ΚΕΦΑΛΑΙΟ 3

Πολυώνυμα με συντελεστές ειλημμένους από κάποιο σώμα

Ιδιαίτερης σημασίας παραδείγματα δακτυλίων αποτελούν οι *πολυωνυμικοί δακτύλιοι*, στη μελέτη των οποίων αφιερώνεται το παρόν κεφάλαιο. Ειδικότερα, ο δακτύλιος $K[\mathsf{X}]$ των πολυωνύμων μιας απροσδιορίστου X με συντελεστές ειλημμένους από κάποιο σώμα K (ιδωμένος ως υποδακτύλιος τού δακτυλίου των επίτυπων δυναμοσειρών $K[\![\mathsf{X}]\!]$) διαδραματίζει καθοριστικό ρόλο σε ευρέα τμήματα τής ύλης τής Γραμμικής Άλγεβρας, όχι μόνον διότι ο ίδιος καθίσταται K-διανυσματικός χώρος (εφοδιαζόμενος με τη συνήθη εξωτερική πράξη τού αριθμητικού πολλαπλασιασμού) και διαθέτει ενδιαφέροντες γραμμικούς υποχώρους αλλά και διότι οι κύριες ιδιότητές του (που αφορούν στη διαιρετότητα, στις θέσεις μηδενισμού, στην επίτυπη παραγώγιση κ.ά.) υπεισέρχονται κατά τρόπο ουσιαστικό σε τεχνικά μέσα που απαιτούνται για την επίλυση προβλημάτων εντασσομένων στη Θεωρία Πινάκων.

3.1 ΕΠΙΤΥΠΕΣ ΔΥΝΑΜΟΣΕΙΡΕΣ

Δοθέντος ενός σώματος K, θεωρούμε το σύνολο $K^{\mathbb{N}_0}$ όλων των ακολουθιών $(a_0, a_1, a_2, \ldots\ldots)$ με τα $a_i \in K$, $i = 0, 1, 2, \ldots$ Προφανώς, δυο στοιχεία

$$\varphi = (a_0, a_1, a_2, \ldots, a_n, \ldots), \quad \psi = (b_0, b_1, b_2, \ldots, b_n, \ldots)$$

τού $K^{\mathbb{N}_0}$ είναι ίσα ($\varphi = \psi$) όταν $a_i = b_i, \forall i \in \mathbb{N}_0$. Επί τού $K^{\mathbb{N}_0}$ ορίζουμε δύο *εσωτερικές* πράξεις *προσθέσεως* και *πολλαπλασιασμού* (κατά συντεταγμένες) ως

ακολούθως:

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

όπου

$$c_m := \sum_{i+j=m} a_i b_j = a_0b_m + a_1b_{m-1} + \cdots + a_mb_0,\ \forall m \in \mathbb{N}_0.$$

Η τριάδα $(K^{\mathbb{N}_0}, +, \cdot)$ αποτελεί έναν μεταθετικό δακτύλιο με μηδενικό του στοιχείο το $(0_K, 0_K,...)$ και μοναδιαίο του στοιχείο το $(1_K, 0_K, 0_K,...)$. *Ταυτίζοντας*[1] κάθε $a \in K$ με το $(a, 0_K, 0_K,...)$ έχουμε τη δυνατότητα θεωρήσεως τού K ως υποδακτυλίου τού $K^{\mathbb{N}_0}$. Εισάγοντας ένα νέο σύμβολο

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

παρατηρούμε ότι, βάσει αυτών των πράξεων,

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

και, γενικότερα,

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

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

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

Εάν λοιπόν το $(a_0, a_1, a_2,...)$ είναι τυχόν στοιχείο τού $K^{\mathbb{N}_0}$, τότε μπορούμε να γράψουμε

$$(a_0,a_1,a_2,...) = a_0 + a_1\mathsf{X} + a_2\mathsf{X}^2 + \cdots + a_n\mathsf{X}^n + \cdots =: \sum_{i=0}^{\infty} a_i\mathsf{X}^i.$$

3.1.1 Ορισμός. Ο δακτύλιος $K^{\mathbb{N}_0}$ συμβολίζεται συνήθως ως $K[\![\mathsf{X}]\!]$ και καλείται **δακτύλιος επίτυπων δυναμοσειρών** (ή **τύποις δυναμοσειρών**) μιας **απροσδιορίστου** X με συντελεστές ειλημμένους από το K. Τα στοιχεία τού $K[\![\mathsf{X}]\!]$ ονομάζονται **επίτυπες δυναμοσειρές** και σημειώνονται ως $\varphi(\mathsf{X}), \psi(\mathsf{X}),$ .. κ.λπ., ενώ τα εκάστοτε αναγραφόμενα $a_0, a_1, a_2,...$ ονομάζονται **συντελεστές** των επίτυπων δυναμοσειρών. (Η **μηδενική** επίτυπη δυναμοσειρά, ήτοι το μηδενικό στοιχείο τού $K[\![\mathsf{X}]\!]$, σημειώνεται ως $\mathbf{0}_{K[\![\mathsf{X}]\!]}$.)

[1] Η εν λόγω ταύτιση υλοποιείται μέσω τού μονομορφισμού δακτυλίων $a \longmapsto (a, 0_K, 0_K,...)$.

Δυο επίτυπες δυναμοσειρές

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in K[\![\mathsf{X}]\!]\,, \;\; \psi(\mathsf{X}) = \sum_{i=0}^{\infty} b_i \mathsf{X}^i \in K[\![\mathsf{X}]\!] \tag{3.1}$$

είναι **ίσες** ($\varphi(\mathsf{X}) = \psi(\mathsf{X})$) εάν και μόνον εάν $a_i = b_i, \forall i \in \mathbb{N}_0$.

3.1.2 Πρόταση. *Ο δακτύλιος $K[\![\mathsf{X}]\!]$ είναι ακεραία περιοχή.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε δυο επίτυπες δυναμοσειρές (3.1). Εάν $\varphi(\mathsf{X}) \neq \mathbf{0}_{K[\![\mathsf{X}]\!]}$ και $\psi(\mathsf{X}) \neq \mathbf{0}_{K[\![\mathsf{X}]\!]}$, τότε ορίζονται οι μη αρνητικοί ακέραιοι

$$i_0 := \min\{\, i \in \mathbb{N}_0 |\, a_i \neq 0_K \}\,, \;\; j_0 := \min\{\, j \in \mathbb{N}_0 |\, b_j \neq 0_K \}\,.$$

Για κάθε $m \in \mathbb{N}_0$, $m \leq i_0 + j_0$, ο συντελεστής τού m-οστού όρου τού γινομένου τους $\varphi(\mathsf{X})\psi(\mathsf{X})$ είναι ο

$$c_m := \sum_{i+j=m} a_i b_j = \begin{cases} 0_K, & \text{όταν } m < i_0 + j_0, \\ a_{i_0} b_{j_0}, & \text{όταν } m = i_0 + j_0. \end{cases}$$

Επειδή το K είναι ακεραία περιοχή (βλ. 2.3.16 (i)), έχουμε

$$\left.\begin{matrix} a_{i_0} \neq 0_K \\ b_{j_0} \neq 0_K \end{matrix}\right\} \Longrightarrow a_{i_0} b_{j_0} = c_{i_0 + j_0} \neq 0_K,$$

οπότε $\varphi(\mathsf{X})\psi(\mathsf{X}) \neq \mathbf{0}_{K[\![\mathsf{X}]\!]}$ και ο $K[\![\mathsf{X}]\!]$ είναι ακεραία περιοχή. □

3.1.3 Πρόταση. *Μια επίτυπη δυναμοσειρά*

$$\varphi(\mathsf{X}) = \sum_{i=0}^{\infty} a_i \mathsf{X}^i \in K[\![\mathsf{X}]\!]$$

είναι αντιστρέψιμο στοιχείο τού δακτυλίου $K[\![\mathsf{X}]\!]$ εάν και μόνον εάν $a_0 \neq 0_K$. Επιπροσθέτως, όταν $a_0 \neq 0_K$, το αντίστροφο στοιχείο τής $\varphi(\mathsf{X})$ είναι η

$$\psi(\mathsf{X}) = \sum_{i=0}^{\infty} b_i \mathsf{X}^i \in K[\![\mathsf{X}]\!] \tag{3.2}$$

όπου $b_0 = a_0^{-1}$, $b_1 = -a_0^{-1} b_0 a_1$ και

$$b_i = -a_0^{-1}(b_{i-1}a_1 + \cdots + b_0 a_i),\ \forall i \in \mathbb{N}.$$

ΑΠΟΔΕΙΞΗ. Εάν η $\varphi(\mathsf{X})$ είναι αντιστρέψιμο στοιχείο τού δακτυλίου $K[\![\mathsf{X}]\!]$, έχουσα την $\sum_{i=0}^{\infty} b_i\mathsf{X}^i \in K[\![\mathsf{X}]\!]$ αντίστροφο, τότε $a_0b_0 = 1_K$, οπότε $a_0 \neq 0_K$. Και αντιστρόφως· εάν $a_0 \neq 0_K$, τότε μπορούμε να προσδιορίσουμε διαδοχικώς $b_0, b_1,..., b_i, b_{i+1},... \in K$, ούτως ώστε να ισχύουν οι ισότητες

$$\begin{cases} b_0a_0 = 1_K, \\ b_1a_0 + b_0a_1 = 0_K, \\ \vdots \\ b_ia_0 + b_{i-1}a_1 + \cdots + b_0a_i = 0_K, \\ \vdots \end{cases}$$

Προφανώς, $b_0 = a_0^{-1}$. Έστω τυχών φυσικός αριθμός $i \in \mathbb{N}$. Υποθέτοντας ότι έχουμε ήδη προσδιορίσει τα b_j, $j \in \{0, 1,..., i-1\}$, ορίζουμε ως b_i το

$$b_i := -a_0^{-1}(b_{i-1}a_1 + \cdots + b_0a_i).$$

Για την (3.2) ισχύει $\varphi(\mathsf{X})\psi(\mathsf{X}) = 1_K\ (= 1_{K[\![\mathsf{X}]\!]})$, οπότε $\psi(\mathsf{X}) = \varphi(\mathsf{X})^{-1}$ και ο ισχυρισμός είναι αληθής. □

3.1.4 Παραδείγματα. (i) Η επίτυπη δυναμοσειρά $\sum_{i=0}^{\infty} \mathsf{X}^i \in K[\![\mathsf{X}]\!]$ έχει ως αντίστροφό της την

$$\left(\sum_{i=0}^{\infty} \mathsf{X}^i\right)^{-1} = 1_K - \mathsf{X} + 0_K + 0_K + \cdots$$

(ii) Η $\sum_{i=0}^{\infty} \binom{i+k-1}{k-1}\mathsf{X}^i \in \mathbb{Q}[\![\mathsf{X}]\!]$ (όπου $k \in \mathbb{N}$) έχει ως αντίστροφό της την

$$\left(\sum_{i=0}^{\infty} \tbinom{i+k-1}{k-1}\mathsf{X}^i\right)^{-1} = (1-\mathsf{X})^k = \sum_{j=0}^{k} \tbinom{k}{j} (-1)^j\, \mathsf{X}^{k-j} + 0 + 0 + \cdots$$

(iii) Η $\sum_{i=0}^{\infty} \frac{1}{i!}\mathsf{X}^i \in \mathbb{C}[\![\mathsf{X}]\!]$ έχει ως αντίστροφό της την

$$\left(\sum_{i=0}^{\infty} \tfrac{1}{i!}\mathsf{X}^i\right)^{-1} = \sum_{i=0}^{\infty} \tfrac{(-1)^i}{i!}\mathsf{X}^i,$$

καθόσον ισχύει

$$\left(\sum_{i=0}^{\infty} \tfrac{1}{i!}\mathsf{X}^i\right)\left(\sum_{i=0}^{\infty} \tfrac{(-1)^i}{i!}\mathsf{X}^i\right) = \sum_{i=0}^{\infty}\left(\sum_{k=0}^{i} \tfrac{(-1)^k}{k!}\tfrac{1}{(i-k)!}\right)\mathsf{X}^i = 1,$$

λαμβανομένου υπ' όψιν τού ότι

$$\sum_{k=0}^{i} \tfrac{(-1)^k}{k!}\tfrac{1}{(i-k)!} = \tfrac{1}{i!}\sum_{k=0}^{i}(-1)^k\tbinom{i}{k} = \begin{cases} 0, & \text{όταν } i \neq 0, \\ 1, & \text{όταν } i = 0. \end{cases}$$

3.2 ΠΟΛΥΩΝΥΜΑ

Δοθέντος ενός σώματος K, θεωρούμε το υποσύνολο $K^{(\mathbb{N}_0)}$ τού συνόλου $K^{\mathbb{N}_0}$ το αποτελούμενο από τις ακολουθίες $(a_0, a_1, a_2,.....)$ με $a_i \in K$, $i = 0, 1, 2,...$, για τις οποίες υπάρχουν *το πολύ πεπερασμένου πλήθους* a_i που είναι διάφορα τού 0_K. Η τριάδα $(K^{(\mathbb{N}_0)}, +, \cdot)$ αποτελεί έναν υποδακτύλιο τού $(K^{\mathbb{N}_0}, +, \cdot)$ με μοναδιαίο στοιχείο του το $(1_K, 0_K, 0_K,...)$. Ταυτίζοντας το $K^{\mathbb{N}_0}$ με το σύνολο $K[\![\mathsf{X}]\!]$ των επίτυπων δυναμοσειρών μιας απροσδιορίστου X, ταυτίζουμε το $K^{(\mathbb{N}_0)}$ με το σύνολο $K[\mathsf{X}]$ των **πολυωνύμων** ως προς την απροσδιόριστο X, καθένα εκ των οποίων γράφεται υπό τη μορφή

$$(a_0, a_1,..., a_n, 0_K, 0_K,...) = a_0 + a_1\mathsf{X} + a_2\mathsf{X}^2 + \cdots + a_n\mathsf{X}^n =: \sum_{i=0}^{n} a_i\mathsf{X}^i,$$

όπου $a_i = 0_K$, για κάθε $i \geq n$, για κάποιον παγιωμένον $n \in \mathbb{N}_0$. Δυο πολυώνυμα

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i\mathsf{X}^i \in K[\mathsf{X}]\,, \quad \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j\mathsf{X}^j \in K[\mathsf{X}]$$

είναι **ίσα** ($\varphi(\mathsf{X}) = \psi(\mathsf{X})$) εάν και μόνον εάν *είτε* αμφότερα είναι ίσα με το μηδενικό στοιχείο $\mathbf{0}_{K[\mathsf{X}]}$ τού δακτυλίου $K[\mathsf{X}]$ *είτε*

$$\max\{\, i \in \{0,...,n\} |\, a_i \neq 0_K\} = \max\{\, j \in \{0,...,m\} |\, b_j \neq 0_K\} \;\; (=: k)$$

και $a_i = b_i$, $\forall i \in \{0,...,k\}$.

3.2.1 Ορισμός. Εάν $\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i\mathsf{X}^i \in K[\mathsf{X}]$ και $a_n \neq 0_K$, τότε λέμε ότι ο αριθμός $\deg(\varphi(\mathsf{X})) := n$ είναι **ο βαθμός** τού πολυωνύμου $\varphi(\mathsf{X})$, το a_0 **ο σταθερός όρος**, το $a_n\mathsf{X}^n$ ο **μεγιστοβάθμιος όρος** και το a_n ο **επικεφαλής συντελεστής** τού $\varphi(\mathsf{X})$. Όταν $a_n = 1_K$, το $\varphi(\mathsf{X})$ καλείται **μονικό** (ή, κατ' άλλους, **μονοστό**) **πολυώνυμο**. Για το **μηδενικό πολυώνυμο**, ήτοι για το μηδενικό στοιχείο $\mathbf{0}_{K[\mathsf{X}]}$ τού δακτυλίου $K[\mathsf{X}]$, θέτουμε εξ ορισμού $\deg(\mathbf{0}_{K[\mathsf{X}]}) := -\infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[2]: $-\infty < n$ για κάθε $n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο ο βαθμός των πολυωνύμων μπορεί να εκληφθεί ως μια απεικόνιση

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

Ένα πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ λέγεται **σταθερό πολυώνυμο** (ή απλώς μια **σταθερά** ανήκουσα στο K) όταν $\deg(\varphi(\mathsf{X})) \leq 0$.

[2]Επίσης, στο $\mathbb{N}_0 \cup \{-\infty\}$ θέτουμε $(-\infty) + (-\infty) := -\infty$, $(-\infty) \cdot (-\infty) := -\infty$ και $(-\infty) + n := n$, $(-\infty) \cdot n := -\infty$, $\forall n \in \mathbb{N}_0$.

3.2.2 Πρόταση. *Για οιαδήποτε* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ *ισχύουν τα εξής*:

(i) $\deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) \leq \max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\}$.

(ii) $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\} \Rightarrow \deg(\varphi(\mathsf{X})\psi(\mathsf{X})) = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$.

(iii) *Εάν* $\deg(\varphi(\mathsf{X})) \neq \deg(\psi(\mathsf{X}))$, *τότε*

$$\deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) = \max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\}. \tag{3.3}$$

ΑΠΟΔΕΙΞΗ. Εάν τουλάχιστον ένα εκ των $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι το μηδενικό πολυώνυμο, τότε τα (i) και (iii) είναι προφανώς αληθή. Ας υποθέσουμε ότι

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in K[\mathsf{X}]\,,\ a_n \neq 0_K, \quad \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in K[\mathsf{X}],\ \ b_m \neq 0_K,$$

όπου $n, m \in \mathbb{N}_0$, και ας ορίσουμε $a_i := 0_K$ για κάθε $i > n$ και $b_j := 0_K$ για κάθε $j > m$.

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

$$\varphi(\mathsf{X}) + \psi(\mathsf{X}) = \sum_{i=0}^{n} (a_i + b_i)\, \mathsf{X}^i, \tag{3.4}$$

οπότε $\deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) \leq n = \max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\}$.

(ii) Το γινόμενο των δύο πολυωνύμων μπορεί να γραφεί ως

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

όπου

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

Επειδή το K είναι ακεραία περιοχή (βλ. 2.3.16 (i)), έχουμε $a_n b_m \neq 0_K$. Κατά συνέπειαν, $\deg(\varphi(\mathsf{X})\psi(\mathsf{X})) = n + m = \deg(\varphi(\mathsf{X})) + \deg(\psi(\mathsf{X}))$.

(iii) Δίχως βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $n > m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_K$ και από την (3.4) έπεται ότι

$$\deg(\varphi(\mathsf{X}) + \psi(\mathsf{X})) = n = \max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\},$$

ήτοι ότι η (3.3) είναι αληθής. □

3.2.3 Πόρισμα. *Ο πολυωνυμικός δακτύλιος* $K[\mathsf{X}]$ *είναι ακεραία περιοχή.*

ΑΠΟΔΕΙΞΗ. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, όπου

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in K[\mathsf{X}]\ ,\ a_n \neq 0_K, \quad \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in K[\mathsf{X}],\ \ b_m \neq 0_K,$$

($n, m \in \mathbb{N}_0$), τότε $a_n b_m \neq 0_K$, διότι το K δεν διαθέτει μηδενοδιαιρέτες. Από το (ii) τής προτάσεως 3.2.2 λαμβάνουμε

$$\deg\left(\varphi(\mathsf{X})\psi(\mathsf{X})\right) = \deg\left(\varphi(\mathsf{X})\right) + \deg(\psi(\mathsf{X})) \in \mathbb{N}_0$$

και, ως εκ τούτου, $\varphi(\mathsf{X})\psi(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$. Άρα ούτε ο δακτύλιος $K[\mathsf{X}]$ δεν έχει μηδενοδιαιρέτες. □

3.3 ΔΙΑΙΡΕΤΟΤΗΤΑ ΠΟΛΥΩΝΥΜΩΝ

► **Ταυτότητα διαιρέσεως και μέγιστος κοινός διαιρέτης.** Έστω K ένα σώμα. Η γνωστή *ταυτότητα διαιρέσεως* η ισχύουσα στον δακτύλιο $\mathbb{Z}$ των ακεραίων, καθώς και οι έννοιες *μέγιστος κοινός διαιρέτης* και *ελάχιστο κοινό πολλαπλάσιο*, γενικεύονται και για τα στοιχεία τού δακτυλίου $K[\mathsf{X}]$.

3.3.1 Θεώρημα. (Ταυτότητα διαιρέσεως) *Δοθέντων δυο πολυωνύμων*

$$\varphi(\mathsf{X}) \in K[\mathsf{X}],\ \ \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\},$$

υπάρχει ένα ζεύγος ***μονοσημάντως ορισμένων*** *πολυωνύμων* $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, *ούτως ώστε να ισχύει*[3]

$$\boxed{\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg\left(\upsilon(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right).} \tag{3.5}$$

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Ύπαρξη των* $\varpi(\mathsf{X}), \upsilon(\mathsf{X})$. Εάν $\deg(\varphi(\mathsf{X})) < \deg(\psi(\mathsf{X}))$, τότε θέτουμε

$$\varpi(\mathsf{X}) := \mathbf{0}_{K[\mathsf{X}]},\ \ \upsilon(\mathsf{X}) := \varphi(\mathsf{X}).$$

Στην περίπτωση όπου $\deg(\varphi(\mathsf{X})) =: n \geq m := \deg(\psi(\mathsf{X})) \geq 0$ και

$$\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i,\ \psi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j\ \ (a_n \neq 0_K, b_m \neq 0_K),$$

[3] Όταν γράφουμε $\deg\left(r(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right)$ συμπεριλαμβάνουμε και την περίπτωση όπου $r(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}$ (επί τη βάσει τού ορισμού τής εννοίας τού βαθμού πολυωνύμου που εισήχθη στο εδάφιο 3.2.1).

χρησιμοποιούμε μαθηματική επαγωγή ως προς τον βαθμό n τού $\varphi(\mathsf{X})$. Εάν $n = 0$, τότε $m = 0$ και

$$\varphi(\mathsf{X}) = a_0, \;\; \psi(\mathsf{X}) = b_0 \neq 0_K,$$

οπότε αρκεί να θέσουμε $\varpi(\mathsf{X}) := a_0 b_0^{-1}$ και $\upsilon(\mathsf{X}) := \mathbf{0}_{K[\mathsf{X}]}$. Ας υποθέσουμε τώρα ότι $n \geq 1$ και ότι ο ισχυρισμός (που αφορά μόνον στην *ύπαρξη* τού εν λόγω ζεύγους πολυωνύμων) είναι αληθής για κάθε πολυώνυμο ανήκον στον $K[\mathsf{X}]$ και έχον βαθμό $< n$. Το πολυώνυμο

$$\widetilde{\varphi}(\mathsf{X}) := \varphi(\mathsf{X}) - (a_n b_m^{-1})\mathsf{X}^{n-m}\psi(\mathsf{X}) = \sum_{i=0}^{n-1} a_i \mathsf{X}^i - \sum_{j=0}^{m-1} (a_n b_m^{-1}) b_j \mathsf{X}^{n-m+j} \in K[\mathsf{X}]$$

έχει βαθμό $\leq n-1$. Κατά την επαγωγική μας υπόθεση υπάρχουν πολυώνυμα $\widetilde{\varpi}(\mathsf{X})$, $\widetilde{\upsilon}(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\widetilde{\varphi}(\mathsf{X}) = \widetilde{\varpi}(\mathsf{X})\psi(\mathsf{X}) + \widetilde{\upsilon}(\mathsf{X}), \quad \deg\left(\widetilde{\upsilon}(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right).$$

Επειδή $\varphi(\mathsf{X}) = \left((a_n b_m^{-1})\mathsf{X}^{n-m} + \widetilde{\varpi}(\mathsf{X})\right)\psi(\mathsf{X}) + \widetilde{\upsilon}(\mathsf{X})$, αρκεί να θέσουμε

$$\varpi(\mathsf{X}) := (a_n b_m^{-1})\mathsf{X}^{n-m} + \widetilde{\varpi}(\mathsf{X}), \;\; \upsilon(\mathsf{X}) := \widetilde{\upsilon}(\mathsf{X}).$$

Βήμα 2ο. *Μοναδικότητα των* $\varpi(\mathsf{X}), \upsilon(\mathsf{X})$. Έστω ότι η συνθήκη (3.5) ικανοποιείται από δύο ζεύγη πολυωνύμων $\varpi_1(\mathsf{X}), \upsilon_1(\mathsf{X})$ και $\varpi_2(\mathsf{X}), \upsilon_2(\mathsf{X})$:

$$\begin{aligned} \varphi(\mathsf{X}) &= \varpi_1(\mathsf{X})\psi(\mathsf{X}) + \upsilon_1(\mathsf{X}), \quad \deg\left(\upsilon_1(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right), \\ \varphi(\mathsf{X}) &= \varpi_2(\mathsf{X})\psi(\mathsf{X}) + \upsilon_2(\mathsf{X}), \quad \deg\left(\upsilon_2(\mathsf{X})\right) < \deg\left(\psi(\mathsf{X})\right). \end{aligned}$$

Τότε $\mathbf{0}_{K[\mathsf{X}]} = \varphi(\mathsf{X}) - \varphi(\mathsf{X}) = \left(\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X})\right)\psi(\mathsf{X}) + \left(\upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X})\right)$, οπότε

$$\left(\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X})\right)\psi(\mathsf{X}) = \upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X}).$$

Εάν ίσχυε $\varpi_1(\mathsf{X}) \neq \varpi_2(\mathsf{X})$, τότε θα είχαμε

$$\deg(\psi(\mathsf{X})) \leq \deg\left(\left(\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X})\right)\psi(\mathsf{X})\right) = \deg(\upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Άτοπο! Συνεπώς, $\varpi_1(\mathsf{X}) = \varpi_2(\mathsf{X})$ και, ως εκ τούτου, $\upsilon_1(\mathsf{X}) = \upsilon_2(\mathsf{X})$. □

3.3.2 Ορισμός. Το πολυώνυμο $\varpi(\mathsf{X})$ στην (3.5) ονομάζεται **πηλίκο** και το $\upsilon(\mathsf{X})$ **υπόλοιπο** τής διαιρέσεως τού $\varphi(\mathsf{X})$ διά τού $\psi(\mathsf{X})$. Όταν $\upsilon(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}$, λέμε ότι το $\psi(\mathsf{X})$ **διαιρεί** (επακριβώς) το $\varphi(\mathsf{X})$ ή ότι το $\psi(\mathsf{X})$ είναι **διαιρέτης** τού $\varphi(\mathsf{X})$ ή ότι το $\varphi(\mathsf{X})$ είναι (πολυωνυμικό) **πολλαπλάσιο** τού $\psi(\mathsf{X})$. (Εν τοιαύτη περιπτώσει χρησιμοποιείται ο συμβολισμός[4]: $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$). Όταν $\upsilon(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}$ και $\deg(\varpi(\mathsf{X})) \geq 1$, το $\psi(\mathsf{X})$ καλείται **γνήσιος διαιρέτης** τού $\varphi(\mathsf{X})$.

[4]Κατ' αντιδιαστολήν, μέσω τού συμβολισμού $\psi(\mathsf{X}) \nmid \varphi(\mathsf{X})$ υποδηλούται ότι το πολυώνυμο $\psi(\mathsf{X})$ δεν διαιρεί (επακριβώς) το πολυώνυμο $\varphi(\mathsf{X})$.

3.3.3 Πρόταση. *Εάν τα* $\theta(\mathsf{X})$, $\varphi(\mathsf{X})$ *και* $\psi(\mathsf{X}), \psi_1(\mathsf{X}),...,\psi_k(\mathsf{X})$ $(k \in \mathbb{N}, k \geq 2)$ *είναι πολυώνυμα ανήκοντα στον* $K[\mathsf{X}]$, *τότε ισχύουν τα ακόλουθα*:

(i) *Εάν* $\varphi(\mathsf{X}) \mid \psi_i(\mathsf{X}), \forall i \in \{1,...,k\}$, *τότε* $\varphi(\mathsf{X}) \mid \sum_{i=1}^{k} \omega_i(\mathsf{X})\psi_i(\mathsf{X})$ *για οιαδήποτε* $\omega_1(\mathsf{X}),...,\omega_k(\mathsf{X}) \in K[\mathsf{X}]$.

(ii) *Εάν* $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ *και* $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$, *τότε* $\psi(\mathsf{X}) \mid \theta(\mathsf{X})$.

(iii) $a \mid \theta(\mathsf{X})$ *για κάθε* $a \in K \setminus \{0_K\}$.

(iv) *Εάν* $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$, *όπου* $\theta(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$, *τότε* $\deg(\varphi(\mathsf{X})) \leq \deg(\theta(\mathsf{X}))$.

(v) *Εάν* $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ *και* $\theta(\mathsf{X}) \mid \varphi(\mathsf{X})$, *τότε* $\theta(\mathsf{X}) = a\varphi(\mathsf{X})$, *για κάποιο* $a \in K \setminus \{0_K\}$.

ΑΠΟΔΕΙΞΗ. Αφήνεται ως άσκηση. □

3.3.4 Λήμμα. *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$ *είναι δυο μονικά πολώνυμα με* $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})$ *και* $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$, *τότε* $\varphi(\mathsf{X}) = \psi(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, υπάρχουν $\varpi(\mathsf{X}), \varpi'(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, τέτοια ώστε να ισχύουν οι ισότητες $\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X})$ και $\psi(\mathsf{X}) = \varpi'(\mathsf{X})\varphi(\mathsf{X})$. Επομένως, $\varphi(\mathsf{X}) = \varpi(\mathsf{X})\varpi'(\mathsf{X})\varphi(\mathsf{X})$ και το (ii) τής προτάσεως 3.2.2 δίδει

$$\left.\begin{array}{r} \deg(\varpi(\mathsf{X})\varpi'(\mathsf{X})) = \deg(\varpi(\mathsf{X})) + \deg(\varpi'(\mathsf{X})) \\ \varpi(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]} \Rightarrow \deg(\varpi(\mathsf{X})) \geq 0 \\ \varpi'(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]} \Rightarrow \deg(\varpi'(\mathsf{X})) \geq 0 \end{array}\right\} \Rightarrow \deg(\varpi(\mathsf{X})) = \deg(\varpi'(\mathsf{X})) = 0,$$

απ' όπου προκύπτει ότι $\varpi(\mathsf{X}) = \varpi'(\mathsf{X}) = 1_K$ (διότι τα $\varpi(\mathsf{X}), \varpi'(\mathsf{X})$ είναι κατ' ανάγκην μονικά πολυώνυμα) και, κατ' επέκτασιν, ότι $\varphi(\mathsf{X}) = \psi(\mathsf{X})$. □

3.3.5 Ορισμός. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, τότε ένα πολυώνυμο $\delta(\mathsf{X}) \in K[\mathsf{X}]$ καλείται **μέγιστος κοινός διαιρέτης των** $\varphi(\mathsf{X})$ **και** $\psi(\mathsf{X})$ (εντός τού $K[\mathsf{X}]$) όταν ισχύουν τα εξής:

(i) Το $\delta(\mathsf{X})$ είναι *κοινός διαιρέτης* των πολυωνύμων $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, ήτοι $\delta(\mathsf{X}) \mid \varphi(\mathsf{X})$ και $\delta(\mathsf{X}) \mid \psi(\mathsf{X})$.

(ii) Εάν $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι *τυχών* κοινός διαιρέτης των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, δηλαδή εάν $\theta(\mathsf{X}) \mid \varphi(\mathsf{X})$ και $\theta(\mathsf{X}) \mid \psi(\mathsf{X})$, τότε $\theta(\mathsf{X}) \mid \delta(\mathsf{X})$.

(iii) Το $\delta(\mathsf{X})$ είναι μονικό πολυώνυμο[5].

3.3.6 Πρόταση. *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, *τότε υπάρχει ένας και μόνον μέγιστος κοινός διαιρέτης* $\delta(\mathsf{X})$ *των* $\varphi(\mathsf{X})$ *και* $\psi(\mathsf{X})$. *Επιπροσθέτως, υπάρχουν* $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, *τέτοια ώστε να ισχύει* $\delta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})$.

