9/3/2020

Ορισμός: Έστω K σώμα (ή $K=\mathbb{Z}$). Ένα πολυώνυμο $h \in K[x]$ λέγεται ΑΝΑΓΩΓΟ/K αν $h \neq 0$, $\deg h > 0$ και δεν υπάρχουν πολυώνυμα $f_1, f_2 \in K[x]$ με $h = f_1 \cdot f_2$ και $\deg f_1 > 0$, $\deg f_2 > 0$.

ΠΡΟΤΑΣΗ : Έστω $\mathbb{F}$ σώμα και $0 \neq h \in \mathbb{F}[x]$

i) Αν $\deg h = 1$, τότε h ανάγωγο / $\mathbb{F}$

ii) Αν το $\deg h \geq 2$ και έχει ρίζα στο $\mathbb{F}$, τότε h ΟΧΙ ΑΝΑΓΩΓΟ.

iii) Αν $\deg h = 2$ ή 3 τότε h ανάγωγο / $\mathbb{F}$ αν και μόνο αν δεν έχει ρίζα στο $\mathbb{F}$.

iv) Το $(x^2+1)^2 \in \mathbb{R}[x]$ δεν είναι ανάγωγο, αλλά δεν έχει ρίζα στο $\mathbb{R}$.

π.χ. Βαθμός 2 ή 3 ανάγωγο / $\mathbb{F} \Leftrightarrow$ δεν έχει ρίζα στο $\mathbb{F}$.
Βαθμός ≥ 4 ανάγωγο / $\mathbb{F} \Rightarrow$ δεν έχει ρίζα στο $\mathbb{F}$.

ΑΠΟΔΕΙΞΗ

i) Προφανές για $h = f_1 \cdot f_2 \Rightarrow \deg h = \deg f_1 + \deg f_2$.

ii) Έστω $0 \neq h \in \mathbb{F}[x]$ με $\deg h \geq 2$ και $a \in \mathbb{F}$ ρίζα του h. Από Ευκλείδεια Διαίρεση του h με το $x - a$, υπάρχει $r \in \mathbb{F}[x]$ σταθερό και $q \in \mathbb{F}[x]$ ώστε $h = (x-a)q + r$. Για $x = a$, αφού $h(a) = 0 \Rightarrow r = 0$. Άρα h όχι ανάγωγο, αφού $\deg q = \deg h - 1 \geq 1$

iii) Έστω $h \neq 0$ με $\deg h = 2$ ή 3 και χωρίς ρίζα στο $\mathbb{F}$. Θα δείξουμε h ανάγωγο / $\mathbb{F}$.

Έστω ότι δεν είναι. Άρα υπάρχουν $f_1, f_2 \in \mathbb{F}[x]$ με $\deg f_1 \geq 1$ $\deg f_2 \geq 1$ ώστε $h = f_1 \cdot f_2$ στο $\mathbb{F}[x]$. Αφού $\deg h = 2$ ή 3 έπεται (ίσως μετά από εναλλαγή f_1, f_2) ότι $\deg f_1 = 1$. Άρα $f_1 = ax + b$ με $a, b \in \mathbb{F}$, $a \neq 0$. Συνεπώς το f_1 έχει την ρίζα $-\frac{b}{a}$, που είναι και ρίζα του h γιατί $h = f_1 \cdot f_2$. Αντίφαση.

iv) Προφανές.

<u>Παράδειγμα</u> Είναι το $x^2 - 2$ ανάγωγο στο $\mathbb{Q}[x]$;

Ναι, γιατί από πρόταση $\deg = 2$ και δεν έχει ρίζα στο $\mathbb{Q}$.

Είναι το $x^3 - 2$ ανάγωγο στο $\mathbb{Q}[x]$;
Ναι, γιατί $\deg = 3$ και δεν έχει ρίζα στο $\mathbb{Q}$.

Είναι το $x^4 - 2$ ανάγωγο στο $\mathbb{Q}[x]$;
Θα δούμε πως ναι.

<u>Θεμελιώδες Θεώρημα Άλγεβρας</u>.

Έστω $h \in \mathbb{C}[x]$ με $\deg h \geq 1$. Τότε το h έχει ρίζα στο $\mathbb{C}$.

<u>Πόρισμα</u> Έστω $0 \neq h \in \mathbb{C}[x]$. Τότε h ανάγωγο$/\mathbb{C}$ $\Longleftrightarrow$ $\deg h = 1$.

