ΚΕΦΑΛΑΙΟ 5

Δακτύλιοι πολυωνύμων μιας μεταβλητής

Στο κεφάλαιο αυτό μελετούμε τον δακτύλιο $R[\mathsf{X}]$ των πολυωνύμων μιας μεταβλητής X με συντελεστές ειλημμένους από έναν τυχόντα 1-δακτύλιο R· εν συνεχεία, αναφερόμαστε στη διαιρετότητα των πολυωνύμων (κυρίως όταν ο R είναι ακεραία περιοχή ή σώμα), στις θέσεις μηδενισμού τους, καθώς και στην πρωταρχική (μονοσήμαντη) διάσπαση των μονικών σε πεπερασμένου πλήθους ανάγωγα πολυώνυμα.

5.1 ΘΕΜΕΛΙΩΔΕΙΣ ΟΡΙΣΜΟΙ

Δοθέντος ενός δακτυλίου R με μοναδιαίο στοιχείο του το $1\,(=1_R)$ θεωρούμε το σύνολο $\mathcal{A}$ όλων των ακολουθιών $(a_0, a_1, a_2, \dots\dots)$ με τα $a_i \in R$, $i = 0, 1, 2, \dots$, για τις οποίες μόνον ένα πεπερασμένο πλήθος των a_i είναι διάφορα τού $0\,(=0_R)$. Έτσι λοιπόν κάθε στοιχείο f τού $\mathcal{A}$ γράφεται υπό τη μορφή

$$f = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$$

για κάποιον ακέραιο αριθμό $n \geq 0$. Επί τού $\mathcal{A}$ ορίζουμε πράξεις *προσθέσεως* και *πολλαπλασιασμού* ως ακολούθως:

$$\left|\begin{array}{lcl} (a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) & := & (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots), \\ \\ (a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) & := & (c_0, c_1, c_2, \dots), \end{array}\right.$$

όπου

$$c_m := \sum_{i+j=m} a_i b_j = a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0,\ \forall m \in \mathbb{N}_0. \tag{5.1}$$

Η τριάδα $(\mathcal{A}, +, \cdot)$ αποτελεί έναν δακτύλιο με μηδενικό του στοιχείο το $(0, 0, \dots)$ και μοναδιαίο του στοιχείο το $(1, 0, 0, \dots)$. Ο R εμφυτεύεται στον $\mathcal{A}$ μέσω τού μονομορφισμού

$$R \longrightarrow \mathcal{A}, \quad a \longmapsto (a, 0, 0, \dots)\,.$$

Ως εκ τούτου, η εικόνα τού R είναι ένας υποδακτύλιος τού $\mathcal{A}$, και μπορούμε χωρίς βλάβη τής γενικότητας να *ταυτίζουμε*, από εδώ και στο εξής, το a με το $(a, 0, 0, \dots)$. Εισάγοντας ένα νέο σύμβολο

$$\mathsf{X} := (0, 1, 0, 0, \dots)$$

παρατηρούμε ότι, βάσει των ως άνω πράξεων,

$$\mathsf{X}^2 = (0, 0, 1, 0, 0, \dots)\,,$$

$$\mathsf{X}^3 = (0, 0, 0, 1, 0, 0, \dots)\,,$$

και, γενικότερα,

$$\mathsf{X}^n = (0, 0, \dots, 0, \underbrace{1}_{n+1\ \text{θέση}}, 0, 0, \dots),\ \forall n \in \mathbb{N}_0.$$

Επίσης, λόγω τής ανωτέρω ταυτίσεως, για κάθε $a \in R$ λαμβάνουμε

$$a\mathsf{X}^n = (0, 0, \dots, 0, \underbrace{a}_{n+1\ \text{θέση}}, 0, 0, \dots),\ \forall n \in \mathbb{N}_0.$$

Εάν λοιπόν το $(a_0, a_1, a_2, \dots)$ είναι τυχόν στοιχείο τού $\mathcal{A}$, όπου $a_i = 0$, για κάθε $i \geq n$, για κάποιον παγιωμένο $n \in \mathbb{N}_0$, τότε μπορούμε να γράψουμε

$$(a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) = a_0 + a_1\mathsf{X} + a_2\mathsf{X} + \cdots + a_n\mathsf{X}^n = \sum_{i=0}^{n} a_i \mathsf{X}^i.$$

5.1.1 Ορισμός. Ο δακτύλιος $\mathcal{A}$ συμβολίζεται συνήθως ως $R\,[\mathsf{X}]$ και καλείται **δακτύλιος πολυωνύμων** (ή **πολυωνυμικός δακτύλιος**) μιας **μεταβλητής** (ή μιας **απροσδιορίστου**) X με συντελεστές ειλημμένους από τον R. Τα στοιχεία του ονομάζονται **πολυώνυμα** και σημειώνονται ως $f(\mathsf{X}), g(\mathsf{X}), ..$ κ.λπ., ενώ τα εκάστοτε αναγραφόμενα $a_0, a_1, a_2, \dots$ ονομάζονται **συντελεστές** των πολυωνύμων.

5.1.2 Παρατήρηση. Βάσει τού ορισμού τού πολλαπλασιασμού πολυωνύμων είναι σαφές ότι ο δακτύλιος $R[\mathsf{X}]$ είναι μεταθετικός όταν ο ίδιος ο R είναι μεταθετικός.

5.1.3 Σημείωση. Εκ των ανωτέρω συμπεραίνουμε ότι δυο πολυώνυμα

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

είναι **ίσα** (γράφοντας $f(\mathsf{X}) = g(\mathsf{X})$) εάν και μόνον εάν

$$n = m \ \text{ και } \ a_i = b_i,\ \ \forall i \in \{1, 2, \dots, n\}.$$

5.1.4 Ορισμός. Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Εάν

$$f(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}] \ \text{ και } \ a_n \neq 0,$$

τότε λέμε ότι ο αριθμός $\deg(f(\mathsf{X})) := n$ είναι **ο βαθμός** τού πολυωνύμου $f(\mathsf{X})$ και ότι ο $\mathrm{LC}(f(\mathsf{X})) := a_n$ είναι ο **επικεφαλής συντελεστής** (ή ο **μεγιστοβάθμιος συντελεστής**) τού πολυωνύμου $f(\mathsf{X})$. Όταν $\mathrm{LC}(f(\mathsf{X})) = 1_R$, τότε το $f(\mathsf{X})$ καλείται **μονικό πολυώνυμο**. Στην περίπτωση όπου το $f(\mathsf{X}) = 0_{R[\mathsf{X}]}$ είναι το **μηδενικό πολυώνυμο**, θέτουμε εξ ορισμού $\deg(f(\mathsf{X})) := -\infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση:

$$-\infty < n,\ \ \forall n \in \mathbb{N}_0.$$

Κατ' αυτόν τον τρόπο ο βαθμός των πολυωνύμων μπορεί να εκληφθεί ως μια απεικόνιση

$$\deg : R[\mathsf{X}] \longrightarrow \mathbb{N}_0 \cup \{-\infty\}\,.$$

Ένα πολυώνυμο $f(\mathsf{X}) \in R[\mathsf{X}]$ λέγεται **σταθερό πολυώνυμο** όταν $\deg(f(\mathsf{X})) \leq 0$.

5.1.5 Λήμμα. *Έστω R ένας* 1*-δακτύλιος. Για οιαδήποτε πολυώνυμα*

$$f(\mathsf{X}), g(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$$

ισχύουν τα εξής:

(i) $\deg(f(\mathsf{X}) + g(\mathsf{X})) \leq \max\{\deg(f(\mathsf{X})), \deg(g(\mathsf{X}))\}$.

(ii) $\deg(f(\mathsf{X}) \cdot g(\mathsf{X})) \leq \deg(f(\mathsf{X})) + \deg(g(\mathsf{X}))$.

(iii) *Εάν* $\deg(f(\mathsf{X})) \neq \deg(g(\mathsf{X}))$, *τότε*

$$\deg(f(\mathsf{X}) + g(\mathsf{X})) = \max\{\deg(f(\mathsf{X})), \deg(g(\mathsf{X}))\}.$$

(iv) *Εάν* $\mathrm{LC}(f(\mathsf{X}))\cdot \mathrm{LC}(g(\mathsf{X})) \neq 0$, *τότε*

$$\deg(f(\mathsf{X}) \cdot g(\mathsf{X})) = \deg(f(\mathsf{X})) + \deg(g(\mathsf{X})).$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι

$$f(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]\ ,\ a_n \neq 0, \quad g(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}],\ \ b_m \neq 0,$$

και ας ορίσουμε $a_i := 0$ για κάθε $i > n$ και $b_j := 0$ για κάθε $j > m$.

(i) Χωρίς βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n \geq m$. Τότε

$$f(\mathsf{X}) + g(\mathsf{X}) = \sum_{i=0}^{n} (a_i + b_i)\, \mathsf{X}^i, \tag{5.2}$$

οπότε $\deg\left(f(\mathsf{X}) + g(\mathsf{X})\right) \leq n = \max\{\deg\left(f(\mathsf{X})\right), \deg(g(\mathsf{X}))\}$.

(ii) Βάσει τής (5.1) το γινόμενο των δύο πολυωνύμων μπορεί να γραφεί ως

$$f(\mathsf{X}) \cdot g(\mathsf{X}) = \sum_{k \geq 0} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) \mathsf{X}^k,$$

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n+m \\ \sum\limits_{i=0}^{n} a_i b_{k-i} + \sum\limits_{i=n+1}^{k} a_i b_{k-i} = 0, & \text{όταν } k \geq n+m+1 \end{cases} \tag{5.3}$$

Κατά συνέπειαν, $\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) \leq n + m = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X}))$.

(iii) Χωρίς βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n > m$. Τότε έχουμε $a_n + b_n = a_n \neq 0$ και από την (5.2) έπεται ότι

$$n = \max\{\deg\left(f(\mathsf{X})\right), \deg(g(\mathsf{X}))\}.$$

(iv) Επειδή $a_n b_m = \mathrm{LC}(f(\mathsf{X}))\cdot \mathrm{LC}(g(\mathsf{X})) \neq 0$, από την ισότητα (5.3) λαμβάνουμε $\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X}))$. □

5.1.6 Παραδείγματα. Σημειωτέον ότι οι ανωτέρω ανισοϊσότητες μπορούν πράγματι να ισχύουν και ως αυστηρές ανισότητες.

(i) Εάν $f(\mathsf{X}) = 2\mathsf{X} + 1$, $g(\mathsf{X}) = -2\mathsf{X} + 1 \in \mathbb{Z}\,[\mathsf{X}]$, τότε

$$0 = \deg\left(f(\mathsf{X}) + g(\mathsf{X})\right) < \max\{\deg\left(f(\mathsf{X})\right), \deg(g(\mathsf{X}))\} = 1.$$

(ii) Εάν $f(\mathsf{X}) = [2]_4\, \mathsf{X} + [1]_4$, $g(\mathsf{X}) = [-2]_4\, \mathsf{X} + [1]_4 \in \mathbb{Z}_4\,[\mathsf{X}]$, τότε

$$f(\mathsf{X}) \cdot g(\mathsf{X}) = [-4]_4\, \mathsf{X}^2 + [1]_4 = [1]_4\,,$$

που σημαίνει ότι

$$0 = \deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) < \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X})) = 2.$$

5.1.7 Πρόταση. *Έστω R μια ακεραία περιοχή. Τότε ισχύουν τα εξής*:

(i) *Ο δακτύλιος $R[\mathsf{X}]$ είναι ακεραία περιοχή.*

(ii) *Για οιαδήποτε πολυώνυμα $f(\mathsf{X}), g(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ έχουμε*

$$\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X})).$$

(iii) $R^\times = \left(R\left[\mathsf{X}\right]\right)^\times$*, ήτοι τα αντιστρέψιμα στοιχεία τού $R\left[\mathsf{X}\right]$ είναι ακριβώς τα αντιστρέψιμα στοιχεία τού R.*

ΑΠΟΔΕΙΞΗ. (i) Ο $R[\mathsf{X}]$ είναι μη τετριμμένος, μεταθετικός δακτύλιος με μοναδιαίο του στοιχείο το 1_R. Εάν $f(\mathsf{X}), g(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$, τότε $\mathrm{LC}(f(\mathsf{X}))\cdot \mathrm{LC}(g(\mathsf{X})) \neq 0$, διότι ο R δεν διαθέτει μηδενοδιαιρέτες. Συνεπώς, $f(\mathsf{X}) \cdot g(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$, οπότε ούτε ο $R[\mathsf{X}]$ μπορεί να έχει μηδενοδιαιρέτες.