[5] Στο πλαίσιο τής (γενικής) Θεωρίας Δακτυλίων είθισται να μην συμπεριλαμβάνουμε τη συνθήκη (iii) στον ορισμό. Εν τοιαύτη περιπτώσει, ο μέγιστος κοινός διαιρέτης είναι μονοσημάντως ορισμένος *μόνον μέχρις πολλαπλασιασμού με κάποια μη μηδενική σταθερά* ανήκουσα στο K. Εδώ, δεν πρόκειται να χρησιμοποιήσουμε τη γενίκευση αυτού τού είδους. Θα αρκεσθούμε στη θεώρηση τού *αυστηρώς* μονοσημάντως ορισμένου, «διακεκριμένου» *μονικού* μεγίστου κοινού διαιρέτη των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Ύπαρξη τού μεγίστου κοινού διαιρέτη.* Θεωρούμε το σύνολο $\mathcal{A} := \{\kappa(\mathsf{X})\varphi(\mathsf{X}) + \mu(\mathsf{X})\psi(\mathsf{X}) |\, \kappa(\mathsf{X}), \mu(\mathsf{X}) \in K[\mathsf{X}]\}$. Προφανώς, $\mathcal{A} \neq \varnothing$ (διότι αμφότερα τα $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ ανήκουν σε αυτό) και περιέχει μονικά πολυώνυμα (διότι εάν $\eta(\mathsf{X}) = \kappa(\mathsf{X})\varphi(\mathsf{X}) + \mu(\mathsf{X})\psi(\mathsf{X})$ είναι τυχόν μη μηδενικό στοιχείο του έχον το $c \in K\smallsetminus\{0_K\}$ ως επικεφαλής συντελεστή, τότε το μονικό πολυώνυμο $c^{-1}\eta(\mathsf{X}) = (c^{-1}\kappa(\mathsf{X}))\varphi(\mathsf{X}) + (c^{-1}\mu(\mathsf{X}))\psi(\mathsf{X})$ ανήκει σε αυτό). Επομένως, έχουμε τη δυνατότητα επιλογής ενός *μονικού* πολυωνύμου

$$\delta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}) \in \mathcal{A} \;\; (\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}])$$

βαθμού $\deg(\delta(\mathsf{X})) := \min\left\{\deg(\theta(\mathsf{X}))|\, \theta(\mathsf{X}) \in K[\mathsf{X}]\smallsetminus\{\mathbf{0}_{K[\mathsf{X}]}\}\right\}$. Αρκεί λοπόν να αποδειχθεί ότι το $\delta(\mathsf{X})$ πληροί τις συνθήκες (i) και (ii) τού ορισμού 3.3.5. Ξεκινούμε με την (ii). Εάν $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι *τυχών* κοινός διαιρέτης των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, τότε

$$\theta(\mathsf{X}) \mid \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}) = \delta(\mathsf{X})$$

λόγω τού (i) τής προτάσεως 3.3.3. Εν συνεχεία, για τον έλεγχο τού ότι το $\delta(\mathsf{X})$ πληροί *και* τη συνθήκη (i) θεωρούμε τυχόν

$$\gamma(\mathsf{X}) = \kappa(\mathsf{X})\varphi(\mathsf{X}) + \mu(\mathsf{X})\psi(\mathsf{X}) \in \mathcal{A} \;\; (\kappa(\mathsf{X}), \mu(\mathsf{X}) \in K[\mathsf{X}]).$$

Σύμφωνα με το θεώρημα 3.3.1 υπάρχει ένα ζεύγος μονοσημάντως ορισμένων πολυωνύμων $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\gamma(\mathsf{X}) = \varpi(\mathsf{X})\delta(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg(\upsilon(\mathsf{X})) < \deg(\delta(\mathsf{X})).$$

Εξ αυτού έπεται ότι

$$\begin{aligned}\upsilon(\mathsf{X}) &= \gamma(\mathsf{X}) - \varpi(\mathsf{X})\delta(\mathsf{X}) \\ &= \kappa(\mathsf{X})\varphi(\mathsf{X}) + \mu(\mathsf{X})\psi(\mathsf{X}) - \varpi(\mathsf{X})(\alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})) \\ &= (\kappa(\mathsf{X}) - \varpi(\mathsf{X})\alpha(\mathsf{X}))\varphi(\mathsf{X}) + (\mu(\mathsf{X}) - \varpi(\mathsf{X})\beta(\mathsf{X}))\psi(\mathsf{X}) \in \mathcal{A}.\end{aligned}$$

Εάν υποθέσουμε ότι $\upsilon(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$ έχον το $c \in K\smallsetminus\{0_K\}$ ως επικεφαλής συντελεστή, τότε το μονικό πολυώνυμο $c^{-1}\upsilon(\mathsf{X})$ ανήκει στο $\mathcal{A}$ και έχει βαθμό

$$0 \leq \deg(c^{-1}\upsilon(\mathsf{X})) = \deg(\upsilon(\mathsf{X})) < \deg(\delta(\mathsf{X})),$$

κάτι το οποίο αντίκειται στον ορισμό τού $\delta(\mathsf{X})$. Κατά συνέπειαν, $\upsilon(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}$ και $\delta(\mathsf{X}) \mid \gamma(\mathsf{X})$. Αυτό σημαίνει ότι το $\delta(\mathsf{X})$ είναι διαιρέτης όλων των στοιχείων τού $\mathcal{A}$ (άρα και των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$).

Βήμα 2ο. *Μοναδικότητα τού μεγίστου κοινού διαιρέτη.* Εάν εκτός τού ανωτέρω $\delta(\mathsf{X})$ υπάρχει και κάποιος άλλος μέγιστος κοινός διαιρέτης $\delta'(\mathsf{X})$ των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, τότε $\delta(\mathsf{X}) \mid \delta'(\mathsf{X})$ και $\delta'(\mathsf{X}) \mid \delta(\mathsf{X})$ (λόγω τής συνθήκης (ii) τού 3.3.5), οπότε $\delta(\mathsf{X}) = \delta'(\mathsf{X})$ δυνάμει τού λήμματος 3.3.4. □

3.3.7 Σημείωση. (i) Εφεξής θα συμβολίζουμε τον (επί τη βάσει τής προηγηθείσας προτάσεως 3.3.6 μονοσημάντως ορισμένο) μέγιστο κοινό διαιρέτη των πολυωνύμων $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ ως μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X}))$.

(ii) Εάν $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$, τότε μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) = c^{-1}\psi(\mathsf{X})$, όπου $c \in K\setminus\{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\psi(\mathsf{X})$.

(iii) Εάν αμφότερα τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι μηδενικά, τότε γενικεύουμε την έννοια τού μεγίστου κοινού διαιρέτη θέτοντας μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) := \mathbf{0}_{K[\mathsf{X}]}$. Εάν μόνον ένα εξ αυτών, ας πούμε το $\varphi(\mathsf{X})$, είναι μηδενικό, τότε θέτουμε *εξ ορισμού* μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) := c^{-1}\psi(\mathsf{X})$, όπου $c \in K\setminus\{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\psi(\mathsf{X})$ (γενικεύοντας το (ii) *και* σε αυτήν την περίπτωση).

(iv) Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ και $c_1, c_2 \in K\setminus\{0_K\}$, τότε

$$\boxed{\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \text{μκδ}(c_1\varphi(\mathsf{X}), c_2\psi(\mathsf{X})).}$$

Πράγματι· εάν $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ και $\delta'(\mathsf{X}) := \text{μκδ}(c_1\varphi(\mathsf{X}), c_2\psi(\mathsf{X}))$, τότε

$$\left.\begin{array}{l}[\delta(\mathsf{X}) \mid \varphi(\mathsf{X}),\ \varphi(\mathsf{X}) \mid c_1\varphi(\mathsf{X})] \Rightarrow \delta(\mathsf{X}) \mid c_1\varphi(\mathsf{X}) \\ [\delta(\mathsf{X}) \mid \psi(\mathsf{X}),\ \psi(\mathsf{X}) \mid c_2\psi(\mathsf{X})] \Rightarrow \delta(\mathsf{X}) \mid c_2\psi(\mathsf{X})\end{array}\right\} \Rightarrow \delta(\mathsf{X}) \mid \delta'(\mathsf{X})$$

(βλ. 3.3.3 (ii) και 3.3.5 (ii)). Από την άλλη μεριά,

$$\delta'(\mathsf{X}) \mid c_1\varphi(\mathsf{X}) \Rightarrow \exists\tilde{\varphi}(\mathsf{X}) \in K[\mathsf{X}]\setminus\{\mathbf{0}_{K[\mathsf{X}]}\} : c_1\varphi(\mathsf{X}) = \tilde{\varphi}(\mathsf{X})\delta'(\mathsf{X}).$$

Επομένως, $\varphi(\mathsf{X}) = c_1^{-1}\tilde{\varphi}(\mathsf{X})\delta'(\mathsf{X}) \Rightarrow \delta'(\mathsf{X}) \mid \varphi(\mathsf{X})$. Κατ' αναλογίαν, $\delta'(\mathsf{X}) \mid \psi(\mathsf{X})$. Άρα $\delta'(\mathsf{X}) \mid \delta(\mathsf{X})$. Κατά το λήμμα 3.3.4, $\delta(\mathsf{X}) = \delta'(\mathsf{X})$.

► **Ευκλείδειος αλγόριθμος**. Η πρόταση 3.3.6 διασφαλίζει μόνον την ύπαρξη και τη μοναδικότητα τού μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X}))$. Δεν περιγράφει κάποια μέθοδο υπολογισμού του. Ωστόσο, δοθέντων δυο πολυωνύμων $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{\mathbf{0}_{K[\mathsf{X}]}\}$ με $\deg(\psi(\mathsf{X})) \leq \deg(\varphi(\mathsf{X}))$, μπορούμε να προσδιορίσουμε επακριβώς τον μέγιστο κοινό διαιρέτη τους *μέσω επαλλήλων εφαρμογών τής ταυτότητας διαιρέσεως πολυωνύμων* (γενικεύοντας καταλλήλως τον γνωστό *ευκλείδειο αλγόριθμο* τον ισχύοντα στον δακτύλιο $\mathbb{Z}$ των ακεραίων). Πράγματι· υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}),\ \ \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Εάν $\upsilon(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}$, τότε ο μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ είναι γνωστός (βλ. 3.3.7 (ii)). Ειδάλλως, θέτουμε $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ και $\delta'(\mathsf{X}) := \text{μκδ}(\psi(\mathsf{X}), \upsilon(\mathsf{X}))$, και παρατηρούμε (κάνοντας χρήση τού (i) τής προτάσεως 3.3.3 και τού (ii) τού ορισμού 3.3.5) ότι

$$\left.\begin{array}{c}\delta(\mathsf{X}) \mid \varphi(\mathsf{X}) \\ \delta(\mathsf{X}) \mid \varphi(\mathsf{X}) - \varpi(\mathsf{X})\psi(\mathsf{X}) = \upsilon(\mathsf{X})\end{array}\right\} \Rightarrow \delta(\mathsf{X}) \mid \delta'(\mathsf{X})$$

και

$$\left.\begin{array}{c}\delta'(\mathsf{X}) \mid \psi(\mathsf{X}) \\ \delta(\mathsf{X}) \mid \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}) = \varphi(\mathsf{X})\end{array}\right\} \Rightarrow \delta'(\mathsf{X}) \mid \delta(\mathsf{X}).$$

Ως εκ τούτου, $\delta(\mathsf{X}) = \delta'(\mathsf{X})$ (βλ. λήμμα 3.3.4). Θέτοντας

$$\upsilon_0(\mathsf{X}) := \varphi(\mathsf{X}),\ \varpi_1(\mathsf{X}) := \varpi(\mathsf{X}),\ \upsilon_1(\mathsf{X}) := \psi(\mathsf{X}),\ \upsilon_2(\mathsf{X}) := \upsilon(\mathsf{X})$$

και επαναμβάνοντας διαδοχικώς την ίδια διαδικασία, προσδιορίζουμε μονοσημάντως ορισμένα πολυώνυμα $\upsilon_3(\mathsf{X}), \upsilon_4(\mathsf{X}),...$ και $\varpi_2(\mathsf{X}), \varpi_3(\mathsf{X}),...$ με

$$\left|\begin{array}{ll}\upsilon_0(\mathsf{X}) = \varpi_1(\mathsf{X})\,\upsilon_1(\mathsf{X}) + \upsilon_2(\mathsf{X}), & \deg(\upsilon_2(\mathsf{X})) < \deg(\upsilon_1(\mathsf{X})), \\ \upsilon_1(\mathsf{X}) = \varpi_2(\mathsf{X})\,\upsilon_2(\mathsf{X}) + \upsilon_3(\mathsf{X}), & \deg(\upsilon_3(\mathsf{X})) < \deg(\upsilon_2(\mathsf{X})), \\ \upsilon_2(\mathsf{X}) = \varpi_3(\mathsf{X})\,\upsilon_3(\mathsf{X}) + \upsilon_4(\mathsf{X}), & \deg(\upsilon_4(\mathsf{X})) < \deg(\upsilon_3(\mathsf{X})), \\ \vdots & \vdots \\ \upsilon_{n-2}(\mathsf{X}) = \varpi_{n-1}(\mathsf{X})\,\upsilon_{n-1}(\mathsf{X}) + \upsilon_n(\mathsf{X}), & \deg(\upsilon_n(\mathsf{X})) < \deg(\upsilon_{n-1}(\mathsf{X})), \\ \upsilon_{n-1}(\mathsf{X}) = \varpi_n(\mathsf{X})\,\upsilon_n(\mathsf{X}), & \end{array}\right. \tag{3.6}$$

όπου για κάποιον $n \geq 2$ έχουμε $\upsilon_i(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$ για κάθε $i \in \{0,...,n\}$ και κατ' ανάγκην $\upsilon_{n+1}(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}$ (διότι οι βαθμοί των $\upsilon_1(\mathsf{X}), \upsilon_2(\mathsf{X}), \upsilon_3(\mathsf{X}),...$ σχηματίζουν μια φθίνουσα ακολουθία εντός τού (επεκτεταμένου) συνόλου $\mathbb{N}_0 \cup \{-\infty\}$), και

$$\begin{aligned}&\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \text{μκδ}(\upsilon_0(\mathsf{X}), \upsilon_1(\mathsf{X})) = \text{μκδ}(\upsilon_1(\mathsf{X}), \upsilon_2(\mathsf{X})) \\ &= \text{μκδ}(\upsilon_2(\mathsf{X}), \upsilon_3(\mathsf{X})) = \cdots = \text{μκδ}(\upsilon_{n-1}(\mathsf{X}), \upsilon_n(\mathsf{X})) = \text{μκδ}(\upsilon_n(\mathsf{X}), \mathbf{0}_{K[\mathsf{X}]}).\end{aligned}$$

Εξ αυτών προκύπτει ότι

$$\boxed{\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \text{μκδ}(\upsilon_n(\mathsf{X}), \mathbf{0}_{K[\mathsf{X}]}) = c^{-1}\upsilon_n(\mathsf{X}),} \tag{3.7}$$

όπου $c \in K \setminus \{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\upsilon_n(\mathsf{X})$. Σημειωτέον ότι μέσω τού ανωτέρω ευκλειδείου αλγορίθμου έχουμε *και* τη δυνατότητα προσδιορισμού δυο πολυωνύμων $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοιων ώστε να ισχύει

$$\boxed{\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}).} \tag{3.8}$$

Προς τούτο θεωρούμε τα

$$\left\{\begin{array}{ll}\alpha_0(\mathsf{X}) := 1_K, & \beta_0(\mathsf{X}) := 0_K, \\ \alpha_1(\mathsf{X}) := 0_K, & \beta_1(\mathsf{X}) := 1_K, \\ \alpha_j(\mathsf{X}) = \alpha_{j-2}(\mathsf{X}) - \alpha_{j-1}(\mathsf{X})\varpi_{j-1}(\mathsf{X}), & \beta_j(\mathsf{X}) = \beta_{j-2}(\mathsf{X}) - \beta_{j-1}(\mathsf{X})\varpi_{j-1}(\mathsf{X}),\end{array}\right.$$

για κάθε $j \in \{2,...,n\}$, όπου τα $\varpi_1(\mathsf{X}), \varpi_2(\mathsf{X}),..., \varpi_n(\mathsf{X})$ είναι τα πηλίκα των διαιρέσεων (3.6).

3.3.8 Πρόταση. *Ως πολυώνυμα* $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, *τέτοια ώστε να ισχύει η* (3.8), *μπορούν να επιλεγούν τα*

$$\boxed{\alpha(\mathsf{X}) := c^{-1}\alpha_n(\mathsf{X})} \text{ και } \boxed{\beta(\mathsf{X}) := c^{-1}\beta_n(\mathsf{X}),} \tag{3.9}$$

όπου $c \in K \setminus \{0_K\}$ *είναι ο επικεφαλής συντελεστής τού* $\upsilon_n(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. Χρησιμοποιώντας τις διαιρέσεις (3.6) θα αποδείξουμε τις ισότητες

$$\upsilon_j(\mathsf{X}) = \alpha_j(\mathsf{X})\varphi(\mathsf{X}) + \beta_j(\mathsf{X})\psi(\mathsf{X}), \ \ \forall j \in \{0, 1, ..., n\}, \tag{3.10}$$

μέσω μαθηματικής επαγωγής ως προς τον j. Για $j = 0$ λαμβάνουμε

$$\varphi(\mathsf{X}) = \upsilon_0(\mathsf{X}) = 1_K \cdot \varphi(\mathsf{X}) + 0_K \cdot \psi(\mathsf{X}) = \alpha_0(\mathsf{X})\varphi(\mathsf{X}) + \beta_0(\mathsf{X})\psi(\mathsf{X}),$$

ενώ για $j = 1$,

$$\psi(\mathsf{X}) = \upsilon_1(\mathsf{X}) = 0_K \cdot \varphi(\mathsf{X}) + 1_K \cdot \psi(\mathsf{X}) = \alpha_1(\mathsf{X})\varphi(\mathsf{X}) + \beta_1(\mathsf{X})\psi(\mathsf{X}).$$

Υποθέτοντας ότι $\upsilon_j(\mathsf{X}) = \alpha_j(\mathsf{X})\varphi(\mathsf{X}) + \beta_j(\mathsf{X})\psi(\mathsf{X})$ για κάθε $j \in \{1, ..., k-1\}$, όπου $2 \leq k \leq n$, έχουμε $\upsilon_k(\mathsf{X}) = \upsilon_{k-2}(\mathsf{X}) - \varpi_{k-1}(\mathsf{X})\,\upsilon_{k-1}(\mathsf{X})$, οπότε, λόγω τής επαγωγικής υποθέσεώς μας,

$$\begin{aligned}
\upsilon_k(\mathsf{X}) &= \left(\alpha_{k-2}(\mathsf{X})\varphi(\mathsf{X}) + \beta_{k-2}(\mathsf{X})\psi(\mathsf{X})\right) - \varpi_{k-1}(\mathsf{X})\left(\alpha_{k-1}(\mathsf{X})\varphi(\mathsf{X}) + \beta_{k-1}(\mathsf{X})\psi(\mathsf{X})\right) \\
&= \left(\alpha_{k-2}(\mathsf{X}) - \alpha_{k-1}(\mathsf{X})\varpi_{k-1}(\mathsf{X})\right)\varphi(\mathsf{X}) + \left(\beta_{k-2}(\mathsf{X}) - \beta_{k-1}(\mathsf{X})\varpi_{k-1}(\mathsf{X})\right)\psi(\mathsf{X}) \\
&= \alpha_k(\mathsf{X})\varphi(\mathsf{X}) + \beta_k(\mathsf{X})\psi(\mathsf{X})
\end{aligned}$$

και οι (3.10) είναι όντως αληθείς. Για $j = n$ λαμβάνουμε

$$c^{-1}\upsilon_n(\mathsf{X}) = (c^{-1}\alpha_n(\mathsf{X}))\varphi(\mathsf{X}) + (c^{-1}\beta_n(\mathsf{X}))\psi(\mathsf{X}) = \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$$

(μέσω των ισοτήτων (3.7)). □

3.3.9 Σημείωση. Τα ως άνω προσδιορισθέντα πολυώνυμα (3.9) *δεν είναι* τα μόνα στοιχεία τού $K[\mathsf{X}]$ που ικανοποιούν την (3.8). Επί παραδείγματι, επειδή για τον $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$

$$\exists \zeta(\mathsf{X}), \theta(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = \delta(\mathsf{X})\zeta(\mathsf{X}), \ \psi(\mathsf{X}) = \delta(\mathsf{X})\theta(\mathsf{X}),$$

η ισότητα

$$\delta(\mathsf{X}) = (\alpha(\mathsf{X}) + \gamma(\mathsf{X})\theta(\mathsf{X}))\varphi(\mathsf{X}) + (\beta(\mathsf{X}) - \gamma(\mathsf{X})\zeta(\mathsf{X}))\psi(\mathsf{X})$$

ισχύει για *κάθε* $\gamma(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$ (!), καθόσον από τις

$$\delta(\mathsf{X})\zeta(\mathsf{X})\psi(\mathsf{X}) = \varphi(\mathsf{X})\psi(\mathsf{X}) = \psi(\mathsf{X})\varphi(\mathsf{X}) = \delta(\mathsf{X})\theta(\mathsf{X})\varphi(\mathsf{X})$$

προκύπτει ότι

$$\left.\begin{aligned} \delta(\mathsf{X})\left(\zeta(\mathsf{X})\psi(\mathsf{X}) - \theta(\mathsf{X})\varphi(\mathsf{X})\right) &= \mathbf{0}_{K[\mathsf{X}]} \\ \delta(\mathsf{X}) &\neq \mathbf{0}_{K[\mathsf{X}]} \end{aligned}\right\} \underset{3.2.3}{\Longrightarrow} \zeta(\mathsf{X})\psi(\mathsf{X}) = \theta(\mathsf{X})\varphi(\mathsf{X}).$$

3.3.10 Παράδειγμα. Για τα $\varphi(\mathsf{X}) := \frac{1}{2}\mathsf{X}^5 + \frac{1}{4}\mathsf{X}^4 - \frac{17}{10}\mathsf{X}^3 + \frac{7}{5}\mathsf{X}^2 - \frac{6}{5}\mathsf{X} + \frac{3}{4} \in \mathbb{Q}[\mathsf{X}]$ και $\psi(\mathsf{X}) := \mathsf{X}^2 + \frac{1}{2}\mathsf{X} - 5 \in \mathbb{Q}[\mathsf{X}]$ έχουμε

$$\begin{aligned}\varphi(\mathsf{X}) &= (\tfrac{1}{2}\mathsf{X}^3 + \tfrac{4}{5}\mathsf{X} + 1)\psi(\mathsf{X}) + (\tfrac{23}{10}\mathsf{X} + \tfrac{23}{4}),\\ \psi(\mathsf{X}) &= (\tfrac{10}{23}\mathsf{X} - \tfrac{20}{23})(\tfrac{23}{10}\mathsf{X} + \tfrac{23}{4}) + 0,\end{aligned}$$

οπότε $\text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \frac{10}{23}(\frac{23}{10}\mathsf{X} + \frac{23}{4}) = \mathsf{X} + \frac{5}{2}$. Επιπροσθέτως,

$$\mathsf{X} + \tfrac{5}{2} = \tfrac{10}{23}\varphi(\mathsf{X}) - \left(\tfrac{5}{23}x^3 + \tfrac{8}{23}x + \tfrac{10}{23}\right)\psi(\mathsf{X}).$$

► **Τι συμβαίνει όταν επεκτείνουμε το σώμα αναφοράς μας;** Βάσει των όσων προαναφέρθησαν, δοθέντων δυο πολυωνύμων $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$, γνωρίζουμε το πώς μπορούμε να προσδιορίσουμε τον μέγιστο κοινό τους διαιρέτη. Ερώτημα: Εάν L είναι μια επέκταση τού K, τότε τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$, θεωρούμενα ως πολυώνυμα *ανήκοντα στον* $L[\mathsf{X}]$, διαθέτουν ωσαύτως έναν (και μόνον) μέγιστο κοινό διαιρέτη αλλά *εντός τού* $L[\mathsf{X}]$. Πώς σχετίζονται αυτοί οι δύο μέγιστοι κοινοί διαιρέτες; Η απάντηση δίδεται στην ακόλουθη πρόταση.

3.3.11 Πρόταση. *Έστω ότι* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ *και ότι* L *είναι μια επέκταση τού* K. *Συμβολίζουμε ως* $\delta_K(\mathsf{X})$ *τον μέγιστο κοινό διαιρέτη των* $\varphi(\mathsf{X}), \psi(\mathsf{X})$ *εντός τού* $K[\mathsf{X}]$ *και ως* $\delta_L(\mathsf{X})$ *τον μέγιστο κοινό διαιρέτη των* $\varphi(\mathsf{X}), \psi(\mathsf{X})$ *εντός τού* $L[\mathsf{X}]$. *Τότε* $\delta_K(\mathsf{X}) = \delta_L(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. Εάν (τουλάχιστον) ένα εκ των $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι το μηδενικό πολυώνυμο, τότε ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι αμφότερα τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι μη μηδενικά. Τότε (σύμφωνα με το θεώρημα 3.3.1) υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}),\ \ \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})). \tag{3.11}$$

Κατ' αναλογίαν, υπάρχουν μονοσημάντως ορισμένα $\varpi'(\mathsf{X}), \upsilon'(\mathsf{X}) \in L[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi'(\mathsf{X})\psi(\mathsf{X}) + \upsilon'(\mathsf{X}),\ \ \deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Όμως η ισότητα (3.11) εξακολουθεί να ισχύει και *εντός τού* $L[\mathsf{X}]$ (διότι έχουμε $K[\mathsf{X}] \subseteq L[\mathsf{X}]$), οπότε (από την ιδιότητα τής μοναδικότητας πηλίκων και υπολοίπων) ισχύει κατ' ανάγκην

$$\varpi'(\mathsf{X}) = \varpi(\mathsf{X}) \in K[\mathsf{X}] \ \text{ και } \ \upsilon'(\mathsf{X}) = \upsilon(\mathsf{X}) \in K[\mathsf{X}].$$

Κατά συνέπειαν, ο κατάλογος των ισοτήτων που εμφανίζονται κατά την εκτέλεση τού ευκλειδείου αλγορίθμου *εντός τού* $L[\mathsf{X}]$ ταυτίζεται με τον κατάλογο (3.6) των

ισοτήτων που εμφανίζονται κατά την εκτέλεση τού ευκλειδείου αλγορίθμου *εντός τού* $K[\mathsf{X}]$. Εξ αυτού έπεται ότι $\delta_K(\mathsf{X}) = \delta_L(\mathsf{X})$. □

► **Μέγιστος κοινός διαιρέτης περισσοτέρων πολυωνύμων.** Άπαξ και έχει ορισθεί ο μέγιστος κοινός διαιρέτης *δύο* πολυωνύμων, ο μέγιστος κοινός διαιρέτης περισσοτέρων πολυωνύμων μπορεί να ορισθεί αναδρομικώς.

3.3.12 Ορισμός. Εάν $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, όπου $k \in \mathbb{N}$, $k \geq 3$, τότε ο **μέγιστος κοινός διαιρέτης** $\mu\kappa\delta(\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X}))$ των $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X})$ ορίζεται μέσω τού αναδρομικού τύπου

$$\mu\kappa\delta(\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X})) := \mu\kappa\delta(\mu\kappa\delta(\varphi_1(\mathsf{X}),...,\varphi_{k-1}(\mathsf{X})),\varphi_k(\mathsf{X})).$$

3.3.13 Πρόταση. *Εάν* $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, *όπου* $k \in \mathbb{N}$, $k \geq 2$, *τότε υφίστανται πολυώνυμα* $\omega_1(\mathsf{X}),...,\omega_k(\mathsf{X}) \in K[\mathsf{X}]$, *τέτοια ώστε να ισχύει*

$$\mu\kappa\delta(\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X})) = \omega_1(\mathsf{X})\varphi_1(\mathsf{X}) + \cdots + \omega_k(\mathsf{X})\varphi_k(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. Λόγω τού αναδρομικού ορισμού 3.3.12 τού μεγίστου κοινού διαιρέτη πολυωνύμων περισσοτέρων των δύο, η απόδειξη ανάγεται επαγωγικώς στην επαλήθευση τού ισχυρισμού όταν $k = 2$. Εν τοιαύτη περιπτώσει χρησιμοποιούμε την πρόταση 3.3.6. (Φυσικά, είναι δυνατός και ο ακριβής *προσδιορισμός* μιας τέτοιας k-άδας πολυωνύμων $\omega_1(\mathsf{X}),...,\omega_k(\mathsf{X}) \in K[\mathsf{X}]$ μέσω επαναλαμβανόμενης εφαρμογής τής προτάσεως 3.3.8.) □

3.3.14 Ορισμός. Έστω ότι $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, όπου $k \in \mathbb{N}$, $k \geq 2$. Λέμε ότι αυτά τα πολυώνυμα είναι

(i) **πρώτα μεταξύ τους** όταν $\mu\kappa\delta(\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X})) = 1_K$, και

(ii) **πρώτα μεταξύ τους (ή σχετικώς πρώτα) ανά δύο** όταν $\mu\kappa\delta(\varphi_i(\mathsf{X}),\varphi_j(\mathsf{X})) = 1_K$ για οιουσδήποτε $i, j \in \{1,...,k\}$, $i < j$.

(Σημειωτέον ότι εάν ικανοποιείται η συνθήκη (ii), τότε ικανοποιείται αυτομάτως και η συνθήκη (i). Ωστόσο, το αντίστροφο δεν είναι εν γένει αληθές όταν $k \geq 3$.)

3.3.15 Πόρισμα. *Εάν* $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, $k \in \mathbb{N}$, $k \geq 2$, *τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Τα* $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X})$ *είναι πρώτα μεταξύ τους.*

(ii) *Υφίστανται πολυώνυμα* $\omega_1(\mathsf{X}),...,\omega_k(\mathsf{X}) \in K[\mathsf{X}]$, *τέτοια ώστε να ισχύει*

$$\omega_1(\mathsf{X})\varphi_1(\mathsf{X}) + \cdots + \omega_k(\mathsf{X})\varphi_k(\mathsf{X}) = 1_K.$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Έπεται άμεσα από την πρόταση 3.3.13.

(ii)⇒(i) Προφανώς, $1_K \mid \omega_i(\mathsf{X})$, $\forall i \in \{1,...,k\}$. Επιπροσθέτως, για οιοδήποτε $\theta(\mathsf{X}) \in K[\mathsf{X}]$, για το οποίο ισχύει $\theta(\mathsf{X}) \mid \omega_i(\mathsf{X})$, $\forall i \in \{1,...,k\}$, έχουμε

$$\theta(\mathsf{X}) \mid \omega_1(\mathsf{X})\varphi_1(\mathsf{X}) + \cdots + \omega_k(\mathsf{X})\varphi_k(\mathsf{X}) = 1_K.$$

(Βλ. 3.3.3 (iii) και (i).) Επομένως, μκδ$(\varphi_1(\mathsf{X}),..., \varphi_k(\mathsf{X})) = 1_K$ (επί τη βάσει τού ορισμού 3.3.5). □

3.3.16 Πόρισμα. *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}), \theta(\mathsf{X}) \in K[\mathsf{X}]$ *με* μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) = 1_K$ *και υποθέσουμε ότι* $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})\theta(\mathsf{X})$, *τότε* $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το πόρισμα 3.3.15 υφίστανται $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει $\alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}) = 1_K$. Εάν $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})\theta(\mathsf{X})$, τότε

$$\theta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X})\theta(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})\theta(\mathsf{X})$$

με $\varphi(\mathsf{X}) \mid \alpha(\mathsf{X})\varphi(\mathsf{X})\theta(\mathsf{X})$ και $\varphi(\mathsf{X}) \mid \beta(\mathsf{X})\psi(\mathsf{X})\theta(\mathsf{X})$, οπότε $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$. □

3.3.17 Πόρισμα. *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}), \theta(\mathsf{X}) \in K[\mathsf{X}]$ *με* μκδ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) = 1_K$, *τότε ισχύει η συνεπαγωγή*

$$\left.\begin{array}{l}\varphi(\mathsf{X}) \mid \theta(\mathsf{X}) \\ \psi(\mathsf{X}) \mid \theta(\mathsf{X})\end{array}\right\} \Longrightarrow \varphi(\mathsf{X})\psi(\mathsf{X}) \mid \theta(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το πόρισμα 3.3.15 υφίστανται $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει $\alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X}) = 1_K$. Εάν $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ και $\psi(\mathsf{X}) \mid \theta(\mathsf{X})$, τότε

$$\theta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X})\theta(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})\theta(\mathsf{X})$$

με $\varphi(\mathsf{X})\psi(\mathsf{X}) \mid \varphi(\mathsf{X})\theta(\mathsf{X})$ και $\varphi(\mathsf{X})\psi(\mathsf{X}) \mid \psi(\mathsf{X})\theta(\mathsf{X})$, οπότε $\varphi(\mathsf{X})\psi(\mathsf{X}) \mid \theta(\mathsf{X})$. □

► **Ελάχιστο κοινό πολλαπλάσιο.** Ο ορισμός αυτού προκύπτει από τον 3.3.5 ύστερα από *εναλλαγή των ρόλων* διαιρετών και πολλαπλασίων ως ακολούθως:

3.3.18 Ορισμός. Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, τότε ένα $\eta(\mathsf{X}) \in K[\mathsf{X}]$ καλείται **ελάχιστο κοινό πολλαπλάσιο των** $\varphi(\mathsf{X})$ **και** $\psi(\mathsf{X})$ (εντός τού $K[\mathsf{X}]$) όταν ισχύουν τα εξής:

(i) Το $\eta(\mathsf{X})$ είναι *κοινό πολλαπλάσιο* των πολυωνύμων $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, ήτοι έχουμε $\varphi(\mathsf{X}) \mid \eta(\mathsf{X})$ και $\psi(\mathsf{X}) \mid \eta(\mathsf{X})$.

