ΠΟΛΥΩΝΥΜΑ ΚΑΙ ΠΟΛΥΩΝΥΜΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ

ΜΙΧΑΛΗΣ ΤΣΙΓΓΕΛΗΣ

Ε.ΔΙ.Π, Τμήμα Ηλεκτρολόγων Μηχανικών & Τεχνολογίας Υπολογιστών,

Πολυτεχνική Σχολή Πανεπιστημίου Πατρών

email: mtsingelis@upatras.gr

ΠΕΡΙΛΗΨΗ

Στην παρούσα εργασία εξετάζουμε τη σχέση που υπάρχει μεταξύ των πολυωνύμων επί ενός δακτυλίου και των πολυωνυμικών συναρτήσεων επί του ίδιου δακτυλίου. Έστω R ένας αντιμεταθετικός δακτύλιος με μονάδα, $R[x]$ ο δακτύλιος πολυωνύμων επί του R, $F(R)$ ο δακτύλιος απεικονίσεων επί του R και $f_{\pi(x)}$ η πολυωνυμική συνάρτηση που αντιστοιχεί στο πολυώνυμο $\pi(x)$. Τότε η απεικόνιση $G: R[x] \to F(R)$ / $\pi(x) \to f_{\pi(x)}$ είναι ομομορφισμός δακτυλίων. Όμως η απεικόνιση G δεν είναι πάντα 1-1 (δηλ. δεν είναι πάντα μονομορφισμός δακτυλίων και επομένως δεν μπορούμε πάντα να "ταυτίζουμε" ένα πολυώνυμο με την αντίστοιχη πολυωνυμική του συνάρτηση). Αποδεικνύουμε ότι αν ένας δακτύλιος R είναι πεπερασμένος με $|R| \geq 2$, τότε η απεικόνιση G δεν είναι 1-1 (και άρα, σε αυτήν την περίπτωση, ένα πολυώνυμο επί του R δεν "ταυτίζεται" με την πολυωνυμική του συνάρτηση). Αν ο δακτύλιος R είναι ένα άπειρο σώμα τότε η απεικόνιση G είναι 1-1 (και άρα στο σύνολο $\mathbb{R}$ των πραγματικών αριθμών όπως και στο σύνολο $\mathbb{C}$ των μιγαδικών αριθμών ισχύει η "αλγεβρική ταύτιση" των πολυωνύμων με τις αντίστοιχες πολυωνυμικές τους συναρτήσεις). Δίνουμε παράδειγμα ενός άπειρου αντιμεταθετικού δακτυλίου με μονάδα για τον οποίο η απεικόνιση G δεν είναι 1-1. Τέλος παρουσιάζουμε μία ικανή και αναγκαία συνθήκη που πρέπει να ικανοποιεί ένας αντιμεταθετικός δακτύλιος με μονάδα ώστε η απεικόνιση G να είναι 1-1 (και επομένως έχουμε μία ικανή και αναγκαία συνθήκη για το πότε μπορούμε να "ταυτίζουμε" ένα πολυώνυμο με την αντίστοιχη πολυωνυμική του συνάρτηση).

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Δακτύλιος πολυωνύμων, μονομορφισμός δακτυλίων, πολυωνυμική συνάρτηση.

1. ΕΙΣΑΓΩΓΗ

<u>Ορισμός 1.1 [4]:</u> Έστω R μη κενό σύνολο και "+", "$\cdot$" δύο πράξεις επί του R (η "+" καλείται πρόσθεση και η "$\cdot$" καλείται πολλαπλασιασμός). Η τριάδα $(R,+,\cdot)$ καλείται δακτύλιος αν ισχύουν τα εξής:

i) Το ζευγάρι $(R,+)$ είναι <u>αβελιανή ομάδα</u>.

Αυτό σημαίνει ότι ισχύουν οι ιδιότητες:

ια) $\alpha+b=b+\alpha$ για κάθε $\alpha, b \in R$ (αντιμεταθετική ιδιότητα πρόσθεσης).

ιβ) $(\alpha+b)+c=\alpha+(b+c)$ για κάθε $\alpha, b, c \in R$ (προσεταιριστική ιδιότητα πρόσθεσης).

ιγ) Υπάρχει ένα στοιχείο $0 \in R$ τέτοιο ώστε για κάθε $\alpha \in R$ να ισχύει $\alpha+0=\alpha$ (ύπαρξη ουδέτερου στοιχείου για την πρόσθεση - καλείται μηδέν).

ιδ) Για κάθε $\alpha \in R$ υπάρχει ένα στοιχείο $-\alpha \in R$ τέτοιο ώστε $\alpha+(-\alpha)=0$ (ύπαρξη συμμετρικού στοιχείου του α ως προς την πρόσθεση - καλείται αντίθετο του α).

ii) Το ζευγάρι $(R,\cdot)$ είναι <u>ημιομάδα</u>.

Αυτό σημαίνει ότι $(\alpha \cdot b)\cdot c=\alpha \cdot (b \cdot c)$ για κάθε $\alpha, b, c \in R$ (προσεταιριστική ιδιότητα πολλαπλασιασμού).

iii) $\alpha(b+c)=\alpha \cdot b+\alpha \cdot c$ και $(\alpha+b)\cdot c=\alpha \cdot c+b \cdot c$ για κάθε $\alpha, b, c \in R$ (επιμεριστική ιδιότητα). □

<u>Ορισμός 1.2]3]:</u> Ένας δακτύλιος $(R,+,\cdot)$ καλείται

i) αντιμεταθετικός αν για κάθε $\alpha, b \in R$ ισχύει: $\alpha \cdot b=b \cdot \alpha$ (αντιμεταθετική ιδιότητα πολλαπλασιασμού).

ii) δακτύλιος με μονάδα (ή μοναδιαίος δακτύλιος) αν υπάρχει ένα στοιχείο $1 \in R$ με την ιδιότητα:

$$\alpha \cdot 1=1 \cdot \alpha=\alpha \text{ για κάθε } \alpha \in \mathbb{R}$$

(ύπαρξη ουδέτερου στοιχείου για τον πολλαπλασιασμό - το 1 καλείται μονάδα) □

<u>Παρατήρηση 1.3:</u> Σε ένα μοναδιαίο δακτύλιο R ισχύει το εξής:

$$|R| \geq 2 \text{ αν και μόνο αν } 1 \neq 0$$

($|R|$ είναι το πλήθος των στοιχείων του συνόλου R). Στα επόμενα σε έναν μοναδιαίο δακτύλιο θα θεωρούμε πάντα $1 \neq 0$ κι άρα θα ισχύει $|R| \geq 2$. □

Παρατήρηση 1.4:

i) Λόγω των ιδιοτήτων **ια)** και **ιβ)** του Ορισμού 1.1 έχουμε ότι με οποιοδήποτε τρόπο και να προσθέσουμε τα στοιχεία α_1, α_2, ..., α_n του R (n θετικός ακέραιος), τότε πάντα παίρνουμε το ίδιο στοιχείο του R το οποίο θα συμβολίζουμε με $\alpha_1 + \alpha_2 + ... + \alpha_n$.

ii) Λόγω της ιδιότητας **ii)** του Ορισμού 1.1 έχουμε ότι με οποιοδήποτε τρόπο και αν πολλαπλασιάσουμε τα στοιχεία α_1, α_2, ..., α_n του R (n θετικός ακέραιος) χωρίς όμως να αλλάξουμε τη (δοσμένη) σειρά α_1, α_2, ..., α_n, τότε πάντα παίρνουμε το ίδιο στοιχείο του R το οποίο θα συμβολίζουμε με $\alpha_1 \cdot \alpha_2 \cdot ... \cdot \alpha_n$.

iii) Για περισσότερες ιδιότητες που αφορούν σε στοιχεία ενός δακτυλίου βλ. [4] § 4.1, 4.2.

□

Θα ορίσουμε τώρα το δακτύλιο πολυωνύμων επί ενός δακτυλίου R [1]. Έστω $(R,+,\cdot)$ μοναδιαίος δακτύλιος (με μονάδα το 1). Για κάθε $\kappa \in \mathbb{Z}$ με $\kappa \geq 0$ θέτουμε $R_\kappa = R$ και στη συνέχεια θεωρούμε το καρτεσιανό γινόμενο $\prod_{i=0}^{\infty} R_i$ (: είναι το σύνολο όλων των "ακολουθιών" με στοιχεία από το R). Η ισότητα στο $\prod_{i=0}^{\infty} R_i$ ορίζεται ως εξής:

$$(\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n, ...) = (b_0, b_1, b_2, ..., b_n, ...) \Leftrightarrow \alpha_j = b_j,\ j = 0,1,2,...$$

Αν $A = (\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n, ...) \in \prod_{i=0}^{\infty} R_i$, τότε θα συμβολίσουμε με $h(A)$ το πλήθος των μη μηδενικών συντεταγμένων του A (προφανώς $h(A) \in \{0,1,2,...\} \cup \{\infty\}$). Θέτουμε

$$\mathfrak{I} = \left\{ A \in \prod_{i=0}^{\infty} R_i : h(A) < \infty \right\}$$

(το $\mathfrak{I}$ είναι το σύνολο των "ακολουθιών" του R των οποίων το πλήθος των μη μηδενικών "συντεταγμένων" τους είναι πεπερασμένο ή όλες τους οι συντεταγμένες είναι μηδέν) και επί του $\mathfrak{I}$ ορίζουμε τις εξής πράξεις:

- $(\alpha_0, \alpha_1, \alpha_2, ...) \oplus (b_0, b_1, b_2, ...) = (\alpha_0 + b_0, \alpha_1 + b_1, \alpha_2 + b_2, ...)$,

- $(\alpha_0, \alpha_1, \alpha_2, ...) \odot (b_0, b_1, b_2, ...) = (c_0, c_1, c_2, ...)$, όπου

$$c_m = \alpha_0 \cdot b_m + \alpha_1 \cdot b_{m-1} + ... + \alpha_m \cdot b_0 \left(= \sum_{\lambda=0}^{m} \alpha_\lambda \cdot b_{m-\lambda} \right),\ m = 0,1,2,...$$

