Προτεινόμενες Λύσεις Ασκήσεων

Λύσεις Ασκήσεων Κεφαλαίου 1

Α-1-1. (a) Εάν τα F και G είναι δυο ομογενή πολυώνυμα βαθμού r και s, αντιστοίχως, ανήκοντα στον $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τότε

$$F = \sum a_{(i_1,i_2,\ldots,i_n)} \mathsf{X}_1^{i_1} \mathsf{X}_2^{i_2} \cdots \mathsf{X}_n^{i_n}, \quad G = \sum b_{(j_1,j_2,\ldots,j_n)} \mathsf{X}_1^{j_1} \mathsf{X}_2^{j_2} \cdots \mathsf{X}_n^{j_n},$$

όπου οι μόνοι μη μηδενικοί συντελεστές $a_{(i_1,i_2,\ldots,i_n)}$ είναι αυτοί που προτάσσονται $k \geq 1$ μονωνύμων βαθμού r και οι μόνοι μη μηδενικοί συντελεστές $b_{(j_1,j_2,\ldots,j_n)}$ είναι αυτοί που προτάσσονται $l \geq 1$ μονωνύμων βαθμού s. Επομένως, το γινόμενο FG αποτελείται από ένα άθροισμα kl μονωνύμων, καθένα των οποίων έχει βαθμό $r+s$. Ως εκ τούτου, το FG είναι ένα ομογενές πολυώνυμο βαθμού $r+s$.

(b) Έστω $F = H \cdot G$, όπου $G, H \in R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Υποθέτοντας ότι το H δεν είναι ομογενές, αρκεί να δείξουμε ότι το F δεν είναι ομογενές. Εάν

$$H = H_{(i)} + H_{(i+1)} + \cdots + H_{(i+j)}, \quad G = G_{(k)} + G_{(k+1)} + \cdots + G_{(k+l)},$$

με το $H_{(\alpha)}$ ομογενές πολυώνυμο βαθμού α για κάθε $\alpha \in \{i, i+1, \ldots, i+j\}$, το $G_{(\beta)}$ ομογενές πολυώνυμο βαθμού β για κάθε $\beta \in \{k, \ldots, k+l\}$ και

$$\begin{cases} i \geq 0,\ j > 0 : H_{(i)} \neq 0_{R[\mathsf{x}_1,\ldots,\mathsf{x}_n]},\ \ H_{(i+j)} \neq 0_{R[\mathsf{x}_1,\ldots,\mathsf{x}_n]}, \\ \\ k, l \geq 0 : G_{(k+l)} \neq 0_{R[\mathsf{x}_1,\ldots,\mathsf{x}_n]}. \end{cases}$$

Επειδή

$$F = H_{(i)}G_{(k)} + (H_{(i+1)}G_{(k)} + H_{(i)}G_{(k+1)}) + \cdots + H_{(i+j)}G_{(k+l)}$$

με $H_{(i)}G_{(k)} \neq 0_{R[\mathsf{x}_1,\ldots,\mathsf{x}_n]},\ \ H_{(i+j)}G_{(k+l)} \neq 0_{R[\mathsf{x}_1,\ldots,\mathsf{x}_n]}$, και

$$\deg(H_{(i)}G_{(k)}) = i + k < i + j + k + l = \deg(H_{(i+j)}G_{(k+l)}),$$

το F είναι πράγματι μη ομογενές. □

Α-1-2. Έστω R μια Π.Μ.Π. και έστω $\mathbf{Fr}(R)$ το σώμα κλασμάτων τής R. Κάθε στοιχείο z τού $\mathbf{Fr}(R)$ μπορεί να γραφεί υπό τη μορφή $z = \frac{a}{b}$, όπου τα $a \in R$, $b \in R \setminus \{0_R\}$, δεν έχουν (γνήσιους) κοινούς παράγοντες. Πράγματι· εάν το $z = \frac{x}{y}$ είναι τυχόν στοιχείο τού $\mathbf{Fr}(R)$, διακρίνουμε δύο περιπτώσεις: Για $x \in R^\times \cup \{0_R\}$ ή $y \in R^\times$, ο ισχυρισμός είναι αληθής. Για $x, y \in R \setminus (R^\times \cup \{0_R\})$, θεωρούμε έναν μ.κ.δ. d των στοιχείων x, y. Τότε $z = \frac{a}{b}$, με $a := \frac{x}{d}$, $b := \frac{y}{d}$, όπου τα $a \in R$, $b \in R \setminus \{0_R\}$, δεν έχουν (γνήσιους) κοινούς παράγοντες. Τούτη η παράσταση είναι μονοσημάντως ορισμένη, με μόνη εξαίρεση τον πολλαπλασιασμό (καθενός των a, b) με κάποιο αντιστρέψιμο στοιχείο τής R, ήτοι «μέχρι συντροφικότητας». Πράγματι· εάν

$$z = \frac{a}{b} = \frac{a'}{b'} \in \mathbf{Fr}(R),$$

όπου τα $a \in R$, $b \in R \setminus \{0_R\}$ (και αντιστοίχως, τα $a' \in R$, $b' \in R \setminus \{0_R\}$) δεν έχουν (γνήσιους) κοινούς παράγοντες, μπορούμε δίχως βλάβη τής γενικότητας να υποθέσουμε ότι $a, b, a', b' \in R \setminus (R^\times \cup \{0_R\})$. Θεωρούμε την παραγοντοποίηση των a, b, a', b' :

$$a = up_1p_2 \cdots p_k,\ \ a' = u'p'_1p'_2 \cdots p'_l,\ \ b = vq_1q_2 \cdots q_m,\ b' = v'q'_1q'_2 \cdots q'_n,$$

όπου $u, u', v, v' \in R^\times$, $k, l, m, n \in \mathbb{N}$ και τα $p_1, \ldots, p_k, p'_1, \ldots, p'_l, q_1, \ldots, q_m, q'_1, \ldots, q'_n$ ανάγωγα στοιχεία τής R. Προφανώς,

$$ab' = a'b \Longrightarrow uv' \left(p_1p_2 \cdots p_k\right)\left(q'_1q'_2 \cdots q'_n\right) = u'v \left(p'_1p'_2 \cdots p'_l\right)\left(q_1q_2 \cdots q_m\right).$$

Εξ υποθέσεως,

$$p_i \underset{\text{συν.}}{\not\sim} q_j, \forall (i,j) \in \{1, \ldots, k\} \times \{1, \ldots, m\},$$

και

$$p'_s \underset{\text{συν.}}{\not\sim} q'_t, \forall (s,t) \in \{1, \ldots, l\} \times \{1, \ldots, n\}.$$

Από την ιδιότητα τού μονοσημάντου τής παραγοντοποιήσεως των δύο μελών τής ανωτέρω ισότητας έπεται ότι $k = l$, $m = n$ και ότι υπάρχουν μετατάξεις $\sigma \in \mathfrak{S}_k$ και $\tau \in \mathfrak{S}_m$, τέτοιες ώστε να ισχύει

$$p_{\sigma(i)} \underset{\text{συν.}}{\sim} p'_i,\ \ \forall i \in \{1, \ldots, k\}, \quad q_{\tau(j)} \underset{\text{συν.}}{\sim} q'_j,\ \ \forall j \in \{1, \ldots, m\}.$$

Κατά συνέπειαν, $a \underset{\text{συν.}}{\sim} a'$ και $b \underset{\text{συν.}}{\sim} b'$. □

Α-1-3. Έστω ότι το $\mathbf{k}$ είναι ένα απειροπληθές σώμα και ότι $F \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Εάν υποτεθεί ότι $F(a_1, \ldots, a_n) = 0$ για όλα τα $a_1, \ldots, a_n \in \mathbf{k}$, θα αποδειχθεί ότι το F

είναι το μηδενικό πολυώνυμο. Θα εργασθούμε επαγωγικώς επί τού n. Για $n = 1$ ο ισχυρισμός είναι αληθής, διότι κάθε $F \in \mathbf{k}[\mathsf{X}] \setminus \{0_{\mathbf{k}[\mathsf{X}]}\}$ διαθέτει το πολύ $\deg(F)$ σημεία μηδενισμού. (Βλ. πόρισμα 1.1.27.) Έστω $n \geq 2$. Τότε κάθε μη μηδενικό πολυώνυμο $F \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ γράφεται ως άθροισμα $F = \sum_{i=1}^{\nu} F_i \mathsf{X}_n^i$, για κάποια πολυώνυμα $F_1, \ldots, F_\nu \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_{n-1}]$, με τουλάχιστον ένα εξ αυτών μη μηδενικό. Σύμφωνα με την επαγωγική υπόθεση, υπάρχουν $a_1, \ldots, a_{n-1} \in \mathbf{k}$, ούτως ώστε το $F(a_1, \ldots, a_{n-1}, \mathsf{X}_n) \in \mathbf{k}[\mathsf{X}_n]$ να μην είναι μηδενικό. Επειδή αυτό το πολυώνυμο διαθέτει πεπερασμένα σημεία μηδενισμού, υπάρχει $a_n \in \mathbf{k}$, τέτοιο ώστε να ισχύει $F(a_1, \ldots, a_{n-1}, a_n) \neq 0_{\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]}$. □

A-1-4. Έστω $\mathbf{k}$ ένα σώμα. Υποθέτουμε ότι υπάρχουν πεπερασμένα ανάγωγα μονικά πολυώνυμα εντός τού $\mathbf{k}[\mathsf{X}]$, ας πούμε τα $F_1, \ldots, F_n$. Έστω $G := F_1 \cdots F_n + 1_{\mathbf{k}}$. Επειδή ο πολυωνυμικός δακτύλιος $\mathbf{k}[\mathsf{X}]$ είναι Π.Μ.Π. (βλ. θεώρημα 1.1.24), το G αποσυντίθεται υπό τη μορφή γινομένου αναγώγων (κατ' ανάγκην μονικών) πολυωνύμων

$$G = G_1 \cdot G_2 \cdots G_m,$$

Εξ υποθέσεως, $G_j = c_j F_{\tau(j)}$, για κάθε $j \in \{1, \ldots, m\}$, όπου $c_j \in \mathbf{k} \setminus \{0_{\mathbf{k}}\}$, $m \leq n$ και

$$\tau : \{1, \ldots, m\} \hookrightarrow \{1, \ldots, n\}$$

κατάλληλη ένριψη. Συνεπώς,

$$\prod_{j=1}^{m} F_{\tau(j)} \left(\prod_{j=1}^{m} c_j - \prod_{i \in \{1, \ldots, n\} \setminus \operatorname{Im}(\tau)}^{m} F_i \right) = 1_{\mathbf{k}}.$$

Επειδή καθένα των $F_{\tau(j)}$, $j \in \{1, \ldots, m\}$, ως ανάγωγο, είναι μη σταθερό, η ανωτέρω ισότητα μας οδηγεί σε αντίφαση. □

A-1-5. Έστω $\mathbf{k}$ ένα αλγεβρικώς κλειστό σώμα. Εάν το $\mathbf{k}$ είναι πεπερασμένο, ας πούμε $\mathbf{k} = \{a_1, \ldots, a_\nu\}$, τότε για το πολυώνυμο

$$F(\mathsf{X}) := \left(\prod_{j=1}^{\nu} (\mathsf{X} - a_j) \right) + 1_{\mathbf{k}} \in \mathbf{k}[\mathsf{X}]$$

ισχύει $F(a_j) = 1_{\mathbf{k}} \neq 0_{\mathbf{k}}, \forall j \in \{1, \ldots, \nu\}$, οπότε το F δεν διαθέτει κανένα σημείο μηδενισμού εντός τού $\mathbf{k}$. Επειδή $\deg(F) = \nu = \sharp(\mathbf{k}) \geq 2$, το $\mathbf{k}$ δεν μπορεί να είναι αλγεβρικώς κλειστό. Άτοπο! Κατά συνέπειαν, το $\mathbf{k}$ οφείλει να είναι απειροπληθές. □

A-1-6. *Απόδειξη προτάσεως* 1.1.34: (a) Επειδή ο $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι ισόμορφος τού $R[\mathsf{X}_1, \ldots, \mathsf{X}_{n-1}][\mathsf{X}_n]$, η απόδειξη έπεται επαγωγικώς (επί τού n) βάσει τού (a) τής προτάσεως 1.1.22.

(b) Για οιαδήποτε μη μηδενικά πολυώνυμα $F, G \in R[\mathsf{X}_1, \dots, \mathsf{X}_n]$,

$$F = \sum_{k\geq 0} F_{(k)}, \text{ όπου } F_{(k)} := \sum_{i_1+i_2+\cdots+i_n=k} a_{(i_1,i_2,\dots,i_n)} \mathsf{X}_1^{i_1}\mathsf{X}_2^{i_2}\cdots\mathsf{X}_n^{i_n}$$

και

$$G = \sum_{l\geq 0} G_{(l)}, \text{ όπου } G_{(l)} := \sum_{j_1+j_2+\cdots+j_n=l} b_{(j_1,j_2,\dots,j_n)} \mathsf{X}_1^{j_1}\mathsf{X}_2^{j_2}\cdots\mathsf{X}_n^{j_n},$$

με $\deg(F) = n$, $\deg(G) = m$, έχουμε

$$F \cdot G = \left(F_{(0)} + \cdots + F_{(n)}\right)\left(G_{(0)} + \cdots + G_{(m)}\right) = F_{(0)} \cdot G_{(0)} + \cdots + F_{(n)} \cdot G_{(m)}.$$

Επειδή ο R είναι ακεραία περιοχή, ο προσθετέος $F_{(n)} \cdot G_{(m)}$ διαθέτει τουλάχιστον έναν συντελεστή $\neq 0_R$, οπότε

$$\deg(F \cdot G) = \deg\left(F_{(n)} \cdot G_{(m)}\right) = n + m.$$

Απόδειξη προτάσεως 1.1.37: Τα (a) και (b) αποδεικνύονται με απευθείας μερική επίτυπη παραγώγιση και πράξεις.

(c) Κατ' αρχάς θα αποδείξουμε το εξής χρηστικό λήμμα: *Εάν ένα (μη μηδενικό) πολυώνυμο* $F \in R[\mathsf{X}_1, \dots, \mathsf{X}_n]$ *είναι ομογενές βαθμού* d, *τότε*

$$F(\lambda\mathsf{X}_1, \dots, \lambda\mathsf{X}_n) = \lambda^d \cdot F(\mathsf{X}_1, \dots, \mathsf{X}_n),\ \forall \lambda \in R.$$

Και αντιστρόφως· όταν η ανωτέρω ισότητα ισχύει για κάποιο $F \in \mathbf{k}[\mathsf{X}_0, \dots, \mathsf{X}_n]$ *και το* $\mathbf{k}$ *είναι απειροπληθές, το* F *οφείλει να είναι ομογενές.*

Απόδειξη λήμματος: Εάν το $F \in R[\mathsf{X}_1, \dots, \mathsf{X}_n]$ είναι ομογενές βαθμού d, τότε θα είναι τής μορφής

$$F = \sum_{i_1+i_2+\cdots+i_n=d} a_{(i_1,i_2,\dots,i_n)} \mathsf{X}_1^{i_1}\mathsf{X}_2^{i_2}\cdots\mathsf{X}_n^{i_n},$$

με κάποιους εκ των συντελεστών $a_{(i_1,i_2,\dots,i_n)} \neq 0$. Συνεπώς,

$$F(\lambda\mathsf{X}_1, \dots, \lambda\mathsf{X}_n) = \sum_{i_1+i_2+\cdots+i_n=d} a_{(i_1,i_2,\dots,i_n)} (\lambda\mathsf{X}_1)^{i_1}\cdots(\lambda\mathsf{X}_n)^{i_n} = \lambda^d \cdot F(\mathsf{X}_1, \dots, \mathsf{X}_n).$$

Και αντιστρόφως· εάν η ανωτέρω ισότητα ισχύει για κάποιο $F \in \mathbf{k}[\mathsf{X}_0, \dots, \mathsf{X}_n]$, το $\mathbf{k}$ είναι απειροπληθές, και υποθέσουμε ότι το F δεν είναι ομογενές, τότε

$$F = F_{(i)} + F_{(i+1)} + \cdots + F_{(i+j)},$$

με το $F_{(\alpha)}$ ομογενές πολυώνυμο βαθμού $\alpha, \forall\ \alpha \in \{i, i+1, \dots, i+j\}$ και $i \geq 0,\ j > 0$: $F_{(i)} \neq 0,\ F_{(i+j)} \neq 0$,

$$\deg(F) = i + j =: d.$$

Συνεπώς,

$$\lambda^d \cdot F(\mathsf{X}_1, \dots, \mathsf{X}_n) = F_{(i)}(\lambda\mathsf{X}_1, \dots, \lambda\mathsf{X}_n) + \cdots + F_{(d)}(\lambda\mathsf{X}_1, \dots, \lambda\mathsf{X}_n)$$

$$\iff \lambda^i \cdot F_{(i)}(\mathsf{X}_1, \dots, \mathsf{X}_n) + \cdots + \lambda^d \cdot \big(F_{(d)}(\mathsf{X}_1, \dots, \mathsf{X}_n) - F(\mathsf{X}_1, \dots, \mathsf{X}_n)\big) = 0,\ \forall \lambda \in R.$$

Εάν θεωρήσουμε το αριστερό μέλος ως ένα πολυώνυμο εντός τού $R\left[\mathsf{X}_1, \dots, \mathsf{X}_n\right][\lambda]$ (και το λ ως μια νέα απροσδιόριστο), αυτό θα έπρεπε (κατά την άσκηση **A-1-3**) να είναι μηδενικό, πράγμα άτοπο, διότι εξ υποθέσεως $F_{(i)} \neq 0$. Άρα το F οφείλει να είναι ομογενές βαθμού d.

Απόδειξη τύπου τού Euler: Από το (a) και την ισότητα τού προηγηθέντος λήμματος έπεται ότι

$$\frac{d}{d\lambda}F(\lambda\mathsf{X}_1, \dots, \lambda\mathsf{X}_n) = \sum_{i=1}^{n} \mathsf{X}_i \frac{\partial}{\partial \mathsf{X}_i}(F(\lambda\mathsf{X}_1, \dots, \lambda\mathsf{X}_n)) = d\lambda^{d-1}F(\mathsf{X}_1, \dots, \mathsf{X}_n).$$

Αρκεί να γίνει αποτίμηση αυτών των εκφράσεων για $\lambda = 1_R$. □

A-1-7. (a) Το F γράφεται ως (πεπερασμένο) άθροισμα τής μορφής

$$\sum \mu_{(j_1, j_2, \dots, j_n)} \mathsf{X}_1^{j_1} \mathsf{X}_2^{j_2} \cdots \mathsf{X}_n^{j_n}.$$

Επομένως,

$$F = \sum_{(j_1, j_2, \dots, j_n)} \mu_{(j_1, j_2, \dots, j_n)} (a_1 + \mathsf{X}_1 - a_1)^{j_1} \cdots (a_n + \mathsf{X}_n - a_n)^{j_n}$$

$$= \sum_{(j_1, j_2, \dots, j_n)} \mu_{(j_1, j_2, \dots, j_n)} \left[\sum_{k_1=0}^{j_1} \tbinom{j_1}{k_1} a_1^{k_1} (\mathsf{X}_1 - a_1)^{j_1 - k_1}\right] \cdots \left[\sum_{k_n=0}^{j_n} \tbinom{j_n}{k_n} a_n^{k_n} (\mathsf{X}_n - a_n)^{j_n - k_n}\right]$$

$$= \sum_{(j_1, j_2, \dots, j_n)} \mu_{(j_1, j_2, \dots, j_n)} \sum_{k_1=0}^{j_1} \cdots \sum_{k_n=0}^{j_n} \left(\prod_{s=1}^{n} \tbinom{j_s}{k_s}\right) \left(\prod_{s=1}^{n} a_s^{k_s}\right) \left(\prod_{s=1}^{n} (\mathsf{X}_s - a_s)^{j_s - k_s}\right)$$

$$= \sum_{(i_1, i_2, \dots, i_n)} \lambda_{(i_1, i_2, \dots, i_n)} \left(\mathsf{X}_1 - a_1\right)^{i_1} \cdots \left(\mathsf{X}_n - a_n\right)^{i_n},$$

όπου $i_m := j_m - k_m,\ \forall m \in \{1, \dots, n\}$, και

$$\lambda_{(i_1, i_2, \dots, i_n)} := \mu_{(j_1, j_2, \dots, j_n)} \sum_{k_1=0}^{j_1} \cdots \sum_{k_n=0}^{j_n} \left(\prod_{s=1}^{n} \tbinom{j_s}{k_s}\right) \left(\prod_{s=1}^{n} a_s^{k_s}\right).$$

(b) Εάν $F(a_1,\dots,a_n)=0$, τότε το

$$F=\sum_{(i_1,i_2,\dots,i_n)}\lambda_{(i_1,i_2,\dots,i_n)}\left(\mathsf{X}_1-a_1\right)^{i_1}\cdots\left(\mathsf{X}_n-a_n\right)^{i_n}$$

δεν διαθέτει σταθερούς όρους διαφορετικούς τού 0 (διότι αλλιώς θα είχαμε $F(a_1,\dots,a_n)\neq 0$). Άρα στο ανωτέρω άθροισμα τουλάχιστον ένας εκ των $i_1,i_2,\dots,i_n$ είναι διάφορος τού μηδενός, πράγμα που σημαίνει ότι υπάρχουν $G_1,\dots,G_n\in\mathbf{k}\left[\mathsf{X}_1,\dots,\mathsf{X}_n\right]$, τέτοια ώστε να ισχύει

$$F=\sum_{i=1}^{n}\left(\mathsf{X}_i-a_i\right)G_i.$$

Για $n\geq 2$ τα $G_1,\dots,G_n$ δεν είναι κατ' ανάγκην μονοσημάντως ορισμένα. Π.χ., για $n=2$, $a_1=a_2=0$ και $F=\mathsf{X}_1\mathsf{X}_2-\mathsf{X}_2^3\mathsf{X}_1$ έχουμε

$$F=\mathsf{X}_1G_1+\mathsf{X}_2G_2=\mathsf{X}_1\widetilde{G}_1+\mathsf{X}_2\widetilde{G}_2,$$

όπου $G_1:=\mathsf{X}_2$, $G_2:=-\mathsf{X}_2^2\mathsf{X}_1$, $\widetilde{G}_1:=-\mathsf{X}_2^3$, $\widetilde{G}_2:=\mathsf{X}_1$. Ωστόσο, για $n=1$, η ταυτότητα τής διαιρέσεως πολυωνύμων καθιστά το G_1 μοναδικό. □

A-1-8. Έστω X ένα *γνήσιο*, αλγεβρικό υποσύνολο τού $\mathbb{A}^1_{\mathbf{k}}$. Τότε υπάρχει κάποια οικογένεια πολυωνύμων $\mathcal{S}=\{F_\lambda:\lambda\in\Lambda\}\subset\mathbf{k}[\mathsf{X}]$ με

$$X=\mathbf{V}(\mathcal{S})=\left\{P\in\mathbb{A}^1_{\mathbf{k}}\middle|\,F_\lambda(P)=0,\ \forall\lambda\in\Lambda\right\}.$$

Υποθέτοντας ότι κανένα εκ των F_λ δεν είναι σταθερό, λαμβάνουμε προφανώς

$$0<\sharp(X)\leq\min\left\{\deg(F_\lambda):\lambda\in\Lambda\right\},$$

απ' όπου έπεται η επαλήθευση τού αρχικού ισχυρισμού (λαμβανομένου υπ' όψιν τού (5) τής προτάσεως 1.2.3). □

A-1-9. Εάν το $\mathbf{k}$ είναι ένα πεπερασμένο σώμα, έχουμε $\sharp(\mathbb{A}^n_{\mathbf{k}})=\sharp(\mathbf{k}^n)=\sharp(\mathbf{k})^n<\infty$, οπότε κάθε υποσύνολο τού $\mathbb{A}^n_{\mathbf{k}}$ είναι κατ' ανάγκην πεπερασμένο και (σύμφωνα με το (5) τής προτάσεως 1.2.3) αλγεβρικό. □

A-1-10. Εντός τού $\mathbb{A}^1_{\mathbb{R}}$ το σύνολο των φυσικών αριθμών γράφεται

$$\mathbb{N}=\bigcup\{n|\,n\in\mathbb{N}\}=\bigcup_{n\in\mathbb{N}}\mathbf{V}(\mathsf{X}-n),$$

δίχως να είναι αλγεβρικό σύνολο (επί τη βάσει τής ασκήσεως **A-1-8**). □

A-1-11. (a) Προφανώς, $\left\{\left(t,t^2,t^3\right)\in\mathbb{A}^3_{\mathbf{k}}\mid t\in\mathbf{k}\right\}=\mathbf{V}(F_1,F_2)$, όπου

$$F_1=\mathsf{Y}-\mathsf{X}^2,\quad F_2=\mathsf{Z}-\mathsf{XY}\subset\mathbf{k}\left[\mathsf{X},\mathsf{Y},\mathsf{Z}\right].$$

(b) Προφανώς,

$$\left\{(\cos(t),\sin(t))\in\mathbb{A}^2_{\mathbb{R}}\mid t\in\mathbb{R}\right\}=\mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1).$$

(c) Επειδή κάθε σημείο $P=(x,y)$ τού $\mathbb{A}^2_{\mathbb{R}}$ γράφεται συναρτήσει πολικών συντεταγμένων ως

$$x=r\cos(\theta),\quad y=r\sin(\theta),\quad r>0,\quad \theta\in\mathbb{R},$$

για το σύνολο των σημείων τού $\mathbb{A}^2_{\mathbb{R}}$, οι πολικές συντεταγμένες (r,θ) των οποίων πληρούν την εξίσωση $r=\sin(\theta)$, έχουμε

$$x=\sin(\theta)\cos(\theta)=\frac{1}{2}\sin(2\theta),\quad y=\sin^2(\theta)=\frac{1}{2}(1-\cos(2\theta)).$$

Ως εκ τούτου, το εν λόγω σύνολο ισούται με το $\mathbf{V}((2\mathsf{X})^2+(1-2\mathsf{Y})^2-1)\subset\mathbb{A}^2_{\mathbb{R}}$. □

A-1-12. Εάν η ευθεία L δίδεται μέσω τής εξισώσεως $\mathsf{Y}=a\mathsf{X}+b, a,b\in\mathbf{k}$, τότε οι συντεταγμένες κάθε σημείου ανήκοντος στην τομή $L\cap C$, όπου $C=\mathbf{V}(F)$ με $F=\sum\lambda_{(i,j)}\mathsf{X}^i\mathsf{Y}^j$, $i+j\leq n$ (και $i+j=n$ για τουλάχιστον ένα ζεύγος (i,j) για το οποίο ισχύει $\lambda_{(i,j)}\neq 0_{\mathbf{k}}$), πληρούν τη συνθήκη

$$F(\mathsf{X},a\mathsf{X}+b)=\sum\lambda_{(i,j)}\mathsf{X}^i\left(a\mathsf{X}+b\right)^j=0.$$

Επειδή το F διαθέτει το πολύ n σημεία μηδενισμού (βλ. πόρισμα 1.1.27) συμπεραίνουμε ότι $\sharp(L\cap C)\leq n$. □

A-1-13. (a) Ας υποθέσουμε ότι το $V:=\left\{(x,y)\in\mathbb{A}^2_{\mathbb{R}}\mid y=\sin(x)\right\}$ είναι αλγεβρικό. Τότε υπάρχει $\mathcal{S}\subset\mathbb{R}\left[\mathsf{X},\mathsf{Y}\right]$ με $V=\mathbf{V}(\mathcal{S})=\cap\left\{\mathbf{V}(F)\mid F\in\mathcal{S}\right\}$. Έστω $L:=\mathbf{V}(\mathsf{Y})$. Προφανώς $L\not\subseteq C$. Κατά την άσκηση **A-1-12** η τομή $L\cap V=\cap\left\{L\cap\mathbf{V}(F)\mid F\in\mathcal{S}\right\}$ περιέχει *πεπερασμένα* στοιχεία, πλήθους σίγουρα μικρότερου ή ίσου τού βαθμού (ως προς X) ενός πολυωνύμου $F_0\in\mathcal{S}$ για το οποίο ισχύει $\deg(F_0(\mathsf{X},0))\leq\deg(F(\mathsf{X},0)),\forall F\in\mathcal{S}$. Τούτο οδηγεί σε άτοπο, καθόσον

$$P=(x,y)\in L\cap V\Longleftrightarrow P\in\left\{(\kappa\pi,0)\in\mathbb{A}^2_{\mathbb{R}}\mid\kappa\in\mathbb{Z}\right\},$$

με το $\left\{(\kappa\pi,0)\in\mathbb{A}^2_{\mathbb{R}}\mid\kappa\in\mathbb{Z}\right\}$ απειροσύνολο.

