Θεωρία Galois

Θεοδώρα Θεοχαρη-Αποστολιδη

Χαρά Χαραλαμπους

Οι σημειωσεις αυτες θα συμπληρωνονται κατα τη διαρκεια των μαθηματων.

13 Δεκεμβρίου 2014

Περιεχόμενα

Κεφάλαιο 3

Μεταθέσεις και ομάδες Galois

3.1 Οι ρίζες του $x^3 - 2$ και οι συμμετρίες του ισόπλευρου τριγώνου.

Θα θεωρήσουμε το πολυώνυμο $x^3 - 2 \in \mathbb{Q}[x]$. Έστω $b = \sqrt[3]{2}$, $\omega = \omega_3 = e^{2\pi i/3}$ και $E = \mathbb{Q}(b, \omega b, \omega^2 b)$. Παρατηρούμε ότι

$$E = \mathbb{Q}(b, \omega b) = \mathbb{Q}(b, \omega_3^2 b) = \mathbb{Q}(\omega b, \omega_3^2 b) = \mathbb{Q}(b, \omega) \ .$$

Θα χρησιμοποιήσουμε την τελευταία έκφραση $E = \mathbb{Q}(b, \omega)$, κυρίως γιατί τα δύο ανάγωγα πολυώνυμα,

$$\mathrm{irr}_{\mathbb{Q},b}(x) = x^3 - 2, \ \mathrm{irr}_{\mathbb{Q},\omega}(x) = x^2 + x + 1$$

θα διευκολύνουν τους υπολογισμούς μας. Παρατηρούμε επίσης ότι οι ρίζες του $x^3 - 2$ είναι ίσες με $\omega^i b$, $i = 0, 1, 2$. Σύμφωνα με το Παράδειγμα 2.2.12 μία $\mathbb{Q}$-βάση για το E είναι το σύνολο $\{1, b, b^2, \omega, \omega b, \omega b^2\}$. Έστω $G = \mathrm{Gal}(E/\mathbb{Q})$. Αν $\phi \in G$ τότε ϕ καθορίζεται πλήρως από τις εικόνες $\phi(b)$, και $\phi(\omega)$ σύμφωνα με τη Πρόταση 2.3.3. Έπεται ότι έχουμε το πολύ 6 στοιχεία στην G. Αφού $E = \mathbb{Q}(\omega)(b)$ και

$$\mathrm{irr}_{(\mathbb{Q}(\omega),b)}(x) = \mathrm{irr}_{(\mathbb{Q},b)}(x) = x^3 - 2,$$

σύμφωνα με το Θεώρημα 2.3.4 υπάρχουν τρία διαφορετικά στοιχεία της G, σύμφωνα με τα οποία $c \mapsto c$, $\forall\ c \in \mathbb{Q}(\omega)$ και b απεικονίζεται σε μία από τις τρεις ρίζες του $x^3 - 2$:

$$b \mapsto \begin{cases} b \\ \omega b \\ \omega^2 b \end{cases} \ .$$

Αντίστοιχα αφού $E = \mathbb{Q}(b)(\omega)$ και

$$\mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x) = \mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^2 + x + 1,$$

υπάρχουν δύο αυτομορφισμοί στην G τέτοιοι ώστε $c \mapsto c$, $\forall\ c \in \mathbb{Q}(b)$ ενώ

$$\omega \mapsto \begin{cases} \omega \\ \omega^2 \end{cases} .$$

Σημειώνουμε ότι όταν $\omega \mapsto \omega$ και $b \mapsto b$ τότε $c \mapsto c\ \forall\ c \in E$ και έχουμε τον ταυτοτικό αυτομορφισμό του E. Έτσι προς το παρόν έχουμε βρει 4 διαφορετικά στοιχεία της G. Οι συνθέσεις τους μας δίνουν άλλους δύο αυτομορφισμούς:

b	b	ωb	$\omega^2 b$	b	ωb	$\omega^2 b$
ω	ω	ω	ω	ω^2	ω^2	ω^2
	id_E	σ_1	σ_2	σ_3	σ_4	σ_5

όπου $\sigma_2 = \sigma_1^2$, $\sigma_4 = \sigma_1 \circ \sigma_3$ ενώ $\sigma_5 = \sigma_3 \circ \sigma_1$. Άρα η ομάδα G δεν είναι αντιμεταθετική. Έστω τώρα $a \in E$ και ας υπολογίσουμε την εικόνα $\sigma_1(a)$. Αφού

$$a = a_0 + a_1 b + a_2 b^2 + a_3\omega + a_4\omega b + a_5\omega b^2$$

και $\sigma_1(a_i) = a_i$, $\sigma_1(b) = \omega b$, $\sigma_1(\omega) = \omega$ έπεται ότι $\sigma_1(b^2) = \omega^2 b^2$, $\sigma_1(\omega b) = \omega^2 b$ και $\sigma_1(\omega b^2) = \omega^3 b^2 = b^2$. Επίσης αφού ω είναι ρίζα του πολυωνύμου $x^2 + x + 1$ έπεται ότι $\omega^2 = -1 - \omega$. Άρα

$$\sigma_1(a) = a_0 - a_4 b + (-a_2 + a_5)b^2 + a_4\omega + (a_1 - a_4)\omega b - a_2\omega b^2 .$$

Είδαμε ότι $|G| = 6$. Γνωρίζουμε ότι με προσέγγιση ισομορφίας υπάρχει μόνο μία μη αντιμεταθετική ομάδα με 6 στοιχεία και ότι αυτή είναι η ομάδα S_3 των μεταθέσεων 3 στοιχείων. Θα εξερευνήσουμε αυτήν την σχέση παρατηρώντας ότι αν $\sigma \in G$ και $X = \{b, \omega b, \omega^2 b\}$ τότε

$$\{\sigma(b), \sigma(\omega b), \sigma(\omega^2 b)\} = X .$$

Για παράδειγμα $\sigma_1(b) = \omega b$, $\sigma_1(\omega b) = \sigma_1(\omega)\sigma_1(b) = \omega^2 b$ ενώ $\sigma_1(\omega^2 b) = \omega^3 b = b$. Γενικώτερα οι ρίζες του $x^3 - 2$ απεικονίζονται σε ρίζες του $x^3 - 2$ και μάλιστα διαφορετικές ρίζες απεικονίζονται διαφορετικές ρίζες αφού τα στοιχεία της G είναι αμφινονότιμες συναρτήσεις του E. Έτσι κάθε στοιχείο της G ορίζει μία μετάθεση του X, δηλαδή μία αμφιμονότιμη συνάρτηση του X στον εαυτό του. Έστω S_X το σύνολο των μεταθέσεων του X. Ορίζουμε την συνάρτηση $\phi :\ G \to S_X$, όπου για $\sigma \in G$, $\phi(\sigma) \in S_X$ είναι η μετάθεση

$$\phi(\sigma) :\ X \to X, \quad \omega^i b \mapsto \sigma(\omega^i b) .$$

Έτσι αναλυτικά οι εικόνες των $\phi(\sigma)$, $\sigma \in G$ είναι:

$$\mathrm{id}_E \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ b & \omega b & \omega^2 b \end{pmatrix},\ \sigma_1 \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega b & \omega^2 b & b \end{pmatrix},\ \sigma_2 \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega^2 b & b & \omega b \end{pmatrix},$$

$$\sigma_3 \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ b & \omega^2 b & \omega b \end{pmatrix},\ \sigma_4 \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega b & b & \omega^2 b \end{pmatrix}\ \sigma_5 \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega^2 b & \omega b & b \end{pmatrix}.$$

Η S_X είναι βέβαια ομάδα, και η ϕ δεν είναι απλά μία αμφιμονότιμη συνάρτηση ανάμεσα σε δύο σύνολα, αλλά ομομορφισμός ομάδων. Πράγματι για κάθε $\sigma, \tau \in G$, ισχύει ότι

$$\phi(\sigma \circ \tau) = \phi(\sigma) \circ \phi(\tau)$$

όπως εύκολα μπορεί να ελεγχθεί αφού $\phi(\sigma_i \circ \tau)$ και $\phi(\sigma_i) \circ \phi(\tau)$ συμφωνούν για τυχαίο $\omega^t b$. Έπεται ότι

$$G \cong S_X\ .$$

Παρατηρούμε επίσης ότι η ομάδα G είναι ισόμορφη με την ομάδα των συμμετριών του ισόπλευρου τριγώνου. Τοποθετούμε τις ρίζες $\omega^t b$ στις κορυφές του ισόπλευρου τριγώνου. Οι συμμετρίες που αντιστοιχούν στις περιστροφές κατά γωνία 0, $2\pi/3$ και $4\pi/3$ θα μετακινήσουν τις ρίζες σε νέες θέσεις που υποδεικνύονται από τις μεταθέσεις id_E, σ_1, σ_2. Οι 3 συμμετρίες που είναι αντικατοπτρισμοί ως προς τις διχοτόμους των 3 πλευρών θα μετακινήσουν τις ρίζες σε νέες θέσεις που υποδεικνύονται από τις μεταθέσεις σ_3, σ_4, σ_5.

