27/4/2020

<u>Ορισμός</u>: Έστω E/F μία επέκταση σωμάτων. Ο βαθμός του E πάνω από το F συμβολίζεται με $[E:F]$ και ισούται με τη διάσταση του E ως F-διανυσματικού χώρου.

<u>Παρ. 2.17)</u> 4. Δύσκολο θεώρημα: το π είναι υπερβατικό επί του $\mathbb{Q}$.

<u>Πρόταση 2.1.8</u> Αν E είναι ενδιάμεσο σώμα της επέκτασης L/F και $[E:F]=\infty$ τότε $[L:F]=\infty$

<u>Ορισμός</u> Έστω E/F μία επέκταση σωμάτων και $a \in F$ αλγεβρικό πάνω από το F. Το μοναδικό κανονικό ανάγωγο πολυώνυμο του $F[x]$ που έχει το a ως ρίζα, ονομάζεται το ανάγωγο πολυώνυμο του a πάνω από το F και συμβολίζεται με $irr_{(F,a)}(x)$. Οι ρίζες του $irr_{(F,a)}(x)$ λέγονται συζυγή στοιχεία του a.

Παρατήρηση: Έστω F υπόσωμα του E και a στοιχείο του E αλγεβρικό επί του F 1) Τότε το $irr_{(F,\alpha)}(x)$ είναι ένα μη σταθερό, ανάγωγο, μονικό στοιχείο του πολυωνυμικού δακτυλίου $F[x]$ με την ιδιότητα $g(a)=0$.

2) Αν h μη μηδενικό του $F[x]$ με την ιδιότητα $h(a)=0$, τότε το g διαιρεί το h στο $F[x]$.

3) Έστω h μη μηδενικό μονικό στοιχείο του $F[x]$, με την ιδιότητα $h(a)=0$. Τα ακόλουθα είναι ισοδύναμα.

Αν h ανάγωγο, τότε $h = irr_{(F,a)}(x)$.

4) Έστω h μη μηδενικό μονικό στοιχείο του $F[x]$, με την ιδιότητα $h(a)=0$. Αν δεν υπάρχει μη μηδενικό πολυώνυμο q γνήσια μικρότερου βαθμού από το h, με την ιδιότητα $q(a)=0$, τότε $h= irr_{(F,a)}(x)$.

Τα 3,4 είναι χρήσιμα για να αποφανθούμε $h = irr_{(F,a)}(x)$.

5) Έστω $d = \text{degree } irr_{(F,a)}(x)$. Τότε αν 1 (μικρότερο ή ίσο) m (μικρότερο ή ίσο) $d-1$, και q στοιχείο του $F[x]$ μη μηδενικό, με $\text{degree } q = m$, τότε $q(a)$ διάφορο του 0.

6) Επιπλέον, $F(a) = F[a]$ και $\text{degree } irr_{(F,a)}(x) = [F(a):F]$, δηλαδή $d = \dim_F F(a)$.

7) Έστω h μη μηδενικό μονικό στοιχείο του $F[x]$, με την ιδιότητα $h(a) = 0$. Έστω $d = [F(a):F]$. Τότε $h = irr_{(F,a)}(x)$ αν και μόνο αν $\text{degree}(h) = d$.

Παράδειγμα 2.2.2.

1. Έστω F υπόσωμα του E και a στοιχείο του E αλγεβρικό επί του F.
Αν το a είναι στοιχείο του F, τότε $irr_{(F,a)}(x) = x - a$. Επιπλέον, $\text{degree } irr_{(F,a)}(x) = 1$ αν και μόνο αν a στοιχείο του F.
(διορθωμένο!)

2. $\mathbb{R}/\mathbb{Q}$ επέκταση και $a=\sqrt{3}$. Αφού $a \notin \mathbb{Q}$ έπεται degree $irr_{(F,a)}(x) \geq 2$. Αφού $\sqrt{3}$ είναι ρίζα του x^2-3 έπεται ότι $irr_{(\mathbb{Q},a)}(x) = x^2-3$.

