13/4/2020

Έστω F σώμα και g μη σταθερό ανάγωγο στοιχείο του F[x]. Το g λέγεται διαχωρίσιμο αν ΜΚΔ (g, παράγωγος του g) = 1.

Αυτό είναι ισοδύναμο με το αν E επέκταση του F ώστε το g αναλύεται πλήρως, τότε το g ΔΕΝ έχει πολλαπλή ρίζα στο E.

Δείξαμε, ότι αν το σώμα F έχει χαρακτηριστική 0, κάθε g μη σταθερό ανάγωγο στοιχείο του F[x] είναι διαχωρίσιμο.

Πόρισμα 1.4.7. Έστω F σώμα τ.ω. charF = p, $g(x) \in F[x]$ είναι ανάγωγο και έστω g(x) αναλύεται σε γινόμενο πρ. παρ. στο L[x] όπου L\F μία επέκταση του F. Το πολ. g(x) δεν είναι διαχωρίσιμο αν-ν: $g(x) = r_0 + r_1 x^p + \ldots + r_n \cdot x^{np}$

Παραδ. Αν χαρακτ. του F = 3, στο πόρισμα 1.4.7 το g πρέπει να είναι της μορφής $g = r_0 + r_1 \cdot x^3 + r_2 \cdot x^6 + r_3 x^9 + r_4 \cdot x^{12} + \ldots$

Παράγωγος του $g = 3r_1 \cdot x^2 + 6r_2 \cdot x^5 + 9r_3 \cdot x^9 + 12 r_4 x^{12} + \ldots = 0$ γιατί charF = 3, σημαίνει $(3k) \cdot u = 0$, $\forall u \in F, \forall k \in \mathbb{Z}$

Παράδ. 1.4.8

2. $f'(x) = 1$ στο $\mathbb{Z}_p[x]$.
άρα δεν έχει πολλαπλές ρίζες

§.

Ορισμός: Έστω F ένα σώμα, $f(x) \in F[x]$ ένα πολυώνυμο και έστω L/F μία επέκταση έτσι ώστε το $f(x)$ να αναλύεται σε γραμμικούς παράγοντες του $L[x]$. Εάν δεν υπάρχει ενδιάμεση επέκταση $F \subseteq E \subsetneq L$ τ.ω το $f(x)$ να αναλύεται σε γραμμ. παράγοντες στο $F[x]$, τότε το L λέγεται σώμα ανάλυσης του $f(x)$ πάνω από το F.

Παράδειγμα Θεωρούμε το x^2-2.

$x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$ το $\mathbb{C}$ δεν είναι σώμα ανάλυσης, γιατί υπάρχει το ενδιάμεσο σώμα $\mathbb{R}[x]$ στο οποίο το πολυώνυμο αναλύεται σε γραμμ. παράγοντες.

Παρατήρηση: Έστω F σώμα και g μη σταθερό στοιχείο του $F[x]$. Τότε F είναι ένα σώμα ανάλυσης το g αν-ν το g αναλύεται πλήρως, δηλ. σε γινόμενο γραμμικών επί του F.

Συμβολισμός: E/F σημαίνει F υπόσωμα του E.
Δηλαδή F μη κενό υποσύνολο του E, με F υποομάδα του $(E,+)$ και $(F\setminus\{0\})$ υποομάδα του $(F\setminus\{0\},\cdot)$.

Ορισμός 2.1.1. Έστω E/F επέκταση σωμάτων και $a \in E$. Το a λέγεται αλγεβρικό πάνω από το F αν υπάρχει $f(x) \in F[x]$, έτσι ώστε $f(x) \neq 0$ και $f(a) = 0$. Αν το a δεν είναι αλγεβρικό πάνω από το F, τότε το a λέγεται υπερβατικό πάνω από το F.

Παράδειγμα

Έστω F υπόσωμα L. Αν a στοιχείο του L αλγεβρικό επί του F, τότε είναι και αλγεβρικό επί του E.