3.2 Μεταθέσεις και ομάδα Galois

Θα ξεκινήσουμε με το βασικό θεώρημα αυτής της παραγράφου, που γενικεύει τα αποτελέσματα της προηγούμενης ενότητας.

Θεώρημα 3.2.1. *Έστω $f(x) \in \Bbbk[x]$ διαχωρίσιμο και ανάγωγο,* $\deg f(x) = n$ *και έστω E σώμα ανάλυσης του $f(x)$. Τότε η ομάδα* $\mathrm{Gal}(E/\Bbbk)$ *εμφυτεύεται στην ομάδα των μεταθέσεων S_n.*

Απόδειξη. Έστω $X = \{b_1, \ldots, b_n\}$ το σύνολο των ριζών του $f(x)$. Τότε $E = \Bbbk(b_1, \ldots, b_n)$. Τα στοιχεία του S_X είναι αμφιμονότιμες συναρτήσεις του X στον εαυτό του και $S_X \cong S_n$. Αν $G = \mathrm{Gal}(E/\Bbbk)$ και $\sigma \in G$ τότε θεωρούμε την συνάρτηση $\theta_\sigma : X \to X$, $\theta_\sigma(b_i) = \sigma(b_i)$ $i = 1, \ldots, n$. Είναι εύκολο να δείξει κανείς ότι $\theta_\sigma \in S_X$, δηλαδή ότι $\theta(b_i) = \theta(b_j) \Leftrightarrow b_i = b_j$. Έτσι οδηγούμαστε στον επόμενο ορισμό:

$$\phi : G \to S_Q, \quad \sigma \mapsto \theta_\sigma.$$

Η συνάρτηση αυτή είναι μονομορφισμός ομάδων. Πράγματι

- $\phi(\sigma \circ \tau) = \phi(\sigma) \circ \phi(\tau)$ για $\sigma, \tau \in G$ και
- ϕ είναι μονομορφισμός, δηλαδή $\phi(\sigma) = \phi(\tau) \Leftrightarrow \sigma = \tau$ για $\sigma, \tau \in G$.

Οι λεπτομέρειες της απόδειξης επαφίονται στον αναγνώστη. □

Το επόμενο παράδειγμα που θα κάνουμε αναλυτικά έχει να κάνει με το πολυώνυμο $x^4 - 2 \in \mathbb{Q}[x]$.

Ορισμοί 3.2.2. Έστω $f(x) = x^4 - 2$. Αν $b = \sqrt[4]{2}$, οι ρίζες του $f(x)$ στο $\mathbb{C}$ είναι $\pm b$, $\pm bi$ και $E = \mathbb{Q}(2^{1/4}, i)$ είναι σώμα ανάλυσης του $f(x)$. Θα δείξουμε ότι η ομάδα $G = \mathrm{Gal}(E/\mathbb{Q})$ είναι ισόμορφη με την ομάδα των συμμετριών του τετραγώνου. Πράγματι η G έχει το πολύ 8 στοιχεία αφού αν $\sigma \in G$, τότε

$$\sigma(b) = \begin{cases} b \\ -b \\ ib \\ -ib \end{cases}, \sigma(i) = \begin{cases} i \\ -i \end{cases} .$$

Η G έχει όντως ακριβώς 8 στοιχεία που προκύπτουνε από τους αυτομορφισμούς $\sigma : \ b \mapsto ib, i \mapsto i$, $\tau : \ b \mapsto b, i \mapsto -i$ και τις συνθέσεις τους. Αναλυτικά τα στοιχεία της G είναι:

b	b	$-b$	b	$-b$	ib	ib	$-ib$	$-ib$
i	i	i	$-i$	$-i$	i	$-i$	i	$-i$
	id_E		τ		σ			

Οι αυτομορφισμοί σ και τ αντιστοιχούν στις μεταθέσεις

$$\begin{pmatrix} b & -b & ib & -ib \\ ib & -ib & -b & b \end{pmatrix} \text{ και } \begin{pmatrix} b & -b & ib & -ib \\ b & -b & -ib & ib \end{pmatrix} .$$

Τοποθετώντας τις ρίζες του $f(x)$ ως κορυφές ενός τετραγώνου αριστερόστροφα με τη σειρά $b, ib, -b, -ib$, παρατηρούμε ότι σ αντιστοιχεί σε αριστερόστροφη περιστροφή με γωνία $3\pi/2 = 2\pi/4 \cdot 3$ ενώ τ αντιστοιχεί σε αντικατοπτρισμό ως προς τη διαγώνιο που περνάει από τις κορυφές $b, -b$.

3.3 Πληθυκότητα της ομάδας Galois

Έχουμε δει ότι αν $\sigma : E_1 \to F_1$ είναι ισομορφισμός σωμάτων, τότε

$$\widehat{\sigma} : E_1[x] \to F_1[x], \ \sum a_i x^i \mapsto \sigma(a_i) x^i$$

είναι ισομορφισμός δακτυλίων. Αυτός ο ισομορφισμός θα χρησιμοποιηθεί στο επόμενο θεώρημα.

Θεώρημα 3.3.1. *Έστω $\sigma : E_1 \longrightarrow F_1$ ισομορφισμός σωμάτων, $f(x) = \sum a_i x^i \in E_1[x]$ διαχωρίσιμο. Έστω E σώμα ανάλυσης του $f(x)$ υπεράνω του E_1, και F σώμα ανάλυσης του $\widehat{\sigma}(f(x))$ υπεράνω του F_1. Υπάρχουν ακριβώς $[E : E_1]$ επεκτάσεις $\tilde{\sigma} : E \to F$ έτσι ώστε $\tilde{\sigma}|_{E_1} = \sigma$*

Απόδειξη. Το Θεώρημα θα προκύψει με επαγωγή στον βαθμό $[E : E_1]$.

- Αν $[E : E_1] = 1$ τότε $E = E_1$ και όλες οι ρίζες του $f(x)$ ανήκουν στο E. Αφού $\tilde{\sigma}$ είναι ισομορφισμός δακτυλίων έπεται ότι οι ρίζες του $\tilde{\sigma}(f(x))$ ανήκουν στο F_1 και άρα $F = F_1$.

- Θα υποθέσουμε τώρα ότι το θεώρημα ισχύει όταν ο βαθμός της επέκτασης $[E : E_1]$ είναι μικρότερος του n.

