# ΚΕΦΑΛΑΙΟ 1

# Συσχετικά Αλγεβρικά Σύνολα

## 1.1 Προκαταρκτικές Αλγεβρικές Έννοιες

Σε αυτήν την ενότητα επαναλαμβάνονται εν συντομία ορισμένες προκαταρκτικές (και γνωστές, από προηγηθείσες παραδόσεις) αλγεβρικές έννοιες.

**(i)** Στις παρούσες σημειώσεις ο όρος **δακτύλιος** θα σημαίνει πάντοτε «*μεταθετικός δακτύλιος με μοναδιαίο πολλαπλασιαστικό στοιχείο*». Εάν οι $R$ και $R'$ είναι δυο δακτύλιοι, τα $1_R, 1_{R'}$ τα μοναδιαία πολλαπλασιαστικά στοιχεία των $R$ και $R'$, αντιστοίχως, και η $f : R \longrightarrow R'$ μια απεικόνιση, τότε η $f$ καλείται **ομομορφισμός** όταν ισχύουν οι ισότητες

$$f(1_R) = 1_{R'}, \quad f(a+b) = f(a) + f(b) \qquad \text{και} \qquad f(ab) = f(a)\, f(b)$$

για όλα τα $a, b \in R$.

Ένας ομομορφισμός δακτυλίων $f : R \longrightarrow R'$ ονομάζεται

| | | |
|---|---|---|
| **μονομορφισμός** | $\underset{\text{ορσ}}{\Longleftrightarrow}$ | η απεικόνιση $f$ είναι ενριπτική, |
| **επιμορφισμός** | $\underset{\text{ορσ}}{\Longleftrightarrow}$ | η απεικόνιση $f$ είναι επιρριπτική, |
| **ισομορφισμός** | $\underset{\text{ορσ}}{\Longleftrightarrow}$ | η απεικόνιση $f$ είναι αμφιρριπτική, |
| **ενδομορφισμός** | $\underset{\text{ορσ}}{\Longleftrightarrow}$ | $R = R'$, |
| **αυτομορφισμός** | $\underset{\text{ορσ}}{\Longleftrightarrow}$ | η $f$ είναι αμφιρριπτικός ενδομορφισμός. |

Εάν οι $R$ και $R'$ είναι δυο δακτύλιοι, τότε γράφουμε $R \cong R'$ και λέμε ότι **ο** $R$ **είναι ισόμορφος με τον** $R'$ (ή, απλούστερα, ότι **ο** $R$ **είναι ισόμορφος τού** $R'$) όταν υπάρχει κάποιος

ισομορφισμός από τον $R$ επί τού $R'$. Ένα μη κενό υποσύνολο $S$ ενός δακτυλίου $R$ καλείται **υποδακτύλιος** τού $R$ όταν το $S$ είναι δακτύλιος ως προς την πράξη τής προσθέσεως και τού πολλαπλασιασμού τού $R$ (δηλαδή όταν το $(S,+)$ είναι μια αβελιανή υποομάδα τής $(R,+)$ και το $S$ είναι «κλειστό» ως προς τον πολλαπλασιασμό) και $1_R \in S$ (οπότε $1_S = 1_R$). Εάν ο $f : R \longrightarrow R'$ είναι ένας ομομορφισμός δακτυλίων, τότε το σύνολο $\mathrm{Ker}(f) := f^{-1}(0_{R'})$ τού $R$ ονομάζεται **πυρήνας** τού $f$.

**(ii) Ακεραία περιοχή** καλείται κάθε δακτύλιος (με τουλάχιστον δύο στοιχεία) στον οποίο ισχύει ο νόμος τής διαγραφής, δηλαδή για $a, b \in R$ και $c \in R \smallsetminus \{0_R\}$,

$$ac = bc \Longrightarrow a = b.$$

Έστω $R$ ένας μη τετριμμένος δακτύλιος (δηλαδή, με $1_R \neq 0_R$). Ένα στοιχείο $a \in R$ λέγεται **αντιστρέψιμο** όταν υπάρχει ένα $b \in R$, τέτοιο ώστε $ab = 1$. Το σύνολο όλων των αντιστρεψίμων στοιχείων ενός μη τετριμμένου δακτυλίου $R$ αποτελεί *πολλαπλασιαστική ομάδα* και συμβολίζεται ως $R^\times$. Ένα στοιχείο $a \in R \smallsetminus \{0_R\}$ λέγεται **μηδενοδιαιρέτης** όταν υπάρχει ένα $b \in R \smallsetminus \{0_R\}$, τέτοιο ώστε $ab = 0_R$. Το σύνολο όλων των μηδενοδιαιρετών ενός δακτυλίου $R$ συμβολίζεται ως $\mathrm{Zdv}(R)$. Ένα στοιχείο $a$ ενός δακτυλίου $R$ λέγεται **μηδενοδύναμο** όταν ισχύει $a^n = 0$ για κάποιον $n \in \mathbb{N}$. Το σύνολο όλων των μηδενοδυνάμων στοιχείων τού $R$ συμβολίζεται ως $\mathrm{Nil}(R)$. Σημειωτέον ότι

$$\mathrm{Nil}(R) \smallsetminus \{0_R\} \subseteq \mathrm{Zdv}\,(R) \subseteq\ R \smallsetminus R^\times \subseteq R.$$

Κάθε ακεραία περιοχή $R$, για την οποία ισχύει η ισότητα $R^\times = R \smallsetminus \{0_R\}$, καλείται **σώμα**. (Κάθε υποδακτύλιος $\mathbf{k}$ ενός σώματος $L$ που είναι αφ' εαυτού σώμα καλείται **υπόσωμα** τού $L$.) Ως $\mathbb{Z}$ θα συμβολίζουμε την ακεραία περιοχή των ακεραίων αριθμών και ως $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ τα σώματα των ρητών, των πραγματικών και των μιγαδικών αριθμών, αντιστοίχως.

Έστω $R$ ένας δακτύλιος. Ας υποθέσουμε ότι υπάρχει ένας $m \in \mathbb{N}$ με την ιδιότητα $ma = 0_R$ για κάθε $a \in R$. Εάν ο $n \in \mathbb{N}$ είναι ο ελάχιστος φυσικός αριθμός με αυτήν την ιδιότητα, τότε ο $n$ λέγεται **χαρακτηριστική** τού δακτυλίου $R$. Εάν δεν υπάρχει κανένας $m \in \mathbb{N}$ με την ανωτέρω ιδιότητα, τότε λέμε πως ο δακτύλιος $R$ έχει **χαρακτηριστική** $0$. Π.χ., οι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ έχουν χαρακτηριστική $0$, ενώ ο $\mathbb{Z}_m,\ m \geq 2$, έχει χαρακτηριστική $m$. (Η χαρακτηριστική ενός δακτυλίου $R$ συμβολίζεται συνήθως ως $\mathrm{χαρ}(R)$.) Σημειωτέον ότι $\mathrm{χαρ}(R) = n > 0 \Longleftrightarrow n = \min\{m \in \mathbb{N} \mid m \cdot 1_R = 0_R\}$.

**1.1.1 Πρόταση.** *Μια ακεραία περιοχή έχει χαρακτηριστική είτε $0$ είτε έναν πρώτο αριθμό.*

**(iii)** Έστω $R$ τυχούσα *ακεραία περιοχή*. Επί τού $R \times (R \smallsetminus \{0\})$ ορίζουμε μια σχέση ισοδυναμίας ως ακολούθως:

$$(a,b) \sim (c,d) \underset{\text{ορσ}}{\Longleftrightarrow} ad = cb.$$

Έστω $\mathbf{Fr}(R) := (R \times (R \smallsetminus \{0_R\})) \,/\, \sim$ το σύνολο κλάσεων ισοδυναμίας ως προς την "$\sim$". Το **κλάσμα** ενός $a \in R$ «διηρημένου» διά ενός $b \in R \smallsetminus \{0\}$ είναι η κλάση ισοδυναμίας

$$\frac{a}{b} := [(a,b)] := \{\, (x,y) \in R \times (R \smallsetminus \{0_R\}) \mid (x,y) \sim (a,b) \}.$$

Το $\mathbf{Fr}(R)$ επιδέχεται πρόσθεση και πολλαπλασιασμό:

$$\begin{cases} \dfrac{a}{b} + \dfrac{c}{d} & := & \dfrac{ad+cb}{bd}, \\ \\ \dfrac{a}{b} \cdot \dfrac{c}{d} & := & \dfrac{ac}{bd}. \end{cases}$$

Μέσω αυτών των πράξεων το $\mathbf{Fr}(R)$ καθίσταται σώμα και καλείται, ιδιαιτέρως, **σώμα κλασμάτων τής** $R$.

**1.1.2 Πρόταση.** *Κάθε ακεραία περιοχή εμφυτεύεται στο σώμα των κλασμάτων της.*

**1.1.3 Πρόταση.** *Εάν η $R$ είναι μια ακεραία περιοχή και το $\mathbf{k}$ ένα σώμα το οποίο την περιέχει, τότε η απεικόνιση $\psi : \mathbf{Fr}(R) \longrightarrow \mathbf{k}$ η οριζόμενη μέσω των*

$$\psi|_R := \mathrm{Id}_R, \quad \psi(\tfrac{a}{b}) := \psi(a)\,\psi(b)^{-1}, \ \ \forall\, (a,b) \in R \times (R \smallsetminus \{0_R\}),$$

*αποτελεί μονομορφισμό σωμάτων.*

**1.1.4 Πόρισμα.** *Εάν η $R$ είναι μια ακεραία περιοχή, τότε το σώμα κλασμάτων $\mathbf{Fr}(R)$ τής $R$ είναι το ελάχιστο σώμα (ως προς τη σχέση τού εγκλεισμού) το οποίο περιέχει την $R$.*

**1.1.5 Πρόταση.** *Εάν δυο ακέραιες περιοχές $R_1$ και $R_2$ είναι ισόμορφες, τότε και τα σώματα κλασμάτων τους $\mathbf{Fr}(R_1)$ και $\mathbf{Fr}(R_2)$ θα είναι ισόμορφα.*

**(iv)** Ένα **ιδεώδες** $I$ ενός δακτυλίου $R$ είναι ένα υποσύνολο τού $R$, το οποίο αποτελεί προσθετική υποομάδα του και για το οποίο ισχύει $ra \in I$ για οιαδήποτε $a \in I$, $r \in R$. Ένα ιδεώδες $I$ ενός δακτυλίου $R$ χαρακτηρίζεται ως **γνήσιο** όταν $I \subsetneqq R$. Ένα ιδεώδες $\mathfrak{p} \subsetneqq R$ ενός δακτυλίου $R$ καλείται **πρώτο ιδεώδες** όταν

$$[ab \in \mathfrak{p} \Longrightarrow \text{ είτε } a \in \mathfrak{p} \ \text{ είτε } b \in \mathfrak{p}], \ \ \forall a, b \in R.$$

Ένα ιδεώδες $\mathfrak{m} \subsetneqq R$ ενός δακτυλίου $R$ καλείται **μεγιστοτικό** (ή, κατ' άλλους, **μεγιστικό**) **ιδεώδες** όταν για κάθε ιδεώδες $\mathfrak{n}$ τού $R$, ισχύει η συνεπαγωγή

$$[\mathfrak{m} \subseteq \mathfrak{n} \subseteq R \Longrightarrow \text{ είτε } \mathfrak{n} = \mathfrak{m} \ \text{ είτε } \mathfrak{n} = R].$$

**1.1.6 Θεώρημα.** *Κάθε μη τετριμμένος δακτύλιος $R$ διαθέτει πάντοτε μεγιστοτικά ιδεώδη. Και μάλιστα ισχύει κάτι ακόμη πιο ισχυρό: Κάθε ιδεώδες τού $R$ (εκτός τού ιδίου τού $R$) περιέχεται σε κάποιο μεγιστοτικό ιδεώδες τού $R$.*

**1.1.7 Θεώρημα.** *Κάθε μεγιστοτικό ιδεώδες ενός δακτυλίου $R$ είναι πρώτο.*

**(v)** Ένα σύνολο $A$ αποτελούμενο από στοιχεία ενός δακτυλίου $R$ παράγει ένα ιδεώδες

$$\begin{aligned} I &= \langle A\rangle := \bigcap \{\text{ιδεώδη } I \text{ τού } R \mid I \supseteq A\} \\ &= \left\{ \sum_{j=1}^{\kappa} r_j\, a_j \;\middle|\; r_1,\ldots,r_\kappa \in R,\ a_1,\ldots,a_\kappa \in A,\ \kappa \in \mathbb{N} \right\}. \end{aligned}$$

Το $I$ καλείται **πεπερασμένως παραγόμενο** όταν το $A$ είναι πεπερασμένο σύνολο. Όταν $A = \{a_1,\ldots,a_\nu\}$, τότε γράφουμε $I = \langle a_1,\ldots,a_\nu\rangle$. Ένα ιδεώδες $I$ τού $R$ καλείται **κύριο ιδεώδες** όταν μπορεί να παραχθεί από ένα και μόνον στοιχείο τού $R$. Κάθε ακεραία περιοχή, τα ιδεώδη τής οποίας είναι κύρια, καλείται **περιοχή κυρίων ιδεωδών (=: Π.Κ.Ι.)**.

**1.1.8 Πρόταση.** *Εάν μια ακεραία περιοχή $R$ είναι Π.Κ.Ι., τότε οιοδήποτε μη τετριμμένο, γνήσιο ιδεώδες της είναι πρώτο εάν και μόνον εάν είναι μεγιστοτικό.*

**(vi)** Έστω $R$ ένας δακτύλιος και έστω $I$ ένα ιδεώδες τού $R$. Επειδή η προσθετική ομάδα τού $R$ είναι αβελιανή, το $I$ αποτελεί μια ορθόθετη προσθετική υποομάδα τής $(R,+)$. Επομένως υπάρχει μια καλώς ορισμένη ομάδα πηλίκων $R/I$ με πρόσθεση:

$$(a+I)+(b+I) := (a+b)+I\,, \quad \text{για κάθε} \quad a,b \in R.$$

Το *ουδέτερο* στοιχείο $0_{R/I}$ τής $(R/I,+)$ είναι προφανώς το $0_R + I = I$. Εξάλλου, για κάθε $a,b \in R$, έχουμε

$$a+I = b+I \Longleftrightarrow a-b \in I.$$

Η προσθετική πηλικοομάδα $(R/I,+)$ μπορεί να εφοδιασθεί με τη δομή ενός δακτυλίου εφόσον για κάθε $a,b \in R$ ορίσουμε τον «πολλαπλασιασμό»*:*

$$(a+I)\ (b+I) := (ab)+I$$

(με *μοναδιαίο του στοιχείο* το $1_R + I$). Ο δακτύλιος $(R/I,+,\cdot)$ ονομάζεται **πηλικοδακτύλιος (ή δακτύλιος κλάσεων υπολοίπων)** τού $R$ **ως προς το** $I$. (Επιπροσθέτως, εάν $r \in R$, το στοιχείο $\overline{r} := r + I \in R/I$ καλείται **κλάση υπολοίπων τού** $r$ **ως προς το** $I$.)

**1.1.9 Πρόταση.** *Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Τότε ο πυρήνας τής $f$ αποτελεί ένα ιδεώδες τού $R$. Και αντιστρόφως· εάν το $I$ είναι ένα ιδεώδες τού $R$, τότε η απεικόνιση $\pi : R \longrightarrow R/I$, η οποία ορίζεται μέσω τής $r \longmapsto r+I$, αποτελεί έναν επιμορφισμό δακτυλίων με πυρήνα της το $I$.*

Η ανωτέρω απεικόνιση $\pi : R \longrightarrow R/I$ ονομάζεται **φυσικός επιμορφισμός (ή επιμορφισμός κλάσεων υπολοίπων)** τού $R$ επί τού πηλικοδακτυλίου $R/I$.

**1.1.10 Πρώτο Θεώρημα Ισομορφισμών.** *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Τότε*

$$R/\mathrm{Ker}(f) \cong \mathrm{Im}\,(f) = f\,(R)\,.$$

**1.1.11 Δεύτερο Θεώρημα Ισομορφισμών.** *Έστω ότι ο $R$ είναι ένας δακτύλιος, ο $S$ ένας υποδακτύλιος τού $R$ και το $I$ ένα γνήσιο ιδεώδες τού $R$. Τότε*

(a) *το $S \cap I$ είναι ένα γνήσιο ιδεώδες τού $S$,*

(b) *το $S + I := \{\, s + a \mid s \in S,\ a \in I\}$ είναι ένας υποδακτύλιος τού $R$ με $S \subseteq S + I$,*

(c) *το $I$ είναι ένα γνήσιο ιδεώδες τού $S + I$, και*

(d) $S/(S \cap I) \cong (S + I)/I$.

**1.1.12 Τρίτο Θεώρημα Ισομορφισμών.** *Εάν ο $R$ είναι ένας δακτύλιος και τα $I, J$ γνήσια ιδεώδη τού $R$ με $I \subseteq J$, τότε ο $J/I$ είναι ιδεώδες τού $R/I$ και $R/J \cong (R/I)\ /\ (J/I)$.*

**1.1.13 Θεώρημα.** *Εάν το $\mathfrak{p}$ είναι ένα ιδεώδες ενός δακτυλίου $R$, τότε τα ακόλουθα είναι ισοδύναμα*:

(a) $\mathfrak{p} \subsetneqq R$ *και το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες τού $R$.*

(b) *Ο πηλικοδακτύλιος $R/\mathfrak{p}$ αποτελεί μια ακεραία περιοχή.*

**1.1.14 Θεώρημα.** *Εάν το $\mathfrak{m}$ είναι ένα ιδεώδες ενός δακτυλίου $R$, τότε τα ακόλουθα είναι ισοδύναμα*:

(a) $\mathfrak{m} \subsetneqq R$ *και το $\mathfrak{m}$ ένα μεγιστοτικό ιδεώδες τού $R$.*

(b) *Ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι ένα σώμα.*

**(vii)** Έστω $R$ μια ακεραία περιοχή. Η $R$ ονομάζεται **ευκλείδεια περιοχή** (=: **Ε.Π.**) όταν υπάρχει μια απεικόνιση $\boldsymbol{\delta} : R\smallsetminus\{0_R\} \longrightarrow \mathbb{N}_0$ με τις ακόλουθες ιδιότητες:

(a) Εάν $a, b \in R\smallsetminus\{0_R\}$, τότε $\boldsymbol{\delta}\,(ab) \geq \boldsymbol{\delta}\,(a)$, και

(b) για οιαδήποτε $a \in R$ και $b \in R\smallsetminus\{0_R\}$ υπάρχουν $(q, r) \in R \times R$ (όχι κατ' ανάγκην μονοσημάντως ορισμένα), τέτοια ώστε να ισχύει

$$a = qb + r,\ \text{ όπου είτε }\ r = 0_R\ \text{ είτε }\ (r \neq 0_R\ \text{ και }\ \boldsymbol{\delta}\,(r) < \boldsymbol{\delta}\,(b))\,.$$

(Η απεικόνιση $\boldsymbol{\delta}$ καλείται **ευκλείδεια στάθμη** ή **ευκλείδεια εκτίμηση**.)

**1.1.15 Θεώρημα.** *Κάθε Ε.Π. είναι Π.Κ.Ι.* (*Το αντίστροφο δεν ισχύει πάντοτε.*)

Επί παραδείγματι, ο *δακτύλιος*

$$\mathfrak{O}_{-19} := \left\{ a + b\left(\tfrac{1+\sqrt{-19}}{2}\right) \;\middle|\; a, b \in \mathbb{Z} \right\}$$

*των ακεραίων* τού τετραγωνικού αριθμητικού σώματος $\mathbb{Q}(\sqrt{-19})$ είναι Π.Κ.Ι. αλλά όχι και Ε.Π.

**(viii)** Έστω $R$ ένας δακτύλιος και έστω $a \in R$. Λέμε ότι το $a$ **διαιρεί το** $b \in R$ ή ότι το $a$ είναι **διαιρέτης** τού $b$ (και σημειώνουμε $a \mid b$) όταν υπάρχει κάποιο στοιχείο $x \in R$, τέτοιο ώστε να ισχύει η ισότητα $b = ax$. Δυο στοιχεία $a, b \in R \setminus \{0\}$ λέγονται **συντροφικά** όταν $a \mid b$ και -ταυτοχρόνως- $b \mid a$. Επίσης, όταν ικανοποιούνται αυτές οι συνθήκες, αναφέρουμε το $a$ ως **σύντροφο** τού $b$ (ή, ισοδυνάμως, λόγω συμμετρίας, το $b$ ως σύντροφο τού $a$). Η σχέση

$$[a \underset{\text{συν.}}{\sim} b \underset{\text{ορσ}}{\Longleftrightarrow} \text{τα } a \text{ και } b \text{ είναι συντροφικά}]$$

αποτελεί μια σχέση ισοδυναμίας επί τού $R$. Επίσης, όταν ο $R$ είναι ακεραία περιοχή,

$$a \underset{\text{συν.}}{\sim} b \Longleftrightarrow \left[\exists x \in R^{\times} : a = bx\right].$$

Έστω $p$ ένα στοιχείο ενός δακτυλίου $R$. Το $p$ καλείται **πρώτο στοιχείο** τού $R$ όταν $p \in R \setminus (R^{\times} \cup \{0_R\})$ και, επιπροσθέτως, για οιαδήποτε $a, b \in R$ ισχύει η συνεπαγωγή:

$$[p \mid ab \Longrightarrow \text{είτε } p \mid a \text{ είτε } p \mid b].$$

Ένα στοιχείο $q \in R$ καλείται **ανάγωγο στοιχείο** τού $R$ όταν $q \in R \setminus (R^{\times} \cup \{0_R\})$ και, επιπροσθέτως, για οιαδήποτε $a, b \in R$ ισχύει η συνεπαγωγή:

$$[q = ab \Longrightarrow \text{είτε } a \in R^{\times} \text{ είτε } b \in R^{\times}].$$

**1.1.16 Πρόταση.** *Έστω $R$ μια ακεραία περιοχή. Τότε ισχύουν τα ακόλουθα*:

(a) *Το $p \in R \setminus (R^{\times} \cup \{0\})$ είναι πρώτο στοιχείο τής $R$ εάν και μόνον εάν το κύριο ιδεώδες $\langle p \rangle$ είναι ένα γνήσιο, πρώτο ιδεώδες τής $R$.*

(b) *Το $q$ είναι ανάγωγο στοιχείο τής $R$ εάν και μόνον εάν το κύριο ιδεώδες $\langle q \rangle$ είναι ένα μεγιστοτικό στοιχείο τού συνόλου όλων των μη τετριμμένων, γνησίων, κυρίων ιδεωδών τής $R$ (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό).*

(c) *Κάθε πρώτο στοιχείο τής $R$ είναι ανάγωγο.*

(d) *Εάν το $p$ είναι ένα πρώτο στοιχείο τής $R$ και $p \underset{\text{συν.}}{\sim} p'$, τότε και το $p'$ είναι ένα πρώτο στοιχείο τής $R$.*

(e) *Εάν το $q$ είναι ένα ανάγωγο στοιχείο τής $R$ και $q \underset{\text{συν.}}{\sim} q'$, τότε και το $q'$ είναι ένα ανάγωγο στοιχείο τής $R$.*

(f) *Οι μόνοι διαιρέτες ενός αναγώγου στοιχείου $q$ τής $R$ είναι τα συντροφικά του στοιχεία και τα αντιστρέψιμα στοιχεία τής $R$.*

**1.1.17 Πόρισμα.** *Έστω $R$ μια Π.Κ.Ι. Τότε ισχύουν τα ακόλουθα*:

(a) *Το $p$ είναι πρώτο στοιχείο τής $R$ εάν και μόνον εάν το κύριο ιδεώδες $\langle p\rangle$ είναι ένα μη τετριμμένο, γνήσιο, πρώτο ιδεώδες τής $R$.*

(b) *Το $q$ είναι ανάγωγο στοιχείο τής $R$ εάν και μόνον εάν το κύριο ιδεώδες $\langle q\rangle$ είναι ένα μεγιστοτικό ιδεώδες τής $R$.*

(c) *Ένα στοιχείο τού $R\setminus(R^\times\cup\{0\})$ είναι πρώτο στοιχείο τής $R$ εάν και μόνον εάν είναι ανάγωγο.*

**(ix)** Μια ακεραία περιοχή $R$ καλείται **περιοχή με παραγοντοποίηση** όταν κάθε στοιχείο $a\in R\setminus(R^\times\cup\{0\})$ διαθέτει σύντροφο παριστώμενο ως γινόμενο πεπερασμένου πλήθους αναγώγων στοιχείων τής $R$, ήτοι όταν γράφεται υπό τη μορφή

$$a=uq_1q_2\cdots q_k,$$

όπου $u\in R^\times$, $k\in\mathbb{N}$ και τα $q_1,q_2,\ldots,q_k$ είναι ανάγωγα στοιχεία τής $R$. Μια ακεραία περιοχή $R$ καλείται **περιοχή με μονοσήμαντη παραγοντοποίηση** (=: **Π.Μ.Π.**) όταν πληροί τις ακόλουθες συνθήκες:

(a) Η $R$ είναι περιοχή με παραγοντοποίηση και

(b) για οιεσδήποτε παραστάσεις

$$a\underset{\text{συν.}}{\sim}q_1q_2\cdots q_k\underset{\text{συν.}}{\sim}q_1'q_2'\cdots q_l'$$

συντρόφων ενός $a\in R\setminus(R^\times\cup\{0\})$ ως γινομένων πεπερασμένου πλήθους αναγώγων στοιχείων τής $R$, έχουμε $k=l$ και υπάρχει μια μετάταξη $\sigma\in\mathfrak{S}_k$ τού συνόλου $\{1,\ldots,k\}$, τέτοια ώστε να ισχύει $q_{\sigma(j)}\underset{\text{συν.}}{\sim}q_j'$, $\forall j\in\{1,\ldots,k\}$. Σημειωτέον ότι κάθε Π.Μ.Π είναι **περιοχή με μ.κ.δ**.[1]

**1.1.18 Θεώρημα.** *Έστω $R$ μια ακεραία περιοχή. Τότε τα ακόλουθα είναι ισοδύναμα*:

(a) *Η $R$ είναι Π.Μ.Π.*

(b) *Η $R$ είναι περιοχή με παραγοντοποίηση και κάθε στοιχείο $q\in R\setminus(R^\times\cup\{0\})$ είναι πρώτο εάν και μόνον εάν είναι ανάγωγο.*

(c) *Κάθε $a\in R\setminus(R^\times\cup\{0\})$ διαθέτει σύντροφο παριστώμενο ως γινόμενο πεπερασμένου πλήθους πρώτων στοιχείων τής $R$.*

**1.1.19 Θεώρημα.** *Κάθε Π.Κ.Ι. είναι Π.Μ.Π.* (*Το αντίστροφο δεν ισχύει πάντοτε.*)

[1] Εάν $n\in\mathbb{N}$, $n\geq 2$, και τα $a_1,\ldots,a_n$ είναι στοιχεία ενός δακτυλίου $R$, τότε ένα $d\in R$ καλείται **μέγιστος κοινός διαιρέτης** (=: **μκδ**) των $a_1,\ldots,a_n$ όταν ο $d$ διαιρεί καθένα εξ αυτών και, ταυτοχρόνως, για οιοδήποτε $c\in R$, για το οποίο ισχύει $c\mid a_1,\ldots,c\mid a_n$, έχουμε $c\mid d$. Οι μέγιστοι κοινοί διαιρέτες είναι μονοσημάντως ορισμένοι *μέχρις συντροφικότητας*. Μια ακεραία περιοχή $R$ καλείται **περιοχή με μ.κ.δ.** όταν οιαδήποτε $a,b\in R\setminus\{0_R\}$ διαθέτουν μ.κ.δ.

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

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

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

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

όπου

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

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

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

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

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

παρατηρούμε ότι, βάσει των ανωτέρω πράξεων,

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

και, γενικότερα,

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

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

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

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

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

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

**1.1.20 Σημείωση.** Εκ των ανωτέρω συμπεραίνουμε ότι δυο πολυώνυμα

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

είναι **ίσα** (γράφοντας $F(\mathsf{X}) = G(\mathsf{X})$) εάν και μόνον εάν $n = m$ και $a_i = b_i$ για κάθε $i \in \{0, 1, \dots, n\}$.

Εάν

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

τότε λέμε ότι ο αριθμός $\deg(F(\mathsf{X})) := n$ είναι **ο βαθμός** τού πολυωνύμου $F(\mathsf{X})$ και ότι ο $\mathbf{LC}(F(\mathsf{X})) := a_n$ είναι ο **επικεφαλής συντελεστής** (ή ο **μεγιστοβάθμιος συντελεστής**) τού πολυωνύμου $F(\mathsf{X})$. Όταν $\mathbf{LC}(F(\mathsf{X})) = 1_R$, τότε το $F(\mathsf{X})$ καλείται **μονικό πολυώνυμο**. Στην περίπτωση όπου το $F(\mathsf{X}) = 0_{R[\mathsf{X}]}$ είναι το μηδενικό πολυώνυμο, θέτουμε εξ ορισμού[2] $\deg(F(\mathsf{X})) := -\infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση: $-\infty < n, \;\; \forall n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο ο βαθμός των πολυωνύμων μπορεί να εκληφθεί ως μια απεικόνιση

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

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

**1.1.21 Λήμμα.** *Για οιαδήποτε πολυώνυμα* $F(\mathsf{X}), G(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ *ισχύουν τα εξής*:

(a) $\deg(F(\mathsf{X}) + G(\mathsf{X})) \leq \max\{\deg(F(\mathsf{X})), \deg(G(\mathsf{X}))\}$.

(b) $\deg(F(\mathsf{X}) \cdot G(\mathsf{X})) \leq \deg(F(\mathsf{X})) + \deg(G(\mathsf{X}))$.

(c) *Εάν* $\deg(F(\mathsf{X})) \neq \deg(G(\mathsf{X}))$, *τότε*

$$\deg(F(\mathsf{X}) + G(\mathsf{X})) = \max\{\deg(F(\mathsf{X})), \deg(G(\mathsf{X}))\}.$$

(d) *Εάν* $\mathbf{LC}(F(\mathsf{X}))\cdot \mathbf{LC}(G(\mathsf{X})) \neq 0_R$, *τότε*

$$\deg(F(\mathsf{X}) \cdot G(\mathsf{X})) = \deg(F(\mathsf{X})) + \deg(G(\mathsf{X})).$$

[2] Ορισμένοι συγγραφείς δεν επισυνάπτουν βαθμό στο μηδενικό πολυώνυμο. Η προκειμένη, ωστόσο, σύμβαση μας διευκολύνει αισθητά επιτρέποντάς μας οικονομία λόγου στις διατυπώσεις αρκετών προτάσεων.

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

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

(b) *Για οιαδήποτε πολυώνυμα $F(\mathsf{X}), G(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ έχουμε*

$$\deg\left(F(\mathsf{X}) \cdot G(\mathsf{X})\right) = \deg\left(F(\mathsf{X})\right) + \deg(G(\mathsf{X})).$$

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

**1.1.23 Πόρισμα.** *Έστω $\mathbf{k}$ ένα σώμα. Εάν $F(\mathsf{X}), G(\mathsf{X}) \in \mathbf{k}[\mathsf{X}] \setminus \{0_{\mathbf{k}[\mathsf{X}]}\}$, τότε*

$$\deg\left(F(\mathsf{X}) \cdot G(\mathsf{X})\right) = \deg\left(F(\mathsf{X})\right) + \deg(G(\mathsf{X})).$$

*Επιπροσθέτως,*

$$\left(\mathbf{k}\left[\mathsf{X}\right]\right)^\times = \mathbf{k}^\times = \mathbf{k} \setminus \{0_{\mathbf{k}}\} = \left\{ F\left(\mathsf{X}\right) \in \mathbf{k}[\mathsf{X}] \mid \deg(F(\mathsf{X})) = 0 \right\}.$$

Εάν ο $R$ είναι ακεραία περιοχή, τότε εντός τού $R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ κανείς ορίζει διαίρεση και αποδεικνύει την ύπαρξη ενός γενικευμένου αλγορίθμου διαιρέσεως, μεγίστων κοινών διαιρετών κ.λπ. Ωστόσο, ο $R[\mathsf{X}]$ δεν είναι Ε.Π. όταν ο $R$ δεν είναι σώμα.

**1.1.24 Θεώρημα.** *Έστω $\mathbf{k}$ ένα σώμα. Τότε ο πολυωνυμικός δακτύλιος $\mathbf{k}[\mathsf{X}]$ είναι Ε.Π. έχων την $\boldsymbol{\delta}(F(\mathsf{X})) := \deg\left(F(\mathsf{X})\right)$ ως ευκλείδεια στάθμη του. Ως εκ τούτου, ο $\mathbf{k}[\mathsf{X}]$ είναι Π.Κ.Ι. και Π.Μ.Π.*

**(xi)** Έστω $S$ ένας δακτύλιος και έστω $R$ ένας υποδακτύλιος τού $S$. Υποθέτουμε ότι το $F(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i$ είναι ένα πολυώνυμο ανήκον στον $R[\mathsf{X}]$.

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

(b) Εάν $R = S$, $s \in S$ και $F(\mathsf{X}) \in R[\mathsf{X}] \setminus \{0_{R[\mathsf{X}]}\}$ με $F(s) = 0$, και εάν -επιπροσθέτως- έχουμε

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

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

$$\mathrm{mult}_s\left(F\right) := m.$$

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

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

Το $s$ ονομάζεται, ιδιαιτέρως, **απλό** (και αντιστοίχως, **πολλαπλό**) **σημείο μηδενισμού** τού $F(\mathsf{X})$ όταν $\text{mult}_s(F) = 1$ (και αντιστοίχως, όταν $\text{mult}_s(F) \geq 2$).

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

$$F(\mathsf{X}) = \mu(\mathsf{X} - s_1)(\mathsf{X} - s_2)\cdots(\mathsf{X} - s_k), \;\; \mu \in S,$$

τότε λέμε πως το $F$ **διασπάται σε πρωτοβαθμίους παράγοντες υπεράνω τού** $S$.

**1.1.25 Πρόταση.** *Έστω ότι ο $R$ είναι μια ακεραία περιοχή και ότι $a \in R$ και $F(\mathsf{X}) \in R[\mathsf{X}]$. Τότε ισχύουν τα εξής*:

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

(b) *Το $a$ είναι ένα σημείο μηδενισμού τού $F(\mathsf{X})$ (εντός τής $R$)* $\Leftrightarrow \mathsf{X} - a \mid F(\mathsf{X})$.

**1.1.26 Πόρισμα.** *Έστω $R$ μια ακεραία περιοχή. Εάν τα $a_1, a_2, \ldots, a_k$ είναι $k$ σαφώς διακεκριμένα σημεία μηδενισμού ενός πολυωνύμου $F(\mathsf{X}) \in R[\mathsf{X}]$, τότε*

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

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

Ένα σώμα $\mathbf{k}$ καλείται **αλγεβρικώς κλειστό** όταν *κάθε* πολυώνυμο $F(\mathsf{X}) \in \mathbf{k}[\mathsf{X}]$ βαθμού $n \geq 1$ διαθέτει τουλάχιστον ένα σημείο μηδενισμού ανήκον στο $\mathbf{k}$. Όταν το $\mathbf{k}$ είναι αλγεβρικώς κλειστό, τότε κάθε πολυώνυμο $F(\mathsf{X}) \in \mathbf{k}[\mathsf{X}]$ βαθμού $n \geq 1$ διασπάται σε πρωτοβαθμίους παράγοντες υπεράνω τού $\mathbf{k}$ :

$$F(\mathsf{X}) = \mu \prod_{i=1}^{\nu} (\mathsf{X} - \lambda_i)^{m_i},$$

όπου $\mu \in \mathbf{k}$, $\lambda_1, \ldots, \lambda_\nu \in \mathbf{k}$ τα σαφώς διακεκριμένα σημεία μηδενισμού τού $F(\mathsf{X})$, και $m_i = \text{mult}_{\lambda_i}(F)$ για κάθε $i \in \{1, \ldots, \nu\}$, $n = m_1 + \cdots + m_\nu$.

