Θεωρία Galois

Θεοδώρα Θεοχαρη-Αποστολιδη

Χαρά Χαραλαμπους

Οι σημειωσεις αυτες θα συμπληρωνονται κατα τη διαρκεια των μαθηματων.

11 Νοεμβρίου 2014

Περιεχόμενα

Κεφάλαιο 2

Σώματα και βαθμοί επεκτάσεων

Έστω $F/\ \Bbbk$ επέκταση σωμάτων. Το σώμα F έχει την πρόσθετη δομή του $\Bbbk$-διανυσματικού χώρου, με τη πράξη του σκαλιανού πολλαπλασιασμού να είναι ο συνήθης πολλαπλασιασμός: $\Bbbk \times F \to F$, $(c, f(x)) \mapsto cf(x)$. Θα χρησιμοποιήσουμε αυτή τη δομή για να καταλάβουμε καλύτερα το F.

2.1 Αλγεβρικά στοιχεία πάνω από ένα σώμα.

Ορισμός 2.1.1. *Έστω $F/\ \Bbbk$ επέκταση σωμάτων και $a \in F$. Το a είναι αλγεβρικό πάνω από το $\Bbbk$ αν υπάρχει $f(x) \in \Bbbk[x]$, έτσι ώστε $f(x) \neq 0$ και $f(a) = 0$. Αν το a δεν είναι αλγεβρικό πάνω από το $\Bbbk$, τότε το a λέγεται υπερβατικό πάνω από το $\Bbbk$.*

Τονίζουμε ότι όταν $f(x) \in \Bbbk[x]$ τότε $f(x) \in F[x]$.

Παραδείγματα 2.1.2.

- Αν $a \in F$, τότε το a είναι αλγεβρικό πάνω από το F αφού είναι ρίζα του $f(x) = x - a \in F[x]$.
- Το $a = \sqrt{3} \in \mathbb{R}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$, αφού a είναι ρίζα του $f(x) = x^2 - 3 \in \mathbb{Q}[x]$.
- Όπως είδαμε στο προηγούμενο κεφάλαιο $\mathbb{Q}[y]/(y^2 - 3)$ είναι επέκταση του $\mathbb{Q}$ και το $a = y + (y^2 - 3)$ είναι ρίζα του πολυωνύμου $x^2 - 3$. Άρα το a είναι αλγεβρικό πάνω από το $\mathbb{Q}$.

- Έστω $f(x) \in \Bbbk[x]$ ένα ανάγωγο πολυώνυμο, $I = (f(x))$ και $F = \Bbbk[x]/I$. Το στοιχείο $x + I \in F$ είναι αλγεβρικό πάνω από το $\Bbbk$, βλ. Θεώρημα ;;.

- Αν $\Bbbk \subset F \subset E$ είναι εγκλεισμός σωμάτων και $a \in E$ είναι αλγεβρικό πάνω από το $\Bbbk$ τότε a είναι αλγεβρικό πάνω από το F.

- Το στοιχείο $i \in \mathbb{C}$ είναι αλγεβρικό πάνω από το $\mathbb{R}$ και του $\mathbb{Q}$.

- Έστω $z = a+bi \in \mathbb{C}$, $a, b \in \mathbb{R}$. Τότε $z-a = bi$ και $z^2-2az+a^2 = -b^2$. Άρα το z είναι ρίζα του πολυωνύμου $x^2-2ax+(a^2+b^2) \in \mathbb{R}[x]$. Επομένως κάθε στοιχείο του $\mathbb{C}$ είναι αλγεβρικό πάνω από το $\mathbb{R}$.

- Τα $a = \sqrt{2}$ και $b = \sqrt{3} \in \mathbb{R}$ είναι αλγεβρικά πάνω από το $\mathbb{Q}$ αφού είναι ρίζες αντίστοιχα των πολυωνύμων $x^2 - 2$ και $x^2 - 3 \in \mathbb{Q}[x]$. Το γινόμενο $a \cdot b = \sqrt{6}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$ αφού είναι ρίζα του πολυωνύμου $x^2 - 6 \in \mathbb{Q}[x]$.

- Το άθροισμα $a+b = \sqrt{2}+\sqrt{3}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$. Πράγματι έστω $c = a + b = \sqrt{2} + \sqrt{3}$. Τότε $c^2 = 5 + 2\sqrt{6}$, άρα $c^2 - 5 = 2\sqrt{6}$. Άρα $(c^2 - 5)^2 = 24$ και $c^4 - 10c + 1 = 0$. Έπεται ότι c είναι ρίζα του πολυωνύμου $f(x) = x^4 - 10x + 1$. Στην επόμενη ενότητα, Παράδειγμα 2.2.12 θα δούμε ότι $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ χρησιμοποιώντας τις διαστάσεις κατάλληλων διανυσματικών χώρων.

- Το $\pi \in \mathbb{R}$ είναι υπερβατικό πάνω από το $\mathbb{Q}$. Η απόδειξη της υπερβατικότητας ενός στοιχείου συνήθως είναι ιδιαίτερα δύσκολη. Η απόδειξη για τον αριθμό π δόθηκε από τον Lindemann το 1882 και στηρίζεται στο ότι ο αριθμός e είναι επίσης υπερβατικός πάνω από το $\mathbb{Q}$, όπως έδειξε ο Hermite το 1873, ενώ $e^{i\pi} = -1$.

- Έστω $E = \Bbbk(x)$ το σώμα κλασμάτων του δακτυλίου $\Bbbk[x]$. Τότε το $x \in E$ είναι υπερβατικό πάνω από το $\Bbbk$.

Έστω ότι $F/\ \Bbbk$ επέκταση σωμάτων και $a \in F$. Για να καταλάβουμε αν το a είναι αλγεβρικό ή υπερβατικό πάνω από το $\Bbbk$ θα μελετήσουμε τον μικρότερο δακτύλιο που περιέχει το $\Bbbk$ και το a.

Ορισμός 2.1.3. *Έστω $F/\ \Bbbk$ επέκταση σωμάτων και $a \in F$. Ορίζουμε $\Bbbk[a] = \{f(a) : f(x) \in \Bbbk[x]\}$, ενώ $\Bbbk(a) = \{f(a)/g(a) : g(a) \neq 0, f(x), g(x) \in \Bbbk[x]\}$.*

Δεν είναι δύσκολο να δείξει κανείς ότι το σύνολο $\Bbbk[a]$ είναι ο μικρότερος δακτύλιος που περιέχει το $\Bbbk$ και το a, ενώ το σύνολο $\Bbbk(a)$ είναι το μικρότερο σώμα που περιέχει το $\Bbbk$ και το a. Έτσι $\Bbbk \subset \Bbbk[a] \subset \Bbbk(a) \subset F$ και $\Bbbk(a)$ είναι το σώμα των κλασμάτων της ακεραίας περιοχής $\Bbbk[a]$. Το σώμα $\Bbbk(a)$ λέγεται

απλή επέκταση του $\Bbbk$. Για να δείξουμε ότι το $\Bbbk[a]$ περιέχεται σε έναν δακτύλιο E αρκεί να δείξουμε ότι $\Bbbk \subset E$ και ότι $a \in E$. Αντίστοιχα για να δείξουμε ότι $\Bbbk(a)$ περιέχεται σε ένα σώμα E αρκεί και πάλι να δείξουμε ότι $\Bbbk \subset E$ και ότι $a \in E$.

