5.10 ΠΟΛΥΩΝΥΜΙΚΟΙ ΔΑΚΤΥΛΙΟΙ ΠΟΥ ΕΙΝΑΙ Π.Μ.Π.

Σε αυτήν την ενότητα θα αποδείξουμε ότι (για μια ακεραία περιοχή R) ο πολυωνυμικός δακτύλιος $R[\mathsf{X}]$ είναι Π.Μ.Π. εάν και μόνον εάν η ίδια η R είναι Π.Μ.Π. (βλ. θεώρημα 5.10.17).

5.10.1 Ορισμός. Έστω R μια Π.Μ.Π. Κάθε πολυώνυμο

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\},\ n \in \mathbb{N}_0,$$

με τους συντελεστές του $a_0, a_1, \ldots, a_n$ σχετικώς πρώτους εντός τής R (βλ. 5.2.16) καλείται **πρωταρχικό πολυώνυμο (υπεράνω τής** R).

5.10.2 Λήμμα. *Έστω R μια ακεραία περιοχή και έστω $p \in R \smallsetminus \{R^\times \cup \{0_R\}\}$ ένα πρώτο στοιχείο τής R. Η απεικόνιση*

$$\boxed{\mathfrak{H}_p : R[\mathsf{X}] \longrightarrow (R/\langle p \rangle)[\mathsf{X}],} \tag{5.173}$$

η οριζόμενη μέσω τού τύπου

$$\sum_{j=0}^{n} a_j \mathsf{X}^j = \varphi(\mathsf{X}) \longmapsto \mathfrak{H}_p(\varphi(\mathsf{X})) := \sum_{j=0}^{n} (a_j + \langle p \rangle) \mathsf{X}^j,$$

είναι επιμορφισμός από την ακεραία περιοχή $R[\mathsf{X}]$ επί τής ακεραίας περιοχής $(R/\langle p \rangle)[\mathsf{X}]$.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τον ορισμό των πράξεων προσθέσεως και πολλαπλασιασμού επί τού $R/\langle p \rangle$ τον θεσπισθέντα μέσω τής προτάσεως 2.6.1. (Σημειωτέον ότι η $\mathfrak{H}_p$ είναι ο επιμορφισμός $\theta^{(1)}_{\pi^R_{\langle p \rangle}}$ ο ορισθείς στην άσκηση **3-38**, όπου $\pi^R_{\langle p \rangle} : R \longrightarrow R/\langle p \rangle$ ο φυσικός επιμορφισμός.) Ο πηλικοδακτύλιος $R/\langle p \rangle$ (και, κατ' επέκταση, και ο πολυωνυμικός δακτύλιος $(R/\langle p \rangle)[\mathsf{X}]$) είναι ακεραία περιοχή, διότι το $\langle p \rangle$ είναι πρώτο ιδεώδες. (Βλ. 5.3.4 (i), 2.6.4 (i)⇒(ii) και 1.3.9 (ii).) □

5.10.3 Πρόταση. (Λήμμα τού Gauss.) *Έστω R μια Π.Μ.Π. Το γινόμενο $\varphi(\mathsf{X})\psi(\mathsf{X})$ δυο πολυωνύμων $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$ είναι πρωταρχικό πολυώνυμο εάν και μόνον καθένα εξ αυτών είναι πρωταρχικό πολυώνυμο.*

ΑΠΟΔΕΙΞΗ. Εάν το $\varphi(\mathsf{X})\psi(\mathsf{X})$ είναι πρωταρχικό πολυώνυμο, τότε *κάθε* κοινός διαιρέτης των συντελεστών τού $\varphi(\mathsf{X})$ διαιρεί καθέναν εκ των συντελεστών τού $\varphi(\mathsf{X})\psi(\mathsf{X})$, οπότε είναι ένα αντιστρέψιμο στοιχείο τής R. Άρα το $\varphi(\mathsf{X})$ είναι ένα πρωταρχικό πολυώνυμο. Μέσω τής ίδιας επιχειρηματολογίας δείχνουμε ότι το $\psi(\mathsf{X})$ είναι ωσαύτως πρωταρχικό.

Αντιστρόφως τώρα· έστω ότι τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι πρωταρχικά πολυώνυμα. Ας υποθέσουμε ότι το γινόμενό τους $\varphi(\mathsf{X})\psi(\mathsf{X})$ *δεν* είναι πρωταρχικό πολυώνυμο. Θεωρούμε έναν μέγιστο κοινό διαιρέτη d των συντελεστών τού $\varphi(\mathsf{X})\psi(\mathsf{X})$ και ένα πρώτο (= ανάγωγο) στοιχείο $p \in R \diagdown \{R^\times \cup \{0_R\}\}$ τής R που διαιρεί τον d. (Προφανώς, $d \notin R^\times \cup \{0_R\}$.) Η εικόνα τού $\varphi(\mathsf{X})\psi(\mathsf{X})$ μέσω τού ομομορφισμού (5.173) είναι η εξής:

$$\mathfrak{H}_p(\varphi(\mathsf{X}))\mathfrak{H}_p(\psi(\mathsf{X})) = \mathfrak{H}_p(\varphi(\mathsf{X})\psi(\mathsf{X})) = 0_{(R/\langle p\rangle)[\mathsf{X}]} = \langle p\rangle\,[\mathsf{X}],$$

καθότι το p διαιρεί όλους τους συντελεστές τού $\varphi(\mathsf{X})\psi(\mathsf{X})$, οπότε καθένας εξ αυτών ανήκει στο κύριο ιδεώδες $\langle p\rangle$. Επειδή ο πηλικοδακτύλιος $R/\langle p\rangle$ είναι ακεραία περιοχή, έχουμε *είτε* $\mathfrak{H}_p(\varphi(\mathsf{X})) = 0_{(R/\langle p\rangle)[\mathsf{X}]}$ είτε $\mathfrak{H}_p(\psi(\mathsf{X})) = 0_{(R/\langle p\rangle)[\mathsf{X}]}$, δηλαδή *είτε* το p είναι κοινός διαιρέτης όλων των συντελεστών τού $\varphi(\mathsf{X})$ *είτε* το p είναι κοινός διαιρέτης όλων των συντελεστών τού $\psi(\mathsf{X})$. Στην πρώτη περίπτωση το p οφείλει να διαιρεί *κάθε* μέγιστο κοινό διαιρέτη των συντελεστών τού $\varphi(\mathsf{X})$, οπότε $p \mid 1_R$ (διότι το $\varphi(\mathsf{X})$ είναι εξ υποθέσεως πρωταρχικό), πράγμα *αδύνατο* (καθόσον $p \notin R^\times$). Κατ' αναλογίαν, δείχνουμε ότι *και* στη δεύτερη περίπτωση καταλήγουμε σε άτοπο (διότι *και* το $\psi(\mathsf{X})$ είναι εξ υποθέσεως πρωταρχικό). □

5.10.4 Λήμμα. *Έστω R μια Π.Μ.Π. Για οιοδήποτε $\varphi(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$ ισχύουν τα ακόλουθα:*

(i) *Υπάρχει κάποιο στοιχείο $c \in \mathbf{Fr}(R)$, καθώς και κάποιο $\widetilde{\varphi}(\mathsf{X}) \in R[\mathsf{X}]\diagdown\{0_{R[\mathsf{X}]}\}$, πρωταρχικό υπεράνω τής R, ούτως ώστε να ισχύει η ισότητα*

$$\varphi(\mathsf{X}) = c\,\widetilde{\varphi}(\mathsf{X}). \tag{5.174}$$

(ii) *Η έκφραση* (5.174) *τού $\varphi(\mathsf{X})$ είναι «κατ' ουσίαν μοναδική» υπό την εξής έννοια: Εάν υπάρχει κάποιο άλλο στοιχείο $c' \in \mathbf{Fr}(R)$, καθώς και κάποιο πολυώνυμο $\widetilde{\varphi}'(\mathsf{X}) \in R[\mathsf{X}]\diagdown\{0_{R[\mathsf{X}]}\}$, πρωταρχικό υπεράνω τής R, ούτως ώστε να ισχύει η ισότητα $\varphi(\mathsf{X}) = c'\,\widetilde{\varphi}'(\mathsf{X})$, τότε $\exists u \in R^\times : c' = uc$, με $\widetilde{\varphi}'(\mathsf{X}) = u^{-1}\widetilde{\varphi}(\mathsf{X})$ όταν $\varphi(\mathsf{X}) \neq 0_{\mathbf{Fr}(R)[\mathsf{X}]}$.*

