6/4/2020

1.3 Ανάγωγα Πολυώνυμα

Πρόταση 1.3.2. Έστω ότι $f(x)=a_nx^n+\dots+a_0\in\mathbb{Z}[x]$ $\deg f(x)=n$. Αν $\frac{r}{s}\in\mathbb{Q}$ $ΜΚΔ(r,s)=1$ και $f\left(\frac{r}{s}\right)=0$ τότε $r\mid a_0$ και $s\mid a_n$.

Πρόταση 1.3.3 Έστω $f(x)\in\mathbb{Z}[x]$ κανονικό πολ. Η ανάλυση $f(x)=f_1(x)\dots f_s(x)$ σε γινόμενο ανάγωγων παραγόντων στον $\mathbb{Z}[x]$ είναι επίσης ανάλυση του $f(x)$ σε γινόμενο ανάγωγων παραγόντων στο $\mathbb{Q}[x]$.

Θεώρημα (Κριτήριο του Eisenstein)
Έστω $f(x)=a_nx^n+\dots+a_0\in\mathbb{Z}[x]$ και $p\in\mathbb{Z}$ φυσικός πρώτος αριθμός. Αν ο p διαιρεί τους συντελεστές a_i, για $i=0,\dots,n-1$, δεν διαιρεί, όμως, τον a_n, ενώ ο p^2 δεν διαιρεί τον a_0, τότε το πολυώνυμο $f(x)$ είναι ανάγωγο στον δακτύλιο $\mathbb{Q}[x]$.

Πρόταση 1.3.7. Έστω σώμα F και $f(x) \in F[x]$. Το πολυώνυμο $f(x)$ είναι ανάγωγο στον $F[x]$ αν-ν $g(x) = f(ax+b)$ είναι ανάγωγο στον $F[x]$ όπου $a, b \in F$ και $a \neq 0$. Το πολυώνυμο $f(x)$ είναι ανάγωγο στον $F[x]$ αν-ν $c \cdot f(x)$ είναι ανάγωγο στο $F[x]$, όπου $c \in F^*$.

Πρόταση Έστω σώμα F, a, b στο F, $a \neq 0$. Ορίζουμε $T: F[x] \longrightarrow F[x]$ με $T(g(x)) = g(ax+b)$. Τότε ο T είναι ισομορφισμός διανυσματικών F-διανυσματικών χώρων, με αντίστροφη απεικόνιση $S: F[x] \longrightarrow F[x]$ με

$$S(g(x)) = g((x-b)/a)$$

$$y = ax+b \Rightarrow \frac{y-b}{a} = x$$

Επίσης, η απεικόνιση T διατηρεί βαθμούς.

Παράδ. 1.3.8 Πολυώνυμο $\phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Q}[x]$, p πρώτος. Αυτό το πολ. είναι ανάγωγο.

$$\phi_p(x)(x-1) = x^p - 1.$$

$\Phi_p(x+1)((x-1)+1) = (x+1)^p - 1 \Rightarrow$

$\Phi_p(x+1)x = (x+1)^p - 1$. Επομένως,

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \dots + \binom{p}{p-1}x + 1 - 1}{x}$$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1} = x^{p-1} + px^{p-2} + \dots + p$$

p πρώτος, άρα $p \mid \binom{p}{n}$, για $n = 1, \dots, p-1$. Το κρ. Eisenstein αποδεικνύει ότι το $\Phi_p(x+1)$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Έτσι ~~το~~ από πρόταση 1.3.2. το πολ. $\Phi_p(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Θεωρούμε τον φυσικό ομομορφ. $\varphi: \mathbb{Z} \to \mathbb{Z}_p$, $a \to \bar{a} = a \bmod p$. Ο φ επεκτείνει τον ομομορφισμό δακτυλίων $\Psi: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, $a_0 + a_1x + \dots + a_nx^n \to \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n$

Πρόταση 1.3.9 $f(x) \in \mathbb{Z}[x]$, p πρώτος τ.ω. $\deg f(x) = \deg \Psi(f(x))$. Αν το $\Psi(f(x))$ είναι ανάγωγο στον $\mathbb{Z}_p[x]$, τότε το $f(x)$ είναι ανάγωγο στον δακτύλιο $\mathbb{Q}[x]$. (Το αντίστροφο δεν ισχύει).

Παρατήρηση 1.3.11 Έστω F σώμα και $f \in F[x]$. Αφού ο $F[x]$ είναι Π.Κ.Ι το πολυώνυμο $f(x)$ είναι ανάγωγο στον $F[x]$ αν-ν το $f(x)$ δεν έχει ανάγωγο παράγοντα βαθμού μικρότερου ή ίσου του μισού του $\deg f(x)$.

