19/5/2020 ①

Παράδειγμα 2.3.5.

f). Πως βγαίνει η ισότητα:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2})(-\sqrt{3})$$

<u>Απάντηση</u>

Ισχυρισμός 1. Έστω E/F επέκταση σωμάτων και a_1, a_2 στοιχεία του E. Τότε $(F(a_1))(a_2) = F(a_1, a_2)$.

<u>Απόδ.</u> (εξ ορισμού) $F(a_1, a_2)$ είναι μικρότερο υπόσωμα του E που περιέχει το $F \cup \{a_1, a_2\}$.

Καθώς προφανώς $F \cup \{a_1, a_2\}$ υποσύνολο $(F(a_1))(a_2)$, έπεται

$F(a_1, a_2)$ υποσύνολο $(F(a_1))(a_2)$ (1)

Αντίστροφα, $F \cup \{a_1\}$ υποσύνολο $F(a_1, a_2)$ άρα $F(a_1)$ υποσύνολο $F(a_1,a_2)$

Αφού $F(a_1) \cup \{a_2\}$ υποσύνολο $F(a_1, a_2)$, έπεται $(F(a_1))(a_2)$ υποσύνολο $F(a_1, a_2)$. (2)

Από (1) και (2) έπεται

$$F(a_1, a_2) = (F(a_1))(a_2).$$

Ισχυρισμός 2 $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2})(-\sqrt{3})$ ②

Απάντηση $\mathbb{Q}(\sqrt{2})(\sqrt{3})$. είναι το μικρότερο υπόσωμα του $\mathbb{C}$ που περιέχει το

$\mathbb{Q}(\sqrt{2}) \cup \{\sqrt{3}\}$.

Αφού $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ υπόσωμα του $\mathbb{C}$ που περιέχη το $\sqrt{3}$, θα περιέχη και το αντίθετο του. Άρα, $\mathbb{Q}(\sqrt{2}) \cup \{-\sqrt{3}\}$ υποσύνολο $\mathbb{Q}(\sqrt{2})(\sqrt{3})$, συνεπώς $\mathbb{Q}(\sqrt{2})(-\sqrt{3})$ υποσύνολο $\mathbb{Q}(\sqrt{2})(\sqrt{3})$.

Επιπλέον, $\mathbb{Q}(\sqrt{2})(-\sqrt{3})$ είναι το μικρότερο υπόσωμα του $\mathbb{C}$ που το $\mathbb{Q}(\sqrt{2}) \cup \{-\sqrt{3}\}$. Αφού $\mathbb{Q}(\sqrt{2})(-\sqrt{3})$ το υπόσωμα του $\mathbb{C}$ που περιέχη το $-\sqrt{3}$, θα περιέχη και το αντίθετο του, και $-(-\sqrt{3}) = \sqrt{3}$.

Άρα $\mathbb{Q}(\sqrt{2}) \cup \{\sqrt{3}\}$ υποσύνολο $\mathbb{Q}(\sqrt{2})(-\sqrt{3})$ συνεπώς $\mathbb{Q}(\sqrt{2})(\sqrt{3})$, υποσύνολο $\mathbb{Q}(\sqrt{2})(-\sqrt{3})$

(2) Η σύνθεση $\sigma_3 = \sigma_1 \circ \sigma_2$ ανήκει στην G επειδή τα σ_1, σ_2 ανήκουν στη G και αυτή είναι ομάδα;

Απάντηση Ναι, ακριβώς.

(3) $|G| \leq 4$

Απόδειξη: Χρησιμοποιούμε το εξής.

Ορισμός Έστω F σώμα. Ορίζουμε πολυωνυμικό δακτύλιο σε δύο μεταβλητές x, y ως εξής: $F[x,y] = (F[x]).[y]$. Σαν πόρισμα, $F[x,y]$ περιέχει τα στοιχεία $c \cdot x^i \cdot y^j$ με $c \in F$, i, j μη αρν. ακέραιος, καθώς και τα πεπερασμένα αθροίσματα αυτών

Πρόταση Έστω E/F επέκταση σωμάτων και a_1, a_2 στοιχεία του E. Τότε:

1) $F[a_1] = \{p(a_1) : p$ στοιχείο του $F[x]\}$.