Παραδείγματα 2.1.4.

- Αφού $i^{2l} = \pm 1$ ενώ $i^{2l+1} = \pm i$, για $l \in \mathbb{N}$, έπεται ότι για τυχαίο $f(x) \in \mathbb{R}[x]$ ισχύει ότι $f(i) = a + bi$, όπου $a, b \in \mathbb{R}$. Άρα $\mathbb{R}[i] = \{a + bi : \ a, b \in \mathbb{R}\} = \mathbb{C}$. Δηλαδή ισχύει ότι $\mathbb{R}[i] = \mathbb{R}(i) = \mathbb{C}$. Μία $\mathbb{R}$-βάση του $\mathbb{R}[i]$ είναι το σύνολο $\{1, i\}$ και $\dim_{\mathbb{R}} \mathbb{R}[i] = 2$.

- Αφού $\sqrt{3}^{2l} = 3^l$ ενώ $\sqrt{3}^{2l+1} = 3^l\sqrt{3}$, για $l \in \mathbb{N}$, έπεται ότι

$$\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : \ a, b \in \mathbb{Q}\} \ .$$

  Παρατηρούμε ότι αν κάποιο από τα $a, b \in \mathbb{Q}$ είναι διάφορο του μηδενός, τότε $0 \neq a^2 - 3b^2 \in \mathbb{Q}$ και θέτοντας $c = a^2 - 3b^2$ βλέπουμε ότι

$$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} \ = \frac{a}{c} - \frac{b}{c}\sqrt{3} \ \in \mathbb{Q}[\sqrt{3}] \ .$$

  Άρα $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}[\sqrt{3}]$ και $\mathbb{Q}[\sqrt{3}] = \mathbb{Q}(\sqrt{3})$. Μία $\mathbb{Q}$-βάση του $\mathbb{Q}[\sqrt{3}]$ είναι το σύνολο $\{1, \sqrt{3}\}$ και $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}] = 2$.

- Θα μελετήσουμε τον δακτύλιο $\mathbb{Q}[\sqrt[3]{2}]$. Έστω ότι $m \in \mathbb{N}$. Τότε $m = 3l + k$, όπου $k, l \in \mathbb{N}$ και $l \leq 2$. Αφού

$$(\sqrt[3]{2})^m = (\sqrt[3]{2})^{3l+k} = 2^l(\sqrt[3]{2})^k$$

  έπεται ότι για τυχαίο $f(x) = \sum c_i x^i \in \mathbb{Q}[x]$ ισχύει ότι

$$f(\sqrt[3]{2}) = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2 : \quad a_i \in \mathbb{Q} \ .$$

  Άρα $\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} : \ a_i \in \mathbb{Q}\}$. Το σύνολο $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ παράγει το $\mathbb{Q}[\sqrt[3]{2}]$ ως $\mathbb{Q}$-διανυσματικό χώρο και άρα $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}] \leq 3$. Στην επόμενη ενότητα θα δούμε ότι $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}] = 3$.

- Έστω $E_1 = \mathbb{Q}[\sqrt{2}]$, $E_2 = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Θα δείξουμε ότι $E_1 \subsetneqq E_2$. Πράγματι

$$-\sqrt{2} + \sqrt{3} = \frac{1}{\sqrt{2} + \sqrt{3}} \in E_2 \ ,$$

  και

$$\sqrt{2} = \frac{(\sqrt{2} + \sqrt{3}) - (-\sqrt{2} + \sqrt{3})}{2} \in E_2 \ .$$

Άρα $E_1 \subset E_2$. Για να δείξουμε ότι $E_2 \neq E_1$ αρκεί να δείξουμε ότι $\sqrt{2}+\sqrt{3} \notin E_1$. Πράγματι αν συνέβαινε το αντίθετο τότε $\sqrt{3} = (\sqrt{2}+\sqrt{3}) - (\sqrt{2}) \in E_1$. Αφού μία $\mathbb{Q}$-βάση του E_1 είναι το σύνολο $\{1, \sqrt{2}\}$ έπεται ότι $\sqrt{3} = a+b\sqrt{2}$, $a, b \in \mathbb{Q}$. Υψώνοντας στο τετράγωνο προκύπτει ότι $3 = a^2+2b^2+2ab\sqrt{2}$, το οποίο εύκολα οδηγεί σε άτοπο αφού $\sqrt{2} \notin \mathbb{Q}$.

- Έστω p πρώτος, $\omega = e^{2\pi i/p}$, και $k \in \mathbb{N}$ έτσι ώστε $\text{ΜΚΔ}(k,p) = 1$. Θα δείξουμε ότι $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^k]$. Ο εγκλεισμός $\mathbb{Q}[\omega^k] \subset \mathbb{Q}[\omega]$ είναι εμφανής αφού $\omega^k \in \mathbb{Q}[\omega]$. Για τον αντίστροφο εγκλεισμό παρατηρούμε ότι υπάρχουν $r, t \in \mathbb{Z}$ έτσι ώστε $rp+tk = 1$. Έπεται ότι $\omega = \omega^{rp+tk} = \omega^{rp}\,\omega^{tk} = \omega^{k^t} \in \mathbb{Q}[\omega^k]$.

Έστω $F/\Bbbk$ επέκταση σωμάτων και $a \in F$. Εύκολα μπορεί να ελεγχθεί ότι

$$\phi : \Bbbk[x] \to \Bbbk[a] \ , \quad \phi(h(x)) = h(a)$$

είναι επιμορφισμός δακτυλίων. Παρατηρούμε ότι $\phi(c) = c$ όταν $c \in \Bbbk$ ενώ $\phi(x) = a$. Έχουμε ακόμα ότι $\ker\phi = \{f(x) \in \Bbbk[x] : \ f(a) = 0\}$. Σύμφωνα με το Πρώτο Θεώρημα Ισομορφίας προκύπτει ότι $\Bbbk[x]/\ker\phi \cong \text{Im}\,\phi = \Bbbk[a]$. Εφόσον $\Bbbk[a]$ είναι ακεραία περιοχή έπεται ότι $\ker\phi$ είναι πρώτο ιδεώδες.