Τότε ισχύει το εξής:

<u>Θεώρημα 1.5 [1]:</u> Η τριάδα $(\mathfrak{I}, \oplus, \odot)$ είναι μοναδιαίος δακτύλιος με μηδέν το $(0,0,0,...,0,...)$ και μονάδα το $(1,0,0,...,0,...)$. □

<u>Παρατήρηση 1.6 [1]:</u> Με τη βοήθεια της πράξης "$\odot$" που ορίσαμε παραπάνω έχουμε τα εξής:

i) Αν το στοιχείο $(0,1,0,0,...,0,...)$ του $\mathfrak{I}$ το συμβολίσουμε με x, τότε:

$$x^0 := (1,0,0,0,...0,...)$$

$$x^1 := x = (0,1,0,0,...0,...)$$

$$x^2 := x \odot x = ... = (0,0,1,0,...0,...)$$

$$x^3 := x \odot x \odot x = ... = (0,0,0,1,0,...0,...)$$

και γενικά

$$x^n := \underset{\leftarrow\ \text{n φορές}\ \rightarrow}{x \odot x \odot ... \odot x} = ... = \Big(0,0,...,0, \underset{\text{n+1 θέση}}{1}, 0,...0,...\Big),\ n \in \mathbb{Z}\ \text{με}\ n \geq 0$$

(δηλ. το x^n έχει το 1 στην $n+1$ θέση και το 0 στις υπόλοιπες).

ii) Για κάθε $\alpha, b \in R$ και για κάθε $n, m \in \mathbb{Z}$ με $n \geq 0$ και $m \geq 0$ έχουμε:

α) $(\alpha,0,0,...,0,...) \odot x^n = (\alpha,0,0,...,0,...) \odot \Big(0,0,...,0, \underset{\text{n+1 θέση}}{1}, 0,...,0,...\Big) = ... =$

$$= \Big(0,0,...,0, \underset{\text{n+1 θέση}}{\alpha}, 0,...,0,...\Big)$$

β)

$$\big((\alpha,0,0,...,0,...) \odot x^n\big) \oplus \big((b,0,0,...,0,...) \odot x^n\big) \underset{\alpha)}{=} \Big(0,0,...,0, \underset{\text{n+1 θέση}}{\alpha}, 0,...,0,...\Big) \oplus \Big(0,0,...,0, \underset{\text{n+1 θέση}}{b}, 0,...,0,...\Big) =$$

$$= \Big(0,0,...,0, \underset{\text{n+1 θέση}}{\alpha+b}, 0,...,0,...\Big) \underset{\alpha)}{=} (\alpha+b,0,0,...,0,...) \odot x^n =$$

$$= \big((\alpha,0,0,...,0,...) \oplus (b,0,0,...,0,...)\big) \odot x^n$$

γ)

$$\left((\alpha,0,0,...,0,...)\odot x^{n}\right)\odot\left((b,0,0,...,0,...)\odot x^{m}\right)\underset{\alpha)}{=}\left(0,0,...,0,\underset{n+1\text{ θέση}}{\alpha},0,...,0,...\right)\odot\left(0,0,...,0,\underset{m+1\text{ θέση}}{b},0,...,0,...\right)=$$

$$=\left(0,0,...,0,\underset{n+m+1\text{ θέση}}{\alpha\cdot b},0,...,0,...\right)\underset{\alpha)}{=}(\alpha\cdot b,0,0,...,0,...)\odot x^{n+m}=$$

$$=\left((\alpha,0,0,...,0,...)\odot(b,0,0,...,0,...)\right)\odot x^{n+m}$$

□

<u>Ορισμός 1.7 [1]:</u> Έστω $(R,+,\cdot)$, $\left(T,\underset{\sim}{+},*\right)$ δύο δακτύλιοι και $f:R\to T$ απεικόνιση. Η f καλείται:

i) <u>ομομορφισμός</u> αν για κάθε $\alpha,b\in R$ ισχύει $f(\alpha+b)=f(\alpha)\underset{\sim}{+}f(b)$ και $f(\alpha\cdot b)=f(\alpha)*f(b)$.

ii) <u>μονομορφισμός</u> αν είναι ομομορφισμός και 1-1.

iii) <u>ισομορφισμός</u> αν είναι μονομορφισμός και επί (τότε γράφουμε $R\underset{f}{\cong}T$). □

<u>Παρατήρηση 1.8 [4]:</u> Αν $f:R\to T$ ομομορφισμός δακτυλίων και τα $0_R\in R$, $0_T\in T$ είναι τα μηδέν των R, T αντίστοιχα, τότε:

i) $f(-\alpha)=-f(\alpha)$ για κάθε $\alpha\in R$.

ii) $f(0_R)=0_T$.

iii) η f είναι 1-1 (και άρα μονομορφισμός) αν και μόνο αν για $x\in R$ ισχύει:

$$f(x)=0_T\Rightarrow x=0_R$$

□

Θεωρούμε τώρα την απεικόνιση

$$\varepsilon:R\to\mathfrak{I}\ /\ \alpha\to(\alpha,0,0,...,0,...)$$

Για την απεικόνιση ε ισχύει η εξής:

<u>Πρόταση 1.9 [1]:</u> Η απεικόνιση ε είναι μονομορφισμός δακτυλίων. □

Επειδή η ε είναι μονομορφισμός, τότε [1] για την εικόνα του R μέσω της ε (δηλ. για το $\varepsilon(R)$) έχουμε αμέσως τα εξής:

α) το $\varepsilon(R)$ είναι υποδακτύλιος του $\mathfrak{I}$,

β) $R \underset{\varepsilon}{\cong} \varepsilon(R)$.

Άρα μπορούμε να ταυτίσουμε τον δακτύλιο R με τον $\varepsilon(R)$ (δηλ. το $\alpha \in R$ με το $(\alpha,0,0,...,0,...) \in \mathfrak{I}$) και επομένως ο δακτύλιος R μπορεί να θεωρηθεί υποδακτύλιος του $\mathfrak{I}$.

Μάλιστα [1] αν $A \in \mathfrak{I}$ τότε (από τον ορισμό του $\mathfrak{I}$) έχουμε αμέσως ότι

$$A = \Big(\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n, \underbrace{0,...,0,...}_{\leftarrow \text{ όλα } 0 \ \rightarrow}\Big)$$

και επομένως από τον ορισμό της πράξης "$\oplus$" και την Παρατήρηση 1.6 έχουμε:

$$\begin{aligned}
A &= \Big(\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n, \underbrace{0,...,0,...}_{\leftarrow \text{ όλα } 0 \ \rightarrow}\Big) = \\
&= (\alpha_0,0,0,...,0,...) \oplus (0,\alpha_1,0,...,0,...) \oplus (0,0,\alpha_2,0,...,0,...) \oplus ... \oplus \Big(0,0,0,...,0, \underset{n+1 \text{ θέση}}{\alpha_n}, 0...,0,...\Big) = \\
&= (\alpha_0,0,0,...,0,...) \oplus \big((\alpha_1,0,0,...,0,...) \odot x\big) \oplus \big((\alpha_2,0,0,...,0,...) \odot x^2\big) \oplus ... \oplus \big((\alpha_n,0,0,...,0,...) \odot x^n\big) \\
&\Big(= \big((\alpha_0,0,0,...,0,...) \odot x^0\big) \oplus \big((\alpha_1,0,0,...,0,...) \odot x^1\big) \oplus \big((\alpha_2,0,0,...,0,...) \odot x^2\big) \oplus ... \oplus \big((\alpha_n,0,0,...,0,...) \odot x^n\big)\Big)
\end{aligned}$$

Τότε (λόγω της προαναφερθείσας ταύτισης του $\alpha \in R$ με το $(\alpha,0,0,...,0,...) \in \mathfrak{I}$) έχουμε ότι

$$A \equiv \alpha_0 \oplus (\alpha_1 \odot x) \oplus (\alpha_2 \odot x^2) \oplus ... \oplus (\alpha_n \odot x^n)$$

και αν (όπως συνήθως συμβαίνει στην πράξη σε ανάλογες περιπτώσεις) χρησιμοποιήσουμε τα ίδια σύμβολα πράξεων για τις πράξεις των δακτυλίων R και $\mathfrak{I}$ (δηλ. αντί των "$\oplus$" και "$\odot$" χρησιμοποιήσουμε "+" και "$\cdot$" αντίστοιχα), τότε έχουμε αμέσως ότι

$$A \equiv \alpha_0 + \alpha_1 \cdot x + \alpha_2 \cdot x^2 + ... + \alpha_n \cdot x^n \qquad (1)$$

(δηλ. τον κλασσικό συμβολισμό των πολυωνύμων). Μάλιστα από την προηγηθείσα ανάλυση έπεται αμέσως ότι

$$A \equiv \alpha_0 \cdot x^0 + \alpha_1 \cdot x^1 + \alpha_2 \cdot x^2 + ... + \alpha_n \cdot x^n = \sum_{m=0}^{n} \alpha_m \cdot x^m$$

Ο δακτύλιος $\mathfrak{I}$ συμβολίζεται με $R[x]$ και καλείται **δακτύλιος πολυωνύμων** επί του R [1]. Τα στοιχεία του $R[x]$ (τα οποία είναι ουσιαστικά της μορφής (1)) συμβολίζονται συνήθως με $\pi(x)$, $q(x)$, $r(x)$, $\varphi(x)$ κ.λπ.. Από τα παραπάνω έπεται αμέσως ότι αν

$\pi(x) = \alpha_0 + \alpha_1 \cdot x + \alpha_2 \cdot x^2 + ... + \alpha_n \cdot x^n$ και $q(x) = b_0 + b_1 \cdot x + b_2 \cdot x^2 + ... + b_m \cdot x^m$ είναι δύο πολυώνυμα του $R[x]$ με $n \le m$, τότε