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

**1.1.29 Σημείωση.** Το θεώρημα 1.1.28 πρωτοαποδείχθηκε το έτος 1799 από τον μέγα γερμανό μαθηματικό C.-F. Gauss· εν τω μεταξύ υπάρχουν πολλές δεκάδες πιο σύγχρονων αποδείξεων, οι γνωστότερες των οποίων προέρχονται από τη Μιγαδική Ανάλυση και την Αλγεβρική Τοπολογία. Για περισσότερες πληροφορίες και σύντομες ιστορικές σημειώσεις παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο σύγγραμμα των B. Fine και G. Rosenberger: *Το Θεμελιώδες Θεώρημα τής Άλγεβρας* (σε μετάφραση των Φ. Λιούτση και Ν. Μαρμαρίδη), εκδόσεις Leader Books, Αθήνα, 2001.

Έστω $R$ ένας δακτύλιος. Για κάθε πολυώνυμο $F(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]$ ορίζουμε την **επίτυπη παράγωγό του (ή τύποις παράγωγό του)** $\frac{d}{d\mathsf{X}}(F(\mathsf{X}))$ ως εξής:

$$\frac{d}{d\mathsf{X}}(F(\mathsf{X})) := \begin{cases} \sum\limits_{i=1}^{n} i a_i \mathsf{X}^{i-1} \in R[\mathsf{X}], & \text{όταν το } F \text{ δεν είναι σταθερό,} \\ 0_{R[\mathsf{X}]}, & \text{όταν το } F \text{ είναι σταθερό.} \end{cases}$$

**1.1.30 Πρόταση.** *Για οιαδήποτε $F(\mathsf{X}), G(\mathsf{X}) \in R[\mathsf{X}]$ ισχύουν τα εξής:*

(a) $\frac{d}{d\mathsf{X}}(F(\mathsf{X}) + G(\mathsf{X})) = \frac{d}{d\mathsf{X}}(F(\mathsf{X})) + \frac{d}{d\mathsf{X}}(G(\mathsf{X}))$,

(b) $\frac{d}{d\mathsf{X}}(F(\mathsf{X}) \cdot G(\mathsf{X})) = \frac{d}{d\mathsf{X}}(F(\mathsf{X})) \cdot G(\mathsf{X}) + \frac{d}{d\mathsf{X}}(G(\mathsf{X})) \cdot F(\mathsf{X})$.

**1.1.31 Πρόταση.** *Έστω $\mathbf{k}$ ένα σώμα και έστω $a \in \mathbf{k}$. Εάν $\operatorname{mult}_a(F) = m \geq 2$ για κάποιο $F(\mathsf{X}) \in \mathbf{k}[\mathsf{X}]$, τότε*

$$\operatorname{mult}_a\left(\frac{d}{d\mathsf{X}}(F(\mathsf{X}))\right) \leq m-1 \ \text{ ή } \ \frac{d}{d\mathsf{X}}(F(\mathsf{X})) = 0_{\mathbf{k}[\mathsf{X}]}.$$

**1.1.32 Παρατήρηση.** Επειδή υπάρχει ένα $G(\mathsf{X}) \in \mathbf{k}[\mathsf{X}]$ με $F(\mathsf{X}) = (\mathsf{X}-a)^m G(\mathsf{X})$ και $G(a) \neq 0$, έχουμε

$$\frac{d}{d\mathsf{X}}(F(\mathsf{X})) = (\mathsf{X}-a)^{m-1}\left[mG(\mathsf{X}) + (\mathsf{X}-a)\frac{d}{d\mathsf{X}}(G(\mathsf{X}))\right].$$

Εάν $\text{χαρ}(\mathbf{k}) = 0$, τότε

$$\left[mG(\mathsf{X}) + (\mathsf{X}-a)\frac{d}{d\mathsf{X}}(G(\mathsf{X}))\right](a) = mG(a) \neq 0,$$

οπότε $\operatorname{mult}_a\left(\frac{d}{d\mathsf{X}}(F(\mathsf{X}))\right) = m-1$. Εάν όμως $\text{χαρ}(\mathbf{k}) = p \neq 0$ ($p$ πρώτος, πρβλ. 1.1.1) και ο $m$ είναι ένα πολλαπλάσιο τού $p$, τότε

$$\operatorname{mult}_a\left(\frac{d}{d\mathsf{X}}(F(\mathsf{X}))\right) < m-1 \ \text{ ή } \ \frac{d}{d\mathsf{X}}(F(\mathsf{X})) = 0_{\mathbf{k}[\mathsf{X}]}.$$

Επί παραδείγματι, όταν $F(\mathsf{X}) = \mathsf{X}^p$, έχουμε $\frac{d}{d\mathsf{X}}(F(\mathsf{X})) = p\mathsf{X}^{p-1} = 0_{\mathbf{k}[\mathsf{X}]}$.

**1.1.33 Πόρισμα.** *Έστω $\mathbf{k}$ ένα σώμα και έστω $a \in \mathbf{k}$. Εάν $\operatorname{mult}_a(F) = 1$ για κάποιο πολυώνυμο $F(\mathsf{X}) \in \mathbf{k}[\mathsf{X}]$, τότε το $a$ δεν αποτελεί σημείο μηδενισμού τής $\frac{d}{d\mathsf{X}}(F(\mathsf{X}))$.*

**(xii) Ο δακτύλιος πολυωνύμων $n$ μεταβλητών** $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ με συντελεστές ειλημμένους από έναν δακτύλιο $R$ ορίζεται επαγωγικώς:

$$R[\mathsf{X}_1, \ldots, \mathsf{X}_n] := R[\mathsf{X}_1, \ldots, \mathsf{X}_{n-1}][\mathsf{X}_n],$$

για $n \geq 2$. Ενίοτε, για $n = 1, n = 2$ και $n = 3$ προσήκει απλώς να γράφουμε $R[\mathsf{X}]$, $R[\mathsf{X}, \mathsf{Y}]$ και $R[\mathsf{X}, \mathsf{Y}, \mathsf{Z}]$, αντιστοίχως. Επίσης, για λόγους οικονομίας, συχνά χρησιμοποιούμε τη συντομογραφία $F \in R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ αντί τού $F(\mathsf{X}_1, \ldots, \mathsf{X}_n) \in R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Ένα **μονώνυμο** τού $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι ένα πολυώνυμο τής μορφής

$$\mathsf{X}_1^{i_1}\mathsf{X}_2^{i_2}\cdots\mathsf{X}_n^{i_n}, \;\; i_j \in \mathbb{N}_0, \;\; \forall j \in \{1, \ldots, n\}.$$

Ως **(συνολικός) βαθμός** του ορίζεται το άθροισμα $i_1 + i_2 + \cdots + i_n$. Κάθε πολυώνυμο $F \in R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ γράφεται μονοσημάντως ως άθροισμα πεπερασμένου πλήθους μονωνύμων

$$F = \sum a_{(i_1,i_2,\ldots,i_n)}\mathsf{X}_1^{i_1}\mathsf{X}_2^{i_2}\cdots\mathsf{X}_n^{i_n}, \tag{1.1}$$

όπου $a_{(i_1,i_2,\ldots,i_n)} \in R$. Το $F$ καλείται **ομογενές πολυώνυμο (ή μορφή) βαθμού** $d \geq 0$ όταν οι μόνοι μη μηδενικοί συντελεστές του $a_{(i_1,i_2,\ldots,i_n)}$ είναι αυτοί που προτάσσονται (κάποιων) μονωνύμων βαθμού $d$. Κάθε πολυώνυμο (1.1) γράφεται μονοσημάντως ως άθροισμα

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

Το $F_{(j)}$ είναι είτε μηδενικό είτε ομογενές πολυώνυμο βαθμού $j$. Εάν υπάρχει τουλάχιστον ένα $j \geq 0$ με το $F_{(j)}$ μη μηδενικό, τότε ορίζουμε τον

$$\deg(F) := \max\left\{ j \in \mathbb{N}_0 \middle| \, F_{(j)} \neq 0_{R[\mathsf{X}_1,\ldots,\mathsf{X}_n]} \right\}$$

ως τον **(συνολικό) βαθμό** τού $F$. (Ειδάλλως, το $F$ είναι το μηδενικό πολυώνυμο, στο οποίο μπορούμε, όπως προηγουμένως, να επισυνάψουμε βαθμό «$-\infty$».)

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

(a) *Ο δακτύλιος $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι ακεραία περιοχή.*

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

$$\deg(F \cdot G) = \deg(F) + \deg(G).$$

**1.1.35 Σημείωση.** Εάν το $\mathbf{k}$ είναι ένα σώμα, τότε το σύνολο

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

των μονωνύμων τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ αποτελεί προφανώς μια βάση τού (απειροδιάστατου) $\mathbf{k}$-*διανυσματικού χώρου* $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$.

**1.1.36 Θεώρημα.** *Εάν ένας δακτύλιος $R$ είναι Π.Μ.Π, τότε και ο $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι ωσαύτως Π.Μ.Π.*

Ο $\mathbb{Z}[\mathsf{X}]$ είναι μια Π.Μ.Π. που δεν είναι Π.Κ.Ι. (διότι π.χ. το $I = \langle 2, \mathsf{X} \rangle$ δεν είναι κύριο).

Εάν το $\mathbf{k}$ είναι ένα σώμα, τότε το σώμα κλασμάτων

$$\mathbf{k}(\mathsf{X}_1, \dots, \mathsf{X}_n) := \mathbf{Fr}(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n])$$

τής Π.Μ.Π. $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ καλείται, ιδιαιτέρως, **σώμα των ρητών συναρτήσεων** ή **ρητών εκφράσεων** σε $n$ **μεταβλητές** υπεράνω τού $\mathbf{k}$.

Τέλος, για οιονδήποτε δακτύλιο $R$, $F \in R[\mathsf{X}_1, \dots, \mathsf{X}_n]$ και οιονδήποτε $i \in \{1, \dots, n\}$ ορίζουμε ως **μερική επίτυπη παράγωγό του** (ή **μερική τύποις παράγωγό του**)

$$\frac{\partial}{\partial \mathsf{X}_i}(F) := \frac{\partial}{\partial \mathsf{X}_i}(F(\mathsf{X}_1, \dots, \mathsf{X}_n))$$

**ως προς τη μεταβλητή** $\mathsf{X}_i$ την επίτυπη παράγωγό του ως προς τη μεταβλητή $\mathsf{X}_i$ *θεωρώντας το ως πολυώνυμο μίας μεταβλητής εντός τού*

$$R[\mathsf{X}_1, \dots, \widehat{\mathsf{X}}_i, \dots, \mathsf{X}_n][\mathsf{X}_i] \cong R[\mathsf{X}_1, \dots, \mathsf{X}_n]$$

(όπου το $\widehat{\mathsf{X}}_i$ υποδηλοί την αφαίρεση τού $\mathsf{X}_i$).

**1.1.37 Πρόταση.** (a) *Εάν* $G_1, \dots, G_n \in R[\mathsf{X}]$ *και* $F \in R[\mathsf{X}_1, \dots, \mathsf{X}_n]$, *τότε*

$$\frac{d}{d\mathsf{X}} F(G_1(\mathsf{X}), \dots, G_n(\mathsf{X})) = \sum_{i=1}^{n} \frac{\partial}{\partial \mathsf{X}_i}(F(G_1, \dots, G_n)) \frac{d}{d\mathsf{X}}(G_i(\mathsf{X})).$$

(b) *Εάν* $F \in R[\mathsf{X}_1, \dots, \mathsf{X}_n]$, *τότε για οιαδήποτε* $i, j \in \{1, \dots, n\}$ *ισχύει η ισότητα*

$$\frac{\partial}{\partial \mathsf{X}_i}\left(\frac{\partial}{\partial \mathsf{X}_j}(F)\right) = \frac{\partial}{\partial \mathsf{X}_j}\left(\frac{\partial}{\partial \mathsf{X}_i}(F)\right).$$

(c) Τύπος Euler: *Εάν το* $F \in R[\mathsf{X}_1, \dots, \mathsf{X}_n]$ *είναι ομογενές πολυώνυμο βαθμού* $d$, *τότε*

$$d \cdot F = \sum_{i=1}^{n} \mathsf{X}_i \frac{\partial}{\partial \mathsf{X}_i}(F).$$

## Ασκήσεις

**Α-1-1.** Έστω $R$ μια ακεραία περιοχή.

(a) Εάν τα $F$ και $G$ είναι δυο ομογενή πολυώνυμα βαθμού $r$ και $s$, αντιστοίχως, ανήκοντα στον $R[\mathsf{X}_1, \dots, \mathsf{X}_n]$, να αποδειχθεί ότι το γινόμενό τους $FG$ είναι ένα ομογενές πολυώνυμο βαθμού $r + s$.

(b) Να αποδειχθεί ότι όλοι οι παράγοντες ενός ομογενούς πολυωνύμου από τον $R[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι ομογενή πολυώνυμα.

**A-1-2.** Έστω $R$ μια Π.Μ.Π. και έστω $\mathbf{Fr}(R)$ το σώμα κλασμάτων τής $R$. Να αποδειχθεί ότι κάθε στοιχείο $z$ τού $\mathbf{Fr}(R)$ μπορεί να γραφεί υπό τη μορφή $z = \frac{a}{b}$, όπου τα στοιχεία $a \in R, b \in R \setminus \{0_R\}$, δεν έχουν (γνήσιους) κοινούς παράγοντες (ήτοι μη αντιστρεψίμους διαιρέτες). Τούτη η παράσταση είναι μονοσημάντως ορισμένη, με μόνη εξαίρεση τον πολλαπλασιασμό (καθενός των $a, b$) με κάποιο αντιστρέψιμο στοιχείο τής $R$.

**A-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 $a_1, \ldots, a_n \in \mathbf{k}$, να αποδειχθεί ότι[5] $F = 0$. (*Υπόδειξη*: Το $F$ γράφεται ως άθροισμα $F = \sum_{i=1}^{\nu} F_i \mathsf{X}_n^i$, για κάποια πολυώνυμα $F_1, \ldots, F_\nu \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_{n-1}]$. Να χρησιμοποιηθεί μαθηματική επαγωγή επί τού $n$, καθώς και το γεγονός ότι το $F(a_1, \ldots, a_{n-1}, \mathsf{X}_n)$ διαθέτει μόνον πεπερασμένα σημεία μηδενισμού όταν $F_i(a_1, \ldots, a_{n-1}) \neq 0$ για όλα τα $i \in \{1, \ldots, \nu\}$.)

**A-1-4.** Έστω $\mathbf{k}$ οιοδήποτε σώμα. Να αποδειχθεί ότι υπάρχουν άπειρα ανάγωγα μονικά πολυώνυμα εντός τού $\mathbf{k}[\mathsf{X}]$. (*Υπόδειξη*: Να υποτεθεί ότι υπάρχουν μόνον πεπερασμένου πλήθους ανάγωγα μονικά πολυώνυμα εντός τού $\mathbf{k}[\mathsf{X}]$, ας πούμε τα $F_1, \ldots, F_n$, και κατόπιν να παραγοντοποιηθεί το $F_1 \cdots F_n + 1$, προκειμένου να αναφανεί η αντίφαση.)

**A-1-5.** Να αποδειχθεί ότι κάθε αλγεβρικώς κλειστό σώμα είναι απειροπληθές.

**A-1-6.** Να αποδειχθούν οι προτάσεις 1.1.34 και 1.1.37.

**A-1-7.** Έστω ότι το $\mathbf{k}$ είναι ένα σώμα, $F \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, και ότι τα $a_1, \ldots, a_n \in \mathbf{k}$.
(a) Να αποδειχθεί ότι

$$F = \sum \lambda_{(i_1, i_2, \ldots, i_n)} (\mathsf{X}_1 - a_1)^{i_1} \cdots (\mathsf{X}_n - a_n)^{i_n}$$

όπου $\lambda_{(i_1, i_2, \ldots, i_n)} \in \mathbf{k}$.
(b) Εάν $F(a_1, \ldots, a_n) = 0$, να αποδειχθεί ότι

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

για κάποια (όχι κατ' ανάγκην μονοσημάντως ορισμένα για $n \geq 2$) πολυώνυμα

$$G_1, \ldots, G_n \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n].$$

[5] Τούτο σημαίνει, ιδιαιτέρως, ότι για οιοδήποτε απειροπληθές σώμα $\mathbf{k}$ η «απεικόνιση αποτιμήσεως»

$$\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \ni F \longmapsto ((a_1, \ldots, a_n) \longmapsto F(a_1, \ldots, a_n)) \in \mathrm{A\Pi}(\mathbf{k}^n, \mathbf{k})$$

είναι ενριπτική. Όταν το $\mathbf{k}$ είναι πεπερασμένο, αυτό δεν είναι εν γένει αληθές. Π.χ., για $n = 2$, $\mathbf{k} = \mathbb{Z}_2$ και $F = \mathsf{X}^2\mathsf{Y} + \mathsf{X}\mathsf{Y}^2$ έχουμε $F([a]_2, [b]_2) = 0$ για όλα τα $[a]_2, [b]_2 \in \mathbb{Z}_2$, παρότι το $F$ είναι μη μηδενικό.

## 1.2 Συσχετικός Χώρος και Αλγεβρικά Σύνολα

Έστω $\mathbf{k}$ ένα σώμα. Κάνοντας χρήση τού συμβόλου $\mathbb{A}^n_{\mathbf{k}}$, όπου $n \in \mathbb{N}$, θα εννοούμε το καρτεσιανό γινόμενο τού $\mathbf{k}$ με τον εαυτό του $n$ φορές. Ως εκ τούτου, το $\mathbb{A}^n_{\mathbf{k}}$ είναι το σύνολο όλων των $n$-άδων στοιχείων ειλημμένων από το $\mathbf{k}$. Το $\mathbb{A}^n_{\mathbf{k}}$ καλείται ο $n$-**διάστατος συσχετικός** (ή **αφφινικός**) **χώρος υπεράνω τού** $\mathbf{k}$, ενώ τα στοιχεία του λέγονται **σημεία**. Ιδιαιτέρως, το $\mathbb{A}^1_{\mathbf{k}}$ καλείται **συσχετική ευθεία** και το $\mathbb{A}^2_{\mathbf{k}}$ **συσχετικό επίπεδο**.

Εάν θεωρήσουμε ένα πολυώνυμο $F \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, τότε ένα σημείο

$$P = (a_1, \dots, a_n) \in \mathbb{A}^n_{\mathbf{k}}$$

καλείται **σημείο μηδενισμού** (ή **θέση μηδενισμού**) τού $F$, όταν ισχύει

$$F(P) = F(a_1, \dots, a_n) = 0.$$

Εάν το $F$ δεν είναι σταθερό, λέμε ότι το σύνολο των σημείων μηδενισμού τού $F$ είναι **η υπερεπιφάνεια η οριζόμενη από το** $F$ και τη συμβολίζουμε ως $\mathbf{V}(F)$. Μια υπερεπιφάνεια εντός τού συσχετικού επιπέδου $\mathbb{A}^2_{\mathbf{k}}$ ονομάζεται **συσχετική επίπεδη καμπύλη**. Μια υπερεπιφάνεια εντός τού $\mathbb{A}^3_{\mathbf{k}}$ ονομάζεται **συσχετική (χωρική) επιφάνεια**. Εάν το $F$ είναι ένα πολυώνυμο βαθμού 1, τότε λέμε ότι η $\mathbf{V}(F)$ είναι ένα **υπερεπίπεδο** εντός τού $\mathbb{A}^n_{\mathbf{k}}$.

Γενικότερα, εάν το $\mathcal{S}$ είναι οιοδήποτε σύνολο πολυωνύμων από τον $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, θέτουμε

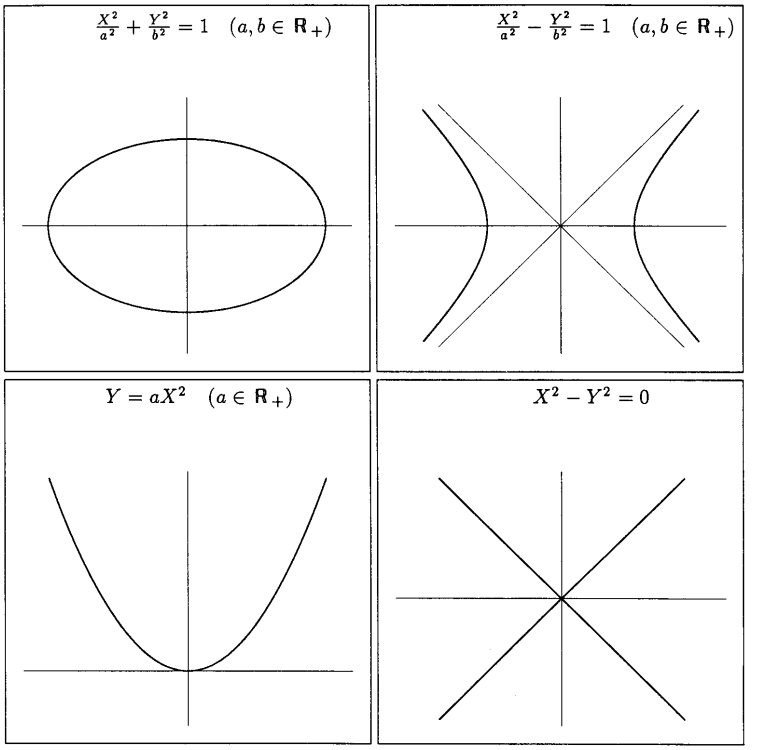
$$\mathbf{V}(\mathcal{S}) := \{P \in \mathbb{A}^n_{\mathbf{k}} \mid F(P) = 0, \ \text{για όλα τα} \ \ F \in \mathcal{S}\} = \bigcap_{F \in \mathcal{S}} \mathbf{V}(F).$$

(Όταν το $\mathcal{S}$ συμβαίνει να είναι πεπερασμένο, π.χ. $\mathcal{S} = \{F_1, \dots, F_\kappa\}$, συνήθως αντί τού $\mathbf{V}(\{F_1, \dots, F_\kappa\})$ γράφουμε $\mathbf{V}(F_1, \dots, F_\kappa)$).

**1.2.1 Ορισμός.** Ορίζουμε ως **συσχετικό αλγεβρικό σύνολο** ή, απλώς, ως **αλγεβρικό σύνολο**, κάθε υποσύνολο $X \subseteq \mathbb{A}^n_{\mathbf{k}}$ για το οποίο ισχύει: $X = \mathbf{V}(\mathcal{S})$, για κάποιο σύνολο πολυωνύμων $\mathcal{S}$ από τον $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$.

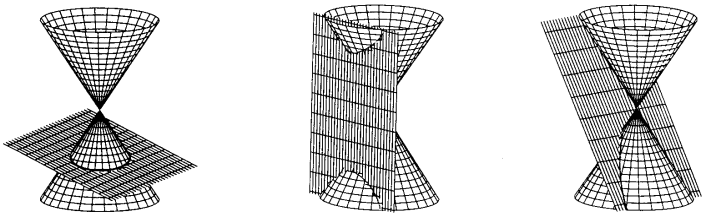
**1.2.2 Παραδείγματα.** (a) Από την κλασική Αναλυτική Γεωμετρία είναι γνωστό ότι οι συσχετικές επίπεδες καμπύλες $\mathbf{V}(F) \subset \mathbb{A}^2_{\mathbb{R}}$ με $\deg(F) = 2$ είναι οι λεγόμενες **κωνικές τομές**. Στο σχήμα **1** δίνονται κατά σειράν οι εξισώσεις που καθορίζουν τη συνήθη **έλλειψη**, **υπερβολή** και **παραβολή**, καθώς και εκείνη ενός **ζεύγους ευθειών** (οι οποίες σχηματίζουν

ορθή γωνία).



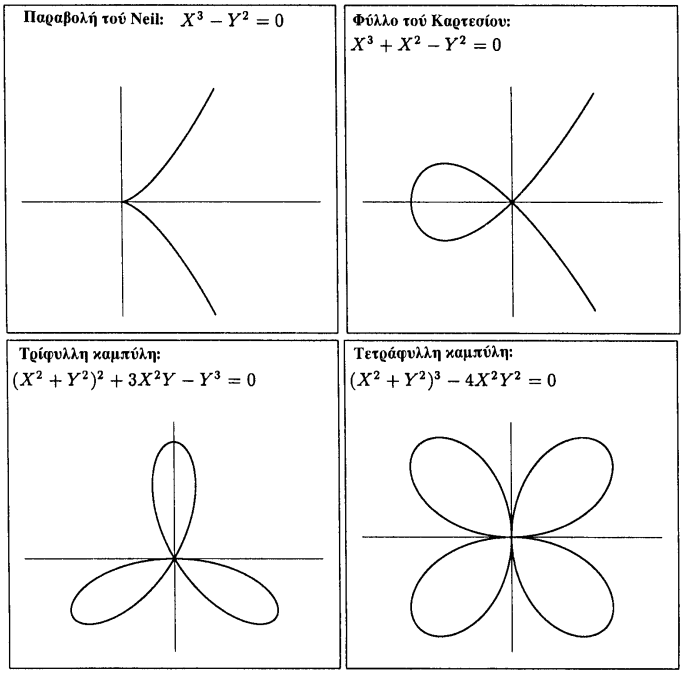

**Σχήμα 1**

Η πρώτη συστηματική μελέτη των κωνικών τομών οφείλεται στον Απολλώνιο από την Πέργαμο (262-190 π.Χ.). Περιώνυμες υπήρξαν οι εφαρμογές τους στους νόμους τού J. Kepler (1571-1630) και στη Μηχανική τού I. Newton (1643-1727). Όπως δηλοί και η ονομασία τους, αυτές προκύπτουν ως τομές ενός (διπλού) κώνου με ένα καταλλήλως επιλεγμένο επίπεδο. (Βλ. σχ. **2**.)

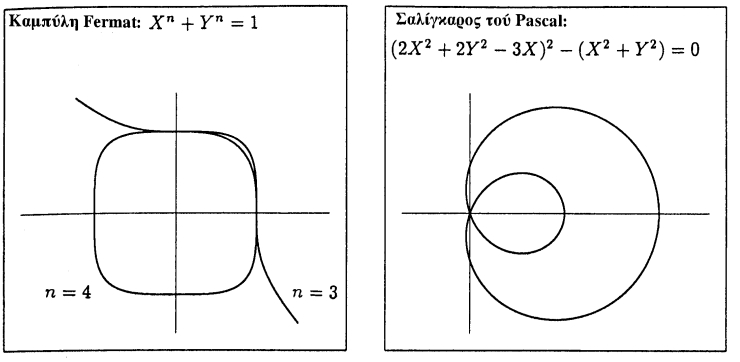


**Σχήμα 2**

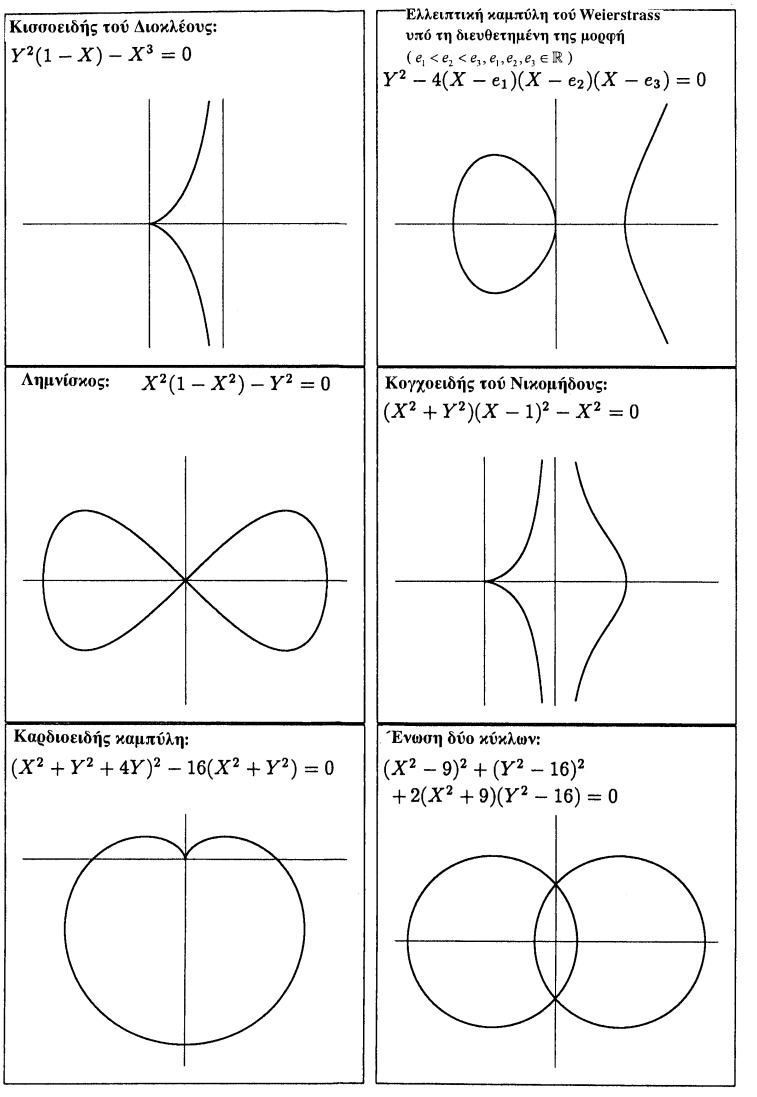
(b) Ειδικές συσχετικές επίπεδες καμπύλες $\mathbf{V}(F) \subset \mathbb{A}^2_{\mathbb{R}}$ με $\deg(F) \geq 3$ (μαζί με τα χαρακτηριστικές ονομασίες τους) εικονογραφούνται στα σχήματα **3**, **4** και **5**.




**Σχήμα 3**

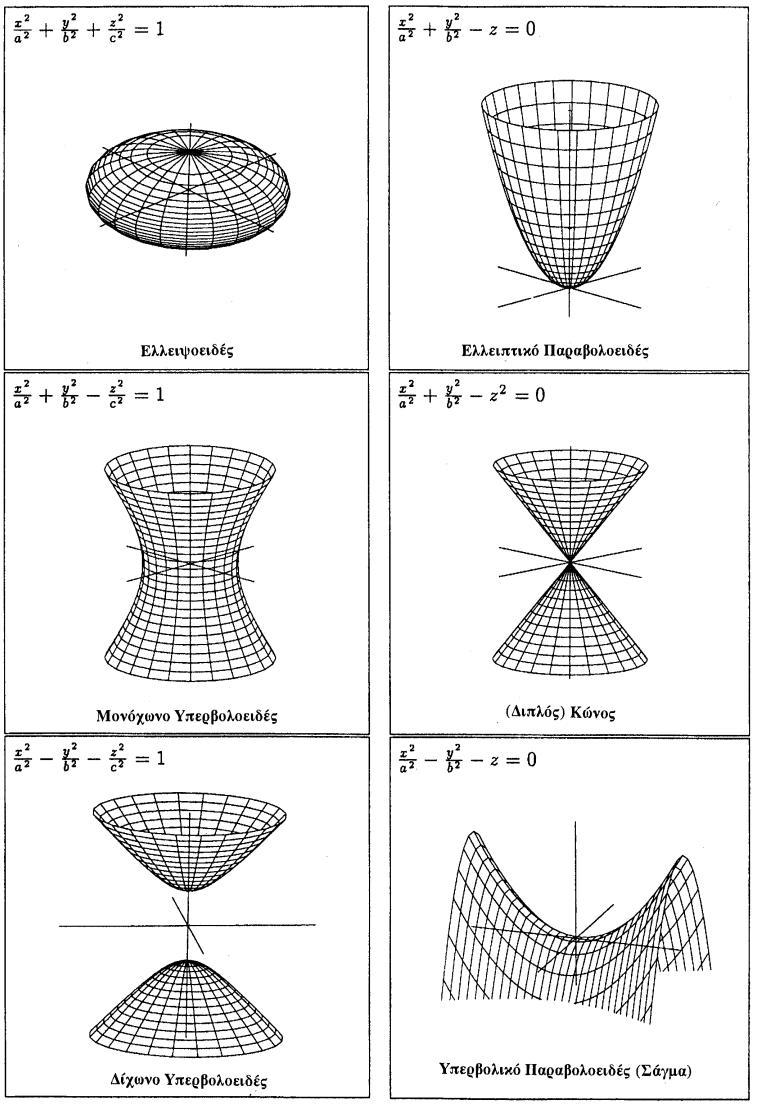



**Σχήμα 4**

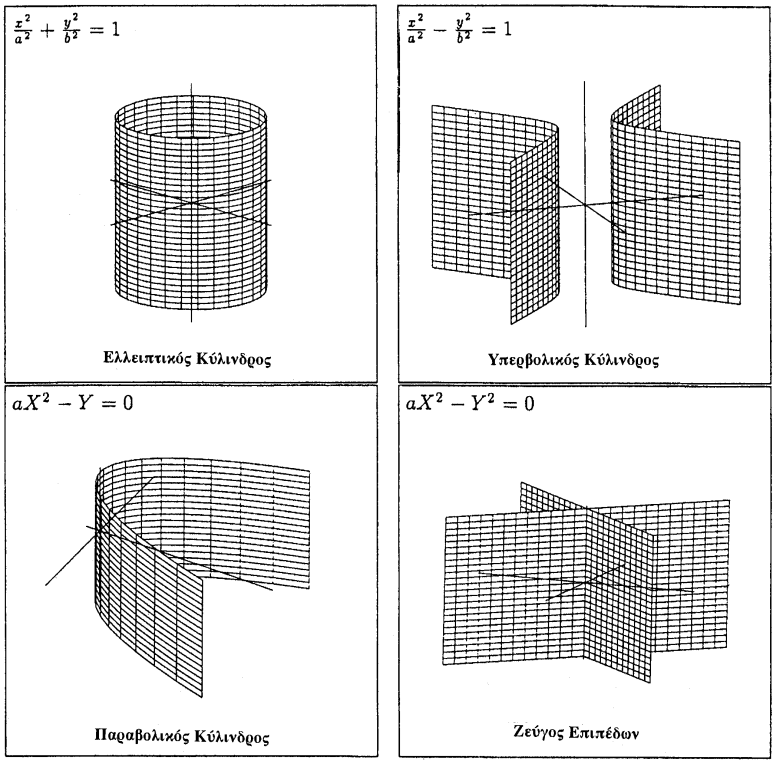

Κισσοειδής τού Διοκλέους:
$Y^2(1-X)-X^3=0$
Ελλειπτική καμπύλη τού Weierstrass
υπό τη διευθετημένη της μορφή
$(e_1<e_2<e_3, e_1,e_2,e_3\in\mathbb{R})$
$Y^2-4(X-e_1)(X-e_2)(X-e_3)=0$
Λημνίσκος: $X^2(1-X^2)-Y^2=0$
Κογχοειδής τού Νικομήδους:
$(X^2+Y^2)(X-1)^2-X^2=0$
Καρδιοειδής καμπύλη:
$(X^2+Y^2+4Y)^2-16(X^2+Y^2)=0$
Ένωση δύο κύκλων:
$(X^2-9)^2+(Y^2-16)^2$
$+2(X^2+9)(Y^2-16)=0$

**Σχήμα 5**

(c) Από την ταξινόμηση των συσχετικών επιφανειών $\mathbf{V}(F) \subset \mathbb{A}^3_{\mathbb{R}}$ με $\deg(F) = 2$ (στο πλαίσιο τής κλασικής Αναλυτικής Γεωμετρίας) υπάρχει εξοικείωση με τις επιφάνειες των σχημάτων **6** και **7**.

