

Κεφάλαιο 6

6.1 6^η Εβδομάδα

Galois (συνέχεια)

Πρόταση 6.1 (Αντίστροφη της Πρότασης 5.25 (1)). *Αν η επέκταση E/F είναι πεπερασμένη και $\mathcal{F}(\mathcal{G}(E/F)) = F$, τότε η E/F είναι Galois.*

Απόδειξη. Πρώτα θ' αποδείξω την κανονικότητα της E/F . Θεωρώ ανάγωγο $f \in F[X]$, το οποίο έχει μία ρίζα $\alpha \in E$ και θα δείξω ότι το f διασπάται στο E . Δίχως βλάβη της γενικότητας, υποθέτω ότι το f είναι μονικό, οπότε $f = \text{Irr}(\alpha, F)$.

Έστω $\mathcal{G}(E/F) = \{\sigma_1 = id_E, \sigma_2, \dots, \sigma_n\}$, $\alpha := \alpha_1 = \sigma_1(\alpha)$ και $\sigma_i(\alpha) := \alpha_i$ για $i = 2, \dots, n$. Έστω ότι ακριβώς r από τα $\alpha_1, \dots, \alpha_n$ διαφορετικά ($r \leq n$). Αριθμώ τους $\sigma_2, \dots, \sigma_n$ έτσι ώστε τα r πρώτα από αυτά να είναι όλα-όλα τα διαφορετικά α_i (που σημαίνει ότι, αν $r < n$, τότε καθένα από τα υπόλοιπα, $\alpha_{r+1}, \dots, \alpha_n$ ισούται με κάποιο από τα $\alpha_1, \dots, \alpha_r$). Ορίζω το

$$g(X) = \prod_{j=1}^r (X - \alpha_j) \in E[X]$$

και πρώτα-πρώτα παρατηρώ ότι είναι διαχωρίσιμο εκ κατασκευής (αφού τα $\alpha_1, \dots, \alpha_r$ έχουν υποτεθεί διαφορετικά). Θα δείξω ότι $g(X) \in F[X]$ ως εξής: Θεωρώ τυχαίο $\sigma_i \in \mathcal{G}(E/F)$ ($1 \leq i \leq n$) και το πολώνυμο

$$\sigma_i g(X) = \prod_{j=1}^r (X - \sigma_i(\alpha_j)) = \prod_{j=1}^r (X - \sigma_i \sigma_j(\alpha)).$$

Είναι $\sigma_i \sigma_j \in \mathcal{G}(E/F) = \{\sigma_1, \dots, \sigma_n\}$, συνεπώς $\sigma_i \sigma_j(\alpha) \in \{\alpha_1, \dots, \alpha_r\}$. Επίσης, οι τιμές $\sigma_i \sigma_j(\alpha)$ είναι διαφορετικές μεταξύ τους διότι, αν $\sigma_i \sigma_j(\alpha) = \sigma_i \sigma_k(\alpha)$, επειδή σ_i είναι 1-1 έπεται ότι $\sigma_j(\alpha) = \sigma_k(\alpha)$ δηλαδή $\alpha_j = \alpha_k$, που αντιφάσκει στο ότι οι $1 \leq k, j \leq r$ και $k \neq j$. Συνεπώς, τα $\sigma_i \sigma_j(\alpha)$, $j = 1, \dots, r$ αποτελούν μετάθεση των $\alpha_1, \dots, \alpha_r$, άρα $\sigma_i g = g$, οπότε κάθε συντελεστής του g μένει αναλλοίωτος από κάθε $\sigma_i \in \mathcal{G}(E/F)$. Αυτό σημαίνει ότι κάθε συντελεστής του g ανήκει στο $\mathcal{F}(\mathcal{G}(E/F)) = F$, άρα $g \in F[X]$. Ισχυρίζομαι τώρα ότι $g = \text{Irr}(\alpha, F)$. Πράγματι, το $f = \text{Irr}(\alpha, F)$ και το g έχουν κοινή ρίζα το α , άρα $f \mid g$. Ειδικότερα $\deg f \leq \deg g = r$. Αφετέρου, η σχέση $f(\alpha) = 0$ συνεπάγεται την $0 = \sigma_i(f(\alpha)) = f(\sigma_i(\alpha)) = f(\alpha_i)$ για κάθε $i = 1, \dots, r$, άρα το f έχει τουλάχιστον r διαφορετικές ρίζες, οπότε $\deg f \geq r$. Έτσι, $\deg f = \deg g$ και, συνεπώς, $f = g$. Αλλά το g , διασπάται στο E , άρα το f διασπάται στο E . Αυτό ολοκληρώνει την απόδειξη της κανονικότητας της επέκτασης E/F . Επιπλέον, απέδειξα παράλληλα ότι κάθε ανάγωγο $f \in F[X]$ είναι διαχωρίσιμο, άρα αν θεωρήσω ένα οποιοδήποτε $\beta \in E$, τότε το $\text{Irr}(\beta, F)$ είναι διαχωρίσιμο, που σημαίνει ότι το β είναι διαχωρίσιμο. Συνεπώς, η επέκταση E/F είναι και διαχωρίσιμη. $\square$

Παρατήρηση 6.2. Οι Προτάσεις 6.1 και 5.25 αποδεικνύουν την ισοδυναμία

Η πεπερασμένη επέκταση E/F είναι Galois αν και μόνο αν ισχύει $\mathcal{F}(\mathcal{G}(E/F)) = F$.

