είναι $(p_i, n) = 1$ για κάθε $i = 1, \ldots, r$. Από το (1) έπεται ότι $f(\omega^{p_1}) = 0$. Το $\omega_1 := \omega^{p_1}$ είναι πρωταρχική n-οστή ρίζα της μονάδας, άρα, από το (1), $f(\omega_1^{p_2}) = 0$, δηλαδή, $f(\omega^{p_1 p_2}) = 0$. Το $\omega_2 := \omega^{p_1 p_2}$ είναι πρωταρχική n-οστή ρίζα της μονάδας, άρα, $f(\omega_2^{p_3}) = 0$, δηλαδή, $f(\omega^{p_1 p_2 p_3}) = 0$ κλπ, μέχρι να καταλήξω στη σχέση $f(\omega^k) = 0$.

Βασισμένος στο (2) θα αποδείξω ότι $\Psi_n = f$. Τα Ψ_n και f έχουν κοινή ρίζα την ω και το f είναι ανάγωγο, άρα $f \mid \Psi_n$. Αντίστρόφως, κάθε ρίζα του Ψ_n είναι της μορφής ω^k με $1 \le k < n$ και $(k, n) = 1$ και είναι απλή. Λόγω του (2), $f(\omega^k) = 0$, άρα, $\Psi_n \mid f$. Τα Ψ_n και f είναι μονικά, άρα, $\Psi_n = f$.

Απόδειξη του (1). Είναι $\Phi_n = fg$, άρα $0 = \Phi_n(\omega^p) = f(\omega^p) g(\omega^p)$. Έστω $f(\omega^p) \neq 0$ (πάω σε άτοπο). Τότε $g(\omega^p) = 0$. Δηλαδή, το πολυώνυμο $g(X^p) \in \mathbb{Z}[X]$ έχει ρίζα το ω, άρα $f(X) \mid g(X^p)$. Έστω $g(X^p) = f(x)h(X)$. Από το Λήμμα 8.1, $h \in \mathbb{Z}[X]$ μονικό. Στην τελευταία ισότητα πολυωνύμων εφαρμόζω την αναγωγή $\bmod p$ (Λήμμα 8.2), οπότε $\overline{g(X)}^p = \overline{f(X)} \cdot \overline{h(X)}$, δηλαδή $\overline{g}^p = \overline{f} \cdot \overline{h}$. Έστω $\overline{q} \in \mathbb{F}_p$ ανάγωγος παράγων του $\overline{f}$ (το ότι το f είναι ανάγωγο πάνω από το $\mathbb{Q}$ δεν συνεπάγεται ότι και το $\overline{f}$

είναι ανάγωγο στο $\mathbb{F}_p$). Το $\overline{q}$ διαιρεί το $\overline{g}^p$ άρα $\overline{q} \mid \overline{g}$. Αυτό συνεπάγεται ότι τα $\overline{g}$ και $\overline{f}$ έχουν κοινή ρίζα (σε κάποια επέκταση του $\mathbb{F}_p$). Αλλά $\overline{\Phi}_n = \overline{f} \cdot \overline{g}$, άρα, λόγω του τελευταίου συμπεράσματος, το $\overline{\Phi}_n \in \mathbb{F}_p[X]$ έχει ρίζα πολλαπλότητας > 1, κάτι που αποκλείεται από το Πόρισμα 4.16 (2). □

Πόρισμα 8.4. *Αν E_n είναι το n-οστό κυκλοτομικό σώμα πάνω από το $\mathbb{Q}$, τότε $\mathcal{G}(E_n/\mathbb{Q}) \cong \mathbb{Z}_n^*$.*

Απόδειξη. Έστω ω πρωταρχική n-οστή ρίζα του 1 πάνω από το $\mathbb{Q}$, οπότε $E_n = \mathbb{Q}(\omega)$. Το ω είναι ρίζα του $\Psi_n \in \mathbb{Q}[X]$, το οποίο είναι ανάγωγο σύμφωνα με το Θεώρημα 8.3. Άρα $\operatorname{Irr}(\omega, \mathbb{Q}) = \Psi_n$ και, συνεπώς, $|\mathcal{G}(E_n/\mathbb{Q})| = [E_n : \mathbb{Q}] = \deg \Psi_n = \phi(n) = |\mathbb{Z}_n^*|$. Από την Πρόταση 7.16, η $\mathcal{G}(E_n/\mathbb{Q})$ είναι ισόμορφη με υποομάδα της $\mathbb{Z}_n^*$ και, στην περίπτωσή μας, οι δύο ομάδες έχουν την ίδια τάξη ($= \phi(n)$), άρα οι ομάδες είναι ισόμορφες. □

