11/5/2020 (1)

Παράδειγμα

Έστω $E = \mathbb{Q}(\omega)$, όπου $\omega = e^{2\pi i/3}$. Παρατηρούμε ότι $irr(\mathbb{Q},\omega) = x^2+x+1$ και $E = \mathbb{Q}(\omega^2)$.

Το ω είναι η 3-ρίζα της μονάδος όπως και το ω^2. Συνεπώς, είναι και τα δύο ρίζες του $x^3-1 = (x-1)(x^2+x+1)$. Αλλά δεν είναι ρίζες του $x-1$. Άρα, και τα δύο είναι ρίζες του $x^2+x+1 = irr(\mathbb{Q},\omega)(x)$. Συνεπώς $irr(\mathbb{Q},\omega) = (x-\omega)(x-\omega^2)$.

$\mathbb{Q}(\omega) = \mathbb{Q}(\omega^2)$

Απόδειξη Φανερά, ω^2 είναι στοιχείο του $\mathbb{Q}(\omega)$, γιατί $\mathbb{Q}(\omega)$ το ελάχιστο υπόσωμα του $\mathbb{C}$ που περιέχει τους ρητούς $\mathbb{Q}$ και το ω. Συνεπώς, αφού $\mathbb{Q}(\omega^2)$ το ελάχ. υπόσωμα $\mathbb{C}$ που ~~πε~~ περιέχει τους ρητούς $\mathbb{Q}$ και ω^2 και το $\mathbb{Q}(\omega)$ έχει αυτήν την ιδιότητα, έπεται ότι $\mathbb{Q}(\omega^2)$ υποσύνολο του $\mathbb{Q}(\omega)$. Αντίστροφα, $\omega = (\omega^2)^2 = \omega^4$. Άρα το ω είναι στοιχείο του $\mathbb{Q}(\omega^2)$ και με το επιχείρημα της προηγούμενης παραγράφου έπεται ότι

$\mathbb{Q}(\omega)$ υποσύνολο του $\mathbb{Q}(\omega^2)$

Άρα $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^2)$

ΠΡΟΣΟΧΗ γενικά $\mathbb{Q}(a^2)$ υποσύνολο του $\mathbb{Q}(a)$. Αλλά μπορεί να μην ισχύει ισότητα, π.χ. αν $a = i$, τότε

$\mathbb{Q}(i^2) = \mathbb{Q}(-1) = \mathbb{Q}$ που είναι γνήσιο υποσύνολο του $\mathbb{Q}(i)$.

Θεμελιώδες Θεώρημα της Θεωρίας Galois.

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

Απόδειξη Έστω $X = \{b_1, \dots, b_n\}$ το σύνολο των ριζών του $f(x)$. Τότε $E = F(b_1, \dots, b_n)$. Τα στοιχεία του S_X είναι αμφιμονοσήμαντες και επί συναρτήσεις του X στον εαυτό του και $S_X \simeq S_n$.

Έστω E/F επέκταση σωμάτων. Υποθέτουμε $a_1, \dots, a_r$ στοιχεία του E ώστε $E = F(a_1, \dots, a_r)$ (Με άλλα λόγια, το ελάχιστο υπόσωμα του E που περιέχει και το F και κάθε a_i είναι το E.) Έστω σ στοιχείο της ομάδας $Gal(E/F)$. Τότε το σ καθορίζεται μονοσήμαντα από τις τιμές των $a_1, \dots, a_r$. Ο λόγος είναι ότι κάθε στοιχείο του E είναι πηλίκο δύο πολυωνύμων $a_1, \dots, a_r$ με συντελεστές το F και $\sigma(c) = c$, $\forall c$ του F. Άρα το $\sigma(u)$ καθορίζεται μονοσήμαντα από τις τιμές του σ στα $a_1, \dots, a_r$.