(ii) Εάν $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι *τυχόν* κοινό πολλαπλάσιο των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, δηλαδή εάν $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ και $\psi(\mathsf{X}) \mid \theta(\mathsf{X})$, τότε $\eta(\mathsf{X}) \mid \theta(\mathsf{X})$.

(iii) Το $\eta(\mathsf{X})$ είναι μονικό πολυώνυμο.

3.3.19 Πρόταση. *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, *τότε υπάρχει ένα και μόνον ελάχιστο κοινό πολλαπλάσιο* $\eta(\mathsf{X})$ *των* $\varphi(\mathsf{X})$ *και* $\psi(\mathsf{X})$. *Τούτο ορίζεται ως εξής:*

$$\eta(\mathsf{X}) := c^{-1}\varphi(\mathsf{X})\psi'(\mathsf{X}) = c^{-1}\psi(\mathsf{X})\varphi'(\mathsf{X}), \tag{3.12}$$

όπου $\varphi'(\mathsf{X}), \psi'(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$ *είναι τα μονοσημάντως ορισμένα πολυώνυμα για τα οποία ισχύει*

$$\varphi(\mathsf{X}) = \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))\varphi'(\mathsf{X}),\ \psi(\mathsf{X}) = \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))\psi'(\mathsf{X})$$

και c *ο επικεφαλής συντελεστής τού* $\varphi(\mathsf{X})\psi'(\mathsf{X}) = \psi(\mathsf{X})\varphi'(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Ύπαρξη τού ελαχίστου κοινού πολλαπλασίου.* Θέτοντας $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ παρατηρούμε ότι

$$\delta(\mathsf{X})\varphi(\mathsf{X})\psi'(\mathsf{X}) = \varphi(\mathsf{X})\psi(\mathsf{X}) = \psi(\mathsf{X})\varphi(\mathsf{X}) = \delta(\mathsf{X})\psi(\mathsf{X})\varphi'(\mathsf{X}),$$

απ' όπου προκύπτει ότι

$$\left.\begin{array}{r} \delta(\mathsf{X})\left(\varphi(\mathsf{X})\psi'(\mathsf{X}) - \psi(\mathsf{X})\varphi'(\mathsf{X})\right) = \mathbf{0}_{K[\mathsf{X}]} \\ \delta(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]} \end{array}\right\} \underset{3.2.3}{\Longrightarrow} \varphi(\mathsf{X})\psi'(\mathsf{X}) = \psi(\mathsf{X})\varphi'(\mathsf{X}).$$

Το (μέσω τής (3.12) οριζόμενο) *μονικό* πολυώνυμο $\eta(\mathsf{X})$ είναι (προφανώς) *κοινό πολλαπλάσιο* των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$. Έστω $\theta(\mathsf{X}) \in K[\mathsf{X}]$ *τυχόν* κοινό πολλαπλάσιο των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$. Τότε

$$\left\{\begin{array}{c} \exists \varphi''(\mathsf{X}) \in K[\mathsf{X}] : \theta(\mathsf{X}) = \varphi(\mathsf{X})\varphi''(\mathsf{X}) \\ \text{και } \exists \psi''(\mathsf{X}) \in K[\mathsf{X}] : \theta(\mathsf{X}) = \psi(\mathsf{X})\psi''(\mathsf{X}). \end{array}\right\}$$

Σύμφωνα με την πρόταση 3.3.6 υπάρχουν $\alpha(\mathsf{X}), \beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει $\delta(\mathsf{X}) = \alpha(\mathsf{X})\varphi(\mathsf{X}) + \beta(\mathsf{X})\psi(\mathsf{X})$. Προφανώς,

$$\begin{aligned} \delta(\mathsf{X}) &= \delta(\mathsf{X})\alpha(\mathsf{X})\varphi'(\mathsf{X}) + \delta(\mathsf{X})\beta(\mathsf{X})\psi'(\mathsf{X}) \\ &= \delta(\mathsf{X})(\alpha(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\psi'(\mathsf{X})) \end{aligned}$$

και

$$\left.\begin{array}{r} \delta(\mathsf{X})\left(\alpha(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\psi'(\mathsf{X}) - 1_K\right) = \mathbf{0}_{K[\mathsf{X}]} \\ \delta(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]} \end{array}\right\} \underset{3.2.3}{\Longrightarrow} \alpha(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\psi'(\mathsf{X}) = 1_K.$$

Εξ αυτού έπεται ότι

$$\begin{aligned} &(\alpha(\mathsf{X})\psi''(\mathsf{X}) + \beta(\mathsf{X})\varphi''(\mathsf{X}))\varphi(\mathsf{X})\psi'(\mathsf{X}) \\ &= \alpha(\mathsf{X})\underbrace{\varphi(\mathsf{X})\psi'(\mathsf{X})}_{=\psi(\mathsf{X})\varphi'(\mathsf{X})}\psi''(\mathsf{X}) + \beta(\mathsf{X})\underbrace{\varphi(\mathsf{X})\varphi''(\mathsf{X})}_{=\theta(\mathsf{X})}\psi'(\mathsf{X}) \\ &= \alpha(\mathsf{X})\theta(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\theta(\mathsf{X})\psi'(\mathsf{X}) = (\alpha(\mathsf{X})\varphi'(\mathsf{X}) + \beta(\mathsf{X})\psi'(\mathsf{X}))\theta(\mathsf{X}) = \theta(\mathsf{X}). \end{aligned}$$

Άρα το $\eta(\mathsf{X})$ είναι ελάχιστο κοινό πολλαπλάσιο των $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$, διότι

$$\left.\begin{array}{r} \eta(\mathsf{X}) \mid c\left(c^{-1}\varphi(\mathsf{X})\psi'(\mathsf{X})\right) = \varphi(\mathsf{X})\psi'(\mathsf{X}) \\ \varphi(\mathsf{X})\psi'(\mathsf{X}) \mid \theta(\mathsf{X}) \end{array}\right\} \Rightarrow \eta(\mathsf{X}) \mid \theta(\mathsf{X}).$$

Βήμα 2ο. *Μοναδικότητα τού ελαχίστου κοινού πολλαπλασίου.* Εάν τα $\eta(\mathsf{X}), \eta'(\mathsf{X})$ είναι ελάχιστα κοινά πολλαπλάσια των $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{\mathbf{0}_{K[\mathsf{X}]}\}$, τότε έχουμε $\eta(\mathsf{X}) \mid \eta'(\mathsf{X})$ και $\eta'(\mathsf{X}) \mid \eta(\mathsf{X})$ (λόγω τής 3.3.18 (ii)), οπότε $\eta(\mathsf{X}) = \eta'(\mathsf{X})$ δυνάμει τού λήμματος 3.3.4. □

3.3.20 Σημείωση. (i) Το ανωτέρω ορισθέν ελάχιστο κοινό πολλαπλάσιο δυο πολυωνύμων $\varphi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{\mathbf{0}_{K[\mathsf{X}]}\}$ και $\psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{\mathbf{0}_{K[\mathsf{X}]}\}$ θα σημειώνεται εφεξής ως εκπ$(\varphi(\mathsf{X}), \psi(\mathsf{X}))$.

(ii) Εάν $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$, τότε εκπ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) = c^{-1}\varphi(\mathsf{X})$, όπου $c \in K\setminus\{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\varphi(\mathsf{X})$.

(iii) Εάν αμφότερα τα $\varphi(\mathsf{X}), \psi(\mathsf{X})$ είναι μηδενικά, τότε γενικεύουμε την έννοια τού ελαχίστου κοινού πολλαπλασίου θέτοντας εκπ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) := \mathbf{0}_{K[\mathsf{X}]}$. Εάν μόνον ένα εξ αυτών, ας πούμε το $\psi(\mathsf{X})$, είναι μηδενικό, τότε θέτουμε *εξ ορισμού* εκπ$(\varphi(\mathsf{X}), \psi(\mathsf{X})) := c^{-1}\varphi(\mathsf{X})$, όπου $c \in K\setminus\{0_K\}$ είναι ο επικεφαλής συντελεστής τού $\varphi(\mathsf{X})$ (γενικεύοντας το (ii) *και* σε αυτήν την περίπτωση).

(iv) Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ και $c_1, c_2 \in K\setminus\{0_K\}$, τότε

$$\boxed{\text{εκπ}(\varphi(\mathsf{X}), \psi(\mathsf{X})) = \text{εκπ}(c_1\varphi(\mathsf{X}), c_2\psi(\mathsf{X})).}$$

Πράγματι· εάν $\eta(\mathsf{X}) := \text{εκπ}(\varphi(\mathsf{X}), \psi(\mathsf{X}))$ και $\eta'(\mathsf{X}) := \text{εκπ}(c_1\varphi(\mathsf{X}), c_2\psi(\mathsf{X}))$, τότε

$$\left.\begin{array}{l} [\varphi(\mathsf{X}) \mid c_1\varphi(\mathsf{X}),\, c_1\varphi(\mathsf{X}) \mid \eta'(\mathsf{X})] \Rightarrow \varphi(\mathsf{X}) \mid \eta'(\mathsf{X}) \\ [\psi(\mathsf{X}) \mid c_2\psi(\mathsf{X}),\, c_2\psi(\mathsf{X}) \mid \eta'(\mathsf{X})] \Rightarrow \psi(\mathsf{X}) \mid \eta'(\mathsf{X}) \end{array}\right\} \Rightarrow \eta(\mathsf{X}) \mid \eta'(\mathsf{X})$$

(βλ. 3.3.3 (ii) και 3.3.18 (ii)). Από την άλλη μεριά,

$$\left\{\begin{array}{l} \eta(\mathsf{X}) = c_1^{-1}\left(c_1\eta(\mathsf{X})\right) \Rightarrow c_1\eta(\mathsf{X}) \mid \eta(\mathsf{X}) \\ \eta(\mathsf{X}) = c_2^{-1}\left(c_2\eta(\mathsf{X})\right) \Rightarrow c_2\eta(\mathsf{X}) \mid \eta(\mathsf{X}) \end{array}\right\},$$

οπότε

$$\left.\begin{array}{l} [c_1\varphi(\mathsf{X}) \mid c_1\eta(\mathsf{X}),\, c_1\eta(\mathsf{X}) \mid \eta(\mathsf{X})] \Rightarrow c_1\varphi(\mathsf{X}) \mid \eta(\mathsf{X}) \\ [c_2\psi(\mathsf{X}) \mid c_2\eta(\mathsf{X}),\, c_2\eta(\mathsf{X}) \mid \eta(\mathsf{X})] \Rightarrow c_2\psi(\mathsf{X}) \mid \eta(\mathsf{X}) \end{array}\right\} \Rightarrow \eta'(\mathsf{X}) \mid \eta(\mathsf{X}).$$

Κατά το λήμμα 3.3.4, $\eta(\mathsf{X}) = \eta'(\mathsf{X})$.

(v) Άπαξ και έχει ορισθεί το ελάχιστο κοινό πολλαπλάσιο *δύο* πολυωνύμων, το ελάχιστο κοινό πολλαπλάσιο περισσοτέρων πολυωνύμων μπορεί να ορισθεί αναδρομικώς: Εάν $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, όπου $k \in \mathbb{N}$, $k \geq 3$, τότε

$$\text{εκπ}(\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X})) := \text{εκπ}(\text{εκπ}(\varphi_1(\mathsf{X}),...,\varphi_{k-1}(\mathsf{X})), \varphi_k(\mathsf{X})).$$

3.4 ΘΕΣΕΙΣ ΜΗΔΕΝΙΣΜΟΥ ΠΟΛΥΩΝΥΜΩΝ

3.4.1 Ορισμός. Για οιοδήποτε στοιχείο λ ενός σώματος K ορίζεται η **συνάρτηση** $\mathfrak{y}_\lambda$ **πολυωνυμικής αποτιμήσεως στο** λ ως εξής:

$$K[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i = \varphi(\mathsf{X}) \overset{\mathfrak{y}_\lambda}{\longmapsto} \mathfrak{y}_\lambda(\varphi(\mathsf{X})) := \varphi(\lambda) := \sum_{i=0}^{n} a_i \lambda^i \in K.$$

3.4.2 Σημείωση. Στο σχολείο είθισται να αντιμετωπίζουμε τα πολυώνυμα ως συνήθεις «συναρτήσεις» (επειδή εκεί γίνεται κυρίως χρήση των σωμάτων $\mathbb{Q}$ και $\mathbb{R}$). Ωστόσο, όταν κανείς θεωρεί *τυχόντα* σώματα K, πρέπει να γνωρίζει ότι κάτι τέτοιο *δεν* αληθεύει εν γένει. Εάν

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

τότε η **συνάρτηση η επαγομένη από το** $\varphi(\mathsf{X})$ είναι η

$$\mathfrak{v}_{\varphi(\mathsf{X})} : K \longrightarrow K, \quad \lambda \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})}(\lambda) := \mathfrak{y}_\lambda(\varphi(\mathsf{X})) = \varphi(\lambda) = \sum_{i=0}^{n} a_i \lambda^i.$$

Μέσω αυτής ορίζεται ο ομομορφισμός δακτυλίων

$$\boxed{K[\mathsf{X}] \longrightarrow K^K, \quad \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})},}$$

που δεν είναι κατ' ανάγκην μονομορφισμός δακτυλίων! Επί παραδείγματι, εάν $K = \mathbb{Z}_3$ και $\varphi(\mathsf{X}) = \mathsf{X} + \mathsf{X}^3, \psi(\mathsf{X}) = [2]_3\, \mathsf{X}$, τότε τα $\varphi(\mathsf{X})$ και $\psi(\mathsf{X})$ -ως πολυώνυμα- είναι διαφορετικά, ενώ

$$\begin{aligned} \mathfrak{v}_{\varphi(\mathsf{X})}([0]_3) &= [0]_3 = \mathfrak{v}_{\psi(\mathsf{X})}([0]_3), \\ \mathfrak{v}_{\varphi(\mathsf{X})}([1]_3) &= [2]_3 = \mathfrak{v}_{\psi(\mathsf{X})}([1]_3), \\ \mathfrak{v}_{\varphi(\mathsf{X})}([2]_3) &= [1]_3 = \mathfrak{v}_{\psi(\mathsf{X})}([2]_3), \end{aligned}$$

πράγμα που σημαίνει ότι $\mathfrak{v}_{\varphi(\mathsf{X})} = \mathfrak{v}_{\psi(\mathsf{X})}$. (Μια ικανή συνθήκη για να είναι ο ως άνω ομομορφισμός δακτυλίων μονομορφισμός δίδεται στο πόρισμα 3.4.9.)

3.4.3 Ορισμός. Έστω L μια επέκταση ενός σώματος K και έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$. Ένα στοιχείο $\lambda \in L$ ονομάζεται **θέση μηδενισμού**[6] (ή **σημείο μηδενισμού**) τού πολυωνύμου $\varphi(\mathsf{X})$ **εντός τού** L όταν

$$\mathfrak{y}_\lambda(\varphi(\mathsf{X}))) := \varphi(\lambda) = 0_L\ (= 0_K),$$

[6] 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 $\varphi(\mathsf{X}) \in \mathbb{C}[\mathsf{X}]$ μπορεί να μηδενίζεται όταν $\mathsf{X} = \lambda \in \mathbb{C}$, χωρίς, ωστόσο, το λ να προκύπτει από επίλυση τής εξισώσεως $\varphi(\mathsf{X}) = 0$ μέσω αποκλειστικής χρήσεως *ριζικών*. (Από την άλλη όμως μεριά, ονομάζουμε, π.χ., τις θέσεις μηδενισμού τής εξισώσεως $\mathsf{X}^\nu = 1$ ν-οστές *ρίζες τής μονάδας*.)

δηλαδή όταν η τιμή τού $\varphi(\mathsf{X})$ για $\mathsf{X} = \lambda$ είναι το μηδενικό στοιχείο.

3.4.4 Πρόταση. *Έστω K ένα σώμα. Εάν $\lambda \in K$ και $\varphi(\mathsf{X}) \in K[\mathsf{X}]$, τότε ισχύουν τα εξής:*

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

(ii) *Το λ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$ εντός τού K εάν και μόνον εάν*

$$\mathsf{X} - \lambda \mid \varphi(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. (i) Σύμφωνα με το θεώρημα 3.3.1 υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\varphi(\mathsf{X}) = (\mathsf{X} - \lambda)\varpi(\mathsf{X}) + \upsilon(\mathsf{X}), \;\; \deg(\upsilon(\mathsf{X})) < \deg(\mathsf{X} - \lambda) = 1.$$

Επομένως, $\upsilon(\mathsf{X}) = a \in K$, οπότε

$$a = \varphi(\mathsf{X}) - (\mathsf{X} - \lambda)\varpi(\mathsf{X}) \Longrightarrow a = \varphi(\lambda).$$

(ii) Το λ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$ (εντός τού K) εάν και μόνον εάν το υπόλοιπο τής διαιρέσεως τού $\varphi(\mathsf{X})$ διά τού $\mathsf{X} - \lambda$ είναι το $\mathbf{0}_{K[\mathsf{X}]}$, πράγμα που σημαίνει ότι $\mathsf{X} - \lambda \mid \varphi(\mathsf{X})$. □

3.4.5 Πόρισμα. *Εάν τα στοιχεία $\lambda_1, ..., \lambda_k \in K$ ($k \in \mathbb{N}$) είναι k σαφώς διακεκριμένες θέσεις μηδενισμού ενός πολυωνύμου $\varphi(\mathsf{X}) \in K[\mathsf{X}]$, τότε*

$$(\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2) \cdots (\mathsf{X} - \lambda_k) \mid \varphi(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. Όταν $k = 1$, αυτό είναι αληθές λόγω τής προτάσεως 3.4.4. Θα εργασθούμε με τη βοήθεια τής μαθηματικής επαγωγής. Υποθέτουμε ότι ο ισχυρισμός είναι αληθής για $k - 1$ θέσεις μηδενισμού, οπότε

$$\varphi(\mathsf{X}) = (\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2) \cdots (\mathsf{X} - \lambda_{k-1})\,\psi(\mathsf{X})$$

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

$$0_K = \varphi(\lambda_k) = (\lambda_k - \lambda_1)(\lambda_k - \lambda_2) \cdots (\lambda_k - \lambda_{k-1})\,\psi(\lambda_k),$$

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

3.4.6 Πόρισμα. *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$ διαθέτει (συνολικώς) το πολύ $\deg(\varphi(\mathsf{X}))$ θέσεις μηδενισμού εντός τού K.*

ΑΠΟΔΕΙΞΗ. Έπεται από το πόρισμα 3.4.5 και το (iv) τής προτάσεως 3.3.3. □

3.4.7 Πόρισμα. *Εάν ένα πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ διαθέτει εντός τού K θέσεις μηδενισμού, το πλήθος των οποίων υπερβαίνει τον βαθμό του, τότε το $\varphi(\mathsf{X})$ είναι το μηδενικό πολυώνυμο.*

3.4.8 Πόρισμα. *Εάν δυο πολυώνυμα $\varphi(\mathsf{X}),\, \psi(\mathsf{X}) \in K[\mathsf{X}] \smallsetminus \{\mathbf{0}_{K[\mathsf{X}]}\}$ λαμβάνουν τις ίδιες τιμές σε σαφώς διακεκριμένα στοιχεία τού K, το πλήθος των οποίων υπερβαίνει το $\max\{\deg(\varphi(\mathsf{X})), \deg(\psi(\mathsf{X}))\}$, τότε έχουμε $\varphi(\mathsf{X}) = \psi(\mathsf{X})$.*

3.4.9 Πόρισμα. *Εάν το (υποκείμενο σύνολο ενός σώματος) K είναι απειροσύνολο, τότε η*

$$K\,[\mathsf{X}] \longrightarrow K^K, \quad \varphi(\mathsf{X}) \longmapsto \mathfrak{v}_{\varphi(\mathsf{X})},$$

(βλ. 3.4.2*) αποτελεί έναν μονομορφισμό δακτυλίων.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντα πολυώνυμα $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ και τις αντίστοιχες συναρτήσεις $\mathfrak{v}_{\varphi(\mathsf{X})}$ και $\mathfrak{v}_{\psi(\mathsf{X})}$. Εάν ισχύει $\mathfrak{v}_{\varphi(\mathsf{X})} = \mathfrak{v}_{\psi(\mathsf{X})}$, τότε η διαφορά $\varphi(\mathsf{X}) - \psi(\mathsf{X})$ έχει ως θέσεις μηδενισμού της όλα τα στοιχεία τού (υποκειμένου συνόλου τού) K. Συνεπώς, δυνάμει τού πορίσματος 3.4.7 έχουμε $\varphi(\mathsf{X}) - \psi(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}$, ήτοι $\varphi(\mathsf{X}) = \psi(\mathsf{X})$. □

3.4.10 Πρόταση. (Τύπος παρεμβολής τού Lagrange) *Έστω $n \in \mathbb{N}$ και έστω K ένα σώμα με πληθικό αριθμό $\operatorname{card}(K) \geq n+1$. Εάν τα $a_0, a_1, ..., a_n$ είναι $n+1$ σαφώς διακεκριμένα στοιχεία τού K και τα $c_0, c_1, ..., c_n$ τυχόντα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία τού K, τότε υπάρχει ένα μονοσημάντως ορισμένο πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $\leq n$ (βλ.* (3.14)*), τέτοιο ώστε να ισχύει*

$$\varphi(a_k) = c_k, \;\; \forall k \in \{0, 1, ..., n\}.$$

ΑΠΟΔΕΙΞΗ. Το ότι ένα τέτοιου είδους πολυώνυμο θα είναι μονοσημάντως ορισμένο έπεται προφανώς από το πόρισμα 3.4.8. Αρκεί λοιπόν να αποδειχθεί η ύπαρξή του. Προς τούτο ορίζουμε πολυώνυμα $\ell_i(\mathsf{X}) \in K[\mathsf{X}]$, $0 \leq i \leq n$, ως εξής:

$$\boxed{\ell_i(\mathsf{X}) := \prod_{j \in \{0,1,..,n\} \smallsetminus \{i\}} (a_i - a_j)^{-1} (\mathsf{X} - a_j)\,.} \tag{3.13}$$

Προφανώς, $\deg(\ell_i(\mathsf{X})) = n$ και για κάθε $(i,k) \in \{0,1,...,n\} \times \{0,1,...,n\}$ έχουμε

$$\ell_i(a_k) = \begin{cases} 0_K, & \text{όταν } i \neq k, \\ 1_K, & \text{όταν } i = k. \end{cases}$$

Κατά συνέπειαν, το πολυώνυμο

$$\boxed{\varphi(\mathsf{X}) := \sum_{i=0}^{n} c_i \ell_i(\mathsf{X})} \tag{3.14}$$

έχει την επιθυμητή ιδιότητα. □

3.4.11 Ορισμός. Τα (3.13) ονομάζονται **πολυώνυμα τού Lagrange**[7] (για τα στοιχεία $a_0, a_1, ..., a_n$), ενώ ο τύπος (3.14), ο οποίος μας παρέχει το $\varphi(\mathsf{X})$, είναι γνωστός ως **τύπος παρεμβολής τού Lagrange**.

3.4.12 Παράδειγμα. Εάν $K = \mathbb{Q}$, $n = 4$, και

$$\left\{ \begin{array}{llllll} a_0 = -5, & a_1 = -2, & a_2 = 0, & a_3 = 2, & a_4 = 5, \\ c_0 = 0, & c_1 = -3, & c_2 = 0, & c_3 = 0, & c_4 = 1 \end{array} \right\}$$

τότε τα πολυώνυμα τού Lagrange που απαιτούνται είναι μόνον τα

$$\left\{ \begin{array}{l} \ell_1(\mathsf{X}) = -\frac{1}{168}\mathsf{X}\,(\mathsf{X}-2)\,(\mathsf{X}-5)\,(\mathsf{X}+5)\,, \\ \ell_4(\mathsf{X}) = \frac{1}{1050}\mathsf{X}\,(\mathsf{X}-2)\,(\mathsf{X}+2)\,(\mathsf{X}+5)\,. \end{array} \right.$$

Ο τύπος παρεμβολής τού Lagrange δίδει το πολυώνυμο

$$\varphi(\mathsf{X}) = c_1\ell_1(\mathsf{X}) + c_4\ell_4(\mathsf{X}) = \tfrac{79}{4200}\mathsf{X}^4 - \tfrac{13}{420}\mathsf{X}^3 - \tfrac{1891}{4200}\mathsf{X}^2 + \tfrac{367}{420}\mathsf{X}.$$

3.4.13 Ορισμός. Έστω K τυχόν σώμα και έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$. Για κάθε $\lambda \in K$ θέτουμε

$$\boxed{\text{mult}\,(\varphi(\mathsf{X}); \lambda) := \max\left\{k \in \mathbb{N}_0 : (\mathsf{X}-\lambda)^k \mid \varphi(\mathsf{X})\right\}.}$$

Προφανώς, εάν $\text{mult}(\varphi(\mathsf{X}); \lambda) = m$, τότε $m \geq 1 \Leftrightarrow$ το λ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$. Όταν $m \geq 1$, λέμε ότι το λ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$ *με πλήθος πολλαπλών εμφανίσεων* ή -απλούστερα- **με πολλαπλότητα** ίση με m. Το λ ονομάζεται, ιδιαιτέρως, **απλή** (και αντιστοίχως, **πολλαπλή** ή **επαναλαμβανόμενη**) **θέση μηδενισμού** τού $\varphi(\mathsf{X})$ όταν $m = 1$ (και αντιστοίχως, όταν $m \geq 2$).

3.4.14 Πρόταση. *Εάν $\varphi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, $\lambda \in K$ και $m \in \mathbb{N}$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\text{mult}(\varphi(\mathsf{X}); \lambda) = m$.

(ii) $\exists \psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X})$ *με* $\psi(\lambda) \neq 0_K$.

[7] Προς τιμήν τού Joseph-Louis Lagrange (1736-1813) ο οποίος δημοσίευσε ένα άρθρο επ' αυτών το 1795 (αν και είχαν ανακαλυφθεί ήδη από το 1779 από τον Edward Waring (1736-1798) και απέρρεαν εύκολα και από έναν άλλον τύπο δημοσιευθέντα το 1783 από τον Leonhand Euler (1707-1783)).

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $\text{mult}(\varphi(\mathsf{X});\lambda) = m$, τότε $(\mathsf{X}-\lambda)^m \mid \varphi(\mathsf{X})$, οπότε υπάρχει κάποιο $\psi(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$ με $\varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X})$. Εάν ίσχυε $\psi(\lambda) = 0_K$, τότε (σύμφωνα με το (ii) τής προτάσεως 3.4.4) θα είχαμε $\mathsf{X}-\lambda \mid \psi(\mathsf{X})$, οπότε $(\mathsf{X}-\lambda)^{m+1} \mid \varphi(\mathsf{X})$, κάτι που θα αντέκειτο στον ορισμό τής πολλαπλότητας τής θέσεως μηδενισμού λ τού $\varphi(\mathsf{X})$. Άρα $\psi(\lambda) \neq 0_K$.

(ii)⇒(i) Εάν $\exists\psi(\mathsf{X}) \in K[\mathsf{X}]\smallsetminus\{\mathbf{0}_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X})$ με $\psi(\lambda) \neq 0_K$, τότε $(\mathsf{X}-\lambda)^m \mid \varphi(\mathsf{X})$. Ας υποθέσουμε ότι υπάρχει κάποιος $m' \in \mathbb{N}$, $m' > m$, με $(\mathsf{X}-\lambda)^{m'} \mid \varphi(\mathsf{X})$. Τότε υπάρχει κάποιο $\theta(\mathsf{X}) \in K[\mathsf{X}]\smallsetminus\{\mathbf{0}_{K[\mathsf{X}]}\}$, τέτοιο ώστε να ισχύει

$$\varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X}) = (\mathsf{X}-\lambda)^{m'}\,\theta(\mathsf{X}).$$

Εξ αυτού έπεται ότι

$$(\mathsf{X}-\lambda)^m\,\psi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,(\mathsf{X}-\lambda)^{m'-m}\,\theta(\mathsf{X}) \Longrightarrow \psi(\mathsf{X}) = (\mathsf{X}-\lambda)^{m'-m}\,\theta(\mathsf{X}),$$

ήτοι ότι $\psi(\lambda) = 0_K$. Άτοπο! Επομένως, $\text{mult}(\varphi(\mathsf{X});\lambda) = m$. □

3.4.15 Ορισμός. Ως **απεικόνιση επίτυπης παραγωγίσεως** (ή **τύποις παραγωγίσεως**) ορίζεται η

$$\boxed{\mathcal{D} : K[\mathsf{X}] \longrightarrow K[\mathsf{X}],\ \mathcal{D}\left(\sum_{i=0}^{n} a_i\mathsf{X}^i\right) := \sum_{i=1}^{n} i a_i \mathsf{X}^{i-1}.}$$

Η εικόνα $\mathcal{D}(\varphi(\mathsf{X}))$ ενός πολυωνύμου $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ μέσω αυτής καλείται **επίτυπη παράγωγος** (ή **τύποις παράγωγος**) τού $\varphi(\mathsf{X})$.

3.4.16 Λήμμα. *Εάν $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ και $c \in K$, τότε ισχύουν τα εξής*:

(i) $\mathcal{D}(c\,\varphi(\mathsf{X})) = c\,\mathcal{D}(\varphi(\mathsf{X}))$.

(ii) $\mathcal{D}(\varphi(\mathsf{X}) + \psi(\mathsf{X})) = \mathcal{D}(\varphi(\mathsf{X})) + \mathcal{D}(\psi(\mathsf{X}))$.

(iii) $\mathcal{D}(\varphi(\mathsf{X})\psi(\mathsf{X})) = \mathcal{D}(\varphi(\mathsf{X}))\psi(\mathsf{X}) + \mathcal{D}(\psi(\mathsf{X}))\varphi(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. Έστω ότι $\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i\mathsf{X}^i$ και $\psi(\mathsf{X}) = \sum_{j=0}^{m} b_j\mathsf{X}^j$. Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $n \geq m$ και θέτουμε $b_i := 0_K$ για κάθε δείκτη $i \in \{m+1,...,n\}$.