(ii) Τούτο έπεται άμεσα από το (i) και το 5.1.5 (iii).

(iii) Εάν το $f(\mathsf{X})$ είναι ένα αντιστρέψιμο στοιχείο τού $R[\mathsf{X}]$, τότε υπάρχει ένα πολυώνυμο $g(\mathsf{X}) \in R[\mathsf{X}]$, τέτοιο ώστε να ισχύει $f(\mathsf{X})g(\mathsf{X}) = 1_{R[\mathsf{X}]}$. Τα $f(\mathsf{X}), g(\mathsf{X})$ είναι μη μηδενικά, καθότι $1_{R[\mathsf{X}]} = 1_R \neq 0_R = 0_{R[\mathsf{X}]}$. Από το (ii) συνάγουμε ότι

$$0 = \deg\left(f(\mathsf{X})g(\mathsf{X})\right) = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X})) \Longrightarrow \deg\left(f(\mathsf{X})\right) = \deg(g(\mathsf{X})) = 0,$$

οπότε τα $f(\mathsf{X}), g(\mathsf{X})$ είναι κατ' ανάγκην αντιστρέψιμα στοιχεία τού R. □

5.1.8 Πόρισμα. *Έστω K ένα σώμα. Εάν $f(\mathsf{X}), g(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_K\}$, τότε*

$$\deg\left(f(\mathsf{X}) \cdot g(\mathsf{X})\right) = \deg\left(f(\mathsf{X})\right) + \deg(g(\mathsf{X})).$$

Επιπροσθέτως,

$$\left(K\left[\mathsf{X}\right]\right)^\times = K^\times = K \setminus \{0_K\} = \left\{\, f\left(\mathsf{X}\right) \in K[\mathsf{X}] \mid \deg(f(\mathsf{X})) = 0 \right\}.$$

5.1.9 Σημείωση. Στο σχολείο είθισται να αντιμετωπίζουμε τα πολυώνυμα ως συνήθεις «απεικονίσεις» (επειδή εκεί γίνεται κυρίως χρήση των δακτυλίων $\mathbb{Q}$ και $\mathbb{R}$). Ωστόσο, όταν κανείς θεωρεί *τυχόντες* 1-δακτυλίους R, πρέπει να γνωρίζει ότι κάτι τέτοιο *δεν* αληθεύει εν γένει. Εάν

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

τότε ορίζεται η **πολυωνυμική απεικόνιση (αποτιμήσεως)**

$$\widetilde{f} : R \longrightarrow R, \quad s \longmapsto \widetilde{f}(s) := f(s) := \sum_{i=1}^{n} a_i s^i,$$

χωρίς όμως η

$$R[\mathsf{X}] \longrightarrow \mathrm{A\Pi}(R,R), \quad f \longmapsto \widetilde{f},$$

να αποτελεί κατ' ανάγκην έναν μονομορφισμό. Επί παραδείγματι, εάν $R = \mathbb{Z}_3$ και

$$f(\mathsf{X}) = \mathsf{X} + \mathsf{X}^3, \quad g(\mathsf{X}) = [2]_3\,\mathsf{X},$$

τότε τα $f(\mathsf{X})$ και $g(\mathsf{X})$ -ως πολυώνυμα- είναι διαφορετικά (πρβλ. 5.1.3), ενώ

$$\begin{aligned}\widetilde{f}([0]_3) &= [0]_3 = \widetilde{g}([0]_3),\\ \widetilde{f}([1]_3) &= [2]_3 = \widetilde{g}([1]_3),\\ \widetilde{f}([2]_3) &= [1]_3 = \widetilde{g}([2]_3),\end{aligned}$$

πράγμα που σημαίνει ότι $\widetilde{f} = \widetilde{g}$. (Μια ικανή συνθήκη για να είναι ο ως άνω ομομορφισμός δακτυλίων μονομορφισμός δίνεται στο πόρισμα 5.3.8.)

5.2 ΔΙΑΙΡΕΤΟΤΗΤΑ ΠΟΛΥΩΝΥΜΩΝ

5.2.1 Ορισμός. Έστω R ένας μεταθετικός 1-δακτύλιος. Λέμε ότι ένα πολυώνυμο $g(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ **διαιρεί** ένα πολυώνυμο $f(\mathsf{X}) \in R[\mathsf{X}]$ (ή ότι το $f(\mathsf{X})$ είναι **πολλαπλάσιο** τού $g(\mathsf{X})$) στον $R[\mathsf{X}]$ (σημειώνοντας $g(\mathsf{X}) \mid f(\mathsf{X})$) όταν υπάρχει κάποιο $h(\mathsf{X}) \in R[\mathsf{X}]$, τέτοιο ώστε

$$f(\mathsf{X}) = g(\mathsf{X})h(\mathsf{X}).$$

5.2.2 Πρόταση. *Έστω R ένας μεταθετικός 1-δακτύλιος. Υποθέτουμε ότι $f(\mathsf{X})$, $g(\mathsf{X})$ και $h(\mathsf{X})$ είναι πολυώνυμα ανήκοντα στον $R[\mathsf{X}]$. Τότε ισχύουν τα ακόλουθα*:

(i) *Εάν $g(\mathsf{X}) \mid f(\mathsf{X})$ και $g(\mathsf{X}) \mid h(\mathsf{X})$, τότε*

$$g(\mathsf{X}) \mid b(\mathsf{X})f(\mathsf{X}) + c(\mathsf{X})h(\mathsf{X})$$

για οιαδήποτε $b(\mathsf{X}), c(\mathsf{X}) \in R[\mathsf{X}]$.

(ii) *Εάν $g(\mathsf{X}) \mid f(\mathsf{X})$ και $h(\mathsf{X}) \mid g(\mathsf{X})$, τότε $h(\mathsf{X}) \mid f(\mathsf{X})$.*

(iii) *$a \mid f(\mathsf{X})$ για κάθε $a \in R^\times$.*

(iv) *Εάν $g(\mathsf{X}) \mid f(\mathsf{X})$, όπου $f(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$, και ο R είναι μια ακεραία περιοχή, τότε*

$$\deg(g(\mathsf{X})) \leq \deg(f(\mathsf{X})).$$

(v) *Εάν $g(\mathsf{X}) \mid f(\mathsf{X})$ και $f(\mathsf{X}) \mid g(\mathsf{X})$, και ο R είναι μια ακεραία περιοχή, τότε*

$$f(\mathsf{X}) = a \cdot g(\mathsf{X}),$$

για κάποιο $a \in R^\times$.

ΑΠΟΔΕΙΞΗ. Αφήνεται ως άσκηση. □

5.2.3 Θεώρημα. (Γενικευμένος Αλγόριθμος Διαιρέσεως) *Δοθέντων δυο πολυωνύμων*

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

με τους συντελεστές τους ειλημμένους από έναν μεταθετικό 1*-δακτύλιο* R*, όπου* $\mathrm{LC}(g) = b_m$*, υπάρχει ένα ζεύγος πολυωνύμων* $q(\mathsf{X})$ *και* $r(\mathsf{X}) \in R[\mathsf{X}]$*, καθώς και ένας* $k \in \mathbb{N}_0$*, ούτως ώστε να ισχύει*

$$(\mathrm{LC}(g))^k \cdot f(\mathsf{X}) = q(\mathsf{X}) \cdot g\,(\mathsf{X}) + r(\mathsf{X}),\ \ \deg\left(r(\mathsf{X})\right) < \deg\left(g\,(\mathsf{X})\right) \tag{5.4}$$

ΑΠΟΔΕΙΞΗ. Εάν ισχύει $\deg(f(\mathsf{X})) < \deg(g(\mathsf{X}))$, τότε θέτοντας $k = 0$, $q(\mathsf{X}) = 0_{R[\mathsf{X}]}$ και $r(\mathsf{X}) = f(\mathsf{X})$, η (5.4) επαληθεύεται. Από εδώ λοιπόν και στο εξής μπορούμε να υποθέσουμε ότι

$$n = \deg(f(\mathsf{X})) \geq \deg(g(\mathsf{X})) = m,\ \ n \geq 0.$$

Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον n. Εάν $n = 0$, τότε $m = 0$ και

$$f(\mathsf{X}) = a_0,\ \ g(\mathsf{X}) = b_0,$$

οπότε αρκεί να θέσουμε $q(\mathsf{X}) = a_0$, $r(\mathsf{X}) = 0_{R[\mathsf{X}]}$ και $k = 1$ για να λάβουμε την (5.4). Εν συνεχεία, υποθέτουμε ότι $n > 0$ και ότι *για κάθε πολυώνυμο* $h(\mathsf{X}) \in R[\mathsf{X}]$ *με* $\deg(h(\mathsf{X})) < n$ υπάρχει ένα ζεύγος πολυωνύμων $q'(\mathsf{X})$ και $r'(\mathsf{X}) \in R[\mathsf{X}]$, καθώς και ένας $k' \in \mathbb{N}_0$, ούτως ώστε να ισχύει

$$(\mathrm{LC}(g))^{k'} \cdot h(\mathsf{X}) = q'(\mathsf{X}) \cdot g\,(\mathsf{X}) + r'(\mathsf{X}),\ \ \deg\left(r'(\mathsf{X})\right) < \deg\left(g\,(\mathsf{X})\right). \tag{5.5}$$

Ορίζουμε ως $h(\mathsf{X})$ το[1]

$$h(\mathsf{X}) := (\mathrm{LC}(g))^k \cdot f(\mathsf{X}) - a_n \cdot \mathsf{X}^{n-m} \cdot g(\mathsf{X}) \in R[\mathsf{X}].$$

Εάν $h(\mathsf{X}) = 0_{R[\mathsf{X}]}$, τότε λαμβάνουμε εκ νέου την (5.4) θέτοντας

$$k = 1,\ \ q(\mathsf{X}) = a_n \cdot \mathsf{X}^{n-m},\ \ r(\mathsf{X}) = 0_{R[\mathsf{X}]}.$$

Ειδάλλως, εκμεταλλευόμενοι την επαγωγική μας υπόθεση (5.5) θέτουμε

$$r(\mathsf{X}) = r'(\mathsf{X}),\ \ q(\mathsf{X}) = q'(\mathsf{X}) + (\mathrm{LC}(g))^{k'} \cdot a_n \cdot \mathsf{X}^{n-m},\ \ k = k' + 1,$$

[1] Ο συντελεστής τού προκειμένου $h(\mathsf{X})$ είναι ο $b_m a_n - a_n b_m = 0_R$, οπότε $\deg(h(\mathsf{X})) < n$.

καταλήγοντας στην ισότητα

$$\begin{aligned}(\mathrm{LC}(g))^k \cdot f(\mathsf{X}) &= (\mathrm{LC}(g))^{k'} \cdot h(\mathsf{X}) + (\mathrm{LC}(g))^{k'} \cdot a_n \cdot \mathsf{X}^{n-m} \cdot g(\mathsf{X}) \\ &= q(\mathsf{X}) \cdot g(\mathsf{X}) + r(\mathsf{X}),\end{aligned}$$

όπου $\deg(r(\mathsf{X})) = \deg(r'(\mathsf{X})) < \deg(g(\mathsf{X}))$. □

5.2.4 Πόρισμα. (Αλγόριθμος Διαιρέσεως) *Δοθέντων δυο πολυωνύμων*

$$f(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]\,, \quad g(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}]$$

*με τους συντελεστές τους από μια ακεραία περιοχή R, όπου $\mathrm{LC}(g) = b_m \in R^\times$, υπάρχει ένα ζεύγος **μονοσημάντως ορισμένων** πολυωνύμων $q(\mathsf{X})$ και $r(\mathsf{X}) \in R[\mathsf{X}]$, τέτοιων ώστε να ισχύει*

$$f(\mathsf{X}) = q(\mathsf{X}) \cdot g(\mathsf{X}) + r(\mathsf{X}), \quad \deg(r(\mathsf{X})) < \deg(g(\mathsf{X}))\,. \tag{5.6}$$

ΑΠΟΔΕΙΞΗ. Κατά το θεώρημα 5.2.3 υπάρχει ένα ζεύγος πολυωνύμων $q_*(\mathsf{X})$ και $r_*(\mathsf{X}) \in R[\mathsf{X}]$, καθώς και ένας $k \in \mathbb{N}_0$, ούτως ώστε να ισχύει

$$(\mathrm{LC}(g))^k \cdot f(\mathsf{X}) = q_*(\mathsf{X}) \cdot g(\mathsf{X}) + r_*(\mathsf{X}), \quad \deg(r_*(\mathsf{X})) < \deg(g(\mathsf{X}))\,.$$