Οπότε,

$$E/F \text{ πεπερασμένη και Galois} \stackrel{5.16}{\iff} E/F \text{ κανονική και διαχωρίσιμη} \iff \mathcal{F}(\mathcal{G}(E/F)) = F.$$

Η ισοδυναμία αυτή ισχύει γενικότερα. Έτσι έχουμε,

$$E/F \text{ αλγεβρική και Galois} \stackrel{5.16}{\iff} E/F \text{ κανονική και διαχωρίσιμη} \iff \mathcal{F}(\mathcal{G}(E/F)) = F.$$

Η τελευταία ισχύει, λοιπόν, ακόμη και στην περίπτωση απείρων επεκτάσεων E/F οι οποίες είναι αλγεβρικές και Galois.

Ο ορισμός της επέκτασης Galois γενικεύεται ακόμη περισσότερο, ώστε να συμπεριλάβει και μη αλγεβρικές επεκτάσεις: Μία επέκταση E/F λέγεται Galois αν ικανοποιεί τη συνθήκη $\mathcal{F}(\mathcal{G}(E/F)) = F$. Παρατηρήστε ότι, για οποιαδήποτε επέκταση E/F , οι Ορισμοί 5.17 και 5.23 εξακολουθούν να έχουν νόημα, ανεξαρτήτως του αν η επέκταση E/F είναι αλγεβρική. Όμως, όταν η E/F δεν είναι αλγεβρική, δεν ισχύει η ισοδυναμία $E/F \text{ Galois} \iff E/F \text{ κανονική και διαχωρίσιμη}$.

Θεμελιώδες Θεώρημα Galois

Το θεώρημα θα χωριστεί σε μικρότερες προτάσεις. Υποθέτω ότι E/F είναι πεπερασμένη επέκταση Galois.

Πρόταση 6.3. Οι απεικονίσεις $\mathcal{G}(E/\bullet)$ και $\mathcal{F}(\bullet)$ είναι αντίστροφες η μία της άλλης, άρα τα σύνολα $\mathcal{E}, \mathcal{O}$ βρίσκονται σε αμφιμονοσήμαντη αντιστοιχία.

Απόδειξη. Θα δείξω ότι $\mathcal{F}(\mathcal{G}(E/\bullet)) = id_{\mathcal{E}}$ και $\mathcal{G}(E/\mathcal{F}(\bullet)) = id_{\mathcal{O}}$.

Για την πρώτη ισότητα, έχω να δείξω ότι αν $F \leq K \leq E$ τότε $\mathcal{F}(\mathcal{G}(E/K)) = K$. Πράγματι, αφού E/F είναι Galois, τότε είναι κανονική και διαχωρίσιμη. Άρα και η E/K είναι κανονική (Πόρισμα 5.15) και διαχωρίσιμη (Θεώρημα 5.5), δηλαδή Galois. Εφαρμόζοντας την Πρόταση 5.25 για το σώμα K στη θέση του F , προκύπτει η ισότητα.

Για την δεύτερη, αν $H \geq \mathcal{G}(E/F)$ θέλω να δείξω ότι $\mathcal{G}(E/\mathcal{F}(H)) = H$. Από την Πρόταση 5.24 (β'), $\mathcal{G}(E/\mathcal{F}(H)) \geq H$ και θα δείξω ότι ισχύει η ισότητα. Έστω ότι η H ήταν γνήσια υποομάδα της $\mathcal{G}(E/\mathcal{F}(H))$. Προηγουμένως έδειξα ότι η επέκταση E/K είναι Galois για κάθε ενδιάμεση επέκταση K . Άρα και η $E/\mathcal{F}(H)$ είναι Galois. Εφαρμόζω την Πρόταση 5.25 (2) με το $\mathcal{F}(H)$ στη θέση του F και έχω: Αν $H \leq \mathcal{G}(E/\mathcal{F}(H))$ τότε $\mathcal{F}(H) \geq \mathcal{F}(H)$ άτοπο. Άρα, αναγκαστικά $\mathcal{G}(E/\mathcal{F}(H)) = H$. $\square$

Παρατήρηση 6.4. Την 1-1 αντιστοιχία της Πρότασης 6.3 συμβολίζουμε $\longleftrightarrow$. Η τυπική περίπτωση φαίνεται στο παρακάτω διάγραμμα:

$$\begin{array}{ccc} E & \longleftrightarrow & \mathcal{G}(E/E) = \langle id_E \rangle \\ | & & | \\ K & \longleftrightarrow & H \\ | & & | \\ F & \longleftrightarrow & \mathcal{G}(E/F) =: G \end{array}$$

Την αντιστοιχία $K \leftrightarrow H$ μπορώ να δω με δύο ισοδύναμους τρόπους: Είτε ότι $H = \mathcal{G}(E/K)$ είτε ότι $K = \mathcal{F}(H)$.