Διακρίνουσα Πολυωνύμου

Ορισμός 8.5. Θεωρώ $f \in F[X]$ με $\deg(f) = n$ και $\alpha_1, \ldots, \alpha_n$ ρίζες του f σε κάποια αλγεβρική κλειστότητα του F. Ορίζω

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$$

και $\mathrm{D}(f) = \Delta(f)^2$. Το $\mathrm{D}(f)$ ορίζεται ως η διακρίνουσα του f.

Παρατήρηση 8.6 (Προφανής)**.** $\mathrm{D}(f) = 0 \iff f$ έχει τουλάχιστον μία ρίζα πολλαπλότητας > 1.

Ορισμός 8.7. Υποθέτω στο εξής ότι οι ρίζες του f είναι διαφορετικές και το $E = F(\alpha_1, \ldots, \alpha_n)$ είναι σώμα διάσπασης του f (πάνω από το F), οπότε η E/F είναι Galois. Όταν λέμε «ομάδα Galois του f» εννοούμε την $\mathcal{G}(E/F)$.

Υπενθύμιση: Η ομάδα S_n δρα «φυσιολογικά» σε κάθε σύνολο με πληθάριθμο n. Αν

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} \tag{8.1}$$

και $X = \{x_1, x_2, \ldots, x_n\}$, τότε η δράση της σ στο X έχει ως αποτέλεσμα το $X^\sigma := \{x_{i_1}, x_{i_2}, \ldots, x_{i_n}\}$, οπότε η δράση της σ σε κάθε παράσταση $h(x_1, x_2, \ldots, x_n) \in F(x_1, x_2, \ldots, x_n)$ έχει ως αποτέλεσμα την $h^\sigma := f(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$. Λέμε ότι μία υποομάδα H της S_n είναι *μεταβατική* αν για κάθε ζεύγος (i, j) με $i, j \in \{1, 2, \ldots, n\}$ υπάρχει $\sigma \in H$, τέτοιο ώστε $\sigma(i) = j$.

Παρατήρηση 8.8 (Πολύ σημαντική!)**.** Έστω τώρα $\sigma \in \mathcal{G}(E/F)$. Τότε ο σ στέλνει κάθε ρίζα του f σε ρίζα του f και διαφορετικές ρίζες τις στέλνει σε διαφορετικές ρίζες. Έστω, λοιπόν,

$$\sigma(\alpha_1) = \alpha_{i_1},\ \sigma(\alpha_2) = \alpha_{i_2}, \ldots, \sigma(\alpha_n) = \alpha_{i_n}.$$

Έτσι είναι «νόμιμο» να ταυτίζομε τον σ με τη μετάθεση (χρησιμοποιούμε το ίδιο γράμμα) (8.1) διότι, γνωρίζοντας τη μετάθεση (8.1) ξέρομε τη δράση του F-αυτομορφισμού σ σε καθένα από τα α_i και, συνεπώς, σε κάθε στοιχείο του $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Έτσι, μέσω αυτής της ταύτισης η $\mathcal{G}(E/F)$ θεωρείται ως υποομάδα της S_n.

Ορισμός 8.9. Αν $\sigma \in S_n$ και έχω μία παράσταση της μορφής $\Delta = \prod_{1 \le i < j \le n} (x_i - x_j)$, τότε, σύμφωνα με τα παράπάνω, η δράση της σ στη Δ είναι

$$\Delta^\sigma = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Αποδεικνύεται (στη Στοιχειώδη Άλγεβρα) ότι, αν η σ είναι αντιμετάθεση, δηλαδή της μορφής (i,j), τότε $\Delta^\sigma = -\Delta$, άρα γενικά

$$\Delta^\sigma = \begin{cases} \Delta & \text{αν η } \sigma \text{ είναι άρτια} \\ -\Delta & \text{αν η } \sigma \text{ είναι περιττή.} \end{cases} \tag{8.2}$$