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν πολυώνυμο $\varphi(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$. Γράφοντας το $\varphi(\mathsf{X})$ αναλυτικώς υπό τη μορφή

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} \frac{a_j}{b_j}\mathsf{X}^j,\ n \in \mathbb{N}_0,$$

όπου $(a_j, b_j) \in R \times (R\diagdown\{0_R\})$, $\forall j \in \{0,\ldots,n\}$, και θέτοντας $b := \prod_{j=0}^{n} b_j$ λαμβάνουμε

$$\varphi(\mathsf{X}) = b^{-1}\psi(\mathsf{X}),\ \text{όπου}\ \psi(\mathsf{X}) := \sum_{j=0}^{n}\left(a_j\left(\prod_{k\in\{0,\ldots,n\}\diagdown\{j\}} b_k\right)\right)\mathsf{X}^j \in R[\mathsf{X}].$$

Εν συνεχεία, θεωρώντας τυχόντα $d \in$ ΜΚΔ$_R$({συντελεστές τού $\psi(\mathsf{X})$}) και θέτοντας

$$\widetilde{\varphi}(\mathsf{X}) := \begin{cases} 1_R, & \text{όταν } \varphi(\mathsf{X}) = 0_{\mathbf{Fr}(R)[\mathsf{X}]}, \\ d^{-1}\psi(\mathsf{X}), & \text{όταν } \varphi(\mathsf{X}) \neq 0_{\mathbf{Fr}(R)[\mathsf{X}]}, \end{cases}$$

παρατηρούμε ότι το $\widetilde{\varphi}(\mathsf{X})$ είναι πρωταρχικό πολυώνυμο υπεράνω τής R. Επειδή $\varphi(\mathsf{X}) = db^{-1}\,\widetilde{\varphi}(\mathsf{X})$ αρκεί να θέσουμε $c := db^{-1}$.

(ii) Εξ υποθέσεως,

$$\varphi(\mathsf{X}) = c\,\widetilde{\varphi}(\mathsf{X}) = c'\,\widetilde{\varphi}'(\mathsf{X}).$$

Εκφράζοντας τα c, c' υπό τη μορφή κλασμάτων:

$$c = \frac{r_1}{r_2},\ c' = \frac{r_1'}{r_2'},\ r_1, r_1' \in R,\ r_2, r_2' \in R \smallsetminus \{0_R\},$$

και λαμβάνοντας υπ' όψιν ότι $r_2 r_2' \neq 0_R$, καταλήγουμε στην ισότητα

$$r_1 r_2' \widetilde{\varphi}(\mathsf{X}) = r_1' r_2 \widetilde{\varphi}'(\mathsf{X}). \tag{5.175}$$

Επειδή τα $\widetilde{\varphi}(\mathsf{X}), \widetilde{\varphi}'(\mathsf{X})$ είναι πρωταρχικά πολυώνυμα, έχουμε

$$\begin{array}{rcl} r_1 r_2' & \in & \text{ΜΚΔ}_R(\{\text{συντελεστές τού } r_1 r_2' \widetilde{\varphi}(\mathsf{X})\}), \\ r_1' r_2 & \in & \text{ΜΚΔ}_R(\{\text{συντελεστές τού } r_1' r_2 \widetilde{\varphi}'(\mathsf{X})\}), \end{array}$$

(βλ. 5.2.35 (iv)), οπότε η (5.175), σε συνδυασμό με το (ii) τής προτάσεως 5.2.12, δίδει $r_1 r_2' \underset{\text{συν.}}{\sim} r_1' r_2$. Άρα υπάρχει κάποιο $u \in R^{\times}$, τέτοιο ώστε να ισχύει

$$r_1' r_2 = u r_1 r_2' \Rightarrow c' = uc$$

(βλ. πόρισμα 5.2.5). Όταν $\varphi(\mathsf{X}) \neq 0_{\mathbf{Fr}(R)[\mathsf{X}]}$, λαμβάνουμε $\widetilde{\varphi}'(\mathsf{X}) = u^{-1}\widetilde{\varphi}(\mathsf{X})$ (καθόσον $c \neq 0_R$ και $c' \neq 0_R$). □

5.10.5 Λήμμα. *Έστω R μια Π.Μ.Π. Εάν $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ είναι ένα πολυώνυμο θετικού βαθμού και εάν υπάρχουν πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$, τέτοια ώστε να ισχύει η ισότητα $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$, τότε*

$$\exists c \in \mathbf{Fr}(R) \smallsetminus \{0_{\mathbf{Fr}(R)}\} : c\,\varphi_1(\mathsf{X}) \in R[\mathsf{X}] \text{ και } c^{-1}\,\varphi_2(\mathsf{X}) \in R[\mathsf{X}].$$

ΑΠΟΔΕΙΞΗ. Έστω $d \in$ ΜΚΔ$_R$({συντελεστές τού $\varphi(\mathsf{X})$}). Προφανώς, $d \neq 0_R$, και το πολυώνυμο $\overline{\varphi}(\mathsf{X}) := d^{-1}\varphi(\mathsf{X}) \in R[\mathsf{X}]$ είναι πρωταρχικό υπεράνω τής R. Σύμφωνα με το (i) τού λήμματος 5.10.4 υπάρχουν $c_1, c_2 \in \mathbf{Fr}(R)$, καθώς και κάποια πολυώνυμα $\widetilde{\varphi}_1(\mathsf{X}), \widetilde{\varphi}_2(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$, πρωταρχικά υπεράνω τής R, ούτως ώστε να ισχύουν οι ισότητες

$$\varphi_1(\mathsf{X}) = c_1\,\widetilde{\varphi}_1(\mathsf{X}) \text{ και } \varphi_2(\mathsf{X}) = c_2\,\widetilde{\varphi}_2(\mathsf{X}).$$

Το γινόμενο $\widetilde{\varphi}_1(\mathsf{X})\widetilde{\varphi}_2(\mathsf{X})$ των πρωταρχικών πολυωνύμων $\widetilde{\varphi}_1(\mathsf{X})$ και $\widetilde{\varphi}_2(\mathsf{X})$ είναι πρωταρχικό (βλ. πρόταση 5.10.3). Επομένως, επειδή αμφότερα τα $\overline{\varphi}(\mathsf{X})$ και $\widetilde{\varphi}_1(\mathsf{X})\widetilde{\varphi}_2(\mathsf{X})$ είναι πρωταρχικά, και

$$d\,\overline{\varphi}(\mathsf{X}) = \varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X}) = (c_1c_2)\,\widetilde{\varphi}_1(\mathsf{X})\widetilde{\varphi}_2(\mathsf{X}),$$

εφαρμόζοντας το (ii) τού λήμματος 5.10.4 (με τα $d, \overline{\varphi}(\mathsf{X}), c_1c_2, \widetilde{\varphi}_1(\mathsf{X})\widetilde{\varphi}_2(\mathsf{X})$ στη θέση των εκεί παρατεθέντων $c\,, \widetilde{\varphi}(\mathsf{X}), c'$ και $\widetilde{\varphi}'(\mathsf{X})$) εξασφαλίζουμε την ύπαρξη ενός στοιχείου $u \in R^{\times}$, τέτοιου ώστε να ισχύει $c_1c_2 = ud$. Θέτοντας $c := c_2$ λαμβάνουμε $c\,\varphi_1(\mathsf{X}) = c_1c_2\,\widetilde{\varphi}_1(\mathsf{X}) \in R[\mathsf{X}]$ και $c^{-1}\,\varphi_2(\mathsf{X}) = \widetilde{\varphi}_2(\mathsf{X}) \in R[\mathsf{X}]$. $\square$

5.10.6 Σημείωση. (i) Έστω R μια ακεραία περιοχή. Προφανώς, ένα πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ είναι ανάγωγο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$ έαν και μόνον εάν

(a) δεν είναι σταθερό πολυώνυμο τής μορφής $\varphi(\mathsf{X}) = r$, $r \in R^{\times} \cup \{0_R\}$, και

(b) γραφόμενο ως γινόμενο $\varphi(\mathsf{X}) = \psi(\mathsf{X})\chi(\mathsf{X})$, $\psi(\mathsf{X}), \chi(\mathsf{X}) \in R\,[\mathsf{X}]$, ισχύει

$$\text{είτε } \psi(\mathsf{X}) = a \in R^{\times} \text{ είτε } \chi(\mathsf{X}) = b \in R^{\times}.$$

(Βλ. 5.3.2 και 1.3.9 (iii).) Εν τοιαύτη περιπτώσει, για λόγους συντομίας, λέμε ότι το $\varphi(\mathsf{X})$ είναι **ανάγωγο υπεράνω τής** R.

