4/5/2020

Παράδειγμα

Έστω $b = \sqrt[3]{2}$ και $\omega = e^{2\pi i/3}$, $E = \mathbb{Q}(b, \omega)$

$\cos(2\pi/3) + i \cdot \sin(2\pi/3)$

ω ρίζα του $(x^3 - 1) = (x-1)(x^2+x+1)$, άρα ω ρίζα του (x^2+x+1) που είναι ανάγωγο επί του $\mathbb{Q}$, γιατί δεν έχει ρίζες στο $\mathbb{Q}$.

$irr_{(\mathbb{Q}, b)}(x) = x^3 - 2$, άρα $[\mathbb{Q}(b) : \mathbb{Q}] = 3$

και ότι $\{1, b, b^2\}$ είναι μία $\mathbb{Q}$-βάση του $\mathbb{Q}(b)$. Γνωρίζουμε ότι $irr_{(\mathbb{Q}, \omega)}(x) = x^2 + x + 1$.

άρα $irr_{(\mathbb{Q}(b), \omega)}(x)$ διαιρεί το $irr_{(\mathbb{Q}, \omega)}(x)$ και έχει βαθμό $x \leq 2$. Όμως, $\omega \notin \mathbb{Q}(b)$ και άρα $\deg irr_{(\mathbb{Q}(b), \omega)} \geq 2$.

Επομένως, $irr(\mathbb{Q}(b), \omega)(x) = irr(\mathbb{Q}, \omega)(x) = x^2 + x + 1$ και $\{1, \omega\}$ είναι μία $\mathbb{Q}(b)$-βάση του E.

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

Παράδειγμα

Εστω $b = \sqrt[5]{2}$, $\omega = e^{2\pi i/5}$ $L = \mathbb{Q}(b,\omega)$

Ισχυρισμός: Έχουμε $\deg irr_{(\mathbb{Q},\omega)} = 4$

Απόδειξη Το ω, επειδή είναι $5^{\underline{\eta}}$ ρίζα της μονάδος, ικανοποιεί το x^5-1. Έχουμε $x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$, άρα ω ρίζα του $x^4+x^3+x^2+x+1$., το πολυώνυμο αυτό είναι ανάγωγο επί του $\mathbb{Q}$. Αφού είναι μονικό και μηδενίζεται στο ω, έπεται ότι $irr_{(\mathbb{Q},\omega)} = x^4+x^3+x^2+x+1$

Πόρισμα Έστω E/F επέκταση σωμάτων και έστω $a_1,\dots,a_n \in E$ αλγεβρικά πάνω από το F. Τότε:

i) Ο $[F(a_1,\dots,a_n):F] < \infty$

ii) Ισχύει ότι $F(a_1,\dots,a_n) = F[a_1,\dots,a_n]$

iii) Η επέκταση $F(a_1,\dots,a_n)/F$ είναι αλγεβρική

<u>ΠΡΟΤΑΣΗ</u> Έστω E/L, L/F

δύο διαδοχικές επεκτάσεις σωμάτων.

Αν η επέκταση F/E είναι αλγεβρική, τότε και οι επεκτάσεις F/L και L/E είναι αλγεβρικές

<u>Απόδειξη</u> Έστω a στοιχείο του E. Μηδενίζεται από μη μηδενικό πολυώνυμο με συντελεστές στο F, άρα και στο L. Συνεπώς, η επέκταση L/E είναι αλγεβρική.

Έστω b στοιχείο του L. Τότε b στοιχείο του E, άρα μηδενίζεται από μη μηδενικό πολυώνυμο με συντελεστές στο F. Συνεπώς, η επέκταση F/L είναι αλγεβρική.

<u>Πόρισμα</u> Έστω E/F επέκταση σωμάτων έτσι ώστε $[E:F]=p$, p πρώτος. Τότε το E είναι απλή επέκταση του F και δεν υπάρχει ενδιάμεσο σώμα L έτσι ώστε $F \subsetneq L \subsetneq E$.

Απόδειξη Αφού $[E:F]=p$, έπεται ότι κάθε στοιχείο του E είναι αλγεβρικό πάνω από το F.

Έστω $a\in E$, $a\notin F$. Τότε το $F\subsetneq F(a)$ και άρα $[F(a):F]\neq 1$.

$[F(a):F]$ διαιρεί το p, άρα $[F(a):F]=p$ και κατά συνέπεια $[E:F(a)]=1$.

Επομένως $F(a)=E$.

Ομάδα Galois

Έστω E/F μία επέκταση σωμάτων. Η ομάδα Galois του E πάνω από το F συμβολίζεται με $Gal(E/F)$ ή $Aut_F(E)$ και είναι το σύνολο των αυτομορφισμών του E που διατηρούν σταθερά τα στοιχεία του F:

$$Gal(E/F):=\{\phi\in Aut(E) : \phi(c)=c,\ \forall c\in F\}$$

Παρατήρηση Έστω F/E επέκταση σωμάτων. Πότε μια συνάρτηση $\phi: E\to E$ είναι στοιχείο της ομάδας Galois $Gal(E/F)$;

Απάντηση: Πρέπει 1. ϕ 1-1 και επί

2. ϕ ομομορφισμός δακτυλίων, δηλαδή $\phi(a+b)=\phi(a)+\phi(b)$ και $\phi(a*b)=\phi(a)*\phi(b)$, $\forall a,b$ στοιχεία του E.

