Πολυωνυμική συνάρτηση

Έστω $\mathbb{K}$ ένα σώμα και $P \in \mathbb{K}[X]$

Αν $P = \sum_{i=0}^{n} a_i X^i$, τότε μπορούμε να ορίσουμε την αντίστοιχη πολυωνυμική συνάρτηση

$$\tilde{P} : \mathbb{K} \longrightarrow \mathbb{K}$$
$$y \longmapsto \sum_{i=0}^{n} a_i y^i$$

Π.χ. $P = X^2 + X - 2$

$$\tilde{P} : \mathbb{R} \longrightarrow \mathbb{R}$$
$$y \longmapsto y^2 + y - 2$$

$\tilde{P}(2) = 2^2 + 2 - 2 = 4$

$\tilde{P}(1) = 1^2 + 1 - 2 = 0$

Σχόλια:

- Πολλές φορές γράφουμε $P(1)$ αντί για $\tilde{P}(1)$
- Οι πολυωνυμικές συναρτήσεις μας βοηθούν να βρούμε το υπόλοιπο της ευκλείδειας διαίρεσης:

Παραδείγματα:

* $P = (X-a)Q + R$, $R \in \mathbb{K}$

$\Rightarrow \tilde{P}(a) = \tilde{R}(a) = R$

Οπότε το υπόλοιπο της Ευκλείδειας διαίρεσης του X^2+X-2 με το $X-2$ είναι 4

★ $P = (X-a)(X-b)Q + R$, $R=0$ ή $\deg R = 0$ ή $\deg R = 1$

δηλ. $R = \lambda X + \mu$ για κάποια $\lambda, \mu \in \mathbb{K}$

$\Rightarrow \tilde{P}(a) = \tilde{R}(a) = \lambda a + \mu$

$\tilde{P}(b) = \tilde{R}(b) = \lambda b + \mu$

Οπότε το υπόλοιπο της Ευκλείδειας διαίρεσης του X^2+X-2 με το $(X-2)(X-1)$ είναι $\lambda X + \mu$ με:

$$\left.\begin{aligned} 2\lambda + \mu &= 4 \\ \lambda + \mu &= 0 \end{aligned}\right\} \Leftrightarrow \begin{aligned} \lambda &= 4 \\ \mu &= -\lambda \end{aligned}$$

Άρα $R = 4X - 4$

Μάλιστα $X^2 + X - 2 = (X-2)(X-1) + 4X - 4$

Ορισμός: Λέμε ότι το $a \in \mathbb{K}$ είναι **ρίζα** του $P \in \mathbb{K}[X]$ αν $\tilde{P}(a) = 0$.

Λήμμα: a ρίζα του $P \in \mathbb{K}[X] \Leftrightarrow (X-a) \mid P$

Ορισμός Λέμε ότι το $a \in \mathbb{K}$ είναι **ρίζα τάξης k (ή k-πλή ρίζα)** του P αν $(X-a)^k \mid P$ αλλά $(X-a)^{k+1} \nmid P$.

Π.χ. Το 1 είναι διπλή ρίζα του πολυωνύμου $(X-1)^2(X-3)$.

Ορισμος Έστω $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$. Το πολυώνυμο $P' := \sum_{i=1}^{n} i a_i X^{i-1}$ ονομάζεται **τυπική παράγωγος** του πολυωνύμου P.

Λήμμα: Έστω $a \in \mathbb{K}$ μια ρίζα του πολυωνύμου $P \in \mathbb{K}[X]$.
Έχουμε ότι το a είναι απλή ρίζα του P (δηλ. ρίζα τάξης 1)
αν και μόνο αν το a δεν είναι ρίζα του P'.

Απόδειξη: $P = (x-a)Q \Rightarrow$

$P' = Q + (x-a)Q' \Rightarrow$

$\tilde{P}'(a) = \tilde{Q}(a)$

$\tilde{P}'(a) = 0 \Leftrightarrow \tilde{Q}(a) = 0 \Leftrightarrow (x-a) \mid Q$.

Παράδειγμα:

$P = X^2 + X - 2$

$P' = 2X + 1$

$\tilde{P}(1) = 0$, $\tilde{P}'(1) = 3 \neq 0$

Άρα το 1 είναι απλή ρίζα του P.