- $\pi(x) = q(x) \Leftrightarrow \begin{cases} \alpha_i = b_i, & i = 1,2,...,n \\ \\ b_j = 0, & j = n+1,...,m \end{cases}$
- $\pi(x) + q(x) = (\alpha_0 + b_0) + (\alpha_1 + b_1) \cdot x + ... + (\alpha_n + b_n) \cdot x^n + b_{n+1} \cdot x^{n+1} + ... + b_m \cdot x^m$
- $\pi(x) \cdot q(x) = c_0 + c_1 \cdot x + c_2 \cdot x^2 + ... + c_{n+m} \cdot x^{n+m}$ όπου

$$c_\rho = \begin{cases} \alpha_0 b_\rho + \alpha_1 b_{\rho-1} + ... + \alpha_\rho b_0, & \rho = 0,1,...,n \\ \\ \alpha_0 b_\rho + \alpha_1 b_{\rho-1} + ... + \alpha_n b_{\rho-n}, & \rho = n+1,...,m \\ \\ \alpha_{\rho-m} b_m + \alpha_{\rho-m+1} b_{m-1} + ... + \alpha_n b_{\rho-n}, & \rho = m+1,...,m+n \end{cases}$$

Επομένως, αν τα πολυώνυμα τα θεωρήσουμε στην μορφή $\alpha_0 + \alpha_1 \cdot x + \alpha_2 \cdot x^2 + ... + \alpha_n \cdot x^n$, τότε για την ισότητά τους και τις πράξεις ισχύουν οι "γνωστές" διαδικασίες (δηλ. της ισότητας των συντελεστών των ομοιοβάθμιων όρων, της αναγωγής όμοιων όρων και του επιμερισμού).

Έστω τώρα $(R,+,\cdot)$ μοναδιαίος δακτύλιος (με μονάδα το 1). Με $F(R)$ συμβολίζουμε το σύνολο όλων των απεικονίσεων από το R στο R. Η ισότητα στο $F(R)$ ορίζεται με το γνωστό τρόπο της ισότητας των απεικονίσεων, δηλαδή για $f, g \in F(R)$ ορίζουμε:

$$f = g \Leftrightarrow f(y) = g(y) \text{ για κάθε } y \in \mathbb{R}$$

Επίσης για κάθε $f, g \in F(R)$ ορίζουμε:

- $f +' g : R \to R \;/\; x \to f(x) + g(x)$
- $f \cdot' g : R \to R \;/\; x \to f(x) \cdot g(x)$

<u>**Θεώρημα 1.10 [2]:**</u> Η τριάδα $(F(R), +', \cdot')$ είναι μοναδιαίος δακτύλιος (με μηδέν την απεικόνιση $\mathbf{0} : R \to R \;/\; x \to 0$, αντίθετη της f την απεικόνιση $-f : R \to R \;/\; x \to -f(x)$ και μονάδα την απεικόνιση $\mathbf{1} : R \to R \;/\; x \to 1$). □

Μάλιστα [2] αν ο δακτύλιος R είναι επιπλέον και αντιμεταθετικός, τότε η τριάδα $\left(F(R),+',\cdot'\right)$ είναι αντιμεταθετικός δακτύλιος με μονάδα. Συνήθως για την πρόσθεση και τον πολλαπλασιασμό του $F(R)$ χρησιμοποιούμε τα ίδια σύμβολα με αυτά του R αφού δεν δημιουργείται σύγχυση διότι στο σύνολο $F(R)$ αναφέρονται σε απεικονίσεις (και όχι σε στοιχεία του R). Επομένως στα επόμενα αντί των "$+'$" και "$\cdot'$" θα χρησιμοποιούμε τα σύμβολα "+" και "$\cdot$" αντίστοιχα.

<u>Ορισμός 1.11 [2]:</u> Μία απεικόνιση $g \in F(R)$ καλείται πολυωνυμική συνάρτηση αν υπάρχουν $n \in \mathbb{Z}$ με $n \geq 0$ και $\alpha_0, \alpha_1, \ldots, \alpha_n \in R$ τέτοια ώστε $g(y) = \alpha_0 + \alpha_1 y + \ldots + \alpha_n y^n$ για κάθε $y \in R$. Τότε λέμε ότι η g είναι η πολυωνυμική συνάρτηση του πολυωνύμου $\pi(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ και θα τη συμβολίζουμε με $f_{\pi(x)}$ - δηλ.

$$f_{\pi(x)} : R \to R \ / \ y \to \alpha_0 + \alpha_1 y + \ldots + \alpha_n y^n$$ □

<u>Παρατήρηση 1.12:</u> Είναι άμεσο ότι σε ίσα πολυώνυμα αντιστοιχούν ίσες πολυωνυμικές συναρτήσεις. Αν όμως δύο πολυωνυμικές συναρτήσεις είναι ίσες, τότε τα πολυώνυμα από τις οποίες προέρχονται είναι ίσα; Όπως θα δούμε στη συνέχεια αυτό δεν ισχύει για όλους τους αντιμεταθετικούς δακτυλίους με μονάδα. □

2. ΚΥΡΙΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Αν $\pi(x)$, $q(x)$ είναι δύο πολυώνυμα με πραγματικούς συντελεστές για τα οποία $\pi(y) = q(y)$ για κάθε $y \in \mathbb{R}$, τότε τα πολυώνυμα $\pi(x)$, $q(x)$ είναι ίσα. Η ιδιότητα αυτή, η οποία ισχύει και για πολυώνυμα με μιγαδικούς συντελεστές, ισχύει σε οποιοδήποτε δακτύλιο πολυωνύμων ή υπάρχουν και δακτύλιοι πολυωνύμων για τους οποίους δεν ισχύει; Στα επόμενα θα προσπαθήσουμε να απαντήσουμε στα προηγούμενα ερωτήματα.
Θεωρούμε την απεικόνιση

$$G : R[x] \to F(R) \ / \ \pi(x) \to f_{\pi(x)}$$

(δηλ. σε κάθε πολυώνυμο αντιστοιχούμε την πολυωνυμική του συνάρτηση).

Για την απεικόνιση G ισχύει η εξής:

<u>Πρόταση 2.1:</u> Έστω $(R,+,\cdot)$ δακτύλιος με μονάδα. Τότε η απεικόνιση G είναι ομομορφισμός δακτυλίων.

<u>Απόδειξη:</u> Η G είναι προφανώς καλά ορισμένη.

Έστω $\pi(x)=\alpha_0+\alpha_1x+...+\alpha_nx^n$, $q(x)=b_0+b_1x+...+b_mx^m$ δύο στοιχεία του $R[x]$. Τα πολυώνυμα $\pi(x)$, $q(x)$ μπορούμε προφανώς να τα γράψουμε στη μορφή:

- $\pi(x)=\alpha_0+\alpha_1x+...+\alpha_nx^n+\alpha_{n+1}x^{n+1}+...+\alpha_{n+m}x^{n+m}$ με $\alpha_{n+1}=...=\alpha_{n+m}=0$,
- $q(x)=b_0+b_1x+...+b_mx^m+b_{m+1}x^{m+1}+...+b_{m+n}x^{m+n}$ με $b_{m+1}=...=b_{m+n}=0$.

i) $\underline{G(\pi(x)+q(x))\overset{?}{=}G(\pi(x))+G(q(x))}$

Έστω $y\in R$. Θα δείξουμε ότι $f_{\pi(x)+q(x)}(y)=\left(f_{\pi(x)}+f_{q(x)}\right)(y)$.

Επειδή $\pi(x)+q(x)=(\alpha_0+b_0)+(\alpha_1+b_1)x+...+(\alpha_{n+m}+b_{n+m})x^{n+m}$, τότε έχουμε:

$$\begin{aligned} f_{\pi(x)+q(x)}(y)&=(\alpha_0+b_0)+(\alpha_1+b_1)y+...+(\alpha_{n+m}+b_{n+m})y^{n+m}= \\ &=\left(\alpha_0+\alpha_1y+...+\alpha_{n+m}y^{n+m}\right)+\left(b_0+b_1y+...+b_{m+n}y^{m+n}\right)= \\ &=f_{\pi(x)}(y)+f_{q(x)}(y)=\left(f_{\pi(x)}+f_{q(x)}\right)(y) \end{aligned}$$

Άρα δείξαμε ότι $f_{\pi(x)+q(x)}(y)=\left(f_{\pi(x)}+f_{q(x)}\right)(y)$ για κάθε $y\in R$. Συνεπώς $f_{\pi(x)+q(x)}=f_{\pi(x)}+f_{q(x)}$ και επομένως $G(\pi(x)+q(x))=G(\pi(x))+G(q(x))$.

ii) $\underline{G(\pi(x)\cdot q(x))\overset{?}{=}G(\pi(x))\cdot G(q(x))}$

Έστω $y\in R$. Θα δείξουμε ότι $f_{\pi(x)\cdot q(x)}(y)=\left(f_{\pi(x)}\cdot f_{q(x)}\right)(y)$.