(b) Ας υποθέσουμε ότι το $V':=\left\{(z,w)\in\mathbb{A}^2_{\mathbb{C}}\;\middle|\;|z|^2+|w|^2=1\right\}$ είναι αλγεβρικό. Τότε υπάρχει $\mathcal{S}\subset\mathbb{C}\left[\mathsf{X},\mathsf{Y}\right]$ με $V'=\mathbf{V}(\mathcal{S})=\cap\left\{\mathbf{V}(F)\mid F\in\mathcal{S}\right\}$. Έστω $L:=\mathbf{V}(\mathsf{Y}-\mathsf{X})$. Προφανώς $L\not\subseteq C$. Κατά την άσκηση **A-1-12** η τομή $L\cap V'=\cap\left\{L\cap\mathbf{V}(F)\mid F\in\mathcal{S}\right\}$ περιέχει

πεπερασμένα στοιχεία, πλήθους σίγουρα μικρότερου ή ίσου τού βαθμού (ως προς X) ενός πολυωνύμου $F_0 \in \mathcal{S}$ για το οποίο ισχύει $\deg(F_0(\mathsf{X},0)) \leq \deg(F(\mathsf{X},0))$, $\forall F \in \mathcal{S}$. Τούτο οδηγεί σε άτοπο, καθόσον

$$P=(x,y)\in L\cap V' \Longleftrightarrow P\in \left\{(z,z)\in \mathbb{A}^2_{\mathbb{C}} \;\middle|\; |z|=\pm\tfrac{\sqrt{2}}{2}\right\},$$

με το $\left\{(z,z)\in \mathbb{A}^2_{\mathbb{C}} \;\middle|\; |z|=\pm\tfrac{\sqrt{2}}{2}\right\}$ απειροσύνολο.

(c) Ας υποθέσουμε ότι το $V'' := \left\{(\cos(t),\sin(t),t)\in \mathbb{A}^3_{\mathbb{R}} \mid t\in\mathbb{R}\right\}$ είναι αλγεβρικό. Τότε υπάρχει $\mathcal{S}\subset \mathbb{R}[\mathsf{X},\mathsf{Y},\mathsf{Z}]$ με $V''=\mathbf{V}(\mathcal{S})=\cap\{\mathbf{V}(F) \mid F\in\mathcal{S}\}$. Εάν $a,b\in\mathbb{R}$ με $a^2+b^2=1$, $B:=\mathbf{V}(\mathsf{X}-a,\mathsf{Y}-b)\subset \mathbb{A}^3_{\mathbb{R}}$ και

$$F_0\in\mathcal{S}:\deg(F_0(a,b,\mathsf{Z}))\leq \deg(F(a,b,\mathsf{Z})),\forall F\in\mathcal{S},$$

τότε $B\cap V''\subseteq B\cap \mathbf{V}(F_0) \Longrightarrow \sharp(B\cap V'')\leq \deg(F_0(a,b,\mathsf{Z}))$. Τούτο οδηγεί σε άτοπο, καθόσον

$$P=(x,y,z)\in B\cap V'' \Longleftrightarrow P\in\left\{(a,b,t)\in\mathbb{A}^3_{\mathbb{R}} \mid t\in\mathbb{R}\right\},$$

με το $\left\{(a,b,t)\in\mathbb{A}^3_{\mathbb{R}} \mid t\in\mathbb{R}\right\}$ απειροσύνολο. □

A-1-14. Επειδή $\sharp(\mathbb{A}^n_{\mathbf{k}})=\sharp(\mathbf{k}^n)=\sharp(\mathbf{k})^n$ και το $\mathbf{k}$ είναι αλγεβρικώς κλειστό (και κατά συνέπειαν απειροπληθές, βλ. άσκηση **A-1-5**), το $\mathbb{A}^n_{\mathbf{k}}$ είναι απειροπληθές για κάθε $n\geq 1$. Για $n=1$ (επειδή κάθε πολυώνυμο τού $\mathbf{k}[\mathsf{X}_1]$ διαθέτει το πολύ τόσα σημεία μηδενισμού του εντός τού $\mathbf{k}$ όσος είναι ο βαθμός του, βλ. πόρισμα 1.1.27) το $\mathbf{V}(F)$ είναι πεπερασμένο και το $\mathbb{A}^1_{\mathbf{k}}\smallsetminus\mathbf{V}(F)$ απειροπληθές. Για $n\geq 2$,

$$\mathbb{A}^n_{\mathbf{k}}\smallsetminus\mathbf{V}(F)=\{(a_1,\ldots,a_n)\in\mathbb{A}^n_{\mathbf{k}} \mid F(a_1,\ldots,a_n)\neq 0\}$$

και $\mathbf{V}(F)=\{(a_1,\ldots,a_n)\in\mathbb{A}^n_{\mathbf{k}} \mid F(a_1,\ldots,a_n)\neq 0\}$. Εάν το $\mathbb{A}^n_{\mathbf{k}}\smallsetminus\mathbf{V}(F)$ ήταν πεπερασμένο και ίσο με $\{P_1,\ldots,P_m\}$, όπου $P_j=(a_{j1},\ldots,a_{jn})$ για κάθε $j\in\{1,\ldots,m\}$, τότε επαναλαμβάνοντας κατά γράμμα την απόδειξη τής ασκήσεως **A-1-3** (με τη μόνη διαφορά στο ότι η υπόθεσή μας θα είναι: $F(b_1,\ldots,b_n)=0$, για *οιαδήποτε* στοιχεία $b_1,\ldots,b_n$ ανήκοντα στο *απειροσύνολο* $\mathbf{k}\smallsetminus\{a_{ji} \mid j\in\{1,\ldots,m\}, i\in\{1,\ldots,n\}\}$) θα συμπεραίναμε ότι

$$F=0\Longrightarrow \mathbf{V}(F)=\varnothing\Longrightarrow \sharp(\mathbb{A}^n_{\mathbf{k}}\smallsetminus\mathbf{V}(F))=\sharp(\mathbb{A}^n_{\mathbf{k}})=\infty.$$

Άτοπο! Κατ' αναλογίαν, εάν το $\mathbf{V}(F)$ ήταν πεπερασμένο και ίσο με $\{P_1,\ldots,P_m\}$, όπου $P_j=(a_{j1},\ldots,a_{jn})$ για κάθε $j\in\{1,\ldots,m\}$, επιλέγοντας στοιχεία $b_1,\ldots,b_n$ ανήκοντα στο *απειροσύνολο* $\mathbf{k}\smallsetminus\{a_{ji} \mid j\in\{1,\ldots,m\}, i\in\{1,\ldots,n\}\}$ και γράφοντας το $F(\neq 0)$ ως άθροισμα $F=\sum_{i=1}^{\nu}F_i\mathsf{X}_n^i$, για κάποια $F_1,\ldots,F_\nu\in\mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_{n-1}]$, με τουλάχιστον ένα εξ αυτών μη μηδενικό, θα είχαμε $F_k(b_1,\ldots,b_{n-1})\neq 0$ για τουλάχιστον έναν δείκτη

$k \in \{1, \dots, \nu\}$ (διότι εάν ίσχυε $F_k(b_1, \dots, b_{n-1}) = 0$ για κάθε δείκτη $k \in \{1, \dots, \nu\}$, τότε $F(b_1, \dots, b_n) = 0$). Επομένως το πολυώνυμο $F(b_1, \dots, b_{n-1}, \mathsf{X}_n) \in \mathbf{k}[\mathsf{X}_n]$ θα ήταν μη μηδενικό, κι επειδή το $\mathbf{k}$ υπετέθη αλγεβρικώς κλειστό θα διέθετε ένα σημείο μηδενισμού εντός τού $\mathbf{k}$, κάτι που θα αντέφασκε προς την επιλογή $b_1, \dots, b_n$. Άρα και το $\mathbf{V}(F)$ είναι απειροπληθές.

Τέλος, εάν το W είναι ένα αλγεβρικό σύνολο εντός τού $\mathbb{A}^n_{\mathbf{k}}$, $n \geq 1$, τότε υπάρχει εξ ορισμού $\mathcal{S} \subset \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ με

$$W = \mathbf{V}(\mathcal{S}) = \bigcap \{\mathbf{V}(F) \mid F \in \mathcal{S}\} \Longrightarrow \mathbb{A}^n_{\mathbf{k}} \smallsetminus W = \bigcup \{\mathbb{A}^n_{\mathbf{k}} \smallsetminus \mathbf{V}(F) \mid F \in \mathcal{S}\}.$$

Σύμφωνα με όσα προείπαμε, το $\mathbb{A}^n_{\mathbf{k}} \smallsetminus W$ οφείλει να είναι απειροπληθές. □

A-1-15. (a) Ας υποτεθεί ότι $V = \mathbf{V}(\mathcal{S})$ και $W = \mathbf{V}(\mathcal{S}')$, όπου

$$\mathcal{S} = \{F_i \mid i \in J\} \subset \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n], \;\; \mathcal{S}' = \{G_j \mid j \in J\} \subset \mathbf{k}[\mathsf{Y}_1, \dots, \mathsf{Y}_m].$$

Τότε ένα σημείο $P = (a_1, \dots, a_n, b_1, \dots, b_m)$ ανήκει στο $V \times W$ εάν και μόνον εάν

$$P \in \mathbf{V}(\mathcal{S}) \times \mathbf{V}(\mathcal{S}') \Longleftrightarrow F_i(a_1, \dots, a_n) = 0, \forall i \in I \text{ και } G_j(b_1, \dots, b_m) = 0, \forall j \in J$$

$$\begin{aligned} &\Longleftrightarrow \quad (F_i(a_1, \dots, a_n), G_j(b_1, \dots, b_m)) = (F_i, G_j)(P) = 0, \forall (i,j) \in I \times J \\ &\Longleftrightarrow \quad P \in \mathbf{V}(\mathcal{S} \times \mathcal{S}'). \end{aligned}$$

Κατά συνέπειαν, το $V \times W$ αποτελεί ένα αλγεβρικό σύνολο εντός τού $\mathbb{A}^{n+m}_{\mathbf{k}}$.

(b) Ακόμη και όταν $n = 2$, η τοπολογία Zariski επί τού $\mathbb{A}^2_{\mathbf{k}} = \mathbb{A}^1_{\mathbf{k}} \times \mathbb{A}^1_{\mathbf{k}}$, όπου $\mathbf{k}$ αλγεβρικώς κλειστό σώμα, είναι διαφορετική τής συνήθους *τοπολογίας γινομένου*. Επί παραδείγματι, θεωρώντας ένα μη σταθερό πολυώνυμο $F(\mathsf{X}) \in \mathbf{k}[\mathsf{X}]$ (ήτοι με $\deg(F) \geq 1$) και την επίπεδη συσχετική καμπύλη $C := \mathbf{V}(\mathsf{Y} - F(\mathsf{X})) \subset \mathbb{A}^2_{\mathbf{k}}$, διαπιστώνουμε τα εξής:

i) Το συμπλήρωμα $\mathbb{A}^2_{\mathbf{k}} \smallsetminus C$ δεν μπορεί να γραφεί ως γινόμενο $U_1 \times U_2$ δύο (κατ' ανάγκην μη κενών και διαφόρων τού $\mathbb{A}^1_{\mathbf{k}}$) ανοικτών υποσυνόλων U_1, U_2 τού $\mathbb{A}^1_{\mathbf{k}}$ (ως προς τη τοπολογία Zariski), διότι θα έπρεπε να ισχύει η ισότητα

$$C = \left(\mathbb{A}^1_{\mathbf{k}} \times \mathbb{A}^1_{\mathbf{k}}\right) \smallsetminus (U_1 \times U_2) = \left(\left(\mathbb{A}^1_{\mathbf{k}} \smallsetminus U_1\right) \times U_2\right) \cup \left(U_1 \times \left(\mathbb{A}^1_{\mathbf{k}} \smallsetminus U_2\right)\right).$$

Τούτο θα σήμαινε (κατά την άσκηση **A-1-8**) ότι τα $\mathbb{A}^1_{\mathbf{k}} \smallsetminus U_1$ και $\mathbb{A}^1_{\mathbf{k}} \smallsetminus U_2$ θα ήταν πεπερασμένα. Εάν λοιπόν είχαμε

$$\mathbb{A}^1_{\mathbf{k}} \smallsetminus U_1 = \{a_1, \dots, a_k\}, \quad \mathbb{A}^1_{\mathbf{k}} \smallsetminus U_2 = \{b_1, \dots, b_l\}, \;\; k, l \in \mathbb{N},$$

τότε

$$C = \left(\mathbb{A}^1_{\mathbf{k}} \times \mathbb{A}^1_{\mathbf{k}}\right) \smallsetminus (U_1 \times U_2) = (\{a_1, \dots, a_k\} \times U_2) \cup (U_1 \times \{b_1, \dots, b_l\}),$$

οπότε

$$C = \{(a_i, F(a_j)) \mid F(a_j) \in U_2 \ , \ i,j \in \{1,\dots,k\}\} \cup \bigcap_{\nu=1}^{l} \left\{ (F(x), b_\nu) \;\middle|\; \begin{array}{c} F(x) - b_\nu = 0, \\ x \in U_1 \end{array} \right\},$$

κάτι που θα έδινε

$$\sharp(C) \leq k^2 + l \cdot \deg(F) < \infty$$

και θα αντέκειτο προς ό,τι αποδείχθηκε στην άσκηση **A-1-14.** Άρα το $\mathbb{A}^2_{\mathbf{k}} \smallsetminus C$ δεν μπορεί να είναι μέλος τής βάσεως τής συνήθους τοπολογίας γινομένου.

ii) Το $\mathbb{A}^2_{\mathbf{k}} \smallsetminus C$ δεν είναι ανοικτό ως προς τη συνήθη τοπολογία γινομένου, διότι δεν μπορεί να γραφεί ούτε ως ένωση

$$\mathbb{A}^2_{\mathbf{k}} \smallsetminus C = \bigcup_{\lambda \in \Lambda} U_1^{(\lambda)} \times U_2^{(\lambda)}$$

στοιχείων τής βάσεώς της. (Πράγματι· εάν συνέβαινε αυτό, τότε θα ίσχυε

$$\begin{aligned} C &= \bigcap_{\lambda \in \Lambda} \mathbb{A}^2_{\mathbf{k}} \smallsetminus \left(U_1^{(\lambda)} \times U_2^{(\lambda)} \right) \\ &= \bigcap_{\lambda \in \Lambda} \left(\{a_1^{(\lambda)}, \dots, a_k^{(\lambda)}\} \times U_2^{(\lambda)} \right) \cup \left(U_1^{(\lambda)} \times \{b_1^{(\lambda)}, \dots, b_l^{(\lambda)}\} \right), \end{aligned}$$

οπότε θα ξαναφθάναμε εκ νέου στην αντίφαση $\sharp(C) < \infty$ με επιχειρήματα ανάλογα εκείνων που χρησιμοποιήθηκαν στο i).) □

A-1-16. Η συνεπαγωγή «$\Longrightarrow$» είναι προφανής. Για να αποδείξουμε την ισχύ τής «$\Longleftarrow$» υποθέτουμε ότι $\mathbf{I}(V) = \mathbf{I}(W)$. Κατά την πρόταση 1.3.1 (5) (a),

$$\mathbf{I}(V) = \mathbf{I}(W) \Longrightarrow \mathbf{V}(\mathbf{I}(V)) = V = W = \mathbf{V}(\mathbf{I}(W)).$$

A-1-17. (a) Προφανώς,

$$P \notin V \Longrightarrow V \subsetneqq V \cup \{P\} \Longrightarrow \mathbf{I}(V \cup \{P\}) \subsetneqq \mathbf{I}(V) \Longrightarrow \exists F \in \mathbf{I}(V) : F(P) \neq 0$$

$$\Longrightarrow \exists F \in \mathbf{k}\,[\mathsf{X}_1, \dots, \mathsf{X}_n] : F(Q) = 0, \ \ \forall Q \in V, \quad \text{ενώ} \ \ F(P) = 1.$$

(Η παραδοχή $F(P) = 1$ γίνεται δίχως βλάβη τής γενικότητας. Εάν για το αρχικώς επιλεχθέν F έχουμε $F = c \in \mathbf{k} \smallsetminus \{0_{\mathbf{k}}\}$, τότε αντ' αυτού μπορούμε να χρησιμοποιήσουμε το $c^{-1}F$.)

(b) Έστω $\{P_1, \dots, P_\kappa\}$ ένα πεπερασμένο σύνολο σημείων εντός τού $\mathbb{A}^n_{\mathbf{k}}$ και έστω

$$V_i := \{P_1, \dots, P_\kappa\} \smallsetminus \{P_i\}, \ \ \forall i \in \{1, \dots, \kappa\}.$$

Το V_i είναι αλγεβρικό σύνολο εντός τού $\mathbb{A}^n_{\mathbf{k}}$ για κάθε $i \in \{1, \dots, \kappa\}$ (βλ. το (5) τής προτάσεως 1.2.3). Βάσει τού (a) υπάρχουν πολυώνυμα $F_1, \dots, F_\kappa \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, τέτοια ώστε

$$F_i(P_j) = 0, \ \text{για δείκτες } \ i \neq j, \quad \text{ενώ } \ F_i(P_i) = 1, \ \ i, j \in \{1, \dots, \kappa\}.$$

(c) Έστω V ένα αλγεβρικό σύνολο εντός τού $\mathbb{A}^n_{\mathbf{k}}$ και $P_1, P_2 \notin V$. Βάσει τού (a) υπάρχουν πολυώνυμα $F_1, F_2 \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, τέτοια ώστε $F_i \in \mathbf{I}(V)$ και $F_i(P_i) \neq 0$ για $i = 1, 2$. Εάν $F_1(P_2) \neq 0$, ορίζουμε ως F το F_1, εάν $F_2(P_1) \neq 0$, ορίζουμε ως F το F_2, ενώ εάν $F_1(P_2) = F_2(P_1) = 0$, ορίζουμε ως F το $F_1 + F_2$. Κατ' αυτόν τον τρόπο ορίζουμε ένα πολυώνυμο $F \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, τέτοιο ώστε

$$F(P_i) \neq 0, \ \text{για τους δείκτες } \ i \in \{1, 2\}, \ \text{ενώ } \ F \in \mathbf{I}(V).$$

A-1-18. Έστω I ένα ιδεώδες ενός δακτυλίου R. Εάν $a, b \in R$ με $a^n \in I$ και $b^m \in I$, για κάποιους $n, m \in \mathbb{N}$, τότε

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \tbinom{n+m}{k} a^k b^{n+m-k} \in I.$$

Το $\mathrm{Rad}(I)$ είναι ένα ιδεώδες τού R. Πράγματι· εάν $a, b \in \mathrm{Rad}(I)$ και $r \in R$, τότε $a^n \in I$ και $b^m \in I$, για κάποιους $n, m \in \mathbb{N}$, με

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} \tbinom{n+m}{k} a^k (-b)^{n+m-k} \in I \Longrightarrow a - b \in \mathrm{Rad}(I),$$

και $(ra)^n = r^n a^n \in I \Longrightarrow ra \in \mathrm{Rad}(I)$. Επίσης, το $\mathrm{Rad}(I)$ είναι ένα ριζικό ιδεώδες τού R, καθότι $\mathrm{Rad}(I) \subseteq \mathrm{Rad}(\mathrm{Rad}(I))$ και για $a \in \mathrm{Rad}(\mathrm{Rad}(I))$

$$\exists n \in \mathbb{N} : a^n \in \mathrm{Rad}(I) \Longrightarrow \exists m \in \mathbb{N} : (a^n)^m = a^{nm} \in I \Longrightarrow a \in \mathrm{Rad}(I),$$

οπότε $\mathrm{Rad}(\mathrm{Rad}(I)) \subseteq \mathrm{Rad}(I)$. Τέλος, κάθε πρώτο ιδεώδες τού R είναι ριζικό. Πράγματι· εάν το J είναι τυχόν πρώτο ιδεώδες τού δακτυλίου R, τότε (προφανώς) $J \subseteq \mathrm{Rad}(J)$, και εάν $a \in \mathrm{Rad}(J)$, τότε $\exists n \in \mathbb{N} : a^n \in J \Longrightarrow a \in J$ (επειδή το J είναι πρώτο ιδεώδες). Άρα $\mathrm{Rad}(J) \subseteq J$. □

A-1-19. Έστω $I := \langle \mathsf{X}^2 + 1 \rangle \subset \mathbb{R}[\mathsf{X}]$. Θεωρούμε τον επιμορφισμό δακτυλίων

$$f : \mathbb{R}[\mathsf{X}] \longrightarrow \mathbb{C}, \quad f(F) := F(i), \forall F \in \mathbb{R}[\mathsf{X}].$$

Κατά το 1ο θεώρημα ισομορφισμών δακτυλίων (βλ. θεώρημα 1.1.10), ο επιμορφισμός δακτυλίων

$$\varphi : \mathbb{R}[\mathsf{X}]/\ \mathrm{Ker}(f) \longrightarrow \mathbb{C}, \quad \varphi(F + \mathrm{Ker}(f)) := f(F), \forall F \in \mathbb{R}[\mathsf{X}],$$

είναι ισομορφισμός, όπου $\mathrm{Ker}(f) = \{F \in \mathbb{R}[\mathsf{X}] \mid F(i) = 0\}$. Προφανώς, $I \subseteq \mathrm{Ker}(f)$. Έστω τώρα τυχόν $F \in \mathrm{Ker}(f)$. Επειδή $F(i) = 0$, είναι γνωστό ότι ισχύει $F(-i) = 0$. Κατά το (b) τής προτάσεως 1.1.25,

$$\mathsf{X} - i \mid F,\ \mathsf{X} + i \mid F \Longrightarrow (\mathsf{X} - i)(\mathsf{X} + i) = \mathsf{X}^2 + 1 \mid F \Longrightarrow \mathrm{Ker}(f) \subseteq I.$$

Άρα $\mathrm{Ker}(f) = I$. Επειδή το $\mathbb{C}$ είναι σώμα, το I είναι μεγιστοτικό και κατ' επέκταση πρώτο και ριζικό ιδεώδες (βλ. θεώρημα 1.1.14, θεώρημα 1.1.7 και άσκηση **A-1-18**). Ωστόσο, το I δεν είναι το ιδεώδες κανενός συνόλου εντός τού $\mathbb{A}^1_{\mathbb{R}}$. Πράγματι· υποθέτοντας την ύπαρξη ενός $V \subseteq \mathbb{A}^1_{\mathbb{R}}$ με $I = \mathbf{I}(V)$ διακρίνουμε δύο περιπτώσεις:

(i) Εάν το V είναι απειροπληθές, τότε $\mathbf{I}(V) = \{0\} \neq I$.

(ii) Εάν το V είναι πεπερασμένο, ας πούμε ίσο με $\{a_1, \ldots, a_k\}$, τότε, επειδή

$$\mathbf{I}(V) = \langle (\mathsf{X} - a_1) \cdots (\mathsf{X} - a_k) \rangle$$

(βλ. πόρισμα 1.1.26) και το $\mathbf{I}(V)$ είναι πρώτο, το πολυώνυμο $(\mathsf{X} - a_1) \cdots (\mathsf{X} - a_k)$ οφείλει να είναι ανάγωγο, οπότε κατ' ανάγκην έχουμε $k = 1$. Τούτο μάς οδηγεί σε άτοπο, διότι θα έπρεπε να ισχύει

$$I = \langle \mathsf{X} - a_1 \rangle = \left\langle \mathsf{X}^2 + 1 \right\rangle,$$

αλλά προφανώς $\mathsf{X}^2 + 1 \nmid \mathsf{X} - a_1$ για κάθε $a_1 \in \mathbb{R}$. □

A-1-20. Έστω I ένα ιδεώδες τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Τότε ισχύουν τα εξής:

(a) $\mathbf{V}(I) = \mathbf{V}(\mathrm{Rad}(I))$. Πράγματι· επειδή $I \subseteq \mathrm{Rad}(I)$ έχουμε $\mathbf{V}(I) \supseteq \mathbf{V}(\mathrm{Rad}(I))$ (βλ. (3) τής προτάσεως 1.2.3). Επίσης, για οιοδήποτε $P \in \mathbf{V}(I)$ και οιοδήποτε $F \in \mathrm{Rad}(I)$,

$$\exists n \in \mathbb{N} : F^n \in I \Longrightarrow F^n(P) = (F(P))^n = 0 \Longrightarrow F(P) = 0 \Longrightarrow P \in \mathbf{V}(\mathrm{Rad}(I)).$$

(b) $\mathrm{Rad}(I) \subseteq \mathbf{I}(\mathbf{V}(I))$. Εάν $F \in \mathrm{Rad}(I)$ και $P \in \mathbf{V}(I)$, τότε

$$\exists n \in \mathbb{N} : F^n \in I \Longrightarrow F^n(P) = (F(P))^n = 0 \Longrightarrow F(P) = 0 \Longrightarrow F \in \mathbf{I}(\mathbf{V}(I)).$$

A-1-21. Εάν $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbf{k}}$ και

$$I := \langle \mathsf{X}_1 - a_1, \ldots, \mathsf{X}_n - a_n \rangle \subset \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$$

θα δείξουμε ότι το I είναι μεγιστοτικό. Ορίζουμε τον ομομορφισμό δακτυλίων

$$\varphi_{(a_1,\ldots,a_n)} : \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \longrightarrow \mathbf{k},\ \ F \longmapsto F(a_1, \ldots, a_n).$$

Παρατηρούμε ότι ο $\varphi_{(a_1,\ldots,a_n)}$ είναι επιμορφισμός. (Για κάθε $\lambda \in \mathbf{k}$, υπάρχει ένα πολυώνυμο, π.χ. το $F_\lambda := \sum_{i=1}^n (\mathsf{X}_i - a_i) - \lambda$, για το οποίο ισχύει $\varphi_{(a_1,\ldots,a_n)}(F_\lambda) = \lambda$).

Χρησιμοποιώντας το 1ο θεώρημα ισομορφισμών δακτυλίων (βλ. θεώρημα 1.1.10) σχηματίζουμε έναν ισομορφισμό

$$\overline{\varphi}_{(a_1,\dots,a_n)} : \mathbf{k}[\mathsf{X}_1,\dots,\mathsf{X}_n] \,/\, \mathrm{Ker}(\varphi_{(a_1,\dots,a_n)}) \xrightarrow{\cong} \mathbf{k}.$$

Αρκεί να δειχθεί ότι ισχύει $\mathrm{Ker}(\varphi_{(a_1,\dots,a_n)}) = I$ (διότι ο ανωτέρω πηλικοδακτύλιος είναι σώμα, βλ. θεώρημα 1.1.14). Ο εγκλεισμός

$$\langle \mathsf{X}_1 - a_1,\dots,\mathsf{X}_n - a_n\rangle \subseteq \mathrm{Ker}(\varphi_{(a_1,\dots,a_n)}) = \{F \in \mathbf{k}[\mathsf{X}_1,\dots,\mathsf{X}_n] \mid F(a_1,\dots,a_n) = 0\}$$

είναι προφανής. Ο αντίστροφος εγκλεισμός "$\supseteq$" έπεται από την άσκηση **A-1-7** (b). Τέλος, είναι εύκολο να αποδειχθεί ότι ο φυσικός ομομορφισμός από το σώμα $\mathbf{k}$ στον $\mathbf{k}[\mathsf{X}_1,\dots,\mathsf{X}_n] \,/\, I$ ο δημιουργούμενος από τη σύνθεση

$$\mathbf{k} \hookrightarrow \mathbf{k}[\mathsf{X}_1,\dots,\mathsf{X}_n] \twoheadrightarrow \mathbf{k}[\mathsf{X}_1,\dots,\mathsf{X}_n] \,/\, I$$

είναι ένας ισομορφισμός, καθότι ισούται με τον $\overline{\varphi}^{-1}_{(a_1,\dots,a_n)}$. □

A-1-22. ► *Απόδειξη προτάσεως 1.4.3*: (a) Επειδή έχουμε $\langle a\rangle = Ra$ και $\langle b\rangle = Rb$, τούτο έπεται άμεσα από το (a) τής σημειώσεως 1.4.2.