Επειδή $\mathrm{LC}(g) \in R^\times$ (οπότε και $(\mathrm{LC}(g))^k \in R^\times$), η (5.6) επαληθεύεται θέτοντας

$$q(\mathsf{X}) := \frac{q_*(\mathsf{X})}{(\mathrm{LC}(g))^k}, \quad r(\mathsf{X}) := \frac{r_*(\mathsf{X})}{(\mathrm{LC}(g))^k}.$$

Αρκεί λοιπόν να αποδειχθεί και το *μονοσήμαντο* μιας τέτοιας εκφράσεως. Εάν πλην των $q(\mathsf{X})$, $r(\mathsf{X})$ υπάρχουν και άλλα δύο πολυώνυμα $q'(\mathsf{X})$ και $r'(\mathsf{X})$, τα οποία πλήρουν τις

$$\begin{gathered}f(\mathsf{X}) = q(\mathsf{X}) \cdot g(\mathsf{X}) + r(\mathsf{X}) = q'(\mathsf{X}) \cdot g(\mathsf{X}) + r'(\mathsf{X}), \\ \deg(r(\mathsf{X})) \le \deg(r'(\mathsf{X})) < \deg(g(\mathsf{X}))\,,\end{gathered}$$

τότε

$$(q(\mathsf{X}) - q'(\mathsf{X})) \cdot g(\mathsf{X}) = r'(\mathsf{X}) - r(\mathsf{X}). \tag{5.7}$$

Υποθέτοντας ότι $r'(\mathsf{X}) \neq r(\mathsf{X})$, η (5.7) μας πληροφορεί ότι $q(\mathsf{X}) \neq q'(\mathsf{X})$, οπότε με τη βοήθεια τής προτάσεως 5.1.7 (ii) συμπεραίνουμε ότι

$$\deg(r'(\mathsf{X})) \ge \deg(r'(\mathsf{X}) - r(\mathsf{X})) = \deg(q(\mathsf{X}) - q'(\mathsf{X})) + \deg(g(\mathsf{X})) \ge \deg(g(\mathsf{X}))\,,$$

πράγμα που αντίκειται προς την προϋποτεθείσα ανίσωση $\deg(r'(\mathsf{X})) < \deg(g(\mathsf{X}))$. Συνεπώς,

$$r'(\mathsf{X}) = r(\mathsf{X}) \underset{(5.7)}{\Longrightarrow} (q(\mathsf{X}) - q'(\mathsf{X}))\, g(\mathsf{X}) = 0_{R[\mathsf{X}]} \Rightarrow q(\mathsf{X}) = q'(\mathsf{X}),$$

όπου η τελευταία συνεπαγωγή έπεται από το γεγονός ότι $g(\mathsf{X}) \neq 0_{R[\mathsf{X}]}$ και από το ότι ο δακτύλιος $R[\mathsf{X}]$ είναι μια ακεραία περιοχή (βλ. 5.1.7 (i)). □

5.2.5 Παράδειγμα. Εάν

$$f(\mathsf{X}) = \mathsf{X}^7 - 2\mathsf{X}^6 + \mathsf{X}^4 - \mathsf{X}^3 + 2\mathsf{X}^2 - 1, \quad g(\mathsf{X}) = \mathsf{X}^6 - 2\mathsf{X}^5 + 2\mathsf{X}^2 - 1 \in \mathbb{Q}[\mathsf{X}],$$

τότε

$$f(\mathsf{X}) = \mathsf{X} \cdot g(\mathsf{X}) + \left(\mathsf{X}^4 - 3\mathsf{X}^3 + 2\mathsf{X}^2 + \mathsf{X} - 1\right).$$

5.2.6 Ορισμός. Το πολυώνυμο $q(\mathsf{X})$ στον τύπο (5.6) ονομάζεται **πηλίκο** και το $r(\mathsf{X})$ **υπόλοιπο** τής διαιρέσεως τού $f(\mathsf{X})$ διά τού $g(\mathsf{X})$.

5.2.7 Ορισμός. Έστω R μια ακεραία περιοχή. Ένα πολυώνυμο $d(\mathsf{X}) \in R[\mathsf{X}]$ ονομάζεται **μέγιστος κοινός διαιρέτης** των $f(\mathsf{X}), g(\mathsf{X}) \in R[\mathsf{X}]$, συμβολιζόμενος ως μκδ$(f(\mathsf{X}), g(\mathsf{X}))$, όταν έχει τις ακόλουθες ιδιότητες:
(i) $d(\mathsf{X}) \mid f(\mathsf{X})$ και $d(\mathsf{X}) \mid g(\mathsf{X})$,
(ii) εάν για κάποιο $h(\mathsf{X}) \in R[\mathsf{X}]$ ισχύει $h(\mathsf{X}) \mid f(\mathsf{X})$ και $h(\mathsf{X}) \mid g(\mathsf{X})$, τότε $h(\mathsf{X}) \mid d(\mathsf{X})$.

Βάσει τού ανωτέρου ορισμού λαμβάνουμε ιδιαιτέρως

$$\text{μκδ}(0_{R[\mathsf{X}]}, 0_{R[\mathsf{X}]}) = 0_{R[\mathsf{X}]}, \ \ \text{μκδ}(f(\mathsf{X}), 0_{R[\mathsf{X}]}) = f(\mathsf{X}), \ \forall f(\mathsf{X}) \in R[\mathsf{X}].$$

Εξάλλου, εάν το $d(\mathsf{X}) \in R[\mathsf{X}]$ είναι μέγιστος κοινός διαιρέτης των πολυωνύμων $f(\mathsf{X}), g(\mathsf{X}) \in R[\mathsf{X}]$, τότε και ο $a \cdot d(\mathsf{X})$ θα είναι μέγιστος κοινός διαιρέτης τους, για κάθε $a \in R^\times$, διότι *πρώτον*: από τις $d(\mathsf{X}) \mid f(\mathsf{X})$ και $d(\mathsf{X}) \mid g(\mathsf{X})$ λαμβάνουμε

$$f(\mathsf{X}) = d(\mathsf{X}) f_*(\mathsf{X}), \ \ g(\mathsf{X}) = d(\mathsf{X}) g_*(\mathsf{X}),$$

για κάποια $f_*(\mathsf{X}), g_*(\mathsf{X}) \in R[\mathsf{X}]$, οπότε

$$\left.\begin{aligned} f(\mathsf{X}) &= a \cdot d \cdot a^{-1} f_*(\mathsf{X}) \\ g(\mathsf{X}) &= a \cdot d \cdot a^{-1} g_*(\mathsf{X}) \end{aligned}\right\} \Longrightarrow a \cdot d(\mathsf{X}) \mid f(\mathsf{X}) \text{ και } a \cdot d(\mathsf{X}) \mid g(\mathsf{X}),$$

και *δεύτερον*: εάν για κάποιο $h(\mathsf{X}) \in R[\mathsf{X}]$ ισχύει $h(\mathsf{X}) \mid f(\mathsf{X})$ και $h(\mathsf{X}) \mid g(\mathsf{X})$, τότε

$$h(\mathsf{X}) \mid d(\mathsf{X}) \Longrightarrow h(\mathsf{X}) \mid a \cdot d(\mathsf{X}).$$

Επομένως ο μέγιστος κοινός διαιρέτης των $f(\mathsf{X}), g(\mathsf{X}) \in R[\mathsf{X}]$ ορίζεται με ακρίβεια, εξαιρουμένου τού πολλαπλασιασμού του με κάποιο αντιστρέψιμο στοιχείο τής ακεραίας περιοχής R.

5.2.8 Σημείωση. Πολλοί συγγραφείς ορίζουν ως «*τον*» *μέγιστο κοινό διαιρέτη* δύο πολυωνύμων εκείνον εκ των (ως άνω ορισθέντων) μεγίστων κοινών διαιρετών ο οποίος είναι ένα μονικό πολυώνυμο, ήτοι εκείνον που έχει το μοναδιαίο στοιχείο τής R ως τον επικεφαλής συντελεστή του. Στην περίπτωση αυτή ο μέγιστος κοινός διαιρέτης δύο πολυωνύμων είναι *αυστηρώς μονοσημάντως ορισμένος*.

5.2.9 Παρατήρηση. Δοθέντων $f(\mathsf{X}) \in R[\mathsf{X}]$ και $g(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ μπορούμε να προσδιορίσουμε (έναν) μέγιστο κοινό διαιρέτη τους μέσω επαλλήλων εκτελέσεων τού αλγορίθμου τής διαιρέσεως πολυωνύμων. Πράγματι· υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $q_0(\mathsf{X}), r_0(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$f(\mathsf{X}) = q_0(\mathsf{X})g(\mathsf{X}) + r_0(\mathsf{X}), \;\; \deg(r_0(\mathsf{X})) < \deg(g(\mathsf{X})).$$

Εάν $r_0(\mathsf{X}) = 0_{R[\mathsf{X}]}$, τότε προφανώς $\mu\kappa\delta(f(\mathsf{X}), g(\mathsf{X})) = g(\mathsf{X})$. Ειδάλλως, επαναμβάνοντας διαδοχικώς την ίδια διαδικασία, προσδιορίζουμε μονοσημάντως ορισμένα πολυώνυμα $r_0(\mathsf{X}), r_1(\mathsf{X}), r_2(\mathsf{X}), \ldots$ και $q_0(\mathsf{X}), q_1(\mathsf{X}), q_2(\mathsf{X}), \ldots$ με

$$\left|\begin{array}{ll} f(\mathsf{X}) = q_0(\mathsf{X})g(\mathsf{X}) + r_0(\mathsf{X}), & \deg(r_0(\mathsf{X})) < \deg(g(\mathsf{X})), \\ g(\mathsf{X}) = q_1(\mathsf{X})\, r_0(\mathsf{X}) + r_1(\mathsf{X}), & \deg(r_1(\mathsf{X})) < \deg(r_0(\mathsf{X})), \\ r_0(\mathsf{X}) = q_2(\mathsf{X})\, r_1(\mathsf{X}) + r_2(\mathsf{X}), & \deg(r_2(\mathsf{X})) < \deg(r_1(\mathsf{X})), \\ \vdots & \vdots \\ r_{n-2}(\mathsf{X}) = q_n(\mathsf{X})\, r_{n-1}(\mathsf{X}) + r_n(\mathsf{X}), & \deg(r_n(\mathsf{X})) < \deg(r_{n-1}(\mathsf{X})), \\ r_{n-1}(\mathsf{X}) = q_{n+1}(\mathsf{X})\, r_n(\mathsf{X}), & \end{array}\right. \tag{5.8}$$

όπου για κάποιον δείκτη n έχουμε κατ' ανάγκην $r_{n+1}(\mathsf{X}) = 0_{R[\mathsf{X}]}$, διότι οι βαθμοί των πολυωνύμων $r_0(\mathsf{X}), r_1(\mathsf{X}), r_2(\mathsf{X}), \ldots$ σχηματίζουν μια φθίνουσα ακολουθία εντός τού $\mathbb{N}_0 \cup \{-\infty\}$. Κατά συνέπειαν[2],

$$\boxed{\mu\kappa\delta(f(\mathsf{X}), g(\mathsf{X})) = r_n(\mathsf{X})}$$

5.2.10 Παράδειγμα. Εάν

$$f(\mathsf{X}) = \mathsf{X}^7 - 2\mathsf{X}^6 + \mathsf{X}^4 - \mathsf{X}^3 + 2\mathsf{X}^2 - 1, \;\; g(\mathsf{X}) = \mathsf{X}^6 - 2\mathsf{X}^5 + 2\mathsf{X}^2 - 1 \in \mathbb{Q}[\mathsf{X}],$$

(όπως στο παράδειγμα 5.2.5) τότε $f(\mathsf{X}) = \mathsf{X} \cdot g(\mathsf{X}) + r_0(\mathsf{X})$, όπου

$$r_0(\mathsf{X}) = \mathsf{X}^4 - 3\mathsf{X}^3 + 2\mathsf{X}^2 + \mathsf{X} - 1.$$

Διαιρώντας τό $g(\mathsf{X})$ διά τού $r_0(\mathsf{X})$, βρίσκουμε υπόλοιπο $r_1(\mathsf{X}) = 0_{\mathbb{Q}[\mathsf{X}]}$, καθόσον

$$g(\mathsf{X}) = q_1(\mathsf{X})\, r_0(\mathsf{X}), \quad q_1(\mathsf{X}) = \mathsf{X}^2 + \mathsf{X} + 1.$$

[2]Εάν θέλουμε να επιλέξουμε «τον» μονικό εκπρόσωπο ως μκδ (βλ. 5.2.8), τότε αντικαθιστούμε το $r_n(t)$ με το $(\mathrm{LC}(r_n(t)))^{-1} \cdot r_n(t)$.