(i)-(ii) Προφανώς,

$$\begin{aligned}\mathcal{D}(c\,\varphi(\mathsf{X})) &= \mathcal{D}(c\sum_{i=0}^{n} a_i\mathsf{X}^i) = \mathcal{D}(\sum_{i=0}^{n} c a_i\mathsf{X}^i)\\ &= \sum_{i=1}^{n} c i a_i \mathsf{X}^{i-1} = c\sum_{i=1}^{n} i a_i\mathsf{X}^{i-1} = c\,\mathcal{D}(\varphi(\mathsf{X}))\end{aligned}$$

και

$$\begin{aligned}\mathcal{D}(\varphi(\mathsf{X}))+\mathcal{D}(\psi(\mathsf{X})) &= \sum_{i=1}^{n} i a_i \mathsf{X}^{i-1}+\sum_{j=1}^{m} j b_j \mathsf{X}^{j-1}\\ &= \sum_{i=1}^{n} i(a_i+b_i)\mathsf{X}^{i-1}=\mathcal{D}(\varphi(\mathsf{X})+\psi(\mathsf{X})).\end{aligned}$$

(iii) Κατ' αρχάς παρατηρούμε ότι για κάθε $(i,j)\in\mathbb{N}_0\times\mathbb{N}_0$ με $(i,j)\neq(0,0)$ ισχύει

$$\begin{aligned}\mathcal{D}(\mathsf{X}^i\mathsf{X}^j) &= \mathcal{D}(\mathsf{X}^{i+j})=(i+j)\mathsf{X}^{i+j-1}\\ &= \left(i\mathsf{X}^{i-1}\right)\mathsf{X}^j+\left(j\mathsf{X}^{j-1}\right)\mathsf{X}^i=\mathcal{D}(\mathsf{X}^i)\mathsf{X}^j+\mathcal{D}(\mathsf{X}^j)\mathsf{X}^i\end{aligned}$$

και $\mathcal{D}(\mathsf{X}^0\mathsf{X}^0)=\mathcal{D}(1_K\cdot 1_K)=\mathcal{D}(1_K)=0_K=\mathcal{D}(\mathsf{X}^0)\mathsf{X}^0+\mathcal{D}(\mathsf{X}^0)\mathsf{X}^0$. Εν συνεχεία, συμπεραίνουμε ότι

$$\begin{aligned}&\mathcal{D}(\varphi(\mathsf{X})\psi(\mathsf{X}))=\mathcal{D}\left(\sum_{i=0}^{n}\sum_{j=0}^{m}\left(a_i\mathsf{X}^i\right)\left(b_j\mathsf{X}^j\right)\right)\\ &=\sum_{i=0}^{n}\sum_{j=0}^{m}a_ib_j\mathcal{D}(\mathsf{X}^i\mathsf{X}^j)=\sum_{i=0}^{n}\sum_{j=0}^{m}a_ib_j(\mathcal{D}(\mathsf{X}^i)\mathsf{X}^j+\mathcal{D}(\mathsf{X}^j)\mathsf{X}^i)\\ &=\left(\sum_{i=0}^{n}a_i\mathcal{D}(\mathsf{X}^i)\right)\left(\sum_{j=0}^{m}b_j\mathsf{X}^j\right)+\left(\sum_{j=0}^{m}b_j\mathcal{D}(\mathsf{X}^j)\right)\left(\sum_{i=0}^{n}a_i\mathsf{X}^i\right)\\ &=\mathcal{D}\left(\sum_{i=0}^{n}a_i\mathsf{X}^i\right)\left(\sum_{j=0}^{m}b_j\mathsf{X}^j\right)+\mathcal{D}\left(\sum_{j=0}^{m}b_j\mathsf{X}^j\right)\left(\sum_{i=0}^{n}a_i\mathsf{X}^i\right)\\ &=\mathcal{D}(\varphi(\mathsf{X}))\psi(\mathsf{X})+\mathcal{D}(\psi(\mathsf{X}))\varphi(\mathsf{X})\end{aligned}$$

κάνοντας χρήση των (i) και (ii). □

3.4.17 Σημείωση. (i) Για κάθε $\varphi(\mathsf{X})\in K[\mathsf{X}]$ έχουμε

$$\deg(\mathcal{D}(\varphi(\mathsf{X})))\begin{cases}=\deg(\varphi(\mathsf{X}))-1, & \text{όταν } \chi\alpha\rho(K)\nmid\deg(\varphi(\mathsf{X})),\\ <\deg(\varphi(\mathsf{X}))-1, & \text{όταν } \chi\alpha\rho(K)\mid\deg(\varphi(\mathsf{X})).\end{cases}$$

(ii) Εάν $\varphi_1(\mathsf{X}),\ldots,\varphi_k(\mathsf{X})\in K[\mathsf{X}]$ ($k\in\mathbb{N}$, $k\geq 2$), τότε η ισότητα 3.4.16 (iii) γενικεύεται επαγωγικώς ως εξής:

$$\mathcal{D}\left(\prod_{j=1}^{k}\varphi_j(\mathsf{X})\right)=\sum_{i=1}^{k}\mathcal{D}\left(\varphi_i(\mathsf{X})\right)\prod_{j\in\{1,\ldots,k\}\setminus\{i\}}\varphi_j(\mathsf{X}). \tag{3.15}$$

(iii) Οι *υψηλότερης τάξεως επίτυπες παράγωγοι* ενός $\varphi(\mathsf{X})\in K[\mathsf{X}]$ ορίζονται κατά τα ειωθότα:

$$\boxed{\mathcal{D}^i(\varphi(\mathsf{X})):=\begin{cases}\varphi(\mathsf{X}), & \text{όταν } i=0,\\ \mathcal{D}(\mathcal{D}^{i-1}(\varphi(\mathsf{X}))), & \text{όταν } i\geq 1.\end{cases}}$$

Συγκεκριμένα, εάν $\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j \mathsf{X}^j$, $a_n \neq 0_K$, τότε

$$\mathcal{D}^i(\varphi(\mathsf{X})) = \begin{cases} i! \left(\sum\limits_{j=i}^{n} \binom{j}{i} a_j \mathsf{X}^{j-i} \right), & \text{όταν } 0 \leq i \leq n, \\ \mathbf{0}_{K[\mathsf{X}]}, & \text{όταν } i > n. \end{cases}$$

(iv) Εάν $\text{χαρ}(K) = p$ (p πρώτος), τότε $\mathcal{D}^p(\varphi(\mathsf{X})) = \mathbf{0}_{K[\mathsf{X}]}$ *για κάθε* $\varphi(\mathsf{X}) \in K[\mathsf{X}]$.

3.4.18 Πρόταση. (Κανόνας τού Leibniz) *Εάν* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$, *τότε για κάθε* $i \in \mathbb{N}_0$ *έχουμε*

$$\boxed{\mathcal{D}^i(\varphi(\mathsf{X})\psi(\mathsf{X})) = \sum_{k=0}^{i} \binom{i}{k} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})).} \tag{3.16}$$

ΑΠΟΔΕΙΞΗ. Η ισότητα (3.16) είναι προφανής για $i = 0$ και $i = 1$ (βλ. 3.4.16 (iii)). Εάν υποθέσουμε ότι $i \geq 2$ και ότι αυτή είναι αληθής για το $i - 1$, τότε

$$\begin{aligned}
&\mathcal{D}^i(\varphi(\mathsf{X})\psi(\mathsf{X})) = \mathcal{D}(\mathcal{D}^{i-1}(\varphi(\mathsf{X})\psi(\mathsf{X}))) \\
&= \mathcal{D}\left(\sum_{l=0}^{i-1} \binom{i-1}{l} \mathcal{D}^l(\varphi(\mathsf{X})) \mathcal{D}^{i-1-l}(\psi(\mathsf{X})) \right) = \sum_{l=0}^{i-1} \binom{i-1}{l} \mathcal{D}(\mathcal{D}^l(\varphi(\mathsf{X})) \mathcal{D}^{i-1-l}(\psi(\mathsf{X}))) \\
&= \sum_{l=0}^{i-1} \binom{i-1}{l} \mathcal{D}^{l+1}(\varphi(\mathsf{X})) \mathcal{D}^{i-1-l}(\psi(\mathsf{X})) + \sum_{l=0}^{i-1} \binom{i-1}{l} \mathcal{D}^l(\varphi(\mathsf{X})) \mathcal{D}^{i-l}(\psi(\mathsf{X})) \\
&= \sum_{k=1}^{i} \binom{i-1}{k-1} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})) + \sum_{k=0}^{i-1} \binom{i-1}{k} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})) \\
&= \sum_{k=1}^{i} \left(\binom{i-1}{k-1} + \binom{i-1}{k} \right) \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})) + \varphi(\mathsf{X}) \mathcal{D}^i(\psi(\mathsf{X})) \\
&= \sum_{k=1}^{i} \binom{i}{k} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})) + \varphi(\mathsf{X}) \mathcal{D}^i(\psi(\mathsf{X})) = \sum_{k=0}^{i} \binom{i}{k} \mathcal{D}^k(\varphi(\mathsf{X})) \mathcal{D}^{i-k}(\psi(\mathsf{X})),
\end{aligned}$$

όπου η δεύτερη ισότητα προκύπτει από την επαγωγική μας υπόθεση, η τρίτη από το (ii) τού λήμματος 3.4.16, η τέταρτη από το (iii) τού λήμματος 3.4.16 και η προτελευταία από την τριγωνική ταυτότητα τού Pascal. Άρα η (3.16) είναι αληθής *για κάθε* $i \in \mathbb{N}_0$. □

3.4.19 Πρόταση. (Τύπος τού Taylor) *Εάν το* $\varphi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$ *είναι ένα πολυώνυμο βαθμού* n *και η χαρακτηριστική τού* K *είναι είτε* 0 *είτε* $> n$, *τότε*[8]

$$\boxed{\varphi(\mathsf{X}) = \sum_{i=0}^{n} (i!)^{-1} \, \mathcal{D}^i(\varphi(\mathsf{X}))\big|_{\mathsf{X}=\lambda} (\mathsf{X} - \lambda)^i, \ \forall \lambda \in K.} \tag{3.17}$$

[8] Πρόκειται για την επίτυπη εκδοχή μιας ειδικής περιπτώσεως τού τύπου τού Άγγλου μαθηματικού Brook Taylor (1685-1731) τού εισαχθέντος το 1715 για πραγματικές n φορές παραγωγίσιμες πραγματικές συναρτήσεις (που συναντούμε στον Απειροστικό Λογισμό). Όταν $\lambda = 0_K$, αυτός δίδει τον γνωστό τύπο τού (Σκωτσέζου μαθηματικού) Colin MacLaurin (1698-1746).

ΑΠΟΔΕΙΞΗ. Επειδή για οιουσδήποτε $i, j \in \{0,...,n\}$, $i \leq j$, ισχύει

$$\mathcal{D}^i(\mathsf{X}^j) = j(j-1)\cdots(j-i+1)\mathsf{X}^{j-i} = i!\tbinom{j}{i}\mathsf{X}^{j-i} \Rightarrow \mathcal{D}^i(\mathsf{X}^j)\Big|_{\mathsf{X}=\lambda} = i!\tbinom{j}{i}\lambda^{j-i},$$

συνάγουμε (μέσω τού δυωνυμικού τύπου και των προϋποτεθέντων περιορισμών για την $\text{χαρ}(K)$) ότι

$$\mathsf{X}^j = ((\mathsf{X}-\lambda)+\lambda)^j = \sum_{i=0}^{j}\tbinom{j}{i}\lambda^{j-i}(\mathsf{X}-\lambda)^i = \sum_{i=0}^{j}(i!)^{-1}\,\mathcal{D}^i(\mathsf{X}^j)\Big|_{\mathsf{X}=\lambda}(\mathsf{X}-\lambda)^i.$$

Εάν $\varphi(\mathsf{X}) = \sum_{j=0}^{n} a_j\mathsf{X}^j$, τότε[9]

$$\begin{aligned}&\sum_{i=0}^{n}(i!)^{-1}\,\mathcal{D}^i(\sum_{j=0}^{n}a_j\mathsf{X}^j)\Big|_{\mathsf{X}=\lambda}(\mathsf{X}-\lambda)^i = \sum_{i=0}^{n}\sum_{j=0}^{n}a_j\,(i!)^{-1}\,\mathcal{D}^i(\mathsf{X}^j)\big|_{\mathsf{X}=\lambda}(\mathsf{X}-\lambda)^i\\ &= \sum_{j=0}^{n}a_j\left(\sum_{i=0}^{n}(i!)^{-1}\,\mathcal{D}^i(\mathsf{X}^j)\big|_{\mathsf{X}=\lambda}(\mathsf{X}-\lambda)^i\right) = \sum_{j=0}^{n}a_j\mathsf{X}^j = \varphi(\mathsf{X})\end{aligned}$$

(λόγω των (i) και (ii) τού λήμματος 3.4.16). □

3.4.20 Θεώρημα. *Εάν* $\varphi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{\mathbf{0}_{K[\mathsf{X}]}\}$, $\lambda \in K$, $m \in \mathbb{N}$, *και η χαρακτηριστική τού* K *είναι είτε* 0 *είτε* $> n := \deg(\varphi(\mathsf{X}))$, *τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) $\text{mult}(\varphi(\mathsf{X});\lambda) = m$.

(ii) *Το* λ *είναι θέση μηδενισμού καθενός εκ των*

$$\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X})), \mathcal{D}^2(\varphi(\mathsf{X})),..., \mathcal{D}^{m-1}(\varphi(\mathsf{X})), \tag{3.18}$$

αλλά δεν είναι θέση μηδενισμού τού $\mathcal{D}^m(\varphi(\mathsf{X}))$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $\text{mult}(\varphi(\mathsf{X});\lambda) = m$, τότε

$$\exists\psi(\mathsf{X}) \in K[\mathsf{X}]\setminus\{\mathbf{0}_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X}-\lambda)^m\,\psi(\mathsf{X}) \text{ με } \psi(\lambda) \neq 0_K.$$

(Βλ. 3.4.14 (i)⇒(ii).) Εφαρμόζοντας για οιονδήποτε $i \in \{0,...,m\}$ τον κανόνα (3.16) τού Leibniz λαμβάνουμε

$$\mathcal{D}^i(\varphi(\mathsf{X})) = \sum_{k=0}^{i}\tbinom{i}{k}\mathcal{D}^k((\mathsf{X}-\lambda)^m)\mathcal{D}^{i-k}(\psi(\mathsf{X})),$$

[9] Για την εικόνα $\mathfrak{y}_\lambda(\mathcal{D}^i(\varphi(\mathsf{X})))$ τής i-οστής επίτυπης παραγώγου ενός πολυωνύμου $\varphi(\mathsf{X})$ μέσω τής $\mathfrak{y}_\lambda$ ($\lambda \in K$) χρησιμοποιείται η συντομογραφία $\mathcal{D}^i(\varphi(\mathsf{X}))\big|_{\mathsf{X}=\lambda}$ για να αποφεύγεται σύγχυση. (Ο συμβολισμός $\mathcal{D}^i(\varphi(\lambda))$ θα μπορούσε να εκληφθεί ως η i-οστή επίτυπη παραγώγος τής *σταθεράς* $\mathfrak{y}_\lambda(\varphi(\mathsf{X})) = \varphi(\lambda)$, η οποία ισούται με 0_K όταν $i \geq 1$.)

όπου $\mathcal{D}^k((\mathsf{X}-\lambda)^m) = k!\binom{m}{k}(\mathsf{X}-\lambda)^{m-k}$. Επομένως,

$$\begin{aligned}\mathcal{D}^i(\varphi(\mathsf{X})) &= \underbrace{i!\tbinom{m}{i}(\mathsf{X}-\lambda)^{m-i}\psi(\mathsf{X})}_{\text{ο όρος για } k=i} + \sum_{k=0}^{i-1}\tbinom{i}{k}k!\tbinom{m}{k}(\mathsf{X}-\lambda)^{m-k}\mathcal{D}^{i-k}(\psi(\mathsf{X}))\\ &= i!\tbinom{m}{i}(\mathsf{X}-\lambda)^{m-i}\psi(\mathsf{X}) + (\mathsf{X}-\lambda)^{m-i+1}\theta_i(\mathsf{X}),\end{aligned}$$

όπου $\theta_i(\mathsf{X}) := \sum_{k=0}^{i-1}\binom{i}{k}k!\binom{m}{k}(\mathsf{X}-\lambda)^{(i-1)-k}\mathcal{D}^{i-k}(\psi(\mathsf{X}))$. Επειδή

$$\big(\mathcal{D}^i(\varphi(\mathsf{X}))\big)\big|_{\mathsf{X}=\lambda} = \begin{cases} 0_K, & \text{όταν } 0 \le i \le m-1,\\ m!\psi(\lambda), & \text{όταν } i = m,\end{cases}$$

με $m!\psi(\lambda) \neq 0_K$ (λόγω των υποθέσεών μας περί τής χαρ(K)), ο ισχυρισμός είναι αληθής.

(ii)⇒(i) Εάν το λ είναι θέση μηδενισμού καθενός εκ των (3.18) αλλά δεν είναι θέση μηδενισμού τού $\mathcal{D}^m(\varphi(\mathsf{X}))$, τότε ο τύπος (3.17) τού Taylor γράφεται ως εξής:

$$\varphi(\mathsf{X}) = \sum_{i=m}^{n}(i!)^{-1}\,\mathcal{D}^i(\varphi(\mathsf{X}))\big|_{\mathsf{X}=\lambda}(\mathsf{X}-\lambda)^i = (\mathsf{X}-\lambda)^m\psi(\mathsf{X}),$$

όπου

$$\psi(\mathsf{X}) := \sum_{i=m}^{n}(i!)^{-1}\,\mathcal{D}^i(\varphi(\mathsf{X}))\Big|_{\mathsf{X}=\lambda}(\mathsf{X}-\lambda)^{i-m} \Rightarrow \psi(\lambda) = (m!)^{-1}\,\mathcal{D}^m(\varphi(\mathsf{X}))|_{\mathsf{X}=\lambda} \neq 0_K.$$

Αυτό σημαίνει ότι $\mathrm{mult}(\varphi(\mathsf{X});\lambda) = m$ (βλ. 3.4.14 (ii)⇒(i)). □

3.4.21 Παραδείγματα. (i) Εάν $\varphi(\mathsf{X}) := \mathsf{X}^\nu - \nu\mathsf{X} + \nu - 1 \in \mathbb{C}[\mathsf{X}]$, όπου $\nu \in \mathbb{N}$, $\nu \ge 2$, τότε

$$\mathcal{D}^i(\varphi(\mathsf{X})) = \begin{cases} \nu\mathsf{X}^{\nu-1} - \nu, & \text{όταν } i = 1,\\ \nu(\nu-1)\mathsf{X}^{\nu-2}, & \text{όταν } i = 2,\\ i!\binom{\nu}{i}\mathsf{X}^{\nu-i}, & \text{όταν } 3 \le i \le \nu,\\ \mathbf{0}_{\mathbb{C}[\mathsf{X}]}, & \text{όταν } i > \nu.\end{cases}$$

Το 1 είναι διπλή θέση μηδενισμού τού $\varphi(\mathsf{X})$, διότι

$$\varphi(1) = \mathcal{D}(\varphi(\mathsf{X}))|_{\mathsf{X}=1} = 0,\ \mathcal{D}^2(\varphi(\mathsf{X}))\big|_{\mathsf{X}=1} = \nu(\nu-1) \neq 0.$$

Επιπροσθέτως, οιαδήποτε θέση μηδενισμού $\lambda \in \mathbb{C}\smallsetminus\{1\}$ τού $\varphi(\mathsf{X})$ είναι απλή, διότι εάν ίσχυε

$$\mathcal{D}(\varphi(\mathsf{X}))|_{\mathsf{X}=\lambda} = \nu(\lambda^{\nu-1} - 1) = 0 \Rightarrow \lambda^{\nu-1} = 1,$$

τότε θα καταλήγαμε σε άτοπο, αφού

$$\left.\begin{array}{r} \varphi(\lambda)=0 \Rightarrow \lambda(\lambda^{\nu-1}-\nu)=1-\nu \\ \lambda^{\nu-1}=1 \end{array}\right\} \underset{\nu\neq 1}{\Longrightarrow} \lambda=1.$$

(ii) Θεωρούμε το $\varphi(\mathsf{X}) := \mathsf{X}^{\nu}-a \in K[\mathsf{X}]$, όπου $\nu \in \mathbb{N}$ και $a \in K\setminus\{0_K\}$. Εάν είτε $\text{χαρ}(K)=0$ είτε $\text{χαρ}(K) \nmid \nu$ και το λ είναι ένα στοιχείο μιας επεκτάσεως K' τού K, εντός τής οποίας ισχύει $\lambda^{\nu}=a$, τότε $\mathcal{D}(\varphi(\mathsf{X}))|_{\mathsf{X}=\lambda}=\nu\lambda^{\nu-1}\neq 0_{K'}$. Αυτό σημαίνει ότι το $\varphi(\mathsf{X})$, ιδωμένο ως στοιχείο τού $L[\mathsf{X}]$, όπου L *τυχούσα επέκταση* τού K, δεν διαθέτει καμία πολλαπλή θέση μηδενισμού. Αντιθέτως, εάν $\text{χαρ}(K)=p$ (p πρώτος), τότε $\mathcal{D}(\varphi(\mathsf{X}))=p\mathsf{X}^{p-1}=\mathbf{0}_{K[\mathsf{X}]}$. Εν τοιαύτη περιπτώσει, κάθε θέση μηδενισμού λ τού $\varphi(\mathsf{X})$ έχει πολλαπλότητα $\text{mult}(\varphi(\mathsf{X});\lambda)=p$, διότι

$$\varphi(\mathsf{X})=\mathsf{X}^{p}-a=\mathsf{X}^{p}-\lambda^{p}=(\mathsf{X}-\lambda)^{p}.$$

3.5 ΑΝΑΓΩΓΑ ΠΟΛΥΩΝΥΜΑ

Όπως οι ακέραιοι αριθμοί έχουν τους πρώτους αριθμούς ως «δομικούς τους λίθους», έτσι και τα πολυώνυμα τα ανήκοντα στον $K[\mathsf{X}]$ (όπου K τυχόν σώμα) αποσυντίθενται σε γινόμενα «αναγώγων» πολυωνύμων.

3.5.1 Ορισμός. Έστω K ένα σώμα. Ένα πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ θετικού βαθμού καλείται **ανάγωγο πολυώνυμο υπεράνω τού** K (ή **ανάγωγο πολυώνυμο εντός τού** $K[\mathsf{X}]$) όταν δεν υπάρχουν πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει η ισότητα

$$\varphi(\mathsf{X})=\varphi_1(\mathsf{X})\varphi_2(\mathsf{X}) \tag{3.19}$$

με $1 \leq \deg(\varphi_1(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$ και $1 \leq \deg(\varphi_2(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$ (ή, ισοδυνάμως, όταν μια παράσταση (3.19) τού $\varphi(\mathsf{X})$ υφίσταται μόνον υπό την προϋπόθεση ότι ακριβώς ένα εκ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ είναι σταθερό, μη μηδενικό πολυώνυμο).

3.5.2 Παρατήρηση. Η αναφορά τού σώματος υπεράνω τού οποίου ένα δοθέν πολυώνυμο είναι (ή δεν είναι) ανάγωγο είναι απαραίτητη. Επί παραδείγματι, το X^2+1 είναι ανάγωγο υπεράνω τού $\mathbb{R}$ άλλά δεν είναι ανάγωγο υπεράνω τού $\mathbb{C}$, διότι $\mathsf{X}^2+1=(\mathsf{X}+i)(\mathsf{X}-i)$, όπου i η φανταστική μονάδα.

3.5.3 Σημείωση. (i) Έστω K τυχόν σώμα. Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού 1 είναι -προφανώς- ανάγωγο. Ο έλεγχος τού κατά πόσον ένα πολυώνυμο βαθμού ≥ 2 είναι ανάγωγο δεν είναι εν γένει κάτι το τετριμμένο. Τα ανάγωγα πολυώνυμα υπεράνω τού $\mathbb{R}$ μπορούν να χαρακτηρισθούν πλήρως (βλ. πρόταση 3.7.3). Όπως

θα δούμε στην επομένη ενότητα (βλ. εδ. 3.6.16 (iii), 3.6.17 και 3.6.19), τα ανάγωγα πολυώνυμα υπεράνω τού $\mathbb{C}$ είναι μόνον τα πρωτοβάθμια. Ωστόσο, ακόμη και υπεράνω τού $\mathbb{Q}[\mathsf{X}]$ ένας *γενικός* χαρακτηρισμός των αναγώγων πολυωνύμων φαντάζει εξαιρετικά δύσκολος.

(ii) Κατά το 3.4.4 (ii) δεν υπάρχει κανένα ανάγωγο πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού ≥ 2 που να έχει θέσεις μηδενισμού εντός τού K. Το αντίστροφο δεν είναι εν γένει αληθές. Επί παραδείγματι, το πολυώνυμο $(\mathsf{X}^2+3)^2 \in \mathbb{R}[\mathsf{X}]$ δεν έχει καμία θέση μηδενισμού εντός τού $\mathbb{R}$, αλλ' εντούτοις δεν είναι ανάγωγο υπεράνω αυτού. Μολαταύτα, υπό ορισμένες ειδικές προϋποθέσεις ισχύει ενίοτε και το αντίστροφο.

3.5.4 Πρόταση. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ με $\deg(\varphi(\mathsf{X})) \in \{2,3\}$. Εάν το $\varphi(\mathsf{X})$ δεν διαθέτει θέσεις μηδενισμού εντός τού K, τότε είναι ανάγωγο υπεράνω τού K.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $\varphi(\mathsf{X})$ δεν είναι ανάγωγο υπεράνω τού K. Τότε το $\varphi(\mathsf{X})$ γράφεται ως γινόμενο δύο μη σταθερών πολυωνύμων

$$\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$$

με $\deg(\varphi_1(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$ και $\deg(\varphi_2(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$. Επειδή

$$\deg(\varphi(\mathsf{X})) = \deg(\varphi_1(\mathsf{X})) + \deg(\varphi_2(\mathsf{X})) \in \{2,3\},$$

τουλάχιστον ένα εκ των $\varphi_1(\mathsf{X})$, $\varphi_2(\mathsf{X})$ 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! □

3.5.5 Πρόταση. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$. Εάν $\deg(\varphi(\mathsf{X})) \geq 1$, τότε υφίσταται τουλάχιστον ένα ανάγωγο πολυώνυμο υπεράνω τού K το οποίο είναι διαιρέτης τού $\varphi(\mathsf{X})$.*

ΑΠΟΔΕΙΞΗ. Έστω $\mathcal{A} := \{\alpha(\mathsf{X}) \in K[\mathsf{X}] : \deg(\alpha(\mathsf{X})) \geq 1 \text{ και } \alpha(\mathsf{X}) \mid \varphi(\mathsf{X})\}$. Το σύνολο $\mathcal{A}$ είναι μη κενό διότι $\varphi(\mathsf{X}) \in \mathcal{A}$. Θέτουμε $n_0 := \min\{\deg(\alpha(\mathsf{X})) \mid \alpha(\mathsf{X}) \in \mathcal{A}\}$ και θεωρούμε τυχόν στοιχείο $\psi(\mathsf{X}) \in \mathcal{A}$ βαθμού $\deg(\psi(\mathsf{X})) = n_0$. Τότε το $\psi(\mathsf{X})$ είναι ένα ανάγωγο πολυώνυμο υπεράνω τού K το οποίο διαιρεί το $\varphi(\mathsf{X})$. Πράγματι· $n_0 \geq 1$ και εάν υποθέσουμε ότι υπάρχουν πολυώνυμα $\psi_1(\mathsf{X}), \psi_2(\mathsf{X}) \in K[\mathsf{X}]$, τέτοια ώστε να ισχύει η ισότητα

$$\psi(\mathsf{X}) = \psi_1(\mathsf{X})\psi_2(\mathsf{X})$$

με $1 \leq \deg(\psi_1(\mathsf{X})) < \deg(\psi(\mathsf{X}))$ και $1 \leq \deg(\psi_2(\mathsf{X})) < \deg(\psi(\mathsf{X}))$, τότε καταλήγουμε σε άτοπο, καθόσον για $i = 1, 2$ έχουμε

$$\left.\begin{array}{r}\psi_i(\mathsf{X}) \mid \psi(\mathsf{X}) \\ \psi(\mathsf{X}) \mid \varphi(\mathsf{X})\end{array}\right\} \Longrightarrow \left.\begin{array}{r}\psi_i(\mathsf{X}) \mid \varphi(\mathsf{X}) \\ \deg(\psi_i(\mathsf{X})) \geq 1\end{array}\right\} \Rightarrow \psi_i(\mathsf{X}) \in \mathcal{A}$$

με $1 \leq \deg(\psi_i(\mathsf{X})) < \deg(\psi_1(\mathsf{X})) + \deg(\psi_2(\mathsf{X})) = \deg(\psi(\mathsf{X})) = n_0$ (κάτι το οποίο αντίκειται στον ορισμό τού $\psi(\mathsf{X})$). □

3.5.6 Λήμμα. *Εάν* $\theta(\mathsf{X}) \in K[\mathsf{X}]$, *τότε για κάθε πολυώνυμο* $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ *που είναι ανάγωγο υπεράνω τού* K *ισχύει είτε* $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$ *είτε* $\text{μκδ}(\varphi(\mathsf{X}), \theta(\mathsf{X})) = 1_K$.

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το θεώρημα 3.3.1, υπάρχει ζεύγος μονοσημάντως ορισμένων πολυωνύμων $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\theta(\mathsf{X}) = \varpi(\mathsf{X})\varphi(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg(\upsilon(\mathsf{X})) < \deg(\varphi(\mathsf{X})).$$

Εάν $\upsilon(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}$, τότε $\varphi(\mathsf{X}) \mid \theta(\mathsf{X})$. Εάν $\upsilon(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$, τότε $\varphi(\mathsf{X}) \nmid \theta(\mathsf{X})$ και

$$\text{μκδ}(\varphi(\mathsf{X}), \theta(\mathsf{X})) = \text{μκδ}(\varphi(\mathsf{X}), \upsilon(\mathsf{X})).$$

Θέτοντας $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X}), \upsilon(\mathsf{X}))$ παρατηρούμε ότι

$$\delta(\mathsf{X}) \mid \varphi(\mathsf{X}) \Rightarrow \exists \alpha(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = \alpha(\mathsf{X})\delta(\mathsf{X}) \tag{3.20}$$

και

$$\delta(\mathsf{X}) \mid \upsilon(\mathsf{X}) \underset{\text{3.3.3 (iv)}}{\Longrightarrow} 0 \leq \deg(\delta(\mathsf{X})) \leq \deg(\upsilon(\mathsf{X})) < \deg(\varphi(\mathsf{X})). \tag{3.21}$$

Επειδή το $\varphi(\mathsf{X})$ είναι εξ υποθέσεως ανάγωγο υπεράνω τού K, από την (3.20) και το (ii) τής προτάσεως 3.2.2 συνάγουμε ότι (ακριβώς) ένα εκ των $\alpha(\mathsf{X}), \delta(\mathsf{X})$ είναι σταθερό μη μηδενικό (ήτοι βαθμού 0) και

$$\deg(\alpha(\mathsf{X})) + \deg(\delta(\mathsf{X})) = \deg(\varphi(\mathsf{X})) > 0.$$

Αυτό σημαίνει ότι *είτε* ισχύει $\deg(\alpha(\mathsf{X})) = 0$ και $\deg(\delta(\mathsf{X})) = \deg(\varphi(\mathsf{X}))$ *είτε* $\deg(\delta(\mathsf{X})) = 0$ και $\deg(\alpha(\mathsf{X})) = \deg(\varphi(\mathsf{X}))$. Το πρώτο ενδεχόμενο αποκλείεται λόγω τής (3.21). Επομένως, $\deg(\delta(\mathsf{X})) = 0$ (διότι $\delta(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$) και $\delta(\mathsf{X}) = 1_K$ (διότι ο μέγιστος κοινός διαιρέτης $\delta(\mathsf{X})$ είναι εξ ορισμού *μονικό* πολυώνυμο). □

3.5.7 Λήμμα. *Εάν τα* $\varphi(\mathsf{X}), \theta_1(\mathsf{X}), \ldots, \theta_n(\mathsf{X}) \in K[\mathsf{X}]$ ($n \in \mathbb{N}$) *είναι ανάγωγα πολυώνυμα υπεράνω τού* K, *τότε ισχύει η συνεπαγωγή*

$$\varphi(\mathsf{X}) \mid \prod_{j=1}^{n} \theta_j(\mathsf{X}) \Longrightarrow \exists j_0 \in \{1, \ldots, n\} : \varphi(\mathsf{X}) = c\,\theta_{j_0}(\mathsf{X}),$$

για κάποια σταθερά $c \in K \setminus \{0_K\}$.