Πρόταση 2.1.5. *Έστω $F/\Bbbk$ επέκταση σωμάτων και έστω $a \in F$. Το a είναι αλγεβρικό πάνω από το $\Bbbk$ αν και μόνο αν $\Bbbk[a] = \Bbbk(a)$. Όταν το a είναι υπερβατικό πάνω από το $\Bbbk$ τότε $\dim_{\Bbbk}\Bbbk[a] = \infty$.*

Απόδειξη. Έστω ότι a είναι αλγεβρικό πάνω από το $\Bbbk$. Τότε υπάρχει $f(x) \in \Bbbk[x]$ έτσι ώστε $f(a) = 0$ και $\ker\phi \neq 0$. Έπεται ότι $\ker\phi$ είναι μέγιστο και άρα ο δακτύλιος $\Bbbk[a] \cong \Bbbk[x]/\ker\phi$ είναι σώμα. Αφού $\Bbbk[a] \subset \Bbbk(a)$ και $\Bbbk(a)$ είναι το μικρότερο σώμα που περιέχει το $\Bbbk$ και το a, έπεται ότι $\Bbbk[a] = \Bbbk(a)$. Αν το a είναι υπερβατικό πάνω από το $\Bbbk$, τότε $\ker\phi = 0$ και $\Bbbk[a] \cong \Bbbk[x]$. Έπεται ότι ο δακτύλιος $\Bbbk[a]$ δεν είναι σώμα και ότι $\dim_{\Bbbk}\Bbbk[a] = \infty$. □

Στην επόμενη ενότητα θα υπολογίσουμε τη διάσταση του $\Bbbk$-διανυσματικού χώρου $\Bbbk[a]$ όταν το a είναι αλγεβρικό. Θα κλείσουμε με έναν τελευταίο ορισμό.

Ορισμός 2.1.6. *Έστω $F/\Bbbk$ επέκταση σωμάτων. Ο βαθμός του F πάνω από το $\Bbbk$ συμβολίζεται με $[F : \Bbbk]$ και ισούται με τη διάσταση του F ως $\Bbbk$-διανυσματικού χώρου.*

Παραδείγματα 2.1.7.

- $[\mathbb{C} : \mathbb{R}] = 2$.
- $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$.
- $[\Bbbk(x) : \Bbbk] = \infty$.
- $[\mathbb{Q}[\pi] : \Bbbk] = \infty$.
- Παρατηρούμε ότι $\mathbb{Q}[\pi] \subset \mathbb{R}$. Και οι δύο δακτύλιοι είναι $\mathbb{Q}$-διανυσματικοί χώροι και μάλιστα ο δακτύλιος $\mathbb{Q}[\pi]$ είναι $\mathbb{Q}$-υποχώρος του $\mathbb{R}$. Γνωρίζουμε ότι η $\mathbb{Q}$-διάσταση $\dim_{\mathbb{Q}}\mathbb{Q}[\pi]$ είναι κατανάγκη μικρότερη ή ίση με τη $\mathbb{Q}$-διάσταση του $\mathbb{R}$. Αφού $\dim_{\mathbb{Q}}\mathbb{Q}[\pi] = \infty$ έπεται ότι $[\mathbb{R} : \mathbb{Q}] = \infty$.
- Αν $\Bbbk \subset F \subset E$ είναι εγκλεισμός σωμάτων και $[F : \Bbbk] = \infty$ τότε $[E : \Bbbk] = \infty$.

2.2 Αλγεβρικά στοιχεία και διάσταση

Έστω $F/\Bbbk$ επέκταση σωμάτων και $a \in F$ αλγεβρικό πάνω από το $\Bbbk$. Θα ξεκινήσουμε με κάποιες παρατηρήσεις.

1. Στη προηγούμενη ενότητα είδαμε ότι $\Bbbk[a] = \Bbbk(a)$ και ότι το σύνολο $I = \{f(x) : \ f(a) = 0\}$ είναι πρώτο ιδεώδες του $\Bbbk[x]$.
2. Αφού το I είναι πρώτο ιδεώδες, σύμφωνα με τις Παρατηρήσεις **;;** έπεται ότι $I = (g(x))$ όπου $g(x)$ είναι ανάγωγο πολυώνυμο του $\Bbbk[x]$.
3. Άρα αν $h(x) \in I$, δηλαδή αν $h(a) = 0$, τότε $h(x) = q(x)g(x)$ και στη περίπτωση που $h(x) \neq 0$ τότε $\deg h(x) \geq \deg g(x)$.
4. Επεται ότι αν $h(x) \in \Bbbk[x]$ είναι ανάγωγο και $h(a) = 0$ τότε $h(x) = cg(x)$ όπου $c \in \Bbbk[x]$.

Οι παραπάνω παρατηρήσεις οδηγούν στον επόμενο ορισμό.

Ορισμός 2.2.1. *Έστω $F/\Bbbk$ επέκταση σωμάτων, $a \in F$ αλγεβρικό πάνω από το $\Bbbk[x]$. Το μοναδικό κανονικό ανάγωγο πολυώνυμο του $\Bbbk[x]$ που έχει το a ως ρίζα ονομάζεται το ανάγωγο πολυώνυμο του a πάνω από το $\Bbbk$ και συμβολίζεται με* $\mathrm{irr}_{(\Bbbk,a)}(x)$.

Παραδείγματα 2.2.2.

- Έστω $a \in F$. Τότε $\mathrm{irr}_{(F,a)}(x) = x - a$.
- Έστω $a = \sqrt{3} \in \mathbb{R}$. Τότε $\mathrm{irr}_{(\mathbb{Q},a)}(x) = x^2 - 3$.
- Έστω p πρώτος και $\omega = e^{2\pi i/p} \in \mathbb{C}$. Τότε $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = \Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$.

Στη συνέχεια εξετάζουμε τη διάσταση του $\Bbbk[a]$ ως $\Bbbk[x]$-διανυσματικού χώρου.

Θεώρημα 2.2.3. *Έστω $F/\Bbbk$ επέκταση σωμάτων, $a \in F$ αλγεβρικό πάνω από το $\Bbbk$, $\deg \mathrm{irr}_{(\Bbbk,a)}(x) = n$. Το σύνολο $\{1, a, \ldots, a^{n-1}\}$ αποτελεί βάση του $\Bbbk$-διανυσματικού χώρου $\Bbbk[a]$.*

Απόδειξη. Θέτουμε $f(x) = \mathrm{irr}_{(\Bbbk,a)}(x)$ και $B = \{1, a, \ldots, a^{n-1}\}$. Έστω $g(a)$ τυχαίο στοιχείο του $\Bbbk[a]$ όπου $g(x) \in \Bbbk[x]$. Σύμφωνα με τον Ευκλείδειο αλγόριθμο $g(x) = f(x)p(x) + r(x)$ όπου $p(x), r(x) \in \Bbbk[x]$, και $t = \deg r(x) < n$. Δηλαδή $r(x) = c_t x^t + \cdots + c_1 x + c_0$ και $c_i \in \Bbbk$ για $i = 0, \ldots, t$. Παρατηρούμε ότι $g(a) = f(a)p(a) + r(a) = r(a) = c_t a^t + \cdots + c_1 a + c_0 \cdot 1$ και ότι $g(a)$ είναι $\Bbbk$-γραμμικός συνδυασμός στοιχείων του συνόλου B. Θα δείξουμε ότι το σύνολο B είναι γραμμικά ανεξάρτητο. Έστω $d_0 \cdot 1 + \cdots + d_{n-1}a^{n-1} = 0$, $d_i \in \Bbbk$ για $i = 0, \ldots, n-1$ μία σχέση γραμμικής εξάρτησης των a^i : $0 \leq i \leq n-1$. Αν $g(x) = d_0 + d_1 x + \cdots + d_{n-1}x^{n-1}$, τότε $g(a) = 0$ και $g(x) \in (f(x))$. Αν $g(x) \neq 0$, αυτό οδηγεί σε άτοπο αφού $\deg g(x) < \deg f(x)$. Άρα ότι $g(x) = 0$ και άρα $d_i = 0$ για $i = 0, \ldots, n-1$. □