(b) Προφανώς,

$$\begin{aligned}
\langle a\rangle\,\langle b\rangle &= \left\{ \sum_{j=1}^{k} (r_j a)\,(s_j b) \;\middle|\; r_1,\dots,r_k,s_1,\dots,s_k \in R,\ k\in\mathbb{N} \right\} \\
&= \left\{ \left(\sum_{j=1}^{k} r_j s_j \right) ab \;\middle|\; r_1,\dots,r_k,s_1,\dots,s_k \in R,\ k\in\mathbb{N} \right\} \\
&= Rab,
\end{aligned}$$

όπου $Rab = \langle ab\rangle$. □

► *Απόδειξη προτάσεως 1.4.4*: (a) Έστω τυχόν $a \in (I_1 + I_2) + I_3$. Το a γράφεται ως άθροισμα $c + a_3$, όπου $c \in I_1 + I_2$ και $a_3 \in I_3$, και το $c = a_1 + a_2$, όπου $a_1 \in I_1$ και $a_2 \in I_2$. Επομένως, λόγω τής προσεταιριστικής ιδιότητας τής προσθέσεως,

$$a = (a_1 + a_2) + a_3 = a_1 + (a_2 + a_3) \in I_1 + (I_2 + I_3)\,,$$

ήτοι $(I_1 + I_2) + I_3 \subseteq I_1 + (I_2 + I_3)$. Και αντιστρόφως· εάν $b \in I_1 + (I_2 + I_3)$, τότε το b γράφεται ως άθροισμα $b_1 + d$, όπου $b_1 \in I_1$ και $d \in I_2 + I_3$, και το $d = b_2 + b_3$, όπου $b_2 \in I_2$ και $b_3 \in I_3$. Επομένως, και πάλι λόγω τής προσεταιριστικής ιδιότητας τής προσθέσεως,

$$b = b_1 + (b_2 + b_3) = (b_1 + b_2) + b_3 \in (I_1 + I_2) + I_3.$$

Κατά συνέπειαν, $(I_1 + I_2) + I_3 = I_1 + (I_2 + I_3)$.
(b) Έστω τυχόν $x \in (I_1\, I_2)\; I_3$. Τότε

$$x = \sum_{j=1}^{k} x_j c_j, \quad \text{όπου } k \in \mathbb{N},\ \ x_j \in I_1\, I_2,\ \ c_j \in I_3,\ \ \forall j \in \{1, \ldots, k\}.$$

Παρομοίως, για κάθε $j \in \{1, \ldots, k\}$,

$$x_j = \sum_{l=1}^{s_j} a_{jl} b_{jl}, \quad \text{όπου } s_j \in \mathbb{N},\ \ a_{jl} \in I_1,\ \ b_{jl} \in I_2,\ \ \forall l \in \{1, \ldots, s_j\}.$$

Επομένως, λόγω τής επιμεριστικής ιδιότητας,

$$x = \sum_{j=1}^{k} \left(\sum_{l=1}^{s_j} a_{jl} b_{jl} \right) c_j = \sum_{j=1}^{k} \sum_{l=1}^{s_j} a_{jl} (b_{jl} c_j) \in I_1\ (I_2\, I_3) \Longrightarrow (I_1\, I_2)\ I_3 \subseteq I_1\ (I_2\, I_3)\,.$$

Αναλόγως αποδεικνύεται και η εγκλειστική σχέση $I_1\ (I_2\, I_3) \subseteq (I_1\, I_2)\ I_3$.
(c) Έστω τυχόν $x \in I_1\ (I_2 + I_3)$. Τότε

$$x = \sum_{j=1}^{k} a_j\,(b_j + c_j)\,, \quad \text{όπου } k \in \mathbb{N},\ a_j \in I_1,\ b_j \in\ I_2,\ c_j \in I_3,\ \ \forall j \in \{1, \ldots, k\},$$

οπότε, λόγω τής επιμεριστικής ιδιότητας,

$$x = \underbrace{\sum_{j=1}^{k} a_j b_j}_{\in I_1\, I_2} + \underbrace{\sum_{j=1}^{k} a_j c_j}_{\in I_1\, I_3},$$

απ' όπου έπεται ότι $I_1\ (I_2 + I_3) \subseteq (I_1\, I_2) + (I_1\, I_3)$. Αναλόγως αποδεικνύεται και η αντίστροφη εγκλειστική σχέση, καθώς και η $(I_1 + I_2)\ I_3' = (I_1\, I_3') + (I_1\, I_3')$. □

► *Απόδειξη προτάσεως 1.4.5* : (a) Εάν $x \in I_1\, I_2$, τότε

$$x = \sum_{j=1}^{k} a_j b_j, \quad \text{όπου } k \in \mathbb{N},\ \ a_j \in I_1,\ \ b_j \in I_2,\ \ \forall j \in \{1, \ldots, k\}.$$

Όμως, από τον ορισμό τού ιδεώδους,

$$\left.\begin{array}{l} (a_j \in I_1 \subseteq R) \Longrightarrow (a_j b_j \in I_2) \Longrightarrow x \in I_2 \\ (b_j \in I_2 \subseteq R) \Longrightarrow (a_j b_j \in I_1) \Longrightarrow x \in I_1 \end{array}\right\} \Longrightarrow x \in I_1 \cap I_2.$$

(b) Έστω τυχόν $x \in (I_1 + I_2)\ (I_1 + I_3)$. Τότε

$$x = \sum_{j=1}^{k} y_j z_j, \quad \text{όπου } k \in \mathbb{N},\ \ y_j \in I_1 + I_2,\ \ z_j \in I_1 + I_3,\ \ \forall j \in \{1, \ldots, k\},$$

οπότε, λόγω τής επιμεριστικής ιδιότητας και τού ότι

$$y_j = a_j + b_j, \quad z_j = c_j + d_j,$$

για κάποια $a_j \in I_1, b_j \in I_2, c_j \in I_1, d_j \in I_3$, $\forall j \in \{1, \ldots, k\}$, έχουμε

$$x = \left(\underbrace{\sum_{j=1}^{k} (a_j c_j + a_j d_j + b_j c_j)}_{\in I_1} + \underbrace{\sum_{j=1}^{k} b_j d_j}_{\in I_2\, I_3} \right) \in I_1 + I_2\, I_3,$$

δηλαδή $(I_1 + I_2)\ (I_1 + I_3) \subseteq I_1 + I_2\, I_3$. Η δεύτερη εγκλειστική σχέση έπεται άμεσα από το (a). □

► *Απόδειξη προτάσεως 1.4.11* : (a) Έστω τυχόν στοιχείο $r \in (I_1 : I_3) + (I_2 : I_3)$. Τότε $r = r_1 + r_2$, όπου $r_1 \in (I_1 : I_3)$ και $r_2 \in (I_2 : I_3)$. Ως εκ τούτου,

$$\left.\begin{array}{l} r_1 I_3 \subseteq I_1 \\ r_2 I_3 \subseteq I_2 \end{array}\right\} \Longrightarrow (r_1 + r_2)\, I_3 \subseteq I_1 + I_2,$$

απ' όπου συνάγεται ότι $r \in (I_1 + I_2) : I_3$, οπότε $(I_1 : I_3) + (I_2 : I_3) \subseteq (I_1 + I_2) : I_3$.
(b) Έστω τυχόν $r \in I_1 : (I_2 + I_3)$. Τότε $ra \in I_1,\ \forall a \in I_2 + I_3$. Επομένως, λαμβάνοντας υπ' όψιν ότι $I_2 \subseteq I_2 + I_3$ και $I_3 \subseteq I_2 + I_3$, συνάγουμε ότι

$$\left.\begin{array}{l} ra \in I_1,\ \ \forall a \in I_2\ (\subseteq I_2 + I_3) \\ ra \in I_1,\ \ \forall a \in I_3\ (\subseteq I_2 + I_3) \end{array}\right\} \Longrightarrow \left.\begin{array}{l} r \in (I_1 : I_2) \\ r \in (I_1 : I_3) \end{array}\right\} \Longrightarrow r \in (I_1 : I_2) \cap (I_1 : I_3)\,.$$

Άρα $I_1 : (I_2 + I_3) \subseteq (I_1 : I_2) \cap (I_1 : I_3)$. Και αντιστρόφως· εάν

$$r \in (I_1 : I_2) \cap (I_1 : I_3) \Longrightarrow rI_2 \subseteq I_1 \ \text{ και } \ rI_3 \subseteq I_1,$$

οπότε

$$rI_2 + rI_3 = r\,(I_2 + I_3) \subseteq I_1 + I_1 = I_1 \Longrightarrow r \in I_1 : (I_2 + I_3)\,.$$

Εν συνεχεία υποθέτουμε ότι $r \in (I_1 \cap I_2) : I_3$, δηλαδή ότι ισχύει η εγκλειστική σχέση $rI_3 \subseteq I_1 \cap I_2$. Επειδή $I_1 \cap I_2 \subseteq I_1$ και $I_1 \cap I_2 \subseteq I_2$, έχουμε $rI_3 \subseteq I_1$ και $rI_3 \subseteq I_2$, δηλαδή $r \in (I_1 : I_3) \cap (I_2 : I_3)$. Και αντιστρόφως· εάν $r \in (I_1 : I_3) \cap (I_2 : I_3)$, τότε $rI_3 \subseteq I_1$ και $rI_3 \subseteq I_2$, οπότε $rI_3 \subseteq I_1 \cap I_2 \Longrightarrow r \in (I_1 \cap I_2) : I_3$.
(c) Έστω τυχόν $r \in (I_1 : I_2)\ I_2$. Τότε

$$r = \sum_{j=1}^{k} a_j b_j, \quad \text{όπου } k \in \mathbb{N},\ \ a_j \in (I_1 : I_2)\,,\ \ b_j \in I_2,\ \ \forall j \in \{1, \ldots, k\},$$

οπότε

$$\left[\begin{array}{r} a_j I_2 \subseteq I_1 \\ b_j \in I_2 \end{array}\right\} \Longrightarrow a_j b_j \in I_1,\ \forall j \in \{1,\dots,k\} \Longrightarrow r \in I_1 \Bigg] \Longrightarrow (I_1 : I_2)\ I_2 \subseteq I_1.$$

Εν συνεχεία υποθέτουμε ότι $r \in I_1$. Προφανώς, $ra \in I_1\, I_2,\ \forall a \in I_2$. Αυτό σημαίνει αυτομάτως ότι $r \in ((I_1\, I_2) : I_2)$, οπότε ισχύει και η εγκλειστική σχέση $I_1 \subseteq ((I_1\, I_2) : I_2)$.
(d) Έστω τυχόν $r \in (I_1 : I_2) : I_3$. Τότε $ra \in I_1 : I_2,\ \forall a \in I_3$, οπότε

$$[(ra)\, b = (rb)\, a \in I_1,\ \forall a \in I_3,\ \forall b \in I_2] \Longrightarrow [rb \in I_1 : I_3,\ \forall b \in I_2] \Longrightarrow r \in (I_1 : I_3) : I_2.$$

Άρα $(I_1 : I_2) : I_3 \subseteq (I_1 : I_3) : I_2$. Και αντιστρόφως· εάν $r \in (I_1 : I_3) : I_2$, τότε $ra \in I_1 : I_3$, για κάθε $a \in I_2$, οπότε

$$[(ra)\, b = (rb)\, a \in I_1,\ \forall a \in I_2,\ \forall b \in I_3] \Longrightarrow [rb \in I_1 : I_2,\ \forall b \in I_3] \Longrightarrow r \in (I_1 : I_2) : I_3,$$

απ' όπου έπεται ότι $(I_1 : I_3) : I_2 \subseteq (I_1 : I_2) : I_3$. Άρα $(I_1 : I_2) : I_3 = (I_1 : I_3) : I_2$. Υπολείπεται να δείξουμε την ισότητα $J_1 = J_2$, όπου

$$J_1 = I_1 : (I_2\, I_3), \quad J_2 = (I_1 : I_2) : I_3.$$

Μέσω τού ορισμού τού πηλίκου ιδεωδών και τής μεταθετικότητας τού δακτυλίου αναφοράς μας λαμβάνουμε

$$\left.\begin{array}{r} J_1\,(I_2\, I_3) \subseteq I_1 \\ J_2 I_3 \subseteq I_1 : I_2 \end{array}\right\} \Longrightarrow \left.\begin{array}{r} (J_1 I_3)\ I_2 \subseteq I_1 \\ (J_2 I_3)\, I_2 \subseteq I_1 \end{array}\right\} \Longrightarrow \left.\begin{array}{r} J_1 I_3 \subseteq I_1 : I_2 \\ J_2\,(I_2 I_3) \subseteq I_1 \end{array}\right\} \Longrightarrow \left.\begin{array}{r} J_1 \subseteq J_2 \\ J_2 \subseteq J_1 \end{array}\right\},$$

οπότε όντως $J_1 = J_2$. □

A-1-23. ►*Απόδειξη πορίσματος 1.4.10*: (a) Έστω τυχόν $a \in \langle m\rangle \cap \langle n\rangle$. Τότε $a \in \langle m\rangle$ και $a \in \langle n\rangle$, οπότε $a = \lambda m = \kappa m$, για κάποιους $\lambda, \kappa \in \mathbb{Z}$. Έστω $d := \text{μκδ}(m,n)$. Προφανώς,

$$\lambda\left(\frac{m}{d}\right) d = \kappa\left(\frac{n}{d}\right) d \Longrightarrow \lambda\left(\frac{m}{d}\right) = \kappa\left(\frac{n}{d}\right) \Longrightarrow \frac{n}{d}\Big|\, \lambda\left(\frac{m}{d}\right),$$

κι επειδή $\text{μκδ}\left(\frac{m}{d}, \frac{n}{d}\right) = 1$, έχουμε

$$\frac{n}{d}\Big|\, \lambda \Longrightarrow \lambda = \nu\, \frac{n}{d},$$

για κάποιον $\nu \in \mathbb{Z}$. Κατά συνέπειαν,

$$a = \lambda m = \nu\, \frac{n}{d}\, m = \left(\frac{mn}{d}\right) \nu = \text{sgn}\,(mn)\ \text{εκπ}\,(m,n)\ \nu \Longrightarrow a \in \langle \text{εκπ}(m,n)\rangle\,,$$

ήτοι $\langle m\rangle \cap \langle n\rangle \subseteq \langle \text{εκπ}(m,n)\rangle$. Και αντιστρόφως· εάν $a \in \langle \text{εκπ}(m,n)\rangle$, τότε ισχύει η ισότητα $a = \mu\, \text{εκπ}(m,n)$, για κάποιον $\mu \in \mathbb{Z}$, οπότε

$$a = \mu\, \frac{|m|\ |n|}{\text{μκδ}(m,n)} = m\left(\frac{\mu\, \text{sgn}\,(m)\ |n|}{\text{μκδ}(m,n)}\right) = n\left(\frac{\mu\, \text{sgn}\,(n)\ |m|}{\text{μκδ}(m,n)}\right),$$

όπου $\frac{\mu\,\mathrm{sgn}(m)\,|n|}{\mu\kappa\delta(m,n)} \in \mathbb{Z}$ και $\frac{\mu\,\mathrm{sgn}(n)\,|m|}{\mu\kappa\delta(m,n)} \in \mathbb{Z}$. Συνεπώς έχουμε $a \in \langle m\rangle \cap \langle n\rangle$, οπότε ισχύει και ο εγκλεισμός $\langle \epsilon\kappa\pi(m,n)\rangle \subseteq \langle m\rangle \cap \langle n\rangle$.

(b) Κατά την πρόταση 1.4.3 (a), $\langle m\rangle + \langle n\rangle = \{\, xm + yn \mid\ x, y \in \mathbb{Z}\}$. Επειδή ο μέγιστος κοινός διαιρέτης των m και n γράφεται ως ακέραιος γραμμικός συνδυασμός των m και n, έχουμε

$$\mu\kappa\delta(m,n) \in (\langle m\rangle + \langle n\rangle) \Longrightarrow \langle \mu\kappa\delta(m,n)\rangle \subseteq \langle m\rangle + \langle n\rangle\,.$$

Και αντιστρόφως· εάν $d := \mu\kappa\delta(m,n)$ και $a \in \langle m\rangle + \langle n\rangle$, τότε

$$(a = \kappa m + \lambda n, \quad \kappa, \lambda \in \mathbb{Z}) \Longrightarrow a = \left(\frac{\kappa m}{d} + \frac{\lambda n}{d}\right) d,$$

όπου $\frac{\kappa m}{d} + \frac{\lambda n}{d} \in \mathbb{Z}$, οπότε $a \in \langle \mu\kappa\delta(m,n)\rangle$. Τούτο σημαίνει ότι $\langle m\rangle + \langle n\rangle \subseteq \langle d\rangle$.

(c) Προφανές επί τη βάσει τής προτάσεως 1.4.3 (b).

(d) Ας υποθέσουμε ότι $r \in \langle m\rangle : \langle n\rangle$. Τότε -εξ ορισμού- $ra \in \langle m\rangle$ για κάθε $a \in \langle n\rangle$. Ιδιαιτέρως,

$$rn \in \langle m\rangle \Longrightarrow [\exists b \in \mathbb{Z} : rn = bm]\,.$$

Εάν $d := \mu\kappa\delta(m,n)$, τότε $\mu\kappa\delta\big(\frac{m}{d}, \frac{n}{d}\big) = 1$, οπότε

$$r\,\frac{n}{d} = b\,\frac{m}{d} \Longrightarrow \frac{n}{d}\Big|\, b\frac{m}{d} \Longrightarrow \frac{n}{d}\Big|\, b \Longrightarrow b = c\frac{n}{d},$$

για κάποιον $c \in \mathbb{Z}$. Άρα

$$r\,\frac{n}{d} = c\,\frac{n}{d}\frac{m}{d} \Longrightarrow r = c\,\frac{m}{d} = c\,\frac{m}{\mu\kappa\delta(m,n)} \Longrightarrow r \in \left\langle \frac{m}{\mu\kappa\delta(m,n)} \right\rangle,$$

ήτοι $\langle m\rangle : \langle n\rangle \subseteq \left\langle \frac{m}{\mu\kappa\delta(m,n)} \right\rangle$. Και αντιστρόφως· εάν $s \in \left\langle \frac{m}{\mu\kappa\delta(m,n)} \right\rangle$, τότε $s = \kappa\frac{m}{d}$, όπου $\kappa \in \mathbb{Z}$ και $d := \mu\kappa\delta(m,n)$, οπότε για *κάθε* στοιχείο λn τού $\langle n\rangle$ ($\lambda \in \mathbb{Z}$), έχουμε

$$s\lambda n = \left(\kappa\frac{m}{d}\right)\lambda n = \left(\kappa\lambda\frac{n}{d}\right) m \in \langle m\rangle \Longrightarrow s \in \langle m\rangle : \langle n\rangle\,,$$

ήτοι $\left\langle \frac{m}{\mu\kappa\delta(m,n)} \right\rangle \subseteq \langle m\rangle : \langle n\rangle$. □

A-1-24. Επειδή για οιαδήποτε ιδεώδη I, J τού R έχουμε $IJ = JI$, εργαζόμαστε επαγωγικώς επί τού κ:

$$\begin{aligned}(I_1 \cdots I_n)^{\kappa+1} &= (I_1 \cdots I_n)^{\kappa} I_1 \cdots I_n \\ &= I_1^{\kappa} \cdots I_n^{\kappa} \cdot I_1 \cdots I_n = I_1^{\kappa+1} \cdots I_n^{\kappa+1}.\end{aligned}$$

(Για $\kappa = 1$ ο ισχυρισμός είναι προφανώς αληθής.) □

A-1-25. Έστω ότι τα I, J είναι δυο ιδεώδη ενός δακτυλίου R. Εάν τα I, J είναι μεταξύ τους πρώτα, τότε, σύμφωνα με το (c) τής προτάσεως 1.4.4, έχουμε

$$R = R^2 = (I + J)(I + J) = I^2 + IJ + J^2 = I(I + J) + J^2 = I + J^2.$$

Ακολουθώντας τήν ίδια συλλογιστική (για τους εκθέτες τού J) αποδεικνύουμε επαγωγικώς ότι

$$I + J^n = R, \ \forall n \in \mathbb{N}.$$

Εν συνεχεία, εναλλάσσοντας τους ρόλους των I και J^n αποδεικνύουμε επαγωγικώς ότι

$$I^m + J^n = R$$

για οιουσδήποτε $m, n \in \mathbb{N}$. □

A-1-26. Εάν τα I, J είναι δυο ιδεώδη τού R, τα οποία είναι πρώτα μεταξύ τους, τότε, σύμφωνα με τις ασκήσεις **A-1-24**, **A-1-25** και το (a) τού λήμματος 1.4.7, έχουμε

$$I + J = R \Rightarrow I^\kappa + J^\kappa = R \Rightarrow I^\kappa \cap J^\kappa = I^\kappa J^\kappa = (IJ)^\kappa = (I \cap J)^\kappa,$$

για κάθε $\kappa \in \mathbb{N}$. Έστω n ένας φυσικός αριθμός ≥ 2. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη τού R και εάν τα ιδεώδη I_i και $J_i := \bigcap \{ I_j | \, j \in \{1, \ldots, n\} \setminus \{i\} \}$ είναι πρώτα μεταξύ τους, τότε, κάνοντας χρήση των ανωτέρω ισοτήτων και επαγωγής επί τού n, λαμβάνουμε

$$\begin{aligned} I_1^\kappa \cap \cdots \cap I_n^\kappa &= \left(I_1^\kappa \cap \cdots \cap I_{n-1}^\kappa\right) \cap I_n^\kappa \\ &= (I_1 \cdots I_{n-1})^\kappa \cap I_n^\kappa \\ &= (I_1 \cdots I_{n-1})^\kappa \cdot I_n^\kappa \\ &= (I_1 \cdots I_n)^\kappa \end{aligned}$$

και

$$\begin{aligned} (I_1 \cap \cdots \cap I_n)^\kappa &= ((I_1 \cap \cdots \cap I_{n-1}) \cap I_n)^\kappa \\ &= (J_n \cap I_n)^k = (J_n \cdot I_n)^k = J_n^\kappa \cdot {I_n}^k \\ &= (I_1 \cap \cdots \cap I_{n-1})^\kappa \cdot {I_n}^k \\ &= (I_1 \cdots I_{n-1})^\kappa \cdot I_n^\kappa \\ &= (I_1 \cdots I_n)^\kappa, \end{aligned}$$

αντιστοίχως. □

A-1-27. (a) Εξ υποθέσεως, $I_1 \subseteq I_2$. Έστω τυχόν $r \in I_1 : I_3$. Τότε

$$ra \in I_1,\ \forall a \in I_3 \Rightarrow ra \in I_2,\ \forall a \in I_3 \Rightarrow r \in I_2 : I_3.$$

Άρα $I_1 : I_3 \subseteq I_2 : I_3$. Έστω τώρα τυχόν $r \in I_3 : I_2$. Προφανώς, $ra \in I_3,\ \forall a \in I_2$. Εάν $b \in I_1$, τότε

$$b \in I_2,\ rb \in I_3 \Rightarrow r \in I_3 : I_1.$$

Κατά συνέπειαν, $I_3 : I_1 \supseteq I_3 : I_2$.
(b) Προφανώς,

$$I_1 : I_2 = R \Leftrightarrow 1_R \in I_1 : I_2 \Leftrightarrow 1_R \cdot a \in I_1,\ \forall a \in I_2 \Leftrightarrow I_2 \subseteq I_1.$$

(c) Εφαρμόζοντας το (d) τής προτάσεως 1.4.11 λαμβάνουμε για κάθε $n \in \mathbb{N}$

$$I_1 : I_2^{n+1} = I_1 : (I_2 \cdot I_2^n) = (I_1 : I_2^n) : I_2 = (I_1 : I_2) : I_2^n.$$

(d) Εφαρμόζοντας το (d) τής προτάσεως 1.4.11 λαμβάνουμε

$$I_1 : (I_1 + I_2) = (I_1 : I_1) \cap (I_1 : I_2) = R \cap (I_1 : I_2) = I_1 : I_2.$$

Τούτο αποπερατώνει τις αποδείξεις μας. □

A-1-28. (a) Υποθέτοντας ότι $I^n \subseteq J$, για κάποιον $n \in \mathbb{N}$, και θεωρώντας τυχόν στοιχείο $r \in \mathrm{Rad}(I)$ συμπεραίνουμε ότι

$$\exists m \in \mathbb{N} : r^m \in I \Rightarrow (r^m)^n \in I^n \Rightarrow r^{mn} \in J \Rightarrow r \in \mathrm{Rad}\,(J)\,,$$

οπότε $\mathrm{Rad}(I) \subseteq \mathrm{Rad}(J)$.
(b) Το ότι $\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I)$ έχει ήδη αποδειχθεί στην άσκηση **A-1-18**.
(c) Προφανώς,

$$I^k \subseteq I,\ \forall k \in \mathbb{N} \Rightarrow \mathrm{Rad}\left(I^k\right) \subseteq \mathrm{Rad}\,(I)\,, \forall k \in \mathbb{N}.$$

Από την άλλη μεριά, λόγω τού (a),

$$I^{k+1} \subseteq I^k,\ \forall k \in \mathbb{N} \Rightarrow \mathrm{Rad}\,(I) \subseteq \mathrm{Rad}\left(I^k\right), \forall k \in \mathbb{N}.$$

Άρα τελικώς $\mathrm{Rad}\left(I^k\right) = \mathrm{Rad}(I)\,, \forall k \in \mathbb{N}$.
(d) Προφανώς, $\mathrm{Rad}(I) + \mathrm{Rad}(J) \subseteq \mathrm{Rad}(\mathrm{Rad}(I) + \mathrm{Rad}(J))$. Επίσης,

$$\left.\begin{array}{l} I \subseteq \mathrm{Rad}(I) \\ J \subseteq \mathrm{Rad}(J) \end{array}\right\},\ I + J \subseteq \mathrm{Rad}(I + J) \Rightarrow \mathrm{Rad}\,(I + J) \subseteq \mathrm{Rad}(\mathrm{Rad}\,(I) + \mathrm{Rad}\,(J)).$$

Έστω τυχόν $r \in \mathrm{Rad}(I) + \mathrm{Rad}(J)$. Τότε $r = y + z$, όπου $y \in \mathrm{Rad}(I)$ και $z \in \mathrm{Rad}(J)$, οπότε

$$\exists m, \kappa \in \mathbb{N} : y^m \in I,\ z^\kappa \in J$$

$$\begin{aligned} \Rightarrow \quad & r^{m+\kappa} = (y+z)^{m+\kappa} = \sum_{j=0}^{m+\kappa} \tbinom{m+\kappa}{j} y^j z^{m+\kappa-j} \\ = \quad & z^\kappa \left(\sum_{j=0}^{m-1} \tbinom{m+\kappa}{j} y^j z^{m-j} \right) + y^m z^\kappa + y^m \left(\sum_{j=m+1}^{m+\kappa} \tbinom{m+\kappa}{j} y^{j-m} z^{m+\kappa-j} \right) \in I + J \end{aligned}$$

$$\Rightarrow r \in \mathrm{Rad}\,(I+J)\,.$$

Εξ αυτού έπεται ότι $\mathrm{Rad}(I) + \mathrm{Rad}(J) \subseteq \mathrm{Rad}(I+J)$ και κατ' επέκτασιν

$$\mathrm{Rad}(\mathrm{Rad}\,(I) + \mathrm{Rad}\,(J)) \subseteq \mathrm{Rad}(\mathrm{Rad}\,(I+J)) \overset{\text{(b)}}{=} \mathrm{Rad}\,(I+J)\,.$$

Άρα τελικώς $\mathrm{Rad}(I) + \mathrm{Rad}(J) \subseteq \mathrm{Rad}(\mathrm{Rad}(I) + \mathrm{Rad}(J)) = \mathrm{Rad}(I+J)$.