ΑΠΟΔΕΙΞΗ. Υποθέτουμε ότι $\varphi(\mathsf{X}) \mid \prod_{j=1}^{n} \theta_j(\mathsf{X})$. Κατ' αρχάς θα αποδείξουμε ότι

$$\exists j_0 \in \{1, \ldots, n\} : \varphi(\mathsf{X}) \mid \theta_{j_0}(\mathsf{X}). \tag{3.22}$$

Εάν $\varphi(\mathsf{X}) \mid \theta_1(\mathsf{X})$, τότε η (3.22) είναι προφανής (με $j_0 = 1$). Εάν $\varphi(\mathsf{X}) \nmid \theta_1(\mathsf{X})$, τότε (σύμφωνα με το λήμμα 3.5.6 και το πόρισμα 3.3.16)

$$\left.\begin{array}{r} \text{μκδ}(\varphi(\mathsf{X}), \theta_1(\mathsf{X})) = 1_K \\ \varphi(\mathsf{X}) \mid \theta_1(\mathsf{X}) \left(\prod_{j=2}^{n} \theta_j(\mathsf{X})\right) \end{array}\right\} \Rightarrow \varphi(\mathsf{X}) \mid \prod_{j=2}^{n} \theta_j(\mathsf{X}).$$

Εάν $\varphi(\mathsf{X}) \mid \theta_2(\mathsf{X})$, τότε η (3.22) ισχύει (με $j_0 = 2$). Εάν $\varphi(\mathsf{X}) \nmid \theta_2(\mathsf{X})$, τότε ομοίως

$$\left.\begin{array}{r} \text{μκδ}(\varphi(\mathsf{X}), \theta_2(\mathsf{X})) = 1_K \\ \varphi(\mathsf{X}) \mid \theta_2(\mathsf{X}) \left(\prod_{j=3}^{n} \theta_j(\mathsf{X})\right) \end{array}\right\} \Rightarrow \varphi(\mathsf{X}) \mid \prod_{j=3}^{n} \theta_j(\mathsf{X}).$$

Επαναλαμβάνοντας (εν ανάγκη) την ίδια διαδικασία (το πολύ $n-2$ ακόμη φορές) εντοπίζουμε τελικώς (με την ίδια συλλογιστική) έναν $j_0 \leq n$ για τον οποίο η (3.22) είναι αληθής. Επειδή αμφότερα τα $\varphi(\mathsf{X})$ και $\theta_{j_0}(\mathsf{X})$ είναι ανάγωγα υπεράνω τού K, έχουμε κατ' ανάγκην ότι $\varphi(\mathsf{X}) = c\,\theta_{j_0}(\mathsf{X})$, για κάποια σταθερά $c \in K \smallsetminus \{0_K\}$. □

3.5.8 Θεώρημα. *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού ≥ 1 γράφεται ως γινόμενο*

$$\boxed{\varphi(\mathsf{X}) = c \prod_{\nu=1}^{r} \theta_\nu(\mathsf{X})} \tag{3.23}$$

αναγώγων (υπεράνω τού K) μονικών πολυωνύμων $\theta_1(\mathsf{X}),...,\theta_r(\mathsf{X}) \in K[\mathsf{X}]$ (όπου $r \in \mathbb{N}$) και μιας σταθεράς $c \in K \smallsetminus \{0_K\}$. Η παράσταση αυτή είναι μονοσημάντως ορισμένη υπό την ακόλουθη έννοια: Εάν

$$\varphi(\mathsf{X}) = c \prod_{\nu=1}^{r} \theta_\nu(\mathsf{X}) = c' \prod_{j=1}^{l} \theta'_j(\mathsf{X}), \tag{3.24}$$

όπου $c' \in K \smallsetminus \{0_K\}$ και $\theta'_1(\mathsf{X}),...,\theta'_l(\mathsf{X}) \in K[\mathsf{X}]$ ($l \in \mathbb{N}$) ανάγωγα (υπεράνω τού K) μονικά πολυώνυμα, τότε $c = c'$, $r = l$ και υπάρχει μια μετάταξη $\sigma \in \mathfrak{S}_r$, ούτως ώστε να ισχύει

$$\theta_\nu(\mathsf{X}) = \theta'_{\sigma(\nu)}(\mathsf{X}),\ \forall \nu \in \{1,...,r\}. \tag{3.25}$$

ΑΠΟΔΕΙΞΗ. Μέσω μαθηματικής επαγωγής ως προς τον $n := \deg(\varphi(\mathsf{X}))$.

► *Ύπαρξη τής παραστάσεως* (3.23). Εάν $n = 1$, τότε ο ισχυρισμός είναι αληθής, καθόσον τα πρωτοβάθμια πολυώνυμα είναι ανάγωγα. Ας υποθέσουμε ότι $n \geq 2$ και ότι αυτός είναι αληθής και για όλα τα μη σταθερά πολυώνυμα βαθμού $< n$. Εάν το $\varphi(\mathsf{X})$ *είναι* ανάγωγο, τότε (εξ ορισμού) $\varphi(\mathsf{X}) = c\,\hat{\varphi}(\mathsf{X})$, όπου το $\hat{\varphi}(\mathsf{X}) \in K[\mathsf{X}]$ είναι μονικό και ανάγωγο υπεράνω τού K, και c ο επικεφαλής συντελεστής τού $\varphi(\mathsf{X})$. Εάν το $\varphi(\mathsf{X})$ *δεν είναι* ανάγωγο, τότε γράφεται ως γινόμενο $\varphi(\mathsf{X}) = \varphi_1(\mathsf{X})\varphi_2(\mathsf{X})$ δύο μη σταθερών πολυωνύμων $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$ με βαθμούς $\deg(\varphi_1(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$ και $\deg(\varphi_2(\mathsf{X})) < \deg(\varphi(\mathsf{X}))$. Σύμφωνα με την επαγωγική μας υπόθεση, υπάρχουν φυσικοί αριθμοί r_1, r_2, σταθερές $c_1, c_2 \in K \smallsetminus \{0_K\}$ και πολυώνυμα $\theta_1^{[1]}(\mathsf{X}),..., \theta_{r_1}^{[1]}(\mathsf{X}) \in K[\mathsf{X}]$ και $\theta_1^{[2]}(\mathsf{X}),..., \theta_{r_2}^{[2]}(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\varphi_1(\mathsf{X}) = c_1 \prod_{\nu=1}^{r_1} \theta_\nu^{[1]}(\mathsf{X}), \quad \varphi_2(\mathsf{X}) = c_2 \prod_{j=1}^{r_2} \theta_j^{[2]}(\mathsf{X}).$$

Κατά συνέπειαν, και σε αυτήν την περίπτωση το $\varphi(\mathsf{X})$ διαθέτει μια παράσταση τής μορφής (3.23), καθότι

$$\varphi(\mathsf{X}) = \underbrace{c_1 c_2}_{\in K\setminus\{0_K\}} \left(\prod_{\nu=1}^{r_1} \theta_\nu^{[1]}(\mathsf{X})\right)\left(\prod_{j=1}^{r_2} \theta_j^{[2]}(\mathsf{X})\right).$$

► *Περί τού μονοσημάντου τής παραστάσεως* (3.23). Εκκινούμε από δυο τυχούσες (τέτοιου είδους) παραστάσεις (3.24) τού $\varphi(\mathsf{X})$. Εάν $n = 1$, τότε ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι $n \geq 2$ και ότι αυτός είναι αληθής και για όλα τα μη σταθερά πολυώνυμα βαθμού $< n$. Η ισότητα $c = c'$ έπεται άμεσα ύστερα από σύγκριση των επικεφαλής συντελεστών. Επειδή

$$\theta_r(\mathsf{X}) \mid \prod_{\nu=1}^{r} \theta_\nu(\mathsf{X}) = \prod_{j=1}^{l} \theta'_j(\mathsf{X}),$$

υπάρχει κάποιος δείκτης $j_0 \in \{1,...,l\}$, τέτοιος ώστε να ισχύει $\theta_r(\mathsf{X}) = a\,\theta'_{j_0}(\mathsf{X})$, για κάποια σταθερά $a \in K\setminus\{0_K\}$ (βλ. λήμμα 3.5.7). Εν προκειμένω, αυτή η σταθερά a οφείλει να ισούται με 1_K (διότι αμφότερα τα $\theta_r(\mathsf{X})$ και $\theta'_{j_0}(\mathsf{X})$ είναι εξ υποθέσεως μονικά), οπότε $\theta_r(\mathsf{X}) = \theta'_{j_0}(\mathsf{X})$.

Περίπτωση πρώτη. Έχουμε $l = 1 \Leftrightarrow r = 1$ (διότι αλλιώς στο ένα μέλος τής ανωτέρω ισότητας θα είχαμε ένα μη ανάγωγο πολυώνυμο και στο άλλο ένα ανάγωγο πολυώνυμο). Άρα ο ισχυρισμός είναι προδήλως αληθής όταν $l = 1$.

Περίπτωση δεύτερη. Υποθέτουμε ότι $l \geq 2$. (Βάσει των προαναφερθέντων έχουμε $r \geq 2$.) Έστω $\tau\,(= \tau^{(j_0,l)}) \in \mathfrak{S}_l$ η αντιμετάθεση με τύπους ορισμού της τους

$$\tau\,(j) := j,\ \forall j \in \{1,...,l\}\setminus\{j_0,l\},\ \text{και}\ \tau\,(j_0) := l,\ \tau\,(l) := j_0.$$

Από την ισότητα $\theta_r(\mathsf{X}) = \theta'_{\tau(l)}(\mathsf{X})$ έπεται ότι

$$\prod_{\nu=1}^{r} \theta_\nu(\mathsf{X}) = \prod_{j=1}^{l} \theta'_{\tau(j)}(\mathsf{X}) \Rightarrow \prod_{\nu=1}^{r-1} \theta_\nu(\mathsf{X}) = \prod_{j=1}^{l-1} \theta'_{\tau(j)}(\mathsf{X}).$$

Επειδή $\deg\left(\prod_{\nu=1}^{r-1} \theta_\nu(\mathsf{X})\right) < n$, από την επαγωγική μας υπόθεση συνάγουμε ότι $r-1 = l-1 \Rightarrow r = l$ και ότι υπάρχει μια μετάταξη $\rho \in \mathfrak{S}_{r-1}$, ούτως ώστε να ισχύει

$$\theta_\nu(\mathsf{X}) = \theta'_{\rho(\tau(\nu))}(\mathsf{X}),\ \forall \nu \in \{1,...,r-1\}.$$

Θεωρώντας τή μετάταξη $\sigma \in \mathfrak{S}_r$ με τύπους ορισμού της τους $\sigma(\nu) := \rho(\tau\,(\nu))$, $\forall \nu \in \{1,...,r-1\}$, και $\sigma(r) := \tau\,(r) = j_0$, καταλήγουμε στις ισότητες (3.25). □

3.5.9 Σημείωση. (i) Η (μέχρις αναδιατάξεως των παραγόντων) μονοσημάντως ορισμένη παράσταση (3.23) καλείται **παράσταση τού** $\varphi(\mathsf{X})$ **ως γινομένου αναγώγων μονικών πολυωνύμων** ή **αποσύνθεση τού** $\varphi(\mathsf{X})$ **σε γινόμενο αναγώγων μονικών**

πολυωνύμων[10].

(ii) Εάν στην παράσταση (3.23) τυγχάνει να ισχύει

$$\theta_1(\mathsf{X}) = \theta_2(\mathsf{X}) = \cdots = \theta_r(\mathsf{X}) =: \psi(\mathsf{X}),$$

τότε $\varphi(\mathsf{X}) = c\,\psi(\mathsf{X})^r$. Ειδάλλως, για να συμπτύξουμε στην (3.23) όσα εκ των $\theta_1(\mathsf{X}), \theta_2(\mathsf{X}),..., \theta_r(\mathsf{X})$ είναι πολλαπλώς εμφανιζόμενα (με την εισαγωγή δυνάμεων) μπορούμε (πιθανώς ύστερα από μια αναδιάταξη δεικτών) να υποθέσουμε ότι

$$\theta_1(\mathsf{X}) = \cdots = \theta_{j_1}(\mathsf{X}), \theta_{j_1+1}(\mathsf{X}) = \cdots = \theta_{j_2}(\mathsf{X}), \cdots\cdots, \theta_{j_{k-1}+1}(\mathsf{X}) = \cdots = \theta_{j_k}(\mathsf{X})$$

για κατάλληλα $\{j_1, j_2,..., j_k\} \subseteq \{1,..., r\},\ 2 \leq k \leq r$, με

$$1 \leq j_1 < j_2 < \cdots < j_{k-1} < j_k = r$$

και $\theta_{j_i}(\mathsf{X}) \neq \theta_{j_{i'}}(\mathsf{X})$ για οιουσδήποτε $i, i' \in \{1,..., k\}$, $i \neq i'$. Θέτοντας

$$m_1 := j_1,\ m_2 := j_2 - j_1,\ ...,\ m_k := j_k - j_{k-1}, \quad \psi_i(\mathsf{X}) := \theta_{j_i}(\mathsf{X}),\ \forall i \in \{1,..., k\},$$

το $\varphi(\mathsf{X})$ γράφεται ως

$$\boxed{\varphi(\mathsf{X}) = c \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i}} \tag{3.26}$$

Η παράσταση (3.26) καλείται **συνεπτυγμένη αποσύνθεση τού** $\varphi(\mathsf{X})$ (σε γινόμενο αναγώγων μονικών πολυωνύμων) και είναι (σε πολλές περιπτώσεις) πιο εύχρηστη από την (3.23). Μάλιστα, έχουμε και τη δυνατότητα να την *γενικεύσουμε ελαφρώς*, ούτως ώστε, συν τοις άλλοις, να μπορούμε να συμπεριλαμβάνουμε σε αυτήν ακόμη και τα σταθερά πολυώνυμα. Προς τούτο αρκεί να επιτρέπουμε σε κάποιους (ή και σε όλους) τους εκθέτες $m_1,..., m_k$ να λαμβάνουν *και* την τιμή 0.

(iii) Ενίοτε, όταν εργαζόμαστε με δύο (ή περισσότερα) πολυώνυμα, είναι αρκούντως διευκολυντικό το να υιοθετούμε την εξής *σύμβαση*: Γράφουμε (λαμβάνοντας υπ' όψιν τα προαναφερθέντα στο (ii)) τις (υπό την ευρεία έννοια) συνεπτυγμένες αποσυνθέσεις τους κατά τέτοιον τρόπο, ώστε τα σε αυτές εμφανιζόμενα ανάγωγα μονικά πολυώνυμα να είναι τα *ίδια*. (Τούτο επιτυγχάνεται με την συμπερίληψη *όλων* των αναγώγων μονικών παραγόντων που εμφανίζονται σε *όλα* τα θεωρούμενα πολυώνυμα στις εν λόγω *υπό την ευρεία έννοια* συνεπτυγμένες αποσυνθέσεις,

[10]Εν προκειμένω, για λόγους συντομίας, *υπονοείται σιωπηρώς* ότι στην εν λόγω αποσύνθεση συμπεριλαμβάνεται (προτασσόμενος σε αυτήν) ο επικεφαλής συντελεστής c τού $\varphi(\mathsf{X})$. (Παρότι ο ίδιος, ως πολυώνυμο βαθμού 0, *δεν είναι* ανάγωγο πολυώνυμο, το γινόμενο αυτού με οιοδήποτε εκ των $\theta_1(\mathsf{X}),..., \theta_n(\mathsf{X})$ *είναι* ανάγωγο αλλά *δεν είναι* μονικό για $c \neq 1_K$. Γι' αυτόν τον λόγο ορισμένοι συγγραφείς αποφεύγουν να χρησιμοποιούν το επίθετο *μονικός* στη σχετική ορολογία, έστω κι αν δι' αυτού τού τρόπου αποδυναμώνουν εν μέρει το τι ακριβώς δίδει το θεώρημα 3.5.8!)

καθόσον είναι δυνατόν να προσθέτουμε παράγοντες υψούμενους στο 0 κατά το δοκούν.) Επί παραδείγματι, *οιαδήποτε* $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in K[\mathsf{X}]$ μπορούν να γραφούν υπό τη μορφή

$$\varphi_1(\mathsf{X}) = c_1 \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}},\ \varphi_2(\mathsf{X}) = c_2 \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}$$

όπου $c_1, c_2 \in K, \psi_1(\mathsf{X}),..., \psi_k(\mathsf{X})$ ανάγωγα και μονικά και $m_i^{[1]}, m_i^{[2]} \in \mathbb{N}_0$ κατάλληλοι εκθέτες για κάθε $i \in \{1,..., k\}$. Σημειωτέον ότι

$$\varphi_1(\mathsf{X}) = \varphi_2(\mathsf{X}) \Leftrightarrow [c_1 = c_2 \text{ και } m_i^{[1]} = m_i^{[2]}, \forall i \in \{1,..., k\}].$$

3.5.10 Πόρισμα. *Έστω* $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ *τυχόν πολυώνυμο και έστω* (3.26) *η συνεπτυγμένη αποσύνθεση αυτού* (*υπό την ευρεία έννοια,* βλ. 3.5.9 (iii)). *Εάν* $\alpha(\mathsf{X}) \in K[\mathsf{X}]$, *τότε ισχύει η αμφίπλευρη συνεπαγωγή*

$$\alpha(\mathsf{X}) \mid \varphi(\mathsf{X}) \Longleftrightarrow \left[\begin{array}{c} \alpha(\mathsf{X}) = a \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i'}, \\ \text{για κάποιους } m_1',..., m_k' \in \mathbb{N}_0 : m_i' \leq m_i, \\ \forall i \in \{1,..,k\}, \text{ και κάποιο } a \in K : a \mid c \end{array}\right]$$

ΑΠΟΔΕΙΞΗ. Η συνεπαγωγή "$\Leftarrow$" είναι προφανής. Θα αποδείξουμε την "$\Rightarrow$". Υποθέτουμε ότι $\alpha(\mathsf{X}) \mid \varphi(\mathsf{X})$. Τότε υπάρχει κάποιο $\beta(\mathsf{X}) \in K[\mathsf{X}]$, τέτοιο ώστε να ισχύει $\varphi(\mathsf{X}) = \alpha(\mathsf{X})\beta(\mathsf{X})$. Εάν

$$\alpha(\mathsf{X}) = a \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i'},\ \beta(\mathsf{X}) = b \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i''},\ a, b \in K,$$

είναι οι (υπό την ευρεία έννοια) συνεπτυγμένες αποσυνθέσεις των $\alpha(\mathsf{X})$ και $\beta(\mathsf{X})$ (νοούμενες όπως στο εδ. 3.5.9 (iii)), τότε

$$\varphi(\mathsf{X}) = ab \left(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i'}\right)\left(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i''}\right) = ab \left(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i'+m_i''}\right),$$

οπότε $c = ab$ και $m_i = m_i' + m_i'' \geq m_i'$ για κάθε $i \in \{1,..., k\}$. □

3.5.11 Πόρισμα. *Εάν τα* $\varphi(\mathsf{X}), \psi(\mathsf{X}) \in K[\mathsf{X}]$ *είναι ανάγωγα υπεράνω τού* K *και μονικά, και* $\varphi(\mathsf{X}) \mid \psi(\mathsf{X})^m$ *για κάποιον* $m \in \mathbb{N}$, *τότε* $\varphi(\mathsf{X}) = \psi(\mathsf{X})^{m'}$ *για κάποιον* $m' \in \mathbb{N}$, *όπου* $m' \leq m$.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το πόρισμα 3.5.10. □

3.5.12 Πόρισμα. *Εάν τα* $\varphi(\mathsf{X}), \theta(\mathsf{X}) \in K[\mathsf{X}]$ *είναι ανάγωγα υπεράνω τού* K *και μονικά, και* $\varphi(\mathsf{X}) \neq \theta(\mathsf{X})$, *τότε*

$$\text{μκδ}(\varphi(\mathsf{X})^m, \theta(\mathsf{X})^n) = 1_K,\ \forall (m, n) \in \mathbb{N} \times \mathbb{N}.$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $\delta(\mathsf{X}) := \text{μκδ}(\varphi(\mathsf{X})^m, \theta(\mathsf{X})^n)$ έχει βαθμό ≥ 1. Σύμφωνα με την πρόταση 3.5.5 υφίσταται τουλάχιστον ένα ανάγωγο πολυώνυμο $\psi(\mathsf{X})$ υπεράνω τού K το οποίο διαιρεί το $\delta(\mathsf{X})$. Αυτό εκφράζεται ως γινόμενο $\psi(\mathsf{X}) = c\hat{\psi}(\mathsf{X})$ μιας σταθεράς $c \in K\setminus\{0_K\}$ (που ισούται με τον επικεφαλής συντελεστή του) και ενός αναγώγου (υπεράνω τού K) *μονικού* πολυωνύμου $\hat{\psi}(\mathsf{X})$. Προφανώς,

$$\left.\begin{array}{c}\hat{\psi}(\mathsf{X}) \mid \psi(\mathsf{X}) \\ \psi(\mathsf{X}) \mid \delta(\mathsf{X})\end{array}\right\} \Longrightarrow \hat{\psi}(\mathsf{X}) \mid \delta(\mathsf{X})$$

και, ως εκ τούτου,

$$\left.\begin{array}{c}\delta(\mathsf{X}) \mid \varphi(\mathsf{X}) \\ \delta(\mathsf{X}) \mid \theta(\mathsf{X})\end{array}\right\} \Rightarrow \left\{\begin{array}{c}\hat{\psi}(\mathsf{X}) \mid \varphi(\mathsf{X}) \\ \hat{\psi}(\mathsf{X}) \mid \theta(\mathsf{X})\end{array}\right\} \Rightarrow \left\{\begin{array}{c}\hat{\psi}(\mathsf{X}) \mid \varphi(\mathsf{X})^m \\ \hat{\psi}(\mathsf{X}) \mid \theta(\mathsf{X})^n\end{array}\right\}.$$

Επειδή $\deg(\hat{\psi}(\mathsf{X})) \geq 1$, το πόρισμα 3.5.11 μας πληροφορεί ότι

$$\left\{\begin{array}{l}\exists m' \in \mathbb{N},\ m' \leq m : \hat{\psi}(\mathsf{X}) = \varphi(\mathsf{X})^{m'} \\ \exists n' \in \mathbb{N},\ n' \leq n : \hat{\psi}(\mathsf{X}) = \theta(\mathsf{X})^{n'}\end{array}\right\} \Rightarrow \varphi(\mathsf{X})^{m'} = \theta(\mathsf{X})^{n'},$$

οπότε $m' = n'$ και $\varphi(\mathsf{X}) = \theta(\mathsf{X})$ (λόγω τού μονοσημάντου τής παραστάσεως (3.23)). Άτοπο! Επομένως, $\deg(\delta(\mathsf{X})) = 0$ (διότι $\delta(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$) και $\delta(\mathsf{X}) = 1_K$ (διότι ο μέγιστος κοινός διαιρέτης $\delta(\mathsf{X})$ είναι εξ ορισμού *μονικό* πολυώνυμο). □

3.5.13 Πόρισμα. *Εάν τα $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X}) \in K[\mathsf{X}]$, $k \in \mathbb{N}$, $k \geq 2$, είναι πολυώνυμα θετικού βαθμού και πρώτα μεταξύ τους ανά δύο, τότε*

$$\text{μκδ}\left(\prod_{j=1}^{k-1} \varphi_j(\mathsf{X}), \varphi_k(\mathsf{X})\right) = 1_K.$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $\delta(\mathsf{X}) := \text{μκδ}(\prod_{j=1}^{k-1} \varphi_j(\mathsf{X}), \varphi_k(\mathsf{X}))$ έχει βαθμό ≥ 1. Σύμφωνα με την πρόταση 3.5.5 υφίσταται τουλάχιστον ένα ανάγωγο πολυώνυμο $\psi(\mathsf{X})$ υπεράνω τού K το οποίο διαιρεί το $\delta(\mathsf{X})$. Αυτό εκφράζεται ως γινόμενο $\psi(\mathsf{X}) = c\hat{\psi}(\mathsf{X})$ μιας σταθεράς $c \in K\setminus\{0_K\}$ (που ισούται με τον επικεφαλής συντελεστή του) και ενός αναγώγου (υπεράνω τού K) *μονικού* πολυωνύμου $\hat{\psi}(\mathsf{X})$. Προφανώς,

$$\left.\begin{array}{c}\hat{\psi}(\mathsf{X}) \mid \psi(\mathsf{X}) \\ \psi(\mathsf{X}) \mid \delta(\mathsf{X})\end{array}\right\} \Longrightarrow \hat{\psi}(\mathsf{X}) \mid \delta(\mathsf{X})$$

και, ως εκ τούτου,

$$\left.\begin{array}{c}\delta(\mathsf{X}) \mid \prod_{j=1}^{k-1} \varphi_j(\mathsf{X}) \\ \delta(\mathsf{X}) \mid \varphi_k(\mathsf{X})\end{array}\right\} \Rightarrow \left\{\begin{array}{c}\hat{\psi}(\mathsf{X}) \mid \prod_{j=1}^{k-1} \varphi_j(\mathsf{X}) \\ \hat{\psi}(\mathsf{X}) \mid \varphi_k(\mathsf{X})\end{array}\right\}.$$

Επειδή $\hat{\psi}(\mathsf{X}) \mid \prod_{j=1}^{k-1}\varphi_j(\mathsf{X})$, υπάρχει κάποιος $j_0 \in \{1,...,k-1\}$, τέτοιος ώστε να ισχύει $\hat{\psi}(\mathsf{X}) \mid \varphi_{j_0}(\mathsf{X})$. Τούτο προκύπτει από το ότι το $\hat{\psi}(\mathsf{X})$, όντας ανάγωγο (υπεράνω τού K) και μονικό, οφείλει να συμπεριλαμβάνεται στους (ανάγωγους) παράγοντες τής συνεπτυγμένης αποσυνθέσεως *τουλάχιστον ενός* εκ των $\varphi_1(\mathsf{X}),...,\varphi_k(\mathsf{X})$. Εκ των ανωτέρω έπεται ότι

$$\left.\begin{matrix}\hat{\psi}(\mathsf{X}) \mid \varphi_{j_0}(\mathsf{X}) \\ \hat{\psi}(\mathsf{X}) \mid \varphi_k(\mathsf{X})\end{matrix}\right\} \Longrightarrow \hat{\psi}(\mathsf{X}) \mid \mu\kappa\delta(\varphi_{j_0}(\mathsf{X}), \varphi_k(\mathsf{X})) = 1_K.$$

Άτοπο! Κατά συνέπειαν, $\deg(\delta(\mathsf{X})) = 0$ (διότι $\delta(\mathsf{X}) \neq \mathbf{0}_{K[\mathsf{X}]}$) και $\delta(\mathsf{X}) = 1_K$ (διότι ο μέγιστος κοινός διαιρέτης $\delta(\mathsf{X})$ είναι εξ ορισμού *μονικό* πολυώνυμο). □

3.5.14 Πρόταση. *Έστω ότι τα πολυώνυμα $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$ έχουν τις*

$$\varphi_1(\mathsf{X}) = c_1 \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}},\ \varphi_2(\mathsf{X}) = c_2 \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}$$

ως συνεπτυγμένες αποσυνθέσεις τους (υπό την ευρεία έννοια). Τότε ισχύουν τα εξής:

(i) *Ο μέγιστος κοινός διαιρέτης των $\varphi_1(\mathsf{X})$ και $\varphi_2(\mathsf{X})$ είναι το πολυώνυμο*

$$\boxed{\mu\kappa\delta(\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})) = \prod_{i=1}^{k} \psi_i(\mathsf{X})^{\min\{m_i^{[1]}, m_i^{[2]}\}}.} \tag{3.27}$$

(ii) *Το ελάχιστο κοινό πολλαπλάσιο των $\varphi_1(\mathsf{X})$ και $\varphi_2(\mathsf{X})$ είναι το*

$$\boxed{\varepsilon\kappa\pi(\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})) = \prod_{i=1}^{k} \psi_i(\mathsf{X})^{\max\{m_i^{[1]}, m_i^{[2]}\}}.} \tag{3.28}$$

ΑΠΟΔΕΙΞΗ. (i) Κατ' αρχάς,

$$\mu\kappa\delta(\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})) = \mu\kappa\delta(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}}, \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}})$$

(βλ. 3.3.7 (iv)). Επειδή $\min\{m_i^{[1]}, m_i^{[2]}\} \leq m_i^{[1]}$ και $\min\{m_i^{[1]}, m_i^{[2]}\} \leq m_i^{[2]}$ για κάθε $i \in \{1,...,k\}$, το πολυώνυμο $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{\min\{m_i^{[1]}, m_i^{[2]}\}}$ διαιρεί αμφότερα τα $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}}$ και $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}$ (βλ. πόρισμα 3.5.10). Εκτός τούτου, εάν

$$\theta(\mathsf{X}) = c \prod_{i=1}^{k} \psi_i(\mathsf{X})^{n_i}$$

είναι η (υπό την ευρεία έννοια) συνεπτυγμένη αποσύνθεση ενός κοινού διαιρέτη $\theta(\mathsf{X})$ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$, τότε

$$[n_i \leq m_i^{[1]} \text{ και } n_i \leq m_i^{[2]}] \Rightarrow n_i \leq \min\{m_i^{[1]}, m_i^{[2]}\},\ \forall i \in \{1,...,k\}.$$

(Σημειωτέον ότι $c \in K \setminus \{0_K\} \Rightarrow c \mid 1_K$, καθώς ισχύει $cc^{-1} = 1_K$.) Επομένως, $\theta(\mathsf{X}) \mid \prod_{i=1}^{k} \psi_i(\mathsf{X})^{\min\{m_i^{[1]}, m_i^{[2]}\}}$ (εκ νέου μέσω τού πορίσματος 3.5.10) και η (3.27) είναι αληθής (βλ. 3.3.5).

(ii) Κατ' αρχάς,

$$\text{εκπ}(\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})) = \text{εκπ}(\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}}, \prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}})$$

(βλ. 3.3.20 (iv)). Επειδή $\max\{m_i^{[1]}, m_i^{[2]}\} \geq m_i^{[1]}$ και $\max\{m_i^{[1]}, m_i^{[2]}\} \geq m_i^{[2]}$ για κάθε $i \in \{1,...,k\}$, αμφότερα τα $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[1]}}$ και $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{m_i^{[2]}}$ διαιρούν το πολυώνυμο $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{\max\{m_i^{[1]}, m_i^{[2]}\}}$ (βλ. πόρισμα 3.5.10). Εκτός τούτου, εάν

$$\zeta(\mathsf{X}) = c \prod_{i=1}^{k} \psi_i(\mathsf{X})^{n_i}$$

είναι η (υπό την ευρεία έννοια) συνεπτυγμένη αποσύνθεση ενός κοινού πολλαπλασίου $\zeta(\mathsf{X})$ των $\varphi_1(\mathsf{X}), \varphi_2(\mathsf{X})$, τότε

$$[n_i \geq m_i^{[1]} \text{ και } n_i \geq m_i^{[2]}] \Rightarrow n_i \geq \max\{m_i^{[1]}, m_i^{[2]}\}, \ \forall i \in \{1,...,k\}.$$

Επομένως, $\prod_{i=1}^{k} \psi_i(\mathsf{X})^{\max\{m_i^{[1]}, m_i^{[2]}\}} \mid \zeta(\mathsf{X})$ (εκ νέου μέσω τού πορίσματος 3.5.10) και η (3.28) είναι αληθής (βλ. 3.3.18). □

3.6 ΔΙΑΣΠΑΣΕΙΣ ΣΕ ΠΡΩΤΟΒΑΘΜΙΟΥΣ ΠΑΡΑΓΟΝΤΕΣ

Το ακόλουθο λήμμα γενικεύει το προηγηθέν πόρισμα 3.4.5.

3.6.1 Λήμμα. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geq 1$. Εάν υποθέσουμε ότι τα στοιχεία $\lambda_1,...,\lambda_k \in K$ ($k \in \mathbb{N},\ k \leq n$) είναι k σαφώς διακεκριμένες θέσεις μηδενισμού τού $\varphi(\mathsf{X})$ και ότι*

$$(\mathsf{X} - \lambda_1)^{\nu_1} \mid \varphi(\mathsf{X}), \ ..... \ (\mathsf{X} - \lambda_k)^{\nu_k} \mid \varphi(\mathsf{X}),$$

για κάποιους $\nu_1,...,\nu_k \in \mathbb{N}$, τότε $\prod_{i=1}^{k} (\mathsf{X} - \lambda_i)^{\nu_i} \mid \varphi(\mathsf{X})$.