Πρόταση 6.5. Αν στην αντιστοιχία Galois είναι $K \leftrightarrow H$ και $\sigma \in \mathcal{G}(E/F)$ τότε $\sigma(K) \leftrightarrow \sigma H \sigma^{-1}$

Απόδειξη. Για να δείξω το ζητούμενο έχω δύο επιλογές. Ή θα δείξω ότι $\sigma H \sigma^{-1} = \mathcal{G}(E/\sigma(K))$ ή ότι $\sigma(K) = \mathcal{F}(\sigma H \sigma^{-1})$. Θα αποδείξω το δεύτερο. Έχω ότι

$$\begin{aligned} u \in \mathcal{F}(\sigma H \sigma^{-1}) &\iff \\ u \text{ μενει αναλοίωτο από κάθε στοιχείο της } \sigma H \sigma^{-1} &\iff \\ \sigma \tau \sigma^{-1}(u) = u, \forall \tau \in H &\iff \\ \tau \sigma^{-1}(u) = \sigma^{-1}(u), \forall \tau \in H &\iff \\ \sigma^{-1}(u) \in \mathcal{F}(H) &\iff \\ \sigma^{-1}(u) \in K &\iff \\ \sigma(\sigma^{-1}(u)) \in \sigma(K) &\iff \\ u \in \sigma(K) \end{aligned}$$

□

Πρόταση 6.6. Αν στην αντιστοιχία Galois είναι $K \leftrightarrow H$, τότε

$$[E : K] = |H| \quad \text{και} \quad [K : F] = [G : H] := \frac{|G|}{|H|}.$$

Απόδειξη. Αφού E/F είναι Galois και η E/K θα είναι επίσης όπως είδαμε και στην απόδειξη της Πρότασης 6.3. Άρα $[E : K] = |\mathcal{G}(E/K)| = |H|$. Επίσης,

$$[K : F] = \frac{[E : F]}{[E : K]} = \frac{|\mathcal{G}(E/F)|}{|H|} = \frac{|G|}{|H|} = [G : H].$$

(Ο τελευταίος φυσικός αριθμός ονομάζεται δείκτης της H στην G και μετρά το πλήθος των αριστερών ή των δεξιών συμπλόκων της H στη G . Τα αριστερά σύμπλοκα και τα δεξιά σύμπλοκα της H στην G είναι εν γένει διαφορετικά. Όμως, το πλήθος τους συμπίπτει και ταυτίζεται με το δείκτη της H στην G) □

Συνέχεια του Θεμελιώδους Θεωρήματος Galois. Έχουμε ήδη δει ότι αν $F \leq K \leq E$ και η επέκταση E/F είναι Galois, τότε και η επέκταση E/K είναι Galois. Μένει λοιπόν το ερώτημα, πότε η K/F είναι Galois. Επειδή είναι πάντα διαχωρίσιμη, το ερώτημα ισοδυναμεί με το πότε η K/F είναι κανονική. Διατηρούμε το συμβολισμό $G = \mathcal{G}(E/F)$ και $H = \mathcal{G}(E/K) \leq G$.

Πρόταση 6.7. Η K/F είναι κανονική (άρα και Galois) αν και μόνο αν $H \trianglelefteq G$ (η H είναι κανονική υποομάδα της G)

Απόδειξη. Έστω C μία αλγεβρική κλειστότητα της E .

“ $\Leftarrow$ ”: Έστω $H \trianglelefteq K$. Για να δείξω ότι η K/F είναι κανονική, αρκεί κάθε F -μονομορφισμός $\sigma : K \hookrightarrow C$ να είναι F -αυτομορφισμός του K σύμφωνα με το Θεώρημα 5.12. Θα πάρω επομένως τυχαίο F -μονομορφισμό $\sigma : K \hookrightarrow C$ και θα δείξω ότι $\sigma(K) = K$. Επειδή η αντιστοιχία Galois είναι αμφιμονοσήμαντη, ισχύει $K = \sigma(K)$ αν και μόνο αν οι αντίστοιχες υποομάδες αυτών είναι ισές. Η υποομάδα που αντιστοιχεί στην K είναι η H και από την Πρόταση 6.5, αυτή που αντιστοιχεί στην $\sigma(K)$ είναι η $\sigma H \sigma^{-1}$. Αφού η H είναι κανονική $H = \sigma H \sigma^{-1}$ άρα $\sigma(K) = K$.

“ $\Rightarrow$ ”: Υποθέτω ότι K/F είναι κανονική και θέλω να δείξω ότι $H \trianglelefteq G$, δηλαδή, ότι για κάθε $\sigma \in G$ ισχύει $\sigma H \sigma^{-1} = H$. Θα δείξω ότι τα αντίστοιχα σταθεροποιούμενα σώματα είναι ίσα. Όμως η $\sigma H \sigma^{-1}$ αντιστοιχεί στο $\sigma(K)$ και η H στο K . Άρα αρκεί να δείξω ότι $K = \sigma(K)$. Ο σ είναι F -αυτομορφισμός του E . Άρα ο $\sigma|_K$ είναι F -μονομορφισμός $K \hookrightarrow E$. Επειδή η K/F είναι κανονική, ο $\sigma|_K$ στην πραγματικότητα είναι F -αυτομορφισμός του K , άρα είναι και επί. Επομένως $\sigma|_K(K) = \sigma(K) = K$.

□

Πρόταση 6.8. Στην περίπτωση που η K/F είναι κανονική ισχύει ότι $\mathcal{G}(K/F) = G/H$, δηλαδή

$$\mathcal{G}(K/F) = \mathcal{G}(E/F) / \mathcal{G}(E/K).$$

Απόδειξη. Θεωρώ την απεικόνιση $\psi : \mathcal{G}(E/F) \rightarrow \mathcal{G}(K/F)$ με $\sigma \mapsto \sigma|_K$. Από την απόδειξη της προηγούμενης πρότασης, η επέκταση K/F είναι κανονική και ο σ_K είναι F -αυτομορφισμός του K άρα η ψ είναι καλά ορισμένη, δηλαδή, $\psi(\sigma) \in \mathcal{G}(K/F)$. Προφανώς, για κάθε $u \in K$ και κάθε $\sigma \in \mathcal{G}(E/F)$, ισχύει $\psi(\sigma)(u) = \sigma(u)$. Από αυτό έπεται ότι, για κάθε $\sigma, \tau \in \mathcal{G}(E/F)$ ισχύει $\psi(\sigma\tau)(u) = (\psi(\sigma)\psi(\tau))(u)$ για κάθε $u \in K$, άρα $\psi(\sigma\tau) = \psi(\sigma)\psi(\tau)$ ο ψ είναι ομομορφισμός ομάδων.