(e) Εάν $r \in \mathrm{Rad}(I \cap J)$, τότε $\exists m \in \mathbb{N} : r^m \in I \cap J$, οπότε $r^m \in I$ και $r^m \in J$, απ' όπου έπεται ότι $r \in \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$. Άρα $\mathrm{Rad}(I \cap J) \subseteq \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$. Και αντιστρόφως· εάν $r \in \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$, τότε

$$\exists m, \kappa \in \mathbb{N} : r^m \in I,\ r^\kappa \in J \Rightarrow r^{m+\kappa} = r^m r^\kappa \in I \cap J \Rightarrow r \in \mathrm{Rad}\,(I \cap J)\,.$$

Άρα

$$\mathrm{Rad}\,(I) \cap \mathrm{Rad}\,(J) \subseteq \mathrm{Rad}\,(I \cap J)\,.$$

Εν συνεχεία θεωρούμε εκ νέου τυχόν στοιχείο $r \in \mathrm{Rad}(I \cap J)$. Προφανώς,

$$\exists m \in \mathbb{N} : r^m \in I \cap J \Rightarrow r^{2m} = r^m r^m \in IJ \Rightarrow r \in \mathrm{Rad}\,(I\,J)\,.$$

Κατά συνέπειαν, $\mathrm{Rad}(I \cap J) \subseteq \mathrm{Rad}(I\,J)$. Και αντιστρόφως· κατά το (a) τής προτάσεως 1.4.5,

$$I\,J \subseteq I \cap J \Rightarrow \mathrm{Rad}\,(I\,J) \subseteq \mathrm{Rad}\,(I \cap J)\,.$$

Άρα τελικώς $\mathrm{Rad}(I) \cap \mathrm{Rad}(J) = \mathrm{Rad}(I \cap J) = \mathrm{Rad}(I\,J)$.

(f) Βάσει τού (a) τής προτάσεως 1.4.5,

$$\mathrm{Rad}\,(I)\ \mathrm{Rad}\,(J) \subseteq \mathrm{Rad}\,(I) \cap \mathrm{Rad}\,(J) \overset{\text{(e)}}{=} \mathrm{Rad}\,(I\,J)\,.$$

Επιπροσθέτως,

$$I\,J \subseteq \mathrm{Rad}\,(I)\ \mathrm{Rad}\,(J) \subseteq \mathrm{Rad}(\mathrm{Rad}\,(I)\ \mathrm{Rad}\,(J)).$$

Εξάλλου, $\text{Rad}(I)\,\text{Rad}(J) \subseteq \text{Rad}(I\,J)$, οπότε

$$\text{Rad}(\text{Rad}\,(I)\ \text{Rad}\,(J)) \subseteq\ \text{Rad}\,(\text{Rad}\,(I\,J)) \overset{\text{(b)}}{=} \text{Rad}\,(I\,J)\,.$$

Άρα τελικώς $\text{Rad}(I\,J) = \text{Rad}(\text{Rad}(I)\,\text{Rad}(J))$.
(g) Έστω τυχόν $r \in \text{Rad}(I\ :\ J)$. Τότε

$$\exists m \in \mathbb{N} : r^m \in \text{Rad}\,(I\ :\ J) \Rightarrow r^m a \in I,\ \forall a \in J.$$

Έστω *τυχόν* $b \in \text{Rad}(J)$. Τότε

$$\exists \kappa \in \mathbb{N} : b^\kappa \in J \Rightarrow r^m b^\kappa \in I,$$

οπότε

$$(rb)^{m+\kappa} = (r^m b^\kappa)\, r^\kappa b^m \in I \Rightarrow rb \in \text{Rad}\,(J)\,.$$

Αυτό σημαίνει ότι $r \in \text{Rad}(I)\ :\text{Rad}(J)$. Άρα $\text{Rad}(I)\ :\text{Rad}(J) \supseteq \text{Rad}(I\ :\ J)$.
(h) Εάν ο $\pi : R \longrightarrow R/I$ είναι ο φυσικός επιμορφισμός και $r \in \text{Rad}(I)$, τότε

$$\exists m \in \mathbb{N} : r^m \in I \Rightarrow \pi(r^m) = \pi(r)^m = 0_{R/I} \Rightarrow \pi(r) \in \text{Nil}(R/I) \Rightarrow r \in \pi^{-1}(\text{Nil}(R/I)).$$

Άρα $\text{Rad}(I)\ \subseteq \pi^{-1}(\text{Nil}(R/I))$. Και αντιστρόφως· εάν $r \in \pi^{-1}(\text{Nil}(R/I))$, τότε

$$\pi(r) \in \text{Nil}(R/I) \Rightarrow \exists m \in \mathbb{N} : \pi(r)^m = \pi(r^m) = 0_{R/I} \Rightarrow r^m \in I \Rightarrow r \in \text{Rad}\,(I)\,,$$

οπότε $\text{Rad}(I)\ \supseteq \pi^{-1}(\text{Nil}(R/I))$. □

A-1-29. Εξ υποθέσεως $\exists \kappa \in \mathbb{N}$ και $a_1, \ldots, a_\kappa \in R : I = \langle a_1, \ldots, a_\kappa \rangle$ και $I \subseteq \text{Rad}(J)$, οπότε

$$\exists m_j \in \mathbb{N} : a_j^{m_j} \in I,\ \ \forall j \in \{1, \ldots, \kappa\}.$$

Θέτουμε $n := m_1 + \cdots + m_\kappa$. Κατά το (d) τής σημειώσεως 1.4.2,

$$I^n = \left\langle \left\{ a_1^{i_1} a_2^{i_2} \cdots a_\kappa^{i_\kappa} \ \middle|\ (i_1, .., i_\kappa) \in \mathbb{N}_0^\kappa : i_1 + \cdots + i_\kappa = n \right\} \right\rangle.$$

Θα συμπεράνουμε ότι $I^n \subseteq J$ αποδεικνύοντας ότι *καθένας των γεννητόρων τού* I^n *ανήκει στο* J. Προς τούτο αρκεί να αποδειχθεί ότι σε *κάθε* γινόμενο

$$a_1^{i_1} a_2^{i_2} \cdots a_\kappa^{i_\kappa},\ i_1 + \cdots + i_\kappa = n,$$

κάποιος εκ των εκθετών i_j, $j \in \{1, \ldots, \kappa\}$, είναι $\geq m_j$ (διότι εν τοιαύτη περιπτώσει και ολόκληρο το γινόμενο $a_1^{i_1} a_2^{i_2} \cdots a_\kappa^{i_\kappa}$ θα ανήκει στο J, αφού το J είναι ιδεώδες τού

R). Υποθέτοντας την ύπαρξη ενός γεννήτορα $a_1^{i_1}a_2^{i_2}\cdots a_\kappa^{i_\kappa}$ τού I^n, για τον οποίο ισχύει $i_j < m_j$ *για κάθε* $j \in \{1,\dots,\kappa\}$, θα καταλήγαμε σε αντίφαση, καθόσον

$$i_1 + \cdots + i_\kappa < m_1 + \cdots + m_\kappa = n.$$

Άρα πράγματι $I^n \subseteq J$. □

A-1-30. (a) Εάν $s \in I_1^{\text{ext}(f)} + I_2^{\text{ext}(f)}$, τότε $s = s_1 + s_2$, όπου $s_1 \in I_1^{\text{ext}(f)}$ και $s_2 \in I_2^{\text{ext}(f)}$, οπότε

$$\exists m \in \mathbb{N},\ a_1,\dots,a_m \in I_1,\ t_1,\dots,t_m \in R' : s_1 = \sum_{i=1}^{m} t_i f(a_i),$$

και

$$\exists n \in \mathbb{N},\ b_1,\dots,b_n \in I_2,\ u_1,\dots,u_n \in R' : s_2 = \sum_{j=1}^{n} u_j f(b_j).$$

Επομένως,

$$\left.\begin{array}{l} s_1 \in f(I_1)R' \subseteq f(I_1+I_2)R' \\ s_2 \in f(I_2)R' \subseteq f(I_1+I_2)R' \end{array}\right\} \Rightarrow s \in f(I_1+I_2)R' = (I_1+I_2)^{\text{ext}(f)},$$

απ' όπου έπεται ότι $I_1^{\text{ext}(f)} + I_2^{\text{ext}(f)} \subseteq (I_1+I_2)^{\text{ext}(f)}$. Και αντιστρόφως· εάν υποθέσουμε ότι $s \in (I_1+I_2)^{\text{ext}(f)}$, τότε

$$\exists m \in \mathbb{N},\ c_1,\dots,c_m \in I_1+I_2,\ t_1,\dots,t_m \in R' : s = \sum_{i=1}^{m} t_i f(c_i).$$

Προφανώς,

$$\exists a_1,\dots,a_m \in I_1,\ b_1,\dots,b_m \in I_2 : c_i = a_i + b_i,$$

για κάθε $i \in \{1,\dots,m\}$. Ως εκ τούτου,

$$s = \underbrace{\sum_{i=1}^{m} t_i f(a_i)}_{\in f(I_1)R'} + \underbrace{\sum_{i=1}^{m} t_i f(b_i)}_{\in f(I_2)R'} \in I_1^{\text{ext}(f)} + I_2^{\text{ext}(f)},$$

οπότε $(I_1+I_2)^{\text{ext}(f)} \subseteq I_1^{\text{ext}(f)} + I_2^{\text{ext}(f)}$.

(b) Εάν $s \in I_1^{\text{ext}(f)} I_2^{\text{ext}(f)}$, τότε $\exists \kappa \in \mathbb{N},\ s_{1,1},\dots,s_{1,\kappa},\in I_1^{\text{ext}(f)},\ s_{2,1},\dots,s_{2,\kappa} \in I_2^{\text{ext}(f)}$:

$$s = \sum_{i=1}^{\kappa} s_{1,i}s_{2,i}.$$

Επομένως, για κάθε $i \in \{1, \dots, \kappa\}$

$$\exists m \in \mathbb{N},\ a_{1,i,1}, \dots, a_{1,i,m} \in I_1,\ t_{1,i,1}, \dots, t_{1,i,m} \in R' : s_{1,i} = \sum_{\mu=1}^{m} t_{1,i,\mu} f(a_{1,i,\mu}),$$

και

$$\exists n \in \mathbb{N},\ a_{2,i,1}, \dots, a_{2,i,n} \in I_2,\ t_{2,i,1}, \dots, t_{2,i,n} \in R' : s_{2,i} = \sum_{\nu=1}^{n} t_{2,i,\nu} f(a_{2,i,\nu}).$$

Εξ αυτού συμπεραίνουμε ότι

$$s = \sum_{i=1}^{\kappa} \left(\sum_{\mu=1}^{m} t_{1,i,\mu} f(a_{1,i,\mu}) \right) \left(\sum_{\nu=1}^{n} t_{2,i,\nu} f(a_{2,i,\nu}) \right) = \sum_{i=1}^{\kappa} \sum_{\lambda=2}^{m+n} \sum_{\mu+\nu=\lambda} \xi_{i,\lambda},$$

όπου

$$\xi_{i,\lambda} := t_{1,i,\mu} t_{2,i,\nu} f(a_{1,i,\mu}) f(a_{2,i,\nu}) = t_{1,i,\mu} t_{2,i,\nu} f(a_{1,i,\mu} a_{2,i,\nu}) \in (I_1 I_2)^{\mathrm{ext}(f)},$$

απ' όπου έπεται ότι $s \in (I_1 I_2)^{\mathrm{ext}(f)}$. Άρα $I_1^{\mathrm{ext}(f)} I_2^{\mathrm{ext}(f)} \subseteq (I_1 I_2)^{\mathrm{ext}(f)}$. Και αντιστρόφως· εάν $s \in (I_1 I_2)^{\mathrm{ext}(f)}$, τότε

$$\exists m \in \mathbb{N},\ r_1, \dots, r_m \in I_1 I_2,\ t_1, \dots, t_m \in R' : s = \sum_{i=1}^{m} t_i f(r_i).$$

Επομένως, για κάθε $i \in \{1, \dots, m\}$

$$\exists \kappa \in \mathbb{N},\ a_{1,1,i}, \dots, a_{1,\kappa,i} \in I_1,\ a_{2,1,i}, \dots, a_{2,\kappa,i} \in I_2 : r_i = \sum_{j=1}^{\kappa} a_{1,j,i} a_{2,j,i}.$$

Εξ αυτού συμπεραίνουμε ότι

$$s = \sum_{i=1}^{m} t_i f\left(\sum_{j=1}^{\kappa} a_{1,j,i} a_{2,j,i} \right) = \sum_{i=1}^{m} \sum_{j=1}^{\kappa} t_i f\left(a_{1,j,i}\right) f\left(a_{2,j,i}\right) \in I_1^{\mathrm{ext}(f)} I_2^{\mathrm{ext}(f)}.$$

Άρα $(I_1 I_2)^{\mathrm{ext}(f)} \subseteq I_1^{\mathrm{ext}(f)} I_2^{\mathrm{ext}(f)}$.

(c) Εάν $s \in (I_1 \cap I_2)^{\mathrm{ext}(f)}$, τότε

$$\exists m \in \mathbb{N},\ r_1, \dots, r_m \in I_1 \cap I_2,\ t_1, \dots, t_m \in R' : s = \sum_{i=1}^{m} t_i f(r_i).$$

Επειδή $f(r_i) \in f(I_1 \cap I_2) \subseteq f(I_j)$ για $j \in \{1, 2\}$, διαπιστώνουμε ότι $s \in I_1^{\mathrm{ext}(f)} \cap I_2^{\mathrm{ext}(f)}$. Κατά συνέπειαν,

$$(I_1 \cap I_2)^{\mathrm{ext}(f)} \subseteq I_1^{\mathrm{ext}(f)} \cap I_2^{\mathrm{ext}(f)}.$$

Εάν υποθέσουμε ότι ο f είναι *επιμορφισμός*, ότι $\text{Ker}(f) \subseteq I_j$, για κάποιον $j \in \{1,2\}$, και ότι $s \in I_1^{\text{ext}(f)} \cap I_2^{\text{ext}(f)}$, τότε υπάρχει $r \in R : f(r) = s$ και (επειδή $I_1^{\text{ext}(f)} = f(I_1)$ και $I_2^{\text{ext}(f)} = f(I_2)$) υπάρχουν $a \in I_1, b \in I_2 : s = f(a) = f(b)$, οπότε

$$\left.\begin{array}{l} r-a \in \text{Ker}\,(f) \subseteq I_j \\ r-b \in \text{Ker}\,(f) \subseteq I_j \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \text{είτε } r \in I_1,\ b \in I_1 \cap I_2 \text{ (όταν } j=1) \\ \text{είτε } r \in I_2,\ a \in I_1 \cap I_2 \text{ (όταν } j=2) \end{array}\right\}.$$

Και στις δύο περιπτώσεις, $s \in f(I_1 \cap I_2) = (I_1 \cap I_2)^{\text{ext}(f)}$. Εξ αυτού συμπεραίνουμε ότι Άρα $I_1^{\text{ext}(f)} \cap I_2^{\text{ext}(f)} \subseteq (I_1 \cap I_2)^{\text{ext}(f)}$.

(d) Εάν $s \in (I_1 : I_2)^{\text{ext}(f)}$, τότε $\exists m \in \mathbb{N},\ r_1, \ldots, r_m \in R,\ t_1, \ldots, t_m \in R' :$

$$s = \sum_{i=1}^{m} t_i f(r_i),$$

με $r_i I_2 \subseteq I_1,\ \forall i \in \{1, \ldots, m\}$, οπότε

$$f(r_i I_2) = f(r_i) f(I_2) \subseteq f(I_1),\ \forall i \in \{1, \ldots, m\} \Rightarrow s \in I_1^{\text{ext}(f)} : I_2^{\text{ext}(f)},$$

απ' όπου συνάγουμε ότι $(I_1 : I_2)^{\text{ext}(f)} \subseteq I_1^{\text{ext}(f)} : I_2^{\text{ext}(f)}$. Εάν υποθέσουμε ότι ο f είναι *επιμορφισμός*, ότι $\text{Ker}(f) \subseteq I_1$ και ότι $s \in I_1^{\text{ext}(f)} : I_2^{\text{ext}(f)}$, τότε

$$s I_2^{\text{ext}(f)} = s f(I_2) \subseteq I_1^{\text{ext}(f)} = f(I_1)$$

και υπάρχει $r \in R : f(r) = s$ και

$$\left.\begin{array}{r} f(r) f(I_2) = f(rI_2) \subseteq f(I_1) \Rightarrow rI_2 \subseteq f^{-1}(f(I_1)) \\ \text{Ker}\,(f) \subseteq I_1 \Rightarrow f^{-1}(f(I_1)) = I_1 \end{array}\right\} \Rightarrow rI_2 \subseteq I_1,$$

οπότε

$$r \in I_1 : I_2 \Rightarrow s = f(r) \in f(I_1 : I_2) = (I_1 : I_2)^{\text{ext}(f)}.$$

Άρα τελικώς $I_1^{\text{ext}(f)} : I_2^{\text{ext}(f)} \subseteq (I_1 : I_2)^{\text{ext}(f)}$.

(e) Εάν $s \in \text{Rad}(I)^{\text{ext}(f)}$, τότε $\exists m \in \mathbb{N},\ r_1, \ldots, r_m \in \text{Rad}(I),\ t_1, \ldots, t_m \in R' :$

$$s = \sum_{i=1}^{m} t_i f(r_i),$$

και

$$\exists \nu_i \in \mathbb{N} : r_i^{\nu_i} \in I,\ \ \forall i \in \{1, \ldots, m\},$$

οπότε

$$f(r_i^{\nu_i}) = f(r_i)^{\nu_i} \in f(I) R' \Rightarrow f(r_i) \in \text{Rad}\left(I^{\text{ext}(f)}\right),\ \forall i \in \{1, \ldots, m\},$$

και -κατ' επέκτασιν- $s \in \mathrm{Rad}\big(I^{\mathrm{ext}(f)}\big)$. Άρα $\mathrm{Rad}(I)^{\mathrm{ext}(f)} \subseteq \mathrm{Rad}\big(I^{\mathrm{ext}(f)}\big)$. Εάν υποθέσουμε ότι ο f είναι *επιμορφισμός*, ότι $\mathrm{Ker}(f) \subseteq I$ και ότι $s \in \mathrm{Rad}\big(I^{\mathrm{ext}(f)}\big)$, τότε υπάρχει $r \in R$: $f(r) = s$ και

$$\left.\begin{array}{r} \exists \kappa \in \mathbb{N} : s^\kappa \in I^{\mathrm{ext}(f)} = f(I) \\ \mathrm{Ker}\,(f) \subseteq I \Rightarrow f^{-1}(f(I)) = I \end{array}\right\} \Rightarrow r^\kappa \in f^{-1}(f(r^\kappa)) = f^{-1}(s^\kappa) \subseteq I$$

οπότε

$$r \in \ \mathrm{Rad}(I) \Rightarrow s = f(r) \in f(\mathrm{Rad}(I)) = \mathrm{Rad}\,(I)^{\mathrm{ext}(f)}\,.$$

Άρα τελικώς $\mathrm{Rad}\big(I^{\mathrm{ext}(f)}\big) \subseteq \mathrm{Rad}(I)^{\mathrm{ext}(f)}$. □

A-1-31. (a) Έστω τυχόν $r \in J_1^{\mathrm{con}(f)} + J_2^{\mathrm{con}(f)}$. Τότε $r = a + b$, για κάποια $a \in f^{-1}(J_1)$ και $b \in f^{-1}(J_2)$, οπότε

$$f(r) = f(a) + f(b) \in J_1 + J_2 \Rightarrow r \in (J_1 + J_2)^{\mathrm{con}(f)},$$

εξ ου και ο εκλεισμός $J_1^{\mathrm{con}(f)} + J_2^{\mathrm{con}(f)} \subseteq (J_1 + J_2)^{\mathrm{con}(f)}$. Εάν υποθέσουμε ότι ο f είναι *επιμορφισμός* και $r \in (J_1 + J_2)^{\mathrm{con}(f)}$, τότε $f(r) \in J_1 + J_2$, ήτοι $f(r) = c + d$, για κάποια $c \in J_1$ και $d \in J_2$, οπότε υπάρχουν $a \in f^{-1}(J_1)$ και $b \in f^{-1}(J_2)$ με $f(a) = c$ και $f(b) = d$. Συνεπώς,

$$f(r) = f(a + b) \Rightarrow f(r - a - b) = 0_{R'} \Rightarrow r - a - b = s \in \mathrm{Ker}(f).$$

Επειδή $0_{R'} \in J_1 \cap J_2 \Rightarrow \mathrm{Ker}(f) = f^{-1}(0_{R'}) \subseteq f^{-1}(J_1) \cap f^{-1}(J_2) \subseteq f^{-1}(J_1) + f^{-1}(J_2)$, έχουμε

$$\left.\begin{array}{r} s \in \mathrm{Ker}(f) \subset f^{-1}(J_1) + f^{-1}(J_2) \\ a + b \in f^{-1}(J_1) + f^{-1}(J_2) \end{array}\right\} \Rightarrow r = s + a + b \in J_1^{\mathrm{con}(f)} + J_2^{\mathrm{con}(f)},$$

οπότε $(J_1 + J_2)^{\mathrm{con}(f)} \subseteq J_1^{\mathrm{con}(f)} + J_2^{\mathrm{con}(f)}$.

(b) Έστω τυχόν $r \in J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)}$. Τότε υπάρχουν $\kappa \in \mathbb{N}$, $a_1, \ldots, a_\kappa \in f^{-1}(J_1)$, $b_1, \ldots, b_\kappa \in f^{-1}(J_2)$:

$$r = \sum_{j=1}^{\kappa} a_j b_j \Rightarrow f(r) = \sum_{j=1}^{\kappa} \underbrace{f(a_j)}_{\in J_1} \underbrace{f(b_j)}_{\in J_2} \in J_1 J_2 \Rightarrow r \in (J_1 J_2)^{\mathrm{con}(f)}\,.$$

Άρα $J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)} \subseteq (J_1 J_2)^{\mathrm{con}(f)}$. Εάν υποθέσουμε ότι ο f είναι *επιμορφισμός* με

$$\mathrm{Ker}\,(f) \subseteq J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)}$$

και $r \in (J_1 J_2)^{\mathrm{con}(f)}$, τότε $\exists \kappa \in \mathbb{N},\ c_1, \dots, c_\kappa \in J_1,\ d_1, \dots, d_\kappa \in J_2$:

$$f(r) = \sum_{j=1}^{\kappa} c_j d_j,$$

καθώς και $a_1, \dots, a_\kappa \in f^{-1}(J_1),\ b_1, \dots, b_\kappa \in f^{-1}(J_2)$:

$$f(a_j) = c_j,\ \ f(b_j) = d_j,\ \ \forall j \in \{1, \dots, \kappa\},$$

οπότε

$$f(r) = \sum_{j=1}^{\kappa} f(a_j) f(b_j) = \sum_{j=1}^{\kappa} f(a_j b_j)$$

$$\Rightarrow r - \sum_{j=1}^{\kappa} a_j b_j = s \in \mathrm{Ker}\,(f) \subseteq J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)},$$

απ' όπου έπεται ότι

$$\left.\begin{array}{r} s \in J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)} \\ \sum_{j=1}^{\kappa} a_j b_j \in J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)} \end{array}\right\} \Rightarrow r = J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)}.$$

Τούτο σημαίνει ότι $(J_1 J_2)^{\mathrm{con}(f)} \subseteq J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)}$.

(c) Προφανώς,

$$(J_1 \cap J_2)^{\mathrm{con}(f)} = f^{-1}(J_1 \cap J_2) = f^{-1}(J_1) \cap f^{-1}(J_2) = J_1^{\mathrm{con}(f)} \cap J_2^{\mathrm{con}(f)}.$$

(d)Έστω τυχόν $r \in (J_1 : J_2)^{\mathrm{con}(f)} = f^{-1}(J_1 : J_2)$. Τότε

$$f(r) \in J_1 : J_2 \Rightarrow f(r)a \in J_1,\ \forall a \in J_2.$$

Για *οιοδήποτε* $b \in f^{-1}(J_2)$ έχουμε

$$f(b) \in J_2 \Rightarrow f(r)f(b) = f(rb) \in J_1 \Rightarrow rb \in f^{-1}(J_1).$$

Άρα $r \in f^{-1}(J_1) : f^{-1}(J_2) = J_1^{\mathrm{con}(f)} : J_2^{\mathrm{con}(f)}$.

Εάν υποθέσουμε ότι ο f είναι *επιμορφισμός* και $r \in J_1^{\mathrm{con}(f)} : J_2^{\mathrm{con}(f)}$, τότε

$$ra \in f^{-1}(J_1), \forall a \in f^{-1}(J_2) \Rightarrow f(ra) = f(r)f(a) \in f(f^{-1}(J_1)) = J_1, \forall a \in f^{-1}(J_2),$$

με $f(f^{-1}(J_2)) = J_2$, απ' όπου έπεται ότι $f(r) \in J_1 : J_2 \Rightarrow r \in (J_1 : J_2)^{\mathrm{con}(f)}$.

(e) Εάν $r \in \mathrm{Rad}(J)^{\mathrm{con}(f)}$, τότε $f(r) \in \mathrm{Rad}(J)$ και

$$\exists m \in \mathbb{N} : f(r)^m = f(r^m) \in J \Rightarrow r^m \in J^{\mathrm{con}(f)} \Rightarrow r \in \mathrm{Rad}\left(J^{\mathrm{con}(f)}\right).$$

Άρα $\mathrm{Rad}(J)^{\mathrm{con}(f)} \subseteq \mathrm{Rad}\big(J^{\mathrm{con}(f)}\big)$. Και αντιστρόφως· εάν $r \in \mathrm{Rad}\big(J^{\mathrm{con}(f)}\big)$, τότε

$$\exists \kappa \in \mathbb{N} : r^{\kappa} \in f^{-1}(J) \Rightarrow f(r^m) = f(r)^m \in J \Rightarrow f(r) \in \mathrm{Rad}\,(J)\,,$$

απ' όπου έπεται ότι $r \in \mathrm{Rad}(J)^{\mathrm{con}(f)}$. Άρα $\mathrm{Rad}\big(J^{\mathrm{con}(f)}\big) \subseteq \mathrm{Rad}(J)^{\mathrm{con}(f)}$. □

A-1-32. (a) Εάν $I \in \mathcal{I}_R$ και $r \in I$, τότε

$$f(r) \in f(I) \subseteq f(I)R' \Rightarrow r \in f^{-1}(f(r)) \subseteq f^{-1}(f(I)R') = (I^{\mathrm{ext}(f)})^{\mathrm{con}(f)},$$

οπότε $I \subseteq (I^{\mathrm{ext}(f)})^{\mathrm{con}(f)}$.
(b) Εάν $J \in \mathcal{I}_{R'}$ και $s \in (J^{\mathrm{con}(f)})^{\mathrm{ext}(f)} = f(f^{-1}(J))R'$, τότε

$$\exists \kappa \in \mathbb{N},\ s_1, \ldots, s_\kappa \in R',\ a_1, \ldots, a_\kappa \in f^{-1}(J) : s = \sum_{j=1}^{\kappa} s_j \underbrace{f(a_j)}_{\in J} \in J,$$

οπότε $(J^{\mathrm{con}(f)})^{\mathrm{ext}(f)} \subseteq J$.
(c) Εάν $I \in \mathcal{I}_R$ και $s \in I^{\mathrm{ext}(f)}$, τότε

$$\exists \kappa \in \mathbb{N},\ s_1, \ldots, s_\kappa \in R',\ a_1, \ldots, a_\kappa \in I : s = \sum_{j=1}^{\kappa} s_j f(a_j).$$

Κατά το (a), $a_j \in I \subseteq (I^{\mathrm{ext}(f)})^{\mathrm{con}(f)}$, οπότε

$$f(a_j) \in ((I^{\mathrm{ext}(f)})^{\mathrm{con}(f)})^{\mathrm{ext}(f)},\ \forall j \in \{1, \ldots, \kappa\} \Rightarrow s \in ((I^{\mathrm{ext}(f)})^{\mathrm{con}(f)})^{\mathrm{ext}(f)}.$$

Άρα $I^{\mathrm{ext}(f)} \subseteq ((I^{\mathrm{ext}(f)})^{\mathrm{con}(f)})^{\mathrm{ext}(f)}$. Από την άλλη μεριά, εφαρμόζοντας το (b) για το ιδεώδες $J := I^{\mathrm{ext}(f)} \in \mathcal{I}_{R'}$, λαμβάνουμε

$$((I^{\mathrm{ext}(f)})^{\mathrm{con}(f)})^{\mathrm{ext}(f)} \subseteq I^{\mathrm{ext}(f)}.$$

Άρα τελικώς $I^{\mathrm{ext}(f)} = ((I^{\mathrm{ext}(f)})^{\mathrm{con}(f)})^{\mathrm{ext}(f)}$.
(d) Εάν $J \in \mathcal{I}_{R'}$ και $r \in ((J^{\mathrm{con}(f)})^{\mathrm{ext}(f)})^{\mathrm{con}(f)}$, τότε

$$r \in f^{-1}((J^{\mathrm{con}(f)})^{\mathrm{ext}(f)}) \Rightarrow f(r) \in (J^{\mathrm{con}(f)})^{\mathrm{ext}(f)} \underset{\text{(b)}}{\subseteq} J$$

$$\Rightarrow r \in f^{-1}(f(r)) \subseteq f^{-1}(J) = J^{\mathrm{con}(f)}.$$

Άρα $((J^{\mathrm{con}(f)})^{\mathrm{ext}(f)})^{\mathrm{con}(f)} \subseteq J^{\mathrm{con}(f)}$. Από την άλλη μεριά, εφαρμόζοντας το (a) για το ιδεώδες $I := J^{\mathrm{con}(f)} \in \mathcal{I}_R$, λαμβάνουμε

$$J^{\mathrm{con}(f)} \subseteq ((J^{\mathrm{con}(f)})^{\mathrm{ext}(f)})^{\mathrm{con}(f)}.$$

Άρα τελικώς $((J^{\mathrm{con}(f)})^{\mathrm{ext}(f)})^{\mathrm{con}(f)} = J^{\mathrm{con}(f)}$.