Άρα

$$\mu\kappa\delta(f(\mathsf{X}), g(\mathsf{X})) = \mathsf{X}^4 - 3\mathsf{X}^3 + 2\mathsf{X}^2 + \mathsf{X} - 1.$$

5.2.11 Ορισμός. Έστω R μια ακεραία περιοχή. Δοθέντων $n \geq 2$ πολυωνύμων

$$f_1(\mathsf{X}), f_2(\mathsf{X}), \ldots, f_n(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$$

ορίζουμε τον **μέγιστο κοινό διαιρέτη** τους (και πάλι ακριβώς, εξαιρουμένου τού πολλαπλασιασμού του με κάποιο αντιστρέψιμο στοιχείο τής R) μέσω επαγωγής:

$$\mu\kappa\delta(f_1(\mathsf{X}), f_2(\mathsf{X}), \ldots, f_n(\mathsf{X})) := \mu\kappa\delta(\mu\kappa\delta(f_1(\mathsf{X}), \ldots, f_{n-1}(\mathsf{X})), f_n(\mathsf{X})) \qquad (5.9)$$

5.2.12 Θεώρημα. *Έστω ότι η R είναι μια ακεραία περιοχή και ότι τα*

$$f_1(\mathsf{X}), f_2(\mathsf{X}), \ldots, f_n(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$$

($n \geq 2$) είναι δοθέντα πολυώνυμα με μέγιστο κοινό διαιρέτη τον $d(\mathsf{X})$. Τότε υπάρχουν πολυώνυμα

$$g_1(\mathsf{X}), g_2(\mathsf{X}), \ldots, g_n(\mathsf{X}) \in R[\mathsf{X}],$$

ούτως ώστε να ισχύει η ισότητα

$$d(\mathsf{X}) = \sum_{j=1}^{n} f_i(\mathsf{X}) g_i(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. Λόγω τού επαγωγικού ορισμού (5.9) τού μκδ πολυωνύμων περισσοτέρων των δύο, αρκεί το θεώρημα να αποδειχθεί μόνον όταν $n = 2$. Σε αυτήν την περίπτωση θέτουμε $f_1 = f$ και $f_2 = g$ και θεωρούμε τις ισότητες (5.8). Από την προτελευταία ισότητα λαμβάνουμε

$$r_n(\mathsf{X}) = r_{n-2}(\mathsf{X}) - q_n(\mathsf{X})\, r_{n-1}(\mathsf{X}).$$

Εν συνεχεία, αντικαθιστώντας τό $r_{n-1}(\mathsf{X})$ με ό,τι βρίσκουμε μέσω τής αμέσως προγούμενης ισότητας κ.ο.κ. φθάνουμε τελικώς σε μία έκφραση τού

$$r_n(\mathsf{X}) = \mu\kappa\delta(f(\mathsf{X}), g(\mathsf{X}))$$

η οποία είναι τής μορφής που επιθυμούμε. □

5.2.13 Ορισμός. Έστω ότι ο R είναι μια ακεραία περιοχή και ότι

$$f_1(\mathsf{X}), f_2(\mathsf{X}), \ldots, f_n(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}.$$

Τότε λέμε ότι τα πολυώνυμα αυτά είναι **πρώτα μεταξύ τους** όταν

$$\mu\kappa\delta(f_1(\mathsf{X}), f_2(\mathsf{X}), \ldots, f_n(\mathsf{X})) \in R^{\times}.$$

5.2.14 Πόρισμα. *Έστω ότι η R είναι μια ακεραία περιοχή και*

$$f_1(\mathsf{X}), f_2(\mathsf{X}), \dots, f_n(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$$

$(n \geq 2)$ *πολυώνυμα τα οποία είναι πρώτα μεταξύ τους. Τότε υπάρχουν πολυώνυμα*

$$g_1(\mathsf{X}), g_2(\mathsf{X}), \dots, g_n(\mathsf{X}) \in R[\mathsf{X}],$$

ούτως ώστε να ισχύει η ισότητα

$$\sum_{j=1}^{n} f_i(\mathsf{X}) g_i(\mathsf{X}) = 1.$$

5.2.15 Σημείωση. Κατά τρόπο ανάλογο εκείνου βάσει τού οποίου ορίσαμε τον μκδ πολυωνύμων (βλ. 5.2.7 και 5.2.13) ορίζεται και το εκπ (= ελάχιστο κοινό πολλαπλάσιο) πολυωνύμων (με συντελεστές ειλημμένους από μια ακεραία περιοχή).

5.3 ΘΕΣΕΙΣ ΜΗΔΕΝΙΣΜΟΥ ΠΟΛΥΩΝΥΜΩΝ

5.3.1 Ορισμός. Έστω S ένας μεταθετικός 1-δακτύλιος και έστω R ένας υποδακτύλιος τού S. Υποθέτουμε ότι το

$$f(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i$$

είναι ένα πολυώνυμο ανήκον στον $R[\mathsf{X}]$.

(i) Ένα στοιχείο $s \in S$ ονομάζεται **θέση μηδενισμού**[3] (ή **σημείο μηδενισμού**) τού πολυωνύμου $f(\mathsf{X})$ **εντός τού** S όταν $\widetilde{f}(s) =: f(s) = 0_S$, δηλαδή όταν η τιμή τού $f(\mathsf{X})$ για $\mathsf{X} = s$ είναι το μηδενικό στοιχείο τού S.

(ii) Εάν $R = S$, $s \in S$ και $f(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ με $\widetilde{f}(s) =: f(s) = 0_S$, και εάν -επιπροσθέτως- έχουμε

$$(\mathsf{X} - s)^m \mid f(\mathsf{X}), \quad \text{και} \quad (\mathsf{X} - s)^{m+1} \nmid f(\mathsf{X})$$

για κάποιον[4] $m \in \mathbb{N}$, τότε λέμε ότι το s είναι μια θέση μηδενισμού τού $f(\mathsf{X})$ *με πλήθος πολλαπλών εμφανίσεων* ή -απλούστερα- **με πολλαπλότητα** ίση με

$$\mathrm{mult}\,(f, s) := m.$$

[3] Εδώ χρησιμοποιούμε τον όρο *θέση μηδενισμού* ακολουθώντας τή γερμανική ορολογία, η οποία, εν προκειμένω, είναι περισσότερο ακριβής απ' ό,τι η αγγλική· ο διαχωρισμός τού όρου Nullstelle από τον όρο Wurzel (αγγλ. *root*, ελλ. *ρίζα*) είναι επιβεβλημένη, καθότι ένα μιγαδικό πολυώνυμο $f(\mathsf{X}) \in \mathbb{C}[\mathsf{X}]$ μπορεί να μηδενίζεται όταν $\mathsf{X} = a \in \mathbb{C}$, χωρίς ωστόσο το a να προκύπτει από επίλυση τής εξισώσεως $f(\mathsf{X}) = 0$ μέσω αποκλειστικής χρήσεως *ριζικών*. (Από την άλλη όμως μεριά, ονομάζουμε π.χ. τις θέσεις μηδενισμού τής εξισώσεως $z^n = 1$ n-οστές *ρίζες* τής μονάδας.)

[4] Σύμβαση: Ο ορισμός αυτός ενίοτε επεκτείνεται και για $m = 0$. Σε αυτήν την περίπτωση, γράφοντας $\mathrm{mult}(f, s) = 0$ ενοούμε ότι $f(s) \neq 0$.

Το s ονομάζεται, ιδιαιτέρως, **απλή** (και αντιστοίχως, **πολλαπλή**) **θέση μηδενισμού** τού $f(\mathsf{X})$ όταν $\mathrm{mult}(f,s)=1$ (και αντιστοίχως, όταν $\mathrm{mult}(f,s)\geq 2$).

(iii) Εάν $R\subseteq S$ και εάν υπάρχουν στοιχεία $s_1,s_2,\dots,s_k$ τού S, τέτοια ώστε (εντός τού $S[\mathsf{X}]$) να ισχύει η ισότητα

$$f(\mathsf{X})=(\mathsf{X}-s_1)(\mathsf{X}-s_2)\cdots(\mathsf{X}-s_k),$$

τότε λέμε ότι το πολυώνυμο f **διασπάται σε πρωτοβαθμίους παράγοντες υπεράνω τού** S.

5.3.2 Πρόταση. *Έστω R μια ακεραία περιοχή και έστω ότι $a\in R$ και $f(\mathsf{X})\in R[\mathsf{X}]$. Τότε ισχύουν τα εξής*:

(i) *Το υπόλοιπο τής διαιρέσεως τού $f(\mathsf{X})$ με το $\mathsf{X}-a$ ισούται με το $f(a)$.*

(ii) *Το a είναι μια θέση μηδενισμού τού $f(\mathsf{X})$ (εντός τού R) εάν και μόνον εάν*

$$\mathsf{X}-a\mid f(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. (i) Σύμφωνα με τον αλγόριθμο τής διαιρέσεως 5.2.4 υπάρχουν πολυώνυμα $q(\mathsf{X})$ και $r(\mathsf{X})\in R[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$f(\mathsf{X})=(\mathsf{X}-a)q(\mathsf{X})+r(\mathsf{X}),\ \ \deg(r(\mathsf{X}))<\deg(\mathsf{X}-a)=1.$$

Επομένως, $r(\mathsf{X})=c\in R$, οπότε

$$c=f(\mathsf{X})-(\mathsf{X}-a)q(\mathsf{X})\Longrightarrow c=f(a).$$

(ii) Το a είναι μια θέση μηδενισμού τού $f(\mathsf{X})$ (εντός τού R) εάν και μόνον εάν το υπόλοιπο τής διαιρέσεως τού $f(\mathsf{X})$ διά τού $\mathsf{X}-a$ είναι 0, πράγμα που σημαίνει ότι $\mathsf{X}-a\mid f(\mathsf{X})$. □

5.3.3 Πόρισμα. *Έστω R μια ακεραία περιοχή. Εάν οι $a_1,a_2,\dots,a_k$ είναι k σαφώς διακεκριμένες θέσεις μηδενισμού ενός πολυωνύμου $f(\mathsf{X})\in R[\mathsf{X}]$, τότε*

$$(\mathsf{X}-a_1)(\mathsf{X}-a_2)\cdots(\mathsf{X}-a_k)\mid f(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. Όταν $k=1$, αυτό είναι αληθές λόγω τής προτάσεως 5.3.2. Θα εργασθούμε με τη βοήθεια μαθηματικής επαγωγής. Υποθέτουμε ότι ο ισχυρισμός είναι αληθής για $k-1$ θέσεις μηδενισμού, οπότε

$$f(\mathsf{X})=(\mathsf{X}-a_1)(\mathsf{X}-a_2)\cdots(\mathsf{X}-a_{k-1})\,g(\mathsf{X})$$

για κάποιο $g(\mathsf{X})\in R[\mathsf{X}]$. Κατόπιν αποτιμήσεως των δύο μελών τής ανωτέρω ισότητας για $\mathsf{X}=a_k$ λαμβάνουμε

$$0=f(a_k)=(a_k-a_1)(a_k-a_2)\cdots(a_k-a_{k-1})\,g(a_k),$$

απ' όπου προκύπτει ότι $g(a_k) = 0$ (λόγω τής αρχικής υποθέσεώς μας). Άρα το πολυώνυμο $g(\mathsf{X})$ διαιρείται διά τού $\mathsf{X} - a_k$, οπότε ο ισχυρισμός είναι εμφανώς αληθής και για k θέσεις μηδενισμού. □

5.3.4 Πόρισμα. *Κάθε πολυώνυμο $f(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0\}$ με τους συντελεστές του ειλημμένους από μια ακεραία περιοχή R διαθέτει (συνολικώς) το πολύ $\deg(f(\mathsf{X}))$ θέσεις μηδενισμού εντός τής R.*

5.3.5 Παρατήρηση. Όταν ο δακτύλιος R δεν είναι ακεραία περιοχή, το συμπέρασμα τού 5.3.4 δεν είναι εν γένει αληθές. Πράγματι· το πολυώνυμο

$$f(\mathsf{X}) = \mathsf{X}^2 - [1]_8 \in \mathbb{Z}_8[\mathsf{X}]$$

είναι βαθμού 2 και έχει ως θέσεις μηδενισμού του τις $[1]_8, [3]_8, [5]_8, [7]_8$.