Επειδή $\pi(x)\cdot q(x)=c_0+c_1x+...+c_{n+m}x^{n+m}$ όπου $c_\kappa=\alpha_0b_\kappa+\alpha_1b_{\kappa-1}+...+\alpha_\kappa b_0$ για $\kappa=0,1,2,...,n+m$, τότε έχουμε:

$$\begin{aligned} f_{\pi(x)\cdot q(x)}(y)&=c_0+c_1y+...+c_{n+m}y^{n+m}= \\ &=\alpha_0\cdot b_0+(\alpha_0\cdot b_1+\alpha_1\cdot b_0)y+...+(\alpha_0\cdot b_{m+n}+\alpha_1\cdot b_{m+n-1}+...+\alpha_{n+m-1}\cdot b_1+\alpha_{n+m}\cdot b_0)y^{n+m}= \\ &=\left(\alpha_0+\alpha_1y+...+\alpha_{n+m}y^{n+m}\right)\cdot\left(b_0+b_1y+...+b_{m+n}y^{m+n}\right) \\ &=f_{\pi(x)}(y)\cdot f_{q(x)}(y)=\left(f_{\pi(x)}\cdot f_{q(x)}\right)(y) \end{aligned}$$

Άρα δείξαμε ότι $f_{\pi(x)\cdot q(x)}(y)=\left(f_{\pi(x)}\cdot f_{q(x)}\right)(y)$ για κάθε $y\in R$. Συνεπώς $f_{\pi(x)\cdot q(x)}=f_{\pi(x)}\cdot f_{q(x)}$ και επομένως $G(\pi(x)\cdot q(x))=G(\pi(x))\cdot G(q(x))$.

Από **i)**, **ii)** και τον Ορισμό 1.7i), έπεται αμέσως ότι η G είναι ομομορφισμός δακτυλίων. □

<u>Παρατήρηση 2.2:</u> Αφού η G είναι ομομορφισμός δακτυλίων, τότε η εικόνα του $G(R[x])$ είναι υποδακτύλιος του $F(R)$ [1] και μάλιστα περιέχει και τη μονάδα του $F(R)$ αφού για το σταθερό πολυώνυμο $\pi(x)=1$ έχουμε αμέσως ότι $f_{\pi(x)}=\mathbf{1}$. Όμως προφανώς το $G(R[x])$ είναι το σύνολο των πολυωνυμικών συναρτήσεων του R. Άρα το σύνολο των πολυωνυμικών συναρτήσεων ενός δακτυλίου με μονάδα είναι δακτύλιος με μονάδα. Επίσης, αφού η αντιμεταθετικότητα προφανώς διατηρείται μέσω ομομορφισμών δακτυλίων, τότε έχουμε αμέσως ότι <u>*το σύνολο των πολυωνυμικών συναρτήσεων ενός αντιμεταθετικού δακτυλίου με μονάδα είναι αντιμεταθετικός δακτύλιος με μονάδα.*</u> □

Εδώ πρέπει να τονίσουμε ότι η απεικόνιση G δεν είναι απαραίτητα μονομορφισμός (δηλ. 1-1) και επομένως δεν μπορούμε πάντα να "ταυτίσουμε" ένα πολυώνυμο $\pi(x)=\alpha_0+\alpha_1x+...+\alpha_nx^n$ με την πολυωνυμική του συνάρτηση $f_{\pi(x)}:R\to R \,/\, y\to \alpha_0+\alpha_1y+...+\alpha_ny^n$ (αυτό εξαρτάται από τον δακτύλιο R) και επομένως ένα πολυώνυμο $\pi(x)$ και η πολυωνυμική του συνάρτηση $f_{\pi(x)}$ μπορεί να έχουν διαφορετική αλγεβρική συμπεριφορά. Επειδή η G είναι ομομορφισμός, τότε η αλγεβρική συμπεριφορά των πολυωνύμων μεταφέρεται και στις πολυωνυμικές τους συναρτήσεις. Το αντίστροφο όμως δεν ισχύει πάντα. (δηλ. η αλγεβρική συμπεριφορά των πολυωνυμικών συναρτήσεων δεν μεταφέρεται πάντα και στα πολυώνυμα από τα οποία προέρχονται). Π.χ. αν $\pi(x)$, $q(x)$, $r(x)$, $\sigma(x)$ είναι πολυώνυμα επί ενός μοναδιαίου δακτυλίου R, τότε:

- επειδή η G είναι ομομορφισμός έχουμε
$$G(\pi(x)\cdot q(x)+r(x))=G(\pi(x))\cdot G(q(x))+G(r(x))$$
και άρα $f_{\pi(x)\cdot q(x)+r(x)}=f_{\pi(x)}\cdot f_{q(x)}+f_{r(x)}$ (δηλ. η πολυωνυμική σχέση $\pi(x)\cdot q(x)+r(x)$ μεταφέρεται και στις πολυωνυμικές τους συναρτήσεις).
- αν ισχύει η σχέση $f_{\sigma(x)}=f_{\pi(x)}\cdot f_{q(x)}+f_{r(x)}$ και άρα (επειδή η G είναι ομομορφισμός) ισχύει η $G(\sigma(x))=G(\pi(x))\cdot G(q(x))+G(r(x))=G(\pi(x)\cdot q(x)+r(x))$, τότε δεν έπεται πάντα ότι $\sigma(x)=\pi(x)\cdot q(x)+r(x)$ (δηλ. η σχέση $f_{\sigma(x)}=f_{\pi(x)}\cdot f_{q(x)}+f_{r(x)}$ των πολυωνυμικών συναρτήσεων $f_{\sigma(x)}$, $f_{\pi(x)}$, $f_{q(x)}$, $f_{r(x)}$ δεν μεταφέρεται πάντα στα πολυώνυμα $\pi(x)$, $q(x)$, $r(x)$, $\sigma(x)$ από τα οποία προέρχονται οι πολυωνυμικές συναρτήσεις $f_{\sigma(x)}$, $f_{\pi(x)}$, $f_{q(x)}$, $f_{r(x)}$ αντίστοιχα).

<u>Παράδειγμα 2.3:</u> Θεωρούμε το σύνολο $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ (ακέραιοι mod 3). Το σύνολο αυτό εφοδιασμένο με τη γνωστή πρόσθεση και το γνωστό πολλαπλασιασμό των ακεραίων mod 3 είναι σώμα (άρα και αντιμεταθετικός δακτύλιος με μονάδα). Οι πίνακες των παραπάνω πράξεων είναι (ως γνωστόν) οι πίνακες 1, 2 αντίστοιχα:

$+$	$\bar{\mathbf{0}}$	$\bar{\mathbf{1}}$	$\bar{\mathbf{2}}$
$\bar{\mathbf{0}}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{\mathbf{1}}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{\mathbf{2}}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Πίνακας 1

$\cdot$	$\bar{\mathbf{0}}$	$\bar{\mathbf{1}}$	$\bar{\mathbf{2}}$
$\bar{\mathbf{0}}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{\mathbf{1}}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{\mathbf{2}}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Πίνακας 2

Επί του $\mathbb{Z}_3[x]$ θεωρούμε τα πολυώνυμα $\sigma(x) = \bar{1}x^2 + \bar{1}x$, $\pi(x) = \bar{1}x$, $q(x) = \bar{1}x^4$ και $r(x) = \bar{1}x^2$. Οι αντίστοιχες πολυωνυμικές συναρτήσεις τους είναι οι εξής:

α) $f_{\sigma(x)} : \mathbb{Z}_3 \to \mathbb{Z}_3 \ / \ \bar{0} \to \bar{0},\ \bar{1} \to \bar{2},\ \bar{2} \to \bar{0}$

β) $f_{\pi(x)} : \mathbb{Z}_3 \to \mathbb{Z}_3 \ / \ \bar{0} \to \bar{0},\ \bar{1} \to \bar{1},\ \bar{2} \to \bar{2}$

γ) $f_{q(x)} : \mathbb{Z}_3 \to \mathbb{Z}_3 \ / \ \bar{0} \to \bar{0},\ \bar{1} \to \bar{1},\ \bar{2} \to \bar{1}$

δ) $f_{r(x)} : \mathbb{Z}_3 \to \mathbb{Z}_3 \ / \ \bar{0} \to \bar{0},\ \bar{1} \to \bar{1},\ \bar{2} \to \bar{1}$

Τότε έπεται ότι

$$f_{\pi(x)} \cdot f_{q(x)} + f_{r(x)} : \mathbb{Z}_3 \to \mathbb{Z}_3 \ / \ \bar{0} \to \bar{0},\ \bar{1} \to \bar{2},\ \bar{2} \to \bar{0}$$

Άρα $f_{\sigma(x)} = f_{\pi(x)} \cdot f_{q(x)} + f_{r(x)}$.

Επίσης, επειδή η G είναι ομομορφισμός, έχουμε ότι

$$f_{\pi(x)} \cdot f_{q(x)} + f_{r(x)} = G(\pi(x)) \cdot G(q(x)) + G(r(x)) = G(\pi(x) \cdot q(x) + r(x)) = f_{\pi(x)\cdot q(x)+r(x)}$$

Άρα $f_{\sigma(x)} = f_{\pi(x)\cdot q(x)+r(x)}$. Όμως $\sigma(x) \neq \pi(x) \cdot q(x) + r(x)$ αφού $\sigma(x) = \bar{1}x^2 + \bar{1}x$ και $\pi(x) \cdot q(x) + r(x) = \bar{1}x \cdot \bar{1}x^4 + \bar{1}x^2 = \bar{1}x^5 + \bar{1}x^2$. □

Αν όμως η απεικόνιση G είναι 1-1 (και άρα η G είναι μονομορφισμός), τότε μπορούμε να "ταυτίσουμε" ένα πολυώνυμο $\pi(x)$ με την πολυωνυμική του συνάρτηση $f_{\pi(x)} = G(\pi(x))$ και επομένως, σε αυτήν την περίπτωση, μπορούμε να "ταυτίσουμε" τους δύο δακτυλίους $R[x]$

και $G(R[x])$ (δηλ. σε αυτήν την περίπτωση μπορούμε να "ταυτίσουμε" τον δακτύλιο πολυωνύμων επί του R με το δακτύλιο των πολυωνυμικών συναρτήσεων επί του R μέσω της "ταύτισης" ενός πολυωνύμου με την πολυωνυμική του συνάρτηση).

<u>**Πρόταση 2.4:**</u> Έστω $(R,+,\cdot)$ <u>πεπερασμένος</u> δακτύλιος με μονάδα. Τότε η απεικόνιση G δεν είναι 1-1 (και άρα, λόγω της Πρότασης 2.1, η G είναι μόνο ομομορφισμός και όχι μονομορφισμός).