3. $\omega = \cos(2\pi/p) + i\cdot\sin(2\pi/p)$, δηλ. ω είναι η αρχική p-ρίζα της μονάδος στους μιγαδικούς. $\omega = e^{2\pi i/p} \in \mathbb{C}$

Το ω είναι ρίζα του $\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1$. Φ_p ανάγωγο στο $\mathbb{Q}$, άρα

$$irr_{(\mathbb{Q},\omega)}(x) = \Phi_p(x) = x^{p-1} + x^{p-2} + \dots + 1.$$

5) Τυπογραφικό: $irr_{(\mathbb{R},z)}(x) = x^2 - 2Re(z)\cdot x + z\cdot\bar{z}$.

Θεώρημα Έστω E/F μία επέκταση σωμάτων, $a \in E$ αλγεβρικό πάνω από το F και $\deg irr_{(F,a)}(x) = n$. Το σύνολο $\{1, a, \dots, a^{n-1}\}$ αποτελεί βάση του F-διαν. χώρου $F(a)$ και $[F(a):F] = n$.

Απόδειξη Θέτουμε $f(x) = irr_{(F,a)}(x)$ και $B = \{1, a, \dots, a^{n-1}\}$. Έστω $g(a) \in F[a]$ τυχαίο, όπου $g(x) \in F[x]$.

Σύμφωνα, με τον Ευκλ. Αλγ.

$$g(x) = f(x)p(x) + r(x), \text{ όπου } p(x), r(x) \in F[x]$$

και $t = \deg r(x) < n$. Δηλ. $r(x) = c_t x^t + \dots + c_1 x + c_0 \cdot 1$.

και όει το $g(a)$ είναι F-γραμμ. συνδ. στοιχείων του συνόλου B. Θ.δ.ο. το B είναι γραμμ. ανεξ. Έστω $d_0 \cdot 1 + \dots + d_n \cdot a^{n-1} = 0$, $d_i \in F$, για $i = 0, \dots, n-1$ μία σχέση γραμμ. εξάρτησης των a^i: $0 \leq i \leq n-1$. Αν $h(x) = d_0 + d_1 x + \dots + d_n x^{n-1}$. Τότε $h(a) = 0$ και $h(x) \in (f(x))$. Αν $h(x) \neq 0$, οδηγούμαστε σε άτοπο, αφού $\deg h(x) < \deg f(x)$. Επομένως, $h(x) = 0$ και άρα $d_i = 0$, για $i = 0, \dots, n-1$.

<u>Πόρισμα</u> Τα ανάγωγα πολυώνυμα του δακτυλίου $\mathbb{R}[x]$ έχουν βαθμό 1 ή 2. Αν $a \in \mathbb{C}$ είναι ρίζα του $f(x) \in \mathbb{R}[x]$ τότε $\bar{a}$ είναι ρίζα του $f(x)$.

<u>Ορισμός</u> Έστω E/F επέκταση σωμάτων. Το σώμα E λέγεται αλγεβρικό πάνω από το F αν κάθε στοιχείο του E είναι αλγεβρικό πάνω από το F και

Σε αυτήν την περίπτωση η επέκταση E/F λέγεται αλγεβρική.

Πρόταση Έστω E/F μία επέκταση σωμάτων έτσι ώστε $[E:F]<\infty$. Τότε η επέκταση E/F είναι αλγεβρική.

Ορισμός 2.2.9 Έστω E/F επέκταση σωμάτων $a_1, \dots, a_n \in E$. Ορίζουμε $F[a_1, \dots, a_n]$ να είναι το σύνολο $F[a_1, \dots, a_n] = \{ f(a_1, \dots, a_n) : f(x_1, \dots, x_n) \in F[x_1, \dots, x_n] \}$.