5.3.6 Πόρισμα. *Εάν ένα πολυώνυμο $f(\mathsf{X})$, με τους συντελεστές του ειλημμένους από μια ακεραία περιοχή R, διαθέτει εντός τής R θέσεις μηδενισμού, το πλήθος των οποίων υπερβαίνει τον βαθμό του, τότε το $f(\mathsf{X})$ είναι το μηδενικό πολυώνυμο.*

5.3.7 Πόρισμα. *Εάν δυο πολυώνυμα $f(\mathsf{X})$, $g(\mathsf{X})$, με τους συντελεστές τους ειλημμένους από μια ακεραία περιοχή R, λαμβάνουν τις ίδιες τιμές σε k σαφώς διακεκριμένα στοιχεία τής R και*

$$k > \max\{\deg(f(\mathsf{X})), \deg(g(\mathsf{X}))\},$$

τότε έχουμε $f(\mathsf{X}) = g(\mathsf{X})$.

5.3.8 Πόρισμα. *Εάν το υποκείμενο σύνολο μιας ακεραίας περιοχής R είναι ένα απειροσύνολο, τότε η απεικόνιση*

$$R[\mathsf{X}] \longrightarrow \text{ΑΠ}(R, R), \quad f \longmapsto \widetilde{f},$$

(*βλ.* 5.1.9) *αποτελεί έναν μονομορφισμό δακτυλίων.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντα πολυώνυμα $f(\mathsf{X}), g(\mathsf{X}) \in R[\mathsf{X}]$ και τις αντίστοιχες πολυωνυμικές απεικονίσεις αποτιμήσεως $\widetilde{f}$ και $\widetilde{g}$. Εάν ισχύει $\widetilde{f} = \widetilde{g}$, τότε η διαφορά $f(\mathsf{X}) - g(\mathsf{X})$ έχει ως θέσεις μηδενισμού της όλα τα στοιχεία τού (υποκειμένου συνόλου τής) R. Συνεπώς, βάσει τού πορίσματος 5.3.6, έχουμε $f(\mathsf{X}) - g(\mathsf{X}) = 0_{R[\mathsf{X}]}$, ήτοι $f(\mathsf{X}) = g(\mathsf{X})$. □

Στο σημείο αυτό θα στραφούμε σε ορισμένες χαρακτηριστικές ιδιότητες των πολυωνύμων με συντελεστές ειλημμένους από ένα *σώμα*. Η ακόλουθη πρόταση βασίζεται στο πόρισμα 5.3.7.

5.3.9 Πρόταση. (Τύπος παρεμβολής τού Lagrange) *Έστω K ένα σώμα. Υποθέτουμε ότι τα $a_0, a_1, \dots, a_n$ είναι $n+1$ σαφώς διακεκριμένα στοιχεία τού K και ότι τα $c_0, c_1, \dots, c_n$ είναι τυχόντα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία τού K. Τότε υπάρχει ένα μονοσημάντως ορισμένο πολυώνυμο $f(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $\leq n$ (βλ.* (5.11)*), τέτοιο ώστε να ισχύει*

$$f(a_i) = c_i, \ \ \forall i, \ \ 0 \leq i \leq n.$$

ΑΠΟΔΕΙΞΗ. Το ότι ένα τέτοιου είδους πολυώνυμο θα είναι μονοσημάντως ορισμένο έπεται προφανώς από το πόρισμα 5.3.7. Αρκεί λοιπόν να αποδειχθεί η ύπαρξή του. Προς τούτο ορίζουμε τα πολυώνυμα $P_i(\mathsf{X}) \in K[\mathsf{X}]$, $0 \leq i \leq n$, ως εξής:

$$P_i(\mathsf{X}) := \prod_{j \in \{0,1,\dots,n\} \setminus \{i\}} \frac{(\mathsf{X} - a_j)}{(a_i - a_j)}. \tag{5.10}$$

Τότε $\deg(P_i(\mathsf{X})) = n$ και

$$P_i(a_j) = \begin{cases} 0_K, & \text{εάν } i \neq j, \\ 1_K, & \text{εάν } i = j. \end{cases}$$

Κατά συνέπειαν, το πολυώνυμο

$$f(\mathsf{X}) = \sum_{i=0}^{n} c_i P_i(\mathsf{X}) \tag{5.11}$$

έχει την επιθυμητή ιδιότητα. □

5.3.10 Ορισμός. Τα (5.10) ονομάζονται **πολυώνυμα Lagrange** (για τα στοιχεία $a_0, a_1, \dots, a_n$), ενώ ο τύπος (5.11), ο οποίος μας παρέχει το $f(\mathsf{X})$, είναι γνωστός ως **τύπος παρεμβολής τού Lagrange**.

5.3.11 Ορισμός. Ένα σώμα K καλείται **αλγεβρικώς κλειστό** όταν *κάθε* πολυώνυμο $f(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $n \geq 1$ διαθέτει τουλάχιστον μία θέση μηδενισμού ανήκουσα στο K.

5.3.12 Πόρισμα. *Έστω K ένα αλγεβρικώς κλειστό σώμα. Τότε κάθε πολυώνυμο $f(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $n \geq 1$ διασπάται σε πρωτοβαθμίους παράγοντες υπεράνω τού K.*

ΑΠΟΔΕΙΞΗ. Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον βαθμό n. Εάν $n = 1$, ο ισχυρισμός είναι προφανής. Η απόδειξη για οιονδήποτε $n \geq 2$ έχει ως εξής: Επειδή το $f(\mathsf{X})$ διαθέτει τουλάχιστον μία θέση μηδενισμού a ανήκουσα

στο K, η πρόταση 5.3.2 μας πληροφορεί ότι υπάρχει ένα πολυώνυμο $g(\mathsf{X}) \in K\,[\mathsf{X}]$, τέτοιο ώστε

$$f(\mathsf{X}) = (\mathsf{X} - a)g(\mathsf{X}), \quad \deg(g(\mathsf{X})) = n - 1.$$

Από την επαγωγική μας το $g(\mathsf{X})$ είναι γινόμενο $n-1$ πρωτοβαθμίων πολυωνύμων. Ως εκ τούτου, ο ισχυρισμός είναι αληθής και για το ίδιο το $f(\mathsf{X})$. □

5.3.13 Σημείωση. Στις παραδόσεις τής Αφηρημένης Άλγεβρας αποδεικνύεται ότι κάθε σώμα K διαθέτει μια αλγεβρικώς κλειστή επέκταση L (δηλαδή ένα αλγεβρικώς κλειστό σώμα L που περιέχει το K ως υπόσωμά του), και μάλιστα ότι υπάρχει μια *ελαχίστη* (τέτοιου είδους) επέκταση $\overline{K}$ τού K, η οποία καλείται **αλγεβρικό έγκλεισμα** τού K. Επειδή κάθε πολυώνυμο $f(\mathsf{X}) \in K\,[\mathsf{X}] \subseteq \overline{K}\,[\mathsf{X}]$ μπορεί να εκληφθεί ως πολυώνυμο τού $\overline{K}\,[\mathsf{X}]$, διασπάται πάντοτε σε πρωτοβαθμίους παράγοντες υπεράνω τού $\overline{K}$. Αυτή η διάσπαση χρησιμοποιείται ευρέως κατά την επιχειρηματολογία που εφαρμόζεται σε ποικίλες αποδεικτικές τεχνικές.

5.3.14 Θεώρημα. (Θεμελιώδες Θεώρημα τής Άλγεβρας) *Το σώμα $\mathbb{C}$ των μιγαδικών αριθμών είναι αλγεβρικώς κλειστό.*

5.3.15 Σημείωση. Το θεώρημα 5.3.14 πρωτοαποδείχθηκε το έτος 1799 από τον μέγα Γερμανό μαθηματικό C.-F. Gauss· εν τω μεταξύ υπάρχουν πολλές δεκάδες πιο σύγχρονων αποδείξεων, οι γνωστότερες των οποίων προέρχονται από τη Μιγαδική Ανάλυση και την Αλγεβρική Τοπολογία. Για περισσότερες πληροφορίες και σύντομες ιστορικές σημειώσεις παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο σύγγραμμα των B. Fine και G. Rosenberger: *Το Θεμελιώδες Θεώρημα τής Άλγεβρας* (μετάφραση στα ελληνικά: Φ. Λιούτση και Ν. Μαρμαρίδη), εκδόσεις Leader Books, Αθήνα, 2001.

5.4 ΑΝΑΓΩΓΑ ΠΟΛΥΩΝΥΜΑ

Όπως οι φυσικοί αριθμοί έχουν τους πρώτους αριθμούς ως «δομικούς τους λίθους», έτσι και τα πολυώνυμα επιδέχονται διάσπαση γραφόμενα ως γινόμενα «αναγώγων» πολυωνύμων.

5.4.1 Ορισμός. Έστω R μια ακεραία περιοχή. Ένα πολυώνυμο $f(\mathsf{X}) \in R\,[\mathsf{X}]$ θετικού βαθμού καλείται **ανάγωγο πολυώνυμο εντός τού** $R\,[\mathsf{X}]$ όταν δεν υπάρχουν πολυώνυμα $g(\mathsf{X}), h(\mathsf{X}) \in R\,[\mathsf{X}]$, τέτοια ώστε να ισχύει η ισότητα

$$f(\mathsf{X}) = g(\mathsf{X})h(\mathsf{X})$$

με $1 \leq \deg(g(\mathsf{X})) < \deg(f(\mathsf{X}))$ και $1 \leq \deg(h(\mathsf{X})) < \deg(f(\mathsf{X}))$.

5.4.2 Σημείωση. Η αναφορά τής ακεραίας περιοχής στην οποία ένα δοθέν πολυώνυμο είναι (ή δεν είναι) ανάγωγο είναι απαραίτητη. Επί παραδείγματι, το X^2+1 είναι ανάγωγο εντός τού $\mathbb{R}\,[\mathsf{X}]$ άλλά δεν είναι ανάγωγο εντός τού $\mathbb{C}\,[\mathsf{X}]$, διότι $\mathsf{X}^2+1=(\mathsf{X}+i)(\mathsf{X}-i)$, όπου i η «φανταστική» μονάδα.

5.4.3 Παρατήρηση. Έστω R μια ακεραία περιοχή.

(i) Κάθε πολυώνυμο $f(\mathsf{X})\in R[\mathsf{X}]$ βαθμού 1 είναι -προφανώς- ανάγωγο. Ο έλεγχος τής αναγωγιμότητας ενός πολυωνύμου βαθμού ≥ 2 δεν είναι εν γένει κάτι το τετριμμένο. Τα ανάγωγα πολυώνυμα εντός τού $\mathbb{R}\,[\mathsf{X}]$ μπορούν να χαρακτηρισθούν πλήρως (βλ. πρόταση 5.4.6). Όπως θα δούμε στη σημείωση 5.4.10, τα ανάγωγα πολυώνυμα εντός τού $\mathbb{C}\,[\mathsf{X}]$ είναι μόνον τα πρωτοβάθμια. Ωστόσο, ακόμη και εντός τού $\mathbb{Q}\,[\mathsf{X}]$ ένας *γενικός* χαρακτηρισμός των αναγώγων πολυωνύμων φαντάζει εξαιρετικά δύσκολος.

(ii) Κατά το 5.3.2 (ii) δεν υπάρχει κανένα ανάγωγο πολυώνυμο $f(\mathsf{X})\in R[\mathsf{X}]$ βαθμού ≥ 2 που να έχει θέσεις μηδενισμού εντός τής R. Το αντίστροφο δεν είναι εν γένει αληθές. Επί παραδείγματι, το πολυώνυμο $(\mathsf{X}^2+3)^2\in\mathbb{R}\,[\mathsf{X}]$ δεν έχει ουδεμία θέση μηδενισμού εντός τού $\mathbb{R}$, αλλ' εντούτοις δεν είναι ανάγωγο εντός τού $\mathbb{R}\,[\mathsf{X}]$. Μολαταύτα, υπό ορισμένες ειδικές προϋποθέσεις ισχύει ενίοτε και το αντίστροφο.