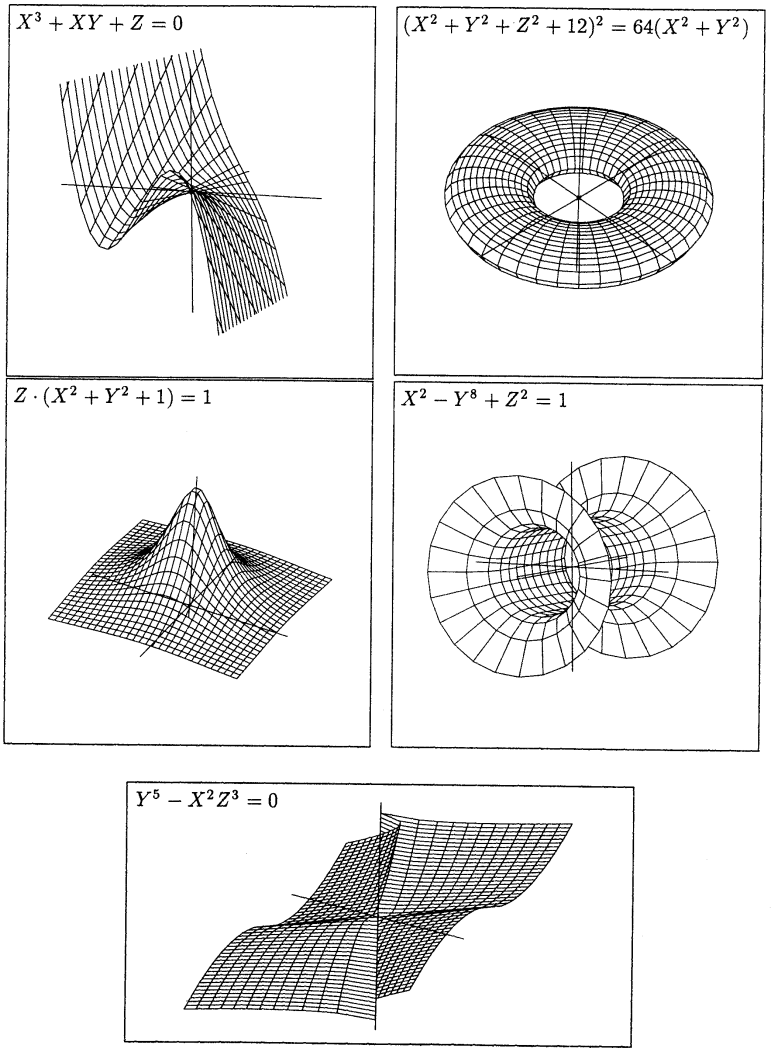



**Σχήμα 6**


$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$
Ελλειπτικός Κύλινδρος
$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$
Υπερβολικός Κύλινδρος
$aX^2 - Y = 0$
Παραβολικός Κύλινδρος
$aX^2 - Y^2 = 0$
Ζεύγος Επιπέδων

**Σχήμα 7**

(d) Στο σχήμα **8** εικονογραφούνται ορισμένες συσχετικές επιφάνειες $\mathbf{V}(F) \subset \mathbb{A}^3_{\mathbb{R}}$ με $\deg(F) \geq 3$.




**Σχήμα 8**

**1.2.3 Πρόταση.** *Έστω* $\mathbf{k}$ *ένα σώμα. Τότε ισχύουν τα εξής*:

(1) *Εάν το* $I$ *είναι ένα ιδεώδες τού* $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ *παραγόμενο από ένα σύνολο* $\mathcal{S}$*, τότε*

$$\mathbf{V}(\mathcal{S}) = \mathbf{V}(I),$$

(οπότε κάθε αλγεβρικό σύνολο είναι ίσο με $\mathbf{V}(I)$ για κάποιο ιδεώδες $I$).

(2) *Εάν η* $\{I_\lambda \mid \lambda \in \Lambda\}$ *είναι μια συλλογή ιδεωδών τού* $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$*, τότε*

$$\mathbf{V}(\bigcup_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda} \mathbf{V}(I_\lambda).$$

(Επομένως, η τομή οιασδήποτε συλλογής αλγεβρικών συνόλων αποτελεί ένα αλγεβρικό σύνολο.)

(3) *Εάν τα* $I, J$ *είναι ιδεώδη τού δακτυλίου* $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$*, με* $I \subseteq J$*, τότε*

$$\mathbf{V}(I) \supseteq \mathbf{V}(J).$$

(4) *Εάν* $F, G \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$*, τότε*

$$\mathbf{V}(FG) = \mathbf{V}(F) \cup \mathbf{V}(G),$$

*ενώ εάν τα* $I, J$ *είναι ιδεώδη τού δακτυλίου* $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$*, τότε*

$$\mathbf{V}(I) \cup \mathbf{V}(J) = \mathbf{V}(\{FG \mid F \in I,\ G \in J\}).$$

(Συνεπώς, η ένωση πεπερασμένου πλήθους αλγεβρικών συνόλων αποτελεί ένα αλγεβρικό σύνολο.)

(5) $\mathbf{V}(0) = \mathbb{A}^n_{\mathbf{k}}$ *και* $\mathbf{V}(1) = \varnothing$*. Επίσης, για* $a_1, \ldots, a_n \in \mathbf{k}$*, έχουμε*

$$\mathbf{V}(\mathsf{X}_1 - a_1, \ldots, \mathsf{X}_n - a_n) = \{(a_1, \ldots, a_n)\}.$$

(Άρα κάθε πεπερασμένο υποσύνολο τού $\mathbb{A}^n_{\mathbf{k}}$ είναι αλγεβρικό).

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς $\mathbf{V}(\mathcal{S}) \subseteq \mathbf{V}(I)$. Πράγματι· εάν $P \in \mathbf{V}(\mathcal{S})$ και $G \in I = \langle \mathcal{S} \rangle$, τότε $\exists k \in \mathbb{N}$ και $a_1, \ldots, a_k \in \mathbf{k}$, $F_1, \ldots, F_k \in \mathcal{S}$ με

$$G = \sum_{i=1}^{k} a_i F_i \Longrightarrow G(P) = \sum_{i=1}^{k} a_i F_i(P) = 0_{\mathbf{k}} \Longrightarrow P \in \mathbf{V}(I).$$

Και αντιστρόφως· εάν $P \in \mathbf{V}(I)$, τότε $G(P) = 0_{\mathbf{k}}$, $\forall G \in I$, οπότε $F(P) = 0_{\mathbf{k}}$, $\forall F \in \mathcal{S}$, απ' όπου συμπεραίνουμε ότι $P \in \mathbf{V}(\mathcal{S})$. Άρα $\mathbf{V}(I) \subseteq \mathbf{V}(\mathcal{S})$.

(2) Κατ' αρχάς $\mathbf{V}(\bigcup_{\lambda\in\Lambda} I_\lambda) \subseteq \bigcap_{\lambda\in\Lambda} \mathbf{V}(I_\lambda)$. Πράγματι· εάν $P \in \mathbf{V}(\bigcup_{\lambda\in\Lambda} I_\lambda)$ και εάν θεωρήσουμε οιονδήποτε δείκτη $\mu \in \Lambda$ και ένα πολυώνυμο $G_\mu \in I_\mu$, τότε $G_\mu \in \bigcup_{\lambda\in\Lambda} I_\lambda$. Εξ υποθέσεως, $G_\mu(P) = 0_{\mathbf{k}}$, πράγμα που σημαίνει ότι $P \in \bigcap_{\lambda\in\Lambda} \mathbf{V}(I_\lambda)$. Και αντιστρόφως· εάν $P \in \bigcap_{\lambda\in\Lambda} \mathbf{V}(I_\lambda)$ και εάν θεωρήσουμε τυχόν πολυώνυμο $F \in \bigcup_{\lambda\in\Lambda} I_\lambda$, θα υπάρχει ένας δείκτης $\lambda_0 \in \Lambda : F \in I_{\lambda_0}$. Εξ υποθέσεως, $F(P) = 0_{\mathbf{k}}$. Επομένως, $F(P) = 0_{\mathbf{k}}$, $\forall F \in \bigcup_{\lambda\in\Lambda} I_\lambda$, οπότε $P \in \mathbf{V}(\bigcup_{\lambda\in\Lambda} I_\lambda)$. Κατά συνέπειαν, $\bigcap_{\lambda\in\Lambda} \mathbf{V}(I_\lambda) \subseteq \mathbf{V}(\bigcup_{\lambda\in\Lambda} I_\lambda)$.

(3) Έστω $P \in \mathbf{V}(J)$ και έστω $F \in I$ με $I \subseteq J$. Τότε $F \in J \Longrightarrow F(P) = 0_{\mathbf{k}}$. Συνεπώς,

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

(4) Προφανώς, $P \in \mathbf{V}(FG)$ ισοδυναμεί με τη συνθήκη

$$FG(P) = F(P)G(P) = 0_{\mathbf{k}} \Longleftrightarrow [\text{είτε } F(P) = 0_{\mathbf{k}} \text{ είτε } G(P) = 0_{\mathbf{k}}] \Longleftrightarrow P \in \mathbf{V}(F) \cup \mathbf{V}(G).$$

Εάν τα $I, J$ είναι ιδεώδη τού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ και $P \in \mathbf{V}(I) \cup \mathbf{V}(J)$, τότε είτε $P \in \mathbf{V}(I)$ είτε $P \in \mathbf{V}(J)$. Επειδή

$$\mathbf{V}(I) \subseteq \mathbf{V}(\{FG \mid F \in I,\ G \in J\}),\ \mathbf{V}(J) \subseteq \mathbf{V}(\{FG \mid F \in I,\ G \in J\}),$$

έχουμε $P \in \mathbf{V}(\{FG \mid F \in I,\ G \in J\})$. Και εάν, αντιστρόφως, θεωρήσουμε ένα σημείο $P \in \mathbf{V}(\{FG \mid F \in I,\ G \in J\})$, τότε για κάθε $F \in I$ και για κάθε $G \in J$

$$FG(P) = 0_{\mathbf{k}} \Longrightarrow P \in \mathbf{V}(F) \cup \mathbf{V}(G),$$

οπότε $P \in \mathbf{V}(I) \cup \mathbf{V}(J)$.

(5) Οι ισότητες αυτές είναι προφανείς. □

**1.2.4 Ορισμός.** Έστω $\mathbf{k}$ ένα σώμα και έστω $n \in \mathbb{N}$. Θέτοντας

$$\mathcal{T}_{\text{Zar}} := \{\mathbb{A}^n_{\mathbf{k}} \smallsetminus V \,|\, V \text{ αλγεβρικά σύνολα εντός τού } \mathbb{A}^n_{\mathbf{k}}\}$$

το ζεύγος $(\mathbb{A}^n_{\mathbf{k}}, \mathcal{T}_{\text{Zar}})$ (λόγω των (2), (4) και (5) τής προτάσεως 1.2.3) αποτελεί έναν τοπολογικό χώρο επί τού $\mathbb{A}^n_{\mathbf{k}}$ (με τα αλγεβρικά ως κλειστά υποσύνολά του). Η $\mathcal{T}_{\text{Zar}}$ καλείται **τοπολογία (τού) Zariski** επί τού $\mathbb{A}^n_{\mathbf{k}}$. Γενικότερα, επί τυχόντος υποσυνόλου $X$ τού $\mathbb{A}^n_{\mathbf{k}}$ ορίζεται η **σχετική τοπολογία (τού) Zariski**

$$\mathcal{T}_{\text{Zar}}|_X := X \cap \{\mathbb{A}^n_{\mathbf{k}} \smallsetminus V \,|\, V \text{ αλγεβρικά σύνολα εντός τού } \mathbb{A}^n_{\mathbf{k}}\}.$$

**1.2.5 Σημείωση.** Όταν $\mathbf{k} = \mathbb{R}$ (και αντιστοίχως, $\mathbf{k} = \mathbb{C}$), τότε κάθε ανοικτό υποσύνολο τού $\mathbb{A}^n_{\mathbb{R}}$ (και αντιστοίχως, τού $\mathbb{A}^n_{\mathbb{C}}$) ως προς την τοπολογία Zariski είναι ανοικτό και ως προς τη συνήθη (ευκλείδεια) τοπολογία. Το αντίστροφο δεν είναι αληθές. Επί παραδείγματι, το

$$\mathbb{A}^2_{\mathbb{R}} \smallsetminus \{(x, y) \in \mathbb{A}^2_{\mathbb{R}} \mid y = \sin(x)\}$$

είναι ανοικτό ως προς τη συνήθη τοπολογία επί τού $\mathbb{A}^2_{\mathbb{R}}$ και μη ανοικτό ως προς την τοπολογία Zariski. (Πρβλ. άσκηση **A-1-13** (a).) Μάλιστα, όταν το σώμα αναφοράς μας είναι απειροπληθές, η τοπολογία Zariski δεν είναι τοπολογία Hausdorff, όπως έπεται από την ακόλουθη πρόταση:

**1.2.6 Πρόταση.** *Έστω* $\mathbf{k}$ *ένα απειροπληθές σώμα και έστω* $n \in \mathbb{N}$. *Τότε δυο τυχόντα μη κενά ανοικτά υποσύνολα τού* $\mathbb{A}^n_{\mathbf{k}}$ *ως προς την τοπολογία Zariski διαθέτουν πάντοτε μη κενή τομή.* (*Ως εκ τούτου, κάθε μη κενό ανοικτό υποσύνολο τού* $\mathbb{A}^n_{\mathbf{k}}$ *είναι* «παντού πυκνό» *ως προς την τοπολογία Zariski.*)

ΑΠΟΔΕΙΞΗ. Εάν τα $U_1, U_2$ είναι δυο τυχόντα μη κενά ανοικτά υποσύνολα τού $\mathbb{A}^n_{\mathbf{k}}$ ως προς την τοπολογία Zariski, τότε υπάρχουν *μη τετριμμένα* [6] ιδεώδη $I, J$ τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ με $U_1 = \mathbb{A}^n_{\mathbf{k}} \smallsetminus \mathbf{V}(I)$ και $U_2 = \mathbb{A}^n_{\mathbf{k}} \smallsetminus \mathbf{V}(J)$. Κατά το (4) τής προτάσεως 1.2.3,

$$U_1 \cap U_2 = \mathbb{A}^n_{\mathbf{k}} \smallsetminus (\mathbf{V}(I) \cup \mathbf{V}(J)) = \mathbb{A}^n_{\mathbf{k}} \smallsetminus \mathbf{V}\left(\{FG \mid F \in I,\ G \in J\}\right).$$

Επειδή τα $I, J$ είναι μη τετριμμένα ιδεώδη (τής *ακεραίας περιοχής* $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$), το ιδεώδες $\langle FG \mid F \in I,\ G \in J\rangle$ θα είναι ωσαύτως μη τετριμμένο, οπότε $U_1 \cap U_2 \neq \varnothing$. □

## Ασκήσεις

**A-1-8.** Να αποδειχθεί ότι τα αλγεβρικά υποσύνολα τού $\mathbb{A}^1_{\mathbf{k}}$ (ήτοι τα κλειστά υποσύνολά του ως προς την $\mathcal{T}_{\text{Zar}}$) είναι ακριβώς τα πεπερασμένα υποσύνολα, μαζί με το $\varnothing$ και το ίδιο το $\mathbb{A}^1_{\mathbf{k}}$.

**A-1-9.** Εάν το $\mathbf{k}$ είναι ένα πεπερασμένο σώμα, να αποδειχθεί ότι όλα τα υποσύνολα τού $\mathbb{A}^n_{\mathbf{k}}$ είναι αλγεβρικά (ήτοι κλειστά ως προς την $\mathcal{T}_{\text{Zar}}$).

**A-1-10.** Να δοθεί ένα παράδειγμα μιας αριθμήσιμης οικογενείας αλγεβρικών συνόλων εντός ενός συσχετικού χώρου $\mathbb{A}^n_{\mathbf{k}}$, η ένωση των οποίων δεν είναι αλγεβρικό υποσύνολό του.

**A-1-11.** Να αποδειχθεί ότι τα ακόλουθα σύνολα είναι αλγεβρικά:

(a) Το $\left\{\left(t, t^2, t^3\right) \in \mathbb{A}^3_{\mathbf{k}} \mid t \in \mathbf{k}\right\}$,

(b) το $\left\{(\cos(t), \sin(t)) \in \mathbb{A}^2_{\mathbb{R}} \mid t \in \mathbb{R}\right\}$, και

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

[6] Εδώ χρησιμοποιείται μια ισχυροποίηση τής πρώτης ισότητας τού (5) τής προτάσεως 1.2.3: Εάν το $\mathbf{k}$ είναι απειροπληθές σώμα και το $I$ ένα ιδεώδες τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τότε $\mathbf{V}(I) = \mathbb{A}^n_{\mathbf{k}} \iff I = \{0\}$. Η κατεύθυνση "$\Longrightarrow$" έπεται από την άσκηση **A-1-3**.

**A-1-12.** Έστω ότι η $C$ είναι μια συσχετική επίπεδη καμπύλη και ότι η $L$ είναι μια ευθεία εντός τού $\mathbb{A}^2_{\mathbf{k}}$, ούτως ώστε να ισχύει $L \nsubseteq C$. Εάν $C = \mathbf{V}(F)$, όπου $F \in \mathbf{k}[\mathsf{X},\mathsf{Y}]$ είναι ένα πολυώνυμο βαθμού $n$, να αποδειχθεί ότι η τομή $L \cap C$ είναι ένα πεπερασμένο σύνολο αποτελούμενο από το πολύ $n$ σημεία. (*Υπόδειξη*: Να υποτεθεί ότι $L = \mathbf{V}(\mathsf{Y} - (a\mathsf{X} + b))$, $a, b \in \mathbf{k}$, και να θεωρηθεί το πολυώνυμο $F(\mathsf{X}, a\mathsf{X} + b) \in \mathbf{k}[\mathsf{X}]$.)

**A-1-13.** Να αποδειχθεί ότι τα ακόλουθα σύνολα δεν είναι αλγεβρικά:

(a) $\left\{(x,y) \in \mathbb{A}^2_{\mathbb{R}} \mid y = \sin(x)\right\}$,

(b) $\left\{(z,w) \in \mathbb{A}^2_{\mathbb{C}} \;\middle|\; |z|^2 + |w|^2 = 1\right\}$, όπου $|x+iy|^2 = x^2 + y^2$, για $x, y \in \mathbb{R}$, και

(c) $\left\{(\cos(t), \sin(t), t) \in \mathbb{A}^3_{\mathbb{R}} \mid t \in \mathbb{R}\right\}$.

**A-1-14.** Έστω $F \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ ένα μη σταθερό πολυώνυμο, με το $\mathbf{k}$ ένα αλγεβρικώς κλειστό σώμα. Να αποδειχθεί ότι η διαφορά $\mathbb{A}^n_{\mathbf{k}} \smallsetminus \mathbf{V}(F)$ είναι απειροπληθής για κάθε $n \geq 1$ και ότι το $\mathbf{V}(F)$ είναι απειροπληθές για κάθε $n \geq 2$. Να εξαχθεί το συμπέρασμα ότι το συμπλήρωμα οιουδήποτε αλγεβρικού συνόλου είναι απειροπληθές. (*Υπόδειξη*: Βλ. άσκηση **A-1-5**).

**A-1-15.** (a) Έστω ότι τα $V \subseteq \mathbb{A}^m_{\mathbf{k}}$ και $W \subseteq \mathbb{A}^n_{\mathbf{k}}$ είναι δυο αλγεβρικά σύνολα. Να αποδειχθεί ότι το

$$V \times W = \{(a_1, \ldots, a_m, b_1, \ldots, b_n) \mid (a_1, \ldots, a_m) \in V,\ (b_1, \ldots, b_n) \in W\}$$

είναι αλγεβρικό σύνολο εντός τού $\mathbb{A}^{m+n}_{\mathbf{k}}$. Το $V \times W$ καλείται **το γινόμενο** των $V$ και $W$.

(b) Να αποδειχθεί ότι η τοπολογία Zariski επί τού $\mathbb{A}^n_{\mathbf{k}} = \underbrace{\mathbb{A}^1_{\mathbf{k}} \times \cdots \times \mathbb{A}^1_{\mathbf{k}}}_{n\text{-φορές}}$, $n \geq 2$, όπου $\mathbf{k}$ αλγεβρικώς κλειστό σώμα, είναι διαφορετική τής *τοπολογίας γινομένου* (τής επαγομένης κατά τον συνήθη τρόπο από την τοπολογία Zariski επί καθενός εκ των παραγόντων).

## 1.3 Το Ιδεώδες ενός Σημειοσυνόλου

Για κάθε υποσύνολο $X$ τού $\mathbb{A}^n_{\mathbf{k}}$ θεωρούμε τα πολυώνυμα τα οποία μηδενίζονται επί τού $X$. Αυτά τα πολυώνυμα συγκροτούν ένα ιδεώδες τού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, το οποίο ονομάζεται **το ιδεώδες τού** $X$ και συμβολίζεται ως $\mathbf{I}(X)$, ήτοι

$$\mathbf{I}(X) := \{F \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \mid F(a_1, \ldots, a_n) = 0, \text{ για όλα τα } (a_1, \ldots, a_n) \in X\}.$$

**1.3.1 Πρόταση.** *Έστω* $\mathbf{k}$ *ένα σώμα και έστω* $\mathbb{A}^n_{\mathbf{k}}$ *ο* $n$*-διάστατος συσχετικός χώρος υπεράνω αυτού. Τότε ισχύουν τα εξής* :

(1) *Για* $X, Y \subseteq \mathbb{A}^n_{\mathbf{k}}$, *όπου* $X \subseteq Y$, *έχουμε* $\mathbf{I}(X) \supseteq \mathbf{I}(Y)$.

(2) $\begin{cases} (a) & \mathbf{I}(\varnothing) = \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n], \\ (b) & \mathbf{I}(\mathbb{A}^n_{\mathbf{k}}) = \{0\}, \text{ } \textit{όταν το } \mathbf{k} \textit{ είναι απειροπληθές,} \\ (c) & \mathbf{I}(\{P\}) = \langle \mathsf{X}_1 - a_1, \ldots, \mathsf{X}_n - a_n \rangle, \ \forall P, \ P = (a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbf{k}}. \end{cases}$

(3) $\begin{cases} (a) & \mathbf{I}(\mathbf{V}(\mathcal{S})) \supseteq \mathcal{S}, \ \ \forall \mathcal{S}, \ \ \mathcal{S} \subseteq \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n], \\ (b) & \mathbf{V}(\mathbf{I}(X)) \supseteq X, \ \ \forall X, \ \ X \subseteq \mathbb{A}^n_{\mathbf{k}}. \end{cases}$

(4) $\begin{cases} (a) & \mathbf{V}(\mathbf{I}(\mathbf{V}(\mathcal{S}))) = \mathbf{V}(\mathcal{S}), \ \ \forall \mathcal{S}, \ \ \mathcal{S} \subseteq \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n], \\ (b) & \mathbf{I}(\mathbf{V}(\mathbf{I}(X))) = \mathbf{I}(X), \ \ \forall X, \ \ X \subseteq \mathbb{A}^n_{\mathbf{k}}. \end{cases}$

(5) $\begin{cases} (a) & \textit{Εάν το } W \textit{ είναι ένα αλγεβρικό σύνολο, τότε } \textbf{W=V(I(W))}. \\ (b) & \begin{cases} \textit{Εάν το } I \textit{ είναι το ιδεώδες ενός αλγεβρικού συνόλου } W, \\ \textit{τότε } I = \mathbf{I}(\mathbf{V}(I)). \end{cases} \end{cases}$

ΑΠΟΔΕΙΞΗ. (1) Έστω $F \in \mathbf{I}(Y)$ και έστω $(a_1, \ldots, a_n) \in X$. Εξ υποθέσεως, $X \subseteq Y$, οπότε $(a_1, \ldots, a_n) \in Y$ και

$$F(a_1, \ldots, a_n) = 0 \Longrightarrow F \in \mathbf{I}(X).$$

(2) (a) Τούτο είναι προφανές επί τη βάσει τού ορισμού.

(b) Όταν το $\mathbf{k}$ είναι απειροπληθές, $\mathbf{I}(\mathbb{A}^n_{\mathbf{k}}) = \{0\}$ επί τη βάσει τού ορισμού τού ιδεώδους τού $\mathbb{A}^n_{\mathbf{k}}$ και τής ασκήσεως **A-1-3**.

(c) Εάν $P = (a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbf{k}}$ και $F \in \mathbf{I}(\{P\})$, τότε έχουμε $F(P) = 0$. Από την άσκηση **A-1-7** (b) συνάγουμε την ύπαρξη πολυωνύμων $G_1, \ldots, G_n \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ για τα οποία ισχύει

$$F = \sum_{i=1}^{n} (\mathsf{X}_i - a_i) \, G_i \Longrightarrow F \in \langle \mathsf{X}_1 - a_1, \ldots, \mathsf{X}_n - a_n \rangle.$$

Άρα $\mathbf{I}(\{P\}) \subseteq \langle \mathsf{X}_1 - a_1, \ldots, \mathsf{X}_n - a_n \rangle$. Η αντίστροφη σχέση εγκλεισμού είναι προφανής.

(3) (a) Έστω $F \in \mathcal{S}$ και έστω $P \in \mathbf{V}(\mathcal{S})$. Τότε $F(P) = 0$, οπότε $F \in \mathbf{I}(\mathbf{V}(\mathcal{S}))$. Άρα όντως $\mathbf{I}(\mathbf{V}(\mathcal{S})) \supseteq \mathcal{S}$.

(b) Έστω $P \in X$ και έστω $F \in \mathbf{I}(X)$. Τότε $F(P) = 0$, οπότε $F \in \mathbf{V}(\mathbf{I}(X))$. Άρα όντως $\mathbf{V}(\mathbf{I}(X)) \supseteq X$.

(4) (a) Έστω $\mathcal{S} \subseteq \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Από το 3 (b) γνωρίζουμε ότι $\mathbf{V}(\mathcal{S}) \subseteq \mathbf{V}(\mathbf{I}(\mathbf{V}(\mathcal{S})))$. Έστω $P \in \mathbf{V}(\mathbf{I}(\mathbf{V}(\mathcal{S})))$ και έστω $F \in \mathcal{S}$. Σύμφωνα με το (3) (a), έχουμε $\mathcal{S} \subseteq \mathbf{I}(\mathbf{V}(\mathcal{S}))$, απ' όπου έπεται ότι $F \in \mathbf{I}(\mathbf{V}(\mathcal{S})) \Longrightarrow F(P) = 0$. Άρα $\mathbf{V}(\mathbf{I}(\mathbf{V}(\mathcal{S}))) \subseteq \mathbf{V}(\mathcal{S})$.

(b) Έστω $X \subseteq \mathbb{A}^n_{\mathbf{k}}$. Από το (3) (a) γνωρίζουμε ότι $\mathbf{I}(X) \subseteq \mathbf{I}(\mathbf{V}(\mathbf{I}(X)))$. Σύμφωνα με το (3) (b), $X \subseteq \mathbf{V}(\mathbf{I}(X))$. Εφαρμόζοντας το (1) συμπεραίνουμε ότι $\mathbf{I}(\mathbf{V}(\mathbf{I}(X))) \subseteq \mathbf{I}(X)$. Άρα τελικώς $\mathbf{I}(\mathbf{V}(\mathbf{I}(X))) = \mathbf{I}(X)$.

(5) Εάν το $W$ είναι ένα αλγεβρικό σύνολο, τότε υπάρχει κάποιο $\mathcal{S} \subseteq \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ με $W = \mathbf{V}(\mathcal{S})$. Το (a) έπεται από το (4) (a) και το (b) από το (4) (b). □

**1.3.2 Ορισμός.** Εάν ο $R$ είναι ένας δακτύλιος και το $I$ ένα ιδεώδες του, ορίζουμε το σύνολο

$$\boxed{\mathrm{Rad}(I) := \{a \in R \mid a^m \in I \quad \text{για κάποιον θετικό ακέραιο } m\}}$$

ως **το ριζικό τού** $I$. Το $\mathrm{Rad}(I)$ είναι ένα ιδεώδες τού $R$ (βλ. άσκηση **A-1-18**). Εάν μάλιστα συμβεί να έχουμε $I = \mathrm{Rad}(I)$, τότε το $I$ ονομάζεται **ριζικό ιδεώδες** τού δακτυλίου $R$.

**1.3.3 Πρόταση.** *Έστω* $\mathbf{k}$ *ένα σώμα και έστω* $\mathbb{A}^n_{\mathbf{k}}$ *ο* $n$*-διάστατος συσχετικός χώρος υπεράνω αυτού. Εάν* $X \subseteq \mathbb{A}^n_{\mathbf{k}}$*, τότε το ιδεώδες* $\mathbf{I}(X)$ *τού* $X$ *αποτελεί ένα ριζικό ιδεώδες τού δακτυλίου* $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$.

ΑΠΟΔΕΙΞΗ. Θα αποδείξουμε ότι $\mathbf{I}(X) = \mathrm{Rad}(\mathbf{I}(X))$. Εάν $F \in \mathbf{I}(X)$, τότε έχουμε

$$F = F^1 \in \mathrm{Rad}(\mathbf{I}(X)).$$

Άρα $\mathbf{I}(X) \subseteq \mathrm{Rad}(\mathbf{I}(X))$. Και αντιστρόφως· εάν $F \in \mathrm{Rad}(\mathbf{I}(X))$, τότε υπάρχει $n \in \mathbb{N}$ : $F^m \in \mathbf{I}(X)$. Επειδή ο πολυωνυμικός δακτύλιος $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι ακεραία περιοχή (βλ. πρόταση 1.1.34 (a)), έχουμε

$$[F^m(P) = (F(P))^m = 0,\ \forall P \in X] \Longrightarrow [F(P) = 0,\ \forall P \in X] \Longrightarrow F \in \mathbf{I}(X).$$

Άρα $\mathrm{Rad}(\mathbf{I}(X)) \subseteq \mathbf{I}(X)$. □

**1.3.4 Πρόταση.** *Έστω* $\mathbf{k}$ *ένα σώμα και έστω* $\mathbb{A}^n_{\mathbf{k}}$ *ο* $n$*-διάστατος συσχετικός χώρος υπεράνω αυτού. Εάν* $X \subseteq \mathbb{A}^n_{\mathbf{k}}$*, τότε*

$$\mathbf{V}(\mathbf{I}(X)) = \mathrm{cl}_{\mathcal{T}_{\mathrm{Zar}}}(X), \tag{1.2}$$

*όπου*

$$\mathrm{cl}_{\mathcal{T}_{\mathrm{Zar}}}(X) := \bigcap \{E \mid (\mathbb{A}^n_{\mathbf{k}} \smallsetminus E) \in \mathcal{T}_{\mathrm{Zar}},\ E \supseteq X\}$$

*η κλειστή θήκη τού* $X$ *ως προς την τοπολογία Zariski.*

ΑΠΟΔΕΙΞΗ. Κατά την πρόταση 1.3.1 (3) (b), $\mathbf{V}(\mathbf{I}(X)) \supseteq X$. Έστω $B$ τυχόν κλειστό υποσύνολο τού $\mathbb{A}^n_{\mathbf{k}}$ ως προς την τοπολογία Zariski, το οποίο περιέχει το $X$. Επειδή (εξ ορισμού) υπάρχει κάποιο ιδεώδες $I$ τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ για το οποίο ισχύει $B = \mathbf{V}(I)$, από το (3) τής προτάσεως 1.2.3 και τα (1) και (5) (a) τής προτάσεως 1.3.1 έπεται ότι

$$B = \mathbf{V}(I) = \mathbf{V}(\mathbf{I}(\mathbf{V}(I))) = \mathbf{V}(\mathbf{I}(B)) \supseteq \mathbf{V}(\mathbf{I}(X)).$$

Επειδή το $\mathrm{cl}_{\mathcal{T}_{\mathrm{Zar}}}(X)$ είναι το *ελάχιστο* κλειστό υποσύνολο τού $\mathbb{A}^n_{\mathbf{k}}$ ως προς την τοπολογία Zariski, το οποίο περιέχει το $X$, η ισότητα (1.2) είναι αληθής. □

## Ασκήσεις

**A-1-16.** Έστω ότι τα $V$ και $W$ είναι δυο αλγεβρικά σύνολα εντός τού $\mathbb{A}^n_{\mathbf{k}}$. Να αποδειχθεί ότι $V = W \iff \mathbf{I}(V) = \mathbf{I}(W)$.

**A-1-17**. (a) Έστω ότι το $V$ είναι ένα αλγεβρικό σύνολο εντός τού συσχετικού χώρου $\mathbb{A}^n_{\mathbf{k}}$ και ότι το $P$ είναι ένα σημείο, το οποίο δεν ανήκει στο $V$. Να αποδειχθεί ότι υπάρχει ένα πολυώνυμο $F \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τέτοιο ώστε να ισχύει

$$F(Q) = 0_{\mathbf{k}}, \ \ \forall Q, \ \ Q \in V, \quad \text{ενώ} \ \ F(P) = 1_{\mathbf{k}}.$$

(*Υπόδειξη*: $\mathbf{I}(V) \neq \mathbf{I}(V \cup \{P\})$).

(b) Έστω $\{P_1, \ldots, P_\kappa\}$ ένα πεπερασμένο σύνολο σημείων εντός τού $\mathbb{A}^n_{\mathbf{k}}$. Να αποδειχθεί ότι υπάρχουν πολυώνυμα $F_1, \ldots, F_\kappa \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τέτοια ώστε

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

(c) Έστω $V$ ένα αλγεβρικό σύνολο εντός τού $\mathbb{A}^n_{\mathbf{k}}$ και $P_1, P_2 \notin V$. Να αποδειχθεί ότι υπάρχει ένα πολυώνυμο $F \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τέτοιο ώστε

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

(*Υπόδειξη*: Να προσδιορισθούν $F_i \in \mathbf{I}(V)$, $i \in \{1, 2\}$, τέτοια ώστε $F_i(P_i) \neq 0_{\mathbf{k}}$ και να συναχθεί ότι $F =$ ή $F_1$ ή $F_2$ ή $F_1 + F_2$).

**A-1-18.** Έστω $I$ ένα ιδεώδες ενός δακτυλίου $R$. Εάν $a^n \in I$ και $b^m \in I$, για κάποιους $n, m \in \mathbb{N}$, να αποδειχθεί ότι $(a + b)^{n+m} \in I$. Επιπροσθέτως, να αποδειχθεί ότι το $\mathrm{Rad}(I)$ είναι ένα ιδεώδες τού $R$, και μάλιστα ένα ριζικό ιδεώδες τού $R$. Τέλος, να αποδειχθεί ότι κάθε πρώτο ιδεώδες τού $R$ είναι ριζικό.

**A-1-19.** Να αποδειχθεί ότι το $I = \langle \mathsf{X}^2 + 1 \rangle \subset \mathbb{R}[\mathsf{X}]$ είναι ένα ριζικό (καθώς και πρώτο) ιδεώδες, παρότι το $I$ δεν είναι το ιδεώδες κανενός συνόλου εντός τού $\mathbb{A}^1_{\mathbb{R}}$.

**A-1-20.** Για κάθε ιδεώδες $I$ τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ να αποδειχθεί η ισχύς των σχέσεων

$$\mathbf{V}(I) = \mathbf{V}(\mathrm{Rad}(I)) \quad \text{και} \quad \mathrm{Rad}(I) \subseteq \mathbf{I}(\mathbf{V}(I)).$$

**A-1-21.** Εάν $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbf{k}}$, να αποδειχθεί ότι το

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

είναι ένα μεγιστοτικό ιδεώδες και ότι ο φυσικός ομομορφισμός από το σώμα $\mathbf{k}$ στον $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \,/\, I$ είναι ένας ισομορφισμός.

## 1.4 Πράξεις με Ιδεώδη

Τα ιδεώδη ενός δακτυλίου μπορούν να προστεθούν, να πολλαπλασιασθούν ή και να διαιρεθούν. Η εξοικείωση με τον «λογισμό με ιδεώδη» θα αποβεί χρήσιμη τόσο για ορισμένα τμήματα τής αναπτυσσόμενης θεωρίας όσο και για την ευχερέστερη επίλυση ασκήσεων.