Ο ψ είναι επιμορφισμός. Έστω $\tau \in \mathcal{G}(K/F)$. Θεωρώ την επέκταση του τ , $\tilde{\tau} : C \hookrightarrow C$ και μετά θεωρώ την $\sigma = \tilde{\tau}|_E$. Ο σ είναι F -μονομορφισμός $E \hookrightarrow C$. Αλλά η E/F είναι κανονική άρα $\sigma \in \mathcal{G}(E/F)$. Προφανώς $\sigma_K = \tau$ άρα η ψ είναι επί.

Τέλος, έστω $\mathcal{G}(E/F) = G$. Είναι $\ker \psi = \{\sigma \in G : \psi(\sigma) = id_K\}$ άρα $\sigma \in \ker \psi \iff \sigma_K = id_K \iff \sigma \in G$. Άρα $\ker \psi = \mathcal{G}(E/K) = H$. Από το πρώτο θεώρημα ομομορφισμών ομάδων έπεται ότι

$$\mathcal{G}(E/F) / \mathcal{G}(E/K) = G/H = G/\ker \psi \cong \text{Im } \psi = \mathcal{G}(K/F).$$

□

Συγκεντρώνοντας τα συμπεράσματα των Προτάσεων 5.25 (1), 6.1, 6.3, 6.5, 6.7, 6.8, διατυπώνουμε το εξής

Θεώρημα 6.9 (Θεμελιώδες Θεώρημα της Θεωρίας Galois). Έστω E/F πεπερασμένη επέκταση Galois, $\mathcal{E}$ το σύνολο των ενδιάμεσων επεκτάσεων και $\mathcal{O}$ το σύνολο των υποομάδων της $G := \mathcal{G}(E/F)$.

1. Οι απεικονίσεις

$$K \in \mathcal{E} \xrightarrow{\mathcal{G}(E/\bullet)} \mathcal{G}(E/K) \in \mathcal{O}$$

$$H \in \mathcal{O} \xrightarrow{\mathcal{F}(\bullet)} \mathcal{F}(H) := \{a \in E : \sigma(a) = a \forall \sigma \in \mathcal{F}(H)\} \in \mathcal{E}$$

είναι αντίστροφες η μία της άλλης, άρα κάθε μία είναι 1-1 και επί. Συμβολικά όταν γράφω $K \leftrightarrow H$ εννοώ αυτή την αμφιμονοσήμαντη αντιστοιχία.

2. Αν $K \in \mathcal{E}$ και $K \leftrightarrow H$ τότε $[E : K] = |H|$ και $[K : F] = [G : H] = \frac{|G|}{|H|}$. Ειδικότερα $[E : F] = |\mathcal{G}(E/F)|$.

3. Αν $K \leftrightarrow H$ τότε για κάθε $\sigma \in G$, $\sigma(K) = \sigma H \sigma^{-1}$.

4. Αν $K \in \mathcal{E}$ τότε η E/K είναι Galois. Επιπλέον η K/F είναι Galois αν και μόνο αν $H \trianglelefteq G$ όπου $H = \mathcal{G}(E/K)$ (δηλαδή $K \leftrightarrow H$). Στην περίπτωση που αυτή η συνθήκη ισχύει, έχουμε τον ισομορφισμό ομάδων $\mathcal{G}(K/F) \cong \mathcal{G}(E/F) / \mathcal{G}(E/K)$.

Υπενθύμιση 6.10 (Για το παράδειγμα που θα ακολουθήσει). Η ομάδα

$$D_n = \langle a, b | a^n = b^2 = 1, ba = a^{n-1}b \rangle$$

ονομάζεται διεδρική βαθμού n και έχει τάξη $|D_n| = 2n$.

Παράδειγμα 6.11. Έστω $f = X^4 - 2 \in \mathbb{Q}[X]$ και E το σώμα διάσπασης του πάνω από το $\mathbb{Q}$. Εύκολα μπορούμε να δούμε ότι $E = \mathbb{Q}(\rho, i)$ με $\rho^4 = 2$ και $i^2 = -1$ και ότι $[E : \mathbb{Q}] = 8$ με βάση τα $\{\rho^k i^l\}_{0 \leq k \leq 3, 0 \leq l \leq 1}$.

Η επέκταση $E/\mathbb{Q}$ είναι Galois αφού είναι κανονική (το E είναι σώμα διάσπασης του f) και διαχωρίσιμη (το $\mathbb{Q}$ έχει χαρακτηριστική 0). Άρα $|\mathcal{G}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 8$. Έστω $G = \mathcal{G}(E/\mathbb{Q})$. Ελέγξτε ότι υπάρχουν $\sigma, \tau \in G$ τέτοιοι ώστε $\sigma(\rho) = i\rho$, $\sigma(i) = i$, $\tau(\rho) = \rho$ και $\tau(i) = -i$.