(ii) Εάν το K είναι τυχόν *σώμα*, τότε ένα πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ είναι ανάγωγο υπεράνω τού K εάν και μόνον εάν

(a′) δεν είναι σταθερό πολυώνυμο (ήτοι $\deg(\varphi(\mathsf{X})) \geq 1$) και

(b′) δεν μπορεί να εκφρασθεί ως γινόμενο $\varphi(\mathsf{X}) = \psi(\mathsf{X})\chi(\mathsf{X})$ δύο πολυωνύμων $\psi(\mathsf{X}), \chi(\mathsf{X}) \in K\,[\mathsf{X}]$, με

$$1 \leq \deg(\psi(\mathsf{X})) < \deg(\varphi(\mathsf{X})) \ \text{ και } \ 1 \leq \deg(\chi(\mathsf{X})) < \deg(\varphi(\mathsf{X})),$$

αφού (σύμφωνα με το (i) τού πορίσματος 1.3.10)

$$K\,[\mathsf{X}]^{\times} = K^{\times} = K \smallsetminus \{0_K\} = \{\,\varphi\,(\mathsf{X}) \in K[\mathsf{X}] \mid \deg(\varphi(\mathsf{X})) = 0\}\,.$$

5.10.7 Λήμμα. *Έστω R μια Π.Μ.Π. Εάν ένα πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ θετικού βαθμού είναι ανάγωγο υπεράνω τής R, τότε είναι ανάγωγο και υπεράνω τού σώματος κλασμάτων $\mathbf{Fr}(R)$ τής R.*

ΑΠΟΔΕΙΞΗ. Έστω $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ ένα πολυώνυμο θετικού βαθμού, ανάγωγο υπεράνω τής R. Εάν το $\varphi(\mathsf{X})$ δεν ήταν ανάγωγο υπεράνω τού σώματος κλασμάτων $\mathbf{Fr}(R)$ τής R, τότε θα υπήρχαν πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}]$ θετικού βαθμού με $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$, καθώς κάποιο στοιχείο $c \in \mathbf{Fr}(R) \smallsetminus \{0_{\mathbf{Fr}(R)}\}$, τέτοιο ώστε $c\,\varphi_1(\mathsf{X}) \in R[\mathsf{X}]$ και $c^{-1}\,\varphi_2(\mathsf{X}) \in R[\mathsf{X}]$ (βλ. λήμμα 5.10.5). Εξ αυτού θα προέκυπτε ότι

$$\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X}) = (c\,\varphi_1(\mathsf{X}))\,(c^{-1}\,\varphi_2(\mathsf{X}))$$

με $\deg(c\varphi_1(\mathsf{X})) \geq 1$ και $\deg(c^{-1}\varphi_2(\mathsf{X})) \geq 1$, κάτι το οποίο θα αντέκειτο προς την αρχική μας υπόθεση. Άρα το $\varphi(\mathsf{X})$ είναι κατ' ανάγκην ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$. □

5.10.8 Λήμμα. *Έστω R μια ακεραία περιοχή και έστω $r \in R$. Για οιοδήποτε*

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in R[\mathsf{X}] \ (n \in \mathbb{N}_0)$$

τα ακόλουθα είναι ισοδύναμα:

(i) $r \mid a_j$, $\forall j \in \{0, \ldots, n\}$.

(ii) *Το r (θεωρούμενο ως σταθερό πολυώνυμο) διαιρεί το $\varphi(\mathsf{X})$ εντός τής ακεραίας περιοχής $R[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εξ υποθέσεως, $\exists b_j \in R : a_j = rb_j$ για κάθε $j \in \{0, \ldots, n\}$. Επομένως,

$$\varphi(\mathsf{X}) = \sum_{j=0}^{n} (rb_j)\, \mathsf{X}^j = r \left(\sum_{j=0}^{n} b_j \mathsf{X}^j \right) \Rightarrow r \mid \varphi(\mathsf{X}).$$

(ii)⇒(i) Εάν $r \mid \varphi(\mathsf{X})$ (εντός τής $R[\mathsf{X}]$), τότε *είτε* $r = 0_R \,(= 0_{R[\mathsf{X}]})$, οπότε έχουμε $\varphi(\mathsf{X}) = 0_{R[\mathsf{X}]}$ (και το (i) είναι προφανές) *είτε*

$$r \neq 0_R \ \text{ και } \ \exists \psi(\mathsf{X}) \in R[\mathsf{X}] : \varphi(\mathsf{X}) = r\psi(\mathsf{X}).$$

Εν τοιαύτη περιπτώσει, $\psi(\mathsf{X}) = 0_{R[\mathsf{X}]}$ όταν $\varphi(\mathsf{X}) = 0_{R[\mathsf{X}]}$, ενώ όταν $\varphi(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$ και $\deg(\varphi(\mathsf{X})) = n$, έχουμε $\deg(\psi(\mathsf{X})) = n$ (βλ. 1.3.9 (i)) και υπάρχουν $c_0, \ldots, c_n \in R$ (με $c_n \neq 0_R$), τέτοια ώστε

$$\psi(\mathsf{X}) = \sum_{j=0}^{n} c_j \mathsf{X}^j \Rightarrow \varphi(\mathsf{X}) = r \left(\sum_{j=0}^{n} c_j \mathsf{X}^j \right) = \sum_{j=0}^{n} (rc_j)\, \mathsf{X}^j,$$

οπότε $a_j = rc_j$ για κάθε $j \in \{0, \ldots, n\}$. □

5.10.9 Λήμμα. *Έστω R μια Π.Μ.Π. Εάν ένα πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}] \subseteq \mathbf{Fr}(R)[\mathsf{X}]$ είναι πρωταρχικό υπεράνω τού R και ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$, τότε είναι ανάγωγο και υπεράνω τής R.*

ΑΠΟΔΕΙΞΗ. Έστω $\varphi(\mathsf{X}) \in R[\mathsf{X}]$ ένα πολυώνυμο πρωταρχικό υπεράνω τού R και ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$. Τότε αυτό είναι προφανώς μη μηδενικό· επιπροσθέτως, έχει θετικό βαθμό (διότι κάθε σταθερό, μη μηδενικό, πρωταρχικό πολυώνυμο ανήκον στην ακεραία περιοχή $R[\mathsf{X}]$ ισούται με ένα αντιστρέψιμο στοιχείο τού R). Ας υποθέσουμε ότι $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$, για κάποια πολυώνυμα

$\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in R[\mathsf{X}]$. Αυτή η ισότητα μπορεί να ιδωθεί και ως μια παραγοντοποίση τού $\varphi(\mathsf{X})$ *εντός τού* $\mathbf{Fr}(R)[\mathsf{X}]$. Επομένως, τουλάχιστον ένα εκ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ οφείλει να είναι σταθερό, μη μηδενικό. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $\varphi_1(\mathsf{X}) = c \in R\smallsetminus\{0_R\}$. Σύμφωνα με το λήμμα 5.10.8 το c διαιρεί όλους τους συντελεστές τού $\varphi(\mathsf{X})$. Αυτό σημαίνει ότι $c \mid 1_{\mathbf{Fr}(R)}$ $(= 1_R)$, διότι το $\varphi(\mathsf{X})$ είναι εξ υποθέσεως πρωταρχικό υπεράνω τού $\mathbf{Fr}(R)$. Επομένως, $c \in R^\times$ ή, ισοδυνάμως, $\varphi_1(\mathsf{X}) \in R[\mathsf{X}]^\times$, οπότε το $\varphi(\mathsf{X})$ είναι ανάγωγο υπεράνω τής R. □

5.10.10 Σημείωση. Η «πρωταρχικότητα» τού $\varphi(\mathsf{X})$ δεν μπορεί να παραλειφθεί από τις προϋποθέσεις τού λήμματος 5.10.9. Επί παραδείγματι, το $4\mathsf{X} + 6$ είναι ανάγωγο υπεράνω τού $\mathbb{Q}$ αλλά δεν είναι ανάγωγο υπεράνω τού $\mathbb{Z}$, διότι $4\mathsf{X} + 6 = 2(2\mathsf{X} + 3)$, όπου $2 \notin \{\pm 1\} = \mathbb{Z}^\times$ και $2\mathsf{X} + 3 \notin \mathbb{Z}^\times$.