- Έστω ότι $[E : E_1] = n$. Τότε υπάρχει $b \in E \setminus E_1$ έτσι ώστε $f(b) = 0$. Έπεται ότι $E_1(b) \neq E_1$ και αφού

$$[E : E_1] = [E : E_1(b)][E_1(b) : E_1]$$

βλέπουμε ότι $[E : E_1(b)] < n$. Έστω τώρα ότι $g(x) = \mathrm{irr}_{E_1,b}(x)$. Τότε $g(x)|f(x)$ και επομένως είναι διαχωρίσιμο. Έστω b' τυχαία ρίζα του $\tilde{\sigma}(g(x))$ στο F. Σύμφωνα με το Θεώρημα 2.3.5 υπάρχει ισομορφισμός $\sigma' : E_1(b) \to F_1(b')$ έτσι ώστε $\sigma'|_{E_1} = \sigma$. Σημειώνουμε ότι E είναι σώμα ανάλυσης του $f(x)$ και υπεράνω του $E_1(b)$ και αντίστοιχα για το F και $\widehat{\sigma}(g(x))$ περάνω του $F_1(b)$. Από την υπόθεση τώρα της επαγωγής έπεται ότι υπάρχει $\tilde{\sigma} : E \to F$ έτσι ώστε $\tilde{\sigma}|_{E_1(b)} = \sigma'$ και μάλιστα υπάρχουν $[E : E_1(b)]$ τέτοιοι ισομορφισμοί $\tilde{\sigma}$. Μένει λοιπόν να μετρήσουμε τους ισομορφισμούς σ'. Αφού $g(x)$ είναι διαχωρίσιμο είχαμε τόσες επιλογές για το b' όσες και οι ρίζες του $\widehat{\sigma}(g(x))$ δηλαδή $[E_1(b) : E_1]$. Έπεται ότι συνολικά έχουμε

$$[E : E_1(b)][E_1(b) : E_1]$$

επιλογές, και αυτός ο αριθμός είναι ίσος με $[E : E_1]$.

□

Τα επόμενα δύο πορίσματα είναι άμεσα.

Πόρισμα 3.3.2. *Έστω $f(x) \in F[x]$, και E, E' δύο σώματα ανάλυσης του $f(x)$ υπεράνω του F. Τότε υπάρχει ισομορφισμός $\tilde{\sigma} : E \to E'$ που διατηρεί σταθερό το F. Αν το $f(x)$ είναι διαχωρίσιμο τότε υπάρχουν ακριβώς $[E : F]$ ισομορφισμοί που διατηρούν σταθερό το F.*

Απόδειξη. Στην απόδειξη του προηγούμενου θεωρήματος χρησιμοποιήσαμε την υπόθεση ότι $f(x)$ είναι διαχωρίσιμο μόνο στο σημείο όπου μετρούσαμε τους αυτομορφισμούς που επεκτείνουν τον σ και όχι για την ύπαρξη των αυτομορφισμών. □

Πόρισμα 3.3.3. *Έστω $f(x) \in F[x]$ διαχωρίσιμο, E είναι σώμα ανάλυσης του $f(x)$. Τότε $|\mathrm{Gal}(E/F)| = [E : F]$.*

Απόδειξη. Θεωρούμε τον ταυτοτικό ισομορφισμό $\mathrm{id}_F : F \to F$ και εφαρμόζουμε το θεώρημα. □

Παραδείγματα 3.3.4.

1. Έστω $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $G = \mathrm{Gal}(E/\mathbb{Q})$. Αφού $[E : \mathbb{Q}] = 8$, (βλ. Άσκηση 2.4.5 έπεται ότι $|G| = 8$. Έστω $\sigma \in G$. Τότε $\sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$, $\sqrt{5} \mapsto \pm\sqrt{5}$. Επεται ότι G είναι αντιμεταθετική και κάθε στοιχείο της έχει τάξη 2, άρα $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. Έστω $b = 2^{1/3}$, $\omega = e^{2\pi i/3}$, $F = \mathbb{Q}(\omega)$, $E = \mathbb{Q}(\omega, b) = F(b)$. Τότε

$$\mathrm{Gal}(E/F) \cong \mathbb{Z}_3 \ .$$

Πράγματι έστω $H = \mathrm{Gal}(E/F)$. E είναι σώμα ανάλυσης του $x^3 - 2$ πάνω από το F όπως και πάνω από το $\mathbb{Q}$. Έχουμε δει αναλυτικά ότι $[E : \mathbb{Q}] = 6$. Αφού $[F : \mathbb{Q}] = 2$ έπεται ότι $|H| = [E : F] = 3$. Επίσης παρατηρούμε ότι αναγκαστικά

$$\mathrm{irr}_{(F,b)}(x) = \mathrm{irr}_{(\mathbb{Q},b)}(x) = x^3 - 2$$

και αν $\sigma \in H$ τότε

$$\sigma(b) = \begin{cases} b \\ \omega b \\ \omega^2 b \end{cases}$$

Είναι εύκολο να δει κανείς ότι αν $\sigma \neq \mathrm{id}_E$ τότε η τάξη του σ είναι 3. Για παράδειγμα έστω ότι $\sigma(b) = \omega b$. Τότε

$$\sigma^2(b) = \sigma(\omega b) = \sigma(\omega) \cdot \sigma(b) = \omega \cdot \omega b = \omega^2 b$$

και

$$\sigma^3(b) = \sigma(\sigma^2(b)) = \sigma(\omega^2 b) = \sigma(\omega^2) \cdot \sigma(b) = \omega^2 \cdot \omega b = \omega^3 b = b \ .$$

Μία βάση του E υπεράνω του F είναι $\{1, b, b^2\}$ και ένα τυχαίο στοιχείο του E είναι F-γραμμικός συνδυασμός:

$$a = a_0 + a_1 b + a_2 b^2, \ a_i \in F \ .$$

Έτσι για παράδειγμα αν $\sigma \in H$, $\sigma(b) = \omega b$ τότε

$$\sigma(a) = \sigma(a_0 + a_1 b + a_2 b^2) = a_0 + (a_1\omega)b + (a_2\omega^2)b^2 \ .$$

Για το επόμενο παράδειγμα θα χρειαστούμε δύο Θεωρήματα από τη Θεωρία Ομάδων :

Θεώρημα 3.3.5. *(Cauchy) Έστω G πεπερασμένη ομάδα, p πρώτος έτσι ώστε p διαιρεί $|G|$. Υπάρχει στοιχείο $g \in G$ έτσι ώστε η τάξη του g να είναι ίση με p.*

Θεώρημα 3.3.6. *Έστω $g_1, g_2 \in S_5$ έτσι ώστε η τάξη του g_1 να είναι 5 και η g_2 να είναι αντιμετάθεση, να ανταλλάσει δηλαδή 2 στοιχεία και να κρατάει τα άλλα σταθερά. Τότε $\langle g_1, g_2 \rangle = S_5$, δηλαδή όλα τα στοιχεία της S_5 προκύπτουν ως συνδυασμοί συνθέσεων των g_1, g_2.*

Παράδειγμα 3.3.7. Έστω $f(x) = x^5 - 4x + 2$, E το σώμα ανάλυσης του $f(x)$ υπεράνω του $\mathbb{Q}$ και $G = \mathrm{Gal}(E/\mathbb{Q})$. Το πολυώνυμο $f(x)$ είναι ανάγωγο σύμφωνα με το κριτήριο του Eisenstein για $p = 2$ και, διαχωρίσιμο αφού $\mathbb{Q}$ έχει χαρακτηριστική 0. Επομένως $f(x)$ έχει 5 διαφορετικές ρίζες. Αφού $f'(x) = 5x^4 - 4$, $f''(x) = 20x^3$ κάνοντας το γράφημα του $f(x)$ στο πραγματικό επίπεδο, παρατηρούμε ότι $f(x)$ συναντά τον άξονα των x ακριβώς 3 φορές. Άρα $f(x)$ έχει 3 πραγματικές ρίζες, έστω a_1, a_2, a_3 και δύο μιγαδικές, έστω a_4, a_5. Γνωρίζουμε ότι οι δύο μιγαδικές ρίζες είναι συζυγείς: αν $a_4 = a + bi$, τότε $a_5 = a - bi$. Έχουμε λοιπόν ότι $E = \mathbb{Q}(a_1, \ldots, a_5)$ και αφού $\mathrm{irr}_{(Q,a_1)}(x) = f(x)$ έπεται ότι

$$|G| = [E : \mathbb{Q}] = [E : \mathbb{Q}(a_1)][\mathbb{Q}(a_1) : Q] = 5[E : \mathbb{Q}(a_1)] \ .$$