Απόδειξη Αν $h \neq 0$ και $\deg h = 1 \Rightarrow$ h ανάγωγο από την πρόταση.
Έστω $\deg h \geq 2$. Από Θεμελ. Θεωρ. Άλγεβρας έχει ρίζα $a \in \mathbb{C}$. Άρα από την Πρόταση $x-a | h$ άρα h όχι ανάγωγο.

ΠΡΟΤΑΣΗ
Κάθε πολυώνυμο περιττού βαθμού $/\mathbb{R}$ έχει ρίζα στο $\mathbb{R}$, άρα όχι ανάγωγο.

Απόδειξη
Έστω $h = a_{2n+1} \cdot x^{2n+1}$ + μικρότεροι όροι
Αν $a_{2n+1} > 0$ $\lim_{x \to -\infty} h = -\infty$, $\lim_{x \to +\infty} h = +\infty$

άρα από συνέχεια έχει ρίζα
Αν $a_{2n+1} < 0$ δουλεύουμε με το $-h$.

ΠΡΟΤΑΣΗ Έστω $0 \neq h \in \mathbb{R}[x]$ με $\deg h \geq 1$.

Τότε h ανάγωγο $/\mathbb{R} \Leftrightarrow \deg h = 1$ ή

($\deg h = 2$ και το h δεν έχει ρίζα στο $\mathbb{R}$)

Απόδειξη
($\Leftarrow$) Άμεσο από γενική Πρόταση

($\Rightarrow$) $h = (x-z) \cdot q$, $q \in \mathbb{C}[x]$

$z \in \mathbb{C} \setminus \mathbb{R}$ $h \in \mathbb{R}[x]$, $z \in \mathbb{C}$ $h(z) = 0 \Rightarrow h(\bar{z}) = 0$

$\Rightarrow q = (x-\bar{z}) \cdot q_1 \Rightarrow h = (x-z)(x-\bar{z}) q_1$

και $(x-j)(x-\bar{j}) \in \mathbb{R}[x] \Rightarrow q_1 \in \mathbb{R}[x]$. Άρα αν $\deg h \geq 3$ και ανάγωγο, αντίφαση.

Π.χ. $a_i \in \mathbb{R}$ $\quad \sum a_i j^i = 0 \Rightarrow \overline{\sum (a_i j^i)} = \bar{0} = 0$

$$\Rightarrow \sum \bar{a_i} (\bar{j})^i = 0 \xRightarrow{a_i \in \mathbb{R} \Rightarrow \bar{a_i} = a_i} \sum a_i (\bar{j})^i = 0$$

ΠΡΟΤΑΣΗ Έστω $0 \neq h \in \mathbb{Z}[x]$ με

$$h = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0, \text{ με } a_0 \neq 0, a_n \neq 0.$$

Έστω $\frac{p}{q} \in \mathbb{Q}$ με $p, q \in \mathbb{Z}$, $q > 0$ ΜΚΔ$(p,q) = 1$ ρίζα του h στο $\mathbb{Q}$. Τότε $p \mid a_0$ και $q \mid a_n$.

ΑΠΟΔΕΙΞΗ $h\left(\frac{p}{q}\right) = 0 \Leftrightarrow a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} +$

$$\ldots + a_1 \frac{p}{q} + a_0 = 0 \Rightarrow$$

$$a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0 \quad (*)$$

$$(*) \Rightarrow p \mid a_0 q^n \xRightarrow[\text{ΜΚΔ}(p,q)=1]{} p \mid a_0$$

$$(*) \Rightarrow q \mid a_n p^n \xRightarrow[\text{ΜΚΔ}(p,q)=1]{} q \mid a_n.$$

ΠΑΡΑΔΕΙΓΜΑ $h = x^3 - 3$. Τότε $a_n = 1$, $a_0 = -3$

$$\{(p,q) : p, q \in \mathbb{Z}, q > 0, \text{ΜΚΔ}(p,q) = 1, p \mid 3 \text{ και } q \mid 1\}$$

$= \{(-3,1), (3,1), (-1,1), (1,1)\}$

$h\left(-\frac{3}{1}\right) \neq 0$, $h\left(\frac{3}{1}\right) \neq 0$, $h\left(\frac{-1}{1}\right) \neq 0$,

$h\left(\frac{1}{1}\right) = -2 \neq 0$. Άρα το h δεν έχει ρίζες στο $\mathbb{Q}$.