5.10.11 Λήμμα. *Έστω R μια Π.Μ.Π. Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}] \subseteq \mathbf{Fr}(R)[\mathsf{X}]$ θετικού βαθμού που είναι πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$, είναι πρώτο στοιχείο και τού $\mathbf{Fr}(R)[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. Έστω $\varphi(\mathsf{X})$ ένα πολυώνυμο θετικού βαθμού που είναι πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$. Τότε το $\varphi(\mathsf{X})$ είναι ανάγωγο στοιχείο τής $R[\mathsf{X}]$ (ήτοι ανάγωγο υπεράνω τής R) επί τη βάσει τού (iii) τής προτάσεως 5.3.4. Σύμφωνα με το λήμμα 5.10.7, αυτό είναι ανάγωγο και υπεράνω τού σώματος κλασμάτων $\mathbf{Fr}(R)$ τής R. Τέλος, επειδή ο πολυωνυμικός δακτύλιος $\mathbf{Fr}(R)[\mathsf{X}]$ είναι Π.Κ.Ι. (βλ. 5.4.24 (iii)⇒(ii)), το $\varphi(\mathsf{X})$ οφείλει να είναι πρώτο στοιχείο *και* τού $\mathbf{Fr}(R)[\mathsf{X}]$ (βλ. 5.3.4 (iv)). □

5.10.12 Λήμμα. *Έστω R μια Π.Μ.Π. Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in R[\mathsf{X}] \subseteq \mathbf{Fr}(R)[\mathsf{X}]$ που είναι πρώτο στοιχείο τού $\mathbf{Fr}(R)[\mathsf{X}]$ και πρωταρχικό υπεράνω τού R, είναι πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. Εάν $\varphi(\mathsf{X}) \mid \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$ εντός τού $R[\mathsf{X}]$ για κάποια πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in R[\mathsf{X}] \subseteq \mathbf{Fr}(R)[\mathsf{X}]$, τότε είτε $\varphi(\mathsf{X}) \mid \varphi_1(\mathsf{X})$ είτε $\varphi(\mathsf{X}) \mid \varphi_2(\mathsf{X})$ *εντός τού* $\mathbf{Fr}(R)[\mathsf{X}]$. Ας υποθέσουμε ότι

$$\exists \psi(\mathsf{X}) \in \mathbf{Fr}(R)[\mathsf{X}] : \varphi_1(\mathsf{X}) = \varphi(\mathsf{X})\psi(\mathsf{X}). \tag{5.176}$$

Έστω $d \in \text{ΜΚΔ}_R(\{\text{συντελεστές τού } \varphi(\mathsf{X})\})$. Προφανώς, $d \neq 0_R$, και το πολυώνυμο $\overline{\varphi}(\mathsf{X}) := d^{-1}\varphi(\mathsf{X}) \in R[\mathsf{X}]$ είναι πρωταρχικό υπεράνω τής R. Σύμφωνα με το (i) τού λήμματος 5.10.4, $\exists c_1, c \in \mathbf{Fr}(R)$, καθώς και κάποια $\widetilde{\varphi}_1(\mathsf{X}), \widetilde{\psi}(\mathsf{X}) \in R[\mathsf{X}]\smallsetminus\{0_{R[\mathsf{X}]}\}$, πρωταρχικά υπεράνω τής R, ούτως ώστε να ισχύουν οι ισότητες $\varphi_1(\mathsf{X}) = c_1\, \widetilde{\varphi}_1(\mathsf{X})$ και $\psi(\mathsf{X}) = c\,\widetilde{\psi}(\mathsf{X})$. Η (5.176) δίδει $c_1\, \widetilde{\varphi}_1(\mathsf{X}) = c\varphi(\mathsf{X})\widetilde{\psi}(\mathsf{X})$. Επειδή (κατά την πρόταση 5.10.3) το πολυώνυμο $\varphi(\mathsf{X})\widetilde{\psi}(\mathsf{X})$ είναι πρωταρχικό υπεράνω τής R, το (ii) τού λήμματος 5.10.4 μας πληροφορεί ότι $\exists u \in R^\times : c = uc_1$. Εάν $\varphi_1(\mathsf{X}) = 0_{R[\mathsf{X}]}$, τότε (προφανώς) $\varphi(\mathsf{X}) \mid \varphi_1(\mathsf{X})$ *εντός τής* $R[\mathsf{X}]$. Εάν $\varphi_1(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$, τότε $c_1 \neq 0_R$ και

$$\widetilde{\varphi}_1(\mathsf{X}) = u\varphi(\mathsf{X})\widetilde{\psi}(\mathsf{X}) \Rightarrow \varphi(\mathsf{X}) \mid \varphi_1(\mathsf{X}) \;\; (\text{εντός τής } R[\mathsf{X}]).$$

(Εάν $\varphi(\mathsf{X}) \mid \varphi_2(\mathsf{X})$ εντός τού $\mathbf{Fr}(R)[\mathsf{X}]$, τότε η απόδειξη τού ότι ισχύει $\varphi(\mathsf{X}) \mid \varphi_2(\mathsf{X})$ *και* εντός τής $R[\mathsf{X}]$ είναι πανομοιότυπη.) Άρα το $\varphi(\mathsf{X})$ είναι πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$. □

5.10.13 Λήμμα. *Έστω R μια ακεραία περιοχή και έστω $p \in R$. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Το p είναι ένα πρώτο στοιχείο τής R.*

(ii) *Το σταθερό πολυώνυμο $\varphi(\mathsf{X}) := p$ είναι ένα πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εξ ορισμού, $p \in R \smallsetminus (R^\times \cup \{0_R\})$. Επειδή $R[\mathsf{X}]^\times = R^\times$ και $0_{R[\mathsf{X}]} = 0_R$, έχουμε

$$\varphi(\mathsf{X}) := p \in R[\mathsf{X}] \smallsetminus (R[\mathsf{X}]^\times \cup \{0_{R[\mathsf{X}]}\}).$$

Έστω ότι $\varphi(\mathsf{X}) := p \mid \psi(\mathsf{X})\chi(\mathsf{X})$, για κάποια πολυώνυμα

$$\psi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}],\ \chi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}].$$

Υποθέτοντας ότι $p \nmid \psi(\mathsf{X})$ και $p \nmid \chi(\mathsf{X})$, το λήμμα 5.10.8 μας πληροφορεί ότι

$$[\exists i_0 \in \{0, \ldots, n\} : p \nmid a_{i_0}] \text{ και } [\exists j_0 \in \{0, \ldots, m\} : p \nmid b_{j_0}].$$

Θέτοντας $k := \min\{i \in \{0, \ldots, n\} : p \nmid a_i\}$ και $l := \min\{j \in \{0, \ldots, m\} : p \nmid b_j\}$, παρατηρούμε ότι

$$p \mid a_i b_j \text{ όταν } i + j = k + l \text{ και είτε } i < k \text{ είτε } j < l,$$

αλλά $p \nmid a_k b_l$, οπότε $p \nmid \sum_{i+j=k+l} a_i b_j$, δηλαδή το p δεν διαιρεί τον $(k+l)$-στό συντελεστή τού πολυωνύμου $\psi(\mathsf{X})\chi(\mathsf{X})$, κάτι το οποίο είναι αδύνατο (εκ νέου λόγω τού λήμματος 5.10.8). Άρα είτε $p \mid \psi(\mathsf{X})$ είτε $p \mid \chi(\mathsf{X})$ και, ως εκ τούτου, το $\varphi(\mathsf{X}) := p$ είναι ένα πρώτο στοιχείο τής ακεραίας περιοχής $R[\mathsf{X}]$.