Κάθε στοιχείο της G χαρακτηρίζεται από τις τιμές του στα ρ και i . Οι δράσεις των αυτομορφισμών της G στα ρ και i φαίνονται στον παρακάτω πίνακα

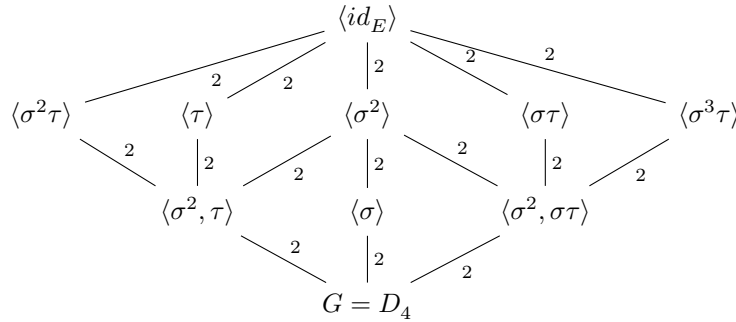
αυτομορφισμός	δράση στο ρ	δράση στο i
id_E	ρ	i
σ	$i\rho$	i
σ^2	$-\rho$	i
σ^3	$-i\rho$	i
τ	ρ	$-i$
$\sigma\tau$	$i\rho$	$-i$
$\sigma^2\tau$	$-\rho$	$-i$
$\sigma^3\tau$	$-i\rho$	$-i$

Ελέγχω ότι $\text{ord}(\sigma) = 4$, $\text{ord}(\tau) = 2$ και ότι $\tau\sigma = \sigma^3\tau$. Άρα μέσα στη G έχω την ομάδα

$$\langle \sigma, \tau \mid \sigma^4 = \text{id} = \tau^2, \tau\sigma = \sigma^3\tau \rangle \cong D_4$$

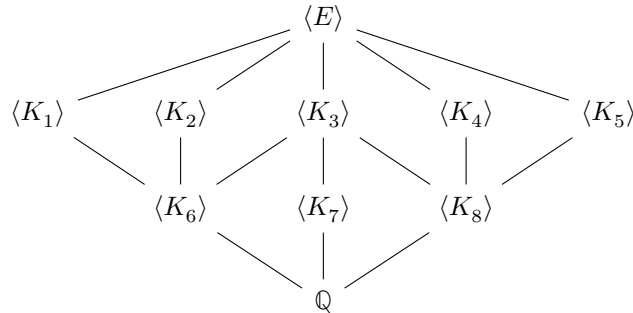
η οποία είναι τάξεως 8, άρα αυτή η ομάδα ταυτίζεται με τη G και $G \cong D_4$.

Το δίκτυο υποομάδων της D_4 είναι



Σε κάθε ακμή σημειώνεται ο δείκτης της υποομάδας που βρίσκεται πάνω, ως προς αυτή από κάτω της. Επιπλέον, βλέπουμε ότι η πρώτη υποομάδα είναι τάξης 1, αυτές της δεύτερης γραμμής είναι τάξης 2, της τρίτης γραμμής είναι τάξης 4 και η G τάξης 8.

Μέσω της αντιστοιχίας Galois, γνωρίζουμε ότι οι ενδιάμεσες επεκτάσεις της E/K είναι σε ένα δίκτυο της ίδιας μορφής



Κάθε K_i αντιστοιχεί, μέσω της αντιστοιχίας Galois, με την υποομάδα του διαγράμματος υποομάδων, η οποία βρίσκεται στην ακριβώς αντίστοιχη θέση. Π.χ. $E \longleftrightarrow \langle id_E \rangle$, $\mathbb{Q} \longleftrightarrow E$, $K_2 \longleftrightarrow \langle \tau \rangle$, $K_8 \longleftrightarrow \langle \sigma^2, \sigma\tau \rangle$. Εδώ, όλες οι διαδοχικές επεκτάσεις είναι βαθμού 2 όσο και οι αντίστοιχοι δείκτες υποομάδων. Επιπλέον μπορούμε να δείξουμε ότι

$$\begin{aligned} K_1 &= \mathbb{Q}(i\rho) \\ K_2 &= \mathbb{Q}(\rho) \\ K_3 &= \mathbb{Q}(i\rho^2) = \mathbb{Q}(i\sqrt{2}) \\ K_4 &= \mathbb{Q}((1+i)\rho) \\ K_5 &= \mathbb{Q}((1-i)\rho) \\ K_6 &= \mathbb{Q}(\sqrt{2}) \\ K_7 &= \mathbb{Q}(i) \\ K_8 &= \mathbb{Q}(i\sqrt{2}) \end{aligned}$$

Πώς αποδεικνύονται αυτές οι ισότητες; Μια κάπως δύσκολη αντιστοιχία είναι

$$\langle \sigma\tau \rangle \longleftrightarrow \mathbb{Q}((1+i)\rho),$$

δηλαδή, $K_4 = \mathbb{Q}((1+i)\rho)$.
Έχω το διάγραμμα

$$\begin{array}{ccc} \langle id_E \rangle & \longrightarrow & E = \mathbb{Q}(i, \rho) \\ \downarrow & & \downarrow 2 \\ \langle \sigma\tau \rangle & \longrightarrow & K_4? \\ \downarrow 2 & & \downarrow 4 \\ G & \longrightarrow & \mathbb{Q} \end{array}$$