**1.4.1 Ορισμός.** Έστω ότι ο $R$ είναι ένας δακτύλιος και τα $I_1, \dots, I_n$ ιδεώδη του. Ορίζουμε το **άθροισμα** και το **γινόμενό** τους ως:

$$\boxed{I_1 + \cdots + I_n := \sum_{j=1}^{n} I_j := \{a_1 + \cdots + a_n \mid a_j \in I_j,\ \forall j,\ 1 \le j \le n\}}$$

και

$$\boxed{I_1 \ \cdots \ I_n := \left\{ \begin{array}{c} \text{αθροίσματα τής μορφής} \\ \displaystyle\sum_{j=1}^{k} a_{1,j}\, a_{2,j} \cdots a_{n,j},\ \text{με } a_{l,j} \in I_l,\ 1 \le l \le n,\ k \in \mathbb{N} \end{array} \right\}}$$

αντιστοίχως. Τα $I_1 + \cdots + I_n$ και $I_1 \ \cdots \ I_n$ αποτελούν ιδεώδη τού $R$.

**1.4.2 Σημείωση.** (a) Εάν τα $I_1, \dots, I_n$ είναι ιδεώδη ενός δακτυλίου $R$, τότε[7]

$$I_1 + \cdots + I_n = \langle I_1 \cup \cdots \cup I_n \rangle .$$

Πράγματι· από τον ορισμό τού $I_1 + \cdots + I_n$ ο εγκλεισμός "$\subseteq$" είναι προφανής. Και επειδή το ιδεώδες $\langle I_1 \cup \cdots \cup I_n \rangle$ ισούται με

$$\left\{ \sum_{i=1}^{\kappa} r_i\, a_i \;\middle|\; r_1, \dots, r_\kappa \in R,\ a_1, ..., a_\kappa \in I_1 \cup \cdots \cup I_n,\ \ \kappa \in \mathbb{N} \right\},$$

κάθε $x \in \langle I_1 \cup \cdots \cup I_n \rangle$ μπορεί (ενδεχομένως ύστερα από κάποια αναδιάταξη δεικτών) να γραφεί υπό τη μορφή $x = x_1 + \cdots + x_n$, όπου για κάθε $j \in \{1, \dots, n\}$,

$$x_j = \sum_{i=1}^{\kappa_j} r_i\, a_i\,,\ \ r_1, \dots, r_{\kappa_j} \in R$$

για κατάλληλα $a_1, ..., a_{\kappa_j} \in I_j$ και $\kappa_j \in \mathbb{N}$. Άρα έχουμε και

$$\langle I_1 \cup \cdots \cup I_n \rangle \subseteq I_1 + \cdots + I_n.$$

[7] Γενικότερα, εάν η $(I_\lambda)_{\lambda \in \Lambda}$ είναι τυχούσα μη κενή οικογένεια ιδεωδών ενός δακτυλίου $R$, τότε ως **άθροισμα** των μελών της *ορίζουμε* το ιδεώδες $\sum_{\lambda \in \Lambda} I_\lambda$ τού $R$ το παραγόμενο από τη (συνολοθεωρητική) ένωση $\bigcup_{\lambda \in \Lambda} I_\lambda$.

(b) Ας σημειωθεί ότι -εν αντιθέσει προς την τομή- η *ένωση* δυο ιδεωδών ενός δακτυλίου μπορεί να *μην* αποτελεί ιδεώδες τού θεωρούμενου δακτυλίου. Επί παραδείγματι, η ένωση $3\mathbb{Z} \cup 5\mathbb{Z}$ των κυρίων ιδεωδών $\langle 3\rangle = 3\mathbb{Z}$ και $\langle 5\rangle = 5\mathbb{Z}$ τού $\mathbb{Z}$ δεν είναι ιδεώδες τού $\mathbb{Z}$, διότι τόσο το 3 όσο και το 5 ανήκουν στην $3\mathbb{Z} \cup 5\mathbb{Z}$, αλλά $2 = 5 - 3 \notin 3\mathbb{Z} \cup 5\mathbb{Z}$.

(c) Στην περίπτωση κατά την οποία $I_1 = \cdots = I_n = I$, συμβολίζουμε το γινόμενο $I_1 \cdots I_n$ και ως $I^n$ (ήτοι εν είδει «δυνάμεως»), προσέχοντας -όμως- να μην το συγχέουμε με το καρτεσιανό γινόμενο τού $I$ ($n$ φορές) με τον εαυτό του! Για κάθε ιδεώδες $I$ ενός δακτυλίου $R$ προκύπτει μια «κατιούσα» (ή «φθίνουσα») αλυσίδα ιδεωδών

$$I \supseteq I^2 \supseteq I^3 \supseteq \cdots \supseteq I^\kappa \supseteq I^{\kappa+1} \supseteq \cdots\,,\ \forall \kappa \in \mathbb{N}.$$

Επί παραδείγματι, εντός τού δακτυλίου $\mathbb{Z}$ των ακεραίων έχουμε

$$\langle 2\rangle \supseteq \langle 4\rangle \supseteq \langle 8\rangle \supseteq \cdots \supseteq \langle 2^\kappa\rangle \supseteq \left\langle 2^{\kappa+1}\right\rangle \supseteq \cdots\,,\ \forall \kappa \in \mathbb{N}.$$

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

Οι προτάσεις 1.4.3, 1.4.4, 1.4.5 και 1.4.11, οι οποίες ακολουθούν, έχουν ως στόχο την περιγραφή ορισμένων βασικών αρχών τού «λογισμού με ιδεώδη».

**1.4.3 Πρόταση.** *Εάν ο $R$ είναι ένας δακτύλιος και $a, b \in R$, τότε*

(a) $\langle a\rangle + \langle b\rangle = \{ xa + yb \mid x, y \in R\}$, *και*

(b) $\langle a\rangle \langle b\rangle = \langle ab\rangle$.

**1.4.4 Πρόταση.** *Έστω ότι ο $R$ ειναι ένας δακτύλιος και $I_1, I_2, I_3, I_3'$ τέσσερα ιδεώδη του. Τότε ισχύουν τα εξής*:

(a) $(I_1 + I_2) + I_3 = I_1 + (I_2 + I_3)$,

(b) $(I_1\, I_2)\ I_3 = I_1\ (I_2\, I_3)$,

(c) $I_1\ (I_2 + I_3) = (I_1\, I_2) + (I_1\, I_3)$, $(I_1 + I_2)\ I_3' = (I_1\, I_3') + (I_2\, I_3')$.

**1.4.5 Πρόταση.** *Έστω ότι ο $R$ είναι ένας δακτύλιος και τα $I_1, I_2, I_3$ ιδεώδη του.Τότε ισχύουν τα εξής*:

(a) $I_1\, I_2 \subseteq I_1 \cap I_2$.

(b) $(I_1 + I_2)\ (I_1 + I_3) \subseteq I_1 + I_2\, I_3 \subseteq I_1 + (I_2 \cap I_3)$.

**1.4.6 Ορισμός.** Λέμε ότι δυο ιδεώδη $I, J$ ενός δακτυλίου $R$ είναι **πρώτα μεταξύ τους** (ή **συμπρώτα**) όταν $I + J = R$. (Η συνθήκη αυτή ισοδυναμεί με την ύπαρξη στοιχείων $a \in I$ και $b \in J$, για τα οποία ισχύει η ισότητα $a + b = 1_R$.)

**1.4.7 Λήμμα.** *Έστω ότι ο $R$ είναι ένας δακτύλιος και $I_1, I_2, I_3$ τρία ιδεώδη του. Τότε ισχύουν τα εξής*:

(a) *Εάν τα $I_1, I_2$ είναι μεταξύ τους πρώτα, τότε $I_1\, I_2 = I_1 \cap I_2$.*

(b) *Εάν τα $I_1, I_2$ και τα $I_1, I_3$ είναι μεταξύ τους πρώτα, τότε και τα $I_1, I_2 I_3$ είναι πρώτα μεταξύ τους.*

ΑΠΟΔΕΙΞΗ. (a) Κατά την πρόταση 1.4.5 (a), $I_1\, I_2 \subseteq I_1 \cap I_2$. Εάν $I_1 + I_2 = R$, τότε εφαρμόζοντας το (c) τής προτάσεως 1.4.4 λαμβάνουμε

$$\begin{aligned} I_1 \cap I_2 &= (I_1 \cap I_2)\, R = (I_1 \cap I_2)(I_1 + I_2) \\ &= (I_1 \cap I_2) I_1 + (I_1 \cap I_2) I_2 \subseteq I_1\, I_2 + I_2\, I_1 = I_1\, I_2. \end{aligned}$$

(b) Εξ υποθέσεως υπάρχουν $a, a' \in I_1, b \in I_2$ και $c \in I_3$, τέτοια ώστε

$$a + b = 1_R,\ \ a' + c = 1_R \Longrightarrow bc = (1_R - a)(1_R - a') = 1_R - a - a' + aa'.$$

Θέτοντας $a'' := a + a' - aa'$ έχουμε $a'' + bc = 1_R$, όπου $a'' \in I_1$ και $bc \in I_2 I_3$, οπότε τα $I_1, I_2 I_3$ είναι όντως πρώτα μεταξύ τους. □

**1.4.8 Θεώρημα. (Κινέζικο θεώρημα για ιδεώδη δακτυλίων)** *Έστω $n$ ένας φυσικός αριθμός $\geq 2$. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου $R$ και $f$ ο ομομορφισμός δακτυλίων*

$$f : R \longrightarrow \bigoplus_{j=1}^{n} (R/I_j),\ \ r \longmapsto f(r) := (r + I_1, \ldots, r + I_n),$$

*τότε ισχύουν τα ακόλουθα*:

(a) *Εάν τα $I_1, \ldots, I_n$ είναι ανά ζεύγη πρώτα μεταξύ τους, τότε*

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n.$$

(b) *Ο $f$ είναι επιμορφισμός $\Longleftrightarrow$ τα $I_1, \ldots, I_n$ είναι ανά ζεύγη πρώτα μεταξύ τους.*

(c) *Ο $f$ είναι μονομορφισμός $\Longleftrightarrow I_1 \cap \cdots \cap I_n = \{0_R\}$.*

(d) *Εάν τα $I_1, \ldots, I_n$ είναι ανά ζεύγη πρώτα μεταξύ τους, τότε*

$$R/I_1 \cdots I_n \cong R/\bigcap_{j=1}^{n} I_j \cong \bigoplus_{j=1}^{n} (R/I_j).$$

ΑΠΟΔΕΙΞΗ. (a) Θα χρησιμοποιήσουμε επαγωγή επί τού $n$. Για $n = 2$ ο ισχυρισμός είναι αληθής επί τη βάσει τού (a) τού λήμματος 1.4.7. Για $n \geq 3$ υποθέτουμε ότι είναι αληθής για τα ιδεώδη $I_1, \ldots, I_{n-1}$. Έστω $J := I_1 \cdots I_{n-1} = I_1 \cap \cdots \cap I_{n-1}$. Κατά το (b) τού λήμματος 1.4.7 τα $J$ και $I_n$ είναι πρώτα μεταξύ τους, οπότε

$$I_1 \cdots I_n = J I_n = J \cap I_n = I_1 \cap \cdots \cap I_{n-1} \cap I_n.$$

(b) Ας υποθέτουμε ότι ο $f$ είναι επιμορφισμός και ας θεωρήσουμε $j,k \in \{1,\dots,n\}$, $j \neq k$. Για το στοιχείο $(I_1,...,1_R+I_j,...,I_n)$ (όπου το $1_R$ βρίσκεται στην $j$-οστή θέση) υπάρχει $r \in R$, για το οποίο ισχύει

$$\begin{aligned} f(r) &= (I_1,...,1_R+I_j,...,I_n) \Longrightarrow 1_R - r \in I_j,\ r \in I_k \\ &\Longrightarrow (1_R-r)+r = 1_R \in I_j+I_k \Longrightarrow I_j+I_k = R, \end{aligned}$$

οπότε τα $I_j, I_k$ είναι πρώτα μεταξύ τους. Εν συνεχεία, ας υποθέσουμε, αντιστρόφως, ότι τα $I_1,\dots,I_n$ είναι ανά ζεύγη πρώτα μεταξύ τους. Θα δείξουμε ότι η $f$ είναι επιρριπτική. Παρατηρούμε ότι η εικόνα οιουδήποτε $r \in R$ μέσω τού $f$ γράφεται ως

$$f(r) = (\pi_1(r),..,\pi_n(r)),$$

όπου $\pi_j : R \longrightarrow R/I_j$ ο φυσικός επιμορφισμός για κάθε $j \in \{1,\dots,n\}$. Έστω τυχόν στοιχείο $(y_1,\dots,y_n) \in \bigoplus_{j=1}^n (R/I_j)$. Τότε υπάρχει $x_j \in R$, τέτοιο ώστε $\pi_j(x_j) = y_j$ για κάθε $j \in \{1,\dots,n\}$. Επιπροσθέτως,

$$R = I_j + \bigcap_{1\leq k\leq n,\ k\neq j} I_k,\ \ \forall j \in \{1,\dots,n\}. \tag{1.3}$$

Πράγματι· για $n=2$ η (1.3) είναι προφανώς αληθής. Υποθέτουμε ότι είναι αληθής και για κάποιον $n=l\geq 2$ και εξετάζουμε την περίπτωση όπου $n=l+1$. Επειδή ο $R$ είναι δακτύλιος με μοναδιαίο πολλαπλασιαστικό στοιχείο, έχουμε για κάθε $j \in \{1,\dots,l+1\}$

$$R = RR = \left(I_j + \bigcap_{1\leq k\leq l,\ k\neq j} I_k\right)(I_j+I_{l+1}) \subseteq I_j + \bigcap_{1\leq k\leq l+1,\ k\neq j} I_k,$$

με τη δεύτερη ισότητα ισχύουσα λόγω της επαγωγικής υποθέσεως και την επακόλουθη εγκλειστική σχέση απορρέουσα από το (b) τής προτάσεως 1.4.5. Επειδή όμως το δεξιό μέλος εμπεριέχεται στον $R$, η (1.3) ισχύει και για $n=l+1$. Άρα για κάθε $j \in \{1,\dots,n\}$

$$\left[(\exists\, u_j \in I_j)\ \ \text{και}\ \ (\exists\, v_j \in \bigcap_{1\leq k\leq n,\ k\neq j} I_k) : u_j+v_j = 1_R\right].$$

Ως εκ τούτου, $v_j - 1_R \in I_j$ και $v_j \in I_k, \forall k \in \{1,\dots,n\}\setminus\{j\}$, απ' όπου έπεται ότι

$$\pi_k(v_j) = v_j + I_k = \begin{cases} 1_R+I_k, & \text{όταν } k=j, \\ I_k, & \text{όταν } k\neq j. \end{cases}$$

Συνεπώς,

$$\begin{aligned} f\left(\sum_{j=1}^n x_j v_j\right) &= \left(\pi_1(\sum_{j=1}^n x_j v_j),\dots,\pi_n(\sum_{j=1}^n x_j v_j)\right) \\ &= (\pi_1(x_1),\dots,\pi_n(x_n)) = (y_1,\dots,y_n), \end{aligned}$$

και η $f$ είναι όντως επιριπτική.

(c) Προφανώς, $\mathrm{Ker}(f) = \bigcap_{j=1}^{n} I_j$.

(d) Εάν τα $I_1, \ldots, I_n$ είναι ανά ζεύγη πρώτα μεταξύ τους, τότε, σύμφωνα με το (b), ο $f$ είναι επιμορφισμός. Αρκεί λοιπόν να εφαρμοσθεί το 1.1.10 και το (a). □

**1.4.9 Ορισμός.** Έστω ότι ο $R$ είναι ένας δακτύλιος και τα $I, J$ δυο ιδεώδη του. Ως **πηλίκο** $I : J$ τού $I$ διά τού $J$ ορίζεται το σύνολο

$$\boxed{I : J := \{r \in R \mid ra \in I \quad \text{για κάθε } a \in J\} = \{r \in R \mid rJ \subseteq I\}}$$

Προφανώς, το $I : J$ αποτελεί ένα ιδεώδες τού $R$.

Οι «πράξεις» που ορίσαμε επί των ιδεωδών δακτυλίων, εφαρμοζόμενες στον δακτύλιο $\mathbb{Z}$, συμπεριφέρονται ως ακολούθως:

**1.4.10 Πόρισμα.** *Εάν $\langle m\rangle$ και $\langle n\rangle$ είναι δυο μη τετριμμένα ιδεώδη τού δακτυλίου $\mathbb{Z}$ των ακεραίων, όπου $m, n \in \mathbb{Z}\setminus\{0\}$, τότε ισχύουν τα εξής*:

(a) $\langle m\rangle \cap \langle n\rangle = \langle \text{εκπ}(m,n)\rangle$,

(b) $\langle m\rangle + \langle n\rangle = \langle \text{μκδ}(m,n)\rangle$,

(c) $\langle m\rangle \langle n\rangle = \langle mn\rangle$,

(d) $\langle m\rangle : \langle n\rangle = \left\langle \frac{m}{\text{μκδ}(m,n)} \right\rangle$.

**1.4.11 Πρόταση.** *Έστω ότι ο $R$ είναι ένας δακτύλιος και $I_1, I_2, I_3$ τρία ιδεώδη του. Τότε ισχύουν τα εξής*:

(a) $(I_1 : I_3) + (I_2 : I_3) \subseteq (I_1 + I_2) : I_3$,

(b) $I_1 : (I_2 + I_3) = (I_1 : I_2) \cap (I_1 : I_3)$, $(I_1 \cap I_2) : I_3 = (I_1 : I_3) \cap (I_2 : I_3)$,

(c) $(I_1 : I_2)\ I_2 \subseteq I_1$, $I_1 \subseteq ((I_1\, I_2) : I_2)$,

(d) $(I_1 : I_2) : I_3 = I_1 : (I_2\, I_3) = (I_1 : I_3) : I_2$.

Το επόμενο θεώρημα περιγράφει το πώς συμπεριφέρονται τα συσχετικά αλγεβρικά σύνολα τα δημιουργούμενα από τα $I + J$, $IJ$ και $I : J$, όπου $I, J$ ιδεώδη τού πολυωνυμικού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$.

**1.4.12 Θεώρημα.** *Εάν τα $I, J$ είναι ιδεώδη τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τότε ισχύουν τα ακόλουθα*[8]:

(a) $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$.

(b) $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

(c) $\mathbf{V}(I : J) \supseteq \mathrm{cl}_{\mathcal{T}_{\mathrm{Zar}}}(\mathbf{V}(I)\setminus\mathbf{V}(J))$.

[8] Γενικότερα, είναι εύκολο να αποδειχθούν τα εξής: (a) Εάν η $(I_\lambda)_{\lambda\in\Lambda}$ είναι μια μη κενή οικογένεια ιδεώδών τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τότε $\mathbf{V}(\sum_{\lambda\in\Lambda} I_\lambda) = \bigcap_{\lambda\in\Lambda} \mathbf{V}(I_\lambda)$. (b) Εάν τα $I_1, \ldots, I_\kappa$ είναι ιδεώδη τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τότε $\mathbf{V}(I_1 \cdots I_\kappa) = \mathbf{V}(I_1) \cup \cdots \cup \mathbf{V}(I_\kappa)$.

ΑΠΟΔΕΙΞΗ. (a) Τούτο έπεται από το (2) τής προτάσεως 1.2.3 και ό,τι προαναφέραμε στο (a) τής σημειώσεως 1.4.2.

(b) Προφανές λόγω τού (4) τής προτάσεως 1.2.3.

(c) Κατά το (a) τής ασκήσεως **A-1-34**, $I : J \subseteq \mathbf{I}(\mathbf{V}(I) \smallsetminus \mathbf{V}(J))$. Εξάλλου, από το (3) τής προτάσεως 1.2.3 έπεται ότι

$$\mathbf{V}(I : J) \supseteq \mathbf{V}(\mathbf{I}(\mathbf{V}(I) \smallsetminus \mathbf{V}(J))).$$

Αρκεί λοιπόν να εφαρμοσθεί η πρόταση 1.3.4. □

## Ασκήσεις

**A-1-22.** Να αποδειχθούν οι προτάσεις 1.4.3, 1.4.4, 1.4.5 και 1.4.11.

**A-1-23.** Να αποδειχθεί το πόρισμα 1.4.10.

**A-1-24.** Έστω $n$ ένας φυσικός αριθμός $\geq 2$. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου $R$ να αποδειχθεί η ισότητα

$$(I_1 \cdots I_n)^\kappa = I_1^\kappa \cdots I_n^\kappa, \ \ \forall \kappa \in \mathbb{N}.$$

**A-1-25.** Έστω ότι τα $I, J$ είναι δυο ιδεώδη ενός δακτυλίου $R$. Εάν τα $I, J$ είναι μεταξύ τους πρώτα, να αποδειχθεί ότι και τα $I^m, J^n$ είναι μεταξύ τους πρώτα για οιουσδήποτε $m, n \in \mathbb{N}$.

**A-1-26.** Έστω $n$ ένας φυσικός αριθμός $\geq 2$. Εάν τα $I_1, \ldots, I_n$ είναι ιδεώδη ενός δακτυλίου $R$ και εάν τα $I_i$ και $J_i := \bigcap \{ I_j \,|\, j \in \{1, \ldots, n\} \smallsetminus \{i\} \}$ είναι πρώτα μεταξύ τους για κάθε $i \in \{1, \ldots, n\}$, να αποδειχθούν οι ισότητες

$$I_1^\kappa \cap \cdots \cap I_n^\kappa = (I_1 \cdots I_n)^\kappa = (I_1 \cap \cdots \cap I_n)^\kappa, \ \ \forall \kappa \in \mathbb{N}.$$

**A-1-27.** Έστω ότι ο $R$ είναι ένας δακτύλιος και τα $I_1, I_2, I_3$ τρία ιδεώδη του. Να αποδειχθούν τα ακόλουθα:

(a) $I_1 \subseteq I_2 \Longrightarrow I_1 : I_3 \subseteq I_2 : I_3$ και $I_3 : I_1 \supseteq I_3 : I_2$,

(b) $I_2 \subseteq I_1 \Longleftrightarrow I_1 : I_2 = R$,

(c) $I_1 : I_2^{n+1} = (I_1 : I_2^n) : I_2 = (I_1 : I_2) : I_2^n, \ \ \forall n \in \mathbb{N}$, και

(d) $I_1 : I_2 = I_1 : (I_1 + I_2)$.

**A-1-28.** Έστω ότι τα $I, J$ είναι δυο ιδεώδη ενός δακτυλίου $R$. Να αποδειχθούν τα εξής:

(a) $I^n \subseteq J$, για κάποιον $n \in \mathbb{N} \Longrightarrow \mathrm{Rad}(I) \subseteq \mathrm{Rad}(J)$,

(b) $\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I)$,

(c) $\mathrm{Rad}\big(I^k\big) = \mathrm{Rad}(I)\,, \forall k \in \mathbb{N}$,

(d) $\mathrm{Rad}(I) + \mathrm{Rad}(J) \subseteq \mathrm{Rad}(\mathrm{Rad}(I) + \mathrm{Rad}(J)) = \mathrm{Rad}(I + J)\,,$

(e) $\mathrm{Rad}(I) \cap \mathrm{Rad}(J) = \mathrm{Rad}(I \cap J) = \mathrm{Rad}(I\,J)\,,$

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

(g) $\mathrm{Rad}(I) : \mathrm{Rad}(J) \supseteq \mathrm{Rad}(I : J)\,.$

(h) Εάν ο $\pi : R \longrightarrow R/I$ είναι ο φυσικός επιμορφισμός, τότε $\mathrm{Rad}(I) = \pi^{-1}(\mathrm{Nil}(R/I))$.

**A-1-29.** Έστω ότι τα $I, J$ είναι δυο ιδεώδη ενός δακτυλίου $R$. Εάν το $I$ είναι πεπερασμένως παραγόμενο και $I \subseteq \mathrm{Rad}(J)$, να αποδειχθεί ότι $I^n \subseteq J$ για κάποιον $n \in \mathbb{N}$.

**A-1-30.** Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Για κάθε ιδεώδες $I$ τού $R$ ορίζεται η **επέκταση τού $I$ μέσω τού $f$** ως το ιδεώδες

$$\boxed{I^{\mathrm{ext}(f)} := f(I)R'}$$

το παραγόμενο από το $f(I)$ εντός τού $R'$. Εάν τα $I_1, I_2, I$ είναι ιδεώδη τού $R$, να αποδειχθεί η ισχύς των ακολούθων ιδιοτήτων:

(a) $I_1^{\mathrm{ext}(f)} + I_2^{\mathrm{ext}(f)} = (I_1 + I_2)^{\mathrm{ext}(f)}$,

(b) $I_1^{\mathrm{ext}(f)} I_2^{\mathrm{ext}(f)} = (I_1 I_2)^{\mathrm{ext}(f)}$,

(c) $(I_1 \cap I_2)^{\mathrm{ext}(f)} \subseteq I_1^{\mathrm{ext}(f)} \cap I_2^{\mathrm{ext}(f)}$ (με τη σχέση αυτή ισχύουσα ως ισότητα όταν ο $f$ είναι επιμορφισμός και είτε $\mathrm{Ker}(f) \subseteq I_1$ είτε $\mathrm{Ker}(f) \subseteq I_2$),

(d) $(I_1 : I_2)^{\mathrm{ext}(f)} \subseteq I_1^{\mathrm{ext}(f)} : I_2^{\mathrm{ext}(f)}$
(με τη σχέση αυτή ισχύουσα ως ισότητα όταν ο $f$ είναι επιμορφισμός και $\mathrm{Ker}(f) \subseteq I_1$),

(e) $\mathrm{Rad}(I)^{\mathrm{ext}(f)} \subseteq \mathrm{Rad}\big(I^{\mathrm{ext}(f)}\big)$
(με τη σχέση αυτή ισχύουσα ως ισότητα όταν ο $f$ είναι επιμορφισμός και $\mathrm{Ker}(f) \subseteq I$).

**A-1-31.** Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Για κάθε ιδεώδες $J$ τού $R'$ ορίζεται η **συστολή τού $J$ μέσω τού $f$** ως το ιδεώδες

$$\boxed{J^{\mathrm{con}(f)} := f^{-1}(J)}$$

τού $R$. Εάν τα $J_1, J_2, J$ είναι ιδεώδη τού $R'$, να αποδειχθεί η ισχύς των ακολούθων ιδιοτήτων:

(a) $J_1^{\mathrm{con}(f)} + J_2^{\mathrm{con}(f)} \subseteq (J_1 + J_2)^{\mathrm{con}(f)}$ (ως ισότητα όταν ο $f$ είναι επιμορφισμός),

(b) $(J_1 J_2)^{\mathrm{con}(f)} \supseteq J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)}$
(ισχύουσα ως ισότητα όταν ο $f$ είναι επιμορφισμός και $\mathrm{Ker}(f) \subseteq J_1^{\mathrm{con}(f)} J_2^{\mathrm{con}(f)}$),

(c) $(J_1 \cap J_2)^{\mathrm{con}(f)} = J_1^{\mathrm{con}(f)} \cap J_2^{\mathrm{con}(f)}$,

(d) $(J_1 : J_2)^{\mathrm{con}(f)} \subseteq J_1^{\mathrm{con}(f)} : J_2^{\mathrm{con}(f)}$ (ως ισότητα όταν ο $f$ είναι επιμορφισμός),

(e) $\mathrm{Rad}(J)^{\mathrm{con}(f)} = \mathrm{Rad}\big(J^{\mathrm{con}(f)}\big)\,.$

**A-1-32.** Έστω $f : R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων και έστω $\mathcal{I}_R$ (και αντιστοίχως, $\mathcal{I}_{R'}$) η συλλογή όλων των ιδεωδών τού δακτυλίου $R$ (και αντιστοίχως τού δακτυλίου $R'$). Να αποδειχθούν τα ακόλουθα:

(a) $I \subseteq (I^{\text{ext}(f)})^{\text{con}(f)},\ \forall I \in \mathcal{I}_R$,

(b) $(J^{\text{con}(f)})^{\text{ext}(f)} \subseteq J,\ \forall J \in \mathcal{I}_{R'}$,

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

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

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

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

είναι αμφιρριπτικές και η μία αντίστροφος τής άλλης.

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

**A-1-33.** Εάν τα $V, W$ είναι οιαδήποτε υποσύνολα τού $\mathbb{A}^n_{\mathbf{k}}$, να αποδειχθούν τα εξής:

$$\mathbf{I}(V) + \mathbf{I}(W) \subseteq \mathbf{I}(V \cap W), \quad \mathbf{I}(V)\mathbf{I}(W) \subseteq \mathbf{I}(V) \cap \mathbf{I}(W) \subseteq \mathbf{I}(V \cup W).$$

**A-1-34.** (a) Εάν τα $I, J$ είναι ιδεώδη τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, να αποδειχθεί ότι

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

(b) Εάν τα $V, W$ είναι αλγεβρικά σύνολα εντός τού $\mathbb{A}^n_{\mathbf{k}}$, να αποδειχθεί η ισότητα

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

**A-1-35.** Έστω $d \in \mathbb{N}$. Ορίζοντας ως

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

τα σύνολα των μονωνύμων τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ που έχουν βαθμό $\leq d$ και $= d$, αντιστοίχως, να αποδειχθούν τα ακόλουθα:

(a) Οι πληθικοί αριθμοί των εν λόγω συνόλων είναι οι

$$\sharp(\text{Mov}(\mathbf{k}\,[\mathsf{X}_1, \ldots, \mathsf{X}_n])_{\leq d}) = \binom{n+d}{n}, \quad \sharp(\text{Mov}(\mathbf{k}\,[\mathsf{X}_1, \ldots, \mathsf{X}_n])_d) = \binom{n-1+d}{n-1}.$$

(b) Εάν $I := \langle \mathsf{X}_1, \ldots, \mathsf{X}_n \rangle \subset \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, να αποδειχθεί ότι ο πηλικοδακτύλιος $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]/I^d$, ιδωμένος ως διανυσματικός χώρος υπεράνω τού σώματος $\mathbf{k}$, έχει διάσταση

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

## 1.5 Το Θεώρημα Βάσεως τού Hilbert

Παρότι έχουμε επιτρέψει σε ένα αλγεβρικό σύνολο να ορίζεται μέσω οιουδήποτε συνόλου πολυωνύμων, στην πραγματικότητα, προς τούτο είναι αρκετή η θεώρηση ενός πεπερασμένου συνόλου πολυωνύμων.

**1.5.1 Πρόταση.** *Έστω* $\mathbf{k}$ *ένα σώμα και* $\mathbb{A}^n_{\mathbf{k}}$ *ο* $n$*-διάστατος συσχετικός χώρου υπεράνω αυτού. Τότε κάθε αλγεβρικό σύνολο* $\varnothing \neq X \subseteq \mathbb{A}^n_{\mathbf{k}}$ *μπορεί να γραφεί ως τομή των μελών μιας οικογενείας πεπερασμένου πλήθους υπερεπιφανειών.*

ΑΠΟΔΕΙΞΗ. Εάν το $\varnothing \neq X \subseteq \mathbb{A}^n_{\mathbf{k}}$ είναι ένα αλγεβρικό σύνολο, τότε θα υπάρχει μια οικογένεια πολυωνύμων $\mathcal{S} \subseteq \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τέτοια ώστε να ισχύει $X = \mathbf{V}(\mathcal{S})$. Σύμφωνα με την πρόταση 1.2.3 (1), $X = \mathbf{V}(\mathcal{S}) = \mathbf{V}(I)$ για κάποιο ιδεώδες $I$ τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Για να αποδείξουμε την προκειμένη πρόταση είναι αρκετό να δείξουμε ότι το $I$ αυτό είναι πεπερασμένως παραγόμενο, ήτοι ότι υπάρχουν $F_1, \ldots, F_r \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τέτοια ώστε $I = \langle F_1, \ldots, F_r \rangle$, οπότε θα έχουμε

$$X = \mathbf{V}(\mathcal{S}) = \mathbf{V}(I) = \mathbf{V}(F_1) \cap \cdots \cap \mathbf{V}(F_r).$$

Αυτό θα αποδειχθεί παρακάτω στο πόρισμα 1.5.7. □

Κατ' αρχάς θα χρειασθούμε ορισμένες επιπρόσθετες αλγεβρικές έννοιες.

**1.5.2 Ορισμός.** Ένας δακτύλιος $R$ καλείται **δακτύλιος (τής) Noether** ή **ναιτεριανός δακτύλιος**[9] όταν κάθε ιδεώδες του είναι πεπερασμένως παραγόμενο.

Προφανώς, τα σώματα και οι Π.Κ.Ι. (περιοχές κυρίων ιδεωδών) αποτελούν παραδείγματα ναιτεριανών δακτυλίων.

**1.5.3 Πρόταση.** *Έστω* $R$ *ένας δακτύλιος. Τότε τα ακόλουθα είναι ισοδύναμα* :

(a) $R$ *είναι ναιτεριανός δακτύλιος.*

(b) $R$ *πληροί τη* συνθήκη των αυξουσών αλυσίδων *για ιδεώδη, δηλαδή κάθε ακολουθία ιδεωδών τού* $R$ :

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_m \subseteq I_{m+1} \subseteq \cdots \tag{1.4}$$

*είναι στάσιμη (ήτοι υπάρχει κάποιος* $k \in \mathbb{N} : I_k = I_{k+1} = I_{k+2} = \cdots$*)*

(c) *Κάθε μη κενή συλλογή* $\mathcal{J}$ *ιδεωδών τού* $R$ *περιέχει ένα μεγιστοτικό στοιχείο (ως προς την εγκλειστική σχέση), δηλαδή υπάρχει ένα ιδεώδες* $I \in \mathcal{J}$*, το οποίο δεν περιέχεται σε κανένα άλλο ιδεώδες τής* $\mathcal{J}$*.*

[9] Προς τιμήν τής Emmy Noether (1882-1935), η οποία μελέτησε (περί τη δεκαετία τού 1920) τις ιδιότητες των αλυσίδων ιδεωδών και κατέδειξε τη θεωρητική σημασία τους.

ΑΠΟΔΕΙΞΗ. (a) $\Longrightarrow$ (b) Για κάθε αλυσίδα ιδεωδών (1.4) δείχνουμε εύκολα ότι το σύνολο $I = \bigcup_{m=1}^{\infty} I_m$ είναι ένα ιδεώδες τού $R$. Σύμφωνα με την υπόθεσή μας, θα είναι πεπερασμένως παραγόμενο· επομένως, θα υπάρχουν $a_1, \dots, a_r \in R$, τέτοια ώστε $I = \langle a_1, \dots, a_r \rangle$. Για *αρκούντως μεγάλο* $m$, θα έχουμε $a_i \in I_m$, για όλα τα $i, 1 \leq i \leq r$, απ' όπου έπεται ότι

$$I_m = I_{m+1} = I_{m+2} = \cdots$$

(b) $\Longrightarrow$ (c) Εάν υποθέσουμε ότι υπάρχει μια μη κενή συλλογή $\mathcal{J}$ ιδεωδών τού $R$ χωρίς μεγιστοτικό στοιχείο (ως προς την εγκλειστική σχέση), τότε για τυχόν ιδεώδες $I_1 \in \mathcal{J}$, θα υπάρχει ένα $I_2 \in \mathcal{J}$, τέτοιο ώστε $I_1 \subsetneqq I_2$. Έτσι, επαναλαμβάνοντας την ίδια διαδικασία, κατασκευάζουμε μια *μη στάσιμη* αλυσίδα ιδεωδών $I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$ τού $R$, πράγμα που αντιφάσκει προς την υπόθεσή μας.

(c) $\Longrightarrow$ (b) Προφανές.