2) $F(a_1) = \{p(a_1)/q(a_1) : p, q$ στοιχεία του $F[x]$ και $q(a_1)$ μη μηδενικό$\}$

3) $F(a_1, a_2) = \{p(a_1, a_2)/q(a_1, a_2) : p, q$ στοιχεία του $F[x,y]$ και $q(a_1, a_2)$ μη μηδενικό

Ισχυρισμός Έστω σ, τ στοιχεία του $Gal(F(a_1, a_2)/F)$. Υποθέτουμε

$\sigma(a_1) = \tau(a_1)$ και $\sigma(a_2) = \tau(a_2)$.

Τότε $\sigma = \tau$.

Απόδ.

Έστω u στοιχείο του $F(a_1, a_2)$

Τότε υπάρχουν p, q στοιχεία του $F[x, y]$ ώστε $q(a_1, a_2)$ μη μηδενικό

και $u = p(a_1, a_2)/q(a_1, a_2)$

Αφού σ, τ ισομορφισμοί δακτυλίων διατηρούν την διαίρεση και έχουμε

$\sigma(u) = \sigma(p(a_1, a_2))/\sigma(q(a_1, a_2))$,

$\tau(u) = \tau(p(a_1, a_2))/\tau(q(a_1, a_2))$

Θέτουμε $b_1 = \sigma(a_1)$, $b_2 = \sigma(a_2)$

Άρα $b_1 = \tau(a_1)$, $b_2 = \tau(a_2)$.

$\sigma(c(a_1)^i \cdot (a_2)^j) = \sigma(c) \cdot \sigma((a_1)^i \sigma(a_2^j)) = c$

$(\sigma(a_1))^i \cdot (\sigma(a_2))^j = c(\sigma(a_1))^i (\sigma(a_2))^j =$

$c(b_1)^i \cdot (b_2)^j$

Άρα, $\sigma(c(a_1)^i(a_2)^j) = \tau(c(a_1)^i(a_2)^j)$

Αφού τα $p(a_1, a_2)$, $q(a_1, a_2)$ είναι πεπερασμένα αθροίσματα τέτοιων όρων και σ, τ ισομορφισμός δακτυλίων έπεται $\sigma(p(a_1, a_2)) = \tau(p(a_1, a_2))$ και $\sigma(q(a_1, a_2)) = \tau(q(a_1, a_2))$

Σαν συνέπεια $\sigma(u) = \tau(u)$, άρα $\sigma = \tau$.

Για το 2.3.6

1) Γιατί το E είναι το σώμα ανάλυσης του $x^3 - 2$ πάνω από το $\mathbb{Q}$;

Απάντηση: Γιατί οι b, ωb, $\omega^2 b$ είναι οι 3 ρίζες του $x^3 - 2$ στο $\mathbb{C}$.

(2) Πως προκύπτει η σειρά ισοτήτων:

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

Παρατήρηση Έστω E/F επέκταση σωμάτων και $a_1, \dots, a_n$ και $b_1, \dots, b_m$ στοιχεία του E. Έχουμε $F(a_1, \dots, a_n) = F(b_1, \dots, b_m)$ αν-ν a_i στοιχείο του $F(b_1, \dots, b_m)$, $\forall i$ και b_j στοιχείο το $F(a_1, \dots, a_n)$, $\forall j$.

Απόδειξη Ισότητας $E = \mathbb{Q}(b, \omega^2 b)$

Αφού $E = \mathbb{Q}(b, \omega b, \omega^2 b)$ για να δείξουμε την ισότητα αρκεί να δείξουμε ότι ωb στοιχείο του $\mathbb{Q}(b, \omega^2 b)$ που ισχύει γιατί

$\omega b = (\omega^2 b)^2 / b$, αφού $\omega^4 = \omega$.