Παρατήρηση 8.10 (επί του συμβολισμού)**.** Έστω $\delta = h(\alpha_1, \alpha_2, \dots, \alpha_n) \in E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ και $\sigma \in \mathcal{G}(E/F)$. Αν βλέπω το δ ως στοιχείο του E, δίχως αναφορά στα α_i, τότε, για τη δράση του σ στο δ προτιμώ τον συμβολισμό $\sigma(\delta)$. Αν, όμως, βλέπω το δ ως συγκεκριμένη έκφραση των α_i, τότε, είναι προτιμότερο να θεωρώ τον σ ως μετάθεση (στοιχείο της S_n) και για τη δράση του σ στο δ προτιμώ τον συμβολισμό δ^σ. Με τον πρώτο συμβολισμό,

$$\sigma(\delta) = \sigma(h(\alpha_1, \alpha_2, \dots, \alpha_n) = h(\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)), \tag{8.3}$$

ενώ, με τον δεύτερο συμβολισμό,

$$\delta^\sigma = h(\alpha_1, \alpha_2, \dots, \alpha_n)^\sigma = h(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \dots, \alpha_{\sigma(n)}). \tag{8.4}$$

Οι δύο παραπάνω εκφράσεις είναι ίσες. Διότι, αν $\sigma(\alpha_1) = \alpha_{i_1}, \sigma(\alpha_2) = \alpha_{i_2}, \dots, \sigma(\alpha_n) = \alpha_{i_n}$, τότε, από την (8.3), $\sigma(\delta) = h(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_n})$. Αφετέρου, ο σ ταυτίζεται με τη μετάθεση (8.1), σύμφωνα με όσα είπαμε πριν. Άρα, από την (8.4), $\delta^\sigma = h(\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_n})$.

Στα παρακάτω, G θα συμβολίζει την ομάδα Galois του f, δηλαδή, $G = \mathcal{G}(E/F)$.

Πρόταση 8.11.

1. $\sigma(\Delta(f)) = \prod_{1 \le i \le j \le n}(\sigma(\alpha_i) - \sigma(\alpha_j)) = \begin{cases} \Delta(f), & \textit{αν η } \sigma \textit{ ταυτίζεται με άρτια μετάθεση} \\ -\Delta(f), & \textit{αν η } \sigma \textit{ ταυτίζεται με περιττή μετάθεση} \end{cases}$
2. $\mathrm{D}(f) \in F$.

Απόδειξη. (1) Άμεση συνέπεια της (8.2).
(2) $\sigma(\mathrm{D}(f)) = \sigma(\Delta(f)^2) = \sigma(\Delta(f))^2 = (\pm\Delta(f))^2 = \Delta(f)^2 = \mathrm{D}(f)$ για κάθε $\sigma \in G$, άρα $\mathrm{D}(f) \in \mathcal{F}(G) = F$. □

Πρόταση 8.12 (Θεωρώντας τη G υποομάδα της S_n)**.** $G \le A_n$ *αν και μόνο αν η διακρίνουσα* $\mathrm{D}(f)$ *είναι τετράγωνο κάποιου στοιχείου του* F *(συμβολικά* $\mathrm{D}(f) \in F^2$*).*[1]

Απόδειξη. Αν $G \le A_n$, τότε, από την Πρόταση 8.11, $\sigma(\Delta(f)) = \Delta(f), \forall \sigma \in G$. Άρα $\Delta(f) \in \mathcal{F}(G) = F$ και $\mathrm{D}(f) = \Delta(f)^2 \in F^2$.