Παράδειγμα

$$u = (c_1 \cdot a_1^2 + c_2 \cdot a_1 \cdot a_2) / (c_3 \cdot a_3^3)$$

τότε

$$\sigma(u) = (c_1 \cdot b_1^2 + c_2 \cdot b_1 b_2) / (c_3 \cdot b_3^3)$$

όπου $b_1 = \sigma(a_1)$, $b_2 = \sigma(a_2)$, $b_3 = \sigma(a_3)$

Παρατήρηση Έχουμε δει ότι αν $\mathrm{char}F = 0$, κάθε πολυώνυμο είναι διαχωρίσιμο.

Παράδειγμα Έστω $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $\omega = e^{2\pi i/3}$, $b = \sqrt[3]{2}$ και $E = \mathbb{Q}(b, \omega b)$. Το E σώμα ανάλυσης του $f(x)$ πάνω στο $\mathbb{Q}$ και η ομάδα $G = Gal(E/\mathbb{Q})$ καθορίζεται από τον πίνακα.

b	b	ωb	$\omega^2 b$	b	ωb	$\omega^2 b$
ω	ω	ω	ω	ω^2	ω^2	ω^2
	id_E	σ	σ^2	τ	$\sigma\tau$	$\tau\sigma$

Η G είναι ισόμορφη με την S_3 και οι εικόνες των στοιχείων της G σύμφωνα με τον ισομορφισμό φα είναι:

$$id_E \to \begin{pmatrix} b & \omega b & \omega^2 b \\ b & \omega b & \omega^2 b \end{pmatrix}, \quad \sigma \to \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega b & \omega^2 b & b \end{pmatrix},$$

$$\sigma^2 \to \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega^2 b & b & \omega b \end{pmatrix}, \quad \tau \to \begin{pmatrix} b & \omega b & \omega^2 b \\ b & \omega^2 b & \omega b \end{pmatrix}$$

$$\sigma\tau \to \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega b & b & \omega^2 b \end{pmatrix}, \quad \tau\sigma \to \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega^2 b & \omega b & b \end{pmatrix}$$

Παρατήρηση Έχουμε $E = \mathbb{Q}(b, \omega) = \mathbb{Q}(b, \omega b) = \mathbb{Q}(b, \omega b, \omega^2 b)$ και $b, \omega \cdot b, \omega^2 b$ είναι οι τρεις ρίζες του f στο E.

1^{o} Εργαλείο: (στο παράδειγμα 2.3.6). Έχουμε $E = \mathbb{Q}(b, \omega)$ και τις διαδοχικές επεκτάσεις

$$\mathbb{Q} \subseteq \mathbb{Q}(b) \subseteq \mathbb{Q}(b, \omega)$$

και

$$\mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \mathbb{Q}(b, \omega)$$

2^{o} εργαλείο: (παράδειγμα 3.1.2) $b, \omega b, \omega^2 b$ είναι οι 3 ρίζες του f στο E, συνεπώς η ομάδα Galois είναι υποομάδα της S_3, πιο ακριβέστερα, του συνόλου $\{T : \{b, \omega b, \omega^2 b\} \to \{b, \omega b, \omega^2 b\},$ με T 1-1 και επί$\}$

<u>Παράδειγμα</u> $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$.

Το $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ είναι σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$, $Gal(E/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ και τα στοιχεία του G καθορίζονται από τον πίνακα:

$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$
	id_E	σ_1	σ_2	$\sigma_1\sigma_2$

Αν διατάξουμε τις ρίζες του $f(x)$ ως το σύνολο $\{\sqrt{2}, \sqrt{3}, -\sqrt{2}, -\sqrt{3}\}$, τότε οι εικόνες των σ_1, σ_2 και $\sigma_3 = \sigma_1\sigma_2$ στην S_4 αντιστοιχούν στις μεταθέσεις $(2,4), (1,3), (1,3)(2,4)$ αντίστοιχα.