Απόδειξη Ισότητας $E = \mathbb{Q}(\omega, b, \omega^2 b)$

Αφού $E = \mathbb{Q}(b, \omega b, \omega^2 b)$, για να δείξουμε την ισότητα αρκεί να δείξουμε ότι ω στοιχείο του E και ωb στοιχείο του $\mathbb{Q}(\omega, b, \omega^2 b)$.

Έχουμε $\omega = \omega b / b$, άρα στοιχείο του E, γιατί E σώμα. Αφού ω, b στοιχεία του $\mathbb{Q}(\omega, b, \omega^2 b)$ και $\mathbb{Q}(\omega, b, \omega^2 b)$ σώμα έπεται ωb στοιχείο του $\mathbb{Q}(\omega, b, \omega^2 b)$.

Απόδειξη Ισότητας $E = \mathbb{Q}(\omega, b)$.

Αφού $E = \mathbb{Q}(b, \omega b, \omega^2 b)$, για να δείξουμε την ισότητα αρκεί να δείξουμε ότι ω στοιχείο του E και $\omega b, \omega^2 b$ στοιχεία του $\mathbb{Q}(\omega, b)$. Το ότι ω στοιχείο του E, δείχτηκε παραπάνω. Το ότι $\omega b, \omega^2 b$ στοιχείο του

$\mathbb{Q}(\omega, b)$ έπεται γιατί $\mathbb{Q}(\omega,b)$ σώμα (7)
που περιέχει το ω και b.

(3) Γιατί ισχύει $irr_{(\mathbb{Q}(\omega),b)}(x) =$
$irr_{(\mathbb{Q},b)}(x) = x^3 - 2$;

Απόδειξη Έχουμε ότι το
$irr_{(\mathbb{Q}(\omega),b)}(x)$ διαιρεί το $irr_{(\mathbb{Q},b)}(x)$,
γιατί διαιρεί κάθε πολυώνυμο με συντελεστές
στο $\mathbb{Q}(\omega)$ που μηδενίζεται στο b, και το
$irr_{(\mathbb{Q},b)}(x)$ είναι ένα από αυτά.
Συνεπώς, degree $irr_{(\mathbb{Q}(\omega),b)}(x) \leq 3$.
Επίσης, ξέρουμε ότι degree $irr_{(\mathbb{Q}(\omega),b)}(x) =$
$[\mathbb{Q}(\omega,b) : \mathbb{Q}(\omega)]$.
Επομένως, αρκεί να δείξουμε ότι $[\mathbb{Q}(\omega,b) : \mathbb{Q}(\omega)] = 3$
που ισχύει, γιατί ξέρουμε
$[\mathbb{Q}(\omega,b) : \mathbb{Q}] = 6$, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ και από
Πρόταση $[\mathbb{Q}(\omega,b) : \mathbb{Q}] = [\mathbb{Q}(\omega,b) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}]$.

Ορισμός: Έστω F σώμα και $f(x) \in F[x]$. ⑧

Η ομάδα Galois του $f(x)$ είναι η ομάδα $Gal(E/F)$, όπου E είναι το σώμα ανάλυσης του $f(x)$ πάνω από το F.

Πόρισμα: Έστω $f(x) \in F[x]$ διαχ. πολυώνυμο και E ένα σώμα ανάλυσης του $f(x)$. Τότε $|Gal(E/F)| = [E:F]$.