(e) Εάν $\mathcal{C}_R(f) := \left\{ J^{\mathrm{con}(f)} \middle| J \in \mathcal{I}_{R'} \right\}$ και $\mathcal{E}_{R'}(f) := \left\{ I^{\mathrm{ext}(f)} \middle| I \in \mathcal{I}_R \right\}$, τότε οι απεικονίσεις

$$\mathcal{C}_R(f) \ni I \longmapsto I^{\mathrm{ext}(f)} \in \mathcal{E}_{R'}(f), \quad \mathcal{E}_{R'}(f) \ni J \longmapsto J^{\mathrm{con}(f)} \in \mathcal{C}_R(f),$$

είναι αμφιρριπτικές και η μία αντίστροφος τής άλλης, διότι κατά τα (c) και (d) έχουμε

$$I^{\mathrm{ext}(f)} = ((I^{\mathrm{ext}(f)})^{\mathrm{con}(f)})^{\mathrm{ext}(f)}, \ \forall I \in \mathcal{I}_R,$$

και

$$((J^{\mathrm{con}(f)})^{\mathrm{ext}(f)})^{\mathrm{con}(f)} = J^{\mathrm{con}(f)}, \ \forall J \in \mathcal{I}_{R'},$$

αντιστοίχως.

(f) Εάν ο f είναι επιμορφισμός, τότε $\mathcal{C}_R(f) = \{ I \in \mathcal{I}_R | \, I \supseteq \mathrm{Ker}(f) \}$, $\mathcal{E}_{R'}(f) = \mathcal{I}_{R'}$, και οι απεικονίσεις

$$\mathcal{C}_R(f) \ni I \longmapsto f(I) \in \mathcal{E}_{R'}(f), \quad \mathcal{E}_{R'}(f) \ni J \longmapsto f^{-1}(J) \in \mathcal{C}_R(f),$$

είναι αμφιρριπτικές και η μία αντίστροφος τής άλλης. Τούτο έπεται άμεσα από τ (e) και από το ότι για κάθε $I \in \mathcal{I}_R$ με $I \supseteq \mathrm{Ker}(f)$ έχουμε $f(I) = I^{\mathrm{ext}(f)} \in \mathcal{E}_{R'}(f)$. □

A-1-33. Έστω τυχόν πολυώνυμο $F \in \mathbf{I}(V) + \mathbf{I}(W)$. Τότε $F = G + H$, για κάποια πολυώνυμα $G \in \mathbf{I}(V)$ και $H \in \mathbf{I}(W)$. Για κάθε $P \in V \cap W$ έχουμε

$$F(P) = G(P) + H(P) = 0_{\mathbf{k}} + 0_{\mathbf{k}} = 0_{\mathbf{k}} \Rightarrow F \in \mathbf{I}(V \cap W).$$

Άρα $\mathbf{I}(V) + \mathbf{I}(W) \subseteq \mathbf{I}(V \cap W)$. Βάσει τής προτάσεως 1.4.5 (a)) ισχύει

$$\mathbf{I}(V)\mathbf{I}(W) \subseteq \mathbf{I}(V) \cap \mathbf{I}(W).$$

Θεωρούμε τυχόντα $F \in \mathbf{I}(V) \cap \mathbf{I}(W)$ και $P \in V \cup W$. Εάν $P \in V$, τότε $F(P) = 0_{\mathbf{k}}$ (διότι $F \in \mathbf{I}(V)$). Κατ' αναλογίαν, εάν $P \in W$, τότε $F(P) = 0_{\mathbf{k}}$ (διότι $F \in \mathbf{I}(W)$). Ως εκ τούτου, $F \in \mathbf{I}(V \cup W)$, οπότε $\mathbf{I}(V)\mathbf{I}(W) \subseteq \mathbf{I}(V \cup W)$. □

A-1-34. (a) Έστω τυχόν $F \in I : J$. Εξ ορισμού, $FG \in I, \forall G \in J$. Εάν $P \in \mathbf{V}(I) \setminus \mathbf{V}(J)$, τότε

$$F(P)G(P) = 0_{\mathbf{k}}, \ \forall G \in J, \ \forall F \in I : J.$$

Επειδή $P \notin \mathbf{V}(J)$, $\exists G \in J : G(P) \neq 0_{\mathbf{k}}$. Επομένως, χρησιμοποιώντας αυτό το G συμπεραίνουμε ότι

$$F(P) = 0_{\mathbf{k}}, \ \forall P \in \mathbf{V}(I) \setminus \mathbf{V}(J) \Longrightarrow F \in \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J)).$$

(b) Θέτοντας $I = \mathbf{I}(V)$, $J = \mathbf{I}(W)$ στο (a) και εφαρμόζοντας το (5) (a) τής προτάσεως 1.3.1, λαμβάνουμε

$$\mathbf{I}(V) : \mathbf{I}(W) \subseteq \mathbf{I}(\mathbf{V}(\mathbf{I}(V)) \smallsetminus \mathbf{V}(\mathbf{I}(W))) = \mathbf{I}(V \smallsetminus W).$$

Και αντιστρόφως· εάν $F \in \mathbf{I}(V \smallsetminus W)$, τότε $F(P) = 0_{\mathbf{k}}$, $\forall P \in V \smallsetminus W$. Προφανώς, $V = (V \smallsetminus W) \cap (V \cap W)$. Εάν $P \in V \smallsetminus W$, τότε $F(P) = 0_{\mathbf{k}}$, ενώ εάν $P \in V \cap W$, έχουμε $F(P)G(P) = 0_{\mathbf{k}}$ για κάθε $G \in \mathbf{I}(W)$. Άρα

$$F(P)G(P) = 0_{\mathbf{k}},\ \forall P \in V,\ \forall G \in \mathbf{I}(W),$$

οπότε $\mathbf{I}(V \smallsetminus W) \subseteq \mathbf{I}(V) : \mathbf{I}(W)$. □

A-1-35. (a) Έστω

$$\text{Μον}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]) := \left\{ \mathsf{X}_1^{i_1} \mathsf{X}_2^{i_2} \cdots \mathsf{X}_n^{i_n} \,\middle|\, (i_1, i_2, \dots, i_n) \in \mathbb{N}_0^n \right\}$$

το σύνολο των μονωνύμων τού $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$. Ορίζοντας ως

$$\text{Μον}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n])_{\leq d}, \quad \text{Μον}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n])_d$$

τα υποσύνολα τού $\text{Μον}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n])$ που έχουν βαθμό $\leq d$ και $= d$, αντιστοίχως, και θέτοντας

$$\varphi_{\leq d}(n) := \sharp(\text{Μον}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n])_{\leq d}) = \sharp\left\{ (i_1, \dots, i_n) \in \mathbb{N}_0^n \,|\, i_1 + \cdots + i_n \leq d \right\},$$

$$\varphi_d(n) := \sharp(\text{Μον}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n])_d) = \sharp\left\{ (i_1, \dots, i_n) \in \mathbb{N}_0^n \,|\, i_1 + \cdots + i_n = d \right\},$$

παρατηρούμε ότι ορίζεται μια αμφίρριψη

$$\begin{array}{c} \left\{ (i_1, \dots, i_n) \in \mathbb{N}_0^n \,|\, i_1 + \cdots + i_n \leq d \right\} \\ \updownarrow \\ \left\{ (\xi_1, \dots, \xi_n) \in \mathbb{N}^n \,|\, 1 \leq \xi_1 < \xi_2 < \cdots < \xi_n \leq n + d \right\}, \end{array}$$

όπου

$$(i_1, \dots, i_n) \longmapsto (\xi_1, \dots, \xi_n) := (i_1 + 1, i_1 + i_2 + 2 \dots, , i_1 + i_2 + \dots + i_n + n).$$

Προφανώς,

$$\varphi_{\leq d}(n) = \sharp\left\{ (\xi_1, \dots, \xi_n) \in \mathbb{N}^n \,|\, 1 \leq \xi_1 < \xi_2 < \cdots < \xi_n \leq n + d \right\} = \binom{n+d}{n}$$

και

$$\varphi_d(n) = \varphi_{\leq d}(n) - \varphi_{\leq d-1}(n) = \binom{n+d}{n} - \binom{n+d-1}{n} = \binom{n-1+d}{n-1}.$$

(b) Εάν $I := \langle \mathsf{X}_1, \dots, \mathsf{X}_n \rangle \subset \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, τότε το I^d παράγεται (εξ ορισμού) από όλα τα μονώνυμα τα ανήκοντα στο $\mathrm{Μον}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n])_d$ (πρβλ. το (d) τής σημειώσεως 1.4.2), οπότε αποτελείται από εκείνα τα πολυώνυμα τού $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, τα οποία δεν περιέχουν κανέναν όρο βαθμού $< d$. Ο πηλικοδακτύλιος $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]/I^d$, ιδωμένος ως διανυσματικός χώρος υπεράνω τού σώματος $\mathbf{k}$, έχει το σύνολο

$$\left\{ \mathsf{X}_1^{i_1} \cdots \mathsf{X}_n^{i_n} + I^d \,\middle|\, (i_1, i_2, \dots, i_n) \in \mathbb{N}_0^n,\ \mathsf{X}_1^{i_1} \cdots \mathsf{X}_n^{i_n} \in \mathrm{Μον}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n])_{\leq d-1} \right\}$$

ως βάση του. Αυτό σημαίνει ότι

$$\dim_{\mathbf{k}}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]/I^d) = \varphi_{\leq d-1}(n) = \binom{n-1+d}{n},$$

οπότε ο ισχυρισμός είναι αληθής. □

A-1-36. Έστω I ένα ιδεώδες ενός δακτυλίου R και έστω $\pi : R \longrightarrow R/I$ ο φυσικός επιμορφισμός.

(a) Εάν το J' είναι ένα ιδεώδες τού R/I, τότε το $\pi^{-1}(J') =: J$ είναι ένα ιδεώδες τού R το οποίο περιέχει το I. Πράγματι· εάν $a, b \in J$ και $r \in R$, τότε

$$\left.\begin{array}{l} a + I = \pi(a) \in J' \\ b + I = \pi(b) \in J' \end{array}\right\} \Longrightarrow (a+I) - (b+I) = (a-b) + I = \pi(a-b) \in J' \Longrightarrow a - b \in J$$

και $r(a+I) = (ra) + I = \pi(ra) \in J' \Longrightarrow ra \in J$, με $I \subseteq J$ (διότι για κάθε $a \in I$ έχουμε $a + I = 0_R + I \in J'$, οπότε $a \in \pi^{-1}(J') =: J$).

Από την άλλη μεριά, εάν το J είναι ένα ιδεώδες τού R, το οποίο περιέχει το I, το $\pi(J) =: J'$ αποτελεί ένα ιδεώδες τού R/I. Πράγματι· εάν $a + I, b + I \in J'$ με $a, b \in J$ και $r + I \in R/I$, τότε

$$\begin{aligned} \pi(a-b) &= (a-b) + I = (a+I) - (b+I) \in J', \\ \pi(ra) &= (ra) + I = r(a+I) \in J'. \end{aligned}$$

Κατ' αυτόν τον τρόπο ορίζεται μέσω τής αντιστοιχίας

$$\{\text{ιδεώδη τού } R/I\} \ni J' \longleftrightarrow J \in \left\{ \begin{array}{c} \text{ιδεώδη τού } R \\ \text{τα οποία περιέχουν το } I \end{array} \right\}$$

η ζητούμενη αμφίρριψη (πρβλ. άσκηση **A-1-32** (f)).

(b) Το J είναι ένα ριζικό ιδεώδες εάν και μόνον εάν το J' είναι ριζικό. Πράγματι· εάν $J = \mathrm{Rad}(J)$, τότε (προφανώς) $J' \subseteq \mathrm{Rad}(J')$ και για οιοδήποτε $(a+I) \in \mathrm{Rad}(J') \subseteq R/I$

$$\exists n \in \mathbb{N} : (a+I)^n = a^n + I \in J' = \pi(J) \Longrightarrow a^n \in J = \mathrm{Rad}(J)$$

$$\Longrightarrow a \in J \Longrightarrow (a+I) \in J'.$$

Και αντιστρόφως· εάν $J' = \text{Rad}(J')$, τότε (προφανώς) $J \subseteq \text{Rad}(J)$ και για οιοδήποτε $a \in \text{Rad}(J)$

$$\exists n \in \mathbb{N} : a^n \in J \Longrightarrow a^n + I = (a+I)^n \in J' = \text{Rad}(J')$$

$$\Longrightarrow (a+I) \in J' = \pi(J) \Longrightarrow a \in J.$$

Επίσης, το J είναι πρώτο (και αντιστοίχως, μεγιστοτικό) ιδεώδες εάν και μόνον εάν το J' είναι πρώτο (και αντιστοίχως, μεγιστοτικό). Πράγματι· θεωρώντας τόν φυσικό επιμορφισμό

$$\varpi : R/I \longrightarrow (R/I)/J', \quad \varpi(r+I) := (r+I) + J', \ \forall r \in R,$$

και ορίζοντας τον επιμορφισμό

$$f := \varpi \circ \pi, \quad f : R \longrightarrow (R/I)/J',$$

έχουμε

$$\begin{aligned} \text{Ker}(f) &= \{r \in R \mid f(r) = J'\} = \{r \in R \mid \varpi(\pi(r)) = J'\} = \{r \in R \mid \varpi(r+I) = J'\} \\ &= \{r \in R \mid (r+I) + J' = J'\} = \{r \in R \mid \pi(r) \in J'\} = \pi^{-1}(J') = J. \end{aligned}$$

Επί τη βάσει τού 1ου θεωρήματος ισομορφισμών δακτυλίων (βλ. θεώρημα 1.1.10) δημιουργείται ο ισομορφισμός

$$\sigma : R/J \longrightarrow (R/I)/J', \ \ \sigma(r+J) := f(r) = (r+I) + J', \ \forall r \in R.$$

Επομένως, [το J είναι πρώτο (και αντιστοίχως, μεγιστοτικό) ιδεώδες τού R] $\Longleftrightarrow$ [ο πηλικοδακτύλιος R/J είναι ακεραία περιοχή (και αντιστοίχως, σώμα, βλ. θεωρήματα 1.1.13 και 1.1.14)] $\Longleftrightarrow$ [ο πηλικοδακτύλιος $(R/I)/J' = \sigma(R/J)$ είναι ακεραία περιοχή (και αντιστοίχως, σώμα)] $\Longleftrightarrow$ [το J' είναι πρώτο (και αντιστοίχως, μεγιστοτικό) ιδεώδες τού R/I (εκ νέου λόγω των θεωρημάτων 1.1.13 και 1.1.14)].

(c) Εάν το J είναι πεπερασμένως παραγόμενο, ας πούμε $J = \langle a_1, \ldots, a_k \rangle$, $k \in \mathbb{N}$, τότε και το J' είναι πεπερασμένως παραγόμενο:

$$J' = \pi(J) = \pi(\langle a_1, \ldots, a_k \rangle) = \langle \pi(a_1), \ldots, \pi(a_k) \rangle = \langle a_1 + I, \ldots, a_k + I \rangle,$$

διότι κάθε $a \in J$ γράφεται ως άθροισμα τής μορφής $a = \sum_{i=1}^{k} r_i a_i$, όπου $r_1, \ldots, r_k \in R$, οπότε

$$\pi(a) = \pi\left(\sum_{i=1}^{k} r_i a_i\right) = \sum_{i=1}^{k} r_i \pi(a_i) = \sum_{i=1}^{k} r_i (a_i + I) \in \langle a_1 + I, \ldots, a_k + I \rangle,$$

και αντιστρόφως, για οιοδήποτε $b \in R$ με $b+I \in \langle a_1+I, \ldots, a_k+I\rangle$ υπάρχουν στοιχεία $s_1, \ldots, s_k \in R$, τέτοια ώστε να ισχύει

$$b+I = \sum_{i=1}^{k} (s_i+I)\,(a_i+I) = \sum_{i=1}^{k} (s_i a_i + I) = \sum_{i=1}^{k} \pi(s_i a_i) = \pi\left(\sum_{i=1}^{k} s_i a_i\right) \in J'.$$

Εξ αυτού συνάγεται άμεσα ότι για οιονδήποτε ναιτεριανό δακτύλιο R ο R/I είναι ναιτεριανός. (Επομένως, και κάθε δακτύλιος τής μορφής $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]\,/\,I$, όπου $\mathbf{k}$ σώμα, είναι ναιτεριανός.) □

A-1-37. Έστω $R := \mathbb{R}[\mathsf{X}]$. Ο R είναι ναιτεριανός (σύμφωνα με το θεώρημα βάσεως 1.5.4 τού Hilbert). Στην οικογένεια ιδεωδών

$$\mathcal{J} := \left\{ \left\langle \mathsf{X}^k \right\rangle \mid k \in \mathbb{N},\ k \geq 2 \right\}$$

τού R το $\left\langle \mathsf{X}^2 \right\rangle$, το οποίο αποτελεί (το μοναδικό) μεγιστοτικό μέλος της, δεν είναι μεγιστοτικό ιδεώδες, καθότι $\left\langle \mathsf{X}^2 \right\rangle \subsetneqq \langle \mathsf{X} \rangle \subsetneqq R$. □

A-1-38. Κάθε γνήσιο ιδεώδες I ενός ναιτεριανού δακτυλίου R περιέχεται σε ένα μεγιστοτικό ιδεώδες. Για την απόδειξη αρκεί να εφαρμοσθεί το (c) τής προτάσεως 1.5.3 για τη συλλογή ιδεωδών

$$\mathcal{J} := \{\text{ιδεώδη } J \subsetneqq R \mid I \subseteq J\}.$$

(Κάθε μεγιστοτικό στοιχείο τής $\mathcal{J}$ είναι κατάλληλο για τους σκοπούς μας.) □

A-1-39. Η ισοδυναμία (a)⇔(b) έπεται άμεσα από τον ορισμό 1.6.1. Η ισοδυναμία (b)⇔(c) έπεται από το ότι

$$U_1 \cap U_2 = \varnothing \Longleftrightarrow Y = (Y \smallsetminus U_1) \cup (Y \smallsetminus U_2).$$

Από την άλλη μεριά, ένα υποσύνολο $U \subseteq Y$ είναι πυκνό στο Y εάν και μόνον εάν η τομή του με οιοδήποτε μη κενό, ανοικτό υποσύνολο τού Y είναι μη κενή. Εξ αυτού έπεται η ισοδυναμία (c)⇔(d). □

A-1-40. (a) Ορίζουμε τον επιμορφισμό δακτυλίων

$$f : \mathbb{C}[\mathsf{X}, \mathsf{Y}] \longrightarrow \mathbb{C}[\mathsf{X}], \quad f(F) := F(\mathsf{X}, \mathsf{X}^2),\ \forall F \in \mathbb{C}[\mathsf{X}, \mathsf{Y}].$$

Επί τη βάσει τού 1ου θεωρήματος ισομορφισμών δακτυλίων (βλ. θεώρημα 1.1.10) δημιουργείται ισομορφισμός

$$\mathbb{C}[\mathsf{X}, \mathsf{Y}]/\mathrm{Ker}(f) \cong \mathbb{C}[\mathsf{X}].$$

Επειδή $\mathrm{Ker}(f) = \mathbf{I}(\mathbf{V}(\mathsf{Y} - \mathsf{X}^2))$ και ο $\mathbb{C}[\mathsf{X}]$ είναι ακεραία περιοχή, το $\mathbf{I}(\mathbf{V}(\mathsf{Y} - \mathsf{X}^2))$ είναι πρώτο ιδεώδες (βλ. θεώρημα 1.1.13), το $\mathbf{V}(\mathsf{Y} - \mathsf{X}^2) \subset \mathbb{A}^2_{\mathbb{C}}$ ανάγωγο (βλ. πρόταση 1.6.1). και $\mathbf{I}(\mathbf{V}(\mathsf{Y} - \mathsf{X}^2)) = \langle \mathsf{Y} - \mathsf{X}^2 \rangle$ (πρβλ. πόρισμα 1.7.2).

(b) Προφανώς,

$$\mathbf{V}(\mathsf{Y}^4 - \mathsf{X}^2, \mathsf{Y}^4 - \mathsf{X}^2\mathsf{Y}^2 + \mathsf{X}\mathsf{Y}^2 - \mathsf{X}^3) = \mathbf{V}(\left(\mathsf{Y}^2 - \mathsf{X}\right)\left(\mathsf{Y}^2 + \mathsf{X}\right), \left(\mathsf{Y}^2 + \mathsf{X}\right)(\mathsf{Y} + \mathsf{X})(\mathsf{Y} - \mathsf{X}))$$

$$= \mathbf{V}(\left(\mathsf{Y}^2 - \mathsf{X}\right)\left(\mathsf{Y}^2 + \mathsf{X}\right)) \cap \mathbf{V}(\left(\mathsf{Y}^2 + \mathsf{X}\right)(\mathsf{Y} + \mathsf{X})(\mathsf{Y} - \mathsf{X}))$$

$$= \left(\mathbf{V}(\mathsf{Y}^2 - \mathsf{X}) \cup \mathbf{V}(\mathsf{Y}^2 + \mathsf{X})\right) \cap \left(\mathbf{V}(\mathsf{Y}^2 + \mathsf{X}) \cup \mathbf{V}(\mathsf{Y} + \mathsf{X}) \cup \mathbf{V}(\mathsf{Y} - \mathsf{X})\right)$$

$$\begin{aligned} = \quad & \mathbf{V}(\mathsf{Y}^2 - \mathsf{X}, \mathsf{Y}^2 + \mathsf{X}) \cup \mathbf{V}(\mathsf{Y}^2 - \mathsf{X}, \mathsf{Y} + \mathsf{X}) \cup \mathbf{V}(\mathsf{Y}^2 - \mathsf{X}, \mathsf{Y} - \mathsf{X}) \\ & \cup \mathbf{V}(\mathsf{Y}^2 + \mathsf{X}) \cup \mathbf{V}(\mathsf{Y}^2 + \mathsf{X}, \mathsf{Y} + \mathsf{X}) \cup \mathbf{V}(\mathsf{Y}^2 + \mathsf{X}, \mathsf{Y} - \mathsf{X}). \end{aligned}$$

Σημειωτέον ότι

$$\mathbf{V}(\mathsf{Y}^2 - \mathsf{X}, \mathsf{Y} + \mathsf{X}) = \{(0,0), (1,-1)\},\ \mathbf{V}(\mathsf{Y}^2 - \mathsf{X}, \mathsf{Y} - \mathsf{X}) = \{(0,0), (1,1)\}$$

και

$$\mathbf{V}(\mathsf{Y}^2 + \mathsf{X}, \mathsf{Y} + \mathsf{X}) = \{(0,0), (-1,1)\},\ \mathbf{V}(\mathsf{Y}^2 + \mathsf{X}, \mathsf{Y} - \mathsf{X}) = \{(0,0), (-1,-1)\},$$

οπότε η αποσύνθεση τού $\mathbf{V}(\mathsf{Y}^4 - \mathsf{X}^2, \mathsf{Y}^4 - \mathsf{X}^2\mathsf{Y}^2 + \mathsf{X}\mathsf{Y}^2 - \mathsf{X}^3) \subset \mathbb{A}^2_{\mathbb{C}}$ σε ανάγωγες συνιστώσες είναι η

$$\mathbf{V}(\mathsf{Y}^2 + \mathsf{X}) \cup \mathbf{V}(\mathsf{X} - 1, \mathsf{Y} + 1) \cup \mathbf{V}(\mathsf{X} - 1, \mathsf{Y} - 1) \cup \mathbf{V}(\mathsf{X} + 1, \mathsf{Y} - 1) \cup \mathbf{V}(\mathsf{X} + 1, \mathsf{Y} + 1),$$

διότι

$$\mathbf{V}(\mathsf{Y}^2 - \mathsf{X}, \mathsf{Y}^2 + \mathsf{X}) = \{(0,0)\} \subset \mathbf{V}(\mathsf{Y}^2 + \mathsf{X}).$$

και το $\mathbf{V}(\mathsf{Y}^2 + \mathsf{X})$ είναι ανάγωγο (πρβλ. (a)). □

A-1-41. Θεωρούμε το πολυώνυμο $F = \mathsf{Y}^2 + \mathsf{X}^2(\mathsf{X} - 1)^2 \in \mathbb{R}[\mathsf{X}, \mathsf{Y}]$. Εάν υποθέσουμε ότι το F είναι μη ανάγωγο, τότε το F θα γράφεται ως γινόμενο $F = F_1 \cdot F_2$ δύο μη σταθερών πολυωνύμων $F_1, F_2 \in \mathbb{R}[\mathsf{X}, \mathsf{Y}]$ τής μορφής

$$F_1 = a_1\mathsf{X}^2 + a_2\mathsf{Y}^2 + a_3\mathsf{X} + a_4\mathsf{Y} + a_5,\ \ F_2 = b_1\mathsf{X}^2 + b_2\mathsf{Y}^2 + b_3\mathsf{X} + b_4\mathsf{Y} + b_5,$$

όπου $a_j, b_j \in \mathbb{R}$ για κάθε $j \in \{1, \ldots, 5\}$. (Σημειωτέον ότι στη ανωτέρω έκφραση των F_1, F_2 δεν είναι αναγκαίο να συμπεριλάβουμε όρους τής μορφής $\lambda(\mathsf{X}\mathsf{Y})^2$ ή $\mu\mathsf{X}\mathsf{Y}$, $\lambda, \mu \in \mathbb{R}$,

λόγω τής ειδικής δομήσεως τού F. Κατ' αυτόν τον τρόπο αποφεύγονται, συν τοις άλλοις, και άσκοπες πράξεις.) Συνεπώς,

$$\begin{aligned}\mathsf{Y}^2+\mathsf{X}^2\left(\mathsf{X}-1\right)^2 &= a_1b_1\mathsf{X}^4+a_1b_2(\mathsf{XY})^2+a_1b_3\mathsf{X}^3+a_1b_4\mathsf{X}^2\mathsf{Y}+a_1b_5\mathsf{X}^2\\ &\quad +a_2b_1(\mathsf{XY})^2+a_2b_2\mathsf{Y}^4+a_2b_3\mathsf{Y}^2\mathsf{X}+a_2b_4\mathsf{Y}^3+a_2b_5\mathsf{Y}^2\\ &\quad +a_3b_1\mathsf{X}^3+a_3b_2\mathsf{Y}^2\mathsf{X}+a_3b_3\mathsf{X}^2+a_3b_4\mathsf{XY}+a_3b_5\mathsf{X}\\ &\quad +a_4b_1\mathsf{X}^2\mathsf{Y}+a_4b_2\mathsf{Y}^3+a_4b_3\mathsf{XY}+a_4b_4\mathsf{Y}^2+a_4b_5\mathsf{Y}\\ &\quad +a_5b_1\mathsf{X}^2+a_5b_2\mathsf{Y}^2+a_5b_3\mathsf{X}+a_5b_4\mathsf{Y}+a_5b_5.\end{aligned}$$

Κατόπιν συγκρίσεως των συντελεστών συνάγουμε (ιδιαιτέρως) ότι τα ακόλουθα οφείλουν να ισχύουν ταυτοχρόνως:

$$a_1b_1 = 1\ (\text{συντελεστές τού } \mathsf{X}^4), \tag{1}$$

$$a_2b_5+a_4b_4+a_5b_2 = 1\ (\text{συντελεστές τού } \mathsf{Y}^2), \tag{2}$$

$$a_1b_2 = a_1b_4=a_2b_1=a_4b_1=0, \tag{3}$$

Από την (1) έπεται ότι $a_1\neq 0$ και $b_1\neq 0$, και (μέσω τής (3))

$$a_2=a_4=b_2=b_4=0.$$

Τούτο είναι αδύνατο, διότι λόγω τής (2) θα έπρεπε να ισχύει

$$0=a_2b_5+a_4b_4+a_5b_2=1.$$

Άρα το F είναι ανάγωγο. Ωστόσο, το

$$\begin{aligned}\mathbf{V}(F) &= \left\{P=(x,y)\in\mathbb{A}^2_{\mathbb{R}}\;\middle|\; y^2+x^2\left(x-1\right)^2=0\right\}=\{(0,0),(1,0)\}\\ &= \{(0,0)\}\cup\{(1,0)\}=\mathbf{V}(\mathsf{Y}^2+\mathsf{X}^2)\cup\mathbf{V}(\mathsf{Y}^2+(\mathsf{X}-1)^2)\end{aligned}$$

είναι μη ανάγωγο αλγεβρικό σύνολο. □

A-1-42. (a) Έστω ότι τα V,W είναι δυο αλγεβρικά σύνολα εντός τού συσχετικού χώρου $\mathbb{A}^n_{\mathbf{k}}$ και ότι $V\subseteq W$. Εάν οι

$$V=V_1\cup\cdots\cup V_m,\quad W=W_1\cup\cdots\cup W_n$$

είναι οι αποσυνθέσεις των V και W, αντιστοίχως, σε ανάγωγες συνιστώσες, τότε για κάθε $i\in\{1,\ldots,m\}$ έχουμε

$$V_i\subseteq V\subseteq W\Longrightarrow V_i=W\cap V_i=\left(\bigcup_{j=1}^{n}W_j\right)\cap V_i=\bigcup_{j=1}^{n}\left(W_j\cap V_i\right)$$

$$\Longrightarrow V_i \subseteq W_{j_{(i)}} \cap V_i \subseteq W_{j_{(i)}}$$

για κάποιον δείκτη $j_{(i)} \in \{1, \dots, n\}$. Άρα κάθε ανάγωγη συνιστώσα τού V περιέχεται σε κάποια ανάγωγη συνιστώσα τού W.