Σύμφωνα με το Θεώρημα του Cauchy η G περιέχει ένα στοιχείο που έχει τάξη 5. Θα θεωρήσουμε τώρα τον αυτομορφισμό του $\mathbb{C}$:

$$\sigma : \ \mathbb{C} \to \mathbb{C}, \ c + di \mapsto c - di \ .$$

Παρατηρούμε ότι $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Επίσης αφού κάθε στοιχείο του E είναι πολυωνυμικός συνδυασμός των a_i και έχουμε ότι $\sigma(a_i) = a_i$ για $i = 1, 2, 3$ ενώ $\sigma(a_4) = a_5$ έπεται ότι αν $b \in E$ τότε $\sigma(b) \in E$:

$$\sigma|_E : \ E \to E \ .$$

Άρα $\sigma|_E \in G$. Όμως $\sigma|_E$ είναι μία αντιμετάθεση δύο ριζών του $f(x)$. Σύμφωνα με το Θεώρημα 3.3.6 έπεται ότι η ομάδα G είναι ισόμορφη με την S_5. Ισοδύναμα, μπορούμε να καταλήξουμε στην ύπαρξη του αυτομορφισμού $\sigma|_E$ θεωρώντας το υπόσωμα $E_1 = \mathbb{Q}(a_1, a_2, a_3)$ και παρατηρώντας ότι $g(x) = \mathrm{irr}_{E_1,a_4}(x)$ έχει βαθμό 2. Από αυτό έπεται ότι $g(x) = (x - a_4)(x - a_5) = x^2 - 2ax + (a^2 + b^2) \in E_1[x]$ και άρα $a, b^2 \in E_1$. Προκύπτει λοιπόν ότι $E = E_1(a + bi) = E_1(bi)$ και η ύπαρξη του $\sigma|_E$ από το Θεώρημα 2.3.4.

3.4 Ενδιάμεσα σώματα και υποομάδες της ομάδας Galois

Έστω $f(x) \in F[x]$ και E/F σώμα ανάλυσης του $f(x)$. Στην ενότητα αυτή θα εξετάσουμε πιο προσεκτικά τη σχέση ανάμεσα στα ενδιάμεσα σώματα $F \subset B \subset E$ και στις υποομάδες της $\mathrm{Gal}(E/F)$.

Πρόταση 3.4.1. *Έστω $F \subset B \subset E$ επέκταση σωμάτων. Τότε $\mathrm{Gal}(E/B)$ είναι υποομάδα της $\mathrm{Gal}(E/F)$.*

Απόδειξη. Αν $\sigma \in \mathrm{Gal}(E/B)$ τότε $\sigma(b) = b$, $\forall b \in B$. Έπεται ότι $\sigma \in \mathrm{Gal}(E/F)$. □

Θεώρημα 3.4.2. *Έστω $F \subset B \subset E$ επέκταση σωμάτων έτσι ώστε B, E είναι σώματα ανάλυσης πάνω από το F. Τότε $\mathrm{Gal}(E/B)$ είναι κανονική υποομάδα της $\mathrm{Gal}(E/F)$ και*

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/F).$$

Απόδειξη. Αφού B είναι σώμα ανάλυσης πάνω από το F έπεται ότι $B = F(b_1, \ldots, b_n)$ όπου b_i είναι ρίζες κάποιου πολυωνύμου $g(x) \in F[x]$. Έστω $\sigma \in \mathrm{Gal}(E/F)$. Θα αποδείξουμε ότι

$$\sigma|_B : \ B \to B \ .$$

Πράγματι αφού τα στοιχεία του B είναι πολυωνυμικοί συνδυασμοί των b_i για $i = 1, \ldots, n$ αρκεί να δείξουμε ότι $\sigma|_B(b_i) \in B$. Αυτό όμως προκύπτει εύκολα αφού $\sigma|_B(b_i) = \sigma(b_i)$ είναι επίσης ρίζα του $g(x)$ σύμφωνα με τη Πρόταση 2.3.3. Θεωρούμε τώρα την συνάρτηση

$$\phi : \ \mathrm{Gal}(E/F) \to \mathrm{Gal}(B/F), \quad \sigma \mapsto \phi|_B \ .$$

Είναι εύκολο να δει κανείς ότι ϕ είναι ομομορφισμός ομάδων. Σύμφωνα με το Πρώτο Θεώρημα Ισομορφίας Ομάδων έπεται ότι $\ker\phi$ είναι κανονική υποομάδα της $\mathrm{Gal}(E/F)$ και

$$\mathrm{Gal}(E/F)/\ker\phi \cong \mathrm{Im}\phi.$$

Στη συνέχεια θα δείξουμε ότι $\ker\phi = \mathrm{Gal}(E/B)$ και ότι $\mathrm{Im}\phi = \mathrm{Gal}(B/F)$.

- Σύμφωνα με τον ορισμό $\ker\phi = \{\sigma \in \mathrm{Gal}(E/F) : \ \phi(\sigma) = \mathrm{id}_B\} = \{\sigma \in \mathrm{Gal}(E/F) : \ \sigma|_B = \mathrm{id}_B\} = \mathrm{Gal}(E/B)$.
- Ισχύει ότι $\mathrm{Im}\phi \subset \mathrm{Gal}(B/F)$. Θα πρέπει να δείξουμε ότι αν $\tau \in \mathrm{Gal}(B/F)$ τότε υπάρχει $\sigma \in \mathrm{Gal}(E/F)$ έτσι ώστε $\sigma|_B = \tau$. Θα χρησιμοποιήσουμε σε αυτό το σημείο ότι E είναι σώμα ανάλυσης του F. Αφού E είναι σώμα ανάλυσης του F τότε είναι και σώμα ανάλυσης του B. Σύμφωνα με το Θεώρημα 3.3.1 υπάρχει ο ζητούμενος αυτομορφισμός του E.

□

Παράδειγμα 3.4.3. Έστω $b = 2^{1/3}$ και $\omega = e^{2\pi i/3}$, $F = \mathbb{Q}(\omega)$, $E = \mathbb{Q}(\omega, b)$, $G = \mathrm{Gal}(E/\mathbb{Q})$. Έχουμε $\mathbb{Q} \subset F \subset E$. Έχουμε δει ότι $|G| = 6$ και ότι η ομάδα $H = \mathrm{Gal}(E/F) \cong \mathbb{Z}_3$. Θα γράψουμε τα 3 αυτά στοιχεία ως στοιχεία της G:

$$\begin{array}{c|ccc} b & b & \omega b & \omega^2 b \\ \hline \omega & \omega & \omega & \omega \end{array}.$$

Αφού F είναι σώμα ανάλυσης του $\mathbb{Q}$ έπεται ότι$H \lhd G$ και ότι $G/H \cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_2$.

Ορισμός 3.4.4. *Έστω E μία επέκταση του F, $G = \mathrm{Gal}(E/F)$ και H υποομάδα της G. Το σύνολο των σταθερών στοιχείων της H είναι το σύνολο*

$$E^H = \{a \in E : \ \sigma(a) = a, \ \forall \sigma \in H \ .$$

Πρόταση 3.4.5. *Το σύνολο E^H είναι σώμα και*

$$F \subset E^H \subset E \ .$$

Αν

$$H_1 \subset H_2 \Rightarrow E^{H_1} \supset E^{H_2} \ .$$

Απόδειξη. Η απόδειξη επαφίεται στον αναγνώστη. □

Παραδείγματα 3.4.6.

1. Έστω $E = \mathbb{Q}(i)$. Τότε $G = \mathrm{Gal}(E/\mathbb{Q}) = \{id_E, \sigma_1 : i \mapsto -i\} \cong \mathbb{Z}_2$. Έχουμε $a + bi = \sigma_1(a + bi) = a - bi \Leftrightarrow b = 0$, επομένως $E^G \cong \mathbb{Q}$.