Παράδ. 3.2.5

1) $E = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$. E σώμα ανάλυσης του διαχ. πολυων. $f(x) = (x^2-2)(x^2-3)(x^2-5)$ πάνω από το Q. $[E:Q] = 8$

Q υποσύνολο $Q(\sqrt{2})$ υποσύνολο $Q(\sqrt{2}, \sqrt{3})$ υποσύνολο $Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Αφού το $\sqrt{2}$ δεν είναι ρητός, και είναι ρίζα του πολυωνύμου x^2-2, έχουμε $[Q(\sqrt{2}):Q] = 2$. Έχουμε δείξει ότι το $\sqrt{3}$ δεν είναι στοιχείο του $Q(\sqrt{2})$, άρα $[Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{2})] \geq 2$

Επιπλέον, το $\sqrt{3}$ είναι ρίζα του πολυωνύμου x^2-3 που έχει συντελεστές στο $Q(\sqrt{2})$.

Συνεπώς

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$$

άρα $\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

Συνεπώς,

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Ισχυρ.: Το $\sqrt{5}$ δεν είναι στοιχείο του $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Συνεπώς, $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}(\sqrt{2},\sqrt{3})] \geq 2$

Επιπλέον, $\sqrt{5}$ είναι ρίζα του πολυωνύμου x^2-5.

Συνεπώς, $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}(\sqrt{2},\sqrt{3})] = 2$

Επομένως, $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}] =$

$$(\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}] : \mathbb{Q}[\sqrt{2},\sqrt{3}]) \cdot ([\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}])$$

$$= 2 \cdot 4 = 8.$$

Παράδ. 3.2.6
Ισχυρισμός: Η ομάδα Galois $f(x)$ επί του $\mathbb{Q}$ είναι ισόμορφη με την S_5.

Συμπέρασμα Χρησιμοποιώντας Θ. Galois και ότι η ομάδα S_5 είναι δεν είναι επιλύσιμη. Οι ρίζες του $f(x)$ στους μιγαδικούς ΔΕΝ μπορούν να γραφούν με ριζικά.

Ενδιάμεσα σώματα και υποομάδες της ομάδας Galois.

Πρόταση Έστω B ενδιάμεσο σώμα της επέκτασης E/F. τότε $Gal(E/B)$ είναι υποομάδα της $Gal(E/F)$.

Θεώρημα Έστω $f(x) \in F[x]$. και E το σώμα ανάλυσης του $f(x)$ πάνω από το F. Αν το B είναι ενδιάμεσο σώμα της επέκτασης E/F και είναι σώμα ανάλυσης του $g(x) \in F[x]$ πάνω από το F, τότε $Gal(E/B)$ είναι κανονική υποομάδα της $Gal(E/F)$ και $Gal(E/F) / Gal(E/B) \cong Gal(B/F)$.

Απόδειξη

F (υπόσωμα) B (υπόσωμα) E και επιπλέον υπόθεση ότι υπάρχει g στοιχείο του $F[X]$ με την ιδιότητα B σώμα ριζών του g.

Ισχυρισμός 1. Έστω T στοιχείο της $Gal(E/F)$. Τότε $T(B)$ υποσύνολο του B.

Απόδειξη Έχουμε $T: E \to E$.

Έστω $b_1, \dots, b_r$ οι ρίζες του g στο E. Τότε $B = F(b_1, \dots, b_r)$. Από Πρόταση, για κάθε i, $T(b_i)$ ρίζα του g, γιατί b_i ρίζα του g. Συνεπώς, υπάρχει j με $T(b_i) = b_j$. Άρα $T = (b_i)$ στοιχείο του B.

Αφού T περιορισμένο στο F είναι η ταυτοτική στο F έπεται ο Ισχυρισμός 1.

Ισχυρισμός 2 Έστω T στοιχείο της $Gal(E/F)$. Τότε $T(B) = B$.

Απόδειξη Έχουμε $B = F(b_1, \ldots, b_r)$.

Αφού T 1-1 η παραπάνω απόδ. μας δίνει ότι η T επάγει 1-1 απεικόνιση ρ από το πεπερασμένο σύνολο $\{b_1, \ldots, b_r\}$ στον εαυτό του. Άρα η ρ είναι επί.

Συνεπώς, κάθε b_j είναι στην εικόνα του $T(B)$.