ΑΠΟΔΕΙΞΗ. Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Για $k = 1$ τούτο είναι προφανές. Υποθέτουμε ότι $k \geq 2$ και ότι ο ισχυρισμός είναι αληθής για $k - 1$ σαφώς διακεκριμένες θέσεις μηδενισμού τού $\varphi(\mathsf{X})$. Το $\mathsf{X} - \lambda_i$ (όντας πρωτοβάθμιο πολυώνυμο) είναι ανάγωγο υπεράνω τού K για κάθε $i \in \{1,...,k\}$. Εξάλλου, για οιουσδήποτε $i, j \in \{1,...,k\}$, $i \neq j$, έχουμε

$$\lambda_i \neq \lambda_j \Rightarrow \mathsf{X} - \lambda_i \neq \mathsf{X} - \lambda_j \underset{3.5.12}{\Longrightarrow} \text{μκδ}((\mathsf{X} - \lambda_i)^{\nu_i}, (\mathsf{X} - \lambda_j)^{\nu_j}) = 1_K.$$

Κατά το πόρισμα 3.5.13,

$$\text{μκδ}(\textstyle\prod_{i=1}^{k-1}(\mathsf{X}-\lambda_i)^{\nu_i}, (\mathsf{X}-\lambda_k)^{\nu_k}) = 1_K. \tag{3.29}$$

Σύμφωνα με την αρχική και την επαγωγική μας υπόθεση,

$$\left.\begin{matrix}(\mathsf{X}-\lambda_k)^{\nu_k} \mid \varphi(\mathsf{X}) \\ \prod_{i=1}^{k-1}(\mathsf{X}-\lambda_i)^{\nu_i} \mid \varphi(\mathsf{X})\end{matrix}\right\} \Longrightarrow \prod_{i=1}^{k}(\mathsf{X}-\lambda_i)^{\nu_i} \mid \varphi(\mathsf{X})$$

(μέσω τής (3.29) και τού πορίσματος 3.3.17). □

3.6.2 Λήμμα. *Έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geq 1$. Εάν τα στοιχεία $\lambda_1,...,\lambda_k \in K$ ($k \in \mathbb{N}$, $k \leq n$) είναι (όλες) οι σαφώς διακεκριμένες θέσεις μηδενισμού τού $\varphi(\mathsf{X})$, τότε υπάρχει $\psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, τέτοιο ώστε το $\varphi(\mathsf{X})$ να γράφεται υπό τη μορφή*

$$\varphi(\mathsf{X}) = \left(\prod_{i=1}^{k}(\mathsf{X}-\lambda_i)^{m_i}\right)\psi(\mathsf{X}), \tag{3.30}$$

όπου $m_i = \text{mult}(\varphi(\mathsf{X}); \lambda_i)$, $\psi(\lambda_i) \neq 0_K$, $\forall i \in \{1,...,k\}$, και $\sum_{i=1}^{k} m_i \leq n$.

ΑΠΟΔΕΙΞΗ. Επειδή $(\mathsf{X}-\lambda_i)^{m_i} \mid \varphi(\mathsf{X})$ για κάθε $i \in \{1,...,k\}$, το λήμμα 3.6.1 μας πληροφορεί ότι το γινόμενό τους είναι διαιρέτης τού $\varphi(\mathsf{X})$. Ως εκ τούτου, το $\varphi(\mathsf{X})$ γράφεται υπό τη μορφή (3.30) για κάποιο κατάλληλο $\psi(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$ και

$$[m_i \geq 1,\ \forall i \in \{1,...,k\}] \Rightarrow n = \deg(\psi(\mathsf{X})) + \sum_{i=1}^{k} m_i \geq \sum_{i=1}^{k} m_i.$$

Επιπροσθέτως, $\psi(\lambda_i) \neq 0_K$, $\forall i \in \{1,...,k\}$, διότι εάν υπήρχε κάποιος δείκτης $i_0 \in \{1,...,k\}$ με $\psi(\lambda_{i_0}) = 0_K$, τότε θα είχαμε $\mathsf{X}-\lambda_{i_0} \mid \psi(\mathsf{X})$ και θα καταλήγαμε στο ότι $(\mathsf{X}-\lambda_{i_0})^{m_{i_0}+1} \mid \varphi(\mathsf{X})$ (ήτοι σε κάτι που θα αντέκειτο στον ορισμό τής πολλαπλότητας $m_{i_0} = \text{mult}(\varphi(\mathsf{X}); \lambda_{i_0})$). □

3.6.3 Ορισμός. Έστω L μια επέκταση ενός σώματος K και έστω $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ βαθμού $n \geq 1$. Εάν υπάρχουν (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία $\lambda_1,...,\lambda_n$ τού L, τέτοια ώστε να ισχύει η ισότητα

$$\varphi(\mathsf{X}) = c\,(\mathsf{X}-\lambda_1)(\mathsf{X}-\lambda_2)\cdots(\mathsf{X}-\lambda_n) \tag{3.31}$$

(για κάποιο $c \in K \setminus \{0_K\}$), τότε λέμε ότι το πολυώνυμο $\varphi(\mathsf{X})$ **διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού** L.

3.6.4 Θεώρημα. (Κριτήριο μη υπάρξεως πολλαπλών θ.μ.) *Εάν* $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ *είναι ένα πολυώνυμο βαθμού* $n \geq 1$ *το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω μιας (όχι κατ' ανάγκην γνήσιας) επεκτάσεως* L *τού* K*, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Το* $\varphi(\mathsf{X})$ *δεν διαθέτει καμία πολλαπλή θέση μηδενισμού εντός τού* L *(δηλαδή τα* $\lambda_1,...,\lambda_n$ *σε μια παράστασή του* (3.31) *είναι σαφώς διακεκριμένα).*

(ii) $\text{μκδ}(\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))) = 1_K\ (= 1_L)$.

ΑΠΟΔΕΙΞΗ. *Επισήμανση*: Επειδή ο μέγιστος κοινός διαιρέτης των $\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))$ *εντός τού* $K[\mathsf{X}]$ ισούται με τον μέγιστο κοινό διαιρέτη των $\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))$ *εντός τού* $L[\mathsf{X}]$ (βλ. πρόταση 3.3.11), στην απόδειξη οι υπολογισμοί θα γίνουν (για ευνόητους λόγους) *εντός τού* $L[\mathsf{X}]$.

(i)⇒(ii) Ας υποθέσουμε ότι το πολυώνυμο $\text{μκδ}(\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X})))$ έχει βαθμό ≥ 1. Επειδή το $\varphi(\mathsf{X})$ διασπάται (εξ υποθέσεως) σε πρωτοβάθμιους παράγοντες υπεράνω τού L, υπάρχει κάποιος κοινός διαιρέτης και, ως εκ τούτου, και κάποια κοινή θέση μηδενισμού $\lambda \in L$ των $\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))$, οπότε

$$\left\{ \begin{array}{l} \exists \alpha(\mathsf{X}) \in L[\mathsf{X}] : \varphi(\mathsf{X}) = (\mathsf{X} - \lambda)\alpha(\mathsf{X}), \\ \exists \beta(\mathsf{X}) \in L[\mathsf{X}] : \mathcal{D}(\varphi(\mathsf{X})) = (\mathsf{X} - \lambda)\beta(\mathsf{X}). \end{array} \right\}$$

Επομένως, $(\mathsf{X} - \lambda)\beta(\mathsf{X}) = \mathcal{D}((\mathsf{X} - \lambda)\alpha(\mathsf{X})) = \alpha(\mathsf{X}) + (\mathsf{X} - \lambda)\mathcal{D}(\alpha(\mathsf{X}))$ και

$$\mathsf{X} - \lambda \mid \alpha(\mathsf{X}) \Longrightarrow (\mathsf{X} - \lambda)^2 \mid \varphi(\mathsf{X}).$$

Τούτο σημαίνει ότι το $\lambda \in L$ είναι μια πολλαπλή (τουλάχιστον διπλή) θέση μηδενισμού τού $\varphi(\mathsf{X})$. Άτοπο!

(ii)⇒(i) Έστω λ *τυχούσα* θέση μηδενισμού τού $\varphi(\mathsf{X})$ *εντός τού* L με πολλαπλότητα $m \geq 1$. Η πρόταση 3.4.14 (με το L στη θέση τού εκεί παρατεθέντος K) μας πληροφορεί ότι

$$\exists \psi(\mathsf{X}) \in L[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X} - \lambda)^m \psi(\mathsf{X})$$

με $\psi(\lambda) \neq 0_K$. Επειδή (σύμφωνα με το (iii) τού λήμματος 3.4.16) ισχύει

$$\mathcal{D}(\varphi(\mathsf{X})) = m\,(\mathsf{X} - \lambda)^{m-1}\,\psi(\mathsf{X}) + (\mathsf{X} - \lambda)^m\,\mathcal{D}(\psi(\mathsf{X})),$$

έχουμε

$$\left. \begin{array}{l} (\mathsf{X} - \lambda)^{m-1} \mid \varphi(\mathsf{X}) \\ (\mathsf{X} - \lambda)^{m-1} \mid \mathcal{D}(\varphi(\mathsf{X})) \end{array} \right\} \Rightarrow (\mathsf{X} - \lambda)^{m-1} \mid \text{μκδ}(\varphi(\mathsf{X}), \mathcal{D}(\varphi(\mathsf{X}))) = 1_L,$$

ήτοι $m - 1 = \deg((\mathsf{X} - \lambda)^{m-1}) \leq 0 \Rightarrow m = 1$. □

3.6.5 Παρατήρηση. Το κριτήριο 3.6.4 είναι λίαν χρήσιμο, καθώς μας επιτρέπει να ελέγξουμε το κατά πόσον το $\varphi(\mathsf{X})$ διαθέτει (ή δεν διαθέτει) πολλαπλές θέσεις μηδενισμού εντός τού L *χωρίς* να υποχρεούμεθα *να υπολογίσουμε τις θέσεις μηδενισμού του*! (Δοθέντος ενός συγκεκριμένου $\varphi(\mathsf{X})$, για την πρακτική εφαρμογή του είναι αρκετό να εκτελεσθεί ένας και μόνον ευκλείδειος αλγόριθμος.)

Το επόμενο θεώρημα δίδει δύο ικανές και αναγκαίες συνθήκες, υπό τις οποίες ένα (μη σταθερό) πολυώνυμο $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού (ιδίου τού) K.

3.6.6 Θεώρημα. *Εάν* $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ *είναι ένα πολυώνυμο βαθμού* $n \geq 1$, *τότε οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Το* $\varphi(\mathsf{X})$ *διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού* K.

(ii) *Εάν το* $\theta(\mathsf{X}) \in K[\mathsf{X}]$ *είναι ένας ανάγωγος (υπεράνω τού* K*) διαιρέτης τού* $\varphi(\mathsf{X})$, *τότε* $\deg(\theta(\mathsf{X})) = 1$.

(iii) *Υπάρχουν* $\lambda_1,...,\lambda_k \in K$ ($k \in \mathbb{N},\ k \leq n$), *τέτοια ώστε να ισχύει η ισότητα* $\sum_{i=1}^{k} \mathrm{mult}(\varphi(\mathsf{X}); \lambda_i) = n$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν υπάρχουν (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία $\lambda_1,...,\lambda_n$ τού K, τέτοια ώστε να ισχύει η ισότητα

$$\varphi(\mathsf{X}) = c(\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2)\cdots(\mathsf{X} - \lambda_n),$$

(για κάποιο $c \in K \setminus \{0_K\}$) και το $\theta(\mathsf{X}) \in K[\mathsf{X}]$ είναι ένας ανάγωγος διαιρέτης τού $\varphi(\mathsf{X})$, τότε εφαρμόζοντας το λήμμα 3.5.7 για τα $\theta(\mathsf{X})$ και $\varphi(\mathsf{X})$ συνάγουμε ότι

$$\exists i_0 \in \{1,...,n\} :\ \theta(\mathsf{X}) = c\,(\mathsf{X} - \lambda_{i_0})\,,$$

για κάποιο $c \in K \setminus \{0_K\}$, οπότε $\deg(\theta(\mathsf{X})) = 1$.

(ii)⇒(iii) Έστω ότι τα $\lambda_1,...,\lambda_k \in K$ ($k \in \mathbb{N},\ k \leq n$) είναι (όλες) οι σαφώς διακεκριμένες θέσεις μηδενισμού τού $\varphi(\mathsf{X})$. Σύμφωνα με το λήμμα 3.6.2 υπάρχει $\psi(\mathsf{X}) \in K\,[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, τέτοιο ώστε το $\varphi(\mathsf{X})$ να γράφεται υπό τη μορφή

$$\varphi(\mathsf{X}) = \left(\prod_{i=1}^{k} (\mathsf{X} - \lambda_i)^{m_i}\right) \psi(\mathsf{X}),$$

όπου $m_i = \mathrm{mult}(\varphi(\mathsf{X}); \lambda_i)$, $\psi(\lambda_i) \neq 0_K$, $\forall i \in \{1,...,k\}$. Εάν υποθέσουμε ότι $\deg(\psi(\mathsf{X})) \geq 1$, τότε (σύμφωνα με την πρόταση 3.5.5) υπάρχει κάποιος ανάγωγος διαιρέτης $\theta(\mathsf{X}) \in K[\mathsf{X}]$ τού $\psi(\mathsf{X})$ (και, κατ' επέκτασιν, και τού $\varphi(\mathsf{X})$, διότι $\psi(\mathsf{X}) \mid \varphi(\mathsf{X})$). Εξ υποθέσεως, $\deg(\theta(\mathsf{X})) = 1$, οπότε το $\theta(\mathsf{X})$ διαθέτει μια θέση μηδενισμού $\lambda \in K$. Κατά συνέπειαν,

$$\theta(\lambda) = 0_K \Rightarrow \psi(\lambda) = 0_K \Rightarrow \varphi(\lambda) = 0_K \Rightarrow \exists i_0 \in \{1,...,k\} : \lambda = \lambda_{i_0}.$$

Αυτό σημαίνει ότι $\psi(\lambda_{i_0}) = 0_K$. Άτοπο! Άρα $\deg(\psi(\mathsf{X})) = 0$ και $\sum_{i=1}^{k} m_i = n$.

(iii)⇒(i) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι ισχύει $\text{mult}(\varphi(\mathsf{X}); \lambda_i) \geq 1$ για κάθε $i \in \{1,...,k\}$ (διότι εάν υπάρχει ένα μη κενό υποσύνολο $\mathcal{A} \subsetneqq \{1,...,k\}$ με $\text{mult}(\varphi(\mathsf{X}); \lambda_j) = 0$ για κάθε $j \in \mathcal{A}$, μπορούμε να χρησιμοποιήσουμε την ίδια επιχειρηματολογία για τα υπολειπόμενα λ_j, $j \in \{1,...,k\} \smallsetminus \mathcal{A}$). Κατά το λήμμα 3.6.2 το $\varphi(\mathsf{X})$ γράφεται υπό τη μορφή (3.30). Εξ αυτής έπεται ότι

$$\sum_{i=1}^{k} m_i = n = \deg(\psi(\mathsf{X})) + \sum_{i=1}^{k} m_i \Rightarrow \deg(\psi(\mathsf{X})) = 0,$$

οπότε το $\psi(\mathsf{X})$ είναι σταθερό μη μηδενικό πολυώνυμο και το $\varphi(\mathsf{X})$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K. □

Εάν το $\varphi(\mathsf{X}) \in K[\mathsf{X}]$ είναι ένα πολυώνυμο βαθμού $n \geq 1$ το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K, τότε αναπτύσσοντας το γινόμενο τού δευτέρου μέλους στην (3.31) καταλήγουμε σε σχέσεις μεταξύ των συντελεστών τού $\varphi(\mathsf{X})$ και των αθροισμάτων όλων των γινομένων των $\lambda_1,..., \lambda_n$ λαμβανομένων ανά k (των λεγομένων k-αστών *στοιχειωδών συμμετρικών συναρτήσεων* των $\lambda_1,..., \lambda_n$), όπου $k \in \{1,...,n\}$. Αυτές είχαν γίνει αντικείμενο μελέτης (σε ειδικές περιπτώσεις και για $K = \mathbb{R}$) ήδη από τα τέλη τού 16ου αιώνα, αναφέρονται δε σε εργασίες των Γάλλων μαθηματικών François Viète (1540-1603) και Albert Girard (1595-1632). Ο πρώτος (γνωστός και υπό το εκλατινισμένο επίθετο Vieta) περιορίσθηκε σε πολυώνυμα με θέσεις μηδενισμού που πληρούν κάποιες ειδικές συνθήκες, ενώ ο δεύτερος εξέτασε τη γενική περίπτωση (τρεις δεκαετίες αργότερα) και προέβη σε συστηματικότερη παρουσίαση των σχετικών τύπων.

3.6.7 Θεώρημα. (Τύποι τού Viète) *Έστω $\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^n \in K[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geq 1$ το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K. Εάν οι θέσεις μηδενισμού του είναι τα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία $\lambda_1,..., \lambda_n \in K$ και εάν θέσουμε*[11]

$$\boxed{s_k := \sum_{\substack{(j_1,...,j_k) \in \mathbb{N}^k: \\ 1 \leq j_1 < \cdots < j_k \leq n}} \lambda_{j_1} \lambda_{j_2} \cdots \lambda_{j_k},\ \forall k \in \{1,...,n\},} \tag{3.32}$$

και $s_0 := 1$, τότε

$$\boxed{s_k = (-1_K)^k\, a_n^{-1}\, a_{n-k},\ \forall k \in \{0,1,...,n\},} \tag{3.33}$$

[11] Όταν $k = 1$, τότε υπονοείται ότι το εν λόγω άθροισμα είναι το $\lambda_1 + \cdots + \lambda_n$.

ή, ισοδυνάμως,

$$\boxed{a_i = (-1_K)^{n-i}\, a_n s_{n-i},\ \forall i \in \{0,1,...,n\}.} \tag{3.34}$$

ΑΠΟΔΕΙΞΗ. Προφανώς, $a_n \neq 0_K$ και

$$\varphi(\mathsf{X}) = a_n(\mathsf{X}-\lambda_1)(\mathsf{X}-\lambda_2)\cdots(\mathsf{X}-\lambda_n)$$

είναι η διάσπαση τού $\varphi(\mathsf{X})$ σε πρωτοβάθμιους παράγοντες υπεράνω τού K. Επειδή

$$a_n^{-1}\varphi(\mathsf{X}) = (\mathsf{X}-\lambda_1)(\mathsf{X}-\lambda_2)\cdots(\mathsf{X}-\lambda_n),$$

αρκεί να αποδείξουμε την ισότητα

$$(\mathsf{X}-\lambda_1)(\mathsf{X}-\lambda_2)\cdots(\mathsf{X}-\lambda_n) = \mathsf{X}^n + \sum_{k=1}^{n}(-1_K)^k s_k \mathsf{X}^{n-k}. \tag{3.35}$$

Εάν $n=1$, τότε $s_1=\lambda_1$ και η (3.35) είναι αληθής. Υποθέτοντας ότι $n\geq 2$ και ότι ισχύει η ισότητα

$$\prod_{\nu=1}^{n-1}(\mathsf{X}-\lambda_\nu) = \mathsf{X}^{n-1} + \sum_{\varrho=1}^{n-1}(-1_K)^\varrho \sum_{\substack{(i_1,\ldots,i_\varrho)\in\mathbb{N}^\varrho:\\ 1\leq i_1<\cdots<i_\varrho\leq n-1}} \lambda_{i_1}\cdots\lambda_{i_\varrho}\mathsf{X}^{n-1-\varrho}$$

(για $n-1$ παράγοντες) παρατηρούμε ότι

$$\begin{aligned}
&(\mathsf{X}^{n-1} + \sum_{\varrho=1}^{n-1}(-1_K)^\varrho \sum_{\substack{(i_1,\ldots,i_\varrho)\in\mathbb{N}^\varrho:\\ 1\leq i_1<\cdots<i_\varrho\leq n-1}} \lambda_{i_1}\cdots\lambda_{i_\varrho}\mathsf{X}^{n-1-\varrho})(\mathsf{X}-\lambda_n)\\
&= \mathsf{X}^n + \sum_{k=1}^{n-1}(-1_K)^k \left(\sum_{\substack{(i_1,\ldots,i_k)\in\mathbb{N}^k:\\ 1\leq i_1<\cdots<i_k\leq n-1}} \lambda_{i_1}\cdots\lambda_{i_k} + \left(\sum_{\substack{(i'_1,\ldots,i'_{k-1})\in\mathbb{N}^{k-1}:\\ 1\leq i'_1<\cdots<i'_{k-1}\leq n-1}} \lambda_{i'_1}\cdots\lambda_{i'_{k-1}} \right)\lambda_n \right)\mathsf{X}^{n-k}\\
&+(-1_K)^n\lambda_1\cdots\lambda_n
\end{aligned}$$

όπου

$$\sum_{\substack{(i_1,\ldots,i_k)\in\mathbb{N}^k:\\ 1\leq i_1<\cdots<i_k\leq n-1}} \lambda_{i_1}\cdots\lambda_{i_k} + \left(\sum_{\substack{(i'_1,\ldots,i'_{k-1})\in\mathbb{N}^{k-1}:\\ 1\leq i'_1<\cdots<i'_{k-1}\leq n-1}} \lambda_{i'_1}\cdots\lambda_{i'_{k-1}} \right)\lambda_n = s_k,$$

οπότε η (3.35) είναι αληθής και σε αυτήν την περίπτωση. □

3.6.8 Παράδειγμα. Θεωρούμε το $\varphi(\mathsf{X}) := (\mathsf{X}+1)^{2\nu+1} - (\mathsf{X}-1)^{2\nu+1} \in \mathbb{C}\,[\mathsf{X}]$ (όπου $\nu \in \mathbb{N}$). Προφανώς,

$$\begin{aligned}\varphi(\mathsf{X}) &= \sum_{i=0}^{2\nu+1} \tbinom{2\nu+1}{i}\mathsf{X}^i - \sum_{i=0}^{2\nu+1} (-1)^{2\nu+1-i}\tbinom{2\nu+1}{i}\mathsf{X}^i \\ &= 2\,(2\nu+1)\,\mathsf{X}^{2\nu} + 2\tbinom{2\nu+1}{3}\mathsf{X}^{2\nu-2} + \cdots + 2\,(2\nu+1)\,(\nu+1)\,\mathsf{X}^2 + 2,\end{aligned}$$

οπότε $\deg(\varphi(\mathsf{X})) = 2\nu$ (με τους συντελεστές των περιττών δυνάμεων τού X ίσους με το 0). Επειδή $\varphi(1) = 2^{2\nu+1} \neq 0$, για $z \in \mathbb{C}\smallsetminus\{1\}$ έχουμε

$$\varphi(z) = 0 \Leftrightarrow \left(\tfrac{z+1}{z-1}\right)^{2\nu+1} = 1 \Leftrightarrow \exists k \in \{0,...,2\nu\} : \tfrac{z+1}{z-1} = e^{\frac{2k\pi i}{2\nu+1}}.$$

Η τιμή $k = 0$ αποκλείεται (για προφανείς λόγους). Για $k \in \{1,...,2\nu\}$ λαμβάνουμε[12]

$$\tfrac{z+1}{z-1} = e^{\frac{2k\pi i}{2\nu+1}} \Leftrightarrow z = \tfrac{e^{\frac{2k\pi i}{2\nu+1}}+1}{e^{\frac{2ik\pi}{2\nu+1}}-1} = \tfrac{e^{\frac{k\pi i}{2\nu+1}}+e^{-\frac{k\pi i}{2\nu+1}}}{e^{\frac{k\pi i}{2\nu+1}}-e^{-\frac{k\pi i}{2\nu+1}}} = -i\cot(\tfrac{k\pi}{2\nu+1}) = -\frac{i}{\tan(\frac{k\pi}{2\nu+1})}.$$

Επομένως το $\varphi(z)$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού $\mathbb{C}$ ως εξής:

$$\varphi(\mathsf{X}) = 2\,(2\nu+1)\prod_{k=1}^{2\nu}\left(\mathsf{X} + i\cot(\tfrac{k\pi}{2\nu+1})\right).$$

Οι τύποι τού Viète οδηγούν, εν προκειμένω, σε ενδιαφέρουσες τριγωνομετρικές ταυτότητες για τις μετέχουσες συνεφαπτομένες. Π.χ.,

$$\sum_{k=1}^{2\nu}\left(-i\cot(\tfrac{k\pi}{2\nu+1})\right) = 0 \Rightarrow \sum_{k=1}^{2\nu}\cot(\tfrac{k\pi}{2\nu+1}) = 0,$$

$$\sum_{1\le j<k\le 2\nu}\cot(\tfrac{j\pi}{2\nu+1})\cot(\tfrac{k\pi}{2\nu+1}) = -\tfrac{1}{2(2\nu+1)}\left(2\tbinom{2\nu+1}{3}\right) = -\tfrac{\nu(2\nu-1)}{3}$$

και (από τον τελευταίο τύπο)

$$\prod_{k=1}^{2\nu}\left(-i\cot(\tfrac{k\pi}{2\nu+1})\right) = \tfrac{1}{2\nu+1} \Longrightarrow \prod_{k=1}^{\nu}\cot(\tfrac{k\pi}{2\nu+1}) = \tfrac{1}{\sqrt{2\nu+1}}.$$

Στην *Invention Nouvelle en l'Algèbre* (1629) ο Girard επεξέτεινε την έρευνά του επί των στοιχειωδών συμμετρικών συναρτήσεων $s_1, s_2,...$ και κατόρθωσε να τις συσχετίσει και με τα *αθροίσματα δυνάμεων* των $\lambda_1,...,\lambda_n$. Οι εξαχθέντες αναδρομικοί τύποι ανακαλύφθηκαν εκ νέου από τον Isaac Newton (1642-1727) περί το 1666. Έκτοτε έχουν δοθεί πολλές (διαφορετικές) αποδείξεις τους.

[12] Ο ορισμός τής συναρτήσεως τής *εφαπτομένης* επεκτείνεται και στο $\mathbb{C}$ ως εξής:

$$\mathbb{C} \ni z \longmapsto \tan(z) := i\left(\tfrac{e^{-iz}-e^{iz}}{e^{-iz}+e^{iz}}\right)$$

και η *συνεφαπτομένη* τού z είναι η $\cot(z) := \frac{1}{\tan(z)}$.

3.6.9 Θεώρημα. (Τύποι των Girard και Newton I)
Έστω $\varphi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^n \in K\,[\mathsf{X}]$ *ένα πολυώνυμο βαθμού* $n \geq 1$ *το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού* K. *Εάν οι θέσεις μηδενισμού του είναι τα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία* $\lambda_1,...,\lambda_n \in K$ *και*

$$\boxed{t_\nu := \lambda_1^\nu + \cdots + \lambda_n^\nu,\ \forall \nu \in \mathbb{N}_0,} \tag{3.36}$$

τότε για οιονδήποτε $k \in \mathbb{N}$ *ισχύει η σχέση*

$$\boxed{t_k - s_1 t_{k-1} + s_2 t_{k-2} + \cdots + (-1_K)^n s_n t_{k-n} = 0_K,} \tag{3.37}$$

όταν $k \geq n$, *και η σχέση*

$$\boxed{t_k - s_1 t_{k-1} + s_2 t_{k-2} + \cdots + (-1_K)^{k-1} s_{k-1} t_1 + (-1_K)^k k s_k = 0_K,} \tag{3.38}$$

όταν $1 \leq k \leq n$, *όπου τα* $s_1, s_2,...$ *είναι τα αθροίσματα* (3.32).

ΑΠΟΔΕΙΞΗ. *Περίπτωση πρώτη.* Εάν $k \geq n$, τότε εφαρμόζοντας σε αμφότερα μέλη τής ισότητας (3.35):

$$\sum_{j=0}^{n} (-1_K)^j s_j \mathsf{X}^{n-j} = (\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2) \cdots (\mathsf{X} - \lambda_n)$$

τη συνάρτηση $\mathfrak{y}_{\lambda_i}$ πολυωνυμικής αποτιμήσεως στο λ_i λαμβάνουμε

$$\sum_{j=0}^{n} (-1_K)^j s_j \lambda_i^{n-j} = 0_K,\ \forall i \in \{1,...,n\}. \tag{3.39}$$

Αρκεί να πολλαπλασιάσουμε αμφότερα τα μέλη των ισοτήτων (3.39) με λ_i^{k-n}:

$$\sum_{j=0}^{n} (-1_K)^j s_j \lambda_i^{k-j} = 0_K,\ \forall i \in \{1,...,n\},$$

και να τις αθροίσουμε, κατόπιν τούτου, κατά μέλη

$$\sum_{i=1}^{n} \sum_{j=0}^{n} (-1_K)^j s_j \lambda_i^{k-j} = \sum_{j=0}^{n} (-1_K)^j s_j \sum_{i=1}^{n} \lambda_i^{k-j} = \sum_{j=0}^{n} (-1_K)^j s_j t_{k-j} = 0_K.$$

Περίπτωση δεύτερη. Εάν $1 \leq k \leq n$, τότε θέτουμε

$$\beta_i(\mathsf{X}) := \prod_{l \in \{1,..,n\} \setminus \{i\}} (\mathsf{X} - \lambda_l),$$

και εκφράζουμε την επίτυπη παράγωγο $\mathcal{D}(\hat{\varphi}(\mathsf{X}))$ τού

$$\hat{\varphi}(\mathsf{X}) := a_n^{-1} \varphi(\mathsf{X}) = (\mathsf{X} - \lambda_1) \cdots (\mathsf{X} - \lambda_n) = \sum_{j=0}^{n} (-1_K)^j s_j \mathsf{X}^{n-j}$$

αφ' ενός μεν ως

$$\mathcal{D}(\hat{\varphi}(\mathsf{X})) = \sum_{i=1}^{n} \beta_i(\mathsf{X}), \tag{3.40}$$

(βλ. (3.15)), αφ' ετέρου δε ως

$$\mathcal{D}(\hat{\varphi}(\mathsf{X})) = \mathcal{D}\left(\sum_{j=0}^{n}(-1_K)^j s_j \mathsf{X}^{n-j}\right) = \sum_{j=0}^{n-1}(-1_K)^j\,(n-j)\,s_j \mathsf{X}^{n-j-1}. \tag{3.41}$$

Επειδή $\hat{\varphi}(\mathsf{X}) = (\mathsf{X}-\lambda_i)\beta_i(\mathsf{X})$ για κάθε $i \in \{1,...,n\}$, έχουμε

$$\begin{aligned}\hat{\varphi}(\mathsf{X}) &= \hat{\varphi}(\mathsf{X}) - \hat{\varphi}(\lambda_i) = \sum_{j=0}^{n}(-1_K)^j s_j \mathsf{X}^{n-j} - \sum_{j=0}^{n}(-1_K)^j s_j \lambda_i^{n-j} \\ &= \sum_{j=0}^{n-1}(-1_K)^j s_j (\mathsf{X}^{n-j} - \lambda_i^{n-j}).\end{aligned}$$

Ως γνωστόν, για κάθε $(i,j) \in \{1,...,n\} \times \{0,1,...,n-1\}$ ισχύει

$$\mathsf{X}^{n-j} - \lambda_i^{n-j} = (\mathsf{X}-\lambda_i)\left(\sum_{\nu=0}^{n-j-1}\lambda_i^{\nu}\mathsf{X}^{n-j-1-\nu}\right),$$

οπότε

$$\begin{aligned}\hat{\varphi}(\mathsf{X}) &= (\mathsf{X}-\lambda_i)\left(\sum_{j=0}^{n-1}(-1_K)^j s_j\left(\sum_{\nu=0}^{n-j-1}\lambda_i^{\nu}\mathsf{X}^{n-j-1-\nu}\right)\right) \\ &= (\mathsf{X}-\lambda_i)\left(\sum_{j=0}^{n-1}\left(\sum_{\varrho=0}^{j}(-1_K)^{\varrho}s_j\lambda_i^{j-\varrho}\right)\mathsf{X}^{n-j-1}\right)\end{aligned}$$

(κατόπιν αναδιατάξεως τής αθροίσεως). Αυτό σημαίνει ότι

$$\beta_i(\mathsf{X}) = \sum_{j=0}^{n-1}\left(\sum_{\varrho=0}^{j}(-1_K)^{\varrho}s_j\lambda_i^{j-\varrho}\right)\mathsf{X}^{n-j-1},\ \forall i \in \{1,...,n\}. \tag{3.42}$$

(καθόσον ο $K\,[\mathsf{X}]$ είναι ακεραία περιοχή). Αθροίζοντας τις (3.42) κατά μέλη λαμβάνουμε μέσω τής (3.40):

$$\begin{aligned}\mathcal{D}(\hat{\varphi}(\mathsf{X})) &= \sum_{i=1}^{n}\beta_i(\mathsf{X}) = \sum_{j=0}^{n-1}\left(\sum_{\varrho=0}^{j}(-1_K)^{\varrho}s_j\left(\sum_{i=1}^{n}\lambda_i^{j-\varrho}\right)\right)\mathsf{X}^{n-j-1} \\ &= \sum_{j=0}^{n-1}\left(\sum_{\varrho=0}^{j}(-1_K)^{\varrho}s_j t_{j-\varrho}\right)\mathsf{X}^{n-j-1}.\end{aligned} \tag{3.43}$$

Συγκρίνοντας τους συντελεστές τού X^{n-j-1} στις δύο εκφράσεις (3.43) και (3.41) τού πολυωνύμου $\mathcal{D}(\hat{\varphi}(\mathsf{X}))$ για $j = k = 1,..., n-1$ καταλήγουμε στη σχέση

$$\sum_{\varrho=0}^{k-1}(-1_K)^{\varrho}s_k t_{k-\varrho} + (-1_K)^k n s_k = (-1_K)^k\,(n-k)\,s_k,$$

από την οποία έπεται η (3.38) για $k \leq n-1$. Το ότι η (3.38) είναι αληθής *και* για $k = n$ είναι πρόδηλο από ό,τι απεδείχθη στην πρώτη περίπτωση. □

3.6.10 Σημείωση. Μια ελαφρά παραλλαγή τής αποδείξεως τής (3.38) έχει ως εξής: Αντί να εκκινήσουμε από την

$$\sum_{k=0}^{n}(-1_K)^k s_k \mathsf{X}^{n-k} = (\mathsf{X}-\lambda_1)\cdots(\mathsf{X}-\lambda_n), \tag{3.44}$$

εκκινούμε από την

$$\sum_{k=0}^{n}(-1_K)^k s_k \mathsf{X}^{k} = (1_K-\lambda_1\mathsf{X})\cdots(1_K-\lambda_n\mathsf{X}) \tag{3.45}$$

(η οποία αποδεικνύεται είτε επαγωγικώς είτε μέσω[13] τής (3.44)). Επίτυπη παραγώγιση των μελών τής (3.45) δίδει

$$\sum_{k=1}^{n}(-1_K)^k k s_k \mathsf{X}^{k-1} = \sum_{i=1}^{n}(-\lambda_i)\prod_{l\in\{1,..,n\}\setminus\{i\}}(1_K-\lambda_l\mathsf{X})$$

και (κατόπιν πολλαπλασιασμού αμφοτέρων των μελών με X)

$$\begin{aligned}
&\sum_{k=1}^{n}(-1_K)^k k s_k \mathsf{X}^{k} = -\sum_{i=1}^{n}(\lambda_i\mathsf{X})\prod_{l\in\{1,..,n\}\setminus\{i\}}(1_K-\lambda_l\mathsf{X})\\
&= -\left(\sum_{i=1}^{n}(\lambda_i\mathsf{X})(1_K-(\lambda_i\mathsf{X}))^{-1}\right)\prod_{l=1}^{n}(1_K-\lambda_l\mathsf{X})\\
&= -\left(\sum_{i=1}^{n}\sum_{j=1}^{\infty}(\lambda_i\mathsf{X})^j\right)\prod_{l=1}^{n}(1_K-\lambda_l\mathsf{X})\\
&= -\left(\sum_{j=1}^{\infty}\left(\sum_{i=1}^{n}\lambda_i^j\right)\mathsf{X}^j\right)\left(\sum_{l=0}^{n}(-1_K)^l s_l\mathsf{X}^l\right)\\
&= \left(\sum_{j=1}^{\infty}t_j\mathsf{X}^j\right)\left(\sum_{l=0}^{n}(-1_K)^{l-1}s_l\mathsf{X}^l\right).
\end{aligned}$$

[13] Εν προκειμένω, μπορεί να εφαρμοσθεί το ακόλουθο *κλασικό τέχνασμα*: Η (3.44) εξακολουθεί να ισχύει αν το X αντικατασταθεί με το $\frac{1}{\mathsf{X}}$, ήτοι με το αντίστροφο τού X εντός τού σώματος κλασμάτων $K(\mathsf{X}) := \mathbf{Fr}(K[\mathsf{X}])$ τής ακεραίας περιοχής $K[\mathsf{X}]$ (Βλ. εδ. 3.8.1). Πολλαπλασιάζοντας λοιπόν (ύστερα από αυτήν την αντικατάσταση) αμφότερα τα μέλη τής προκύπτουσας ισότητας με X^n λαμβάνουμε την (3.45).