(b) $\Longrightarrow$ (a) Ας υποθέσουμε ότι υπάρχει ένα ιδεώδες $I$ τού $R$, το οποίο δεν είναι πεπερασμένως παραγόμενο, και ότι $a_1, \dots, a_r \in I$. Τότε $\langle a_1, \dots, a_r \rangle \subsetneqq I$. Συνεπώς υπάρχει ένα $a_{r+1} \in I : a_{r+1} \notin \langle a_1, \dots, a_r \rangle$. Η αύξουσα αλυσίδα ιδεωδών τού $R$ :

$$\langle a_1 \rangle \subsetneqq \langle a_1, a_2 \rangle \subsetneqq \langle a_1, a_2, a_3 \rangle \subsetneqq \cdots$$

είναι προφανώς μη στάσιμη. □

**1.5.4 Θεώρημα. (Θεώρημα Βάσεως τού Hilbert)** *Για κάθε ναιτεριανό δακτύλιο $R$, ο πολυωνυμικός δακτύλιος $R[\mathsf{X}]$ είναι ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Θα δείξουμε πως εάν ο $R[\mathsf{X}]$ δεν είναι ναιτεριανός δακτύλιος, τότε και ο ίδιος ο $R$ δεν είναι ναιτεριανός. Έστω λοιπόν $I$ ένα ιδεώδες τού $R[\mathsf{X}]$ μη πεπερασμένως παραγόμενο. Τότε, εάν

$$F_1 \in I, \ \text{με} \ \deg(F_1) = \min\{\deg(F) : F \in I\},$$

μπορούμε να ορίσουμε διαδοχικώς πολυώνυμα:

$$F_{k+1} \in I \smallsetminus \langle F_1, \dots, F_k \rangle, \ \text{με} \ \deg(F_{k+1}) = \min\{\deg(F) : F \in I \smallsetminus \langle F_1, \dots, F_k \rangle\},$$

για $k = 1, 2, 3, \dots$, και να θέσουμε $n_k := \deg(F_k)$, $R \ni a_k :=$ συντελεστής τού μεγιστοβαθμίου όρου τού $F_k$. Κατ' αυτόν τον τρόπο τού ορισμού των $F_1, F_2, \dots$ διασφαλίζεται αφ' ενός μεν η ισχύς των ανισοϊσοτήτων

$$n_1 \leq n_2 \leq \cdots \leq n_k \leq n_{k+1} \leq \cdots,$$

αφ' ετέρου δε η ισχύς των ακολούθων εγκλειστικών σχέσεων

$$\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \langle a_1, a_2, a_3 \rangle \subseteq \cdots \subseteq \langle a_1, \dots, a_k \rangle \subseteq \langle a_1, \dots, a_k, a_{k+1} \rangle \subseteq \cdots$$

Θα δείξουμε ότι αυτή η αύξουσα αλυσίδα ιδεωδών τού $R$ δεν είναι στάσιμη. Πράγματι· εάν για κάποιον φυσικό αριθμό $k$ είχαμε

$$\langle a_1, \dots, a_k \rangle = \langle a_1, \dots, a_k, a_{k+1} \rangle ,$$

τότε το $a_{k+1}$ θα εγράφετο ως

$$a_{k+1} = \sum_{i=1}^{k} b_i a_i, \quad (b_i \in R, \ \forall i, \ 1 \leq i \leq k) ,$$

οπότε το πολυώνυμο

$$\begin{aligned} I \smallsetminus \langle F_1, \dots, F_k \rangle \quad &\ni \quad G := F_{k+1} - \sum_{i=1}^{k} b_i \, \mathsf{X}^{n_{k+1}-n_i} \, F_i \\ &= \quad (a_{k+1}\mathsf{X}^{n_{k+1}} + \cdots) - \sum_{i=1}^{k} b_i \, \mathsf{X}^{n_{k+1}-n_i} \, (a_i \mathsf{X}^{n_i} + \cdots) \end{aligned}$$

θα είχε βαθμό $\deg(G) < \deg(F_{k+1})$, πράγμα άτοπο βάσει τής επιλογής τού $F_{k+1}$. Κατά συνέπειαν, η εν λόγω αλυσίδα ιδεωδών δεν είναι στάσιμη, οπότε, σύμφωνα με την πρόταση 1.5.3, ο $R$ δεν είναι ναιτεριανός δακτύλιος. □

**1.5.5 Σημείωση.** Η ανωτέρω σύντομη και πολύ κομψή απόδειξη τού θεωρήματος βάσεως τού Hilbert οφείλεται στη μαθηματικό H. Sarges (*Ein Beweis des Hilbertschen Basissatzes*, J. reine ang. Math. **283/284** (1976), 436-437.)

**1.5.6 Πόρισμα.** *Για κάθε ναιτεριανό δακτύλιο $R$, ο δακτύλιος $R[\mathsf{X}_1, \dots, \mathsf{X}_n]$ είναι ναιτεριανός.*

ΑΠΟΔΕΙΞΗ. Επειδή ο $R[\mathsf{X}_1, \dots, \mathsf{X}_n]$ είναι ισόμορφος τού $R[\mathsf{X}_1, \dots, \mathsf{X}_{n-1}][\mathsf{X}_n]$, η απόδειξη έπεται επαγωγικώς (επί τού $n$) βάσει τού θεωρήματος 1.5.4. □

**1.5.7 Πόρισμα.** *Ο $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ είναι ναιτεριανός δακτύλιος για κάθε σώμα $\mathbf{k}$.*

## Άσκηση

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

(a) Για κάθε ιδεώδες $J'$ τού $R/I$, το $\pi^{-1}(J') = J$ είναι ένα ιδεώδες τού $R$, το οποίο περιέχει το $I$, ενώ για κάθε ιδεώδες $J$ τού $R$, το οποίο περιέχει το $I$, το $\pi(J) = J'$

αποτελεί ένα ιδεώδες τού $R/I$. Μέσω τής αντιστοιχίας

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

ορίζεται μια αμφίρριψη. (*Υπόδειξη*: Βλ. άσκηση **A-1-32** (f)).

(b) Το $J'$ είναι ένα ριζικό (και αντιστοίχως, πρώτο/μεγιστοτικό) ιδεώδες εάν και μόνον εάν το $J$ είναι ριζικό (και αντιστοίχως, πρώτο/μεγιστοτικό).

(c) Εάν το $J$ είναι πεπερασμένως παραγόμενο, τότε και το $J'$ είναι πεπερασμένως παραγόμενο. Εξ αυτού να συναχθεί ότι για οιονδήποτε ναιτεριανό δακτύλιο $R$ ο πηλικοδακτύλιος $R/I$ είναι ναιτεριανός. Επομένως, κάθε δακτύλιος τής μορφής $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \,/\, I$, όπου $\mathbf{k}$ σώμα, είναι ναιτεριανός.

## 1.6 Ανάγωγες Συνιστώσες Αλγεβρικών Συνόλων

**1.6.1 Ορισμός.** Έστω $X$ ένα μη κενό σύνολο εφοδιασμένο με μια τοπολογία $\mathcal{T}$. Ένα μη κενό υποσύνολο $Y \subseteq X$ καλείται **ανάγωγο** όταν δεν μπορεί να γραφεί ως ένωση $Y = Y_1 \cup Y_2$ δυο *γνησίων* υποσυνόλων $Y_1, Y_2$ τού $Y$, καθένα των οποίων είναι κλειστό ως προς την επαγομένη τοπολογία $\mathcal{T}|_Y$ επί τού $Y$. (*Σύμβαση*: Προσοχή! Το κενό σύνολο δεν θα λογίζεται ως ανάγωγο!)

**1.6.2 Πρόταση.** *Έστω $X$ ένα μη κενό σύνολο εφοδιασμένο με μια τοπολογία $\mathcal{T}$. Τότε για ένα μη κενό υποσύνολο $Y \subseteq X$ οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(a) *Το $Y$ είναι ανάγωγο υποσύνολο τού $X$.*

(b) *Εάν $Y = Y_1 \cup Y_2$, όπου τα $Y_1, Y_2$ είναι κλειστά υποσύνολα τού $Y$ (ως προς την $\mathcal{T}|_Y$), τότε είτε $Y = Y_1$ είτε $Y = Y_2$.*

(c) *Για δυο τυχόντα μη κενά, ανοικτά υποσύνολα $U_1, U_2$ τού $Y$ (ως προς την $\mathcal{T}|_Y$) έχουμε $U_1 \cap U_2 \neq \varnothing$.*

(d) *Κάθε ανοικτό σύνολο $\varnothing \neq U \subseteq Y$ (ως προς την $\mathcal{T}|_Y$) είναι πυκνό στο $Y$, δηλαδή $\mathrm{cl}_{\mathcal{T}|_Y}(U) = Y$.*

**1.6.3 Σημείωση.** Κάθε ανάγωγος τοπολογικός χώρος είναι προφανώς συνεκτικός, αλλά το αντίστροφο δεν είναι πάντοτε αληθές. Επί παραδείγματι, η πραγματική ευθεία $\mathbb{R}$ με τη συνήθη τοπολογία είναι συνεκτική, μη ανάγωγη. (Τα μόνα ανάγωγα υποσύνολά της είναι τα μονοσύνολα.)

**1.6.4 Πόρισμα.** *Εάν ο $X$ είναι ένας ανάγωγος τοπολογικός χώρος, τότε κάθε μη κενό, ανοικτό υποσύνολο $Y$ τού $X$ είναι ανάγωγο.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $Y$ γράφεται ως ένωση $Y = Y_1 \cup Y_2$ δυο κλειστών υποσυνόλων $Y_1, Y_2$ τού $Y$. Τότε υπάρχουν κλειστά υποσύνολα $Z_1, Z_2$ τού $X$, τέτοια ώστε να ισχύουν οι ισότητες $Y_1 = Y \cap Z_1$ και $Y_2 = Y \cap Z_2$. Κατά συνέπειαν,

$$X = (X \smallsetminus Y) \cup Y = (X \smallsetminus Y) \cup (Y \cap Z_1) \cup (Y \cap Z_2)$$

$$\Rightarrow X = ((X \smallsetminus Y) \cup Z_1) \cup ((X \smallsetminus Y) \cup Z_2)\,,$$

απ' όπου έπεται ότι είτε $Z_1 = Y$ είτε $Z_2 = Y$ (βλ. 1.6.2 (b)). Άρα είτε $Y = Y_1$ είτε $Y = Y_2$. Αρκεί λοιπόν να εφαρμοσθεί εκ νέου το (b) τής προτάσεως 1.6.2 για να αποδειχθεί ότι το $Y$ είναι όντως ανάγωγο. □

**1.6.5 Πόρισμα.** *Η κλειστή θήκη* $\mathrm{cl}_{\mathcal{T}}(Y)$ *οιουδήποτε αναγώγου υποσυνόλου* $Y$ *ενός* (*μη κενού* ) *τοπολογικού χώρου* $(X, \mathcal{T})$ *είναι ανάγωγη.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $\mathrm{cl}_{\mathcal{T}}(Y)$ γράφεται ως ένωση $\mathrm{cl}_{\mathcal{T}}(Y) = Z_1 \cup Z_2$ δυο κλειστών υποσυνόλων $Z_1, Z_2$ τού $X$. Τότε (λόγω τού (d) τής προτάσεως 1.6.2)

$$Y = \mathrm{cl}_{\mathcal{T}|_Y}(Y) = Y \cap \mathrm{cl}_{\mathcal{T}}(Y) = (Y \cap Z_1) \cup (Y \cap Z_2)\,,$$

οπότε είτε $Y = Y \cap Z_1$ είτε $Y = Y \cap Z_2$ (βλ. 1.6.2 (b)). Στην πρώτη περίπτωση,

$$Y \subseteq Z_1 \Rightarrow \mathrm{cl}_{\mathcal{T}}(Y) \subseteq \mathrm{cl}_{\mathcal{T}}(Z_1) = Z_1.$$

Όμως εξ υποθέσεως, $Z_1 \subseteq \mathrm{cl}_{\mathcal{T}}(Y)$. Άρα $\mathrm{cl}_{\mathcal{T}}(Y) = Z_1$. Αναλόγως δείχνουμε την ισότητα $\mathrm{cl}_{\mathcal{T}}(Y) = Z_2$ στη δεύτερη περίπτωση. Αρκεί λοιπόν να εφαρμοσθεί εκ νέου το (b) τής προτάσεως 1.6.2 για να αποδειχθεί ότι το $\mathrm{cl}_{\mathcal{T}}(Y)$ είναι όντως ανάγωγο. □

**1.6.6 Πόρισμα.** *Έστω* $\varphi : X \longrightarrow X'$ *μια συνεχής απεικόνιση μεταξύ δυο τοπολογικών χώρων* $X, X'$. *Εάν το* $Y$ *είναι ένα ανάγωγο υποσύνολο τού* $X$, *τότε η εικόνα* $Y' = \varphi(Y)$ *τού* $Y$ *μέσω τής* $\varphi$ *είναι ένα ανάγωγο υποσύνολο τού* $X'$.

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι το $Y'$ γράφεται ως ένωση $Y' = Z_1 \cup Z_2$ δυο κλειστών υποσυνόλων $Z_1, Z_2$ τού $Y'$. Τότε

$$Y = \varphi^{-1}(\varphi(Y)) = \varphi^{-1}(Y') = \varphi^{-1}(Z_1 \cup Z_2) = \varphi^{-1}(Z_1) \cup \varphi^{-1}(Z_2)\,.$$

Επειδή η $\varphi$ υπετέθη συνεχής, τα $\varphi^{-1}(Z_1), \varphi^{-1}(Z_2) \subseteq Y$ είναι κλειστά, οπότε είτε $Y = \varphi^{-1}(Z_1)$ είτε $Y = \varphi^{-1}(Z_2)$. Επομένως, είτε $Y' = \varphi(\varphi^{-1}(Z_1)) = Z_1$ είτε $Y' = \varphi(\varphi^{-1}(Z_2)) = Z_2$, κάτι που σημαίνει ότι το $Y'$ είναι ανάγωγο υποσύνολο τού $X'$ (βάσει τού (b) τής προτάσεως 1.6.2). □

**1.6.7 Πρόταση.** *Έστω* $\mathbb{A}^n_{\mathbf{k}}$ *ο* $n$*-διάστατος συσχετικός χώρος υπεράνω ενός σώματος* $\mathbf{k}$, *εφοδιασμένος με την τοπολογία Zariski* $\mathcal{T}_{\mathrm{Zar}}$ (βλ. 1.2.4). *Τότε ένα συσχετικό αλγεβρικό σύνολο* $V \subseteq \mathbb{A}^n_{\mathbf{k}}$ *είναι ανάγωγο εάν και μόνον εάν το ιδεώδες του* $\mathbf{I}(V)$ *είναι πρώτο.*

ΑΠΟΔΕΙΞΗ. Εάν το $\mathbf{I}(V)$ δεν είναι πρώτο, τότε υπάρχουν $F_1, F_2 \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τέτοια ώστε $F_1F_2 \in \mathbf{I}(V)$ ενώ $F_1 \notin \mathbf{I}(V)$, $F_2 \notin \mathbf{I}(V)$. Επομένως,

$$V = (V \cap \mathbf{V}(F_1)) \cup (V \cap \mathbf{V}(F_2)), \quad V \cap \mathbf{V}(F_1) \subsetneqq V, \quad V \cap \mathbf{V}(F_2) \subsetneqq V,$$

δηλαδή το $V$ θα είναι μη ανάγωγο. Και αντιστρόφως· εάν το $\mathbf{I}(V)$ είναι πρώτο και υποθέσουμε ότι $V = V_1 \cup V_2$, όπου τα $V_1, V_2$ είναι αλγεβρικά σύνολα εντός τού $\mathbb{A}^n_{\mathbf{k}}$ με $V_1 \subsetneqq V$, $V_2 \subsetneqq V$, τότε, σύμφωνα με την πρόταση 1.3.1 (1) και την άσκηση **A-1-16** έχουμε

$$\mathbf{I}(V) \subsetneqq \mathbf{I}(V_1), \ \ \mathbf{I}(V) \subsetneqq \mathbf{I}(V_2).$$

Έστω $F \in \mathbf{I}(V_1) \smallsetminus \mathbf{I}(V)$ και έστω $G \in \mathbf{I}(V_2)$. Επειδή $V = V_1 \cup V_2$, το γινόμενο $FG$ μηδενίζεται σε κάθε σημείο τού $V$, κι επομένως $FG \in \mathbf{I}(V)$. Αλλά το $\mathbf{I}(V)$ είναι πρώτο ιδεώδες, οπότε είτε $F \in \mathbf{I}(V)$ είτε $G \in \mathbf{I}(V)$. Αφού $F \in \mathbf{I}(V_1) \smallsetminus \mathbf{I}(V)$, έχουμε αναγκαστικώς $G \in \mathbf{I}(V)$. Άρα, και πάλι κατά την άσκηση **A-1-16**, $\mathbf{I}(V) = \mathbf{I}(V_2) \Rightarrow V = V_2$, πράγμα άτοπο. □

**1.6.8 Ορισμός.** Ένας μη κενός τοπολογικός χώρος $(X, \mathcal{T})$ καλείται **ναιτεριανός χώρος** όταν πληροί τη *συνθήκη των φθινουσών αλυσίδων* για κλειστά υποσύνολα, δηλαδή όταν κάθε ακολουθία κλειστών υποσυνόλων τού $X$:

$$Y_1 \supseteq Y_2 \supseteq Y_3 \supseteq \cdots \supseteq Y_m \supseteq Y_{m+1} \supseteq \cdots \tag{1.5}$$

είναι *στάσιμη* (ήτοι υπάρχει κάποιος $k \in \mathbb{N} : Y_k = Y_{k+1} = Y_{k+2} = \cdots$).

**1.6.9 Λήμμα.** *Για έναν μη κενό τοπολογικό χώρο $(X, \mathcal{T})$ οι κάτωθι συνθήκες είναι ισοδύναμες*:

(a) *$O\,(X, \mathcal{T})$ είναι ναιτεριανός χώρος.*

(b) *Κάθε ακολουθία ανοικτών υποσυνόλων τού $X$*:

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \cdots \subseteq U_m \subseteq U_{m+1} \subseteq \cdots \tag{1.6}$$

*είναι στάσιμη (ήτοι υπάρχει κάποιος $k \in \mathbb{N} : U_k = U_{k+1} = U_{k+2} = \cdots$).*

(c) *Κάθε μη κενή συλλογή $\mathcal{Y}$ κλειστών υποσυνόλων τού $X$ περιέχει ένα ελαχιστοτικό στοιχείο (ως προς την εγκλειστική σχέση), δηλαδή υπάρχει ένα στοιχείο $Y \in \mathcal{Y}$, το οποίο δεν περιέχει κανένα άλλο στοιχείο τής $\mathcal{Y}$.*

ΑΠΟΔΕΙΞΗ. Η ισοδυναμία είναι (a)⇔(b) είναι εμφανής, καθότι κανείς μεταβαίνει από μια ακολουθία κλειστών υποσυνόλων (1.5) τού $X$ σε μια ακολουθία ανοικτών υποσυνόλων (1.6) τού $X$ (και αντιστρόφως) ύστερα από θεώρηση των συμπληρωμάτων των μελών της (ως προς τον $X$). Η συνεπαγωγή (c)⇒(a) είναι προφανής. Για την απόδειξη τής συνεπαγωγής (a)⇒(c) υποθέτουμε ότι υπάρχει μια μη κενή συλλογή $\mathcal{Y}$ κλειστών υποσυνόλων τού $X$ χωρίς ελαχιστοτικό στοιχείο (ως προς την εγκλειστική σχέση). Για τυχόν

$Y_1 \in \mathcal{Y}$ υπάρχει ένα $Y_2 \in \mathcal{Y}$, τέτοιο ώστε $Y_2 \subsetneqq Y_1$. Έτσι, επαναλαμβάνοντας την ίδια διαδικασία, κατασκευάζουμε μια *μη στάσιμη* ακολουθία $Y_1 \supsetneqq Y_2 \supsetneqq Y_3 \supsetneqq \cdots$ κλειστών υποσυνόλων τού $X$, πράγμα που αντιφάσκει προς την υπόθεσή μας. □

**1.6.10 Σημείωση.** Προφανώς, τόσον οι ανοικτοί όσον και οι κλειστοί υπόχωροι ενός ναιτεριανού τοπολογικού χώρου είναι ναιτεριανοί.

**1.6.11 Θεώρημα.** *Έστω $(X, \mathcal{T})$ ένας ναιτεριανός χώρος και έστω $Y$ ένα μη κενό, κλειστό υποσύνολό του. Τότε υπάρχουν μονοσημάντως ορισμένα (μέχρις αναδιατάξεως δεικτών) κλειστά ανάγωγα υποσύνολα $Y_1, \ldots, Y_m$ τού $X$,τέτοια ώστε*

$$Y = Y_1 \cup Y_2 \cup \cdots \cup Y_m \text{ και } Y_i \nsubseteqq Y_j, \ \forall i, j \in \{1, 2, \ldots, m\}, \ i \neq j.$$

ΑΠΟΔΕΙΞΗ. Έστω

$$\mathcal{Y} := \left\{ \text{κλειστά υποσύνολα } \varnothing \neq Y \subseteq X \;\middle|\; \begin{array}{l} \text{το } Y \text{ δεν γράφεται ως ένωση} \\ \text{πεπερασμένου πλήθους αναγώγων} \\ \text{κλειστών υποσυνόλων τού } X \end{array} \right\}.$$

Θα δείξουμε ότι $\mathcal{Y} = \varnothing$. Υποθέτουμε ότι $\mathcal{Y} \neq \varnothing$ και επιλέγουμε ένα ελαχιστοτικό στοιχείο $Y_0$ τής συλλογής $\mathcal{Y}$ (βλ. λήμμα 1.6.9). Το $Y_0 \in \mathcal{Y}$ είναι μη ανάγωγο, οπότε μπορεί να γραφεί ως

$$Y_0 = Y_1 \cup Y_2, \ \ Y_1 \subsetneqq Y_0, \ Y_2 \subsetneqq Y_0.$$

Τότε για $i = 1, 2$, τα $Y_i$ δεν ανήκουν στην $\mathcal{Y}$, οπότε μπορούν να γραφούν ως

$$Y_i = Y_{i1} \cup Y_{i2} \cup \cdots \cup Y_{im_i},$$

όπου τα $Y_{ij}$ είναι ανάγωγα κλειστά υποσύνολα τού $X$ για τα $i \in \{1, 2\}$ και για όλους τους (υπο)δείκτες $j \in \{1, 2, \ldots, m_i\}$. Τούτο είναι άτοπο, διότι

$$\bigcup \{Y_{ij} \mid \ i \in \{1, 2\}, \ j \in \{1, 2, \ldots, m_i\}\} = Y_0.$$

Άρα όντως $\mathcal{Y} = \varnothing$, κι έτσι κάθε κλειστό υποσύνολο $Y$ τού $X$ μπορεί να γραφεί ως ένωση *αναγώγων* κλειστών υποσυνόλων τού $X$

$$Y = Y_1 \cup Y_2 \cup \cdots \cup Y_m.$$

Για να διασφαλισθεί η ισχύς και τής δεύτερης επιπρόσθετης συνθήκης, δεν έχουμε παρά να αγνοήσουμε κάθε ανάγωγο κλειστό υποσύνολο $Y_\kappa$ τού $X$ για το οποίο $Y_\kappa \subseteq Y_\lambda$, για κάποια $\kappa, \lambda \in \{1, 2, \ldots, m\}, \kappa \neq \lambda$. Απομένει λοιπόν να αποδείξουμε το μονοσήμαντο αυτής τής αποσυνθέσεως. Έστω

$$Y = Z_1 \cup Z_2 \cup \cdots \cup Z_{m'}$$

μια άλλη αποσύνθεση τού $Y$ (αυτού τού είδους). Τότε

$$Y_i \nsubseteqq Y_j,\ \ \forall i,j \in \{1,2,\dots,m\},\ i \neq j,$$

και

$$Z_\mu \nsubseteqq Z_\nu,\ \ \forall \mu,\nu \in \{1,2,\dots,m'\},\ \mu \neq \nu,$$

ενώ για κάθε $\kappa, 1 \leq \kappa \leq m$, έχουμε

$$Y_\kappa = \left(\bigcup_{\mu=1}^{m'} Z_\mu\right) \cap Y_\kappa.$$

Έστω $s : \{1,\dots,m\} \longrightarrow \{1,2,\dots,m'\}$ η απεικόνιση

$$s(\kappa) := \min\left\{\mu \in \{1,2,\dots,m'\} \,|Y_\kappa = (Z_1 \cup \cdots \cup Z_\mu) \cap Y_\kappa\right\},\ \ \forall \kappa \in \{1,\dots,m\}.$$

Επειδή

$$\left(Z_1 \cup \cdots \cup Z_{s(\kappa)-1}\right) \cap Y_\kappa \subsetneqq Y_\kappa,$$

ισχύει η ισότητα

$$\left(\left(Z_1 \cup \cdots \cup Z_{s(\kappa)-1}\right) \cap Y_\kappa\right) \cup \left(Z_{s(\kappa)} \cap Y_\kappa\right) = Y_\kappa.$$

Επιπροσθέτως, επειδή αμφότερα τα

$$\left(Z_1 \cup \cdots \cup Z_{s(\kappa)-1}\right) \cap Y_\kappa,\ \ Z_{s(\kappa)} \cap Y_\kappa$$

είναι κλειστά υποσύνολα τού αναγώγου κλειστού υποσυνόλου $Y_\kappa$ τού $X$, έχουμε

$$Z_{s(\kappa)} \cap Y_\kappa = Y_\kappa \Longrightarrow Y_\kappa \subseteq Z_{s(\kappa)}. \tag{1.7}$$

Από την άλλη μεριά, για οιοδήποτε $\lambda, 1 \leq \lambda \leq m'$,

$$Z_\lambda = \left(\bigcup_{i=1}^{m} Y_i\right) \cap Z_\lambda.$$

Ορίζοντας την απεικόνιση $t : \{1,\dots,m'\} \longrightarrow \{1,2,\dots,m\}$ μέσω τού τύπου

$$t(\lambda) := \min\left\{i \in \{1,2,\dots,m\} \,|Z_\lambda = (Y_1 \cup \cdots \cup Y_i) \cap Z_\lambda\right\},\ \ \forall \lambda \in \{1,\dots,m'\},$$

αποδεικνύουμε με ανάλογη επιχειρηματολογία ότι

$$Y_{t(\lambda)} \cap Z_\lambda = Z_\lambda \Longrightarrow Z_\lambda \subseteq Y_{t(\lambda)}. \tag{1.8}$$

Από τους εγκλεισμούς (1.7) και (1.8) συμπεραίνουμε ότι

$$\left\{ \begin{array}{l} Y_\kappa \subseteq Z_{s(\kappa)} \subseteq Y_{t(s(\kappa))} \Longrightarrow \kappa = t(s(\kappa)),\ \ Y_\kappa = Z_{s(\kappa)},\ \ \forall \kappa \in \{1, \dots, m\} \\ \\ Z_\lambda \subseteq Y_{t(\lambda)} \subseteq Z_{s(t(\lambda))} \Longrightarrow \lambda = s(t(\lambda)),\ \ Z_\lambda = Y_{t(\lambda)},\ \ \forall \lambda \in \{1, \dots, m'\} \end{array} \right\},$$

οπότε $t \circ s = \mathrm{Id}_{\{1,\dots,m\}}$, $s \circ t = \mathrm{Id}_{\{1,\dots,m'\}} \Longrightarrow m = m'$, $s = t^{-1}$, και η ιδιότητα τού μονοσημάντου (μέχρις αναδιατάξεως δεικτών) είναι προφανής. □

**1.6.12 Ορισμός.** Τα $Y_1, \dots, Y_m$ τού θεωρήματος 1.6.11 λέγονται **ανάγωγες συνιστώσες** τού $Y$ και η μονοσήμαντη αποσύνθεση $Y = \bigcup_{i=1}^m Y_i$ **αποσύνθεση τού** $Y$ **σε ανάγωγες συνιστώσες.**

**1.6.13 Λήμμα.** *Ο $n$-διάστατος συσχετικός χώρος $\mathbb{A}^n_{\mathbf{k}}$ υπεράνω ενός σώματος $\mathbf{k}$, εφοδιασμένος με την τοπολογία Zariski $\mathcal{T}_{\mathrm{Zar}}$* (βλ. 1.2.4)*, αποτελεί έναν ναιτεριανό χώρο.*

ΑΠΟΔΕΙΞΗ. Έστω $V_1 \supseteq V_2 \supseteq \cdots \supseteq V_m \supseteq V_{m+1} \supseteq \cdots$ μια ακολουθία κατά Zariski κλειστών (ήτοι αλγεβρικών) υποσυνόλων τού $\mathbb{A}^n_{\mathbf{k}}$. Λόγω τού (1) τής προτάσεως 1.3.1 αυτή επάγει την ακολουθία ιδεωδών

$$\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \cdots \subseteq \mathbf{I}(V_m) \subseteq \mathbf{I}(V_{m+1}) \subseteq \cdots$$

τού πολυωνυμικού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$. Επειδή ο $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ είναι ναιτεριανός δακτύλιος (βλ. θεώρημα 1.5.4), υπάρχει κάποιος $k \in \mathbb{N} : \mathbf{I}(V_k) = \mathbf{I}(V_{k+1}) = \cdots$. Μέσω τής ασκήσεως **A-1-16** συμπεραίνουμε ότι $V_k = V_{k+1} = \cdots$. Άρα ο $\mathbb{A}^n_{\mathbf{k}}$ αποτελεί έναν ναιτεριανό χώρο. □

**1.6.14 Θεώρημα.** *Έστω $\mathbb{A}^n_{\mathbf{k}}$ ο $n$-διάστατος συσχετικός χώρος υπεράνω ενός σώματος $\mathbf{k}$ και έστω $V$ ένα αλγεβρικό υποσύνολό του. Τότε υπάρχουν μονοσημάντως ορισμένα* (*μέχρις αναδιατάξεως δεικτών*) *ανάγωγα αλγεβρικά σύνολα $V_1, \dots, V_m$* (***οι ανάγωγες συνιστώσες τού $V$***)*, τέτοια ώστε*

$$V = V_1 \cup V_2 \cup \cdots \cup V_m \ \textit{και}\ \ V_i \nsubseteq V_j,\ \ \forall i, j \in \{1, 2, \dots, m\},\ i \neq j.$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το θεώρημα 1.6.11 και το λήμμα 1.6.13. □

## Ασκήσεις

**A-1-37.** Να δοθεί ένα παράδειγμα μιας άπειρης οικογενείας ιδεωδών $\mathcal{J}$ ενός ναιτεριανού δακτυλίου, ούτως ώστε κανένα μεγιστοτικό μέλος τής $\mathcal{J}$ να μην είναι μεγιστοτικό ιδεώδες.

**A-1-38**. Να αποδειχθεί ότι κάθε γνήσιο ιδεώδες ενός ναιτεριανού δακτυλίου περιέχεται σε ένα μεγιστοτικό ιδεώδες. (*Υπόδειξη*: Εάν το $I$ είναι ένα ιδεώδες, να εφαρμοσθεί το (c) τής προτάσεως 1.5.3 για την οικογένεια όλων των γνησίων ιδεωδών, τα οποία περιέχουν το $I$.)

**A-1-39**. Να αποδειχθεί η πρόταση 1.6.2.

**A-1-40**. (a) Να αποδειχθεί ότι το $\mathbf{V}(\mathsf{Y}-\mathsf{X}^2) \subset \mathbb{A}^2_{\mathbb{C}}$ είναι ανάγωγο και ότι ισχύει η ισότητα: $\mathbf{I}(\mathbf{V}(\mathsf{Y}-\mathsf{X}^2)) = \langle \mathsf{Y}-\mathsf{X}^2 \rangle$.

(b) Να αποσυντεθεί το $\mathbf{V}(\mathsf{Y}^4-\mathsf{X}^2, \mathsf{Y}^4-\mathsf{X}^2\mathsf{Y}^2+\mathsf{X}\mathsf{Y}^2-\mathsf{X}^3) \subset \mathbb{A}^2_{\mathbb{C}}$ σε ανάγωγες συνιστώσες.

**A-1-41**. Να αποδειχθεί ότι το πολυώνυμο $F = \mathsf{Y}^2+\mathsf{X}^2\,(\mathsf{X}-1)^2 \in \mathbb{R}[\mathsf{X},\mathsf{Y}]$ είναι ανάγωγο, ενώ η υπερεπιφάνεια $\mathbf{V}(F)$ είναι μη ανάγωγη.

**A-1-42**. (a) Έστω ότι τα $V, W$ είναι δυο αλγεβρικά σύνολα εντός τού συσχετικού χώρου $\mathbb{A}^n_{\mathbf{k}}$ και ότι $V \subseteq W$. Να αποδειχθεί ότι 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, να αποδειχθεί ότι $V_i \nsubseteq \bigcup_{j\in\{1,2,\ldots,m\}\smallsetminus\{i\}} V_j$, για κάθε $i, 1 \le i \le m$.

**A-1-43**. Εάν το $\mathbf{k}$ είναι ένα απειροπληθές σώμα και $n \in \mathbb{N}$, να αποδειχθεί ότι ο συσχετικός χώρος $\mathbb{A}^n_{\mathbf{k}}$ είναι ανάγωγος.

## 1.7 Αλγεβρικά Υποσύνολα τού Συσχετικού Επιπέδου

Προτού αναπτύξουμε τη γενική θεωρία περί αλγεβρικών συνόλων θα ρίξουμε μια σύντομη ματιά στο συσχετικό επίπεδο $\mathbb{A}^2_{\mathbf{k}}$ και θα προσδιορίσουμε όλα τα αλγεβρικά υποσύνολά του. Σύμφωνα με το θεώρημα 1.6.14, προς τούτο είναι αρκετό να βρούμε τα ανάγωγα αλγεβρικά υποσύνολά του.

**1.7.1 Πρόταση.** *Έστω ότι το* $\mathbf{k}$ *είναι ένα σώμα και ότι τα* $F, G$ *είναι πολυώνυμα ανήκοντα στον* $\mathbf{k}[\mathsf{X},\mathsf{Y}]$, *χωρίς κοινούς παράγοντες. Τότε το σύνολο*

$$\mathbf{V}(F,G) = \mathbf{V}(F) \cap \mathbf{V}(G)$$

*αποτελεί ένα πεπερασμένο σημειοσύνολο τού* $\mathbb{A}^2_{\mathbf{k}}$.

