25/5/2020

Παράδειγμα 3.2.5

(1) Πως από το ότι $\sqrt{3}$ είναι ρίζα του πολυωνύμου x^2-3, που έχει συντελεστές στο $Q(\sqrt{2})$, προκύπτει ότι: $[Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})] \leq 2$;

Απάντηση

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

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

degree $irr_{Q(\sqrt{2})(\sqrt{3})}(x)$

Αφού το $\sqrt{3}$ είναι ρίζα του x^2-3, που έχει συντελεστές στο $Q(\sqrt{2})$ έπεται ότι το $irr_{Q(\sqrt{2})(\sqrt{3})}(x)$ διαιρεί το x^2-3, συνεπώς degree $irr_{Q(\sqrt{2},\sqrt{3})}(x) \leq 2$.

(2) Έχουμε Q υπόσωμα F υπόσωμα E.

Γιατί $Gal(E/F)$ υποσύνολο $Gal(E/Q)$ και επίσης, πως δείχνεται αναλυτικά ότι

$[Gal(E/Q):Gal(E/F)]=2$;

Απάντηση Από τον ορισμό αν σ στοιχείο του $Gal(E/F)$ η $\sigma: E \to E$ είναι ισομορφισμός δακτυλίων που περιοριζόμενη στο F είναι η ταυτοτική του F. Αφού Q υποσύνολο του F, η $\sigma: E \to E$ είναι ισομορφισμός δακτυλίων που περιοριζόμενη στο Q είναι η ταυτοτική του Q. Άρα σ στοιχείο του $Gal(E/Q)$. Επίσης, από τον ορισμό του δείκτη υποομάδας πεπερασμένης υποομάδας,

$$[Gal(E/Q) : Gal(E/F)] = \# Gal(E/Q) / \# Gal(E/Q) = 6/3 = 2.$$

Παράδειγμα 3.2.6.

Πως από το ότι $char(Q) = 0$ προκύπτει ότι το $f(x)$ έχει 5 διαφορετικές ρίζες.

Απάντηση Από το Πόρισμα 1.4.6 το $f(x)$ είναι διαχωρίσιμο επί του Q. Επίσης, είναι ανάγωγο επί του Q. Άρα, οι ρίζες του, σε οποιαδήποτε επέκταση σωμάτων F του Q στο οποίο το $f(x)$ αναλύεται σε γινόμενο πρωτοβάθμιων είναι απλές.

Αφού είναι βαθμού 5, σαν συνέπεια θα έχει 5 διαφορετικές ρίζες.

Παρατήρηση Πιο γενικά αν F σώμα χαρακτηριστικής 0, $g(x)$ ανάγωγο πολυώνυμο επί του F βαθμού n.

E/F επέκταση σωμάτων ώστε το $g(x)$ να αναλύεται σαν γινόμενο πρωτοβαθμίων επί του E.

Από το πόρισμα έπεται ότι το $g(x)$ έχει ακριβώς n διαφορετικές ρίζες στο E.

Η υπόθεση F σώμα χαρακτηριστικής 0, μπορεί να αντικατασταθεί με το ΜΚΔ ($g(x)$, παράγωγος του $g(x)$ ως προς x) $= 1$.

Εμφύτευση σωμάτων

Αν F, E σώματα μια εμφύτευση σωμάτων από το F στο E είναι, εξ' ορισμού, ένας 1-1 ομομορφισμός δακτυλίων $g: F \to E$.

- Στο παράδειγμα 3.3.5(2), γιατί η E^G ισόμορφη με την E

Απάντηση

Αφού η G περιέχει μόνο την ταυτοτική του E, και αυτή στέλνει το E στο E, έπεται ότι $E^G = E$, δηλ. ισότητα συνόλων.

Στο 3.3.5(3) πως καταλήγουμε στην ισότητα $E^H = Q(\omega)$ από το ότι δεν υπάρχει ενδιάμεσο σώμα B_j

Απάντηση

Έχουμε $\sigma(b) \neq b$ και σ στοιχείο του H.

Άρα b όχι στοιχείο του E^H, άρα E^H διάφορο του E. Από τη θεωρία το E^H είναι ένα υπόσωμα του E που περιέχει το $Q(\omega)$.

Αφού δεν υπάρχει ενδιάμεσο σώμα B, έπεται $E^H = E$ ή $E^H = Q(\omega)$.

Το πρώτο όμως δείξαμε ότι δεν ισχύει.

Ορισμός

Έστω F σώμα και $g(x)$ μη σταθερό στοιχείο του $F[X]$. Συμβολίζουμε με E_g ένα σώμα ανάλυσης του $g(x)$. Εξ ορισμού, η ομάδα Galois του $g(x)$ επί του F είναι η ομάδα $Gal(E_g/F)$.

Ως προς ισομορφισμό, δεν εξαρτάται από την επιλογή του E_g.

Παρατήρηση

Υποθέτουμε $F = Q$ και $g(x)$ ανάγωγο πολυώνυμο στο $Q[X]$ βαθμού n. Έστω $b_1, \dots, b_n$ οι ρίζες του $g(x)$

στο E. Έχουμε δει, ότι με φυσιολογικό τρόπο η $Gal(E_g/F)$ μπορεί να θεωρηθεί υποομάδα της $S_n = \{ f : \{b_1, \dots, b_n\}$ στο $\{b_1, \dots, b_n\}$ με f 1-1 και επί $\}$.

Ερώτημα Υπολογίστε την ομάδα $Gal(E_g/F)$.