(ii)⇒(i) Τούτο είναι προφανές. □

5.10.14 Πρόταση. *Ο δακτύλιος $R[\mathsf{X}]$ είναι Π.Μ.Π. για κάθε Π.Μ.Π. R.*

ΑΠΟΔΕΙΞΗ. Έστω R τυχούσα Π.Μ.Π. και έστω $\varphi(\mathsf{X}) \in R[\mathsf{X}] \smallsetminus (R[\mathsf{X}]^\times \cup \{0_{R[\mathsf{X}]}\})$. Αρκεί να αποδείξουμε ότι το $\varphi(\mathsf{X})$ διαθέτει κάποιο συντροφικό του πολυώνυμο παριστώμενο ως γινόμενο πεπερασμένου πλήθους πρώτων στοιχείων τής ακεραίας περιοχής $R[\mathsf{X}]$ (βλ. 5.6.3 (iii)⇒(i)). Το $\varphi(\mathsf{X})$ γράφεται υπό τη μορφή $\varphi(\mathsf{X}) = d\overline{\varphi}(\mathsf{X})$, όπου $d \in \text{ΜΚΔ}_R(\{\text{συντελεστές τού } \varphi(\mathsf{X})\})$ και $\overline{\varphi}(\mathsf{X}) \in R[\mathsf{X}]$ είναι πρωταρχικό υπεράνω τής R. Προφανώς, $d \neq 0_R$. Επιπροσθέτως, είναι αδύνατον να ισχύει $d \in R^\times$

και *ταυτοχρόνως* $\overline{\varphi}(\mathsf{X}) \in R[\mathsf{X}]^{\times}$ $(= R^{\times})$, διότι $\varphi(\mathsf{X}) \notin R[\mathsf{X}]^{\times}$. Άρα υπάρχουν τρία ενδεχόμενα:

Περίπτωση πρώτη. $d \notin R^{\times}$ και $\overline{\varphi}(\mathsf{X}) \in R[\mathsf{X}]^{\times}$ $(= R^{\times})$.

Περίπτωση δεύτερη. $d \in R^{\times}$ και $\overline{\varphi}(\mathsf{X}) \notin R[\mathsf{X}]^{\times}$.

Περίπτωση τρίτη. $d \notin R^{\times}$ και $\overline{\varphi}(\mathsf{X}) \notin R[\mathsf{X}]^{\times}$.

Στην πρώτη περίπτωση έχουμε $\overline{\varphi}(\mathsf{X}) = w$, για κάποιο $w \in R^{\times}$, και το d γράφεται υπό τη μορφή $d = uq_1 \cdots q_k$, όπου $u \in R^{\times}$, $k \in \mathbb{N}$, και τα $q_1, \ldots, q_k$ είναι πρώτα στοιχεία τής R (διότι η R είναι Π.Μ.Π.). Άρα

$$\varphi(\mathsf{X}) = d\overline{\varphi}(\mathsf{X}) = (uw)q_1 \cdots q_k,$$

όπου τα $q_1, \ldots, q_k$ (θεωρούμενα ως σταθερά πολυώνυμα) είναι πρώτα στοιχεία τής ακεραίας περιοχής $R[\mathsf{X}]$ (βλ. 5.10.13 (i)⇒(ii)).

Εν συνεχεία, θα εξετάσουμε τη δεύτερη και την τρίτη περίπτωση. Εάν το $\overline{\varphi}(\mathsf{X})$ είναι σταθερό, δηλαδή εάν $\overline{\varphi}(\mathsf{X}) = r$ για κάποιο $r \in R \smallsetminus (R^{\times} \cup \{0_R\})$, τότε γράφοντας το r υπό τη μορφή $r = zt_1 \cdots t_l$, όπου $z \in R^{\times}$, $l \in \mathbb{N}$, και τα $t_1, \ldots, t_k$ πρώτα στοιχεία τής R, λαμβάνουμε

$$\varphi(\mathsf{X}) = \begin{cases} (dz)\, t_1 \cdots t_l, & \text{όταν } d \in R^{\times}, \\ (uz) q_1 \cdots q_k t_1 \cdots t_l, & \text{όταν } d = uq_1 \cdots q_k \text{ (όπως στην 1η περ.)} \end{cases}$$

Εάν $\deg(\overline{\varphi}(\mathsf{X})) \geq 1$, τότε το $\overline{\varphi}(\mathsf{X})$, ιδωμένο ως στοιχείο τού $\mathbf{Fr}(R)[\mathsf{X}]$, παριστάται ως γινόμενο

$$\overline{\varphi}(\mathsf{X}) = \lambda \psi_1(\mathsf{X}) \cdots \psi_m(\mathsf{X}), \ \lambda \in R^{\times}, \ m \in \mathbb{N}, \tag{5.177}$$

μιας σταθεράς και m πρώτων στοιχείων $\psi_1(\mathsf{X}), \ldots, \psi_m(\mathsf{X})$ τού $\mathbf{Fr}(R)[\mathsf{X}]$ (καθόσον ο $\mathbf{Fr}(R)[\mathsf{X}]$ είναι Π.Μ.Π., βλ. 5.4.24 (iii)⇒(ii), πόρισμα 5.6.8 και 5.6.3 (i)⇒(iii)). Σύμφωνα με το (i) τού λήμματος 5.10.4 υπάρχουν πολυώνυμα $\chi_i(\mathsf{X}) \in R[\mathsf{X}]$, πρωταρχικά υπεράνω τού R, και

$$\exists (a_i, b_i) \in R \times (R \smallsetminus \{0_R\}) : \psi_i(\mathsf{X}) = \frac{a_i}{b_i} \chi_i(\mathsf{X}),$$

για κάθε $i \in \{1, \ldots, m\}$. Εντός τής ακεραίας περιοχής $R[\mathsf{X}]$ ισχύει η ισότητα

$$b\, \overline{\varphi}(\mathsf{X}) = (\lambda a)\, \chi_1(\mathsf{X}) \cdots \chi_m(\mathsf{X}),$$

όπου τόσον το $\overline{\varphi}(\mathsf{X})$ (εκ κατασκευής) όσον και το γινόμενο $\chi_1(\mathsf{X}) \cdots \chi_m(\mathsf{X})$ (λόγω τής προτάσεως 5.10.3) είναι πρωταρχικά πολυώνυμα υπεράνω τού R. Το (ii) τού λήμματος 5.10.4 μας πληροφορεί ότι $\exists \xi \in R^{\times} : \lambda a = \xi b$. Επομένως η (5.177) δίδει

$$b \neq 0_R \Longrightarrow \overline{\varphi}(\mathsf{X}) = \xi\, \chi_1(\mathsf{X}) \cdots \chi_m(\mathsf{X}).$$

Σημειωτέον ότι για κάθε δείκτη $i \in \{1, \ldots, m\}$ έχουμε

$$\psi_i(\mathsf{X}) \neq 0_{\mathbf{Fr}(R)[\mathsf{X}]} \Rightarrow a_i \neq 0_R \Rightarrow \frac{a_i}{b_i} \in \mathbf{Fr}(R) \smallsetminus \{0_{\mathbf{Fr}(R)}\} \ (= \mathbf{Fr}(R)^{\times}),$$

οπότε τα $\psi_i(\mathsf{X})$ και $\chi_i(\mathsf{X})$ είναι συντροφικά εντός τού $\mathbf{Fr}(R)[\mathsf{X}]$. Επειδή το $\psi_i(\mathsf{X})$ είναι πρώτο στοιχείο τού $\mathbf{Fr}(R)[\mathsf{X}]$, το $\chi_i(\mathsf{X})$ είναι ωσαύτως πρώτο στοιχείο τού $\mathbf{Fr}(R)[\mathsf{X}]$ (βλ. 5.3.4 (v)) και, κατ' επέκταση, *πρώτο στοιχείο τής ακεραίας περιοχής* $R[\mathsf{X}]$ (δυνάμει τού λήμματος 5.10.12). Τελικώς λοιπόν η

$$\varphi(\mathsf{X}) = \begin{cases} (d\xi)\,\chi_1(\mathsf{X})\cdots\chi_m(\mathsf{X}), & \text{όταν } d \in R^{\times}, \\ (u\xi)q_1\cdots q_k\,\chi_1(\mathsf{X})\cdots\chi_m(\mathsf{X}), & \text{όταν } d = uq_1\cdots q_k \\ & \text{(όπως στην 1η περ.)} \end{cases}$$

είναι η ζητούμενη παραγοντοποίηση. □

5.10.15 Σημείωση. (i) Σύμφωνα με την πρόταση 5.10.14, ο πολυωνυμικός δακτύλιος $\mathbb{Z}[\mathsf{X}]$ είναι Π.Μ.Π. Ωστόσο, όπως γνωρίζουμε από την πρόταση 5.4.24, αυτός δεν είναι Π.Κ.Ι.