ΕΡΩΤΗΜΑ Για ποια $a, b \in \mathbb{Z}$ το $x^3 + ax^2 + bx - 3 \in \mathbb{Q}[x]$ είναι ανάγωγο; (άσκηση)

ΕΡΩΤΗΜΑ Έστω $0 \neq h \in \mathbb{Q}[x]$. Πως μπορούμε να βρούμε όλες τις υποψήφιες ρίζες του στο $\mathbb{Q}$;

ΑΠΑΝΤΗΣΗ Πολλαπλασιάζουμε με το ΕΚΠ των παρονομαστών των συντελεστών του h. Έτσι έχουμε ένα πολυώνυμο $h_1 \in \mathbb{Z}[x]$ με ίδιες ρίζες με το h και εφαρμόζουμε την Πρόταση.

π.χ. $h = \frac{2}{3}x^4 + \frac{5}{2}x - \frac{1}{5}$

$h_1 = 30 \quad h = 20x^4 + 75x - 6.$

ΠΡΟΤΑΣΗ Κριτήριο Eisenstein

Έστω $h = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Q}[x]$ με $a_i \in \mathbb{Z}$ $n \geq 2$, $a_n \neq 0$. Υποθέτουμε ότι υπάρχει πρώτος $p \in \mathbb{Z}$ με:

i) $p \mid a_0, \ p \mid a_1, \ \dots, \ p \mid a_{n-1}$

ii) $p \nmid a_n$

iii) $p^2 \nmid a_0$.

Τότε h ανάγωγο / $\mathbb{Q}$.

(Δηλ. p διαιρεί όλους τους συντελεστές εκτός του a_n και $p^2 \nmid$ σταθερό όρο).

ΕΦΑΡΜΟΓΗ Έστω $n \geq 2$. Δείξτε ότι το

$x^n - 3$ είναι ανάγωγο / $\mathbb{Q}$

ΑΠΟΔΕΙΞΗ $h = x^n + 0x^{n-1} + \dots + 0x + (-3)$

Για $p=3$ από το κριτήριο Eisenstein

ΠΟΡΙΣΜΑ Έστω $n \geq 1$. Τότε υπάρχει ανάγωγο $0 \neq h \in \mathbb{Q}[x]$ ανάγωγο με $\deg h = n$.

ΠΑΡΑΤΗΡΗΣΗ Η εφαρμογή δουλεύει για το $x^n - pa$ όπου $a \in \mathbb{Z} \setminus \{0\}$ και ΜΚΔ$(p, a) = 1$ και p πρώτος.

ΘΕΩΡΗΜΑ ("Λήμμα Gauss") Έστω $h_1 \neq 0$, $h_2 \neq 0$ με $h_1, h_2 \in \mathbb{Q}[x]$. Υποθέτουμε $h_1 \cdot h_2 \in \mathbb{Z}[x]$.

Τότε υπάρχουν $r, s \in \mathbb{Q}$ με $r \cdot s = 1$ και $rh_1 \in \mathbb{Z}[x]$, $s \cdot h_2 \in \mathbb{Z}[x]$.

Άρα θέτοντας $\widetilde{h_1} = rh_1$, $\widetilde{h_2} = sh_2$, έχουμε $\widetilde{h_1} \in \mathbb{Z}[x]$, $\widetilde{h_2} \in \mathbb{Z}[x]$, $\deg \widetilde{h_1} = \deg h_1$, $\deg \widetilde{h_2} = \deg h_2$ και $\widetilde{h_1} \widetilde{h_2} = h_1 \cdot h_2$

ΑΠΟΔΕΙΞΗ Χωρίς απόδειξη.

ΕΦΑΡΜΟΓΗ Έστω $g \neq 0$, $g \in \mathbb{Z}[x]$. Αν το g στο $\mathbb{Q}[x]$ δεν είναι ανάγωγο, τότε υπάρχουν $\tilde{h}_1, \tilde{h}_2 \in \mathbb{Z}[x]$ ΜΗ σταθερά με $g = \tilde{h}_1 \cdot \tilde{h}_2$.

ΠΡΟΤΑΣΗ Το $g = x^4 + 1$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

ΑΠΟΔΕΙΞΗ Βήμα 1 Έστω ότι g όχι ανάγωγο

γιατί $x \in \mathbb{Q} \Rightarrow x^4 \geq 0 \Rightarrow x^4 + 1 \geq 2$.
(ή με πιθανές ρίζες όπως προηγούμενη πρόταση).