Η απόδειξη του παρακάτω πορίσματος είναι άμεση:

Πόρισμα 2.2.4. *Έστω $F/\Bbbk$ επέκταση σωμάτων, $a \in F$. Τότε το a είναι αλγεβρικό πάνω από το $\Bbbk$ αν και μόνο αν $[\Bbbk[a] : \Bbbk] < \infty$.*

Παράδειγμα 2.2.5. Αφού $x^3 - 2$ είναι ανάγωγο στο $\mathbb{Q}[x]$ έπεται ότι $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

Ορισμός 2.2.6. *Έστω $F/\Bbbk$ επέκταση σωμάτων. Το F λέγεται αλγεβρικό πάνω από το F αν κάθε στοιχείο του F είναι αλγεβρικό πάνω από το $\Bbbk$.*

Παράδειγμα 2.2.7. Το σώμα $\mathbb{C}$ είναι αλγεβρικό πάνω από το $\mathbb{R}$. Το σώμα $\mathbb{R}$ δεν είναι αλγεβρικό πάνω από το $\mathbb{Q}$.

Πρόταση 2.2.8. *Έστω $F/\Bbbk$ επέκταση σωμάτων έτσι ώστε $[F : \Bbbk] < \infty$. Τότε F είναι αλγεβρικό πάνω από το $\Bbbk$.*

Απόδειξη. Έστω ότι $[F : \Bbbk] = n$ και ότι a τυχαίο στοιχείο του F. Το σύνολο $\{1, a, \ldots, a^n\}$ έχει $n+1$ στοιχεία και είναι γραμμικά εξαρτημένο. Άρα υπάρχει μία σχέση γραμμικής εξάρτησης $d_0 \cdot 1 + \cdots + d_n a^n = 0$, όπου $d_i \in \Bbbk$ για $i = 0, \ldots, n$ και τουλάχιστον ένα από αυτά δεν είναι μηδέν. Θεωρούμε το μη μηδενικό πολυώνυμο $g(x) = d_0 + d_1 x + d_n x^n \in \Bbbk[x]$. Το a είναι ρίζα του $g(x)$, άρα είναι αλγεβρικό πάνω από το $\Bbbk$. □

Ορισμός 2.2.9. *Έστω $F/\Bbbk$ επέκταση σωμάτων, $a_1, \ldots, a_n \in F$. Ορίζουμε $\Bbbk[a_1, \ldots, a_n]$ να είναι ο μικρότερος δακτύλιος που περιέχει το $\Bbbk$ και τα στοιχεία $a_1, \ldots, a_n$. Αντίστοιχα $\Bbbk(a_1, \ldots, a_n)$ είναι το μικρότερο σώμα που περιέχει το $\Bbbk$ και τα στοιχεία $a_1, \ldots, a_n$.*

Δεν είναι δύσκολο να αποδείξει κανείς ότι

$$\Bbbk[a_1, \ldots, a_n] = \Bbbk[a_1, \ldots, a_{n-1}][a_n] \quad \text{και} \quad \Bbbk(a_1, \ldots, a_n) = \Bbbk(a_1, \ldots, a_{n-1})(a_n)$$

Παράδειγμα 2.2.10. Θα αποδείξουμε ότι $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Στο Παράδειγμα 2.1.4 είδαμε ότι $\sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ και άρα $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Με τον ίδιο τρόπο προκύπτει ότι $\sqrt{3} \in \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ και άρα $\mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}] \subset \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Για τον αντίστροφο εγκλεισμό παρατηρούμε ότι το στοιχείο $\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Άρα $\mathbb{Q}[\sqrt{2} + \sqrt{3}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ και τελικά

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}] \ .$$

Έστω $\Bbbk \subset F \subset E$ εγκλεισμός σωμάτων. Το σώμα E έχει τη δομή του F-διανυσματικού χώρου καθώς και τη δομή του $\Bbbk$-διανυσματικού χώρου.

Πρόταση 2.2.11. *Έστω $\Bbbk \subset F \subset E$ εγκλεισμός σωμάτων, $[F : \Bbbk] < \infty$, $[E : F] < \infty$. Τότε $[E : \Bbbk] = [E : F][F : \Bbbk]$.*

Απόδειξη. Έστω F-$\{a_1, \ldots, a_n\}$ μία βάση του E και $\{b_1, \ldots, b_m\}$ μία $\Bbbk$-βάση του F. Θα δείξουμε ότι το σύνολο $\{a_i b_j : \ i = 1, \ldots, n, \ j = 1, \ldots, m\}$ είναι μία $\Bbbk$-βάση του E.

Θα ξεκινήσουμε με τη γραμμική ανεξαρτησία. Έστω

$$\sum_{i,j} d_{ij}(a_i b_j) = 0, \ d_{ij} \in \Bbbk, \ i = 1, \ldots, n, \ j = 1, \ldots, m \ .$$

Τότε

$$\sum_i (\sum_j d_{ij} b_j) a_i = 0, \ i = 1, \ldots, n, \ j = 1, \ldots, m \ .$$

Αφού $\sum_j d_{ij} b_j \in F$, η F-γραμμική ανεξαρτησία των $\{a_1, \ldots, a_n\}$ αναγκάζει για $i = 1, \ldots, n$ το άθροισμα $\sum_j d_{ij} b_j = 0$. Για κάθε μία τέτοια εξίσωση,

η $\Bbbk$-γραμμική ανεξαρτησία των $\{b_1, \ldots, b_m\}$ αναγκάζει για $j = 1, \ldots, m$ τον συντελεστή $d_{ij} = 0$.

Το τελευταίο κομμάτι της απόδειξης, δηλαδή το ότι τα στοιχεία παράγουν τον E ως $\Bbbk$-διανυσματικό χώρο επαφίεται ως άσκηση. □

Παρατηρούμε ότι αν $\Bbbk \subset F \subset E$ και $a \in E$ αλγεβρικό πάνω από το $\Bbbk$ τότε $\mathrm{irr}_{(F,a)}(x)$ διαιρεί το πολυώνυμο $\mathrm{irr}_{(\Bbbk,a)}(x)$ και $\deg \mathrm{irr}_{(F,a)}(x) \leq \deg \mathrm{irr}_{(\Bbbk,a)}(x)$.

Παραδείγματα 2.2.12.