Θεωρούμε 1-1 και επί απεικόνιση

$T: \{1,2,3,4\} \to \{\sqrt{2}, \sqrt{3}, -\sqrt{2}, -\sqrt{3}\}$

που στέλνει το 1 στο $\sqrt{2}$, το 2 στο $\sqrt{3}$, το 3 στο $-\sqrt{2}$, το 4 στο $-\sqrt{3}$.

Τότε, η ομάδα Galois της επέκτασης μπορεί να ταυτιστεί μέσω της T, με την εξής υποομάδα της S_4: $\{id_4, (2,4), (1,3), (2,4)(1,3)\}$.

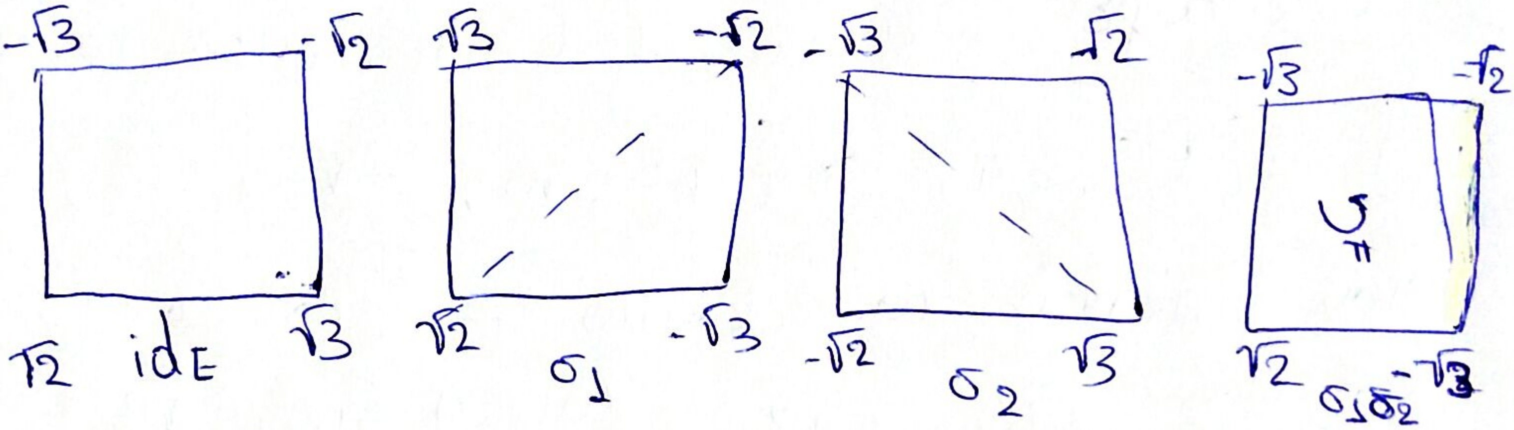
Αυτό σημαίνει ότι η ομάδα Galois της επέκτασης είναι οι εξής 1-1 και επί απεικονίσεις του X στον εαυτό του:

id_X,

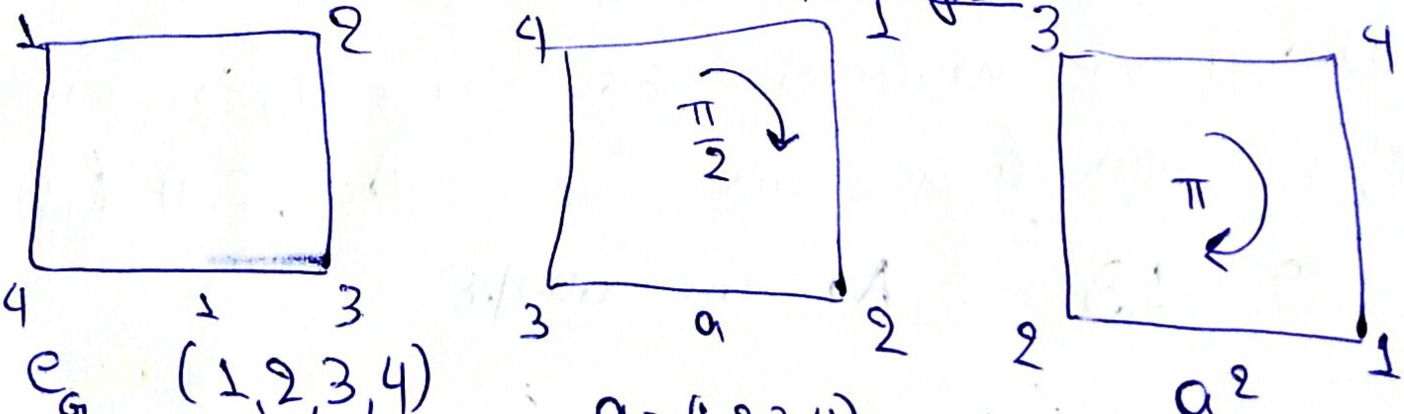
$$\begin{pmatrix} \sqrt{2} & \sqrt{3} & -\sqrt{2} & -\sqrt{3} \\ \sqrt{2} & -\sqrt{3} & -\sqrt{2} & -\sqrt{3} \end{pmatrix} = (2,4)$$

$$\begin{pmatrix} \sqrt{2} & \sqrt{3} & -\sqrt{2} & -\sqrt{3} \\ -\sqrt{2} & \sqrt{3} & \sqrt{2} & -\sqrt{3} \end{pmatrix} = (1,3)$$

$$\begin{pmatrix} \sqrt{2} & \sqrt{3} & -\sqrt{2} & -\sqrt{3} \\ -\sqrt{2} & -\sqrt{3} & \sqrt{2} & \sqrt{3} \end{pmatrix} = (2,4)(1,3)$$



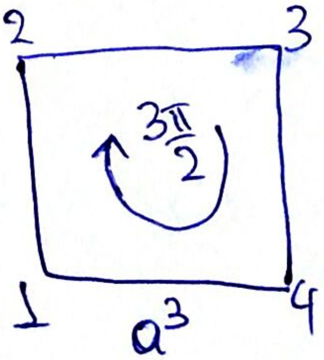
Διεδρική ομάδα D_4 τάξης 8



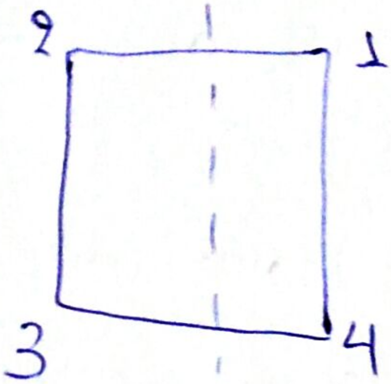
e_G (1,2,3,4)