Έστω F σώμα και $F[x]$ πολυωνυμικός δακτύλιος επί του F σε μία μεταβλητή x και $F[y]$ πολυωνυμικός δακτύλιος επί του F σε μία μεταβλητή y. Θ έτουμε E να είναι το σώμα κλασμάτων του $F[y]$. Τα στοιχεία του είναι πηλίκα στοιχείων του $F[y]$ με τον παρονομαστή μη μηδενικό.

Το E είναι σώμα με πρόσθεσ:

$$(f_1/f_2) + (g_1/g_2) = (f_1 \cdot g_2 + g_1 \cdot f_2)/(g_1 \cdot g_2)$$

και πολλαπλασιασμό

$$(f_1/f_2) \cdot (g_1/g_2) = (f_1 \cdot f_2)/(g_1 \cdot g_2)$$, όπου

f_1, f_2, g_1, g_2 στοιχεία του $F[y]$.

<u>Ισχυρισμός</u>: Το στοιχείο $y = y/1$ είναι υπερβατικό επί του F.

<u>ΑΠΟΔΕΙΞΗ</u> Έστω ότι δεν ισχύει. Άρα είναι αλγεβρικό επί του F. Συνεπώς, υπάρχει μη μηδενικό πολυώνυμο $h = r_0 + r_1 \cdot x + \dots + r_n \cdot x^n$ ώστε $h(y) = 0$. Συνεπώς, $r_0 + r_1 \cdot y + \dots + r_n y^n = 0$ στον πολυωνυμικό δακτύλιο $F[y]$.

Άρα $r_0 = r_1 = \dots = r_n = 0_F$, αντίφαση, γιατί το h είναι μη μηδενικό πολυώνυμο, άρα υπάρχει i με $r_i \neq 0_F$.

(Ταυτίζουμε το F με το υπόσωμα $\{a/1 : a$ στοιχείο του $F\}$ του E, άρα F υπόσωμα του E.)

<u>Ορισμός 2.1.3</u> Έστω E/F επέκταση σωμάτων και $a \in E$. Ορίζουμε $F[a]$ και $F(a)$ να είναι τα παρακάτω υποσύνολα του E: $F[a] = \{f(a) : f(x) \in F[x]\}$

$$F(a) = \left\{ \frac{f(a)}{g(a)} : g(a) \neq 0,\ f(x), g(x) \in F[x] \right\}.$$

Έστω E/F επέκταση σωμάτων και $a \in E$. $F[a]$ υποδακτύλιος του E, άρα το $F[a]$ είναι ακέραια περιοχή και το $F(a)$ είναι το σώμα κλασμάτων του $F[a]$. Το σώμα $F(a)$ λέγεται <u>απλή</u> επέκταση του F.

$$\begin{array}{c} E \\ | \\ F(a) \\ | \\ F \end{array}$$

<u>Παρατήρηση</u>: Έστω F υπόσωμα του E και a στοιχείο του E. Τότε

i) $F[a]$ υποσύνολο του $F(a)$.

ii) $F[a]$ υποδακτύλιος του E, ο ελάχιστος που περιέχει το $F \cup \{a\}$.

iii) $F(\alpha)$ υπόσωμα του E, το ελάχιστο που περιέχει $F \cup \{\alpha\}$.

iv) Θα δείξουμε ότι αν α αλγεβρικό επί του F, τότε $F[\alpha] = F(\alpha)$.

Επιπλέον $F[\alpha]$ γνήσιο υποσύνολο του $F(\alpha)$ αν α υπερβατικό επί του F.

<u>Παράδειγμα</u> Έστω gamma μιγαδικός. Υπολογίστε τα R[gamma] και R(gamma), όπου R το σώμα των πραγματικών αριθμών.

<u>Λύση</u> <u>Περίπτωση 1</u> : gamma πραγματικός. Τότε έχουμε R[gamma] $=$ R(gamma) $= R$

<u>Περίπτωση 2</u> : Το gamma όχι πραγματικός.