Εκτός Ύλης

Ορισμός Η επέκταση E/F λέγεται επέκταση Galois αν το E είναι σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου $f(x) \in F[x]$.

Θεώρημα

Έστω E/F πεπερασμένη επέκταση. Τότε $[E : E^G] \geq n$, όπου $G = Gal(E/F)$ και n η τάξη της G.

Θεώρημα

Έστω E/F μία πεπερασμένη επέκταση σωμάτων έτσι ώστε $E^{Gal(E/F)} = F$. Κάθε ανάγωγο πολυώνυμο $p(x) \in F[x]$ που έχει μια ρίζα στο E είναι διαχωρίσιμο και έχει όλες του τις ρίζες στο E

Θεώρημα

Έστω E/F μία πεπερασμένη επέκταση σωμάτων και $G = Gal(E/F)$. Οι επόμενες συνθήκες είναι ισοδύναμες:

i. Η επέκταση E/F είναι επέκταση του Galois.

ii. $F = E^{G} = \{a \in E : \sigma(a) = a, \ \forall \sigma \in G\}$

iii. Κάθε ανάγωγο πολυώνυμο $p(x) \in F[X]$ που έχει μία ρίζα στο E είναι διαχωρίσιμο και έχει όλες τις ρίζες του στο E.

Θεμελιώδες Θεώρημα της Θεωρίας Galois

Έστω E/F μία επέκταση του Galois $G = Gal(E/F)$. Τότε υπάρχει μία αμφιμονότιμη και επί συνάρτηση f μεταξύ των στοιχείων του συνόλου A των ενδιάμεσων σωμάτων της επέκτασης E/F και των στοιχείων του συνόλου D των υποομάδων της G:

$f : A \to D$, $B \mapsto Gal(E/B)$.

Αντίστροφα, αν H είναι υποομάδα της G τότε η αντιστοιχία $\phi : D \to A$, $H \mapsto E^{H}$ έχει τις εξής ιδιότητες.

i. $[B : F] = [G : Gal(E/B)]$ και $[G : H] = [E^{H} : F]$

ii. $E^{Gal(E/B)} = B$ και $Gal(E/E^{H}) = H$.

7

iii. $B|F$ είναι η επέκταση Galois αν-ν $Gal(E|B) \trianglelefteq G$.

<u>Παρατήρηση</u> Οι συναρτήσεις f και φ του θεμελιώδους θεωρήματος της θεωρίας Galois. αντιστρέφουν την διάταξη.
Πράγματι, έστω H_1 υποομάδα H_2 υποομάδα G. Τότε E^{H_2} υπόσωμα E^{H_1}, γιατί u στοιχείο E^{H_2}, συνεπάγεται $\sigma(u)=u$ για κάθε στοιχείο σ της H_2, άρα αφού H_1 υποομάδα H_2.

$\sigma(u)=u$ για κάθε στοιχείο σ της H_1, συνεπώς u στοιχείο E^{H_1}. Αντίστροφα, έστω F υπόσωμα B_1 υπόσωμα B_2 υπόσωμα E.
Τότε $Gal(E/B_2)$ υποομάδα της ομάδας $Gal(E/B_1)$, γιατί αν $\sigma: E \to E$ ισομορφισμός δακτυλίων με σ περιοριζόμενο στο B_2 η ταυτοτική απεικόνιση του B_2, τότε αφού B_1 υπόσωμα B_2 και σ περιοριζόμενο στο B_1 η ταυτοτική του B_1.

<u>Πόρισμα</u>: Έστω E/F μία επέκταση Galois. Η επέκταση έχει πεπερασμένο αριθμό ενδιαμέσων σωμάτων.

<u>Προσοχή</u> Υπάρχουν πεπερασμένες επεκτάσεις σωμάτων E/F με $[E:F]$ πεπερασμένο ώστε το σύνολο των ενδιαμέσων σωμάτων να είναι άπειρο!!! Φυσικά, δεν είναι Galois, γιατί από το Πόρισμα αν E/F Galois με $[E:F]$ πεπερασμένο, το σύνολο των ενδιαμέσων σωμάτων είναι πεπερασμένο.

$f(x) \in F[X]$ ένα κανονικό, ανάγωγο, διαχωρίσιμο πολυώνυμο n βαθμού, E σώμα ανάλυσης του $f(x)$ πάνω ~~στο~~ από το F και $X = \{a_1, \dots, a_n\} \subset E$ το σύνολο των ριζών του $f(x)$. Με Δ συμβολίζουμε το στοιχείο $\Delta = \prod_{i<j}(a_i - a_j) \in E$.

Προκύπτει ότι $\sigma \in Gal(E/F)$, τότε $\sigma(\Delta) = \pm \Delta$

Παράδειγμα

a_1, a_2, a_3 $\quad \Delta = (a_1 - a_2)\cdot(a_2 - a_3)\cdot(a_1 - a_3)$

σ μεταθέτει τις ρίζες.

Έστω για παράδειγμα $\sigma(a_1) = a_2$,

$\sigma(a_2) = a_1$, $\quad \sigma(a_3) = a_3$

Τότε $\sigma(\Delta) = (a_2 - a_1)(a_1 - a_3)(a_2 - a_3) = -\Delta =$

(πρόσημο σ) $* \Delta$.

$\sigma(a_1) = a_2 \quad \sigma(a_2) = a_3 \quad \sigma(a_3) = a_1$.

Τότε $\sigma(\Delta) = (a_2 - a_3)(a_3 - a_1)(a_2 - a_1) = \Delta$