Βήμα 2 Έστω $g = h_1 h_2$ με $h_1, h_2 \in \mathbb{Q}[x]$, $\deg h_1 \geq 1$, $\deg h_2 \geq 1$.
Τότε $4 = \deg h_1 + \deg h_2$. Αφού το g δεν έχει ρίζα στο $\mathbb{Q}$ έπεται $\deg h_1 = \deg h_2 = 2$

Βήμα 3 Από Λήμμα Gauss (Θετ. $\tilde{h}_1 = r h_1$, $\tilde{h}_2 = r h_2$) υπάρχουν $\tilde{h}_1, \tilde{h}_2 \in \mathbb{Z}[x]$ με $\deg \tilde{h}_1 = \deg \tilde{h}_2 = 2$ ώστε $g = \tilde{h}_1 \cdot \tilde{h}_2$.

Έστω
$$\tilde{h}_1 = ax^2 + bx + c$$
$$\tilde{h}_2 = dx^2 + ex + f$$
Τότε $x^4 + 1 = (ax^2 + bx + c)(dx^2 + ex + f)$
με $a, b, c, d, e, f \in \mathbb{Z}$.

Άρα
$$\begin{cases} ad = 1 \\ ae + bd = 0 \\ af + be + cd = 0 \quad (*) \\ bf + ce = 0 \quad (**) \\ cf = 1 \end{cases}$$

Άρα, $ad=1 \Rightarrow (a,d)=(1,1)$ ή $(a,d)=(-1,-1)$
$a,d \in \mathbb{Z}$

Πολλαπλ. με -1 στην περίπτωση που $(a,d)=(-1,-1)$ μπορούμε να υποθ. $\boxed{a=1,\ d=1}$

$cf=1 \Rightarrow (c,f)=(1,1)$ ή $(c,f)=(-1,-1)$
$c,f \in \mathbb{Z}$

Βήμα 4 Περίπτωση 1 $\boxed{c=f=1}$

(**) $\Rightarrow b+e=0 \Rightarrow e=-b$ και (*) $\Rightarrow 1-b^2+1=0 \Rightarrow b^2=2$
αντίφαση, αφού $b \in \mathbb{Z}$.

Περίπτωση 2 $c=f=-1$ άρα

(*) $\Rightarrow b+e=0 \Rightarrow e=-b$ και
(*): $-1-b^2-1=0 \Rightarrow b^2+2=0$, αντίφαση αφού $b \in \mathbb{Z}$.

Άρα x^4+1 ανάγωγο στο $\mathbb{Q}[x]$.

ΠΑΡΑΤΗΡΗΣΗ (ΧΩΡΙΣ ΑΠΟΔΕΙΞΗ)
Έστω $0 \neq h \in \mathbb{Q}[x]$ μη σταθερό.
Τότε υπάρχει αλγόριθμος που μας λέει αν το h είναι ανάγωγο επί του $\mathbb{Q}$ ή όχι.

Πολλ. με ΕΚΠ παρονομαστών, υποθ. $g \in \mathbb{Z}[x]$
π.χ. $\deg g = 5$ έστω ότι όχι ανάγωγο. Τότε υπάρχουν από λήμμα Gauss $\tilde{h}_1, \tilde{h}_2 \in \mathbb{Z}[x]$ με $g=\tilde{h}_1 \cdot \tilde{h}_2$ και $(\deg\tilde{h}_1, \deg\tilde{h}_2)=(1,4)$ ή $(\deg\tilde{h}_1, \deg\tilde{h}_2)=(2,3)$

Ισχυρισμός 1 (χωρίς απόδειξη) Δοθέντος $g \in \mathbb{Z}[x]$, υπάρχει $N>0$ που εξαρτάται μόνο από το g ώστε κάθε συντελεστής των $\tilde{h}_1, \tilde{h}_2$ να είναι ακέραιος με απόλυτη τιμή $4N$.

Άρα υπάρχει πεπερασμένο πλήθος υποψηφίων $\tilde{h}_1, \tilde{h}_2$, άρα υπάρχει αλγόριθμος.

ΠΑΡΑΤΗΡΗΣΗ Αυτός ο αλγόριθμος μας επιτρέπει και να παραγοντοποιήσουμε το g σαν γινόμενο αναγώγων πολυωνύμων.