(b) Εάν η $V = V_1 \cup V_2 \cup \cdots \cup V_m$ είναι η αποσύνθεση ενός αλγεβρικού συνόλου σε ανάγωγες συνιστώσες, τότε κατά το θεώρημα 1.6.13 έχουμε

$$V_i \nsubseteqq V_j, \ \ \forall i, j \in \{1, 2, \dots, m\}, \ i \neq j.$$

Εξ αυτού έπεται άμεσα ότι

$$V_i \nsubseteqq \bigcup_{j \in \{1,2,\dots,m\} \smallsetminus \{i\}} V_j,$$

για κάθε $i, 1 \leq i \leq m$. □

A-1-43. Κατά την πρόταση 1.3.1 (2) (b), $\mathbf{I}(\mathbb{A}^n_{\mathbf{k}}) = \{0\}$, ήτοι ένα πρώτο ιδεώδες. Σύμφωνα με την πρόταση 1.6.7 το $\mathbb{A}^n_{\mathbf{k}} = \mathbf{V}(0_{\mathbf{k}})$ είναι ανάγωγο αλγεβρικό σύνολο. □

A-1-44. Προφανώς, το $\mathsf{Y}^2 + \mathsf{X}^2 + 1$ είναι ανάγωγο στοιχείο τού $\mathbb{R}[\mathsf{X}, \mathsf{Y}]$ και

$$\mathbf{V}(\mathsf{Y}^2 + \mathsf{X}^2 + 1) = \varnothing \Longrightarrow \mathbf{I}(\mathbf{V}(\mathsf{Y}^2 + \mathsf{X}^2 + 1)) = \langle 1 \rangle \ = \mathbb{R}[\mathsf{X}, \mathsf{Y}] \supsetneqq \left\langle \mathsf{Y}^2 + \mathsf{X}^2 + 1 \right\rangle.$$

Άρα το πόρισμα 1.7.2 δεν ισχύει πάντοτε όταν το $\mathbf{V}(F)$ δεν είναι απειροπληθές. □

A-1-45. (a) Προφανώς,

$$\mathsf{Y}^2 - \mathsf{XY} - \mathsf{X}^2\mathsf{Y} + \mathsf{X}^3 = \mathsf{Y}(\mathsf{Y} - \mathsf{X}) - \mathsf{X}^2(\mathsf{Y} - \mathsf{X}) = \left(\mathsf{Y} - \mathsf{X}^2\right)(\mathsf{Y} - \mathsf{X}),$$

οπότε

$$\mathbf{V}(\mathsf{Y}^2 - \mathsf{XY} - \mathsf{X}^2\mathsf{Y} + \mathsf{X}^3) = \mathbf{V}(\mathsf{Y} - \mathsf{X}^2) \cup \mathbf{V}(\mathsf{Y} - \mathsf{X})$$

με $\mathbf{V}(\mathsf{Y} - \mathsf{X}^2) \nsubseteqq \mathbf{V}(\mathsf{Y} - \mathsf{X})$ και $\mathbf{V}(\mathsf{Y} - \mathsf{X}) \nsubseteqq \mathbf{V}(\mathsf{Y} - \mathsf{X}^2)$ τόσον εντός τού $\mathbb{A}^2_{\mathbb{R}}$ όσον και εντός τού $\mathbb{A}^2_{\mathbb{C}}$. Επειδή τα $\mathbf{V}(\mathsf{Y} - \mathsf{X}^2), \mathbf{V}(\mathsf{Y} - \mathsf{X})$ είναι απειροπληθή, αρκεί (λόγω τού πορίσματος 1.7.2) να δειχθεί ότι τα $\mathsf{Y} - \mathsf{X}^2$ και $\mathsf{Y} - \mathsf{X}$ είναι ανάγωγα. Για να αποφύγουμε την «εις άτοπον απαγωγή» και τις πράξεις με τους συντελεστές (πρβλ. άσκηση **A-1-41**) μπορούμε να χρησιμοποιήσουμε το *κριτήριο τού Eisenstein*: *Εάν ο* R *είναι μια* Π.Μ.Π. *και*

$$F = \sum_{j=0}^{n} a_j \mathsf{X}^j \in R[\mathsf{X}], \ \ \deg(F) = n \geq 1,$$

και υπάρχει ανάγωγο στοιχείο $p \in R$, *τέτοιο ώστε να πληρούνται οι συνθήκες*

$$p \nmid a_n, \ \ p \mid a_i, \ \forall i \in \{0, \dots, n-1\}, \ \ p^2 \nmid a_0,$$

τότε το F *είναι ανάγωγο στοιχείο τού* $\mathbf{Fr}(R)[\mathsf{X}]$. *Εάν, επιπροσθέτως,*

$$\mu\kappa\delta(a_0, \dots, a_n) \underset{\text{συν.}}{\sim} 1_R,$$

τότε το F *είναι ανάγωγο στοιχείο και τού* $R[\mathsf{X}]$.

Αρκεί να εφαρμόσουμε αυτό το κριτήριο αναγωγιμότητας για το $F = \mathsf{Y} - \mathsf{X}^2$ με

$$R = \mathbb{R}[\mathsf{Y}] \text{ (αντ., } R = \mathbb{C}[\mathsf{Y}]), \;\; a_2 = -1, \; a_1 = 0, \;\; a_0 = \mathsf{Y}, \;\; p = \mathsf{Y}.$$

(Παρομοίως εργαζόμαστε και με το $F = \mathsf{Y} - \mathsf{X}$.) Άρα οι ανάγωγες συνιστώσες τού αλγεβρικού συνόλου $\mathbf{V}(\mathsf{Y}^2 - \mathsf{XY} - \mathsf{X}^2\mathsf{Y} + \mathsf{X}^3)$ είναι οι $\mathbf{V}(\mathsf{Y} - \mathsf{X}^2)$ και $\mathbf{V}(\mathsf{Y} - \mathsf{X})$,τόσον εντός τού $\mathbb{A}^2_{\mathbb{R}}$ όσον και εντός τού $\mathbb{A}^2_{\mathbb{C}}$.

(b) Εφαρμόζοντας εκ νέου το προαναφερθέν κριτήριο τού Eisenstein για το πολυώνυμο $F = \mathsf{Y}^2 - \mathsf{X}(\mathsf{X}^2 - 1)$ με

$$R = \mathbb{R}[\mathsf{X}] \text{ (αντ., } R = \mathbb{C}[\mathsf{X}]), \;\; a_2 = 1, \; a_1 = 0, \;\; a_0 = -\mathsf{X}(\mathsf{X}^2 - 1), \;\; p = \mathsf{X},$$

διαπιστώνουμε ότι το F είναι ανάγωγο στοιχείο τόσον τού $\mathbb{R}[\mathsf{X}, \mathsf{Y}]$ όσον και τού $\mathbb{C}[\mathsf{X}, \mathsf{Y}]$. Επειδή το $\mathbf{V}(F)$ είναι (προφανώς) απειροπληθές, είναι κατ' ανάγκην και ανάγωγο αλγεβρικό σύνολο τόσον εντός τού $\mathbb{A}^2_{\mathbb{R}}$ όσον και εντός τού $\mathbb{A}^2_{\mathbb{C}}$. (Βλ. πόρισμα 1.7.2.) Εντός τού $\mathbb{A}^2_{\mathbb{R}}$ η καμπύλη που προκύπτει είναι το *φύλλο τού Καρτεσίου*, βλ. σχήμα 4. Τέλος, επειδή

$$\mathsf{X}^3 + \mathsf{X} - \mathsf{X}^2\mathsf{Y} - \mathsf{Y} = (\mathsf{X} - \mathsf{Y})(\mathsf{X}^2 + 1),$$

το $\mathsf{X} - \mathsf{Y}$ είναι ανάγωγο στοιχείο τόσον τού πολυωνυμικού δακτυλίου $\mathbb{R}[\mathsf{X}, \mathsf{Y}]$ όσον και τού $\mathbb{C}[\mathsf{X}, \mathsf{Y}]$, και το $\mathsf{X}^2 + 1$ ανάγωγο στοιχείο τού $\mathbb{R}[\mathsf{X}, \mathsf{Y}]$ και μη ανάγωγο στοιχείο τού $\mathbb{C}[\mathsf{X}, \mathsf{Y}]$. Η μοναδική ανάγωγη συνιστώσα τού $\mathbf{V}(\mathsf{X}^3 + \mathsf{X} - \mathsf{X}^2\mathsf{Y} - \mathsf{Y})$ εντός τού $\mathbb{A}^2_{\mathbb{R}}$ είναι η $\mathbf{V}(\mathsf{X} - \mathsf{Y})$ (διότι $\mathbf{V}(\mathsf{X}^2 + 1) = \varnothing$), ενώ οι ανάγωγες συνιστώσες τού ιδίου εντός τού $\mathbb{A}^2_{\mathbb{C}}$ είναι οι $\mathbf{V}(\mathsf{X} - \mathsf{Y})$, $\mathbf{V}(\mathsf{X} - i)$ και $\mathbf{V}(\mathsf{X} + i)$. □

A-1-46. Θα δοθούν αντιπαραδείγματα (που δείχνουν ότι τα θεωρήματα 1.8.1 και 1.8.2, καθώς και τα παρατεθέντα πορίσματά τους είναι εν γένει λανθασμένα όταν το $\mathbf{k}$ *δεν* είναι αλγεβρικώς κλειστό) για $\mathbf{k} = \mathbb{R}$.

► *Αντιπαράδειγμα στο θεώρημα* 1.8.1: Εάν $I := \langle \mathsf{X}^2 + 1 \rangle \subset \mathbb{R}[\mathsf{X}]$, τότε $\mathbf{V}(I) = \varnothing$.

► *Αντιπαράδειγμα στο θεώρημα* 1.8.2: Εάν $I := \langle \mathsf{X}^2 + 1 \rangle \subset \mathbb{R}[\mathsf{X}]$, τότε (κατά την άσκηση **A-1-19**)

$$\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(\varnothing) = \mathbb{R}[\mathsf{X}] \supsetneqq \mathrm{Rad}(I) = I.$$

► *Αντιπαράδειγμα στο πόρισμα* 1.8.3: Εάν $I := \langle \mathsf{X}^2 + 1 \rangle \subset \mathbb{R}[\mathsf{X}]$, τότε

$$\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(\varnothing) = \mathbb{R}[\mathsf{X}] \supsetneqq I.$$

► *Αντιπαράδειγμα στο πόρισμα* 1.8.4: Εάν $I := \langle (\mathsf{X}^2+1)\,\mathsf{X}\rangle \subset \mathbb{R}\,[\mathsf{X}]$, τότε το αλγεβρικό σύνολο $\mathbf{V}(I) = \{0\}$ είναι ένα σημείο τού $\mathbb{A}^1_{\mathbb{R}}$. Ωστόσο, το I δεν είναι μεγιστοτικό ιδεώδες τού $\mathbb{R}\,[\mathsf{X}]$, διότι $I \subsetneqq \langle \mathsf{X}\rangle \subsetneqq \mathbb{R}\,[\mathsf{X}]$. Επίσης, εάν $I := \langle F\rangle \subset \mathbb{R}[\mathsf{X},\mathsf{Y}]$, όπου

$$F := \mathsf{Y}^2 + \mathsf{X}^2\,(\mathsf{X}-1)^2\,,$$

τότε το F (κατά την άσκηση **A-1-41**) είναι ανάγωγο πολυώνυμο. Επειδή ο δακτύλιος $\mathbb{R}[\mathsf{X},\mathsf{Y}]$ είναι Π.Μ.Π (βλ. θεώρημα 1.1.36), το F είναι πρώτο στοιχείο τού $\mathbb{R}[\mathsf{X},\mathsf{Y}]$ (βλ. θεώρημα 1.1.18 (b)) και το I πρώτο ιδεώδες τού $\mathbb{R}[\mathsf{X},\mathsf{Y}]$ (επί τη βάσει τού (a) τής προτάσεως 1.1.16). Όμως το $\mathbf{V}(I)$ (και πάλι κατά την άσκηση **A-1-41**) είναι μη ανάγωγο αλγεβρικό σύνολο εντός τού $\mathbb{A}^2_{\mathbb{R}}$.

► *Αντιπαράδειγμα στο πόρισμα* 1.8.5: Εάν $F := (\mathsf{X}^2+1)\,(\mathsf{X}-a) \in \mathbb{R}\,[\mathsf{X}]$, $a \in \mathbb{R}$, τότε η

$$\mathbf{V}(F) = \mathbf{V}(\mathsf{X}^2+1) \cup \mathbf{V}(\mathsf{X}-a)$$

δεν αποτελεί την αποσύνθεση τού $\mathbf{V}(F)$ σε ανάγωγες συνιστώσες, καθότι

$$\mathbf{V}(\mathsf{X}^2+1) = \varnothing \subseteq \mathbf{V}(\mathsf{X}-a) = \{a\}.$$

► *Περί τού πορίσματος* 1.8.8: Έστω I ένα γνήσιο ιδεώδες τού $\mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n]$, όπου $\mathbf{k}$ *τυχόν* σώμα. Τότε η διάσταση $\dim_{\mathbf{k}}\left(\mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n]\,/\,I\right)$ είναι πεπερασμένη *εάν και μόνον εάν* υπάρχει σωματική, αλγεβρικώς κλειστή επέκταση L τού $\mathbf{k}$, ούτως ώστε το $\mathbf{V}(I)$ να είναι ένα πεπερασμένο σύνολο *εντός τού* $\mathbb{A}^n_L$. Βλ. T. Becker & V. Weispfenning: *Gröbner Bases. A Computational Approach to Commutative Algebra*, GTM, Vol. **141**, Springer-Verlag, Theorem 6.54, pp. 274-275 & Proposition 8.27, p. 347. □

A-1-47. (a) Είναι εύκολο να διαπιστώσει κανείς (στοιχειωδώς) ότι το $\mathsf{X}^2+\mathsf{Y}^2-1$ είναι ανάγωγο στοιχείο τού $\mathbb{C}[\mathsf{X},\mathsf{Y},\mathsf{Z}]$. Προφανώς,

$$\mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1,\mathsf{X}^2-\mathsf{Z}^2-1) = \mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1,\mathsf{Y}^2+\mathsf{Z}^2)$$

$$= \mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1,(\mathsf{Y}+i\mathsf{Z})\,(\mathsf{Y}-i\mathsf{Z})) = \mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1) \cap \mathbf{V}((\mathsf{Y}+i\mathsf{Z})\,(\mathsf{Y}-i\mathsf{Z}))$$

$$= \mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1) \cap (\mathbf{V}(\mathsf{Y}+i\mathsf{Z}) \cup \mathbf{V}(\mathsf{Y}-i\mathsf{Z}))$$

$$= \mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1,\mathsf{Y}+i\mathsf{Z}) \cup \mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1,\mathsf{Y}-i\mathsf{Z}).$$

(b) Έστω $V = \{(t,t^2,t^3) \in \mathbb{A}^3_{\mathbb{C}} \mid t \in \mathbb{C}\}$. Κατά την άσκηση **A-1-11** (a),

$$V = \mathbf{V}(\mathsf{Y}-\mathsf{X}^2,\mathsf{Z}-\mathsf{X}\mathsf{Y}).$$

Θεωρούμε τον επιμορφισμό δακτυλίων $\varphi : \mathbb{C}[\mathsf{X},\mathsf{Y},\mathsf{Z}] \longrightarrow \mathbb{C}[\mathsf{T}]$ τον οριζόμενο μέσω των συνθηκών

$$\varphi|_{\mathbb{C}} = \mathrm{Id}_{\mathbb{C}},\ \ \varphi(\mathsf{X}) = \mathsf{T},\ \ \varphi(\mathsf{Y}) = \mathsf{T}^2,\ \ \varphi(\mathsf{Z}) = \mathsf{T}^3.$$

Κατά το 1ο θεώρημα ισομορφισμών δακτυλίων (βλ. θεώρημα 1.1.10),

$$\mathbb{C}[\mathsf{X},\mathsf{Y},\mathsf{Z}]/\mathrm{Ker}(\varphi) \cong \mathbb{C}[\mathsf{T}],$$

όπου

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \left\{F \in \mathbb{C}[\mathsf{X},\mathsf{Y},\mathsf{Z}] \mid\ F\left(\mathsf{T},\mathsf{T}^2,\mathsf{T}^3\right) = 0\right\}\\ &= \left\{F \in \mathbb{C}[\mathsf{X},\mathsf{Y},\mathsf{Z}] \mid\ F(P) = 0,\ \forall P \in \mathbf{V}(\langle \mathsf{Y}-\mathsf{X}^2, \mathsf{Z}-\mathsf{XY}\rangle)\right\}\\ &= \mathbf{I}(\mathbf{V}(\mathsf{Y}-\mathsf{X}^2,\mathsf{Z}-\mathsf{XY})) = \mathbf{I}(V).\end{aligned}$$

Επειδή ο $\mathbb{C}[\mathsf{T}]$ είναι ακεραία περιοχή (βλ. πρόταση 1.1.22 (a)), το $\mathbf{I}(V)$ (σύμφωνα με το θεώρημα 1.1.13) είναι πρώτο και το V ανάγωγο αλγεβρικό σύνολο εντός τού $\mathbb{A}^3_{\mathbb{C}}$ (βλ. πρόταση 1.6.1). □

A-1-48. (a) Εάν $F \in R[\mathsf{X}]$ και $\deg(F) \in \{2,3\}$, τότε για ένα $a \in R$ ισχύουν οι ισοδυναμίες

$$F(a) = 0_R \Longleftrightarrow \mathsf{X}-a \mid F \Longleftrightarrow \exists G \in R[\mathsf{X}] : \deg(G) \in \{1,2\},\ F = (\mathsf{X}-a)\cdot G$$

$\Longleftrightarrow F$ μη ανάγωγο. Το (b) είναι προφανές λόγω τού (a). □

A-1-49. Έστω $\mathbf{k}$ ένα αλγεβρικώς κλειστό σώμα και έστω $\lambda \in \mathbf{k}$. Επειδή για το πολυώνυμο (δύο μεταβλητών)

$$F := \mathsf{Y}^2 - \mathsf{X}(\mathsf{X}-1)(\mathsf{X}-\lambda) \in \mathbf{k}[\mathsf{X},\mathsf{Y}] \cong (\mathbf{k}[\mathsf{X}])[\mathsf{Y}]$$

δεν υπάρχει μη μηδενικό πολυώνυμο $G \in \mathbf{k}[\mathsf{X}]$ με

$$\mathsf{X}(\mathsf{X}-1)(\mathsf{X}-\lambda) = G^2$$

(διότι $\deg(G^2) = 2\deg(G) \neq 3$), το F οφείλει να είναι ανάγωγο (σύμφωνα με την άσκηση **A-1-48** (b)). Ως εκ τούτου, βάσει τής ασκήσεως **A-1-14** και τού πορίσματος 1.7.2, το $\mathbf{V}(F) \subset \mathbb{A}^2_{\mathbf{k}}$ αποτελεί μια ανάγωγη συσχετική επίπεδη καμπύλη. □

A-1-50. Έστω $\mathbf{k}$ ένα σώμα και έστω $F \in \mathbf{k}[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geq 1$. Οι κλάσεις υπολοίπων $\{\overline{1}, \overline{\mathsf{X}}, \ldots, \left(\overline{\mathsf{X}}\right)^{n-1}\}$ εντός τού $\mathbf{k}[\mathsf{X}]/\langle F\rangle$ συγκροτούν μια βάση του ως διανυσματικού χώρου υπεράνω τού $\mathbf{k}$. Πράγματι· εάν $\lambda_1, \ldots, \lambda_n \in \mathbf{k}$ με

$$\sum_{j=1}^{n} \lambda_j \left(\overline{\mathsf{X}}\right)^{j-1} = I \Longrightarrow \sum_{j=1}^{n} \lambda_j \mathsf{X}^{j-1} \in I \Longrightarrow \exists G \in \mathbf{k}[\mathsf{X}] : \sum_{j=1}^{n} \lambda_j \mathsf{X}^{j-1} = G\cdot F,$$

τότε $\deg(\sum_{j=1}^{n}\lambda_j \mathsf{X}^{j-1}) \leq n-1$ και είτε $\deg(G\cdot F)\geq n$ είτε $G=0$. Άρα

$$\lambda_1 = \cdots = \lambda_n = 0_{\mathbf{k}},$$

οπότε το $\{\overline{1}, \overline{\mathsf{X}}, \ldots, \left(\overline{\mathsf{X}}\right)^{n-1}\}$ είναι γραμμικώς ανεξάρτητο υπεράνω τού $\mathbf{k}$. Εξάλλου, εάν

$$(G+\langle F\rangle)\in \mathbf{k}\left[\mathsf{X}\right]/\langle F\rangle\,,\ \ G=\sum_{j=0}^{m} a_j\mathsf{X}^j,\ m\in\mathbb{N}_0,\ a_j\in\mathbf{k},\ \forall j\in\{0,\ldots,m\},$$

και $a_m\neq 0_{\mathbf{k}}$, τότε, εάν $m\leq n-1$, έχουμε $G+\langle F\rangle=\sum_{j=0}^{m} a_j\overline{\mathsf{X}}^j$, ενώ εάν $m\geq n$,

$$\exists! G_1, G_2\in \mathbf{k}\left[\mathsf{X}\right] : G = G_1\cdot F + G_2$$

και είτε $0\leq \deg(G_2)<n=\deg(F)$ είτε $G_2=0$ (βάσει τού αλγορίθμου τής διαιρέσεως), οπότε

$$G+\langle F\rangle = (G_1\cdot F+G_2)+\langle F\rangle = G_2+\langle F\rangle\,.$$

Κατά συνέπειαν, το $\{\overline{1}, \overline{\mathsf{X}}, \ldots, \left(\overline{\mathsf{X}}\right)^{n-1}\}$ παράγει τον $\mathbf{k}\left[\mathsf{X}\right]/\langle F\rangle$ ως διανυσματικό χώρο υπεράνω τού $\mathbf{k}$. □

A-1-51. Έστω $I:=\left\langle \mathsf{Y}^2-\mathsf{X}^2, \mathsf{Y}^2+\mathsf{X}^2\right\rangle\subset\mathbb{C}[\mathsf{X},\mathsf{Y}]$. Προφανώς,

$$\begin{aligned}\mathbf{V}\left(I\right) &= \mathbf{V}\left(\mathsf{Y}^2-\mathsf{X}^2,\mathsf{Y}^2+\mathsf{X}^2\right)=\mathbf{V}\left(\left(\mathsf{Y}-\mathsf{X}\right)\left(\mathsf{Y}+\mathsf{X}\right),\left(\mathsf{Y}-i\mathsf{X}\right)\left(\mathsf{Y}+i\mathsf{X}\right)\right)\\ &= \left(\mathbf{V}\left(\mathsf{Y}-\mathsf{X}\right)\cup\mathbf{V}\left(\mathsf{Y}+\mathsf{X}\right)\right)\cap\left(\mathbf{V}\left(\mathsf{Y}-i\mathsf{X}\right)\cup\mathbf{V}\left(\mathsf{Y}+i\mathsf{X}\right)\right)\\ &= \{(0,0)\}\Longrightarrow \sharp(\mathbf{V}\left(I\right))=1.\end{aligned}$$

Από την άλλη μεριά, σύμφωνα με όσα ειπώθηκαν στην απόδειξη τού πορίσματος 1.8.8, το σύνολο $\{\overline{1}, \overline{\mathsf{X}}, \overline{\mathsf{Y}}, \overline{\mathsf{XY}}\}$ παράγει τον $\mathbb{C}[\mathsf{X},\mathsf{Y}]/I$ ως διανυσματικό χώρο υπεράνω τού $\mathbb{C}$. Θεωρούμε $\lambda_1,\lambda_2,\lambda_3,\lambda_4\in\mathbb{C}$ με

$$\lambda_1+\lambda_2\overline{\mathsf{X}}+\lambda_3\overline{\mathsf{Y}}+\lambda_4\overline{\mathsf{XY}}=I\Longrightarrow \lambda_1+\lambda_2\mathsf{X}+\lambda_3\mathsf{Y}+\lambda_4\mathsf{XY}\in I$$

$$\Longrightarrow \exists G_1,G_2\in\mathbb{C}[\mathsf{X},\mathsf{Y}]:\lambda_1+\lambda_2\mathsf{X}+\lambda_3\mathsf{Y}+\lambda_4\mathsf{XY}=G_1\cdot\left(\mathsf{Y}^2-\mathsf{X}^2\right)+G_2\cdot\left(\mathsf{Y}^2+\mathsf{X}^2\right),$$

Επειδή $\deg(\lambda_1+\lambda_2\mathsf{X}+\lambda_3\mathsf{Y}+\lambda_4\mathsf{XY})\leq 2$ και το $\lambda_1+\lambda_2\mathsf{X}+\lambda_3\mathsf{Y}+\lambda_4\mathsf{XY}$ δεν περιέχει τα μονώνυμα X^2, Y^2, ενώ είτε

$$\deg(G_1\cdot\left(\mathsf{Y}^2-\mathsf{X}^2\right)+G_2\cdot\left(\mathsf{Y}^2+\mathsf{X}^2\right))\geq 2$$

είτε $G_1=G_2=0$, έχουμε κατ' ανάγκην $G_1=G_2=0$ και $\lambda_1=\lambda_2=\lambda_3=\lambda_4=0$. Άρα το $\{\overline{1}, \overline{\mathsf{X}}, \overline{\mathsf{Y}}, \overline{\mathsf{XY}}\}$ αποτελεί βάση τού $\mathbb{C}$-δ.χ. $\mathbb{C}[\mathsf{X},\mathsf{Y}]/I$ και

$$\dim_{\mathbb{C}}\left(\mathbb{C}[\mathsf{X},\mathsf{Y}]/I\right)=4>1=\sharp(\mathbf{V}\left(I\right)).$$

Εν προκειμένω, η ανισοϊσότητα που αποδείχθηκε στο πόρισμα 1.8.8 ισχύει ως *γνήσια ανισότητα*.