Αντιστρόφως, έστω ότι $\mathrm{D}(f) = c^2$ για καποιο $c \in F$. Τότε $c^2 = \Delta(f)^2$ άρα $\Delta(f) = \pm c \in F$. Συνεπώς, για κάθε $\sigma \in G$, έχω $\sigma(\Delta(f)) = \Delta(f)$, άρα ο σ ταυτίζεται με άρτια μετάθεση. □

Παρατήρηση 8.13. Έστω ότι το f είναι ανάγωγο (υπενθυμίζεται ότι έχει ήδη υποτεθεί ότι οι ρίζες του f είναι διαφορετικές· βλ. Ορισμό 8.7). Αν $1 \le i, j \le n$, ξέρομε ότι υπάρχει F-ισομορφισμός από το $F(\alpha_i)$ στο $F\alpha_j$, που στελνει το α_i στο α_j και μπορεί να επεκταθεί σε $\sigma \in G$. Δηλαδή, διατυπωμένο με όρους μεταθέσεων $\forall i, j \in \{1, \dots, n\} \exists \sigma \in G : \sigma(\rho_i) = \rho_j$. Βλέποντας τη G σαν υποομάδα της S_n, το συμπέρασμα αυτό διατυπώνεται ως εξης: *Η* G *είναι μεταβατική υποομάδα της* S_n. (Βλ. τρεις γραμμές κάτω από τη (8.1).)

[1] A_n είναι η υποομάδα αρτίων μεταθέσεων της S_n και τάξη της είναι $\frac{1}{2}n!$.

Παράδειγμα 8.14. Εφαρμογή στο κυβικό πολυώνυμο. Έστω σώμα F χαρακτηριστικής $\neq 3$ και ανάγωγο διαχωρίσιμο $g = X^3 + aX^2 + bX + c \in F[X]$. Το $f(X) := g(X - a/3)$ είναι της μορφής $f(X) = X^3 + pX + q \in F[X]$. Αν ρ_1, ρ_2, ρ_3 είναι οι ρίζες του g, τότε οι ρίζες του f είναι $\alpha_i := \rho_i + a/3$, άρα $\Delta(f) = \Delta(g)$. Επίσης, τα f, g έχουν την ίδια ομάδα Galois G γιατί $F(\rho_1, \rho_2, \rho_3) = F(\alpha_1, \alpha_2, \alpha_3)$. Συνεπώς, εστιάζομε τη μελέτη μας στο απλούστερης μορφής πολυώνυμο f. Υπολογίζεται ότι $\mathrm{D}(g) = -4p^3 - 27q^2$.

Η G είναι υποομάδα της $S_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$ τάξεως 6. Οι υποομάδες της είναι οι

$$\langle id\rangle, \langle(1,2)\rangle,\ \langle(1,3)\rangle,\ \langle(2,3)\rangle,\ A_3 = \langle(1,2,3)\rangle = \{id, (1,2,3), (1,3,2)\}.$$

Την απαίτηση της μεταβατικότητας ικανοποιούν μόνο η S_3 και η A_3. Άρα, βάσει της Παρατήρησης 8.13, $G \cong A_3$ ή $G \cong S_3$.

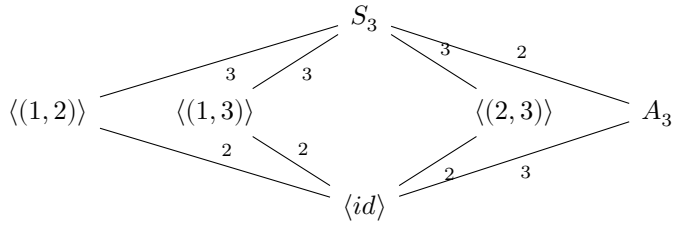
Έστω $G \cong A_3$. Η A_3 δεν έχει γνήσιες υποομάδες πλήν της $\langle id\rangle$, άρα δεν υπάρχει ενδιάμεση επέκταση μεταξύ των F και $E = F(\alpha_1, \alpha_2, \alpha_3)$. Αυτή η περίπτωση ισχύει αν και μόνο αν το $\mathrm{D}(f) \in F^2$ (Πρόταση 8.11). Επίσης, $[E : F] = |G| = 3$ άρα $E = F(\rho_1) = F(\rho_2) = F(\rho_3)$ αφού και $[F(\rho_i) : F] = \deg g = 3$. Άρα οι ρ_2, ρ_3 είναι πολυωνυμικές εκφράσεις του ρ_1 κλπ. Αριθμητικό παράδειγμα αυτής της περίπτωσης είδαμε στην άσκηση 3.16.