2. Έστω $E = \mathbb{Q}(2^{1/3})$, $G = \mathrm{Gal}(E/\mathbb{Q})$. Τότε $G = \{id_E\}$ και $E^G \cong E$.

3. Έστω $E = \mathbb{Q}(\omega, b)$ όπου $\omega = e^{2\pi i/3}$, $b = 2^{1/3}$, $G = \mathrm{Gal}(E/\mathbb{Q})$. Έστω $H = \langle \sigma_1 \rangle$, όπου $\sigma_1 : \ b \mapsto \omega b, \omega \mapsto \omega$. Θα δείξουμε ότι $E^H = \mathbb{Q}(\omega)$. Πράγματι είναι ξεκάθαρο ότι $\mathbb{Q}(\omega) \subset E^H$. Θεωρούμε τη $\mathbb{Q}$-βάση του E $\{1, \omega, b, b\omega, b^2, b^2\omega\}$. Κάθε στοιχείο a του E είναι γραμμικός συνδυασμός

$$a = a_0 + a_1\omega + a_2 b + a_3 b\omega + a_4 b^2 + a_5 b^2\omega, \ a_i \in \mathbb{Q} \ .$$

Τότε

$$\begin{aligned} \sigma_1(a) &= a_0 + a_1\omega + a_2\omega b + a_3 b\omega^2 + a_4 b^2\omega^2 + a_5 b^2\omega^3 \\ &= a_0 + a_1\omega + a_2 b + a_3 b(-\omega - 1) + a_4 b^2(-\omega - 1) + a_5 b^2 \\ &= a_0 + a_1\omega + (a_2 - a_3)b - a_3 b\omega + (a_5 - a_4)b^2 - a_4 b^2\omega \ . \end{aligned}$$

Επομένως

$$\sigma_1(a) = a \ \Leftrightarrow \ a_2 = a_3 = 0 = a_4 = a_5 \ .$$

Έτσι

$$E^H = \{a_0 + a_1\omega : \ a_i \in \mathbb{Q}\} = \mathbb{Q}(\omega) \ .$$

Το ίδιο συμπέρασμα προκύπτει και χωρίς αναλυτικούς υπολογισμούς παρατηρώντας ότι $[E : \mathbb{Q}(\omega)] = 3$ και άρα δεν υπάρχει ενδιάμεσο σώμα B έτσι ώστε $\mathbb{Q}(\omega) \subsetneq B \subsetneq E$. Αφού $\sigma(b) \neq b$ έπεται ότι $E^H \neq E$ και άρα $E^H = \mathbb{Q}(\omega)$.

Στην επόμενη ενότητα θα δούμε ότι αναγκαία και ικανή συνθήκη για να ισχύει η *δυική* σχέση

$$E^{\mathrm{Gal}(E/F)} = B$$

είναι E να είναι σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου $f(x) \in F[x]$.

3.5 Θεμελιώδες Θεώρημα Θεωρίας Galois

Θα λέμε ότι η επέκταση E/F είναι *επέκταση Galois* υπεράνω του F αν E είναι σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου $f(x) \in F[x]$.

Θεμελιώδες Θεώρημα της Θεωρίας Galois *Έστω E επέκταση Galois υπεράνω του F, $G = \mathrm{Gal}(E/F)$. Τότε υπάρχει μία αμφιμονότιμη αντιστοιχία ανάμεσα στα στοιχεία του συνόλου των ενδιάμεσων σωμάτων $\{B : \ F \subset B \subset E\}$ και στα στοιχεία του συνόλου των υποομάδων της G:*

$$B \mapsto \mathrm{Gal}(E/B)$$

Αντίστροφα αν H είναι υποομάδα της G τότε η αντιστοιχία

$$H \mapsto E^H$$

έχει τις εξής ιδιότητες:

- $[B : F] = [G : \mathrm{Gal}(E/B)]$ *και* $[G : H] = [E^H : F]$
- $E^{\mathrm{Gal}(E/B)} = B$ *και* $\mathrm{Gal}(E/E^H) = H$
- B *είναι επέκταση Galois πάνω από το F αν και μόνο αν* $\mathrm{Gal}(E/B) \triangleleft G$.

Έχουμε δει νωρίτερα κάποιες από τις συνεπαγωγές. Στη συνέχεια θα αποδείξουμε μία ειδική περίπτωση της δεύτερης ιδιότητας:

Θεώρημα 3.5.1. *Έστω E επέκταση Galois υπεράνω του F. Τότε*

$$E^{\mathrm{Gal}(E/F)} = F \ .$$

Απόδειξη. Έστω $G = \mathrm{Gal}(E/F) = \{\sigma_1 \ldots, \sigma_n\}$. Γνωρίζουμε ότι $|G| = [E : F]$ και ότι $F \subset E^G$. Έπεται ότι

$$E^G = F \Leftrightarrow [E^G : F] = 1 \Leftrightarrow [E : E^G] = n \ .$$

- Αν $G = \{\mathrm{id}_E\}$ τότε $E = F = E^G$ και δεν υπάρχει τίποτα να αποδείξουμε.
- Έστω λοιπόν ότι $n > 1$ και ότι $[E : E^G] = m < n$. Σημειώνουμε ότι $E \neq E^G$ αφού $|G| = [E : F] > 1$. Έστω $\{a_1, \ldots, a_m\}$ μία E^G-βάση του E. Έτσι κάθε στοιχείο $b \in E$ γράφεται ως E^G-γραμμικός συνδυασμός:

  $$b = c_1 a_1 + \cdots + c_m a_m = \sum c_i a_i, \ c_i \in E^G \ .$$

  Έπεται ότι αν $\sigma \in G$ τότε $\sigma(c_i) = c_i$ για $i = 1, \ldots, m$ και άρα $\sigma \in G$ είναι E^G γραμμική συνάρτηση:

  $$\sigma(b) = \sigma(\sum c_i a_i) = \sum c_1 \sigma(a_i) \ .$$

  Θεωρούμε το ομογενές σύστημα με m εξισώσεις και n αγνώστους στο E:

  $$\begin{aligned} \sigma_1(a_1)x_1 + \cdots + \sigma_n(a_1)x_n &= 0 \\ &\vdots \\ \sigma_1(a_m)x_1 + \cdots + \sigma_n(a_m)x_n &= 0 \end{aligned}$$

  Αφού $m < n$, το σύστημα έχει μία μη μηδενική λύση στο E: έστω $(y_1, \ldots, y_n) \neq 0$ μία τέτοια λύση. Δηλαδή για $i = 1, \ldots, m$ ισχύει ότι

  $$y_1\sigma_1(a_i) + \cdots + y_n\sigma_n(a_i) = 0 \ . \tag{3.1}$$

  Δεν είναι δύσκολο να δείξουμε ότι η αντίστοιχη σχέση ισχύει για κάθε $b \in E$, δηλαδή ότι

  $$y_1\sigma_1(b) + \cdots + y_n\sigma_n(b) = 0 \ . \tag{3.2}$$

  Πράγματι πολλαπλασιάζουμε την εξίσωση 3.1 με c_i και παρατηρούμε ότι $c_i\sigma_j(a_i) = \sigma_j(c_i)\sigma_i(a_i) = \sigma_j(c_i a_i)$. Για $i = 1, \ldots, m$ προκύπτει λοιπόν η εξίσωση

  $$\sum_j y_j \sigma_j(c_i a_i) = 0 \ .$$

Προσθέτοντας αυτές τις σχέσεις για $i = 1, \ldots, m$ προκύπτει ότι

$$\sum_i \sum_j y_j \sigma_j(c_i a_i) = \sum_j y_j \sigma_j(c_1 a_1 + \cdots + c_m a_m) = \sum_j y_j \sigma_j(b) = 0 \ .$$

Χωρίς περιορισμό της γενικότητας θα υποθέσουμε ότι $y_n \neq 0$. Αφού $\sigma_n \neq \sigma_1$, υπάρχει $c \in E \setminus E^G$ έτσι ώστε $\sigma_n(c) \neq \sigma_1(c)$. Παρατηρούμε ότι $c \neq 0$ και επομένως $\sigma_1(c)\sigma_n(c) \neq 0$.