5.4.4 Πρόταση. *Έστω K ένα σώμα και έστω $f(\mathsf{X})\in K[\mathsf{X}]$. Εάν $\deg(f(\mathsf{X}))\in\{2,3\}$ και το $f(\mathsf{X})$ δεν διαθέτει θέσεις μηδενισμού εντός τού K, τότε το $f(\mathsf{X})$ είναι ανάγωγο εντός τού $K[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $f(\mathsf{X})$ δεν είναι ανάγωγο εντός τού $K[\mathsf{X}]$. Τότε το $f(\mathsf{X})$ γράφεται ως γινόμενο δύο πολυωνύμων

$$f(\mathsf{X})=g(\mathsf{X})h(\mathsf{X})$$

με $\deg(g(\mathsf{X}))<\deg(f(\mathsf{X}))$ και $\deg(h(\mathsf{X}))<\deg(f(\mathsf{X}))$. Επειδή

$$\deg(f(\mathsf{X}))=\deg(g(\mathsf{X}))+\deg(h(\mathsf{X}))\in\{2,3\}$$

ένα τουλάχιστον εκ των $g(\mathsf{X})$, $h(\mathsf{X})$ οφείλει να έχει βαθμό ίσον με το 1. Αλλά κάθε πολυώνυμο τού $K[\mathsf{X}]$ με βαθμό ίσον με το 1 είναι τής μορφής $a\mathsf{X}+b$, όπου $a\neq 0$, και έχει ως θέση μηδενισμού του το $a^{-1}b\in K$. Άτοπο! □

5.4.5 Λήμμα. *Έστω $f(\mathsf{X})\in\mathbb{R}\,[\mathsf{X}]$. Εάν ο μιγαδικός αριθμός $z=a+ib\in\mathbb{C}$ είναι μια θέση μηδενισμού τού $f(\mathsf{X})$, τότε το ίδιο ισχύει και για τον συζυγή του $\overline{z}=a-ib$.*

ΑΠΟΔΕΙΞΗ. Εάν $f(\mathsf{X})=a_0+a_1\mathsf{X}+\cdots+a_n\mathsf{X}^n$ και $f(z)=0$, τότε

$$\begin{aligned}0=\overline{f(z)}\;&=\overline{a_0+a_1z+\cdots+a_nz^n}=\overline{a_0}+\overline{a_1z}+\cdots+\overline{a_nz^n}\\&=\overline{a_0}+\overline{a_1}\,\overline{z}+\cdots+\overline{a_n}\,\overline{z^n}=a_0+a_1\,\overline{z}+\cdots+a_n\,\overline{z}^n\\&=f(\overline{z}),\end{aligned}$$

οπότε και ο συζυγής $\overline{z}$ τού z αποτελεί μια θέση μηδενισμού τού $f(\mathsf{X})$. □

5.4.6 Πρόταση. (Ανάγωγα πολυώνυμα με πραγματικούς συντελεστές) *Ένα πολυώνυμο $f(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ είναι ανάγωγο (εντός τού $\mathbb{R}[\mathsf{X}]$) εάν και μόνον εάν είναι τής μορφής*

$$\begin{cases} f(\mathsf{X}) = a\mathsf{X} + b, & \text{όπου } a \neq 0, \text{ή} \\ f(\mathsf{X}) = a\mathsf{X}^2 + b\mathsf{X} + c, & \text{όπου } b^2 - 4ac < 0. \end{cases}$$

ΑΠΟΔΕΙΞΗ. Εάν $f(\mathsf{X}) = a\mathsf{X}+b$, όπου $a \neq 0$, τότε το $f(\mathsf{X})$ είναι προφανώς ανάγωγο. Ένα πολυώνυμο τής μορφής $f(\mathsf{X}) = a\mathsf{X}^2 + b\mathsf{X} + c$ είναι ανάγωγο (βλ. την πρόταση 5.4.4) εάν και μόνον εάν δεν διαθέτει καμία πραγματική θέση μηδενισμού. Αλλά τούτο ισοδυναμεί με το ότι η διακρίνουσα $b^2 - 4ac$ είναι αρνητική. Επομένως, για την αποπεράτωση τής αποδείξεως αρκεί να διαπιστώσουμε ότι δεν υπάρχουν ανάγωγα πολυώνυμα $f(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ βαθμού ≥ 3. Ας υποθέσουμε ότι ένα τέτοιου είδους ανάγωγο πολυώνυμο $f(\mathsf{X})$ υπάρχει. Βάσει τού Θεμελιώδους Θεωρήματος τής Άλγεβρας το $f(\mathsf{X})$ θα διαθέτει μια θέση μηδενισμού $z \in \mathbb{C}$. Προφανώς, $z \notin \mathbb{R}$, διότι αλλιώς το $f(\mathsf{X})$ δεν θα είναι ανάγωγο. Κατά το λήμμα 5.4.5 ο συζυγής $\overline{z}$ τού z θα αποτελεί μια θέση μηδενισμού τού $f(\mathsf{X})$. Θεωρώντας τό $f(\mathsf{X})$ ως πολυώνυμο τού $\mathbb{C}[\mathsf{X}]$, λαμβάνουμε

$$\mathsf{X} - z \mid f(\mathsf{X}) \text{ και } \mathsf{X} - \overline{z} \mid f(\mathsf{X}),$$

οπότε (δυνάμει τού 5.3.3 και τού ότι $z \neq \overline{z}$, αφού $z \in \mathbb{C} \setminus \mathbb{R}$)

$$(\mathsf{X} - z)(\mathsf{X} - \overline{z}) \mid f(\mathsf{X}).$$

Όμως το

$$(\mathsf{X} - z)(\mathsf{X} - \overline{z}) = \mathsf{X}^2 - (z + \overline{z})\mathsf{X} + z\overline{z}$$

έχει πραγματικούς συντελεστές, διότι -ως γνωστόν- τόσο το άθροισμα $z+\overline{z}$ όσο και το γινόμενο $z\overline{z}$ δυο μιγαδικών συζυγών αριθμών είναι ένας πραγματικός αριθμός. Άρα το $f(\mathsf{X})$ δεν είναι ανάγωγο εντός τού $\mathbb{R}[\mathsf{X}]$. Άτοπο! □

5.4.7 Θεώρημα. (Πρωταρχική διάσπαση πολυωνύμων) *Έστω K ένα σώμα. Τότε κάθε μονικό πολώνυμο $f(\mathsf{X}) \in K[\mathsf{X}]$ θετικού βαθμού γράφεται ως γινόμενο αναγώγων μονικών πολυωνύμων (εντός τού $K[\mathsf{X}]$):*

$$f(\mathsf{X}) = g_1(\mathsf{X}) \cdot g_2(\mathsf{X}) \cdot \cdots \cdot g_m(\mathsf{X}). \tag{5.12}$$

Η παράσταση αυτή είναι μονοσημάντως ορισμένη υπό την ακόλουθη έννοια: Εάν

$$f(\mathsf{X}) = g_1(\mathsf{X}) \cdot g_2(\mathsf{X}) \cdot \cdots \cdot g_m(\mathsf{X}) = h_1(\mathsf{X}) \cdot h_2(\mathsf{X}) \cdot \cdots \cdot h_n(\mathsf{X})$$

είναι δυο διαφορετικές παραστάσεις τού $f(\mathsf{X})$ ως γινομένου μονικών αναγώγων πολυωνύμων (εντός τού $K[\mathsf{X}]$), τότε $m = n$ και υπάρχει μια μετάταξη $\sigma \in \mathfrak{S}_m$, ούτως ώστε να ισχύει

$$g_i(\mathsf{X}) = h_{\sigma(i)}(\mathsf{X}),\ \forall i,\ \ 1 \leq i \leq m.$$

ΑΠΟΔΕΙΞΗ. Θα εφαρμόσουμε τη μέθοδο τής μαθηματικής επαγωγής επί τού βαθμού $k := \deg(f(\mathsf{X}))$. Εάν $k = 1$, τότε ο ισχυρισμός είναι αληθής, διότι το $f(\mathsf{X})$ είναι ανάγωγο εντός τού $K[\mathsf{X}]$. Ας υποθέσουμε ότι $k > 1$ και ότι το θεώρημα ισχύει για όλα τα μονικά πολυώνυμα βαθμού μικροτέρου τού k. Εάν το $f(\mathsf{X})$ δεν είναι ανάγωγο, τότε θα υπάρχει ένας ανάγωγος διαιρέτης του, ας τον πούμε $g_1(\mathsf{X})$, οπότε θα έχουμε

$$f(\mathsf{X}) = g_1(\mathsf{X})p(\mathsf{X}),\quad 0 < \deg(p(\mathsf{X})) < k,$$

για κάποιο $p(\mathsf{X}) \in K[\mathsf{X}]$. Μπορούμε να υποθέσουμε ότι το $p(\mathsf{X})$ είναι μονικό, οπότε και το $g_1(\mathsf{X})$ θα είναι μονικό. Σύμφωνα με την επαγωγική μας υπόθεση το $p(\mathsf{X})$ διαθέτει μια μονοσήμαντη παραγοντοποίηση τής μορφής

$$p(\mathsf{X}) = g_2(\mathsf{X}) \cdot \cdots \cdot g_m(\mathsf{X})$$

κάνοντας χρήση μονικών αναγώγων πολυωνύμων. Εξ αυτού συνάγουμε την (5.12). Υποθέτουμε τώρα ότι υπάρχει μια άλλη παραγοντοποίηση

$$f(\mathsf{X}) = h_1(\mathsf{X}) \cdot h_2(\mathsf{X}) \cdot \cdots \cdot h_n(\mathsf{X}).$$

Επειδή $g_1(\mathsf{X}) \mid h_1(\mathsf{X}) \cdot h_2(\mathsf{X}) \cdot \cdots \cdot h_n(\mathsf{X})$, το $g_1(\mathsf{X})$ θα διαιρεί τουλάχιστον ένα από τα πολυώνυμα $h_1(\mathsf{X}), \ldots, h_n(\mathsf{X})$. Χωρίς βλάβη τής γενικότητας ας υποθέσουμε ότι $g_1(\mathsf{X}) \mid h_1(\mathsf{X})$. Επειδή τα $g_1(\mathsf{X}), h_1(\mathsf{X})$ είναι μονικά και ανάγωγα θα έχουμε

$$g_1(\mathsf{X}) = h_1(\mathsf{X}).$$

Άρα

$$p(\mathsf{X}) = h_2(\mathsf{X}) \cdot \cdots \cdot h_n(\mathsf{X}).$$

Και επειδή η παραγοντοποίηση τού $p(\mathsf{X})$ είναι μονοσήμαντη, θα υπάρχει μια μετάταξη δεικτών $\sigma \in \mathfrak{S}_m$, ούτως ώστε να ισχύει

$$g_i(\mathsf{X}) = h_{\sigma(i)}(\mathsf{X}),\ \forall i,\ \ 1 \leq i \leq m.$$

(Εμείς εδώ, χάριν ευκολίας, θέσαμε $\sigma\,(1) = 1$). □

5.4.8 Σημείωση. (i) Η παράσταση (5.12) καθενός μονικού $f(\mathsf{X}) \in K[\mathsf{X}]$ θετικού βαθμού ως γινομένου μονοσημάντως ορισμένων αναγώγων μονικών πολυωνύμων (εντός τού $K[\mathsf{X}]$) ονομάζεται ιδιαιτέρως **πρωταρχική διάσπαση** τού $f(\mathsf{X}) \in K[\mathsf{X}]$.

(ii) Το θεώρημα 5.4.7 μπορεί να γενικευθεί και για τον $R[\mathsf{X}]$, όπου το R είναι μια ειδικής φύσεως ακεραία περιοχή (που ονομάζεται ΠΜΠ[5]), με μόνη επιβάρυνσή μας το ότι η μονοσημαντότητα είναι ακριβής εξαιρουμένης τής δυνατότητας πολλαπλασιασμού με αντιστρέψιμα στοιχεία τής R.