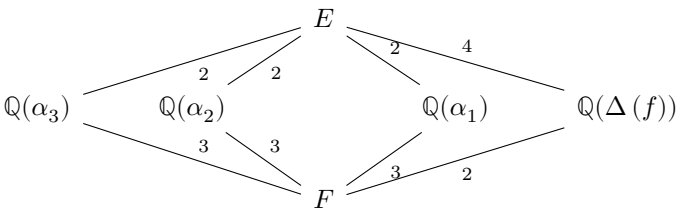
Έστω $G \cong S_3$. Τότε $[E : F] = |G| = 6$. Η G έχει ακριβώς τέσσερις γνήσιες υποομάδες πλήν της $\langle id\rangle$, άρα υπάρχουν ακριβώς τέσσερις γνήσιες ενδιάμεσες επεκτάσεις μεταξύ των F και E. Αυτές είναι τα σταθεροποιούμενα σώματα των $\langle(1,2)\rangle, \langle(1,3)\rangle, \langle(1,2)\rangle$ και A_3. Οι τρεις πρώτες είναι υποομάδες τάξης 2, άρα ο βαθμός της επέκτασης που αντιστοιχεί σε αυτές είναι βαθμού $6/2 = 3$.

Πιο συγκεκριμμένα, το $\mathcal{F}((1,2))$ είναι το $\mathbb{Q}(\alpha_3)$ η $\mathbb{Q}(\alpha_3)/\mathbb{Q}$ διότι αυτή ειναι βαθμού 3 και ο σ που αντιμεταθέτει τις α_1, α_2 αφήνει σταθερό το α_3. Αντίστοιχα, $\mathcal{F}((1,3)) = \mathbb{Q}(\alpha_2)$ και $\mathcal{F}((2,3)) = \mathbb{Q}(\alpha_1)$.

Μένει ο υπολογισμός του $K = \mathcal{F}(A_3)$. Για κάθε $\sigma \in A_3$ είναι $\sigma(\Delta(f)) = \Delta(f)$ (Πρόταση 8.11), άρα $\mathbb{Q}(\Delta(f)) \leq K$. Επίσης, $S_3 = G \not\leq A_3$, άρα, από την Πρόταση 8.12, $\Delta(f) \notin F$ και το $X^2 - \mathrm{D}(f)$ είναι ανάγωγο. Έπεται ότι η επέκταση $\mathbb{Q}(\Delta(f))/\mathbb{Q}$ είναι βαθμού 2, άρα $K = \mathbb{Q}(\Delta(f))$.

Έτσι, στην περίπτωση που $G \cong S_3$, καταλήγομε στα παρακάτω διαγράμματα υποομάδων και επεκτάσεων:





Στην περαιτέρω μελέτη των ομάδων Galois πολυωνύμων είναι χρήσιμο το εξής:

Λήμμα 8.15. *(i)* $S_n = \langle(1\,2), (1\,3), \ldots, (1\,n)\rangle$

(ii) $S_n = \langle(1\,2), (2\,3), \ldots, ((n-1)\,n)\rangle$

(iii) $S_n = \langle(1\,2), (1\,2\,3 \ldots (n-1)\,n)\rangle$

(iv) $S_n = \langle (1\,2), (2\,3\,\ldots\,(n-1)\,n) \rangle$

Λήμμα 8.16. *Έστω $f \in F[X]$ ανάγωγο, διαχωρίσιμο, βαθμού n και ομάδα Galois G . Τότε $n \mid |G|$. Επιπλέον, αν $n = p$ πρώτος, τότε η G (ως υποομάδα της S_n) περιέχει ένα p-κύκλο δηλαδή κάποιο $(i_1, \ldots, i_p)$ με $i_1, \ldots, i_p$ μετάθεση των $1, \ldots, p$.*

Απόδειξη. Έστω $E = F(\alpha_1, \ldots, \alpha_n)$ όπου $\alpha_1, \ldots, \alpha_n$ ρίζες του f (διαφορετικές αφού το f είναι διαχωρίσιμο). Έχομε το παρακάτω διάγραμμα αντιστοιχίας Galois:

$$\begin{array}{ccc} E & \longleftrightarrow & \langle id \rangle \\ | & & | \\ F(\alpha_1) & \longleftrightarrow & H \\ |n & & | \\ F & \longleftrightarrow & G \end{array}$$

Η E/F είναι Galois ως σώμα διάσπασης του διαχωρίσιμου πολυωνύμου f πάνω από το f. Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois 6.9, $n = [G : H]$. Είναι $|G| = |H|\,[G : H]$, άρα $n \mid |G|$.