(*Σημείωση*: Μια παραλλαγή τής αποδείξεως, χωρίς να γίνει επίκληση τής αποδείξεως τού πορίσματος 1.8.8 έχει ως εξής: Έστω $J := \langle \mathsf{X}^2, \mathsf{Y}^2 \rangle \subset \mathbb{C}[\mathsf{X}, \mathsf{Y}]$. Προφανώς,

$$\left.\begin{array}{l} \mathsf{Y}^2 - \mathsf{X}^2 \in J \\ \mathsf{Y}^2 + \mathsf{X}^2 \in J \end{array}\right\} \Longrightarrow I \subseteq J,$$

και

$$\left.\begin{array}{l} \mathsf{X}^2 = \frac{1}{2}\left(\mathsf{Y}^2 + \mathsf{X}^2\right) - \frac{1}{2}\left(\mathsf{Y}^2 - \mathsf{X}^2\right) \in I \\ \mathsf{Y}^2 = \frac{1}{2}\left(\mathsf{Y}^2 + \mathsf{X}^2\right) + \frac{1}{2}\left(\mathsf{Y}^2 - \mathsf{X}^2\right) \in I \end{array}\right\} \Longrightarrow J \subseteq I,$$

οπότε $I = J$. Για κάθε $F \in \mathbb{C}[\mathsf{X}, \mathsf{Y}]$ υπάρχουν $\mu_1, \mu_2, \mu_3, \mu_4 \in \mathbb{C}$ με

$$F + J = \mu_1 + \mu_2\overline{\mathsf{X}} + \mu_3\overline{\mathsf{Y}} + \mu_4\overline{\mathsf{XY}},$$

απ' όπου έπεται ότι το $\{\overline{1}, \overline{\mathsf{X}}, \overline{\mathsf{Y}}, \overline{\mathsf{XY}}\}$ παράγει τον $\mathbb{C}$-δ.χ. $\mathbb{C}[\mathsf{X}, \mathsf{Y}] \,/\, J$. Εν συνεχεία, θεωρούμε $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{C}$ με

$$\lambda_1 + \lambda_2\overline{\mathsf{X}} + \lambda_3\overline{\mathsf{Y}} + \lambda_4\overline{\mathsf{XY}} = J \Longrightarrow \lambda_1 + \lambda_2\mathsf{X} + \lambda_3\mathsf{Y} + \lambda_4\mathsf{XY} \in J$$

$$\Longrightarrow \exists G_1, G_2 \in \mathbb{C}[\mathsf{X}, \mathsf{Y}] : \lambda_1 + \lambda_2\mathsf{X} + \lambda_3\mathsf{Y} + \lambda_4\mathsf{XY} = G_1 \cdot \mathsf{X}^2 + G_2 \cdot \mathsf{Y}^2.$$

Για $\mathsf{X} = 0$ λαμβάνουμε

$$\lambda_1 + \lambda_3\mathsf{Y} = G_2(0, \mathsf{Y}) \cdot \mathsf{Y}^2 \Longrightarrow G_2(0, \mathsf{Y}) = 0, \;\; \lambda_1 = \lambda_3 = 0.$$

Για $\mathsf{Y} = 0$ λαμβάνουμε

$$\lambda_1 + \lambda_2\mathsf{X} + \lambda_3\mathsf{Y} + \lambda_4\mathsf{XY} = \lambda_2\mathsf{X} = G_1(\mathsf{X}, 0) \cdot \mathsf{X}^2 \Longrightarrow G_1(\mathsf{X}, 0) = 0, \;\; \lambda_2 = 0.$$

Επειδή λοιπόν

$$\lambda_1 + \lambda_2\mathsf{X} + \lambda_3\mathsf{Y} + \lambda_4\mathsf{XY} = \lambda_4\mathsf{XY} = G_1 \cdot \mathsf{X}^2 + G_2 \cdot \mathsf{Y}^2,$$

έχουμε αναγκαστικώς $G_1 = G_2 = 0$ και κατ' επέκτασιν $\lambda_4 = 0$. Άρα το $\{\overline{1}, \overline{\mathsf{X}}, \overline{\mathsf{Y}}, \overline{\mathsf{XY}}\}$ αποτελεί βάση τού $\mathbb{C}$-δ.χ. $\mathbb{C}[\mathsf{X}, \mathsf{Y}] \,/\, J$.) □

A-1-52. Έστω $\mathbf{k}$ ένα αλγεβρικώς κλειστό σώμα και έστω I ένα ριζικό ιδεώδες I τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Θεωρούμε την αποσύνθεση

$$\mathbf{V}(I) = V_1 \cup \cdots \cup V_r$$

τού $\mathbf{V}(I)$ σε ανάγωγες συνιστώσες. Σύμφωνα με το θεώρημα θέσεων μηδενισμού τού Hilbert (βλ. θεώρημα 1.8.2),

$$I = \mathrm{Rad}(I) = \mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(V_1 \cup \cdots \cup V_r) = \mathbf{I}(V_1) \cap \cdots \cap \mathbf{I}(V_r)$$

Κατά την πρόταση 1.6.1 το $\mathbf{I}(V_j)$ είναι πρώτο ιδεώδες τού πολυωνυμικού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ για κάθε $j \in \{1, \ldots, r\}$. □

Α-1-53. (a) Έστω R μια Π.Μ.Π. και έστω $\mathfrak{p} = \langle t \rangle$, $t \in R$, ένα κύριο, γνήσιο, πρώτο ιδεώδες. Υποθέτουμε ότι υπάρχει κάποιο κύριο, πρώτο ιδεώδες Q τής R, ούτως ώστε να ισχύει $\{0\} \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{p}$. Κατ' αρχάς παρατηρούμε ότι $t \notin \mathfrak{q}$ (διότι αλλιώς $\mathfrak{q} = \mathfrak{p}$) και ότι για τυχόν $a \in \mathfrak{q}$ με $a = qt$, $q \in R$, έχουμε κατ' ανάγκην $q \in \mathfrak{q}$. (Επειδή $\mathfrak{q} \ni a = qt$ και το $\mathfrak{q}$ είναι πρώτο και $t \notin \mathfrak{q}$, έχουμε $q \in \mathfrak{q}$.) Επιπροσθέτως, κανένα στοιχείο τού $\mathfrak{q}$ δεν είναι ανάγωγο στοιχείο τού R. (Εάν υπήρχε κάποιο ανάγωγο $a \in (R \setminus (R^\times \cup \{0\})) \cap \mathfrak{q}$, επειδή $a = qt$ για κάποιο $q \in \mathfrak{q}$, θα έπρεπε είτε $q \in R^\times$ είτε $t \in R^\times$. Αυτό θα σήμαινε ότι είτε $\mathfrak{q} = R$ είτε $\mathfrak{p} = R$, ενδεχόμενα εξ υποθέσεως αποκλεισθέντα.)

Εν συνεχεία, θεωρούμε τυχόν $a \in \mathfrak{q}$. Επειδή ο R είναι Π.Μ.Π., το a θα είναι συντροφικό ενός γινομένου αναγώγων στοιχείων τού R. Συγκεκριμένα, βάσει των όσων προαναφέρθησαν, το a θα γράφεται υπό τη μορφή $a = up_1p_2 \cdots p_k$, όπου $u \in R^\times$ και $p_1, p_2, \ldots, p_k$ ανάγωγα στοιχεία *ανήκοντα στο* $R \setminus \mathfrak{q}$. Επειδή $a = qt$ για κάποιο $q \in \mathfrak{q}$, το t θα διαιρεί το $p_1p_2 \cdots p_k$. Εξάλλου, επειδή το $\mathfrak{p} = \langle t \rangle$ είναι εξ υποθέσεως γνήσιο, πρώτο ιδεώδες, το t είναι πρώτο στοιχείο τού R (βλ. πρόταση 1.1.16 (a)) και κατ' επέκτασιν ανάγωγο (βλ. θεώρημα 1.1.18 (b)). Τούτο έχει ως συνέπεια ότι $\exists i \in \{1, \ldots, k\}$ και $w \in R^\times$ με $wt = p_i$. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $i = 1$. Προφανώς, κατά τα προαναφερθέντα,

$$\mathfrak{q} \ni (uw)^{-1} a = (p_2 \cdots p_k)\, t \Longrightarrow p_2 \cdots p_k \in \mathfrak{q}.$$

Επειδή $p_2 \cdots p_k \in \mathfrak{q} \subsetneqq \mathfrak{p} = \langle t \rangle$, το t θα διαιρεί και το $p_2 \cdots p_k$. Μέσω τής ιδίας επιχειρηματολογίας αποδεικνύουμε ότι $p_3 \cdots p_k$ (όταν $k \geq 3$). Επαναλαμβάνοντας την εν λόγω διαδικασία άλλες $k-3$ φορές (όταν $k \geq 4$) συμπεραίνουμε τελικώς ότι $p_k \in \mathfrak{q}$. Άτοπο!

(b) Έστω $V = \mathbf{V}(F)$ μια ανάγωγη υπερεπιφάνεια εντός τού $\mathbb{A}^n_{\mathbf{k}}$ (όπου $\mathbf{k}$ ένα αλγεβρικώς κλειστό σώμα). Υποθέτουμε ότι υπάρχει κάποιο ανάγωγο αλγεβρικό σύνολο W, τέτοιο ώστε να ισχύει $V \subsetneqq W \subsetneqq \mathbb{A}^n_{\mathbf{k}}$. Τότε, σύμφωνα με το πόρισμα 1.8.5, και τα (1), (2) (b) και 5 (a) τής προτάσεως 1.3.1, έπεται ότι

$$\{0\} = \mathbf{I}(\mathbb{A}^n_{\mathbf{k}}) \subsetneqq \mathbf{I}(W) \subsetneqq \mathbf{I}(\mathbf{V}(F)) = \langle F \rangle .$$

Άτοπο επί τη βάσει όσων έχουμε αποδείξει στο (a)! □

Α-1-54. Έστω $I = \left\langle \mathsf{X}^2 - \mathsf{Y}^3, \mathsf{Y}^2 - \mathsf{Z}^3 \right\rangle \subset \mathbf{k}[\mathsf{X}, \mathsf{Y}, \mathsf{Z}]$ (όπου το $\mathbf{k}$ είναι ένα αλγεβρικώς κλειστό σώμα) και έστω $\alpha : \mathbf{k}[\mathsf{X}, \mathsf{Y}, \mathsf{Z}] \to \mathbf{k}[\mathsf{T}]$ ο ομομορφισμός δακτυλίων ο οριζόμενος μέσω των συνθηκών $\alpha(\mathsf{X}) = \mathsf{T}^9, \alpha(\mathsf{Y}) = \mathsf{T}^6$ και $\alpha(\mathsf{Z}) = \mathsf{T}^4$.

(a) Έστω $\overline{F} = F + I$ ένα (μη μηδενικό) στοιχείο τού πηλικοδακτυλίου $\mathbf{k}[\mathsf{X},\mathsf{Y},\mathsf{Z}]/I$, όπου

$$F = \sum \lambda_{(i,j,k)} \mathsf{X}^i \mathsf{Y}^j \mathsf{Z}^k.$$

Υπενθυμίζουμε τον *αλγόριθμο τής διαιρέσεως πολυωνύμων* με συντελεστές ειλημμένους από οιαδήποτε ακεραία περιοχή R: *Εάν τα* $F, G \in R[\mathsf{X}]$ *είναι δυο μη μηδενικά πολυώνυμα με* $\mathbf{LC}(G) \in R^\times$, *τότε υπάρχουν μονοσημάντως ορισμένα πολυώνυμα* $Q, Q' \in R[\mathsf{X}]$ *για τα οποία ισχύει*

$$F = G \cdot Q + Q', \quad \deg(Q') < \deg(G).$$

Εφαρμόζοντάς τον για $R = \mathbf{k}[\mathsf{Y},\mathsf{Z}]$, F το προαναφερθέν και $G = \mathsf{X}^2 - \mathsf{Y}^3$ λαμβάνουμε

$$F = \left(\mathsf{X}^2 - \mathsf{Y}^3\right) \cdot Q + Q',$$

όπου ο βαθμός $\deg_{\mathsf{X}}(Q')$ τού Q' ως πολυωνύμου τής μεταβλητής X είναι $0, 1$ ή $-\infty$. Κατά συνέπειαν, $Q' = a + b\mathsf{X}$ για κατάλληλα πολυώνυμα $a, b \in \mathbf{k}[\mathsf{Y},\mathsf{Z}]$. Εν συνεχεία, εφαρμόζοντάς τον άλλη μία φορά για $R = \mathbf{k}[\mathsf{X},\mathsf{Z}]$, όπου F το Q' και $G = \mathsf{Y}^2 - \mathsf{Z}^3$ λαμβάνουμε

$$Q' = a + b\mathsf{X} = \left(\mathsf{Y}^2 - \mathsf{Z}^3\right) \cdot Q'' + Q''', \ \deg_{\mathsf{Y}}(Q''') \in \{-\infty, 0, 1\},$$

οπότε $Q''' = \Xi_1 + \Xi_2\mathsf{Y}$, για κατάλληλα πολυώνυμα $\Xi_1, \Xi_2 \in \mathbf{k}[\mathsf{X},\mathsf{Z}]$ με

$$\deg_{\mathsf{X}}(\Xi_1), \deg_{\mathsf{X}}(\Xi_2) \in \{-\infty, 0, 1\}.$$

Θέτοντας τα Ξ_1, Ξ_2 υπό τη μορφή

$$\Xi_1 = A + B\mathsf{X}, \ \ \Xi_2 = C + D\mathsf{X},$$

για κατάλληλα $A, B, C, D \in \mathbf{k}[\mathsf{Z}]$, λαμβάνουμε τελικώς

$$F = \left(\mathsf{X}^2 - \mathsf{Y}^3\right) \cdot Q + \left(\mathsf{Y}^2 - \mathsf{Z}^3\right) \cdot Q'' + (A + B\mathsf{X}) + (C + D\mathsf{X})\,\mathsf{Y}$$

$$\Longrightarrow \overline{F} = ((A + B\mathsf{X}) + (C + D\mathsf{X})\,\mathsf{Y}) + I = \overline{A} + \overline{B\mathsf{X}} + \overline{C\mathsf{Y}} + \overline{D\mathsf{X}\mathsf{Y}}.$$

(b) Εάν $F = A + B\mathsf{X} + C\mathsf{Y} + D\mathsf{X}\mathsf{Y}$, όπου $A, B, C, D \in \mathbf{k}[\mathsf{Z}]$, και

$$\alpha(F) = \alpha(A + B\mathsf{X} + C\mathsf{Y} + D\mathsf{X}\mathsf{Y}) = \alpha(A) + \alpha(B)\,\mathsf{T}^9 + \alpha(C)\,\mathsf{T}^6 + \alpha(D)\,\mathsf{T}^{15} = 0,$$

τότε, το $\alpha(A)$ θα είναι ένα πολυώνυμο (ως πολυώνυμο με μεταβλητή του το T) με δυνάμεις τού T ανήκουσες στο σύνολο $\{4k \mid k \in \mathbb{N}_0\}$, το $\alpha(B)\,\mathsf{T}^9$ πολυώνυμο με δυνάμεις τού T ανήκουσες στο σύνολο $\{4k+9 \mid k \in \mathbb{N}_0\}$, το $\alpha(C)\,\mathsf{T}^6$ πολυώνυμο με δυνάμεις τού T ανήκουσες στο σύνολο $\{4k+6 \mid k \in \mathbb{N}_0\}$ και το $\alpha(D)\,\mathsf{T}^{15}$ πολυώνυμο με δυνάμεις τού T ανήκουσες στο σύνολο $\{4k+15 \mid k \in \mathbb{N}_0\}$. Προφανώς, για κάθε $k \in \mathbb{N}_0$ ισχύει

$$4k \equiv 0 (\mathrm{mod}\ 4), \ \ 4k+9 \equiv 0 (\mathrm{mod}\ 5), \ \ 4k+6 \equiv 0 (\mathrm{mod}\ 2), \ \ 4k+15 \equiv 0 (\mathrm{mod}\ 3).$$

Εξ αυτού εξάγεται το συμπέρασμα ότι $F = 0$.

(c) Ορίζοντας τον ισομορφισμό

$$\psi : \mathbf{k}\left[\mathsf{X},\mathsf{Y},\mathsf{Z}\right]/I \longrightarrow \mathbf{k}\left[\mathsf{T}^9,\mathsf{T}^6,\mathsf{T}^4\right], \quad \psi(F+I) := \alpha(F), \ \ \forall F \in \mathbf{k}\left[\mathsf{X},\mathsf{Y},\mathsf{Z}\right],$$

μεταξύ τού θεωρηθέντος πηλικοδακτυλίου και τής ακεραίας περιοχής $\mathbf{k}\left[\mathsf{T}^9,\mathsf{T}^6,\mathsf{T}^4\right]$ διαπιστώνουμε ότι το I είναι πρώτο και -κατ' επέκτασιν- ριζικό ιδεώδες (βλ. θεώρημα 1.1.13 και άσκηση **A-1-18**) και (μέσω τού (b), τού θεωρήματος 1.8.2 των θέσεων μηδενισμού τού Hilbert και τού πορίσματος 1.8.4) ότι $I = \mathrm{Rad}(I) = \mathbf{I}(\mathbf{V}(I))$ με το $\mathbf{V}(I)$ ανάγωγο αλγεβρικό σύνολο εντός τού $\mathbb{A}^3_{\mathbf{k}}$. □

A-1-55. Ο εγκλεισμός " $\supseteq$ " έχει αποδειχθεί στο (c) τού θεωρήματος 1.4.12. Ο αντίστροφος εγκλεισμός " $\subseteq$ " οφείλεται στο ότι, σύμφωνα με την υπόθεσή μας, το $\mathbf{k}$ είναι αλγεβρικώς κλειστό. Έστω τυχόν $F \in \mathbf{I}(\mathbf{V}(I)\smallsetminus\mathbf{V}(J))$. Εάν $G \in J$, τότε το FG μηδενίζεται στο $\mathbf{V}(I)$, διότι το F μηδενίζεται στο $\mathbf{V}(I)\smallsetminus\mathbf{V}(J)$ και το G μηδενίζεται στο $\mathbf{V}(J)$. Επομένως, από το θεώρημα μηδενικών θέσεων τού Hilbert 1.8.2 προκύπτει ότι

$$FG \in \mathrm{Rad}(I) = I.$$

Άρα

$$FG \in I, \ \forall G \in J \Longrightarrow \mathbf{I}(\mathbf{V}(I)\smallsetminus\mathbf{V}(J)) \subseteq I : J$$

$$\Longrightarrow \mathbf{V}(I:J) \subseteq \mathbf{V}(\mathbf{I}(\mathbf{V}(I)\smallsetminus\mathbf{V}(J))) = \mathrm{cl}_{\mathcal{T}_{\mathrm{Zar}}}\left(\mathbf{V}(I)\smallsetminus\mathbf{V}(J)\right).$$

(Βλ. το (3) τής προτάσεως 1.2.3 και την πρόταση 1.3.4.) □

A-1-56. (a) Σύμφωνα με το θεώρημα μηδενικών θέσεων τού Hilbert 1.8.2, το (a) τού θεωρήματος 1.4.12 και το (5) (a) τής προτάσεως 1.3.1 έχουμε

$$\begin{aligned}\mathrm{Rad}(\mathbf{I}(V)+\mathbf{I}(W)) &= \mathbf{I}(\mathbf{V}(\mathbf{I}(V)+\mathbf{I}(W)))\\ &= \mathbf{I}(\mathbf{V}(\mathbf{I}(V))\cap\mathbf{V}(\mathbf{I}(W))) = \mathbf{I}(V\cap W).\end{aligned}$$

(b) Σύμφωνα με το θεώρημα μηδενικών θέσεων τού Hilbert 1.8.2, το (b) τού θεωρήματος 1.4.12 και το (5) (a) τής προτάσεως 1.3.1 έχουμε

$$\begin{aligned}\mathrm{Rad}(\mathbf{I}(V)\mathbf{I}(W)) &= \mathbf{I}(\mathbf{V}(\mathbf{I}(V)\mathbf{I}(W)))\\ &= \mathbf{I}(\mathbf{V}(\mathbf{I}(V))\cup\mathbf{V}(\mathbf{I}(W))) = \mathbf{I}(V\cup W).\end{aligned}$$

Εξάλλου, από το (e) τής ασκήσεως **A-1-28**, το θεώρημα μηδενικών θέσεων τού Hilbert 1.8.2 και το (4) (b) τής προτάσεως 1.3.1 συνάγουμε ότι

$$\begin{aligned}\mathrm{Rad}(\mathbf{I}(V)\mathbf{I}(W)) &= \mathrm{Rad}(\mathbf{I}(V))\cap\mathrm{Rad}(\mathbf{I}(W))\\ &= \mathbf{I}(\mathbf{V}(\mathbf{I}(V)))\cap\mathbf{I}(\mathbf{V}(\mathbf{I}(V)))\\ &= \mathbf{I}(V)\cap\mathbf{I}(W).\end{aligned}$$

Κατά συνέπειαν, $\mathbf{I}(V \cup W) = \mathrm{Rad}(\mathbf{I}(V)\mathbf{I}(W)) = \mathbf{I}(V) \cap \mathbf{I}(W)$. □

A-1-57. (a)⇒(b): Εάν τα I, J είναι πρώτα μεταξύ τους, τότε

$$\exists F \in I,\ G \in J : F + G = 1_{\mathbf{k}},$$

οπότε $\mathbf{V}(I) \cap \mathbf{V}(J) = \varnothing$, διότι εάν υπήρχε $P \in \mathbf{V}(I) \cap \mathbf{V}(J)$, θα καταλήγαμε στο εξής άτοπο συμπέρασμα:

$$1_{\mathbf{k}} = (F + G)(P) = F(P) + G(P) = 0_{\mathbf{k}} + 0_{\mathbf{k}} = 0_{\mathbf{k}}.$$

(b)⇒(a): Εάν $\varnothing = \mathbf{V}(I) \cap \mathbf{V}(J) = \mathbf{V}(I + J)$ (πρβλ. θεώρημα 1.4.12 (a)), τότε, σύμφωνα με τα θεωρήματα 1.8.1 και 1.8.2, και την άσκηση **A-1-29**, ισχύει

$$\mathbf{I}(\mathbf{V}(I + J)) = \mathbf{I}(\varnothing) = \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \Longrightarrow \mathrm{Rad}(I + J) = \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] = \langle 1_{\mathbf{k}} \rangle$$

$$\Longrightarrow \exists n \in \mathbb{N} : (\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n])^n \,(= \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]) \subseteq I + J \Longrightarrow \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] = I + J,$$

οπότε τα I, J είναι πρώτα μεταξύ τους. □

A-1-58. Όταν ο δακτύλιος S είναι μοδιακώς πεπερασμένος υπεράνω τού R,

$$\exists s_1, \ldots, s_\nu \in S : S = \sum_{i=1}^{\nu} R\, s_i,$$

οπότε (εξ ορισμού) $S = R\,[s_1, s_2, \ldots, s_\nu]$ (ήτοι είναι και δακτυλιακώς πεπερασμένος υπεράνω τού R). □

A-1-59. Ο δακτύλιος πολυωνύμων μίας μεταβλητής $S = R[\mathsf{X}]$ είναι (προφανώς) δακτυλιακώς πεπερασμένος (από την απροσδιόριστο X) υπεράνω τού R, δίχως όμως να είναι και μοδιακώς πεπερασμένος υπεράνω αυτού, αφού κάθε R-υπομόδιος τού S, ο οποίος παράγεται από ένα πεπερασμένο υποσύνολο $\{F_1, \ldots, F_k\}$, είναι τής μορφής

$$\sum_{i=1}^{k} R\, F_i = \left\{ \sum_{i=1}^{k} r_i\, F_i \ \mid\ r_1, \ldots, r_k \in R \right\},$$

οπότε δεν μπορεί να ταυτισθεί με ολόκληρο τον $S = R[\mathsf{X}]$. □

A-1-60. Έστω L μια πεπερασμένως παραγόμενη δακτυλιακή επέκταση τού $\mathbf{k}$, όπου τα $\mathbf{k}$ και L είναι σώματα. Τότε

$$\exists v_1, \ldots, v_n \in L : L = \mathbf{k}[v_1, \ldots, v_n].$$

Το σώμα κλασμάτων $\mathbf{k}\left(v_1,\ldots,v_n\right)$ τού $\mathbf{k}[v_1,\ldots,v_n]$ είναι το ελάχιστο υπόσωμα τού L που περιέχει τα $v_1,\ldots,v_n$ και (εξ υποθέσεως) $L=\mathbf{k}[v_1,\ldots,v_n]$, οπότε έχουμε

$$\mathbf{k}[v_1,\ldots,v_n]\supseteq\mathbf{k}\left(v_1,\ldots,v_n\right).$$

Όμως, από τον ορισμό τού σώματος πηλίκων,

$$\mathbf{k}[v_1,\ldots,v_n]\subseteq\mathbf{k}\left(v_1,\ldots,v_n\right).$$

Άρα το $L=\mathbf{k}\left(v_1,\ldots,v_n\right)$ είναι όντως μια πεπερασμένως παραγόμενη σωματική επέκταση τού $\mathbf{k}$. □

A-1-61. Το σώμα $L=\mathbf{k}(\mathsf{X})$ (ήτοι το *σώμα των ρητών συναρτήσεων μίας μεταβλητής*) είναι μια πεπερασμένως παραγόμενη σωματική επέκταση τού $\mathbf{k}$ (επί τη βάσει τού ορισμού τού L). Ωστόσο, δεν είναι και πεπερασμένως παραγόμενη δακτυλιακή επέκταση τού $\mathbf{k}$. Πράγματι· εάν υπήρχαν $f_1,\ldots,f_n\in L=\mathbf{k}(\mathsf{X})$,

$$f_j=\frac{F_j}{G_j},\ \ F_j\in\mathbf{k}\left[\mathsf{X}\right],\ G_j\in\mathbf{k}\left[\mathsf{X}\right]\smallsetminus\{0_{\mathbf{k}[\mathsf{X}]}\},\ \forall j\in\{1,\ldots,n\},$$

τέτοια ώστε να ισχύει $L=\mathbf{k}[f_1,\ldots,f_n]$, τότε για κάθε $f\in L\smallsetminus\mathbf{k}$ θα είχαμε

$$f=\sum\lambda_{(i_1,\ldots,i_n)}\,f_1^{i_1}\,\cdots\,f_n^{i_n},\ \ \lambda_{(i_1,\ldots,i_n)}\in\mathbf{k},$$

με

$$f=\sum\lambda_{(i_1,\ldots,i_n)}\,\frac{F_1^{i_1}\,\cdots\,F_n^{i_n}}{G_1^{i_1}\,\cdots\,G_n^{i_n}}=\frac{H}{H'},\qquad(*)$$

για κατάλληλα $H,H'\in\mathbf{k}\left[\mathsf{X}\right]$, όπου ο παρονομαστής H' θα μπορούσε να περιέχει το πολύ εκείνα τα ανάγωγα πολυώνυμα, τα οποία διαιρούν κάποιο G_j, $j\in\{1,\ldots,n\}$. Εάν επιλέγαμε ένα ανάγωγο πολυώνυμο $\Xi\in\mathbf{k}\left[\mathsf{X}\right]$ με $\Xi\nmid G_j$, για κάθε $j\in\{1,\ldots,n\}$, τότε θα καταλήγαμε σε άτοπο, καθόσον (λόγω τού μονοσημάντου τής παραγοντοποιήσεως σε ανάγωγους παράγοντες εντός τού $\mathbf{k}\left[\mathsf{X}\right]$) το $f=\frac{1}{\Xi}\in L\smallsetminus\mathbf{k}$ *δεν θα μπορούσε να γραφεί*[1] υπό τη μορφή (*). Αρκεί λοιπόν να αποδείξουμε *την ύπαρξη* ενός τέτοιου Ξ. Προς τούτο θα χρησιμοποιήσουμε την άσκηση **A-1-5**. Βάσει αυτής διαπιστώνουμε άμεσα ότι το σύνολο $\mathcal{A}$ των ανά ζεύγη μη συντροφικών αναγώγων πολυωνύμων που ανήκουν στον $\mathbf{k}\left[\mathsf{X}\right]$ είναι *απειροπληθές*· αντιθέτως, το σύνολο $\mathcal{B}$ των αναγώγων πολυωνύμων τού $\mathbf{k}\left[\mathsf{X}\right]$ που διαιρούν τα G_j, για κάθε $j\in\{1,\ldots,n\}$, είναι *πεπερασμένο*. Ως εκ τούτου, $\mathcal{A}\smallsetminus\mathcal{B}\neq\varnothing$ και οιοδήποτε πολυώνυμο $\Xi\in\mathcal{A}\smallsetminus\mathcal{B}$ είναι κατάλληλο για να την ικανοποίηση των ανωτέρω συνθηκών. □

[1] Είναι αδύνατον να ισχύει $\Xi\cdot H=H'$, διότι (εξ υποθέσεως) $\Xi\nmid H'$.