(ii) Πηλικοδακτύλιοι δομούμενοι μέσω περιοχών μονοσήμαντης παραγοντοποιήσεως δεν είναι απαραιτήτως Π.Μ.Π. Επί παραδείγματι, έχουμε

$$\mathbb{Z}[\mathsf{X}]/\left\langle \mathsf{X}^2+3\right\rangle \cong \mathbb{Z}[\sqrt{-3}],$$

όπου η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{-3}]$ δεν είναι Π.Μ.Π.

5.10.16 Πόρισμα. *Ο πολυωνυμικός δακτύλιος $R[\mathsf{X}_1,\ldots,\mathsf{X}_n]$ είναι Π.Μ.Π. για κάθε Π.Μ.Π. R και για κάθε $n \in \mathbb{N}$.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί η πρόταση 5.10.14 και μαθηματική επαγωγή ως προς τον n. □

5.10.17 Θεώρημα. *Έστω R μια ακεραία περιοχή. Οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Η R είναι Π.Μ.Π.*

(ii) *Η ακεραία περιοχή $R[\mathsf{X}]$ είναι Π.Μ.Π.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Βλ. πρόταση 5.10.14.

(ii)⇒(i) Εάν η ακεραία περιοχή $R[\mathsf{X}]$ είναι Π.Μ.Π. και $a \in R\smallsetminus(R^{\times}\cup\{0_R\})$, τότε, θεωρώντας τό a ως ένα σταθερό πολυώνυμο ανήκον στην $R[\mathsf{X}]$, το γράφουμε υπό τη μορφή

$$a = u\gamma_1(\mathsf{X})\cdots\gamma_k(\mathsf{X}),\ k\in\mathbb{N},\ u\in R[\mathsf{X}]^{\times} = R^{\times},$$

όπου τα $\gamma_1(\mathsf{X}),\ldots,\gamma_k(\mathsf{X})$ είναι ανάγωγα (και, ως εκ τούτου, πρώτα) στοιχεία τής $R[\mathsf{X}]$. Επειδή ο βαθμός τού αριστερού μέλος τής ανωτέρω ισότητας οφείλει να ισούται με τον βαθμό τού δεξιού της μέλους, λαμβάνουμε

$$\deg(\gamma_1(\mathsf{X})) = \cdots = \deg(\gamma_k(\mathsf{X})) = 0$$

οπότε καθένα εκ των $\gamma_1(\mathsf{X}),\ldots,\gamma_k(\mathsf{X})$ είναι ένα μη μηδενικό σταθερό πολυώνυμο, ήτοι ένα πρώτο στοιχείο τής R (βλ. 5.10.13 (ii)⇒(i)). Κατά συνέπειαν, και η ίδια η R είναι Π.Μ.Π. (βλ. 5.6.3 (iii)⇒(i)). □

5.10.18 Πόρισμα. *Έστω R μια ακεραία περιοχή. Οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Η R είναι Π.Μ.Π.*

(ii) *Η ακεραία περιοχή $R[\mathsf{X}_1,\ldots,\mathsf{X}_n]$ είναι Π.Μ.Π. για κάθε $n\in\mathbb{N}$.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το θεώρημα 5.10.17 και το πόρισμα 5.10.16. □

5.10.19 Σημείωση. Η πρόταση 5.10.14 και το πόρισμα 5.10.16 παύουν να ισχύουν (χωρίς ειδικούς επιπρόσθετους περιορισμούς) εάν κανείς αντικαταστήσει τον $R[\mathsf{X}]$ (και αντιστοίχως, τον $R[\mathsf{X}_1,\ldots,\mathsf{X}_n]$) με τον δακτύλιο των επίτυπων δυναμοσειρών $R[\![\mathsf{X}]\!]$ (και αντιστοίχως, τον $R[\![\mathsf{X}_1,\ldots,\mathsf{X}_n]\!]$). Επί παραδείγματι, ο P. Salmon απέδειξε το[110] 1966 ότι για οιοδήποτε σώμα K ο πηλικοδακτύλιος

$$R:=K(\mathsf{Y})[\![\mathsf{Z}_1,\mathsf{Z}_2,\mathsf{Z}_3]\!]/\left\langle \mathsf{Z}_1^2+\mathsf{Z}_2^3+\mathsf{Y}\mathsf{Z}_3^6\right\rangle$$

είναι Π.Μ.Π. αλλά ο $R[\![\mathsf{X}]\!]$ *δεν είναι* Π.Μ.Π.!

► **Κριτήριο τού Eisenstein**. Κάνοντας χρήση τού επιμορφισμού (5.173) και τού λήμματος 5.10.5 είναι δυνατόν να αποδειχθεί το ακόλουθο λίαν σημαντικό θεώρημα:

5.10.20 Θεώρημα. (Eisenstein, 1850) *Έστω R μια Π.Μ.Π. και έστω*

$$\varphi(\mathsf{X})=\sum_{i=0}^{n}a_i\mathsf{X}^i\in R[\mathsf{X}]$$

ένα πολυώνυμο βαθμού $n\geq 1$. Εάν υπάρχει ένα πρώτο στοιχείο p τής R, τέτοιο ώστε

(i) $p\mid a_i,\ \forall i\in\{0,\ldots,n-1\}$,

(ii) $p\nmid a_n$ *και*

(iii) $p^2\nmid a_0$,

τότε το $\varphi(\mathsf{X})$ είναι ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$ (και ανάγωγο υπεράνω τής R όταν είναι πρωταρχικό υπεράνω τής R).

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι $\varphi(\mathsf{X})=\varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$ για κάποια πολυώνυμα $\varphi_1(\mathsf{X}),\varphi_2(\mathsf{X})\in\mathbf{Fr}(R)[\mathsf{X}]$ *θετικού βαθμού*. Τότε

$$\varphi(\mathsf{X})=\psi_1(\mathsf{X})\psi_2(\mathsf{X}),\ \psi_1(\mathsf{X})=t\,\varphi_1(\mathsf{X})\in R[\mathsf{X}],\psi_2(\mathsf{X})=t^{-1}\,\varphi_2(\mathsf{X})\in R[\mathsf{X}],$$

[110] P. Salmon: *Su un problema posto da P. Samuel*, Atti Accad. Naz. Lincei Rend. Sci. Fis. Mat. Natur. (8) **40** (1966), 801-803.