ΑΠΟΔΕΙΞΗ. Εάν τα $F, G$ δεν διαθέτουν κοινούς παράγοντες (δηλαδή εάν δεν υπάρχουν ανάγωγα πολυώνυμα που να διαιρούν αμφότερα) εντός τού δακτυλίου $\mathbf{k}[\mathsf{X},\mathsf{Y}] \cong \mathbf{k}[\mathsf{X}][\mathsf{Y}]$, τότε δεν θα διαθέτουν κοινούς παράγοντες ούτε εντός τού $\mathbf{k}\,(\mathsf{X})\,[\mathsf{Y}]$. Επειδή ο δακτύλιος $\mathbf{k}\,(\mathsf{X})\,[\mathsf{Y}]$ είναι Π.Κ.Ι. (βλ. θεώρημα 1.1.24), είναι και περιοχή με μ.κ.δ. Προφανώς μ.κ.δ.$(F,G) \underset{\text{συν.}}{\sim} 1$ εντός τού $\mathbf{k}\,(\mathsf{X})\,[\mathsf{Y}]$, οπότε

$$S\cdot F + \widetilde{S}\cdot G = 1 \;\text{ για κάποια }\; S, \widetilde{S} \in \mathbf{k}\,(\mathsf{X})\,[\mathsf{Y}].$$

Ταυτοχρόνως (από τον ορισμό τού σώματος κλασμάτων) το $S$ γράφεται ως

$$S = \sum_{i=1}^{n} s_i \mathsf{Y}^i,\ s_i = \frac{F_i}{G_i},\ \text{ όπου }\ F_i \in \mathbf{k}[\mathsf{X}],\ G_i \in \mathbf{k}[\mathsf{X}] \setminus \{\mathbf{0}\},\ \forall i,\ 1 \leq i \leq n,$$

για κάποιον $n \in \mathbb{N}$. Επομένως,

$$\left( \prod_{i=1}^{n} G_i \right) S = \sum_{i=1}^{n} F_i \left( \prod_{j \in \{1,2,\ldots,n\} \setminus \{i\}}^{n} G_j \right) \mathsf{Y}^i \in \mathbf{k}[\mathsf{X}, \mathsf{Y}] \tag{1.9}$$

Ομοίως ισχύει

$$\left( \prod_{\kappa=1}^{m} \widetilde{G}_\kappa \right) \widetilde{S} = \sum_{\kappa=1}^{m} \widetilde{F}_\kappa \left( \prod_{\lambda \in \{1,2,\ldots,n\} \setminus \{\kappa\}}^{n} \widetilde{G}_\lambda \right) \mathsf{Y}^\kappa \in \mathbf{k}[\mathsf{X}, \mathsf{Y}] \tag{1.10}$$

για το πολυώνυμο $\widetilde{S}$ που γράφεται υπό τη μορφή

$$\widetilde{S} = \sum_{\kappa=1}^{m} \widetilde{s}_\kappa \mathsf{Y}^\kappa,\ \widetilde{s}_\kappa = \frac{\widetilde{F}_\kappa}{\widetilde{G}_\kappa},\ \text{ όπου }\ \widetilde{F}_\kappa \in \mathbf{k}[\mathsf{X}],\ \widetilde{G}_\kappa \in \mathbf{k}[\mathsf{X}] \setminus \{\mathbf{0}\},\ \forall \kappa,\ 1 \leq \kappa \leq m,$$

για κάποιον $m \in \mathbb{N}$. Ορίζοντας λοιπόν ως $D$ το

$$D := \left( \prod_{i=1}^{n} G_i \right) \cdot \left( \prod_{\kappa=1}^{m} \widetilde{G}_\kappa \right) \in \mathbf{k}[\mathsf{X}] \setminus \{\mathbf{0}\}$$

και ως $A$ και $B$ τα

$$A := \left( \sum_{i=1}^{n} F_i \left( \prod_{j \in \{1,2,\ldots,n\} \setminus \{i\}}^{n} G_j \right) \mathsf{Y}^i \right) \cdot \left( \prod_{\kappa=1}^{m} \widetilde{G}_\kappa \right) \in \mathbf{k}[\mathsf{X}, \mathsf{Y}]$$

και

$$B := \left( \sum_{\kappa=1}^{m} \widetilde{F}_\kappa \left( \prod_{\lambda \in \{1,2,\ldots,n\} \setminus \{\kappa\}}^{n} \widetilde{G}_\lambda \right) \mathsf{Y}^\kappa \right) \cdot \left( \prod_{i=1}^{n} G_i \right) \in \mathbf{k}[\mathsf{X}, \mathsf{Y}],$$

αντιστοίχως, λαμβάνουμε μέσω των (1.9) και (1.10):

$$\begin{cases} D \cdot S = A,\ D \cdot \widetilde{S} = B \Longrightarrow A \cdot F + B \cdot G = D \\ \\ \Longrightarrow \left[ \forall P,\ P = (a,b) \in \mathbf{V}(F,G) \subseteq \mathbb{A}^2_{\mathbf{k}} \Longrightarrow D\,(a) = 0 \right]. \end{cases}$$

Όμως το $D$ έχει πεπερασμένο πλήθος σημείων μηδενισμού. Τελικώς, μόνον πεπερασμένο πλήθος X-συντεταγμένων (τετμημένων) εμφανίζεται σε όλο το εύρος που καταλαμβάνουν τα σημεία τού $\mathbf{V}(F,G)$. Κι επειδή η διαδικασία αυτή μπορεί να επαναληφθεί εφαρμοζόμενη για τις Y-συντεταγμένες (τεταγμένες) των σημείων τού $\mathbf{V}(F,G)$, έπεται ότι το $\mathbf{V}(F,G)$ αποτελεί ένα πεπερασμένο σημειοσύνολο τού $\mathbb{A}^2_{\mathbf{k}}$. □

**1.7.2 Πόρισμα.** *Εάν το $F$ είναι ένα ανάγωγο πολυώνυμο τού $\mathbf{k}[\mathsf{X},\mathsf{Y}]$ και εάν το $\mathbf{V}(F)$ είναι απειροπληθές, τότε*

$$\mathbf{I}(\mathbf{V}(F)) = \langle F\rangle$$

*και το $\mathbf{V}(F)$ είναι ανάγωγο.*

ΑΠΟΔΕΙΞΗ. Προφανώς $\langle F\rangle \subseteq \mathbf{I}(\mathbf{V}(F))$. Εάν $G \in \mathbf{I}(\mathbf{V}(F))$ και το $\mathbf{V}(F)$ είναι απειροπληθές, τότε και το $\mathbf{V}(F,G)$ θα είναι άπειρο (διότι $\forall P \in \mathbf{V}(F)$, $G(P)=0$, οπότε $\forall P \in \mathbf{V}(F)$, $P \in \mathbf{V}(G)$, που σημαίνει ότι $\mathbf{V}(F) \subseteq \mathbf{V}(G)$, απ' όπου έπεται ότι $\mathbf{V}(F,G) = \mathbf{V}(F)$). Έτσι, σύμφωνα με την πρόταση 1.7.1, $F \mid G$, ήτοι $G \in \langle F\rangle$. Άρα $\mathbf{I}(\mathbf{V}(F)) \subseteq \langle F\rangle$. Εξάλλου, το γεγονός ότι το $\mathbf{V}(F)$ είναι ανάγωγο, απορρέει άμεσα από την πρόταση 1.6.7 και από το ότι το $\langle F\rangle = \mathbf{I}(\mathbf{V}(F))$ είναι πρώτο ιδεώδες (αφού το $F$ είναι ανάγωγο πολυώνυμο). □

**1.7.3 Πόρισμα.** *Εάν υποθέσουμε ότι το $\mathbf{k}$ είναι ένα απειροπληθές σώμα, τότε τα ανάγωγα αλγεβρικά σύνολα εντός τού $\mathbb{A}^2_{\mathbf{k}}$ θα είναι ακριβώς τα: $\mathbb{A}^2_{\mathbf{k}}$, σημεία και ανάγωγες συσχετικές επίπεδες καμπύλες $\mathbf{V}(F)$, όπου το $F$ είναι ένα ανάγωγο πολυώνυμο και το $\mathbf{V}(F)$ ένα άπειρο σημειοσύνολο.*

ΑΠΟΔΕΙΞΗ. Έστω $W$ ένα ανάγωγο αλγεβρικό σύνολο εντός τού $\mathbb{A}^2_{\mathbf{k}}$. Εάν το $W$ είναι πεπερασμένο ή $\mathbf{I}(W) = \{0\}$, τότε το $W$ είναι τού απαιτούμενου τύπου. (Στην πρώτη περίπτωση το ένα και μόνον σημείο τού επιπέδου και στη δεύτερη ολόκληρος ο $\mathbb{A}^2_{\mathbf{k}}$, αφού

$$\mathbf{I}(W) = \{0\} = \mathbf{I}\left(\mathbb{A}^2_{\mathbf{k}}\right),$$

και από την άσκηση **A-1-16**, $W = \mathbb{A}^2_{\mathbf{k}}$). Στην αντίθετη περίπτωση, το ιδεώδες τού $\mathbf{I}(W)$ θα περιέχει ένα μη σταθερό πολυώνυμο $H$. Και επειδή (κατά την παραδοχή μας και την πρόταση 1.6.7) το $\mathbf{I}(W)$ είναι πρώτο, κάποιος ανάγωγος παράγοντας, ας τον πούμε $F$, τού πολυωνύμου $H$ θα ανήκει στο $\mathbf{I}(W)$. Τότε $\mathbf{I}(W) = \langle F\rangle$. (Πράγματι· εάν υποθέσουμε ότι $\langle F\rangle \subsetneqq \mathbf{I}(W)$ και ότι υπάρχει ένα $G \in \mathbf{I}(W)$, τέτοιο ώστε $G \notin \langle F\rangle$, τότε θα έχουμε $F \nmid G$, οπότε από την πρόταση 1.7.1 το σύνολο $\mathbf{V}(F,G)$ θα είναι πεπερασμένο. Ταυτοχρόνως,

$$F, G \in \mathbf{I}(W) \Longrightarrow [\forall P \in W : F(P) = G(P) = 0],$$

που σημαίνει ότι

$$[\forall P \in W : P \in \mathbf{V}(F) \cap \mathbf{V}(G) = \mathbf{V}(F,G)] \Longrightarrow W \subseteq \mathbf{V}(F,G),$$

απ' όπου έπεται ότι το $W$ οφείλει να είναι πεπερασμένο. Αυτό προφανώς αντιτίθεται προς την αρχική μας παραδοχή).

Τώρα, επειδή

$$F \in \mathbf{I}(W) \Longrightarrow W \subseteq \mathbf{V}(F),$$

και το $W$ υποτίθεται ότι είναι απειροπληθές, έπεται ότι *και* το $\mathbf{V}(F)$ είναι απειροπληθές. Εφαρμόζοντας το πόρισμα 1.7.2 λαμβάνουμε $\mathbf{I}(\mathbf{V}(F)) = \langle F \rangle = \mathbf{I}(W)$, οπότε $W = \mathbf{V}(F)$ (βάσει τής ασκήσεως **A-1-16**). □

**1.7.4 Πόρισμα.** *Έστω ότι το* $\mathbf{k}$ *είναι ένα αλγεβρικώς κλειστό σώμα και ότι θεωρούμε ένα* $F \in \mathbf{k}[\mathsf{X}, \mathsf{Y}]$. *Εάν η*

$$F = F_1^{n_1} \cdot F_2^{n_2} \cdot \cdots \cdot F_\kappa^{n_\kappa}$$

*είναι η αποσύνθεση τού* $F$ *ως γινομένου* $\kappa$ *σαφώς διακεκριμένων αναγώγων πολυωνύμων, υψωμένων σε κατάλληλες δυνάμεις, τότε η*

$$\mathbf{V}(F) = \mathbf{V}(F_1) \cup \mathbf{V}(F_2) \cup \cdots \cup \mathbf{V}(F_\kappa)$$

*αποτελεί την αποσύνθεση τού* $\mathbf{V}(F)$ *σε ανάγωγες συνιστώσες και ισχύει*

$$\mathbf{I}(\mathbf{V}(F)) = \langle F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa \rangle .$$

ΑΠΟΔΕΙΞΗ. Εξ αιτίας τού ότι κανένα $F_i$ δεν διαιρεί το $F_j$, για $i, j \in \{1, 2, ..., \kappa\}$, $i \neq j$, δεν ισχύει καμία εγκλειστική σχέση μεταξύ των $\mathbf{V}(F_1), \mathbf{V}(F_2), \ldots, \mathbf{V}(F_\kappa)$. Εξάλλου, καθένα των $\mathbf{V}(F_i)$, $i = 1, 2, ..., \kappa$, (σύμφωνα με την άσκηση **A-1-14**) είναι απειροπληθές, κι επομένως (από το πόρισμα 1.7.2) έχουμε:

$$\mathbf{I}(\mathbf{V}(F)) = \mathbf{I}(\bigcup_{i=1}^{\kappa} \mathbf{V}(F_i)) = \bigcap_{i=1}^{\kappa} \mathbf{I}(\mathbf{V}(F_i)) = \bigcap_{i=1}^{\kappa} \langle F_i \rangle .$$

Επειδή δε κάθε πολυώνυμο διαιρούμενο διά τού $F_i$ διαιρείται και διά τού γινομένου $F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa$, ισχύει η ισότητα $\bigcap_{i=1}^{\kappa} \langle F_i \rangle = \langle F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa \rangle$. □

## Ασκήσεις

**A-1-44**. Έστω $\mathbf{k} = \mathbb{R}$. Να αποδειχθεί ότι $\mathbf{I}(\mathbf{V}(\mathsf{Y}^2 + \mathsf{X}^2 + 1)) = \langle 1 \rangle \ (= \mathbb{R}[\mathsf{X}, \mathsf{Y}])$.

(Αυτό καθιστά σαφές το γιατί συνήθως απαιτούμε από το θεωρούμενο σώμα να είναι αλγεβρικώς κλειστό.)

**A-1-45**. (a) Να προσδιορισθούν οι ανάγωγες συνιστώσες τού $\mathbf{V}(\mathsf{Y}^2 - \mathsf{XY} - \mathsf{X}^2\mathsf{Y} + \mathsf{X}^3)$ τόσον εντός τού $\mathbb{A}^2_{\mathbb{R}}$ όσον και εντός τού $\mathbb{A}^2_{\mathbb{C}}$.

(b) Να γίνει το ίδιο για τα $\mathbf{V}(\mathsf{Y}^2 - \mathsf{X}(\mathsf{X}^2 - 1))$ και $\mathbf{V}(\mathsf{X}^3 + \mathsf{X} - \mathsf{X}^2\mathsf{Y} - \mathsf{Y})$.

## 1.8 Το Θεώρημα των Θέσεων Μηδενισμού τού Hilbert

Εάν μας δοθεί ένα αλγεβρικό σύνολο $V$ εντός τού $n$-διάστατου συσχετικού χώρου $\mathbb{A}^n_{\mathbf{k}}$, η πρόταση 1.6.7 μας παρέχει ένα κριτήριο για τη διαπίστωση τού κατά πόσον το $V$ είναι ανάγωγο ή όχι. Επί τού παρόντος, αυτό που λείπει είναι ένας τρόπος περιγραφής τού $V$ με τη βοήθεια τού δοθέντος συνόλου των πολυωνύμων, μέσω τού οποίου ορίζεται το $V$. Τα όσα ειπώθηκαν στην προηγούμενη ενότητα αποτελούν την αφετηρία για την αντιμετώπιση τού προκύπτοντος προβλήματος, αλλά είναι το «Θεώρημα των Μηδενικών Θέσεων» τού Hilbert εκείνο που τελικώς μας γνωστοποιεί την ακριβή σχέση μεταξύ των ιδεωδών και των αλγεβρικών συνόλων.

Θα ξεκινήσουμε με τη διατύπωση ενός ασθενέστερου θεωρήματος και θα δείξουμε το πώς η απόδειξή του ανάγεται σε μια καθαρώς αλγεβρική επιχειρηματολογία. Στο υπόλοιπο τής παρούσας ενότητας θα καταπιαστούμε με τη διαδικασία παραγωγής τού κυρίου αποτελέσματος από αυτό το ασθενές θεώρημα και θα παράσχουμε ορισμένες εφαρμογές.

**Στην παρούσα ενότητα το σώμα $\mathbf{k}$ θα είναι αλγεβρικώς κλειστό.**

**1.8.1 Θεώρημα. (Ασθενές Θεώρημα των Θέσεων Μηδενισμού)** *Εάν το $I$ είναι ένα γνήσιο ιδεώδες τού $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, τότε $\mathbf{V}(I) \neq \varnothing$.*

ΑΠΟΔΕΙΞΗ. Μπορούμε, δίχως βλάβη τής γενικότητας, να υποθέσουμε ότι το $I$ είναι ένα μεγιστοτικό ιδεώδες (κι αυτό, διότι εν γένει, σύμφωνα με την άσκηση **A-1-38**, υπάρχει ένα μεγιστοτικό ιδεώδες $J$, το οποίο περιέχει οιοδήποτε $I$, και για το οποίο ισχύει ο εγκλεισμός $\mathbf{V}(J) \subseteq \mathbf{V}(I)$). Επομένως, μπορεί να υποτεθεί ότι το $L = \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n] \,/\, I$ είναι ένα σώμα (βλ. θεώρημα 1.1.14), ενώ το $\mathbf{k}$ μπορεί να θεωρηθεί ως υπόσωμα τού $L$.

Προς στιγμήν, ας *υποθέσουμε νοερά*, ότι $\mathbf{k} = L$. Τότε για κάθε $i, 1 \leq i \leq n$, θα υπάρχει ένα στοιχείο $a_i \in \mathbf{k}$, τέτοιο ώστε η κλάση υπολοίπων τού $\mathsf{X}_i$ ως προς το το $I$ να είναι το $a_i + I$ ή, ισοδυνάμως, να έχουμε $\mathsf{X}_i - a_i \in I$. Συνεπώς, σύμφωνα με την άσκηση **A-1-21**, το ιδεώδες $\langle \mathsf{X}_1 - a_1, \dots, \mathsf{X}_n - a_n \rangle$ είναι ένα μεγιστοτικό ιδεώδες, οπότε θα ισχύει $I = \langle \mathsf{X}_1 - a_1, \dots, \mathsf{X}_n - a_n \rangle$ και $\mathbf{V}(I) = \{(a_1, \dots, a_n)\} \neq \varnothing$. □

Ως εκ τούτου, έχουμε αναγάγει την αποπεράτωση τής όλης αποδείξεως στο έλεγχο τής αληθείας τού ακολούθου ισχυρισμού:

$\boxed{*}$ *Εάν ένα αλγεβρικώς κλειστό σώμα $\mathbf{k}$ αποτελεί υπόσωμα ενός σώματος $L$ και εάν υπάρχει ένας επιμορφισμός δακτυλίων από τον $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ επί τού $L$ (ο οποίος, περιοριζόμενος στο $\mathbf{k}$, είναι η ταυτοτική απεικόνιση), τότε $\mathbf{k} = L$.*

Οι αλγεβρικές έννοιες, οι οποίες απαιτούνται για τη διαπίστωση τής ισχύος ενός τέτοιου συμπεράσματος, θα μελετηθούν στις ενότητες 1.9 και 1.10, ενώ ο ισχυρισμός $\boxed{*}$ θα αποδειχθεί στην ενότητα 1.11.

**1.8.2 Θεώρημα. (Θεώρημα Θέσεων Μηδενισμού τού Hilbert)** *Έστω $I$ ένα ιδεώδες τού* $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$. *Τότε έχουμε*

$$\boxed{\mathbf{I}(\mathbf{V}(I)) = \mathrm{Rad}(I).}$$

*Συγκεκριμένα, τούτο σημαίνει ότι εάν $F_1, F_2, \dots, F_m, G \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ και εάν το $G$ μηδενίζεται οποτεδήποτε μηδενίζονται τα $F_1, F_2, \dots, F_m$, τότε υπάρχουν πολυώνυμα $A_1, A_2, \dots, A_m \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ και ένας θετικός ακέραιος αριθμός $\nu$, ούτως ώστε να ισχύει η εξίσωση*:

$$\boxed{G^\nu = A_1 \cdot F_1 + A_2 \cdot F_2 + \cdots + A_m \cdot F_m.}$$

ΑΠΟΔΕΙΞΗ. Κατά την άσκηση **A-1-20**, $\mathrm{Rad}(I) \subseteq \mathbf{I}(\mathbf{V}(I))$. Θα αποδείξουμε ότι ισχύει και η αντίστροφη εγκλειστική σχέση $\mathbf{I}(\mathbf{V}(I)) \subseteq \mathrm{Rad}(I)$. Έστω λοιπόν ένα $G \in \mathbf{I}(\mathbf{V}(I))$. Σύμφωνα με το πόρισμα 1.5.7 υπάρχουν

$$F_1, F_2, \dots, F_m \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n] : I = \langle F_1, F_2, \dots, F_m \rangle \Longrightarrow G \in \mathbf{I}(\mathbf{V}(\langle F_1, F_2, \dots, F_m \rangle)).$$

Ορίζουμε το ιδεώδες:

$$J := \langle F_1, F_2, \dots, F_m, \mathsf{X}_{n+1} G - 1 \rangle \subseteq \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n, \mathsf{X}_{n+1}].$$

Το $\mathbf{V}(J)$ είναι κενό, διότι το $G$ μηδενίζεται εκεί ακριβώς όπου μηδενίζονται και τα $F_1, \dots, F_m$. (Πράγματι· εάν $(a_1, \dots, a_n, a_{n+1}) \in \mathbb{A}^{n+1}_{\mathbf{k}}$, τότε το σημείο $(a_1, \dots, a_n)$ ή ανήκει ή δεν ανήκει στο $\mathbf{V}(\langle F_1, \dots, F_m \rangle)$. Στην πρώτη περίπτωση, εξ ορισμού $G(a_1, \dots, a_n) = 0$. Επομένως το πολυώνυμο $\mathsf{X}_{n+1} G - 1$, στο σημείο $(a_1, \dots, a_n, a_{n+1})$, λαμβάνει την τιμή

$$a_{n+1} G(a_1, \dots, a_n) - 1 = 1 \neq 0 \Longrightarrow (a_1, \dots, a_n, a_{n+1}) \notin \mathbf{V}(J).$$

Στη δεύτερη περίπτωση, για κάποιον δείκτη $i \in \{1, 2, ..., m\}$, $F_i(a_1, \dots, a_n) \neq 0$. Εκλαμβάνοντας το $F_i$ ως συνάρτηση $\mathbb{A}^{n+1}_{\mathbf{k}} \longrightarrow \mathbf{k}$ *μη εξαρτώμενη* από την τελευταία μεταβλητή, έχουμε

$$F_i(a_1, \dots, a_n, a_{n+1}) \neq 0 \Longrightarrow (a_1, \dots, a_n, a_{n+1}) \notin \mathbf{V}(J),$$

Άρα $\mathbf{V}(J) = \varnothing$). Εν συνεχεία, εφαρμόζοντας το ασθενές θεώρημα των θέσεων μηδενισμού 1.8.1 για το $J$ λαμβάνουμε

$$J = \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n, \mathsf{X}_{n+1}] = \langle 1 \rangle \Longrightarrow 1 \in J.$$

Επομένως υπάρχουν

$$B, B_1, B_2, \dots, B_m \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n, \mathsf{X}_{n+1}] : \sum_{i=1}^{m} B_i \cdot F_i + B \cdot (\mathsf{X}_{n+1} G - 1) = 1. \quad (1.11)$$

Έστω

$$\varphi : \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n, \mathsf{X}_{n+1}] \longrightarrow \mathbf{k}(\mathsf{X}_1, \dots, \mathsf{X}_n)$$

ο ομομορφισμός δακτυλίων ο καθοριζόμενος μέσω των συνθηκών

$$\varphi(\lambda) := \lambda,\ \forall \lambda \in \mathbf{k},\ \ \varphi(\mathsf{X}_i) := \mathsf{X}_i,\ \forall i \in \{1, ..., n\},\ \ \varphi(\mathsf{X}_{n+1}) := \frac{1}{G}.$$

Εφαρμόζοντας τον $\varphi$ σε αμφότερα τα μέλη τής (1.11) καταλήγουμε στην

$$\sum_{i=1}^{m} B_i \left( \mathsf{X}_1, \dots, \mathsf{X}_n, \frac{1}{G} \right) \cdot F_i = 1. \tag{1.12}$$

Έστω $\nu$ ένας μη αρνητικός ακέραιος $\geq$ *τού μεγίστου* των βαθμών των $B_1, B_2, \dots, B_m$ θεωρουμένων ως πολυωνύμων τής (μίας) μεταβλητής $\mathsf{X}_{n+1}$ και με συντελεστές ειλημμένους από τον $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$. Πολλαπλασιάζοντας αμφότερα τα μέλη τής (1.12) με $G^\nu$ λαμβάνουμε

$$G^\nu = \sum_{i=1}^{m} A_i \cdot F_i. \qquad \left( A_i := G^\nu \cdot B_i \left( \mathsf{X}_1, \dots, \mathsf{X}_n, \frac{1}{G} \right) \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n],\ \forall i \in \{1, ..., m\}. \right)$$

Άρα τελικώς $G^\nu \in \langle F_1, F_2, \dots, F_m \rangle = I$. □

Η ως άνω απόδειξη οφείλεται στον S. Rabinowitsch (1929). Ως άμεσα επακόλουθα τού θεωρήματος 1.8.2 φέρονται τα εξής πορίσματα:

**1.8.3 Πόρισμα.** *Εάν το $I$ είναι ένα ριζικό ιδεώδες τού $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, τότε*

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

*Συνεπώς υπάρχει μια αμφίρριψη*

$$\boxed{\{\text{ριζικά ιδεώδη τού } \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]\} \underset{\mathbf{I}}{\overset{\mathbf{V}}{\rightleftarrows}} \left\{ \begin{array}{c} \text{αλγεβρικά σύνολα} \\ \text{εντός τού } \mathbb{A}^n_{\mathbf{k}} \end{array} \right\}}$$

*η οποία αναστρέφει τις σχέσεις εγκλεισμού, που σημαίνει ότι*:

$$[I_1 \subseteq I_2 \Longrightarrow \mathbf{V}(I_1) \supseteq \mathbf{V}(I_2)], \qquad [V_1 \subseteq V_2 \Longrightarrow \mathbf{I}(V_1) \supseteq \mathbf{I}(V_2)].$$

ΑΠΟΔΕΙΞΗ. Το ότι οι σχέσεις εγκλεισμού αντιστρέφονται, μας είναι γνωστό. (Βλ. προτάσεις 1.2.3 (3) και 1.3.1 (1)). Εάν αποδείξουμε, ότι για κάθε αλγεβρικό σύνολο $V$ εντός τού $\mathbb{A}^n_{\mathbf{k}}$ ισχύει $\mathbf{V}(\mathbf{I}(V)) = V$, τότε η "$\mathbf{I}$" (ιδωμένη ως απεικόνιση από το σύνολο των αλγεβρικών υποσυνόλων τού $\mathbb{A}^n_{\mathbf{k}}$ στο σύνολο των ιδεωδών τού $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$) θα είναι ενριπτική και θα διαθέτει εξ αριστερών αντίστροφο. Ας υποθέσουμε ότι $V = \mathbf{V}(F_1, \dots, F_\kappa)$.

Ως γνωστόν (βλ. πρόταση 1.3.1 (3)), $V \subseteq \mathbf{V}(\mathbf{I}(V))$. Από την άλλη μεριά, εξ ορισμού, $F_1, \ldots, F_\kappa \in \mathbf{I}(V)$. Επομένως,

$$\langle F_1, \ldots, F_\kappa \rangle \subseteq \mathbf{I}(V) \Longrightarrow \mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}\left(F_1, \ldots, F_\kappa\right) = V.$$

Επειδή τώρα το $\mathbf{I}(V)$, κατά την πρόταση 1.3.3, είναι ριζικό, μπορούμε να εκλάβουμε την "$\mathbf{I}$" ως μια απεικόνιση από το σύνολο των αλγεβρικών συνόλων εντός τού $\mathbb{A}^n_{\mathbf{k}}$ στο σύνολο των ριζικών ιδεωδών τού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Υπό αυτήν την προϋπόθεση, και δεδομένου ότι, αφ' ενός μεν $\mathbf{V}(\mathbf{I}(V)) = V$ για κάθε αλγεβρικό σύνολο $V$ εντός τού $\mathbb{A}^n_{\mathbf{k}}$, αφ' ετέρου δε $\mathbf{I}(\mathbf{V}(I)) = \mathrm{Rad}(I) = I$, συνάγουμε ότι οι "$\mathbf{I}$" και "$\mathbf{V}$" είναι αμοιβαίως αντίστροφες απεικονίσεις, κι ότι γι' αυτόν τον λόγο επάγουν αμφιρρίψεις μεταξύ των προκειμένων συνόλων. □

**1.8.4 Πόρισμα.** *Εάν το $I$ είναι ένα πρώτο ιδεώδες τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, τότε το $\mathbf{V}(I)$ είναι ανάγωγο. Επομένως υπάρχουν αμφιρρίψεις*:

| | | |
|---|---|---|
| $\{$πρώτα ιδεώδη τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]\}$ | $\longleftrightarrow$ | $\left\{ \begin{array}{c} \text{ανάγωγα αλγεβρικά} \\ \text{σύνολα εντός τού } \mathbb{A}^n_{\mathbf{k}} \end{array} \right\}$ |
| $\cup$ | | $\cup$ |
| $\{$μεγιστοτικά ιδεώδη τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]\}$ | $\longleftrightarrow$ | $\{$σημεία τού $\mathbb{A}^n_{\mathbf{k}}\}$ |

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. Ο πρώτος ισχυρισμός είναι προφανής επί τη βάσει τού θεωρήματος 1.8.2 και τής προτάσεως 1.6.7. Εξάλλου, κάθε πρώτο ιδεώδες είναι ριζικό (βλ. άσκηση **A-1-18**). Επομένως, η πρώτη εξ αυτών των αμφιρρίψεων αποτελεί τον περιορισμό τής αμφιρρίψεως που κατασκευάσθηκε στο προηγηθέν πόρισμα 1.8.3, λαμβανομένου, βεβαίως, υπ' όψιν τού ότι το $\mathbf{I}(V)$ είναι πρώτο εάν και μόνον εάν το $V$ είναι ανάγωγο (βλ. πρόταση 1.6.7).

**Βήμα 2ο**. Κατ' αρχάς θα δείξουμε (πρβλ. άσκηση **A-1-21**) ότι κάθε ιδεώδες $I$ τού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$, το οποίο γράφεται ως $\langle \mathsf{X}_1 - a_1, \ldots, \mathsf{X}_n - a_n \rangle$, όπου $a_1, \ldots, a_n \in \mathbf{k}$, είναι μεγιστοτικό. (Τούτο ισχύει ακόμη και όταν το $\mathbf{k}$ δεν είναι κατ' ανάγκην αλγεβρικώς κλειστό σώμα). Πράγματι· εάν ορίσουμε τον ομομορφισμό δακτυλίων

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

παρατηρούμε πως ο $\varphi_{(a_1,\ldots,a_n)}$ είναι επιμορφισμός. (Για κάθε $\lambda \in \mathbf{k}$, υπάρχει ένα πολυώνυμο $F_\lambda\left(\mathsf{X}_1, \ldots, \mathsf{X}_n\right) := \sum_{i=1}^n \left(\mathsf{X}_i - a_i\right) - \lambda$, για το οποίο $\varphi_{(a_1,\ldots,a_n)}\left(F_\lambda\right) = \lambda$). Χρησιμοποιώντας το 1ο θεώρημα ισομορφισμών δακτυλίων 1.1.10 σχηματίζουμε έναν ισομορφισμό

$$\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \,/\, \mathrm{Ker}(\varphi_{(a_1,\ldots,a_n)}) \cong \mathbf{k}.$$

Αρκεί να δειχθεί ότι ισχύει $\mathrm{Ker}(\varphi_{(a_1,\dots,a_n)}) = \langle \mathsf{X}_1 - a_1, \dots, \mathsf{X}_n - a_n \rangle$ (διότι ο ως άνω 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**.

**Βήμα 3ο**. Εν συνεχεία, θα δείξουμε ότι *κάθε* μεγιστοτικό ιδεώδες $I$ τού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ είναι τής μορφής $\langle \mathsf{X}_1 - a_1, \dots, \mathsf{X}_n - a_n \rangle$, όπου $a_1, \dots, a_n \in \mathbf{k}$. (Τούτο ισχύει *μόνον* υπό την προϋπόθεση ότι το $\mathbf{k}$ είναι αλγεβρικώς κλειστό σώμα). Έστω λοιπόν $I$ ένα μεγιστοτικό ιδεώδες τού $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$. Τότε $I \subsetneqq \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$, οπότε $\mathbf{V}(I) \neq \varnothing$ βάσει τού θεωρήματος 1.8.1. Έστω $(a_1, \dots, a_n)$ ένα σημείο τού $\mathbf{V}(I)$. Προφανώς,

$$\mathrm{Rad}\,(I) = I = \mathbf{I}(\mathbf{V}(I)) \subseteq \mathbf{I}(\{(a_1, \dots, a_n)\}) = \langle \mathsf{X}_1 - a_1, \dots, \mathsf{X}_n - a_n \rangle \subsetneqq \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n],$$

που σημαίνει ότι $I = \langle \mathsf{X}_1 - a_1, \dots, \mathsf{X}_n - a_n \rangle$, διότι το $I$ είναι μεγιστοτικό. Επομένως, η

$$\mathbb{A}^n_{\mathbf{k}} \ni (a_1, \dots, a_n) \longmapsto \langle \mathsf{X}_1 - a_1, \dots, \mathsf{X}_n - a_n \rangle \in \{\text{μεγιστοτικά ιδεώδη τού } \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]\}$$

αποτελεί την επιθυμητή αμφίρριψή μας. □

**1.8.5 Πόρισμα.** *Έστω $F \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ και έστω $F = F_1^{n_1} \cdot F_2^{n_2} \cdot \cdots \cdot F_\kappa^{n_\kappa}$ η αποσύνθεση τού $F$ σε σαφώς διακεκριμένους ανάγωγους παράγοντες (υψωμένους σε κατάλληλες δυνάμεις). Τότε η*

$$\mathbf{V}(F) = \mathbf{V}(F_1) \cup \mathbf{V}(F_2) \cup \cdots \cup \mathbf{V}(F_\kappa)$$

*αποτελεί την αποσύνθεση τού $\mathbf{V}(F)$ σε ανάγωγες συνιστώσες και ισχύει*

$$\mathbf{I}(\mathbf{V}(F)) = \langle F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa \rangle .$$

ΑΠΟΔΕΙΞΗ. Εξ αιτίας τού ότι κανένα $F_i$ δεν διαιρεί το $F_j$, για $i, j \in \{1, 2, ..., \kappa\}$, $i \neq j$, δεν ισχύει καμία εγκλειστική σχέση μεταξύ των $\mathbf{V}(F_1), \mathbf{V}(F_2), \dots, \mathbf{V}(F_\kappa)$. Συνεπώς ο πρώτος ισχυρισμός είναι προφανής. Κι επειδή $\mathbf{I}(\mathbf{V}(F)) = \mathrm{Rad}(\langle F \rangle)$, αρκεί να αποδείξουμε ότι

$$\langle F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa \rangle = \mathrm{Rad}\,(\langle F \rangle) .$$

Έστω $\nu$ οιοσδήποτε ακέραιος αριθμός με την ιδιότητα

$$\nu > \max\{n_1, \dots, n_\kappa\} .$$

Τότε η δύναμη

$$(F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa)^\nu = F_1^{\nu - n_1} F_2^{\nu - n_2} \cdot \cdots \cdot F_\kappa^{\nu - n_\kappa} \cdot F$$

τού $F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa$ παρουσιάζεται ως ένα πολλαπλάσιο τού $F$. Αυτό σημαίνει ότι

$$F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa \in \mathrm{Rad}\left(\langle F\rangle\right) \Longrightarrow \langle F_1 \cdot F_2 \cdot \cdots \cdot F_\kappa\rangle \subseteq \mathrm{Rad}\left(\langle F\rangle\right).$$

Για τη απόδειξη τής αντίστροφης εγκλειστικής σχέσεως θεωρούμε ένα $G \in \mathrm{Rad}(\langle F\rangle)$. Τότε υπάρχει ένας θετικός ακέραιος $m$, τέτοιος ώστε να ισχύει $G^m \in \langle F\rangle$. Επομένως το $G^m$ γράφεται υπό τη μορφή $G^m = H \cdot F$, για κάποιο $H \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Ας υποθέσουμε ότι η

$$G = G_1^{\lambda_1} \cdot G_2^{\lambda_2} \cdot \cdots \cdot G_s^{\lambda_s}$$

είναι η αποσύνθεση τού $G$ ως γινομένου σαφώς διακεκριμένων αναγώγων πολυωνύμων, υψωμένων σε κατάλληλες δυνάμεις $\geq 1$. Τότε ισχύει

$$G_1^{\lambda_1 m} \cdot G_2^{\lambda_2 m} \cdot \cdots \cdot G_s^{\lambda_s m} = H \cdot F_1^{n_1} \cdot F_2^{n_2} \cdot \cdots \cdot F_\kappa^{n_\kappa}. \tag{1.13}$$

Όμως, επειδή ο δακτύλιος $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ είναι μια Π.Μ.Π., τα ανάγωγα πολυώνυμα τού πρώτου και τού δευτέρου μέλους τής (1.13) οφείλουν να είναι ίσα μεταξύ τους (τουλάχιστον ύστερα από ενδεχόμενη αναδιάταξη δεικτών και «μέχρις πολλαπλασιασμού» με κάποια σταθερά μη μηδενικά πολυώνυμα, ήτοι με κάποια στοιχεία τού $\mathbf{k}\setminus\{0_\mathbf{k}\}$). Κι επειδή τα $F_1, \ldots, F_\kappa$ είναι ανάγωγα, κάθε $F_i, 1 \leq i \leq \kappa \leq s$, οφείλει να είναι τής μορφής $F_i = c_i \cdot G_{j(i)}$ για κάποιον $j(i) \in \{1, \ldots, s\}$ και για κάποια σταθερά $c_i \in \mathbf{k}\setminus\{0_\mathbf{k}\}$. Κατά συνέπειαν, το

$$G = G_1^{\lambda_1} \cdot G_2^{\lambda_2} \cdot \cdots \cdot G_s^{\lambda_s} = \left(\prod_{j(i)\in\{1,\ldots,s\}} c_i^{-1} F_i^{\lambda_{j(i)}-1}\right) \cdot F_1 \cdots F_\kappa$$

είναι ένα (πολυωνυμικό) πολλαπλάσιο τού $F_1 \cdots F_\kappa$, οπότε $\mathrm{Rad}(\langle F\rangle) \subseteq \langle F_1 \cdots F_\kappa\rangle$.□

Για την παράθεση μιας αρκετά «κατασκευαστικής» αποδείξεως για το επόμενο πόρισμα, θα χρειασθούμε ένα λήμμα από τη θεωρία των βάσεων Gröbner, παρότι δεν θα υπεισέλθουμε σε λεπτομέρειές της.