- Έστω $E = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Μία $\mathbb{Q}$-βάση για το E προκύπτει από τον εγκλεισμό $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset E$ και είναι ίση με $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Στο Παράδειγμα 2.1.2 είδαμε ότι το πολυώνυμο $f(x) = x^4 - 10x + 1$ μηδενίζεται στο $\sqrt{2} + \sqrt{3}$. Μπορούμε τώρα να δείξουμε ότι $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Πράγματι αφού

  $$4 = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = \deg \mathrm{irr}_{(\mathbb{Q},\sqrt{2}+\sqrt{3})}(x)$$

  έπεται ότι $\mathrm{irr}_{(\mathbb{Q},\sqrt{2}+\sqrt{3})}(x) = f(x)$. Έτσι μία άλλη $\mathbb{Q}$-βάση για το E είναι το σύνολο $\{1, \sqrt{2} + \sqrt{3}, (\sqrt{2} + \sqrt{3})^2, (\sqrt{2} + \sqrt{3})^3\}$.

- Έστω $b = \sqrt[3]{2}$, $\omega = e^{2\pi i/3}$, $E = \mathbb{Q}[b, \omega]$. Αφού $\mathrm{irr}_{(\mathbb{Q},b)}(x) = x^3 - 2$ έπεται ότι $[\mathbb{Q}[b] : \mathbb{Q}] = 3$ και ότι $\{1, b, b^2\}$ είναι μία $\mathbb{Q}$-βάση του $\mathbb{Q}[b]$. Γνωρίζουμε ότι $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^2 + x + 1$. Άρα $\mathrm{irr}_{(\mathbb{Q}[b],\omega)}(x)$ διαιρεί το πολυώνυμο $\mathrm{irr}_{(\mathbb{Q},\omega)}(x)$ και έχει βαθμό ≤ 2. Όμως $\omega \notin \mathbb{Q}[b]$ και άρα $\deg \mathrm{irr}_{(Q[b],\omega)} \geq 2$. Έπεται ότι

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

  και $\{1, \omega\}$ είναι μία $\mathbb{Q}[b]$-βάση του E. Προκύπτει ότι $[E : \mathbb{Q}] = 6$ και ότι μία $\mathbb{Q}$-βάση του E είναι το σύνολο $\{1, b, b^2, \omega, \omega b, \omega b^2\}$.

- Έστω $b = \sqrt[5]{2}$, $\omega = e^{2\pi i/5}$, $E = \mathbb{Q}[b, \omega]$. Αφού

  $$[E : \mathbb{Q}] = [E : \mathbb{Q}(b)][\mathbb{Q}(b) : \mathbb{Q}] \tag{2.1}$$

  και $\deg \mathrm{irr}_{(\mathbb{Q},b)}(x) = 5$ έπεται ότι 5 διαιρεί $[E : \mathbb{Q}]$. Αντίστοιχα αφού

  $$[E : \mathbb{Q}] = [E : Q(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}]$$

  και $\deg \mathrm{irr}_{(\mathbb{Q},\omega)}(x) = 4$ έπεται ότι 4 διαιρεί τον βαθμό $[E : \mathbb{Q}]$. Άρα το 20 διαιρεί τον βαθμό $[E : \mathbb{Q}]$ και επομένως $[E : \mathbb{Q}] \geq 20$. Όμως $[E : \mathbb{Q}(b)] = \deg \mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x)$ και

  $$\deg \mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x) \leq \deg \mathrm{irr}_{(\mathbb{Q},\omega)}(x) = 4 \ .$$

Αντικαθιστώντας στην 2.1 προκύπτει ότι $[E : \mathbb{Q}] \leq 20$. Έπεται ότι $[E : \mathbb{Q}] = 20$ και ότι $\mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x) = x^4+x^3+x^2+x+1$ ενώ $\mathrm{irr}_{(\mathbb{Q}(\omega),b)}(x) = x^5 - 2$.

Έστω $\Bbbk \subset E$ εγκλεισμός σωμάτων. Το σώμα F καλείται *ενδιάμεσο* σώμα αν $\Bbbk \subset F \subset E$. Το Θεώρημα 2.2.11 θα εφαρμοστεί στα παρακάτω πορίσματα.

Πόρισμα 2.2.13. *Έστω $\Bbbk \subset E$ εγκλεισμός σωμάτων και $[E : \Bbbk] = p$, p πρώτος. Τότε δεν υπάρχει ενδιάμεσο σώμα F έτσι ώστε $\Bbbk \subsetneq F \subsetneq E$ και E είναι απλή επέκταση του $\Bbbk$.*

Απόδειξη. Η απόδειξη για τον πρώτο ισχυρισμό αυτού του Πορίσματος είναι προφανής. Για τον δεύτερο, έστω $a \in E$, $a \notin \Bbbk$. Έπεται ότι $\Bbbk \subsetneq \Bbbk[a]$ και επομένως $\Bbbk[a] = E$. □

Πόρισμα 2.2.14. *Τα ανάγωγα πολυώνυμα του δακτυλίου $\mathbb{R}[x]$ έχουν βαθμό 1 ή 2.*

Απόδειξη. Έστω $f(x) \in \mathbb{R}[x]$ ανάγωγο. Σύμφωνα με το Θεμελιώδες Θεώρημα της Άλγεβρας υπάρχει $a \in C$ έτσι ώστε $f(a) = 0$. Αν $a \in R$ τότε $(x-a) \mid f(x)$. Αφού $f(x)$ είναι ανάγωγο έπεται ότι $x - a = cf(x)$ όπου $c \in \mathbb{R}$ και ο βαθμός του $f(x)$ είναι 1. Αν $a \notin R$ τότε αφού $[\mathbb{C} : \mathbb{R}] = 2$, σύμφωνα με το προηγούμενο πόρισμα έπεται ότι $\mathbb{R}[a] = \mathbb{C}$. Αφού $f(x) = \mathrm{irr}_{(\mathbb{R},a)}(x)$ έπεται ότι $\deg f(x) = [\mathbb{R}[a] : \mathbb{R}] = 2$. □

2.3 Ομάδα Galois.

Ορισμός 2.3.1. *Έστω $F/\ \Bbbk$ επέκταση σωμάτων. Το σύνολο των αυτομορφισμών του F που διατηρούν σταθερό το $\Bbbk$, δηλαδή το σύνολο*

$$\mathrm{Aut}_{\Bbbk}(F) = \{\phi : F \xrightarrow{\cong} F,\ \phi(c) = c,\ \forall c \in \Bbbk\}$$

λέγεται ομάδα Galois του F πάνω από το $\Bbbk$ και θα συμβολίζεται με $\mathrm{Gal}(F/\Bbbk)$.

Παρατήρηση 2.3.2. Το σύνολο $G = \mathrm{Gal}(F/\Bbbk)$ είναι όντως ομάδα, με πράξη τη σύνθεση συναρτήσεων. Πράγματι είναι εύκολο να επιβεβαιώσει κανείς ότι αν $f, g \in G$ τότε $f \circ g : F \longrightarrow F$ είναι επίσης αυτομορφισμός και αν $c \in \Bbbk$ τότε $f \circ g(c) = f(g(c)) = f(c) = c$, άρα $f \circ g \in G$. Επίσης αν $f \in G$ τότε και $f^{-1} : F \longrightarrow F$ είναι ισομορφισμός και αν $c \in \Bbbk$ τότε $f^{-1}(c) = f^{-1}(f(c)) = (f^{-1} \circ f)(c) = \mathrm{id}_E(c) = c$, και άρα $f^{-1} \in G$. Έπεται ότι G είναι υποομάδα της ομάδας των ομομορφισμών από το F στο F. Τονίζουμε ότι G δεν είναι πάντα αντιμεταθετική ομάδα.