<u>**Απόδειξη:**</u> Έστω $R=\{\alpha_1,\alpha_2,...,\alpha_n\}$ ($n\in\{2,3,4,...\}$). Θεωρούμε το πολυώνυμο

$$\pi(x)=(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$$

Θα δείξουμε ότι $G(\pi(x))=\mathbf{0}$. <u>Πράγματι:</u>

Επειδή προφανώς $f_{\pi(x)}(\alpha_i)=(\alpha_i-\alpha_1)...(\alpha_i-\alpha_i)...(\alpha_i-\alpha_n)=0$ για κάθε $i=1,...,n$, τότε έχουμε αμέσως ότι $f_{\pi(x)}(y)=0$ για κάθε $y\in R$. Άρα $f_{\pi(x)}=\mathbf{0}$ δηλαδή $G(\pi(x))=\mathbf{0}$. Όμως

$$\pi(x)=x^n-(\alpha_1+\alpha_2+...+\alpha_n)x^{n-1}+...+(-1)^n\alpha_1\cdot\alpha_2\cdot...\cdot\alpha_n$$

Άρα το πολυώνυμο $\pi(x)$ είναι μη μηδενικό αφού ο συντελεστής του x^n είναι διάφορος από το μηδέν (βλ. Παρατήρηση 1.3). Επομένως η G δεν είναι 1-1 (βλ. Παρατήρηση 1.8iii)). □

<u>**Παρατήρηση 2.5:**</u> Από την προηγούμενη Πρόταση έχουμε τα εξής:

i) Για τους δακτυλίους πολυωνύμων $\mathbb{Z}_m[x]$ με $m=2,3,4,...$ η απεικόνιση G δεν είναι 1-1 (άμεσο αφού $|\mathbb{Z}_m|=m$).

ii) Για κάθε πεπερασμένο μοναδιαίο δακτύλιο R, ο δακτύλιος πολυωνύμων $R[x]$ και ο δακτύλιος των πολυωνυμικών συναρτήσεων επί του R δεν ταυτίζονται (με την έννοια ότι η απεικόνιση G δεν είναι μονομορφισμός). □

<u>**Ορισμός 2.6:**</u> Έστω $(R,+,\cdot)$ μοναδιαίος δακτύλιος, $\pi(x)=\alpha_0+\alpha_1x+...+\alpha_nx^n\in R[x]$ και $c\in R$. Τότε με $\pi(c)$ συμβολίζουμε το στοιχείο $\alpha_0+\alpha_1c+...+\alpha_nc^n$ (δηλ. $\pi(c)=f_{\pi(x)}(c)$). □

<u>Θεώρημα 2.7:</u> Έστω $(R,+,\cdot)$ δακτύλιος με μονάδα. Τα εξής είναι ισοδύναμα:

i) Ο R έχει την ακόλουθη ιδιότητα:

$$\text{Αν } \pi(x) \in R[x] \text{ με } \pi(c)=0 \text{ για κάθε } c \in R, \text{ τότε } \pi(x)=\mathbf{0}$$

ii) Η απεικόνιση G είναι 1-1 (και άρα η G είναι μονομορφισμός - βλ. και Πρόταση 2.1).

<u>Απόδειξη:</u>

i)$\Rightarrow$ii) Υποθέτουμε ότι ο R έχει την ιδιότητα που διατυπώνεται στο i). Θα δείξουμε ότι η G είναι 1-1 εφαρμόζοντας την Παρατήρηση 1.8iii). Γι' αυτό έστω $\pi(x) \in R[x]$ με $G(\pi(x))=\mathbf{0}$. Πρέπει δείξουμε ότι $\pi(x)=\mathbf{0}$.

Αφού $G(\pi(x))=f_{\pi(x)}$, τότε έχουμε $f_{\pi(x)}=\mathbf{0}$. Άρα $f_{\pi(x)}(y)=0$ για κάθε $y \in R$. Δηλαδή $\pi(y)=0$ για κάθε $y \in R$. Τότε, από την ιδιότητα που υποθέσαμε ότι έχει ο R, έπεται αμέσως ότι $\pi(x)=\mathbf{0}$. Επομένως η G είναι 1-1.

ii)$\Rightarrow$i) Υποθέτουμε ότι η G είναι 1-1. Έστω τώρα $\pi(x) \in R[x]$ με $\pi(c)=0$ για κάθε $c \in R$. Θα δείξουμε ότι $\pi(x)=\mathbf{0}$. Αφού $\pi(c)=0$ για κάθε $c \in R$, τότε $f_{\pi(x)}(c)=0$ για κάθε $c \in R$. Επομένως $f_{\pi(x)}=\mathbf{0}$ και άρα $G(\pi(x))=\mathbf{0}$. Όμως η G είναι 1-1 και συνεπώς, από την Παρατήρηση 1.8iii), έπεται αμέσως ότι $\pi(x)=\mathbf{0}$. □

Η ιδιότητα του i) του προηγούμενου Θεωρήματος αποτελεί ικανή και αναγκαία συνθήκη για να είναι η απεικόνιση G 1-1 (και άρα μονομορφισμός).

<u>Παρατήρηση 2.8:</u> Επομένως, στην περίπτωση που ο δακτύλιος R έχει την ιδιότητα i) του Θεωρήματος 2.7, τότε:

i) έχουμε αμέσως ότι δύο πολυώνυμα είναι ίσα αν και μόνο αν οι πολυωνυμικές συναρτήσεις τους είναι ίσες.

ii) μπορούμε να ταυτίσουμε ένα πολυώνυμο $\pi(x) \in R[x]$ με την πολυωνυμική του συνάρτηση $f_{\pi(x)}$ $(=G(\pi(x)))$ και επομένως τον $R[x]$ με την εικόνα του $G(R[x])$. Αυτό σημαίνει ότι η αλγεβρική συμπεριφορά των $\pi(x)$ και $f_{\pi(x)}$ είναι ίδια (και άρα ο δακτύλιος πολυωνύμων επί του R είναι ισόμορφος με τον δακτύλιο των πολυωνυμικών συναρτήσεων επί του R - δηλ. $R[x] \underset{G}{\cong} G(R[x])$. □

<u>Ορισμός 2.9 [4]:</u> Έστω $(\mathrm{R},+,\cdot)$ αντιμεταθετικός δακτύλιος με μονάδα. Ο R καλείται σώμα αν κάθε μη μηδενικό στοιχείου του R έχει αντίστροφο ως προς τον πολλαπλασιασμό (δηλ. για κάθε $x \in \mathrm{R}$ με $x \neq 0$ υπάρχει $y \in \mathrm{R}$ τέτοιο ώστε $x \cdot y = 1$). □

<u>Θεώρημα 2.10 [2]:</u> Έστω $(\mathrm{R},+,\cdot)$ σώμα. Τα εξής είναι ισοδύναμα:

i) Η απεικόνιση G είναι 1-1 (και άρα η G είναι μονομορφισμός - βλ. και Πρόταση 2.1).

ii) Το R είναι άπειρο. □

<u>Παρατήρηση 2.11:</u> Αν ο δακτύλιος με μονάδα $(\mathrm{R},+,\cdot)$ δεν είναι σώμα, τότε δεν ισχύει υποχρεωτικά η συνεπαγωγή $\mathrm{ii}) \Rightarrow \mathrm{i})$ του προηγούμενου Θεωρήματος. Δηλαδή υπάρχει άπειρος δακτύλιος $(\mathrm{R},+,\cdot)$ για τον οποίο η απεικόνιση G δεν είναι 1-1 (και επομένως τότε, λόγω του Θεωρήματος 2.10, ο δακτύλιος $(\mathrm{R},+,\cdot)$ δεν μπορεί να είναι σώμα). □

Το επόμενο παράδειγμα αποδεικνύει τον ισχυρισμό της Παρατήρησης 2.11:

<u>Παράδειγμα 2.12:</u> Έστω Ε άπειρο σύνολο (π.χ. ως Ε μπορούμε να θεωρήσουμε το σύνολο των φυσικών αριθμών $\mathbb{N}$) και $P(\mathrm{E})$ το σύνολο των υποσυνόλων του. Προφανώς το σύνολο $P(\mathrm{E})$ είναι άπειρο. Επί του $P(\mathrm{E})$ ορίζουμε δύο πράξεις "+" και " $\cdot$ " ως εξής:

$$\mathrm{A}+\mathrm{B}=(\mathrm{A}-\mathrm{B}) \cup(\mathrm{B}-\mathrm{A})$$

$$\mathrm{A} \cdot \mathrm{B}=\mathrm{A} \cap \mathrm{B}$$

Τότε [3] η τριάδα $(P(\mathrm{E}),+,\cdot)$ είναι αντιμεταθετικός μοναδιαίος δακτύλιος (με μηδέν το κενό υποσύνολο $\varnothing$ και μονάδα το σύνολο Ε) για τον οποίο ισχύει $\mathrm{X} \cdot \mathrm{X}=\mathrm{X}$ για κάθε $\mathrm{X} \in P(\mathrm{E})$ (ένας δακτύλιος R με την ιδιότητα $\alpha^2=\alpha$ για κάθε $\alpha \in \mathrm{R}$ καλείται **δακτύλιος του Boole**) <u>κι άρα ο δακτύλιος</u> $(P(\mathrm{E}),+,\cdot)$ <u>δεν είναι σώμα</u>. Μάλιστα για κάθε $\mathrm{X} \in P(\mathrm{E})$ ισχύει:

$$\mathrm{E} \cdot \mathrm{X}^2+\mathrm{E} \cdot \mathrm{X}=\mathrm{X}^2+\mathrm{X}=\mathrm{X}+\mathrm{X}=\varnothing$$

Αυτό σημαίνει ότι αν θεωρήσουμε το πολυώνυμο $\pi(x)=\mathrm{E} \cdot x^2+\mathrm{E} \cdot x$, τότε έχουμε αμέσως ότι

- $\pi(x) \neq \mathbf{0}$, και
- για την πολυωνυμική συνάρτηση $f_{\pi(x)} \left(= G(\pi(x))\right)$ ισχύει $f_{\pi(x)}(y) = \varnothing$ για κάθε $y \in P(E)$.