Αντικαθιστούμε στη σχέση 3.2 στη θέση του b το στοιχείο bc. Έστω ότι $\sigma_i(c) = c_i$. Έπεται ότι

$$y_1 c_1 \sigma_1(b) + \cdots + y_n c_n \sigma_n(b) = 0. \tag{3.3}$$

Πολλαπλασιάζοντας την 3.2 με c_1 και αφαιρώντας από την 3.3 βρίσκουμε ότι

$$y_2(c_2 - c_1)\sigma_2(b) + \cdots + y_n(c_n - c_1)\sigma_n(b) = 0 \ . \tag{3.4}$$

Παρατηρούμε ότι ο συντελεστής του $\sigma_n(b)$ στη σχέση 3.4 είναι και πάλι διάφορος του μηδενός. Άρα υπάρχει $(z_2, \ldots, z_n)$ όπου $z_n \neq 0$ έτσι ώστε

$$\forall b \in E: \ z_2\sigma_2(b) + \cdots + z_n\sigma_n(b) = 0.$$

Επαναλαμβάνουμε αυτή τη διαδικασία άλλες $n-2$ φορές. Καταλήγουμε ότι υπάρχει μη μηδενικό $t \in E$ έτσι ώστε $t\sigma_n(b) = 0$, $\forall b \in E$. Άρα $\forall b \in E$, $\sigma_n(b) = 0$. Αυτό όμως είναι αδύνατο αφού σ_n είναι αυτομορφισμός του E.

□

Θα δείξουμε ότι ισχύει και το αντίστροφο του Θεωρήματος 3.5.1.

Θεώρημα 3.5.2. *Έστω $[E : F] < \infty$, $G = \mathrm{Gal}(E/F)$, $E^G = F$. Τότε E είναι το σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου υπεράνω του F.*

Απόδειξη. Θα δείξουμε ότι $E = F(a_1, \ldots, a_n)$ όπου a_i είναι ρίζες ενός διαχωρίσιμου πολυωνύμου.

- Αν $E = F$ τότε θέτοντας $f(x) = x$ παρατηρούμε ότι $f(x)$ είναι διαχωρίσιμο και ότι E είναι σώμα ανάλυσης του $f(x)$ πάνω από το F.
- Έστω τώρα $E \neq F$. Άρα υπάρχει $a_1 \in E \setminus F$. Αφού $[E : F] < \infty$, έπεται ότι a_1 είναι αλγεβρικό υπεράνω του F. Έστω $p_1(x) = \mathrm{irr}_{(F,a_1)}(x)$. Θα δείξουμε ότι οι ρίζες του $p_1(x)$ είναι απλές και ότι $p_1(x)$ είναι διαχωρίσιμο. Πράγματι έστω $X = \{\sigma(a_1) : \ \sigma \in G\}$. Τότε $|X| = n$ και έστω $X =$

$\{a_1, \ldots, a_n\}$. Σύμφωνα με τη Πρόταση 2.3.3 τα στοιχεία του X είναι ρίζες του $p_1(x)$. Θα δείξουμε ότι $p_1(x)$ είναι διαχωρίσιμο σε κάποιο σώμα ανάλυσης (άρα και σε κάθε σώμα ανάλυσης). Θεωρούμε το πολυώνυμο

$$g_1(x) = (x - a_1) \cdots (x - a_n) =$$
$$x^n - (a_1 + \cdots + a_n)x^{n-1} + (a_1a_2 + \cdots + a_{n-1}a_n)x^{n-2} + \cdots + (-1)^n a_1 \cdots a_n$$
$$= \sum c_j x^j \in E[x]$$

Παρατηρούμε ότι $\deg g_1(x) \leq \deg p_1(x)$ εκ κατασκευής. Θα δείξουμε ότι $g_1(x) = p_1(x)$. Πράγματι, οι συντελεστές c_j του x^j είναι εκφράσεις συμμετρικές ως προς τα a_i, $i = 1, \ldots, n$. Έπεται ότι αν $\sigma \in G$ τότε $\sigma(c_j) = c_j$. Άρα $c_j \in E^G$. Αφού $E^G = F$ έπεται ότι $g_1(x) \in F[x]$. Αφού $p_1(x) = \mathrm{irr}_{(F,a_1)}(x)$ και $g_1(a_1) = 0$ έπεται ότι $p_1 | g_1(x)$ στο $F[x]$ και άρα $\deg p_1(x) \leq \deg g_1(x)$. Έπεται ότι $g_1(x) = p_1(x)$, δηλ. $p_1(x)$ είναι διαχωρίσιμο. Άρα $F_1 = F(a_1, \ldots, a_n)$ είναι σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου. Αν $F_1 = E$ τότε το θεώρημα έχει αποδειχθεί. Σε διαφορετική περίπτωση $[E : F_1] < [E : F]$ και υπάρχει $b_1 \in E \setminus F_1$. Επαναλαμβάνουμε τη προηγούμενη διαδικασία και πέρνουμε το σώμα $F_2 = F_1(b1, \ldots, b_t) = F(b_1, \ldots, b_t)$. Συνεχίζουμε με τον ίδιο τρόπο. Παρατηρούμε ότι η διαδικασία αυτή θα σταματήσει όταν $[E : F_i] = 1$.

□

Θα απομονώσουμε ένα από τα συμπεράσματα της παραπάνω απόδειξης:

Πόρισμα 3.5.3. *Έστω E επέκταση Galois υπεράνω του F, $p(x) \in F[x]$ έτσι ώστε $p(b) = 0$ για κάποιο $b \in E$. Τότε $p(x)$ είναι διαχωρίσιμο και όλες οι ρίζες του ανήκουν στο E.*

Έπεται ότι αν E επέκταση Galois υπεράνω του F, $F \subset B \subset E$, B σώμα ανάλυσης του $g(x) \in F[x]$, τότε B είναι επίσης επέκταση Galois υπεράνω του F. Επίσης παρατηρούμε ότι με την απόδειξη του Θεωρήματος 3.3.1 δείξαμε ότι αν $F \subset B \subset E$ τότε B είναι επέκταση Galois υπεράνω του F αν και μόνο αν $\sigma(B) = B$ γιά κάθε $\sigma \in \mathrm{Gal}(E/F)$. Θέτουμε κάποια σχετικά ερωτήματα:

Ερωτήματα 3.5.4.

- Ποιές ομάδες μπορούμε να αναγνωρίσουμε ως ομάδες Galois μίας επέκτασης E υπεράνω ενός σώματος F (χωρίς περιορισμούς στα E, F);
- Ποιές ομάδες μπορούμε να αναγνωρίσουμε ως ομάδες Galois μίας επέκτασης E υπεράνω του $\mathbb{Q}$;

- Ποιά είναι η ιδιότητα που χαρακτηρίζει την ομάδα Galois ενός πολυωνύμου που μπορεί να επιλυθεί με ριζικά;

3.6 Παραδείγματα και Εφαρμογές

Παράδειγμα 3.6.1. Έστω E σώμα ανάλυσης του διαχωρίσιμου ανάγωγου πολυωνύμου $f(x) \in F[x]$, $G = \mathrm{Gal}(E/F)$. Έστω $\deg f(x) = n$ και $X = \{\omega_1, \ldots, \omega_n\}$ το σύνολο των ριζών του $f(x)$. Έστω

$$\Delta = (\omega_n - \omega_{n-1})(\omega_n - \omega_{n-1}) \cdots (\omega_2 - \omega_1) \ .$$

Αν $\sigma \in G$ τότε $\sigma(\Delta) = \pm\Delta$ και $\sigma(\Delta^2) = \Delta^2$. Έπεται ότι $\Delta^2 \in E^G = F$. Το στοιχείο Δ^2 ονομάζεται η *διακρίνουσα* του $f(x)$ και δεν εξαρτάται από την αρίθμηση των ριζών του $f(x)$. Έστω ότι $\Delta \notin F$. Τότε $B = F(\Delta)$ είναι σώμα ανάλυσης πάνω από το F του πολυωνύμου $x^2 - \Delta^2$. Έπεται ότι

$$2 = [F(\Delta) : F] = [G : \mathrm{Gal}(E/F(\Delta))]$$

και άρα

$$\mathrm{Gal}(E/F(\Delta)) \lhd G \ .$$

θα εφαρμόσουμε τα παραπάνω όταν $f(x)$ είναι ανάγωγο βαθμού 3.