1.4 Σώμα Ανάλυσης ενός Πολυωνύμου

Παράδειγμα 1.4.1. $x^2+1 \in \mathbb{R}[x]$

$x^2+1 = (x-i)(x+i)$ αναλύεται σε γινόμενο δε. παρ. στον $\mathbb{C}[x]$. Είναι φανερό ότι δεν υπάρχει σώμα F έτσι ώστε $\mathbb{R} \subsetneq F \subsetneq \mathbb{C}$ που να περιέχει τις ρίζες $\pm i$.

Θεώρημα 1.4.2. F σώμα και $p(x)$ ανάγωγο πολυώνυμο του $F[x]$. Τότε το $p(x)$ έχει μία ρίζα στο $F(y)/\langle p(y)\rangle$.

Απόδειξη Έστω $I = \langle p(y)\rangle$ και $E = F(y)/I$.

$y+I \in E$ είναι ρίζα του $p(x)$.

Έστω $p(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$.

Τότε $p(y+I) = a_0(1+I) + a_1(y+I) + \ldots + a_n(y+I)^n = (a_0+I) + (a_1y+I) + \ldots + (a_ny^n+I) = p(y)+I = I$.

Θεώρημα 1.4.3 (Kronecker) Έστω $f(x) \in F[x]$, F σώμα. Υπάρχει επέκταση σωμάτων L/F έτσι ώστε το $f(x)$ να αναλύεται σε γραμμικούς παράγοντες στο $L[x]$.

Απόδειξη f στο F[X]. Αν ... αναλύεται πλήρως στο F τελειώσαμε.

Υποθέτουμε ότι δεν αναλύεται πλήρως στο f. Αυτό συνεπάγεται ότι υπάρχει ανάγωγο g_1 βαθμού τουλάχιστον δύο και h_1 μη μηδενικό ώστε $f = g_1 \cdot h_1$.

Θέτουμε $F_1 = F[y]/(g_1(y))$ Αυτό είναι σώμα που περιέχει το F και στο οποίο το g_1 έχει ρίζα. Συνεπώς, αν πούμε τη ρίζα a_1, έχουμε στο $F_1[X]$ $f(x - a_1) g_2 h_1$.

Συνεχίζουμε με επαγωγή την διαδικασία για το πολυώνυμο $g_2 h_1$ που έχει βαθμό ίσο με (το βαθμό του f μείον ένα). Μετά από πεπερασμένο (το πολύ deg(f)) πλήθος βημάτων, έχουμε μια επέκταση F_r του F ώστε το f να αναλύεται πλήρως στο $F_r[X]$.

Ορισμός 1.4.4 F σώμα και $f(x) = c_n x^n + \dots + c_1 x + c_0 \in F[X]$

Παράγωγος του f(x) λέγεται το πολυώνυμο $c_1 + 2c_2 + \dots + n c_n x^{n-1}$, και συμβολίζεται με $f'(x)$.

• Ο ορισμός δουλεύει για κάθε σώμα F.

• Όταν F είναι ρητοί, πραγματικοί κ.α. τότε ο ορισμός ταυτίζεται με τον συνήθη ορισμό της παραγώγου.

Παράδειγμα Ποια είναι η παράγωγος του x^2+1 σαν πολυώνυμο του $\mathbb{Z}_2[x]$;

Απάντηση: Το μηδενικό πολυώνυμο, γιατί στο $\mathbb{Z}_2$ $[2]=[0]$.

Παράδειγμα Ποια είναι η παράγωγος του x^2+1 σαν πολυώνυμο του $\mathbb{Z}_5[x]$;

Απάντηση: Το πολυώνυμο $[2]_5 \cdot x$, που είναι μη μηδενικό.

Παράδειγμα Ποια είναι η παράγωγος του x^2+1 σαν πολυώνυμο του $\mathbb{Z}_7[x]$;

Απάντηση: Το πολυώνυμο

$$[7]_5 \cdot x^6 = [2]_5 \cdot x^6,$$ που είναι μη μηδενικό.

Πρόταση 1.4.5 Έστω $f(x)=c_0+c_1x+\dots+c_nx^n \in F[x]$.

όπου F είναι ένα σώμα και έστω $L \mid F$ μία επέκταση του F όπου το $f(x)$ αναλύεται σε γινόμενο γραμμ. παραγ. Το $f(x)$ έχει πολλαπλές ρίζες στο L αν-ν $ΜΚΔ(f(x), f'(x)) \neq 1$.

Παρατήρηση: Έστω L επέκταση σώματος F και g_1, g_2 μη μηδενικά πολυώνυμα επί του F. Τότε $ΜΚΔ(g_1, g_2)$ στο F είναι ίσος με τον $ΜΚΔ(g_1, g_2)$, όπου τα θεωρούμε πολυώνυμα στο $L[x]$.

Ο λόγος είναι ότι ο ΜΚΔ υπολογίζεται με Ευκλείδια Διαίρεση που είναι ίδια και στα δύο σώματα.