Άρα περιμένω το σταθεροποιούμενο απ το $\langle \sigma\tau \rangle$ να είναι επέκταση του $\mathbb{Q}$ βαθμού 4.
Βάση της $E/\mathbb{Q} : 1, \rho, \rho^2, \rho^3, i, i\rho, i\rho^2, i\rho^3$. Έστω

$$u = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 + b_0i + b_1i\rho + b_2i\rho^2 + b_3i\rho^3 \in K_4$$

με τα $a_i, b_i \in \mathbb{Q}$. Τότε,

$$u = \sigma\tau(u) = a_0 + a_1i\rho + a_2(-\rho^2) + a_3(-i\rho^3) - b_0i + b_1\rho + b_2i\rho^2 - b_3\rho^3$$

Άρα,

$$\begin{aligned} a_1 &= b_1 \\ a_2 &= -a_2 \\ b_3 &= -a_3 \\ -b_0 &= b_0 \\ a_1 &= b_1 \\ b_3 &= -a_3, \end{aligned}$$

οπότε $a_2 = b_0 = 0$ και ελεύθερες παράμετροι είναι τα a_0, a_1, a_3 και b_2 . Συνεπώς,

$$\begin{aligned} u &= a_0 + a_1\rho + a_3\rho^3 + a_1i\rho + b_2i\rho^3 + a_3i\rho^3 \\ &= a_0 + a_1\rho(1+i) + b_2i\rho^2 + a_3(1-i)\rho^3 \end{aligned}$$

Αν $\lambda := \rho(1+i)$, τότε $\lambda^2 = 2\rho^2i$ και $\lambda^3 = \rho^32(i-1)$. Επομένως,

$$u = a_0 + a_1\lambda + \frac{b_2}{2}\lambda^2 - \frac{a_3}{2}\lambda^3$$

Άρα το u είναι γραμμικός συνδιασμός των $1, \lambda, \lambda^2, \lambda^3$. Συνεπώς, $u = \sigma\tau(u) \iff u \in \mathbb{Q}(\lambda)$. Αλλά

$$\lambda^4 = (\rho^2(1+i)^2)^2 = (\sqrt{2}(2i))^2 = -8,$$

άρα το λ είναι ρίζα του $X^4 + 8$.

Με ανάλογο τρόπο, μπορώ να δείξω την αντιστοιχία

$$\langle \sigma^3\tau \rangle \longleftrightarrow \mathbb{Q}((1-i)\rho).$$

Αν $\mu = (1-i)\rho$, τότε πάλι

$$\mu^4 = ((1-i)^2\rho^2)^2 = ((-2i)\sqrt{2})^2 = -8$$

Είναι $\langle \sigma\tau \rangle \neq \langle \sigma^3\tau \rangle$, άρα (λόγω του 1-1 της αντιστοιχίας Galois) $\mathbb{Q}(\mu) \neq \mathbb{Q}(\lambda)$, παρά το ότι τα μ, λ είναι ρίζες του ίδιου ανάγωγου πολυωνύμου $X^4 + 8$.

Ερώτηση: Είναι η $\langle \sigma\tau \rangle$ κανονική υποομάδα της G ;

Ισοδύναμο ερώτημα: Είναι η $\mathbb{Q}(\lambda)/\mathbb{Q}$ επέκταση Galois;

Επειδή είναι διαχωρήσιμη, ισοδύναμο ερώτημα: Είναι η $\mathbb{Q}(\lambda)/\mathbb{Q}$ κανονική επέκταση;

Απάντηση, όχι! Το $X^4 + 8$ έχει τη ρίζα $\lambda \in \mathbb{Q}(\lambda)$, όμως $\mu \notin \mathbb{Q}(\lambda)$, διότι $\mathbb{Q}(\mu) \neq \mathbb{Q}(\lambda)$.

Το ότι $(1-i)\rho \notin \mathbb{Q}((1+i)\rho)$ δεν είναι προφανές αν δεν κάνω χρήση του θεωρήματος Galois! Αν όμως κάνω χρήση του θεωρήματος, τότε καθώς $\langle \sigma\tau \rangle \neq \langle \sigma^3\tau \rangle$, προκύπτει αμέσως ότι $\mathbb{Q}(\mu) \neq \mathbb{Q}(\lambda)$ και, άρα, $\mu \notin \mathbb{Q}(\lambda)$.

Ένα δεύτερο παράδειγμα αντιστοιχίας που απαιτεί λιγότερες πράξεις:

$$\langle \sigma^2 \rangle \longleftrightarrow \mathbb{Q}(i, \sqrt{2}),$$

δηλαδή, $K_3 = \mathbb{Q}(i, \sqrt{2})$. Αυτή η ισότητα προκύπτει αμέσως, ως εξής: Είναι $\sigma(i) = i$, άρα $\sigma^2(i) = i$. Επίσης, $\sigma(\sqrt{2}) = \sigma(\rho^2) = (\sigma(\rho))^2 = (i\rho)^2 = -\sqrt{2}$, οπότε $\sigma^2(\sqrt{2}) = \sqrt{2}$. Συνεπώς, τα i και $\sqrt{2}$ ανήκουν στο σταθεροποιούμενο σώμα του σ^2 . Αυτό συνεπάγεται ότι $\mathbb{Q}(i, \sqrt{2}) \leq \mathcal{F}(\langle \sigma^2 \rangle)$. Από το Θεώρημα Galois, το $\mathcal{F}(\langle \sigma^2 \rangle)$ έχει βαθμό πάνω από το $\mathbb{Q}$ ίσο με τον δείκτη $[G : \langle \sigma^2 \rangle] = 4$. Επειδή είναι και $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$, συμπεραίνω ότι $K_3 = \mathcal{F}(\langle \sigma^2 \rangle) = \mathbb{Q}(i, \sqrt{2})$.