για κάποιο κατάλληλο $t \in \mathbf{Fr}(R)\smallsetminus\{0_{\mathbf{Fr}(R)}\}$ (δυνάμει τού λήμματος 5.10.5). Σημειωτέον ότι $\deg(\psi_1(\mathsf{X})) = \deg(\varphi_1(\mathsf{X}))$ και $\deg(\psi_2(\mathsf{X})) = \deg(\varphi_2(\mathsf{X}))$. Λόγω των προϋποτεθεισών συνθηκών (i) και (ii) η εφαρμογή τού επιμορφισμού (5.173) στο $\varphi(\mathsf{X})$ δίδει

$$\begin{aligned} \mathfrak{H}_p(\psi_1(\mathsf{X}))\mathfrak{H}_p(\psi_2(\mathsf{X})) &= \mathfrak{H}_p(\psi_1(\mathsf{X})\psi_2(\mathsf{X})) \\ &= \mathfrak{H}_p(\varphi(\mathsf{X})) = (a_n + \langle p\rangle)\,\mathsf{X}^n \end{aligned}$$

και οι εικόνες των $\psi_1(\mathsf{X}), \psi_2(\mathsf{X})$ μέσω αυτού οφείλουν να εκφράζονται ως εξής:

$$\mathfrak{H}_p(\psi_1(\mathsf{X})) = (b_m + \langle p\rangle)\,\mathsf{X}^m,\ \mathfrak{H}_p(\psi_2(\mathsf{X})) = (c_{n-m} + \langle p\rangle)\,\mathsf{X}^{n-m}, \tag{5.178}$$

για κάποιον φυσικό αριθμό m με $0 < m < n$ και $b_m, c_{n-m} \in R$ (διότι ο πολυωνυμικός δακτύλιος $(R/\langle p\rangle)[\mathsf{X}]$) είναι ακεραία περιοχή, πρβλ. 1.3.9 (i)). Επιπροσθέτως, τα $\psi_1(\mathsf{X}), \psi_2(\mathsf{X})$ είναι κατ' ανάγκην τής μορφής

$$\psi_1(\mathsf{X}) = \sum_{j=0}^{m} b_j\mathsf{X}^j,\ \psi_2(\mathsf{X}) = \sum_{k=0}^{n-m} c_k\mathsf{X}^k,$$

όπου $b_0, \ldots, b_{m-1}, c_0, \ldots, c_{n-m-1} \in R$ με $p \mid b_0$ και $p \mid c_0$ (λόγω των (5.178)!). Επομένως, $p^2 \mid b_0c_0 = a_0$, κάτι που αντίκειται προς τη συνθήκη (iii). Κατά συνέπειαν, τουλάχιστον ένα εκ των (εκ κατασκευής μη μηδενικών) $\psi_1(\mathsf{X}), \psi_2(\mathsf{X})$ είναι σταθερό και, ως εκ τούτου, τουλάχιστον ένα εκ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ είναι σταθερό. Αυτό σημαίνει ότι το $\varphi(\mathsf{X})$ είναι ανάγωγο υπεράνω τού $\mathbf{Fr}(R)$ (και ανάγωγο υπεράνω τής R όταν είναι πρωταρχικό υπεράνω τής R επί τη βάσει τού λήμματος 5. 10.9). $\square$

5.10.21 Παράδειγμα. Έστω $\varphi(\mathsf{X}) := 3\mathsf{X}^5 + 15\mathsf{X}^4 - 20\mathsf{X}^3 + 10\mathsf{X} + 20 \in \mathbb{Z}[\mathsf{X}]$. Το $\varphi(\mathsf{X})$ είναι πρωταρχικό υπεράνω τού $\mathbb{Z}$. Μέσω τού κριτηρίου τού Eisenstein διαπιστώνουμε ότι αυτό είναι ανάγωγο τόσον υπεράνω τού $\mathbb{Q}$ όσον και υπεράνω τού $\mathbb{Z}$, καθότι $5 \nmid 3$, $25 \nmid 20$ και το 5 διαιρεί τους ακεραίους $15, -20, 10$ και 20.

5.11 ΑΔΡΟΜΕΡΗΣ ΙΕΡΑΡΧΗΣΗ ΑΚΕΡΑΙΩΝ ΠΕΡΙΟΧΩΝ

Οι ιδιότητες τής διαιρετότητας, οι μελετηθείσες στο παρόν κεφάλαιο, μας οδηγούν στη σύνταξη τού πίνακα τής σελίδας 343, μέσω τού οποίου γίνεται μια (έστω και) αδρομερής ιεράρχηση (διαφόρων ειδών) ακεραίων περιοχών.

5.11.1 Σημείωση. Οι εγκλειστικές σχέσεις (μεταξύ των ποικίλων κλάσεων δακτυλίων) που περιλαμβάνονται σε αυτόν τον πίνακα (από κάτω προς τα επάνω και εξ αριστερών προς τα δεξιά) προκύπτουν από τα εδάφια 2.7.3 (i), 2.3.3, 2.3.2, 5.4.3 (i), 4.2.3, 5.4.21, 5.6.8, 5.6.13, 5.6.16, 5.3.6, 5.6.5 και 5.6.6. (Εξαιρούνται μόνον οι λεγόμενες *περιοχές τού Dedekind*, οι οποίες δεν εστάθη δυνατόν να ορισθούν και να μελετηθούν κατά τη διάρκεια των παραδόσεων λόγω ελλείψεως χρόνου.)

5.11.2 Παραδείγματα. Όλοι οι εγκλεισμοί τού πίνακα είναι *αυστηροί*. Δειγματοληπτικώς (και εκ νέου από κάτω προς τα επάνω και εξ αριστερών προς τα δεξιά) αναφέρουμε τα εξής:

(i) Οι δακτύλιοι $\mathbb{Z}_{\langle p\rangle}$ (όπου p πρώτος) και $K[\![\mathsf{X}]\!]$ (όπου K σώμα) αποτελούν παραδείγματα τοπικών δακτυλίων που δεν είναι σώματα. (Βλ. 2.7.3 (ii) και (iv).)

(ii) Ο δακτύλιος $\mathbb{H}_{\mathbb{R}}$ των τετρανίων υπεράνω τού σώματος $\mathbb{R}$ είναι ένα στρεβλό σώμα (= διαιρετικός δακτύλιος) που δεν είναι σώμα. (Βλ. 1.2.19 (ii).)

(iii) Ο δακτύλιος $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ είναι ένας απλός δακτύλιος με μοναδιαίο στοιχείο που δεν είναι στρεβλό σώμα. (Βλ. προτάσεις 2.3.4 και 1.2.14.)

(iv) Ο $\mathbb{Z}$ μπορεί να εφοδιασθεί με ευκλείδειες στάθμες αλλά (προφανώς) δεν είναι σώμα. (Βλ. 5.4.3 (ii).)

(v) Ο $\mathbb{Z}/m\mathbb{Z}$, όπου m ένας σύνθετος φυσικός αριθμός, είναι ένας μεταθετικός δακτύλιος κυρίων ιδεωδών με μοναδιαίο στοιχείο που δεν είναι ούτε διαιρετικός δακτύλιος ούτε Π.Κ.Ι. (Βλ. πόρισμα 4.2.7.)

(vi) Ο δακτύλιος $\mathfrak{O}_m$ των ακεραίων τού $\mathbb{Q}(\sqrt{m})$ είναι Π.Κ.Ι. αλλά όχι και ευκλείδεια περιοχή όταν $m \in \{-163, -67, -43, -19\}$. (Βλ. πόρισμα 5.5.16.)

(vii) Ο δακτύλιος $\mathbb{Z}[\mathsf{X}]$ είναι Π.Μ.Π. αλλά δεν είναι Π.Κ.Ι. (Βλ. 5.10.15 (i).)

(viii) Ο δακτύλιος $R := \left\{ z \in \mathbb{C} \,|\, \varphi(z) = 0, \text{ για κάποιο μονικό } \varphi(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}] \smallsetminus \{0_{\mathbb{Z}[\mathsf{X}]}\} \right\}$ είναι μια περιοχή με μ.κ.δ. που δεν είναι Π.Μ.Π.

(ix) Εάν για κάθε $n \in \mathbb{N}_0$ θέσουμε $\xi_n := \sqrt[2^n]{2}$, τότε ορίζεται η ακεραία περιοχή

$$R_n := \mathbb{Z}[\xi_n] = \{\varphi(\xi_n) \,|\, \varphi(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]\}$$

και σχηματίζεται μια ανιούσα ακολουθία ακεραίων περιοχών

$$\mathbb{Z} = R_0 \subsetneqq R_1 \subsetneqq R_2 \subsetneqq \cdots \subsetneqq R_{n-1} \subsetneqq R_n \subsetneqq \cdots$$

Ο υποδακτύλιος $R := \bigcup_{n\in\mathbb{N}_0} R_n$ τού $\mathbb{R}$ που προκύπτει ως ένωση αυτών είναι ωσαύτως μια ακεραία περιοχή. Αφήνεται ως άσκηση η απόδειξη τού ότι $\xi_n \notin R^{\times}$, $\forall n \in \mathbb{N}_0$, και τού ότι (στην ακολουθία $(\xi_n)_{n\in\mathbb{N}_0}$) ο όρος ξ_{n+1} είναι ένας γνήσιος διαιρέτης τού ξ_n (καθόσον $\xi_{n+1}^2 = \xi_n$). Μέσω αυτής συμπεραίνουμε ότι η ακεραία περιοχή R *δεν πληροί* τη συνθήκη των αλυσίδων γνησίων διαιρετών. (Βλ. 5.6.4.)