Ποιο είναι το υπόλοιπο της Ευκλείδειας διαίρεσης του P με το $(x-1)^2$;

$P = (X-1)^2 Q + R$, $R = \lambda X + \mu$ για κάποια $\lambda, \mu \in \mathbb{R}$

$\tilde{P}(1) = \tilde{R}(1) \Rightarrow 0 = \lambda + \mu$

$P' = 2(X-1)Q + (X-1)^2 Q' + R'$

$\tilde{P}'(1) = \tilde{R}'(1) \Rightarrow 3 = \lambda$

Άρα $R = 3X - 3$

Παρατήρηση 1:

Αν $P = (X-a)(X-b)Q + R$, τότε

$P' = (2X-a-b)Q + (X-a)(X-b)Q' + R'$

οποτε $\tilde{P}'(a) = (a-b)\tilde{Q}(a) + \tilde{R}'(a)$ και $\tilde{P}'(b) = (b-a)\tilde{Q}(b) + \tilde{R}'(b)$

Παρατήρηση 2:

Οι ρίζες ενός δευτεροβάθμιου πολυωνύμου βρίσκονται με τη μεθοδο της διακρίνουσας: Έστω $P = aX^2 + bX + c \in \mathbb{K}[X]$ με $a \neq 0$

Έστω $\Delta := b^2 - 4ac$ και δ τέτοιο ώστε $\delta^2 = \Delta$

Αν δεν υπάρχει τέτοιο δ, το P δεν έχει ρίζες μέσα στο $\mathbb{K}$.

Αλλιώς, οι ρίζες είναι $\rho_{1,2} = \dfrac{-b \pm \delta}{2a}$, δηλ $P = \left(X - \dfrac{-b-\delta}{2a}\right)\left(X - \dfrac{-b+\delta}{2a}\right)$

Αν $\delta = 0$, τότε $P = \left(X + \dfrac{b}{2a}\right)^2$ και το P έχει διπλή ρίζα.

Π.χ. $P = x^2 + x - 2$, $\Delta = 9$, $\rho_{1,2} = \dfrac{-1 \pm 3}{2} \Rightarrow \rho_1 = 1, \rho_2 = -2$

$P = (x-1)(x+2)$

Επίσης έχουμε $\rho_1 + \rho_2 = -\dfrac{b}{a}$ και $\rho_1 \rho_2 = \dfrac{c}{a}$, οποτε μπορούμε να βρούμε και τις ρίζες έτσι.

Ορισμός: Ένα πολυώνυμο $P \in \mathbb{K}[X]$ με $\deg P \geq 1$ ονομάζεται **ανάγωγο** αν οποτεδήποτε $P = A \cdot B$ με $A, B \in \mathbb{K}[X]$, έχουμε $A \in \mathbb{K}^*$ (ισοδύναμα $\deg A = 0$) ή $B \in \mathbb{K}^*$ (ισοδύναμα $\deg B = 0$)

Παρατηρήσεις:

- $\deg P = 1 \Rightarrow P$ ανάγωγο

  [αν $P = AB \Rightarrow \deg A + \deg B = \deg P = 1 \Rightarrow \deg A = 0$ ή $\deg B = 0$]

- Αν $\deg P > 1$ και P έχει ρίζα στο $\mathbb{K}$, τότε το P δεν είναι ανάγωγο.

  [αν $a \in \mathbb{K}$ είναι ρίζα του P, τότε $P = (x-a)Q$ με $\deg Q = \deg P - 1 > 0$]

- $P \in \mathbb{K}[X]$ έχει ρίζα στο $\mathbb{K} \Leftrightarrow \exists\, A \in \mathbb{K}[X]$ με $\deg A = 1$ τ.ώ. $A \mid P$

  ["$\Rightarrow$" Προφανές

  "$\Leftarrow$" Αν $A = \lambda X + \mu$ με $\lambda \neq 0$, τότε $P = (\lambda X + \mu)Q$ και $\tilde{P}\left(-\frac{\mu}{\lambda}\right) = 0$]

- Αν $\deg P \in \{2,3\}$, τότε P ανάγωγο $\Leftrightarrow$ P δεν έχει ρίζα στο $\mathbb{K}$

  [αν $P = AB \Rightarrow \deg A + \deg B \in \{2,3\} \overset{\deg A \neq 1}{\underset{\deg B \neq 1}{\Longrightarrow}} \deg A = 0$ ή $\deg B = 0$]

- Αν $\deg P \geq 4$, τοτε αυτό δεν ισχύει

  [π.χ. $P = (x^2+1)(x^2+2)$ δεν έχει ρίζες στο $\mathbb{R}$, αλλά δεν είναι ανάγωγο]

ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΤΗΣ ΑΛΓΕΒΡΑΣ:

Κάθε πολυώνυμο βαθμού ≥ 1 στο $\mathbb{C}[X]$ έχει τουλάχιστον μια ρίζα στο $\mathbb{C}$.