$a = (1,2,3,4)$

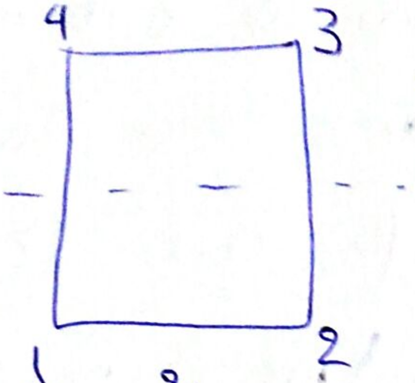
$a^2 = (1,3)(2,4)$



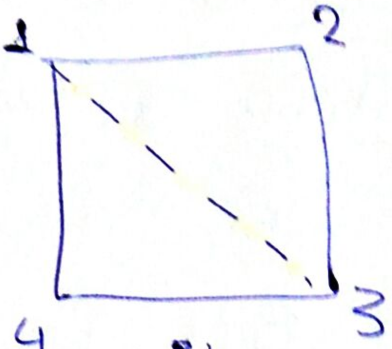
$a^3 = (1,4,3,2) = (4,3,2,1) = a^{-1}$



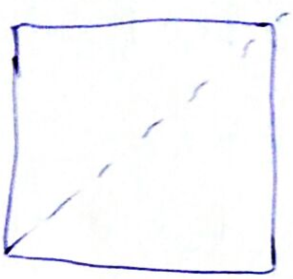
b



$a^2b =$
$(1,4)(2,3)$



$a^3b = (2,4)$



$ab = (1,3)$

$G = \{e_G, a, a^2, a^3, b, ab, a^2b, a^3b\}$

$\mathrm{ord}(a) = 4 \quad \mathrm{ord}(b) = 2$

$bab^{-1} = a^3$

$\mathrm{ord}(a^2) = 2 \quad \mathrm{ord}(a^3) = 4$

$\mathrm{ord}(ab) = \mathrm{ord}(a^2b) = \mathrm{ord}(a^3b) = 2.$

<u>Παράδειγμα</u> $f(x) = x^4 - 2$, $b = \sqrt[4]{2}$

οι ρίζες του $f(x)$ στο $\mathbb{C}$ είναι $\pm b, \pm bi$

και $E = \mathbb{Q}(b, ib, -b, -ib)$ από τον ορισμό του σώματος ανάλυσης πολυωνύμων.

Ισχυρισμός $E = \mathbb{Q}(b, i)$

<u>Απόδειξη</u> Φανερά E υποσύνολο του $\mathbb{Q}(b,i)$ γιατί E είναι το ελάχιστο υπόσωμα του $\mathbb{C}$

που περιέχη το $\mathbb{Q}$ και τα $b, ib, -b, -ib$ και αυτά φανερά περιέχονται στο $\mathbb{Q}(b,i)$.

Τώρα θα δείξουμε ότι $\mathbb{Q}(b,i)$ (υποσύνολο) E

Αφού $\mathbb{Q}(b,i)$ είναι το ελάχιστο υπόσωμα του $\mathbb{C}$ που περιέχη το $\mathbb{Q}$ και τα b, i αρκεί να δείξουμε ότι $\mathbb{Q}$ (υποσύνολο) E, που προφανώς ισχύει, ότι b στοιχείο του E, που προφανώς ισχύει, και ότι i στοιχείο του E που ισχύει, γιατί b, bi στοιχεία του E, και b μη μηδενικό, και E σώμα, άρα $i = (bi)/b$ είναι επίσης στοιχείο του E.

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

$irr_{(F,b)} = x^4 - 2$, $F = \mathbb{Q}(i)$

$E = F(b)$, υπάρχη αυτομορφισμός $\sigma \in G$

$\sigma : b \to ib, \; i \to i$

υπάρχη $\tau \in G$. $(G = Gal(E/\mathbb{Q}))$

$\tau : b \to b, \; i \to -i$

b	b	$-b$	b	$-b$	ib	ib	$-ib$	$-ib$
i	i	i	$-i$	$-i$	i	$-i$	i	$-i$
	id_E	σ^2	τ	$\sigma^2\tau$	σ	$\sigma\tau$	σ^3	$\sigma^3\tau$.

$\sigma(b) = ib, \quad \sigma(i) = i$

άρα, $\sigma(-b) = -\sigma(b) = -ib$

$$\sigma(ib) = \sigma(i)\cdot\sigma(b) = i\cdot ib = -b$$
$$\sigma(-ib) = -\sigma(ib) = -(-b) = b$$

Πόρισμα Έστω F ένα σώμα $f(x) \in F[X]$ και E, E' δύο σώματα ανάλυσης του $f(x)$ πάνω από το F. Τότε υπάρχει F-ισομορφισμός $\varphi : E \to E'$ και επομένως το σώμα ανάλυσης του $f(x) \in F[X]$ είναι μοναδικό με προσέγγιση F-ισομορφίας.