Θεώρημα Έστω F ένα σώμα και $f(x) \in F[x]$. Τότε υπάρχει επέκταση σωμάτων L/F, τ.ω. $[L:F]<\infty$ και το L να είναι ένα σώμα ανάλυσης του $f(x)$ πάνω από το F.

Απόδειξη υπάρχει επέκταση E/F, τ.ω. το $f(x)$ να αναλύεται σε γραμμ. παράγ. στο $E[x]$. Έστω ότι $f(x) = \prod_{i=1}^{n} (x-a_i)$, $a_i \in E$.

Είναι η ανάλυση του $f(x)$ σε γινόμενο γραμμικών παραγόντων στο $E[x]$, όπου $n = \deg f(x)$.
Θεωρούμε το σώμα $L := F(a_1, \dots, a_n)$. Είναι φανερό ότι το L είναι σώμα ανάλυσης του $f(x)$ πάνω από το F.

<u>Ερώτημα</u> Έστω F σώμα και g μη σταθερό πολυώνυμο στο $F[x]$ βαθμού 5.
Έστω L_1/F και L_2/F δύο επεκτάσεις σωμάτων, ώστε το g να αναλύεται πλήρως στα $L_1(x)$ και $L_2(x)$.

Μπορεί να συμβεί το g να έχει ακριβώς δύο ρίζες στο L_1 και ακριβώς 3 στο L_2;
Δηλαδή, μπορεί $f = (x-a_1)^2 \cdot (x-a_2)^3$ στο $L_1[x]$, με a_1, a_2 στο L_1 διαφορετικά, ενώ
$f = (x-b_1)^2 \cdot (x-b_2)^2 \cdot (x-b_3)$ στο $L[x]$, με b_1, b_2, b_3 στο L_2 διαφορετικά ανά δύο;

Απάντηση Θα δούμε πως όχι.

Αν $f=(x-a_1)^2\cdot(x-a_2)^3$ στο $L_1[x]$ με a_1, a_2 στο L_1 διαφορετικά τότε αναγκαστικά υπάρχουν b_1, b_2 στο L_2 διαφορετικά, με $f=(x-b_1)^2\cdot(x-b_2)^3$ στο $L_2[x]$.

Παράδειγμα Θα αποδ. ότι $\mathbb{Q}[\sqrt{2},\sqrt{3}]=\mathbb{Q}[\sqrt{2}+\sqrt{3}]$

Θέτουμε $c=\sqrt{2}+\sqrt{3}$

Ισχυρισμός 1, c αλγεβρικό επί $\mathbb{Q}$.

Απόδειξη $c-\sqrt{2}=\sqrt{3}$

Συνεπώς $(c-\sqrt{2})^2=(\sqrt{3})^2$. Άρα

$c^2-2\sqrt{2}\cdot c+2=3$, άρα $c^2-1=2\sqrt{2}c$.

Συνεπώς, $(c^2-1)^2=(2\sqrt{2}c)^2$, άρα

$c^4-2c^2+1=4\cdot2\cdot c^2=8c^2$, άρα

$c^4-2c^2+1=8c^2$, συνεπώς το c είναι αλγεβρικό επί του $\mathbb{Q}$

Ισχυρισμός 2 $\mathbb{Q}[c] = \mathbb{Q}(c)$

Απόδειξη Άμεσο από την θεωρία, γιατί από Ισχυρισμό 1, c αλγεβρικό επί του $\mathbb{Q}$.

Ισχυρισμός 3

Οι αριθμοί $\sqrt{2}$, $\sqrt{3}$ περιέχονται στο $\mathbb{Q}[c]$.

Απόδειξη Είδαμε στην απόδ. του Ισχ. 1 ότι $c^2 - 1 = 2\sqrt{2}\cdot c$

Συνεπώς, $\sqrt{2} = \dfrac{c^2-1}{2c}$, άρα $\sqrt{2}$ είναι στοιχείο του $\mathbb{Q}(c)$.