Αφού T ισομορφισμός ομάδων, το $T(B)$ είναι υπόσωμα του E που περιέχει το F και κάθε b_j. Άρα B υποσύνολο του $T(B)$. Από ισχυρισμό 1, $T(B)$ υποσύνολο του B. Συνεπώς $T(B) = B$.

Ορισμός: Ορίζουμε την απεικόνιση

$A: Gal(E/F) \to Gal(B/F)$ με

$A(T) = T$ περιορισμένη στο B.

Τότε η A είναι καλά ορισμένος επιμορφισμός ομάδων και $\ker A = Gal(E/B)$

Άρα, η $Gal(E/B)$ είναι κανονική υποομάδα της $Gal(E/F)$ και το πηλίκο είναι ισόμορφο με το $Gal(B/F)$.

<u>ΑΠΟΔΕΙΞΗ</u> Αφού από ισχ. 2, $\tau(B) = B$,

και η τ είναι 1-1 και επί ομομορφισμός δακτυλίων που περιορισμένη στο F είναι ταυτοτική έπεται ότι η $A(\tau): B$ στο B είναι και αυτή 1-1 και επί ομομορφισμός δακτυλίων που περιοριζόμενη στο F είναι η ταυτοτική. Συνεπώς A καλώς ορισμένη.

Η A ομομορφ. ομάδων, γιατί ο περιορισμός της σύνθεσης στο B είναι ίσος με την σύνθεση των περιορισμών δύο συναρτήσεων. Φανερά, τ στοιχείο του πυρήνα της A αν-ν ο περιορισμός της τ στο B είναι η ταυτοτική του B, το οποίο είναι ισοδύναμο με τ στοιχείο της $Gal(E/B)$.

Μένει να δείξουμε ότι A είναι επί.

Με άλλα λόγια, ότι αν τ_1 στοιχείο του $Gal(B/F)$, τότε υπάρχει τ στοιχείο του $Gal(E/F)$, ώστε $\tau_1 =$ ο περιορισμός της τ στο B.

Εδώ θα χρησιμοποιούμε την έξτρα υπόθεση.

(έξτρα υπόθεση: ότι υπάρχει f στοιχείο του $F[X]$ με την ιδιότητα E σώμα ριζών του f επί του F και το τεχνικό Θεώρημα 3.2.1).

Παράδειγμα $F = \mathbb{Q}$ (υπόσωμα) $B = \mathbb{Q}(\omega)$ (υπόσωμα) $E = \mathbb{Q}(b, \omega)$.

Στόχος: Έστω E/F επέκταση σωμάτων.

Θέτουμε $G = Gal(E/F)$

Συμβολίζουμε cal A το σύνολο των υποσ. του E που περιέχουν το F.

Συμβολίζουμε cal B το σύνολο των υποομάδων της G.

Ορίζουμε τις απεικονίσεις φ : cal A $\to$ cal B και ψ : cal B $\to$ cal A ως εξής:

$\varphi(B)$ η υποομάδα $Gal(E|B)$ της G.

$\psi(H) = E^H$, δηλ. $\psi(H) = \{u : u$ στοιχείο της E και $\sigma(u) = u$, $\forall \sigma \in H\}$.

Ερώτημα Ισχύει φ, ψ 1-1 και επί;

Ισχύει πιο ισχυρά $\varphi = \psi^{-1}$;

Απάντηση Ναι, υπό προϋποθέσεις για την επέκταση E/F. Όχι πάντως γενικά.

Ερώτημα Όταν ισχύει $\varphi = \psi^{-1}$, γιατί είναι χρήσιμο;

Απάντηση Η G είναι πεπερασμένη ομάδα και συχνά είναι εύκολο να υπολογίσουμε το calB. Άρα αφού ισχύει και $\varphi = \psi^{-1}$ μπορούμε να υπολογίσουμε το calA, δηλαδή το σύνολο των ενδιάμεσων υποσωμάτων της επέκτασης E/F!!!