Τώρα έχουμε το διάγραμμα

$$\begin{array}{ccc} E & \longrightarrow & \langle id \rangle \\ \downarrow 2 & & \downarrow \\ K_3 = \mathbb{Q}(i, \sqrt{2}) & \longrightarrow & \langle \sigma^2 \rangle \\ \downarrow 4 & & \downarrow \\ \mathbb{Q} & \longrightarrow & G \end{array}$$

Η επέκταση $K_3/\mathbb{Q}$ είναι προφανώς κανονική ως σώμα διάσπασης του $(X^2 + 1)(X^2 - 2)$, άρα, από το Θεώρημα Galois συμπεραίνω ότι $\sigma^2 \trianglelefteq G$ και, ακόμη, ότι $\mathcal{G}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) \cong G/\langle \sigma^2 \rangle$.

Έχω τώρα, $G/\langle \sigma^2 \rangle = \{\bar{1}, \bar{\sigma}, \bar{\tau}, \bar{\tau\sigma}\}$, όπου $\bar{1} = \{id_E, \sigma^2\}$, $\bar{\sigma} = \{\sigma, \sigma^3\}$, $\bar{\tau} = \{\tau, \tau\sigma^2\}$, $\bar{\tau\sigma} = \{\tau\sigma, \tau\sigma^3\}$. Ο πίνακας της ομάδας $G/\langle \sigma^2 \rangle$ είναι

	$\bar{1}$	$\bar{\sigma}$	$\bar{\tau}$	$\bar{\tau\sigma}$
$\bar{1}$	$\bar{1}$	$\bar{\sigma}$	$\bar{\tau}$	$\bar{\tau\sigma}$
$\bar{\sigma}$	$\bar{\sigma}$	$\bar{1}$	$\bar{\tau\sigma}$	$\bar{\tau}$
$\bar{\tau}$	$\bar{\tau}$	$\bar{\tau\sigma}$	$\bar{1}$	$\bar{\sigma}$
$\bar{\tau\sigma}$	$\bar{\tau\sigma}$	$\bar{\tau}$	$\bar{\sigma}$	$\bar{1}$

Βλέπουμε πως έχουμε τον πίνακα ομάδας τάξεως 4, της οποίας κάθε στοιχείο έχει τάξη 2, άρα είναι η «ομάδα των τεσσάρων» $Klein \langle a, b | a^2 = b^2 = 1, ba = ab \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Πώς «μεταφράζω» το ότι $\mathcal{G}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) \cong G/\langle \sigma^2 \rangle$; Αφού η ομάδα στα δεξιά είναι ομάδα Klein, έπεται ότι η ομάδα $\mathcal{G}(K_3/\mathbb{Q})$ ($K_3 = \mathbb{Q}(i, \sqrt{2})$) παράγεται από δύο αυτομορφισμούς, έστω $\phi, \psi \in \mathcal{G}(K/\mathbb{Q})$, για τους οποίους ισχύει $\phi^2 = \psi^2 = id_K$.

Εις αναζήτησιν $\mathbb{Q}$ -αυτομορφισμού ϕ του $K = \mathbb{Q}(i, \sqrt{2})$ με τις παραπάνω ιδιότητες: Ξέρω ότι $\phi(i) \in \{\pm i\}$ και $\phi(\sqrt{2}) \in \{\pm\sqrt{2}\}$. Επιλέγω τον ϕ να ικανοποιεί τις σχέσεις $\phi(i) = -i$ και $\phi(\sqrt{2}) = \sqrt{2}$. Ανάλογα επιλέγω τον ψ να ικανοποιεί τις $\psi(i) = i$ και $\psi(\sqrt{2}) = -\sqrt{2}$. Ελέγχοντας τη δράση των ϕ^2 και ψ^2 στα στοιχεία $i, \sqrt{2}$ βλέπω ότι τα αφήνουν αναλλοίωτα, άρα $\phi^2 = \psi^2 = id_K$.

Γιατί υπάρχει τέτοιος ϕ ; Είναι επέκταση του ταυτοτικού $id_{\mathbb{Q}(\sqrt{2})}$ στο παρακάτω διάγραμμα στέλνοντας το i στο $-i$.

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}, i) & \xrightarrow{\phi} & \mathbb{Q}(\sqrt{2}, i) \\ | & & | \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow{id} & \mathbb{Q}(\sqrt{2}) \end{array}$$

Ανάλογα αποδεικνύεται και η ύπαρξη του ψ .

Ασκήσεις

Άσκηση 6.12. Έστω πεπερασμένη επέκταση Galois E/F και η αλυσίδα ενδιάμεσων επεκτάσεων $F = K_0 \leq K_1 \leq \dots \leq K_n = E$. Έστω $G = \mathcal{G}(E/F)$ και H_i η υποομάδα της G που αντιστοιχεί στο K_i ($i = 0, 1, \dots, n$). Αποδείξτε ότι, για οποιοδήποτε $i \in \{1, \dots, n\}$ ισχύει ότι η επέκταση K_i/K_{i-1} είναι Galois αν και μόνο αν $H_i \trianglelefteq H_{i-1}$.