Έστω τώρα ότι $a \in F$ είναι αλγεβρικό πάνω από το $\Bbbk$ και έστω ότι $\phi \in G$. Θα δούμε ότι a και $\phi(a)$ έχουν το ίδιο ανάγωγο πολυώνυμο και έτσι αναγκαστικά $\phi(a)$ είναι μία από τις ρίζες του $\mathrm{irr}_{(\Bbbk,a)}(x)$.

Πρόταση 2.3.3. *Έστω $F/\ \Bbbk$ επέκταση σωμάτων $a \in F$ αλγεβρικό πάνω από το $\Bbbk$. Έστω $\phi \in \mathrm{Aut}_{\Bbbk}(F)$ και $\phi(a) = b$. Τότε $\mathrm{irr}_{(\Bbbk,a)}(x) = \mathrm{irr}_{(\Bbbk,b)}(x)$.*

Απόδειξη. Έστω $q(x) = \mathrm{irr}_{(\Bbbk,a)}(x) = \sum c_i x^i$. Αφού $q(x)$ μηδενίζεται στο a έπεται ότι $\sum c_i a^i = 0$. Επομένως $0 = \phi(\sum c_i a^i) = \sum \phi(c_i a^i) = \sum \phi(c_i)\phi(a^i) = \sum c_i \phi(a)^i = \sum c_i b^i$. Έπεται ότι $q(x) = \mathrm{irr}_{(\Bbbk,b)}(x)$. □

Για την αντίστροφη κατεύθυνση αυτής της πρότασης έχουμε το εξής Θεώρημα.

Θεώρημα 2.3.4. *Έστω $F/\ \Bbbk$ επέκταση σωμάτων, $a, b \in F$ αλγεβρικά πάνω από το $\Bbbk$ και $\mathrm{irr}_{(\Bbbk,a)}(x) = \mathrm{irr}_{(\Bbbk,b)}(x)$. Υπάρχει ένας ισομορφισμός σωμάτων $\phi : \Bbbk[a] \longrightarrow \Bbbk[b]$ έτσι ώστε $\phi|_{\Bbbk} = \mathrm{id}_{\Bbbk}$ και $\phi(a) = b$.*

Απόδειξη. Έστω $I = (\mathrm{irr}_{(\Bbbk,a)}(x))$. Ο επιμορφισμός $\phi_1 : \Bbbk[x] \to \Bbbk[a]$, $\phi_1(f(x)) = f(a)$ δίνει τον ισομορφισμό $\overline{\phi_1} : \Bbbk[x]/I \to \Bbbk[a]$, $\overline{\phi_1}(f(x) + I) = f(a)$. Συγκεκριμένα $\overline{\phi_1}(x + I) = a$ ενώ $\overline{\phi_1}(c + I) = c$ για $c \in \Bbbk$. Αντίστοιχα έχουμε τον ισομορφισμό $\overline{\phi_2} : \Bbbk[x]/I \to \Bbbk[b]$, $\overline{\phi_1}(f(x) + I) = f(b)$. Έπεται ότι $\overline{\phi_2} \circ \overline{\phi_1}^{-1} :\ \Bbbk[a] \to \Bbbk[b]$ έχει τις επιθυμητές ιδιότητες. □

Είναι εύκολο να δει κανείς ότι αν $\sigma :\ \Bbbk \to \Bbbk'$ είναι ισομορφισμός σωμάτων, τότε η συνάρτηση

$$\widehat{\sigma} :\ \Bbbk[x] \to \Bbbk'[x], \quad \sum a_i x^i \mapsto \sum \sigma(a_i) x^i$$

είναι ισομορφισμός. Σημειώνουμε έτσι την άμεση γενίκευση του Θεωρήματος 2.3.4, και αφήνουμε την απόδειξη ως άσκηση για τον αναγνώστη.

Θεώρημα 2.3.5. *Έστω $\Bbbk \subset F$, $\Bbbk' \subset F'$ επεκτάσεις σωμάτων, $b \in F$, $b' \in F'$ αλγεβρικά υπεράνω των $\Bbbk$, $\Bbbk'$ αντίστοιχα, και $\sigma :\ \Bbbk \to \Bbbk'$ ισομορφισμός έτσι ώστε*

$$\widehat{\sigma}(\mathrm{irr}_{(\Bbbk,b)}(x)) = \mathrm{irr}_{(\Bbbk',b')}(x)\ .$$

Υπάρχει ένας ισομορφισμός σωμάτων $\phi : \Bbbk[b] \longrightarrow \Bbbk'[b']$ έτσι ώστε $\phi|_{\Bbbk} = \sigma$ και $\phi(b) = b'$.

Στα επόμενα παραδείγματα θα υπολογίσουμε την ομάδα Galois σε διάφορες περιπτώσεις. Παρατηρούμε ότι αν $\Bbbk \subset F$ είναι εγκλεισμός σωμάτων τότε id_F ανήκει αυτόματα στην ομάδα $G = \mathrm{Aut}_{\Bbbk} F$.

Παραδείγματα 2.3.6.

- $\mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\}$.

- Γενικότερα αν $\Bbbk$ είναι σώμα τότε $\mathrm{Gal}(\Bbbk/\Bbbk) = \mathrm{Aut}_{\Bbbk}(\Bbbk) = \{\mathrm{id}_{\Bbbk}\}$.

- Έστω $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Τότε $G \cong \mathbb{Z}_2$. Πράγματι $\mathbb{C} = \mathbb{R}(i)$ είναι το σώμα ανάλυσης του $f(x) = x^2+1$ υπεράνω του $\mathbb{R}$. Τα στοιχεία της G στέλνουν τα στοιχεία του $\mathbb{R}$ στον εαυτό τους και καθορίζονται από την εικόνα του i: $\sigma_0 : i \mapsto i$ και $\sigma_1 : i \mapsto -i$. Έτσι $\sigma_0 = id_{\mathbb{C}}$ και $\sigma_1(a+bi) = a - bi$.

- Έστω $F = \mathbb{Q}(\omega)$ όπου $\omega = e^{2\pi i/3}$. Αφού $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^2 + x + 1$ κάθε στοιχείο του F είναι της μορφής $c + d\omega : \ c, d \in \mathbb{Q}$. Αν $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ τότε $\sigma(c) = c, \ \forall c \in \mathbb{Q}$ και

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

  Έπεται ότι $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}_2$.