Εξειδικεύω στην περίπτωση που $n = p$ πρωτος. Τότε έστω $|G| = p^r m$, όπου $r \geq 1$ και $p \nmid m$. Από το 1ο θεώρημα Sylow, υπάρχει υποομάδα P_i της G (p-ομάδα Sylow) τάξεως p^i για κάθε $i = 1, \ldots, r$. Ειδικότερα $|P_1| = p$ άρα η P_1 είναι κυκλική τάξεως p, δηλαδη υπάρχει $sigma \in G$ τάξεως p οπότε οι $id, \sigma, \ldots, \sigma^{p-1}$ είναι διαφορετικοί και $\sigma^p = id$. (Εναλλακτικά, το θεώρημα Cauchy για ομάδες λέει ότι αν η G είναι πεπερασμένη ομάδα και ο πρώτος p διαιρεί την τάξη $|G|$, τότε υπάρχει στοιχείο της G τάξεως p.)

Ο σ γράφεται σε γινόμενο ξένων κύκλων, έστω $\sigma = \kappa_1 \ldots \kappa_2 \ldots \kappa_m$ της S_p. Είναι $p = \mathrm{ord}\,(\sigma) = \mathrm{lcm}(\mathrm{ord}\,(\kappa_1), \ldots \mathrm{ord}\,(\kappa_m))$. Άρα κάποιος κύκλος, έστω ο κ_1 έχει τάξη p. Αυτό, επίσης, σημαίνει ότι $\sigma = \kappa_1$, καθώς οι $\kappa_1, \ldots, \kappa_m$ έχουν υποτεθεί ξένοι και αφού ο κ_1 έχει p στοιχεία, δεν υπάρχει ξένος προς αυτόν κύκλος. □

Πρόταση 8.17. *Έστω πρώτος $p \geq 3$, $f \in \mathbb{Q}(X)$ ανάγωγο, βαθμού p,*[2] *το οποίο έχει ένα ακριβώς ζεύγος συζυγών μιγαδικών ριζών και τις υπόλοιπες $p-2$ πραγματικές. Τότε η ομάδα Galois του f είναι ισόμορφη με την S_p.*

Απόδειξη. Έστω ότι οι γνήσιες μιγαδικές ρίζες είναι $\alpha_1, \alpha_2 = \bar{\alpha_1}$ και οι πραγματικές οι $\alpha_3, \ldots, \alpha_p$. Έχω τον $\mathbb{Q}$-αυτομορφισμό του $\mathbb{C}$ με $z \mapsto \bar{z}$. Περιορίζοντας αυτόν στο σώμα διάσπασης του f, έστω Ε παίρνω κάποιον $\tau \in G := \mathcal{G}\,(E/\mathbb{Q})$. Αν δω τον τ ως μετάθεση του S_p τότε αυτός είναι ο $(1, 2)$. Από το Λήμμα 8.16 υπάρχει $\sigma \in G$ που είναι p-κύκλος. Αν αριθμήσω κατάλληλα τις πραγματικές ρίζες, τότε η G περιέχει τη μετάθεση $(1, 2, \ldots, p-1, p)$.[3] Καταλήγω στο συμπέρασμα ότι η G περιέχει τις μεταθέσεις $(1, 2)$ και $(1, 2, \ldots, p-1, p)$, άρα, από το Λήμμα 8.15, $G \cong S_p$. □

[2] Αφού είμαστε πάνω από το $\mathbb{Q}$, το f είναι διαχωρίσιμο.

[3] Αυτό είναι εμφανές από το παρακάτω παράδειγμα. Έστω $p = 5$ και $\sigma = (1, 3, 4, 2, 5)$, τότε $\sigma^3 = (1, 2, 3, 5, 4)$. Οι $3, 4, 5$ αντιστοιχούν στις πραγματικές ρίζες οπότε αν αλλάξω την αρίθμηση των πραγματικών ριζών ($\alpha_4 \leftarrow a_5$ και $\alpha_5 \leftarrow a_4$) τότε ο σ ταυτίζεται με τον $(1, 2, 3, 4, 5)$.