A-1-62. Έστω R ένας υποδακτύλιος ενός δακτυλίου S. Υποθέτουμε ότι ο S είναι υποδακτύλιος ενός δακτυλίου T.

(a) Εάν $S = \sum_{i=1}^{n} R\, v_i$ και $T = \sum_{j=1}^{m} S\, w_j$, και εάν θεωρήσουμε τυχόν $t \in T$, τότε

$$\exists s_1, \dots, s_m \in S : t = \sum_{j=1}^{m} s_j\, w_j,$$

και για κάθε $j \in \{1, \dots, m\}$

$$\exists r_{i1}, \dots, r_{im} \in R : s_j = \sum_{j=1}^{m} r_{ij} v_i.$$

Κατά συνέπειαν,

$$t = \sum_{j=1}^{m} \left(\sum_{j=1}^{m} r_{ij} v_i \right) w_j,$$

οπότε

$$T = \sum_{1 \le i \le n, 1 \le j \le m} R\, v_i w_j.$$

(b) Εάν $S = R[v_1, v_2, \dots, v_n]$ και $T = S[w_1, w_2, \dots, w_m]$, και εάν θεωρήσουμε τυχόν $t \in T$, τότε

$$t = \sum s_{(j_1, \dots, j_n)}\, w_1^{j_1} w_2^{j_2} \cdots w_m^{j_m}, \quad s_{(j_1, \dots, j_n)} \in S,$$

και για κάθε $(j_1, \dots, j_n)$

$$s_{(j_1, \dots, j_n)} = \sum r_{(i_1, \dots, i_n)}\, v_1^{i_1} v_2^{i_2} \cdots v_n^{i_n}, \quad r_{(i_1, \dots, i_n)} \in R.$$

Κατά συνέπειαν,

$$t = \sum \left(\sum r_{(i_1, \dots, i_n)}\, v_1^{i_1} v_2^{i_2} \cdots v_n^{i_n} \right) w_1^{j_1} w_2^{j_2} \cdots w_m^{j_m},$$

οπότε

$$T = R[v_1, v_2, \dots, v_n, w_1, w_2, \dots, w_m].$$

(c) Εάν οι R, S και T είναι τρία σώματα, όπου $S = R(v_1, v_2, \dots, v_n)$ και, αντιστοίχως, $T = S(w_1, w_2, \dots, w_m)$, τότε το

$$T = R(v_1, v_2, \dots, v_n)(w_1, w_2, \dots, w_m)$$

περιέχει τα R και $v_1, \ldots, v_n, w_1, \ldots, w_m$, ενώ το $R(v_1, \ldots, v_n, w_1, \ldots, w_m)$ είναι το ελάχιστο σώμα με αυτήν την ιδιότητα. Συνεπώς,

$$T \subseteq R(v_1, \ldots, v_n, w_1, \ldots, w_m).$$

Εξάλλου, κάθε $u \in R(v_1, \ldots, v_n, w_1, \ldots, w_m)$ γράφεται υπό τη μορφή

$$u = \frac{\sum r_{(i_1,\ldots,i_n,j_1,\ldots,j_n)}\, v_1^{i_1} \cdots v_n^{i_n} w_1^{j_1} \cdots w_m^{j_m}}{\sum r'_{(i'_1,\ldots,i'_n,j'_1,\ldots,j'_n)}\, v_1^{i'_1} \cdots v_n^{i'_n} w_1^{j'_1} \cdots w_m^{j'_m}},$$

για κατάλληλα $r_{(i_1,\ldots,i_n,j_1,\ldots,j_n)}$, $r'_{(i'_1,\ldots,i'_n,j'_1,\ldots,j'_n)} \in R$ (και μη μηδενικό παρονομαστή). Επειδή

$$r_{(i_1,\ldots,i_n,j_1,\ldots,j_n)}\, v_1^{i_1} \cdots v_n^{i_n},\ \ r'_{(i'_1,\ldots,i'_n,j'_1,\ldots,j'_n)}\, v_1^{i'_1} \cdots v_n^{i'_n} \in R[v_1, \ldots, v_n] \subseteq R(v_1, \ldots, v_n),$$

έχουμε $u \in T$. Άρα τελικώς $T = R(v_1, \ldots, v_n, w_1, \ldots, w_m)$. □

A-1-63. Έστω ότι ο R είναι ένας υποδακτύλιος κάποιου δακτυλίου S και ότι ο S είναι ένας υποδακτύλιος κάποιου δακτυλίου T. Υποθέτουμε ότι ο S είναι ακέραιος υπεράνω τού R και ο T ακέραιος υπεράνω τού S. Έστω $t \in T$. Τότε υπάρχουν $a_1, \ldots, a_n \in S$, τέτοια ώστε να ισχύει

$$t^n + a_1 t^{n-1} + \cdots + a_n = 0.$$

Το a_1 είναι ακέραιο υπεράνω τού R. Το a_2 είναι ακέραιο υπεράνω τού $R[a_1] \supseteq R$. Κατά την πρόταση 1.10.2 ο $R[a_2]$ είναι μοδιακώς πεπερασμένος υπεράνω τού $R[a_1]$ και κατά το (a) τής ασκήσεως **A-1-62** ο $R[a_1, a_2]$ είναι μοδιακώς πεπερασμένος υπεράνω τού R. Επίσης, το a_3 είναι ακέραιο υπεράνω τού $R[a_1, a_2] \supseteq R$. Επαναλαμβάνοντας την ίδια συλλογιστική αποδεικνύουμε ότι ο $R[a_1, \ldots, a_n]$ είναι μοδιακώς πεπερασμένος υπεράνω τού R. Επιπροσθέτως, το t (λόγω τής ανωτέρω εξισώσεως) είναι ακέραιος υπεράνω τού $R[a_1, \ldots, a_n]$, οπότε (κατά την πρόταση 1.10.2) ο

$$R[a_1, \ldots, a_n, t] \cong R[a_1, \ldots, a_n][t]$$

είναι μοδιακώς πεπερασμένος υπεράνω τού $R[a_1, \ldots, a_n]$. Εφαρμόζοντας τη μεταβατική ιδιότητα τού «μοδιακώς πεπερασμένου» (βλ. το (a) τής ασκήσεως **A-1-62**) διαπιστώνουμε ότι ο $R[a_1, \ldots, a_n, t]$ είναι μοδιακώς πεπερασμένος υπεράνω τού R. Κατά συνέπειαν, σύμφωνα με την πρόταση 1.10.2 για $R' = S = R[a_1, \ldots, a_n, t] \supseteq R[t]$, το t είναι ακέραιο υπεράνω τού R, οπότε ο T είναι ακέραιος υπεράνω τού R. □

A-1-64. Έστω ότι ο S είναι δακτυλιακώς πεπερασμένος υπεράνω τού R, δηλαδή ότι

$$\exists v_1, \ldots, v_n \in S : S = R[v_1, \ldots, v_n].$$

Εάν ο S είναι μοδιακώς πεπερασμένος υπεράνω τού R, τότε εφαρμόζοντας τη συνεπαγωγή (3) $\Rightarrow$ (1) τής προτάσεως 1.10.2 για τα v_i, $i \in \{1, \dots, n\}$, και $R' = S$, συνάγουμε ότι κάθε v_i, $i \in \{1, \dots, n\}$, είναι ακέραιος υπεράνω τού R. Εξάλλου, επειδή κάθε $r \in R$ είναι ακέραιο υπεράνω τού R (ως σημείο μηδενισμού τού $\mathsf{X} - r \in R[\mathsf{X}]$), κάθε $s \in S$ θα είναι ακέραιο υπεράνω τού R (διότι το

$$s = \sum \lambda_{(i_1,\dots,i_n)}\, v_1^{i_1} v_2^{i_2} \cdots v_n^{i_n}$$

ανήκει στον δακτύλιο των ακεραίων στοιχείων τού S υπεράνω τού R επί τη βάσει τού πορίσματος 1.10.3).

Και αντιστρόφως· εάν ο S είναι ακέραιος υπεράνω τού R και $n = 1$, τότε το v_1 είναι ακέραιο υπεράνω τού R και (βάσει τής προτάσεως 1.10.2) ο $S = R[v_1]$ μοδιακώς πεπερασμένος υπεράνω τού R. Για $n \geq 2$ κάνουμε χρήση επαγωγής. Υποθέτοντας ότι ο $R[v_1, \dots, v_{n-1}]$ είναι μοδιακώς πεπερασμένος υπεράνω τού R, το v_n είναι ακέραιο υπεράνω τού $R[v_1, \dots, v_{n-1}]$ (αφού είναι ακέραιο υπεράνω τού $R \subseteq R[v_1, \dots, v_{n-1}]$) και (λόγω τής επαγωγικής υποθέσεως) ο S είναι μοδιακώς πεπερασμένος υπεράνω τού $R[v_1, \dots, v_{n-1}]$. Κατά συνέπειαν, βάσει τού (a) τής ασκήσεως **A-1-62**, ο S είναι μοδιακώς πεπερασμένος υπεράνω τού R. □

A-1-65. Έστω L ένα σώμα και έστω $\mathbf{k}$ ένα αλγεβρικώς κλειστό υπόσωμά του.

(a) Έστω τυχόν $l \in L$, το οποίο είναι αλγεβρικό υπεράνω τού $\mathbf{k}$. Τότε

$$\exists F = \mathsf{X}^n + a_1 \mathsf{X}^{n-1} + a_2 \mathsf{X}^{n-2} + \cdots + a_{n-1}\mathsf{X} + a_n \in \mathbf{k}\,[\mathsf{X}] : F(l) = 0.$$

Επειδή το $\mathbf{k}$ είναι αλγεβρικώς κλειστό, τα σημεία μηδενισμού τού F ανήκουν στο $\mathbf{k}$, οπότε $l \in \mathbf{k}$.

(b) Έστω $L = \mathbf{k}(v_1, \dots, v_n)$ μια πεπερασμένη επέκταση τού $\mathbf{k}$. Εάν αυτή είναι μοδιακώς πεπερασμένη, τότε (κατά την άσκηση **A-1-64**) κάθε στοιχείο τού L είναι αλγεβρικό υπεράνω τού $\mathbf{k}$, οπότε (σύμφωνα με το (a)) $L \subseteq \mathbf{k}$. Άρα $L = \mathbf{k}$. □

A-1-66. Έστω $\mathbf{k}$ ένα σώμα και έστω $L = \mathbf{k}(\mathsf{X})$ το σώμα των ρητών συναρτήσεων μιας μεταβλητής υπεράνω τού $\mathbf{k}$.

(a) Έστω $z \in L$. Το z γράφεται ως κλάσμα $z = \frac{F}{G}$, όπου τα F και G είναι μεταξύ τους πρώτα (βλ. άσκηση **A-1-2**). Εάν το z είναι ακέραιο υπεράνω τού $\mathbf{k}\,[\mathsf{X}]$, τότε

$$\exists F_1, \dots, F_n \in \mathbf{k}\,[\mathsf{X}] : z^n + F_1\, z^{n-1} + F_2\, z^{n-2} + \cdots + F_{n-1}\, z + F_n = 0,$$

οπότε

$$F^n + F_1 \cdot F^{n-1} \cdot G + F_2 \cdot F^{n-2} \cdot G^2 + \cdots + F_n \cdot G^n = 0 \Longrightarrow G \mid F \Longrightarrow z \in \mathbf{k}\,[\mathsf{X}]\,.$$

(b) Υποθέτουμε ότι υπάρχει ένα μη μηδενικό πολυώνυμο $F \in \mathbf{k}[\mathsf{X}]$, ούτως ώστε να ισχύει:

$$[\exists n \in \mathbb{N} : F^n z \text{ είναι ακέραιο υπεράνω τού } \mathbf{k}[\mathsf{X}], \ \forall z \in L.]$$

Εάν $z = \frac{1}{G}$, όπου το G ένα ανάγωγο πολυώνυμο που δεν διαιρεί το F, καταλήγουμε σε άτοπο μέσω τού (a). □

A-1-67. Έστω $\mathbf{k}$ ένα υπόσωμα ενός σώματος L.

(a) Κατά το πόρισμα 1.10.3 το σύνολο των στοιχείων τού L που είναι αλγεβρικά υπεράνω τού $\mathbf{k}$ αποτελεί έναν υποδακτύλιο τού L, ο οποίος περιέχει το $\mathbf{k}$. Θα δείξουμε ότι ο εν λόγω υποδακτύλιος είναι σώμα. Πρός τούτο αρκεί να δειχθεί ότι κάθε μη μηδενικό στοιχείο του v είναι αντίστροφο. Εξ υποθέσεως,

$$\exists a_1, \ldots, a_n \in \mathbf{k} : v^n + a_1 v^{n-1} + \cdots + a_n = 0_{\mathbf{k}}.$$

Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $a_n \neq 0_{\mathbf{k}}$. (Εάν $a_n = 0_{\mathbf{k}}$ και $i := \max\{ j \in \{1, \ldots, n-1\} |\ a_j \neq 0_{\mathbf{k}}\}$, τότε

$$v^i(v^{n-i} + a_1 v^{n-i-1} + \cdots + a_i) = 0_{\mathbf{k}},$$

κι επειδή $v \neq 0_{\mathbf{k}}$, έχουμε $v^{n-i} + a_1 v^{n-i-1} + \cdots + a_i = 0_{\mathbf{k}}$.) Επειδή

$$v\left(v^{n-1} + a_1 v^{n-2} + \cdots + a_{n-1}\right) = -a_n \neq 0_{\mathbf{k}},$$

το v έχει το $-a_n^{-1}(v^{n-1} + \cdots + a_{n-1})$ ως αντίστροφό του.

(b) Έστω ότι το L είναι μοδιακώς πεπερασμένο υπεράνω τού $\mathbf{k}$ και ότι $\mathbf{k} \subseteq R \subseteq L$, όπου R ένας δακτύλιος. Για οιοδήποτε $v \in R \smallsetminus \{0_R\} \subseteq L$ το v είναι αλγεβρικό υπεράνω τού $\mathbf{k}$ λόγω τής συνεπαγωγής (3) ⇒ (1) τής προτάσεως 1.10.2 (για $R' = L \supseteq \mathbf{k}[v]$). Βάσει τού (a) ο R είναι σώμα. □

A-1-68. Έστω $\mathbf{k}$ ένα σώμα και έστω $F \in \mathbf{k}[\mathsf{X}]$ ένα ανάγωγο πολυώνυμο βαθμού $n \geq 1$.

(a) Επειδή ο $\mathbf{k}[\mathsf{X}]$ είναι Π.Κ.Ι. (βλ. θεώρημα 1.1.24), το ιδεώδες $\langle F \rangle$ είναι μεγιστοτικό (βλ. πόρισμα 1.1.17 (b)) και ο πηλικοδακτύλιος $L := \mathbf{k}[\mathsf{X}] \,/\, \langle F \rangle$ σώμα (βλ. θεώρημα 1.1.14). Ο περιορισμός $\pi|_{\mathbf{k}}$ τού φυσικού επιμορφισμού $\pi : \mathbf{k}[\mathsf{X}] \longrightarrow L$ επί τού $\mathbf{k}$ είναι μη μηδενικός (καθόσον το $1_{\mathbf{k}}$ απεικονίζεται στο $1_{\mathbf{k}} + \langle F \rangle \neq \langle F \rangle$) και, ταυτοχρόνως, μονομορφισμός, διότι ο πυρήνας $\mathrm{Ker}(\pi|_{\mathbf{k}})$ τού $\pi|_{\mathbf{k}}$ είναι ιδεώδες τού σώματος $\mathbf{k}$. Μπορούμε, ως εκ τούτου, να ταυτίζουμε το $\mathbf{k}$ με την εικόνα του μέσω τού π εντός τού L και να θεωρούμε το $\mathbf{k}$ ως υπόσωμα τού L. Σημειωτέον ότι, εάν το x είναι η κλάση υπολοίπων τού X εντός τού L, το σώμα $\mathbf{k}(x)$ είναι το ίδιο το L, αφού

$$B(x) = B(\mathsf{X} + \langle F \rangle) = B(\mathsf{X}) + \langle F \rangle, \ \forall B \in \mathbf{k}[\mathsf{X}],$$

οπότε $\mathbf{k}(x) = \mathbf{k}(\mathsf{X} + \langle F\rangle) = L$. Ιδιαιτέρως, για $B = F$ λαμβάνουμε

$$F(x) = F(\mathsf{X} + \langle F\rangle) = F(\mathsf{X}) + \langle F\rangle = 0.$$

(b) Εάν υποτεθεί ότι το L' είναι μια σωματική επέκταση τού $\mathbf{k}$ και $y \in L'$, ούτως ώστε να ισχύει $F(y) = 0$, τότε ο ομομορφισμός $\varphi : \mathbf{k}[\mathsf{X}] \to L'$, ο οποίος απεικονίζει το X στο y, επάγει έναν ισομορφισμό

$$\mathbf{k}[\mathsf{X}] \,/\, \mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi) = \varphi\,(\mathbf{k}[\mathsf{X}]) = \mathbf{k}[y].$$

Επειδή ο $\mathbf{k}[\mathsf{X}]$ είναι Π.Κ.Ι. (βλ. θεώρημα 1.1.24) $\exists H \in \mathbf{k}[\mathsf{X}] : \mathrm{Ker}(\varphi) = \langle H\rangle$. Επίσης,

$$F \in \langle H\rangle \Longrightarrow \exists H' \in \mathbf{k}[\mathsf{X}] : F = H \cdot H',$$

κι επειδή το F είναι ανάγωγο, είτε το H είτε το H' είναι σταθερό. Εν πάση περιπτώσει, $\mathrm{Ker}(\varphi) = \langle F\rangle$ (που είναι μεγιστοτικό ιδεώδες), οπότε

$$\mathbf{k}[y] = \mathbf{k}(y) \Longrightarrow L := \mathbf{k}[\mathsf{X}] \,/\, \langle F\rangle \cong \mathbf{k}(y).$$

(c) Εάν $G \in \mathbf{k}[\mathsf{X}]$ με $G(y) = 0$, τότε

$$G \in \mathrm{Ker}(\varphi) = \langle F\rangle \Longrightarrow F \mid G.$$

(d) Σύμφωνα με όσα ειπώθηκαν στο (a), το $\mathbf{k}$ μπορεί να θεωρηθεί ως υπόσωμα τού L και, ως εκ τούτου, ο δακτύλιος $\mathbf{k}[\mathsf{X}]$ ως υποδακτύλιος τού $L[\mathsf{X}]$. Επειδή $F(x) = 0$ με $x \in L$, έχουμε $F = (\mathsf{X} - x) \cdot H$, για κάποιο $H \in L[\mathsf{X}]$. □

A-1-69. Έστω $\mathbf{k}$ ένα σώμα και έστω

$$F = a_0\mathsf{X}^n + a_1\,\mathsf{X}^{n-1} + \cdots + a_{n-1}\,\mathsf{X} + a_n \in \mathbf{k}[\mathsf{X}], \quad a_0 \neq 0.$$

Όταν $n = 1$, το F είναι πρωτοβάθμιο (και ανάγωγο) και δεν έχουμε να δείξουμε τίποτα. (Απλώς θέτουμε $\lambda = a_0$, $x_1 = -\frac{a_n}{a_0} \in \mathbf{k}$ και $L = \mathbf{k}\,(x_1) = \mathbf{k}$.) Για $n \geq 2$ θα χρησιμοποιήσουμε επαγωγή. Επίσης, δίχως βλάβη τής γενικότητας μπορούμε να αποδείξουμε την αλήθεια τού ισχυρισμού μόνον για ανάγωγα πολυώνυμα. (Για τυχόντα πολυώνυμα βαθμού ≥ 1 και ανήκοντα στον $\mathbf{k}[\mathsf{X}]$ μπορεί κανείς να δείξει το ίδιο εργαζόμενος με τους ανάγωγους παράγοντές τους.) Έστω λοιπόν $F \in \mathbf{k}[\mathsf{X}]$ ένα ανάγωγο πολυώνυμο βαθμού $n \geq 2$. Τότε κατά το (d) τής ασκήσεως **A-1-68** υπάρχει μια σωματική επέκταση $L_1 = \mathbf{k}[\mathsf{X}] \,/\, \langle F\rangle \cong \mathbf{k}(x_1)$ τού $\mathbf{k}$, τέτοια ώστε να ισχύει $F(x_1) = 0$ και να

$$\exists H \in L_1[\mathsf{X}] : F = (\mathsf{X} - x_1) \cdot H.$$

Επειδή $\deg(H) \leq n - 1$, η επαγωγική υπόθεση εξασφαλίζει την ύπαρξη μιας σωματικής επεκτάσεως L τού L_1, καθώς και στοιχείων $\lambda, x_2, \ldots, x_n \in L$, τέτοιων ώστε να ισχύει

$$H = \lambda \prod_{i=2}^{n} (\mathsf{X} - x_i),$$

Κατά συνέπειαν, $F = \lambda \prod_{i=1}^{n}(\mathsf{X} - x_i) \in L[\mathsf{X}]$. □

A-1-70. Έστω ότι το $\mathbf{k}$ είναι ένα σώμα χαρακτηριστικής μηδέν και ότι το $F \in \mathbf{k}[\mathsf{X}]$ είναι ένα ανάγωγο πολυώνυμο βαθμού $n \geq 1$. Έστω L το σώμα διασπάσεως τού F, όπου

$$F = \lambda \prod_{i=1}^{n}(\mathsf{X} - x_i) \in L[\mathsf{X}].$$

Τότε

$$\frac{\partial F}{\partial \mathsf{X}} = \lambda \left(\sum_{i=1}^{n} (\mathsf{X} - x_1) \cdots \widehat{(\mathsf{X} - x_i)} \cdots (\mathsf{X} - x_n) \right),$$

(όπου το «καπελάκι» δηλοί παράλειψη τού όρου) και $\deg(\frac{\partial F}{\partial \mathsf{X}}) = n - 1$. Επειδή το F είναι ανάγωγο, τα F και $\frac{\partial F}{\partial \mathsf{X}}$ είναι μεταξύ τους πρώτα (εντός τού $\mathbf{k}[\mathsf{X}]$). Άρα υπάρχουν $H_1, H_2 \in \mathbf{k}[\mathsf{X}]$, τέτοια ώστε να ισχύει η ισότητα

$$F \cdot H_1 + \frac{\partial F}{\partial \mathsf{X}} \cdot H_2 = 1. \tag{1}$$

Εάν το x_i ήταν πολλαπλό σημείο μηδενισμού τού F (ήτοι $m_i = \text{mult}(F; x_i) \geq 2$), για κάποιο $i \in \{1, \ldots, n\}$, τότε το F θα εγράφετο ως

$$F = (\mathsf{X} - x_i)^{m_i} \cdot G,$$

για κάποιο $G \in L[\mathsf{X}]$ με $G(x_i) \neq 0$ και θα είχαμε

$$\frac{\partial F}{\partial \mathsf{X}} = (\mathsf{X} - x_i)^{m_i} \cdot \frac{\partial G}{\partial \mathsf{X}} + m_i(\mathsf{X} - x_i)^{m_i - 1} \cdot G, \tag{2}$$

κάτι που θα μας οδηγούσε σε αντίφαση, καθότι η (1) θα έδινε

$$F(x_i) = 0 \Longrightarrow \frac{\partial F}{\partial \mathsf{X}}(x_i) \cdot H_2(x_i) = 1 \Longrightarrow \frac{\partial F}{\partial \mathsf{X}}(x_i) \neq 0,$$

ενώ η (2) θα έδινε $\frac{\partial F}{\partial \mathsf{X}}(x_i) = 0$. Άρα τα $x_1, \ldots, x_n$ είναι σαφώς διακεκριμένα.

Σημείωση: Η συνθήκη $\text{χαρ}(\mathbf{k}) = 0$ χρειάζεται για να αποκλεισθεί το ενδεχόμενο τής εμφανίσεως τού μηδενικού πολυωνύμου ως επίτυπης παραγώγου $\frac{\partial F}{\partial \mathsf{X}}$. Πρβλ. παρατήρηση 1.1.32. □

A-1-71. Έστω R μια ακεραία περιοχή με σώμα κλασμάτων της το $\mathbf{k}$ και έστω L μια πεπερασμένη αλγεβρική επέκταση τού $\mathbf{k}$.

(a) Έστω τυχόν στοιχείο v τού L. Επειδή το v είναι εξ υποθέσεως αλγεβρικό υπεράνω τού $\mathbf{k}$

$$\exists F = \mathsf{X}^n + \lambda_1 \mathsf{X}^{n-1} + \lambda_2 \mathsf{X}^{n-2} + \cdots + \lambda_{n-1}\mathsf{X} + \lambda_n \in \mathbf{k}[\mathsf{X}] : F(v) = 0.$$

Εάν $\lambda_i = \frac{b_i}{c_i}$, $b_i \in R$, $c_i \in R \setminus \{0_R\}$, για $i \in \{1, \dots, n\}$, και εάν λάβουμε ως a κάποιο κοινό πολλαπλάσιο των $c_1, \dots, c_n$, τότε

$$(av)^n + ab_1 (av)^{n-1} + \cdots + ab_n = 0,$$

οπότε το av είναι όντως ακέραιο υπεράνω τού R.

(b) Εάν $[L : \mathbf{k}] = m$ και η $\{w_1, \dots, w_m\}$ είναι μια βάση τού δ.χ. L υπεράνω τού $\mathbf{k}$, τότε (κατά το (a)) υπάρχουν $a_j \in R \setminus \{0_R\}$ με τα $v_j := a_j w_j$ ακέραια στοιχεία υπεράνω τού R για κάθε $j \in \{1, \dots, m\}$. Θα δείξουμε ότι το σύνολο $\{v_1, \dots, v_m\}$ αποτελεί βάση τού δ.χ. L υπεράνω τού $\mathbf{k}$. Εν πρώτοις θεωρούμε $\mu_1, \dots, \mu_m \in \mathbf{k}$, τέτοια ώστε να ισχύει η ισότητα $\mu_1 v_1 + \cdots + \mu_m v_m = 0$. Τότε

$$(\mu_1 a_1) w_1 + \cdots + (\mu_m a_m) w_m = 0 \Longrightarrow \mu_1 a_1 = \cdots = \mu_m a_m = 0,$$

κι επειδή $a_j \in R \setminus \{0_R\}$, $\forall j \in \{1, \dots, m\}$, έχουμε $\mu_1 = \cdots = \mu_m = 0$, οπότε το $\{v_1, \dots, v_m\}$ είναι γραμμικώς ανεξάρτητο υπεράνω τού $\mathbf{k}$. Από την άλλη μεριά, για οιοδήποτε $\ell \in L$ υπάρχουν $l_1, \dots, l_m \in \mathbf{k}$, τέτοια ώστε να ισχύει

$$\ell = \sum_{j=1}^{m} l_j w_j = \sum_{j=1}^{m} \left(\frac{l_j}{a_j} \right) v_j.$$

Εξ αυτού έπεται ότι το $\{v_1, \dots, v_m\}$ παράγει τον L. Άρα τελικώς το $\{v_1, \dots, v_m\}$ αποτελεί βάση τού δ.χ. L υπεράνω τού $\mathbf{k}$. □