Ισοδύναμα:

Κάθε πολυώνυμο βαθμού ≥ 1 στο $\mathbb{C}[X]$ έχει όλες τις ρίζες του στο $\mathbb{C}$

Ισοδύναμα:

Κάθε πολυώνυμο βαθμού $n \geq 1$ στο $\mathbb{C}[X]$ γράφεται ως γινόμενο n πρωτοβάθμιων πολυωνύμων στο $\mathbb{C}$ (δηλ. έχει n ρίζες στο $\mathbb{C}$)

Ισοδύναμα:

Κάθε ανάγωγο πολυώνυμο στο $\mathbb{C}[X]$ είναι βαθμού 1.

<u>Υπενθύμιση:</u> Έστω $P \in \mathbb{R}[X] \subseteq \mathbb{C}[X]$.

Έχουμε δει, όταν μιλούσαμε για τους μιγαδικούς αριθμούς, ότι

$\tilde{P}(z) = 0 \Leftrightarrow \tilde{P}(\bar{z}) = 0$ για $z \in \mathbb{C}$.

Οπότε, αν $z \in \mathbb{C} \setminus \mathbb{R}$ είναι ρίζα του P, τότε το πολυώνυμο

$f_z = (x-z)(x-\bar{z}) = x^2 - (z+\bar{z})x + z\bar{z} = x^2 - Re(z)x + |z|^2 \in \mathbb{R}[X]$ ⊛

διαιρεί το P στο $\mathbb{R}[X]$, γιατί αν $R = \lambda X + \mu$ είναι το υπόλοιπο

της αντίστοιχης Ευκλείδειας διαίρεσης, τότε $\tilde{R}(z) = 0$ και

αυτό είναι δυνατό μόνο αν $\lambda = \mu = 0$ (αφού $\lambda, \mu \in \mathbb{R}$ και $z \notin \mathbb{R}$).

Επίσης, η πολλαπλότητα του z ως ρίζα του P είναι ίδια με αυτήν

του $\bar{z}$ (αφού τα ίδια ισχύουν και για τα P', P'', κτλ)

Αυτό φυσικά δεν ισχύει αν $z \in \mathbb{R}$. Τότε, το μόνο που μπορούμε

να πούμε με σιγουριά είναι ότι $(x-z) \mid P$.

<u>Πόρισμα 1:</u> Έστω $P \in \mathbb{R}[X]$ με $\deg P$ περιττό. Τότε το P έχει

τουλάχιστον μια ρίζα στο $\mathbb{R}$.

<u>Απόδειξη:</u> Από το Θ.Θ.Α, το P έχει $\deg P$ ρίζες στο $\mathbb{C}$. Αφού οι

μη πραγματικές ρίζες έρχονται σε ζεύγη (με την ίδια πολλαπλότητα)

πρέπει αναγκαστικά μια ρίζα να είναι πραγματική.

<u>Πόρισμα 2:</u> Έστω $P \in \mathbb{R}[X]$. Τότε P ανάγωγο $\Leftrightarrow$ $\deg P = 1$ ή

$\deg P = 2$ και το P δεν έχει ρίζα στο $\mathbb{R}$

Απόδειξη: "$\Leftarrow$" Από τις Παρατηρήσεις.

"$\Rightarrow$" Αν $\deg P \geq 2$ και το P έχει ρίζα στο $\mathbb{R}$, τότε δεν είναι ανάγωγο.

Αν το P δεν έχει ρίζα στο $\mathbb{R}$ και $\deg P > 2$, τότε από το Θ.Θ.Α. έχει ρίζα $z \in \mathbb{C} \setminus \mathbb{R}$ και διαιρείται από το πολυώνυμο f_z (βλ. ⊛)

Οπότε και πάλι το P δεν είναι ανάγωγο.

Παρατήρηση:

Στο $\mathbb{Q}[X]$ υπάρχουν ανάγωγα πολυώνυμα οποιουδήποτε βαθμού.

Π.χ. Το πολυώνυμο $x^n - 2 \in \mathbb{Q}[X]$ είναι ανάγωγο $\forall\, n \in \mathbb{N}^*$

Κριτήριο Eisenstein:

Έστω $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ με $a_n \neq 0$. Αν υπάρχει πρώτος αριθμός p τέτοιος ώστε:

- $p \mid a_i \quad \forall\, i = 0, 1, \ldots, n-1$
- $p \nmid a_n$
- $p^2 \nmid a_0$

τότε το P είναι ανάγωγο στο $\mathbb{Q}[X]$.

Παρατήρηση: Έστω $\mathbb{K} \subseteq \mathbb{L}$ σώματα και $P \in \mathbb{K}[X]$.

P ανάγωγο στο $\mathbb{L}[X] \Rightarrow P$ ανάγωγο στο $\mathbb{K}[X]$.

Το αντίστροφο δεν ισχύει (π.χ. $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{R}$, $P = x^2 - 2$).