5.4.9 Πόρισμα. *Έστω K ένα σώμα. Τότε κάθε πολώνυμο $f(\mathsf{X}) \in K[\mathsf{X}]$ θετικού βαθμού γράφεται ως γινόμενο ενός στοιχείου $a \in K \setminus \{0_K\}$ και πεπερασμένου πλήθους, μονοσημάντως ορισμένων αναγώγων μονικών πολυωνύμων* (εντός τού $K[\mathsf{X}]$):

$$f(\mathsf{X}) = a \cdot g_1(\mathsf{X}) \cdot g_2(\mathsf{X}) \cdot \cdots \cdot g_m(\mathsf{X}). \tag{5.13}$$

Η παράσταση αυτή είναι μονοσημάντως ορισμένη υπό την ακόλουθη έννοια: *Εάν*

$$f(\mathsf{X}) = a \cdot g_1(\mathsf{X}) \cdot g_2(\mathsf{X}) \cdot \cdots \cdot g_m(\mathsf{X}) = b \cdot h_1(\mathsf{X}) \cdot h_2(\mathsf{X}) \cdot \cdots \cdot h_n(\mathsf{X})$$

είναι δυο διαφορετικές παραστάσεις τού $f(\mathsf{X})$ (εντός τού $K[\mathsf{X}]$)*, τότε $m = n$ και υπάρχει μια μετάταξη $\sigma \in \mathfrak{S}_m$ και $a_i \in K, 1 \leq i \leq m$, ούτως ώστε να ισχύει*

$$g_i(\mathsf{X}) = a_{\sigma(i)} \cdot h_{\sigma(i)}(\mathsf{X}),\ \forall i,\ \ 1 \leq i \leq m.$$

5.4.10 Σημείωση. (Ανάγωγα πολυώνυμα με μιγαδικούς συντελεστές) Κατά το πόρισμα 5.3.12 και το Θεμελιώδες Θεώρημα τής Άλγεβρας 5.3.14, κάθε πολώνυμο $f(\mathsf{X}) \in \mathbb{C}[\mathsf{X}]$ γράφεται ως γινόμενο πρωτοβαθμίων (και συνεπώς αναγώγων) πολυωνύμων. Ως εκ τούτου, από το μονοσήμαντο των μη σταθερών όρων τής παραστάσεως (5.13) καθενός $f(\mathsf{X}) \in \mathbb{C}[\mathsf{X}]$ (βλ. πόρισμα 5.4.9) έπεται ότι *τα ανάγωγα πολυώνυμα εντός τού $\mathbb{C}[\mathsf{X}]$ είναι ακριβώς τα πρωτοβάθμια πολυώνυμα.*

5.4.11 Σημείωση. (Το σώμα των ρητών εκφράσεων) Προτού κλείσουμε το παρόν κεφάλαιο προσήκει να αναφέρουμε εν σπουδή ότι το σώμα κλασμάτων τής ακεραίας περιοχής $K[\mathsf{X}]$ (όπου K ένα σώμα) συμβολίζεται ως

$$K(\mathsf{X}) := \mathbf{Fr}\,(K[\mathsf{X}]) = \left\{ \frac{f(\mathsf{X})}{g(\mathsf{X})} \;\middle|\; f(\mathsf{X}) \in K[\mathsf{X}], g(\mathsf{X}) \in K[\mathsf{X}] \setminus \{0_K\} \right\}$$

και καλείται ιδιαιτέρως **σώμα των ρητών εκφράσεων** υπεράνω τού K. Η ακεραία περιοχή $K[\mathsf{X}]$ μπορεί, ως γνωστόν, να *εμφυτευθεί* στο $K(\mathsf{X})$ (βλ. προτάσεις 4.7.5 και 4.7.7). Επίσης, κάθε στοιχείο $\frac{f(\mathsf{X})}{g(\mathsf{X})}$ τού $K(\mathsf{X})$, όπου $\deg(f(\mathsf{X})) < \deg(g(\mathsf{X}))$, $g(\mathsf{X})$ μονικό, και

$$g(\mathsf{X}) = (h_1(\mathsf{X}))^{n_1} \cdot (h_2(\mathsf{X}))^{n_2} \cdot \cdots \cdot (h_k(\mathsf{X}))^{n_k}$$

[5] ΠΜΠ = περιοχή μονοσήμαντης παραγοντοποιήσεως.

η πρωταρχική διάσπαση τού $g(\mathsf{X})$ ως γινομένου αναγώγων μονικών και *σαφώς διακεκριμένων* πολυωνύμων (εντός τού $K[\mathsf{X}]$), γράφεται υπό τη μορφή

$$\frac{f(\mathsf{X})}{g(\mathsf{X})} = \sum_{j=1}^{k} \frac{p_j(\mathsf{X})}{(h_j(\mathsf{X}))^{n_j}},$$

για κατάλληλα $p_1(\mathsf{X}), \ldots, p_k(\mathsf{X}) \in K[\mathsf{X}]$ και $\deg(p_j(\mathsf{X})) < \deg\left((h_j(\mathsf{X}))^{n_j}\right)$, για κάθε δείκτη $j,\ 1 \leq j \leq k$.

5.5 ΠΕΡΙ ΤΗΣΑΝΑΓΩΓΙΜΟΤΗΤΑΣ ΠΟΛΥΩΝΥΜΩΝ ΑΝΗΚΟΝΤΩΝ ΣΤΟΥΣ $\mathbb{Z}[\mathsf{X}]$, $\mathbb{Z}_p[\mathsf{X}]$ ΚΑΙ $\mathbb{Q}[\mathsf{X}]$

Η διάσπαση ενός πολυωνύμου ανήκοντος στον $\mathbb{Q}[\mathsf{X}]$ μπορεί να αναχθεί στη διάσπαση ενός πολυωνύμου ανήκοντος στον $\mathbb{Z}[\mathsf{X}]$. Πράγματι· εάν

$$f(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in \mathbb{Q}[\mathsf{X}] \setminus \{0_{\mathbb{Q}[\mathsf{X}]}\}$$

και εάν ως c συμβολίσουμε το ελάχιστο κοινό πολλαπλάσιο των παρονομαστών των $a_0, a_1, ..., a_n$, τότε $c\, f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}] \setminus \{0_{\mathbb{Z}[\mathsf{X}]}\}$.

5.5.1 Θεώρημα. (Κριτήριο ρητών θέσεων μηδενισμού.) *Εάν ένα πολυώνυμο*

$$f(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in \mathbb{Z}[\mathsf{X}],\ \ a_n \neq 0,\ \ n \geq 1,$$

δέχεται ως θέση μηδενισμού του τον ρητό αριθμό $\frac{\lambda}{\mu}$, *όπου* $\lambda \in \mathbb{Z}$, $\mu \in \mathbb{Z} \setminus \{0\}$ *και* $\mu\kappa\delta(\lambda, \mu) = 1$, *τότε*

$$\lambda \mid a_0 \ \text{ και } \ \mu \mid a_n.$$

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, $f(\frac{\lambda}{\mu}) = 0$, οπότε

$$\sum_{j=0}^{n} a_j \left(\frac{\lambda}{\mu}\right)^j = 0 \Rightarrow -\mu^n a_0 = \lambda \left(\sum_{j=1}^{n} a_j \lambda^{j-1} \mu^{n-j}\right) \Rightarrow \lambda \mid \mu^n a_0.$$

Χρησιμοποιώντας τό πόρισμα 2.2.9 και μαθηματική επαγωγή ως προς το n αποδεικνύουμε τη συνεπαγωγή

$$\mu\kappa\delta(\lambda, \mu) = 1 \Rightarrow \mu\kappa\delta(\lambda, \mu^n) = 1,$$

απ' όπου έπεται ότι $\lambda \mid a_0$ επί τη βάσει τού πορίσματος 2.2.10. Παρομοίως,

$$\sum_{j=0}^{n} a_j \left(\frac{\lambda}{\mu}\right)^j = 0 \Rightarrow -\lambda^n a_n = \mu \left(\sum_{j=0}^{n-1} a_j \lambda^j \mu^{n-1-j}\right) \Rightarrow \mu \mid \lambda^n a_n.$$

Επειδή μκδ$(\lambda, \mu) = 1 \Rightarrow$ μκδ$(\lambda^n, \mu) = 1$, έχουμε $\mu \mid a_n$ επί τη βάσει τού πορίσματος 2.2.10. □

5.5.2 Παράδειγμα. Έστω $f(\mathsf{X}) = \mathsf{X}^3 + 4\mathsf{X}^2 + \mathsf{X} - 1 \in \mathbb{Z}[\mathsf{X}]$. Εάν το $f(\mathsf{X})$ διέθετε ως θέση μηδενισμού του τον ρητό αριθμό $\frac{\lambda}{\mu}$, όπου $\lambda \in \mathbb{Z}$, $\mu \in \mathbb{Z}\smallsetminus\{0\}$ και μκδ$(\lambda, \mu) = 1$, τότε θα έπρεπε να έχουμε $\lambda, \mu \in \{\pm 1\}$, κάτι που είναι αδύνατο, καθόσον ισχύει $f(\pm 1) \neq 0$. Τούτο σημαίνει, ιδιαιτέρως, ότι το $f(\mathsf{X})$ είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$ (λόγω τής προτάσεως 5.4.4).

5.5.3 Λήμμα. (Αναγωγή κατά μόδιο m.) *Έστω $m \in \mathbb{N}$, $m \geq 2$. Η απεικόνιση*

$$\Psi_m : \mathbb{Z}[\mathsf{X}] \longrightarrow \mathbb{Z}_m[\mathsf{X}],$$

η οριζόμενη μέσω τού τύπου

$$\Psi_m(f(\mathsf{X})) := \sum_{j=0}^{n} [a_j]_m \mathsf{X}^j, \quad \forall f(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in \mathbb{Z}[\mathsf{X}],$$

είναι ομομορφισμός δακτυλίων.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τον ορισμό των πράξεων προσθέσεως και πολλαπλασιασμού επί τού $\mathbb{Z}_m$ τον θεσπισθέντα μέσω τού θεωρήματος 2.4.28. □

5.5.4 Ορισμός. Εάν $f(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in \mathbb{Z}[\mathsf{X}]\smallsetminus\{0_{\mathbb{Z}[\mathsf{X}]}\}$ με $a_n \neq 0$, τότε ο αριθμός

$$\text{cont}(f(\mathsf{X})) := \text{ μκδ}(a_0, a_1, \ldots, a_n)$$

καλείται **περιεχόμενο** τού πολυωνύμου $f(\mathsf{X})$. Κάθε $f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]\smallsetminus\{0_{\mathbb{Z}[\mathsf{X}]}\}$ με $\text{cont}(f(\mathsf{X})) = 1$ καλείται **πρωταρχικό πολυώνυμο**.

5.5.5 Πρόταση. (Λήμμα τού Gauss.) *Το γινόμενο δυο πρωταρχικών πολυωνύμων (ανηκόντων στο $\mathbb{Z}[\mathsf{X}]\smallsetminus\{0_{\mathbb{Z}[\mathsf{X}]}\}$) είναι πάντοτε ένα πρωταρχικό πολυώνυμο.*

ΑΠΟΔΕΙΞΗ. Έστω ότι τα $f(\mathsf{X}), g(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]\smallsetminus\{0_{\mathbb{Z}[\mathsf{X}]}\}$ είναι δυο πρωταρχικά πολυώνυμα. Ας υποθέσουμε ότι το γινόμενό τους $f(\mathsf{X})g(\mathsf{X})$ *δεν* είναι πρωταρχικό πολυώνυμο. Έστω p ένας πρώτος αριθμός που διαιρεί το $\text{cont}(f(\mathsf{X})g(\mathsf{X}))$. Τότε έχουμε προφανώς $\Psi_p(f(\mathsf{X})), \Psi_p(g(\mathsf{X})) \in \mathbb{Z}_p[\mathsf{X}]$ και, σύμφωνα με το λήμμα 5.5.3,

$$\Psi_p(f(\mathsf{X}))\Psi_p(g(\mathsf{X})) = \Psi_p(f(\mathsf{X})g(\mathsf{X})) = 0_{\mathbb{Z}_p[\mathsf{X}]},$$

οπότε *είτε* ο p διαιρεί κάθε συντελεστή τού πολυωνύμου $f(\mathsf{X})$ *είτε* ο p διαιρεί κάθε συντελεστή τού πολυωνύμου $g(\mathsf{X})$. Αυτό σημαίνει ότι *είτε* το $f(\mathsf{X})$ *είτε* το $g(\mathsf{X})$ *δεν* είναι πρωταρχικό. Άτοπο! □

5.5.6 Πρόταση. *Εάν ένα πολυώνυμο $f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ είναι ανάγωγο εντός τού πολυωνυμικού δακτυλίου $\mathbb{Z}[\mathsf{X}]$, τότε είναι ανάγωγο και εντός τού $\mathbb{Q}[\mathsf{X}]$.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ δεν ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$. Τότε υπάρχουν πολυώνυμα $g(\mathsf{X}), h(\mathsf{X}) \in \mathbb{Q}[\mathsf{X}]$ βαθμού ≥ 1, τέτοια ώστε να ισχύει η ισότητα $f(\mathsf{X}) = g(\mathsf{X})h(\mathsf{X})$. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι το $f(\mathsf{X})$ είναι πρωταρχικό (ειδάλλως θεωρούμε αντ' αυτού το $\frac{1}{\mathrm{cont}(f(\mathsf{X}))} f(\mathsf{X})$). Έστω a (και αντιστοίχως, b) το εκπ των παρονομαστών των συντελεστών τού $g(\mathsf{X})$ (και αντιστοίχως, τού $h(\mathsf{X})$). Τότε

$$a\, g(\mathsf{X}), b\, h(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}] \Rightarrow ab\, f(\mathsf{X}) = (a\, g(\mathsf{X}))(b\, h(\mathsf{X})) \in \mathbb{Z}[\mathsf{X}].$$