- Έστω $E = \mathbb{Q}(\sqrt{2}) = \{c_0 \cdot 1 + c_1 \cdot \sqrt{2} : \ c_i \in \mathbb{Q}\}$. Θα υπολογίσουμε την ομάδα $G = \mathrm{Gal}(\mathbb{Q}/E)$. Αφού $\mathrm{irr}_{\mathbb{Q}} \sqrt{2} = x^2 - 2$ έπεται ότι $\phi(\sqrt{2}) = \pm\sqrt{2}$ για $\phi \in G$. Ένα τυχαίο στοιχείο a του E είναι της μορφής

$$a = c_0 \cdot 1 + c_1 \cdot \sqrt{2}$$

  άρα

$$\begin{aligned} \phi(a) &= \phi(c_0 \cdot 1 + c_1 \cdot \sqrt{2}) = \phi(c_0 \cdot 1) + \phi(c_1 \cdot \sqrt{2}) \\ &= \phi(c_0) \cdot \phi(1) + \phi(c_1)\phi(\sqrt{2}) = c_0 \cdot 1 + c_1\phi(\sqrt{2}) \ . \end{aligned}$$

  Έπεται ότι $\phi \in G$ καθορίζεται πλήρως από $\phi(\sqrt{2})$, και ότι αν $\phi_1, \phi_2 \in G$ και $\phi_1(\sqrt{2}) = \phi_2(\sqrt{2})$ τότε $\phi_1 = \phi_2$. Έπεται ότι $|G| \leq 2$. Παρατηρούμε ότι $\mathrm{id}_E(\sqrt{2}) = \sqrt{2}$. Επίσης το Θεώρημα 2.3.4 εγγυάται ότι υπάρχει ισομορφισμός $\sigma : \ E \to \mathbb{Q}(-\sqrt{2})$, $\phi(\sqrt{2}) = -\sqrt{2}$. Αφού $E = \mathbb{Q}(-\sqrt{2})$ έπεται ότι $\sigma \in G$ είναι το δεύτερο στοιχείο της G. Άρα $|G| = 2$ και $G \cong \mathbb{Z}_2$.

- Έστω $E = \mathbb{Q}(\sqrt[3]{2})$, $G = \mathrm{Gal}(\mathbb{Q}/E)$. Έστω $b = \sqrt[3]{2}$. Τότε $\mathrm{irr}_{(\mathbb{Q},b)}(x) = x^3 - 2$ και μία $\mathbb{Q}$-βάση του E είναι το σύνολο $\{1, b, b^2\}$. Έστω $a \in E$, $\phi \in G$. Τότε

$$a = c_0 + c_1 b + c_2 b^2 : \ c_i \in \mathbb{Q}$$

  και

$$\phi(a) = \phi(c_0) + \phi(c_1)\phi(b) + \phi(c_2)\phi(b^2) = c_0 + c_1\phi(b) + c_2\phi(b)^2 \ .$$

Άρα κάθε $\phi \in G$ καθορίζεται πλήρως από την εικόνα $\phi(b)$. Σύμφωνα με το Θεώρημα 2.3.3 $\phi(b)$ πρέπει να είναι μία ρίζα του $\mathrm{irr}_{(\mathbb{Q},b)}(x)$. Θα πρέπει βέβαια $\phi(b) \in E$. Η μόνη ρίζα του $x^3 - 2$ που ανήκει στο E είναι το b. Άρα αν $\phi \in G$ τότε $\phi(b) = b$ και $\phi = \mathrm{id}_E$. Έπεται ότι $G = \{\mathrm{id}_E\}$.

- Έστω $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $G = \mathrm{Gal}(\mathbb{Q}/E)$. Μία $\mathbb{Q}$-βάση του E είναι το σύνολο $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Έστω ότι $\phi \in G$. Τότε $\phi(1) = 1$ και $\phi(\sqrt{6}) = \phi(\sqrt{2})\phi(\sqrt{3})$. Έπεται ότι ϕ καθορίζεται πλήρως από τις εικόνες των $\sqrt{2}$ και $\sqrt{3}$. Σύμφωνα με το Θεώρημα 2.3.3 $\phi(\sqrt{2}) = \pm\sqrt{2}$, ενώ $\phi(\sqrt{3}) = \pm\sqrt{3}$. Έπεται ότι G έχει το πολύ 4 στοιχεία. Σίγουρα $\mathrm{id}_E \in G$: $\mathrm{id}_E(\sqrt{2}) = \sqrt{2}$, $\mathrm{id}_E(\sqrt{3}) = \sqrt{3}$. Θα δείξουμε ότι και οι άλλες 3 δυνατότητες αντιστοιχούν σε στοιχεία του G. Πράγματι θεωρούμε το E ως απλή επέκταση του $E_1 = \mathbb{Q}(\sqrt{2})$:

$$E = E_1(\sqrt{3}) \ .$$

Σύμφωνα με το Θεώρημα 2.3.4

$$\exists\ \phi_1 :\ E_1(\sqrt{3}) \to E_1(-\sqrt{3}),\ \phi_1(\sqrt{3}) = -\sqrt{3},\ \phi_1(c) = c,\ \forall c \in E_1 \ .$$

Αφού $E_1(-\sqrt{3}) = E_1(\sqrt{3})$ έπεται ότι

$$\phi_1 \in G,\ \phi_1(\sqrt{2}) = \sqrt{2},\ \phi_1(\sqrt{3}) = -\sqrt{3} \ .$$

Ομοίως αντιμετωπίζοντας το E ως απλή επέκταση του $E_2 = \mathbb{Q}(\sqrt{3})$ προκύπτει ότι

$$\exists\ \phi_2 \in G,\ \phi_2(\sqrt{2}) = -\sqrt{2},\ \phi_2(\sqrt{3}) = \sqrt{3} \ .$$

Επίσης

$$\phi_3 = \phi_1 \circ \phi_2 \in G,\ \phi_3(\sqrt{2}) = -\sqrt{2},\ \phi_3(\sqrt{3}) = -\sqrt{3} \ .$$

Άρα $|G| = 4$. Υπάρχουν ακριβώς δύο ομάδες τεσσάρων στοιχείων με προσέγγιση ισομορφίας: η κυκλική ομάδα με 4 στοιχεία που είναι ισόμορφη με την $\mathbb{Z}_4$ και η ομάδα του Klein που είναι ισόμορφη με την $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Παρατηρούμε ότι η G έχει ένα στοιχείο τάξης 1 τον ταυτοτικό ομομορφισμό και 3 στοιχεία τάξης 2. Για παράδειγμα

$$\phi_1^2 :\ \sqrt{2} \mapsto \sqrt{2} \mapsto \sqrt{2}, \quad \sqrt{3} \mapsto -\sqrt{3} \mapsto -(-\sqrt{3}) = \sqrt{3}$$

και $\phi_1^2 = \mathrm{id}_E$. Έπεται ότι $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Θα επανέλθουμε στην ύπαρξη του ϕ_3 με το επόμενο παράδειγμα. Η μέθοδος του Παραδείγματος αυτού θα χρησιμοποιηθεί για την εύρεση της ομάδας Galois στη γενική περίπτωση, βλέπε Θεώρημα 2.3.5.