(Στη δεύτερη και στην τρίτη ισότητα χρησιμοποιήσαμε το ότι η επίτυπη δυναμοσειρά $\sum_{j=0}^{\infty}(\lambda_i\mathsf{X})^j$ είναι αντιστρέψιμη εντός τής ακεραίας περιοχής $K[\![\mathsf{X}]\!]$, έχουσα ως αντίστροφό της το $1_K-(\lambda_i\mathsf{X})$, οπότε $(\lambda_i\mathsf{X})(1_K-(\lambda_i\mathsf{X}))^{-1}=\sum_{j=1}^{\infty}(\lambda_i\mathsf{X})^j$. Πρβλ. εδ. 3.1.4 (i).) Η (3.38) προκύπτει άμεσα από το ότι ο συντελεστής τού X^k, $k\in\{1,...,n\}$, στο γινόμενο

$$\left(\sum_{j=1}^{\infty}t_j\mathsf{X}^j\right)\left(\sum_{l=0}^{n}(-1_K)^{l-1}s_l\mathsf{X}^l\right)=(t_1\mathsf{X}+t_2\mathsf{X}^2+\cdots)(-1_K+s_1\mathsf{X}-s_2\mathsf{X}^2+\cdots)$$

είναι ίσος με $\sum_{\varrho=1}^{k}(-1_K)^{k-\varrho-1}t_\varrho s_{k-\varrho}$.

3.6.11 Πόρισμα. (Τύποι των Girard και Newton II)
Έστω $\varphi(\mathsf{X})=\sum_{i=0}^{n}a_i\mathsf{X}^n\in K[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n\geq 1$ το οποίο διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K. Εάν οι θέσεις μηδενισμού του είναι τα (όχι κατ' ανάγκην σαφώς διακεκριμένα) στοιχεία $\lambda_1,...,\lambda_n\in K$, τότε για οιονδήποτε $k\in\mathbb{N}$ ισχύει η σχέση

$$\boxed{a_nt_k+a_{n-1}t_{k-1}+a_{n-2}t_{k-2}+\cdots+a_0t_{k-n}=0_K,} \tag{3.46}$$

όταν $k\geq n$, και η σχέση

$$\boxed{a_nt_k+a_{n-1}t_{k-1}+a_{n-2}t_{k-2}+\cdots+a_{n-k+1}t_1+ka_{n-k}=0_K,} \tag{3.47}$$

όταν $1\leq k\leq n$, όπου τα $t_1,t_2,...$ είναι τα αθροίσματα (3.36).

ΑΠΟΔΕΙΞΗ. Η (3.46) (και αντιστοίχως, η (3.47)) έπεται άμεσα από τις σχέσεις (3.37) και (3.33) (και αντιστοίχως, από τις (3.38) και (3.33)). □

► **Σώματα διασπάσεως**. Για να μετατρέψει κανείς δοθέν $\varphi(\mathsf{X})\in K[\mathsf{X}]$ που δεν διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K σε διασπώμενο (ούτως ώστε να είναι σε θέση να εκμεταλλευθεί τις προαναφερθείσες όμορφες ιδιότητες των διασπώμενων) αρκεί να επεκτείνει καταλλήλως το σώμα αναφοράς K εφαρμόζοντας το θεώρημα 3.6.12 τού Leopold Kronecker (1823-1891) (και το συνακόλουθό του 3.6.15 που το ισχυροποιεί[14]).

3.6.12 Θεώρημα. (Kronecker, 1887) *Για οιοδήποτε $\varphi(\mathsf{X})\in K[\mathsf{X}]$ βαθμού ≥ 1 υφίσταται κάποια επέκταση L τού K, υπεράνω τής οποίας το $\varphi(\mathsf{X})$ διασπάται σε πρωτοβάθμιους παράγοντες.*

[14] Οι αποδείξεις αυτών των θεωρημάτων παραλείπονται, καθώς ανήκουν στη Θεωρία Σωμάτων.

3.6.13 Ορισμός. Έστω $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$. Μια επέκταση L τού K καλείται **σώμα διασπάσεώς** του όταν το $\varphi(\mathsf{X})$

(i) διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω αυτής και

(ii) δεν διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω οιουδήποτε γνησίου υποσώματός της.

Η συνθήκη (ii) μπορεί να αντικατασταθεί με την ακόλουθη:

(ii)′ Εάν οι $\lambda_1,...,\lambda_n$ είναι οι (όχι κατ' ανάγκην σαφώς διακεκριμένες) θέσεις μηδενισμού τού $\varphi(\mathsf{X})$ εντός τού L, τότε $L = K(\lambda_1,...,\lambda_n)$.

3.6.14 Παραδείγματα. (i) Το $\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \middle| \, a, b \in \mathbb{Q} \right\} \subsetneqq \mathbb{R}$ αποτελεί σώμα διασπάσεως τού $\varphi(\mathsf{X}) := \mathsf{X}^2 - 2 \in \mathbb{Q}\,[\mathsf{X}]$, διότι

$$\varphi(\mathsf{X}) = (\mathsf{X} - \sqrt{2})(\mathsf{X} - (-\sqrt{2})) \in \mathbb{Q}(\sqrt{2}), \;\; \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

Σημειωτέον ότι *και* το $\psi(\mathsf{X}) := \mathsf{X}^4 - 2\mathsf{X}^3 - 3\mathsf{X}^2 + 4\mathsf{X} + 2 \in \mathbb{Q}\,[\mathsf{X}]$ έχει το $\mathbb{Q}(\sqrt{2})$ ως (ένα) σώμα διασπάσεώς του, διότι

$$\psi(\mathsf{X}) = (\mathsf{X} - \sqrt{2})(\mathsf{X} - (-\sqrt{2}))(\mathsf{X} - (1 + \sqrt{2}))(\mathsf{X} - (1 - \sqrt{2}))$$

και $1 \pm \sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

(ii) Το $\theta(\mathsf{X}) := (\mathsf{X}^2 - 2)(\mathsf{X}^2 + 1) \in \mathbb{Q}\,[\mathsf{X}]$ διαθέτει δύο θέσεις μηδενισμού εντός τού $\mathbb{Q}(\sqrt{2})$ αλλά δεν διασπάται *πλήρως* σε πρωτοβάθμιους παράγοντες υπεράνω αυτού. Άρα το $\mathbb{Q}(\sqrt{2})$ δεν είναι σώμα διασπάσεως τού $\theta(\mathsf{X})$. Ένα σώμα διασπάσεώς του είναι το $\mathbb{Q}(\sqrt{2}, i) \subsetneqq \mathbb{C}$ (όπου i η φανταστική μονάδα). Από την άλλη μεριά, παρότι το $\theta(\mathsf{X})$ διασπάται σε πρωτοβάθμιους παράγοντες *και* υπεράνω τού $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[3]{2}, i)$, αυτό το σώμα δεν αποτελεί σώμα διασπάσεώς του (διότι περιέχει πλεονάζοντα στοιχεία και δεν πληροί, ως εκ τούτου, τη συνθήκη 3.6.13 (ii)′).

3.6.15 Θεώρημα. *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ βαθμού ≥ 1 διαθέτει (τουλάχιστον ένα) σώμα διασπάσεως. Επιπροσθέτως, για δυο σώματα διασπάσεως L_1, L_2 ενός πολυωνύμου $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ βαθμού ≥ 1 υφίσταται πάντοτε ένας ισομορφισμός σωμάτων $f : L_1 \longrightarrow L_2$ με $f|_K = \mathrm{id}_K$.*

► **Αλγεβρικώς κλειστά σώματα**. Η έννοια τού σώματος διασπάσεως ορίζεται για ένα (και μόνον) δοθέν (μη σταθερό) πολυώνυμο. Ωστόσο, υπάρχουν κάποια ειδικής φύσεως σώματα K, τα λεγόμενα *αλγεβρικώς κλειστά σώματα,* υπεράνω των οποίων *κάθε* $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ βαθμού ≥ 1 διασπάται σε πρωτοβάθμιους παράγοντες.

3.6.16 Θεώρημα. *Δοθέντος ενός σώματος K, οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ βαθμού $n \geq 1$ διαθέτει τουλάχιστον μία θέση*

μηδενισμού ανήκουσα στο K.

(ii) *Κάθε πολυώνυμο* $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ *βαθμού* $n \geq 1$ *διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού* K.

(iii) *Κάθε ανάγωγο πολυώνυμο υπεράνω τού* K *έχει βαθμό* 1.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Έστω $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ τυχόν πολυώνυμο βαθμού $n \geq 1$. Κατά την υπόθεσή μας, το $\varphi(\mathsf{X})$ διαθέτει τουλάχιστον μία θέση μηδενισμού ανήκουσα στο K. Εάν τα $\lambda_1,...,\lambda_k \in K$ ($k \in \mathbb{N},\ k \leq n$) είναι (όλες) οι σαφώς διακεκριμένες θέσεις μηδενισμού του εντός τού K, τότε (σύμφωνα με το λήμμα 3.6.2) υπάρχει $\psi(\mathsf{X}) \in K\,[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, τέτοιο ώστε το $\varphi(\mathsf{X})$ να γράφεται υπό τη μορφή

$$\varphi(\mathsf{X}) = \left(\prod_{i=1}^{k} (\mathsf{X} - \lambda_i)^{m_i}\right) \psi(\mathsf{X}),$$

όπου $m_i = \mathrm{mult}(\varphi(\mathsf{X}); \lambda_i)$, $\psi(\lambda_i) \neq 0_K$, $\forall i \in \{1,...,k\}$, και

$$\sum_{i=1}^{k} m_i \leq n.$$

Εάν ο βαθμός τού $\psi(\mathsf{X})$ ήταν ≥ 1, τότε σύμφωνα με την υπόθεσή μας (για το $\psi(\mathsf{X})$!) θα υπήρχε τουλάχιστον μία θέση μηδενισμού $\lambda \in K$ τού $\psi(\mathsf{X})$. Αυτή θα ήταν θέση μηδενισμού *και* τού $\varphi(\mathsf{X})$, οπότε θα είχαμε $\lambda = \lambda_{i_0}$ για κάποιον $i_0 \in \{1,...,k\}$, ήτοι κάτι που θα ήταν αδύνατο. Τούτο σημαίνει ότι $\deg(\psi(\mathsf{X})) = 0$, δηλαδή ότι το $\psi(\mathsf{X})$ είναι σταθερό και $\sum_{i=1}^{k} m_i = n$. Άρα το $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ διασπάται σε πρωτοβάθμιους παράγοντες υπεράνω τού K.

(ii)⇒(iii) Έστω $\theta(\mathsf{X})$ τυχόν ανάγωγο πολυώνυμο υπεράνω τού K. Σύμφωνα με την υπόθεσή μας υπάρχουν $\lambda_1,...,\lambda_n \in K$, τέτοια ώστε να ισχύει η ισότητα

$$\theta(\mathsf{X}) = c\,(\mathsf{X} - \lambda_1)(\mathsf{X} - \lambda_2)\cdots(\mathsf{X} - \lambda_n)$$

για κάποιο $c \in K \setminus \{0_K\}$. Από την ιδιότητα τής μοναδικότητας τής παραστάσεώς του ως γινομένου αναγώγων μονικών πολυωνύμων (την περιγραφόμενη στο θεώρημα 3.5.8) συνάγουμε ότι $n = 1$, οπότε $\deg(\theta(\mathsf{X})) = 1$.

(iii)⇒(i) Έστω $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ τυχόν πολυώνυμο βαθμού $n \geq 1$. Υποθέτουμε ότι

$$\varphi(\mathsf{X}) = c \prod_{\nu=1}^{r} \theta_\nu(\mathsf{X})$$

είναι η παράσταση αυτού ως γινομένου αναγώγων μονικών πολυωνύμων (όπου $r \in \mathbb{N}$, $c \in K \setminus \{0_K\}$). Σύμφωνα με την υπόθεσή μας, καθένα εκ των $\theta_\nu(\mathsf{X})$, $\nu \in \{1,...,r\}$, έχει βαθμό 1 και, ως εκ τούτου, (ακριβώς) μία θέση μηδενισμού εντός τού K. Επειδή $r \geq 1$, το $\varphi(\mathsf{X})$ διαθέτει τουλάχιστον μία θέση μηδενισμού ανήκουσα στο K. □

3.6.17 Ορισμός. Ένα σώμα K καλείται **αλγεβρικώς κλειστό** όταν πληροί μία (και, κατ' επέκτασιν, και τις τρεις) εκ των συνθηκών τού θεωρήματος 3.6.16.

3.6.18 Πρόταση. *Εάν το K είναι ένα σώμα αλγεβρικώς κλειστό, τότε (το υποκείμενο σύνολό του) είναι κατ' ανάγκην απειροσύνολο.*

ΑΠΟΔΕΙΞΗ. Έστω $K = \{a_1,...,a_q\}$ ένα πεπερασμένο σώμα. Εάν υποθέσουμε ότι το K είναι αλγεβρικώς κλειστό, τότε καταλήγουμε σε άτοπο, καθότι το πολυώνυμο

$$\varphi(\mathsf{X}) := (\mathsf{X} - a_1)(\mathsf{X} - a_2)\cdots(\mathsf{X} - a_q) + 1_K \in K\,[\mathsf{X}]$$

δεν διαθέτει καμία θέση μηδενισμού ανήκουσα στο K. □

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

Το θεώρημα 3.6.19 πρωτοαπεδείχθη 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, την Άλγεβρα και την Αλγεβρική Τοπολογία. Για περισσότερες πληροφορίες και σύντομες ιστορικές σημειώσεις ο ενδιαφερόμενος αναγνώστης παραπέμπεται στο σύγγραμμα των B. Fine και G. Rosenberger: *Το Θεμελιώδες Θεώρημα τής Άλγεβρας* (σε μετάφραση των Φ. Λιούτση και N. Μαρμαρίδη), εκδόσεις Leader Books, Αθήνα, 2001. Στην ενότητα ?? θα παραθέσουμε μια απόδειξη (οφειλόμενη στον Harm Derksen[15]) που χρησιμοποιεί την (κλασική) πρόταση 3.7.2 και λοιπά τεχνικά μέσα προερχόμενα *μόνον* από τη *Γραμμική Άλγεβρα*.

3.6.20 Σημείωση. (i) Στις παραδόσεις τής Αφηρημένης Άλγεβρας αποδεικνύεται ότι *κάθε σώμα K διαθέτει μια αλγεβρικώς κλειστή επέκταση* και μάλιστα ότι υπάρχει μια (μέχρις ισομορφισμού σωμάτων μονοσημάντως ορισμένη) *ελαχίστη* (τέτοιου είδους) *επέκταση* $\overline{K}$ τού K, η οποία καλείται **αλγεβρική θήκη** (ή **αλγεβρικό έγκλεισμα**) τού K. Πολλές φορές, δοθέντος ενός $\varphi(\mathsf{X}) \in K\,[\mathsf{X}]$ βαθμού $n \geq 1$ (όπου K *τυχόν* σώμα), είναι αρκετό το να εργαζόμαστε με την αλγεβρική θήκη $\overline{K}$ τού K αντί να αναζητούμε το σώμα διασπάσεώς του. Επειδή το $\varphi(\mathsf{X}) \in K\,[\mathsf{X}] \subseteq \overline{K}\,[\mathsf{X}]$ μπορεί να εκληφθεί ως πολυώνυμο τού $\overline{K}\,[\mathsf{X}]$, διασπάται πάντοτε σε πρωτοβάθμιους παράγοντες υπεράνω τού $\overline{K}$ (κάτι που είθισται να χρησιμοποιείται ευρέως κατά την επιχειρηματολογία που εφαρμόζεται σε ποικίλες αποδεικτικές τεχνικές). (ii) Επειδή η αλγεβρική θήκη τού σώματος $\mathbb{R}$ είναι το $\mathbb{C}$, *κάθε* $\varphi(\mathsf{X}) \in \mathbb{R}\,[\mathsf{X}] \subseteq \mathbb{C}\,[\mathsf{X}]$ βαθμού $n \geq 1$, εκλαμβανόμενο ως πολυώνυμο τού $\mathbb{C}\,[\mathsf{X}]$, διασπάται πάντοτε σε πρωτοβάθμιους παράγοντες υπεράνω τού $\mathbb{C}$.

[15] H. Derksen: *The Fundamental Theorem of Algebra and Linear Algebra*, Amer. Math. Monthly, **110**, No 7, (2003) 620-623.

3.7 ΠΟΛΥΩΝΥΜΑ ΜΕ ΠΡΑΓΜΑΤΙΚΟΥΣ ΣΥΝΤΕΛΕΣΤΕΣ

Δύο σημαντικές ιδιότητες των πολυωνύμων με πραγματικούς συντελεστές περιγράφονται στις προτάσεις 3.7.2 και 3.7.3.

3.7.1 Λήμμα. *Έστω $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n > 1$. Εάν ο μιγαδικός αριθμός $z = a + ib \in \mathbb{C}$ είναι μια θέση μηδενισμού τού $\varphi(\mathsf{X})$, τότε το ίδιο ισχύει και για τον συζυγή του $\overline{z} = a - ib$. Επιπροσθέτως, εάν $z \in \mathbb{C} \setminus \mathbb{R}$, τότε*

$$\mathrm{mult}(\varphi(\mathsf{X}); z) = \mathrm{mult}(\varphi(\mathsf{X}); \overline{z}).$$

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

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

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

$$m := \mathrm{mult}(\varphi(\mathsf{X}); z), \quad m' := \mathrm{mult}(\varphi(\mathsf{X}); \overline{z})$$

και $b \neq 0$, τότε (σύμφωνα με την πρόταση 3.4.14 και το λήμμα 3.6.1)

$$\exists \psi(\mathsf{X}) \in \mathbb{C}[\mathsf{X}] \setminus \{\mathbf{0}_{\mathbb{C}[\mathsf{X}]}\} : \varphi(\mathsf{X}) = (\mathsf{X} - z)^m\,(\mathsf{X} - \overline{z})^{m'}\,\psi(\mathsf{X})$$

με $\psi(z) \neq 0$ και $\psi(\overline{z}) \neq 0$. Ας υποθέσουμε ότι $m > m'$. Τότε

$$\begin{aligned} \varphi(\mathsf{X}) &= (\mathsf{X} - (a + ib))^m\,(\mathsf{X} - (a - ib))^{m'}\,\psi(\mathsf{X}) \\ &= \big((\mathsf{X} - a)^2 + b^2\big)^{m'}\,\gamma(\mathsf{X}), \end{aligned}$$

όπου το $\gamma(\mathsf{X}) := (\mathsf{X} - (a + ib))^{m-m'}\,\psi(\mathsf{X})$ (ως πηλίκο δύο πολυωνύμων με πραγματικούς συντελεστές) ανήκει στον $\mathbb{R}[\mathsf{X}]$ και έχει τον $z = a + ib$ ως μια θέση μηδενισμού του. Άρα, σύμφωνα με την ήδη αποδειχθείσα ιδιότητα, θα δέχεται ως θέση μηδενισμού του και τον συζυγή του $\overline{z} = a - ib$, οπότε

$$\gamma(\overline{z}) = \gamma(a - ib) = (-2bi)^{m-m'}\,\psi(\overline{z}) = 0.$$

Τούτο είναι αδύνατον, καθόσον $b \neq 0$ και $\psi(\overline{z}) \neq 0$. Με τον ίδιο τρόπο αποδεικνύεται ότι δεν μπορεί να ισχύει ούτε η ανισότητα $m < m'$. Άρα $m = m'$. □

3.7.2 Πρόταση. *Κάθε πολυώνυμο $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ περιττού βαθμού διαθέτει (τουλάχιστον) μία πραγματική θέση μηδενισμού.*

ΑΠΟΔΕΙΞΗ ΠΡΩΤΗ (ανεξάρτητη τού 3.6.19). Έστω $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ τυχόν πολυώνυμο βαθμού $n = 2k+1$, $k \in \mathbb{N}_0$. Αυτό μπορεί να θεωρηθεί ως πραγματική συνεχής συνάρτηση

$$\varphi : \mathbb{R} \longrightarrow \mathbb{R},\ x \longmapsto \varphi(x) := a_0 + a_1 x + \cdots + a_n x^n.$$

(Πρβλ. εδ. 3.4.2 και 3.4.9.) Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $a_n > 0$. (Όταν $a_n < 0$, η απόδειξη είναι πανομοιότυπη.) Παρατηρούμε ότι

$$\lim_{n \longrightarrow -\infty} \varphi(x) = \lim_{n \longrightarrow -\infty} (a_n x^n) = -\infty,\ \lim_{n \longrightarrow \infty} \varphi(x) = \lim_{n \longrightarrow \infty} (a_n x^n) = \infty$$

(διότι $a_n > 0$ και ο n είναι περιττός). Άρα υπάρχουν κάποιοι $x_1, x_2 \in \mathbb{R},\ x_1 < x_2$, τέτοιοι ώστε να ισχύει $\varphi(x_1) < 0$ και $\varphi(x_2) > 0$. Σύμφωνα με το *θεώρημα τής ενδιάμεσης τιμής*[16],

$$\exists \xi \in \mathbb{R} : x_1 < \xi < x_2 \ \text{ και } \ \varphi(\xi) = 0.$$

ΑΠΟΔΕΙΞΗ ΔΕΥΤΕΡΗ. Έστω $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ τυχόν πολυώνυμο βαθμού $n = 2k+1$, $k \in \mathbb{N}_0$. Εάν $k = 0$, τότε $\varphi(\mathsf{X}) = a\mathsf{X} + b$ για κάποιους $a \in \mathbb{R} \setminus \{0\}$, $b \in \mathbb{R}$, έχον τον πραγματικό αριθμό $-a^{-1}b$ ως (μοναδική) θέση μηδενισμού. Ας υποθέσουμε ότι ο ισχυρισμός είναι αληθής για πολυώνυμα (με πραγματικούς συντελεστές) βαθμού $2k+1$ για κάποιον $k \geq 0$ και ότι το $\varphi(\mathsf{X})$ έχει βαθμό $2(k+1)+1$. Κατά το Θεμελιώδες Θεώρημα τής Άλγεβρας 3.6.19, $\exists z \in \mathbb{C} : \varphi(z) = 0$. Κατά το λήμμα 3.7.1 ο συζυγής $\overline{z}$ τού z θα αποτελεί μια μιγαδική θέση μηδενισμού τού $\varphi(\mathsf{X})$. Θεωρώντας τό $\varphi(\mathsf{X})$ ως πολυώνυμο τού $\mathbb{C}[\mathsf{X}]$, λαμβάνουμε

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

οπότε (δυνάμει τού πορίσματος 3.4.5 και τού ότι $z \neq \overline{z}$, αφού $z \in \mathbb{C} \setminus \mathbb{R}$)

$$(\mathsf{X} - z)\,(\mathsf{X} - \overline{z}) \mid \varphi(\mathsf{X}). \tag{3.48}$$

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- τόσον το άθροισμα $z + \overline{z}$ όσον και το γινόμενο $z\overline{z}$ δυο συζυγών μιγαδικών αριθμών είναι ένας πραγματικός αριθμός. Άρα

$$\exists \varpi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}] \setminus \{\mathbf{0}_{\mathbb{R}[\mathsf{X}]}\} : \varphi(\mathsf{X}) = \varpi(\mathsf{X}) \underbrace{(\mathsf{X}^2 - (z + \overline{z})\,\mathsf{X} + z\overline{z})}_{\in \mathbb{R}[\mathsf{X}] \setminus \{\mathbf{0}_{\mathbb{R}[\mathsf{X}]}\}}.$$

(Παρά το γεγονός ότι η διαίρεση (3.48) εκτελείται *εντός τού* $\mathbb{C}[\mathsf{X}]$, το πηλίκο $\varpi(\mathsf{X})$ έχει κατ' ανάγκην *πραγματικούς* συντελεστές, καθόσον δεν αλλάζει τίποτα εάν

[16] **Θεώρημα τής ενδιάμεσης τιμής**: Εάν $\varphi : [x_1, x_2] \longrightarrow \mathbb{R}$ είναι μια συνεχής συνάρτηση με $\varphi(x_1) < \varphi(x_2)$ και $y \in \mathbb{R}$, $\varphi(x_1) < y < \varphi(x_2)$, τότε $\exists \xi \in \mathbb{R} : x_1 < \xi < x_2$ και $\varphi(\xi) = y$.

αυτή εκτελεσθεί *εντός τού* $\mathbb{R}[\mathsf{X}]$. Βλ. την απόδειξη τής προτάσεως 3.3.11 για τα σώματα $K = \mathbb{R}$ και $L = \mathbb{C}$.) Επειδή $\deg(\varpi(\mathsf{X})) = 2k+1$, το $\varpi(\mathsf{X})$ (σύμφωνα με την επαγωγική υπόθεσή μας) διαθέτει (τουλάχιστον) μία πραγματική θέση μηδενισμού. Άρα *και* το $\varphi(\mathsf{X})$ διαθέτει (τουλάχιστον) μία πραγματική θέση μηδενισμού και ο ισχυρισμός είναι αληθής.