Θέτοντας $c_1 := \mathrm{cont}(a\, g(\mathsf{X}))$ και $c_2 := \mathrm{cont}(b\, h(\mathsf{X}))$ έχουμε

$$a\, g(\mathsf{X}) = c_1\, \widetilde{g}(\mathsf{X}), \;\; b\, h(\mathsf{X}) = c_2\, \widetilde{h}(\mathsf{X}),$$

για κάποια $\widetilde{g}(\mathsf{X}), \widetilde{h}(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ βαθμού ≥ 1 με $\mathrm{cont}(\widetilde{g}(\mathsf{X})) = \mathrm{cont}(\widetilde{h}(\mathsf{X})) = 1$. Προφανώς,

$$\left.\begin{aligned} ab\, f(\mathsf{X}) &= c_1 c_2\, \widetilde{g}(\mathsf{X})\widetilde{h}(\mathsf{X}), \\ \mathrm{cont}(f(\mathsf{X})) = 1 &\Longrightarrow \mathrm{cont}(ab\, f(\mathsf{X})) = ab, \\ \mathrm{cont}(\widetilde{g}(\mathsf{X})\widetilde{h}(\mathsf{X})) \underset{5.5.5}{=} 1 &\Longrightarrow \mathrm{cont}(c_1 c_2\, \widetilde{g}(\mathsf{X})\widetilde{h}(\mathsf{X})) = c_1 c_2, \end{aligned}\right\} \Longrightarrow ab = c_1 c_2,$$

οπότε $f(\mathsf{X}) = \widetilde{g}(\mathsf{X})\widetilde{h}(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$, πράγμα που σημαίνει ότι το $f(\mathsf{X})$ δεν ανάγωγο ούτε εντός τού $\mathbb{Z}[\mathsf{X}]$. □

5.5.7 Θεώρημα. (Κριτήριο αναγωγιμότητας $\bmod p$.) *Έστω p ένας πρώτος αριθμός και έστω $f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ βαθμού ≥ 1. Εάν το $\Psi_p(f(\mathsf{X}))$ είναι ανάγωγο εντός τού $\mathbb{Z}_p[\mathsf{X}]$ και*

$$\deg(f(\mathsf{X})) = \deg(\Psi_p(f(\mathsf{X}))),$$

τότε το $f(\mathsf{X})$ είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$.

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι πληρούνται οι ως άνω συνθήκες και ότι το $f(\mathsf{X})$ *δεν* είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$. Τότε, σύμφωνα με την πρόταση 5.5.6, το το $f(\mathsf{X})$ *δεν* είναι ανάγωγο ούτε εντός τού $\mathbb{Z}[\mathsf{X}]$, οπότε θα υπάρχουν $g(\mathsf{X}), h(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ βαθμού ≥ 1, τέτοια ώστε να ισχύει $f(\mathsf{X}) = g(\mathsf{X})h(\mathsf{X})$. Επειδή κατά το λήμμα 5.5.3,

$$\Psi_p(f(\mathsf{X})) = \Psi_p(g(\mathsf{X})h(\mathsf{X})) = \Psi_p(g(\mathsf{X}))\Psi_p(h(\mathsf{X})),$$

με

$$\deg(\Psi_p(g(\mathsf{X}))) \leq \deg(g(\mathsf{X})) < \deg(f(\mathsf{X})) = \deg(\Psi_p(f(\mathsf{X})))$$

και

$$\deg(\Psi_p(h(\mathsf{X}))) \leq \deg(h(\mathsf{X})) < \deg(f(\mathsf{X})) = \deg(\Psi_p(f(\mathsf{X}))),$$

το $\Psi_p(f(\mathsf{X}))$ δεν είναι ανάγωγο εντός τού $\mathbb{Z}_p[\mathsf{X}]$. Άτοπο! □

5.5.8 Παραδείγματα. (i) Έστω $f(\mathsf{X}) = 21\mathsf{X}^3 - 3\mathsf{X}^2 + 2\mathsf{X} + 9 \in \mathbb{Z}[\mathsf{X}]$. Προφανώς,

$$\Psi_2(f(\mathsf{X})) = \mathsf{X}^3 + \mathsf{X}^2 + [1]_2 \in \mathbb{Z}_2[\mathsf{X}].$$

Επειδή $\Psi_2(f([0]_2)) = [1]_2 \neq [0]_2$ και $\Psi_2(f([1]_2)) = [1]_2 \neq [0]_2$ το $\Psi_2(f(\mathsf{X}))$ είναι ανάγωγο εντός τού $\mathbb{Z}_2[\mathsf{X}]$ (βλ. πρόταση 5.4.4), οπότε το θεώρημα 5.5.7 μας πληροφορεί ότι το $f(\mathsf{X})$ είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$.

(ii) Το αντίστροφο τού θεωρήματος 5.5.7 δεν είναι πάντοτε αληθές: Εάν το $f(\mathsf{X})$ ανήκει στον $\mathbb{Z}[\mathsf{X}]$ και εάν το $\Psi_p(f(\mathsf{X}))$ δεν είναι ανάγωγο εντός τού $\mathbb{Z}_p[\mathsf{X}]$ για κάποιον πρώτο αριθμό p, τότε ενδέχεται το $f(\mathsf{X})$ *να είναι* ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$. Π.χ., εάν $f(\mathsf{X}) = 21\mathsf{X}^3 - 3\mathsf{X}^2 + 2\mathsf{X} + 8 \in \mathbb{Z}[\mathsf{X}]$ και $p = 2$, τότε το

$$\Psi_2(f(\mathsf{X})) = \mathsf{X}^3 + \mathsf{X}^2 = \mathsf{X}^2(\mathsf{X} + [1]_2)$$

δεν είναι ανάγωγο εντός τού $\mathbb{Z}_2[\mathsf{X}]$, οπότε δεν μπορούμε να κάνουμε χρήση τού θεωρήματος 5.5.7. Αντιθέτως, εργαζόμενοι με το $p = 5$ διαπιστώνουμε ότι το $\Psi_5(f(\mathsf{X}))$ δεν διαθέτει καμία θέση μηδενισμού εντός τού $\mathbb{Z}_5$, οπότε *είναι* ανάγωγο εντός τού $\mathbb{Z}_5[\mathsf{X}]$ (βλ. πρόταση 5.4.4). Άρα και το το $f(\mathsf{X})$ *είναι* ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$ (αφού για $p = 5$ έχουμε τη δυνατότητα εφαρμογής τού θεωρήματος 5.5.7).

5.5.9 Θεώρημα. (Κριτήριο αναγωγιμότητας τού Eisenstein, 1850.) *Έστω*

$$f(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j \in \mathbb{Z}[\mathsf{X}] \text{ με } \deg(f(\mathsf{X})) = n \geq 1.$$

Εάν υπάρχει πρώτος αριθμός p, ο οποίος πληροί τις ακόλουθες συνθήκες:

$$p \mid a_0,\ p \mid a_1, \ldots,\ p \mid a_{n-1},\ p \nmid a_n,\ p^2 \nmid a_0,$$

τότε το $f(\mathsf{X})$ είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$.

ΑΠΟΔΕΙΞΗ. Δυνάμει τής προτάσεως 5.5.6 αρκεί να δειχθεί ότι το $f(\mathsf{X})$ είναι ανάγωγο εντός τού $\mathbb{Z}[\mathsf{X}]$. Ας υποθέσουμε ότι αυτό δεν ισχύει, ήτοι ότι το $f(\mathsf{X})$ *δεν* είναι ανάγωγο εντός τού $\mathbb{Z}[\mathsf{X}]$, εφαρμόζοντας «εις άτοπον απαγωγή». Τότε υπάρχουν πολυώνυμα $g(\mathsf{X}), h(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$ βαθμού ≥ 1, τέτοια ώστε να ισχύει η ισότητα

$f(\mathsf{X}) = g(\mathsf{X})h(\mathsf{X})$. Έστω ότι

$$\left.\begin{array}{l} g(\mathsf{X}) = b_0 + b_1\mathsf{X} + \cdots + b_r\mathsf{X}^r, \;\; b_r \neq 0, \\ h(\mathsf{X}) = c_0 + c_1\mathsf{X} + \cdots + c_s\mathsf{X}^s, \;\; c_s \neq 0. \end{array}\right\}$$

Επειδή $p \mid a_0,\ p^2 \nmid a_0$ και $a_0 = b_0c_0$, ο p διαιρεί έναν εκ των b_0, c_0, αλλά όχι αμφοτέρους! Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $p \mid b_0$ και $p \nmid c_0$. Επειδή $p \nmid a_n = b_rc_s$, έχουμε $p \nmid b_r$, οπότε $\{\nu \in \{0, 1, \ldots, n\} \mid p \nmid b_\nu\} \neq \varnothing$. Θέτοντας $m := \min\{\nu \in \{0, 1, \ldots, n\} \mid p \nmid b_\nu\}$ και λαμβάνοντας υπ' όψιν ότι

$$a_\nu = \sum_{i+j=\nu} b_ic_j, \;\; \forall \nu \in \{0, 1, \ldots, n\},$$

συνάγουμε ότι $0 < m \leq r < n$. Επειδή

$$a_m = b_mc_0 + (b_{m-1}c_1 + \cdots + b_0c_m),$$

και επειδή

$$\left.\begin{array}{l} p \nmid b_m \\ p \nmid c_0 \end{array}\right\} \Longrightarrow p \nmid b_mc_0,$$

ενώ όλοι οι άλλοι προσθετέοι (οι ευρισκόμενοι εντός τής παρενθέσεως) διαιρούνται διά τού p (λόγω τού ορισμού τού m), συμπεραίνουμε ότι $p \nmid a_m$. Άτοπο! □

5.5.10 Παράδειγμα. Έστω $f(\mathsf{X}) = 3\mathsf{X}^5 + 15\mathsf{X}^4 - 20\mathsf{X}^3 + 10\mathsf{X} + 20 \in \mathbb{Z}[\mathsf{X}]$. Το $f(\mathsf{X})$ είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$, διότι $5 \nmid 3$, $25 \nmid 20$ και το 5 διαιρεί τους ακεραίους $15, -20, 10$ και 20.

5.5.11 Ορισμός. Έστω p κάποιος πρώτος αριθμός. Το

$$\Phi_p(\mathsf{X}) := \frac{\mathsf{X}^p - 1}{\mathsf{X} - 1} = \sum_{j=0}^{p-1} \mathsf{X}^j \in \mathbb{Z}[\mathsf{X}]$$

καλείται p-**οστό κυκλοτομικό πολυώνυμο**.

5.5.12 Πρόταση. *Το* $\Phi_p(\mathsf{X})$ *είναι ανάγωγο εντός τού* $\mathbb{Q}[\mathsf{X}]$.

ΑΠΟΔΕΙΞΗ. Έστω $f_p(\mathsf{X}) := \Phi_p(\mathsf{X} + 1)$. Τότε

$$f_p(\mathsf{X}) = \frac{(\mathsf{X}+1)^p - 1}{(\mathsf{X}+1) - 1} = \mathsf{X}^{p-1} + \binom{p}{1}\mathsf{X}^{p-2} + \binom{p}{2}\mathsf{X}^{p-3} + \cdots + \binom{p}{p-1}.$$

Προφανώς, $p \nmid 1$, $p^2 \nmid \binom{p}{p-1} = p$. Επειδή, κατά το λήμμα 2.4.11,

$$p \mid \binom{p}{k}, \;\; \forall k \in \{1, ..., p-1\},$$

το κριτήριο αναγωγιμότητας 5.5.9 τού Eisenstein μάς πληροφορεί ότι το $f_p(\mathsf{X})$ είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$. Αλλά αυτό σημαίνει ότι και το ίδιο το $\Phi_p(\mathsf{X})$ είναι ανάγωγο εντός τού $\mathbb{Q}[\mathsf{X}]$. (Πράγματι· εάν υπήρχαν πολυώνυμα $g(\mathsf{X}), h(\mathsf{X}) \in \mathbb{Q}[\mathsf{X}]$ βαθμού ≥ 1, τέτοια ώστε $\Phi_p(\mathsf{X}) = g(\mathsf{X})h(\mathsf{X})$, τότε θα είχαμε $f_p(\mathsf{X}) = g(\mathsf{X}+1)h(\mathsf{X}+1)$, με καθένα εκ των πολυωνύμων $g(\mathsf{X}+1), h(\mathsf{X}+1)$ βαθμού ≥ 1, κάτι που θα αντέφασκε προς την αποδειχθείσα αναγωγιμότητα τού $f_p(\mathsf{X})$ εντός τού $\mathbb{Q}[\mathsf{X}]$.) □