Επομένως, από την Παρατήρηση 1.8iii), έπεται τότε αμέσως ότι η G δεν είναι 1-1. □

3. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από το Θεώρημα 2.7 και το Θεώρημα 2.9 έχουμε αμέσως το εξής:

Θεώρημα 3.1: Έστω $(R,+,\cdot)$ σώμα. Τα εξής είναι ισοδύναμα:

i) Το σώμα R έχει την ακόλουθη ιδιότητα:

$$\text{Αν } \pi(x) \in R[x] \text{ με } \pi(c) = 0 \text{ για κάθε } c \in R\text{, τότε } \pi(x) = \mathbf{0}$$

ii) Η απεικόνιση G είναι 1-1 (και άρα η G είναι μονομορφισμός - βλ. και Πρόταση 2.1).

iii) Το σώμα R είναι άπειρο. □

Αν τώρα ως R θεωρήσουμε το (σώμα των πραγματικών αριθμών) $\mathbb{R}$ ή το (σώμα των μιγαδικών αριθμών) $\mathbb{C}$, τότε ο R έχει προφανώς την ιδιότητα iii) του Θεωρήματος 3.1. Επομένως έχουμε αμέσως το εξής:

Πόρισμα 3.2: Για τους δακτυλίους πολυωνύμων $\mathbb{R}[x]$ και $\mathbb{C}[x]$ η απεικόνιση G είναι 1-1 (και άρα η G είναι μονομορφισμός - βλ. και Πρόταση 2.1). □

Παρατήρηση 3.3: Συνεπώς (βλ. Παρατήρηση 2.8 και Πόρισμα 3.2) για τους δακτυλίους πολυωνύμων $\mathbb{R}[x]$ και $\mathbb{C}[x]$ ισχύουν τα εξής:

i) Η ισότητα δύο πολυωνυμικών συναρτήσεων συνεπάγεται την ισότητα των πολυωνύμων από τα οποία προκύπτουν (και αντίστροφα).

ii) Ένα πολυώνυμο του $\mathbb{R}[x]$ (ή του $\mathbb{C}[x]$) μπορούμε να το ταυτίσουμε με την πολυωνυμική του συνάρτηση (όπως συνήθως κάνουμε στην πράξη).

iii) Οι δακτύλιοι πολυωνύμων $\mathbb{R}[x]$, $\mathbb{C}[x]$ είναι ισόμορφοι (μέσω της απεικόνισης G) με τους δακτυλίους των πολυωνυμικών συναρτήσεων επί των $\mathbb{R}$, $\mathbb{C}$ αντίστοιχα (και συνεπώς μπορούμε να ταυτίσουμε αλγεβρικά, μέσω της απεικόνισης G, τους δακτυλίους

$\mathbb{R}[x]$, $\mathbb{C}[x]$ με τους δακτυλίους των πολυωνυμικών συναρτήσεων επί των $\mathbb{R}$, $\mathbb{C}$ αντίστοιχα). □

Απόδειξη Θεωρήματος 2.10

Έστω ένα μη μηδενικό πολυώνυμο $\pi(x)$. Τότε αυτό γράφεται προφανώς στη μορφή

$$\pi(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \equiv (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$$

με $a_n \neq 0$. Ορίζουμε *βαθμό* του $\pi(x)$ (συμβολισμός $\deg \pi(x)$) τον μη αρνητικό ακέραιο *n*, δηλ. $\deg \pi(x) = n$. Για το μηδενικό πολυώνυμο δεν ορίζουμε βαθμό. Ένας δακτύλιος $(R, +, \cdot)$ καλείται *ακέραια περιοχή* για $a, b \in R$ ισχύει

$$a \cdot b = 0 \Rightarrow a = 0 \text{ ή } b = 0$$

(δηλ. ο *R* δεν έχει διαιρέτες του μηδενός). Για $\pi(x), q(x) \in R[x]$ με *R* ακέραια περιοχή και $\pi(x) \neq \mathbf{0} \neq q(x)$ ισχύουν προφανώς τα εξής:

- Αν $\pi(x) + q(x) \neq \mathbf{0}$, τότε
$$\deg(\pi(x) + q(x)) \leq \max(\deg \pi(x), \deg q(x))$$
- $\deg(\pi(x) \cdot q(x)) = \deg \pi(x) + \deg q(x)$

<u>Λήμμα 1:</u> Έστω $(R, +, \cdot)$ σώμα και $p(x), q(x) \in R[x]$ με $p(x) \neq \mathbf{0} \neq q(x)$ και $\deg q(x) \leq \deg p(x)$. Τότε υπάρχει $\sigma(x) \in R[x]$ τέτοιο ώστε $p(x) - \sigma(x)q(x) = \mathbf{0}$ ή $p(x) - \sigma(x)q(x) \neq \mathbf{0}$ με $\deg(p(x) - \sigma(x)q(x)) < \deg p(x)$.

<u>Απόδειξη:</u> Έστω $p(x) = a_0 + a_1x + \ldots + a_nx^n$ και $q(x) = b_0 + b_1x + \ldots + b_mx^m$ με $a_n \neq 0 \neq b_m$. Τότε $\deg q(x) = m$ και $\deg p(x) = n$. Άρα $m \leq n$. Αφού το *R* είναι σώμα και $b_m \in R - \{0\}$, τότε υπάρχει το b_m^{-1}. Θέτουμε

$$\sigma(x) := a_nb_m^{-1}x^{n-m}$$

και έχουμε

- $\sigma(x)q(x) = a_nb_m^{-1}x^{n-m}\left(b_0 + b_1x + \ldots + b_{m-1}x^{m-1} + b_mx^m\right) = \ldots =$

$$= a_n b_m^{-1} b_0 x^{n-m} + a_n b_m^{-1} b_1 x^{n-m+1} + \ldots + a_n b_m^{-1} b_{m-1} x^{n-1} + a_n x^n$$

- $p(x) - \sigma(x) q(x) =$

$$= a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + \cancel{a_n x^n} - a_n b_m^{-1} b_0 x^{n-m} - a_n b_m^{-1} b_1 x^{n-m+1} - \ldots - a_n b_m^{-1} b_{m-1} x^{n-1} - \cancel{a_n x^n}$$

Επομένως $p(x) - \sigma(x) q(x) = \mathbf{0}$ ή

$$p(x) - \sigma(x) q(x) \neq \mathbf{0} \text{ με } \deg\big(p(x) - \sigma(x) q(x)\big) < n = \deg p(x) \qquad \square$$

<u>Θεώρημα 2:</u> Έστω $(R, +, \cdot)$ σώμα και $p(x), q(x) \in R[x]$ με $q(x) \neq \mathbf{0}$. Τότε υπάρχουν μοναδικά πολυώνυμα $\pi(x), \upsilon(x) \in R[x]$ τέτοια ώστε

$$p(x) = \pi(x) q(x) + \upsilon(x), \; \upsilon(x) = \mathbf{0} \text{ ή } \upsilon(x) \neq \mathbf{0} \text{ με } \deg \upsilon(x) < \deg q(x)$$

<u>Απόδειξη:</u> Θα δείξουμε πρώτα την ύπαρξη τέτοιων πολυωνύμων $\pi(x), \upsilon(x)$.

I) Αν $\underline{p(x) = \mathbf{0}}$. Τότε αν θεωρήσουμε $\pi(x) = \upsilon(x) = \mathbf{0}$, έχουμε αμέσως

$$p(x) = \pi(x) q(x) + \upsilon(x) \text{ με } \upsilon(x) = \mathbf{0}$$

II) Αν $\underline{p(x) \neq \mathbf{0}}$. Διακρίνουμε δύο περιπτώσεις:

IIA) $\underline{\deg p(x) < \deg q(x)}$

Τότε αν θεωρήσουμε $\pi(x) = \mathbf{0}$ και $\upsilon(x) = p(x)$ έχουμε αμέσως

$$p(x) = \pi(x) q(x) + \upsilon(x) \text{ με } \deg \upsilon(x) < \deg q(x)$$

IIB) $\underline{\deg p(x) \geq \deg q(x)}$

Τότε εφαρμόζοντας το Λήμμα 1 έχουμε αμέσως ότι υπάρχει $\sigma_1(x) \in R[x]$ τέτοιο ώστε $p(x) - \sigma_1(x) q(x) = \mathbf{0}$ ή $p(x) - \sigma_1(x) q(x) \neq \mathbf{0}$ με $\deg\big(p(x) - \sigma_1(x) q(x)\big) < \deg p(x)$.