Παράδειγμα 2.3.7. Στο παράδειγμα αυτό θα αποδείξουμε απευθείας την ύπαρξη $\phi_3 \in \mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{2},\sqrt{3})$ έτσι ώστε $\phi_3(\sqrt{2}) = -\sqrt{2}$, $\phi_3(\sqrt{3}) = -\sqrt{3}$. Σύμφωνα με το Θεώρημα 2.3.4 υπάρχει

$$\psi_1 :\ \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}),\ \psi_1(\sqrt{2}) = -\sqrt{2})\ , \phi_1(c) = c,\ \forall\ c \in \mathbb{Q}\ .$$

Παρατηρούμε ότι $\psi(a + b\sqrt{2}) = a - b\sqrt{2}$. Θέτουμε $E_1 = \mathbb{Q}(\sqrt{2})$. Ο ισομορφισμός σωμάτων ψ_1 επεκτείνεται σε ισομορφισμό δακτυλίων

$$\psi_2 = \widehat{\psi_1} :\ E_1[x] \to E_1[x], \quad \sum a_i x^i \mapsto \sum \psi_1(a_i)\ x^i\ .$$

Το ιδεώδες $I = (x^2 - 3)$ είναι μέγιστο στον δακτύλιο $E_1[x]$. Θεωρούμε τον κανονικό επιμορφισμό

$$\psi_3 :\ E_1[x] \to E_1[x]/I, \quad f(x) \mapsto \psi_2(f(x)) + I\ .$$

Έχουμε $\psi_3(\sqrt{2}) = -\sqrt{2} + I$, $\psi_3(x) = x + I$ και ότι $\ker \psi_3 = (x^2 - 3) = I$. Επομένως σύμφωνα με το Πρώτο Θεώρημα Ισομορφίας Δακτυλίων έχουμε τον ισομορφισμό σωμάτων

$$\psi_4 :\ E_1[x]/I \to E_1[x]/I, \quad f(x) + I \mapsto \psi_2(f(x)) + I\ .$$

Τονίζουμε ότι ψ_4 δεν είναι ο ταυτοτικός μορφισμός αφού $\psi_4(\sqrt{2}+I) = -\sqrt{2}+I$. Τέλος παρατηρούμε ότι αφού $\pm\sqrt{3}$ είναι οι δύο ρίζες του $x^3 - 3$ έχουμε τους ισομορφισμούς $\sigma_1 :\ E_1(\sqrt{3}) \to E_1[x]/I$, $\sqrt{3} \mapsto x + I$ και $\sigma_2 :\ E_1(-\sqrt{3}) \to E_1[x]/I$, $-\sqrt{3} \mapsto x + I$. Παρατηρούμε ότι $E_1(\sqrt{3}) = E_1(-\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ και ότι η σύνθεση $\phi = {\sigma_2}^{-1}\psi_4\sigma_1$ είναι ο ισομορφισμός σωμάτων με τις επιθυμητές ιδιότητες:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \to \mathbb{Q}(\sqrt{2},\sqrt{3}),\ \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}, c \mapsto c, \forall c \in \mathbb{Q}\ .$$

Στο επόμενο κεφάλαιο θα αποδείξουμε το παρακάτω θεώρημα:

Θεώρημα 2.3.8. *Έστω ότι $\phi :\ \Bbbk \to \Bbbk'$ ισομορφισμός σωμάτων και έστω $L/\ \Bbbk$ σώμα ανάλυσης του $f(x)$, $L'/\ \Bbbk'$ σώμα ανάλυσης του $f^*(x)$. Τότε υπάρχει ισομορφισμός $\sigma :\ L \to L'$ που επεκτείνει τον ϕ.*

Ολοκληρώνουμε αυτήν την ενότητα με την μέθοδο που έχουμε ακολουθήσει ως τώρα για την εύρεση της ομάδας $G = \mathrm{Aut}_{\Bbbk}(F)$.

- Βρίσκουμε μία $\Bbbk$-βάση του F.
- Βρίσκουμε τα ανάγωγα πολυώνυμα για *κρίσιμα* στοιχεία της βάσης του F.
- Βρίσκουμε τις πιθανές εικόνες των των κρίσιμων στοιχείων ως ρίζες των αναγώγων πολυωνύμων τους και τα πιθανά στοιχεία της G.
- Αποδεικνύουμε την ύπαρξη ενός στοιχείων της G χρησιμοποιώντας το Θεώρημα 2.3.3.

2.4 Ασκήσεις

1. Να περιγραφούν τα σώματα: $\mathbb{Q}(\sqrt{5},\sqrt{7})$, $\mathbb{Q}(i\sqrt{11})$.
2. Να βρεθεί το πολυώνυμο $\mathrm{irr}_{(\mathbb{Q},a)}(x)$ όταν
   - $a=\sqrt{7}+1/2$,
   - $a=i\sqrt{3}-1/2$.
3. Να υπολογισθεί η ομάδα Galois $\mathrm{Gal}(\mathbb{Q}(a)/\mathbb{Q})$ όταν
   - $a=\sqrt{5}$,
   - $a=\omega^{2\pi i/5}$
   - $a=\sqrt[3]{-2}$
4. Να βρεθούν οι βαθμοί των επεκτάσεων:
   - $\mathbb{C}/\ \mathbb{Q}$,
   - $\mathbb{Z}_5(x)/\ \mathbb{Z}_5$,
   - $\mathbb{R}(\sqrt{5})/\ \mathbb{R}$,
   - $\mathbb{Q}(\sqrt[7]{3})/\ \mathbb{Q}$.
5. Έστω $E=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. Να αποδείξετε ότι $[E:\mathbb{Q}]=8$.
6. Έστω ότι $a,b\in E$ είναι αλγεβρικά υπεράνω του F. Να αποδείξετε τα ακόλουθα
   - $[F(a+b):F]<\infty$
   - Το στοιχείο $a+b$ είναι αλγεβρικό υπεράνω του F.

7.
   - Να αποδείξετε ότι $\mathbb{Q}(\sqrt{5}+\sqrt{2}) = \mathbb{Q}(\sqrt{5},\sqrt{2})$.
   - Να βρείτε το ανάγωγο πολυώνυμο του $\sqrt{5}+\sqrt{2}$ υπεράνω του $\mathbb{Q}(\sqrt{2})$.
   - Να βρείτε το ανάγωγο πολυώνυμο του $\sqrt{5}+\sqrt{2}$ υπεράνω του $\mathbb{Q}(\sqrt{5},\sqrt{2})$.
   - Να βρείτε το ανάγωγο πολυώνυμο του $\sqrt{5}+\sqrt{2}$ υπεράνω του $\mathbb{Q}$.

8. Έστω $[L:\Bbbk] < \infty$ μία πεπερασμένη επέκταση και $f(x) \in \Bbbk[x]$ ανάγωγο. Να αποδείξετε ότι αν οι φυσικοί αριθμοί $\deg f(x) > 1$ και $[L:\Bbbk]$ είναι πρώτοι μεταξύ τους, τότε το $f(x)$ δεν έχει ρίζες στο L.