Ασκήσεις

Άσκηση 8.18. Έστω E_n το n-οστό κυκλοτομικό πολυώνυμο πάνω από το $\mathbb{Q}$. Για τις απαντήσεις στα ερωτήματα που ακολουθούν, σημαντικό ρόλο παίζει το Πόρισμα 8.4, καθώς και ο ορισμός του μονομορφισμού ψ, ο οποίος ορίσθηκε αμέσως πριν την εκφώνηση της Πρότασης 7.16.

(α΄) Προσδιορίστε με ποια ομάδα είναι ισόμορφη η $\mathcal{G}(E_5/\mathbb{Q})$ και διαπιστώστε ότι είναι κυκλική. Έστω $\mathcal{G}(E_5/\mathbb{Q}) = \langle\sigma\rangle$ και ω πρωταρχική 5^{η} ρίζα της μονάδας. Ποια είναι η τιμή του $\sigma(\omega)$; Διαπιστώστε ότι υπάρχει μία μόνο γνήσια υποομάδα H της $\mathcal{G}(E_5/\mathbb{Q})$ διαφορετική από την $\langle id\rangle$ και υπολογίστε το σταθεροποιούμενο σώμα της K. Η απάντησή σας θα είναι της μορφής $K = \mathbb{Q}(\sqrt{d})$.

(β΄) Δείξτε ότι η $\mathcal{G}(E_8/\mathbb{Q})$ είναι ισόμορφη με την V_4 (ομάδα Klein). Έστω $\mathcal{G}(E_8/\mathbb{Q}) = \langle\sigma,\tau\rangle$ και ω πρωταρχική 8^{η} ρίζα της μονάδας. Ποια είναι η τιμή των $\sigma(\omega)$ και $\tau(\omega)$; Διαπιστώστε ότι υπάρχουν ακριβώς τρεις γνήσιες υποομάδες της $\mathcal{G}(E_8/\mathbb{Q})$ διαφορετικές από την $\langle id\rangle$ και υπολογίστε τα αντίστοιχα σταθεροποιούμενα σώματά τους. Και τα τρία θα είναι της μορφής $\mathbb{Q}(\sqrt{d})$.

(γ΄) Προσδιορίστε με ποια ομάδα είναι ισόμορφη η $\mathcal{G}(E_7/\mathbb{Q})$ και διαπιστώστε ότι είναι κυκλική. Έστω ω πρωταρχική 7^{η} ρίζα της μονάδας. Προσδιορίστε τον ελάχιστο θετικό ακέραιο k για τον οποίο ο $\sigma \in \mathcal{G}(E_7/\mathbb{Q})$ που ορίζεται από τη σχέση $\sigma(\omega) = \omega^k$, παράγει την ομάδα $\mathcal{G}(E_7/\mathbb{Q})$. Εξηγήστε γιατί υπάρχουν ακριβώς δύο γνήσιες υποομάδες της $\mathcal{G}(E_7/\mathbb{Q})$ διαφορετικές από την $\langle id\rangle$. Αποδείξτε ότι ο γεννήτορας τής μιας από αυτές τις υποομάδες (συμβολίστε την H_1) αφήνει αναλλοίωτο το $\zeta := \omega^4+\omega^2+\omega$ και αποδείξτε ότι το ζ είναι ρίζα του X^2+X+2. Ποιο είναι το σταθεροποιούμενο σώμα της H_1; Αποδείξτε ότι ο γεννήτορας τής άλλης υποομάδας (συμβολίστε την H_2) αφήνει αναλλοίωτο το $\xi := \omega+\omega^{-1}$. Υπολογίστε ένα πολυώνυμο $g \in \mathbb{Q}[X]$ τρίτου βαθμού το οποίο έχει ρίζα το ξ. Γιατί το g είναι ανάγωγο; Υπολογίστε τη διακρίνουσα του g και αποδείξτε ότι η επέκταση $\mathbb{Q}(\xi)/\mathbb{Q}$ είναι κανονική. Δείξτε ότι το σταθεροποιούμενο σώμα της H_2 είναι το $\mathbb{Q}(\xi)$.