- Αν $\underline{p(x) - \sigma_1(x) q(x) = \mathbf{0}}$, τότε αν θεωρήσουμε $\pi(x) = \sigma_1(x)$ και $\upsilon(x) = p(x) - \sigma_1(x) q(x)$, έχουμε αμέσως

$$p(x) = \pi(x) q(x) + \upsilon(x) \text{ με } \upsilon(x) = \mathbf{0}$$

- Αν $\underline{p(x) - \sigma_1(x) q(x) \neq \mathbf{0}}$ με $\underline{\deg\big(p(x) - \sigma_1(x) q(x)\big) < \deg p(x)}$
  - Αν $\underline{\deg\big(p(x) - \sigma_1(x) q(x)\big) < \deg q(x)}$

Τότε αν θεωρήσουμε $\pi(x)=\sigma_1(x)$ και $\upsilon(x)=p(x)-\sigma_1(x)q(x)$ έχουμε αμέσως

$$p(x)=\pi(x)q(x)+\upsilon(x) \text{ με } \deg\upsilon(x)<\deg q(x)$$

- Αν $\underline{\deg\left(p(x)-\sigma_1(x)q(x)\right)\geq\deg q(x)}$

  Τότε αν εφαρμόσουμε το Λήμμα 1 για τα πολυώνυμα $p(x)-\sigma_1(x)q(x)$ και $q(x)$, έχουμε αμέσως ότι υπάρχει $\sigma_2(x)\in R[x]$ τέτοιο ώστε

$$p(x)-\sigma_1(x)q(x)-\sigma_2(x)q(x)=\mathbf{0}\Leftrightarrow p(x)-\left(\sigma_1(x)+\sigma_2(x)\right)q(x)=\mathbf{0}$$

ή

$p(x)-\left(\sigma_1(x)+\sigma_2(x)\right)q(x)\neq\mathbf{0}$ με

$$\deg\left(p(x)-\left(\sigma_1(x)+\sigma_2(x)\right)q(x)\right)<\deg\left(p(x)-\sigma_1(x)q(x)\right)$$

Με διαδοχικές εφαρμογές της παραπάνω διαδικασίας (επειδή τα "παραγόμενα" πολυώνυμα μέσω του Λήμματος 1 είτε είναι τα μηδενικά είτε έχουν βαθμό γνήσια μικρότερο του αντίστοιχου πολυωνύμου του προηγούμενου βήματος – σε αυτήν μάλιστα την περίπτωση, αν ο βαθμός του "παραγόμενου" πολυωνύμου είναι μεγαλύτερος ή ίσος του $\deg q(x)$, τότε συνεχίζουμε όμοια τη διαδικασία με επόμενο βήμα) καταλήγουμε στην ύπαρξη $\sigma_1(x),\sigma_2(x),...,\sigma_\kappa(x)\in R[x]$ τέτοιων ώστε

$p(x)-\left(\sigma_1(x)+\sigma_2(x)+...+\sigma_\kappa(x)\right)q(x)=\mathbf{0}$ ή

$p(x)-\left(\sigma_1(x)+\sigma_2(x)+...+\sigma_\kappa(x)\right)q(x)\neq\mathbf{0}$ με

$$\deg\left(p(x)-\left(\sigma_1(x)+\sigma_2(x)+...+\sigma_\kappa(x)\right)q(x)\right)<\deg\left(p(x)-\left(\sigma_1(x)+\sigma_2(x)+...+\sigma_{\kappa-1}(x)\right)q(x)\right)$$

και $\deg\left(p(x)-\left(\sigma_1(x)+\sigma_2(x)+...+\sigma_\kappa(x)\right)q(x)\right)<\deg q(x)$.

Οπότε θέτοντας $\pi(x)=\sigma_1(x)+\sigma_2(x)+...+\sigma_\kappa(x)$ και

$\upsilon(x)=p(x)-\left(\sigma_1(x)+\sigma_2(x)+...+\sigma_\kappa(x)\right)q(x)$ έχουμε αμέσως ότι

$$p(x)=\pi(x)q(x)+\upsilon(x),\ \upsilon(x)=\mathbf{0} \text{ ή } \upsilon(x)\neq\mathbf{0} \text{ με } \deg\upsilon(x)<\deg q(x)$$

Συνεπώς από I) και II) έχουμε ότι υπάρχουν πολυώνυμα $\pi(x),\upsilon(x)\in R[x]$ τέτοια ώστε

$$p(x)=\pi(x)q(x)+\upsilon(x),\ \upsilon(x)=\mathbf{0} \text{ ή } \upsilon(x)\neq\mathbf{0} \text{ με } \deg\upsilon(x)<\deg q(x)$$

Στη συνέχεια θα δείξουμε τη μοναδικότητα των πολυωνύμων $\pi(x),\upsilon(x)$ με τις απαιτούμενες από την εκφώνηση ιδιότητες. Έστω $\pi_1(x),\pi_2(x),\upsilon_1(x),\upsilon_1(x)\in R[x]$ τέτοια ώστε

$$p(x)=\pi_1(x)q(x)+\upsilon_1(x),\ \upsilon_1(x)=\mathbf{0} \text{ ή } \upsilon_1(x)\neq\mathbf{0} \text{ με } \deg\upsilon_1(x)<\deg q(x)$$

και

$$p(x)=\pi_2(x)q(x)+\upsilon_2(x),\ \upsilon_2(x)=\mathbf{0} \text{ ή } \upsilon_2(x)\neq\mathbf{0} \text{ με } \deg\upsilon_2(x)<\deg q(x)$$

Τότε έχουμε

$$\begin{aligned}&\pi_1(x)q(x)+\upsilon_1(x)=\pi_2(x)q(x)+\upsilon_2(x)\Leftrightarrow\\&\Leftrightarrow(\pi_1(x)-\pi_2(x))q(x)=\upsilon_2(x)-\upsilon_1(x)\end{aligned}\qquad(1)$$

Ας υποθέσουμε ότι $\pi_1(x)\neq\pi_2(x)$ ($\Leftrightarrow\pi_1(x)-\pi_2(x)\neq\mathbf{0}$ - άρα ορίζεται $\deg(\pi_1(x)-\pi_2(x))$). Τότε επειδή $q(x)\neq\mathbf{0}$ και το R είναι σώμα (άρα και ακέραια περιοχή), από την (1) έπεται αμέσως ότι

$$\upsilon_2(x)-\upsilon_1(x)\neq\mathbf{0}\Leftrightarrow\upsilon_1(x)\neq\upsilon_2(x)\qquad(2)$$

(δηλ. ορίζεται $\deg(\upsilon_2(x)-\upsilon_1(x))$) κι επομένως η (1) δίνει

$$\begin{aligned}\deg(\upsilon_2(x)-\upsilon_1(x))&=\deg((\pi_1(x)-\pi_2(x))q(x))=\\&=\deg(\pi_1(x)-\pi_2(x))+\deg q(x)\geq\deg q(x)\end{aligned}\qquad(3)$$

i) $\underline{\upsilon_1(x)=\mathbf{0}}$

Τότε από την (2) έπεται $\upsilon_2(x)\neq\mathbf{0}$ και άρα $\deg\upsilon_2(x)<\deg q(x)$ οπότε $\deg(\upsilon_2(x)-\upsilon_1(x))=\deg\upsilon_2(x)<\deg q(x)$. Άτοπο λόγω της (3).

ii) $\underline{\upsilon_1(x)\neq\mathbf{0}}$

Τότε $\deg\upsilon_1(x)<\deg q(x)$.

iiα) Αν $\underline{\upsilon_2(x)=\mathbf{0}}$, τότε έχουμε

$$\deg(\upsilon_2(x)-\upsilon_1(x))=\deg(-\upsilon_1(x))=\deg(\upsilon_1(x))<\deg q(x)$$

Άτοπο λόγω της (3).

iiβ) Αν $\underline{\upsilon_2(x)\neq\mathbf{0}}$, τότε $\deg\upsilon_2(x)<\deg q(x)$. Όμως

$$\deg\left(\upsilon_2(x)-\upsilon_1(x)\right)\le \max\left(\deg\upsilon_2(x),\deg\left(-\upsilon_1(x)\right)\right)=\max\left(\deg\upsilon_2(x),\deg\upsilon_1(x)\right)<$$
$$\underset{\left(\substack{\deg\upsilon_2(x)<\deg q(x)\\ \deg\upsilon_1(x)<\deg q(x)}\right)}{<}\deg q(x)$$

και άρα $\deg\left(\upsilon_2(x)-\upsilon_1(x)\right)<\deg q(x)$. Άτοπο λόγω της (3).

Από i) και ii) έπεται αμέσως ότι δεν μπορεί $\pi_1(x)\neq\pi_2(x)$ κι επομένως $\pi_1(x)=\pi_2(x)$. Τότε από την (1) έχουμε αμέσως ότι $\upsilon_1(x)=\upsilon_2(x)$. □

Το $a\in R$ καλείται *ρίζα* του $p(x)\in R[x]$ (R δακτύλιος με μονάδα) αν $p(a)=0$.

<u>Πρόταση 3:</u> Έστω $(R,+,\cdot)$ σώμα, $p(x)\in R[x]$ και $a\in R$. Τότε $p(a)=0$ (δηλ. το a είναι ρίζα του $p(x)$) αν και μόνο αν υπάρχει $\pi(x)\in R[x]$ τέτοιο ώστε $p(x)=\pi(x)(x-a)$ (δηλ. το $x-a$ *διαιρεί* το $p(x)$).

<u>Απόδειξη:</u> Εφαρμόζοντας το Θεώρημα 2 για τα πολυώνυμα $p(x)$ και $x-a$ ($\neq\mathbf{0}$), έχουμε αμέσως (αφού $\deg(x-a)=1$) ότι υπάρχουν $\pi(x)\in R[x]$ και $b\in R$ τέτοια ώστε

$$p(x)=\pi(x)(x-a)+b$$

Άρα $p(a)=b$. Επομένως έχουμε

$$p(a)=0\Leftrightarrow b=0\Leftrightarrow p(x)=\pi(x)(x-a)$$ □

<u>Θεώρημα 4:</u> Έστω $(R,+,\cdot)$ σώμα και $p(x)\in R[x]$ με $p(x)\neq\mathbf{0}$ και $\deg p(x)=n$. Τότε το $p(x)$ έχει το πολύ *n* ρίζες.

<u>Απόδειξη:</u> Αν το $p(x)$ δεν έχει καμία ρίζα τότε προφανώς (αφού $n=\deg p(x)\ge 0$) το Θεώρημα ισχύει. Έστω τώρα ότι το $p(x)$ έχει (τουλάχιστον μία) ρίζα και έστω $a_1,a_2,\ldots,a_\kappa\in R$ ($\kappa\in\mathbb{N}$ με $\kappa\ge 1$) οι διακεκριμένες ρίζες του $p(x)$. Θα δείξουμε $\kappa\le n$.