Άσκηση 6.13. Η άσκηση έχει να κάνει αποκλειστικά με ομάδες, αλλά χρειάζεται σε ένα ερώτημα της επόμενης άσκησης. Έστω ομάδα $(G, \cdot)$, $H \leq G$ και $J = \bigcap_{g \in G} gHg^{-1}$. Αποδείξτε ότι $J \trianglelefteq G$.

Άσκηση 6.14. Έστω πεπερασμένη διαχωρίσιμη επέκταση E/F και N κανονική κλειστότητα του E πάνω από το F .

(α') Αποδείξτε ότι η N/F είναι Galois.

Υπόδειξη. Από το Θεώρημα 5.20, η επέκταση E/F είναι απλή. Έστω $E = F(\alpha)$, $f = \text{Irr}(\alpha, F)$ και $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n \in N$ όλες οι ρίζες του f . Δείξτε ότι $N = F(\alpha_1, \dots, \alpha_n)$.

(β') Έστω $G = \mathcal{G}(N/F)$ και $H = \mathcal{G}(N/E)$.

(β'.1) Έστω $H' \trianglelefteq G$ τέτοια ώστε $H' \leq H$. Αποδείξτε ότι στην επέκταση N/F το σταθεροποιούμενο σώμα της H' είναι το N και συμπεράνετε ότι $H' = \langle id_N \rangle$.

(β'.2) Εφαρμόζοντας την άσκηση 6.13 αποδείξτε ότι $\bigcap_{\sigma \in G} \sigma H \sigma^{-1} = \langle id_N \rangle$.

Άσκηση 6.15. Έστω $\bar{\mathbb{Q}}$ αλγεβρική κλειστότητα του $\mathbb{Q}$ (δεν είναι απαραίτητο να τη δείτε ως υπόσωμα του $\mathbb{C}$). Θεωρούμε τους $\alpha, \beta, \gamma \in \bar{\mathbb{Q}}$ που ικανοποιούν τις σχέσεις $\alpha^2 = 2$, $\beta^2 = 3$ και $\gamma^2 = 5$.

(1) Αποδείξτε ότι το $X^2 - 3$ είναι ανάγωγο πάνω από το $\mathbb{Q}(\alpha)$.

(2) Έστω $K = \mathbb{Q}(\alpha, \beta)$. Αποδείξτε ότι η επέκταση $K/\mathbb{Q}$ είναι Galois. Αποδείξτε, επίσης, ότι υπάρχουν $\sigma, \tau \in \mathcal{G}(K/\mathbb{Q})$ με τις εξής ιδιότητες: $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$ και $\tau(\alpha) = \alpha$, $\tau(\beta) = -\beta$. Δείξτε ότι $\mathcal{G}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$ και αυτή η ομάδα είναι η V_4 («ομάδα των τεσσάρων του Klein»). Κατασκευάστε το δίκτυο των υποομάδων της $\mathcal{G}(K/\mathbb{Q})$ και το αντίστοιχο δίκτυο ενδιάμεσων επεκτάσεων της $K/\mathbb{Q}$.

(3) Αποδείξτε με «έξυπνο» τρόπο, δίχως καθόλου πράξεις (εκμεταλλευόμενοι το (2)), ότι το $X^2 - 5$ είναι ανάγωγο πάνω από το K . Συμπεράνετε ότι η επέκταση E/K είναι βαθμού 2, όπου $E = \mathbb{Q}(\alpha, \beta, \gamma)$. Αποδείξτε ότι η E/K είναι Galois, βαθμού 8 και βρείτε μια βάση της.

(4) Έστω $G = \mathcal{G}(E/\mathbb{Q})$. Αποδείξτε ότι υπάρχουν $\phi, \chi, \psi \in G$ με τις εξής ιδιότητες:

$$\phi(\alpha) = -\alpha, \phi(\beta) = \beta, \phi(\gamma) = \gamma$$

$$\chi(\alpha) = \alpha, \chi(\beta) = -\beta, \chi(\gamma) = \gamma$$

$$\psi(\alpha) = \alpha, \psi(\beta) = \beta, \psi(\gamma) = -\gamma$$

Κατασκευάστε πίνακα που θα δείχνει πώς δρουν στα α, β, γ οι αυτομορφισμοί $\text{id}_E, \phi, \chi, \psi, \phi\chi, \phi\psi, \chi\psi, \phi\chi\psi$.

(5) Αποδείξτε ότι $G = \langle \phi, \chi, \psi \rangle$, η G είναι αβελιανή, τάξεως 8 και τα στοιχεία της έχουν τάξη 2

(6) Θεωρήστε δεδομένα τα εξής: Όλες οι υποομάδες της G τάξεως 2 είναι οι

$$\langle \phi \rangle, \langle \chi \rangle, \langle \psi \rangle, \langle \phi\chi \rangle, \langle \phi\psi \rangle, \langle \chi\psi \rangle, \langle \phi\chi\psi \rangle.$$

Όλες οι υποομάδες της G τάξεως 4 είναι οι

$$\langle \phi, \chi \rangle, \langle \phi, \psi \rangle, \langle \chi, \psi \rangle, \langle \phi, \chi\psi \rangle, \langle \chi, \phi\psi \rangle, \langle \psi, \phi\chi \rangle, \langle \phi\chi, \phi\psi \rangle.$$

Με τη βοήθεια του πίνακα του ερωτήματος (4) υπολογίστε την ενδιάμεση επέκταση που αντιστοιχεί σε κάθε μία από τις παραπάνω 14 υποομάδες.