Αφού από Ισχυρισμό 2 $\mathbb{Q}[c] = \mathbb{Q}(c)$ έπεται ότι $\sqrt{2}$ είναι στοιχείο του $\mathbb{Q}[c]$

Τώρα $\sqrt{2}+\sqrt{3}$ στοιχείο του $\mathbb{Q}[c]$ και μόλις δείξαμε ότι $\sqrt{2}$ είναι στοιχείο του $\mathbb{Q}[c]$.

Αφού $\mathbb{Q}[c]$ δακτύλιος, έπεται και ότι $\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2}$ στοιχείο του $\mathbb{Q}[c]$.

Θεώρημα Έστω E ένα ενδιάμεσο σώμα της επέκτασης L/F, $[E:F]<\infty$ και $[L:E]<\infty$. Τότε $[L:F]=[L:E][E:F]$

ΕΡΩΤΗΜΑ: Έχουμε την επέκταση σωμάτων

$$\mathbb{Q}(\sqrt{2}+\sqrt{3})\,/\,\mathbb{Q}(\sqrt{2})$$

Γιατί έχει βαθμό 2;

ΑΠΑΝΤΗΣΗ: Στην απόδειξη του Ισχυρισμού 1 δείξαμε ότι $c^2-2\sqrt{2}\cdot c+2=3$. Συνεπώς, το $c=\sqrt{2}+\sqrt{3}$ είναι ρίζα ενός πολυωνύμου βαθμού 2 με συντελεστές $\mathbb{Q}\sqrt{2}$. Άρα, $irr_{(\mathbb{Q}(\sqrt{2}),c)}$ έχει βαθμό 1 ή 2.

Αν είχε βαθμό 1, θα είχαμε σαν συνέπεια ότι το $\sqrt{2}+\sqrt{3}$ θα ήταν στοιχείο του $\mathbb{Q}(\sqrt{2})$.

Έχουμε, αφού $\sqrt{2}$ είναι αλγεβρικό επί του $\mathbb{Q}$, ότι $\mathbb{Q}(\sqrt{2})=\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2} : a,b \text{ στο } \mathbb{Q}\}$

Άρα, αν είχε βαθμό 1, θα είχαμε ότι υπάρχουν ρητοί a,b με $\sqrt{2}+\sqrt{3}=a+b\sqrt{2}$

Συνεπώς, $(b-1)\cdot\sqrt{2}+a=\sqrt{3}$. Αν $b=1$,

έπεται $\sqrt{3}$ στοιχείο του $\mathbb{Q}$, αντίφαση.

Άρα, $b\neq 1$.

Συνεπώς, $((b-1)\sqrt{2}+a)^2=(\sqrt{3})^2$, το οποίο

συνεπάγεται ότι $2\cdot(b-1)\cdot a\cdot\sqrt{2}$ ρητός.

Αν $a\neq 0$, αντίφαση, γιατί $\sqrt{2}$ όχι ρητός.

Άρα $a=0$. Συνεπώς, $(b-1)\sqrt{2}=\sqrt{3}$.

Το $b-1$ είναι ρητός επομένως γράφεται

σαν $b-1=u/w$, με u,w ακέραιους, $w>0$ και

$ΜΚΔ(u,w)=1$.

Άρα, $(u/w)\sqrt{2}=\sqrt{3}$, συνεπώς $2u^2=3w^2$,

άρα το 2 διαιρεί στους ακεραίους το w, συνεπώς

υπάρχει ακέραιος w_1 με $w=2w_1$.

Σαν συνέπεια, $2u^2=3\cdot 2^2\cdot w_1^2$ το οποίο

συνεπάγεται ότι 2 διαιρεί το u^2, άρα, διαιρεί

το u. Συνεπώς 2 διαιρεί το $ΜΚΔ(u,w)=1$,

αντίφαση.