**1.8.6 Ορισμός.** Έστω $F = \sum \lambda_{(\boldsymbol{\kappa})} \mathsf{X}_1^{\kappa_1} \cdots \mathsf{X}_n^{\kappa_n} \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ ένα μη μηδενικό πολυώνυμο. Εφοδιάζουμε τον δακτύλιο $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ με μια μονωνυμιακή διάταξη «$\prec$» (π.χ. με τη λεξικογραφική διάταξη[10]). Ορίζουμε ως $\prec$-**βαθμό** $\deg_\prec(F)$ τού $F$ τον αριθμό

$$\deg_\prec(F) := \max\{\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_n) \in \mathbb{N}_0^n \mid \lambda_{(\boldsymbol{\kappa})} \neq 0\}.$$

[10] $[\mathsf{X}_1^{\kappa_1} \cdots \mathsf{X}_n^{\kappa_n} \succ_{\text{lex}} \mathsf{X}_1^{\kappa'_1} \cdots \mathsf{X}_n^{\kappa'_n}] \underset{\text{ορσ}}{\Longleftrightarrow} [\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_n) \succ_{\text{lex}} \boldsymbol{\kappa}' = (\kappa'_1, \ldots, \kappa'_n)] \underset{\text{ορσ}}{\Longleftrightarrow}$ η πρώτη (εξ αριστερών εμφανιζόμενη) *μη μηδενική* συντεταγμένη τού διανύσματος διαφοράς $\boldsymbol{\kappa} - \boldsymbol{\kappa}' \in \mathbb{Z}^n$ είναι θετική. Π.χ., $(1,2,0) \succ_{\text{lex}} (0,3,5)$ και $(3,7,6) \succ_{\text{lex}} (3,7,2)$.

(Το max λαμβάνεται ως προς την «$\prec$»). Ο **επικεφαλής συντελεστής** (leading coefficient) $\mathbf{LC}_{\prec}(F)$ τού $F$ **ως προς την** «$\prec$» είναι ο $\mathbf{LC}_{\prec}(F) := \lambda_{(\deg_{\prec}(F))}$ και το **επικεφαλής μονώνυμο** (leading monomial) $\mathbf{LM}_{\prec}(F)$ τού $F$ το $\mathbf{LM}_{\prec}(F) := \mathsf{X}^{\deg_{\prec}(F)}$. Ορίζουμε τον **επικεφαλής όρο** (leading term) τού $F$:

$$\mathbf{LT}_{\prec}(F) := \mathbf{LC}_{\prec}(F) \cdot \mathbf{LM}_{\prec}(F).$$

**1.8.7 Λήμμα.** *Έστω $I$ ένα ιδεώδες τού πολυωνυμικού δακτυλίου $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$. Τότε ο πηλικοδακτύλιος $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n] \,/\, I$, ως $\mathbf{k}$-διανυσματικός χώρος, είναι ισόμορφος με τον*

$$\mathbf{Span}_{\mathbf{k}}\left(\text{μονώνυμα } \mathsf{X}_1^{\kappa_1} \cdots \mathsf{X}_n^{\kappa_n} \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n] \;\middle|\; \mathsf{X}_1^{\kappa_1} \cdots \mathsf{X}_n^{\kappa_n} \notin \langle \mathbf{LT}_{\prec}(I) \rangle \right),$$

*όπου*

$$\mathbf{LT}_{\prec}(I) := \{ c \cdot \mathsf{X}_1^{\kappa_1} \cdots \mathsf{X}_n^{\kappa_n} \in \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n] \;|\; \exists F \in I : \mathbf{LT}_{\prec}(F) = c \cdot \mathsf{X}_1^{\kappa_1} \cdots \mathsf{X}_n^{\kappa_n},\ c \in \mathbf{k} \}.$$

ΑΠΟΔΕΙΞΗ. Βλέπε π.χ. W.W. Adams, P. Loustaunau: *An Introduction to Gröbner Bases*, Graduate Studies in Math., Vol. **3**, Amer. Math. Soc., 1994, Prop. 2.1.6. □

**1.8.8 Πόρισμα.** *Έστω $I$ ένα ιδεώδες τού $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$. Το $\mathbf{V}(I)$ είναι ένα πεπερασμένο σύνολο εάν και μόνον εάν ο δακτύλιος πηλίκων $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n] \,/\, I$ είναι ένας διανυσματικός χώρος πεπερασμένης διαστάσεως υπεράνω τού $\mathbf{k}$. Εάν μάλιστα κάτι τέτοιο συμβαίνει, τότε*

$$\boxed{|\mathbf{V}(I)| \leq \dim_{\mathbf{k}} \left(\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n] \,/\, I\right).} \tag{1.14}$$

*Ιδιαιτέρως, όταν το $\mathbf{V}(I)$ είναι ένα πεπερασμένο σημειοσύνολο και το $I$ ένα ριζικό ιδεώδες, η σχέση* (1.14) *ισχύει ως ισότητα.*

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. Εάν το $\mathbf{V}(I) = \{P_1, P_2, \dots, P_m\}$ είναι πεπερασμένο, όπου

$$P_i = (a_{i1}, a_{i2}, \dots, a_{in}),\ \forall i,\ i \in \{1, 2, \dots, m\},$$

ορίζουμε τα πολυώνυμα

$$F_j := \prod_{i=1}^{m} (\mathsf{X}_j - a_{ij}) \in \mathbf{k}[\mathsf{X}_j] \hookrightarrow \mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n],\ \forall j,\ \ j \in \{1, 2, \dots, n\}.$$

Επειδή $F_j \in \mathbf{I}(\mathbf{V}(I))$, κατά το θεώρημα 1.8.2 υπάρχει ένας θετικός ακέραιος αριθμός $\nu_j$, τέτοιος ώστε $F_j^{\nu_j} \in I$. Εφοδιάζοντας τον δακτύλιο $\mathbf{k}[\mathsf{X}_1, \dots, \mathsf{X}_n]$ με μια μονωνυμιακή διάταξη «$\prec$», διαπιστώνουμε ότι

$$F_j^{\nu_j} \in I \Longrightarrow \mathsf{X}_j^{\nu_j\, m} \in \langle \mathbf{LT}_{\prec}(I) \rangle.$$

Επομένως, όλα τα μονώνυμα $\mathsf{X}_1^{\kappa_1}\cdots\mathsf{X}_n^{\kappa_n}$, για τα οποία κάποια $\kappa_j$ είναι $\geq \nu_j\, m$, ανήκουν στο ιδεώδες $\langle \mathbf{LT}_{\prec}(I)\rangle$. Άρα τα μονώνυμα τού υποχώρου

$$\mathbf{Span_k}\left(\, \mathsf{X}_1^{\kappa_1}\cdots\mathsf{X}_n^{\kappa_n} \in \mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n] \;\middle|\; \mathsf{X}_1^{\kappa_1}\cdots\mathsf{X}_n^{\kappa_n} \notin \langle \mathbf{LT}_{\prec}(I)\rangle \,\right)$$

τού $\mathbf{k}$-διανυσματικού χώρου $\mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n]$ οφείλουν να έχουν εκθέτες $\kappa_j \leq \nu_j\, m-1$, *για κάθε* $j\in\{1,2,\ldots,n\}$, οπότε, βάσει τού λήμματος 1.8.7,

$$\begin{aligned}&\dim_{\mathbf{k}}\left(\mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n]\,/\,I\right)\\ &=\dim_{\mathbf{k}}\mathbf{Span}\left(\, \mathsf{X}_1^{\kappa_1}\cdots\mathsf{X}_n^{\kappa_n} \in \mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n] \;\middle|\; \mathsf{X}_1^{\kappa_1}\cdots\mathsf{X}_n^{\kappa_n} \notin \langle \mathbf{LT}_{\prec}(I)\rangle \,\right) \leq \prod_{j=1}^{n}\nu_j\, m.\end{aligned}$$

**Βήμα 2ο**. Για να αποδείξουμε ότι το $\mathbf{V}(I)$ είναι ένα πεπερασμένο σημειοσύνολο, υπό την προϋπόθεση ότι ο πηλικοδακτύλιος $\mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n]\,/\,I$ είναι ένας διανυσματικός χώρος πεπερασμένης διαστάσεως υπεράνω τού $\mathbf{k}$, αρκεί να δείξουμε ότι για κάθε $i, 1\leq i\leq n$, μπορούν να εμφανισθούν μόνον πεπερασμένες δυνατότητες για την επιλογή των τιμών τής $i$-οστής συντεταγμένης των σημείων τού $\mathbf{V}(I)$. Ας παγιώσουμε, από εδώ και στο εξής, ένα $i$, κι ας θεωρήσουμε τις κλάσεις υπολοίπων $\overline{\mathsf{X}}_i^j := \mathsf{X}_i^j + I \in \mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n]\,/\,I$, όπου $j=0,1,2,\ldots$ Επειδή $\dim_{\mathbf{k}}\left(\mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n]\,/\,I\right)<\infty$, το σύνολο αυτών των κλάσεων υπολοίπων ως προς $I$ οφείλει να είναι γραμμικώς εξαρτημένο. Επομένως υπάρχουν σταθερά στοιχεία (όχι όλα μηδενικά) $c_j$ τού $\mathbf{k}$, καθώς και ένας μη αρνητικός ακέραιος $m$, ούτως ώστε να ισχύει

$$\sum_{j=0}^{m} c_j\overline{\mathsf{X}}_i^j = \overline{\sum_{j=0}^{m} c_j\mathsf{X}_i^j} = \overline{0} \Longrightarrow \sum_{j=0}^{m} c_j\mathsf{X}_i^j \in I.$$

Επειδή το $\mathbf{k}$ είναι αλγεβρικώς κλειστό, κάθε μη μηδενικό πολυώνυμο μιας μεταβλητής (με συντελεστές από το $\mathbf{k}$) διαθέτει το πολύ πεπερασμένου πλήθους σημεία μηδενισμού (από το $\mathbf{k}$), οπότε οι $i$-οστές συντεταγμένες των σημείων τού $\mathbf{V}(I)$ μπορούν να λάβουν μόνον πεπερασμένου πλήθους τιμές.

**Βήμα 3ο**. Έστω $\mathbf{V}(I)=\{P_1,P_2,\ldots,P_m\}$ ένα πεπερασμένο σημειοσύνολο πληθικότητας ίσης με $m$. Επιλέγουμε πολυώνυμα

$$F_1,F_2,\ldots,F_m\in\mathbf{k}[\mathsf{X}_1,\ldots,\mathsf{X}_n]: \left[\,\forall i,j\in\{1,2,\ldots,m\}\Longrightarrow F_i\left(P_j\right)=\begin{cases}0_{\mathbf{k}}, & i\neq j\\ 1_{\mathbf{k}}, & i=j\end{cases}\,\right]$$

(η ύπαρξη των οποίων είναι διασφαλισμένη από την άσκηση **A-1-17**). Εν συνεχεία, συμβολίζουμε ως $\overline{F}_i$ την κλάση υπολοίπων τού $F_i$ ως προς το $I$. Εάν ισχύει

$$\sum_{i=1}^{m}\lambda_i\overline{F}_i=\overline{0},\ \text{ για κάποια (όχι όλα μηδενικά) } \lambda_1,\lambda_2,\ldots,\lambda_m\in\mathbf{k},$$

τότε (από την κατασκευή των $F_1,F_2,\ldots,F_m$):

$$\sum_{i=1}^{m}\lambda_iF_i\in I\Longrightarrow\lambda_j=\left(\sum_{i=1}^{m}\lambda_iF_i\right)(P_j)=0_{\mathbf{k}},\ \forall j\in\{1,\ldots,m\}.$$

Συνεπώς το σύνολο $\left\{\overline{F}_1, \overline{F}_2, \ldots, \overline{F}_m\right\}$ είναι γραμμικώς ανεξάρτητο υπεράνω τού $\mathbf{k}$ και ισχύει

$$m \leq \dim_{\mathbf{k}} \left(\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \,/\, I\right).$$

**Βήμα 4ο**. Εάν το $\mathbf{V}(I) = \{P_1, P_2, \ldots, P_m\}$ είναι ένα πεπερασμένο σημειοσύνολο πληθικότητας ίσης με $m$ και το $I$ ένα ριζικό ιδεώδες, τότε, προκειμένου να αποδειχθεί ότι η (1.14) ισχύει ως ισότητα, αρκεί να δείξουμε ότι το σύνολο $\left\{\overline{F}_1, \overline{F}_2, \ldots, \overline{F}_m\right\}$, το οποίο κατασκευάσθηκε στο 3ο βήμα, παράγει τον $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \,/\, I$ ως $\mathbf{k}$-διανυσματικό χώρο. Έστω λοιπόν ένα στοιχείο

$$\overline{G} \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \,/\, I.$$

Ορίζουμε το πολυώνυμο

$$H := G - \sum_{i=1}^{m} G\left(P_i\right) \overline{F}_i.$$

Επειδή ισχύει $H\left(P_i\right) = 0_{\mathbf{k}},\ \forall i \in \{1, \ldots, m\}$, έχουμε $H \in \mathbf{I}(\mathbf{V}(I))$. Σύμφωνα με το θεώρημα 1.8.2, $\mathbf{I}(\mathbf{V}(I)) = \mathrm{Rad}(I) = I$, οπότε $H \in I$. Συνεπώς,

$$\overline{H} = \overline{0} \in \mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n] \,/\, I \Longrightarrow \overline{G} = \sum_{i=1}^{m} G\left(P_i\right) \overline{F}_i,$$

πράγμα που αποπερατώνει την απόδειξή μας. □

## Ασκήσεις

**Α-1-46.** Να αποδειχθεί ότι τα θεωρήματα 1.8.1 και 1.8.2, καθώς και όλα τα παρατεθέντα πορίσματά τους είναι εν γένει λανθασμένα όταν το $\mathbf{k}$ *δεν* είναι αλγεβρικώς κλειστό.

**Α-1-47**. (a) Να αποσυντεθεί το $\mathbf{V}(\mathsf{X}^2+\mathsf{Y}^2-1, \mathsf{X}^2-\mathsf{Z}^2-1) \subset \mathbb{A}^3_{\mathbb{C}}$ σε ανάγωγες συνιστώσες.

(b) Έστω $V := \left\{\left(t, t^2, t^3\right) \in \mathbb{A}^3_{\mathbf{k}} \mid t \in \mathbf{k}\right\}$ ($\mathbf{k}$ αλγεβρικώς κλειστό). Να προσδιορισθεί το ιδεώδες $\mathbf{I}\left(V\right)$ και να αποδειχθεί ότι το $V$ είναι ανάγωγο.

**Α-1-48**. Έστω $R$ μια Π.Μ.Π.

(a) Να αποδειχθεί ότι ένα μονικό πολυώνυμο βαθμού 2 ή 3, ανήκον στον $R[\mathsf{X}]$, είναι ανάγωγο εάν και μόνον εάν δεν διαθέτει κανένα σημείο μηδενισμού εντός τής $R$.

(b) Το $\mathsf{X}^2 - a \in R[\mathsf{X}]$ είναι ανάγωγο $\Longleftrightarrow$ το $a$ δεν είναι τετραγωνική ρίζα ($\in R$).

**Α-1-49**. Να αποδειχθεί ότι το $\mathbf{V}(\mathsf{Y}^2-\mathsf{X}(\mathsf{X}-1_{\mathbf{k}})(\mathsf{X}-\lambda)) \subset \mathbb{A}^2_{\mathbf{k}}$ (όπου $\mathbf{k}$ αλγεβρικώς κλειστό σώμα) αποτελεί μια ανάγωγη συσχετική επίπεδη καμπύλη για κάθε $\lambda \in \mathbf{k}$.

**A-1-50**. Έστω $\mathbf{k}$ ένα σώμα και έστω $F \in \mathbf{k}[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geq 1$. Να αποδειχθεί ότι 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 $\mathbf{k}$.

**A-1-51**. Έστω

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

Να προσδιορισθεί το $\mathbf{V}(I)$ και να υπολογισθεί η διάσταση

$$\dim_{\mathbb{C}} \left(\mathbb{C}[\mathsf{X}, \mathsf{Y}] \,/\, I\right).$$

**A-1-52**. Έστω $\mathbf{k}$ ένα αλγεβρικώς κλειστό σώμα και έστω $I$ ένα ριζικό ιδεώδες $I$ τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$. Να αποδειχθεί ότι το $I$ μπορεί να γραφεί ως τομή των μελών μιας οικογενείας πεπερασμένου πλήθους πρώτων ιδεωδών τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$.

**A-1-53**. (a) Έστω $R$ μια Π.Μ.Π. και έστω $\mathfrak{p} = \langle t\rangle$, $t \in R$, ένα κύριο, γνήσιο, πρώτο ιδεώδες. Να αποδειχθεί ότι δεν υπάρχει κανένα τέτοιο πρώτο ιδεώδες $\mathfrak{q}$ τής $R$, ούτως ώστε να ισχύει $\{0\} \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{p}$.

(b) Έστω $V = \mathbf{V}(F)$ μια ανάγωγη υπερεπιφάνεια εντός τού $\mathbb{A}^n_{\mathbf{k}}$. Να αποδειχθεί ότι δεν υπάρχει κανένα ανάγωγο αλγεβρικό σύνολο $W$, τέτοιο ώστε να ισχύει $V \subsetneqq W \subsetneqq \mathbb{A}^n_{\mathbf{k}}$ (όπου $\mathbf{k}$ ένα αλγεβρικώς κλειστό σώμα).

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

(a) Να αποδειχθεί ότι κάθε στοιχείο τού πηλικοδακτυλίου $\mathbf{k}[\mathsf{X}, \mathsf{Y}, \mathsf{Z}]/I$ είναι η κλάση υπολοίπων ενός στοιχείου τής μορφής $A + B\mathsf{X} + C\mathsf{Y} + D\mathsf{XY}$, για κάποια πολυώνυμα $A, B, C, D \in \mathbf{k}[\mathsf{Z}]$.

(b) Εάν $F = A + B\mathsf{X} + C\mathsf{Y} + D\mathsf{XY}$, όπου $A, B, C, D \in \mathbf{k}[\mathsf{Z}]$, και $\alpha(F) = 0$, να γίνει σύγκριση ομοίων δυνάμεων τού $\mathsf{T}$ για να εξαχθεί το συμπέρασμα ότι $F = 0$.

(c) Να αποδειχθεί ότι $\mathrm{Ker}(\alpha) = I$ (οπότε το $I$ είναι πρώτο ιδεώδες), ότι το $\mathbf{V}(I)$ είναι ανάγωγο και ότι $\mathbf{I}(\mathbf{V}(I)) = I$.

**A-1-55**. Εάν τα $I, J$ είναι ιδεώδη τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ ($\mathbf{k}$ αλγεβρικώς κλειστό), με το $I$ ριζικό ιδεώδες, να αποδειχθεί ότι

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

(*Υπόδειξη*: Ο εγκλεισμός " $\supseteq$ " έχει αποδειχθεί, χωρίς περιορισμούς για το $\mathbf{k}$,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, οπότε μπορεί να εφαρμοσθεί το θεώρημα μηδενικών θέσεων τού Hilbert.)

**A-1-56.** Εάν τα $V, W \subseteq \mathbb{A}^n_{\mathbf{k}}$ είναι αλγεβρικά σύνολα και το $\mathbf{k}$ είναι αλγεβρικώς κλειστό, να αποδειχθούν τα εξής:

$$\mathbf{I}(V \cap W) = \mathrm{Rad}(\mathbf{I}(V) + \mathbf{I}(W)), \quad \mathbf{I}(V \cup W) = \mathrm{Rad}(\mathbf{I}(V)\mathbf{I}(W)) = \mathbf{I}(V) \cap \mathbf{I}(W).$$

**A-1-57.** Εάν τα $I, J$ είναι ιδεώδη τού $\mathbf{k}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ ($\mathbf{k}$ αλγεβρικώς κλειστό), να αποδειχθεί ότι οι κάτωθι συνθήκες είναι ισοδύναμες:

(a) Τα $I, J$ είναι μεταξύ τους πρώτα (βλ. ορσ. 1.4.6).

(b) $\mathbf{V}(I) \cap \mathbf{V}(J) = \varnothing$.

## 1.9 Μόδιοι και «Συνθήκες τού Πεπερασμένου»

**1.9.1 Ορισμός.** Έστω $R$ ένας δακτύλιος. Ένας $R$-**μόδιος** $M$ (ή ένας **μόδιος υπεράνω τού** $R$) είναι μια αβελιανή (= μεταθετική) ομάδα (η πράξη τής οποίας σημειώνεται ως «+» και το ουδέτερο στοιχείο της ως $0_M$, ή, όταν δεν υφίσταται κίνδυνος συγχύσεως, απλώς ως $0$), η οποία είναι εφοδιασμένη με έναν «αριθμητικό» (ή «βαθμωτό») πολλαπλασιασμό:

$$R \times M \ni (r, m) \longmapsto rm \in M,$$

και πληροί τα ακόλουθα αξιώματα:

(a) $(r + s)\, m = r\, m + s\, m, \ \ \forall r, s \in R, \ \ \forall m \in M,$

(b) $r(m + m') = r\, m + r\, m', \ \ \forall r \in R, \ \ \forall m, m' \in M,$

(c) $(r\, s)\, m = r\, (s\, m), \ \ \forall r, s \in R, \ \ \forall m \in M,$

(d) $1_R\, m = m, \forall m \in M$, όπου $1_R$ το μοναδιαίο πολλαπλασιαστικό στοιχείο τού $R$.

**1.9.2 Σημείωση.** Γιά κάθε $m \in M$ έχουμε $0_R\, m = 0_M$, διότι από το μονοσήμαντο τού ουδετέρου στοιχείου $0_M$ τής πρόσθεσης στον $M$ έπεται ότι

$$0_R\, m = (0_R + 0_R)\, m = 0_R\, m + 0_R\, m \Longrightarrow 0_R\, m = 0_M.$$

**1.9.3 Παραδείγματα.** (a) Προφανώς κάθε δακτύλιος $R$ είναι ένας $R$-μόδιος.

(b) Κάθε ιδεώδες ενός δακτυλίου $R$ είναι ένας $R$-μόδιος.

(c) Εάν $I$ είναι ένα ιδεώδες ενός δακτυλίου $R$, τότε ο δακτύλιος πηλίκων $R/I$ εφοδιάζεται με τη δομή ενός $R$-μοδίου μέσω τού αριθμητικού πολλαπλασιασμού

$$R \times (R/I) \ni (r, a + I) \longmapsto (ra) + I \in R/I.$$

(d) Κάθε $\mathbb{Z}$-μόδιος $M$ είναι μια αβελιανή ομάδα στην οποία

$$(\pm\kappa)\, m = \pm(\underbrace{m + m + \cdots + m + m}_{\kappa\text{-φορές}}), \quad \forall m \in M, \quad \forall \kappa \in \mathbb{N}_0.$$

(e) Όταν το $\mathbf{k}$ είναι ένα σώμα, τότε οι έννοιες τού $\mathbf{k}$-μοδίου και τού διανυσματικού χώρου υπεράνω τού $\mathbf{k}$ συμπίπτουν.

(f) Εάν ο $\varphi : R \longrightarrow S$ είναι ένας ομομορφισμός δακτυλίων, τότε ο δακτύλιος $S$ εφοδιάζεται με τη δομή ενός $R$-μοδίου[11] ($R$-**άλγεβρας**) μέσω τού αριθμητικού πολλαπλασιασμού

$$R \times S \ni (r, s) \longmapsto r\, s := \varphi\,(r)\ s \in S.$$

(Ειδικότερα, εάν ο $R$ είναι υποδακτύλιος τού $S$, ο $S$ είναι ένας $R$-μόδιος).

**1.9.4 Ορισμός.** Ένα υποσύνολο $N$ ενός $R$-μοδίου $M$ λέγεται **υπομόδιος** τού $M$ όταν ισχύει

$$[(\forall r, s \in R) \wedge (\forall m, m' \in N) \Longrightarrow r\, m + s\, m' \in N]\,,$$

δηλαδή όταν το ίδιο το $N$ μπορεί να καταστεί ένας $R$-μόδιος.

**1.9.5 Παραδείγματα.** (a) Κάθε ιδεώδες ενός δακτυλίου $R$ είναι υπομόδιος τού $R$.

(b) Εάν το $I$ είναι ένα ιδεώδες ενός δακτυλίου $R$, τότε οι $R$-υπομόδιοι τού $R/I$ είναι ακριβώς τα ιδεώδη τού $R/I$.

**1.9.6 Ορισμός.** Ένας **ομομορφισμός** $f : M \longrightarrow N$ μεταξύ δυο $R$-μοδίων $M, N$ είναι μια απεικόνιση για την οποία ισχύει $f(r\, m + s\, m') = r f(m) + s f(m')$ για οιαδήποτε $r, s \in R$ και $m, m' \in M$. (Ενριπτικοί, επιρριπτικοί και αμφιρριπτικοί ομομορφισμοί $R$-μοδίων καλούνται **μονομορφισμοί**, **επιμορφισμοί** και **ισομορφισμοί** $R$-μοδίων, αντιστοίχως.) Αυτές οι έννοιες ειδικεύονται (κατ' αναλογίαν) για $R$-άλγεβρες εάν κανείς λαβει υπ' όψιν τα προναφερθέντα στο 1.9.3 (f).

**1.9.7 Ορισμός.** Εάν το $\mathcal{S}$ είναι ένα υποσύνολο ενός $R$-μοδίου $M$, τότε ο υπομόδιος τού $M$ **ο παραγόμενος από το** $\mathcal{S}$ είναι ο

$$\left\{ \sum_{i=1}^{\kappa} r_i s_i \;\middle|\; r_1, \ldots, r_\kappa \in R,\ \ s_1, \ldots, s_\kappa \in \mathcal{S},\ \ \kappa \in \mathbb{N} \right\}.$$

Αυτός αποτελεί τον ελάχιστο $R$-υπομόδιο τού $M$, ο οποίος περιέχει το $\mathcal{S}$. Εάν το $\mathcal{S}$ συμβεί να είναι πεπερασμένο, ας πούμε $\mathcal{S} = \{s_1, \ldots, s_\nu\}$, τότε ο $R$-υπομόδιος τού $M$, ο παραγόμενος από αυτό, συμβολίζεται ως $\sum_{i=1}^{\nu} R\, s_i$.

[11] Σε αυτήν την περίπτωση ο $S$ ονομάζεται, εναλλακτικώς, και $R$-**άλγεβρα**. Μάλιστα, όταν ο $S$ είναι πεπερασμένως παραγόμενος ως $R$-μόδιος (ήτοι **μοδιακώς πεπερασμένος υπεράνω τού** $R$), τότε ονομάζεται ενίοτε και **πεπερασμένη** $R$-**άλγεβρα** ή **άλγεβρα πεπερασμένη υπεράνω τού** $R$.)

**1.9.8 Ορισμός.** Ένας $R$-μόδιος $M$ καλείται **πεπερασμένως παραγόμενος** όταν υπάρχει ένα πεπερασμένο υποσύνολό του $\mathcal{S} = \{s_1, \dots, s_\nu\}$, ούτως ώστε να ισχύει

$$M = \sum_{i=1}^{\nu} R\, s_i.$$

Ας σημειωθεί ότι αυτή η έννοια είναι πλήρως εναρμονισμένη με τις γνωστές έννοιες τής πεπερασμένως παραγομένης αβελιανής ομάδας, τού πεπερασμένως παραγομένου ιδεώδους ενός δακτυλίου, καθώς και τού πεπερασμένως παραγομένου $\mathbf{k}$-διανυσματικού χώρου (όταν το $R = \mathbf{k}$ είναι ένα σώμα).

**1.9.9 Ορισμός.** Έστω $R$ ένας υποδακτύλιος ενός δακτυλίου $S$. Υπάρχουν διαφορετικές «*συνθήκες τού πεπερασμένου*», τις οποίες θα μπορούσε να πληροί ο $S$ υπεράνω τού $R$, εξαρτώμενες από το κατά πόσον ο $S$ θεωρείται ως $R$-μόδιος, ως δακτύλιος ή συμβαίνει να είναι σώμα.

(a) Ο $S$ καλείται **μοδιακώς πεπερασμένος υπεράνω τού** $R$ όταν ο $S$ είναι πεπερασμένως παραγόμενος ως $R$-μόδιος. (Στην περίπτωση κατά την οποία οι $R$ και $S$ είναι σώματα, θα κάνουμε χρήση τού συμβολισμού $[S : R] = \dim_R(S)$).

(b) Υπενθυμίζουμε ότι ο υποδακτύλιος, ο παραγόμενος από ένα υποσύνολο $U$ τού $S$, είναι ο ελάχιστος υποδακτύλιος τού $S$ ο οποίος περιέχει το $U$. Ο υποδακτύλιος τού $S$, ο οποίος περιέχει τόσο τον $R$ όσο και το $U$, συμβολίζεται ως $R[U]$ και ισούται με

$$R[U] = \left\{ \sum \lambda_{(i_1,\dots,i_\kappa)}\, v_1^{i_1} v_2^{i_2} \cdots v_\kappa^{i_\kappa} \;\middle|\; \lambda_{(i_1,\dots,i_\kappa)} \in R,\ \ \kappa \in \mathbb{N} \right\}.$$

Εάν $S = R[U]$, για κάποιο υποσύνολο $U$ τού $S$, τότε λέμε πως ο $S$ είναι μια **δακτυλιακή επέκταση τού** $R$. Στη συνέχεια, ας υποθέσουμε ότι το $U = \{v_1, v_2, \dots, v_n\}$ είναι ένα *πεπερασμένο* υποσύνολο τού $S$. Ορίζουμε τον ομομορφισμό δακτυλίων

$$R\left[\mathsf{X}_1, \mathsf{X}_2, \dots, \mathsf{X}_n\right] \ni F \longmapsto \varphi\left(F\right) = F\left(v_1, v_2, \dots, v_n\right) \in S.$$

Αυτός έχει ως εικόνα του την

$$\mathrm{Im}\left(\varphi\right) = R\left[v_1, v_2, \dots, v_n\right],$$

γραφόμενη υπό τη μορφή

$$R\left[v_1, v_2, \dots, v_n\right] = \left\{ \sum \lambda_{(i_1,\dots,i_n)}\, v_1^{i_1} v_2^{i_2} \cdots v_n^{i_n} \;\middle|\; \lambda_{(i_1,\dots,i_n)} \in R \right\}.$$

Ο $S$ καλείται **δακτυλιακώς πεπερασμένος υπεράνω τού** $R$ (ή **πεπερασμένως παραγόμενη δακτυλιακή επέκταση**[12] **τού** $R$) όταν ισχύει $S = R\left[v_1, v_2, \dots, v_n\right]$ για κάποια

[12] Αντ' αυτού χρησιμοποιείται ενίοτε και το «**πεπερασμένως παραγόμενη** $R$-**άλγεβρα**».

$v_1, v_2, \ldots, v_n \in S$.

(c) Ας υποθέσουμε τώρα ότι τα $R = \mathbf{k}$ και $S = L$ είναι σώματα. Εάν $v_1, \ldots, v_n \in L$, έστω $\mathbf{k}(v_1, \ldots, v_n)$ το σώμα των κλασμάτων τού $\mathbf{k}[v_1, \ldots, v_n]$. Θεωρούμε το $\mathbf{k}(v_1, \ldots, v_n)$ ως υπόσωμα τού $L$. Υπ' αυτήν την προϋπόθεση, το $\mathbf{k}(v_1, \ldots, v_n)$ είναι το ελάχιστο υπόσωμα τού $L$, το οποίο περιέχει τόσον το $\mathbf{k}$ όσον και τα $v_1, v_2, \ldots, v_n$. Το $L$ λέγεται **πεπερασμένως παραγόμενη σωματική επέκταση** τού $\mathbf{k}$ όταν μπορεί να γραφεί υπό τη μορφή $L = \mathbf{k}(v_1, \ldots, v_n)$ για κάποια $v_1, \ldots, v_n \in L$.

**1.9.10 Ορισμός.** Έστω $R$ ένας δακτύλιος. Ένας $R$-μόδιος $M$ καλείται **ναιτεριανός μόδιος** όταν κάθε υπομόδιος $N$ τού $M$ είναι πεπερασμένως παραγόμενος υπό την έννοια τού ορισμού 1.9.8. (Πρόκειται για άμεση γενίκευση τού 1.5.2 για $R$-μοδίους.)

**1.9.11 Πρόταση.** *Εάν ο $R$ είναι ένας ναιτεριανός δακτύλιος και ο $M$ ένας πεπερασμένως παραγόμενος $R$-μόδιος, τότε ο $M$ είναι ναιτεριανός μόδιος.*

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως υπάρχουν $m_1, \ldots, m_\nu \in M$, τέτοια ώστε να ισχύει

$$M = Rm_1 + \cdots + Rm_\nu.$$

Συνεπώς υπάρχει ένας επιμορφισμός $R$-μοδίων $\beta : R^\nu \longrightarrow M$ με

$$\beta(0_R, \ldots, 0_R, \underbrace{1_R}_{i\text{-οστή θέση}} 1_R, 0_R, \ldots, 0_R) = m_i, \ \ \forall i \in \{1, \ldots, \nu\}.$$

Εάν ο $N$ είναι ένας υπομόδιος τού $M$, τότε και η αντίστροφη εικόνα $\beta^{-1}(N)$ είναι ένας υπομόδιος τού $R^\nu$. Ως εκ τούτου, είναι αρκετό να επαληθευθεί ο ισχυρισμός για τον $R^\nu$. Θα εργασθούμε επαγωγικώς επί τού $\nu$. Για $\nu = 1$ ο ισχυρισμός είναι εξ υποθέσεως αληθής. Έστω τώρα ένας υπομόδιος $N$ τού $R^\nu$, όπου $\nu \geq 2$. Οι πρώτες συντεταγμένες $x_1$ των στοιχείων $x = (x_1, \ldots, x_n) \in N$ συγκροτούν ένα ιδεώδες $I$ τού $R$. Το $I$ είναι εξ υποθέσεως πεπερασμένως παραγόμενο, ήτοι

$$\exists \kappa \in \mathbb{N} : I = \left\langle x_1^{(1)}, \ldots, x_1^{(\kappa)} \right\rangle.$$

Θεωρούμε στοιχεία $x^{(i)} \in N$ έχοντα το $x_1^{(1)}$ ως πρώτη τους συντεταγμένη. Για *τυχόν* $x = (x_1, \ldots, x_n) \in N$ υπάρχουν $r_1, \ldots, r_\kappa \in R$ με

$$x_1 = r_1 x_1^{(1)} + \cdots + r_\kappa x_1^{(\kappa)},$$

οπότε το στοιχείο $x - (r_1 x^{(1)} + \cdots + r_\kappa x^{(\kappa)})$ είναι τής μορφής $(0_R, x_2', \ldots, x_n')$. Έστω $M' \cong R^{\nu-1} \subset R^\nu$ ο υπομόδιος των στοιχείων τού $R^\nu$, η πρώτη συντεταγμένη των οποίων ισούται με $0_R$. Κατά την επαγωγική μας υπόθεση ο υπομόδιος $N' := N \cap M'$ τού μοδίου $M' \cong R^{\nu-1}$ είναι πεπερασμένως παραγόμενος, ήτοι

$$\exists l \in \mathbb{N} : N' = Ry_1 + \cdots + Ry_l.$$

Άρα $N = Rx^{(1)} + \cdots + Rx^{(\kappa)} + Ry_1 + \cdots + Ry_l$. □

## Ασκήσεις

**A-1-58.** Εάν ο δακτύλιος $S$ είναι μοδιακώς πεπερασμένος υπεράνω τού $R$, να αποδειχθεί ότι ο $S$ είναι και δακτυλιακώς πεπερασμένος υπεράνω τού $R$.