(x) Η τετραγωνική αριθμητική περιοχή $\mathbb{Z}[\sqrt{-5}]$ είναι περιοχή με παραγοντοποίηση αλλά δεν είναι ούτε περιοχή με μ.κ.δ. ούτε Π.Μ.Π. (Βλ. 5.2.43 (iii) και 5.6.7 (i).)

(xi) Έστω $\mathcal{O}(\mathbb{C}) := \{\text{συναρτήσεις } f : \mathbb{C} \longrightarrow \mathbb{C} \,|\, f \text{ ολόμορφη}\}$ η ακεραία περιοχή των λεγομένων *ακεραίων συναρτήσεων* μιας μιγαδικής μεταβλητής (βλ. 3.5.6 (iii)). Τα αντιστρέψιμα στοιχεία της είναι οι ακέραιες συναρτήσεις που δεν μηδενίζονται πουθενά. Είναι εύκολο να αποδειχθεί ότι *κάθε ανάγωγο στοιχείο της είναι πρώτο* και ότι το σύνολο των αναγώγων (= πρώτων) στοιχείων της αποτελείται από τις γραμμικές συναρτήσεις τής μορφής $z - a$, $a \in \mathbb{C}$. Ως εκ τούτου, η $\mathcal{O}(\mathbb{C})$ *δεν είναι περιοχή με παραγοντοποίηση*. (Εάν υποθέταμε το αντίθετο, τότε θα έπρεπε *κάθε* $f \in \mathcal{O}(\mathbb{C})$ να γράφεται ως γινόμενο $f = gh_1 \cdots h_k$ μιας πουθενά μηδενιζόμενης συνάρτησης $g \in \mathcal{O}(\mathbb{C})^{\times}$ και πεπερασμένου πλήθους συναρτήσεων τής μορφής

$$h_1(z) = z - a_1, \ldots , h_k(z) = z - a_k,\ k \in \mathbb{N},\ a_1, \ldots , a_k \in \mathbb{C},$$

κάτι που θα ήταν αδύνατο, καθόσον υπάρχουν συναρτήσεις $f \in \mathcal{O}(\mathbb{C})$, όπως, π.χ., η $f(z) = \sin z$, που διαθέτουν άπειρα (σαφώς διακεκριμένα) σημεία τού μιγαδικού επιπέδου ως σημεία μηδενισμού της. Σημειωτέον ότι στο εδάφιο 4.1.14 χρησιμοποιήσαμε παρόμοια επιχειρήματα για να αποδείξουμε ότι η $\mathcal{O}(\mathbb{C})$ *δεν είναι ναιτεριανή*.)

(xii) Για κάθε σώμα K υφίσταται μια ανιούσα ακολουθία ακεραίων περιοχών

$$K[\mathsf{X}_1] \subsetneqq K[\mathsf{X}_1, \mathsf{X}_2] \subsetneqq \cdots \subsetneqq K[\mathsf{X}_1, \ldots , \mathsf{X}_{n-1}] \subsetneqq K[\mathsf{X}_1, \ldots , \mathsf{X}_n] \subsetneqq \cdots$$

Ο πολυωνυμικός δακτύλιος άπειρων (αριθμήσιμων, ανεξάρτητων) απροσδιορίστων

$$K[\mathsf{X}_1, \mathsf{X}_2, \ldots , \mathsf{X}_{m-1}, \mathsf{X}_m, \ldots] := \bigcup_{n\in\mathbb{N}} K[\mathsf{X}_1, \ldots , \mathsf{X}_n],$$

που προκύπτει ως ένωση αυτών, είναι μια περιοχή με παραγοντοποίηση (και μάλιστα μια Π.Μ.Π.) αλλά δεν είναι ναιτεριανή περιοχή, διότι το $\langle\{\, \mathsf{X}_n \,|\, n \in \mathbb{N}\}\rangle$ δεν είναι πεπερασμένως παραγόμενο ιδεώδες αυτής. (Βλ. θεώρημα 4.1.11.)

(xiii) Ο $\mathbb{Z}_6$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο που δεν είναι ακεραία περιοχή. (Βλ. πόρισμα 1.2.27.)

(xiv) Ο $2\mathbb{Z}$ είναι ένας μεταθετικός δακτύλιος χωρίς μοναδιαίο στοιχείο. (Βλ. εδάφιο 1.1.4 (iii).)

$$
\begin{array}{ccccc}
\{\text{Ακέραιες περιοχές}\} & \subset & \left\{\begin{matrix}\text{Μεταθετικοί}\\ \text{1-δακτύλιοι}\end{matrix}\right\} & \subset & \left\{\begin{matrix}\text{Μεταθετικοί}\\ \text{δακτύλιοι}\end{matrix}\right\} \\
\cup & & & & \cup \\
\left\{\begin{matrix}\text{Περιοχές με}\\ \text{παραγοντοποίηση}\end{matrix}\right\} & \supset & \{\text{Ναιτεριανές περιοχές}\} & \supset & \left\{\begin{matrix}\text{Περιοχές}\\ \text{τού}\\ \text{Dedekind}\end{matrix}\right\} \\
\cup & & & & \\
\left\{\begin{matrix}\text{Περιοχές}\\ \text{που πληρούν}\\ \text{τη συνθήκη}\\ \text{των αλυσίδων}\\ \text{γνησίων}\\ \text{διαιρετών}\end{matrix}\right\} & & \left\{\begin{matrix}\text{Περιοχές,}\\ \text{στις οποίες}\\ \text{κάθε ανάγωγο}\\ \text{στοιχείο}\\ \text{είναι πρώτο}\end{matrix}\right\} & & \\
\cup & & \cup & & \\
\left\{\begin{matrix}\text{Περιοχές}\\ \text{μονοσήμαντης}\\ \text{παραγοντοποιήσεως}\\ \text{(Π.Μ.Π)}\end{matrix}\right\} & \subset & \left\{\begin{matrix}\text{Περιοχές με}\\ \text{μ.κ.δ.}\end{matrix}\right\} & & \left\{\begin{matrix}\text{Δακτύλιοι}\\ \text{κυρίων}\\ \text{ιδεωδών}\\ \text{(Δ.Κ.Ι)}\end{matrix}\right\} \\
\cup & & & & \cup \\
\left\{\begin{matrix}\text{Περιοχές κυρίων}\\ \text{ιδεωδών (Π.Κ.Ι)}\end{matrix}\right\} & \subset & \left\{\begin{matrix}\text{Μεταθετικοί}\\ \text{δακτύλιοι}\\ \text{κυρίων}\\ \text{ιδεωδών}\end{matrix}\right\} & & \left\{\begin{matrix}\text{1-δακτύλιοι}\\ \text{κυρίων}\\ \text{ιδεωδών}\end{matrix}\right\} \\
\cup & & & & \\
\{\text{Ευκλείδειες περιοχές}\} & & & & \cup \\
\cup & & & & \\
\{\text{Σώματα}\} & \subset & \left\{\begin{matrix}\text{Στρεβλά}\\ \text{σώματα}\end{matrix}\right\} & = & \left\{\begin{matrix}\text{Διαιρετικοί}\\ \text{δακτύλιοι}\end{matrix}\right\} \\
\parallel & & \cap & & \\
\left\{\begin{matrix}\text{Απλοί μεταθετικοί}\\ \text{1-δακτύλιοι}\end{matrix}\right\} & & \left\{\begin{matrix}\text{Απλοί}\\ \text{1-δακτύλιοι}\end{matrix}\right\} & & \\
\cap & & & & \\
\left\{\begin{matrix}\text{Τοπικοί}\\ \text{δακτύλιοι}\end{matrix}\right\} & & & &
\end{array}
$$