Παράδειγμα 3.6.2. Έστω $f(x) \in F[x]$, $\deg f(x) = 3$, $f(x)$ ανάγωγο και διαχωρίσιμο. Αν E είναι το σώμα ανάλυσης του $f(x)$ πάνω από το F γνωρίζουμε ότι $\mathrm{Gal}(E/F)$ εμφυτεύτεται στο S_3 και θα έχει τάξη 3 ή 6. Αν $\Delta \notin F$ τότε 2 διαιρεί $|\mathrm{Gal}(E/F)|$ και άρα $\mathrm{Gal}(E/F) \cong S_3$. Έστω τώρα ότι $\Delta \in F$ και ότι οι ρίζες του $f(x)$ είναι οι $\omega_1, \omega_2, \omega_3$. Αφού

$$\Delta = (\omega_3 - \omega_2)(\omega_3 - \omega_1)(\omega_2 - \omega_1)$$

έπεται ότι δεν υπάρχει στην G αυτομορφισμός που θα αντιμεταθέσει δύο από τις ρίζες του $f(x)$. Έπεται ότι τα στοιχεία της G έχουν τάξη 1 ή 3 και άρα $G \cong A_3 \cong \mathbb{Z}_3$.

Μπορεί κανείς να δείξει ότι αν $f(x) = x^3 + px + q$ τότε $\Delta^2 = -4p^3 - 27q^2$. Έτσι αν $f(x) = x^3 - 3x - 1$ έπεται ότι $\Delta \in \mathbb{Q}$. Αν E είναι το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$, έπεται ότι $\mathrm{Gal}(E/\mathbb{Q}) \cong A_3$.

Πρόταση 3.6.3. *Έστω E επέκταση Galois υπεράνω του F. Υπάρχει πεπερασμένος αριθμός ενδιάμεσων σωμάτων $F \subset B \subset E$.*

Απόδειξη. Η ομάδα $\mathrm{Gal}(E/F)$ είναι πεπερασμένη και έχει πεπερασμένο αριθμό υποομάδων. □

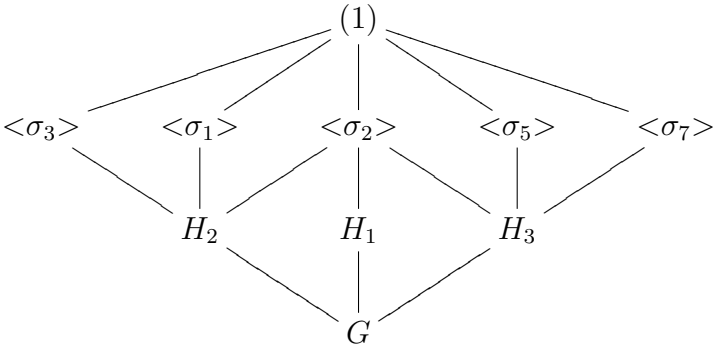
Παράδειγμα 3.6.4. Έστω $f(x) = x^4 - 2 \in \mathbb{Q}$ και $E \subset \mathbb{C}$ σώμα ανάλυσης του $f(x)$. Θέτουμε $b = 2^{1/4}$. Οι ρίζες του $f(x)$ είναι $\{\pm b, \pm ib\}$ και $E = \mathbb{Q}(b, i)$. Έστω $G = \mathrm{Gal}(E/\mathbb{Q})$. Έχουμε δει ότι $G \cong D_8$ και ότι τα στοιχεία της G είναι:

b	b	b	$-b$	$-b$	ib	ib	$-ib$	$-ib$
i	i	$-i$	i	$-i$	i	$-i$	i	$-i$
	id_E	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7

Οι γνήσιες μη τετριμμένες υποομάδες της G είναι:

- $H_1 = <\sigma_4> = \{\sigma_0, \sigma_4, \sigma_2 = \sigma_4^2, \sigma_6 = \sigma_4^3\}$
- $H_2 = \{\sigma_0, \sigma_2, \sigma_1, \sigma_3\}$
- $H_3 = \{\sigma_0, \sigma_2, \sigma_5, \sigma_7\}$
- $<\sigma_3> = \{\mathrm{id_E}, \sigma_3\}$
- $<\sigma_1> = \{\mathrm{id_E}, \sigma_1\}$
- $<\sigma_2>\{\mathrm{id_E}, \sigma_2\}$
- $<\sigma_5> = \{\mathrm{id_E}, \sigma_5\}$
- $<\sigma_7> = \{\mathrm{id_E}, \sigma_7\}$

Το διάγραμμα λοιπόν των υποομάδων της G είναι:



Υπάρχει μόνο μία κανονική υποομάδα τάξης 2, η ομάδα $<\sigma_2>$, ενώ και οι 3 υποοομάδες τάξης 4 είναι κανονικές. Θα υπολογίσουμε τα ενδιάμεσα σώματα σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois. Θα ξεκινήσουμε με την ομάδα $<\sigma_5>$. Μία βάση του E ως προς το $\mathbb{Q}$ είναι το σύνολο $\{1, b, b^2, b^3, i, ib, ib^2, ib^3\}$. Επομένως ένα τυχαίο στοιχείο y του E είναι κάποιος γραμμικός συνδυασμός

$$y = a_0 + a_1 b + a_2 b^2 + a_3 b^3 + a_4 i + a_5 ib + a_6 ib^2 + a_7 ib^3,$$

όπου $a_i \in \mathbb{Q}$. Έπεται ότι

$$\sigma_5(y) = a_0 + a_1 ib - a_2 b^2 - ia_3 b^3 - a_4 i + a_5 b + a_6 ib^2 - a_7 b^3$$

Θα ισχύει $\sigma_5(y) = y$ αν και μόνο αν

$$a_1 = a_5, a_2 = 0, a_3 = -a_7, a_4 = 0,$$

και

$$y = a_0 + a_1 b(1+i) + a_3 b^3(1-i) + a_6 ib^2.$$

Άρα

$$E^{<\sigma_5>} = \mathbb{Q}(b(1+i), b^3(1-i), ib^2),$$

και αφού $(b(1+i))^2 = 2ib^2$, $(b(1+i))^3 = -2b^3(1-i)$, έχουμε ότι

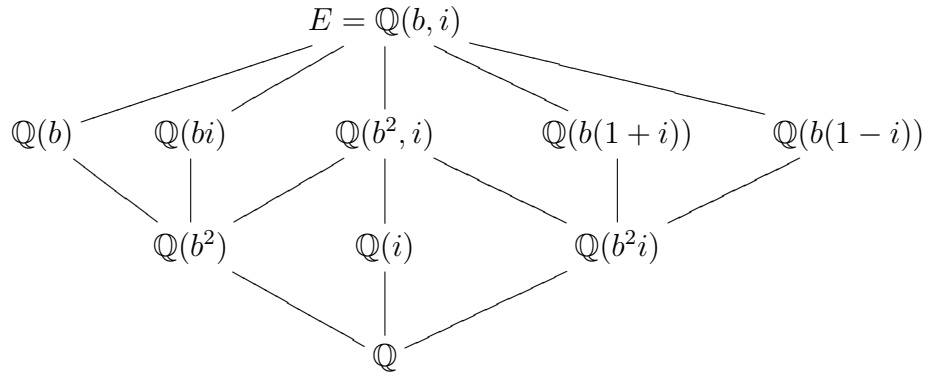
$$E^{<\sigma_5>} = \mathbb{Q}(b(1+i)).$$

Στη συνέχεια θα βρούμε το σώμα $E^{<\sigma_2>}$. Στη περίπτωση αυτή παρατηρούμε ότι $[G : <\sigma_2>] = 4$. Αφού $\sigma_2(i) = i$ και $\sigma_2(b^2) = \sigma_2(b)^2 = (-b)^2 = b^2$ έπεται ότι $\mathbb{Q}(b^2, i) \subset E^{<\sigma_2>}$. Αφού

$$\mathbb{Q} \subsetneq \mathbb{Q}(i) \subsetneq \mathbb{Q}(i, b^2) \subsetneq E$$

έπεται ότι $[\mathbb{Q}(i, b^2) : \mathbb{Q}] = 4$. Επομένως $E^{<\sigma_2>} = \mathbb{Q}(i, b^2)$. Με αυτές τις τεχνικές βρίσκουμε και τα άλλα ενδιάμεσα σώματα του E.