**A-1-59**. Να αποδειχθεί ότι ο $S = R[\mathsf{X}]$ (ο δακτύλιος πολυωνύμων μίας μεταβλητής) είναι δακτυλιακώς πεπερασμένος υπεράνω τού $R$, δίχως όμως να είναι και μοδιακώς πεπερασμένος υπεράνω αυτού.

**A-1-60**. Έστω $L$ μια πεπερασμένως παραγόμενη δακτυλιακή επέκταση τού $\mathbf{k}$, όπου τα $\mathbf{k}$ και $L$ είναι σώματα. Να αποδειχθεί ότι το $L$ αποτελεί μια πεπερασμένως παραγόμενη σωματική επέκταση τού $\mathbf{k}$.

**A-1-61**. Να αποδειχθεί ότι το σώμα $L = \mathbf{k}(\mathsf{X})$ (ήτοι το *σώμα των ρητών συναρτήσεων μίας μεταβλητής* ) είναι μια πεπερασμένως παραγόμενη σωματική επέκταση τού $\mathbf{k}$, δίχως όμως να είναι και πεπερασμένως παραγόμενη δακτυλιακή επέκταση τού $\mathbf{k}$. (*Υπόδειξη*: Να χρησιμοποιηθεί η άσκηση **A-1-4**).

**A-1-62**. Εάν ο $R$ είναι ένας υποδακτύλιος ενός δακτυλίου $S$ και ο $S$ είναι υποδακτύλιος ενός δακτυλίου $T$, να αποδειχθούν τα ακόλουθα:

(a) Εάν $S = \sum_{i=1}^{n} R\, v_i$ και $T = \sum_{j=1}^{m} S\, w_j$,τότε το $T$ γράφεται ως εξής:

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

(b) Εάν $S = R\left[v_1, v_2, \ldots, v_n\right]$ και $T = S\left[w_1, w_2, \ldots, w_m\right]$, τότε

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

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

$$T = R\left(v_1, v_2, \ldots, v_n, w_1, w_2, \ldots, w_m\right).$$

(Αυτό σημαίνει ότι όλες οι «συνθήκες τού πεπερασμένου» ενός δακτυλίου υπεράνω ενός άλλου είναι *μεταβατικές*.)

## 1.10 Ακέραια Στοιχεία

**1.10.1 Ορισμός.** Έστω $R$ ένας υποδακτύλιος ενός δακτυλίου $S$. Ένα στοιχείο $v \in S$ λέγεται **ακέραιο στοιχείο** υπεράνω τού $R$ όταν υπάρχει ένα μονικό πολυώνυμο

$$F = \mathsf{X}^n + a_1\,\mathsf{X}^{n-1} + a_2\,\mathsf{X}^{n-2} + \cdots + a_{n-1}\,\mathsf{X} + a_n \in R\,[\mathsf{X}]\,,$$

τέτοιο ώστε να ισχύει $F(v) = 0$. Στην περίπτωση κατά την οποία τα $R$ και $S$ είναι *σώματα* αντί τού όρου «ακέραιο στοιχείο» χρησιμοποιούμε τον όρο **αλγεβρικό στοιχείο** υπεράνω τού $R$.

**1.10.2 Πρόταση.** *Έστω $R$ ένας υποδακτύλιος τού $S$ και έστω $v$ ένα στοιχείο τού $S$. Τότε τα ακόλουθα είναι ισοδύναμα*:

(1) *Το $v$ είναι ακέραιο υπεράνω τού $R$.*

(2) *Ο $R[v]$ είναι μοδιακώς πεπερασμένος υπεράνω τού $R$.*

(3) *Υπάρχει ένας υποδακτύλιος $R'$ τού $S$, ο οποίος περιέχει τον $R[v]$ και είναι μοδιακώς πεπερασμένος υπεράνω τού $R$.*

ΑΠΟΔΕΙΞΗ. (1) $\Rightarrow$ (2). *Πρώτη απόδειξη.* Εάν το $v$ είναι αλγεβρικό υπεράνω τού $R$, τότε υφίσταται μια σχέση τής μορφής

$$v^n + a_1\,v^{n-1} + a_2\,v^{n-2} + \cdots + a_{n-1}\,v + a_n = 0,$$

όπου $a_1, \ldots, a_n \in R$. Επομένως το $v^n$ περιέχεται στον $\sum_{i=0}^{n-1} Rv^i$. Αντιστοίχως, οι σχέσεις

$$v^{n+m} + a_1\,v^{n+m-1} + a_2\,v^{n+m-2} + \cdots + a_{n-1}\,v^{m+1} + a_n\,v^m = 0$$

δείχνουν ότι $v^{n+m} \in \sum_{i=0}^{n+m-1} Rv^i$. Χρησιμοποιώντας τήν ισότητα

$$v^{n+m} = -a_1\,v^{n+m-1} - a_2\,v^{n+m-2} - \cdots - a_{n-1}\,v^{m+1} - a_n\,v^m$$

και μαθηματική επαγωγή επί τού $m$, αποδεικνύεται εύκολα ότι

$$v^m \in \sum_{i=0}^{n-1} Rv^i$$

για κάθε $m \in \mathbb{N}_0$.

*Δεύτερη απόδειξη.* Επειδή

$$R[v] = \{G\,(v) \mid G \in R\,[\mathsf{X}]\},$$

εάν υπάρχει ένα

$$F = \mathsf{X}^n + a_1\,\mathsf{X}^{n-1} + a_2\,\mathsf{X}^{n-2} + \cdots + a_{n-1}\,\mathsf{X} + a_n \in R\,[\mathsf{X}]\,,$$

τέτοιο ώστε $F(v) = 0$, μπορούμε να εφαρμόσουμε τον αλγόριθμο τής διαιρέσεως ενός $G \in R\,[\mathsf{X}]$ διά τού $F$, βρίσκοντας

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

Ύστερα από αποτίμηση τού $G$ στο $v$ λαμβάνουμε $G(v) = Q(v)$. Εξ αυτού έπεται ότι

$$R[v] = \{Q(v) \in R\,[\mathsf{X}] \mid \deg(Q) < n\} = \sum_{i=0}^{n-1} Rv^i.$$

(2) ⇒ (3). Αυτή η συνεπαγωγή είναι προφανής εάν θέσουμε $R' = R[v]$.

(3) ⇒ (1). Έστω ότι $R' = \sum_{j=1}^{n} Rw_j$. Δίχως βλάβη τής γενικότητας υποθέτουμε ότι υπάρχει ένας δείκτης $\varrho \in \{1, \ldots, n\}$, τέτοιος ώστε να ισχύει $w_\varrho = 1$. (Κι αυτό, διότι σε κάθε πεπερασμένο σύνολο, το οποίο παράγει έναν $R$-μόδιο, μπορούμε προφανώς να επισυνάπτουμε το μοναδιαίο πολλαπλασιαστικό στοιχείο τού δακτυλίου $R$). Επειδή για κάθε $j \in \{1, \ldots, n\}$ τα $vw_j$ ανήκουν στον $R'$, ικανοποιούνται εξισώσεις τής μορφής

$$v\,w_j = \sum_{\kappa=1}^{n} a_{\kappa\,j}\,w_\kappa \Longleftrightarrow \sum_{\kappa=1}^{n} (a_{\kappa\,j} - \delta_{j\,\kappa}\,v)\;w_\kappa = 0,$$

για κατάλληλα $a_{\kappa\,j} \in R$, όπου το

$$\delta_{j\,\kappa} := \delta_{\kappa\,j} := \begin{cases} 1, & \text{όταν } j = \kappa \\ 0, & \text{όταν } j \neq \kappa \end{cases}$$

είναι το σύμβολο τού Kronecker. Ορίζουμε

$$b_{j\,\kappa} := a_{\kappa\,j} - \delta_{j\,\kappa}\,v, \quad 1 \leq j, \kappa \leq n,$$

καθώς και τον $(n \times n)$-πίνακα $\mathfrak{B} = (b_{j\,\kappa})$ με στοιχεία ανήκοντα στον δακτύλιο $R[v]$. Όπως και στη συνήθη θεωρία τής Γραμμικής Άλγεβρας, η ορίζουσα $\det(\mathfrak{B})$ ενός τέτοιου πίνακα ικανοποιεί τη σχέση

$$\mathfrak{B}\;(\mathbf{adj}\,(\mathfrak{B})) = \mathbf{adj}\,(\mathfrak{B})\;\;\mathfrak{B} = \det(\mathfrak{B}) \cdot \mathbf{I}_n = \begin{pmatrix} \det(\mathfrak{B}) & 0 & \cdots & 0 \\ 0 & \det(\mathfrak{B}) & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & \det(\mathfrak{B}) \end{pmatrix},$$

όπου με $\mathbf{I}_n$ συμβολίζουμε τον μοναδιαίο $(n \times n)$-πίνακα και με $\mathbf{adj}\,(\mathfrak{B})$ τον «προσαρτημένο» ή $(n \times n)$-πίνακα

$$\mathbf{adj}\,(\mathfrak{B}) = \begin{pmatrix} \widetilde{b}_{1\,1} & \widetilde{b}_{2\,1} & \cdots & \widetilde{b}_{n\,1} \\ \widetilde{b}_{1\,2} & \widetilde{b}_{2\,2} & \cdots & \widetilde{b}_{n\,2} \\ \cdots & \cdots & \cdots & \cdots \\ \widetilde{b}_{1\,n} & \widetilde{b}_{2\,n} & \ldots & \widetilde{b}_{n\,n} \end{pmatrix}$$

τού $\mathfrak{B}$. Τα στοιχεία τού $\mathbf{adj}\,(\mathfrak{B})$ ορίζονται μέσω τού τύπου

$$\widetilde{b}_{ij} = (-1)^{i+j}\ \det\left(C_{ij}\right),$$

όπου ο $C_{ij}$ είναι ο ελάσσων $(n-1)\times(n-1)$-πίνακας, ο σχηματιζόμενος από τον $\mathfrak{B}$ ύστερα από τη διαγραφή τής $i$-οστής στήλης και τής j-οστής γραμμής. Προφανώς,

$$0 = \sum_{\kappa=1}^{n} b_{j\,\kappa} w_\kappa$$

$$\Longrightarrow 0 = \sum_{j=1}^{n} \widetilde{b}_{ij} (\sum_{\kappa=1}^{n} b_{j\,\kappa} w_\kappa) = \sum_{\kappa=1}^{n}\sum_{j=1}^{n} \widetilde{b}_{ij} b_{j\,\kappa} w_\kappa = \sum_{\kappa=1}^{n} \det(\mathfrak{B})\,\delta_{i\,\kappa} w_\kappa = \det(\mathfrak{B})\, w_i$$

Επειδή $w_\varrho = 1$, η τελευταία αυτή εξίσωση (θέτοντας $i = \varrho$) μας δίνει

$$\det(\mathfrak{B}) = \det\left(\left(a_{\kappa\,j} - \delta_{j\,\kappa}\, v\right)_{j\,\kappa}\right) = 0$$

Επομένως, το $v$ αποτελεί σημείο μηδενισμού τού πολυωνύμου

$$F = \det\left(\left(\delta_{j\,\kappa}\,\mathsf{X} - a_{\kappa\,j}\right)_{j\,\kappa}\right) = \begin{vmatrix} \mathsf{X}-a_{1\,1} & -a_{1\,2} & \cdots & -a_{1\,n} \\ -a_{2\,1} & \mathsf{X}-a_{2\,2} & \cdots & -a_{2\,n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n\,1} & -a_{n\,1} & \ldots & \mathsf{X}-a_{n\,n} \end{vmatrix} \in R\,[\mathsf{X}]$$

(ήτοι τού «χαρακτηριστικού» πολυωνύμου τού πίνακα $\left(a_{\kappa\,j}\right)_{j\,\kappa}$), γραφόμενο υπό τη μορφή

$$F = \mathsf{X}^n + G, \quad G \in R\,[\mathsf{X}]\,, \quad \deg(G) < n,$$

Άρα το $v$ είναι όντως αλγεβρικό υπεράνω τού $R$. □

**1.10.3 Πόρισμα.** *Το σύνολο όλων των στοιχείων τού $S$, τα οποία είναι ακέραια υπεράνω τού $R$, συγκροτούν έναν υποδακτύλιο τού $S$ που περιέχει τον $R$.*

ΑΠΟΔΕΙΞΗ. Εάν τα $a$ και $b$ είναι στοιχεία τού $S$ ακέραια υπεράνω τού $R$, τότε το $b$ είναι ακέραιο και υπεράνω τού $R\,[a] \supseteq R$. Σύμφωνα με την πρόταση 1.10.2, ο $R[a,b]$ είναι μοδιακώς πεπερασμένος υπεράνω τού $R[a]$. Από το (a) τής ασκήσεως **A-1-62** συμπεραίνουμε ότι ο $R[a,b]$ είναι μοδιακώς πεπερασμένος υπεράνω τού $R$. Από την άλλη μεριά έχουμε $a \pm b, ab \in R[a,b]$, οπότε και τα $a \pm b, ab$ θα είναι αλγεβρικά υπεράνω τού $R$ (και πάλι βάσει τής προτάσεως 1.10.2). □

**1.10.4 Σημείωση.** Ιδιαιτέρως, λέμε ότι ο $S$ είναι ένας **ακέραιος δακτύλιος** υπεράνω τού $R$ όταν *κάθε* στοιχείο του είναι ακέραιο υπεράνω τού $R$. Στην περίπτωση κατά την οποία οι $R$ και $S$ είναι σώματα, και το $S$ είναι ακέραιο υπεράνω τού $R$, λέμε ότι το $S$ αποτελεί μια **αλγεβρική επέκταση** τού $R$.

## Ασκήσεις

**A-1-63.** Έστω ότι ο $R$ είναι ένας υποδακτύλιος κάποιου δακτυλίου $S$ και ότι ο $S$ είναι ένας υποδακτύλιος κάποιου δακτυλίου $T$. Εάν ο $S$ είναι ακέραιος υπεράνω τού $R$ και ο $T$ ακέραιος υπεράνω τού $S$, να αποδειχθεί ότι και ο $T$ είναι ακέραιος υπεράνω τού $R$. (*Υπόδειξη*: Έστω $t \in T$ με $t^n + a_1 t^{n-1} + \cdots + a_n = 0$, $a_i \in S$. Τότε ο $R[a_1, \ldots, a_n, t]$ είναι μοδιακώς πεπερασμένος υπεράνω τού $R$.)

**A-1-64**. Υποθέτοντας ότι ο $S$ είναι δακτυλιακώς πεπερασμένος υπεράνω τού $R$ να αποδειχθεί ότι ο $S$ είναι μοδιακώς πεπερασμένος υπεράνω τού $R$ εάν και μόνον εάν ο $S$ είναι ακέραιος υπεράνω τού $R$.

**A-1-65**. Έστω $L$ ένα σώμα και έστω $\mathbf{k}$ ένα αλγεβρικώς κλειστό υπόσωμά του. Να αποδειχθούν τα ακόλουθα:

(a) Κάθε στοιχείο τού $L$, το οποίο είναι αλγεβρικό υπεράνω τού $\mathbf{k}$, οφείλει να ανήκει στο ίδιο το $\mathbf{k}$.

(b) Κανένα αλγεβρικώς κλειστό σώμα δεν διαθέτει μοδιακώς πεπερασμένες σωματικές επεκτάσεις πέραν τής τετριμμένης (ήτοι πέραν τού εαυτού του).

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

(a) Κάθε στοιχείο τού $L$, το οποίο είναι ακέραιο υπεράνω τού $\mathbf{k}[\mathsf{X}]$, οφείλει να ανήκει στο ίδιο το $\mathbf{k}[\mathsf{X}]$. (*Υπόδειξη*: Εάν ισχύει $z^n + a_1 z^{n-1} + \cdots = 0$, να γραφεί το $z$ ως κλάσμα $z = \frac{F}{G}$, όπου τα $F$ και $G$ είναι μεταξύ τους πρώτα. Τότε $F^n + a_1 F^{n-1} G + \cdots = 0$, οπότε το $G$ διαιρεί το $F$.)

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

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

(*Υπόδειξη*: Να θεωρηθεί το $z = \frac{1}{G}$, όπου το $G$ είναι ένα ανάγωγο πολυώνυμο που δεν διαιρεί το $F$).

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

(a) Να αποδειχθεί ότι το σύνολο των στοιχείων τού $L$, τα οποία είναι αλγεβρικά υπεράνω τού $\mathbf{k}$, αποτελεί ένα υπόσωμα τού $L$ που περιέχει το $K$. (*Υπόδειξη*: Εάν υποτεθεί ότι $v^n + a_1 v^{n-1} + \cdots + a_n = 0$, όπου $a_n \neq 0$, τότε $v(v^{n-1} + \cdots) = -a_n$.)

(b) Έστω ότι το $L$ είναι μοδιακώς πεπερασμένο υπεράνω τού $\mathbf{k}$ και ότι

$$\mathbf{k} \subseteq R \subseteq L,$$

όπου ο $R$ είναι ένας δακτύλιος. Να αποδειχθεί ότι ο $R$ είναι εφοδιασμένος με τη δομή σώματος.

## 1.11 Επεκτάσεις Σωμάτων

**(i)** Ας υποθέσουμε ότι το $\mathbf{k}$ είναι ένα υπόσωμα τού $L$ (ή -ισοδυνάμως- ότι το $L$ είναι μια **επέκταση** τού $\mathbf{k}$) και ότι $L = \mathbf{k}(v)$ για κάποιο στοιχείο $v \in L$. Έστω $\varphi$ ο ομομορφισμός

$$\varphi : \mathbf{k}[\mathsf{X}] \longrightarrow L, \quad \varphi(G) = G(v).$$

Επειδή ο $\mathbf{k}[\mathsf{X}]$ είναι μια Π.Κ.Ι (βλ. θεώρημα 1.1.24), ο πυρήνας του οφείλει να είναι τής μορφής $\mathrm{Ker}(\varphi) = \langle F \rangle$, για κάποιο πολυώνυμο $F \in \mathbf{k}[\mathsf{X}]$. Από την άλλη μεριά, έχουμε $\mathrm{Im}(\varphi) = \mathbf{k}[v]$, οπότε από το 1ο θεώρημα ισομορφισμών δακτυλίων 1.1.10 έπεται ότι

$$\mathbf{k}[\mathsf{X}] \,/\, \langle F \rangle \cong \mathbf{k}[v] \Longrightarrow \text{το ιδεώδες } \langle F \rangle \text{ είναι πρώτο}$$

(διότι ο $\mathbf{k}[v]$ είναι ακεραία περιοχή, βλ. θεώρημα 1.1.24). Θα εξετάσουμε τώρα τις δύο δυνατές εκδοχές για τη φύση τού πολυωνύμου $F$ χωριστά.

• **Πρώτη περίπτωση**. $F = 0$. Τότε έχουμε

$$\mathbf{k}[\mathsf{X}] \cong \mathbf{k}[v] \Longrightarrow \mathbf{k}(\mathsf{X}) \cong \mathbf{k}(v) = L.$$

Σε αυτήν την περίπτωση το $L$ δεν είναι ούτε δακτυλιακώς ούτε μοδιακώς πεπερασμένο υπεράνω τού $\mathbf{k}$ (σύμφωνα με την άσκηση **A-1-61**). Εν προκειμένω, λέμε ότι το $v$ είναι ένα **υπερβατικό στοιχείο** τού $L$ υπεράνω τού $\mathbf{k}$.

• **Δεύτερη περίπτωση**. $F \neq 0$. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι το $F$ είναι ένα μονικό πολυώνυμο. (Πράγματι· εάν $F = \sum_{i=0}^{n} a_i X^i$, με $a_n \notin \{0, 1\}$, τότε αντ' αυτού θα μπορούσαμε να θεωρήσουμε το μονικό πολυώνυμο $a_n^{-1}F$, για το οποίο ισχύει $\langle F \rangle = \langle a_n^{-1}F \rangle$). Εξ αιτίας τού ότι το $\langle F \rangle$ είναι πρώτο ιδεώδες, το $F$ οφείλει να είναι ανάγωγο πολυώνυμο· και επειδή ο $\mathbf{k}[\mathsf{X}]$ είναι Π.Κ.Ι., το $\langle F \rangle$ οφείλει να είναι, συγχρόνως, και μεγιστοτικό ιδεώδες του (σύμφωνα με το (d) τού πορίσματος 1.1.17). Αυτό όμως σημαίνει ότι το $\mathbf{k}[v]$ είναι σώμα, οπότε, αφού $v \in \mathbf{k}[v]$ και το ελάχιστο σώμα με αυτήν την ιδιότητα είναι το $\mathbf{k}(v)$, θα έχουμε

$$\mathbf{k}[v] \supseteq \mathbf{k}(v) \Rightarrow \mathbf{k}[v] = \mathbf{k}(v).$$

Δεδομένου δε τού ότι $F(v) = 0$, όπου το $F$ είναι μονικό, το $v$ θα αποτελεί ένα **αλγεβρικό στοιχείο** τού $L$ υπεράνω τού $\mathbf{k}$, οπότε το $L = \mathbf{k}[v]$ θα είναι μοδιακώς πεπερασμένο υπεράνω τού $\mathbf{k}$.

**(ii)** Για να αποπερατωθεί η απόδειξη τού «Ασθενούς Θεωρήματος των Μηδενικών Θέσεων» (βλ. θεώρημα 1.8.1), θα πρέπει να αποδείξουμε την αλήθεια τού ισχυρισμού $\boxed{*}$ (τής σελίδας 51), τον οποίο είχαμε προσωρινώς παρακάμψει. Αυτός μάς πληροφορεί πως, εάν ένα σώμα $L$ είναι δακτυλιακώς πεπερασμένη επέκταση ενός αλγεβρικώς κλειστού σώματος $\mathbf{k}$, τότε έχουμε $L = \mathbf{k}$. Σύμφωνα με την άσκηση **A-1-65** (b), για να δειχθεί

αυτό, αρκεί κανείς να διαπιστώσει ότι το $L$ είναι μοδιακώς πεπερασμένο υπεράνω τού $\mathbf{k}$. Στο **(i)** δικαιολογήσαμε το γιατί μια δακτυλιακώς πεπερασμένη επέκταση μιας ειδικής μορφής είναι και μοδιακώς πεπερασμένη υπεράνω τού $\mathbf{k}$. Στην επομένη πρόταση θα δείξουμε ότι αυτό είναι αληθές για *οιεσδήποτε* δακτυλιακώς πεπερασμένες επεκτάσεις υπεράνω τού $\mathbf{k}$ (συμπληρώνοντας, κατ' αυτόν τον τρόπο, την απόδειξη τού θεωρήματος 1.8.1).

**1.11.1 Πρόταση. (Oscar Zariski)** *Εάν ένα σώμα $L$ είναι δακτυλιακώς πεπερασμένο υπεράνω ενός υποσώματός του $\mathbf{k}$, τότε το $L$ είναι μοδιακώς πεπερασμένο (και, κατ' επέκτασιν, επί τη βάσει τής ασκήσεως **A-1-64**, και αλγεβρικό ) υπεράνω τού $\mathbf{k}$.*

ΑΠΟΔΕΙΞΗ. Έστω $L = \mathbf{k}[v_1, \dots, v_n]$. Θα εργασθούμε κάνοντας χρήση μαθηματικής επαγωγής επί τού $n$. Για $n = 1$ ο ισχυρισμός τής προτάσεως είναι πρόδηλος σύμφωνα με τα όσα προαναφέραμε στο **(i)** τής παρούσας ενότητας. Υποθέτουμε ότι ο ισχυρισμός αυτός είναι αληθής για όλες τις επεκτάσεις που παράγονται από $n-1$ στοιχεία (όπου $n \geq 2$). Έστω $\mathbf{k}_1 := \mathbf{k}(v_1)$. Βάσει τής επαγωγικής υποθέσεώς μας, το $L = \mathbf{k}_1[v_2, \dots, v_n]$ είναι μοδιακώς πεπερασμένο (και, κατ' επέκτασιν, επί τη βάσει τής ασκήσεως **A-1-64**, και αλγεβρικό) επί τού $\mathbf{k}_1$. Επιπροσθέτως, μπορούμε να υποθέσουμε ότι το $v_1$ είναι *υπερβατικό* υπεράνω τού $\mathbf{k}_1$ (διότι αλλιώς η απόδειξη λήγει χρησιμοποιώντας -κατά σειράντις ασκήσεις **A-1-63**, **A-1-64** και **A-1-62** (a)). Καθένα από τα υπολειπόμενα $v_i$ (όντας αλγεβρικό υπεράνω τού $\mathbf{k}_1$) θα ικανοποιεί μια εξίσωση τής μορφής:

$$v_i^{m_i} + a_{i\,1} v_i^{m_i - 1} + a_{i\,2} v_i^{m_i - 2} + \cdots + a_{i\,m_i} = 0,$$

όπου $a_{i\,j} \in \mathbf{k}_1$ για όλα τα $i \in \{2, \dots, n\}$ και $j \in \{1, 2, \dots, m_i\}$. Εάν λοιπόν γράψουμε τα $a_{i\,j}$ ως κλάσματα

$$a_{i\,j} = \frac{F_{i\,j}(v_1)}{G_{i\,j}(v_1)}, \quad F_{i\,j},\ G_{i\,j} \in \mathbf{k}[\mathrm{X}],\ \ G_{i\,j}(v_1) \neq 0,$$

και θεωρήσουμε κάποιο κοινό πολλαπλάσιο $B_i$ όλων των $G_{i\,j}(v_1)$, ήτοι

$$B_i = \Delta_{i\,j} \cdot G_{i\,j}(v_1) \in \mathbf{k}[v_1], \text{για κάποια } \Delta_{i\,j} \in \mathbf{k}[v_1],$$

$\forall i \in \{2, \dots, n\}$, και $\forall j \in \{1, 2, \dots, m_i\}$,τότε προκύπτουν οι εξισώσεις

$$v_i^{m_i} + \frac{F_{i\,1}(v_1)}{G_{i\,1}(v_1)}\, v_i^{m_i - 1} + \frac{F_{i\,2}(v_1)}{G_{i\,2}(v_1)}\, v_i^{m_i - 2} + \cdots + \frac{F_{i\,m_i}(v_1)}{G_{i\,m_i}(v_1)} = 0$$

$$\Longrightarrow \left[\prod_{j=1}^{m_i} G_{i\,j}(v_1)\right] v_i^{m_i} + \left[\prod_{j=2}^{m_i} G_{i\,j}(v_1)\right] F_{i\,1}(v_1)\, v_i^{m_i - 1} + \cdots + \left[\prod_{j=1}^{m_i - 1} G_{i\,j}(v_1)\right] F_{i\,m_i}(v_1) = 0$$

$$\Longrightarrow \left[\prod_{j=1}^{m_i} \frac{B_i}{\Delta_{i\,j}}\right] v_i^{m_i} + \left[\prod_{j=2}^{m_i} \frac{B_i}{\Delta_{i\,j}}\right] F_{i\,1}(v_1)\, v_i^{m_i - 1} + \cdots + \left[\prod_{j=1}^{m_i - 1} \frac{B_i}{\Delta_{i\,j}}\right] F_{i\,m_i}(v_1) = 0$$

$$\Longrightarrow \frac{1}{\prod_{j=1}^{m_i} \Delta_{i\,j}} \cdot (B_i v_i)^{m_i} + \frac{1}{\prod_{j=2}^{m_i} \Delta_{i\,j}} \cdot F_{i\,1}(v_1)\, (B_i v_i)^{m_i - 1} + \cdots + \frac{1}{\prod_{j=1}^{m_i - 1} \Delta_{i\,j}} \cdot F_{i\,m_i}(v_1)\, B_i^{m_i - 1} = 0.$$

Πολλαπλασιάζοντας και τα δύο μέλη με το γινόμενο

$$\prod_{j=1}^{m_i} \Delta_{i\,j} \neq 0,$$

λαμβάνουμε

$$(B_i v_i)^{m_i} + \Delta_{i\,1} F_{i\,1}(v_1)\ (B_i v_i)^{m_i - 1} + \cdots + \Delta_{i\,m_i}\ F_{i\,m_i}(v_1)\ B_i^{m_i - 1} = 0$$

$$\Longrightarrow (B_i v_i)^{m_i} + \Delta_{i\,1} G_{i\,1}(v_1)\ a_{i\,1}\,(B_i v_i)^{m_i - 1} + \cdots + \Delta_{i\,m_i}\ G_{i\,m_i}(v_1)\ a_{i\,m_i}\ B_i^{m_i - 1} = 0$$

$$\Longrightarrow (B_i v_i)^{m_i} + [B_i\, a_{i\,1}]\ (B_i v_i)^{m_i - 1} + \cdots + [B_i a_{i\,m_i}]\ B_i^{m_i - 1} = 0.$$

Επειδή $B_i\, a_{i\,j} = \Delta_{i\,j} F_{i\,j}(v_1) \in \mathbf{k}[v_1],\ \forall j \in \{1, 2, \ldots, m_i\}$, από την τελευταία αυτή εξίσωση συνάγουμε ότι όλα τα $B_i v_i$ είναι αλγεβρικά υπεράνω τού $\mathbf{k}[v_1]$. Ας θεωρήσουμε τώρα *οιοδήποτε* στοιχείο $z \in L = \mathbf{k}_1[v_2, \ldots, v_n]$. Το $z$ θα γράφεται υπό τη μορφή

$$z = \sum \lambda_{(\xi_1, \xi_2, \ldots, \xi_n)}\ v_1^{\xi_1}\, v_2^{\xi_2}\ \cdots\ v_n^{\xi_n}.$$

Εάν επιλέξουμε για κάθε $i \in \{2, ..., n\}$ έναν φυσικό αριθμό $N_i$, τέτοιον ώστε να ισχύει $N_i > \xi_i$ για *κάθε* $\xi_i$ που εμφανίζεται σε έναν έκαστο των προσθετέων *ως εκθέτης τού* $v_i$ (στην ανωτέρω παράσταση τού $z$), καθώς και έναν φυσικό αριθμό $N$, τέτοιον ώστε $N > \max\{N_i \mid 2 \leq i \leq n\}$, τότε, θέτοντας

$$\mathcal{B} := B_2 \cdot B_3 \cdot \cdots \cdot B_n \in \mathbf{k}[v_1],$$

θα έχουμε

$$\begin{aligned} \mathcal{B}^N \cdot z &= (B_2 \cdot B_3 \cdot \cdots \cdot B_n)^N \cdot z \\ &= \sum \lambda'_{(\varrho_2, \ldots, \varrho_n, \xi_1, \ldots, \xi_n)}\ B_2^{\varrho_2}\, B_3^{\varrho_3}\ \cdots\ B_n^{\varrho_n}\, v_1^{\xi_1}\ (B_2 v_2)^{\xi_2}\ \cdots\ (B_n v_n)^{\xi_n}, \end{aligned}$$

όπου οι $\varrho_2, \ldots, \varrho_n$ είναι κατάλληλοι εκθέτες $\geq 0$ (εμφανιζόμενοι αναγκαίως λόγω των επιλογών των $N_i$ και $N$). Τόσο τα $B_i$ και $B_i v_i$, όσο και το $v_1$, είναι αλγεβρικά υπεράνω τού $\mathbf{k}[v_1]$. Ως εκ τούτου, κατά το πόρισμα 1.10.3, και οι εκάστοτε δυνάμεις $B_i^{\varrho_i}$, $(B_i v_i)^{\xi_i}$, $v_1^{\xi_1}$, καθώς και τα αθροίσματά τους, αποτελούν αλγεβρικά στοιχεία υπεράνω τού $\mathbf{k}[v_1]$. Άρα τελικώς και το $\mathcal{B}^N \cdot z$, όπου $\mathcal{B} \in \mathbf{k}[v_1]$ και $z \in L$, θα είναι αλγεβρικό υπεράνω τού $\mathbf{k}[v_1]$. (Ιδιαιτέρως, το $\mathcal{B}^N \cdot z$, όπου $\mathcal{B} \in \mathbf{k}[v_1]$ και $z \in \mathbf{k}[v_1] \subseteq \mathbf{k}(v_1)$, θα είναι αλγεβρικό υπεράνω τού $\mathbf{k}[v_1]$.) Κι επειδή το $v_1$, κατά την υπόθεσή μας, είναι υπερβατικό, θα ισχύει

$$\mathbf{k}_1 = \mathbf{k}(v_1) \cong \mathbf{k}(\mathsf{X}).$$

(Πρβλ. **(i)**, περίπτωση πρώτη). Αυτό όμως είναι *άτοπο* βάσει τής ασκήσεως **A-1-66** (b). Επομένως, το $v_1$ πρέπει να είναι όντως αλγεβρικό. □

## Ασκήσεις

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

(a) Να αποδειχθεί ότι το $L = \mathbf{k}[\mathsf{X}] \,/\, \langle F \rangle$ είναι ένα σώμα και ότι, εάν το $x$ είναι η κλάση υπολοίπων τού $\mathsf{X}$ εντός τού $L$, τότε $F(x) = 0$.
(b) Εάν υποτεθεί ότι το $L'$ είναι μια σωματική επέκταση τού $\mathbf{k}$ και $y \in L'$, ούτως ώστε να ισχύει $F(y) = 0$, να αποδειχθεί ότι ο ομομορφισμός $\mathbf{k}[\mathsf{X}] \to L'$, ο οποίος απεικονίζει το $\mathsf{X}$ στο $y$, επάγει έναν ισομορφισμό $L \cong \mathbf{k}(y)$.

(c) Με τα $L'$ και $y$ όπως στο (b), να αποδειχθεί ότι το $F$ διαιρεί το $G$, για κάθε $G \in \mathbf{k}[\mathsf{X}]$ για το οποίο $G(y) = 0$.

(d) Να αποδειχθεί ότι $F = (X - x) \cdot H$, για κάποιο $H \in L[\mathsf{X}]$.

**A-1-69**. Έστω $\mathbf{k}$ ένα σώμα και έστω $F \in \mathbf{k}[\mathsf{X}]$ ένα πολυώνυμο βαθμού $n \geq 1$. Να αποδειχθεί ότι υπάρχει ένα σώμα $L$, το οποίο περιέχει το $\mathbf{k}$, ούτως ώστε να ισχύει

$$F = \lambda \prod_{i=1}^{n} (\mathsf{X} - x_i) \in L[\mathsf{X}], \quad \lambda, x_1, \ldots, x_n \in L.$$

(*Υπόδειξη*: Να χρησιμοποιηθεί η άσκηση **A-1-68** (d) και επαγωγή επί τού $n$.) Το $L$ καλείται **σώμα διασπάσεως** τού $F$.

**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 $F = \lambda \prod_{i=1}^{n} (\mathsf{X} - x_i) \in L[\mathsf{X}]$. Να αποδειχθεί ότι τα $x_1, \ldots, x_n$ είναι σαφώς διακεκριμένα (ήτοι ανα δύο διαφορετικά).

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

(a) Για κάθε στοιχείο $v$ τού $L$, υπάρχει ένα μη μηδενικό στοιχείο $a \in R$, τέτοιο ώστε το $av$ να είναι ακέραιο υπεράνω τού $R$.

(b) Υπάρχει μια βάση $\{v_1, \ldots, v_m\}$ τού $L$ υπεράνω τού $\mathbf{k}$ (με το $L$ θεωρούμενο ως διανυσματικός χώρος υπεράνω τού $\mathbf{k}$), τέτοια ώστε κάθε $v_j, 1 \leq j \leq m$, να είναι ακέραιο υπεράνω τού $R$.