Σύμφωνα με την Πρόταση 3 έχουμε αμέσως ότι υπάρχει $\pi_1(x)\in R[x]$ τέτοιο ώστε $p(x)=\pi_1(x)(x-a_1)$. Επειδή το a_2 είναι ρίζα του $p(x)$, τότε

$$p(a_2)=0 \Leftrightarrow \pi_1(a_2)(a_2-a_1)=0 \underset{\left(\substack{a_2\neq a_1 \Leftrightarrow \\ \Leftrightarrow a_2-a_1\neq 0}\right)}{\Leftrightarrow} \pi_1(a_2)=0$$

Άρα το a_2 είναι ρίζα του $\pi_1(x)$ κι επομένως από την Πρόταση 3 έπεται υπάρχει $\pi_2(x)\in R[x]$ τέτοιο ώστε $\pi_1(x)=\pi_2(x)(x-a_2)$. Συνεπώς

$$p(x)=\pi_1(x)(x-a_1)=\pi_2(x)(x-a_2)(x-a_1)$$

Συνεχίζοντας με όμοιο τρόπο (μετά από κ βήματα από την αρχή) καταλήγουμε στο συμπέρασμα ότι υπάρχει $\pi_\kappa(x)\in R[x]$ τέτοιο ώστε

$$p(x)=\pi_\kappa(x)(x-a_\kappa)...(x-a_1) \qquad (1)$$

Αφού $p(x)\neq \mathbf{0}$, τότε προφανώς και $\pi_\kappa(x)\neq \mathbf{0}$. Άρα ορίζεται το $\deg \pi_\kappa(x)$ κι επομένως από την (1) έχουμε

$$\begin{aligned}\deg p(x) &= \deg\big(\pi_\kappa(x)(x-a_\kappa)...(x-a_1)\big)=\deg \pi_\kappa(x)+\deg(x-a_\kappa)+...+\deg(x-a_1)=\\ &=\deg \pi_\kappa(x)+\underbrace{1+...+1}_{\kappa\ \text{φορές}}=\deg \pi_\kappa(x)+\kappa\geq \kappa\end{aligned}$$

Άρα $n\geq \kappa$. □

<u>Πόρισμα 5:</u> Έστω $(R,+,\cdot)$ σώμα και $p(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0\in R[x]$. Αν το $p(x)$ έχει $n+1$ διακεκριμένες ρίζες, τότε $p(x)=\mathbf{0}$.

<u>Απόδειξη:</u> Έστω $p(x)\neq \mathbf{0}$ (άρα ορίζεται το $\deg p(x)$ και μάλιστα $\deg p(x)\leq n$). Από το Θεώρημα 4 έχουμε τότε ότι το $p(x)$ έχει το πολύ $\deg p(x)$ ρίζες. Αυτό όμως είναι άτοπο επειδή $\deg p(x)\leq n<n+1$ και το $p(x)$ έχει (από υπόθεση) $n+1$ διακεκριμένες ρίζες. Άρα $p(x)=\mathbf{0}$. □

<u>Πόρισμα 6:</u> Έστω $(R,+,\cdot)$ άπειρο σώμα και $p(x)\in R[x]$ τέτοιο ώστε $p(c)=0$ για κάθε $c\in R$. Τότε $p(x)=\mathbf{0}$.

<u>Απόδειξη:</u> Έστω $p(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$, $a_i\in R$ για $i=0,1,...,n$. Αφού το σώμα R είναι άπειρο και $p(c)=0$ για κάθε $c\in R$, τότε το $p(x)$ έχει σίγουρα $n+1$ διακεκριμένες ρίζες. Τότε από το Πόρισμα 5 έπεται αμέσως ότι $p(x)=\mathbf{0}$. □

<u>Θεώρημα 7 (2.10):</u> Έστω $(R,+,\cdot)$ σώμα. Τα εξής είναι ισοδύναμα:

i) Η απεικόνιση G είναι 1-1.

ii) Το R είναι άπειρο.

<u>Απόδειξη:</u>

i)$\Rightarrow$ii) Άμεσο από την Πρόταση 2.4.

ii)$\Rightarrow$i) Έστω ότι το R είναι άπειρο κι έστω $p(x)\in R[x]$ τέτοιο ώστε $p(c)=0$ για κάθε $c\in R$. Τότε από το Πόρισμα 6 έπεται αμέσως ότι $p(x)=\mathbf{0}$. Αυτό σημαίνει ότι το R έχει την ιδιότητα i) του Θεωρήματος 2.7 κι επομένως από το Θεώρημα 2.7 i)$\Rightarrow$ii) έχουμε αμέσως ότι η G είναι 1-1. □

<u>2η απόδειξη του Πορίσματος 5</u>

Έστω $(R,+,\cdot)$ σώμα και $p(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0\in R[x]$. Έστω ακόμη ότι το $p(x)$ έχει $n+1$ διακεκριμένες ρίζες. Αυτό σημαίνει ότι υπάρχουν $\rho_{1,},...,\rho_{n+1}\in R$ τέτοια ώστε:

- $\rho_i\neq\rho_j$ $(\Leftrightarrow\rho_j-\rho_i\neq 0)$, $1\leq i<j\leq n+1$, και
- $p(\rho_\lambda)=0$ (δηλ. $a_n\rho_\lambda{}^n+a_{n-1}\rho_\lambda{}^{n-1}+...+a_1\rho_\lambda+a_0=0$) για κάθε $\lambda=1,2,..,n,n+1$.

<u>Θα δείξουμε ότι</u> $a_n=...=a_1=a_0=0$.

Αφού $a_n\rho_\lambda{}^n+a_{n-1}\rho_\lambda{}^{n-1}+...+a_1\rho_\lambda+a_0=0$ για κάθε $\lambda=1,2,..,n,n+1$, τότε

$$\left\{\begin{array}{l} a_n\rho_1{}^n+a_{n-1}\rho_1{}^{n-1}+...+a_1\rho_1+a_0=0\\ a_n\rho_2{}^n+a_{n-1}\rho_2{}^{n-1}+...+a_1\rho_2+a_0=0\\ \qquad\qquad ...\\ a_n\rho_n{}^n+a_{n-1}\rho_n{}^{n-1}+...+a_1\rho_n+a_0=0\\ a_n\rho_{n+1}{}^n+a_{n-1}\rho_{n+1}{}^{n-1}+...+a_1\rho_{n+1}+a_0=0 \end{array}\right\} \qquad (1)$$

Οι σχέσεις (1) αποτελούν τετραγωνικό ομογενές σύστημα με άγνωστους τους a_n, a_{n-1}, …, a_1, a_0 και πίνακα συντελεστών τον $(n+1)\times(n+1)$ πίνακα

$$
\boldsymbol{A}=\begin{bmatrix} \rho_1{}^n & \rho_1{}^{n-1} & \dots & \rho_1 & 1 \\ \rho_2{}^n & \rho_2{}^{n-1} & \dots & \rho_2 & 1 \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ \rho_n{}^n & \rho_n{}^{n-1} & \dots & \rho_n & 1 \\ \rho_{n+1}{}^n & \rho_{n+1}{}^{n-1} & \dots & \rho_{n+1} & 1 \end{bmatrix}
$$

Για την ορίζουσα του παραπάνω πίνακα έχουμε

$$
\left|\boldsymbol{A}\right|=\left|\boldsymbol{A}^{\mathrm{T}}\right|=\begin{vmatrix} \rho_1{}^n & \rho_2{}^n & \dots & \rho_n{}^n & \rho_{n+1}{}^n \\ \rho_1{}^{n-1} & \rho_2{}^{n-1} & \dots & \rho_n{}^{n-1} & \rho_{n+1}{}^{n-1} \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ \rho_1 & \rho_2 & \dots & \rho_n & \rho_{n+1} \\ 1 & 1 & \dots & 1 & 1 \end{vmatrix}=\left(-1\right)^{\frac{n(n+1)}{2}}\begin{vmatrix} 1 & 1 & \dots & 1 & 1 \\ \rho_1 & \rho_2 & \dots & \rho_n & \rho_{n+1} \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ \rho_1{}^{n-1} & \rho_2{}^{n-1} & \dots & \rho_n{}^{n-1} & \rho_{n+1}{}^{n-1} \\ \rho_1{}^n & \rho_2{}^n & \dots & \rho_n{}^n & \rho_{n+1}{}^n \end{vmatrix} \underset{\left(\substack{\text{ορίζουσα} \\ \text{Vandermonde}}\right)}{=}
$$

$$
=\left(-1\right)^{\frac{n(n+1)}{2}}\prod_{1\le i<j\le n+1}\left(\rho_j-\rho_i\right)\neq 0
$$

Άρα το τετραγωνικό ομογενές σύστημα (1) έχει μοναδική λύση τη μηδενική, δηλ. την $a_n=\dots=a_1=a_0=0$ κι επομένως $p\left(x\right)=\mathbf{0}$. □

ΑΝΑΦΟΡΕΣ

[**1**] Ανδρεαδάκης, Στυλιανός Α., (1986). Εισαγωγή στην Άλγεβρα, Αθήνα, Κεφ. 3 §3.

[**2**] Μπεληγιάννης, Απόστολος, (2015). Μία Εισαγωγή στη Βασική Άλγεβρα (ISBN 978-960-603-262-2), Ιωάννινα: Εκδόσεις Κάλλιπος, Κεφ. 9 §9.3.

[**3**] Στρατηγόπουλος, Δημήτριος, (1997). Σύγχρονη Άλγεβρα Ι (ISBN 960-266-051-1), Εκδόσεις Συμμετρία, Κεφ. 0 §1, 12, Κεφ. 2 §2, Κεφ. 7 §1.

[**4**] Fraleigh, John B., (2006). Εισαγωγή στην Άλγεβρα (ISBN 960-7309-71-5, μετάφραση από το πρωτότυπο: A first course in Abstract Algebra), Πανεπιστημιακές Εκδόσεις Κρήτης, 5η Έκδοση, σελ. 275, Κεφ. 5 §5.1.