Ισχυρισμός: R[gamma] $=$ R(gamma) $= \mathbb{C}$, όπου $\mathbb{C}$ το σώμα των μιγαδικών αριθμών.

<u>Απόδειξη</u> Αφού gamma όχι πραγματικός έχουμε gamma $= a + b \cdot i$, με a, b πραγματικούς και b όχι μηδέν

Συνεπώς, $i = (gamma - a)/b$ που είναι στοιχείο του $R[gamma]$ γιατί $a, 1/b$ πραγματικοί.

Άρα, αφού το i είναι στοιχείο του $R(gamma)$ έπεται $R[i]$ υποσύνολο του $R[gamma]$. Αλλά έχουμε δει ότι $R[i] = C$. Συνεπώς, αφού $R(gamma)$ υποσύνολο του C έχουμε $C = R[i]$ υποσύνολο $R[gamma]$ υποσύνολο $R(gamma)$ υποσύνολο C.

Συνεπώς, $R[gamma] = R(gamma) = C$.

Παρ.4 σελ.27 <u>Ισχυρισμός</u>: $Q[\sqrt{3}] = \{a + b\sqrt{3} : a, b \text{ ρητοί}\}$

<u>Απόδειξη</u> Έστω $f = r_0 + r_1 x + \dots + r_n x^n$, με r_i ρητοί

Τότε $f(\sqrt{3}) = r_0 + r_1\sqrt{3} + 3 \cdot r_2 3 + 3\sqrt{3} r_3 + 9 r_4 + 9\sqrt{3} r_5 + \dots =$ δηλαδή $a + b\sqrt{3}$ για κατάλληλα a, b ρητούς.

Πρόταση 2.1.5 Έστω E/F μία επέκταση σωμάτων και έστω ότι $a \in E$. Το a είναι αλγεβρικό πάνω από το F αν-ν $F[a] = F(a)$. Όταν το a είναι υπερβατικό πάνω από το F, τότε $F[x] \simeq F[a]$ και $\dim_F F[a] = \infty$.

Παρατήρηση Η απόδειξη της Πρότασης 2.1.5. χρησιμοποιεί το εξής: Έστω F σώμα, και I πρώτο ιδεώδες $F[x]$, με I μη μηδενικό ιδεώδες.

Τότε υπάρχει ανάγωγο πολυώνυμο g στο $F[x]$ που παράγει το ιδεώδες I. Σαν συνέπεια το ιδεώδες I είναι maximal, άρα $F[x]/I$ είναι σώμα.

Παρατήρηση Έστω F υπόσωμα του E και a στοιχείο του E, υπερβατικό επί του F. Τότε η απεικόνιση

Phi : πολυωνυμικός δακτύλιο $F[x] \to F[a]$

με $\text{phi}(g) = g(a)$ είναι ισομορφισμός δακτυλίων.

Άρα, $F[a]$ όχι σώμα, γιατί το $F[X]$ δεν είναι (τα μόνα αντιστρέψιμα στοιχεία του $F[X]$ είναι τα μη μηδενικά σταθερά πολυώνυμα).

Επιπλέον, το $F[a]$ έχει διάσταση σαν F-διανυσματικός χώρος άπειρη, γιατί το $F[X]$ έχει την ίδια ιδιότητα. (Αν $g_1, \dots, g_r$ πεπερασμένο πλήθος μη μηδενικών στοιχείων του $F[X]$ και d ο μέγιστος βαθμός από τα g_i, τότε το πολυώνυμο $x^{(d+1)}$ δεν είναι γραμμικός συνδυασμός με συντελεστές από το F των $g_1, \dots, g_r$. Συνεπώς, το $F[X]$ δεν είναι πεπερασμένα παραγόμενος F-διανυσματικός χώρος, άρα σαν F-διανυσματικός χώρος έχει άπειρη διάσταση.)