Έστω $f(x) = c(x-a_1)^{s_1} \dots (x-a_t)^{s_t} \in L[x]$

Παρατηρούμε ότι αν $s_i > 1$, για κάποιο $i \in \{1, \dots t\}$ τότε το $x-a_i$ διαιρεί το $f(x)$ και το $f'(x)$ άρα $ΜΚΔ(f(x), f'(x)) \neq 1$.

Έστω $f = (x-a_1)(x-a_2)(x-a_3)$ στο $L[x]$, με a_i διάφορο του a_j για i διάφορο του j. Τότε, $f' = (x-a_2)(x-a_3) + (x-a_1)(x-a_3) + (x-a_1)(x-a_2)$ Φανερά, το $x-a_1$ δεν διαιρεί το f' γιατί διαιρεί τα $(x-a_1)(x-a_3) + (x-a_1)(x-a_2)$ το ίδιο ισχύει για $x-a_2, x-a_3$ αλλά όχι το $(x-a_2)(x-a_3)$. Επιπλέον, οι μόνοι ανάγωγοι παράγοντες του f στο $L[x]$ είναι οι

$(x-a_1), (x-a_2), (x-a_3)$. Συνεπώς, $ΜΚΔ(f, f') = 1$

Ορισμός: Ένα ανάγωγο πολ. $g(x)$ λέγεται διαχωρίσιμο όταν οι ρίζες του στην επέκταση είναι απλές. Αν δεν είναι ανάγωγο λέγεται διαχωρίσιμο αν κάθε ανάγωγος παράγοντας του έχει απλές ρίζες.

Ορισμός: Έστω F ένα σώμα. Λέμε ότι το F έχει χαρακτηριστική 0 αν η τάξη του 1_F σαν στοιχείο της ομάδας $(F, +)$ είναι άπειρη. Ισοδύναμα, αν η 1_F δεν είναι μηδέν στο F, για κάθε θετικό ακέραιο n.

Παράδειγμα: Τα σώματα $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ έχουν χαρακτηριστική 0. Αν p πρώτος, το σώμα $\mathbb{Z}/(p)$ δεν έχει χαρακτηριστική 0, γιατί $p \cdot 1_F = 0_F$

Πόρισμα: F σώμα, $g(x) \in F[x]$ ένα ανάγωγο πολυώνυμο. Αν το F έχει χαρακτηριστική 0 τότε το $g(x)$ είναι διαχωρίσιμο.

Πρόταση: Έστω F σώμα χαρακτηριστικής 0 και a στο F στοιχείο μη μηδενικό και $n>0$ ακέραιος. Τότε $n \cdot a$ είναι μη μηδενικό στο F.

Απόδειξη: Έστω $n \cdot a = 0$ στο F. Άρα $n(1_F \cdot a) = 0$ στο F, συνεπώς $(n \cdot 1_F) \cdot a = 0$, αντίφαση, γιατί F σώμα, a μη μηδενικό, και $n \cdot 1_F$ μη μηδενικό αφού η χαρακτηριστική του F είναι ίση με 0.

Πόρισμα: Έστω F σώμα χαρακτηριστικής 0, και g μη μηδενικό στοιχείο του $F[X]$ βαθμού $n>0$. Τότε το g είναι μη μηδενικό πολυώνυμο βαθμού $n-1$.

Ορισμός: Έστω F ένα σώμα που δεν έχει χαρακτηριστική 0. Ορίζουμε χαρακτηριστική του F την τάξη του 1_F σαν στοιχείο της ομάδας $(F, +)$.

Τότε χαρακτηριστική είναι πρώτος. Ο λόγος είναι ότι αν η χαρακτηριστική του F ήταν $d = d_1 \cdot d_2$ με $d_1, d_2 > 1$

$d \cdot 1_F = 0$ συνεπάγεται $(d_1 \cdot 1_F)(d_2 \cdot 1_F) = 0$, αντίφαση, γιατί F σώμα, και $d_1 < d$ άρα $d_1 \cdot 1_F$ όχι μηδέν και $d_2 < d$ άρα $d_2 \cdot 1_F$ όχι μηδέν.

Συμπέρασμα: Η χαρακτηριστική ενός σώματος είναι είτε 0 είτε πρώτος ακέραιος.

Παρατήρηση: Αν το σώμα F έχει χαρακτηριστική $p > 0$ ισχύει ότι για n θετικό ακέραιο, και a μη μηδενικό στοιχείο του σώματος ότι $n \cdot a = 0_F$ όταν και μόνο όταν το n είναι πολλαπλάσιο του p.

Απόδ: Έστω $n \cdot a = 0$ στο F. Άρα $n(1_F \cdot a) = 0$ στο F συνεπώς $(n \cdot 1_F) \cdot a = 0$. Αφού a μη μηδενικό έπεται $(n \cdot 1_F) = 0_F$. Συνεπώς, το p διαιρεί το n. Αντιστρόφως, αν το p διαιρεί το n φανερά $(n \cdot 1_F) = 0_F$, άρα $n \cdot a = (n \cdot 1_F) \cdot a = 0_F \cdot a = 0_F$.