3. $\phi(1_E) = 1_E$

4. $\phi(c) = c$, $\forall c$ στοιχείο του F.

Παρατήρηση Αφού $1_E = 1_F$ το 3. έπεται από το 4.

Παράδειγμα 1 Η ταυτοτική συνάρτηση του E.

Ερώτημα: Βρείτε δύο στοιχεία της ομάδας Galois $Gal(\mathbb{C}|\mathbb{R})$

Απάντηση: Το ένα είναι η ταυτοτική απεικόνιση στο $\mathbb{C}$, η δεύτερη είναι η απεικόνιση συζυγίας

$a+bi$ (απεικονίζεται στο) $a-bi$, για a,b πραγμ.

Πρόταση Έστω $E|F$ μία επέκταση σωμάτων, $a \in E$ αλγεβρικό πάνω από το F και $\sigma \in Gal(E|F)$. Τότε $irr_{(F,a)}(x) = irr_{(F,\sigma(a))}(x)$.

Απόδειξη. Έστω $q(x) = irr_{(F,a)}(x) = \sum c_i x^i$.

Αφού $q(a)=0$, έπεται ότι $\sum c_i a^i = 0$.

Επομένως, $0 = \sigma\left(\sum c_i a^i\right) = \sum \sigma(c_i a^i) = \sum \sigma(c_i)\cdot\sigma(a^i) =$

$\sum c_i \sigma(a)^i = \sum c_i b^i$. άρα $q(x) = irr_{(F,b)}(x)$.

<u>Παράδειγμα</u> Δείξτε ότι $Gal(\mathbb{C}|\mathbb{R}) =$

$\{$ (ταυτοτική του $\mathbb{C}$), (συζυγία στο $\mathbb{C}$) $\}$

έχει τάξη 2.

<u>Απόδειξη</u> Φανερά, (η ταυτοτική του $\mathbb{C}$) και

η (συζυγία στο $\mathbb{C}$) είναι στοιχεία της $Gal(\mathbb{C}|\mathbb{R})$

Έστω ϕ στοιχείο της ομάδας $Gal(\mathbb{C}|\mathbb{R})$

και $z = a+bi$, μιγαδικός με a, b πραγματικός.

Τότε, από ιδιότητες 2 και 4

$$\phi(a+bi) = \phi(a) + \phi(bi) =$$

$$\phi(a) + \phi(b)\cdot\phi(i) = a + b\cdot\phi(i).$$

Από Πρόταση, αφού $irr_{(\mathbb{R},i)} = x^2+1 = (x-i)(x+i)$

έχουμε ότι $\phi(i) = i$ ή $\phi(i) = -i$.

Στην πρώτη περίπτωση, $\phi =$ ταυτοτική του $\mathbb{C}$

στην δεύτερη περίπτωση $\phi =$ (συζυγία στο $\mathbb{C}$).

<u>Θεώρημα</u> Έστω E/F μια επέκταση σωμάτων

και $a, b \in E$ αλγεβρικά πάνω από το F τ.ω.

$irr_{(F,a)}(x) = irr_{(F,b)}(x)$. Τότε υπάρχει ένας ισομορφι-

σμός σωμάτων $\phi : F(a) \to F(b)$ έτσι ώστε

$\phi|_F = id_F$ και $\phi(a) = b$.

<u>Απόδειξη</u> Θεωρούμε το κύριο ιδεώδες I του $F[x]$ που παράγεται από το $irr_{(F,\alpha)}(x)$. Ο επιμορφισμός $\phi_1 : F[x] \to F[\alpha]$, $\phi_1(f(x)) = f(\alpha)$ δίνει τον ισομορφισμό $\bar{\phi}_1 : F[x]/I \to F(\alpha)$,

$$\bar{\phi}_1(f(x)+I) = f(\alpha)$$

Συγκεκριμένα: $\bar{\phi}_1(x+I) = \alpha$, ενώ $\bar{\phi}_1(c+I) = c$, για $c \in F$. Αντίστοιχα έχουμε τον ισομορφισμό $\bar{\phi}_2 : F[x]/I \to F(b)$, $\bar{\phi}_2(f(x)+I) = f(b)$

Επομένως η σύνθεση $\bar{\phi}_2 \circ \bar{\phi}_1^{-1} : F(\alpha) \to F(b)$ έχει τις επιθυμητές ιδιότητες.

<u>Θεώρημα</u> Έστω E/F και E'/F' επεκτάσεις σωμάτων, $b \in E$, $b' \in E'$ αλγεβρικά πάνω από τα F, F' αντίστοιχα και $\sigma : F \to F'$ ισομορφισμός έτσι ώστε $\hat{\sigma}(irr_{(F,b)}(x)) = irr_{(F',b')}(x)$

Υπάρχει ένας ισομορφισμός σωμάτων $\phi : F(b) \to F'(b')$ έτσι ώστε $\phi|_F = \sigma$ και $\phi(b) = b'$

— — — — — — —