ΑΠΟΔΕΙΞΗ ΤΡΙΤΗ. Έστω $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ τυχόν πολυώνυμο περιττού βαθμού n. Κατά το Θεμελιώδες Θεώρημα τής Άλγεβρας 3.6.19 αυτό διαθέτει (εν συνόλω, προσμετρουμένων και των τυχόν πολλαπλών εμφανίσεώς τους) n μιγαδικές θέσεις μηδενισμού $z_1,...,z_n$. Μάλιστα, σύμφωνα με το δεύτερο μέρος τού λήμματος 3.7.1, $\mathrm{card}(\{z \in \mathbb{C}\smallsetminus\mathbb{R} \mid \varphi(z) = 0\}) \in 2\mathbb{Z}$. Άρα η διάσπαση τού $\varphi(\mathsf{X})$ σε πρωτοβάθμιους παράγοντες υπεράνω τού $\mathbb{C}$ είναι κατ' ανάγκην τής μορφής

$$\varphi(\mathsf{X}) = c\left(\prod_{z\in\mathcal{A}\cap(\mathbb{C}\smallsetminus\mathbb{R})}(\mathsf{X}-z)\right)\left(\prod_{z\in\mathcal{A}\cap\mathbb{R}}(\mathsf{X}-z)\right),$$

όπου $c \in \mathbb{C}\smallsetminus\{0\}$ και $\mathcal{A} := \{z_1,...,z_n\}$. Επειδή ο n είναι περιττός και

$$\deg\left(\prod_{z\in\mathcal{A}\cap(\mathbb{C}\smallsetminus\mathbb{R})}(\mathsf{X}-z)\right) \in 2\mathbb{Z},$$

έχουμε κατ' ανάγκην $\mathrm{card}(\mathcal{A}\cap\mathbb{R}) \geq 1$. □

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

$$\left|\begin{array}{ll} \varphi(\mathsf{X}) = a\mathsf{X}+b, & \text{όπου } a \in \mathbb{R}\smallsetminus\{0\}, \text{ ή} \\ \\ \varphi(\mathsf{X}) = a\mathsf{X}^2+b\mathsf{X}+c, & \text{όπου } a,b,c \in \mathbb{R} \text{ με } b^2-4ac<0. \end{array}\right.$$

ΑΠΟΔΕΙΞΗ. Εάν $\varphi(\mathsf{X}) = a\mathsf{X}+b$, όπου $a \neq 0$, τότε το $\varphi(\mathsf{X})$ είναι προφανώς ανάγωγο υπεράνω τού $\mathbb{R}$. Ένα πολυώνυμο τής μορφής $\varphi(\mathsf{X}) = a\mathsf{X}^2+b\mathsf{X}+c$ είναι ανάγωγο υπεράνω τού $\mathbb{R}$ (βλ. την πρόταση 3.5.4) 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 $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ βαθμού ≥ 3 υπεράνω τού $\mathbb{R}$. Ας υποθέσουμε ότι ένα τέτοιου είδους ανάγωγο πολυώνυμο $\varphi(\mathsf{X})$ υπάρχει. Βάσει τού Θεμελιώδους Θεωρήματος τής Άλγεβρας το $\varphi(\mathsf{X})$ θα διαθέτει (τουλάχιστον) μία θέση μηδενισμού $z \in \mathbb{C}$. Προφανώς, $z \notin \mathbb{R}$, διότι αλλιώς το $\varphi(\mathsf{X})$ δεν θα είναι ανάγωγο υπεράνω τού $\mathbb{R}$. Κατά το λήμμα 3.7.1 ο συζυγής $\overline{z}$ τού z θα

αποτελεί θέση μηδενισμού τού $\varphi(\mathsf{X})$. Θεωρώντας τό $\varphi(\mathsf{X})$ ως πολυώνυμο τού $\mathbb{C}[\mathsf{X}]$, λαμβάνουμε

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

οπότε (δυνάμει τού πορίσματος 3.4.5 και τού ότι $z \neq \overline{z}$, αφού $z \in \mathbb{C} \setminus \mathbb{R}$)

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

Όμως το $(\mathsf{X}-z)\,(\mathsf{X}-\overline{z}) = \mathsf{X}^2 - (z+\overline{z})\,\mathsf{X} + z\overline{z}$ έχει πραγματικούς συντελεστές. Άρα το $\varphi(\mathsf{X})$ δεν είναι ανάγωγο υπεράνω τού $\mathbb{R}$. Άτοπο! □

3.7.4 Πόρισμα. *Για κάθε πολυώνυμο $\varphi(\mathsf{X}) \in \mathbb{R}[\mathsf{X}]$ βαθμού ≥ 1 υπάρχουν φυσικοί αριθμοί k, l, μη αρνητικοί ακέραιοι αριθμοί $m_1,...,m_k, n_1,...,n_l$ (με τουλάχιστον έναν εξ αυτών $\neq 0$), και πραγματικοί αριθμοί $b_1,...,b_k, \mathrm{A}_1,...,\mathrm{A}_l, \mathrm{B}_1,...,\mathrm{B}_l$ και $c \neq 0$, τέτοιοι ώστε να ισχύει $\mathrm{A}_j^2 - 4\mathrm{B}_j < 0$ για κάθε $j \in \{1,...,l\}$ και*

$$\varphi(\mathsf{X}) = c\left(\prod_{i=1}^{k}(\mathsf{X}+b_i)^{m_i}\right)\left(\prod_{j=1}^{l}(\mathsf{X}^2+\mathrm{A}_j\mathsf{X}+\mathrm{B}_j)^{n_j}\right). \tag{3.49}$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από την πρόταση 3.7.3. Η παράσταση (3.49) αποτελεί τη συνεπτυγμένη (υπό την ευρεία έννοια) αποσύνθεση τού $\varphi(\mathsf{X})$ υπεράνω τού σώματος $\mathbb{R}$. □

3.7.5 Παράδειγμα. Εάν $\nu \in \mathbb{N}$, τότε το $\mathsf{X}^\nu - 1 \in \mathbb{R}[\mathsf{X}]$ διαθέτει ν (απλές) μιγαδικές θέσεις μηδενισμού, ήτοι τις *ν-οστές ρίζες τής μονάδας* ζ_ν^k, $k \in \{0,1,...,\nu-1\}$, όπου $\zeta_\nu := e^{\frac{2\pi i}{\nu}} = \cos\left(\frac{2\pi}{\nu}\right) + i\sin\left(\frac{2\pi}{\nu}\right)$. Άρα διασπάται σε πρωτοβάθμιους παράγοντες *υπεράνω τού* $\mathbb{C}$ ως ακολούθως:

$$\mathsf{X}^\nu - 1 = \prod_{k=0}^{\nu-1}\left(\mathsf{X}-\zeta_\nu^k\right).$$

Σημειωτέον ότι $\zeta_\nu^k\overline{\zeta_\nu^k} = 1$ για κάθε $k \in \{0,1,...,\nu-1\}$ και

$$\zeta_\nu^k + \overline{\zeta_\nu^k} = \begin{cases} 2\cos\left(\frac{k\pi}{\varrho}\right), & \text{όταν } \nu = 2\varrho,\ \varrho \in \mathbb{N}, \\ 2\cos\left(\frac{2k\pi}{2\varrho+1}\right), & \text{όταν } \nu = 2\varrho+1,\ \varrho \in \mathbb{N}_0, \end{cases}$$

οπότε

$$\left(\mathsf{X}-\zeta_\nu^k\right)\left(\mathsf{X}-\overline{\zeta_\nu^k}\right) = \begin{cases} \mathsf{X}^2 - 2\cos\left(\frac{k\pi}{\varrho}\right)\mathsf{X} + 1, & \text{όταν } \nu = 2\varrho,\ \varrho \in \mathbb{N}, \\ \mathsf{X}^2 - 2\cos\left(\frac{2k\pi}{2\varrho+1}\right)\mathsf{X} + 1, & \text{όταν } \nu = 2\varrho+1,\ \varrho \in \mathbb{N}_0. \end{cases}$$

Κατά συνέπειαν, η συνεπτυγμένη αποσύνθεση (3.49) τού $\mathsf{X}^\nu - 1$ *υπεράνω τού σώματος* $\mathbb{R}$ είναι η

$$\mathsf{X}^\nu - 1 = \begin{cases} \mathsf{X} - 1, & \text{όταν } \nu = 1, \\ (\mathsf{X}-1)\,(\mathsf{X}+1)\,, & \text{όταν } \nu = 2, \\ (\mathsf{X}-1)\,(\mathsf{X}+1)\prod\limits_{k=1}^{\varrho-1}(\mathsf{X}^2 - 2\cos\left(\frac{k\pi}{\varrho}\right)\mathsf{X}+1), & \text{όταν } \nu = 2\varrho,\ \varrho \geq 2, \\ (\mathsf{X}-1)\prod\limits_{k=1}^{\varrho}(\mathsf{X}^2 - 2\cos\left(\frac{2k\pi}{2\varrho+1}\right)\mathsf{X}+1), & \text{όταν } \nu = 2\varrho+1,\ \varrho \geq 1. \end{cases}$$

(Ως εκ τούτου, οι *πραγματικές* θέσεις μηδενισμού αυτού είναι τα 1 και -1 όταν ο ν είναι άρτιος, και μόνον το 1 όταν ο ν είναι περιττός.)

3.8 ΠΕΡΙ ΤΟΥ ΣΩΜΑΤΟΣ ΤΩΝ ΡΗΤΩΝ ΕΚΦΡΑΣΕΩΝ

Για οιοδήποτε σώμα K οι δακτύλιοι $K[\mathsf{X}]$ και $K[\![\mathsf{X}]\!]$ είναι ακέραιες περιοχές (βλ. πόρισμα 3.2.3 και πρόταση 3.1.2), με την πρώτη υποπεριοχή τής δεύτερης. Επομένως, ορίζονται τα *σώματα κλασμάτων* αυτών (βλ. εδ. 2.3.20 και 2.3.22)

$$\boxed{K(\mathsf{X}) := \mathbf{Fr}(K[\mathsf{X}])} \quad \text{και} \quad \boxed{K(\!(\mathsf{X})\!) := \mathbf{Fr}(K[\![\mathsf{X}]\!])}$$

(με το πρώτο υπόσωμα τού δευτέρου).

3.8.1 Ορισμός. Το σώμα $K(\mathsf{X})$ καλείται, ιδιαιτέρως, **σώμα των ρητών εκφράσεων** μιας απροσδιορίστου X υπεράνω τού K, τα δε στοιχεία του **πολυωνυμικά κλάσματα** (ή **ρητές εκφράσεις** ή **ρητές συναρτήσεις** ως προς την X). Κάθε πολυωνυμικό κλάσμα έχον ως παρονομαστή του μια δύναμη ενός ανάγωγου μονικού πολυωνύμου και ως αριθμητή του ένα πολυώνυμο βαθμού μικροτέρου τού βαθμού τού παρονομαστή του, καλείται **απλό** (ή **μερικό**) **πολυωνυμικό κλάσμα** (υπεράνω τού K).

Θα αποδείξουμε ότι *κάθε* πολυωνυμικό κλάσμα μπορεί να εκφρασθεί μονοσημάντως ως άθροισμα (πεπερασμένου πλήθους) απλών πολυωνυμικών κλασμάτων και ενός ειδικού πολυωνύμου (τού λεγομένου *ακεραίου μέρους του*).

3.8.2 Λήμμα. *Κάθε πολυωνυμικό κλάσμα* $\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} \in K(\mathsf{X})$ *γράφεται κατά τρόπο μοναδικό υπό τη μορφή*

$$\boxed{\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} = \varpi(\mathsf{X}) + \frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})},} \tag{3.50}$$

όπου $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$ *με* $\deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X}))$. *Η μοναδικότητα, μάλιστα, αυτή διατηρείται και υπό την ακόλουθη ευρύτερη έννοια*: *Εάν*

$$\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} = \varpi'(\mathsf{X}) + \frac{\upsilon'(\mathsf{X})}{\psi'(\mathsf{X})}, \tag{3.51}$$

όπου $\varpi'(\mathsf{X}), \upsilon'(\mathsf{X}) \in K[\mathsf{X}], \psi'(\mathsf{X}) \in K[\mathsf{X}] \setminus \{\mathbf{0}_{K[\mathsf{X}]}\}$, *με* $\deg(\upsilon'(\mathsf{X})) < \deg(\psi'(\mathsf{X}))$, *τότε*

$$\varpi'(\mathsf{X}) = \varpi(\mathsf{X}) \ \textit{και} \ \frac{\upsilon'(\mathsf{X})}{\psi'(\mathsf{X})} = \frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}. \tag{3.52}$$

ΑΠΟΔΕΙΞΗ. Σύμφωνα με το θεώρημα 3.3.1 υπάρχει ένα ζεύγος μονοσημάντως ορισμένων πολυωνύμων $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in K[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\varphi(\mathsf{X}) = \varpi(\mathsf{X})\psi(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X})).$$

Εξ αυτού έπεται η (3.50). Επιπροσθέτως, εάν ισχύει η (3.51), τότε

$$K[\mathsf{X}] \ni \varpi(\mathsf{X}) - \varpi'(\mathsf{X}) = \frac{\upsilon'(\mathsf{X})}{\psi'(\mathsf{X})} - \frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})} = \frac{\upsilon'(\mathsf{X})\psi(\mathsf{X}) - \upsilon(\mathsf{X})\psi'(\mathsf{X})}{\psi(\mathsf{X})\psi'(\mathsf{X})},$$

και από τις ανισότητες $\deg(\upsilon(\mathsf{X})) < \deg(\psi(\mathsf{X}))$ και $\deg(\upsilon'(\mathsf{X})) < \deg(\psi'(\mathsf{X}))$ προκύπτει ότι

$$\begin{aligned}
&\deg(\upsilon(\mathsf{X})) + \deg(\upsilon'(\mathsf{X})) < \deg(\psi(\mathsf{X})\psi'(\mathsf{X})),\\
&\deg(\upsilon(\mathsf{X})\psi'(\mathsf{X})) + \deg(\upsilon'(\mathsf{X})\psi(\mathsf{X})) \leq \deg(\upsilon(\mathsf{X})) + \deg(\upsilon'(\mathsf{X})),\\
&\deg(\upsilon'(\mathsf{X})\psi(\mathsf{X}) - \upsilon(\mathsf{X})\psi'(\mathsf{X})) \leq \deg(\upsilon(\mathsf{X})\psi'(\mathsf{X})) + \deg(\upsilon'(\mathsf{X})\psi(\mathsf{X})).
\end{aligned}$$

Ως εκ τούτου,

$$\left.\begin{aligned}\psi(\mathsf{X})\psi'(\mathsf{X}) \mid \upsilon'(\mathsf{X})\psi(\mathsf{X}) - \upsilon(\mathsf{X})\psi'(\mathsf{X})\\ \deg(\upsilon'(\mathsf{X})\psi(\mathsf{X}) - \upsilon(\mathsf{X})\psi'(\mathsf{X})) < \deg(\psi(\mathsf{X})\psi'(\mathsf{X}))\end{aligned}\right\} \Rightarrow \varpi(\mathsf{X}) - \varpi'(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]},$$

καταλήγοντας στις ισότητες (3.52). □

3.8.3 Ορισμός. Το $\varpi(\mathsf{X})$ καλείται **ακέραιο μέρος** και το $\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}$ **αμιγώς κλασματικό μέρος** τού $\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} \in K(\mathsf{X})$.

3.8.4 Θεώρημα. *Το αμιγώς κλασματικό μέρος* $\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}$ *οιουδήποτε πολυωνυμικού κλάσματος* (3.50) *γράφεται κατά τρόπο μοναδικό υπό τη μορφή*

$$\boxed{\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})} = \sum_{i=1}^{k}\left(\sum_{j=1}^{m_i}\frac{\beta_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}}\right),} \tag{3.53}$$

όπου

$$\psi(\mathsf{X}) = c\prod_{i=1}^{k}\psi_i(\mathsf{X})^{m_i}$$

είναι η συνεπτυγμένη αποσύνθεση τού $\psi(\mathsf{X})$ (βλ. 3.5.9 (ii)) *και* $\beta_{i,j}(\mathsf{X}) \in K[\mathsf{X}]$ *πολυώνυμα με*

$$\deg(\beta_{i,j}(\mathsf{X})) < \deg(\psi_i(\mathsf{X})),\ \forall j \in \{1,...,m_i\}\ \textit{και}\ \ \forall i \in \{1,...,k\}.$$

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Υπάρχουν πολυώνυμα* $\alpha_1(\mathsf{X}),...,\alpha_k(\mathsf{X}) \in K[\mathsf{X}]$ *μονοσημάντως ορισμένα μέσω των ιδιοτήτων*

$$\deg(\alpha_i(\mathsf{X})) < \deg(\psi_i(\mathsf{X})^{m_i}),\ \forall i \in \{1,...,k\},$$

και

$$\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})} = \frac{c^{-1}\upsilon(\mathsf{X})}{\prod_{i=1}^{k}\psi_i(\mathsf{X})^{m_i}} = \sum_{i=1}^{k}\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}. \tag{3.54}$$

Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Όταν $k = 1$, αρκεί να τεθεί $\alpha_1(\mathsf{X}) := c^{-1}\upsilon(\mathsf{X})$. Όταν $k = 2$,

$$\psi_1(\mathsf{X}) \neq \psi_2(\mathsf{X}) \underset{3.5.12}{\Longrightarrow} \mu\kappa\delta(\psi_1(\mathsf{X})^{m_1}, \psi_2(\mathsf{X})^{m_2}) = 1_K$$

$$\underset{3.3.15}{\Longrightarrow} \exists\omega_1(\mathsf{X}),\omega_2(\mathsf{X}) \in K[\mathsf{X}] : \omega_1(\mathsf{X})\psi_1(\mathsf{X})^{m_1} + \omega_2(\mathsf{X})\psi_2(\mathsf{X})^{m_2} = 1_K,$$

οπότε

$$\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X})\psi_1(\mathsf{X})^{m_1} + \left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X})\psi_2(\mathsf{X})^{m_2} = c^{-1}\upsilon(\mathsf{X}). \tag{3.55}$$

Εάν ισχύει $\deg(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1})$, τότε θα ισχύει και η ανισότητα

$$\deg(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X})) < \deg(\psi_2(\mathsf{X})^{m_2}),$$

διότι $\deg(c^{-1}\upsilon(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1}\psi_2(\mathsf{X})^{m_2})$ και

$$\deg(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X})\psi_2(\mathsf{X})^{m_2}) < \deg(\psi_1(\mathsf{X})^{m_1}\psi_2(\mathsf{X})^{m_2}).$$

Εν τοιαύτη περιπτώσει θέτουμε

$$\alpha_1(\mathsf{X}) := \left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X}),\ \alpha_2(\mathsf{X}) := \left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X}). \tag{3.56}$$

Εάν ισχύει $\deg(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X})) \geq \deg(\psi_1(\mathsf{X})^{m_1})$, τότε

$$\exists\zeta(\mathsf{X}),\eta(\mathsf{X}) \in K[\mathsf{X}] : \left(c^{-1}\upsilon(\mathsf{X})\right)\omega_2(\mathsf{X}) = \zeta(\mathsf{X})\psi_1(\mathsf{X})^{m_1} + \eta(\mathsf{X})$$

με $\deg(\eta(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1})$ και η (3.55) δίδει

$$\left(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X}) + \zeta(\mathsf{X})\psi_2(\mathsf{X})^{m_2}\right)\psi_1(\mathsf{X})^{m_1} + \eta(\mathsf{X})\psi_2(\mathsf{X})^{m_2} = c^{-1}\upsilon(\mathsf{X}). \quad (3.57)$$

Επειδή οι βαθμοί των $c^{-1}\upsilon(\mathsf{X})$ και $\eta(\mathsf{X})\psi_2(\mathsf{X})^{m_2}$ είναι $< \deg(\psi_1(\mathsf{X})^{m_1}\psi_2(\mathsf{X})^{m_2})$, από την (3.57) προκύπτει ότι

$$\deg(\left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X}) + \zeta(\mathsf{X})\psi_2(\mathsf{X})^{m_2}) < \deg(\psi_2(\mathsf{X})^{m_2}).$$

Εν τοιαύτη περιπτώσει θέτουμε

$$\alpha_1(\mathsf{X}) := \eta(\mathsf{X}),\ \alpha_2(\mathsf{X}) := \left(c^{-1}\upsilon(\mathsf{X})\right)\omega_1(\mathsf{X}) + \zeta(\mathsf{X})\psi_2(\mathsf{X})^{m_2}. \quad (3.58)$$

Τα (μέσω των (3.56) και (3.58)) ορισθέντα πολυώνυμα $\alpha_1(\mathsf{X}), \alpha_2(\mathsf{X})$ είναι τα μοναδικά πολυώνυμα για τα οποία ισχύει η (3.54) για $k = 2$. Πράγματι· εάν

$$\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})} = \frac{\alpha_1(\mathsf{X})}{\psi_1(\mathsf{X})^{m_1}} + \frac{\alpha_2(\mathsf{X})}{\psi_2(\mathsf{X})^{m_2}} = \frac{\alpha_1'(\mathsf{X})}{\psi_1(\mathsf{X})^{m_1}} + \frac{\alpha_2'(\mathsf{X})}{\psi_2(\mathsf{X})^{m_2}},$$

όπου $\alpha_1'(\mathsf{X}), \alpha_2'(\mathsf{X}) \in K[\mathsf{X}]$ με

$$\deg(\alpha_1'(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1}),\ \deg(\alpha_2'(\mathsf{X})) < \deg(\psi_2(\mathsf{X})^{m_2}),$$

τότε $\frac{\alpha_1(\mathsf{X})-\alpha_1'(\mathsf{X})}{\psi_1(\mathsf{X})^{m_1}} = \frac{\alpha_2(\mathsf{X})-\alpha_2'(\mathsf{X})}{\psi_2(\mathsf{X})^{m_2}}$, οπότε

$$\left.\begin{aligned}\psi_1(\mathsf{X})^{m_1}(\alpha_2(\mathsf{X}) - \alpha_2'(\mathsf{X})) = \psi_2(\mathsf{X})^{m_2}\left(\alpha_1(\mathsf{X}) - \alpha_1'(\mathsf{X})\right)\\ \text{μκδ}(\psi_1(\mathsf{X})^{m_1}, \psi_2(\mathsf{X})^{m_2}) = 1_K\end{aligned}\right\} \underset{3.3.16}{\Longrightarrow} \psi_1(\mathsf{X})^{m_1} \mid \alpha_1(\mathsf{X}) - \alpha_1'(\mathsf{X})$$

και

$$\left.\begin{aligned}\deg(\alpha_1(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1})\\ \deg(\alpha_1'(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1})\\ \deg\left(\alpha_1(\mathsf{X}) - \alpha_1'(\mathsf{X})\right)\\ \leq \max\{\deg\left(\alpha_1(\mathsf{X})\right), \deg(\alpha_1'(\mathsf{X}))\}\end{aligned}\right\} \Longrightarrow \deg\left(\alpha_1(\mathsf{X}) - \alpha_1'(\mathsf{X})\right) < \deg(\psi_1(\mathsf{X})^{m_1}).$$

Επομένως,

$$\left.\begin{aligned}\psi_1(\mathsf{X})^{m_1} \mid \alpha_1(\mathsf{X}) - \alpha_1'(\mathsf{X})\\ \deg(\alpha_1(\mathsf{X}) - \alpha_1'(\mathsf{X})) < \deg(\psi_1(\mathsf{X})^{m_1})\end{aligned}\right\} \Rightarrow \alpha_1(\mathsf{X}) - \alpha_1'(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]},$$

απ' όπου έπεται ότι $\alpha_1(\mathsf{X}) = \alpha_1'(\mathsf{X})$ και $\alpha_2(\mathsf{X}) = \alpha_2'(\mathsf{X})$. Εν συνεχεία, υποθέτουμε ότι $k \geq 3$ και ότι ο ισχυρισμός είναι αληθής για πολυώνυμα, το πλήθος των οποίων είναι $< k$. Επειδή $\text{μκδ}(\prod_{i=1}^{k-1}\psi_i(\mathsf{X})^{m_i}, \psi_k(\mathsf{X})^{m_k}) = 1_K$ (βλ. πόρισμα 3.5.13), υπάρχουν μονοσημάντως ορισμένα $\alpha(\mathsf{X}), \alpha_k(\mathsf{X}) \in K[\mathsf{X}]$ με

$$\deg(\alpha(\mathsf{X})) < \deg(\textstyle\prod_{i=1}^{k-1}\psi_i(\mathsf{X})^{m_i}),\ \deg(\alpha_k(\mathsf{X})) < \deg(\psi_k(\mathsf{X})^{m_k}),$$

τέτοια ώστε να ισχύει

$$\frac{\upsilon(\mathsf{X})}{\psi(\mathsf{X})}=\frac{c^{-1}\upsilon(\mathsf{X})}{\prod\limits_{i=1}^{k}\psi_i(\mathsf{X})^{m_i}}=\frac{\alpha(\mathsf{X})}{\prod\limits_{i=1}^{k-1}\psi_i(\mathsf{X})^{m_i}}+\frac{\alpha_k(\mathsf{X})}{\psi_k(\mathsf{X})^{m_k}}. \tag{3.59}$$

Κατά την επαγωγική μας υπόθεση υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\alpha_1(\mathsf{X}),...,\alpha_{k-1}(\mathsf{X})\in K[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\frac{\alpha(\mathsf{X})}{\prod\limits_{i=1}^{k-1}\psi_i(\mathsf{X})^{m_i}}=\sum_{i=1}^{k-1}\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}} \tag{3.60}$$

και $\deg(\alpha_i(\mathsf{X}))<\deg(\psi_i(\mathsf{X})^{m_i}),\ \forall i\in\{1,...,k-1\}$. Η (3.54) έπεται από τις (3.59) και (3.60).

Βήμα 2ο. *Για κάθε* $i\in\{1,...,k\}$ *υπάρχουν μονοσημάντως ορισμένα πολυώνυμα* $\beta_{i,1}(\mathsf{X}),...,\beta_{i,m_i}(\mathsf{X})\in K[\mathsf{X}]$ *με*

$$\deg(\beta_{i,j}(\mathsf{X}))<\deg(\psi_i(\mathsf{X})),\ \forall j\in\{1,...,m_i\},$$

και

$$\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\sum_{j=1}^{m_i}\frac{\beta_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}}. \tag{3.61}$$

Πράγματι· εάν ορίσουμε ως $\beta_{i,1}(\mathsf{X})$ το υπόλοιπο τής διαιρέσεως τού $\alpha_i(\mathsf{X})$ διά τού $\psi_i(\mathsf{X})$, ως $\beta_{i,2}(\mathsf{X})$ το υπόλοιπο τής διαιρέσεως τού πηλίκου της διά τού $\psi_i(\mathsf{X})$ κ.ο.κ., λαμβάνουμε διαδοχικώς

$$\begin{array}{ll}
\alpha_i(\mathsf{X})=\varpi_{i,1}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,1}(\mathsf{X}), & \deg\left(\beta_{i,1}(\mathsf{X})\right)<\deg\left(\psi_i(\mathsf{X})\right),\\
\varpi_{i,1}(\mathsf{X})=\varpi_{i,2}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,2}(\mathsf{X}), & \deg\left(\beta_{i,2}(\mathsf{X})\right)<\deg\left(\psi_i(\mathsf{X})\right),\\
\varpi_{i,2}(\mathsf{X})=\varpi_{i,3}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,3}(\mathsf{X}), & \deg\left(\beta_{i,3}(\mathsf{X})\right)<\deg\left(\psi_i(\mathsf{X})\right),\\
\vdots & \vdots\\
\varpi_{i,m_i-3}(\mathsf{X})=\varpi_{i,m_i-2}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,m_i-2}(\mathsf{X}), & \deg\left(\beta_{i,m_i-2}(\mathsf{X})\right)<\deg\left(\psi_i(\mathsf{X})\right),\\
\varpi_{i,m_i-2}(\mathsf{X})=\varpi_{i,m_i-1}(\mathsf{X})\,\psi_i(\mathsf{X})+\beta_{i,m_i-1}(\mathsf{X}), & \deg\left(\beta_{i,m_i-1}(\mathsf{X})\right)<\deg\left(\psi_i(\mathsf{X})\right),
\end{array}$$

όπου

$$\deg\left(\varpi_{i,j}\right)<\deg\left(\psi_i(\mathsf{X})^{m_i-j}\right),\ \forall j\in\{1,...,m_i-1\}.$$

Θέτοντας $\beta_{i,m_i}(\mathsf{X}):=\varpi_{i,m_i-1}(\mathsf{X})$ συνάγουμε ότι

$$\tfrac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\tfrac{\varpi_{i,1}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-1}}+\tfrac{\beta_{i,1}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\tfrac{\varpi_{i,2}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-2}}+\tfrac{\beta_{i,2}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-1}}+\tfrac{\beta_{i,1}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}}=\cdots$$

καταλήγοντας στην (3.61). Απομένει να αποδειχθεί ότι τα κατ' αυτόν τον τρόπο ορισθέντα πολυώνυμα $\beta_{i,1}(\mathsf{X}),...,\beta_{i,m_i}(\mathsf{X})$ είναι τα μόνα πολυώνυμα με αυτήν την ιδιότητα. Εάν

$$\frac{\alpha_i(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i}} = \sum_{j=1}^{m_i} \frac{\beta'_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}}, \tag{3.62}$$

για κάποια $\beta'_{i,1}(\mathsf{X}),...,\beta'_{i,m_i}(\mathsf{X}) \in K[\mathsf{X}]$ με

$$\deg(\beta'_{i,j}(\mathsf{X})) < \deg(\psi_i(\mathsf{X})),\ \forall j \in \{1,...,m_i\},$$

τότε (ύστερα από αφαίρεση τής (3.62) από την (3.61) κατά μέλη) λαμβάνουμε

$$\sum_{j=1}^{m_i} \frac{\beta_{i,j}(\mathsf{X}) - \beta'_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}} = 0_{K(\mathsf{X})}. \tag{3.63}$$

Πολλαπλασιασμός αμφοτέρων των μελών τής (3.63) με $\psi_i(\mathsf{X})^{m_i-1}$ δίδει

$$\frac{\beta_{i,1}(\mathsf{X}) - \beta'_{i,1}(\mathsf{X})}{\psi_i(\mathsf{X})} = -\sum_{j=2}^{m_i} (\beta_{i,j}(\mathsf{X}) - \beta'_{i,j}(\mathsf{X}))\psi_i(\mathsf{X})^{j-2} \in K[\mathsf{X}],$$

απ' όπου έπεται ότι

$$\left.\begin{array}{r} \psi_i(\mathsf{X}) \mid \beta_{i,1}(\mathsf{X}) - \beta'_{i,1}(\mathsf{X}) \\ \deg(\beta_{i,1}(\mathsf{X}) - \beta'_{i,1}(\mathsf{X})) < \deg(\psi_i(\mathsf{X})) \end{array}\right\} \Rightarrow \beta_{i,1}(\mathsf{X}) - \beta'_{i,1}(\mathsf{X}) = \mathbf{0}_{K[\mathsf{X}]}.$$

Τώρα η (3.63) γράφεται ως εξής:

$$\sum_{j=2}^{m_i} \frac{\beta_{i,j}(\mathsf{X}) - \beta'_{i,j}(\mathsf{X})}{\psi_i(\mathsf{X})^{m_i-j+1}} = 0_{K(\mathsf{X})}.$$

Επαναλαμβάνοντας την ίδια επιχειρηματολογία (με τα $\beta_{i,2}(\mathsf{X}), \beta'_{i,2}(\mathsf{X})$ στη θέση των $\beta_{i,1}(\mathsf{X}), \beta'_{i,1}(\mathsf{X})$ κ.ο.κ.) συμπεραίνουμε τελικώς ότι $\beta_{i,2}(\mathsf{X}) = \beta'_{i,2}(\mathsf{X}),...,$ $\beta_{i,m_i}(\mathsf{X}) = \beta'_{i,m_i}(\mathsf{X})$. □

3.8.5 Ορισμός. Η (μονοσημάντως ορισμένη) παράσταση ενός πολυωνυμικού κλάσματος $\frac{\varphi(\mathsf{X})}{\psi(\mathsf{X})} \in K(\mathsf{X})$, η οποία δίδεται από τις (3.50) και (3.53), καλείται **διάσπαση** (αυτού) **σε απλά** (ή σε **μερικά**) **πολυωνυμικά κλάσματα**.

3.8.6 Παρατήρηση. (i) Κάθε απλό πολυωνυμικό κλάσμα υπεράνω τού $\mathbb{C}$ είναι τής μορφής

$$\frac{a}{(\mathsf{X}+b)^k},\ \text{όπου}\ k \in \mathbb{N},\ a,b \in \mathbb{C}.$$

(ii) Κάθε απλό πολυωνυμικό κλάσμα υπεράνω τού $\mathbb{R}$ είναι τής μορφής

$$\frac{a}{(\mathsf{X}+b)^k} \quad \text{ή} \quad \frac{r\mathsf{X}+s}{(\mathsf{X}^2+\mathrm{A}\mathsf{X}+\mathrm{B})^l},$$

όπου $k,l\in\mathbb{N},\ a,b,r,s,\mathrm{A},\mathrm{B}\in\mathbb{R},\ \mathrm{A}^2-4\mathrm{B}<0$.

3.8.7 Παραδείγματα. (i) Εάν $a,b,c,r,s\in\mathbb{R}$ και $(a-b)(b-c)(c-a)\neq 0$, τότε

$$\begin{aligned}\frac{\mathsf{X}^2+r\mathsf{X}+s}{(\mathsf{X}-a)(\mathsf{X}-b)(\mathsf{X}-c)} &= \frac{(a-b)^{-1}(a-c)^{-1}(a^2+ra+s)}{\mathsf{X}-a}\\ &\quad+\frac{(b-c)^{-1}(c-a)^{-1}(b^2+rb+s)}{\mathsf{X}-b}+\frac{(c-a)^{-1}(a-b)^{-1}(c^2+rc+s)}{\mathsf{X}-c}.\end{aligned}$$

(ii) Παράδειγμα με μη μηδενικό ακέραιο μέρος:

$$\frac{\mathsf{X}^5-2\mathsf{X}^4+3\mathsf{X}^3+2\mathsf{X}^2+\mathsf{X}+1}{(\mathsf{X}-1)^3}=\mathsf{X}^2+\mathsf{X}+3+\frac{9}{\mathsf{X}-1}+\frac{11}{(\mathsf{X}-1)^2}+\frac{4}{(\mathsf{X}-1)^3}.$$

(iii) Ένα κατά τι πιο σύνθετο παράδειγμα είναι το εξής:

$$\frac{1}{\mathsf{X}^8+\mathsf{X}^7-\mathsf{X}^4-\mathsf{X}^3}=-\frac{1}{\mathsf{X}}+\frac{1}{\mathsf{X}^2}-\frac{1}{\mathsf{X}^3}+\frac{9/8}{\mathsf{X}+1}+\frac{1/4}{(\mathsf{X}+1)^2}+\frac{1/8}{\mathsf{X}-1}-\frac{1/4(\mathsf{X}+1)}{\mathsf{X}^2+1}.$$