Έτσι έχουμε το παρακάτω διάγραμμα για τα ενδιάμεσα σώματα:



Τέλος παρατηρούμε ότι στις κανονικές υποομάδες της G αντιστοιχούν τα εξής σώματα ανάλυσης υπεράνω του $\mathbb{Q}$:

- $\mathbb{Q}(b^2)$ είναι το σώμα ανάλυσης του $x^2 - b$ υπεράνω του $\mathbb{Q}$
- $\mathbb{Q}(i)$ είναι το σώμα ανάλυσης του $x^2 + 1$ υπεράνω του $\mathbb{Q}$,
- $\mathbb{Q}(b^2 i)$ είναι το σώμα ανάλυσης του $x^2 + 2$ υπεράνω του $\mathbb{Q}$,
- $\mathbb{Q}(b^2, i)$ είναι το σώμα ανάλυσης του $(x^2 - b)(x^2 + 1)$ υπεράνω του $\mathbb{Q}$.

3.7 Ασκήσεις

1. Για κάθε μία από τις παρακάτω περιπτώσεις να δώσετε ένα παράδειγμα επεκτάσεων $\mathbb{Q} \subsetneqq B \subsetneqq E$ ή να εξηγήσετε γιατί είναι αδύνατον να συμβεί:

   - E επέκταση Galois υπεράνω του $\mathbb{B}$, B επέκταση Galois υπεράνω του $\mathbb{Q}$ αλλά E να μην είναι επέκταση Galois υπεράνω του $\mathbb{Q}$,
   - E όχι επέκταση Galois υπεράνω του B, B επέκταση Galois υπεράνω του $\mathbb{Q}$ και E επέκταση Galois υπεράνω του $\mathbb{Q}$,
   - E επέκταση Galois υπεράνω του B, B να μην είναι επέκταση Galois υπεράνω του $\mathbb{Q}$ και E να είναι επέκταση Galois υπεράνω του $\mathbb{Q}$.

2. Έστω $f(x)$ το πολυώνυμο $f(x) = x^4 - 4 \in \mathbb{Q}[x]$, E το σώμα ανάλυσης του $f(x)$ υπεράνω του $\mathbb{Q}$ και $G = \mathrm{Gal}(E/\mathbb{Q})$.

   - Να υπολογίσετε το E.
   - Να γράψετε τα στοιχεία της G ως στοιχεία του S_4.
   - Να αποδείξετε ότι $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
   - Για τα υποσώματα $B_1 = \mathbb{Q}(i\sqrt{2})$, $B_2 = \mathbb{Q}(i)$, $B_3 = \mathbb{Q}(\sqrt{2})$ του E, να βρείτε τις υποομάδες $\mathrm{Gal}(E/B_1)$ $\mathrm{Gal}(E/B_2)$ $\mathrm{Gal}(E/B_3)$ της G.
   - Έστω $a = \sqrt{2} + i$. Να υπολογίσετε την εικόνα του a, για κάθε έναν από τους αυτομορφισμούς του E. Να αποδείξετε ότι $E = \mathbb{Q}(a)$.
   - Να γράψετε το στοιχείο a^{-1} ως γραμμικό συνδυασμό δυνάμεων του a.

3. Έστω $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

   - Να αποδείξετε ότι E είναι επέκταση Galois υπεράνω του $\mathbb{Q}$, να υπολογίσετε τον βαθμό $[E : \mathbb{Q}]$, και να βρείτε μία βάση του E υπεράνω του $\mathbb{Q}$.
   - Να περιγράψετε τα στοιχεία της ομάδας $G = \mathrm{Gal}(E/\mathbb{Q})$.
   - Να βρείτε όλα τα ενδιάμεσα σώματα B του E υπεράνω του $\mathbb{Q}$ και να υπολογίσετε τις ομάδες $\mathrm{Gal}(B/\mathbb{Q})$ και $\mathrm{Gal}(E/B)$.
   - Να βρείτε ανάγωγο πολυώνυμο $f(x)$ έτσι ώστε E να είναι σώμα ανάλυσης του $f(x)$ υπεράνω του $\mathbb{Q}$.

4. Έστω $E = \mathbb{Q}(\omega, \sqrt[5]{3})$ και $G = \mathrm{Gal}(E/\mathbb{Q})$, όπου $\omega = e^{2\pi i/5}$.

- Να βρείτε πολυώνυμο $f(x) \in \mathbb{Q}[x]$ έτσι ώστε E να είναι το σώμα ανάλυσης του $f(x)$, και να υπολογίσετε τον βαθμό $[E : \mathbb{Q}]$.
- Να αποδείξετε ότι η G εμφυτεύεται στην S_5 και ότι $G \ncong S_5$.
- Να βρείτε τα στοιχεία της $G_1 = \mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{3}))$. Να υπολογίσετε $\sigma(a)$ όπου a τυχαίο στοιχείο της E και $\sigma \in G_1$, $\sigma \neq id_E$, (για ένα μόνο τέτοιο στοιχείο). Να δείξετε ότι η G_1 είναι κυκλική ομάδα.
- Να βρείτε τα στοιχεία της $G_2 = \mathrm{Gal}(E/\mathbb{Q}(\omega))$. Να δείξετε ότι η G_2 είναι κυκλική ομάδα. Να υπολογίσετε $\sigma(a)$ όπου a τυχαίο στοιχείο της E και $\sigma \in G_2$, $\sigma \neq id_E$, (για ένα μόνο τέτοιο στοιχείο).
- Να βρείτε δύο στοιχεία της ομάδας $G = \mathrm{Gal}(E/\mathbb{Q})$ που δεν αντιμετατίθενται.

5. Έστω $E = \mathbb{Q}(\omega)$, όπου $\omega = e^{2\pi i/5}$.
   - Να δείξετε ότι E είναι επέκταση Galois υπεράνω του $\mathbb{Q}$ και να βρείτε τον βαθμό $[E : \mathbb{Q}]$.
   - Έστω $G = \mathrm{Gal}(E/\mathbb{Q})$. Να αποδείξετε ότι η G είναι κυκλική ομάδα.
   - Να βρείτε όλα τα ενδιάμεσα σώματα του E.
6. Έστω $|E| = 2^8$, $G = \mathrm{Gal}(E/\mathbb{Z}_2)$.
   - Να δείξετε αναλυτικά ότι η συνάρτηση $\sigma : E \to E$, $\sigma(b) = b^2$ είναι αυτομορφισμός του E και $\sigma \in G$.
   - Να δείξετε αναλυτικά ότι η τάξη του σ είναι 8 και επομένως $G = \langle\sigma\rangle \cong Z_8$.
7. Έστω E επέκταση Galois του F, $a \in E$, $G = \mathrm{Gal}(E/F)$. Να αποδείξετε ότι $N(a) \in F$ όπου
$$N(a) = \prod_{\sigma \in G} \sigma(a) \ .$$